網路中文
www.net-chinese.com.tw

CSR 生成與憑證安裝指南
適用於 Windows

2022 年 4 月更新 二版

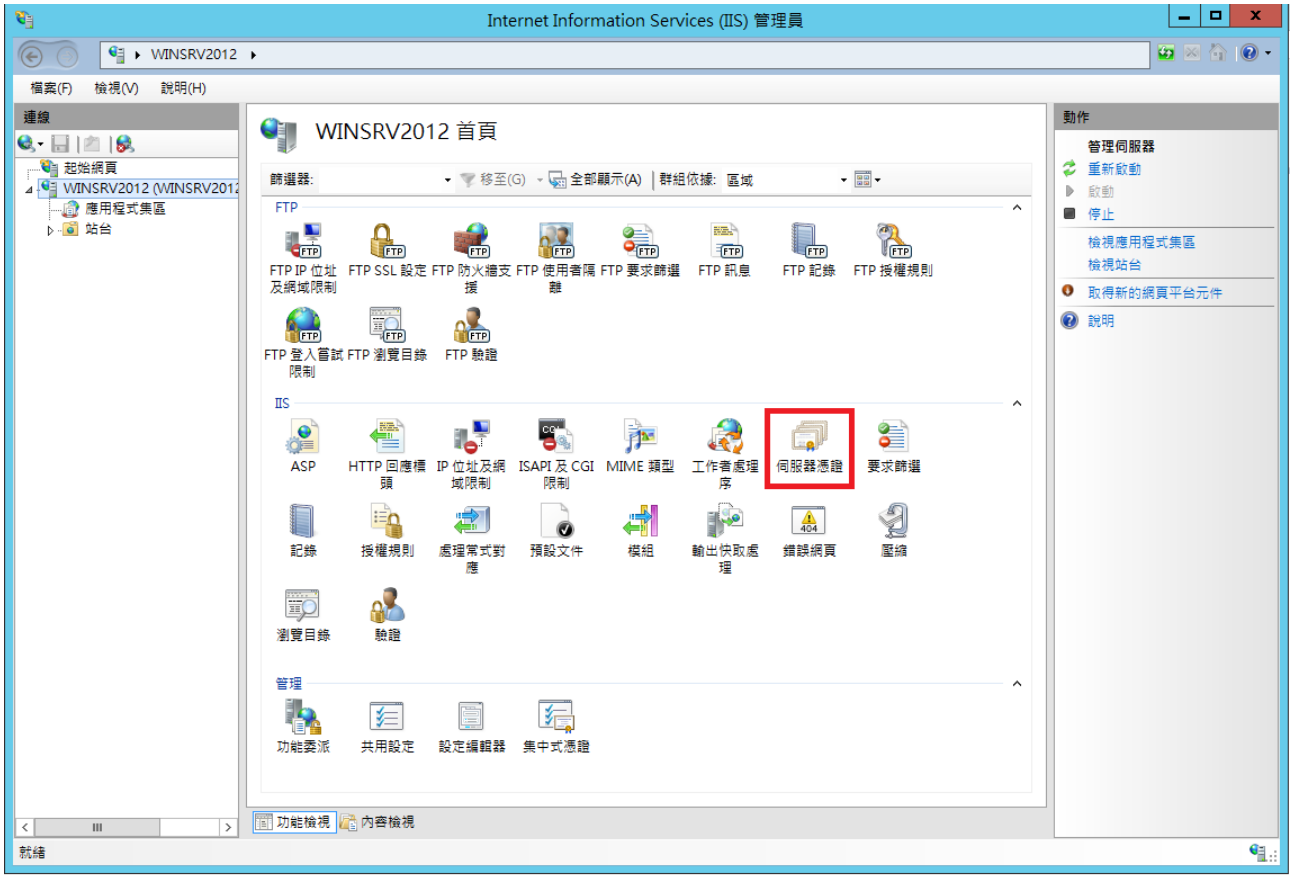
章 節

1

生成 CSR 憑證請求檔

本章節將開始帶您操作如何使用 IIS 網站伺服器產生申請憑證時必要的 CSR(Certificeate Signing Request) 文件。

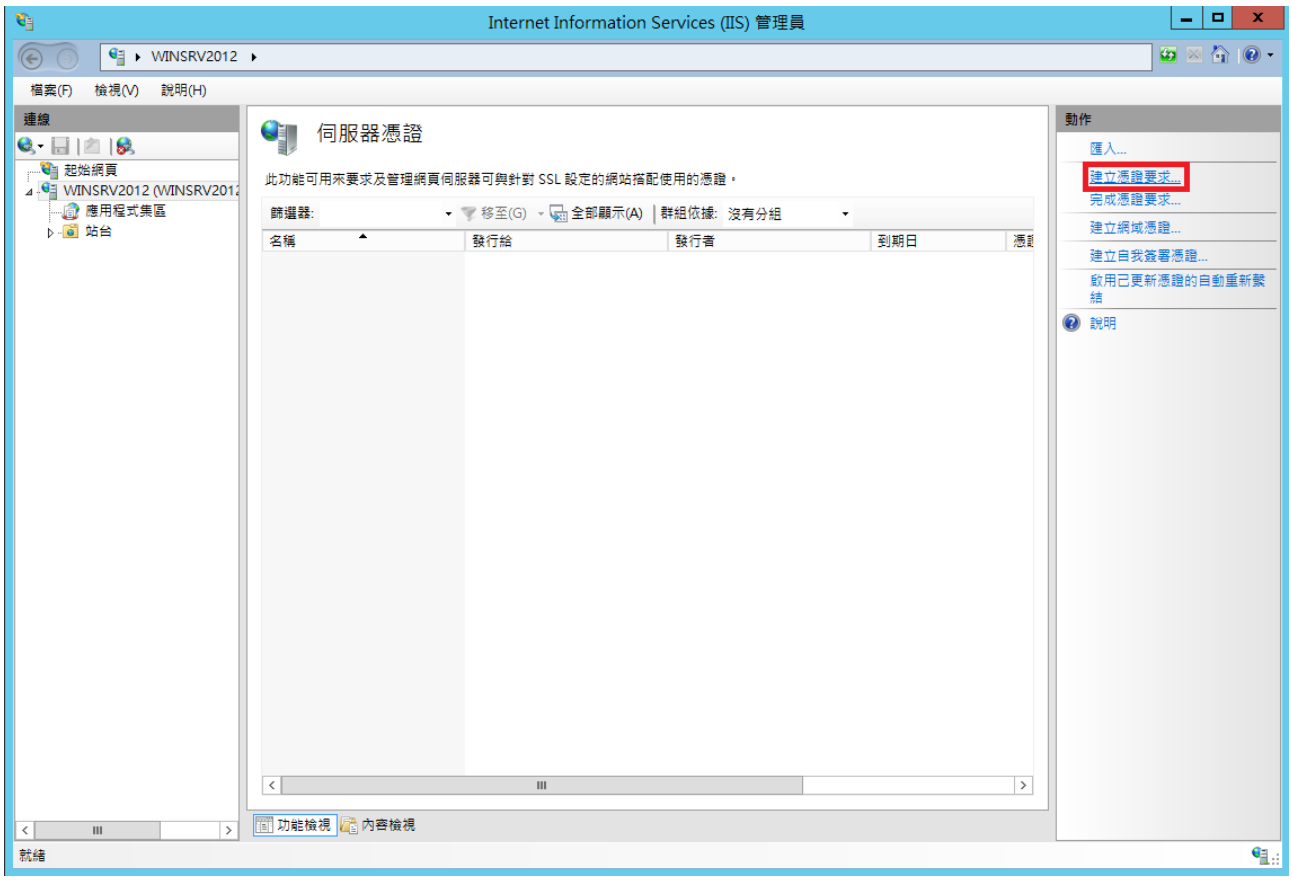
一、至 IIS 首頁中找尋「伺服器憑證」並點擊進入



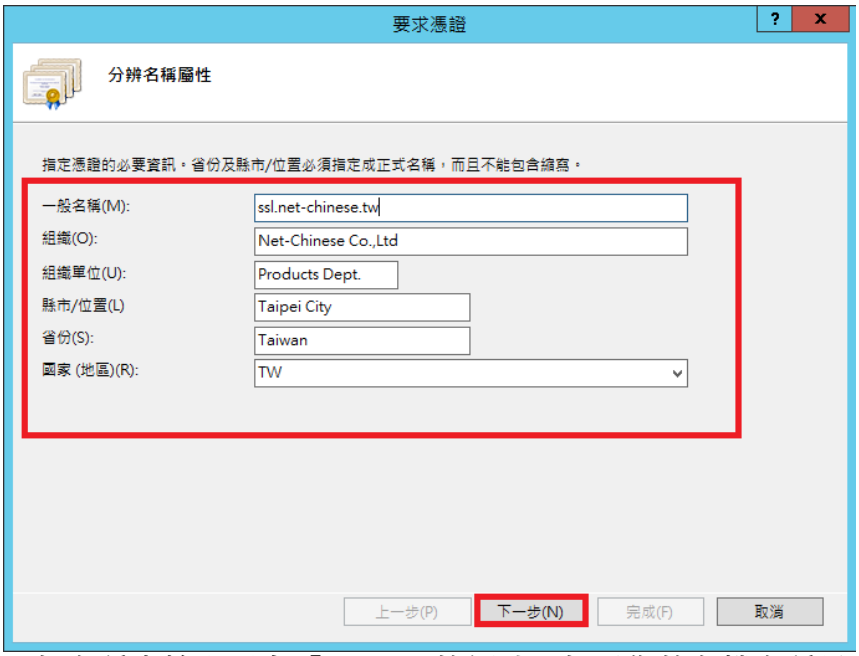
「伺服器憑證」的圖示會位在 IIS 的左側樹狀結構中，寫著您電腦主機名稱的那一個部份。

如果您找不到的 IIS 的話，可以透過 Windows 的搜尋功能中輸入「IIS」 或「Internet Information Services」進行查找。

二、點選右欄動作中的「建立憑證要求」



三、填寫 CSR 資料

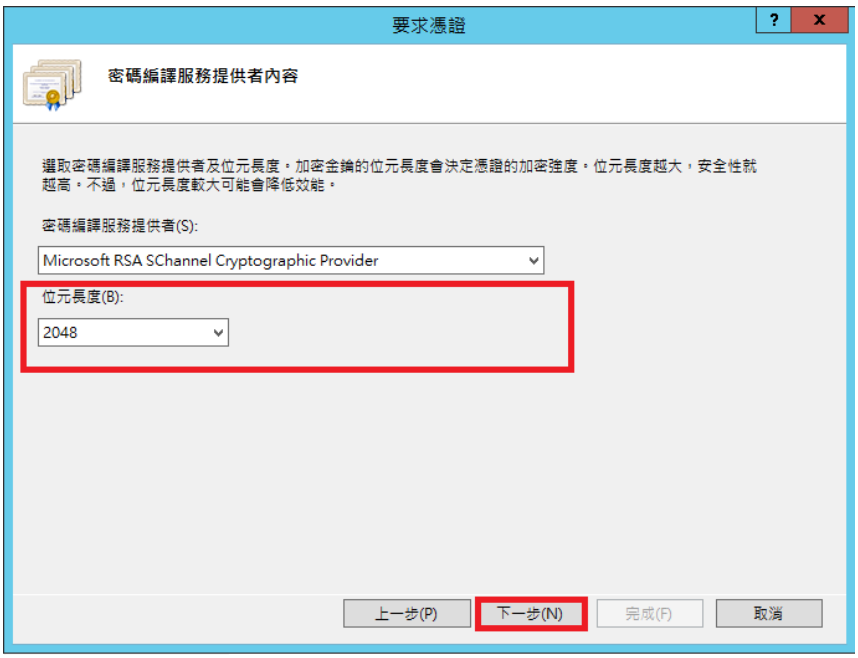


依上圖指示，在一般名稱中輸入不含「http//」的網址，如果您的主機名稱是 www 則請輸入「www. 你的域名 . 域名後綴」，若為其他子域名申請，則請帶入該子域名的主機名稱。如果您申請的是通用型憑證，則請輸入「*. 你的域名 . 域名後綴」。例如：*.net-chinese.tw

另外，組織為必填欄位、縣市建議填您所在縣市即可，省份帶入 Taiwan 即可。

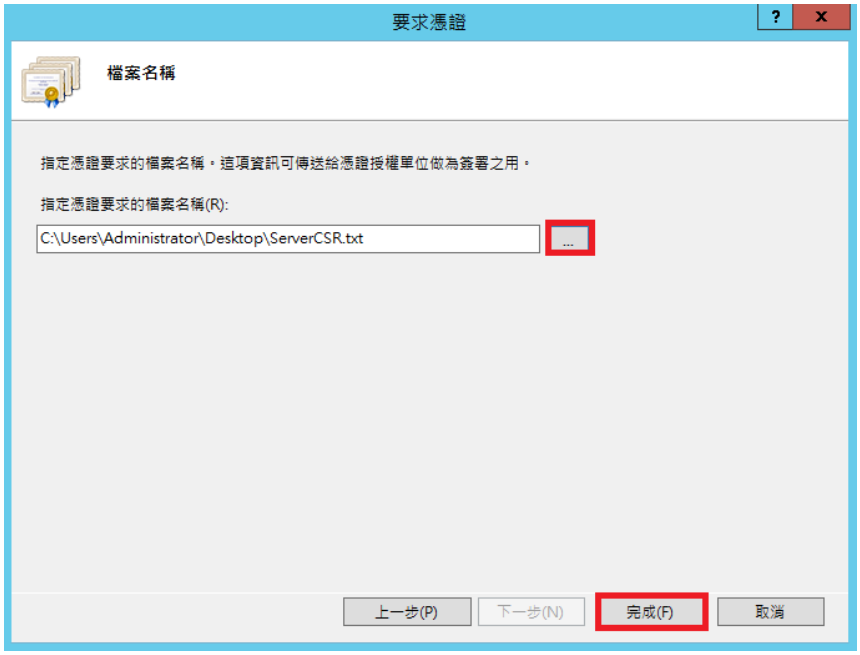
最後，建議您全程以英文填寫，填寫完後請按「下一步」。

四、選擇密碼編譯服務提供者及位元長度



在密碼編譯服務提供者中有兩個選項，預設值為「Microsoft RSA SChannel Cryptographic Provider」，請維持這個選項，不需要更動。位元長度請用下拉式選單選擇「2048」，確認無誤後請點擊「下一步」。

五、請選擇 CSR 的儲存路徑後點擊完成



在這邊會讓您選擇您要將 CSR 檔案給儲存在那裡，您可以點選右邊的「…」按鈕後選擇儲存路徑，選擇好之後按下「完成」。

CSR 檔案在 Windows 中是以 .txt 文本格式進行儲存。

六、到您儲存的路徑找尋 CSR 檔案並開啟它

當您開啟儲存的 CSR 檔案後，您就可以到網路中文網站進行送件了。

Windows 平台生成的 CSR 有一個與其他平台非常不同的點在於「**Windows 的私密金鑰不會匯出供管理員存取**」。

所以您無法在 Windows 的主機中找到與存取您的私密金鑰，從產出、匯入憑證到繫結，您完全都不會接觸到私密金鑰，若您有要將 Windows 憑證移機到其他平台進行佈署的需求，我們將會在後面的說明帶您操作。

章節 2

將憑證匯入IIS網頁伺服器

本章節將帶您操作在您取得憑證後，如何將憑證與中繼憑證匯入到您的 IIS 中。與其他平台很不一樣的地方在於，它有三種方式可以匯入憑證，將在本章之中各別和您說明

在本章節您可以學習三種憑證匯入方法：

A. 使用 IIS 完成憑證請求方式匯入憑證
B. 使用 MMC(主控台) 方式匯入憑證
C. 使用 IIS 的「匯入」方式匯入 .PFX 格式的憑證

三種匯入方式有什麼樣的不同？

- 收到的憑證只有一個 .cer 格式的憑證：選擇 A
- 收到的憑證有數個憑證 (網站憑證、中繼憑證及根憑證)：選擇 B
- 其他 Windows 匯出的憑證，或是原部署於其他作業系統 (如 Linux) 移裝，且有私密金鑰檔的時候：選擇 C。

會有這樣的分別，主要是因為，在 Linux 系統中，通常會使用 Open SSL 利用演算機制去產生私密金鑰，再由私密金鑰去產生一組與之配對的公鑰，即 CSR，而使用者再利用這個 CSR 送交給憑證發行機構進行簽署，簽署完成後再將簽署過的公鑰交給您。這就是您拿到的終端憑證。

這就像是，CSR 其實只是一張上面寫了您網域、公司的空白執照，但是這空白的執照並沒有獲得第三方認可，因此不具效力，而送交第三方公證機構簽署或是蓋印章的執照，才具有公信力。

而 Windows Internet Information 的機制下生成 CSR，會將其金鑰留在生成的主機裡面，並不會匯出給使用者，也許是基於資訊安全考量。(就算是開放系統，您也不應該隨意將私密金鑰交給第三方)。

在一些特殊的情況之下 (例如您同時有 Windows 系統的網頁主機及 Linux 的網頁主機)，會需要做多重部署的情況。這時您需要將運行在 Linux 或開放式傳統的憑證同時一併部署於 Windows(通常是通用型憑證或是多域名型憑證)，就會需要將憑證、信任鏈 (中繼憑證 / 根憑證) 與終端憑證轉換成 PKCS#12 文件格式以對其中的憑證、私密金鑰以再加密的方式包覆起來 - PFX 格式即為 PKCS#12 的文件格式。

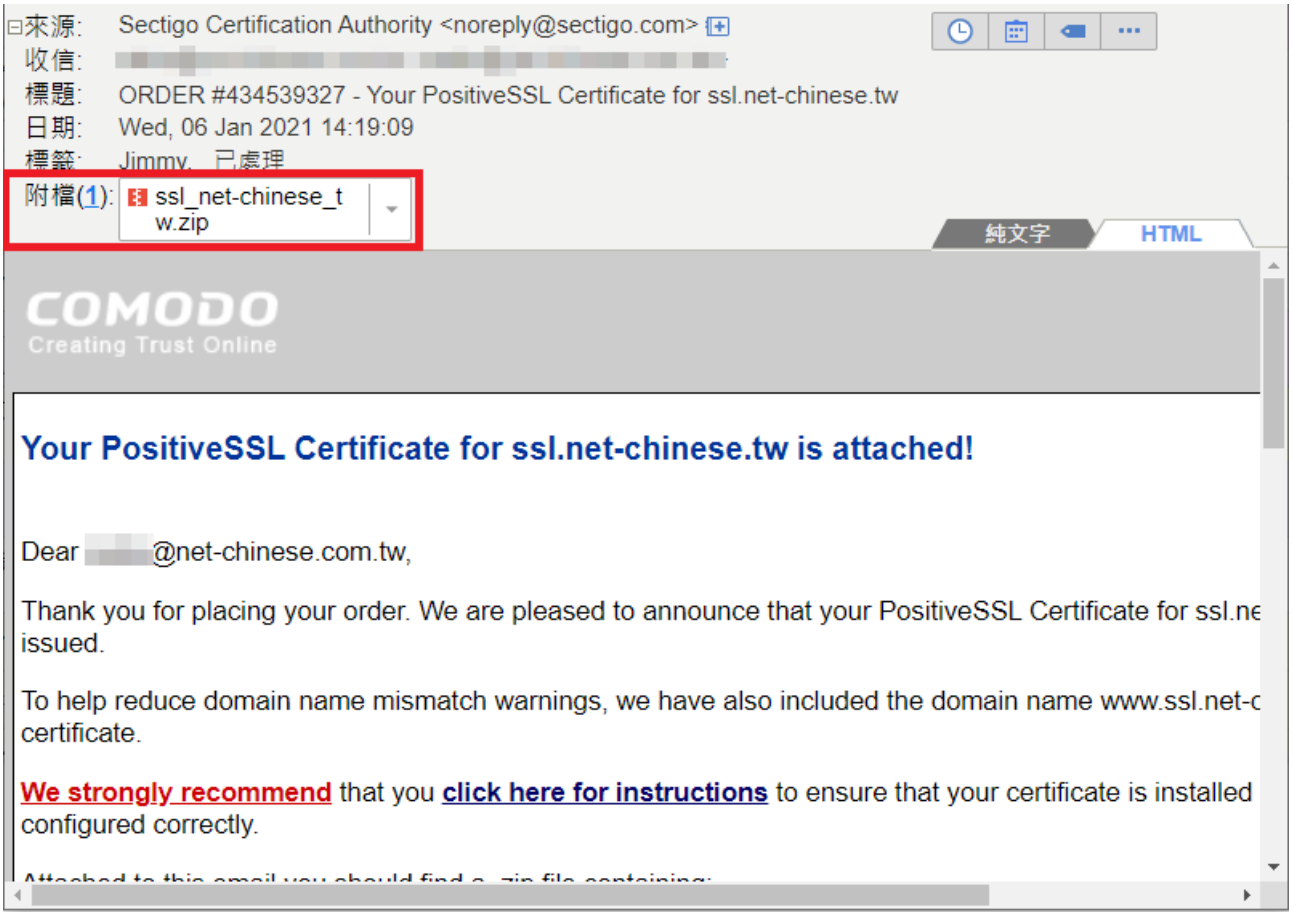
在這樣的方式之下，您就必須以 .PFX 格式將原先部署於開放式系統主機上的憑證匯入 Windows。

A、 使用 IIS 完成憑證請求方式匯入憑證

使用對象：

1. 以 Windows Internet Information Services 依照第一章的方式產生 CSR 的使用者。
2. 在遞交資料時的伺服器選擇 Internet Information Services 或 IIS 5.0 及 later 版本的使用者。
3. 收到的憑證是上游廠商以 .cer 給您的憑證。

一、查看您申請憑證時填入的管理人信箱是否收到發證機構來信



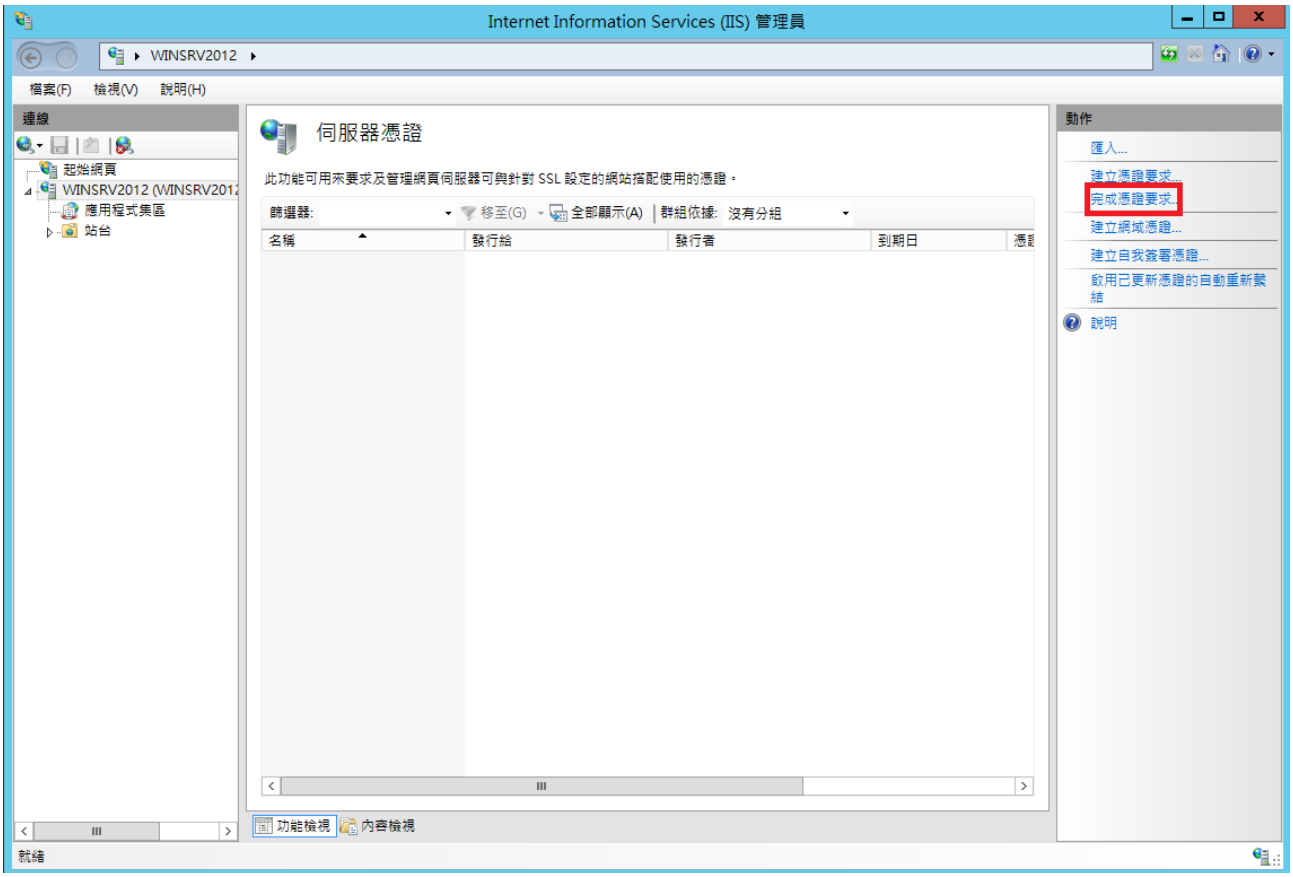
有些發證機構會將憑證以 ZIP 壓縮檔的方式附件給申請人 (Sectigo/Comodo)

