中華電信 GlobalSign SSL/TLS 憑證（R46 根憑證）
Tomcat 伺服器憑證暨中繼憑證簡易安裝教學

2026/04/14 初版

⛔ 操作警告

在 Tomcat（Java Keytool）環境下，更新憑證必須嚴格遵守「先匯入根憑證、中繼憑證，**最後才匯入伺服器憑證**」的順序。若順序錯誤，私鑰將無法正確建立憑證鏈連結，屆時需透過複雜的 PFX 轉檔程序重建 Keystore 檔案。

安裝流程總覽

第一節　確認設定檔與 Keystore 位置

在進行任何憑證匯入前，請先確認 Tomcat 正在使用的 Keystore 路徑與密碼，以免操作到錯誤的檔案。

1. 開啟 server.xml 檔案，該檔案通常位於 ${catalina.home}/conf/ 目錄下。

> **${catalina.home}** 為 Tomcat 安裝目錄的路徑變數。

2. 搜尋 keystoreFile 關鍵字，找到 SSL Connector 設定區塊，記錄以下三個參數：

- **keystoreFile** ← Keystore 或 .pfx 檔案路徑。
- **keystorePass** ← Keystore 或 .pfx 密碼。
- **keystoreType** ← 格式（JKS 或 PKCS12），使用 Keystore 檔案時可能不會有這個參數。

server.xml 設定範例

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
           maxThreads="150" scheme="https" secure="true"
           clientAuth="false" sslProtocol="TLS"
           keystoreFile="${catalina.home}/conf/my.keystore"
           keystorePass="mykeystorepassword"
           keystoreType="JKS" />
```

⚠ 提示

若 server.xml 中找不到 keystoreFile，代表 Tomcat 可能使用預設的 Keystore 路徑：${user.home}/.keystore。請視實際情況調整後續指令中的路徑。

	${user.home} 為使用者資料夾目錄的路徑變數。

第二節　匯入根憑證與中繼憑證

請依序執行以下兩道指令，將中華電信提供的憑證檔案匯入既有的 Keystore。執行前請先切換到憑證檔案所在目錄，或在指令中輸入完整路徑。

⚠ 操作順序不可顛倒

必須先匯入 rootr46.crt（根憑證）和 CHTOVCA.crt（中繼憑證），最後才能匯入伺服器憑證。順序錯誤將無法建立新憑證串鏈。

步驟 1　匯入根憑證（rootr46.crt）

終端機指令

```
keytool -import -alias rootr46
        -file rootr46.crt
        -keystore <您的 Keystore 路徑>
```

```
D:\test>keytool -import -alias rootr46 -file rootr46.crt -keystore test.keystore
```

系統詢問「信任這個憑證？（trust the certificate？）」時，請輸入 y 或 yes 後按 Enter。

步驟 2　匯入中繼憑證（CHTOVCA.crt）

終端機指令

```
keytool -import -alias chtovca
        -file CHTOVCA.crt
        -keystore <您的 Keystore 路徑>
```

