

中華電信通用憑證管理中心 (PublicCA)

Windows IIS 6.0 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，若因參考本說明文件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。

目錄

Windows IIS 6.0 SSL 憑證請求檔製作手冊.....	2
從未安裝過憑證的伺服器產生憑證請求檔操作步驟.....	2
已安裝過憑證的伺服器產生憑證請求檔操作步驟.....	10
Windows IIS 6.0 SSL 憑證安裝操作手冊.....	46
安裝根憑證(eCA)及中繼憑證(PublicCA).....	46
從未安裝過憑證的伺服器，安裝憑證操作步驟.....	64
已安裝過憑證的伺服器，安裝憑證操作步驟.....	73
附件一：單一 IP 多網域憑證安裝步驟.....	91

Windows IIS 6.0 SSL 憑證請求檔製作手冊

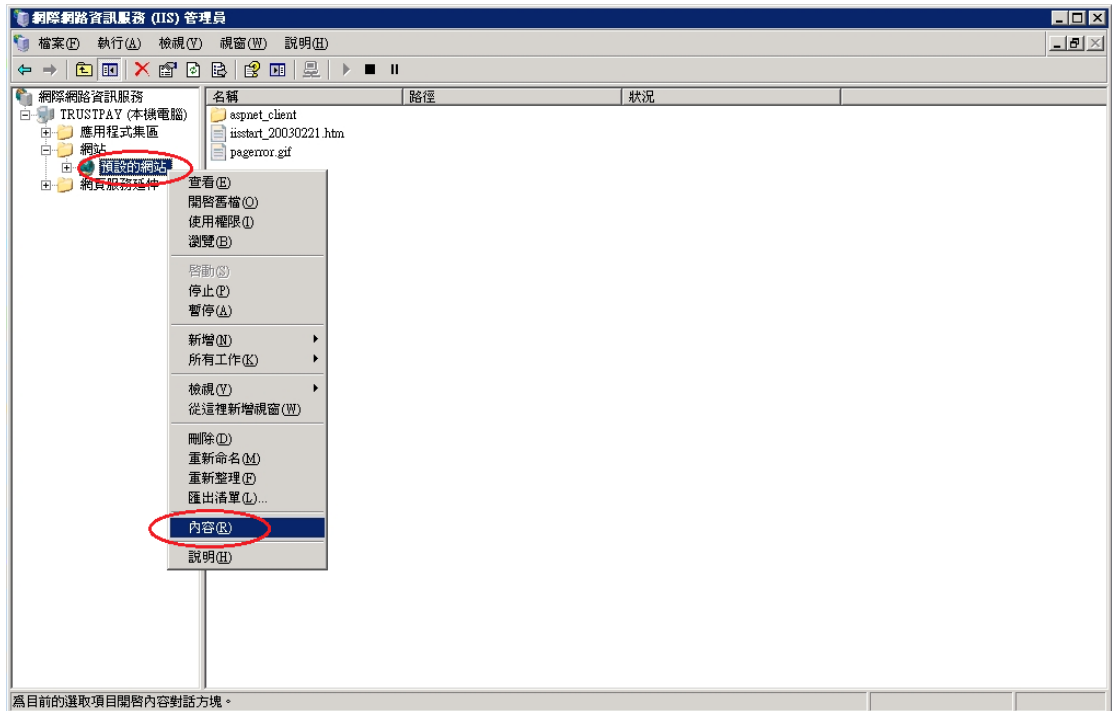
從未安裝過憑證的伺服器產生憑證請求檔操作步驟

一、將「網際網路資訊服務(IIS)管理員」開啟。



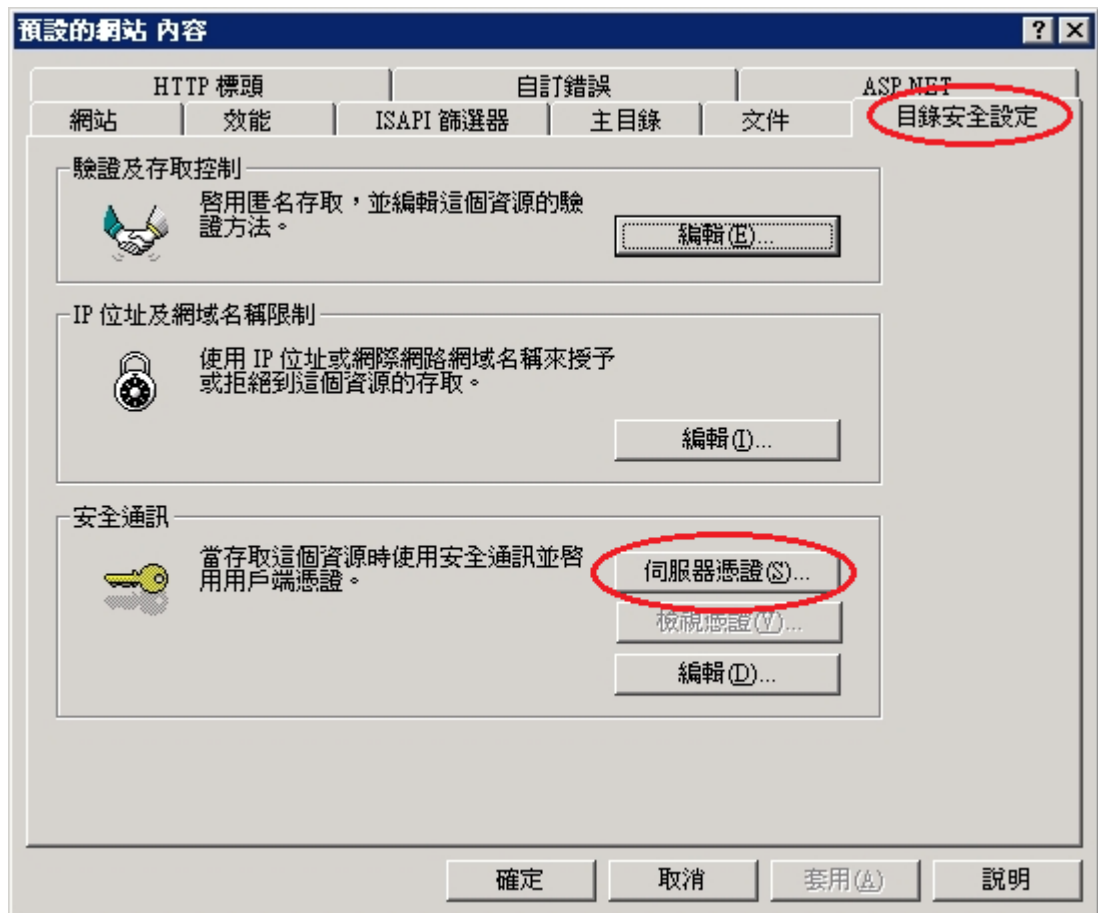
二、產生憑證請求檔

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

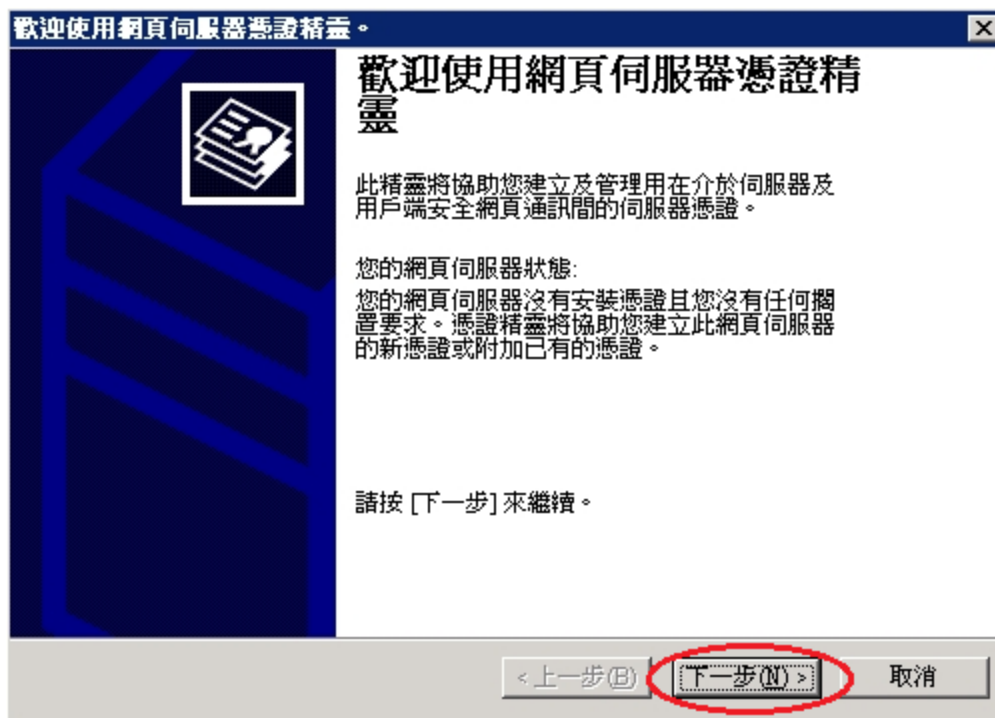


接著將頁面切到「目錄安全設定」頁面。

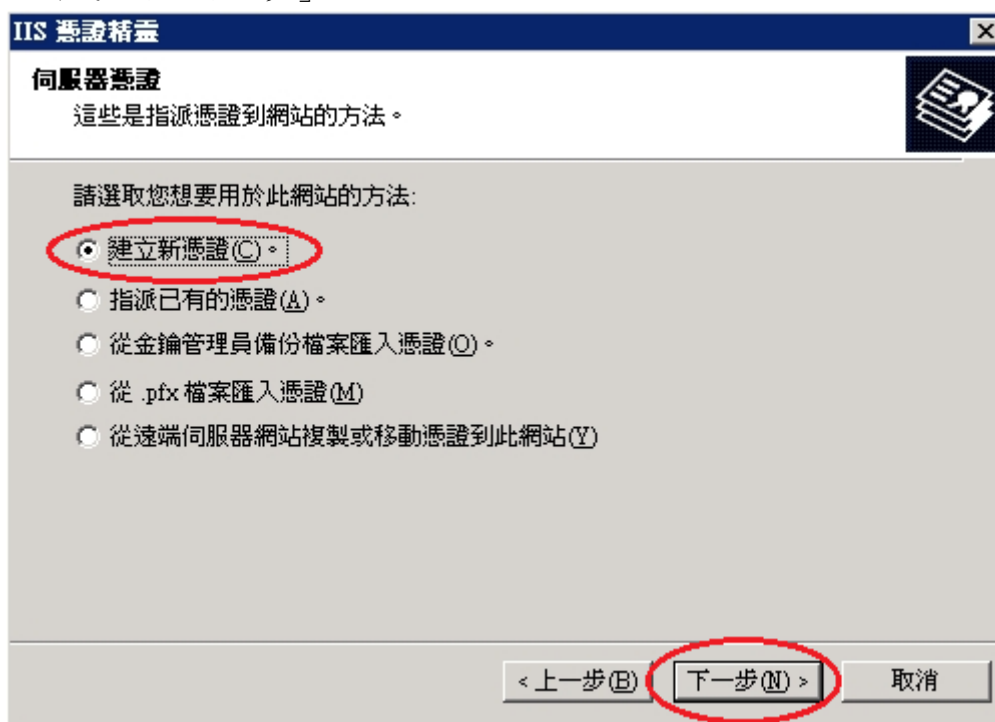
在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。



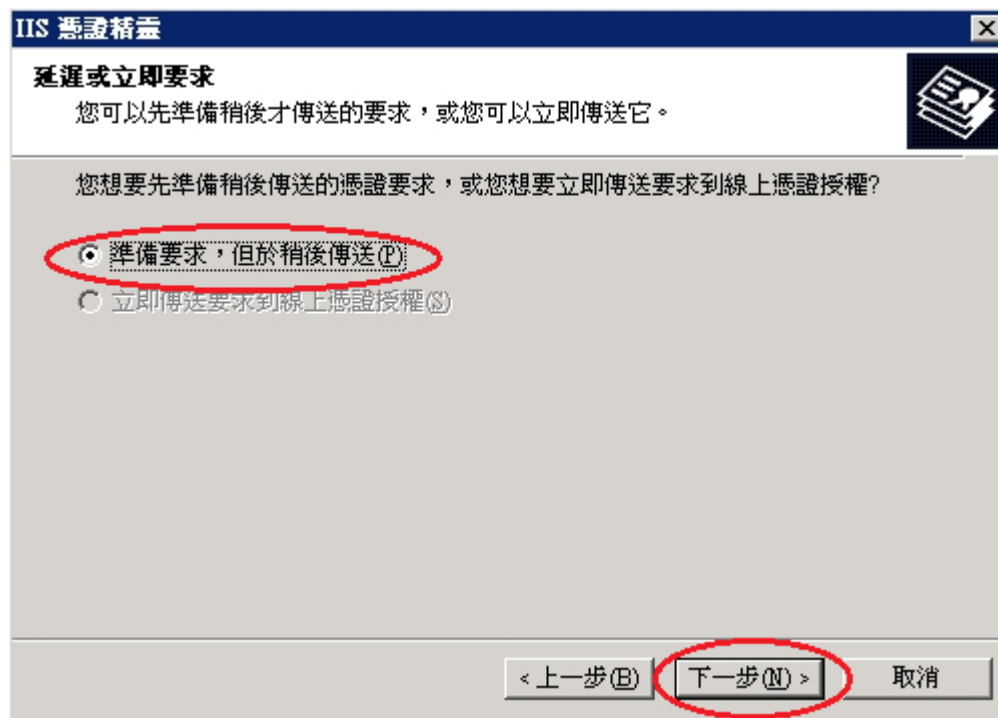
接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，以滑鼠按下「下一步」按鈕，開始製作 Windows 2003 IIS 6.0 伺服器憑證請求檔。



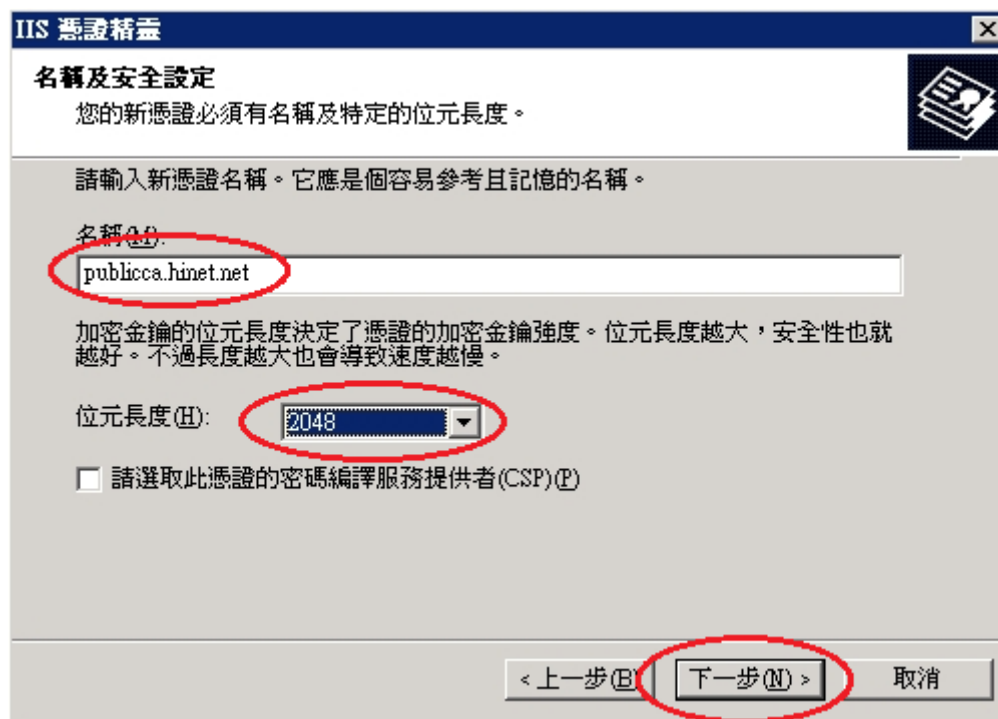
接著畫面會到「伺服器憑證」視窗，以滑鼠點選「建立新憑證(C)」，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「延遲或立即要求」視窗，以滑鼠點選「準備要求，但稍後再傳送(P)」，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「名稱及安全設定」視窗，以滑鼠點選「名稱(M)」欄位後並輸入網站名稱，接著以滑鼠點選「位元長度(H)」為「2048」bits 後，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「公司資訊」視窗，以滑鼠點選「公司(O)」欄位後並輸入組織名稱或公司名稱，接著以滑鼠點選「單位(U)」欄位後並輸入組織或公司的單位名稱，接著以滑鼠按下「下一步」按鈕。

IIS 憑證精靈

公司資訊

您的憑證中必須有您公司的資訊，這些資訊將用來區別您的及其他的公司。

請選取或輸入您的公司名稱及單位。通常這是您公司及部門的正式名稱。

若需進一步資訊，請與憑證授權單位的網站聯絡。

公司(O):
中華電信股份有限公司數據通信分公司

單位(U):
政府網路處

< 上一步(B) 下一步(N) > 取消

接著畫面會到「您站台的一般名稱」視窗，以滑鼠點選「一般名稱(C)」欄位後並輸入一般名稱(即站台的網址「Domain Name」)，接著以滑鼠按下「下一步」按鈕。

IIS 憑證精靈

您網站的一般名稱

您的網站的一般名稱是一個完全符合規定的網域名稱。

請為您的網站輸入一般名稱。若伺服器在網際網路上，請用有效的 DNS 名稱。若伺服器在近端內部網路上，您也許想用電腦的 NetBIOS 名稱。

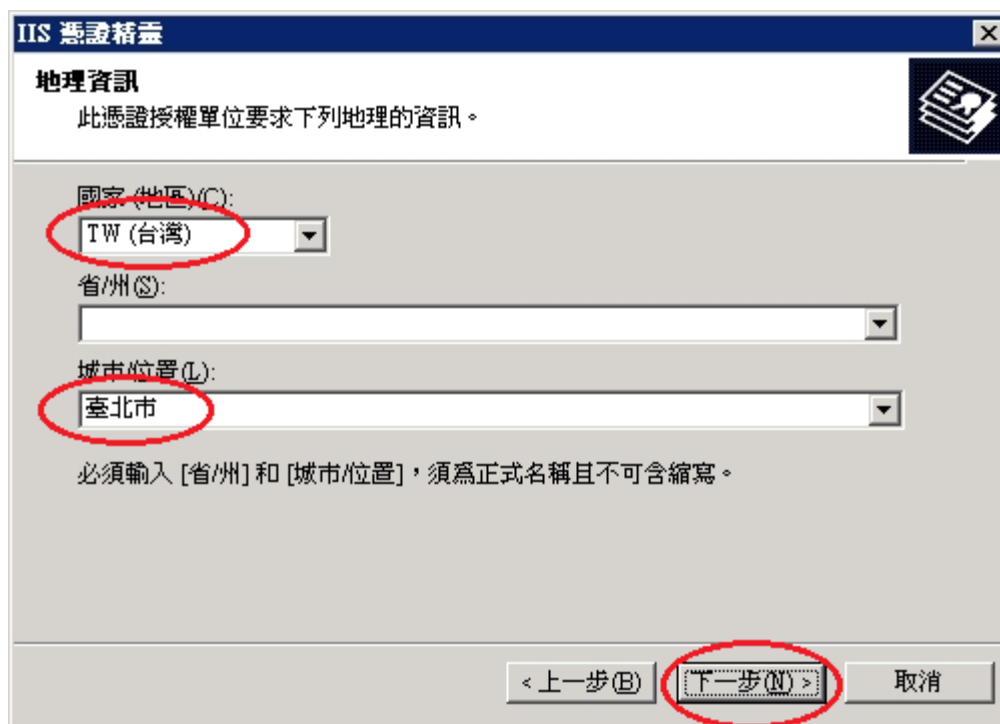
如果變更一般名稱，您將需要取得新的憑證。

般名稱(C):
publicca.hinet.net

< 上一步(B) 下一步(N) > 取消

接著畫面會到「地理資訊」視窗，接著以滑鼠點選「國家(地區)(C)」，以滑鼠點選「TW(台灣)」，接著以滑鼠點選「州/省(S)」欄位後依照所在地輸入正確的州/省名稱，如圖為輸入「空白」或輸入「臺灣省」亦可，接著以

滑鼠點選「城市/位置(L)」欄位後依照所在地輸入正確的城市名稱，如圖為輸入「臺北市」，接著以滑鼠按下「下一步」按鈕。



IIS 憑證精靈

地理資訊

此憑證授權單位要求下列地理的資訊。

國家(地區)(C):
TW (台灣)

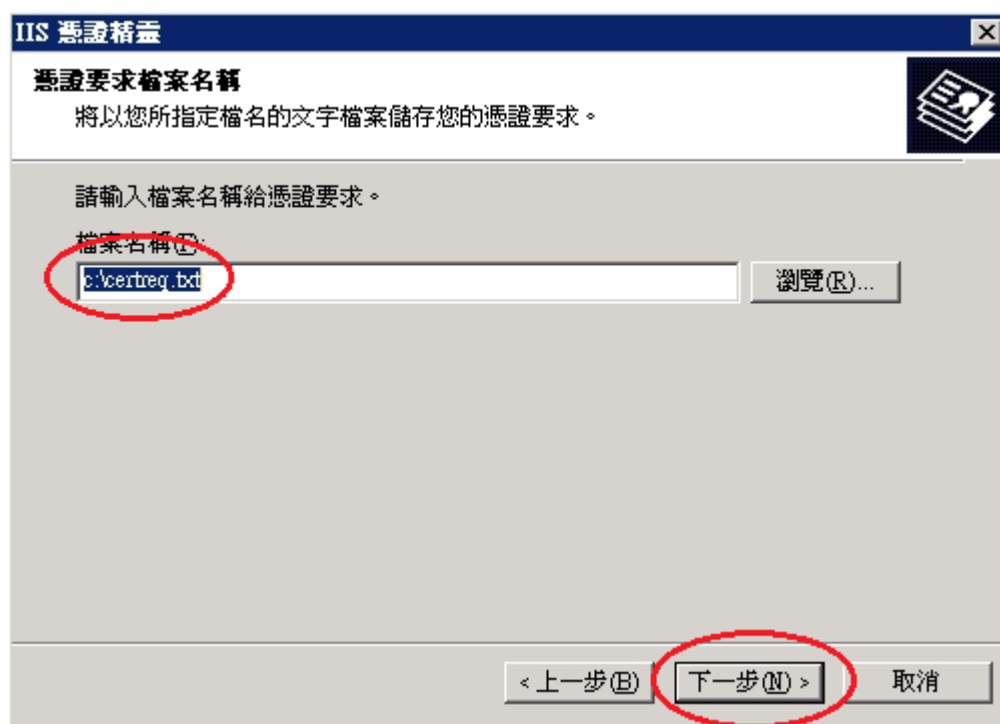
省/州(S):

城市位置(L):
臺北市

必須輸入 [省/州] 和 [城市/位置]，須為正式名稱且不可含縮寫。

< 上一步(B) **下一步(N) >** 取消

接著畫面會到「憑證要求檔案名稱」視窗，接著以滑鼠點選「檔案名稱(F)」欄位後並輸入路徑及要存的檔案名稱。如下圖所示，通常都是依照如下圖之預設值路徑及檔案名稱存放，接著以滑鼠按下「下一步」按鈕。



IIS 憑證精靈

憑證要求檔案名稱

將以您所指定檔名的文字檔案儲存您的憑證要求。

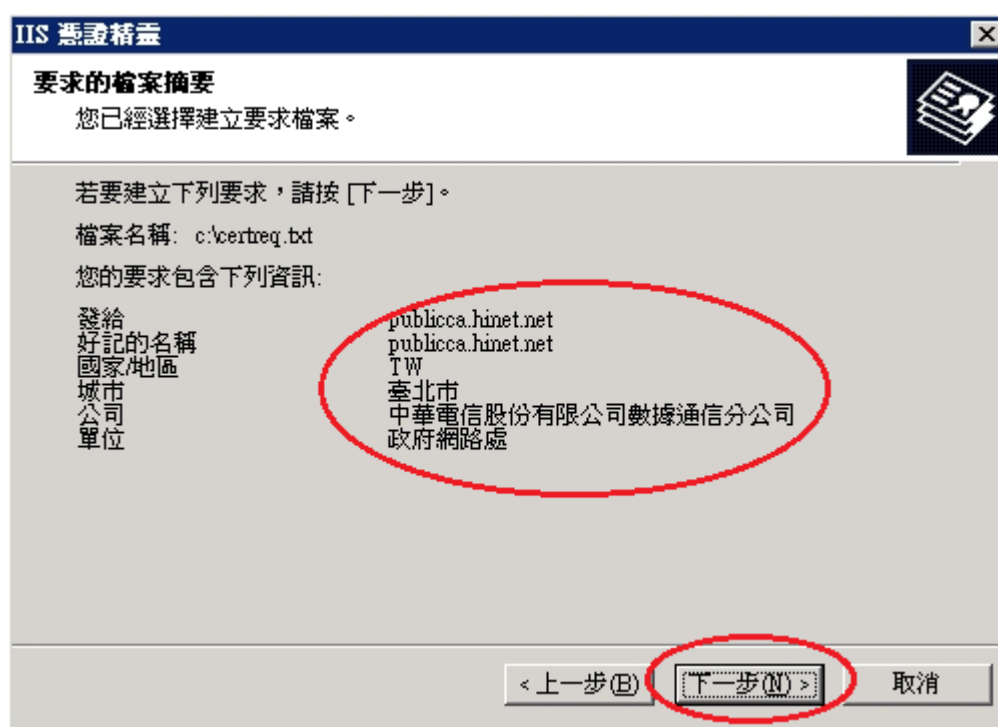
請輸入檔案名稱給憑證要求。

檔案名稱(F):
.\certreq.txt 瀏覽(R)...

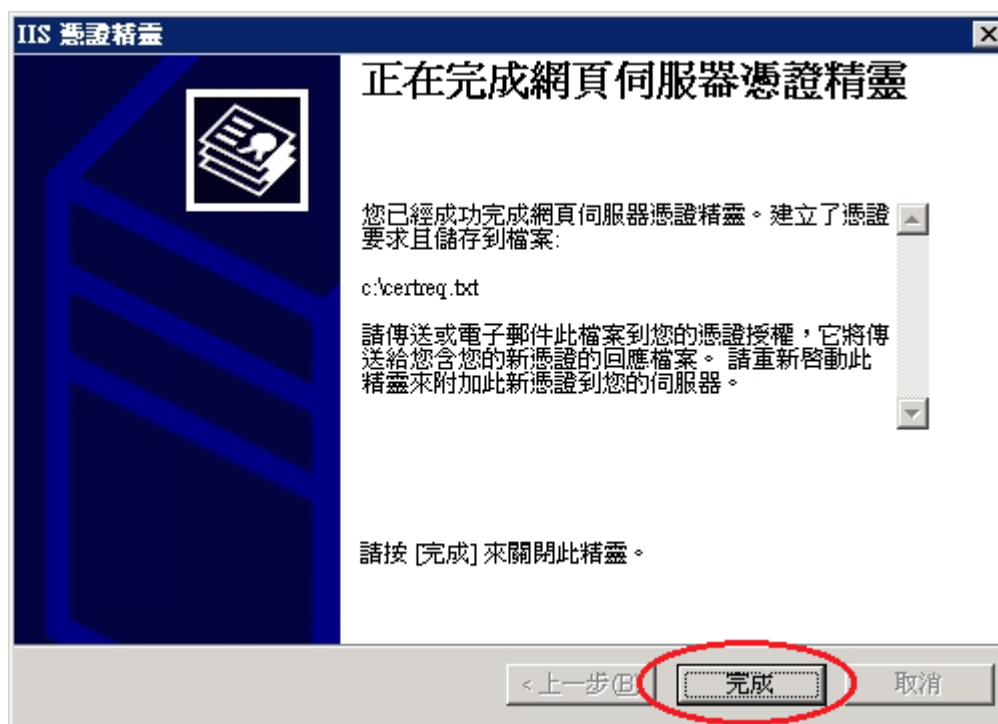
< 上一步(B) **下一步(N) >** 取消

接著畫面會到「要求的檔案摘要」視窗，檢視剛才各步驟所設定的值是否無

誤。如果沒有問題，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成結束製作憑證請求檔動作。



三、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔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。

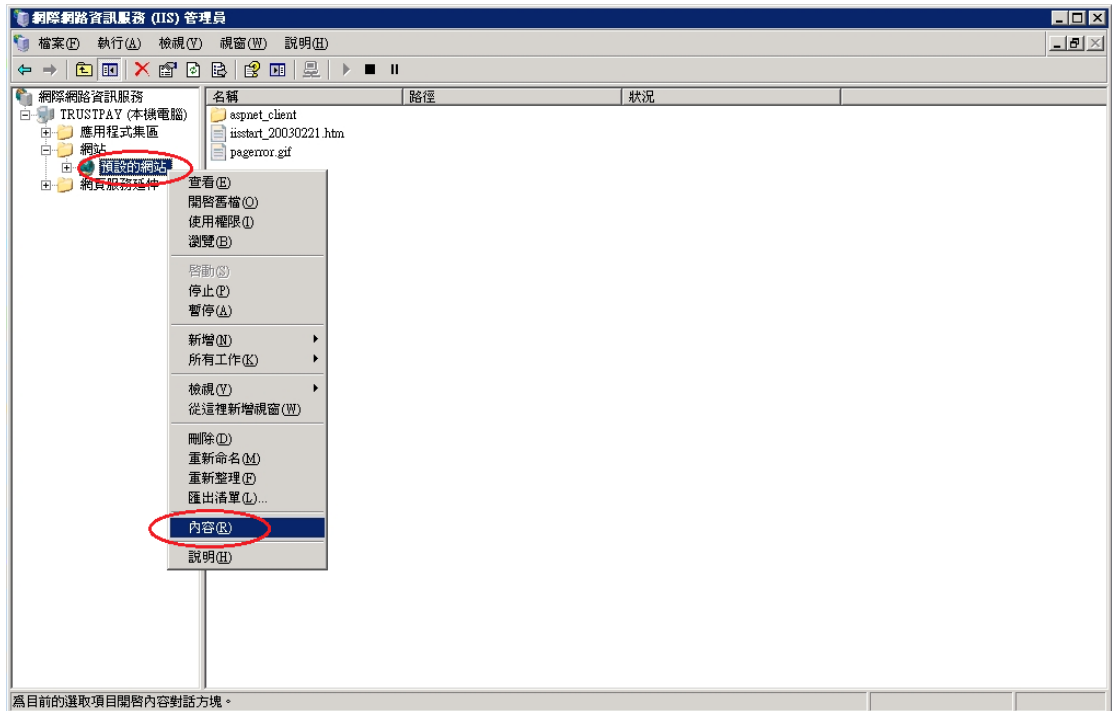
已安裝過憑證的伺服器產生憑證請求檔操作步驟

一、將「網際網路資訊服務(IIS)管理員」開啟。

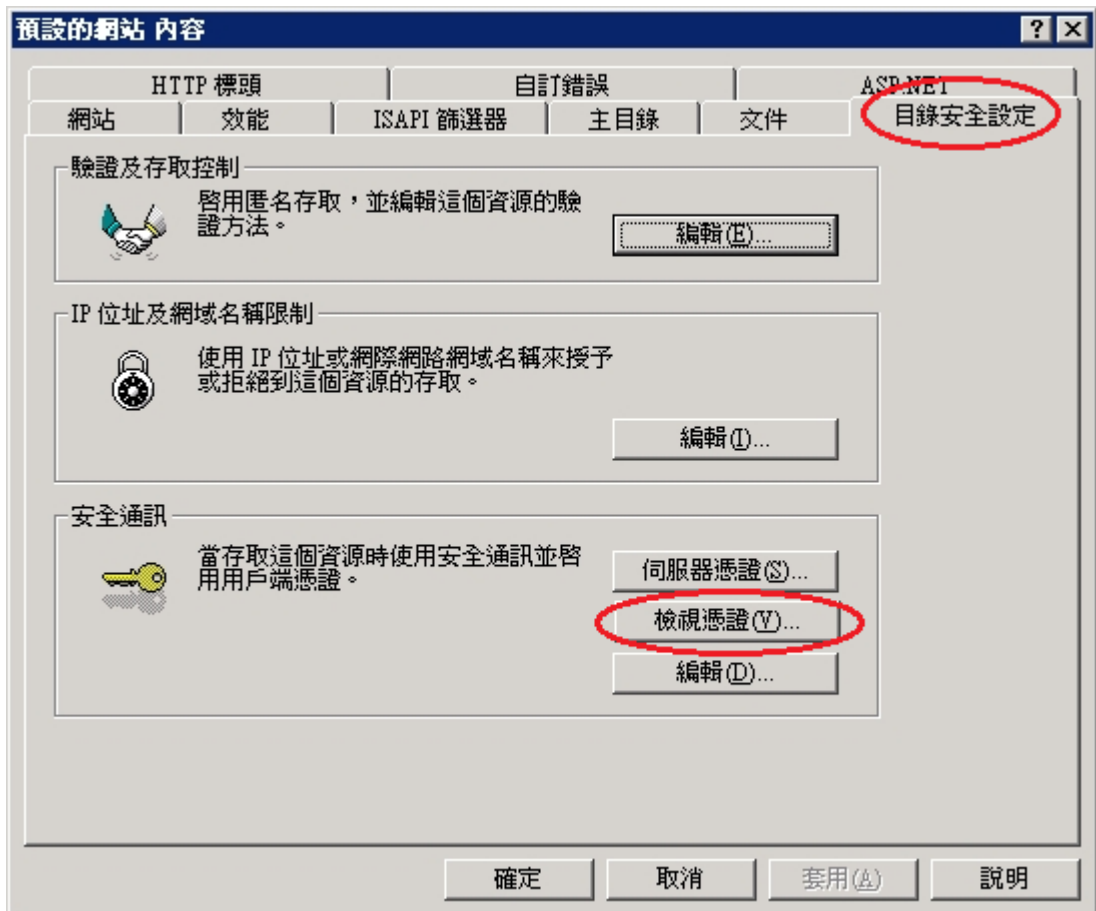


二、將私密金鑰及憑證匯出備份。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

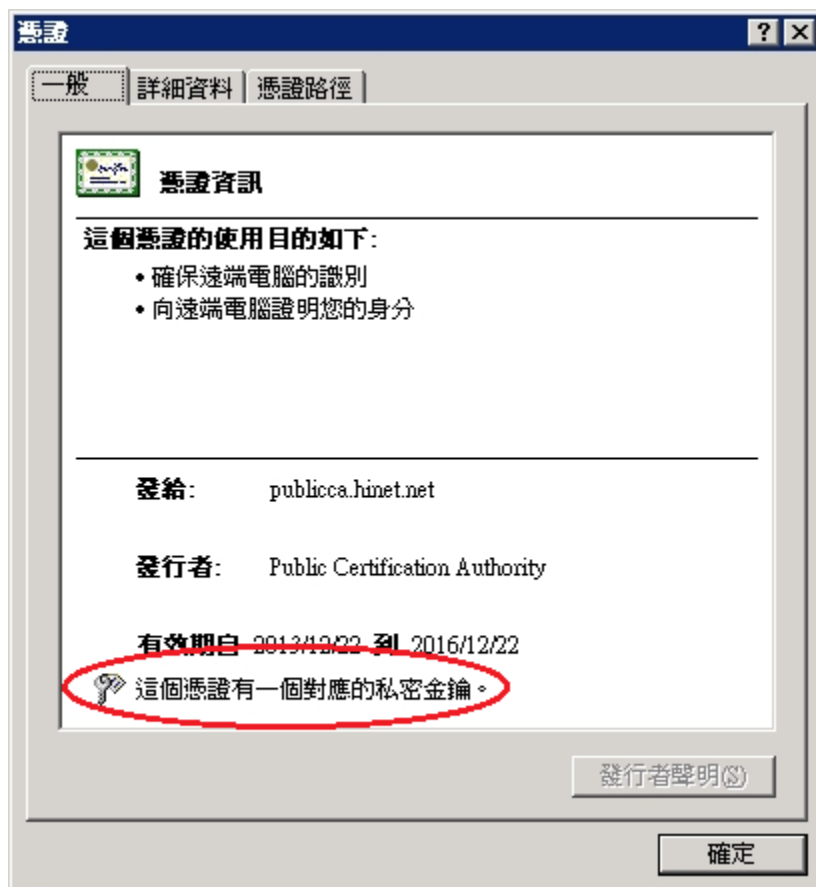


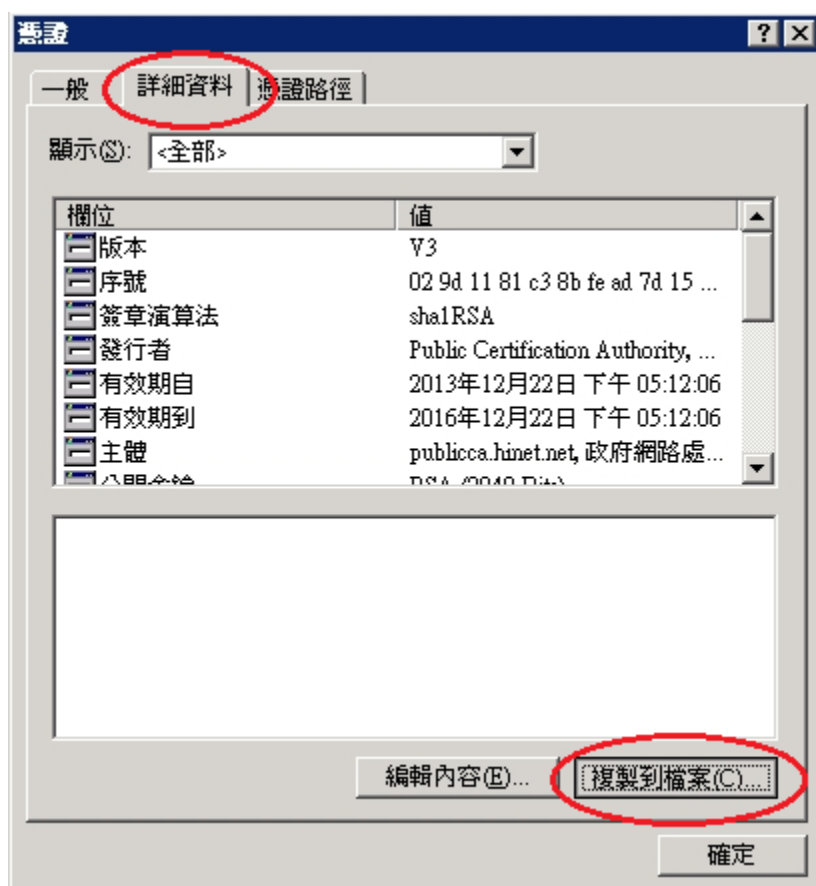
接著將頁面切到「目錄安全設定」頁面，在「目錄安全設定」頁面，以滑鼠按下「檢視憑證」按鈕。



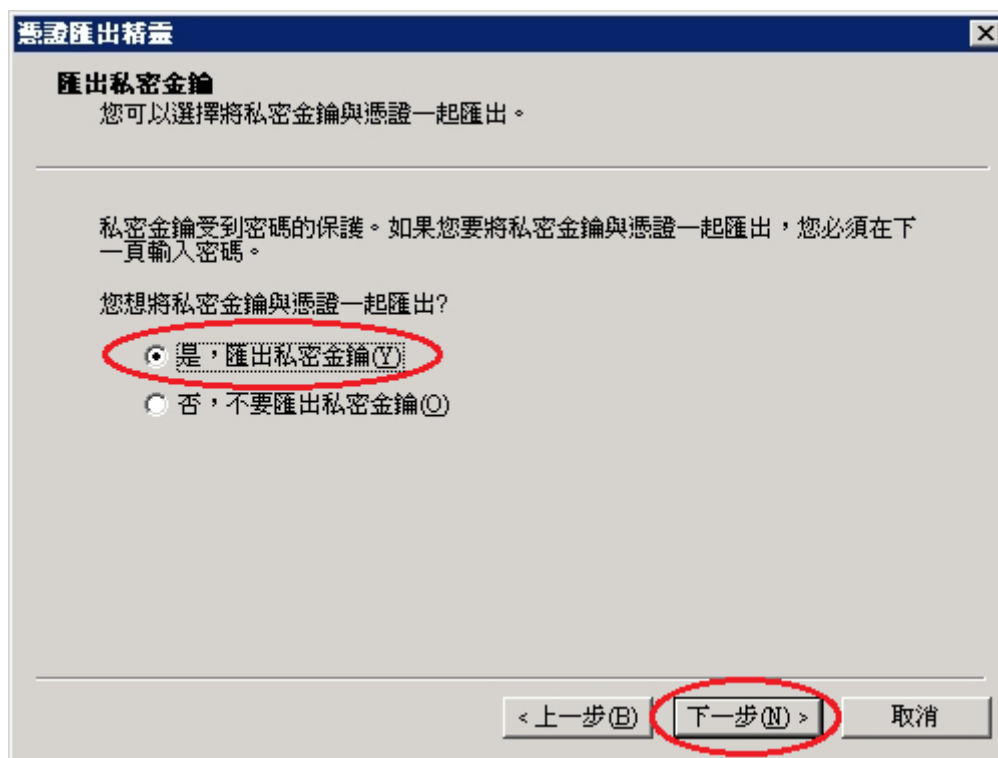
將目前線上金鑰及憑證進行備份。憑證視窗如下出現有「這個憑證有一個對

應的私密金鑰」，代表這張憑證的私密金鑰跟憑證皆有存在。接著切「詳細資料」頁面，並點選「複製到檔案」按鈕。



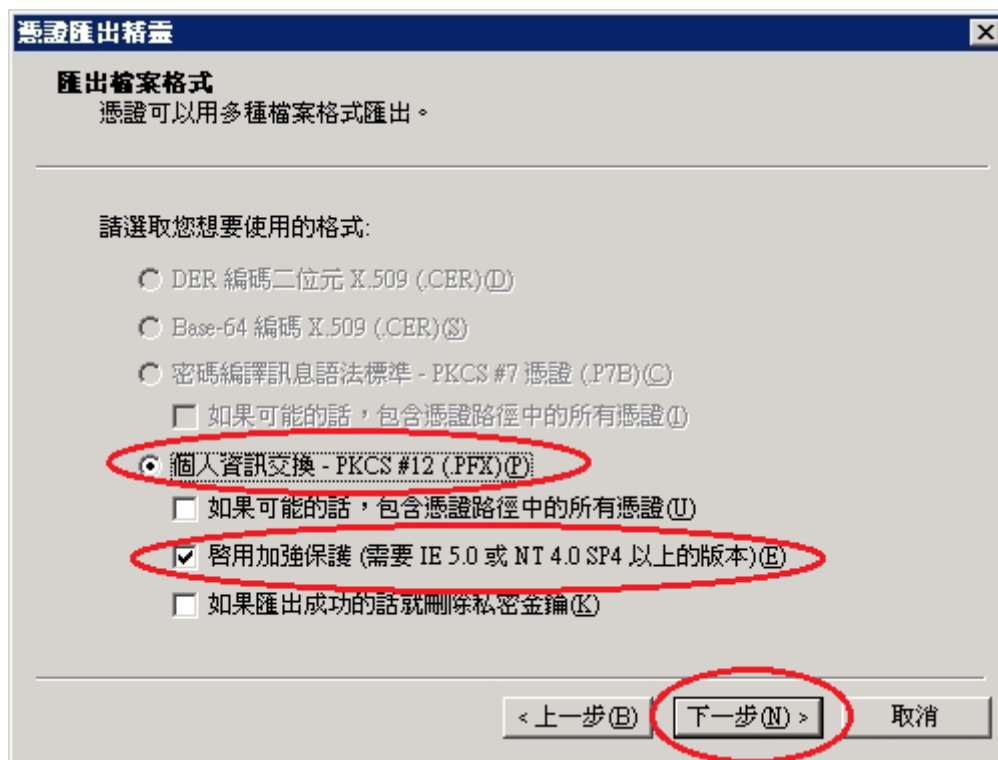


接著出現「憑證匯出精靈」，「匯出私密金鑰」頁面選擇「是，匯出私密金鑰」後，以滑鼠按下「下一步」按鈕。

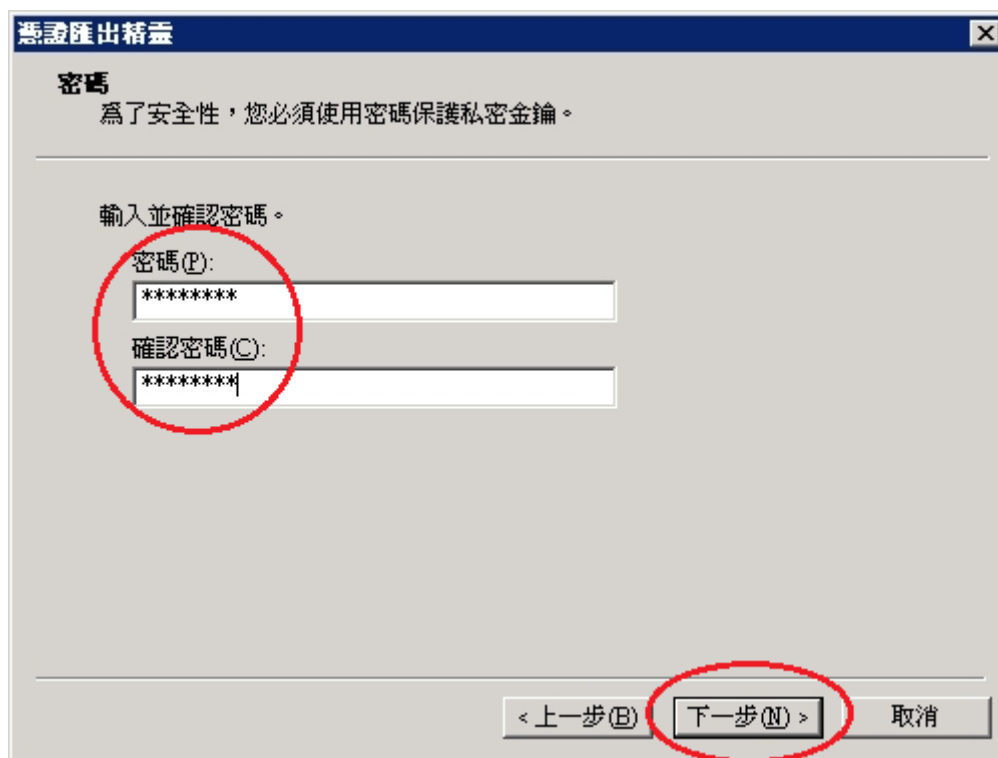


接著出現「匯出檔案格式」頁面，選擇「個人資訊交換 - PKCS #12

(.PFX)(P)」，並勾選「啓用加強保護(需要 IE 5.0 或 NT 4.0 SP4 以上的版本)(E)」，接著以滑鼠按下「下一步」按鈕。

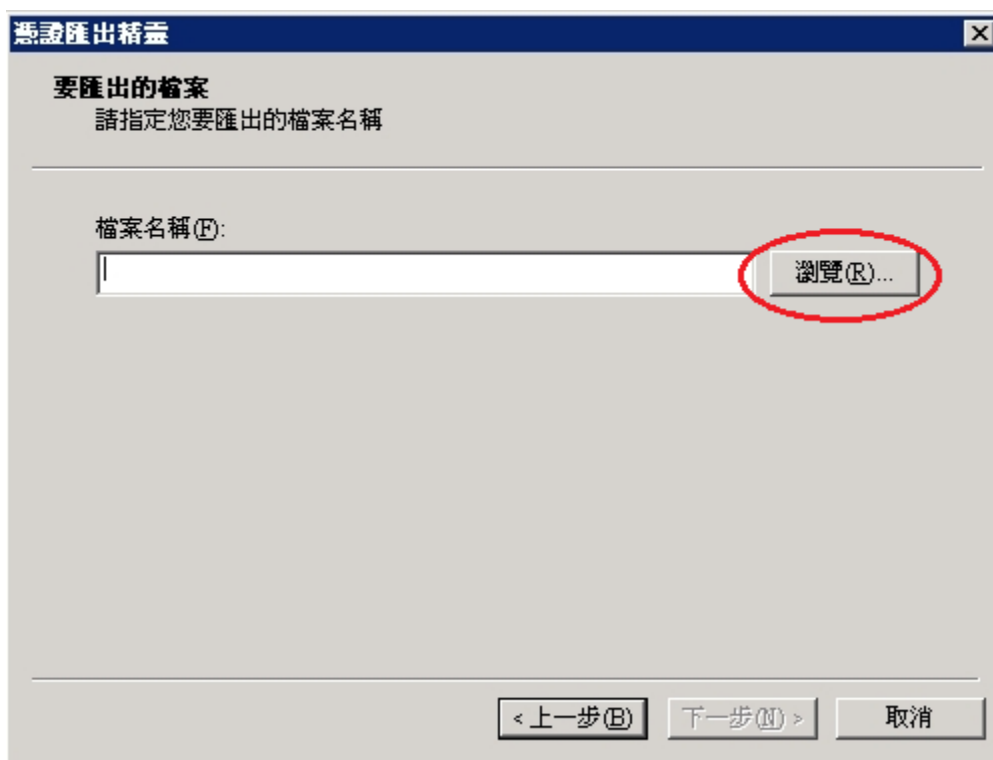


接著出現「密碼」頁面，輸入保護私密金鑰的密碼。請務必記住此密碼，到時需要將金鑰刪除產製新金鑰後需要將原來私密金鑰及憑證匯回時，就要輸入此密碼。輸入密碼完成後，接著以滑鼠按下「下一步」按鈕。