通常在您完成發證機構所要求的驗證程序後 (域名驗證 / 組織驗證)，您會在申請憑證時填寫的管理人信箱收到信件，寄信的內容會依照各家發證機構不同而有不同方式的形式表現，但大致上可以分為兩種類型：

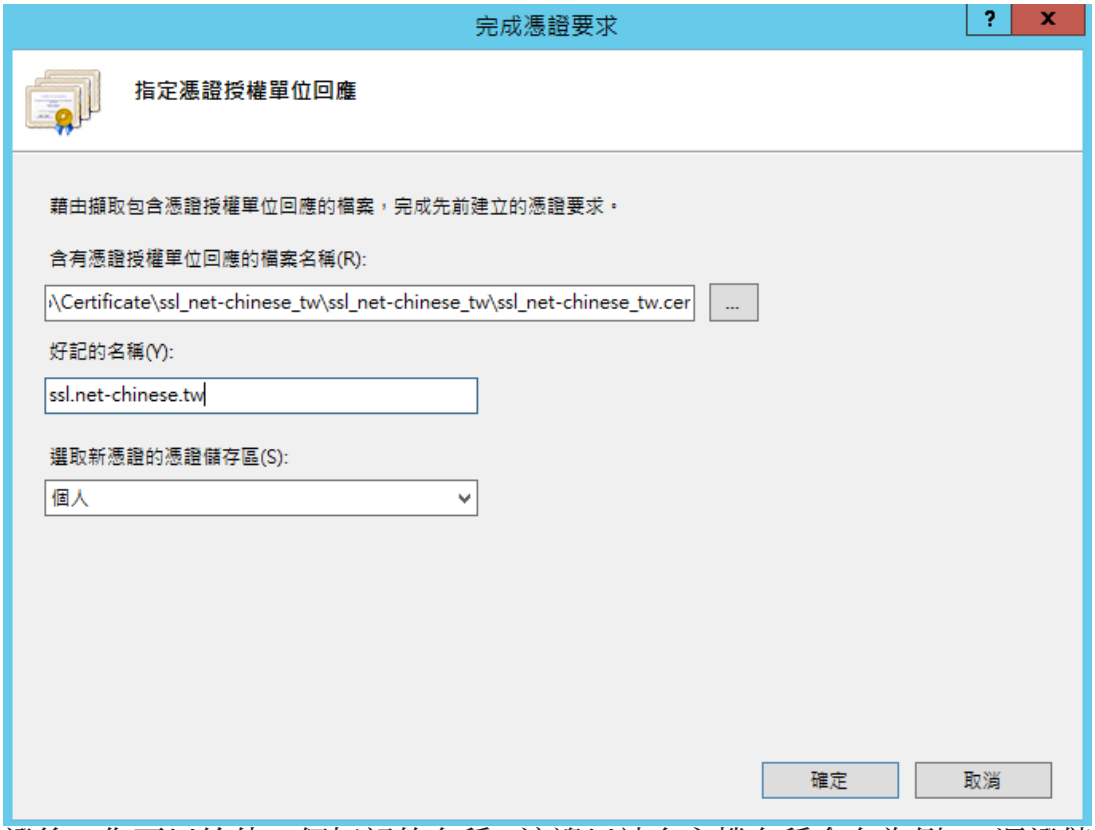
1. 以附件檔夾帶憑證檔案，以壓縮格式寄送 (如 .zip 檔)
2. 以文本格式記出，以文字方式表示。

以附件檔夾帶的憑證檔，有時會有較為簡化的方式做附件，如您選擇的伺服器是 Apache 就會給你一個 Bundle 檔 (根憑證與中繼憑證信任鏈) 和一個網站憑證檔，如果是 IIS 可能就會給你一個 .cer 格式的檔案，如果是 Other 類型可能就會給你完整的根憑證、中繼憑證及網站憑證檔案。(如下圖)

二、回到「伺服器憑證」中點選「完成憑證請求」



三、設定名稱與儲存區



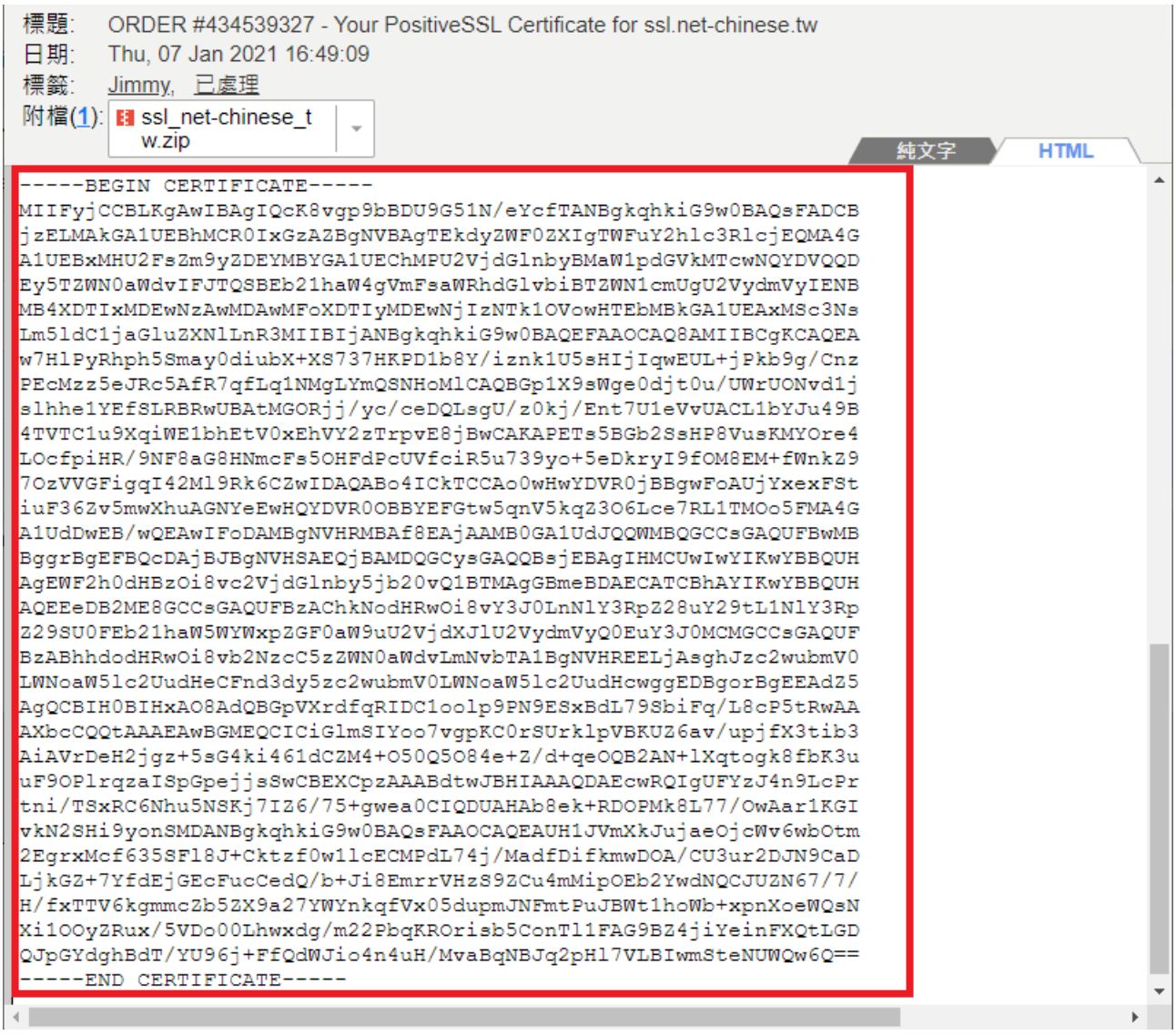
選好憑證後，您可以給他一個好記的名稱 (這邊以站台主機名稱命名為例)，憑證儲存區若您是以 Administrator 身份的話可以選個人，或是以本機為主的 Web Hosting，比較不易受執行身份影響，設定無誤後按請「確定」。

B、 以 MMC(主控台) 的方式匯入憑證

使用對象：

1. 以 Windows Internet Information Services 依照第一章的方式產生 CSR 的使用者。
2. 在遞交資料時的伺服器選擇非 Internet Information Services 或 IIS 5.0 及 later 版本的使用者。
3. 收到的憑證是上游廠商以文本格式或是 .crt 格式給您的憑證。

一、查看您申請憑證時填入的管理人信箱是否收到發證機構來信

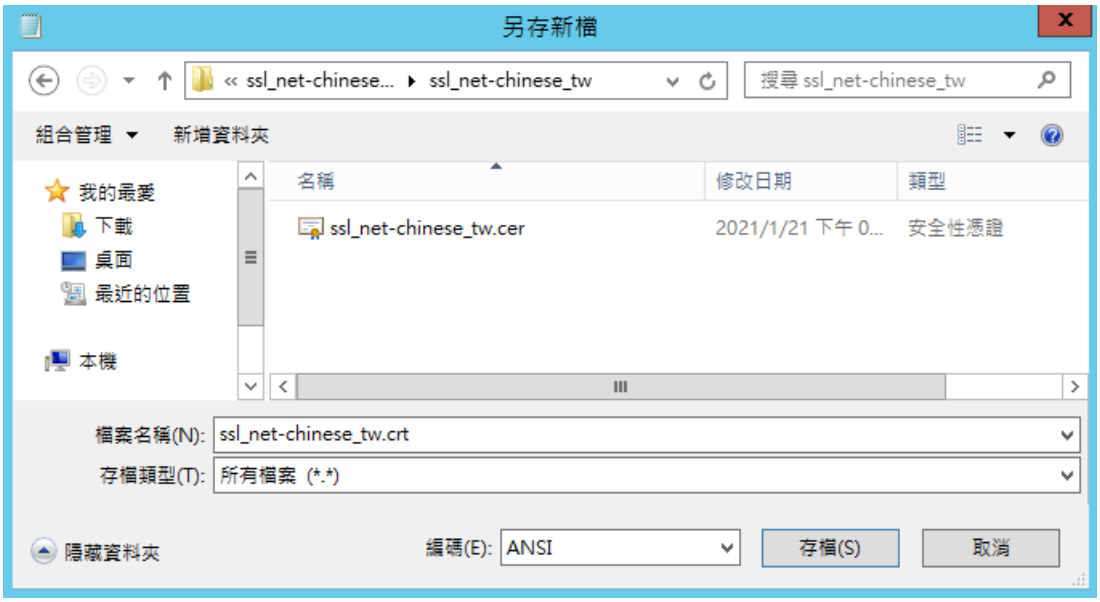


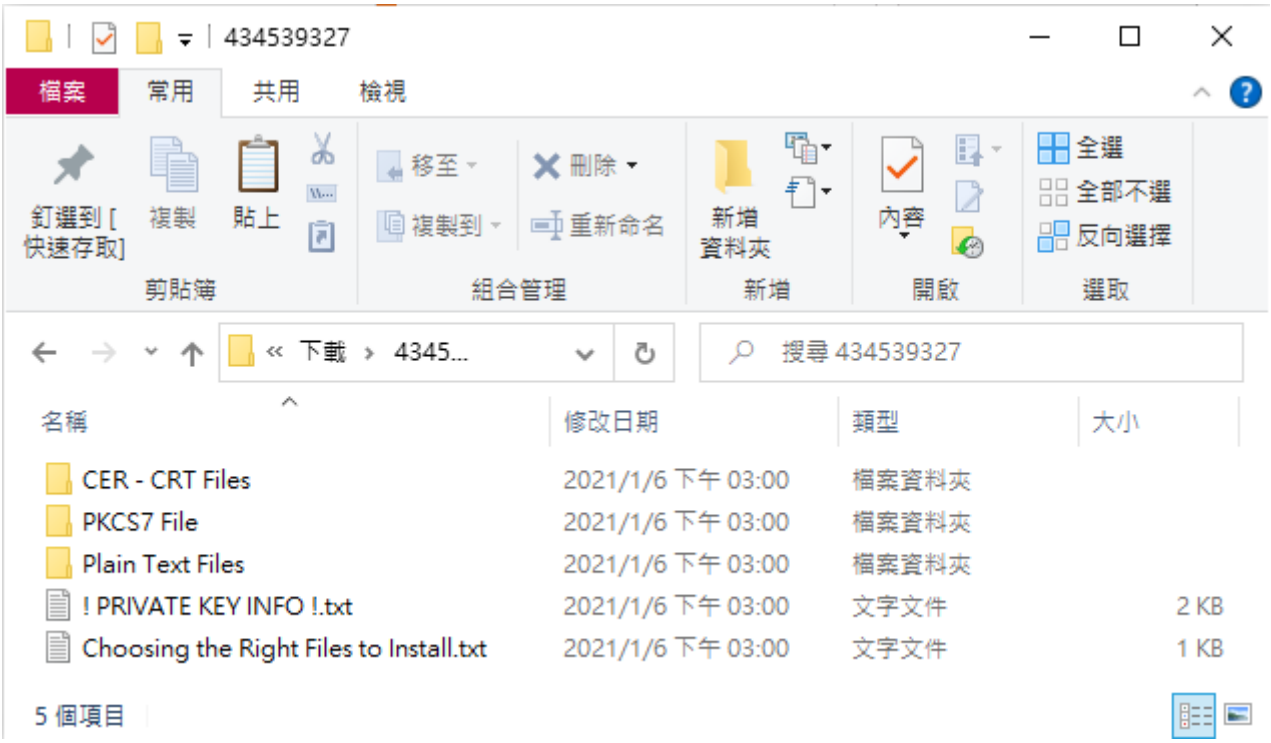
以文字格式的方式做為憑證檔案寄送給申請人

在大多數的情況之下，發證機構將會以文字格式做為終端憑證寄送給客戶。而並不會包含中繼憑證 (Intermediate) 及根憑證 (Root)。而中繼憑證與根憑證將會以公開方式放在發證機構供有需要的使用者下載。

如果您有需要，您可自行至發證機構網站下載。

如果今天收到的憑證是以文字格式的話，我們可以利用記事本軟體，將憑證給複製 (需要包含 -----BEGIN CERTIFICATE----- 及 -----END CERTIFICATE----- 貼入空白的記事本。然後選擇「另存新檔」存檔案時一樣要選擇「所有檔案 (*.*)」，然後檔名您可以自訂，並在檔名最後加上副檔名 (.crt)，編碼的話選擇 ASCII 或是 UTF-8 都可以。





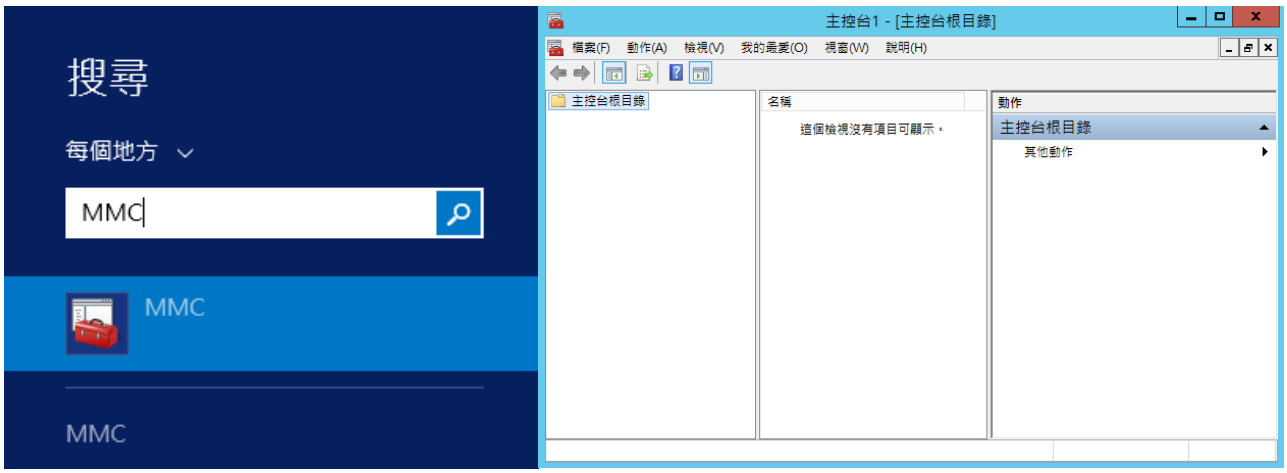
如果您是在網路中文下載的憑證，或是由網中客服寄發給您的憑證，解壓縮之後，您也許會看到的內容如上，以下將針對各資料夾與內容物進行說明。

- CER - CRT Files - 以副檔名為 .CRT 格式的憑證檔案，內含網站憑證、根憑證、中繼憑證。
  Sectigo(COMODO) 品牌
  - xxx_xxx_xx.crt 是網站憑證，其中 xx 會是您的域名。
  - AAA Certificate Service.crt (AddTrust) 為 Sectigo 品牌的根憑證。
  - USERTrustRSAAddTrust.crt 為 Sectigo 品牌的互簽憑證。
  - SectigoRSA(Domain/Organization/Extended)ValidationSecureServerCA.crt 為 Sectigo 品牌的中繼憑證。
  - My_CA_Bundle.ca-bundle 為根憑證、互簽憑證及中繼憑證的三合一信任鏈憑證。

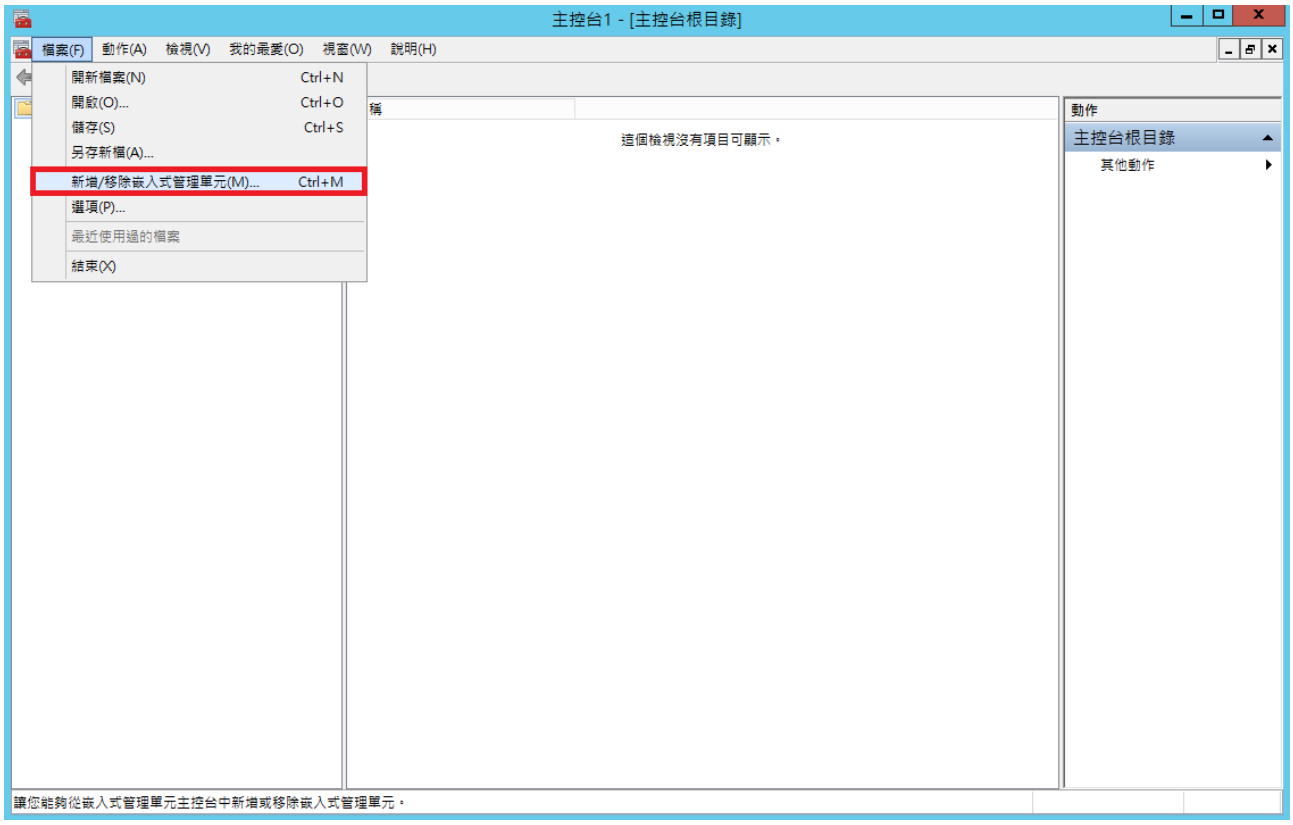
  非 Sectigo 品牌
  未必會有附上中繼憑證及根憑證，但我們可以從關鍵字中查詢。
  - 有 Root 字樣 - 根憑證。
  - 有 Intermediate 字樣 - 中繼憑證。
- PKCS7 File - 加密訊息語法標準檔，用來使用對訊息簽章或加解密，Microsoft Windows 系統、AZURE 雲端服務及 JAVA Tomcat 有機會用到，該檔案只會包含憑證與中繼憑證。
- Plain Text Files - 為 CER - CRT Files 中憑證的純文字文件，您可以利用另存新檔方式儲存成 .crt 格式。
- !PRIVATE KEY INFO !.txt - 憑證檔不含私密金鑰指南及宣告。
- Choosing the Right Files to Install.txt - 用來告知您各資料夾的內容物檔案。

