SSL 伺服器數位憑證 IIS 6.0
伺服器操作手冊

台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

機密等級：公開
版本：V3.0
文件編號：MNT-03-071
生效日期： 2005 年 11 月 14 日

目　　錄

1.目的

1.1. 主要介紹 SSL 伺服器數位憑證 IIS 6.0 伺服器之憑證申請檔產製步驟及憑證安裝說明。

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。

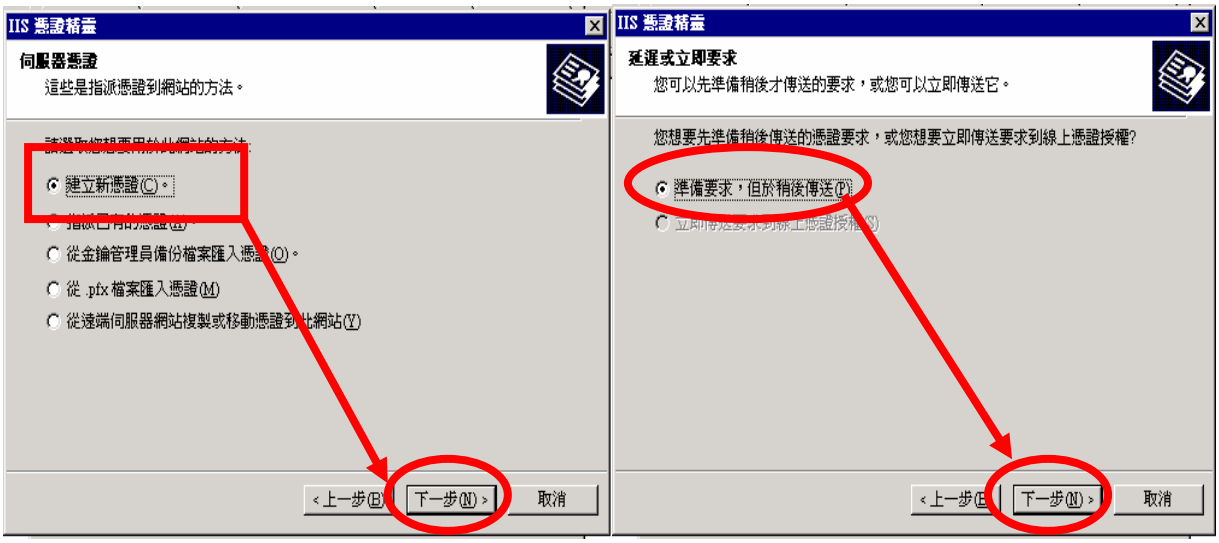
4.作業程序

4.1 如何產生「憑證申請檔(CSR)」？

※在產生的過程中，所有需要填入的資料，請務必以英文方式填寫！

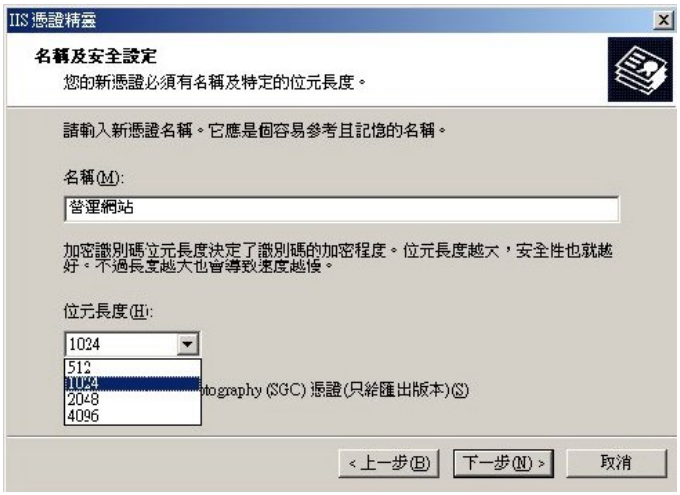
4.1.1「開始」→「程式集」→「系統管理員」→「網際網路資訊服務(IIS)管理員」畫面中在欲執行 SSL 模式的站臺上按右鍵→「內容」→「目錄安全設定」→「伺服器憑證」，以啟始 Web 伺服器憑證精靈→「下一步」。

4.1.2 準備產生憑證請求檔，「建立新憑證」→「下一步」→「準備要求，但稍後傳送」→「下一步」。



4.1.3 輸入憑證資訊

4.1.3.1 名稱：出現在憑證管理清單中的名稱，填入較有意義之文字，需以英文方式填寫！位元長度：**若要申請 40 位元 SSL 憑證，請選擇 512；若要申請 128 位元 SSL 憑證，則選擇 1024。**

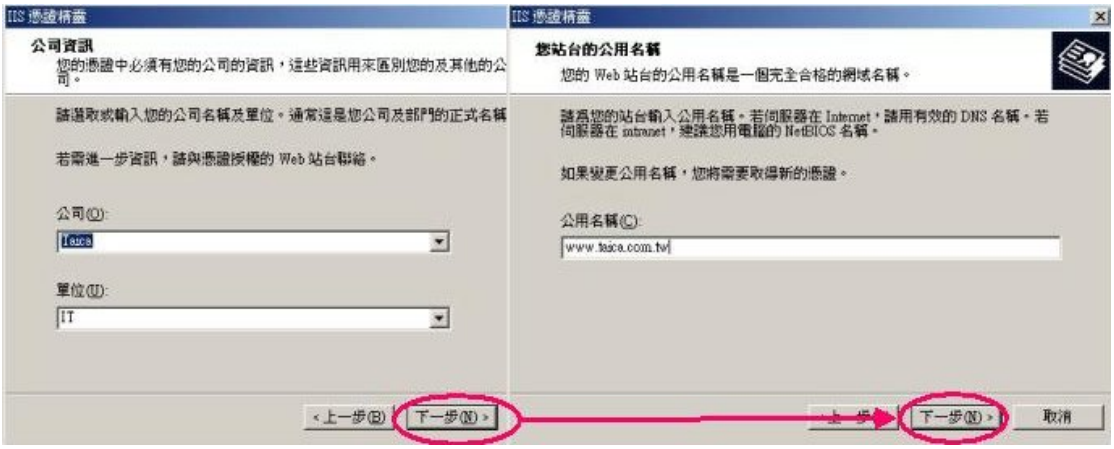


4.1.3.2 以下三個欄位將會出現在憑證內容之中，請慎填！各欄位說明如下：

公司：公司名稱，需以英文方式填寫！。(如：TWCA)

單位：使用該憑證之單位名稱，需以英文方式填寫！(如：IT)

公用名稱：網站名稱(如：www.taica.com.tw) ，即申請同意書上之 Common Name 欄位內容！

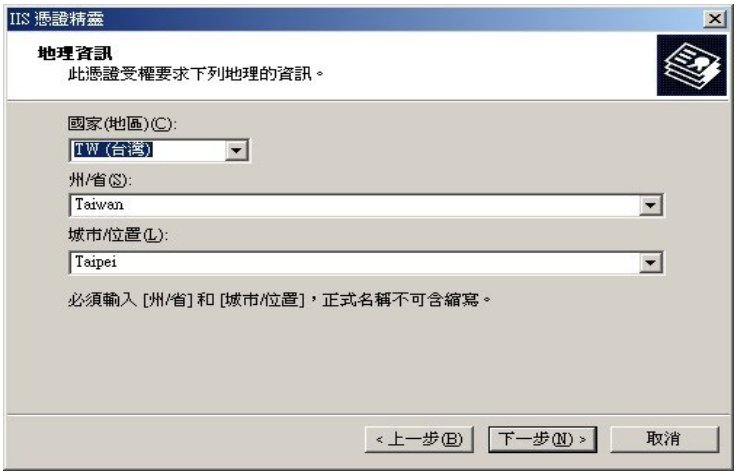


4.1.3.3 以下三個欄位亦會出現在憑證內容之中，請慎填！各欄位說明如下：

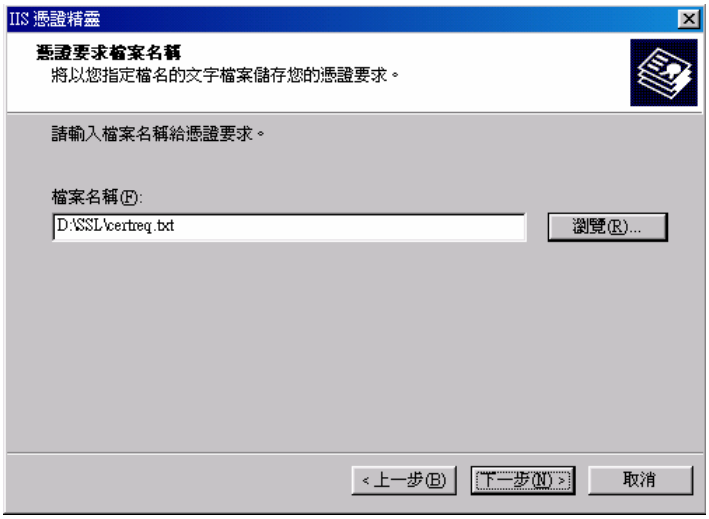
國家／區域：兩碼之國碼，需以英文方式填寫！（如：臺灣為 TW）

州／省：國家全名，需以英文方式填寫！（如： Taiwan）

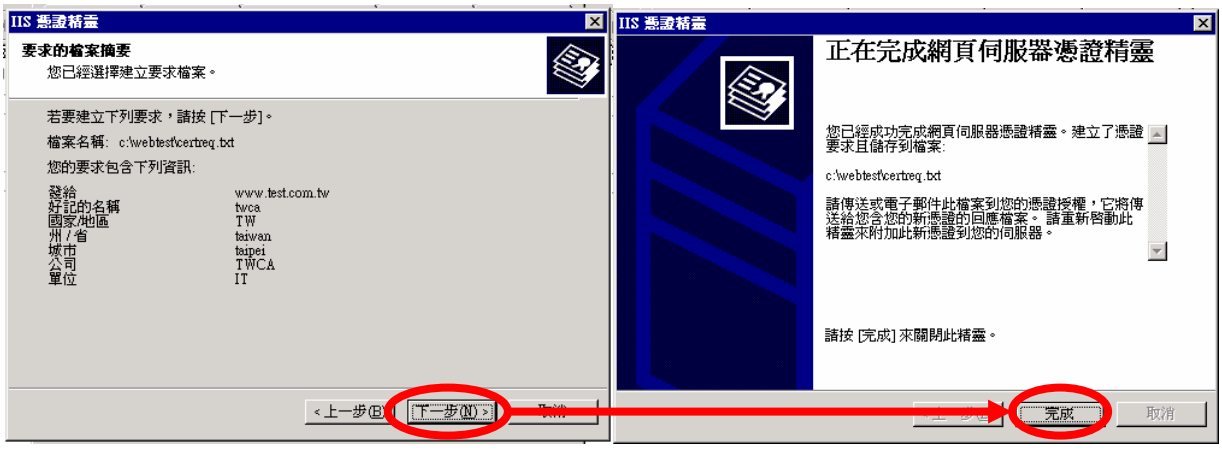
城市／位置：城市全名，需以英文方式填寫！（如： Taipei）



4.1.3.4 指定執行出之憑證申請檔(CSR)檔案存放路徑。(如：D:\SSL\certreq.txt)



