

政府伺服器數位憑證管理中心(GTLSCA)
金鑰對未改變，僅更換 TLS 憑證操作手冊

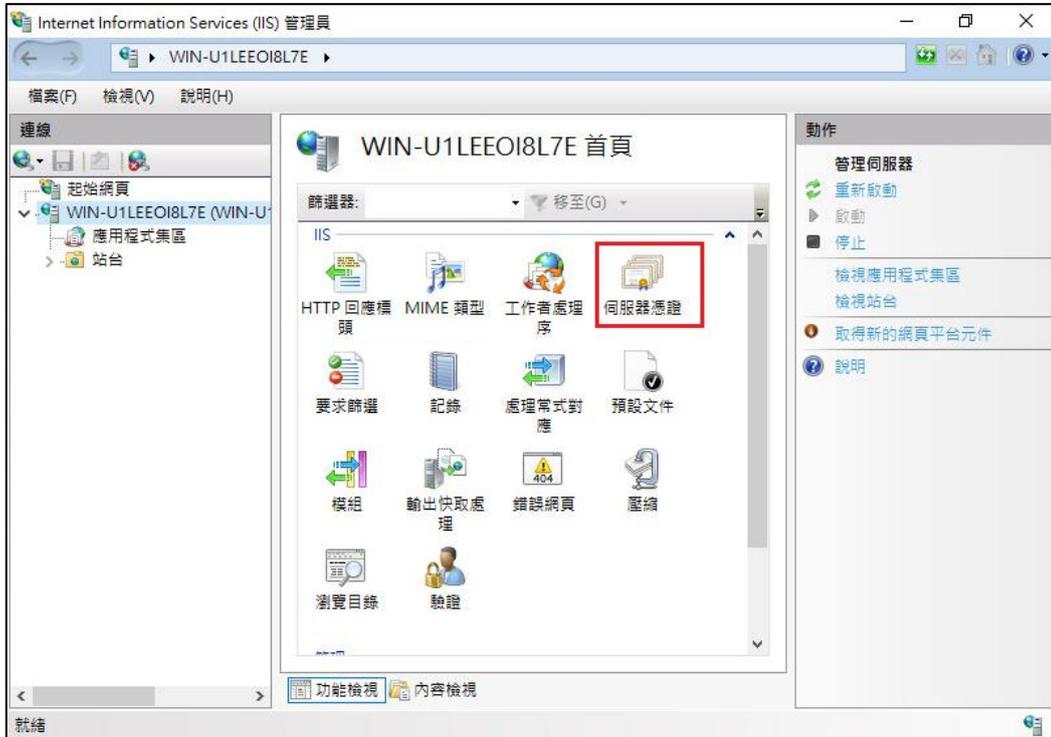
中華民國 113 年 5 月

目錄

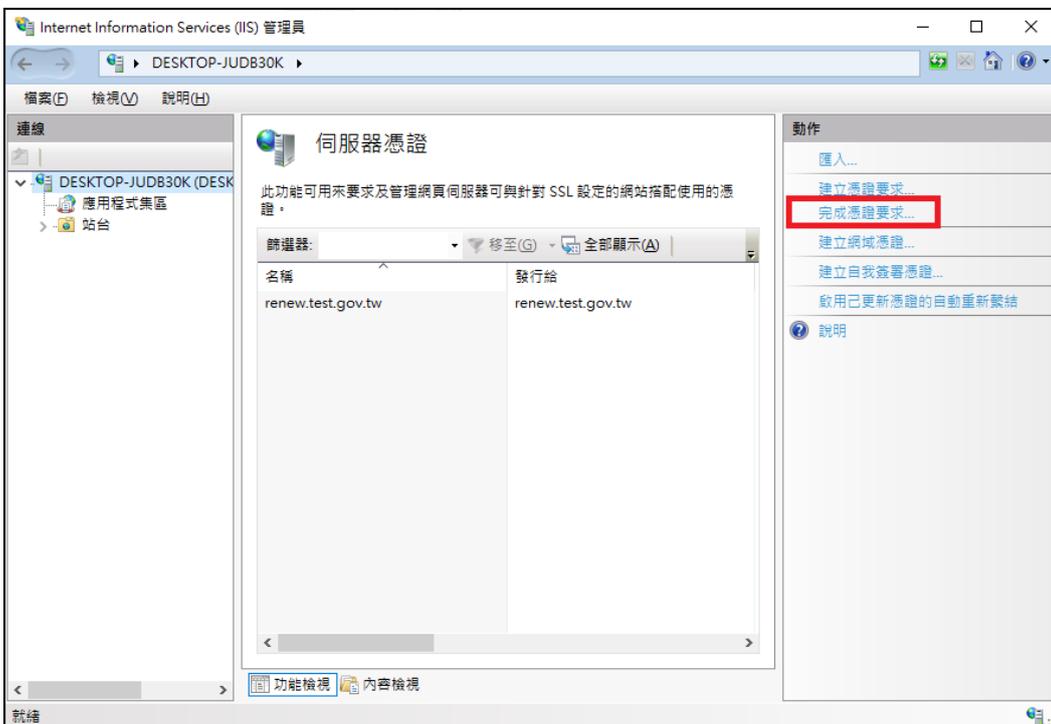
網站伺服器：IIS	3
網站伺服器：Apache	19
網站伺服器：Tomcat	23

網站伺服器：IIS

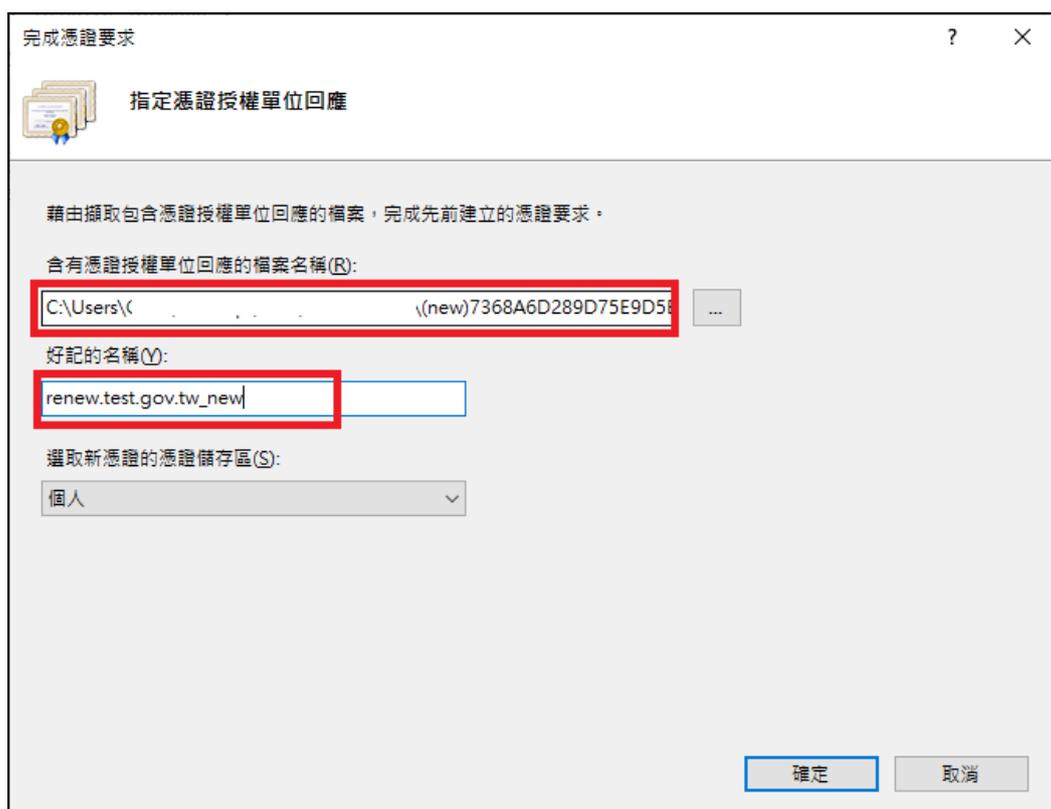
1. 開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



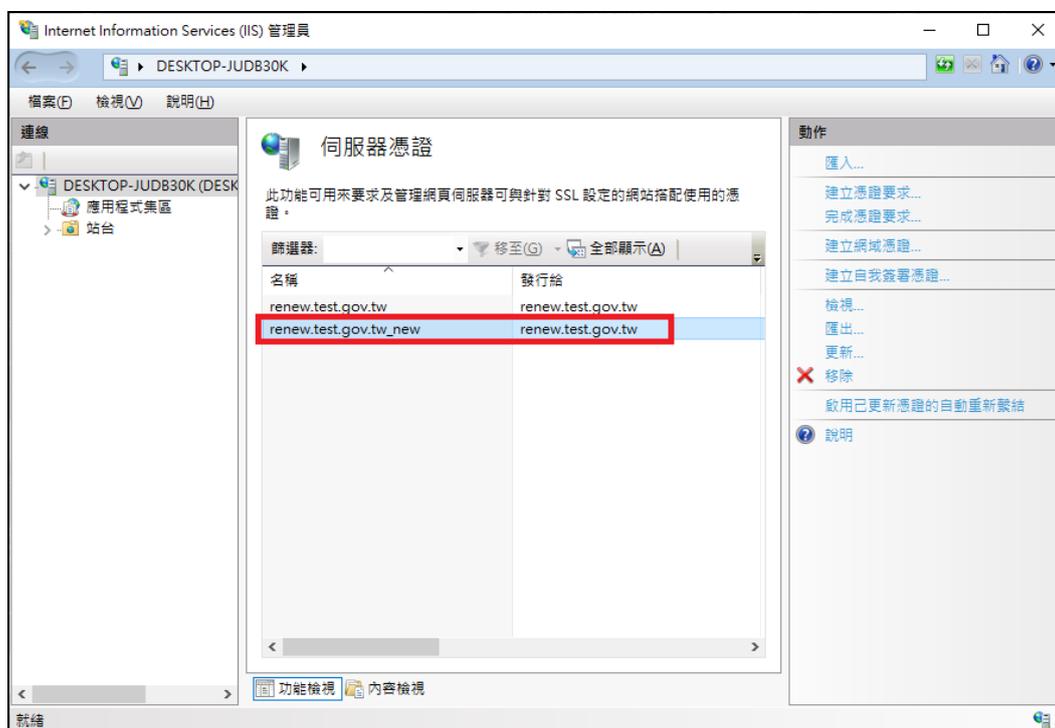
2. 點選「完成憑證要求」。(請確認原憑證是否已安裝於同一台伺服器裡。)



3. 選擇新的 TLS 憑證，並輸入好記的名稱。



4. 按「確定」，出現完成憑證要求的畫面，多一條新憑證列表。



5. 點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」。



6. 選擇已存在的 https 443 連接埠，點選「編輯」。



7. 重新選擇要安裝在此站台新的 TLS 憑證。(其餘設定皆不需變動)

編輯站台繫結

類型(T): https
IP 位址(I): 全部未指派
連接埠(P): 443

主機名稱(H):

需要伺服器名稱指示(N)

SSL 憑證(C):
renew.test.gov.tw_new

選取(L)... 檢視(V)...

