

中華電信 HiPKI 憑證管理中心 (OVTLSCA)

Windows IIS 10.0 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，若因參考本手冊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

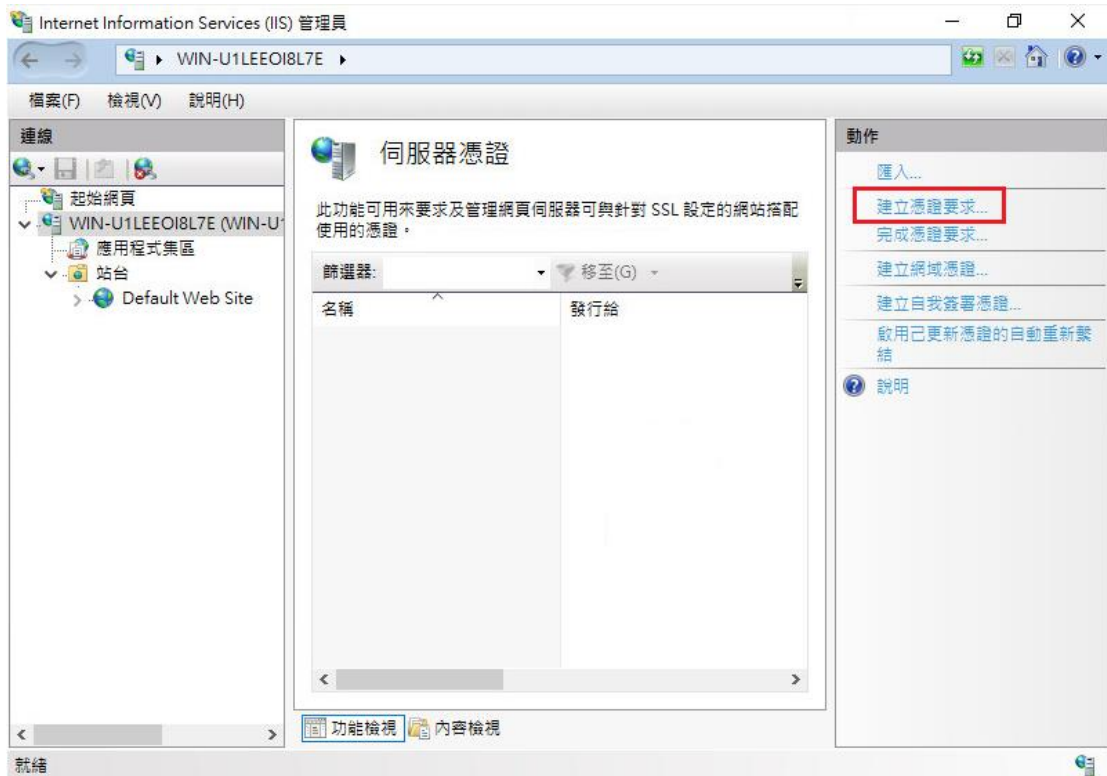
Windows IIS 10.0 SSL 憑證請求檔製作手冊.....	2
Windows IIS 10.0 SSL 憑證安裝操作手冊.....	6

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」

要求憑證

分辨名稱屬性

指定憑證的必要資訊，省份及縣市/位置必須指定成正式名稱，而且不能包含縮寫。

一般名稱(M):

組織(O):

組織單位(U):

縣市/位置(L):

省份(S):

國家/地區(R):

上一步(P) **下一步(N)** 完成(F) 取消

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。

The screenshot shows a dialog box titled "要求憑證" (Require Certificate) with a subtitle "密碼編譯服務提供者內容" (Password Translation Service Provider Content). The main text reads: "選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度越大，安全性就越高。不過，位元長度較大可能會降低效能。" (Select a password translation service provider and bit length. The bit length of the encryption key will determine the encryption strength of the certificate. The larger the bit length, the higher the security. However, a larger bit length may reduce performance.)

Below the text, there are two dropdown menus:

- "密碼編譯服務提供者(S):" (Password Translation Service Provider(S)): Microsoft RSA SChannel Cryptographic Provider
- "位元長度(B):" (Bit Length(B)): 2048

At the bottom, there are four buttons: "上一步(P)" (Previous), "下一步(N)" (Next), "完成(F)" (Finish), and "取消" (Cancel). The "下一步(N)" button is highlighted with a red box.

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」。

The screenshot shows the same dialog box, now at the "檔案名稱" (File Name) step. The main text reads: "指定憑證要求的檔案名稱。這項資訊可傳送給憑證授權單位做為簽署之用。" (Specify the file name for the certificate request. This information can be sent to the certificate authority for signing.)

Below the text, there is a text input field labeled "指定憑證要求的檔案名稱(R):" (Specify the file name for the certificate request(R):) containing the text "C:\certreq.txt". To the right of the input field is a button with three dots "...".

At the bottom, there are four buttons: "上一步(P)" (Previous), "下一步(N)" (Next), "完成(F)" (Finish), and "取消" (Cancel). The "完成(F)" button is highlighted with a red box.

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公開金鑰基礎建設服務網站 (<https://chtca.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 1: 中華電信公開金鑰基礎建設服務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]。

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 憑證串鍊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 4 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)eCA to HRCA 交互憑證(eCA 簽發給 HRCA 之交互憑證)、(3)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(4)OV TLS CA 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 4 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、eCA to HRCA 交互憑證(檔名為 eCA1-to-HRCA1.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.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 4 個檔案。

2. 從網站查詢與下載：

eCA 憑證：

https://eca.hinet.net/download/ROOTeCA_64.crt

eCA to HRCA 憑證：

<https://eca.hinet.net/download/eCA1-to-HRCA1.crt>

HiPKI OV TLS CA 憑證：

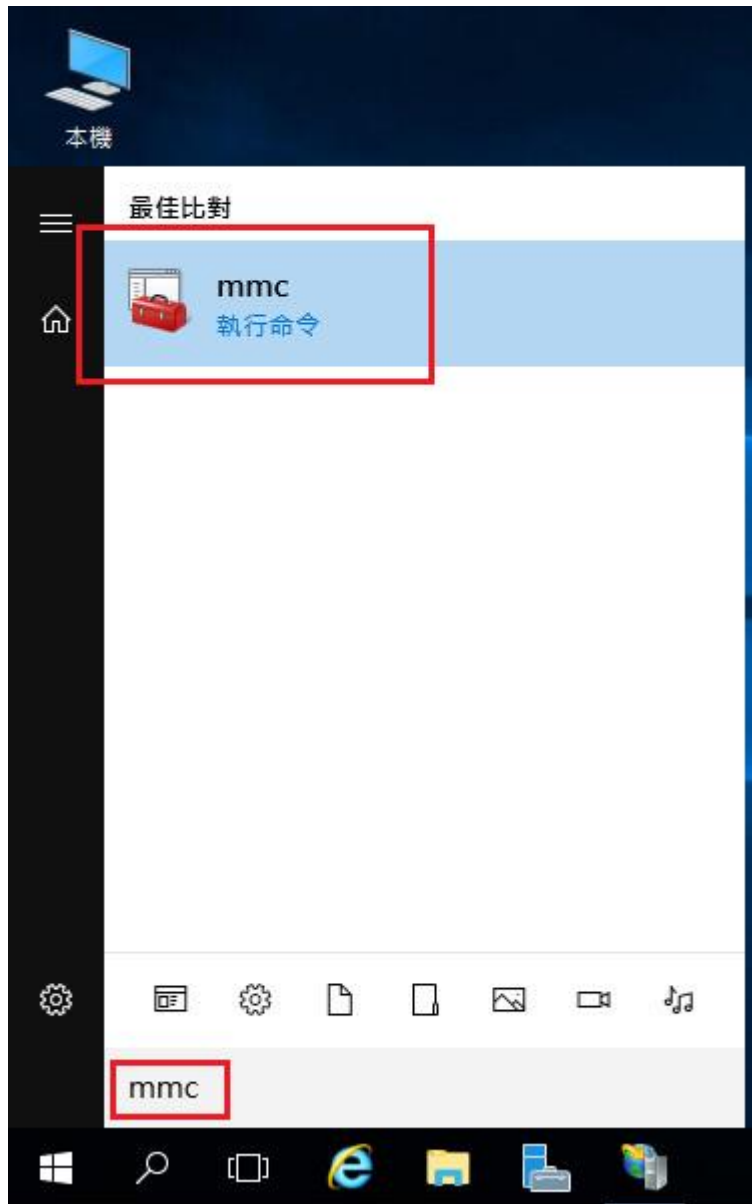
https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

