

SSL 伺服器數位憑證 Nginx 操作手冊



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

機密等級：公開

版本：5.2

文件編號：MNT-03-120

生效日期：110 年 8 月 10 日

目錄

1.目的	1
2.範圍	2
3.參考資料	3
4.定義	4
5.作業程序	5
5.1 前置作業.....	5
5.2 產製「金鑰」	6
5.3 產生「憑證請求檔(CSR)」	7
5.4 將製作好的憑證請求檔(CSR)上傳	9
5.5 下載已核發憑證.....	15
5.6 合併憑證檔.....	18
5.7 SSL 安裝與設定	23
5.8 備份／復原憑證.....	24
5.9 更新憑證.....	25
6.常見問題	26
7.附件	27

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。

2. 範圍

無。

3. 參考資料

無。

4. 定義

無。

5.作業程序

5.1 前置作業

5.1.1 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。

5.1.2 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。

5.2 產製「金鑰」

5.2.1 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



5.3 產生「憑證請求檔(CSR)」

5.3.1 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 5.2.1 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

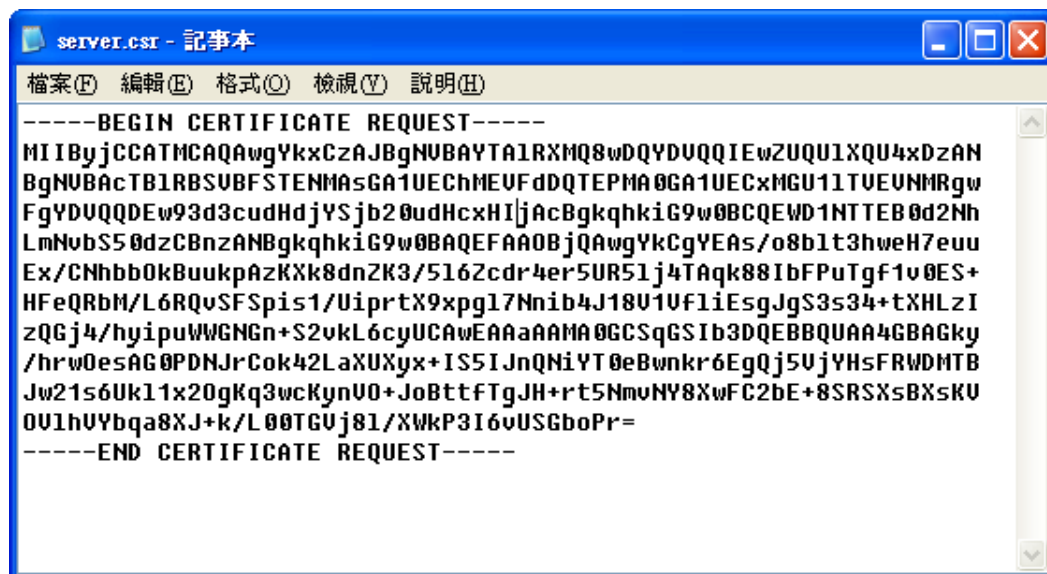
```
Email Address []:SSL@twca.com.tw
```

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，

使用文字編輯器打開金鑰檔後可看到如下內容



```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwYkxCZAJBgNVBAYTA1RXMQ8wDQYDVQQIEwZUQU1XQU4x
BgNVBAcTB1RBSVBFSTENMA5GA1UEChMEVFdDQTEPMA0GA1UECxMGU11T
VUUNMRgwFgYDVQQDEw93d3cudHdjYSjb20udHcxHIjAcBgkqhkiG9w0B
CQEWd1NTTEB0d2NhLmNvbS50dzCBnzANBgkqhkiG9w0BAQEFAA0BjQAw
YkCgYEA5/o8b1t3hweH7euvEx/CNhbb0kBuukpAzKXk8dnZK3/5162
cdr4er5UR51j4TAqk88IbFPuTgf1v0ES+HFeQRbM/L6RQvSFSpis1/
UiprtX9xpg17Nnib4J18U1UFlieSgJgS3s34+tXHLzIzQGj4/hyip
uWVGNGn+S2vkl6cyUCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAGky
/hrw0esAG0PDNjrCok42LaXUXyx+IS5IJnQNiYT0eBwnkr6EgQj5Vj
YHsFRWDMTBjw21s6Uk1x20gKq3wcKynU0+JoBttfTgJH+rt5NmVNY
8XwFC2bE+8SRsXsBXsKV0U1hUYbqa8XJ+k/L00TGVj81/XWkP3I6v
USGboPr=
-----END CERTIFICATE REQUEST-----
```

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.