請注意，其內容物會因為您所選擇的品牌、驗證方式而有不同。

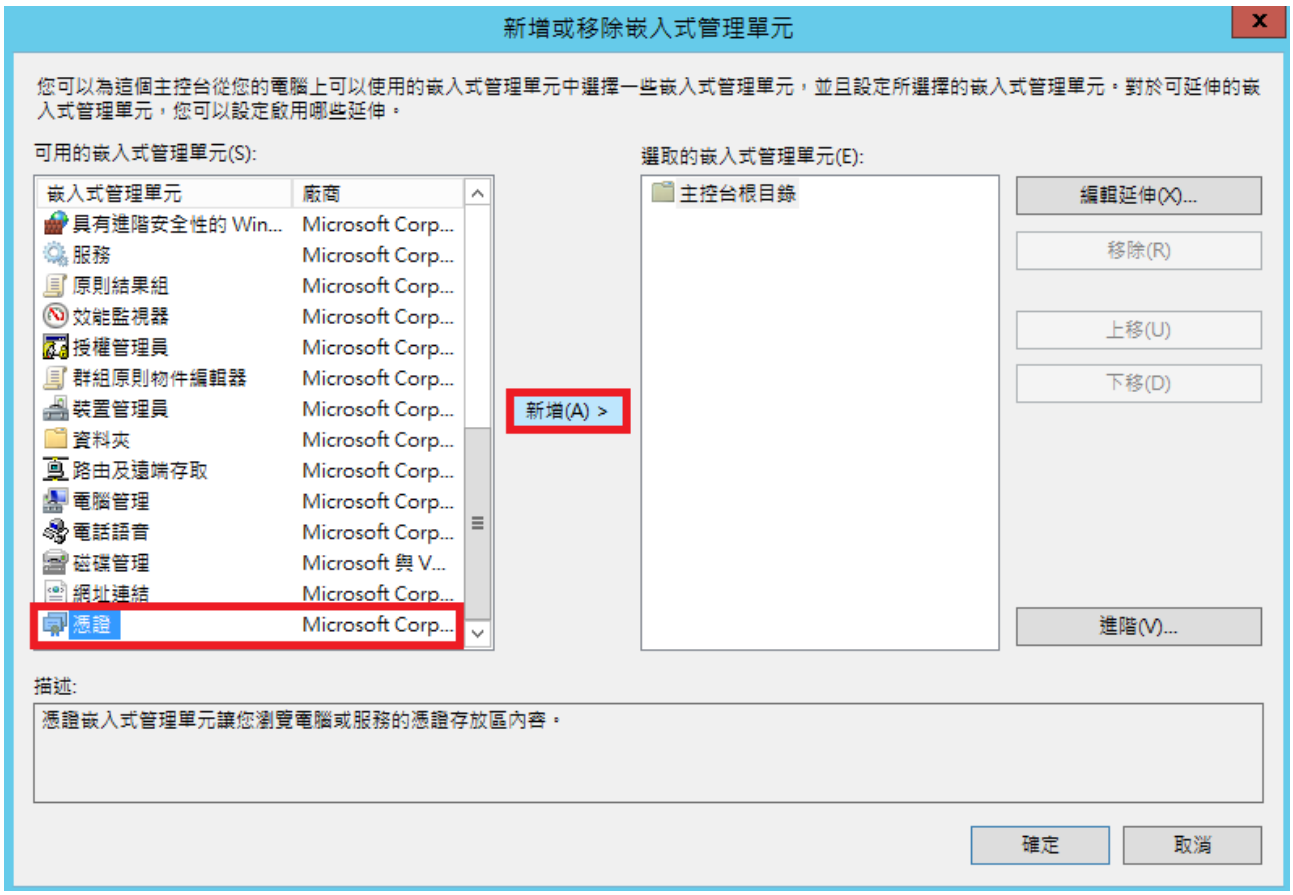
二、在搜尋輸入「MMC」開啟主控台



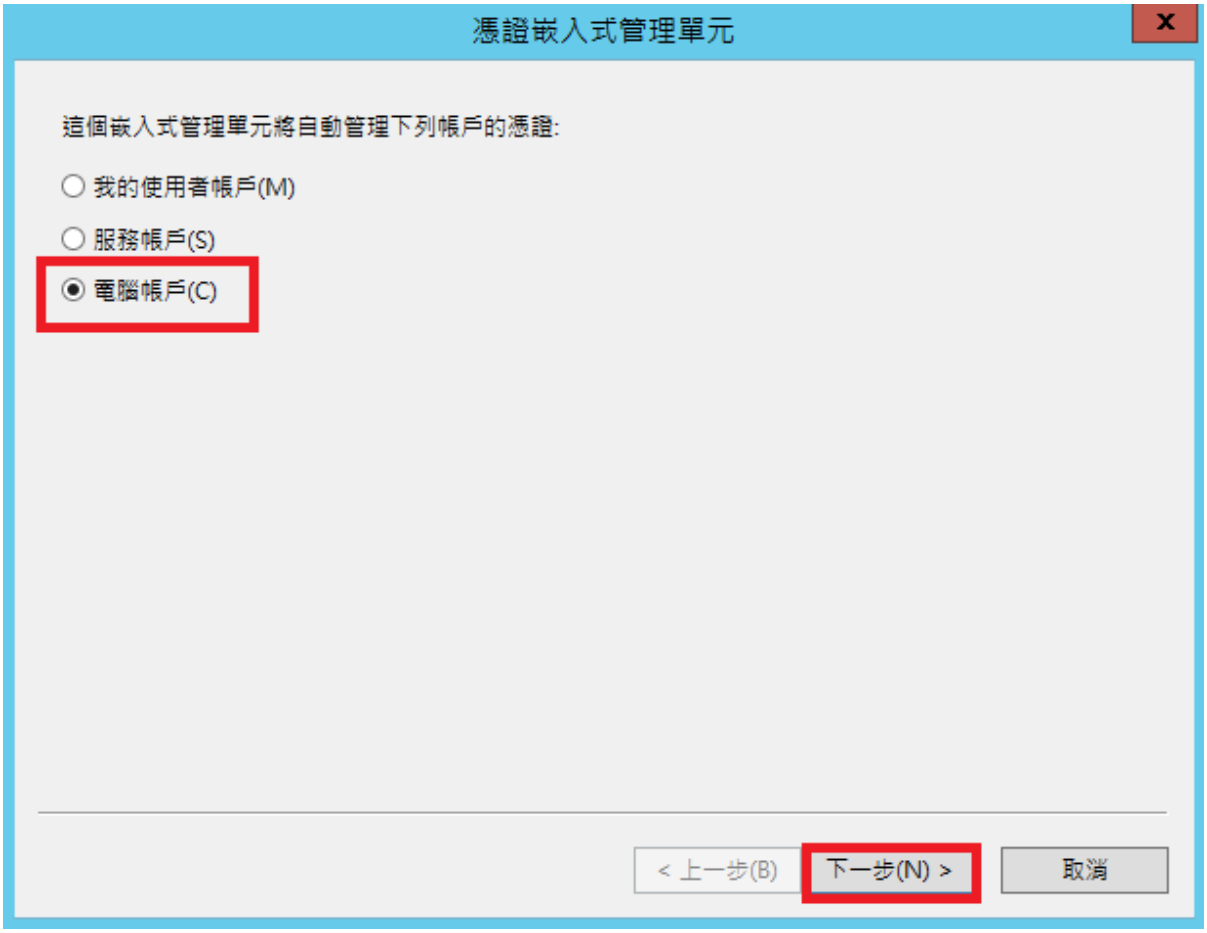
三、在 MMC 點選「檔案」下面的「新增 / 移除嵌入式管理單元」



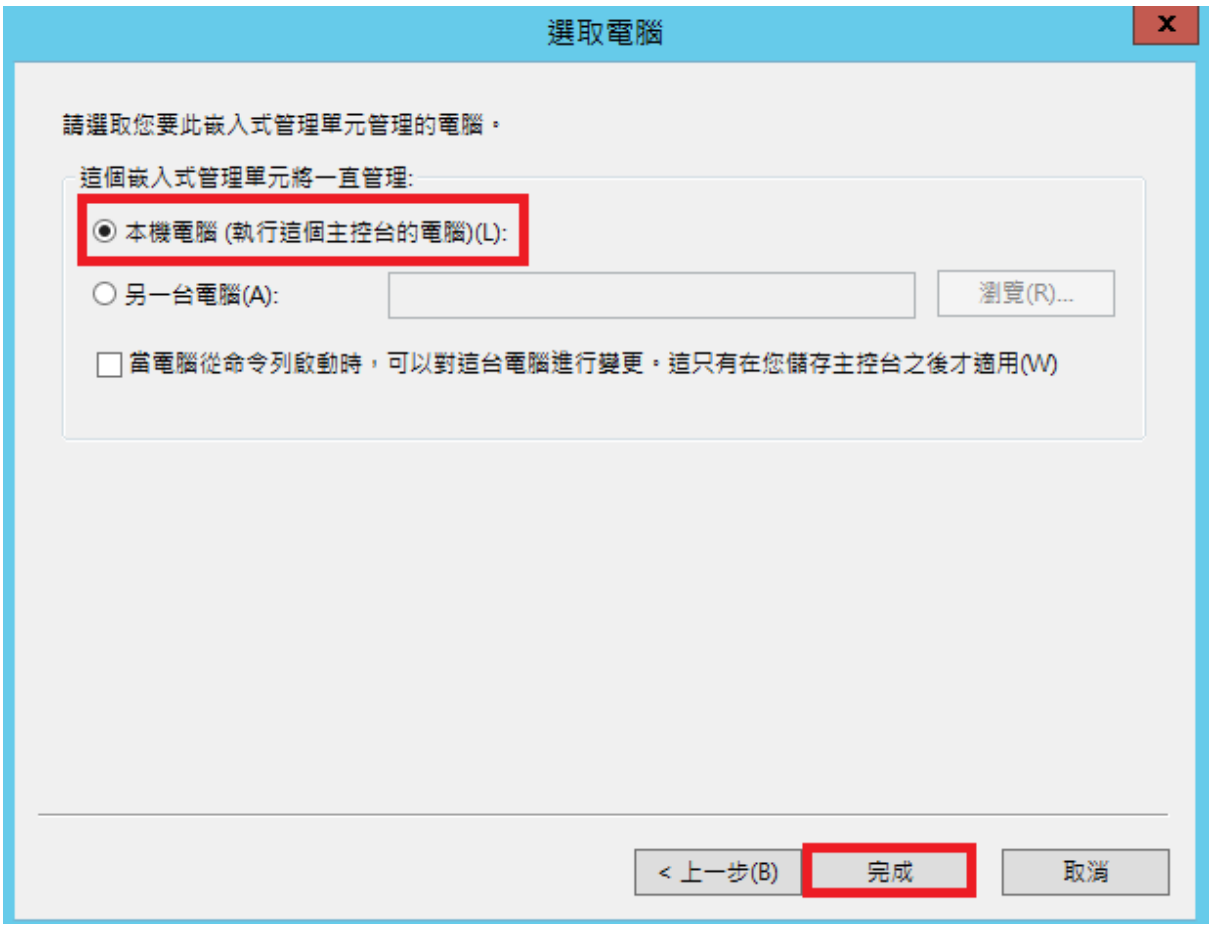
四、在「新增 / 移除嵌入式管理單元」中選擇「憑證」後按「新增」



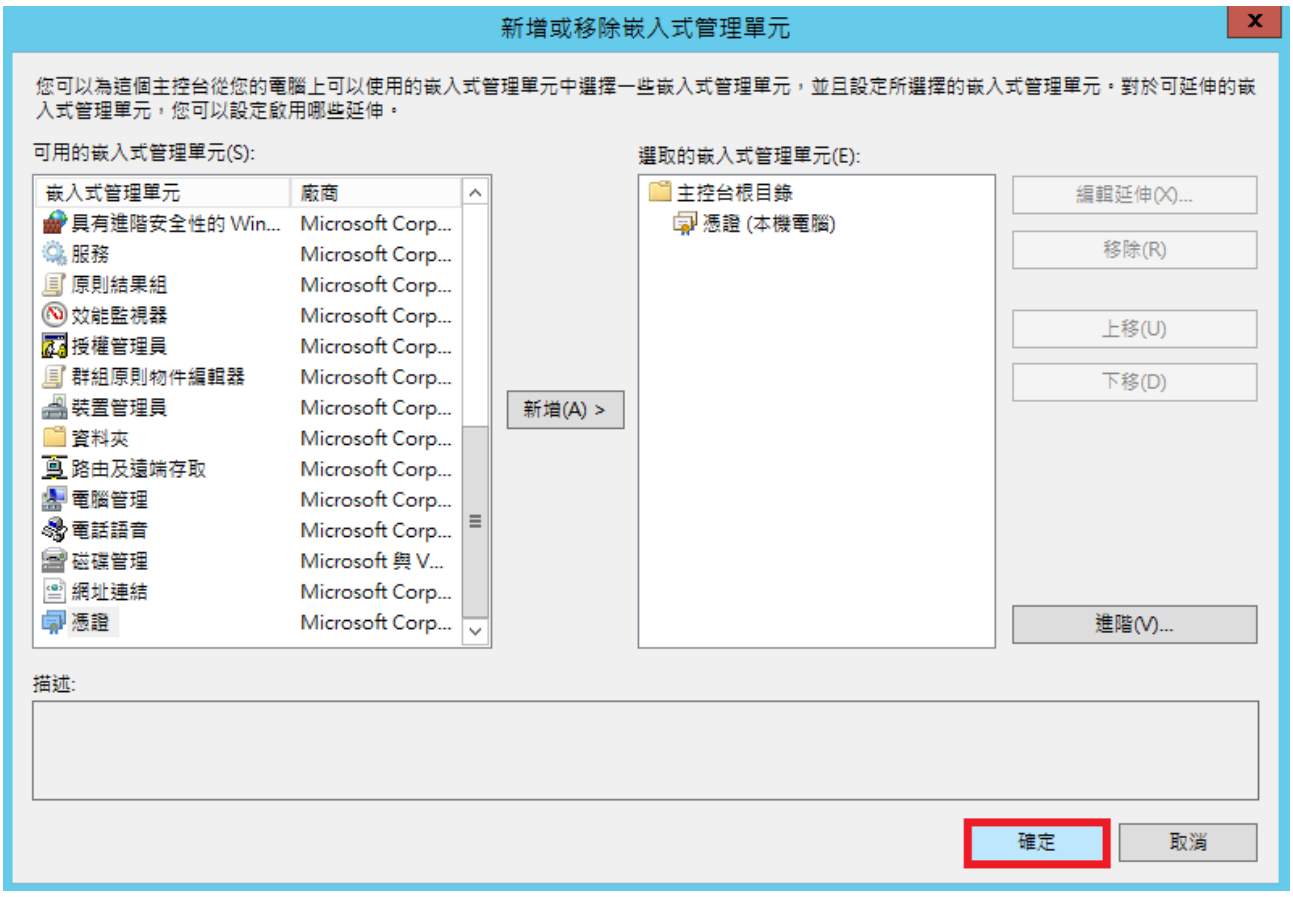
五、在嵌入式管理單元選擇管理「電腦帳戶」的憑證。



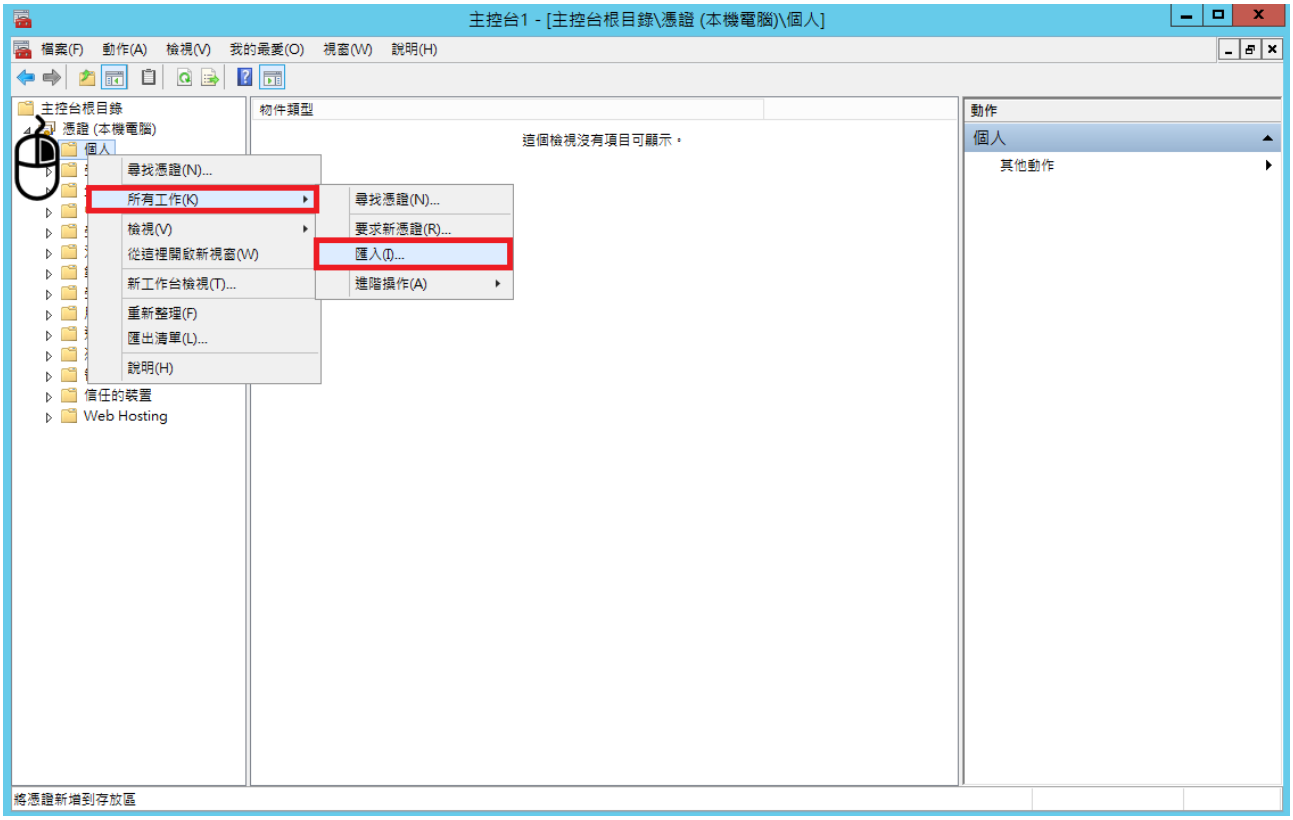
六、 在嵌入式管理單元管理的電腦中選擇「本機電腦」後按「完成」



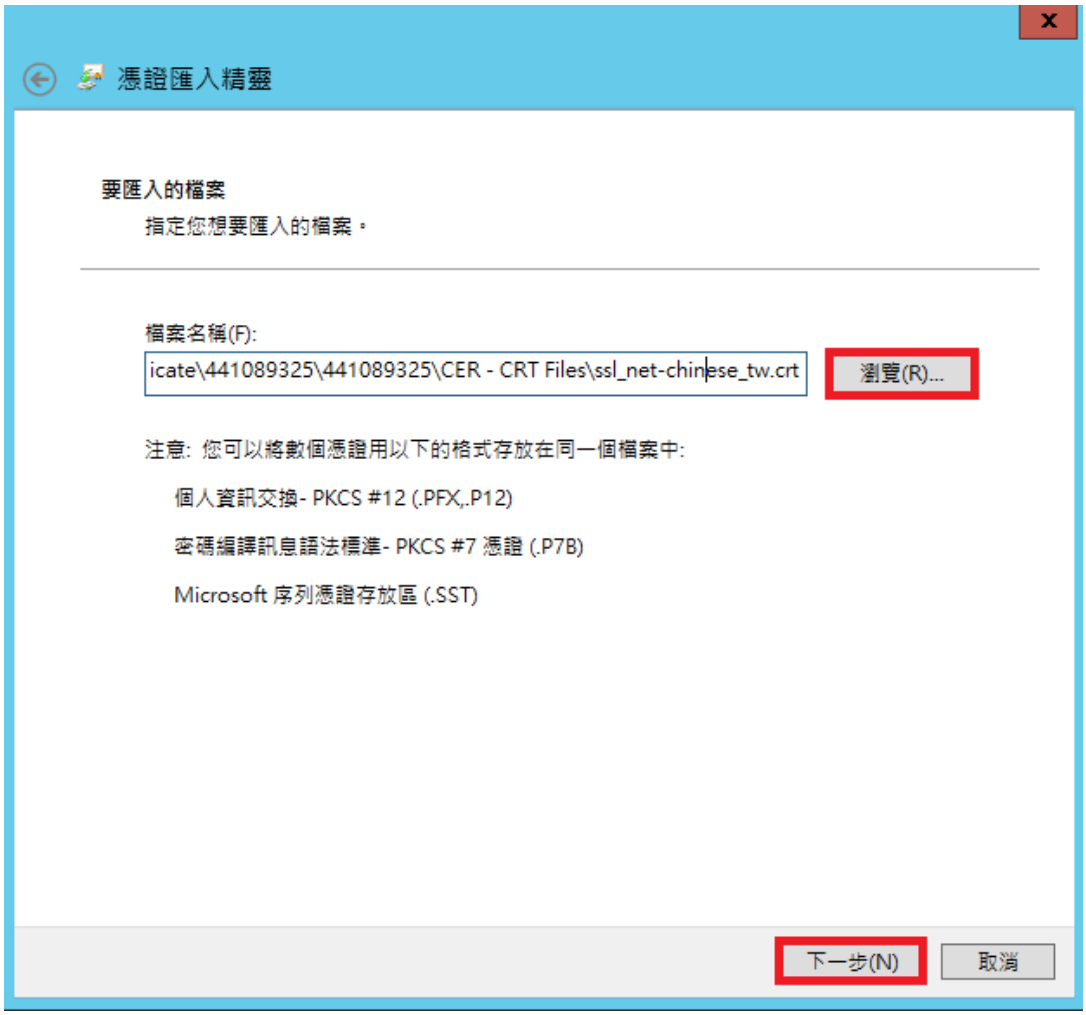
七、確認選取的嵌入式管理單元無誤後點擊「確定」



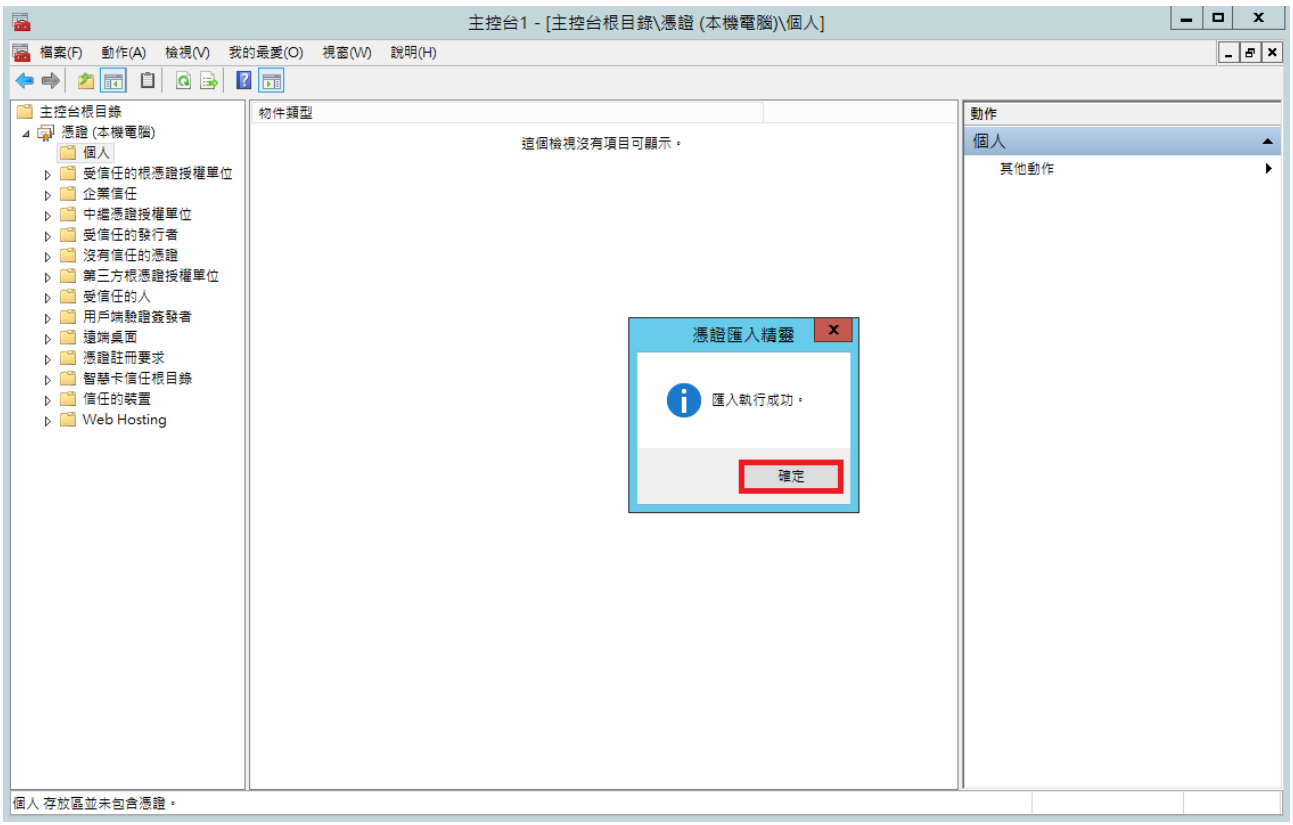
八、 在憑證樹的「個人」資料夾中按滑鼠右鍵選「所有工作」 匯入



九、 按「瀏覽」選擇網站憑證的來源路徑後按「下一步」



一〇、 點擊憑證匯入精靈的對話框「確認」按鈕



在匯入憑證後，您必須按右鍵將之重新整理，已匯入的憑證就會在裡面。
但請注意，用 MMC 主控台方式匯入的終端憑證，此時是不可以用在網站繫結的，您在 IIS 會看不到這張憑證。您必須將金鑰進行指派給憑證 (憑證旁邊會有金鑰圖示)

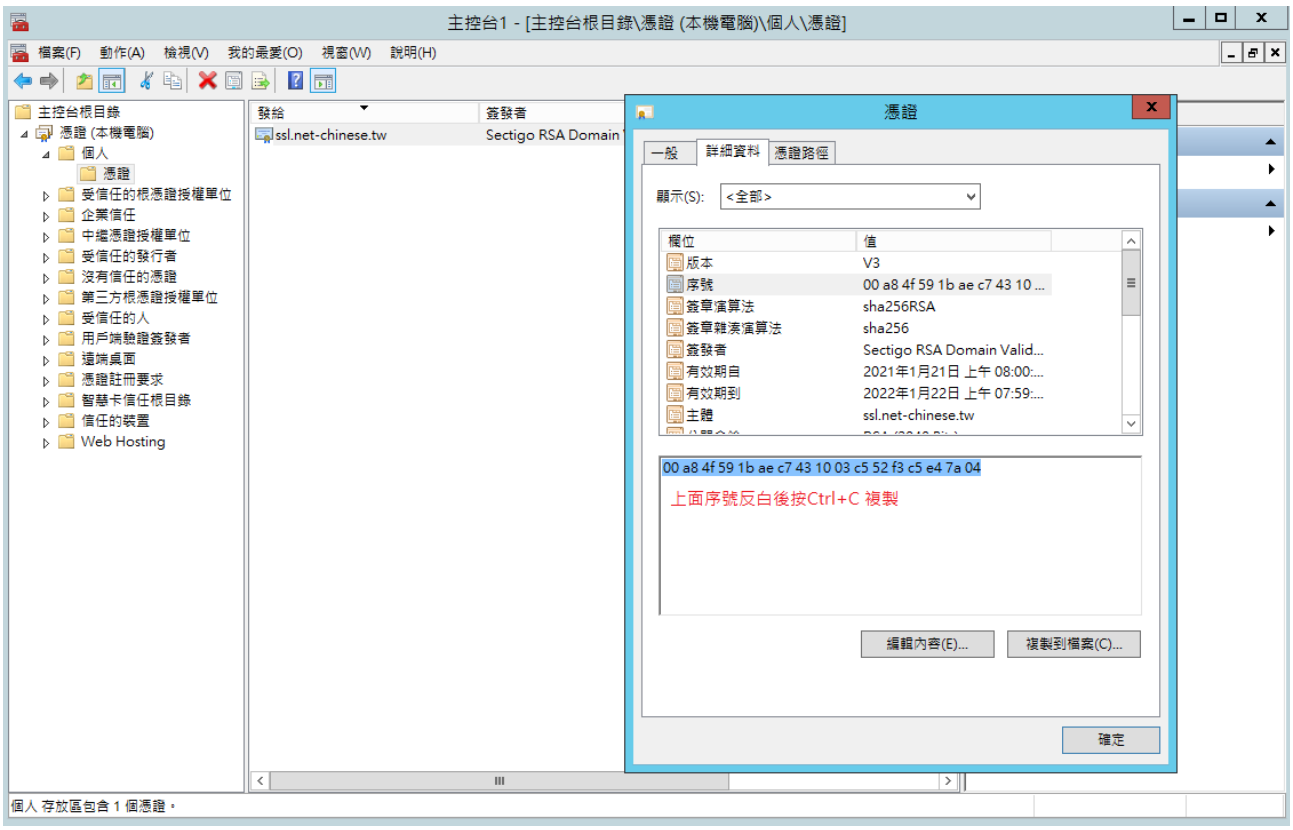
發給	簽發者	到期日	使用目的
ssl.net-chinese.tw	Sectigo RSA Domain Validation...	2022/1/22	伺服器驗證, 用戶端...

