SSL 憑證 Apache 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-03-160
生效日期： 109 年 3 月 3 日

目　　錄

1.目的

1.1. 介紹 SSL 憑證 Apache 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 Apache 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 Tomcat 轉 Apache

5.1.1 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
```

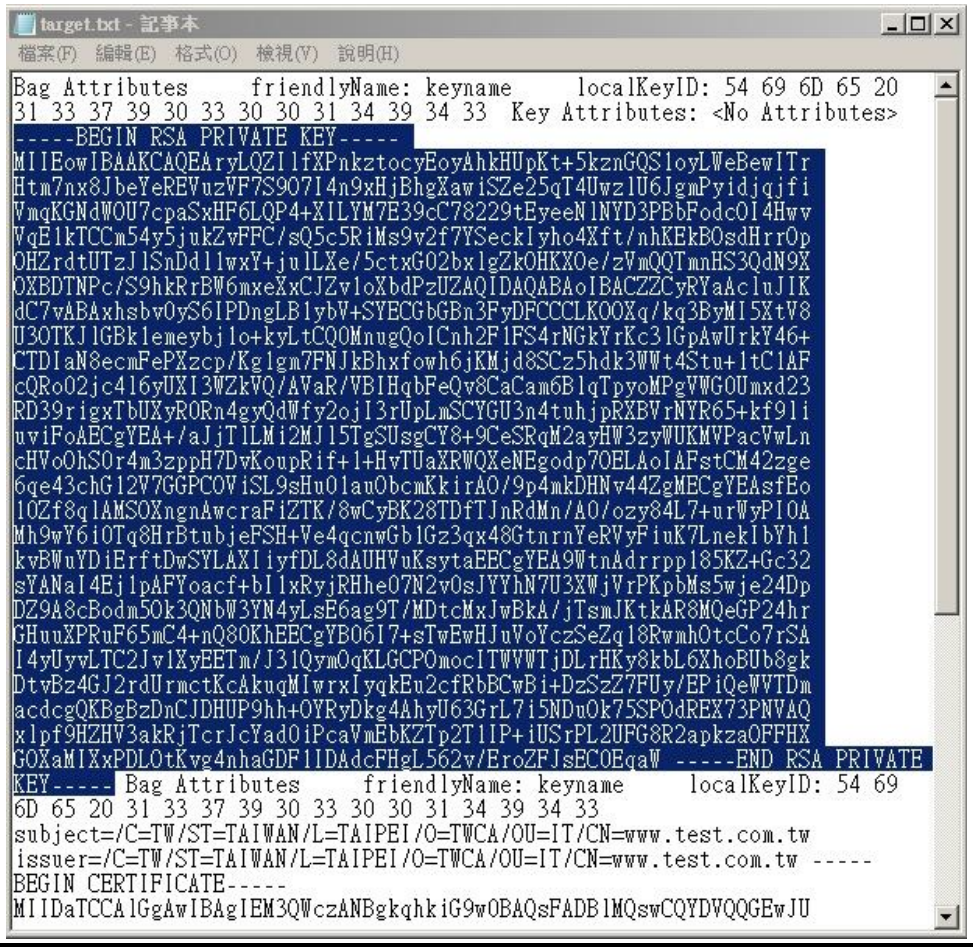
```
C:\Users\tas191>keytool -importkeystore -srckeystore D:\test.jks -destkeystore D
:\mytest.pfx -srcalias keyname -srcstoretype jks -deststoretype pkcs12
請輸入目的地金鑰儲存庫密碼:
重新輸入新密碼:
請輸入來源金鑰儲存庫密碼:
```

5.1.2 利用 OPENSSL 擷取 PFX 中的私密金鑰，指令如下：

