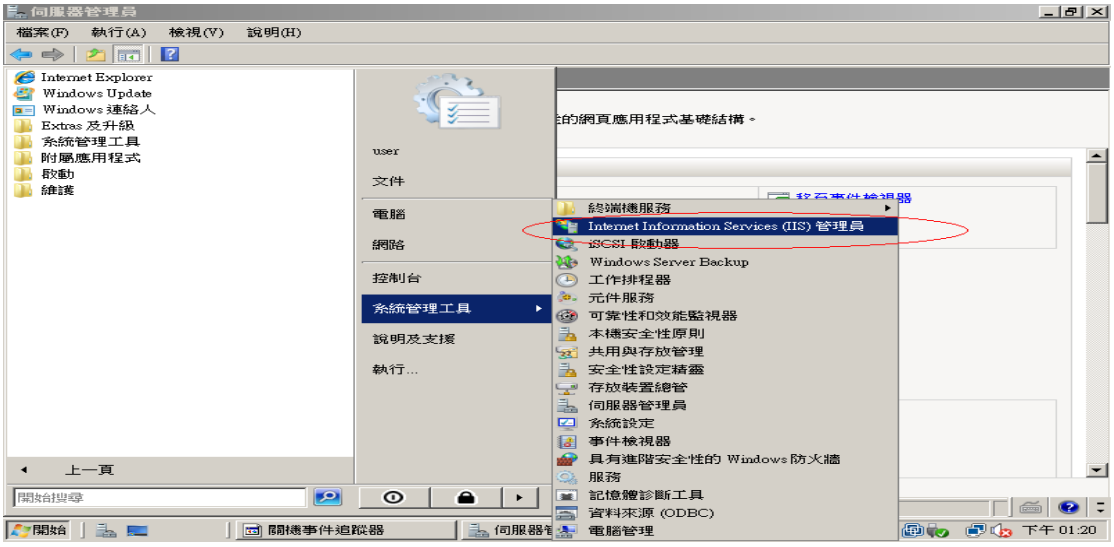
政府伺服器數位憑證管理中心(GTLSCA)

Windows IIS 7.0 SSL 憑證請求檔製作與憑證安裝手冊

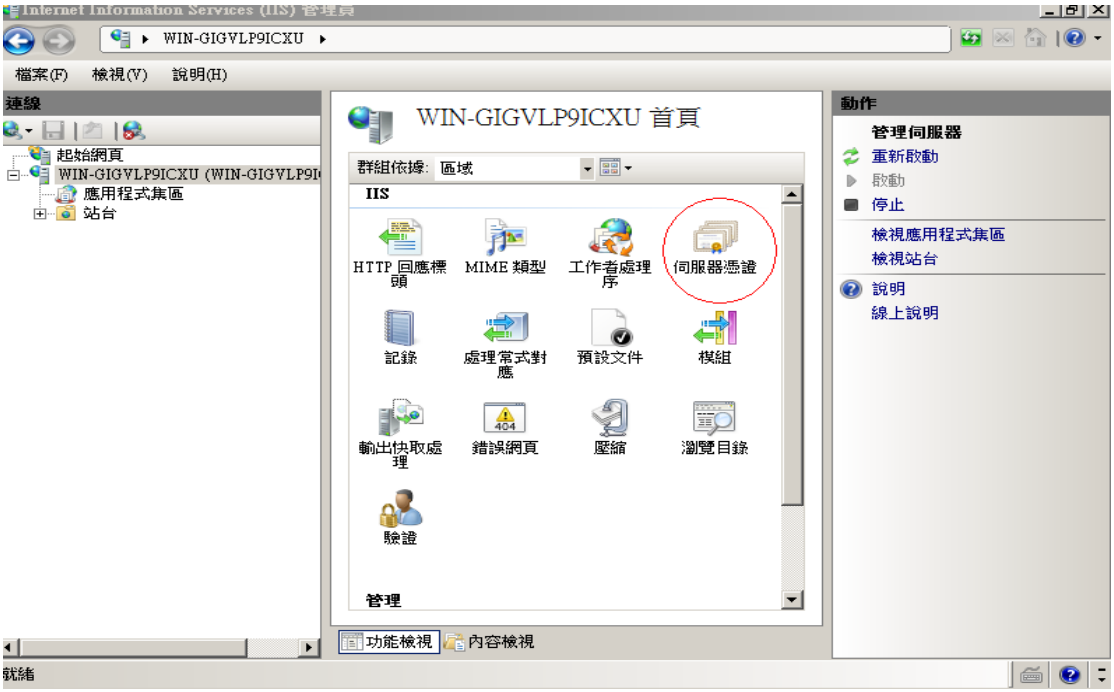
目錄

Windows IIS 7.0 SSL 憑證請求檔製作手冊

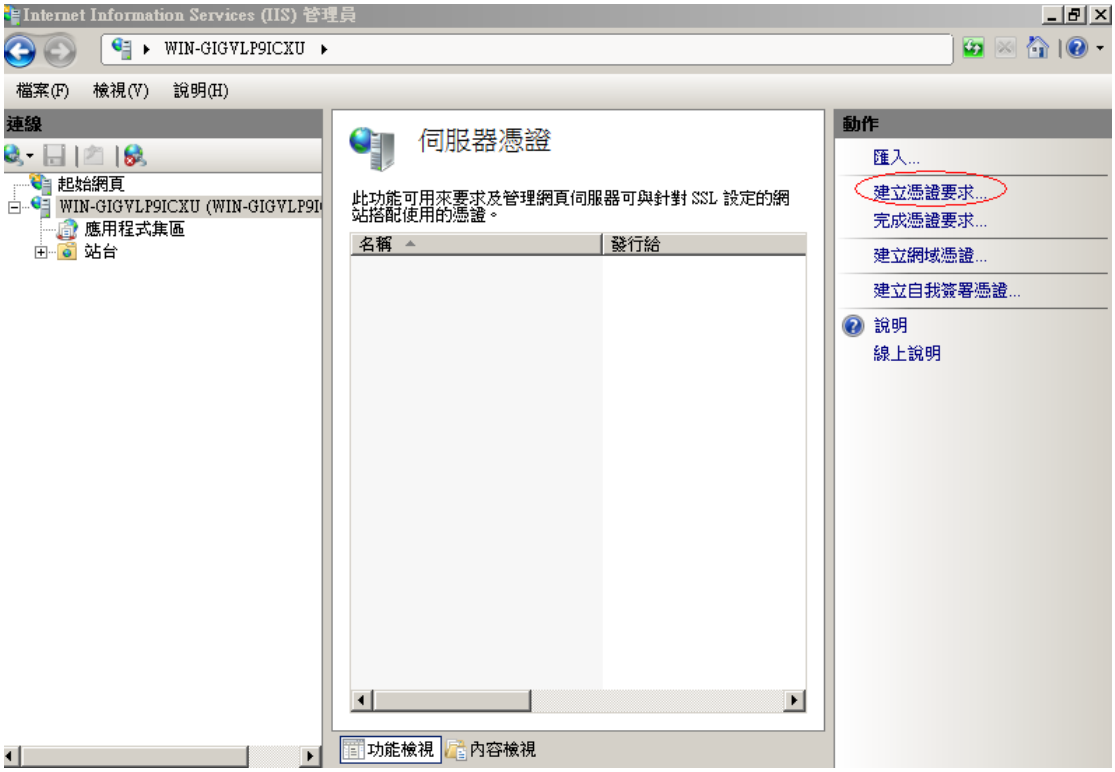
一、點選 「開始」→「系統管理工具」→「Internet Information Services (IIS)管理員」



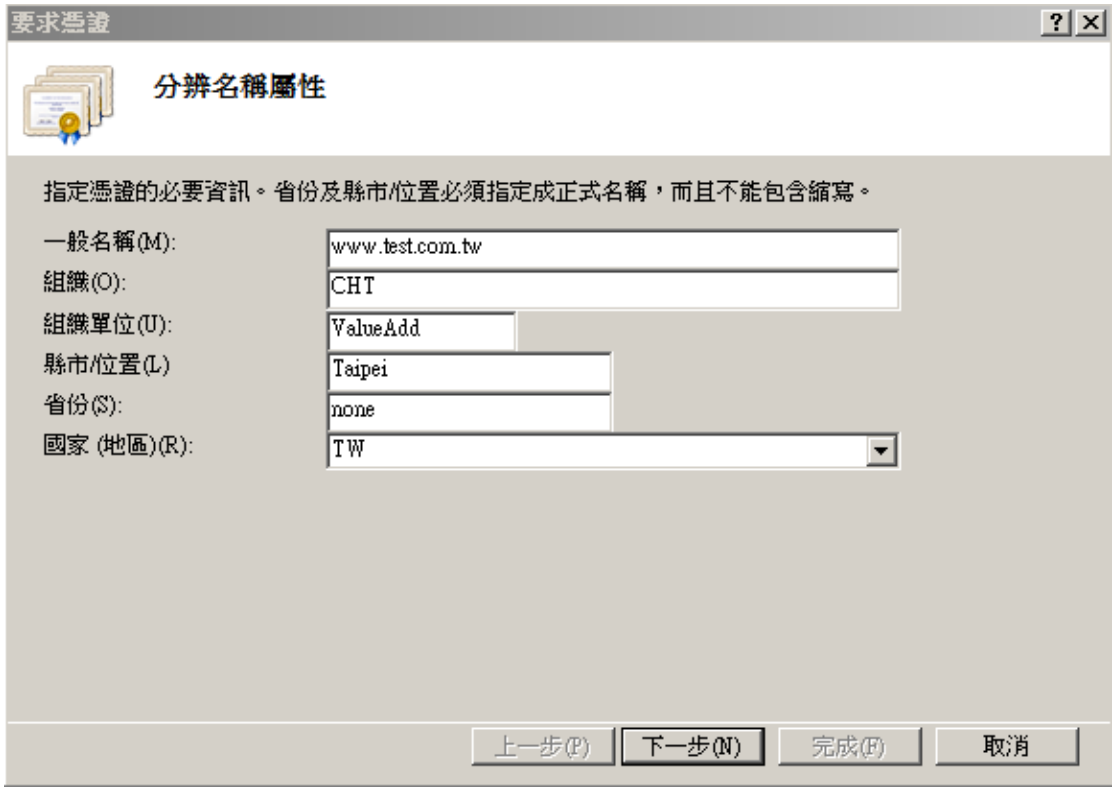
二、點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」