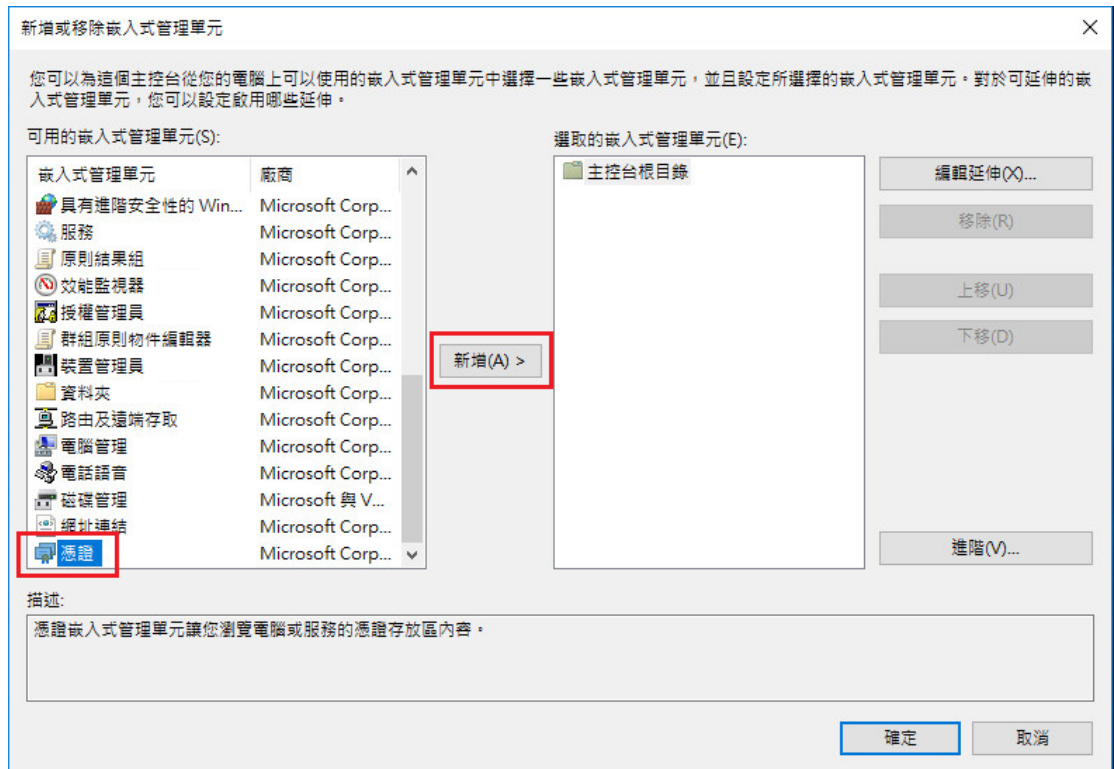
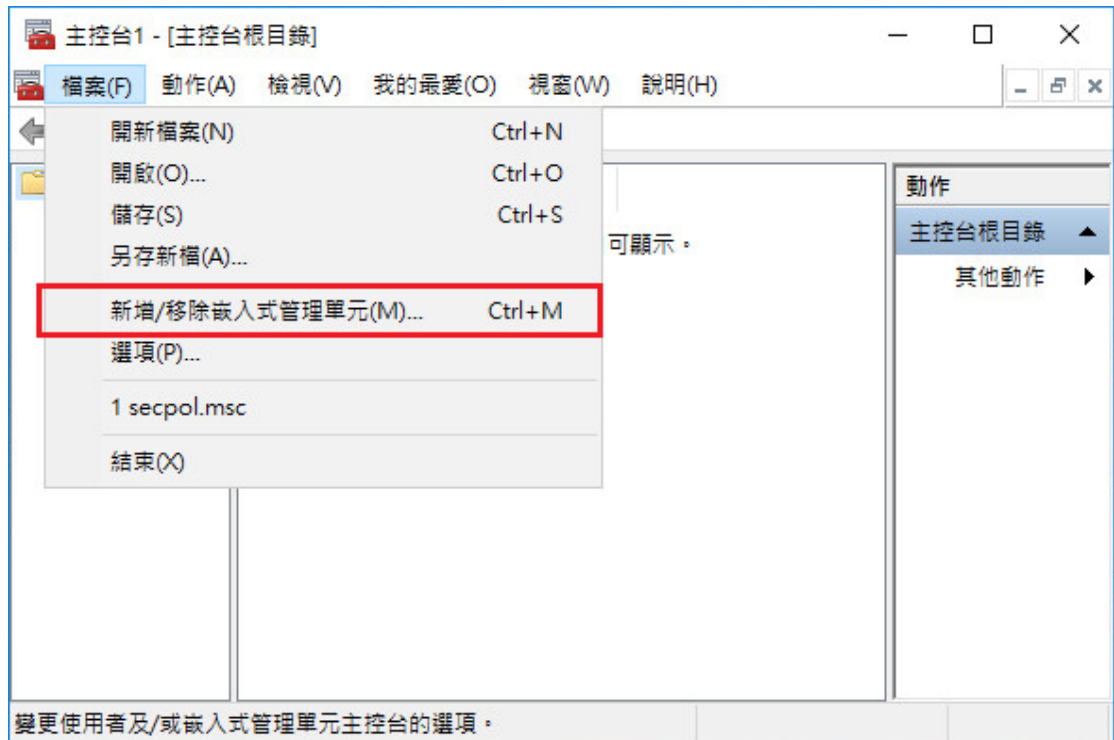
SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，進行 SSL 憑證下載。

