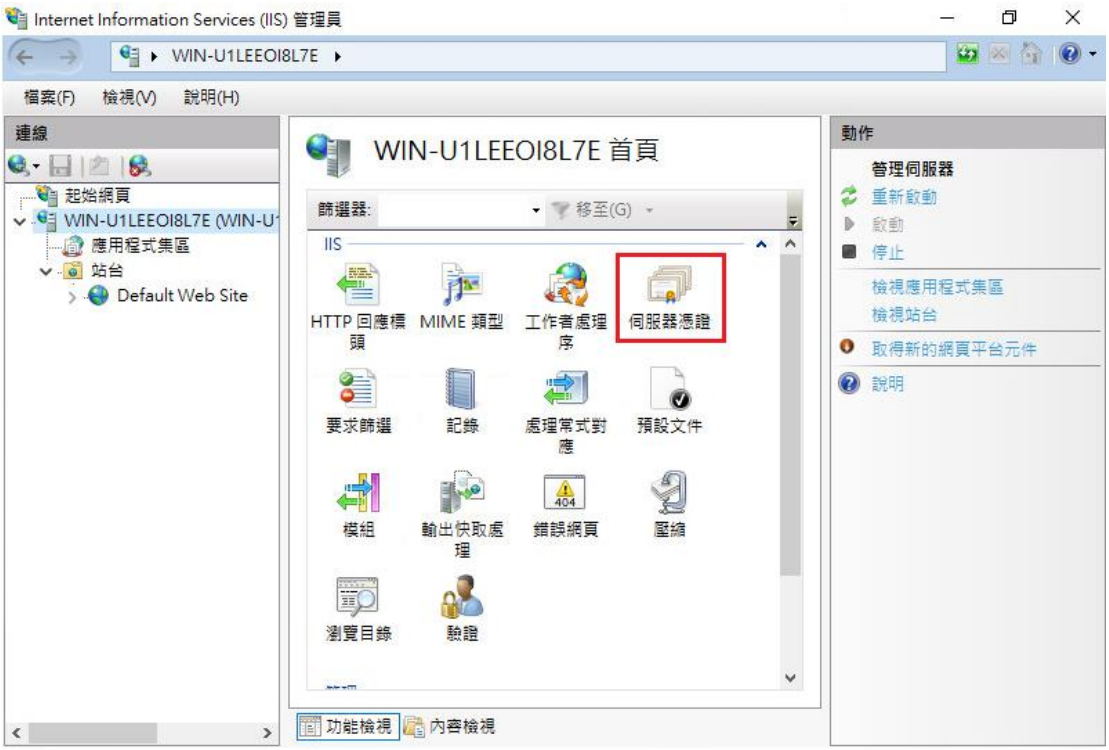
政府伺服器數位憑證管理中心(GTLSCA)

Windows IIS 10.0 SSL 憑證請求檔製作與憑證安裝手冊

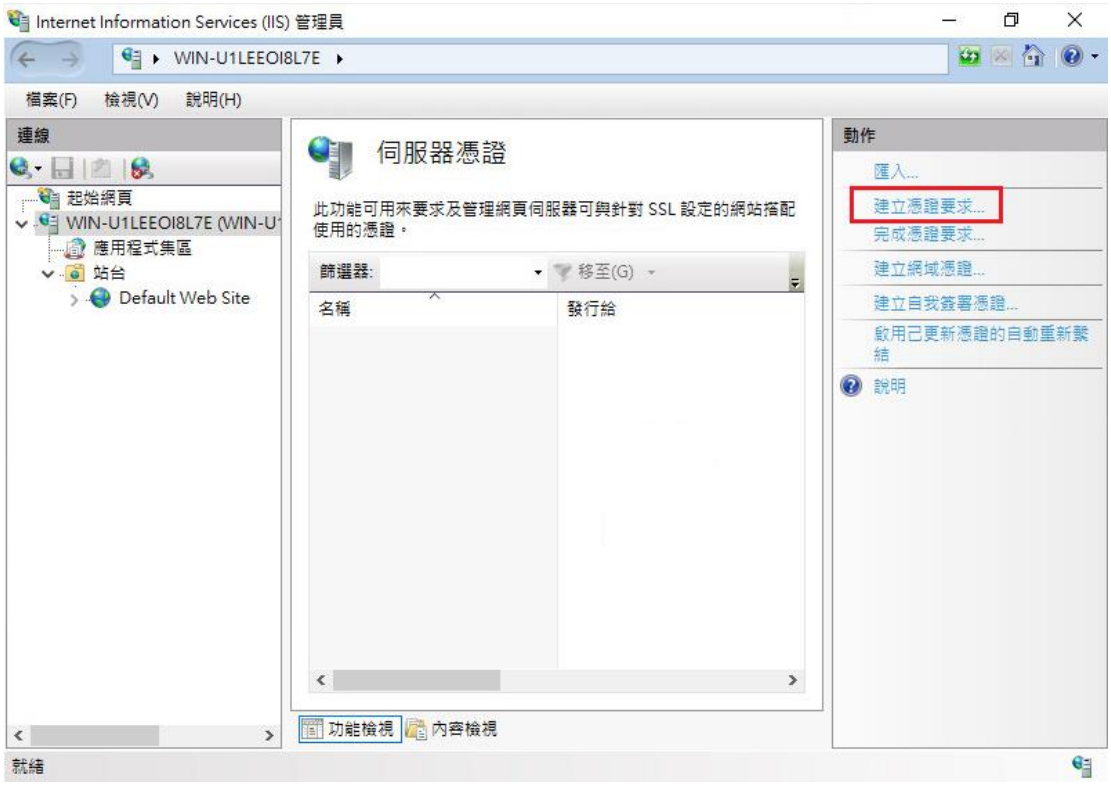
目錄

Windows IIS 10.0 SSL 憑證請求檔製作手冊

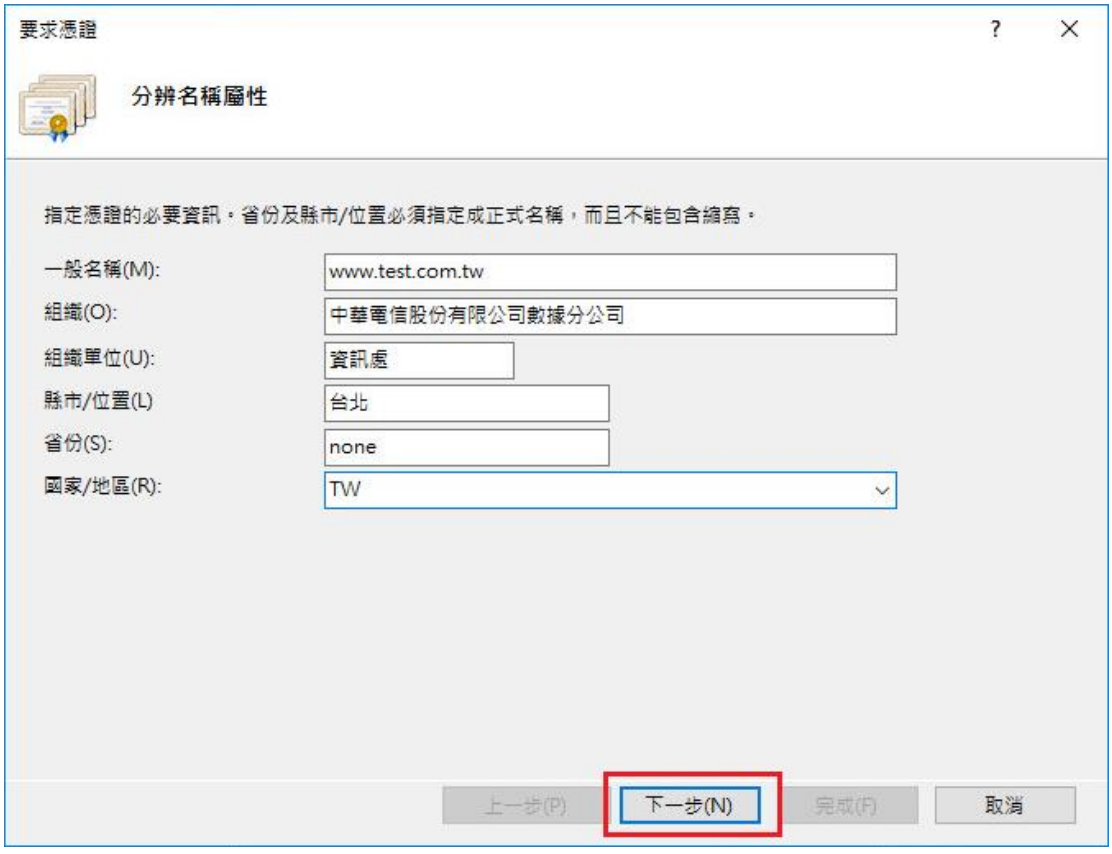
一、開啟「Internet Information Services (IIS)管理員」並點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」兩下。