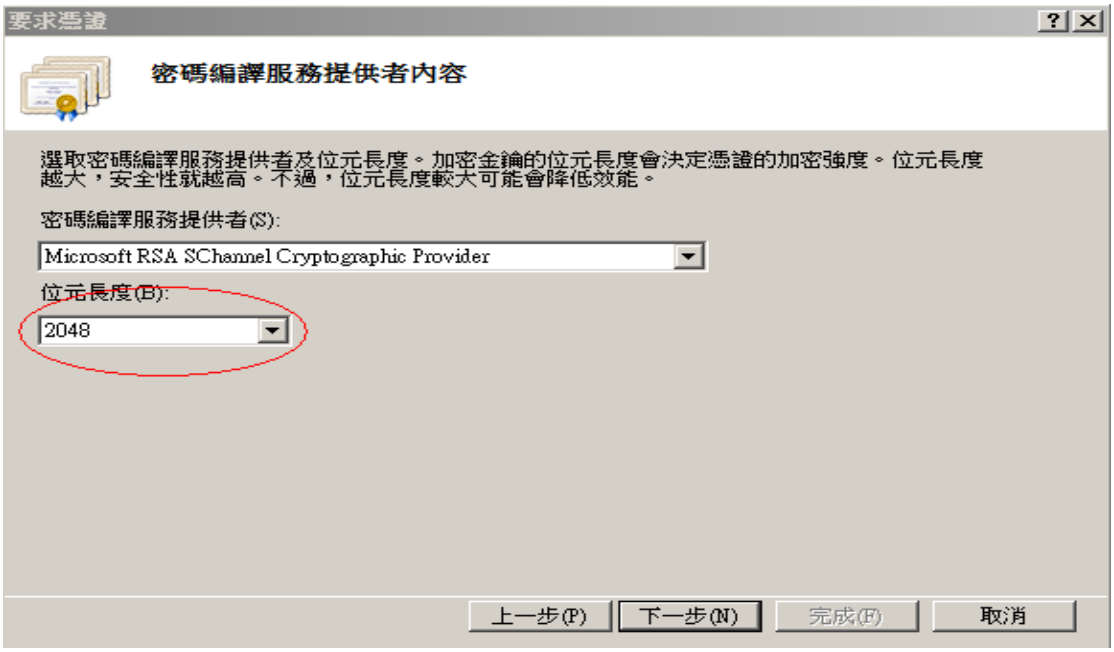
三、點選「建立憑證要求」



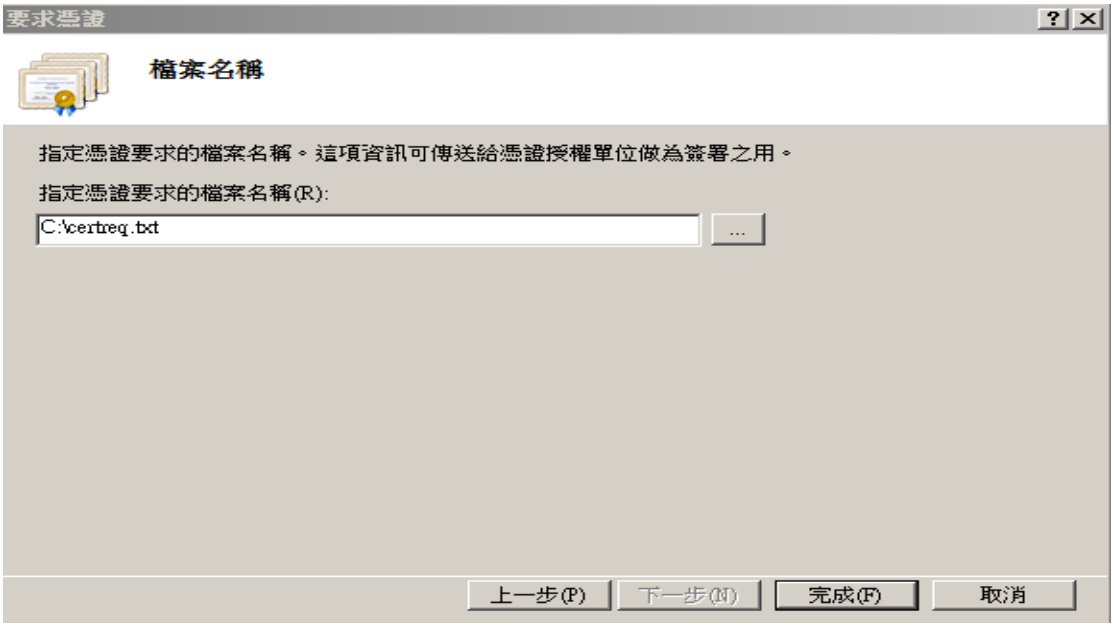
四、輸入以下所有欄位資料，輸入完成後點點選「下一步」，多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主。



五、選擇密碼編譯服務提供者『Microsoft RSA SChannel Cryptographic Provider』，金鑰長度選擇 『2048』位元。



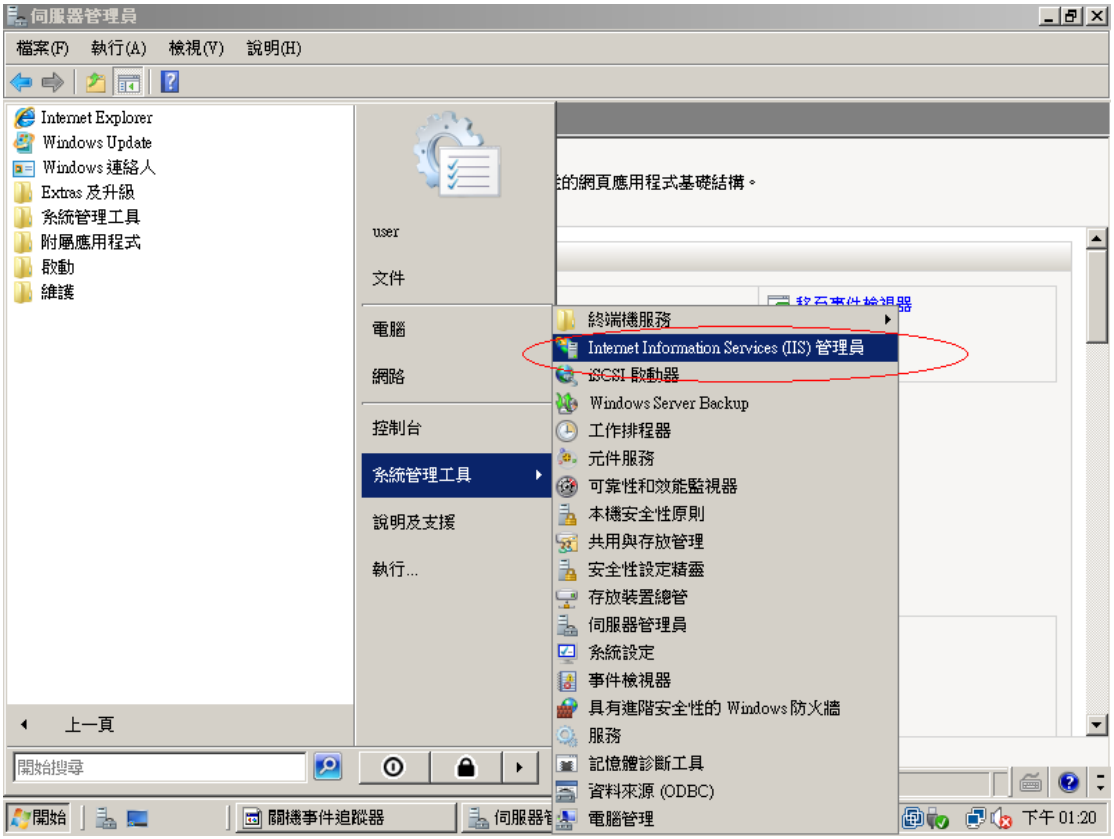
六、指定要儲存憑證請求檔檔案名稱與存放位置，確認後點選「完成」。



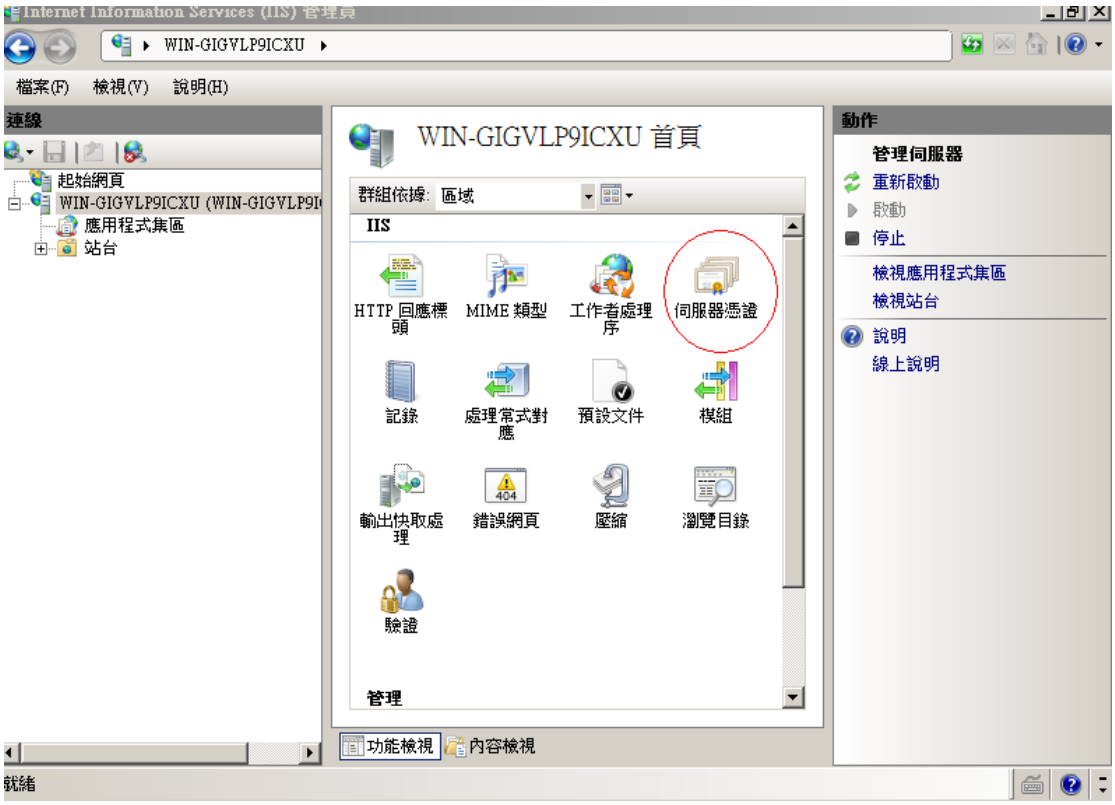
七、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至憑證管理中心網站(https://gca.nat.gov.tw)進行 SSL 憑證申請作業。

