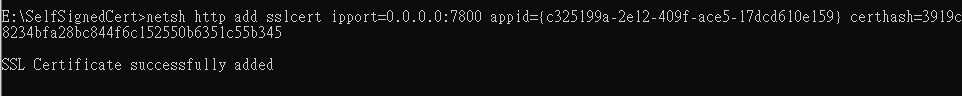
* 1. 快速部屬至伺服器(需已經產生憑證)
     + - 1. 複製預先產生好的憑證檔案Server.pfx至欲安裝的伺服器
         2. 用系統管理員身分執行httpCertSet.bat [PASSWORD]



**以下各節為原理說明，如何產生快速佈署的憑證與commands**

* 1. 產生自簽憑證
     1. 使用 Git 內建的 OpenSSL 工具

當安裝好 Git for Windows 的時候，其實就已經內建了 OpenSSL 工具，預設執行檔路徑為 C:\Program Files\Git\usr\bin\openssl.exe，你可以將 C:\Program Files\Git\usr\bin 路徑加入到 PATH 環境變數之中，以後就可以直接輸入 openssl 來執行此工具。

* + 1. 憑證產生設定檔 ssl.conf

[req]

prompt = no

default\_md = sha256

default\_bits = 2048

distinguished\_name = dn

x509\_extensions = v3\_req

[dn]

C = TW

ST = Taiwan

L = Hsinchu

O = AnaSystem

OU = Research Department

emailAddress = richard@anasystem.com.tw

CN = MobilePumpSystemWebAPi

[v3\_req]

subjectAltName = @alt\_names

[alt\_names]

DNS.1 = anasystem.com.tw

* + 1. 產生憑證命令
       1. 產生 .cer .eky .pfx

openssl req -x509 -new -nodes -sha256 -utf8 -days 10000 -newkey rsa:2048 -keyout server.key -out server.cer -config ssl.conf

openssl pkcs12 -export -in server.cer -inkey server.key -out server.pfx

產生過程會要求輸入private key密碼，此密碼不可忘記，在合併與匯入憑證時需要。

* + - 1. 合併 .cer 即 .pfx

certutil -MergePFX server.cer server.pfx

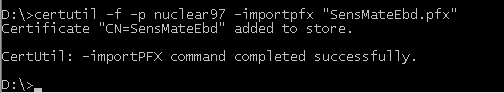
pvk2pfx -pvk server.pvk -spc server.cer -out server.pfx

執行完畢後會產生合併成功的 server.pfx

* 1. 匯入憑證至目標伺服器
     1. 方法一，使用Command line匯入
        + 1. 將上節產生的cer檔案複製到XPAC
          2. 在cer檔案所在目錄下，執行以下命令

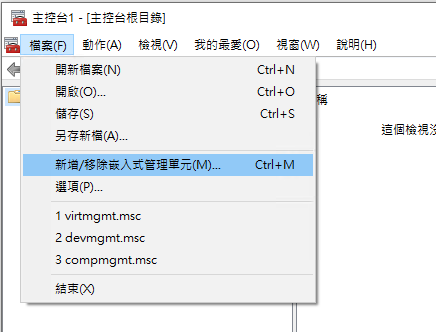
certutil -f -p PASSWORD -importpfx "Server.pfx"

