

中華電信通用憑證管理中心

Apache 伺服器 SSL 伺服器軟體憑證安裝說明

本說明書適用於 Apache+mod_ssl 環境下之 SSL 伺服器軟體憑證安裝，並假設 Apache Server 係執行於 Unix like 的平台上(例如:Linux)。本說明書的安裝程序，已經在 Apache_1.3.29 及 mod_ssl 2.8.18 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。

以下為 Apache+mod_ssl 環境下之 SSL 伺服器軟體憑證安裝程序，整個安裝程序包含四個部份：

- 一、取得 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈
- 二、安裝 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈
- 三、安裝 SSL 伺服器軟體憑證
- 四、散佈 eCA 自簽憑證到 Web 用戶端

一、取得 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈

當您向 PublicCA 申請的 SSL 伺服器軟體憑證經核准並簽發之後，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 憑證之憑證串鏈，並在 Apache Server 上安裝 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈，使您的 Apache Server 信賴 eCA 及 PublicCA 的憑證，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 PublicCA 憑證之憑證串鏈，則您可以跳過此取得 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈及下一階段的安裝 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈的步驟，直接進行 SSL 伺服器應用軟體憑證的安裝。

安全取得 eCA 自簽憑證及 PublicCA 憑證之憑證串鏈的步驟如下：（註：以下步驟必須在 Windows 平台上使用 IE 瀏覽器來進行

1、登入 Windows 系統。

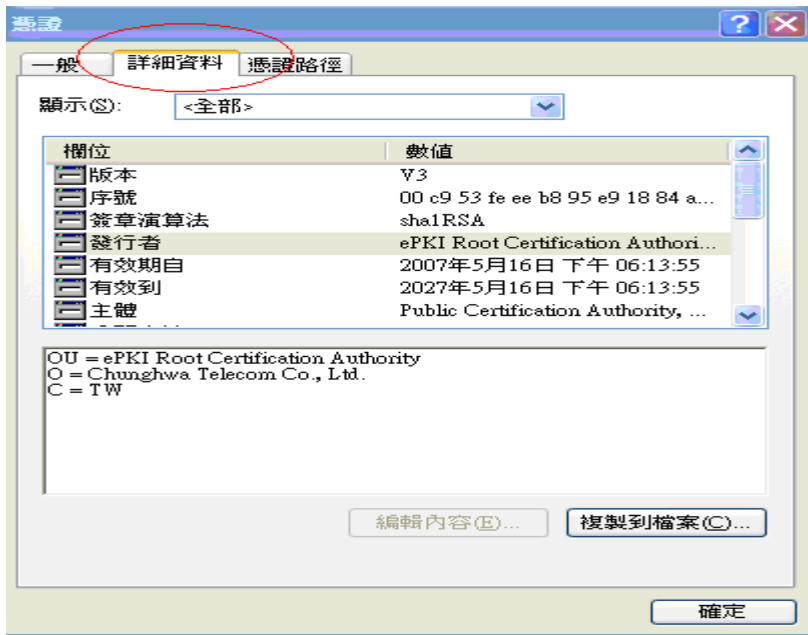
（註：如果您使用的 Windows 系統為 Windows 2000、Windows XP、Windows 2003 或以上版本，則必須使用具有 Administrator 權限帳號登入）