Windows IIS 7.0 SSL 憑證安裝操作手冊

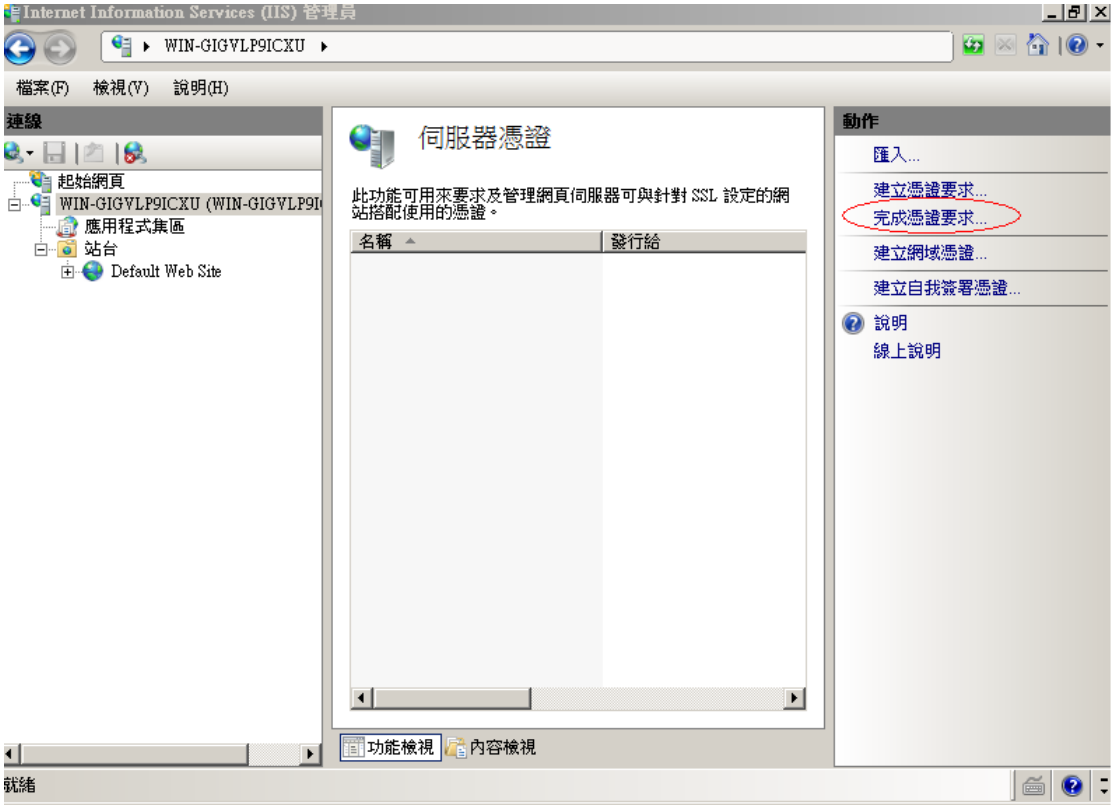
一、點選 「開始」→ 「系統管理工具」→「Internet Information Services (IIS) 管理員」。



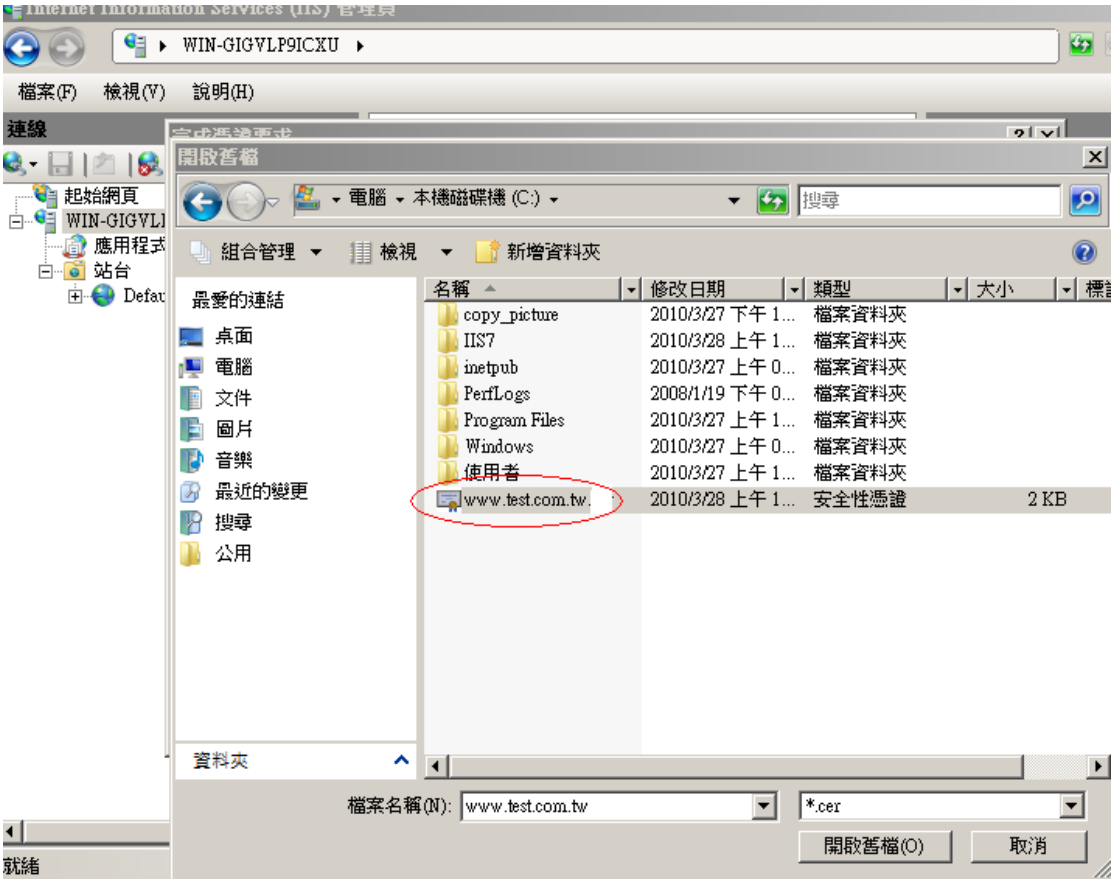
二、點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。

