SSL 常見技術問題手冊

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-03-158
生效日期：109 年 3 月 3 日

目　　錄

1.目的

1.1. 因應市場發展與客戶需求，整理常見技術問題，提供客戶安裝發生問題時參照處理。

1.2. 符合本公司資訊安全政策之規範。

2.參考資料

無。

3.定義

無。

4.作業程序

4.1 IIS 相關

Q1、在 IIS 匯入憑證後，為何憑證消失了？

原因說明:在執行**「完成憑證要求」**時的伺服器，必須與**「建立憑證要求」**時的伺服器**同一台**，因建立憑證要求時，私密金鑰會一併產生在該伺服器，如果憑證發下來是裝在另一台伺服器就會找不到當初那一把私密金鑰，以致於無法順利完成憑證要求，**現象是安裝完成後會看到憑證，但是按下 F5 重新整理後，該憑證就會立即消失**。另一種可能的情況是，當上傳完 CSR，在拿到核發的憑證前，又多做了一次「建立憑證要求」，導致先前產生的那一把私密金鑰，被多做的這一次覆蓋掉。因此，當憑證核發下來，安裝時，憑證會找不到對應的那把私密金鑰。

解決方式:請確認現在安裝的這台伺服器，是否為當初建立憑證要求的伺服器，若安裝的伺服器已經是當初建立憑證要求的伺服器，則表示金鑰已遺失，**請參考以下作法，重新產製 CSR 並交付給 TWCA 客服，等待再一次核發憑證。**

因金鑰遺失，無法安裝憑證者，步驟如下：
＊憑證重發需 3-5 工作日，重發新憑證之同時，也會同步廢止前一張憑證＊ （重要提醒） 1. 請重製新 CSR（含:新金鑰）並上傳至 www.twca.com.tw/Portal/service/ssl_1_3.html，完成後，請 copy 畫面，貼在信件內文。 2. 告知要重發的 CN 名稱及公司統編，並留下您的聯絡資料。 3. 信件主旨，填：需重發憑證（已上傳 CSR 檔）。 4. Email 至：sslcc@twca.com.tw。 5. TWCA 重發後，會寄到原本申請單所填之技術人員信箱。(請向原技術同仁取得憑證檔)。 6. 新憑證安裝好後，建議依手冊 5.9 章節進行**備份**作業（金鑰與憑證）。

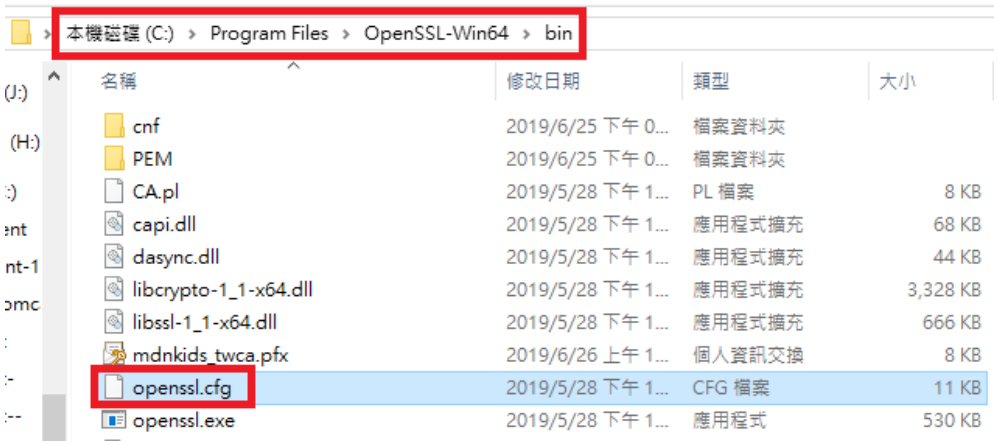
注意:**建立憑證要求之後，安裝前盡量避免對伺服器異動，減少金鑰再次遺失的可能**。

4.2 Apache 相關

Q1、Apache 產製 CSR 時，出現「Unable to load config info ftom /usr/local/ssl/openssl.cnf」？