未將金鑰與憑證進行關聯時的狀態

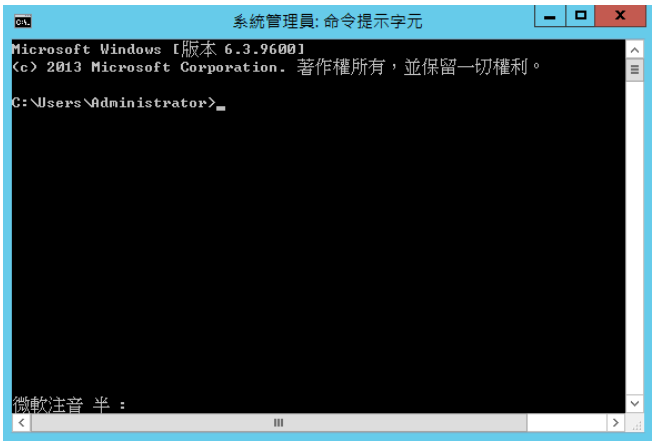
發給	簽發者	到期日	使用目的
ssl.net-chinese.tw	Sectigo RSA Domain Validation...	2022/1/22	伺服器驗證, 用戶端...

已將金鑰指派給憑證時的狀態

一一、 雙擊已匯入的憑證並切換至詳細資料頁籤查看序號並復製



一二、 在搜尋輸入「CMD」或「命令提示字元」開啟主控台

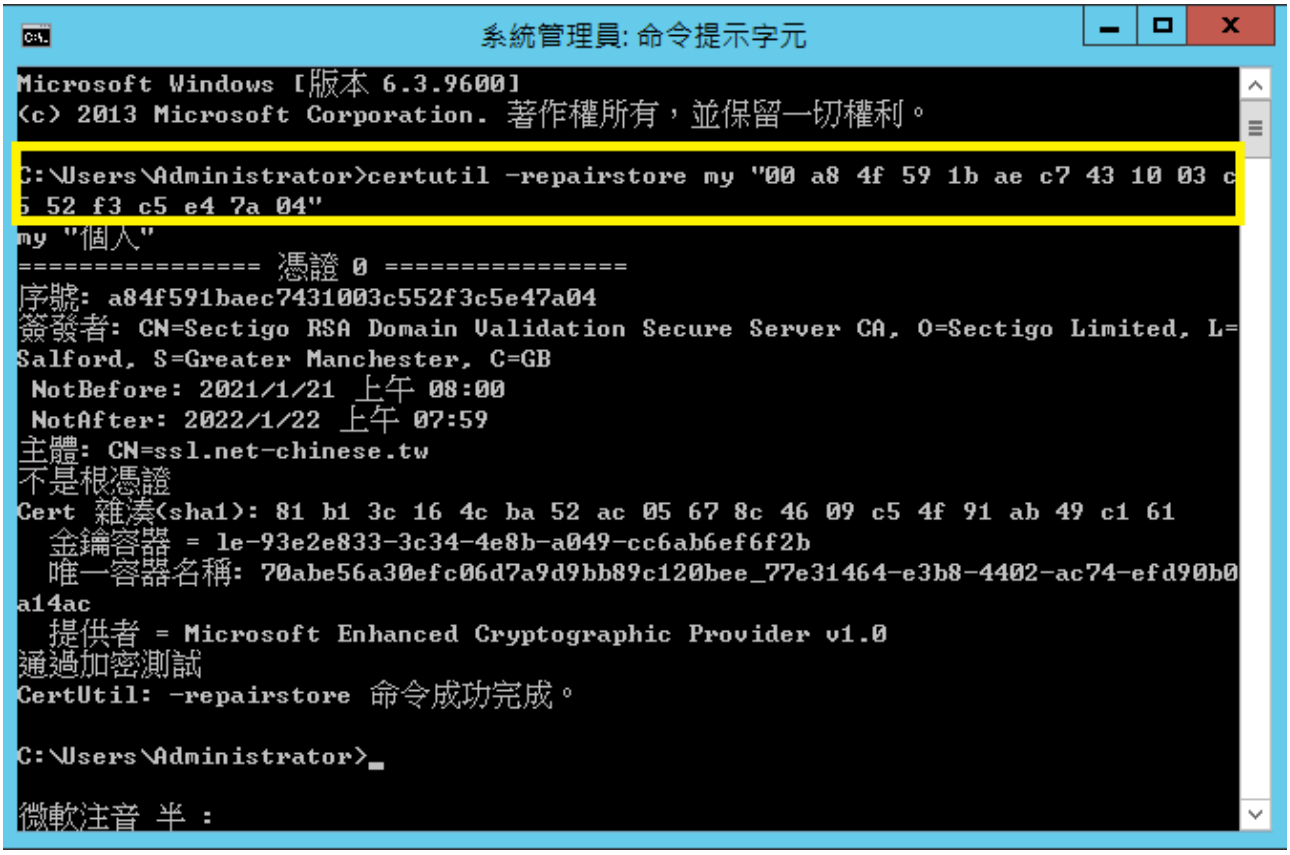


一三、 輸入以下指令讓憑證與私密金鑰相關聯

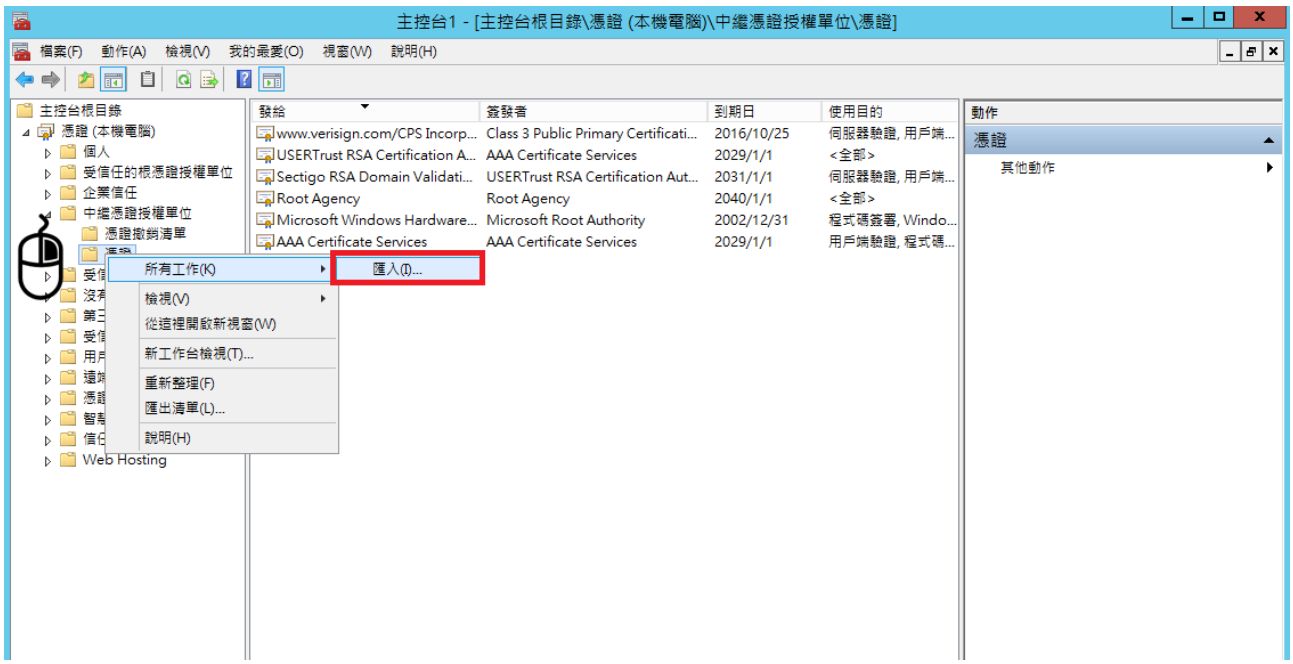
主控台
certutil -repairstore my "SerialNumber"