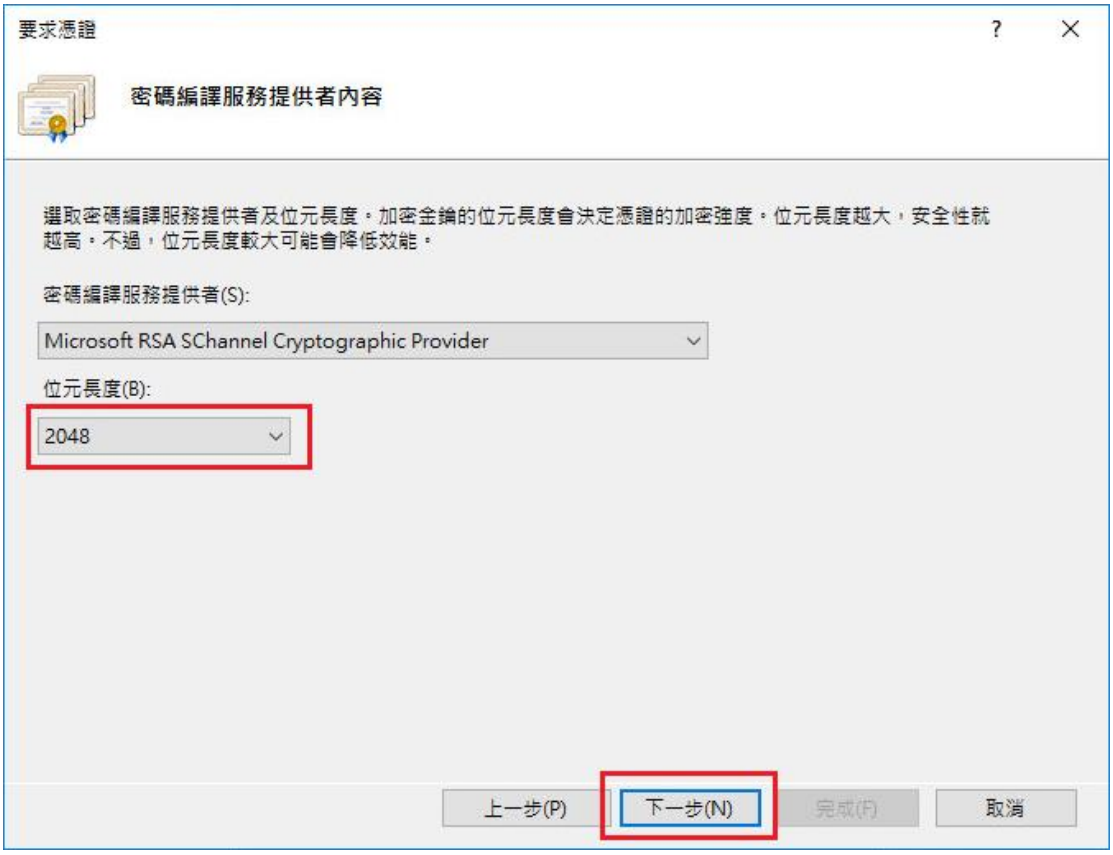
二、點選「建立憑證要求」



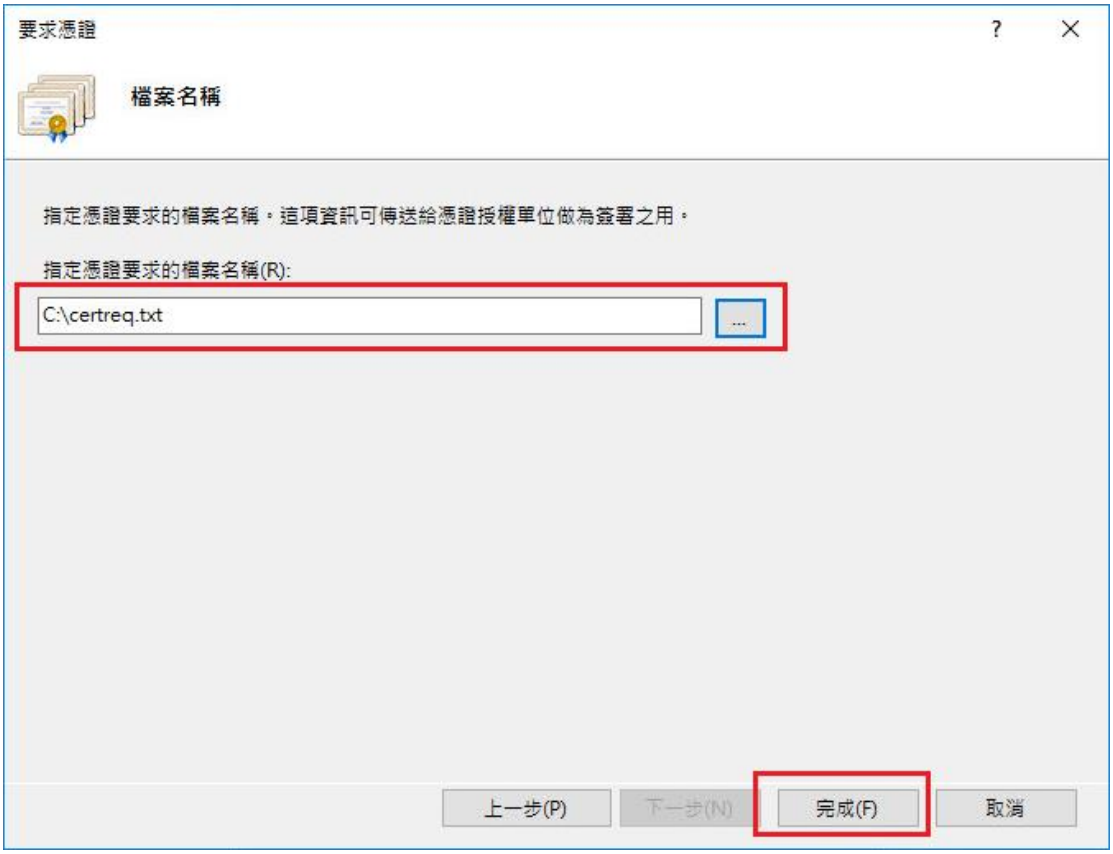
三、輸入以下所有欄位資料，輸入完成後請點選「下一步」，多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主。



四、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。



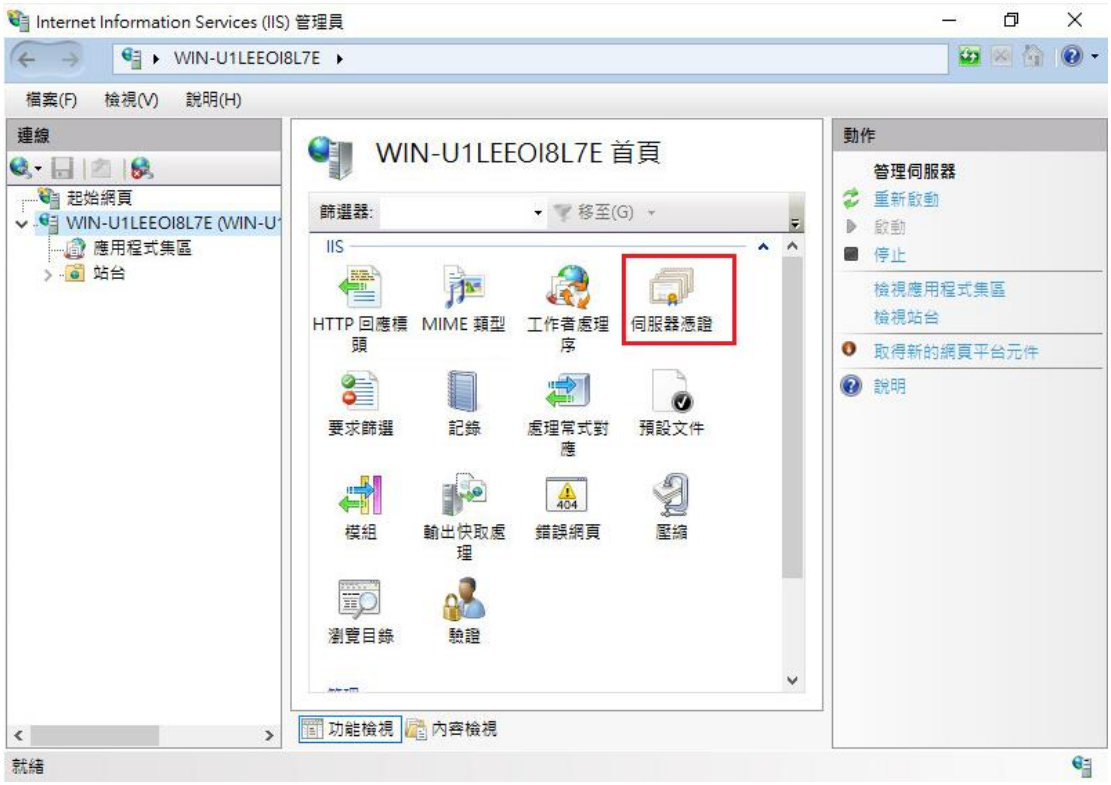
五、指定儲存憑證請求檔的檔案名稱與存放位置，確認後請點選「完成」。



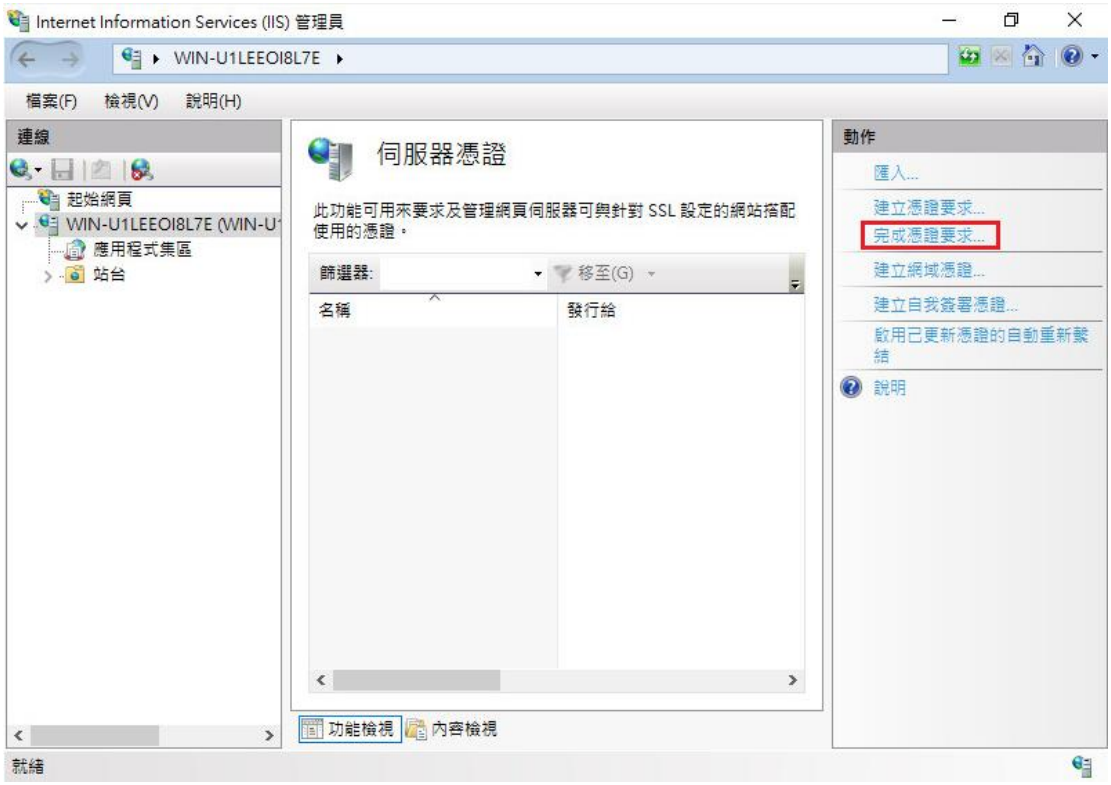
六、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至憑證管理中心（https://gca.nat.gov.tw）申請 SSL 憑證。