原因說明:因為 OPENSSL 找不到 openssl.cnf 設定檔所致。

解決方式:找出正確的 config 檔的路徑與檔名（註:OpenSSL config 檔的副檔名可能是 cfg 或 cnf）



再執行 set 指令，set OPENSSL_CONF=openssl.cfg 或 openssl.cnf 設定檔存放位置，請將框起來的路徑設定正確，讓系統能在正確的位置讀到設定檔，接再進行憑證安裝手冊上產製 CSR 的指令。

Q2、安裝 Apache 憑證後，啟動 Apache 會出現「certificate routines:X509_check_private_key:key values mismatch」錯誤訊息？

原因說明:因金鑰檔與伺服器憑證公鑰比對不一致。

解決方式:請確認 Apache 設定參數金鑰檔(SSLCertificateKeyFile)與伺服器憑證檔(SSLCertificateFile)讀取的檔案是否正確。可利用 OpenSSL 指令確認憑證與金鑰 Private Key 的雜湊值是否一致。

1、 首先計算憑證 modulus 的雜湊值，指令如下:openssl x509 -noout -modulus -in "憑證檔路徑"

2、 再計算金鑰 modulus 的雜湊值，指令如下:openssl rsa -noout -modulus -in "金鑰檔路徑"

3、 比對憑證與金鑰 modulus 的雜湊值是否相等

4.3 Tomcat 相關

Q1、Tomcat 已依照手冊完成伺服器憑證匯入動作，但 Server 服務無法正常啟動？

原因說明: 可能在執行匯入伺服器憑證時，輸入的 alias 別名與產製 keystore 檔時所取的金鑰別名不一致。

解決方式: 重新執行匯入伺服器憑證動作，keytool -import -trustcacerts -alias keyname -file server.cer -keystore mykeystore.jks。其中輸入黃底部分必須與產製 keystore 檔時所取的金鑰別名一致。

- 利用查詢指令 keytool -list -v -keystore {JKS 檔絕對路徑值}，金鑰儲存庫項目必須大於 1，才代表憑證鏈匯入成功。

Q2、Tomcat 利用 keytool 指令執行 Server 憑證安裝，出現「keytool error: java.lang.Exception: Public keys in reply and keystore don't match」，原因為何？

原因說明:

- 安裝時使用到與當初產生 CSR 不同的 keystore 金鑰檔。
- 曾經改過 keystore 金鑰檔內如 alias name 資訊。

解決方式:

- 請使用當初產生 CSR 的 keystore 金鑰檔進行安裝。
- 執行指令時請使用正確的 alias name。

4.4 憑證格式相關

Q1、安裝憑證需要.crt 檔(或 PEM 格式檔)，可是 TWCA 核發的 SSL 憑證都是.cer 檔，該如何進行格式轉換？

說明:TWCA 提供的.cer 檔預設編碼和.crt 的編碼格式一樣,都是 PEM(Base64)格式，.cer 可直接安裝或將副檔名改成.crt 或.pem 使用即可。

Q2、IIS 備份(匯出)的是.pfx 檔案,可是設備安裝 SSL 需要的是 PKCS12 或.p12 檔案，格式該如何轉換？

說明：.pfx 和.p12 是相同的。兩者都是 PKCS#12 文件，IIS 匯出的.pfx 檔案可直接使用在您的設備，不須轉換。

Q3、憑證格式轉換手冊:

SSL 憑證 IIS 與 Apache 格式互轉說明手冊

http://www.twca.com.tw/picture/file/SSL 憑證 IIS 與 Apache 格式互轉說明手冊.pdf

SSL 憑證 Apache 及 Tomcat 格式互轉說明手冊

http://www.twca.com.tw/picture/file/SSL 憑證 Apache 及 Tomcat 格式互轉說明手冊.pdf

SSL 憑證 IIS 及 Tomcat 格式互轉說明手冊

http://www.twca.com.tw/picture/file/SSL 憑證 IIS 及 Tomcat 格式互轉說明手冊.pdf

4.5 連線異常相關

Q1、憑證安裝完成後執行 https 連線測試，瀏覽器回應顯示「此網站的安全性憑證有問題」、「此網站的憑證不受信任」、「網站的安全性憑證不可靠」、「憑證無效且無法用於驗證此網站的識別」、「您的連線不是私人連線 (ERR_CERT_AUTHORITY_INVALID)」等錯誤訊息，請問原因為何？