執行完畢後如果出現

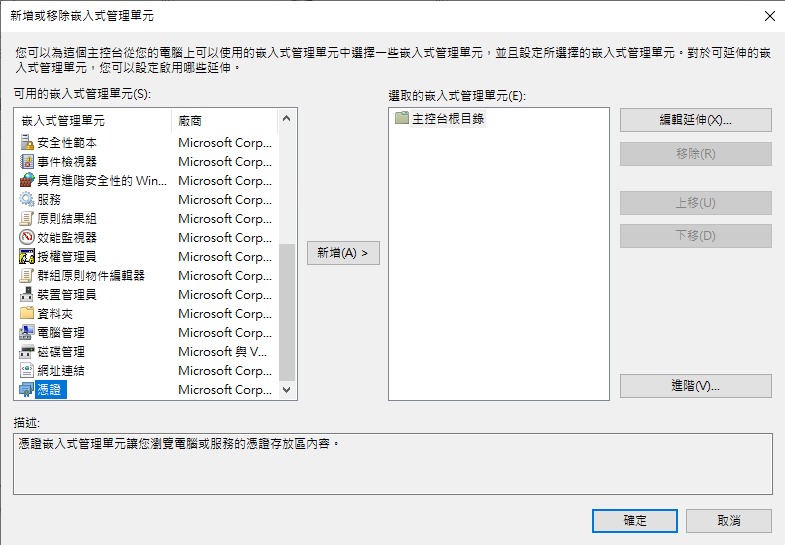


即代表匯入成功，若要查看匯入的憑證，可以依照2.2所述步驟，但跳過匯入憑證步驟，至最後一步

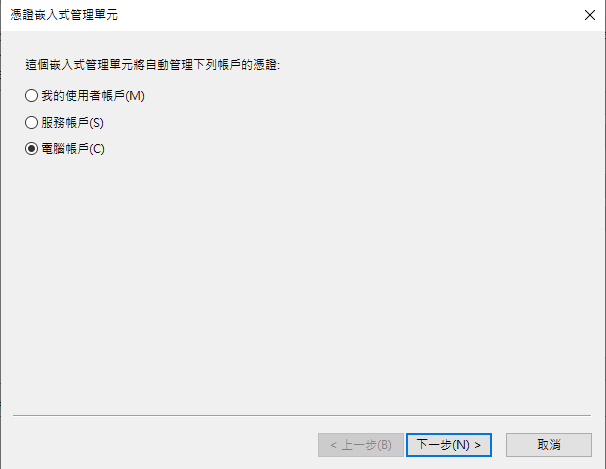
* + 1. 方法二，使用憑證主控台匯入
       1. 建立「本機電腦憑證管理主控台」
          1. 按下window key + r，輸入 mmc
          2. 選擇 檔案 🡪 新增/移除嵌入式管理單元



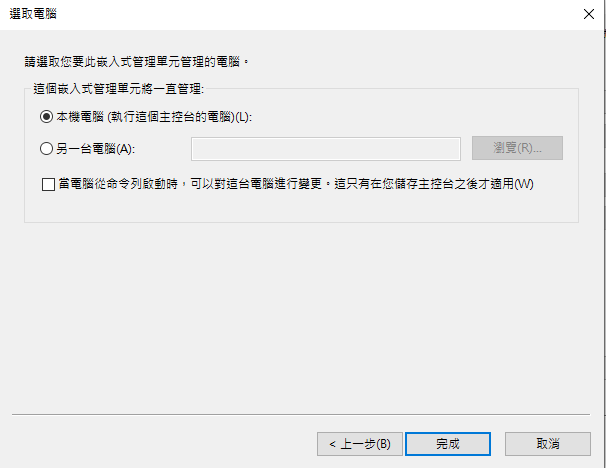
* + - * 1. 選擇憑證 新增(A)



