SSL 伺服器數位憑證 Tomcat 8.5

伺服器操作手冊

機密等級：公開
版本：V5.2
文件編號：MNT-03-131
生效日期：110 年 8 月 10 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 Tomcat 8.5 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.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 安裝 Java JDK/JRE 軟體

本操作手冊安裝環境為 jdk1.8.0_191。

5.1.2 安裝 Tomcat 8.5 Web 伺服器軟體

本操作手冊安裝環境為 Tomcat 8.5.35 (Windows 版)。

5.2 產製「金鑰」

5.2.1 在%JDK%\bin\目錄下，輸入>keytool -genkey -alias keyname -keyalg RSA -keysize 2048 -keystore c:\mykeystore.jks

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -genkey -alias keyname -keyalg RSA
  -keysize 2048 -keystore c:\mykeystore.jks
```

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說　明
-genkey	產製金鑰必要指令
-alias	指定產製的金鑰名稱，安裝憑證時會使用，請自行指定
-keyalg	產製金鑰所用的演算法，固定填 RSA 即可
-keysize	產製的金鑰長度，固定填 2048 即可
-keystore	金鑰存放的金鑰儲存庫檔案路徑及名稱，請自行指定

此時會要求輸入金鑰儲存庫密碼(最少 6 個字元)，請直接輸入金鑰儲存庫密碼並確認

出現您的名字與姓氏為何?請輸入貴公司欲加密的網站名稱，例 www.twca.com.tw

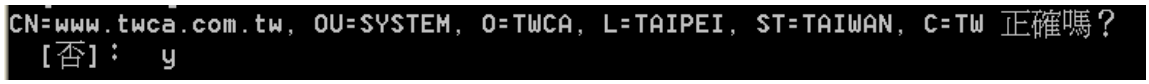
出現您的組織單位名稱為何?請輸入組織單位名稱，例 SYSTEM

出現您的組織名稱為何?請輸入組織名稱，例 TWCA

出現您所在的城市或地區名稱為何?請輸入城市或地區，例 TAIPEI

出現您所在的州及省份名稱為何?請輸入城市或地區，例 TAIWAN

出現單位的二個字母國碼為何?請輸入單位的二個字母國碼，例 TW



完成後會確認輸入資訊是否正確，如果正確請按 Y，要重填請按 N，

此時會要求輸入金鑰密碼(與金鑰儲存庫密碼不同)，不要輸入任何密碼直接按 Enter 即可，保持金鑰儲存庫及金鑰密碼相同。

完成上列指令後會在 C:\下產生檔案名稱為 mykeystore.jks 的金鑰檔

5.3 產生「憑證請求檔(CSR)」

5.3.1 在%JDK%\bin\目錄下，輸入

keytool -certreq -alias keyname -file c:\mycsr.txt -keystore c:\mykeystore.jks

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -certreq -alias keyname -file c:\
mycsr.txt -keystore c:\mykeystore.jks
```

指令參數說明如下(指令反白部份請依實際路徑決定)

參數	說　　明
-certreq	產製 CSR 必要指令
-alias	產製 CSR 所使用的金鑰名稱，請跟 5.2.1 章節所產製的金鑰名稱相同
-file	產製 CSR 後存放的路徑及檔案名稱，請自行指定
-keystore	金鑰存放的金鑰儲存庫檔案路徑及名稱，請跟 5.2.1 章節所產生的金鑰儲存庫路徑及名稱相同

```
輸入金鑰儲存庫密碼:
```

此時會要求輸入金鑰儲存庫密碼，請輸入密碼後按 Enter 即可，

完成上列指令後會在 C:\下產生檔案名稱為 mycsr.txt 的憑證請求檔

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。

5.4.2 連接 TWCA 網站(2)

點選申請憑證。

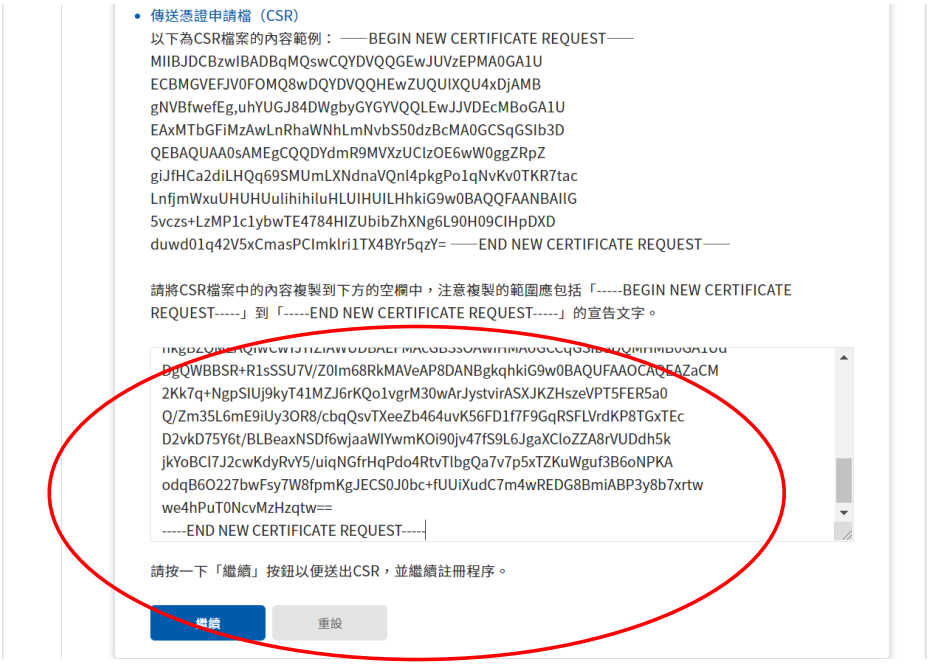
※如申請 EV SSL 伺服器憑證，請點選 EV SSL 憑證。

5.4.3 連接 TWCA 網站(3)

