政府憑證管理中心（GCA）

SSL 憑證重新設定 5 層串鍊說明

目錄

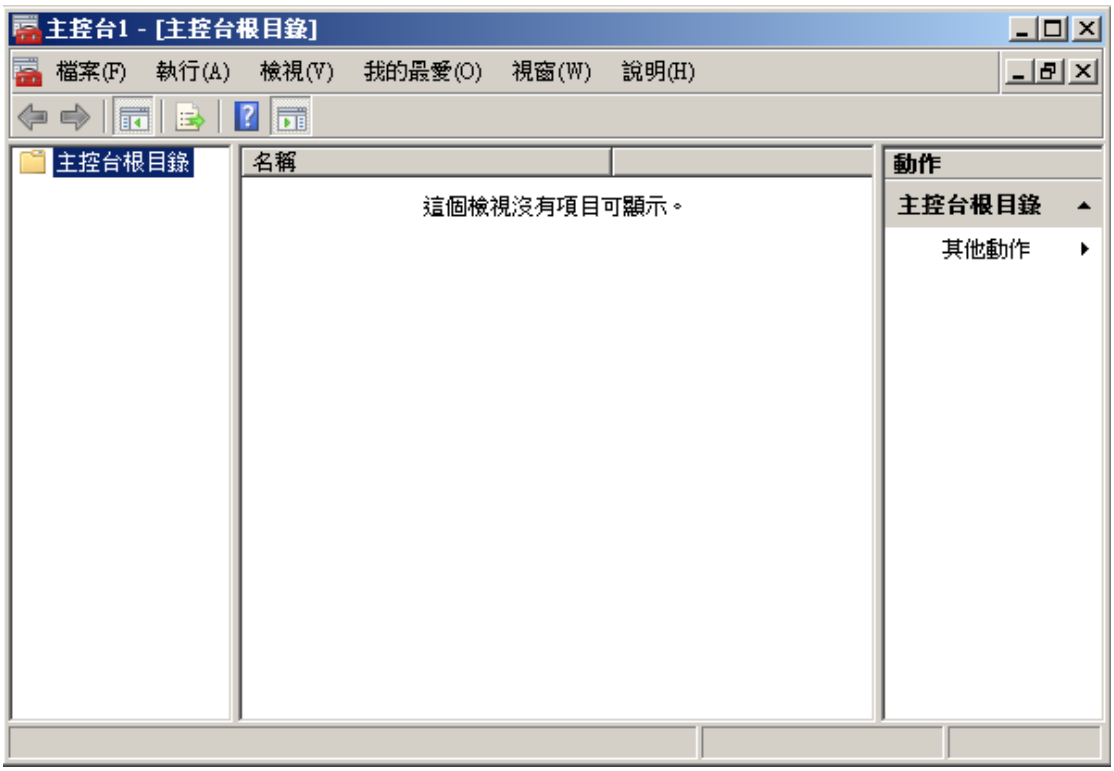
前言

本說明是針對先前已經安裝過GCA SSL憑證串鍊的網站伺服器參考操作使用，若您的網站伺服器為第一次安裝 GCA SSL 憑證，請直接參考安裝手冊即可。

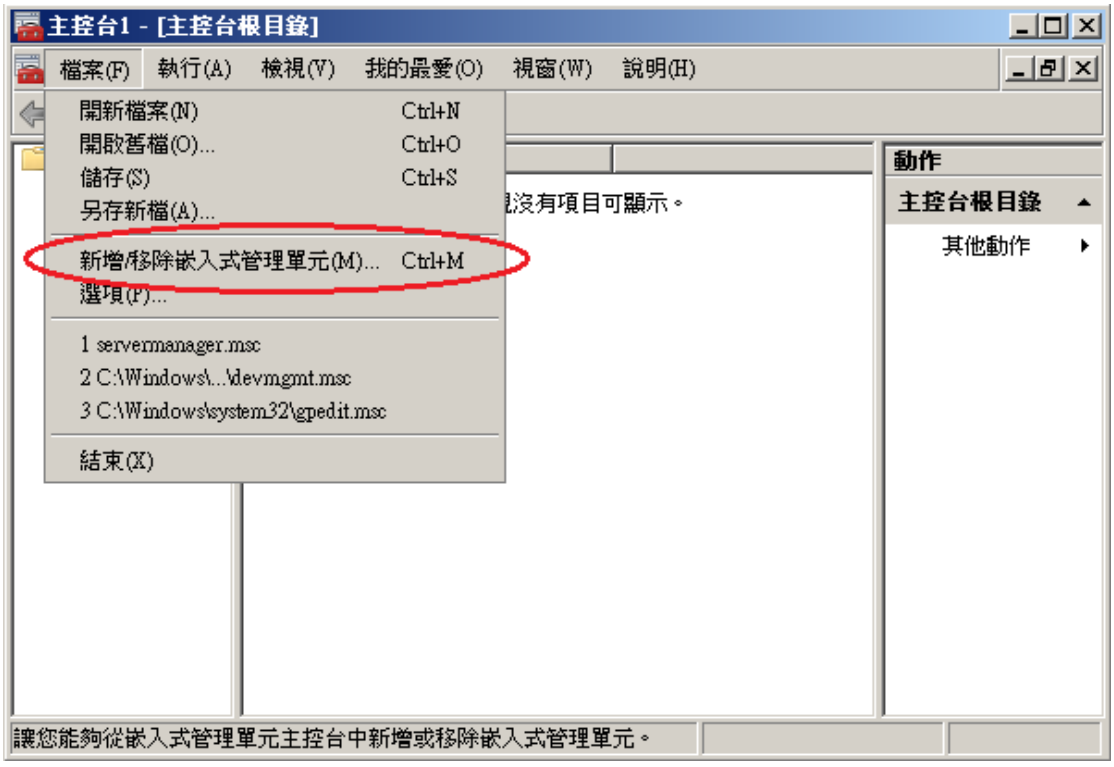
本說明提到之5層串鍊為GRCA1 -> GRCA1_to_GRCA1_5 -> GRCA1_5_to_GRCA2 -> GCA2 -> SSL，其中 GRCA1 為根憑證，針對根憑證的部分，瀏覽器會自行參考自己的憑證信賴清單決定是否信任，因此根憑證並不是 SSL 必須傳送的項目，故會因為不同的檢測網站或軟體而有顯示與不顯示根憑證的差異，所以若檢測結果只出現4層串鍊亦為正常現象，只要 Firefox 與 Android 平台能正常連線網站即為正常。

