# SSL 憑證 IIS 及 Tomcat 格式互轉

# 說明手冊

臺灣網路認證股份有限公司
**TAIWAN-CA. Inc.**
台北市 100 延平南路 85 號 10 樓
電話:02-2370-8886
傳真:02-2370-0728
**www.twca.com.tw**

機密等級：公開
版本：V5.0
文件編號：MNT-03-161
生效日期： 109 年 3 月 3 日

# 目　　錄

# 1.目的

1.1. 介紹 SSL 憑證 IIS 及 Tomcat 格式互轉步驟及 SSL 伺服器數位憑證安裝說明。

1.2. 符合本公司資訊安全政策之規範。

# 2.範圍

2.1. 本操作手冊適用於 IIS 或 Tomcat 伺服器憑證格式互轉。

# 3.參考資料

無。

# 4.定義

無。

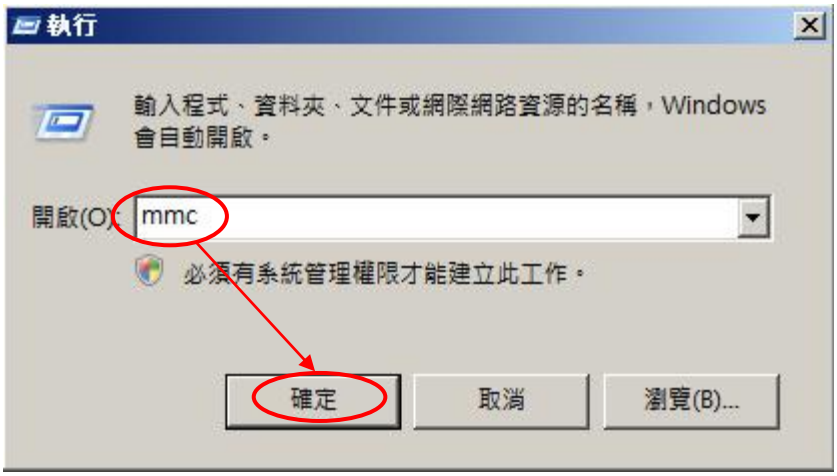
# 5.作業程序

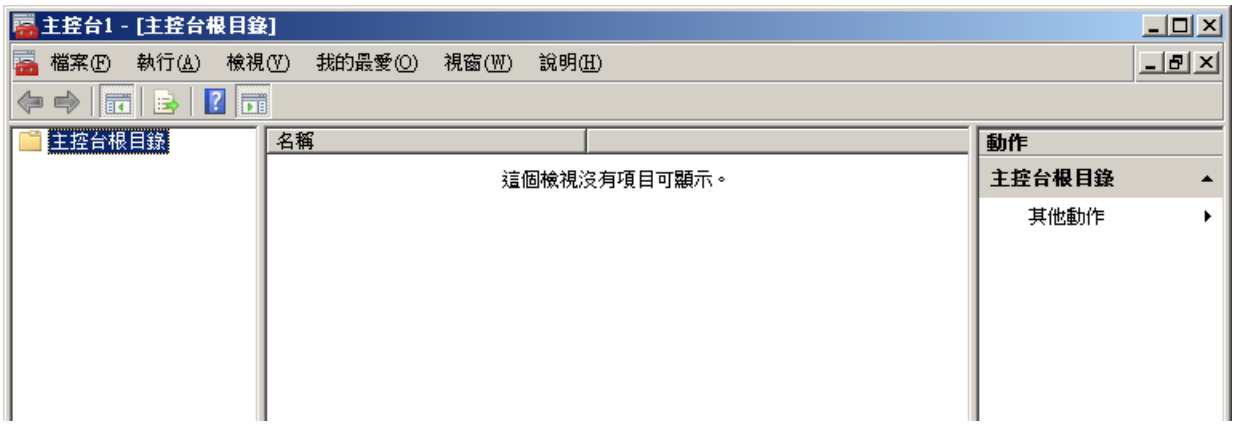
## 5.1 IIS 轉 TOMCAT 格式

### 5.1.1 新增憑證管理單元

#### 5.1.1.1 開啟 MMC 主控台

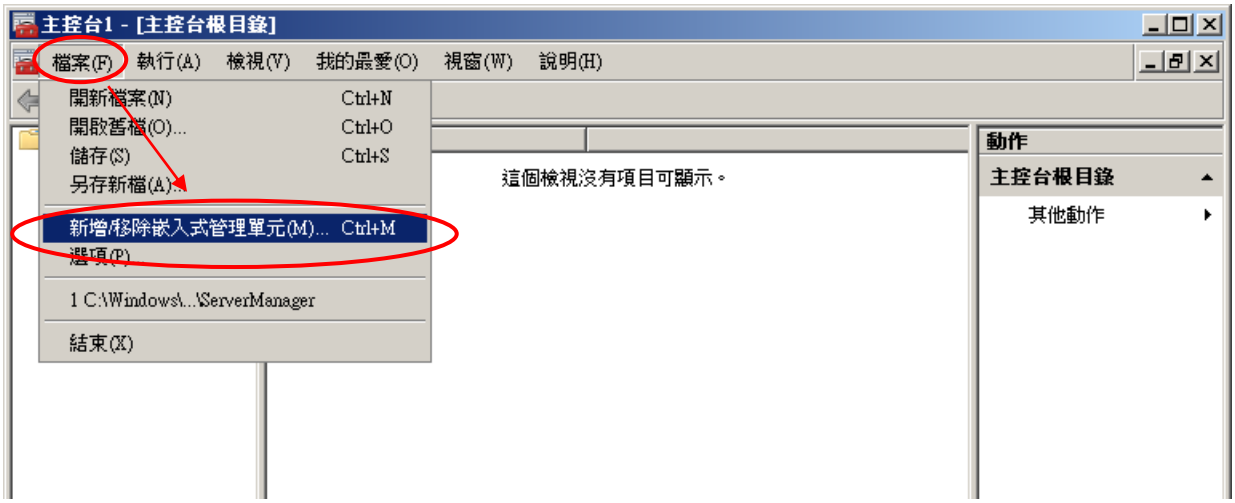
點選開始→點選執行→輸入 mmc 並按下確定。