將瀏覽器視窗畫面往下拉，上傳 CSR。

5.4.4 貼上憑證請求檔

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。



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 EAMIL 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

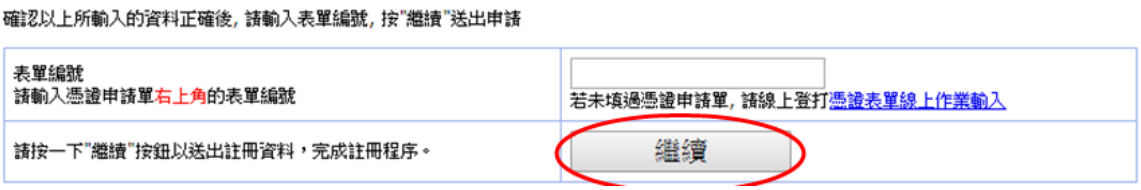
二、檔案驗證：請您填入收取該檔案收件人 EMAIL,您將在此 EMAIL 收到一附件檔案,請您依照信件說明將檔案放入,完成後請通知我們進行檔案驗證作業。

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,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。



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

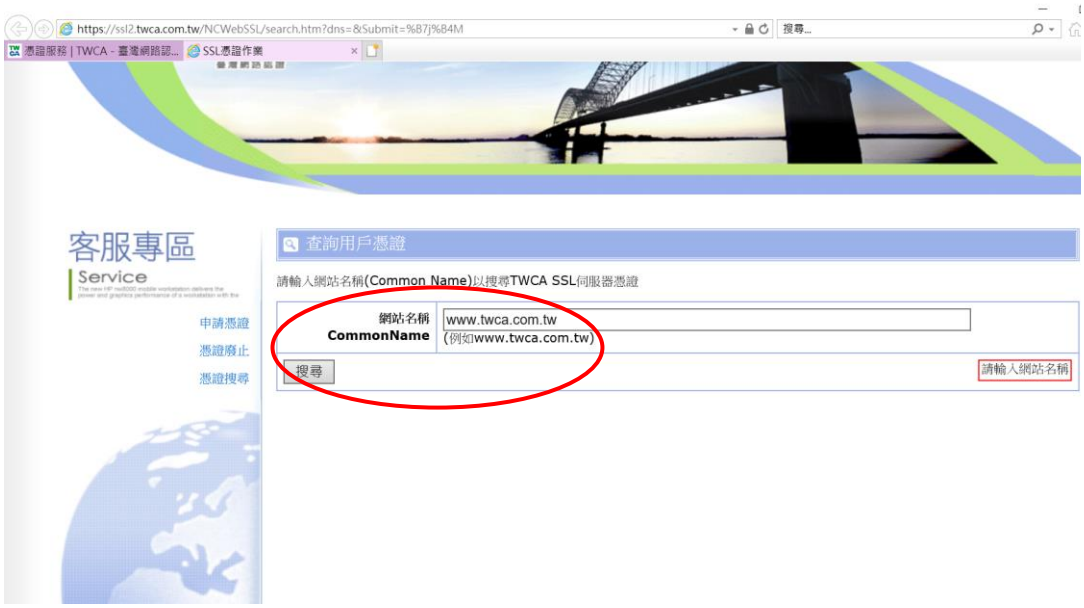
點選憑證服務，點選 SSL 憑證。

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 安裝憑證

5.6.1 Tomcat 在安裝 SSL 憑證時會使用到以下檔案：

- 於 5.2 章節產製的 SSL 金鑰儲存庫「mykeystore.jks」
- 於 5.5 章節取得的三個憑證鏈檔

將憑證鏈檔其存放至%JDK%\bin 目錄下(實際目錄可自行決定)。

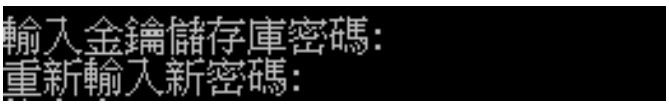
5.6.2 請將憑證由上至下(根憑證 root.cer、中繼憑證 uca.cer、伺服器憑證 server.cer)一一匯入金鑰儲存庫。

5.6.2.1 匯入根憑證 root.cer

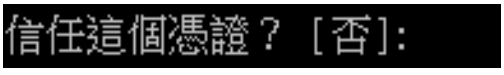
keytool -import -trustcacerts -alias root -file root.cer -keystore C:\mykeystore.jks

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說　　明
-import	匯入憑證必要指令
-trustcacerts	建立為信任的憑證鏈
-alias	設定根憑證別名，請自行決定即可
-file	要匯入的根憑證路徑及名稱，請依實際位置指定
-keystore	金鑰儲存庫檔案所在路徑及名稱，請依實際位置指定



