

中華電信通用憑證管理中心 (PublicCA)

Windows IIS 7.0 SSL 憑證請求檔製作與憑證安裝手冊

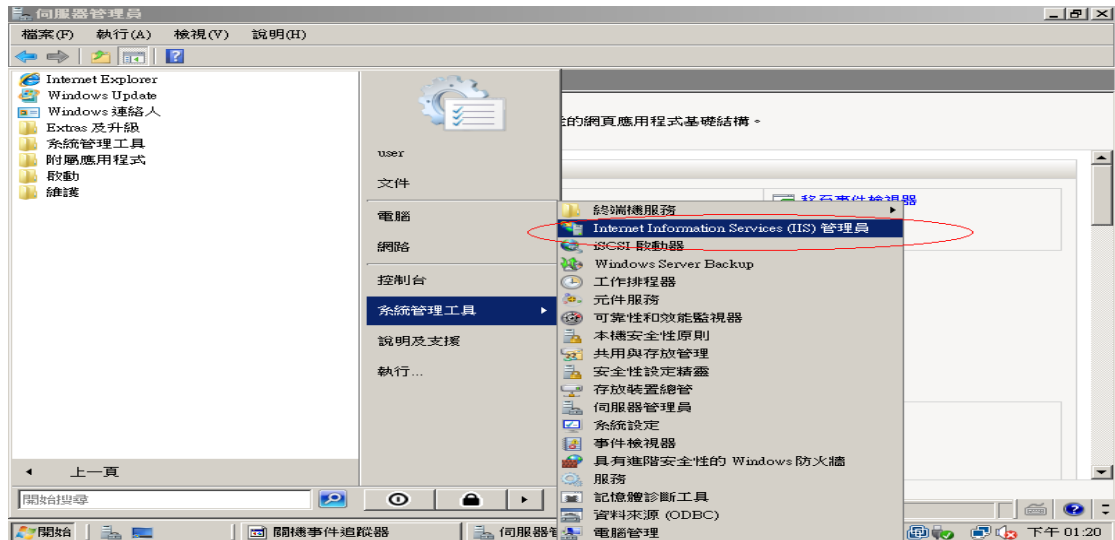
聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本說明文件所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

目錄

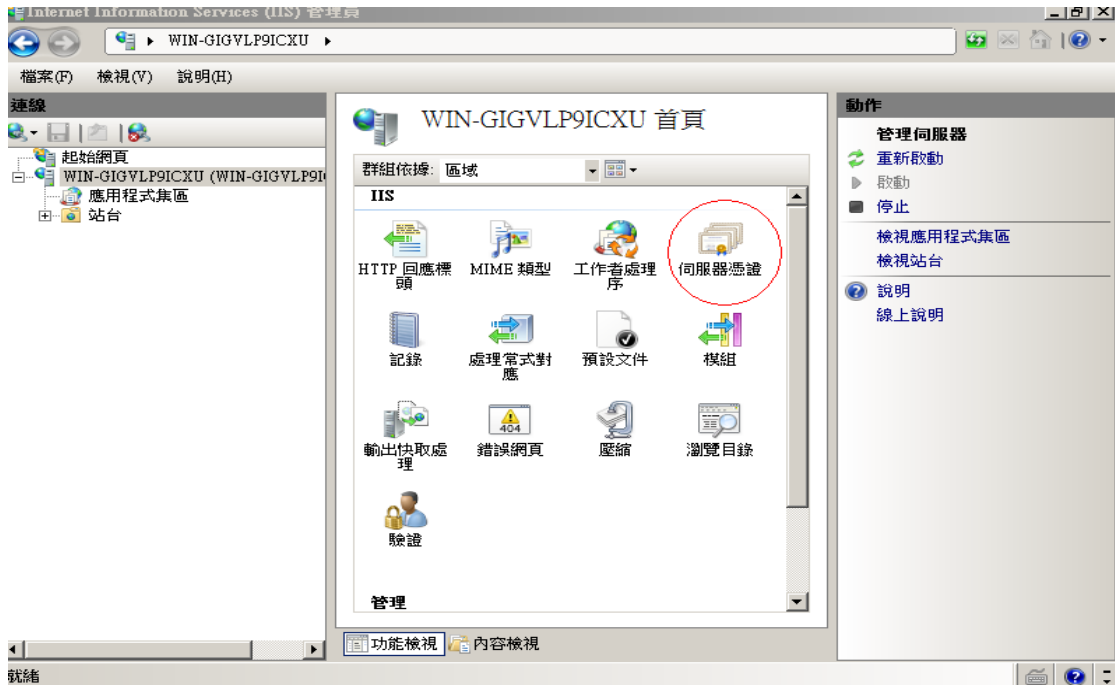
Windows IIS 7.0 SSL 憑證請求檔製作手冊.....	2
Windows IIS 7.0 SSL 憑證安裝操作手冊.....	5
附件一：設定 SSL 安全通道的加密強度.....	19
附件二：單一 IP，多站台啟用 SSL	28

Windows IIS 7.0 SSL 憑證請求檔製作手冊

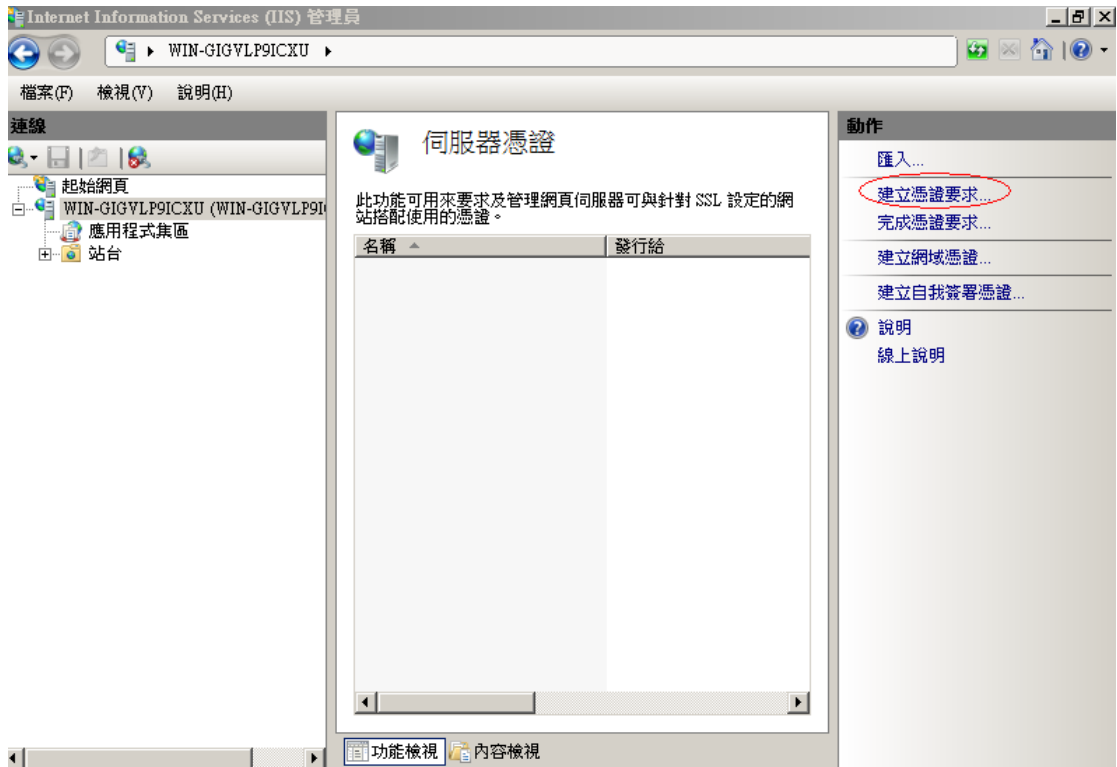
- 一、點選「開始」「系統管理工具」「Internet Information Services (IIS) 管理員」



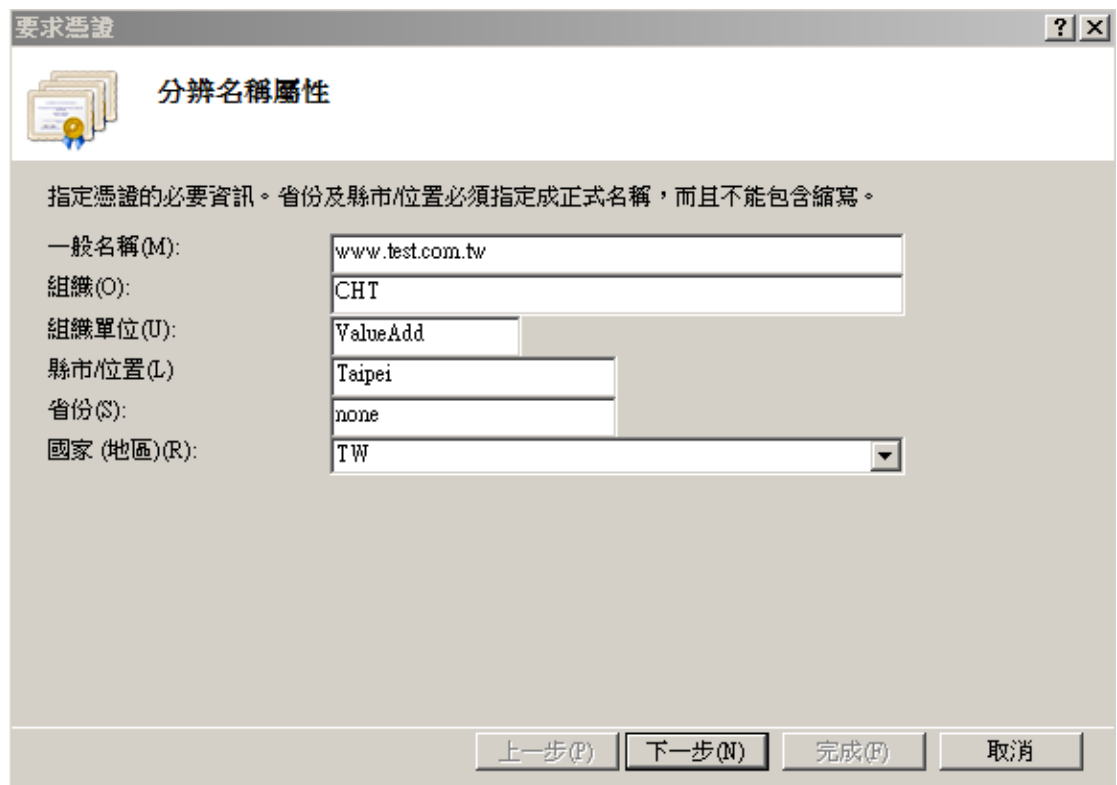
- 二、點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」



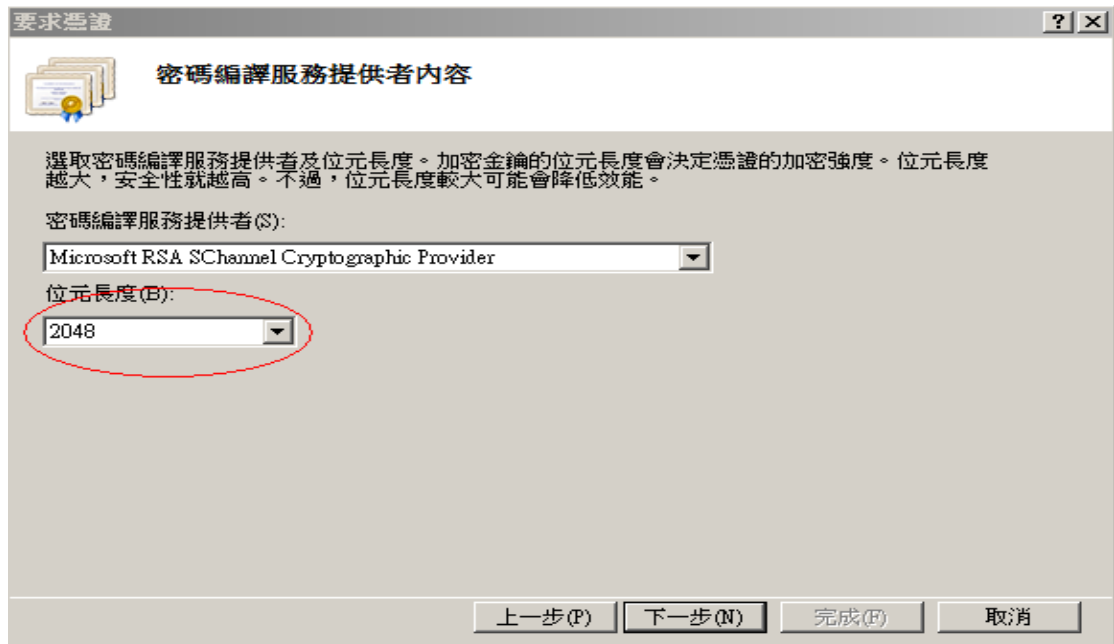
- 三、點選「建立憑證要求」



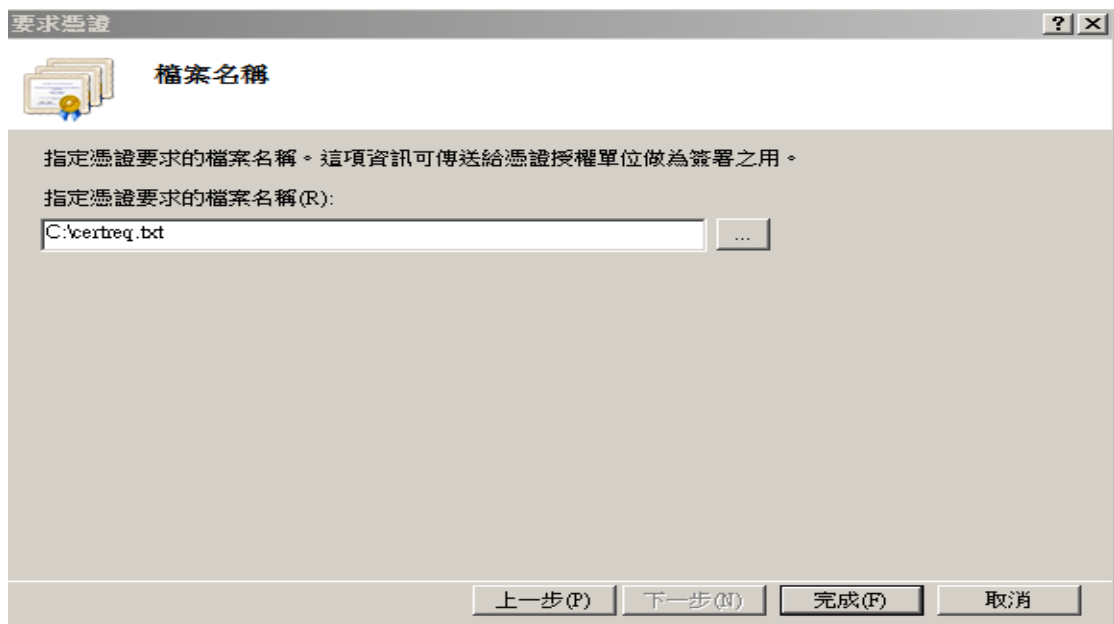
四、輸入以下所有欄位資料，輸入完成後點點選「下一步」



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。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。



