中華電信通用憑證管理中心（PublicCA）

Windows Server IIS 5、6、7、8、10 憑證備份與還原

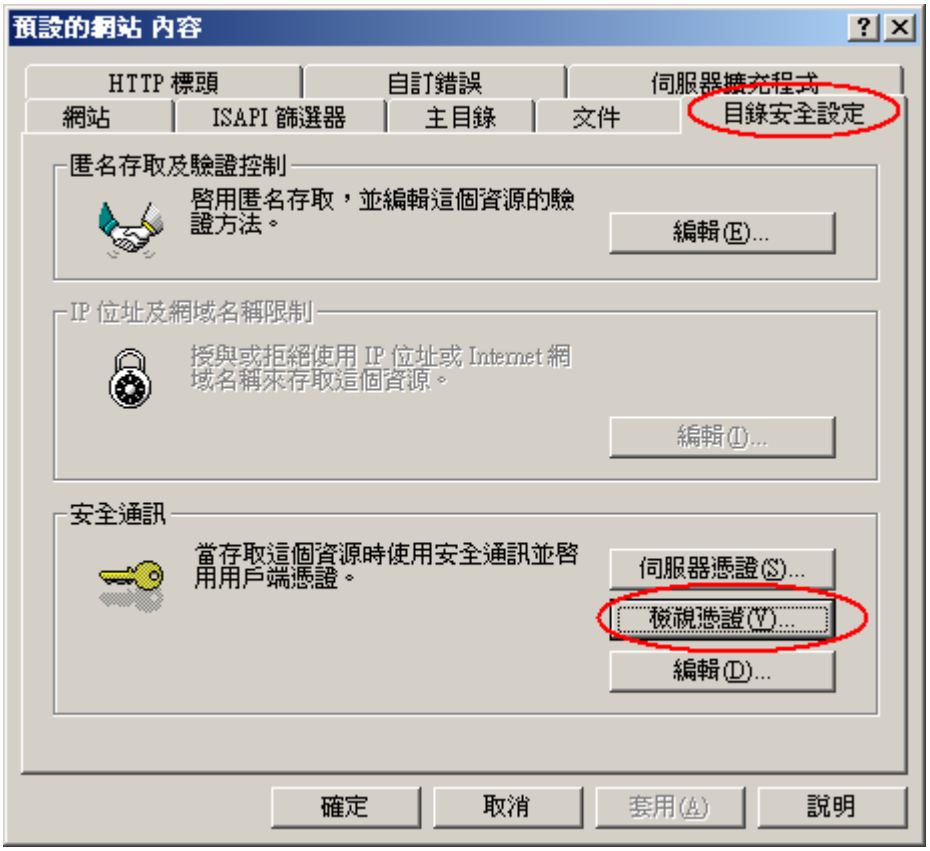
請依照您的Server(2003、2008、2012、2016)版本，參考對應的憑證備份與還原步驟。

目錄

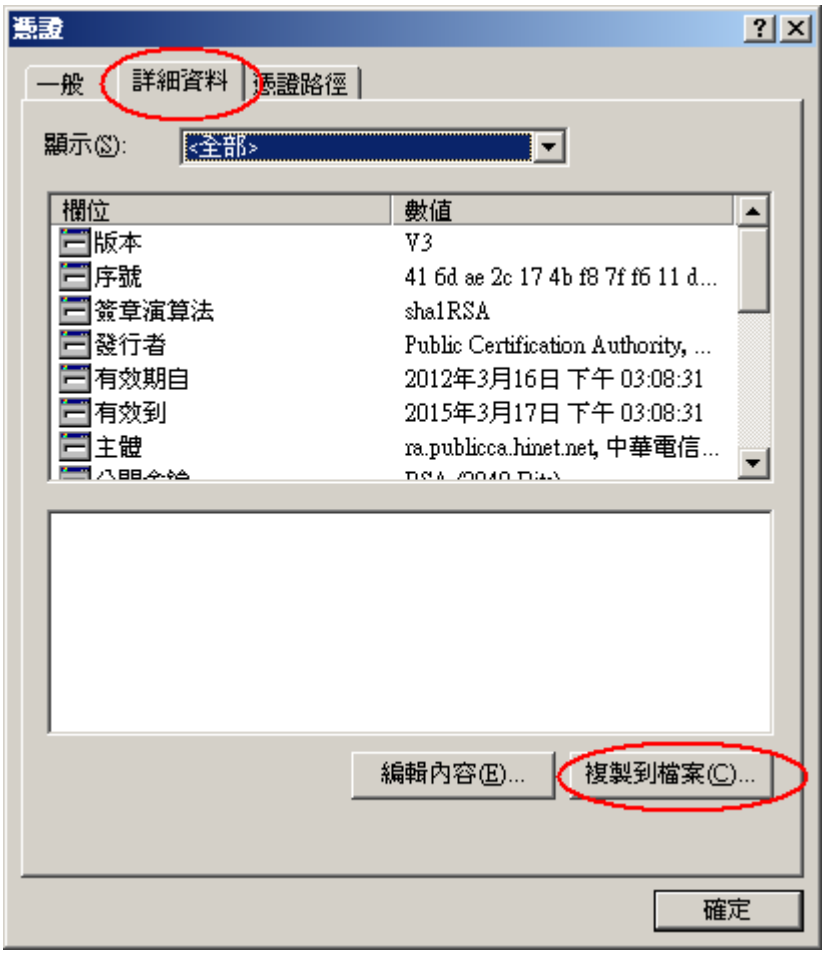
憑證備份步驟

Windows Server 2003

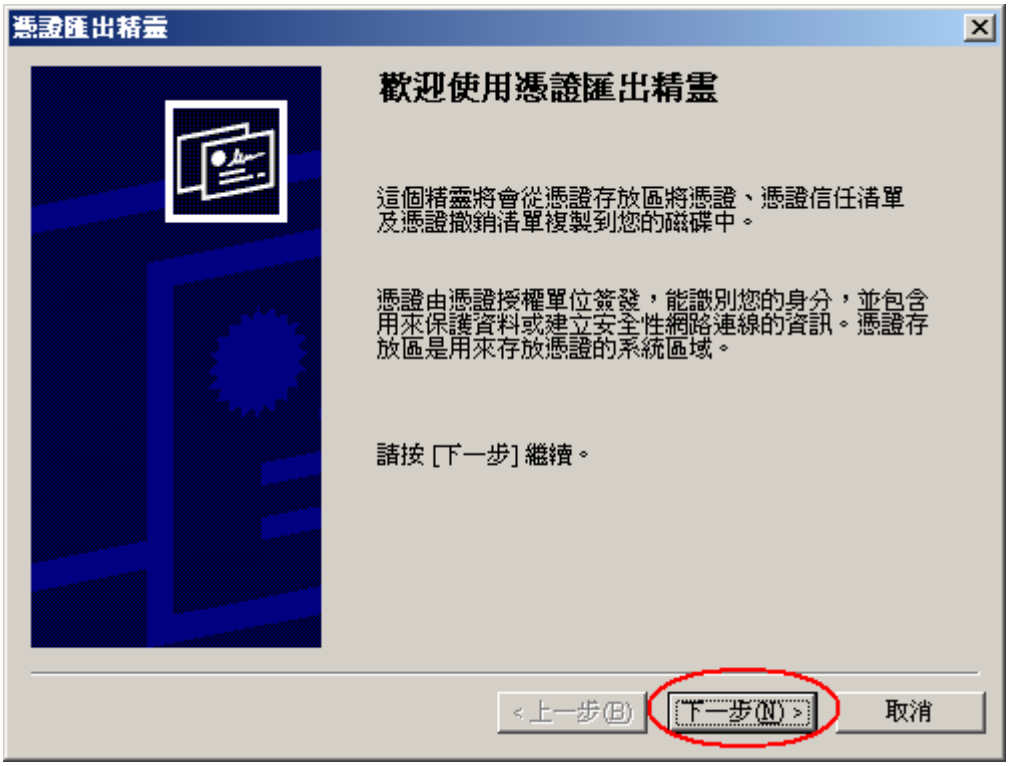
1. 「開始」→「設定」→「控制台」→「系統管理工具」→「Internet 服務管理員」→點選服務站台(滑鼠右鍵、選內容) →「目錄安全設定」→「檢視憑證」。



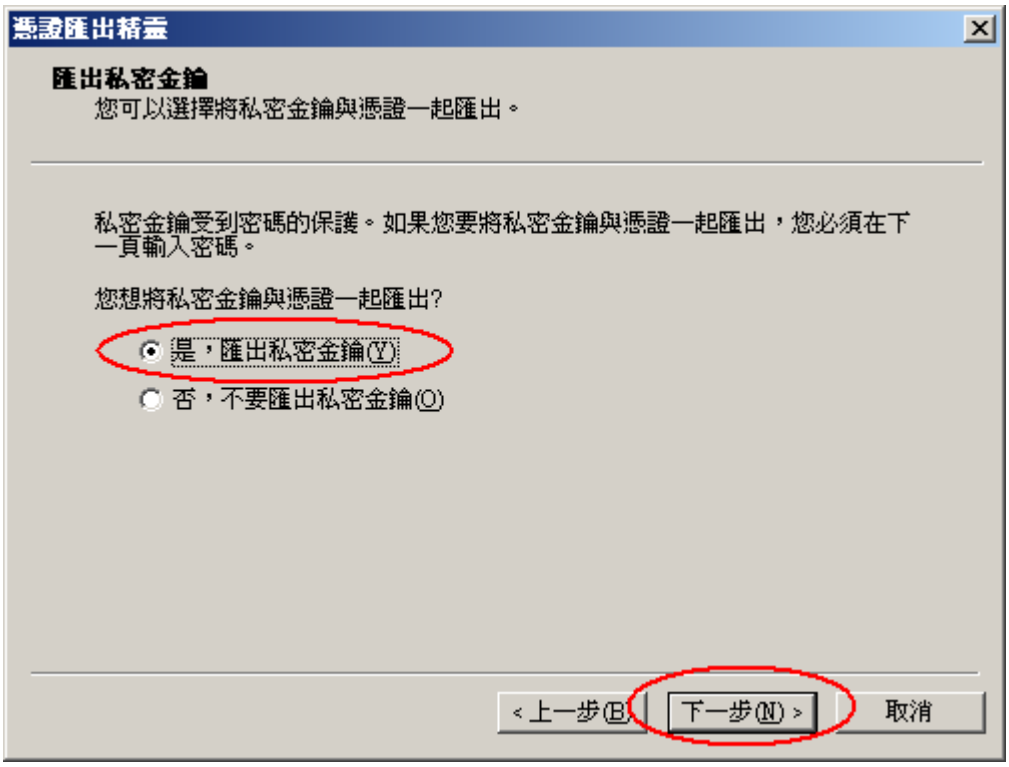
2. 點選「詳細資料」→「複製到檔案」。



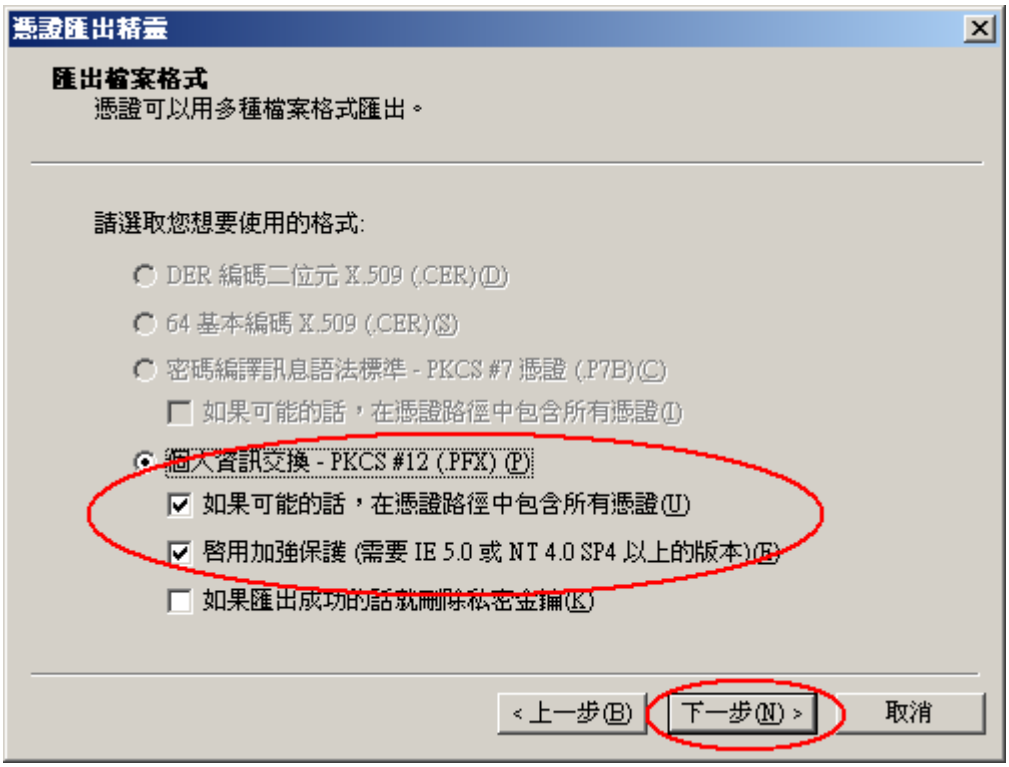
3. 點選「下一步」



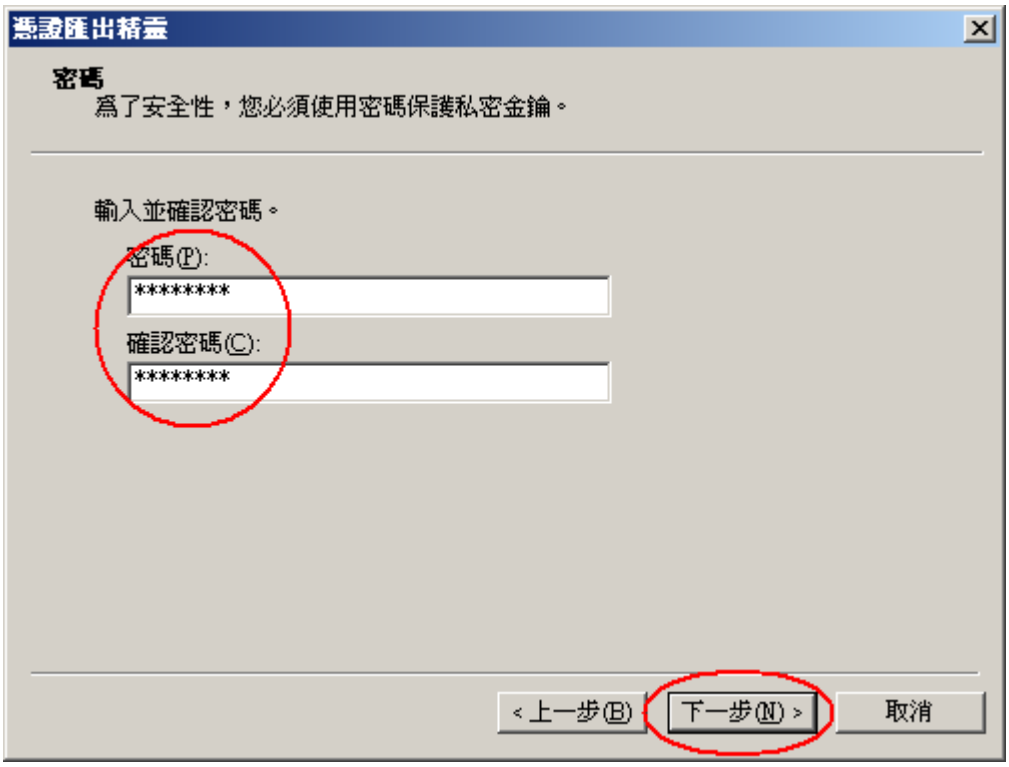
4. 選擇 「匯出私密金鑰」→「下一步」



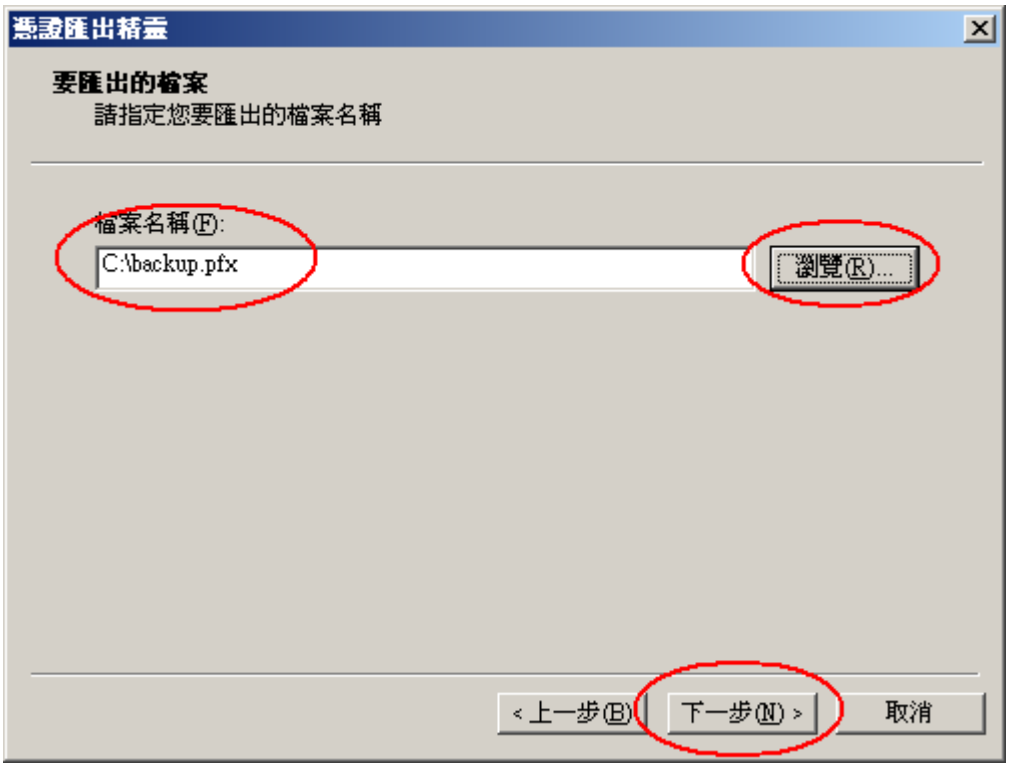
5. 選擇「啟用加強保護」



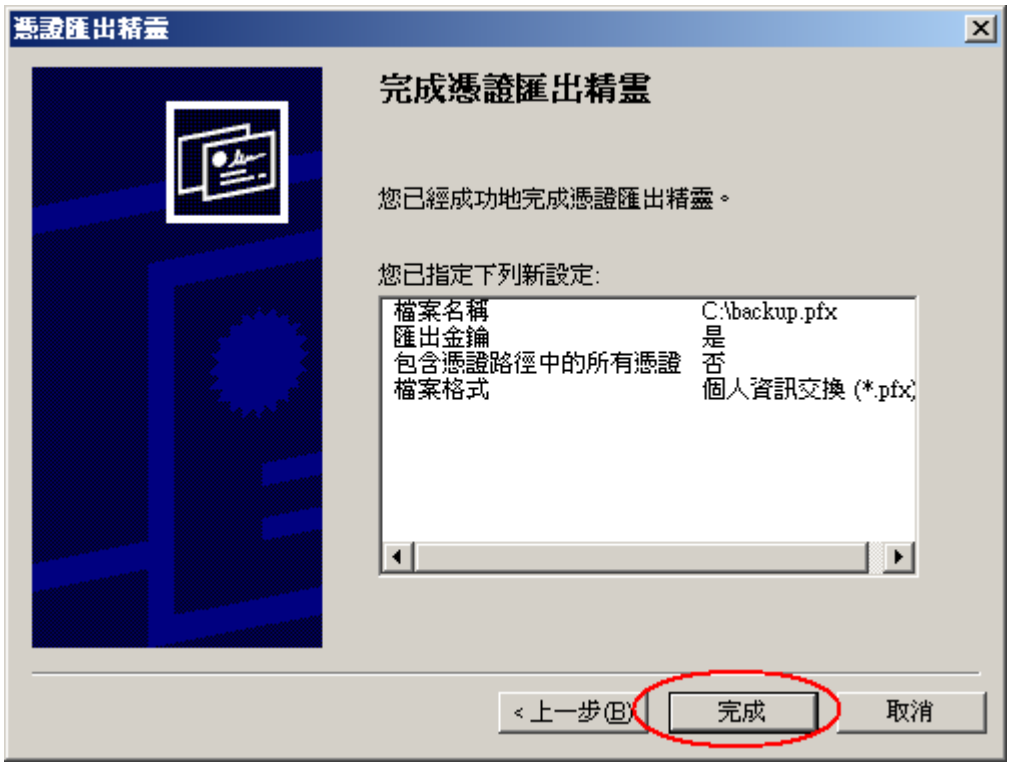
6. 輸入密碼保護



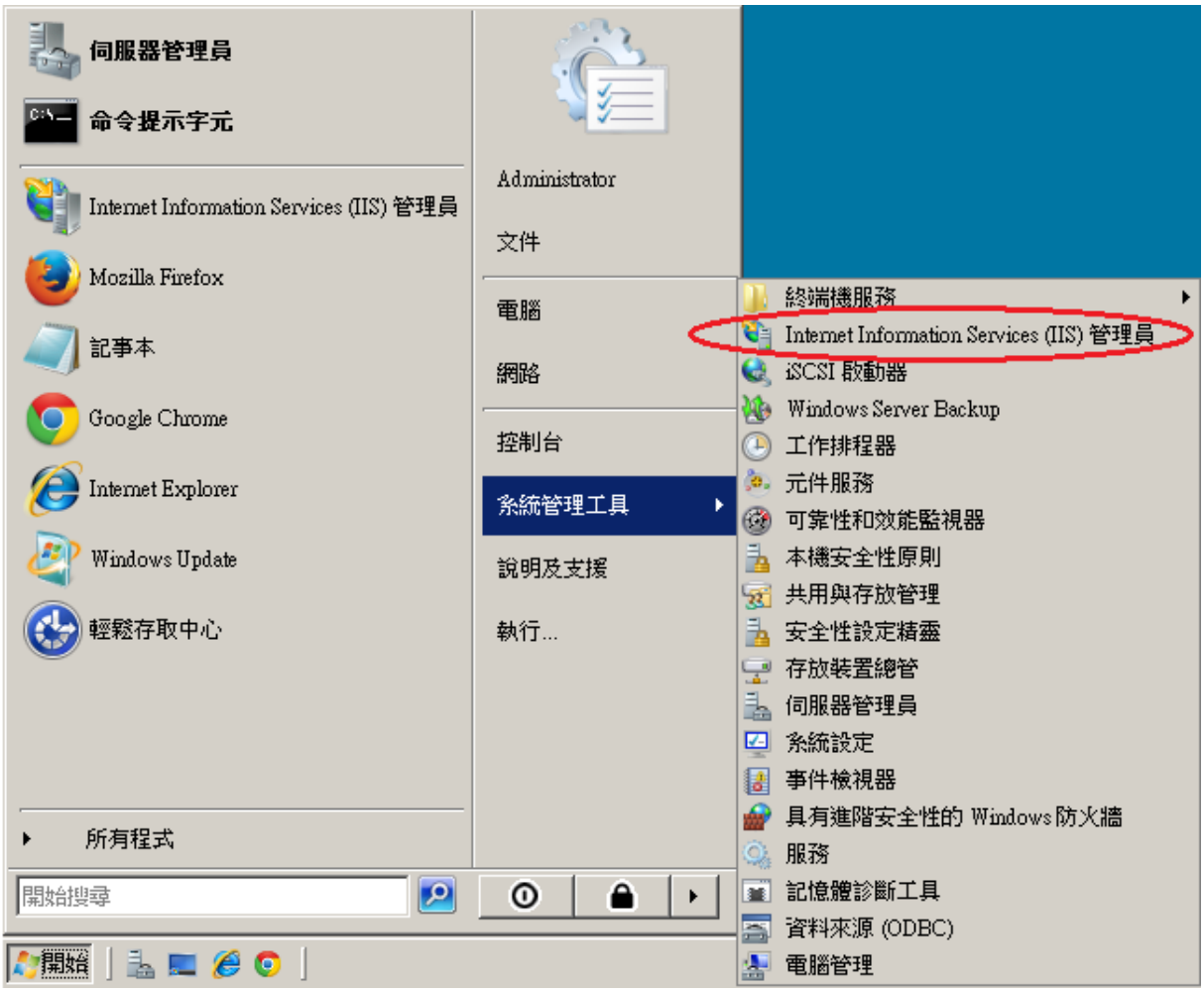
7. 輸入自定檔案名稱*.PFX



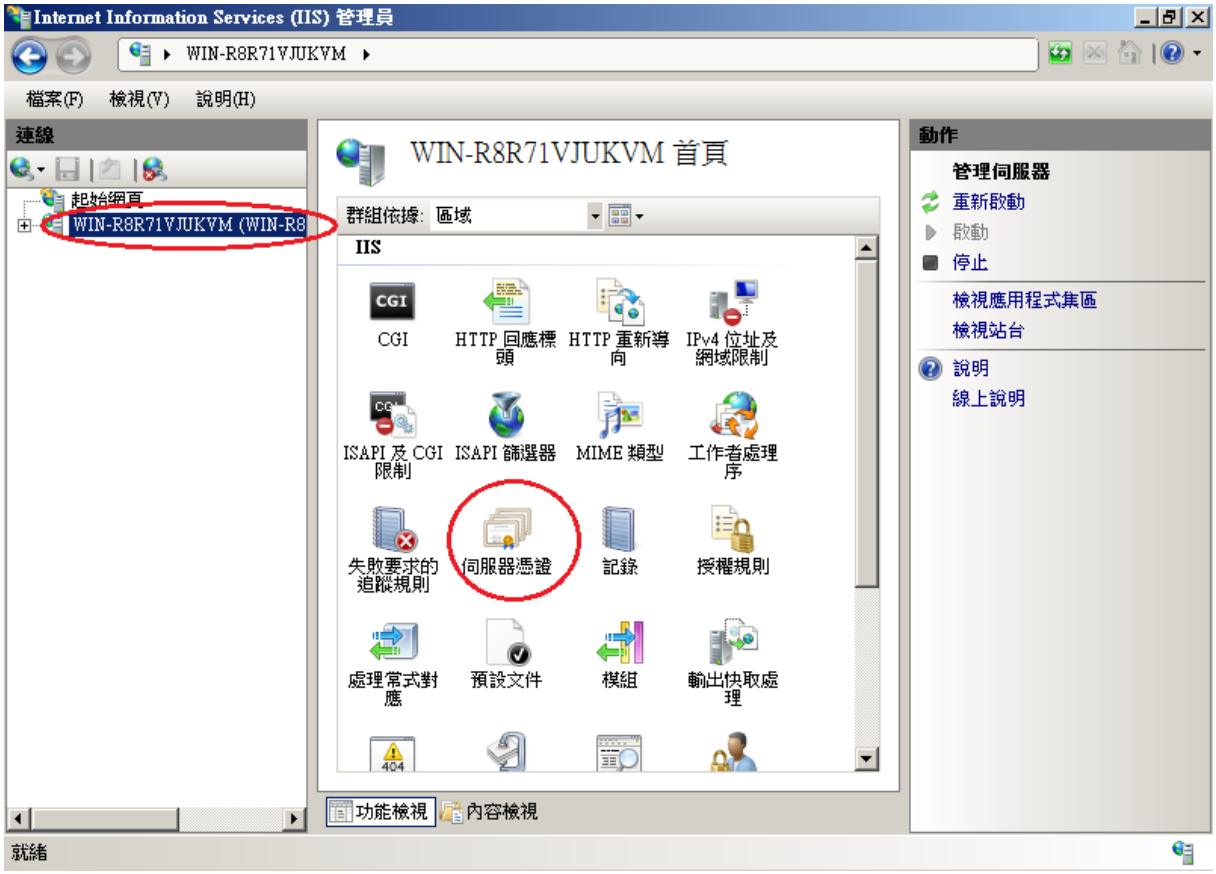
8. 完成匯出憑證


憑證匯出精靈
完成憑證匯出精靈
您已經成功地完成憑證匯出精靈。
您已指定下列新設定:
檔案名稱 C:\backup.pfx
匯出金鑰 是
包含憑證路徑中的所有憑證 否
檔案格式 個人資訊交換 (*.pfx)
< 上一步(B)
完成
取消

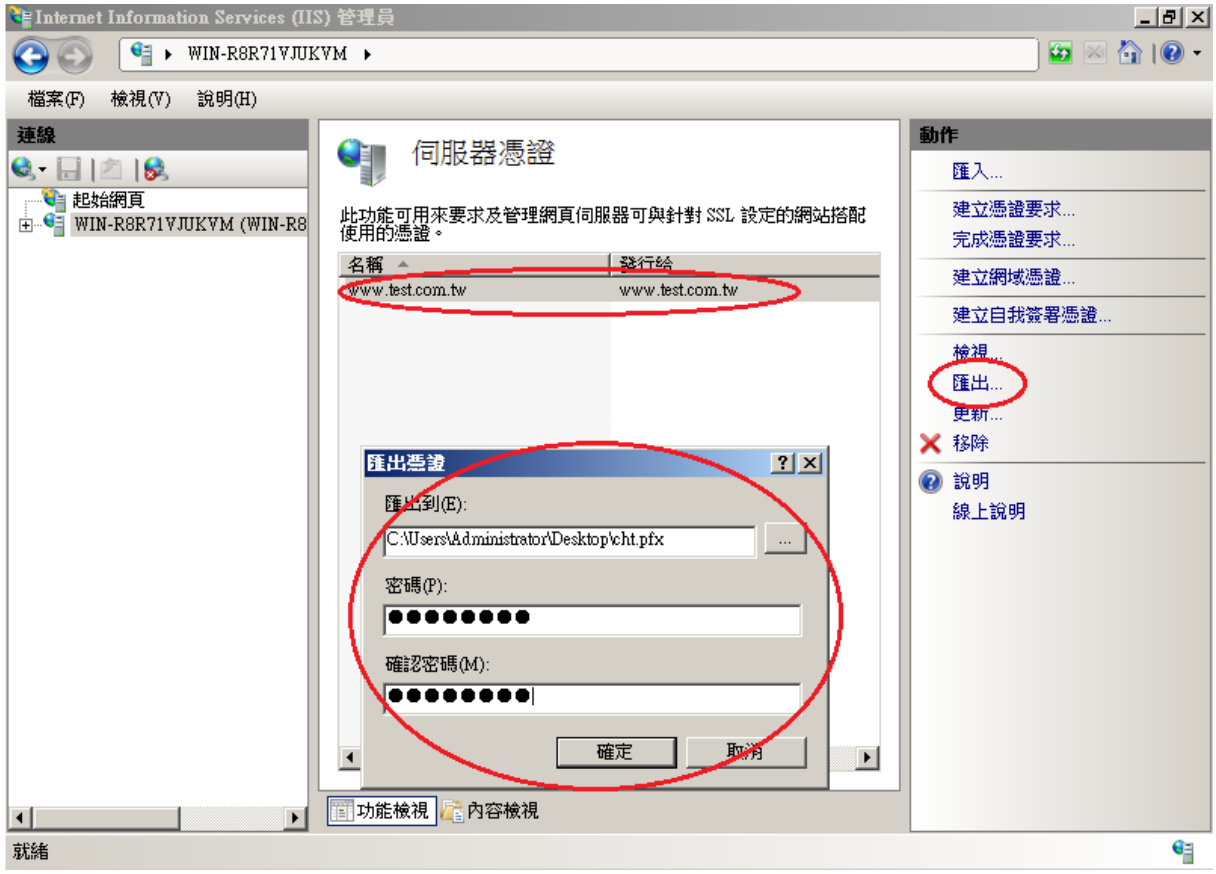
1．點選 「開始」→ 「系統管理工具」→「Internet Information Services (IIS)管理員」。



