

政府伺服器數位憑證管理中心(GTLSCA)

Tomcat 伺服器 SSL 憑證請求檔製作與憑證安裝手冊

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 SSL 伺服器軟體憑證用戶參考，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。

本手冊的申請程序，已經在 Windows 系統 + Tomcat 9.0 版測試過，您所使用的版本或環境可能與本手冊所測試的版本有所差異，若是如此則請參考您的 Tomcat 相關使用手冊，適度調整申請步驟。

目錄

Tomcat SSL 憑證請求檔製作手冊.....	2
Tomcat SSL 憑證安裝操作手冊.....	4
附件一：停用 SSLv3.0、TLS 1.0 和 TLS 1.1	7

Tomcat SSL 憑證請求檔製作手冊

一、 如何產生「金鑰對」

1.1 由「開始」→執行→輸出「cmd」確認。

1.2 在 %JAVA_HOME%\bin 目錄下，請執行

```
keytool -genkey -alias <金鑰的 alias name> -keyalg RSA -keysize 2048  
-keystore <keystore 儲存路徑>(請自行輸入需要的路徑與檔名)。
```

- 若您非第 1 次申請憑證，請確認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。
- 請妥善保管此".keystore"檔，建議可先備份此檔案，以防後續憑證安裝操作有誤可以立即復原重新操作。
- 上述指令中的 alias name 在之後 SSL 憑證安裝時會用到，請牢記此名稱。

```
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>:
```

1.3 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)。

1.4 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 (多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主)。

1.5 出現「您的組織單位名稱為何?」：請填入公司單位名稱。

1.6 出現「您的組織名稱為何?」：請填入公司名稱。

- 1.7 出現「您所在的城市或地區名稱為何？」：請填入公司所在地。
- 1.8 出現「您所在的州及省份名稱為何？」：可以不用輸入，按 Enter 跳過。
- 1.9 出現「此單位的兩個字母國別代碼為何？」：請填入 **TW**。
- 1.10 檢查所輸入的資料是否正確,若正確,請輸入 **Y**。
- 1.11 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 1.3 步驟所設的密碼一致，否則 tomcat 將無法使用此金鑰來啟動 SSL**)。
- 1.12 政府憑證管理中心之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於步驟 1.4-1.9 所輸入之資訊，而是以於申請網頁上所填入的機關或單位資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準而記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)或憑證主體別名(Subject Alternative Name)等欄位]。

二、 如何產製憑證請求檔

- 2.1 在 %JAVA_HOME%\bin 下，執行
keytool -certreq -alias <步驟1.2 所設定的 alias name> -file <憑證請求檔儲存路徑> -keystore <keystore 檔案所在路徑>

```
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:
```

- 2.2 出現「輸入 keystore(金鑰儲存庫)密碼」：請輸入步驟 1.3 所設定的密碼。
- 2.3 請複製憑證請求檔(certreq.txt)後，至憑證管理中心網站 (<https://gca.nat.gov.tw>)進行 SSL 憑證申請作業。

Tomcat SSL 憑證安裝操作手冊

一、 取得憑證串鍊檔案

1.1 請至 GTLSCA 網站下載已經壓縮打包好的憑證串鍊檔案，下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip

1.2 將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案

二、 安裝 SSL 憑證，請使用您之前產生憑證請求檔的 Keystore 來執行匯入動作(依信任關係，由最上層憑證，依序往下安裝)

2.1 安裝 eCA 憑證(共 2 張)。

在 %JAVA_HOME%\bin 目錄下執行

```
keytool -import -alias eca -file D:\ROOTeCA_64.crt -keystore <keystore 檔案所在路徑>
```

```
keytool -import -alias eca2 -file D:\eCA1_to_eCA2-New.crt -keystore <keystore 檔案所在路徑>
```

- 請依實際您存放檔案的位置調整指令。
- 待出現 Enter keystore password：請輸入密碼。
- 待出現 Trust this certificate：請輸 y。

2.2 安裝 GTLSCA 憑證。

在 %JAVA_HOME%\bin 目錄下執行

```
keytool -import -alias gtlscA -file D:\GTLSCA.crt -keystore <keystore 檔案所在路徑>
```