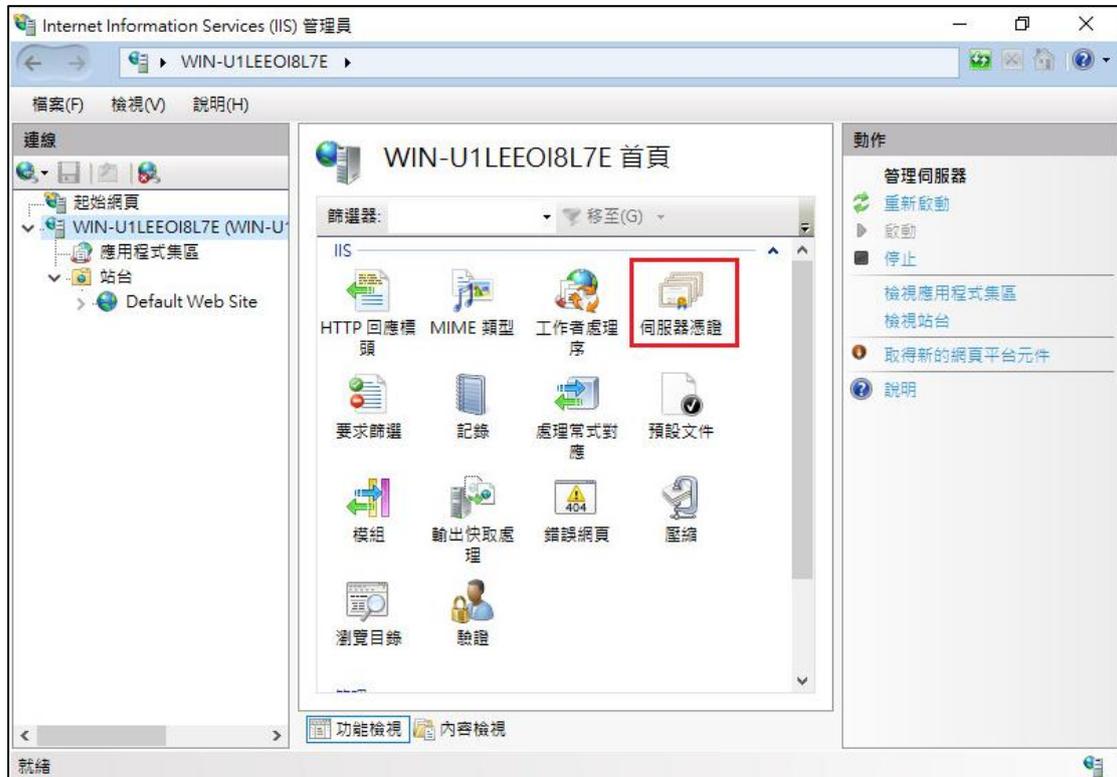
確定 取消

◆ 若因遠端連線匯入無法成功，可改下方操作方式。

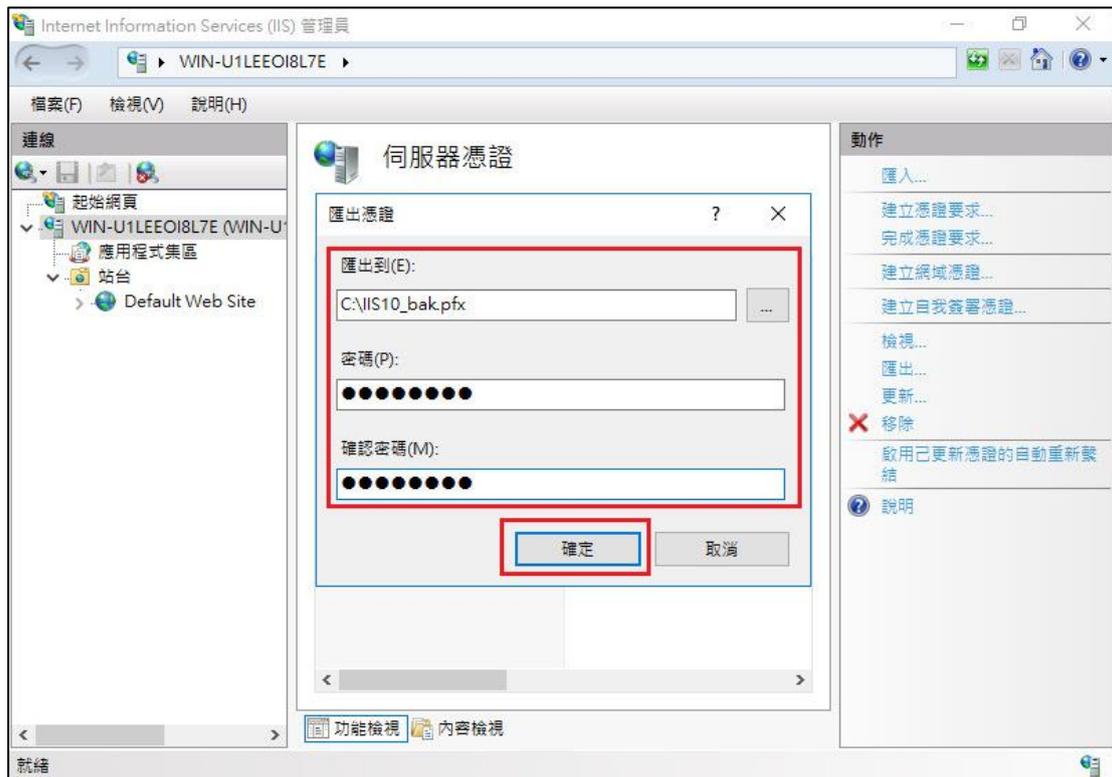
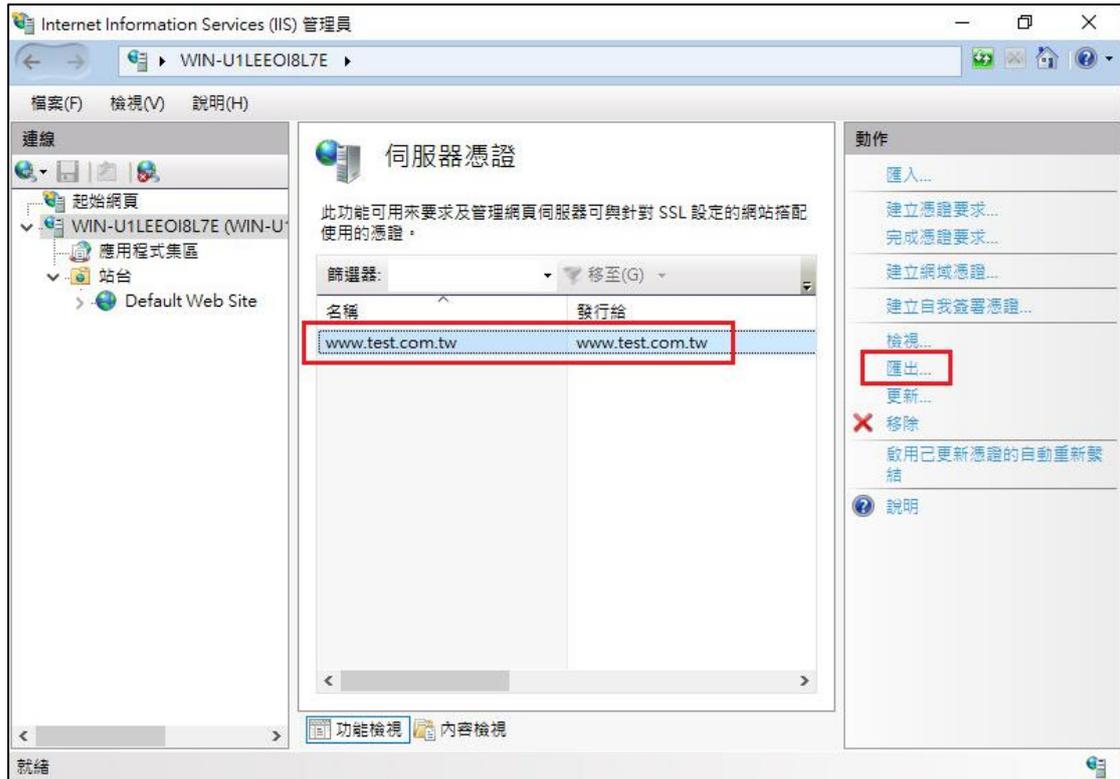
1. 請將原憑證備份匯出。

