政府憑證管理中心（GCA）

SSL 憑證串鍊設定說明

國家發展委員會

中華民國 106 年 8 月

目錄

一、前言

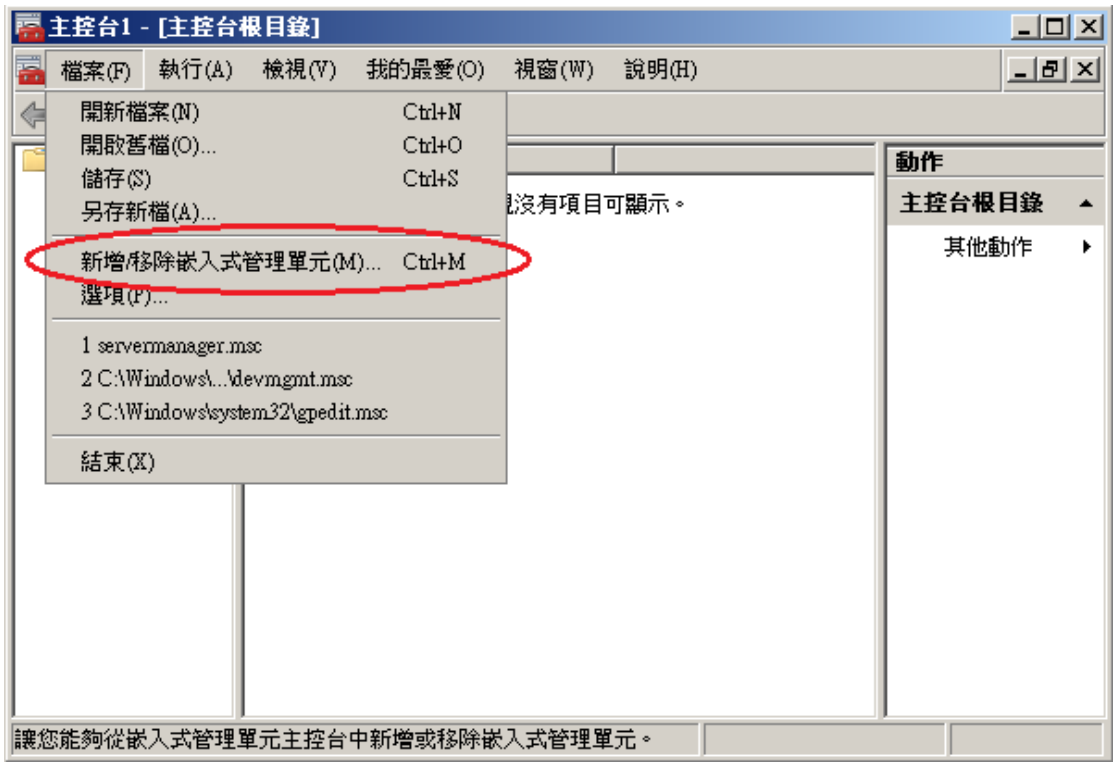
- 本本文件係針對機關網站已導入 HTTPS 機制(先前已安裝過 GCA SSL 憑證)的網站伺服器參考操作使用，請依照貴機關網路伺服器版本執行安裝設定。
- 若貴機關網站尚未導入 HTTPS 機制，則不須重新安裝設定。

