

# 中華電信通用憑證管理中心(PublicCA)

## Apache SSL 憑證請求檔製作與憑證安裝手冊

聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本手冊所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

本手冊適用於 Apache+mod\_ssl 環境下之 SSL 伺服器軟體憑證安裝，Apache Server 可執行於 Unix like 的平台上(例如:Linux)或是 Windows 平台，請依照您的作業系統選擇適當的手冊參考。本手冊的安裝程序，已經在 Apache 1.3.29 或 Apache 2.4.12 版測試過，您所使用的版本或環境可能與本版本有所差異，若是如此則請參考您的 Web Server 及 SSL 模組相關使用手冊，適度調整 SSL 伺服器軟體憑證安裝步驟。

### 目錄

Linux Apache SSL 憑證請求檔製作手冊 .....	2
Linux Apache SSL 憑證安裝操作手冊 .....	5
Windows Apache SSL 憑證請求檔製作手冊 .....	14
Windows Apache SSL 憑證安裝操作手冊 .....	18
附件一：設定 SSL 安全通道的加密強度.....	26
附件二：停用 SSLv3.0.....	27
附件三：更換 SHA 256 憑證.....	29

# Linux Apache SSL 憑證請求檔製作手冊

## 一、產生憑證請求檔

(1) 產生憑證請求檔 (Certificate Signing Request file, 簡稱 CSR 檔) 需使用 OpenSSL 工具, 此工具通常安裝在 /usr/local/ssl/bin 目錄下(可以使用 `$ find / -name openssl -print` 指令找到您安裝的目錄, 請確定您已經安裝成功再執行下列指令。

(2) 開始前, 請確認您 OpenSSL 的版本沒有受到 Heartbleed Bug 的影響, 您可輸入以下指令來確認您 OpenSSL 的版本。若您的版本有 Heartbleed Bug, 建議先升級到修復版本, 再執行以下操作。

**`$ openssl version`**

影響範圍: 1.0.1 ~ 1.0.1f / 1.0.2-beta ~ 1.0.2-beta1

修復版本: 1.0.1g / 1.0.2-beta2 以後

(3) 產生以 3-DES 加密, PEM 格式的私密金鑰(長度需為 RSA 2048 位元) 執行 openssl 程式如下:

**`$ openssl genrsa -des3 -out server.key 2048`**

- 若您的 SSL 憑證即將到期, 需更新憑證, 建議可以另開一個新的資料夾, 並在此資料夾下執行上述指令, 以避免線上使用的 **server.key 被覆蓋**。

- 依照國際密碼學規範, 請使用 RSA 2048 位元(含)以上金鑰長度。

(4) 執行完畢後會產生私密金鑰檔案, 檔名為 server.key, 請您將此檔案**備份**, 執行過程會要求您輸入密碼(pass phrase)

**Enter PEM pass phase:**

**一定要牢記此密碼**, 日後每次啟動 TLS 通訊模式時, 皆會用到。

```
[root@Franklin bin]# openssl
OpenSSL> exit
[root@Franklin bin]# openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[root@Franklin bin]# _
```

(5) 產生憑證請求檔

**`$ openssl req -new -key server.key -out certreq.txt`**

執行過程會要求輸入密碼, 完畢後會產生憑證請求檔, 檔名為 certreq.txt 請輸入憑證主體資訊到憑證請求檔中, 不過 PublicCA 網站 SSL 憑證申請頁面只會擷取憑證請求檔的公開金鑰數值, 並不會使用以下憑證主體資訊, 而是以您在 PublicCA 網頁投單所登打之組織與網站名稱資訊為準

進行身分審驗。

Country Name : TW

State or Province Name :

Locality Name : 城市(如 : Taipei)

Organization Name : 組織名稱(如 : CHT)

Organizational Unit Name : 單位名稱(如:Information)

Common name : 網站名稱(如 : www.abc.com.tw)

Email address : 伺服器管理者電子郵件 (如:abc@abc.com.tw)

challenge password : 不需輸入，按 enter 鍵略過

optional company name : 不需輸入，按 enter 鍵略過

```
root@Franklin bin]# openssl req -new -key server.key -out certreq.txt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:TW
State or Province Name (full name) [Berkshire]:Taiwan
Locality Name (eg, city) [Newbury]:Taipei
Organization Name (eg, company) [My Company Ltd]:CHT
Organizational Unit Name (eg, section) []:Information
Common Name (eg, your name or your server's hostname) []:www.abc.com.tw
```

```
Email Address []:test@test.com.tw
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

(6) 檢視憑證請求檔

您可使用下面指令檢視您所產生的憑證請求檔

***\$openssl req -noout -text -in certreq.txt***

請求檔內容範例如下：

