e-Cert (Server) User Guide

For Apache Web Server

Revision Date: June 2018

Table of Content

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 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 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 Apache 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	Specify organizational unit	My Organizational Unit
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**, 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.*

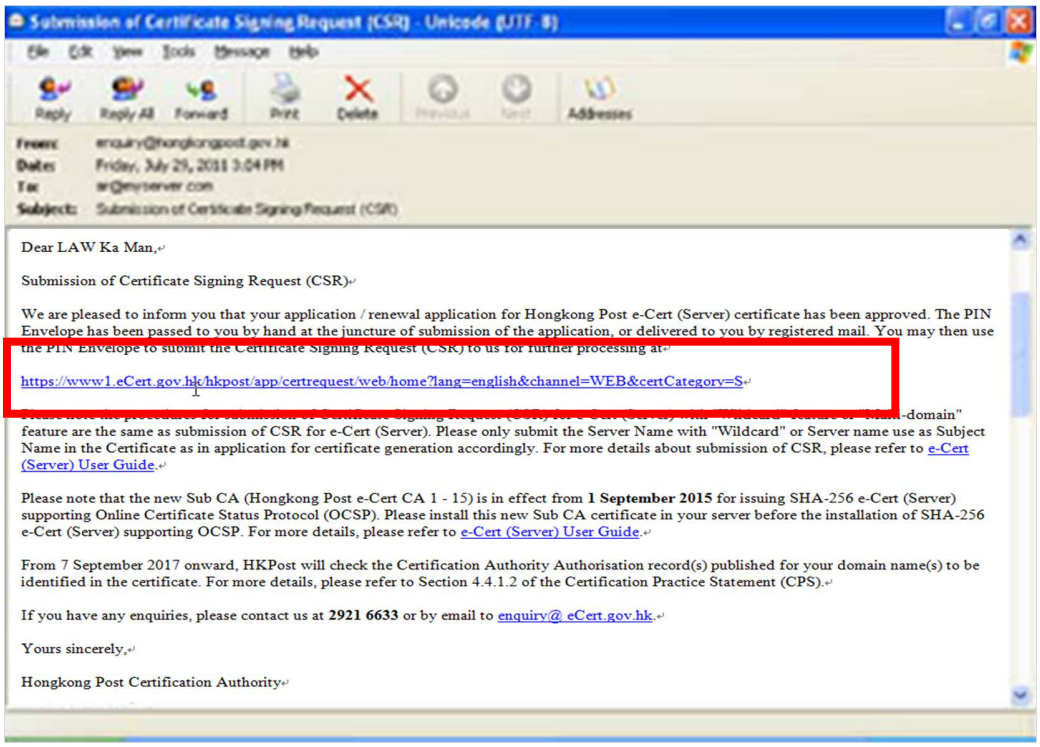
***For application of e-Cert (Server) with "Wildcard" feature,** please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.*

```
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) []:My Organizational Unit
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 []:
```