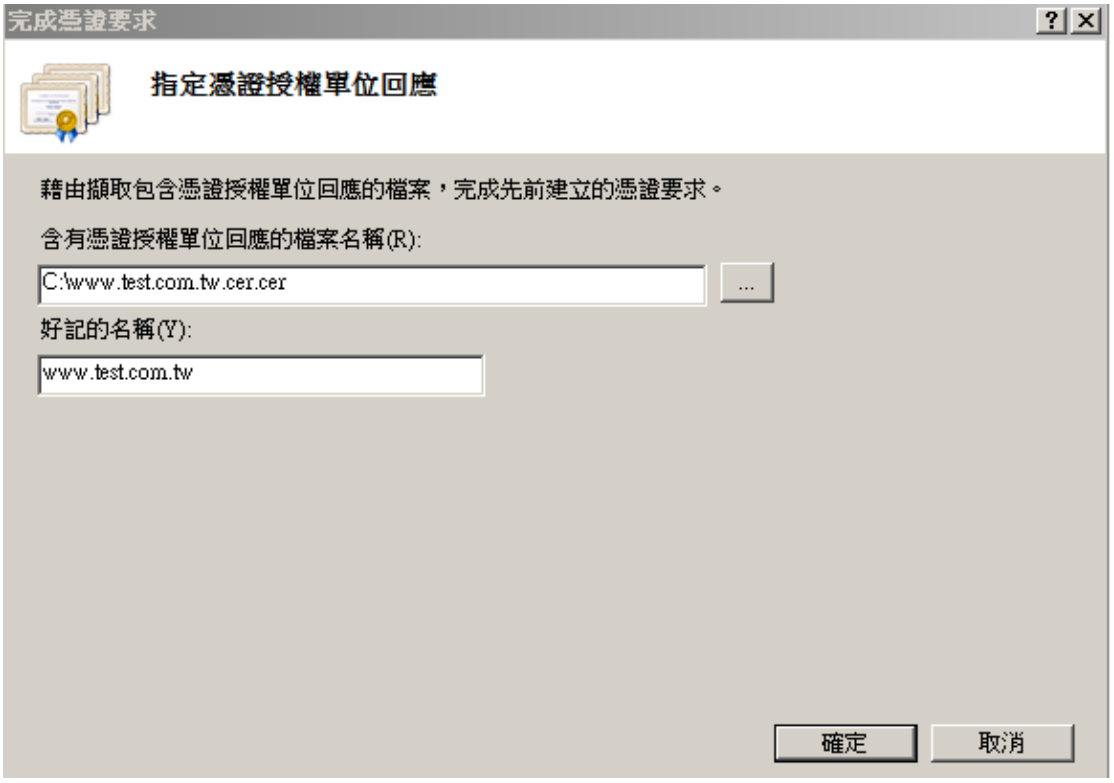


三、點選「完成憑證要求」。

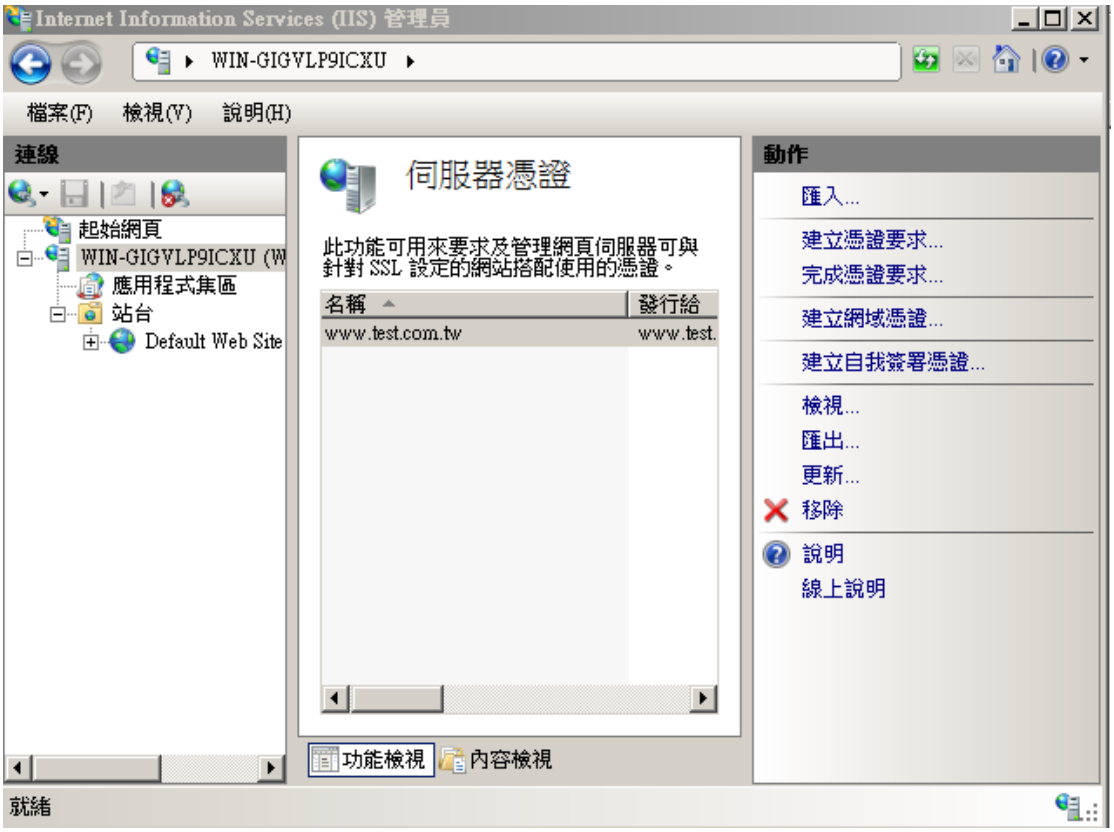


四、選擇至憑證管理中心申請之 SSL 憑證，並輸入好記名稱(一般填寫 Domain Name)。





五、步驟 4 按「確定」，出現完成憑證要求的畫面。



六、至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip

七、將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案。

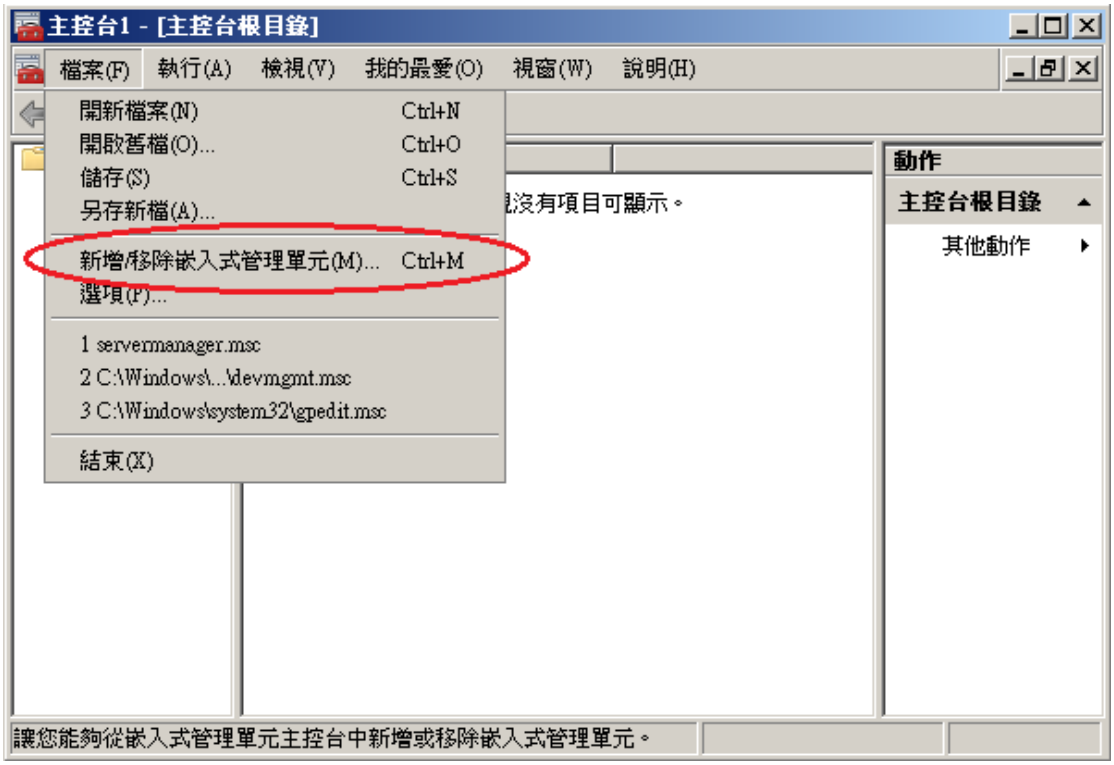
八、接著要安裝 eCA 自發憑證及 GTLSCA 憑證。

請先點選「開始」→輸入「mmc」→按下「Enter」。

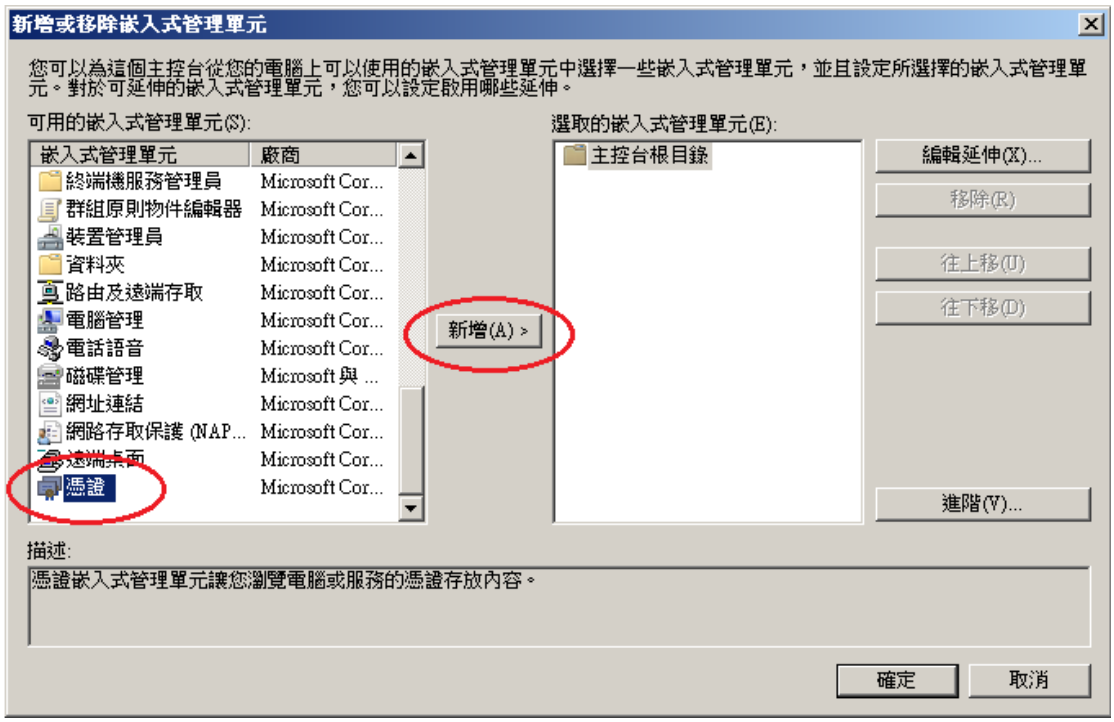

程式集
mmc.exe
檔案
MMC
Administrator
文件
電腦
網路
控制台
系統管理工具
說明及支援
執行...
搜尋每個地方
搜尋網際網路
mmc
開始


主控台1 - [主控台根目錄]
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
名稱
這個檢視沒有項目可顯示。
動作
主控台根目錄
其他動作