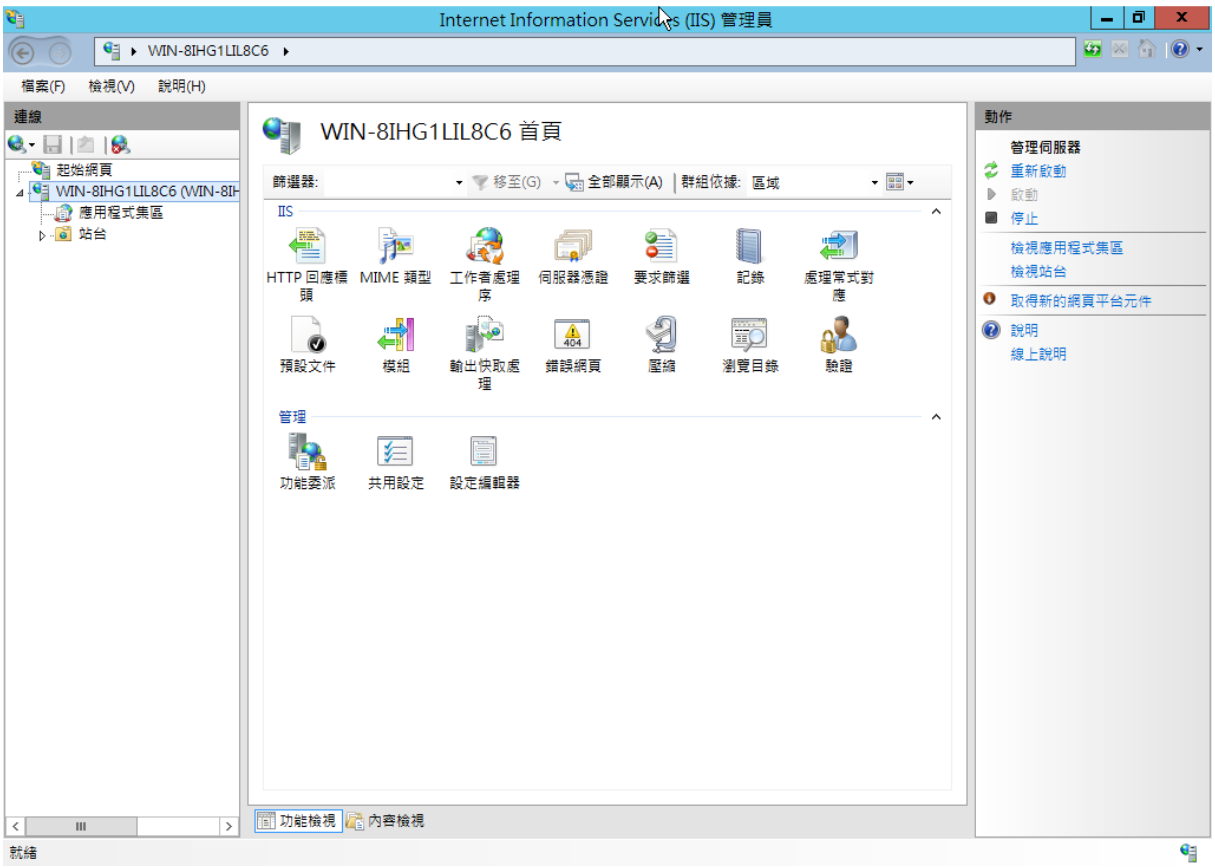
2．在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



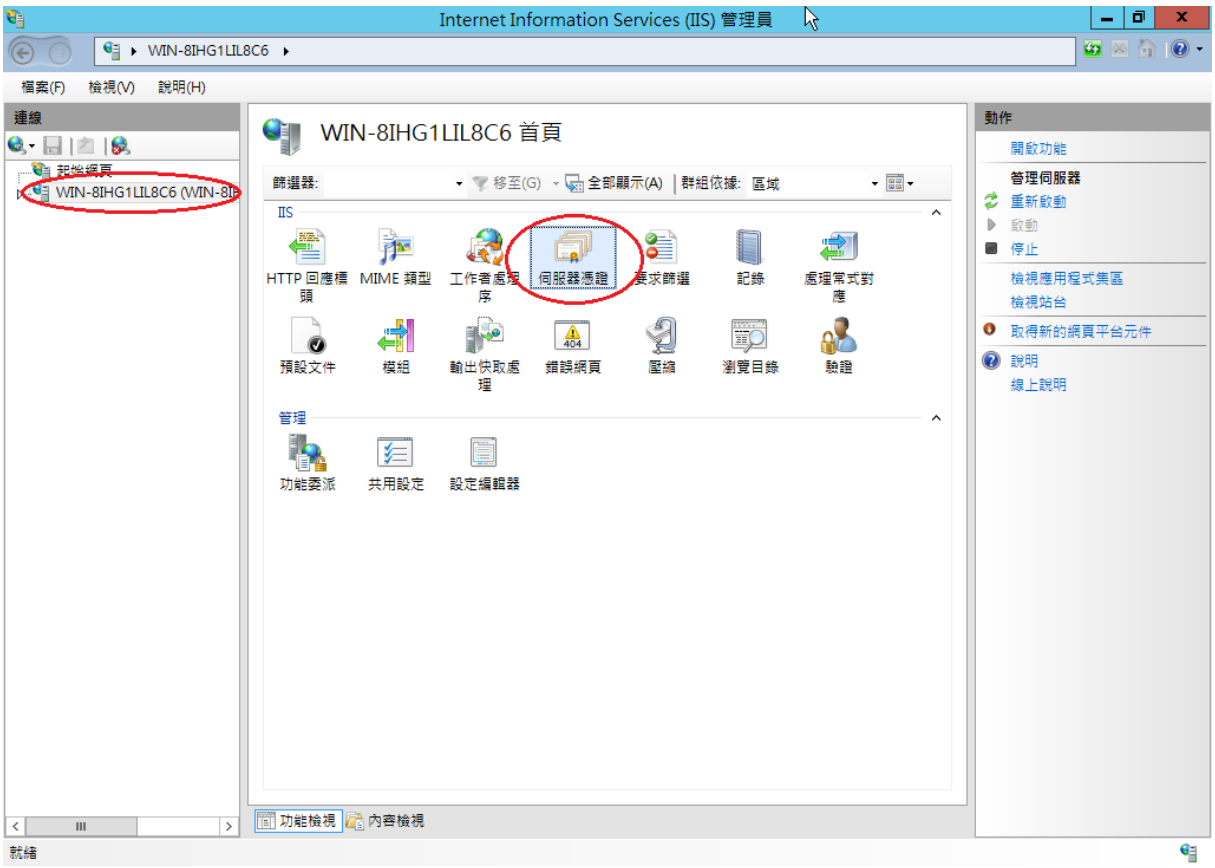
3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。



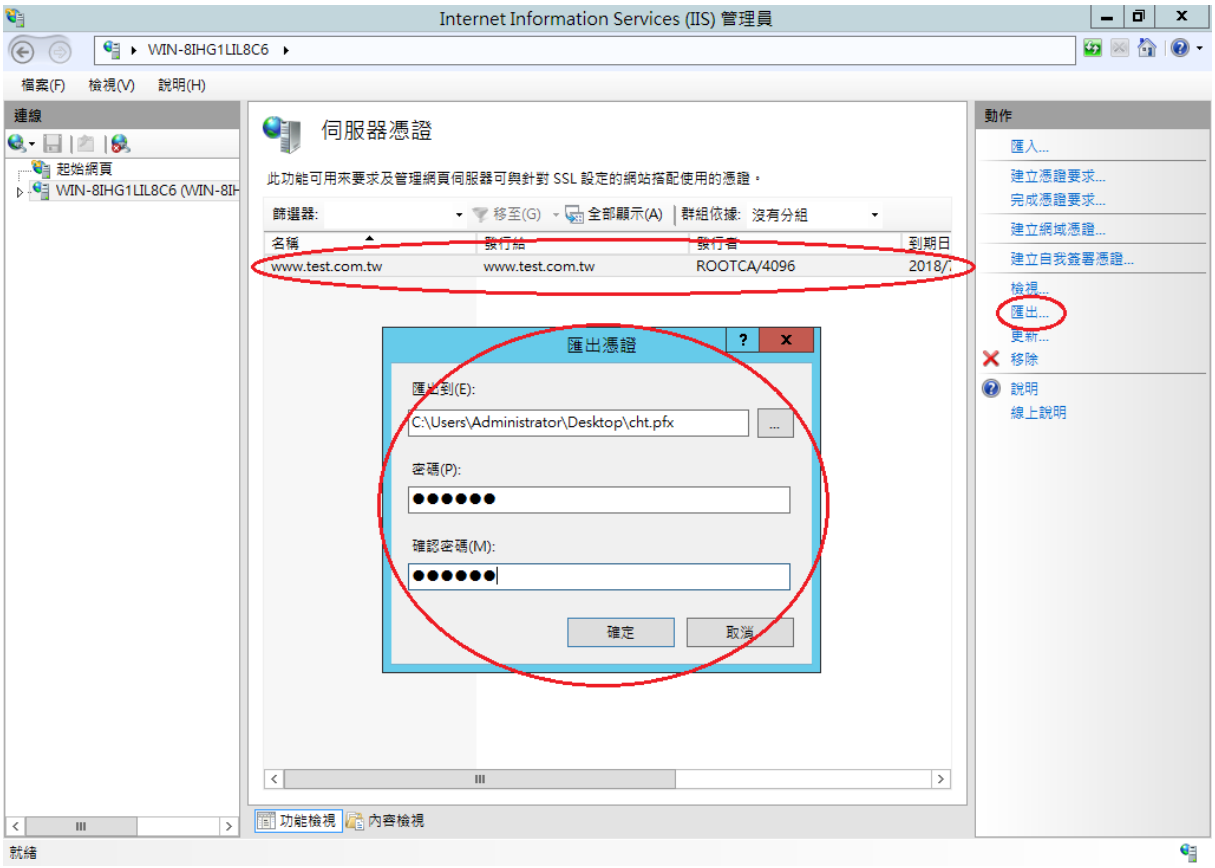
1. 開啟「Internet Information Services (IIS)管理員」。



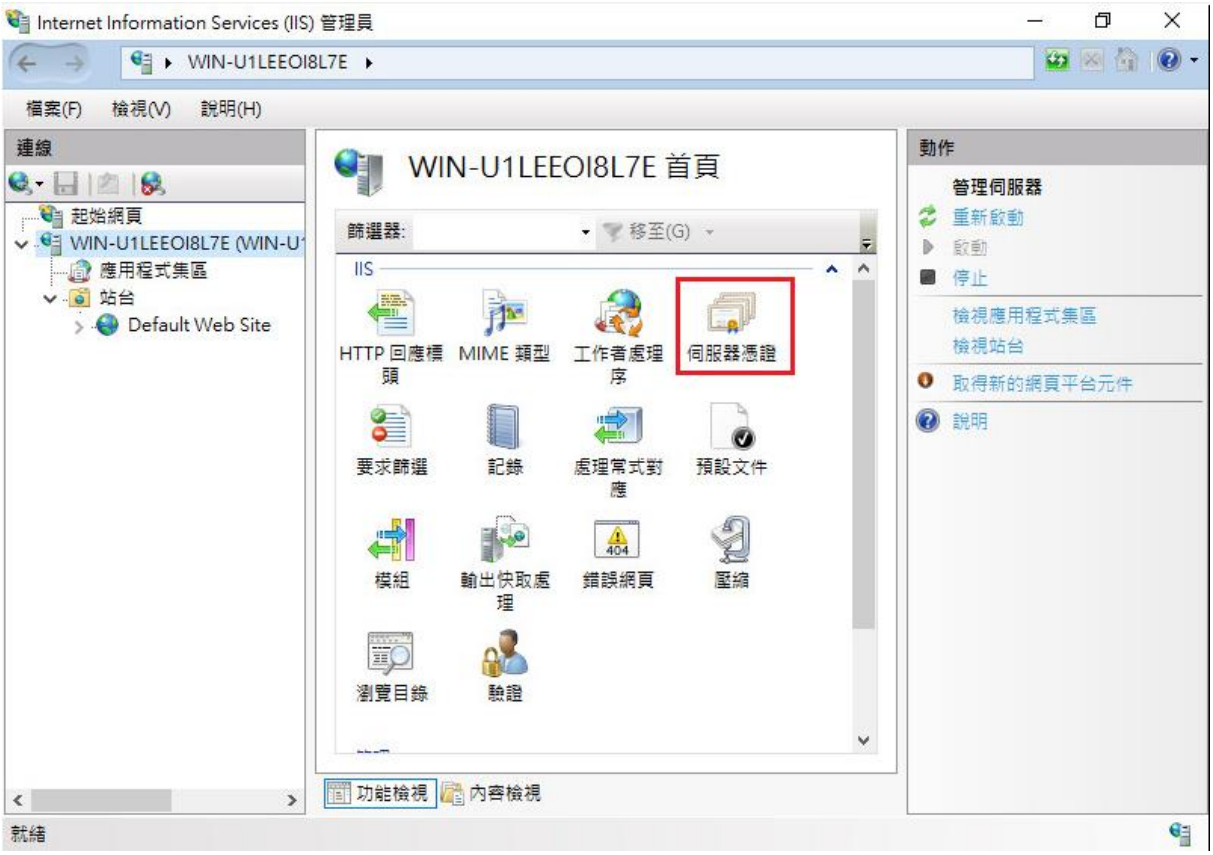
2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



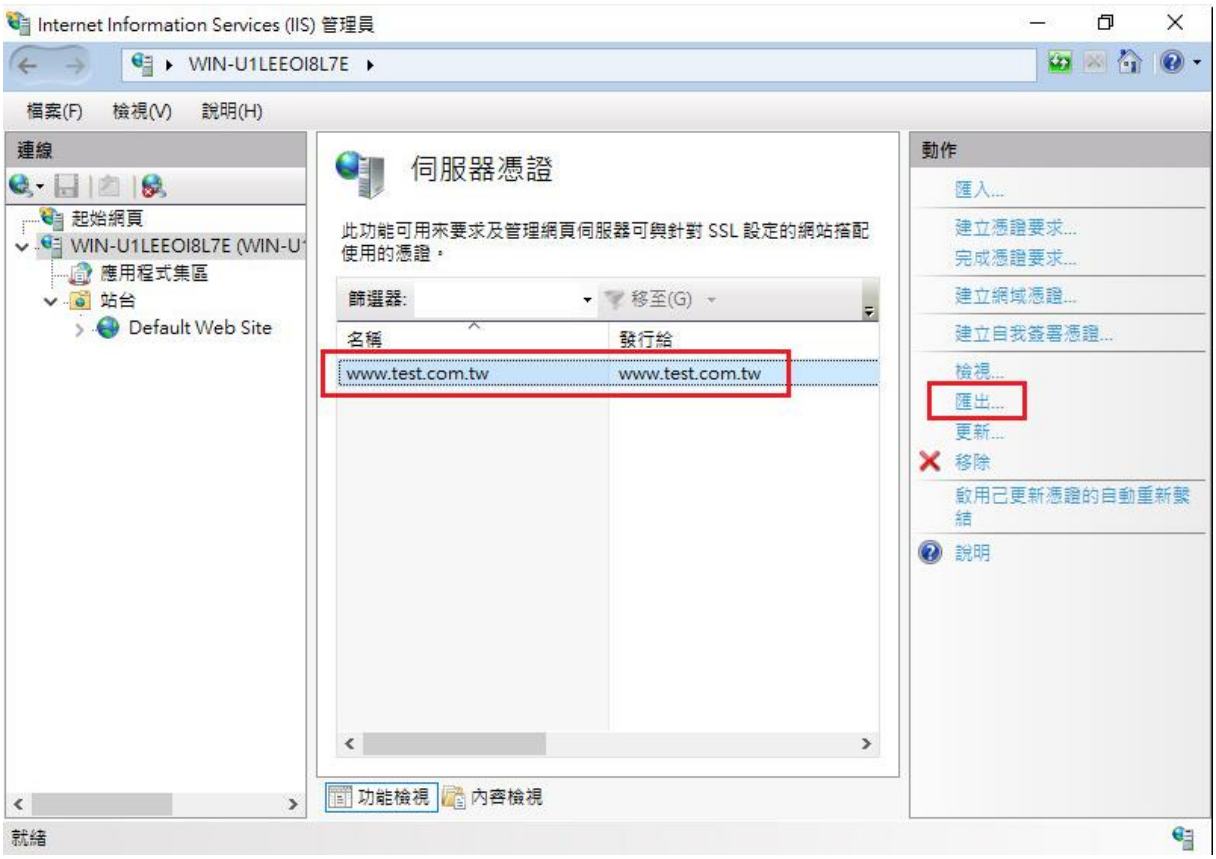
3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

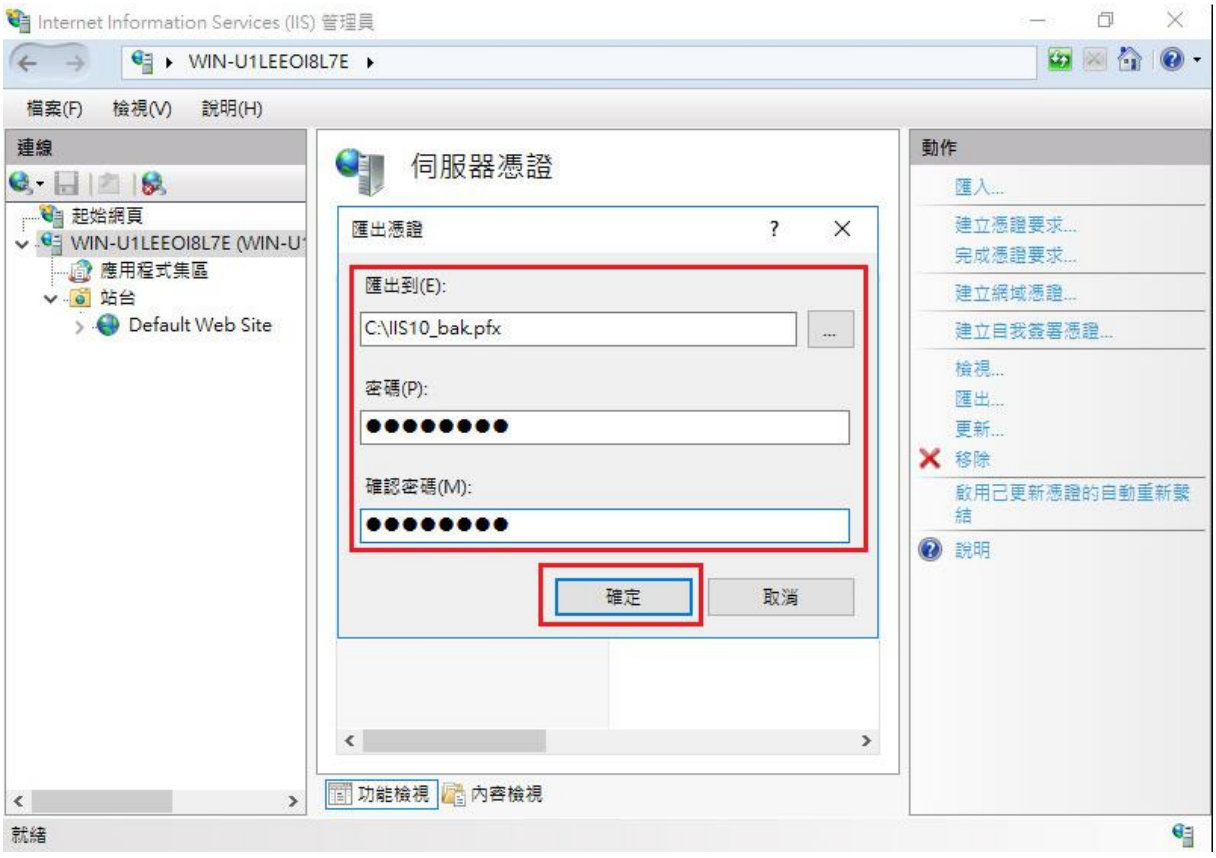


1. 開啟「Internet Information Services (IIS)管理員」。
2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

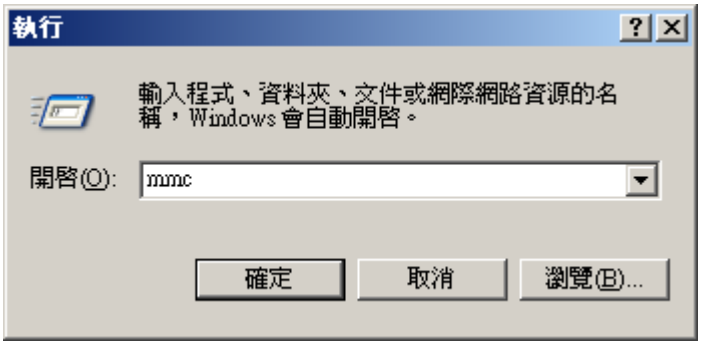

Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U1
應用程式集區
站台
Default Web Site
伺服器憑證
此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。
篩選器:
移至(G)
名稱
發行給
www.test.com.tw
www.test.com.tw
功能檢視
內容檢視
就緒
動作
匯入...
建立憑證要求...
完成憑證要求...
建立網域憑證...
建立自我簽署憑證...
檢視...
匯出...
更新...
移除
啟用已更新憑證的自動重新繫結
說明


Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U1
應用程式集區
站台
Default Web Site
伺服器憑證
匯出憑證
匯出到(E):
C:\IIS10_bak.pfx
...
密碼(P):
確認密碼(M):
確定
取消
功能檢視
內容檢視
就緒
動作
匯入...
建立憑證要求...
完成憑證要求...
建立網域憑證...
建立自我簽署憑證...
檢視...
匯出...
更新...
移除
啟用已更新憑證的自動重新繫結
說明

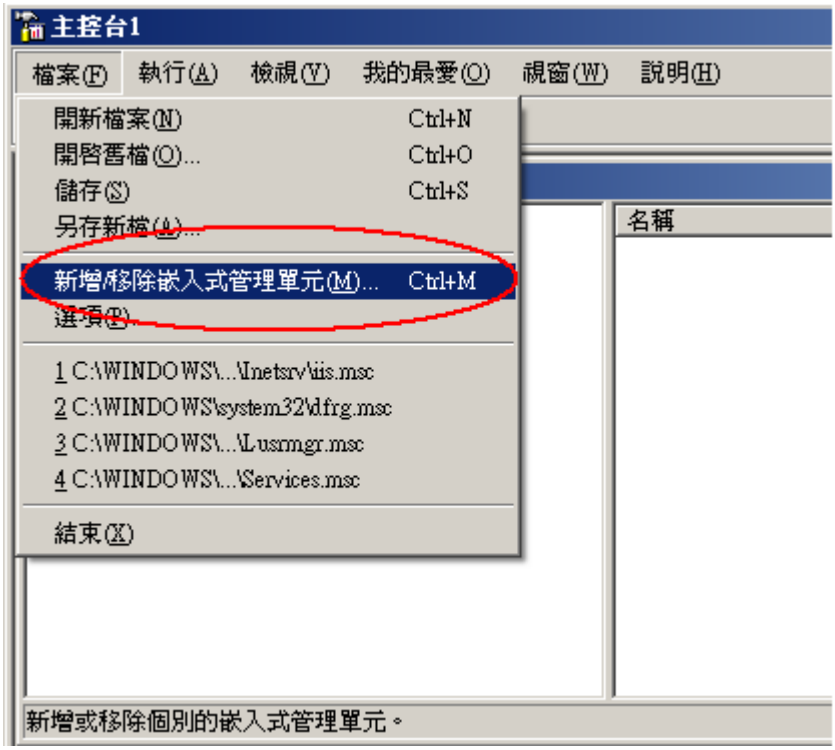
憑證還原步驟

Windows Server 2003

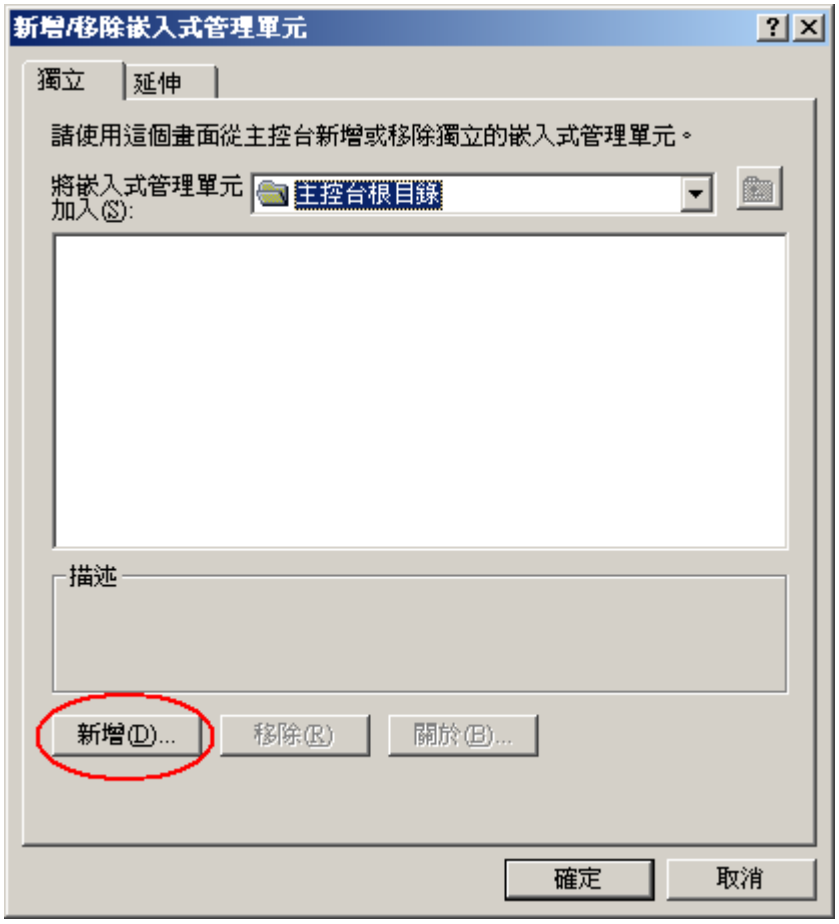
1. 由「開始」→執行→輸入 mmc，執行主控台



2. 進入主控台後，選擇「新增/移除嵌入式入式管理單元」

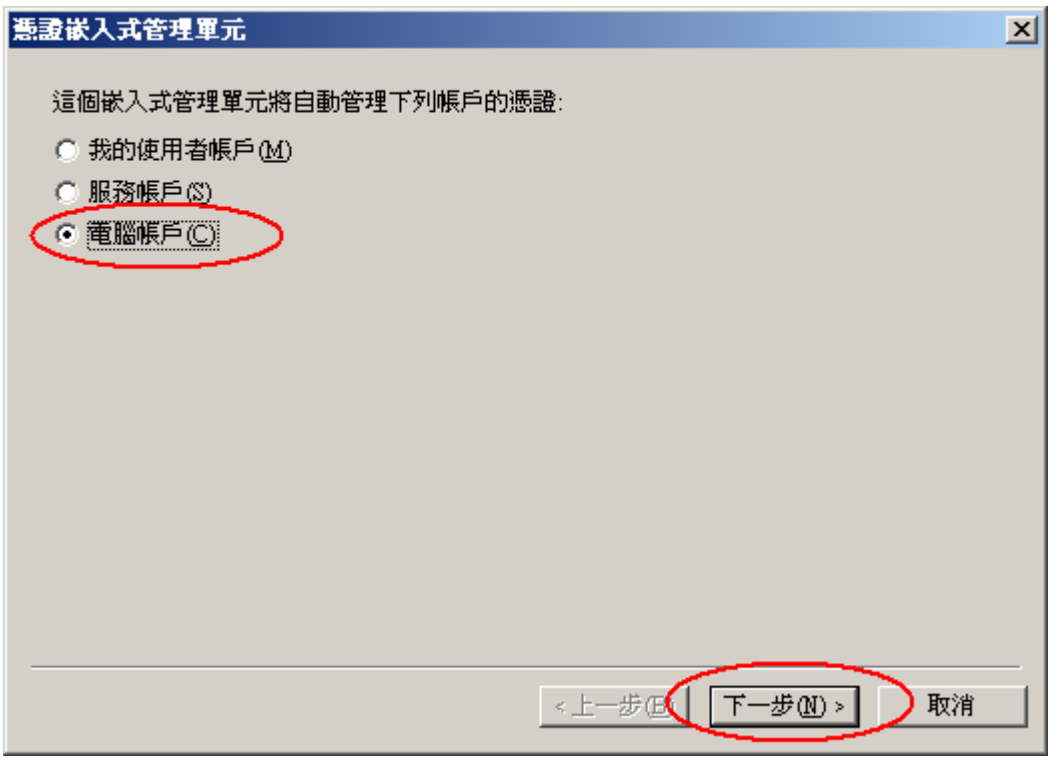


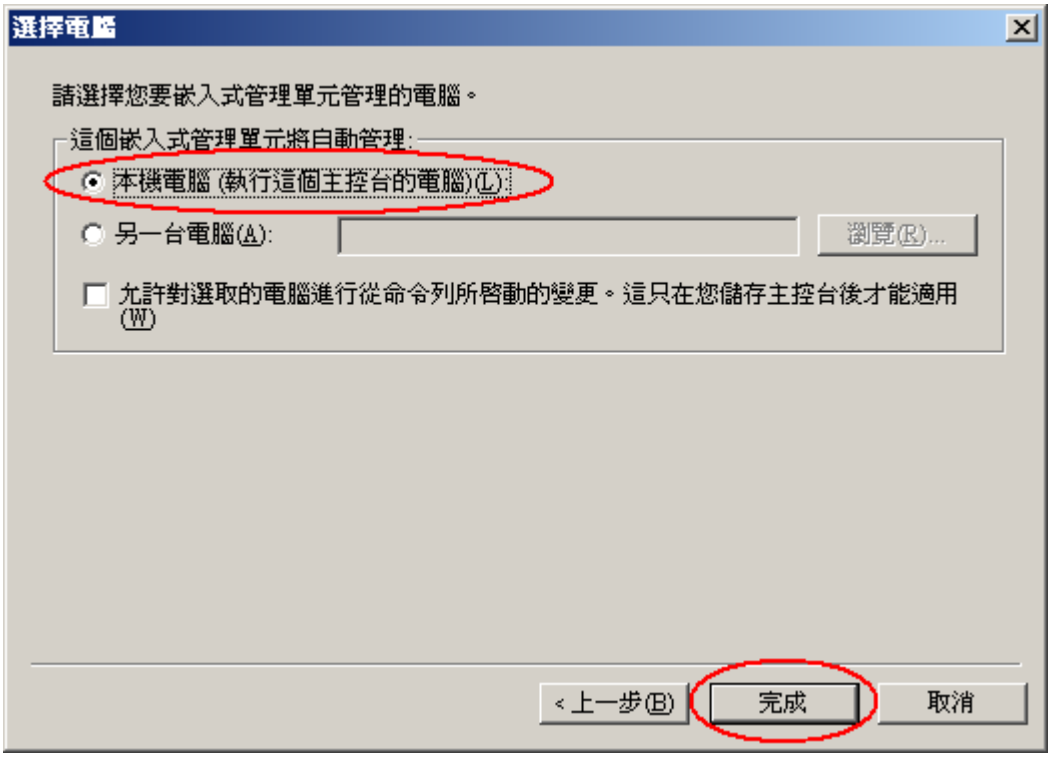
新增憑證管理單元。點選「新增」

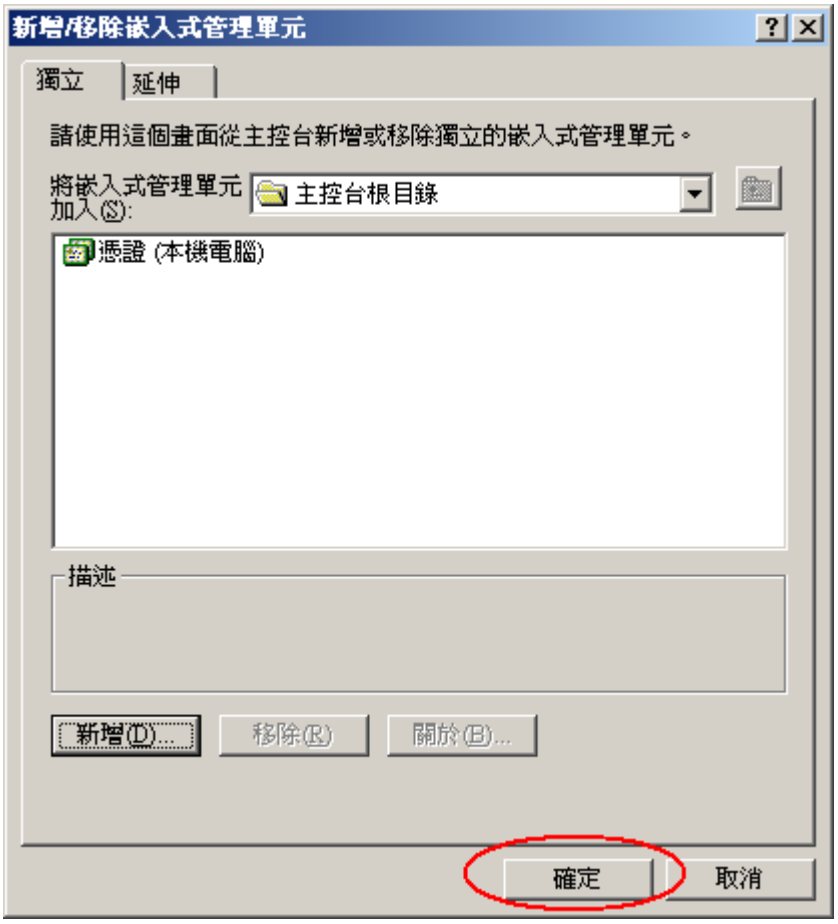


選擇「憑證」

點選電腦帳戶及本機電腦


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 (執行這個主控台的電腦)(L)
另一台電腦(A):
瀏覽(R)...
允許對選取的電腦進行從命令列所啓動的變更。這只在您儲存主控台後才能適用(W)
< 上一步(B)
完成
取消

