SSL 伺服器數位憑證 Apache2.2

伺服器操作手冊

機密等級：公開
版本：V1.3
文件編號：MNT-03-083
生效日期：101 年 9 月 27 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

1.1. 介紹 Apache2.2 網頁伺服器之金鑰、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。

2.參考資料

無。

3.定義

無。

4.作業程序

4.1 前置作業

4.1.1 安裝 Apache 2.2 Web 伺服器軟體

Apache 2.2 Web 伺服器軟體是由 Apache 組織所提供的 Web 伺服器軟體，可至 http://httpd.apache.org/下載，本操作手冊安裝環境為 Apache 2.2 (Windows 版)，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。

4.1.2 安裝 OpenSSL 軟體

Apache 需搭配 OpenSSL 軟體來產製金鑰，Apache 2.2 已內建 OpenSSL 軟體，軟體存在%Apache2.2%\bin\目錄裡，如果要另外安裝 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。

4.2 產製「金鑰」

4.2.1 在%Apache2.2%\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

4.3 產生「憑證請求檔(CSR)」

4.3.1 在% Apache2.2%\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 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

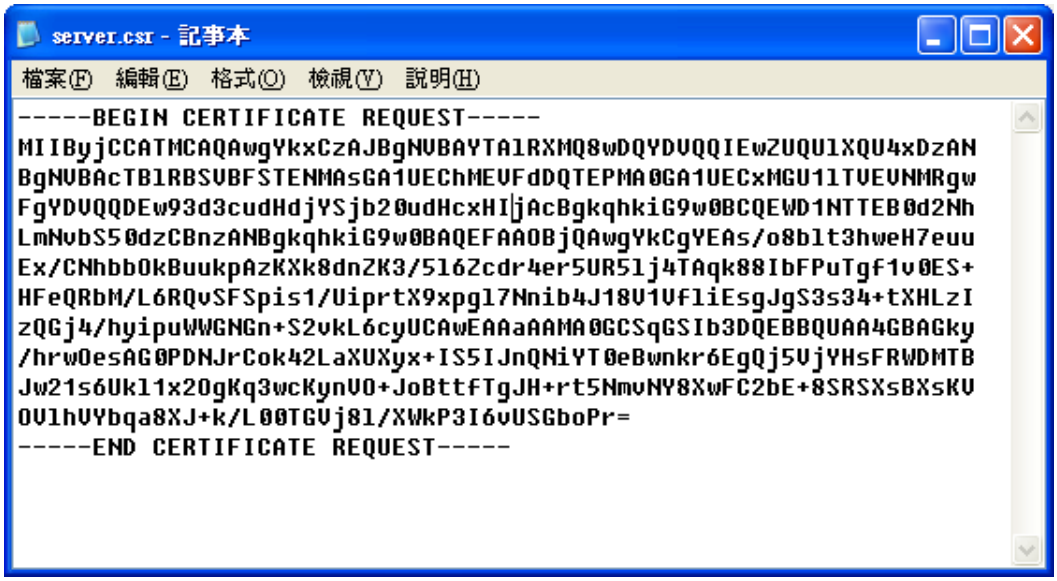
```
Email Address []:SSL@twca.com.tw
```

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



4.4 將製作好的憑證請求檔(CSR)上傳

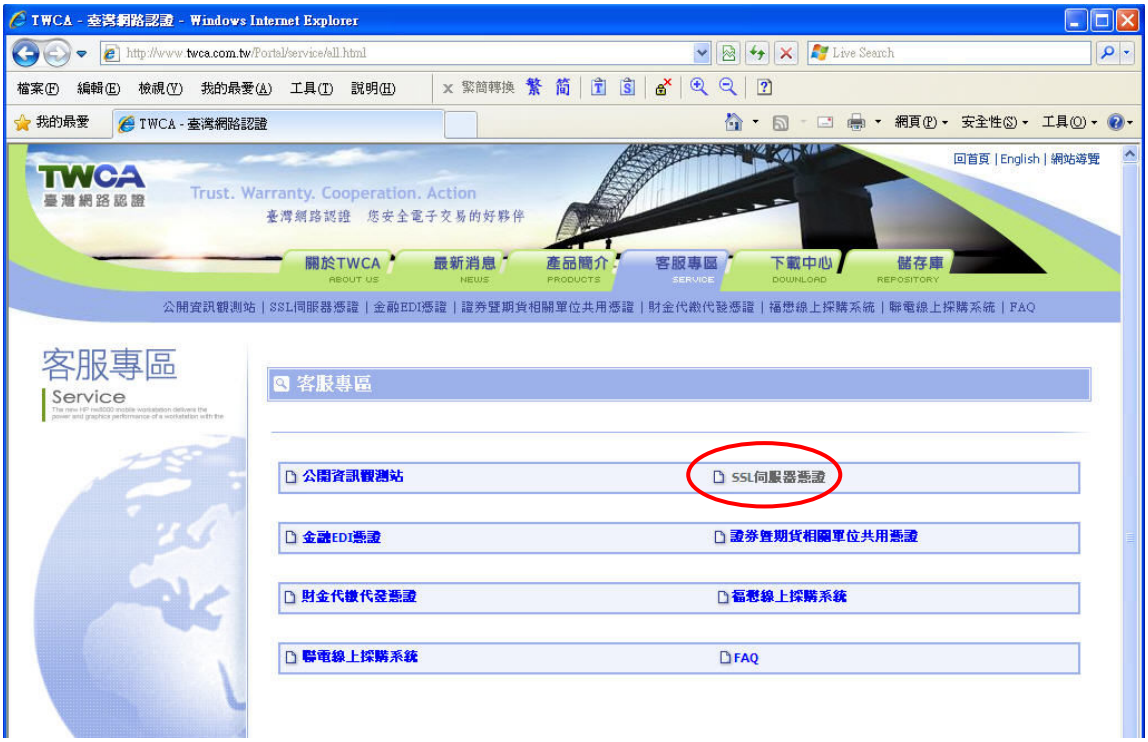
4.4.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw

點選右上方圖示憑證申請展期或註銷請由此進入。

4.4.2 連接 TWCA 網站(2)