5.4 將製作好的憑證請求檔(CSR)上傳

5.4.1 連接 TWCA 網站(1)

連接至本公司首頁 <https://www.twca.com.tw>

點選 **憑證服務**，點選 **SSL 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.

5.4.2 連接 TWCA 網站(2)

點選申請憑證。

※如申請 EV SSL 伺服器憑證，請點選EV SSL 憑證。



■ 上傳 CSR (WEB)

上傳憑證請求檔(CSR)

請依據適用之『憑證操作手冊』產生憑證請求檔(CSR)，手冊取得請來電02-2370-8886#9 洽詢。

產生憑證請求檔(CSR)後

請將CSR以純文字的方式儲存成為檔案（建議檔案名稱為Certreq.txt）後，請以純ASCII的文字編輯器（如記事本）來開啟此檔。注意不要使用文書處理軟體（如WORD）開啟，因為它們會額外插入文字的格式指令及控制字元。

- 傳送憑證申請檔（CSR）
以下為CSR檔案的內容範例：——BEGIN NEW CERTIFICATE REQUEST——
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U
ECBMBGVEFJV0FOMQ8wDQYDVQQHEwZUQUXQU4xDjAMB
gNVBfweFEg,uhYUGJ84DWgbyGYGYVQLEwJJVDEcMBoGA1U
EAXMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCSqGSIb3D
QEBAQUAA0sAMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ
giJfHca2diLHqQ69SMUuLXNdnVQnl4kgPo1qNvkv0TKR7tac
LnfmWxuUHUHUulihihiluHLUIHUILHhkiG9w0BAQQFAANBAIIG
5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD
duwd01q42V5xCMasPCImkIri1TX4BYr5qzY=——END NEW CERTIFICATE REQUEST——

請將CSR檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

開啟在 5.3 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**。

● 傳送憑證申請檔 (CSR)

以下為CSR檔案的內容範例：——BEGIN NEW CERTIFICATE REQUEST——

```
MIIBJDCBzwIBADBQMqswCQYDVQQGEwJUVzEPMA0GA1U
ECBMGVEFJV0FOMQ8wDQYDVQQHEwZUQUXIUQx4DjAMB
gNVBwFefEg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U
EAXMTbGFiMzAwLnRhaWNhLmNvbS50dzBcMA0GCsGSIb3D
QEBAQUAA0sAMEgCQQDYdmR9MVXzUclzOE6wW0ggZRpZ
giJfHca2dILHqQ69SMUmLXNdnvQnI4pkpPo1qkvNv0TKR7tac
LnfmjWxuUHUHUulihihiluHLUIHUIlHhkiG9w0BAQQFAANBAIIG
5vczs+LzMP1c1ybwTE4784HLZUbibZhXNg6L90H09CIHpDXD
duwd01q42V5xCmasPCImkrlrITX4BYr5qZy=——END NEW CERTIFICATE REQUEST——
```

請將CSR檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBJDCBzwIBADBQMqswCQYDVQQGEwJUVzEPMA0GA1U
ECBMGVEFJV0FOMQ8wDQYDVQQHEwZUQUXIUQx4DjAMB
gNVBwFefEg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U
EAXMTbGFiMzAwLnRhaWNhLmNvbS50dzBcMA0GCsGSIb3D
QEBAQUAA0sAMEgCQQDYdmR9MVXzUclzOE6wW0ggZRpZ
giJfHca2dILHqQ69SMUmLXNdnvQnI4pkpPo1qkvNv0TKR7tac
LnfmjWxuUHUHUulihihiluHLUIHUIlHhkiG9w0BAQQFAANBAIIG
5vczs+LzMP1c1ybwTE4784HLZUbibZhXNg6L90H09CIHpDXD
duwd01q42V5xCmasPCImkrlrITX4BYr5qZy=-----END NEW CERTIFICATE REQUEST-----

