SSL 伺服器數位憑證 Nginx

操作手冊

機密等級：公開
版本：5.0
文件編號：MNT-03-120
生效日期：114 年 6 月 3 日

臺灣網路認證股份有限公司
TAIWAN-CA. Inc.
台北市 100 延平南路 85 號 10 樓
電話:02-2370-8886
傳真:02-2370-0728
www.twca.com.tw

目錄

1.目的 1

2.參照資料 2

3.定義 3

4.作業程序 4

4.1 前置作業 4
4.2 產製「金鑰」 5
4.3 產生「憑證請求檔(CSR)」 6
4.4 將製作好的憑證請求檔(CSR)上傳 8
4.5 下載已核發憑證 11
4.6 合併憑證檔 13
4.7 SSL 安裝與設定 17
4.8 備份／復原憑證 18
4.9 更新憑證 19

5.常見問題 20

6.附件 21

1.目的

1.1. 介紹 Nginx 網頁伺服器之憑證請求檔產製步驟及 SSL 伺服器數位憑證安裝說明。

1.2. 符合本公司資訊安全政策之規範。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

2.參照資料

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

3.定義

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.作業程序

4.1 前置作業

4.1.1 利用 OpenSSL 產生金鑰與 CSR

Nginx 網頁伺服器建議按本手冊方式利用 OpenSSL 產生金鑰與 CSR，待憑證核發後再匯入 Nginx 網頁伺服器完成 SSL 伺服器數位憑證安裝，便於日後金鑰與憑證檔案維護。

4.1.2 安裝 OpenSSL 軟體

OpenSSL 可至 http://www.openssl.org/下載，在此不另外說明安裝方法，如對安裝過程有任何問題，請聯絡本公司協助處理。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.2 產製「金鑰」

4.2.1 在%OpenSSL%\bin\目錄下，輸入

openssl genrsa -out c:\server.key 2048

(指令反白部份請依實際路徑決定，-out 即為產生的金鑰檔存放位置)

```
openssl genrsa -out c:\server.key 2048
```

完成上列指令後會在 C:\下產生檔案名稱為 server.key 的 2048 位元長度 RSA 金鑰檔，使用文字編輯器打開金鑰檔後可看到如下內容



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.3 產生「憑證請求檔(CSR)」

4.3.1 在% OpenSSL%\bin\目錄下，輸入

openssl *req -new -key c:\server.key* -out c:\server.*csr*

(指令反白部份請依實際路徑決定，-key 所指定的路徑即為 4.2.1 節所產生的金鑰檔位置，-out 即為產生的 CSR 存放位置)

```
openssl req -new -key c:\server.key -out c:\server.csr
```

此時會要求輸入憑證內容，說明如下：

請輸入 2 碼國碼(如 TW)，必填

```
Country Name (2 letter code) [AU]:TW
```

請輸入州/省別(如 TAIWAN)，必填

```
State or Province Name (full name) [Some-State]:TAIWAN
```

請輸入所在城市(如 TAIPEI)，必填

```
Locality Name (eg, city) []:TAIPEI
```

請輸入組織名稱(如 TWCA)，必填

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TWCA
```

請輸入單位名稱(如 IT、SYSTEM)，必填

```
Organizational Unit Name (eg, section) []:SYSTEM
```

請輸入貴公司欲加密的網站名稱(如 www.twca.com.tw)，必填

```
Common Name (eg, YOUR name) []:www.twca.com.tw
```

請輸入申請人員 Email，可不填

```
Email Address []:SSL@twca.com.tw
```

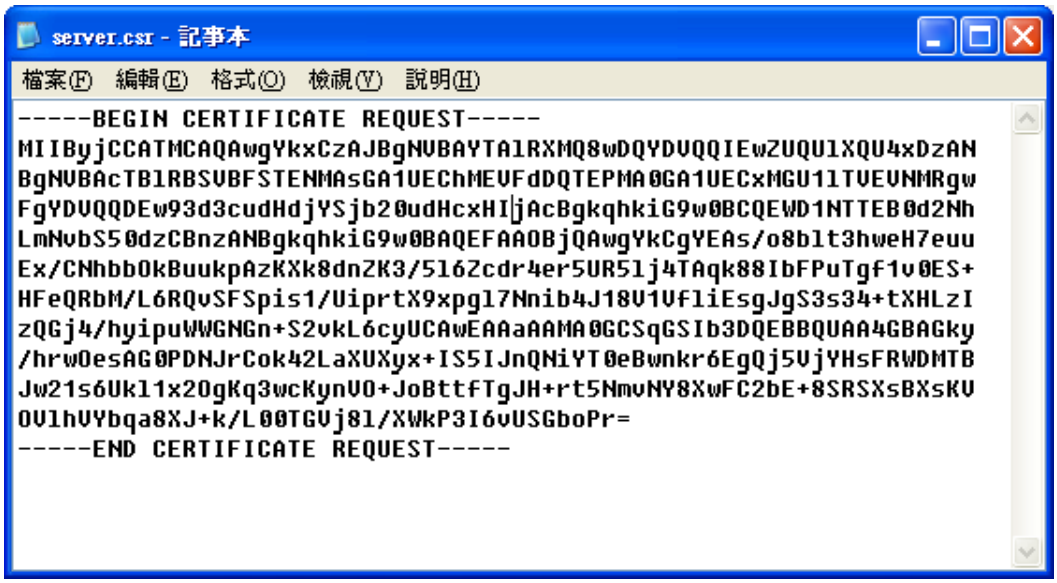
最後會要求輸入額外資訊，請勿填寫任何資料，直接按 Enter 即可