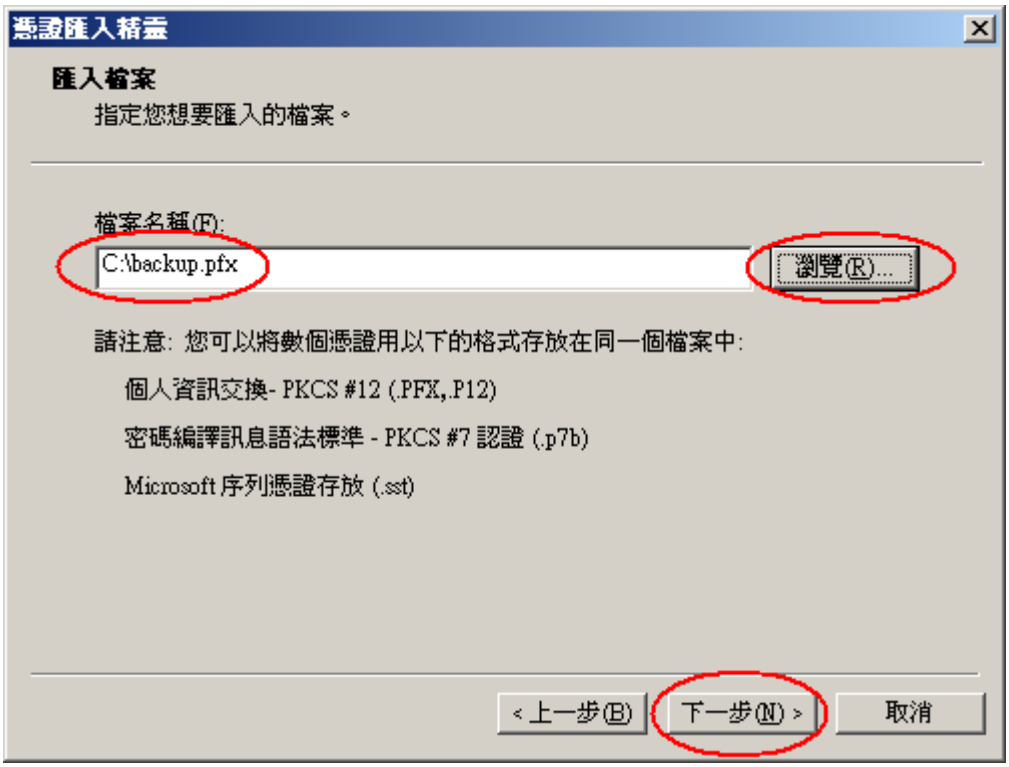


3. 匯入憑證。

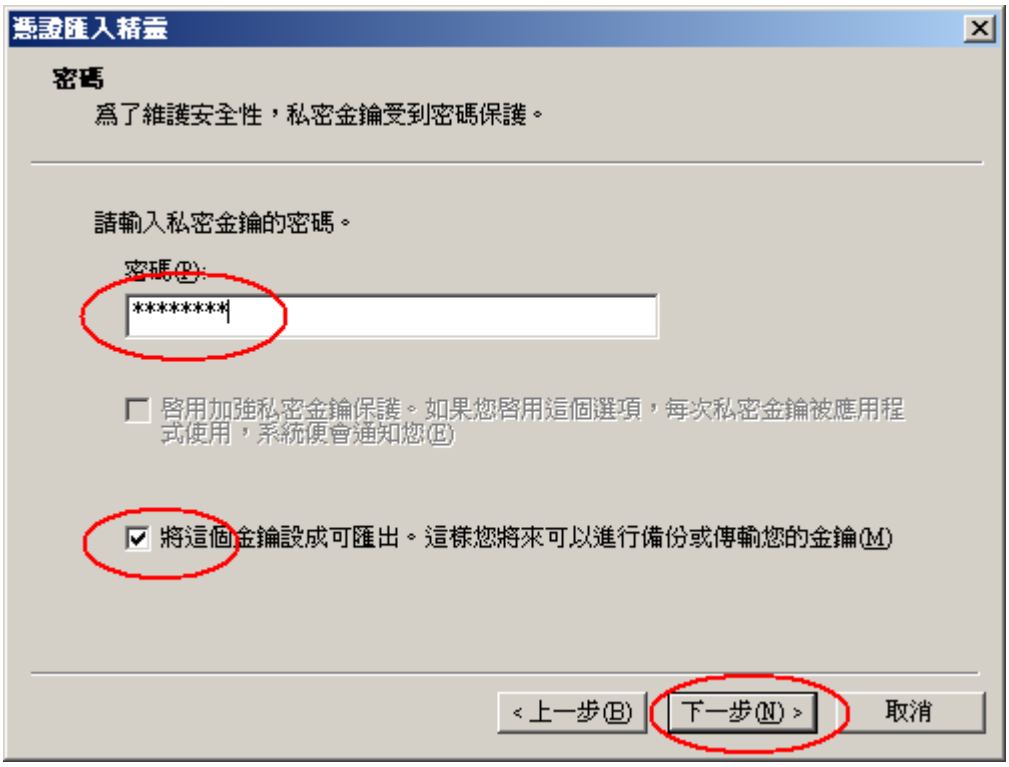
點選「個人」→憑證→所有工作→匯入

使用憑證匯入精靈→下一步

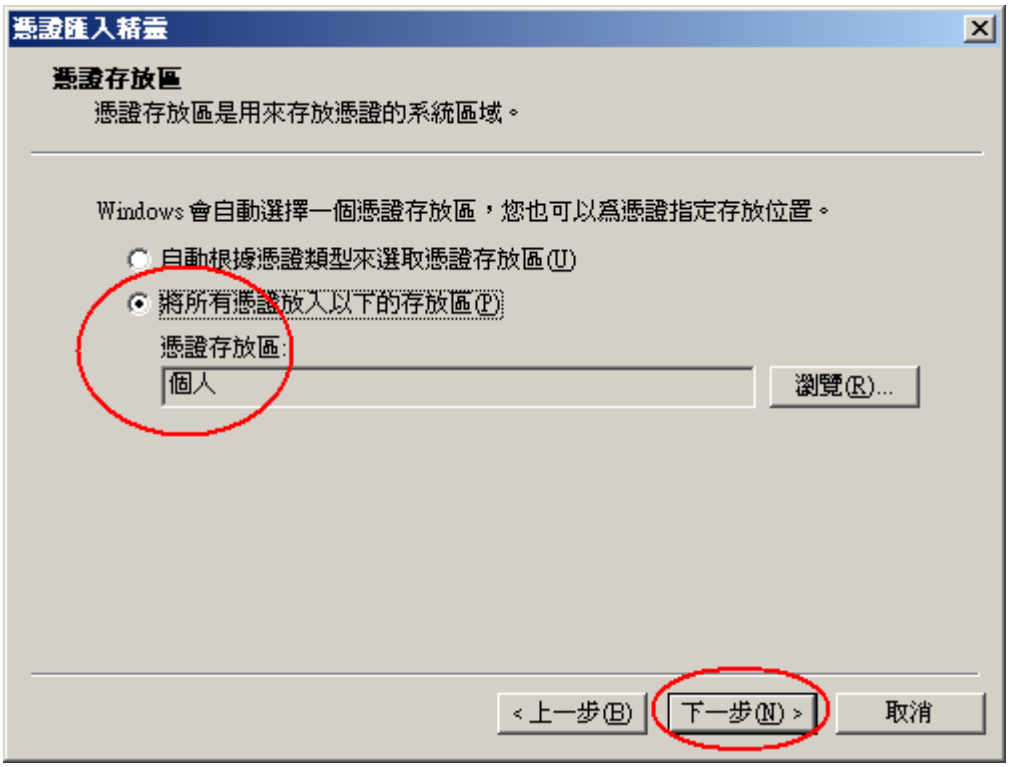
瀏覽→選擇備份之*.pfx



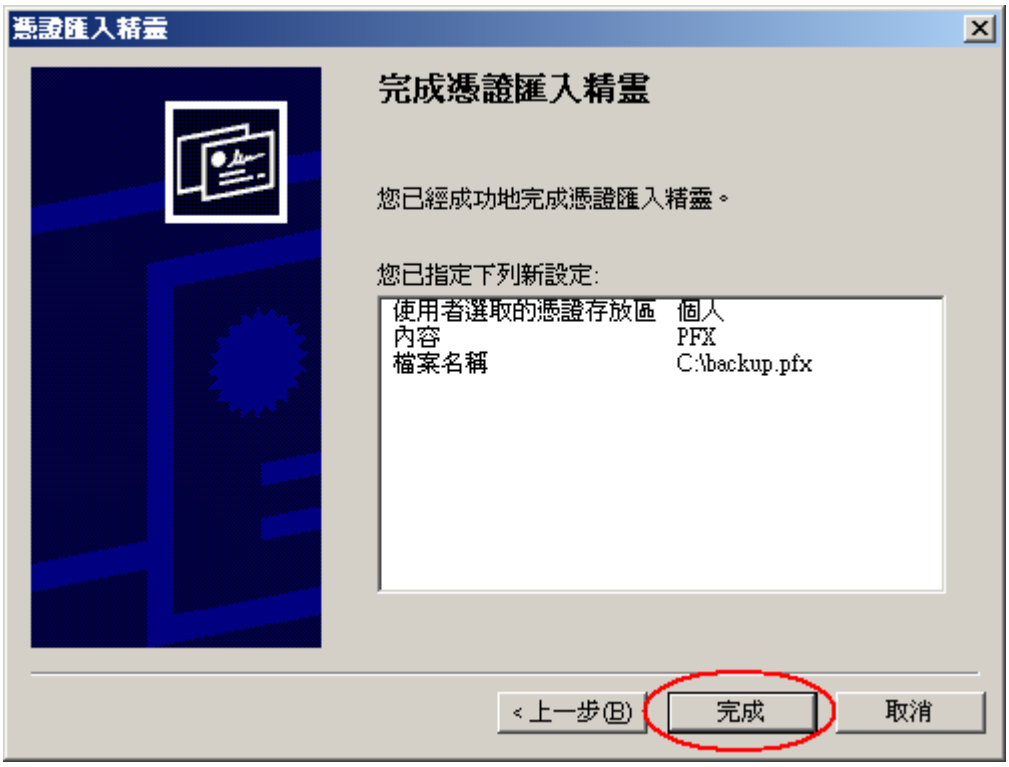
輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。



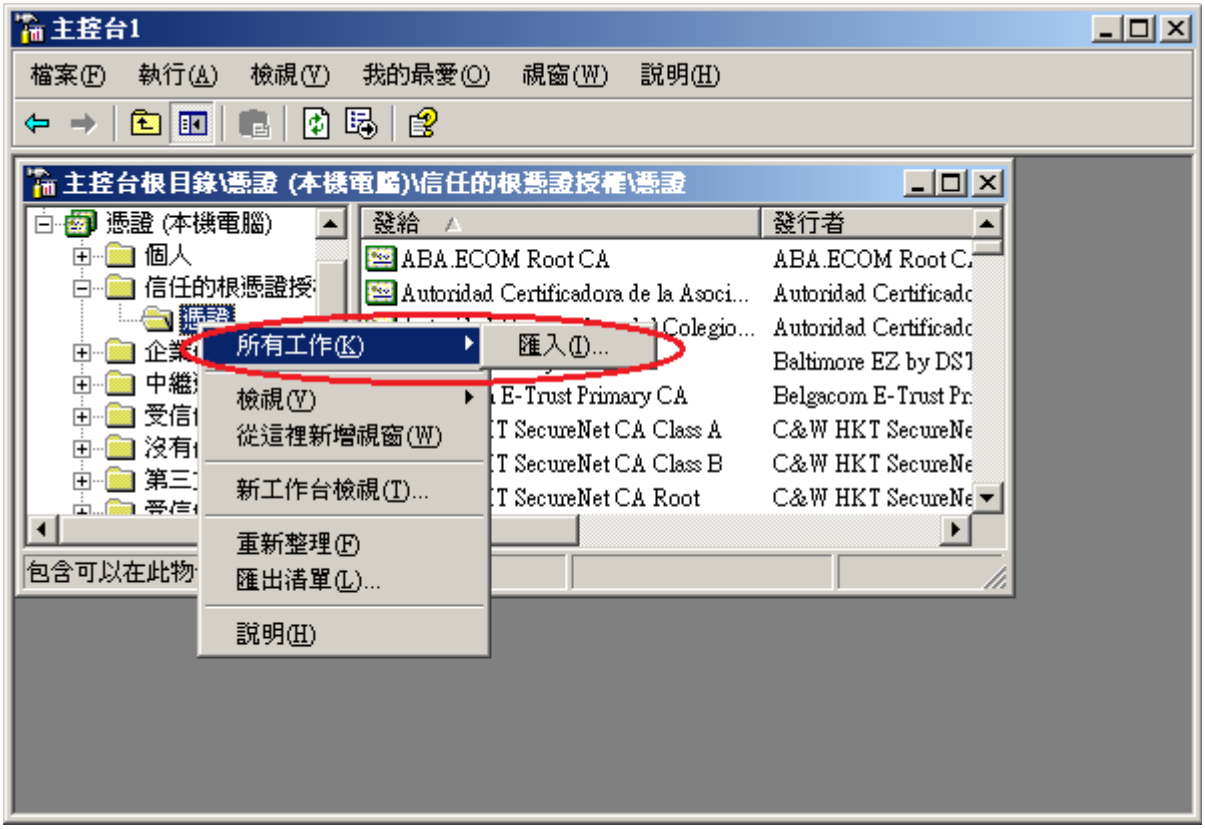
憑證匯入到個人→下一步

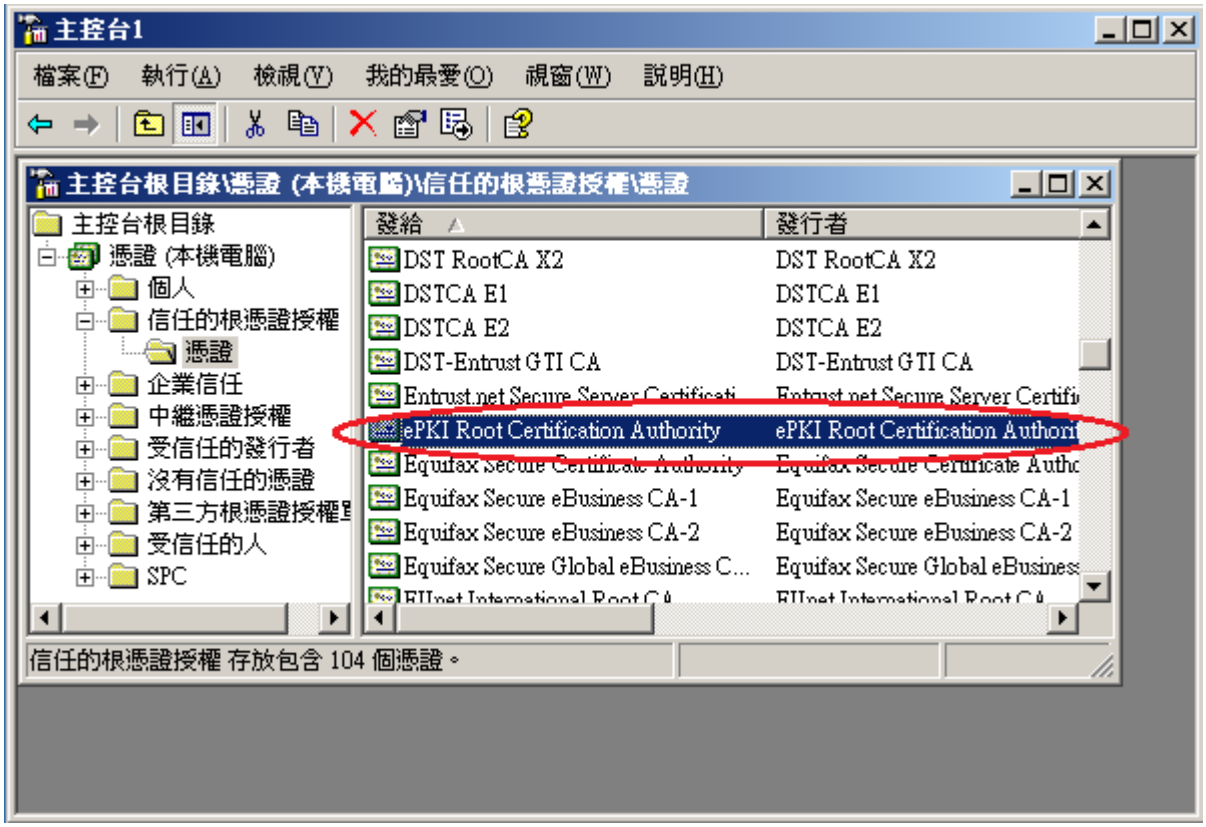


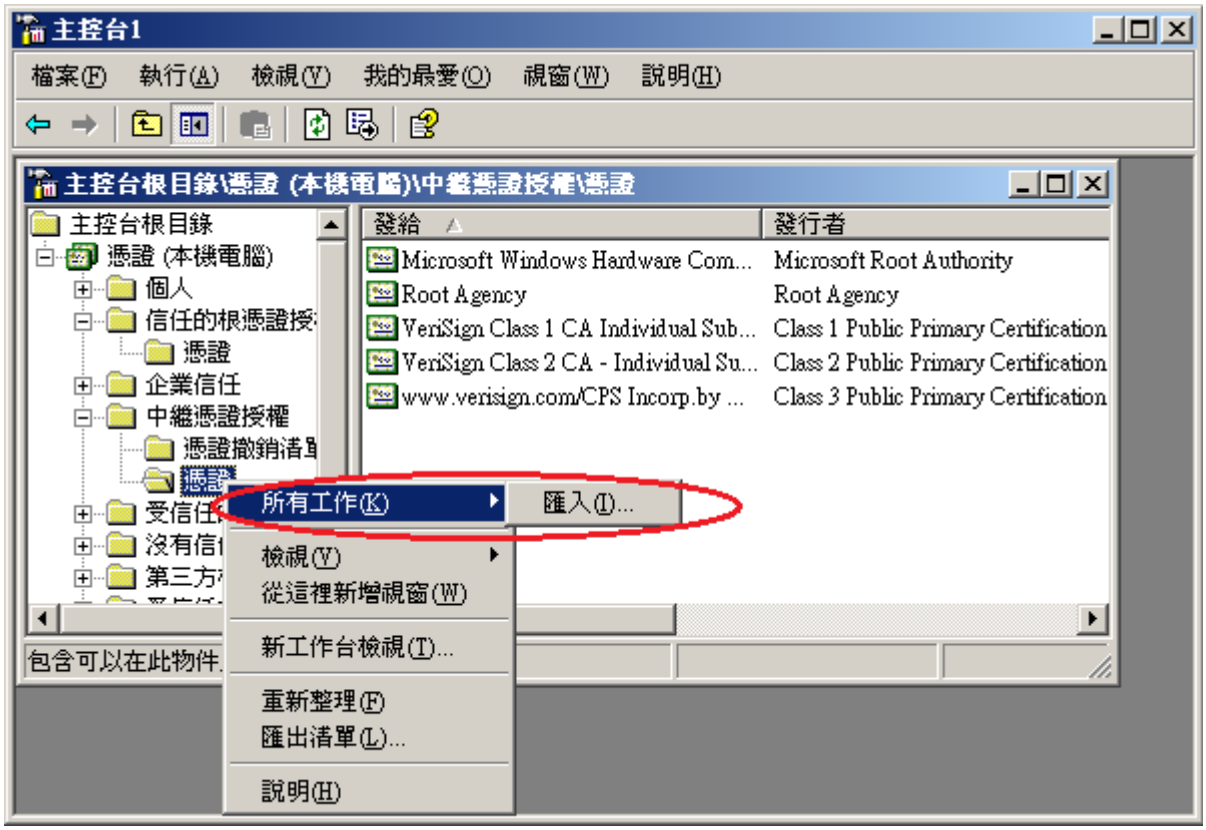
完成匯入憑證

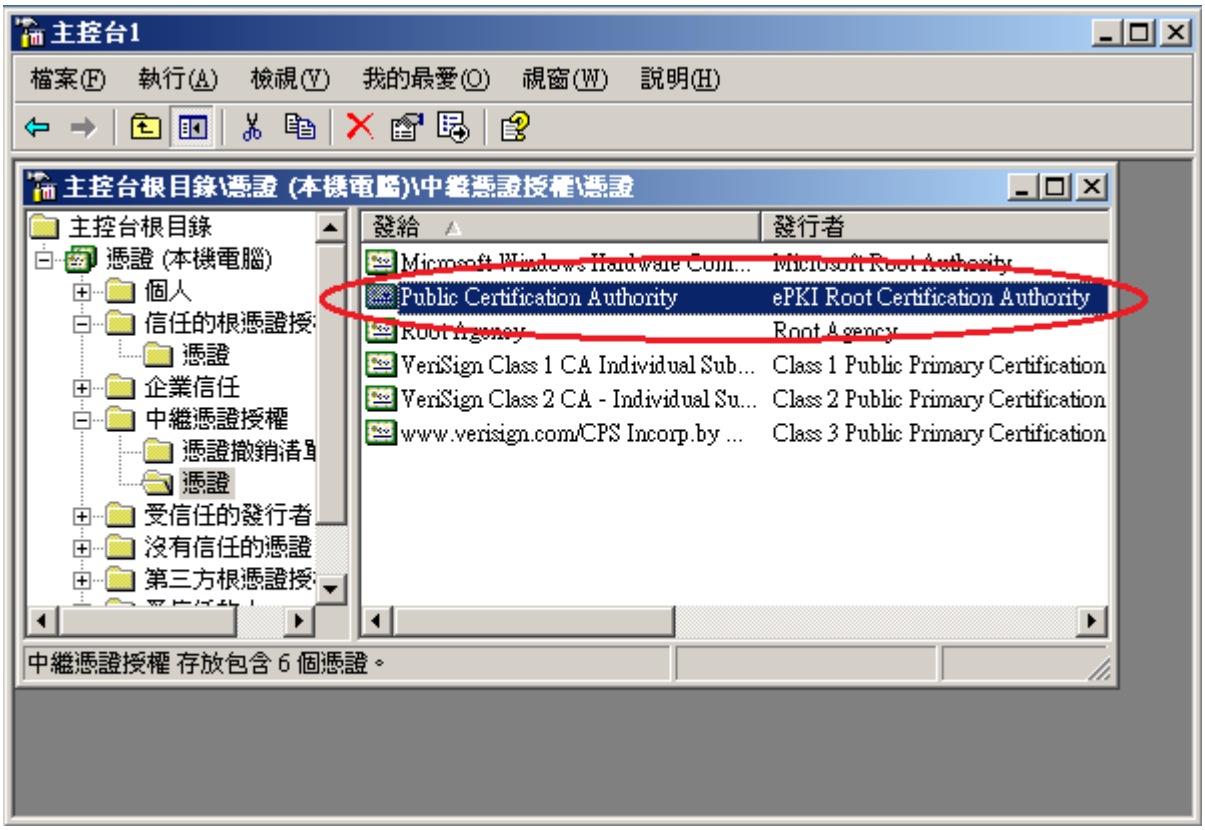


4. 於「信任的根憑證授權」與「中繼憑證授權」匯入 eCA 與 Public CA。
   eCA 憑證：http://eca.hinet.net/download/ROOTeCA_64.crt
   PublicCA2 憑證：http://eca.hinet.net/download/PublicCA2_64.crt



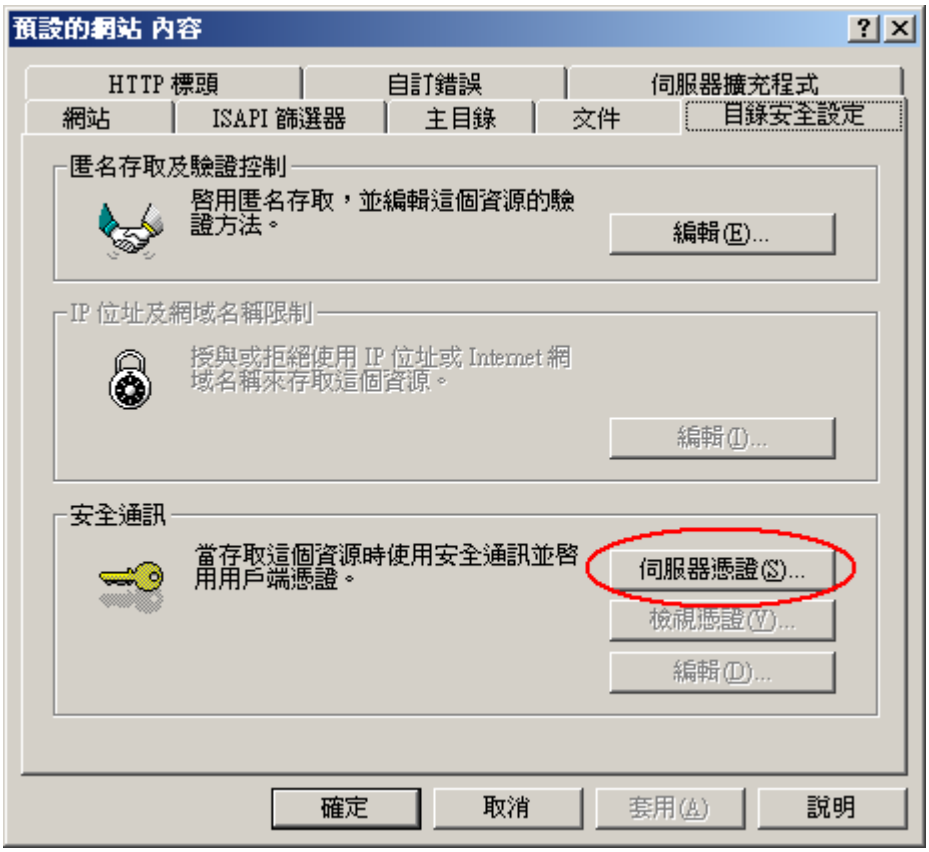

主控台1
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄\憑證 (本機電腦)\信任的根憑證授權\憑證
主控台根目錄
憑證 (本機電腦)
個人
信任的根憑證授權
憑證
企業信任
中繼憑證授權
受信任的發行者
沒有信任的憑證
第三方根憑證授權
受信任的人
SPC
發給
發行者
DST RootCA X2
DST RootCA X2
DSTCA E1
DSTCA E1
DSTCA E2
DSTCA E2
DST-Entrust GTI CA
DST-Entrust GTI CA
ePKI Root Certification Authority
ePKI Root Certification Authority
Equifax Secure eBusiness CA-1
Equifax Secure eBusiness CA-1
Equifax Secure eBusiness CA-2
Equifax Secure eBusiness CA-2
Equifax Secure Global eBusiness C...
Equifax Secure Global eBusiness
信任的根憑證授權 存放包含 104 個憑證。


主控台1
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\憑證 (本機電腦)\中繼憑證授權\憑證
主控台根目錄
憑證 (本機電腦)
個人
信任的根憑證授
憑證
企業信任
中繼憑證授權
憑證撤銷清單
憑證
受信任
沒有信
第三方
發給
發行者
Microsoft Windows Hardware Com...
Microsoft Root Authority
Root Agency
Root Agency
VeriSign Class 1 CA Individual Sub...
Class 1 Public Primary Certification
VeriSign Class 2 CA - Individual Su...
Class 2 Public Primary Certification
www.verisign.com/CPS Incorp.by ...
Class 3 Public Primary Certification
所有工作(K)
匯入(I)...
檢視(V)
從這裡新增視窗(W)
新工作台檢視(T)...
重新整理(F)
匯出清單(L)...
說明(H)
包含可以在此物件



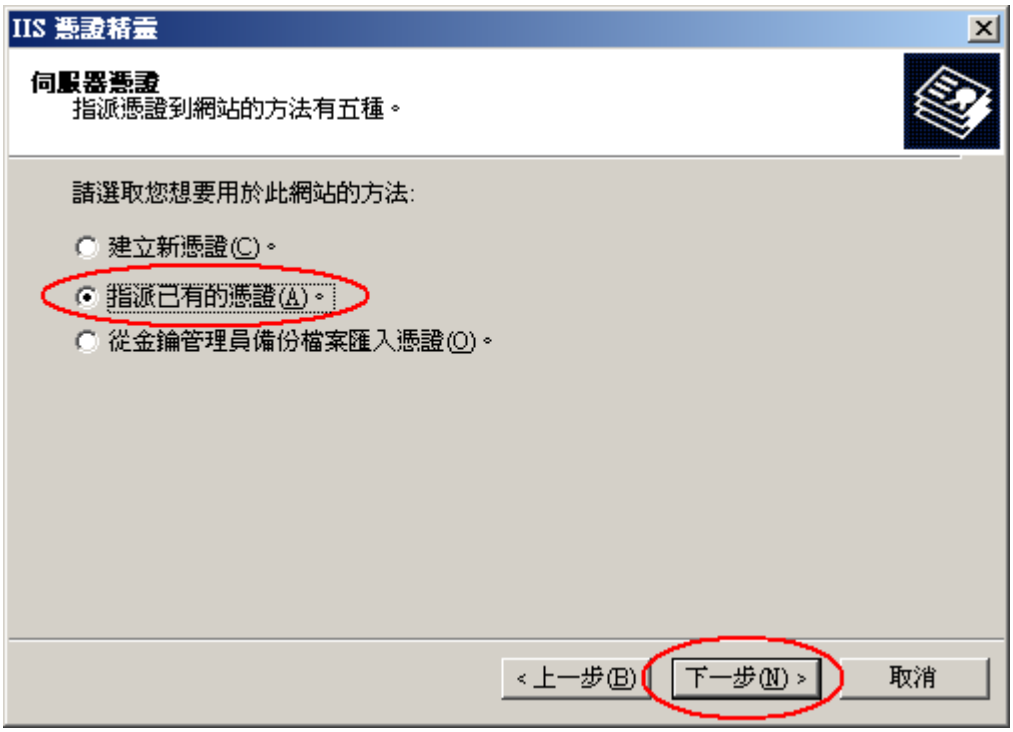
5. 設定 IIS。

開始」→「設定」→「控制台」→「系統管理工具」→「Internet 服務管理員」→點選服務站台(滑鼠右鍵、選內容)→「目錄安全設定」→「伺服器憑證」

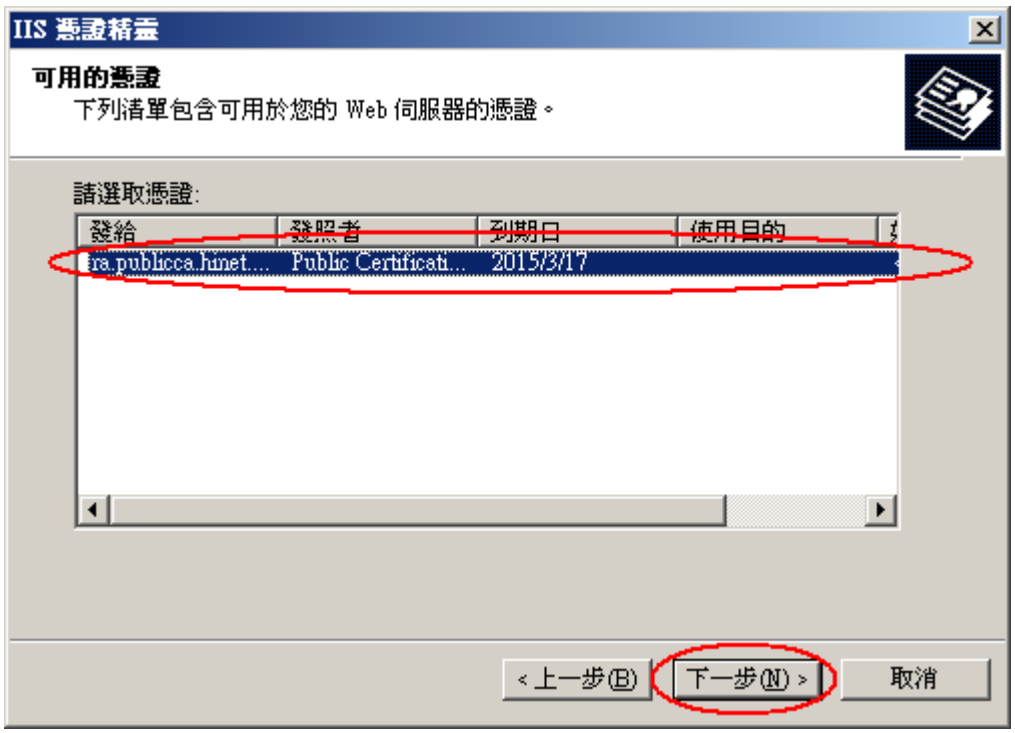


點選「下一步」

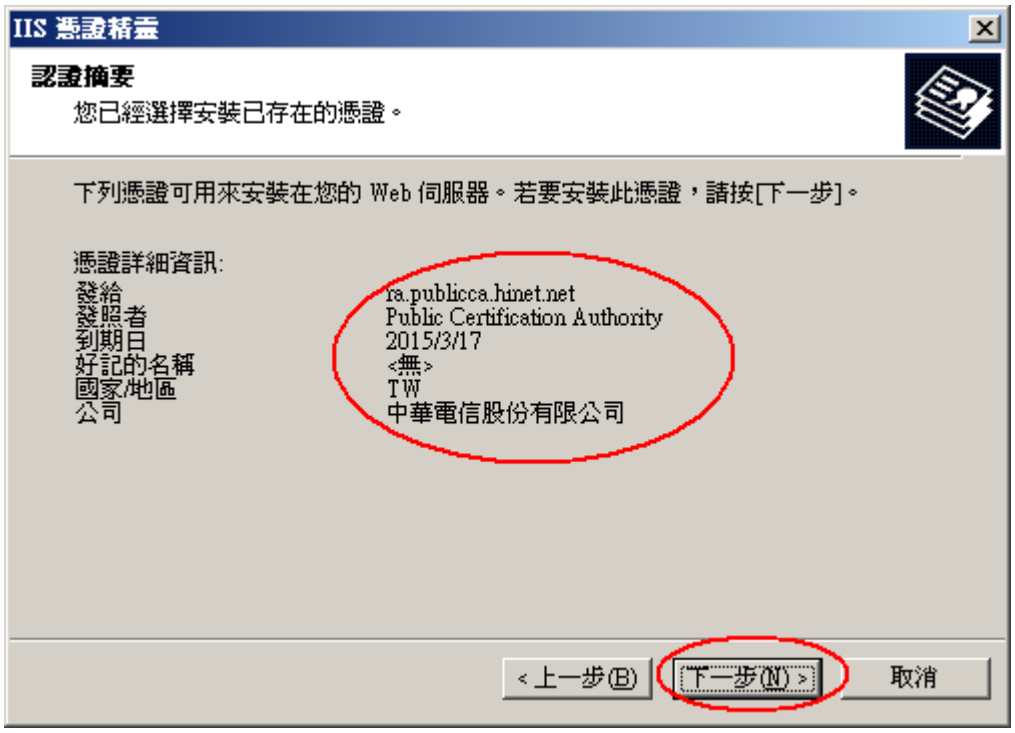
點選「指派已有的憑證」



選擇匯入之憑證→下一步


IIS 憑證精靈
可用的憑證
下列清單包含可用於您的 Web 伺服器的憑證。
請選取憑證:
發給
發照者
到期日
使用目的
ra.publicca.hinet...
Public Certificati...
2015/3/17
< 上一步(B)
下一步(N) >
取消