```
D:\test>keytool -import -alias chtovca -file CHTOVCA.crt -keystore test.keystore
```

系統詢問「信任這個憑證？」時，請輸入 y 或 yes 後按 Enter。

第三節　匯入伺服器憑證

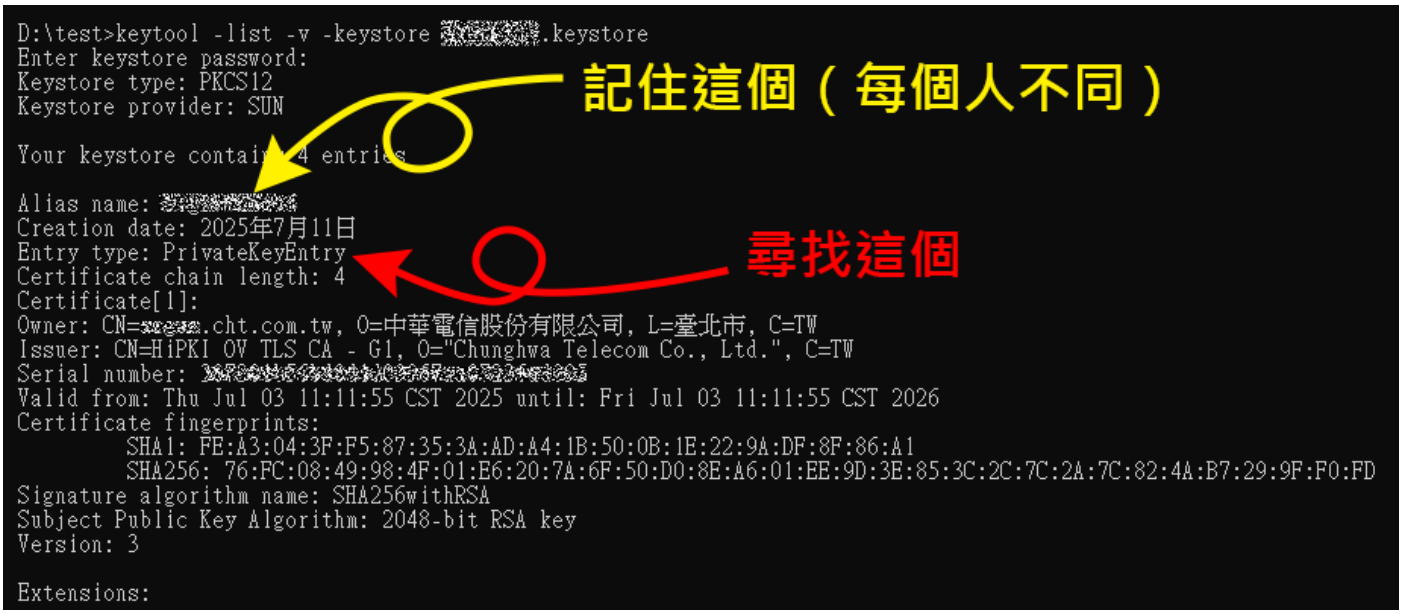
匯入伺服器憑證時，**別名**（Alias name）必須與 Keystore **私鑰**的別名完全一致，否則系統會建立一筆新的憑證 Entry，導致私鑰與新憑證分離。

步驟 1　查詢私鑰別名

執行以下指令，在輸出結果中尋找 Entry type 為 PrivateKeyEntry 的區塊，記下其 Alias name(如下圖黃色箭頭處)，後續匯入憑證時會用到。

終端機指令

```
keytool -list -v -keystore <您的 Keystore 路徑>
```



顯示欄位	說明
Alias name	別名，匯入伺服器憑證時需使用此值
Entry type	尋找後面有 PrivateKeyEntry 字值的那一個區塊

步驟 2　匯入伺服器憑證

將上一步查到的別名填入 -alias 後面的參數（以下範例假設別名為 tomcat）：

終端機指令

```
keytool -import -alias tomcat
        -file [憑證序號].cer
        -keystore <您的 Keystore 路徑>
```

✔ **成功訊息**

若操作順序正確，系統應顯示：

```
Certificate reply was installed in keystore
憑證回覆已安裝在金鑰儲存庫中
```

若出現其他訊息，請勿繼續，先確認別名是否正確。

✘ **錯誤訊息**

若出現下列訊息，則安裝失敗：

```
java.lang.Exception: Failed to establish chain from reply
無法從回覆中將鏈建立起來
```

上述訊息表示根憑證或中繼憑證有缺漏，請先將憑證鏈的根憑證或中繼憑證安裝至金鑰儲存庫中。