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」。



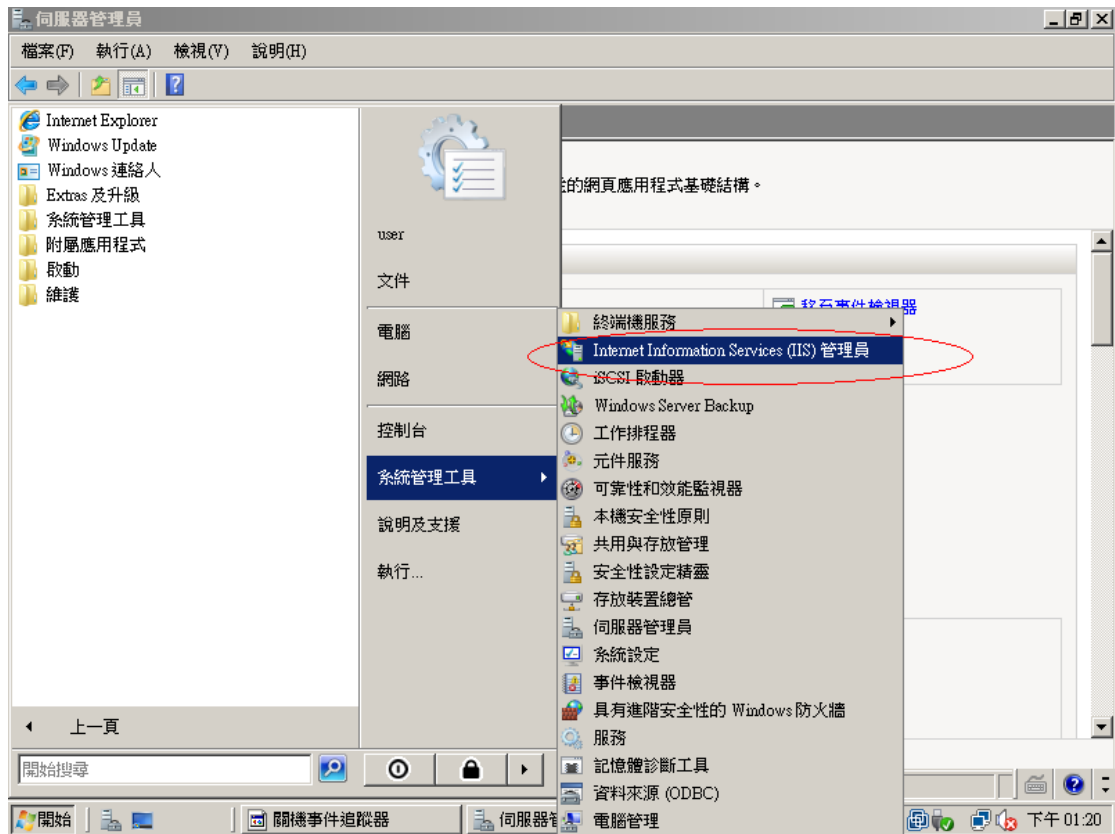
七、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證。

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。

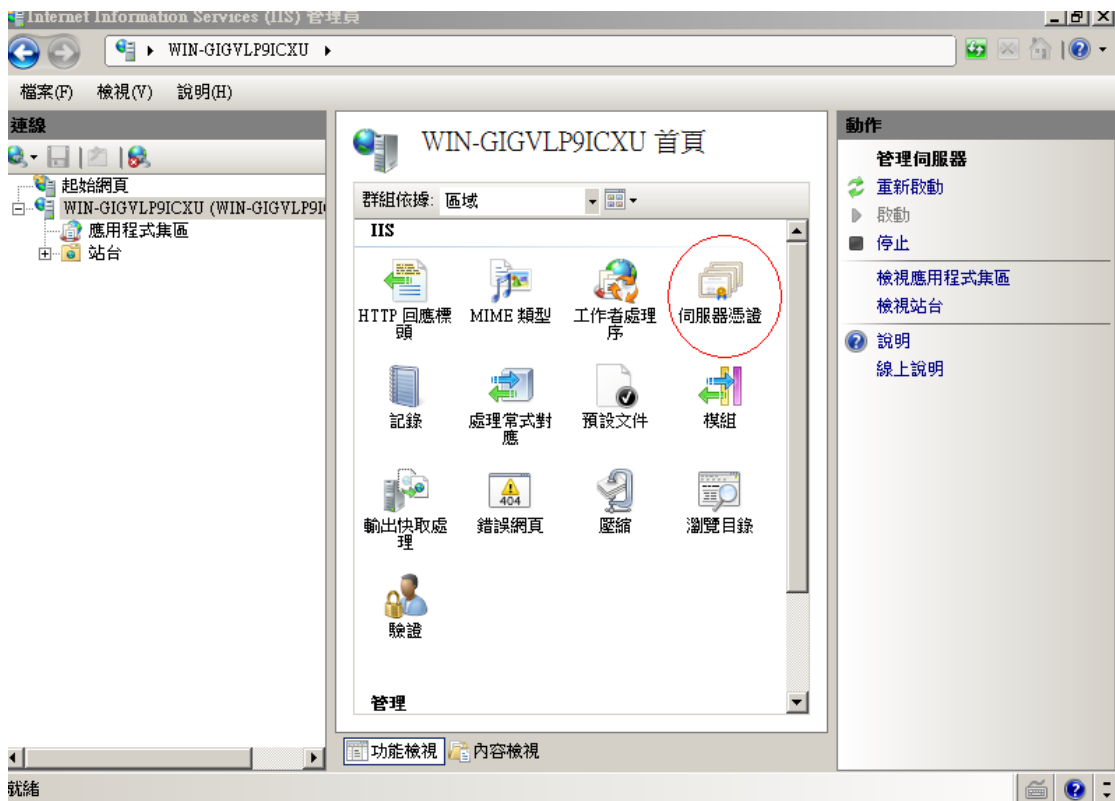
Windows IIS 7.0 SSL 憑證安裝操作手冊

- 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

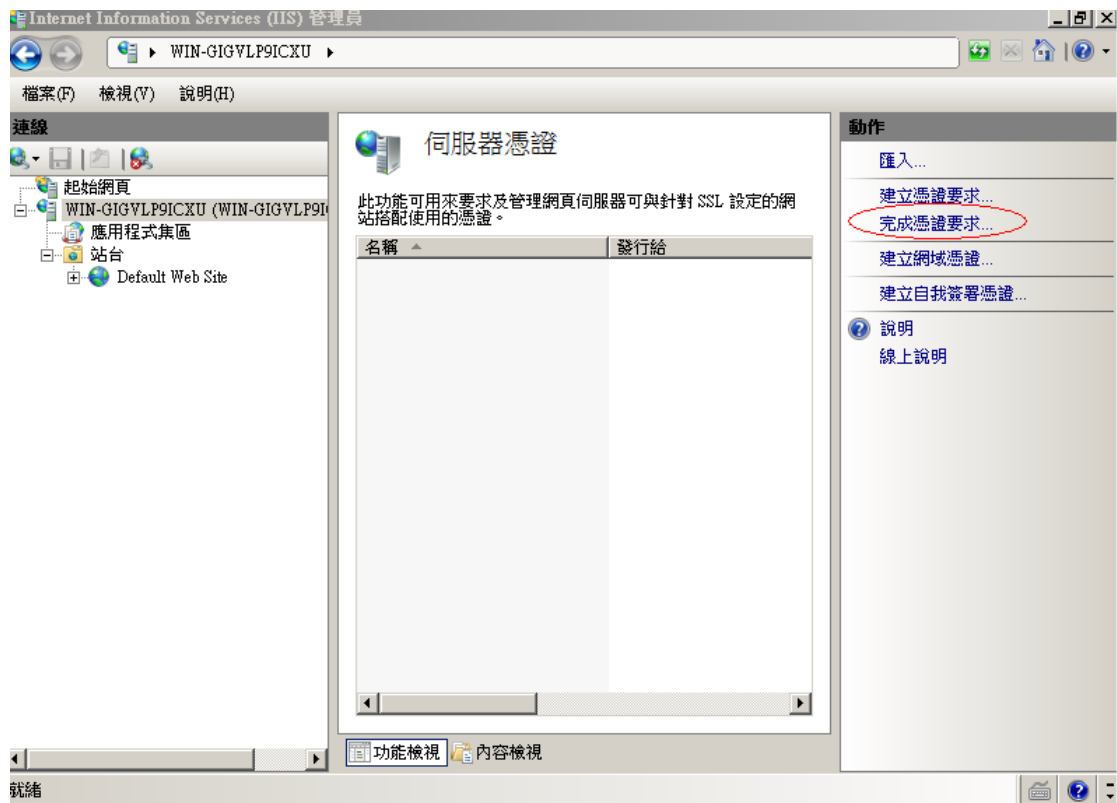
PublicCA G2 憑證：
http://epki.com.tw/download/PublicCA2_64.crt
SSL 憑證下載：您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，進行 SSL 憑證下載。
若您是中華電信之員工，負責管理單位之伺服器，請至 <http://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。
- 二、有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(<https://publicca.hinet.net/SSL-08-06.htm>)
- 三、點選「開始」→「系統管理工具」→「Internet Information Services (IIS) 管理員」。



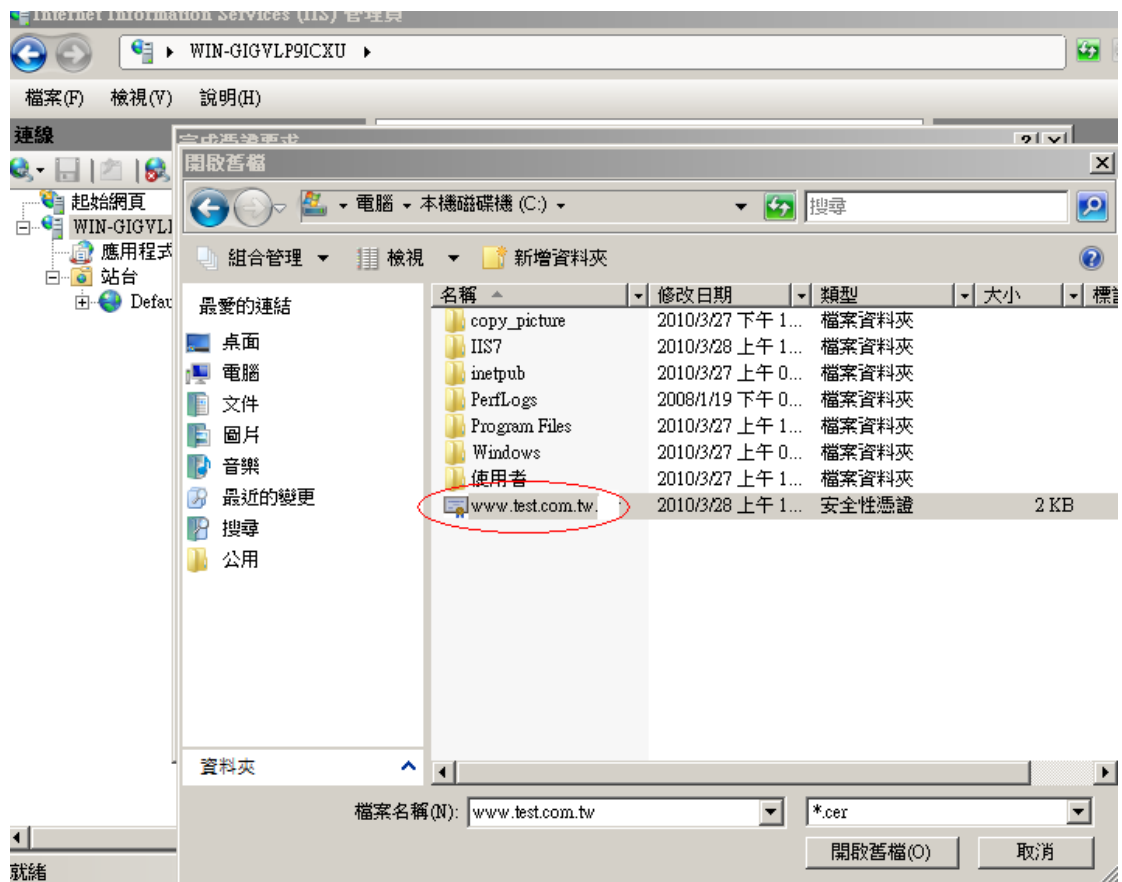
四、點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。