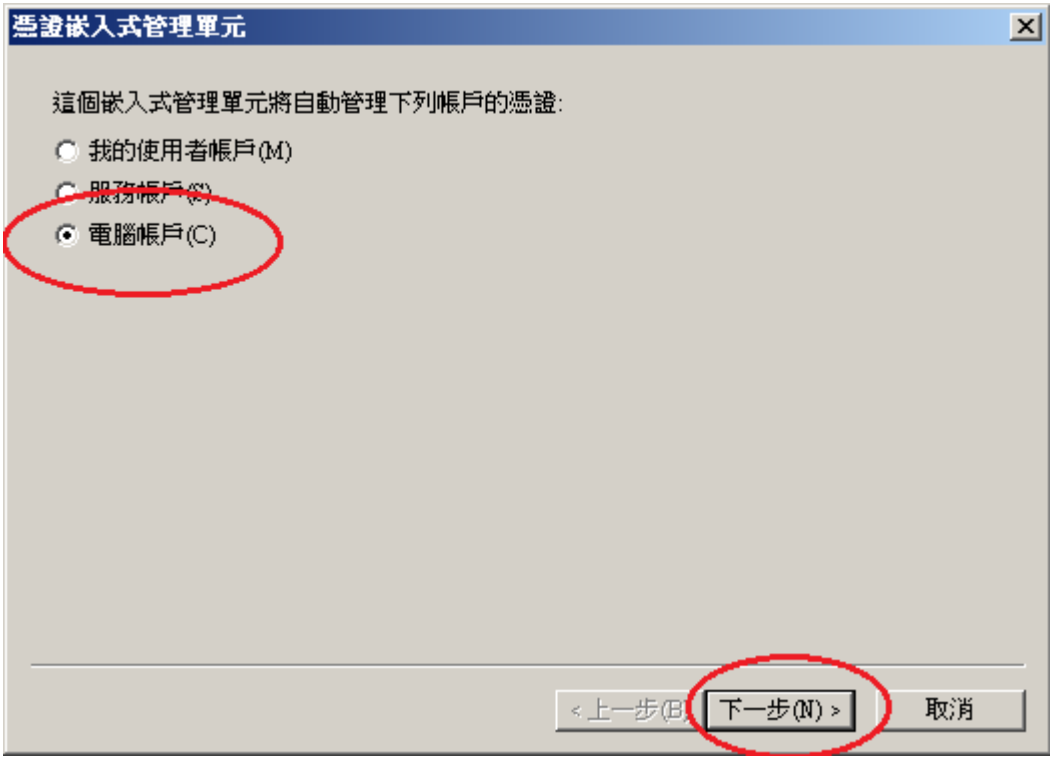
九、選擇「新增/移除嵌入式管理單元」。

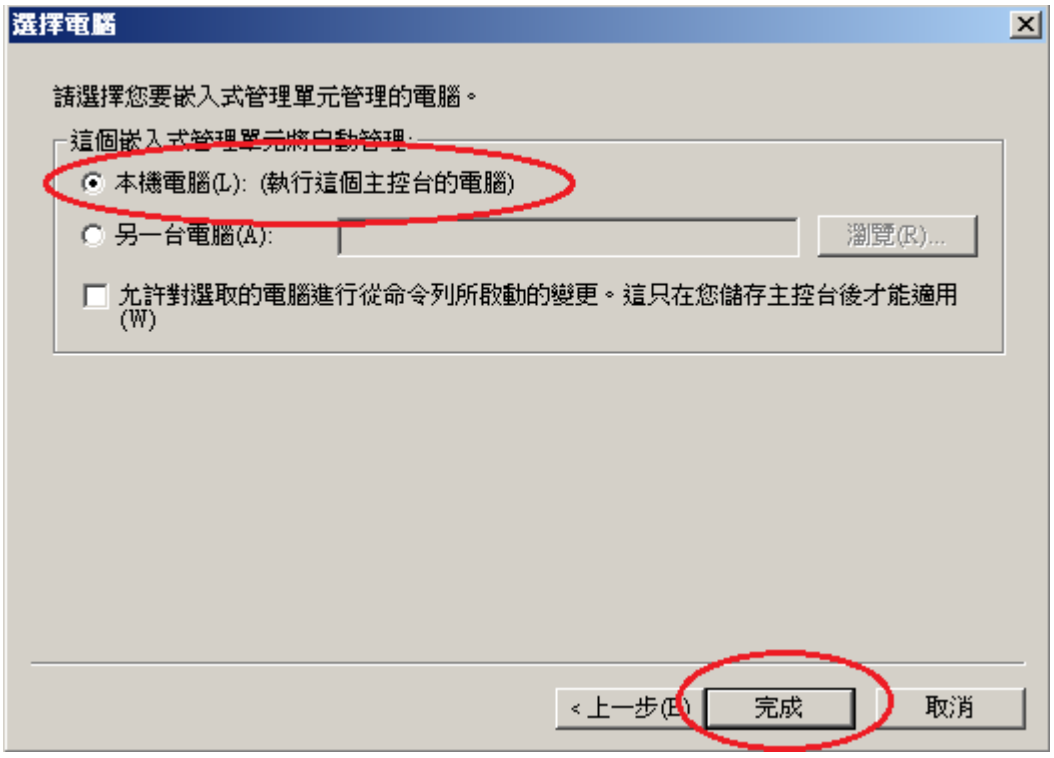


十、接著點選「憑證」→「新增」。

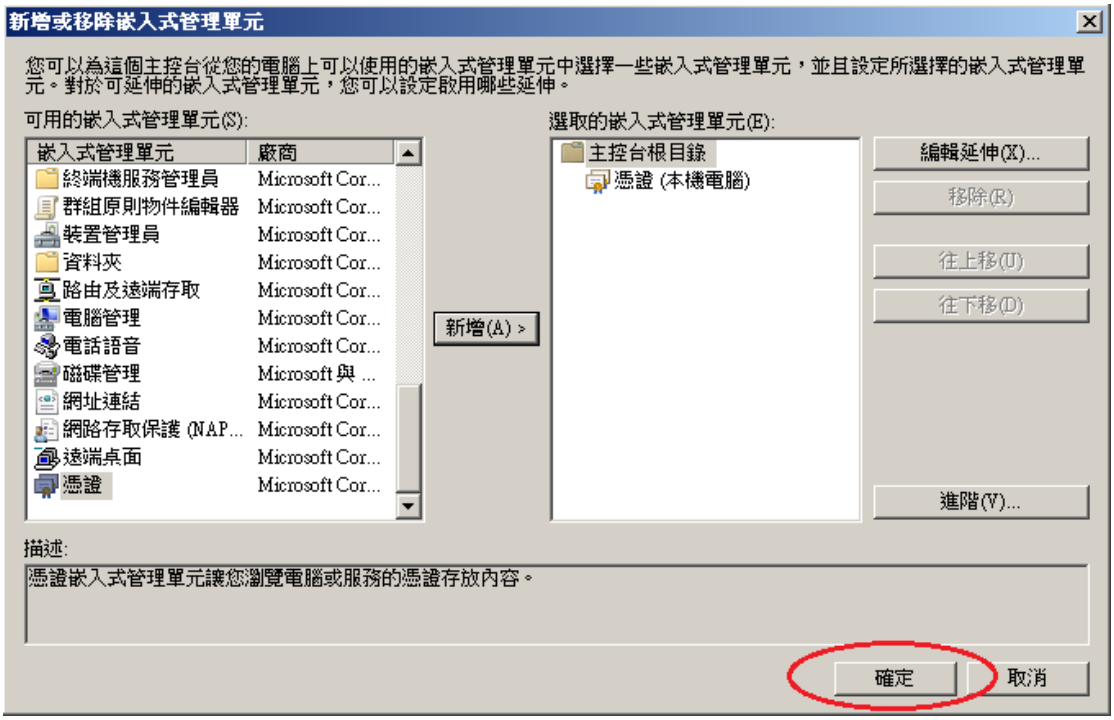


選擇「電腦帳戶」→「下一步」→「完成」。

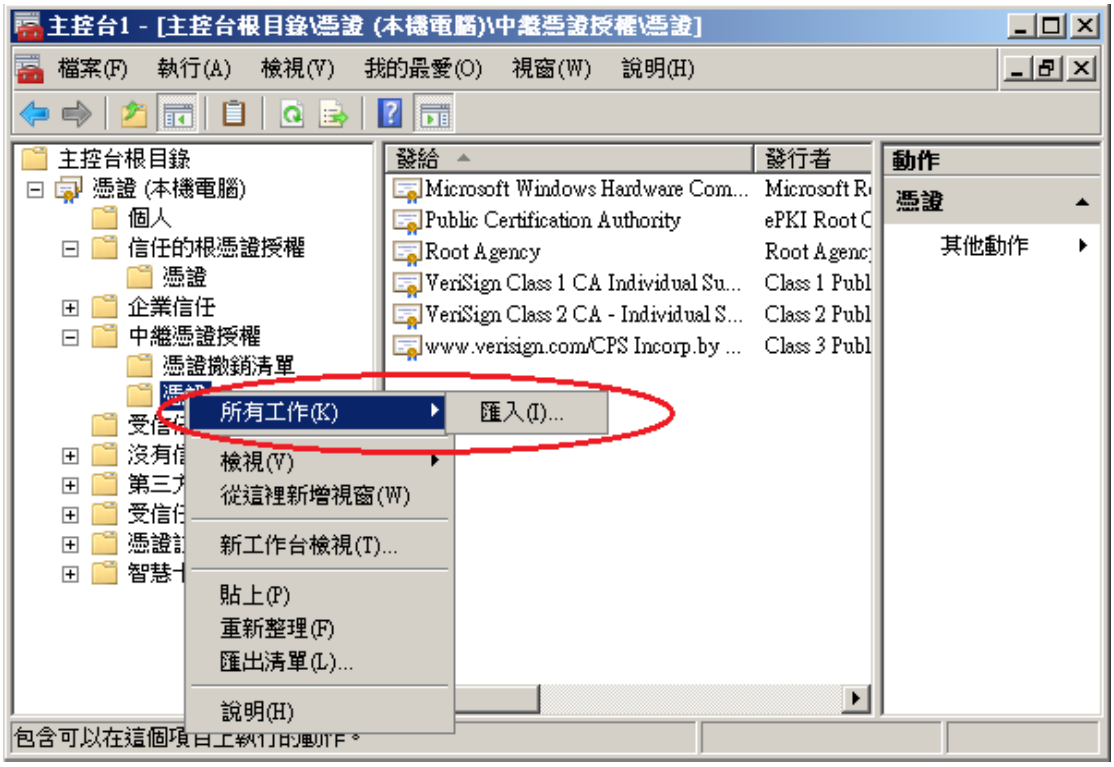

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


選擇電腦
請選擇您要嵌入式管理單元管理的電腦。
這個嵌入式管理單元將自動管理:
本機電腦(L): (執行這個主控台的電腦)
另一台電腦(A):
瀏覽(R)...
允許對選取的電腦進行從命令列所啟動的變更。這只在您儲存主控台後才能適用(W)
< 上一步(B)
完成
取消