請按一下「繼續」按鈕以送出CSR，並繼續註冊程序。

繼續

重設

5.4.5 再次檢視上傳之憑證請求檔案內容



5.4.6 設定通行密碼及選擇身分審驗方式

5.4.6.1 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。

請輸入通行密碼

通行密碼 此密碼是廢止憑證所需，請務必記得，並儲存在安全的地方	建立通行密碼
------------------------------------	------------------------------------

5.4.6.2 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 EMAIL 或者請選擇

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，

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.

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。

網域所有權

網域管理者	為符合SSL憑證國際審放標準，將審驗網域所有權請您選擇以下一種審驗方式。
	☒ 網域所有權EMAIL驗證：點選確認後，系統將會自動寄出驗證信，請用戶務必至該信箱收信並點擊確認即可。 ☒ maintain@twca.com.tw (網域註冊資料來源由WHOIS取得) 或請選擇 ☐ admin@twca.com.tw ☐ administrator@twca.com.tw ☐ webmaster@twca.com.tw ☐ hostmaster@twca.com.tw ☐ postmaster@twca.com.tw
	☐ 網站檔案驗證：(Whois資料設定為不揭露) 請您填入接收電子信箱： maintain@twca.com.tw ，將郵寄檔案及說明給您。
	☐ 電話驗證：我們將以電話驗證方式確認網域所有權 請您留下方便聯絡的時間： ☒ 皆可 ☐ 上午時段 ☐ 下午時段

5.4.6.3 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。

確認以上所輸入的資料正確後，請輸入表單編號，按“繼續”送出申請

表單編號 請輸入憑證申請單 右上角 的表單編號	
請按一下“繼續”按鈕以送出註冊資料，完成註冊程序。	若未填過憑證申請單，請線上登打 憑證表單線上作業輸入 <input checked="" type="button" value="繼續"/>

5.4.7 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。



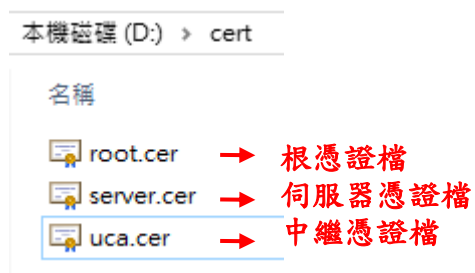
5.5 下載已核發憑證

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。

5.5.1 連接 TWCA 網站(1)

連接至本公司首頁 <https://www.twca.com.tw>

點選 **憑證服務**，點選 **SSL 憑證**。



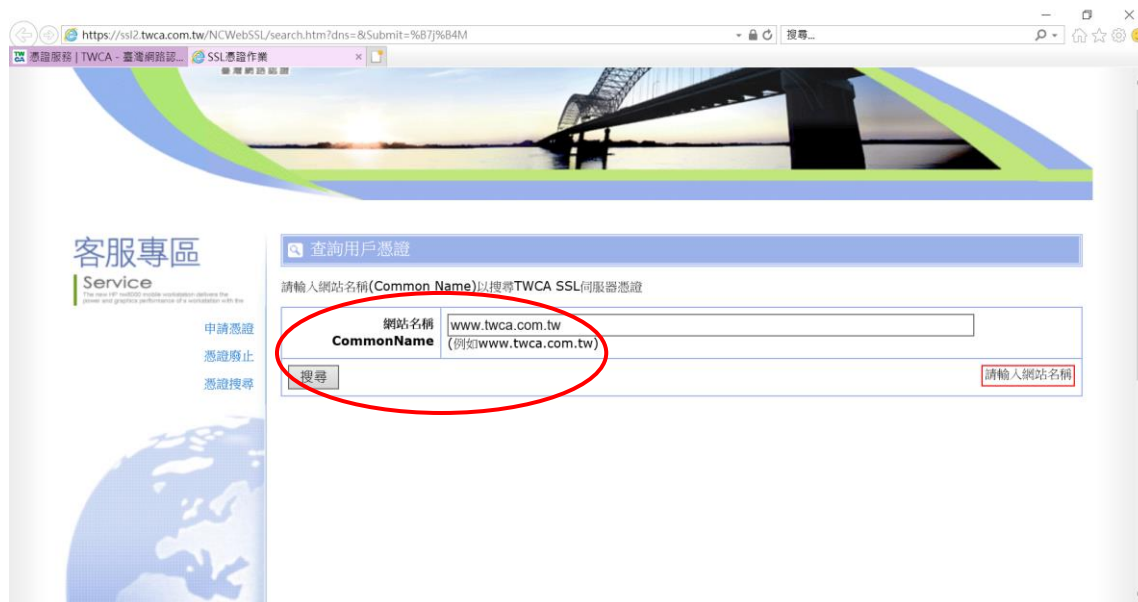
5.5.2 連接 TWCA 網站(2)

