

SSL 伺服器數位憑證 Resin 操作手冊

機密等級：公開
版本：V5.0
文件編號：MNT-03-094
生效日期：109 年 3 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
4.2.1 <i>OpenSSL</i> 模式.....	5
4.2.2 <i>Java keytool</i> 模式.....	6
4.3 產生「憑證請求檔(CSR)」	8
4.3.1 <i>OpenSSL</i> 模式.....	8
4.3.2 <i>Java keytool</i> 模式.....	10
4.4 將製作好的憑證請求檔(CSR)上傳	11
4.5 下載已核發憑證.....	17
4.6 安裝憑證.....	21
4.6.1 <i>OpenSSL</i> 模式.....	21
4.6.2 <i>Java keytool</i> 模式	25
4.7 備份／復原憑證.....	29
4.7.1 <i>OpenSSL</i> 模式.....	29
4.7.2 <i>Java keytool</i> 模式.....	29
4.8 更新憑證.....	30
5.常見問題	31
6.附件	32

1.目的

- 1.1. 介紹 Resin 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 Resin 支援兩種安裝模式

Resin 支援 OpenSSL 與 Java keytool 安裝，本手冊將分別說明兩種模式安裝步驟，請自行選用安裝模式。

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。

4.1.3 安裝 Java JDK/JRE 軟體

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。

4.2 產製「金鑰」

4.2.1 OpenSSL 模式

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



```
server.key - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC6IjbjIC512WY0FyxQ2MDSYd1y+7UcIP13P2J39U+wIn3TmCRb
k01RvMwXpqR1n+/j71108UHj0+W3f4J+w6yGFEmnFS+pg80hGKGR0tV6519MWXS
4XnJ9ekI2j7CWn4YeP02szyp4v+WjM9UKx/iimLG6U8t1785+r07ThPcPwIDAQAB
AoGAGjUvHRQ09rEh3vvUU23vqK/3CpW+t7Y9emkGaHW2PsrchMrLc8mN/2BjFdyt
E5LtqF6tLTY7XM+2TNw7d7X9uMSWHwMaQrE648d/08i146II/qY+4UQcgrkihTM2
GiB5pvLdJAHxQjHv0tY7zPGBtsAHw9wxGDDEj1H5yubX40ECQQDaW8MY4tSa/UyF
LSH6+kFYmKsKEoAJw1FXt9uUhzEXQiUciWuoBDeUvc6o0FK1gS6Ffv692FGNxQaU
U28WXPWpAkEA2jhcPUQA2ZSUzuH7Kvxid/pWTW5Z14QFFASxtCb2AvqxjqQz9F3
Neptvr/IDg0s+tU/kkAzxyAmH+jDJ/2jpwJAVIkJ8ux+GrLTySS6SIvyGHaiYPfg
keakzyzi2ZGtM6/R/vNEtntLeU4yX7CnFJW6iPwtaxqhJZ2NeocCjsnWYQJAJsU0
vf8Nb00yu08Ma2RxWcnKr+r3sgHoc+3WfbqCtFQIFog5SnMw9wdb0FRKuxK0HSze
SqHvKT+JBopYgjZyaQJBAI213YJYGES1j41z4XpAmKF0hVdDqbUHu1k+85U+ebK0
rM816xnXUDW0ES1si0Rn3/uUuctb0hitPpSpqc4sq2==
-----END RSA PRIVATE KEY-----
```

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.

4.2.2 Java keytool 模式

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

```
輸入 keystore 密碼：
重新輸入新密碼：
```

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

```
您的名字與姓氏為何？
[Unknown] : www.twca.com.tw
```

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

```
您的編制單位名稱為何？
[Unknown] : SYSTEM
```

出現您的編制單位名稱為何?請輸入編制單位名稱，例 SYSTEM

```
您的組織名稱為何？
[Unknown] : TWCA
```

出現您的組織名稱為何?請輸入組織名稱，例 TWCA

```
您所在的城市或地區名稱為何？
[Unknown] : TAIPEI
```

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

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.

```
您所在的州及省份名稱為何?  
[Unknown]: TAIWAN
```

