

# API 技術客服

## 使用 keytool 製作憑證請求檔製作手冊

聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請伺服器應用軟體憑證用戶參考，若因參考本手冊所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

### 目錄

使用 keytool 製作憑證請求檔手冊.....	2
---------------------------	---

# 使用 Keytool 製作憑證請求檔製作手冊

## 一、確認 Java 版本

- 1.1 如果其所使用的 Java(JDK)版本是 1.5 版以前的版本，將無法安裝 RSA 4096 位元金鑰長度的 GRCA 憑證，因為舊版的 Java 最多只支援 RSA 2048 bits 的金鑰長度，建議請使用最新版本的 Java(JDK)版本。

## 二、如何產生「金鑰對」

- 2.1 由「開始」→執行→輸出「cmd」確認。
- 2.2 在 %JAVA\_HOME%\bin 目錄下，請執行

***keytool -genkey -alias tomcat -keyalg RSA -keysize 2048 -keystore D:\.keystore***(請自行輸入需要的路徑與檔名)。

- 若您非第一次申請憑證，請確認指令 ***-keystore*** 後面您所指定的路徑與檔名不會覆蓋線上正在使用的憑證。
- 此指令會在指定目錄下產生".keystore"檔(內含私密金鑰)，請勿於提出憑證申請後重複執行此指令，否則舊的".keystore"檔將會被覆蓋。
- 依照國際密碼學之規範，2014 年起不要再使用 RSA 1024 位元之憑證，請產製 RSA 2048 位元(含)以上金鑰長度的金鑰對。
- 請妥善保管此".keystore"檔。

```
C:\Program Files\Java\jdk1.7.0_17\bin>keytool -genkey -alias tomcat -keyalg RSA
-keysize 2048 -keystore D:\.keystore
輸入金鑰儲存庫密碼:
重新輸入新密碼:
您的名字與姓氏為何?
[Unknown]: www.test.com.tw
您的組織單位名稱為何?
[Unknown]: 政府網路處
您的組織名稱為何?
[Unknown]: 中華電信股份有限公司數據分公司
您所在的城市或地區名稱為何?
[Unknown]: Taipei
您所在的州及省份名稱為何?
[Unknown]:
此單位的兩個字母國別代碼為何?
[Unknown]: TW
CN=www.test.com.tw, OU=政府網路處, O=中華電信股份有限公司數據分公司, L=Taipei, S
T=Unknown, C=TW 正確嗎?
[否]: Y
輸入 <tomcat> 的金鑰密碼
<RETURN 如果和金鑰儲存庫密碼相同>:
```

- 工商憑證管理中心只會截取請求檔案中的公開公鑰，不會使用憑證請求檔案中於步驟 2.5-2.10 所輸入之資訊，而是根據申請網頁上所填寫資訊為主。
- 2.3 出現「輸入 keystore(金鑰儲存庫)密碼」：請輸入一個密碼，用以保護此儲存庫(請妥善保存此組密碼)。
- 2.4 出現「您的名字與姓氏為何?」：請填入欲申請的網站名稱  
ex：www.test.com.tw。
- 2.5 出現「您的組織單位名稱為何?」：請填入公司單位名稱。
- 2.6 出現「您的組織名稱為何?」：請填入公司名稱。
- 2.7 出現「您所在的城市或地區名稱為何?」：請填入公司所在地。
- 2.8 出現「您所在的州及省份名稱為何?」：可以不用輸入，按 Enter 跳過。
- 2.9 2.9 出現「此單位的兩個字母國別代碼為何?」：請填入 TW。
- 2.10 檢查所輸入的資料是否正確,若正確,請輸入 Y。
- 2.11 出現「輸入 <tomcat> 的金鑰密碼」：請直接按"Enter"鍵。(注意：此步驟所設的密碼必須與 2.3 步驟所設的密碼一致)。

### 三、如何產製憑證請求檔

- 3.1 在 %JAVA\_HOME%\bin 下，執行

```
keytool -certreq -alias tomcat -file D:\certreq.txt -keystore D:\.keystore
```

- 製作請求檔案放置地方，請看 -file 指令後面給指定你放置請求檔位址與檔名 (certreq.txt)。
- 私密金鑰來源地方，請看 - keystore 指令後面給指定你放置私密金鑰。

```
C:\Program Files\Java\jdk1.7.0_17\bin>keytool -certreq -alias tomcat -file D:\certreq.txt -keystore D:\.keystore  
輸入金鑰儲存庫密碼:
```

- 3.2 出現「輸入 keystore(金鑰儲存庫)密碼」：請輸入上一個步驟所設定的密碼。
- 3.3 請妥善保存憑證請求檔(certreq.txt)至經濟部工商憑證管理中心 ( <http://moeaca.nat.gov.tw/nonic.html> ) 依照網頁說明申請非 IC 卡類憑證。