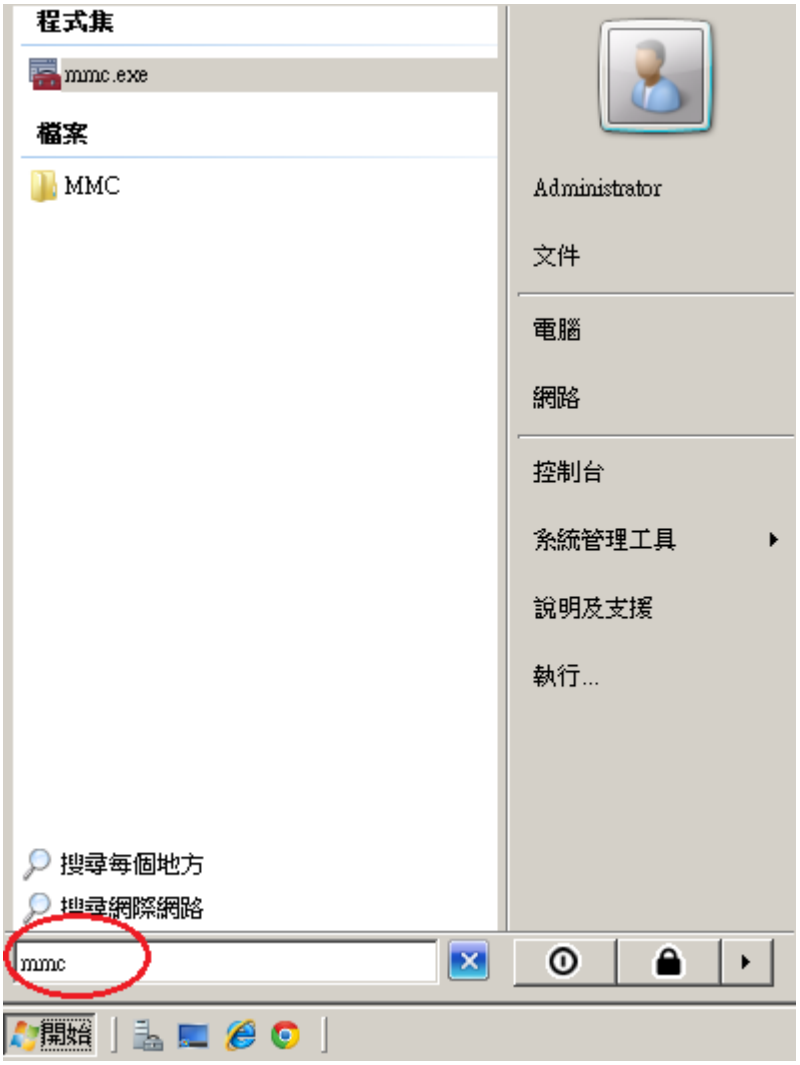
檢視憑證詳細資料


IIS 憑證精靈
認證摘要
您已經選擇安裝已存在的憑證。
下列憑證可用來安裝在您的 Web 伺服器。若要安裝此憑證，請按[下一步]。
憑證詳細資訊:
發給
發照者
到期日
好記的名稱
國家/地區
公司
ra.publicca.hinet.net
Public Certification Authority
2015/3/17
<無>
TW
中華電信股份有限公司
< 上一步(B)
下一步(N) >
取消

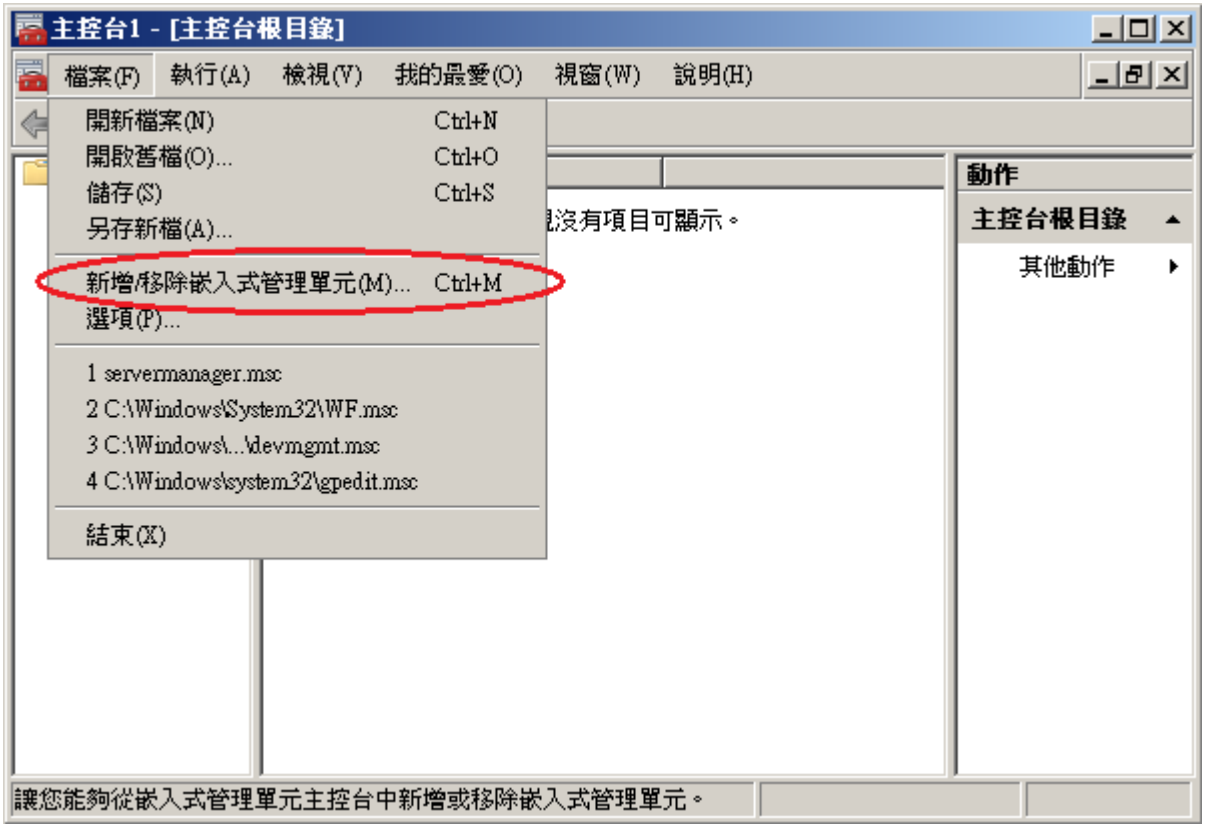
完成


IIS 憑證精靈
正在完成 Web 伺服器憑證精靈
您已經成功完成 Web 伺服器憑證精靈。
目前已安裝憑證在此電腦。
如果您將來需要更新，取代，或刪除此新憑證，請再次使用精靈。
請按 [完成] 來關閉此精靈。
< 上一步(B)
完成
取消

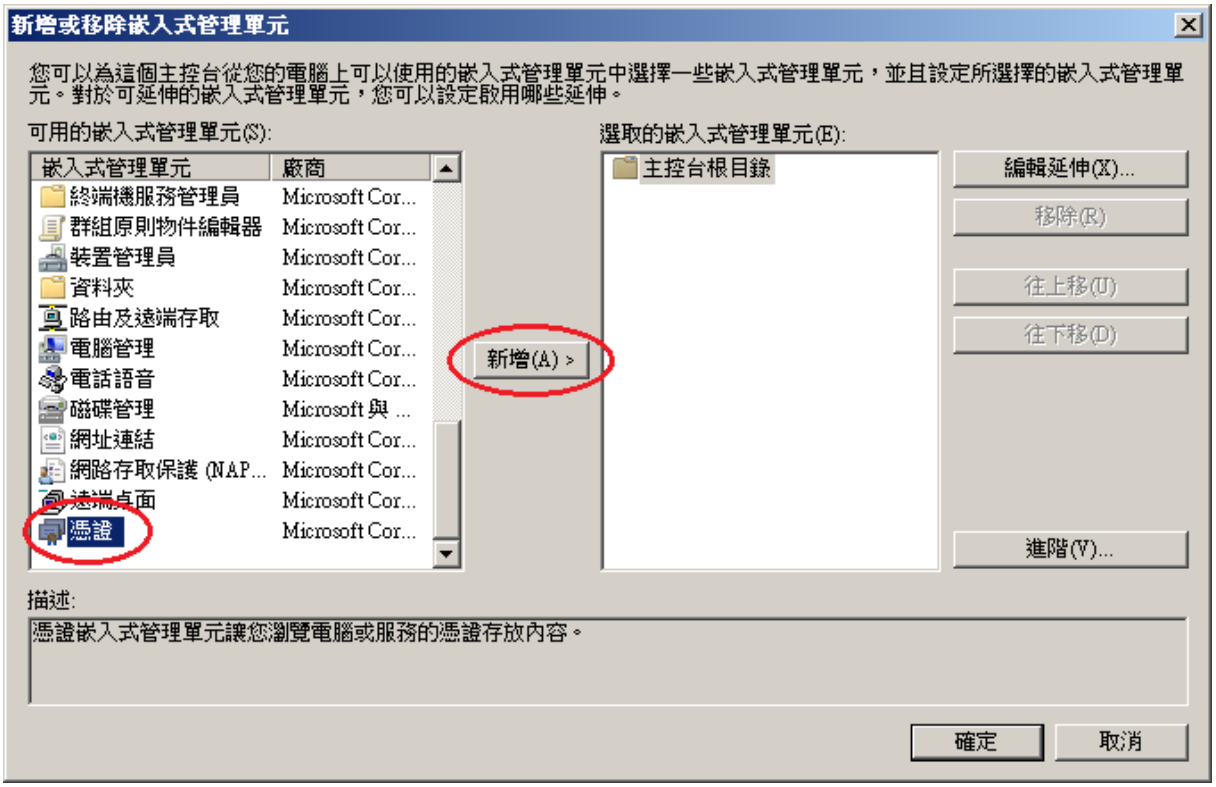
1. 「開始」→「輸入 mmc」，按下「Enter」。



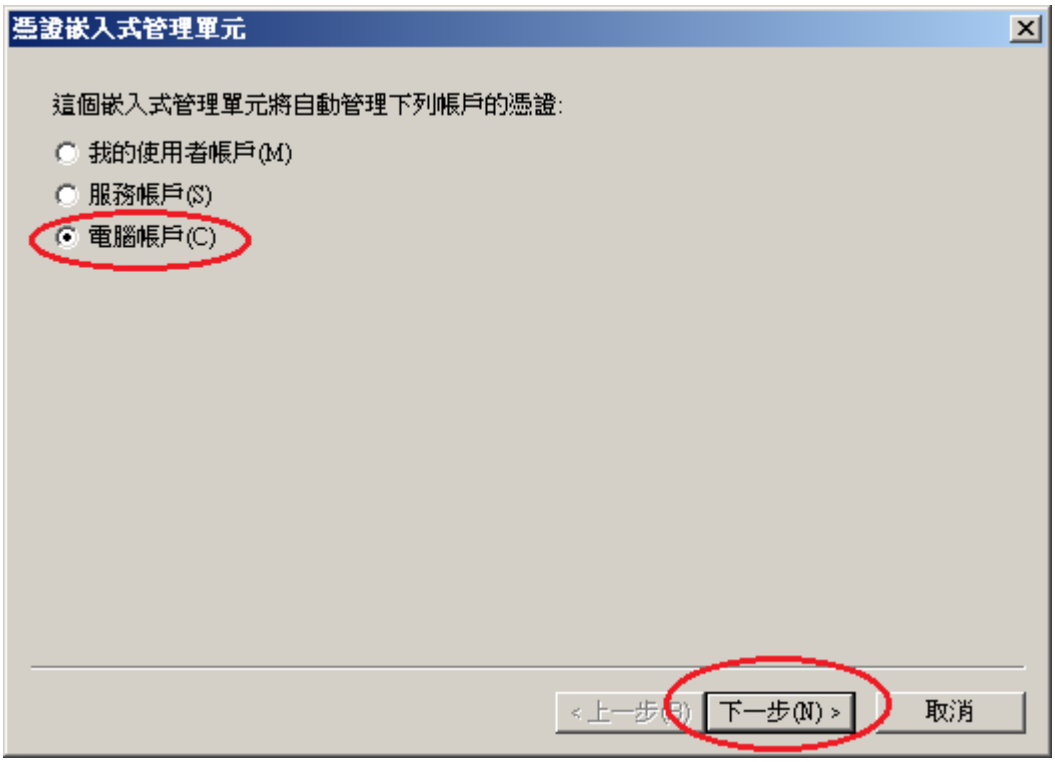
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

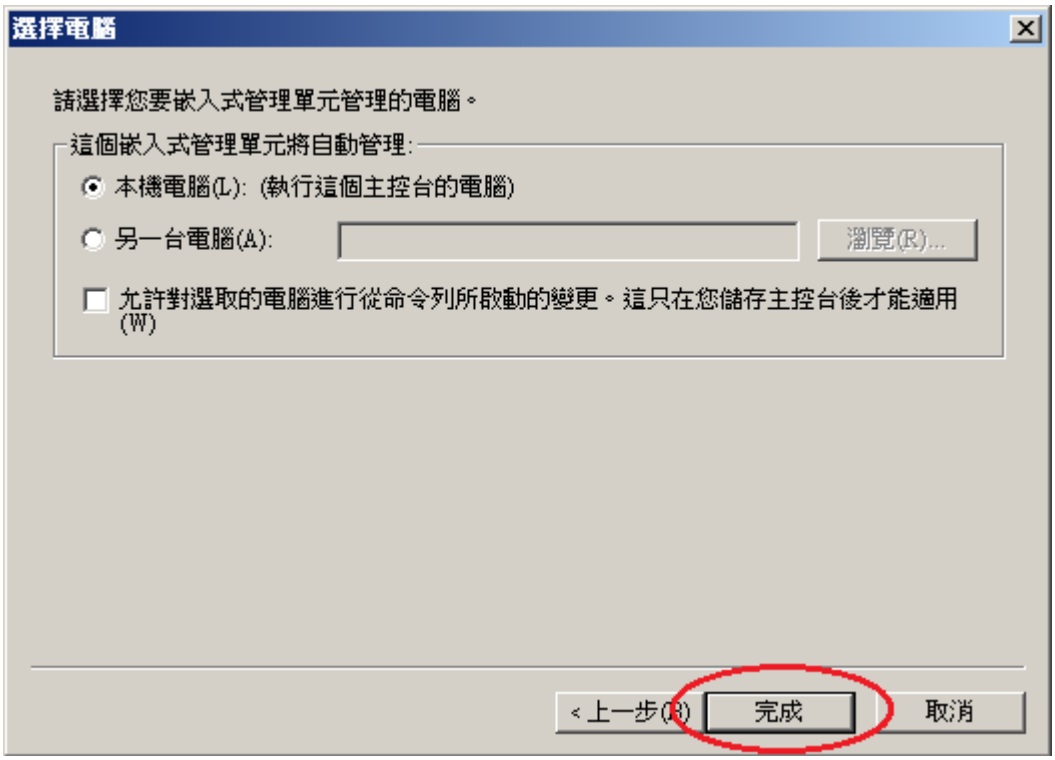


3. 點選「憑證」→「新增」

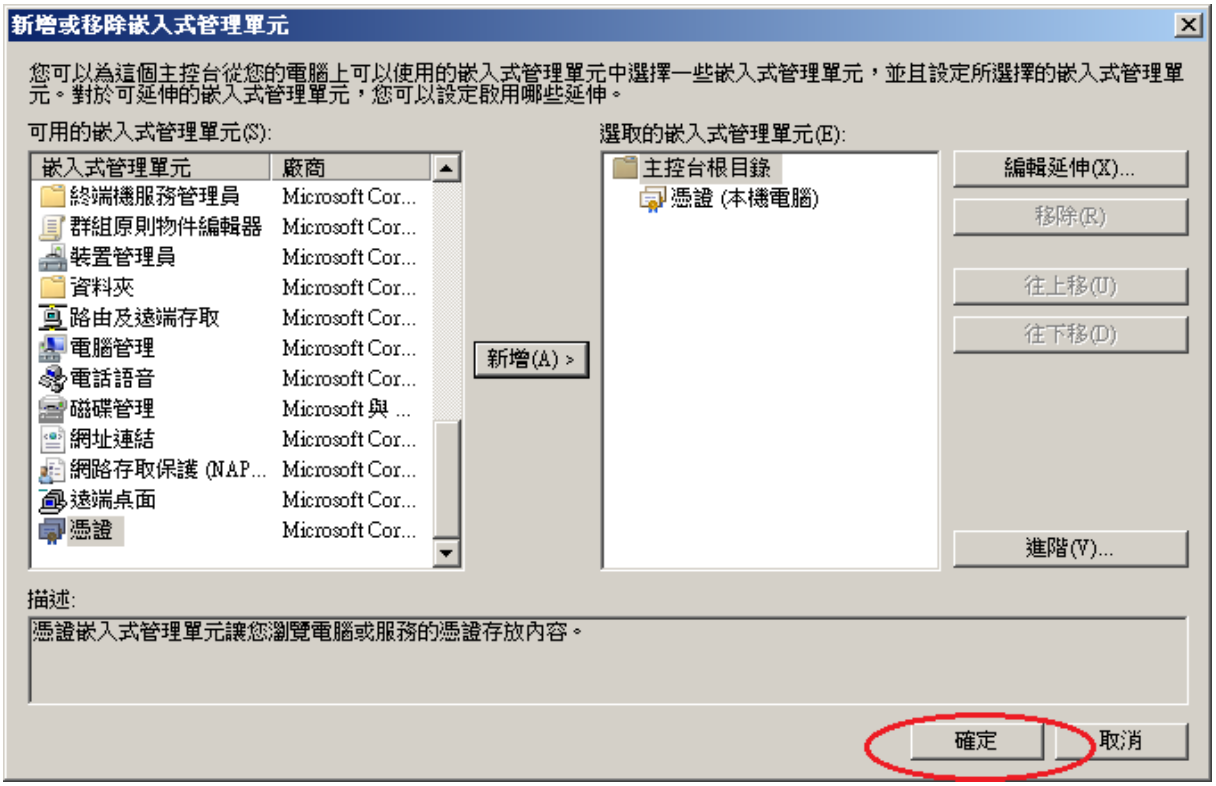


「電腦帳戶」→「下一步」→「完成」。

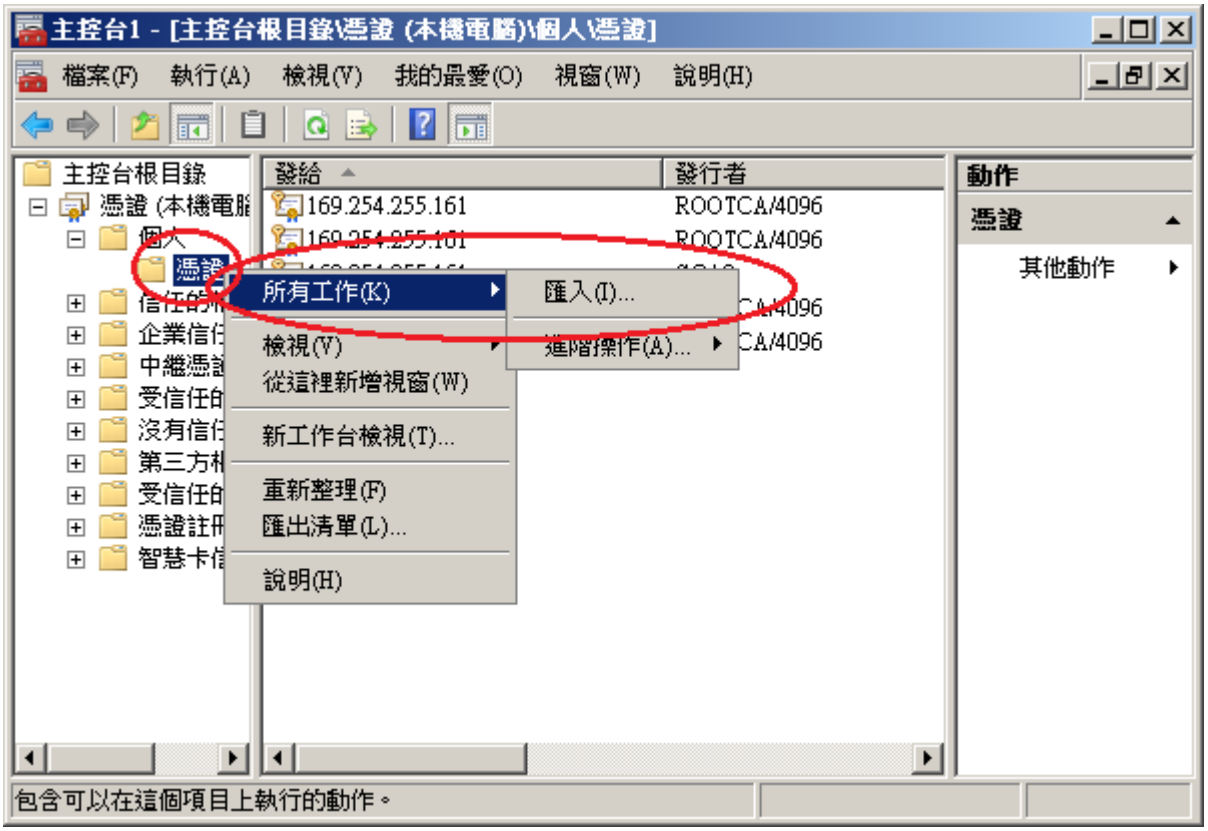

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


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

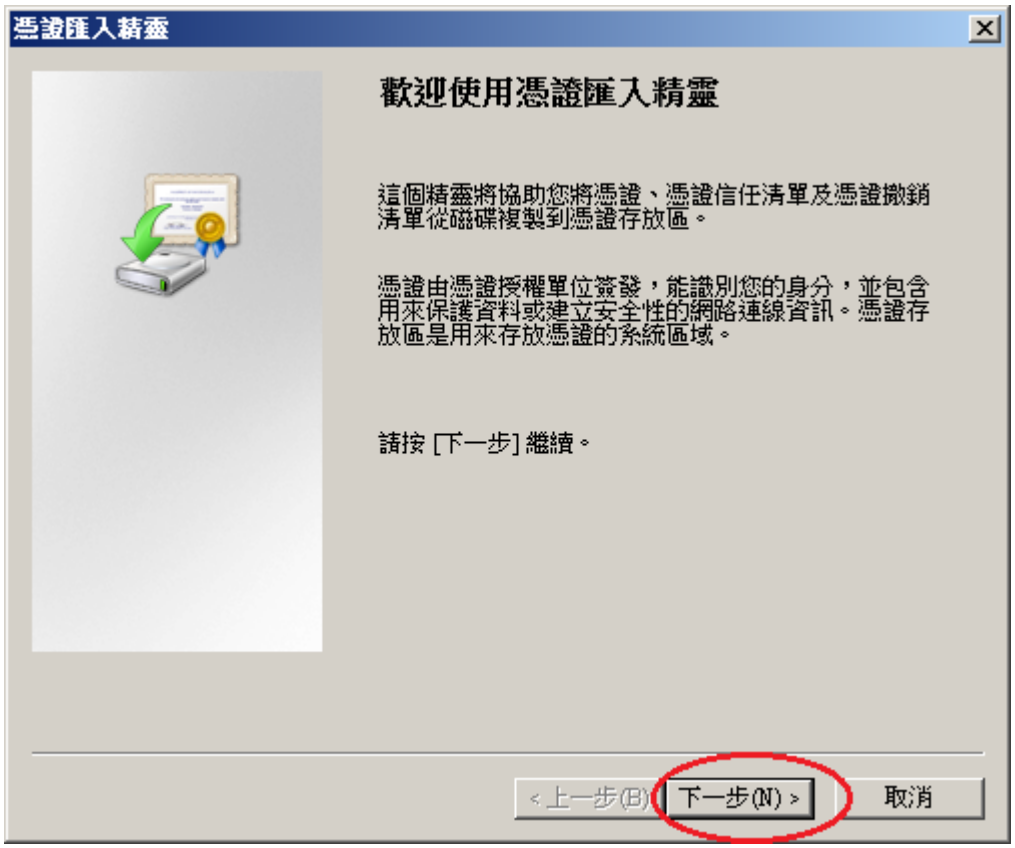
「確定」。

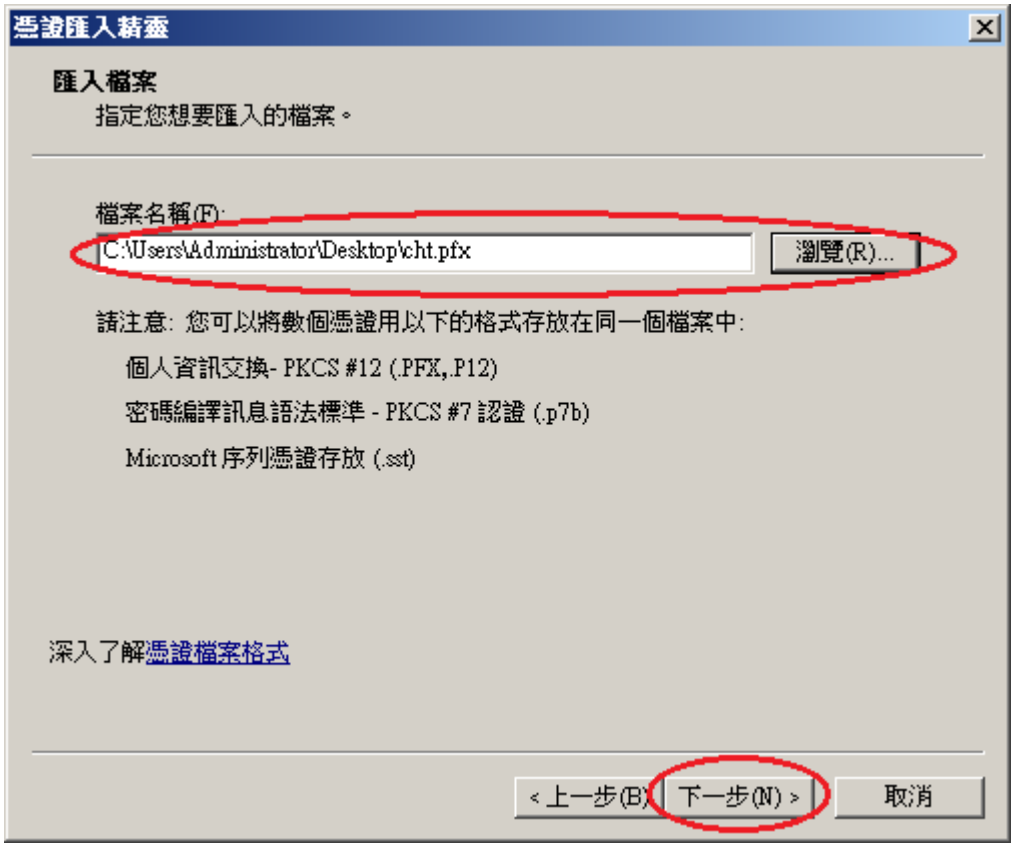


4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

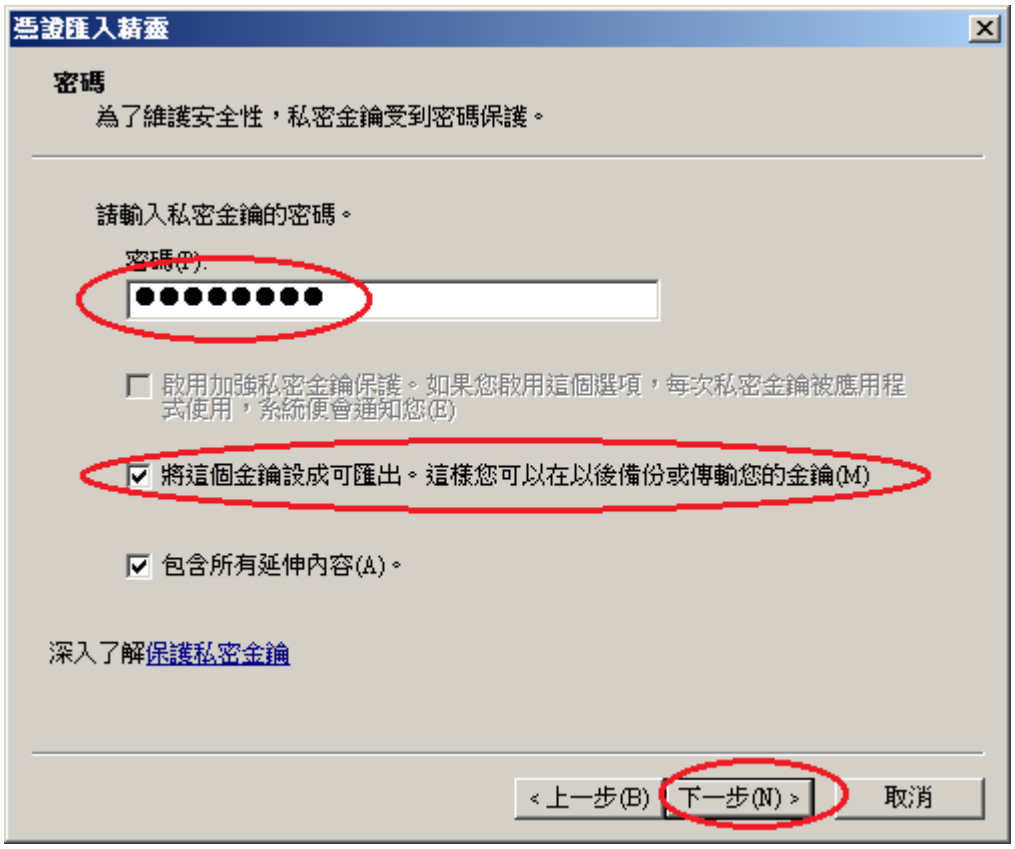


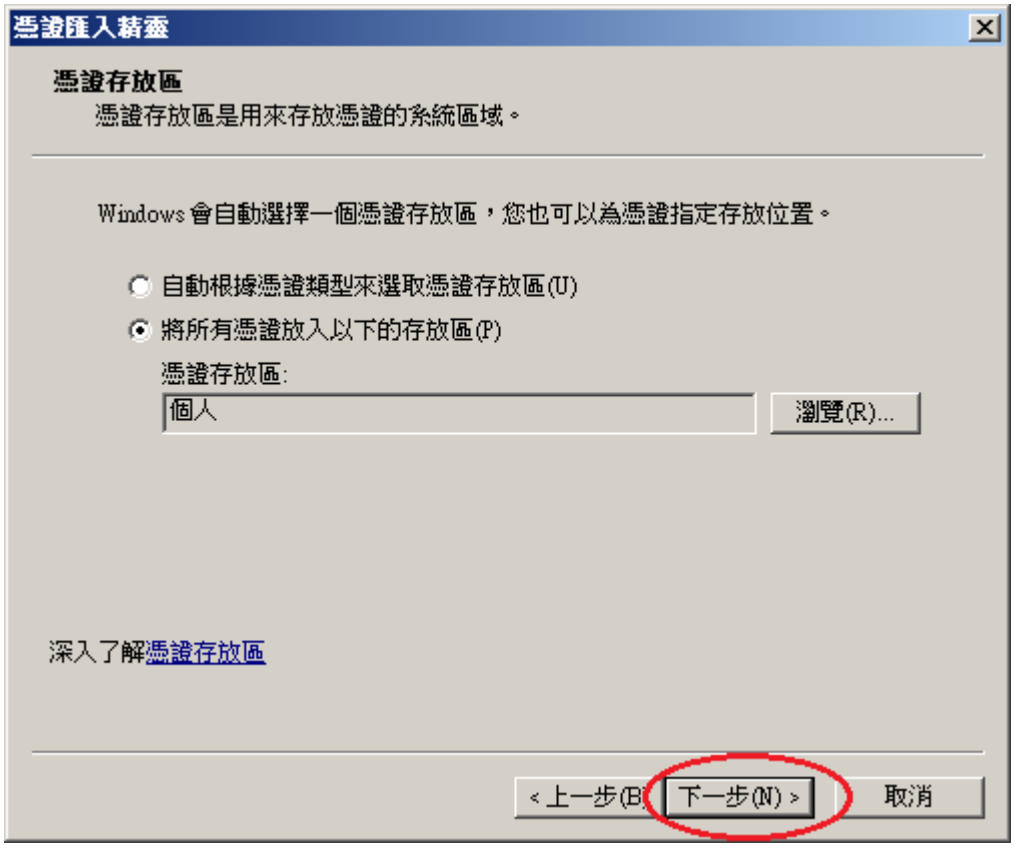
5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