出現您所在的州及省份名稱為何?請輸入城市或地區，例 TAIWAN

```
該單位的二字國碼為何  
[Unknown]: TW
```

出現單位的二字國碼為何?請輸入單位二字國碼，例 TW

```
CN=www.twca.com.tw, OU=SYSTEM, O=TWCA, L=TAIPEI, ST=TAIWAN, C=TW 正確嗎?  
[否]: y
```

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，

```
輸入 <keyname> 的主密碼  
(RETURN 如果和 keystore 密碼相同) :
```

此時會要求輸入金鑰密碼，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 OpenSSL 模式

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，

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.

4.3.2 Java keytool 模式

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 4.2.2 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 4.2.2 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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBqTCCARICAQAwTElMAkGA1UEBhMCVFcxZDZANBgNVBAgTB1RBSUdBTjEPMA0GA1UEBxMGVEFJ
UEUJMQ0wCwYDUQKQEWRUU0NBMQ8wDQYDUQLEwZTWUNURU0xGDAWBgNVBAmtD3d3dy50d2NhLmNu
bS50dzCBnzANBGMkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAgrYL1/nNyudd1x5mJhZsBMMSUDIo jTKk
6Z1rdyTd0pG44FFueFAhsoXx+XUuglJBpF7xg0FirYSU1veUtmwvtgiq8PzXbXAmAK3wMJ5epxKJ
JMQ9AW5uBSt+qGhe56HK85NmEP+0sFhCKSnu3yUjzhDtILrNM4nH2oxFIygIatUCAwEAaAAMA0G
CSqGSIb3DQEBBQUAA4GBAEbGy0t5ILoILSxwsG1C0bhUFDJZkRyUrod0c10aSZmA+y/NUhhocr5
luit38TPs1iRwryjW4o5pEuYtFiaoIjsaJyEa8HI+5W5Hed9kqw845aBY7T3jNb2D9CIP2A3nCnU
qUSQekG1EPHL3mBzprHTPdxU5hUgM+ZXq4Jj05Wx
-----END NEW 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.

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**。



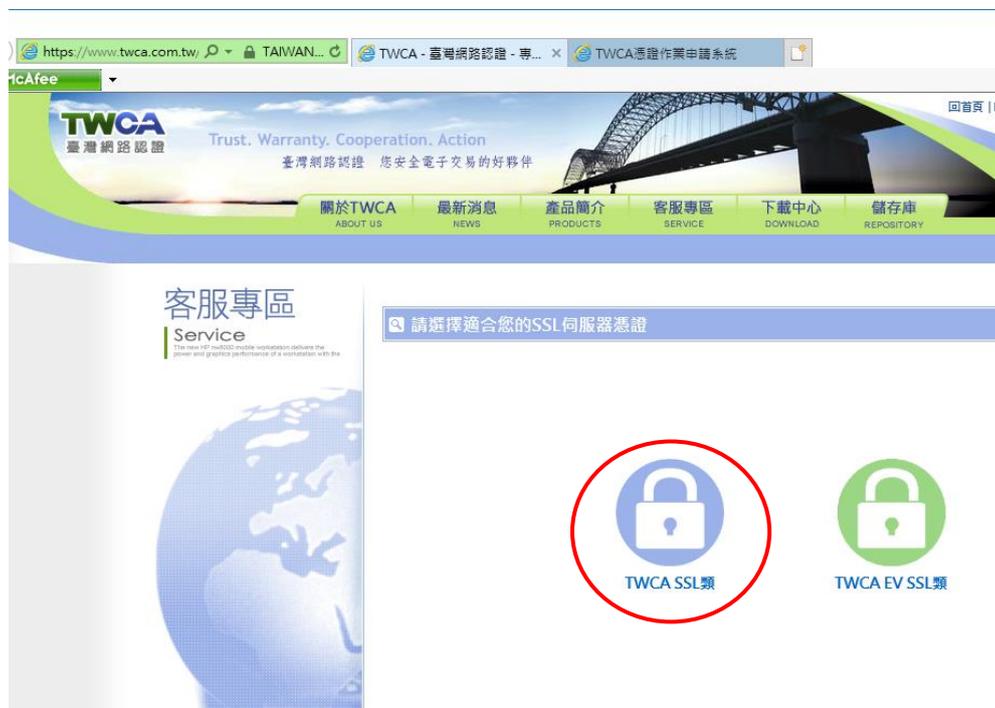
本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

