中華電信通用憑證管理中心(PublicCA)

Ubuntu Apache2 伺服器 SSL 憑證請求檔製作與憑證安裝手冊

本手冊的安裝程序，已經在 Ubuntu13.10 + Apache2.4.6 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 伺服軟體憑證安裝步驟。本手冊分為製作憑證請求檔（Certificate Signing Request file, 簡稱 CSR 檔）、安裝憑證與安裝 SSL 安全認證標章，並提供附件說明如何設定 SSL 安全通道的加密強度、停用 SSL v3.0 與更換 SHA 256 憑證。

目錄

Ubuntu Apache2 SSL 憑證請求檔製作手冊

一、 製作憑證請求檔

(1) 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

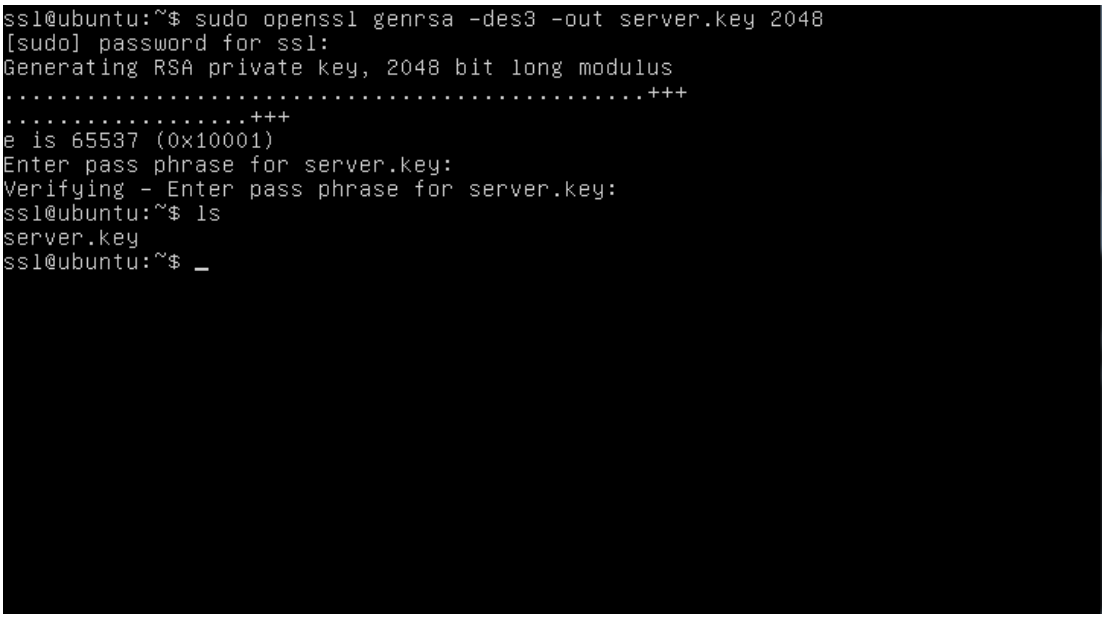
影響範圍：1.0.1 ~ 1.0.1f / 1.0.2-beta ~ 1.0.2-beta1

修復版本：1.0.1g / 1.0.2-beta2 以後

(2) 請執行以下指令來產生金鑰，金鑰會產生在當前的目錄下

$ sudo 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。



(3) 執行時會輸入兩次密碼，請牢記此組密碼，日後啟動 Apache 時皆會使用，並請妥善保管此金鑰(server.key)。

(4) 請執行以下指令，以產生憑證請求檔

$ sudo openssl req -new -key server.key -out certreq.txt

```
ssl@ubuntu:~$ sudo openssl req -new -key server.key -out certreq.txt
Enter pass phrase for server.key:
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) []:GND
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 []:
ssl@ubuntu:~$ ls
certreq.txt  server.key
ssl@ubuntu:~$ _
```

（5）請先輸入剛才設定的私密金鑰密碼，接著依照畫面填入所需資料：

Country Name:	填入 TW
State or Province Name:	不需要填，按 Enter 跳過
Locality Name:	城市(ex: Taipei)
Organization Name:	組織名稱(ex: CHT)
Organization Unit Name:	單位名稱(ex: GND)
Common Name:	網域名稱(ex: www.test.com.tw)
Email Address:	可不填，按 Enter 跳過
A challenge password:	不需要填，按 Enter 跳過
An optional company name:	不需要填，按 Enter 跳過

二、 將憑證請求檔存到儲存媒體，完成製作憑證請求檔的製作。

三、 請持產製好的憑證請求檔(certreq.txt)，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。

Ubuntu Apache2 SSL 安裝操作手冊

一、 取得 eCA 自簽憑證及 Public CA 憑證之憑證串鏈

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，可採以下兩種方式之一取得：

- 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 3 個檔案。
- 從網站查詢與下載：

  eCA 憑證：

  http://epki.com.tw/download/ROOTeCA_64.crt

  PublicCA G2 憑證：

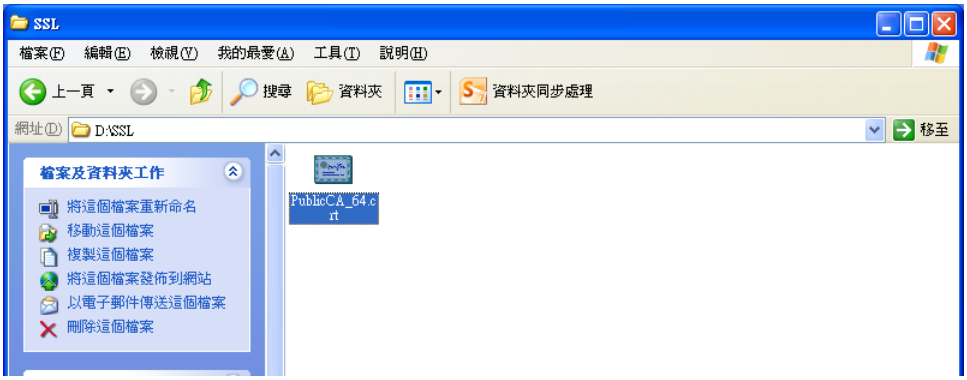
  http://epki.com.tw/download/PublicCA2_64.crt

