

SSL 憑證 IIS 與 Apache 格式互轉說明手冊

機密等級：公開
版本：V5.0
文件編號：MNT-03-161
生效日期：年 月 日



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

目 錄

1.目的	1
2.範圍	2
3.參考資料	3
4.定義	3
5.作業程序	5
5.1 IIS 轉至 APACHE.....	5
5.2 APACHE 轉至 IIS	8
6.附件	9

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

3. 參考資料

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

4. 定義

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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。

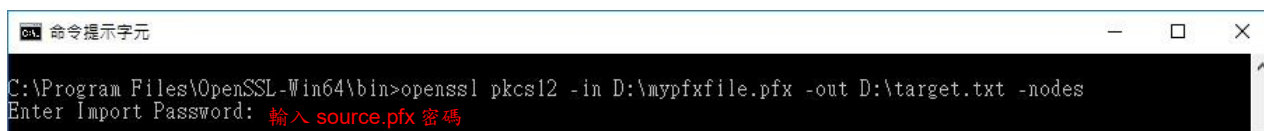
5.1.2 使用 openssl 轉換，指令如下：

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

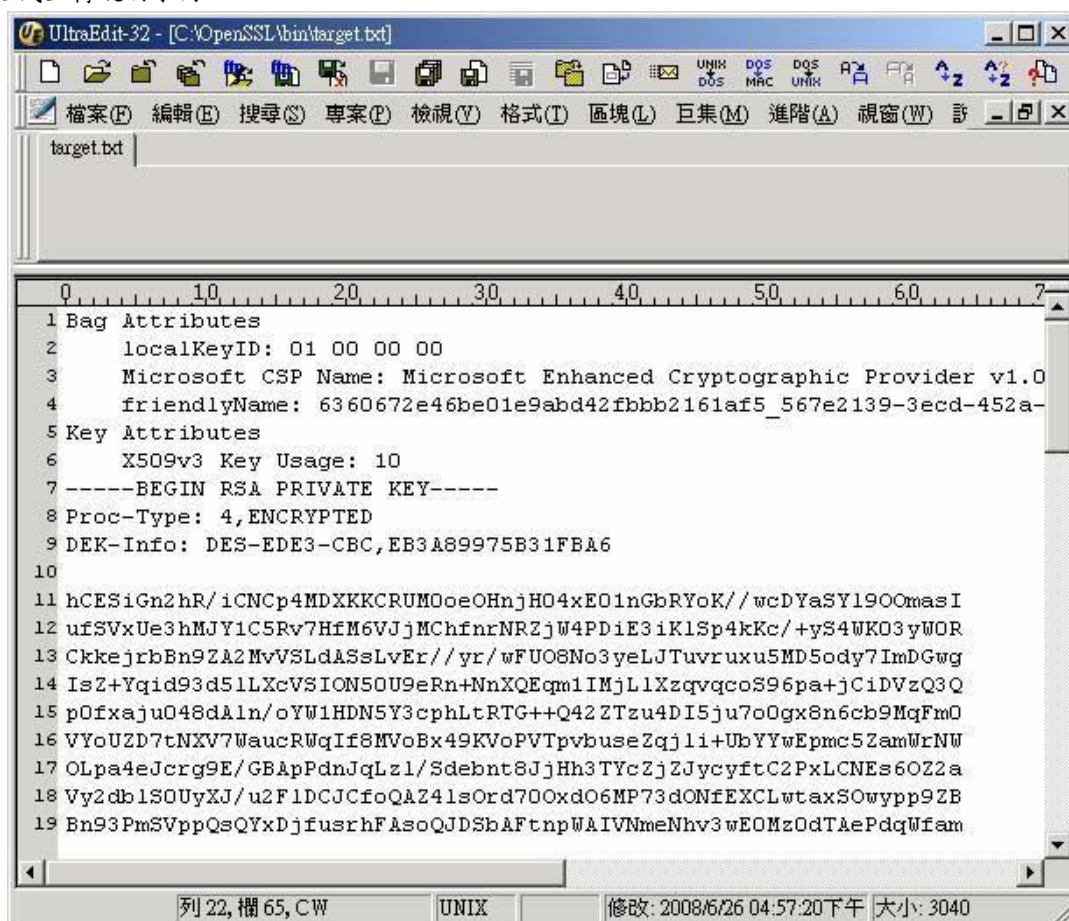
5.1.3 需輸入來源 pfx 密碼。



```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs12 -in D:\mypfxfile.pfx -out D:\target.txt -nodes
Enter Import Password: 輸入 source.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。

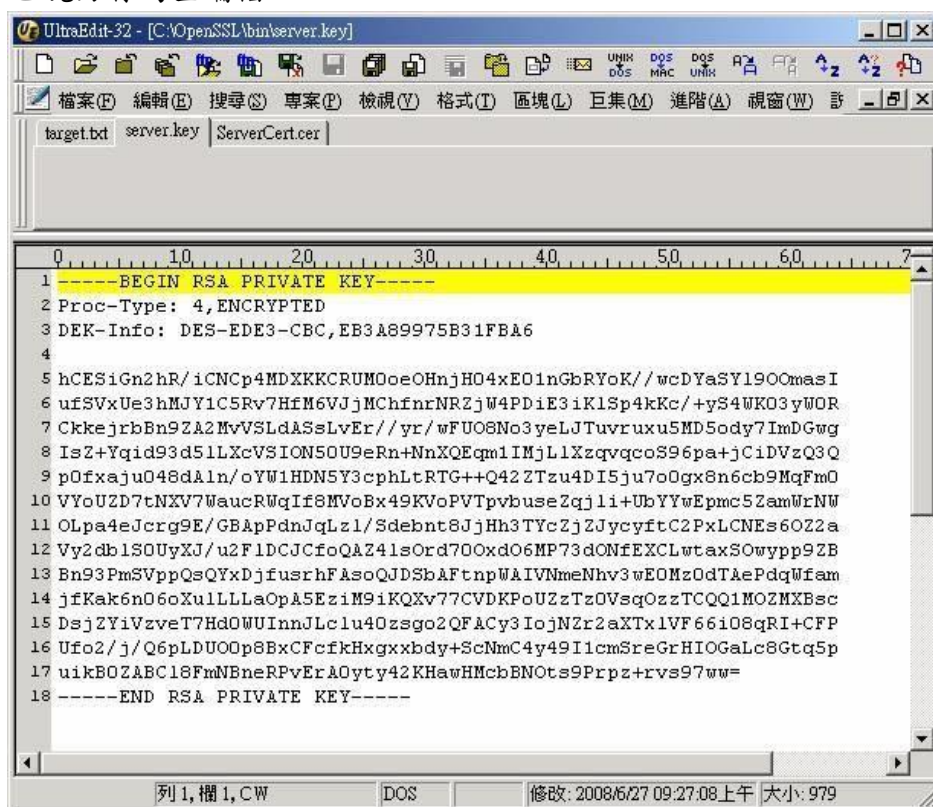


