Hongkong Post e-Cert
香港郵政電子核證

電子證書（伺服器）用戶指南

Nginx 網頁伺服器適用

修訂日期：2023 年 3 月

目錄

A. 電子證書（伺服器）申請人指引

香港郵政核證機關在收到及批核電子證書 (伺服器) 申請後，會向獲授權代表發出主旨為 “Submission of Certificate Signing Request (CSR)” 的電郵，要求獲授權代表到香港郵政核證機關的網站提交 CSR。

本用戶指南旨在提供參考給電子證書（伺服器）申請人如何在 nginx 網頁伺服器上產生配對密碼匙和證書簽署要求(CSR)的詳細步驟。包含公匙的 CSR 將會提 交到香港郵政核證機關以作證書簽署。

如閣下在證書簽發後遺失密碼匙，您將不能安裝或使用該證書。因此強烈建議閣下於**提交證書簽署要求(CSR)前**為密碼匙進行備份。

B. 產生證書簽署要求(CSR)

1. 本用戶指南使用來自 OpenSSL 軟件包的 “openssl” 公用程式產生配對 密碼匙和證書簽署要求(CSR) 以作參考。由於個別伺服器的公用程式所 在目錄路徑各有不同，所以申請人應參考本身伺服器的相關文件。

   於提示符輸入以下指令產生一個用 Triple-DES (3DES) 加密的 2048 位元的 RSA 密碼匙(myserver.key)。您將被提示輸入及確認密碼。

   注意：小於 2048 位元的密碼匙或未能提供足夠保密程度，相反大於 2048 位元有可能與某些瀏覽器不兼容。建議選擇長度為 2048 位元的密碼匙，從而提供較佳的保密程度。

   注意：請牢記這個非常重要的密碼。當您啟動您的 nginx 伺服器時，您需要提供這個密碼。

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

2. 於提示符輸入以下指令用上述制作的密碼匙(myserver.key)產生一個證書簽署要求(CSR)(myserver.csr)。您將被提示輸入密碼。

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

   當指令提示以下 X.509 證書屬性時，請輸入以下資料：

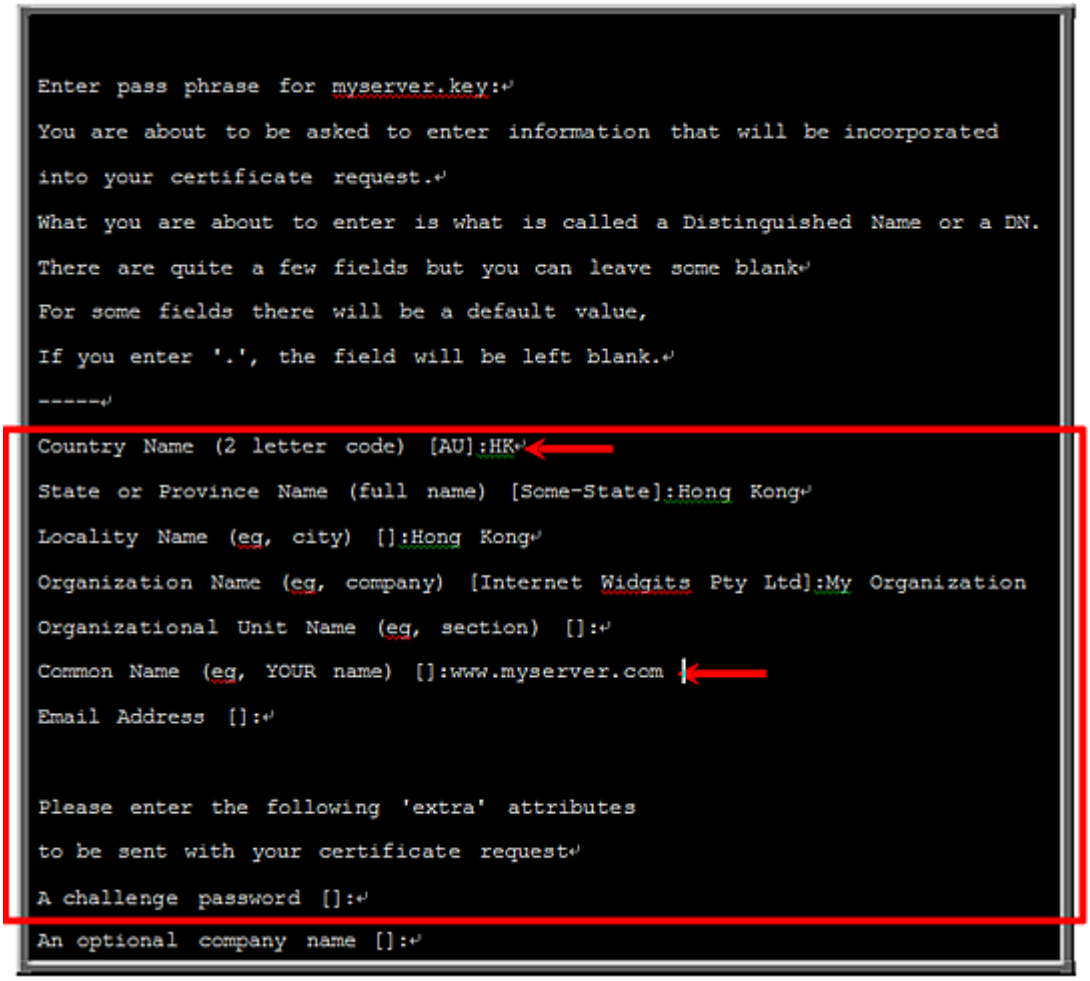
屬性	描述	範例
Country	輸入 “HK”	HK
State or Province	輸入 “Hong Kong”	Hong Kong
Locality	輸入 “Hong Kong”	Hong Kong
Organization	輸入公司名稱	My Organization
Organizational Unit	按 <Enter> 留空	
Common Name	輸入伺服器名稱	www.myserver.com
Email Address	按 <Enter> 留空	

