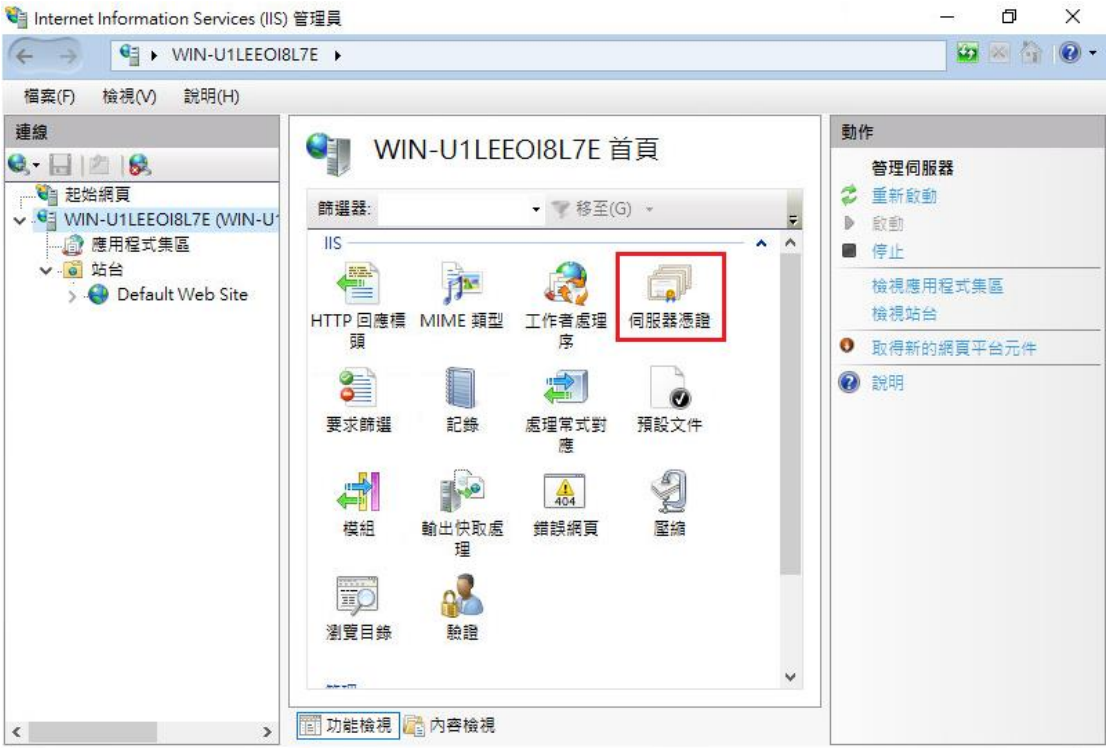
中華電信通用憑證管理中心（PublicCA）

Windows IIS 10.0 SSL 憑證請求檔製作與憑證安裝手冊

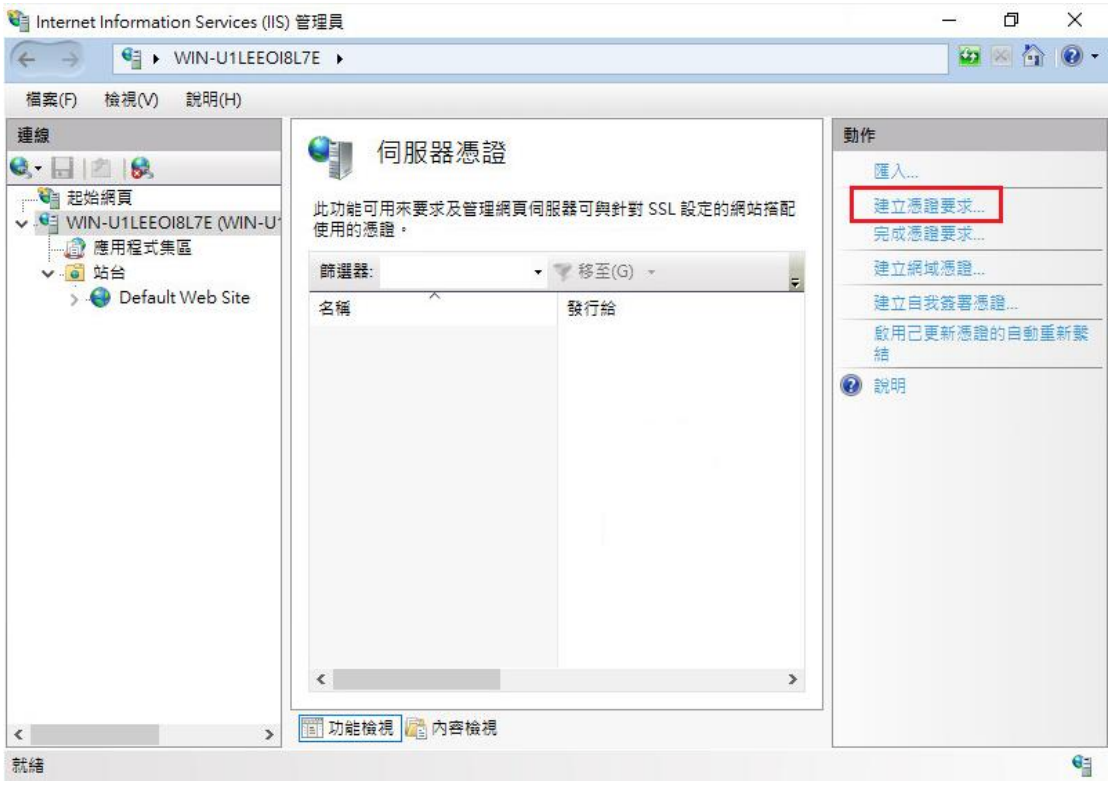
目錄

Windows IIS 10.0 SSL 憑證請求檔製作手冊

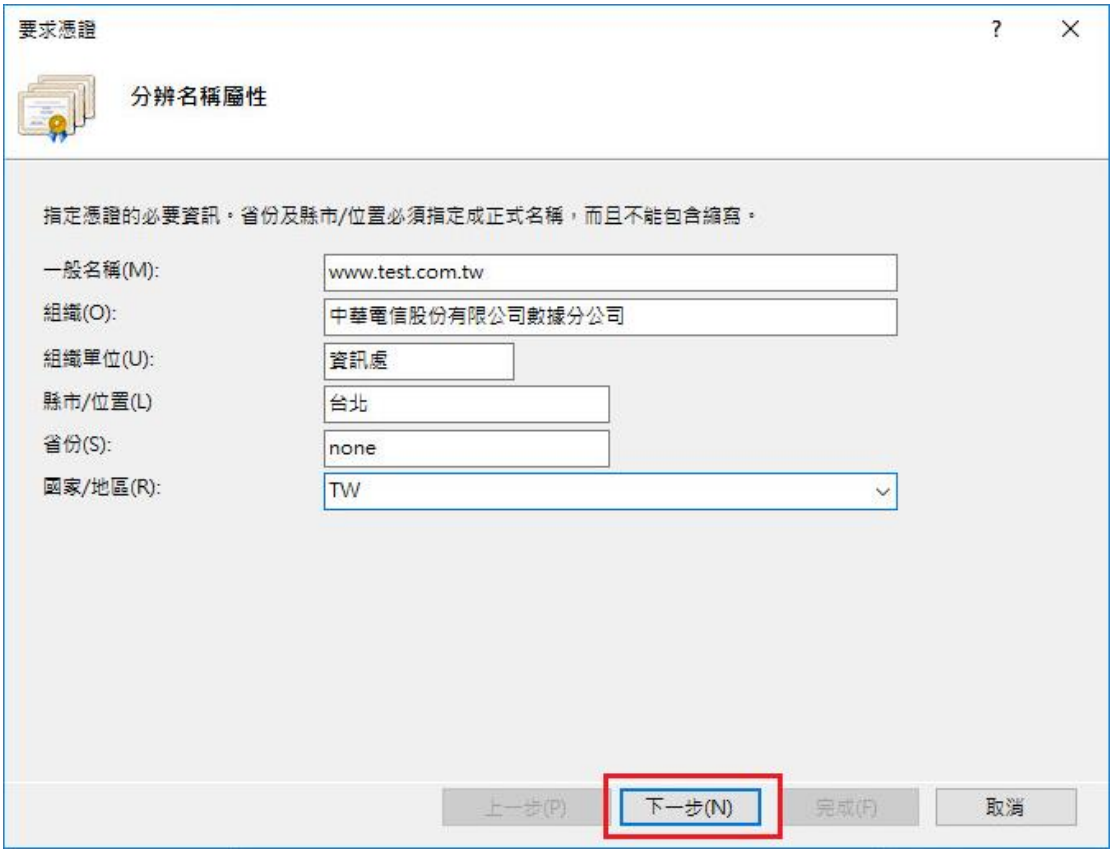
一、　開啟「Internet Information Services (IIS)管理員」並點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」兩下。