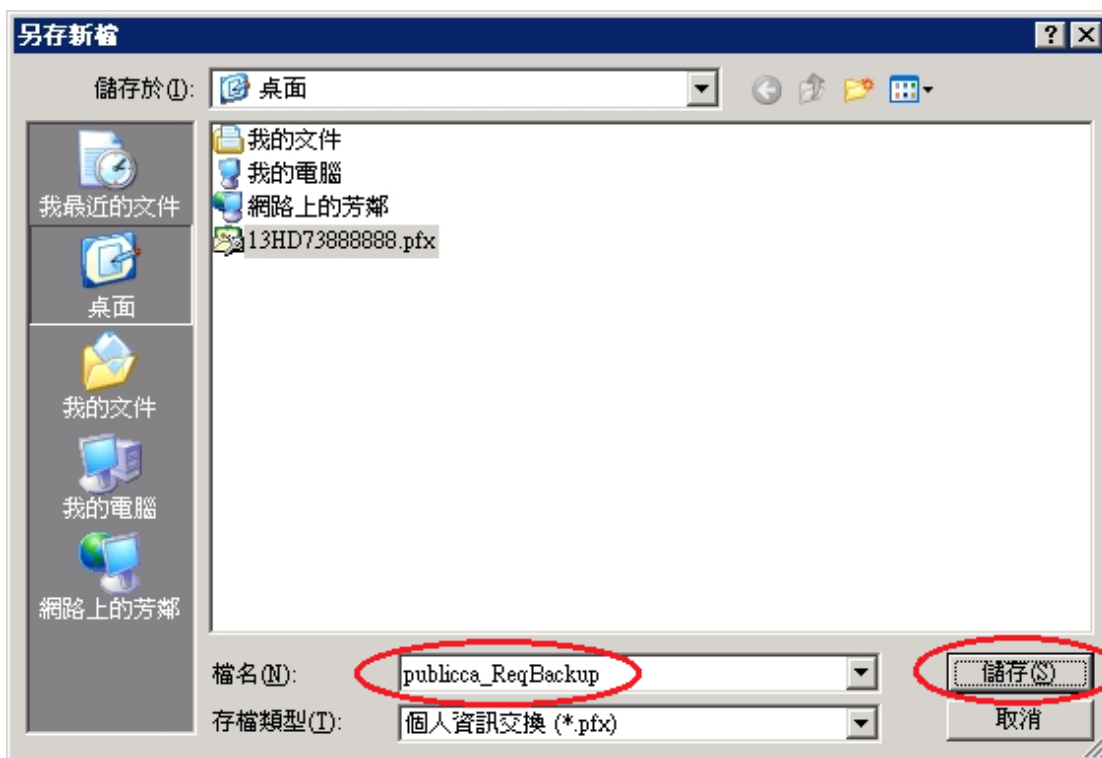


接著出現「要匯出的檔案」頁面，點選「瀏覽」選擇存放位置，或直接在「檔

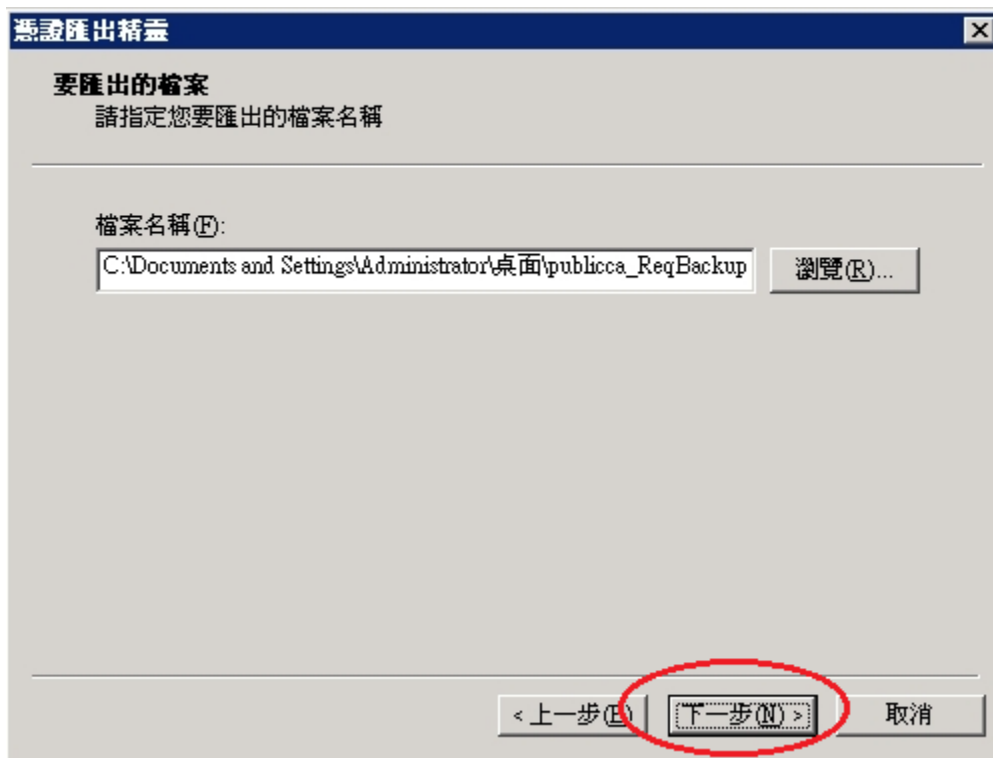
案名稱(F)」打上路徑及檔案名稱也可以。



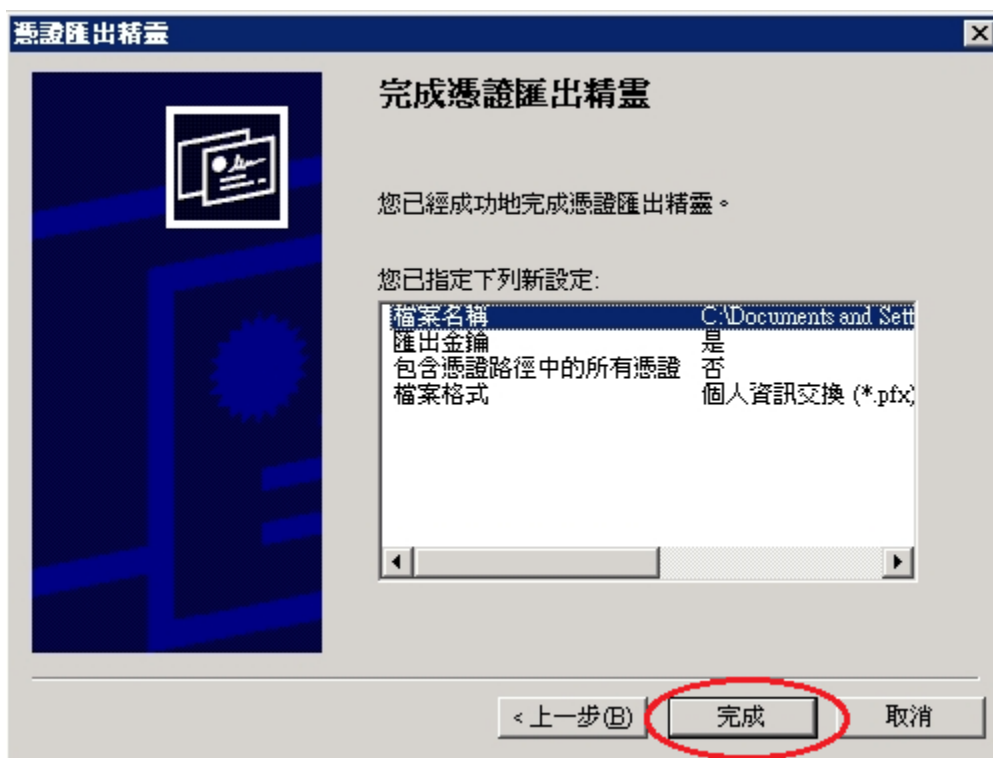
如果有按下「瀏覽」，則可選擇檔案路徑及輸入所要儲存的私密金鑰及憑證.pfx 檔檔名。輸入完成後，按下儲存後，接著會跳回「要匯出的檔案」頁面，並於頁面上出現存放檔案路徑及檔案名稱。



輸入完成後，接著以滑鼠按下「下一步」按鈕。



接著出現「完成憑證匯出精靈」頁面，按下「完成」以完成匯出私密金鑰及憑證動作。

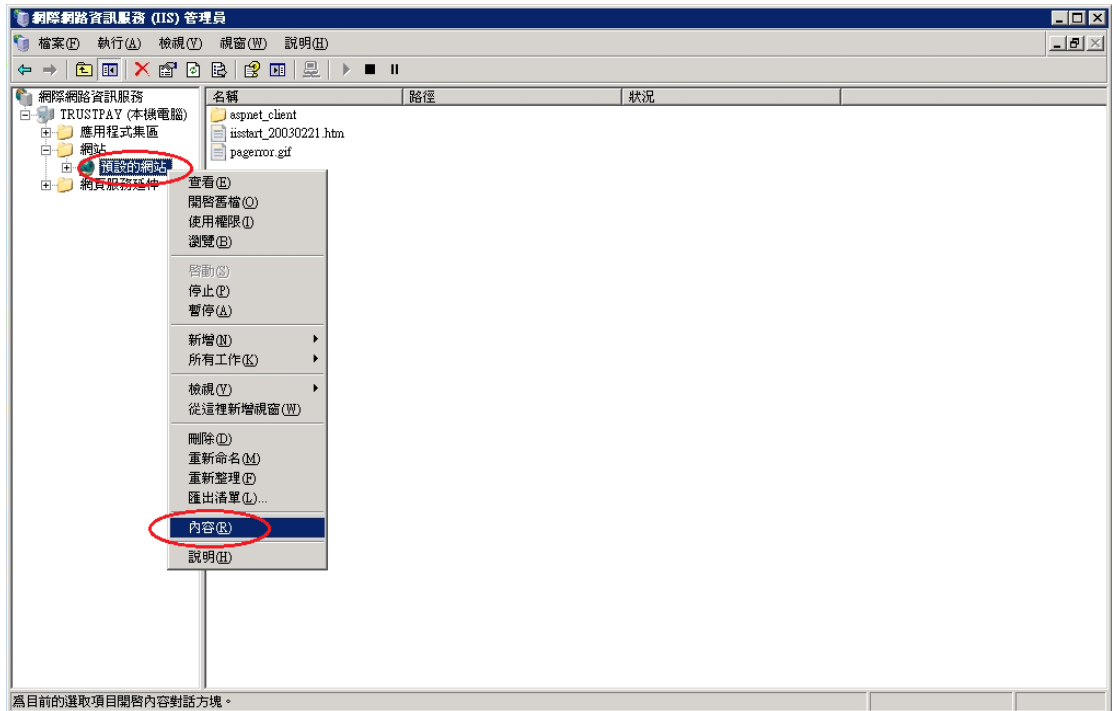


如果匯出完成，會出現如下訊息「匯出成功」。

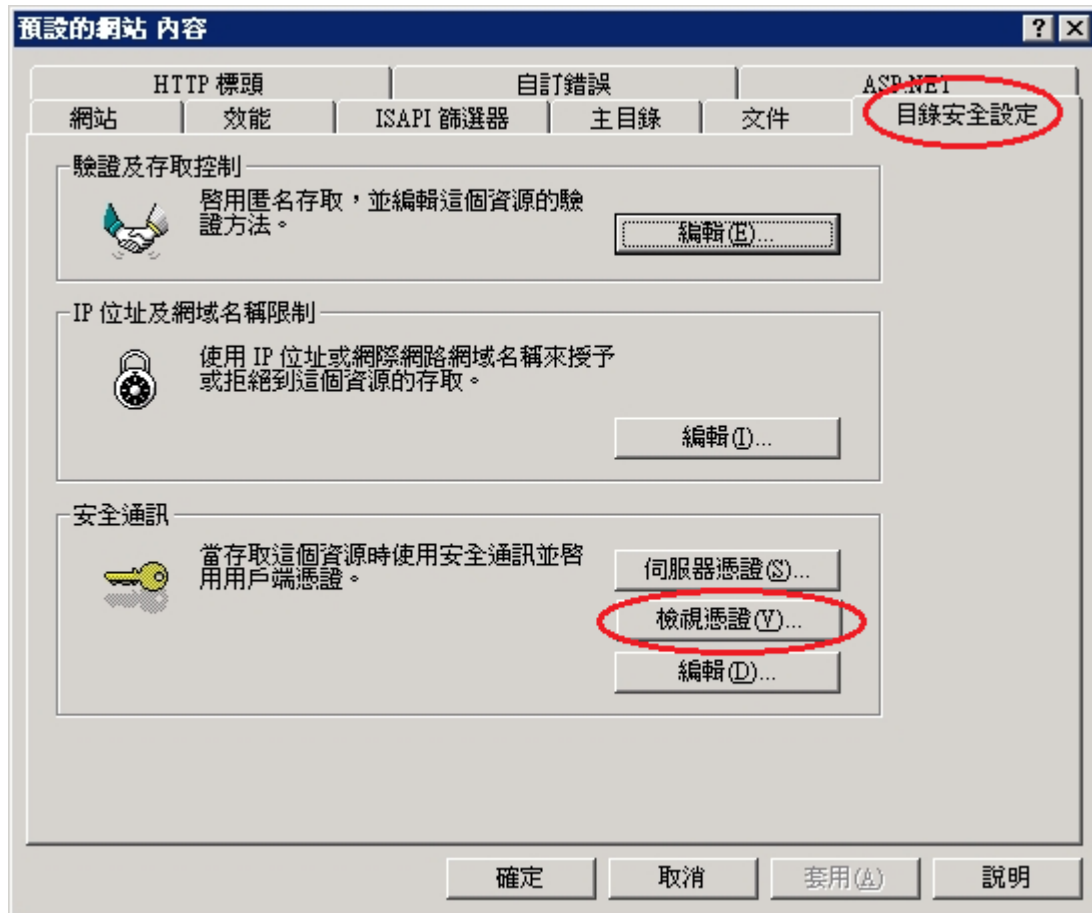


三、刪除原來的私密金鑰及憑證。

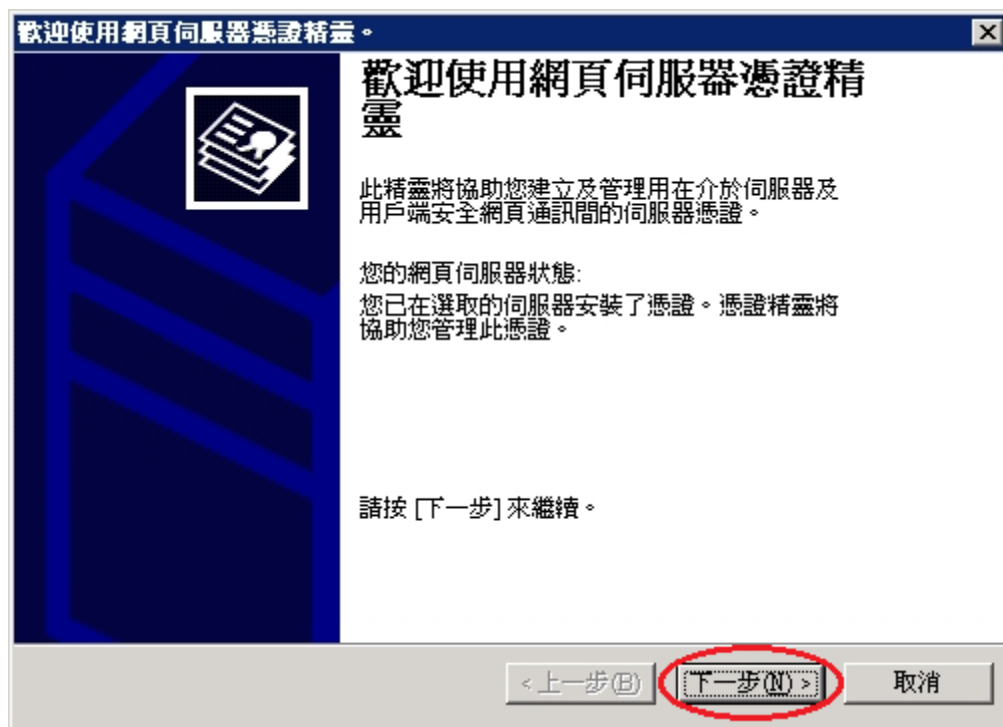
於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。



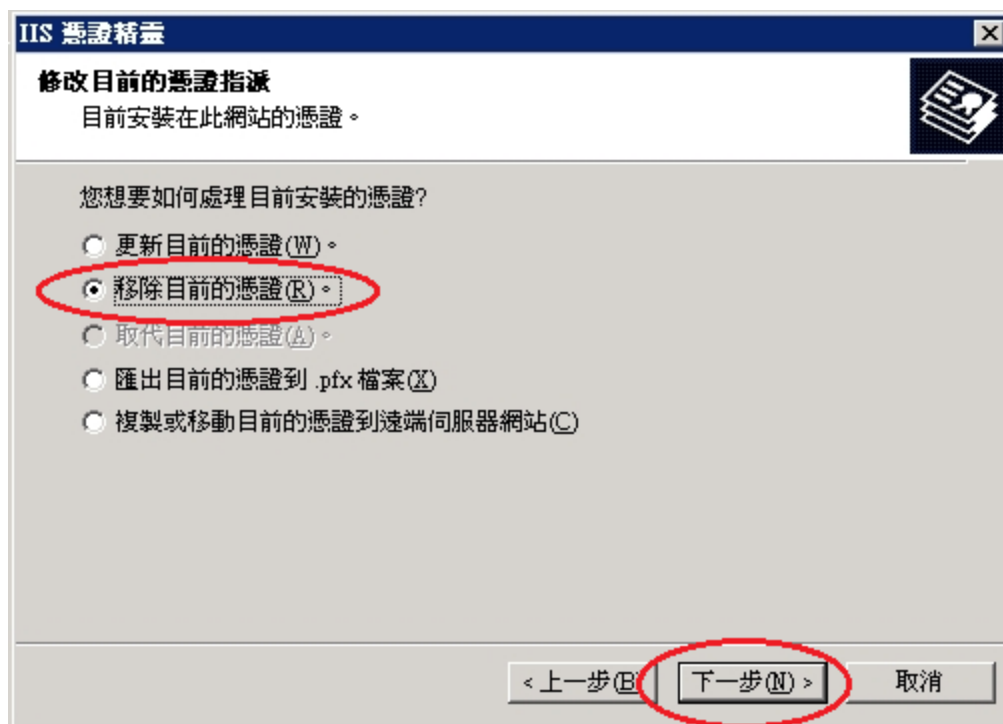
接著將頁面切到「目錄安全設定」頁面，在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。



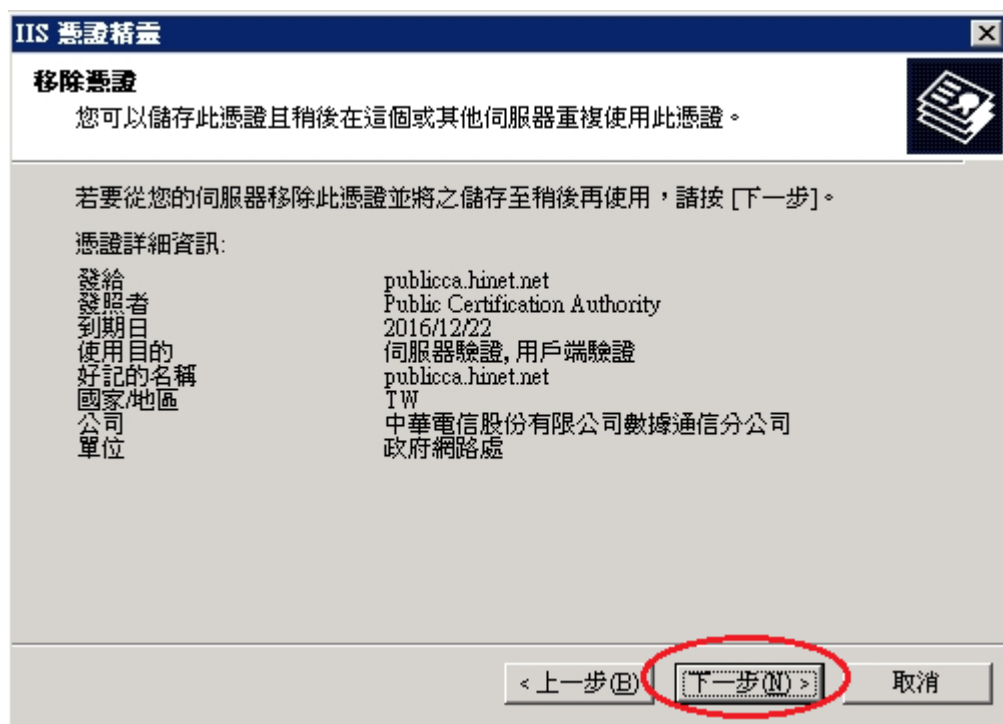
接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，按下「下一步」後，開始刪除原來的私密金鑰及憑證。



接著出現「修改目前的憑證指派」頁面，選擇「移除目前的憑證」，接著按下「下一步」。



接著出現「移除憑證」頁面，頁面上會顯示目前憑證的詳細資訊，請務必執行之前的私密金鑰及憑證備份後，才可執行此步驟移除憑證，否則憑證一移除，將無法救回，接著按下「下一步」。



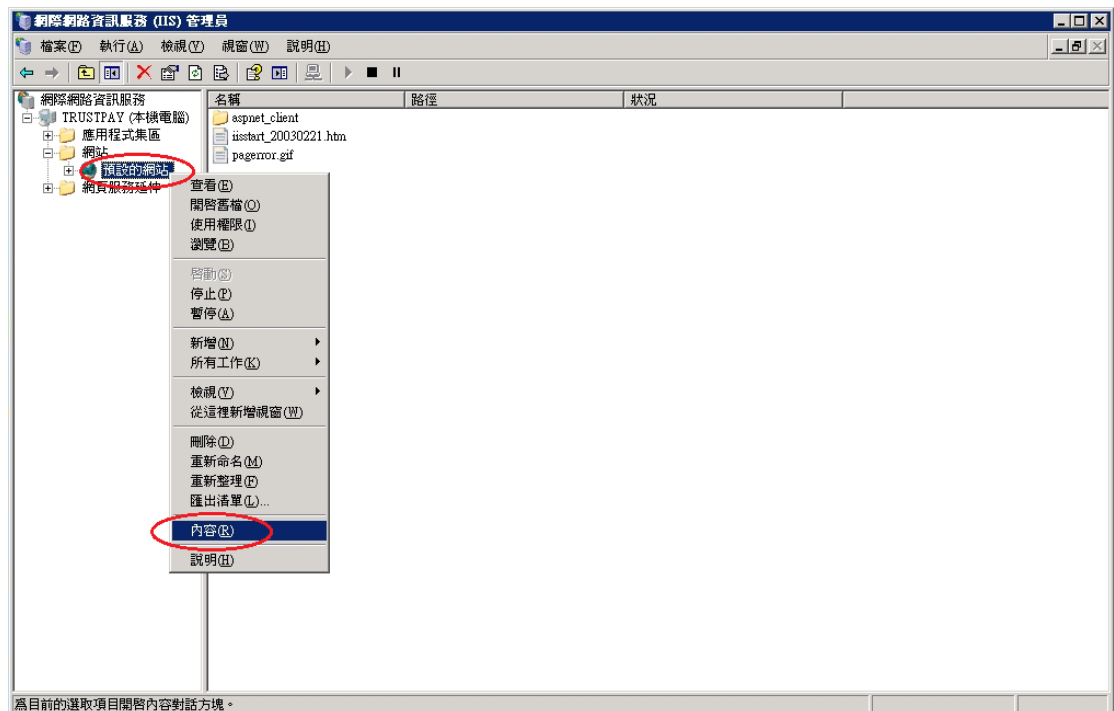
接著出現「正在完成網頁伺服器憑證精靈」頁面，按下「完成」以完成刪除

憑證動作。

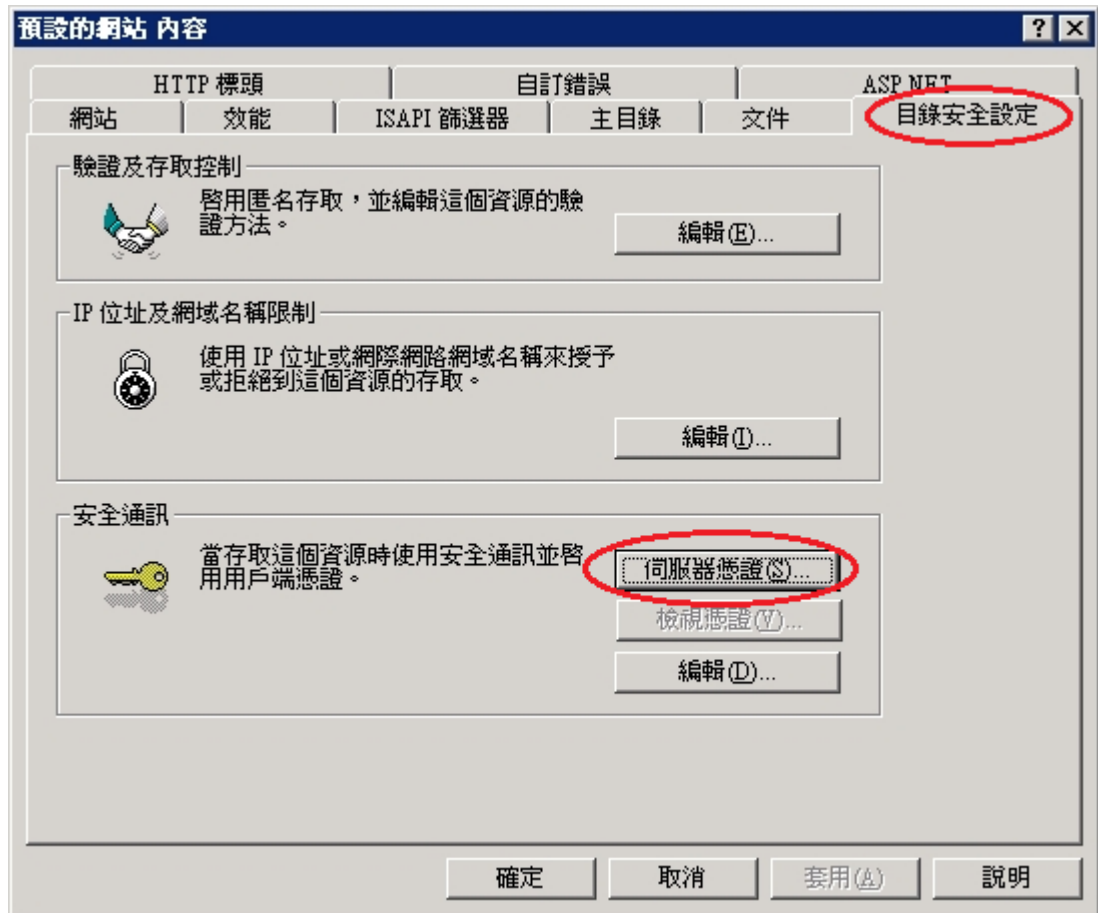


四、開始產製私密金鑰及憑證。

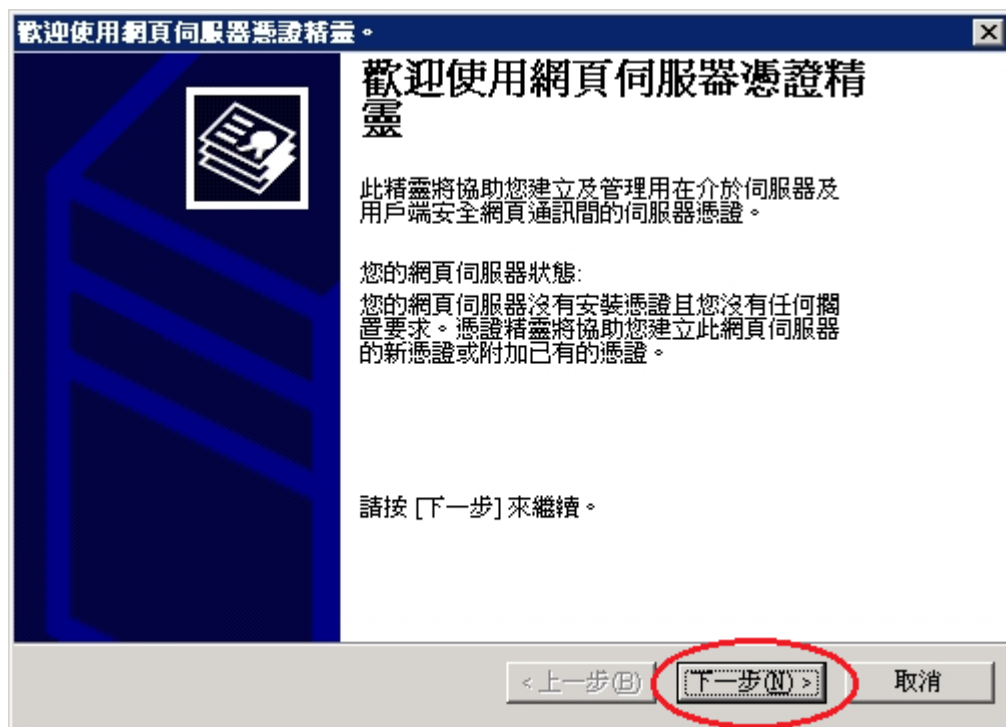
於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。



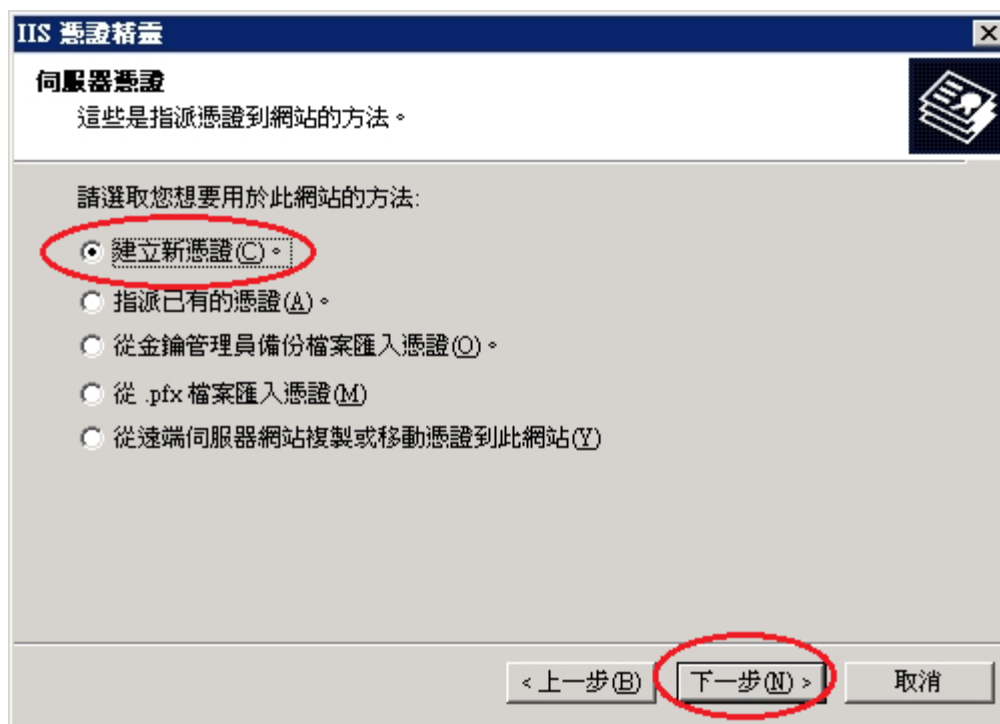
接著將頁面切到「目錄安全設定」頁面，在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。



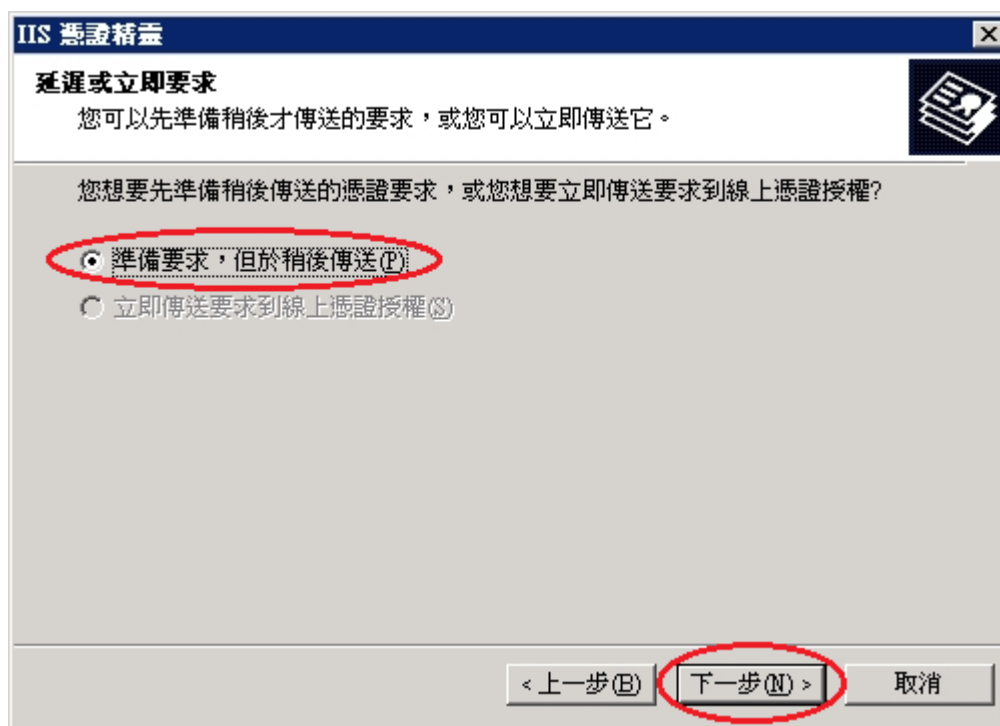
接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，以滑鼠按下「下一步」按鈕，開始製作 Windows 2003 IIS 6.0 伺服器憑證請求檔。



接著畫面會到「伺服器憑證」視窗，以滑鼠點選「建立新憑證」，接著以滑鼠按下「下一步」按鈕。

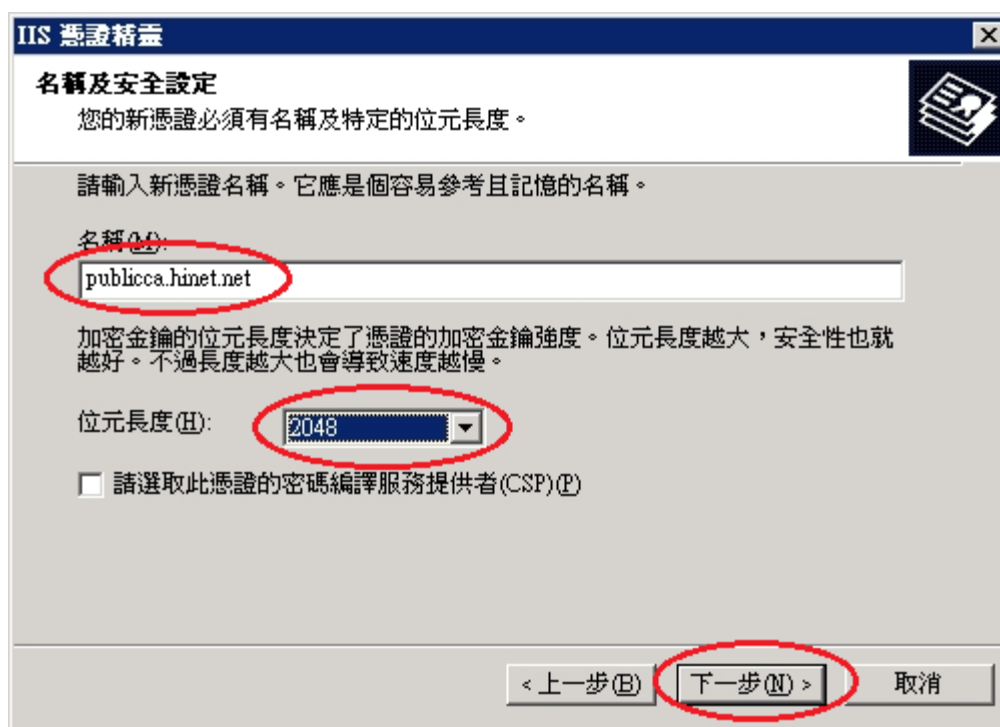


接著畫面會到「延遲或立即要求」視窗，以滑鼠點選「準備要求，但稍後再傳送(P)」，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「名稱及安全設定」視窗，以滑鼠點選「名稱(M)」欄位後並輸入網站名稱，接著以滑鼠點選「位元長度(H)」為「2048」bits 後，接著

以滑鼠按下「下一步」按鈕。



IIS 憑證精靈

名稱及安全設定

您的新憑證必須有名稱及特定的位元長度。

請輸入新憑證名稱。它應是個容易參考且記憶的名稱。

名稱(N):
publicca.hinet.net

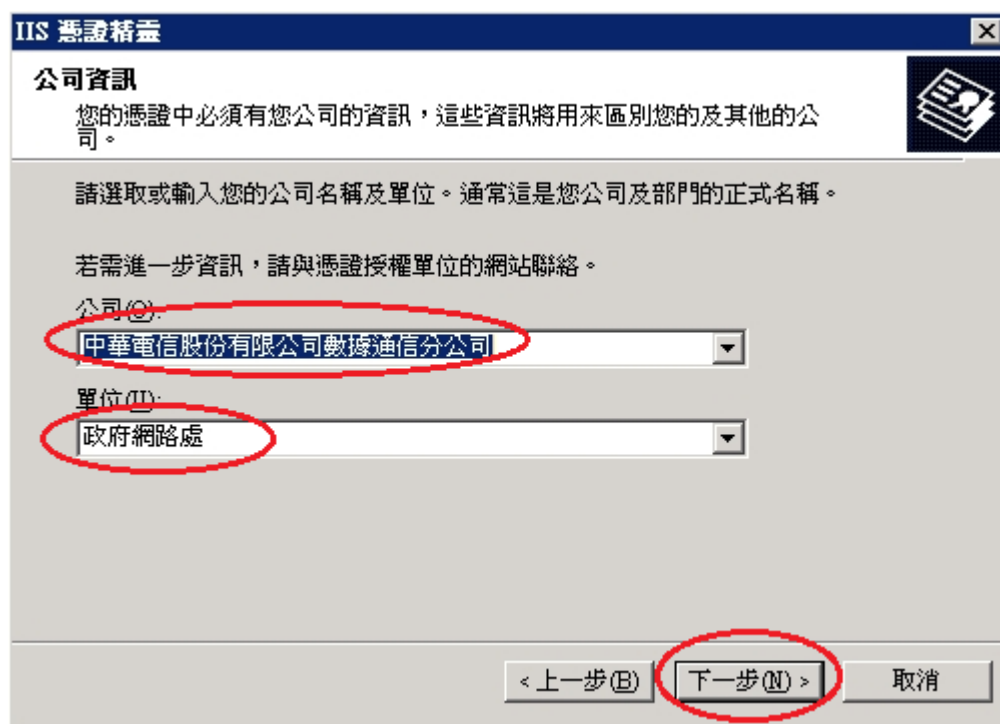
加密金鑰的位元長度決定了憑證的加密金鑰強度。位元長度越大，安全性也就越好。不過長度越大也會導致速度越慢。

位元長度(B): 2048

請選取此憑證的密碼編譯服務提供者(CSP)(P)

< 上一步(B) **下一步(N) >** 取消

接著畫面會到「公司資訊」視窗，以滑鼠點選「公司(O)」欄位後並輸入組織名稱或公司名稱，接著以滑鼠點選「單位(U)」欄位後並輸入組織或公司的單位名稱，接著以滑鼠按下「下一步」按鈕。



IIS 憑證精靈

公司資訊

您的憑證中必須有您公司的資訊，這些資訊將用來區別您的及其他的公司。

請選取或輸入您的公司名稱及單位。通常這是您公司及部門的正式名稱。

若需進一步資訊，請與憑證授權單位的網站聯絡。

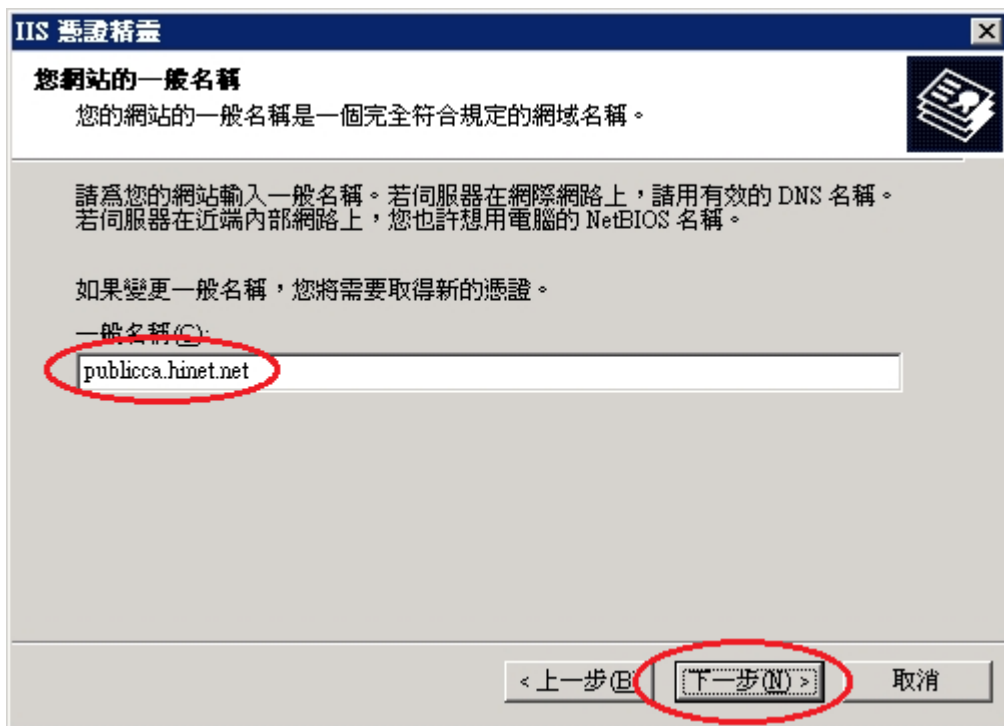
公司(O):
中華電信股份有限公司數據通信分公司

單位(U):
政府網路處

< 上一步(B) **下一步(N) >** 取消

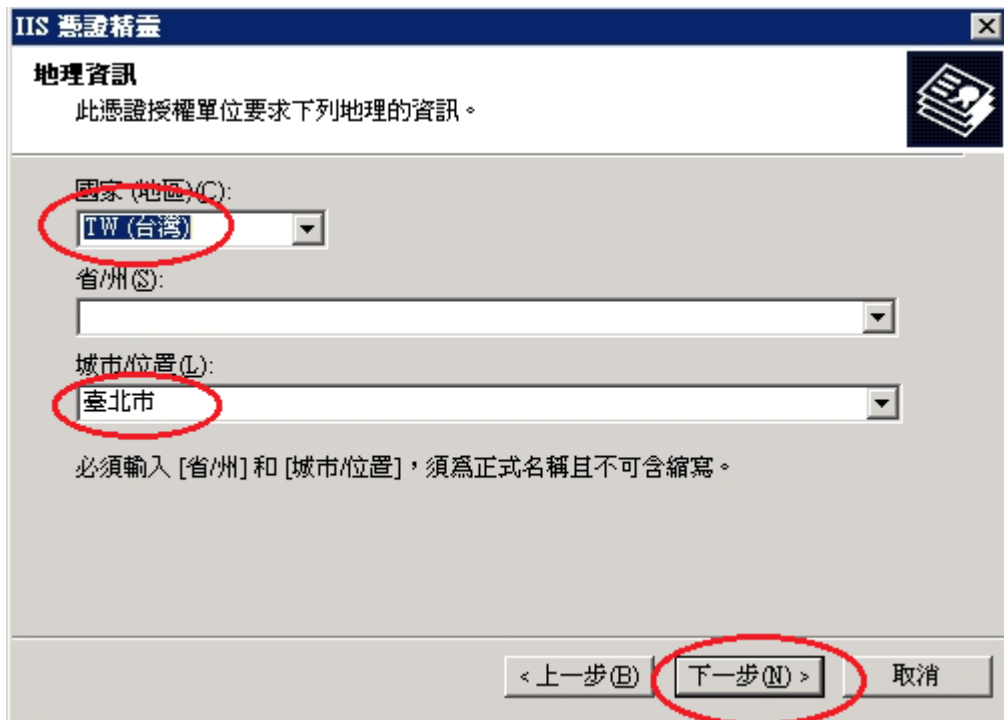
接著畫面會到「您網站的一般名稱」視窗，以滑鼠點選「一般名稱(C)」欄位後並輸入一般名稱(即網站的網址「Domain Name」)，接著以滑鼠按下「下

一步」按鈕。



The screenshot shows the 'IIS 憑證精靈' (IIS Wizard) window at the '您網站的一般名稱' (General Name) step. The title bar reads 'IIS 憑證精靈'. The main heading is '您網站的一般名稱' (General Name of your website). Below the heading, there is a text box containing 'publicca.hinet.net'. At the bottom of the window, there are three buttons: '< 上一步(B)' (Previous), '下一步(N) >' (Next), and '取消' (Cancel). The 'Next' button is circled in red.

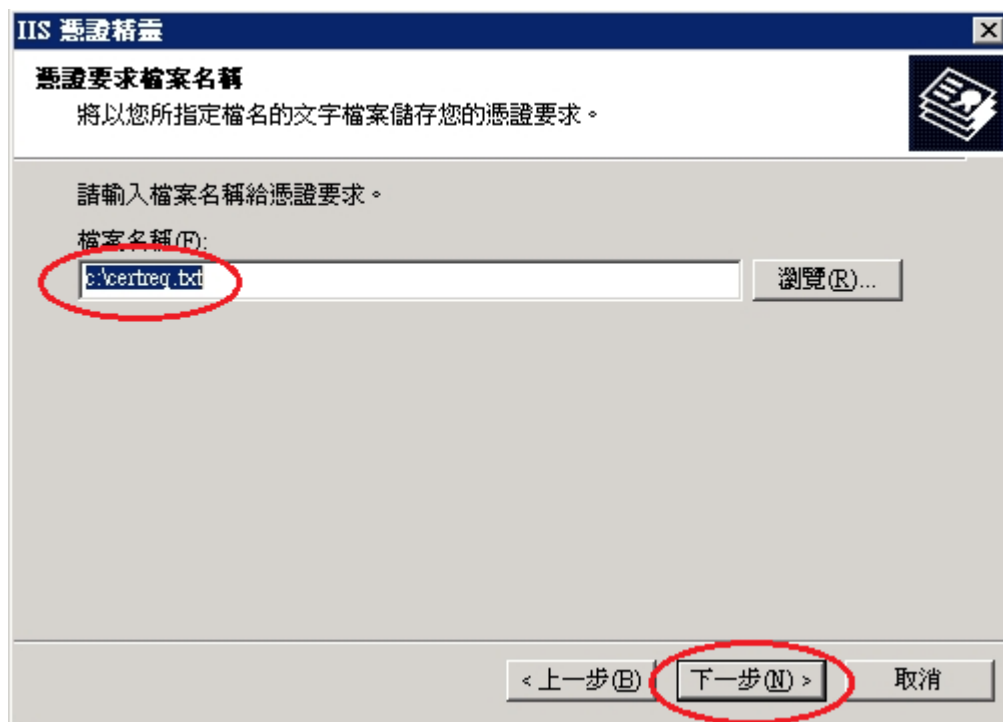
接著畫面會到「地理資訊」視窗，接著以滑鼠點選「國家(地區)(C)」，以滑鼠點選「TW(台灣)」，接著以滑鼠點選「州/省(S)」欄位後依照所在地輸入正確的州/省名稱，如圖為輸入「空白」或輸入「臺灣省」亦可，接著以滑鼠點選「城市/位置(L)」欄位後依照所在地輸入正確的城市名稱，如圖為輸入「臺北市」，接著以滑鼠按下「下一步」按鈕。



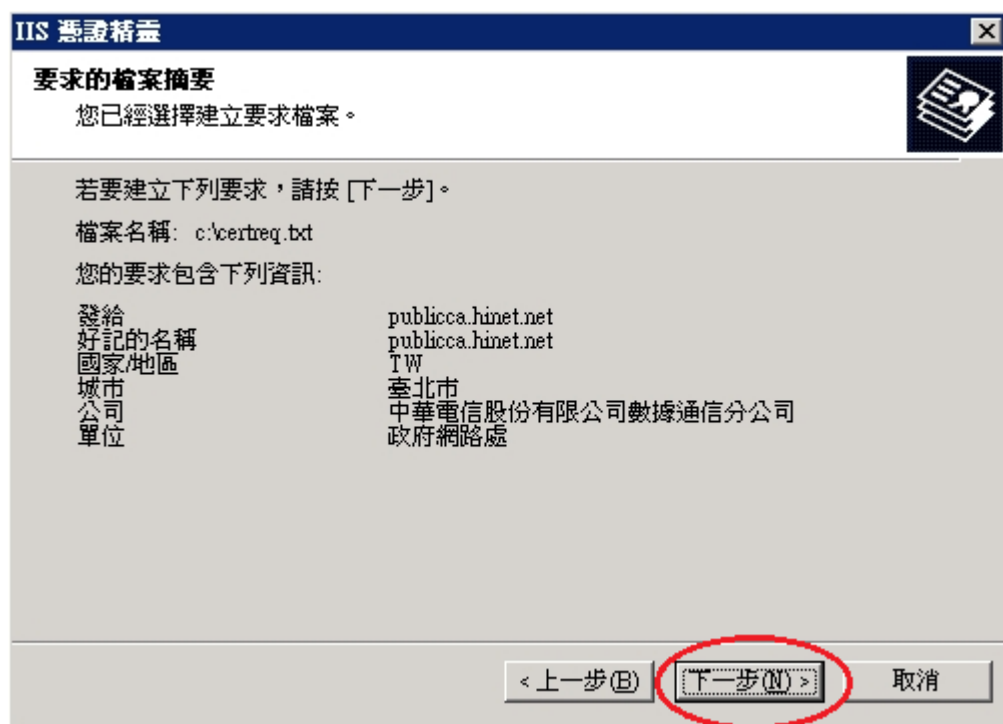
The screenshot shows the 'IIS 憑證精靈' (IIS Wizard) window at the '地理資訊' (Geographic Information) step. The title bar reads 'IIS 憑證精靈'. The main heading is '地理資訊' (Geographic Information). Below the heading, there is a text box containing '此憑證授權單位要求下列地理的資訊。' (This certificate authority requires the following geographic information). There are three dropdown menus: '國家(地區)(C):' (Country/Region) with 'TW(台灣)' selected, '省/州(S):' (State/Province) which is empty, and '城市/位置(L):' (City/Location) with '臺北市' selected. At the bottom of the window, there are three buttons: '< 上一步(B)' (Previous), '下一步(N) >' (Next), and '取消' (Cancel). The 'Next' button is circled in red.