此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼並確認



如出現上面訊息，請輸入 y 再按 Enter 即可，

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

5.6.2.2 匯入中繼憑證 uca.cer

keytool -import -trustcacerts -alias uca -file uca.cer -keystore C:\mykeystore.jks

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說　　明
-import	匯入憑證必要指令
-trustcacerts	建立為信任的憑證鏈
-alias	設定中繼憑證別名，請自行決定即可
-file	要匯入的中繼憑證路徑及名稱，請依實際位置指定
-keystore	金鑰儲存庫檔案所在路徑及名稱，請依實際位置指定

此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼，

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

5.6.2.3 匯入伺服器憑證 server.cer

keytool -import -trustcacerts -alias keyname -file server.cer -keystore C:\mykeystore.jks

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -import -trustcacerts -alias keyna
me -file server.cer -keystore C:\mykeystore.jks
```

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說　　明
-import	匯入憑證必要指令
-trustcacerts	建立為信任的憑證鏈
-alias	指定伺服器金鑰名稱，請與 5.2.1 章節設定的名稱相同
-file	要匯入的伺服器憑證路徑及名稱，請依實際位置指定
-keystore	金鑰儲存庫檔案所在路徑及名稱，請依實際位置指定

```
輸入金鑰儲存庫密碼:
```

此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼，

```
憑證回覆已安裝在金鑰儲存庫中
```

出現「憑證回覆已安裝至金鑰儲存庫中」即匯入完成。

若出現下列訊息，則安裝失敗:

```
金鑰工具錯誤: java.lang.Exception: 無法從回覆中將鏈建立起來
```

安裝伺服器憑證出現上列訊息，表示根憑證及中繼憑證尚未安裝完成，請先將根憑證及中繼憑證安裝至金鑰儲存庫中。

```
金鑰工具錯誤: java.lang.Exception: 回覆時的公開金鑰與金鑰儲存庫不符
```

安裝伺服器憑證出現上列訊息，表示金鑰儲存庫內的私鑰無法與伺服器憑證裡的公鑰配對，請確認產製 CSR 時指定的金鑰儲存庫跟匯入憑證指定的金鑰儲存庫是同一個。

5.6.2.4 檢視憑證是否安裝成功

keytool -list -keystore C:\mykeystore.jks

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -list -keystore C:\mykeystore.jks
```

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說　　明
-list	顯示金鑰儲存庫中的憑證資訊
-keystore	金鑰儲存庫檔案所在路徑及名稱，請依實際位置指定

```
輸入金鑰儲存庫密碼:
```

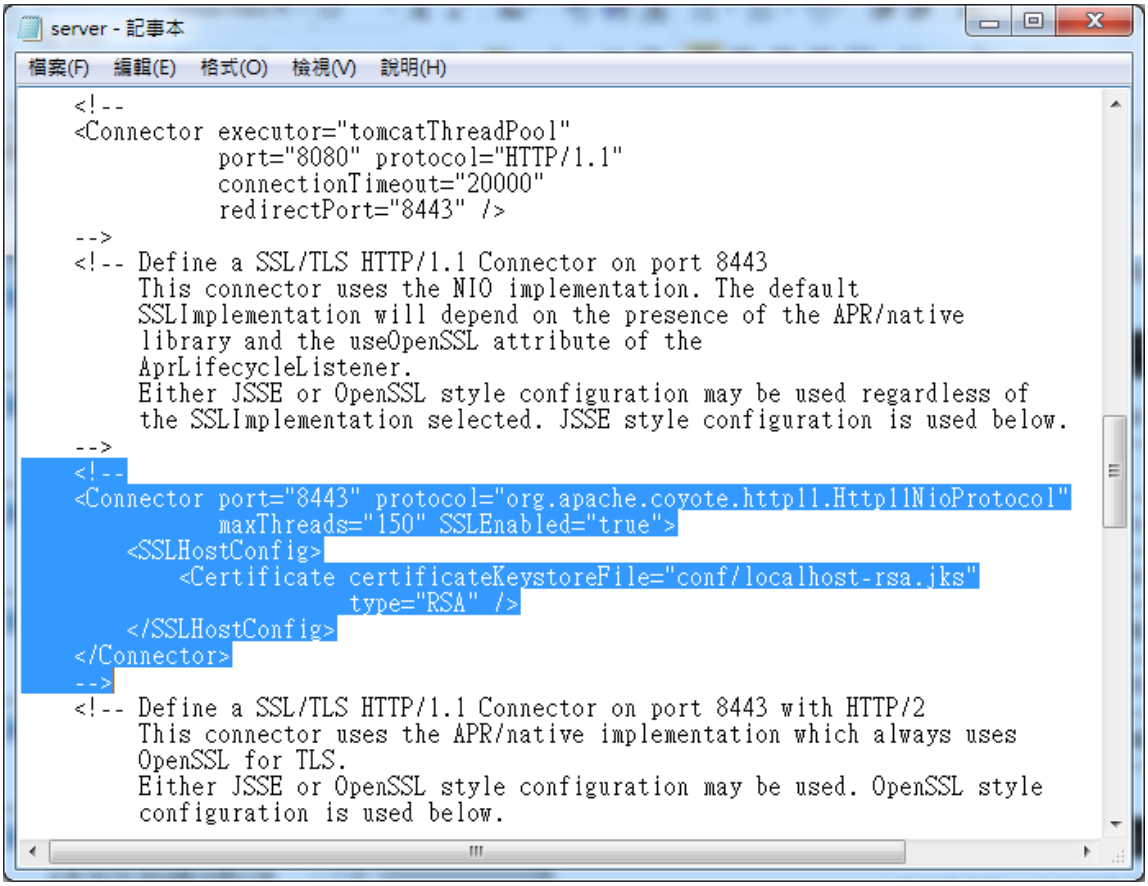
此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼

