The Will Will Web

記載著 Will 在網路世界的學習心得與技術分享

← 如何將 Protractor 設定檔 (protractor.conf.js) 加入 TypeScript 型別檢查

Ubuntu 18.04.1 LTS 執行 apt update 遇到 Hash Sum mismatch 的處理方式 →

如何使用 OpenSSL 建立開發測試用途的自簽憑證 (Self-Signed Certificate)

2019/02/25 12:57 Will 保哥 Linux, Windows, 介紹好用工具, 系統管理 分享

讚 分享 364 人說這個讚。成為朋友中第一個說讚的人。

如果要產生開發測試用途的自簽憑證，說到底還是跨平台的 OpenSSL 好用，這篇文章我就來談談如何透過 OpenSSL 工具來產生可信賴的 SSL/TLS 自簽憑證。

安裝 OpenSSL 工具

在進行安裝之前，請先檢查是否已經安裝過，因為你很有可能系統已經內建，或是曾經安裝過卻忘記了。建議開啟終端機視窗 (命令提示字元)，輸入 `openssl version` 檢查看看是否會顯示目前安裝的 OpenSSL 版本。

- Windows
  - 使用 Git 內建的 OpenSSL 工具

    當你安裝好 Git for Windows 的時候，其實就已經內建了 OpenSSL 工具，預設執行檔路徑為 `C:\Program Files\Git\usr\bin\openssl.exe`，你可以將 `C:\Program Files\Git\usr\bin` 路徑加入到 `PATH` 環境變數之中，以後就可以直接輸入 `openssl` 來執行此工具。
  - 透過預先編譯好的 OpenSSL 安裝程式

    Win32/Win64 OpenSSL Installer for Windows - Shining Light Productions (下載第一個)
  - 透過 Chocolatey 進行自動安裝

    Chocolatey Gallery | OpenSSL – The Open Source SSL and TLS toolkit 1.1.1.20181020

    ```
    choco install openssl.light -y
    ```
- Linux
  - Ubuntu

    ```
    sudo apt install openssl
    ```
  - CentOS / RedHat

    ```
    sudo yum install openssl
    ```
- macOS
  - Homebrew

    ```
    brew update
    brew install openssl
    echo 'export PATH="/usr/local/opt/openssl/bin:$PATH"' >> ~/.bash_profile
    source ~/.bash_profile
    ```
  - 手動安裝

    請參考 Installing OpenSSL on macOS 相關說明。

使用 OpenSSL 建立自簽憑證

基本上按照下列步驟，就一定能建立出合法的自簽憑證：

1. 建立 `ssl.conf` 設定檔

   ```
   [req]
   prompt = no
   default_md = sha256
   default_bits = 2048
   distinguished_name = dn
   x509_extensions = v3_req

   [dn]
   C = TW
   ST = Taiwan
   L = Taipei
   O = Duotify Inc.
   OU = IT Department
   emailAddress = admin@example.com
   CN = localhost

   [v3_req]
   subjectAltName = @alt_names

   [alt_names]
   DNS.1 = *.localhost
   DNS.2 = localhost
   IP.1 = 192.168.2.100
   ```

   上述設定檔內容的 `[dn]` 區段 (Distinguished Name) 為憑證的相關資訊，你可以自由調整為你想設定的內容，其中 `O` (Organization) 是公司名稱，`OU` (Organization Unit) 是部門名稱，而 `CN` (Common Name) 則是憑證名稱，你可以設定任意名稱，設定中文也可以，但請記得檔案要以 UTF-8 編碼存檔，且不能有 BOM 字元。

   設定檔的 `[alt_names]` 區段，則是用來設定 SSL 憑證的域名，這部分設定相當重要，如果沒有設定的話，許多瀏覽器都會將憑證視為無效憑證。這部分你要設定幾組域名都可以，基本上沒有什麼上限，因為自簽憑證主要目的是用來開發測試之用，因此建議可以把可能會用到的本機域名 (`localhost`) 或是區域網路的 IP 地址都加上去，以便後續進行遠端連線測試。