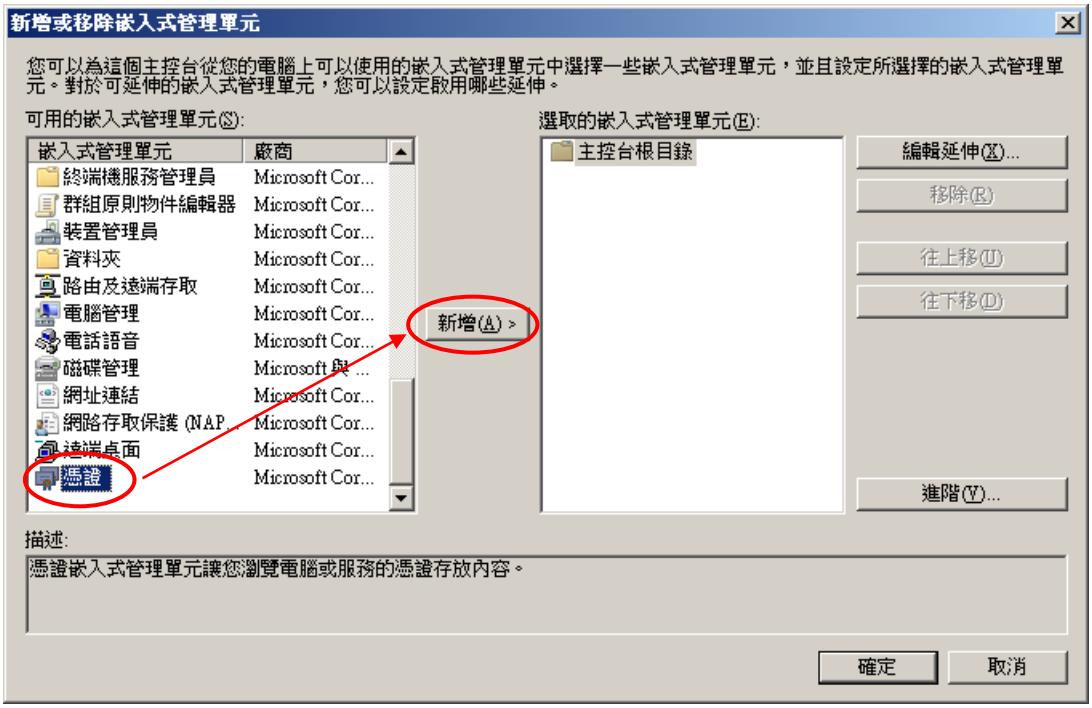

#### 5.1.1.2 新增/移除嵌入式管理單元

點選檔案→點選新增/移除嵌入式管理單元。



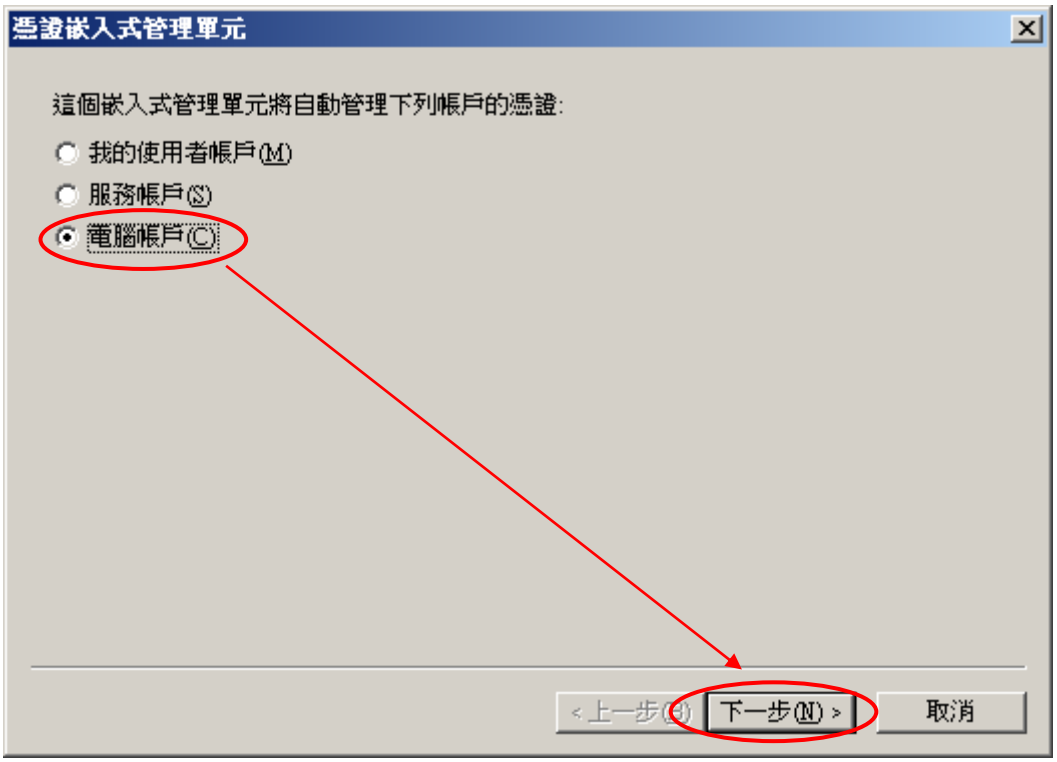

### 5.1.1.3 新增憑證管理單元(1)

點選憑證→點選新增。



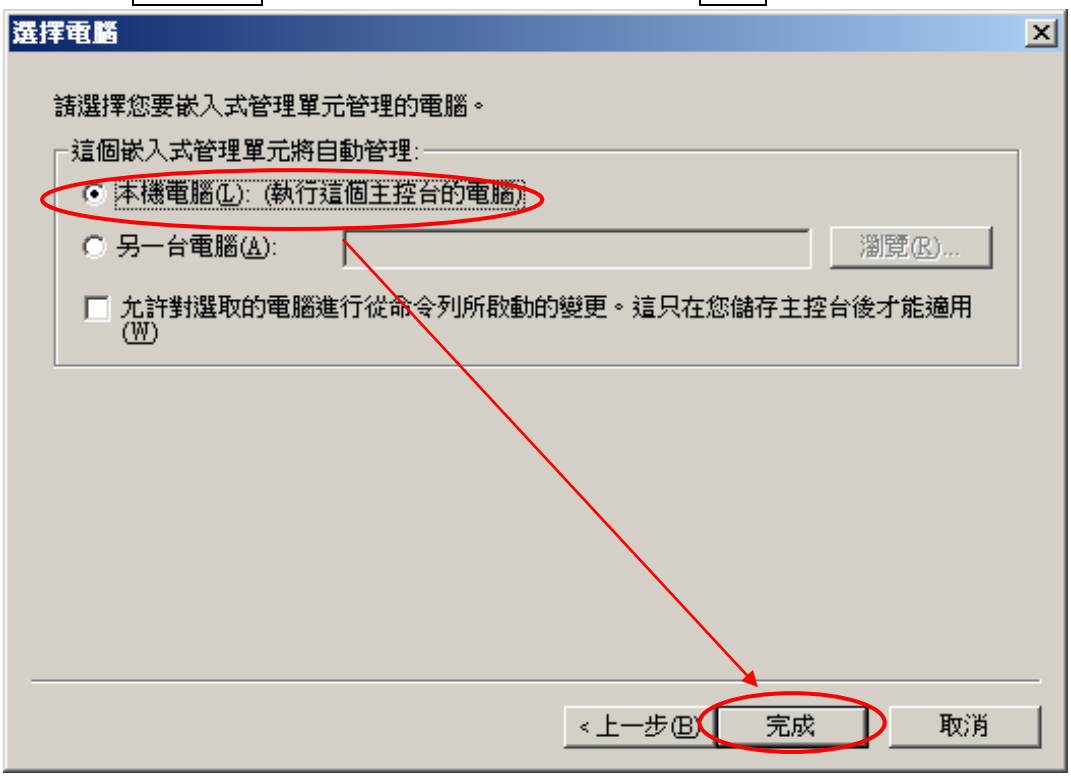

### 5.1.1.4 新增憑證管理單元(2)

選擇電腦帳戶→點選下一步。



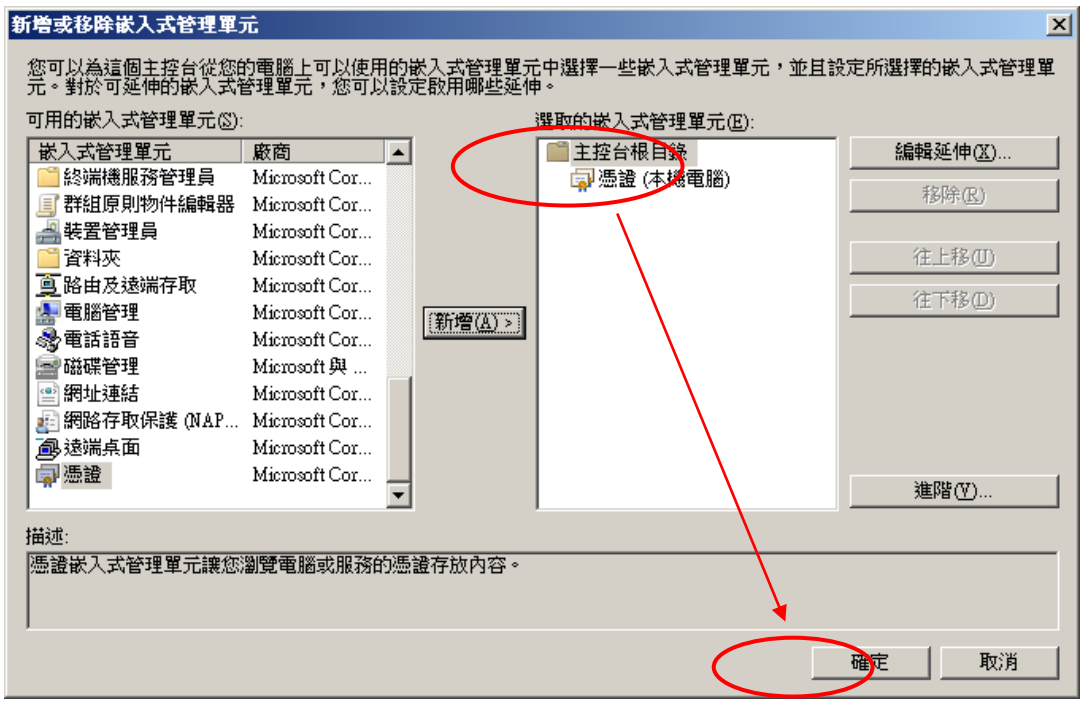
### 5.1.1.5 新增憑證管理單元(3)