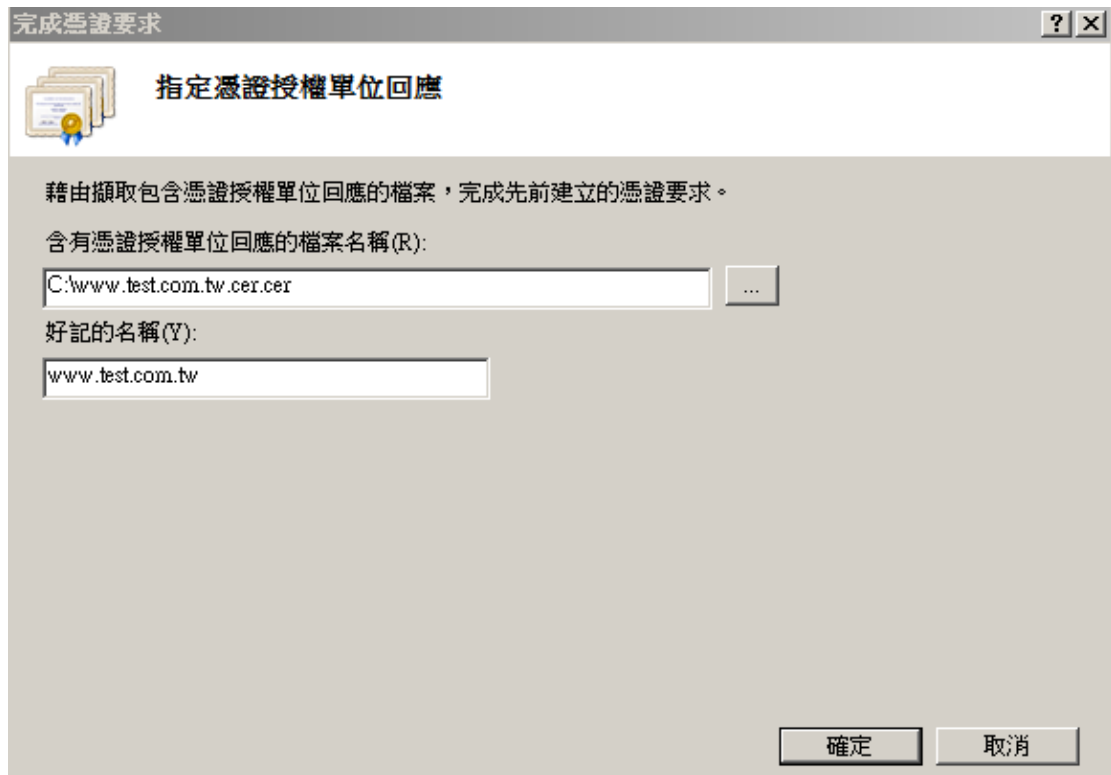


五、點選「完成憑證要求」。

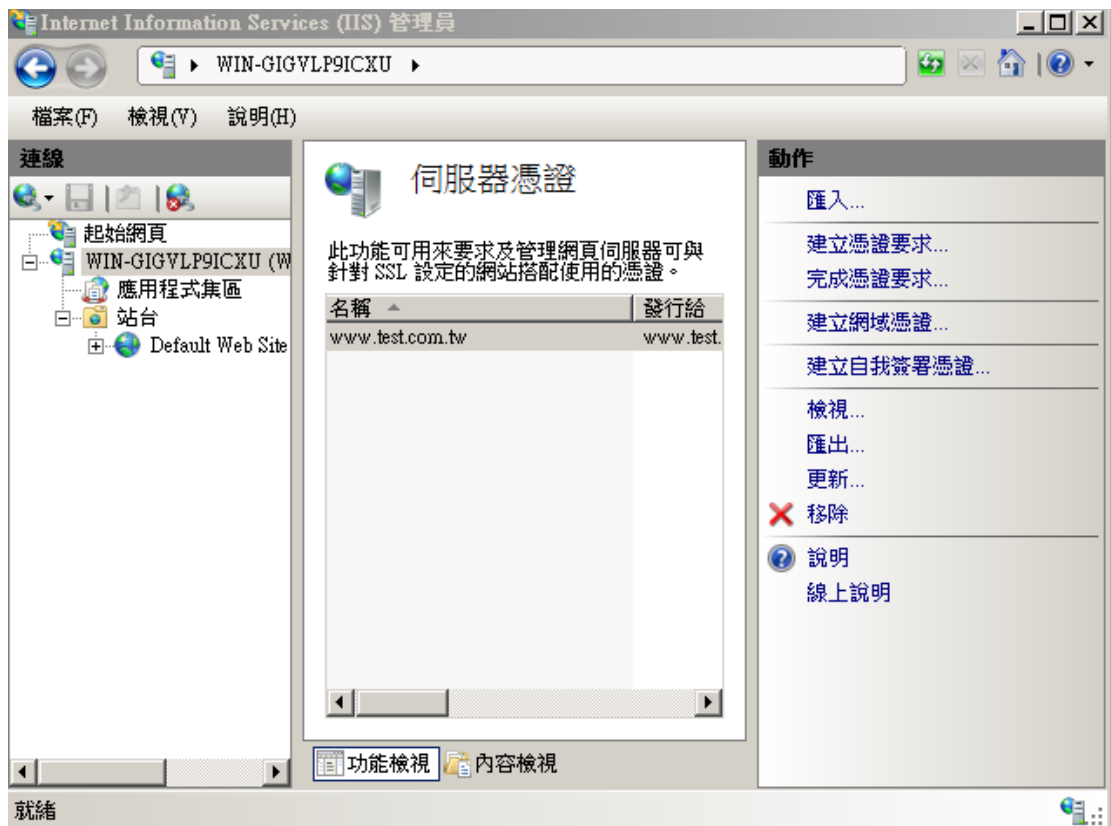


六、選擇至憑證管理中心申請之 SSL 憑證，並輸入好記名稱(一般填寫 Domain Name)。





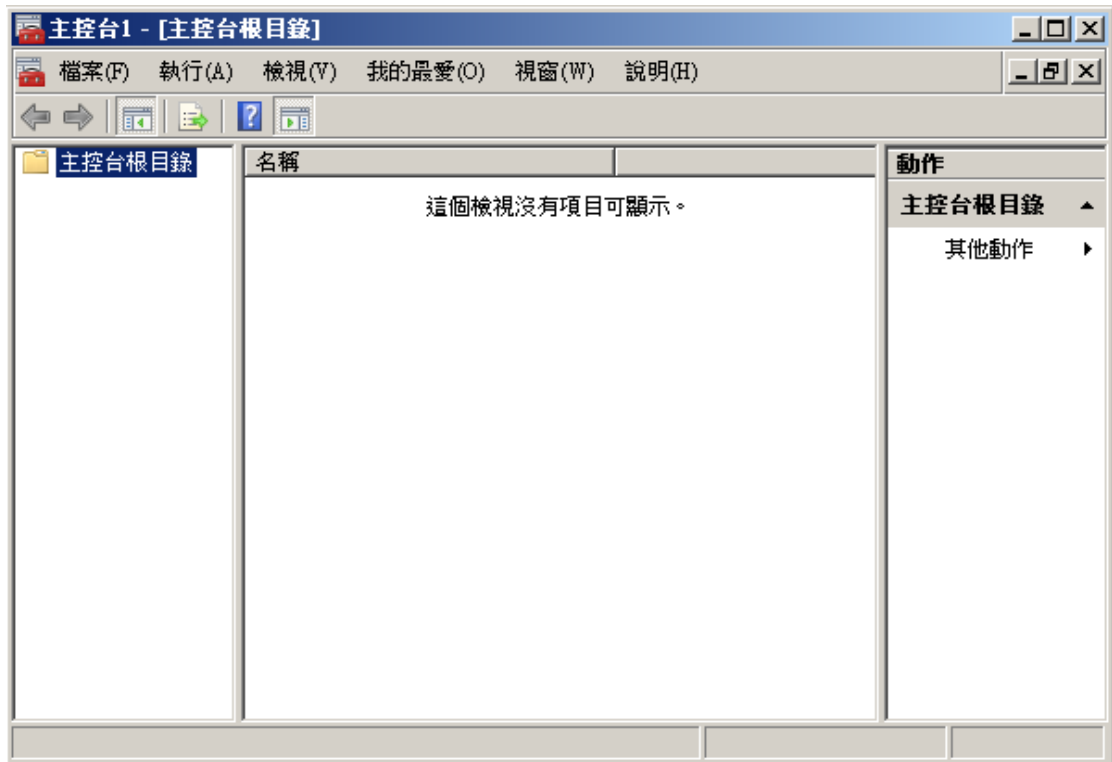
七、步驟 4 按「確定」，出現完成憑證要求的畫面。



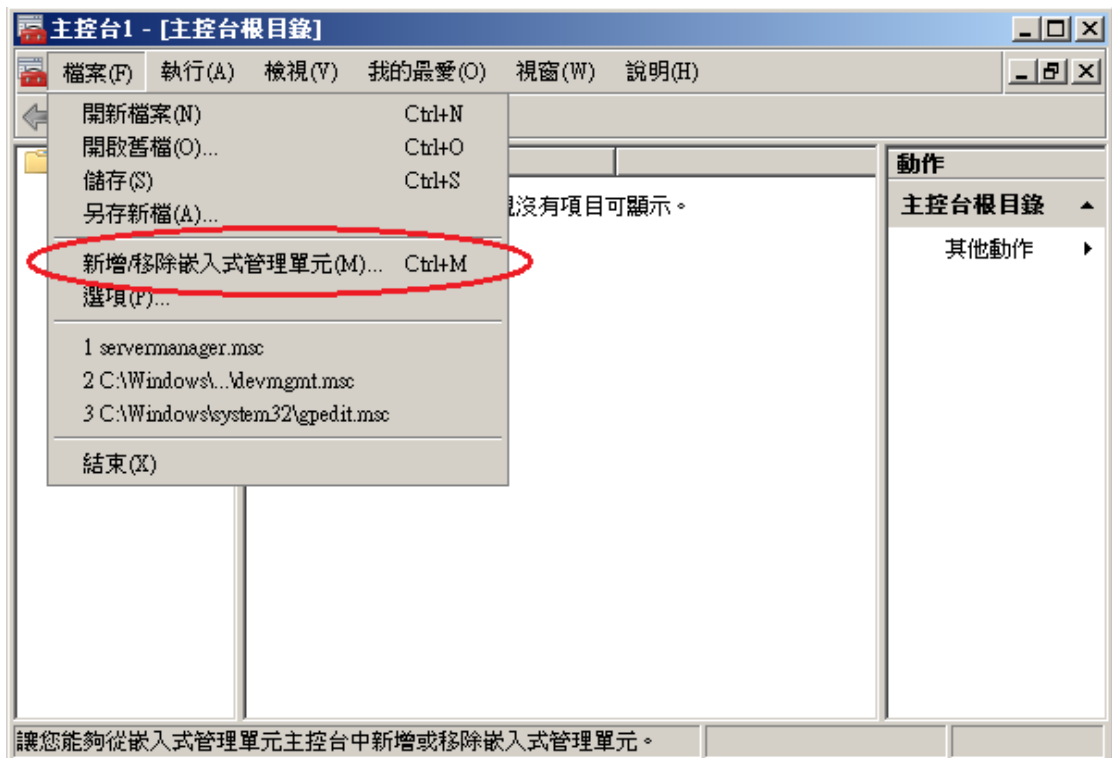
八、接著要安裝 eCA 及 PublicCA 憑證。

