SSL 伺服器數位憑證 Tomcat 6.0

伺服器操作手冊

機密等級：公開
版本：V1.2
文件編號：MNT-03-084
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 Tomcat 6.0 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 Java JDK/JRE 軟體

Tomcat 運作時需要 JDK/JRE 環境，也需要 Java keytool 軟體來產製金鑰，安裝 JDK/JRE 請至 http://java.sun.com/javase/downloads/index.jsp 下載，本操作手冊安裝環境為 jdk1.6.0_26，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 Tomcat 6.0 Web 伺服器軟體

Tomcat 6.0 Web 伺服器軟體是由 Apache 組織所提供的 Web 伺服器軟體，可至 http://tomcat.apache.org/下載，本操作手冊安裝環境為 Tomcat 6.0.35 (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。

4.2 產製「金鑰」

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

```
C:\Program Files\Java\jdk1.6.0_26\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 keystore 檔案路徑及名稱，請自行指定

此時會要求輸入 keystore 密碼(最少 6 個字元)，請直接輸入 keystore 密碼並確認

出現您的名字與姓氏為何?請輸入網站名稱，例 www.twca.com.tw

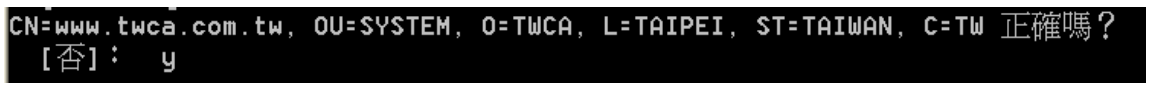
出現您的編制單位名稱為何?請輸入編制單位名稱，例 SYSTEM

出現您的組織名稱為何?請輸入組織名稱，例 www.twca.com.tw

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

出現單位的二字國碼為何?請輸入單位二字國碼，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 keystore 密碼不同)，不要輸入任何密碼直接按 Enter 即可，保持 keystore 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

4.3 產生「憑證請求檔(CSR)」

4.3.1 在%JDK%\bin\目錄下，輸入

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -certreq -alias keyname -file c:\m
ycsr.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 4.2.1 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 keystore 檔案路徑及名稱，請跟 4.2.1 章節所產生的 keystore 路徑及名稱相同