```
java.lang.Exception: Public keys in reply and keystore don't match
回覆時的公開金鑰與金鑰儲存庫不符
```

這則訊息表示金鑰儲存庫內的私鑰無法與伺服器憑證裡的公鑰成對，請確認產製 CSR 時所建立的金鑰儲存庫跟準備匯入憑證的金鑰儲存庫是同一個。

第四節　驗證憑證鏈

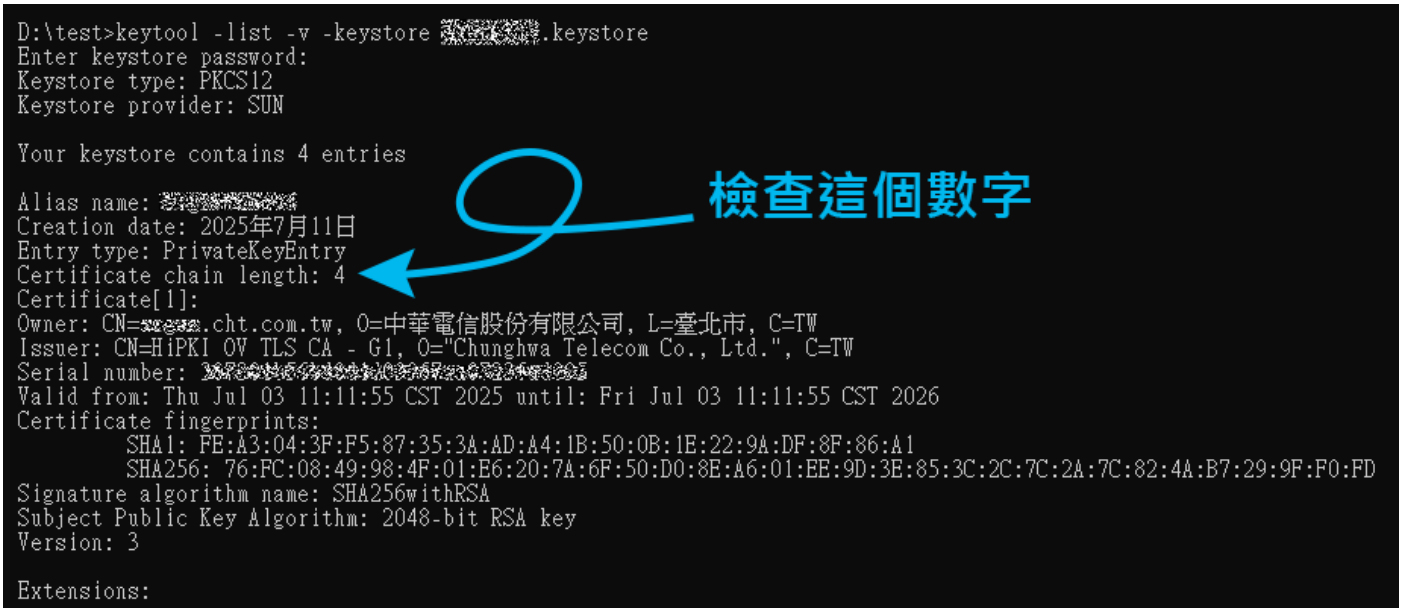
安裝完成後，務必檢查憑證鏈是否正確串接，再進行後續重啟動作。

1. 再次執行 keytool -list 指令。

終端機指令

```
keytool -list -v -keystore <您的 Keystore 路徑>
```

2. 找到 PrivateKeyEntry 那筆記錄，確認 **Certificate chain length** 的值。
   檢查 Certificate chain length 的值是否顯示為 3 或以上，
   若該值顯示為 1，代表中繼憑證未正確匯入，請重新確認第二節步驟。



chain length 顯示	代表意義	處理方式
3（或以上）	✔ 憑證鏈完整	可繼續進行第五節
1	✘ 只有伺服器憑證	重做第二節，或者參考附錄重構 keystore 檔案

第五節　套用設定並重啟 Tomcat

1. 將更新後的 Keystore 檔案存回原路徑，確認檔案位置與 server.xml 中 keystoreFile 的設定值相符。

2. 重啟 Tomcat 服務，使新憑證生效。

重啟指令（擇一使用）

```
# Linux / macOS
# 如果您的 tomcat 被 systemd 管理（現代主流 Linux 發行版本）
sudo systemctl restart tomcat
(tomcat 要替換成實際使用名稱，例如 tomcat8)