Windows IIS 10.0 SSL 憑證安裝操作手冊

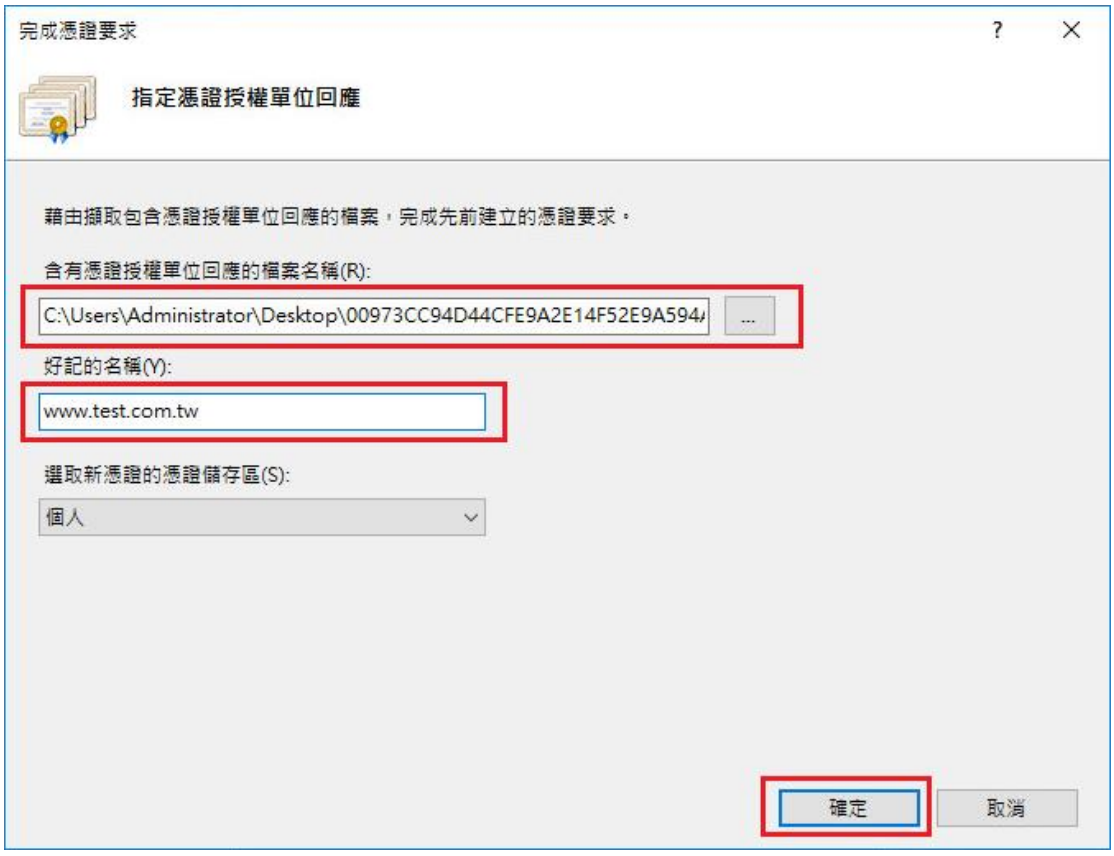
一、開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



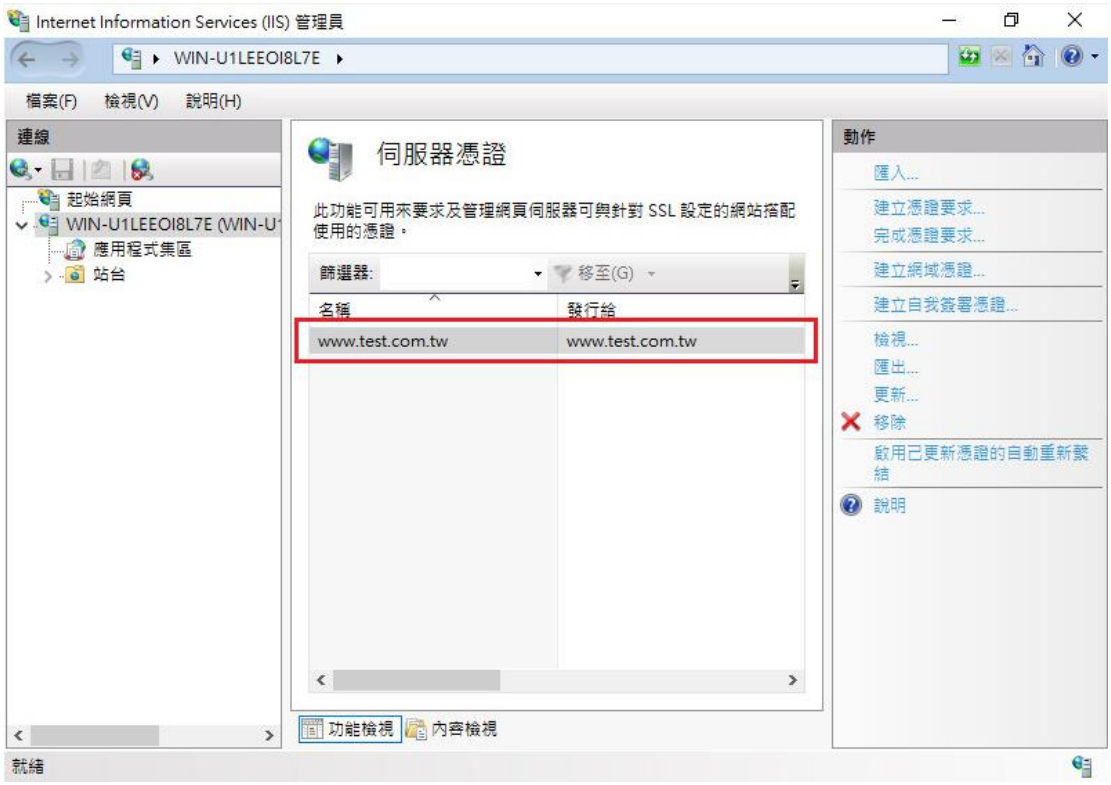
二、點選「完成憑證要求」。



三、如下圖，選擇至憑證管理中心申請之 SSL 憑證，並輸入好記的名稱(一般填寫 Domain Name)。



四、步驟 4 按「確定」，出現完成憑證要求的畫面。

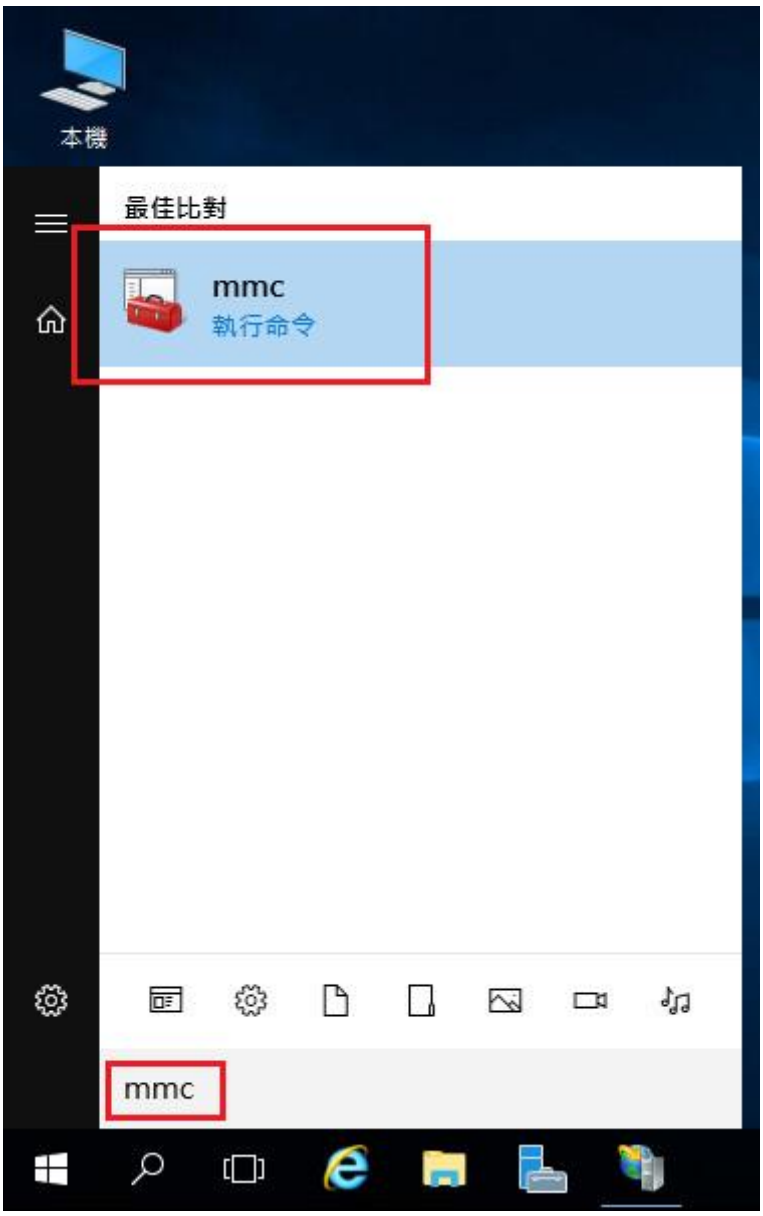


五、至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip

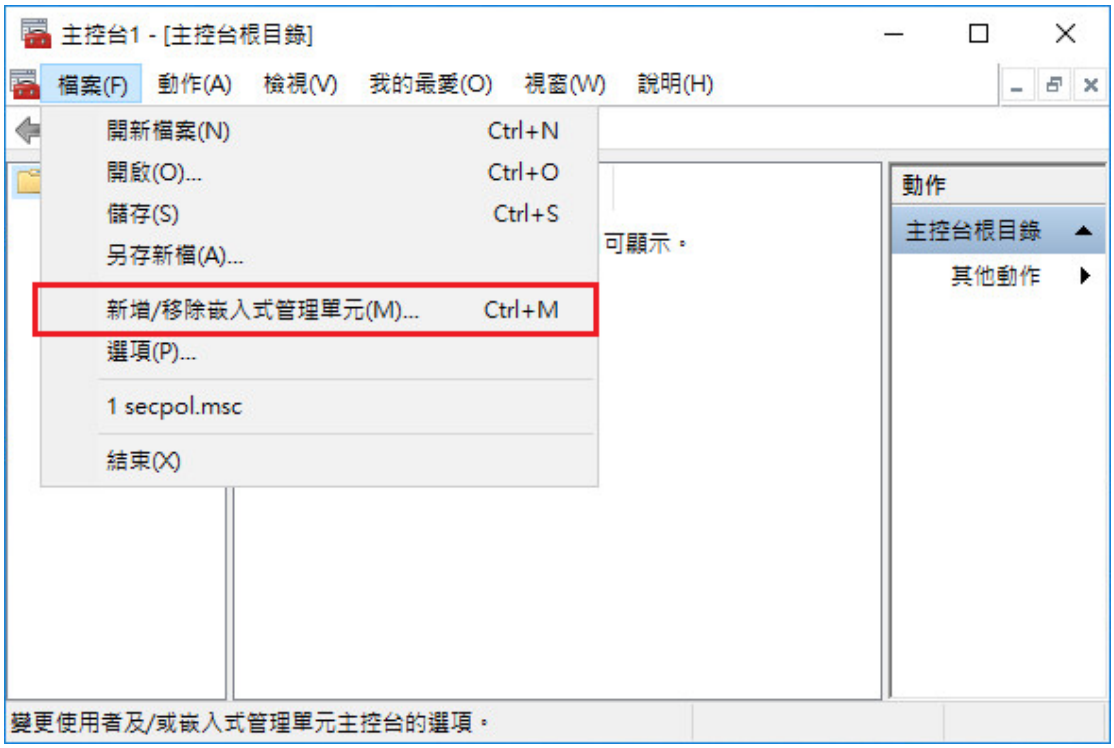
六、將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案。