SerialNumber 是您在步驟 11 查看的憑證序號

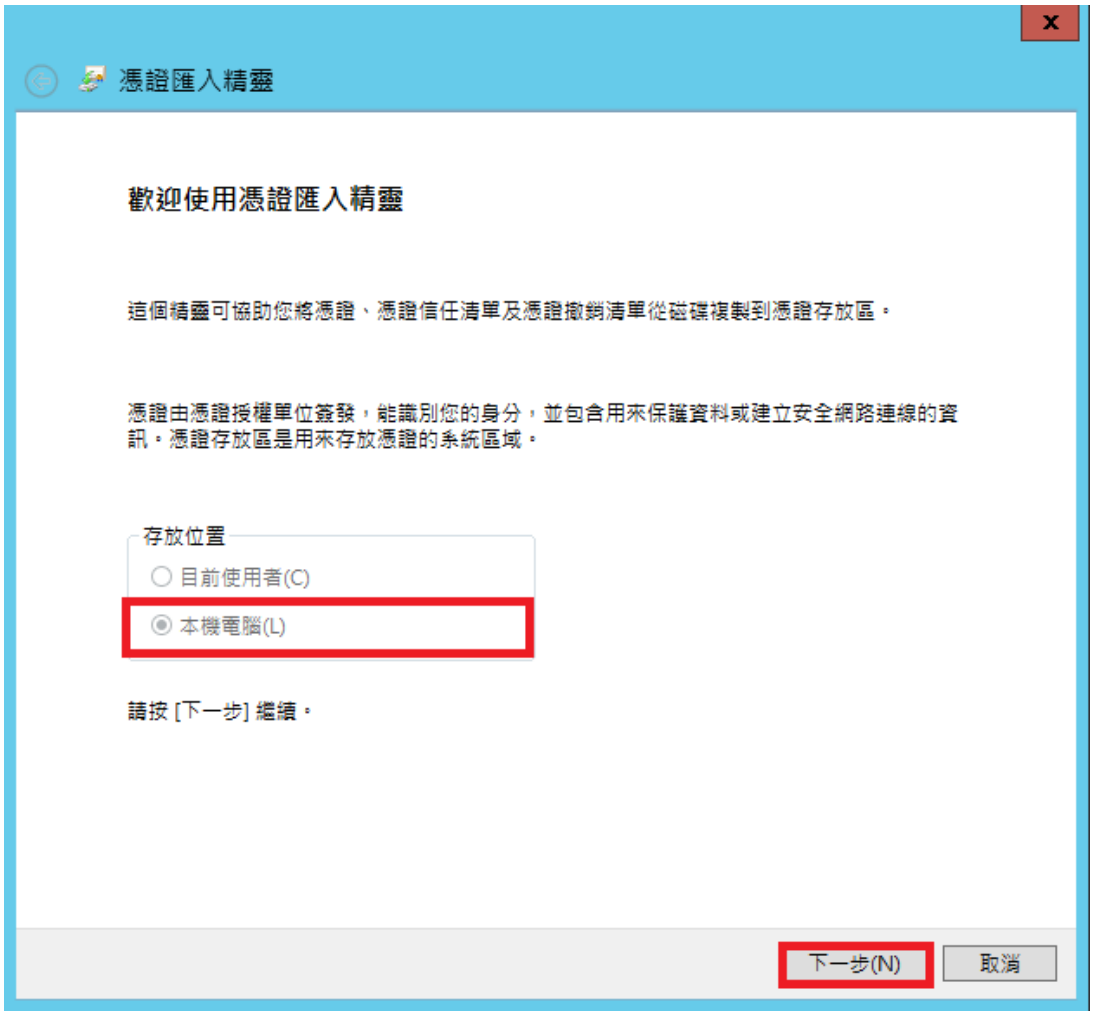
指令實際執行結果



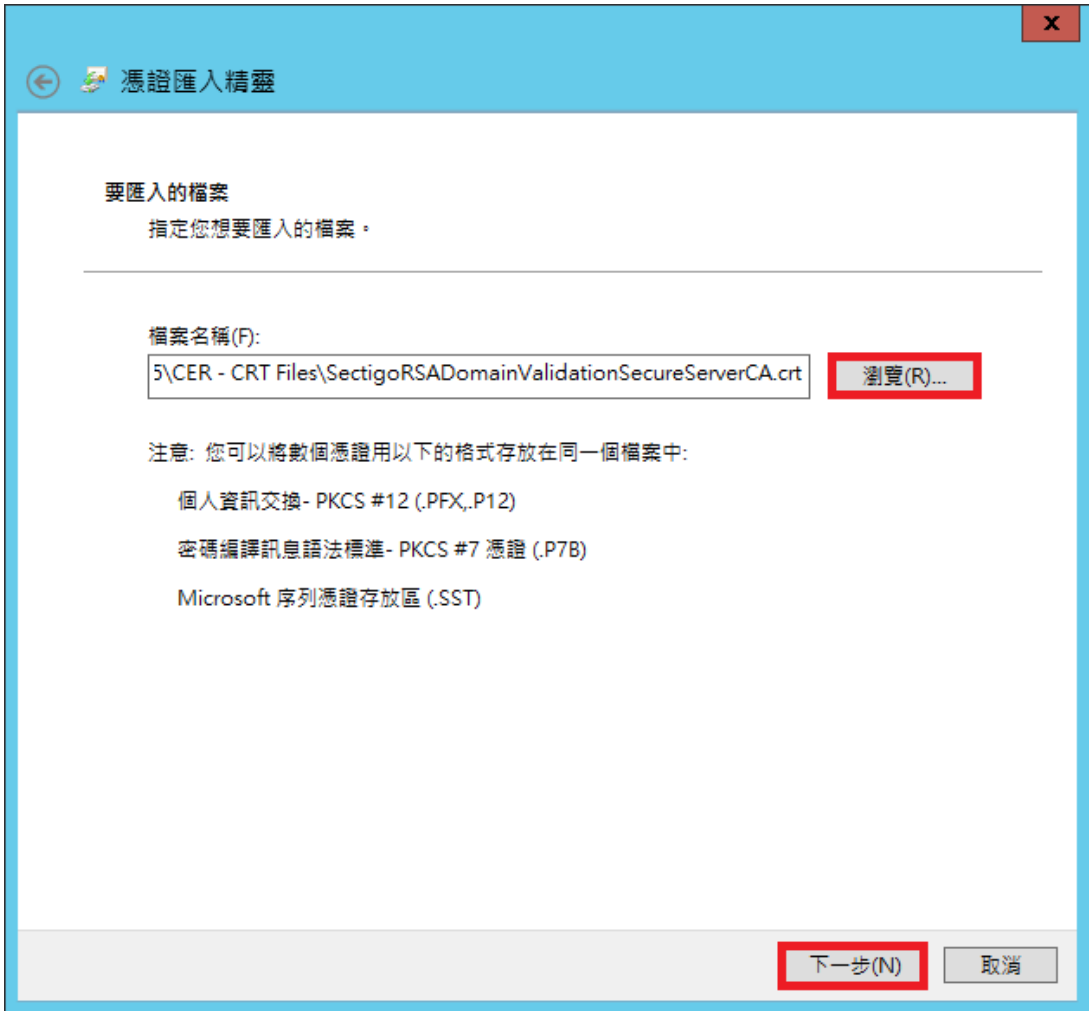
一四、 匯入中繼憑證 - 在中繼憑證授權單位 \ 憑證下按右鍵匯入



一五、 選擇中繼憑證存放位置為本機電腦

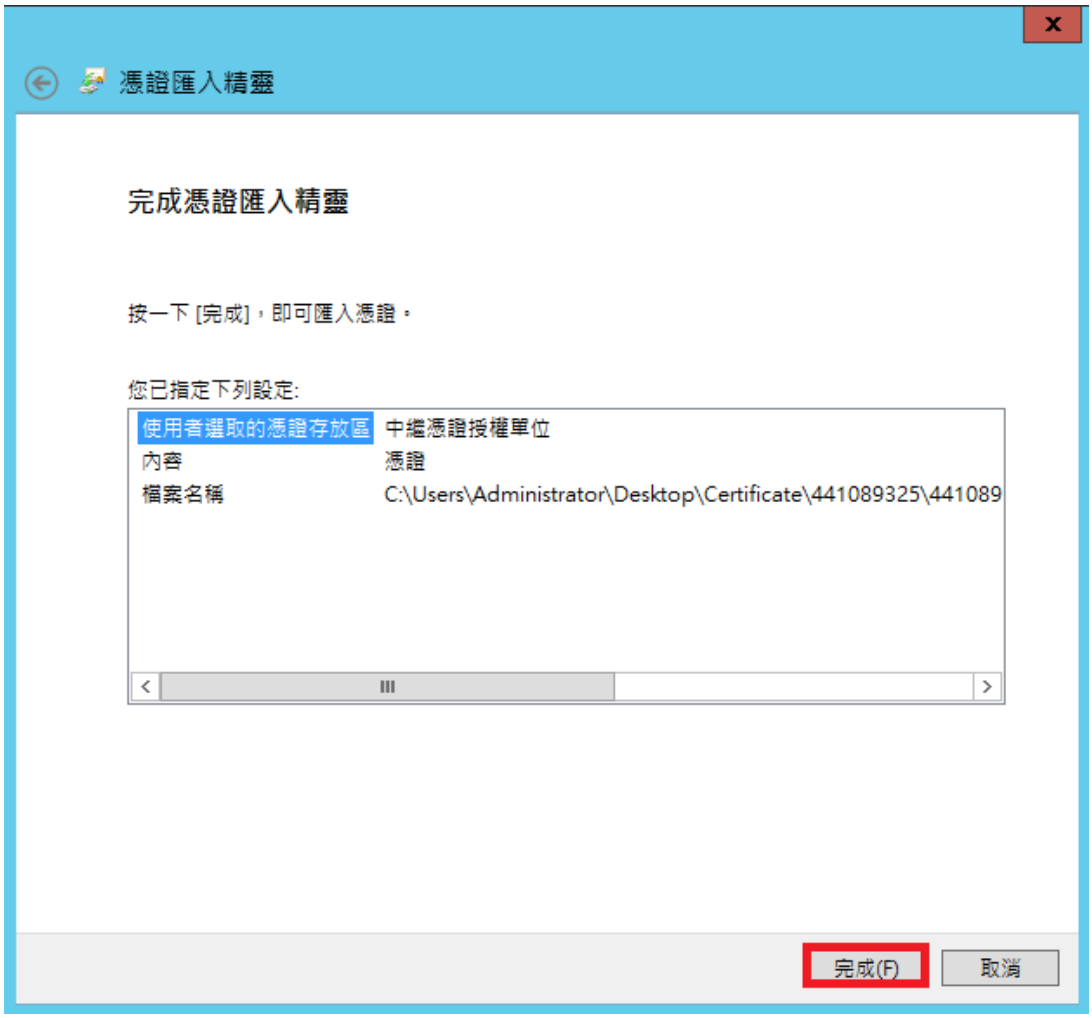


一六、 選擇中繼憑證來源路徑後進行下一步

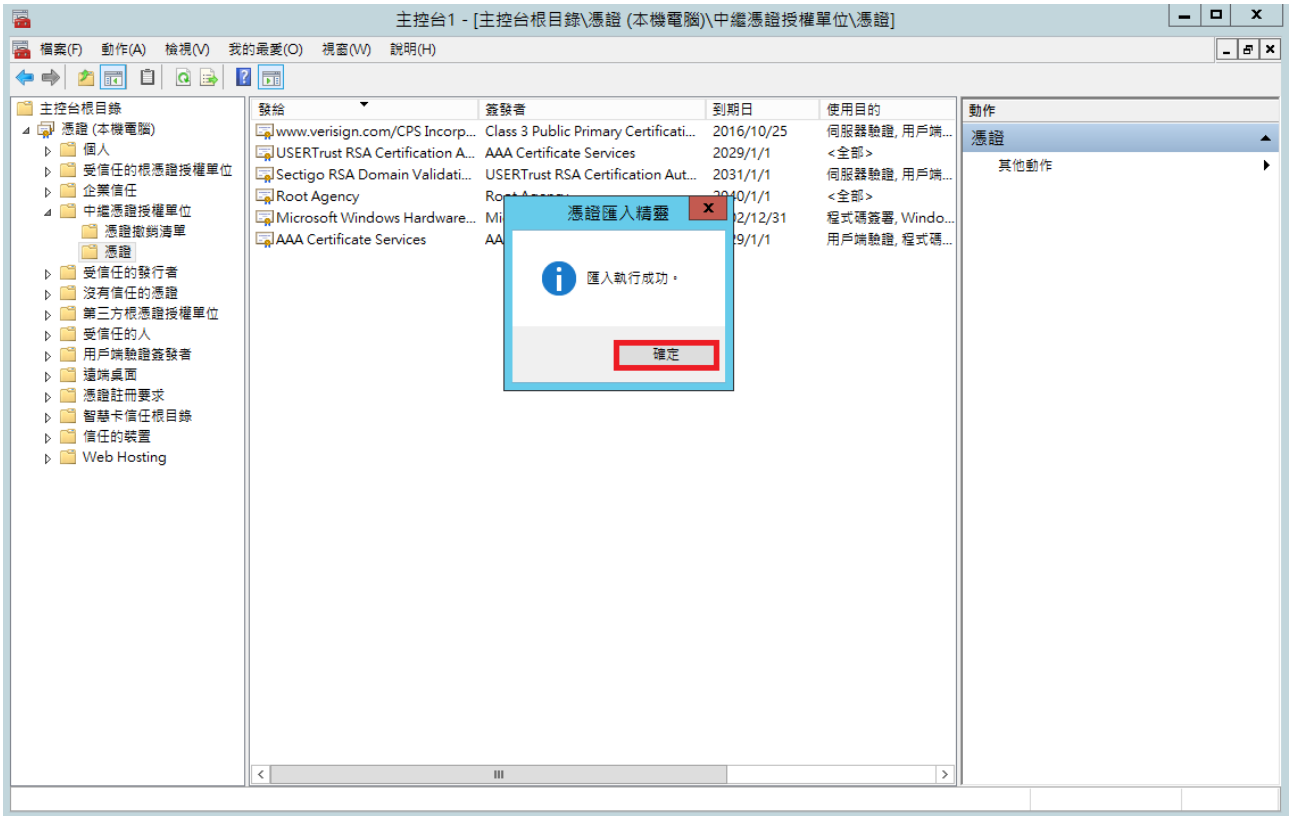


一七、 選擇中繼憑證存放區為「中繼憑證授權單位」進行下一步

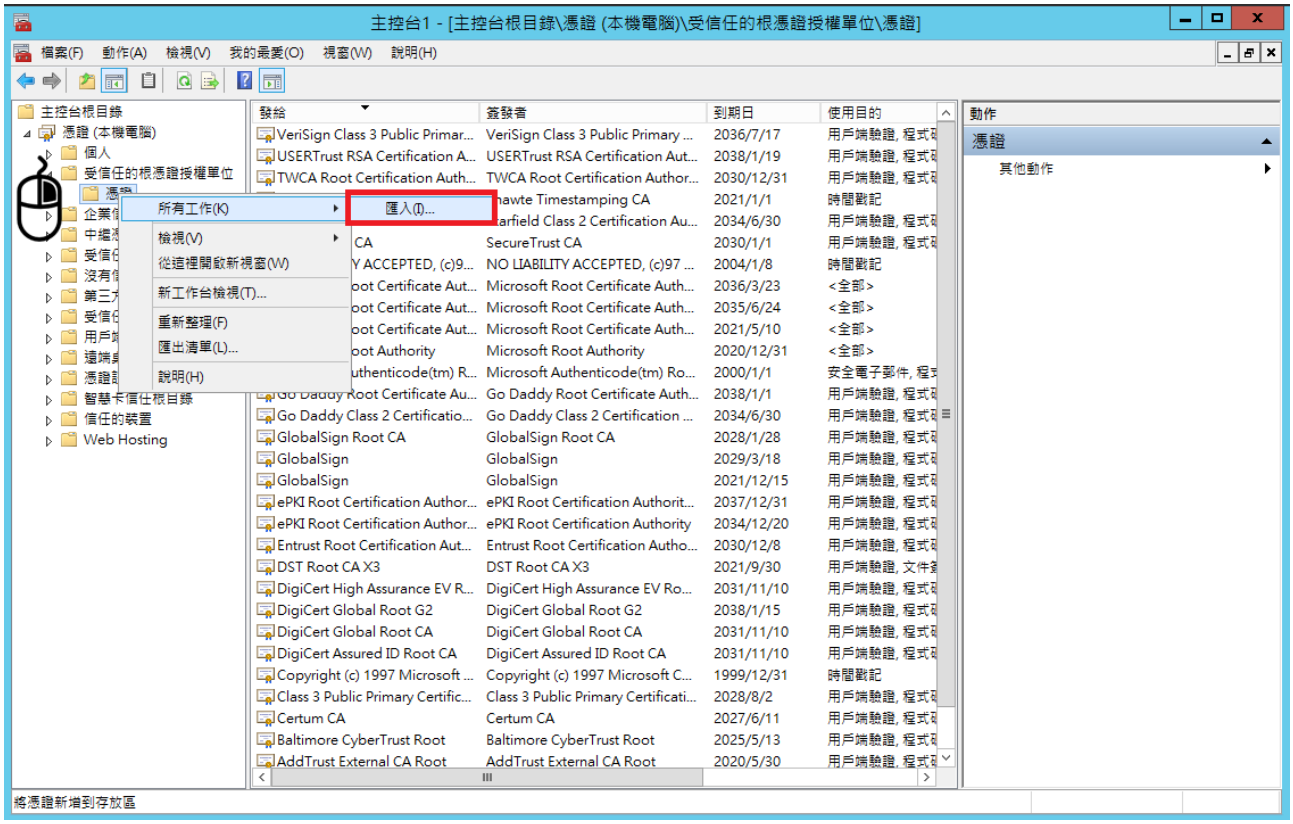
一八、 點擊完成



一九、 點擊憑證匯入精靈的對話框「確認」按鈕



二〇、 匯入根憑證 - 在受信任的憑證授權單位 \ 憑證下 匯入



根憑證的匯入其步驟與匯入中繼憑證的步驟 15-19 雷同，唯憑證存放區域不一樣，但存放區應是與您選擇之憑證樹下存放區的資料夾雷同，故不再贅述步驟。

若有必要，請在「第三方根憑證授權單位 \ 憑證」下一併匯入根憑證。

「受信任的根憑證授權單位」與「第三方根憑證授權單位」的差別，依據微軟的說明其差異性如下：

受信任的根憑證授權

隱含的信任憑證授權單位。包括所有在 [第三方根憑證授權單位] 存放檔中的憑證，以及來自您的組織及 Microsoft 的根憑證。

如果您是系統管理員，而且想要將協力廠商憑證授權單位授予的憑證新增至此存放區中，以供 Windows Server 2003 Active Directory 網域中的所有電腦使用，則可使用 [群組原則] 將受信任的根憑證分送到您的組織中。如需相關資訊，請參閱 信任的根憑證授權原則

第三方根憑證授權單位

此受信任根憑證是指來自 Microsoft 或您組織以外的憑證授權單位。

有關於各品牌中繼憑證與根憑證資訊，請參閱附錄資料。

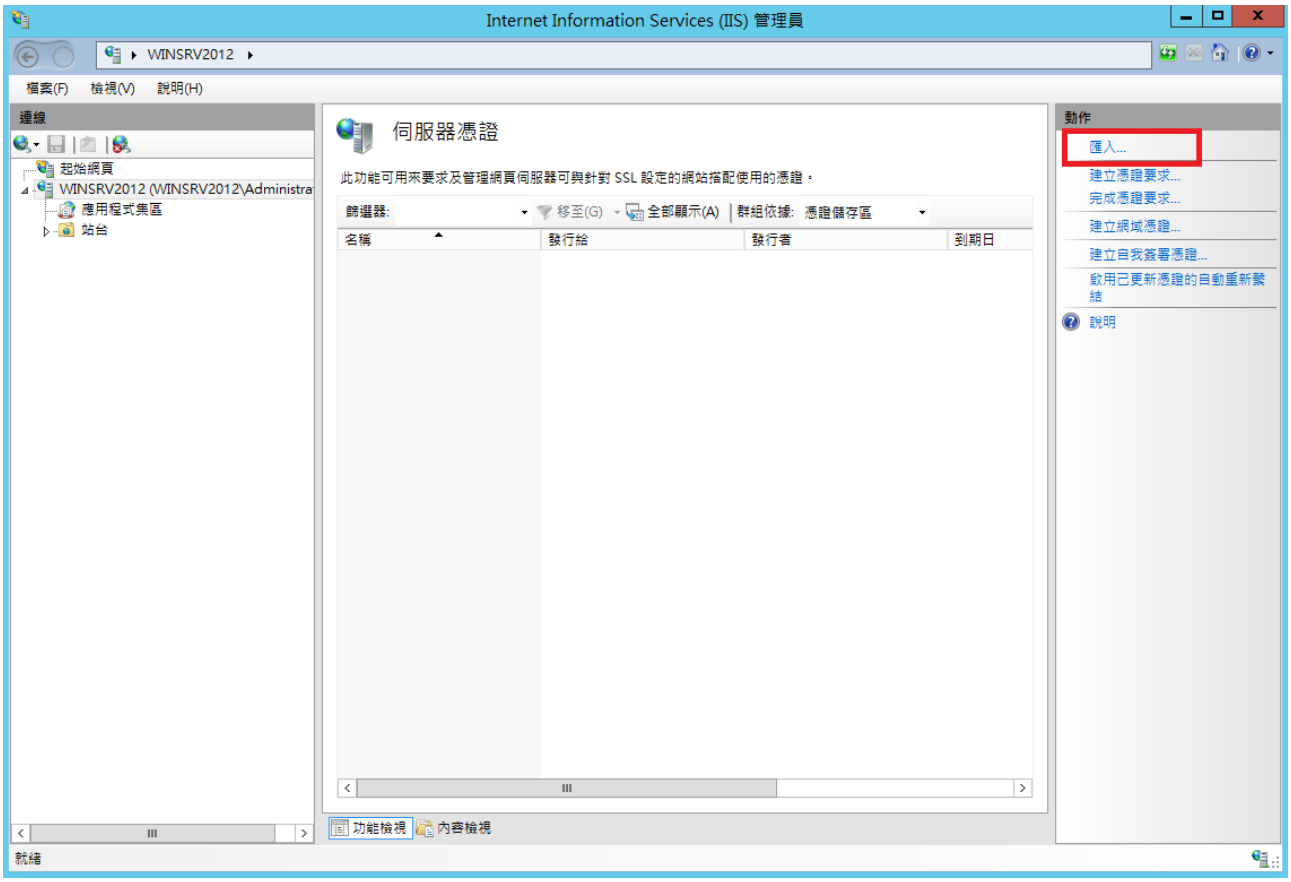
C、 使用「匯入」方法將 PFX 格式憑證匯入 IIS 或 MMC

使用對象：

1. 原先以 Linux 或其他開放平台生成 CSR 與私密金鑰的使用者。
2. 購買了多域名型憑證或是通用型憑證且有混合佈署的使用者。
3. 有做混合系統部署或是 Web Farm 等多主機負載平衡的使用者。

將 PFX 格式憑證匯入 IIS

一、打開 IIS 並點選「伺服器憑證」後，按下動作欄的「匯入」



什麼是 PFX 格式？

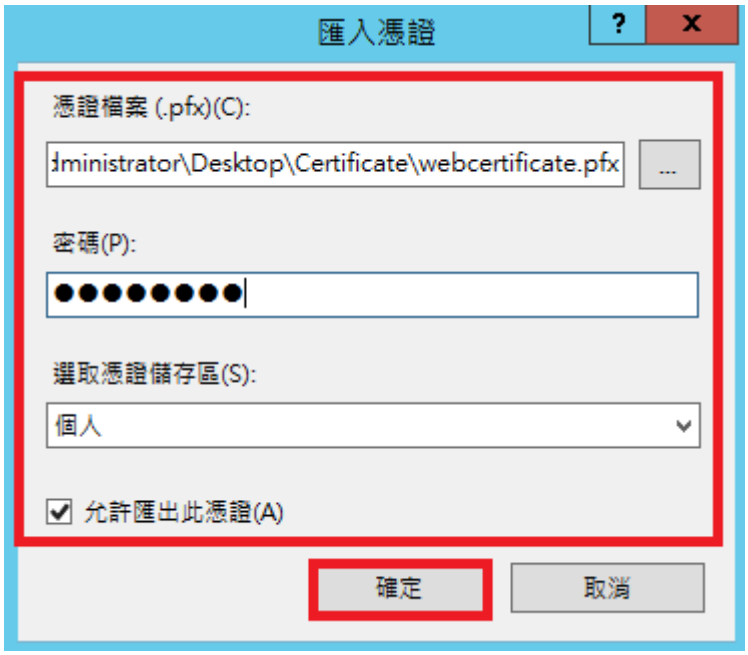
在密碼學之中，PKCS#12 定義了一種存檔格式，通常用它來打包一個私密金鑰及有關的 X.509(PEM 格式) 憑證，或者是信任鏈的全部項目。

一個 PKCS#12 格式文件通常是被加密的，同時又單獨存在 (存檔文件格式)。所以可以用一個容器的概念去理解它 - 一個裡面放了憑證與金鑰，且上了密碼鎖的箱子。