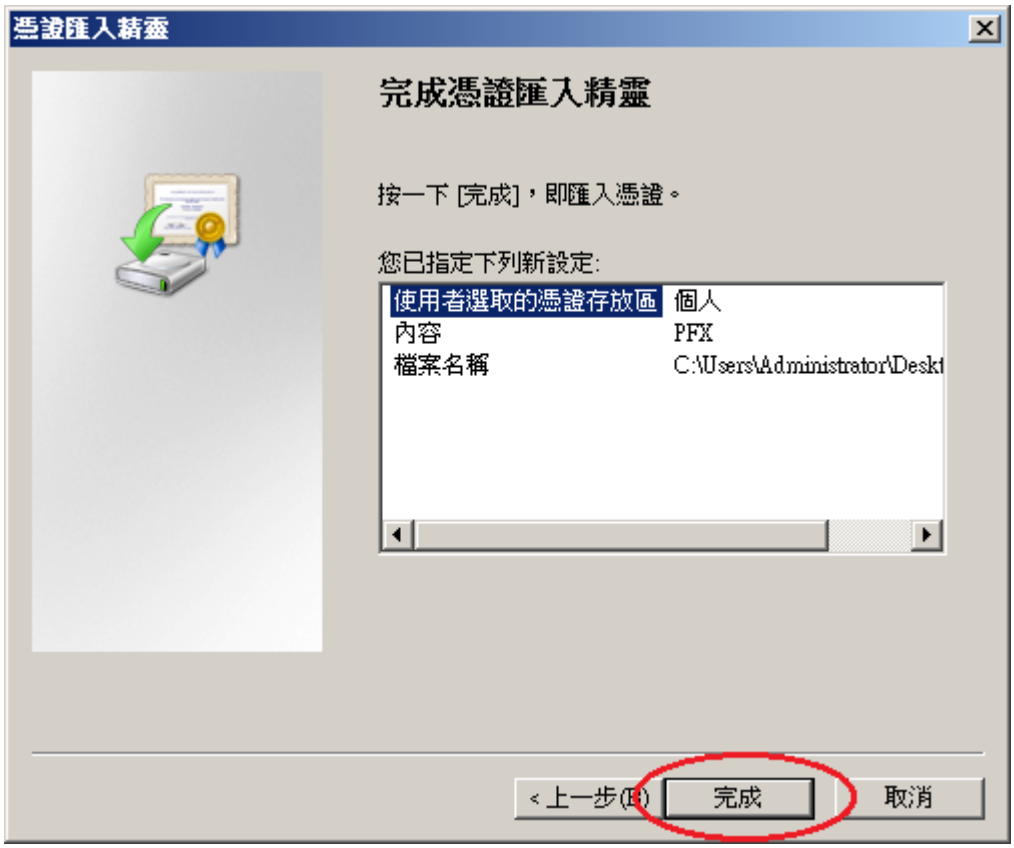




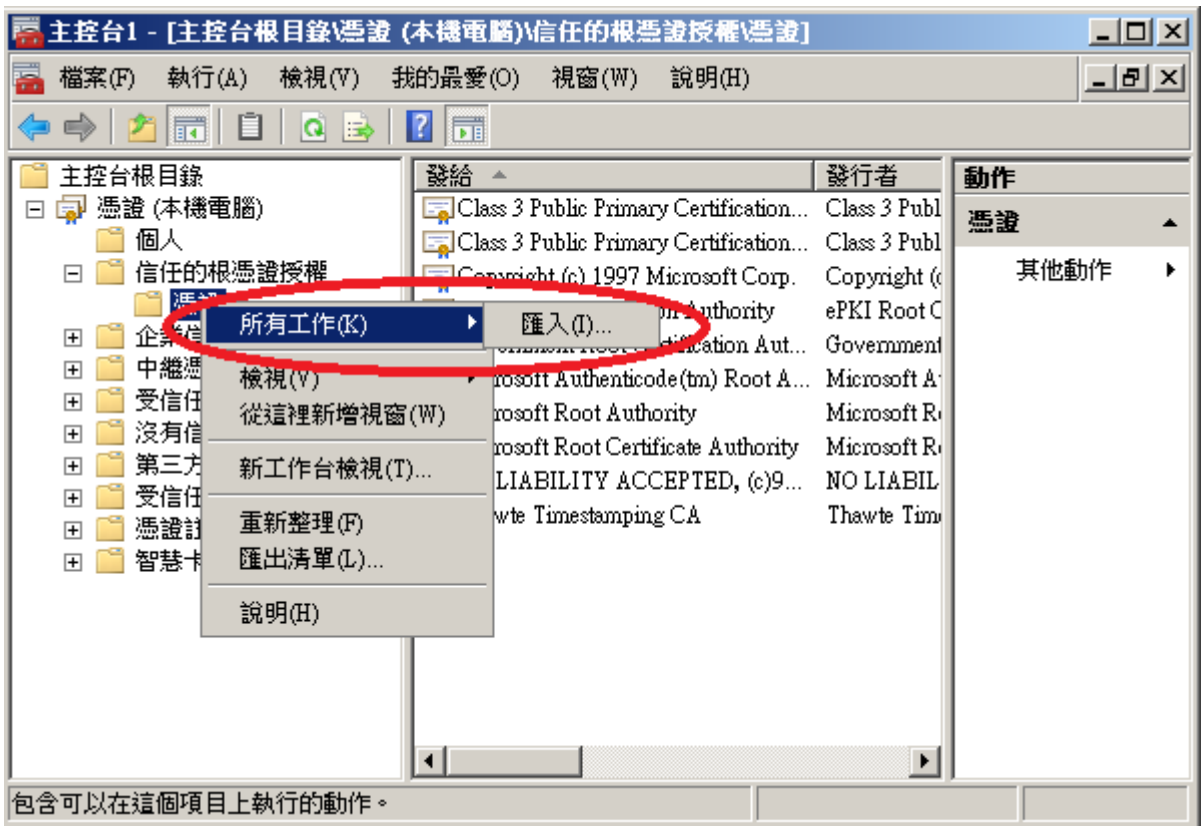
輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。

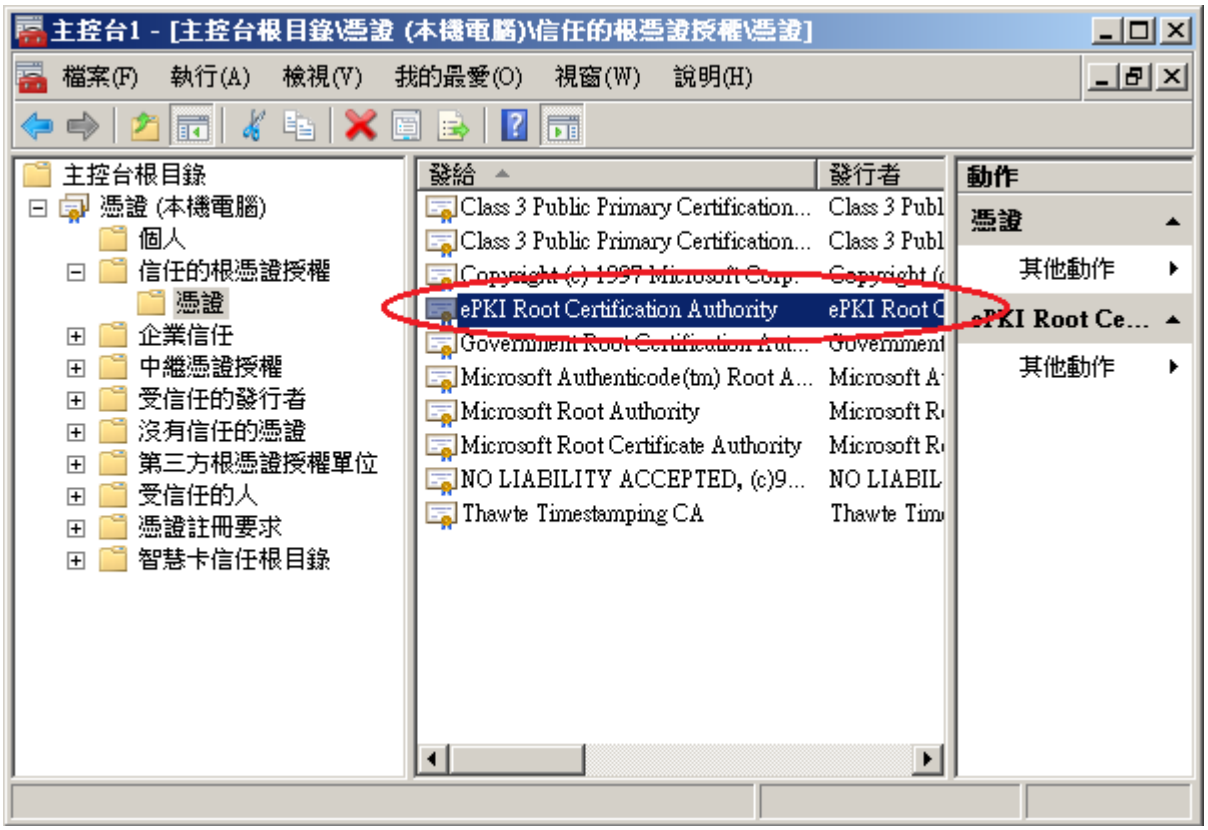

憑證匯入精靈
密碼
為了維護安全性，私密金鑰受到密碼保護。
請輸入私密金鑰的密碼。
密碼(P):
●●●●●●●●
啟用加強私密金鑰保護。如果您啟用這個選項，每次私密金鑰被應用程式使用，系統便會通知您(E)
將這個金鑰設成可匯出。這樣您可以在以後備份或傳輸您的金鑰(M)
包含所有延伸內容(A)。
深入了解保護私密金鑰
< 上一步(B)
下一步(N) >
取消

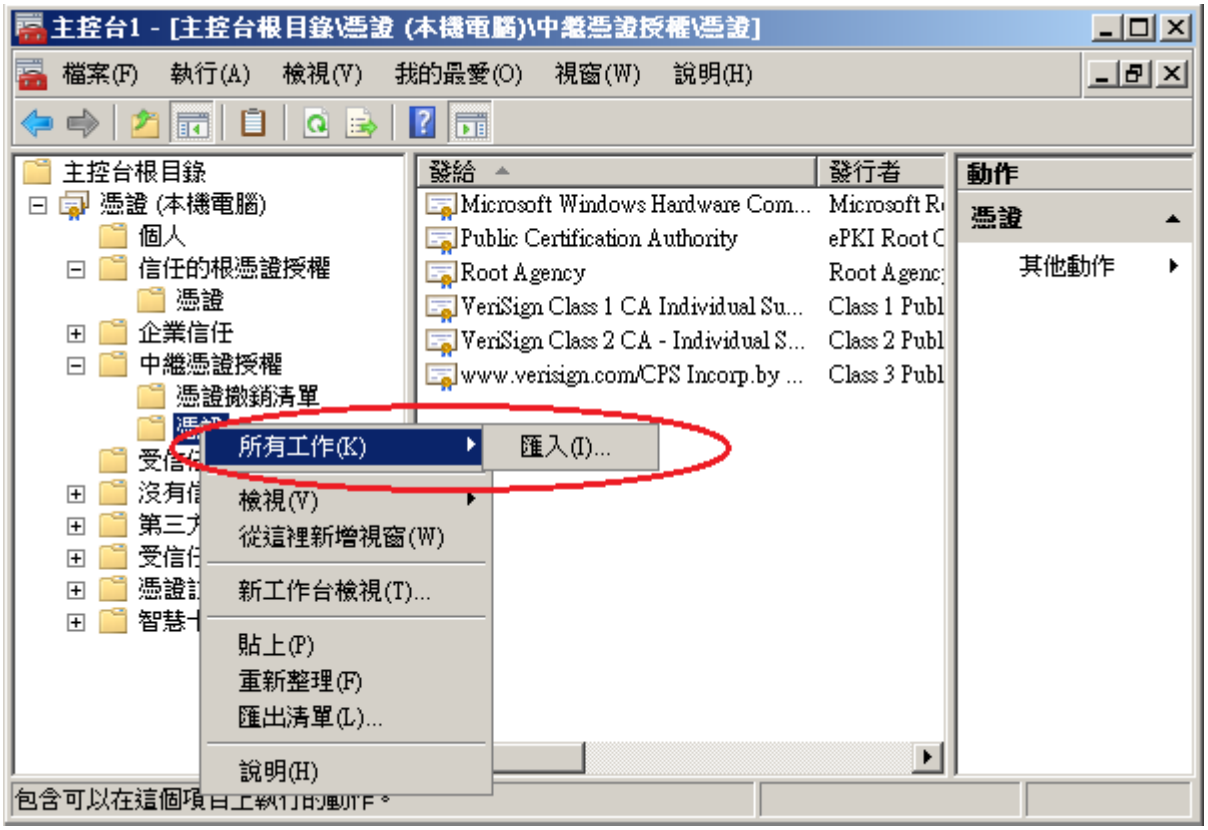

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 會自動選擇一個憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
個人
瀏覽(R)...
深入了解憑證存放區
< 上一步(B)
下一步(N) >
取消

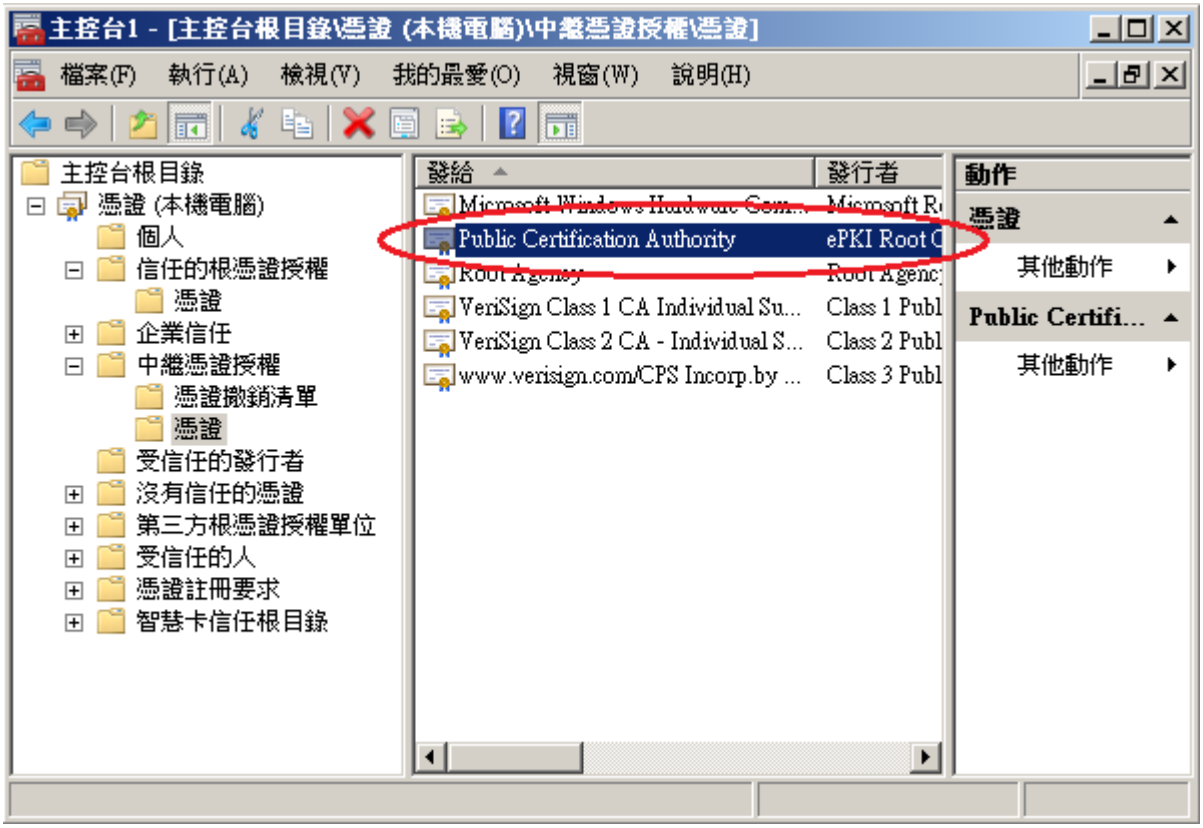


6. 於「信任的根憑證授權」與「中繼憑證授權」匯入 eCA 與 Public CA。
eCA 憑證：http://eca.hinet.net/download/ROOTeCA_64.crt
PublicCA2 憑證：http://eca.hinet.net/download/PublicCA2_64.crt

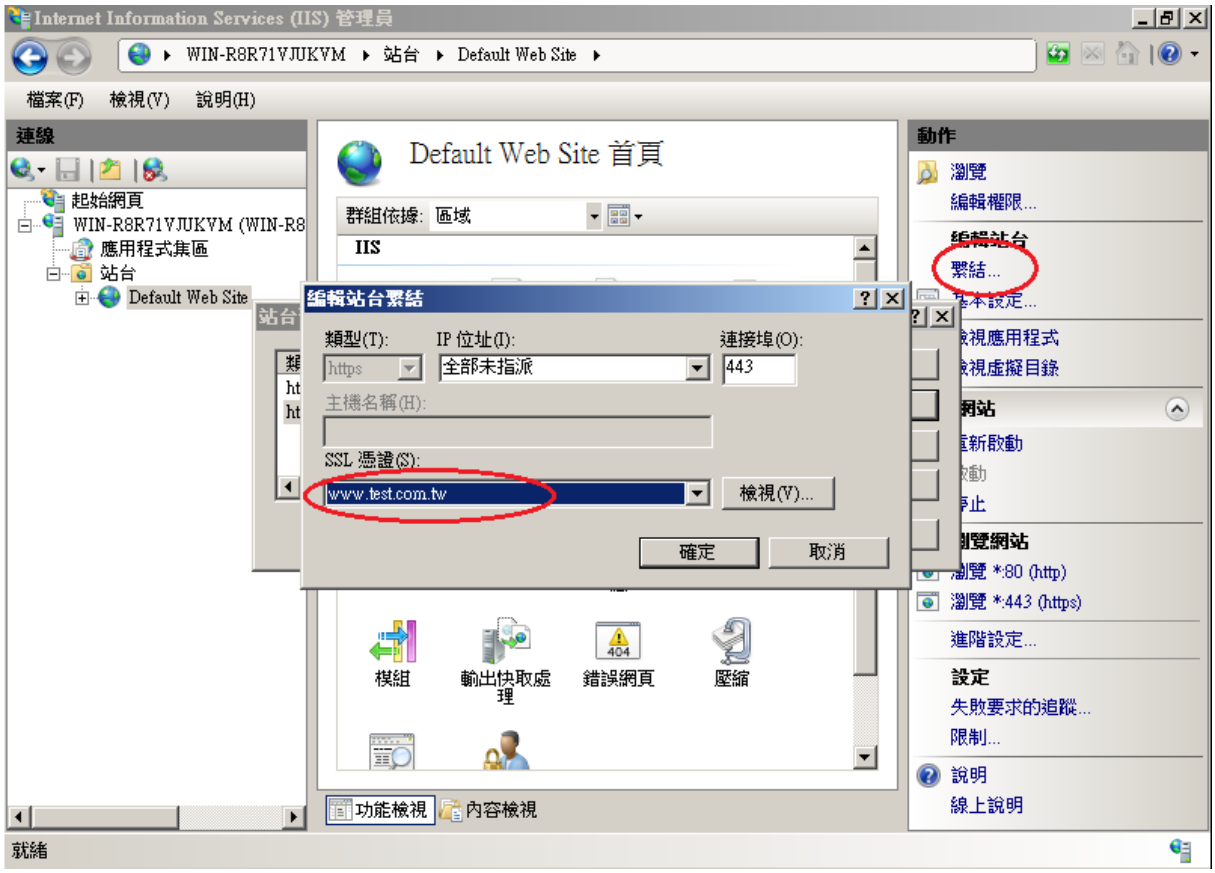



主控台1 - [主控台根目錄\憑證 (本機電腦)\信任的根憑證授權\憑證]
檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
信任的根憑證授權
憑證
企業信任
中繼憑證授權
受信任的發行者
沒有信任的憑證
第三方根憑證授權單位
受信任的人
憑證註冊要求
智慧卡信任根目錄
發給
發行者
Class 3 Public Primary Certification...
Class 3 Publ
Class 3 Public Primary Certification...
Class 3 Publ
ePKI Root Certification Authority
ePKI Root C
Microsoft Authenticode(tm) Root A...
Microsoft A
Microsoft Root Authority
Microsoft R
Microsoft Root Certificate Authority
Microsoft R
NO LIABILITY ACCEPTED, (c)9...
NO LIABIL
Thawte Timestamping CA
Thawte Tim
動作
憑證
其他動作
其他動作


主控台1 - [主控台根目錄\憑證 (本機電腦)\中繼憑證授權\憑證]
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
憑證 (本機電腦)
個人
信任的根憑證授權
憑證
企業信任
中繼憑證授權
憑證撤銷清單
發給
發行者
Microsoft Windows Hardware Com...
Public Certification Authority
ePKI Root C
Root Agency
VeriSign Class 1 CA Individual Su...
Class 1 Publ
VeriSign Class 2 CA - Individual S...
Class 2 Publ
www.verisign.com/CPS Incorp.by ...
Class 3 Publ
所有工作(K)
匯入(I)...
檢視(V)
從這裡新增視窗(W)
新工作台檢視(T)...
貼上(P)
重新整理(F)
匯出清單(L)...
說明(H)
動作
憑證
其他動作

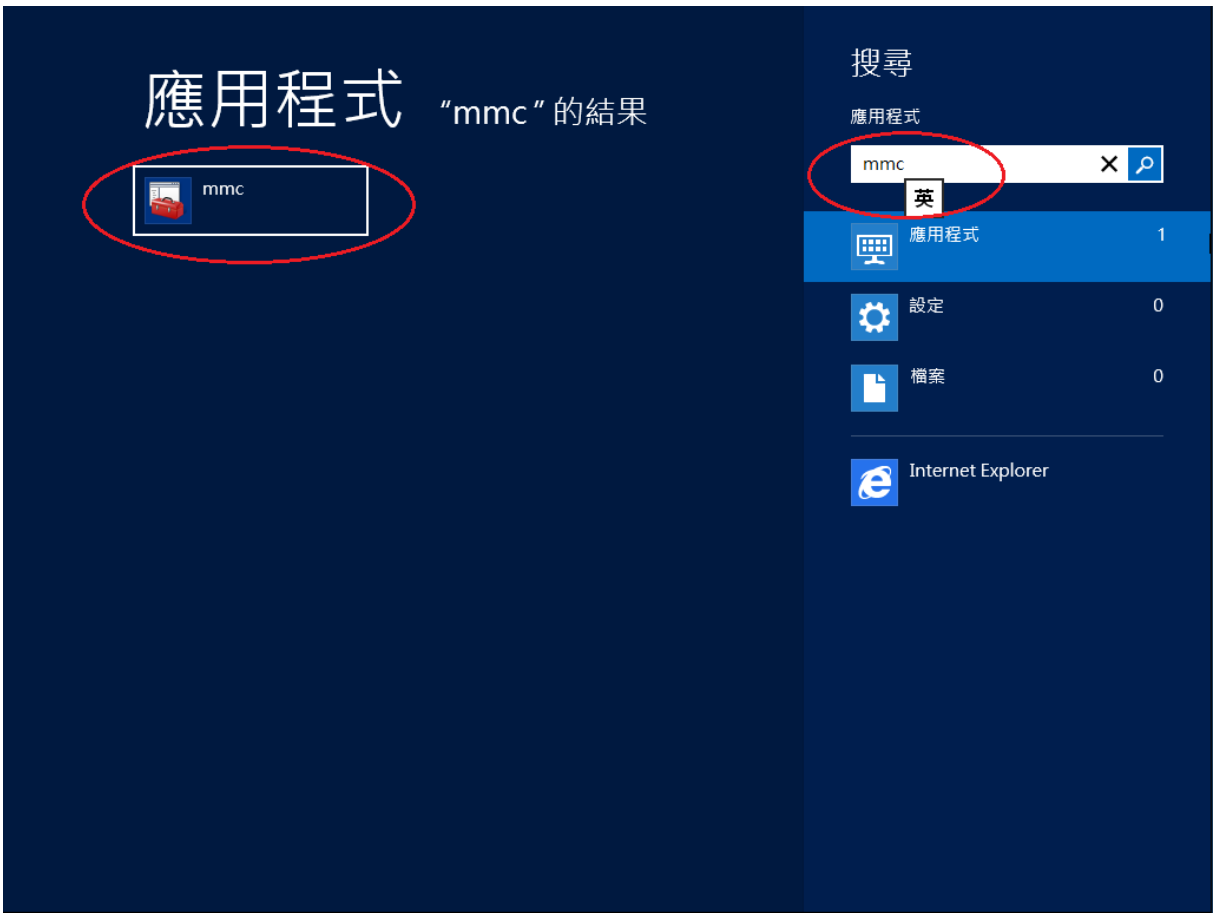


7. 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。

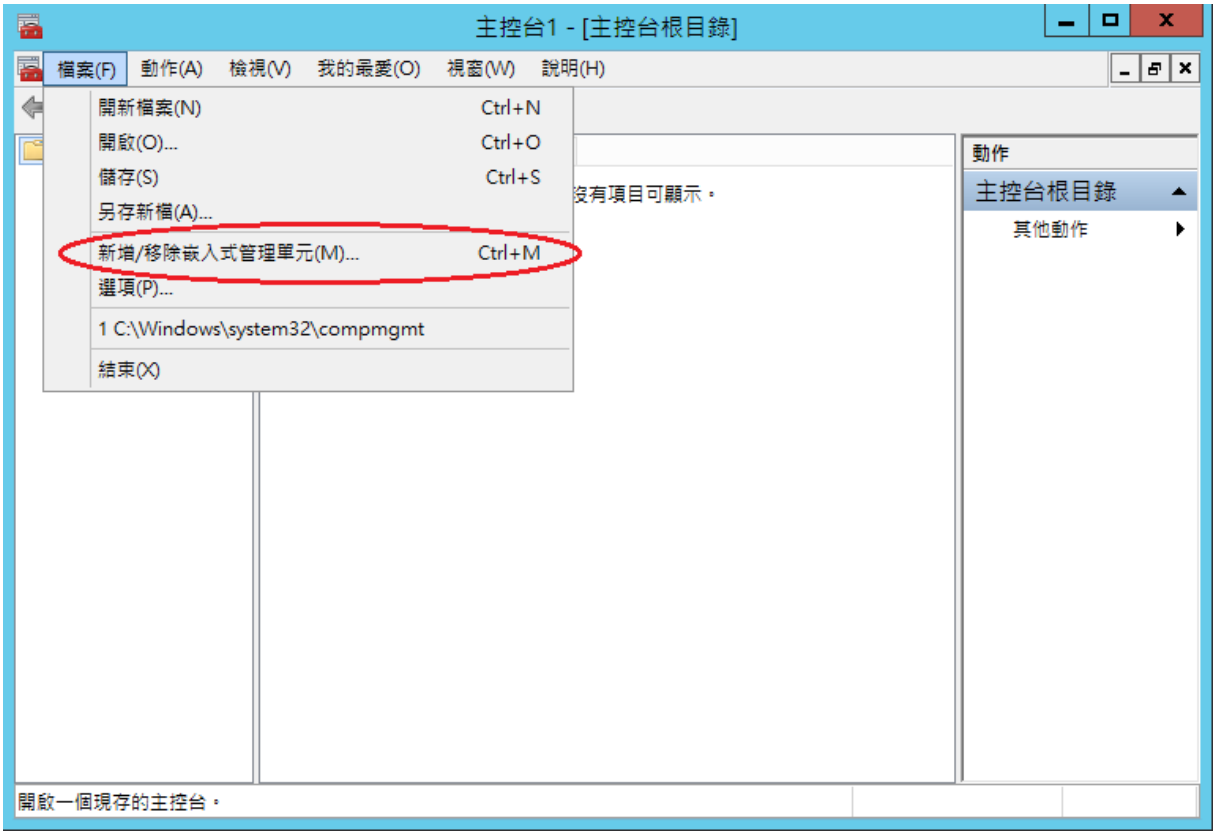


8. 以 https 連線，測試 https 網頁是否正常。

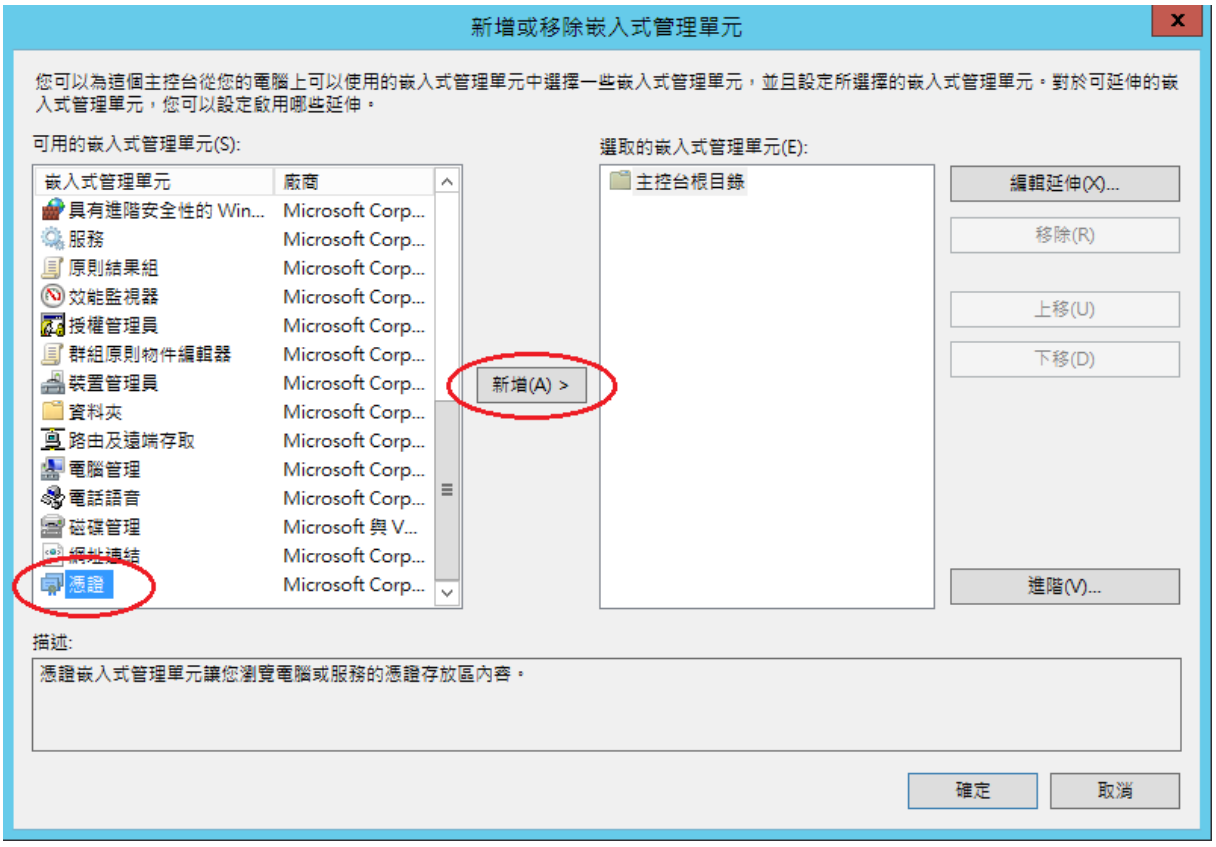
1. 「開始」→「輸入 mmc」，按下「Enter」。



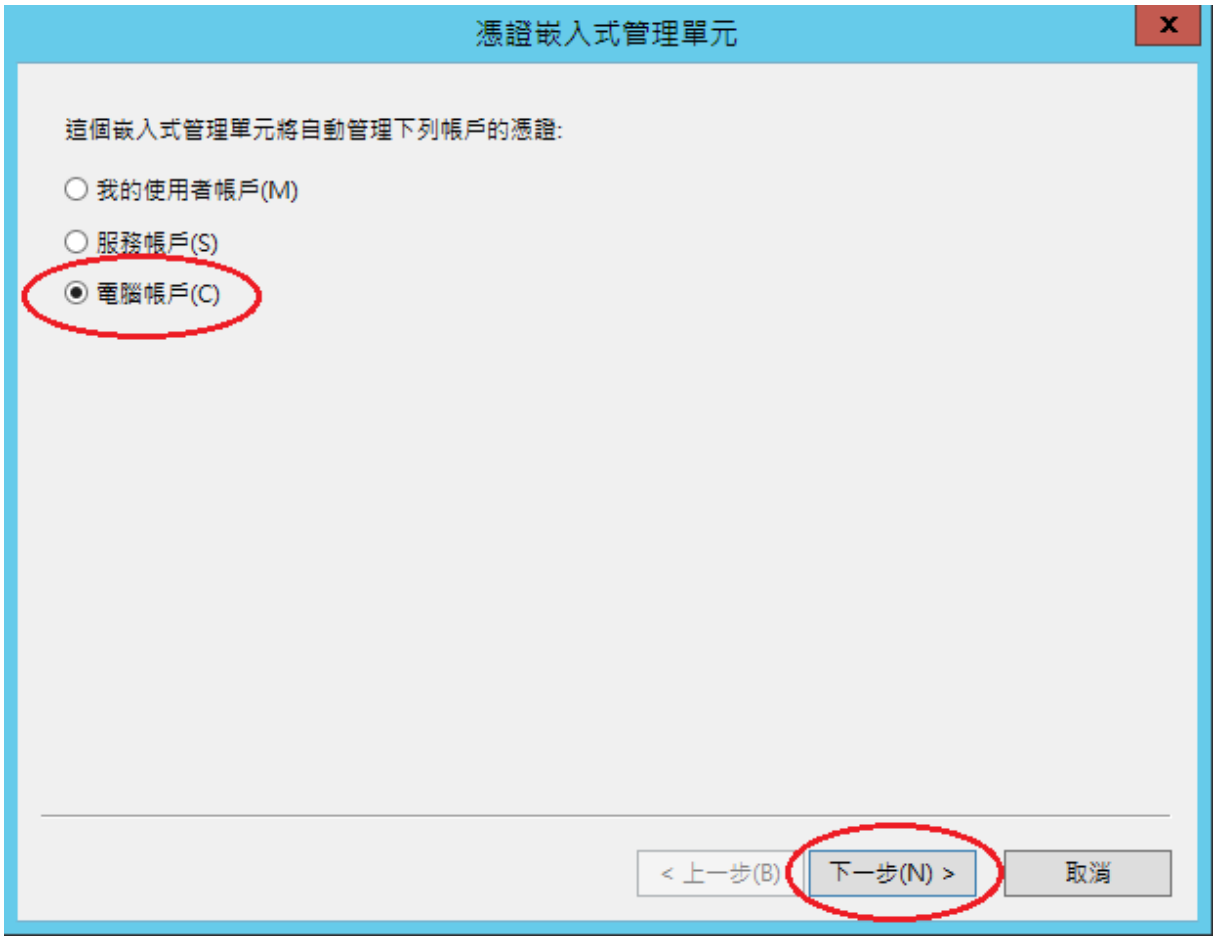
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

