創作內容

OpenSSL 產憑證研究

0 GP

作者：pupu | 2017-07-04 16:34:03 | 巴幣：0 | 人氣：3387

緣由

因為測試服務越來越多用HTTPS，自己產完憑證，每次使用都要再加一次覺得麻煩。
因此來研究怎麼做根憑證與套用根憑證授權，以後直接加一次根憑證，後面授權的就可以全都用。

基本的就不介紹了，網路上有文章詳述。

(http://blog.yogo.tw/2009/11/ssl.html 或 google https, ssl 等等關鍵字)

有空有閒的話也許會有理論篇... (逃

開始

首先，要有安裝 OpenSSL ，在公司是用 CentOS，windows 上面也可以裝。
(http://slproweb.com/products/Win32OpenSSL.html)
下面使用 Win32OpenSSL_Light-1_1_0f.exe 版本。

創建根憑證

產生 Private Key。(-out 後面接輸出檔名；數字是key長度，越長越安全)

openssl genrsa -des3 -out RootCA.key 2048

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe genrsa -des3 -out RootCA.key 2048
Generating RSA private key, 2048 bit long modulus
.........................+++
.....................................................................................................+++
e is 65537 (0x010001)
Enter pass phrase for RootCA.key: 輸入CA密碼
Verifying - Enter pass phrase for RootCA.key: 再次輸入CA密碼
```

Linux 上通常會再執行 chmod，鎖定 key 檔存取權限。

chmod og-rwx RootCA.key

！！！ key 檔請注意保存 ！！！
憑證會有公鑰(crt)跟私鑰(key)，用一把鑰匙加密的東西可以用另一把解開，ROOT CA的私鑰被拿走以後，基本上拿走的人想簽甚麼就可以簽甚麼。

產生申請檔

openssl req -new -key RootCA.key -out RootCA.req

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe req -new -key RootCA.key -out RootCA.req
Can't open C:\Program Files (x86)\Common Files\SSL/openssl.cnf for reading, No such file or directory
2444:error:02001003:system library:fopen:No such process:crypto\bio\bss_file.c:74:fopen('C:\Program Files (x86)\Common F
iles\SSL/openssl.cnf','r')
2444:error:2006D080:BIO routines:BIO_new_file:no such file:crypto\bio\bss_file.c:81:
Enter pass phrase for RootCA.key:
2444:error:28069065:UI routines:UI_set_result:result too small:crypto\ui\ui_lib.c:778:You must type in 4 to 1023 charact
ers
```

作品資料夾

塗鴉 (14)
3D (8)
心得 (5)
教學(繪圖) (1)
程式 (4)
碎碎念 (2)
未分類 (2)

SET OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg

```
C:\OpenSSL-Win32\bin>SET OPENSSL_CONF=C:\OpenSSL-Win32\bin\openssl.cfg
```

再一次就成功了，下面就是輸入一些憑證資料，可以去網上查查。

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe req -new -key RootCA.key -out RootCA.req
Enter pass phrase for RootCA.key:輸入CA密碼
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyUnit
Common Name (e.g. server FQDN or YOUR name) []:Babu
Email Address []:babu@email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

產生憑證檔

days 後面是有效天數，3650 = 十年；編碼方式這邊用 sha256，**不建議用 sha1 ，有破解風險，新版瀏覽器也開始檔 SHA1 憑證了**。

openssl x509 -req -days 3650 -sha256 -signkey RootCA.key -in RootCA.req -out RootCA.crt

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe x509 -req -days 3650 -sha256 -signkey RootCA.key -in RootCA.req -out RootCA.crt

Signature ok
subject=C = TW, ST = Taiwan, L = Taipei, O = MyCompany, OU = MyUnit, CN = Babu, emailAddress = babu@email.com
Getting Private key
Enter pass phrase for RootCA.key: 輸入CA密碼
```

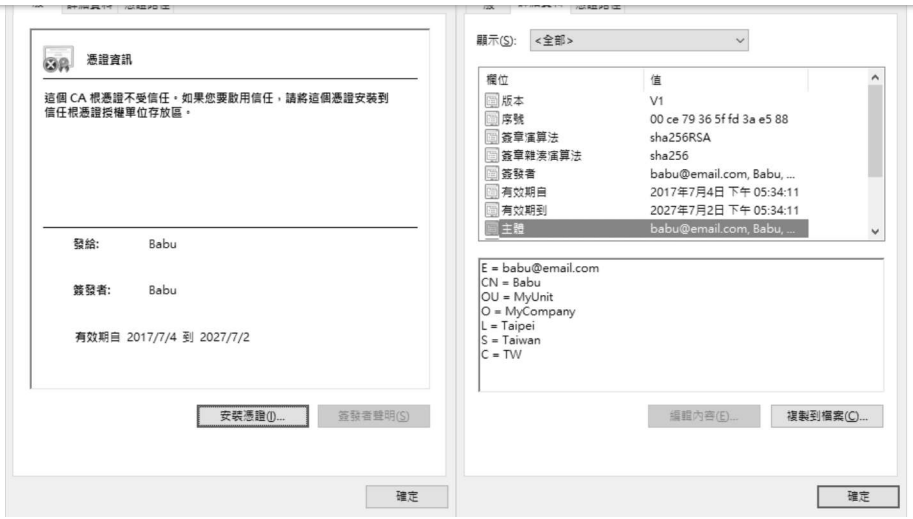
就這樣根憑證完成了，會有三個檔案：

RootCA.key：Private Key 要好好保存，被別人拿到就可以偷聽你的 HTTPS 連線內容，甚至用來簽發未經授權的憑證。

RootCA.crt：Public Key 公開給大家用的，後面簽憑證也會用到。

RootCA.req：申請檔(用不太到了)

crt 內容：



創建伺服器憑證

產生 Private Key

openssl genrsa -out ServerC.key 2048

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe genrsa -out ServerC.key 2048
Generating RSA private key, 2048 bit long modulus
....+++
.....................................+++
e is 65537 (0x010001)
```