```

Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
 00:b0:63:9d:fe:90:27:09:b5:99:b8:53:c3:7c:5d:
 78:66:27:2a:f5:44:b9:45:68:b2:4e:2c:77:fb:a2:
 d1:26:25:7a:ef:9f:4e:18:9c:a9:20:97:f0:69:ff:
 49:4d:86:0e:70:5d:6b:09:18:00:27:ac:38:13:1d:
 d3:f9:18:0f:25:c5:a5:6d:08:50:2f:0d:ff:89:cb:
 fd:ca:b8:ab:bc:b0:5f:1d:e0:8e:03:41:2b:4d:9e:
 41:1a:a5:7a:60:03:94:94:44:dd:41:3a:c9:f4:a3:
 95:cd:5d:11:c5:9f:8a:bc:0f:90:1d:14:d6:3d:5c:
 25:5e:99:c0:7a:2b:31:b1:df:b3:fc:e0:46:12:0b:
 10:6f:95:cc:98:d7:a0:38:ea:db:33:9c:17:cd:64:
 8a:ca:1b:47:16:8a:b8:a5:0c:4d:f8:02:2e:3a:40:
 9d:13:cf:26:bc:c7:63:76:10:b4:d0:17:57:74:2e:
 72:f6:c0:1b:24:e3:f1:2e:df:c0:e7:f7:b9:33:69:
 ae:5d:e7:43:ef:36:0f:0b:0d:14:68:d7:ee:6f:6c:
 7d:c0:33:14:79:af:14:9e:5d:54:6c:42:83:6d:96:
 dd:72:06:8d:3b:69:c7:59:d7:35:80:f7:33:41:15:
 df:6b:b1:72:e3:74:53:9f:62:73:ab:50:ec:4d:06:
 eb:ef
Exponent: 65537 (0x10001)
Attributes:
  a0:00
Signature Algorithm: sha1WithRSAEncryption
 4f:f3:18:8d:bd:e7:86:88:2c:bf:07:d8:70:5e:bb:c9:28:3c:
 75:64:f6:17:77:75:f8:92:65:bd:07:ba:1a:ba:30:be:8c:d0:
 93:64:52:b9:64:34:c0:fa:13:32:46:fc:8d:2f:7b:05:69:0b:
 26:c4:0c:50:e6:18:93:e8:cb:fe:10:df:43:a3:34:37:7d:69:
 e5:36:cd:92:ce:9f:89:e0:c5:85:8a:d3:24:79:2a:73:c4:9d:
 d0:9d:cc:6c:71:0f:95:8f:df:d7:3b:bc:3f:f5:31:33:10:ac:
 35:da:55:7e:8b:4f:a7:f3:15:da:38:2c:39:35:15:3b:07:9f:
 f6:da:27:ed:79:d1:d3:f8:21:e9:ac:b1:6d:f6:bb:d3:cc:ed:
 21:25:67:ad:a8:54:3c:eb:f0:98:e4:b7:5b:e3:31:25:3b:ee:
 60:dc:1a:f6:c6:57:06:85:4f:cd:ef:af:67:fe:f6:fa:81:d6:
 1e:ee:97:da:f4:04:cf:f1:f4:19:8e:89:e6:e6:09:4c:e8:0e:
 e9:c5:65:8a:7c:69:f8:f3:ad:dd:90:e8:26:9f:ca:2b:21:c1:
 28:7f:5d:dc:59:a2:64:f4:7c:a7:4d:92:4d:a3:5b:08:7c:19:
 f1:aa:fe:2c:57:02:3a:71:83:ae:38:d0:7a:30:a0:33:ad:75:
 7c:39:a3:5f

```

- 二、 將憑證請求檔存到儲存媒體，完成製作憑證請求檔動作。
- 三、 請將產生的憑證請求檔(certreq.txt)複製，請至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

# Linux Apache SSL 憑證安裝操作手冊

## 一、取得 eCA 自簽憑證及 Public CA 憑證之憑證串鏈

當您向 Public CA 申請的 SSL 伺服器軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服器軟體憑證，而必須先取得 eCA 自簽憑證及 PublicCA CA 憑證之憑證串鏈，並在 Apache Server 上安裝 eCA 自簽憑證及 PublicCA CA 憑證之憑證串鏈，使您的 Apache Server 信賴 eCA 及 Public CA 的 CA 憑證，這樣您接下來安裝的 SSL 伺服器軟體憑證才會正常運作。如果您以前曾經在同一部 Apache Server 上成功安裝過 eCA 自簽憑證及 Public CA CA 憑證之憑證串鏈，則您可以跳過此步驟，直接進行 SSL 伺服器應用軟體憑證的安裝。

下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採取以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA\_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2\_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈三個檔案。

2. 從網站查詢與下載：

eCA 憑證：

[http://epki.com.tw/download/ROOTeCA\\_64.crt](http://epki.com.tw/download/ROOTeCA_64.crt)

PublicCA G2 憑證：

[http://epki.com.tw/download/PublicCA2\\_64.crt](http://epki.com.tw/download/PublicCA2_64.crt)

SSL 憑證下載：您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，進行 SSL 憑證下載。

若您是中華電信之員工，負責管理單位之伺服器，請至

<http://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證(請選擇 Based 64 格式)。

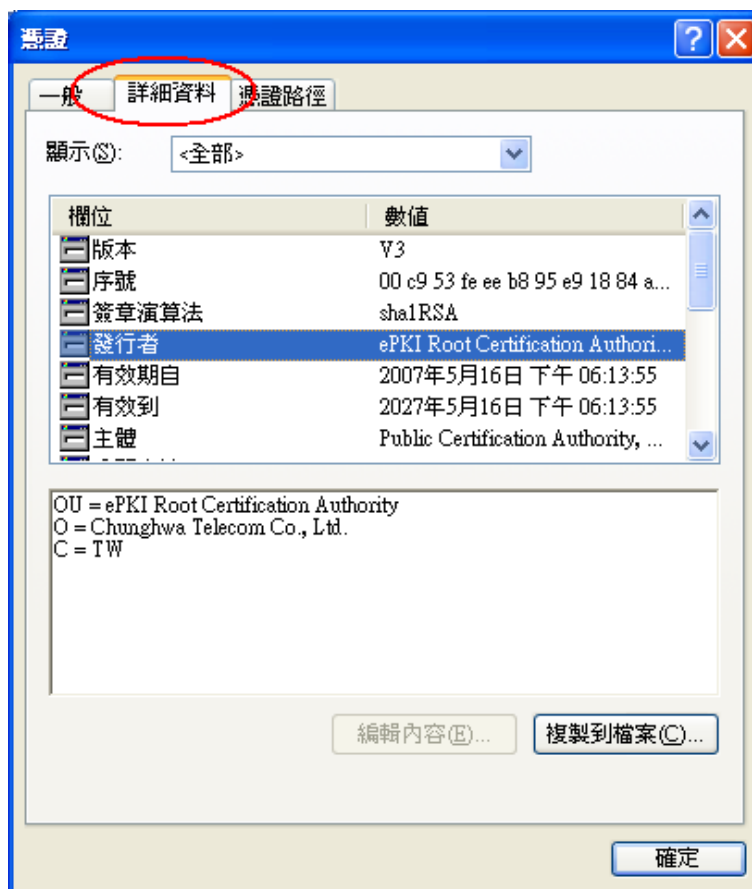
(註：使用 IE 下載.crt 格式的憑證時，IE 會將副檔名.crt 改為.cer，但編碼格式還是屬於 Base64)

3. 以下步驟，以 SHA-1 憑證為安裝範例。

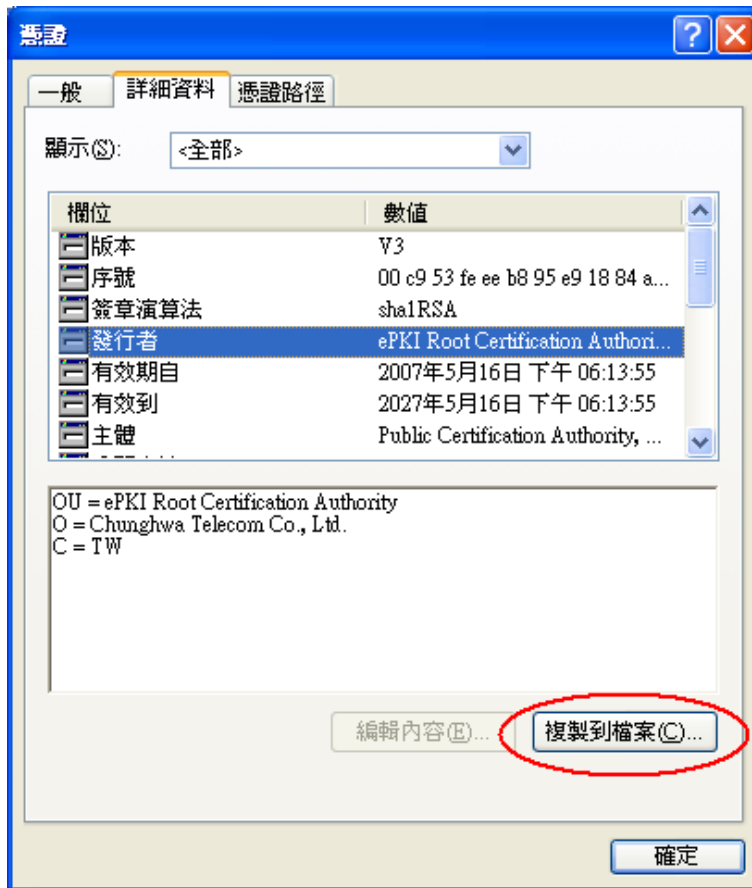
打開儲存的 PublicCA\_64.crt(PublicCA\_64.cer)。



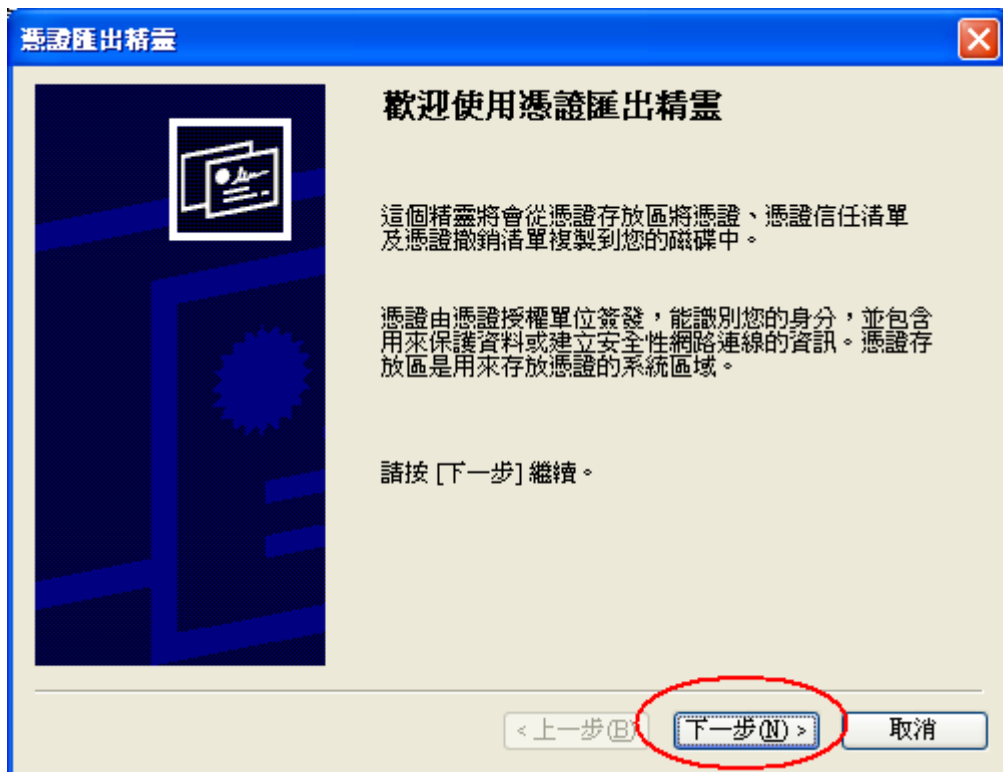
4. 出現以下憑證檢視的畫面，請點選「詳細資料」。



5. 出現以下憑證詳細資料的畫面，請點選「複製到檔案」。

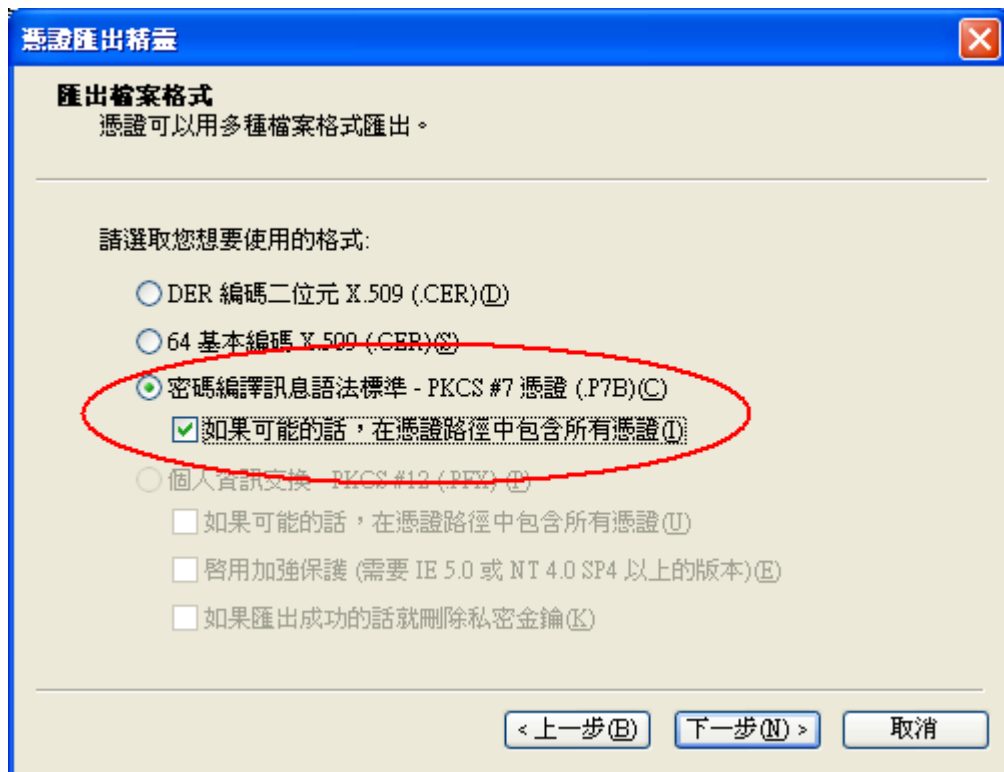


6. 出現以下憑證匯出精靈的畫面，請點選「下一步」。

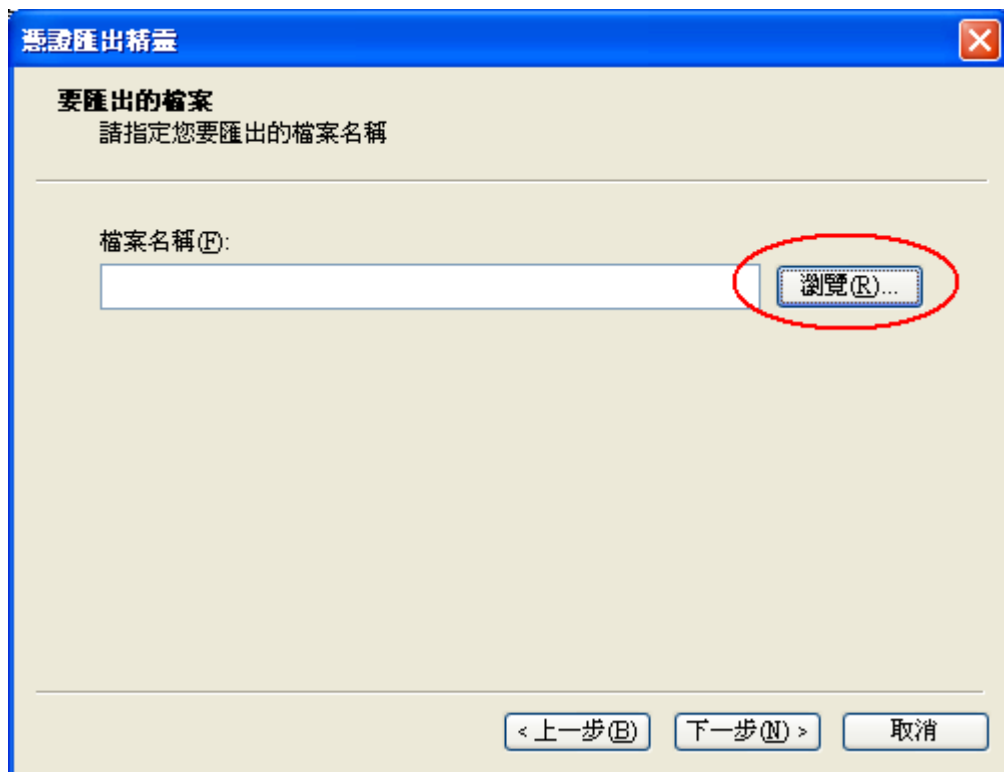


7. 請勾選「密碼編譯訊息語法標準-PKCS#7 憑證」及「如果可能的話，在

憑證路徑中包含所有憑證」兩個選項，然後點選「下一步」。  
(註：勾選「如果可能的話，在憑證路徑中包含所有憑證」，會將 PublicCA 中繼憑證與 eCA 根憑證一起匯出)

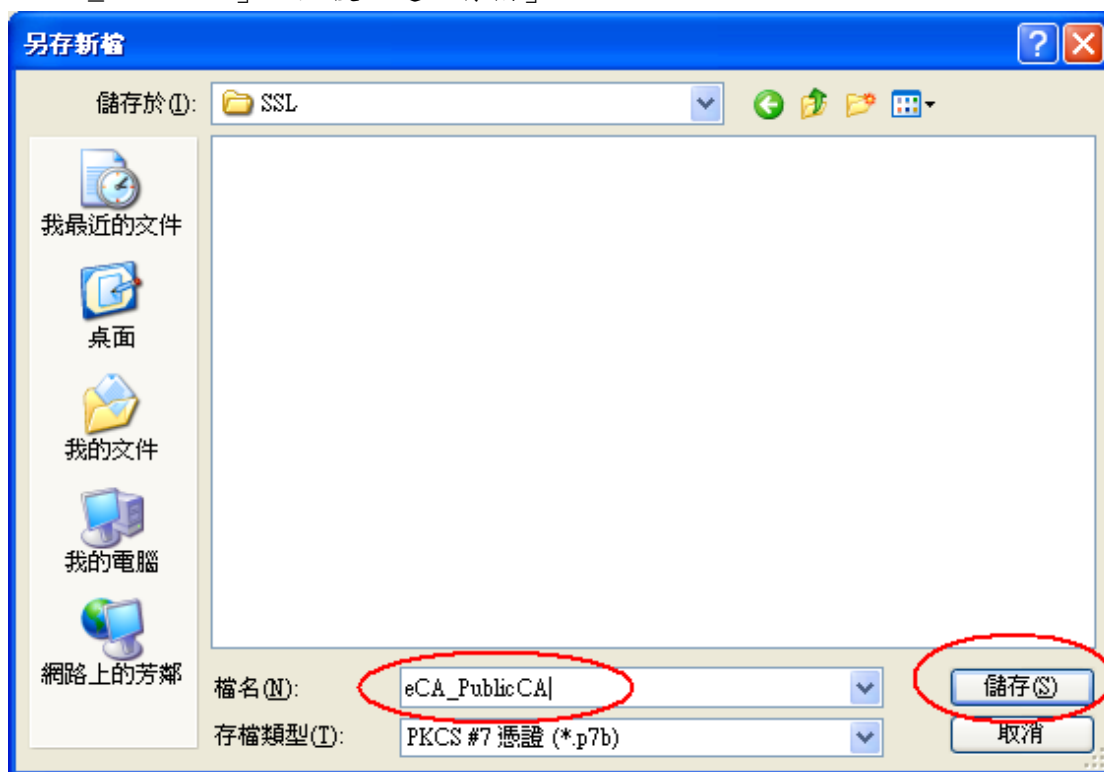


8. 點選「瀏覽」。

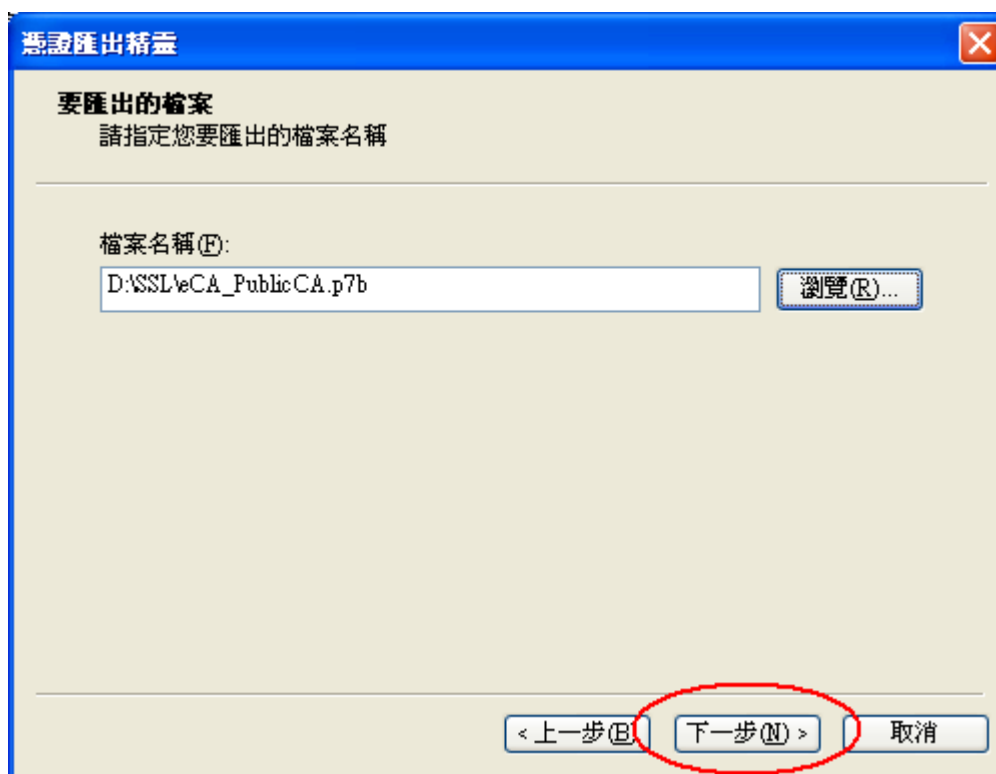




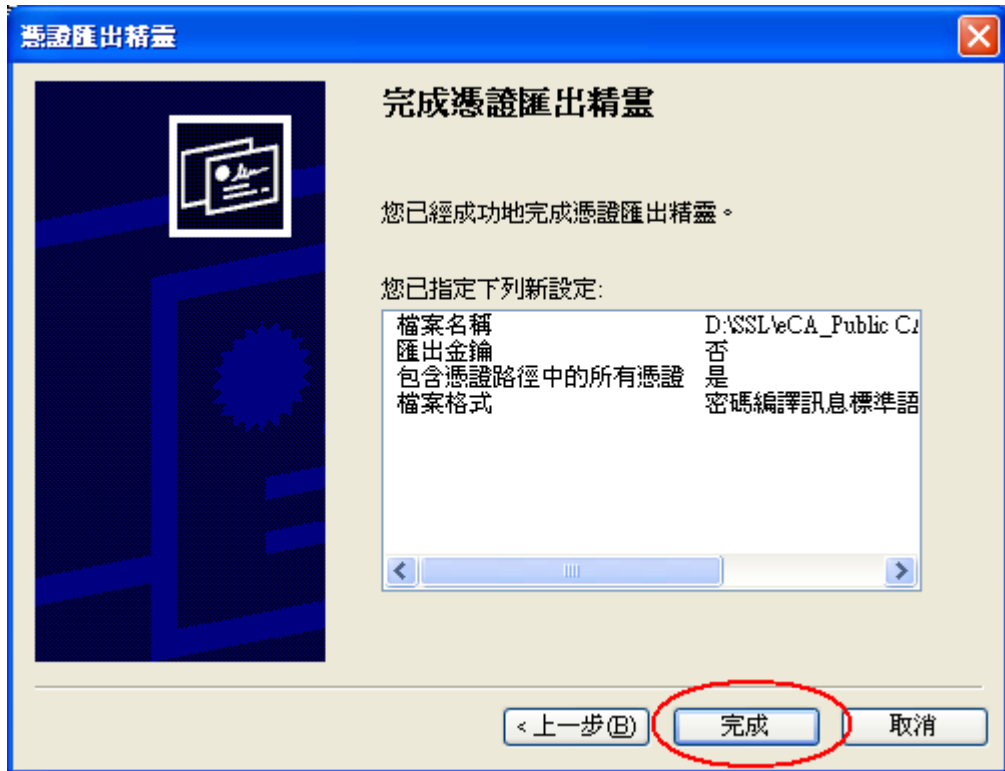
9. 出現另存新檔的畫面，請選擇適當的資料夾位置，檔案名稱請輸入「eCA\_PublicCA」，然後點選「存檔」。



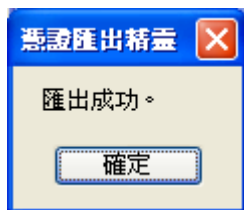
10. 出現以下憑證匯出精靈的畫面，請點選「下一步」。



11. 出現以下憑證匯出精靈的畫面，請點選「完成」。



12. 出現以下憑證匯出精靈的畫面，請點選「確定」，即完成了 eCA 根憑證及 PublicCA CA 憑證之憑證串鏈的取得。



## 二、 安裝 eCA 根憑證及 PublicCA 憑證之憑證串鏈

接下來要在 Apache Server 上安裝 eCA 根憑證及 Public CA CA 憑證之憑證串鏈，使您的 Apache Server 信賴 eCA 及 Public CA 的 CA 憑證。步驟如下：

13. 登入 Apache Server 機器（註：您登入的帳號必須具有 root 或 apache 管理員的權限）
14. 把您在上一階段取得的 eCA 根憑證及 Public CA 憑證之憑證串鏈 eCA\_PublicCA.p7b，複製一份或傳送一份（注意：如果使用 FTP 必須使用 Binary 模式來傳送）到您的 Apache Server 的機器中。
15. 執行以下命令將憑證串鏈檔案由 DER 編碼格式轉換成 PEM 編碼格式，即 Base64 編碼格式：
 