原因說明:原因為 SSL 憑證鏈未安裝完整，以致瀏覽器進行 https 加密連線時會有不受信任的錯誤訊息。(有時候使用手機連網站會顯示不安全，但 IE 或 Chrome 連線卻正常，是因為作業系統內建的憑證鏈較新、或瀏覽器可能會自動下載憑證鏈，就算 Server 沒安裝好憑證鏈也可以信任)

解決方式:請確實安裝 SSL 憑證鏈，中繼憑證=uca.cer、根憑證=root.cer。

Q2、使用 HTTPS 連線網頁，Chrome 瀏覽器為何會出現警告訊息(不安全網頁)？

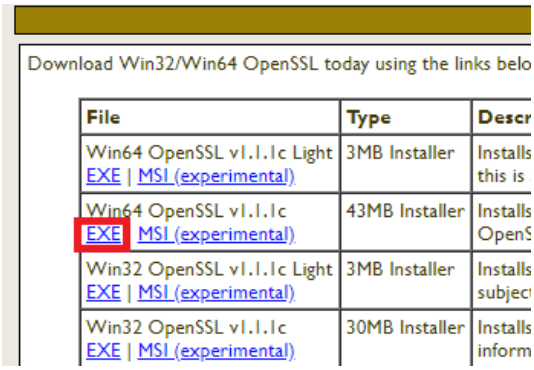
原因說明:您的網頁，可能有嵌入一些非經 https 加密連線取得的內容。為了用戶隱私和安全，一旦使用 Google 的 Chrome 瀏覽器連線到某個網頁，原始內容包含非經 https 加密連線取得的圖片、影片、音訊等，瀏覽器就會將該網站視為不安全。

解決方式:使用 Chrome 瀏覽器連到網站後按 F12，點選 Console 可看到錯誤訊息，藉此確認您的網頁有哪些非經 https 加密連線取得的內容。請移除這些內容，或改由 https 方式取得，再使用 chrome 以 https://連線您的網站，確認是否不再出現不安全網頁訊息。

