电子证书（伺服器）用户指南

Nginx 网页伺服器适用

修订日期：2023 年3 月

目录

A. 电子证书（伺服器）申请人指引 2
B. 产生证书签署要求(CSR)..... 3
C. 提交证书签署要求(CSR)..... 6
D. 安装伺服器证书..... 11

A. 电子证书（伺服器）申请人指引

香港邮政核证机关在收到及批核电子证书（伺服器）申请后，会向获授权代表发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮，要求获授权代表到香港邮政核证机关的网站提交 CSR。

本用户指南旨在提供参考给电子证书（伺服器）申请人如何在 nginx 网页伺服器上产生配对密码匙和证书签署要求(CSR)的详细步骤。包含公匙的 CSR 将会提交到香港邮政核证机关以作证书签署。

如阁下在证书签发后遗失密码匙，您将不能安装或使用该证书。因此强烈建议阁下于**提交证书签署要求(CSR)前**为密码匙进行备份。

B. 产生证书签署要求(CSR)

1. 本用户指南使用来自 OpenSSL 软件包的“openssl” 公用程式产生配对密码匙和证书签署要求(CSR) 以作参考。由于个别伺服器的公用程式所在目录路径各有不同，所以申请人应参考本身伺服器的相关文件。

   于提示符输入以下指令产生一个用 Triple-DES (3DES) 加密的 2048 位元的 RSA 密码匙(myserver.key)。 您将被提示输入及确认密码。

   注意：小于 2048 位元的密码匙或未能提供足够保密程度，相反大于 2048 位元有可能与某些浏览器不兼容。建议选择长度为 2048 位元的密码匙，从而提供较佳的保密程度。

   注意：请牢记这个非常重要的密码。 当您启动您的 nginx 伺服器时，您需要提供此密码。

   ```
   openssl genrsa -des3 -out myserver.key 2048
   ```

2. 于提示符输入以下指令用上述制作的密码匙(myserver.key)产生一个证书签署要求(CSR)(myserver.csr)。您将被提示输入密码。

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

   当指令提示以下 X.509 证书属性时，请输入以下资料：

属性	描述	范例
Country	输入 “HK”	HK
State or Province	输入 “Hong Kong”	Hong Kong
Locality	输入 “Hong Kong”	Hong Kong
Organization	输入公司名称	My Organization
Organizational Unit	按 <Enter> 留空	
Common Name	输入伺服器名称	www.myserver.com
Email Address	按 <Enter> 留空	

   您亦会被提示输入其他属性（即 challenge password 及 optional company name）。按 <Enter> 将它们留空。

注意：请确保于「Common Name」一栏输入正确的登记伺服器名称及「Country Name」一栏输入「HK」。

注意：若申请电子证书（伺服器）"多域版"或延伸认证电子证书（伺服器）"多域版"，请在「Common Name」一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名 称」相同的登记伺服器名称。而「电子证书主体别名内的额外伺服器名 称」，则无需在产生证书签署要求(CSR)过程中输入，香港邮政核证机关 系统在签发证书时，会根据申请表格所申请的资料自动填写。

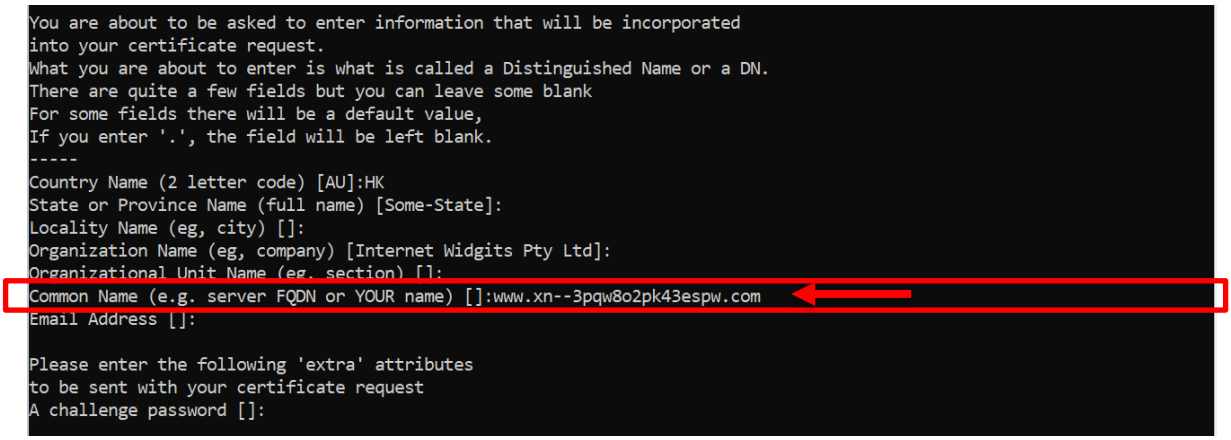
若申请电子证书（伺服器）"通用版"，请在「Common Name」一欄中，输入与申请表格中所填写的「有通配符的电子证书伺服器名称」相同的登记伺服器名称(伺服器名称的最左部份需包括有通配符「」的部份)。例如 *.myserver. com。*

```
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 []:
```

