



## 電子證書（伺服器）用戶指南

**Nginx** 網頁伺服器適用

## 目錄

|                         |    |
|-------------------------|----|
| A. 電子證書（伺服器）申請人指引 ..... | 2  |
| B. 產生證書簽署要求(CSR) .....  | 3  |
| C. 提交證書簽署要求(CSR) .....  | 6  |
| D. 安裝伺服器證書 .....        | 12 |

## 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 AES-256 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 -aes256 -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。

```
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:若申請中文伺服器名稱的電子證書（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。

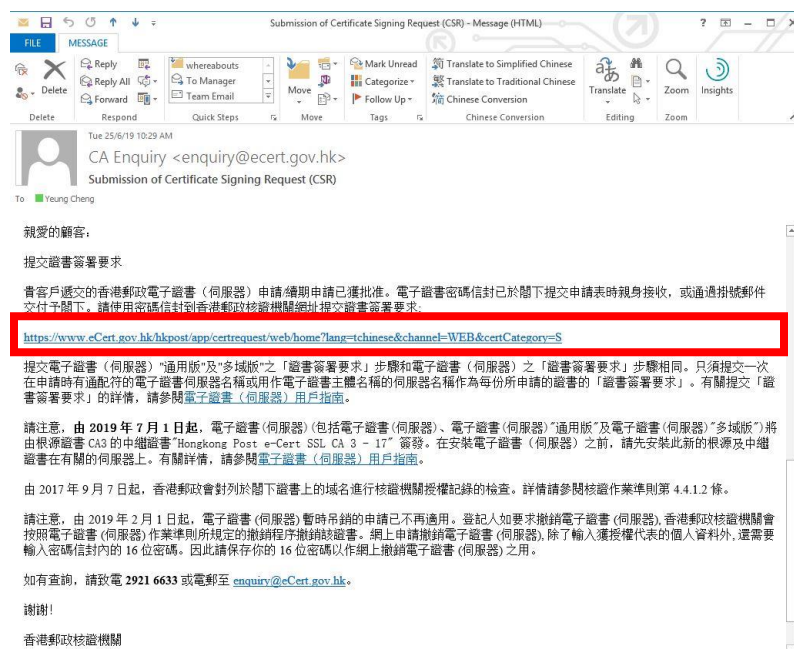
| BeforeConversion | After Conversion            |
|------------------|-----------------------------|
| www.我的伺服器.com    | www.xn--3pqw8o2pk43espw.com |