Windows IIS7

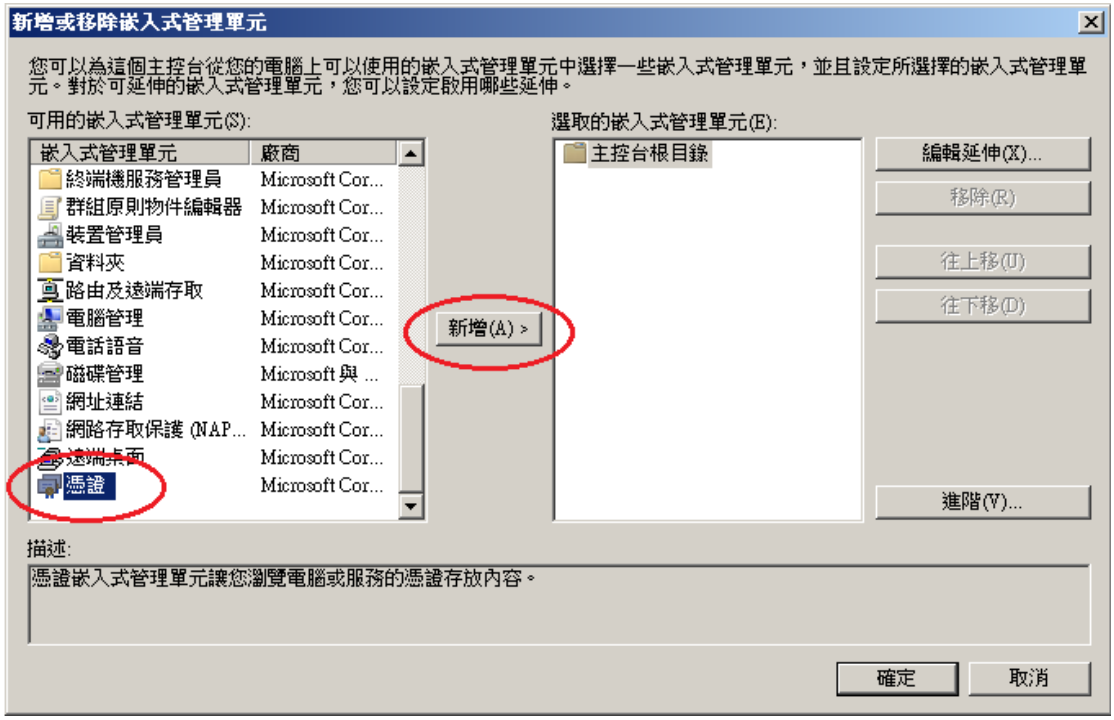
一、請先點選「開始」→輸入「mmc」→按下「Enter」。



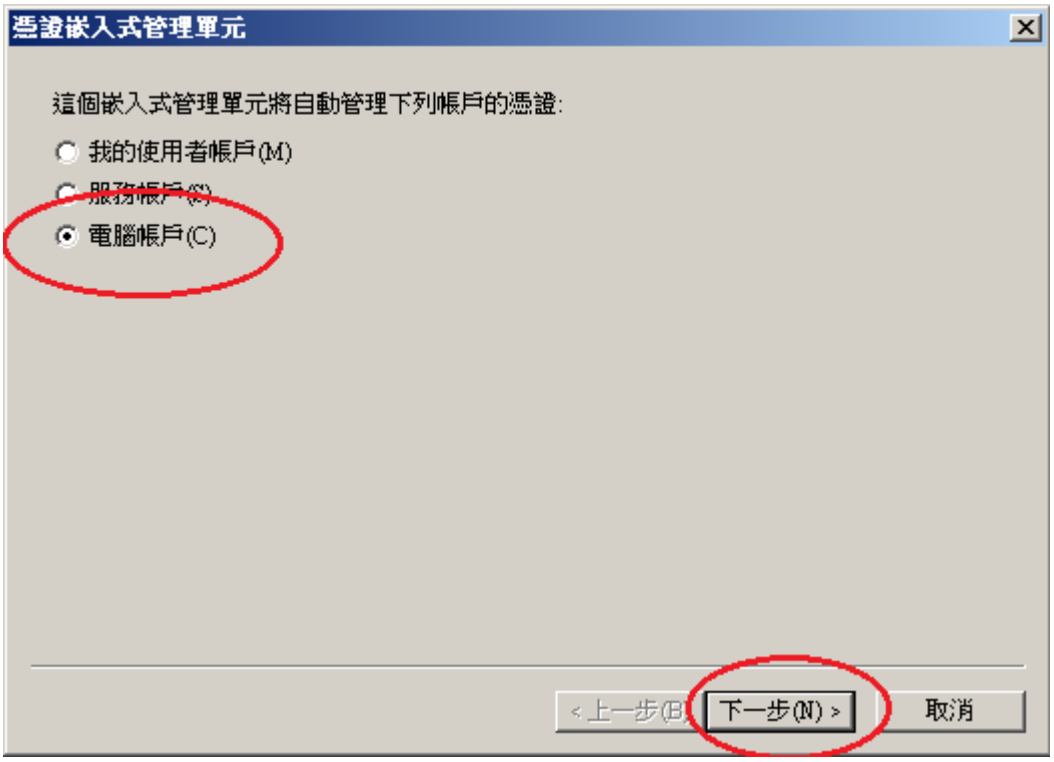
二、選擇「新增/移除嵌入式管理單元」。