七、接著要安裝 eCA 自發憑證及 GTLSCA。

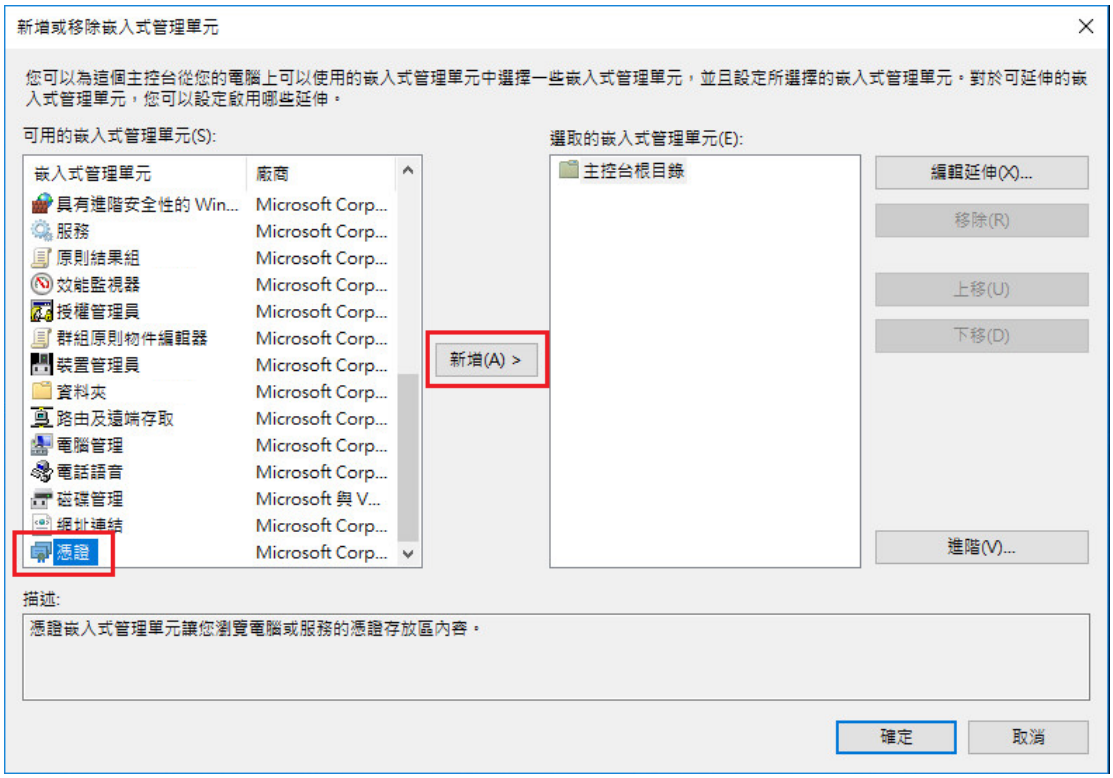
請先點選左下角的「Windows」圖示→輸入「mmc」→按下「Enter」。



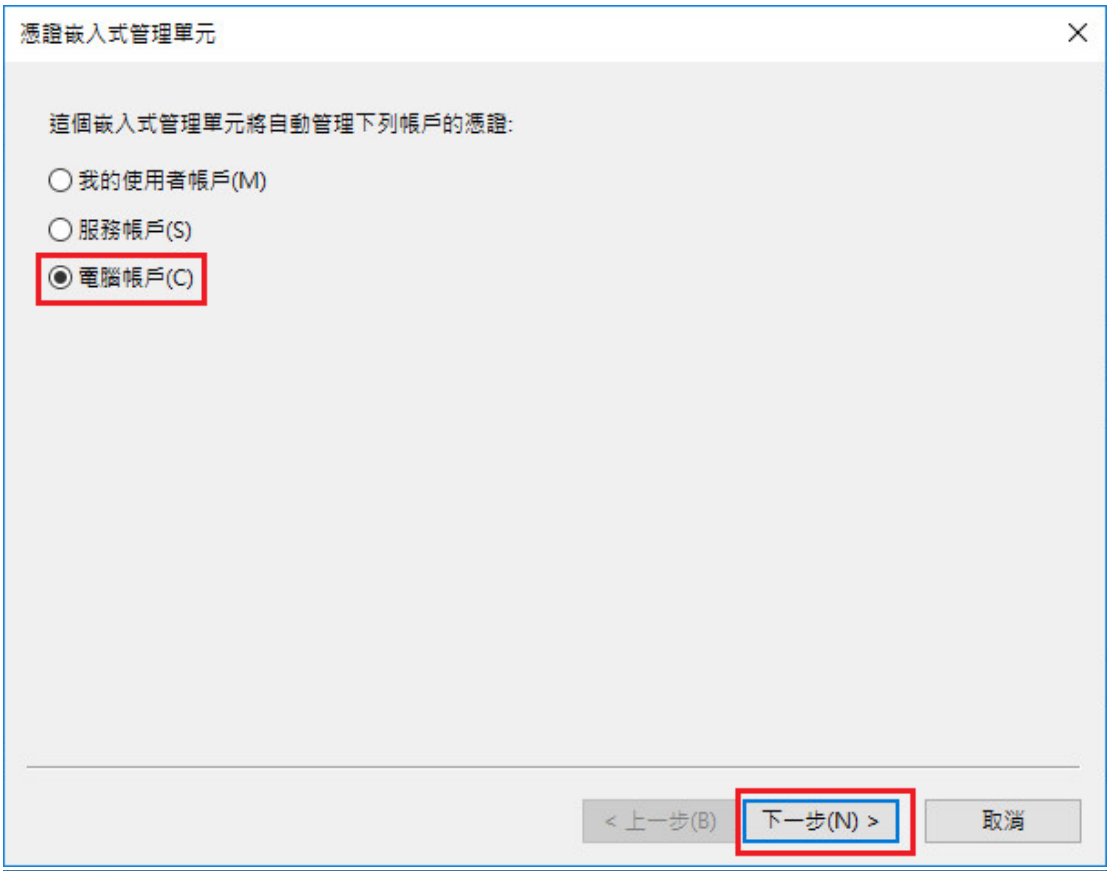
八、選擇「新增/移除嵌入式管理單元」。

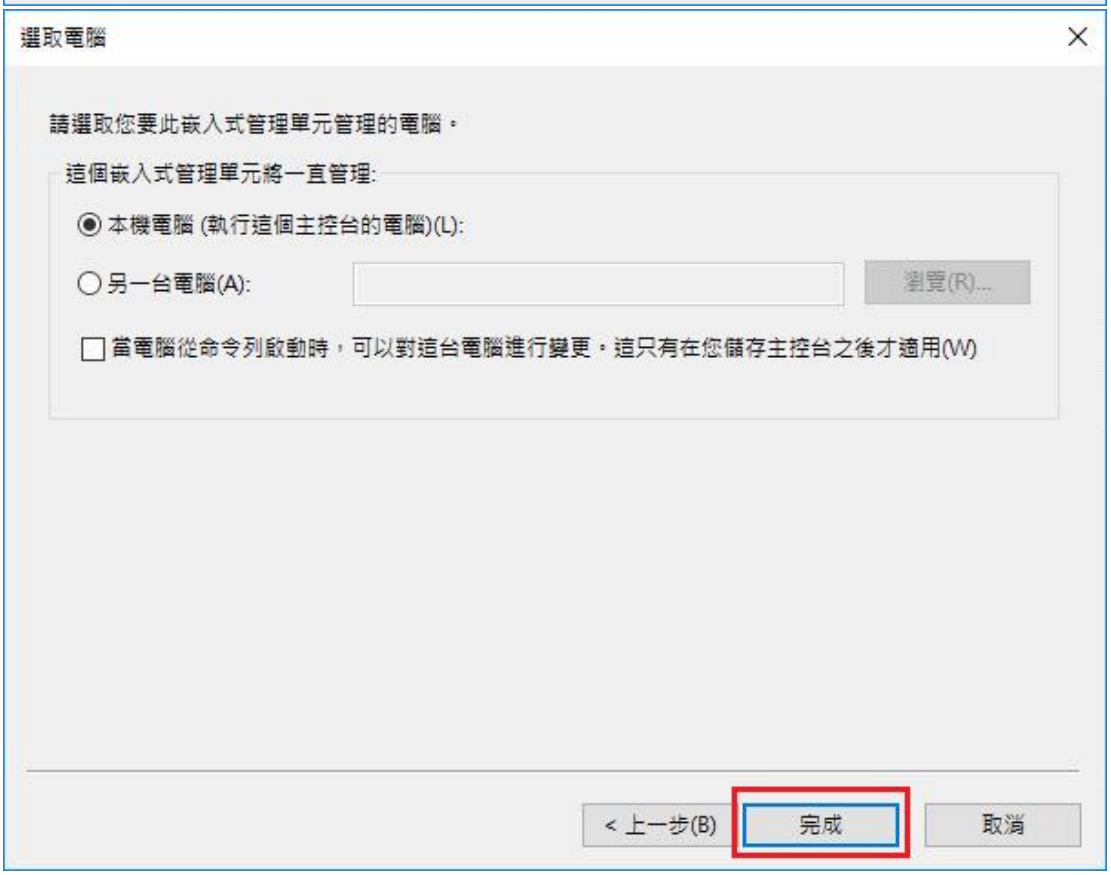


九、接著點選「憑證」→「新增」。

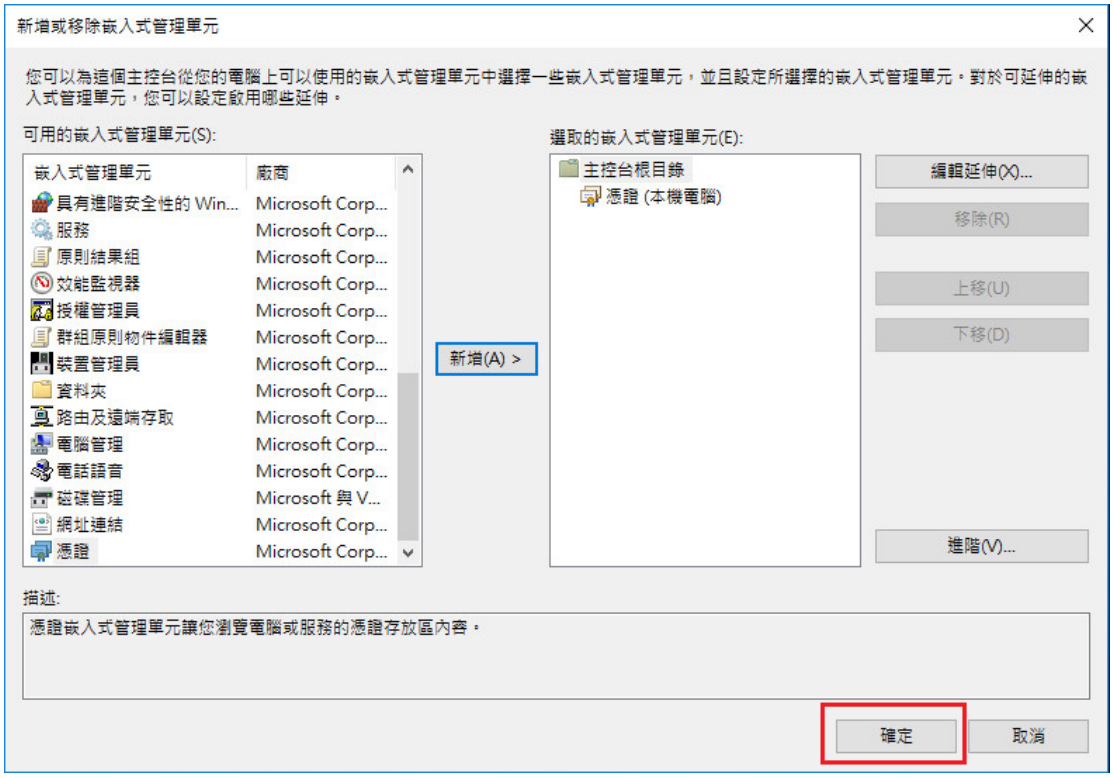


