SSL 憑證 IIS 與 Apache 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-03-159
生效日期：109 年 3 月 3 日

目　　錄

1.目的

1.1. 介紹 SSL 憑證 IIS 及 Apache 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 IIS 或 Apache 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 IIS 轉至 Apache

5.1.1 先由 IIS 匯出 SSL 憑證交換檔，匯出格式為 pfx。

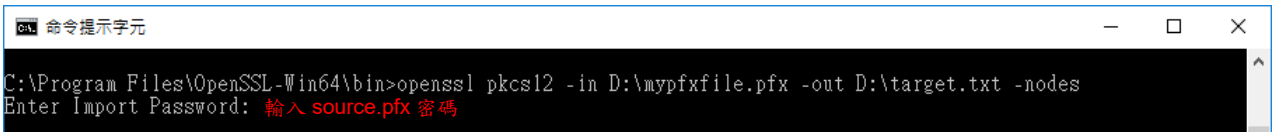
5.1.2 2. 使用 openssl 轉換，指令如下:

openssl pkcs12 -in {來源 pfx 檔案路徑} -out {輸出 txt 的檔案路徑} -nodes

source.pfx：由 IIS 匯出之包含金鑰憑證交換檔

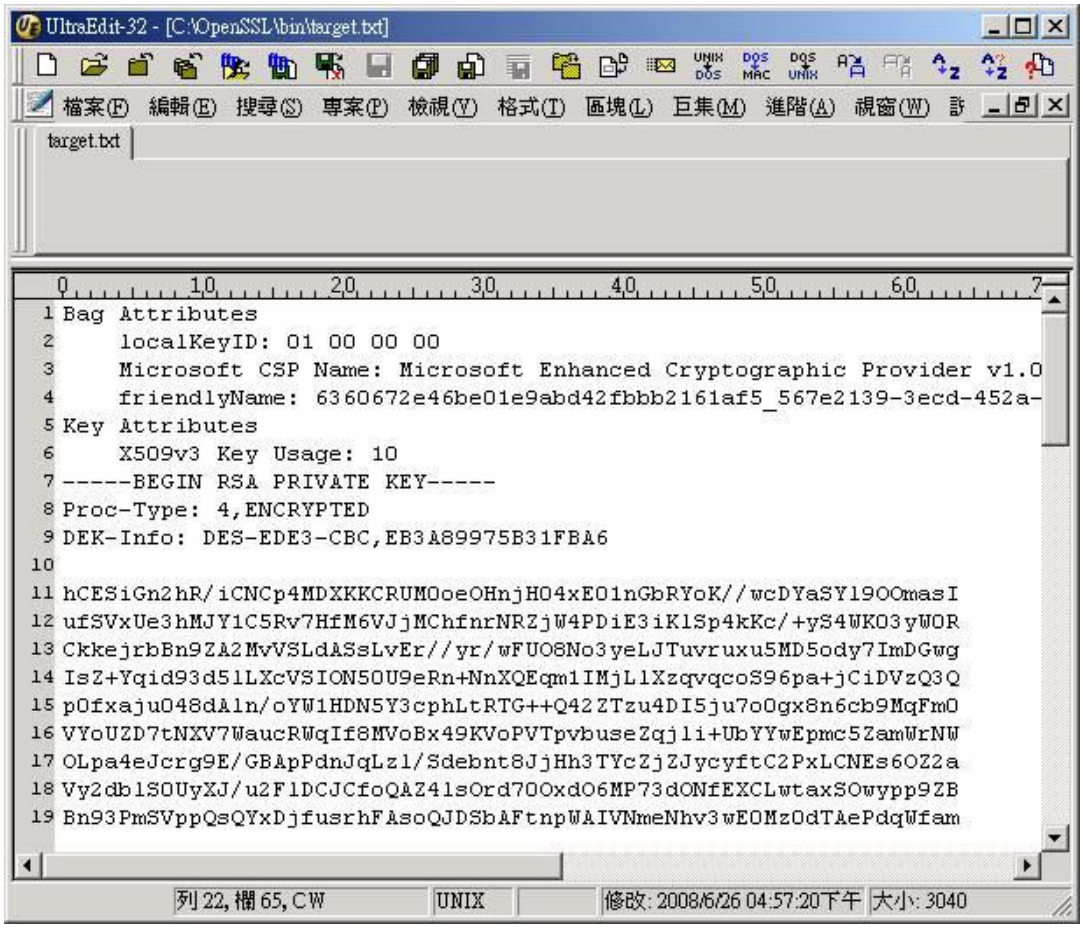
target.txt：將 source.pfx 轉換成文字檔輸出之檔案

5.1.3 需輸入來源 pfx 密碼。

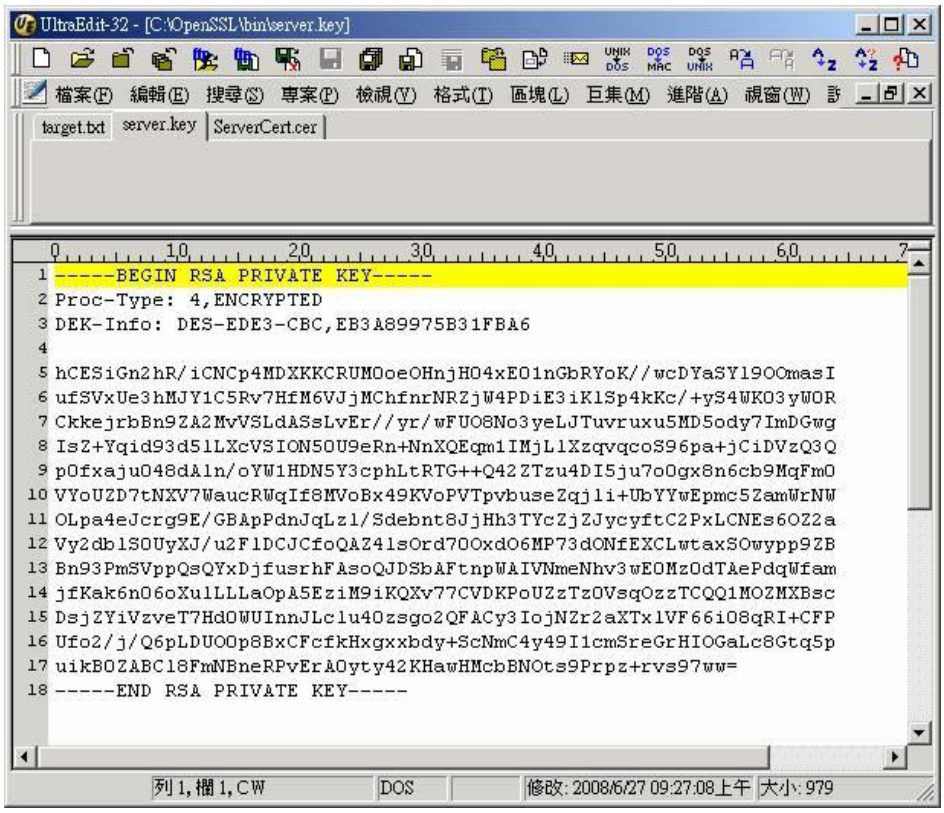


5.1.4 此時會產生 target.txt 檔案(內含金鑰及憑證資訊)。