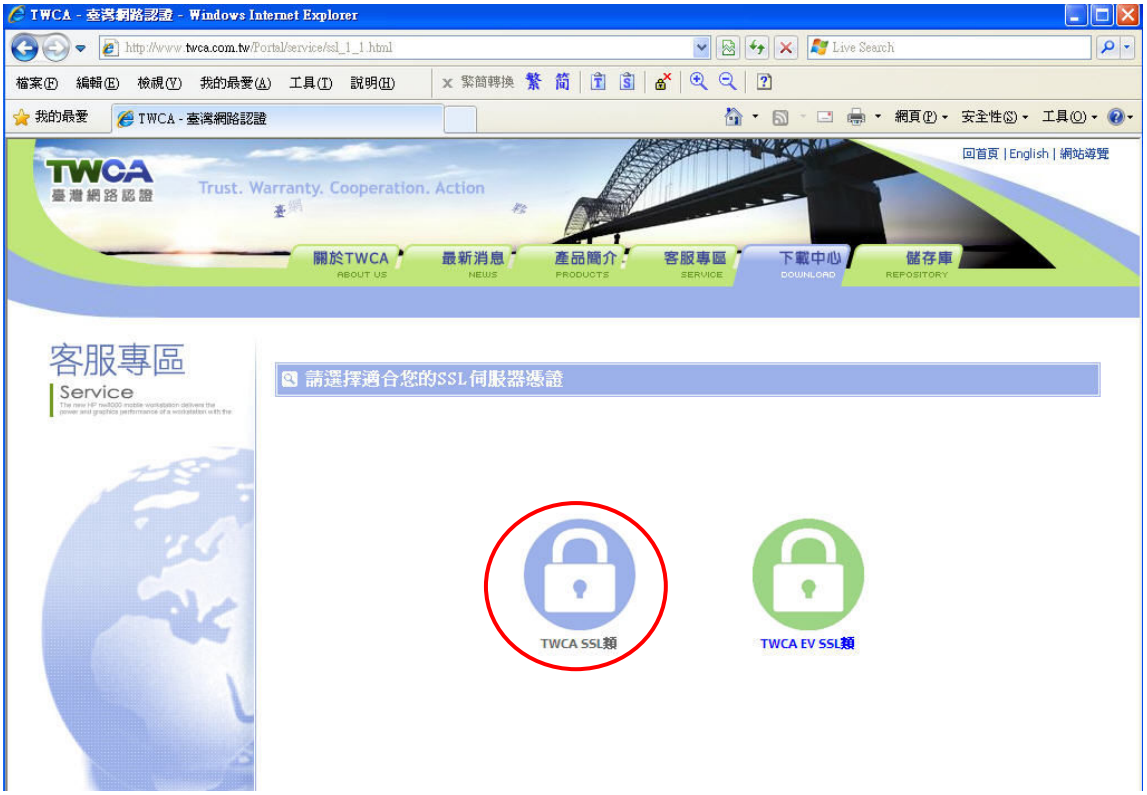
點選 SSL 伺服器憑證。



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。

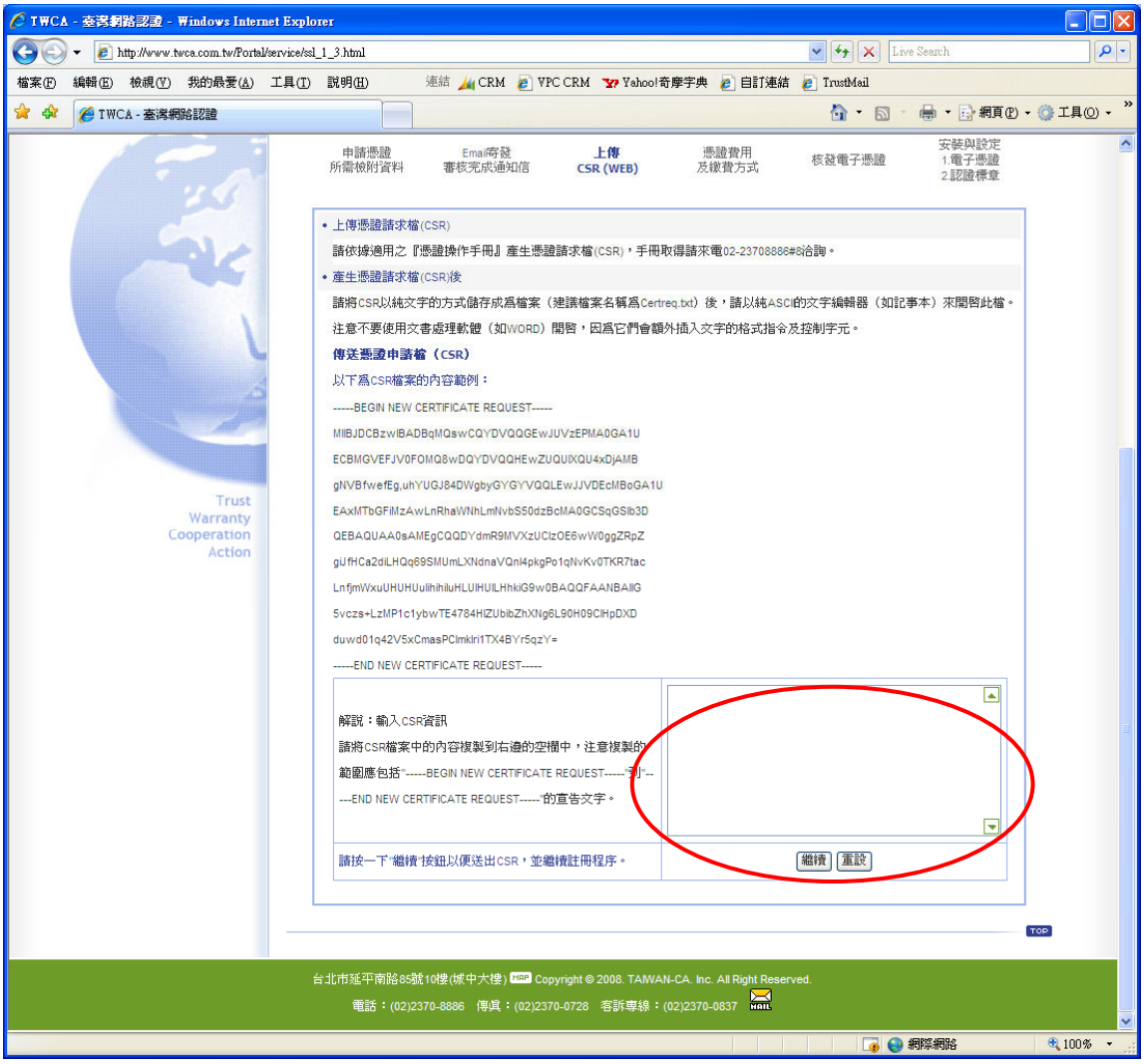


4.4.4 連接 TWCA 網站(4)

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 4.3 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。



4.4.6 再次檢視上傳之憑證請求檔案內容

4.4.7 填寫聯絡人基本資料

使用視窗右方式下拉移動方式，將申請之伺服器與聯絡資料填入適當欄位(聯絡資料欄位請務必與申請同意書所填內容相符)。

請輸入伺服器資訊

伺服器軟體廠商： 請從右邊的下拉式選單中選擇您伺服器軟體的廠商。如果不在清單中，請選擇其他。	Microsoft IIS
通行密碼：(至少六碼) 請在右邊的欄位中輸入一個您容易記憶，但不易為人所臆測的文字或片語。當您 申請、 更新或 註銷此SSL伺服器憑證時都需使用到這個通行密碼。另外，當您對本公司提出技術支援服務時，本公司亦會要求您提供此通行密碼。若有必要，請將此密碼記錄下來，並儲存在安全的地方。	輸入密碼： 再輸入一次密碼以確認：