二、　點選「建立憑證要求」



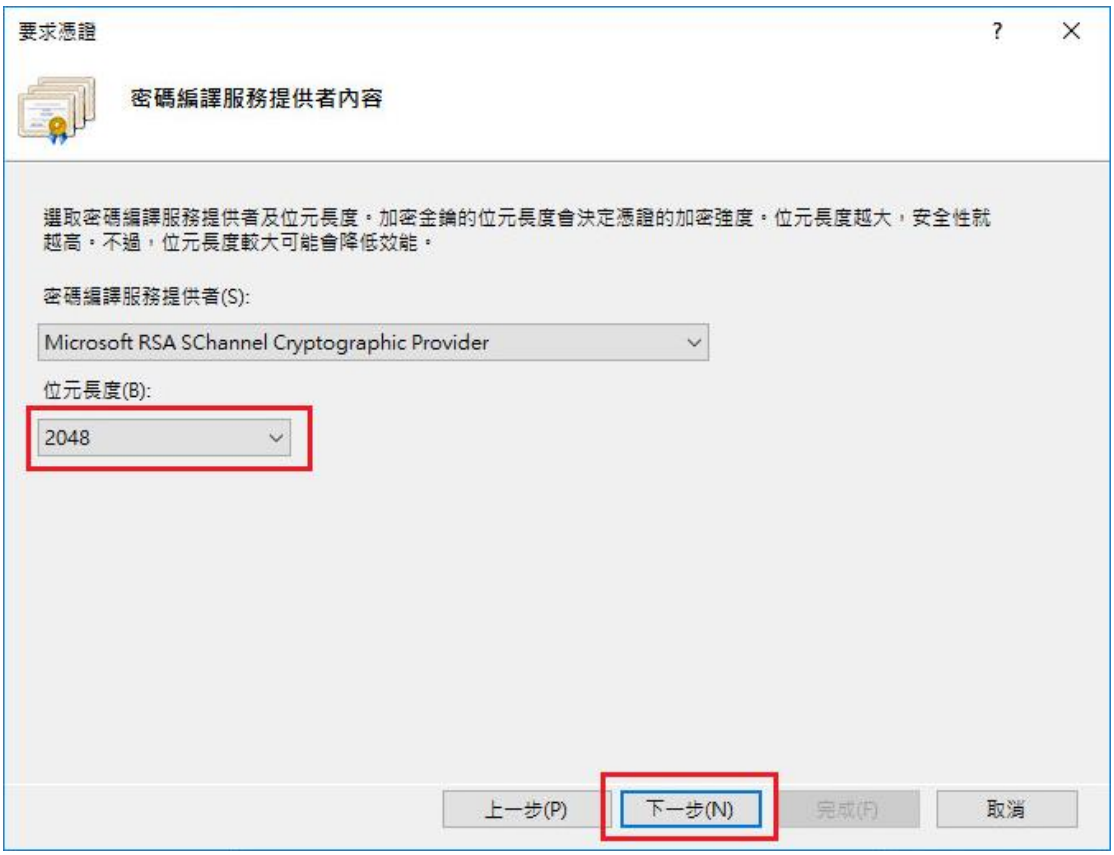
三、　輸入以下所有欄位資料，輸入完成後請點選「下一步」



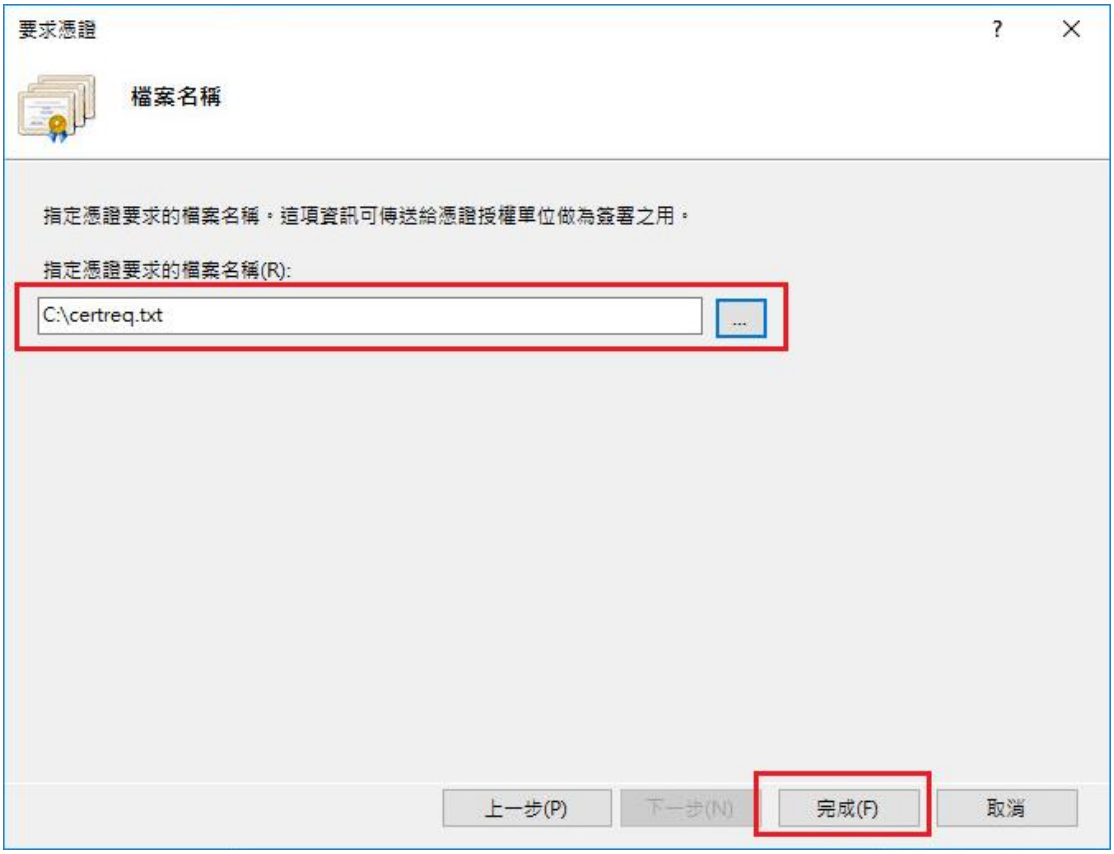
補充說明 1：中華電信通用憑證管理中心之程式會擷取憑證請求檔中的公

開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

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。請注意依照國際密碼學趨勢，請使用 RSA 2048 位元(含)以上金鑰長度。



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」。此時憑證請求檔製作完成，使用憑證請求檔至中華電信通用憑證管理中心申請 SSL 憑證。



六、　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（https://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。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔（產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

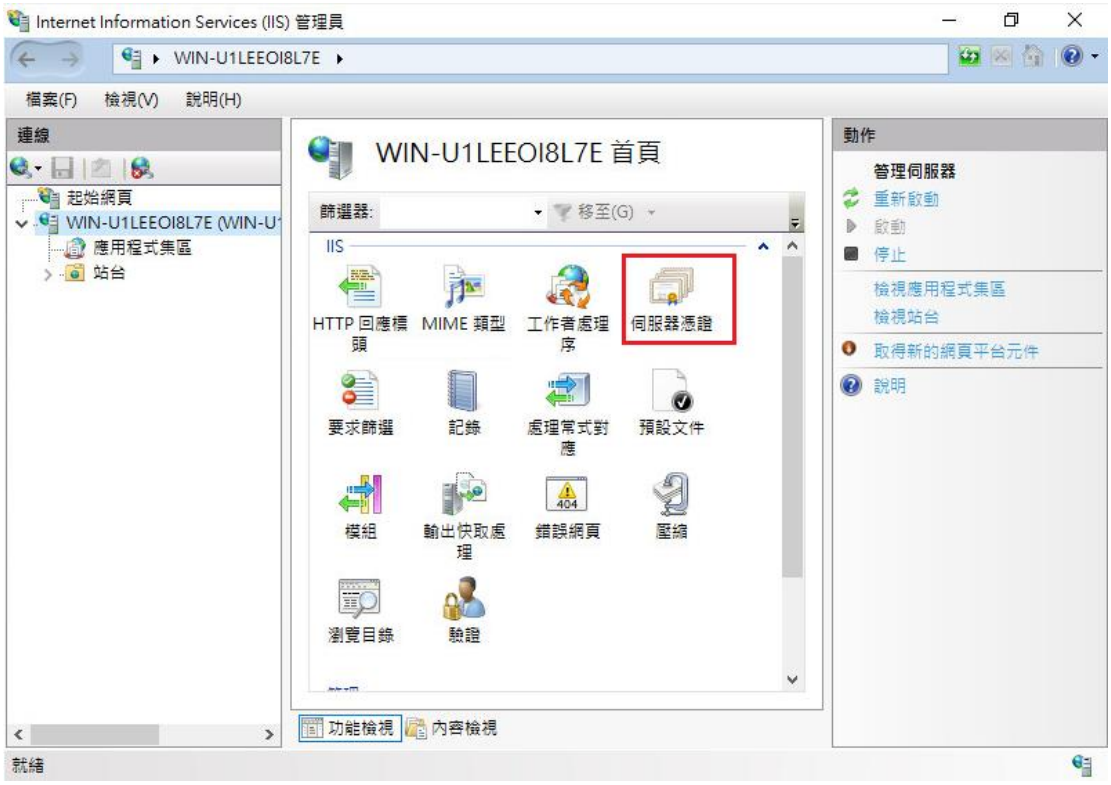
Windows IIS 10.0　SSL 憑證安裝操作手冊

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：

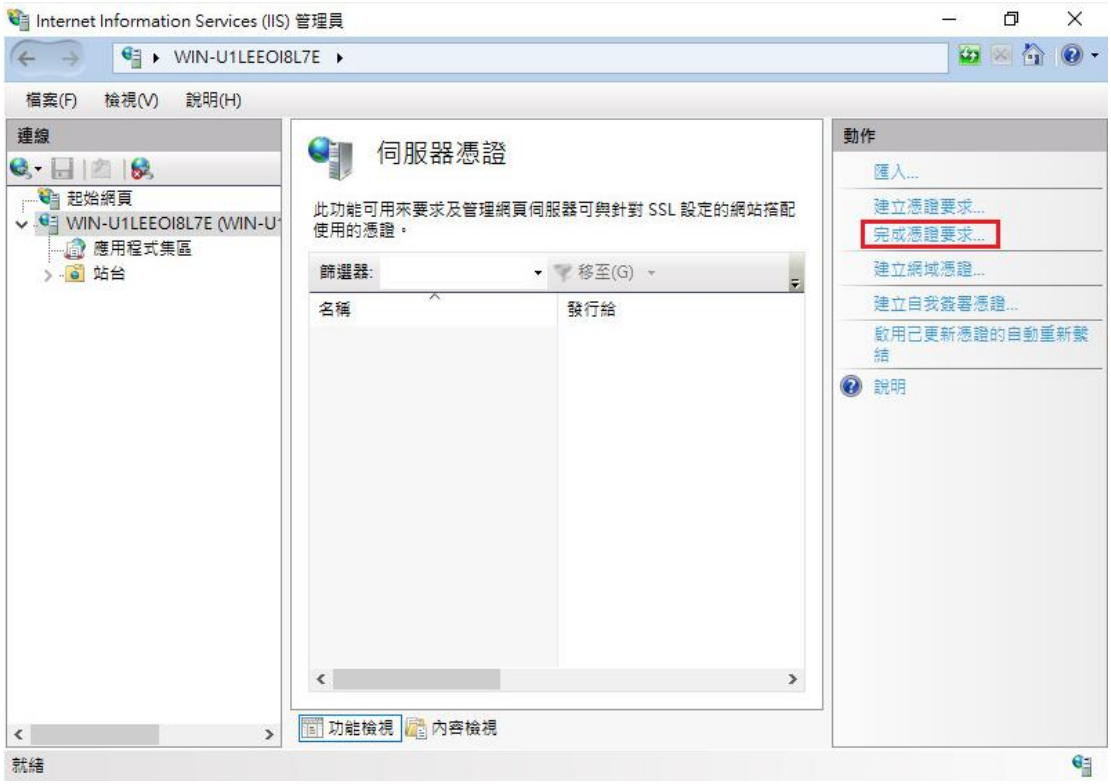
1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。
2. 從網站查詢與下載：
   eCA 憑證：
   http://epki.com.tw/download/ROOTeCA_64.crt
   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、　有關國際間已淘汰 SHA-1 SSL 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)