```
A challenge password []:
An optional company name []:
```

完成上列指令後會在 C:\下產生 server.csr 的檔案，此檔即為憑證請求檔，

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

使用文字編輯器打開金鑰檔後可看到如下內容



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.4 將製作好的憑證請求檔(CSR)上傳

4.4.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw

點選客服專區，點選 SSL 伺服器憑證。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.4.2 連接 TWCA 網站(2)

點選 SSL 伺服器憑證。

4.4.3 連接 TWCA 網站(3)

點選 TWCA SSL 類。

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。

4.4.4 連接 TWCA 網站(4)

點選上傳 CSR（WEB）。

4.4.5 貼上憑證請求檔

將瀏覽器視窗畫面往下拉，開啟在 5.1 章節產生的憑證請求檔，利用全選後複製貼上的方式(CSR 檔案內容包含-----BEGIN CERTIFICATE REQUEST-----、-----END CERTIFICATE REQUEST-----)，將製作好之憑證請求檔（CSR）內容貼到申請欄位中→選擇繼續。

4.4.6 再次檢視上傳之憑證請求檔案內容

4.4.7 設定通行密碼及選擇身分審驗方式

4.4.7.1 請自行設定通行密碼,該密碼請牢記，如您需要廢止憑證時,必須輸入此通行密碼。

4.4.7.2 為符合 SSL 憑證國際審放標準，將審驗網域所有權者請您選擇以下一種審驗方式:

一、EMAIL 驗證：將會自動帶出網域註冊之 EAMIL 或者請選擇

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

admin@網域、administrator@網域、webmaster@網域、hostmaster@網域、postmaster@網域此六個 EMAIL 任一個 EMAIL 皆可進行身分驗證作業，選擇送出後系統將會寄出驗證信，請務必至該信箱完成驗證作業

二、檔案驗證：請您填入收取該檔案收件人 EMAIL,您將在此 EMAIL 收到一附件檔案,請您依照信件說明將檔案放入,完成後請通知我們進行檔案驗證作業。

三、電話驗證：網域所有權人的資料可公開查詢到才能使用電話驗證,請您選擇進行電話驗證的時段,我們將依照您所選擇的去電驗證。

4.4.7.3 填寫表單編號，並確認以上表單內容輸入正確後，按繼續送出申請。

4.4.8 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，近日會完成驗證(以下畫面為選擇電話驗證的顯示結果)，憑證簽發後會以 Email 通知業務及技術聯絡人(TWCA SSL 伺服器數位憑證下載通知)，憑證亦可以在 TWCA 網站搜尋及下載。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.5 下載已核發憑證

1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經審驗通過，將會寄送「SSL 伺服器數位憑證下載通知」電子郵件給相關聯絡人，郵件內容包含附件憑證鏈壓縮檔（cert.zip）及 TWCA SSL 動態認證標章之安裝說明與標章圖檔連結。

將附件憑證鏈壓縮檔 cert.zip 解壓縮後，可得到三個憑證鏈檔。

※內容及憑證用途如下圖所式：

2 檔案下載說明

如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

4.5.1 連接 TWCA 網站(1)

連接至本公司首頁 https://www.twca.com.tw

點選客服專區，點選 SSL 伺服器憑證。

4.5.2 連接 TWCA 網站(3)

點選 TWCA SSL 類。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。

4.5.3 連接 TWCA 網站(4)

點選憑證搜尋。

4.5.4 輸入申請之網站名稱

在網站名稱中輸入憑證申請單上填寫之網站名稱(Common Name)，如 www.twca.com.tw (**注意，大小寫需一致，不必加 http://或 https://**)，輸入完成後，按下搜尋鍵。

4.5.5 下載憑證鏈壓縮檔

確認憑證相關資訊與申請相符後點選下載→憑證鏈，另開檔案下載視窗，按下另存新檔，儲存憑證鏈壓縮檔 cert.zip。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.6 合併憑證檔

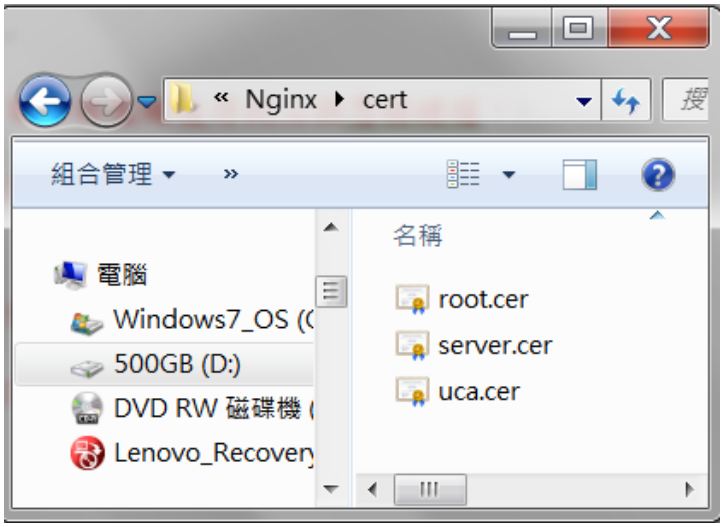
4.6.1 準備 Nginx 所需安裝憑證檔

- 於 4.5 章節取得的伺服器憑證檔「server.cer」
- 於 4.5 章節取得的中繼憑證檔「uca.cer」

先備妥並將 4.5 章節取得憑證檔存放同一個目錄內(實際目錄請自訂)。

※ 如 4.5 章節解壓縮後得到三個憑證鏈檔，

存放內容應如下圖所示：



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.6.2 合併憑證指令

4.6.2.1 開啟命令提示字元，於 4.6.1 章節所說明檔案存放目錄下，輸入

copy SSL 伺服器憑證檔+中繼憑證檔 DomainCert.cer

(DomainCert.cer 為範例，實際產生檔名可自訂)