  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。

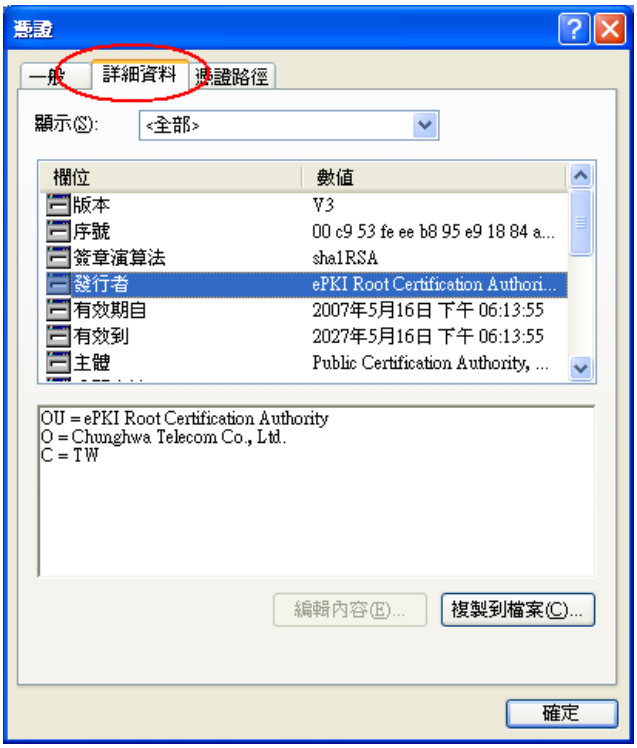
  若您是中華電信之員工，負責管理單位之伺服器，請至 http://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，輸入查詢條件，下載 SSL 憑證。