點選 **憑證搜尋**。



5.5.3 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。



5.5.4 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。



5.6 合併憑證檔

5.6.1 準備 Nginx 所需安裝憑證檔

- 於 5.5 章節取得的伺服器憑證檔「server.cer」
- 於 5.5 章節取得的中繼憑證檔「uca.cer」

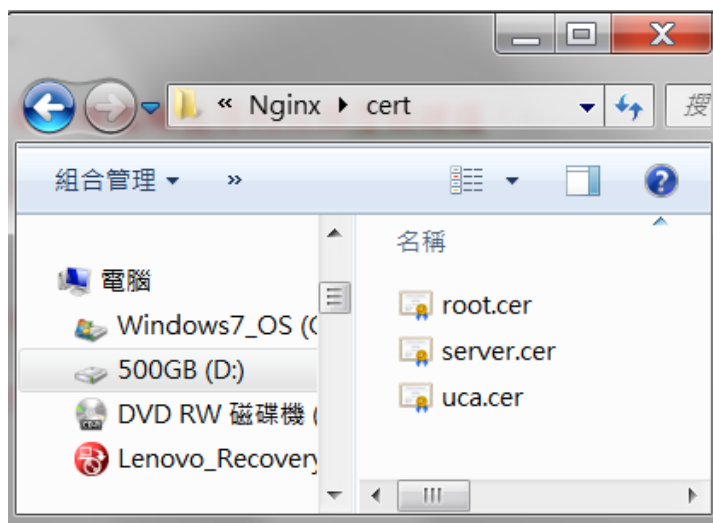
本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

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.

先備妥並將 5.5 章節取得憑證檔存放同一個目錄內(實際目錄請自訂)。

※ 如 5.5 章節解壓縮後得到三個憑證鏈檔，

存放內容應如下圖所示：



5.6.2 合併憑證指令

5.6.2.1 開啟命令提示字元，於 5.6.1 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-----