   您亦會被提示輸入其他屬性 (即 challenge password 及 optional company name)。按 <Enter> 將它們留空。

注意：請確保於「Common Name」一欄輸入正確的登記伺服器名稱及「Country Name」一欄輸入「HK」。

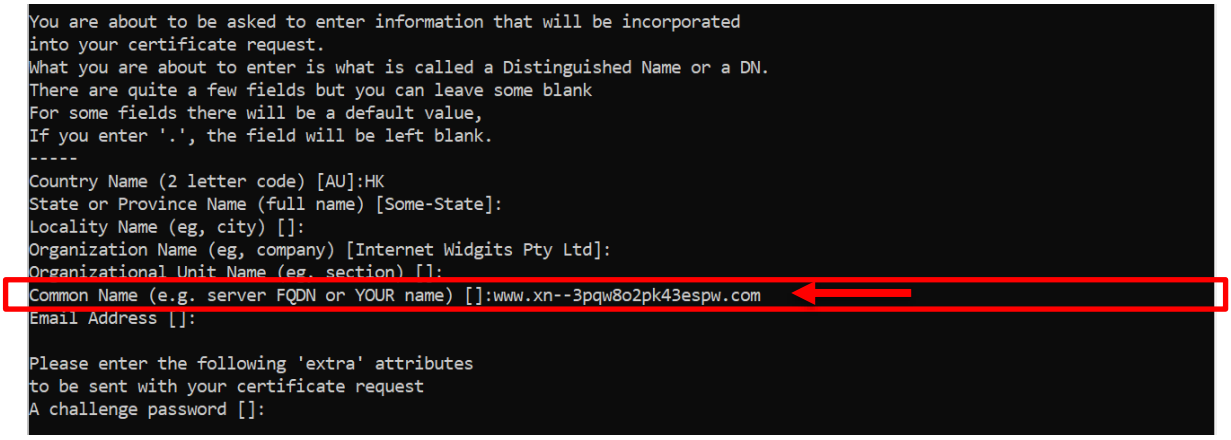
注意：若申請電子證書（伺服器）“多域版”或延伸認證電子證書（伺服器）“多域版”,請在「Common Name」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。而「電子證書主體別名內的額外伺服器名稱」，則無需在產生證書簽署要求(CSR)過程中輸入，香港郵政核證機關系統在簽發證書時，會根據申請表格所申請的資料自動填寫。