選擇「電腦帳戶」→「下一步」→「完成」。

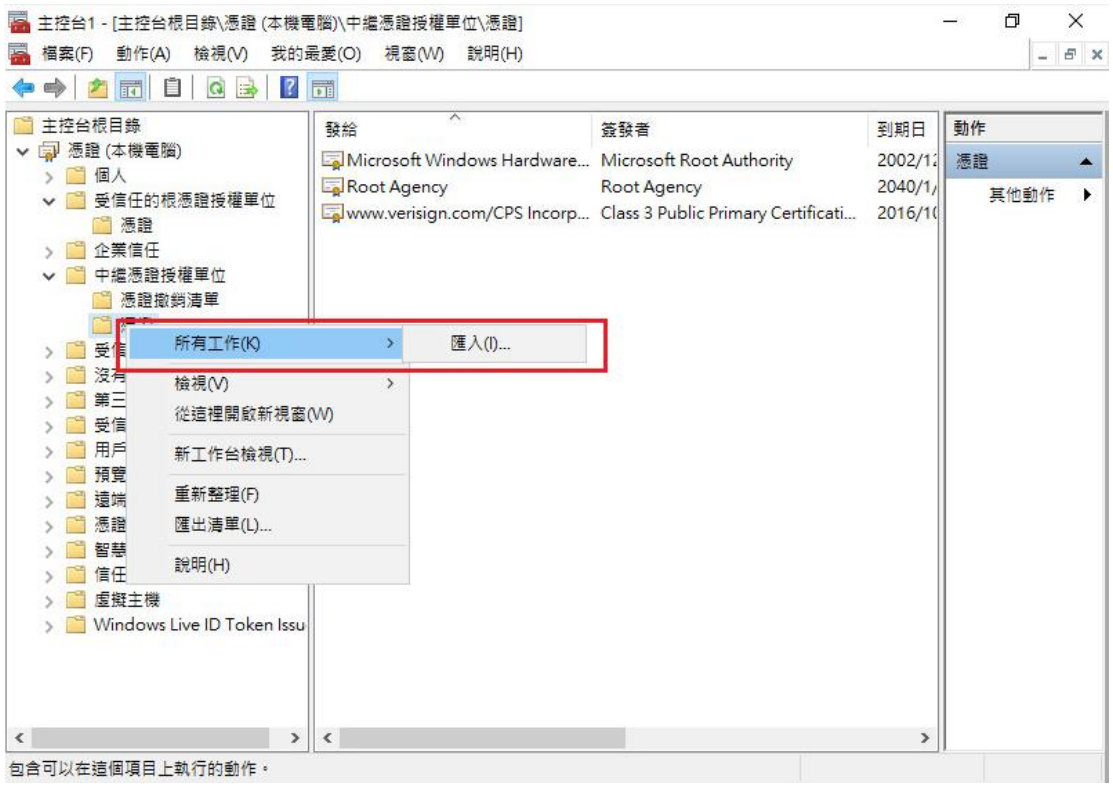

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


選取電腦
請選取您要此嵌入式管理單元管理的電腦。
這個嵌入式管理單元將一直管理:
本機電腦 (執行這個主控台的電腦)(L):
另一台電腦(A):
瀏覽(R)...
當電腦從命令列啟動時，可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)
< 上一步(B)
完成
取消