點選本機電腦(執行這個主控台的電腦)→點選完成。



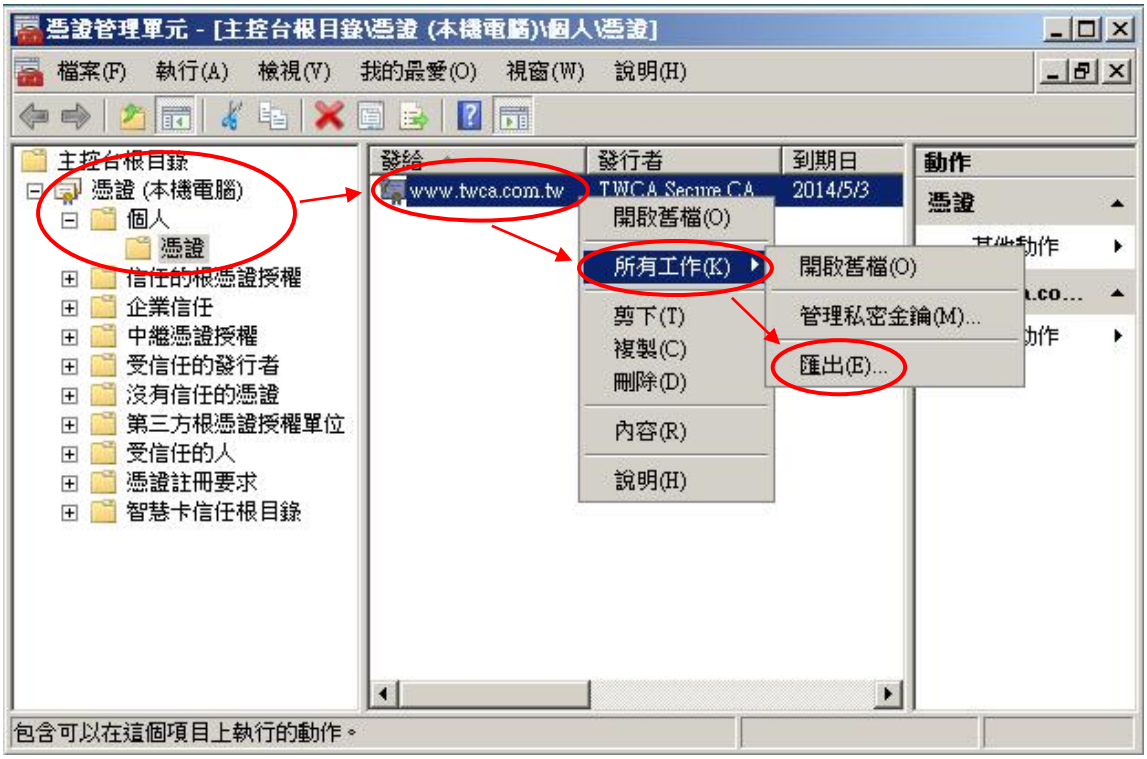

### 5.1.1.6 新增憑證管理單元完成

當憑證(本機電腦)新增完成後→點選確定。



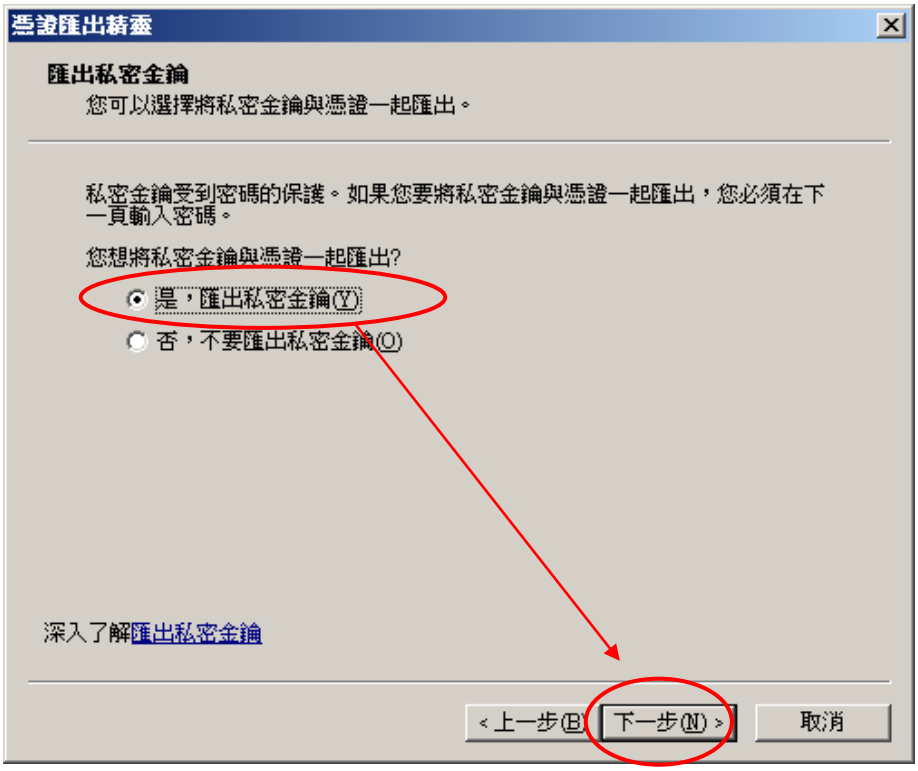
### 5.1.2 匯出憑證

5.1.2.1 點選展開主控台根目錄內的憑證（本機電腦）→個人→憑證，在欲匯出的伺服器憑證上按右鍵所有工作→點選匯出。

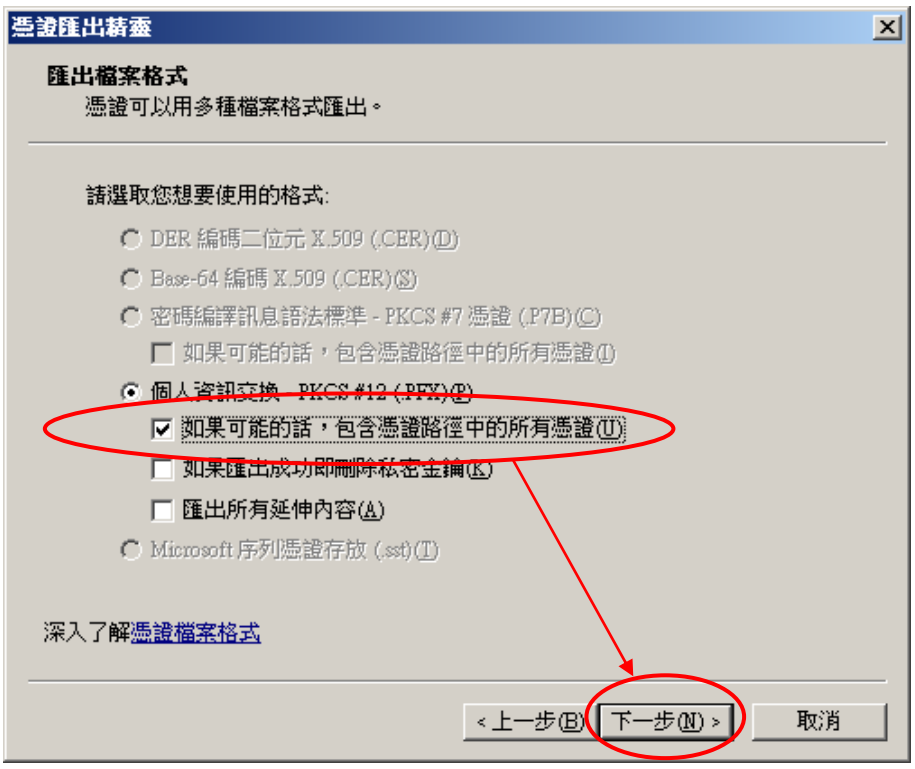