二、安裝方式

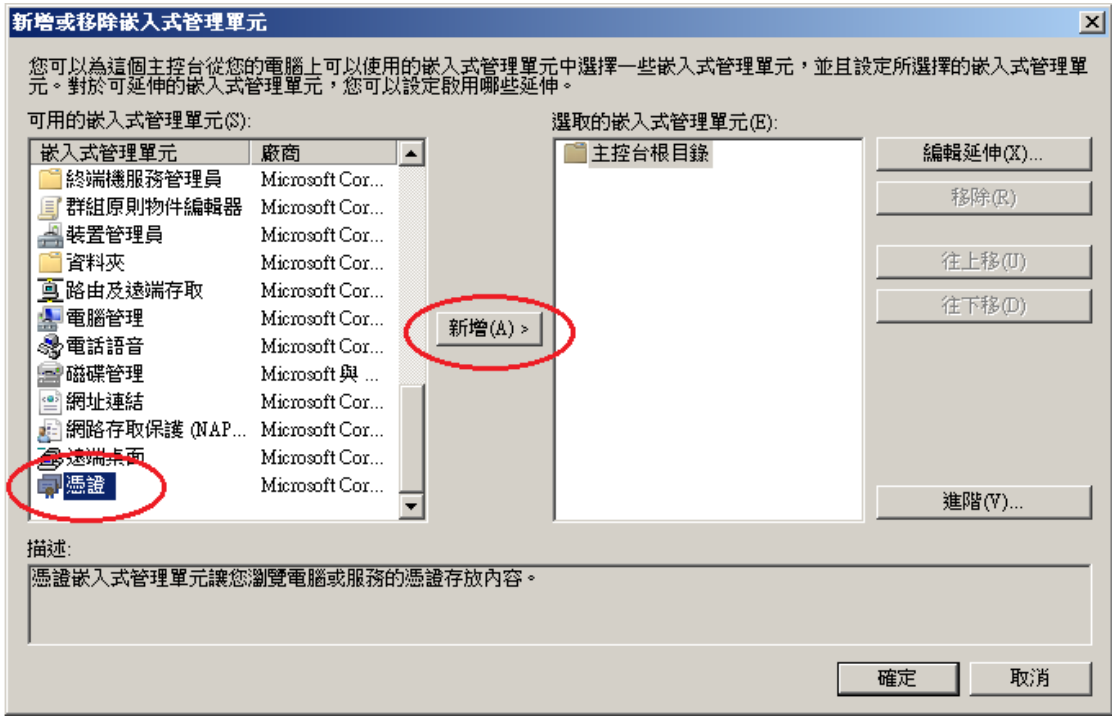
(一)網站伺服器：Windows IIS 7

1. 請先點選「開始」→輸入「mmc」→按下「Enter」。

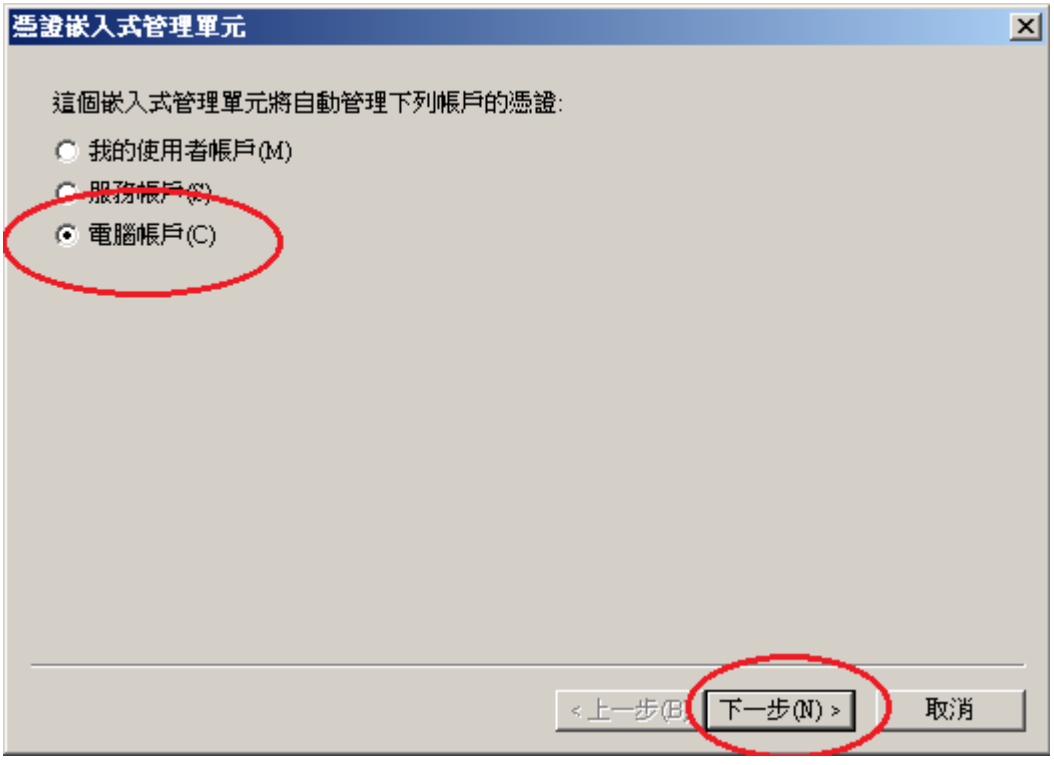
2. 選擇「新增/移除嵌入式管理單元」。

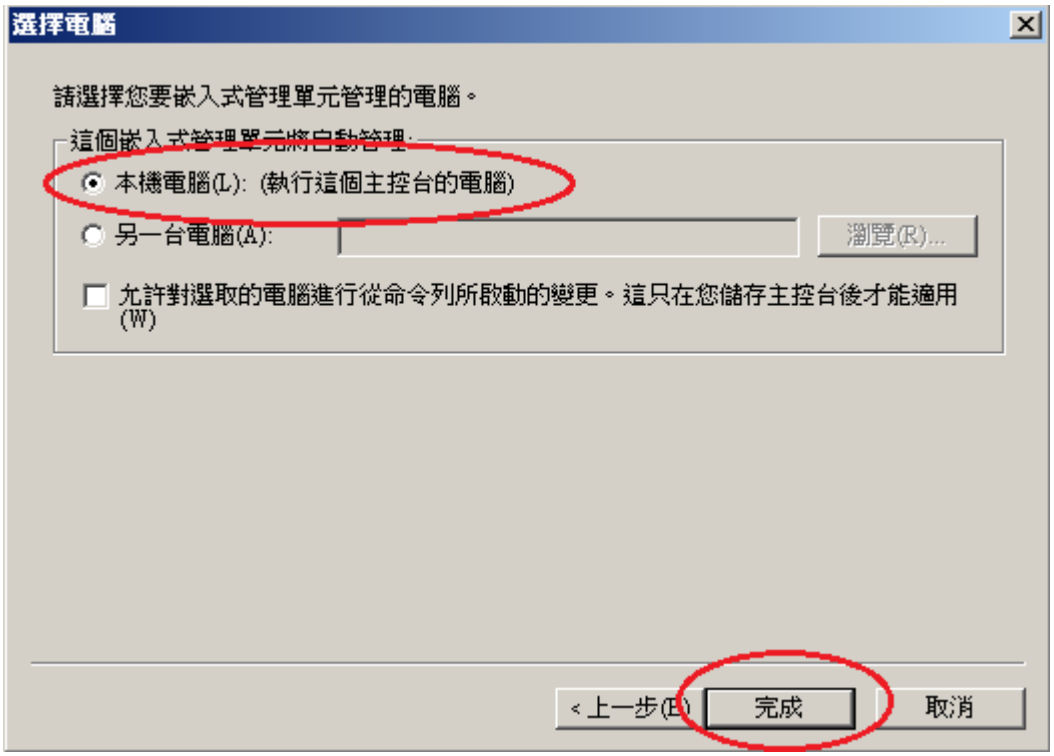


3. 接著點選「憑證」→「新增」。

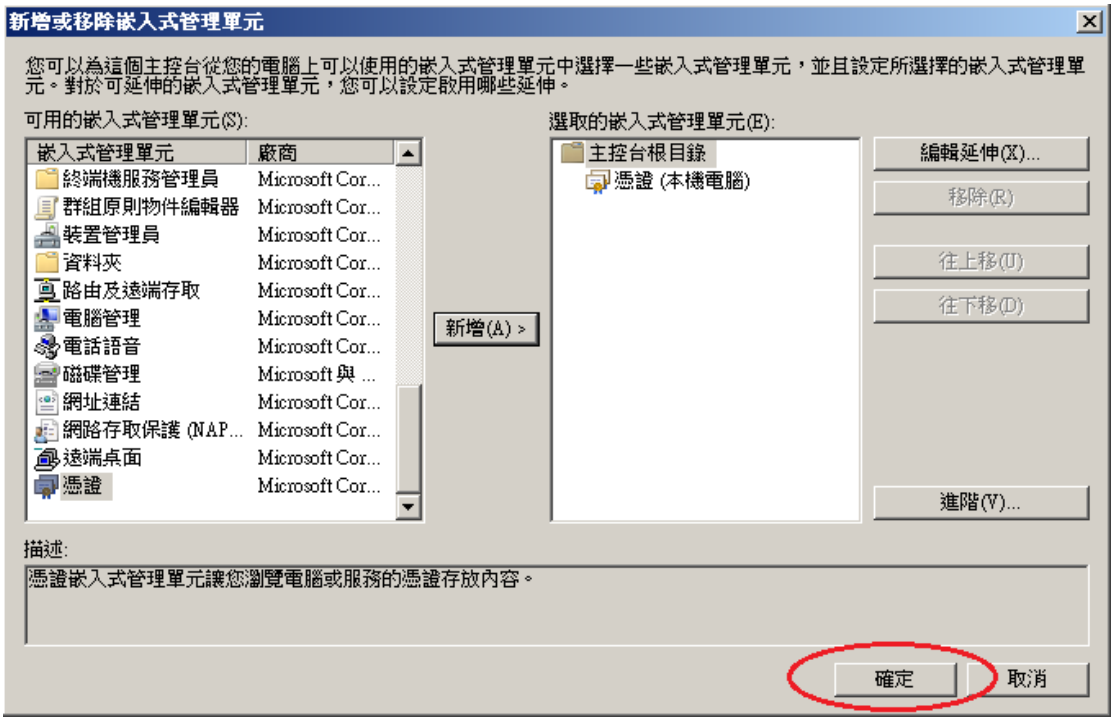


選擇「電腦帳戶」→「下一步」→「完成」。





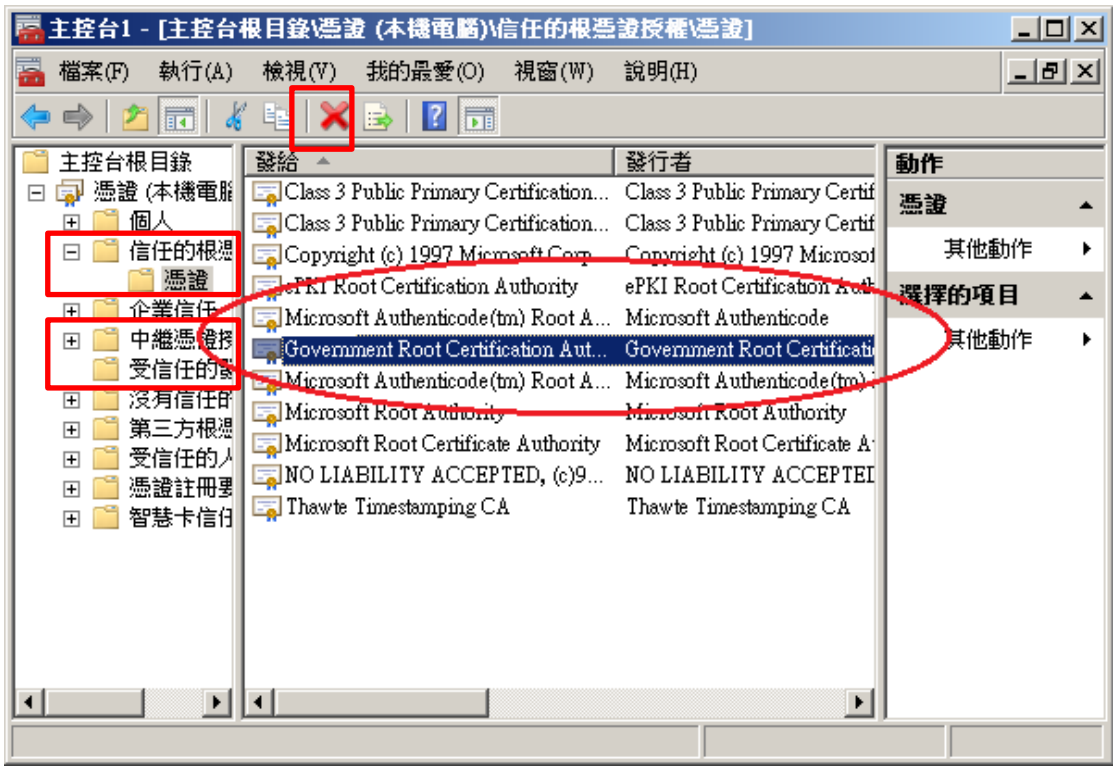
最後按下「確定」。



4. 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。



5. 檢查中繼憑證授權單位中是否有 GRCA 的自發憑證(到期日為 2032/12/5)，若有請刪除。

6. 請至下列網址下載 2 張自發憑證

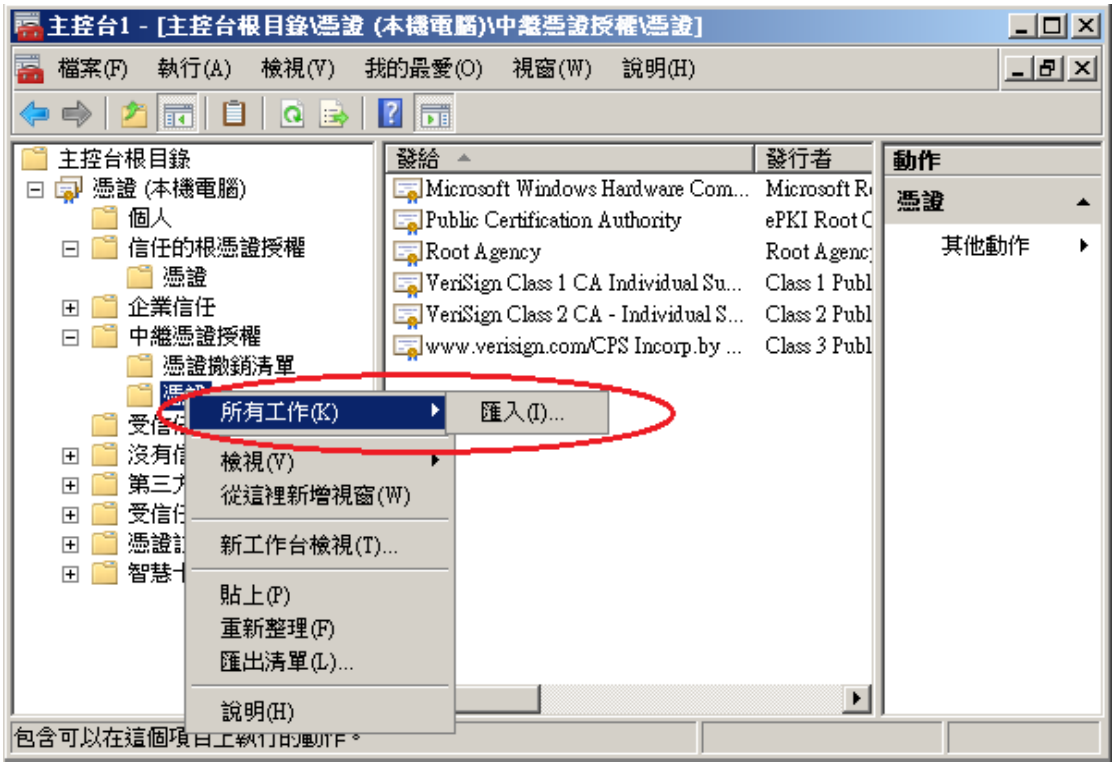
第 1 張 GRCA 自發憑證(GRCA1 簽 GRCA1.5)

http://grca.nat.gov.tw/repository/Certs/GRCA1_to_GRCA1_5.cer

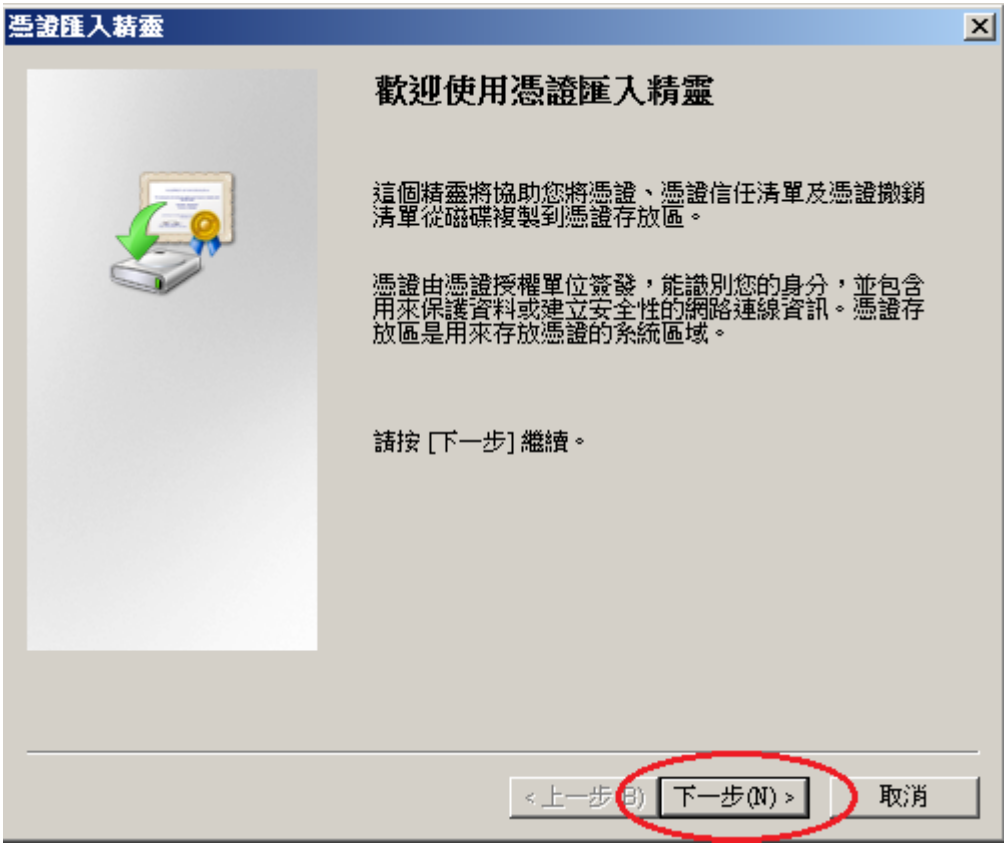
第 2 張 GRCA 自發憑證(GRCA1.5 簽 GRCA2)

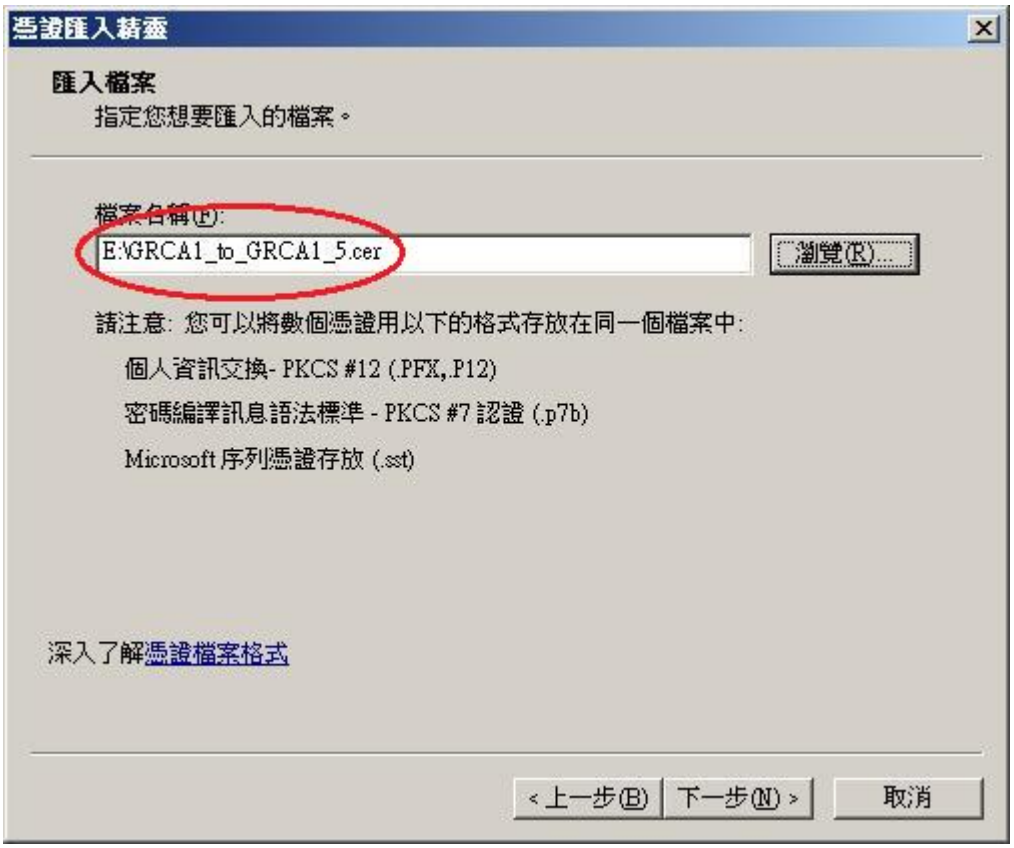
http://grca.nat.gov.tw/repository/Certs/GRCA1_5_to_GRCA2.cer

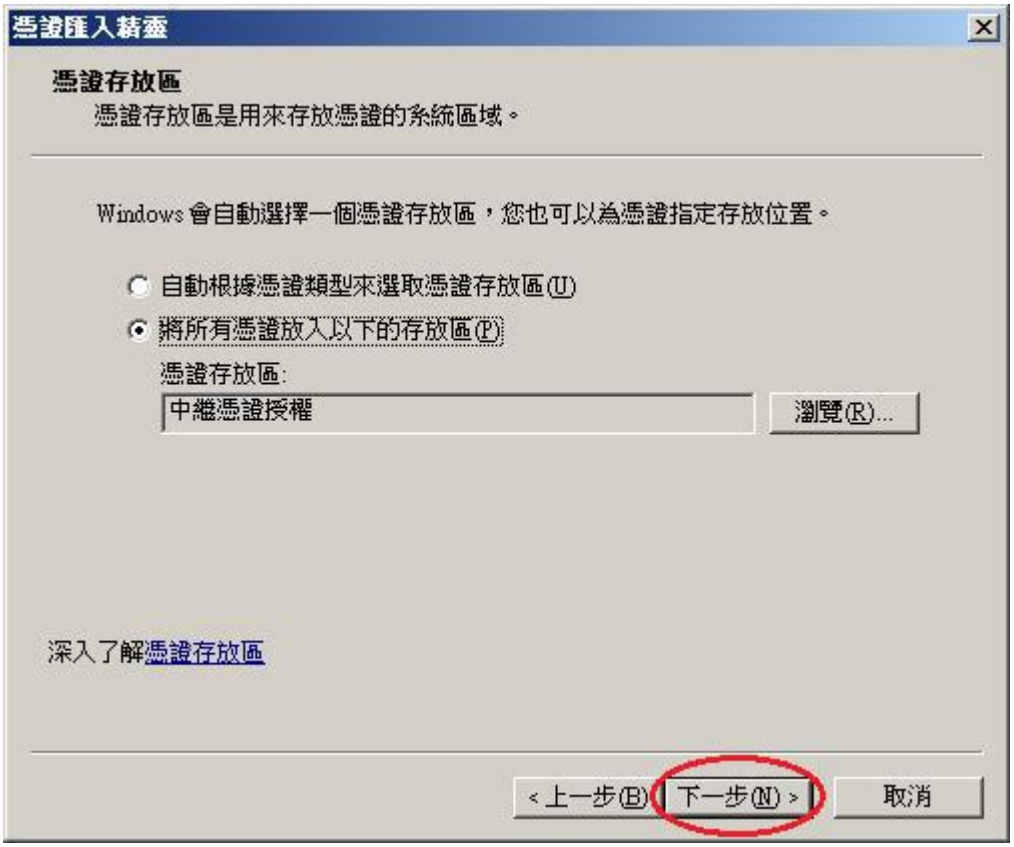
7. **匯入第 1 張自發憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