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 **TWCA SSL 類**。

※如申請 EV SSL 伺服器憑證，請點選 **TWCA EV 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.

4.4.3 連接 TWCA 網站(3)

點選 **上傳 CSR (WEB)**。



4.4.4 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**。



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.

4.4.5 再次檢視上傳之憑證請求檔案內容

The screenshot shows the TWCA SSL upload page. The browser address bar is <https://ssl2.twca.com.tw/NCWebSSL/upload.htm>. The page title is "SSL憑證作業". The main content area is titled "檢查CSR內容" (Check CSR Content). It contains a table with the following data:

解說	您的CSR內容
一般名稱: 此名稱所代表的網站之安全性, 將由此SSL伺服器憑證所保護	www.twca.com.tw
組織單位: 這是一個可以用來區分組織部門的欄位	SYSTEM
組織: 即貴公司的名稱	TWCA
城市/位置: 即貴公司進行商業行為的所在[例: Taipei]	TAIPEI
州/省: 即貴公司進行商業行為的州/省所在地, 請不要用縮寫的地名填寫此欄位[例: Taiwan]	TAIWAN
國別: 此欄係以ISO組織的國家代碼來表示, 舉例來說, TW代表台灣, US代表美國	TW
CSR金鑰長度(bits)	2048
適用之安全強度(bits)	128

Below the table, there are sections for "請輸入伺服器資訊" (Enter server information) and "請輸入公司基本資料" (Enter company basic information). The server information section includes a dropdown for "伺服器軟體廠商" (Server software vendor) and a text input for "通行密碼" (Access password). The company information section is partially visible.

4.4.6 設定通行密碼及選擇身分審驗方式

4.4.6.1 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 <input type="password"/>
--------------------------------------	------------------------------------

4.4.6.2 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

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.

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。
	<input checked="" type="radio"/> 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。 <input checked="" type="radio"/> maintain@twca.com.tw (網域註冊資料來源由WHOIS取得) 或請選擇 <input type="radio"/> admin@twca.com.tw <input type="radio"/> administrator@twca.com.tw <input type="radio"/> webmaster@twca.com.tw <input type="radio"/> hostmaster@twca.com.tw <input type="radio"/> postmaster@twca.com.tw
	<input type="radio"/> 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: <input type="text" value="maintain@twca.com.tw"/> ,將郵寄檔案及說明給您。
	<input type="radio"/> 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: <input checked="" type="radio"/> 皆可 <input type="radio"/> 上午時段 <input type="radio"/> 下午時段

4.4.6.3 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	<input type="text"/> 若未填過憑證申請單,請線上登打 憑證表單線上作業輸入
請按一下"繼續"按鈕以送出註冊資料,完成註冊程序。	<input type="button" value="繼續"/>

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.

4.4.7 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。



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。

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.

4.5.1 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**。

※如申請 EV SSL 伺服器憑證，請點選 **TWCA EV 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.

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。



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.

4.5.5 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。

The screenshot shows the TWCA website interface. At the top, there is a navigation bar with links for '關於TWCA', '最新消息', '產品簡介', '客服專區', '下載中心', and '儲存庫'. Below this is a search bar for '查詢用戶憑證'. The search results show a table with 4 records. The 'Download' column for each record has a '憑證鏈' link. A red circle highlights the '憑證鏈' link for the first record. Below the table, a download dialog box is open, showing the file name 'cert.zip (5.28 KB)' and a '另存新檔(A)' button, which is also circled in red.