4.1.3.5 伺服器憑證精靈會將前幾個步驟所設定的憑證申請檔內容,供使用者再次確認設定內容。**請先確認畫面所列出之內容是否皆為英文方式書寫且正確無誤**→「下一步」→「完成」。



4.1.3.6 完成之憑證請求檔內容如下。

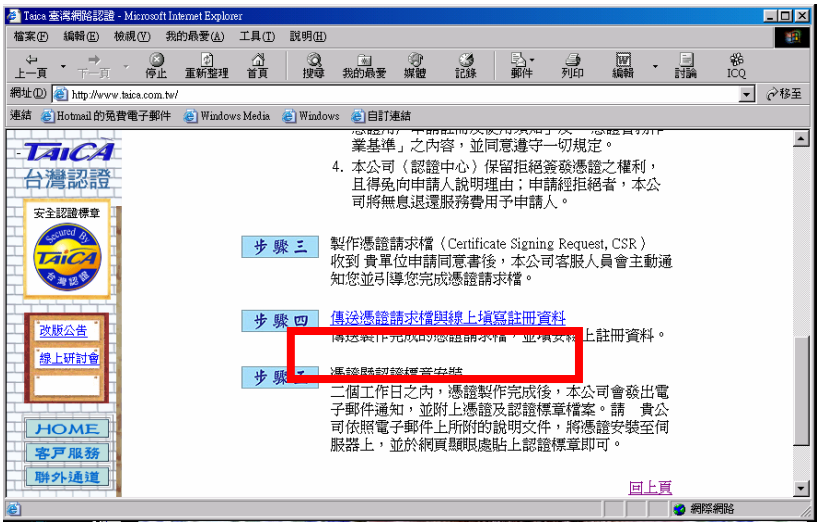

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDAjCCAmsCAQAwbTEWMBQGA1UEAxMNMTkyLjE2OC4wLjEwMjEUMBIGA1UECxML
SVRMZW9uIFR1c3QxDjAMBgNVBAoTBUVRhaWNhMQ8wDQYDVQQHEwZUYW1wZWkxDzAN
BgNVBAgTB1RhaXdhbjELMAkGA1UEBhMCVFcwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAKNXzRByH5zCa8vN1/bd47VaxAD68DVV8CDMTYh7SBXZBue0Cs3Hv+Fo
rflHMQEd2cjm/bKvRjKk/LrGXAYHDrLBXJtLrgDi7rjXn+C6Z31dPEbUWvWnLw3t
KeX5H8wa6aaIC2ApEVA+z07QOBIZGeeilie14DUBb4JUXe6wZIYrAgMBAAGgggFT
MBoGCisGAQQBgjcNAgMxDBYKNS4wLjIxOTUuMjA1BgorBgEEAYI3AgEOMScwJTAO
BgNVHQ8BAf8EBAMCBPAwEwYDVR01BAwwCgYIKwYBBQUHAwEwgf0GCisGAQQBgjcN
AgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgA
YQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYA
aQBkAGUAcgOBiQAgdwtIPabCtP1fjfzHtSbBt/b6Jwj0AXTsDaesxyUjwlNxcENE