接著畫面會到「憑證要求檔案名稱」視窗，接著以滑鼠點選「檔案名稱(F)」

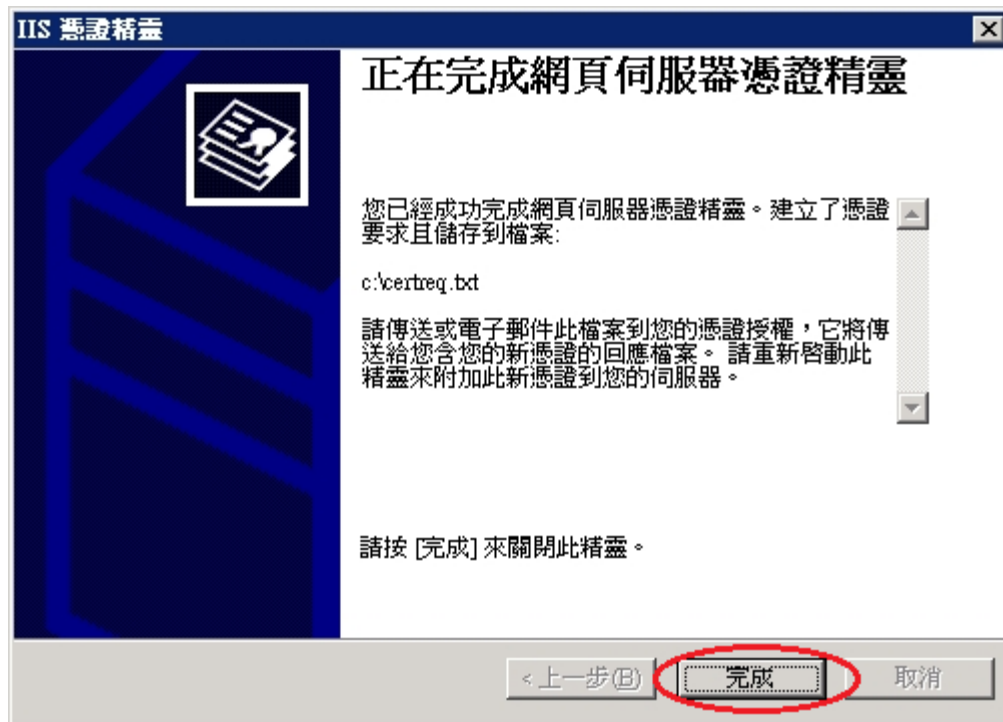
欄位後並輸入路徑及要存的檔案名稱，如下圖所示，通常都是依照如下圖之預設值路徑及檔案名稱存放，接著以滑鼠按下「下一步」按鈕。



接著畫面會到「要求的檔案摘要」視窗，檢視剛才各步驟所設定的值是否無誤，如果沒有問題，接著以滑鼠按下「下一步」按鈕。

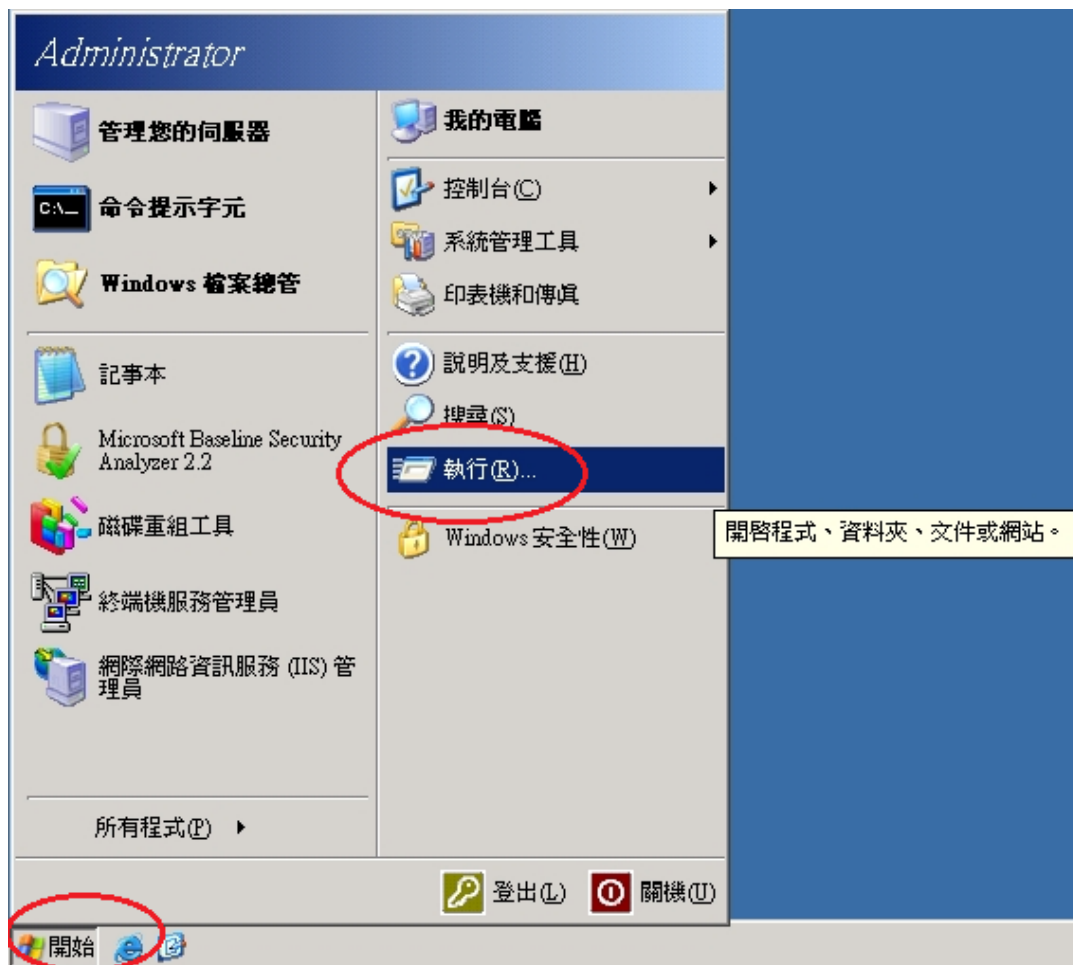


接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成結束製作憑證請求檔動作。

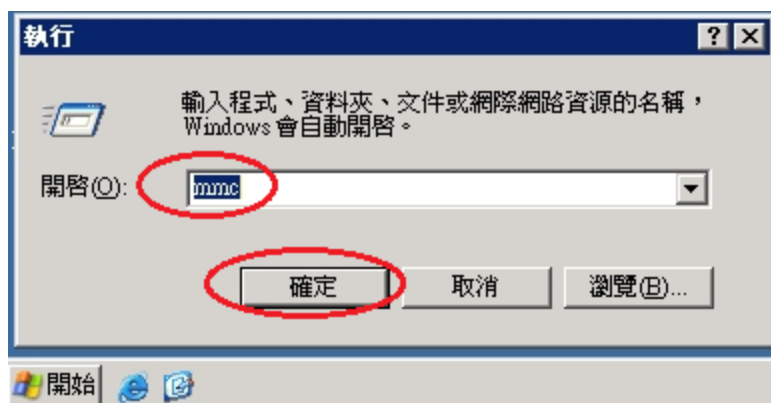


五、備份產製私密金鑰及憑證請求檔後的私密金鑰及憑證檔。

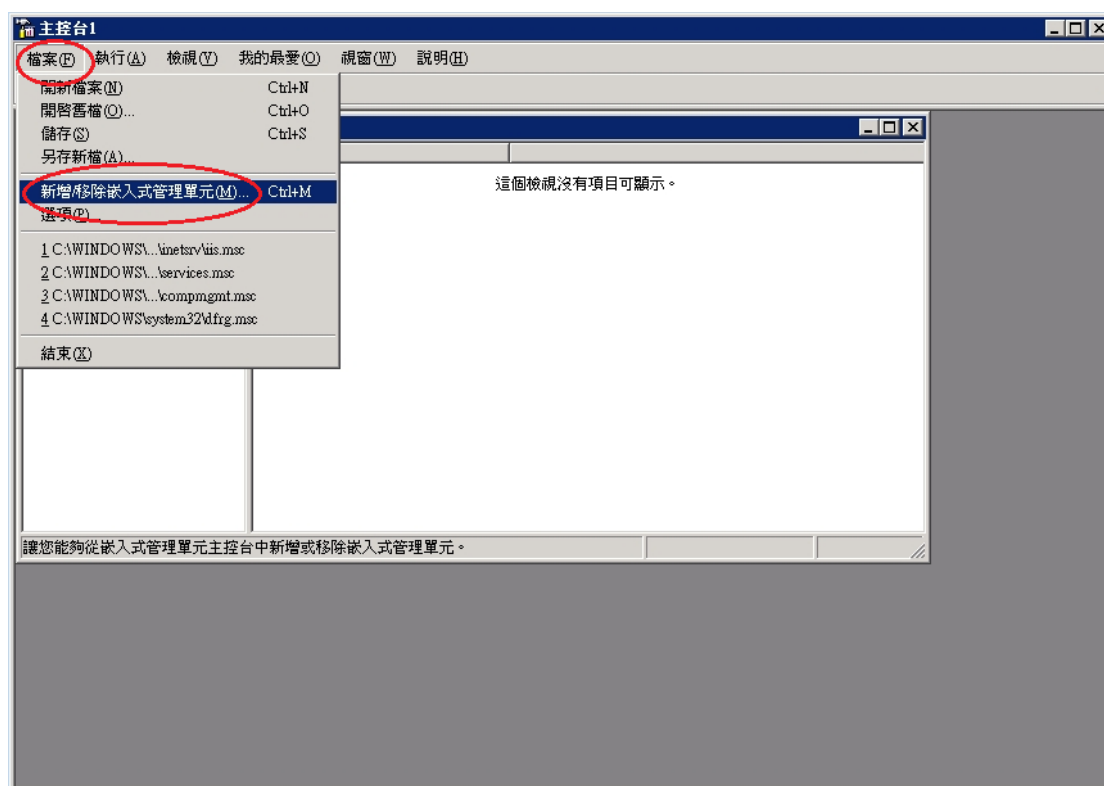
點選「開始」→「執行」



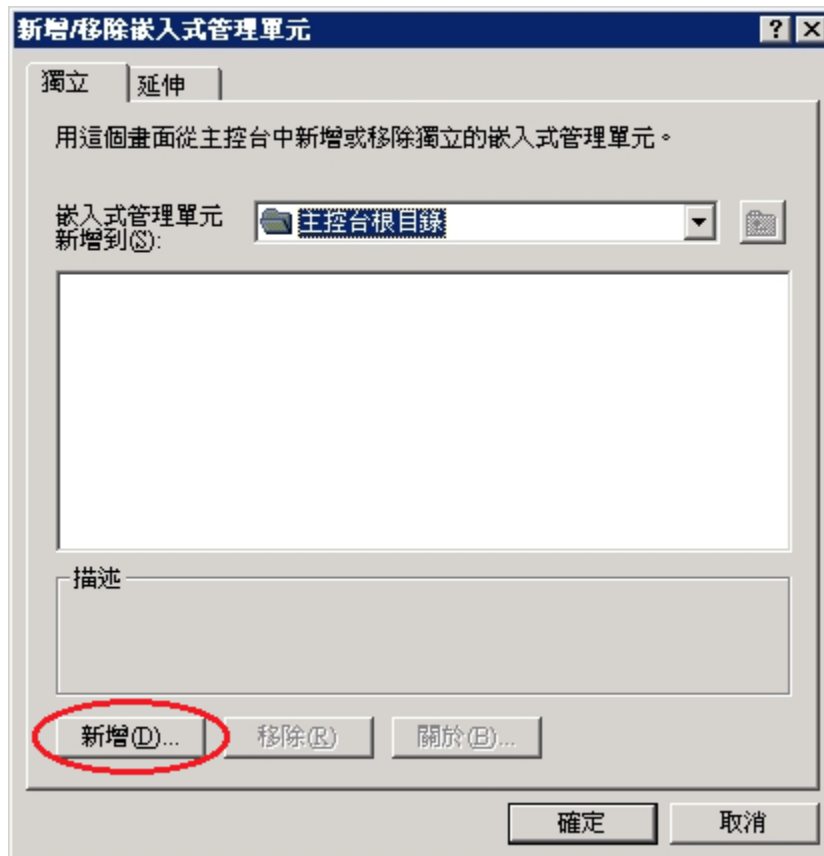
於「開啟(O)」欄位輸入 mmc 後，按下「確定」按鈕。



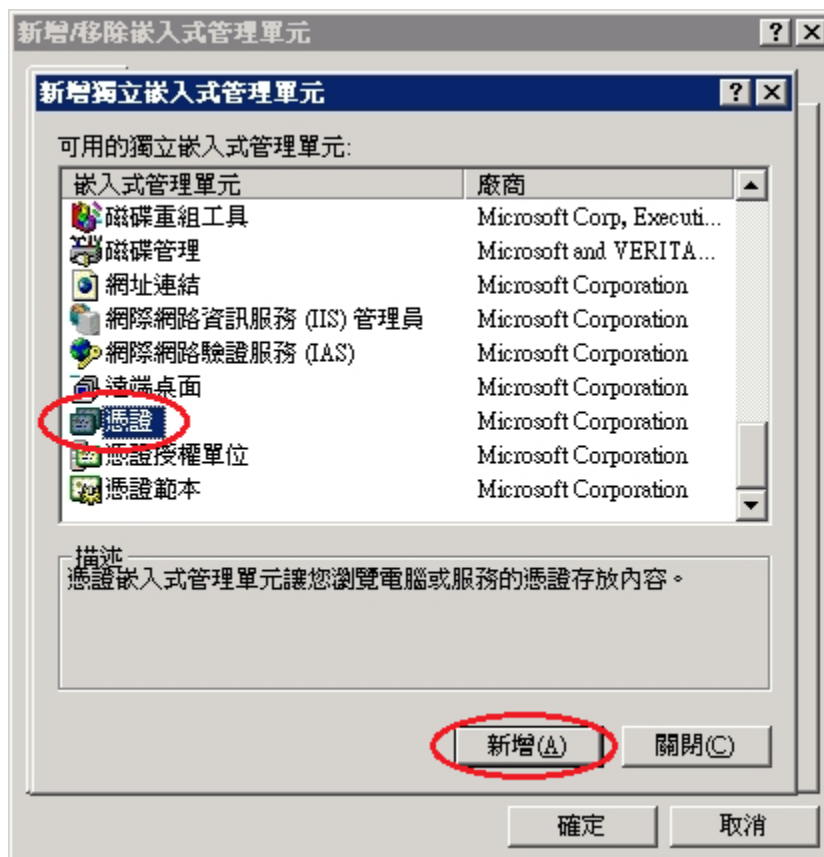
於主控台點選「檔案」→「新增/移除嵌入式管理單元」。



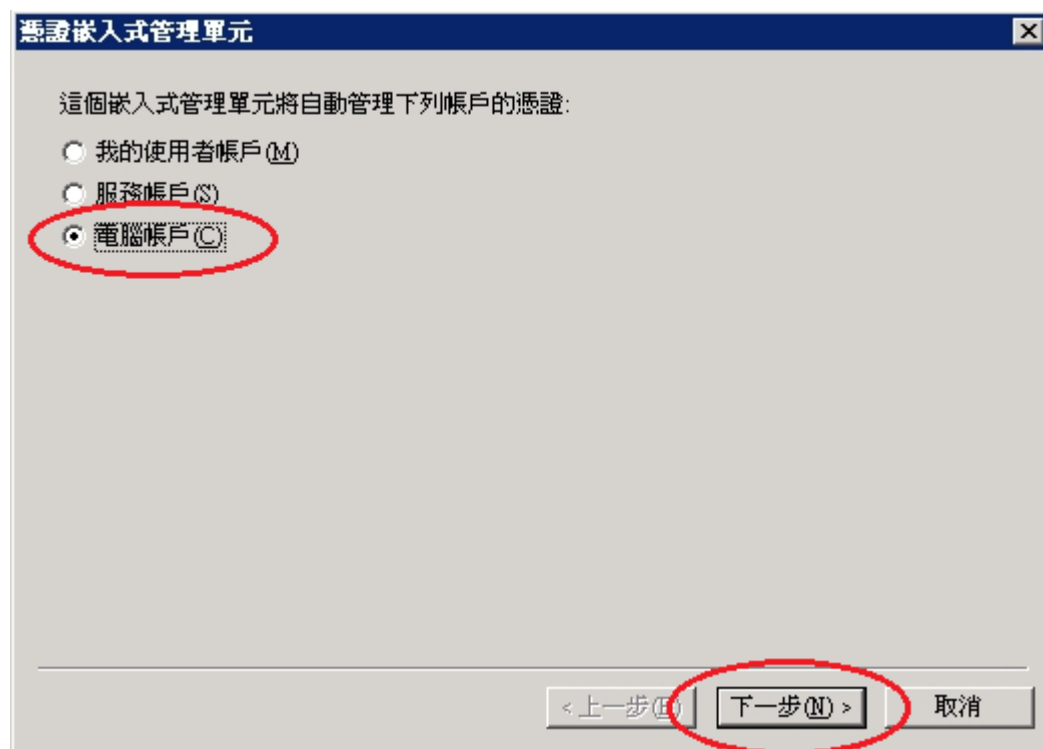
接著出現「新增/移除嵌入式管理單元」畫面，點選「新增」按鈕。



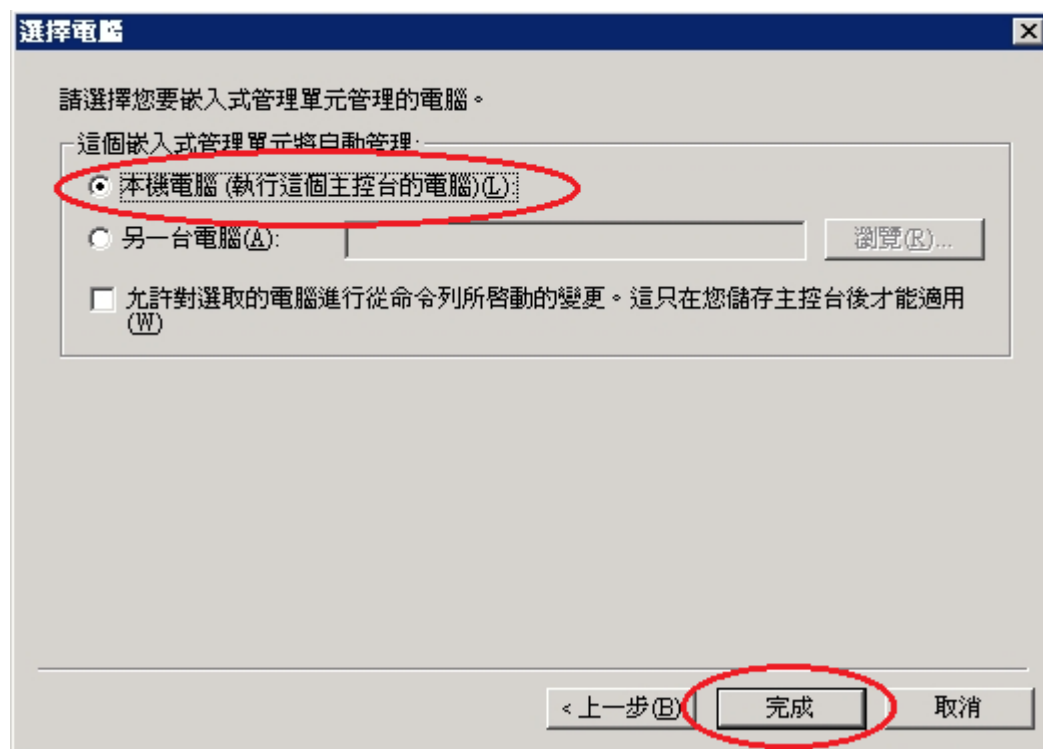
接著出現「新增獨立嵌入式管理單元」畫面，於「可用的獨立嵌入式管理單元」點選「憑證」項目後，按下「新增」按鈕。



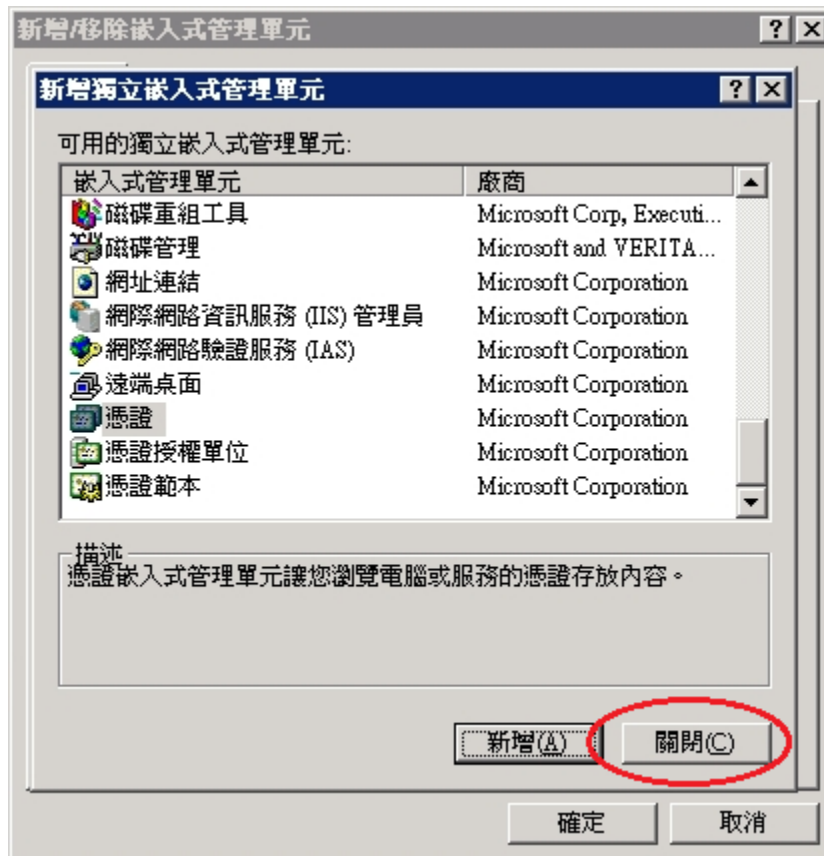
接著出現「憑證嵌入式管理單元」畫面，於「這個嵌入式管理單元將自動管理下列帳戶的憑證:」點選「電腦帳戶」後，點選「下一步」按鈕。



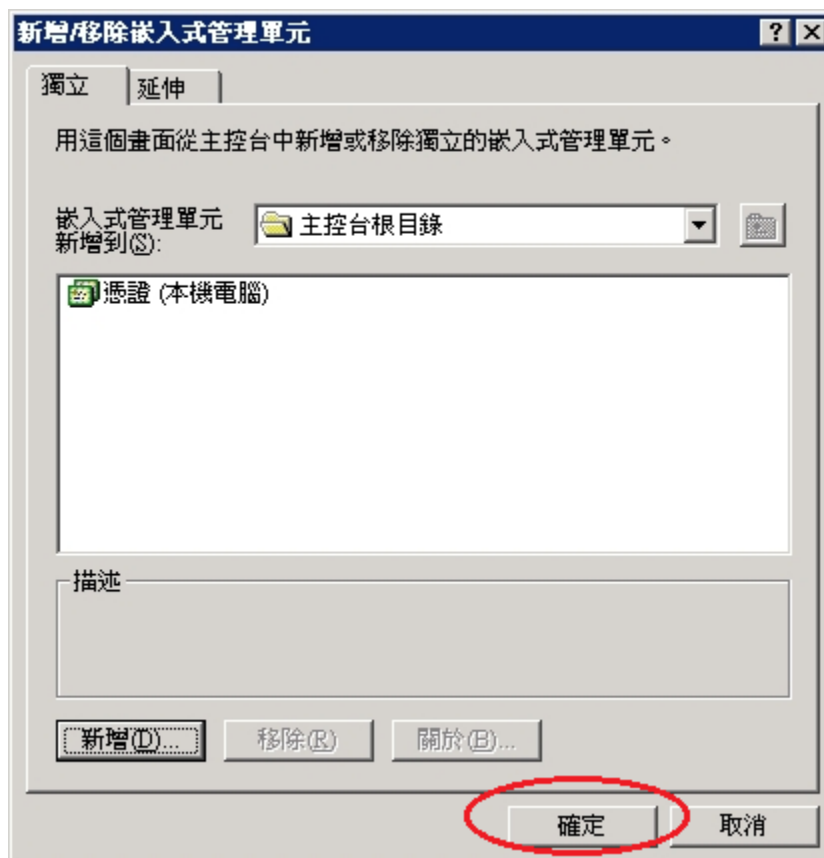
接著出現「選擇電腦」畫面，於「這個嵌入式管理單元將自動管理:」點選「本機電腦(執行這個主控台的電腦)(L)」後，點選「完成」按鈕。



回到「新增獨立嵌入式管理單元」畫面，點選「關閉」按鈕。

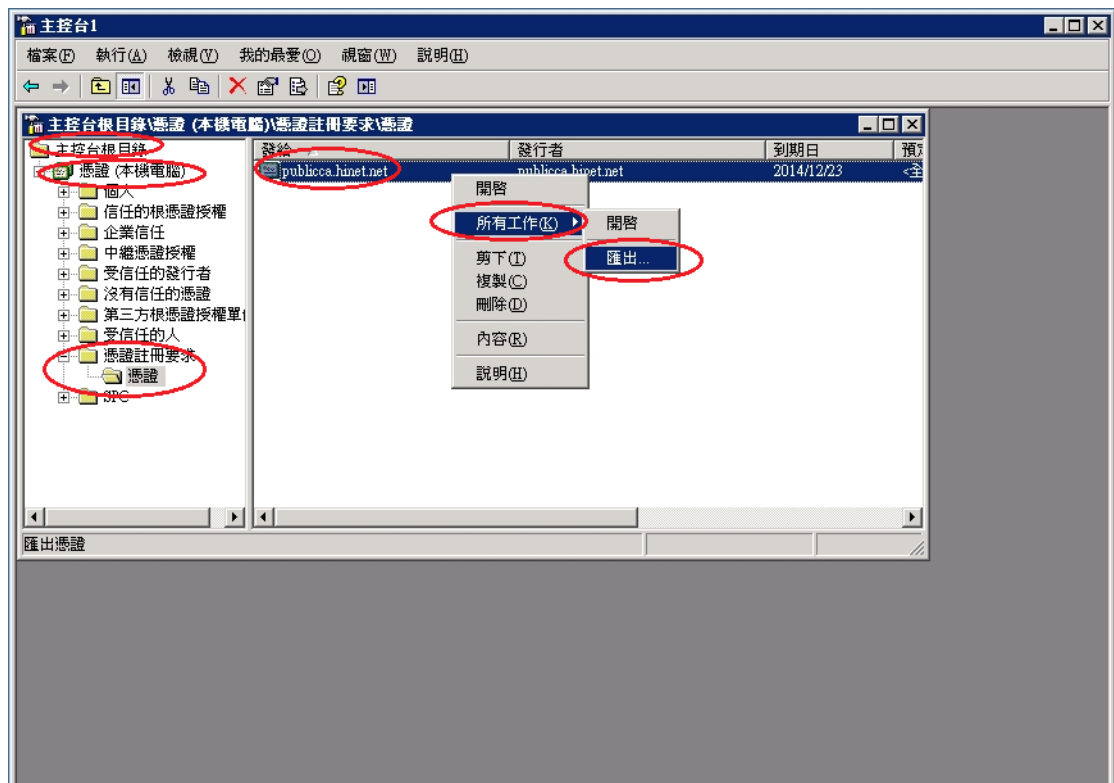


回到「新增/移除嵌入式管理單元」畫面，點選「確定」按鈕。

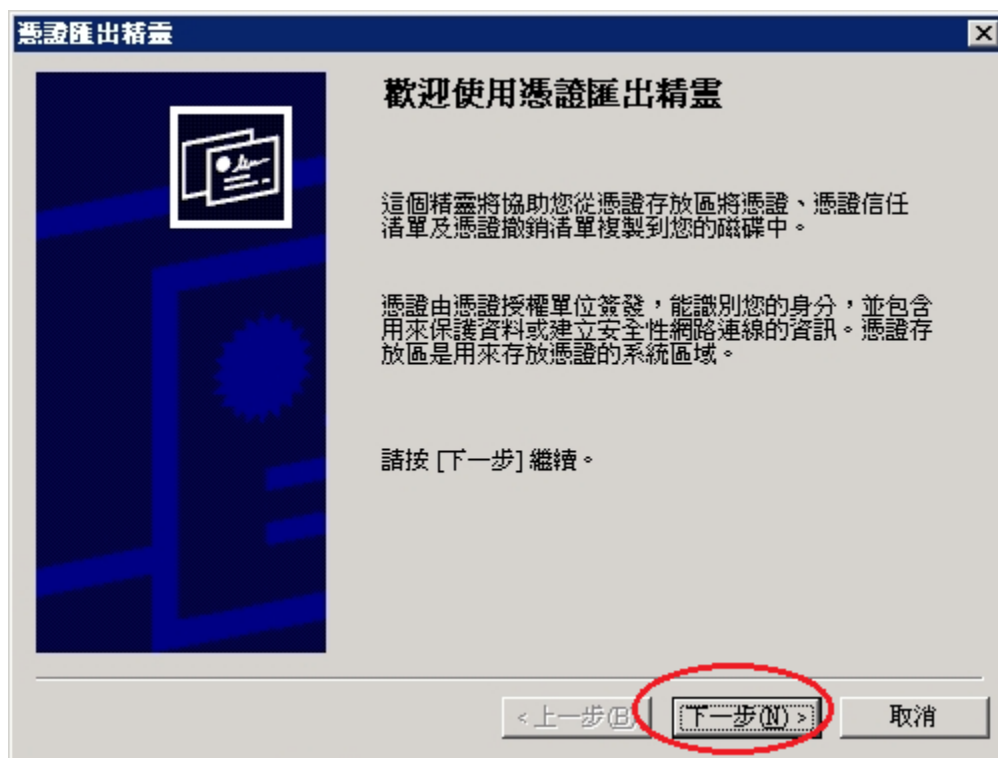


於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「憑證註冊要

求」→「憑證」找到產生憑證請求檔的憑證及私密金鑰，以滑鼠右鍵點選該「憑證請求檔的私密金鑰及憑證」，接著點選「所有工作(K)」→「匯出」。

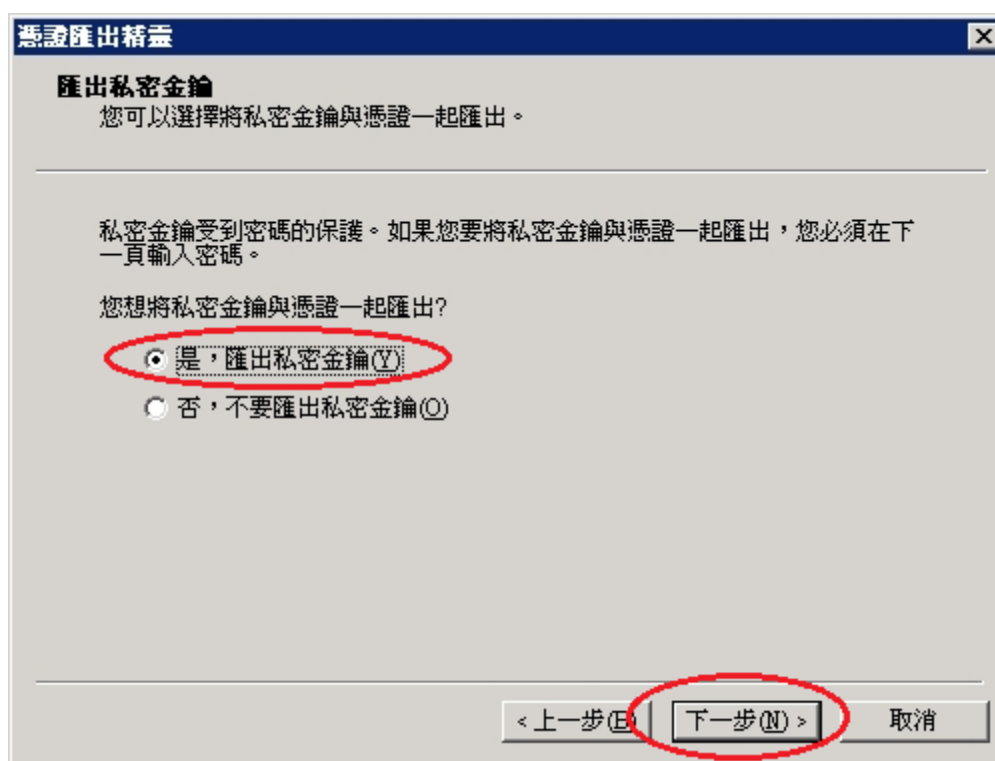


接著出現「憑證匯出精靈」畫面，於「歡迎使用憑證匯出精靈」點選「下一步」按鈕。

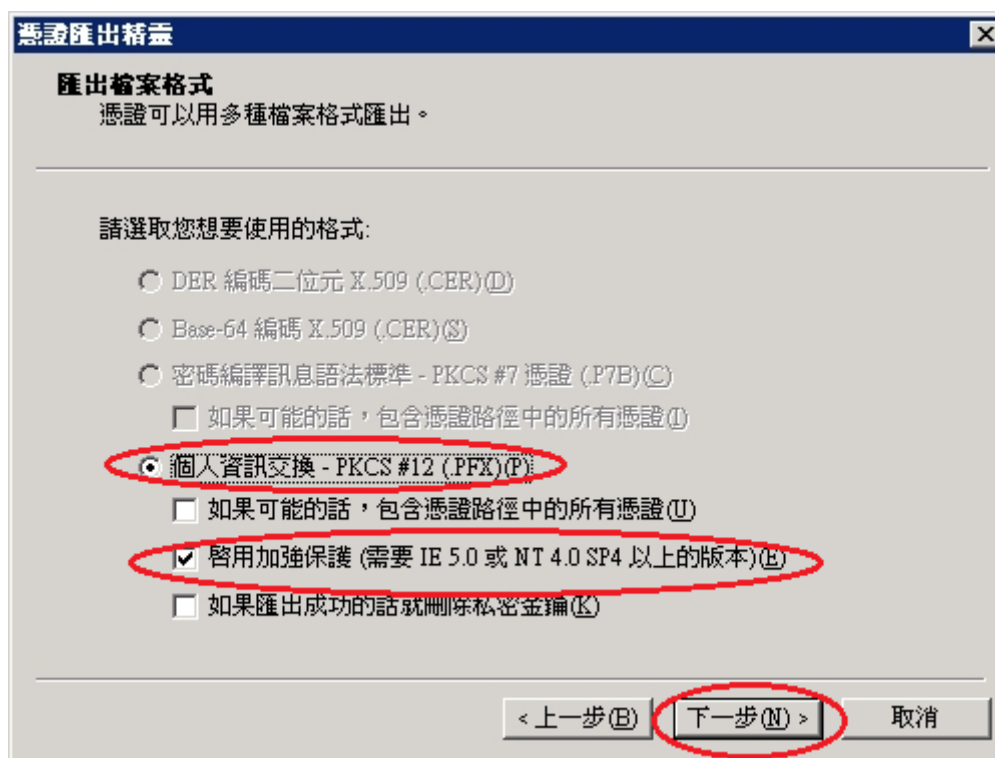


接著出現「憑證匯出精靈」，「匯出私密鑰」頁面選擇「是，匯出私密金鑰

(Y)」後，以滑鼠按下「下一步」按鈕。



接著出現「匯出檔案格式」頁面，選擇「個人資訊交換 - PKCS #12 (. PFX)(P)」，並勾選「啓用加強保護(需要 IE 5.0 或 NT 4.0 SP4 以上的版本)(E)」，接著以滑鼠按下「下一步」按鈕。



接著出現「密碼」頁面，輸入保護私密金鑰的密碼。請務必記住此密碼，到時需要將金鑰刪除產製新金鑰後需要將原來私密金鑰及憑證匯回時就要輸

入此密碼。輸入密碼完成後，接著以滑鼠按下「下一步」按鈕。

憑證匯出精靈

密碼
為了安全性，您必須使用密碼保護私密金鑰。

輸入並確認密碼。

密碼(P):

確認密碼(C):

< 上一步(B) 下一步(N) > 取消

接著出現「要匯出的檔案」頁面，點選「瀏覽」選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。

憑證匯出精靈

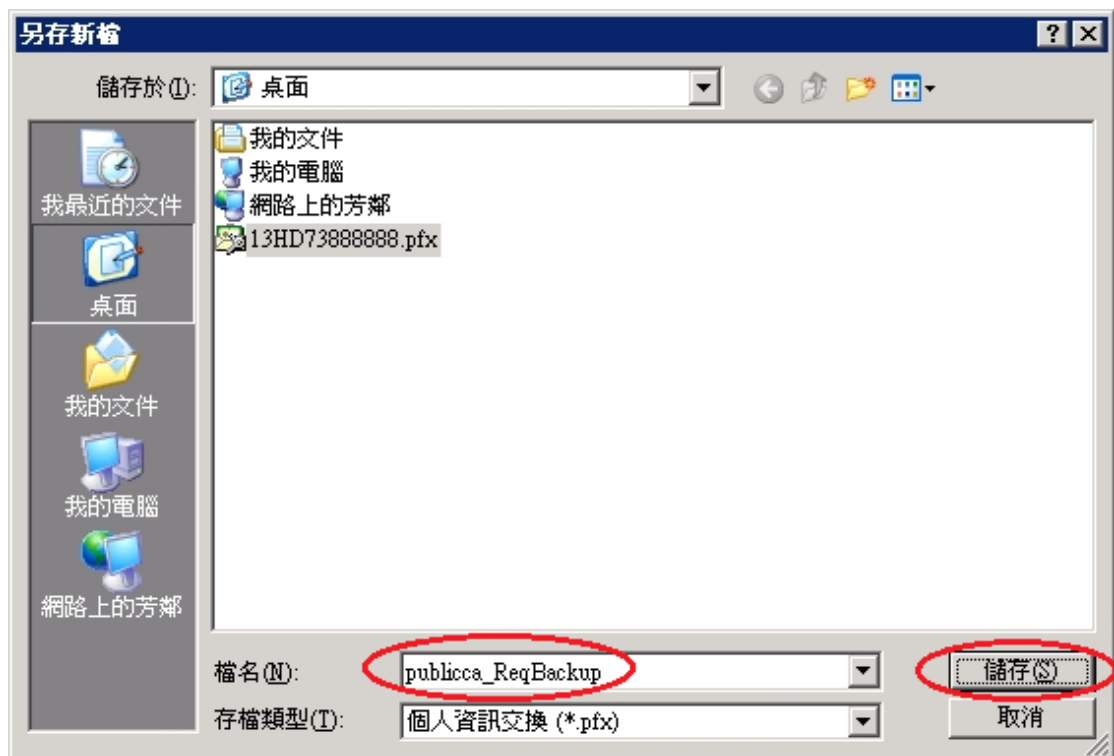
要匯出的檔案
請指定您要匯出的檔案名稱

檔案名稱(F):

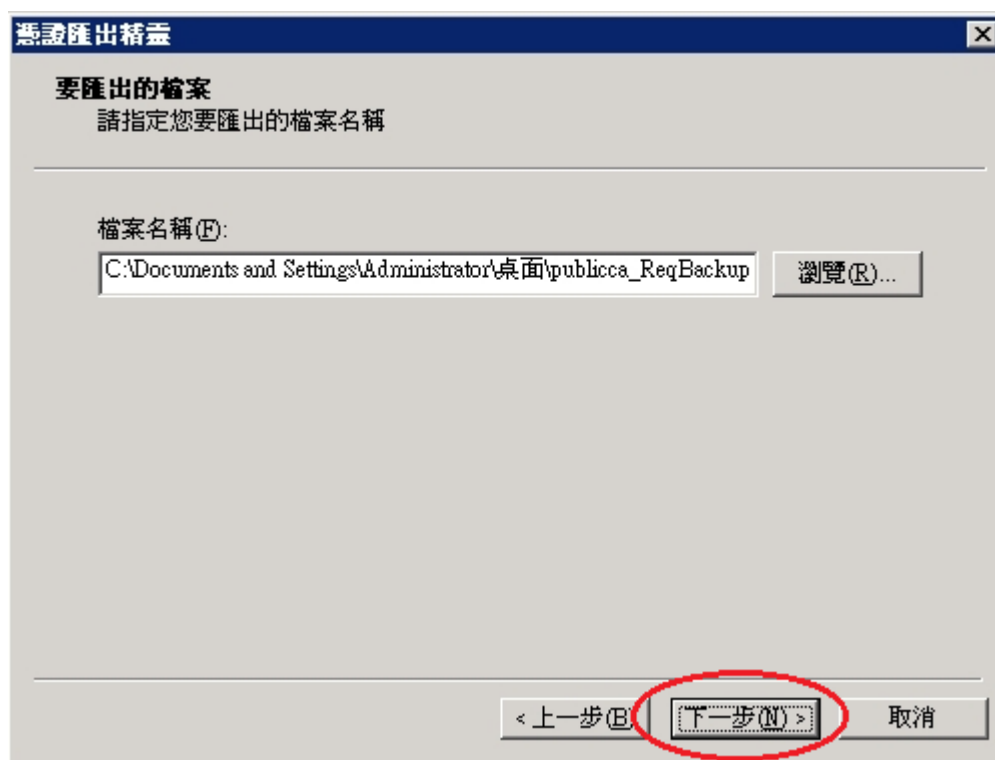
瀏覽(B)...

< 上一步(B) 下一步(N) > 取消

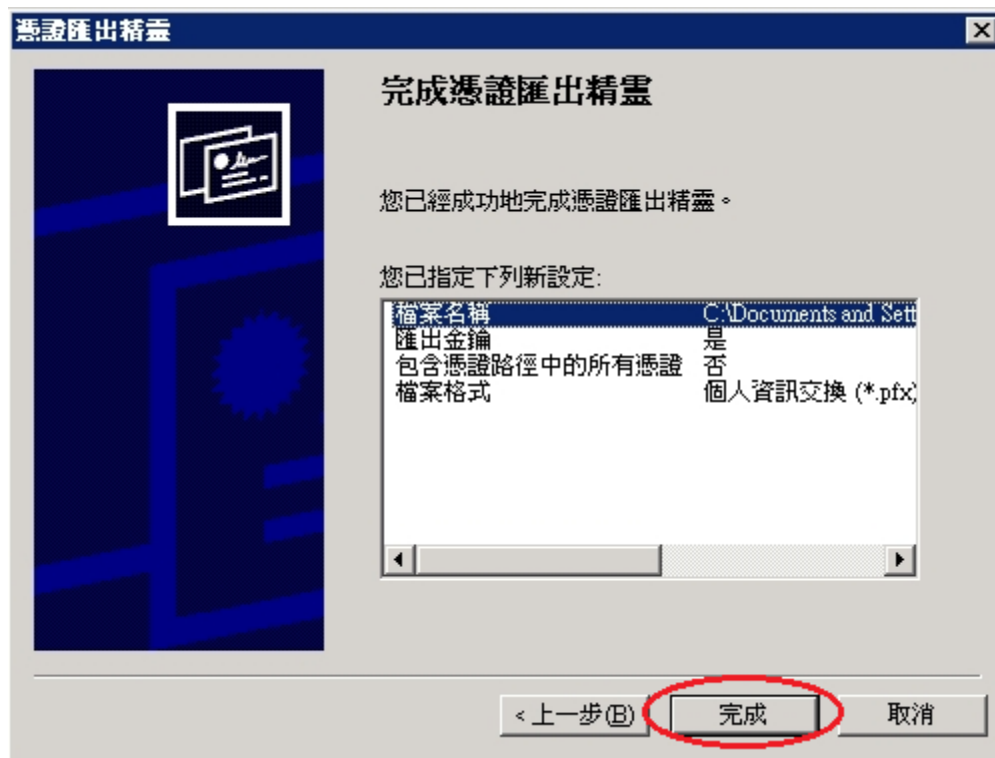
如果有按下「瀏覽」，則可選擇檔案路徑及輸入所要儲存的私密金鑰及憑證.pfx 檔檔名。輸入完成後，按下「儲存」後，接著會跳回「要匯出的檔案」頁面，並於頁面上出現存放檔案路徑及檔案名稱。



輸入完成後，接著以滑鼠按下「下一步」按鈕。



接著出現「完成匯出精靈」頁面，按下「完成」以完成匯出私密金鑰及憑證動作。

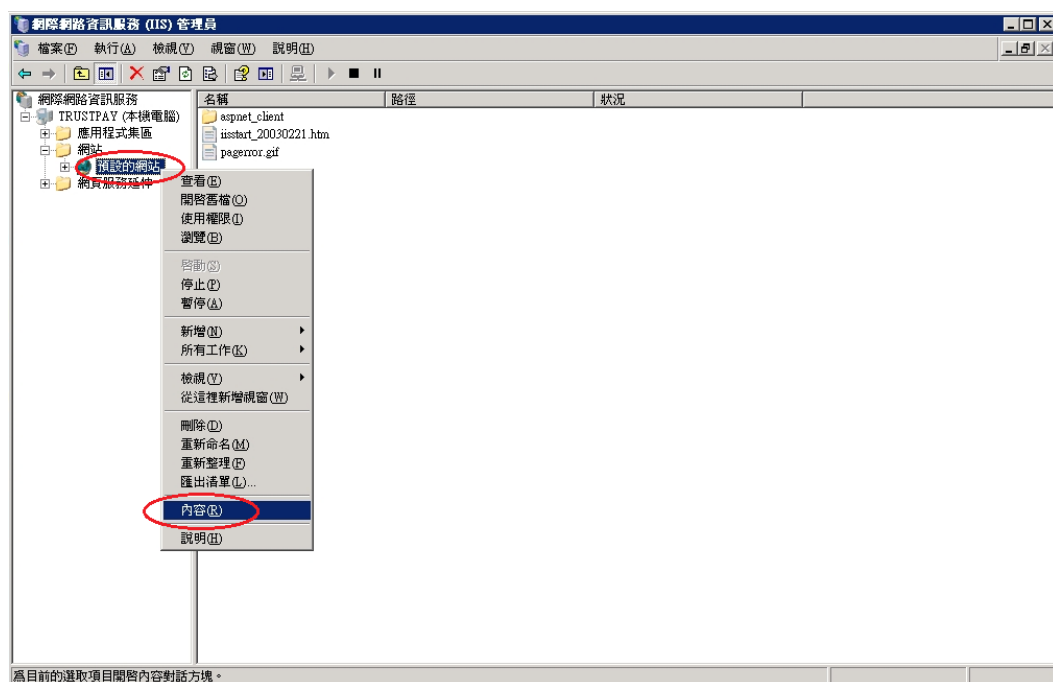


如果匯出完成，會出現如下訊息「匯出成功」。

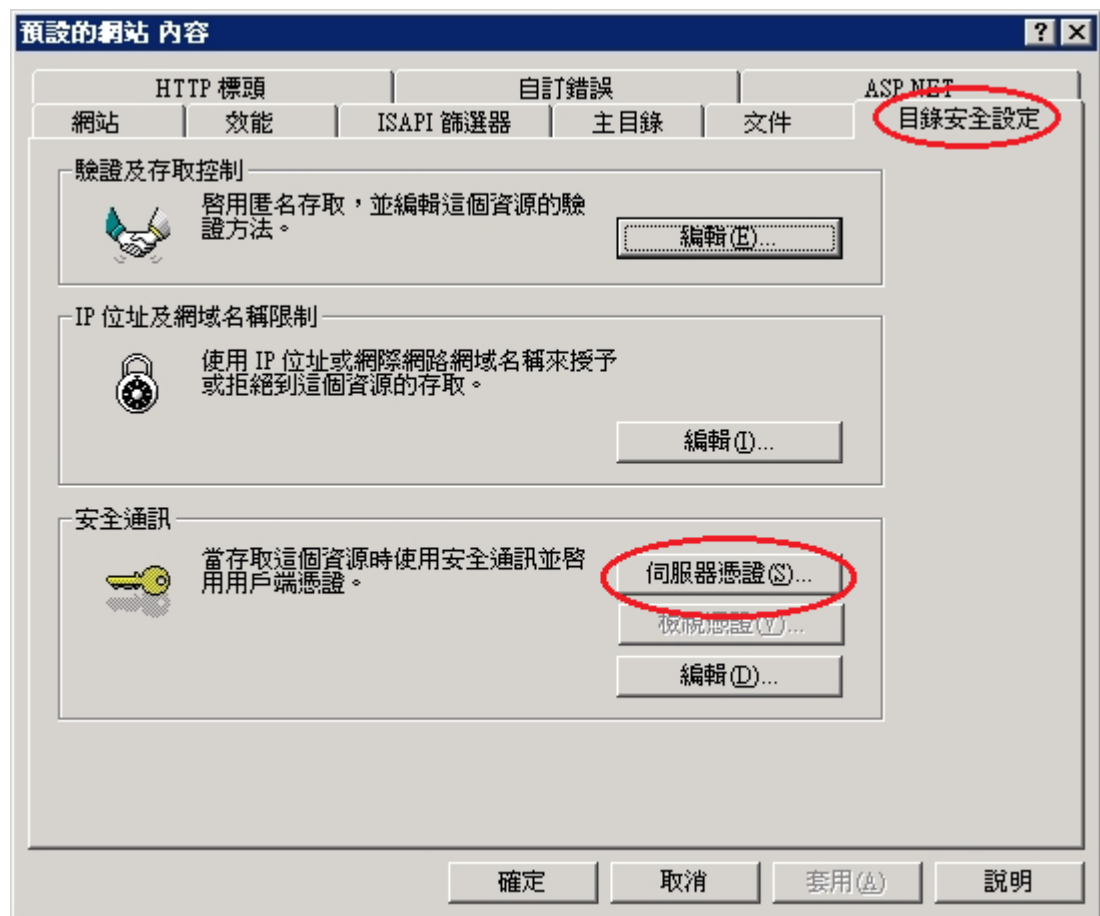


六、刪除憑證請求檔擱置要求，與將原來備份的私密金鑰及憑證檔(.pfx 檔)匯入。

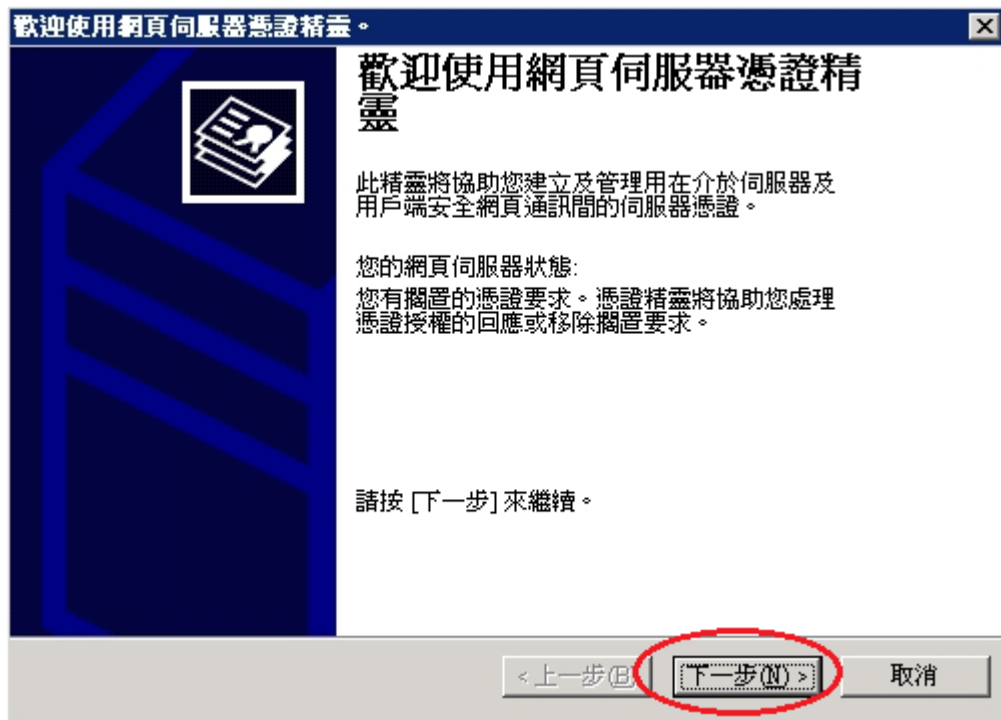
於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。



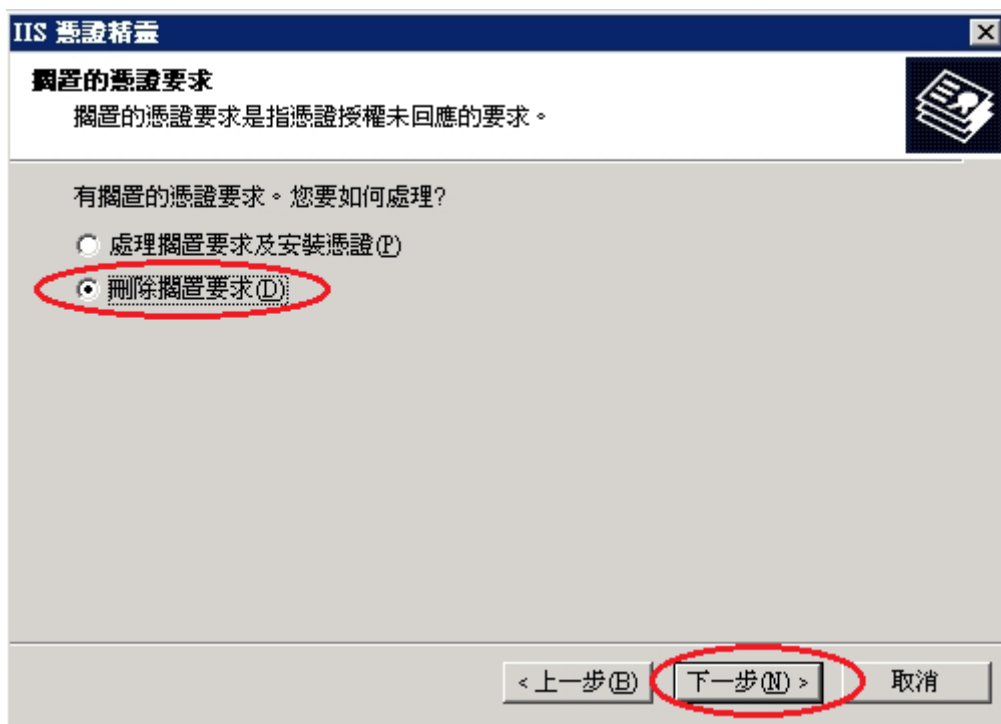
接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。