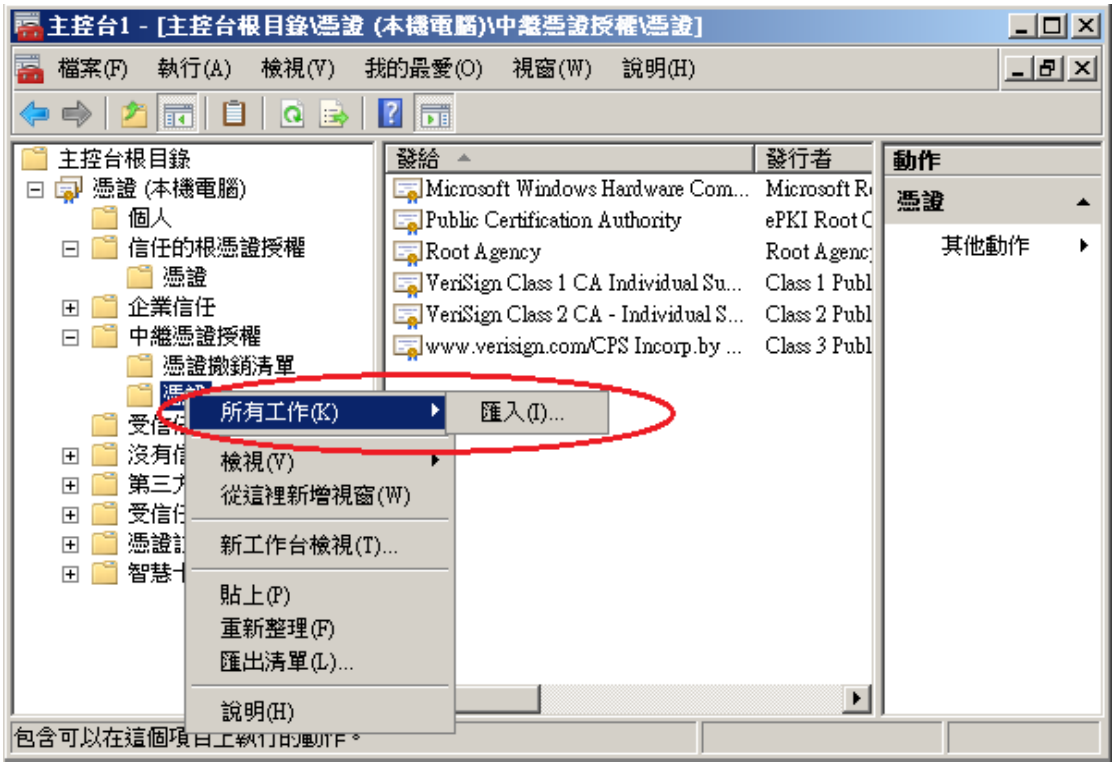
出現以下畫面後，點選「下一步」→「下一步」→「完成」。



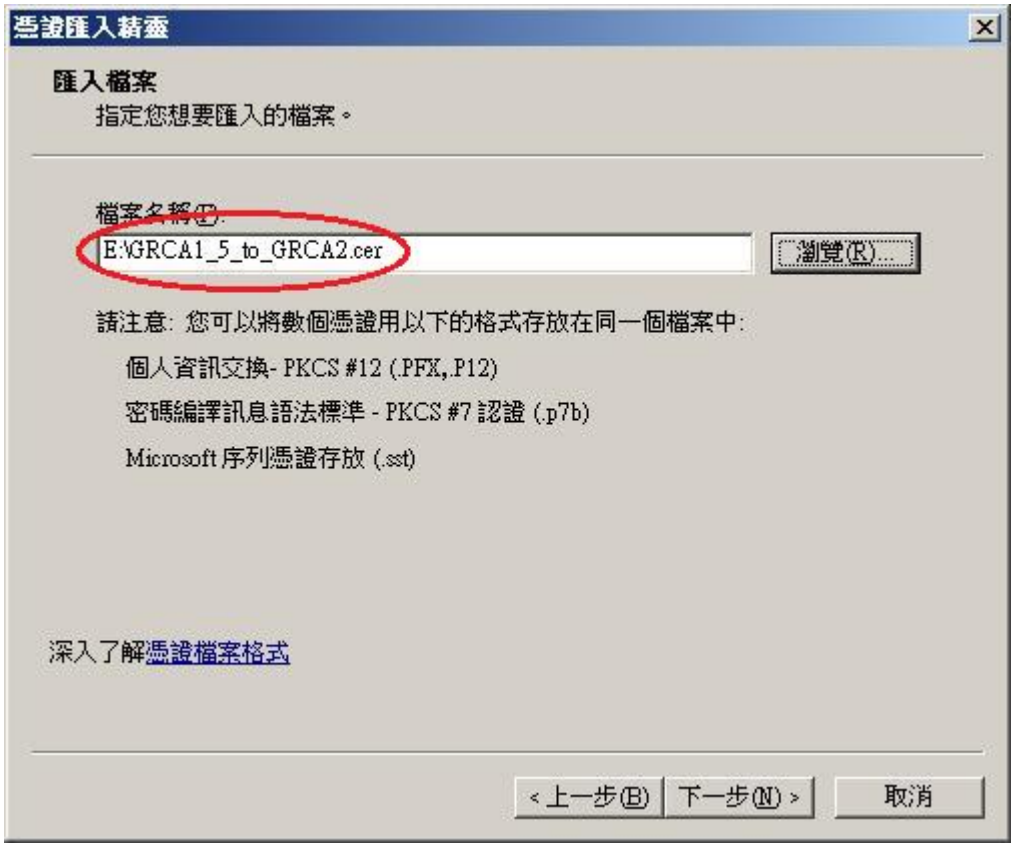

憑證匯入精靈
匯入檔案
指定您想要匯入的檔案。
檔案名稱(F):
E:\GRCA1_to_GRCA1_5.cer
瀏覽(R)...
請注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準 - PKCS #7 認證 (.p7b)
Microsoft 序列憑證存放 (.sst)
深入了解憑證檔案格式
< 上一步(B)
下一步(N) >
取消


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:
中繼憑證授權
瀏覽(R)...
深入了解憑證存放區
< 上一步(B)
下一步(N) >
取消

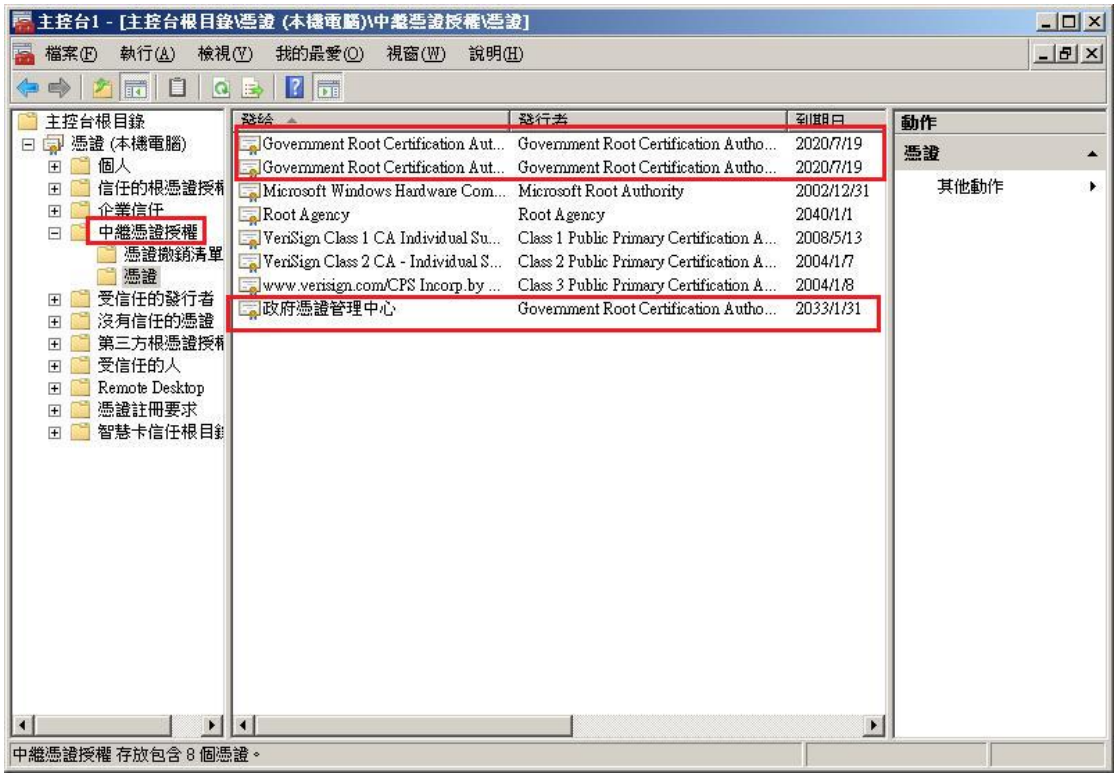
8. **匯入第 2 張自發憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