oBaREDcuhxJ+/SNAjK1Pd6vR4dU0LXdmFOpVh0Lp16yHMrZgBUY4YmzV+g6dXuNU
o3NjeIpScstRhbLOvOnHWbdhj+stOCO+Pzr5Ftln/Z3s1KzKxEjNjz+AdQAAAAAA
AAAAMA0GCSqGSIb3DQEBBQUAA4GBAFikYzMbPOb/vz+NTOEll8+GixDF1qQx5VF6
t1wBDLL58I3U+knb6bEfa4NVQSvW6QfkEDC62mY71e5hhVhjjzAUWtz2dDdaWdWK
OK8hexLEuTxQJObqrDDPa1xcyXJT41unl/sZ+TRfjNO1EBPJ104bJl1C/gzSUMzJ
iAWYzlKa
-----END NEW CERTIFICATE REQUEST-----
```


4.2 如何將製作好的憑證申請檔(CSR)上傳？

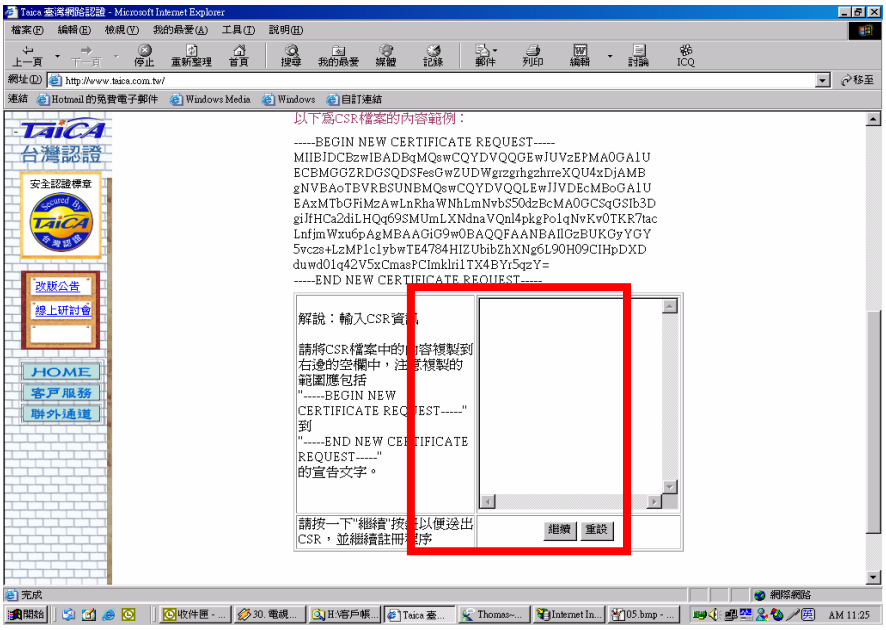
4.2.1 連接至本公司首頁 http://www.twca.com.tw。

4.2.2 點選「SSL 伺服器憑證」→「憑證申請」→「憑證申請」。

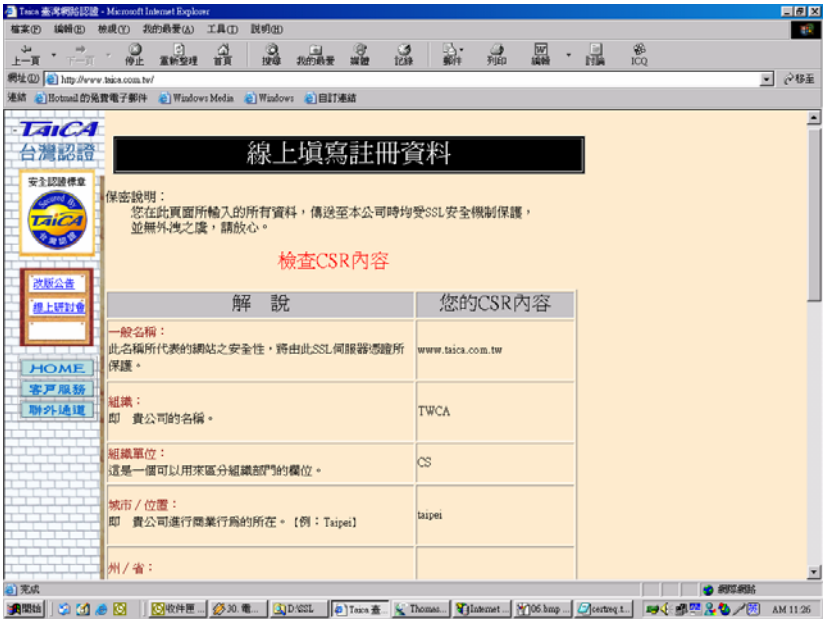
4.2.3 選擇「步驟四 傳送憑證請求檔與線上填寫註冊資料」



4.2.4 用複製貼上的方式，將製作好之憑證申請檔(CSR)內容貼到申請欄位中→選擇「繼續」。



4.2.5 再次檢視上傳之憑證申請檔案內容。



4.2.6 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)。

4.3 下載已核發憑證作業

4.3.1 若上傳之 CSR 及相關聯絡資料經過審驗通過,將會由系統自動發送伺服器憑證下載通知給相關聯絡人。其中技術聯絡人所收到的通知含有憑證檔案及安全標章之附檔及安裝說明：

※ ServerCert.crt →伺服器憑證檔。

※ TaiCASecureCA_Prod.crt（或 EntrustCA_Prod.crt）→中繼憑證檔。

※ mark1.gif、mark2.gif、mark3.gif →認證標章圖形檔。