憑證序號	一般名稱	憑證生效日	憑證到期日	憑證狀態	詳細資訊	下載	註銷	重新申請
1707611566 (65c815ae)	www.twca.com.tw	2010-11-01 14:17:46	2013-11-01 23:59:59	有效	檢視	憑證鏈	註銷	
1707616998 (65c82ae6)	www.twca.com.tw	2011-05-03 18:22:47	2014-05-03 23:59:59	有效	檢視	憑證鏈	註銷	
1707621282 (65c83ba2)	www.twca.com.tw	2011-10-03 16:10:47	2014-10-31 23:59:59	有效	檢視	憑證鏈	註銷	重新申請
85076818910922642191034040465334971642 (4001330612000000000000af23acfa)	www.twca.com.tw	2012-11-06 17:55:12	2014-11-30 23:59:59	有效	檢視	憑證鏈	註銷	重新申請

你要儲存來自 ssl2.twca.com.tw 的 cert.zip (5.28 KB) 嗎?

儲存(S) 另存新檔(A) 儲存並開啟(O)

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 安裝憑證

4.6.1 OpenSSL 模式

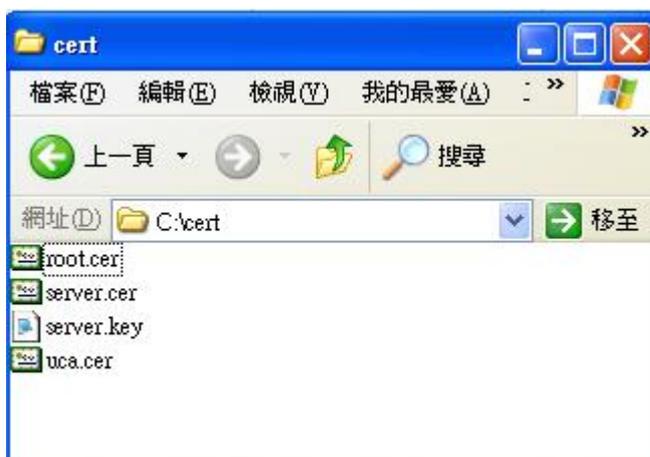
4.6.1.1 Resin 利用 OpenSSL 模式安裝 SSL 憑證時會使用到四種檔案：

- 於 4.2.1 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」
- 於 4.5 章節取得的根憑證檔「root.cer」

先備妥並將所有檔案存放同一個目錄內(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，

存放內容應如下圖所示：



4.6.1.2 產生 Resin 所支援憑證鏈檔

開啟命令提示字元，於 4.6.1.1 章節所說明檔案存放目錄下，輸入
copy 伺服器憑證+中繼憑證+根憑證 CertificateChains.cer
(CertificateChains.cer 為範例，實際產生檔名可自訂)

```
C:\cert>copy server.cer+uca.cer+root.cer CertificateChains.cer
```

或

```
C:\cert>copy server.cer+uca_2.cer+uca_1.cer+root.cer CertificateChains.cer
```