```
openssl pkcs12 –in { PFX 檔案路徑} –out {輸出文字檔路徑} -nodes
```

```
OpenSSL> pkcs12 -in D:\mytest.pfx -out D:\target.txt -nodes
Enter Import Password:
MAC verified OK
```

5.1.3 檢視產出之文字檔，將擷取之私密金鑰(下圖反白部分，包含-----BEGIN RSA PRIVATE KEY-----與-----END RSA PRIVATE KEY-----)，另存為金鑰檔(server.key)。



5.1.4 將擷取之私密金鑰另存為金鑰檔。

5.1.5 將成功擷取之金鑰檔、及本公司核發的中繼憑證檔、伺服器憑證檔移轉至 Apache 主機，參考 Apache 伺服器操作手冊，下載、安裝憑證章節完成 Apache 之 SSL 憑證安裝設定。

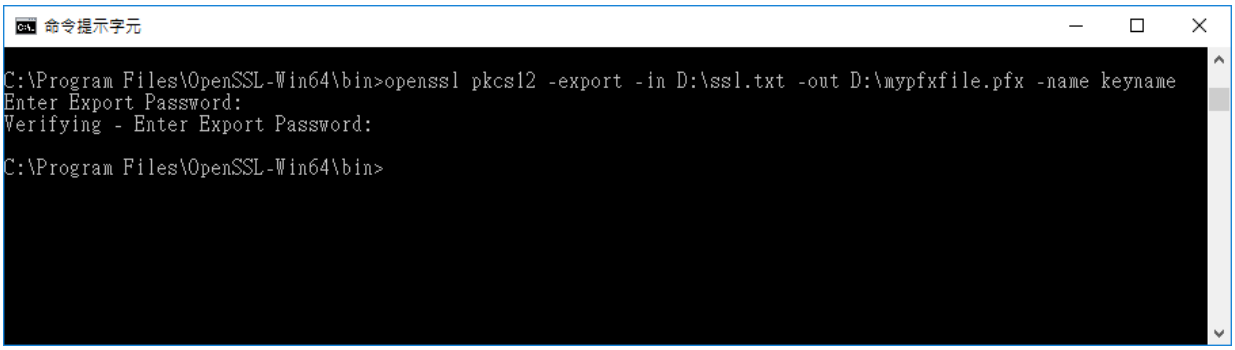
5.2 Apache 轉 Tomcat

5.2.1 使用文書編輯新檔 ssl.txt，其內容請參考以下圖例說明，包含憑證鏈及金鑰依序貼至 ssl.txt，因本公司憑證鏈共四層，所以 ssl.txt 檔由上至下依序為根憑證(root.cer)、中繼憑證(uca.cer)、伺服器憑證(server.cer)及伺服器金鑰。

5.2.2 使用 openssl 將 ssl.txt 轉換為 Tomcat 金鑰檔

openssl pkcs12 -export –in {ssl.txt 檔案路徑} -out {PFX 檔案路徑} -name {金鑰別名}

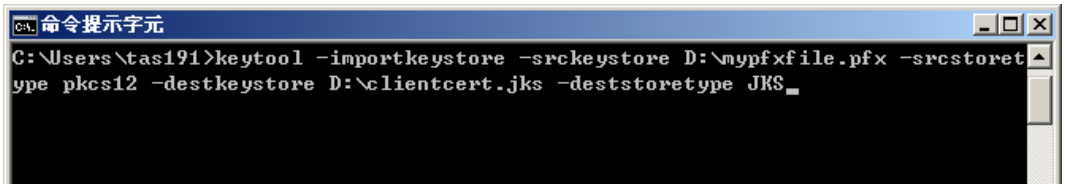
5.2.3 設定轉換成 PFX 檔的密碼



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

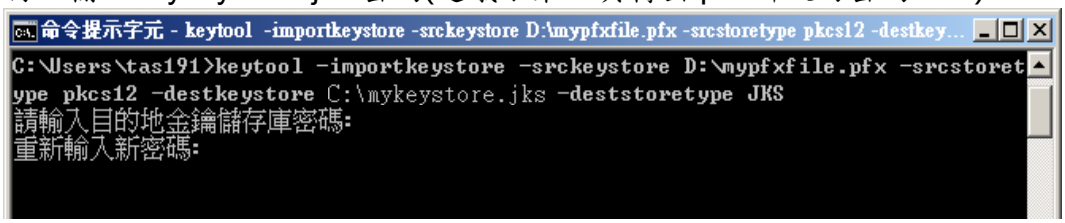
```
keytool -importkeystore -srckeystore mypfxfile.pfx -
srcstoretype pkcs12 -destkeystore clientcert.jks -
deststoretype JKS
```

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

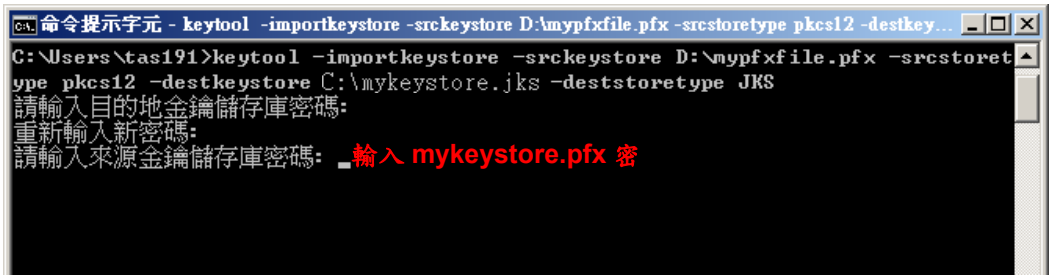


設定 mykeystore.jks 密碼(建議跟第 8 頁轉出 pfx 所設的密碼一致)

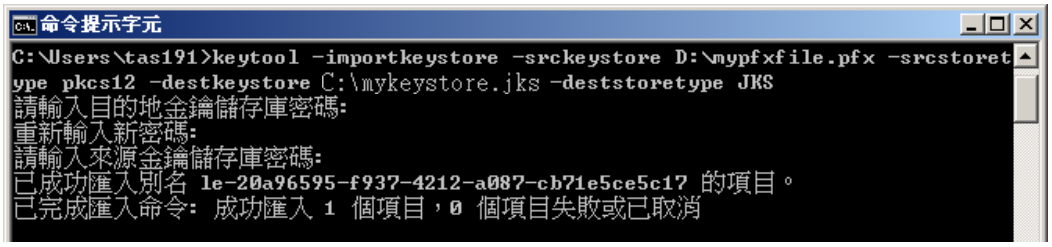
再次輸入 mykeystore.jks 密碼(建議跟第 8 頁轉出 pfx 所設的密碼一致)



輸入 mykeystore.pfx 密碼(建議跟第 8 頁轉出 pfx 所設的密碼一致)



匯出成功



5.2.5 匯入憑證鏈

5.2.5.1 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)。

5.2.5.2 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。

5.2.5.2.1 匯入根憑證 root.cer

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