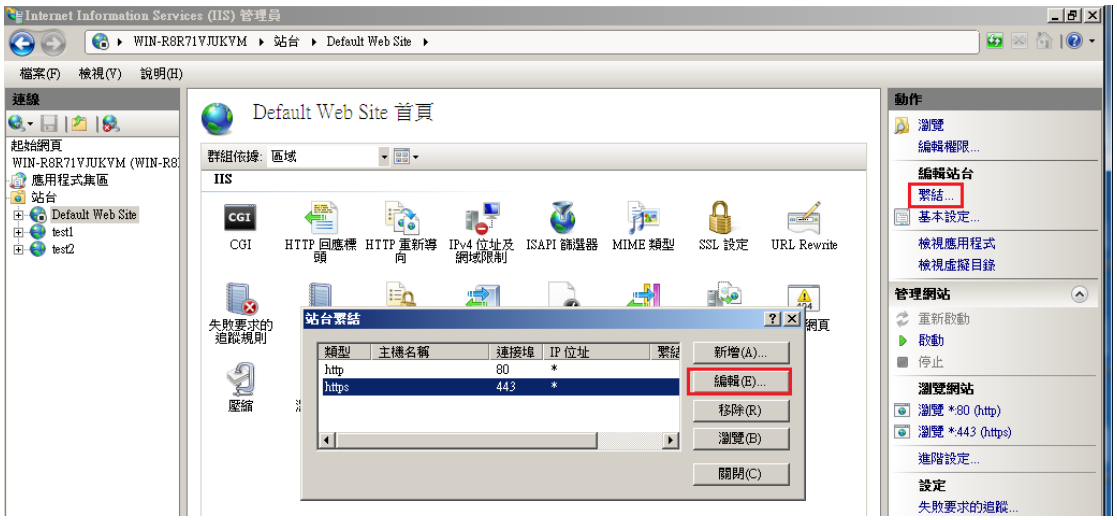
依照上述匯入第 1 張 GRCA 自發憑證的步驟，匯入第 2 張自發憑證。

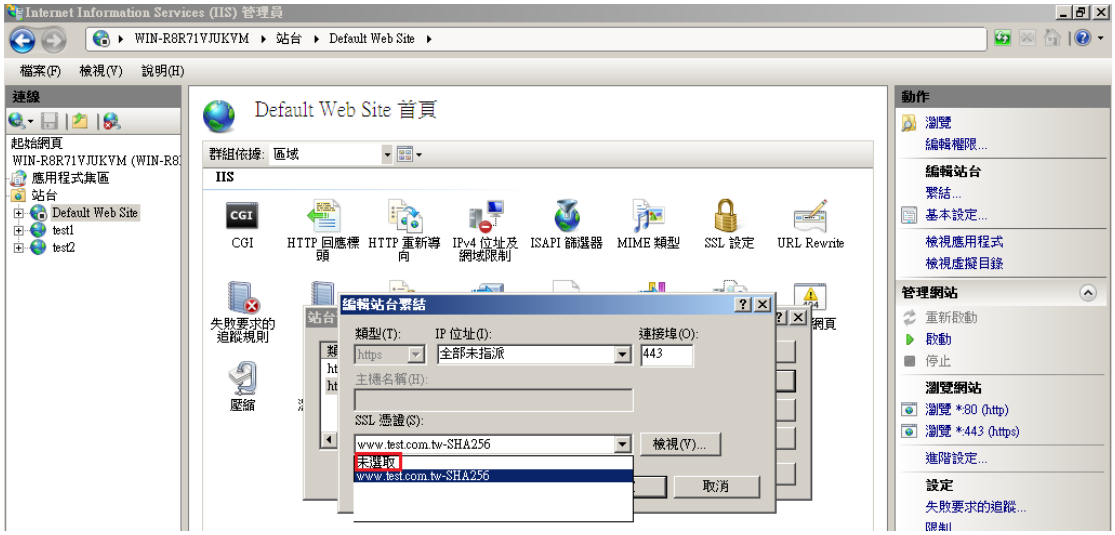


匯入完成後的中繼授權單位只會有下圖中的 3 張憑證。



9. 請**重新繫結**(Binding)，進入編輯站台繫結後，請先選擇「未選取」，之後再選原本的 SSL 憑證並按確定。

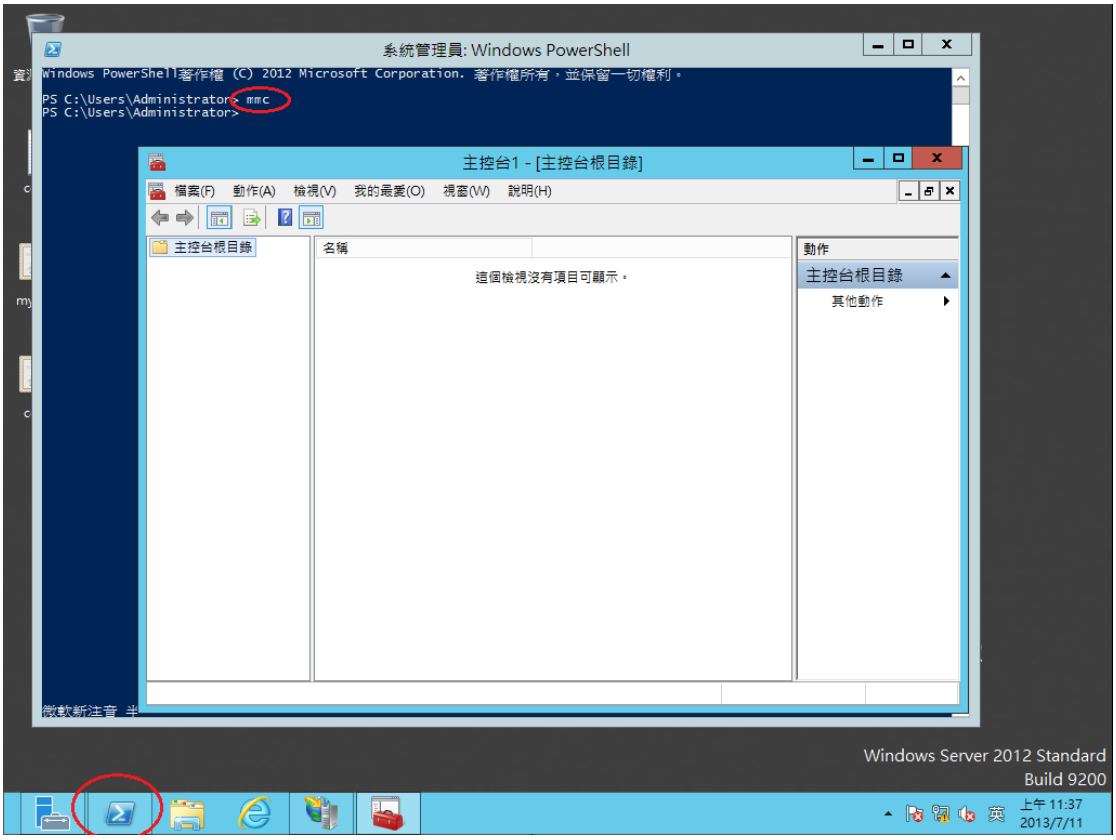




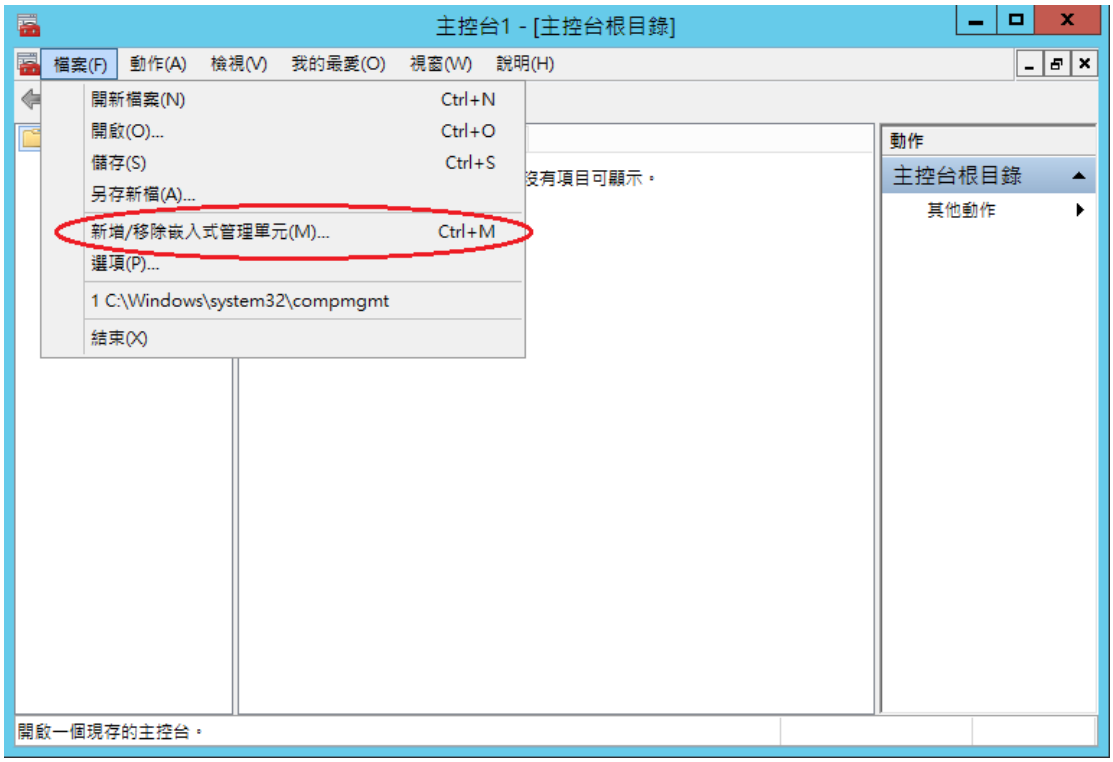
10. 若重新繫結後依然沒有更新為 5 層憑證串鍊，請將主機重開機。

(二)網站伺服器：Windows IIS 8

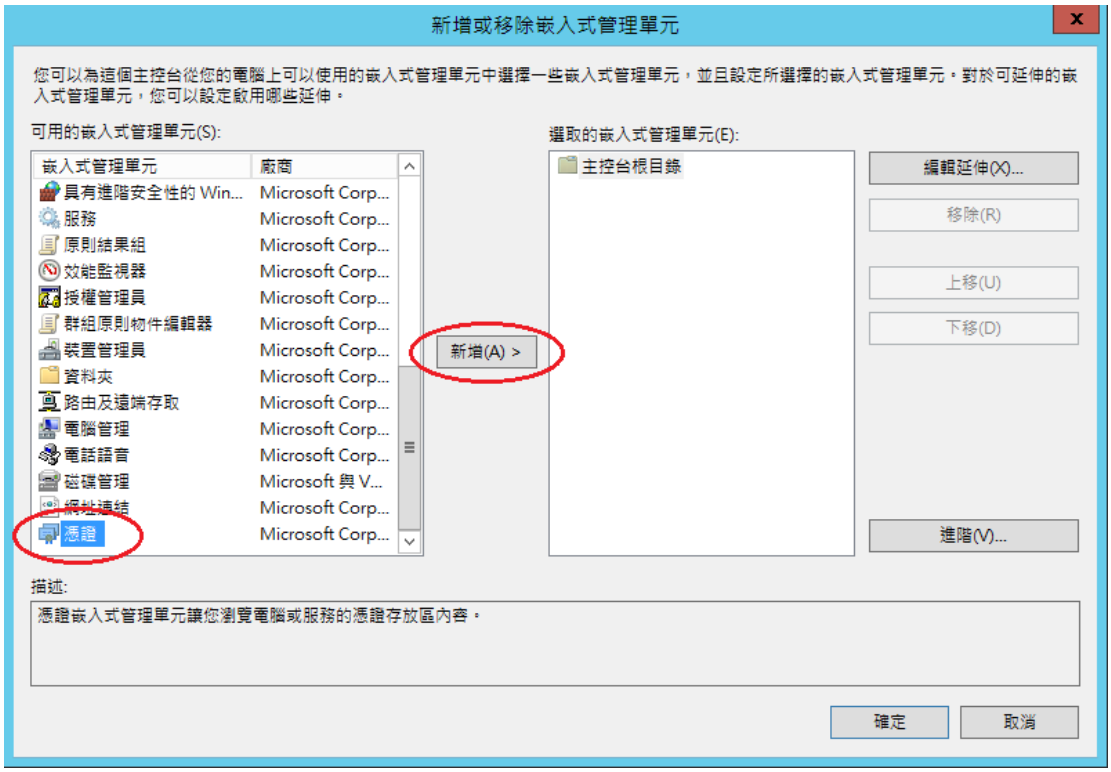
1. 請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。



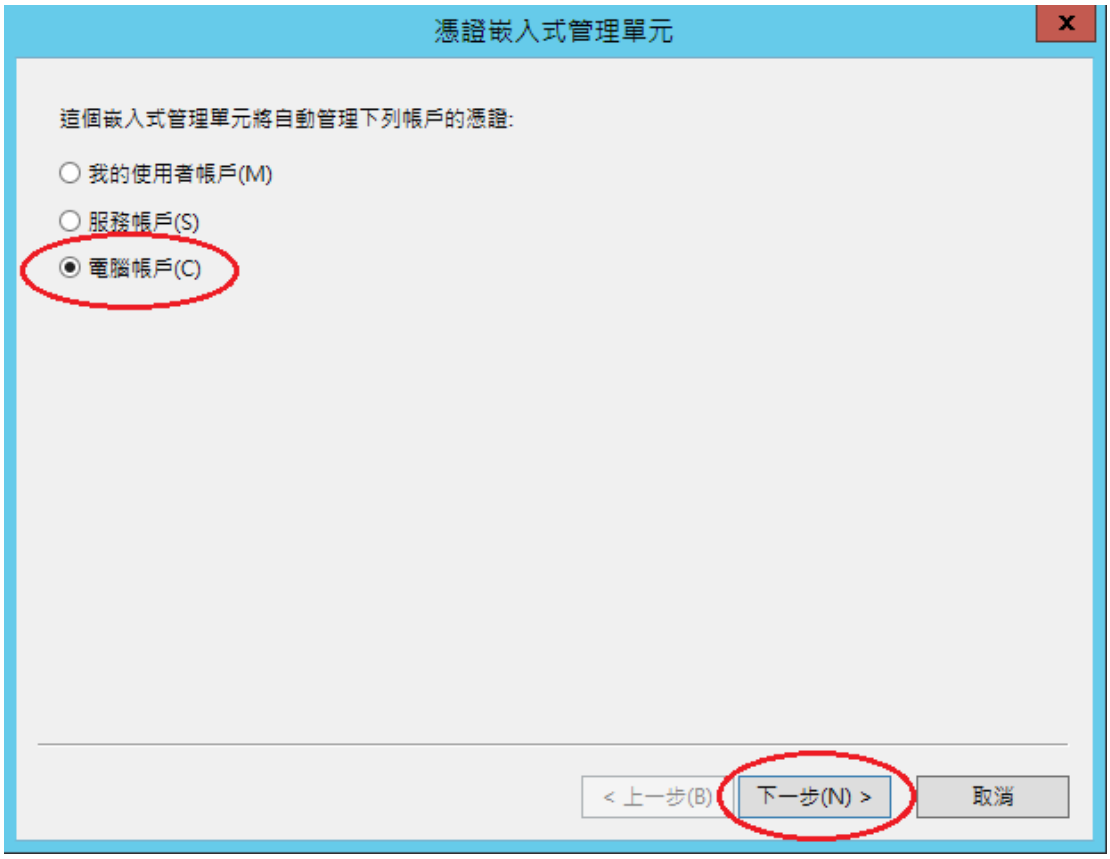
2. 選擇「新增/移除嵌入式管理單元」。

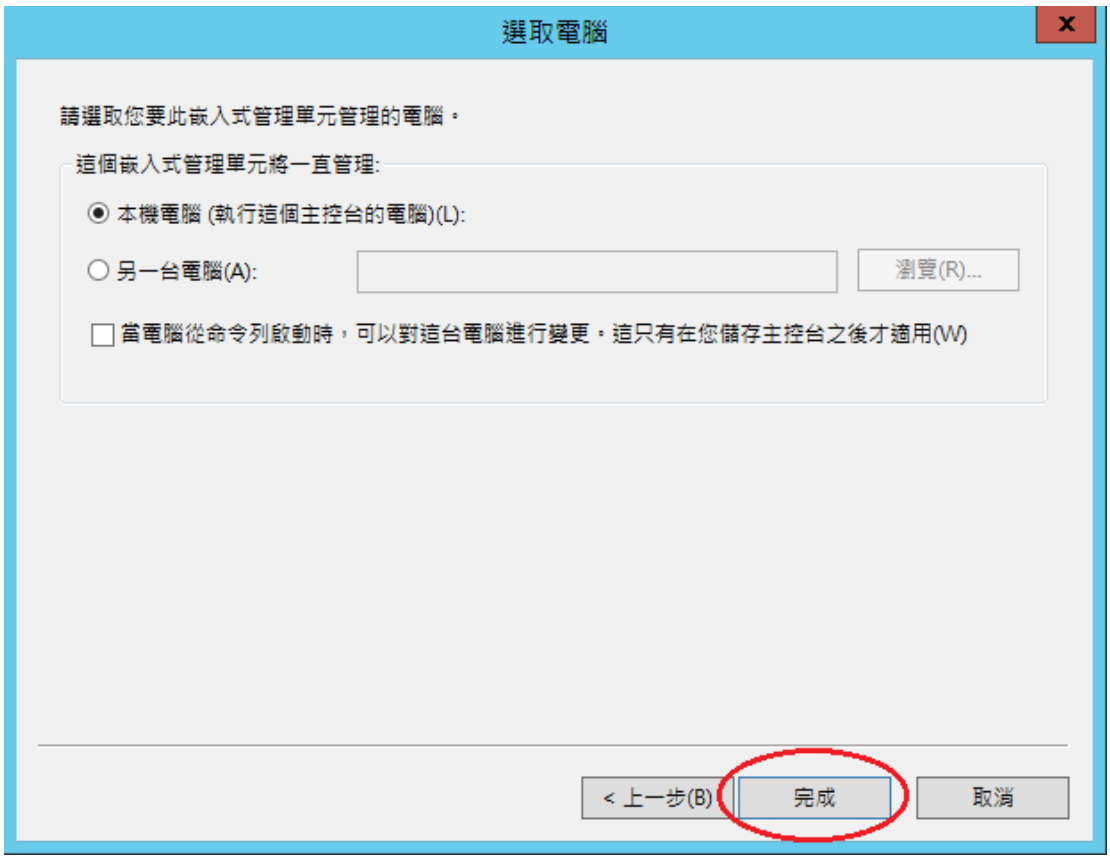

主控台1 - [主控台根目錄]
檔案(F)
動作(A)
檢視(V)
我的最愛(O)
視窗(W)
說明(H)
開新檔案(N) Ctrl+N
開啟(O)... Ctrl+O
儲存(S) Ctrl+S
另存新檔(A)...
新增/移除嵌入式管理單元(M)... Ctrl+M
選項(P)...
1 C:\Windows\system32\compmgmt
結束(X)
沒有項目可顯示。
動作
主控台根目錄
其他動作
開啟一個現存的主控台。

3. 接著點選「憑證」→「新增」。

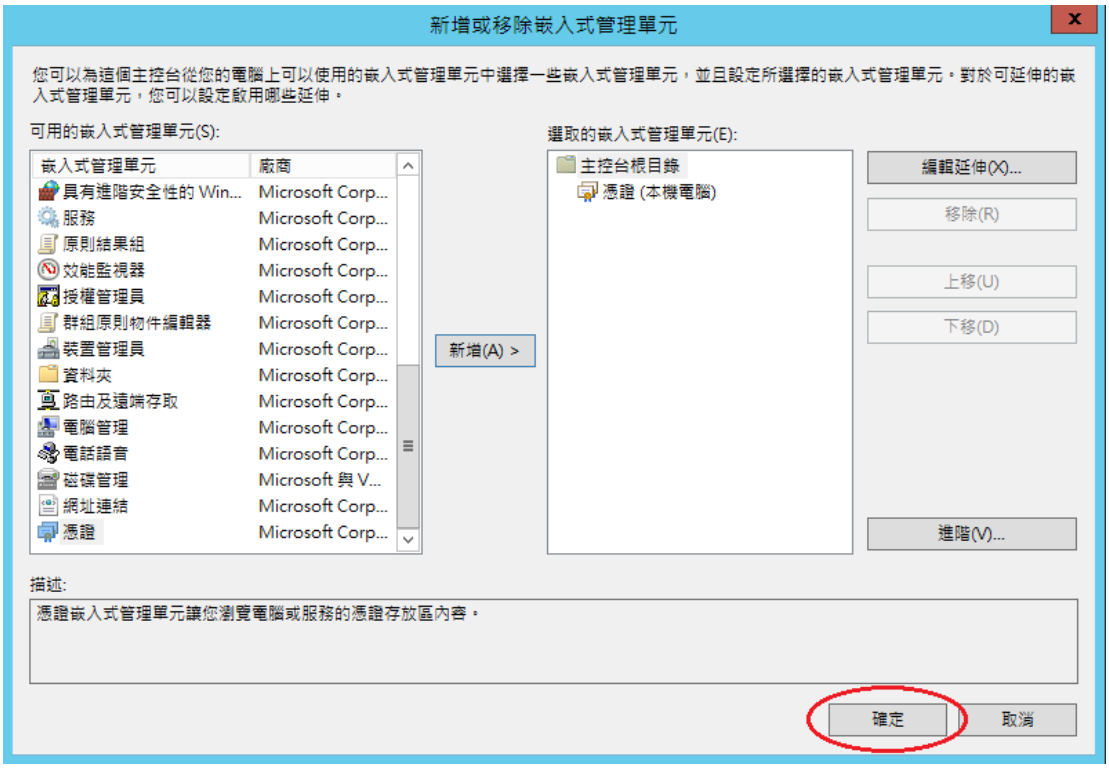

新增或移除嵌入式管理單元
您可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式管理單元，並且設定所選擇的嵌入式管理單元。對於可延伸的嵌入式管理單元，您可以設定啟用哪些延伸。
可用的嵌入式管理單元(S):
嵌入式管理單元
廠商
具有進階安全性的 Win... Microsoft Corp...
服務 Microsoft Corp...
原則結果組 Microsoft Corp...
效能監視器 Microsoft Corp...
授權管理員 Microsoft Corp...
群組原則物件編輯器 Microsoft Corp...
裝置管理員 Microsoft Corp...
資料夾 Microsoft Corp...
路由及遠端存取 Microsoft Corp...
電腦管理 Microsoft Corp...
電話語音 Microsoft Corp...
磁碟管理 Microsoft 與 V...
憑證 Microsoft Corp...
新增(A) >
選取的嵌入式管理單元(E):
主控台根目錄
編輯延伸(X)...
移除(R)
上移(U)
下移(D)
進階(V)...
描述:
憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放區內容。
確定
取消