```
輸入 keystore 密碼:
```

此時會要求輸入 keystore 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

4.4 將製作好的憑證請求檔(CSR)上傳

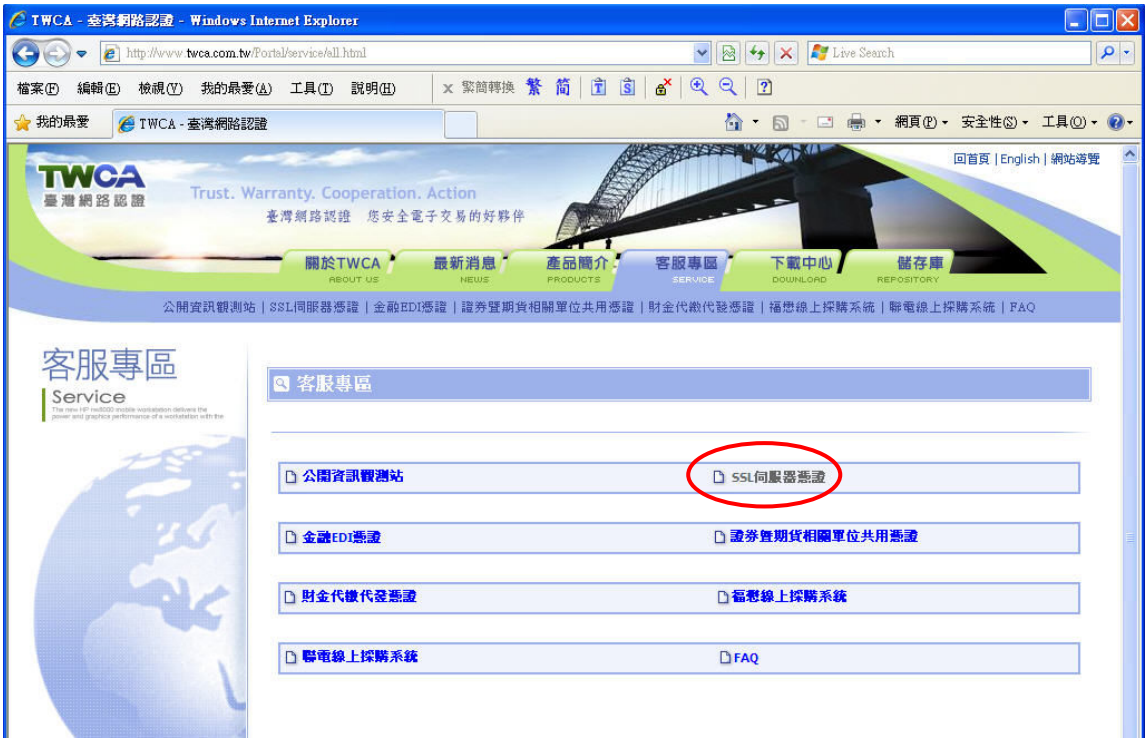
4.4.1 連接 TWCA 網站(1)

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)

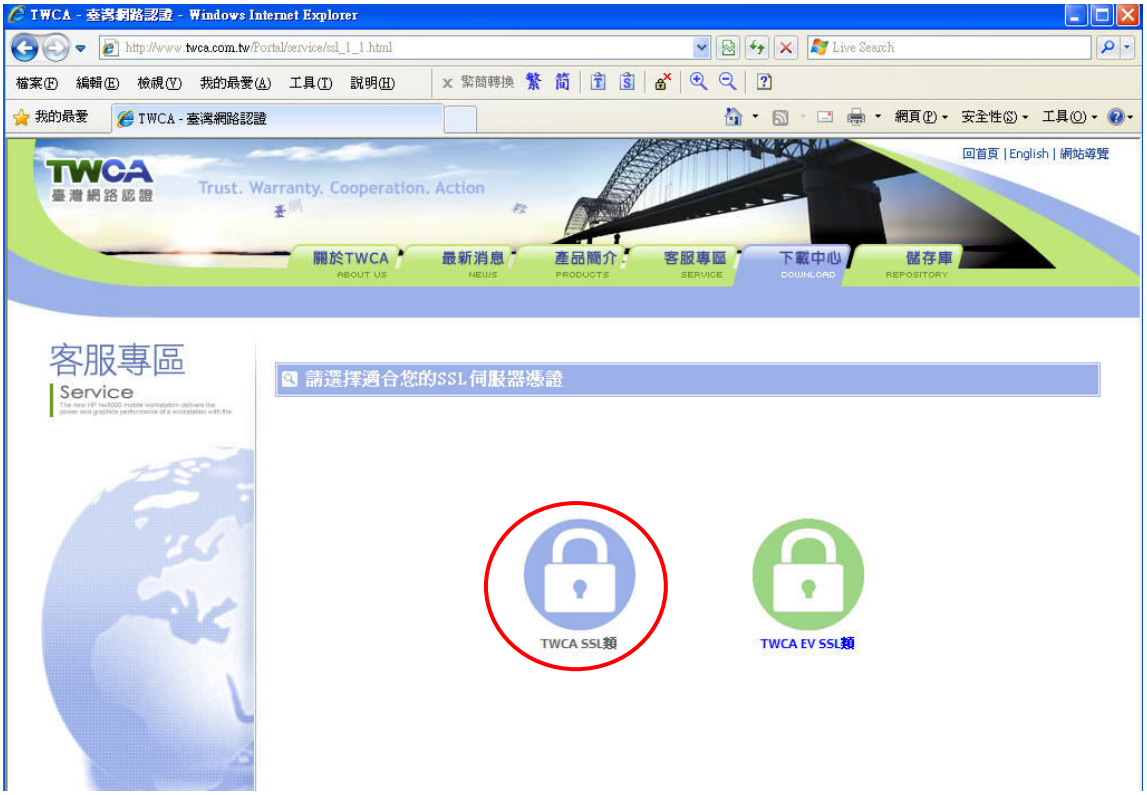
點選 SSL 伺服器憑證。



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。

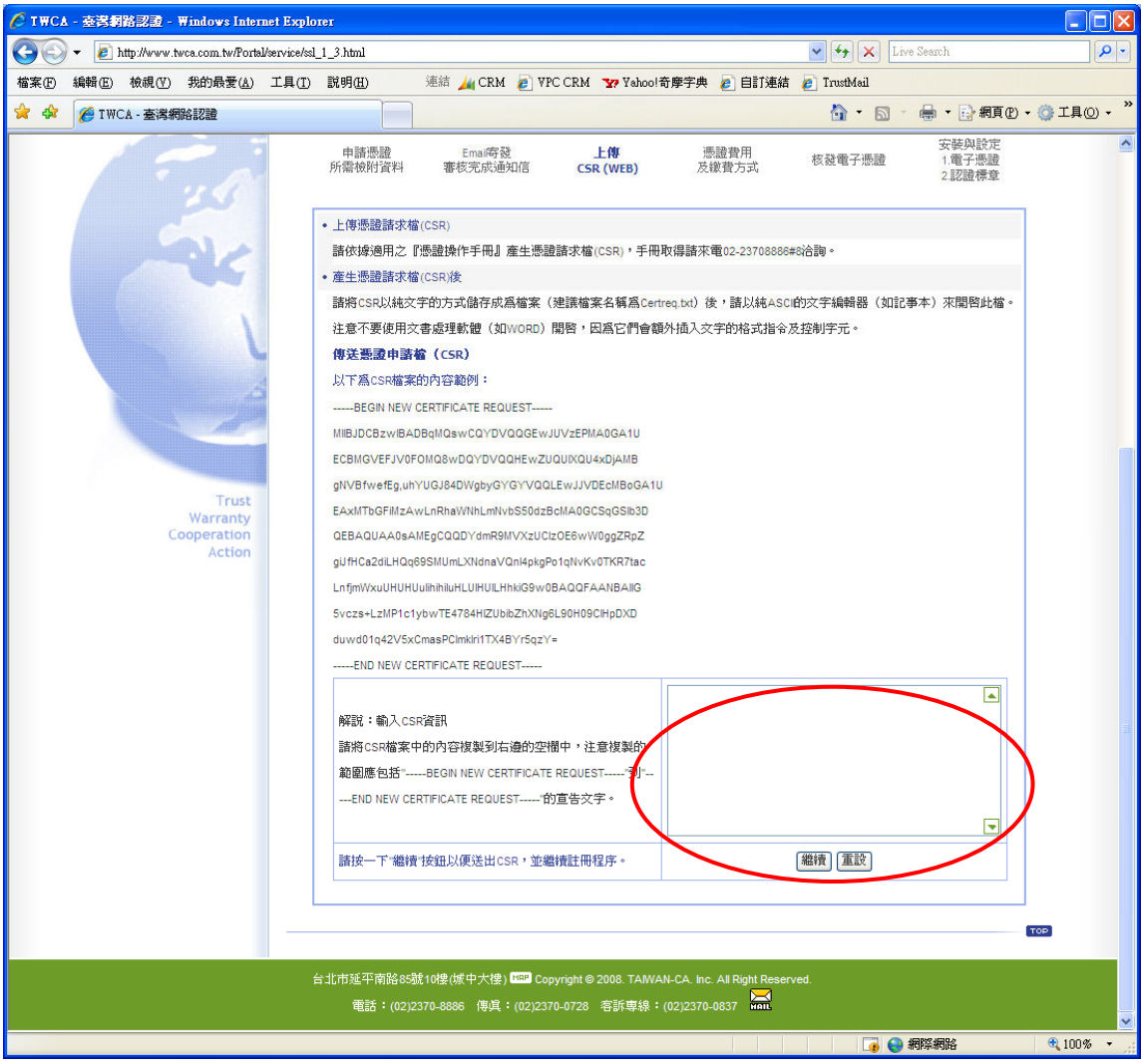


4.4.4 連接 TWCA 網站(4)

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

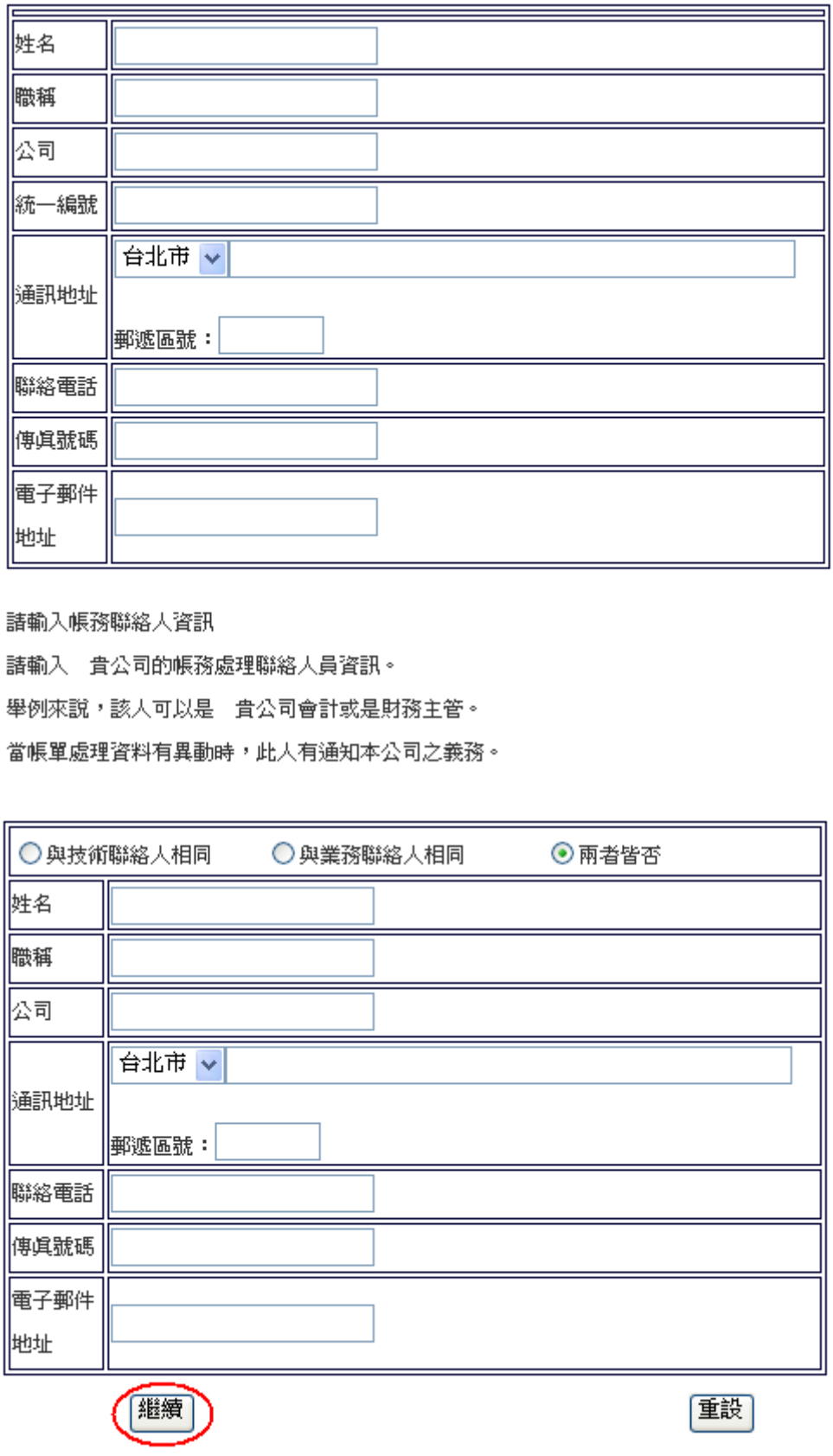
請輸入 貴公司負責SSL伺服器憑證業務聯絡人資訊於下表，並填寫本公司所要求的資訊。