```
openssl pkcs7 -in eCA_PublicCA.p7b -inform DER -print_certs -out eCA_PublicCA.pem
```
16. 執行以下命令將 PEM 編碼格式的憑證串鏈檔案複製為 Apache+mod\_ssl 的 SSLCertificateChainFile：

`cp eCA_PublicCA.pem /usr/local/apache/conf/ssl.crt/ca.crt` (註 1：以上命令假設您的 `ssl.conf` 或 `httpd.conf` 中的 `SSLCertificateChainFile` Directive 是指向 `/usr/local/apache/etc/ssl.crt/ca.crt`，您可以依照自己的環境不同選擇使用不同的檔案位置。註 2：以上命令將會覆蓋原來存在 `SSLCertificateChainFile` Directive 所指向的檔案，您可能會想要先將舊檔案備份起來，以防萬一。)

17. 以文字編輯器編輯 `/usr/local/apache/conf/ssl.conf` 檔 (`mod_ssl` 的組態設定檔)，在組態設定檔中找到 `SSLCertificateChainFile` Directive，並修成以下內容：  
`SSLCertificateChainFile /usr/local/apache/conf/ssl.crt/ca.crt` (註 1：在有些 `Apache+mod_ssl` 環境中，`mod_ssl` 並沒有獨立的態設定檔，在這種情形之下，`SSLCertificateChainFile` Directive 將會直接寫在 `Apache` 的 `httpd.conf` 組態設定檔中。如果是這樣的話，則您必須編輯 `httpd.conf` 而不是 `ssl.conf`。註 2：如果原來的 `SSLCertificateChainFile` Directive 之前有 `#` 註解符號，請記得 `#` 註解符號刪除，否則 Directive 並不會生效。)
18. 記得儲存編輯後的組態設定檔。

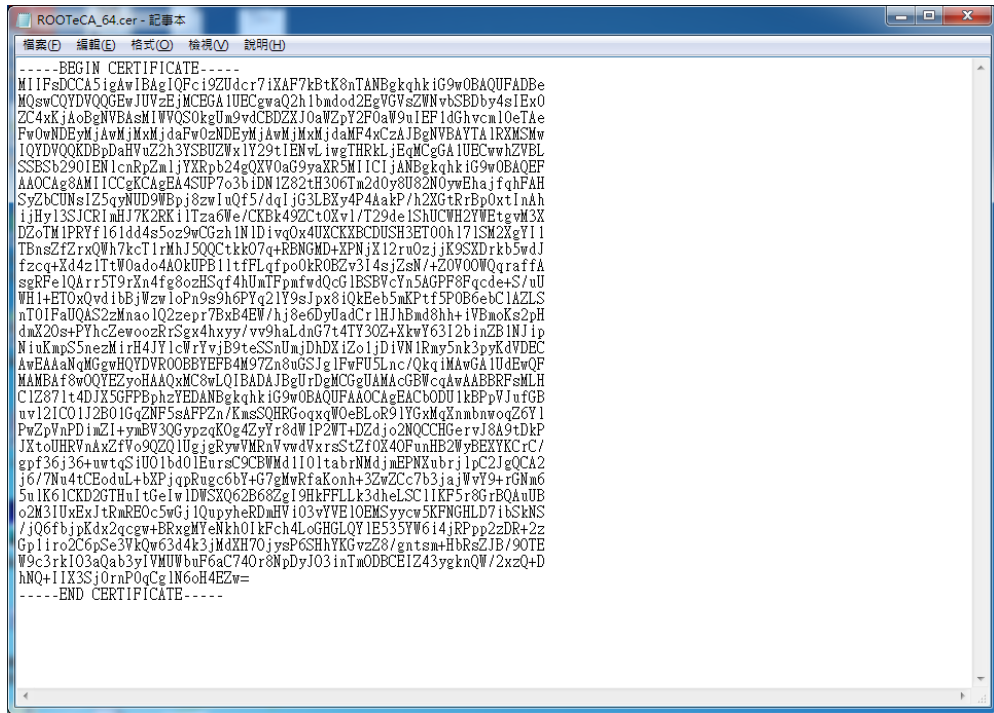
### 三、安裝 SSL 伺服器軟體憑證

接下來要把 `PublicCA` 簽發給您的 `SSL` 伺服器軟體憑證安裝到您的 `Apache Server` 上，其步驟如下：

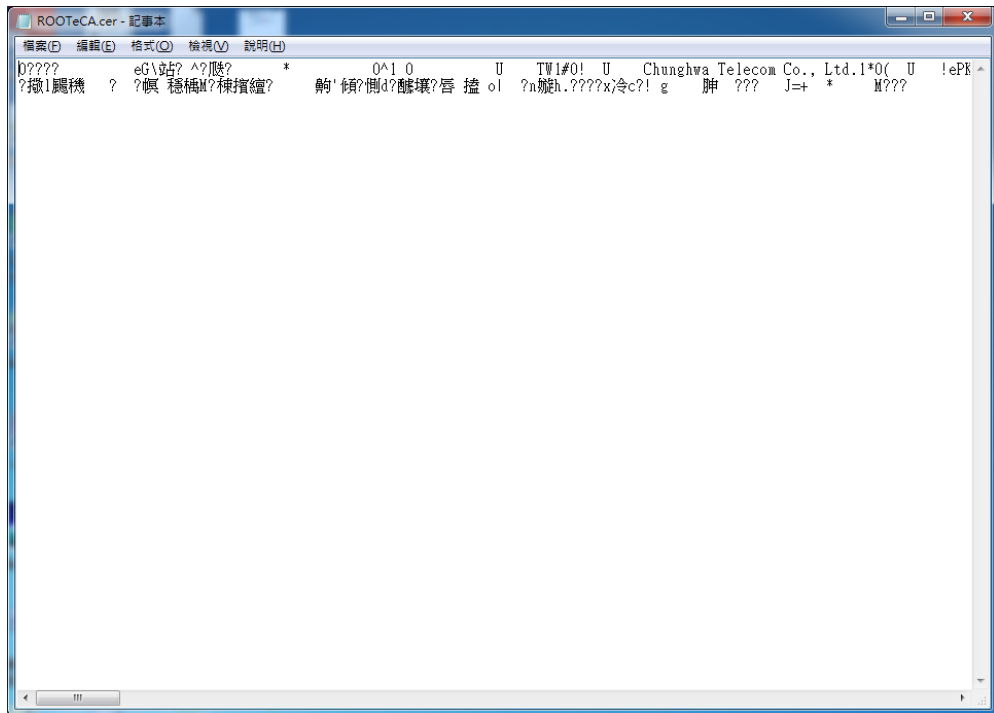
18. 請確定已下載儲存已簽發之 `SSL` 伺服器軟體憑證(檔名為 32 個英數字所組成的 `cer` 或是 `crt` 檔案)。  
(註：以下步驟假設您下載之 `SSL` 伺服器軟體憑證的檔名已經改名為 `server.cer`，如果您並非使用這個檔名，請自行調整下面的步驟。)
19. 登入到 `Apache Server` 機器。  
(註：您登入的帳號必須具有 `root` 或 `apache` 管理員的權限)
20. 目前已簽發之 `SSL` 伺服器軟體憑證皆為 `PEM` 編碼格式(即 `Base64` 編碼格式)，若您的 `SSL` 伺服器軟體憑證為 `DER` 編碼格式，請執行以下命令將 `SSL` 伺服器軟體憑證由 `DER` 編碼格式轉換成 `PEM` 編碼格式  
`openssl x509 -in server.cer -inform DER -out server.pem`

**如何確認憑證編碼格式：**請利用文字編輯器將憑證檔案開啟，根據出現的畫面來判別憑證編碼格式。

`PEM` 編碼格式：



DER 編碼格式：



21. 執行以下命令將 PEM 編碼格式的憑證串鏈檔案複製為 Apache+mod\_ssl 的 SSLCertificateFile：
 

```
cp server.pem /usr/local/apache/conf/ssl.crt/server.crt
```

 (註：以上命令假設您的 ssl.conf 或 httpd.conf 中的 SSLCertificateFile Directive 是指向 /usr/local/apache/conf/ssl.crt/server.crt，您可以依照自己的環境不同選擇使用不同的檔案位置。)

22. 以文字編輯器編輯/usr/local/apache/conf/ssl.conf 檔 (mod\_ssl 的組態設定檔)，在組態設定檔找到 SSLCertificateFile Directive，並修正以下內容：