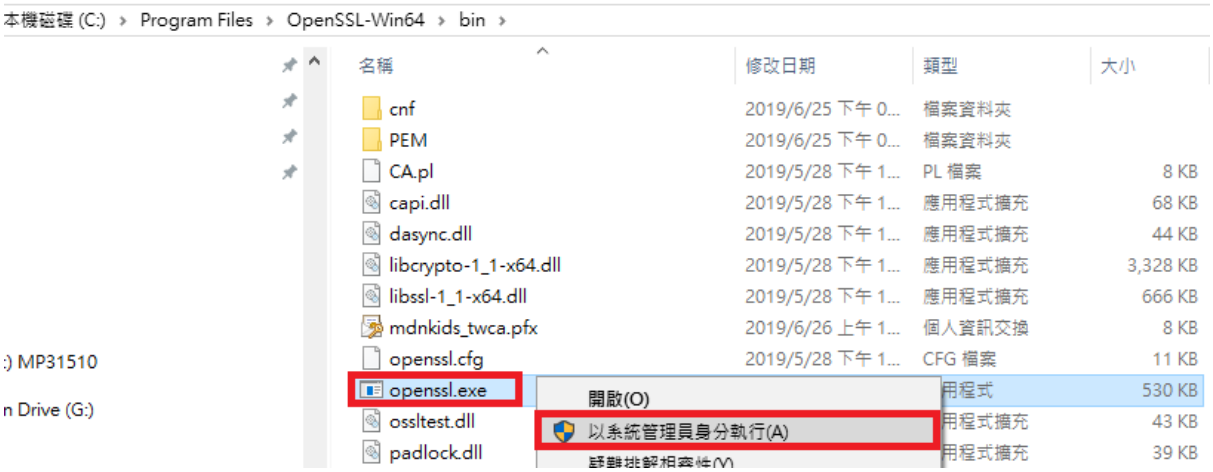
4.6 其他共同問題

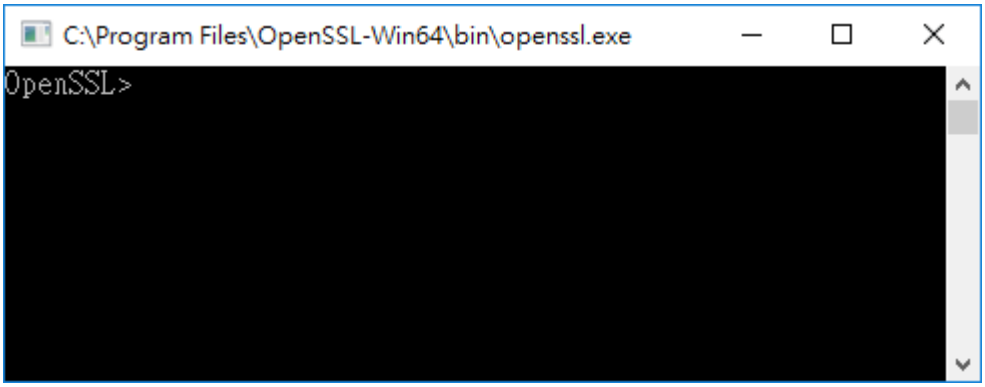
Q1、如何以工具檢測憑證鏈是否有安裝(使用 openssl 工具)?

說明: 請至 https://slproweb.com/products/Win32OpenSSL.html，依照您的作業系統版本，下載 exe 執行檔並安裝(請不要安裝 light 版本)，安裝步驟一直點選下一步，直到安裝完畢。