完成上列指令後會在該目錄下產生檔案名稱為 CertificateChains.crt
的檔案，此檔案即為 Resin 所支援憑證鏈檔。

4.6.1.3 驗證 Resin 所支援憑證鏈檔

使用文字編輯器(記事本)打開 CertificateChains.cer 檔
可看到如下內容

```
-----BEGIN RSA PRIVATE KEY-----
```

```
$SOME TEXT
```

```
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
```

```
$SOME TEXT
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
$SOME TEXT
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

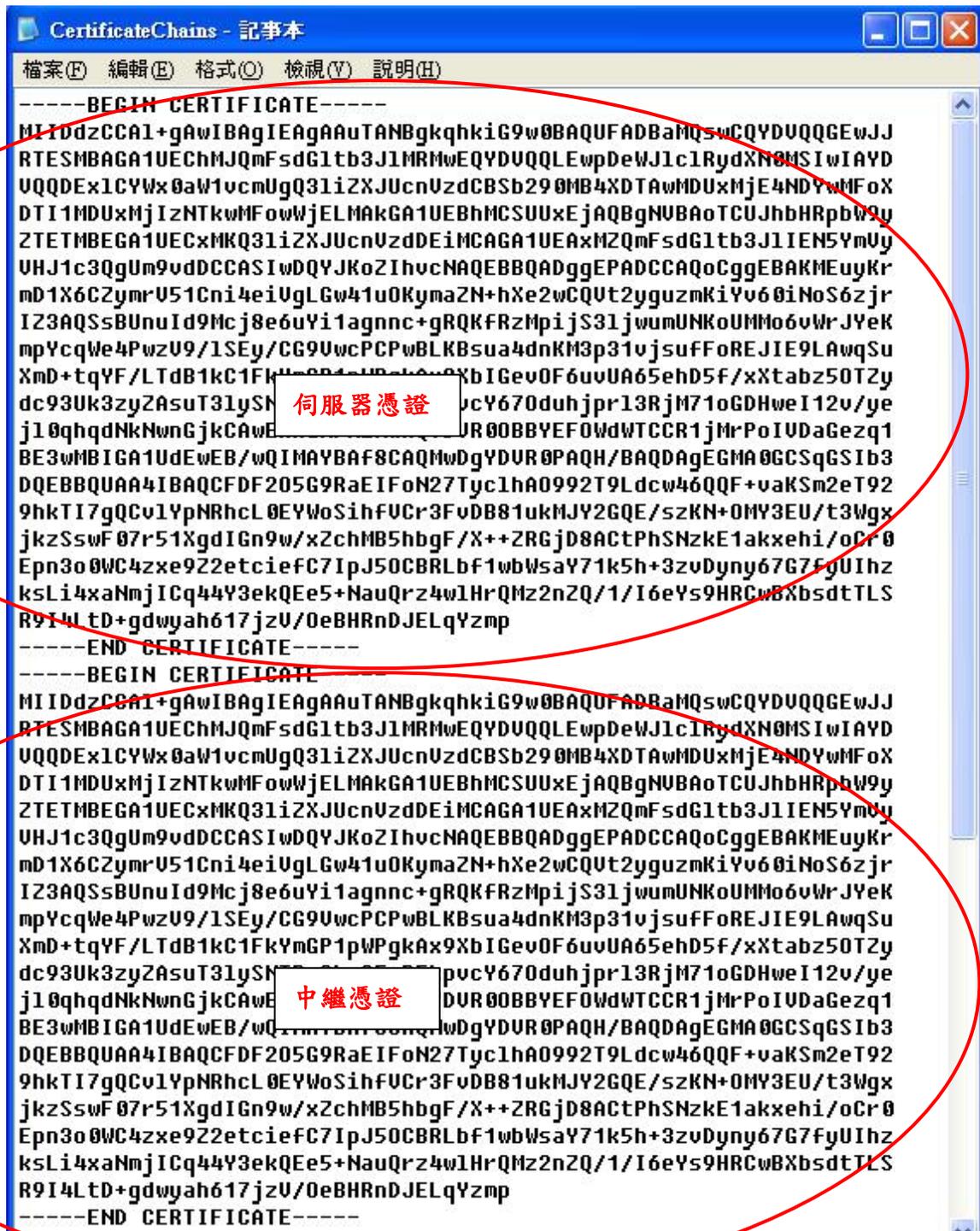
```
$SOME TEXT
```