5.1.2.2 啟動歡迎使用憑證匯出精靈→點選下一步。

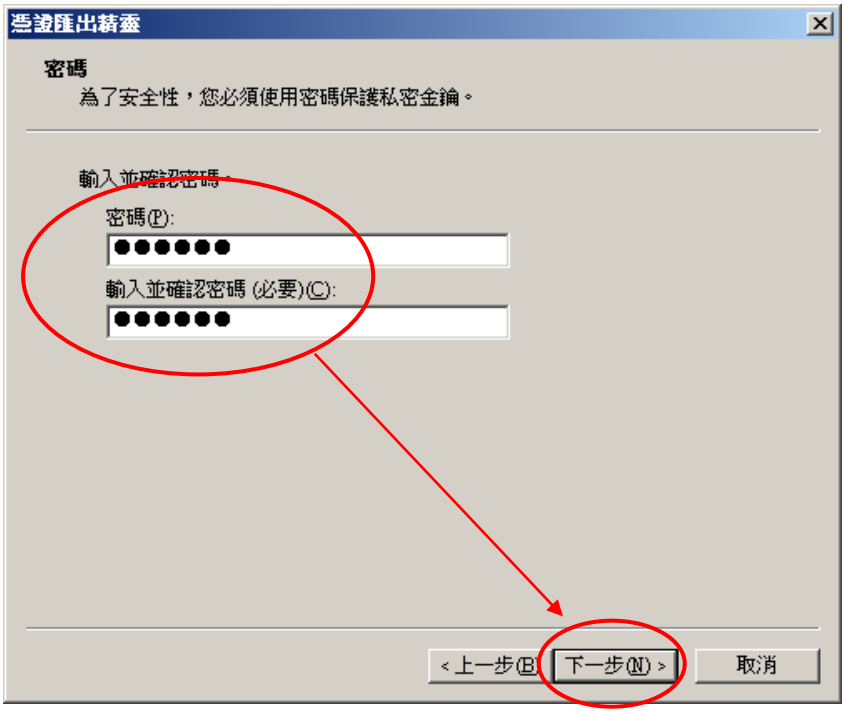
5.1.2.3 點選是，匯出私密金鑰(Y)→點選下一步。



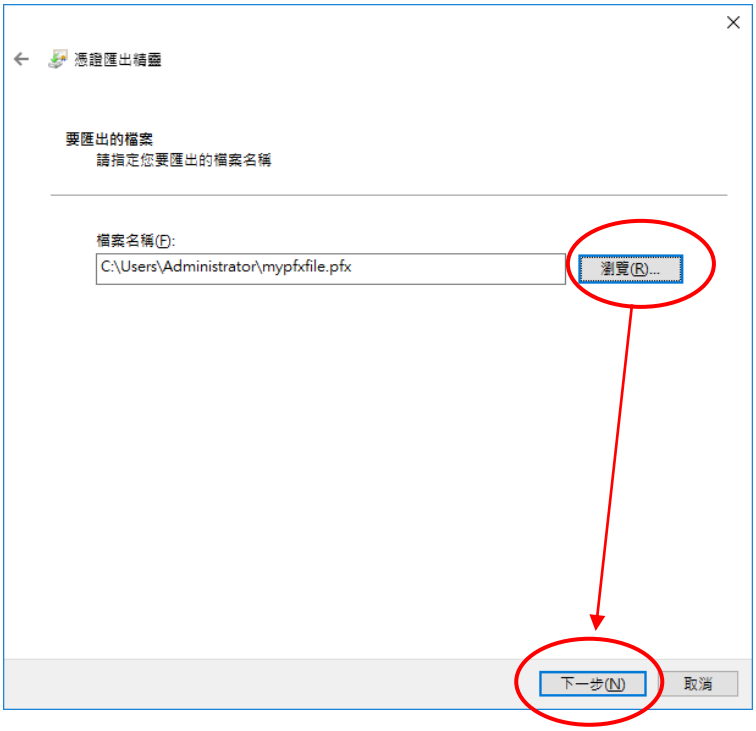

5.1.2.4 點選個人資訊交換-PKCS#12(.PFX)→勾選如果可能的話，包含憑證中所有的憑證→點選下一步。



5.1.2.5 設定匯出資料的保護密碼→點選下一步。(請務必記住此密碼，匯入憑證時需使用)




5.1.2.6 點選瀏覽→指定一個匯出檔案存放的路徑與檔名(副檔名固定為.PFX)→點選下一步。

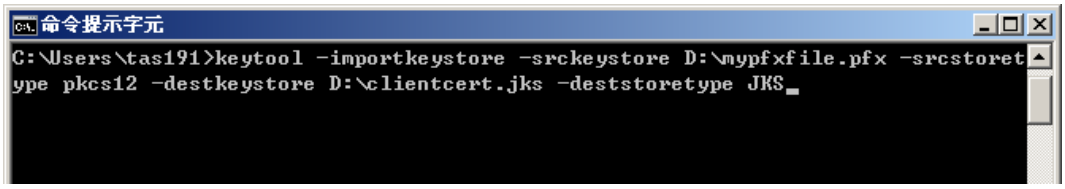


5.1.2.7 點選完成，完成匯出憑證(備份)。


### 5.1.3 使用 JAVA keytool 軟體將 PFX 檔轉換 JKS 金鑰資料庫檔

```
keytool -importkeystore -srckeystore mypfxfile.pfx -
srcstoretype pkcs12 -destkeystore clientcert.jks -
deststoretype JKS
```