```
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) []:
Common Name (e.g. server FQDN or YOUR name) []:www.xn--3pqw8o2pk43espw.com
Email Address []:
```

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

## 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]。



香港郵政電子核證



CERTIZEN



香港郵政



W3C WAI-AA WCAG 2.0

The solution for e-Security

### 提交「簽發證書要求」- 電子證書（伺服器）

你在此申請表格所填報的個人資料，香港郵政及其電子核證服務之營運商會用作為你提供電子證書服務的事宜。除非所作用途為法例容許又或屬法例規定，否則我們不會用足以辨識你身分的方式，向他人披露你的資料。你向我們提供你的個人資料，全屬自願性質。如未能提供有關資料，可能會影響處理你的電子證書申請。根據《個人資料（私隱）條例》，你有權查閱或更改香港郵政保存有關你的個人資料。如常查閱或更改資料，請填妥《查閱資料要求表格》(Pos736) 或《改正個人資料要求表格》(Pos736A)，然後交回任何一間郵政局或寄交香港郵政個人資料私隱主任。《查閱資料要求表格》和《改正個人資料要求表格》亦可於各郵政局索取。

伺服器資料：

伺服器名稱：

電子證書密碼信封資料：

參考編號：  
(印於密碼信封面；九位數字)

電子證書密碼：  
(十六位數字密碼內的空白地方無須填寫)

請注意，由2025年5月1日起，電子證書（伺服器）會以新中繼證書簽發。為確保順利過渡，請：

1. 從你的伺服器中移除舊有中繼證書（如適用）。
2. 下載並安裝新中繼證書（標示為「自2025年5月1日起生效」）。
3. 安裝於2025年5月1日或之後簽發的電子證書（伺服器）。

有關詳情，請參閱電子證書（伺服器）用戶指南。

不包含EKU欄位的舊有中繼證書將於2026年6月15日之前被撤銷。

2007 © | 重要告示 | 私隱政策

- 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。)



The screenshot shows the '提交「簽發證書要求」 - 電子證書（伺服器）' (Submit Certificate Request - Electronic Certificate (Server)) form on the Hong Kong Post e-Cert website. The form is titled '提交「簽發證書要求」 - 電子證書（伺服器）' and is part of the 'The solution for e-Security' initiative. It includes a sidebar with logos for CERTIZEN, Hong Kong Post, and W3C. The main content area contains a table for registration details and a section for certificate information.

| 登記人資料              |                                                                                   |
|--------------------|-----------------------------------------------------------------------------------|
| 伺服器名稱：             | www.ecert.gov.hk                                                                  |
| 機構名稱：              | Hong Kong SAR Government<br>香港特別行政區政府<br>HKPO-Business Development Branch<br>香港郵政 |
| 分行/部門名稱：           |                                                                                   |
| 商業登記證編號：           |                                                                                   |
| 公司註冊證編號 / 公司登記證編號： |                                                                                   |
| 其他註冊證明文件：          | HKPO-BDB                                                                          |

| 有關所申請的電子證書的資料 |           |
|---------------|-----------|
| 證書類型：         | 電子證書（伺服器） |
| 登記期：          | 1年        |

此頁用以確認申請資料，如以上資料正確，請按[確認]鍵繼續：  
如選擇在電子證書內顯示「中文機構名稱」，請按[確認使用中文]鍵繼續：

\*如使用中文域名註冊，請務必確認清楚字元正確性，註冊後即不能修改。

2007 © | 重要告示 | 私隱政策

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. （自 **2026 年 3 月 15 日起生效，且僅適用於非政府登記人**）請從適用於您的電子證書（伺服器）的網域控制驗證 (DCV) 方法清單中選擇您所需的方法，並按照螢幕上的指示進行操作。確認後，系統將自動驗證並確認您對電子證書（伺服器）所包含域名的控制權。如果 DCV 驗證成功，您將可以提交 CSR。

（請注意，系統只會顯示適用於您的電子證書（伺服器）類型的驗證方法供您選擇。）

- A. 如選擇「網站變更」網域控制驗證 (DCV) 方法，請下載驗證檔案“fileauth.txt”，並將其上傳到您電子證書（伺服器）所包含的每個域名對應的網站上的指定位置。上傳檔案並確認檔案可公開存取後，按「確認」繼續。**請注意，此方法不適用於電子證書（伺服器）“通用版”。**