若看到以下畫面則表示憑證安裝成功:包含一個 PrivateKeyEntry(伺服器金鑰)、和兩個 trustedCertEntry(根憑證、中繼憑證)

```
root, 2018/11/27, trustedCertEntry,
憑證指紋 (SHA1): CF:9E:87:6D:D3:EB:FC:42:26:97:A3:B5:A3:7A:A0:76:A9:06:23:48
uca , 2018/11/27, trustedCertEntry,
憑證指紋 (SHA1): FD:54:E4:64:3B:49:70:5A:2A:AA:E5:06:53:C4:F5:6C:2D:F8:08:3D
keyname, 2018/11/27, PrivateKeyEntry,
憑證指紋 (SHA1): 99:AC:40:24:F6:D9:4C:0B:00:43:AB:39:3D:92:EA:5A:6E:D3:9E:4F
```

5.6.3 編輯%Tomcat 8.5%\conf 目錄下的 server.xml 檔案，

5.6.3.1 搜尋「org.apache.coyote.http11.Http11NioProtocol」字串，可找到其中跟 SSL 相關的指令，



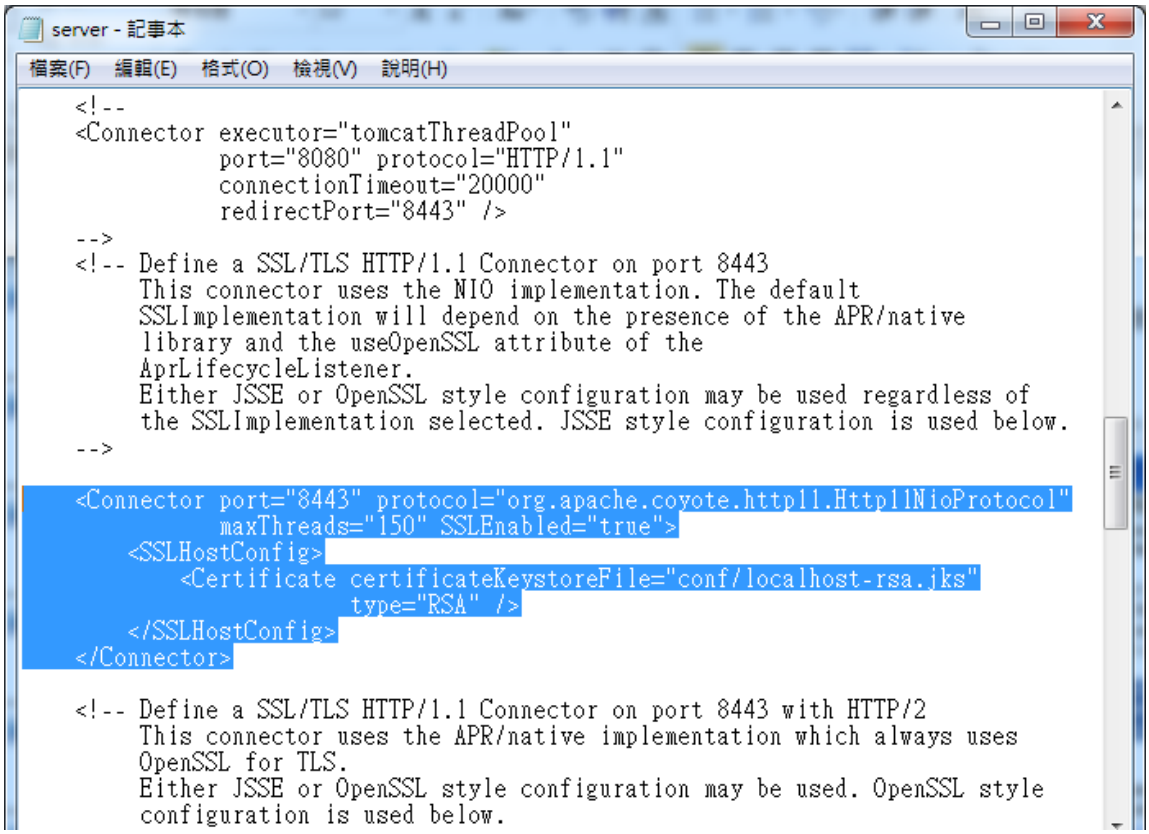
如果是第一次進行 SSL 設定，請將

```
<!--
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150" SSLEnabled="true">
<SSLHostConfig>
<Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
type="RSA" />
</SSLHostConfig>
</Connector>
-->
```