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

在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。

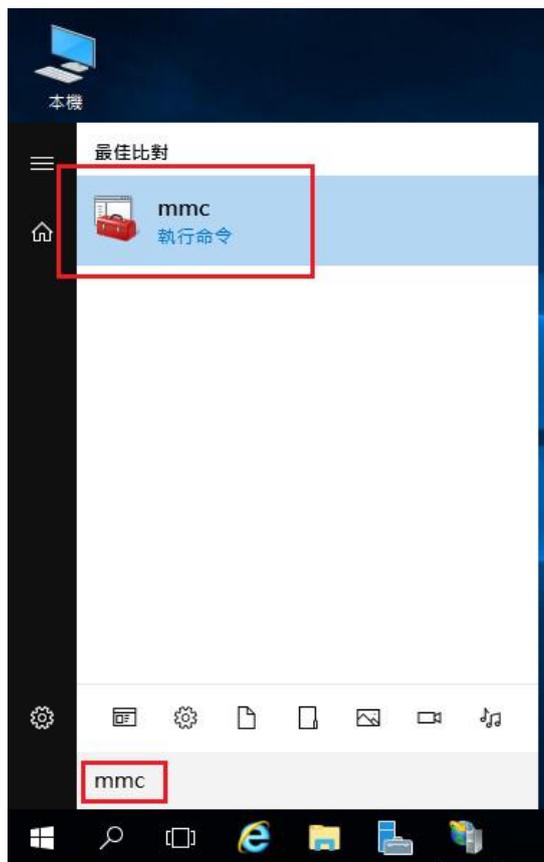


(2) 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

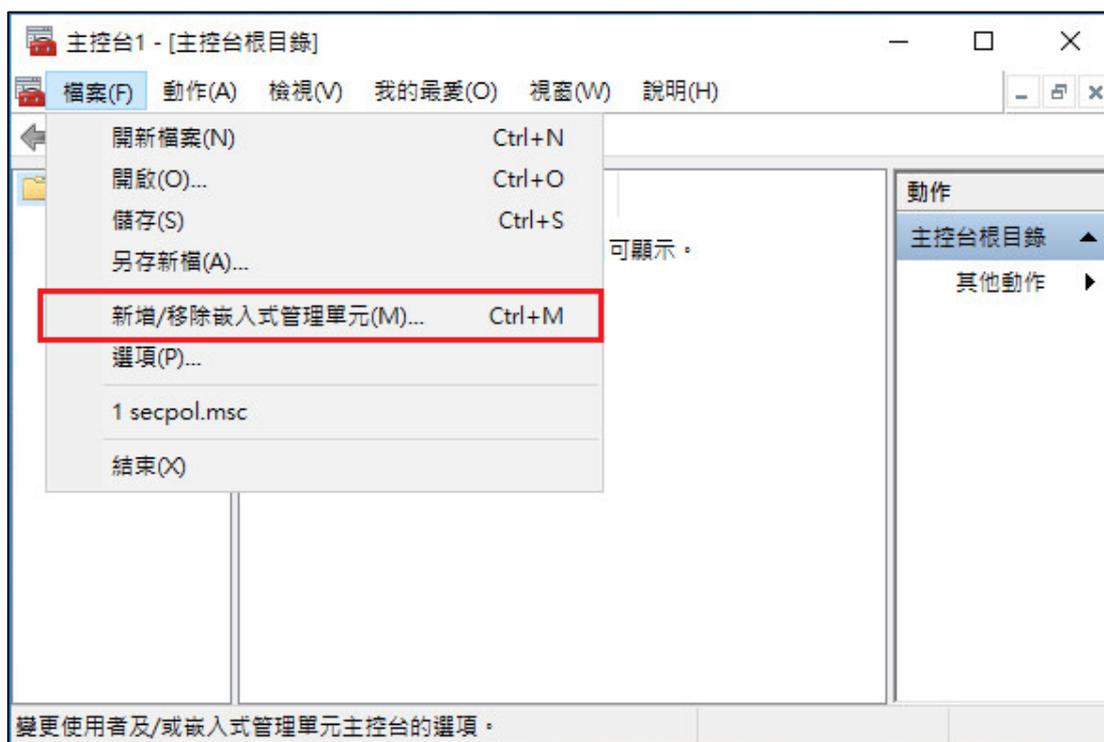


2. 將匯出的 PFX 檔匯入至其他有安裝 IIS 的電腦(請利用 mmc 匯入方式)。

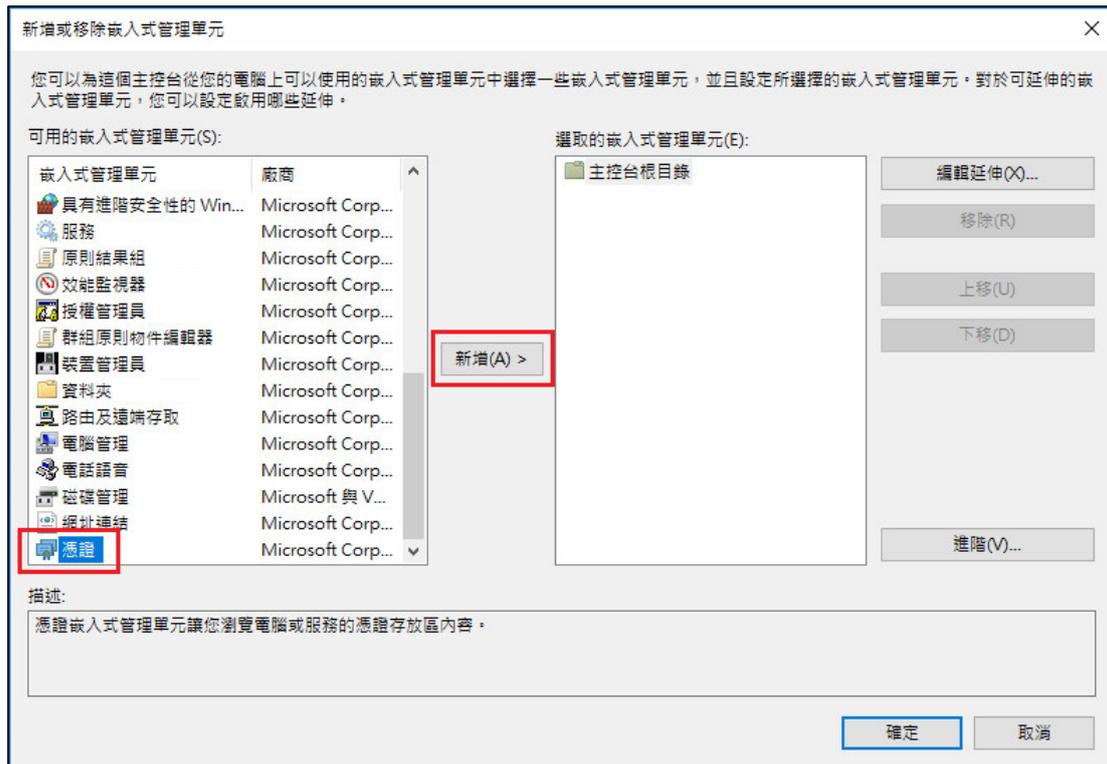
(1) 「開始」→「輸入 mmc」，按下「Enter」。



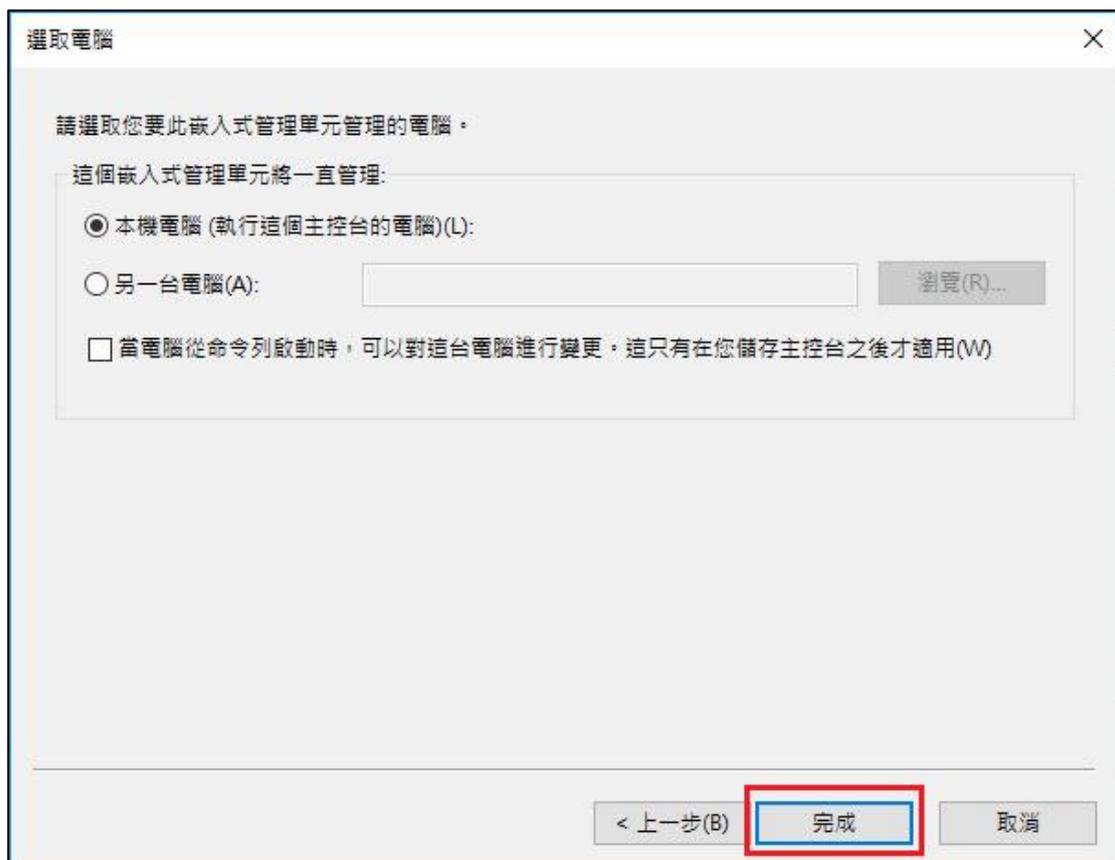
(2) 選擇「檔案」→「新增/移除嵌入式管理單元」。



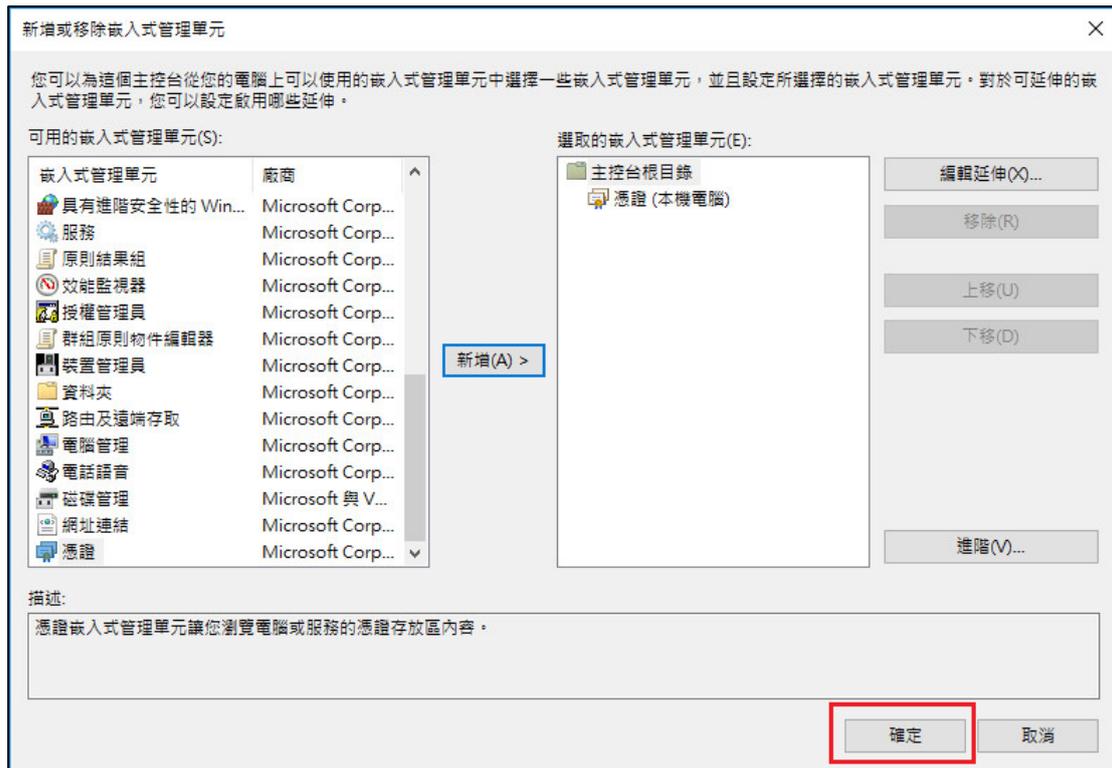
(3) 點選「憑證」→「新增」



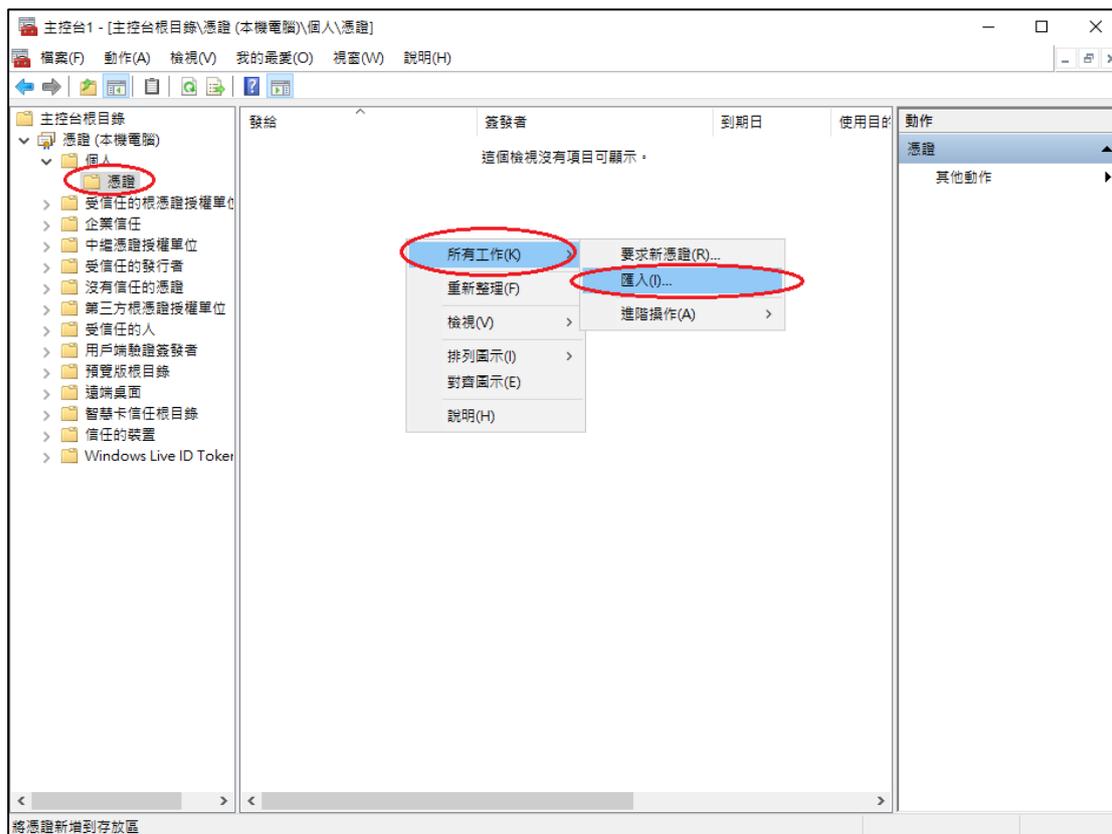
(4) 「電腦帳戶」→「下一步」→「完成」。