※ 請確實將伺服器憑證檔及中繼憑證檔安裝於伺服器中。

4.3.2 若因為貴公司之 mail server 設定，導致無法順利取得附件之憑證檔案，請依照下列步驟，下載相關檔案。

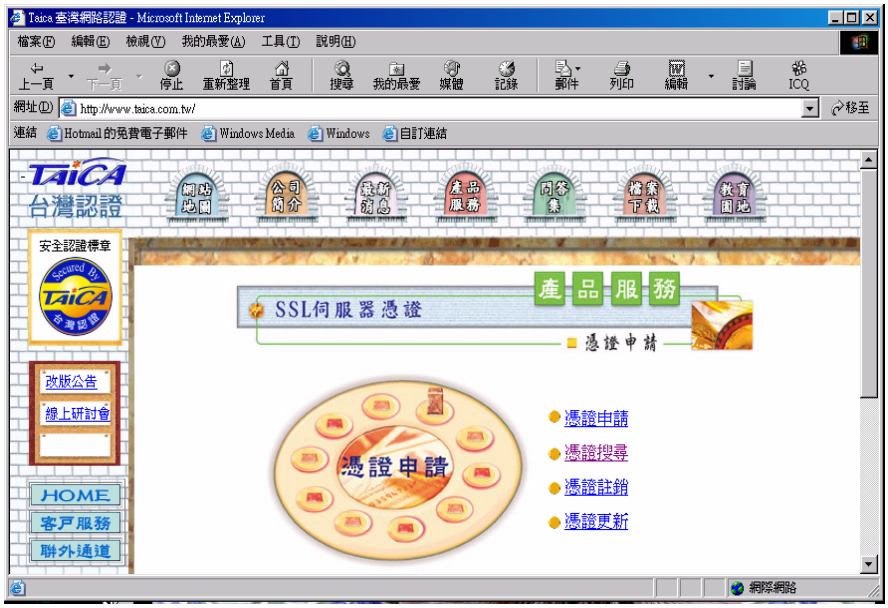
4.3.3 下載伺服器憑證：

4.3.3.1 先連至本公司首頁 (http://www.twca.com.tw)。

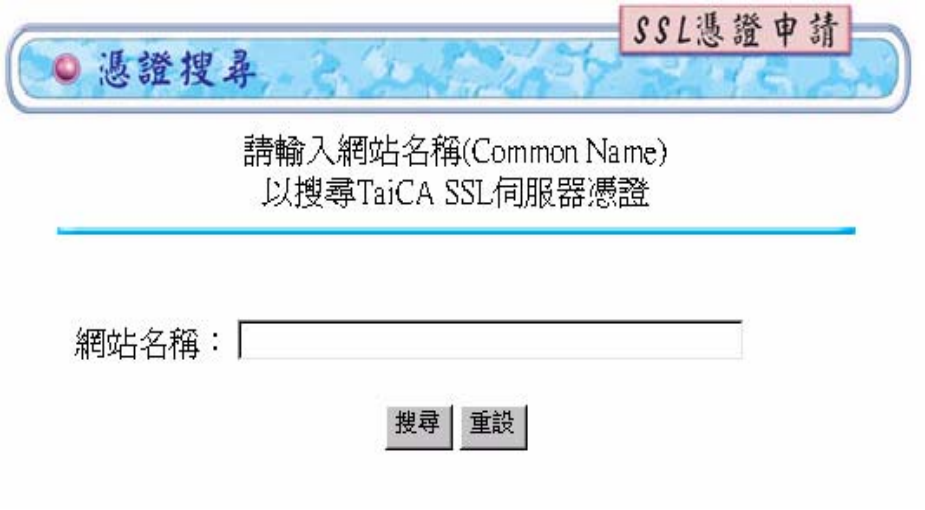
4.3.3.2 點選 SSL 伺服器憑證。

4.3.3.3 點選 憑證申請。

4.3.3.4 點選 憑證搜尋。



4.3.3.5 輸入申請之 DNS 位址填寫當初所申請的憑證之網站名稱，如 www.abc.com.tw (注意，大小寫需一致)，輸入完成後，按下搜尋鍵



4.3.3.6 點選 下載憑證。

4.3.4 下載中繼憑證。

下載網址：https://ssl.taica.com.tw/cacert/taicasecureca_prod.crt

4.3.5 安裝安全認證標章，認證標章(mark1.gif, mark2.gif, mark3.gif)：(請依貴公司需求選擇適合之圖檔)。

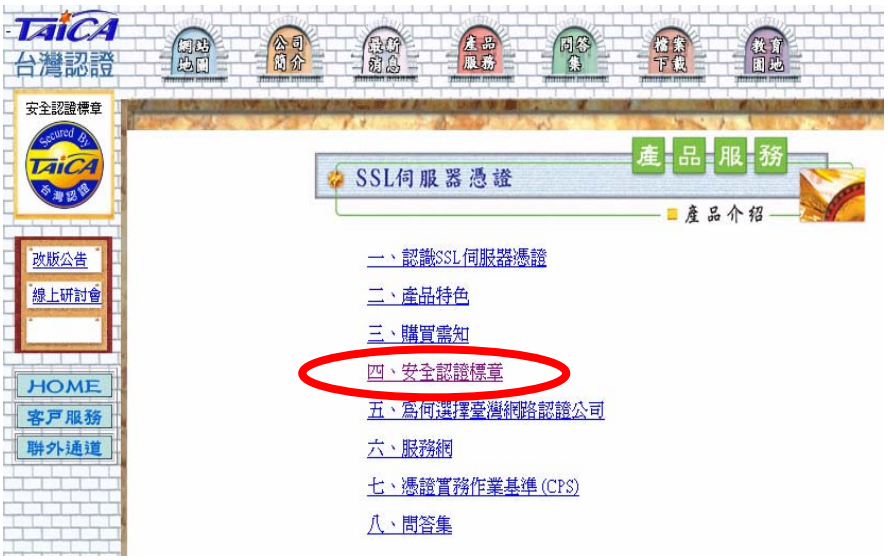
4.3.5.1 先連至本公司首頁（http://www.twca.com.tw ）。

4.3.5.2 點選 產品服務。

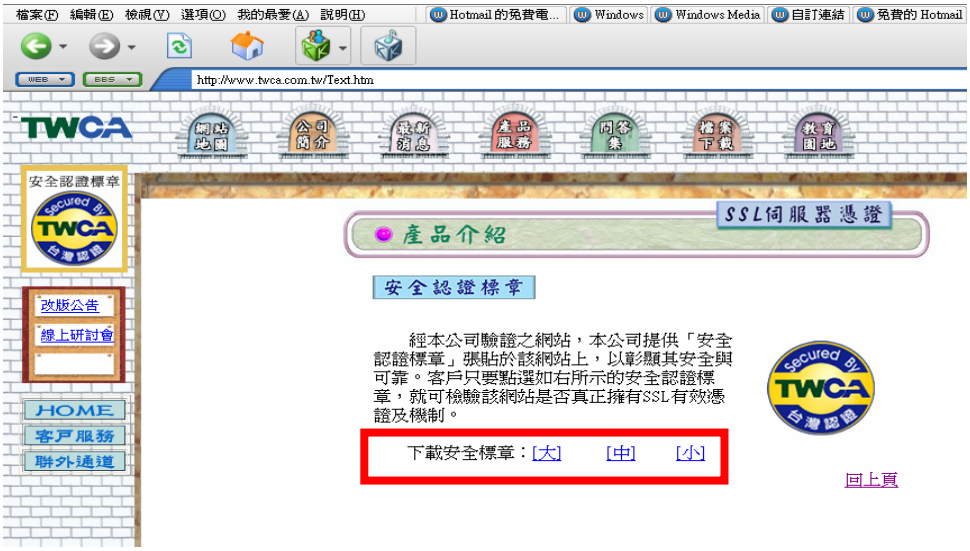
4.3.5.3 點選 SSL 伺服器憑證。

4.3.5.4 點選 產品介紹。

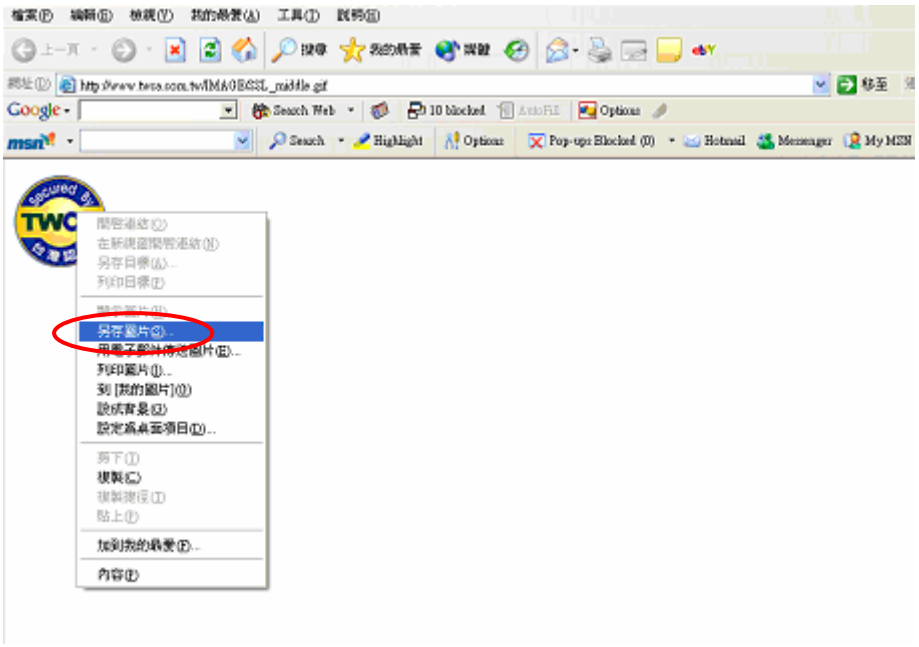
4.3.5.5 點選　四、安全認證標章。



4.3.5.6 請依貴公司需求選擇適合之圖檔規格。



4.3.5.7 按滑鼠右鍵 →選 另存圖片。



4.3.5.8請在 貴公司的網頁上加上本公司認證標章及以下超連結語法，以便讓使用者查詢 貴公司憑證狀態