```
SSLCertificateFile /usr/local/apache/conf/ssl.crt/ca.crt
```

(註 1：在有些 Apache+mod\_ssl 環境中，mod\_ssl 並沒有獨立的態設定檔，在這種情形之下，SSLCertificateFile Directive 及 SSLCertificateKeyFile Directive 將會直接寫在 Apache 的 httpd.conf 組態設定檔中。如果是這樣的話，則您必須編輯 httpd.conf 而不是 ssl.conf。

註 2：以上步驟假設您的 SSLCertificateKeyFile 是 /usr/local/apache/conf/ssl.key/server.key 這個檔案，如果您的 SSL Server 金鑰並不是存放在這個位置，請在 SSLCertificateKeyFile Directive 中指定正確的位置。請注意這個 SSL Server 金鑰必須是當初您用來產生憑證請求檔(CSR 檔)的同一個金鑰，否則將無法成功建立 SSL 連線。)

23. 記得儲存編輯後的組態設定檔。
24. 使用以下兩個命令，重新啟動 Apache Server：

```
/usr/local/apache/bin/apachectl stop
```

```
/usr/local/apache/bin/apachectl start
```

25. 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。
26. 安裝 SSL 安全認證標章：

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，內有 SSL 安全認證標章安裝說明，請參考將網站 SSL 安全認證標章安裝成功。

## Windows Apache SSL 憑證請求檔製作手冊

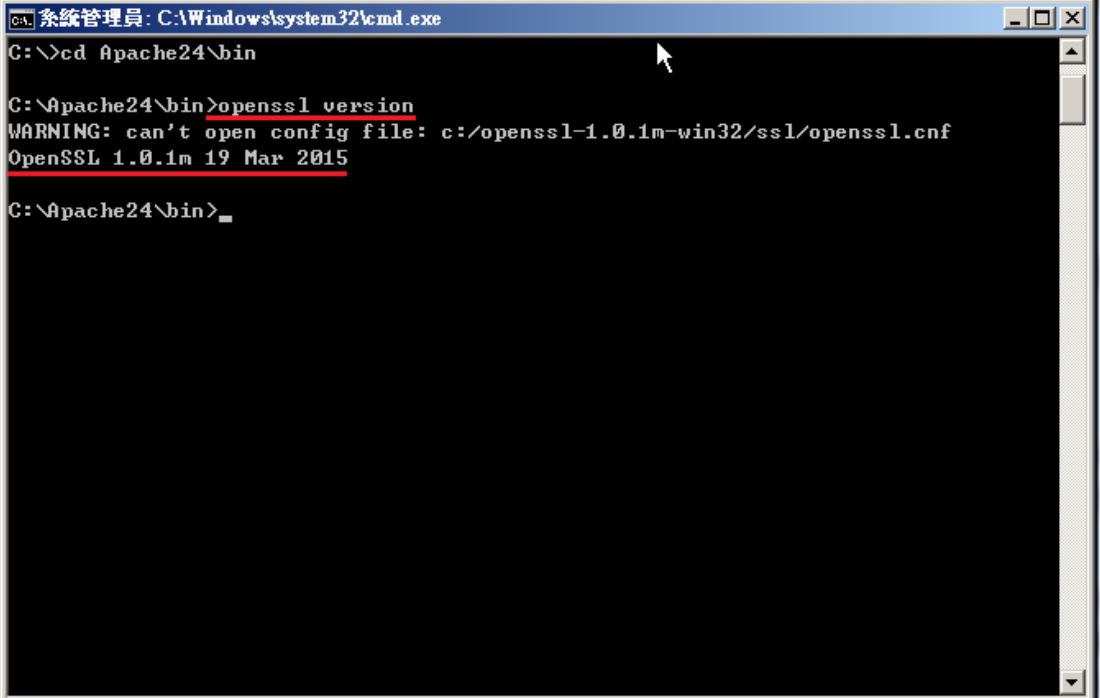
### 一、產生憑證請求檔

- (1) 產生憑證請求檔 (Certificate Signing Request file, 簡稱 CSR 檔)  
需使用 OpenSSL 工具，此工具通常安裝在 <apache 安裝目錄>/bin 目錄下，會包含一個 openssl.exe 檔案。
- (2) 開始前，請確認您 OpenSSL 的版本沒有受到 Heartbleed Bug 的影響，您可輸入以下指令來確認您 OpenSSL 的版本。若您的版本有 Heartbleed Bug，建議先升級到修復版本，再執行以下操作。

#### *\$ openssl version*

影響範圍：1.0.1 ~ 1.0.1f / 1.0.2-beta ~ 1.0.2-beta1

修復版本：1.0.1g / 1.0.2-beta2 以後



```
系統管理員: C:\Windows\system32\cmd.exe
C:\>\cd Apache24\bin

C:\Apache24\bin>openssl version
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
OpenSSL 1.0.1m 19 Mar 2015

C:\Apache24\bin>_
```

- (3) 因 Windows 系統下的 Apache 無法詢問私密金鑰密碼，故產生不加密之 PEM 格式的私密金鑰(長度需為 RSA 2048 位元)

執行 openssl 程式如下：

*\$ openssl genrsa -out <server.key 儲存路徑> 2048*

```
系統管理員: C:\Windows\system32\cmd.exe
C:\>cd Apache24\bin

C:\Apache24\bin>openssl version
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
OpenSSL 1.0.1m 19 Mar 2015

C:\Apache24\bin>openssl genrsa -out C:\SSL\server.key 2048
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

C:\Apache24\bin>
```

- 若您的 SSL 憑證即將到期，需更新憑證，建議可以另開一個新的資料夾，並在此資料夾下執行上述指令，以避免線上使用的 **server.key** 被覆蓋。
  - 依照國際密碼學規範，請使用 RSA 2048 位元(含)以上金鑰長度。
- (4) 執行完畢後會產生私密金鑰檔案，檔名為 server.key，請您將此檔案 **備份**。若是在提出憑證申請後，金鑰遺失，核發下來的憑證將會無法使用，需要重新提出申請與廢止憑證。
- (5) 產生憑證請求檔

***\$ openssl req -new -key <server.key 路徑> -out <certreq.txt 儲存路徑>***

- 若您在執行此指令時遇到「**WARNING: can't open config file...**」的訊息，請先找出 Apache 安裝目錄下的 openssl.cnf，然後執行以下環境變數設定後，在執行產製憑證請求檔指令  
***set OPENSSL\_CONF=<openssl.cnf 所在路徑>***

請輸入憑證主體資訊到憑證請求檔中，不過 PublicCA 網站 SSL 憑證申請頁面只會擷取憑證請求檔的公開金鑰數值，並不會使用以下憑證主體資訊，而是以您在 PublicA 網頁投單所登打之組織與網站名稱資訊為準進行身分審驗。

Country Name : TW

State or Province Name : 不需輸入，按 enter 鍵略過

Locality Name : 城市(如 : Taipei)

Organization Name : 組織名稱(如 : CHT)

Organizational Unit Name : 單位名稱(如 : Information)

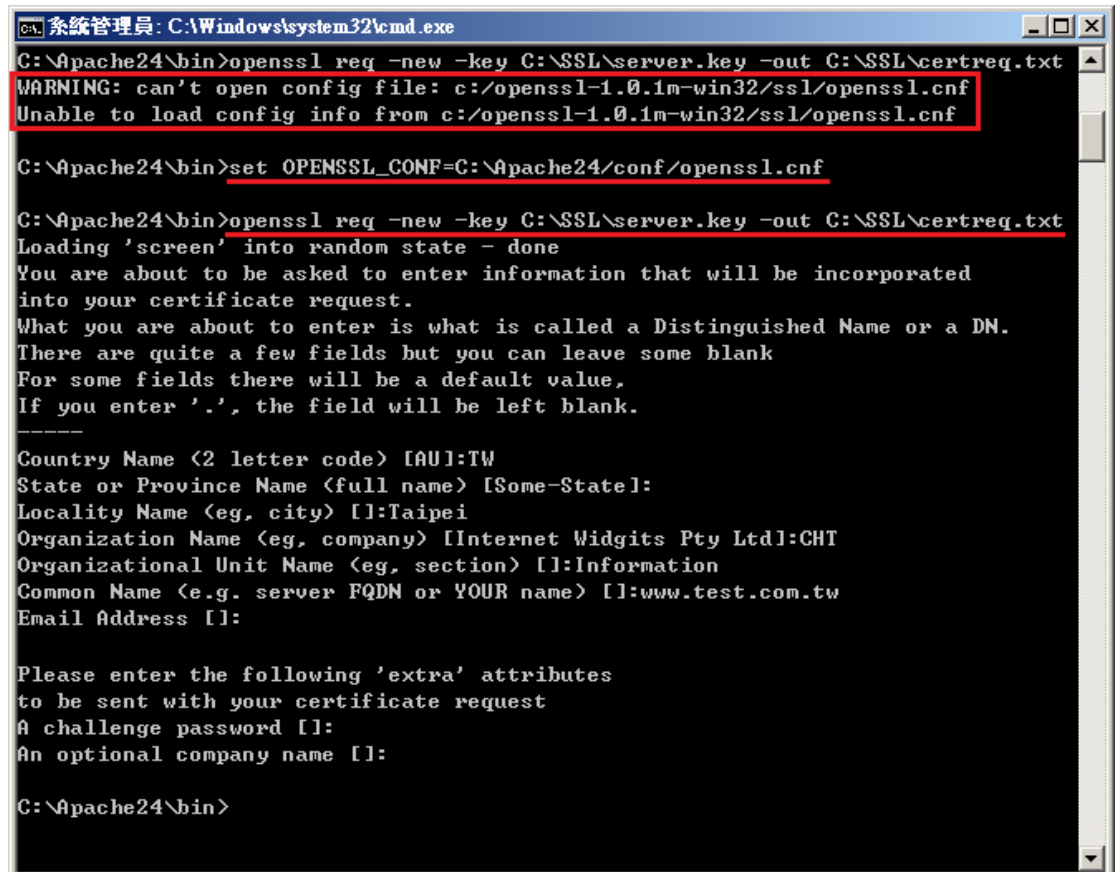


Common name：網站名稱(如：www.abc.com.tw)

Email address：伺服器管理者電子郵件 (如:abc@abc.com.tw)

A challenge password：不需輸入，按 enter 鍵略過

An optional company name：不需輸入，按 enter 鍵略過



```
系統管理員: C:\Windows\system32\cmd.exe
C:\Apache24\bin>openssl req -new -key C:\SSL\server.key -out C:\SSL\certreq.txt
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
Unable to load config info from c:/openssl-1.0.1m-win32/ssl/openssl.cnf

C:\Apache24\bin>set OPENSSL_CONF=C:\Apache24\conf\openssl.cnf

C:\Apache24\bin>openssl req -new -key C:\SSL\server.key -out C:\SSL\certreq.txt
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CHT
Organizational Unit Name (eg, section) []:Information
Common Name (e.g. server FQDN or YOUR name) []:www.test.com.tw
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Apache24\bin>
```

(6) 檢視憑證請求檔

您可使用下面指令檢視您所產生的憑證請求檔

***\$openssl req -noout -text -in <certreq.txt 所在路徑>***

請求檔內容範例如下：