(1) **以下步驟，以 SHA-1 憑證為安裝範例。**

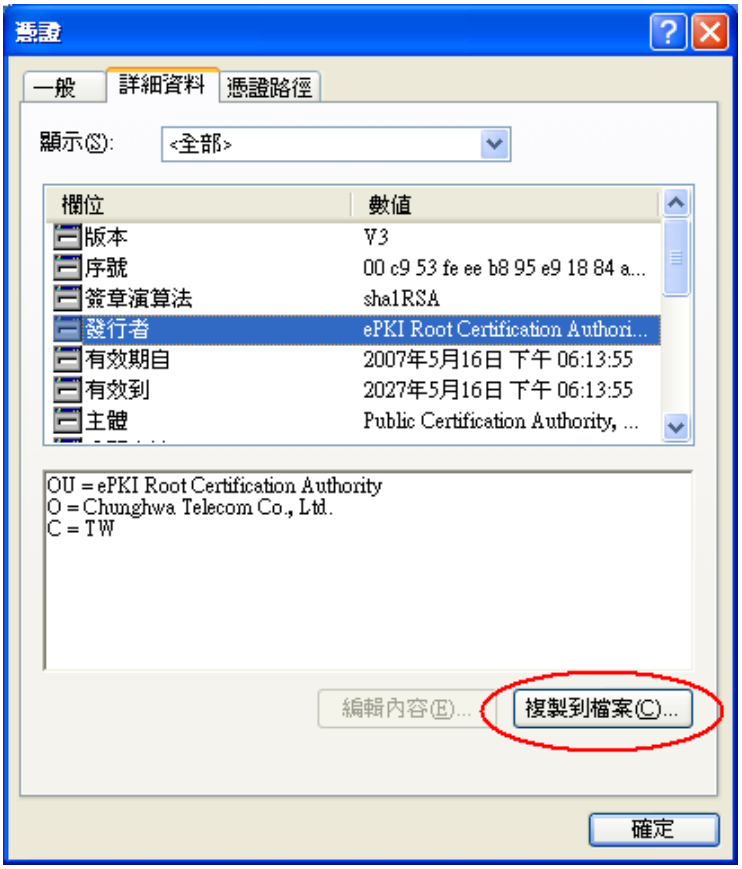
點開 PublicCA_64.crt。



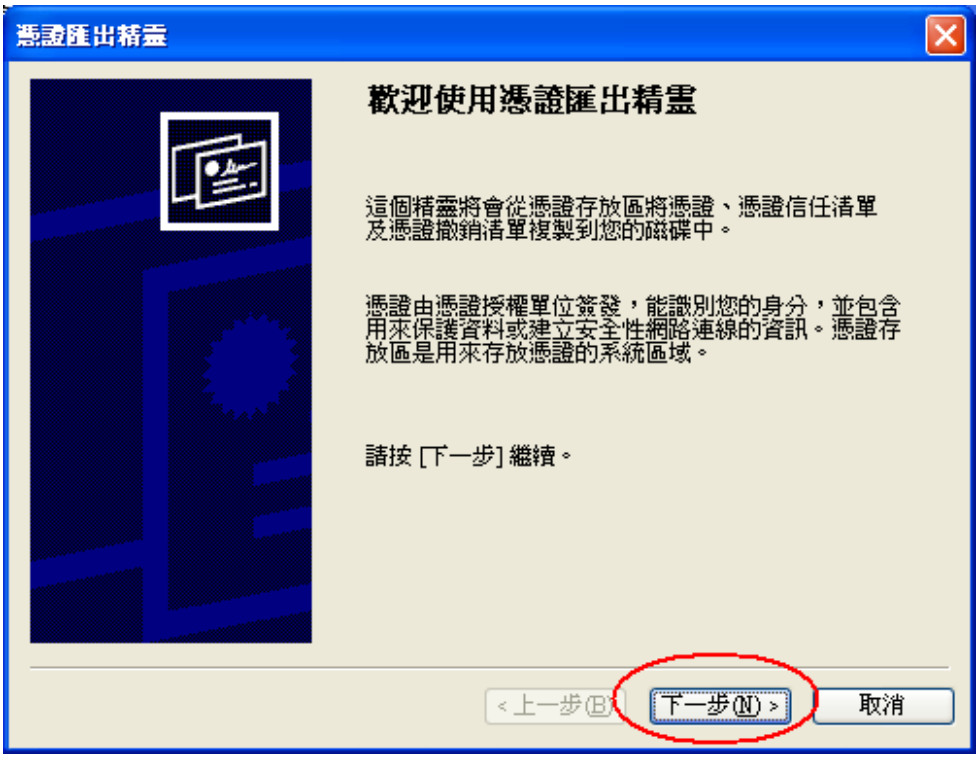
點選「詳細資料」。



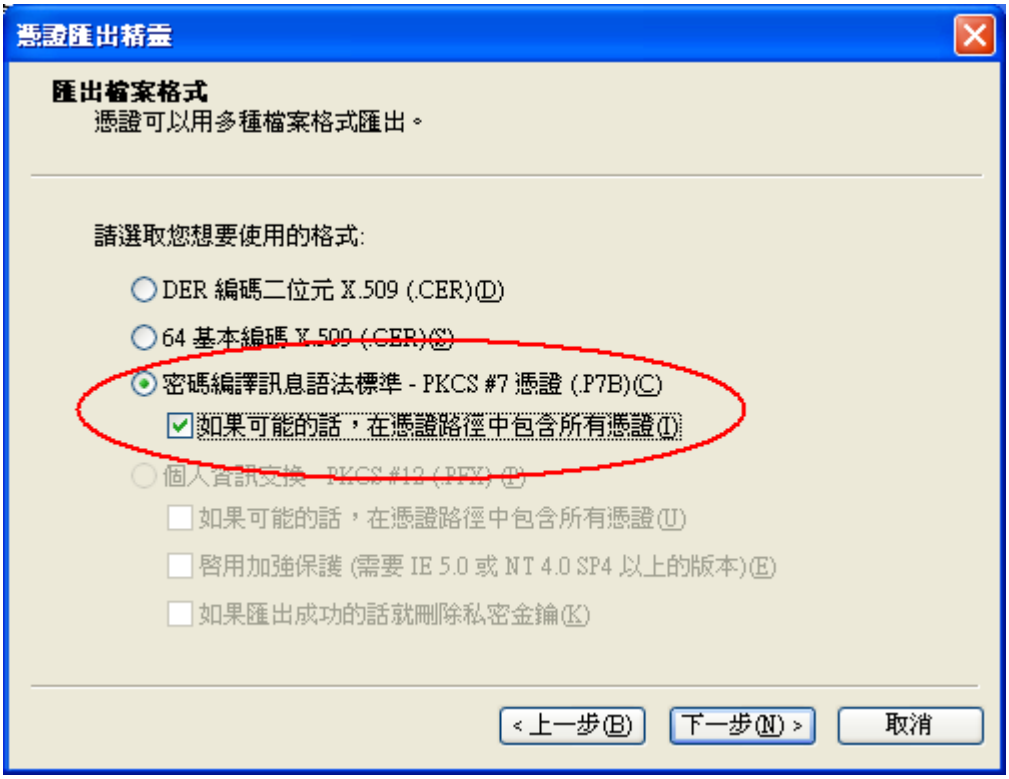
點選「複製到檔案」。



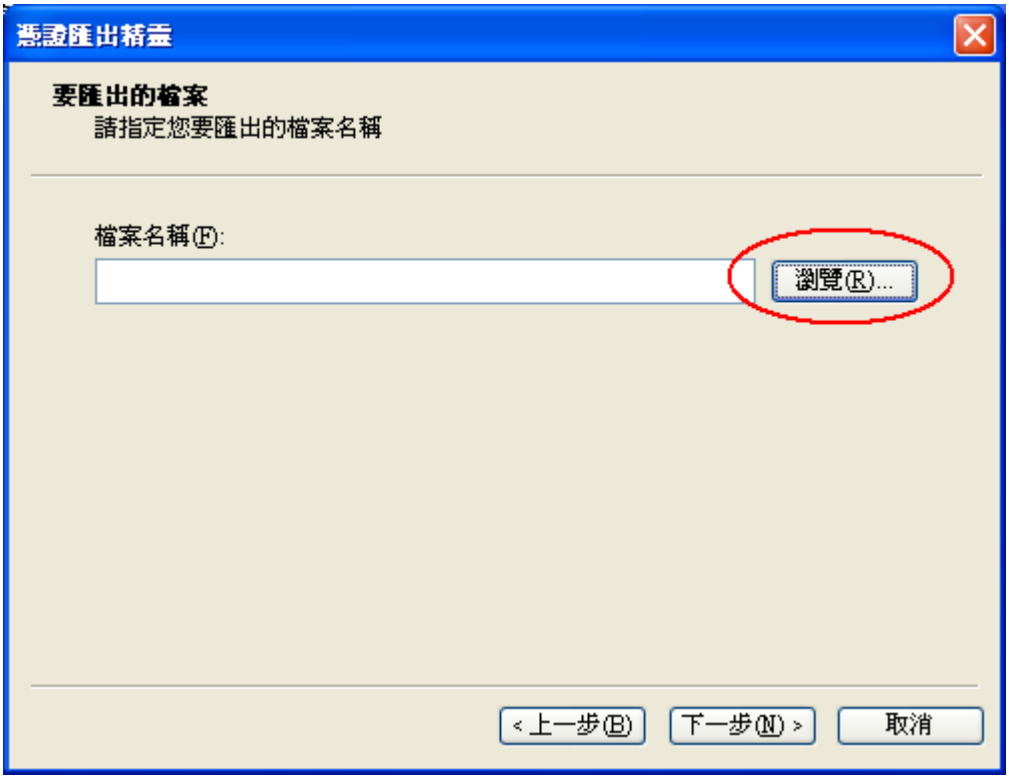
出現以下憑證匯出精靈的畫面，請點選「下一步」。



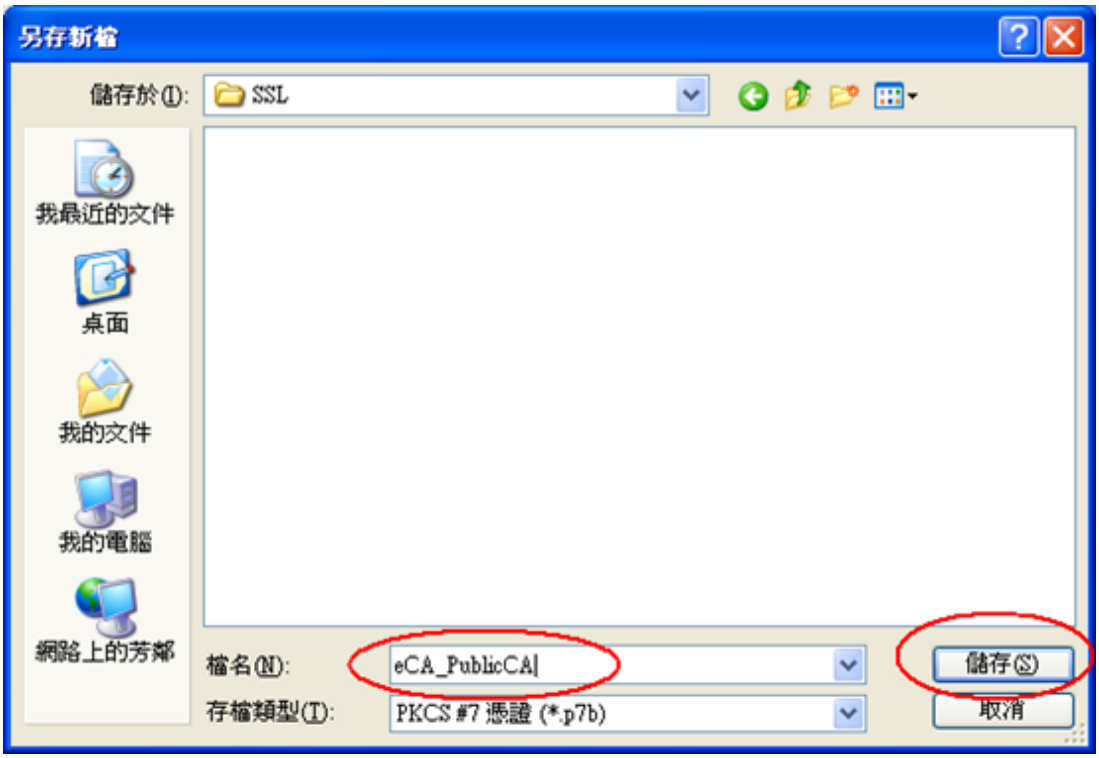
出現以下憑證匯出精靈的畫面，請勾選「密碼編譯訊息語法標準-PKCS#7 憑證」及「如果可能的話，在憑證路徑中包含所有憑證」兩個選項，然後點選「下一步」。



