

HP / April 08, 2010 09:59PM

[建立HTTPS \(SSL\) 網站的方法：1. 簽發憑證\(CA\)、2. 修改 httpd.conf 設定](#)

1. 自我簽發憑證

此法相對於付費的憑證(由Versign、Thawte等授權機構簽發，台灣代理商一年大約二、三萬台幣)，沒有經過公正第三方的認證，不過如果是給「自己人」或者是一般「相信你的網站」的網友，基本上是夠用的。不過「自我簽發憑證」的HTTPS網站，在進入時候，瀏覽器基本上都會有：「您即將進入非安全性的網站，您確定嗎？」之類的提示。點選「是」或「我要進入」就可了。

1a 找到 Apache 內建的憑證產生器：certificate.sh。

一般而言，路徑是在：`cd /usr/share/doc/packages/apache2/`

先修改裡面的最後一個字 test，改為 custom。修改後內容為：

```
#!/bin/sh
```

```
./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom
```

1b 執行憑證產生器：Shell> `./certificate.sh`

執行後會開始一連串（九個步驟）的互動產生模式。以下簡要提示需要輸入的資訊。

STEP 0：Signature Algorithm 選「R」或直接按 Enter。(RSA加密支持度比較高)

STEP 1：產生 Private Key (ca.key)。不需輸入資訊。

STEP 2：建立憑證簽發請求 (ca.csr)。需輸入以下資訊：

Country Name: TW

State or Province Name: Taiwan (或「.」)

Locality Name: Taipei

Organization Name: 填入您所屬的組織，例如 National Taiwan Univerisy

Organization Unit Name: 填入您在組織中所屬的單位，例如 Department of Eletronic Engineering

Common Name: 可以輸入您的組織名稱或網站名稱，例如 www.yoursite.com

Email Address: 簽發憑證擁有人的電子郵件（在這裡是我們自己）

STEP 3：選擇X.509憑證 (ca.crt) 的版本，預設值是第三版。此處按 Enter 即可。

STEP 4：對HTTP伺服器產生 RSA Private Key (server.key)。不需輸入資訊。

STEP 5：對HTTP伺服器建立X.509憑證簽發請求 (server.csr)。需輸入的資訊和 STEP 2 相似，除了 Common Name 的地方注意要輸入網站URL，例如 www.yoursite.com。

STEP 6：選擇對 Server 的 X.509憑證 (server.crt) 的版本，預設值是第三版。此處按 Enter 即可。

STEP 7：選擇是否對 CA憑證的 Private Key 加密。如果選擇加密需設定密碼。住後開啟或重啟 Apache Server 皆需輸入此密碼。

STEP 8：選擇是否對 Server憑證的 Private Key 加密。與上步相同，如果選擇加密需設定密碼。住後開啟或重啟 Apache Server 皆需輸入此密碼。

經過此九個步驟，憑證的產生就大功告成了。另需注意，此 Script (certificate.sh) 產生的憑證有效期限為一年，過了一年後需重新簽發。

2. 修改 Apache Server 相關設定

底下這個類似 Tutorial 的文章寫得非常好，尤其是用 SUSE 的朋友特別適合(其他的版本大致上只是路徑不同)：

http://jamesrome.home.comcast.net/~jamesrome/Apache/SSL_in_Apache_2.html

(寫得有點累了，先放這篇文章作為設定的介紹)

如果有什麼問題，歡迎提問啊！

另外，如果要將 HTTPS 網站提升安全性，提升為 Strong Encryption 的網站(SSLv2-only、strong encryption only等網站設定)，

請參見寫得很詳細、清楚的官方網頁：

[SSL/TLS Strong Encryption: How-To](#) (Apache 2.2 Documentation)

Edited 4 time(s). Last edit at 04/30/2010 11:46PM by HP.