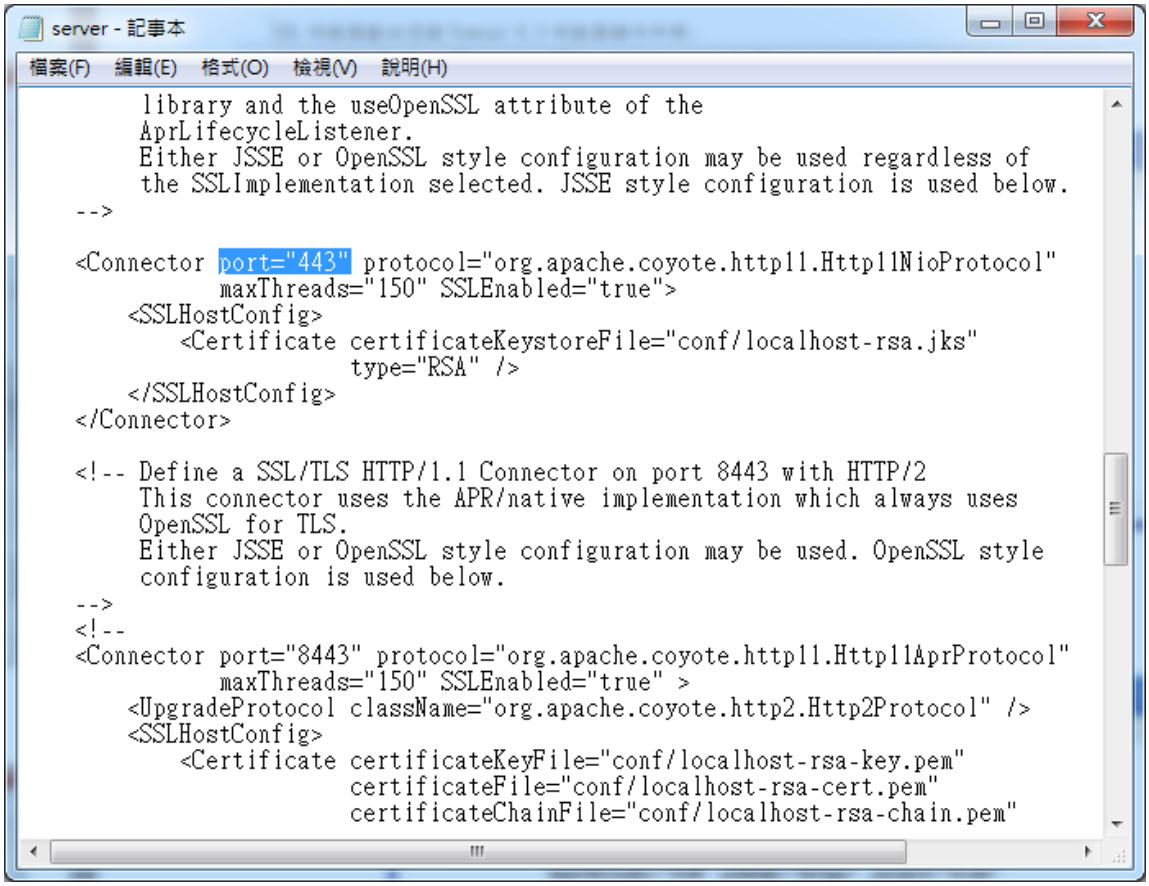
前後的**<!--**及**-->**符號移除，因為在 Tomcat 設定檔中，由<!--及-->符號