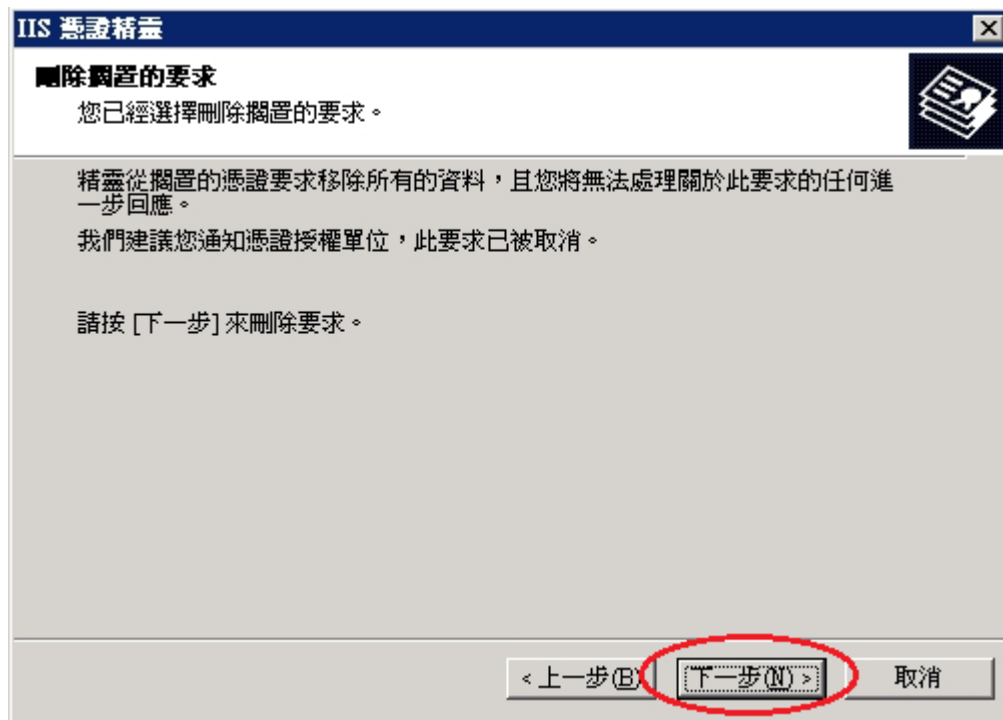
接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，以滑鼠按下「下一步」按鈕，開始刪除憑證請求檔擱置要求。



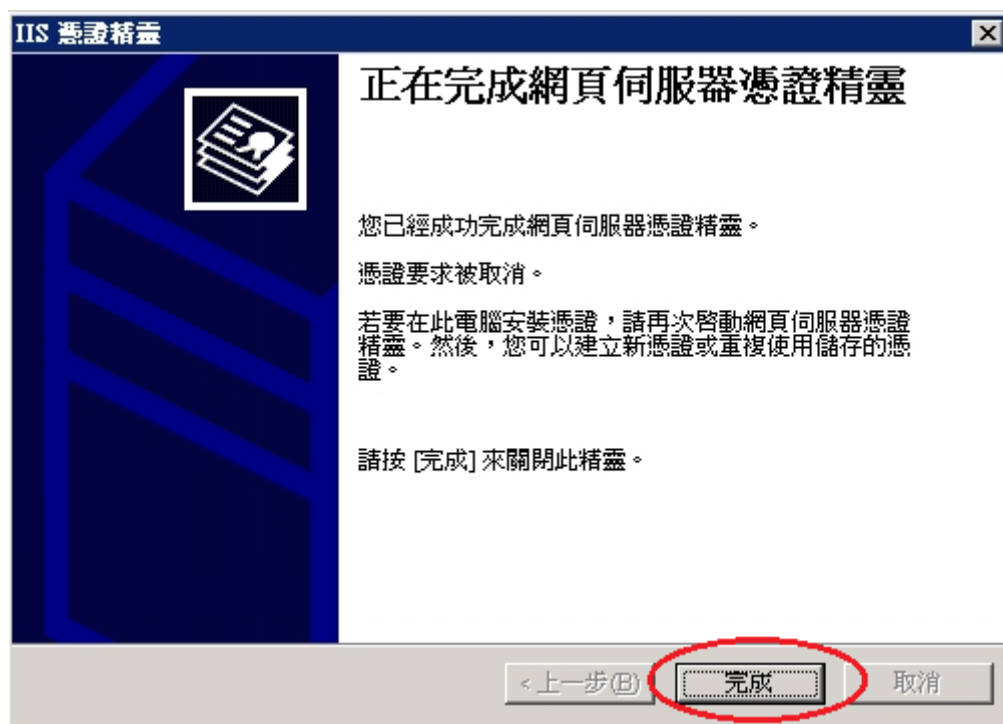
接著畫面會到「擱置的憑證要求」視窗，以滑鼠點選「刪除擱置要求(D)」，接著以滑鼠按下「下一步」按鈕。



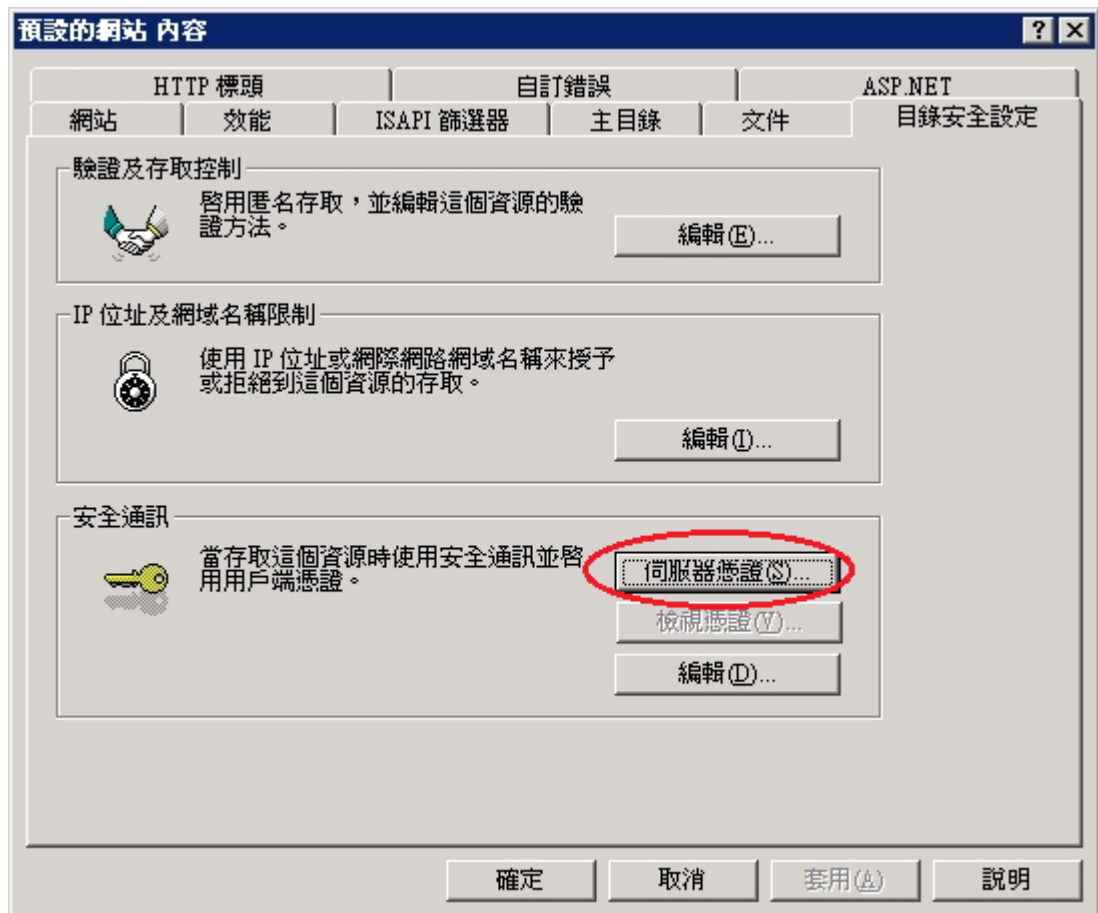
接著畫面會到「請按「下一步」來刪除要求。」視窗，接著以滑鼠按下「下一步」按鈕。



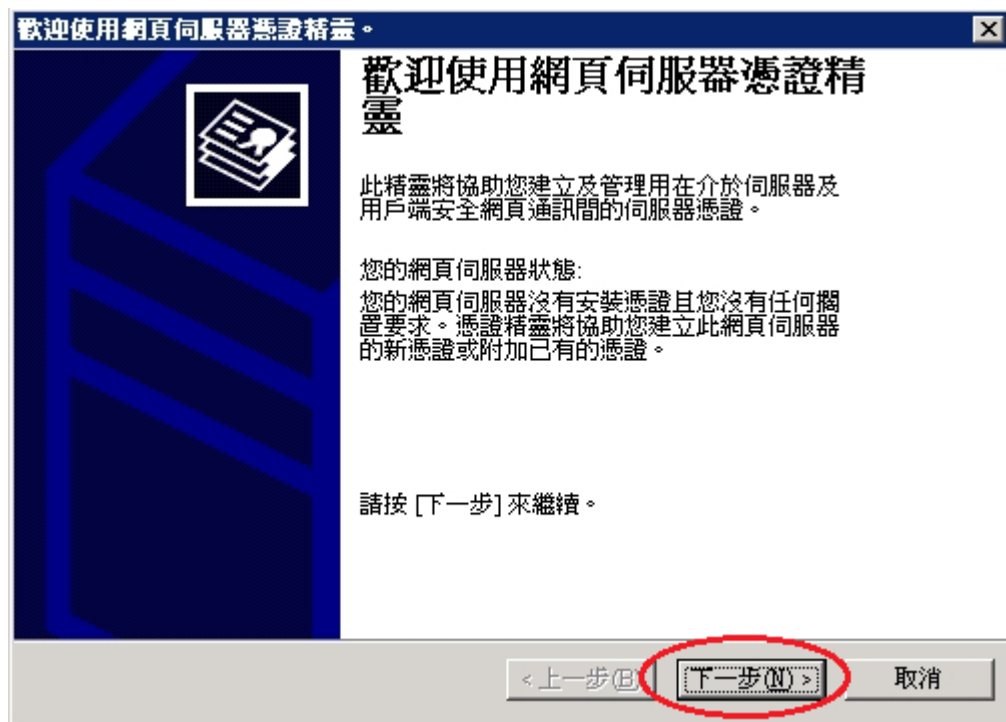
接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成刪除憑證擱置要動作。



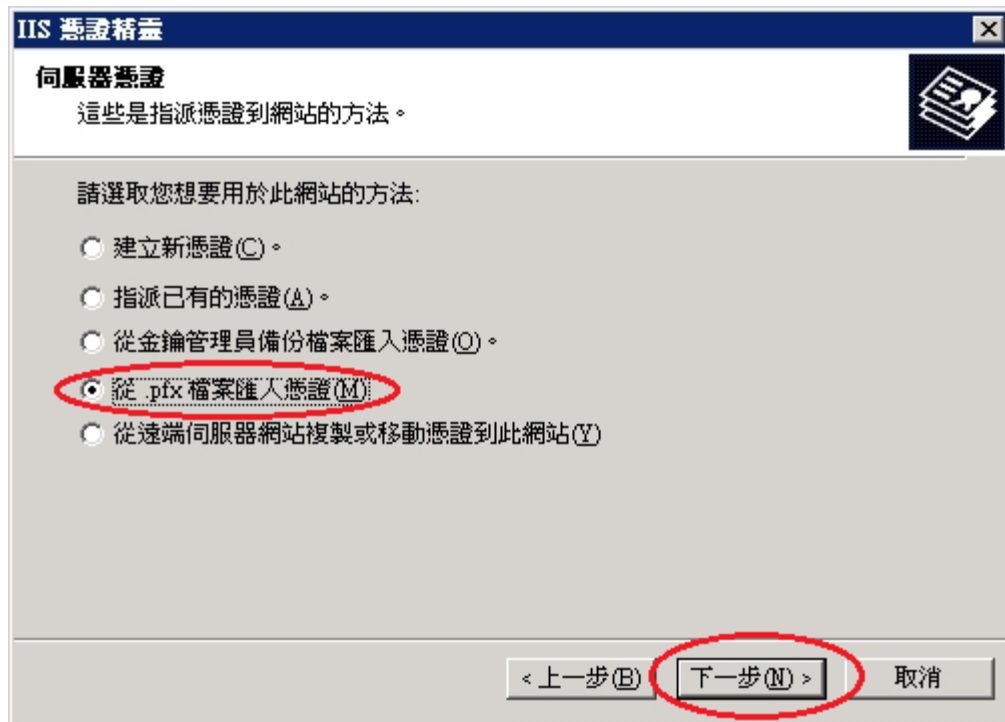
回到「預設的網站」「內容」畫面，接著再按下「伺服器憑證」按鈕。



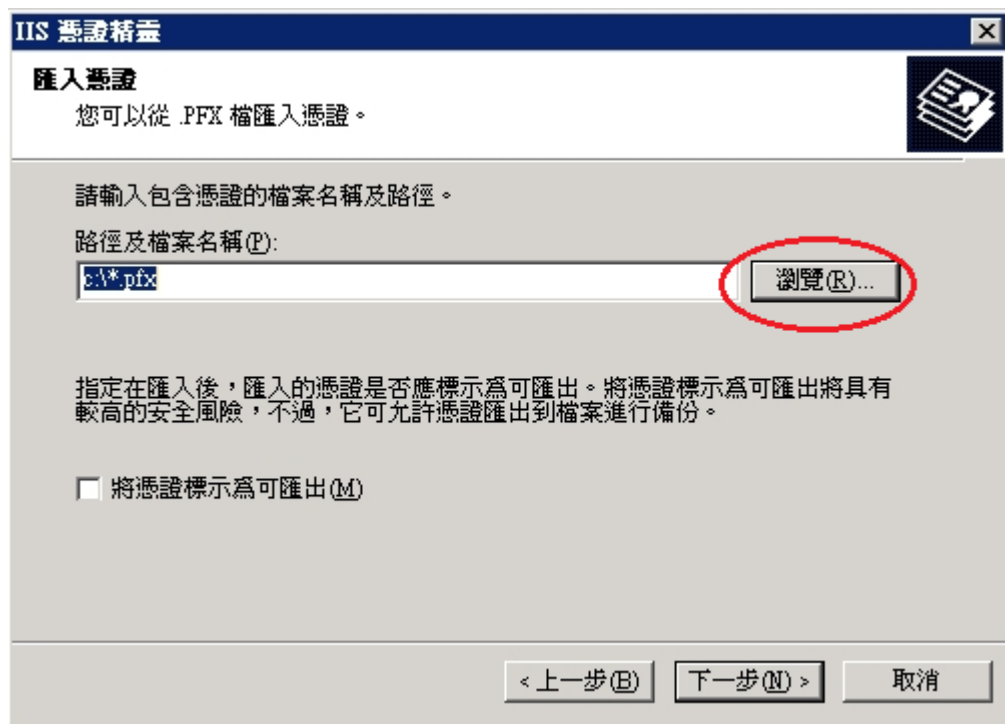
再次開啟「歡迎使用網頁伺服器憑證精靈」視窗畫面，以滑鼠按下「下一步」按鈕，開始匯入原先備份的私密金鑰及憑證(.pfx 檔)。



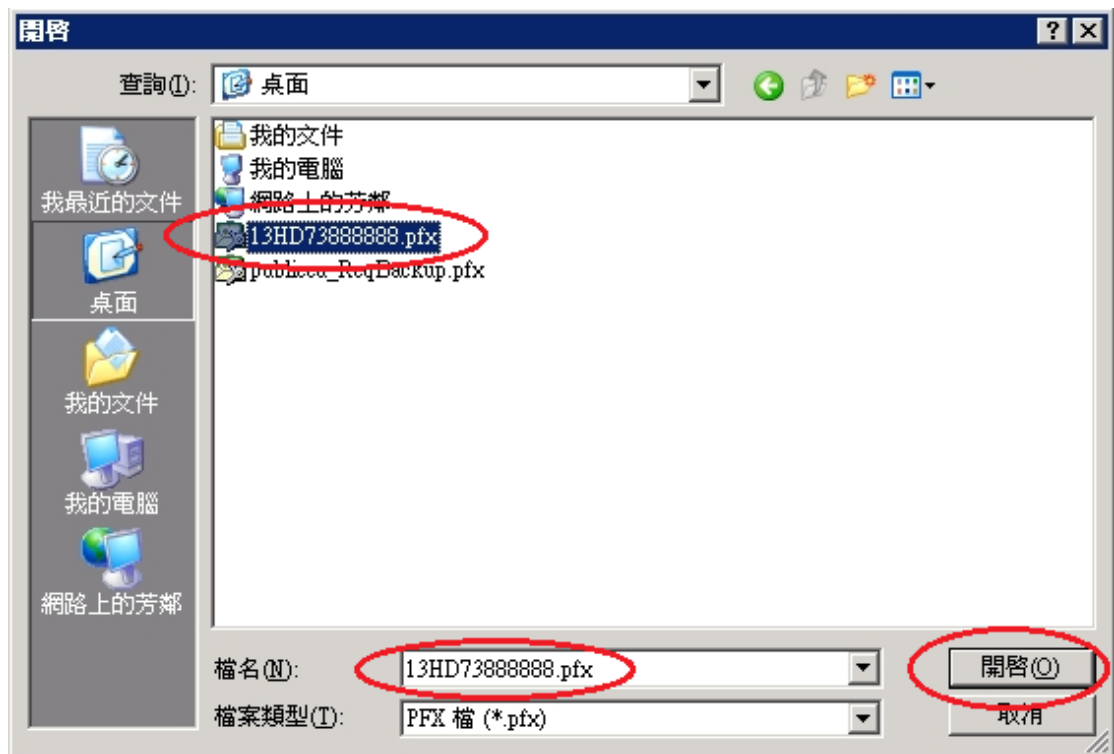
接著畫面會到「伺服器憑證」視窗，以滑鼠點選「從.pfx 檔案匯入憑證」，接著以滑鼠按下「下一步」按鈕。



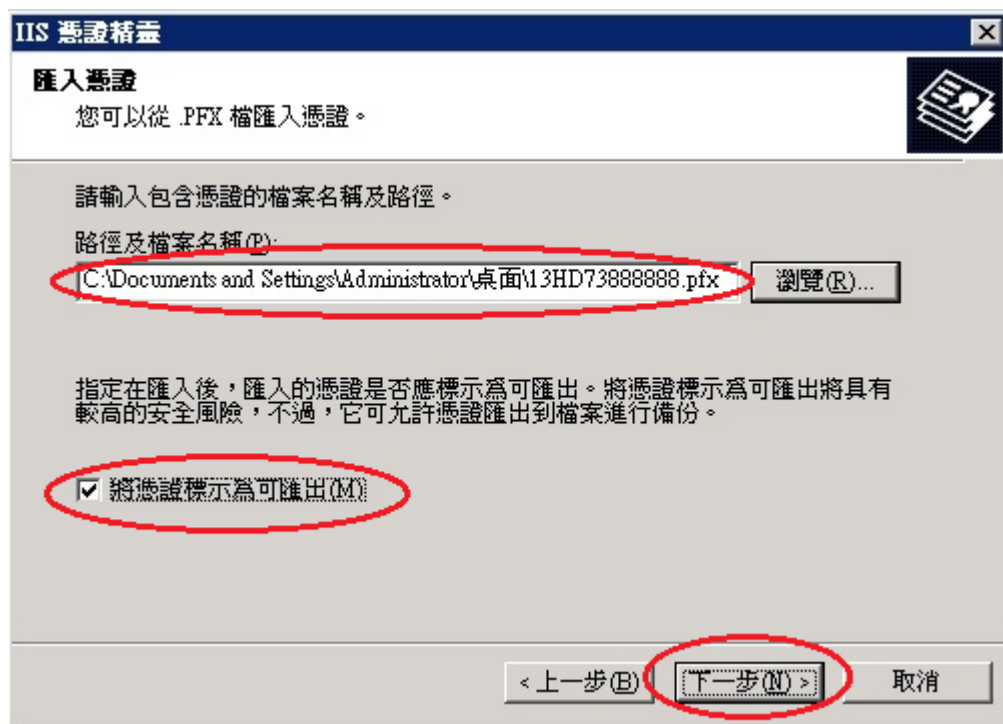
接著出現「匯入檔案」頁面，點選「瀏覽」選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。



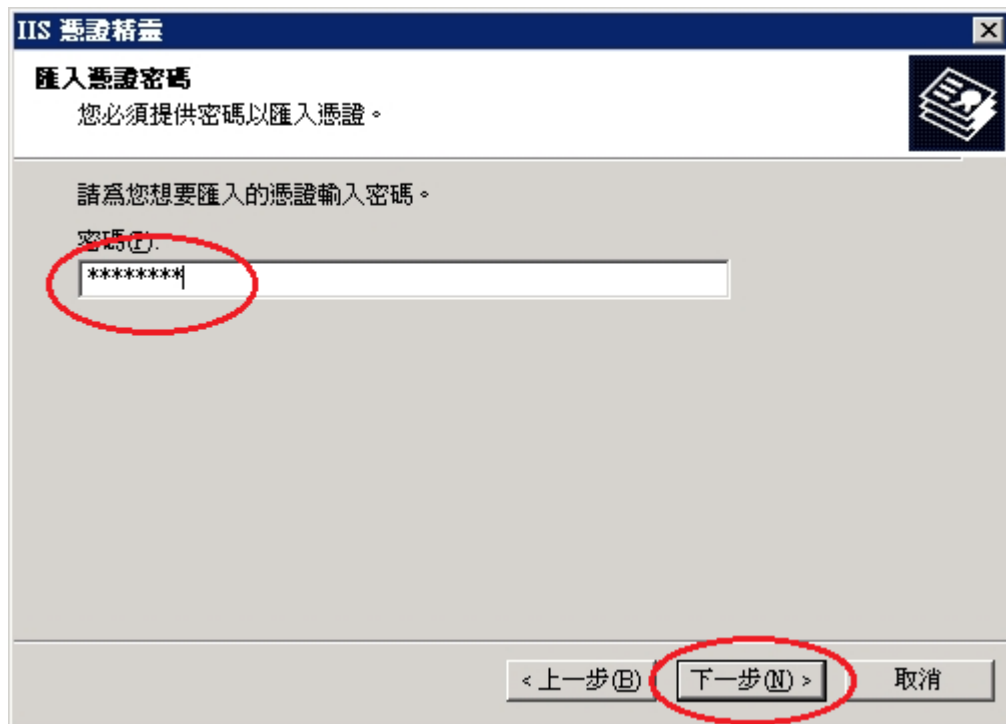
按下「瀏覽」，則可選擇檔案路徑及選擇私密金鑰及憑證.pfx 檔檔名。選擇完成後，按下「開啟」後，接著會跳回「匯入憑證」頁面，並於頁面上出現私密金鑰及憑證.pfx 檔檔案路徑及檔案名稱。



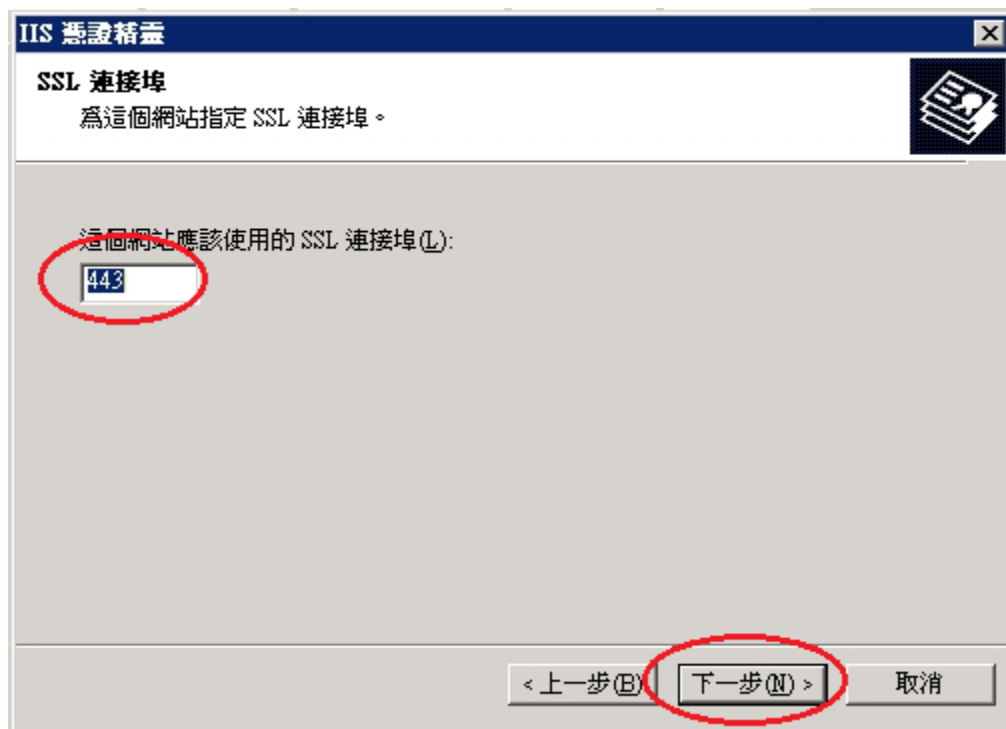
輸入完成後，並勾選「將憑證標示為可匯出(M)」，接著以滑鼠按下「下一步」按鈕。



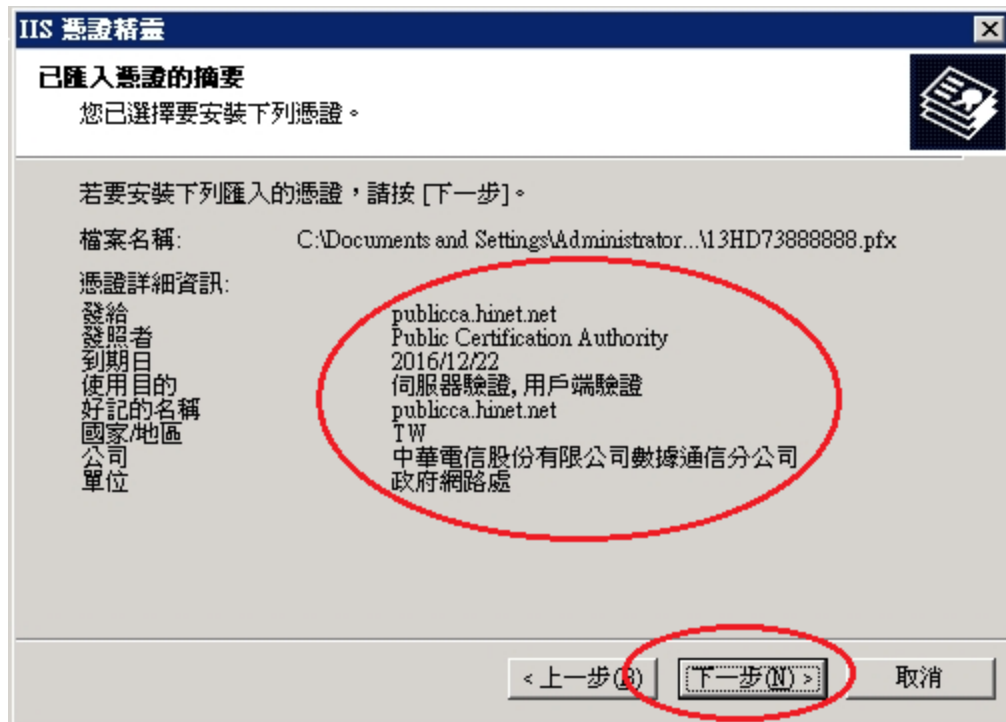
接著出現「匯入憑證密碼」頁面，輸入保護私密金鑰的密碼。



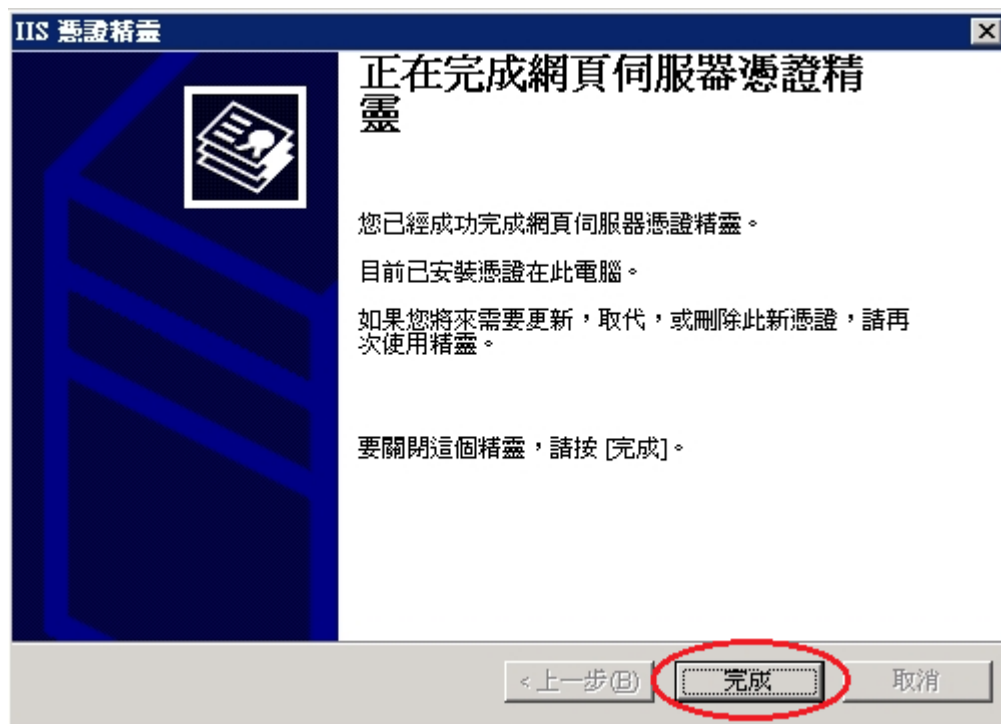
接著出現「SSL 連接埠」頁面，並設定「這個網站應該使用的 SSL 連接埠(L)」，請依網站需求自行設定，接著以滑鼠按下「下一步」按鈕。



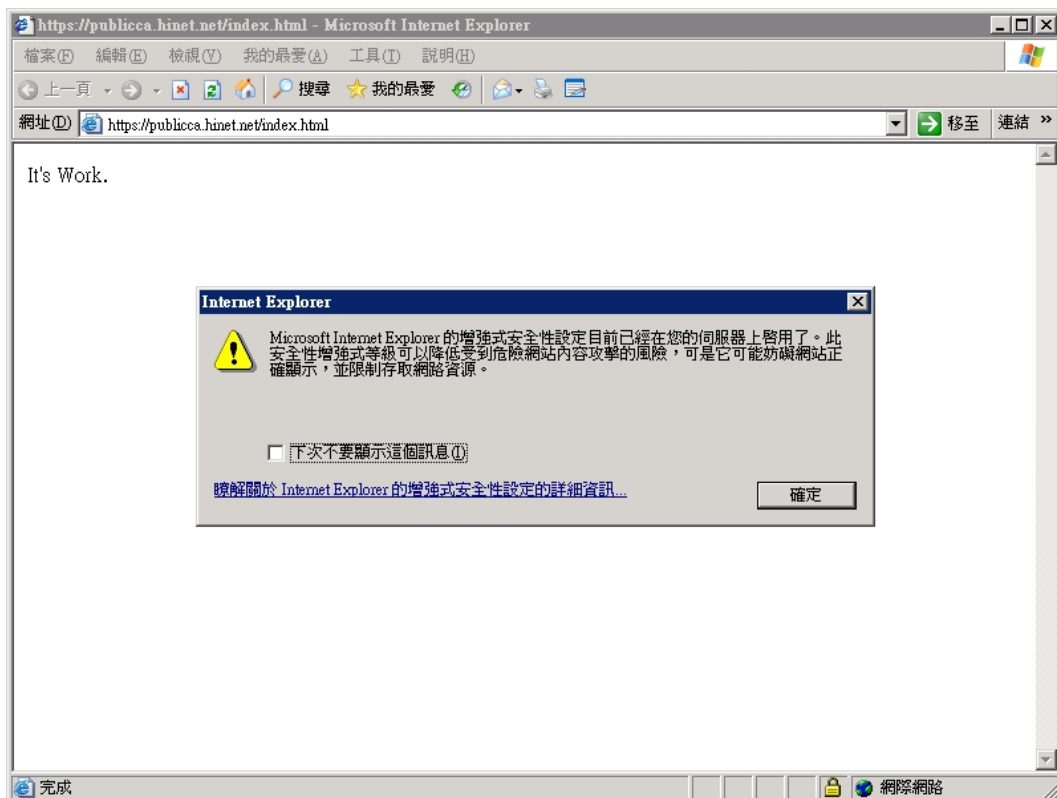
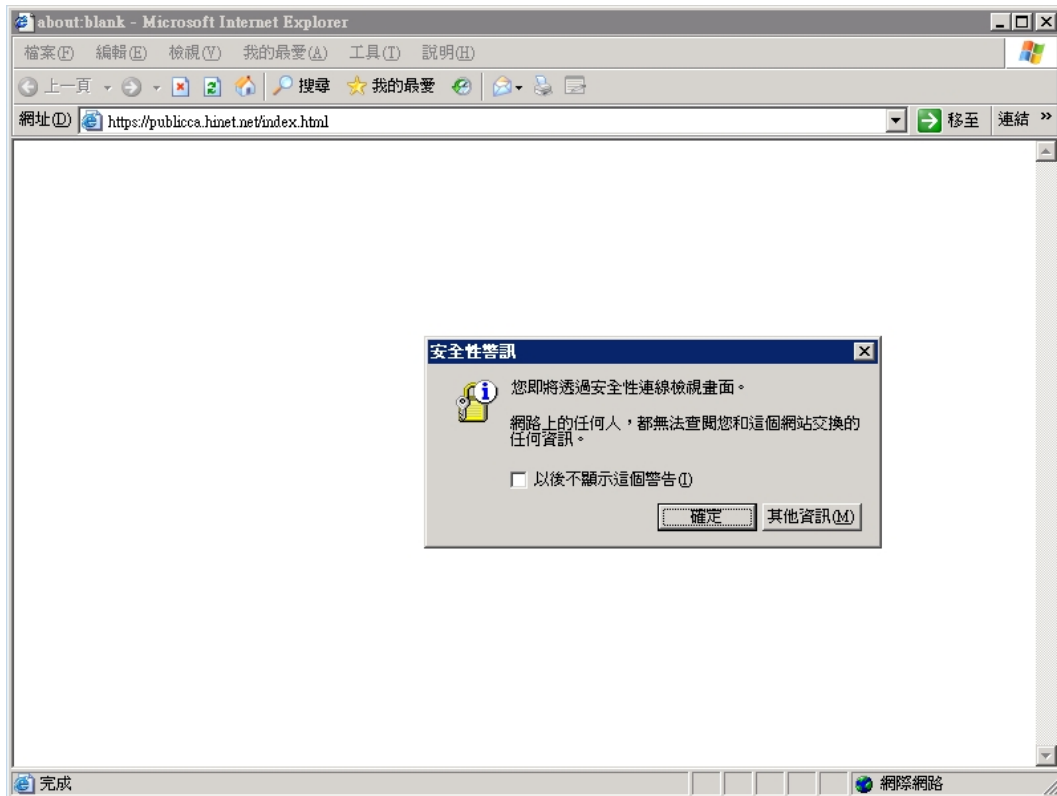
接著出現「已匯入憑證的摘要」頁面，確認憑證內容無誤後，接著以滑鼠按下「下一步」按鈕。



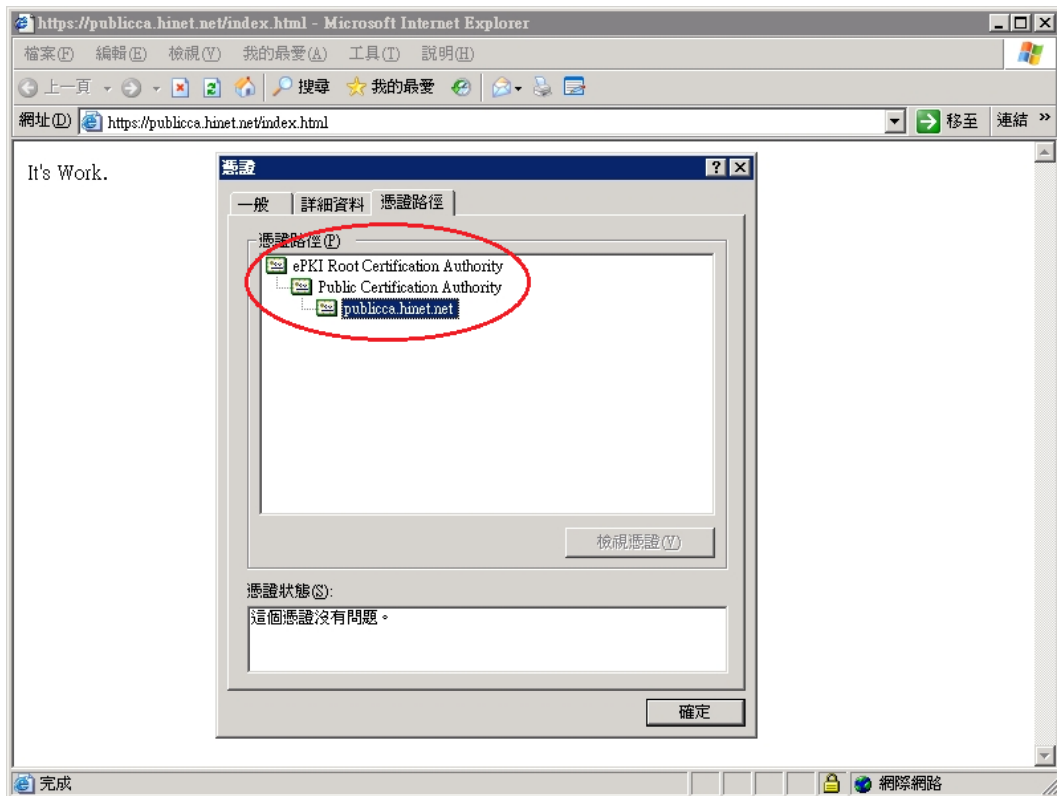
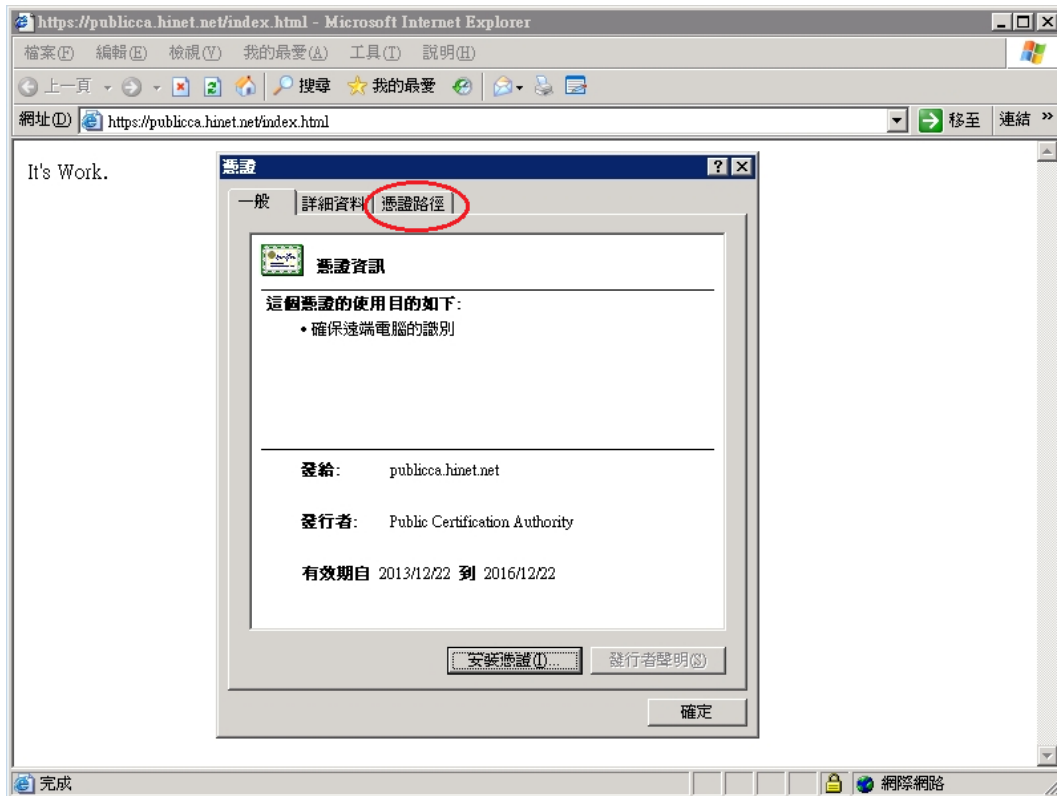
接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成匯入私密金鑰及憑證.pfx 檔動作。



透過瀏覽器連線測試網頁 https 是否連線正常。



檢查 SSL 憑證串鏈是否正常。



以上動作即完成 Windows 2003 IIS 6.0 重新產製金鑰及憑證請求檔動作，並還原原先的 SSL 私密金鑰及憑證動作。

Windows IIS 6.0 SSL 憑證安裝操作手冊

安裝根憑證(eCA)及中繼憑證(PublicCA)

此步驟為該伺服器網站從未安裝根憑證(eCA)及中繼憑證(PublicCA)才需執行。

一、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：

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 3 個檔案。

2. 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」，下載 SSL 憑證。

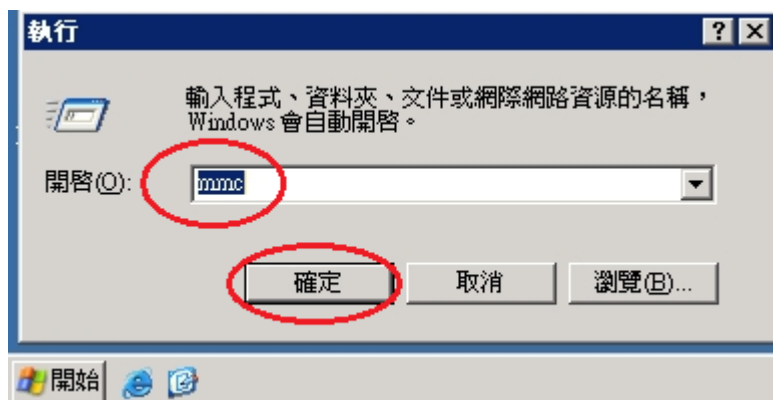
二、有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(<https://publicca.hinet.net/SSL-08-06.htm>)

三、點選「開始」→「執行」

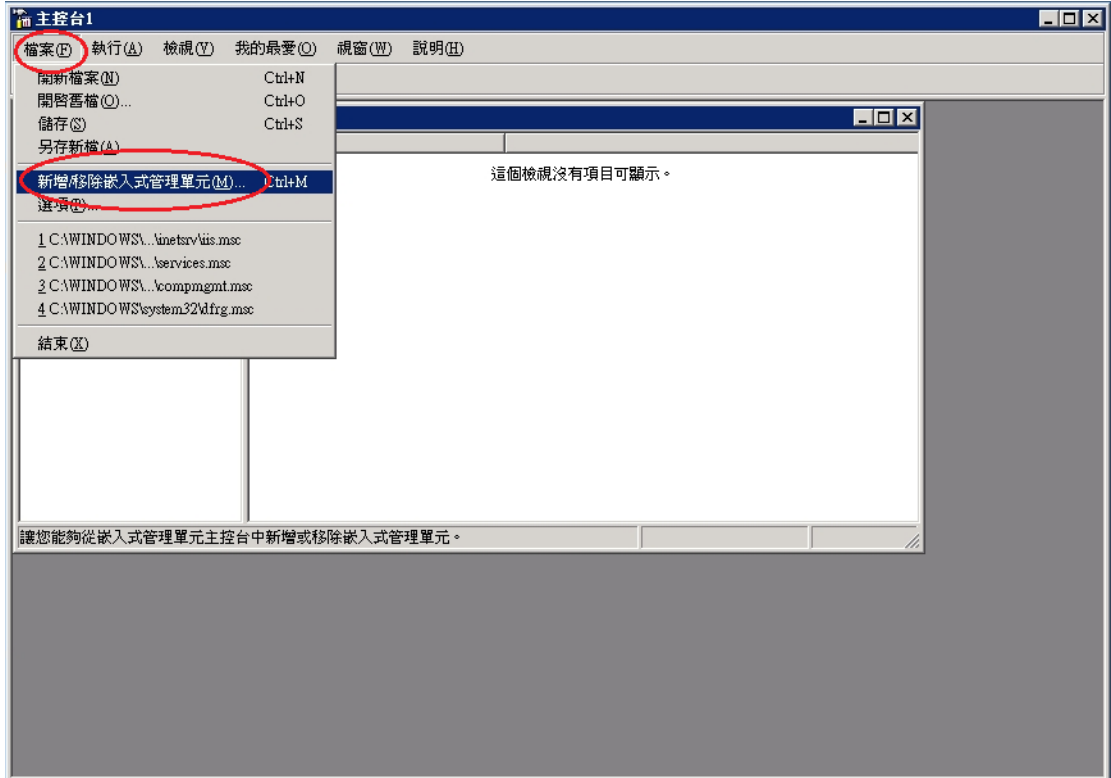


於「開啟

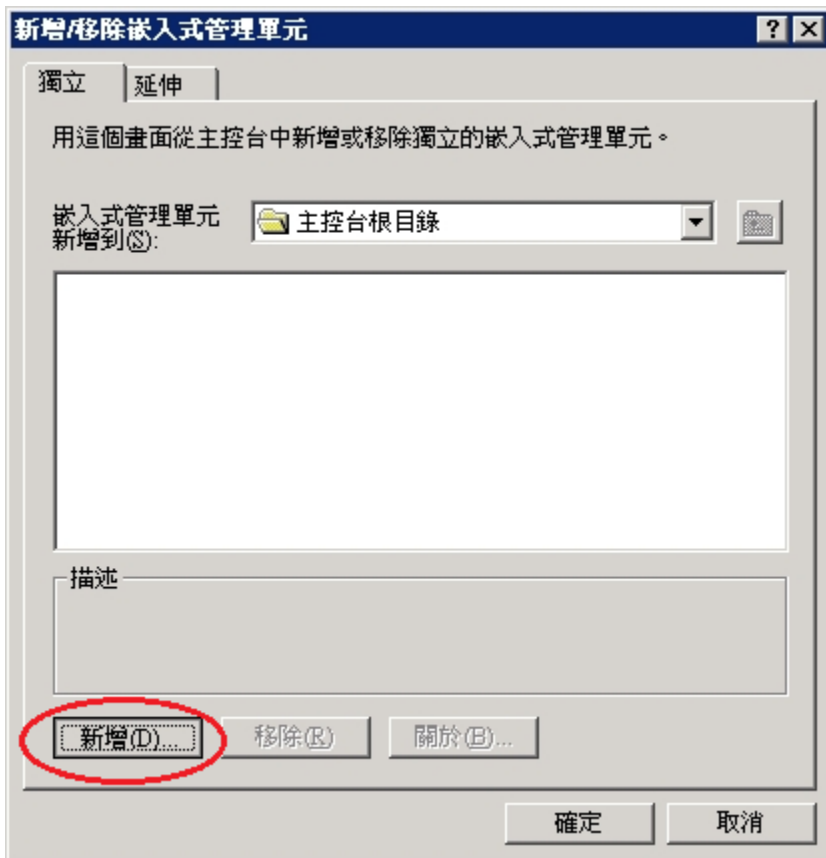
(0)」欄位輸入 mmc 後，按下「確定」按鈕。



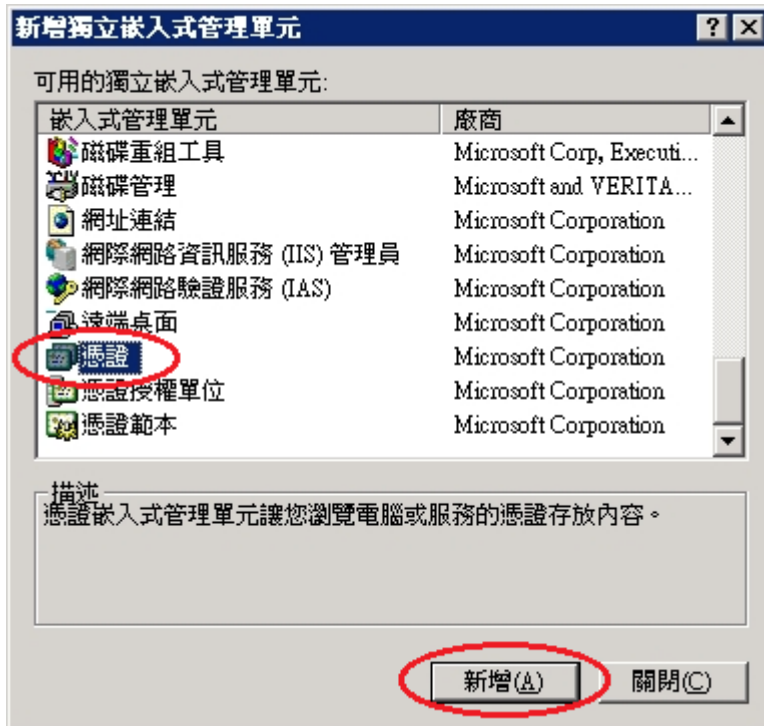
於主控台點選「檔案」→「新增/移除嵌入式管理單元」。



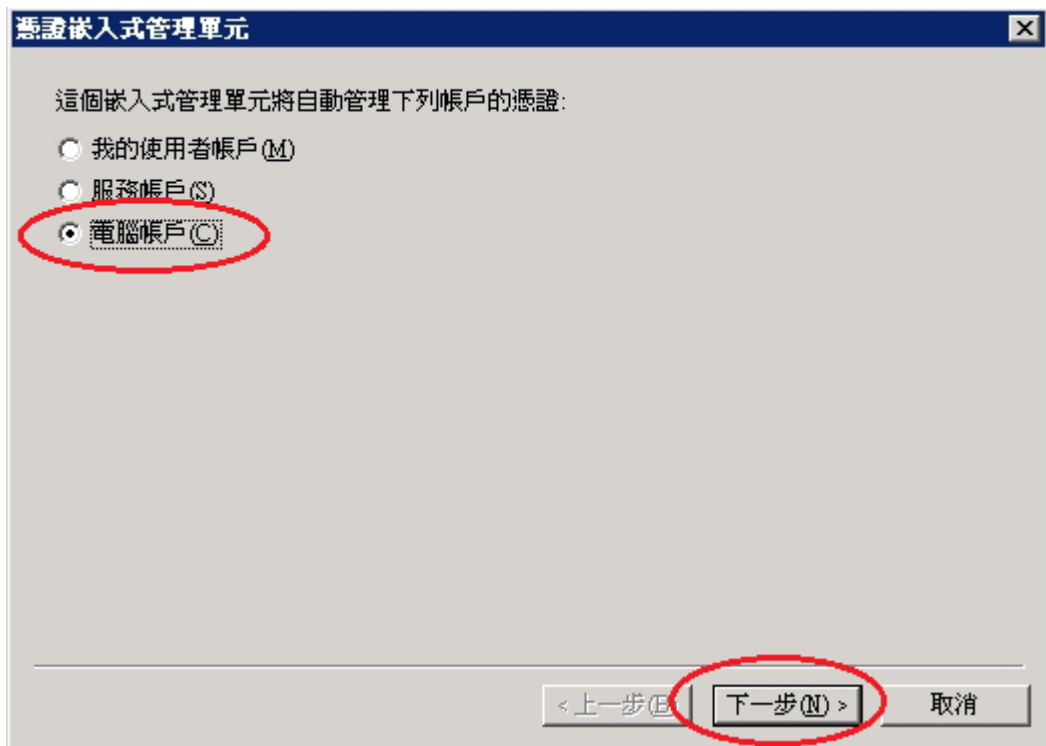
接著出現「新增/移除嵌入式管理單元」畫面，點選「新增」按鈕。



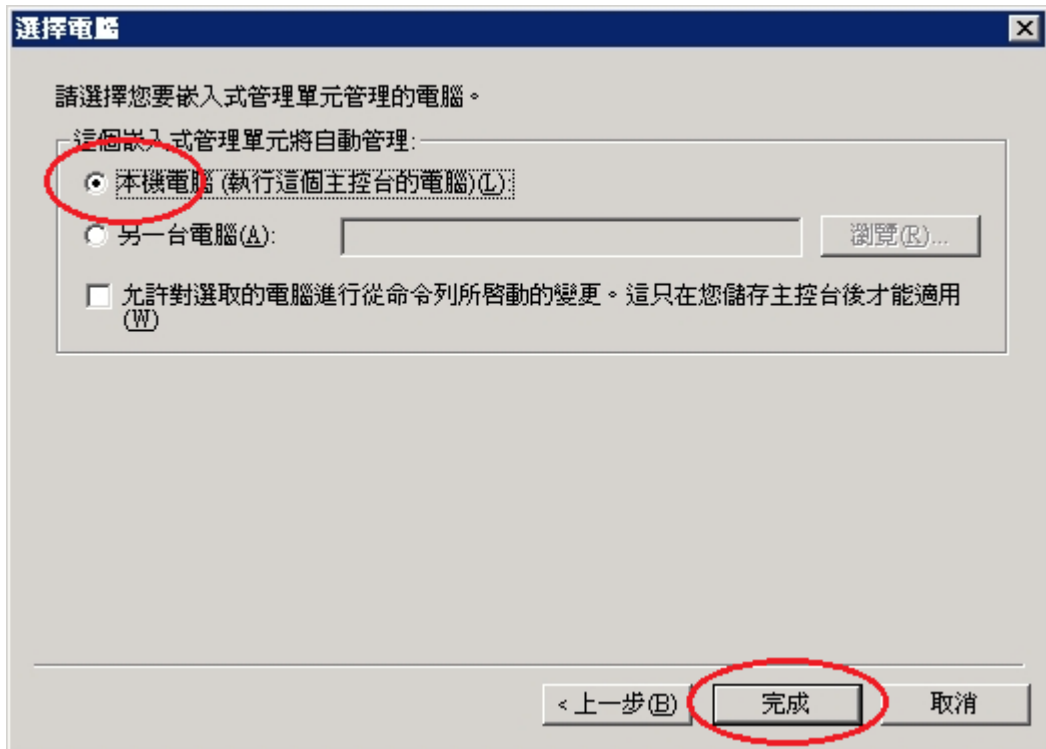
接著出現「新增獨立嵌入式管理單元」畫面，於「可用的獨立嵌入式管理單元」點選「憑證」項目後，按下「新增」按鈕。