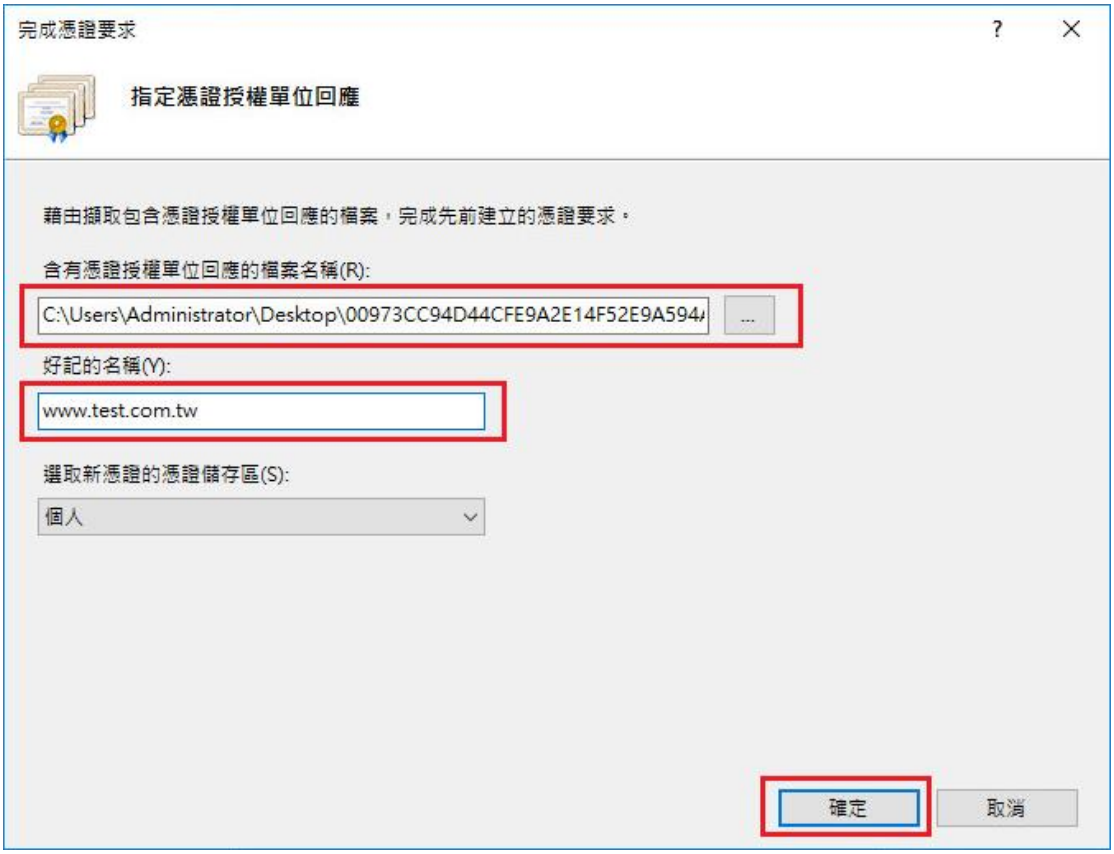
三、　開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