請先點選「開始」→輸入「mmc」→按下「Enter」。

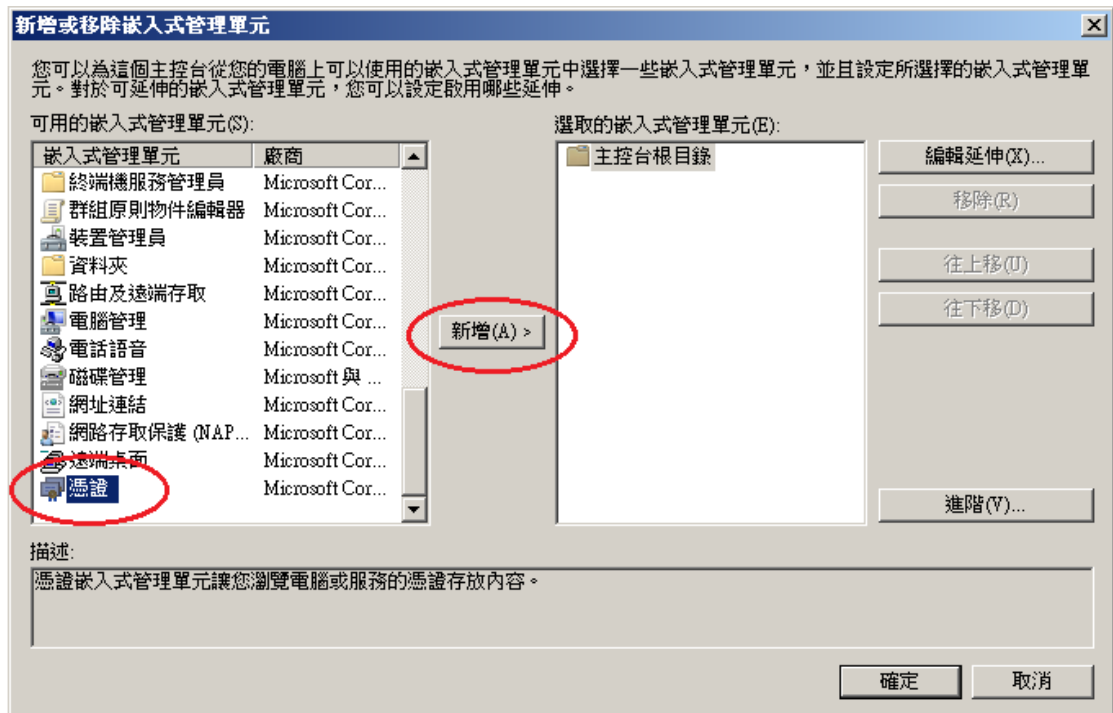




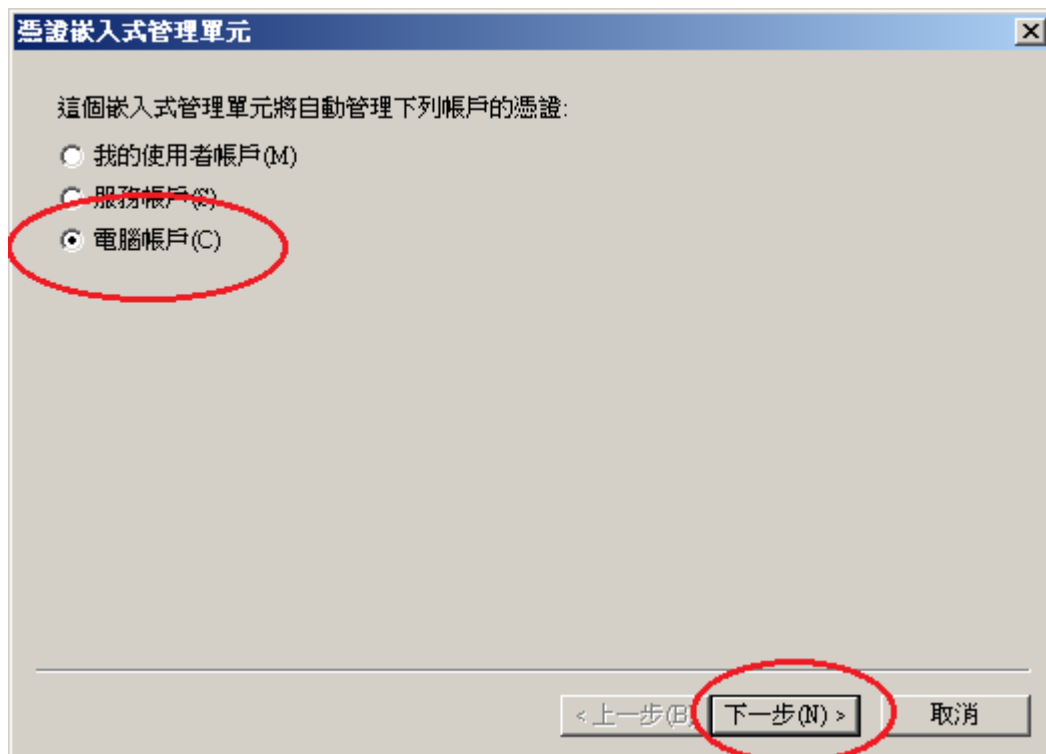
九、選擇「新增/移除嵌入式管理單元」。

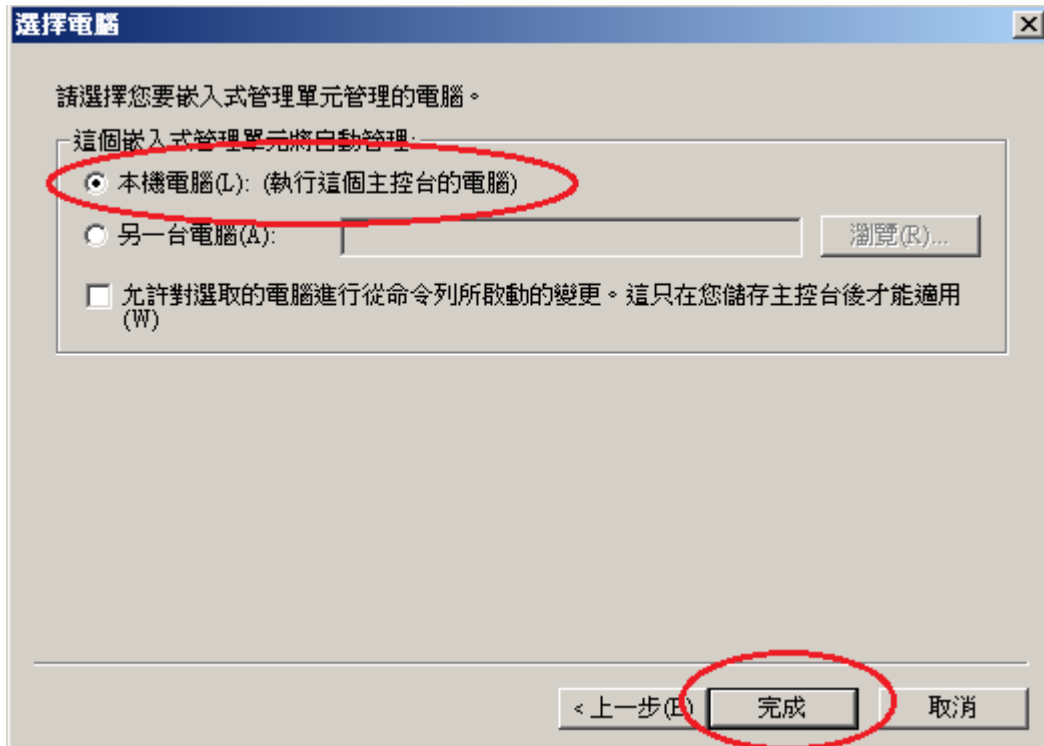


十、接著點選「憑證」→「新增」。

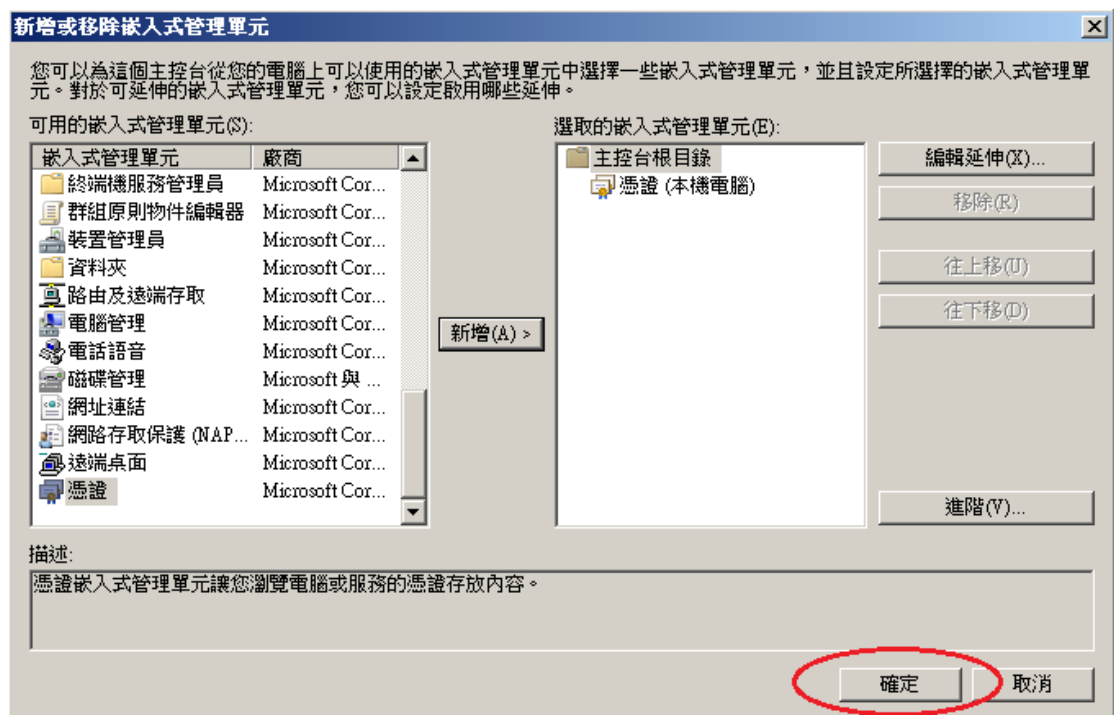


選擇「電腦帳戶」→「下一步」→「完成」。

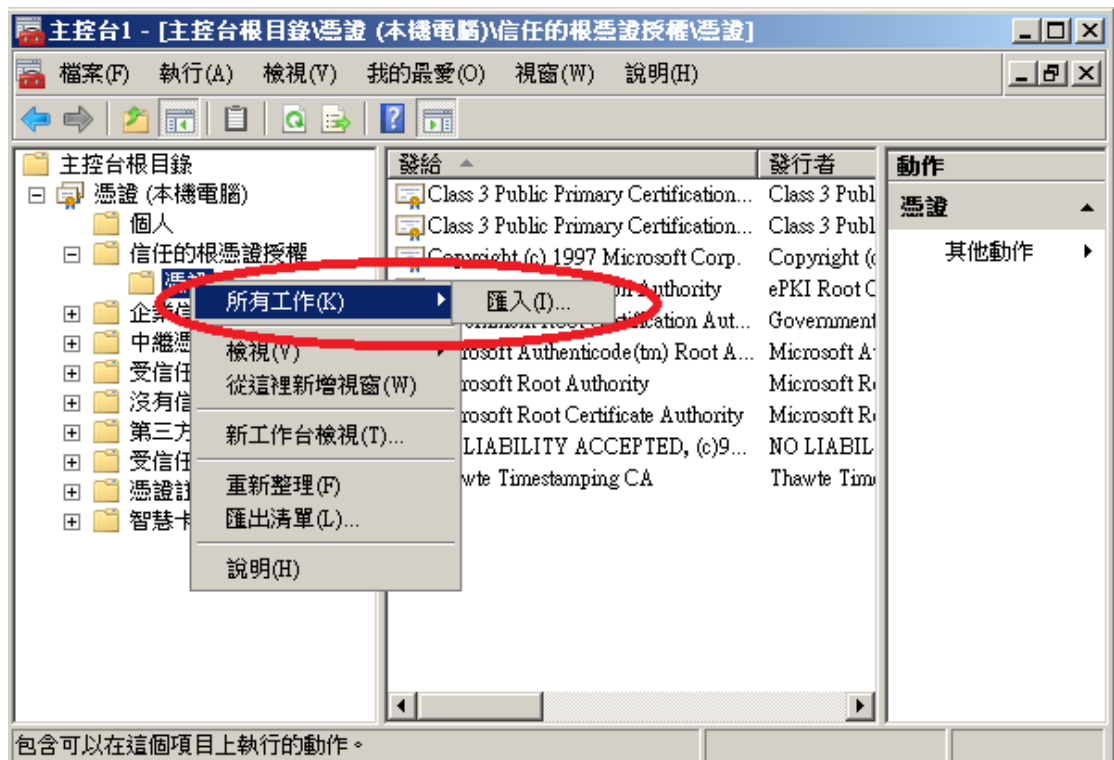