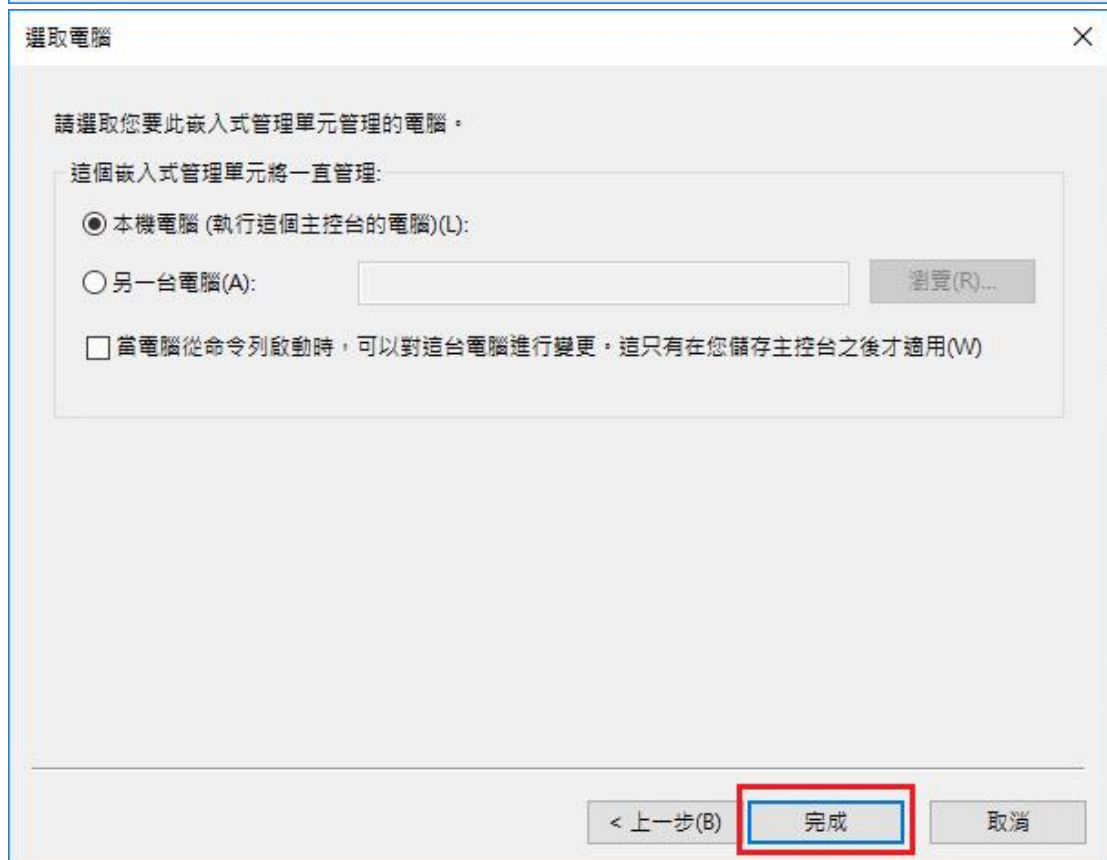
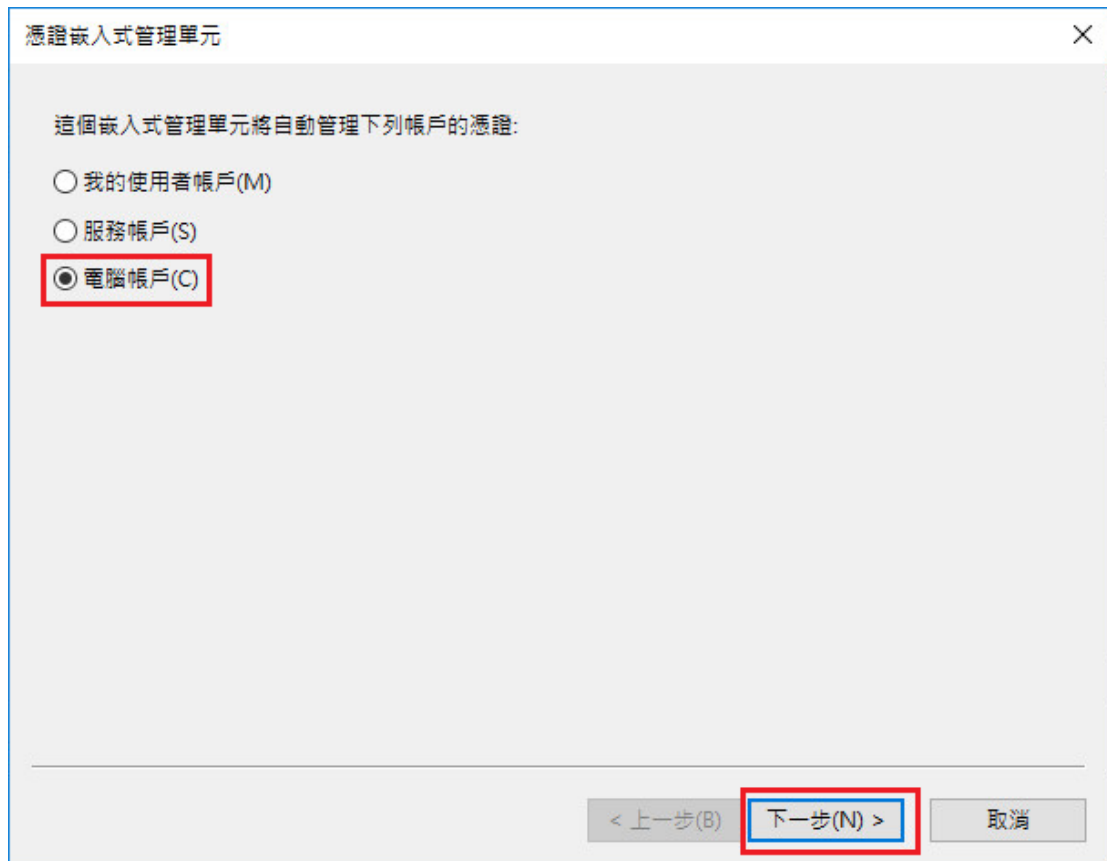
若您是中華電信之員工，負責管理單位之伺服器，請至 <https://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

