The Will Will Web
記錄著 Will 在網路世界的學習心得與技術分享

← 認識 Angular Library 函式庫專案並學會自製 Angular 表單驗證器模組

深入理解 C# 7.1 提供的 async 非同步 Main() 方法 →

如何在收到 PFX 或 CER 憑證檔之後使用 OpenSSL 進行常見的格式轉換

分享

2019/04/17 17:19　Will 保哥　系統管理

由於我們公司有經銷代理 TWCA SSL 憑證，最近有個客戶續約 SSL 憑證時，卻不知道如何進行安裝，這部份我已經寫過很多篇文章，不過我們這次的客戶比較不一樣，因為該客戶所署的環境有 IIS、Apache 與 .NET Core 2.2 三種不同的網站伺服器，這種情況下勢必需對不同的憑證格式轉換，所以我今天打算用這篇文章整理 PFX 與 PEM 格式之間轉換的技巧。

簡介憑證申請的過程

這個段落我只打算簡介這個過程，詳細的介紹我已經寫過不少文章，各位可以參考如下：

- 認識 PKI 架構下的數位憑證格式與憑證格式轉換的心得分享
- 如何在 IIS7 / IIS7.5 安裝 SSL 憑證（含 IIS7 匯入憑證的 Bug）
- 購買與安裝 SSL 憑證完全攻略（以 IIS7 為例）
- 免費申請 StartSSL™ 個人數位簽章與網站 SSL 憑證完全攻略

基本的憑證申請程序如下：

1. 客戶　建立一個　私密金鑰檔　(Private Key File)
2. 客戶　利用這個　私密金鑰檔　建立一個　憑證要求檔　(CSR) (Certificate Signing Request)
3. 客戶　將　憑證要求檔　提交給　憑證經銷商　申請憑證
4. 憑證經銷商　將　憑證要求檔　交給　憑證簽署廠商　(TWCA) 核發　伺服器憑證　檔案
5. 憑證簽署廠商 (TWCA) 將　伺服器憑證　檔案交回　憑證經銷商
6. 憑證經銷商　將　伺服器憑證　交給　客戶
7. 客戶　將　伺服器憑證　與　私密金鑰檔　合併為 PFX 檔案
8. 客戶　將 PFX 檔案安裝至 IIS 或 .NET Core 應用程式
9. 客戶　將 PFX 檔案匯出　伺服器憑證檔　與　私密金鑰檔　並安裝至 Apache 或 Nginx

以上就是大致的步驟，從安全的角度來看，任何人拿到憑證檔案都是無效的，只有擁有　私密金鑰檔　的人，才能將憑證解開使用。

> 備註：有些客戶對上述流程並不熟悉，所以很多時候就必須代替客戶產生好現成的 PFX 檔案，讓他們直接便利的安裝到網站伺服器中，**方便性**與**安全性**總是衝突的！

將　伺服器憑證　與　私密金鑰檔　合併為 PFX 檔案

這應該是最常見的操作，最簡單的方式就是透過 OpenSSL 進行合併，命令如下：

```
openssl pkcs12 -in server.cer -inkey my.key -export -out server.pfx -password pass:vEryComPleXPw
```

參數解說：

- `pkcs12` 代表你要執行 PKCS#12 憑證格式的相關操作
- `-in server.cer` 代表你的輸入憑證檔
  - 這個 `server.cer` 就是申請憑證時核發過的　伺服器憑證　檔案
- `-inkey my.key` 代表你當時建立　憑證要求檔　時所用的　私密金鑰檔
  - 這個 `my.key` 必須為當時建立 CSR 檔案用的那一把私密金鑰
- `-export` 代表你想輸出一份 PKCS#12 憑證檔案
- `-out server.pfx` 代表你想輸出的 `*.pfx` 檔名
- `-password pass:vEryComPleXPw` 代表你想設定的 PFX 檔案密碼 (因為 PFX 檔案被要求一定要設定密碼)
  - 這個參數可以省略不打，執行命令的時候他會自動提醒你輸入密碼
  - 這裡的 `vEryComPleXPw` 就是你要設定給 PFX 的密碼 (明碼)，請記得留住！