*若申請電子證書(伺服器) “通用版”，請在「Common Name」一欄中，輸入與申請表格中所填寫的「有通配符的電子證書伺服器名稱」相同的登記伺服器名稱(伺服器名稱的最左部份需包括有通配符「＊」的部份)。例如 *.myserver.com。*



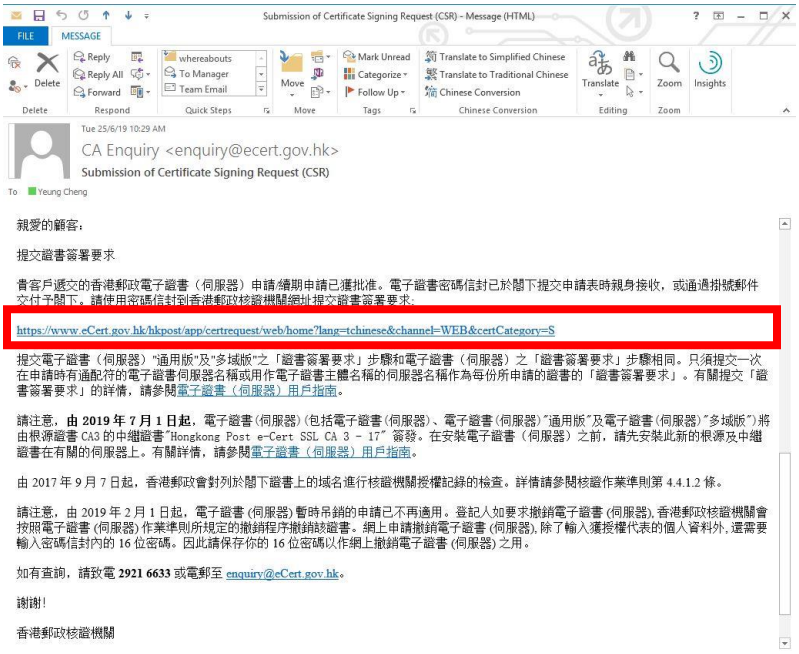
注意:若申請中文伺服器名称的電子證書（伺服器），請使用國際網域名稱轉換工具把中文網域名稱轉換成 ASCII 字元，並可以在"通用名稱"一欄中輸入轉換後的名稱。

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



C. 提交證書簽署要求(CSR)

1. 在香港郵政核證機關發出主旨為 “Submission of Certificate Signing Request (CSR)” 的電郵內按一下超連結以連線至香港郵政核證機關的網站。