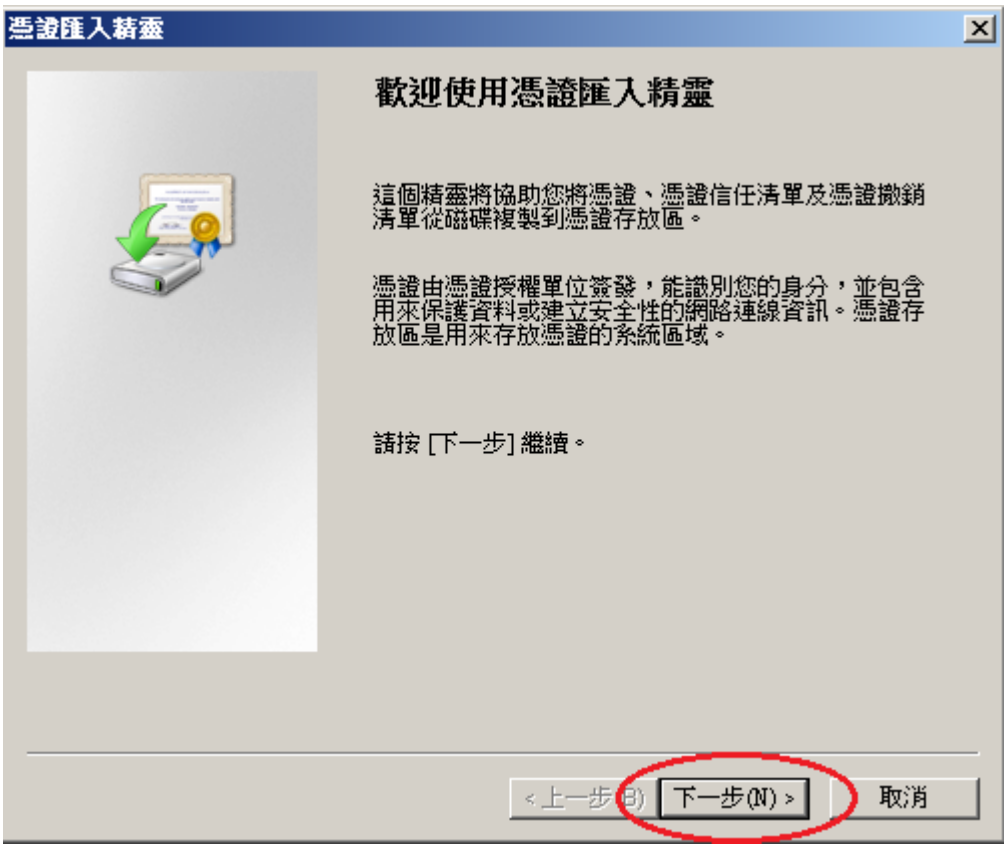
最後按下「確定」。

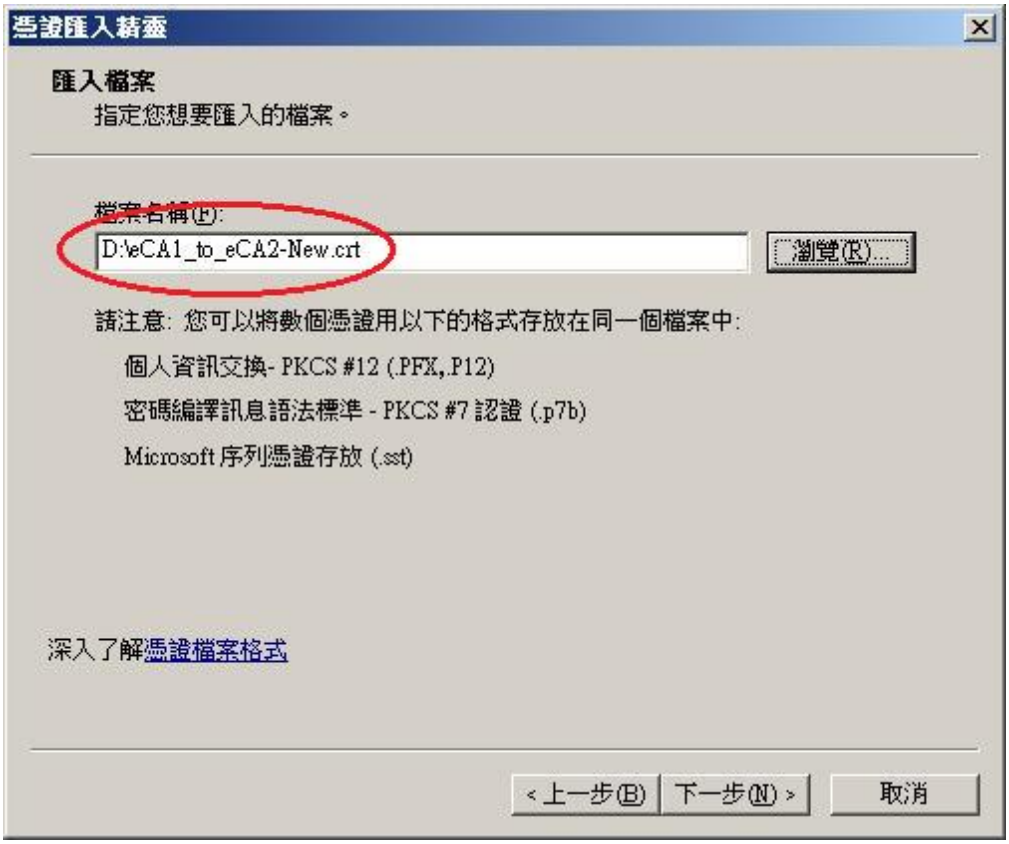


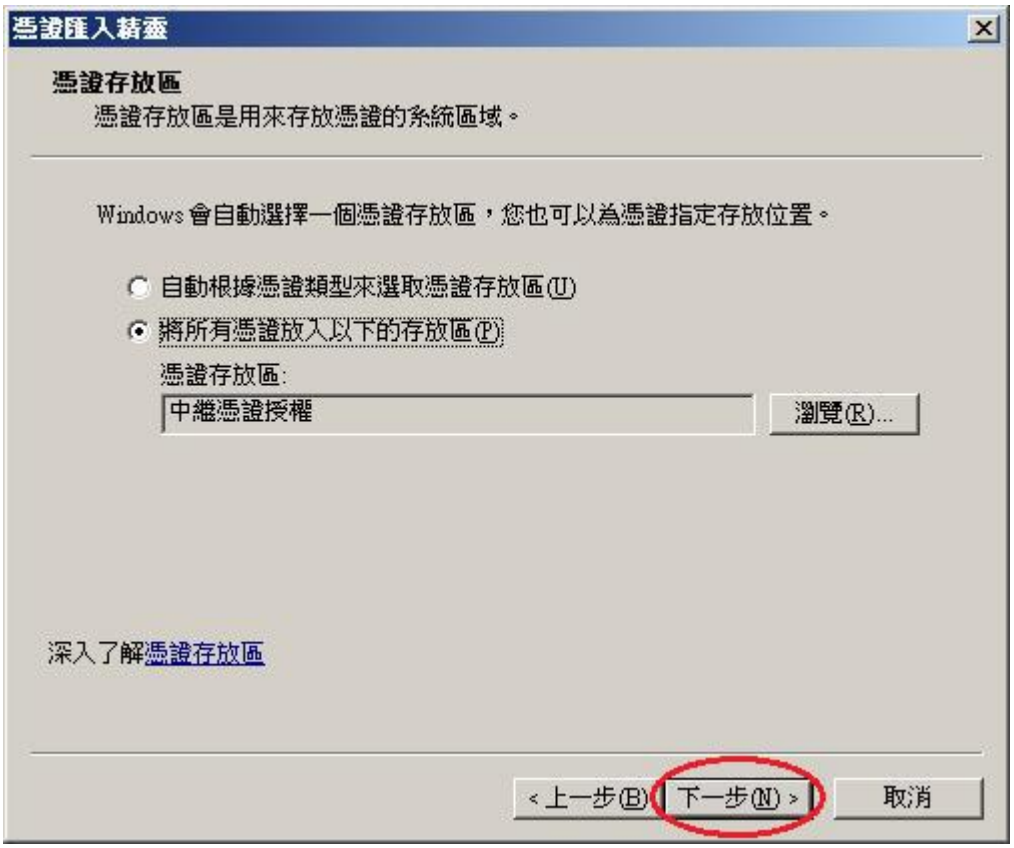
十一、 **匯入 eCA 自發憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



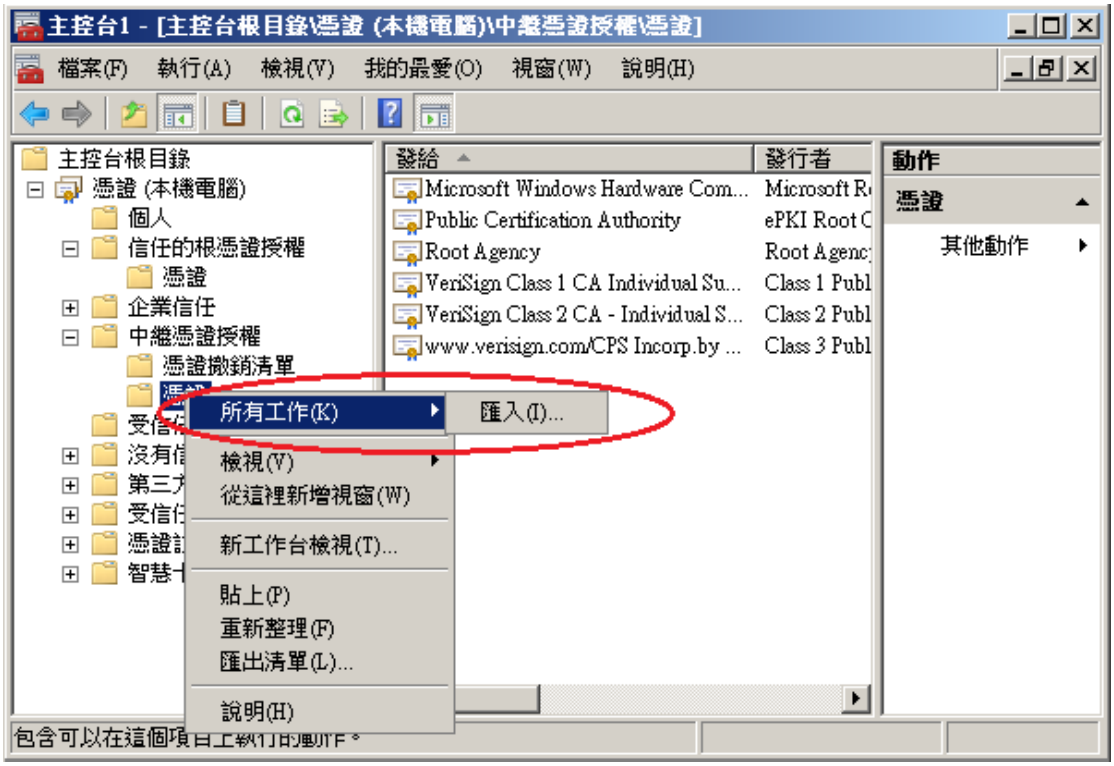
出現以下畫面後，點選「下一步」→「下一步」→「完成」。


憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈將協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
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性的網路連線資訊。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