將 PFX 檔案轉換成　伺服器憑證檔　與　私密金鑰檔

我們拿到 PFX 檔案後，如果你想將憑證安裝到 Apache 或 Nginx 之中，通常需要再做格式轉換，轉換成兩個獨立的　伺服器憑證　與　私密金鑰檔　。

這時你可能會想問，用原本拿到的　伺服器憑證檔　與　私密金鑰檔　不行嗎？

因為產生　憑證要求檔　的　私密金鑰檔　通常都會加密過，如果用這組有加密過的金鑰，當 Apache 或 Nginx 啟動的時候就需要人為介入輸入憑證密碼才能繼續，如此一來就會卡住整個網站伺服器的啟動程序！所以實務上來說，我們會將　私密金鑰檔　解密，用　無密碼保護　的　私密金鑰檔　進行部署。

> 請注意　私密金鑰檔　的檔案權限設定，不要讓沒有權限的人取得該檔案。

所以，你可能會有兩種選擇：

1. 直接移除　私密金鑰檔　的密碼保護

   ```
   openssl rsa -in my.key -out server.key
   ```

   有加密的 `*.key` 檔案，前三行是這樣的，你可以看到一個 `ENCRYPTED` 字樣：

   ```
   -----BEGIN RSA PRIVATE KEY-----
   Proc-Type: 4,ENCRYPTED
   DEK-Info: DES-EDE3-CBC,1B11BF47006C0CB8
   ```

   未加密的 `*.key` 檔案，第一行是這樣的：

   ```
   -----BEGIN RSA PRIVATE KEY-----
   ```

   接著你就可以拿 `server.key` 與 `server.cer` 進行部署，直接到 Apache 或 Nginx 設定檔進行 SSL 相關設定即可。

2. 直接從 PFX 檔案匯出　伺服器憑證檔　與　私密金鑰檔

   畢竟你已經拿到了 PFX 檔案，裡面已經包含了　伺服器憑證檔　與　私密金鑰檔　，如果當時手邊並沒有當初建立 CSR 的　私密金鑰檔　時，你就需要學會如何直接從 PFX 檔案匯出　伺服器憑證檔　與　私密金鑰檔　！

   假設你手邊只有一個 `server.pfx` 檔案，其密碼為 `vEryComPleXPw`，你想匯出 `server.cer` 與 `server.key` 檔案，那麼你可以執行以下命令：

   1. 產生　伺服器憑證　(`server.cer`)

      命令提示字元 (Windows)

      ```
      openssl pkcs12 -in server.pfx -nokeys -password "pass:vEryComPleXPw" -out - 2>nul
      | openssl x509 -out server.crt
      ```

      Linux Shell 環境

      ```
      openssl pkcs12 -in server.pfx -nokeys -password "pass:vEryComPleXPw" -out - 2>/de
      v/null | openssl x509 -out server.crt
      ```

   2. 產生　私密金鑰檔　(`server.key`)

      ```
      openssl pkcs12 -in server.pfx -nocerts -password "pass:vEryComPleXPw" -nodes -out
      server.key
      ```

   參數解說：

   - `-nokeys` 代表你不要輸出　私密金鑰檔　(僅輸出憑證檔案)
   - `-nocerts` 代表你不要輸出　伺服器憑證檔　(僅輸出金鑰檔案)
   - `-nodes` 是 No DES 的意思，代表你想輸出一個**沒有密碼保護**的　私密金鑰檔

相關連結

- /docs/man1.0.2/man1/openssl-pkcs12.html
- /docs/man1.0.2/man1/openssl-rsa.html
- openssl 指令 command line - 轉檔 pem/der/p7b/pfx/cer | SSORC.tw
- Jimmy's Blog: OpenSSL 操作筆記 - 檔案格式轉換

標籤：pfx, certificate, 憑證, apache, nginx, iis

相關文章

如何在收到 PFX 或 CER 憑證檔之後使用 OpenSSL 進行常見的格式轉換
由於我們公司有經銷代理 TWCA SSL 憑證，最近有個客戶續約 SSL 憑證時，卻不知道如何進行安裝，這部份我已經寫過很多篇文章...

如何在 Windows Containers 建立內含正式 SSL/TLS 憑證的 IIS 網站
張傑晨 ASP.NET 網站安裝至 Windows Containers 專題中，其實遠簡單，直接使用微軟官方提供的 mcr.microsoft.com/dotnet/fra...

如何使用 Certbot 建立免費的 TLS/SSL 網域憑證並自動產生 PFX 憑證
我之前有寫過一篇 如何使用 Certbot 命令列工具建立免費的 TLS/SSL 萬萬網域憑證 文章，萬神的情境是我的域名是 萬萬網域 (nake...

你覺得這篇文章如何？
11 Responses