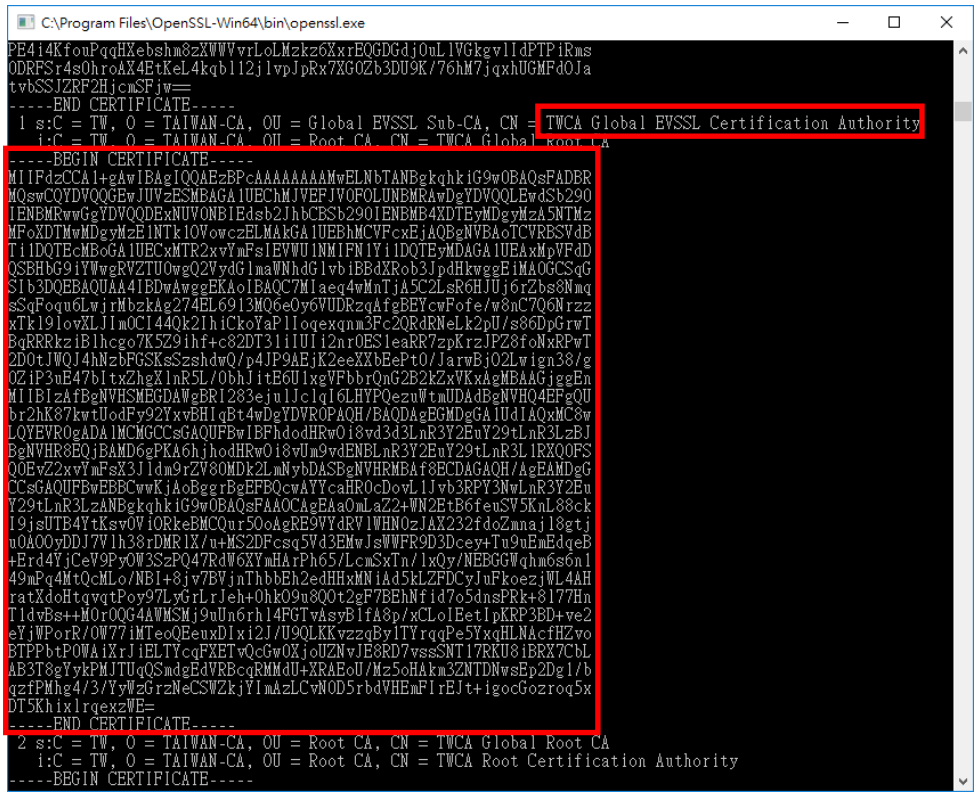


接著到 openssl 目錄的 bin 底下，以系統管理員身分執行 openssl.exe。





執行指令: s_client -connect www.twca.com.tw:443 -showcerts，其中 www.twca.com.tw 請改成您的網站 CN，執行後可以此網站安裝了那些憑證，每一個-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----所包夾的區塊即為一張憑證，而該區塊上面就是該憑證的資訊， CN 可識別這是哪一張憑證。注意:需要看到至少回應兩個區塊(兩張憑證)以上。



Q2、若新憑證安裝後，由 internet 連線網站顯示仍為舊憑證，分為以下幾種可能？

1 更新完憑證後服務未重啟。

2 憑證是安裝在多台伺服器上，每一台皆需更換。

3 裝錯台伺服器。

4 前端可能有其他網路設備有安裝憑證，需一併更換。

5 您的網站有可能是委外管理。

請先在伺服器本機確認網站所顯示的憑證為新憑證，在依以上幾種情況確認。

情況 1:

解決方式:請重啟服務，重新由 internet 連線網站再次確認。

情況 2:

原因說明:您的網站可能是架設在多台伺服器上，因為您現在連線到的剛好是沒有更新到憑證的伺服器，才會看到舊的憑證。

解決方式:請確認每一台伺服器都匯入憑證後，再重新連線網站確認是否看到新憑證。

情況 3:

原因說明:您安裝憑證的這台伺服器，並不是對外提供服務的伺服器。

解決方式:若懷疑憑證裝錯台，可藉由關閉目前這台伺服器的服務，重新由 internet 連線網站，確認是否已看不到憑證資訊，若依舊看的到，則代表此台伺服器並非提供服務的伺服器。等找到正確的伺服器後再將憑證匯入。

情況 4:

原因說明:使用者從 internet 連線至貴公司網站，可能會先經過網路設備，

再到網站伺服器。所以若網站伺服器已更換憑證，網路設備卻沒一併更換，當連線經過網路設備時，就會看到舊的憑證。

解決方式:若要確認從 internet 上看到的憑證是不是目前這台伺服器所裝的，可藉由關閉目前這台伺服器的服務，重新由 internet 連線網站，確認是否已看不到憑證資訊，若看不到，可確認憑證確實是裝在這台伺服器。

情況 5:

原因說明:您的網站伺服器並非建在公司內部，而是建在外部廠商那一端。

解決方式:若您的 CSR 是由廠商提供的，請直接將憑證轉交給廠商，請他們協助安裝;若 CSR 是由貴公司產製，請將憑證及金鑰一併提供給廠商，再請他們協助安裝。

4.7 其他

Q1、TWCA 核發的各種 SSL 憑證其作用為何？Server 端為何需要安裝完整憑證鏈？

說明：

- 根憑證 root.cer：階層式信任架構最高層，信任根憑證即信任全部憑證鏈；中繼憑證 uca.cer：階層式信任架構界接伺服器憑證與根憑證；伺服器憑證 server.cer：安裝於 AP 或 WEB 伺服器上的網站憑證。
- SSL 憑證為階層式信任，由上而下根憑證→中繼憑證→伺服器憑證
- Server 端安裝中繼憑證，伺服器憑證才可認得根憑證；Server 與 Client 共同信任根憑證，https 加密得以正常信任。
- 所以只要 Web Server 端安裝完整憑證鏈，且 Client 與 Server 網路連線是正常的，Client 端無須再安裝任何憑證，即可正常瀏覽網站內容且不會出現憑證不受信任錯誤訊息。

5.附件

無。