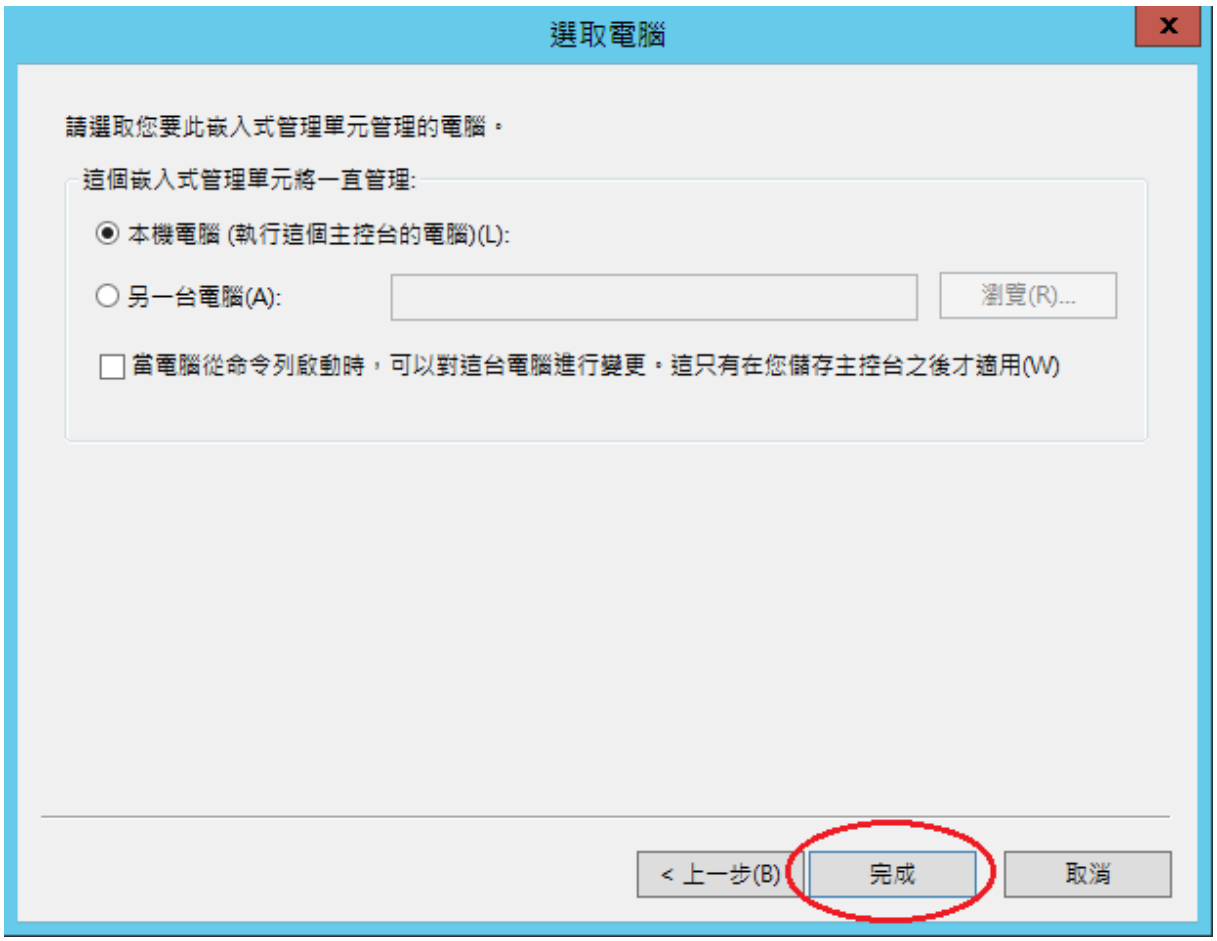


3. 點選「憑證」→「新增」

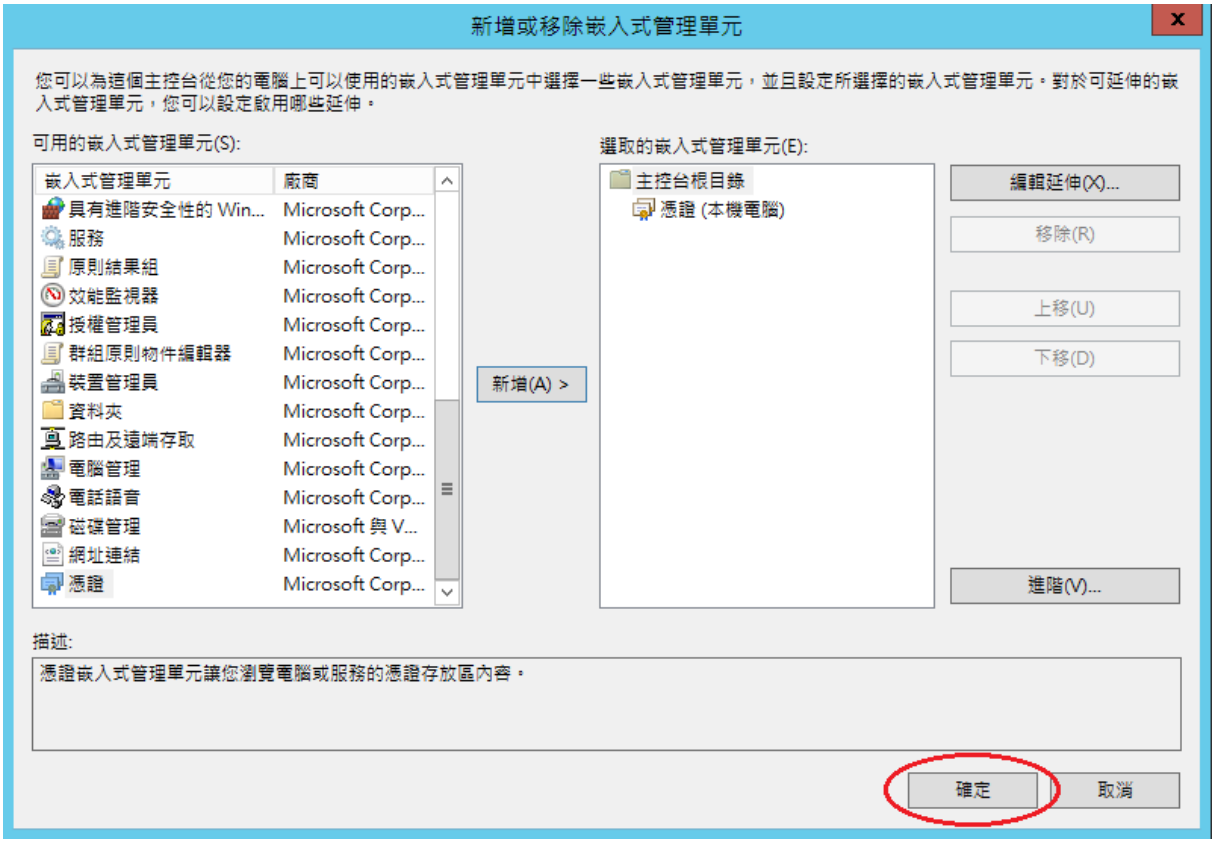


「電腦帳戶」→「下一步」→「完成」。

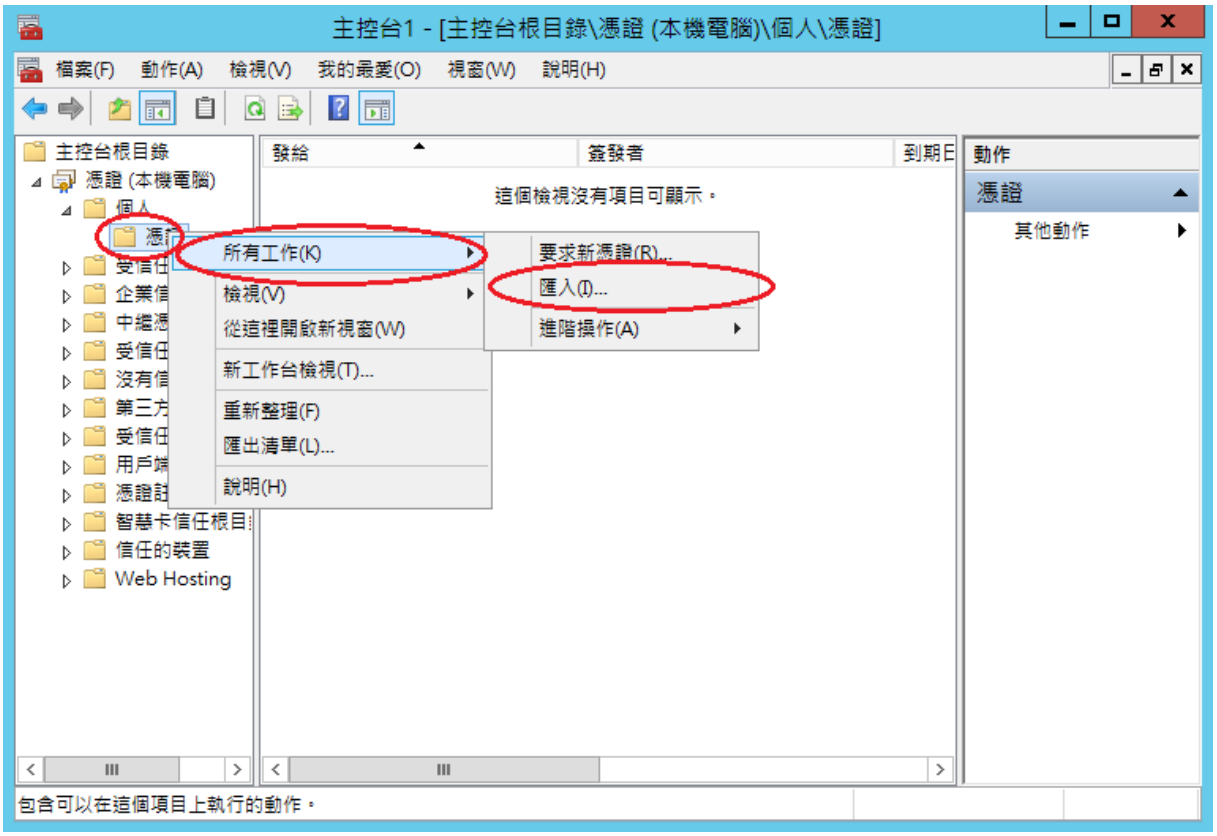

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


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

「確定」。



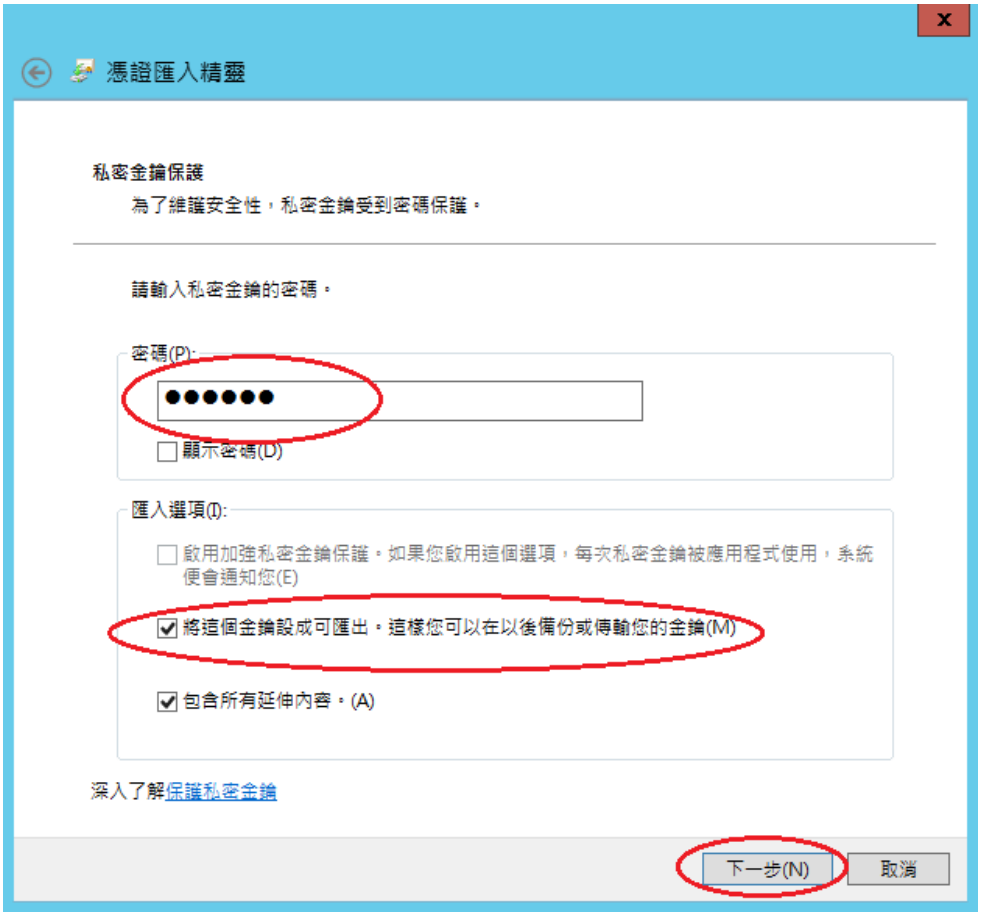
4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

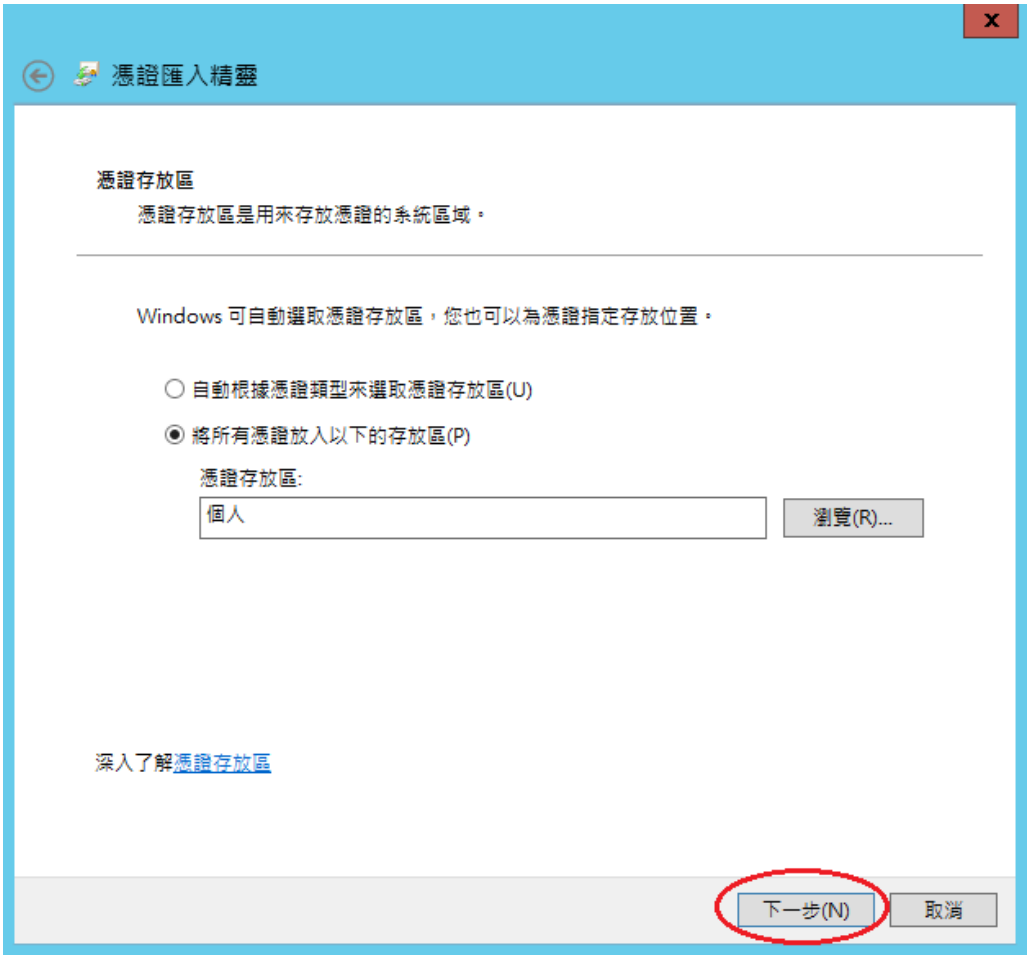


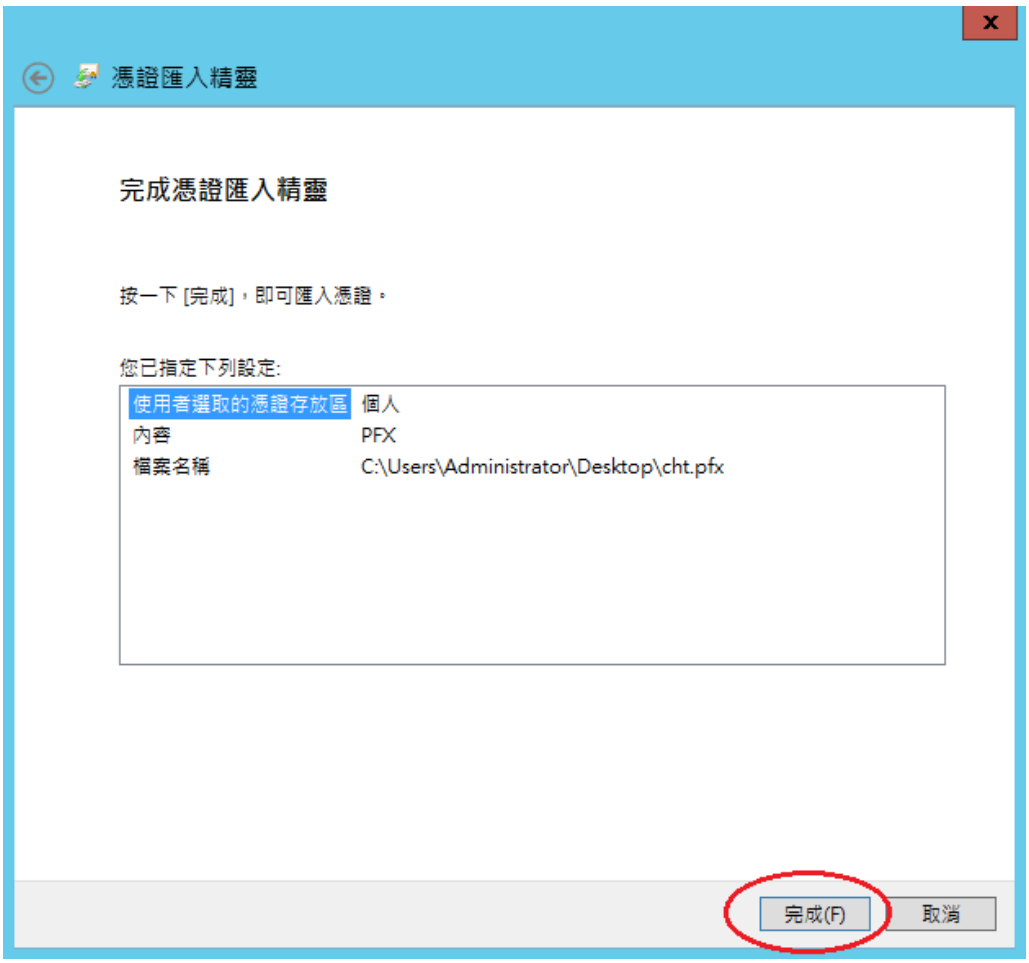
5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

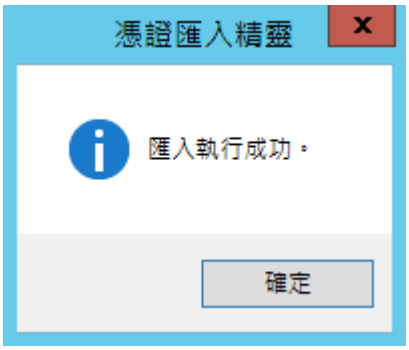

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消

輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。

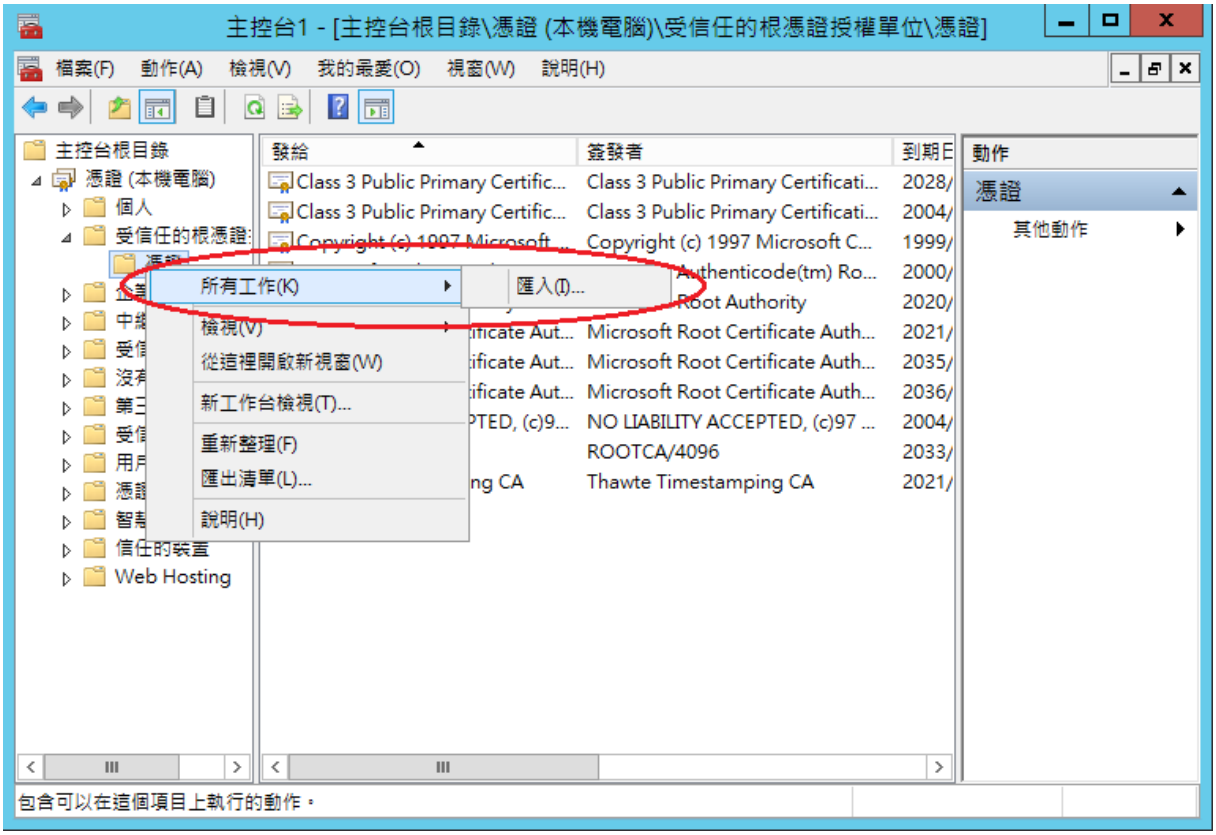


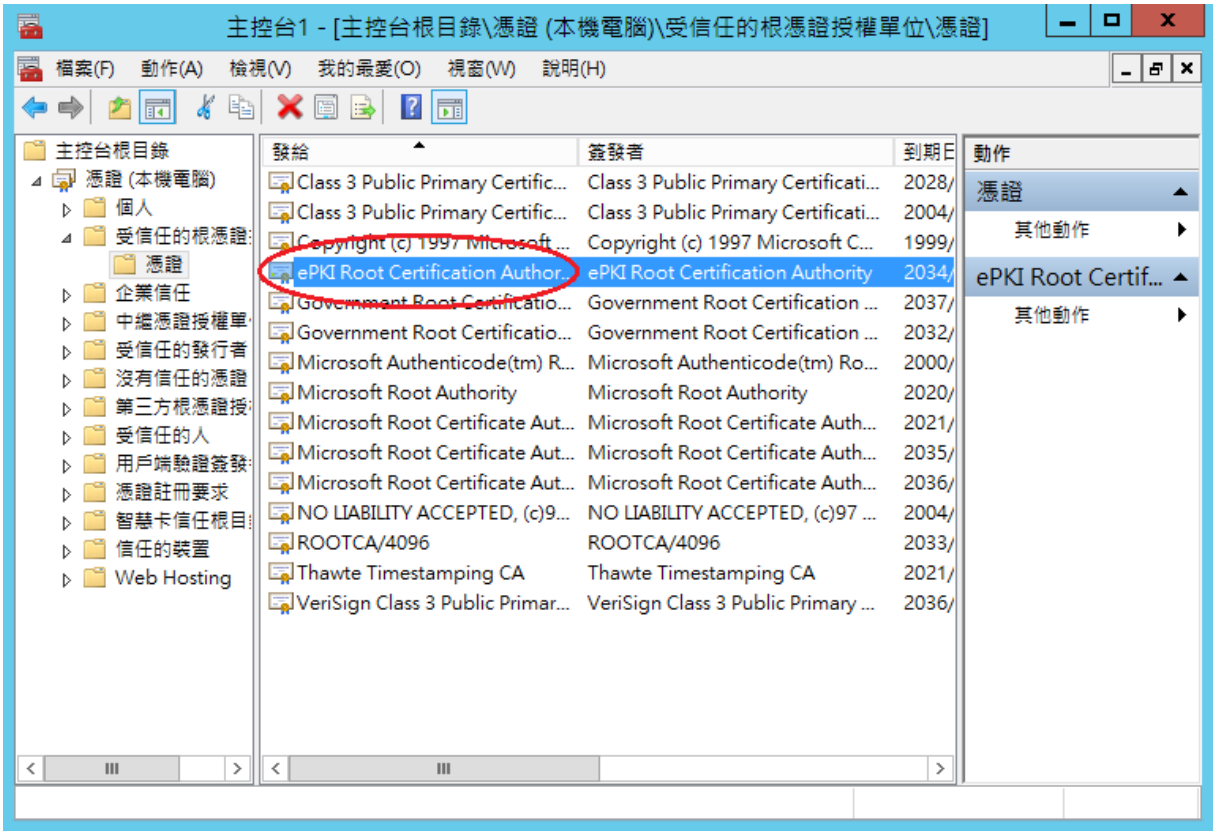

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
個人
瀏覽(R)...
深入了解憑證存放區
下一步(N)
取消

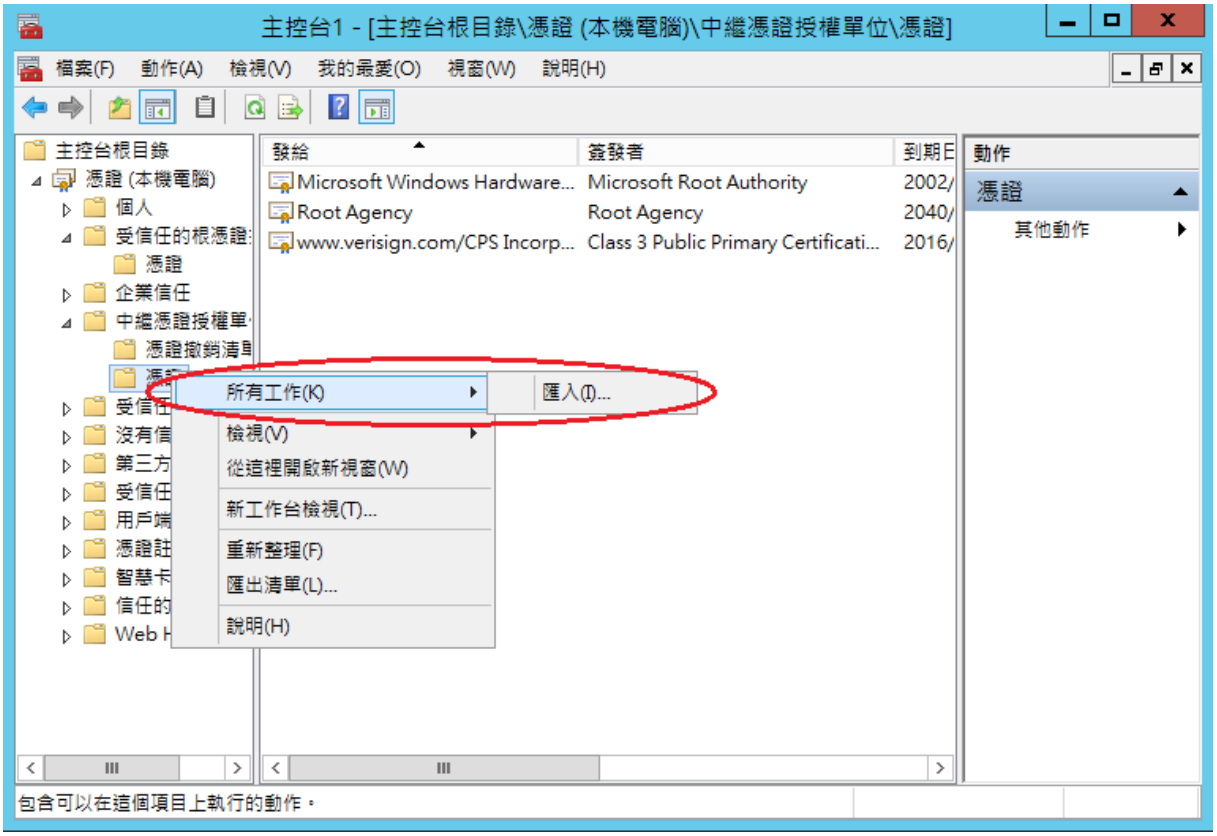

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即可匯入憑證。
您已指定下列設定:
使用者選取的憑證存放區 個人
內容 PFX
檔案名稱 C:\Users\Administrator\Desktop\cht.pfx
完成(F)
取消