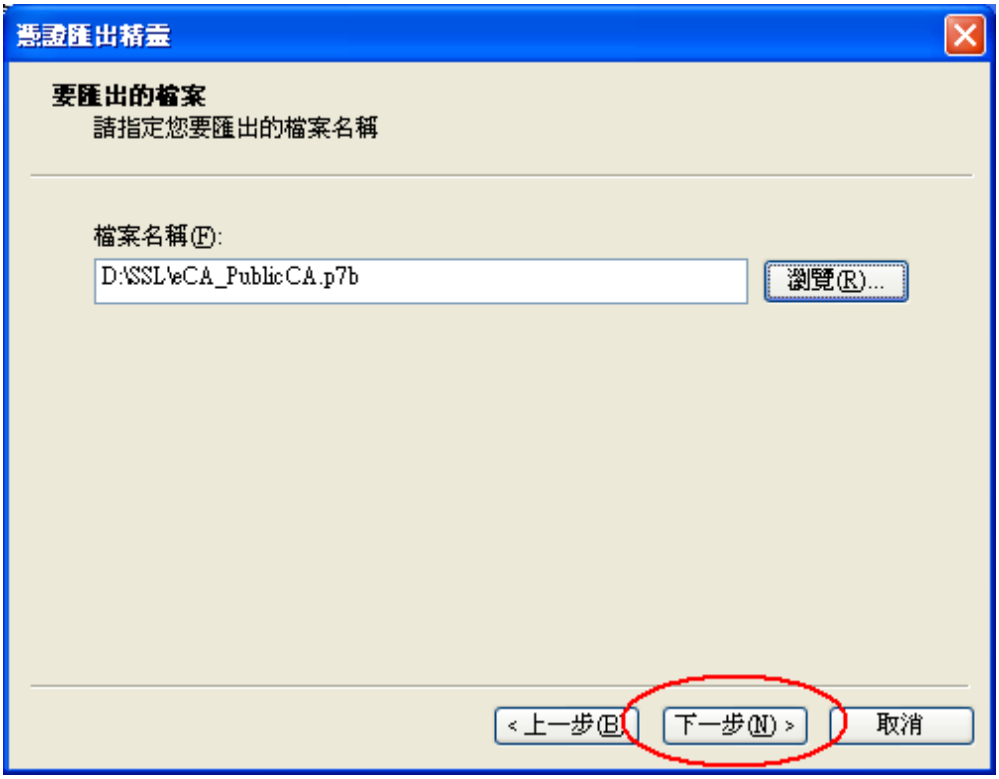
點選「瀏覽」。



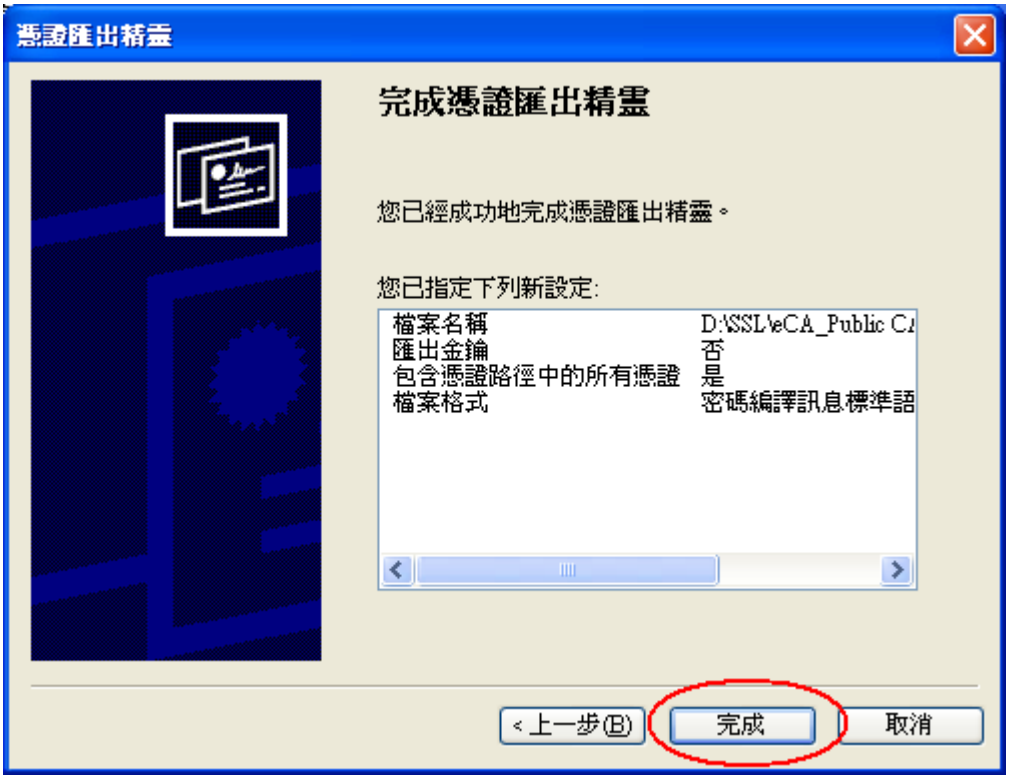
出現另存新檔的畫面，請選擇適當的資料夾位置，檔案名稱請輸入「eCA_PublicCA」，然後點選「存檔」。



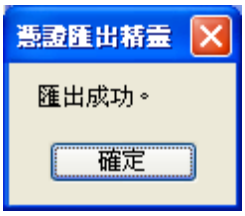
出現以下憑證匯出精靈的畫面，請點選「下一步」。



出現以下憑證匯出精靈的畫面，請點選「完成」。



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 憑證之憑證串鏈的取得。



(2) 把在上一階段取得的 eCA 根憑證及 PublicCA 憑證之憑證串鏈 eCA_PublicCA.p7b 以及由憑證管理中心簽發給 SSL 伺服器的憑證，複製 1 份或傳送 1 份（請注意：如果使用 FTP 必須使用 Binary 模式來傳送）到伺服器中。

(3) 執行以下指令將憑證串鏈檔案由 DER 編碼格式轉換成 PEM(Base64)編碼格式：

$ sudo openssl pkcs7 -in eCA_PublicCA.p7b -inform DER -print_certs -out eCA_PublicCA.crt

(4) 接著，可以將 server.key、eCA_PublicCA.crt、SSL 伺服器憑證移到某個資料夾(ex: /etc/ssl/webssl/)，以方便管理

(5) 使用以下指令來啟動 Apache2 的 SSL 模組

$ sudo a2enmod ssl

(6) 檢視 /etc/apache2/ports.conf 是否有 Listen 443 埠號（port）

```
ssl@ubuntu:/etc/apache2$ more ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default

Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ssl@ubuntu:/etc/apache2$ _
```