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。

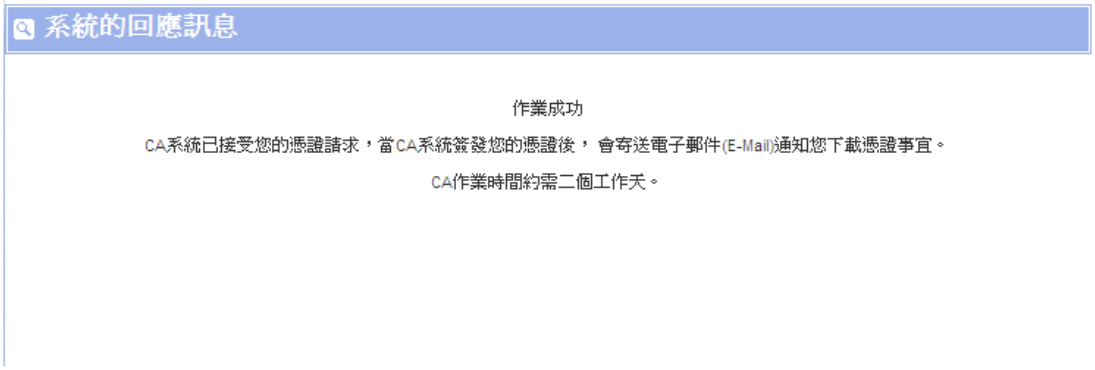
業務聯絡人與技術聯絡人不應為同一人，您應該分別指定。

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

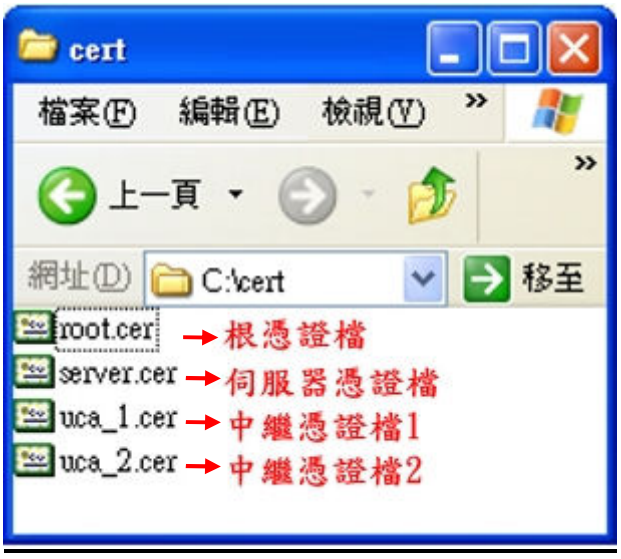
1 相關檔案說明

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

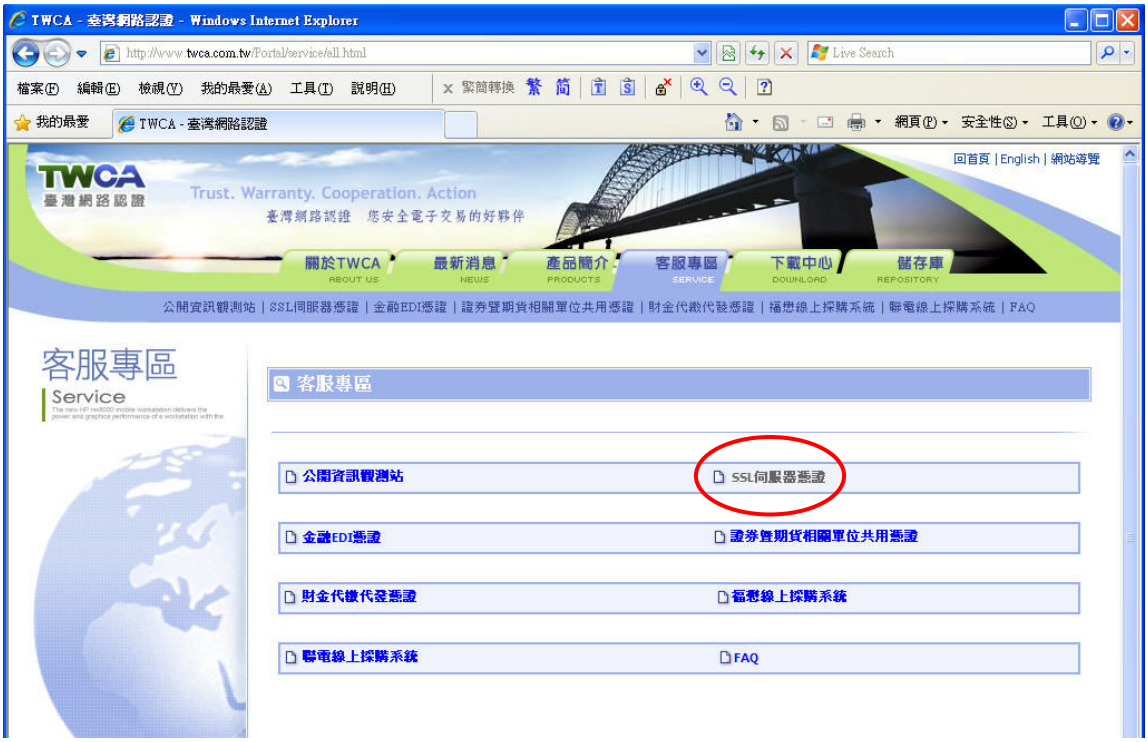
如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

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)

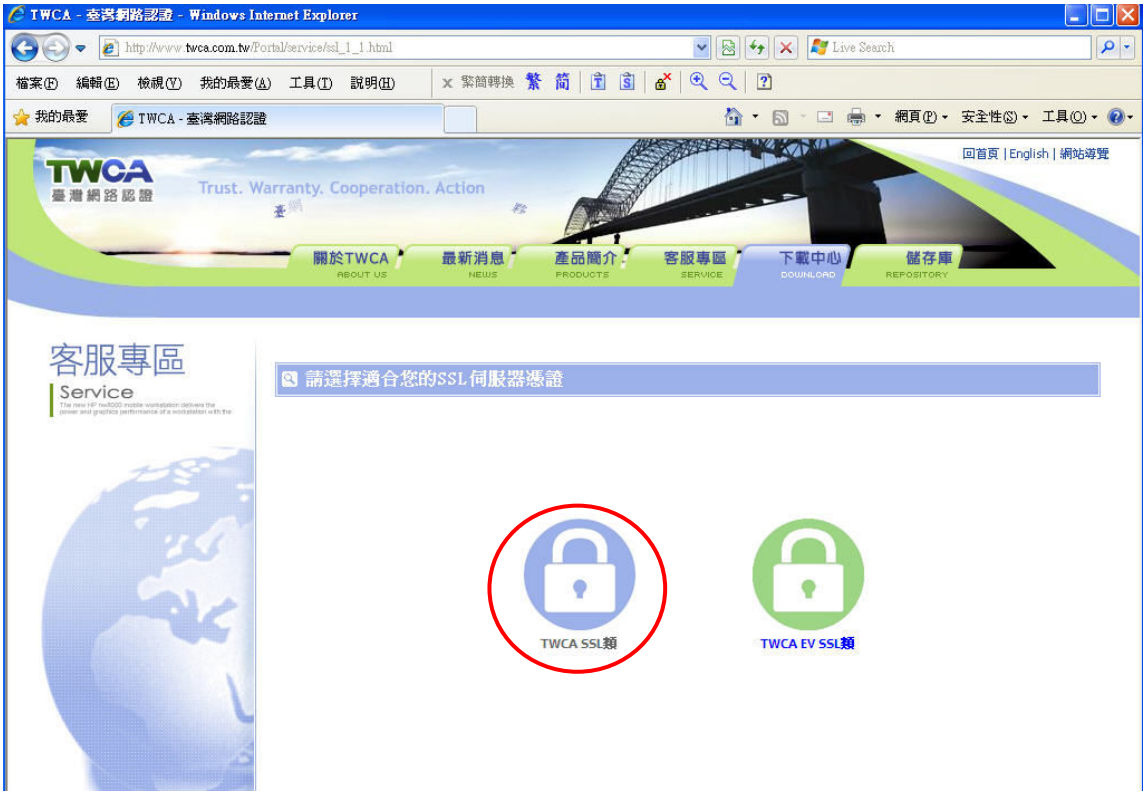
點選 SSL 伺服器憑證。



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 Tomcat 在安裝 SSL 憑證時會使用到四種檔案：

- 於 4.2 章節產製的 SSL 金鑰儲存庫「mykeystore.jks」
- 於 4.5 章節取得的根憑證檔「root.cer」
- 於 4.5 章節取得的中繼憑證檔「uca.cer」
- 於 4.5 章節取得的伺服器憑證檔「server.cer」

先備妥並將其存放至%JDK%\bin 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，請依照 4.6.2 章節步驟安裝憑證。

※ 如 4.5 章節解壓縮後得到四個憑證鏈檔，請依照 4.6.3 章節步驟安裝憑證。

4.6.2 如得到**三個憑證鏈檔**，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。

4.6.2.1 匯入根憑證 root.cer

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias root
-file root.cer -keystore 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
在 <root> 的別名之下，認證已經存在於 CA keystore 整個系統之中
您仍然想要將之新增至自己的 keystore 嗎？ [否]：  y
```