<A target=new href="https://ssl.taica.com.tw/servlet/ShowServerCertInfo?DNS=申請之DNS位址 ">

<img src="/mark.gif" tppabs="/mark.gif" border="0">

</A>

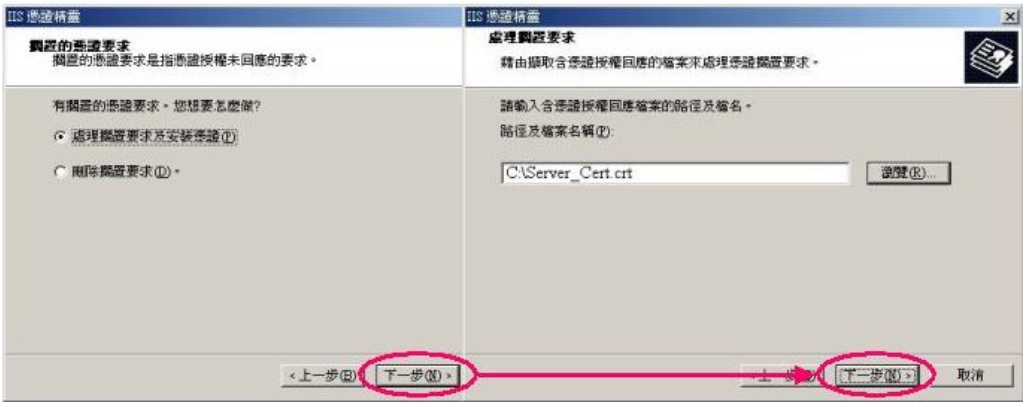
其中 src="/mark.gif"這一段，請依 貴公司的狀況調整路徑名

4.4 如何安裝自我憑證？

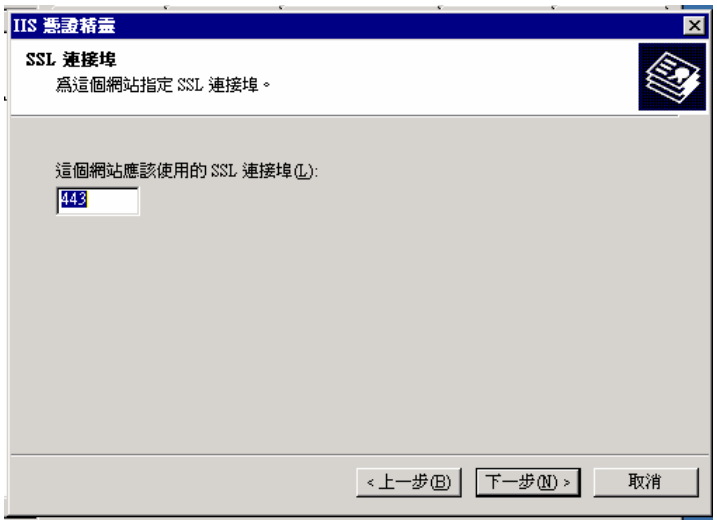
4.4.1 請先將自 CA 取得的自我憑證檔(ServerCert.crt)儲存於硬碟中。

4.4.2 使用憑證精靈，將伺服器憑證匯入「網際網路資訊服務(IIS)管理員」畫面中在欲執行 SSL 模式的站臺上按右鍵→「內容」→「目錄安全設定」→「伺服器憑證」，以啟始網頁伺服器憑證精靈→「下一步」。

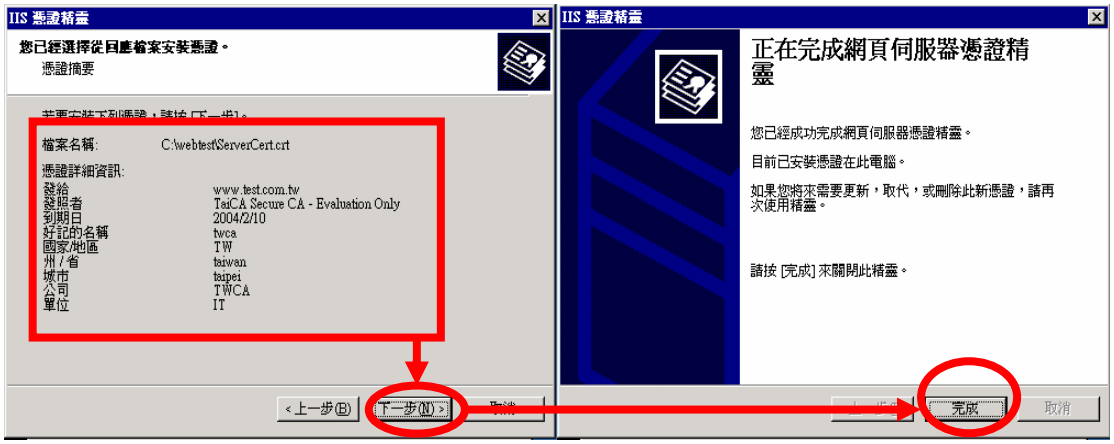
4.4.3「處理擱置要求及安裝憑證」→「下一步」→指定到取得的Server_Cert.crt檔案→「下一步」。



4.4.4 請先設定 SSL 連接埠為 443 →「下一步」。



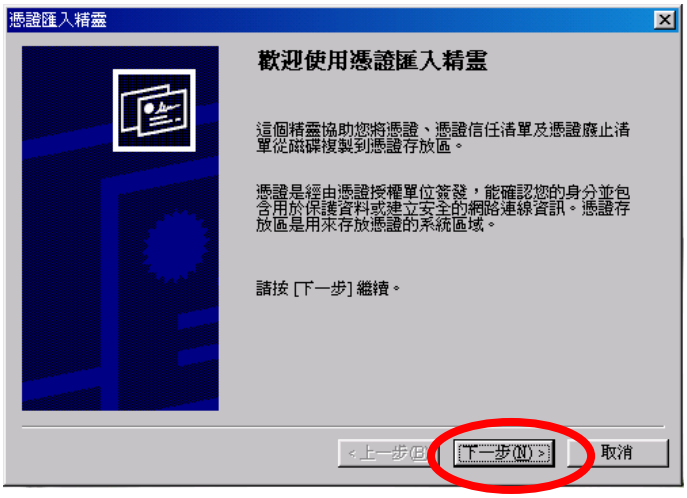
4.4.5 **請先確認畫面所列出之內容是否為提出申請憑證之內容**→「下一步」→「完成」。



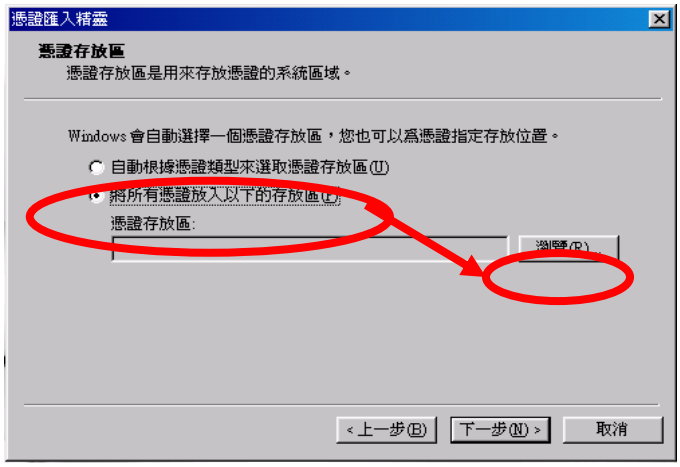
4.5 如何安裝中繼憑證？

4.5.1 將臺灣網路認證公司的憑證(TaiCASecureCA_Prod.crt)儲存於硬碟中，使用檔案總管尋找到儲存的檔案，選擇此憑證檔案按滑鼠右鍵，選擇「安裝憑證」。

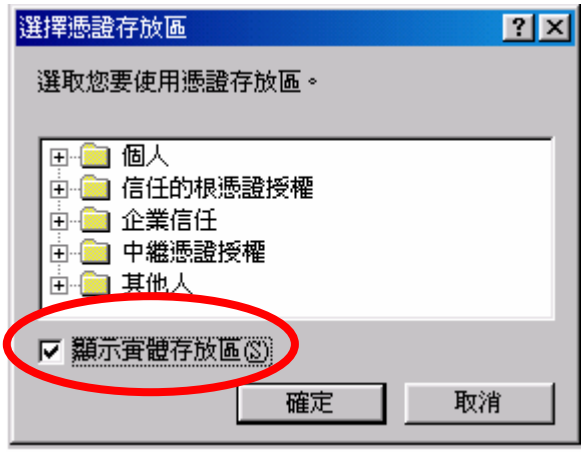
4.5.2 將出現使用憑證匯入精靈的畫面，請選擇「下一步」。



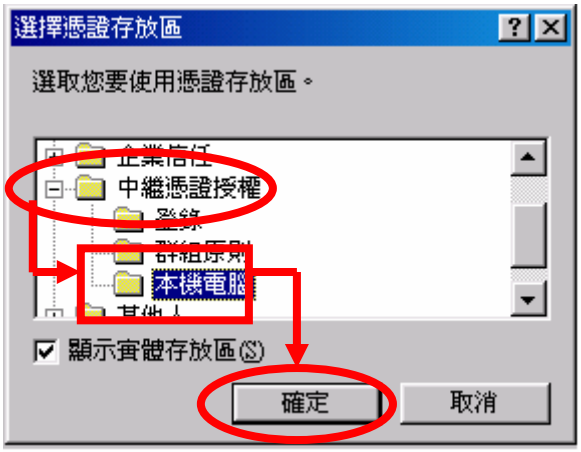
4.5.3「將所有憑證放入以下的存放區」→「瀏覽」。