常用的副檔名格式為 .P12、.PFX。

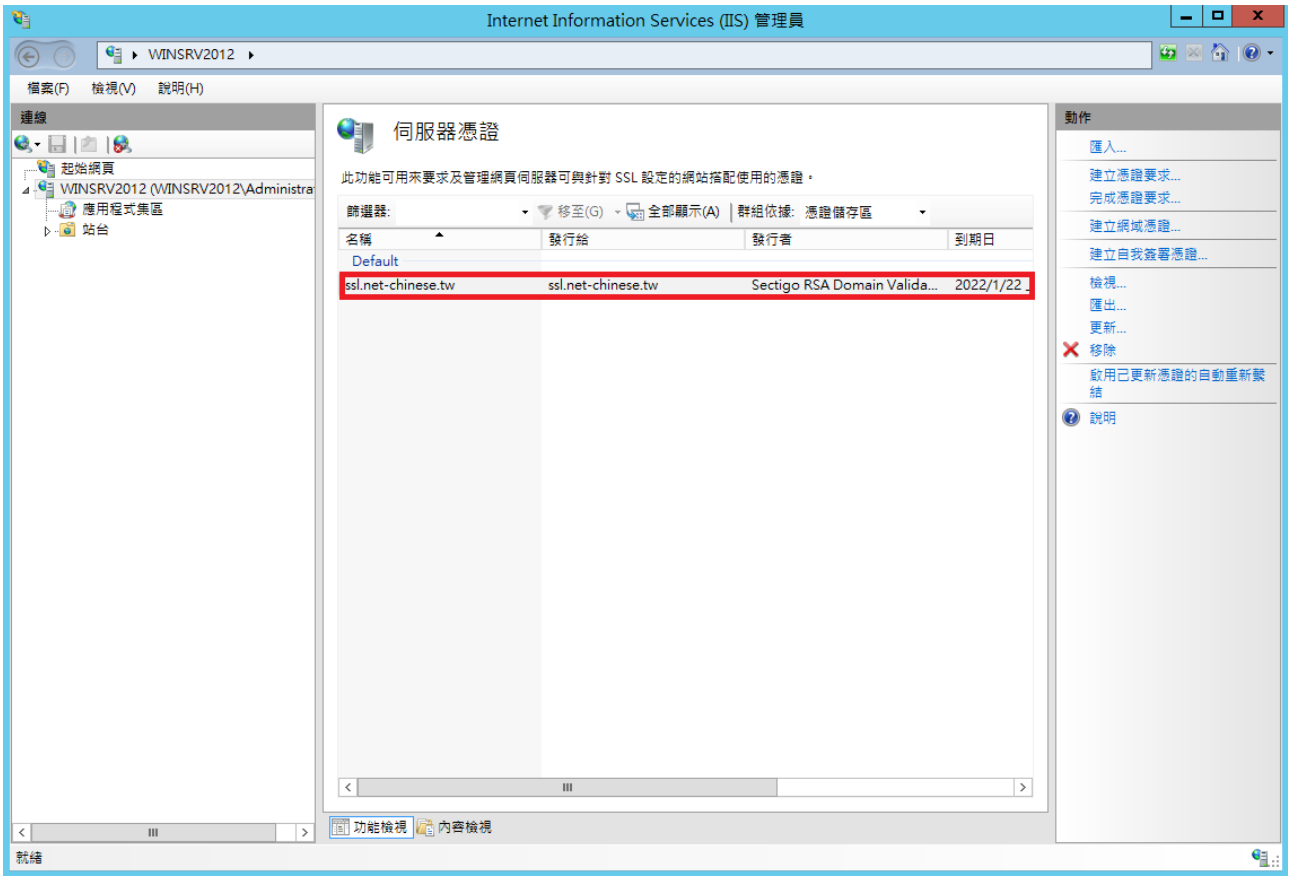
可以透過 OpenSSL 的指令對 PFX 文件進行打包、拆包的轉換工作。

二、選取憑證來源並輸入密碼，選擇憑證儲存區後，按下「確定」。



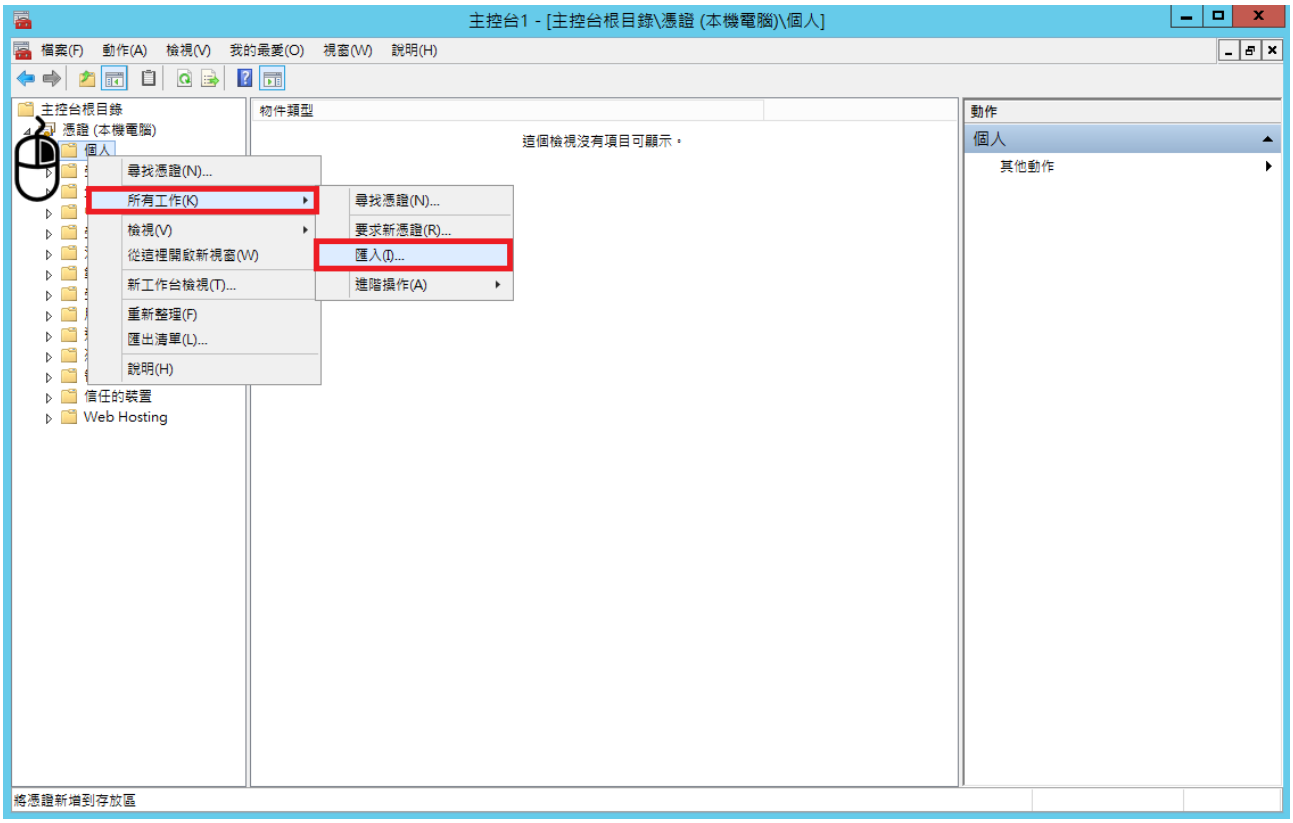
小提醒：
如果未來還有想要在這台主機上匯出憑證時，請記得勾選「允許匯出此憑證」

三、若是在這邊有看到憑證，即代表憑證匯入成功。

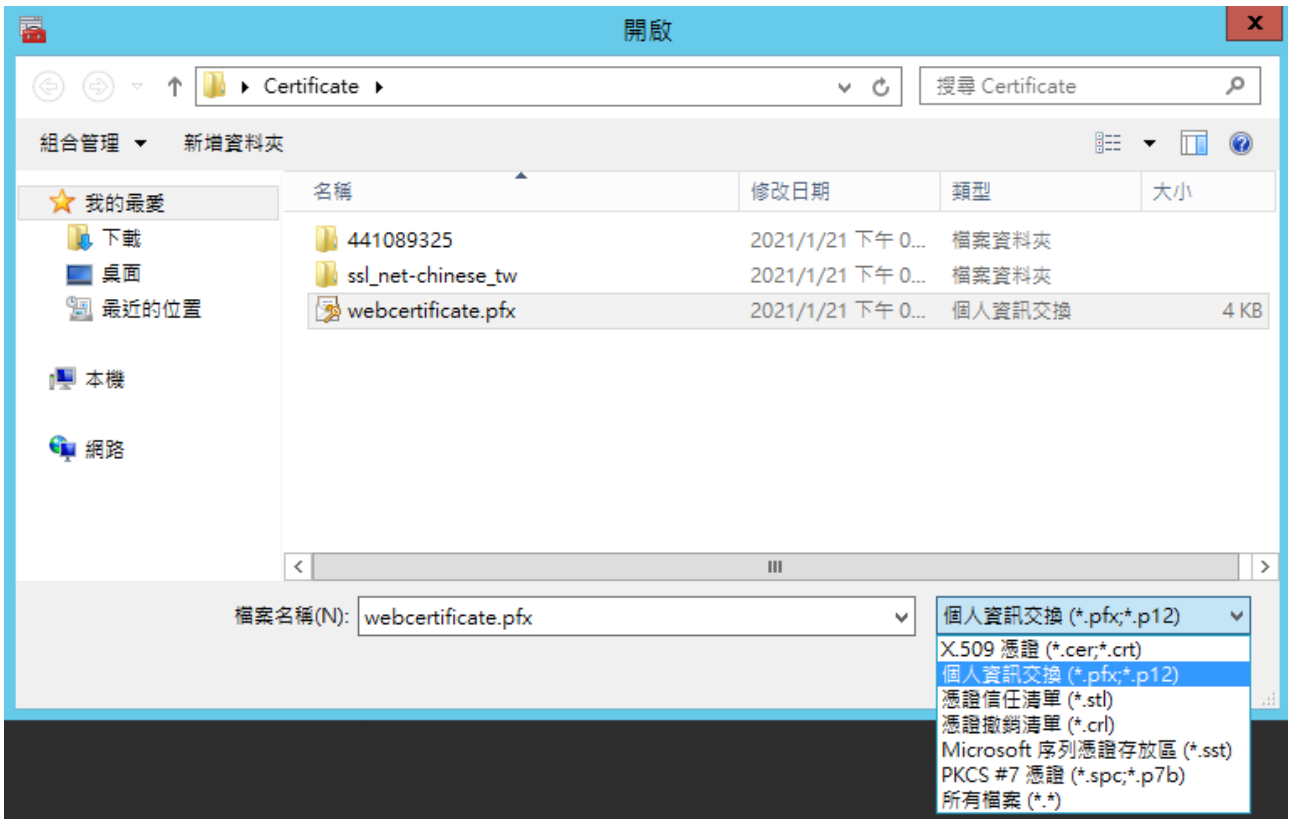


將 PFX 格式憑證匯入 MMC

一、 在憑證樹的「個人」資料夾中按滑鼠右鍵選「所有工作」 匯入



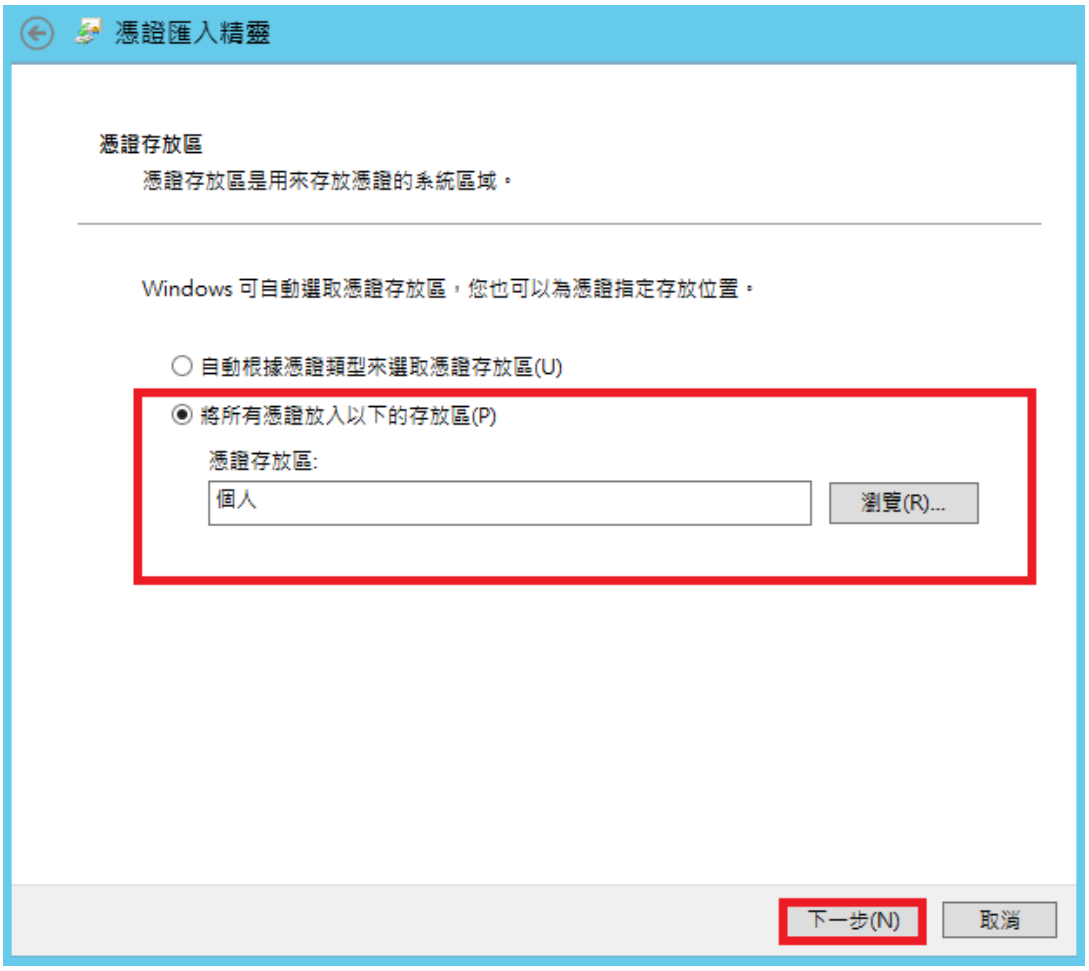
二、 按「瀏覽」選擇網站憑證的來源，無誤後按「下一步」。



如果在瀏覽時找不到 PFX 格式，請記得在旁邊的下拉選單選取「個人資訊交換 (*.pfx;*.p12)」

三、 輸入 PFX 密碼，如未來有匯出需求請把匯入選項中的方塊打勾

四、 選擇憑證存放區為「個人」，無誤後按「下一步」



五、 確認匯入資訊，無誤後按「完成」

六、 點選「確定」結束匯入成功的對話方塊。

在這個章節中分別示範了兩種匯入憑證的方法，兩者都可以使用。主要還是看憑證發行機構給你何種類型的憑證，還有取決於您需不需要匯入中繼憑證、根憑證等信任鏈憑證的需求。

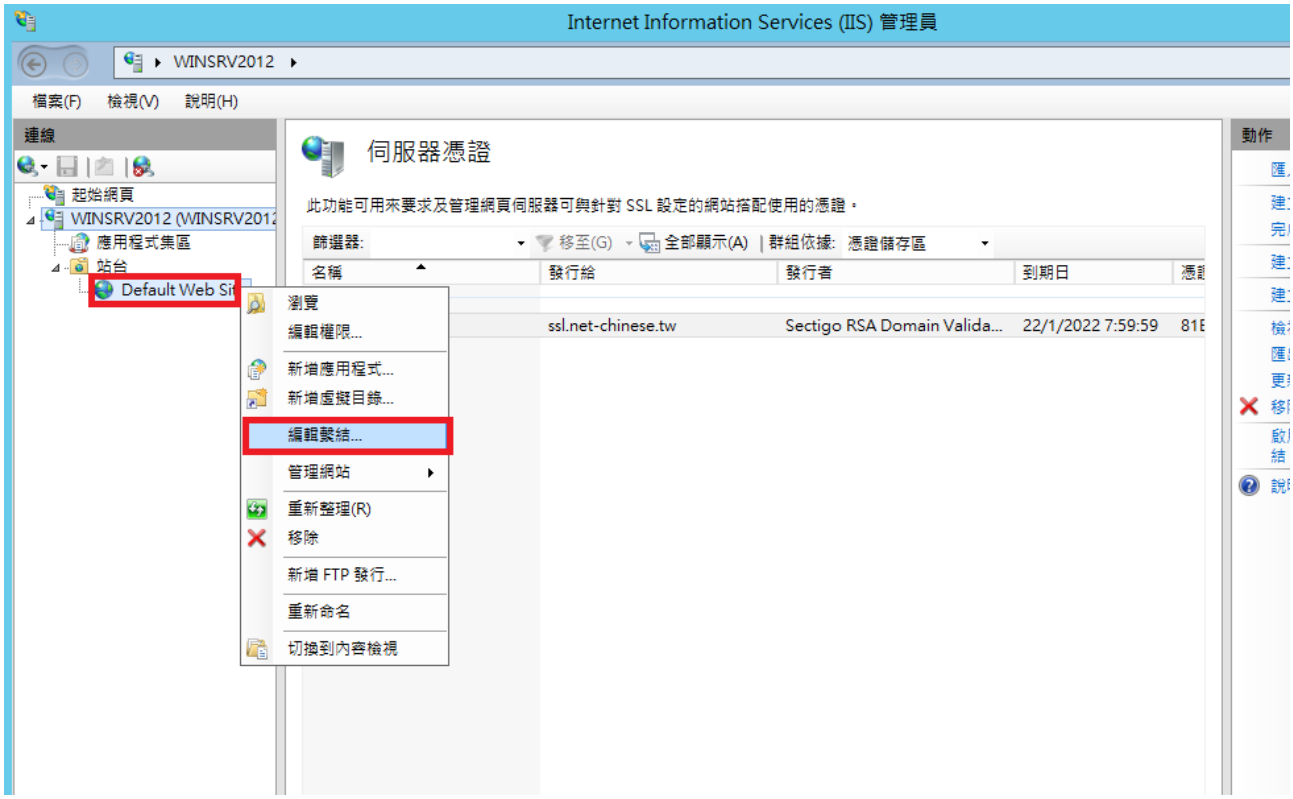
PFX 的確是一個比較麻煩的格式，需要做拆解包的動作，這個動作需要借助一些工具來執行，將會在後面進行教學。

章節 3

將已裝好的憑證與站台繫結

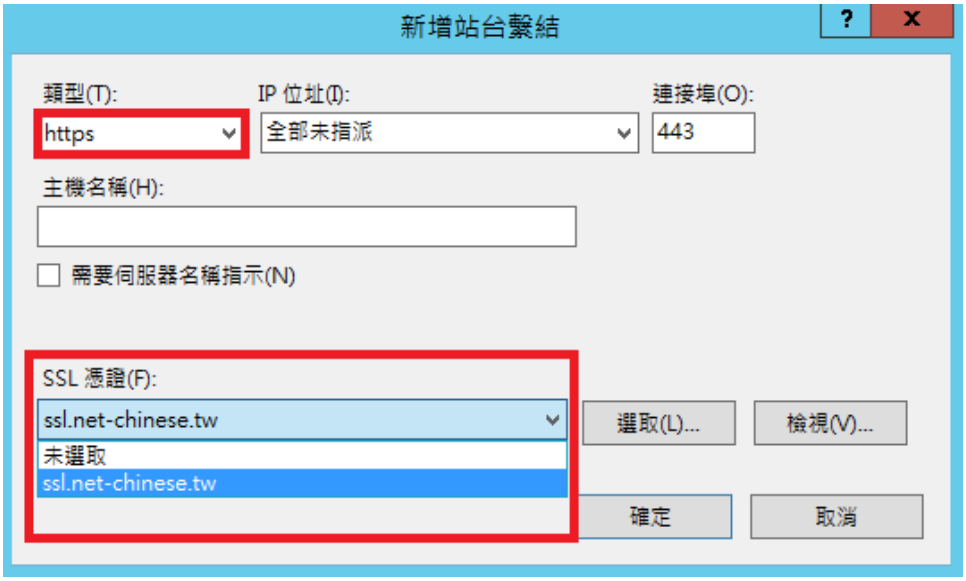
本章節將帶領您操作如何將已匯入主機的憑證給繫結到您的站台上，讓您的網頁可以正常的使用 SSL 憑證。

一、在 IIS 的「站台」圖示點右鍵選擇「編輯繫結」



二、在站台繫結中先點「新增」

三、類型選擇「HTTPS」且 SSL 憑證下拉您匯入的憑證

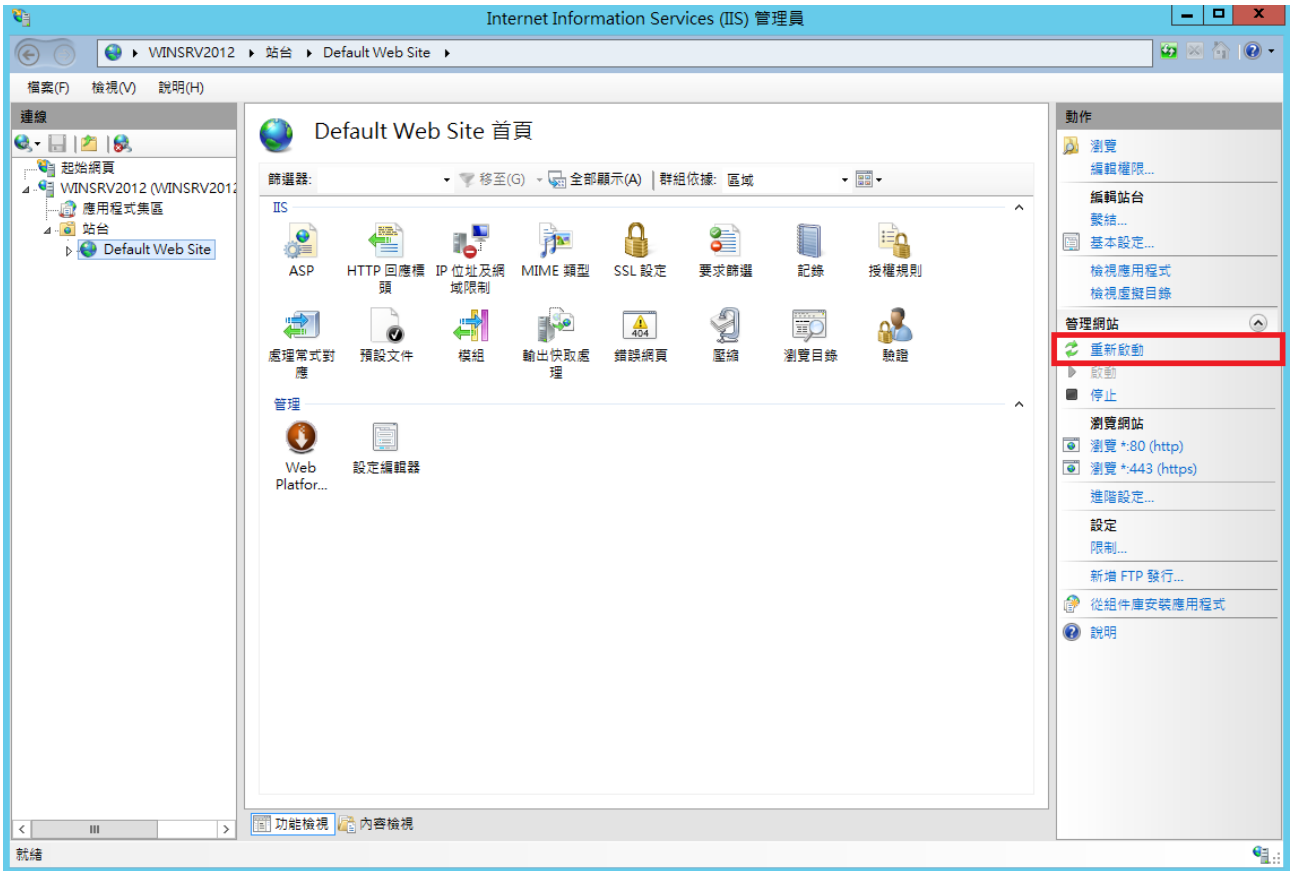


在您選擇類型為 https 時，預設的連接埠是 443，除非有特殊需求，否則無需更動連接埠號碼。若您對此做了更動，建議您在聯外路由及防火牆開通相應的連接埠接口。

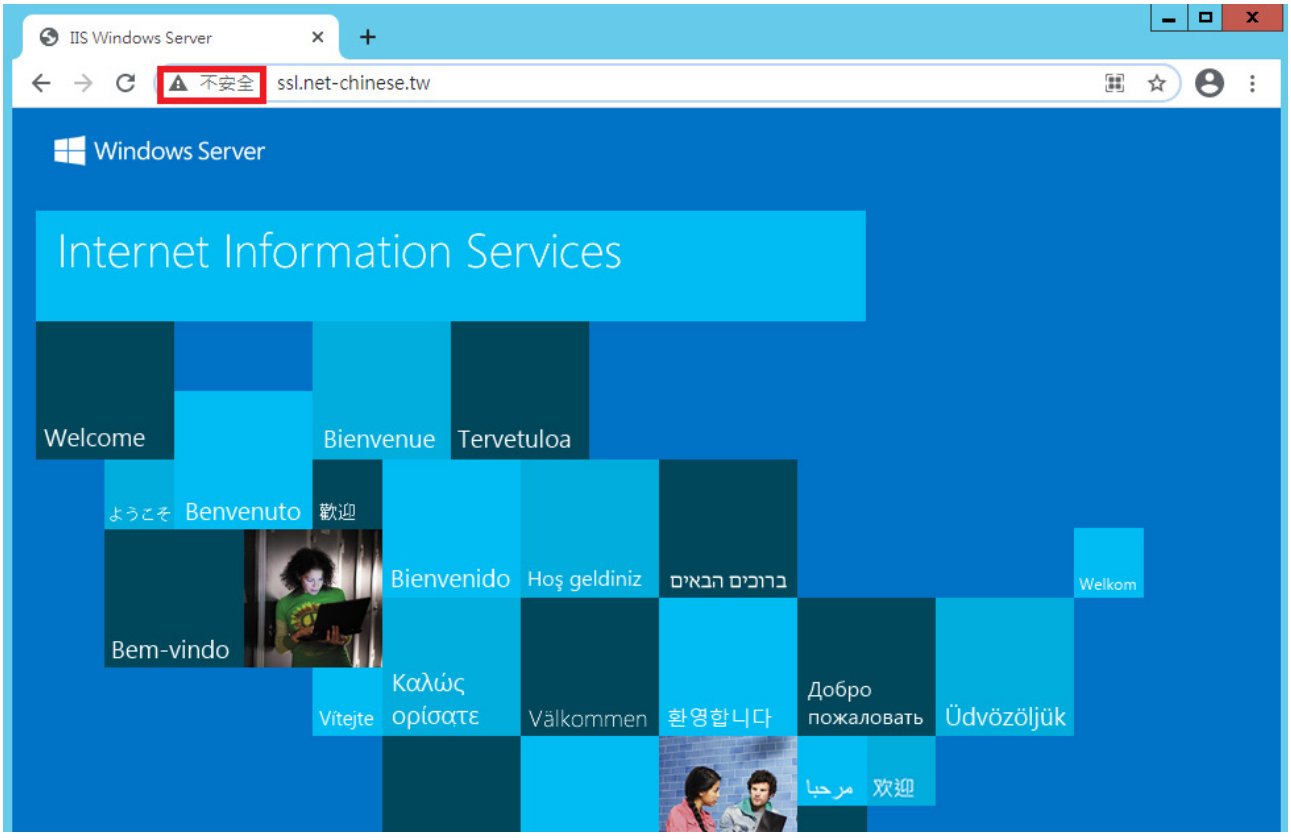
如果您有多個 Virtual Host(虛擬主機)，主機名稱要設定含主機名稱網址，例如：mail.net-chinese-.tw

四、確認站台繫結中已新增了 HTTPS 後關閉視窗

五、重新啟動 IIS



六、開啟瀏覽器進行測試

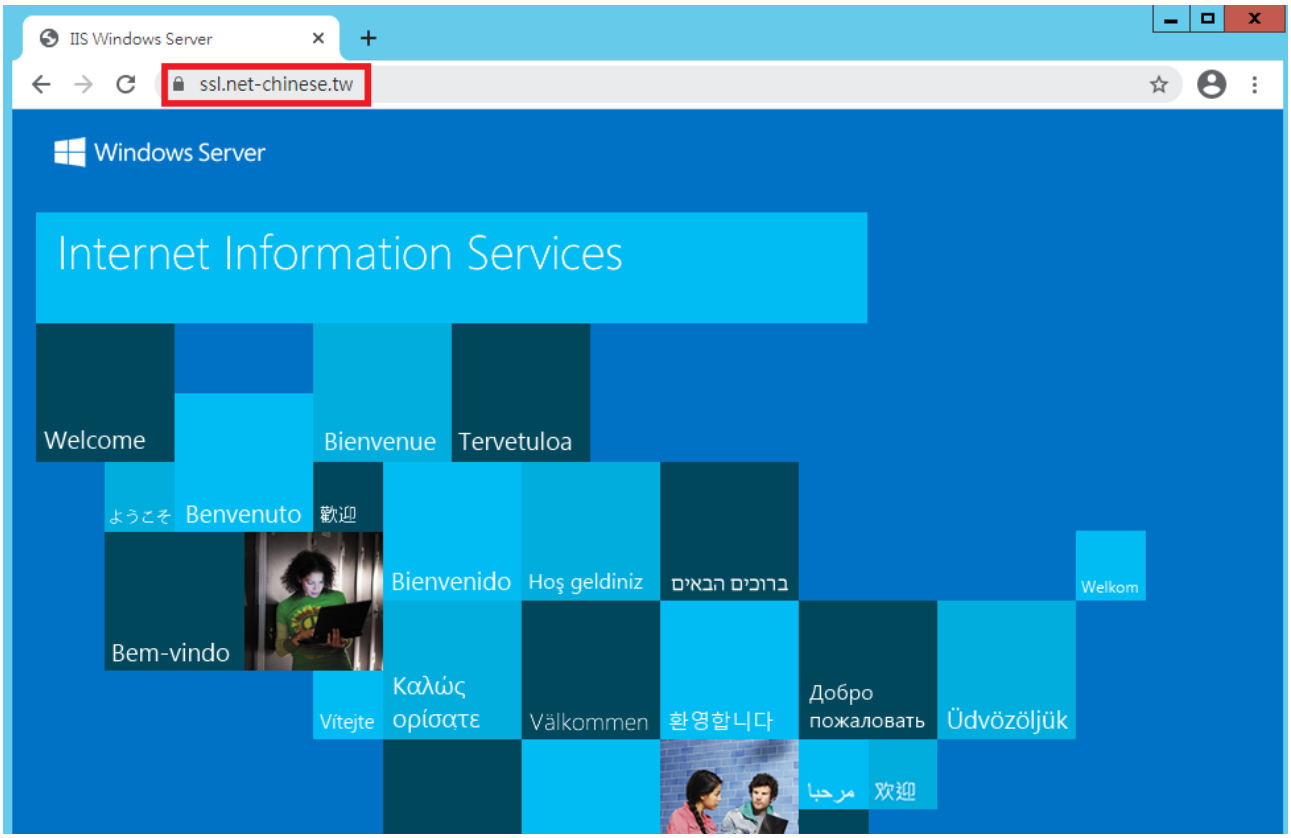


為什麼會顯示不安全？

當您設好了繫結，也放了憑證，為什麼還是顯示不安全呢？在上一步的站台繫結中，我們同時了保留連接埠 80 的非安全通道，及新增了 443 埠的安全通道，所以實際上網站的運作是安全通道及非安全通道都可以開啟網頁的。我們在這裡不建議您刪除 80 埠的非安全通道，因為您沒有辦法預期客戶會怎樣開啟您的網頁，會建議您改用導轉的方式將其導引至安全的通道。(請參照附錄 A)

讓我們試著在網址前加入「https」看看吧。

一般的網頁都會有快取 (Cache) 機制，其作用是將您瀏覽過的頁面預存在電腦中，再透過 Cookie 的方式做一些記憶，所以很多時候當您只輸入 URL 而不特別加前置的 http:// 或 https:// 時，瀏覽器都會用您過去瀏覽的經驗去連接該網站的主機。所以您必須告訴瀏覽器說您要走的通道是加密或非加密的通道。



加入了「https://」後，是不是看到鎖頭出現了呢？這樣代表憑證設置已經完成

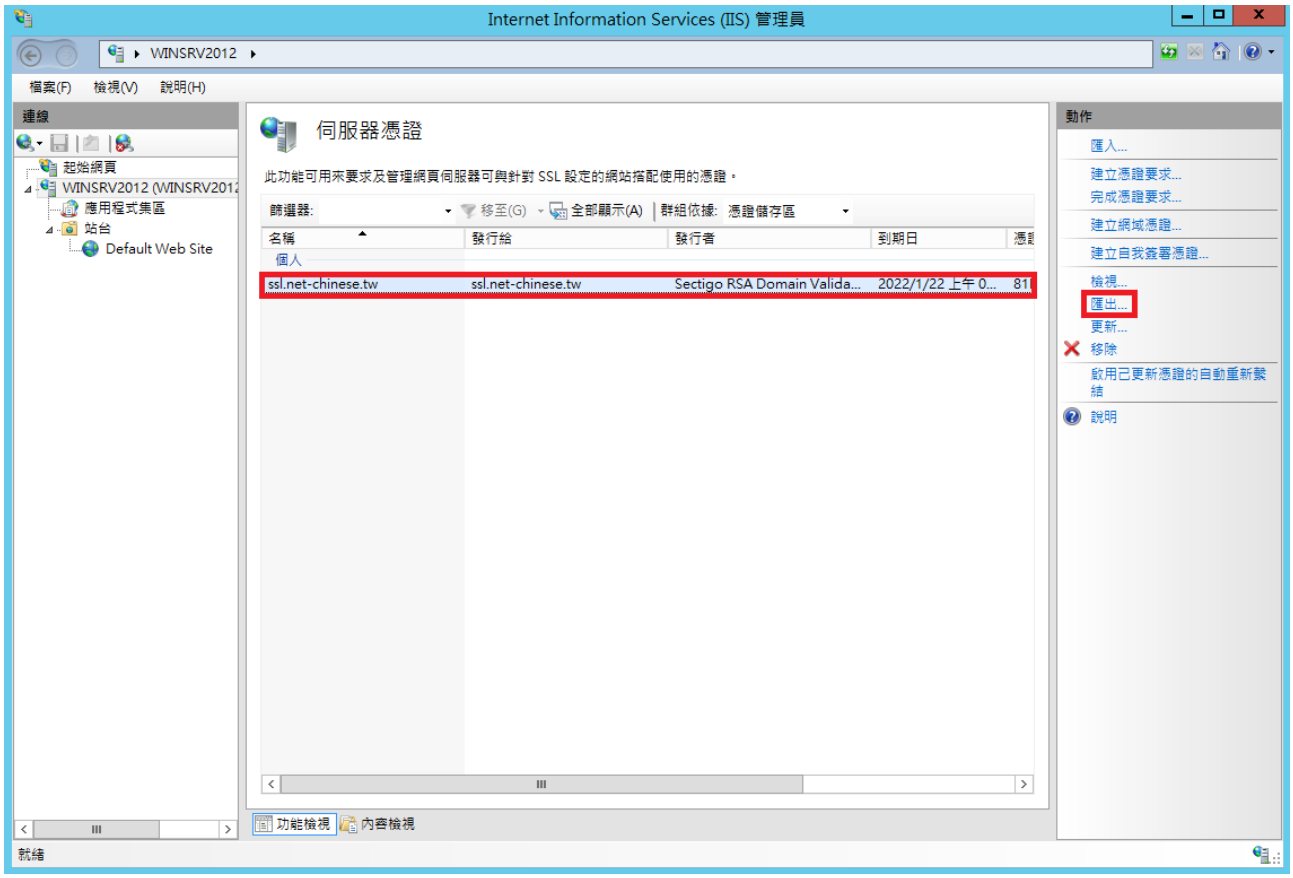
章節 4

匯出憑證以供其他主機使用

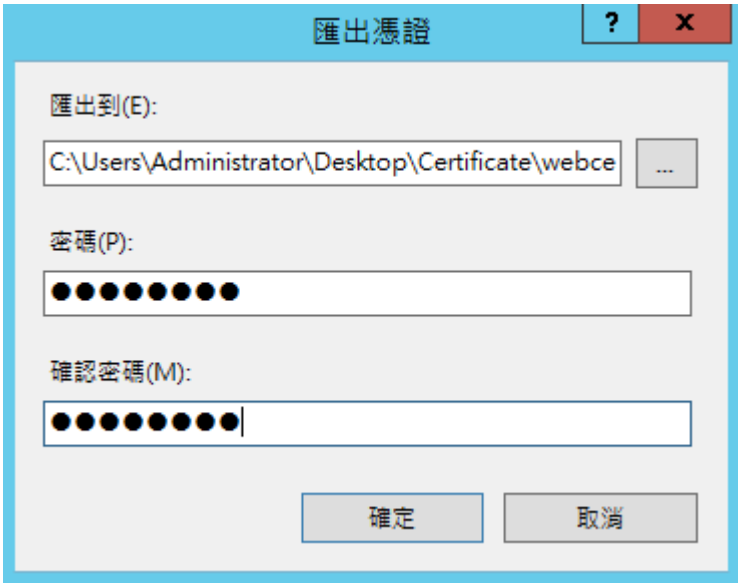
本章節將帶領您操作如何將已匯入主機的憑證給匯出來，以便您帶著憑證至其他主機上安裝。