- 待出現 Enter keystore password：請輸入密碼。
- 待出現 Trust this certificate：請輸 y。

2.3 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
- 若您的 keystore 沒有 PrivateKeyEntry，放入 server 後，SSL 也無法成功連線。請找出原 keystore 檔案，或是重新申請。

```
cmd 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>_
```

2.4 匯入 SSL 伺服器應用軟體憑證。

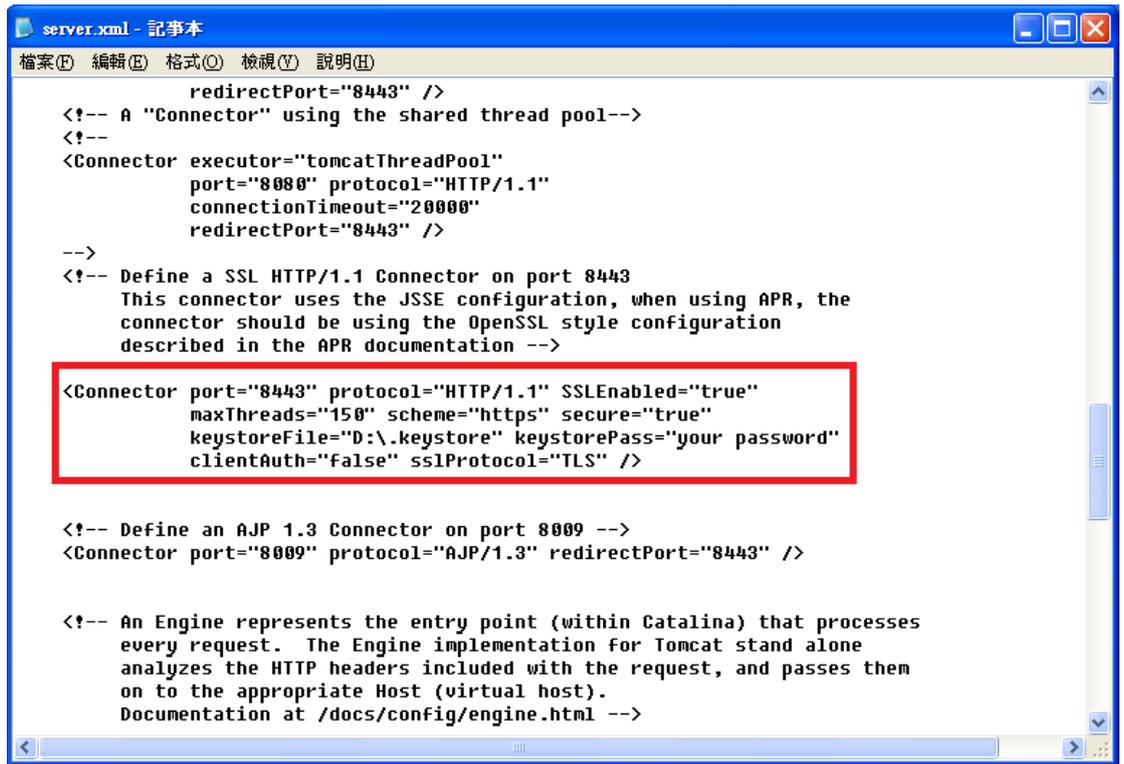
在 %JAVA_HOME%\bin 目錄下執行

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。

2.5 修改 Tomcat server.xml 設定

- 開啟 %TOMCAT_HOME%\conf\server.xml
- 找到如下圖的地方，修改(加入) keystoreFile、keystorePass 的參數，並確認其餘 https 相關參數設定正確。



```
server.xml - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

    redirectPort="8443" />
<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
    port="8080" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443" />
-->
<!-- Define a SSL HTTP/1.1 Connector on port 8443
This connector uses the JSSE configuration, when using APR, the
connector should be using the OpenSSL style configuration
described in the APR documentation -->
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="150" scheme="https" secure="true"
    keystoreFile="D:\.keystore" keystorePass="your password"
    clientAuth="false" sslProtocol="TLS" />

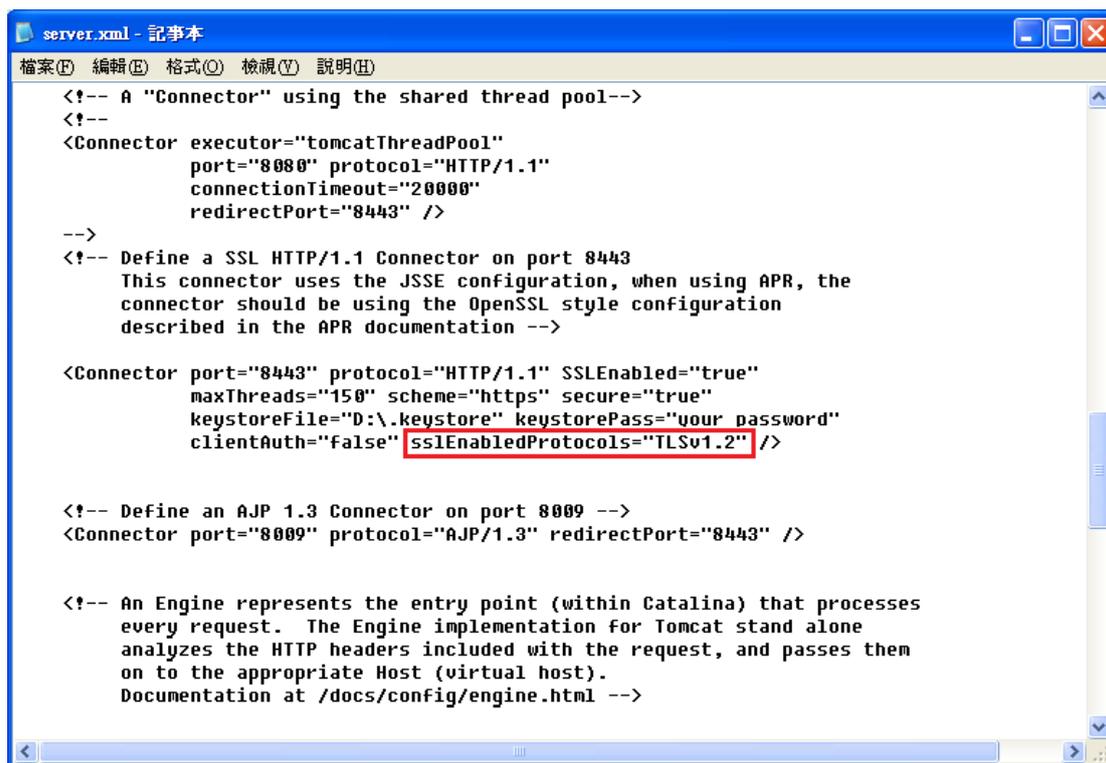
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
Documentation at /docs/config/engine.html -->
```