請輸入技術聯絡人資訊

請輸入本公司寄送SSL伺服器憑證給您時的技術聯絡人資訊於下表。舉例來說，此人可以是您的網站管理者，或是您網路撥接商的技術支援人員。

請注意此人必須擁有存取您網頁伺服器的權利。本公司在發放SSL伺服器憑證以前，會先以電話與此技術聯絡人取得聯繫。

當網頁伺服器的安全出現顧慮時，此技術聯絡人有通知本公司的義務。

另若有憑證更新的訊息，本公司也會寄送給技術聯絡人及　貴公司的業務聯絡人。

姓名	
職稱	
公司	
統一編號	
通訊地址	台北市 郵遞區號：
聯絡電話	
傳真號碼	
電子郵件地址	

請輸入業務聯絡人資訊

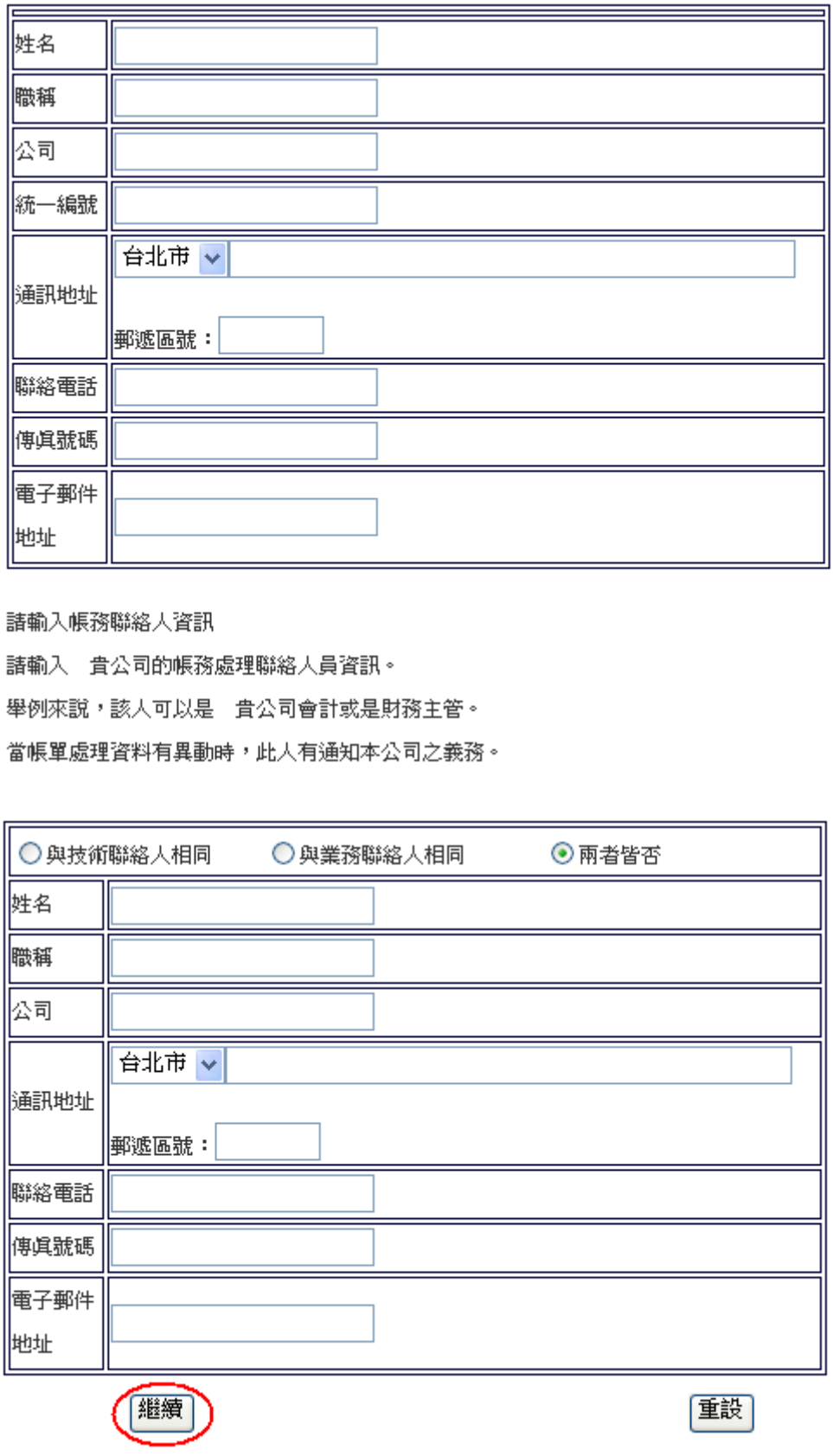
請輸入　貴公司負責SSL伺服器憑證業務聯絡人資訊於下表，並填寫本公司所要求的資訊。

舉例來說，此人可以是　貴公司的決策者或是高階的經理人。

請注意業務聯絡人必須為　貴公司組織內之一份子。本公司在發放SSL伺服器憑證以前，會先以電話與此業務聯絡人取得聯繫。

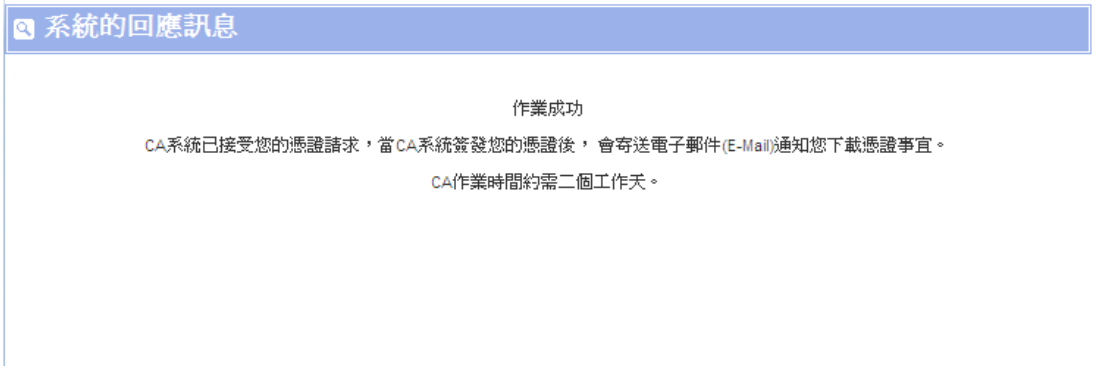
業務聯絡人與技術聯絡人不應為同一人，您應該分別指定。

另外，本公司若有更新的資料也會同時寄給上述這兩個人。



4.4.8 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，三個工作天內會完成資料審查作業，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。



4.5 下載已核發憑證

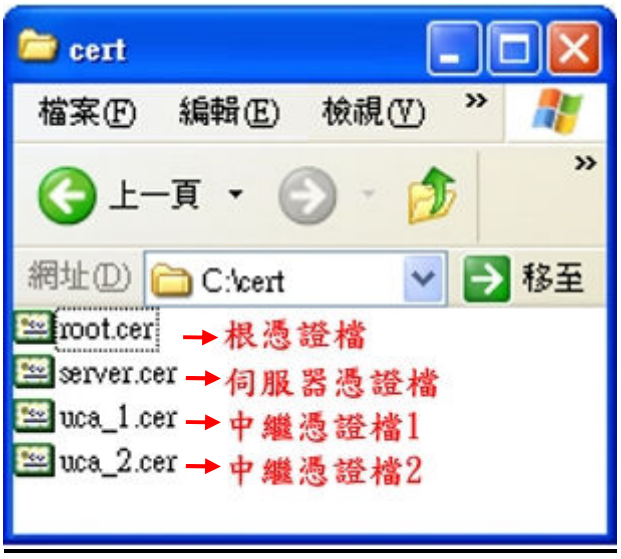
1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經過審驗通過，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，可得到三個或四個憑證鏈檔。