如出現上面訊息，請輸入 y 再按 Enter 即可，

```
認證已新增至 keystore 中
```

出現「認證已新增至 keystore 中」即匯入完成。

4.6.2.2 匯入中繼憑證 uca.cer

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias uca -
file uca.cer -keystore 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
認證已新增至 keystore 中
```

出現「認證已新增至 keystore 中」即匯入完成。

4.6.2.3 匯入伺服器憑證 server.cer

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias keyna
me -file server.cer -keystore 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 4.2.1 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
認證回覆已安裝在 keystore 中
```

出現「認證回覆已安裝在 keystore 中」即匯入完成。

```
keytool 錯誤： java.lang.Exception: 無法從回覆中將鍵建立起來
```

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 keystore 中。

```
keytool 錯誤： java.lang.Exception: 回覆時的公開金鑰與 keystore 不符
```

安裝伺服器憑證出現上列訊息，表示 keystore 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 keystore 跟匯入憑證指定的 keystore 是同一個。

4.6.3 如得到**四個憑證鏈檔**，請將憑證由上至下(根憑證 root.cer、中繼憑證 uca_1.cer、中繼憑證 uca_2.cer、伺服器憑證 server.cer)一一匯入金鑰儲存庫。

4.6.3.1 匯入根憑證 root.cer

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias root
-file root.cer -keystore 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼:
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
在 <root> 的別名之下，認證已經存在於 CA keystore 整個系統之中
您仍然想要將之新增至自己的 keystore 嗎? [否]:  y
```

如出現上面訊息，請輸入 y 再按 Enter 即可，

```
認證已新增至 keystore 中
```

出現「認證已新增至 keystore 中」即匯入完成。

4.6.3.2 匯入中繼憑證 uca_1.cer

keytool -import -trustcacerts -alias uca1 -file uca_1.cer -keystore mykeystore.jks

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias uca1
-file uca_1.cer -keystore 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
認證已新增至 keystore 中
```

出現「認證已新增至 keystore 中」即匯入完成。

4.6.3.3 匯入中繼憑證 uca_2.cer

keytool -import -trustcacerts -alias uca2 -file uca_2.cer -keystore mykeystore.jks

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias uca2
-file uca_2.cer -keystore 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
認證已新增至 keystore 中
```

出現「認證已新增至 keystore 中」即匯入完成。

4.6.3.4 匯入伺服器憑證 server.cer

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

```
C:\Program Files\Java\jdk1.6.0_26\bin>keytool -import -trustcacerts -alias keyna
me -file server.cer -keystore 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 4.2.1 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	keystore 檔案所在路徑及名稱，請依實際位置指定

```
輸入 keystore 密碼：
```

此時會要求輸入 keystore 密碼，請直接輸入 keystore 密碼，

```
認證回覆已安裝在 keystore 中
```

出現「認證回覆已安裝在 keystore 中」即匯入完成。

```
keytool 錯誤： java.lang.Exception: 無法從回覆中將鍵建立起來
```

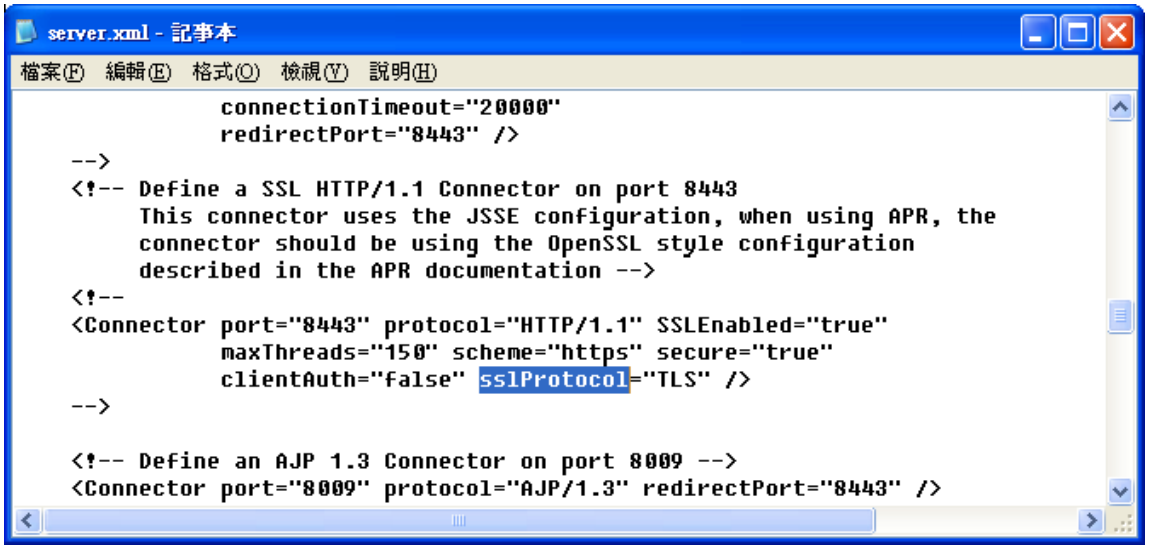
安裝伺服器憑證出現上列訊息，表示根憑證及中繼憑證尚未安裝完成，請先將根憑證及中繼憑證安裝至 keystore 中。

```
keytool 錯誤： java.lang.Exception: 回覆時的公開金鑰與 keystore 不符
```

安裝伺服器憑證出現上列訊息，表示 keystore 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 keystore 跟匯入憑證指定的 keystore 是同一個。