- 最後請將 tomcat 重新啟動，並以 https 連線測試 SSL 加密通道。
- 請注意，tomcat 預設 https 使用 8443 port，如需要 443 port，請自行修改。
- 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

附件一：停用 SSLv3.0、TLS 1.0 和 TLS 1.1

- 開啟 % TOMCAT_HOME%\conf\server.xml
- 找到如下圖的地方，修改(加入)
 - 若您使用的 Tomcat 版本為 5 或 6(6.0.38 以前)
sslProtocols="TLSv1.2"的參數
 - 若您使用的 Tomcat 版本為 6(6.0.38 以後)或 7
sslEnabledProtocols="TLSv1.2"的參數



```
<!-- A "Connector" using the shared thread pool-->
<!--
<Connector executor="tomcatThreadPool"
            port="8080" protocol="HTTP/1.1"
            connectionTimeout="20000"
            redirectPort="8443" />

-->
<!-- Define a SSL HTTP/1.1 Connector on port 8443
This connector uses the JSSE configuration, when using APR, the
connector should be using the OpenSSL style configuration
described in the APR documentation -->

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
            maxThreads="150" scheme="https" secure="true"
            keystoreFile="D:\.keystore" keystorePass="your password"
            clientAuth="false" sslEnabledProtocols="TLSv1.2" />

<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />

<!-- An Engine represents the entry point (within Catalina) that processes
every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes them
on to the appropriate Host (virtual host).
Documentation at /docs/config/engine.html -->
```

- 重新啟動 Tomcat