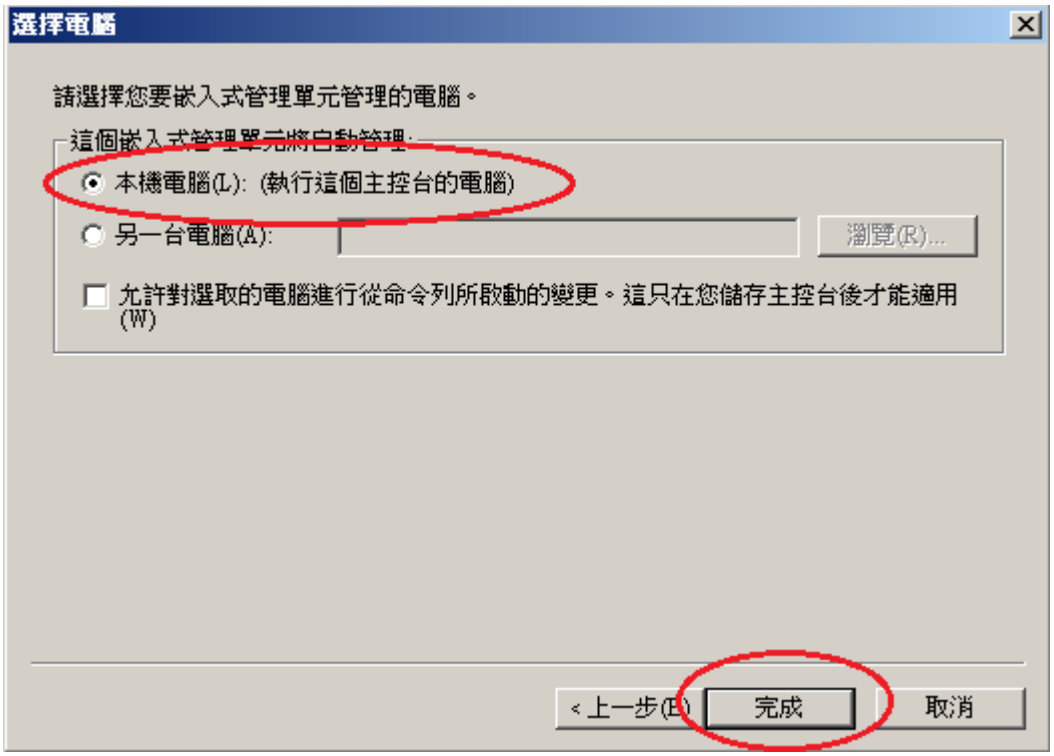


三、接著點選「憑證」→「新增」。

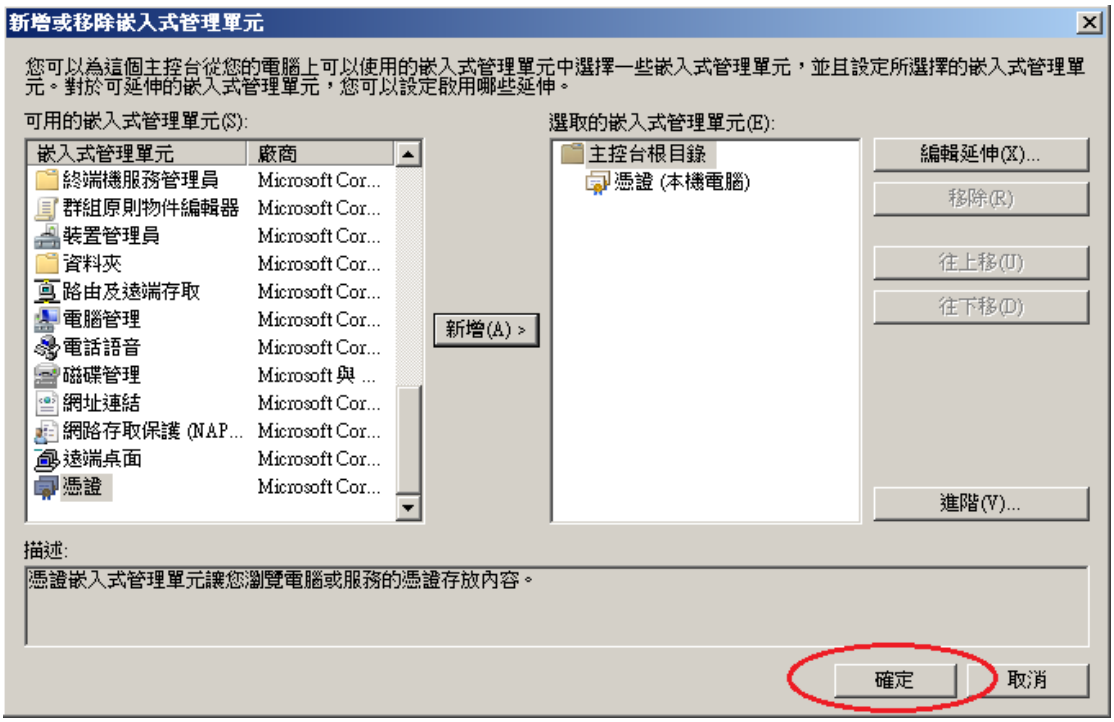


選擇「電腦帳戶」→「下一步」→「完成」。



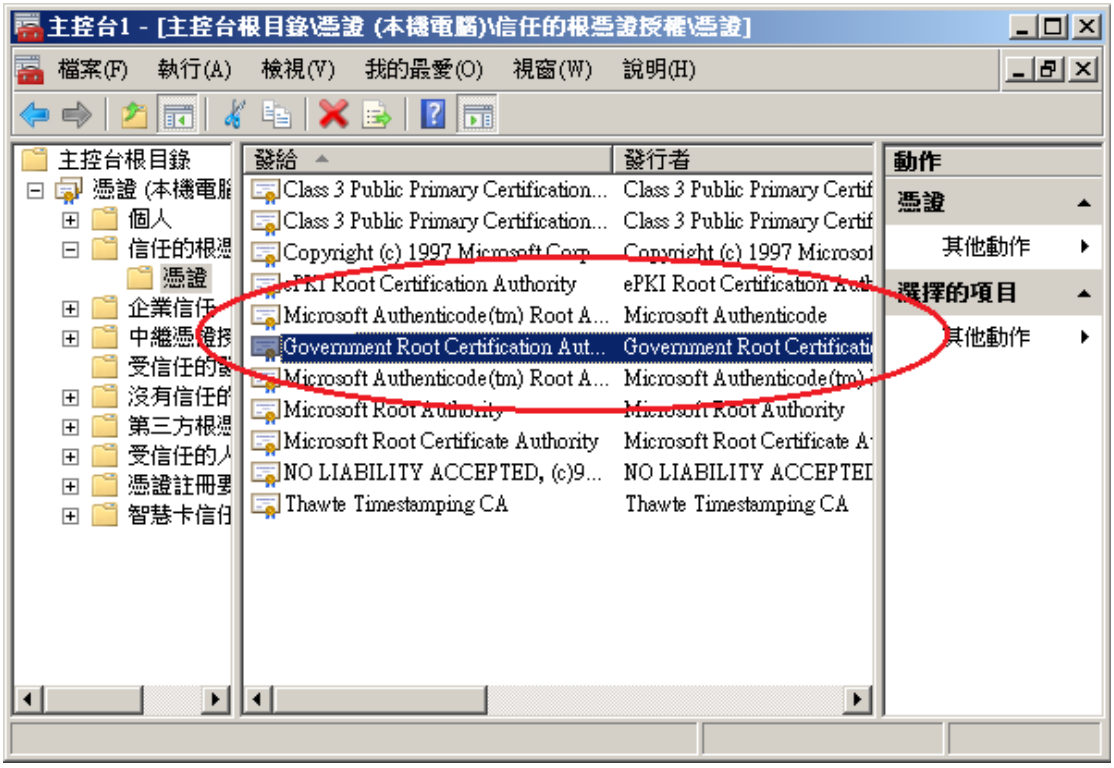


最後按下「確定」。