所

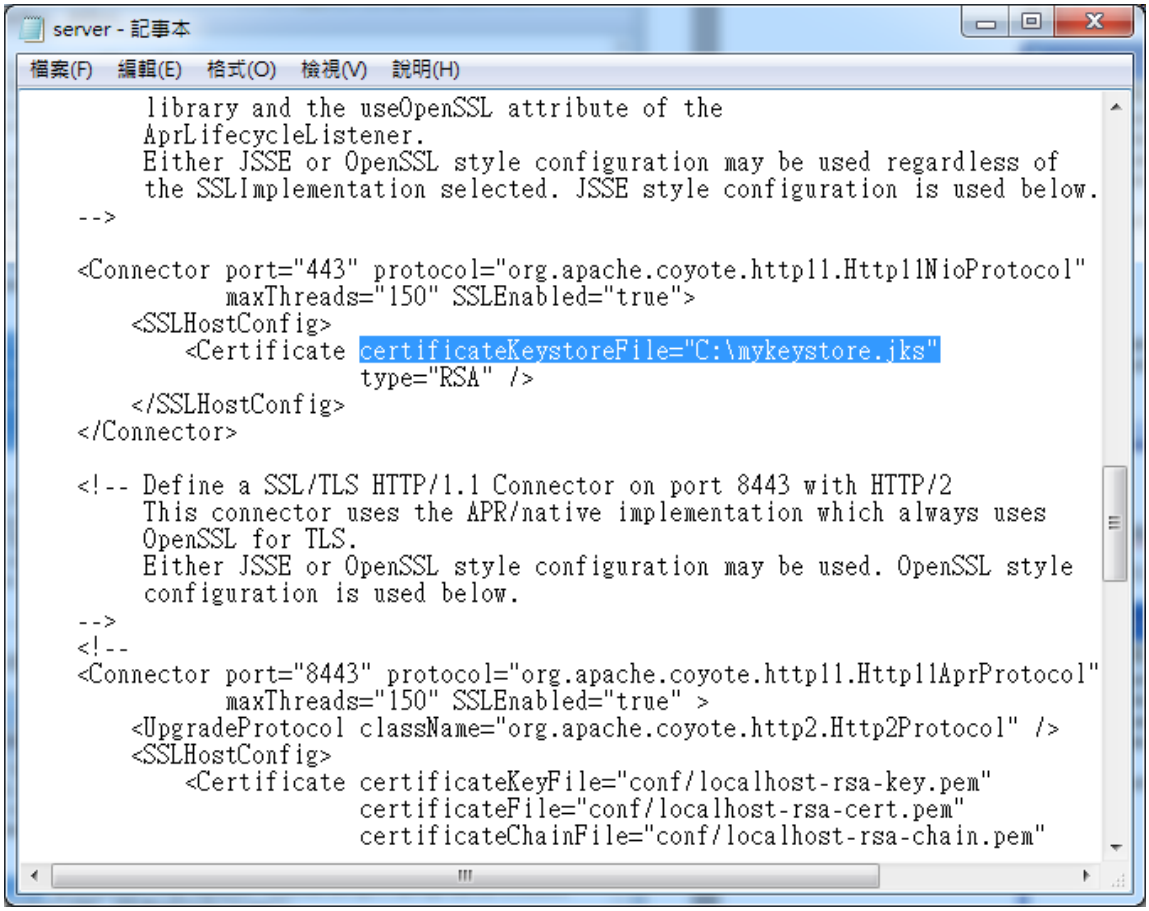
包含的文字視為註解。



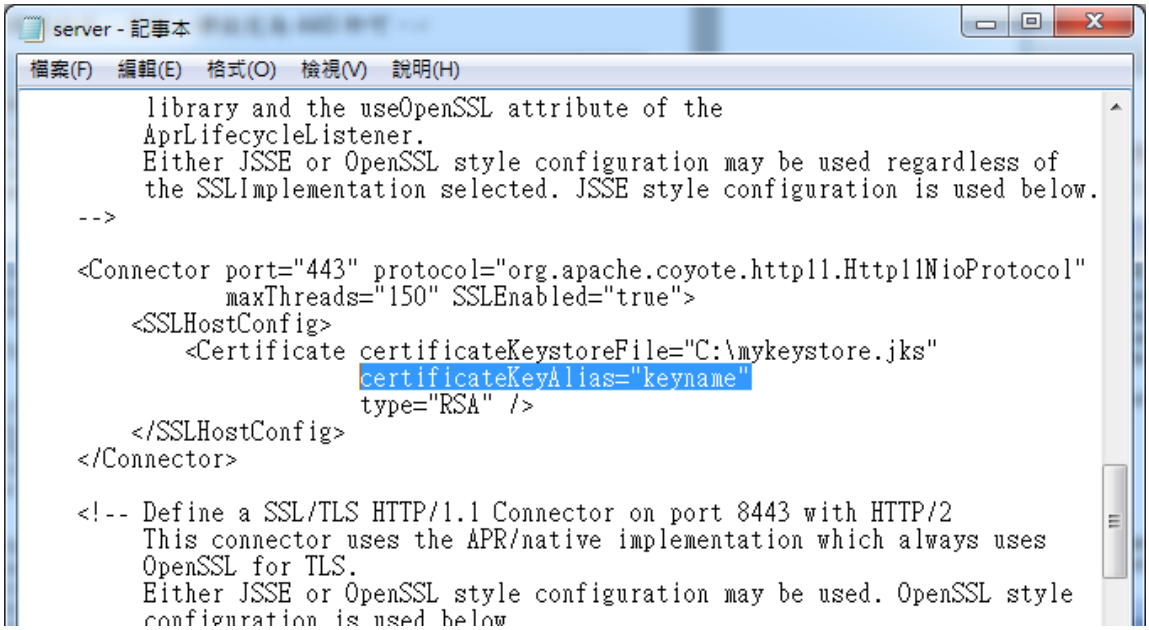
5.6.3.2 將 Port 改為 443，443 Port 是 SSL(https)功能的預設 Port，如果要設定為其他 Port 再修改設定，否則一律設定為 443 即可。



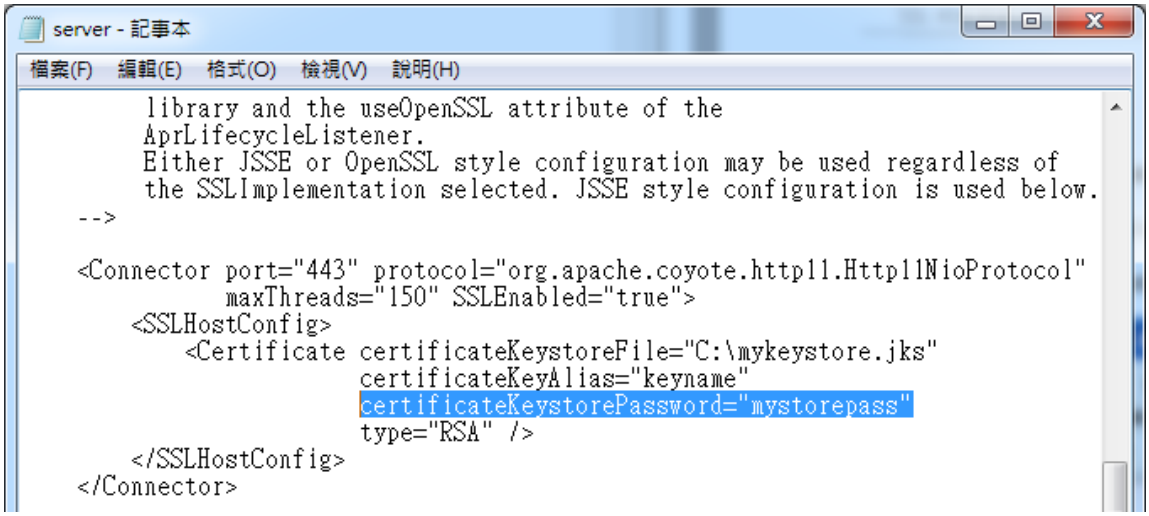
5.6.3.3 新增「certificatekeystoreFile」設定，此設定是金鑰儲存庫存放完整路徑，請依檔案實際存放路徑設定即可，路徑前後請用「"」包起來。