```
C:\Program Files\Java\jdk1.8.0_191\bin>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

```
輸入金鑰儲存庫密碼:
重新輸入新密碼:
```

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並確認

```
信任這個憑證？ [否]:
```

如出現上面訊息，請輸入 y 再按 Enter 即可，

```
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。

5.2.5.2.2 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，

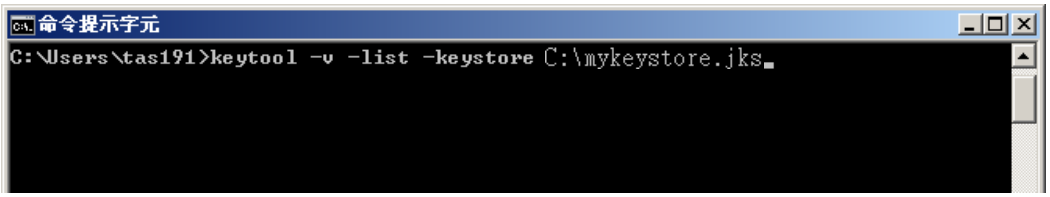
```
憑證已新增至金鑰儲存庫中
```

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

5.2.6 使用 keytool 檢視 JKS 金鑰資料庫檔案內容

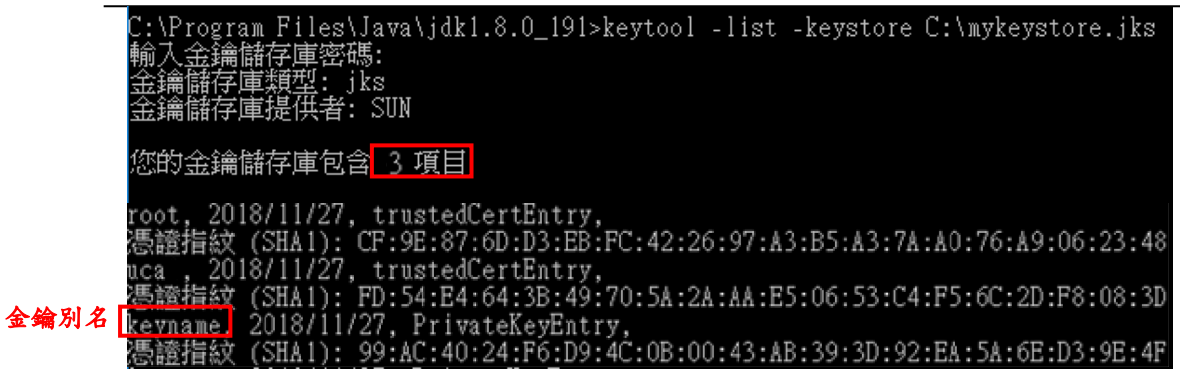
```
keytool -v -list -keystore mykeystore.jks
```

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



5.2.7 調整設定

5.2.7.1 接著請依您的伺服器版本進行 SSL 及憑證的設定。

6.附件

無。