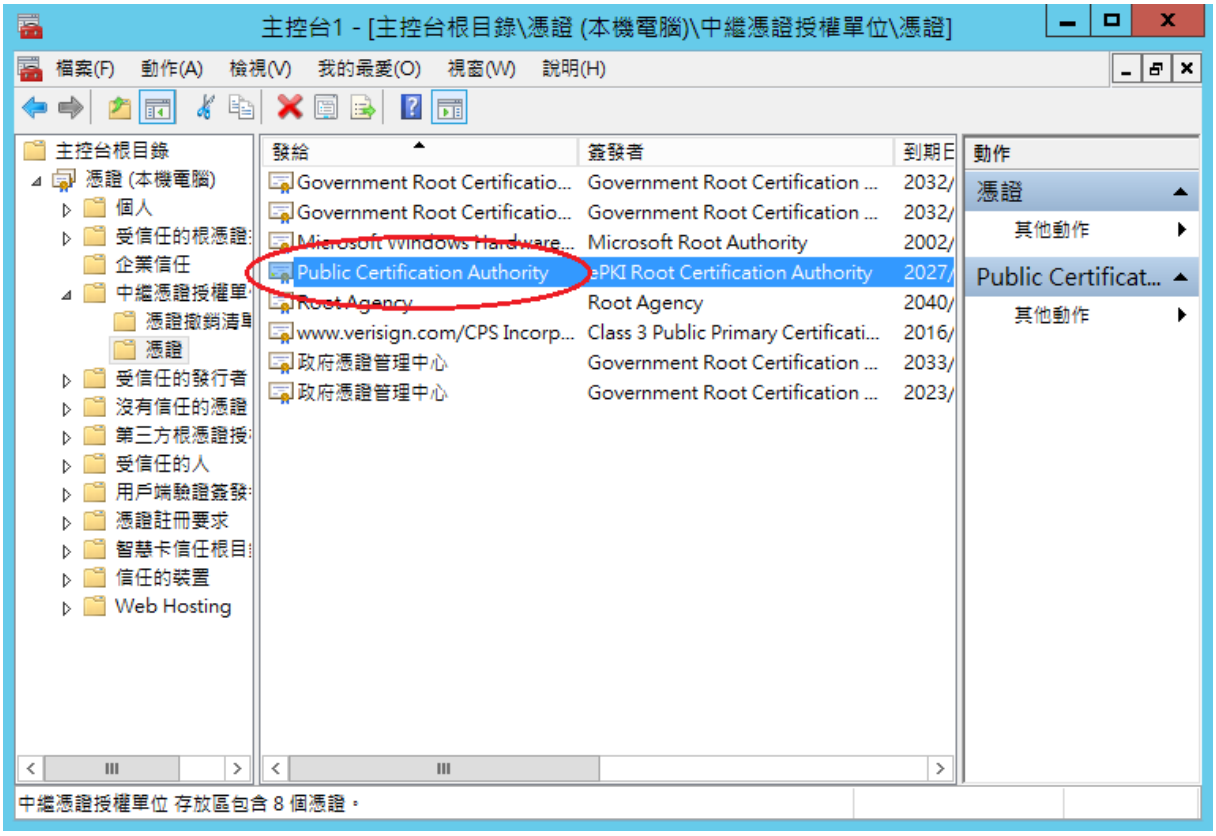


6. 於「信任的根憑證授權」與「中繼憑證授權」匯入 eCA 與 Public CA。
   eCA 憑證：http://eca.hinet.net/download/ROOTeCA_64.crt
   PublicCA2 憑證：http://eca.hinet.net/download/PublicCA2_64.crt

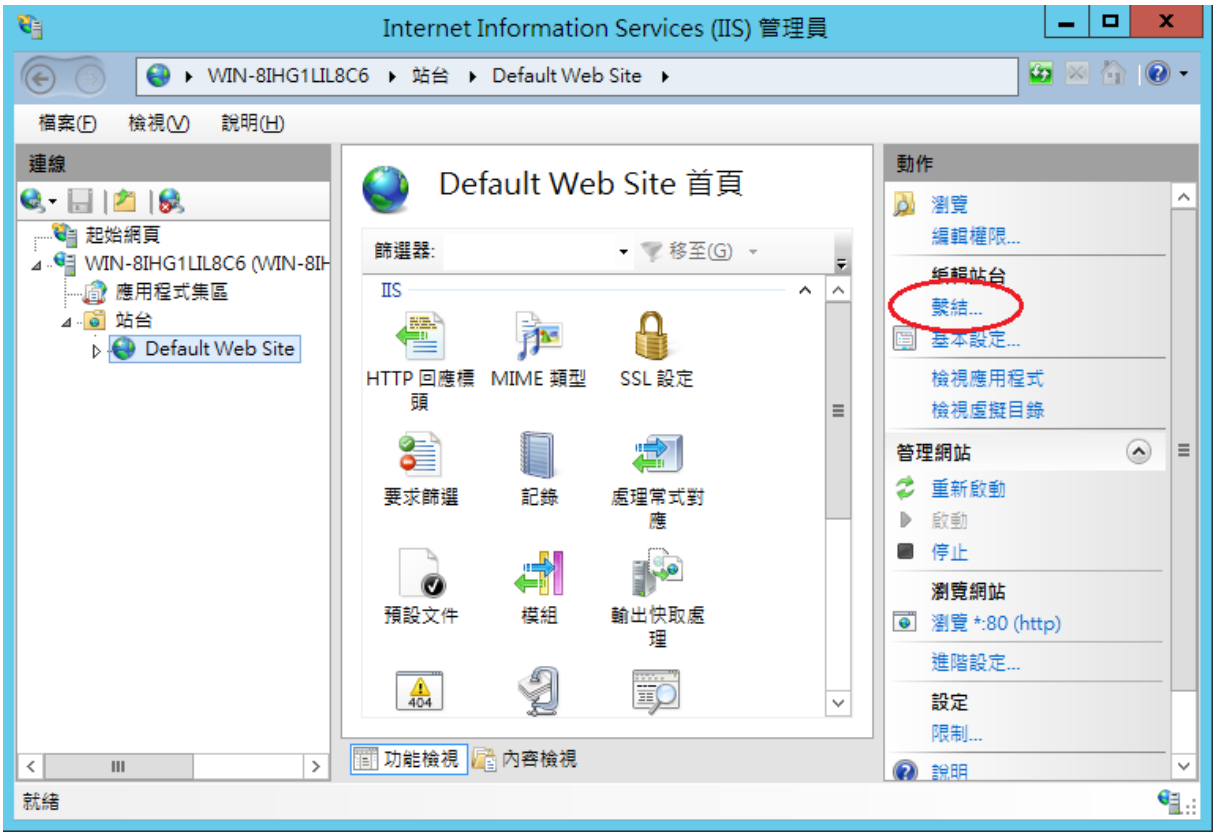


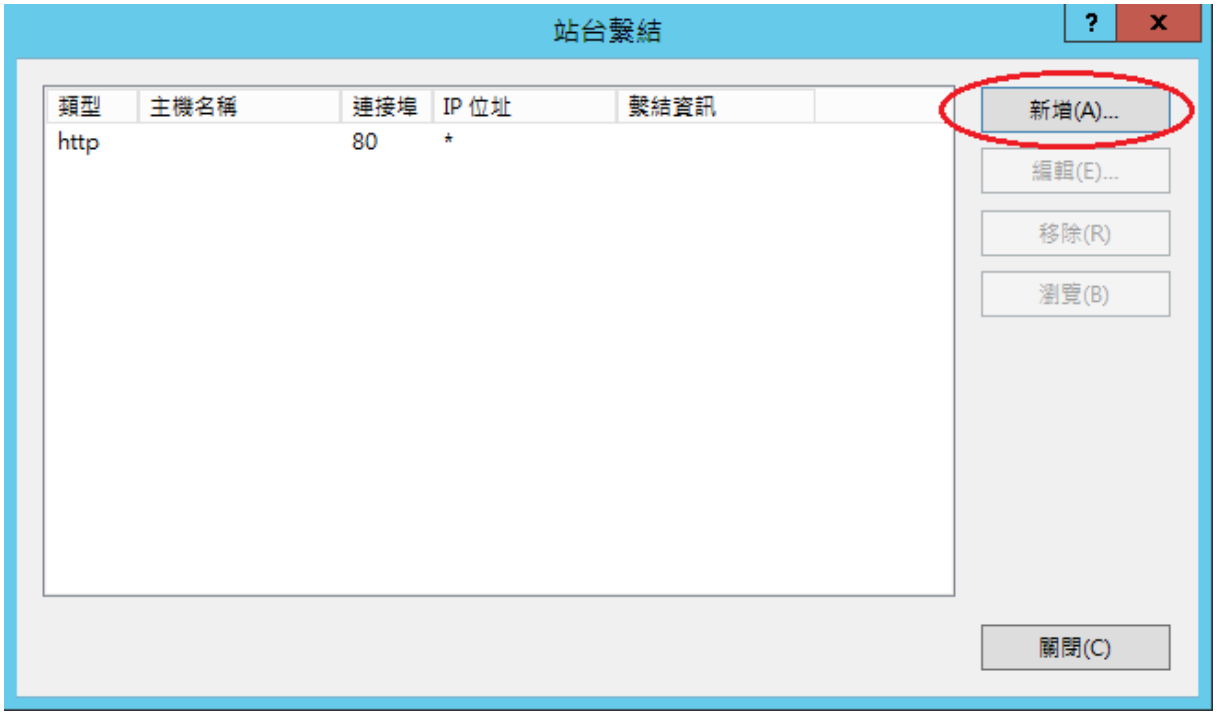

主控台1 - [主控台根目錄\憑證 (本機電腦)\受信任的根憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證
憑證
企業信任
中繼憑證授權單
受信任的發行者
沒有信任的憑證
第三方根憑證授
受信任的人
用戶端驗證簽發
憑證註冊要求
智慧卡信任根目
信任的裝置
Web Hosting
發給
簽發者
到期日
Class 3 Public Primary Certific... Class 3 Public Primary Certificati... 2028/
Class 3 Public Primary Certific... Class 3 Public Primary Certificati... 2004/
Copyright (c) 1997 Microsoft ... Copyright (c) 1997 Microsoft C... 1999/
ePKI Root Certification Author... ePKI Root Certification Authority 2034/
Government Root Certificatio... Government Root Certification ... 2037/
Government Root Certificatio... Government Root Certification ... 2032/
Microsoft Authenticode(tm) R... Microsoft Authenticode(tm) Ro... 2000/
Microsoft Root Authority Microsoft Root Authority 2020/
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2021/
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2035/
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2036/
NO LIABILITY ACCEPTED, (c)9... NO LIABILITY ACCEPTED, (c)97 ... 2004/
ROOTCA/4096 ROOTCA/4096 2033/
Thawte Timestamping CA Thawte Timestamping CA 2021/
VeriSign Class 3 Public Primar... VeriSign Class 3 Public Primary ... 2036/
動作
憑證
其他動作
ePKI Root Certif...
其他動作


主控台1 - [主控台根目錄\憑證 (本機電腦)\中繼憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證
憑證
企業信任
中繼憑證授權單
憑證撤銷清單
憑證
發給
簽發者
到期日
Microsoft Windows Hardware... Microsoft Root Authority 2002/
Root Agency Root Agency 2040/
www.verisign.com/CPS Incorp... Class 3 Public Primary Certificati... 2016/
所有工作(K)
匯入(I)...
檢視(V)
從這裡開啟新視窗(W)
新工作台檢視(T)...
重新整理(F)
匯出清單(L)...
說明(H)
動作
憑證
其他動作
包含可以在這個項目上執行的動作。



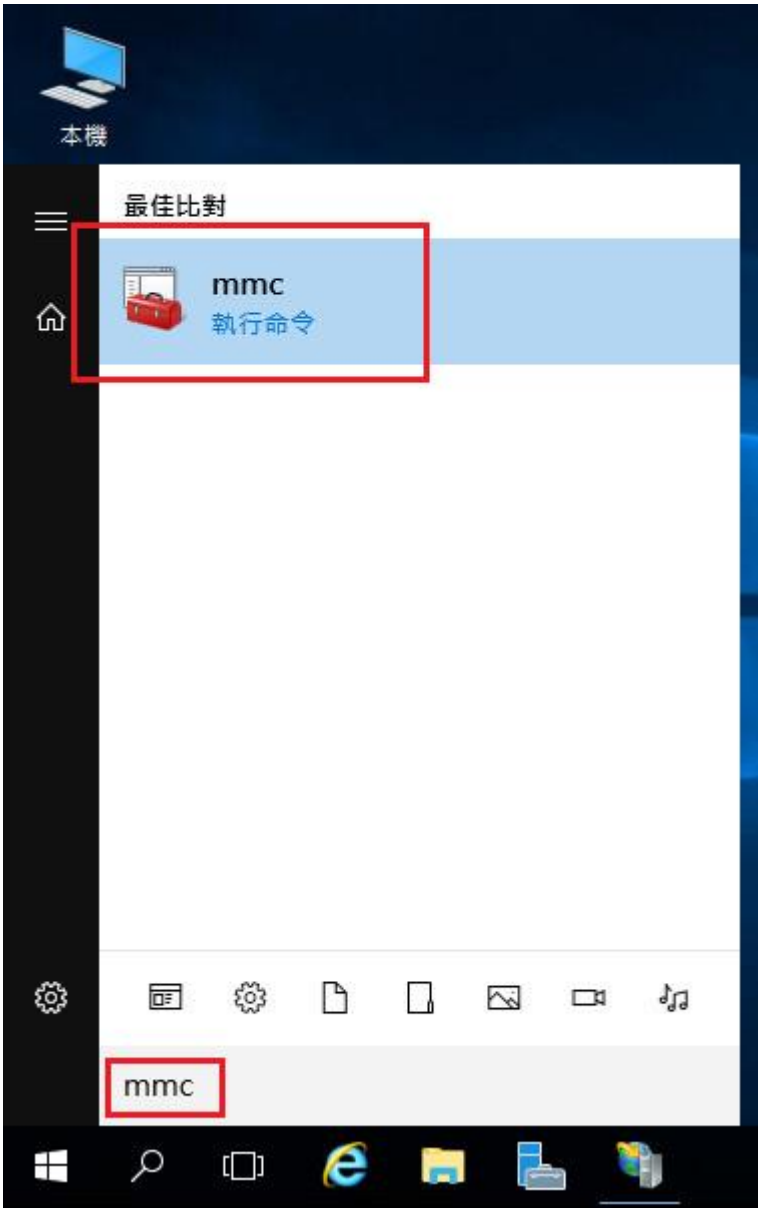
7. 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。



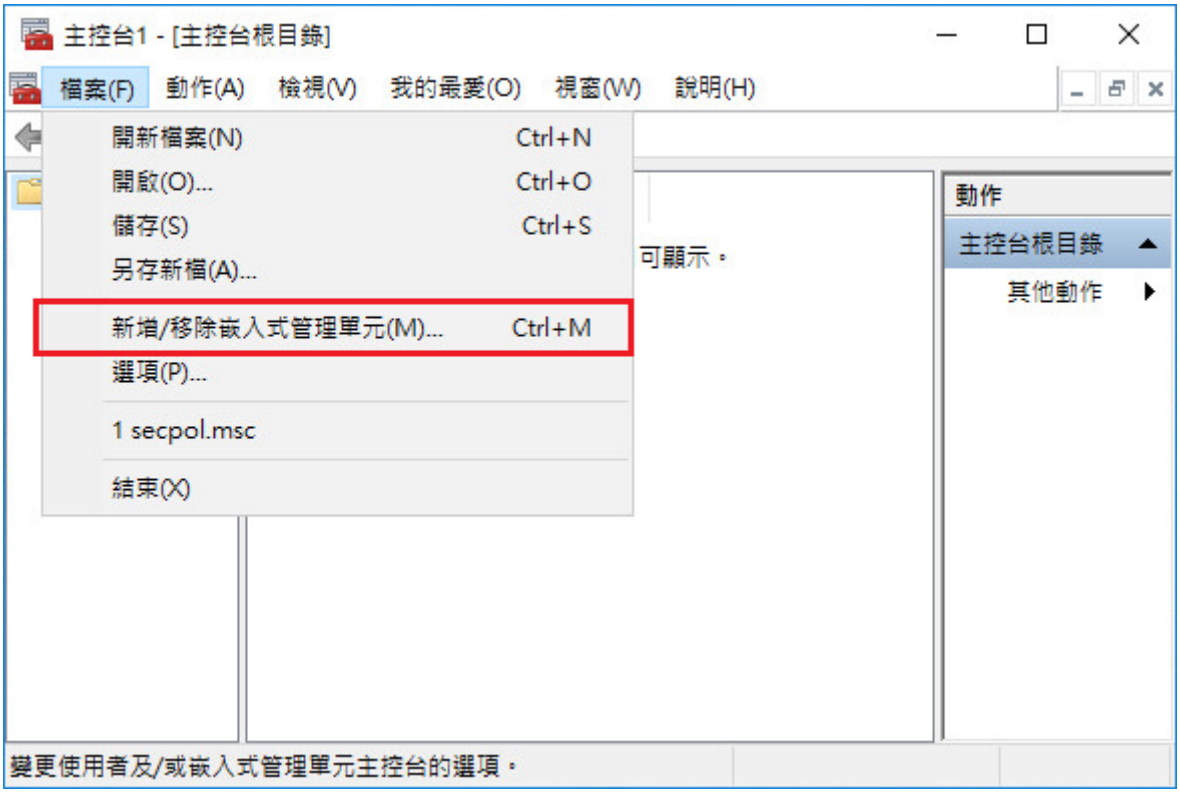


8. 以 https 連線，測試 https 網頁是否正常。

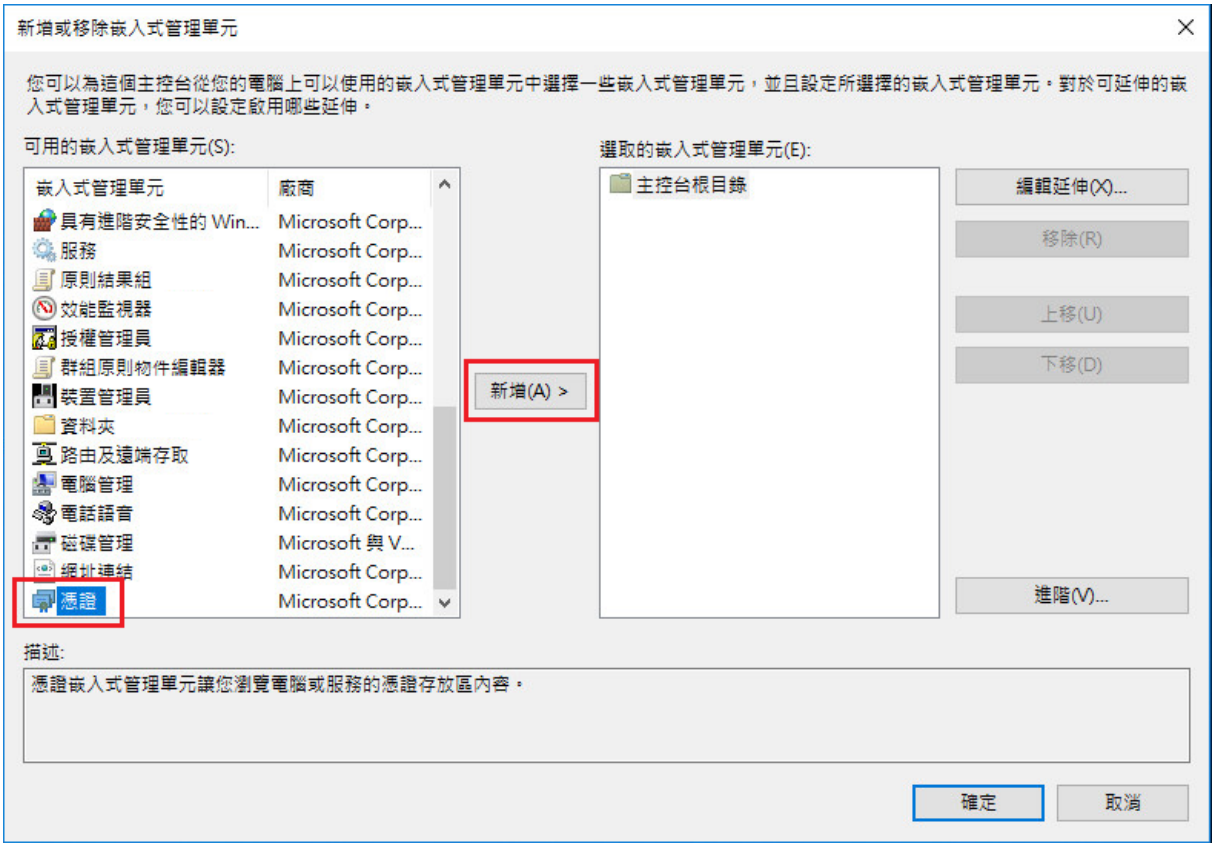
1. 「開始」→「輸入 mmc」，按下「Enter」。



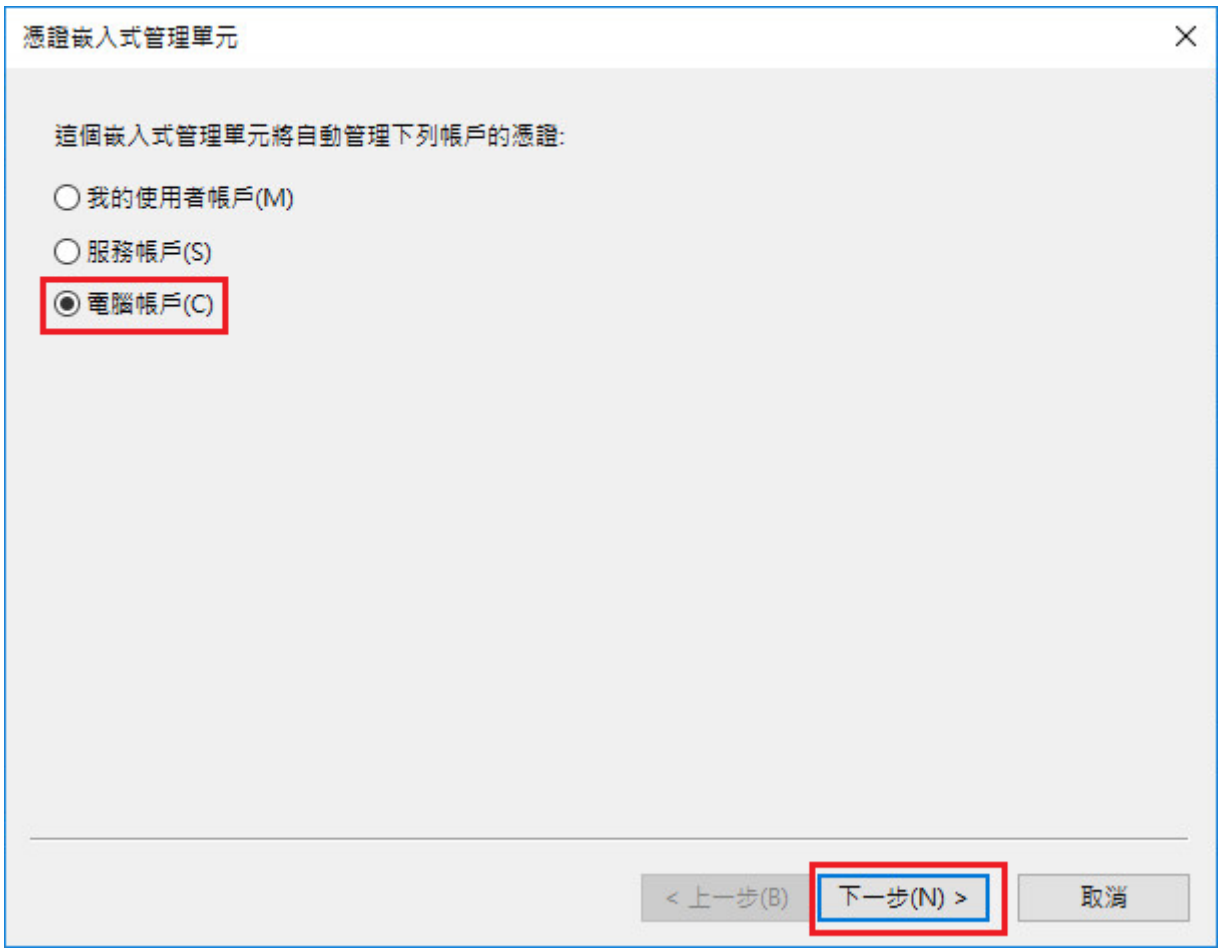
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