```
系統管理員: C:\Windows\system32\cmd.exe
C:\Apache24\bin>openssl req -noout -text -in C:\SSL\certreq.txt
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=TW, ST=Some-State, L=Taipei, O=CHT, OU=Information, CN=www.test.com.tw
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:bb:12:9c:9a:6b:ae:cd:d5:66:4f:18:3a:fe:a6:
      b4:75:b2:d5:46:c5:75:36:8b:6d:e9:46:52:fb:3b:
      8a:b3:a7:76:e5:1f:39:e8:20:33:4a:d5:d0:4a:f1:
      b8:09:5b:57:6d:bb:90:69:45:62:08:35:12:81:ae:
      e1:0c:2f:00:0a:e4:6b:27:01:80:37:fd:61:a1:c0:
      f0:dc:53:05:25:e0:22:90:19:a6:c9:3e:75:d1:b4:
      63:cd:82:aa:fa:d9:ab:5e:38:58:81:3f:66:54:64:
      8b:0c:c4:4e:67:b8:2e:4c:62:19:82:af:73:7b:f4:
      6c:b4:a1:9c:b5:6c:01:f8:6f:fa:01:58:45:e4:36:
      f1:1b:7d:cb:60:c2:17:1f:38:41:31:5d:2a:e5:23:
      4e:45:17:f8:67:b7:8c:d1:55:66:71:89:4f:87:91:
      17:d1:5c:61:b0:5b:40:1a:2c:23:fd:f1:83:ad:f9:
      2e:77:4c:66:f8:35:e6:fc:30:ec:13:21:bd:f9:88:
      6e:77:7b:32:b2:28:00:b5:b9:75:56:75:be:60:35:
      14:66:05:21:36:2f:3d:6c:02:6a:f4:c2:17:17:38:
      3f:ec:87:51:3c:47:82:0f:21:63:61:82:3c:bb:ee:
      30:f9:7a:6c:ee:21:ed:90:9e:0b:4e:4b:19:92:db:
      31:a3
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha1WithRSAEncryption
  40:c4:47:4b:1a:00:dc:77:7f:7f:f3:9a:07:78:b0:2a:a5:5e:
  d9:90:bc:ec:1e:ba:80:5b:2d:56:b9:0c:dc:d6:76:68:a0:92:
  64:83:41:92:21:89:b1:b3:17:7e:2b:a5:3d:5d:98:c7:5f:9a:
  68:f2:0a:e6:82:62:b9:86:0e:77:48:78:dc:94:31:d4:71:e0:
  3c:72:31:11:6b:c0:59:93:c4:18:88:e7:87:b5:a6:ee:69:1c:
  06:ba:23:dd:f1:fe:d1:7d:ff:ef:97:b0:47:7e:f6:5c:f8:ce:
  ab:fb:2c:33:7c:d9:fb:82:f2:06:84:fb:51:58:83:f3:c6:fe:
  a4:ae:c9:7a:e6:05:b6:b0:48:30:07:fb:ef:27:b2:47:26:41:
  35:e2:68:e3:c4:35:c9:72:dd:0d:f1:2c:93:bf:46:f8:b9:39:
  28:15:eb:2f:19:8b:f8:71:23:3c:5e:dd:a1:19:63:f7:ca:2c:
  e6:4b:6b:d2:02:77:2b:5f:a0:8b:3b:b9:57:a7:5e:05:6c:c3:
  f5:b4:7c:2a:a4:89:db:bf:f1:01:80:63:e7:a0:6e:a5:8d:d1:
  4f:09:ef:17:70:25:3c:46:3a:30:14:86:b4:31:d0:85:f4:3b:
  25:9a:19:e4:d2:68:3b:2d:dd:54:e7:e5:24:e7:fd:61:6d:c9:
  f3:30:1c:4c
C:\Apache24\bin>
```

- 二、 將憑證請求檔存到儲存媒體，完成製作憑證請求檔動作。
- 三、 請將產生的憑證請求檔(certreq.txt)複製，請至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

# Windows Apache SSL 憑證安裝操作手冊

## 一、 取得 eCA 自簽憑證及 Public CA 憑證之憑證串鏈

當您向 Public CA 申請的 SSL 伺服器軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服器軟體憑證，而必須先取得 eCA 自簽憑證及 PublicCA CA 憑證之憑證串鏈，並在 Apache Server 上安裝 eCA 自簽憑證及 PublicCA CA 憑證之憑證串鏈，使您的 Apache Server 信賴 eCA 及 Public CA 的 CA 憑證，這樣您接下來安裝的 SSL 伺服器軟體憑證才會正常運作。如果您以前曾經在同一部 Apache Server 上成功安裝過 eCA 自簽憑證及 Public CA CA 憑證之憑證串鏈，則您可以跳過此步驟，直接進行 SSL 伺服器應用軟體憑證的安裝。