選擇「電腦帳戶」→「下一步」→「完成」。

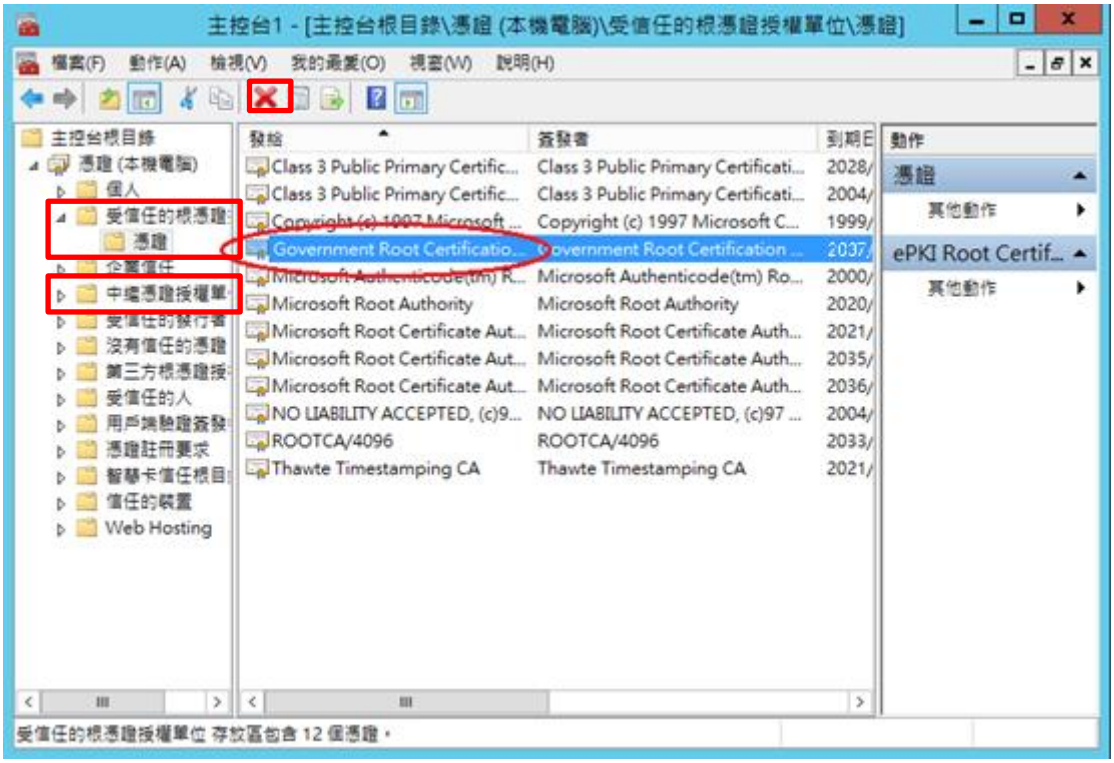




最後按下「確定」。



4. 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。



5. 檢查中繼憑證授權單位中是否有 GRCA 的自發憑證(到期日為 2032/12/5)，若有請刪除。

6. 請至下列網址下載 2 張自發憑證

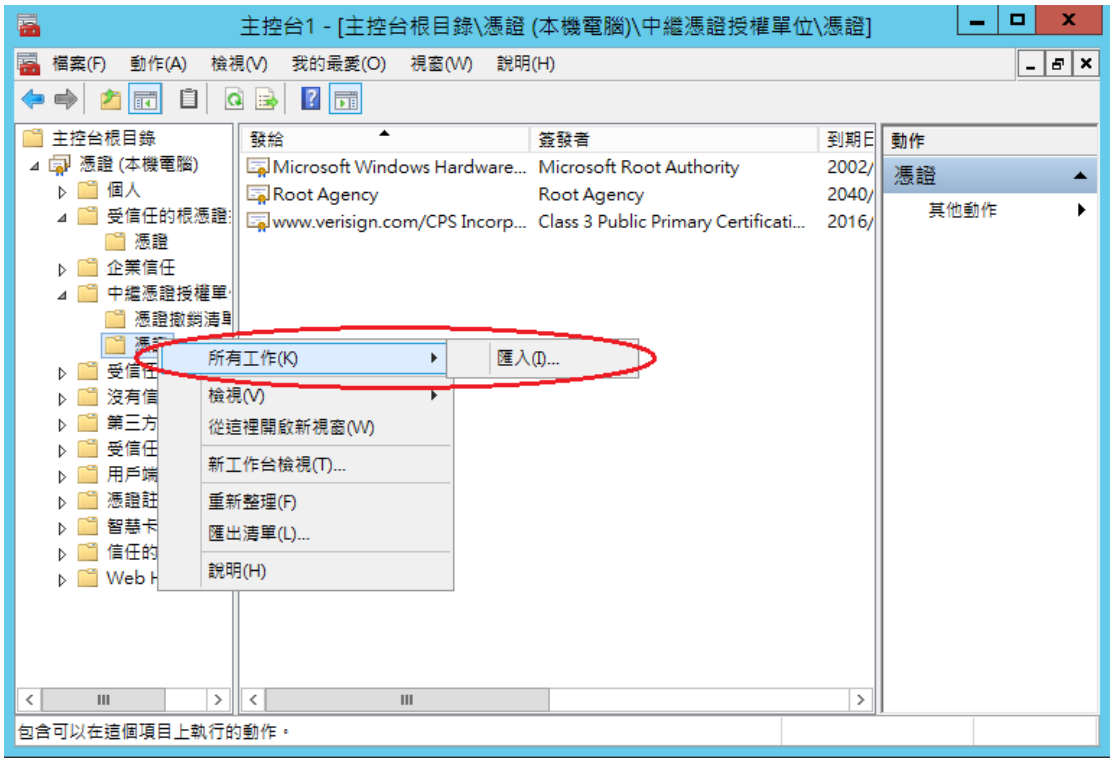
第 1 張 GRCA 自發憑證(GRCA1 簽 GRCA1.5)

http://grca.nat.gov.tw/repository/Certs/GRCA1_to_GRCA1_5.cer

第 2 張 GRCA 自發憑證(GRCA1.5 簽 GRCA2)

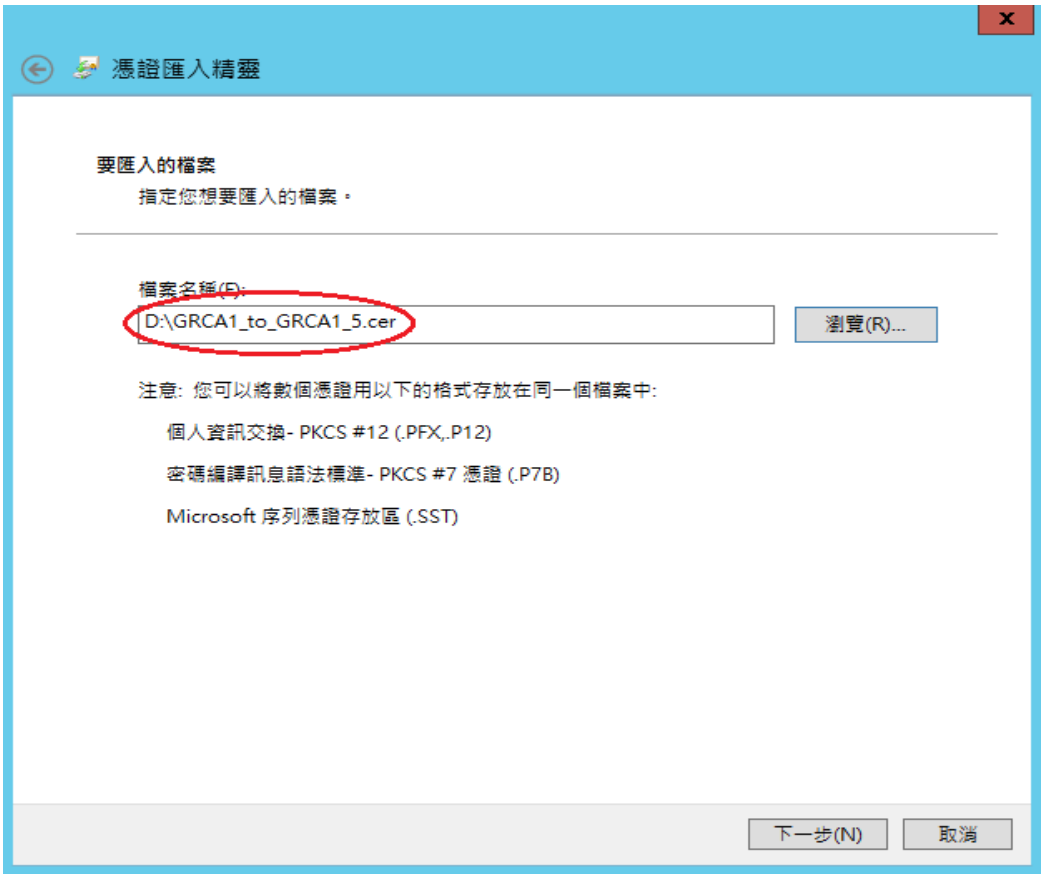
http://grca.nat.gov.tw/repository/Certs/GRCA1_5_to_GRCA2.cer

7. **匯入第 1 張 GRCA 自發憑證**。在「中繼憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



依照下列步驟匯入自發憑證。

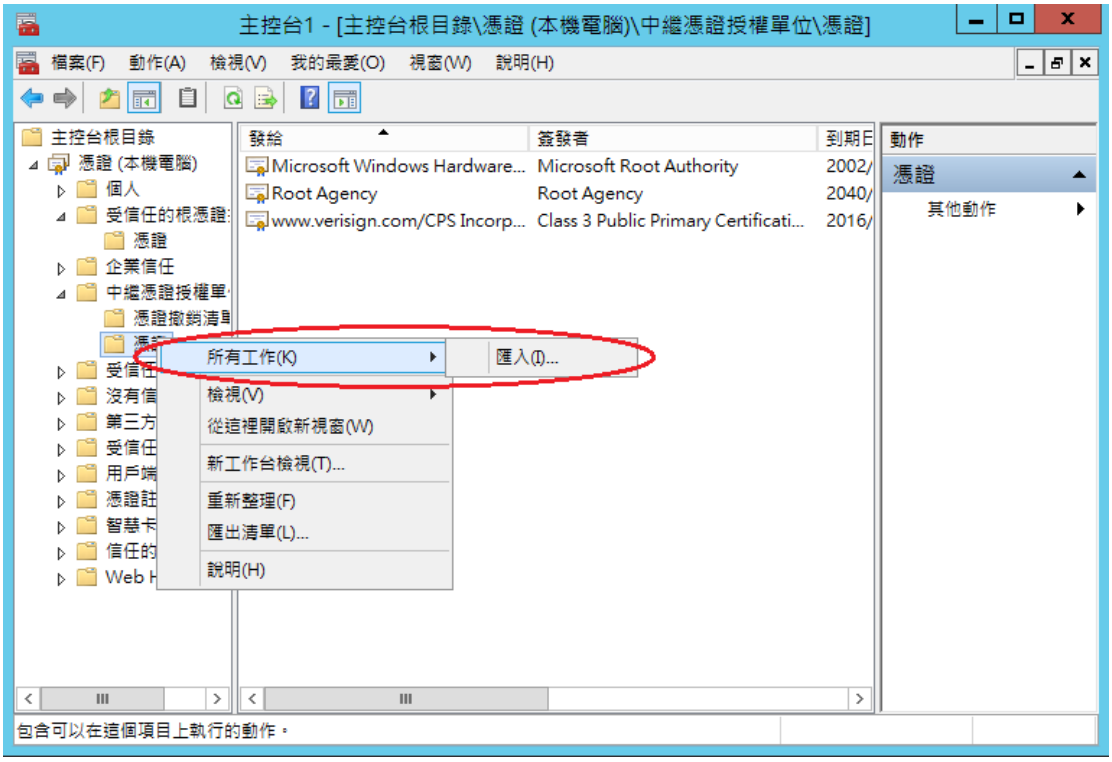

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消


憑證匯入精靈
要匯入的檔案
指定您想要匯入的檔案。
檔案名稱(F):
D:\GRCA1_to_GRCA1_5.cer
瀏覽(R)...
注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)
Microsoft 序列憑證存放區 (.SST)
下一步(N)
取消