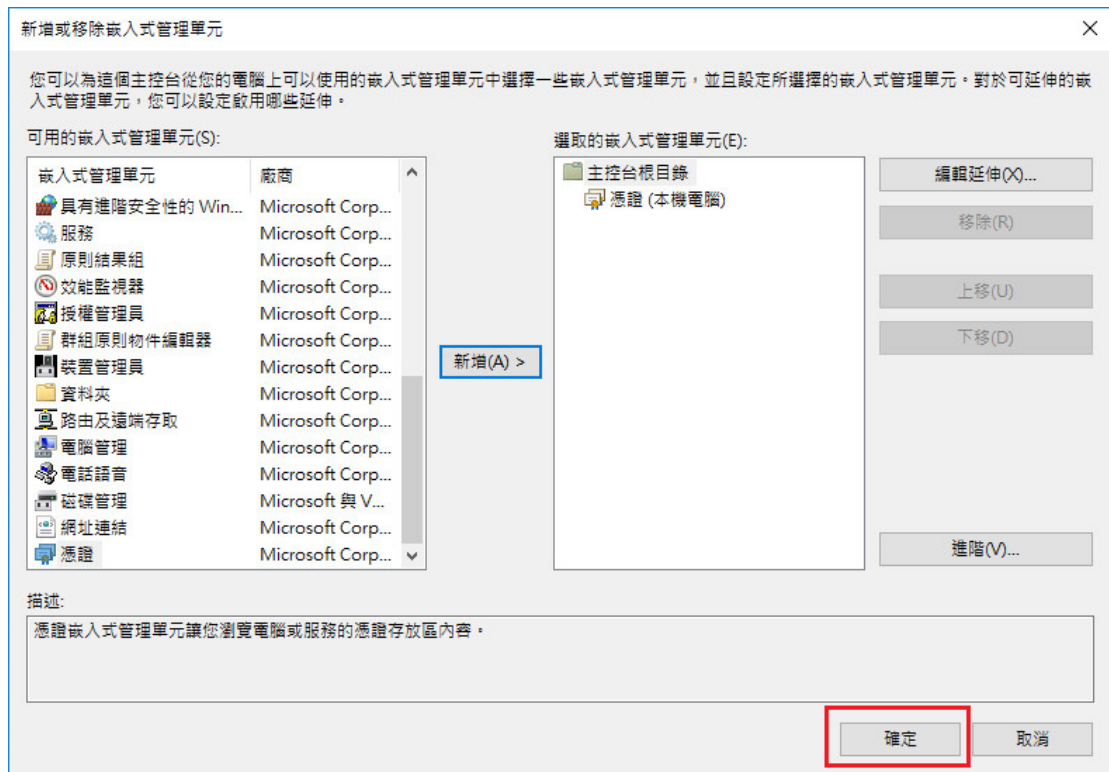
二、 開啟 mmc 安裝根憑證及中繼憑證。

點選「開始」→輸入「mmc」→點選「mmc.exe」，並依下圖操作。

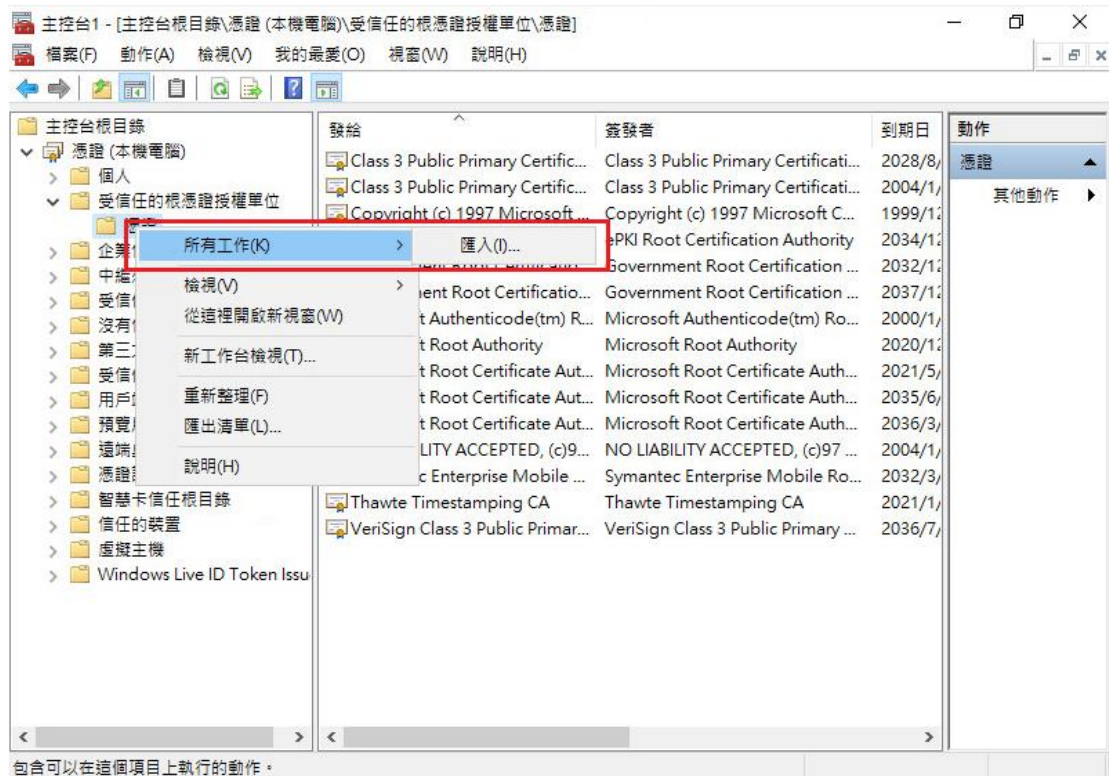






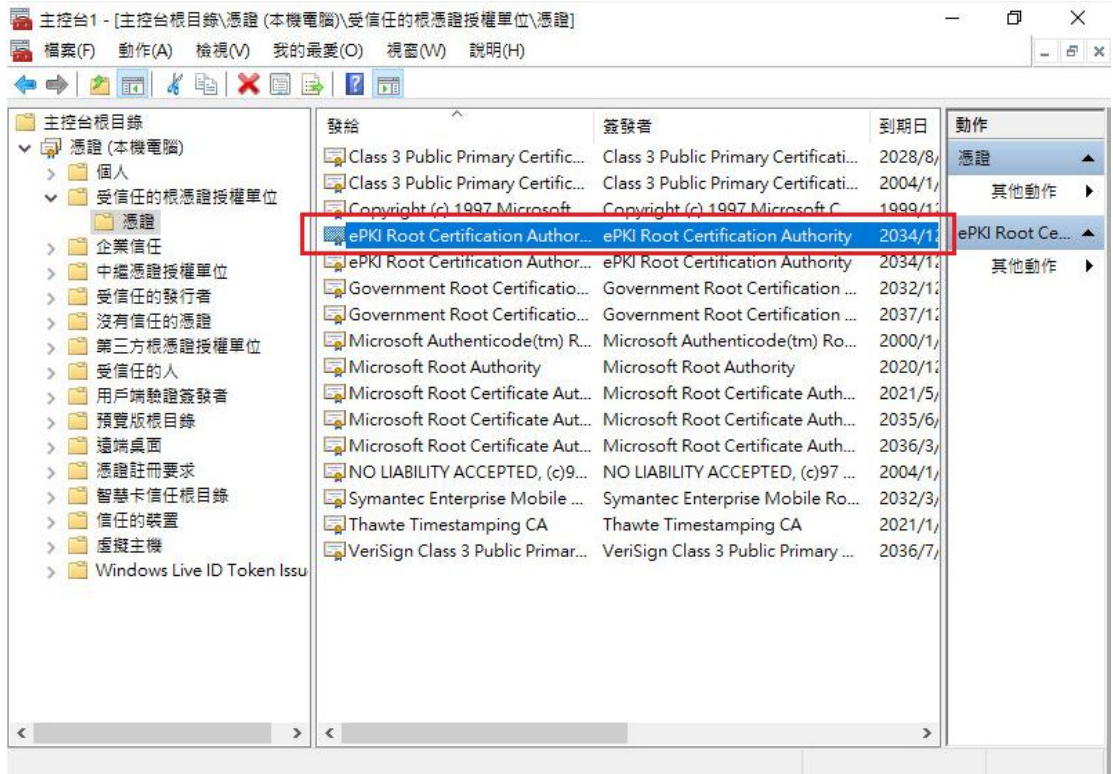
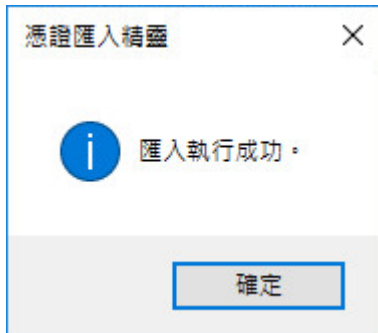