下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採取以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA\_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2\_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈三個檔案。

2. 從網站查詢與下載：

eCA 憑證：

[http://epki.com.tw/download/ROOTeCA\\_64.crt](http://epki.com.tw/download/ROOTeCA_64.crt)

PublicCA G2 憑證：

[http://epki.com.tw/download/PublicCA2\\_64.crt](http://epki.com.tw/download/PublicCA2_64.crt)

SSL 憑證下載：您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，進行 SSL 憑證下載。

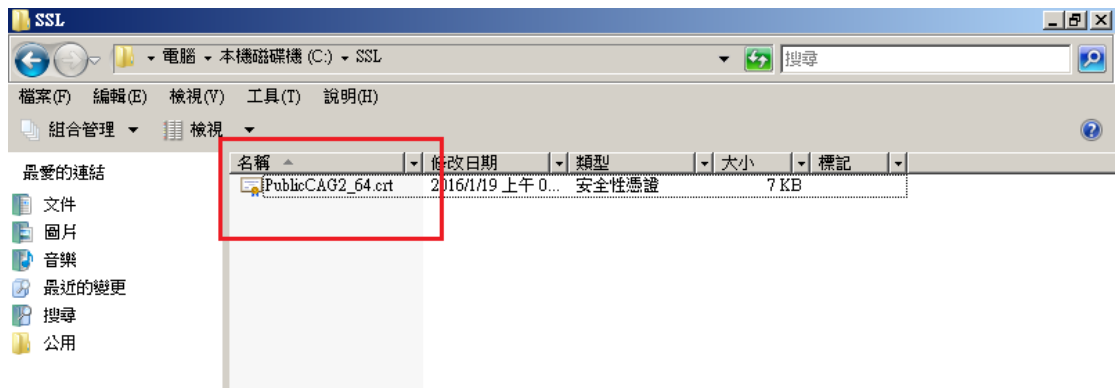
若您是中華電信之員工，負責管理單位之伺服器，請至

<http://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證(請選擇 Based 64 格式)。

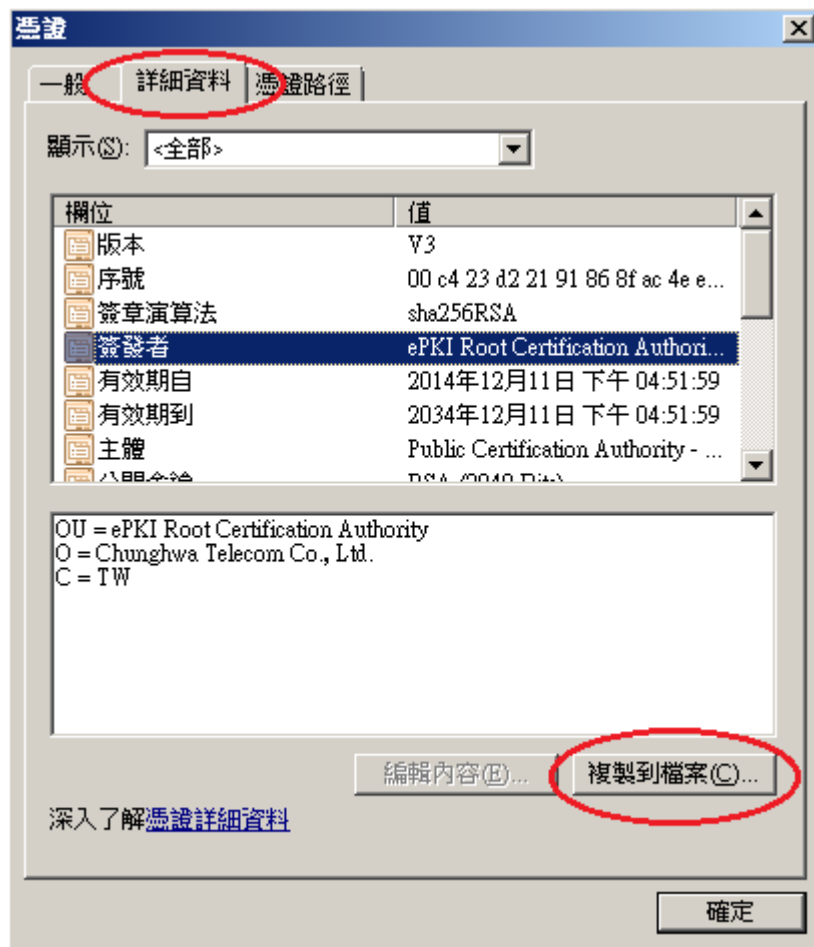
(註：使用 IE 下載.crt 格式的憑證時，IE 會將副檔名.crt 改為.cer，但編碼格式還是屬於 Base64)

3. **以下步驟，以 SHA 256 憑證為安裝範例。**

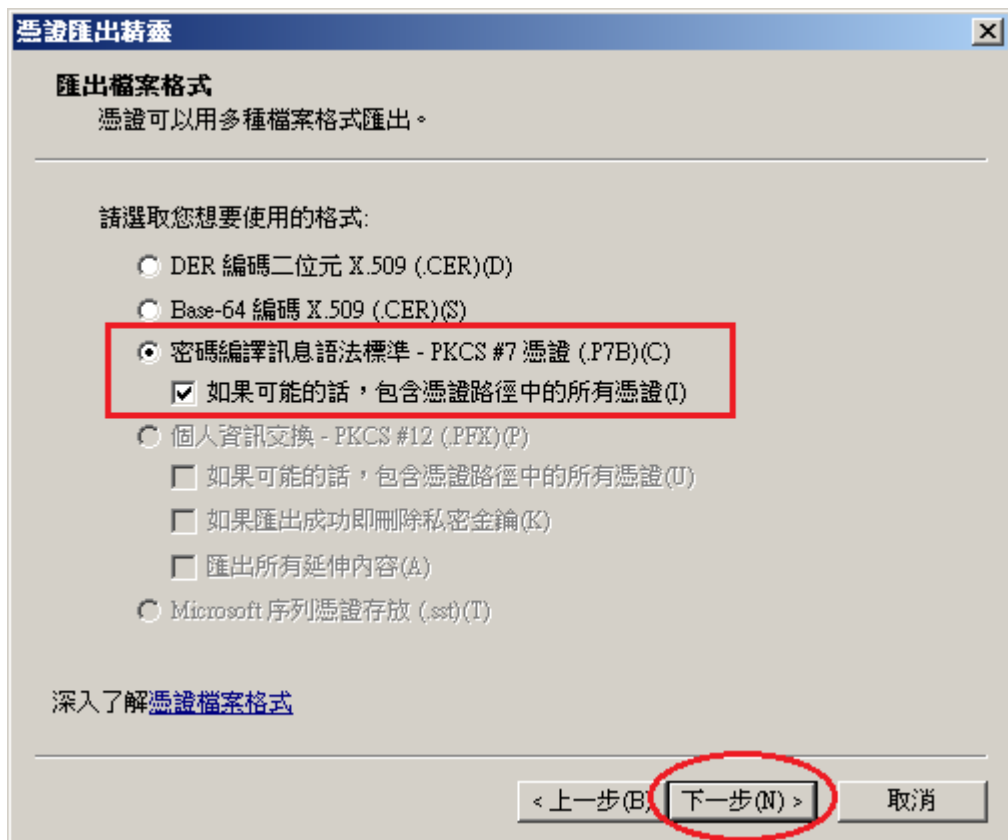
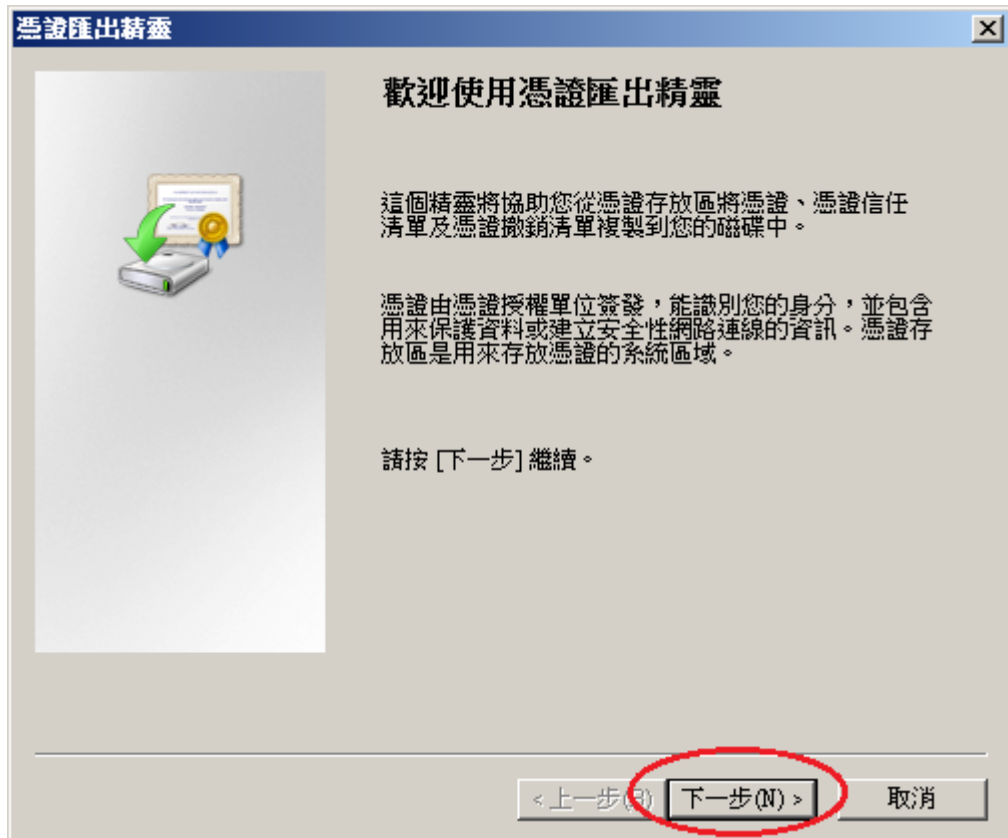
打開儲存的 PublicCA2\_64.crt(PublicCA2\_64.cer)。

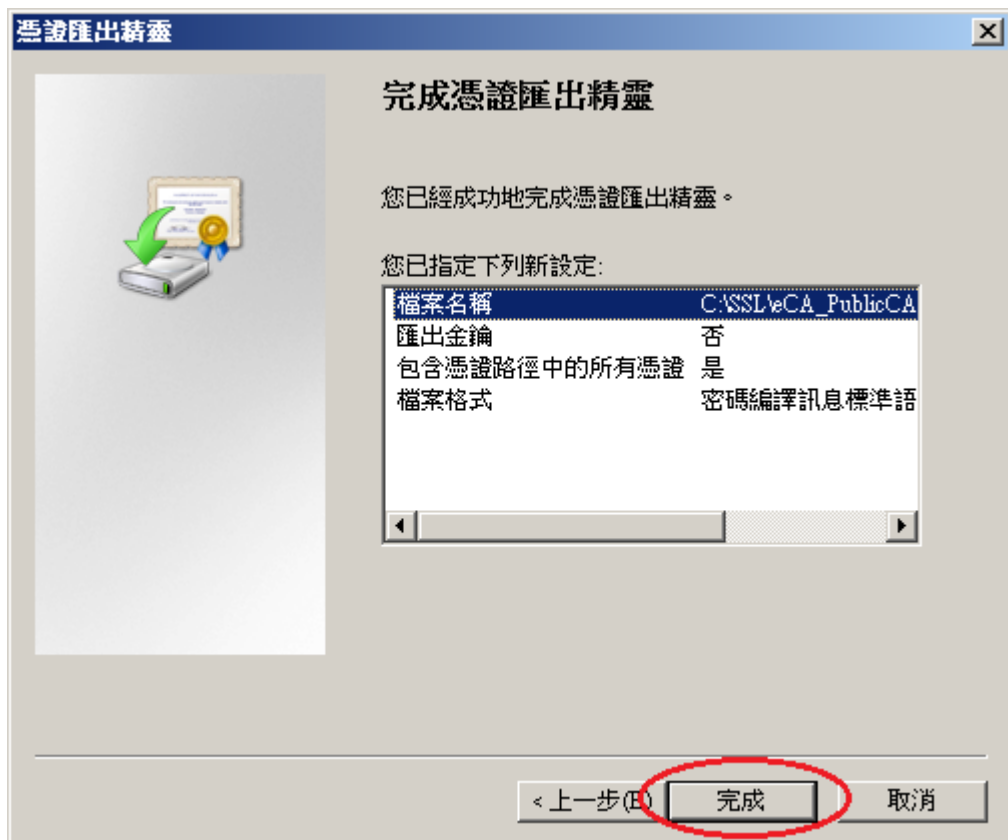
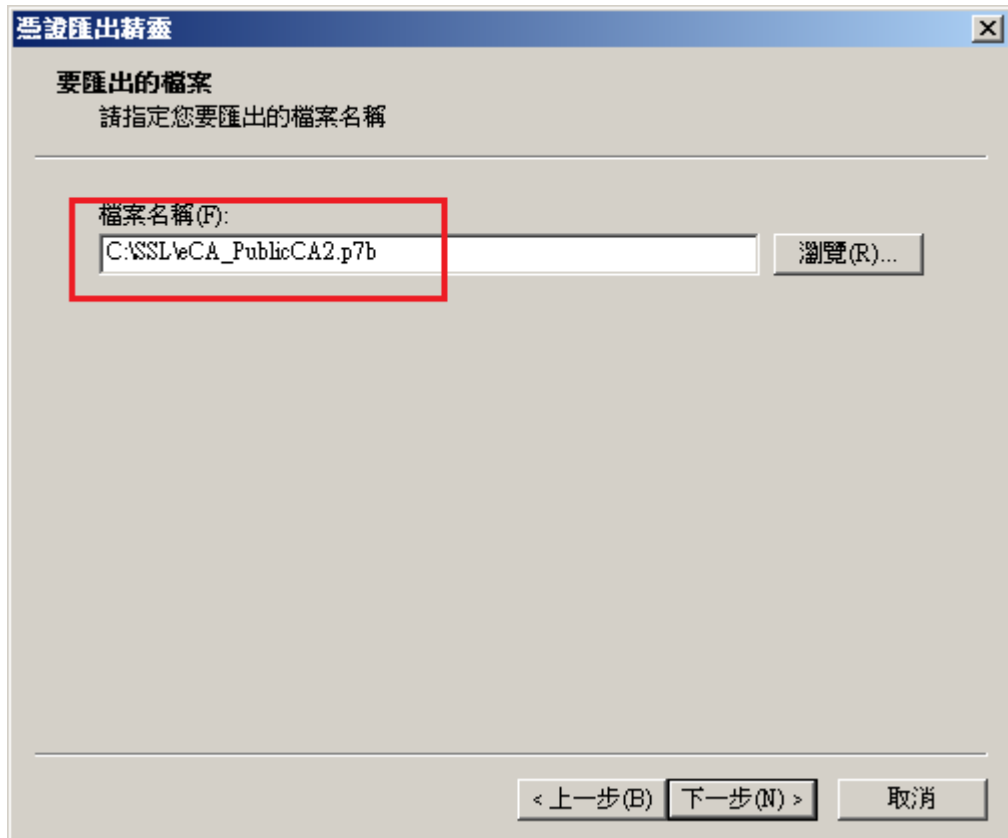


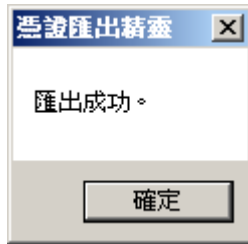
4. 出現憑證檢視的畫面後，請點選「詳細資料」→「複製到檔案」。



5. 請依照下面步驟，匯出 PKCS7 格式檔案。





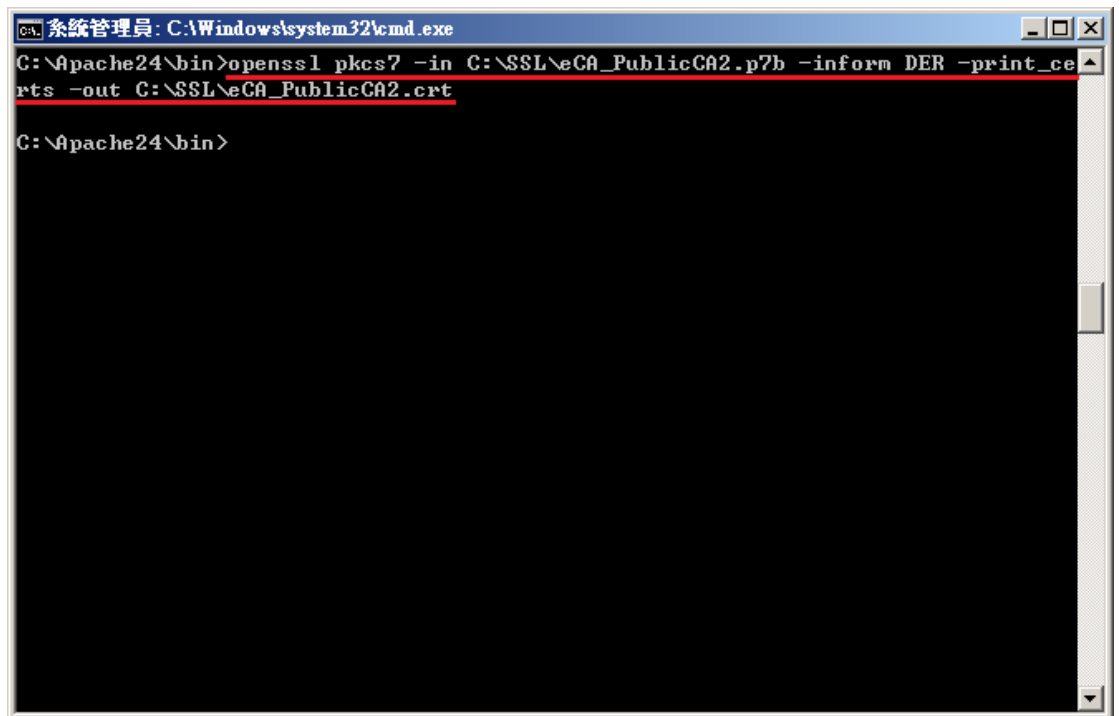


## 二、安裝 eCA 根憑證及 PublicCA 憑證之憑證串鏈與 SSL 憑證

接下來要在 Apache Server 上安裝 eCA 根憑證及 Public CA 中繼憑證之憑證串鏈，使您的 Apache Server 信賴 eCA 及 Public CA 的 CA 憑證。步驟如下：

1. 利用 OpenSSL，將上一階段取得之 eCA\_PublicCA2.p7b 由 DER 編碼格式轉換成 PEM 編碼格式，即 Base64 編碼格式

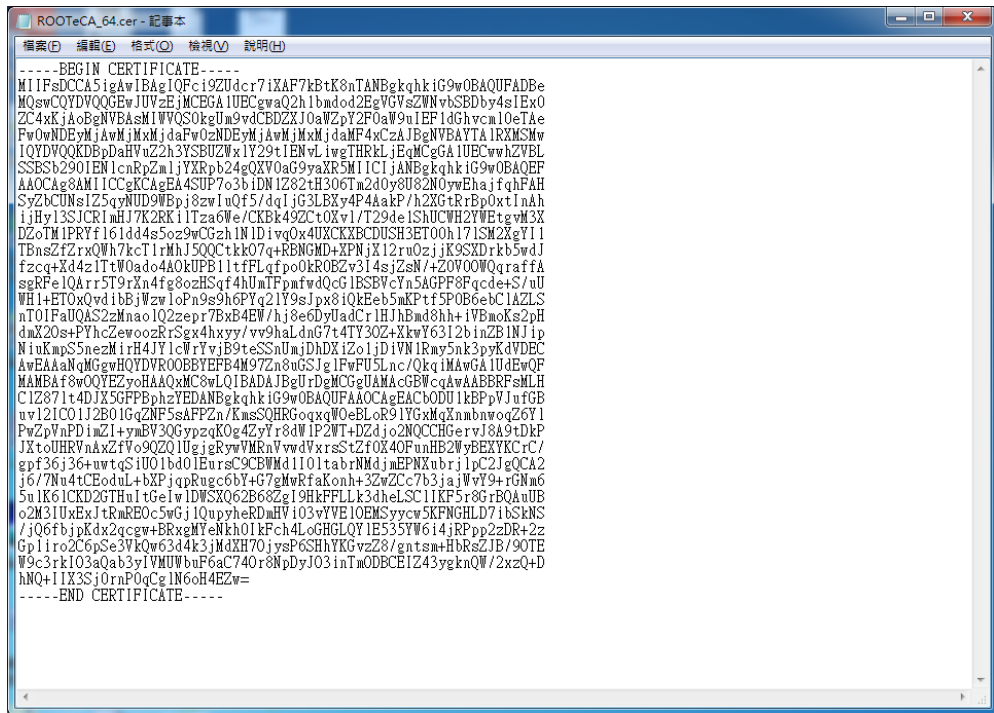
***openssl pkcs7 -in <eCA\_PublicCA.p7b 檔案所在路徑> -inform DER  
-print\_certs -out <eCA\_PublicCA.crt 檔案儲存路徑>***



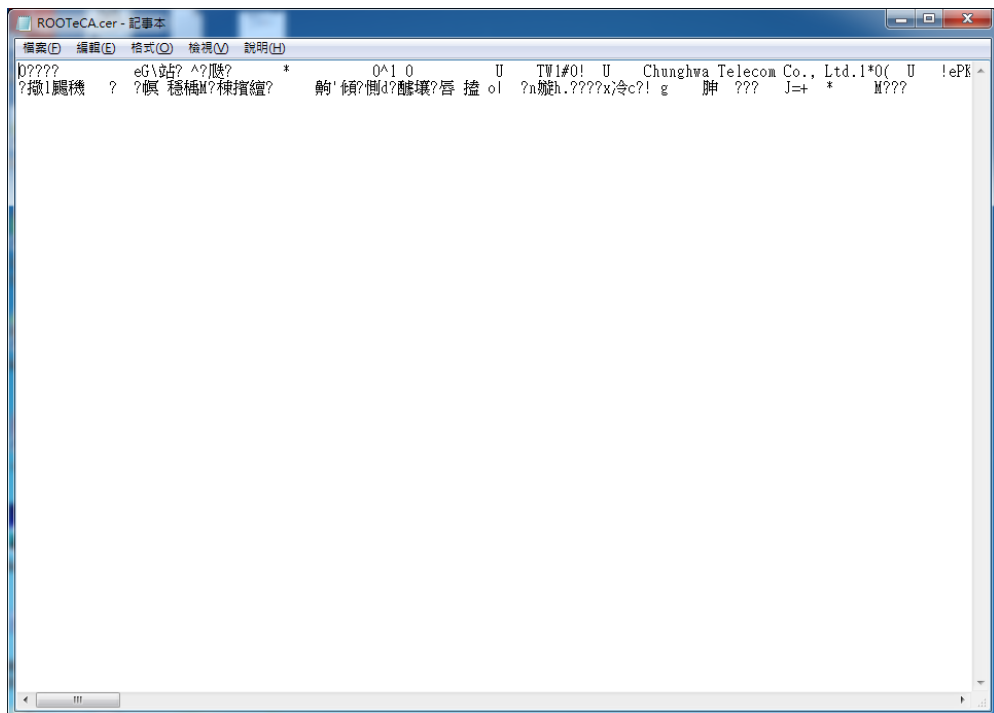
2. 請確定已下載儲存已簽發之 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成的 cer 或是 crt 檔案)。
3. 目前已簽發之 SSL 伺服器軟體憑證皆為 PEM 編碼格式(即 Base64 編碼格式)，若您的 SSL 伺服器軟體憑證為 DER 編碼格式，請執行以下命令將 SSL 伺服器軟體憑證由 DER 編碼格式轉換成 PEM 編碼格式  
***openssl x509 -in <伺服器憑證路徑> -inform DER -out <server.crt 檔案儲存路徑>***

**如何確認憑證編碼格式：**請利用文字編輯器將憑證檔案開啟，根據出現的畫面來判別憑證編碼格式。

PEM 編碼格式：



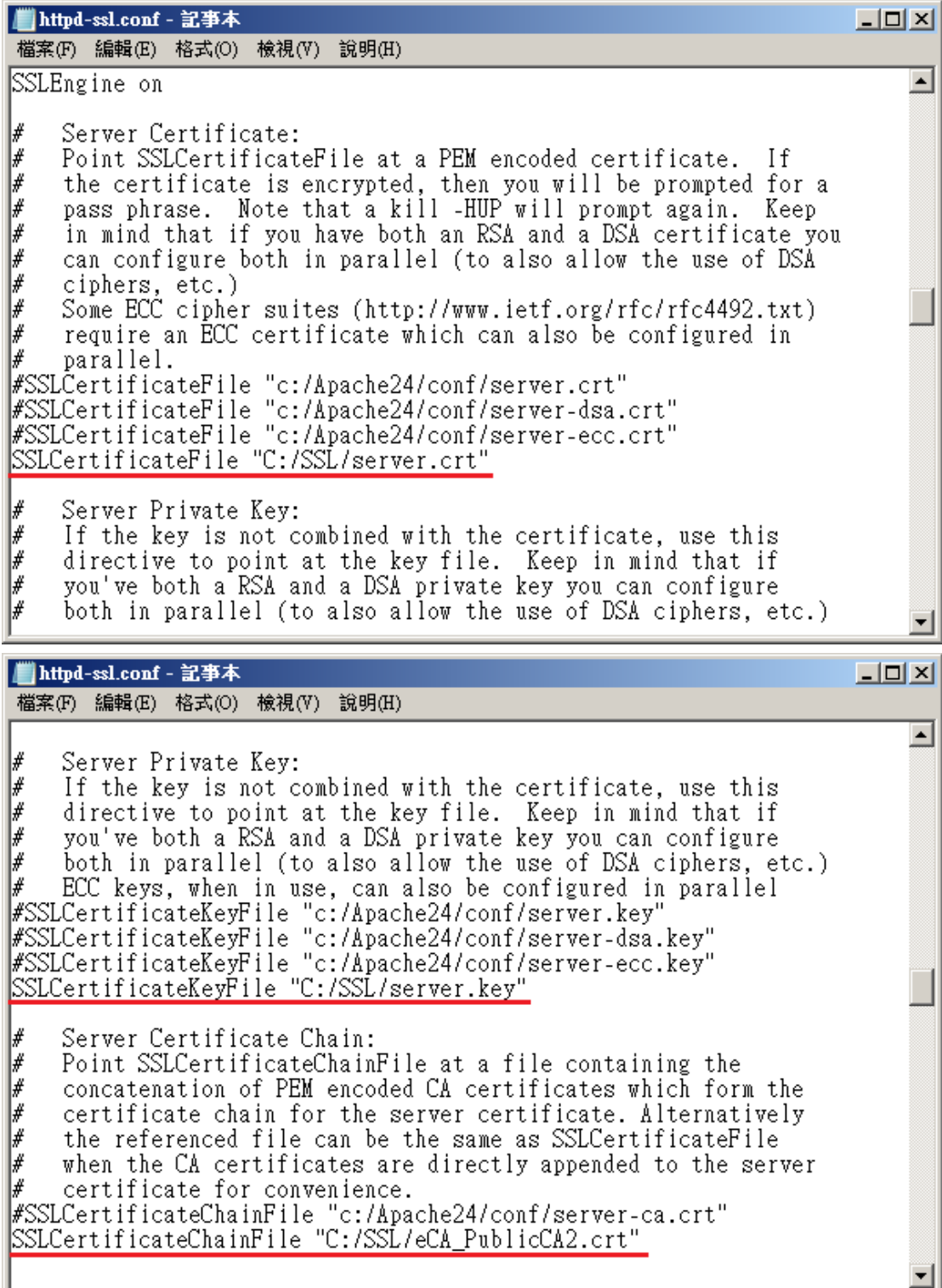
DER 編碼格式：



4. 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為 <apache 安裝路徑>\conf\extra\ 目錄下。
5. 修改以下三個參數並存檔
  - SSLCertificateFile：伺服器憑證(.cer 或.crt)檔案路徑
  - SSLCertificateKeyFile：私密金鑰檔案路徑
  - SSLCertificateChainFile：eCA\_PublicCA2.crt 檔案路徑



請注意這個 `SSLCertificateKeyFile` 所指向的金鑰必須是當初您用來產生憑證請求檔(CSR 檔)的同一個金鑰，否則將無法成功建立 SSL 連線。