4.6.4 編輯%Tomcat 6.0%\conf 目錄下的 server.xml 檔案，

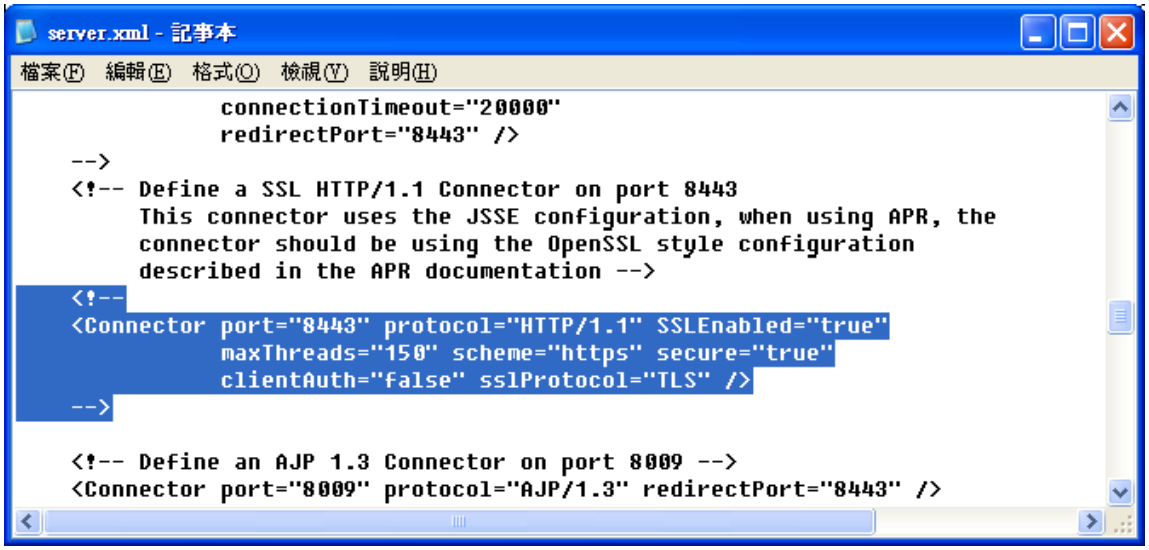
4.6.4.1 搜尋「sslProtocol」字串，可找到其中跟 SSL 相關的指令，

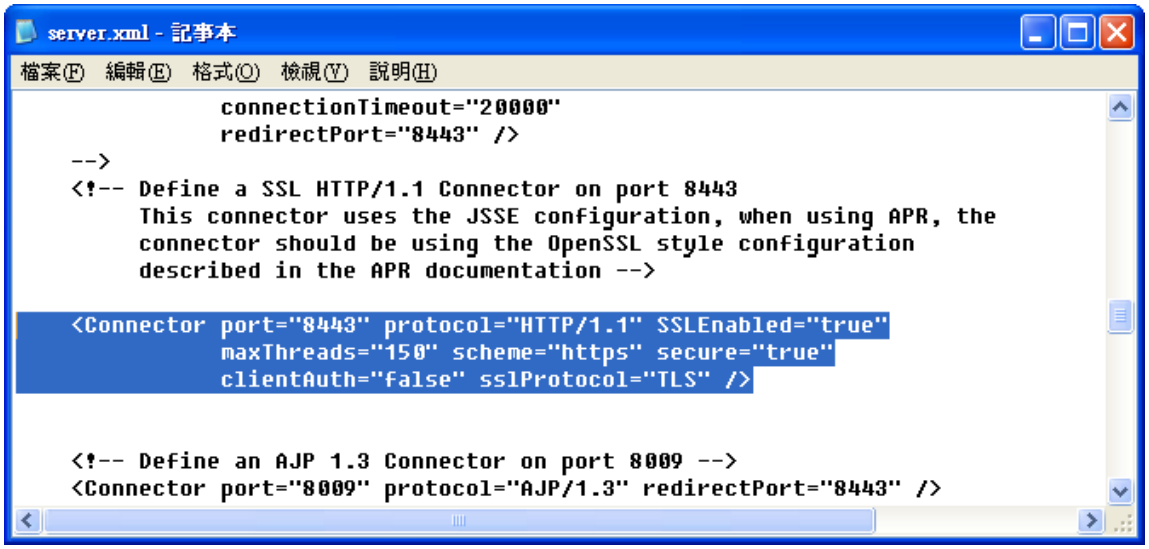


如果是第一次進行 SSL 設定，請將

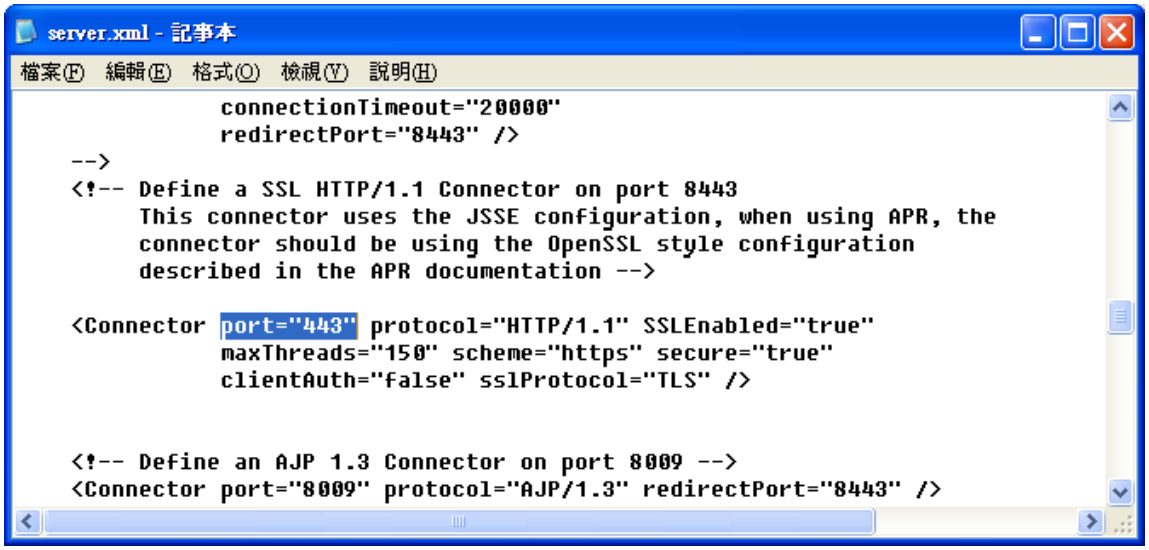
```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS" />
```