2、打開 IE 瀏覽器，並連線到 [PublicCA 網站](#)，下載 PublicCA 憑證，並存檔。

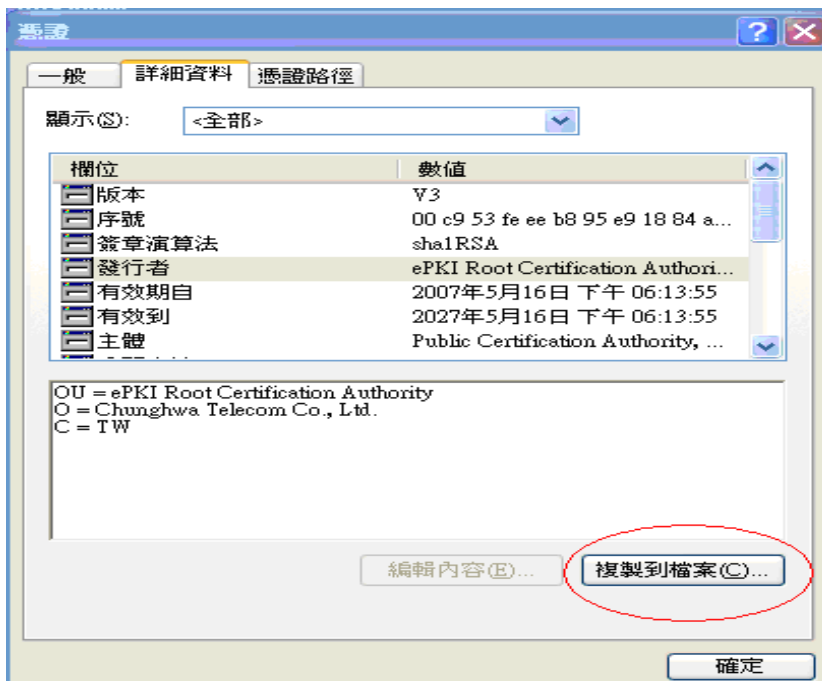
3、打開您剛儲存的資料匣，然後打開剛存的 PublicCA.cer。



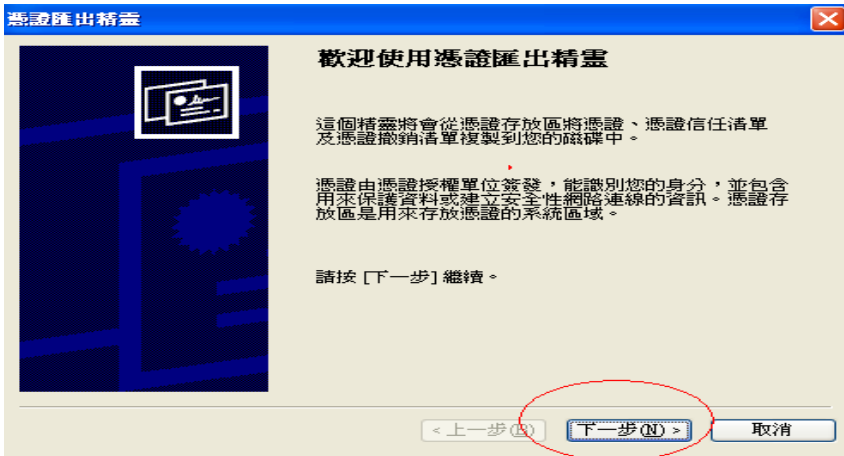
4、出現以下憑證檢視的畫面，請點選「詳細資料」。



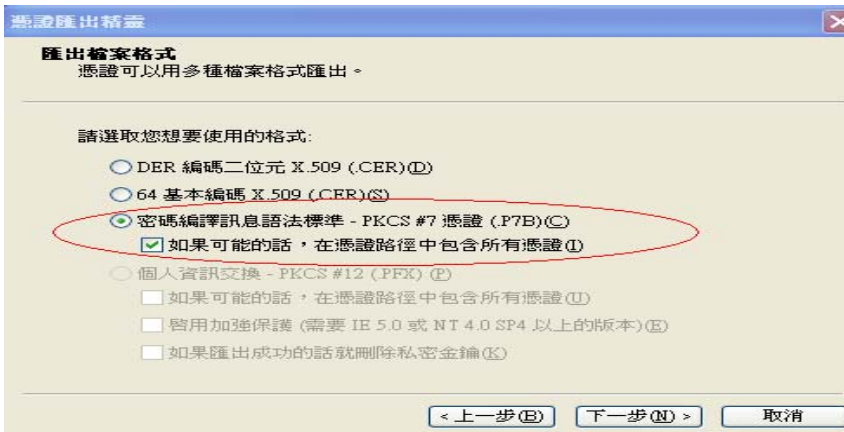
5、出現以下憑證詳細資料的畫面，請點選「複製到檔案」。



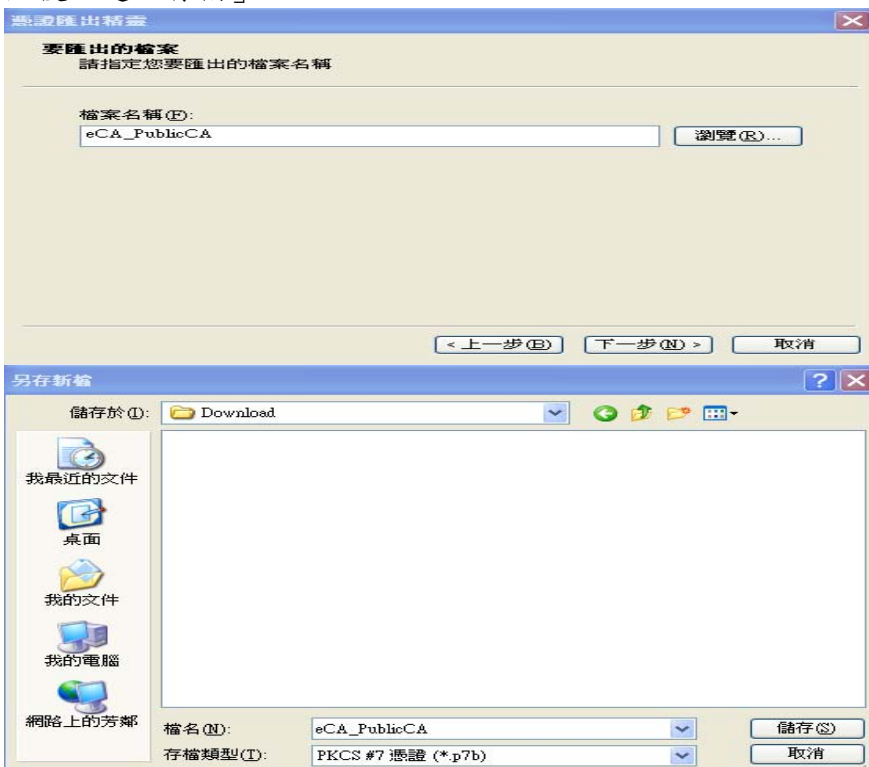
6、出現以下憑證匯出精靈的畫面，請點選「下一步」。



7、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」。



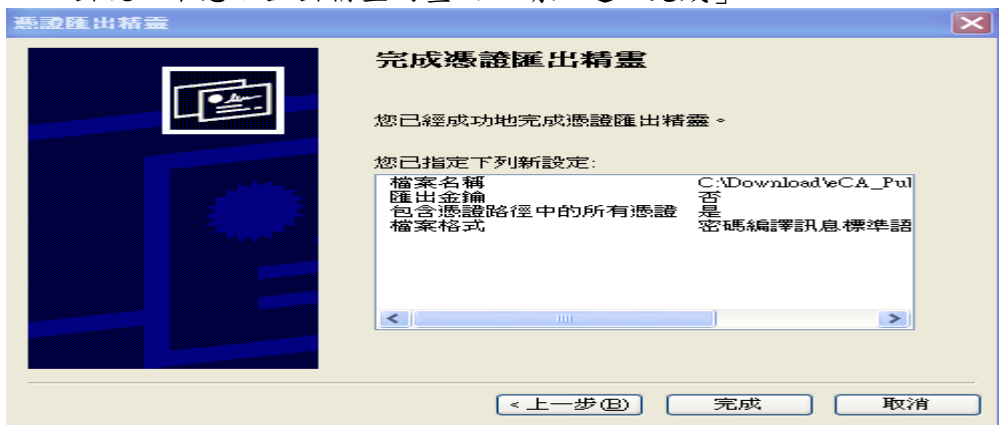
8、出現以下另存新檔的畫面，請選擇適當的資料夾位置，檔案名稱請輸入「eCA_PublicCA」，然後點選「存檔」。



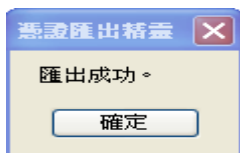
9、出現以下憑證匯出精靈的畫面，請點選「下一步」。



10、出現以下憑證匯出精靈的畫面，請點選「完成」。



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



二、安裝eCA自簽憑證及PublicCA憑證之憑證串鏈

接下來要在Apache Server上安裝eCA自簽憑證及PublicCA憑證之憑證串鏈，使您的Apache Server信賴eCA及PublicCA的憑證。步驟如下：

12、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)

13、把您在上一階段取得的eCA自簽憑證及PublicCA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。

14、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）：
（註：以下%符號表示Shell的prompt，不是命令的一部分）

```
% openssl pkcs7 -in eCA_PublicCA.p7b -inform DER -print_certs -out eCA_PublicCA.pem
```

15、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，您可能想要先將舊檔案備份起來，以防萬一。）

16、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。）

17、記得儲存編輯後的組態設定檔。

三、安裝SSL伺服器軟體憑證

18、接下要把安裝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：

19、請確定您已完成憑證接受作業，並下載儲存已簽發之SSL伺服器軟體憑證(*.cer)。
（註：以下步驟假設您下載之SSL伺服器軟體憑證的檔名已經被改名為server.cer，如果您並非使用這個檔名，則您應該自行調整下面的步驟。）