※如解壓縮後得到三個憑證鏈檔，內容及憑證用途如下圖所式：

※如解壓縮後得到四個憑證鏈檔，內容及憑證用途如下圖所式：



2 檔案下載說明

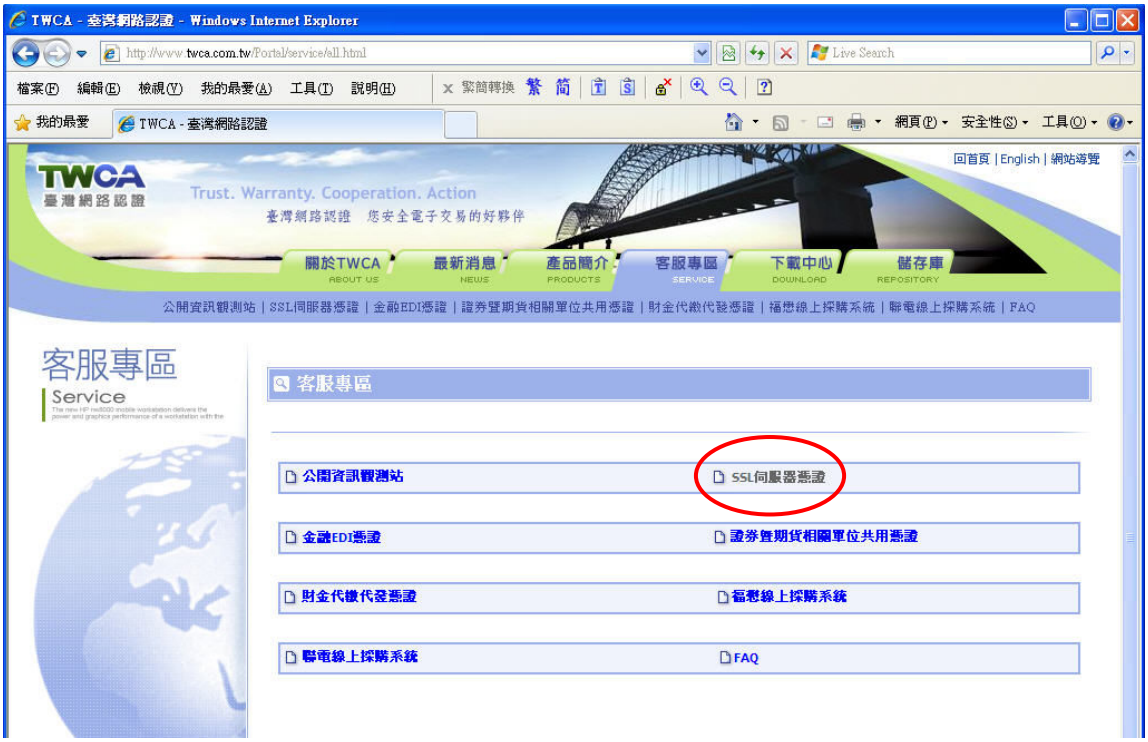
如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

4.5.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw，點選右上方憑證申請展期或註銷請由此進入。

4.5.2 連接 TWCA 網站(2)

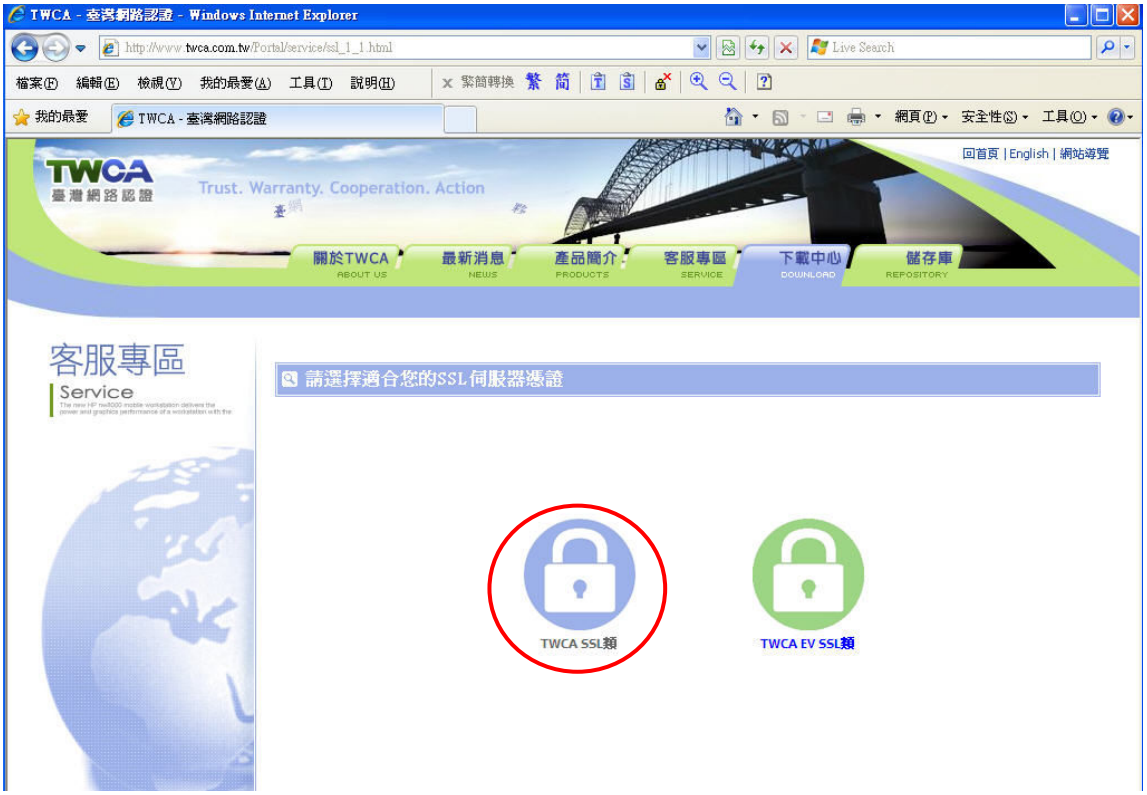
點選 SSL 伺服器憑證。



4.5.3 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。



4.5.4 連接 TWCA 網站(4)

點選憑證搜尋。

4.5.5 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。

4.5.6 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，按下儲存，儲存憑證鏈壓縮檔 cert.zip。