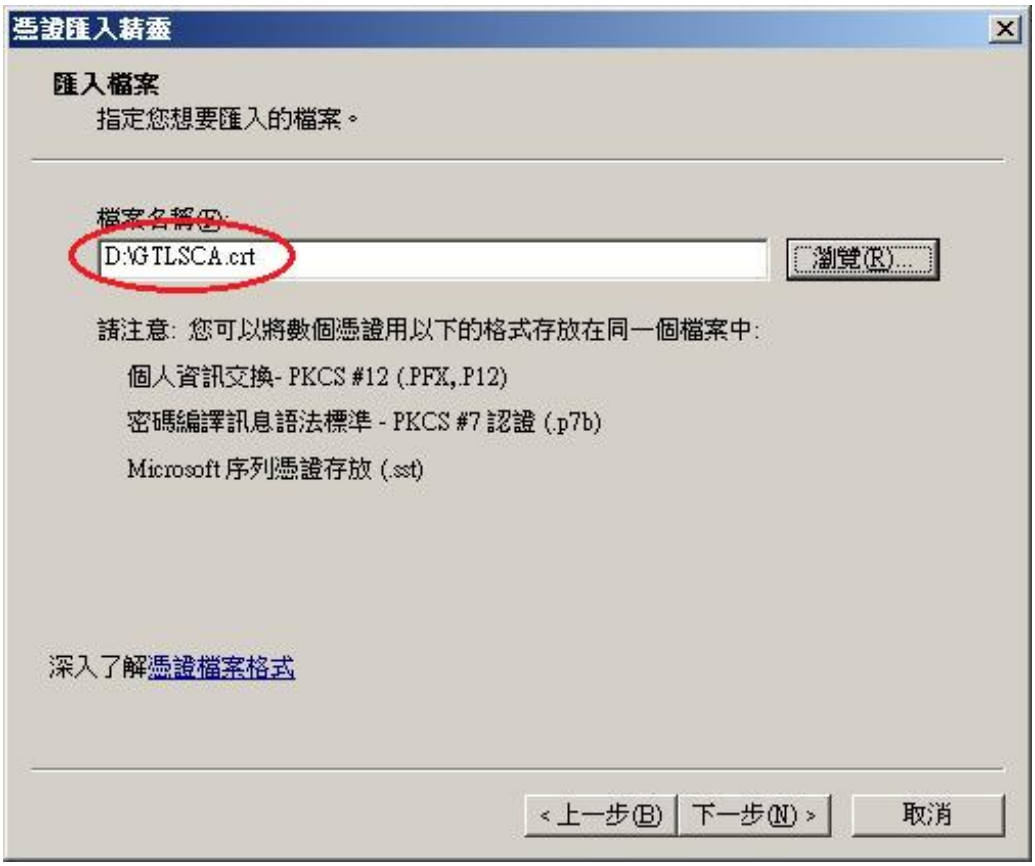

憑證匯入精靈
匯入檔案
指定您想要匯入的檔案。
檔案名稱(F):
D:\eCA1_to_eCA2-New.crt
瀏覽(R)...
請注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準 - PKCS #7 認證 (.p7b)
Microsoft 序列憑證存放 (.sst)
深入了解憑證檔案格式
< 上一步(B)
下一步(N) >
取消



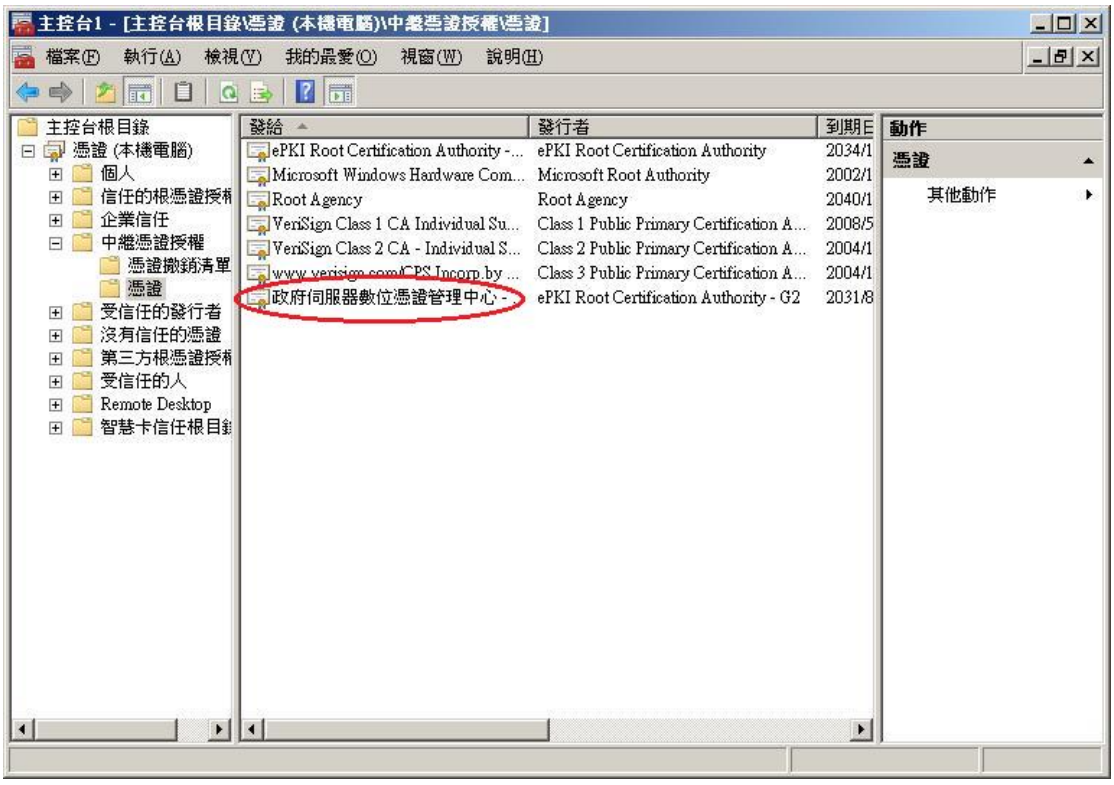
十二、 **匯入 GTLSCA 憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