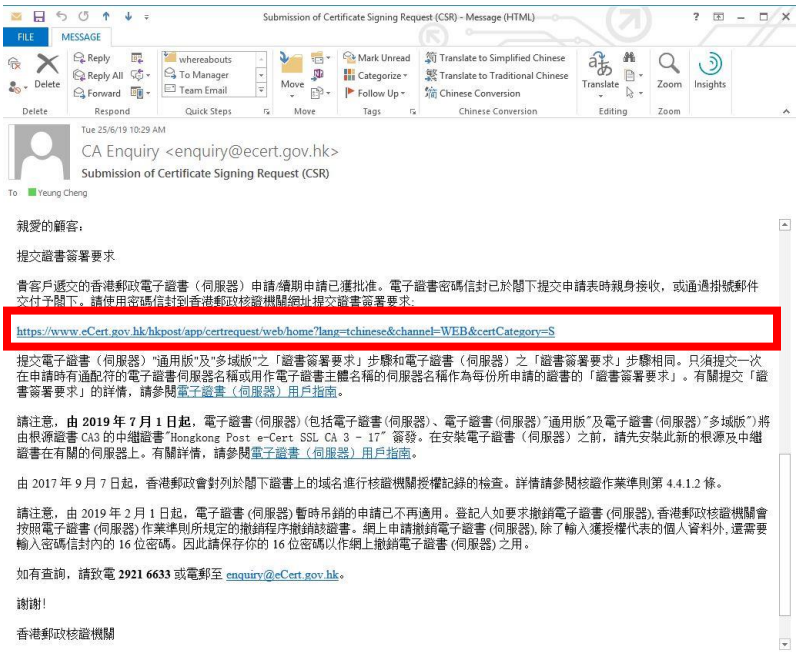
注意:若申请中文伺服器名称的电子证书（伺服器），请使用国际网域名称转换工具把中文网域名称转换成 ASCII 字元，并可以在"通用名称"一栏中输入转换后的名称。

转换前	转换后
www. 我的伺服器.com	www.xn--3pqw8o2pk43espw.com



C. 提交证书签署要求(CSR)

1. 在香港邮政核证机关发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮内按一下超连结以连线至香港邮政核证机关的网站。



2. 输入[伺服器名称]、印于密码信封面的[参考编号](九位数字)及印于密码信封内的[电子证书密码]（十六位数字），然后按[**提交**]。

3. 按［**提交**］确认申请资料。(如发现资料不正确，请电邮至 enquiry@eCert.gov.hk 联络香港邮政核证机关。)

注意：若电子证书申请表格上提供了机构中文名称和/或分部中文名称，如要发出一张主体名称为机构中文名称的电子证书（伺服器），请按[确认使用中文]键。

4. 用文字编辑器(例如：记事本)开启早前产生的证书签署要求(CSR)及复制全部内容包括 “-----BEGIN NEW CERTIFICATE REQUEST-----” 及 “-----END NEW CERTIFICATE REQUEST-----” 。(您可参考 B 部的步骤 6 的证书要求文件的位置。)

5. 在方格内贴上内容，然后按[**提交**]。

6. 按［**接受**］确认接受此证书。

7. 下载 Hongkong Post e-Cert (Server)证书。

注意：

1. *您也可以从搜索及下载证书网页下载您的电子证书（伺服器）。*
   http://www.eCert.gov.hk/tc/sc/index_c.html
2. *就所有类型的电子证书（伺服器）而言：*

   安装由根源证书 Root CA3 签发的中继证书"Hongkong Post e-Cert SSL CA3 - 17"。 可于以下网址下载：
   http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

   安装交叉证书"Hongkong Post Root CA 3 (交叉证书 2022)"。 可于以下网址下载：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

3. *就所有类型的延伸认证电子证书（伺服器）而言：*

   安装由根源证书 Root CA3 签发的中继证书"Hongkong Post e-Cert EV SSLCA 3 - 17"。 可于以下网址下载：
   http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt

   安装交叉证书"Hongkong Post Root CA 3 (交叉证书 2022）"。可于以下网址下载：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安装伺服器证书

1. 将早前于 B 部的步骤 1 所产生的密码匙及于 C 部的步骤 7 下载的三个证书档案复制到下列 nginx 伺服器的目录内。(根据不同系统，目录路径可能有所不同。)

   例如：

   a) 安装由中继证书 **"Hongkong Post e-Cert SSL CA 3 - 17"** 签发的**电子证书（伺服器）：**

   ```
   /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) 安装由中继证书 **"Hongkong Post e-Cert EV SSL CA 3 - 17"** 签发的**延伸认证电子证书（伺服器）：**

   ```
   /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. 换到 nginx 伺服器的证书档案目录 (例如：/etc/nginx/ssl.crt/) 内，然后于提示符输入以下指令制作一个包含中继证书及交叉证书的证书链档案 (myserver_hkpostca.crt)。

   例如：

   a）安装由中继证书 **"Hongkong Post e-Cert SSL CA 3 - 17"** 签发的**电子证书（伺服器）：**

   ```
   cat cert0000812104.cer ecert_ssl_ca_3-17_pem.crt
   root_ca_3_x_gsca_r3_pem.crt > myserver_hkpostca.crt
   ```

   b）安装由中继证书 **"Hongkong Post e-Cert EV SSL CA 3 - 17"** 签发的**延伸认证电子证书（伺服器）：**

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

3. 用文字编辑器打开 nginx HTTPS 配置文件案 (例如：/etc/nginx/nginx.conf)。

4. 找出您的 HTTPS server 区块，然后于虚拟伺服器区块内更改以下设定。如果设定不存在，请自行加上。

```
# 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. 储存变更及离开文字编辑器。

6. 于提示符输入以下指令重新启动您的 nginx 伺服器。 (根据不同系统，指令可能有所不同。)

```
systemctl stop nginx

systemctl start nginx
```