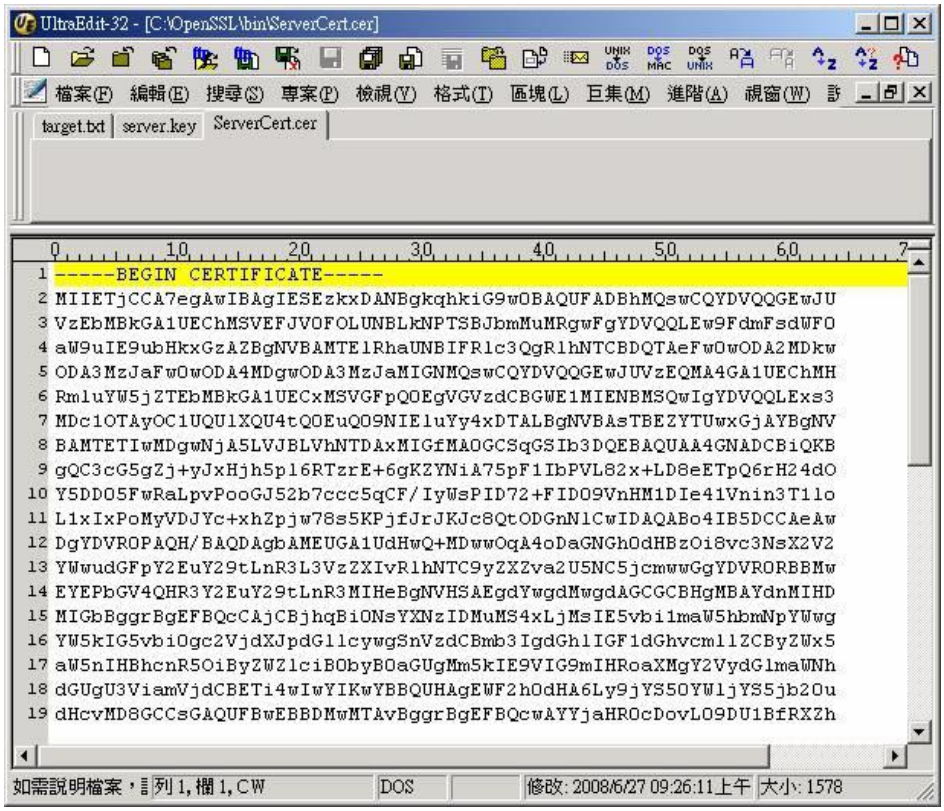
5.1.5 使用文書編輯軟體打開 target.txt。



5.1.6-----BEGIN RSA PRIVATE KEY-----及-----END RSA PRIVATE KEY-----區塊另存為金鑰檔。



5.1.7-----BEGIN CERTIFICATE-----及-----END CERTIFICATE-----區塊另存為憑證檔。



5.1.8 接著請參考 Apache 操作手冊，從下載已核發憑證章節，繼續往下完成憑證安裝步驟。

註:在安裝憑證章節所需要的 SSL 伺服器金鑰就是 5.1.6 章節另存的金鑰檔。

5.2 Apache 轉至 IIS

5.2.1 請參考以下轉換指令，將 Apache 相關憑證檔案，轉換為 IIS 所需要的 pfx 檔。

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.cer -certfile uca.cer

server.pfx：匯出之金鑰憑證交換檔

server.key：金鑰檔路徑

sever.cer：TWCA 核發之伺服器憑證檔路徑

uca.cer：TWCA 核發之中繼憑證檔路徑

輸入匯出 pfx 指令的密碼。

輸入第二次密碼確認。

5.2.2 參考 IIS 操作手冊，從安裝根憑證章節開始，完成所有安裝步驟，其中伺服器憑證就是剛剛匯出的 server.pfx。

6.附件

無。