```

target.txt
0 10 20 30 40 50 60 70
1 Bag Attributes
2   localKeyID: 01 00 00 00
3   Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
4   friendlyName: 6360672e46be01e9abd42fbbb2161af5_567e2139-3ecd-452a-
5 Key Attributes
6   X509v3 Key Usage: 10
7 -----BEGIN RSA PRIVATE KEY-----
8 Proc-Type: 4, ENCRYPTED
9 DEK-Info: DES-EDE3-CBC, EB3A89975B31FBA6
10
11 hCESiGn2hR/iCNCp4MDXKKCRUM0oeOHnjH04xE01nGbRYoK//wcDYaSY190OmasI
12 uFSVxUe3hMJY1C5Rv7HfM6VJjMChfNRZjW4PdiE3iK1Sp4kKc/+yS4WK03yWOR
13 CkkejrbBn9ZA2MvVSLdASsLvEr//yr/wFU08No3yeLJTuvruxu5MD5ody7ImDGwg
14 IsZ+Yqid93d51LXcVSI0N50U9eRn+NnXQEqm1IMjL1XzqvqcoS96pa+jCiDVzQ3Q
15 pOfxaju048dAln/oYW1HDN5Y3cphLRTG++Q42ZTzu4DI5ju7o0gx8n6cb9MqFm0
16 VYoUZD7tNXV7WaucRWqIf8MVoBx49KVoPVTpvbuseZqj1i+UoYYwEpmc5ZamWnNW
17 OLpa4eJcrg9E/GBApPdnJqLz1/Sdebnt8JjHh3TYcZjZJycyftC2PxLCNEs6OZ2a
18 Vy2db1S0UyXJ/u2F1DCJCfoQA241sOrd70OxdO6MP73dONfEXCLwtaxSowyp9ZB
19 Bn93PmSVppQsQYxDjfusrhFAsoQJDSbAftnpWAIvNmeNhv3wEOMzOdTAEpdqWfam
列 22, 欄 65, CW UNIX 修改: 2008/6/26 04:57:20 下午 大小: 3040

```

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