C. Submitting Certificate Signing Request (CSR)

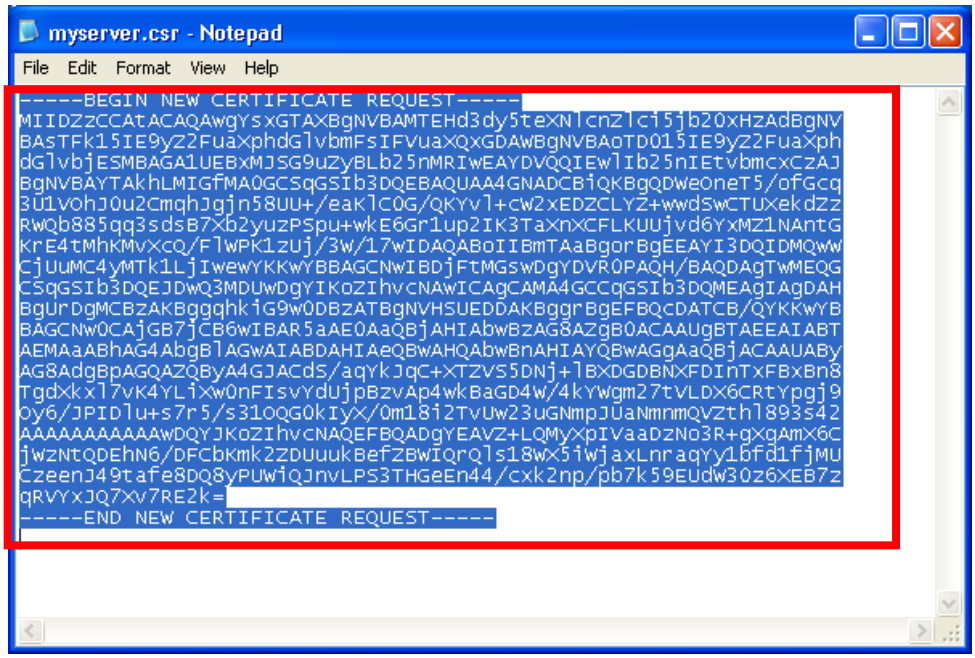
1. Click on the hyperlink in the e-mail with subject "Submission of Certificate Signing Request (CSR)" sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.



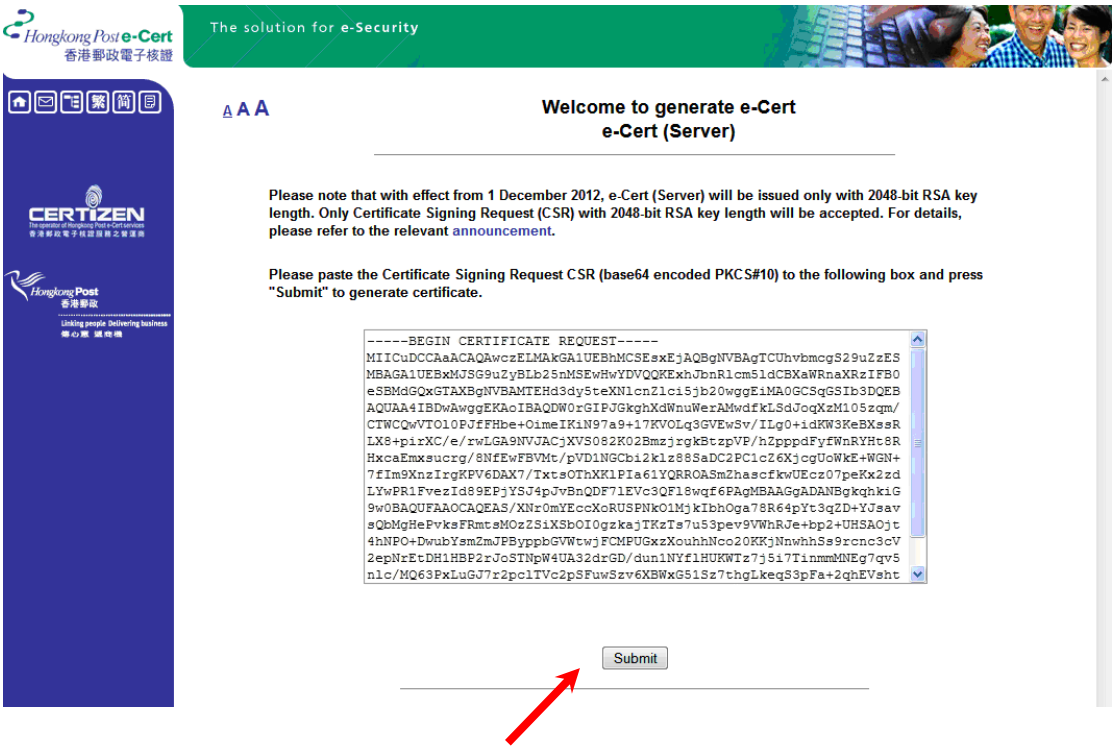
2. Type the "Server Name", the "Reference Number" (9-digit) as shown on the cover of the PIN Envelope and the "e-Cert PIN" (16-digit) as shown inside the PIN Envelope, and then click "Submit".