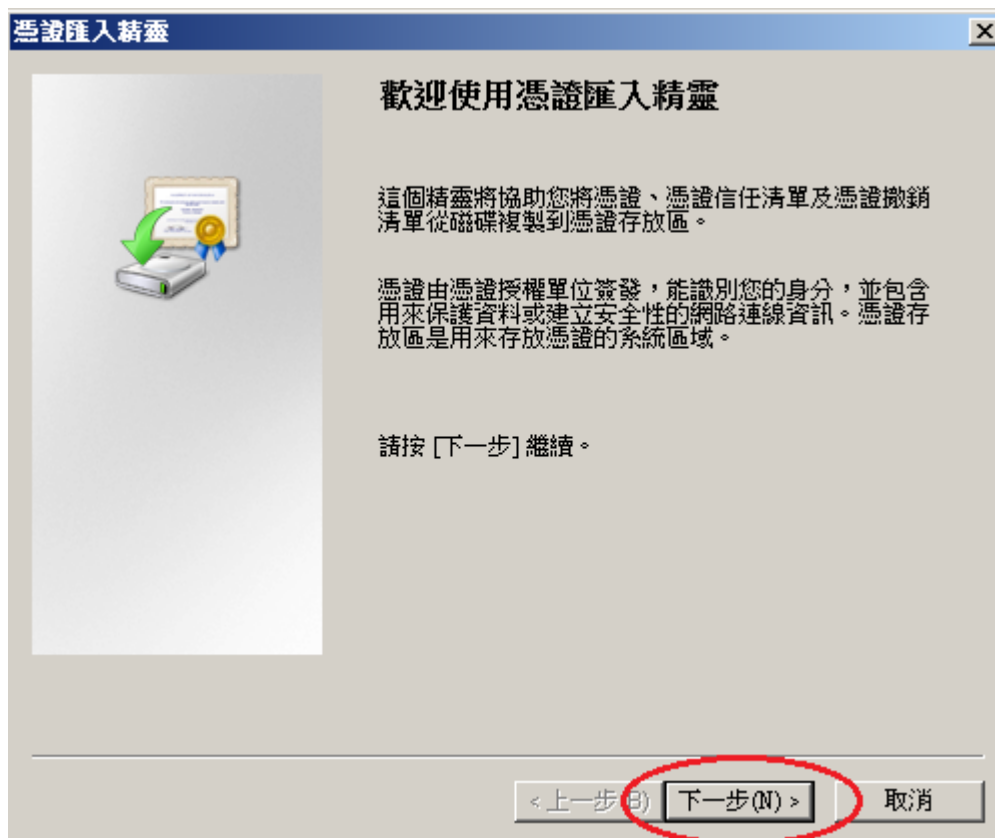
最後按下「確定」。

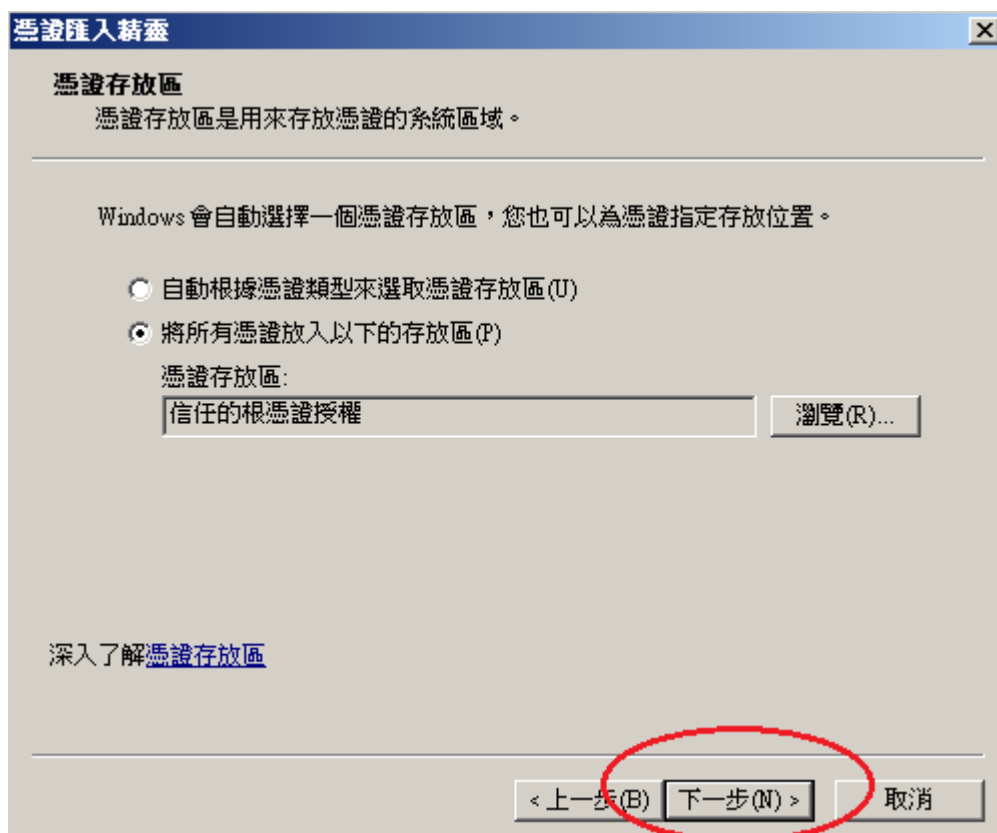
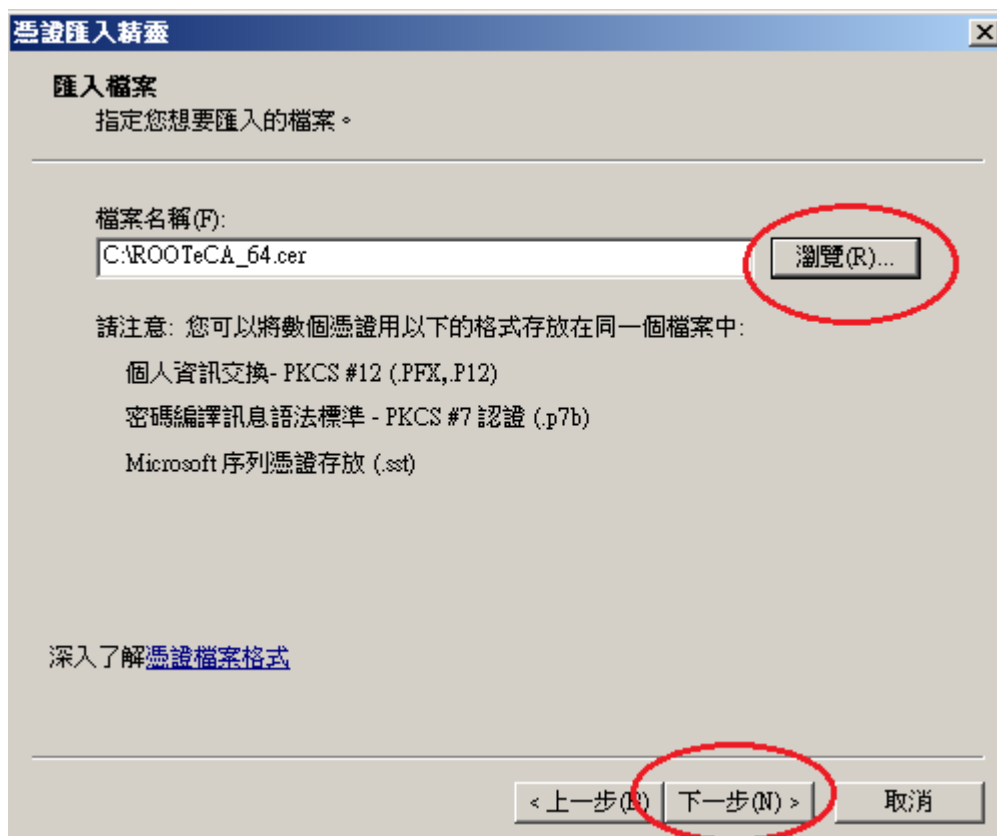


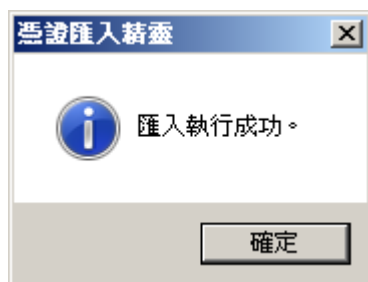
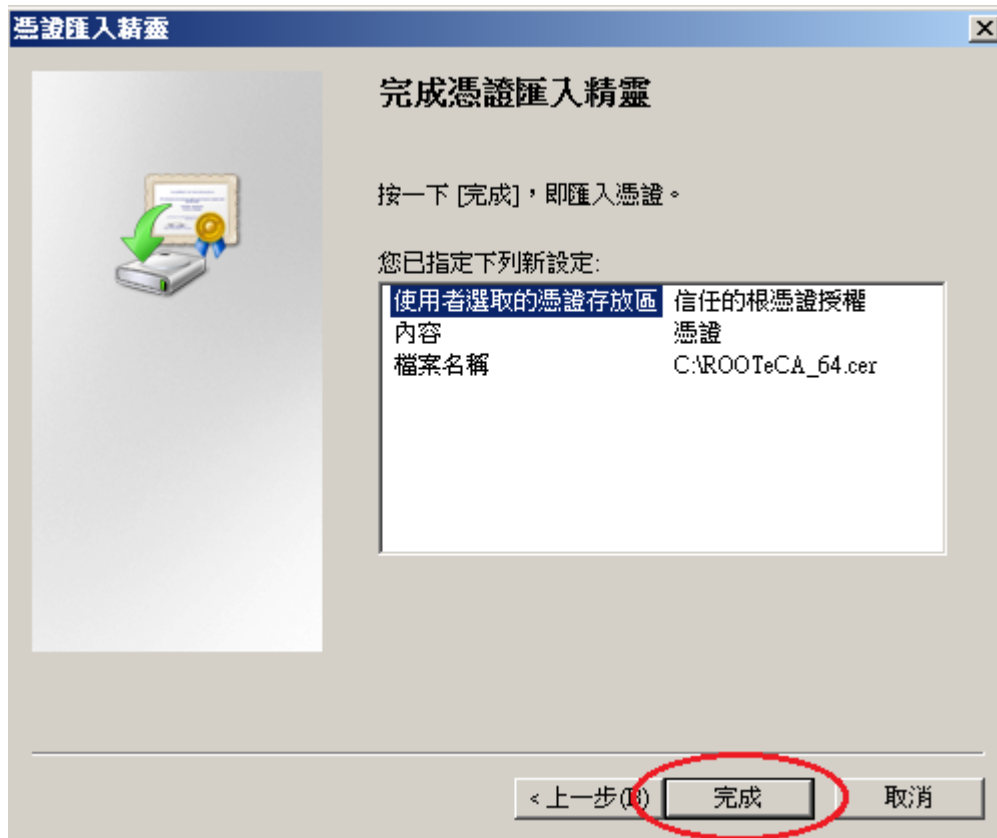
十一、 先匯入根憑證。在「信任的根憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