三、於「受信任的根憑證授權單位」匯入根憑證。

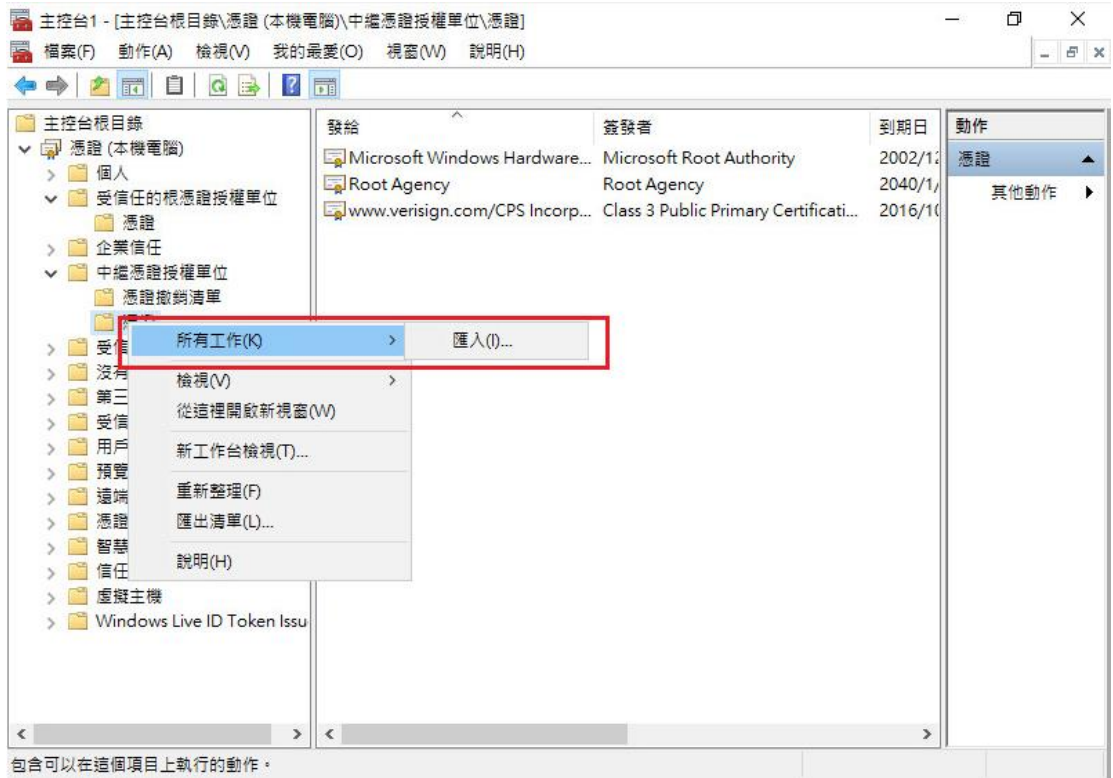








四、於「中繼憑證授權單位」匯入交互憑證。依照上述匯入根憑證的步驟，匯入交互憑證。



← 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:\eCA1-to-HRCA1.crt

瀏覽(B)...

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：

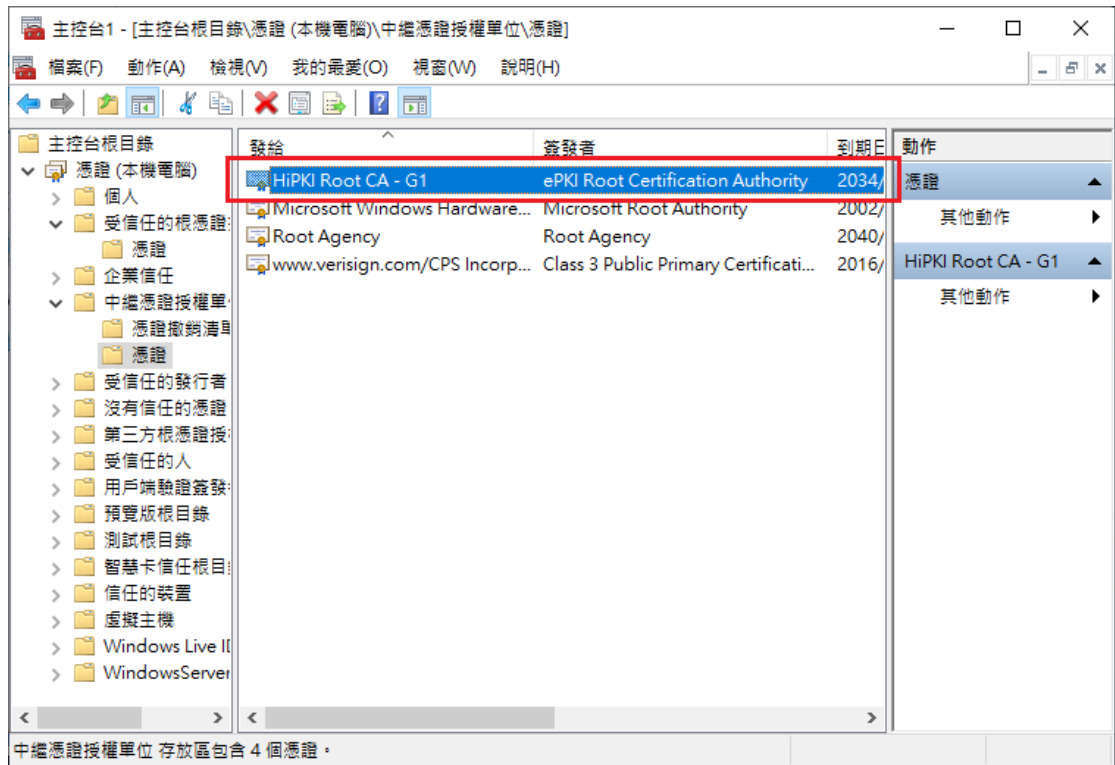
個人資訊交換- PKCS #12 (.PFX,.P12)

密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)

Microsoft 序列憑證存放區 (.SST)