5.6.3.4 新增「certificatekeyAlias」設定，此設定是 SSL 伺服器憑證金鑰名稱，請與 5.2.1 章節設定的名稱相同，前後請用「"」包起來。



5.6.3.5 新增「certificatekeystorePassword」設定，此設定是金鑰儲存庫密碼，直接填寫密碼即可，前後請用「"」包起來，



5.6.3.6 重新啟動 Tomcat 服務

重新啟動完成即可進入 5.7 章節，驗證 SSL 功能。

如果完成 5.6 章節設定後，重新啟動 Tomcat 失敗，或是啟動成功，但是 SSL 功能無法正常連線，表示 SSL 設定有誤，請檢視 %Tomcat%\logs\catalina.yyyy-mm-dd.log 檔，該檔案內會記錄啟動錯誤訊息，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。

5.7 驗證 SSL 功能

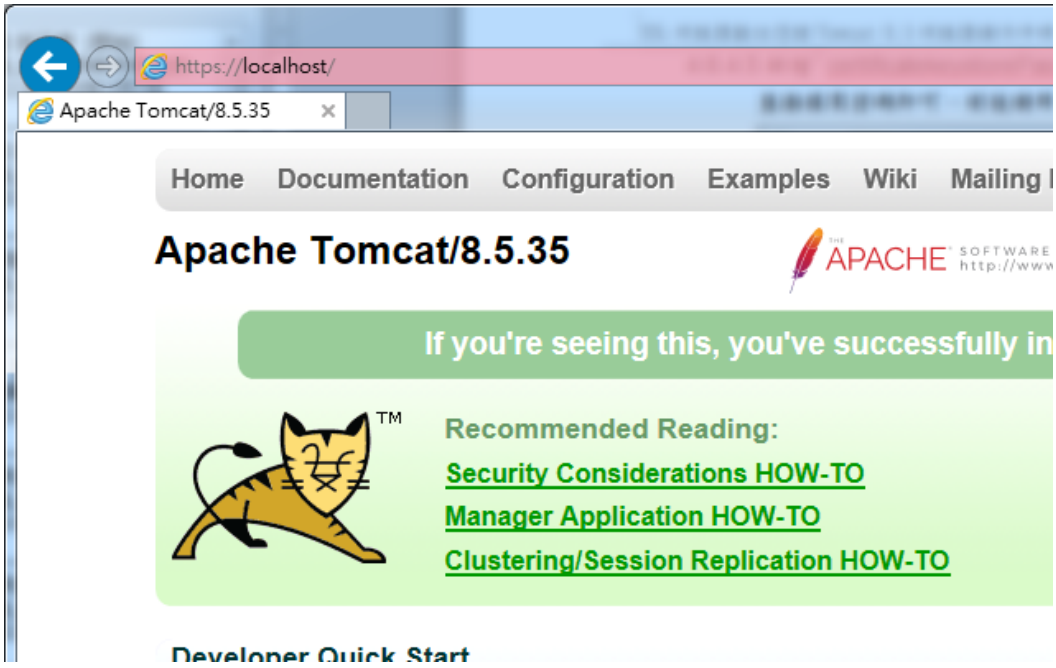
5.7.1 本機驗證

Tomcat 重新啟動完成後開啟瀏覽器直接連接至本 https://localhost，

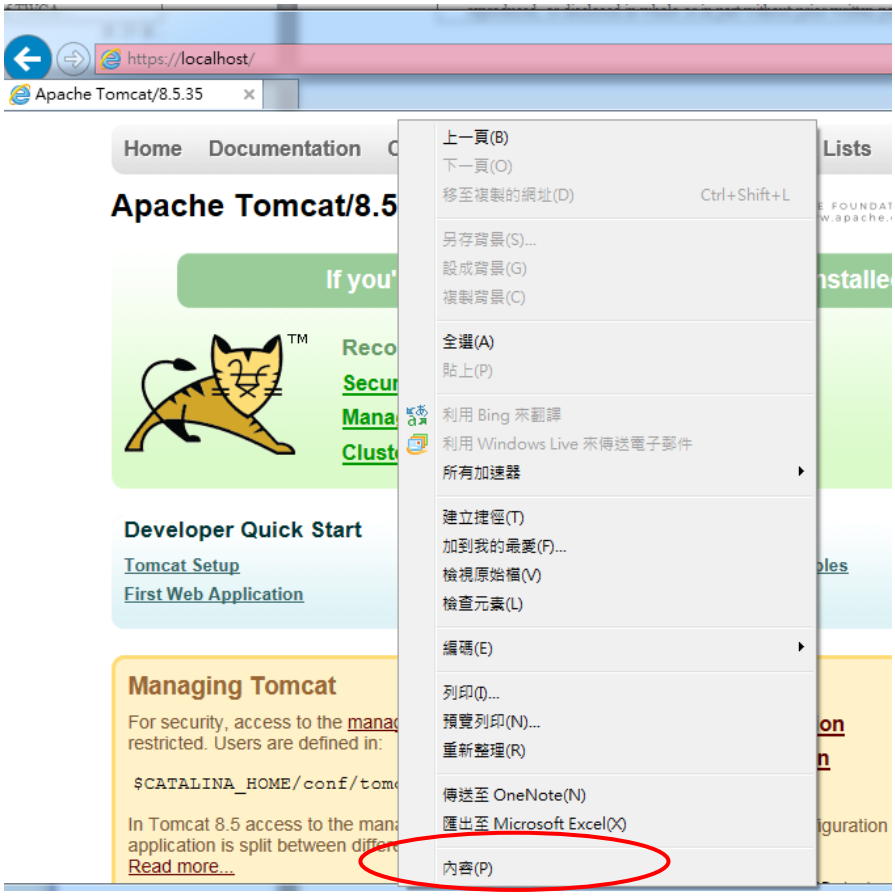
此時出現警告訊息是正常的，因為憑證記載內容與網址不符

(非 localhost)，請點選「繼續瀏此網站(不建議)」即可。

如果瀏覽器出現 Tomcat 歡迎頁面表示已正常服務，且 SSL 功能已啟動，