(7) 修改 /etc/apache2/site-enabled 下的網站設定，加入以下內容(只要修改需要掛上憑證的網站)

<VirtualHost [your ip address]:443>

SSLEngine On

SSLCertificateFile /etc/ssl/webssl/<伺服器憑證>.crt 或.cer

SSLCertificateKeyFile /etc/ssl/webssl/server.key

SSLCertificateChainFile /etc/ssl/webssl/eCA_PublicCA.crt

ServerName www.test.com.tw:443

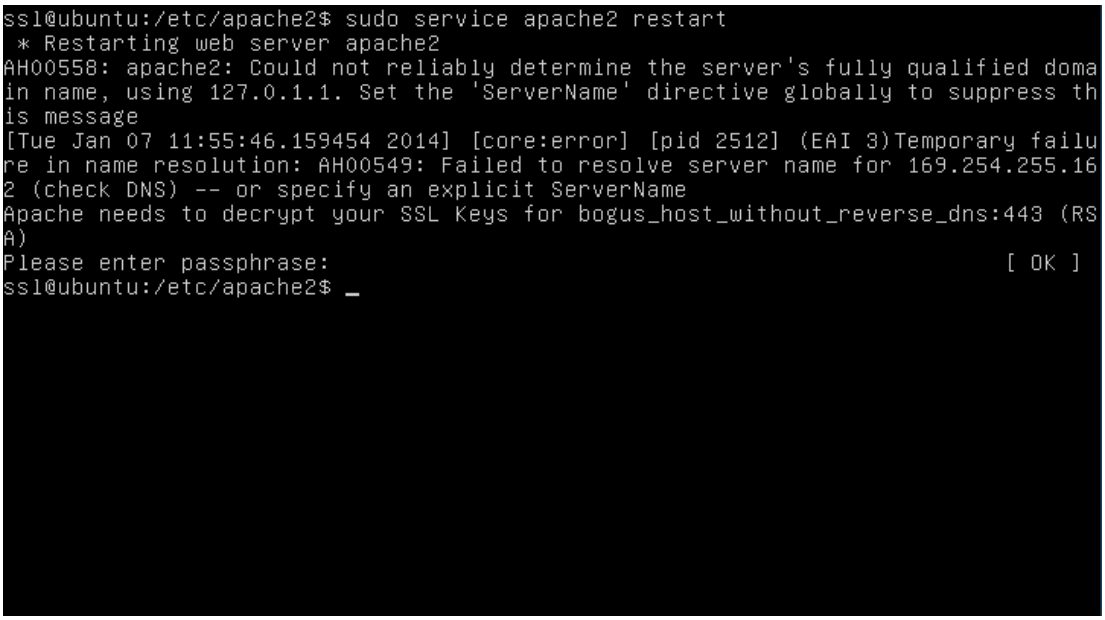
ServerAlias www.test.com.tw

DocumentRoot 網站的路徑，預設應該為 /var/www

</VirtualHost>

（8）重新啟動 apache

$ sudo service apache2 restart



重新啟動時，apache2 會要求輸入 server.key 的密碼。

（9）成功後，請以 https 連線試試 SSL 加密通道。

（10） 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

二、 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的 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的 SSL 憑證之狀態與資訊。

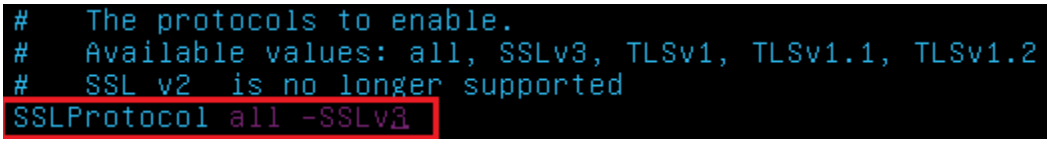
請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

附件一：設定 SSL 安全通道的加密強度

- Apache2 使用 OpenSSL 的加密套件來做資料加密，而 Apache2 加密套件的使用順序可在/etc/apache2/mods-enabled/ssl.conf 中的 SSLCipherSuite 找到。
- 預設值是「HIGH:MEDIUM:!aNULL:!MD5」，也就是高加密(HIGH encryption cipher suites，如 AES 256 bit)、中加密(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***」。
- 所以只要網站與客戶端瀏覽器兩端之密碼模組妥適搭配，即可支援最高等級之 256 位元對稱金鑰加密強度。

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。
- 請於/etc/apache2/mods-enabled/ssl.conf 中找到 SSLProtocol，並將"SSLProtocol all"改為"SSLProtcol all -SSLv3"，並重新啟動 Apache。



- 啟動完成後，使用可以測試工具（註 1、註 2）進行檢測，看 SSL3.0 是否已停用。

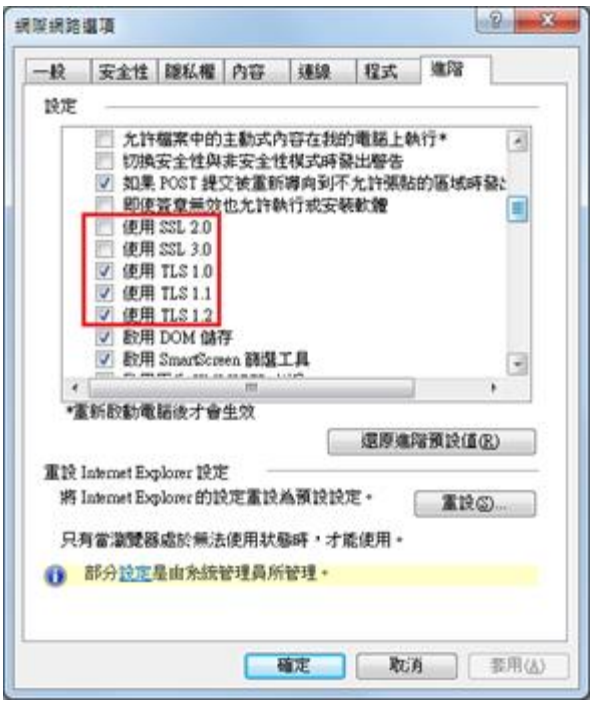
註 1:例如行政院國家資通安全會報技服中心網頁 http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh 有介紹兩種檢測伺服器端 SSL 協定的工具：(1) TestSSLServer（http://www.bolet.org/TestSSLServer/）(2) QUALYS SSL LABS SSL Server Test 檢測工具(https://www.ssllabs.com/ssltest/index.html, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定，因 2014 年 10 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/sslv3/browsers.html 之英文說明