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。

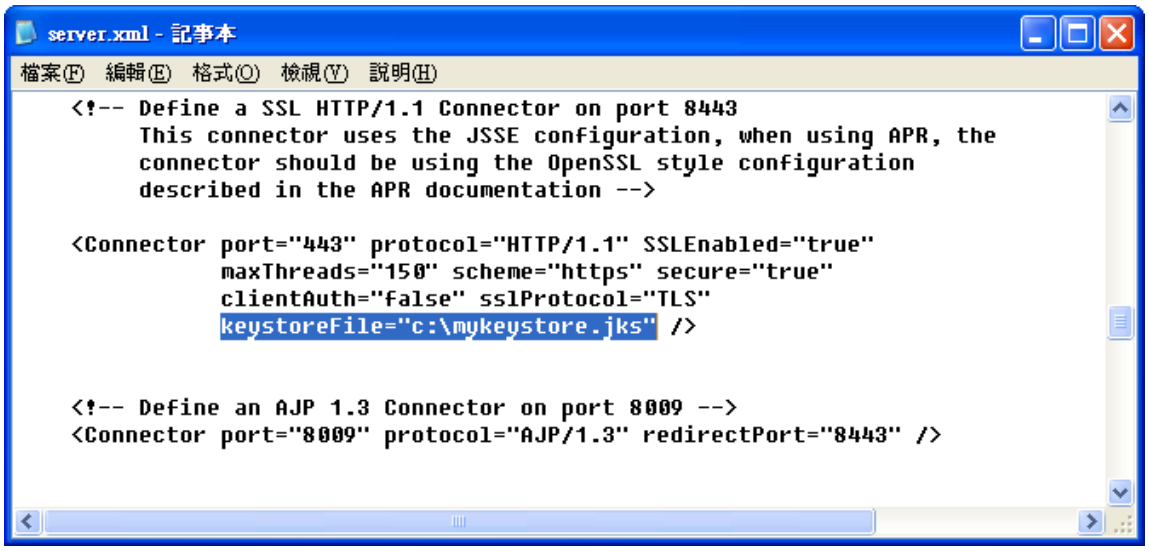




4.6.4.2 將 Port 改為 443，443 Port 是 SSL(https)功能的預設 Port，如果要設定為其他 Port 再修改設定，否則一律設定為 443 即可。



4.6.4.3 新增「keystoreFile」設定，此設定是 keystore 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。