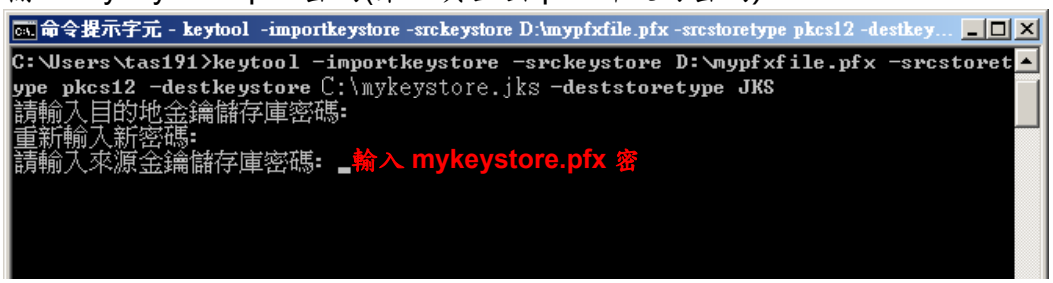
mypfxfile.pfx：由 IIS 匯出之金鑰憑證交換檔絕對路徑
clientcert.jks：將 mypfxfile.pfx 轉換成 JKS 金鑰資料庫輸出之檔案路徑與名稱



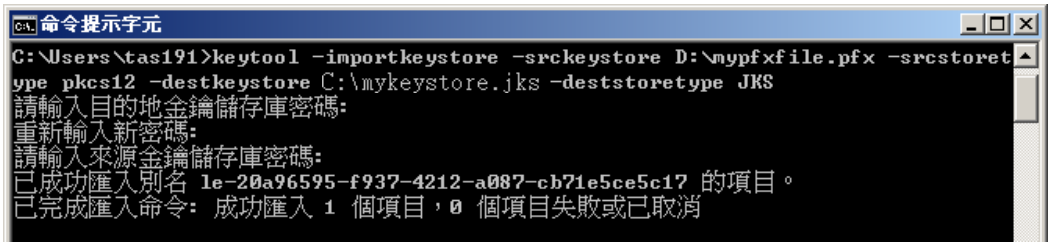

設定 mykeystore.jks 密碼(建議跟第七頁匯出 pfx 所設的密碼一致)


再次輸入 mykeystore.jks 密碼(建議跟第七頁匯出 pfx 所設的密碼一致)


輸入 mykeystore.pfx 密碼(第七頁匯出 pfx 所設的密碼)




匯出成功



5.1.4 匯入憑證鏈

5.1.4.1 將憑證鏈檔(根憑證 root.cer、中繼憑證 uca.cer)存放至%JDK%\bin 目錄下(實際目錄可自行決定)。

5.1.4.2 請將憑證由上至下(根憑證 root.cer、中繼憑證 uca.cer)一一匯入金鑰儲存庫。

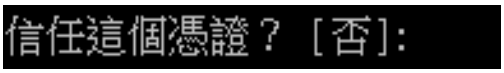
5.1.4.2.1 匯入根憑證 root.cer

keytool -import -trustcacerts -alias root -file root.cer -keystore C:\mykeystore.jks


指令參數說明如下(指令反白部份請依實際配置決定)

| 參數 | 說　　明 |
|---|---|
| -import | 匯入憑證必要指令 |
| -trustcacerts | 建立為信任的憑證鏈 |
| -alias | 設定根憑證別名，請自行決定即可 |
| -file | 要匯入的根憑證路徑及名稱，請依實際位置指定 |
| -keystore | keystore 檔案所在路徑及名稱，請依實際位置指定 |


此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼並確認




如出現上面訊息，請輸入 y 再按 Enter 即可，


出現「憑證已新增至金鑰儲存庫中」即匯入完成。

5.1.4.2.2 匯入中繼憑證 uca.cer

keytool -import -trustcacerts -alias uca -file uca.cer -keystore C:\mykeystore.jks

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -import -trustcacerts -alias uca -
file uca.cer -keystore C:\mykeystore.jks
```

指令參數說明如下(指令反白部份請依實際配置決定)

| 參數 | 說　　明 |
|---|---|
| -import | 匯入憑證必要指令 |
| -trustcacerts | 建立為信任的憑證鏈 |
| -alias | 設定中繼憑證別名，請自行決定即可 |
| -file | 要匯入的中繼憑證路徑及名稱，請依實際位置指定 |
| -keystore | keystore 檔案所在路徑及名稱，請依實際位置指定 |