4.6 安裝憑證

4.6.1 Apache 在安裝 SSL 憑證時會使用到三種檔案：

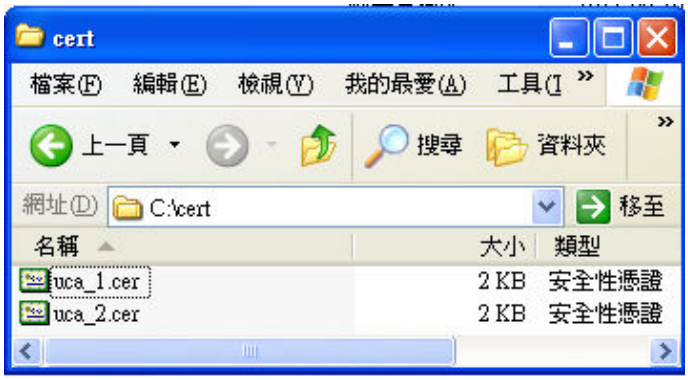
- 於 4.2 章節產製的 SSL 伺服器金鑰「server.key」
- 於 4.5 章節取得的伺服器憑證檔「server.cer」
- 於 4.5 章節取得的中繼憑證檔「uca.cer」

先備妥並將其存放至%Apache2.2%\conf 目錄下(實際目錄可自行決定)。

※ 如 4.5 章節解壓縮後得到三個憑證鏈檔，請直接至 4.6.3 章節安裝 SSL 憑證。

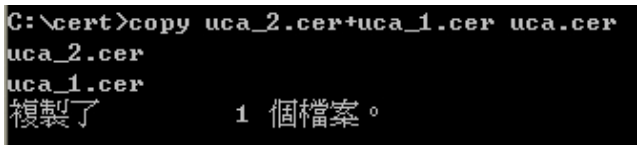
※ 如解壓縮後得到四個憑證鏈檔，請先依照下列步驟，將 uca_1.cer 與 uca_2.cer 憑證內容合併，再提供 4.6.3.3 章節中繼憑證安裝使用。

先將 uca_1.cer 與 uca_2.cer 存放同一個目錄內(實際目錄可自行決定)