   如果你希望在 Google Chrome 瀏覽器也能瀏覽受信任的 SSL 網站，那麼設定正確的域名是非常重要的，這部分的相關知識我在 如何使用 PowerShell 建立開發測試用途的自簽憑證 (Self-Signed Certificate) 這篇文章中有完整說明。
2. 透過 OpenSSL 命令產生出自簽憑證與相對應的私密金鑰

   透過以下命令就可以建立出 **私密金鑰** (`server.key`) 與 **憑證檔案** (`server.crt`)：

   ```
   openssl req -x509 -new -nodes -sha256 -utf8 -days 3650 -newkey rsa:2048 -keyout server.
   key -out server.crt -config ssl.conf
   ```

   請注意：上述命令會建立一個「未加密」的私密金鑰檔案，使用 PEM 格式輸出。
3. 透過 OpenSSL 命令產生 PKCS#12 憑證檔案 (`*.pfx` 或 `*.p12`)

   如果你想將建立好的 **私密金鑰** (`server.key`) 與 **憑證檔案** (`server.crt`) 組合成一個 PFX 憑證檔案 (PKCS#12)，可以透過以下命令產生 `server.pfx` 檔案。由於 `*.pfx` 格式的檔案必須設定一組密碼，因此在執行過程中會需要輸入密碼，用以保護這個 `*.pfx` 檔案。

   ```
   openssl pkcs12 -export -in server.crt -inkey server.key -out server.pfx
   ```

如此以來，你就擁有三個檔案，分別是：

1. `server.key` (私密金鑰) (使用 PEM 格式) (無密碼保護)
2. `server.crt` (憑證檔案) (使用 PEM 格式)
3. `server.pfx` (PFX 檔案) (使用 PKCS#12 格式)

   ※ 設定 IIS 網站繫結的時候，必須使用 PFX 格式的憑證檔案。

接下來，就是將憑證與金鑰安裝到網站伺服器中，有上述三個檔案就幾乎足以讓你設定給 IIS, Apache, nginx, Angular Live Development Server 等不同網站環境使用了。

匯入自簽憑證到「受信任的根憑證授權單位」

光是建立好自簽憑證還是不夠的，網站伺服器也設定正確才行，這畢竟是一個 PKI 基礎架構，你還必須讓**所有需要安全連線的端點**都能**互相信任**才行，因此你還須將建立好的自簽憑證安裝到「**受信任的根憑證授權單位**」之中，這樣子你的作業系統或瀏覽器才能將你的自簽憑證視為「可信任的連線」，以下是不同作業系統平台的設定方式：

- Windows

  請以「系統管理員身分」執行以下命令，即可將憑證匯入到 Windows 的憑證儲存區之中：

  ```
  certutil -addstore -f "ROOT" server.crt
  ```

  若要以手動方式匯入，可以參考以下步驟：

  1. 開啟檔案總管，並滑鼠雙擊 `server.crt` 檔案
  2. 點擊「安裝憑證」按鈕
  3. 選取「目前使用者」並按「下一步」繼續
  4. 選取「將所有憑證放入以下的存放區」並按下「瀏覽」按鈕
  5. 選取「受信任的根憑證授權單位」並按下「確定」
  6. 按「下一步」繼續
  7. 按「完成」繼續
  8. 在 **安全性警告** 視窗按下「是(Y)」即可完成設定

  請注意：在匯入完成後 Google Chrome 瀏覽器可能不會立刻顯示這是個有效憑證 (因為快取的關係)，但你只要過一段時間重開 Chrome 瀏覽器，即可看見網址列的變化，不會再出現**紅色不安全**的提示。
- Linux (Ubuntu 18.04)

  注意：憑證的副檔名一定要是 `*.crt`

  ```
  sudo cp server.crt /usr/share/ca-certificates/
  sudo dpkg-reconfigure ca-certificates
  ```

  執行 `sudo dpkg-reconfigure ca-certificates` 的時候，會出現選單畫面，請記得勾選你複製進去的那張憑證，按下 Enter 之後就會全自動設定完成。
- Linux (Ubuntu, Debian)

  ```
  sudo cp server.crt /usr/local/share/ca-certificates/
  sudo update-ca-certificates
  ```
- Linux (CentOS 6, RedHat)