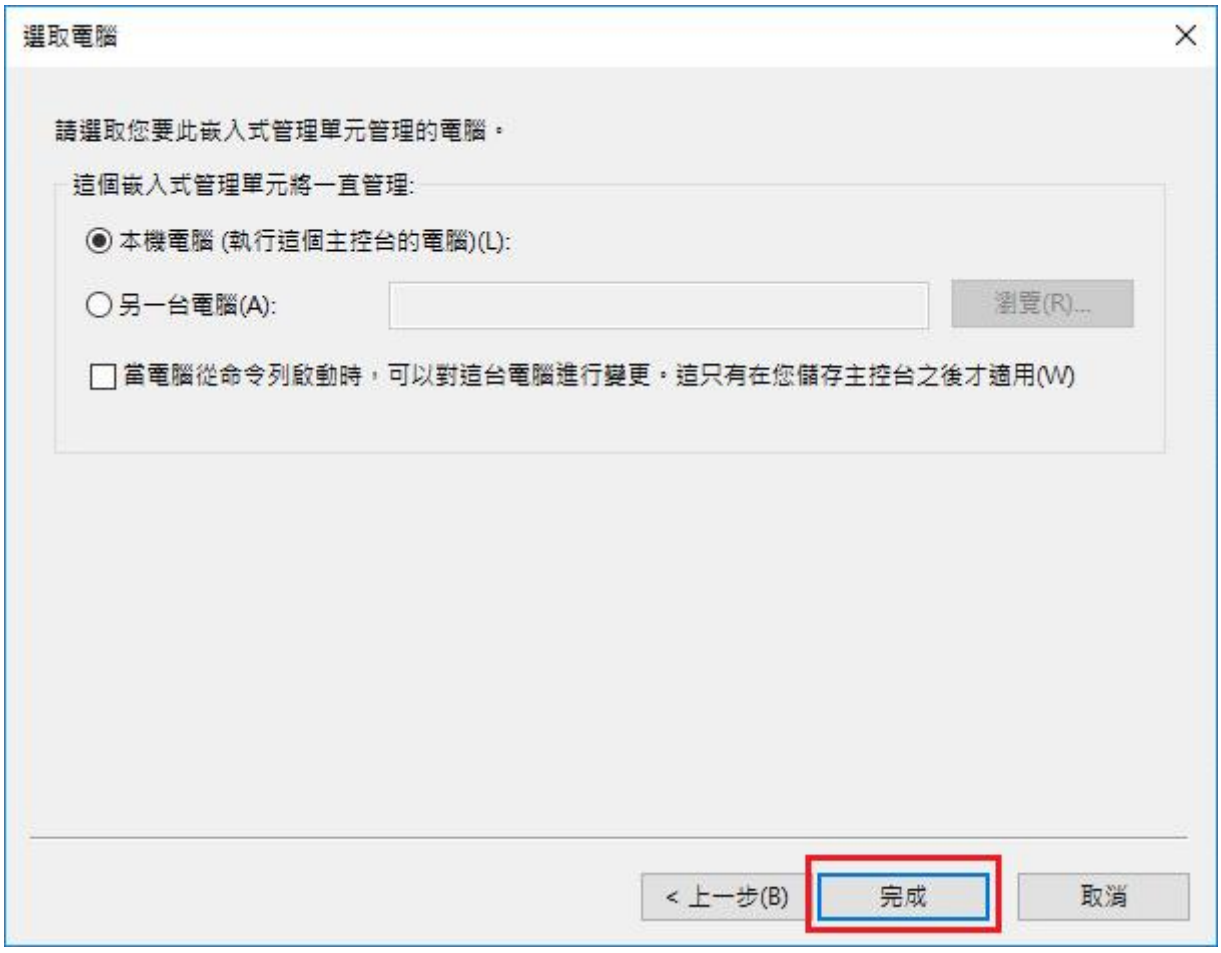


3. 點選「憑證」→「新增」

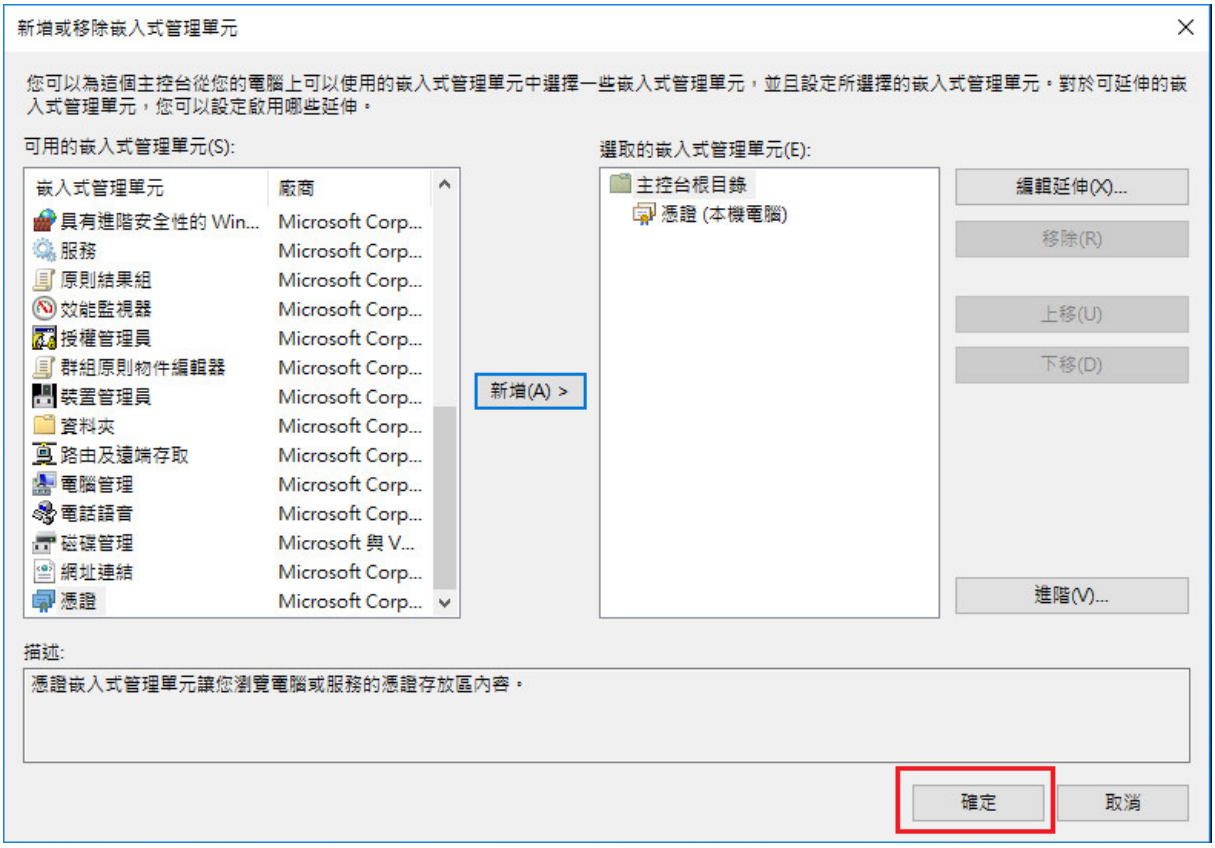


「電腦帳戶」→「下一步」→「完成」。


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

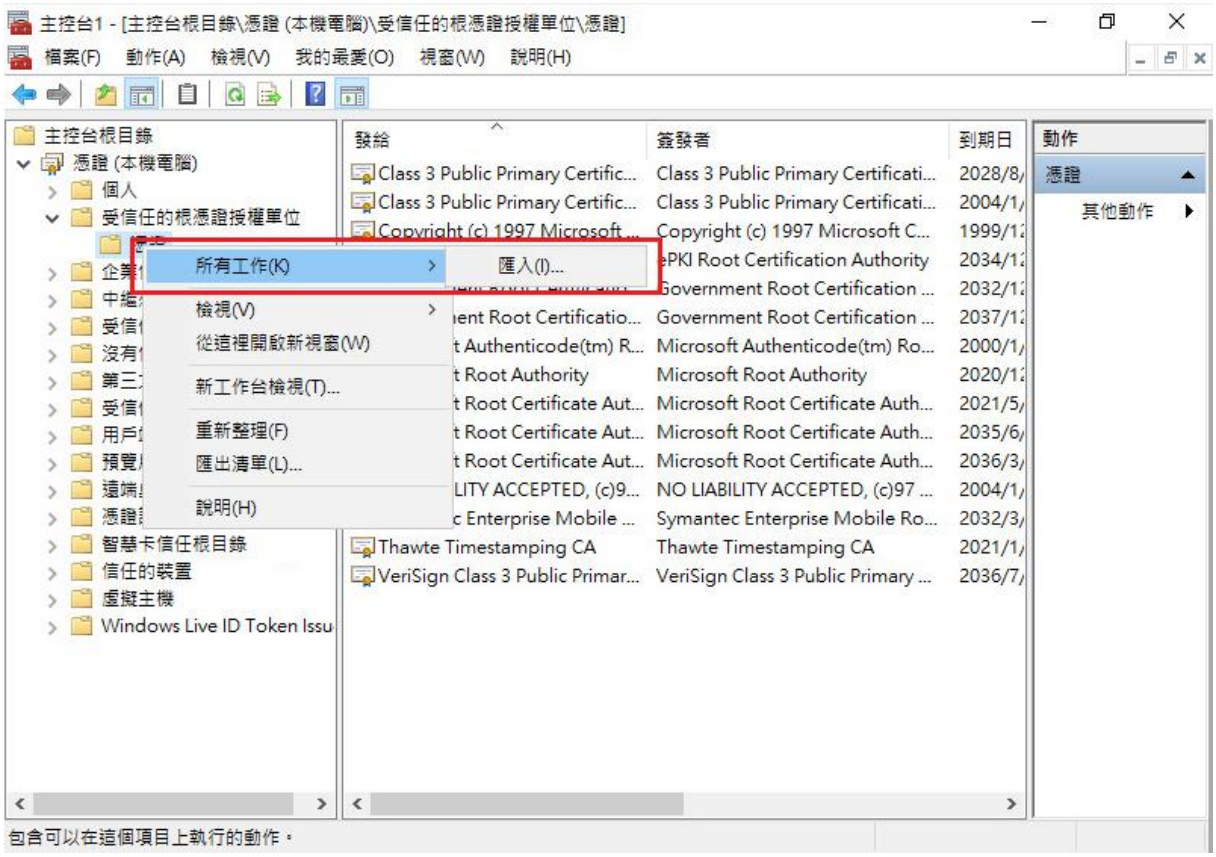
「確定」。

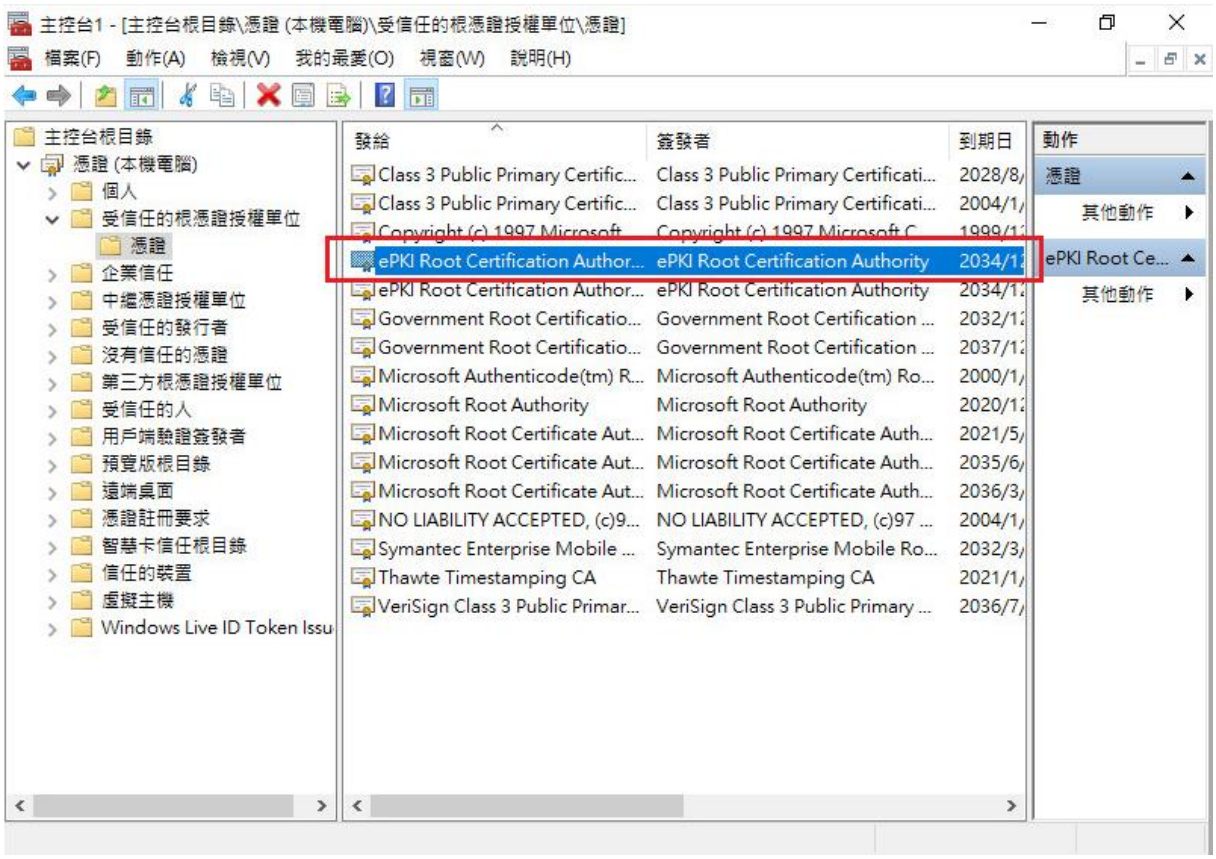


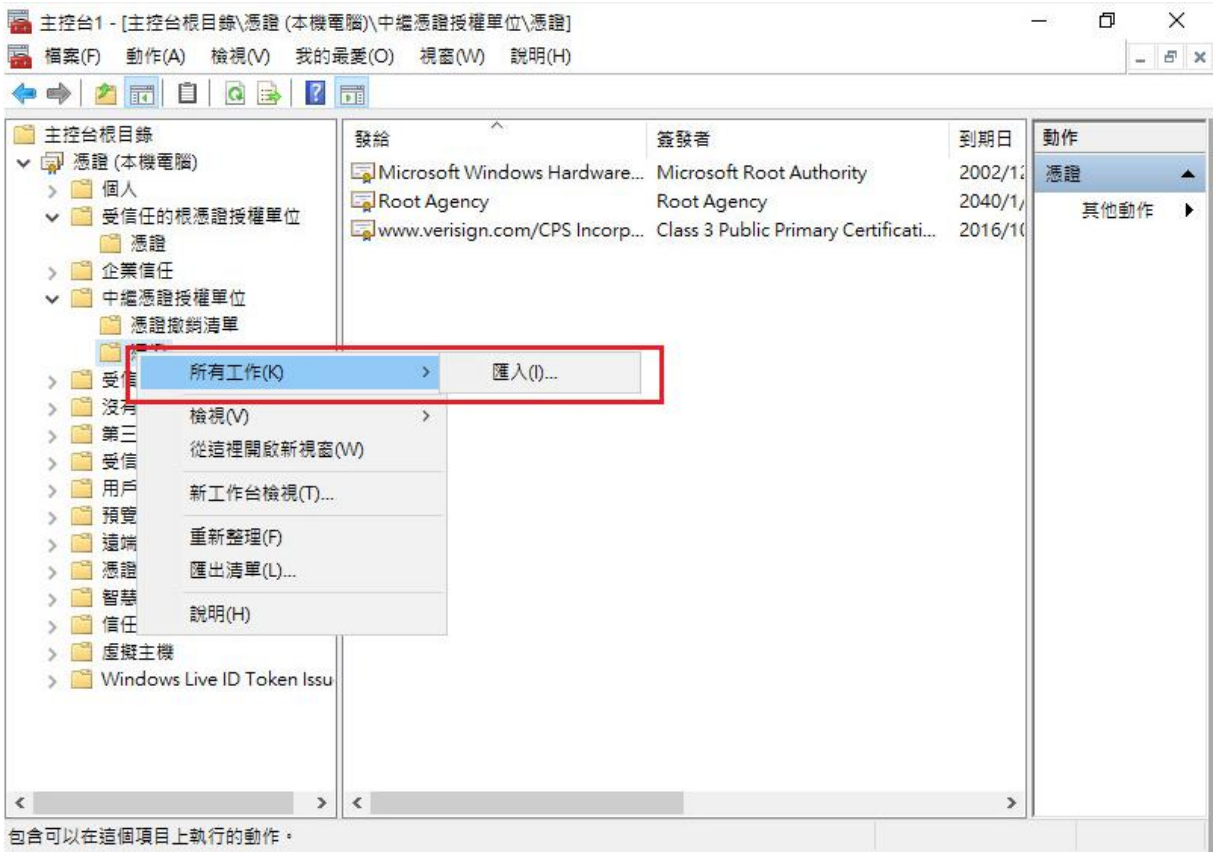
4. 於「信任的根憑證授權」與「中繼憑證授權」匯入 eCA 與 Public CA。

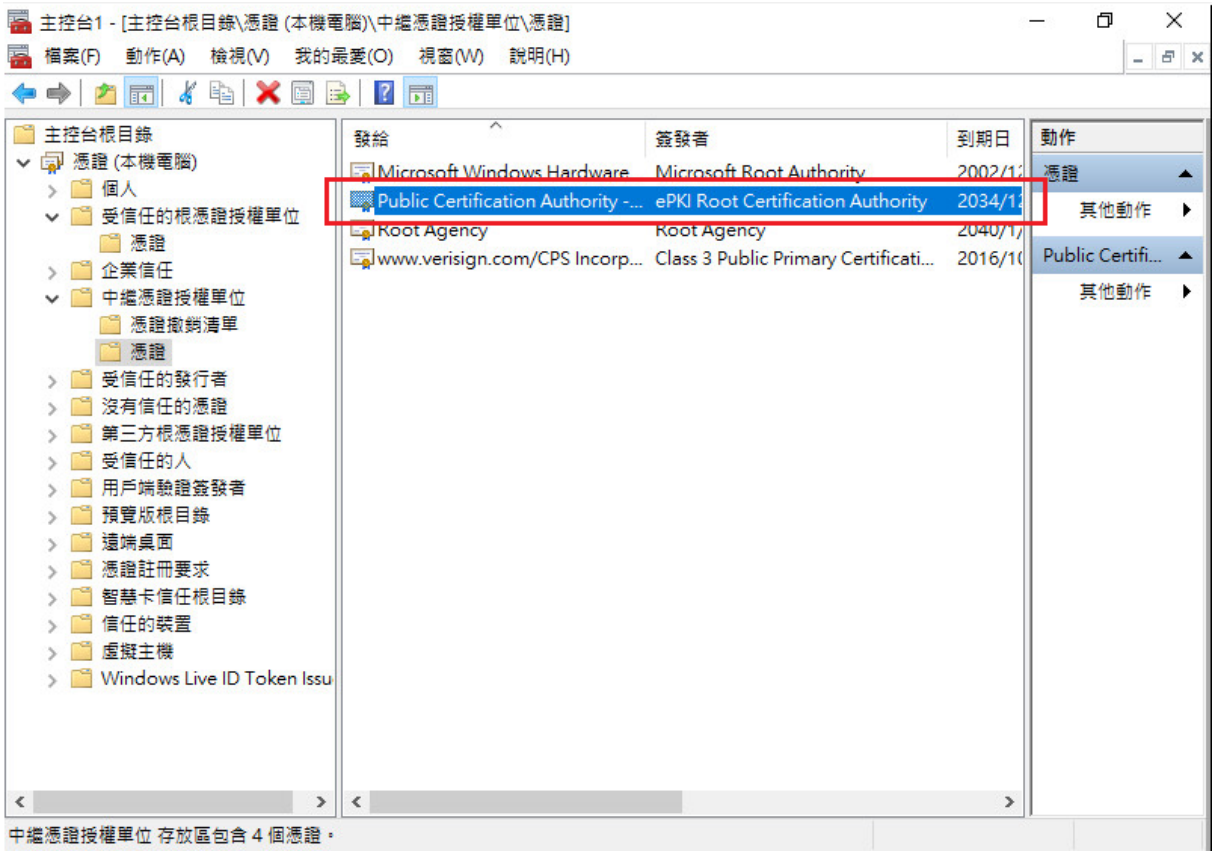
eCA 憑證：http://eca.hinet.net/download/ROOTeCA_64.crt

PublicCA2 憑證：http://eca.hinet.net/download/PublicCA2_64.crt

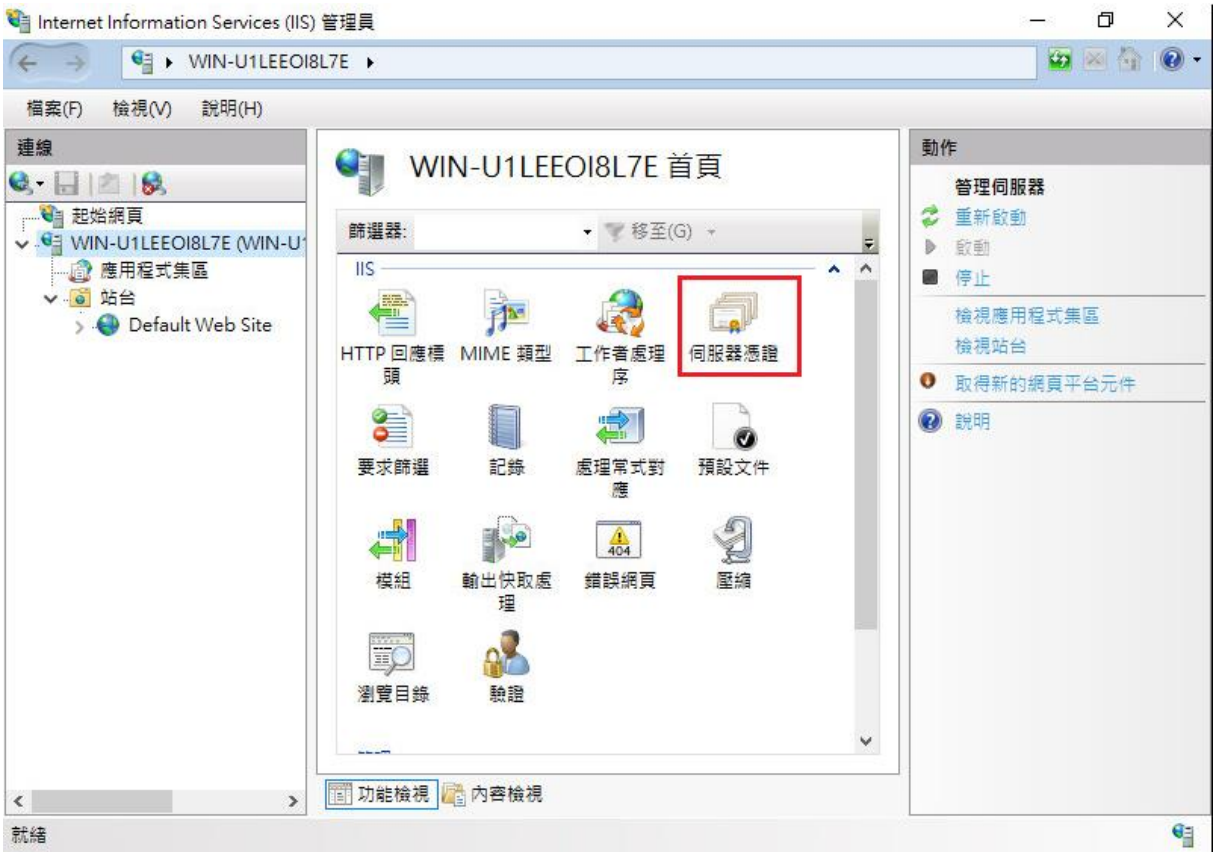



主控台1 - [主控台根目錄\憑證 (本機電腦)\受信任的根憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證授權單位
憑證
企業信任
中繼憑證授權單位
受信任的發行者
沒有信任的憑證
第三方根憑證授權單位
受信任的人
用戶端驗證簽發者
預覽版根目錄
遠端桌面
憑證註冊要求
智慧卡信任根目錄
信任的裝置
虛擬主機
Windows Live ID Token Issu
發給
簽發者
到期日
Class 3 Public Primary Certific... Class 3 Public Primary Certificati... 2028/8/
Class 3 Public Primary Certific... Class 3 Public Primary Certificati... 2004/1/
Copyright (c) 1997 Microsoft ... Copyright (c) 1997 Microsoft C... 1999/1
ePKI Root Certification Author... ePKI Root Certification Authority 2034/1
ePKI Root Certification Author... ePKI Root Certification Authority 2034/1
Government Root Certificatio... Government Root Certification ... 2032/1
Government Root Certificatio... Government Root Certification ... 2037/1
Microsoft Authenticode(tm) R... Microsoft Authenticode(tm) Ro... 2000/1/
Microsoft Root Authority Microsoft Root Authority 2020/1
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2021/5/
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2035/6/
Microsoft Root Certificate Aut... Microsoft Root Certificate Auth... 2036/3/
NO LIABILITY ACCEPTED, (c)9... NO LIABILITY ACCEPTED, (c)97 ... 2004/1/
Symantec Enterprise Mobile ... Symantec Enterprise Mobile Ro... 2032/3/
Thawte Timestamping CA Thawte Timestamping CA 2021/1/
VeriSign Class 3 Public Primar... VeriSign Class 3 Public Primary ... 2036/7/
動作
憑證
其他動作
ePKI Root Ce...
其他動作

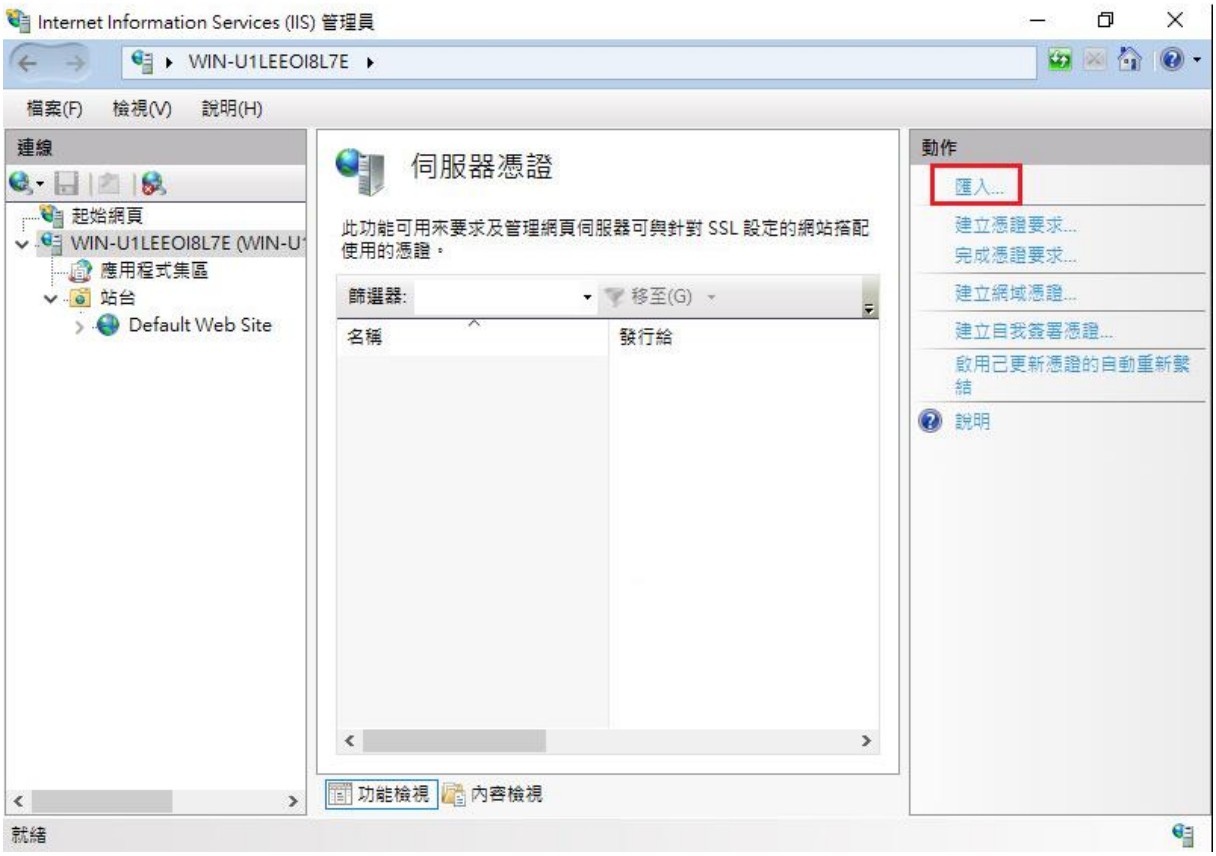

主控台1 - [主控台根目錄\憑證 (本機電腦)\中繼憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證授權單位
憑證
企業信任
中繼憑證授權單位
憑證撤銷清單
憑證
Windows Live ID Token Issu
發給
簽發者
到期日
Microsoft Windows Hardware... Microsoft Root Authority 2002/12
Root Agency Root Agency 2040/1/
www.verisign.com/CPS Incorp... Class 3 Public Primary Certificati... 2016/10
動作
憑證
其他動作
所有工作(K)
匯入(I)...
檢視(V)
從這裡開啟新視窗(W)
新工作台檢視(T)...
重新整理(F)
匯出清單(L)...
說明(H)
包含可以在這個項目上執行的動作。



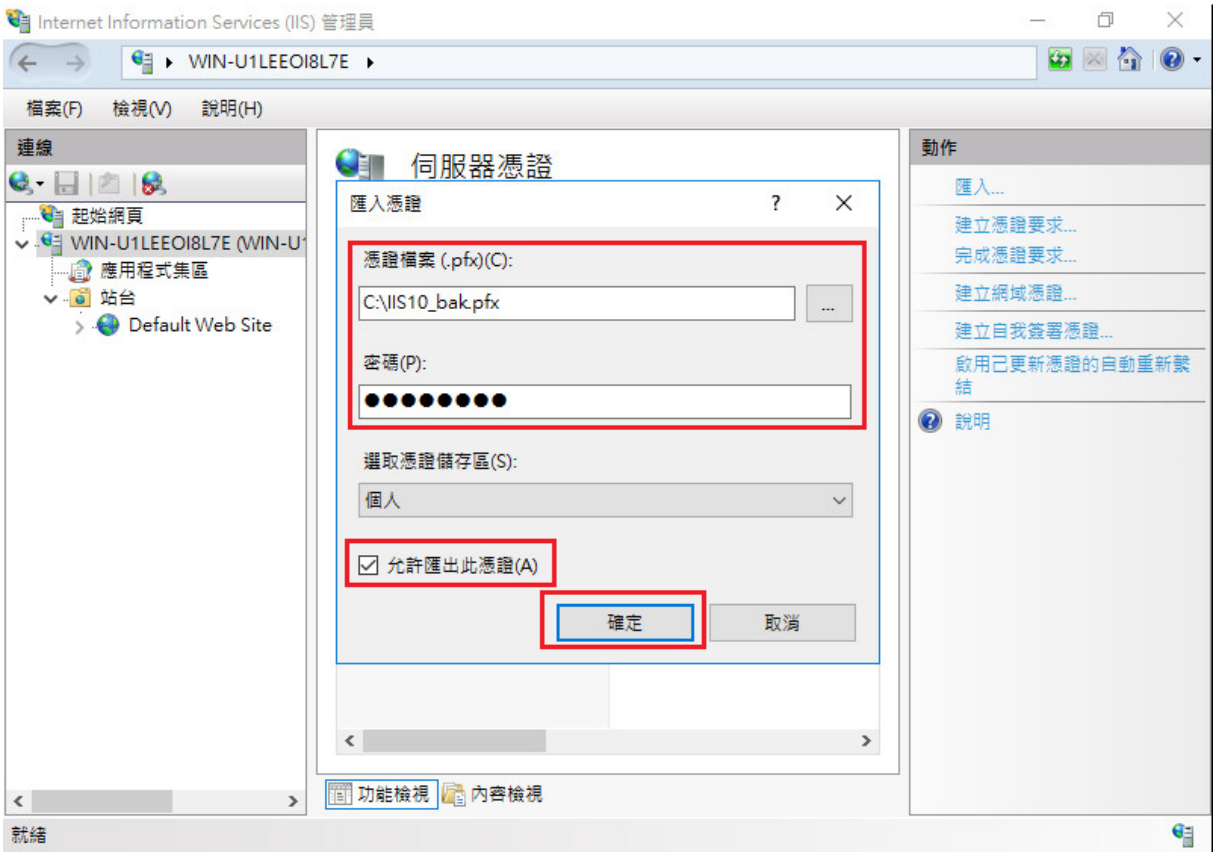
5. 開啟「Internet Information Services (IIS)管理員」。
6. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。

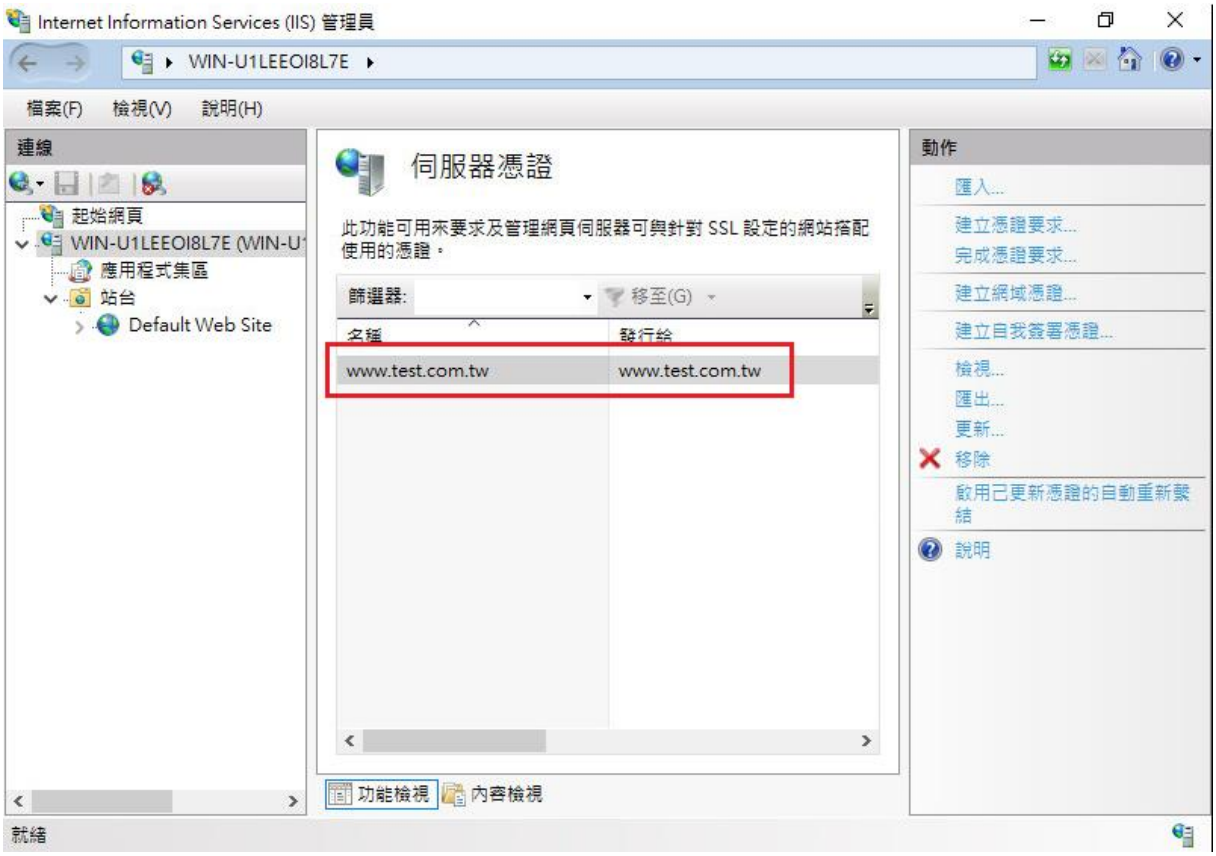


7. 點選右邊的「匯入」。

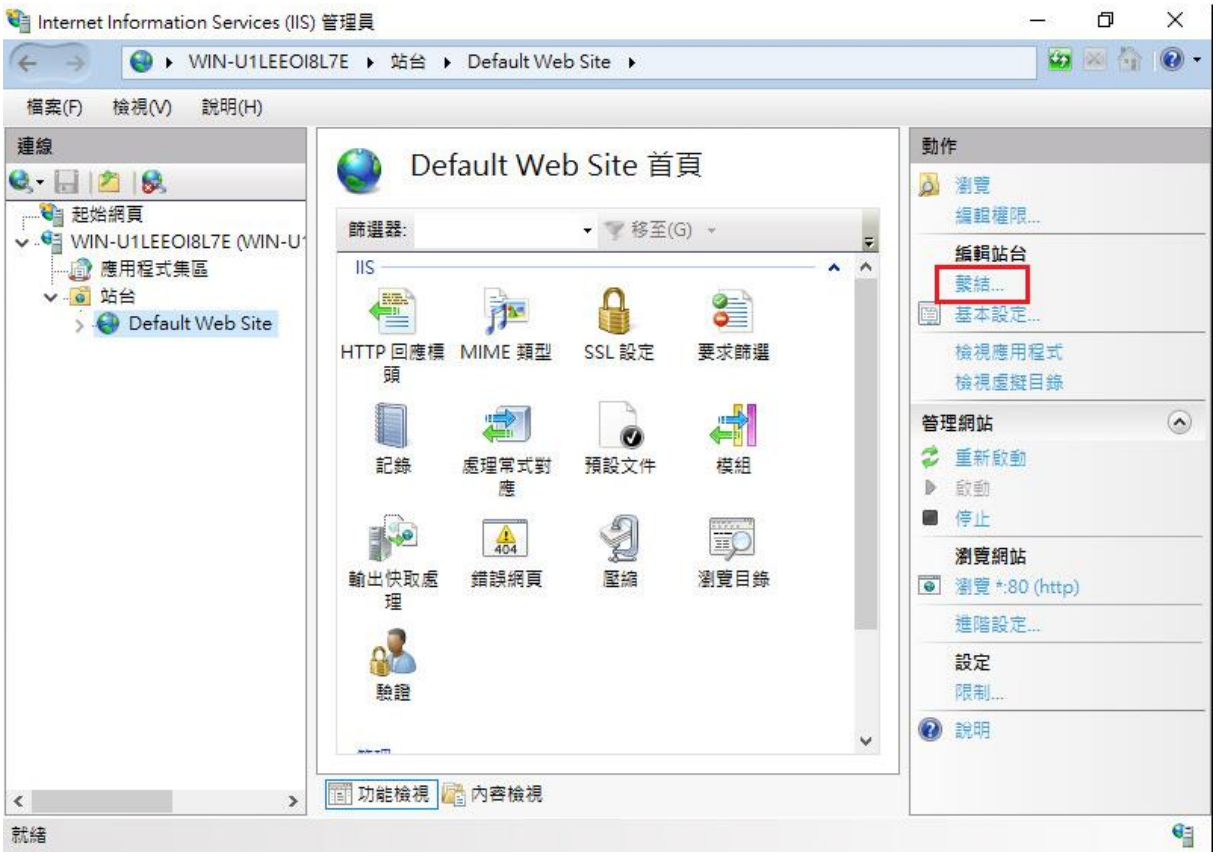


8. 輸入憑證檔案路徑與密碼，並勾選「允許匯出此憑證」後，按下確定。

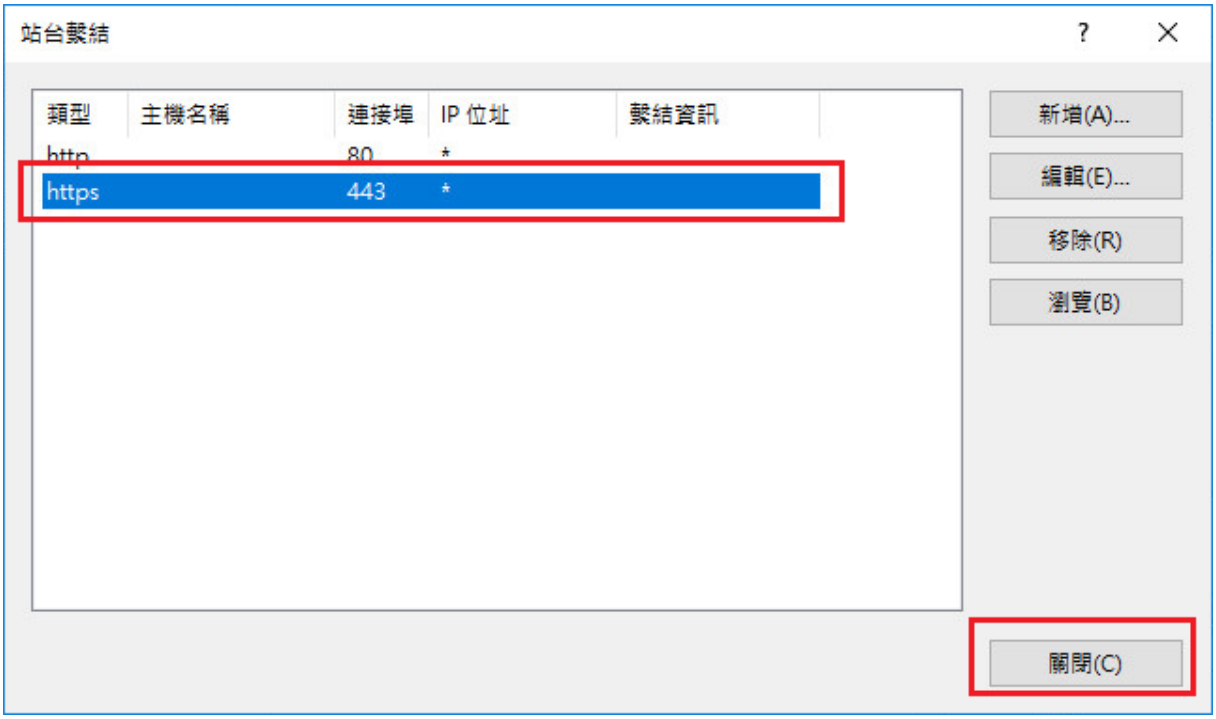




9. 點選左邊的站台。之後重新透過「繫結」來啟用憑證與 https。




站台繫結
類型
主機名稱
連接埠
IP 位址
繫結資訊
http
80
*
新增(A)...
編輯(E)...
移除(R)
瀏覽(B)
關閉(C)
新增站台繫結
類型(T):
https
IP 位址(I):
全部未指派
連接埠(O):
443
主機名稱(H):
需要伺服器名稱指示(N)
SSL 憑證(F):
www.test.com.tw
選取(L)...
檢視(V)...
確定
取消



10. 以 https 連線，測試 https 網頁是否正常。