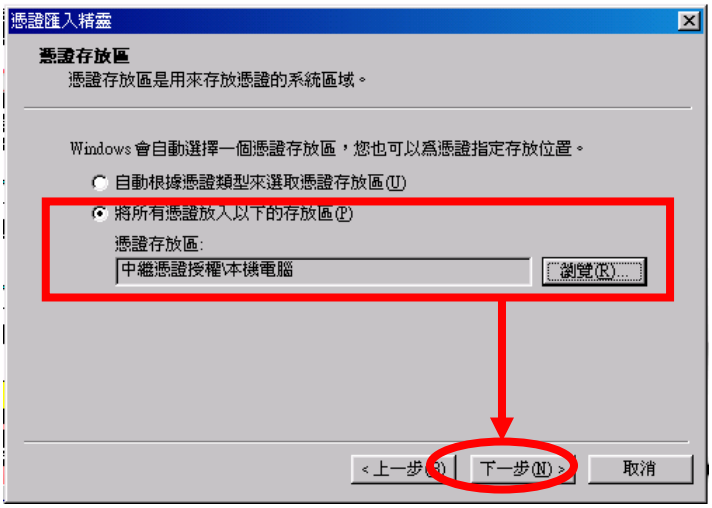
4.5.4 勾選「顯示實體存放區」。



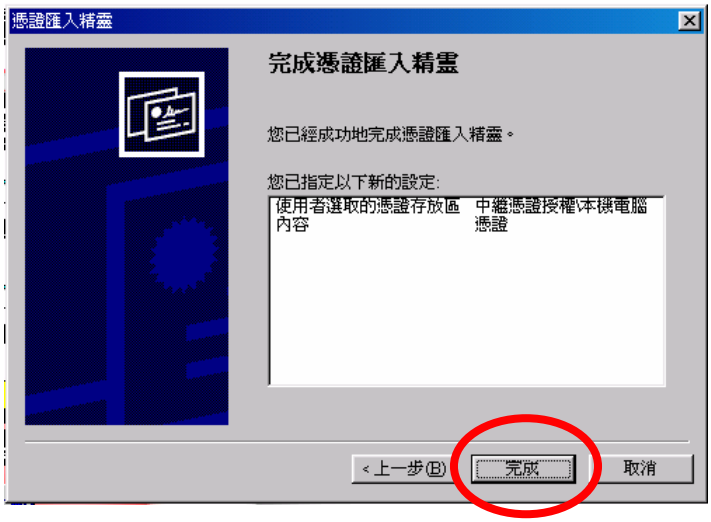
4.5.5 點選並開啟「中繼憑證授權」→「本機電腦」→「確定」。



4.5.6 點選「下一步」。



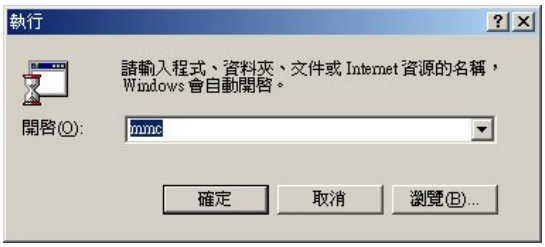
4.5.7 點選「完成」。



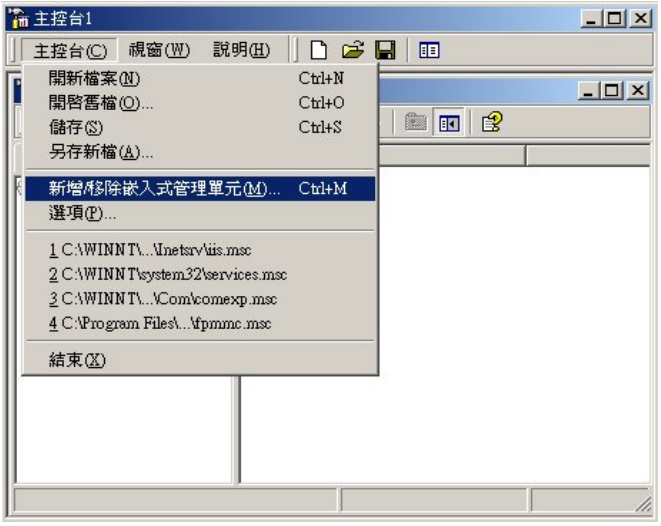
4.5.8 完成畫面。

4.6 如何備份憑證(匯出)?

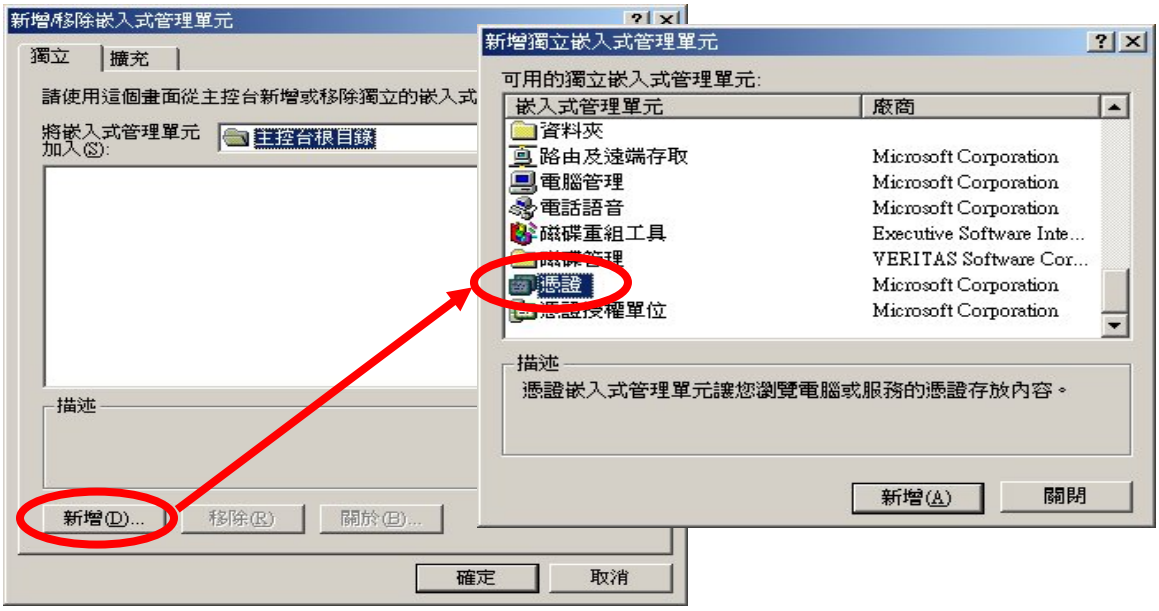
4.6.1 由「開始」→「執行」→開啟 MMC ，執行「主控台」。



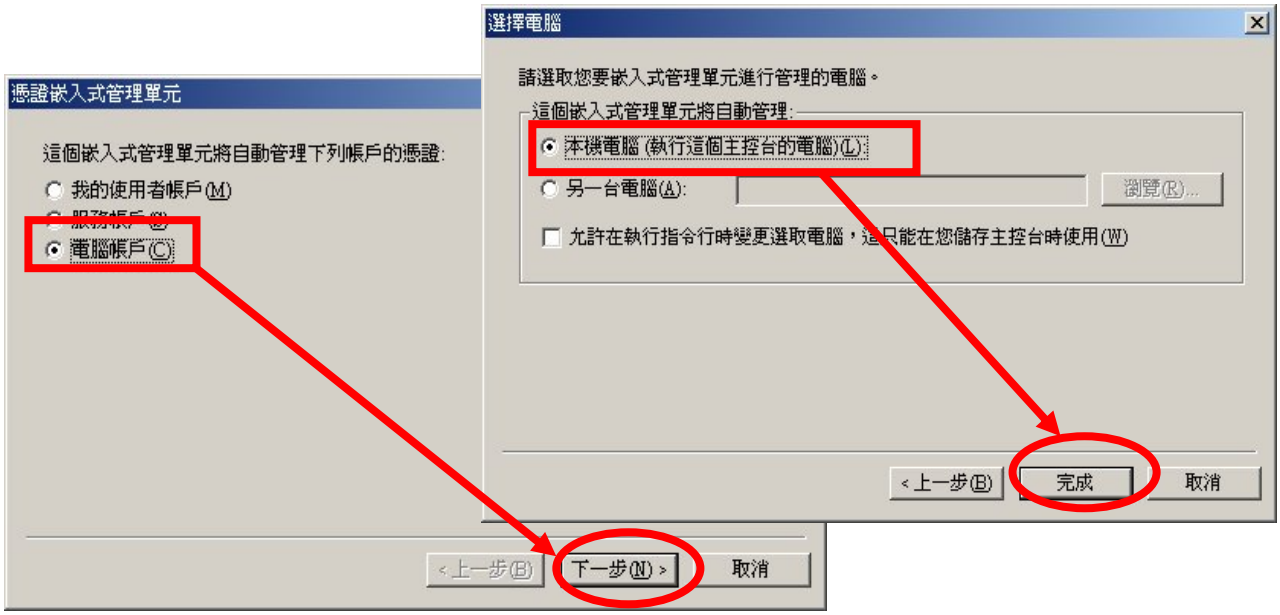
4.6.2 進入主控台後，選擇「新增／移除嵌入式管理單元」。



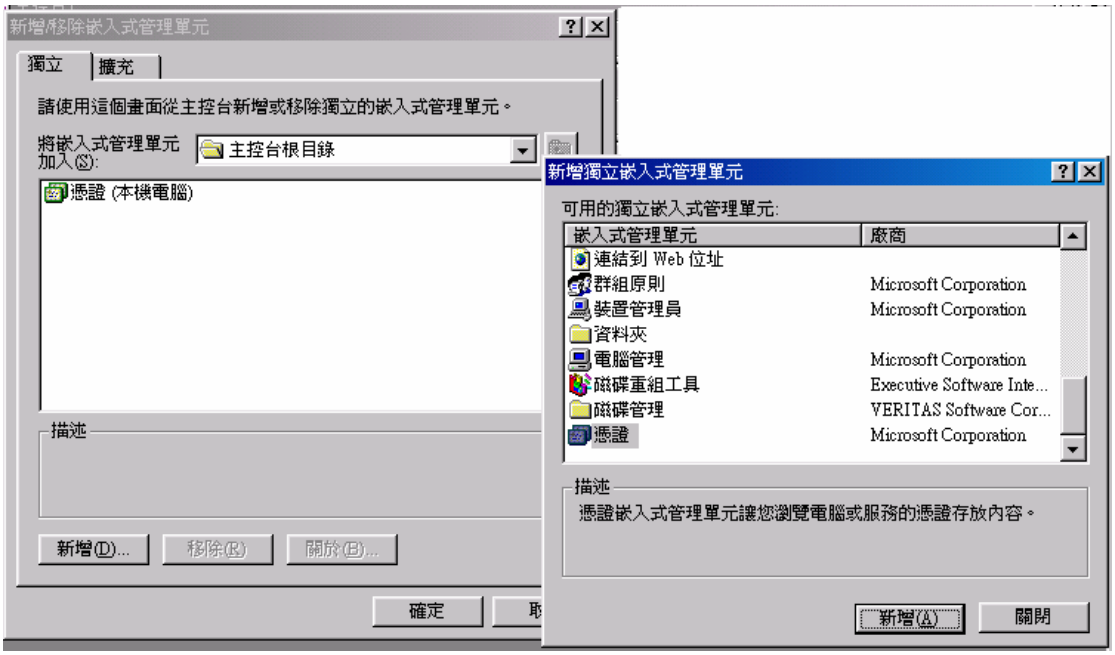
4.6.3「新增」憑證管理單元→ 憑證 →「新增」。



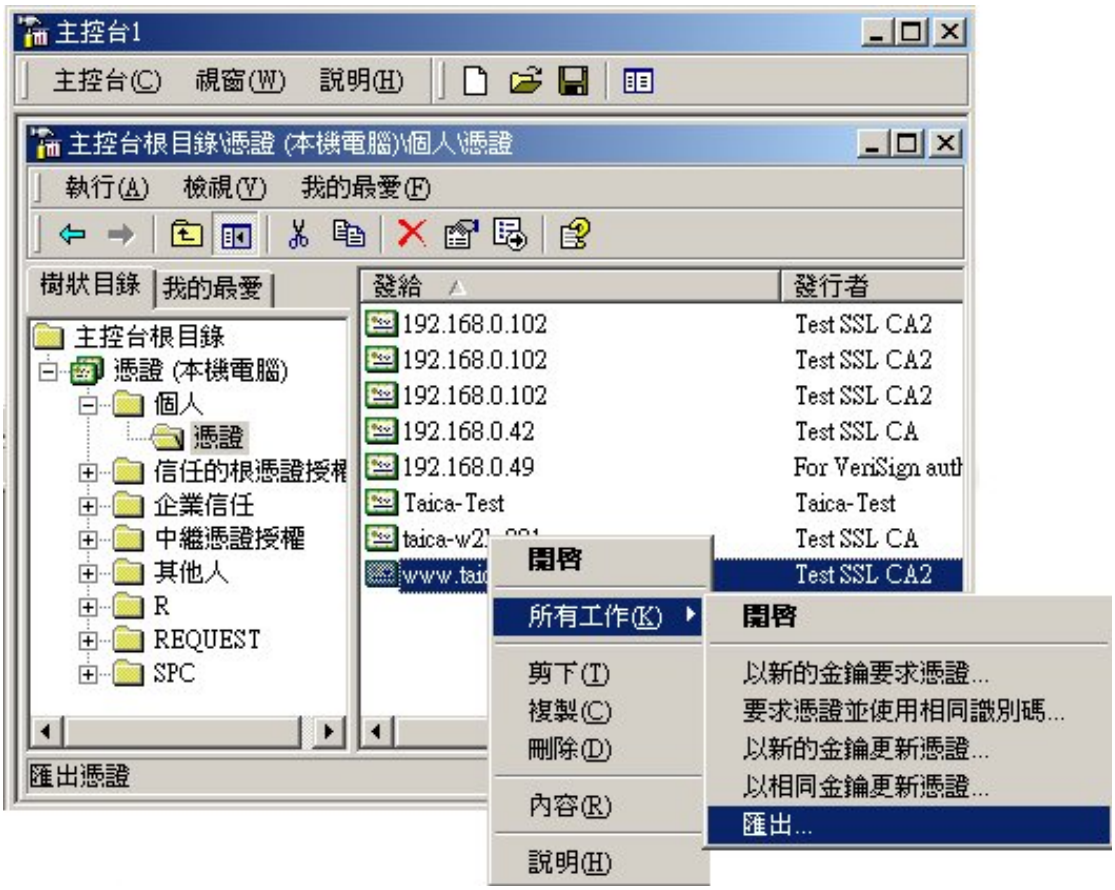
4.6.4「電腦帳戶」→「下一步」→「本機電腦(執行這個主控台的電腦)」→「完成」。



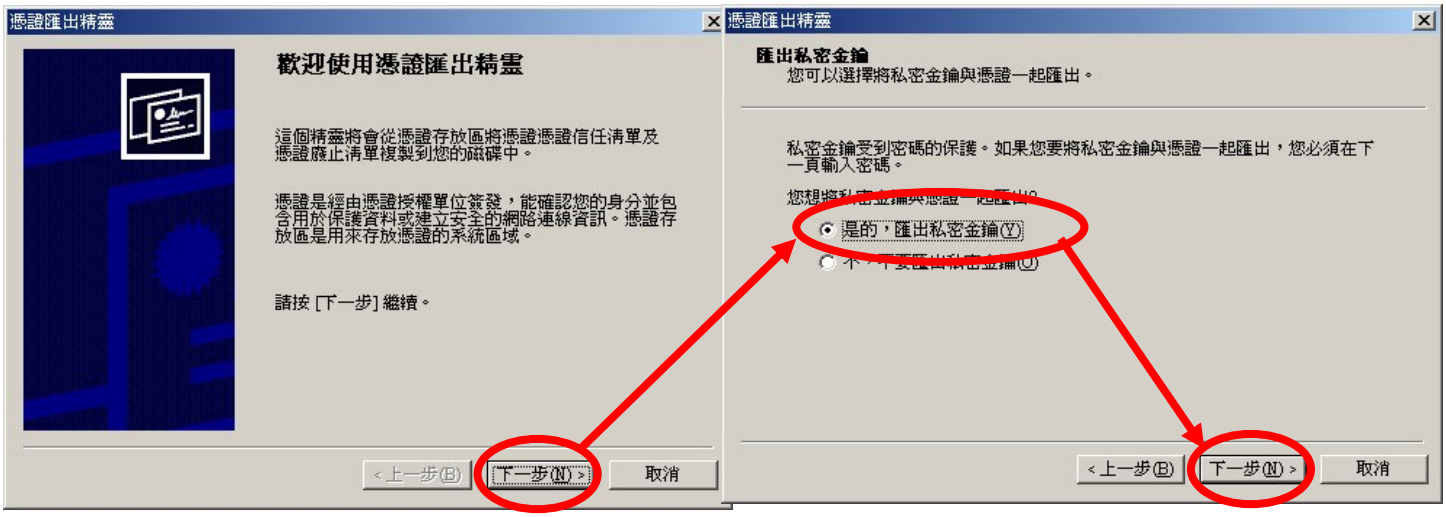
4.6.5 當 憑證(本機電腦) 新增出來後→「關閉」→「確定」。



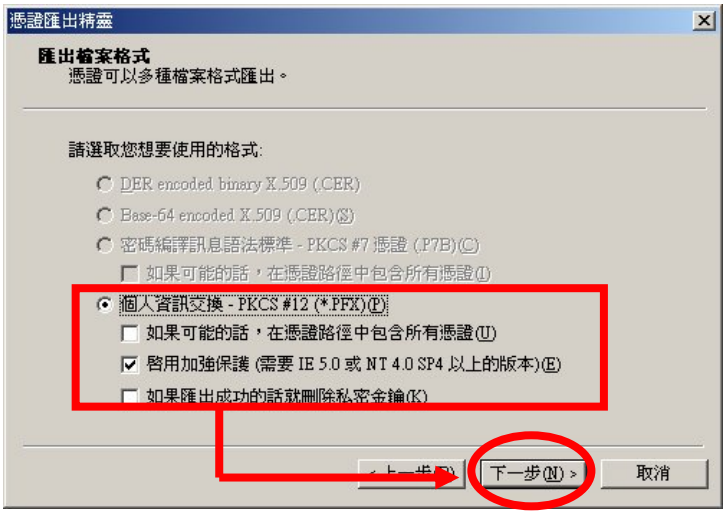
4.6.6 主控台中多出憑證管理項目，可在欲匯出的憑證上按右鍵執行匯出動作。



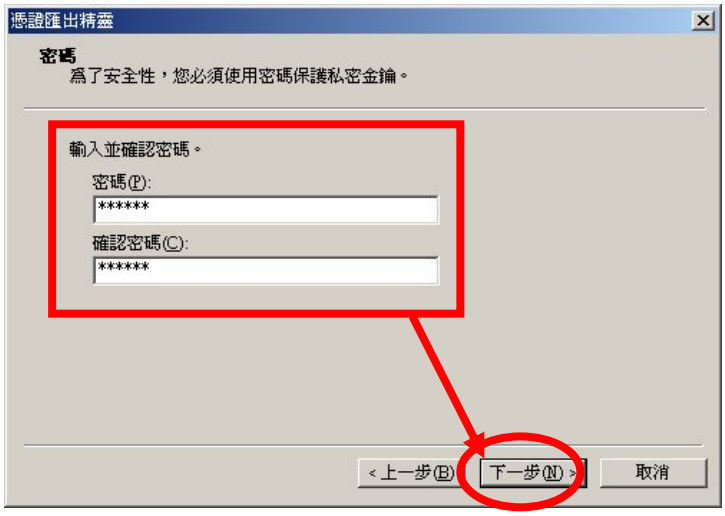
4.6.7 將出現使用憑證匯出精靈的畫面，請選擇「下一步」→「是的，匯出私密金鑰(Y)」→「下一步」。



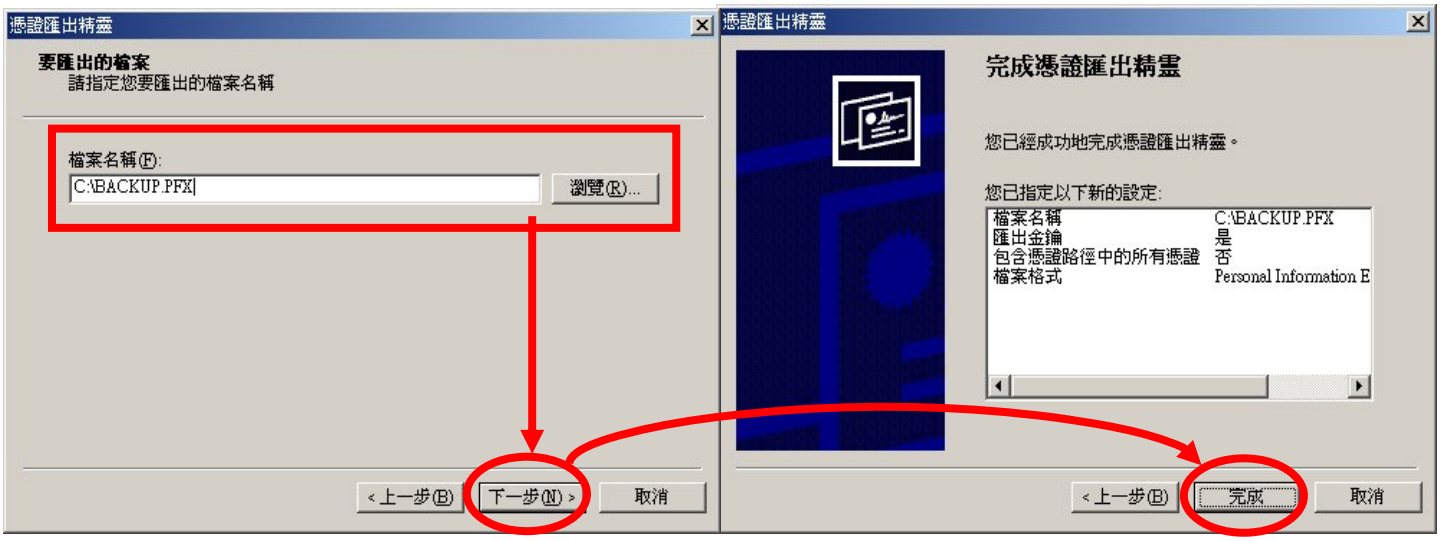
4.6.8「個人資訊交換-PKCS#12(*.PFX)」→「啟用加強保護(需要 IE5.0 或 NT4.0 SP4 以上的版本)」→「下一步」。