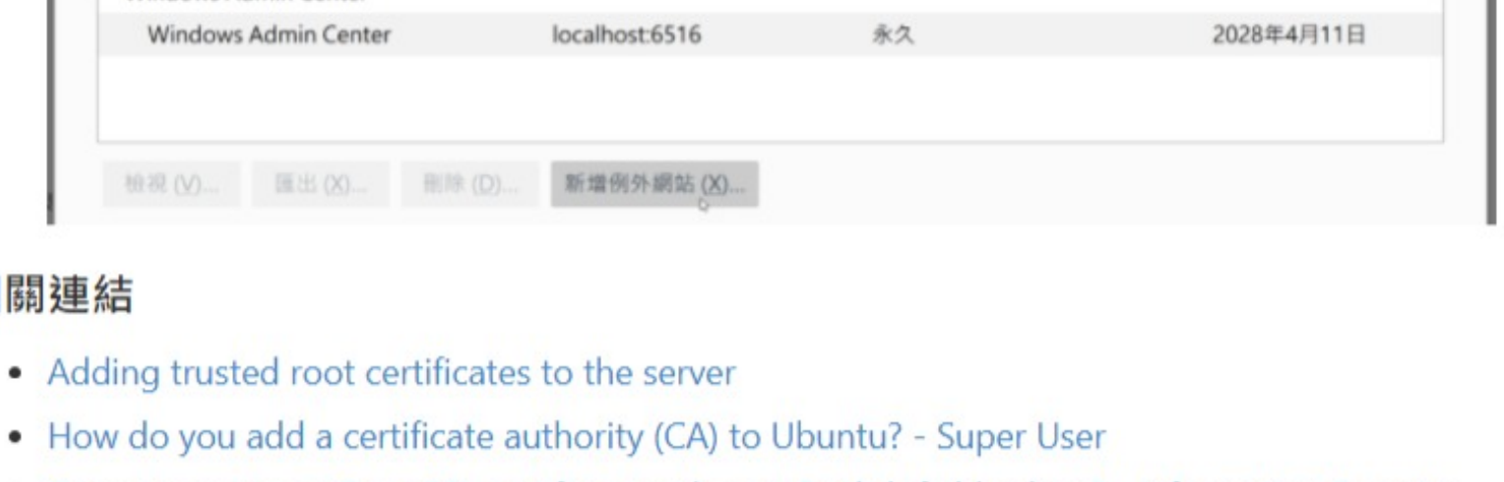
  ```
  sudo yum install ca-certificates
  sudo update-ca-trust force-enable
  sudo cp server.crt /etc/pki/ca-trust/source/anchors/
  sudo update-ca-trust extract
  ```
- Linux (CentOS 5)

  ```
  sudo cat server.crt >> /etc/pki/tls/certs/ca-bundle.crt
  ```
- macOS

  ```
  sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain se
  rver.crt
  ```
- Firefox

  因為 Firefox 瀏覽器內部自行維護了一份「受信任的根憑證授權單位」，因此就算你已經安裝自簽憑證到作業系統裡，還是要額外到 Firefox 瀏覽器的**設定**中手動加入**伺服器**憑證才行。

  1. 開啟 [選項] 功能
  2. 點擊「隱私權與安全性」
  3. 找到最下方的「檢視憑證」按鈕
  4. 點選「伺服器」頁籤
  5. 點擊「新增例外網站」
  6. 輸入網站網址 (位置) 並按下「取得憑證」
  7. 最後按下「確認安全例外」即可設定完成



您有可識別下列伺服器的憑證

憑證名稱	伺服器	有效時間	過期於
DigiNotar			
DigiNotar Root CA	*	永久	2025年4月1日
DigiNotar B.V.			
DigiNotar PKIoverheid CA Organisati...	*	永久	2020年3月23日
Windows Admin Center			
Windows Admin Center	localhost:6516	永久	2028年4月11日