```
輸入金鑰儲存庫密碼:
```

此時會要求輸入金鑰儲存庫密碼，請直接輸入金鑰儲存庫密碼，

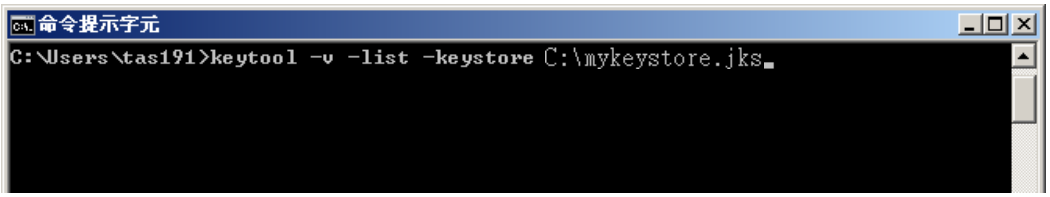
```
憑證已新增至金鑰儲存庫中
```

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

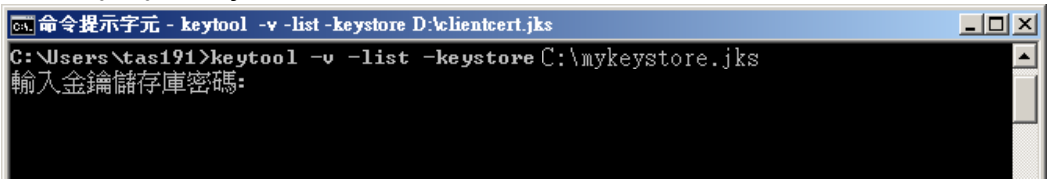
### 5.1.5 使用 keytool 檢視 JKS 金鑰資料庫檔案內容

```
keytool -v -list -keystore mykeystore.jks
```

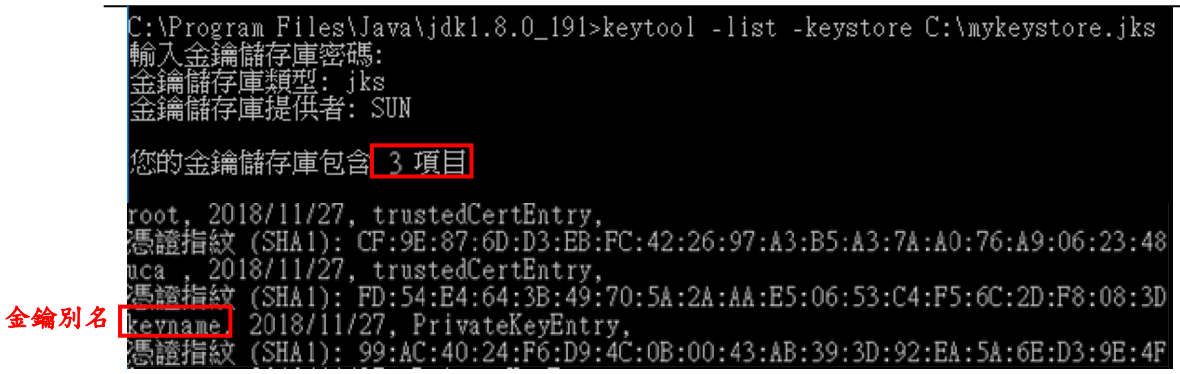
mykeystore.jks：將 mypfxfile.pfx 轉換成 JKS 金鑰資料庫輸出之檔案路徑與名稱




輸入 mykeystore.jks 檔密碼




即可檢視 mykeystore.jks 檔內容，金鑰儲存庫項目必須大於 1 為正常



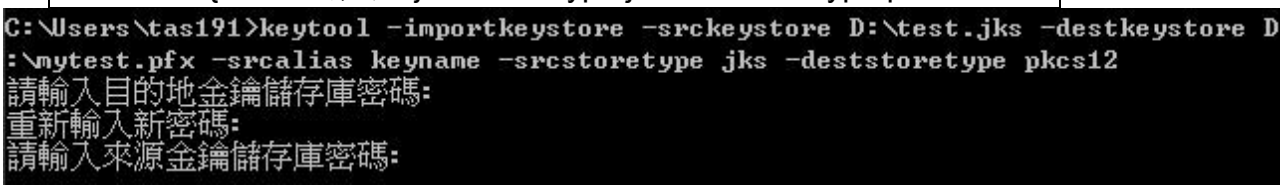

5.1.6 調整設定

5.1.6.1 接著請依您的伺服器版本進行 SSL 及憑證的設定。

## 5.2 TOMCAT 轉 IIS 格式

### 5.2.1 利用 keytool 將 JKS 轉換成 PFX，指令如下：(來源、目的金鑰儲存庫的密碼都用同一組)

```
keytool -importkeystore -srckeystore {JKS 檔案路徑} -destkeystore
{PFX 檔案路徑}
  -srcalias {JKS 金鑰別名} -srcstoretype jks -deststoretype pkcs12
```




### 5.2.2 參考 IIS 操作手冊，從匯入憑證鏈(根憑證、中繼憑證、伺服器憑證)章節繼續完成所有憑證安裝步驟，其中伺服器憑證就是剛剛匯出的 mytest.pfx。

# 6.附件

無。