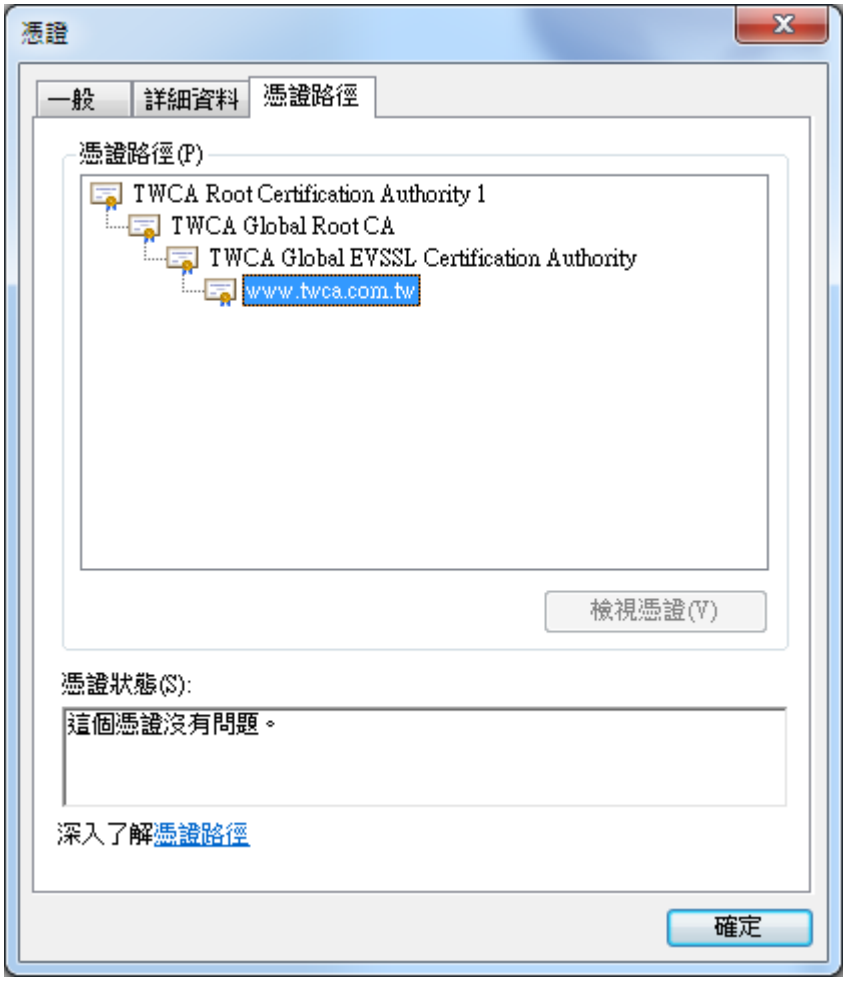


在瀏覽器按滑鼠右鍵出現功能清單，點選「內容」，



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。



5.7.2 外部驗證

驗證程序和 5.7.1 章節相同，只是連線位址改為實際網址，

如 https://www.twca.com.tw

5.7.3 為何連線位址正確卻無法顯示網頁?

https 連線預設使用 443 Port，如果 5.6.5.2 章節設定 Connector Port 非 443，則連線時須指定連線 Port，如 https://www.twca.com.tw:8443

5.8 備份／復原憑證

用戶只需將 5.6.2 章節 keystore(內含根憑證、中繼憑證及伺服器憑證)備份至安全的位置，復原時再依照「5.6.3 編輯%Tomcat 8.5%\conf 目錄下的 server.xml 檔案」的敘述進行即可。

5.9 更新 SSL 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

5.9.2.1 備份憑證檔

在進行更新前請記得備份您原有的伺服器金鑰檔(金鑰儲存庫)。

5.9.2.2 更新憑證

請參照 5.2 至 5.6 章節的步驟重新申請安裝憑證，即可完成 SSL 憑證更新。

5.常見問題

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

6.附件

無。