4.6.9 設定匯出資料的保護密碼→「下一步」。



4.6.10「瀏覽」→指定一個匯出檔案存放的路徑與檔名(副檔名固定為.PFX)→「下一步」→「完成」。



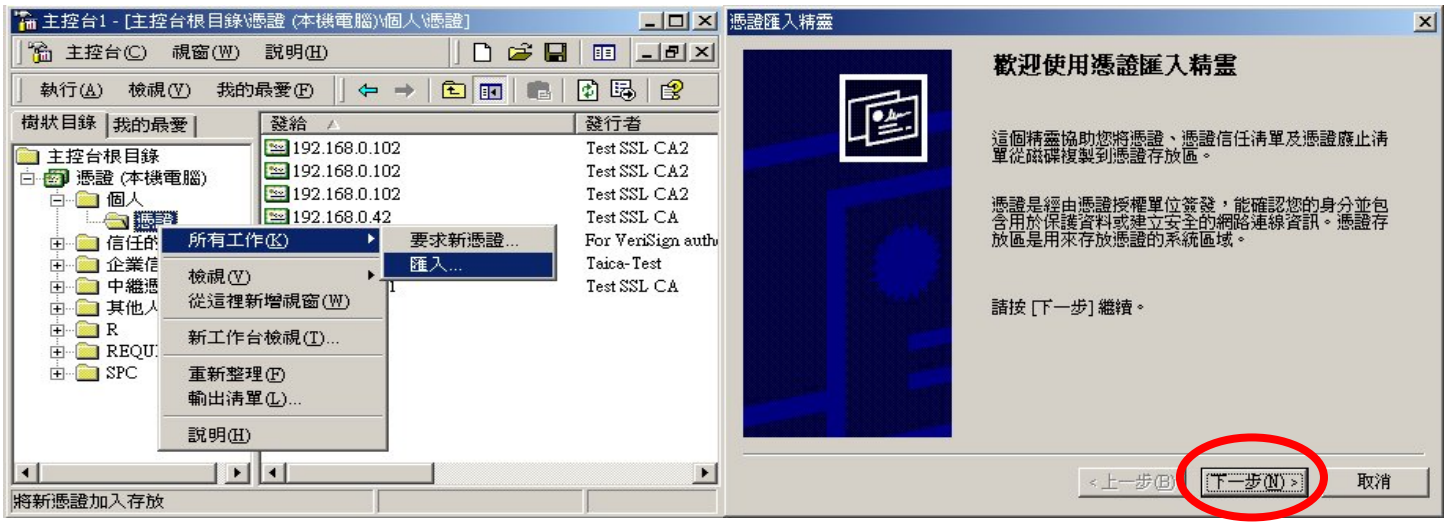
4.6.11 以上匯出動作為備份自我憑證檔與私密金鑰,請牢記匯出時設定的密碼。

4.6.12 請將下載之中繼憑證檔(TaiCASecureCA_Prod.crt），一併另行保存與備份。

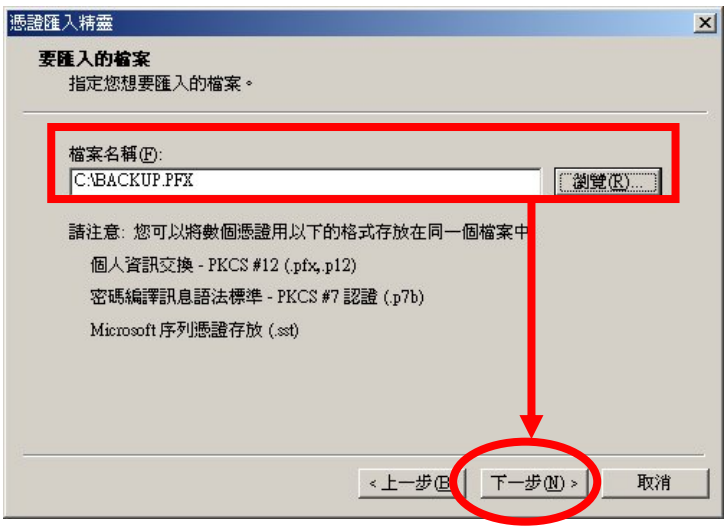
4.7 如何復原憑證(匯入)？

4.7.1 若要執行復原(匯入)工作，亦是進入主控台，從所有工作中執行匯入功能；如為新的伺服器設備請先執行說明 6.1 至 6.6 新增一個憑證管理單元。

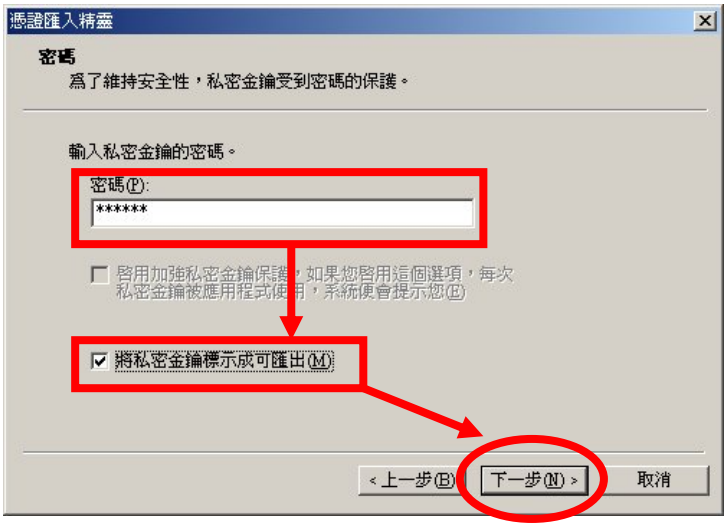
4.7.2 按滑鼠右鍵→「所有工作」 →「匯入」 →啟動憑證匯入精靈 →「下一步」。



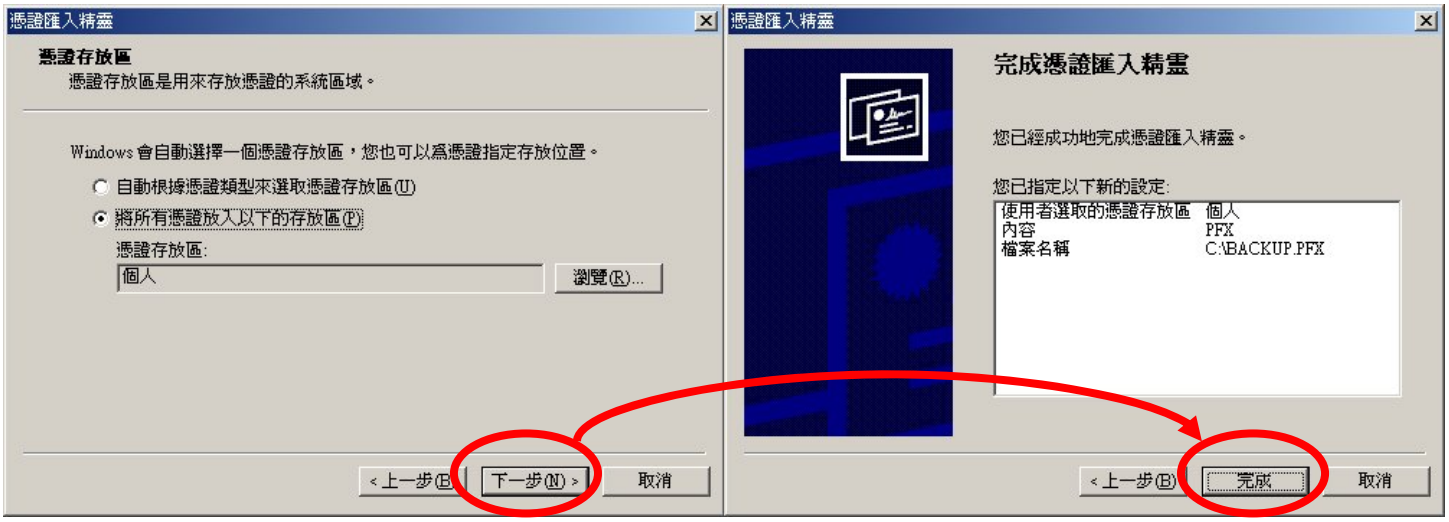
4.7.3「瀏覽」 →指定到當初匯出備份的檔案(*.PFX) →「下一步」。



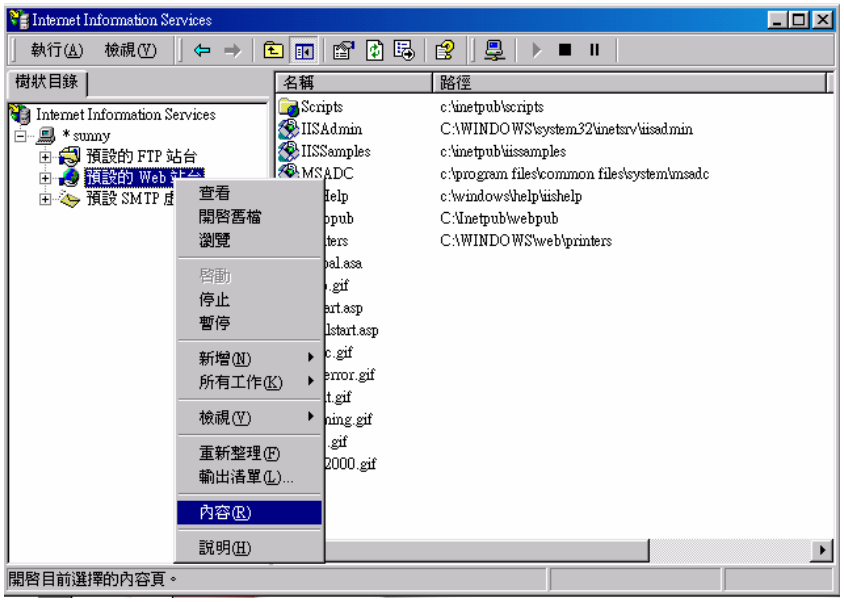
4.7.4 輸入當初匯出備份時所設定的密碼 →勾選「將私密金鑰標示成可匯出」 →「下一步」。



4.7.5 確定選擇「將所有憑證放入以下的存放區」 →存放區顯示位個人→「下一步」 →「完成」。

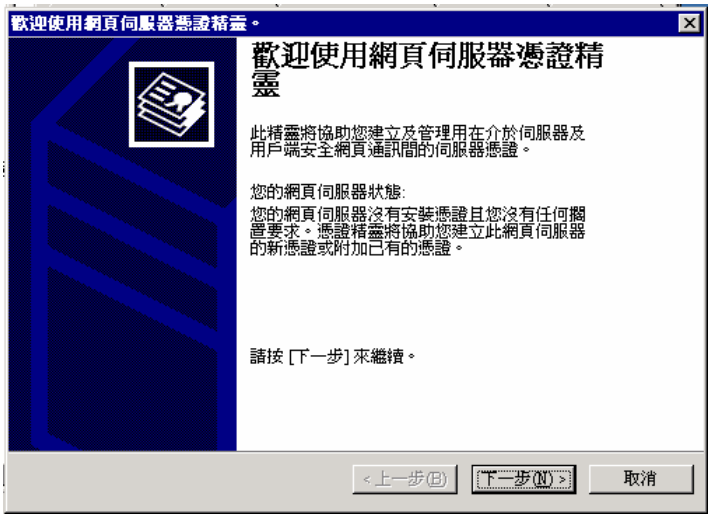


4.7.6 從 IIS 站台上按滑鼠右鍵→「內容」。

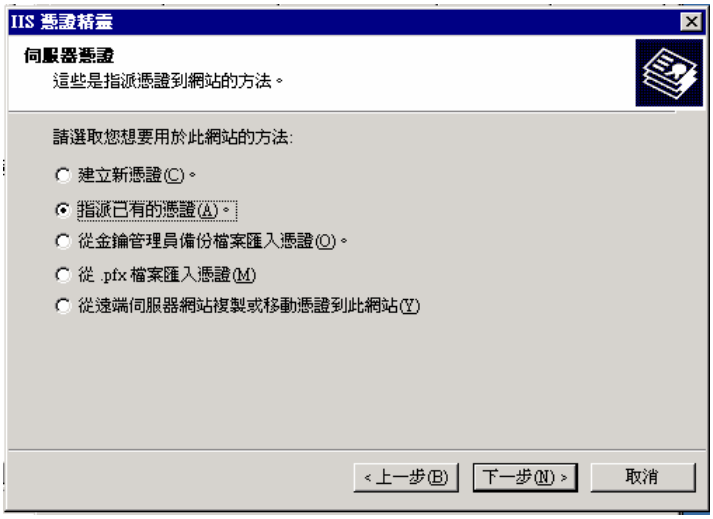


4.7.7「目錄安全設定」→「伺服器憑證」。

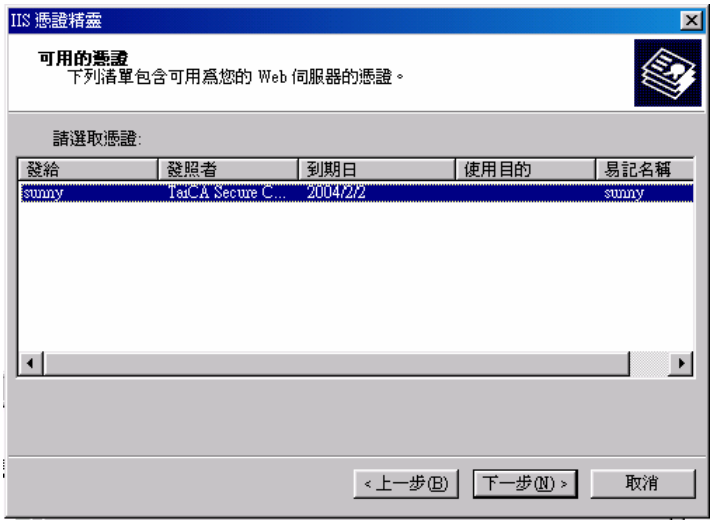
4.7.8 啟動網頁伺服器憑證精靈→「下一步」。



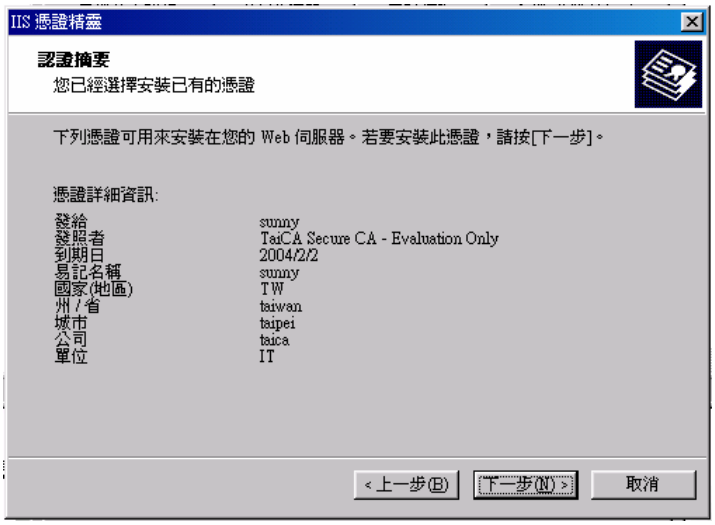
