

← 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

讚

分享

199 人說過讚，成為朋友中第一個說讚的人。



由於我們公司有經銷代理 TWCA SSL 憑證，最近有個客戶續的 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，因為該客戶佈署的環境有 IIS、Apache 與 .NET Core 2.2 三種不同的網站伺服器，這種情況下勢必面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：

- 客戶 建立一個 **私密金鑰檔** (Private Key File)
- 客戶 利用這個 **私密金鑰檔** 建立一個 **憑證要求檔** (CSR) (Certificate Signing Request)
- 客戶 將 **憑證要求檔** 提交給 **憑證經銷商** 申請憑證
- 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
- 憑證簽署廠商** (TWCA) 將 **伺服器憑證** 檔案交由 **憑證經銷商**
- 憑證經銷商** 將 **伺服器憑證** 交給 **客戶**
- 客戶 將 **伺服器憑證** 與 **私密金鑰檔** 合併為 PFX 檔案
- 客戶 將 PFX 檔案安裝至 IIS 或 .NET Core 應用程式
- 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)，請記得修改！

### 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 **伺服器憑證檔** 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，你可能會會有兩種選擇：

- 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,1B11BF4708EBCB8
```

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。

- 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：

- 產生 **伺服器憑證檔** ( **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>/dev/null | openssl x509 -out server.crt
```

- 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

若想像 ASP.NET 網站安裝至 Windows Containers 容器中，其實還算簡單，直接使用微軟官方所提供的 mcr.microsoft.com/dotnet/framework...

#### 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 證書網域憑證 文章，當時的傳聞是我的域名是 頂層網域 (make...

你覺得這篇文章如何？

11 Responses



太棒了



風趣幽默



超愛這篇



有震撼到

1 Comment

The Will Will Web

Disqus' Privacy Policy

Login

Favorite

Tweet

Share

Sort by Best

Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

DISQUS

Subscribe

Add Disqus to your site

Do Not Sell My Data

### 聯播文章

- 黑暗執行緒2022 香魚馬Git 實戰 - 將檔案從歷史 Commit 中移除【茶包射手筆記】AD Domain Controller 出現某主機的本地帳號登入錯誤
- Scott HanselmanUsing Home Assistant to integrate a Unifi Pro...JavaScript and TypeScript Projects with React...A Nightscout Segment for OhMyPosh shows my re...

Download OPML file

### 免責聲明

本網站對於任何使用或引用本網站網頁資料引致之損失或損害，概不負責。本網站亦有權隨時刪除、暫停或編輯本網站所登載之各項資料，以維護本網站之權益。除法律有強制規定外，在任何情況下，本網站對於 (1) 使用或無法使用本網站之各項服務；(2) 經由本網站取得訊息或進行交易；(3) 第三人在本網站上之陳述或作為；以及 (4) 其他與本網站服務有關之事項所致生之任何直接、間接、附帶、特別、懲罰性或衍生性損害，一概不負賠償責任。

### 工商服務 (廣告)



搜尋...

搜尋

### 每月文章

2022

三月 (7)

二月 (9)

一月 (15)

2021

2020

2019

2018

2017

2016

2015

2014

2013

2012

2011

2010

2009

2008

2007

### 文章分類

- .Net (215)
- .NET Core (53)
- Accessibility (3)
- Angular (22)
- AngularJS (11)
- ASP.NET (222)
- ASP.NET 5 (3)
- ASP.NET Blazor (1)
- ASP.NET Core (31)
- ASP.NET Identity (2)
- ASP.NET MVC (104)
- ASP.NET Web API (13)
- Azure DevOps (24)
- C# (124)
- Cloud Computing (4)
- CSS (29)
- DevOps (20)
- Docker (23)
- Entity Framework (21)
- Git (28)
- Golang (2)
- HTML5 (8)
- IIS (103)
- Java (7)
- JavaScript (108)
- Jenkins (7)
- Kubernetes (9)
- LINQ (36)
- Linux (108)
- Microsoft Azure (35)
- MySQL (15)
- Office (49)
- Office 365 (28)
- Oracle (10)
- PHP (25)
- Scrum (1)
- Security (60)
- SQL Server (125)
- Subversion (35)
- System Center (2)
- TFS (6)
- TFS2010 (10)
- Tips (188)
- Unit Testing (10)
- Usability (1)
- VBA (5)
- Visual Basic (5)
- Visual Studio (122)
- Visual Studio 11 (2)
- Visual Studio 2012 (10)
- Visual Studio 2013 (4)
- VS2010 Tips (23)
- Web (167)
- WebMatrix (8)
- Windows (38)
- Windows 8 (14)
- Windows Azure (18)
- Windows Phone 7 (14)
- 介紹好用工具 (221)
- 心得分享 (85)
- 多奇快訊 (7)
- 系統管理 (358)
- 前端工程研究 (18)
- 專案管理 (8)
- 團隊合作 (9)
- 網路管理 (18)

### 專業證照



微軟最有價值專家 & Google 開發專家