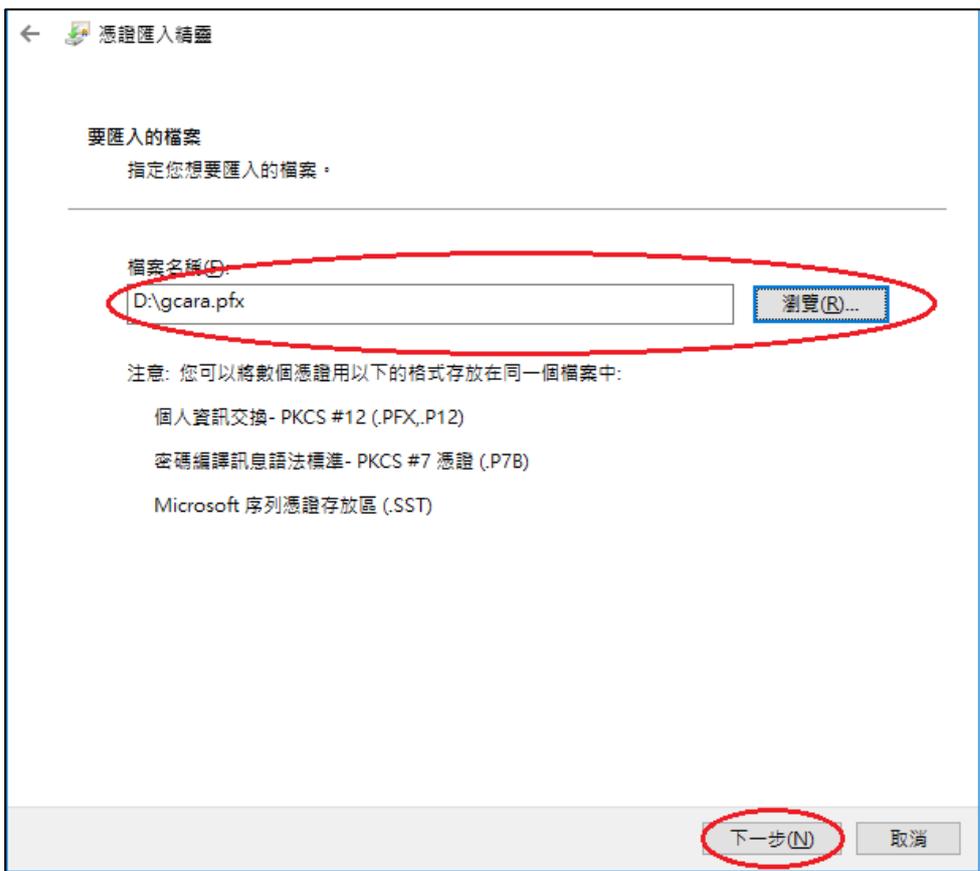
(5) 「確定」。



(6) 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」



(7) 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。



(8) 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

私密金鑰保護
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):
●●●●●●●●
 顯示密碼(D)

匯入選項(O):
 啟用強式私密金鑰保護。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)

下一步(N) 取消

← 憑證匯入精靈

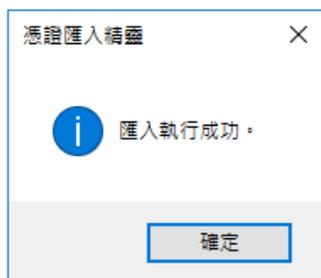
憑證存放區
憑證存放區是用來存放憑證的系統區域。

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)

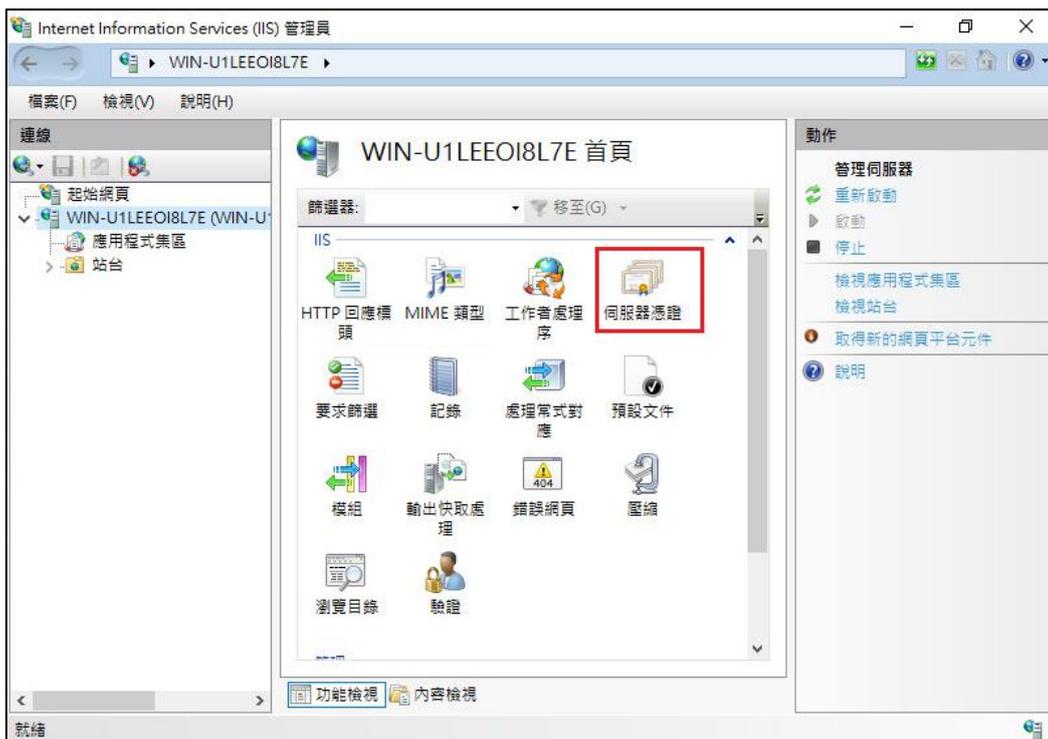
憑證存放區:
個人 瀏覽(R)...