```
-----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.

```

-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBAMQswCQYD
VUQGEwJJRTESMBAGA1UEChMJQmFsdG1tb3JlMRMwEQYDUQQL
EwpDeWJlc1RydXN0MSIwIAYD
VUQGEwJ1c3QgUm9vdDCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKMEuyKr
mD1X6CZymrV51Cni4eiUgLGw41uOKymaZN+hXe2wCQUt2yguzmKiYv60iNoS6zjr
I23AQSSBUnuId9Mcj8e6uYi1agnnc+gRQKFRzMpijs31jwumUNKoUMMo6vWrJYeK
mpYcqWe4PwzU9/1SEy/CG9UwcPCPwBLKBSua4dnKM3p31vjsuffoREJIE9LAWqSu
XmD+ tqYF/LTdB1kC1FkYmGP1pWPgkAx9XbIGevOF6uvUA65ehD5f/xXtabz50T2y
dc93Uk3zyZAsuT31ySN...ucY670duhjpr13Rjm71oGDHweI12v/ye
j10qhqdNkNwnGjkCAwE 根憑證 UR00BBYEFOWdWTCCR1jMrPoIVDaGezq1
BE3wMBIGA1UdEwEB/wQ...gYDUR0PAQH/BAQDAgEGMA0GCSqGSIb3
DQEBBQUAA4IBAQCDFD205G9RaEIFoN27Tyc1hA0992T9Ldcw46QQF+vaKSm2eT92
9hkTI7gQCv1YpNRhCL0EYWoSihfUCr3FvDB81ukMJY2GQE/szKN+OMY3EU/t3Wgx
jkzSswF07r51XgdIGN9w/xZchMB5hbgF/X++ZRGjD8ACTPhSNzkE1akxehi/0CF0
Epn3o0WC4zxe9Z22etciefC7IpJ50CBRLbf1wbWsaY71k5h+3zvDyny67G7fgUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4w1HrQMz2nZQ/1/I6eYs9HRCw8XbsdtTLS
R9I4LTd+gdwyah617jzV/OeBHRnDJELqYZmp
-----END CERTIFICATE-----

```

4.6.1.3 設定 SSL

Resin4.x 利用 編輯 resin.xml 來設定 SSL

Resin3.x 及 Resin2.x 利用 編輯 resin.conf 來設定 SSL

```
<openssl>
```

```
<certificate-file>伺服器憑證</certificate-file>
```

```
<certificate-key-file>SSL 伺服器金鑰</certificate-key-file>
```

```
<certificate-chain-file> 4.6.1.2 章節合併之憑證鏈檔</certificate-chain-file>
```

```
</openssl>
```

範例如下

```
<openssl>
```

```
<certificate-file>server.cer</certificate-file>
```

```
<certificate-key-file>server.key</certificate-key-file>
```

```
<certificate-chain-file>CertificateChains.cer</certificate-chain-file>
```

```
</openssl>
```

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 Java keytool 模式

4.6.2.1 Resin 利用 Java keytool 模式安裝 SSL 憑證時會使用到四種檔案：

- 於 4.2.2 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)。

4.6.2.2 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。

4.6.2.2.1 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。

4.6.2.2.2 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。

4.6.2.2.3 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 keyname -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。

4.6.2.3 設定 SSL

Resin4.x 利用 編輯 resin.xml 來設定 SSL

Resin3.x 及 Resin2.x 利用 編輯 resin.conf 來設定 SSL

```
<jsse-ssl>
```

```
<key-store-type>jks</key-store-type>
```

```
<key-store-file>4.6.2.2 或 4.6.2.3 章節 keystore(內含根憑證、中繼憑證及伺服器憑證)</key-store-file>
```

```
<password>keystore 密碼</password>
```

```
</jsse-ssl>
```

範例如下

```
<jsse-ssl>
```

```
<key-store-type>jks</key-store-type>
```

```
<key-store-file>mykeystore.jks</key-store-file>
```

```
<password>keystore 密碼</password>
```

```
</jsse-ssl>
```

4.7 備份／復原憑證

4.7.1 OpenSSL 模式

請將 4.2.1 章節產製之 SSL 伺服器金鑰、4.5 章節取得之伺服器憑證 ServerCert.crt 與 4.6.1.2 章節合併之憑證鏈檔備份至安全的位置，復原時再依照 4.6.1.3 章節的敘述設定即可。

4.7.2 Java keytool 模式

請將 4.6.2.2 或 4.2.2.3 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 4.6.2.4 章節的敘述設定即可。

4.8 更新憑證

4.8.1 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。

4.8.2 更新步驟

請參照 4.2 至 4.6 章節步驟申請安裝憑證，即可完成 SSL 憑證更新。

5. 常見問題

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