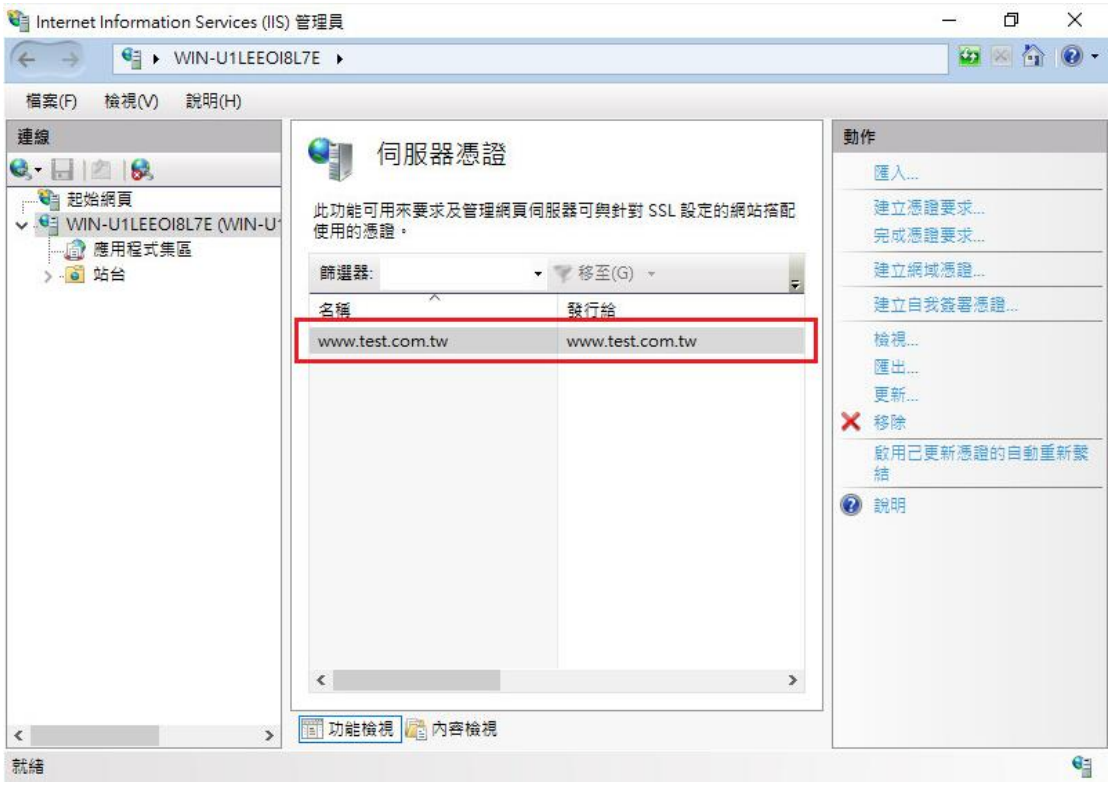
四、 點選「完成憑證要求」。



五、 如下圖，選擇存放由中華電信通用憑證管理中心所簽發之 SSL 憑證的位置，並輸入好記名稱(一般填寫 Domain Name)。

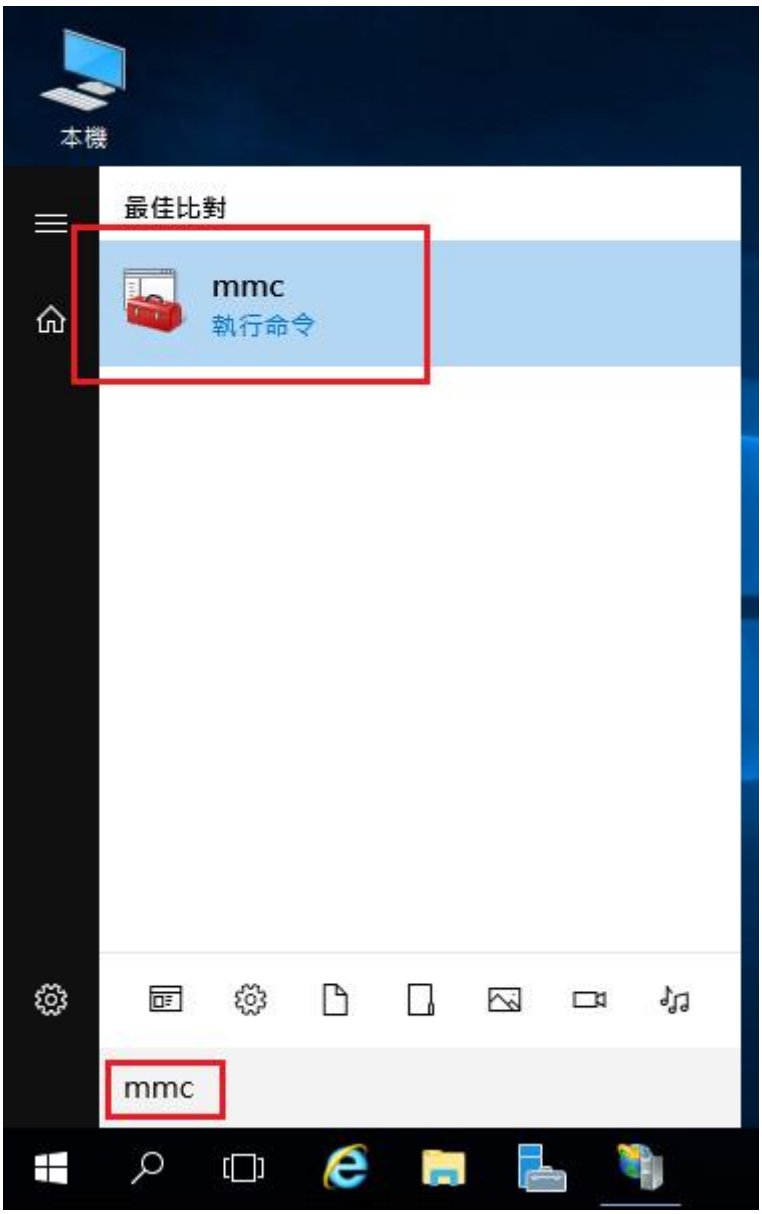


六、　步驟 4 按「確定」，出現完成憑證要求的畫面。

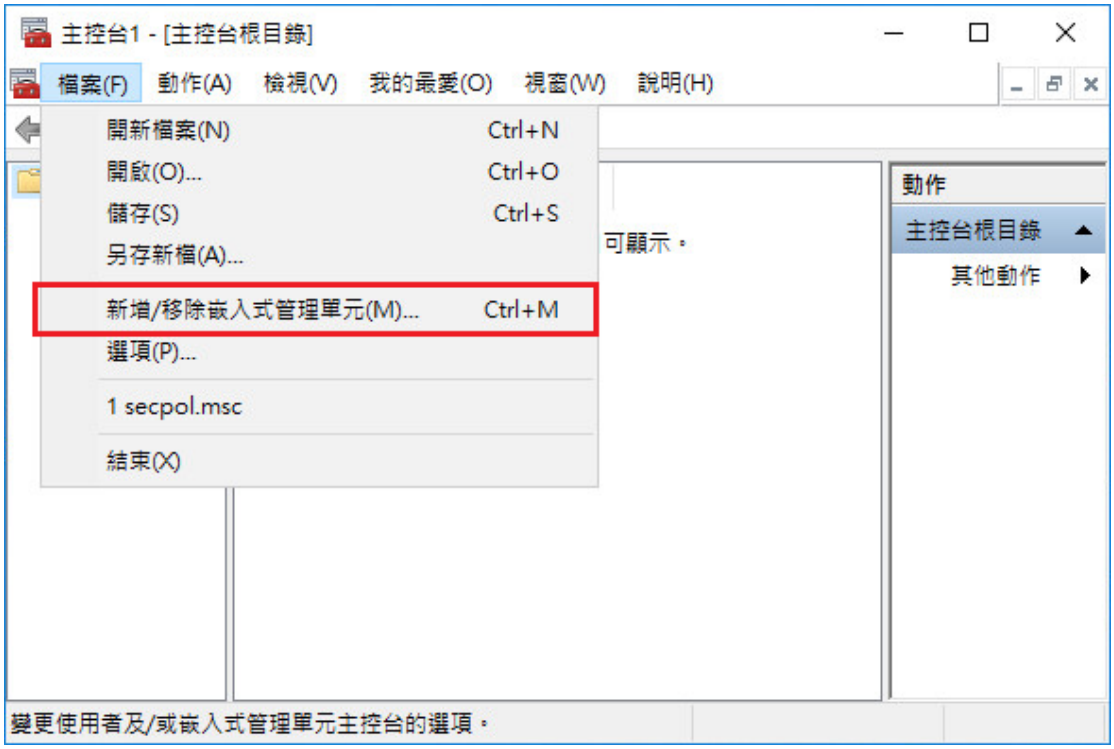


七、　接著要安裝 eCA 及 PublicCA 憑證。

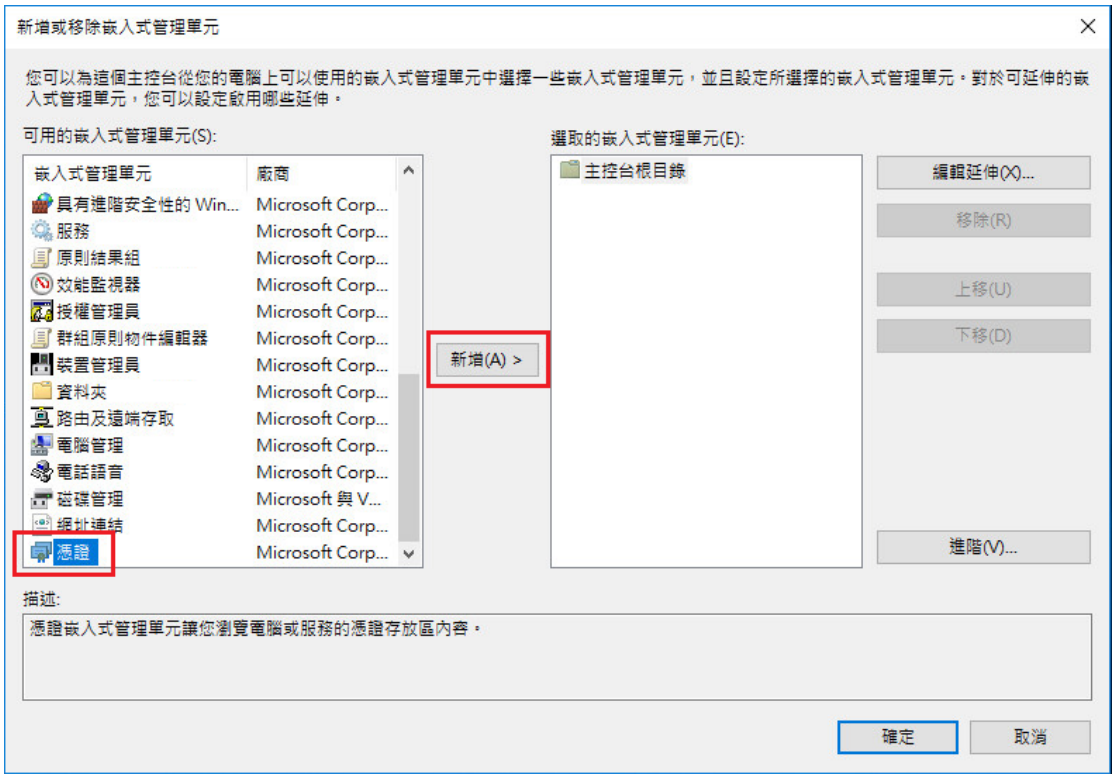