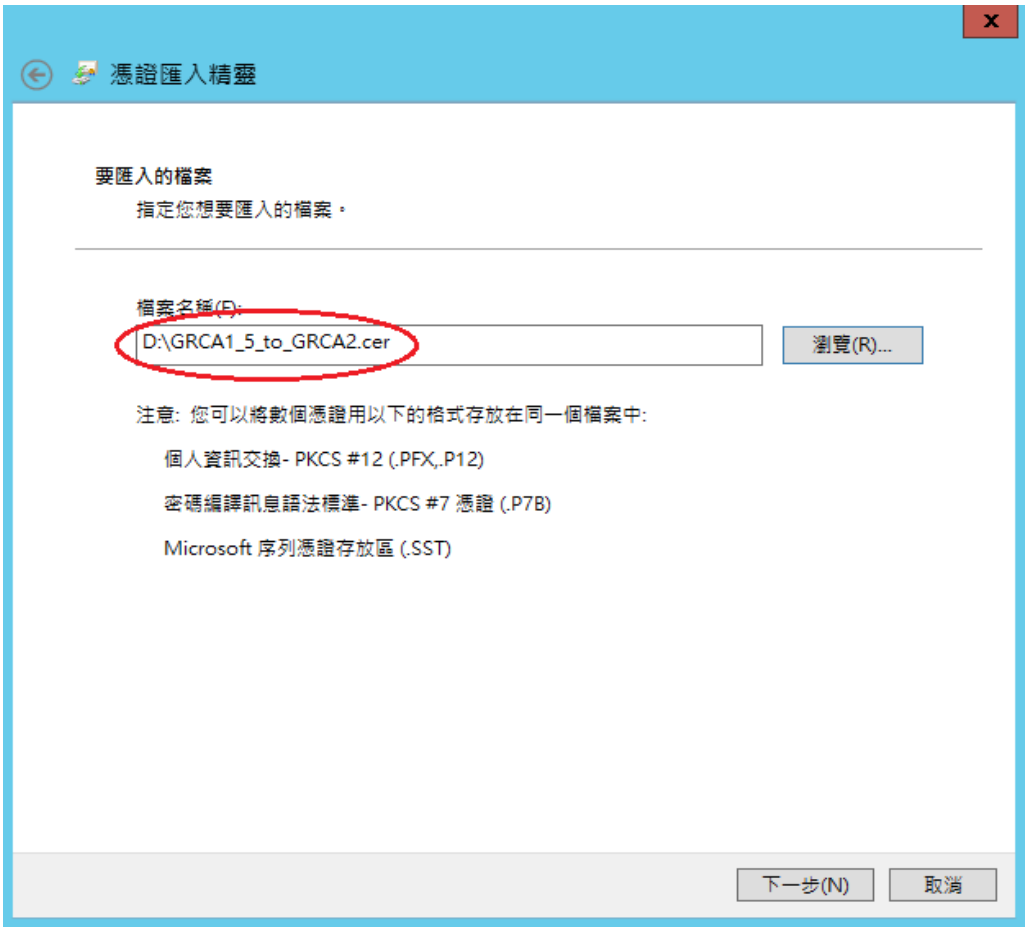

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
中繼憑證授權單位
瀏覽(R)...
下一步(N)
取消


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 中繼憑證授權單位
內容 憑證
檔案名稱 D:\GRCA1_to_GRCA1_5.cer
完成(F)
取消

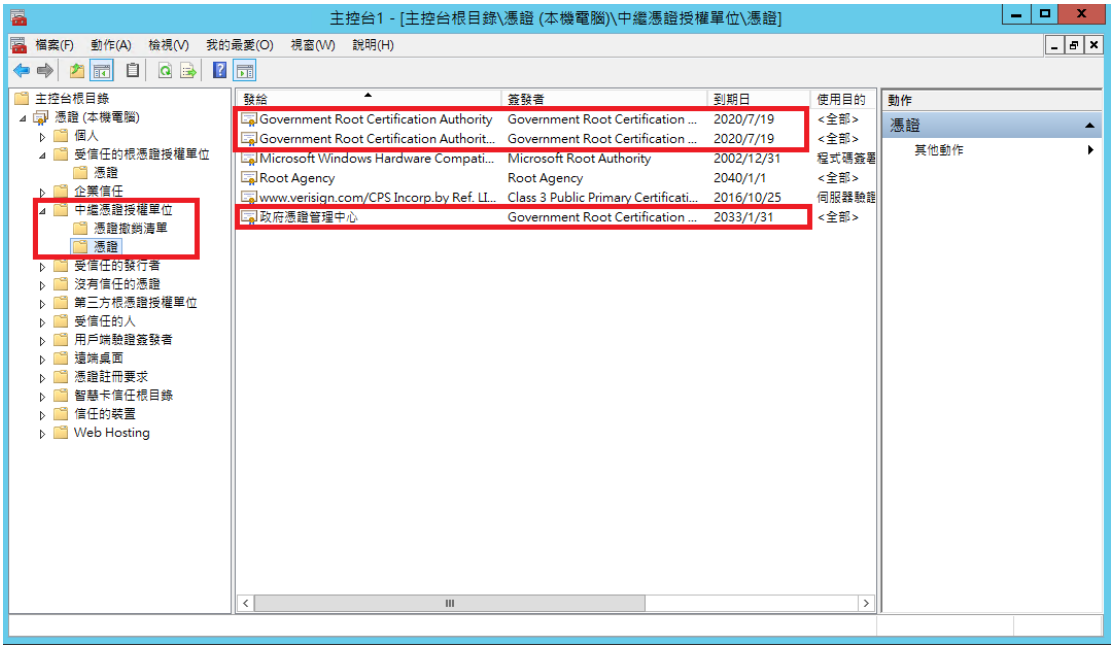
8. **匯入第 2 張自發憑證**。在「中繼憑證授權」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



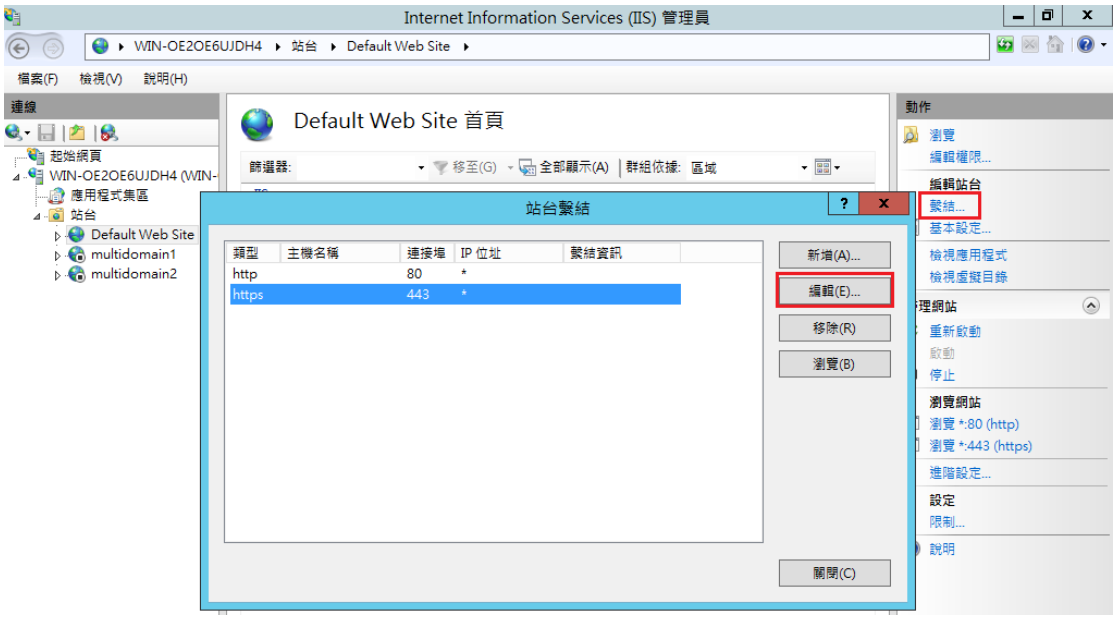
依照上述匯入第 1 張 GRCA 自發憑證的步驟，匯入第 2 張自發憑證。

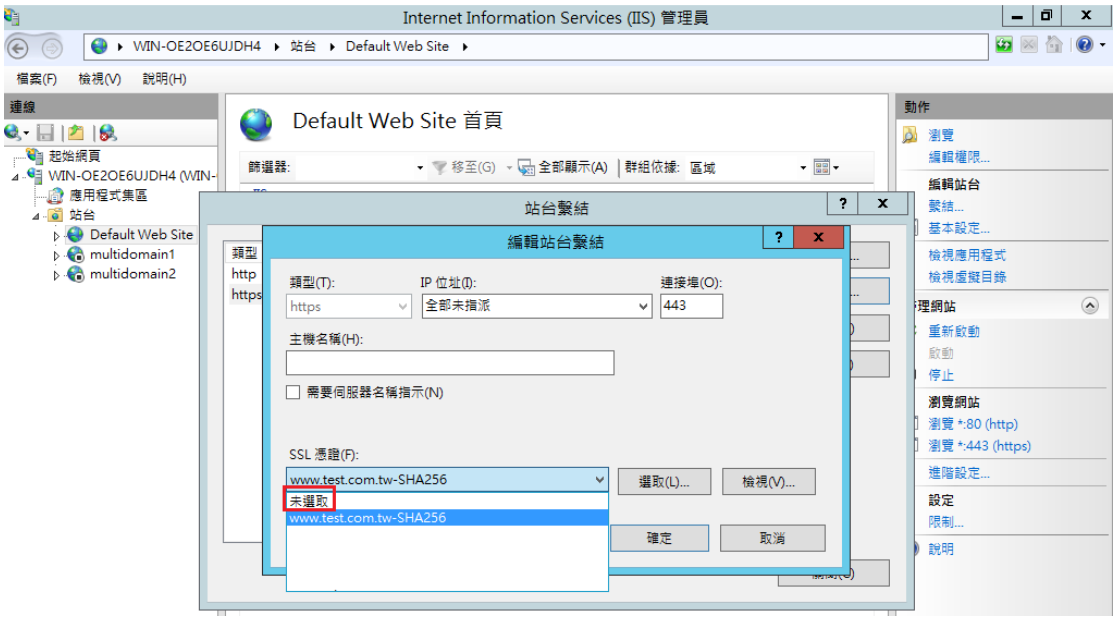


匯入完成後的中繼授權單位只會有下圖中的 3 張憑證。



9. 請**重新繫結**(Binding)，進入編輯站台繫結後，請先選擇「未選取」，之後再選原本的 SSL 憑證並按確定。





10. 若重新繫結後依然沒有更新為 5 層憑證串鍊，請將主機重開機。

(三)網站伺服器：Apache

1. 請至 GCA 網站下載已經製作好的憑證串鏈檔案，格式為 PEM 編碼，下載網址為 http://gca.nat.gov.tw/download/GRCA1_5_GCA2.zip。
2. 將下載的 GRCA1_5_GCA2.zip 解壓縮得到 GRCA1_5_GCA2.crt。
3. 若 Apache 版本 < 2.4.8，請參考以下步驟操作
   (1) 將 GRCA1_5_GCA2.crt 放置於 Apache Server 存放憑證的目錄中，舊的憑證串鍊檔案(NewWithOld_GCA2.crt)可刪除。
   (2) 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。
   (3) 若在 httpd-ssl.conf 找不到 **SSLCertificateChainFile** 參數，則請確認私密金鑰檔案路徑設定的 conf 檔案為何(ex: httpd.conf, httpd-vhosts.conf)，此參數會與私密金鑰放在同一設定檔中。
4. 若 Apache 版本 >= 2.4.8，請參考以下步驟操作
   (1) 將 GRCA1_5_GCA2.crt 使用文字編輯軟體開啟，複製全部的內容。
   (2) 用文字編輯軟體開啟目前已經安裝的網站 SSL 憑證，檔案路

徑為 SSLCertificateFile 參數指定之位址，以下為範例。

```
SSLCertificateFile "/export/httpd-2.    /certs/gca_server.crt"
SSLCertificateKeyFile "/export/httpd-2.    /certs/gca_server.key"
```

(3) 在開啟之 SSL 憑證檔案最後面間隔一空白行，貼上步驟(1)複製的憑證串鍊內容，可參考下圖。

```
1  -----BEGIN CERTIFICATE-----
2  MIIFNzCCBB+gAwIBAgIQboDPTayQ/0nvVYN0jC89TzANBgkqhkiG9w0BAQsFADBE
3  MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQLDBjmlL/l
4  upzmhpHorYnnrqHnkIbkuK3lv4MwHhcNMTUwNjI2MDcyOTEzWhcNMTgwNjI2MDcy
5  OTEzWjB4MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQL
6  DBjmlL/lupzmhpHorYnnrqHnkIbkuK3lv4MxFzAVBgNVBAMTDmdjYS5uYXQuZ292
7  LnR3MRkwFwYDVQQFExAwMDAwMDAwMDEwMDI0OTMxMIIBIjANBgkqhkiG9w0BAQEF
8  AAOCAQ8AMIIBCgKCAQEA36nu2MtLzMzB1Of71CqnV2VC/qpwk8Yh/nbYXJ/KCkB0
9  raDPxAD5IjJYHkAR5RcwkbdCEXyEylfsBmoqikpT8NLRJQZKBmc0cciltIeFRZWX
10 ymNhEBkmMo3jhK2r/3o1WLIcnoAIrSifLBC0TAR3xjzHQ1xIG4/FkC89APo0PZNR
11 Beo8h67YSgnGbSA/1fG/KCKCc3dbzKi4PADffrvUzmpIvIsm1MTxo028TT/BkrP2
12 LpxLr8p6+fc7s7b7mcr1nLBLETGAT+/tGIn+v1T14DnrK/0kbjUiyTlOkr1q8bYO
13 Vc4Znr7+lf8Vt6jYlBFDEdr5SJBIZD/cMgjUChTzrwIDAQABo4IB7zCCAeswHwYD
14 VR0jBBgwFoAU0Rhnw1f+EpqRa19fMeo+woSH+70wHQYDVR0OBBYEFIFlLP6lDPXX
15 psjH64JagS2rR1ZZMIGYBggrBgEFBQcBAQSBizCBiDBFBggrBgEFBQcwAoY5aHR0
16 cDovL2djYS5uYXQuZ292LnR3L3JlcG9zaXRvcnkvQ2VydHMvSXNzdWVkVG9UaGlz
17 Q0EucDdiMD8GCCsGAQUFBzABhjNodHRwOi8vZ2NhLm5hdC5nb3YudHcvY2dpLWJp
18 bi9PQ1NQMi9vY3NwX3NlcnZlci5leGUwDgYDVR0PAQH/BAQDAgWgMBQGA1UdIAQN
19 MAswCQYHYIZ2ZQADAzAZBgNVHREEEjAQgg5nY2EubmF0Lmdvdi50dzAgBgNVHQkE
20 GTAXMBUGB2CGdgFkAgExCgYIYIZ2AWQDAwEwgYgGA1UdHwSBgDB+MD2gO6A5hjdo
21 dHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9HQ0E0L0NSTDIvQ1JMXzAw
22 MDEuY3JsMD2gO6A5hjdodHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9H
23 Q0E0L0NSTDIvY29tcGxldGUuY3JsMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggr
24 BgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAs71WC1KbhEmLBKu5HmUpHARv5lVa
25 rGusMOPNlBiKwLnfIP9WgcEzwInHdlC8YYEzWYM5K6qagP1spWhzA4rGIg4660ZO
26 z91Sk6sqE1hhYza/BnYlpvz63y8XjCUAOw0WWpbKpCJWGeuTg7FaN2ZpQs4POMbU
27 36aernb1KLTIFOQUFmfklmUiHNKe3+g03xTINzyZ+lJCRtk6frG1CyqqO7h0d2Zc
28 iHgCOkChSiqpSJL5/42dl5yYc/W9eU4gFfSdvC0f1OHb8cCspbmtTI6RWnU5UoY8
29 aJofnhLb1x/k8GwgizPvQk7axgOFaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA==
30 -----END CERTIFICATE-----
31
32 與END CERTIFICATE間隔一空白行，貼上複製的憑證串鍊內容
```