The screenshot shows the Hongkong Post e-Cert website interface. The main heading is "提交「簽發證書要求」- 電子證書（伺服器）". Below it, a dropdown menu is set to "網站變更（建議）". The instructions are as follows:

**網域控制驗證 (DCV) 方法：** 網站變更（建議）

**指示：**

- 下載驗證檔案：**  
下載包含驗證碼的驗證檔案 (fileauth.txt)。
- 將驗證檔案上傳到您的網頁伺服器：**  
將檔案上傳到您的電子證書（伺服器）所包含的每個域名對應的網站上的指定位置。該檔案應可透過以下任一網址存取。
  - [http://\[域名\]/well-known/pki-validation/fileauth.txt](http://[域名]/well-known/pki-validation/fileauth.txt)
  - [https://\[域名\]/well-known/pki-validation/fileauth.txt](https://[域名]/well-known/pki-validation/fileauth.txt)
- 檢查檔案：**  
上傳檔案後，請確保可以透過瀏覽器存取任一網址來確認其是否已可公開存取。您應該可以看到驗證檔案內的驗證碼。
- 確認：**  
確認檔案可公開存取後，請按「確認」繼續。您可以稍後返回此頁面完成網域控制驗證 (DCV) 程序，但請務必在30天內完成。否則，您需要使用新的驗證碼完成驗證程序。

Buttons: 確認, 返回上頁

Footer: 2007 © | 重要告示 | 私隱政策

- B. 如選擇「網域名稱系統變更」網域控制驗證 (DCV) 方法，請為您的電子證書（伺服器）所包含的每個域名新增包含驗證碼的 DNS TXT 記錄。新增 DNS 記錄並確保可公開解析後，按「確認」繼續。

Hongkong Post e-Cert  
香港郵政電子核證

The solution for e-Security

提交「簽發證書要求」- 電子證書（伺服器）

網域控制驗證 (DCV) 方法：

指示：

1. 新增 DNS 記錄：  
請為您的電子證書（伺服器）所包含的每個域名新增 DNS TXT 記錄。

記錄類型：TXT  
主機：[域名]  
記錄值：[驗證碼]   
TTL：3600

2. 檢查 DNS 記錄：  
確保 DNS 記錄是可公開解析的。

3. 確認：  
新增 DNS 記錄並確認可公開解析後，請按「確認」繼續。您可以稍後返回此頁面完成網域控制驗證 (DCV) 程序，但請務必在30天內完成。否則，您需要使用新的驗證碼完成驗證程序。

2007 © | 重要告示 | 私隱政策

- C. 如選擇「構建電郵」網域控制驗證 (DCV) 方法，請選擇指定的電子郵件地址，然後按「發送驗證碼」。收到電子郵件後，在網頁中輸入驗證碼，然後按「確認」繼續。**請注意，此方法不適用於電子證書（伺服器）“多域版”。**

Hongkong Post e-Cert  
香港郵政電子核證

The solution for e-Security

提交「簽發證書要求」- 電子證書（伺服器）

網域控制驗證 (DCV) 方法：

指示：

1. 接收驗證碼：  
請選擇指定的電子郵件地址以接收驗證碼。

admin @ [域名]

2. 確認：  
驗證碼：  
輸入驗證碼，然後按「確認」繼續。

2007 © | 重要告示 | 私隱政策

5. 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-----”。在方格內貼上內容，然後按[提交]。


The solution for e-Security



  
A A A



CERTIZEN  
香港電子證書認證中心



Hongkong Post  
香港郵政

Linking people. Enriching business.  
聯心合眾 誠信無欺



## 提交「簽發證書要求」 - 電子證書（伺服器）

**請貼上「簽發證書要求」（Certificate Signing Request, CSR）（已被base64 編碼的PKCS#10）於下面的方格內，並按[提交]鍵繼續。**

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmzCCATMCAQAwKDElMAkGA1UEBhMCSEwGTAxKgNVAzMHEHd3dySlY2VydC5n
bSYuaGSwgwgELMAOGFsc3QoEBAQAQA1BDwawgwEKAoIBAQC1jaStenPcNIz
erGyMa/1W1U1CN/+Pi+qBTQR4m4fAzHoMZDAtOEmKFppzvrvVv/U28eSMJHe6W
GH1L750WvdU19D4WfaAQmhjlv1XkojEuAlwDuuvva+CY1MtDxSWSQwnJ1IKBuNm
2LACC6Ho+OVbeRyDOwgyOvoAWhd8toMDnBIJsv7Q/cWNRSQIzSGCgHSQJaqcTZK
9UX4MOS9OM9/hR7AspR5gqpIXlgNxyDFHburYH30AS3DNuzSoYUkh/jSTx/XkUa
qwqvadhSeSE49yztRmln3com8VfvcKDj11ljyWgo824aIx3yDYfnOTMghNGM1For
e6TExDfAgMBAAAGLJA8BgqhkhIG9wOBCC4KhZadMBsGA1UdeEQUMBECEHd3dySl
Y2VydC5naGSwgwgVYVkdC5nIHRvbnNAQEQLBSQAdggEBAHIS3TX1UJMLNAvZhPlpT+y
zgSe4TE2qyNSseHzYV6/24e/lge06eNPBYb7ANQEBodrl6OLcf8KzmAnFo/d5
7SE7JNhuyky89WQdcjTODIus2BewOkcrZFkvUk+ROEAa+JP8tlxk/4IMOUBudREyY
O/ZmxgHlaTMHfRBOJglzFPW1SS8ddSKH9zxrk3tuA6+7Lzk4aTBkTRhgSySWbt
UjITV4s10tkIEIRU78A/Oz32ULDUxsob3Sh6IRcKxbMuIS/xjalx53GE8wtcnFU
WjNOPe1NJdH7yjzzTyrVMB8ECbvLEKE7+75a445rxlpA25ylbZ43yzTE9whdCYA=
```