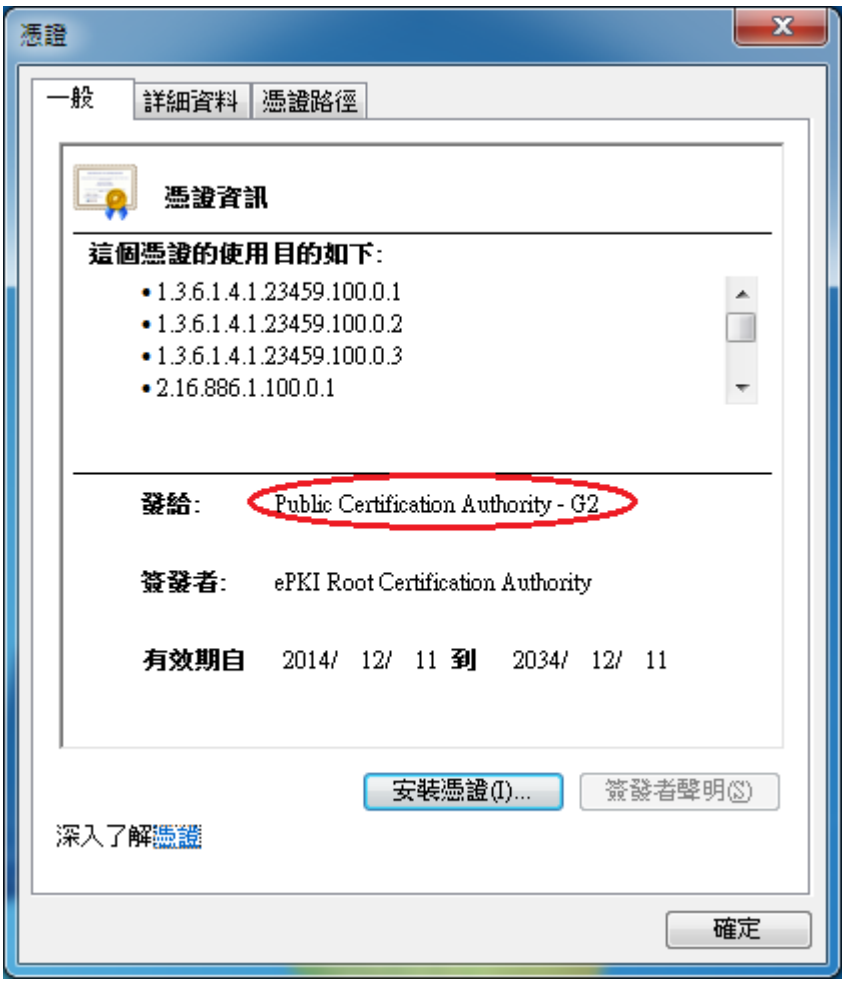
(2) 請超連結至 https://dev.ssllabs.com/ssltest/viewMyClient.html 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。

(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）

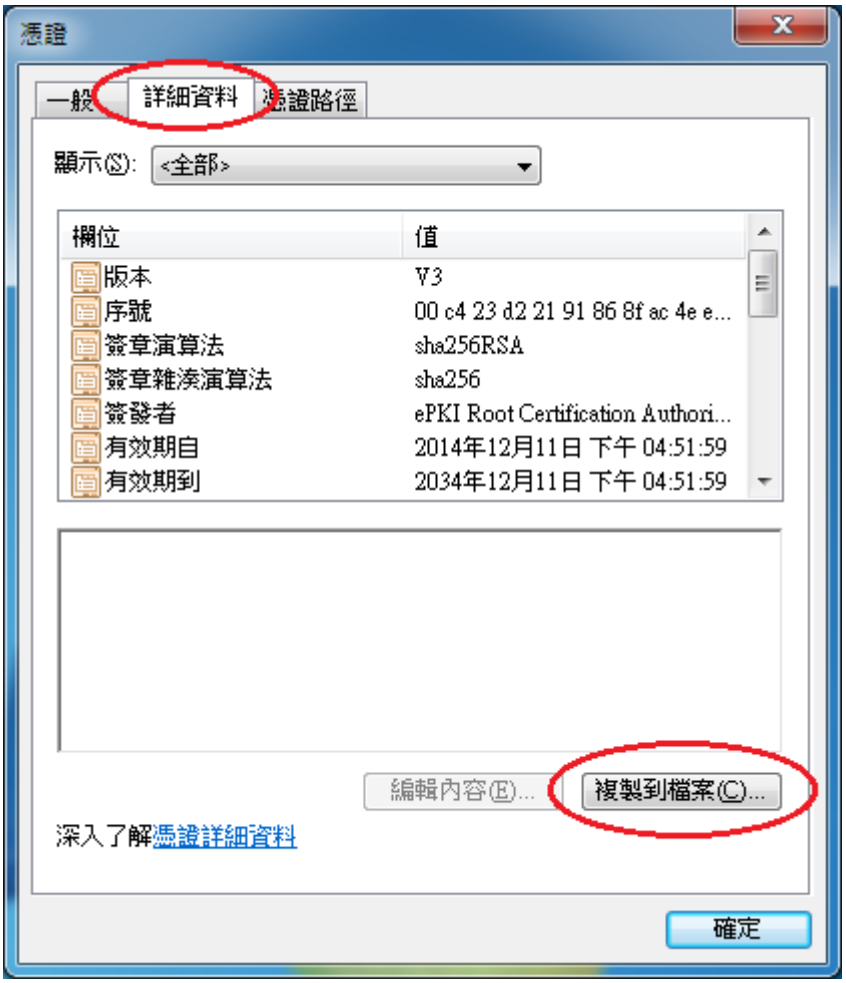

網際網路選項
一般
安全性
隱私權
內容
連線
程式
進階
設定
允許檔案中的主動式內容在我的電腦上執行*
切換安全性與非安全性模式時發出警告
如果 POST 提交被重新導向到不允許張貼的區域時發出
即使簽章無效也允許執行或安裝軟體
使用 SSL 2.0
使用 SSL 3.0
使用 TLS 1.0
使用 TLS 1.1
使用 TLS 1.2
啟用 DOM 儲存
啟用 SmartScreen 篩選工具
*重新啟動電腦後才會生效
還原進階預設值(R)
重設 Internet Explorer 設定
將 Internet Explorer 的設定重設為預設設定。
重設(S)...
只有當瀏覽器處於無法使用狀態時，才能使用。
部分設定是由系統管理員所管理。
確定
取消
套用(A)