接著出現「憑證嵌入式管理單元」畫面，於「這個嵌入式管理單元將自動管理下列帳戶的憑證:」點選「電腦帳戶」後，點選「下一步」按鈕。



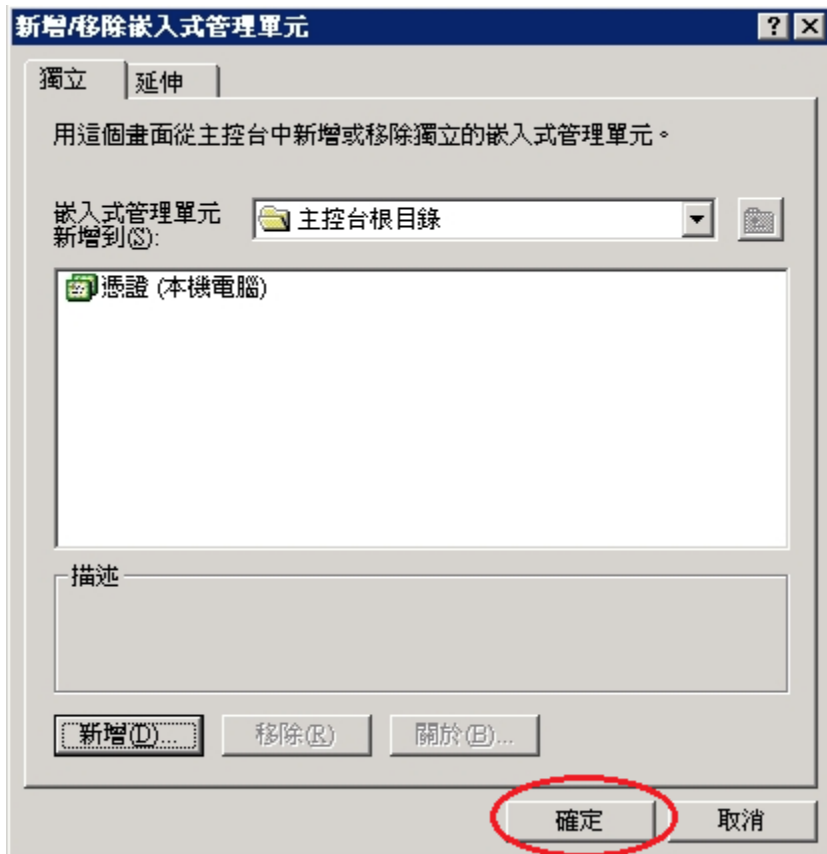
接著出現「選擇電腦」畫面，於「這個嵌入式管理單元將自動管理:」點選「本機電腦(執行這個主控台的電腦)(L)」後，點選「完成」按鈕。



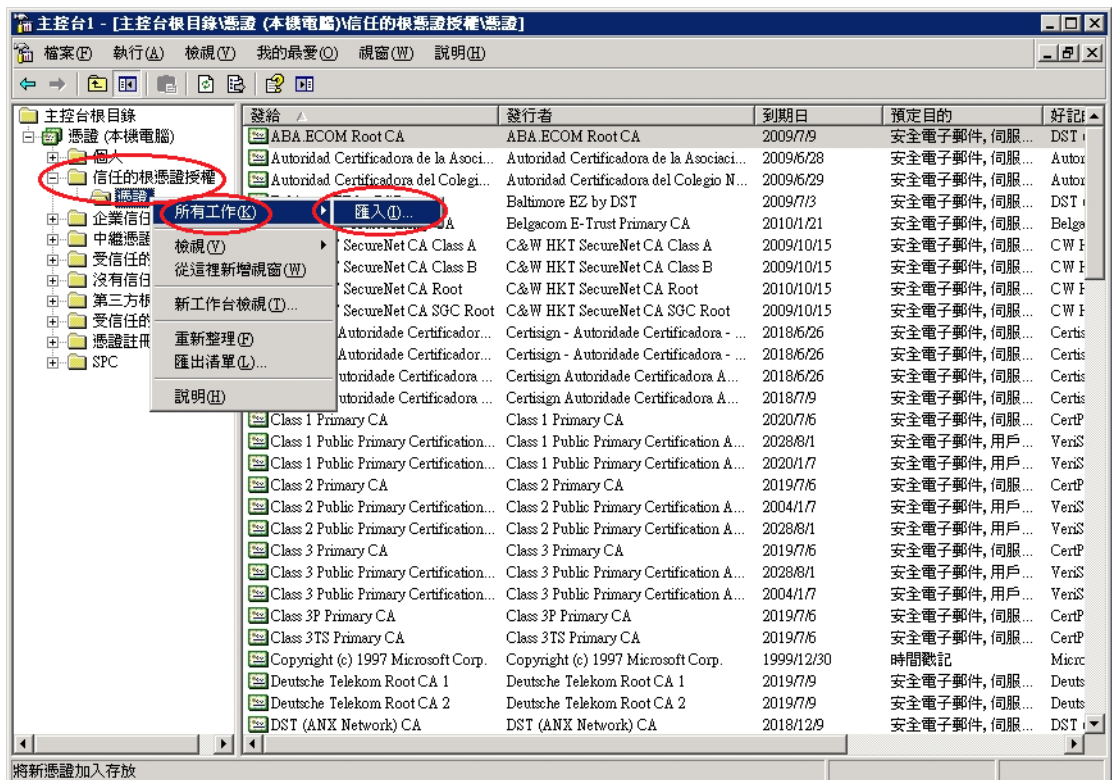
回到「新增獨立嵌入式管理單元」畫面，點選「關閉」按鈕。



回到「新增/移除嵌入式管理單元」畫面，點選「確定」按鈕。

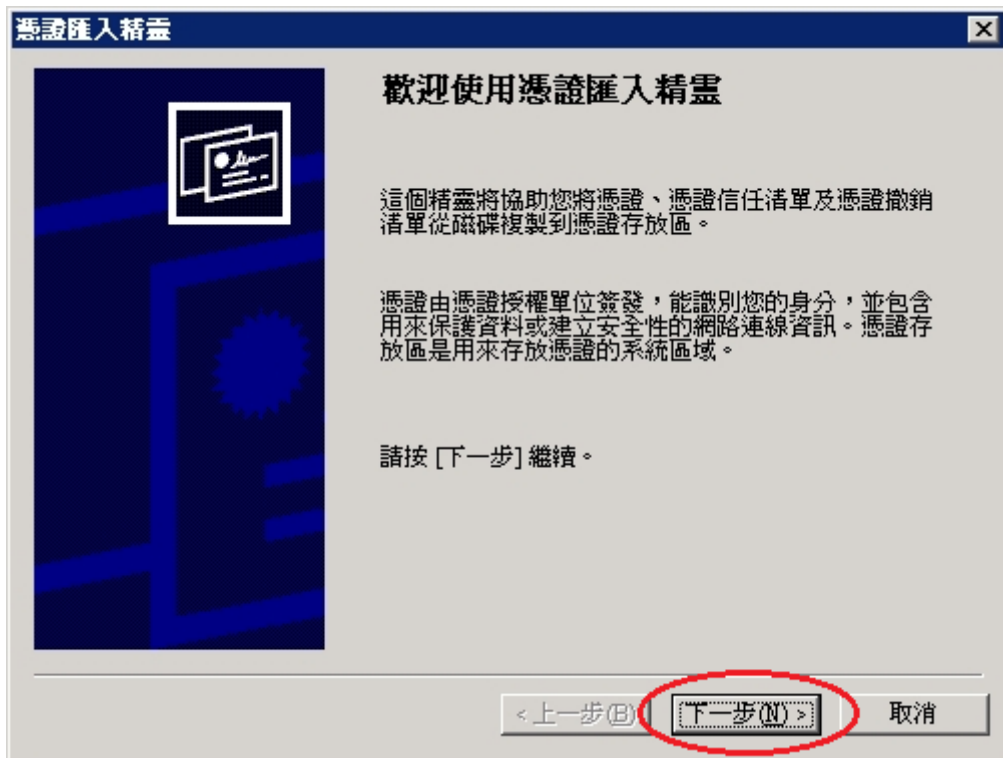


於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「信任的根憑證授權」→「憑證」→「所有工作(K)」→「匯入(I)」。

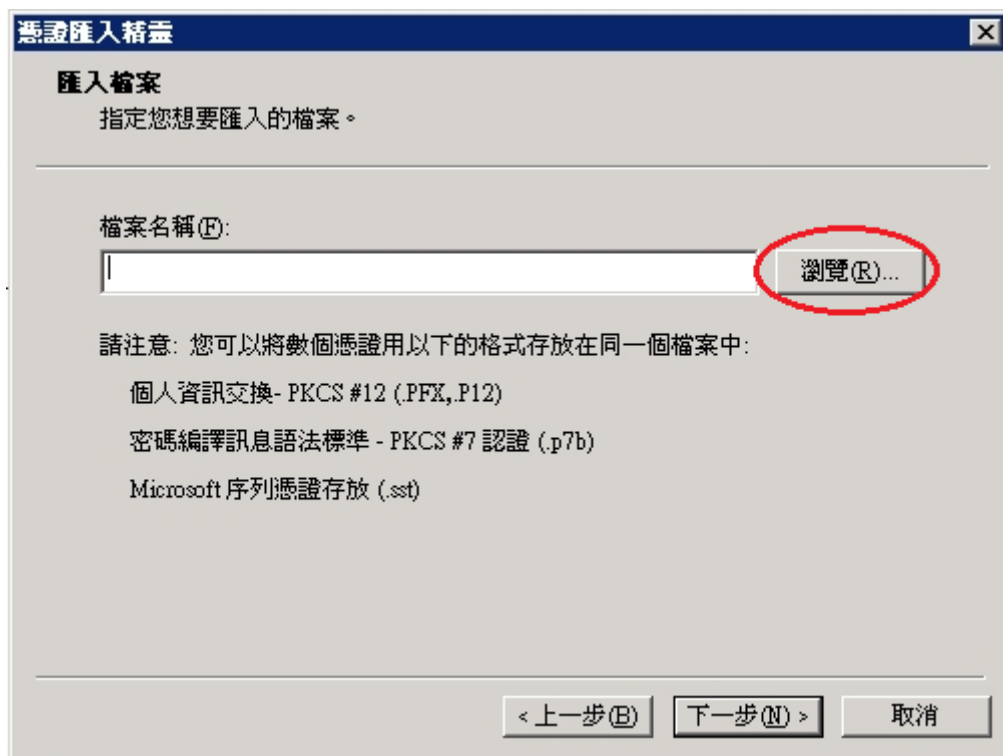


接著出現「憑證匯入精靈」畫面，於「歡迎使用憑證匯入精靈」點選「下

一步」按鈕。

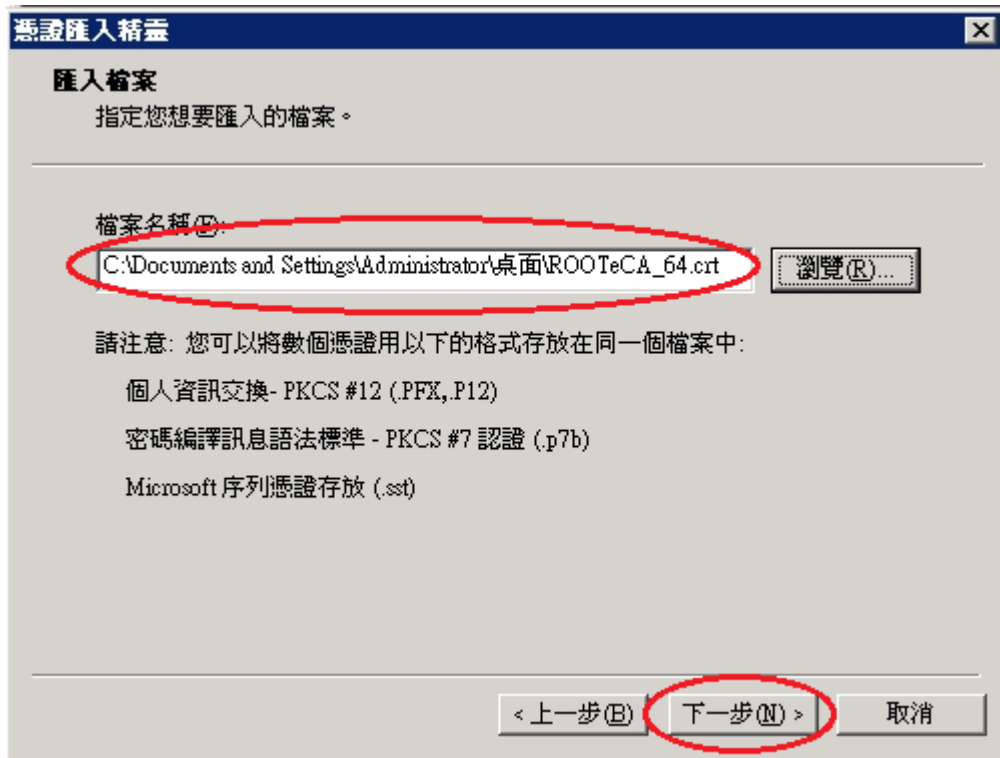


接著出現「匯入檔案」畫面，點選「瀏覽」選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。

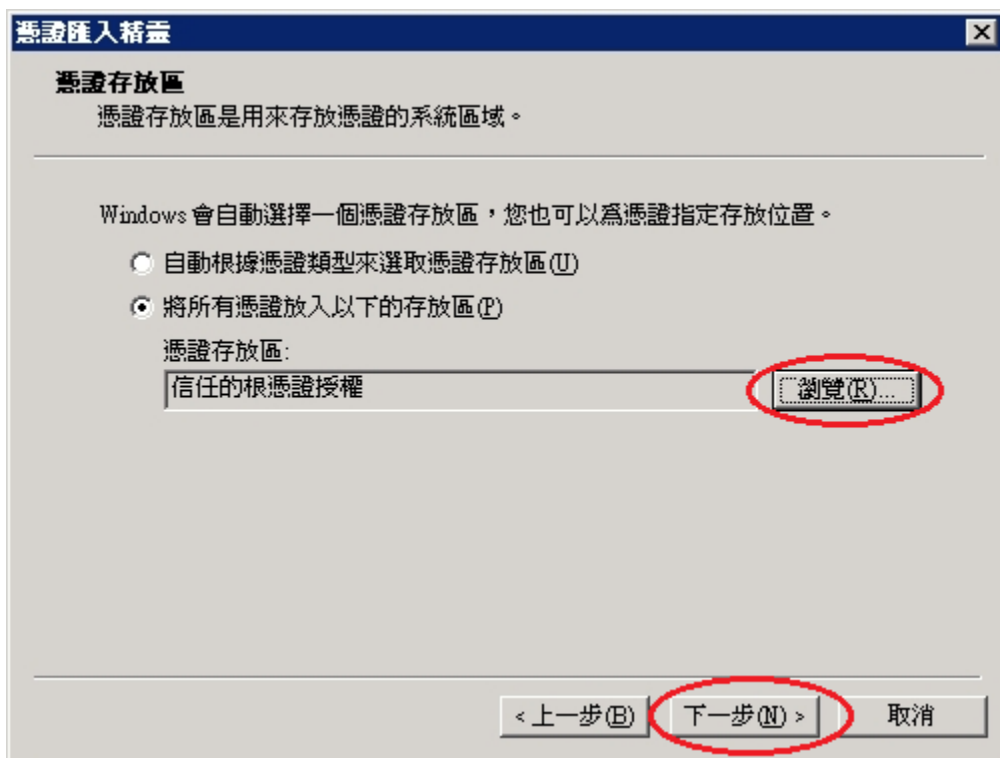


如果有按下「瀏覽」，則可選擇要匯入的檔案路徑及所要選取的根憑證檔名「ROOTeCA_64.crt」。選取完成後，按下開啟後，接著會跳回「匯入檔案」頁面，並於頁面上出現要匯入的檔案路徑及檔案名稱，並點選「下一

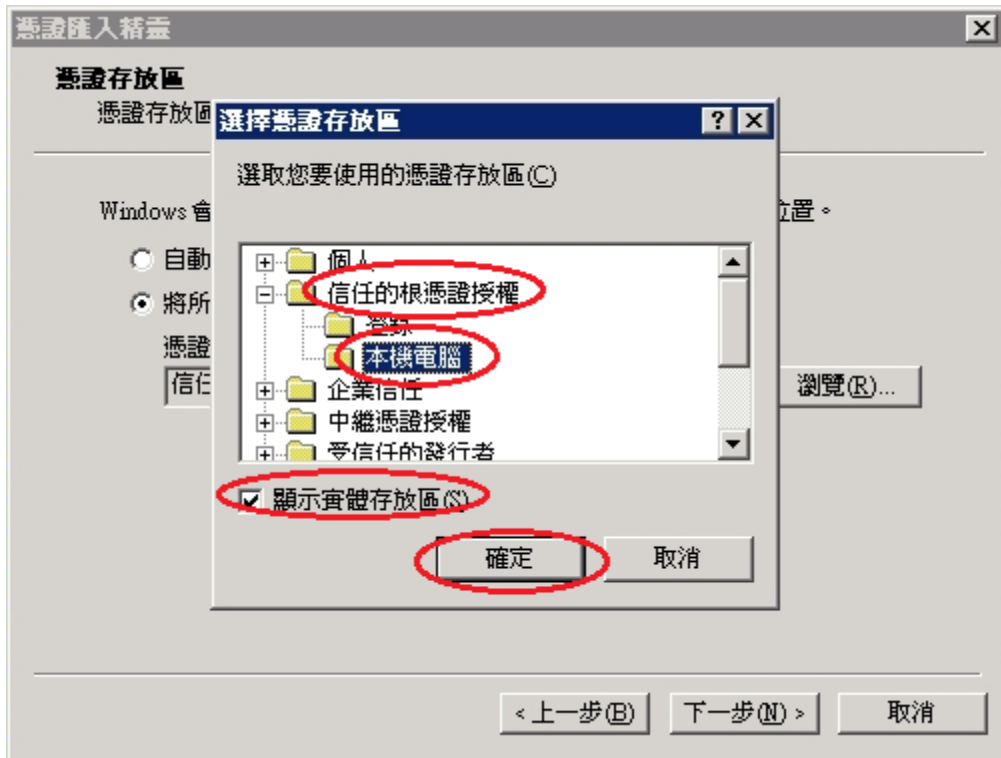
步」按鈕。



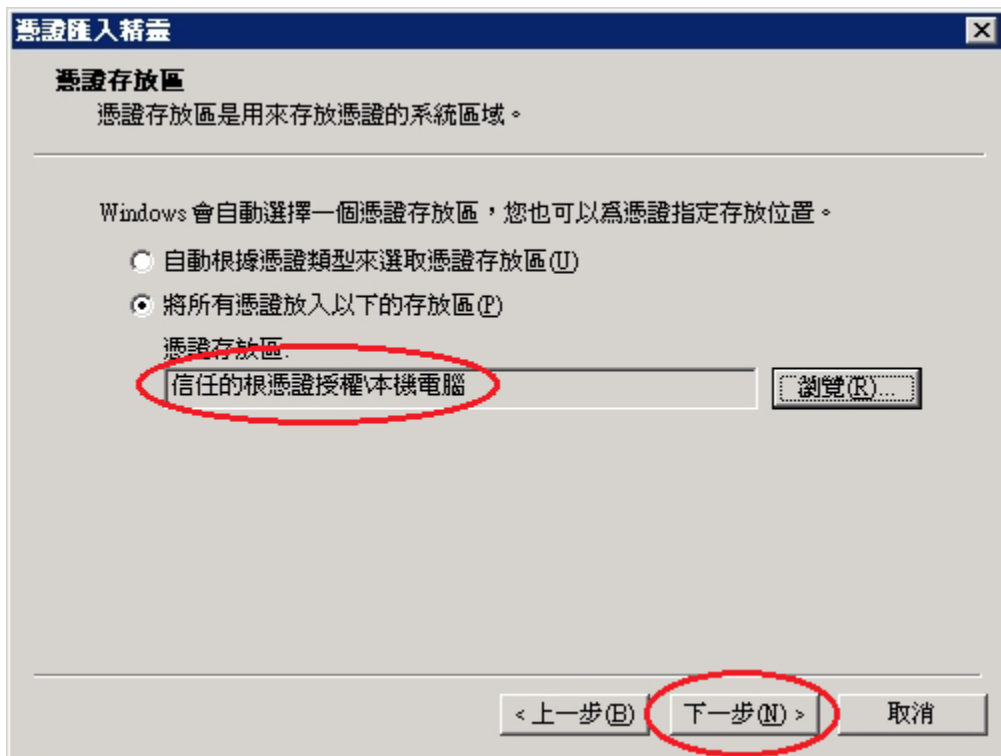
接著出現「憑證存放區」畫面，點選「將所有憑證放入以下的存放區(P)」，點選「瀏覽」按鈕。



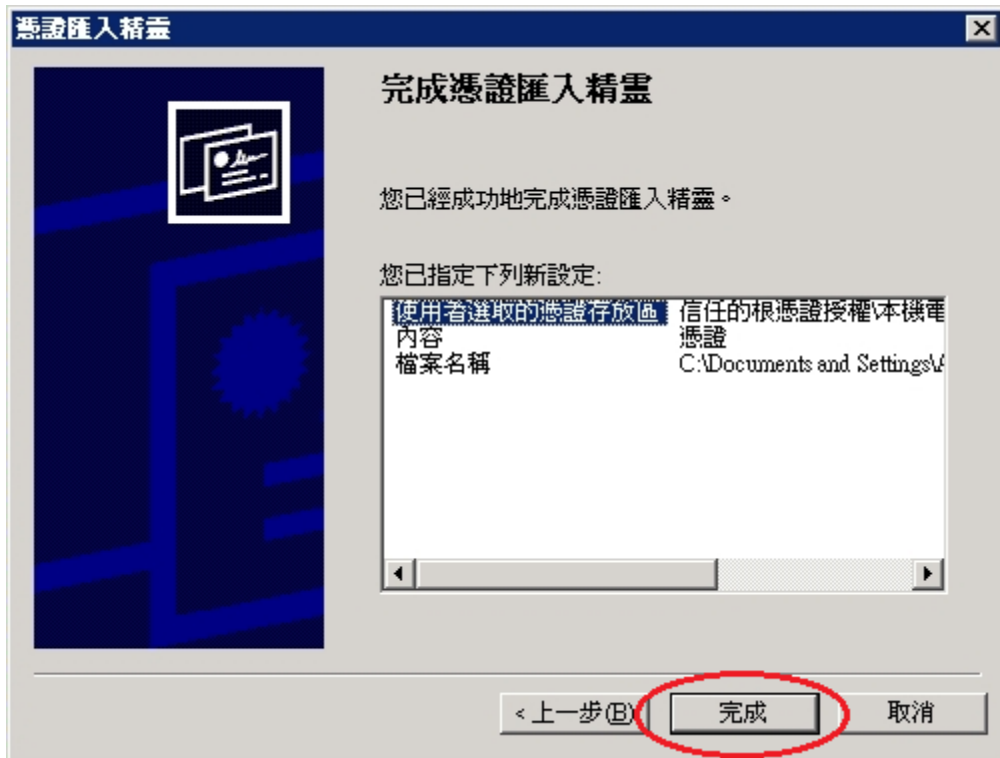
接著出現「選擇憑證存放區」畫面，先點選「顯示實體存放區(S)」，選擇「信任的根憑證授權」→「本機電腦」後，並點選「確定」按鈕。



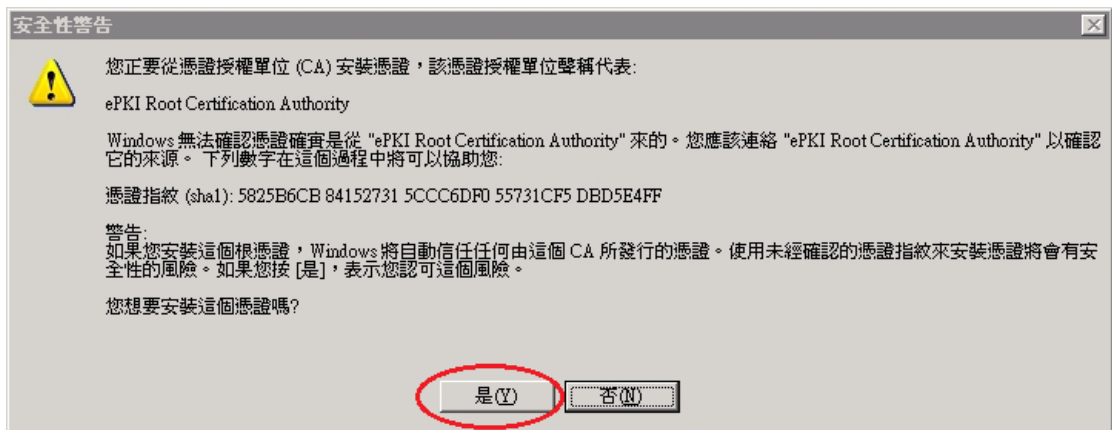
回到「憑證存放區」畫面後，以滑鼠按下「下一步」按鈕。



接著出現「完成憑證匯入精靈」頁面，按下「完成」以完成 eCA 根憑證匯入動作。



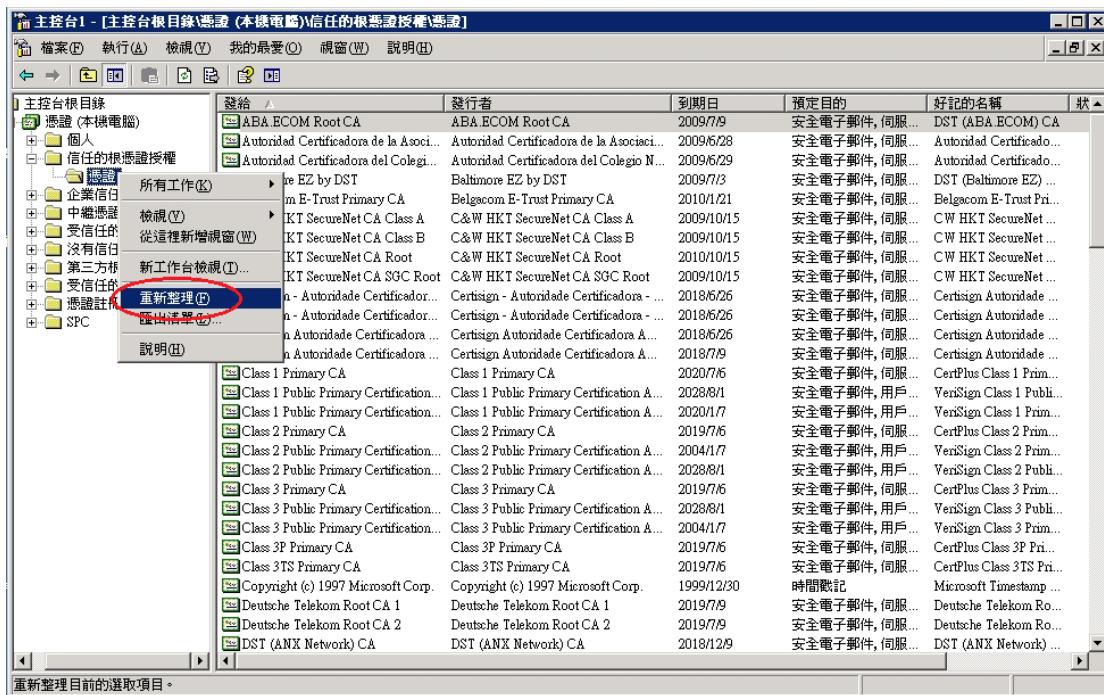
按下完成後，如有出現類似以下訊息，則直接按下「是」，即可匯入完成。



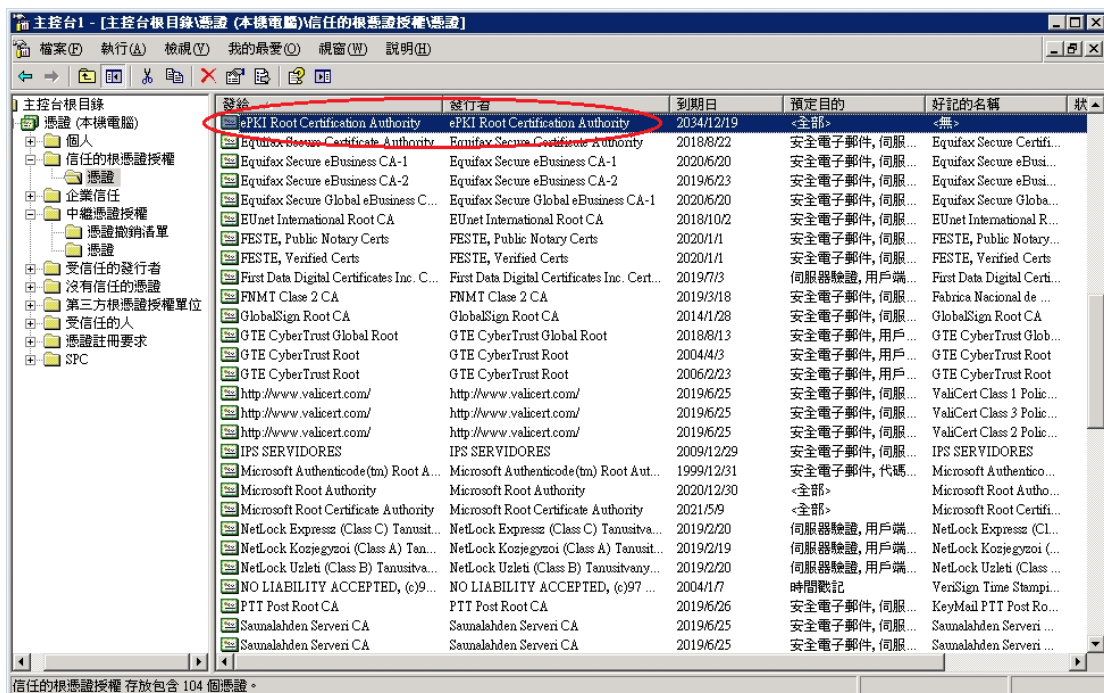
匯入完成，會出現如下訊息「匯入執行成功」訊息。



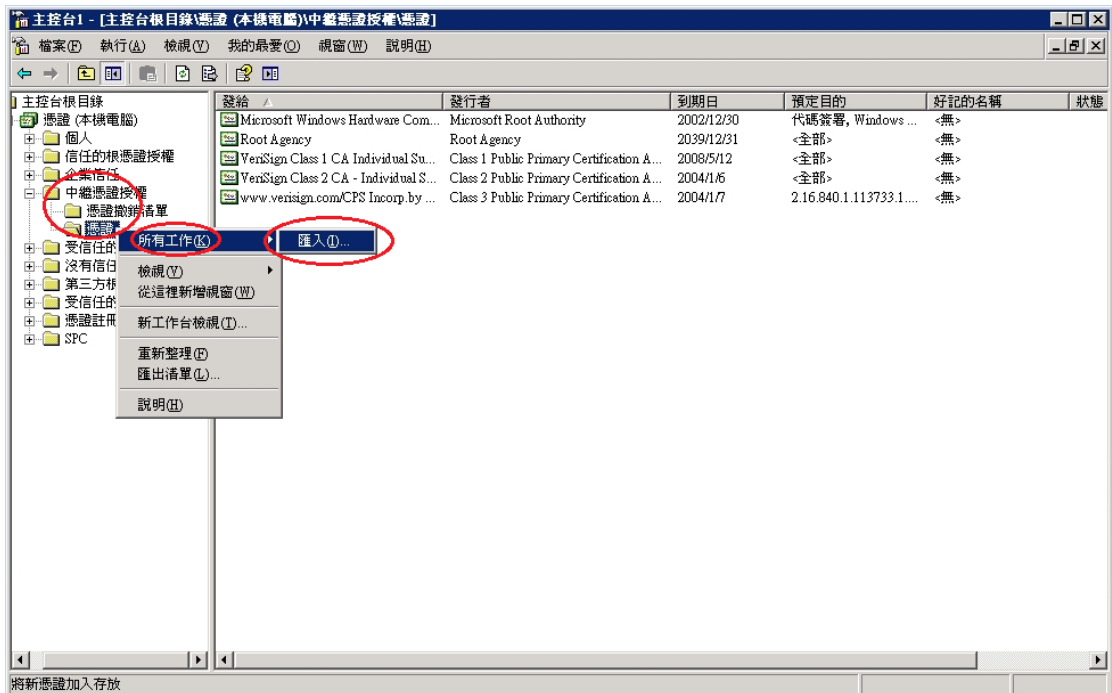
匯入完成後，請在「信任的根憑證授權」→「憑證」以滑鼠按下右鍵，點選「重新整理」。



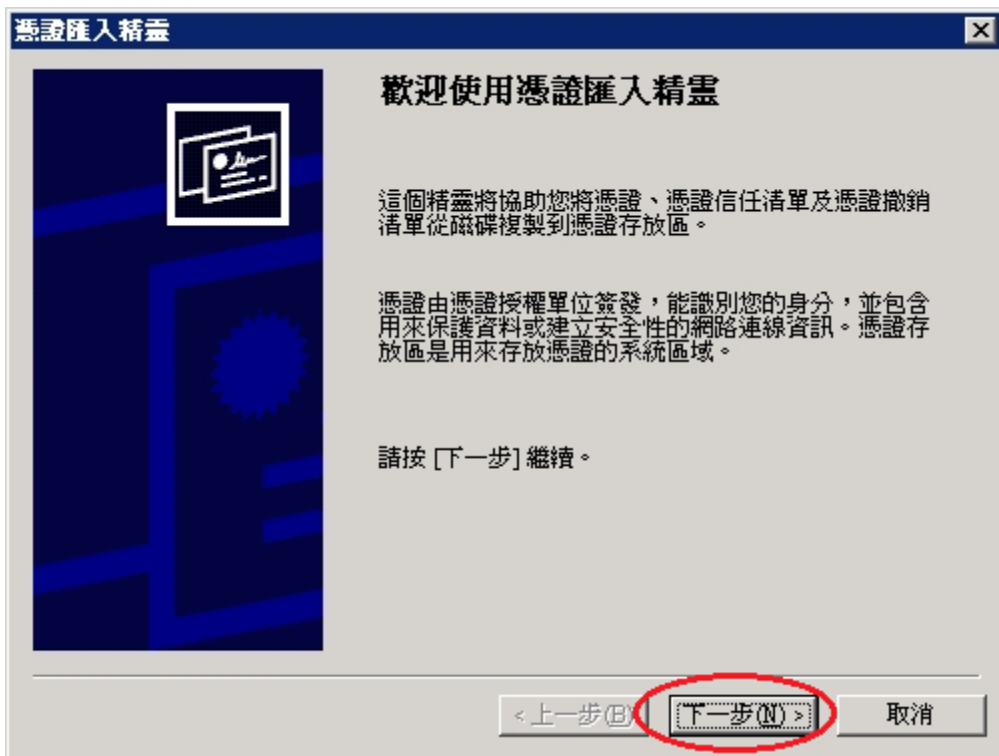
檢查一下，找到「ePKI Root Certification Authority」且看到憑證到期日為 2034/12/19 即是 eCA 憑證有匯入成功。



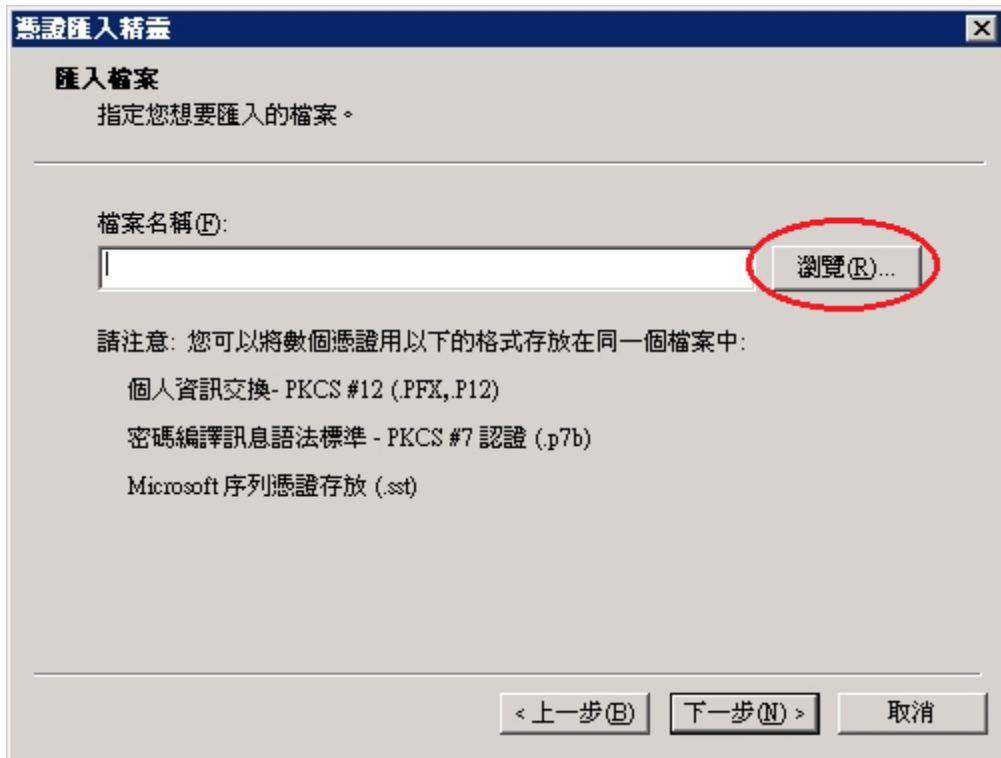
四、於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「中繼憑證授權」→「憑證」→「所有工作(K)」→「匯入(I)」。



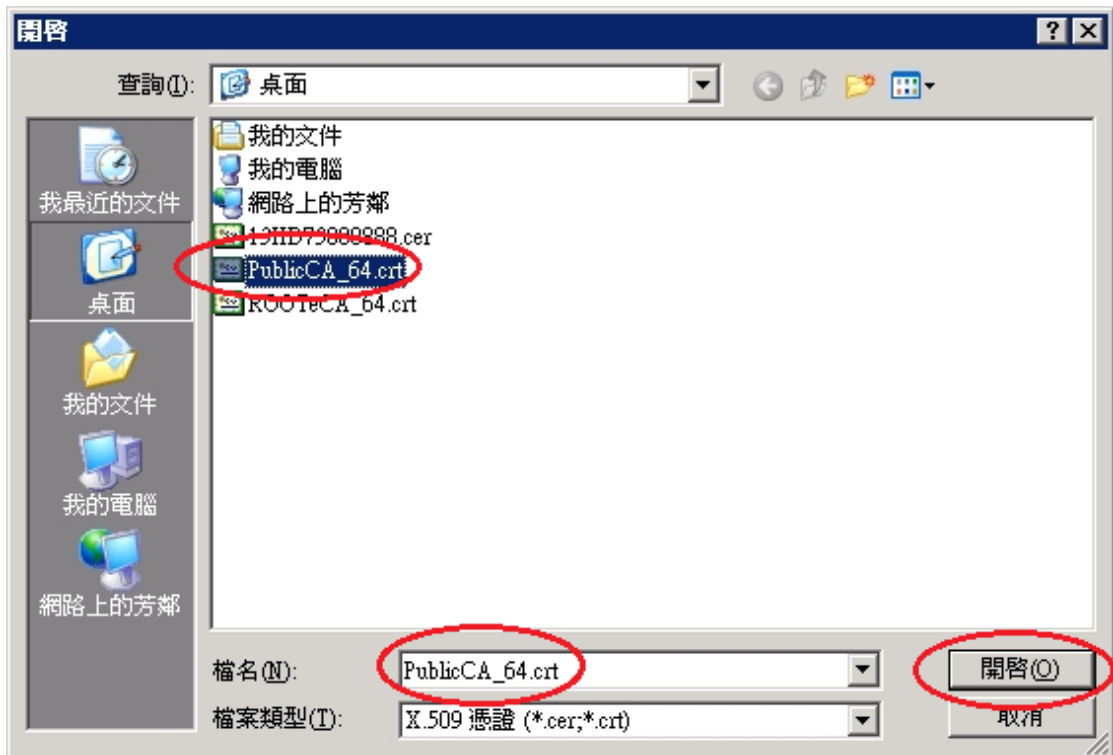
接著出現「憑證匯入精靈」畫面，於「歡迎使用憑證匯入精靈」點選「下一步」按鈕。



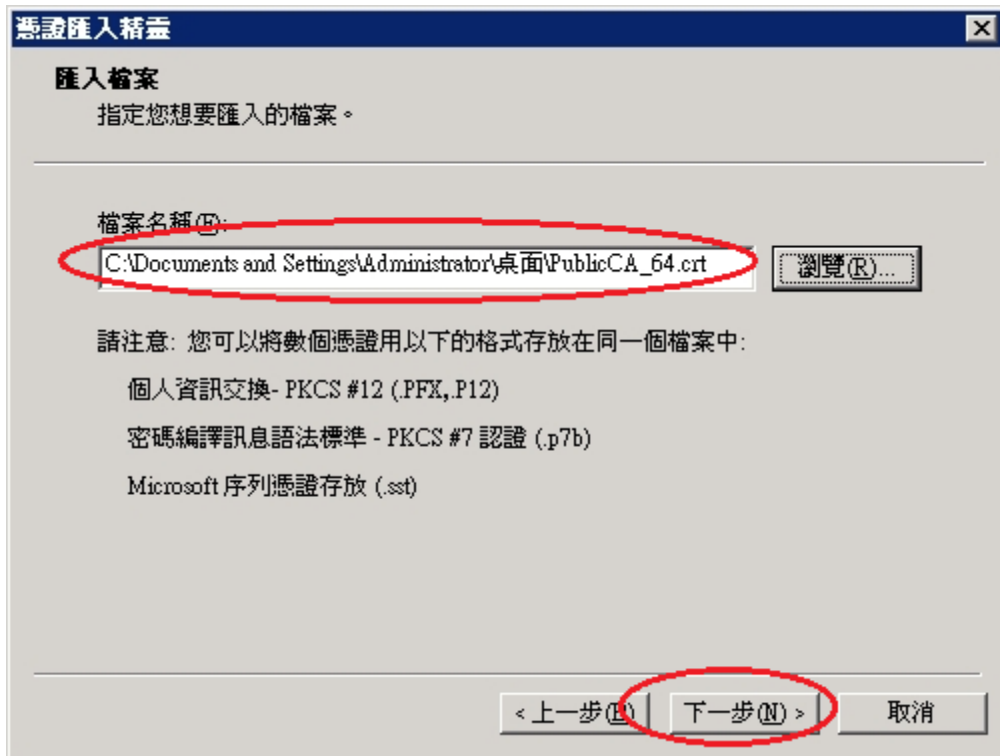
接著出現「匯入檔案」畫面，點選瀏覽選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。



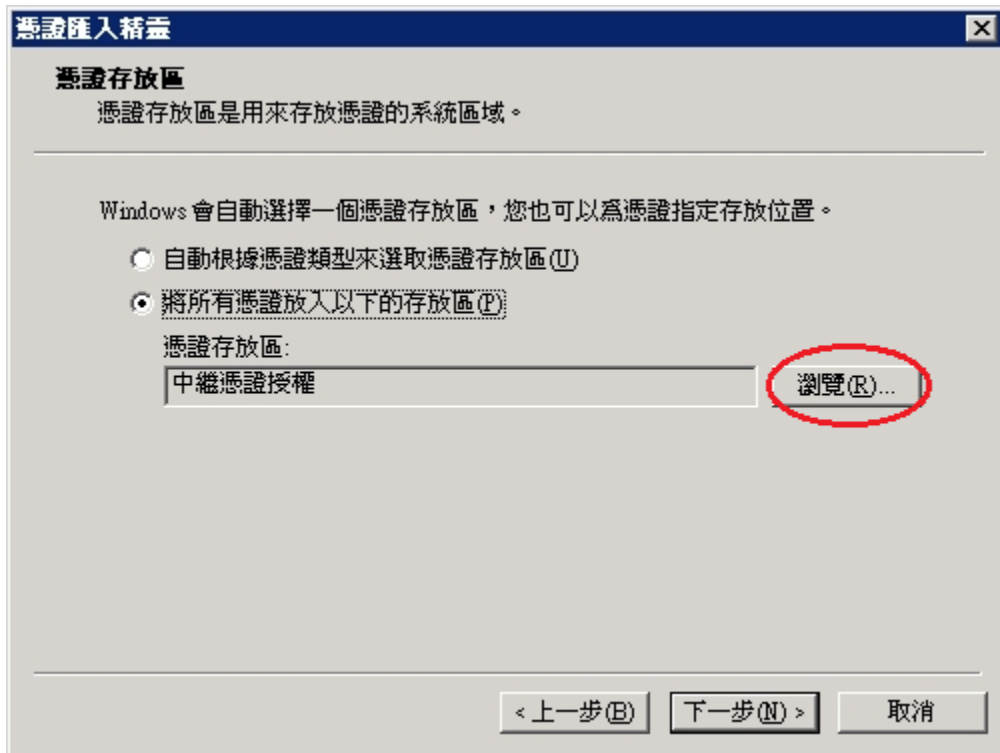
如果有按下「瀏覽」，則可選擇要匯入的檔案路徑及中繼憑證檔檔名 (PublicCA_64.crt)。選取完成後，按下「開啟」後，接著會跳回「匯入檔案」頁面，並於頁面上出現要匯入的檔案路徑及檔案名稱。