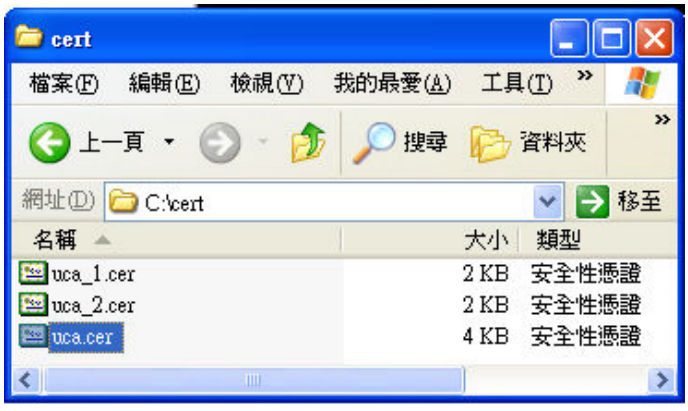


開啟命令提示字元，於前述兩個檔案存放目錄下，輸入

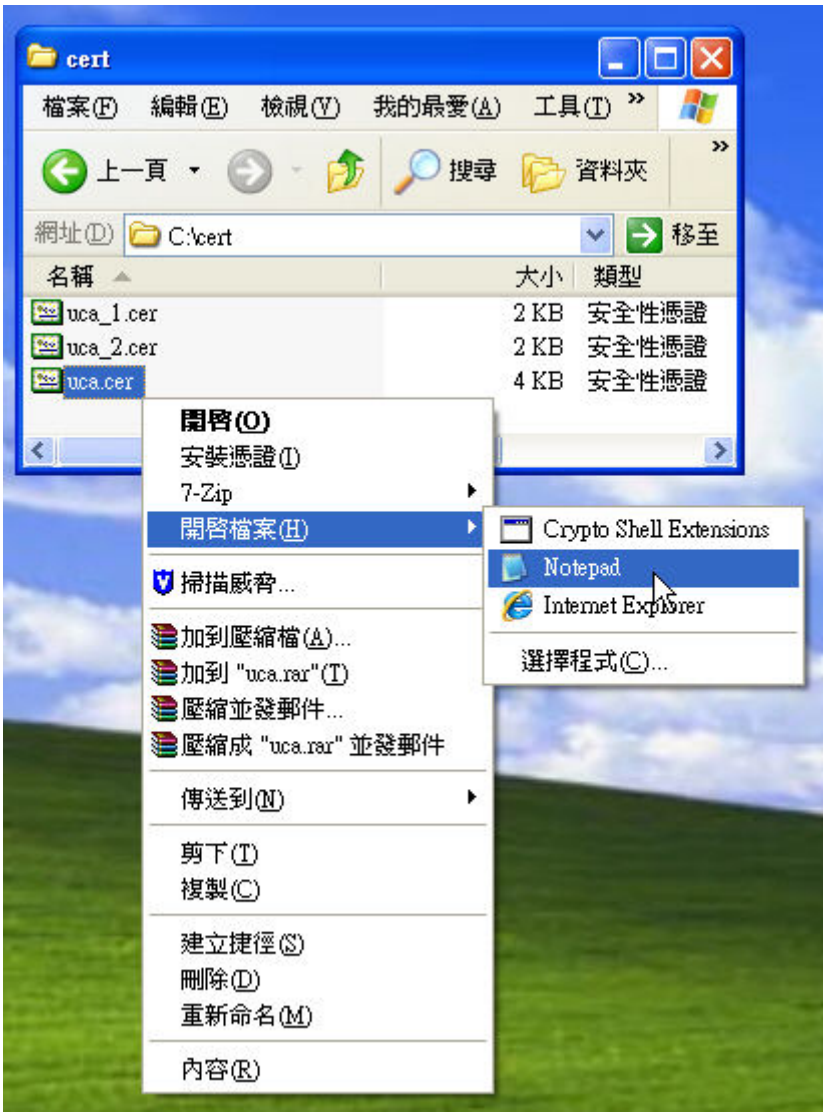
copy uca_2.cer+uca_1.cer uca.cer



完成上列指令後，該目錄下會新增一檔名為 uca.cer 的檔案。



使用文字編輯器打開 uca.cer 檔



可看到如下內容

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

$SOME TEXT

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

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

$SOME TEXT

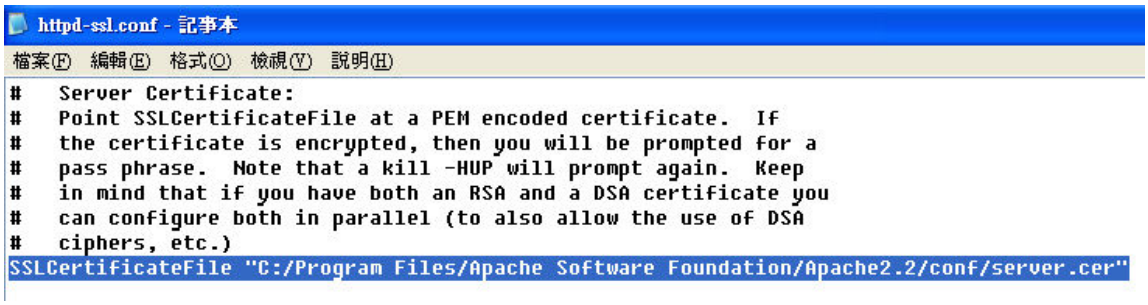
-----END CERTIFICATE-----

內容範例如下圖所示

4.6.3 編輯%Apache2.2%\conf\extra 目錄下的 httpd-ssl.conf 檔案

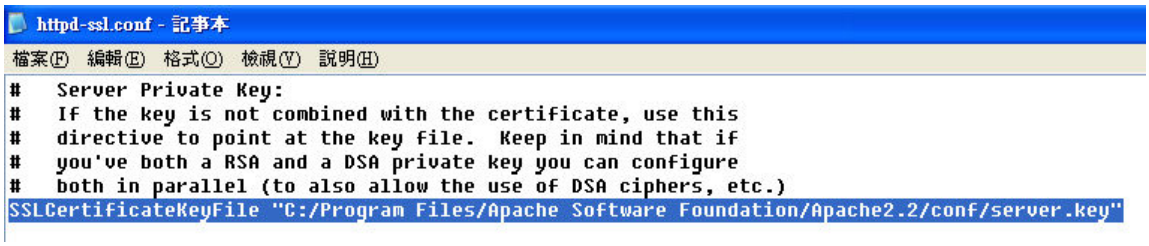
4.6.3.1 安裝伺服器憑證

搜尋「SSLCertificateFile」字串，可找到其中的 SSLCertificateFile 設定，此設定是 SSL 伺服器憑證存放完整路徑，請依 4.6.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。



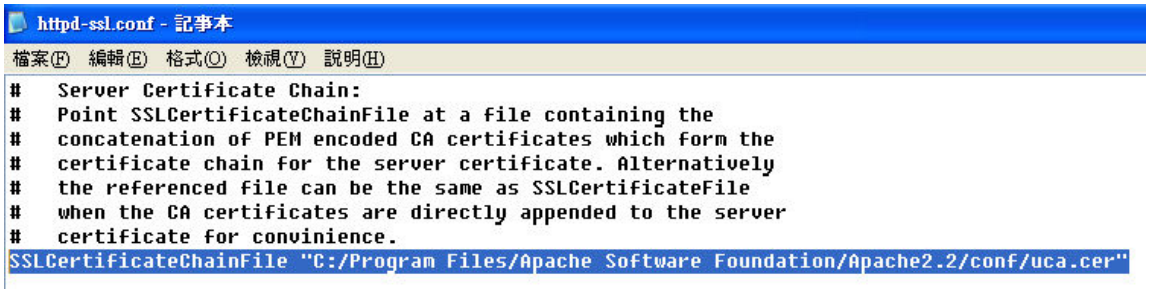
4.6.3.2 安裝 SSL 伺服器金鑰

搜尋「SSLCertificateKeyFile」字串，可找到其中的 SSLCertificateKeyFile 設定，此設定是 SSL 伺服器金鑰存放完整路徑，請依 4.6.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。



4.6.3.3 安裝中繼憑證

搜尋「SSLCertificateChainFile」字串，可找到其中的 SSLCertificateChainFile 設定，此設定是中繼憑證存放完整路徑，請依 4.6.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。



完成「httpd-ssl.conf」內上述設定後儲存檔案，即完成憑證安裝。

4.6.4 重新啟動 Apache 服務

重新啟動完成即可進入 4.8 節，驗證 SSL 功能。

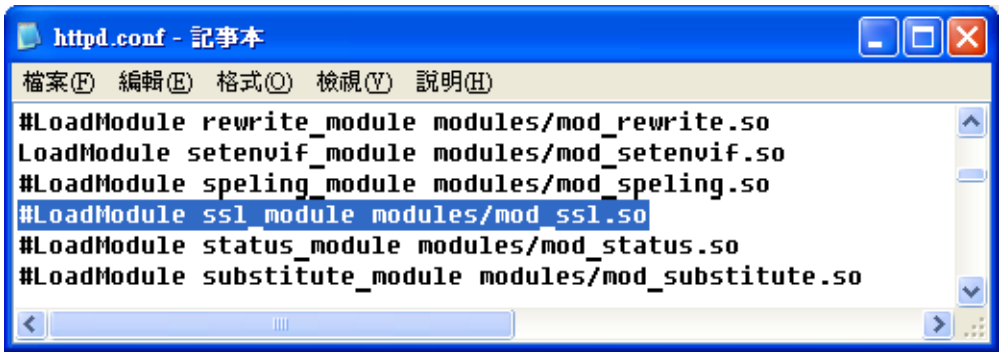
4.7 設定 SSL 模式

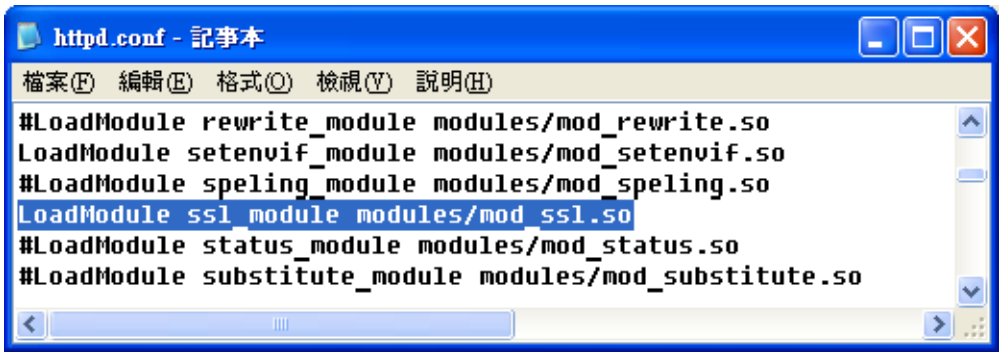
※若安裝主機非首次申請 SSL 憑證，SSL 功能正常，此章節可跳過不必設定！

4.7.1 編輯%Apache2.2%\conf 目錄下的 httpd.conf 檔案

4.7.1.1 載入 SSL 模組

搜尋「mod_ssl.so」字串，可找到其中的 LoadModule ssl_module modules/mod_ssl.so 指令，如果指令前有#字號，請將該指令前的#字號移除。





4.7.1.2 載入額外的設定檔 httpd-ssl.conf

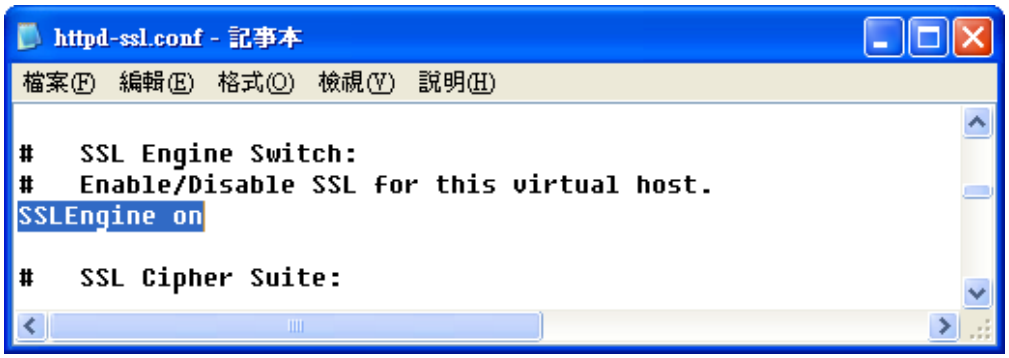
搜尋 httpd-ssl.conf (httpd-ssl.conf 設定檔是負責 SSL 的相關設定)，可找到其中的 Include conf/extra/httpd-ssl.conf 指令，如果指令前有#字號，請將該指令前的#字號移除。