在 IIS 中匯出憑證

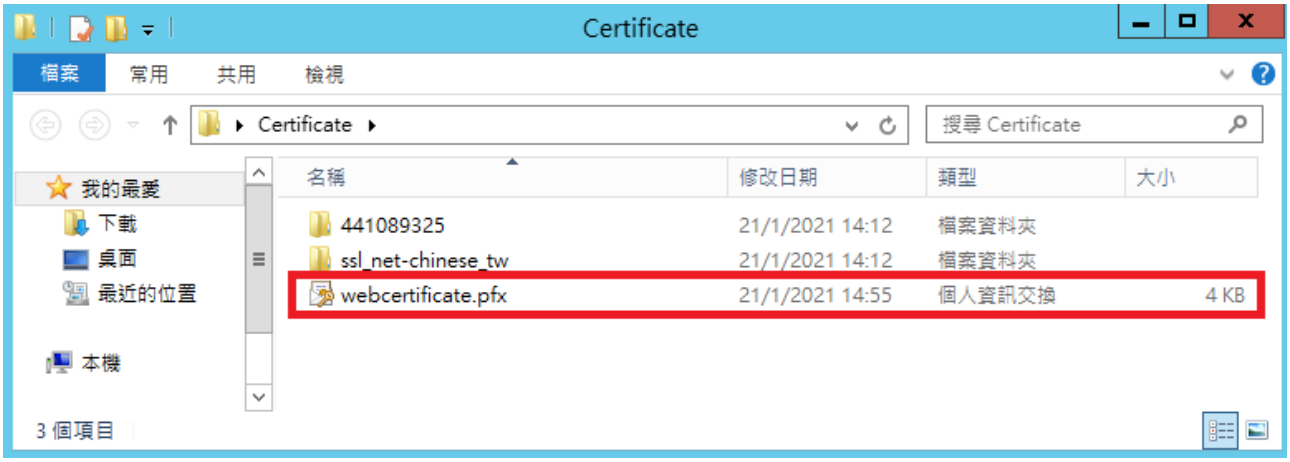
一、在「伺服器憑證」選擇憑證後於動作欄中選擇「匯出」



二、選定存檔的路徑並自行設定密碼

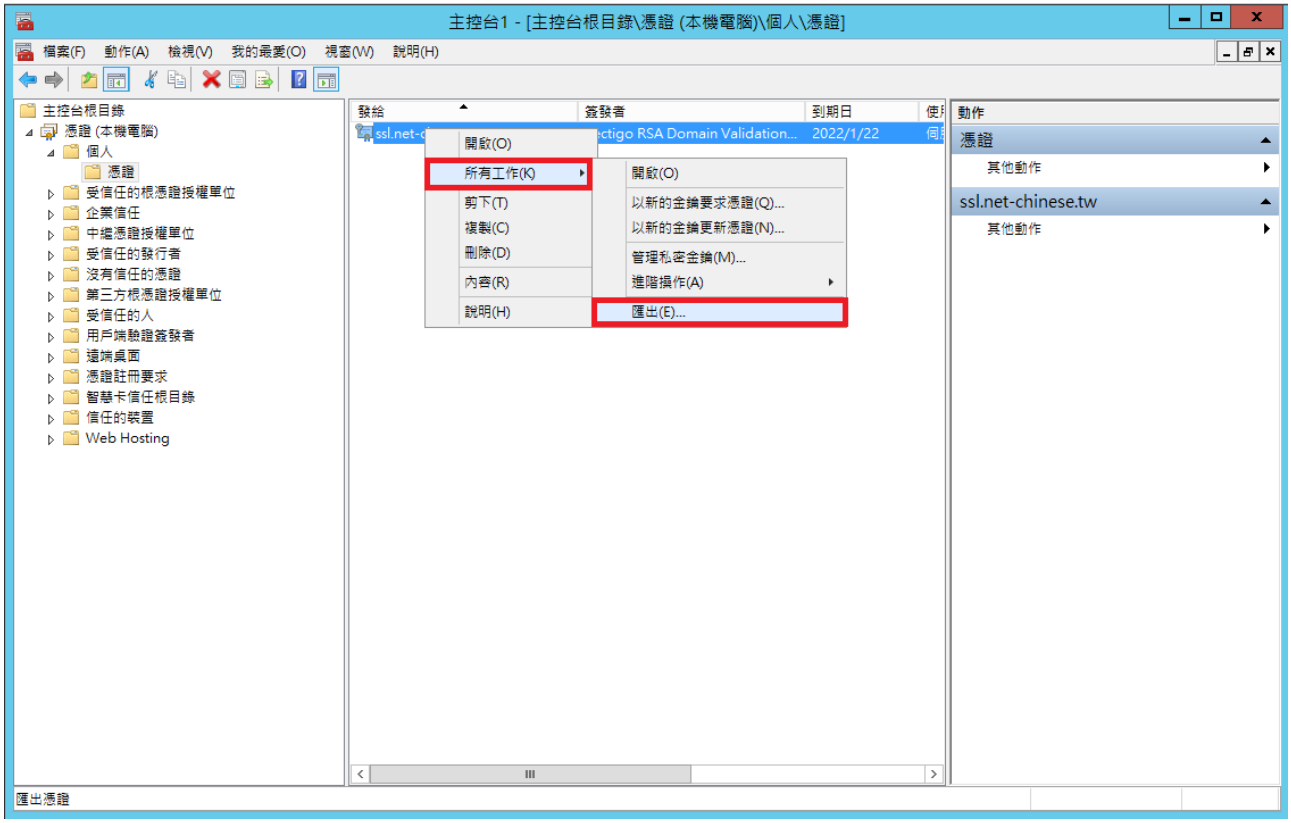


三、到存檔路徑找尋匯出的憑證

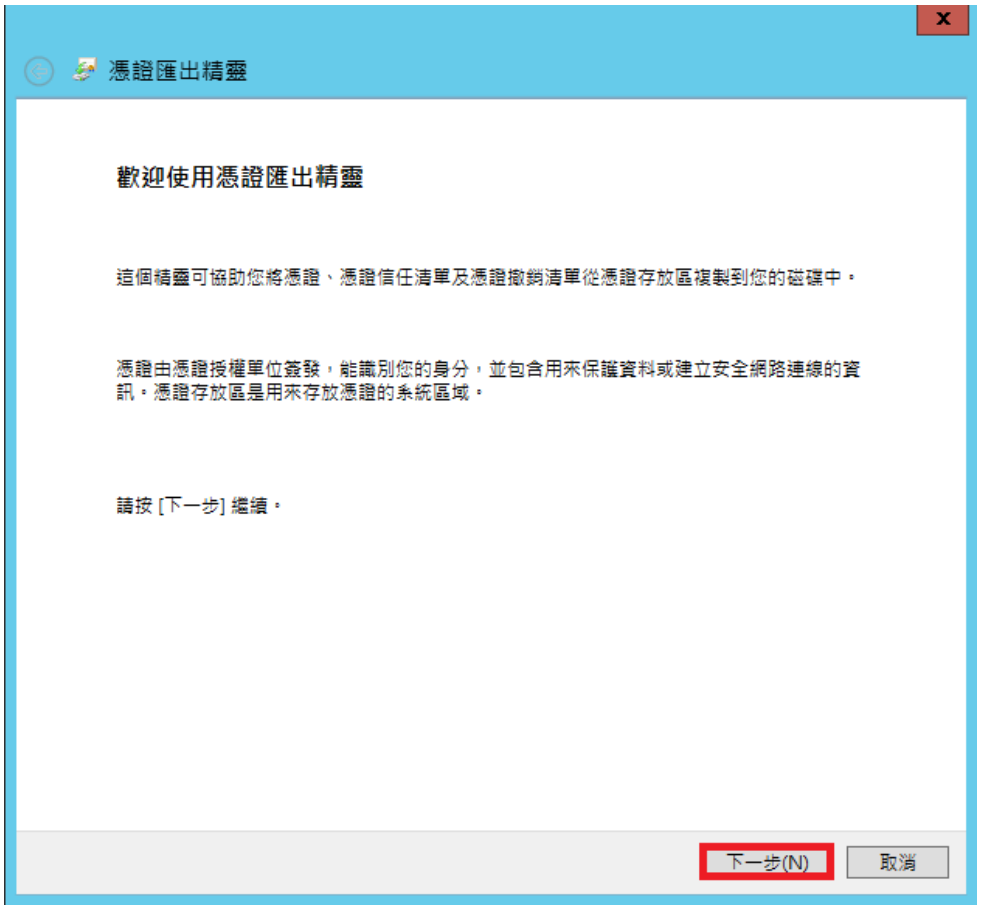


在 MMC 中匯出憑證

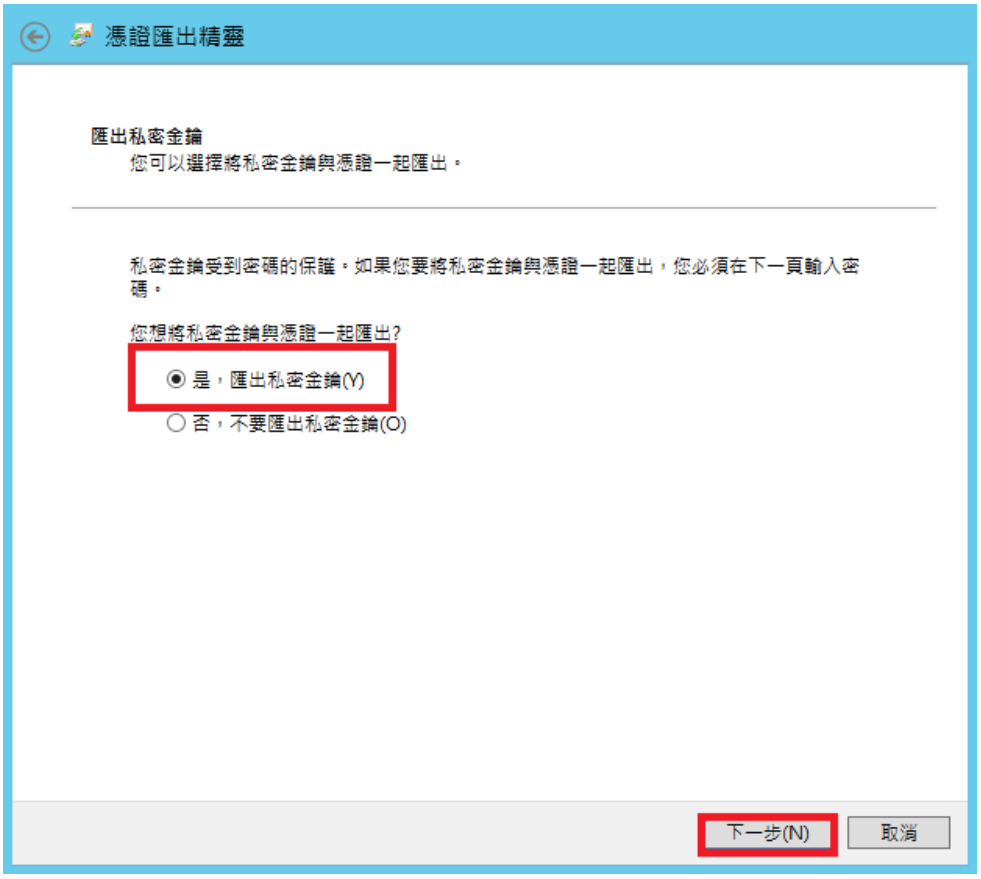
一、在 MMC 的「憑證 (本機電腦)」中個人項下的憑證點右鍵匯出



二、在憑證匯出精靈中按下一步繼續。

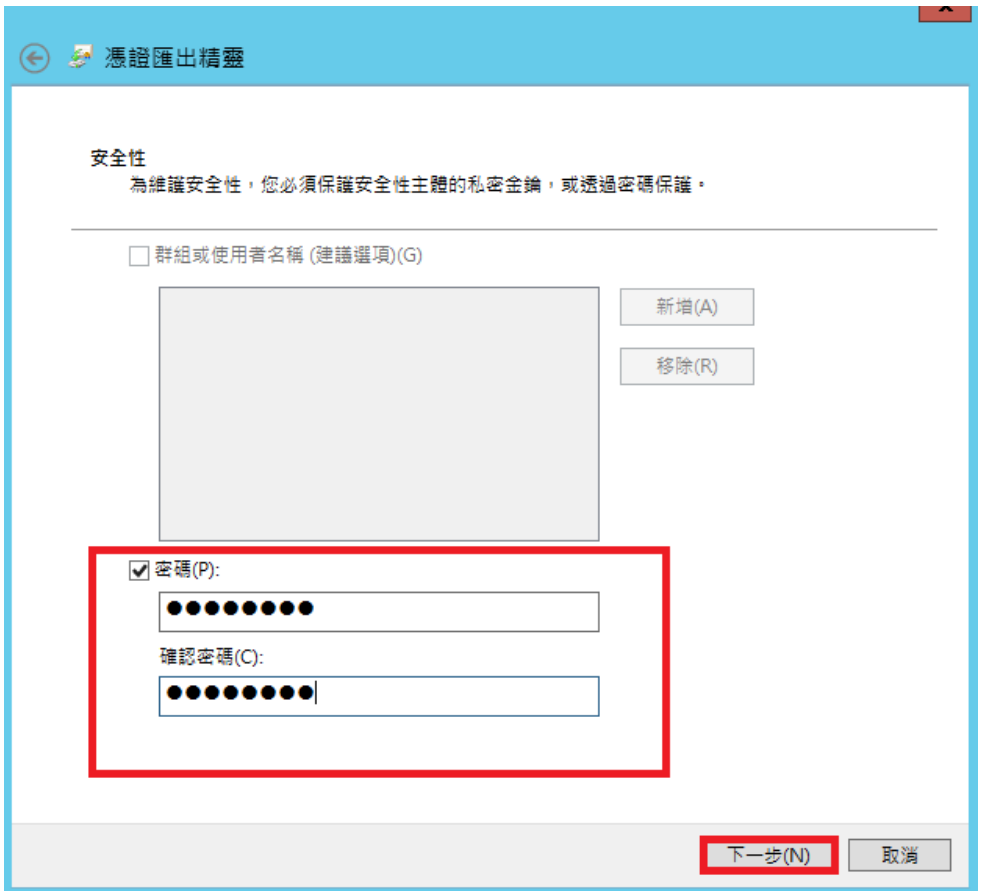


三、選取「是，匯出憑證金鑰」後按「下一步」

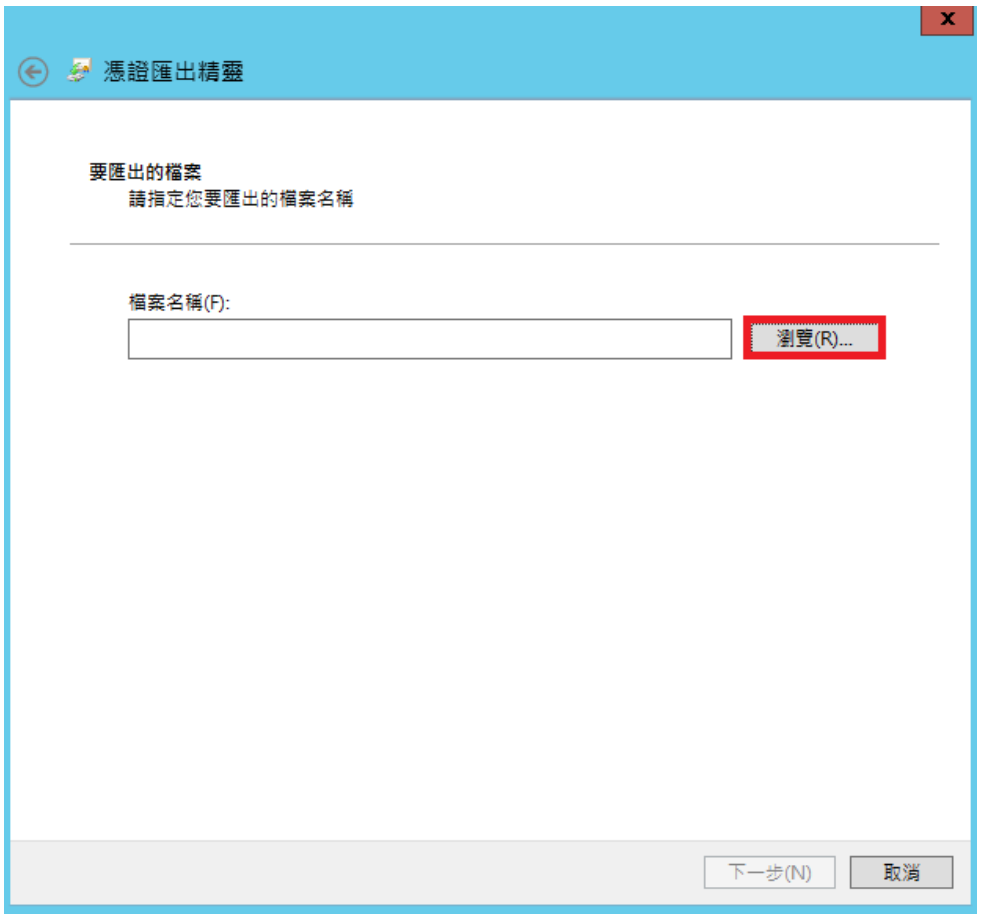


四、選擇個人資訊交換並勾選包含路徑所有憑證及匯出延伸內容

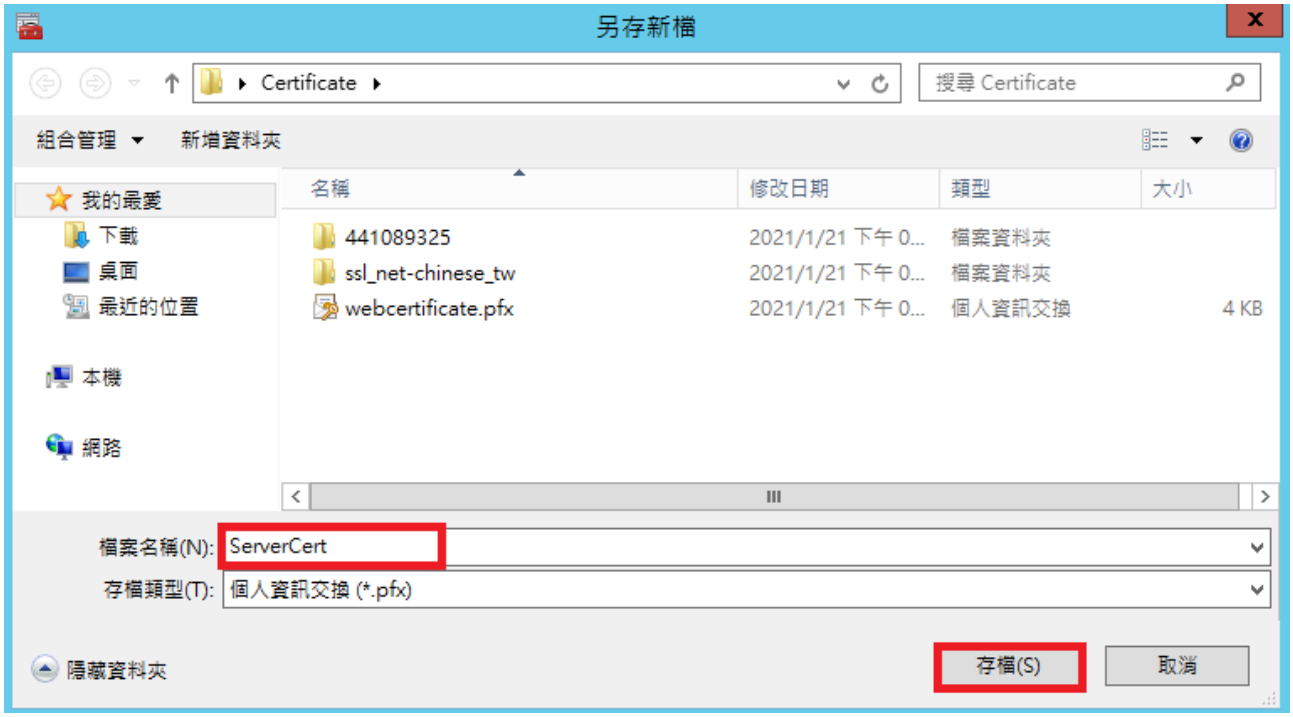
五、設定密碼後按下「下一步」



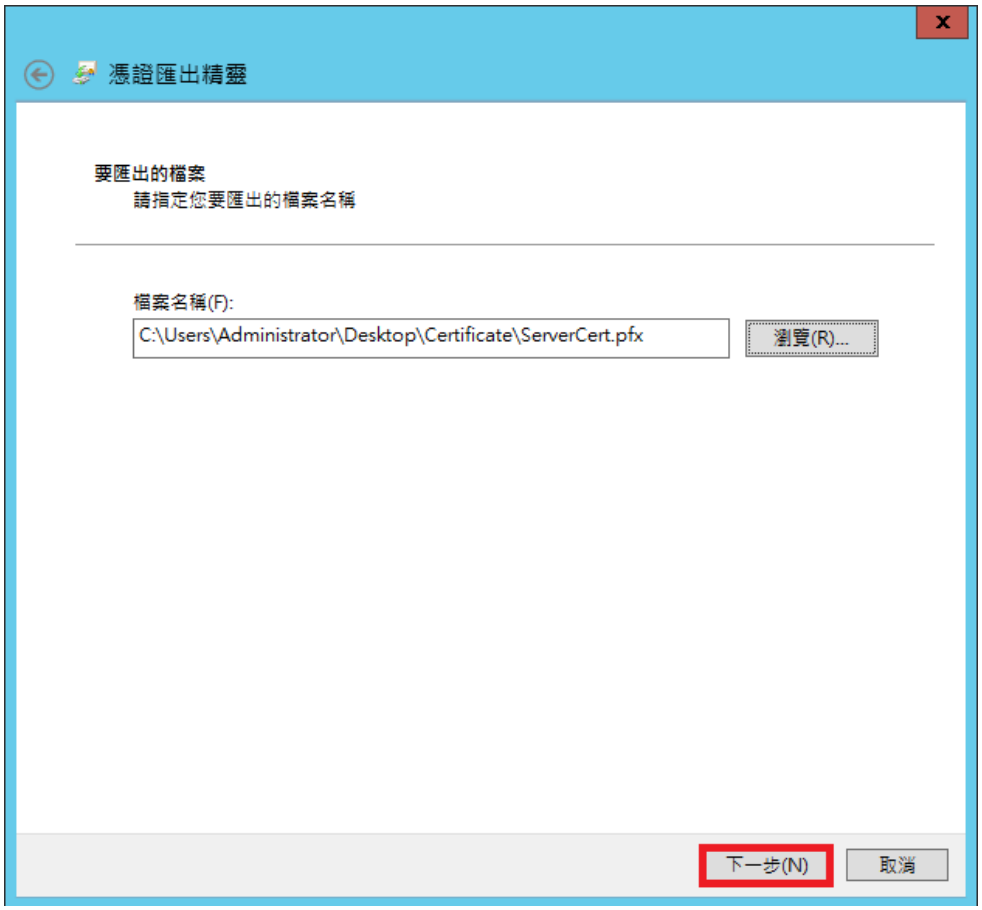
六、點選「瀏覽」設定儲存路徑



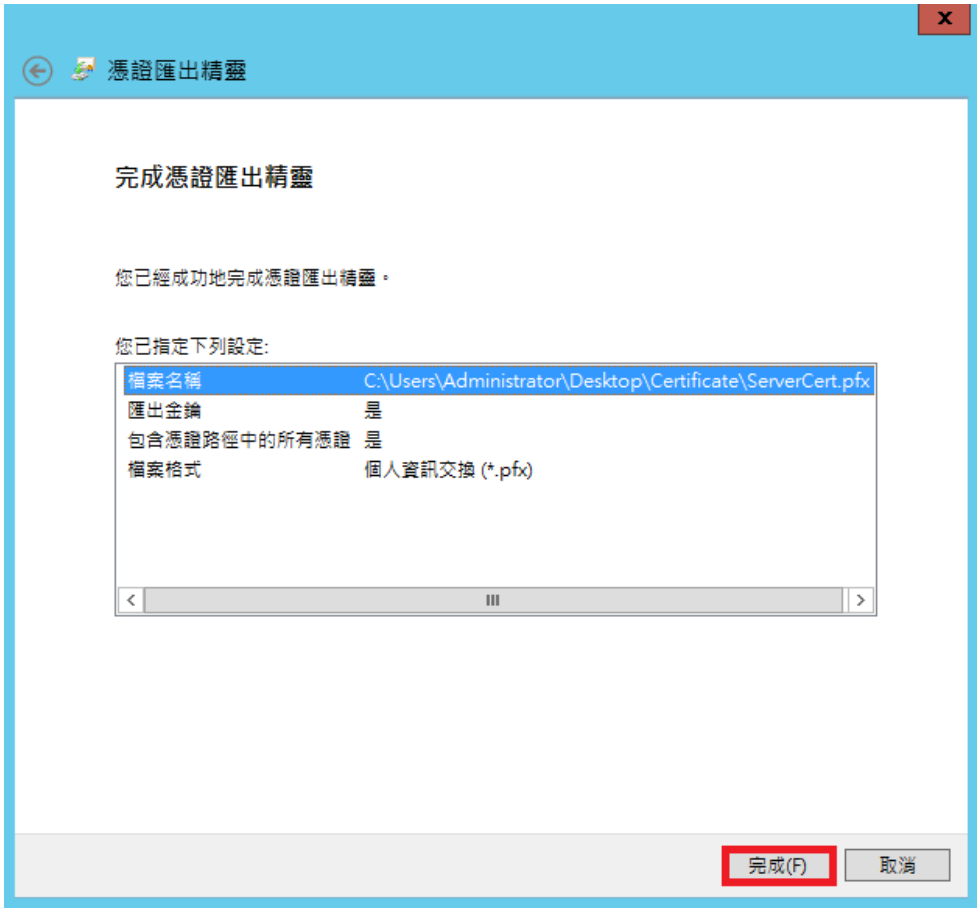
七、選好路徑輸入檔名後按「存檔」



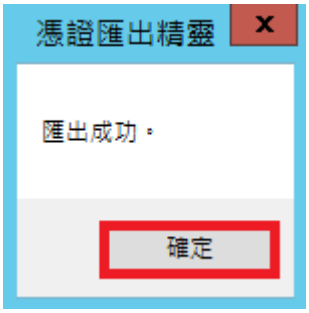
八、設定好存檔檔名與路徑後按下「下一步」



九、確認資訊無誤後按下「完成」



一〇、 按下「確定」以結束對話框



附錄 A- 注意事項：

- **不要使用特殊字元**
  在申請伺服器憑證時，不要出現某些特殊字元，否則在您提交 CSR 後，可能會出現錯誤。這個錯誤是由於在您產生 CSR 時，輸入的資訊中包含一些特殊字元，如：(@,#,&,!, 等等，例如：您可以將 "&" 用 "and" 代替)。