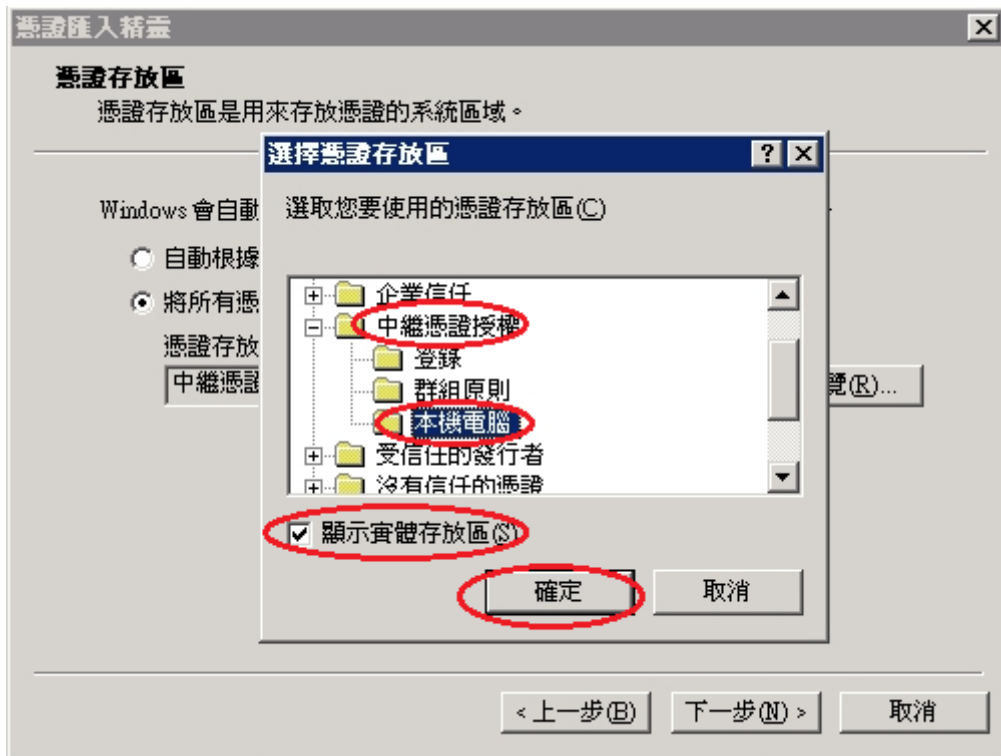
選取完成後，接著以滑鼠按下「下一步」按鈕。



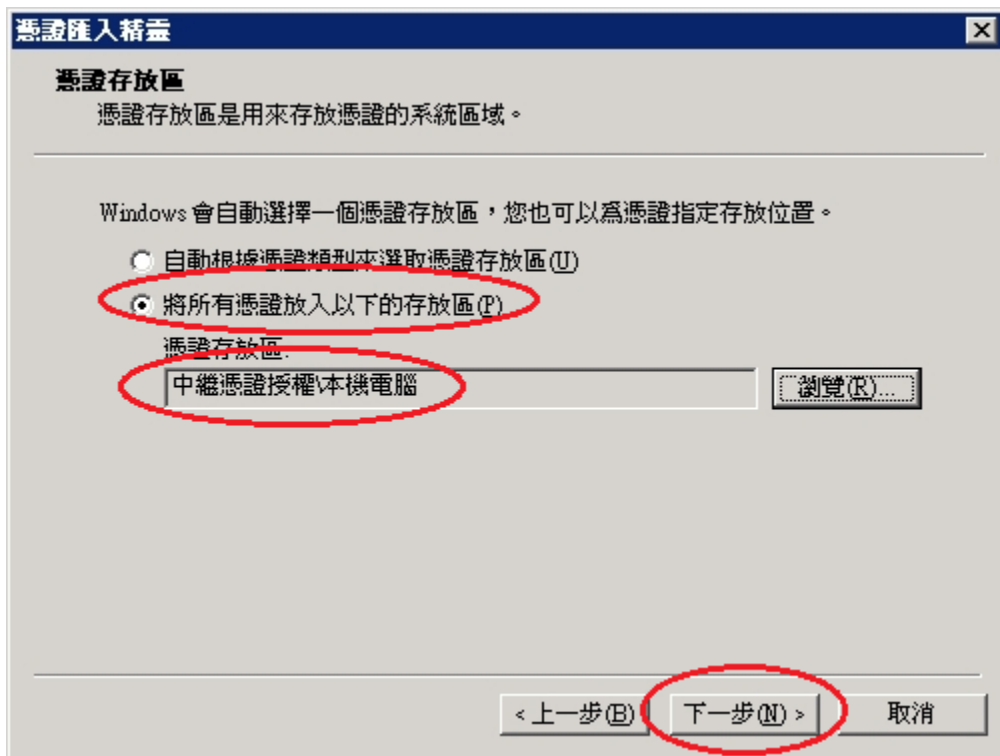
接著出現「憑證存放區」畫面，點選「將所有憑證放入以下的存放區 (P)」，點選「瀏覽」按鈕。



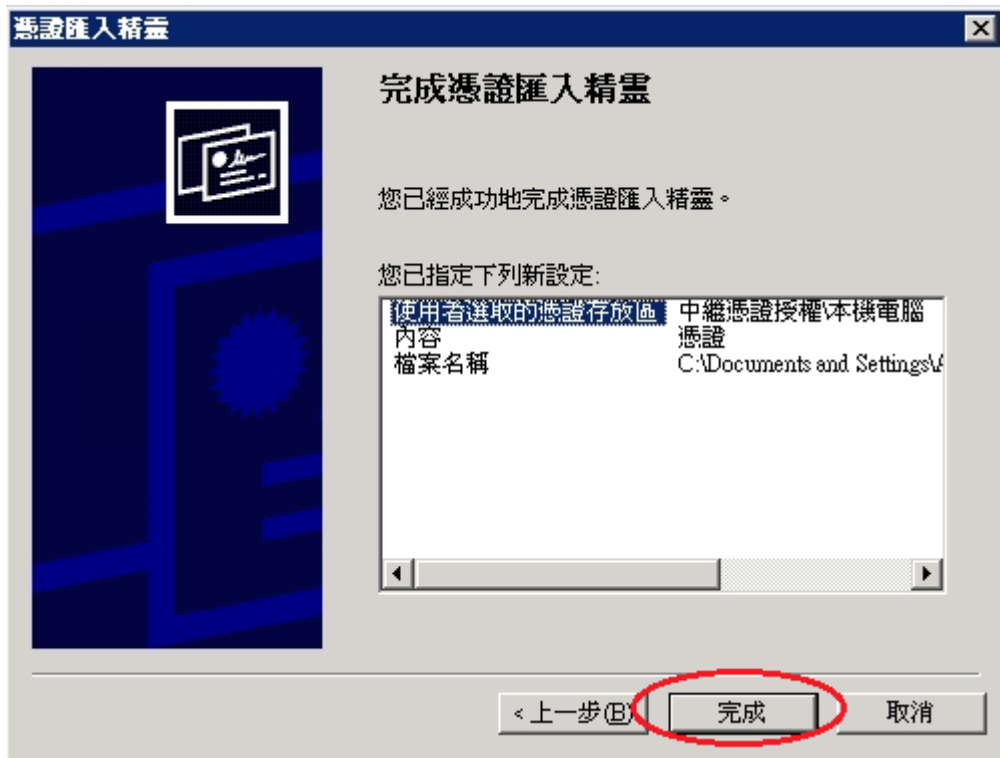
接著出現「選擇憑證存放區」畫面，先點選「顯示實體存放區 (S)」，選擇「中繼憑證授權」→「本機電腦」後，並點選「確定」按鈕。



回到「憑證存放區」畫面後，以滑鼠按下「下一步」按鈕。



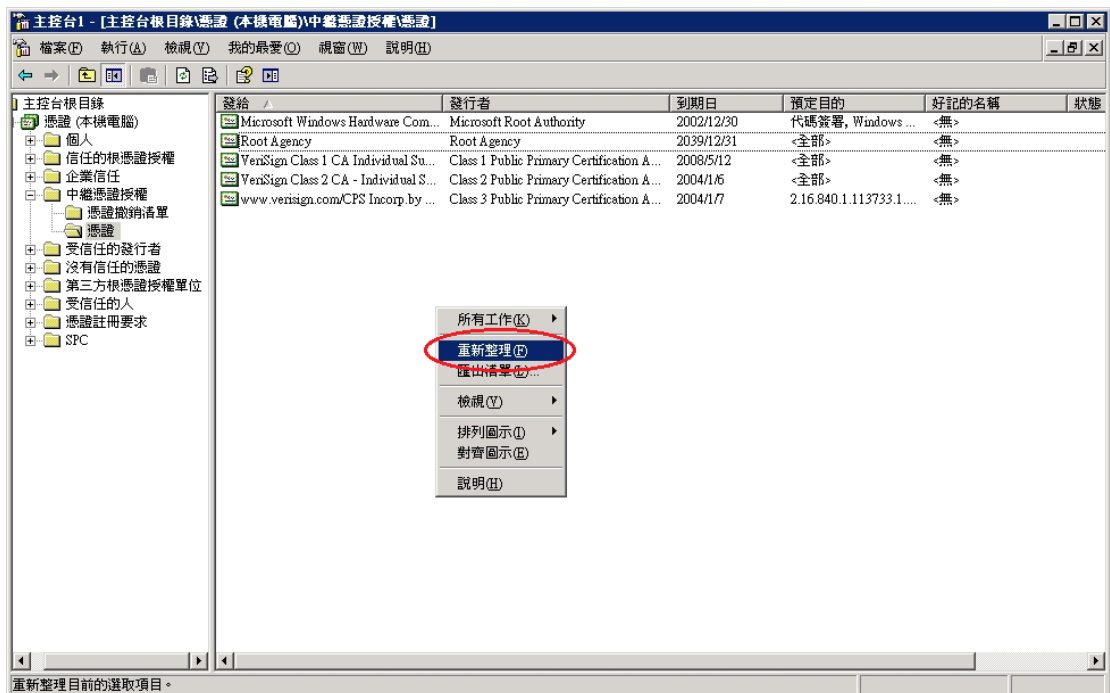
接著出現「完成憑證匯入精靈」頁面，按下「完成」以完成 PublicCA 中繼憑證匯入動作。



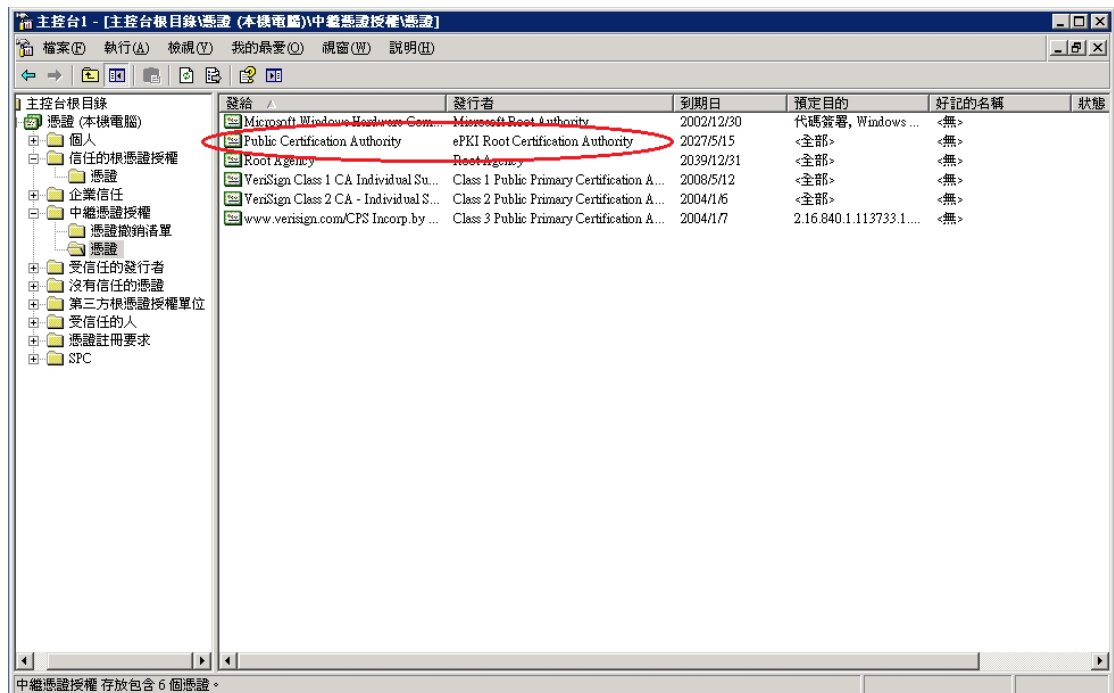
匯入完成，會出現如下訊息「匯入執行成功」訊息。



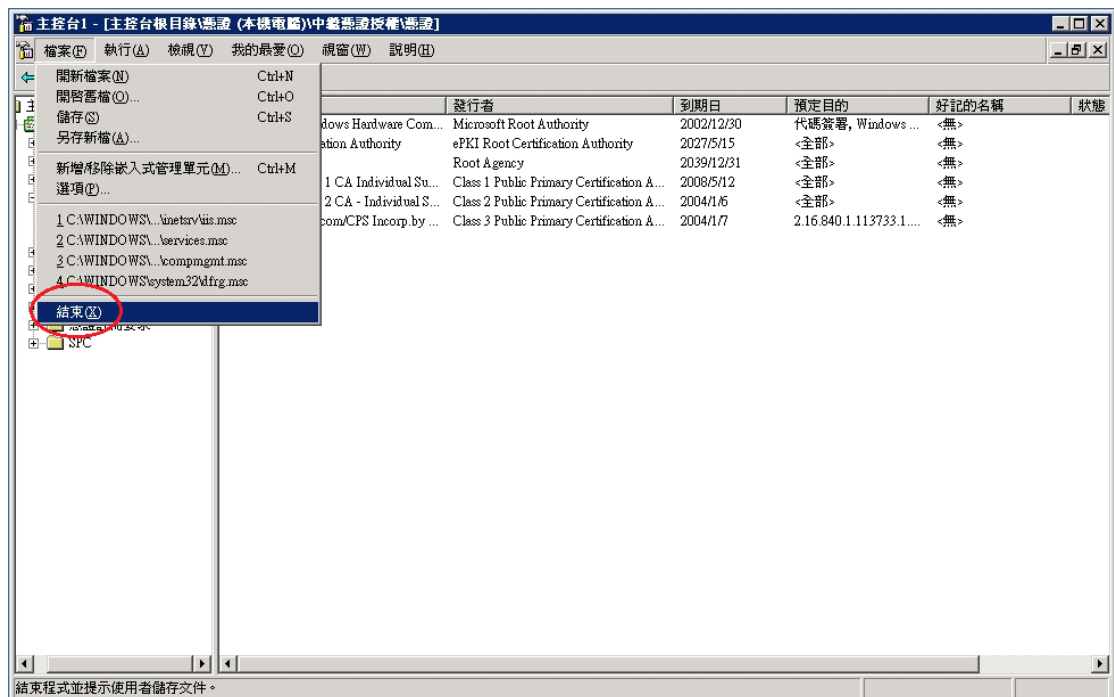
匯入完成後，請在「中繼憑證授權憑證」→「憑證」以滑鼠按下右鍵，點選「重新整理」。



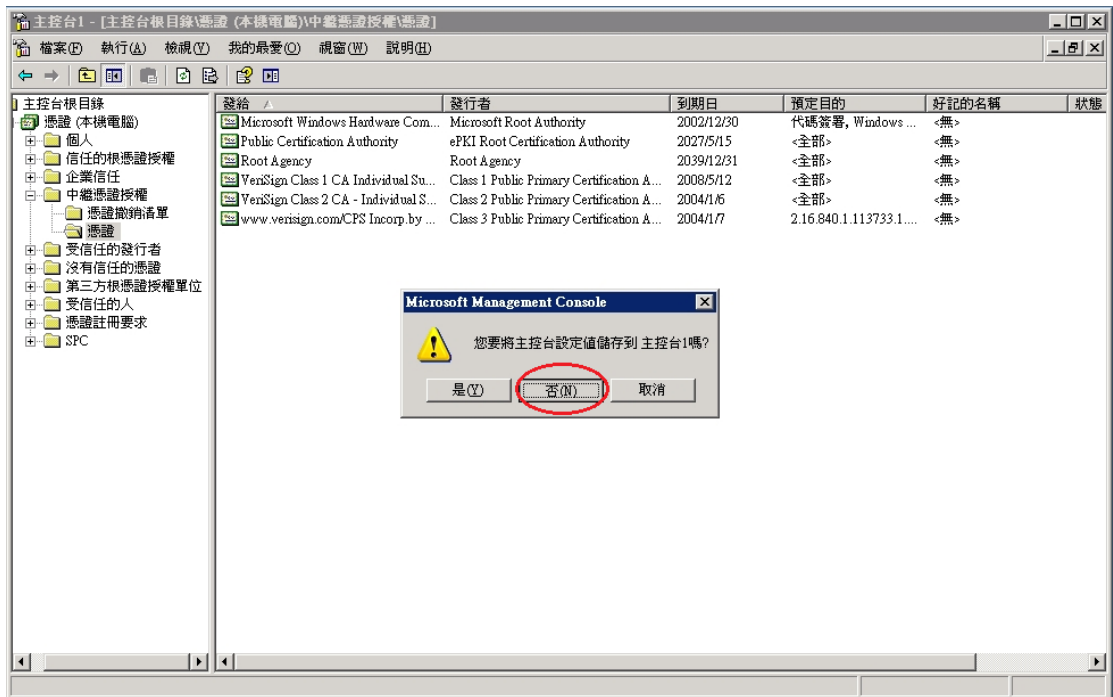
檢查一下，找到「Public Certification Authority」且看到憑證到期日為 2027/5/15 即是 PublicCA 中繼憑證有匯入成功。



回到「主控台」頁面，點選「檔案」→「結束」，以結束「主控台」。



接著會跳出「您要將主控台設定值儲存到主控台 1 嗎？」訊息，點選「否」，結束「主控台」。



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

六、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 SSLSealisppec.txt，將網站 SSL 安全認證標章安裝成功。

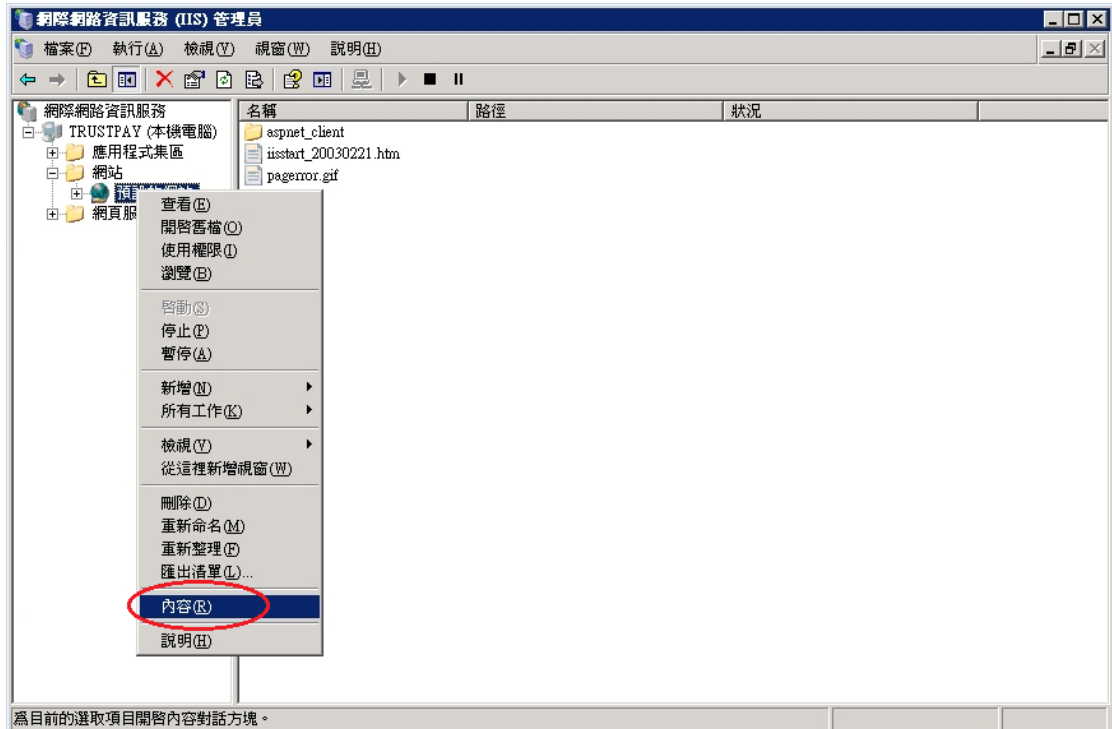
從未安裝過憑證的伺服器，安裝憑證操作步驟

一、將「網際網路資訊服務(IIS)管理員」開啟。

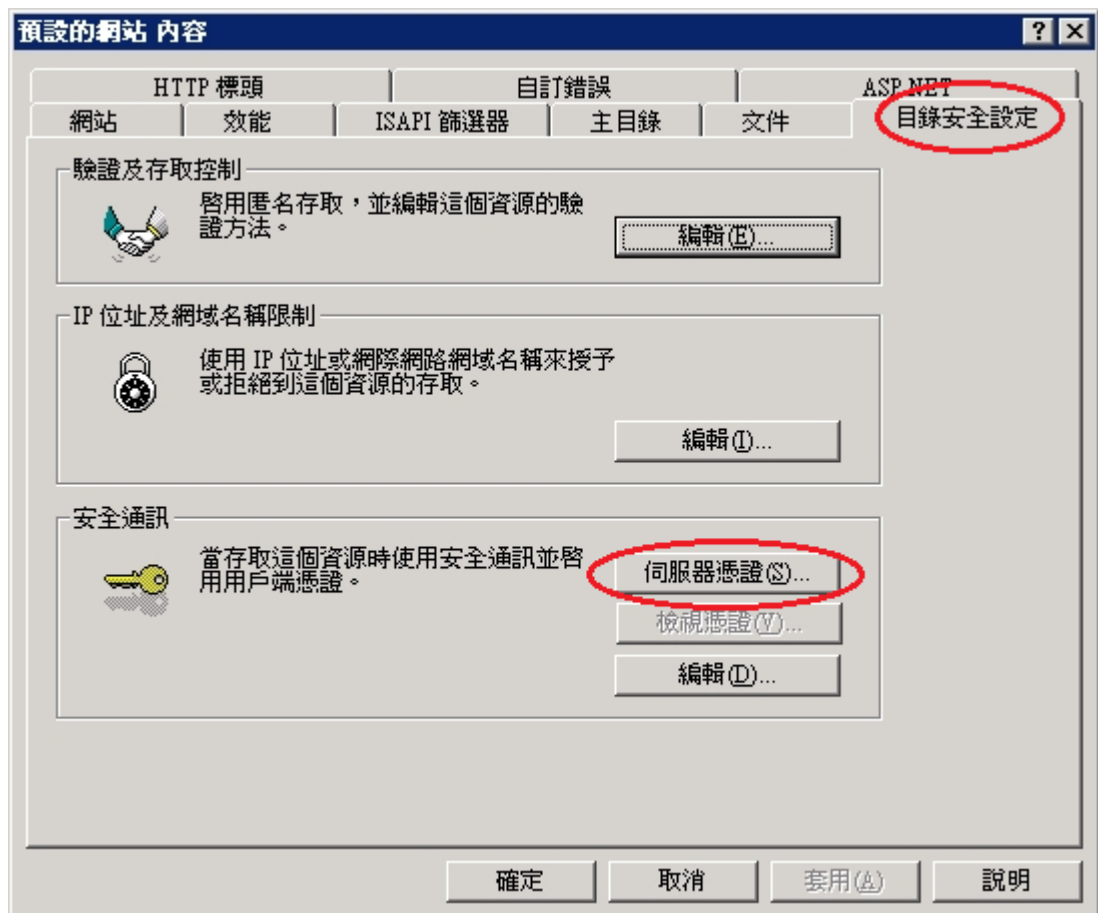


二、安裝 SSL 憑證

於之前申請憑證網站的站台上按滑鼠右鍵點選「內容」。

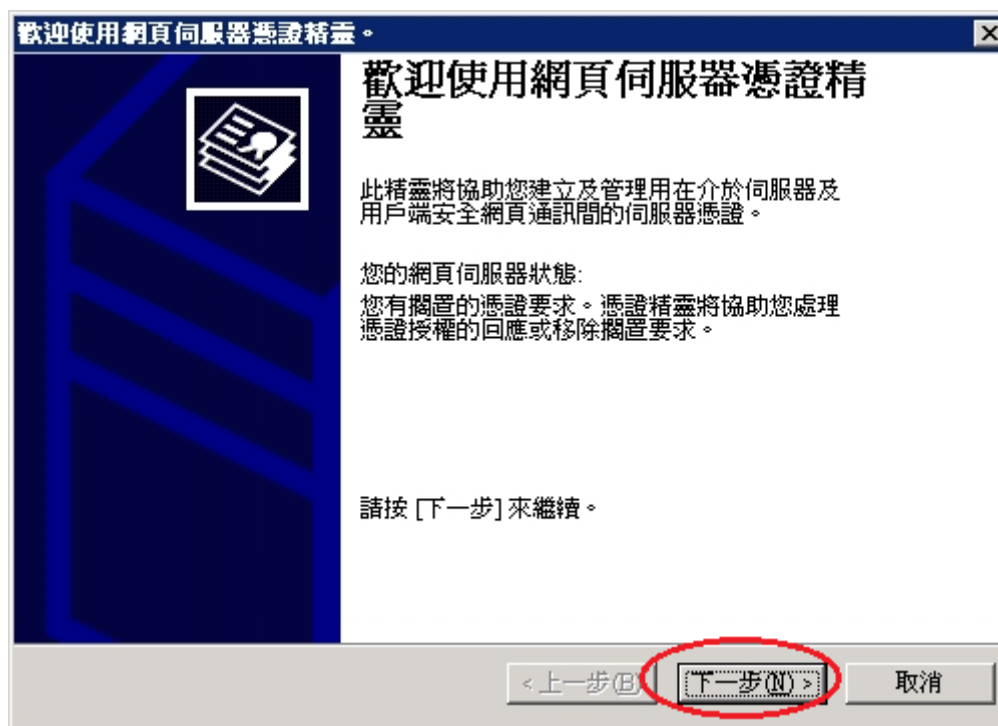


接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。

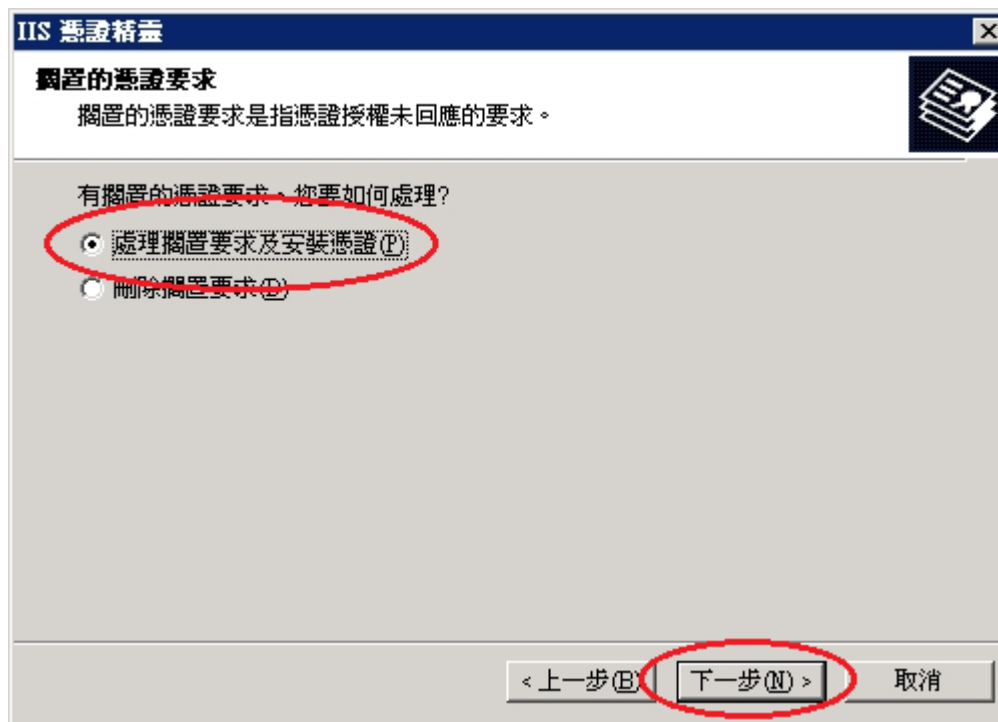


接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，以滑鼠按下「下一步」

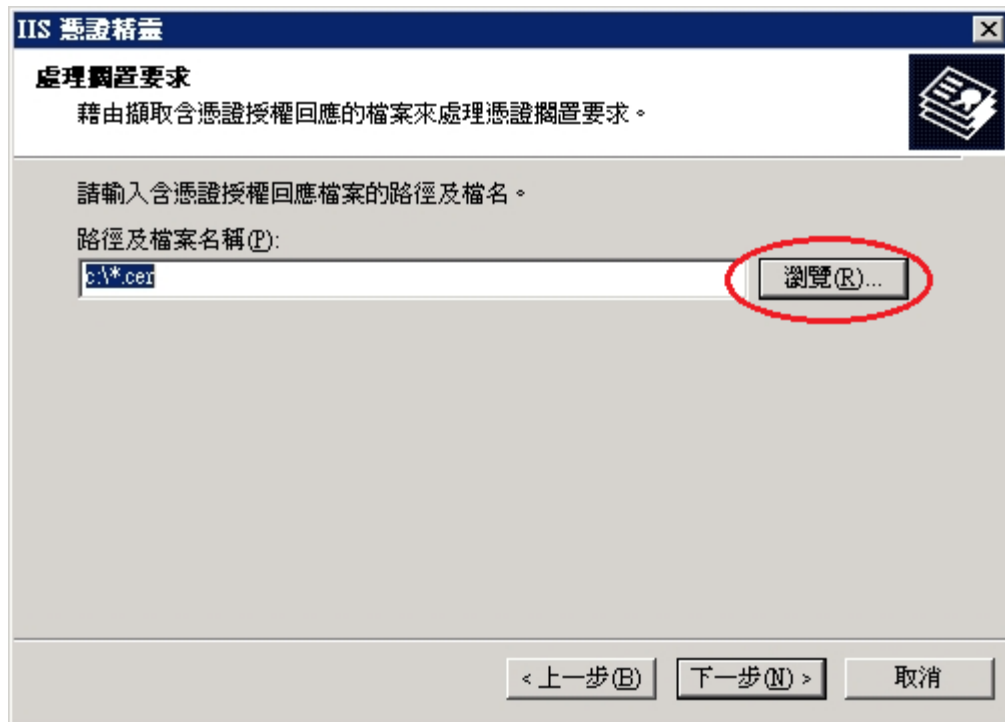
按鈕，開始安裝 Windows 2003 IIS 6.0 伺服器憑證。



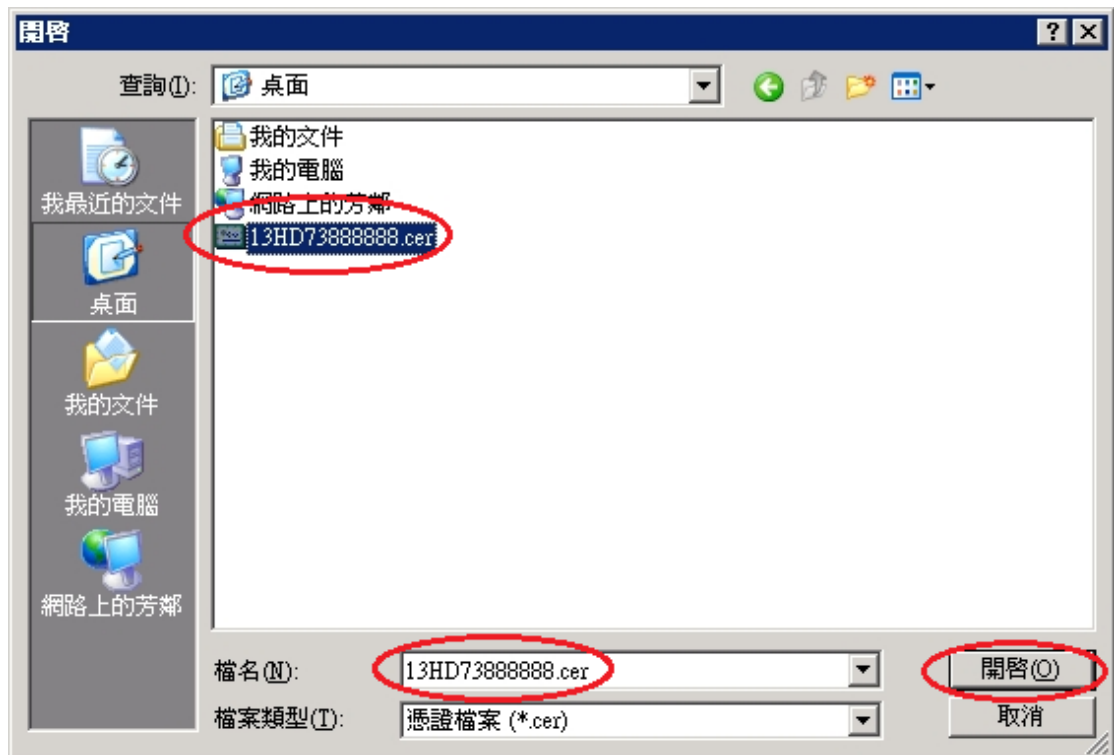
接著畫面會到「擱置的憑證要求」視窗，點選「處理擱置要求及安裝憑證(P)」，以滑鼠按下「下一步」按鈕，開始安裝 Windows 2003 IIS 6.0 伺服器憑證。



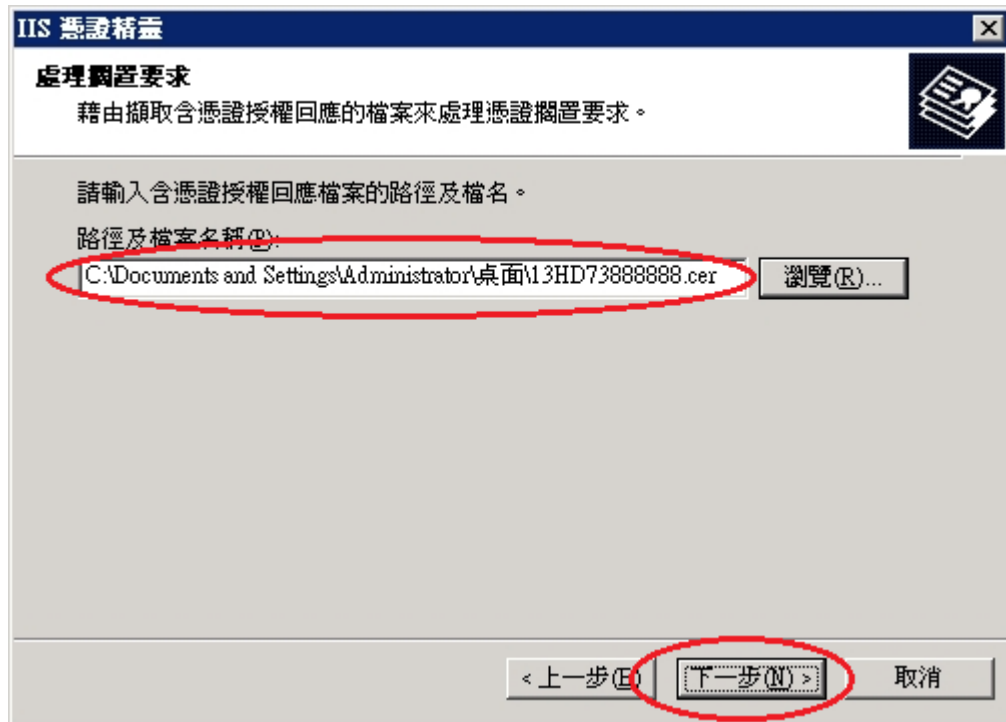
接著畫面會到「處理擱置要求」視窗，點選「瀏覽」選擇存放位置，或直接在「路徑及檔案名稱(P)」欄位打上路徑及檔案名稱也可以。



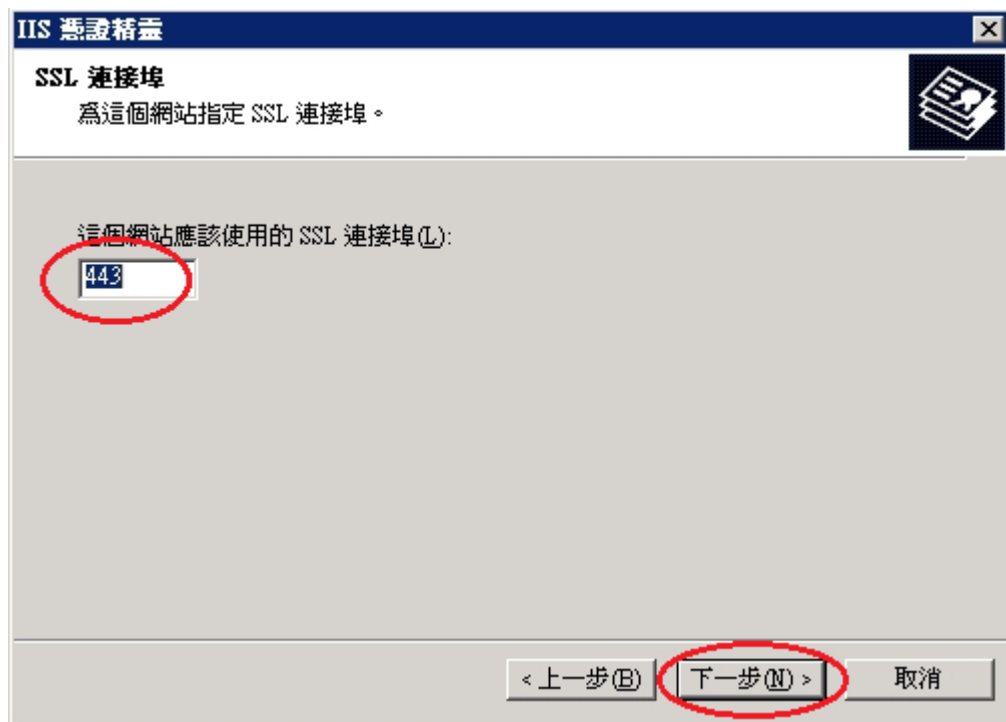
如果有按下「瀏覽」，則可選擇檔案路徑及輸入所要開啟的 SSL 伺服器憑證.cer 檔檔名（中華電信通用憑證管理中心(PublicCA)核發的伺服器 SSL 憑證檔名類似 00HD73000000.cer）。輸入完成後，按下「開啟」後，接著會跳回「處理擱置要求」頁面，並於頁面上出現存放檔案路徑及檔案名稱。



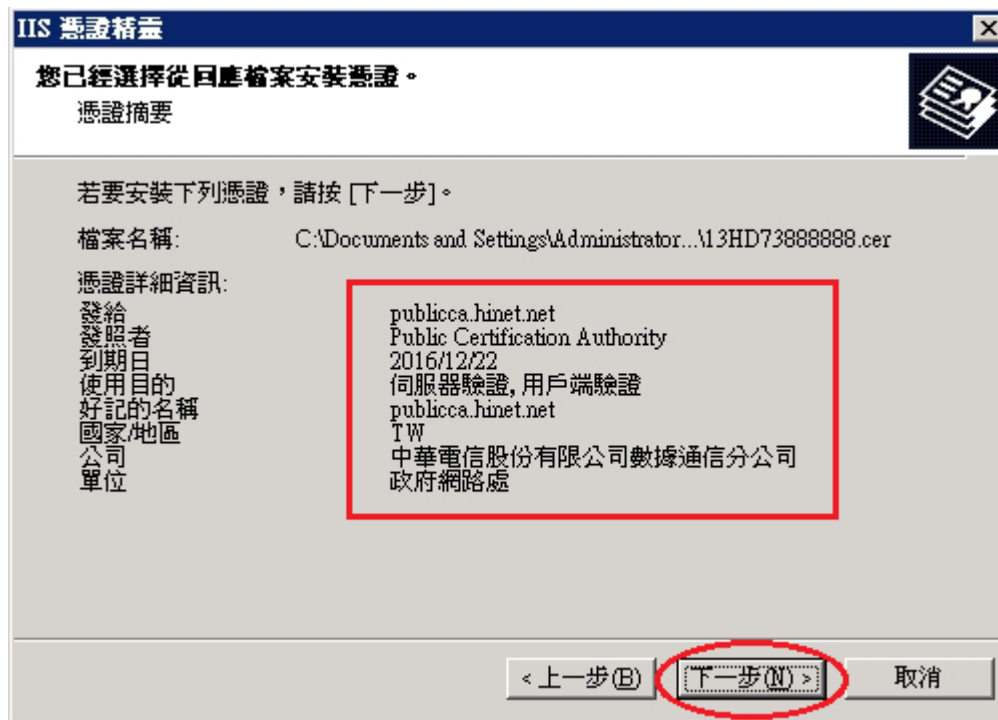
開啟完成後，接著以滑鼠按下「下一步」按鈕。



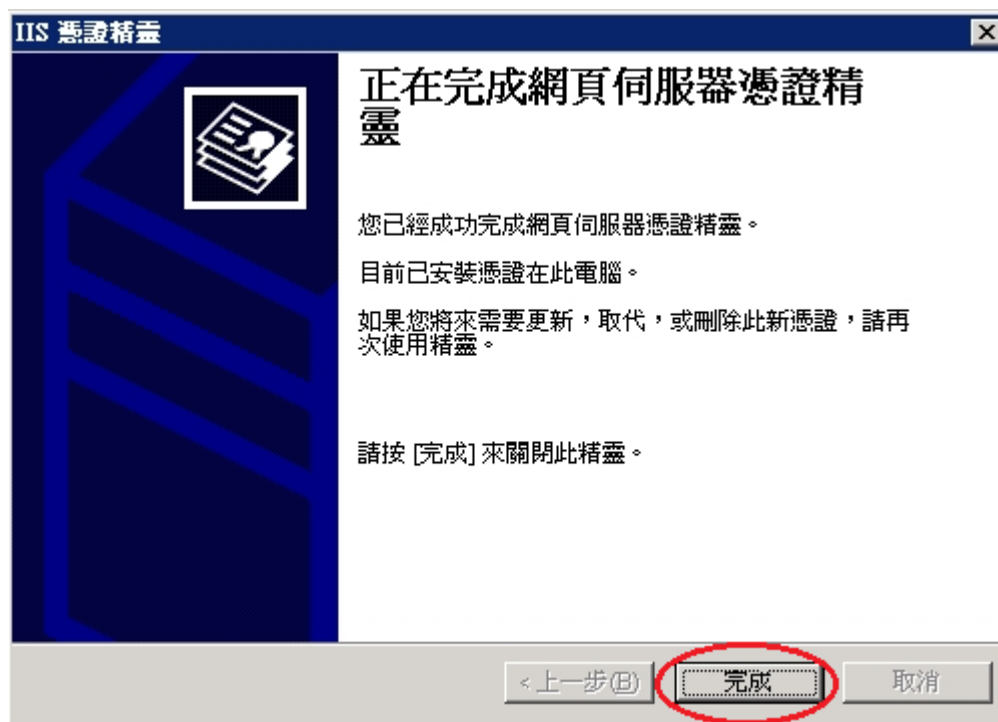
接著出現「SSL 連接埠」頁面，並設定「這個網站應該使用的 SSL 連接埠(L)」，請依網站需求自行設定，接著以滑鼠按下「下一步」按鈕。



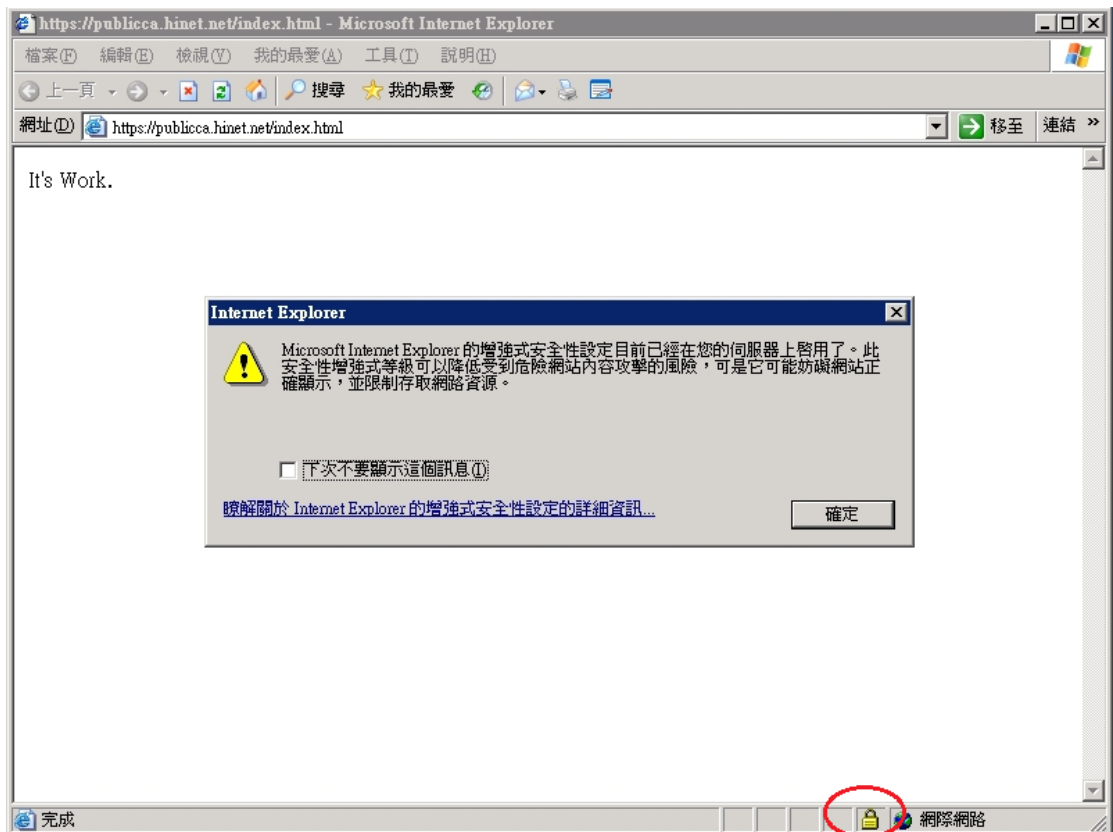
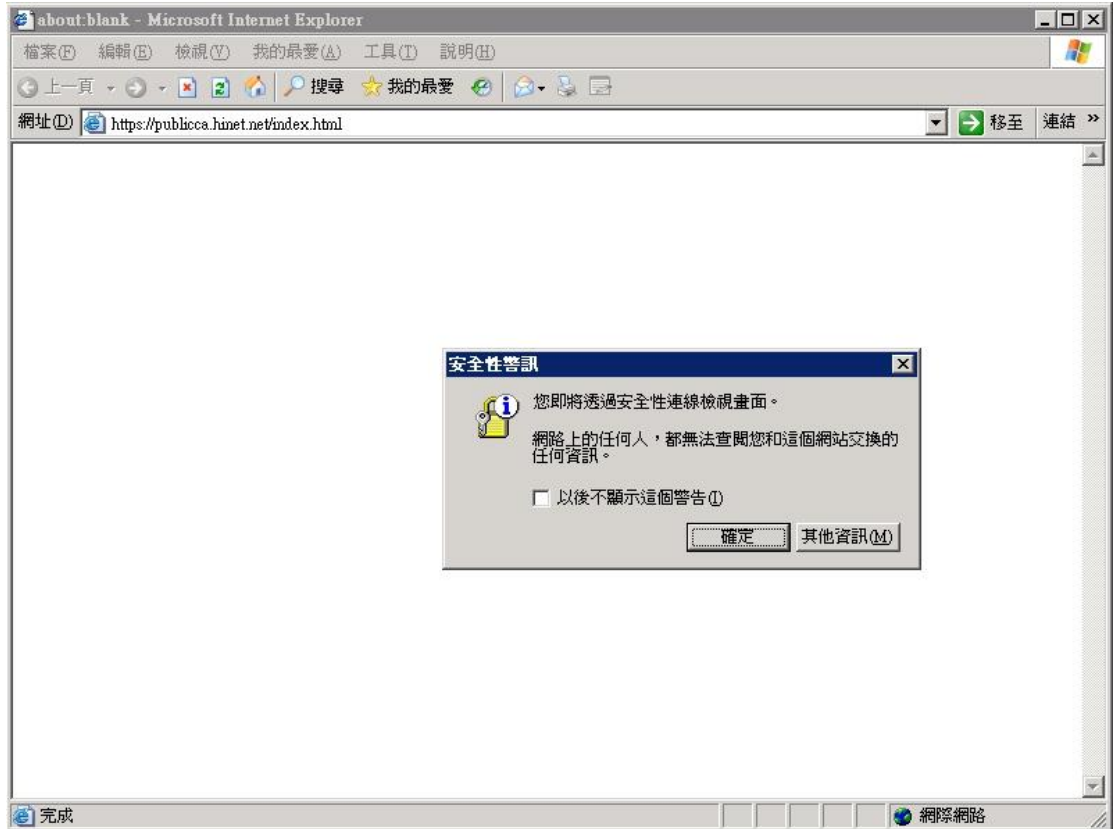
接著出現「憑證摘要」頁面，確認憑證內容無誤後，接著以滑鼠按下「下一步」按鈕。



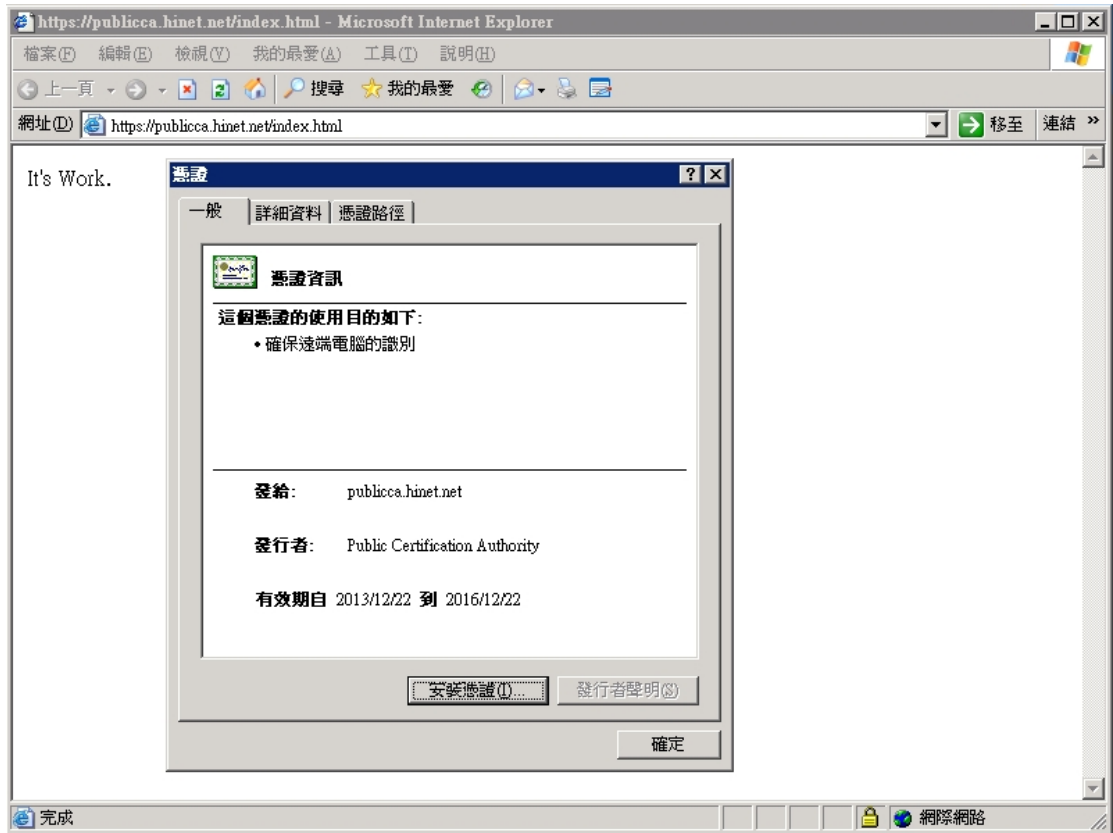
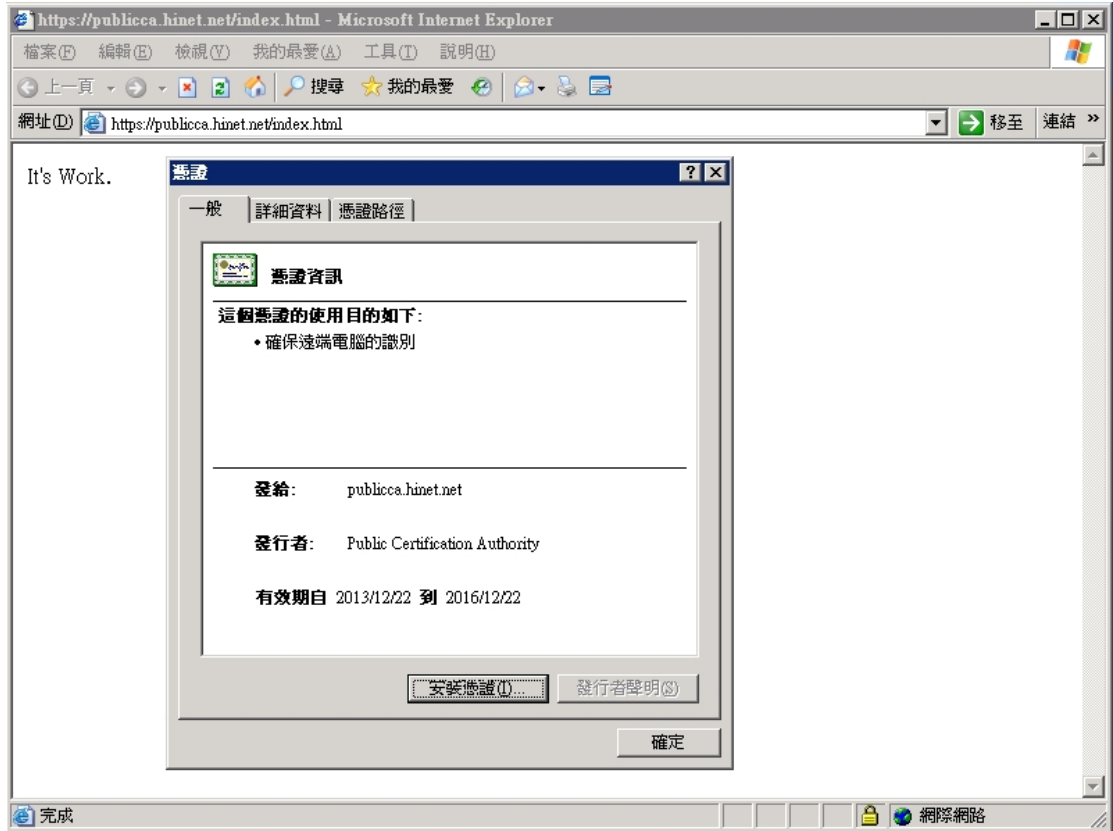
接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成匯入憑證.cer 檔動作。