不用輸入密碼。

Linux 上鎖權限。

chmod og-rwx ServerC.key

產生申請檔

openssl req -new -key ServerC.key -out ServerC.req

```
E:\cert>c:\OpenSSL-Win32\bin\openssl.exe req -new -key ServerC.key -out Serve
rC.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyUnit
Common Name (e.g. server FQDN or YOUR name) []:babu.com
Email Address []:babu@email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

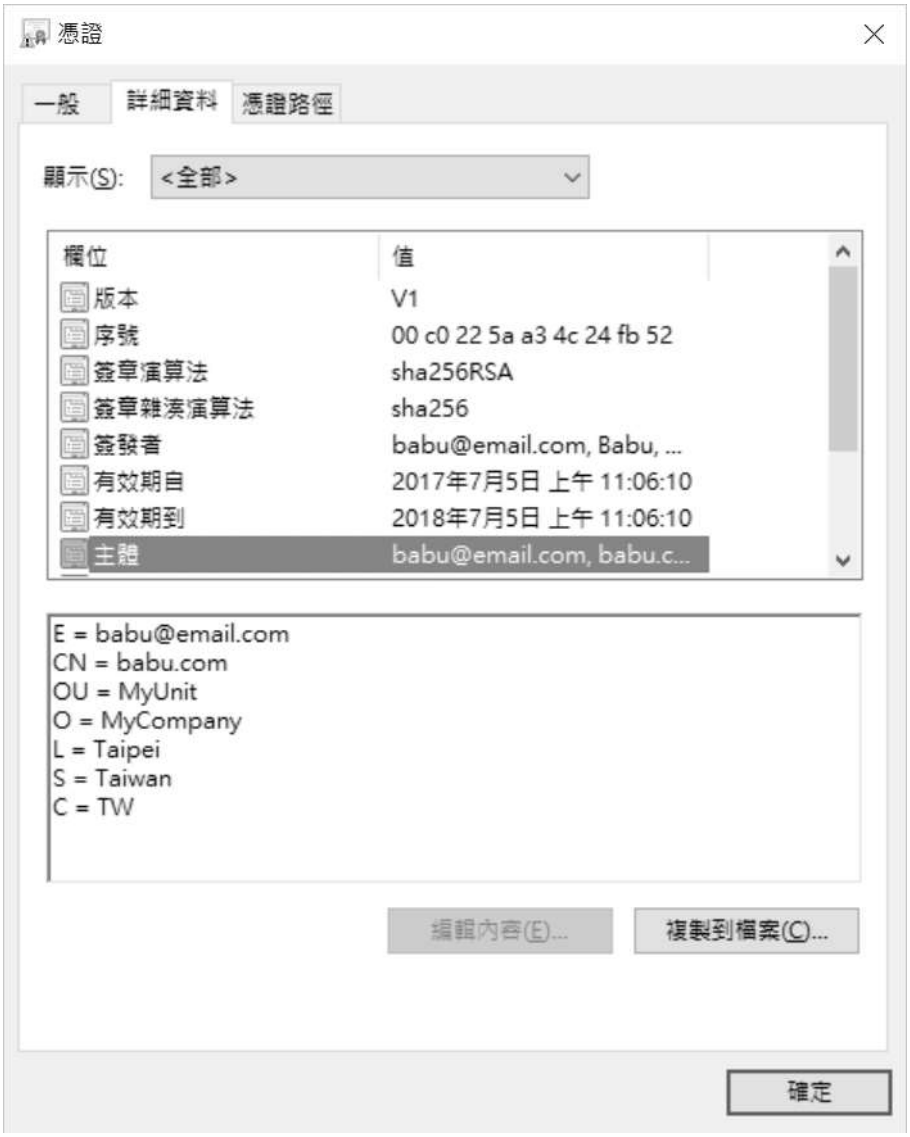
這邊要注意，**Common Name 不能跟上層的一樣**，否則會是有問題的憑證。

openssl x509 -req -days 365 -sha256 -CA RootCA.crt -CAkey RootCA.key -CAserial RootCA.srl -CAcreateserial -in ServerC.req -out ServerC.crt