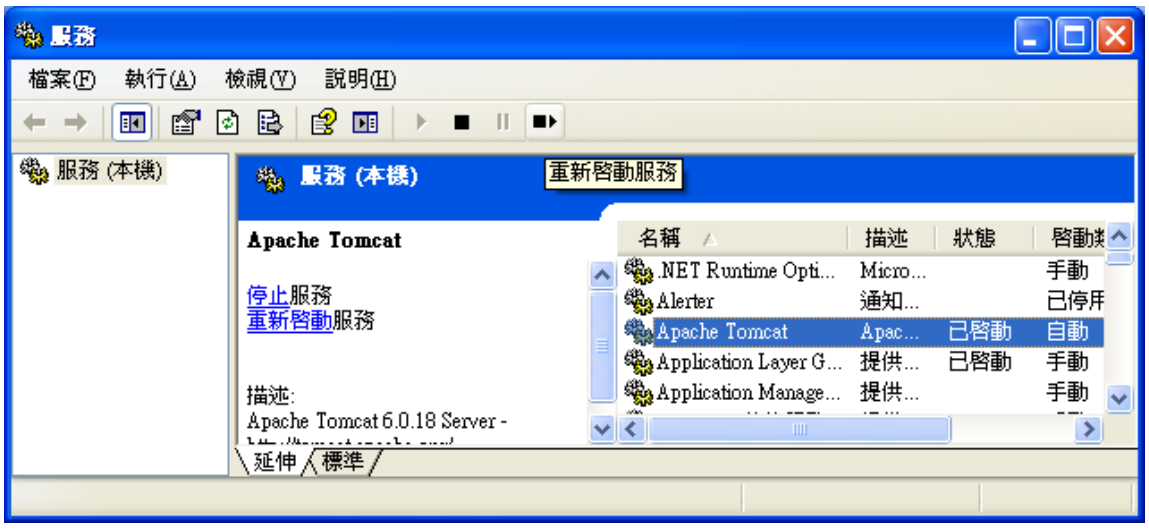


4.6.4.4 新增「keyAlias」設定，此設定是 SSL 伺服器憑證金鑰名稱，請與 4.2.1 章節設定的名稱相同，前後請用「"」包起來。

4.6.4.5 新增「keystorePass」設定，此設定是 keystore 密碼，直接填寫密碼即可，前後請用「"」包起來，

4.6.4.6 重新啟動 Tomcat 服務

重新啟動完成即可進入 4.7 章節，驗證 SSL 功能。



如果完成 4.6 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。

4.7 驗證 SSL 功能

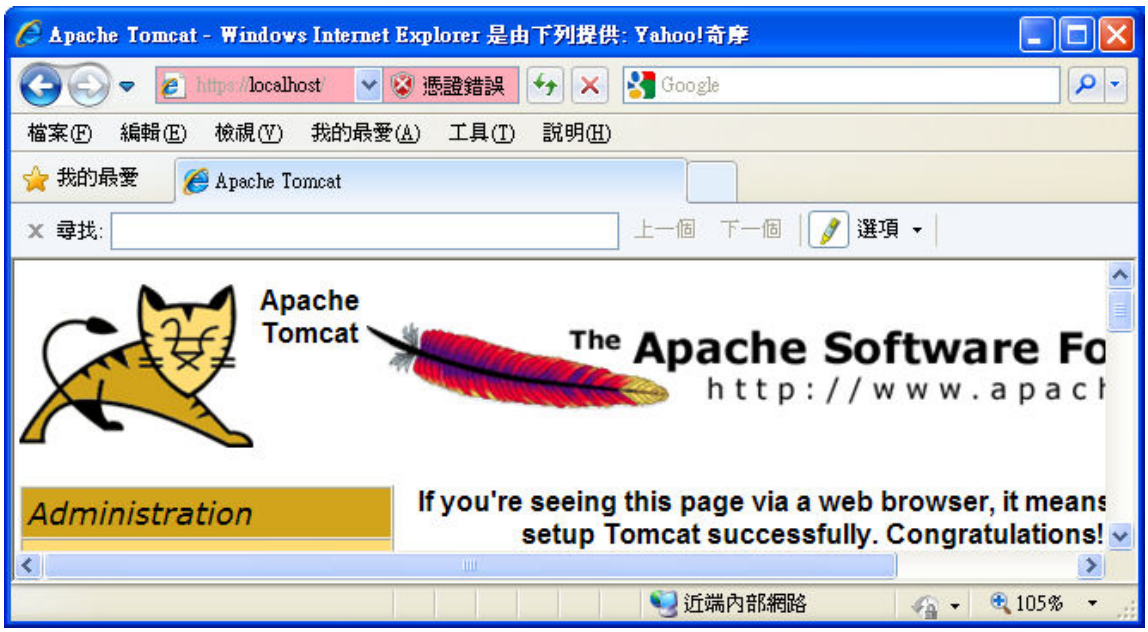
4.7.1 本機驗證

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

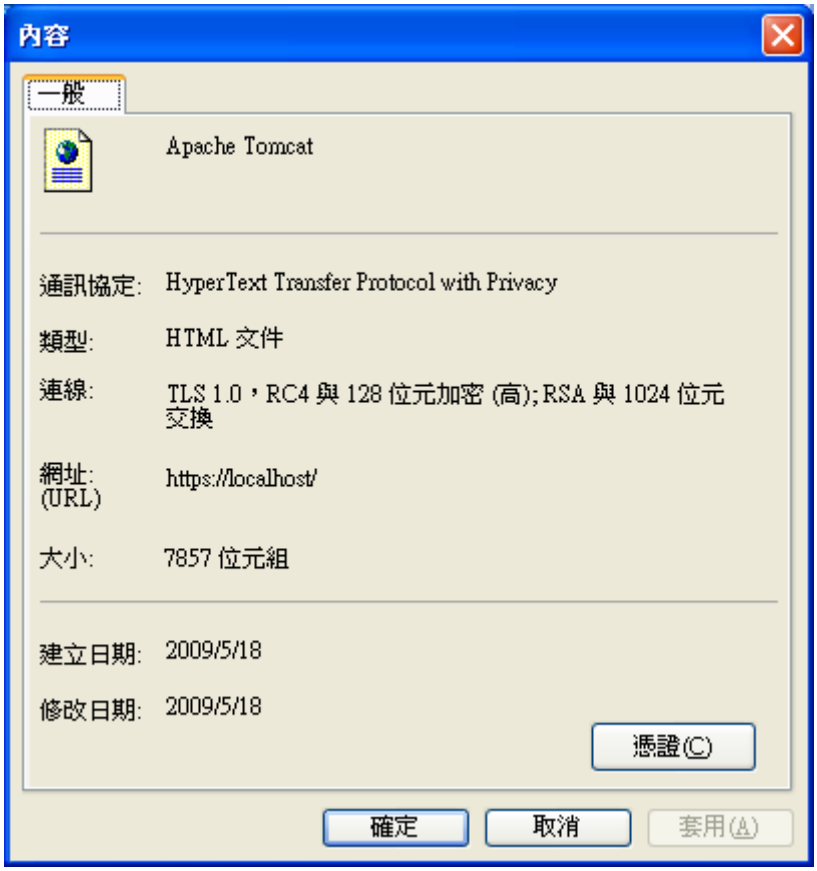
(非 localhost)，請點選「繼續瀏此網站(不建議)」即可。

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

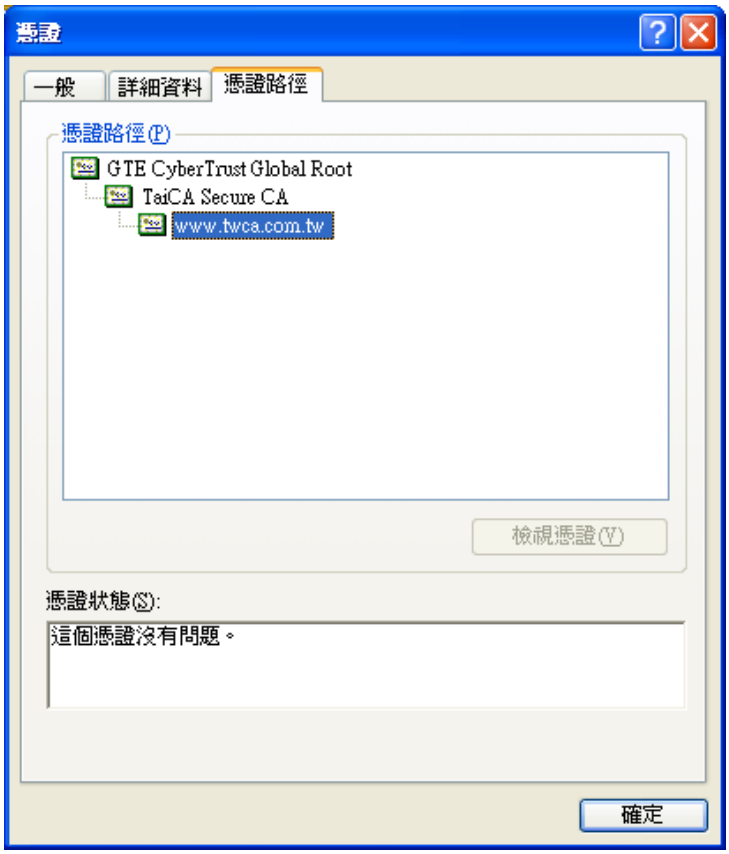


在瀏覽器按滑鼠右鍵出現功能清單，點選「內容」，

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。



4.7.2 外部驗證

驗證程序和 4.7.1 章節相同，只是連線位址改為實際網址，

如 https://www.twca.com.tw

4.7.3 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 4.6.3.2 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

4.8 備份／復原憑證

用戶只需將 4.6.2.3 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「4.6.3 編輯%Tomcat 6.0%\conf 目錄下的 server.xml 檔案」的敘述進行即可。

4.9 更新 SSL 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

4.9.2.1 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(keystore)。

4.9.2.2 更新憑證

請參照 4.2 至 4.6 章節的步驟重新申請安裝憑證，即可完成 SSL 憑證更新。

5.附件

無。