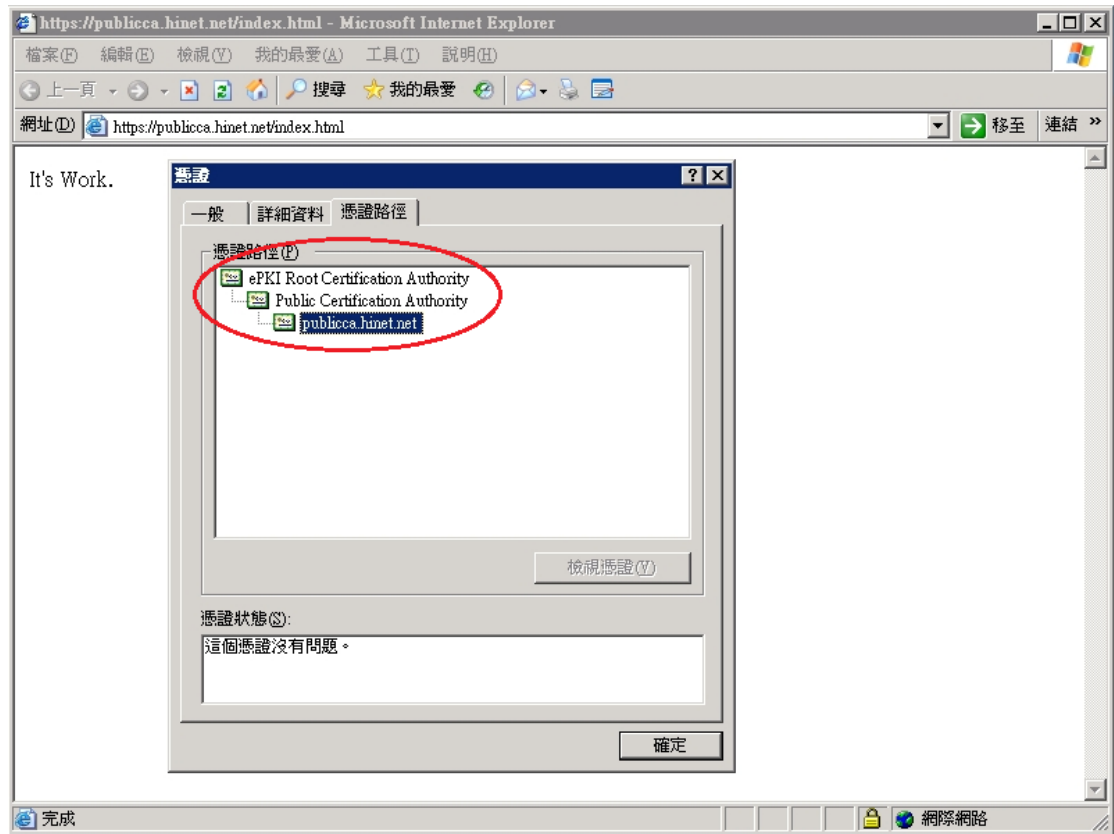


三、透過瀏覽器連線測試網頁 https 是否連線正常。



檢查 SSL 憑證串鏈是否正常。



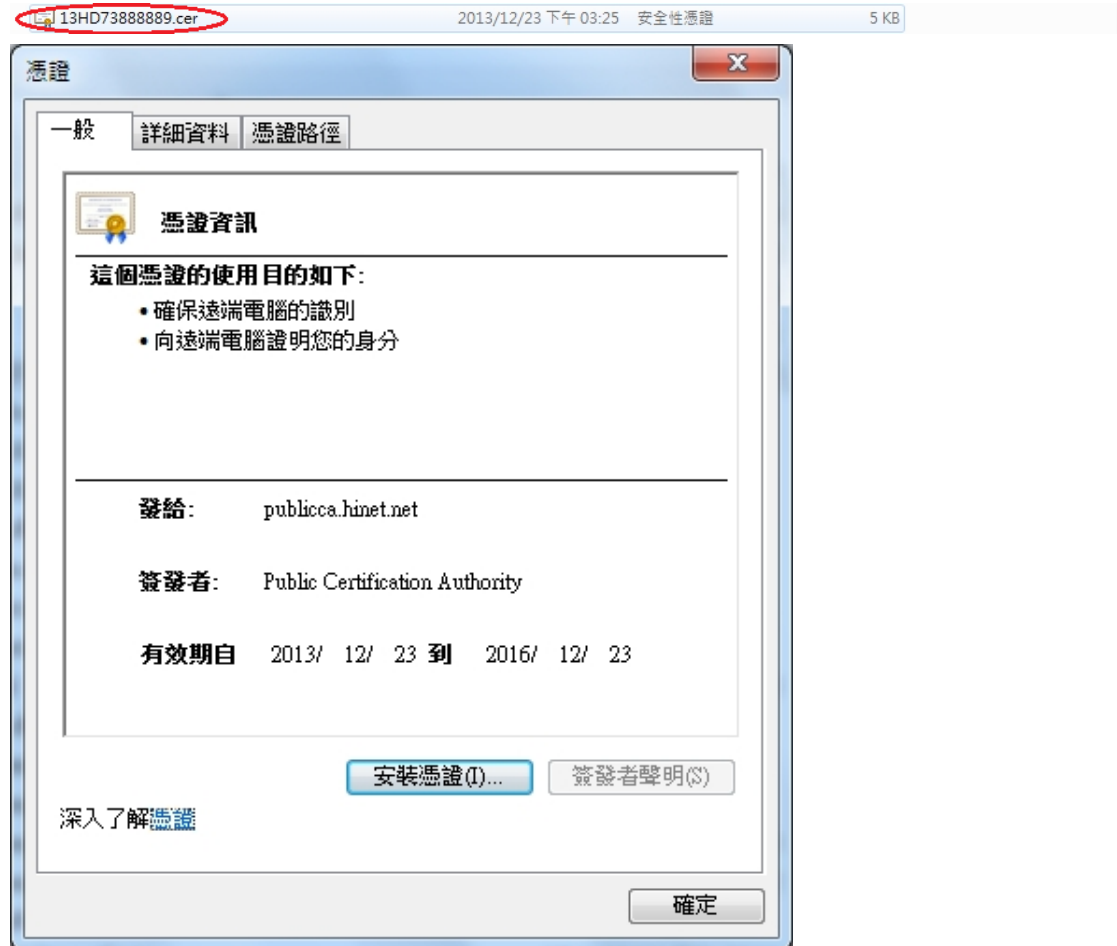


四、依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

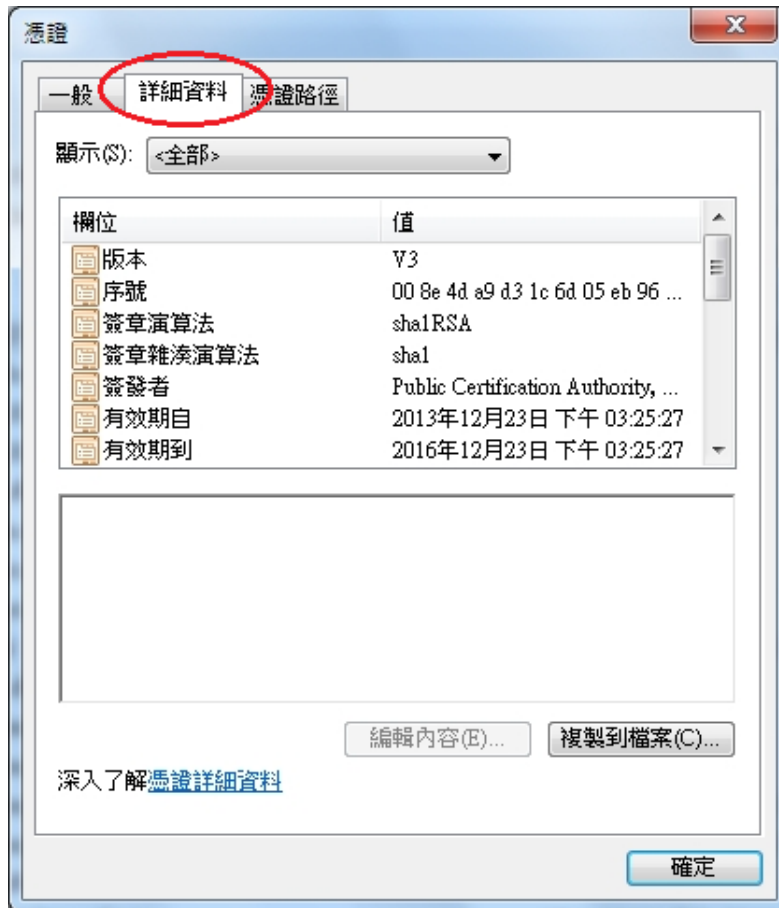
已安裝過憑證的伺服器，安裝憑證操作步驟

一、將憑證核發的伺服器 SSL 憑證轉換成 P7B 格式的憑證檔。

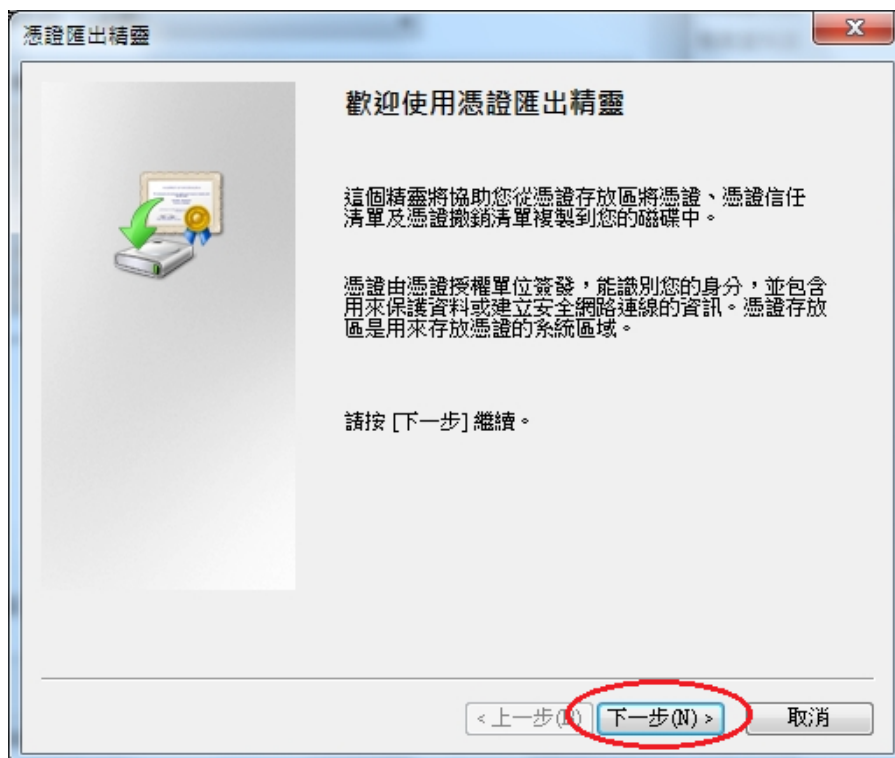
在 Microsoft Windows 作業系統下，將中華電信通用憑證管理中心 PublicCA 核發的憑證 00HD73000000.cer 以滑鼠點兩下打開。



切換至「詳細資料」頁面。

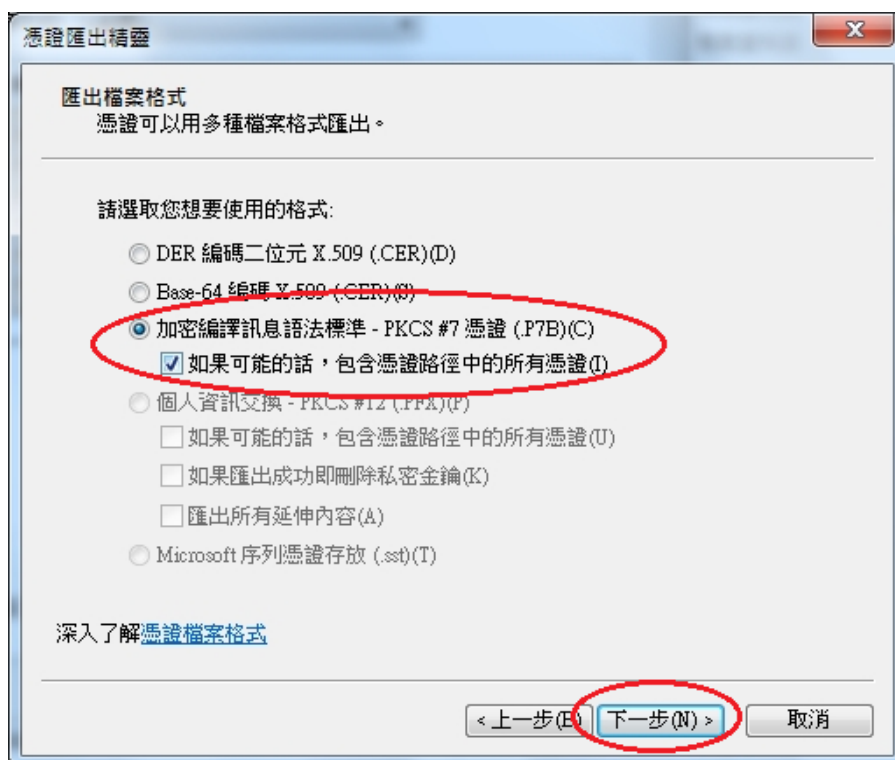


接著出現「憑證匯出精靈」畫面，於「歡迎使用憑證匯出精靈」點選「下一步」按鈕。

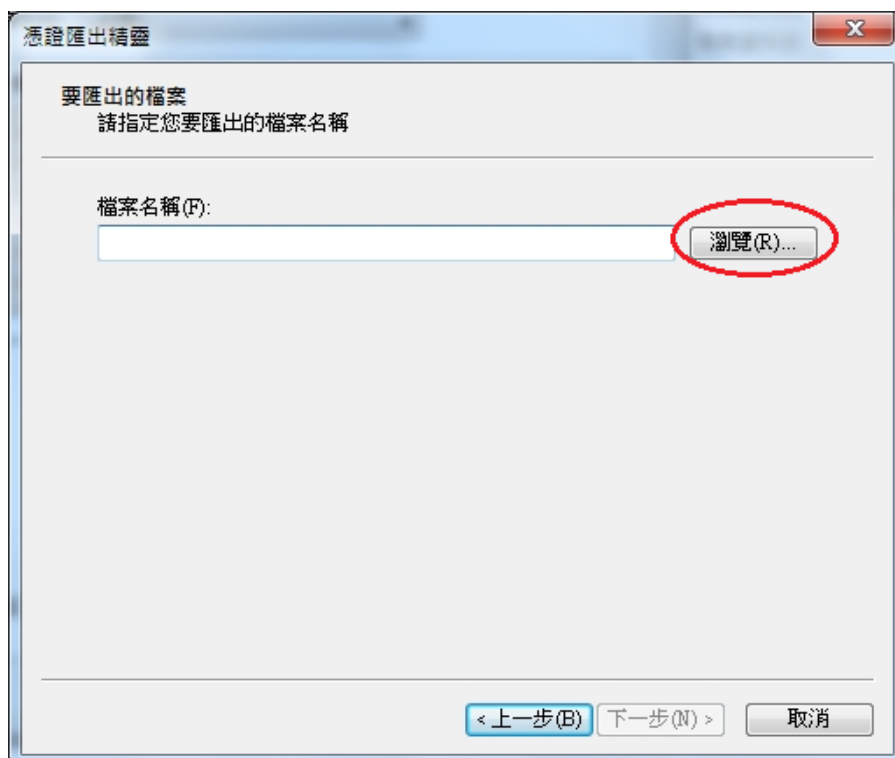


接著出現「匯出檔案格式」畫面，點選「加密編譯訊息語法標準 - PKCS #7

憑證 (.P7B)(C)」，並勾選「如果可能的話，包含憑證路徑中的所有憑證(I)」，以滑鼠點選「下一步」按鈕。

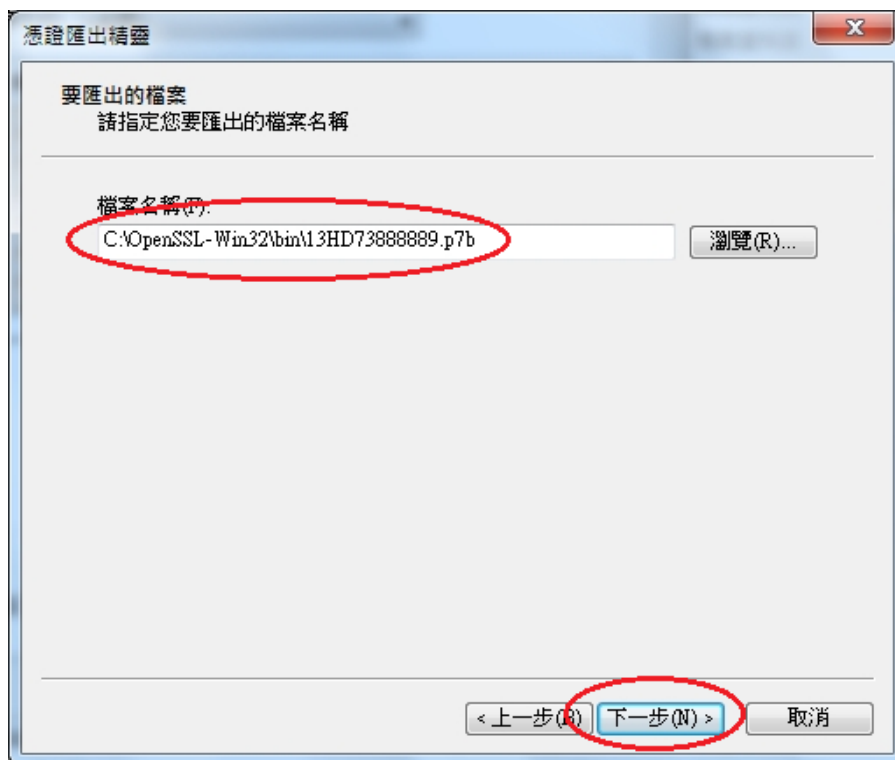


接著出現「要匯出的檔案」畫面，點選「瀏覽」選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。

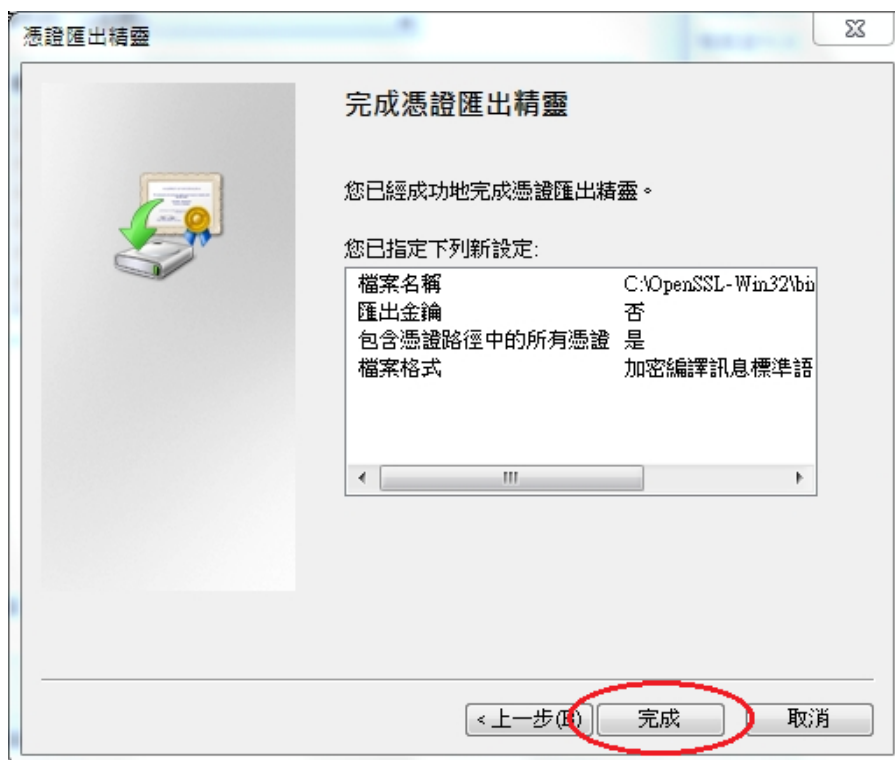


如果有按下「瀏覽」，則可選擇要匯出的檔案路徑及要匯出核發的伺服器 SSL 憑證檔檔名(.P7B)。輸入完成，按下儲存後，接著會跳回「要匯出的檔案」

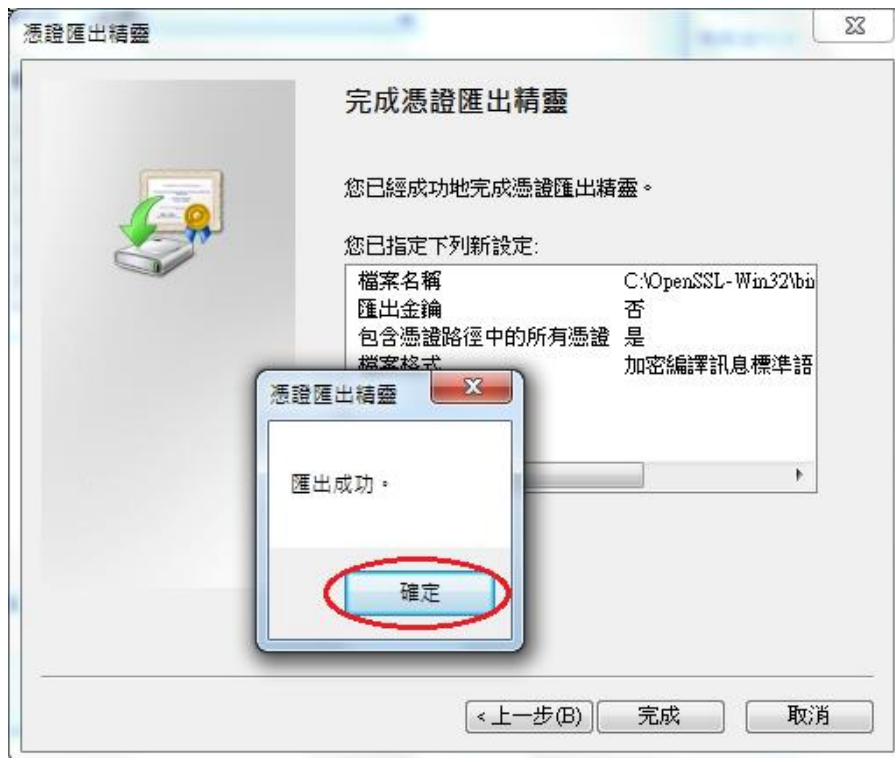
頁面，並於頁面上出現要儲存的檔案路徑及檔案名稱，並點選「下一步」按鈕。



接著出現「完成憑證匯出精靈」頁面，按下「完成」以完成伺服器 SSL 憑證檔 (.P7B)匯出動作。



匯出完成，會出現如下訊息「匯出成功」訊息。



二、使用 OpenSSL 將產製請求檔匯出的金鑰及憑證取出金鑰，及與新核發的憑證結合為.pfx 檔。

接著使用 Windows OpenSSL 將產製請求檔匯出的金鑰及憑證取出金鑰，此時會需要匯出私密金鑰及憑證檔.pfx 檔的密碼。

指令：

```
openssl pkcs12 -in filename.pfx -out filename.pem
```

範例：

```
openssl pkcs12 -in publicca_ReqBackup.pfx -out publicca_ReqBackup.pem
```

指令：

```
openssl rsa -in filename.pem -out filename.key
```

範例：

```
openssl rsa -in publicca_ReqBackup.pem -out publicca_ReqBackup.key
```

```
命令提示字元
c:\OpenSSL-Win32\bin>dir publicca_ReqBackup.pfx
磁碟區 C 中的磁碟是 系統磁碟
磁碟區序號: 128E-E610

c:\OpenSSL-Win32\bin 的目錄

2013/12/23 下午 03:24          2,585 publicca_ReqBackup.pfx
                1 個檔案          2,585 位元組
                0 個目錄      47,963,156,400 位元組可用

c:\OpenSSL-Win32\bin>openssl pkcs12 -in publicca_ReqBackup.pfx -out publicca_ReqBackup.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

c:\OpenSSL-Win32\bin>openssl rsa -in publicca_ReqBackup.pem -out publicca_ReqBackup.key
Enter pass phrase for publicca_ReqBackup.pem:
writing RSA key

c:\OpenSSL-Win32\bin>openssl pkcs7 -in 13HD73888889.p7b -inform DER -print_certs -out 13HD73888889.pem

c:\OpenSSL-Win32\bin>openssl pkcs12 -export -in 13HD73888889.pem -inkey publicca_ReqBackup.key -out publicca_ReqBackup.pfx
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'

c:\OpenSSL-Win32\bin>
```

將上面所匯出的憑證檔(.P7B)檔案轉成 Base64 格式。

指令：

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

範例：

```
openssl pkcs7 -in 13HD73888889.p7b inform DER -print_certs -out
13HD73888889.pem
```

將取出的請求檔金鑰與新核發憑證結合為私密金鑰及憑證檔.pfx 檔，並設定好密碼。

指令：

```
openssl pkcs12 -export -in filename.pem -inkey filename.key -out filename.pfx
```

範例：

```
openssl pkcs12 -export -in 13HD73888889.pem -inkey publicca_ReqBackup.key
-out publicca_ReqBackup.pfx
```

```

命令提示字元
c:\OpenSSL-Win32\bin>dir publicca_ReqBackup.pfx
磁碟區 C 中的磁碟是 系統磁碟
磁碟區序號: 128E-E610

c:\OpenSSL-Win32\bin 的目錄

2013/12/23 下午 03:24                2,585 publicca_ReqBackup.pfx
1 個檔案                2,585 位元組
0 個目錄            47,963,156,400 位元組可用

c:\OpenSSL-Win32\bin>openssl pkcs12 -in publicca_ReqBackup.pfx -out publicca_ReqBackup.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

c:\OpenSSL-Win32\bin>openssl rsa -in publicca_ReqBackup.pem -out publicca_ReqBackup.key
Enter pass phrase for publicca_ReqBackup.pem:
writing RSA key

c:\OpenSSL-Win32\bin>openssl pkcs7 -in 13HD73888889.p7b -inform DER -print_certs -out 13HD73888889.pem

c:\OpenSSL-Win32\bin>openssl pkcs12 -export -in 13HD73888889.pem -inkey publicca_ReqBackup.key -out publicca_ReqBackup.pfx
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:
unable to write 'random state'

c:\OpenSSL-Win32\bin>

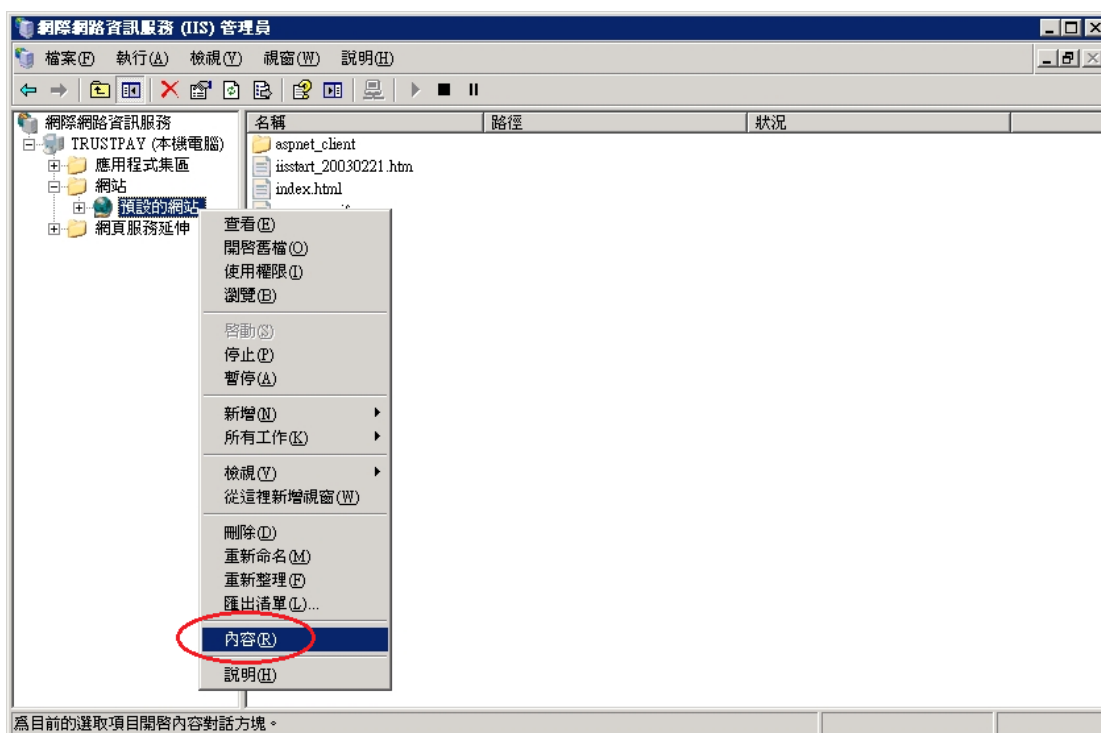
```

三、移除舊私密金鑰及憑證，及將結合後的私密金鑰及憑證匯入要安裝的 Windows 2003 IIS 6.0 伺服器。

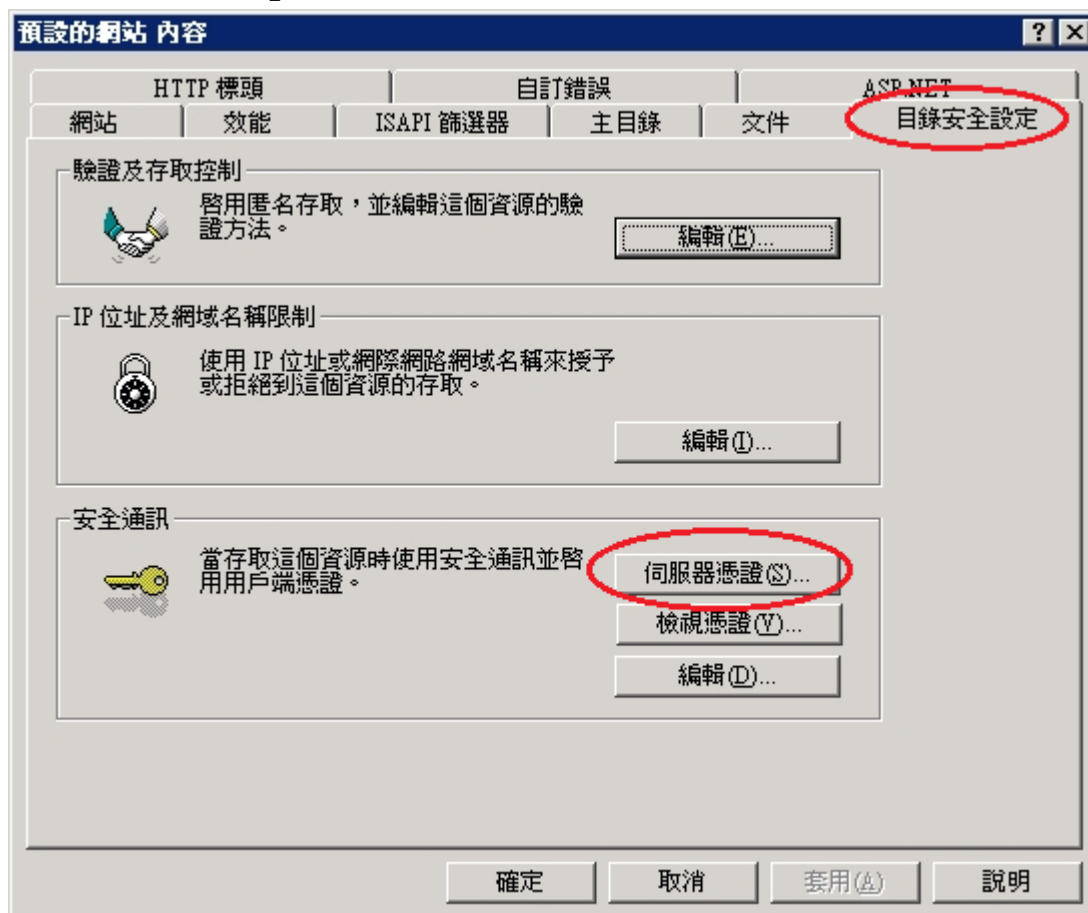
將「網際網路資訊服務(IIS)管理員」開啟。



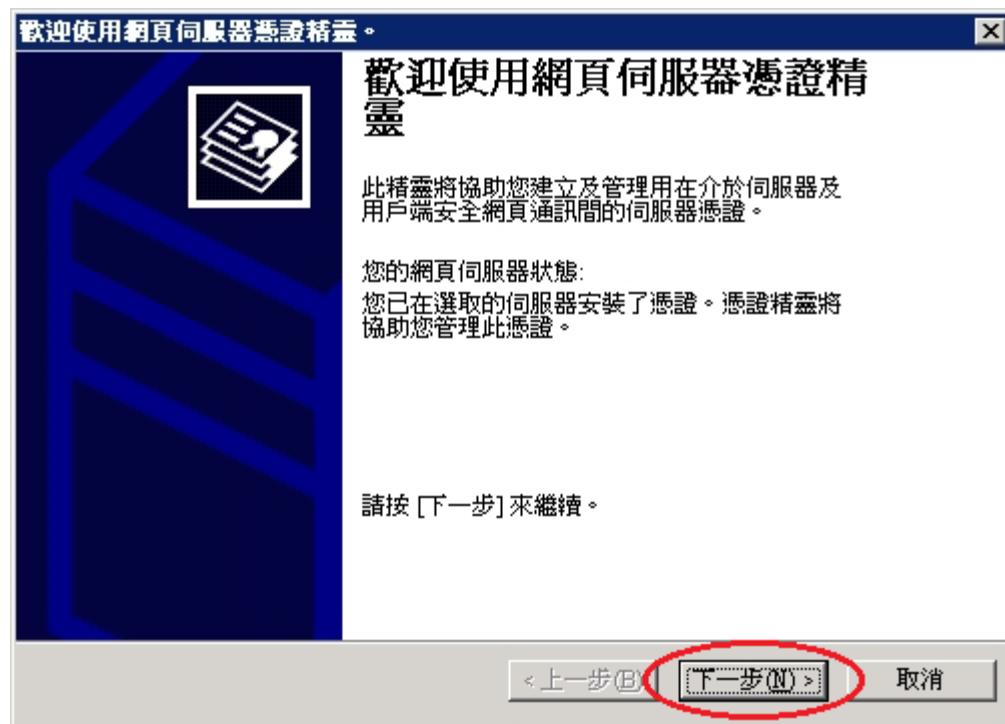
於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。



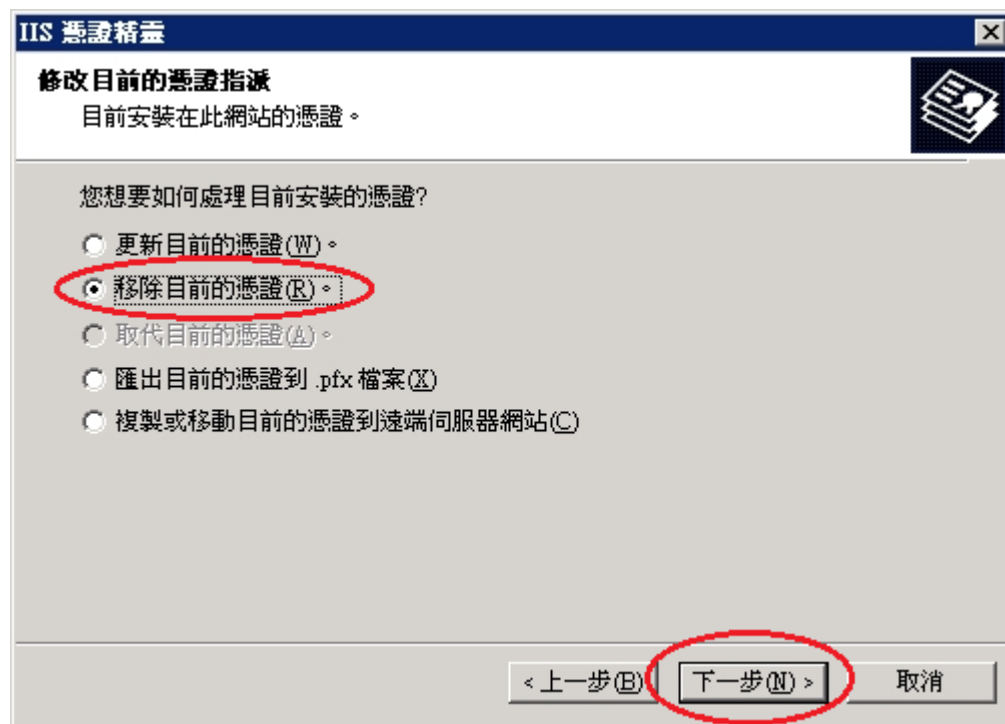
接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面，以滑鼠按下「伺服器憑證」按鈕。



接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗，以滑鼠按下「下一步」按鈕，開始安裝 Windows 2003 IIS 6.0 伺服器憑證。

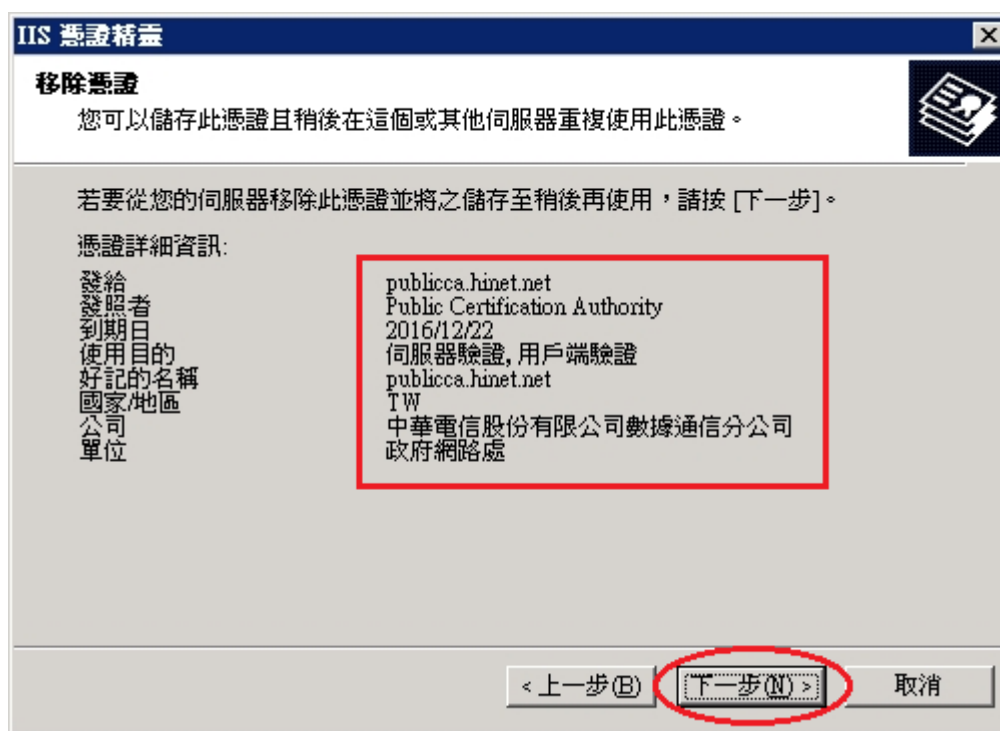


接著出現「修改目前的憑證指派」頁面，選擇「移除目前的憑證」，接著按下「下一步」。

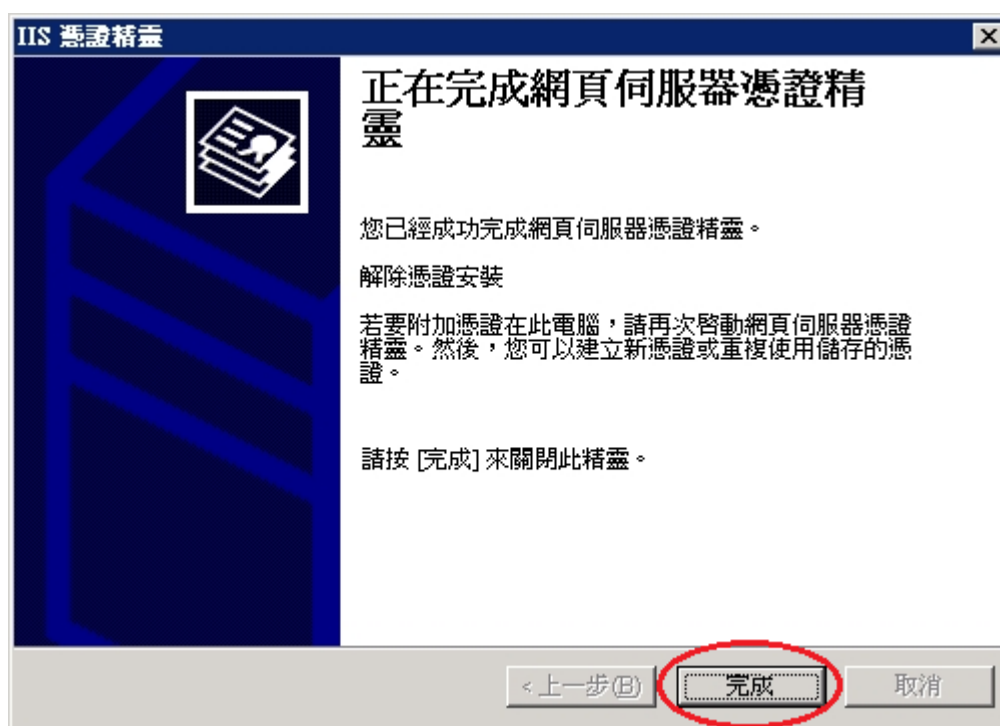


接著出現「移除憑證」頁面，頁面上會顯示目前憑證的詳細資訊，請務必執行之前的私密金鑰及憑證備份後，才可執行此步驟移除憑證，否則憑證一移

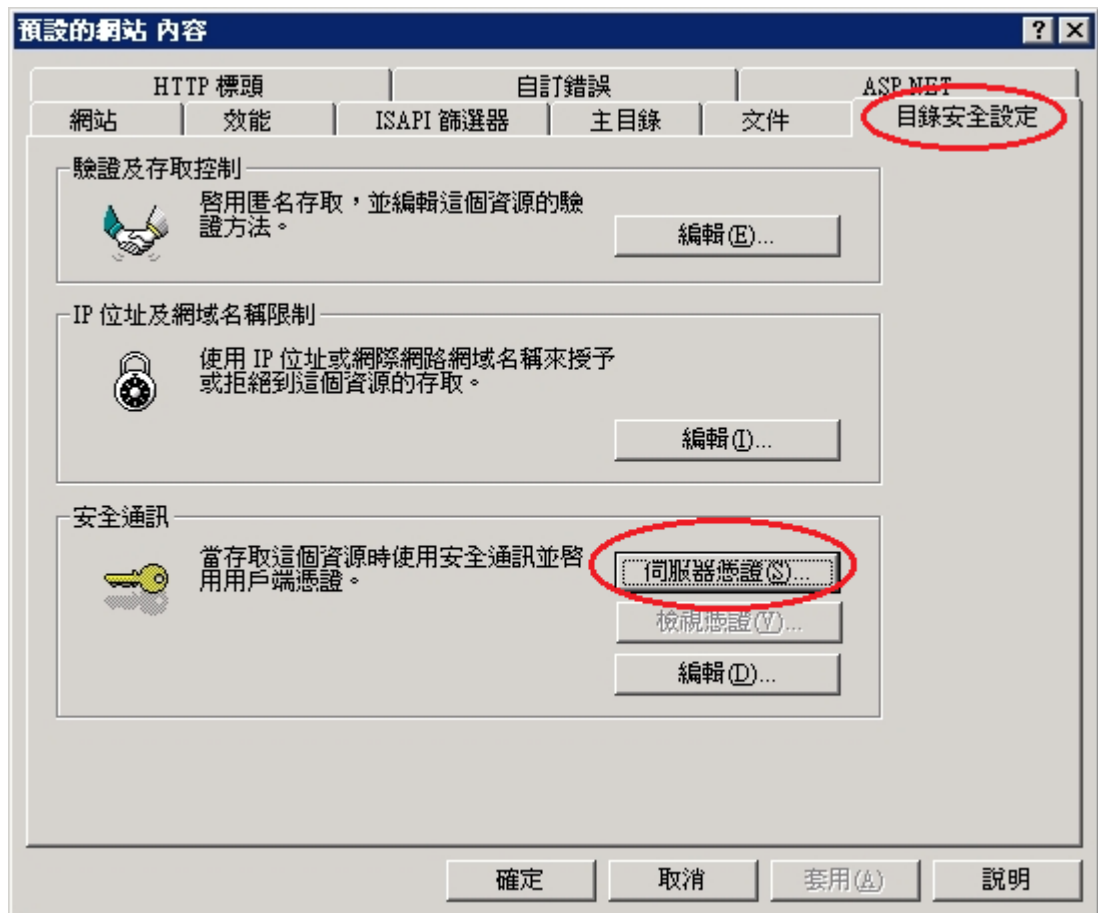
除，將無法救回，接著按下「下一步」。



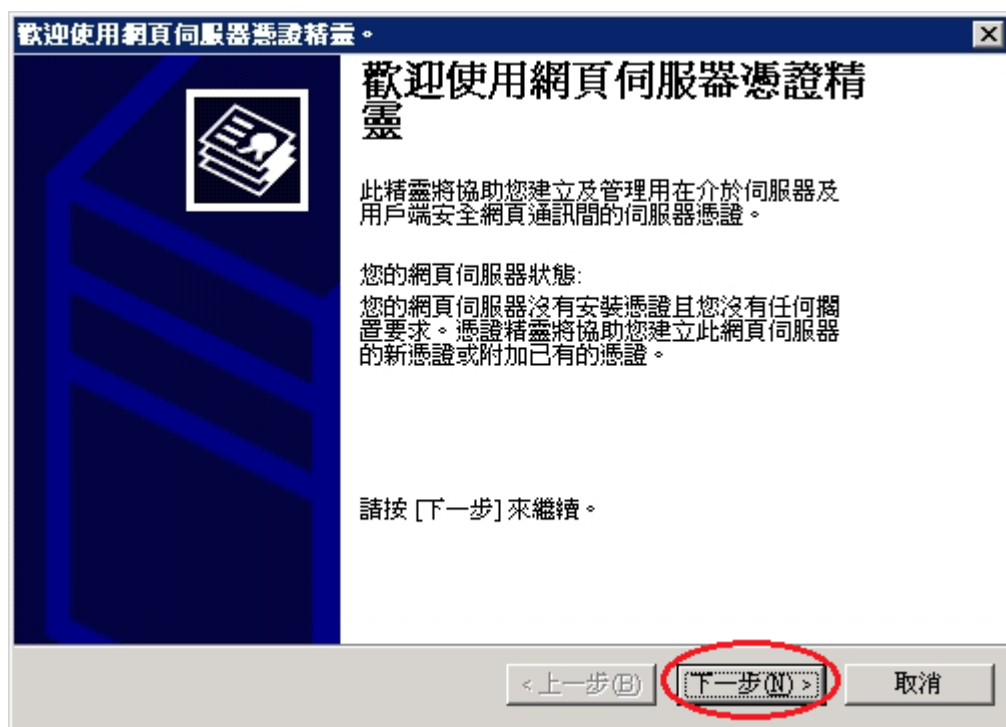
接著出現「正在完成網頁伺服器憑證精靈」頁面，按下「完成」以完成刪除憑證動作。



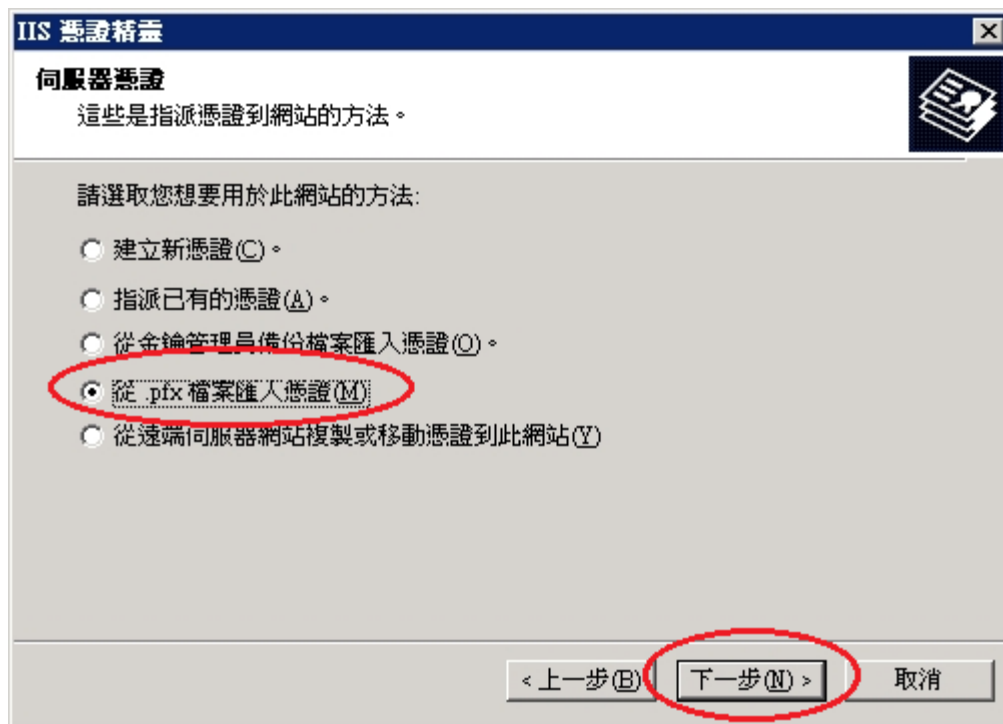
回到「預設的網站」「內容」畫面，接著再按下「伺服器憑證」按鈕。



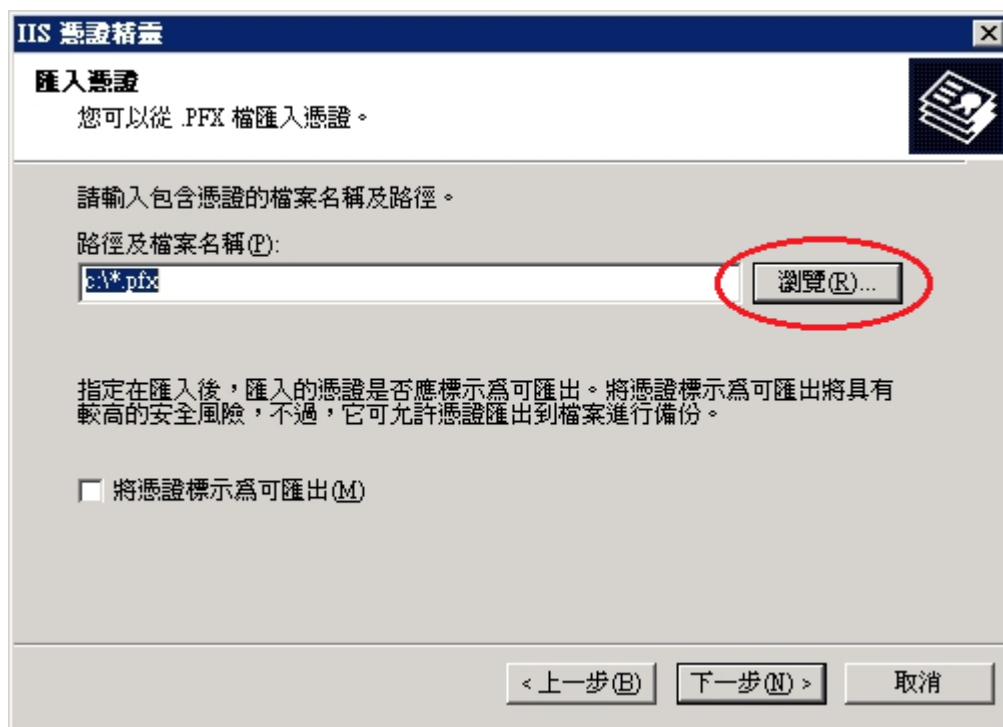
再次開啟「歡迎使用網頁伺服器憑證精靈」視窗畫面，以滑鼠按下「下一步」按鈕，開始匯入「產製請求檔匯出的金鑰及憑證所取出金鑰與新核發的憑證結合的.pfx 檔」。