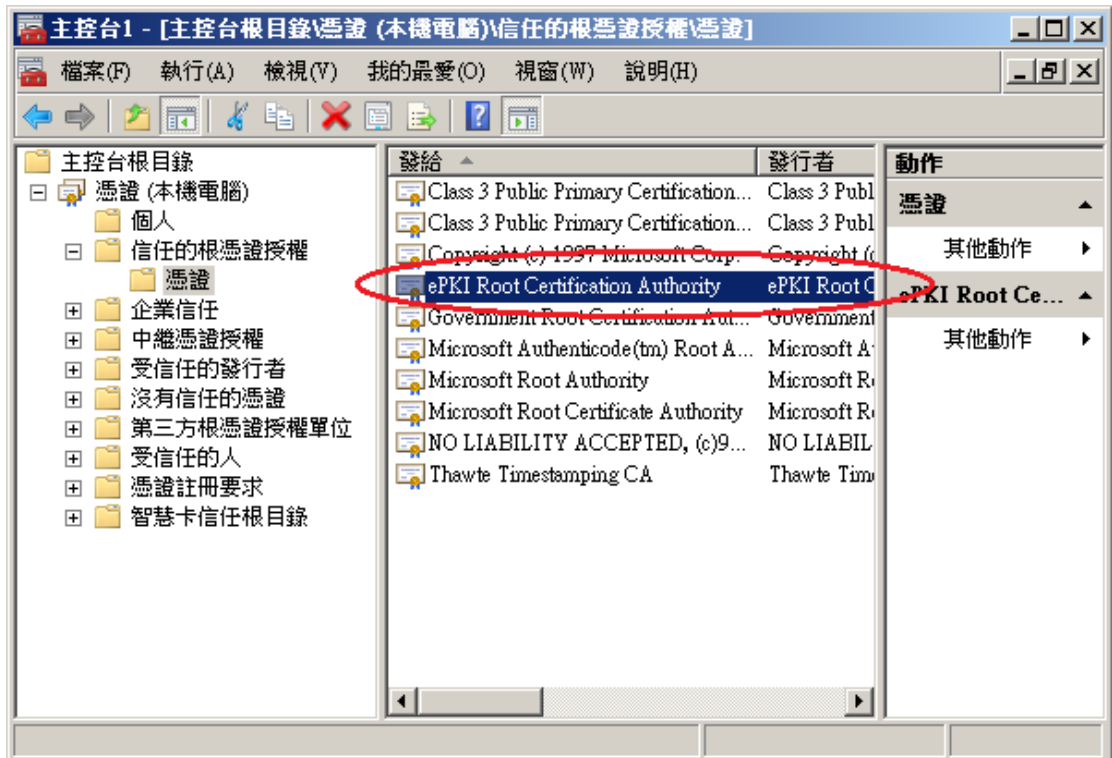
十二、 出現以下畫面後，點選「下一步」→「下一步」→「完成」。



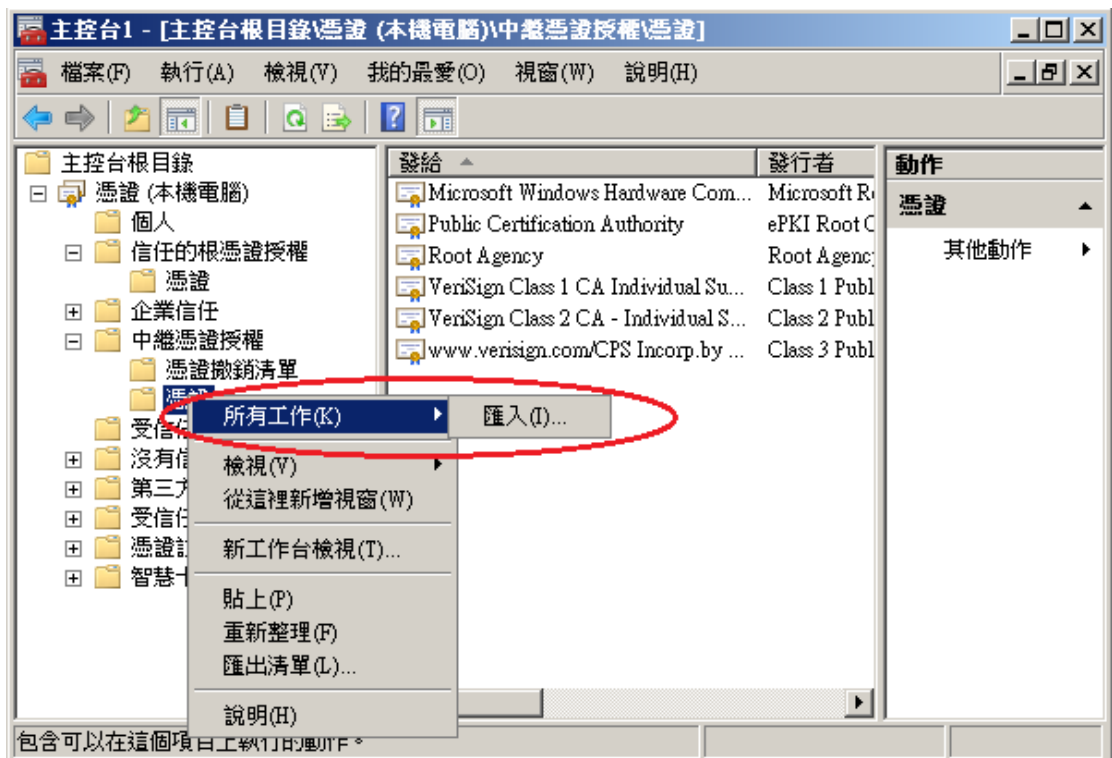




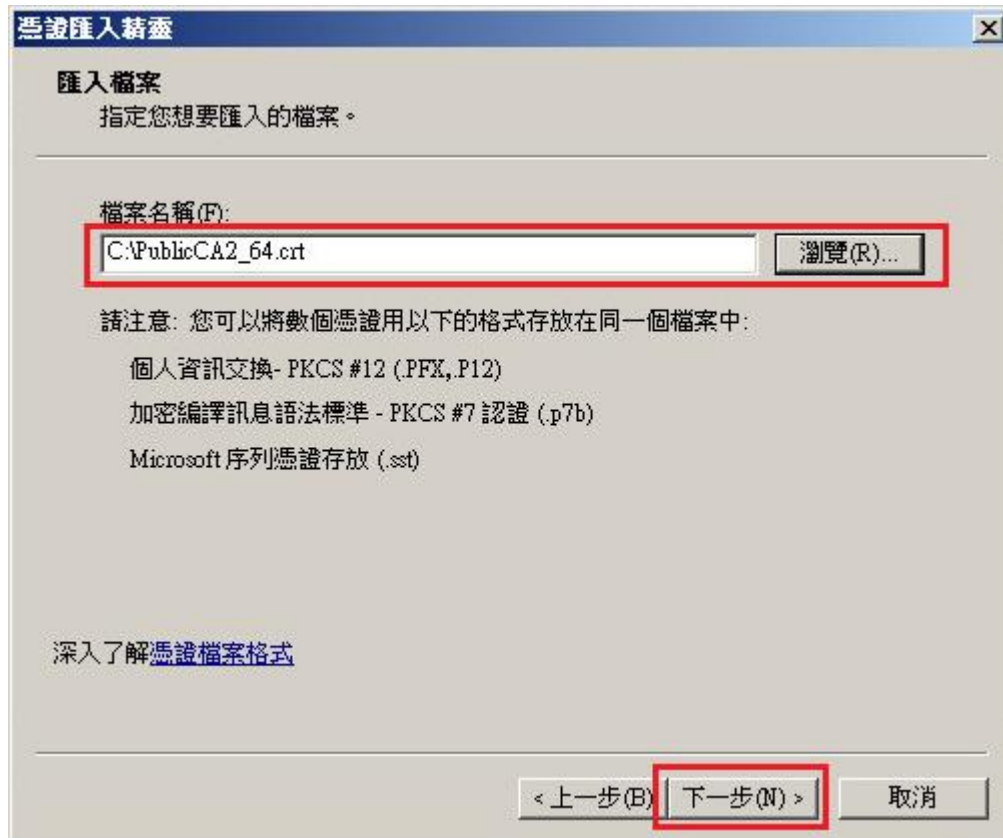
十三、 匯入成功後，可以看到 eCA 的根憑證。



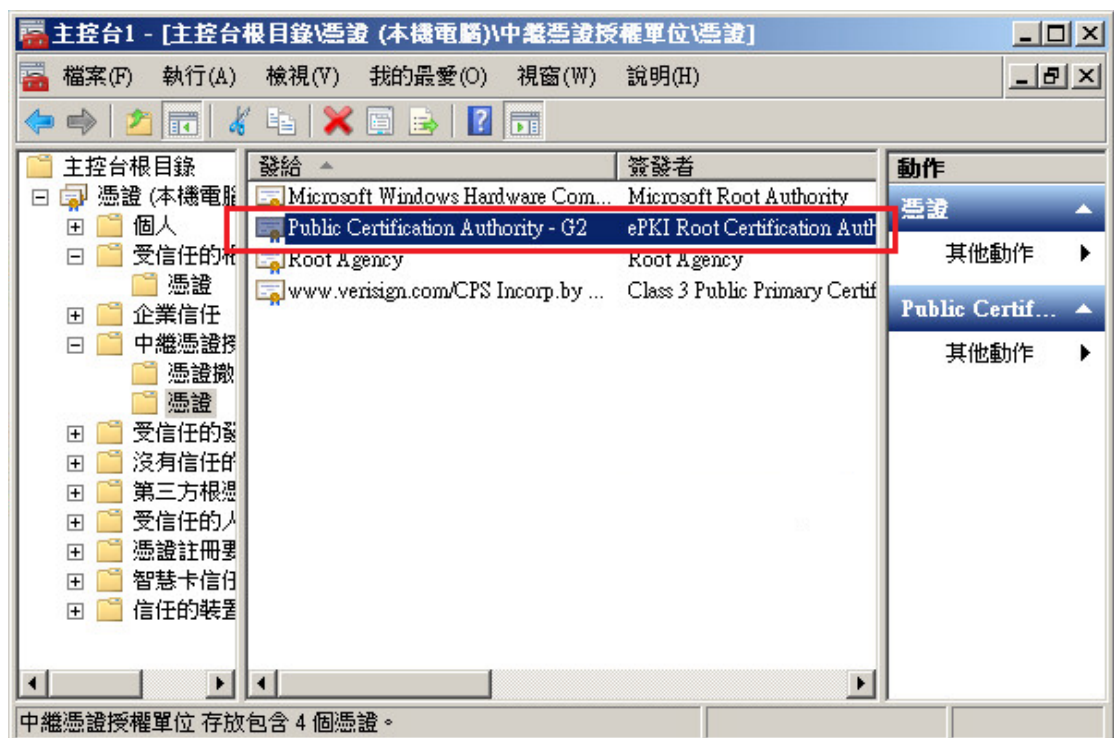
十四、 第二步，匯入中繼憑證。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



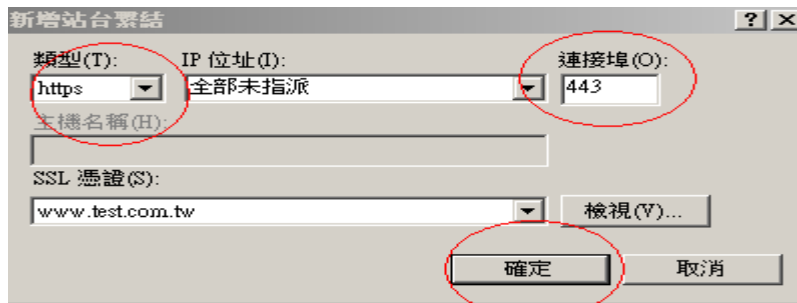
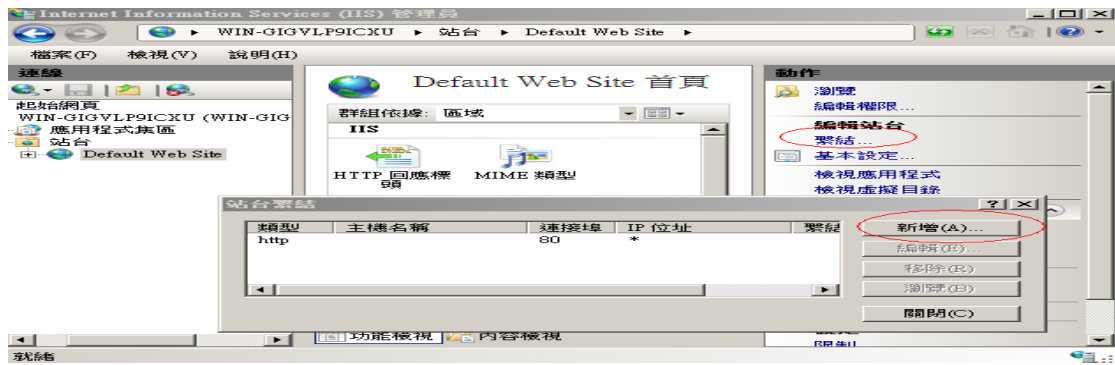
依照上述匯入 eCA 根憑證的步驟，匯入 PublicCA G2 中繼憑證。



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。

十七、 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。

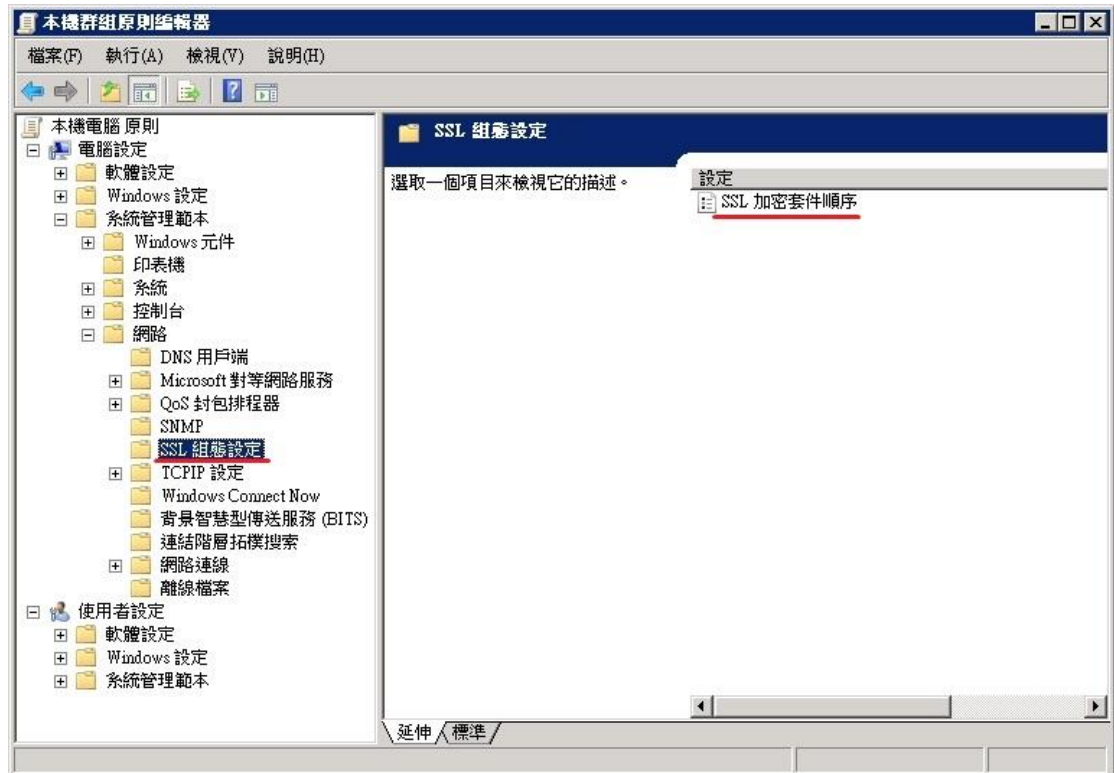
附件一：設定 SSL 安全通道的加密強度

IIS 7.0 預設使用 AES 128 位元來進行資料加密，欲使用 AES 256 位元來進行資料加密的話，可以參考以下步驟：

一、啟動 gpedit.msc 程式



二、選擇 SSL 組態設定，對著「SSL 加密套件順序」點兩下。



三、選擇「已啟用」，並修改 SSL 加密套件的欄位。

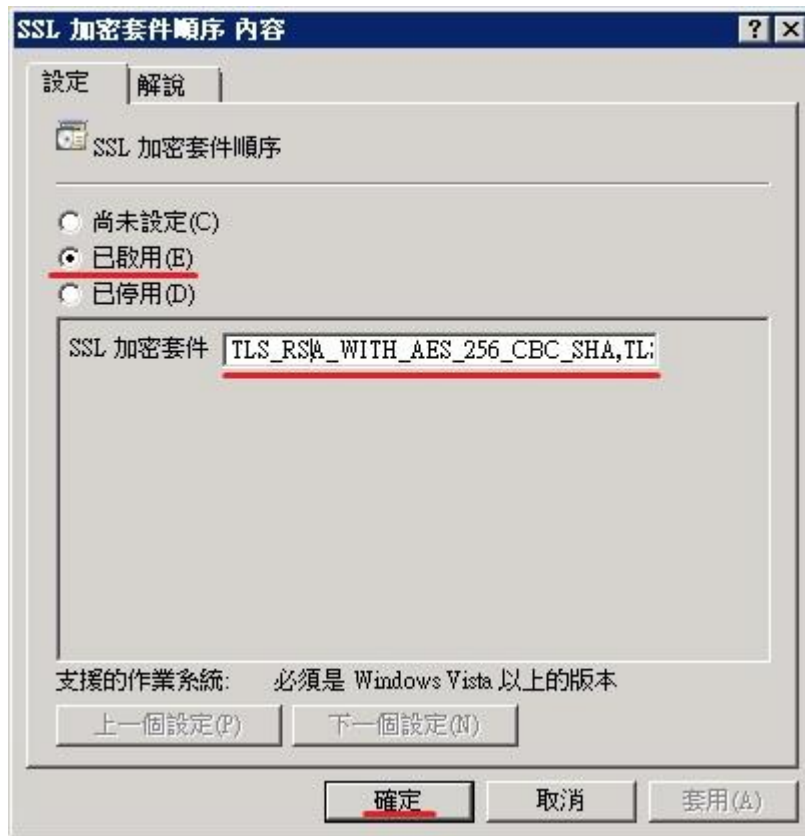
原加密套件順序：

TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_RC4_128_MD5, SSL_CK_RC4_128_WITH_MD5, SSL_CK_DES_192_EDE3_CBC_WITH_MD5, TLS_RSA_WITH_NULL_MD5, TLS_RSA_WITH_NULL_SHA

修改後的加密套件順序：

TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES

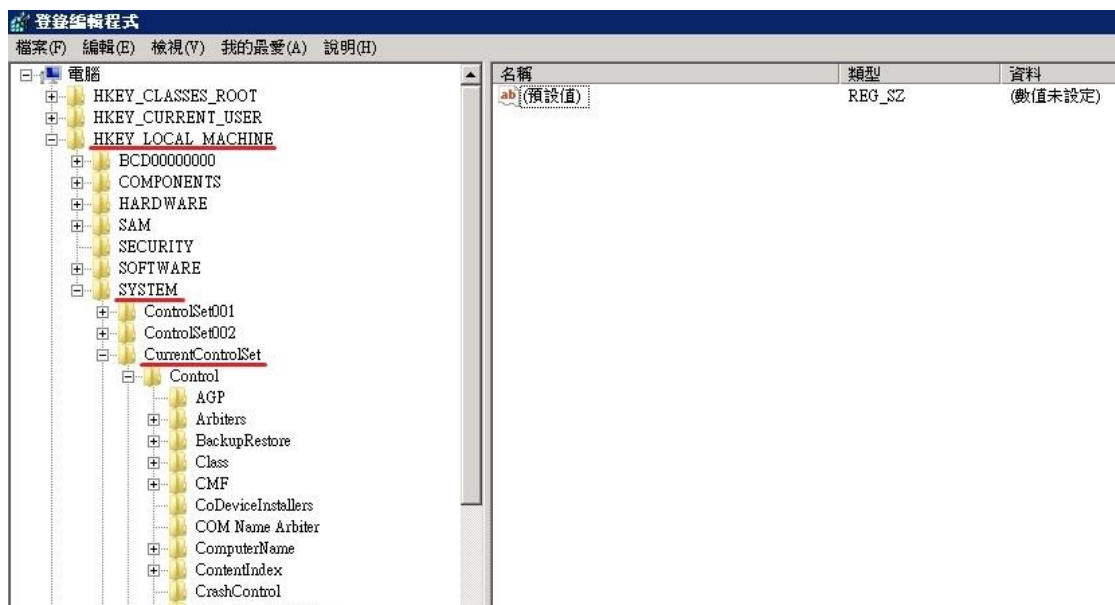
_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_RC4_128_MD5,SSL_CK_RC4_128_WITH_MD5,SSL_CK_DES_192_EDE3_CBC_WITH_MD5,TLS_RSA_WITH_NULL_MD5,TLS_RSA_WITH_NULL_SHA