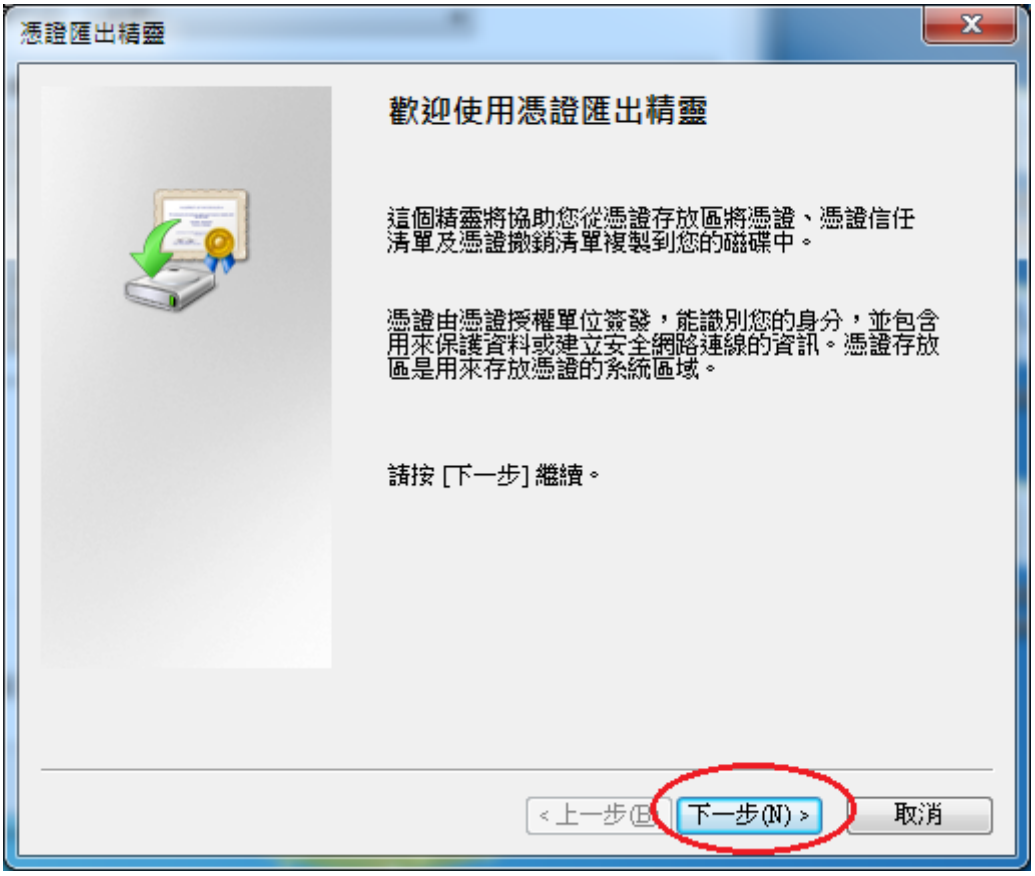
附件三：更換 SHA 256 憑證

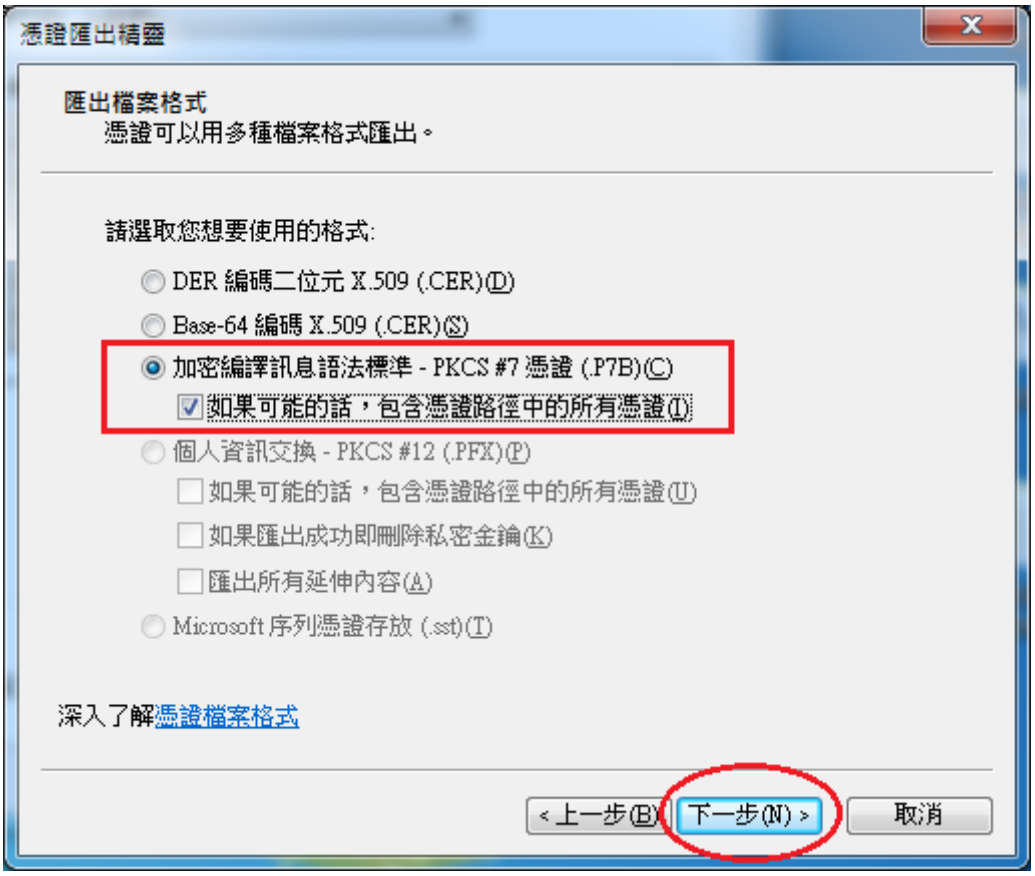
- 適用於申請時，有同時取得 SHA-1、SHA 256 憑證。或是憑證在效期內，經由審驗人員再次核發 SHA256 憑證者。
- 有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(https://publicca.hinet.net/SSL-08-06.htm)
- 點開「PublicCA2_64.crt」，並確認為「Public Certification Authority - G2」