```

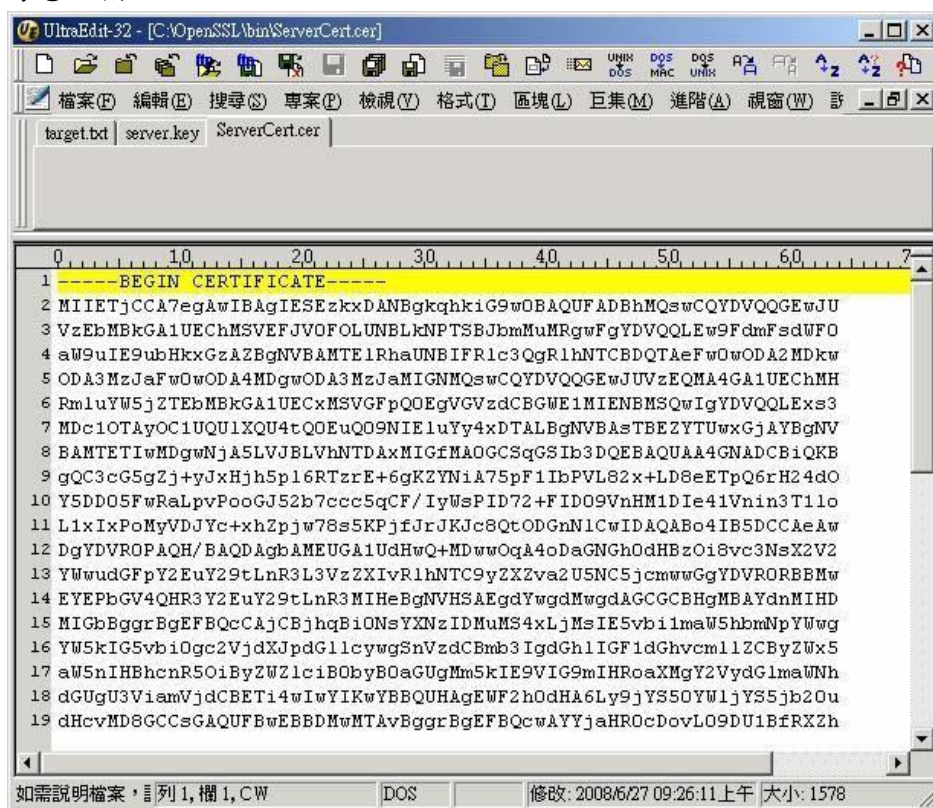
UltraEdit-32 - [C:\OpenSSL\bin\server.key]
檔案(F) 編輯(E) 搜尋(S) 專案(P) 檢視(V) 格式(T) 區塊(L) 巨集(M) 進階(A) 視窗(W) 語
target.txt server.key ServerCert.cer
0 10 20 30 40 50 60 70
1 -----BEGIN RSA PRIVATE KEY-----
2 Proc-Type: 4, ENCRYPTED
3 DEK-Info: DES-EDE3-CBC, EB3A89975B31FBA6
4
5 hCESiGn2hR/iCNCp4MDXKKCRUM0oeOHnjH04xE01nGbRYoK//wcDYaSY190OmasI
6 uFSVxUe3hMJY1C5Rv7HfM6VJjMChfNRZjW4PdiE3iK1Sp4kKc/+yS4WK03yWOR
7 CkkejrbBn9ZA2MvVSLdASsLvEr//yr/wFU08No3yeLJTuvruxu5MD5ody7ImDGwg
8 IsZ+Yqid93d51LXcVSI0N50U9eRn+NnXQEqm1IMjL1XzqvqcoS96pa+jCiDVzQ3Q
9 pOfxaju048dAln/oYW1HDN5Y3cphLRTG++Q42ZTzu4DI5ju7o0gx8n6cb9MqFm0
10 VYoUZD7tNXV7WaucRWqIf8MVoBx49KVoPVTpvbuseZqj1i+UoYYwEpmc5ZamWnNW
11 OLpa4eJcrg9E/GBApPdnJqLz1/Sdebnt8JjHh3TYcZjZJycyftC2PxLCNEs6OZ2a
12 Vy2db1S0UyXJ/u2F1DCJCfoQA241sOrd70OxdO6MP73dONfEXCLwtaxSowyp9ZB
13 Bn93PmSVppQsQYxDjfusrhFAsoQJDSbAftnpWAIvNmeNhv3wEOMzOdTAEpdqWfam
14 jfKak6n06oXullLlaOpA5EziM9iKQXv77CVDKPoUzZTzOVsqOzzTCQQ1MOZMXBsc
15 Dsj2YiVzveT7HdOWUInnJLcl1u40zsgo2QFACy3IoJNzr2aXTx1VF66i08qRI+CFP
16 Ufo2/j/Q6pLDUOp8BxCfCfKXgxxbdy+ScNmC4y49I1cmSreGrHIOGaLc8Gtq5p
17 uikB0ZABC18FmNBneRPvErA0yty42KHawHMcbENots9Prpz+rvs97ww=
18 -----END RSA PRIVATE KEY-----
列 1, 欄 1, CW DOS 修改: 2008/6/27 09:27:08 上午 大小: 979

```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

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
```

```
C:\Program Files\OpenSSL-Win64\bin>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。

```
Enter Export Password:
```

輸入第二次密碼確認。

```
Verifying - Enter Export Password:
```

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。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.