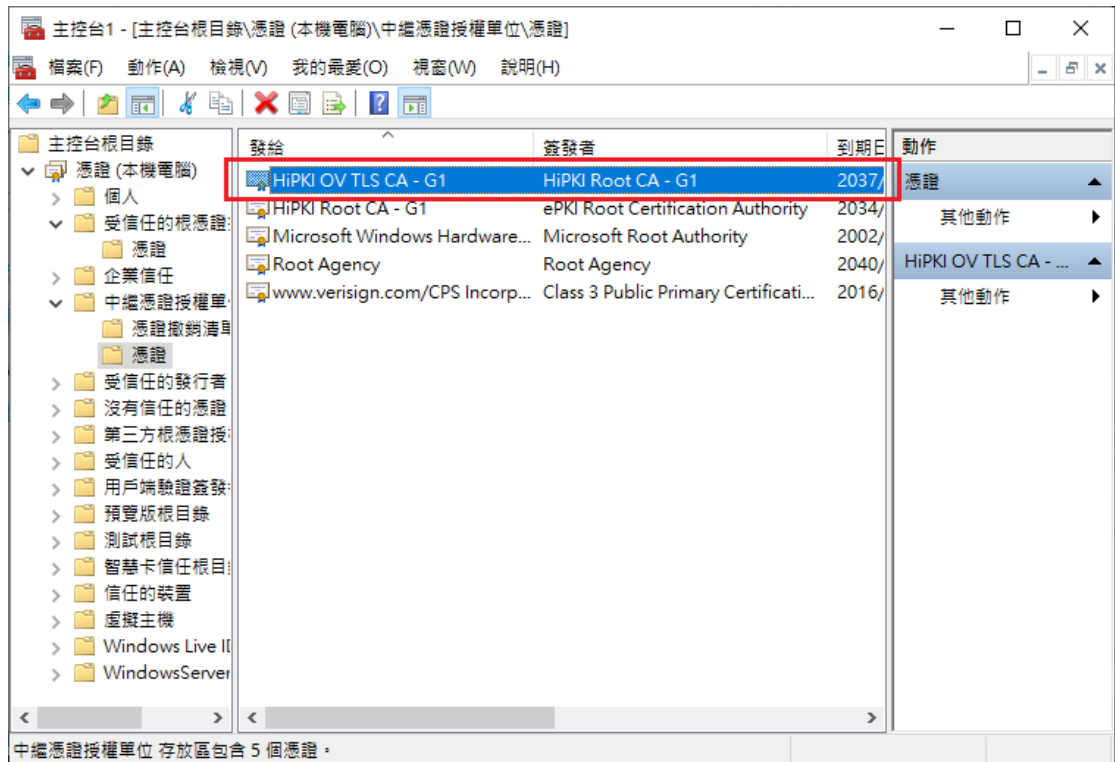
下一步(N)