- **什麼是主要名稱 (COMMON NAME)**
  在產生 CSR 的時候，主要名稱 (又稱憑證名稱 /Common Name)，是一定要填寫的，但我們發現有許多的客戶常常在這個地方出現錯誤，或不符合申請規範。

  主要名稱 (Common Name) 是您的主機名稱 + 網域名稱，例如 www.net-chinese.com.tw 的伺服器憑證是頒發給某一台主機的，而不是一個域名，您的主要名稱（Common Name）必須與您要使用伺服器憑證的主機的全名完全相同，因為 www.domain.com 與 domain.com 是不同的兩台主機，除非您將兩個 A 記錄指向同一台主機。

  另外，用戶在產生 CSR 的時候，若 Domain 為 yourdomain.com 請記得產出 CSR 為 www.yourdomain.com。

  如果您今天申請的是單域名通用型域名，則主機名稱請以「*」代替，在主要名稱中輸入 *.yourdomain.com。

- **不要將 CSR 與 KEY 加密**
  有的人使用一些工具進行 CSR 與私密金鑰的生成 (如 OpenSSL 或是 Linux 環境)，在產出過程中，系統會問您需不需要為 CSR 與私密金鑰加上密碼，請記得留空，不要加密。

- **請保管好您的私密金鑰**
  欲產生 CSR 檔案時，則必然會有一組私密金鑰與之相配對，私密金鑰與憑證是密不可分的。一旦您遺失了私鑰，簽發下來的憑證就無法與之配對了，此時您可能就需要重新產生新的私密金鑰與 CSR 檔案來進行重發憑證，重發憑證是否需要費用，則視發證機構的規定。

  若您有多台主機，需要將憑證佈署在多台主機上，則必須所有的主機使用同一組憑證與私密金鑰。

- **私密金鑰長度必須為 2048 位元 (bit)**
  為加強憑證安全強度，目前發證機構已不再頒發低於 2048 位元的 CSR 憑證提交資訊，所以請您在產生 CSR 時務必選擇 2048 位元的位元長度。

附錄 B- 使用網路中文工具對 PFX 進行解離與捆包：

雖然網路中文有提供 CSR 產生工具，但基本上還是建議由主機商或是資訊人員在本機產出 CSR 與 Key 會比較好。如在生成 CSR 的章節有提到，Windows 生成時並不會把 Key 生成給資訊人員。所以如果透過外部工具生成，還需要再捆包成 PFX 格式才能被 Windows 主機可接受。

但如果你同時擁有 Windows 主機與 Linux 主機的話，難免就會需要轉換憑證，才能將其佈署在兩種平台機器上。這個章節就教您如何使用網路中文的工具來做憑證轉換。

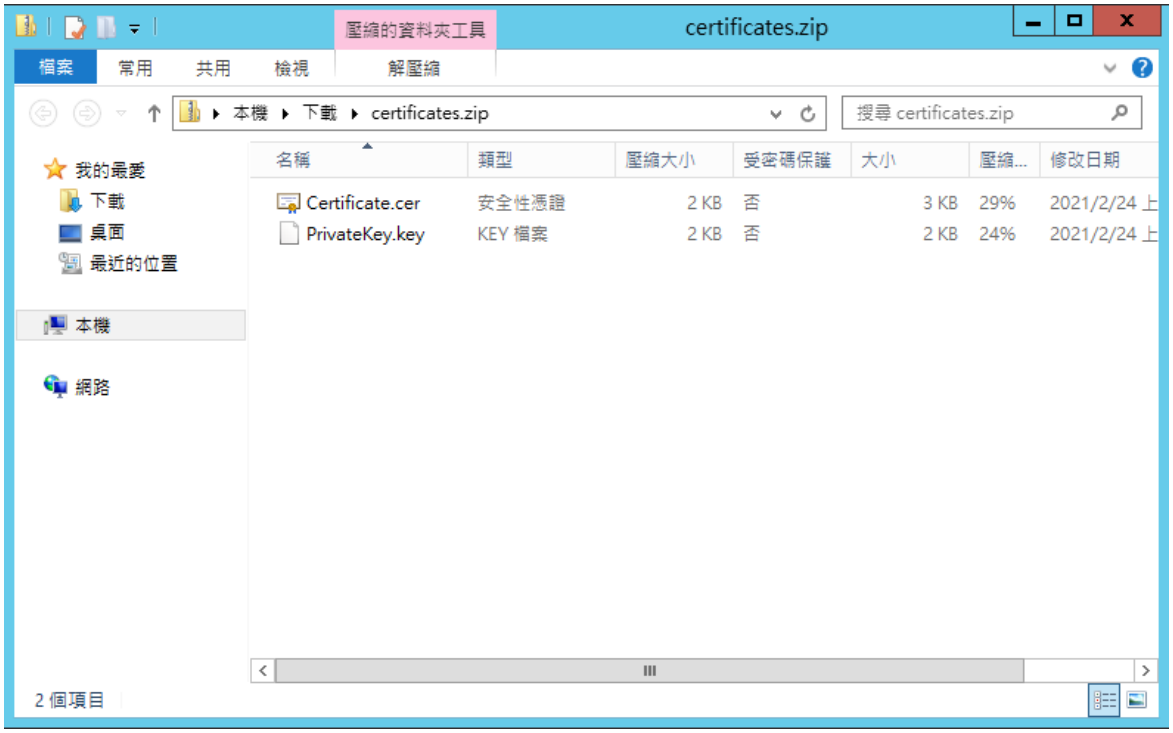
在網路中文的首頁上，您可以透過以下連結開啟。

然後就會看到這樣的畫面，將畫面動捲動至下面

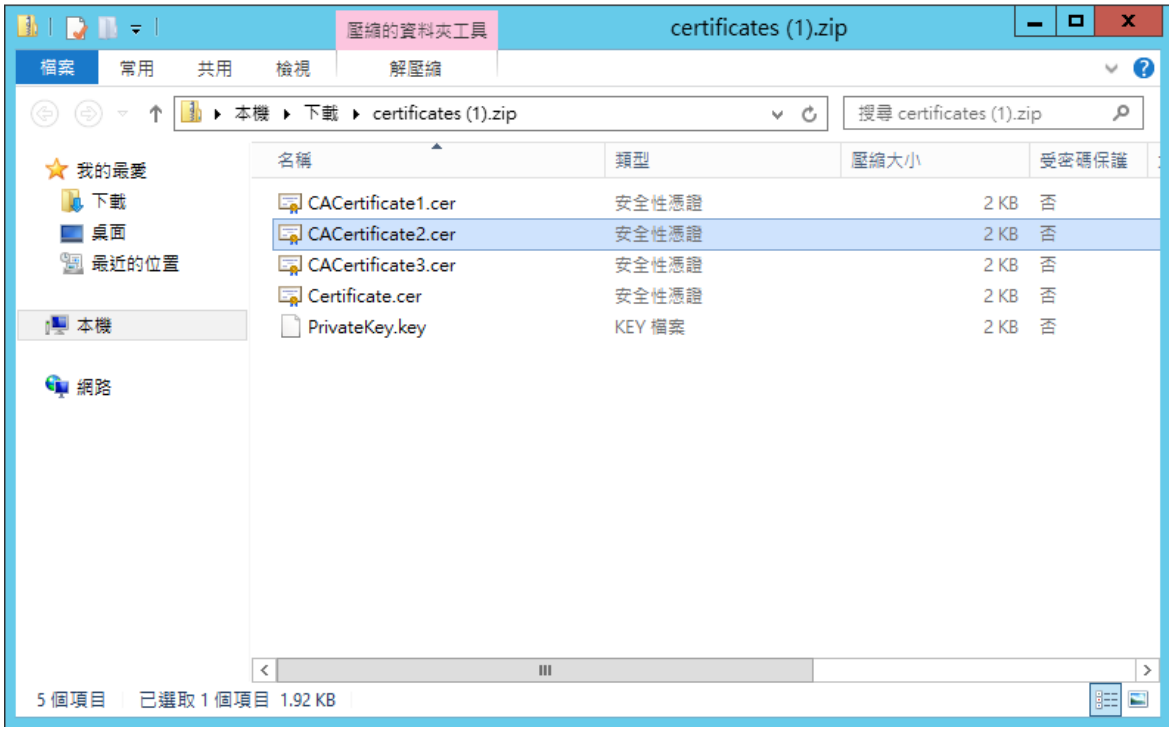
依照下圖格式，選擇現在格式為 PFX，欲轉換成 PEM，並放入 PFX 憑證檔，輸入密碼後就可以進行轉換。

注意：密碼必須輸入正確，否則會轉換失敗。

轉換完憑證後，就會將憑證下載，此時再把他解壓縮即可得到憑證。



如果依照第四章的方式使用 MMC 匯出所有憑證的話，則中繼憑證也會在裡面，只是需要逐一去查看內容才能辨示那些是中繼憑證或根憑證。因為相關憑證將被命名為 Certificate(1)、Certificate(2)……等等



依照此方法轉換的憑證檔雖然是 .cer 格式，但是副檔名已無法明確代表屬於編碼屬性了，所以請使用記事本開啟，如果是 -----BEGIN .....----- 開頭的，即是 Base 64 的 X509 編碼 (PEM 即屬此類)。就可以自由利用。

將 PEM 格式轉換成 PFX

將您的私密金鑰及取得的憑證依照下面的圖示放置憑證檔案與私密金鑰，並設定密碼，中繼憑證與根憑證不是必要檔案。但如果您有需要的話，也可以一併放入。

檔案副檔名建議為：.txt/.key/.crt/.cer

如果在您的轉換上失敗的話，請先用記事本開啟相關檔案。檢查是不是憑證 / 金鑰文件檔案的內容有空格，如果有的話，請先使用 Backspace 將其空格字元取消後存檔再行轉換。

```
 -----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDv0D0sTSaBF9zZ
oOS0haKuQxLCpGOnRvsmE5yz799vci1xNmdkaZOeEgk8df48wbiO5tY6HU5ZcqSv
sKuSMbW4ic0DsGQMrF0fMvGs+CJuQ4O9n+ojOG7Oml/Gih7AhYfKCOPRWIipNZeA
8t7At+36bfnBrYV61chy0ngPutu3L0InN/HJsqkRZOfqeCTkWn9e76omGbO5BrU6
vxhovv456x1qIkou8/oF/LvRzvLC5wdO5NAuCPweMzaS692qyXt0FIfxoFctIiXj
s6M11RAK6/I3g2Op+YC2IR2zFDMFNQL17I3q5S01YwYZX0FRsW2GcHufsO0Onwsq
51yiKW1rAgMBAAECggEBAOyecz17Ajrt6KNy9TaJhPKci64xtYIfrz7qqvt/+t5j
siK6o1mYMmcNNL/LTId2PTwC1+2PbPck/wm7MA6Xrc3facHyEUXP7DIUehFI4/AX
/azkVI1b7Tk9aLL1JWKgX1MiYmb1DCKpFkvNV6yfztgCGyTWqZVCpP1mXcBnhtM+
jPq0Kifo3rdX39kZAj51K1H15wBAx/uC+0ON3hn5E/Kc3GkaTdLd7Ubkg1wubv/e
w0K+iiQ4Zhe0JH/vouKaJy46xnAT/v0Rz0RORS+NLJ9HVQMyH4NL0U1NJaqTNoiS
qJHpg004kRmUAKBGkNUE3GfWtXa7Nzu5Jadtw64mzcECgYEA9+LhC4j0xAAfsO0t
bdJmQcHc5oXwg7CbwPHHX1qBGpEbisxySmL/yTn/kmbB3d3MqUvjwOdwBs22WGWS
016k0JvnwvUDTRWr685jy8ht0sSpatL/kFgD86r7EXN/rTcaJEuP4Soc7oZig8xX
o+P4SMtFnPXHZJL5jqxG9zc/5j0CgYEA96m3EPYkxNtW7B1GzmoQ9ryFqgrc2802
UjptEBNoTjgWzjrIY/PwpJGENCbsOcyAz9UzPVCosJZIXyicxzHuWAWtz97VKjPF
3QIpEc5moQWSOpRXmfkz5Mzzve0Smieio+3vQt1P7nvjz1O3MmWPpfaqa9VUv7jd
o18Qe4I+hMcCgYEA4U1XUo50NbYPF1NXWFpCCT1RsEjGoEjgJWkX0s7aSvTaXTkW
Hjj/Uzjc54dwZ13wZWTNZ0Jv9B79vDUETSErFVS8O91F2Mb7auI2nLxZ45ZMiwOc
tOjpHomkiOW5gg10PsxVxUPq63VDD5m1hRPpUO89IzvUrb1OCbbVAFU8Q9kCgYBi
m9JmEHtHXkXXsTh2C01B1IIr2DNj2OteBiFSm0eWjUKXT1RnZ8NS4xWOZkj8Im7P
UYYbTbg8xz19mgACV+EcbvZro7+gFAkeHDQaAOJgDoXQiSvwBIci/G+4GWKkuk9J
kf0H0tq+i9mCV1bD3Cg73mCwmroptAObGNrJMmyOFQKBgDXsOt/6vnCcQvxUgrOv
TMLnNACHMoX56jEL+50cVME1ga2qru61QxZO7ijon5KYHN0r0joLRBARv0J3t12z
i/65aZw1OFtX9RNt6bpXpet0XAIwK5/xZSh51RP1axXnNOycv80cWzAfm3T1aOtA
Igd3ZV9kOvIHUDodoGu9Dscy
-----END PRIVATE KEY-----
```

以上圖為例，在 -----BEGIN PRIVATE KEY----- 本文前面有一個空格，這個空格會導致轉換失敗。而 -----END PRIVATE KEY---- 則沒有空格，這樣的錯誤會導致轉換失敗，請特別注意。

附錄 C- 使用 OEPNSSL 工具進行 PFX 憑證格式的轉換：

在 OpenSSL 環境下，輸入以下的指令列以將 PFX 轉換成 PEM

A. 匯出檔案 (含 Key、CA 中繼憑證、CRT 憑證)
openssl pkcs12 -in < 檔案名稱 .pfx> -out < 自訂名稱 .pem> -nodes -password pass:< 自訂密碼 >
1. 用記事本打開 pem 檔案
2. 分別用記事本存成網站憑證、中繼憑證、KEY

B. 匯出檔案 (只有 CRT 憑證與 CA 中繼憑證)【多了 -nokeys 參數】
openssl pkcs12 -in < 檔案名稱 .pfx> -nokeys -out < 自訂名稱 .crt> -nodes -password pass:< 自訂密碼 >

C. 匯出檔案 (只取 Key 檔) 【多了 -nocerts 參數】
openssl pkcs12 -in < 檔案名稱 .pfx> -nocerts -out < 自訂名稱 .key> -nodes -password pass:< 自訂密碼 >

下圖為執行過程，如果覺得 PEM 不好開啟，可以輸出為 .txt 檔案
(本範例使用 Mac OSX 終端機搭配 OpenSSL Command Line 指令列執行上面的類型 A 指令)

```
OpenSSL> exit
changchiaofu@zhangqiofudeMBP ~ % clear

changchiaofu@zhangqiofudeMBP ~ % openssl
OpenSSL> pkcs12 -in ServerCert.pfx -out cert.pem -nodes -password pass:70535344
MAC verified OK
OpenSSL>
```

經輸入指印後，會產出下面的結果，再使用文字工具將 ---BEGIN.....---- 字段的內容復製，憑證及金鑰都會在該檔案裡面，請逐個複製。

```
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: {A614F1A3-8CA8-4808-89EB-0E6D19222406}
    Microsoft CSP Name: Microsoft RSA SChannel Cryptographic Provider
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQClsZk3w1ZSLt4d
P/vE5BlRDEbEYXJ5cOpUO9jAkCMcpdgCzYirkmv/uSR5r6E+xbrLyjHUwpRoE3MD
oFUIbJoAidiGCCo4IE6zTOKlYXVg38yrQKMJCNo9L98jZMPvACjQxic9dywtlBiH
iuYpNlgs+Gpvp8pAuoyjk9gLJ9Ncw8++eEH7UiEkMcig5z5pY8ZZIRqLVk7+UyNn
4mh9FpuPln2HKhlzJVRJkZ6pVblVEKoik9MiV3Z9n4HEZKpBTu8KIKCk9OUR+EIu
AC1GasR64ZYGB2SB+eZIp++6MQe90nhaCEBt8aWrU75ZdiUYvgtAQoNU2hFj2KkG
qtSZflgPAgMBAAECggEADhOnjVBAHioZkelkrcm/L0Tx7vv+A++iFaPvLageA4oN
1WpTlfGSBIWP+4wxqinJGkhd5J7fVq3VwKId3a7BHd7+kTlSW1BYJbpLd+EIXg5f
AqTMyEpQC2pTJ8IHNcZESwn6o9zJcqamHqw6TGTWJ7cdiJZ8HVtIvxqJYtejiLoX
qh5PNlZf6AjuU5fNOl1yIa+wBcX79z47hO1W6zPoL9N4p/aCLir33AigwA/729EM
0codIyMH1gjjlmuqXcCCL14fH1ZN24vvpCTdN1p8GHhyR5ilKJjkf5NeivJg8oOl
QPL2EX5lwjaxg4KaUD0JBhSJrk5eqjrjX1QuQ9uLmQKBqQDiqEX0HszY34oWUMtz
eT7pmhKTfytM2tLDya86BpqlqTS3u9gctMWGnlCd5HzywHyNoSNimHhT56GRp0pg
NHqU7sYKiq0huTOFNvfzGNDL85TZDq5Jh7Kv7xoDY4EkMa4qCtIFC/ulDket1Q6c
1R93mc3DDsNGYdjYFMqc7iwqAwKBgQC7JOku0ICeOGLgoEoZ+hcjR9xcHB9OE2ZZ
7+UBqopC0QfhIa3T4izzId2baM9KEfUWf72292KUhJ2OczDRxQWkkgUW6DLm0lFo
E1LCsB78He2z2ezYmdS68KDCqtbiNbPHeP8fAuR2trgeuXVskGpVQ8TZAh79OcjA
hT1XycSCBQKBgQC6TrNhnMepJQYuva7edjU+c4T9dLS08dH5WYztgOwxSul4dZGI
1xbeNtfxUVVbfNlk2aVqcAXIqkeQoEJEnh58uWBUXXG53K/6ulpJmoZWfxxE5wpq
Koi4kQOC8ZG/nI6axFYqC9WHsRs+Sjk+tPiuqOA3i7T774X85+o74JKw3QKBgQCh
VHuU+Pe37iIHRQc8h6VEq+Fione2RfEZHT6Nhig024TaRr9khnl7i7lQDTWNxBdF
sw+oWHFqWTy+Hb17SMMzcRHkIn4nEC5Pi0DwRwYfD+nn/rk4LLz//wqHRGXckrEO
B9ffMw4i7PeivPxmf8S6/5B+B18Rq6vNk89DC9RUxQKBgQDKJWWHALs7ZIDCmKjw
iHCndcUGauojhsTMMgvHB7aDn7lT6u6dQZdvQaL+qgwNptzJc+shd9exWarNeWfF
d5o2pWtezViVk+N0W9bRxo3IrVF2H0T+keGNbxsDfuJs24FviNbFaQSlpaNu/fam
s9zh/K7gDQM3czws1j3vKZ5BmA==
-----END PRIVATE KEY-----
Bag Attributes
    1.3.6.1.4.1.311.17.3.75: 00 00
    localKeyID: 01 00 00 00
    1.3.6.1.4.1.311.17.3.20: F8 26 BA 26 71 56 92 69 2A 65 2B A9 A6 91 11 78 EC 41 19 2A
    friendlyName: ssl.net-chinese.tw
subject=/CN=ssl.net-chinese.tw
issuer=/C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain
Validation Secure Server CA
-----BEGIN CERTIFICATE-----
```

上圖的輸出結果，在 Linux 的指令列也可以使用。 Windows 版本要使用 OPEN SSL 的話，由於 OpenSSL 官方並沒有提供 Windows 版本的安裝包，可以選擇其他開源平臺提供的工具。例如 :https://slproweb.com/products/Win32OpenSSL.html

使用 OEPNSSL 工具將 PEM 格式轉換成 PFX

1. 準備好憑證與 KEY(.crt 與 .key) 在工作路徑之下
2. 進行合併，輸入指令碼如下
   openssl pkcs12 -export -in < 憑證絕對路徑 \ 憑證檔案 > -inkey < 私鑰絕對路徑 \ 私鑰檔案 > -out < 自訂名稱 .pfx> -certfile < 中繼與根憑證絕對路徑 \ 中繼憑證或根憑證 > -password pass:< 自定密碼 > (若在 openssl 環境下可以不打 openssl 敘述句)

參數說明：

- pkcs12 -export：將憑證匯出成 pkcs12 編碼格式的 PFX 憑證檔
- -in < 憑證檔案 >：將網站憑證放入
- -inkey < 私鑰檔案 >：將金鑰憑證放入
- -out < 自訂名稱 .pfx>：轉換後產出的 pfx 名稱
- -certfile < 中繼與根憑證 >：合併入中繼憑證 (若不加可省略)
- -password pass:< 自定密碼 >：為設定匯入之密碼，Windows IIS 通常會要求。 (若不加可省略)

下圖為執行過程，如果覺得 PEM 不好開啟，可以輸出為 .txt 檔案
(本範例使用 Mac OSX 終端機搭配 OpenSSL Command Line 指令列執行上面的類型 A 指令)

```
changchiaofu@zhangqiofudeMBP ~ % openssl
OpenSSL> pkcs12 -export -in ssl_net-chinese_tw.crt -inkey PrivateKey.key -out IIS
Cert.pfx -certfile My_CA_Bundle.crt -password pass:70535344
OpenSSL>
```

如果您的 Windows 有安裝開源平台的 OpenSSL for Windows 的話，則請用命令提示字元完成上述的工作就可以轉換。