下一步(N) 取消

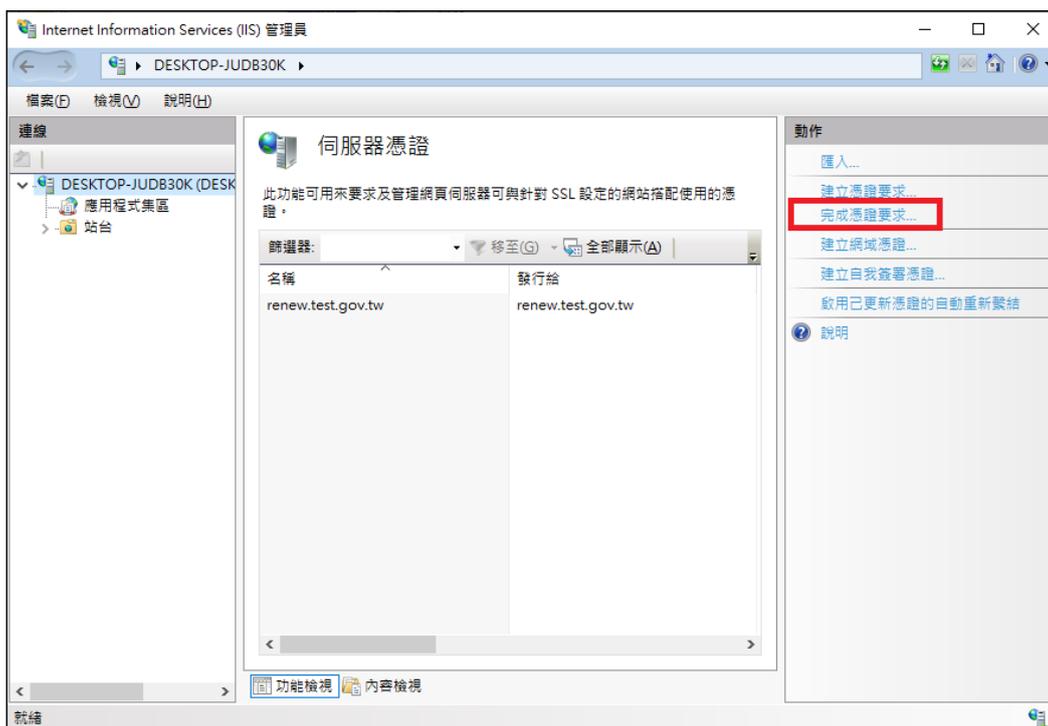


3. 於 IIS 完成註冊要求，匯入新憑證。

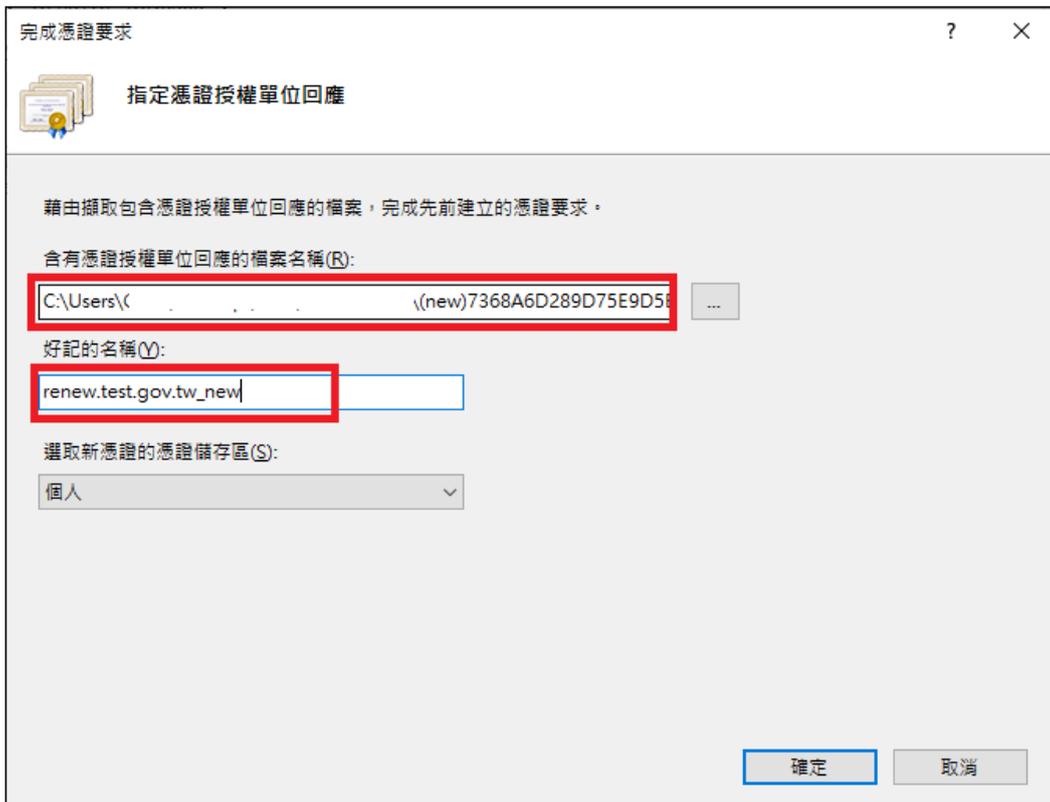
- (1) 開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



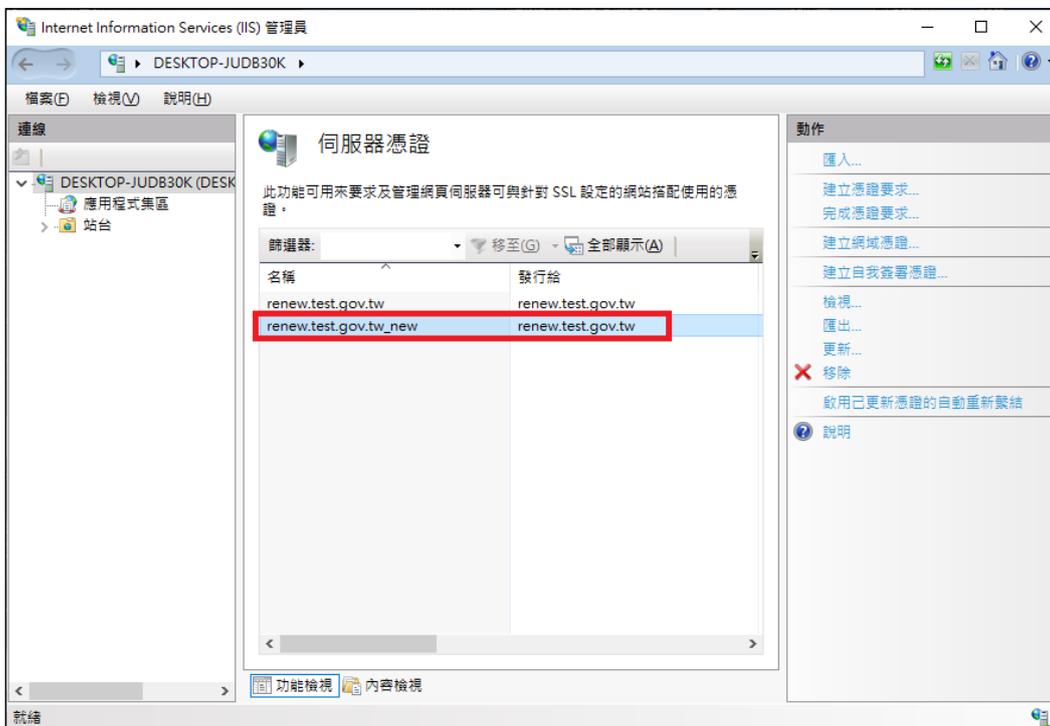
(2) 點選「完成憑證要求」。



(3) 選擇新的 TLS 憑證，並輸入好記的名稱。

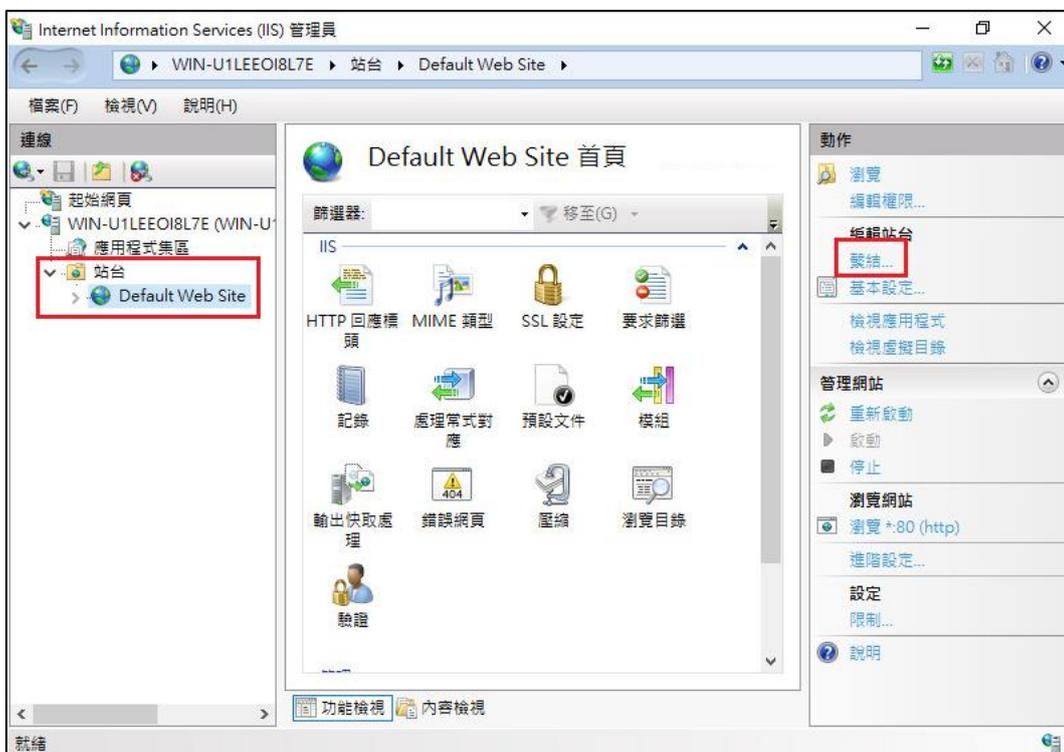


(4) 按「確定」，出現完成憑證要求的畫面，多一條新憑證列表。(請重新整理確認憑證沒有消失，將憑證點 2 下開啟確認是否有其對應的私鑰。)