四、刪除已經無用之 GRCA2 憑證

檢查信賴的根憑證中是否有 GRCA2 的憑證(到期日為 2037/12/31)，若有請刪除

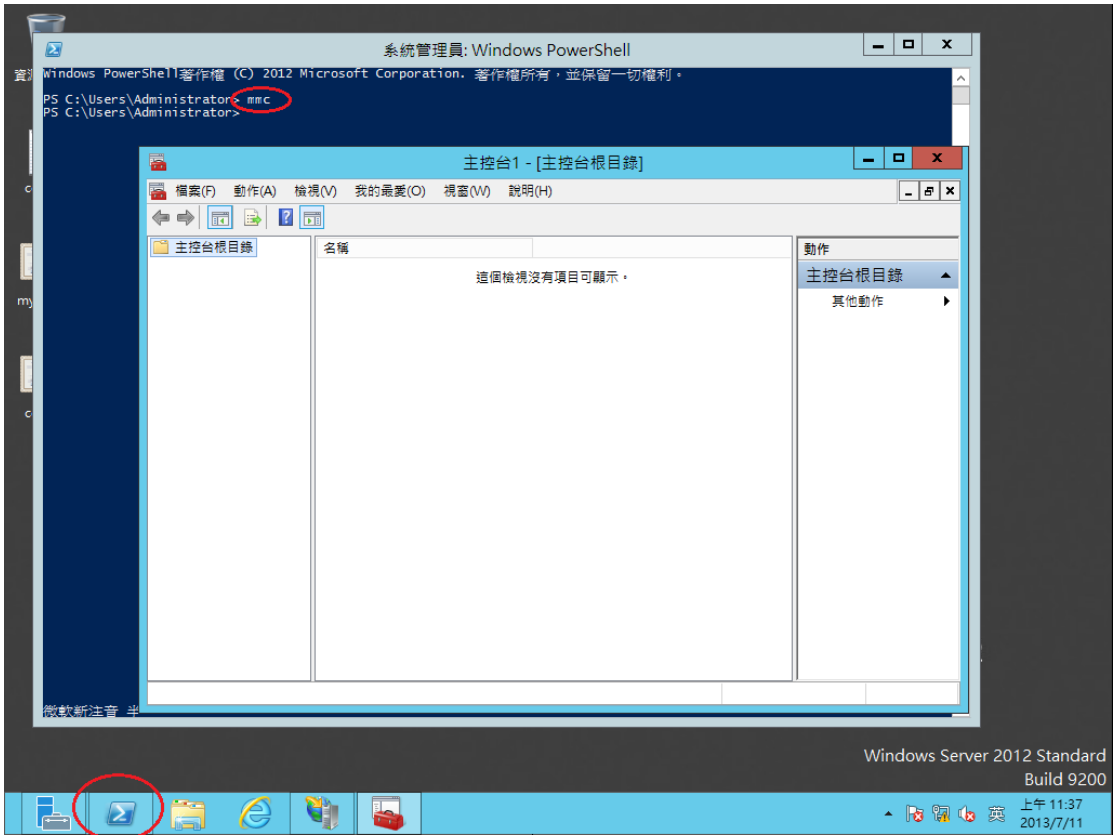


五、後續請參考安裝手冊將 2 張自發憑證匯入中繼憑證授權單位中

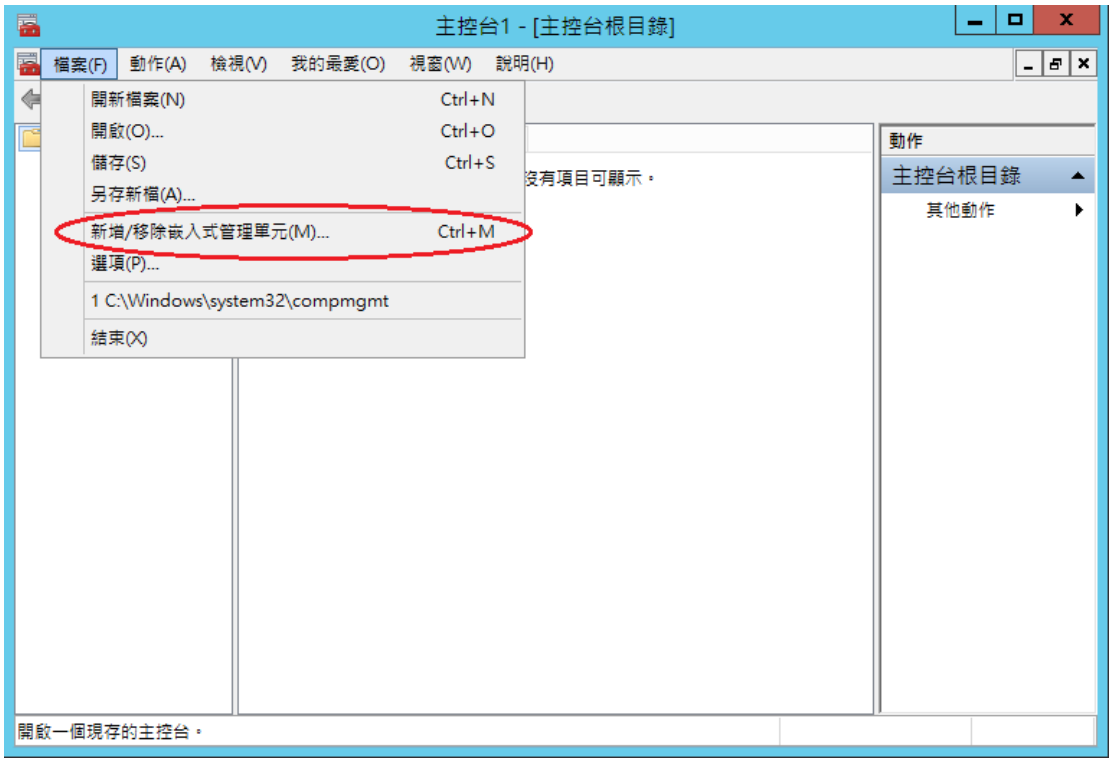