取消

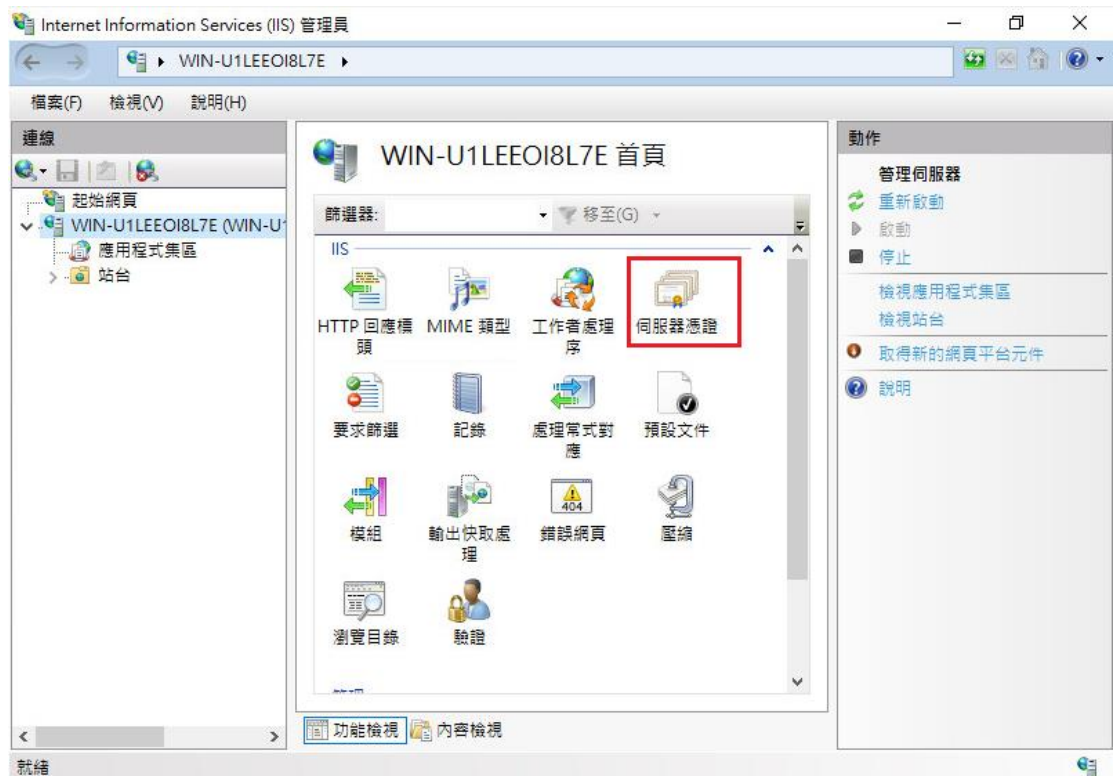


五、於「中繼憑證授權單位」匯入中繼憑證。依照上述匯入根憑證的步驟，匯入中繼憑證。

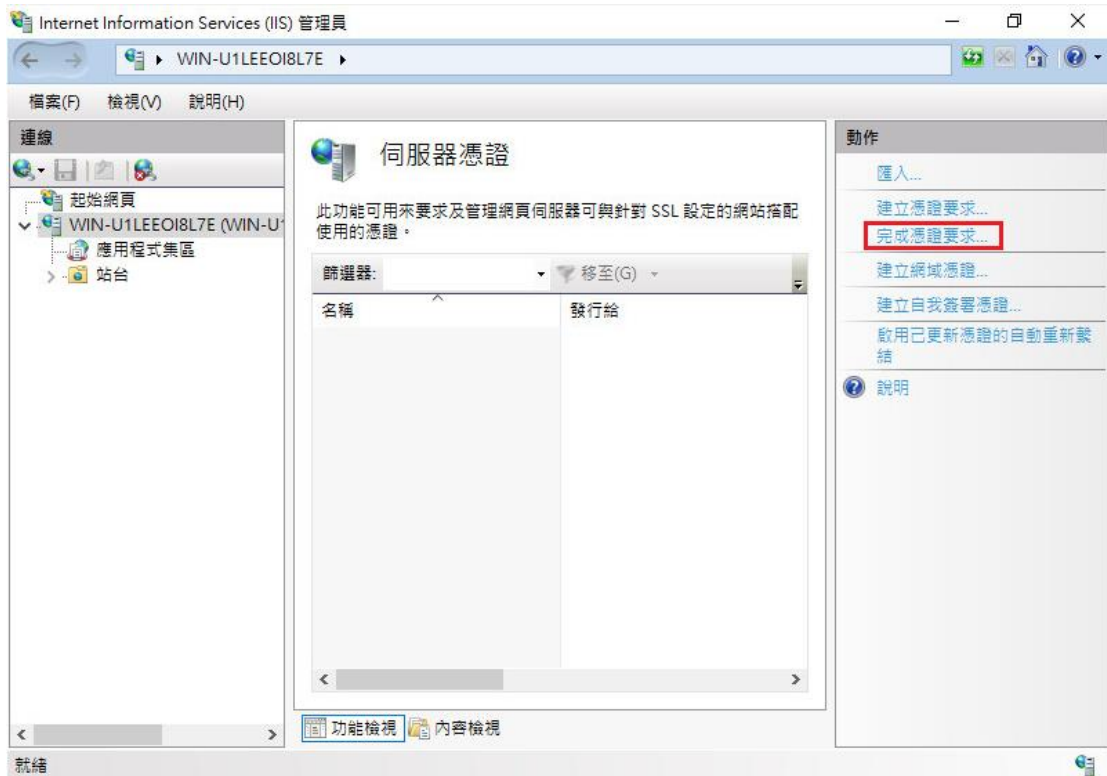




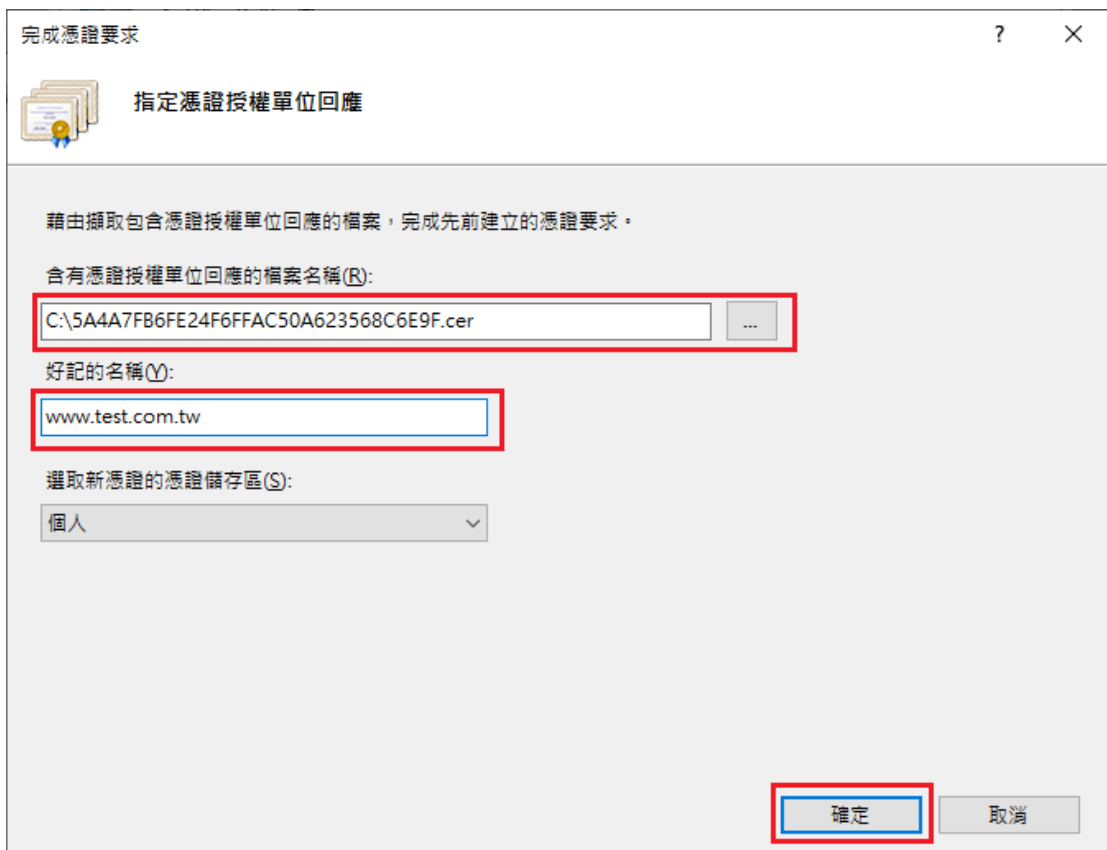
六、 開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