4. 將與私鑰結合的新憑證匯出並匯入至原主機，於 IIS 站台繫結選取新憑證即可。

- (1) 匯出新憑證請參考第 1 點操作步驟(p.7 至 p.8)
- (2) 匯入新憑證請參考第 2 點操作步驟(p.9 至 p.14)
- (3) 至原主機開啟「Internet Information Services (IIS)管理員」，點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」。



(4) 選擇已存在的 https 443 連接埠，點選「編輯」。



(5) 重新選擇要安裝在此站台新的 TLS 憑證。

編輯站點屬性

類型(T): https IP 位址(I): 全部未指派 連接埠(O): 443

主機名稱(H):

關閉伺服器名稱指示(N)

SSL 憑證(E):

renew.test.gov.tw_new 選取(L)... 檢視(V)...

確定 取消

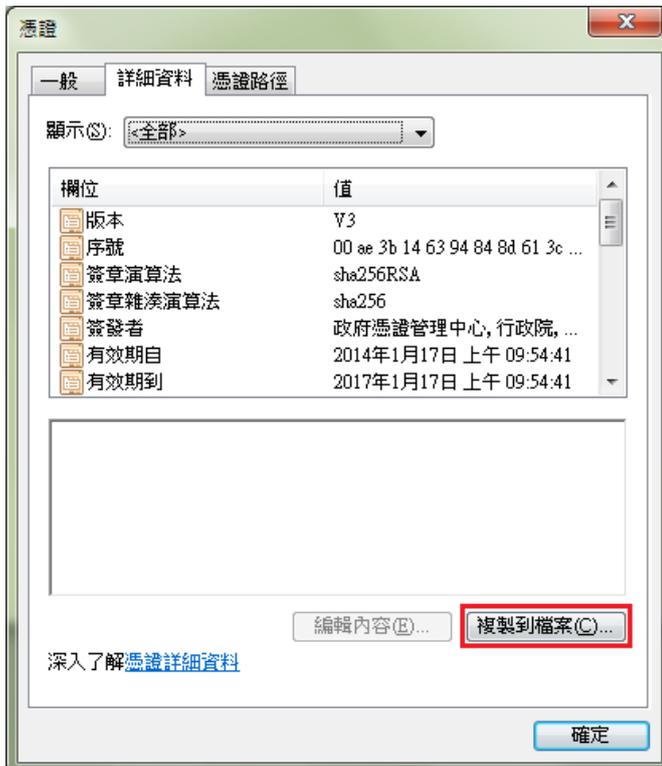
網站伺服器：Apache

1. 將憑證由 DER 格式轉換為 Base64 格式。

(1) 點選憑證檔案後，選擇詳細資料。



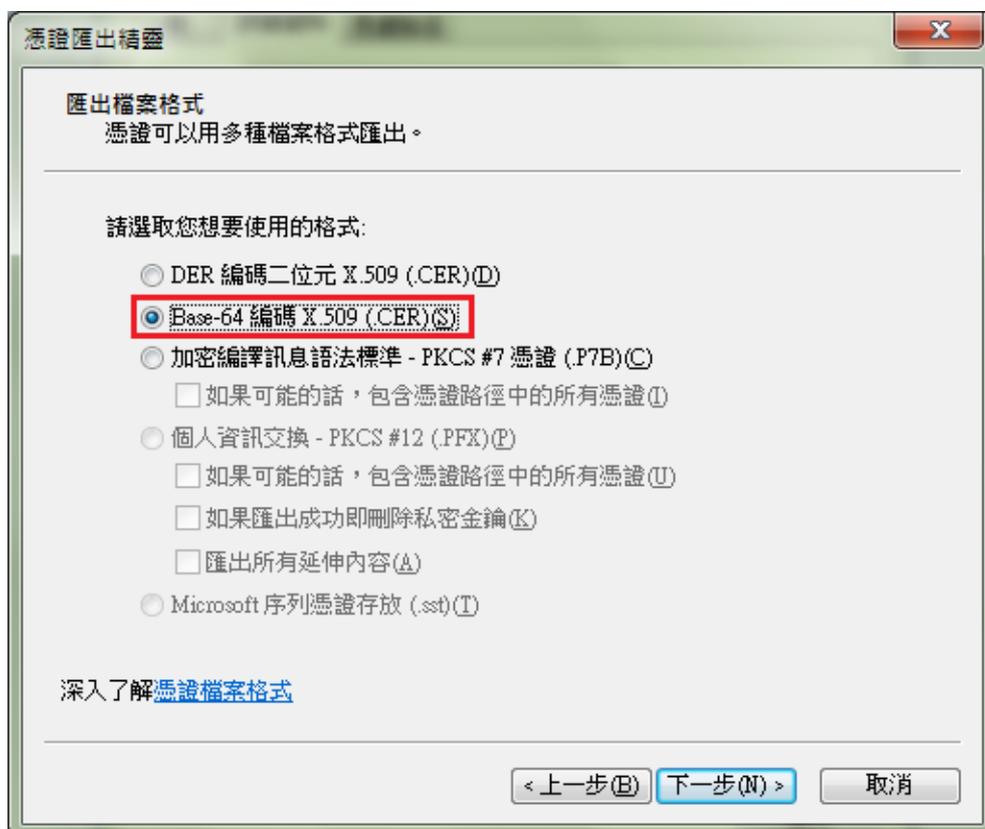
(2) 選擇複製到檔案。



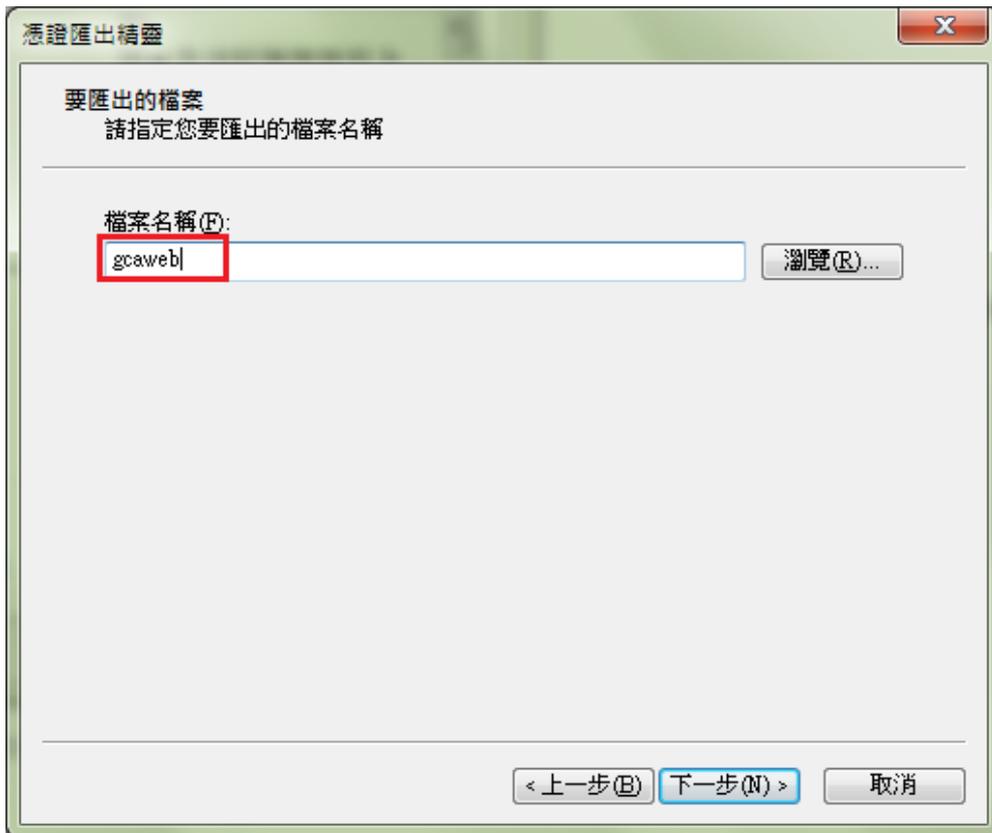
(3) 點選下一步。



(4) 選擇 Base64 編碼。



(5) 輸入檔案名稱。



(6) 完成轉換。

2. 以文字編輯器開啟 Base64 格式憑證，並與原憑證設定檔中的 TLS 憑證更換。

(1) 若 Apache 版本 < 2.4.8，請參考以下步驟操作

- i. 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 SSLCertificateFile：伺服器憑證(*.crt)檔案路徑。

(2) 若 Apache 版本 >= 2.4.8，請參考以下步驟操作

- i. 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。
- ii. 利用文字編輯器開啟原指定的憑證檔(範例為 sever.crt)，
SSLCertificateFile 參數指定之位址。

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

- iii. 將憑證檔內容最上面的原 TLS 憑證，更換為步驟 1 轉換成 Base64 格式的新 TLS 憑證內容，可參考下圖。

```
9KmS6KznEVKBRq7/w3SouQznO0wRGcS8TxOSvIkWfMDmeU2081kvqMmDLblLxpya
W4cljrcgogMqe3JzJSbN5rZBqgnQseAnV0HktCrs9MDig3Sd7yLpSrgLJIdlPvni
vA==
-----END CERTIFICATE-----
```