請先點選左下角的「Windows」圖示→輸入「mmc」→按下「Enter」。



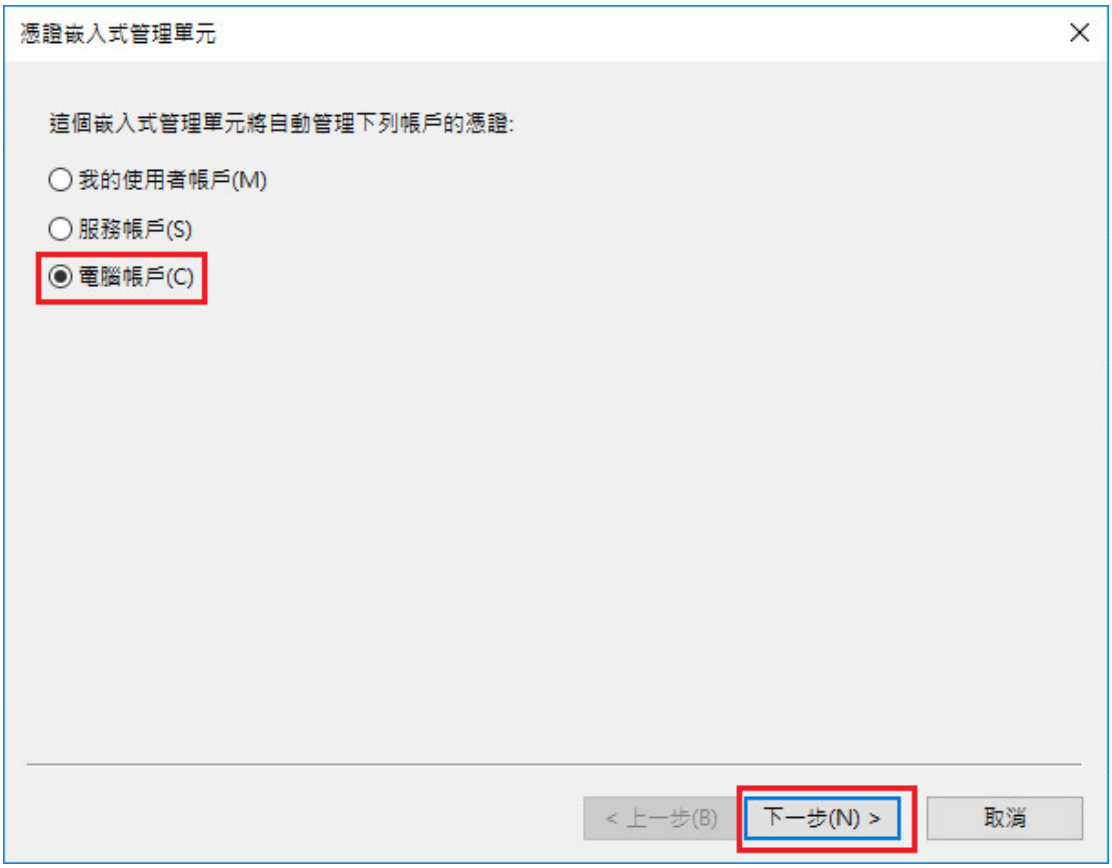
八、　　選擇「新增/移除嵌入式管理單元」。

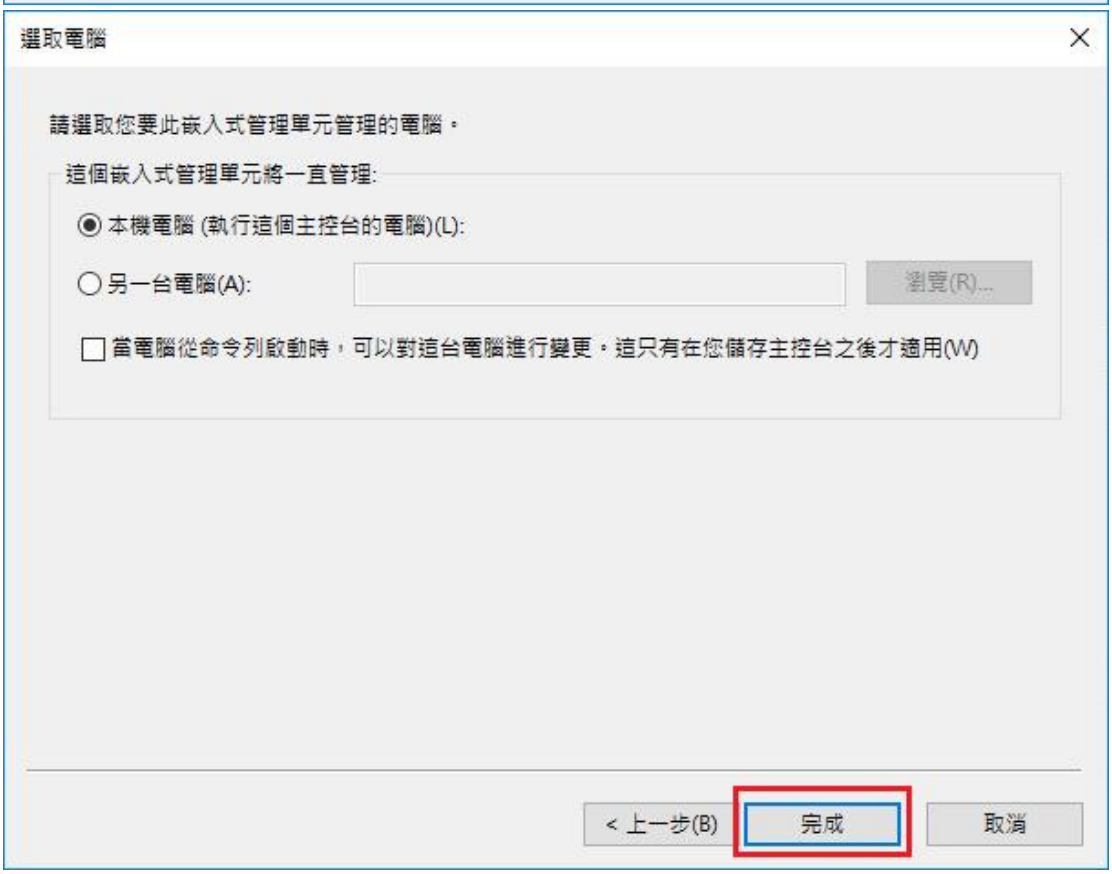


九、 接著點選「憑證」→「新增」。

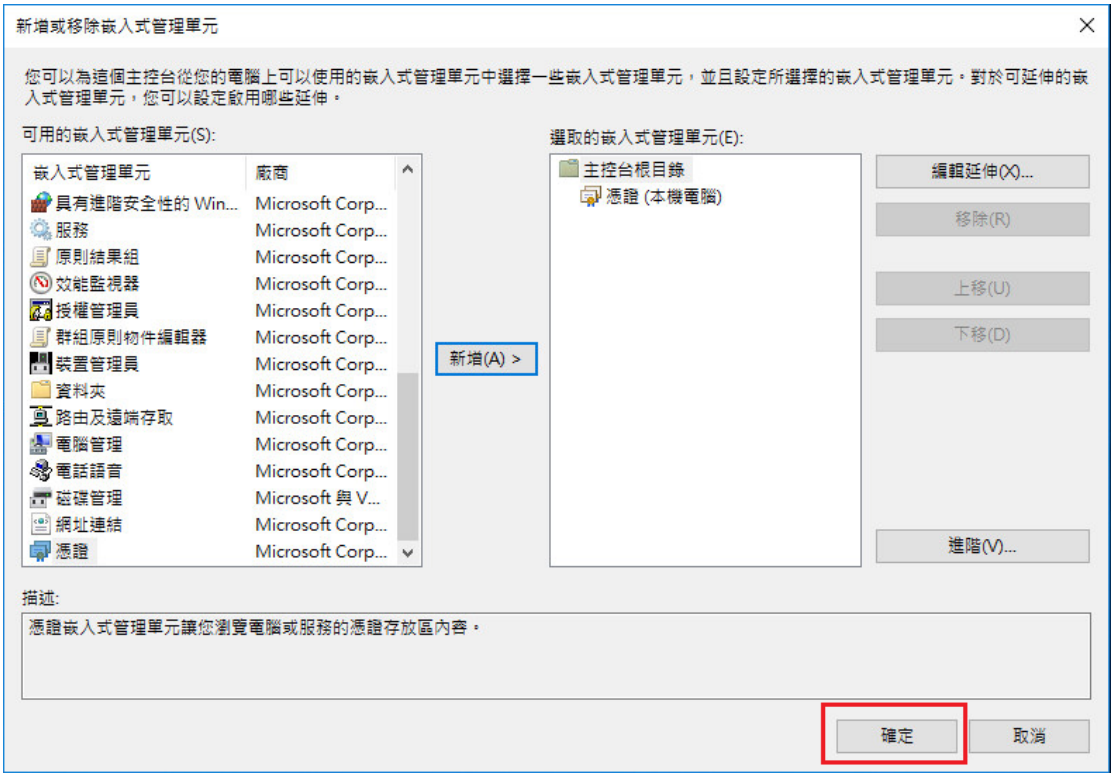


選擇「電腦帳戶」→「下一步」→「完成」。

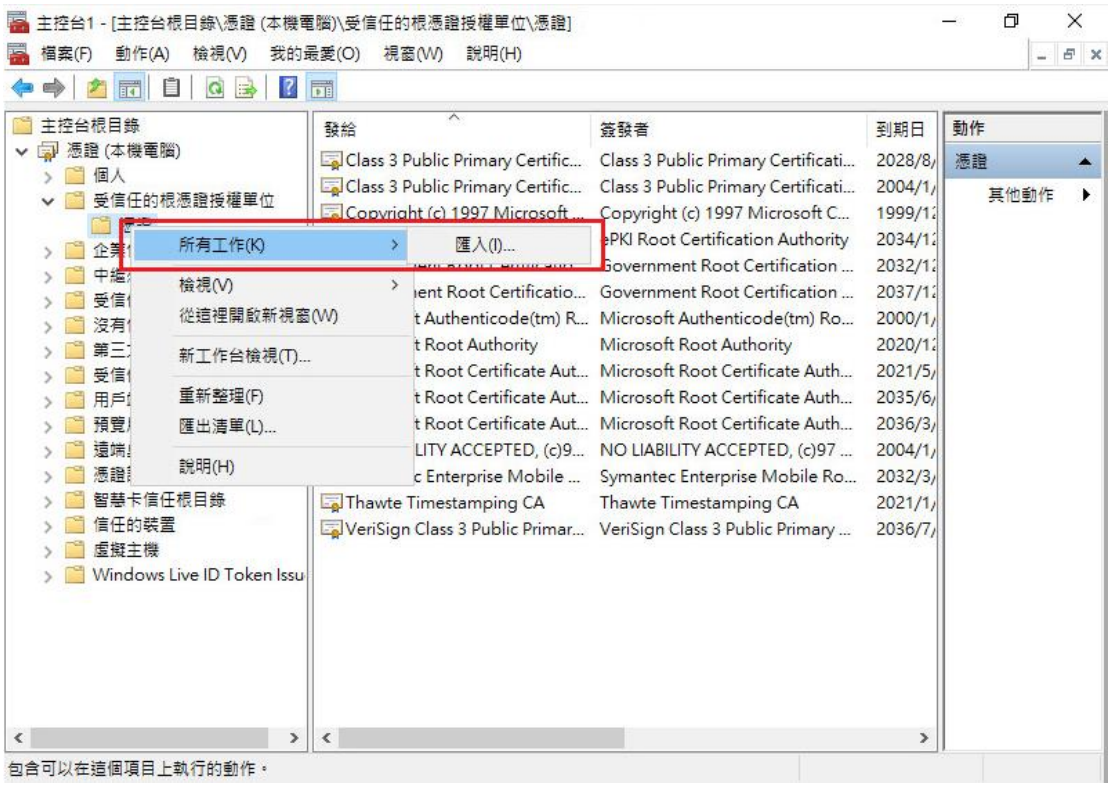