2007 © | 重要告示 | 私隱政策

6. 按 **[接受]** 確認接受此證書。



The solution for e-Security



提交「簽發證書要求」 - 電子證書 (伺服器)

以下為你的電子證書內的資料：

|                   |                                  |
|-------------------|----------------------------------|
| 用戶資料              |                                  |
| 伺服器名稱：            | www.ecert.gov.hk                 |
| 機構名稱：             | Hong Kong SAR Government         |
| 分行/部門名稱：          | HKPO-Business Development Branch |
| 商業登記證編號：          |                                  |
| 公司註冊編號 / 公司登記證編號： |                                  |
| 其他註冊證明文件：         | HKPO-BDB                         |

其他資料 (由香港郵政核證機關系統產生)

|          |                                                             |
|----------|-------------------------------------------------------------|
| 登記人參考編號： |                                                             |
| 證書類型：    | Hongkong Post Trial e-Cert (Server)                         |
| 簽發機關：    | Hongkong Post Trial e-Cert SSL CA 3 - 17                    |
| 證書序號：    | 45 b9 30 00 2d 44 89 87 4c 74 c4 88 35 4b d1 92 08 b8 6c 20 |
| 證書有效日期：  | 13/01/2026 - 31/07/2026 (199日)                              |

如使用中文域名註冊，請務必確認清楚字元正確性，註冊後即不能變更或修改。

請按[接受]確認接受上述證書，並同意香港郵政根據電子交易條例的規定將該證書於儲存庫公布。

(注意：香港郵政收集你的個人資料，只會用於處理你的電子證書申請事宜。你有權根據個人資料(私隱)條例的規定，要求查詢及更正你的個人資料。)

接受

不接受

2007 © | 重要告示 | 私隱政策

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



The screenshot shows the Hongkong Post e-Cert website. The header includes the logo and the tagline "The solution for e-Security". The main content area is titled "提交「簽發證書要求」 - 電子證書（伺服器）" and lists three steps: 1. Download "Hongkong Post e-Cert (Server)" certificate, 2. Download Hong Kong Post Root Certificate, and 3. Download Hongkong Post e-Cert (Server) User Guide. A note mentions that users with older versions of the Root CA3 certificate should update to the 2022 version. The footer includes the year 2007 and links to important notices and privacy policy.

提交「簽發證書要求」 - 電子證書（伺服器）

你現可以：

1. 下載 "Hongkong Post e-Cert (Server)" 證書
2. 下載香港郵政根源證書
3. 下載電子證書（伺服器）用戶指南

提示  
為使"未有預載根源證書CA3的舊版本移動/桌面裝置"在根源證書CA1到期後能繼續進入你們已安裝電子證書（伺服器）的網站/伺服器，請謹記在你們的網站/伺服器安裝"Hongkong Post Root CA 3（交叉證書 2022）"。詳情請參閱公告。

2007 © | 重要告示 | 私隱政策

### 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）。  
[https://www.ecert.gov.hk/tc/sc/index\\_c.html](https://www.ecert.gov.hk/tc/sc/index_c.html)
2. 安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert SSL CA 3 - 17"。下載地址如下：  
[http://www1.ecert.gov.hk/root/ecert\\_ssl\\_ca\\_3-17\\_pem.crt](http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt)  
安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。  
下載地址如下：  
[http://www1.ecert.gov.hk/root/root\\_ca\\_3\\_x\\_gscar3\\_pem.crt](http://www1.ecert.gov.hk/root/root_ca_3_x_gscar3_pem.crt)
3. 安裝由根源證書 Root CA3 簽發的中繼證書"Hongkong Post e-Cert EV SSL CA 3 - 17"。下載地址如下：  
[http://www1.ecert.gov.hk/root/ecert\\_ev\\_ssl\\_ca\\_3-17\\_pem.crt](http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt)  
安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。  
下載地址如下：  
[http://www1.ecert.gov.hk/root/root\\_ca\\_3\\_x\\_gscar3\\_pem.crt](http://www1.ecert.gov.hk/root/root_ca_3_x_gscar3_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
```