更換為新的TLS憑證

```
subject=/C=TW/O=\xE8\xA1\x8C\xE6\x94\xBF\xE9\x99\xA2/CN=\xE6\x94\xBF\xE5\xBA\x9C\xE4\xBC\x
issuer=/C=TW/O=Chunghwa Telecom Co., Ltd./CN=ePKI Root Certification Authority - G2
-----BEGIN CERTIFICATE-----
MIIGtjCCBJ6gAwIBAgIRAJltX+mt4Wzcjs2/7bFKMpUwDQYJKoZIhvcNAQELBQAw
YzELMAkGA1UEBhMCVFcxiZAhBgNVBAoMGkNodW5naHdhIFRlbGVjb20gQ28uLCBM
dGQumS8wLQYDVQQDDCZlUetJlFJvb3QgQ2VydGlmaWNhdGlvb1BBdXRob3JpdHkg
LSBHMjAeFw0xOTA3MTkwNjQ2NDVhFw0zMTA4MTkwNjQ2NDVhMFgxCzAJBgNVBAYT
AlRlRmRlEAYDVOQKkDAnooYzmlL/pmaIxNTAzBgNVBAMMLoUv+W6nOS8suuacjWZ
gOaVuOS9jeaGeit1teeuoeeQhuS4reW/gyAtIEcxMIICiJANBgkqhkiG9w0BAQEF
AAOCAg8AMIICGKCAgEAwg5R4LGoDj+mZIXmchMrYv501jsSLIm7EoX/Kat74uN2
yDR436V2EWkFwHd+TS4sx2/3JCRW+KE+IX8NYBKjsWuK9OMY4Gu4FEWJpBulXCW
YjTPKyhHdEhDpxRvx9l32k68XgK7j2U5sEzCPx13Qjkh7qc/Mo5BFiro8YsYafx
gCoa/rzFEsXy2KXRJeIDw7t+1PxVy2cbQ0Unlo09670LGoOVzYVkyABv3IwZo+JR
tj+tj7rLjB7xQKYmfJOA2Jc96yPm6l17zHrIQYfohGPDANmWR9opNNqY0o+LtsIYo
t3/cLp9YgAaiGdrA1KrbBEVkyH+zKzAHolf5mPBn+h3OElyfygESitWRBp2bwfOG
JwAYseTuorQHpyQps1GGcn9vcfnLhvLxa3DMrCAvSjB3SvHCyqahQz0KROIPcu+V
LW3icaqlbJausGIGYqp8VSN6FJ0pgmYdbunBLYclv23VvjmVml+xNJoasFEUscmS
gA4CuYANhKWSANK8HI9rNbvmyuyWhSv7tUXY6UB67mHp4ypGcKYbXrj1Kqahv6QL
UEb7S8FD7lDs75F2vMeO407716j0Bs/L2E6WZJvSronzJcXL0IwmpYaOaSoFOf0e
GVsPBVKn+z4Bq0WA0+r7plfWofDbUGmx92un++rWhoDXrma+odubNlXj1Rj1L3sC
AwEAAaOCAN4wggFqMB8GAlUdIwQYMBaAFHJbuqpyOO4lkCS1lCL6CYjKiwr7MB0G
AlUdDgQWBBT6y2dyf4ru3CILrgHsVmw9IMiajAOBgNVHQ8BAf8EBAMCAYYwPAYD
VR0fBDUwMzAxOC+gLYYraHR0cDovL2VjYS5oaW5ldC5uZXQvcnVwb3NpdG9yeS9D
UkwyL0NBLmNybDcBggYIRwYBBQUHAQEEdjB0MDsGCCsGAQUFBzAChi9odHRhOi8v
ZWNhLmhhpbmV0Lm5ldC9yZXBvc2l0b3J5L0NlcnRzL2V2DQUCyLmNydDALBgggBgEF
BQcwAYYpAHR0cDovL29jc3AuZWNhLmhhpbmV0Lm5ldC9PQlNQL29jc3BHMnNoYTIw
EgYDVR0TAQH/BAgwBgEB/wIBADAiBgNVHSAEGzAZMA0GCysGAQQBgbgcjZAADMAGG
EmeBDAECAjAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcN
AQELBQADggIBAeyrsJ9vU16nEfw00vgAoFeFXpCRF+uDsMG/8F6OV9VRnbtzBwaz
HbxVmaBvDRVofLfoXWtr+Nd8dd3BXVUNxemNrkZa8Hdgdv4s8yFbrs0W6fRTWkhCc
c39RpQtSeV7kyxCP1rMTVRSqCA9F+FcdMLXJiZzrz17Tn6guIyqcfzV6sRN7CbbT
rYKSc0JX4t26WGFun2zLjzH8kx1T2457TE4yyj1loSzdgiWL6Hz7l+nbTe6WqPVV
m4am2AamaQaLgnceGlae17PIHx9Nc4sy7KdOMTc5r0BPCGhAiJ6ueQ6aVd49pra7
BDIQFMA7Myy4pXRYfqFnjq9RuROWYiIluzLNUSxlaPtTMUVQnWjJxn1X1BDLX9L4
OAXToVdbtcNNSlGK+WlcWiYdTOWF4HTu5pvdUn/+8yVE4E7MPb0vGuxv3S1lQG6J
tVPuHkX6BGqRXHo253gY77HZU0g3g9qVs9Ua2jWS5UTcqdqLmmOQnH7USAJ9/4rX
Ru/P8IWMPG2s6tvlDRVQV5xfq2lPQ4y53ytVd0+/lp0L743+1AjnOw0I8t9QxP6c
2ti+oo43rxm8YE3etVLQBeWsmJc00GOWa/XmFACsy8Lkctx0QScAAyWcFB2accfx
j9hEXlc6MAeVUVp04YJx4dtjoiFTPIl/MFX+PkxMq4Fs6k+mxSm7tNvv
-----END CERTIFICATE-----
```

憑證串鍊內容不動

```
subject=/C=TW/O=Chunghwa Telecom Co., Ltd./CN=ePKI Root Certification Authority - G2
issuer=/C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority
-----BEGIN CERTIFICATE-----
MIIEhDCCBWCgAwIBAgIQO+7gkY6IhqlGD+iukQycujANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJVUzEjMCEGAlUECgwaQ2h1bmdod2EgVGVzZWNvbSBDb3R5IEEx0
```

- iv. 將修改後的 TLS 憑證檔案存檔，檔案放置路徑跟原本 SSLCertificateFile 參數相同。
3. 重新啟動 Apache Server。

網站伺服器：Tomcat

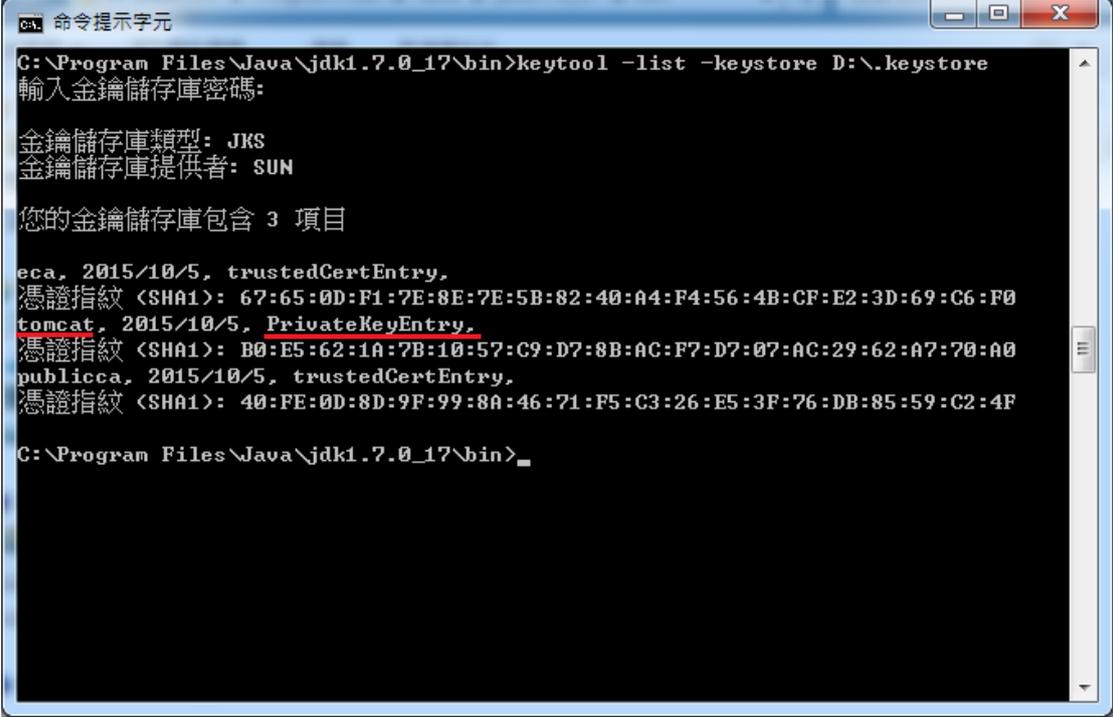
1. 請直接於原憑證安裝的 Keystore 重新匯入新憑證即可。

(1) 確認 PrivateKeyEntry 的 alias name

在 %JAVA_HOME%\bin 目錄下執行

keytool -list -keystore <keystore 檔案所在路徑>

- 待出現 Enter keystore password：請輸入密碼。
- 找到 PrivateKeyEntry 對應的 alias name，範例為 tomcat



```
ca. 命令提示字元
C:\Program Files\Java\jdk1.7.0_17\bin>keytool -list -keystore D:\.keystore
輸入金鑰儲存庫密碼:
金鑰儲存庫類型: JKS
金鑰儲存庫提供者: SUN
您的金鑰儲存庫包含 3 項目
eca, 2015/10/5, trustedCertEntry,
憑證指紋 <SHA1>: 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0
tomcat, 2015/10/5, PrivateKeyEntry,
憑證指紋 <SHA1>: B0:E5:62:1A:7B:10:57:C9:D7:8B:AC:F7:D7:07:AC:29:62:A7:70:A0
publicca, 2015/10/5, trustedCertEntry,
憑證指紋 <SHA1>: 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F
C:\Program Files\Java\jdk1.7.0_17\bin>_
```

(2) 匯入新的 TLS 伺服器應用軟體憑證。

在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias <PrivateKeyEntry 的 alias name> -file D:\(憑證名稱.cer) -keystore <keystore 檔案所在路徑>