(4) 貼上後之檔案範例如下圖。

```
iHgCOkChSiqpSJL5/42dl5yYc/W9eU4gFfSdvC0f1OHb8cCspbmtTI6RWnU5UoY8
aJofnhLb1x/k8GwgizPvQk7axgOFaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA==
-----END CERTIFICATE-----
```

原本SSL憑證之內容

```
subject=/C=TW/O=\xE8\xA1\x8C\xE6\x94\xBF\xE9\x99\xA2/OU=\xE6\x94\xBF\xE5\xBA\x9C\xE6\x8
issuer=/C=TW/O=Government Root Certification Authority
-----BEGIN CERTIFICATE-----
MIIFLzCCAxegAwIBAgIQMe5Y77XBpI+a7fR13bilwTANBgkqhkiG9w0BAQsFADA/
MQswCQYDVQQGEwJUVzEwMC4GA1UECgwnR292ZXJubWVudCBSb290IEN1cnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTEzMDEzMTAzMjIzNFoXDTMzMDEzMTAzMjIzNFow
RDELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCeihjOaUv+mZojEhMB8GA1UECwwY5pS/
5bqc5oaR6K2J566h55CG5Lit5b+DMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAtX7xPZUtp5iBGQvqYghJUoLeyCJJoaTcc1bcOGHij64WUBYpDu8KKEQK
R1y3zjcDXrLcZX483tmNs92DXSNuBHlx+we1aFyuLpKQVCji97ys3KeMxAEcaXqo
3cZu8nY3g//zkvX80G4RoCyDR86Z420R3mb0GlVw/9TEK8+oduZqAArEdfionpbE
K5zZ/8qaaHafgqMBQGuzfccDKLoWRcTzu3S0IvOpVU6pcB0rJOtc4F7c16tQdXfo
a8sjfcveKKbUQF6AklwugRufHdLqEVpOiGRcDPaHtT6SHJ7D/t+A/rAXMPidcksQ
rea/E+5+lehqEMHSA/gSLa9Ph+/gDQIDAQABo4IBIDCCARwwHwYDVR0jBBgwFoAU
lWcd4Jx6LJzLxZjnHQcmKobsdM0wHQYDVR0OBBYEFNEYZ8NX/hKakWtfXzHqPsKE
h/u9MA4GA1UdDwEB/wQEAwIBBjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vZ3Jj
YS5uYXQuZ292LnR3L3JlcG9zaXRvcnkvQ1JMMi9DQS5jcmwwVgYIKwYBBQUHAQEE
SjBIMEYGCCsGAQUFBzAChjpodHRwOi8vZ3JjYS5uYXQuZ292LnR3L3JlcG9zaXRv
cnkvQ2VydHMvSXNzdWVkVG9UaGlzQ0EucDdiMBIGA1UdEwEB/wQIMAYBAf8CAQAw
HgYDVR0gBBcwFTAJBgdghnZlAAMDMAgGBmeBDAECAjANBgkqhkiG9w0BAQsFAAOC
AgEAs3KvqDSIq6GERR/SonDfYnrpF/IdZLM9gBfsIIafNeeWjFCIuC5Ah7LEIhZY
PP/D8y00OCRlZ7GoY4JZIvTFA1fb2umEmKC/ssCwQdUxyd52JfbqBL5N0cP2eU1x
lZG8d1z8uIq7ItyfO5ML1eAboYMHsO7c10pLmtufZj8VZ4zp4DTRxVzROPKwlIbR
QSKNlymWgAop+Eg9b40lfBMBxFppb3R4IZpijCpy0RbPOzvtmDpen3WZmJ+vsCqc
D8b8JqDeRG5zQI1sIeV15qqGZuV8oL5gFi4niltkLNS3fGYAr4+LXVojMWIO/Noe
Ji+i3AtfhnN/w3Ixzhxi39pN+hYzFGtsZNioUC2MQexFJS+AQ4s8D41cRCMwovfi
DerTbWKhTPoQXirUDV/ZSUjUlLDbXzdiUB+mxWd2k16HYcvMFUevxbNzJAxP355T
q9tliZpM/7MVq0/Bw4SGxxQRQF1uVQjMBtEsRYHKVZ1IBBJVOe8jZhc81Sw3jDmm
rtyjx1o2m8VVImsiIP2iPI3hlw/UCwCGRg5xvqqW72w2niT9pXdvZowBVbhP24wt
umuA45M5h4UNZRNo4/NG3UwS9eLKtfB06YFf3DcBban/Drf8LX8OGvF++Im3SeGJ
5zhUlYOVJcTHpR6TToXoKzvuzegRL2vQ4k22B++JtOQgsAg=
-----END CERTIFICATE-----

subject=/C=TW/O=Government Root Certification Authority
issuer=/C=TW/CN=Government Root Certification Authority - G1.5
-----BEGIN CERTIFICATE-----
MIIGcTCCBFmgAwIBAgIRAKOUO28QJlHOulORI3SaKiowDQYJKoZIhvcNAQELBQAw
NjELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCeihjOaUv+mZojE3MDUGA1UEAwwuR292
ZXJubWVudCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzEuNTAeFw0x
NzA3MTkwMjUxNDhaFw0yMDA3MTkwMjUxNDhaMD8xCzAJBgNVBAYTAlRXMTAwLgYD
VQQKDCdHb3Zlcm5tZW50IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC2/5c8gb4BWCQnr44BK9ZykjAy
```

複製貼上的憑證串鍊內容

(5) 將修改後的 SSL 憑證檔案存檔，檔案放置路徑跟原本 SSLCertificateFile 參數相同，此 SSL 檔案經由修改已經包含憑證串鍊。

(6) 檢查 conf 檔案中是否有 **SSLCertificateChainFile** 參數，若有請註解該行(前方加上#)。

5. 重新啟動 Apache Server。

(四)網站伺服器：Tomcat

下列步驟兩個%中間之路徑或名稱，請依照實際主機環境進行調整。

1. 請先將原本的 keystore 檔案備份，避免之後操作錯誤造成私密金鑰遺失。

2. 打斷原本 keystore 中之憑證串鍊，步驟如下。

   (1) 將 keystore 轉換為 pfx 檔案

   keytool -importkeystore -srckeystore %keystoreFile% -destkeystore %pfxFile% -srcstoretype jks -deststoretype PKCS12 -srcalias %aliasName% -destalias %aliasName%

   (2) 從 pfx 檔案中分離私密金鑰(.key)

   openssl pkcs12 -in %pfxFile% -nocerts -nodes -out %server.key%

   (3) 利用私密金鑰產生 CSR 檔案

   openssl req -new -key %server.key% -out %server.csr%

   (4) 利用 OpenSSL 與私密金鑰產生自簽憑證

   openssl x509 -req -days 7305 -sha1 -extfile openssl.cfg -extensions v3_ca -signkey %server.key% -in %server.csr% -out %server.cer%

   (5) 將自簽憑證匯入原本的 Keystore 中，以打斷原本的憑證串鍊

   keytool -import -keystore %keystoreFile% -alias %private key entry% -file %server.cer%

3. 刪除 keystore 內之前已匯入的 GRCA 及 GCA 憑證。

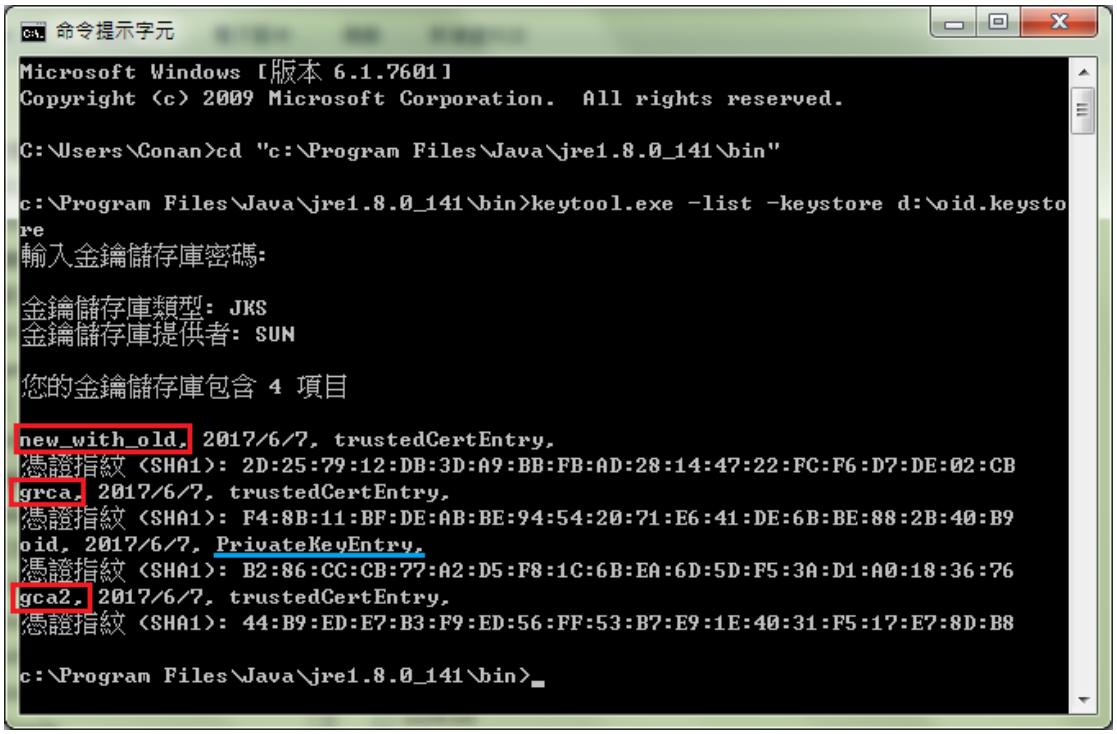
   (1) 在 %JAVA_HOME%\bin 目錄下執行

   keytool -list -keystore %keystoreFile%

   (2) 待出現 Enter keystore password：請輸入密碼

(3) 將除了 PrivateKeyEntry 之外的項目都刪除 (下列指令以下圖為例，實際 alias 名稱請依據畫面顯示輸入)

keytool -delete -alias new_with_old -keystore %keystoreFile%
keytool -delete -alias grca -keystore %keystoreFile%
keytool -delete -alias gca2 -keystore %keystoreFile%



(4) 待出現 Enter keystore password：請輸入密碼

4. 請至下列網址下載 4 張憑證：

GRCA1 自簽憑證

http://grca.nat.gov.tw/repository/Certs/GRCA.cer

GRCA 自發憑證(GRCA1 簽 GRCA1.5)

http://grca.nat.gov.tw/repository/Certs/GRCA1_to_GRCA1_5.cer

GRCA 自發憑證(GRCA1.5 簽 GRCA2)

http://grca.nat.gov.tw/repository/Certs/GRCA1_5_to_GRCA2.cer

GCA2 自簽憑證

http://gca.nat.gov.tw/repository/Certs/GCA2.cer

5. 依照下列步驟重新匯入新憑證串鍊。

安裝 GRCA 憑證(共 3 張)

(1) 在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias grca -file D:\GRCA.cer -keystore %keystoreFile%
keytool -import -alias grca2 -file D:\GRCA1_to_GRCA1_5.cer -keystore %keystoreFile%
keytool -import -alias grca3 -file D:\GRCA1_5_to_GRCA2.cer -keystore %keystoreFile%

(2) 待出現 Enter keystore password：請輸入密碼

(3) 若出現 Trust this certificate：請輸 y

安裝 GCA 憑證(共 1 張)

(1) 在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias gca2 -file D:\GCA2.cer -keystore %keystoreFile%

(2) 待出現 Enter keystore password：請輸入密碼

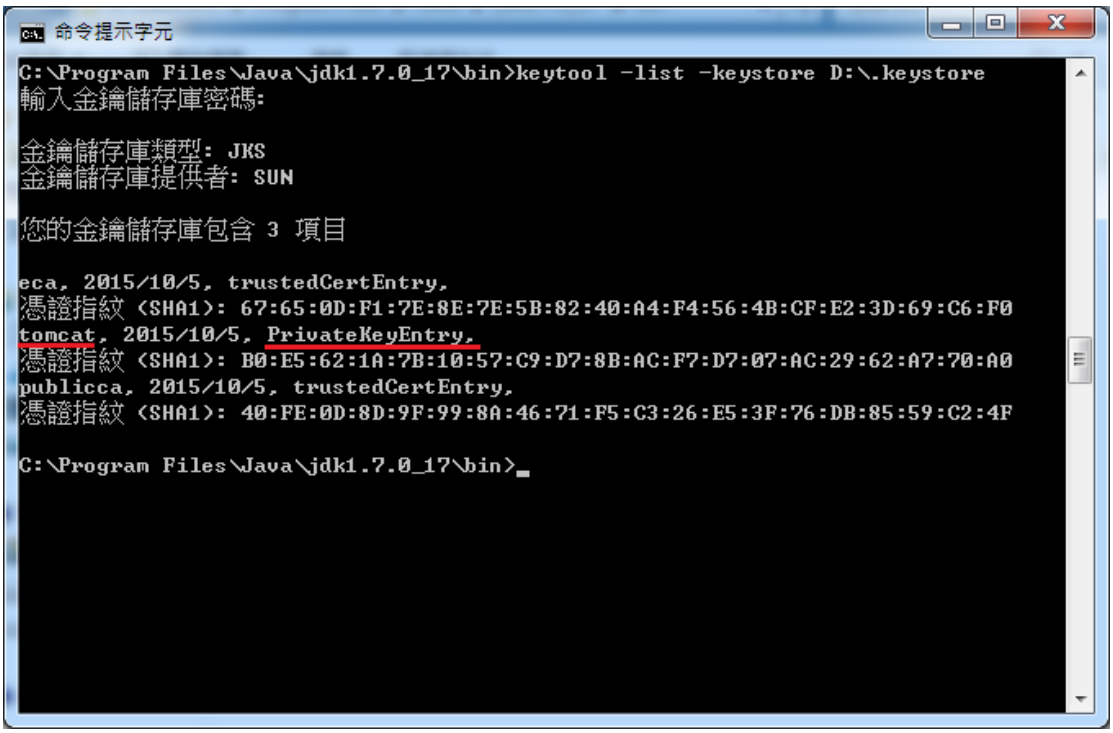
6. 確認 PrivateKeyEntry 的 alias name。

(1) 在 %JAVA_HOME%\bin 目錄下執行

keytool -list -keystore %keystoreFile%

(2) 待出現 Enter keystore password：請輸入密碼

(3) 找到 PrivateKeyEntry 對應的 alias name，下圖範例為 tomcat



7. 匯入 SSL 伺服器應用軟體憑證。

(1) 在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias %PrivateKeyEntry 的 alias name% -file %SSL 憑證檔案所在路徑% -keystore %keystoreFile%