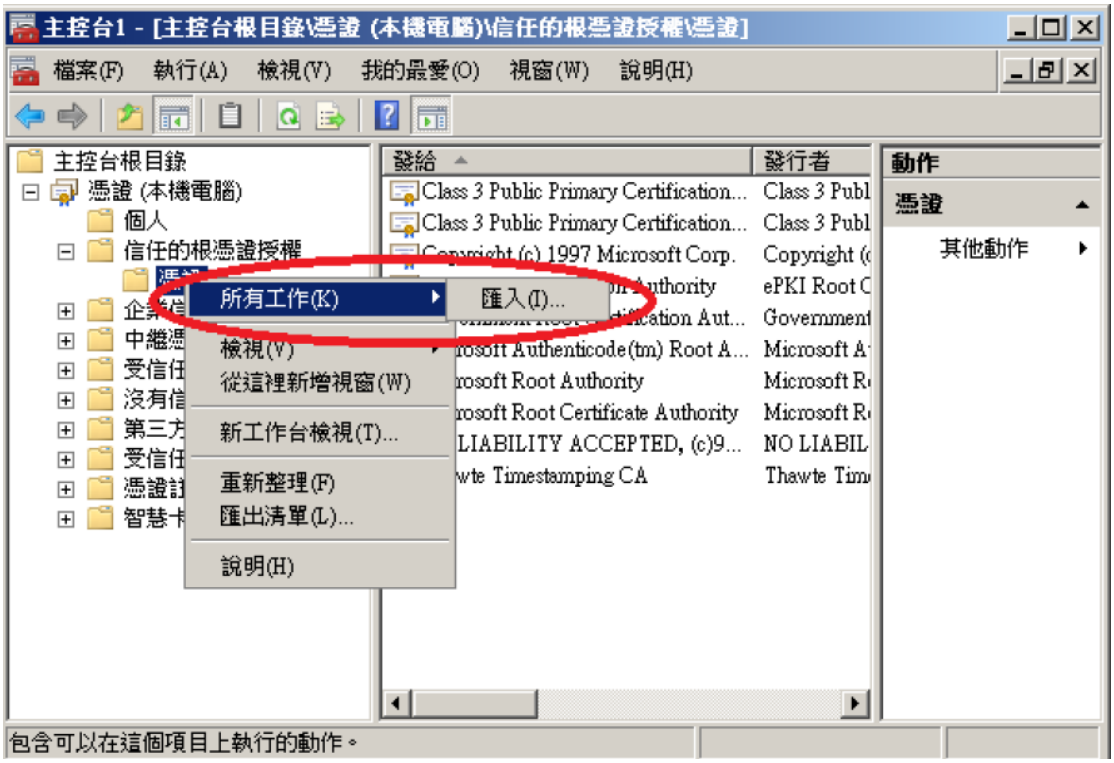
依照上述匯入 eCA 自發憑證的步驟，匯入 GTLSCA 憑證。

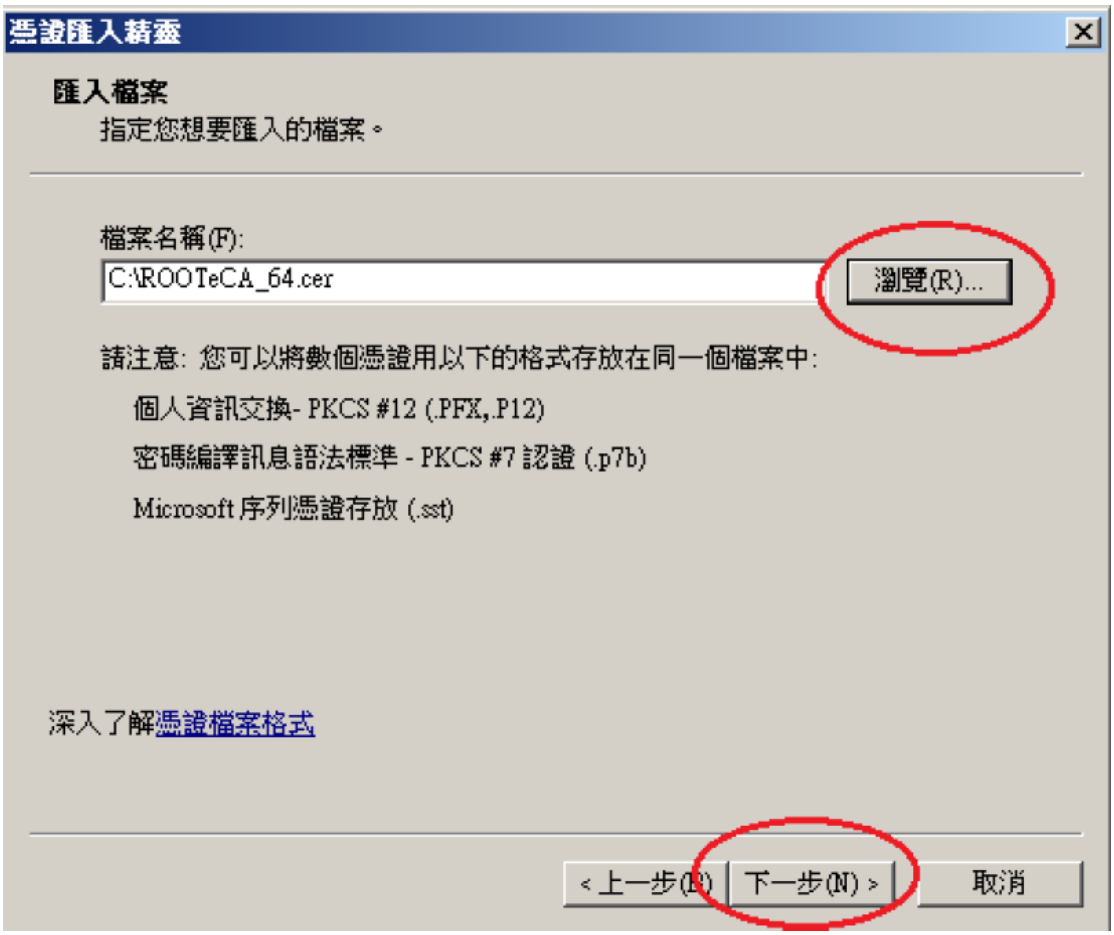


成功匯入後，可以看到 GTLSCA 的憑證。

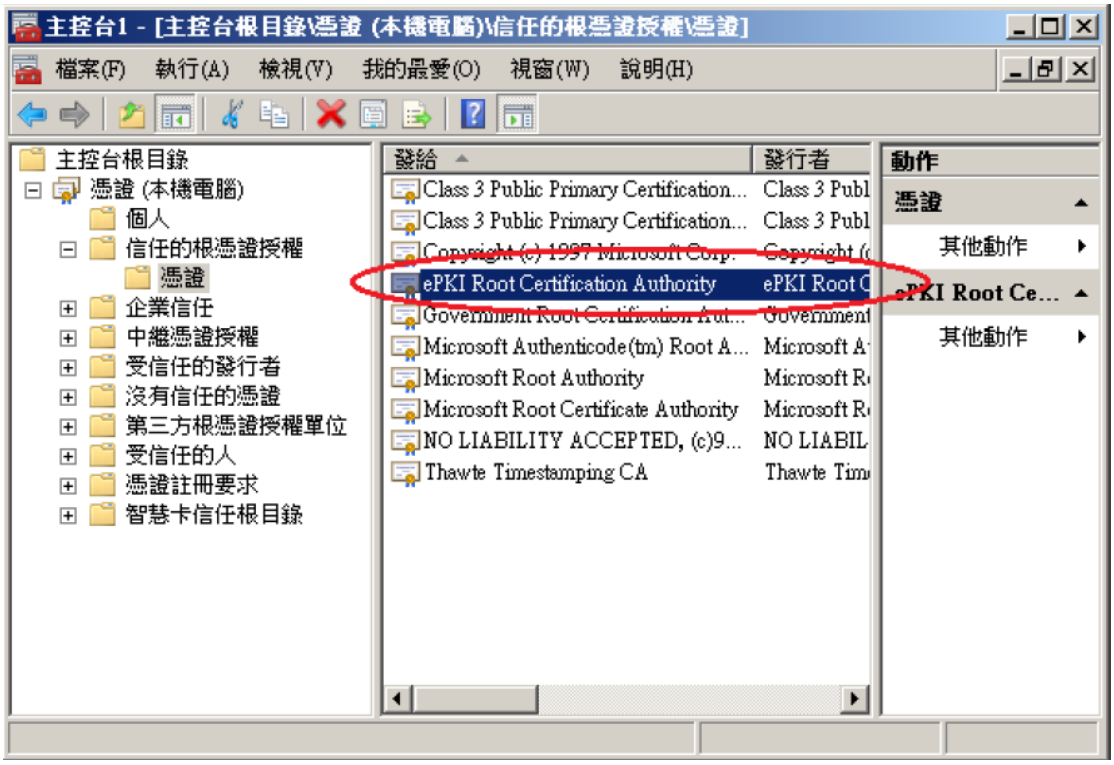


十三、 **匯入 eCA 根憑證**。在「信任的根憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



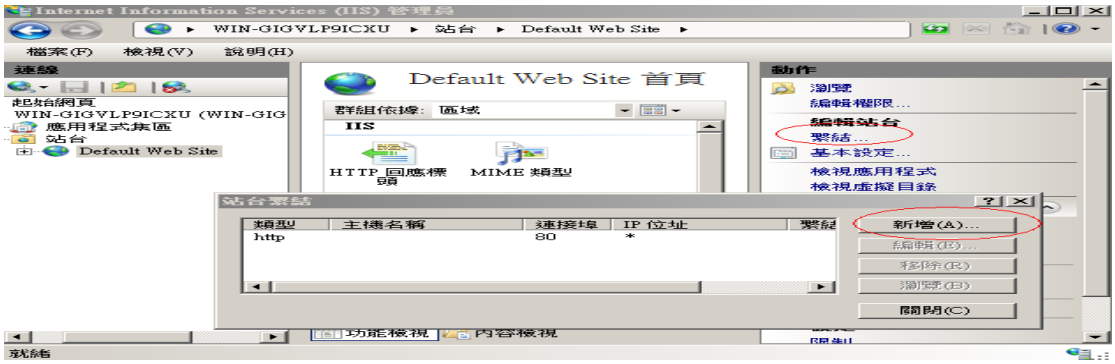


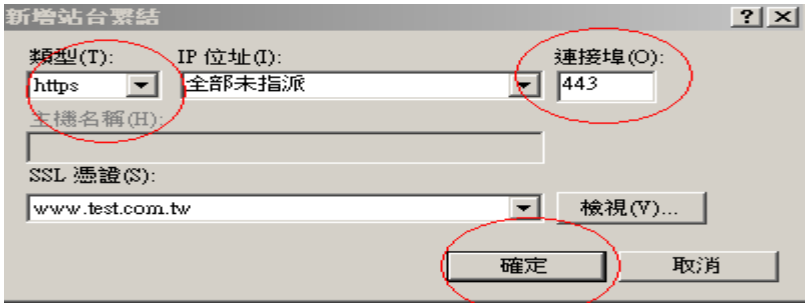
成功匯入後，可以看到 eCA 的根憑證。



十四、　檢查「信任的根憑證授權」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。

十五、　點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」→ 新增→類型『https』、連接埠 『443』，選擇要安裝在此站台之 SSL 憑證 (www.test.com.tw) 。





十六、　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：停用 SSLv2、SSLv3、TLS 1.0 和 TLS 1.1

- 需修改 Windows Registry (HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders \SCHANNEL\Protocols)
- 可直接於 GTLSCA 網站下載已經製作好之.reg 檔案，解壓縮後點兩下即可進行設定，可免除手動修改 Registry 之麻煩 https://gtlsca.nat.gov.tw/download/Disable_Protocols.zip
- 本.reg 檔案會開啟 TLS 1.2 Server 端協定，並關閉 SSLv2、SSLv3、TLS 1.0 和 TLS 1.1 之 Server 端協定
- 重新啟動電腦。

附件二：單一 IP，多站台啟用 SSL

IIS7 在只有一個 IP 的情況下，只能有一個網站使用 443 Port，針對這個狀況，TLS 協定有新增 SNI(Server Name Indication)的技術解決這個問題，但以 IIS 來說，需 IIS8 以上版本才支援 SNI 的技術，相關支援性請參考維基百科的資訊 (https://en.wikipedia.org/wiki/Server_Name_Indication)。

基於上述原因，若需使用 SNI 的技術，必須將 Windows Server 升級到 2012 的版本(IIS8)，或是改用其他的 Web Server(例如：Apache, Tomcat 等)。