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


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

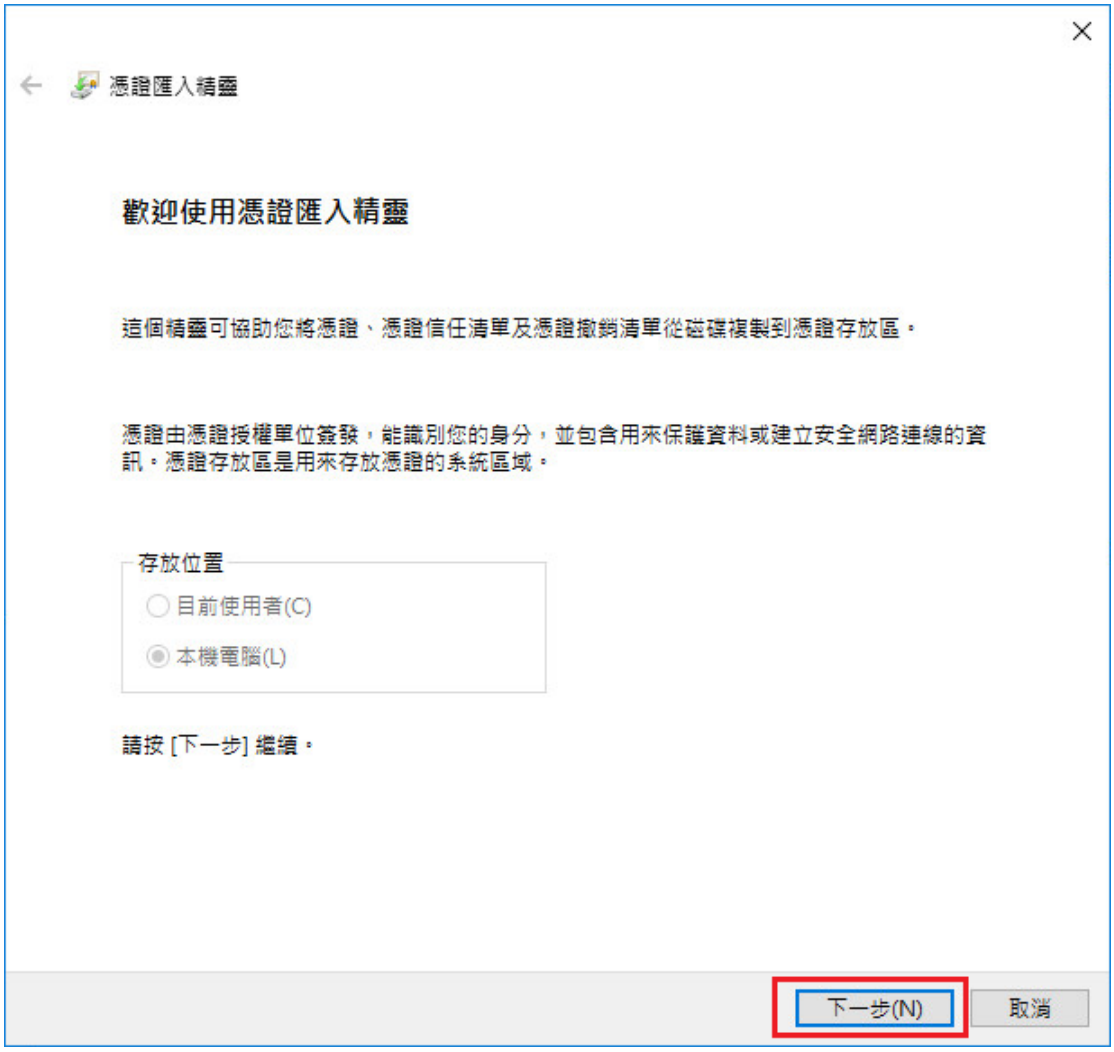
最後按下「確定」。

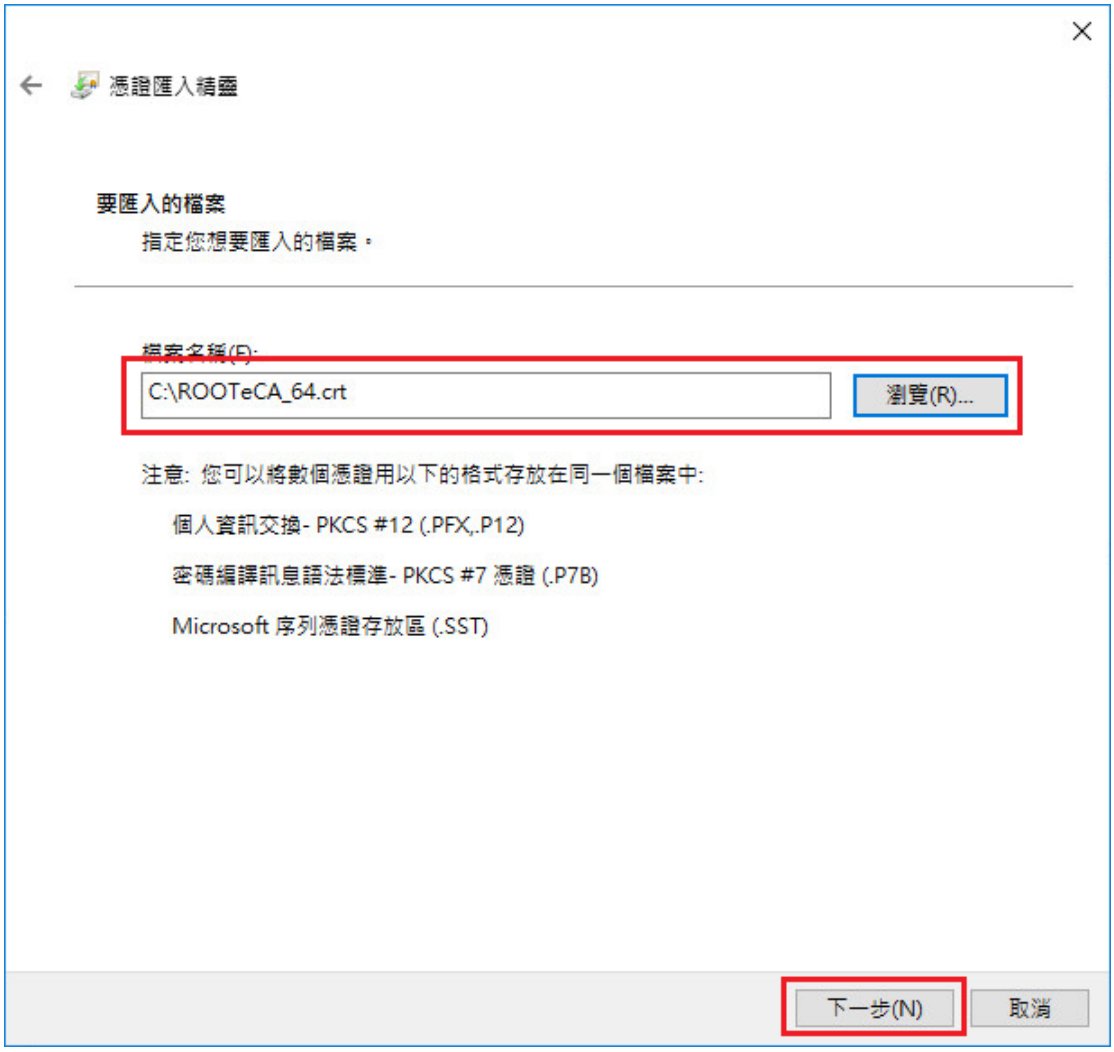


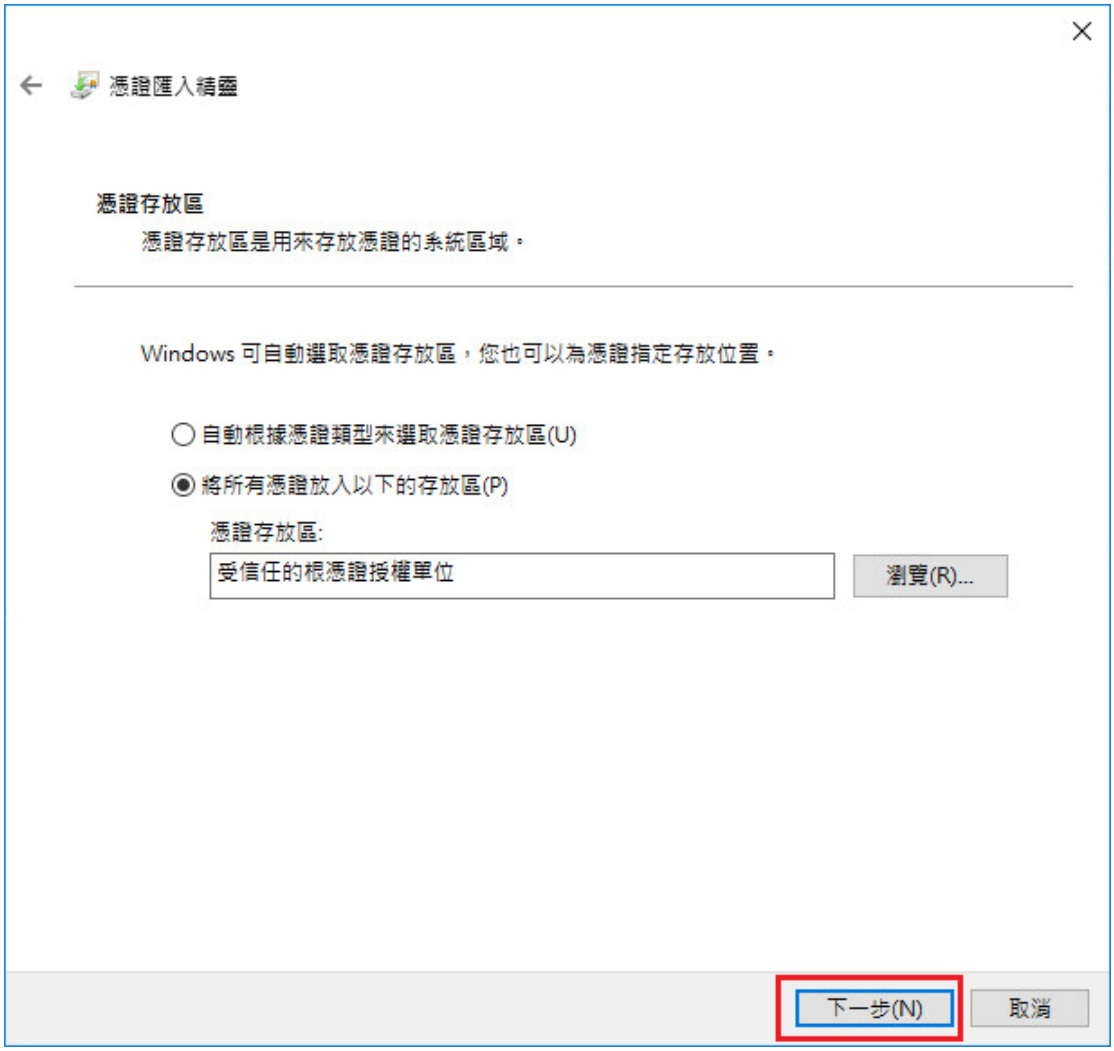
十、 **先匯入根憑證**。在「信任的根憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。