# 如果您的 tomcat 在安裝時使用 init scripts 安裝（常見於 Linux 早期發行版本）
sudo service tomcat restart
(tomcat 要替換成實際使用名稱，例如 tomcat8)

# 如果您的 tomcat 使用 binary 安裝，移動至 tomcat 安裝資料夾下，執行 shell 腳本
$CATALINA_HOME/bin/shutdown.sh
$CATALINA_HOME/bin/startup.sh



# Windows
# 方法一：開啟 Windows「服務」(services.msc)，選取 tomcat 服務，然後右鍵選單重新啟動
```

```
# 方法二：移動至 tomcat 安裝資料夾下，執行以下 bat 批次檔
%CATALINA_HOME%\bin\shutdown.bat
%CATALINA_HOME%\bin\startup.bat

# 註解：%CATALINA_HOME% 為 tomcat 的安裝目錄
```

☑ 驗證

重啟後，以瀏覽器造訪 *https://您的網站網址*，點選網址列左端圖示查看網站資訊。

憑證階層應顯示：

```
GlobalSign R46 Root CA
  Chunghwa Telecom GCC R46 OV TLS CA 2025
    伺服器憑證的 CN
```

也可使用 SSL Labs（https://ssllabs.com/ssltest）進行線上完整驗證。

附錄　Keystore ↔ PFX 格式轉換指令

以下指令用於 .Keystore（JKS）與 .pfx / .p12（PKCS12）兩種格式之間的相互轉換，常見於憑證搬家或跨平台部署時使用。

一、Keystore（JKS）→ PFX（PKCS12）

使用場景：需要將 Tomcat Keystore 轉出給 IIS 或其他支援 PFX 的伺服器、防火牆使用。

終端機指令

```
keytool -importkeystore
        -srckeystore <來源.keystore 路徑>
        -srcstoretype jks
        -destkeystore <輸出.pfx 路徑>
        -deststoretype pkcs12
```

```
D:\test>keytool -importkeystore -srckeystore test.keystore -srcstoretype jks -destkeystore test.pfx -deststoretype pkcs12
```

二、PFX（PKCS12）→ Keystore（JKS）

使用場景：從其他伺服器（如 IIS）取得 PFX 檔案後，轉換成 Tomcat 的 Keystore 格式。

終端機指令

```
keytool -importkeystore
        -srckeystore <來源.pfx 路徑>
        -srcstoretype pkcs12
        -destkeystore <輸出.keystore 路徑>
        -deststoretype jks
```

```
D:\test>keytool -importkeystore -srckeystore test.pfx -srcstoretype pkcs12 -destkeystore test.keystore -deststoretype jks
```

⚠ 小心機敏資訊

轉換過程中系統會要求輸入來源與目的地的密碼，請妥善保管。PFX 檔案包含私鑰，傳輸或存放時請嚴格控管存取權限，避免外流。

三、憑證匯入順序錯誤的補救流程

若不慎先匯入伺服器憑證再匯入中繼憑證，導致憑證鏈無法更新，須依以下流程重建 Keystore：

① 將現有 Keystore 轉為 PFX 格式（使用附錄一的指令）。

② 從 PFX 檔案中抽取私鑰：

終端機指令

```
openssl pkcs12 -in <來源.pfx 路徑> -nocerts -nodes -out private.key
```

```
D:\test>openssl pkcs12 -in server.pfx -nocerts -nodes -out private.key
```

③ 使用私鑰和正確排序的中繼憑證重新製作 PFX：

終端機指令

```
openssl pkcs12 -export -inkey private.key
               -in [憑證序號].cer
               -certfile CHTOVCA.crt -certfile rootr46.crt
               -out <輸出.pfx 路徑>
```

```
D:\test>openssl pkcs12 -export -inkey private.key -in D51B26052F06B16F868020F32FA82E42.cer
                                -certfile CHTOVCA.crt -certfile rootr46.crt -out server.pfx
```

④ 將新 PFX 檔案轉回 Keystore 格式（使用附錄二的指令）。

>> 執行 PFX → Keystore 轉檔指令成功後，會出現以下系統互動訊息：

```
Enter destination keystore password: ← 設定新的 keystore 密碼
Re-enter new password: ← 重新輸入剛剛設定的新密碼
Enter source keystore password: ← 輸入原本.pfx 檔案的密碼
```

⑤ 以新 Keystore 替換舊檔案，重啟 Tomcat。