3. Click “Submit” to confirm the application information. (If the information is incorrect, please contact Hongkong Post Certification Authority.)

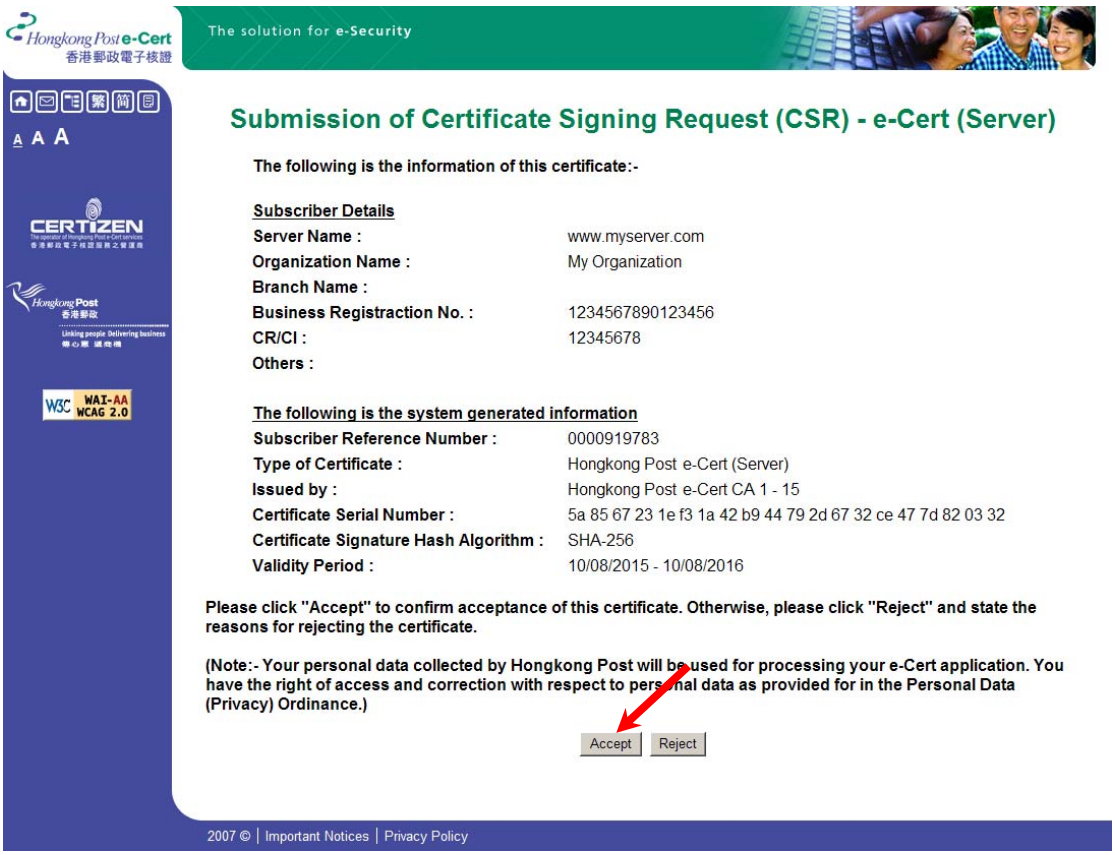
4. Open the Certificate Signing Request (CSR) that you previously generated in Part B Step 2 with a text editor (e.g. Notepad) and copy the entire content including the lines "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----".