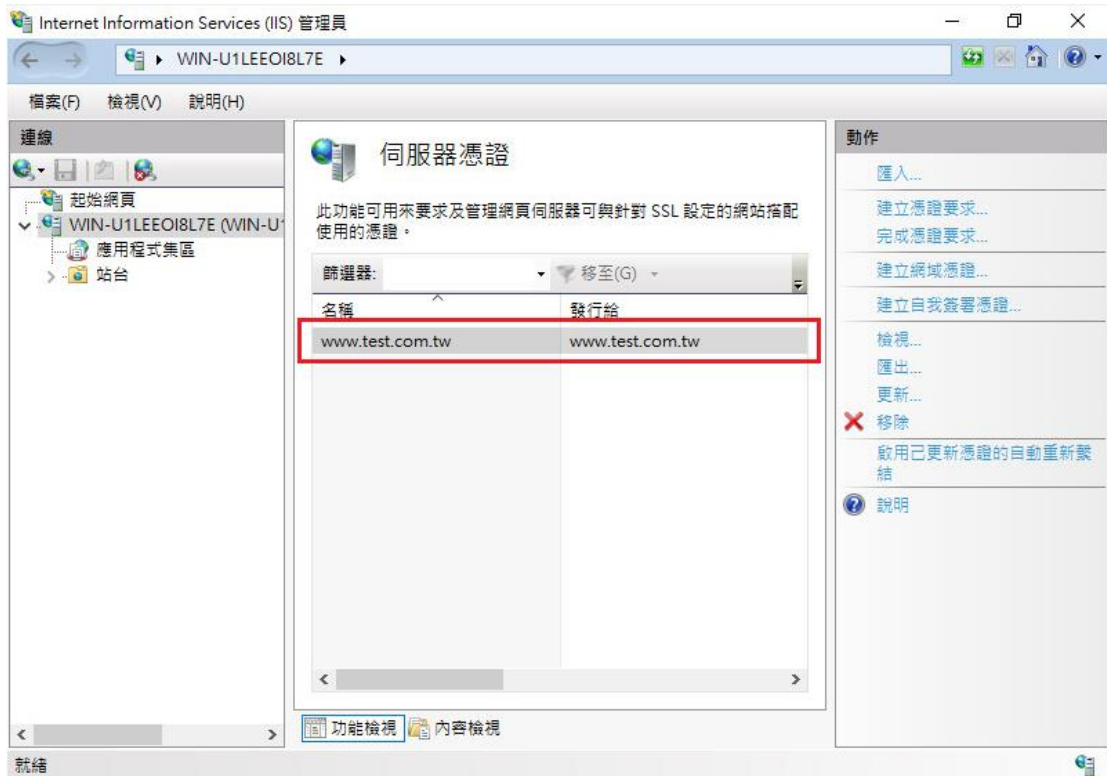
七、 點選「完成憑證要求」。



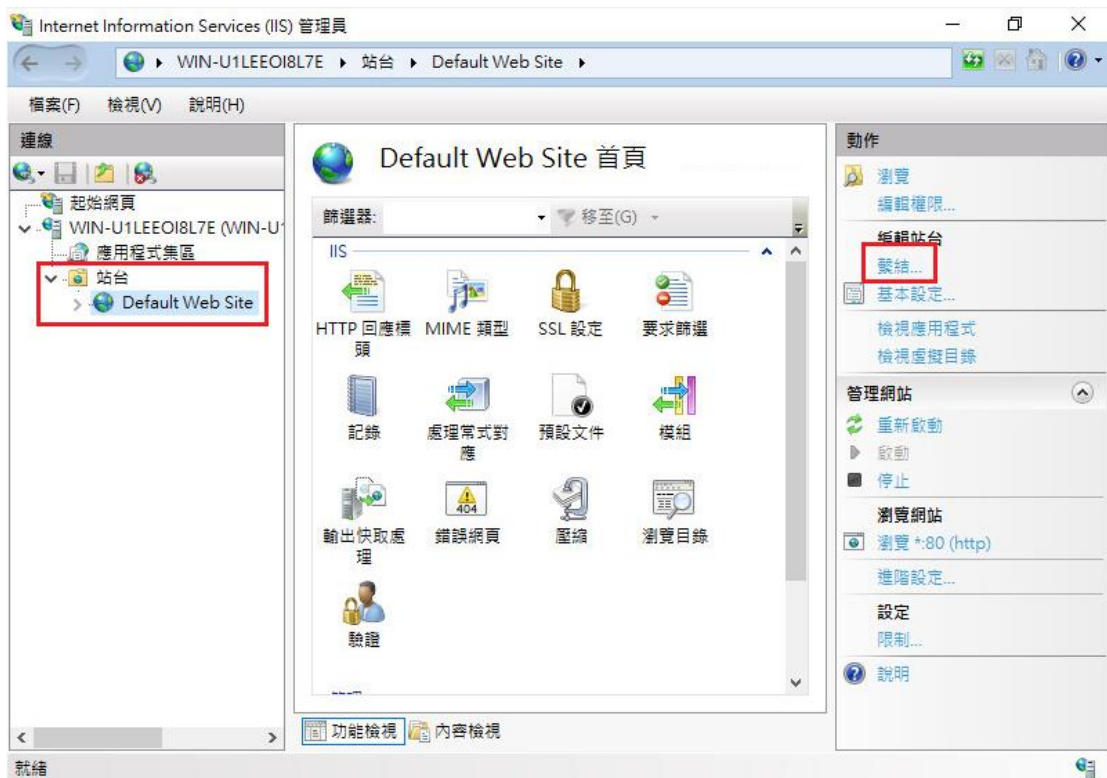
- 八、 選擇由憑證管理中心所簽發之 SSL 憑證路徑，並輸入好記名稱(範例填寫 Domain Name)。

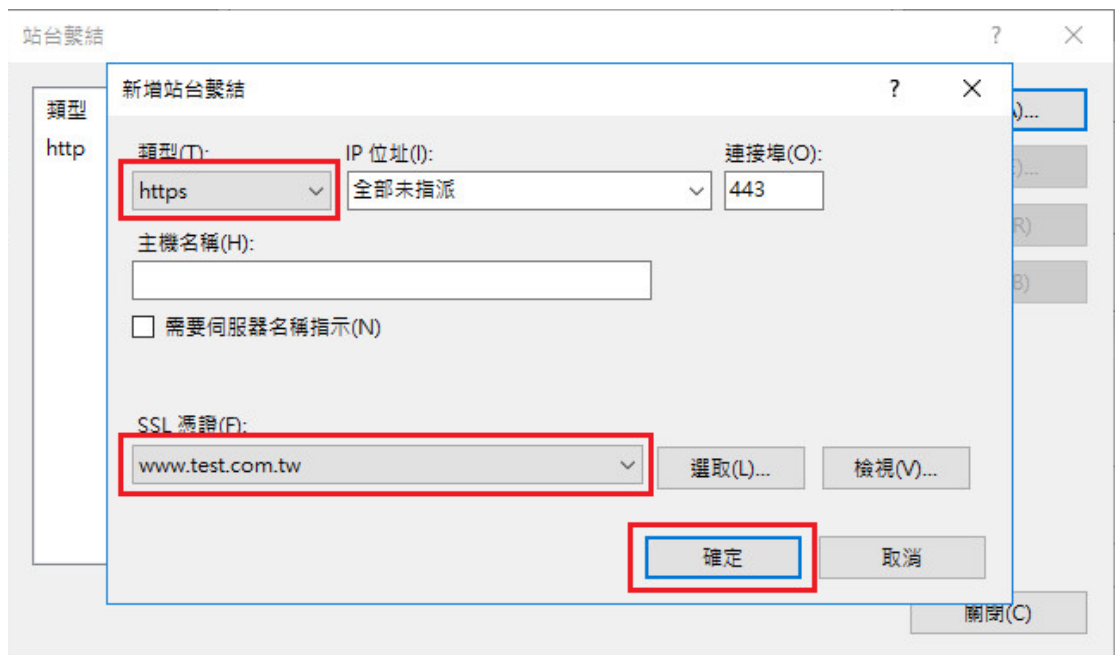
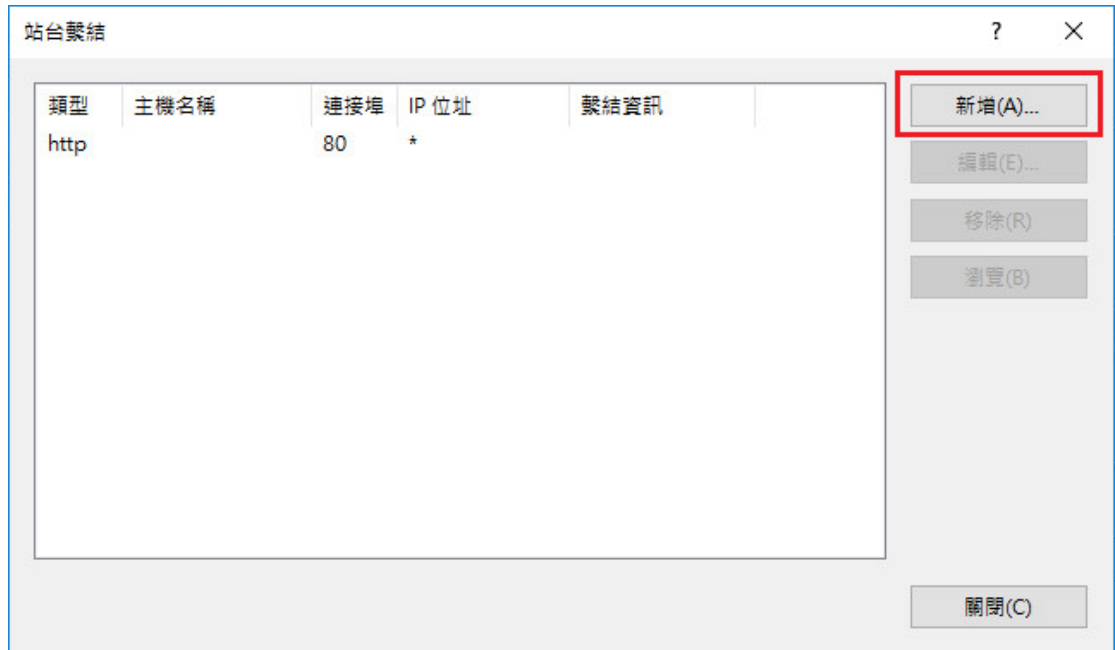


- 九、 伺服器憑證出現匯入的憑證項目。



- 十、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)。





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

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