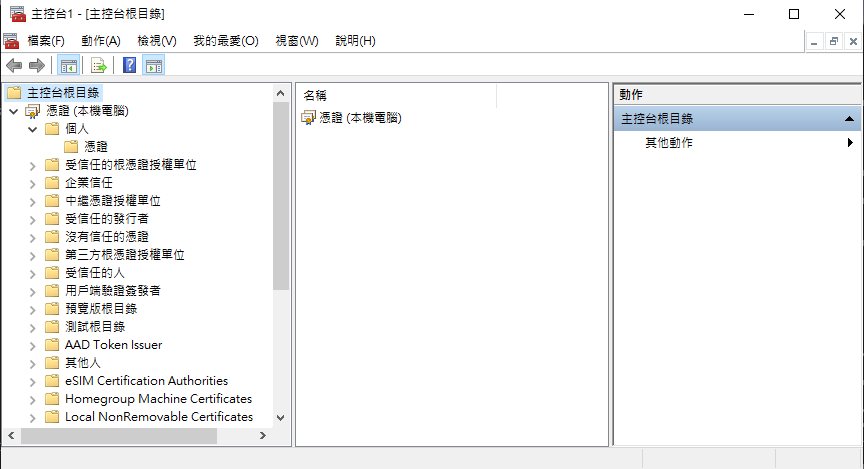
* + - * 1. 選擇電腦帳戶



* + - * 1. 選擇本機電腦

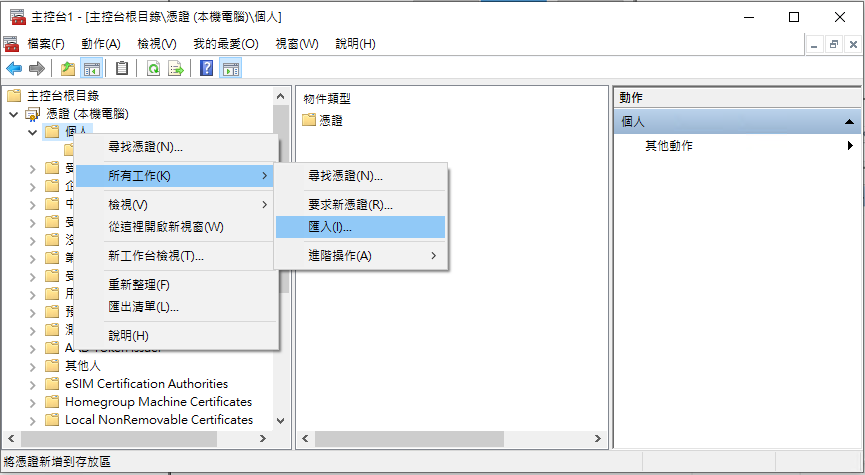


完成後會顯示畫面如下

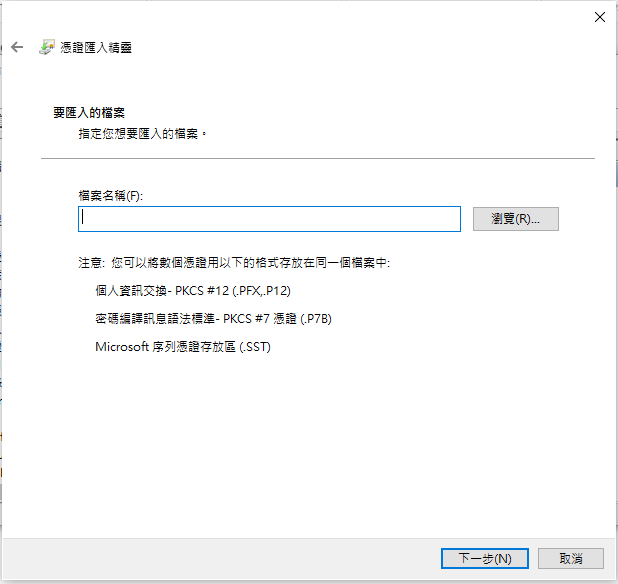


完成後可將此主控台設定儲存起來，放在桌面，以後操作憑證就不用重複建立憑證管理主控台。

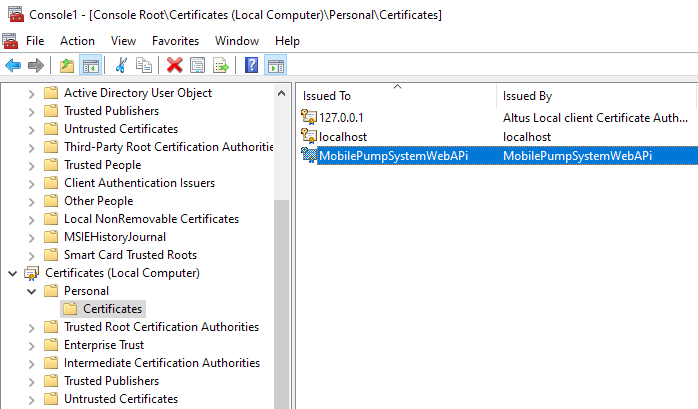
* + - 1. 匯入憑證
         1. 在「個人」按右鍵，選所有工作🡪匯入



* + - * 1. 選擇cer檔案所在位置匯入

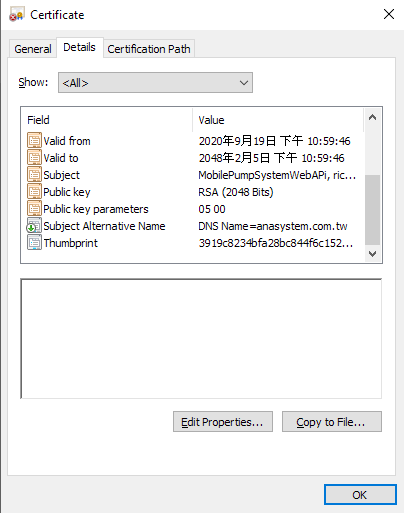


* + - * 1. 匯入成功後，會在憑證目錄下看到此憑證



* 1. 建立https通道
     1. 取得憑證指紋

點選憑證檔案，按下右鍵選擇開啟，切換至詳細資料，並點選憑證指紋



複製憑證指紋，並去掉所有空白，以本憑證為例，為

3919c8234bfa28bc844f6c152550b6351c55b345

* + 1. 建立通道

在啟用Https服務電腦的控制台(管理員權限模式)，執行

netsh http add sslcert ipport=0.0.0.0:[port] appid={[app guid]}

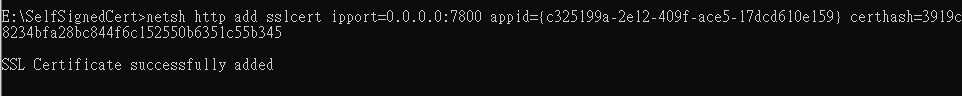
certhash=[憑證指紋]

其中{port}為SensMateEbd的https port，設定為7800，app guid可任意產生，不同台伺服器可以相同。

**範例**

netsh http add sslcert ipport=0.0.0.0:7800 appid={26333edb-6011-494d-80c5-61a9abe090bd}   
certhash=1 3919c8234bfa28bc844f6c152550b6351c55b345

成功之後會出現



* + 1. 刪除通道

若操作錯誤需刪除通道，可使用以下命令刪除

netsh http delete sslcert ipport=0.0.0.0:7800