```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
#SSLCertificateFile "c:/Apache24/conf/server.crt"
#SSLCertificateFile "c:/Apache24/conf/server-dsa.crt"
#SSLCertificateFile "c:/Apache24/conf/server-ecc.crt"
SSLCertificateFile "C:/SSL/server.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)

httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
#SSLCertificateKeyFile "c:/Apache24/conf/server.key"
#SSLCertificateKeyFile "c:/Apache24/conf/server-dsa.key"
#SSLCertificateKeyFile "c:/Apache24/conf/server-ecc.key"
SSLCertificateKeyFile "C:/SSL/server.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile "c:/Apache24/conf/server-ca.crt"
SSLCertificateChainFile "C:/SSL/eCA_PublicCA2.crt"
```

6. 重新啟動 Apache
7. 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。
8. 成功後，請以 https 連線試試加密通道。



### 三、 安裝 SSL 安全認證標章

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，內有 SSL 安全認證標章安裝說明，請參考將網站 SSL 安全認證標章安裝成功。

## 附件一：設定 SSL 安全通道的加密強度

- Apache 使用 OpenSSL 的加密套件來做資料加密，而 Apache 加密套件的使用順序可在 `http.conf` 或是 `http-ssl.conf` 中的 `SSLCipherSuite` 找到。
- 預設值是「HIGH:MEDIUM:!aNULL:!MD5」，也就是加密強度「高」(HIGH encryption cipher suites，如 AES 256 bit)、加密強度「中」(MEDIUM encryption cipher suites，如 AES 128 bit)的順序，因此，只要 OpenSSL 有支援 AES 256 bit 的加密套件，伺服器預設就會優先使用 AES 256bit，不需要做額外設定，但需要檢查 OpenSSL 的版本。
- OpenSSL 於 0.9.7 版開始支援 AES Cipher Suites，請透過以下指令檢查 OpenSSL 版本是否高於 0.9.7 「*openssl version*」。

## 附件二：停用 SSLv3.0

- OpenSSL 1.0.1j 版本有針對 POODLE 弱點進行修補，您可選擇同時更新 OpenSSL 版本與停用 SSLv3.0，或是直接停用 SSLv3.0。
- 先開啟 http.conf 或是 http-ssl.conf 檔案，並找到“SSLProtocol all -SSLv2”，其意思為所有 SSL 通訊協定，扣除 SSLv2.0。因此，若要停用 SSLv3.0，只要將上述改為“SSLProtocol all -SSLv2 -SSLv3”，重新啟動 Apache 即可。