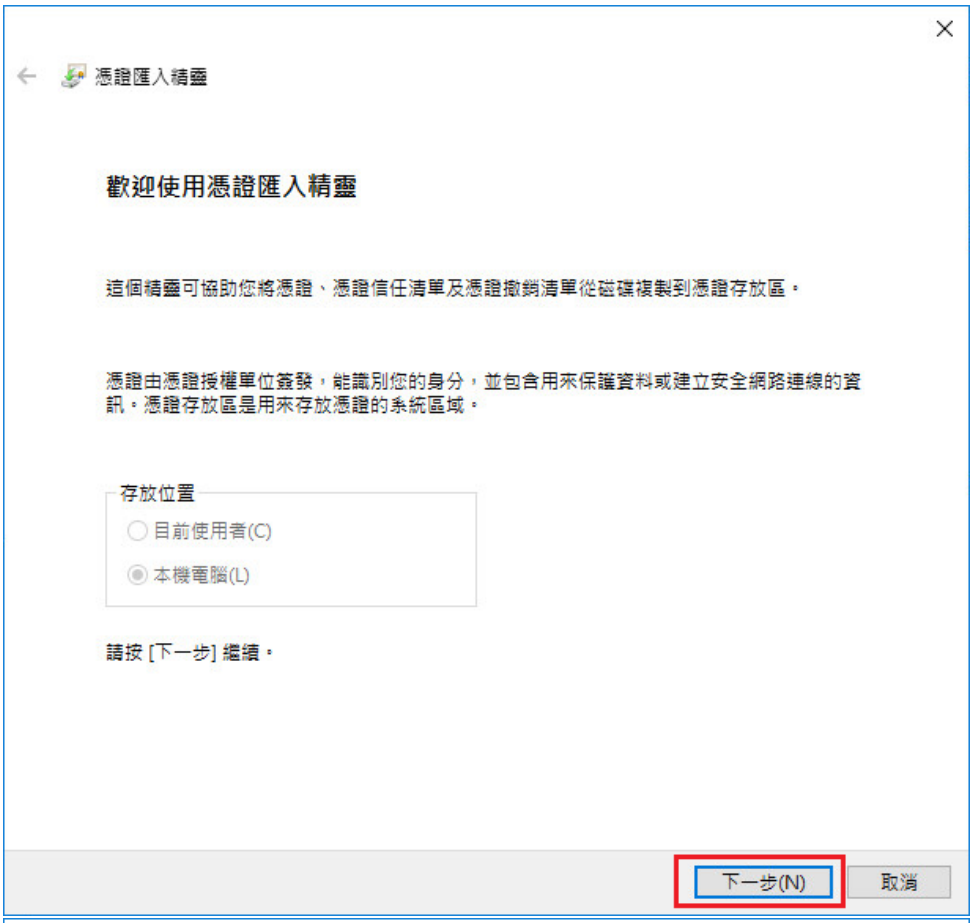
最後按下「確定」。

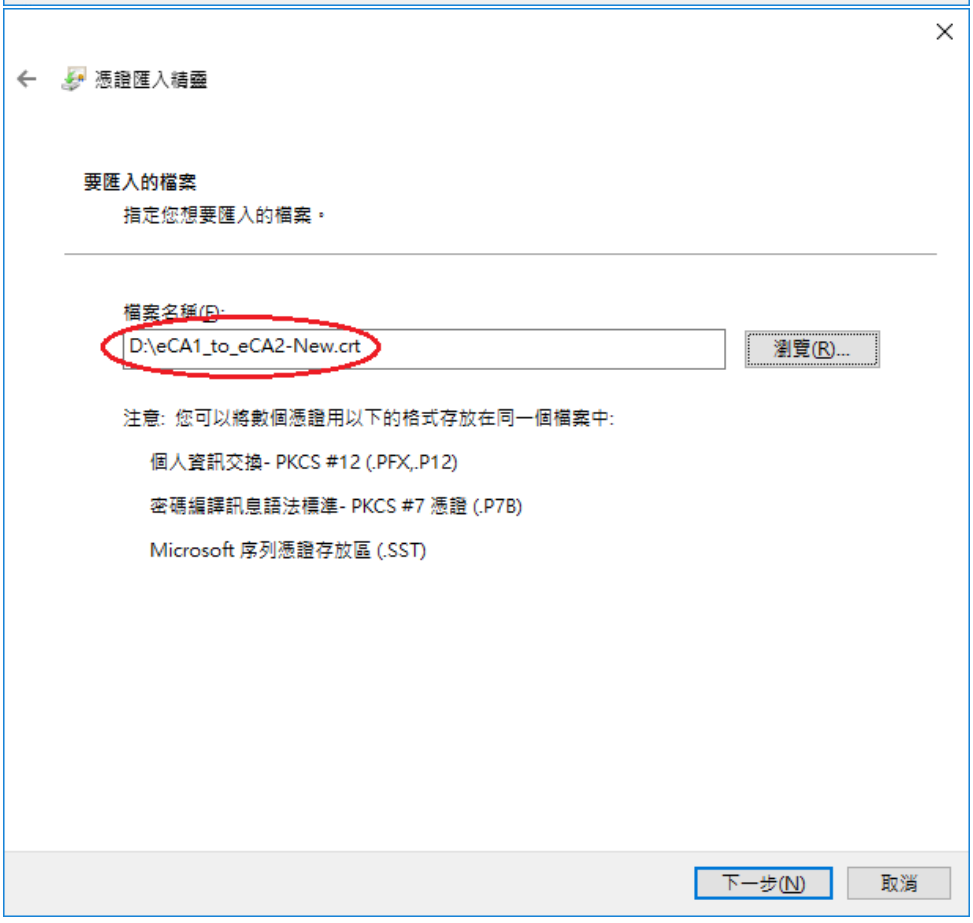


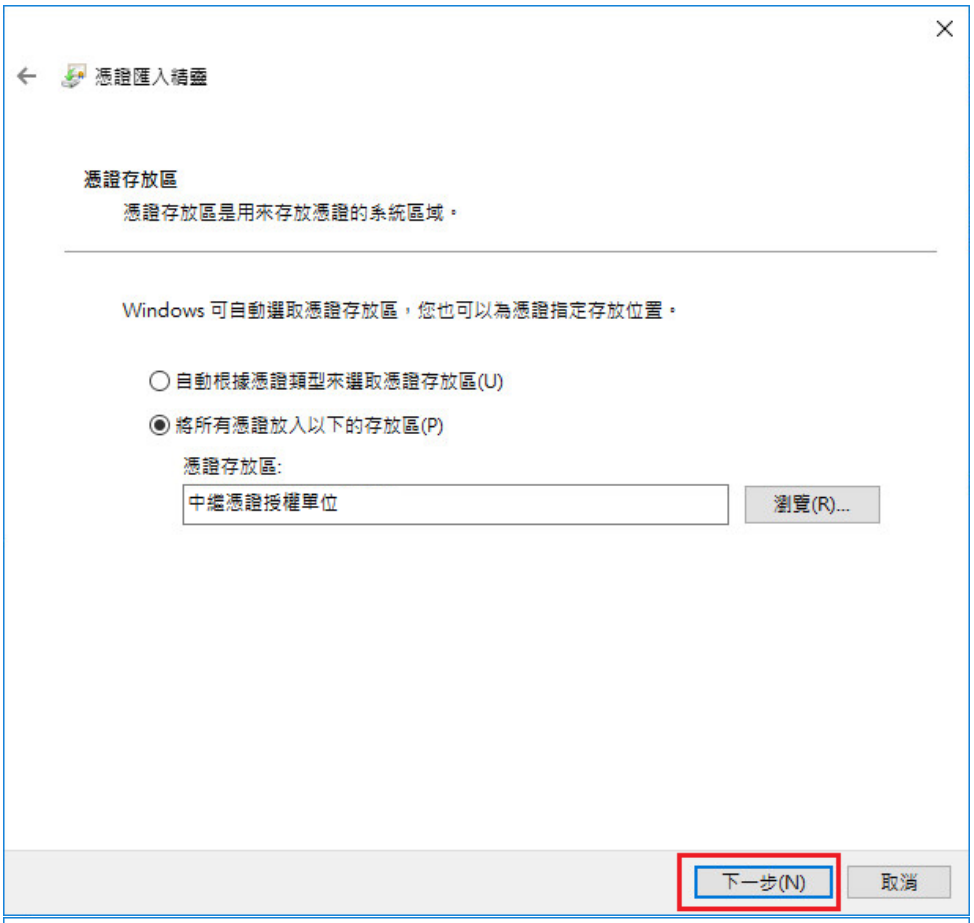
十、**匯入 eCA 自發憑證**。在「中繼憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。

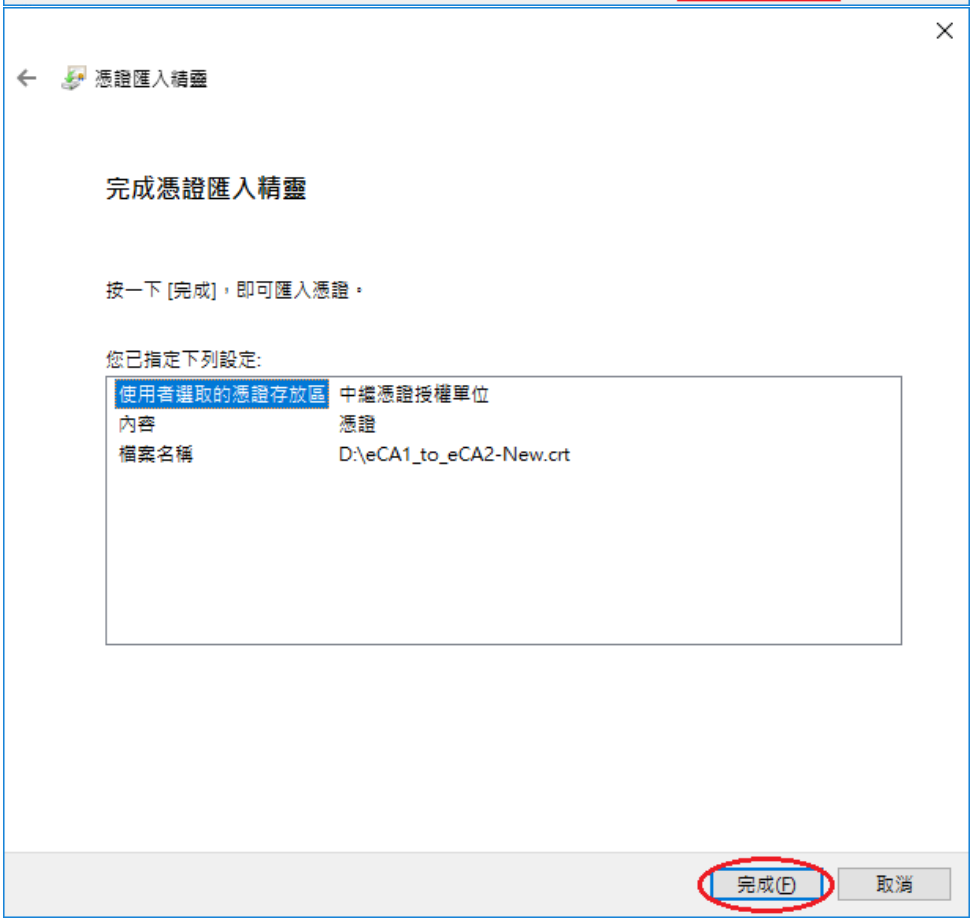


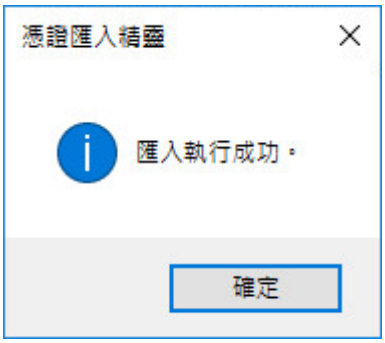
十一、依照下列步驟匯入自發憑證。


憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、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網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消

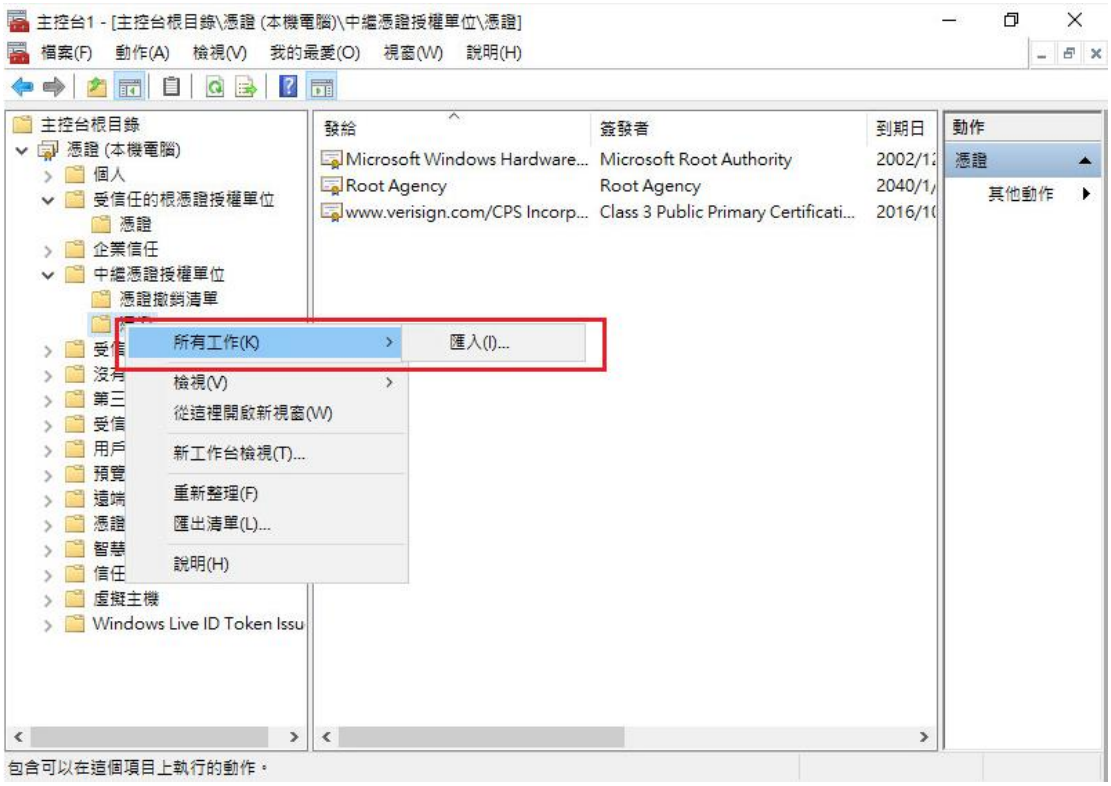

憑證匯入精靈
要匯入的檔案
指定您想要匯入的檔案。
檔案名稱(F):
D:\eCA1_to_eCA2-New.crt
瀏覽(R)...
注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)
Microsoft 序列憑證存放區 (.SST)
下一步(N)
取消


憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
中繼憑證授權單位
瀏覽(R)...
下一步(N)
取消