相關連結

- Adding trusted root certificates to the server
- How do you add a certificate authority (CA) to Ubuntu? - Super User
- Can you create an OpenSSL certificate with non-English field values? - Information Security Stack Exchange
- Command Line Utilities - OpenSSLWiki

標籤 : openssl, 自簽憑證, linux, windows, macOS

相關文章

如何使用 OpenSSL 建立開發測試用途的自簽憑證 (Self-Signed Certificate)
如果要產生開發測試用途的自簽憑證，說到底還是跨平台的 OpenSSL 好用，這篇文章我就來談談如何透過 OpenSSL 工具來產生可...

如何使用 MakeCert 建立開發測試用途的自簽憑證 (Self-Signed Certificate)
無論我們開發網站或撰寫應用程式，都有可能會需要手動建立測試用的憑證，好讓我們的測試環境可以有效模擬像是 TLS/SSL 連線...

如何使用 PowerShell 建立開發測試用途的自簽憑證 (Self-Signed Certificate)
前篇文章我們學會了用老牌的 MakeCert 建立自簽憑證 (self-signed certificates)，對於大部分數位憑證的需求已經綽綽有餘，確實...

你覺得這篇文章如何？

21 Responses

太棒了 風趣幽默 超愛這篇 有震撼到

11 Comments The Will Will Web Disqus' Privacy Policy 1 Login

♡ Favorite 1 Tweet Share Sort by Best

Join the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS ?

Name

康賀鈞 · a month ago · edited
保哥，想請教一下
如果是上網購買申請到的憑證
還需要匯入到「受信任的根憑證授權單位」之中嗎？
-
另外
"光是建立好自簽憑證，網站伺服器也設定正確，還是不夠的。"
感覺改成這樣會比較好閱讀 =>
"光是建立好自簽憑證，還是不夠的，網站伺服器也設定正確。"
1 ^ | v · Reply · Share ›

> **Will** Mod → 康賀鈞 · a month ago
> 付費購買申請到的憑證通常不匯入到「受信任的根憑證授權單位」之中！
>
> 已調整文章描述，謝謝。
> 2 ^ | v · Reply · Share ›

Ignacio Chiu Yang · 2 years ago
想請教, 若是Socket Client /Server 間使用SSL通訊, 做法上該如何調整呢?
^ | v · Reply · Share ›

> **Will** Mod → Ignacio Chiu Yang · 2 years ago
> 看你用什麼程式語言吧
> ^ | v · Reply · Share ›

Terry Lin · 2 years ago
IP address不能這樣寫喔～
"DNS.3 = 192.168.2.100"

應該要改成如下：
"IP.1 = 192.168.2.100"
^ | v · Reply · Share ›

> **Will** Mod → Terry Lin · 2 years ago
> 我剛再確認，兩種設定對瀏覽器來說都可以識別。但你說的沒錯，用 IP.1 比較標準，我會調整文章中的範例，多謝！👍
> ^ | v · Reply · Share ›

> **Will** Mod → Terry Lin · 2 years ago
> 好像是耶！我印象中寫成 DNS 好像也可以？
> ^ | v · Reply · Share ›

James Li · 2 years ago
感謝分享, 請問我可以分享紀錄到自己的BLOG嗎?
^ | v · Reply · Share ›

> **Will** Mod → James Li · 2 years ago
> 可以
> ^ | v · Reply · Share ›

William Huang · 3 years ago
想請教自然人憑証可以轉成pfx檔案否
^ | v · Reply · Share ›

> **Will** Mod → William Huang · 3 years ago
> 沒辦法喔
> ^ | v · Reply · Share ›

Subscribe Add Disqus to your site Do Not Sell My Data DISQUS

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

Microsoft CERTIFIED Professional Developer — Web Developer 4

Microsoft CERTIFIED Technology Specialist — .NET Framework 4, Web Applications

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 出現某主機的本機帳號登入錯誤

Scott Hanselman
- Using 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

微軟最有價值專家 & Google 開發專家

MVP Microsoft® Most Valuable Professional

Experts 2019 Angular GDE