四、開啟登錄檔編輯程式。



五、依照下圖進行登錄檔編輯。



登錄編輯程式

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128
 RC4 56/128
 RC4 64/128

登錄編輯程式

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128
 RC4 56/128

登錄編輯程式

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128
 RC4 56/128
 RC4 64/128

登錄編輯程式

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128

登錄編輯程式

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

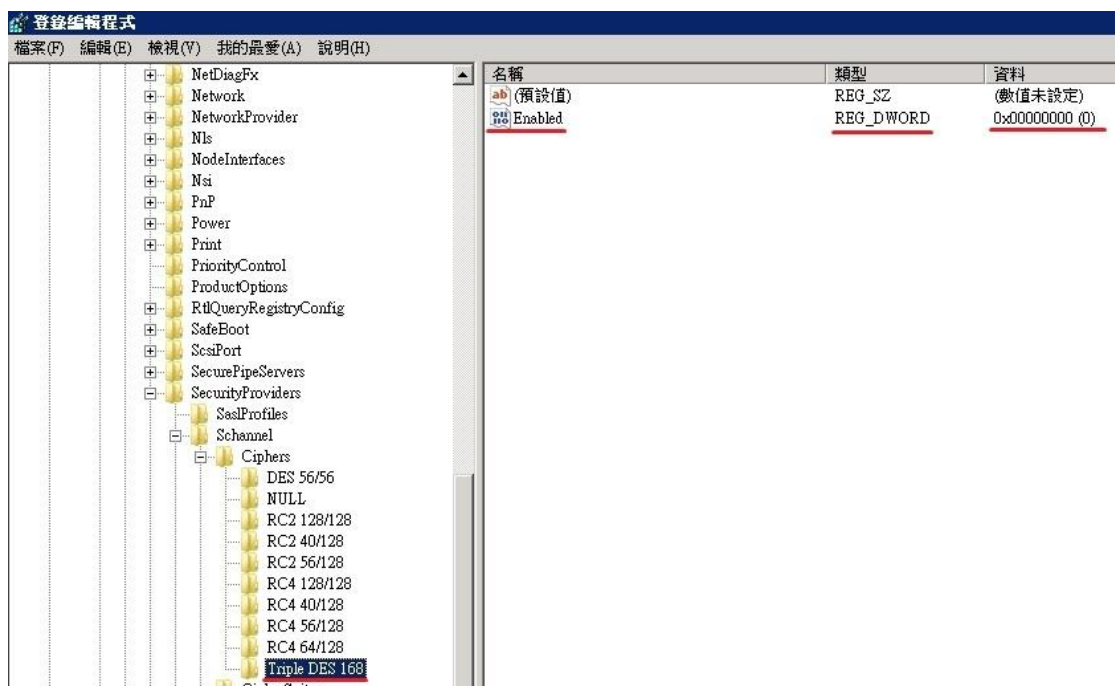
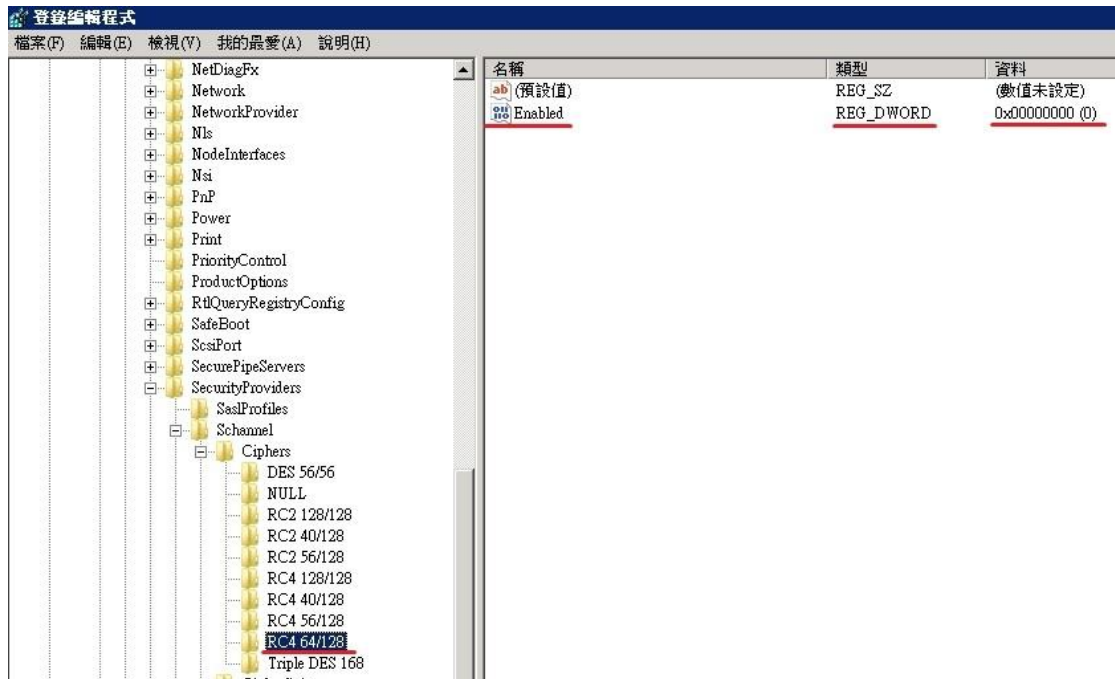
NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128
 RC4 56/128
 RC4 64/128

登錄編輯程式

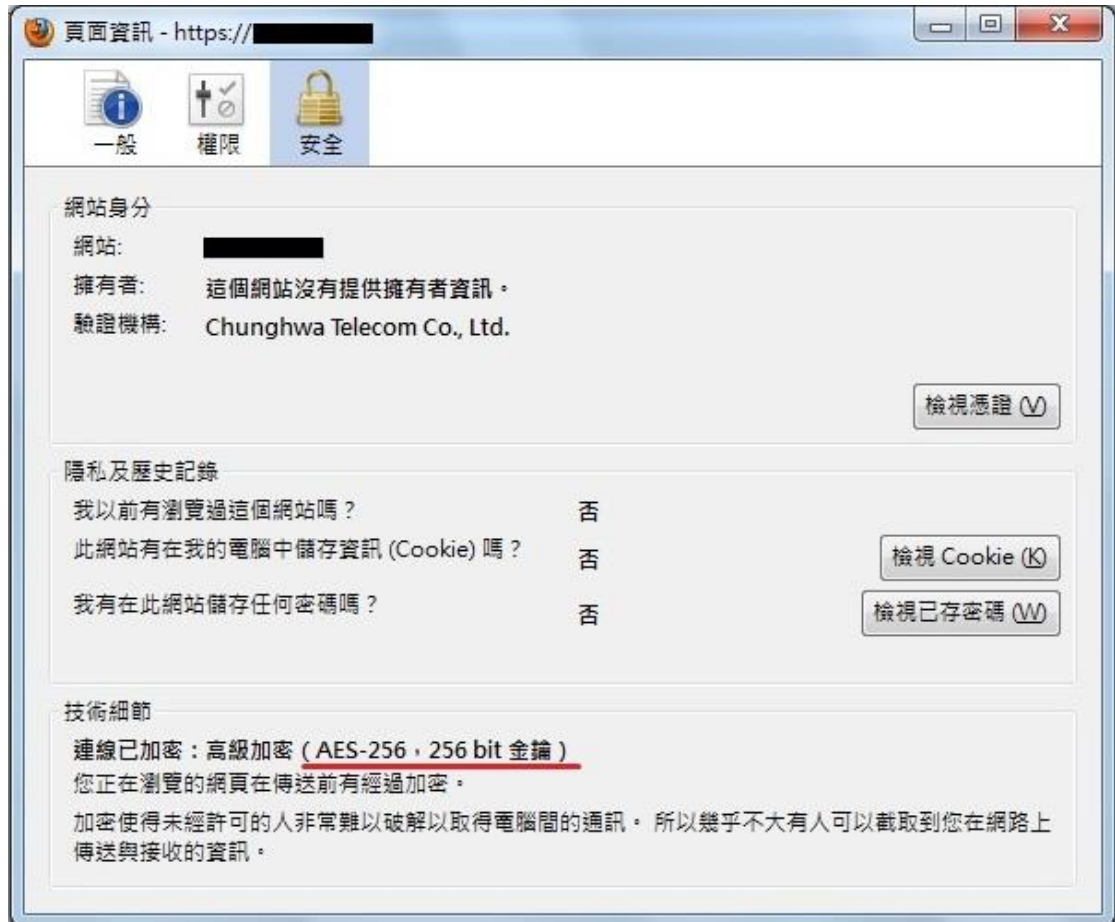
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)

名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)
Enabled	REG_DWORD	0x00000000 (0)

NetDiagFx
 Network
 NetworkProvider
 Nls
 NodeInterfaces
 Nsi
 PnP
 Power
 Print
 PriorityControl
 ProductOptions
 RtlQueryRegistryConfig
 SafeBoot
 ScsiPort
 SecurePipeServers
 SecurityProviders
 SaslProfiles
 Schannel
 Ciphers
 DES 56/56
 NULL
 RC2 128/128
 RC2 40/128
 RC2 56/128
 RC4 128/128
 RC4 40/128
 RC4 56/128
 RC4 64/128
 Triple DES 168