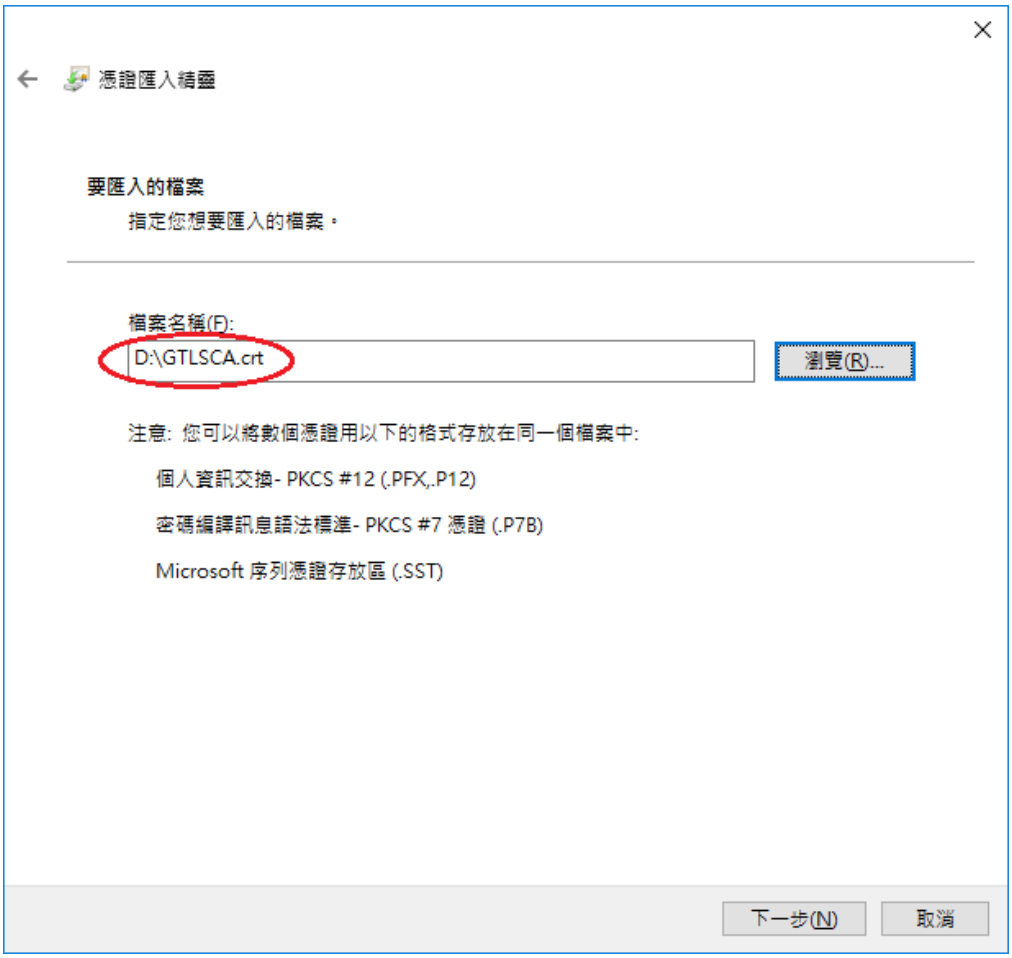

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即可匯入憑證。
您已指定下列設定:
使用者選取的憑證存放區 中繼憑證授權單位
內容 憑證
檔案名稱 D:\eCA1_to_eCA2-New.crt
完成(F)
取消



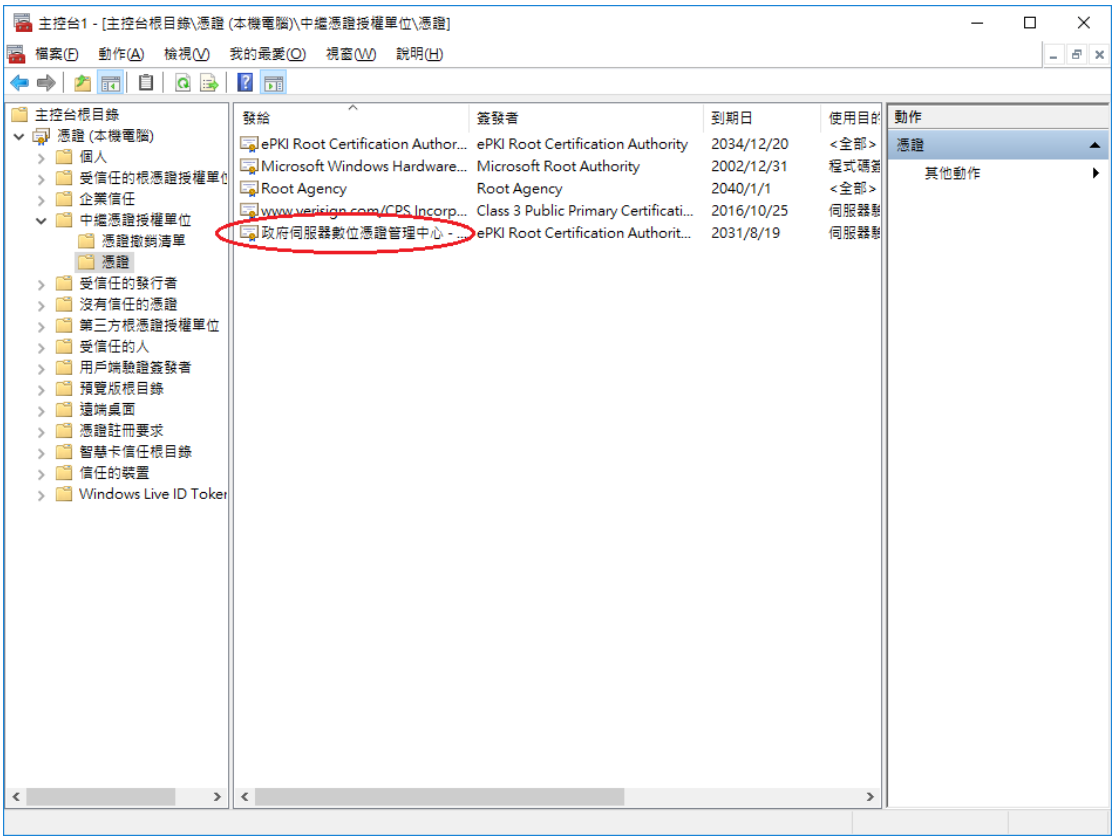
十二、**匯入 GTLSCA 憑證**。在「中繼憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