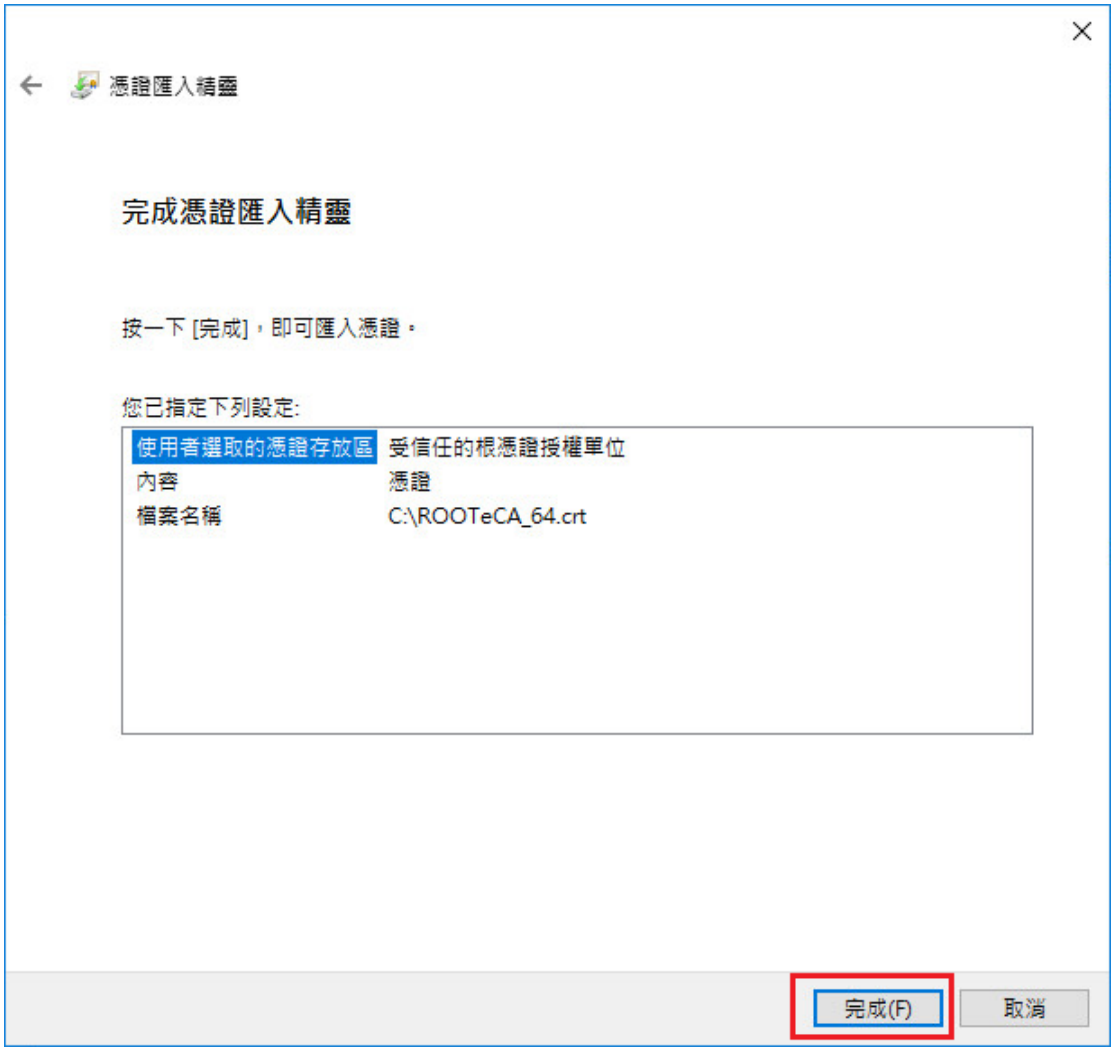


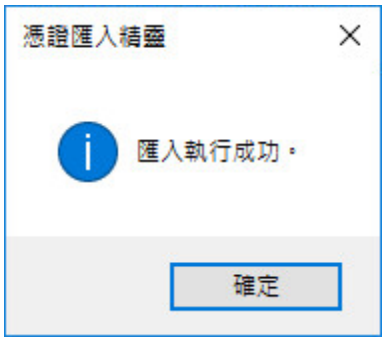
十一、 依照下圖步驟匯入根憑證。


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

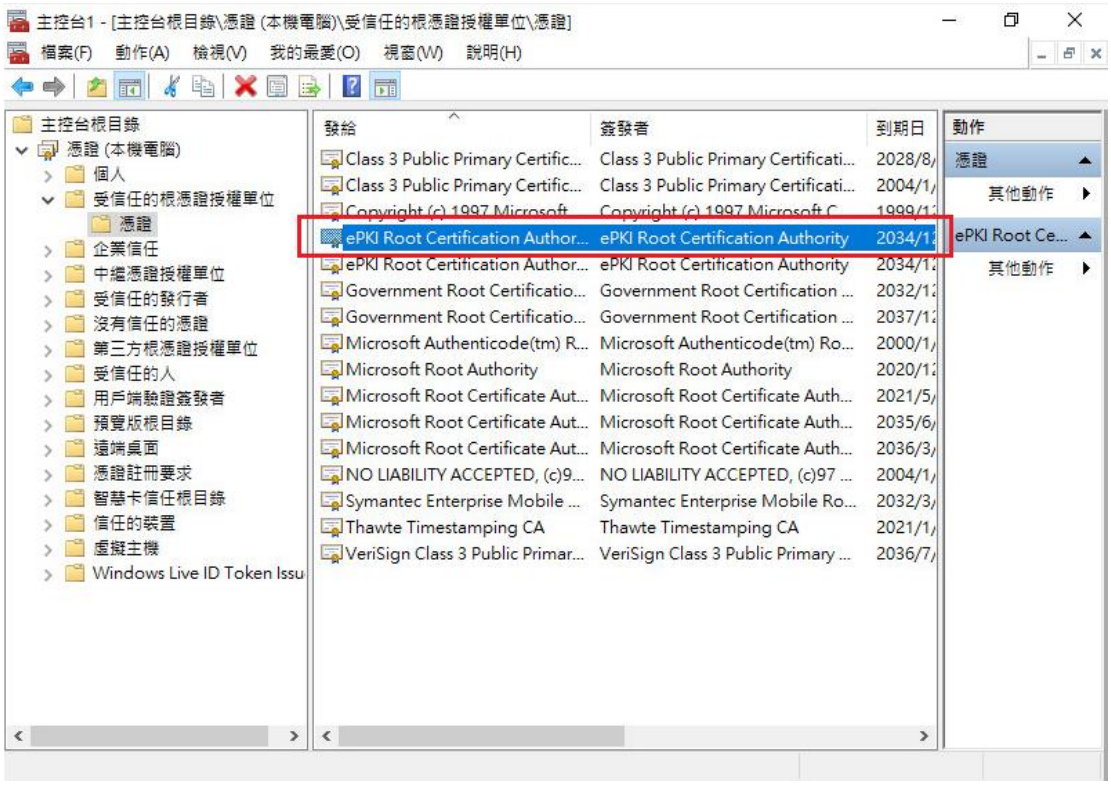

憑證匯入精靈
要匯入的檔案
指定您想要匯入的檔案。
檔案名稱(F):
C:\ROOTeCA_64.crt
瀏覽(R)...
注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)
Microsoft 序列憑證存放區 (.SST)
下一步(N)
取消


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:
受信任的根憑證授權單位
瀏覽(R)...
下一步(N)
取消