```
# SSL Protocol support:
# List the protocol versions which clients are allowed to
# connect with. Disable SSLv2 by default (cf. RFC 6176).
SSLProtocol all -SSLv2 -SSLv3
```

- 啟動完成後，可使用測試工具（註 1、註 2）進行檢測，看 SSLv3.0 是否已停用。

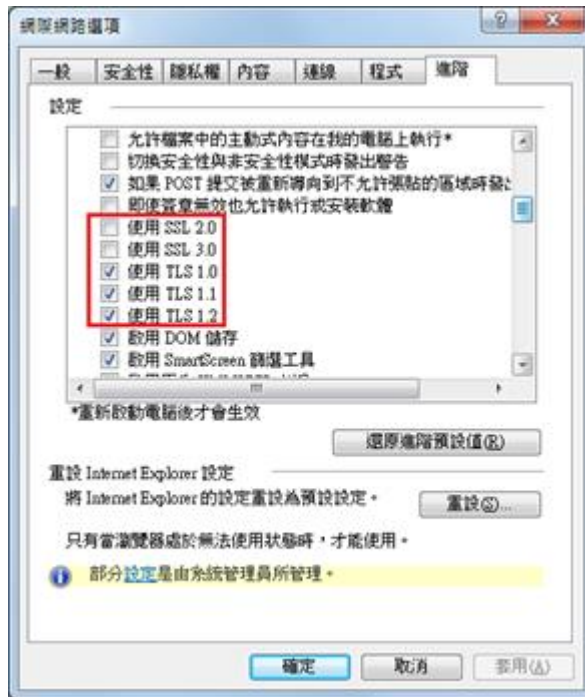
註 1: 例如行政院國家資通安全會報技服中心網頁

<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh> 有介紹兩種檢測伺服器端 SSL 協定的工具：(1) TestSSLServer

(<http://www.bolet.org/TestSSLServer/>) (2) QUALYS SSL LABS SSL Server Test 檢測工具(<https://www.ssllabs.com/ssltest/index.html>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定，因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點，弱點編號 CVE-2014-3566 (POODLE)，故建議不要使用 SSL V3 協定，請改用 TLS 最新協定。

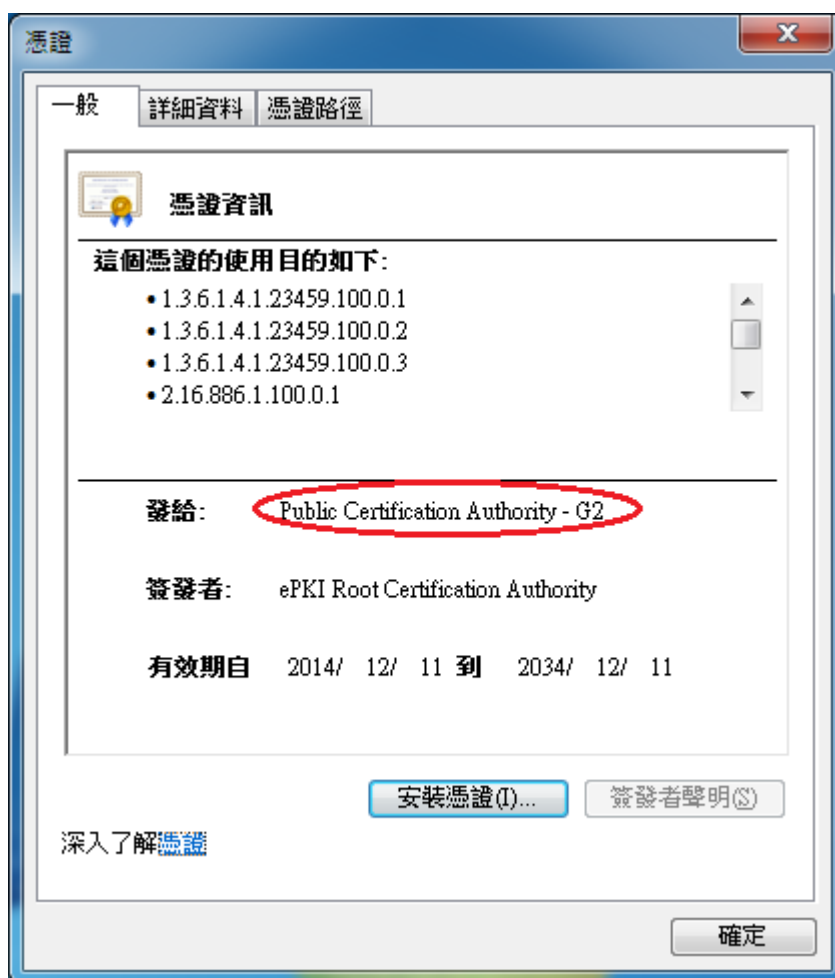
註 2:

- (1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <https://zmap.io/ssl3/browsers.html> 之英文說明
- (2) 請超連結至 <https://dev.ssllabs.com/ssltest/viewMyClient.html> 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。
- (3) 若是 I.E. 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選使用 SSL V3 與使用 SSL V2，或參考下圖設定（取材自行政院國家資通安全會報技服中心網頁 <http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh>）

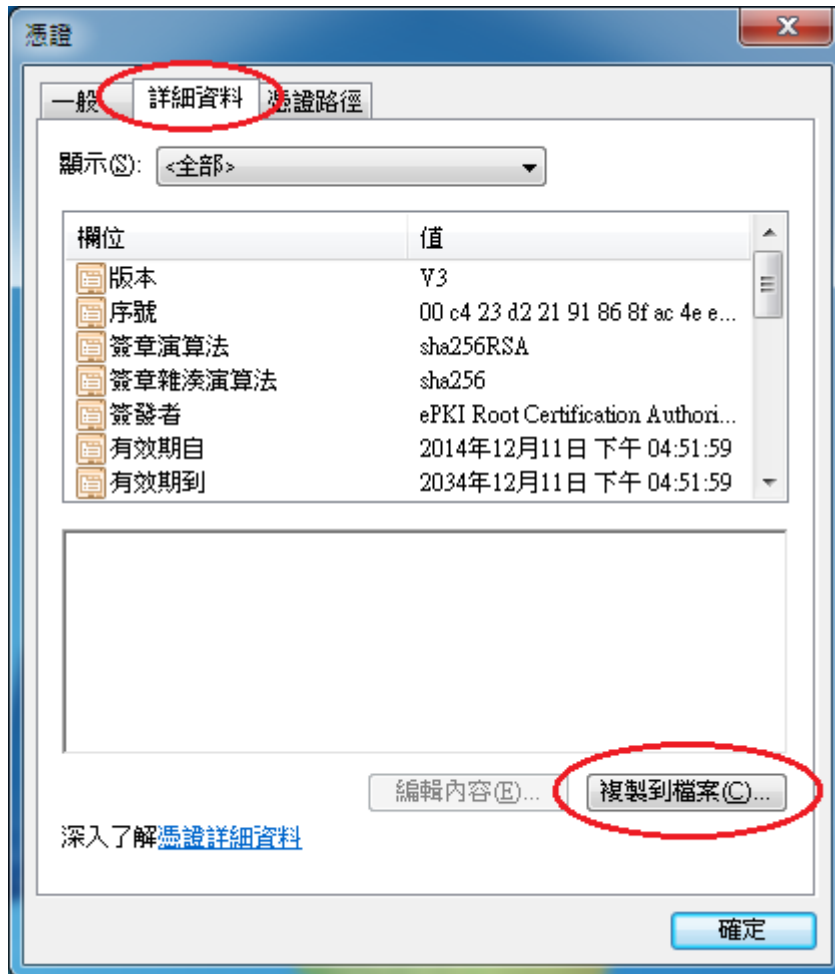


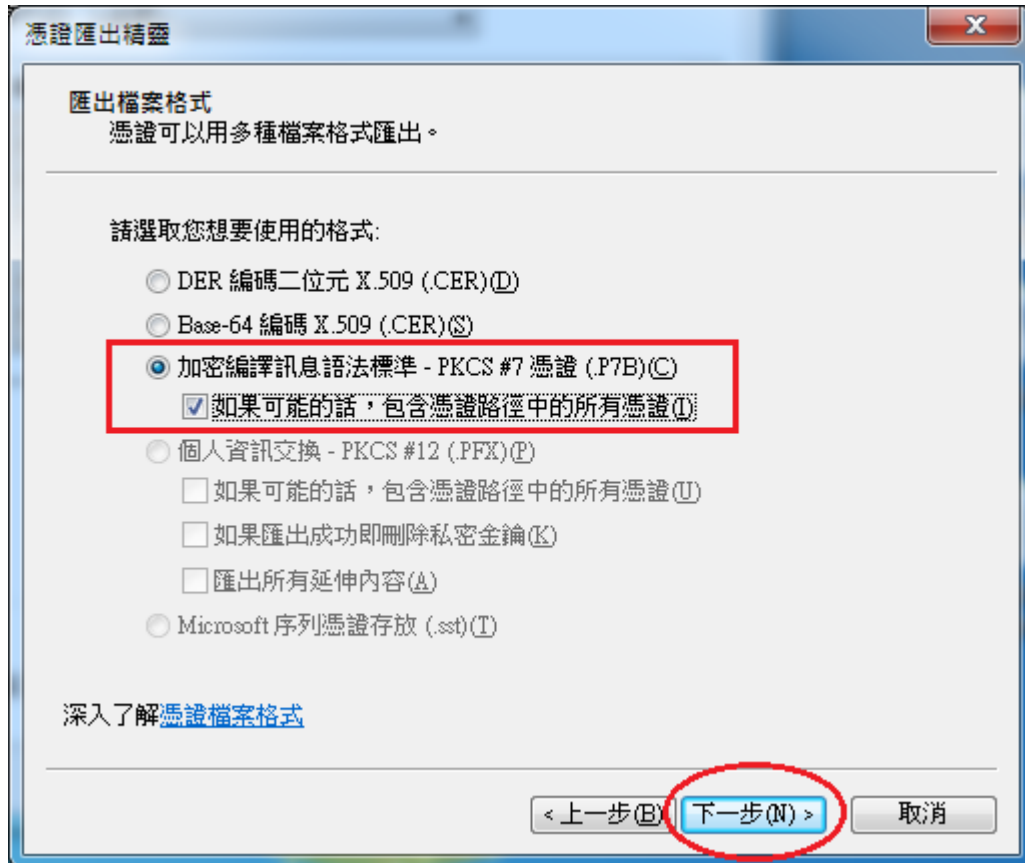
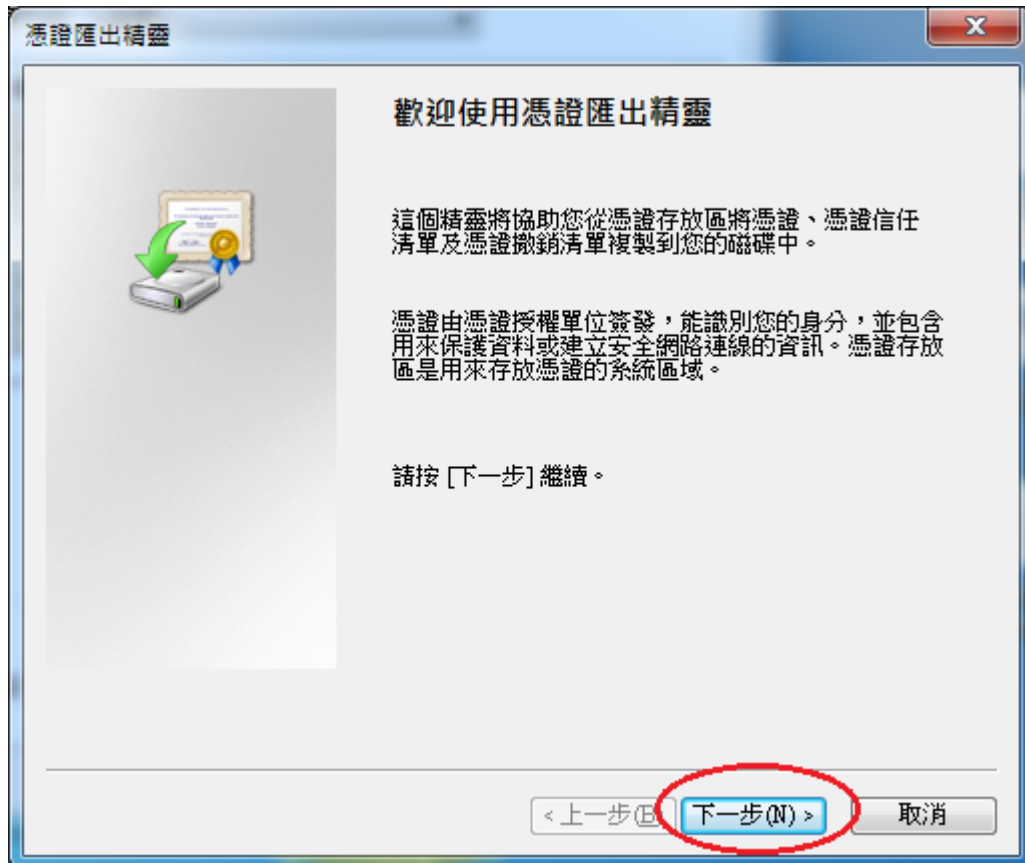
## 附件三：更換 SHA 256 憑證

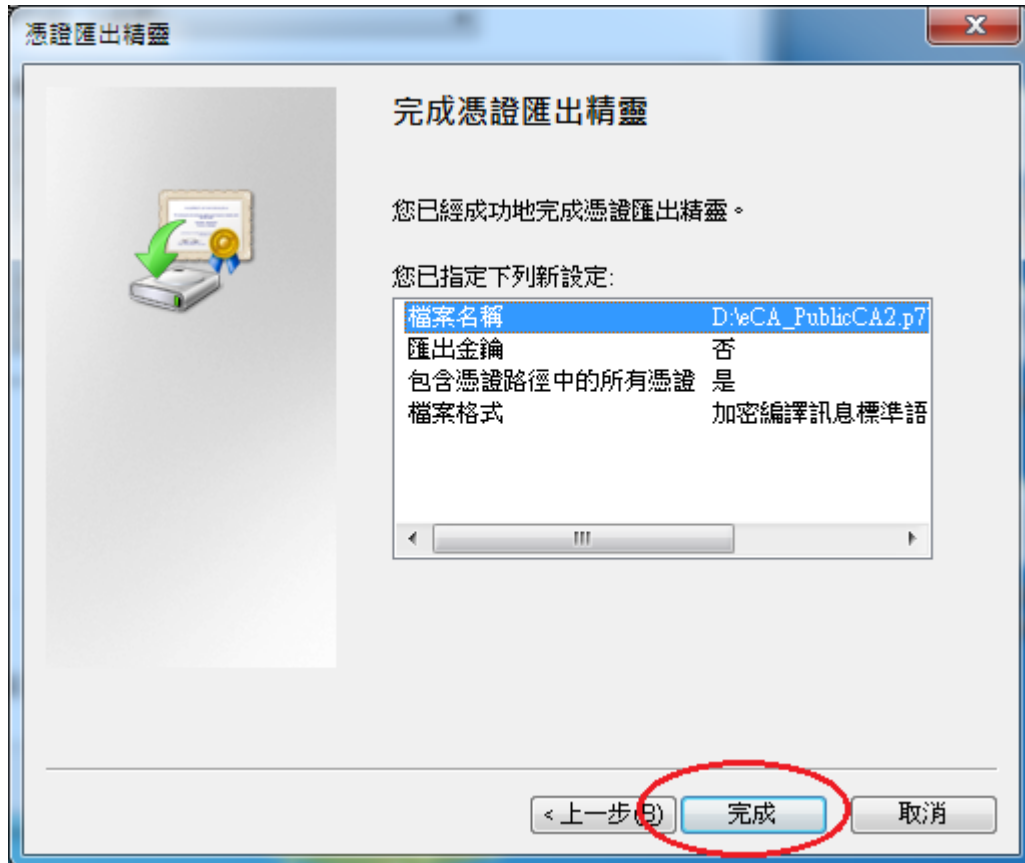
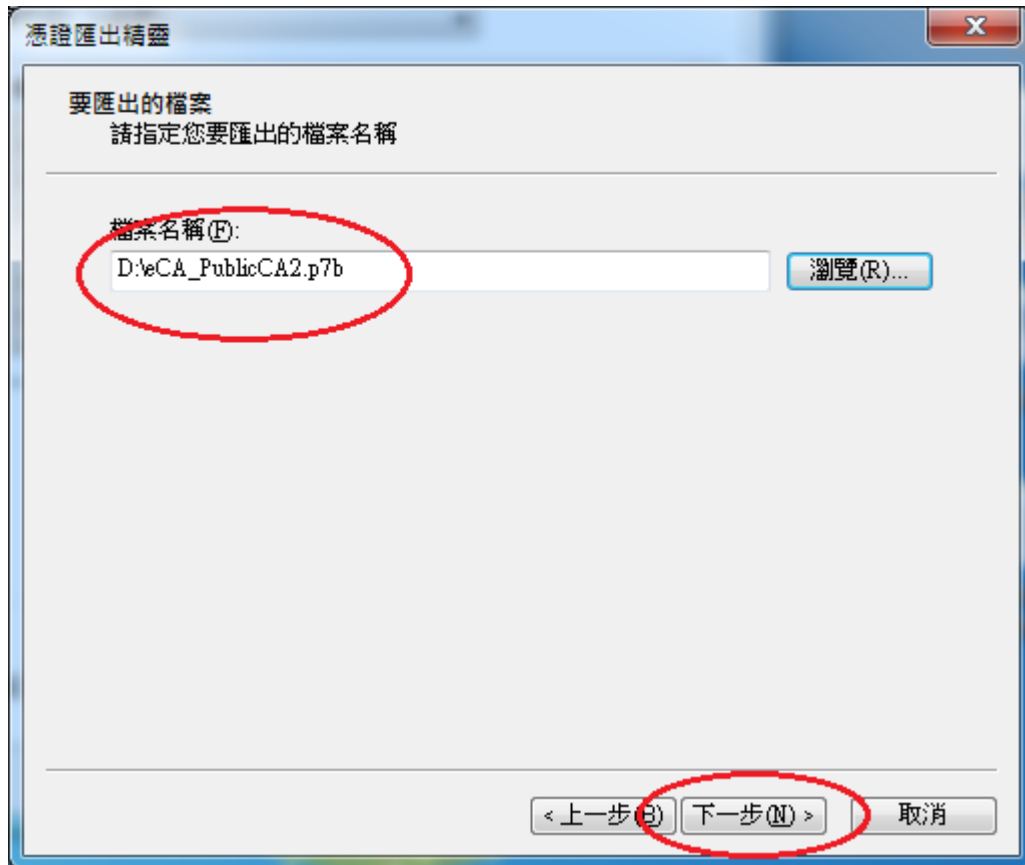
- 適用於申請時，有同時取得 SHA-1、SHA 256 憑證。或是憑證在效期內，經由審驗人員再次核發 SHA256 憑證者。
- 有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(<https://publicca.hinet.net/SSL-08-06.htm>)。
- 點開「PublicCA2\_64.crt」，並確認為「Public Certification Authority - G2」



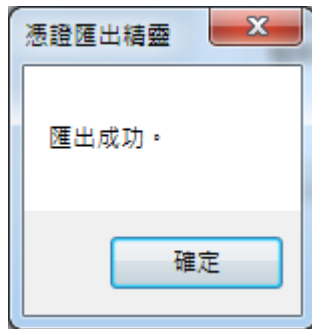
切換至「詳細資料」，點選「複製到檔案」











- 執行以下命令將憑證串鏈檔案由 DER 編碼格式轉換成 PEM 編碼格式  
*openssl pkcs7 -in eCA\_PublicCA2.p7b -inform DER -print\_certs -out eCA\_PublicCA2.pem*
- 修改  
SSLCertificateFile：指向 SHA256 用戶端憑證路徑  
SSLCertificateChainFile：指向”eCA\_PublicCA2.pem”路徑  
SSLCertificateKeyFile：不需要修改
- 重新啟動 Apache Server