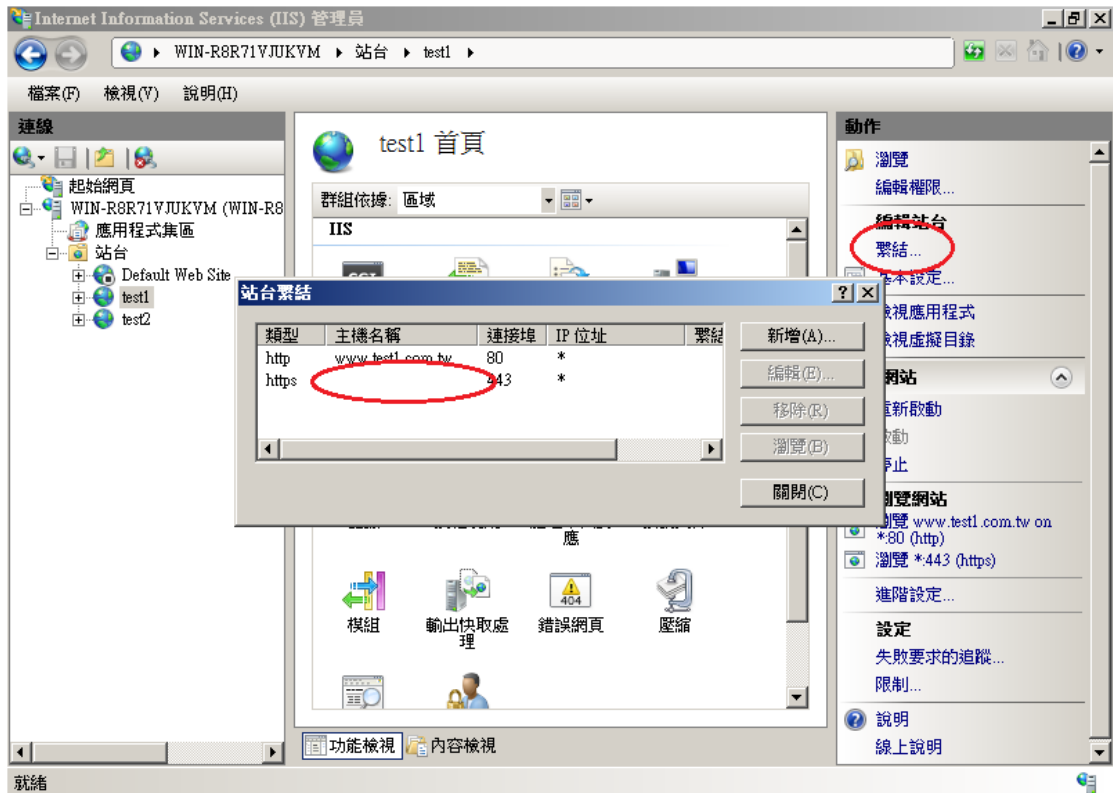
六、設定完成後，重開機，即可達到 AES 256 位元的加密效果。



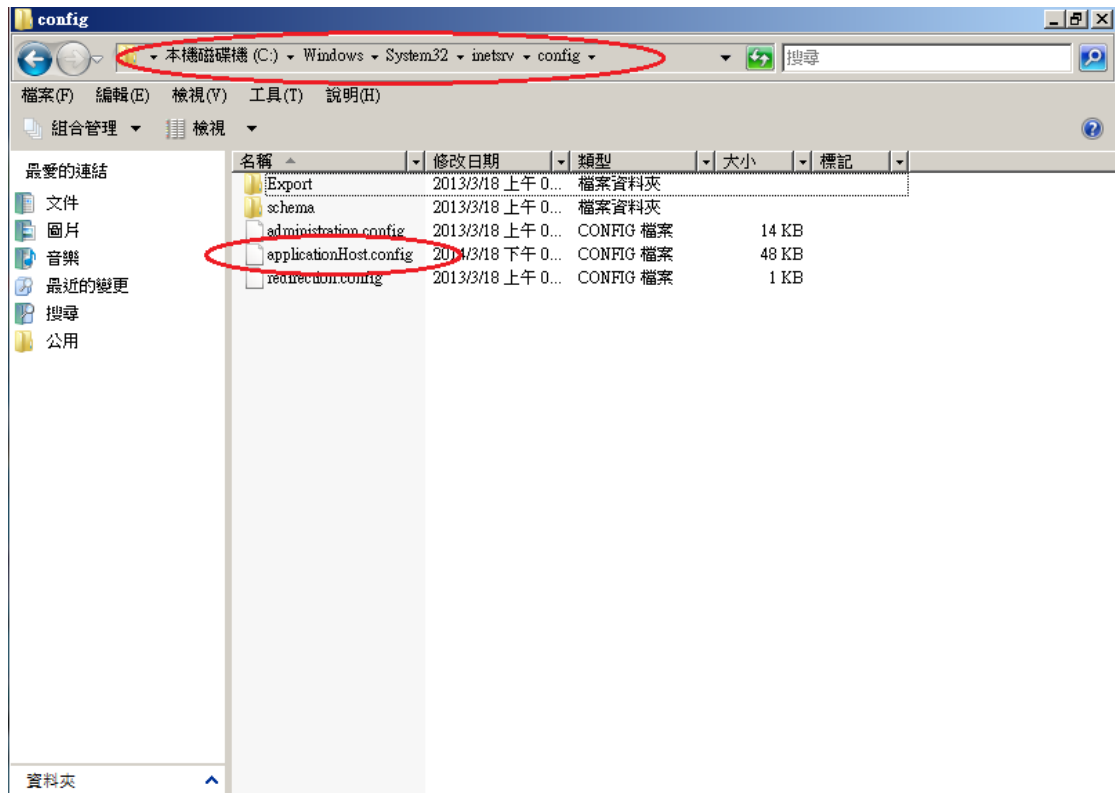
附件二：單一 IP，多站台啟用 SSL

IIS7 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，即可在多個網站上啟用 443 port。

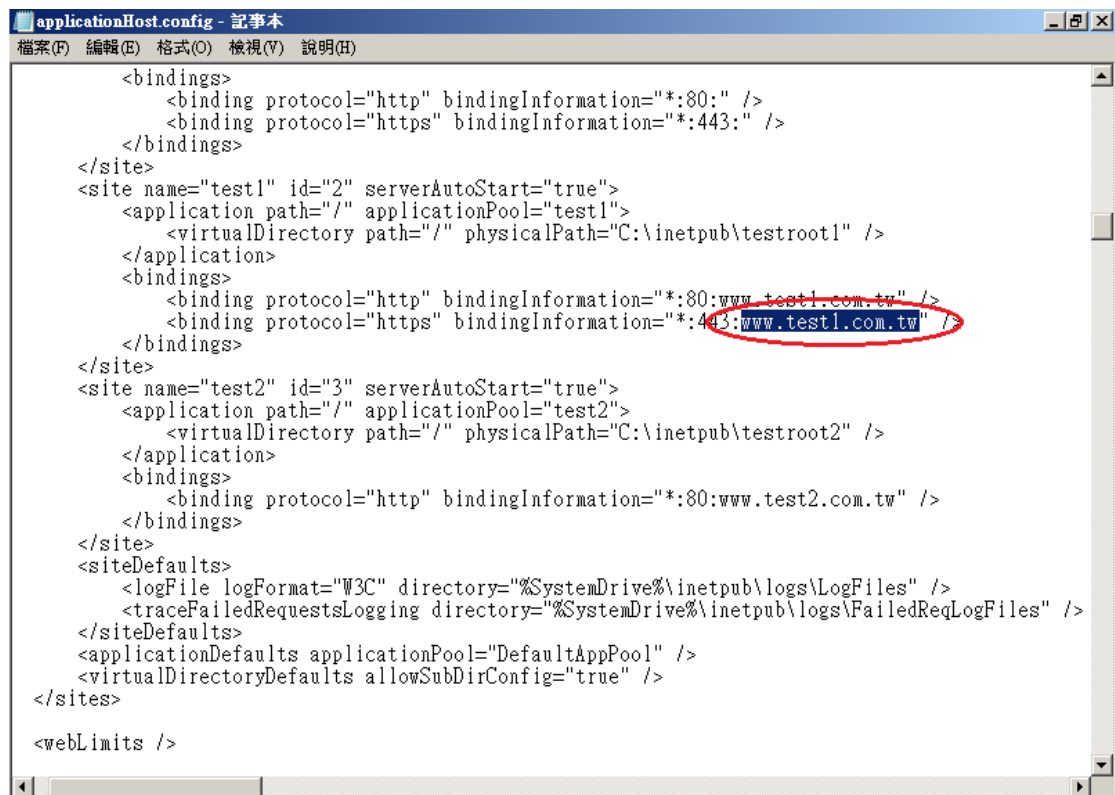
- 一、依照前述的憑證安裝步驟，先在其中一網站上安裝憑證，並以 HTTPS 測試連線是否正常。
- 二、再點選 1 次「繫結」，會看到主機名稱下面是空的。



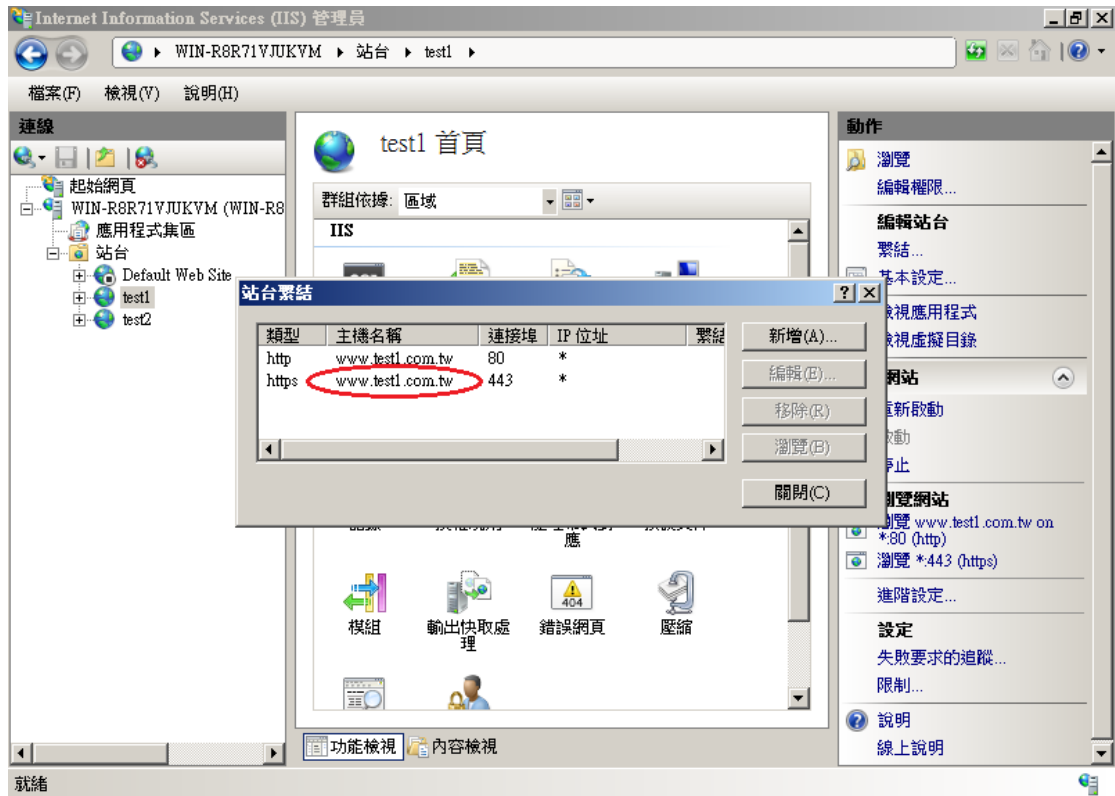
- 三、到以下目錄：「C:\Windows\System32\inetsrv\config」，以記事本開啟「applicationHost.config」



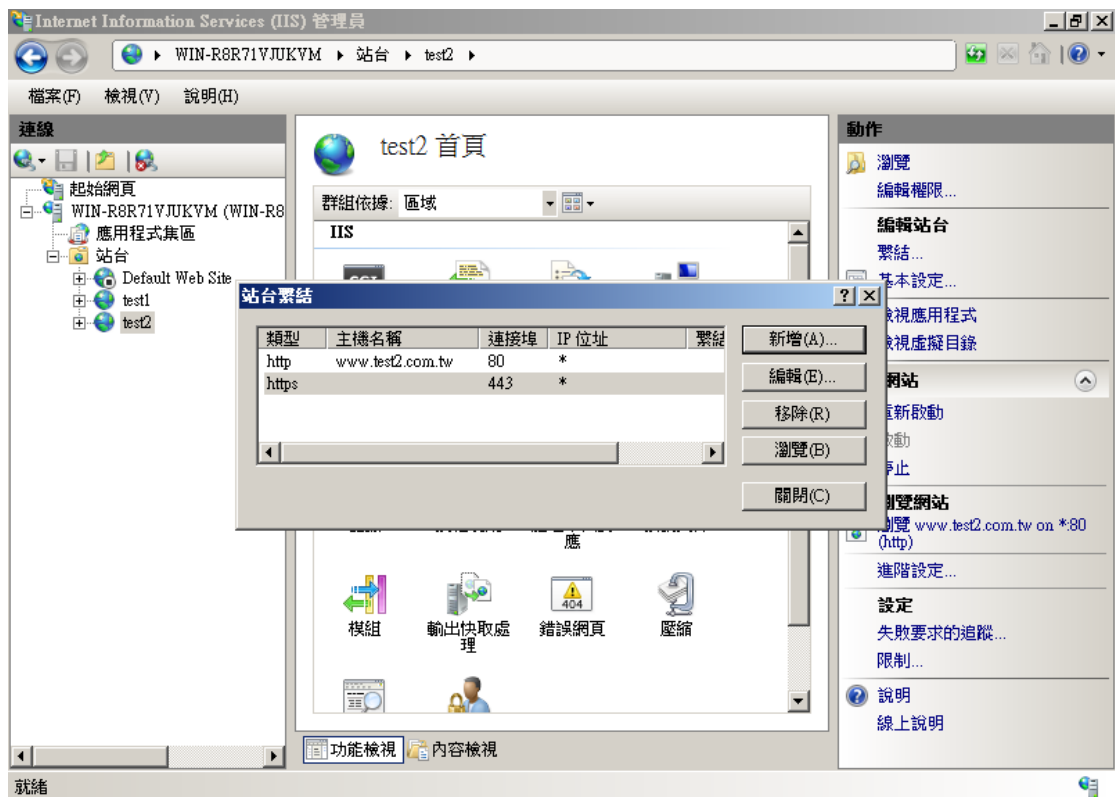
四、找到剛剛有新增 443 port 的網站後，將 domain name 加入 443：之後，存檔並關閉，如圖。



五、回 IIS 管理員，重新點選「繫結」，會看到主機名稱下出現之前輸入的 domain name，這樣即表示修改成功。



六、接著，可以先將第 2 個網站新增 443 port 以及掛上憑證，同樣去修改「applicationHost.config」

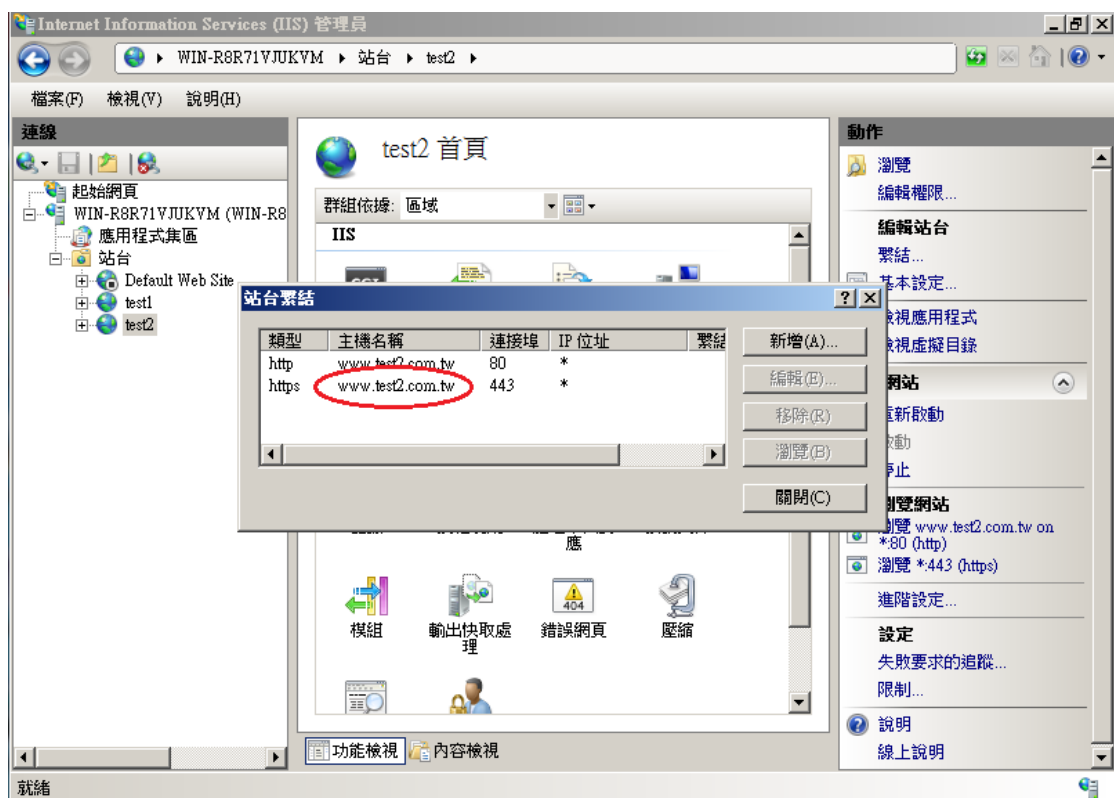


```
applicationHost.config - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

ding protocol="https" bindingInformation="*:443:" />
</s>

test1" id="2" serverAutoStart="true">
  <binding path="/" applicationPool="test1">
    <physicalDirectory path="/" physicalPath="C:\inetpub\testroot1" />
  </binding>
</s>
<binding protocol="http" bindingInformation="*:80:www.test1.com.tw" />
<binding protocol="https" bindingInformation="*:443:www.test1.com.tw" />
</s>

test2" id="3" serverAutoStart="true">
  <binding path="/" applicationPool="test2">
    <physicalDirectory path="/" physicalPath="C:\inetpub\testroot2" />
  </binding>
</s>
<binding protocol="http" bindingInformation="*:80:www.test2.com.tw" />
<binding protocol="https" bindingInformation="*:443:www.test2.com.tw" />
</s>
```



七、其他需要掛上憑證的網站依照上述步驟操作。完成後，請以 HTTPS 連線測試，是否所有網站皆正常。