確認完 httpd.conf 內上述兩項設定後儲存檔案。

4.7.2 編輯%Apache2.2%\conf\extra 目錄下的 httpd-ssl.conf 檔案

4.7.2.1 啟用 SSL 功能

搜尋「SSLEngine」字串，可找到其中的指令 SSLEngine on / off ，SSLEngine on 表示啟用 SSL 功能，如果不啟用 SSL 就將 on 改為 off 即可，這裡請設定為 on。



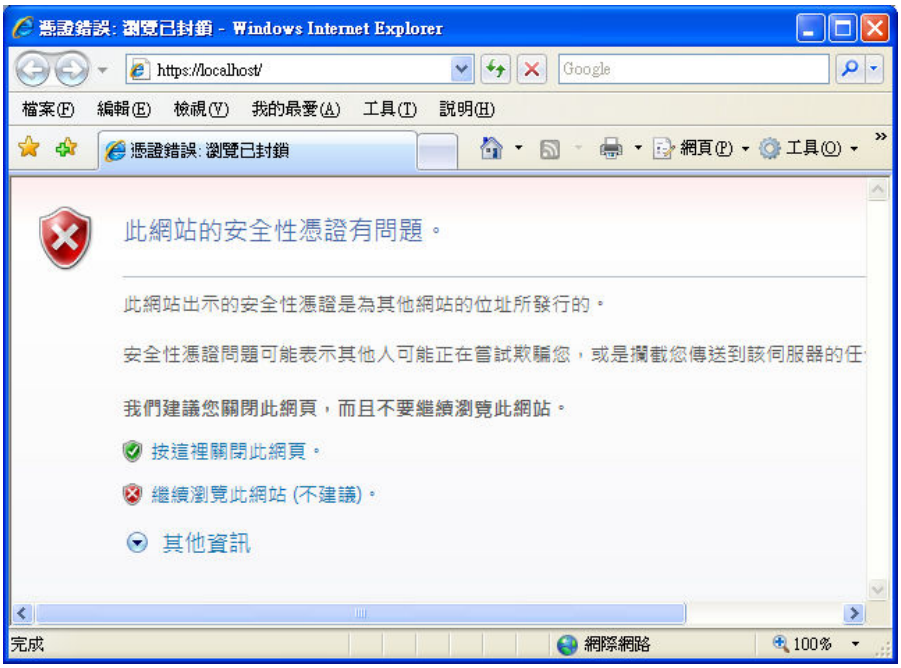
4.7.2.2 設定 SSL 連接埠

搜尋「Listen」字串，可找到其中的指令 Listen 443，443 Port 是 SSL(https)功能的預設 Port，如果要設定為其他 Port 再修改設定，否則一律設定為 443 即可。

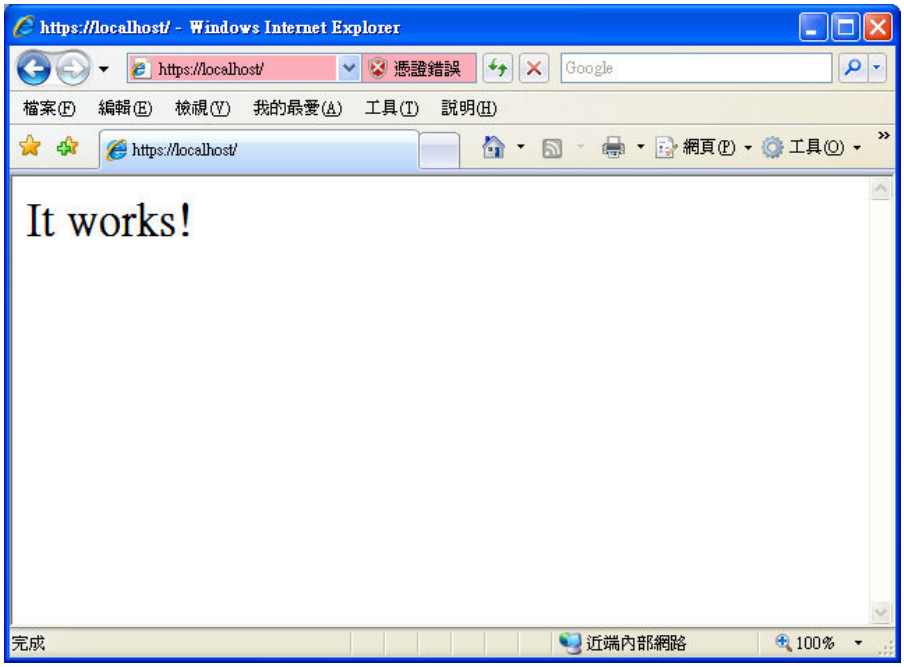
4.8 驗證 SSL 功能

4.8.1 本機驗證

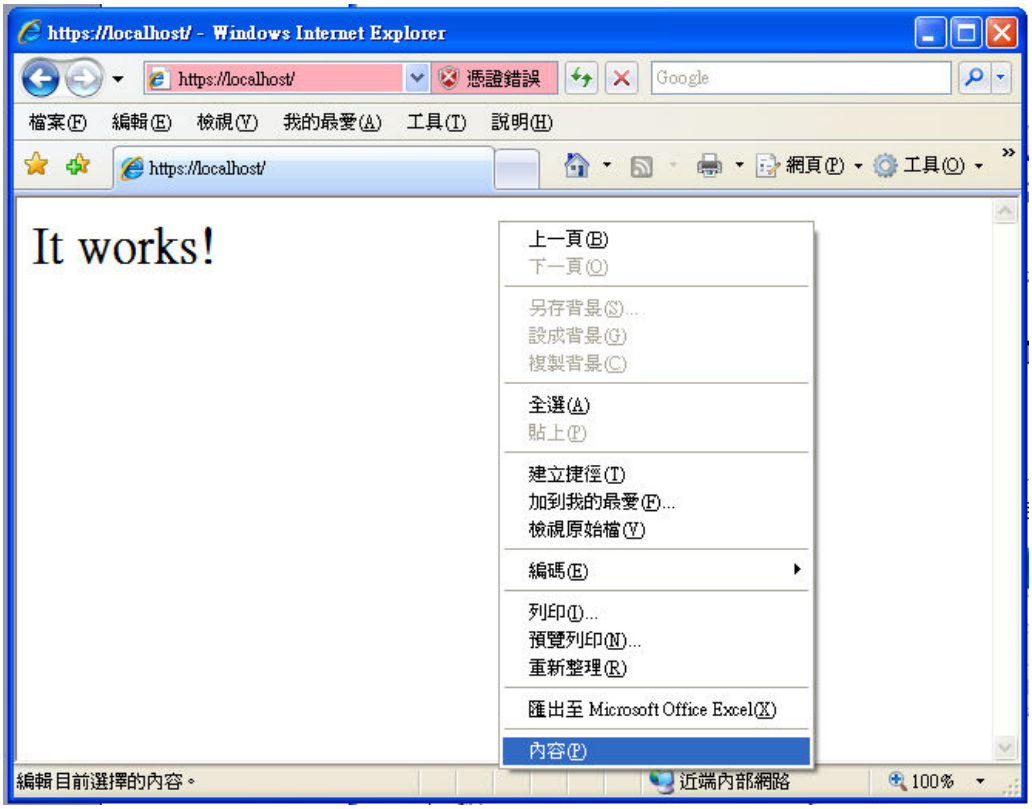
Apache 重新啟動完成後開啟瀏覽器直接連接至本機 https://localhost，此時出現警告訊息是正常的，因為憑證記載內容與網址不符(非 localhost)，請點選「繼續瀏此網站(不建議)」即可。