```
E:\cert>c:\OpenSSL-Win32\bin\openssl.exe x509 -req -days 365 -sha256 -CA Root
CA.crt -CAkey RootCA.key -CAserial RootCA.srl -CAcreateserial -in ServerC.req
 -out ServerC.crt
Signature ok
subject=C = TW, ST = Taiwan, L = Taipei, O = MyCompany, OU = MyUnit, CN = bab
u.com, emailAddress = babu@email.com
Getting CA Private Key
Enter pass phrase for RootCA.key: 輸入CA密碼
```

這樣就完成了，憑證授權的 domain 就是 babu.com，也就是上面輸入的 FQDN 欄位，但是**新版 chrome 檢查方式不同了，建議使用後面的方式產**。

crt 內容：



※ IIS 用的是 pfx 格式，需要另外打包，附錄有。

創建多 Domain 憑證

產生 Private Key

openssl genrsa -out ServerM.key 2048

```
E:\cert>C:\OpenSSL-Win32\bin\openssl.exe genrsa -out ServerM.key 2048
Generating RSA private key, 2048 bit long modulus
.........................................+++
.............+++
e is 65537 (0x010001)
```

不用輸入密碼。

Linux 鎖權限。

chmod og-rwx ServerM.key

產生申請檔

openssl req -new -key ServerM.key -out ServerM.req

```
E:\cert>c:\OpenSSL-Win32\bin\openssl.exe req -new -key ServerM.key -out Serve
rM.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:TW
State or Province Name (full name) [Some-State]:Taiwan
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyUnit
Common Name (e.g. server FQDN or YOUR name) []:babu.net
Email Address []:babu@email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

準備 conf 檔

ServerM.ext.conf

basicConstraints = CA:FALSE
subjectAltName = @alt_names

[alt_names]
DNS.1 = DomainA.com
DNS.2 = DomainB.com
DNS.3 = DomainC.com
IP.4 = 10.1.1.1

因為是 end entity 所以 CA 設為 FALSE，下方自己配置多個 domain、IP，domain 使用 DNS，IP 使用 IP。

對參數有興趣可以參考：https://www.openssl.org/docs/manmaster/man5/x509v3_config.html

產生憑證檔

openssl x509 -req -days 3650 -sha256 -CA RootCA.crt -CAkey RootCA.key -CAserial RootCA.srl -CAcreateserial -in ServerM.req -out ServerM.crt -extfile ServerM.ext.conf

這樣就完成了，憑證授權的 domain 就是 DomainA.com、DomainB.com、DomainC.com，IP 是 10.1.1.1。

crt 內容：

可以發現他是V3版的憑證，下面的 Subject Alternative Name 有三個 domain，一個 IP。

最後在所有要正常驗證憑證的電腦加上最開始產生的 RootCA.crt ，所有由他產出的憑證就通通有效囉！

好處就是以後有新的測試機不用一直在加新憑證囉~

以上內容建議只在自己環境測試用。

其實RootCA通常只用來簽署中繼使用，一般憑證都是用中繼去簽署比較安全，畢竟根憑證外流就...

詳細可以參考：https://jamielinux.com/docs/openssl-certificate-authority/index.html

附錄

PFX 打包

openssl pkcs12 -export -in ServerC.crt -inkey ServerC.key -out ServerC.pfx -certfile RootCA.crt

in：傳入的公開憑證
inkey：傳入的私密憑證
out：打包完的 pfx 檔
certfile：額外包入的憑證檔

到IIS匯入PFX順便輸入密碼即可。

中繼憑證(Intermediate Certification)

解釋參考『憑證串鍊(Certificate chain)是什麼?為何如此重要!』

IIS Server 需要將中繼憑證加到 Intermediate Certification 裡去。(點憑證檔直接加到該分類)

參考網頁

http://slproweb.com/products/Win32OpenSSL.html

http://fannys23.pixnet.net/blog/post/30619452-%5Bwindows%5D-%E9%80%8F%E9%81%8E-openssl-%E7%94%A2%E8%A3%BD%E9%87%91%E9%91%B0%E6%AA%94%E8%88%87%E6%86%91

https://www.sslbuyer.com/index.php?option=com_content&view=article&id=183:what-is-certificate-chain&catid=25&Itemid=4031

https://jamielinux.com/docs/openssl-certificate-authority/index.html

https://gist.github.com/Soarez/9688998

https://www.ssl.com/how-to/create-a-pfx-p12-certificate-file-using-openssl/

https://www.openssl.org/docs/manmaster/man5/x509v3_config.html

相關創作

【2022/01/09】台灣地區聯盟賽台北站十六強戰報

【生活日記】2022/01/16拜日、北車NOTCH咖啡工場披薩網羅

[黏土]委託作品 小紅帽 & 小紅帽

【人文專欄】宋明理學的創始人──周敦頤

【翻譯】山田和鮫魚

留言

共 0 篇留言

我要留言

提醒：您尚未登入，請先登入再留言

留言請注意禮節與尊重他人，良好的交流環境需要你我共同維護。

★babu61509 可決定是否刪除您的留言，請勿發表違反站規文字。 喜歡 送出

前一篇：SONY 10 RBT ... 回創作列表 回頂端 後一篇：ProRender fo...