- 待出現 Enter keystore password：請輸入密碼。

◆ 若直接於 Keystore 安裝新憑證有問題，也可參考以下方式安裝新憑證。

1. 先執行以下指令得到 keystore(jks 檔)裏含有私鑰(PrivateKeyEntry)的 alias name

keytool -list -keystore tomcat.jks



```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。

C:\certtemp\1118>keytool -list -keystore server.jks
Enter keystore password:
Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

tomcat, 2022年9月29日, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 66:29:F1:AF:DF:FE:CF:6A:2E:78:86:EE:70:5C:F2:1F:A3:AB:B1:C2:66:6D:85:F1:34:88:FF:1C:8E:FE:04:B6

Warning:
<tomcat> #4 of 4 uses the SHA1withRSA signature algorithm which is considered a security risk. This algorithm will be disabled in a future update.
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore server.jks -destkeystore server.jks -deststoretype pkcs12".
```

2. 執行以下 keytool 指令，將 JAVA Keystore (JKS) 轉檔為 PFX 檔

keytool -importkeystore -srckeystore tomcat.jks -destkeystore server.pfx -srcstoretype jks -deststoretype pkcs12 -srcalias tomcat

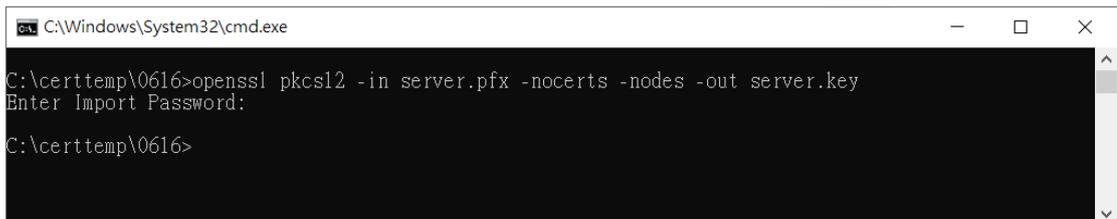


```
C:\Windows\System32\cmd.exe

C:\certtemp\1118>keytool -importkeystore -srckeystore server.jks -destkeystore server.pfx -srcstoretype jks -deststoretype pkcs12 -srcalias tomcat
Importing keystore server.jks to server.pfx...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
```

3. 得到 PFX 檔案(範例為 server.pfx)後，再到有安裝 openssl 的電腦執行下面的指令，這樣就會得到私鑰 server.key

openssl pkcs12 -in server.pfx -nocerts -nodes -out server.key



```
C:\Windows\System32\cmd.exe

C:\certtemp\0616>openssl pkcs12 -in server.pfx -nocerts -nodes -out server.key
Enter Import Password:

C:\certtemp\0616>
```

4. 重新至以下連結下載憑證串鏈檔，再依後續步驟執行

https://gtlscn.nat.gov.tw/download/GTLSCA_All.zip

5. 重新至 GCP 網站下載已簽發憑證，並命名為 install.crt，並依以下指令將 DER 格式憑證轉換為 B64 格式憑證，此處刻意將另存的 Base64 格式憑證命名為 install_B64.crt

openssl x509 -inform der -in install.crt -out install_B64.crt

6. 以文字編輯器開啟 install_B64.crt，並將憑證串鏈檔 GTLSCA_All.zip 解開之所有憑證依下列順序以文字編輯器開啟，並全選貼至 install_B64.crt 後存檔，檔案大小約 11kb，此時 install_B64.crt 即具備所有中繼憑證。

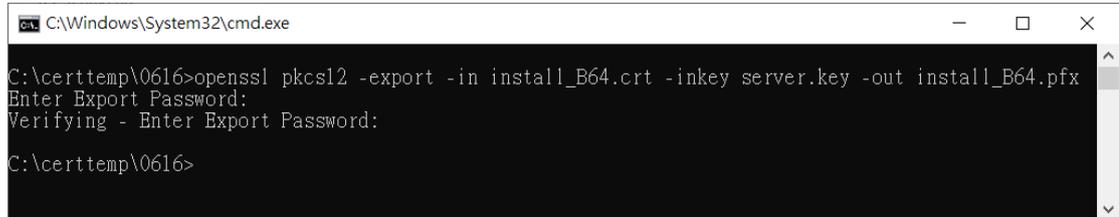
憑證順序由上而下為 install_B64.crt -> GTLSCA.crt -> eCA1_to_eCA2-New.crt -> ROOTeCA_64.crt

*linux: cat install_B64.crt GTLSCA.crt eCA1_to_eCA2-New.crt ROOTeCA_64.crt > server.crt ,

再將 server.crt 改名為 install_B64.crt 以進行後續步驟

7. 將憑證及私鑰依以下步驟再次轉換為 pfx 格式

openssl pkcs12 -export -in install_B64.crt -inkey server.key -out install_B64.pfx

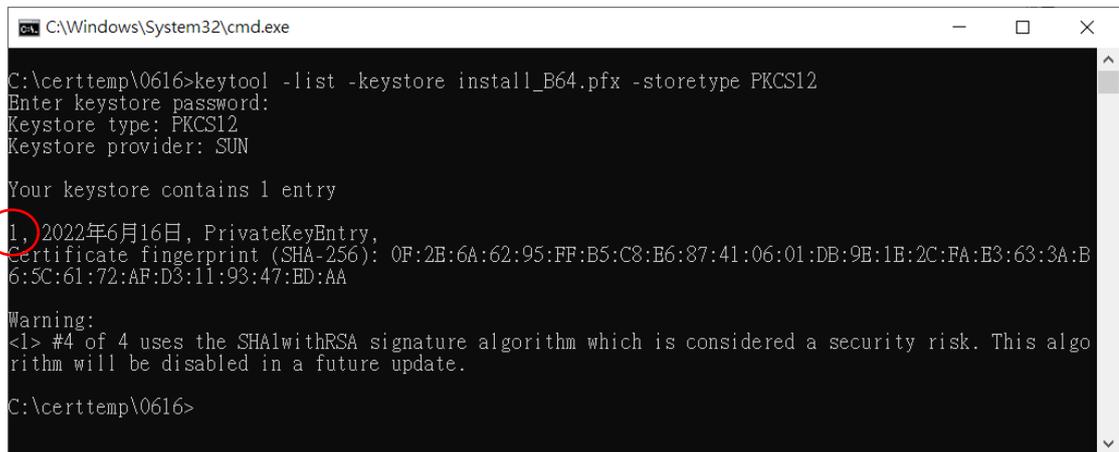


```
C:\Windows\System32\cmd.exe
C:\certtemp\0616>openssl pkcs12 -export -in install_B64.crt -inkey server.key -out install_B64.pfx
Enter Export Password:
Verifying - Enter Export Password:
C:\certtemp\0616>
```

8. 將 pfx 轉換為 jks 格式

(1) 先以底下指令得到 pfx 檔私鑰(PrivateKeyEntry)的 alias name(下圖紅框處)

keytool -list -keystore install_B64.pfx -storetype PKCS12



```
C:\Windows\System32\cmd.exe
C:\certtemp\0616>keytool -list -keystore install_B64.pfx -storetype PKCS12
Enter keystore password:
Keystore type: PKCS12
Keystore provider: SUN

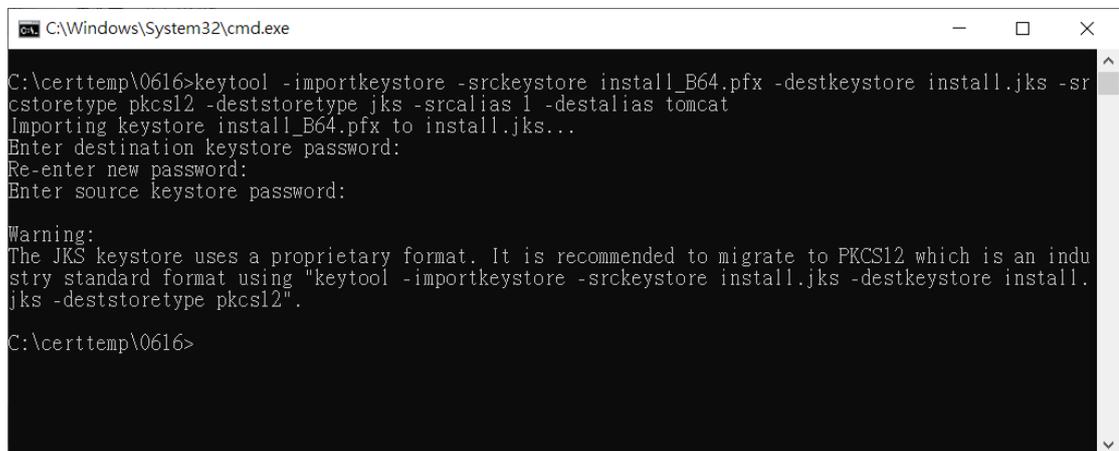
Your keystore contains 1 entry

1. 2022年6月16日, PrivateKeyEntry,
Certificate fingerprint (SHA-256): 0F:2E:6A:62:95:FF:B5:C8:B6:87:41:06:01:DB:9E:1E:2C:FA:E3:63:3A:B
6:5C:61:72:AF:D3:11:93:47:ED:AA

Warning:
<1> #4 of 4 uses the SHA1withRSA signature algorithm which is considered a security risk. This algo
rithm will be disabled in a future update.
C:\certtemp\0616>
```

(2) 依前述得到的 alias name 填入下列指令，以將 pfx 轉檔為 install.jks(alias name 為 tomcat，可自行替換)

keytool -importkeystore -srkeystore install_B64.pfx -destkeystore install.jks -srcstoretype pkcs12 -deststoretype jks -sralias 1 -destalias tomcat



```
C:\Windows\System32\cmd.exe
C:\certtemp\0616>keytool -importkeystore -srkeystore install_B64.pfx -destkeystore install.jks -sr
cstoretype pkcs12 -deststoretype jks -sralias 1 -destalias tomcat
Importing keystore install_B64.pfx to install.jks...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an indu
stry standard format using "keytool -importkeystore -srkeystore install.jks -destkeystore install.
jks -deststoretype pkcs12".
C:\certtemp\0616>
```