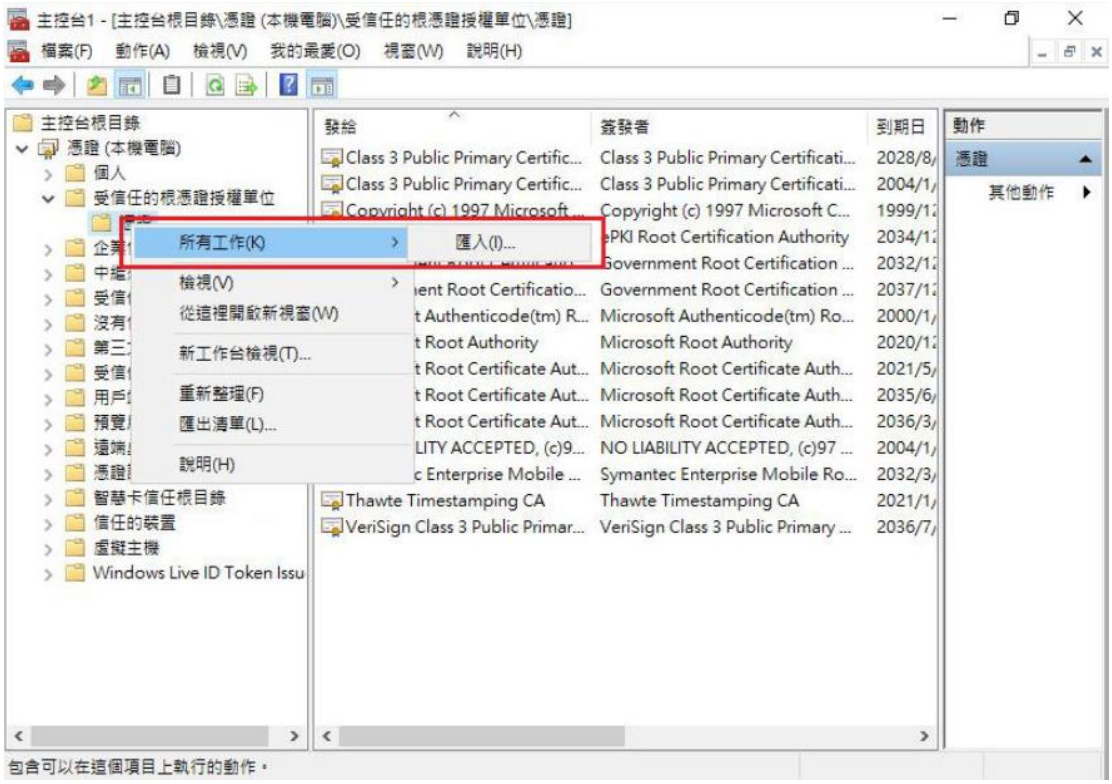
依照上述匯入 eCA 自發憑證的步驟，匯入 GTLSCA 憑證。

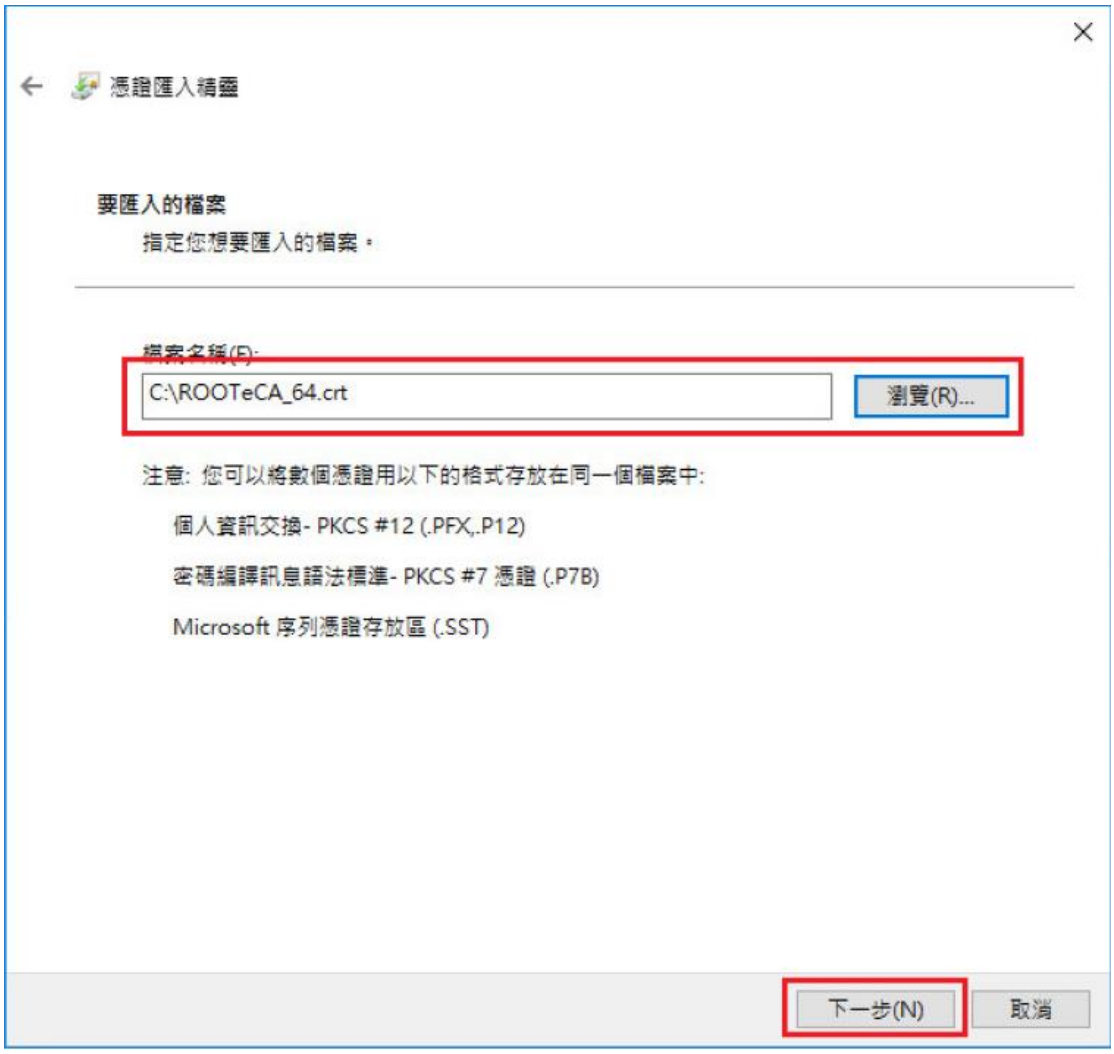


成功匯入後，可以看到 GTLSCA 的憑證。

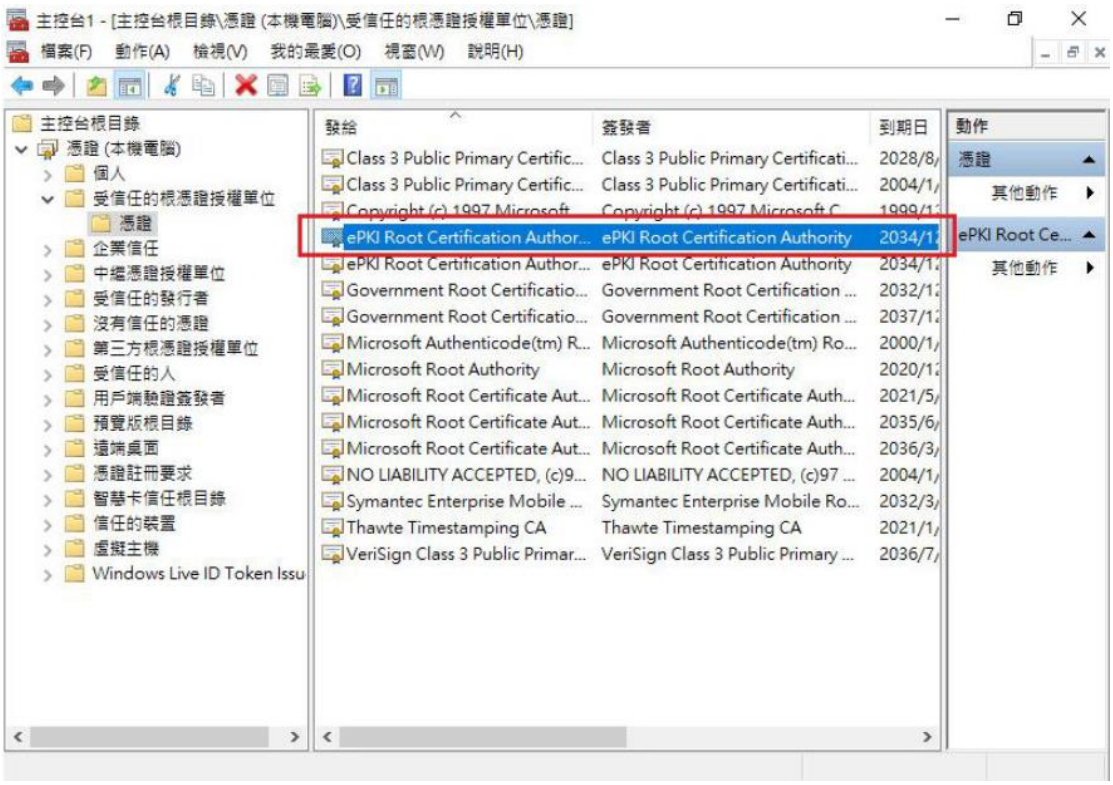


十三、**匯入 eCA 根憑證**。在「受信任的根憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



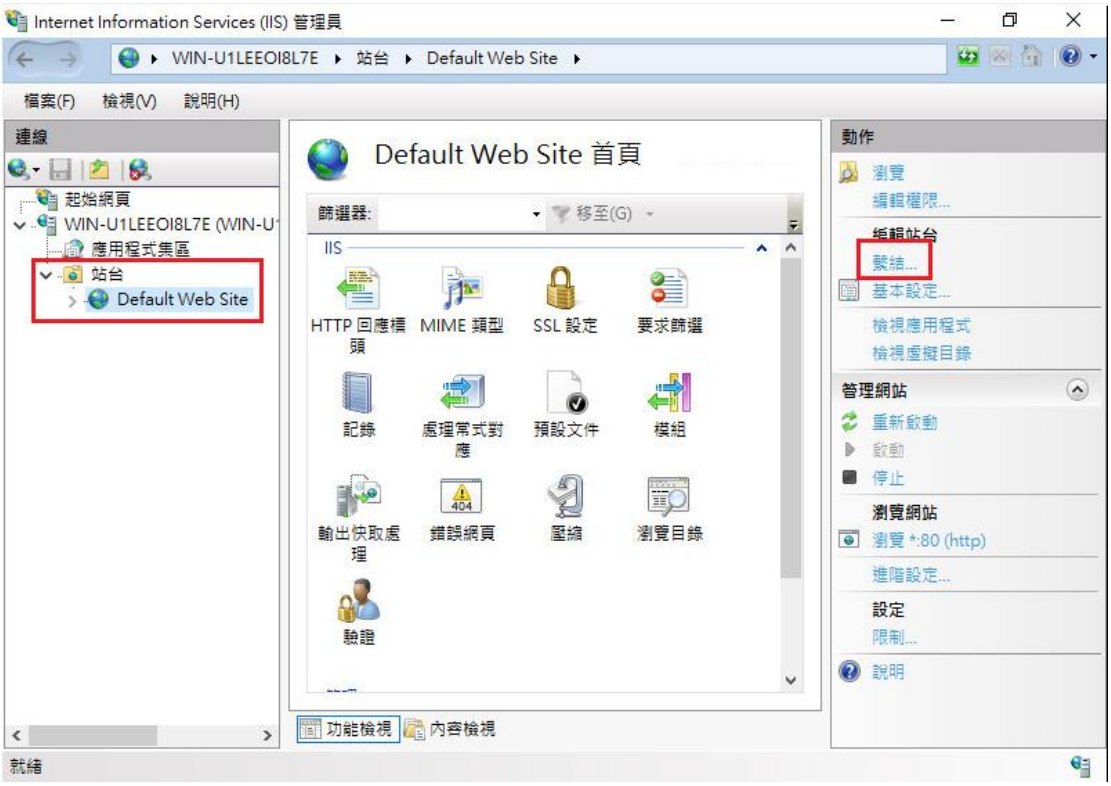


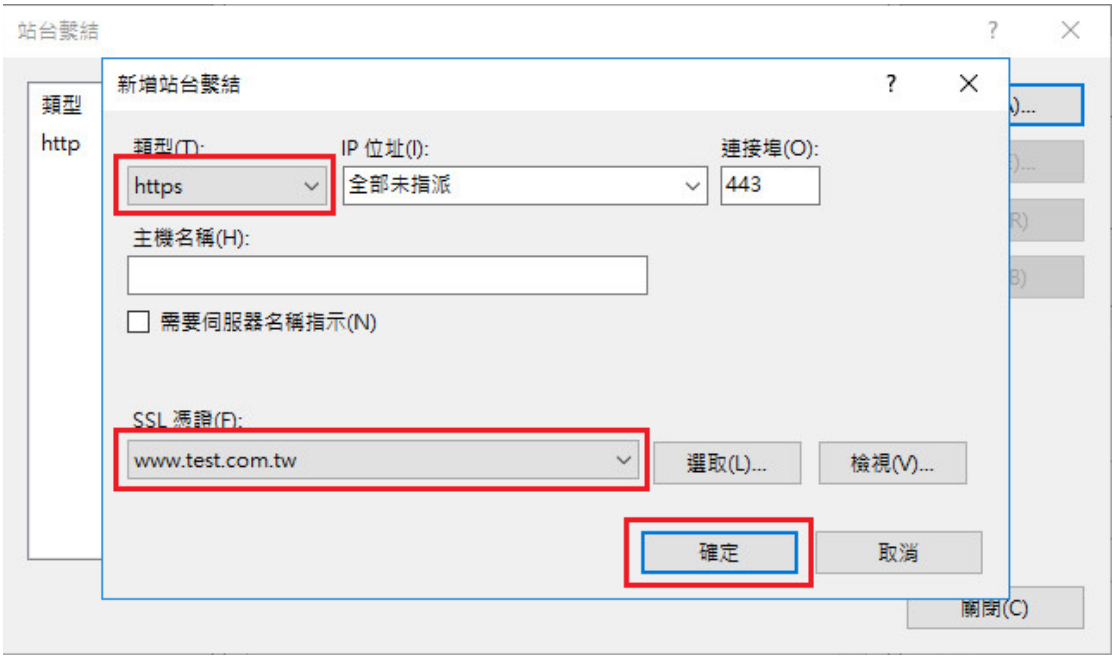
成功匯入後，可以看到 eCA 的根憑證。



十四、檢查「受信任的根憑證授權單位」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。