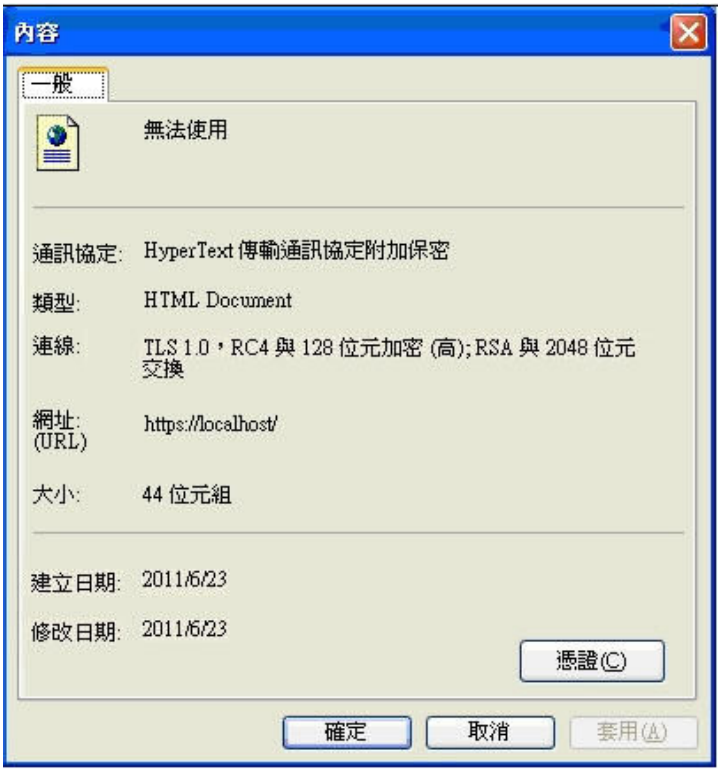
如果瀏覽器出現 It Works!字樣代表 Apache 已正常服務，且 SSL 功能已啟用。



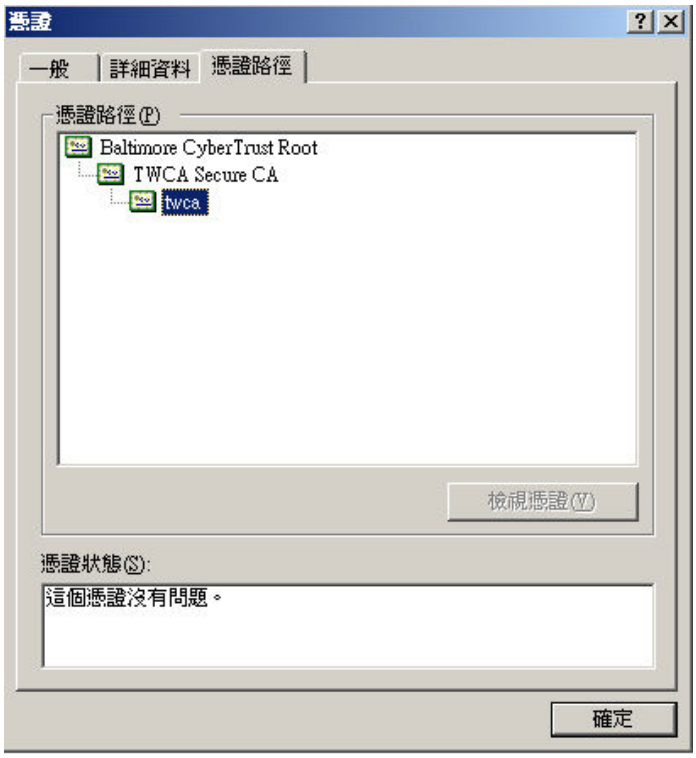
在瀏覽器按滑鼠右鍵出現功能清單，點選「內容」，



此時會出現網頁資訊，確認網頁是否已加密，點選憑證可檢視憑證資訊



憑證路徑欄位：請確認憑證鏈是否正確，且憑證狀態顯示這個憑證沒有問題，可確認憑證已安裝成功。



4.8.2 外部驗證

驗證程序和 4.8.1 節相同，只是連線位址改為實際網址，

如 https://www.twca.com.tw

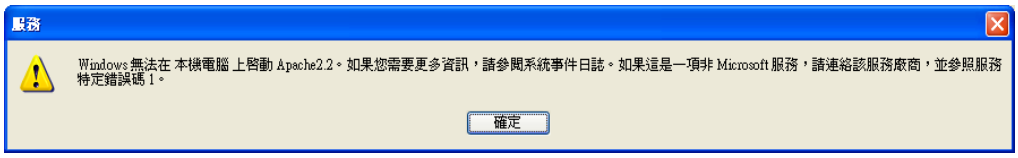
4.8.3 為何連線位址正確卻無法顯示網頁?

https 連線埠預設使用 443 Port，如果 4.7.7.2 節設定 Listen Port 非 443，則連線時須指定連線 Port，如 https://www.twca.com.tw:8443

4.9 異常排除

如果完成 4.6 及 4.7 章節設定後，重新啟動 Apache 時出現下面的錯誤訊息，表示 SSL 設定有誤，請檢視%Apache2.2%\logs\error.log 檔，該檔案內會記錄啟動失敗原因，待問題排除後再重新啟動。

如果持續發生問題，請聯絡本公司協助處理。



4.10 備份／復原憑證

請將 4.6.1 章節指定的三個檔案備份起來(金鑰、伺服器憑證、中繼憑證)，再依照 4.6 章節的步驟設定，即可復原憑證。

4.11 更新 SSL 憑證

4.11.1 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。

4.11.2 更新步驟

4.11.2.1 備份憑證檔

在進行更新前請記得備份原有的 SSL 伺服器憑證及伺服器金鑰。

4.11.2.2 更新憑證

若安裝主機(站台)非首次申請 SSL 憑證，SSL 功能正常，
請參照 4.2 至 4.6 章節申請安裝憑證，即可完成 SSL 憑證更新。

5.附件

無。