20、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）

21、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（即Base64編碼格式）（註：以下%符號表示Shell的prompt，不是命令的一部分）
% openssl x509 -in server.cer -inform DER -out server.pem

22、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1：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。)

23、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簽發請求CSR檔的同一個金鑰，否則將無法成功建立SSL連線。)

24、記得儲存編輯後的組態設定檔。

25、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
```

四、散佈eCA自簽憑證到Web用戶端

用戶端如果是 Windows XP，不必安裝任何憑證，只要用戶端可以連線到 Internet，則 Windows XP 會自動去微軟取得 eCA 憑證。

用戶端如果是 Windows 2000(含)以前的系統，則需要安裝 eCA 憑證。步驟如下：

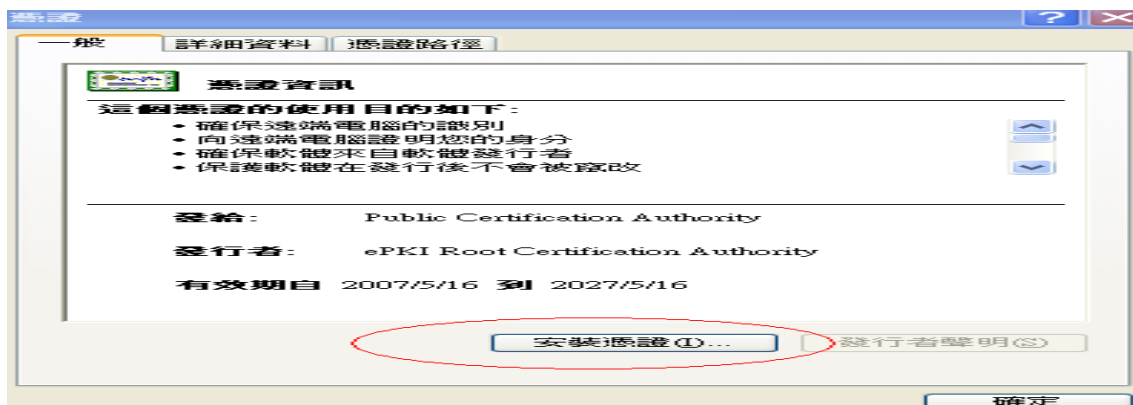
1、下載 eCA 自簽憑證



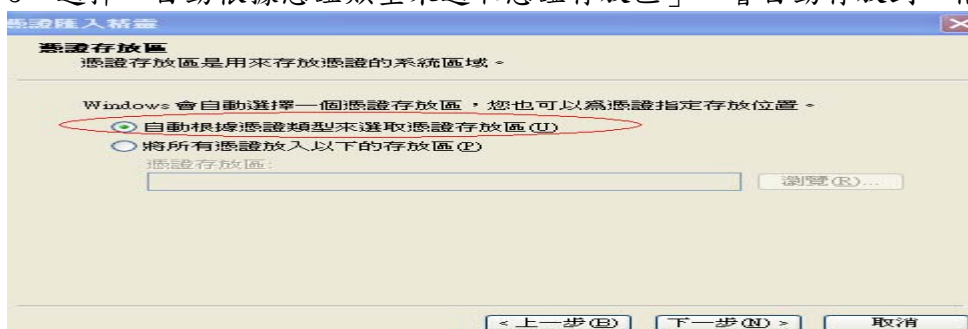
The screenshot shows a web browser window with the address bar displaying "http://epki.com.tw/repository.htm". The page title is "中華電信公開金鑰基礎建設" (China Telecom Public Key Infrastructure). The main content area features a navigation bar with "eCA", "CHTCA", "PublicCA", "PKI安全保密產品", and "儲存庫". Below the navigation bar, there is a table with the following content:

檔案下載	備註	檔案格式
eCA憑證下載	中華電信憑證總管理中心(eCA)，自身憑證下載	CER
eCA憑證廢止清冊	eCA憑證廢止清冊(CARL)公布，提供信賴憑證者檢驗憑證之憑證狀態	CRL

2、打開 ROOTeCA.cer → 「安裝憑證」



3、選擇「自動根據憑證類型來選取憑證存放區」，會自動存放到「信任的根憑證授權」



4、完成匯入



或用戶可以連線到 Windows Update 網站更新 Root CA 憑證，即會自動安裝 eCA 憑證。