```
C:\>copy server.cer+uca.cer DomainCert.cer
```

完成上列指令後會在該目錄下產生檔案名稱為 DomainCert.cer 的檔案，此檔案即為 Nginx 所需安裝憑證檔。

使用文字編輯器打開 DomainCert.cer 檔，可看到如下內容。

-----BEGIN CERTIFICATE-----

$SOME TEXT

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

$SOME TEXT

-----END CERTIFICATE-----

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

內容範例如下圖所示



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.7 SSL 安裝與設定

4.7.1 編輯%nginx%目錄下的 nginx.conf 檔案(Nginx 預設的設定檔)

4.7.2 於 nginx.conf 新增以下設定(#為設定說明)

```
ssl on;
listen 443;
ssl_certificate_key /path/server.key;
ssl_certificate /path/DomainCert.cer;
#啟用 SSL 功能。
# SSL(https)功能的預設 Port，如果要使用其他 Port 再修改設定。
#SSL 金鑰檔路徑，請依 4.2.1 章節產製金鑰存放路徑設定。
#SSL 憑證檔路徑，請依 4.6.1 章節檔案存放路徑設定。
```

4.7.3 重新啟動 Nginx 網頁伺服器服務，完成 SSL 憑證安裝與設定。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.8 備份／復原憑證

請將 4.6.1 章節所產生 Nginx 所支援憑證檔與 4.2.1 章節所產生之金鑰檔備份至安全的位置，復原時再依照 4.7 章節的敘述設定即可。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4.9 更新憑證

4.9.1 申請說明

臺灣網路認證公司會在 SSL 伺服器憑證到期前二個月發出憑證更新通知信給　貴公司。這二個月內您隨時可以至本公司網站 http://www.twca.com.tw 下載申請表單，填寫完畢後寄回臺灣網路認證公司，即可進行 SSL 憑證更新申請。

4.9.2 更新步驟

請參照 4.2 至 4.7 章節步驟申請安裝憑證，即可完成 SSL 憑證更新。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

5.常見問題

5.1 請參閱 http://www.twca.com.tw/picture/file/SSL 常見技術問題手冊.pdf。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

6.附件

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。
The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.