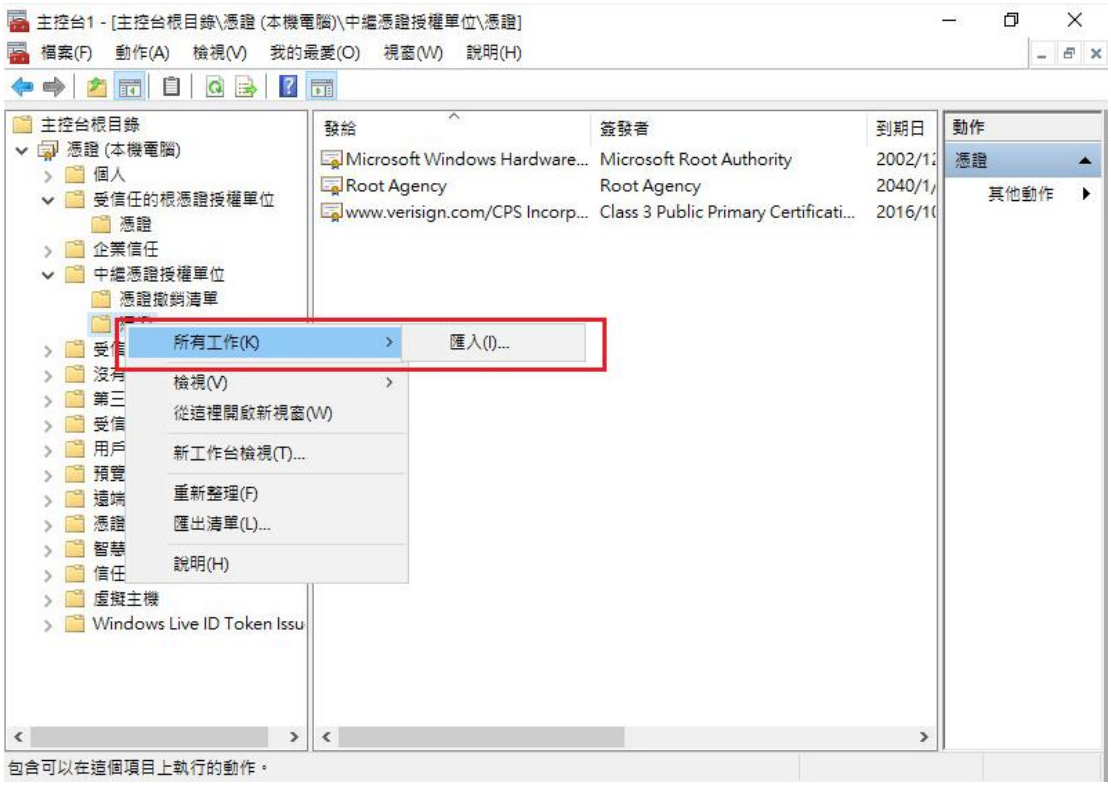




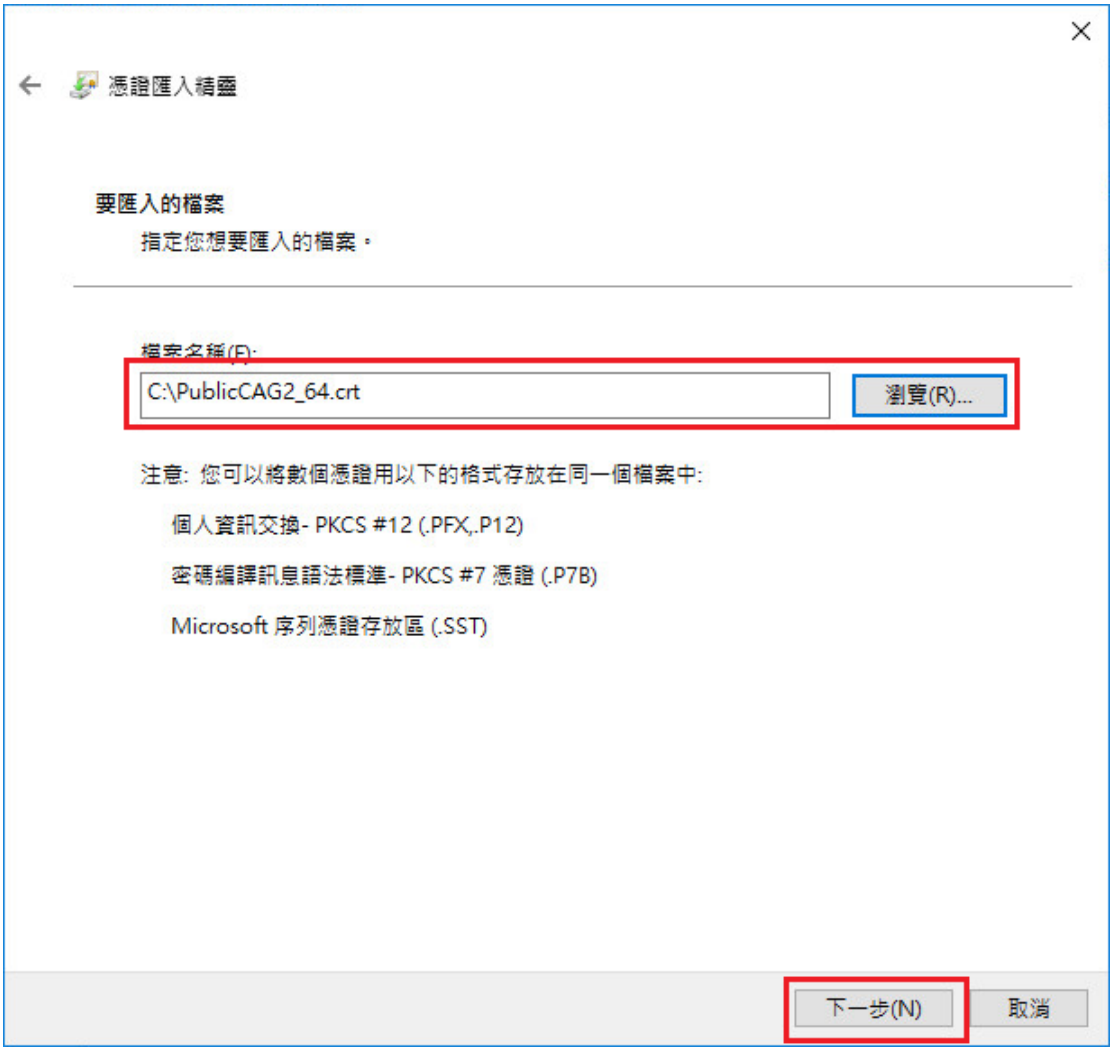
十二、　匯入成功後，可以看到 eCA 的根憑證。



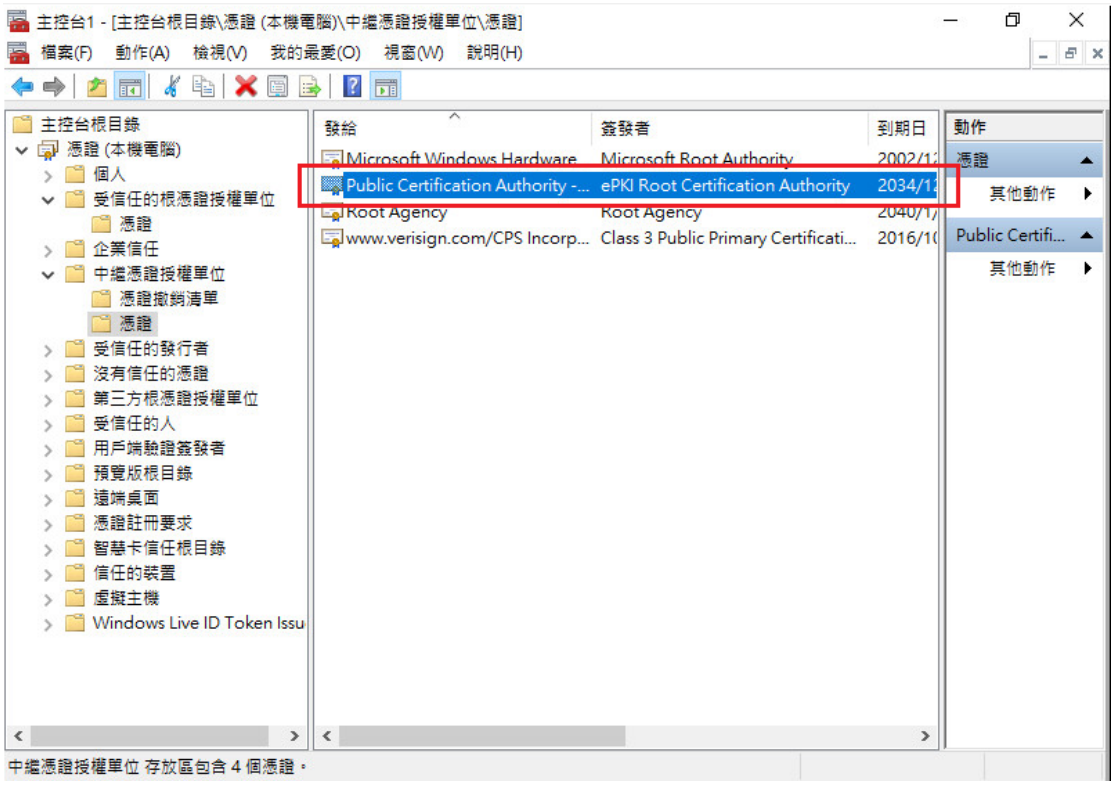
十三、 **第二步，匯入中繼憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



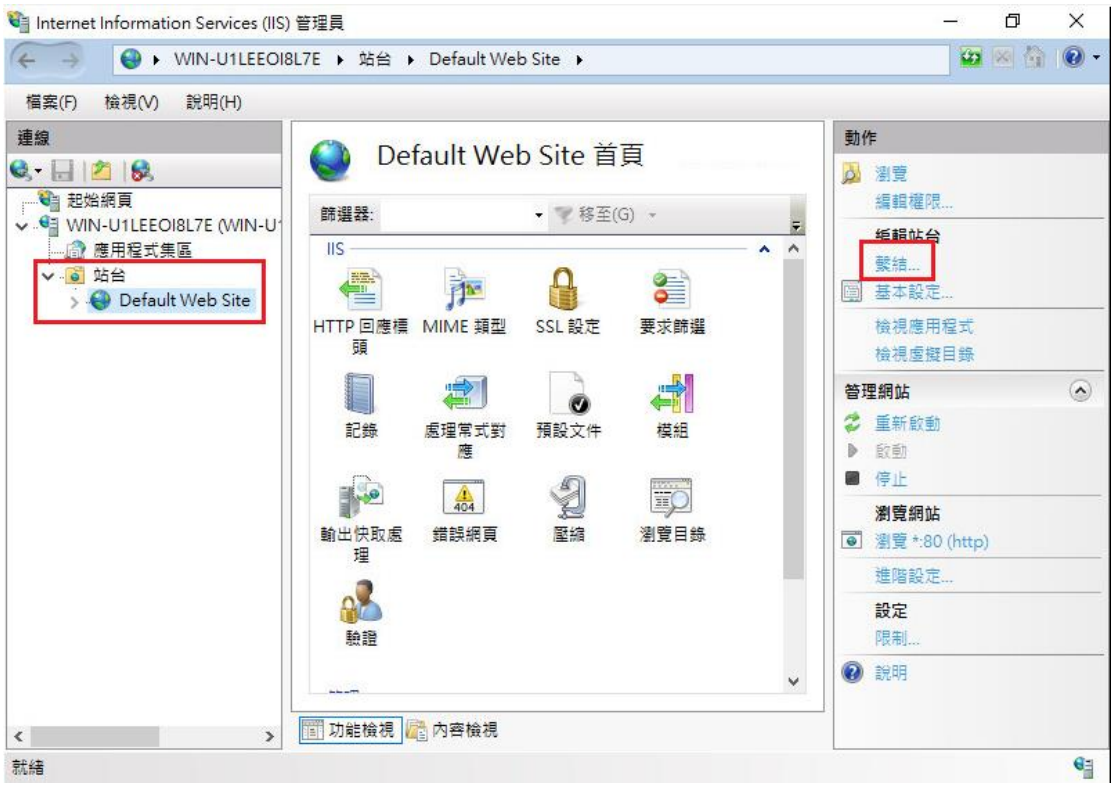
依照上述匯入 eCA 根憑證的步驟，匯入 PublicCA G2 中繼憑證。

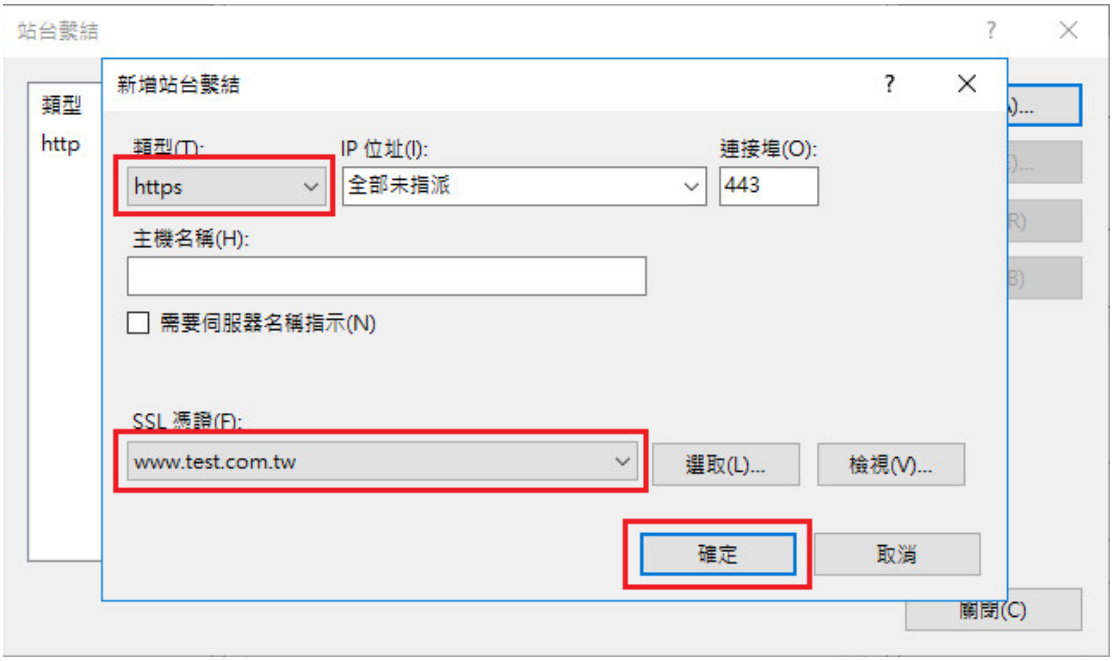


成功匯入後，可以看到 PublicCA G2 的中繼憑證。



十四、 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。**

十六、 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的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 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。