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.*
   http://www.eCert.gov.hk/en/sc
2. *e-Cert (Server) supporting OCSP will be issued by default starting from 1 September 2015. For e-Cert (Server) supporting OCSP, Hongkong Post e-Cert CA 1 - 15 should be installed on your server instead of "Hongkong Post e-Cert CA 1 - 10" or "Hongkong Post e-Cert CA 1 - 14". Click following link to download:*
   http://www1.eCert.gov.hk/root/ecert_ca_1-15_pem.crt
3. *If SHA-1 e-Cert (Server) with 1-year validity period is issued upon your written request, the "Hongkong Post e-Cert CA 1 - 10" certificate should be installed on your server instead of "Hongkong Post e-Cert CA 1 - 14" or "Hongkong Post e-Cert CA 1 - 15". Click following link to download:*
   http://www1.eCert.gov.hk/root/ecert_ca_1-10_pem.crt
4. *If SHA-256 e-Cert (Server) not supporting OCSP with 1-year validity period is issued upon your written request, the "Hongkong Post e-Cert CA 1 - 14" certificate should be installed on your server instead of "Hongkong Post e-Cert CA 1 - 10" or "Hongkong Post e-Cert CA 1 - 15". Click following link to download:*
   http://www1.eCert.gov.hk/root/ecert_ca_1-14_pem.crt
5. *HongKong Post e-Cert Root CA 1 can be downloaded from Hong Kong Post web site:*
   http://www1.eCert.gov.hk/root/root_ca_1_pem.crt


Hongkong Post e-Cert
The solution for e-Security
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
CERTIZEN
2007 © | Important Notices | Privacy Policy

D. Installing Server Certificate

1. Copy the private key that you previously generated in Part B Step 1 and the 3 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 SHA-256 e-Cert (Server) supporting OCSP
   ```
   /usr/local/apache/conf/ssl.key/myserver.key
   /usr/local/apache/conf/ssl.crt/cert0000812104.cer
   /usr/local/apache/conf/ssl.crt/ecert_ca_1-15_pem.crt
   /usr/local/apache/conf/ssl.crt/root_ca_1_pem.crt
   ```
   b) For installation of SHA-256 e-Cert (Server) not supporting OCSP
   ```
   /usr/local/apache/conf/ssl.key/myserver.key
   /usr/local/apache/conf/ssl.crt/cert0000812104.cer
   /usr/local/apache/conf/ssl.crt/ecert_ca_1-14_pem.crt
   /usr/local/apache/conf/ssl.crt/root_ca_1_pem.crt
   ```
   c) For installation of SHA-1 e-Cert (Server)
   ```
   /usr/local/apache/conf/ssl.key/myserver.key
   /usr/local/apache/conf/ssl.crt/cert0000812104.cer
   /usr/local/apache/conf/ssl.crt/ecert_ca_1-10_pem.crt
   /usr/local/apache/conf/ssl.crt/root_ca_1_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 both the "Hongkong Post e-Cert CA 1 - 15" certificate ("Hongkong Post e-Cert CA 1 - 10" certificate or "Hongkong Post e-Cert CA 1 - 14" certificate) and the "Hongkong Post Root CA 1" certificate.

   a) For installation of SHA256 e-Cert (Server) supporting OCSP
   ```
   cat root_ca_1_pem.crt ecert_ca_1-15_pem.crt >
   hkpostca.crt
   ```
   b) For installation of SHA256 e-Cert (Server) not supporting OCSP
   ```
   cat root_ca_1_pem.crt ecert_ca_1-14_pem.crt >
   hkpostca.crt
   ```
   c) For installation of SHA1 e-Cert (Server)
   ```
   cat root_ca_1_pem.crt ecert_ca_1-10_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 _default_:443>

# Private Key
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/myserver.key
# Hongkong Post e-Cert (Server)
SSLCertificateFile /usr/local/apache/conf/ssl.crt/cert0000812084.cer
# Hongkong Post Root 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 startssl