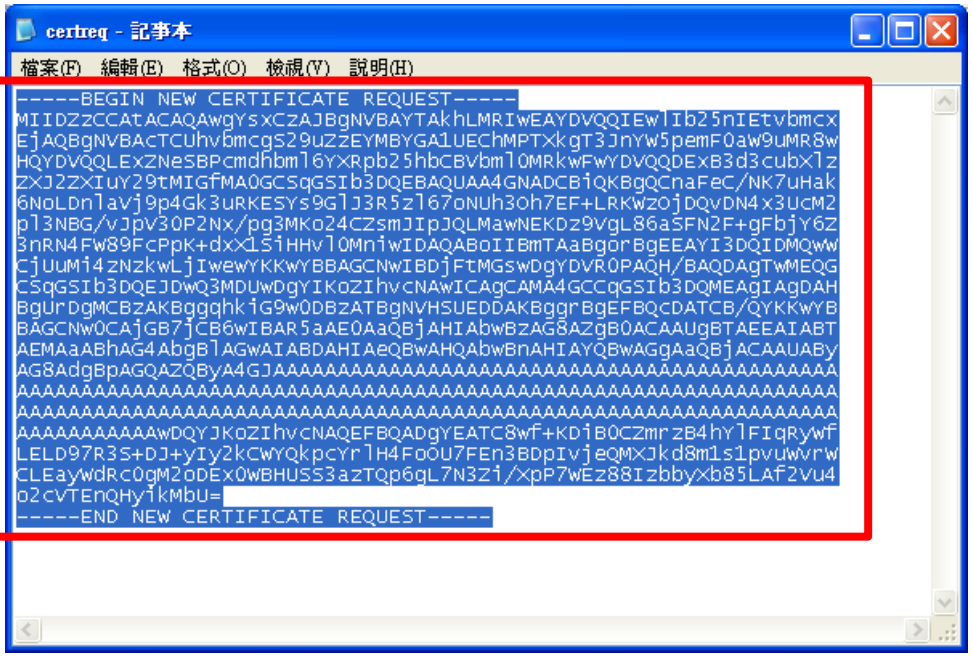


2. 輸入[伺服器名稱]、印於密碼信封面的[參考編號](九位數字)及印於密碼 信封內的[電子證書密碼](十六位數字)，然後按[提交]。

3. 按[提交]確認申請資料。(如發現資料不正確，請電郵至 enquiry@eCert.gov.hk 聯絡香港郵政核證機關。)

注意：若電子證書申請表格上提供了機構中文名稱和/或分部中文名稱，如要發出一張主體名稱為機構中文名稱的電子證書(伺服器)，請按[確認使用中文]鍵。

4. 用文字編輯器(例如：記事本)開啟早前產生的證書簽署要求(CSR)及複製全部內容包括 “-----BEGIN NEW CERTIFICATE REQUEST-----” 及 “-----END NEW CERTIFICATE REQUEST-----” 。(您可參考 B 部的步驟 6 的憑證要求檔案的位置。)



5. 在方格內貼上內容，然後按[提交]。

6. 按 [**接受**] 確認接受此證書。

7. 下載 Hongkong Post e-Cert (Server)證書。

注意：

1. *您也可以從搜尋及下載證書網頁下載您的電子證書（伺服器）。*
   http://www.eCert.gov.hk/tc/sc/index_c.html
2. *就所有類型的電子證書（伺服器）而言:*

   安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert SSL CA3 - 17"。可於以下網址下載：
   http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

   安裝交叉證書"Hongkong Post Root CA 3（交叉證書 2022）"。可於以下網址下載：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

3. *就所有類型的延伸認證電子證書（伺服器）而言:*

   安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert EV SSLCA 3 - 17"。可於以下網址下載：
   http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt

   安裝交叉證書"Hongkong Post Root CA 3（交叉證書 2022）"。可於以下網址下載：
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安裝伺服器證書

1. 將早前於 B 部的步驟 1 所產生的密碼匙及於 C 部的步驟 7 下載的三個證書檔案複製到下列 nginx 伺服器的目錄內。(根據不同系統，目錄路徑可能有所不同。)

   例如：

   a) 安裝由中繼證書“Hongkong Post e-Cert SSL CA 3 - 17”簽發的**電子證書（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) 安裝由中繼證書“Hongkong Post e-Cert EV SSL CA 3 - 17”簽發的**延伸認證電子證書（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. 換到 nginx 伺服器的證書檔案目錄(例如：/etc/nginx/ssl.crt/) 內，然後於提示符輸入以下指令制作一個包含中繼證書及交叉證書的證書鏈檔案(myserver_hkpostca.crt)。

   例如：

   a) 安裝由中繼證書“Hongkong Post e-Cert SSL CA 3 - 17”簽發的**電子證書（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) 安裝由中繼證書“Hongkong Post e-Cert EV SSL CA 3 - 17”簽發的**延伸認證電子證書（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. 用文字編輯器打開 nginx HTTPS 組態設定檔案(例如：/etc/nginx/nginx.conf)。

4. 找出您的 HTTPS server 區塊，然後於虛擬伺服器區塊內更改以下設定。如果設定不存在，請自行加上。

```
# 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. 儲存變更及離開文字編輯器。

6. 於提示符輸入以下指令重新啟動您的 nginx 伺服器。(根據不同系統，指令可能有所不同。)

```
systemctl stop nginx

systemctl start nginx
```