伺服器憑證

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.

```

-----BEGIN CERTIFICATE-----
MIIFWTCCBEGgAwIBAgIQQAEBzU+QAAAAAAAAAAmyl0baTANBgkqhkiG9w0BAQsFADBF
MQswCQYDVQQGEwJUVzESMBAGA1UECgwJVEFJV0FOLUNBMRAwDgYDVQQLEwQDadSb290
IENBMSowKAYDVQDDCFUVONBIFJvb3QgQ2VydGhmaWNhdGlvbiBBdXR0b3NpdHkw
HicNMTQxMDI4MDczODMxWmcNMzAxMDI4MTU1OTU5WjBRMQswCQYDVQQGEwJUVzES
MBAGA1UECgwJVEFJV0FOLUNBMRAwDgYDVQQLEwQDadSb290IENBMRwwGgYDVQQDEwNU
VONBIEdsb2JhbCBSb290IENBMIIIClANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
AgEAsAXbyOuMxG6Kle+OTZxxCh9Sc01tgpyXxddMTkVJy0BCtR10bBnCdkQxX4UC
1+xDMwpt0pyMjre4edsr1WryjmbE7isBB5LUs9AC31D2Va9mDsvgR2AvKz15NV16
KIP4exbGGLhi1kclkc7wGRJNrWP10z91XynwoTAcKqCYphW97v0ZNVdikuOP+srW
ECdJTO/dwGfGcJvK6qhaQ/xthm9z6TdFqfA2x8yldR67bAb/m2s+F+xbqnF8xh2i
90npFbU81qFh9RH3BW8d/RG+0DAHwimwCU4m300iqJFqH8KRRYhc5Zi4caUVGcl8
dRHMCHRPLZsdcUT9Viig/ruGasj6XAtY3MZLdsir1tlzD6X0WgKJP0+eloLuonRT
Kj1tJ2kdbI4yLGQAJmNhNk6jRrc/fbMtrG2QopWizs/aguchNBmW6bghqil+pji+
ji1KIWZ5H7PDtQln3tbUB0bzKtAP6ciVf79VkvQV6zz0VwG/eCZQB
g9c0G8xApfC4m2fVmJE7p4R41S0837gUjujfqYlsZ51zHcC30uyS
yL4JvywpBW8Ca57vvL8qvFvAU19BCHGHSkZ3BKmBozKvru5rF4uysf5s4ZCMiKiX
SM7ITcvzBs9fagpCsR4edy+0o0aSDgb8BSLSJuExUX0y3A8CAwEAAaOCAR0wggEZ
MB8GA1UdIwQYMBaAFGo4WyaN3ota8k96VIMZGOMINaa6MB0GA1UdDgQWBBR1283e
julJclqI6LHYPQezuWtmUDA0BgNVHQ8BAf8EBAMCAQYwOAYDVROgBDEwLzAtBgRV
HSAAMCUwIwYIKwYBBQUHAgEWF2h0dHA6Ly93d3cuZm9udHcvMEIGAlUd
HwQ7MDkwN6A1oDOGMMh0dHA6Ly93d3cuZm9udHcvVfDQVJDQS9y
ZXZva2VfMjA0OC5jcmwwDwYDVROTAQH/BAUwAwEB/zA4BggrBgEFBQcBAQQsMCow
KAYIKwYBBQUHMAGGHGh0dHA6Ly93d3cuZm9udHcvZm9udHcvZm9udHcvZm9udHcv
hvcNAQELBQADggEBACKLbsSU3GJZk3paTF3cmT60qPv5oI8b2SdwbfguXkhpYRdA
EImqA7gcy9+8bChUH8U9UuWv/xMR8oLd8PMZntvuTYlafnBke2Plp6iIuiCt4nI
qtAg50qslsvT/ZPFGvxekWhh8hx56ekuYBryc7NiiWczdMJpTL6JNFRfzwxmUfq
H6dvboTNrtiuNWrWy+C+E8GiMcvuH+km37cGxglFCuerRVcetwGbmfxYBUBFhtGC
G9BLIdsgguMi6U/jXSvEORIXKMa5Z7F94bJ8duU2hNpOXqw4tmv47qEDxLDEXBJM
bmbaOkRltjaXDBh50EaXmx+rUqj03le0KBM4t6w=
-----END CERTIFICATE-----

```

中繼憑證

5.7 SSL 安裝與設定

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

5.7.2 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 5.2.1 章節產製金鑰存放路徑設定。

#SSL 憑證檔路徑，請依 5.6.1 章節檔案存放路徑設定。

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

5.8 備份／復原憑證

請將 5.6.1 章節所產生 Nginx 所支援憑證檔與 5.2.1 章節所產生之金鑰檔備份至安全的位置，復原時再依照 5.7 章節的敘述設定即可。

5.9 更新憑證

5.9.1 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 <https://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。

5.9.2 更新步驟

請參照 5.2 至 5.7 章節步驟申請安裝憑證，即可完成 SSL 憑證更新。

6. 常見問題

6.1 請參閱 [https://www.twca.com.tw/picture/file/SSL 常見技術問題手冊.pdf](https://www.twca.com.tw/picture/file/SSL%20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.

7. 附件

無。