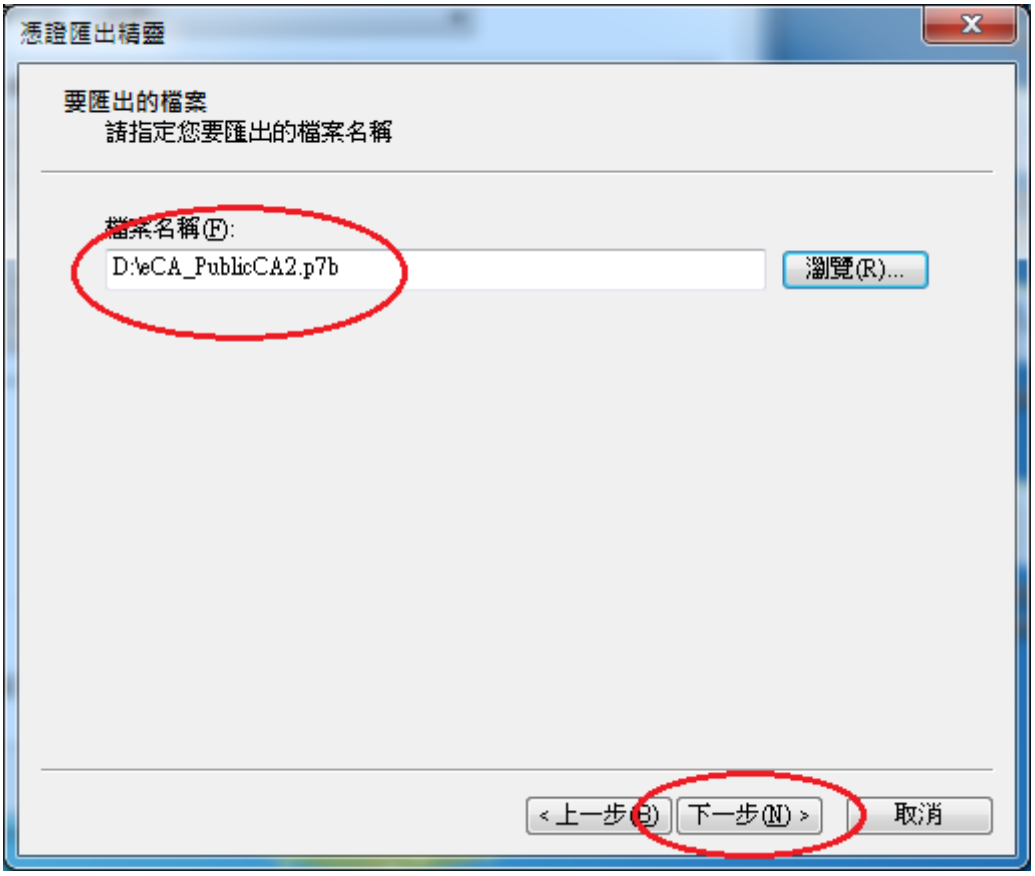


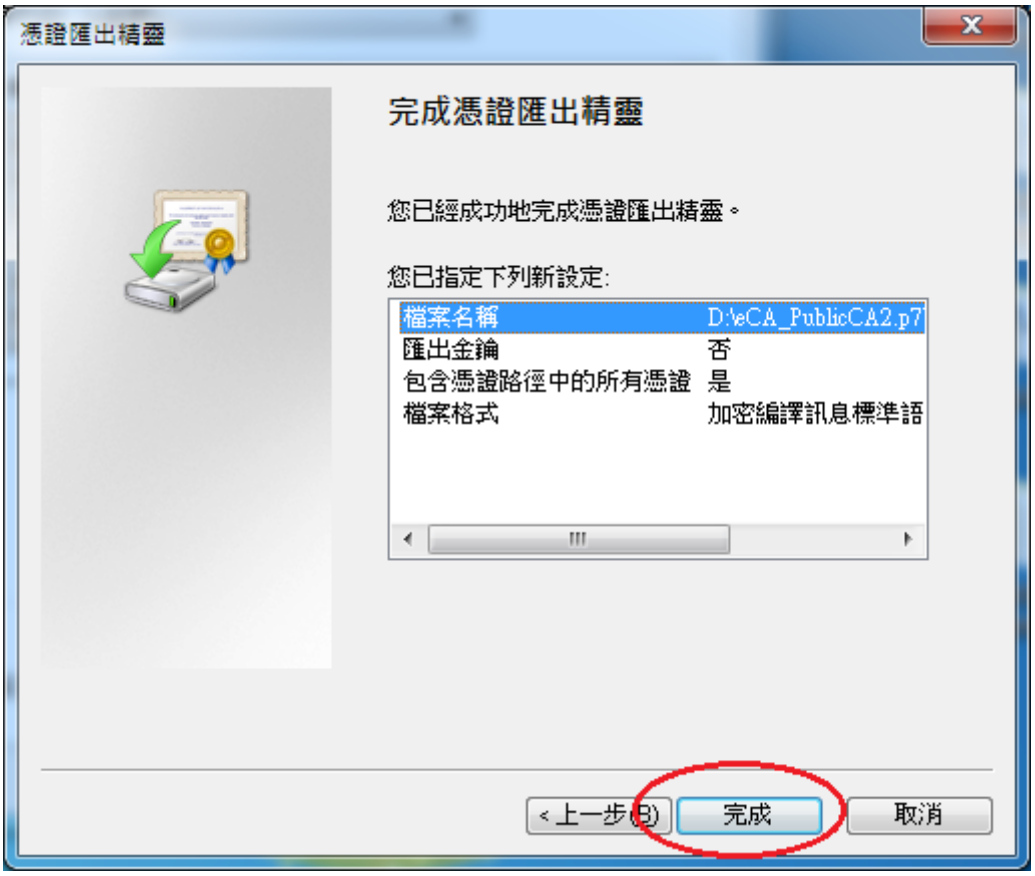
切換至「詳細資料」，點選「複製到檔案」

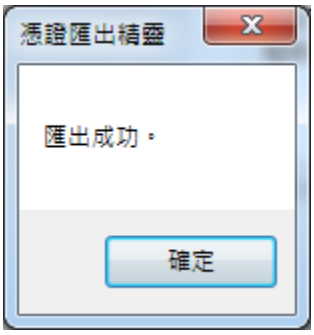

憑證
一般
詳細資料
憑證路徑
顯示(S):
<全部>
欄位
值
版本
V3
序號
00 c4 23 d2 21 91 86 8f ac 4e e...
簽章演算法
sha256RSA
簽章雜湊演算法
sha256
簽發者
ePKI Root Certification Authori...
有效期自
2014年12月11日 下午 04:51:59
有效期到
2034年12月11日 下午 04:51:59
編輯內容(E)...
複製到檔案(C)...
深入了解憑證詳細資料
確定


憑證匯出精靈
歡迎使用憑證匯出精靈
這個精靈將協助您從憑證存放區將憑證、憑證信任清單及憑證撤銷清單複製到您的磁碟中。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
請按 [下一步] 繼續。
< 上一步(B)
下一步(N) >
取消


憑證匯出精靈
匯出檔案格式
憑證可以用多種檔案格式匯出。
請選取您想要使用的格式:
DER 編碼二位元 X.509 (.CER)(D)
Base-64 編碼 X.509 (.CER)(S)
加密編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)
如果可能的話，包含憑證路徑中的所有憑證(I)
個人資訊交換 - PKCS #12 (.PFX)(P)
如果可能的話，包含憑證路徑中的所有憑證(U)
如果匯出成功即刪除私密金鑰(K)
匯出所有延伸內容(A)
Microsoft 序列憑證存放 (.sst)(T)
深入了解憑證檔案格式
< 上一步(B)
下一步(N) >
取消


憑證匯出精靈
要匯出的檔案
請指定您要匯出的檔案名稱
檔案名稱(F):
D:\eCA_PublicCA2.p7b
瀏覽(R)...
< 上一步(B)
下一步(N) >
取消


憑證匯出精靈
完成憑證匯出精靈
您已經成功地完成憑證匯出精靈。
您已指定下列新設定:
檔案名稱 D:\eCA_PublicCA2.p7
匯出金鑰 否
包含憑證路徑中的所有憑證 是
檔案格式 加密編譯訊息標準語
< 上一步(B)
完成
取消



- 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 /etc/apache2/site-enabled 下的參數設定
  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