4.7.9「指派已有的憑證」→「下一步」。



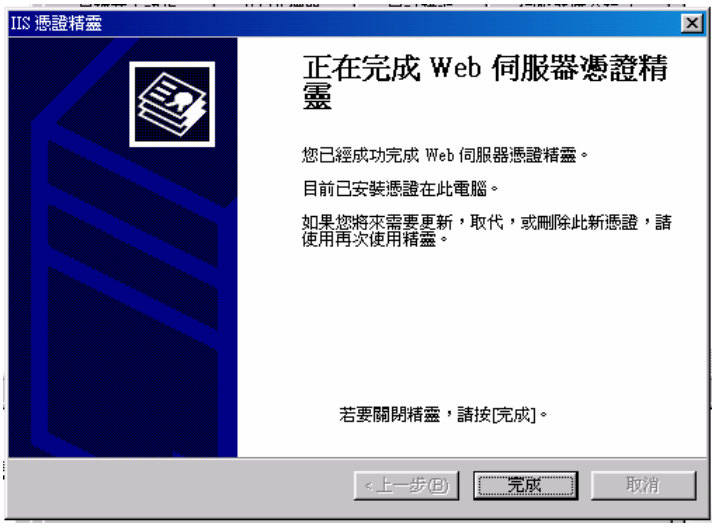
4.7.10 選擇匯入的憑證項目→「下一步」。



4.7.11 檢視已選取安裝憑證資訊→「下一步」。



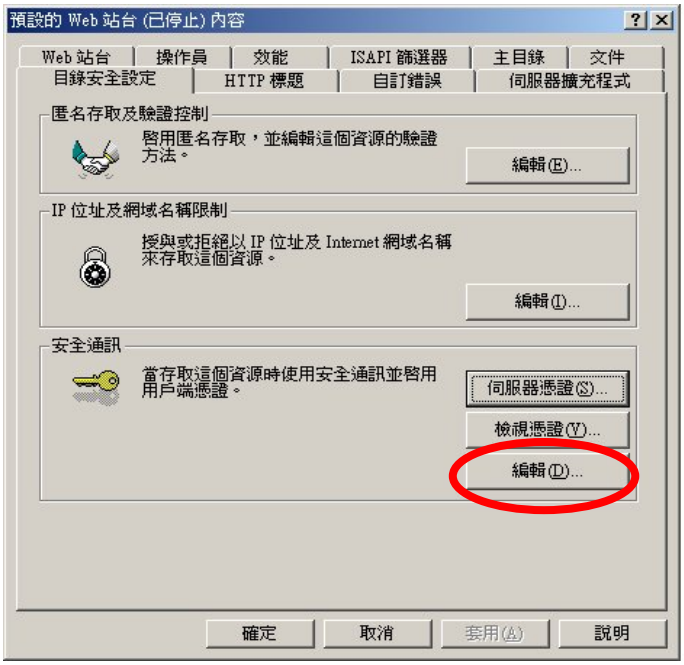
4.7.12「完成」。



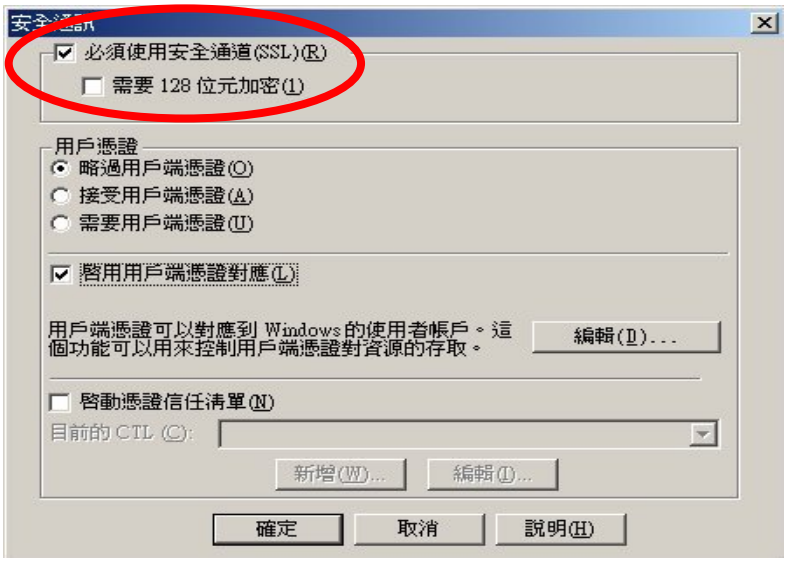
4.7.13 執行完以上步驟後，請參照第 4 節說明安裝中繼憑證檔(TaiCASecureCA_Prod.crt)。

4.8 如何啟動 SSL 模式？

4.8.1 開始→程式集→Microsoft Internet 伺服器→Internet 服務管理員畫面中在欲執行 SSL 模式的站臺上按右鍵→內容→目錄安全設定→選擇「安全通訊」中的「編輯」。



4.8.2 在安全通訊視窗中，將「必須使用安全通道(SSL)」的選項選取，將網站重新啟動後，使用者存取此網站或網站下目錄的檔案時，就必須使用 SSL 模式通訊。若要強迫用戶連上網站皆必須使用 128 位元之 SSL 模式的話，則將「需要 128 位元加密」選取即可。



4.9 如何更新 SSL 憑證？

4.9.1 臺灣網路認證公司所發出的 SSL 伺服器憑證效期可分為一年期及二年期，並會在憑證到期前二個月發出憑證更新通知信給　貴公司。在這二個月內您隨時可以至臺灣網路認證公司下載申請表單，填寫完畢後寄回台灣網路認證公司即可進行更新申請。

4.9.2 在進行更新前請記得備份您原有的 SSL 伺服器憑證。

4.9.3 由於 IIS 預設的「更新憑證」功能有誤，無法產生正確的憑證申請檔，所以更新憑證的時候，請使用同一台伺服上的其他站臺(例如：系統管理 Web 站台)，以產生一個新的憑證請申請檔。並依照第 4.1 及 4.2 的描述，申請並安裝 SSL 伺服器憑證及新的臺灣網路認證公司憑證。

4.9.4 安裝完伺服器憑證及中繼憑證後，回到欲更新憑證的站台，按右鍵→內容→目錄安全設定→伺服器憑證，啟始 Web 伺服器憑證精靈後，按下「取代目前的憑證」。

5.附件

無。