六、請參考安裝手冊重新繫結(Binding)一次後重開機

Windows IIS 8.0

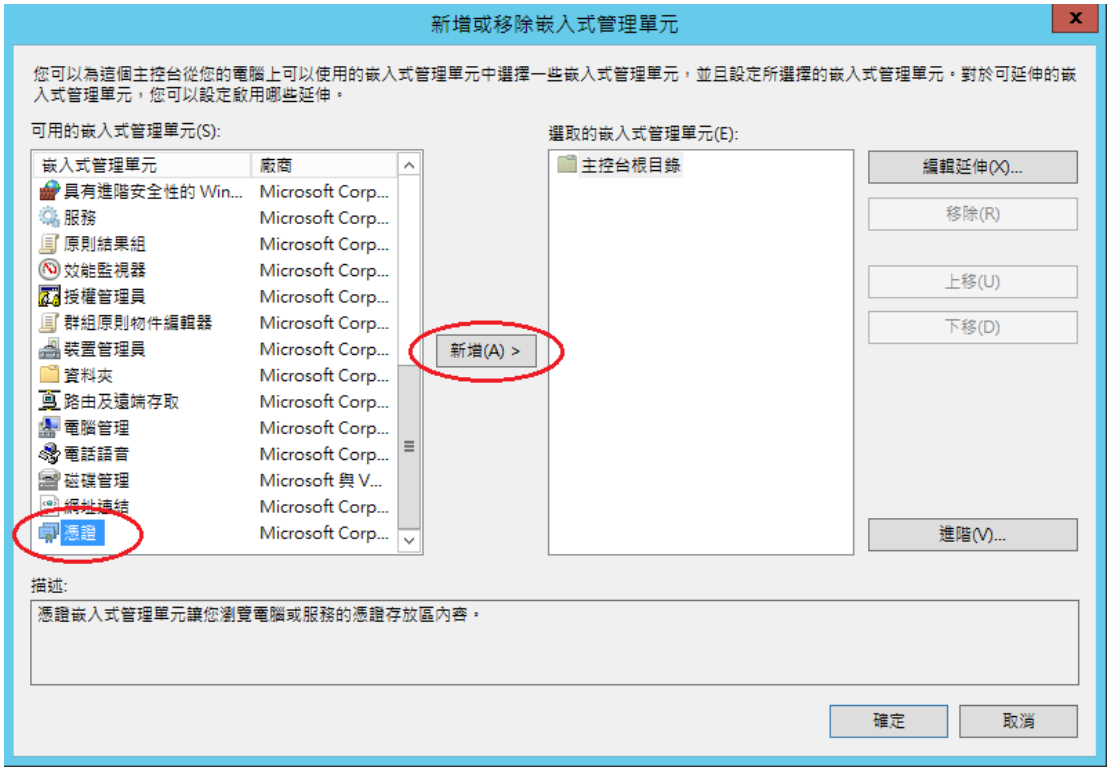
一、　請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。