(2) 待出現 Enter keystore password：請輸入密碼

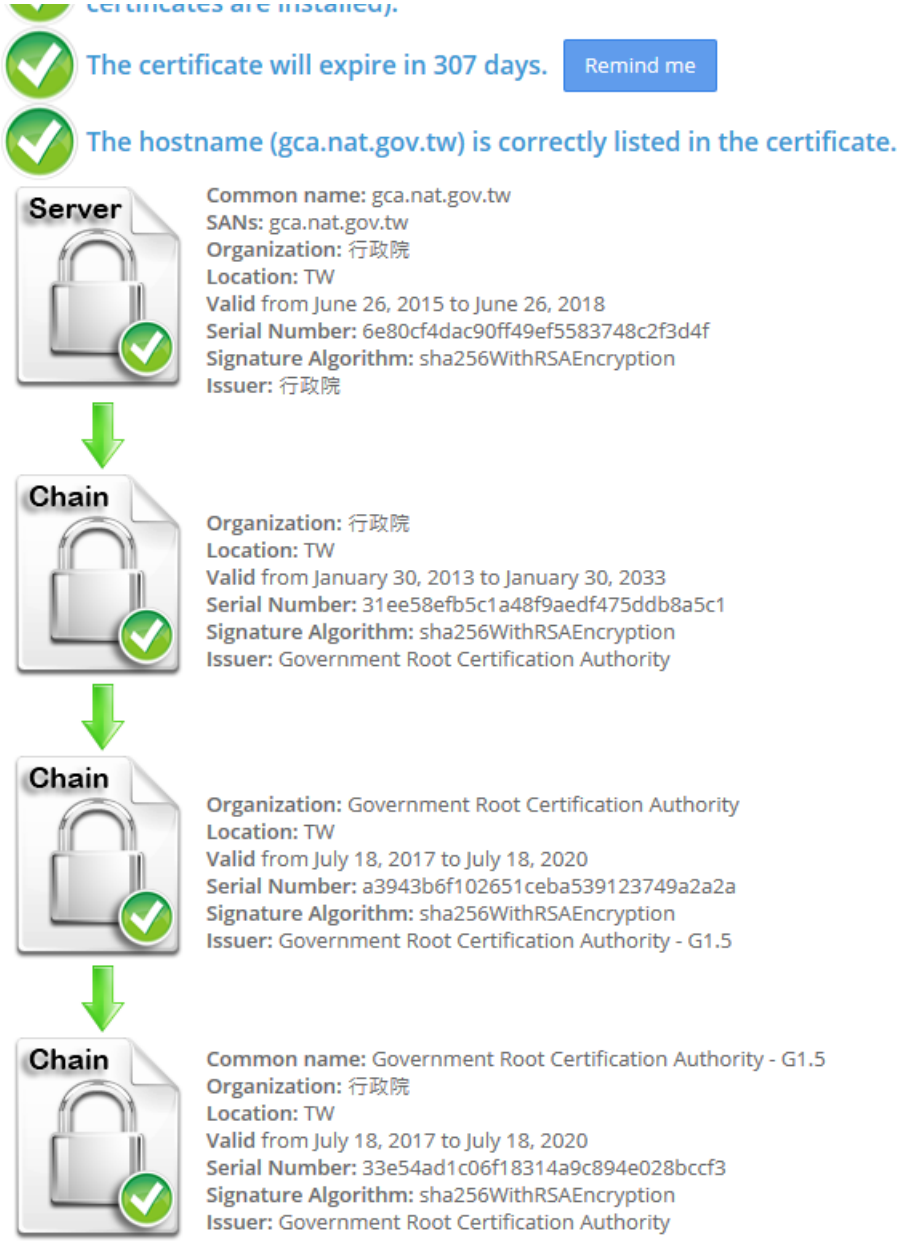
8. 將 Tomcat 重新啟動。

三、憑證串鍊檢測方式

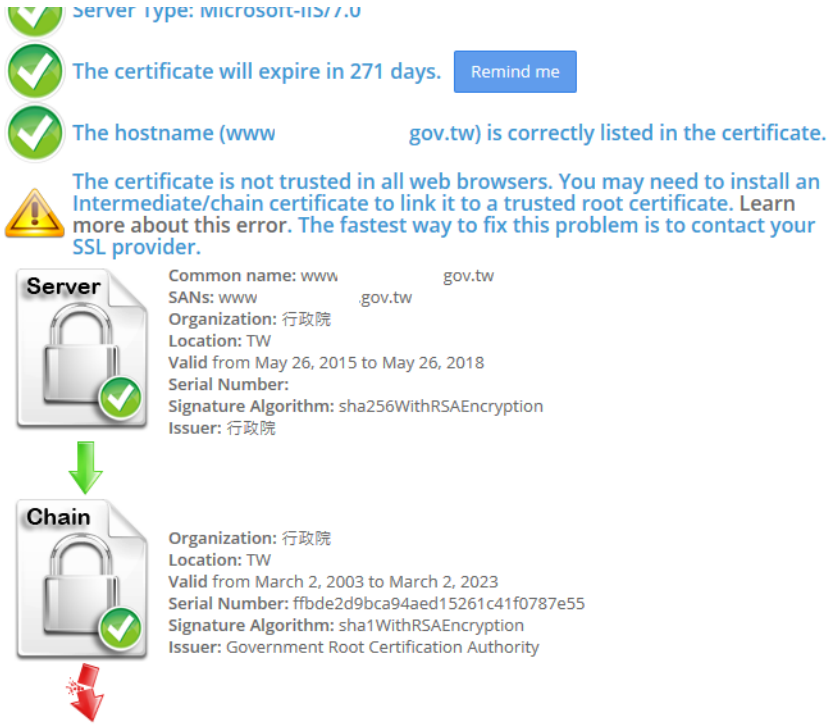
1. 可連線到 SSL Checker 網站

(https://www.sslshopper.com/ssl-checker.html)進行憑證串鍊檢測。

2. 正確的憑證串鍊檢測結果會類似下方截圖。



若憑證串鍊有錯誤，則會有紅色斷鍊，如下圖

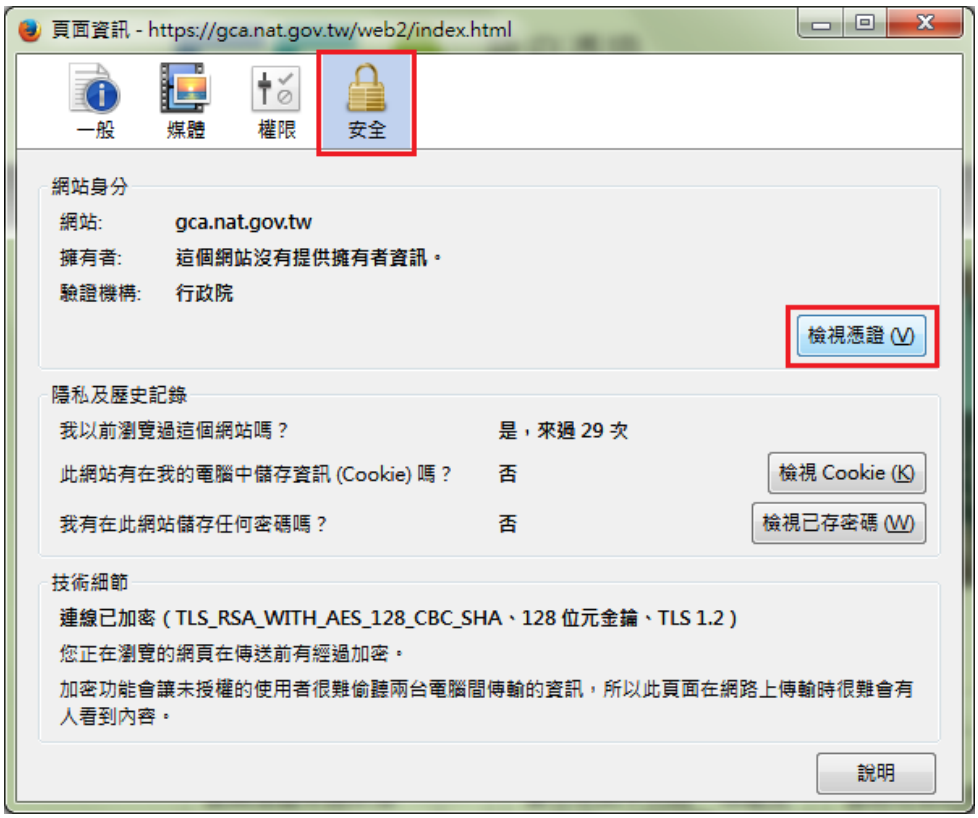


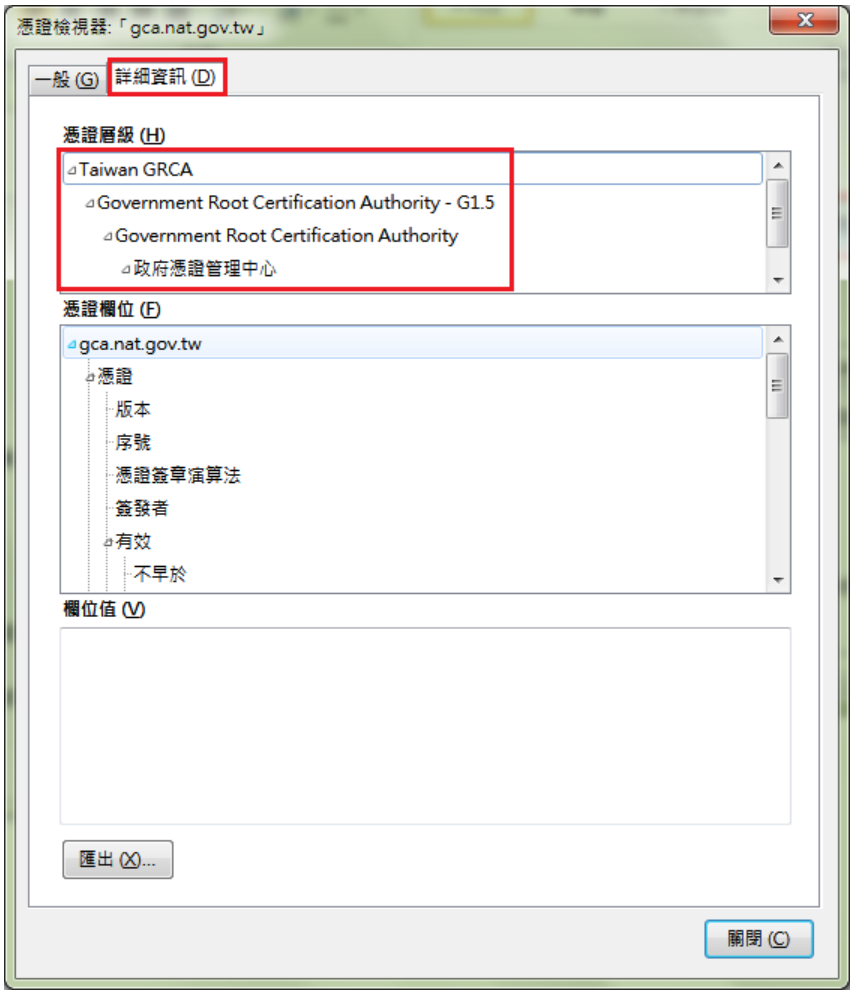
3. GCA SSL 5 層憑證串鍊為 **GRCA1 -> GRCA1_to_GRCA1_5 -> GRCA1_5_to_GRCA2 -> GCA2 -> SSL**，其中 GRCA1 為根憑證，針對根憑證的部分，瀏覽器會自行參考自己的憑證信賴清單決定是否信任，因此根憑證並不是 SSL 協定必須傳送的項目，故會因為不同的檢測網站或軟體而有顯示與不顯示根憑證的差異，若檢測結果只出現 4 層串鍊亦為正常現象，只要 Firefox 與 Android 手機能正常連線貴單位網站，即代表憑證串鍊安裝正確。

4. 亦可使用 Firefox 進行確認，詳細步驟如下


檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
GCA政府憑證管理中心
https://gca.nat.gov.tw/web2/index.html
gca.nat.gov.tw
安全連線
權限
您並未授予此網站任何特殊權限。
網站導覽 | 政府憑證總覽 | 關於GC
憑證作業
訊息公告
儲存庫
常用連結
最新憑證屆期通知
憑證申請
修改及補列印申請書
開卡作業
鎖卡解碼/重設PIN碼
用戶代碼重設
HiCOS卡片管理工具
政府電子採購網
政府標案查詢的好幫手
衛材藥品查


檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)
GCA政府憑證管理中心
https://gca.nat.gov.tw/web2/index.html
gca.nat.gov.tw
安全連線
驗證機構: 行政院
更多資訊
網站導覽 | 政府憑證總覽 | 關於GC
憑證作業
訊息公告
儲存庫
常用連結
最新憑證屆期通知
憑證申請
修改及補列印申請書
開卡作業
鎖卡解碼/重設PIN碼
用戶代碼重設
HiCOS卡片管理工具
政府電子採購網
政府標案查詢的好幫手
衛材藥品查


頁面資訊 - https://gca.nat.gov.tw/web2/index.html
一般
媒體
權限
安全
網站身分
網站: gca.nat.gov.tw
擁有者: 這個網站沒有提供擁有者資訊。
驗證機構: 行政院
檢視憑證 (V)
隱私及歷史記錄
我以前瀏覽過這個網站嗎？ 是，來過 29 次
此網站有在我的電腦中儲存資訊 (Cookie) 嗎？ 否
檢視 Cookie (K)
我有在此網站儲存任何密碼嗎？ 否
檢視已存密碼 (W)
技術細節
連線已加密 (TLS_RSA_WITH_AES_128_CBC_SHA、128 位元金鑰、TLS 1.2)
您正在瀏覽的網頁在傳送前有經過加密。
加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊，所以此頁面在網路上傳輸時很難會有人看到內容。
說明


憑證檢視器:「gca.nat.gov.tw」
一般 (G)
詳細資訊 (D)
憑證層級 (H)
Taiwan GRCA
Government Root Certification Authority - G1.5
Government Root Certification Authority
政府憑證管理中心
憑證欄位 (F)
gca.nat.gov.tw
憑證
版本
序號
憑證簽章演算法
簽發者
有效
不早於
欄位值 (V)
匯出 (X)...
關閉 (C)