接著畫面會到「伺服器憑證」視窗，以滑鼠點選「從 .pfx 檔案匯入憑證(M)」，接著以滑鼠按下「下一步」按鈕。

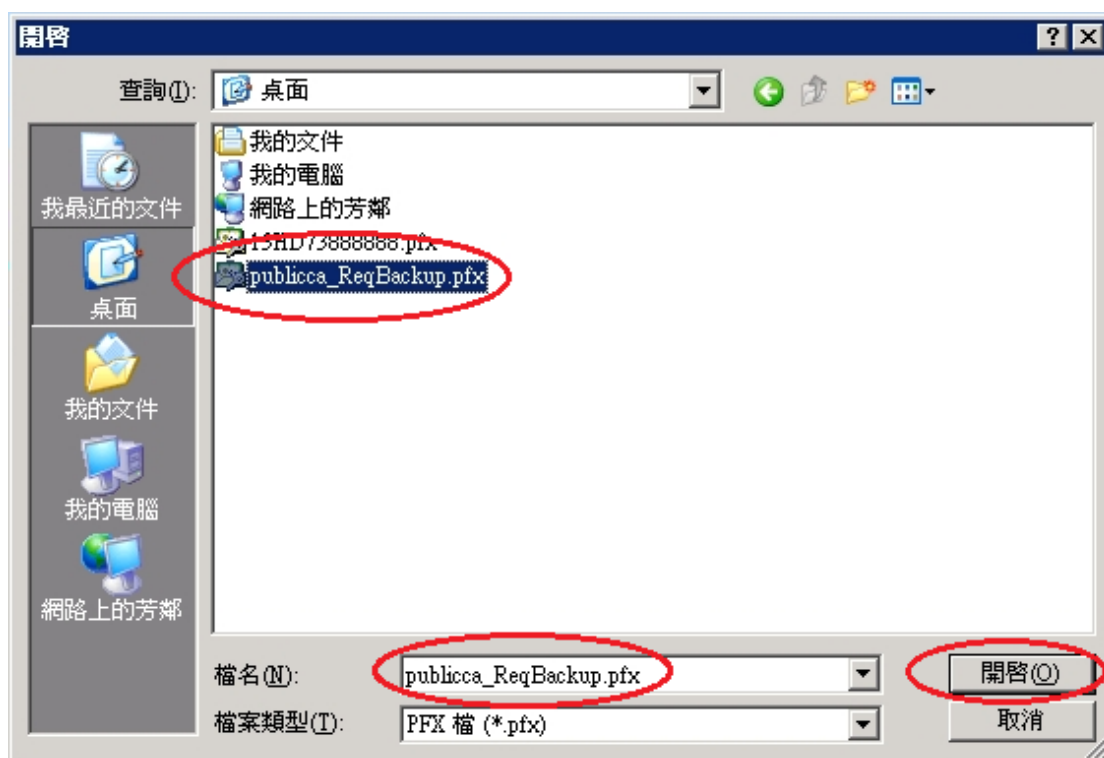


接著出現「匯入檔案」頁面，點選「瀏覽」選擇存放位置，或直接在檔案名稱打上路徑及檔案名稱也可以。

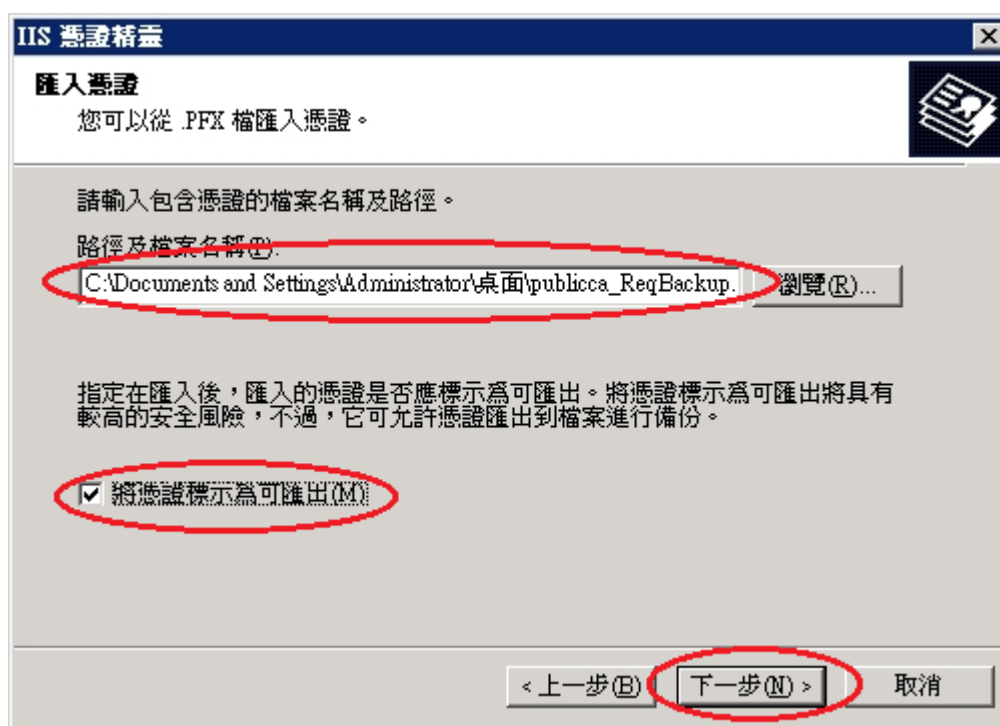


按下「瀏覽」，則可選擇檔案路徑及選擇私密金鑰與憑證.pfx 檔檔名。選擇完成後，按下「開啟」後，接著會跳回「匯入憑證」頁面，並於頁面上出

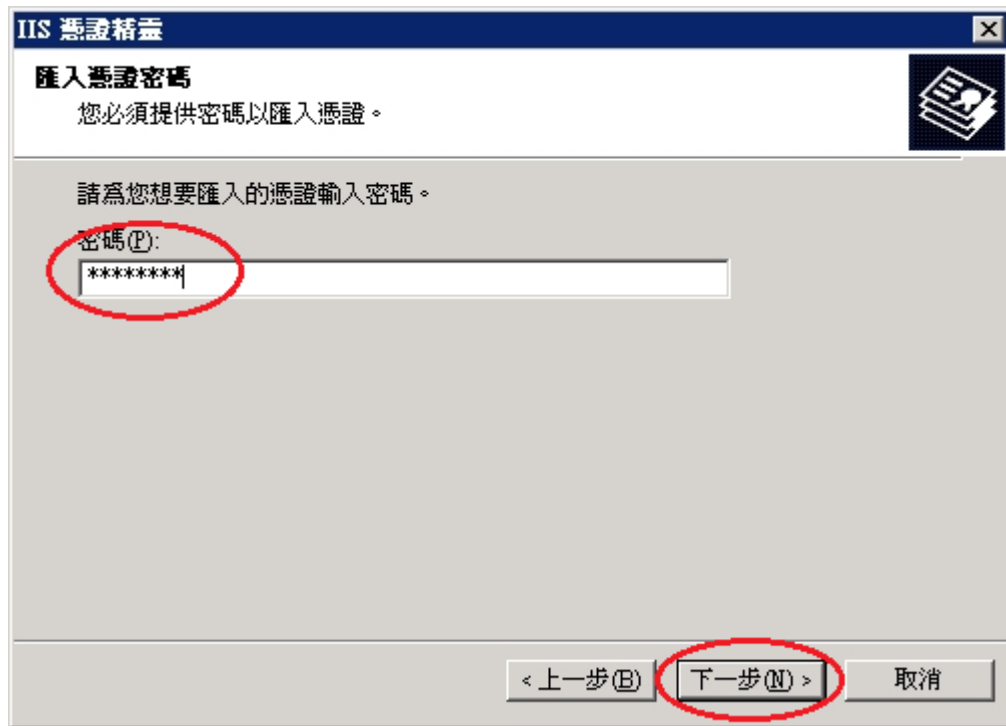
現私密金鑰及憑證.pfx 檔檔案路徑及檔案名稱。



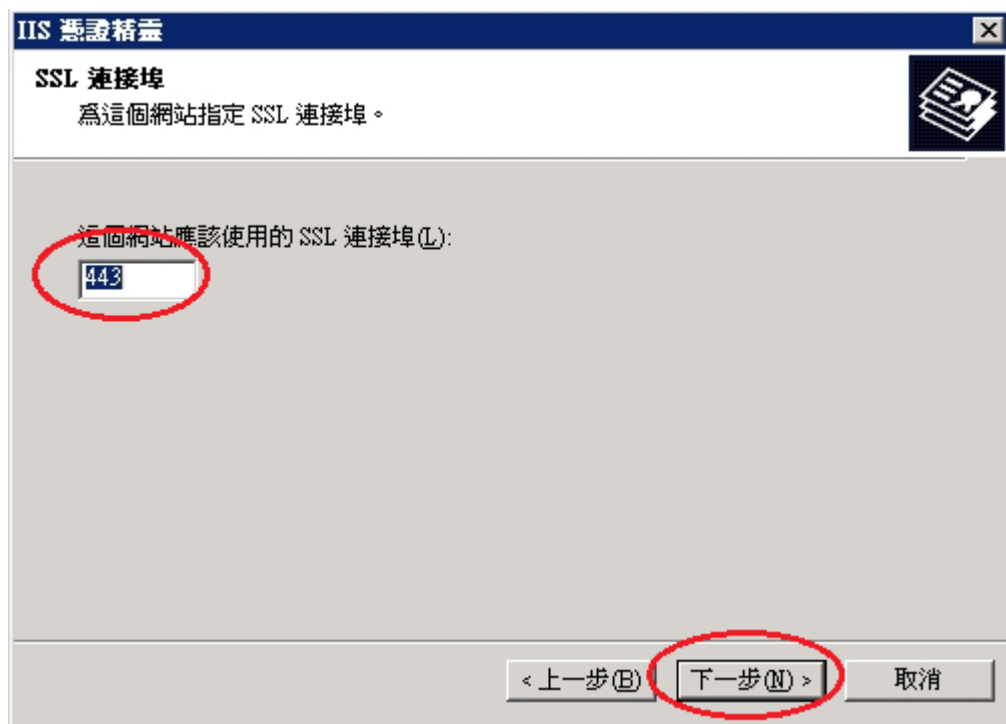
輸入完成後，並勾選「將憑證標示為可匯出(M)」，接著以滑鼠按下「下一步」按鈕。



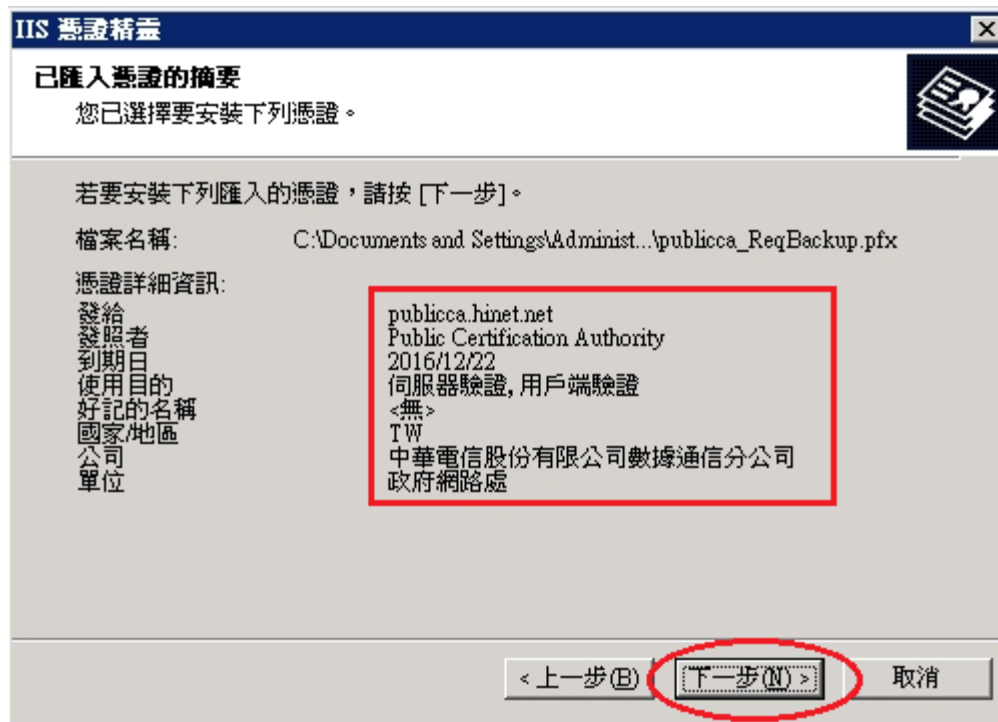
接著出現「匯入憑證密碼」頁面，輸入保護私密金鑰的密碼。



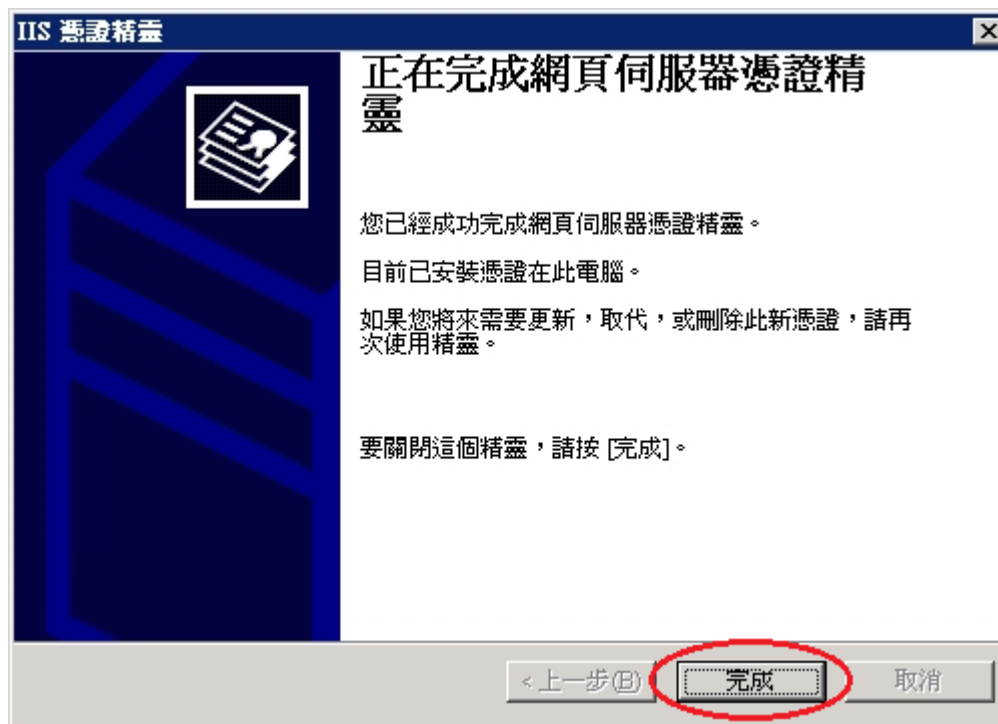
接著出現「SSL 連接埠」頁面，並設定「這個網站應該使用的 SSL 連接埠(L)」，請依網站需求自行設定，接著以滑鼠按下「下一步」按鈕。



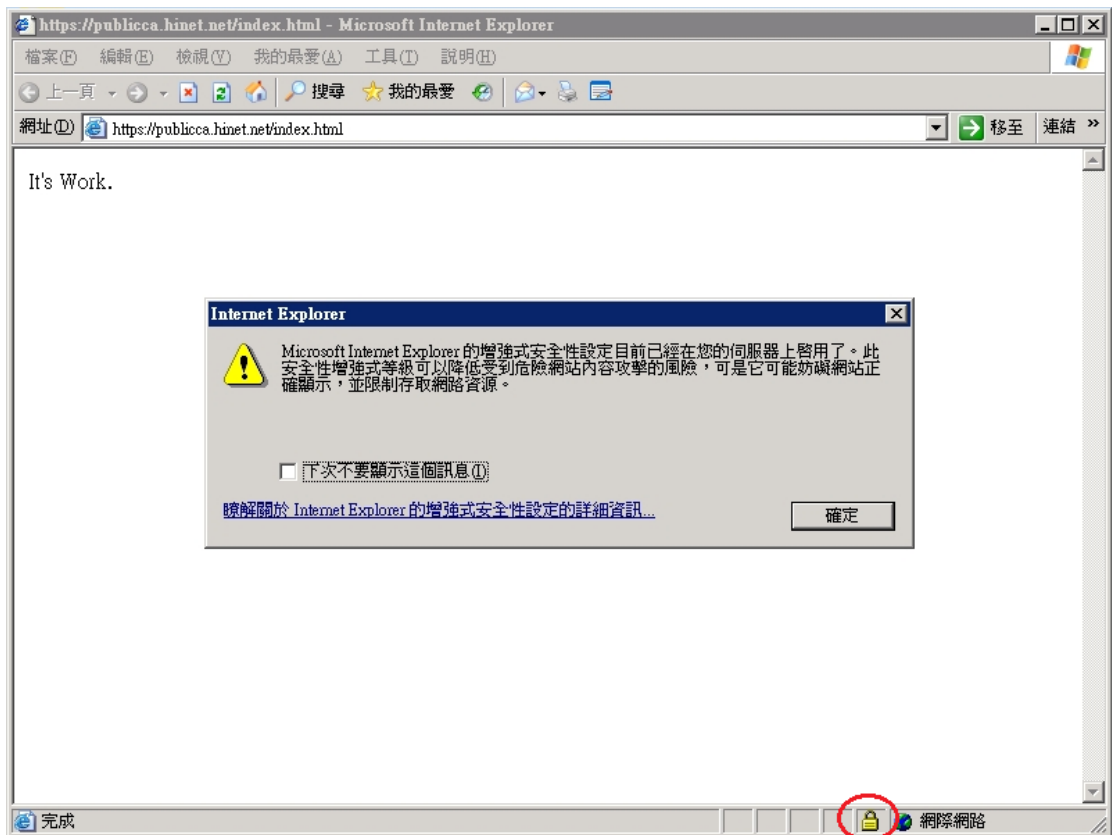
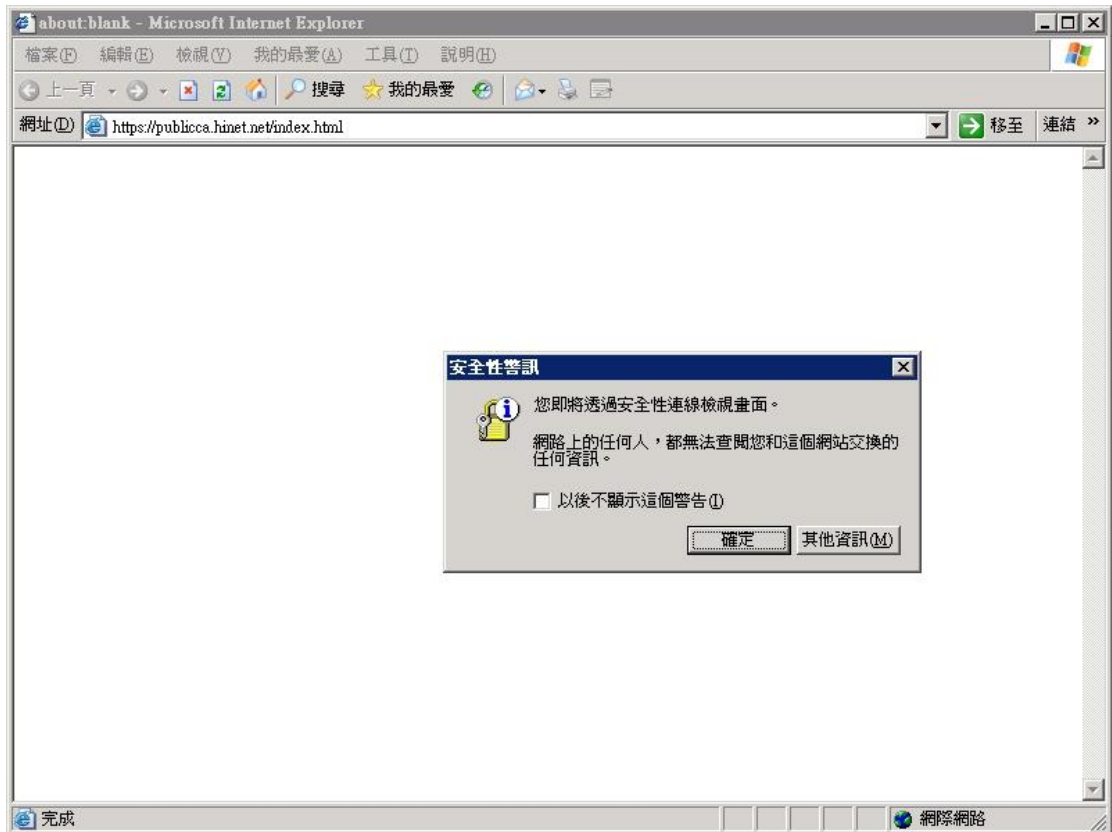
接著出現「已匯入憑證的摘要」頁面，確認憑證內容無誤後，接著以滑鼠按下「下一步」按鈕。



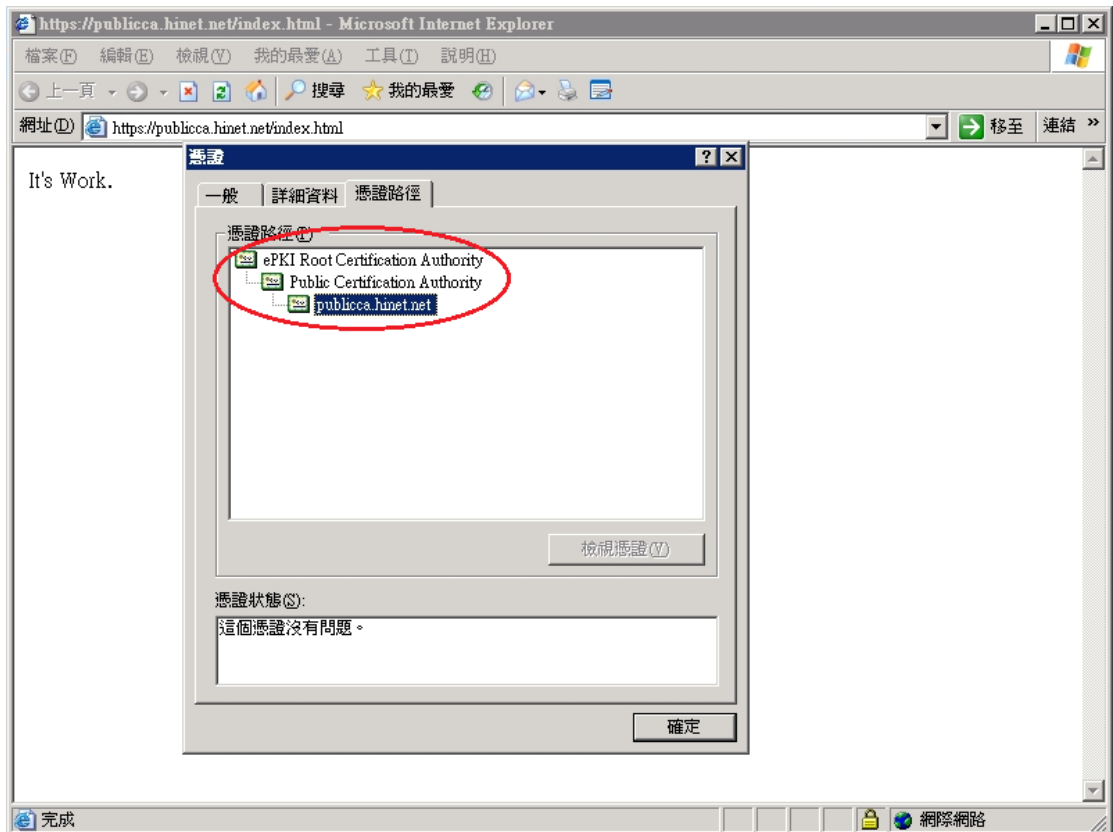
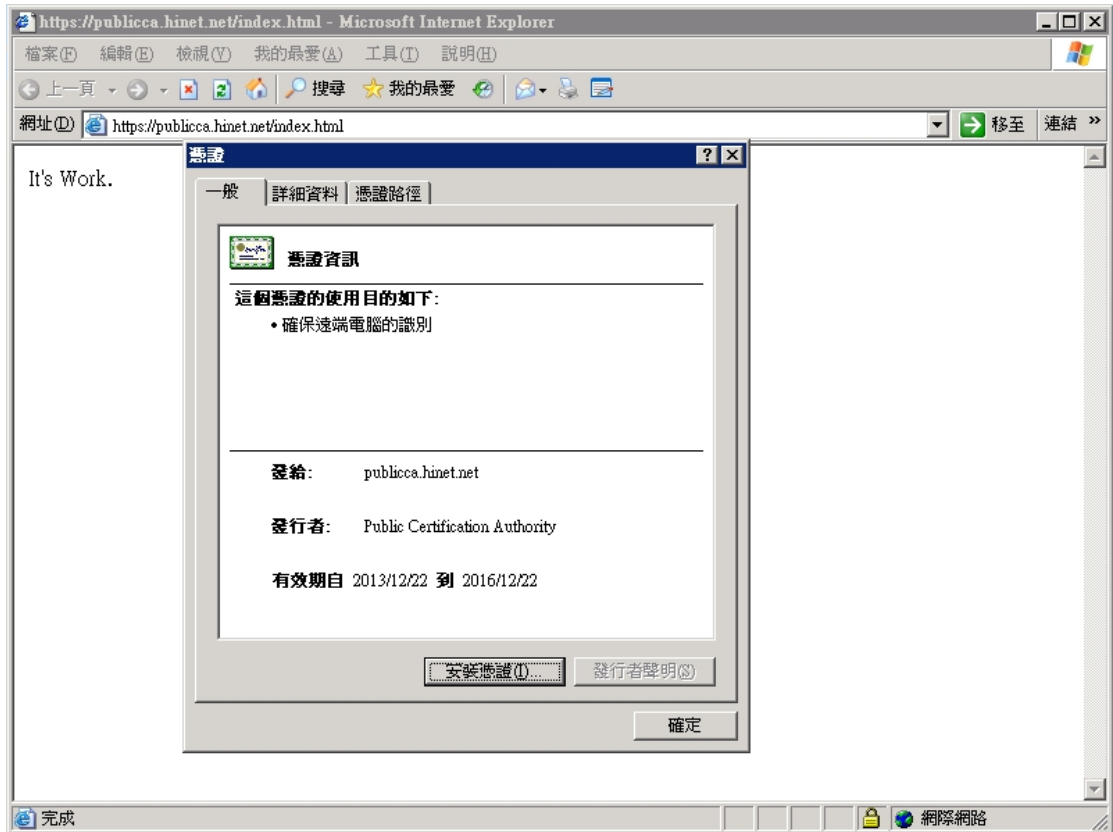
接著畫面會到「正在完成網頁伺服器憑證精靈」視窗，按下「完成」後，即完成匯入私密金鑰及憑證.pfx 檔動作。



透過瀏覽器連線測試網頁 https 是否連線正常。



檢查 SSL 憑證串鏈是否正常。



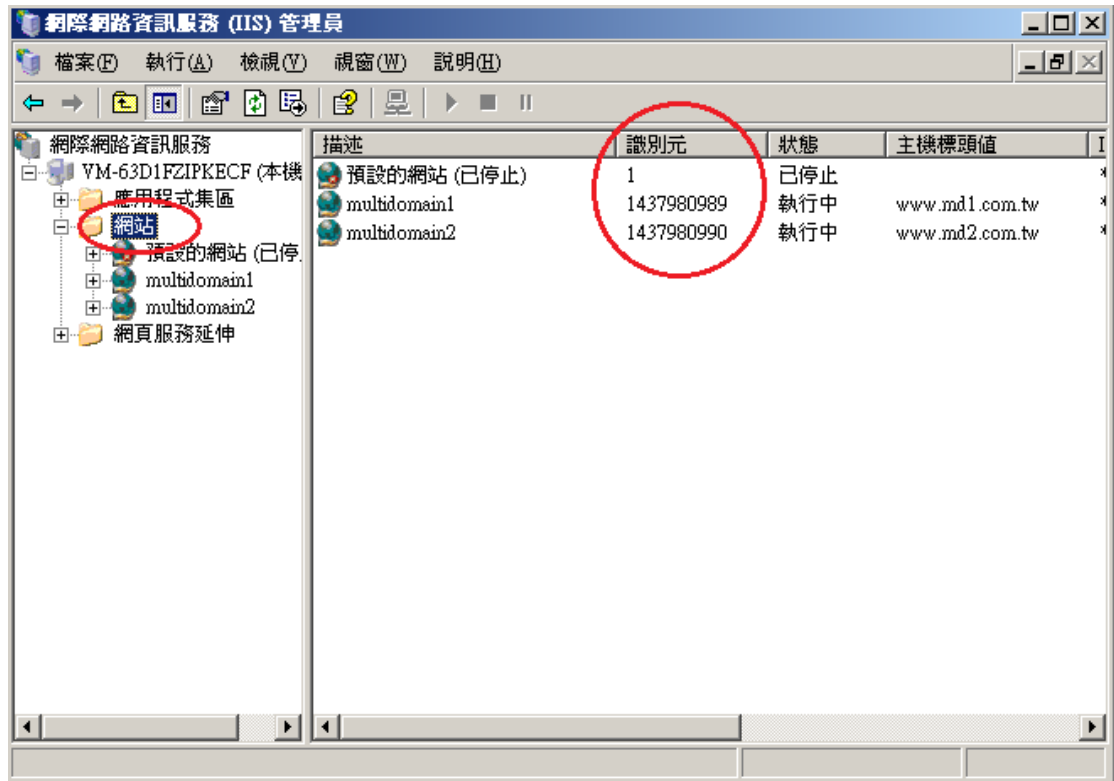
以上動作即完成 Windows 2003 IIS 6.0 重新產製金鑰狀況下，安裝伺服器 SSL 憑證檔動作。

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

附件一：單一 IP 多網域憑證安裝步驟

IIS 6 在只有一個 IP 的情況下，預設只能有一個網站使用 443 port。依照以下步驟操作，即可在多個網站上安裝多網域憑證。

- 一、先在第一個站台安裝好憑證，範例使用站台為 multidomain1
- 二、開啟 IIS 管理員，確認站台識別元。



- 三、開啟命令提示字元

切換至 `cd C:\Inetpub\AdminScripts` 目錄

執行：

`cscript adsutil.vbs set /w3svc/ 站台識別元/SecureBindings ":443: 站台 1FQND"`

```
命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd ..

C:\Documents and Settings>cd ..

C:\>cd Inetpub

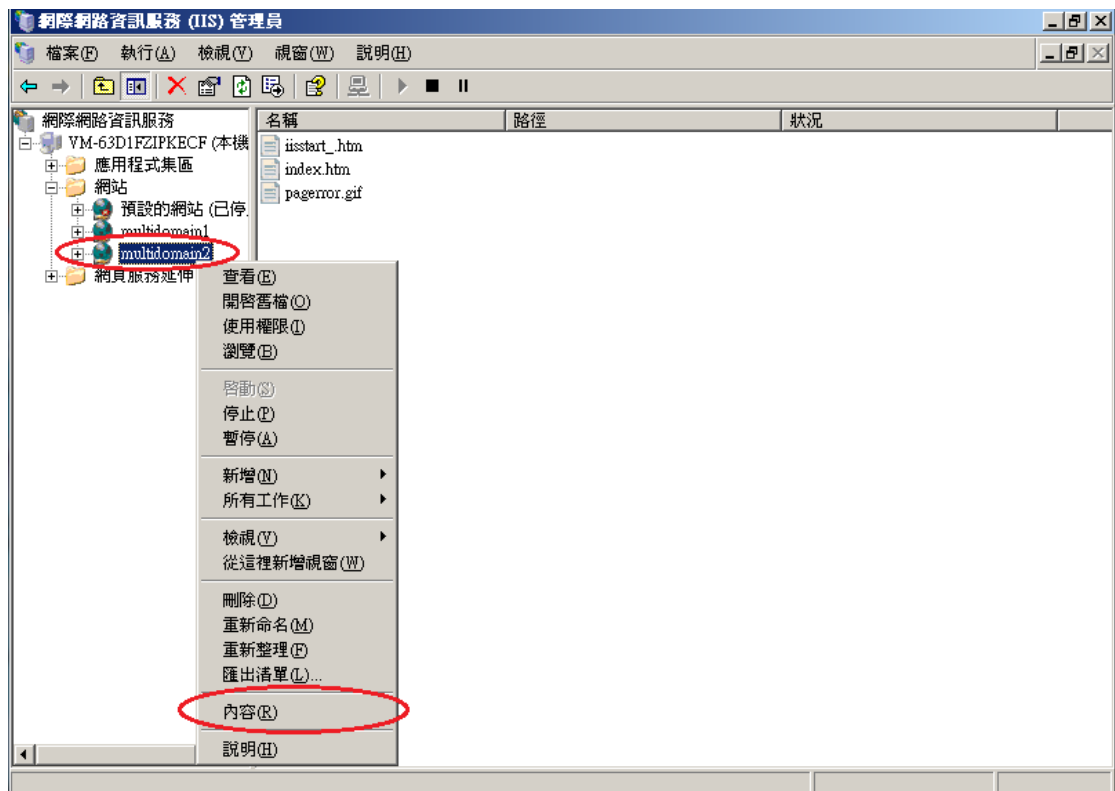
C:\Inetpub>cd AdminScripts

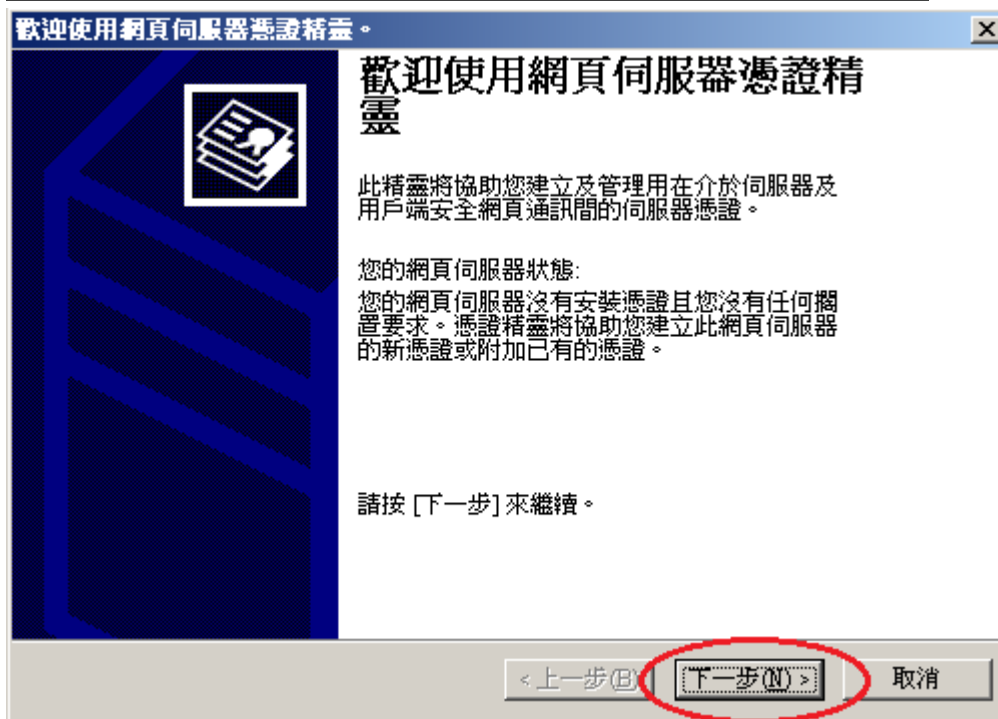
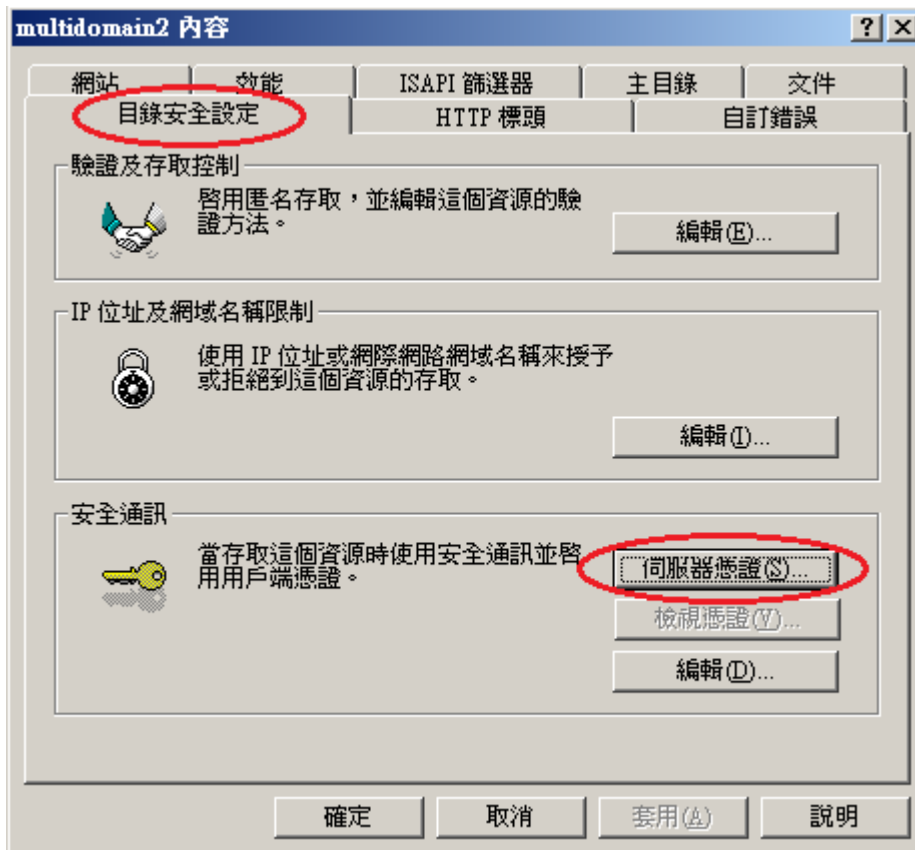
C:\Inetpub\AdminScripts>cscript adsutil.vbs set /w3svc/1437980989/SecureBindings
":443:www.md1.com.tw"
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

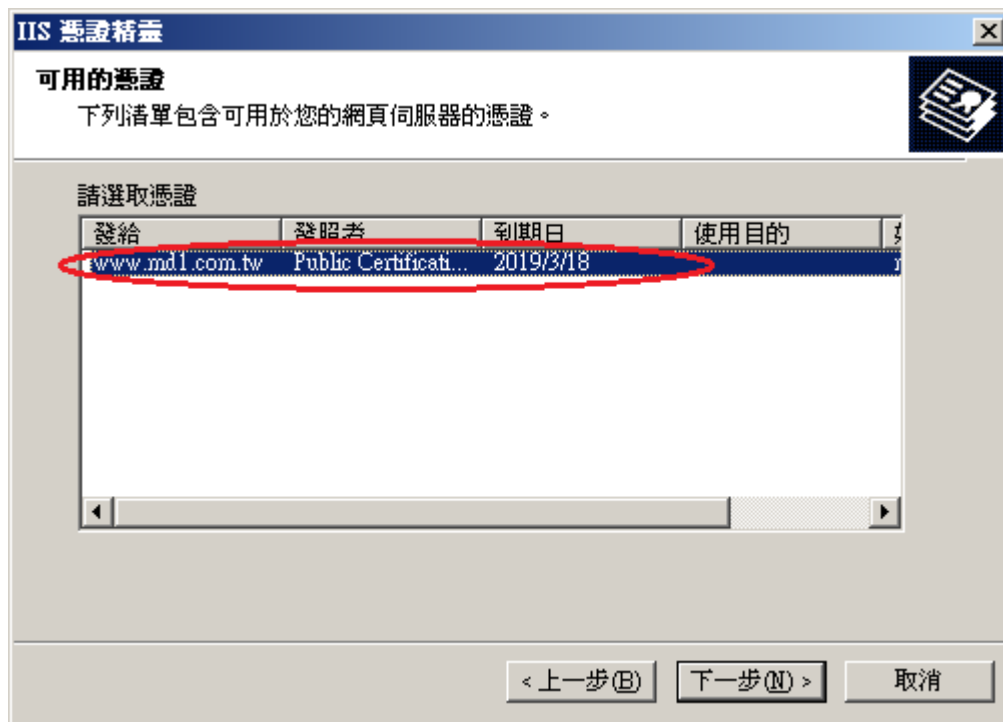
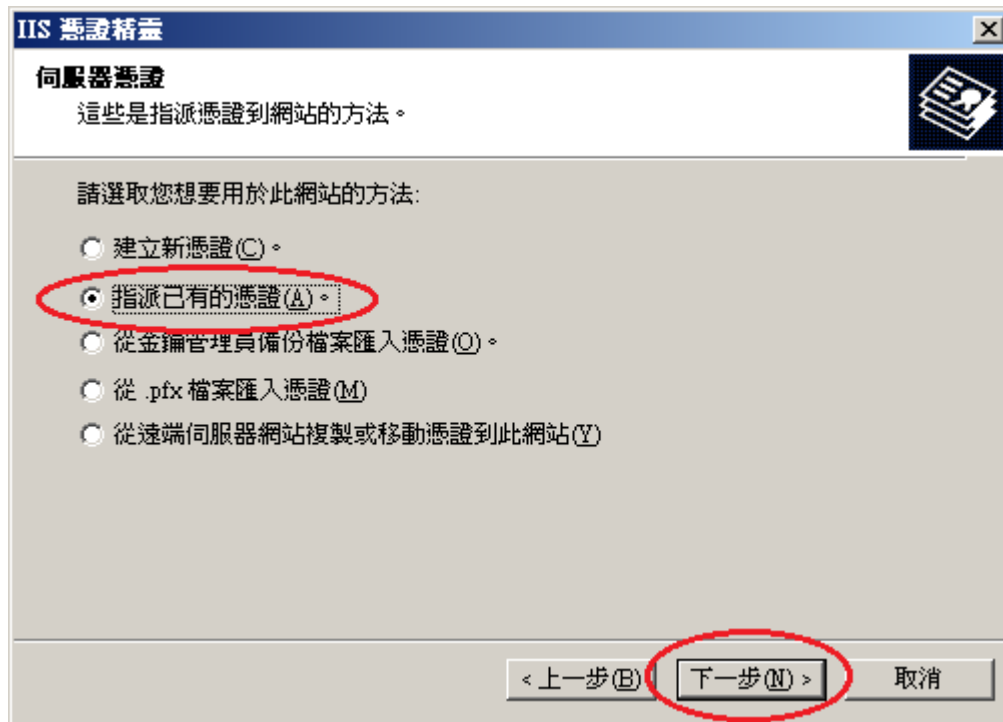
SecureBindings           : (LIST) ":443:www.md1.com.tw"

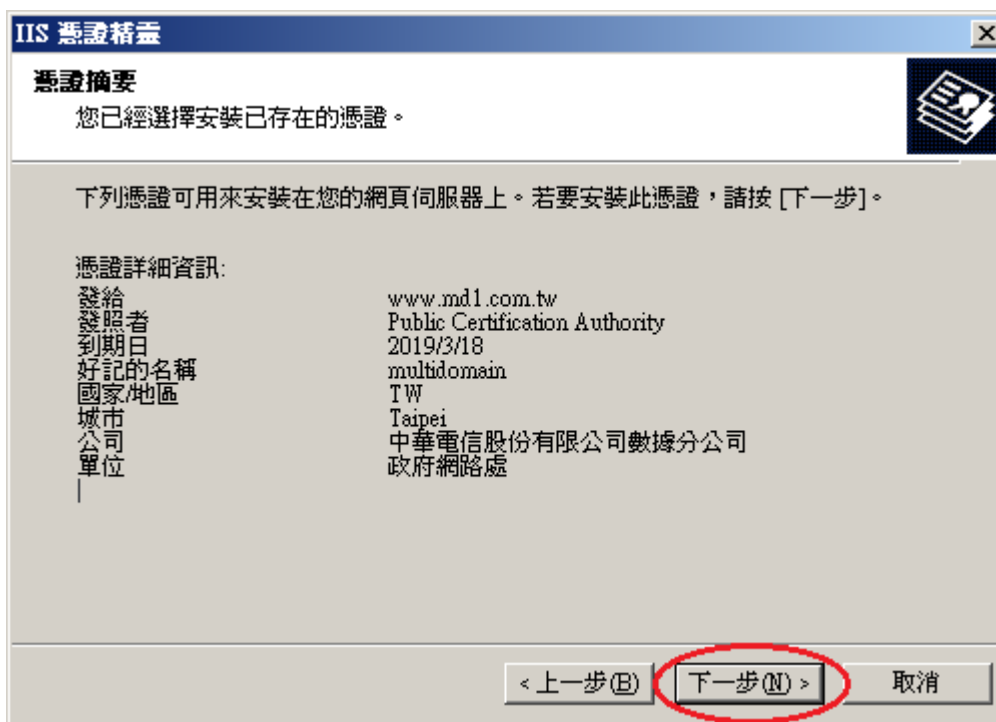
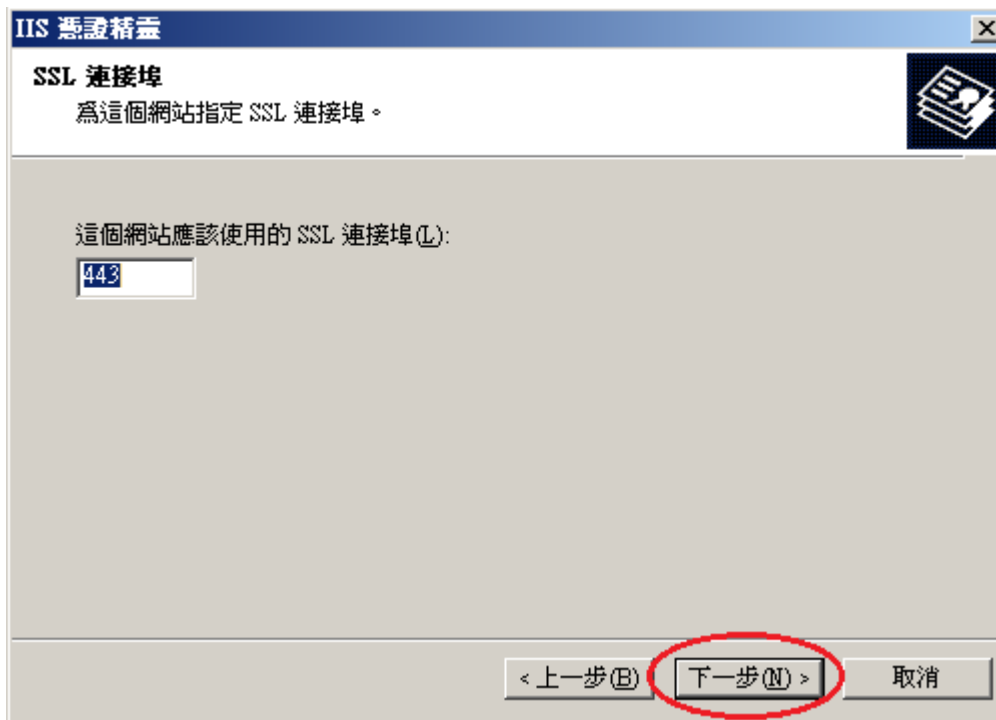
C:\Inetpub\AdminScripts>
```

四、於第 2 個站台安裝多網域憑證。











五、執行 SecureBindings 指令

cscript adsutil.vbs set /w3svc/站台識別元/SecureBindings ":443:站台 2FQND"

```

命令提示字元
(C) 版權所有 1985-2003 Microsoft Corp.
C:\Documents and Settings\Administrator>cd ..
C:\Documents and Settings>cd ..
C:\>cd Inetpub
C:\Inetpub>cd AdminScripts
C:\Inetpub\AdminScripts>cscript adsutil.vbs set /w3svc/1437980989/SecureBindings
":443:www.md1.com.tw"
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

SecureBindings          : <LIST> ":443:www.md1.com.tw"

C:\Inetpub\AdminScripts>cscript adsutil.vbs set /w3svc/1437980990/SecureBindings
":443:www.md2.com.tw"
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

SecureBindings          : <LIST> ":443:www.md2.com.tw"

C:\Inetpub\AdminScripts>

```

六、至此兩個站台已安裝多網域憑證，可使用瀏覽器連線試試。