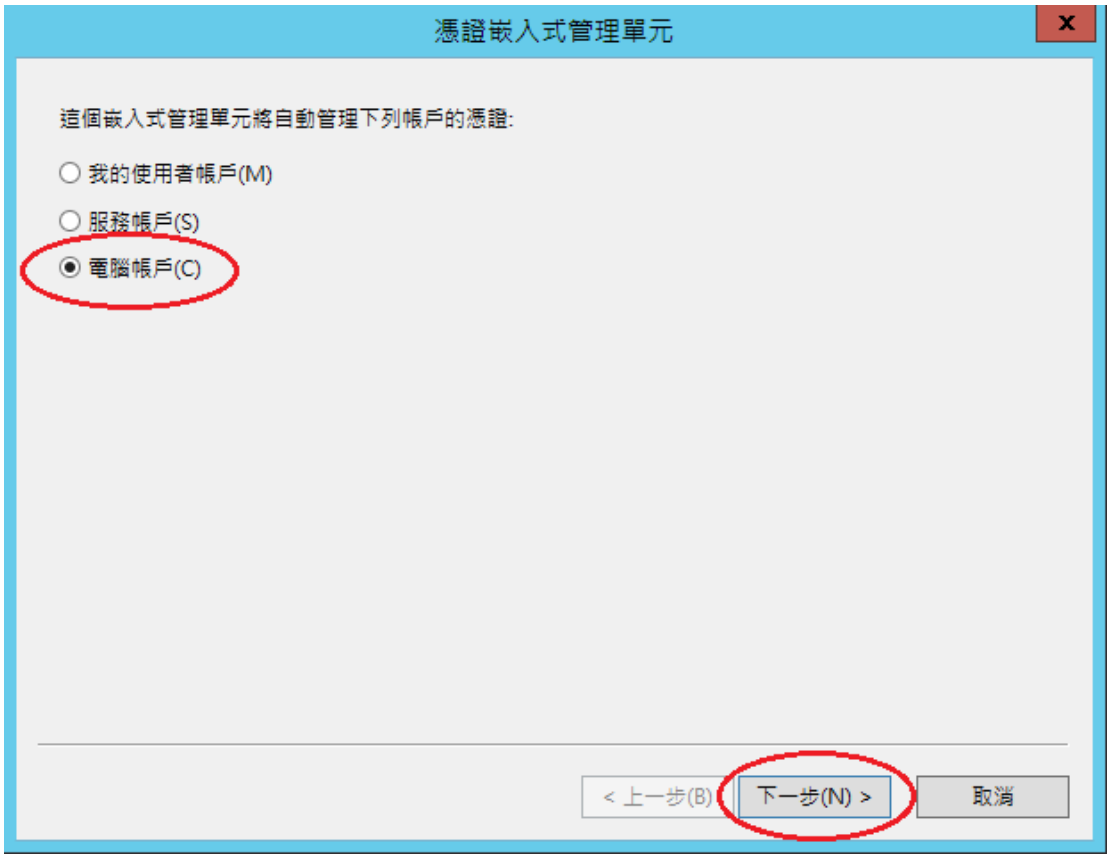
二、　選擇「新增/移除嵌入式管理單元」。

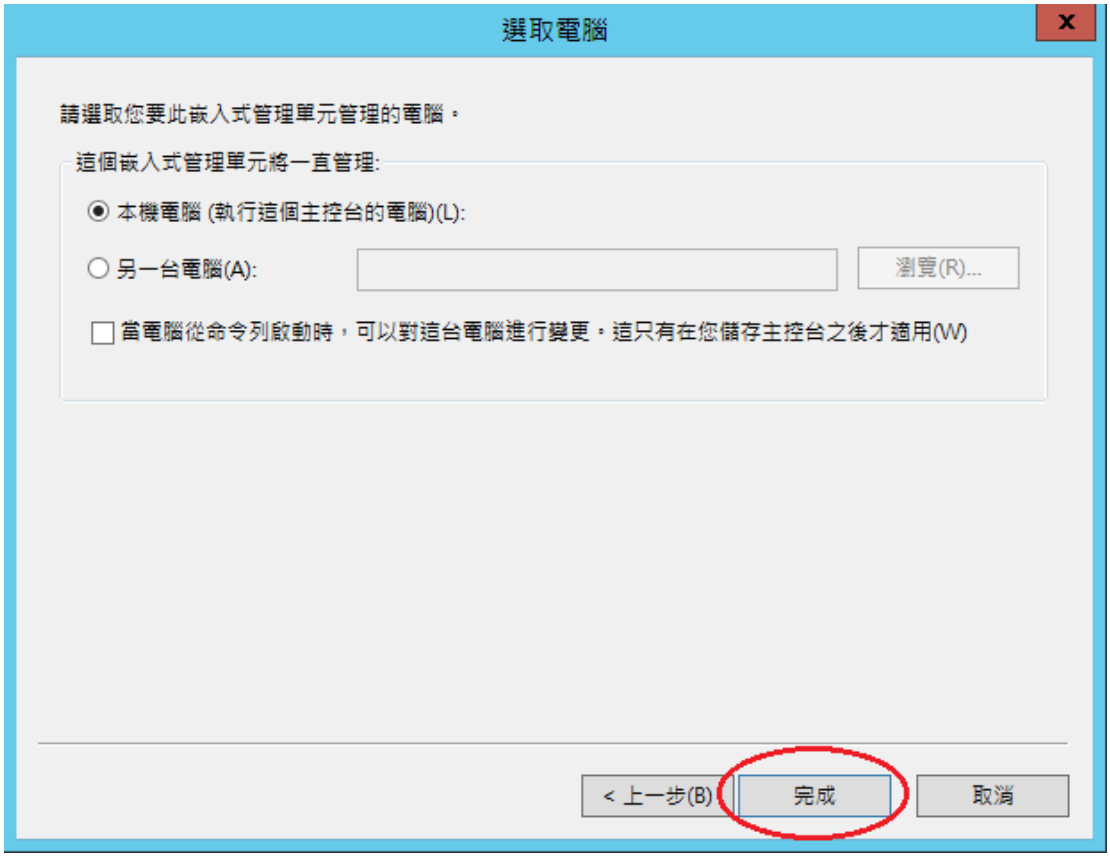


三、 接著點選「憑證」→「新增」。

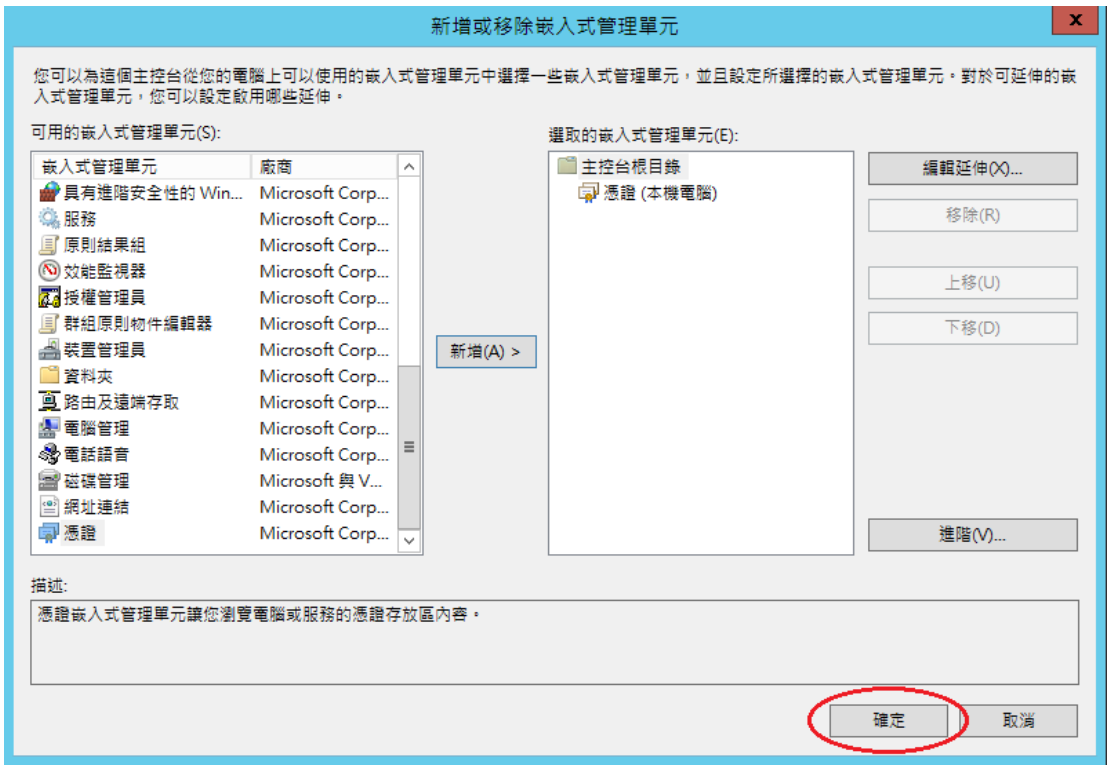


選擇「電腦帳戶」→「下一步」→「完成」。

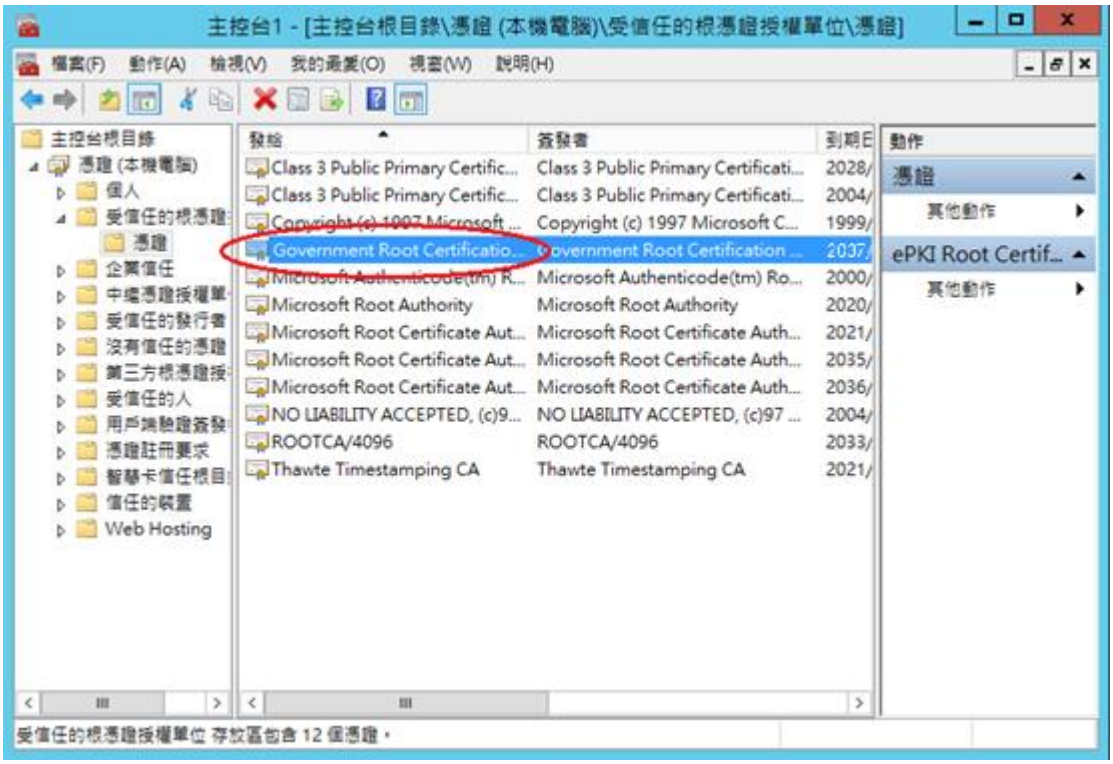

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


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

最後按下「確定」。



四、檢查信賴的根憑證中是否有 GRCA2 的憑證(到期日為 2037/12/31)，若有請刪除



五、 後續請參考安裝手冊將 2 張自發憑證匯入中繼憑證授權單位中

六、 請參考安裝手冊重新繫結(Binding)一次後重開機

Linux Apache

一、參考安裝手冊先取得 GRCA1_5_GCA2.crt

二、利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為
<apache 安裝路徑>\conf\extra\ 目錄下。
修改以下參數並存檔
SSLCertificateChainFile：GRCA1_5_GCA2.crt 檔案路徑

Tomcat

一、打斷原本 keystore 中之憑證串鍊，詳細步驟請參考說明會投影片附錄之內容
http://grca.nat.gov.tw/download/gpki_training2017/GPKI_Training.pdf
二、請參考安裝手冊，依照手冊步驟重新匯入手冊上提到的憑證