中華電信通用憑證管理中心(PublicCA)

Lighttpd 伺服器 SSL 伺服軟體憑證安裝說明

本說明書適用於 Lighttpd +mod_ssl 環境下之 SSL 伺服器軟體憑證安裝，並假設 Lighttpd Server 係執行於 Unix like 的平台上(例如:Linux)。本說明書的安裝程序，已經在 lighttpd-1.4.35 及 mod_ssl 2.8.18 版測試過，您所使用的版本或環境可能與本版本有所差異，若是如此則請參考您的 Web Server 及 SSL 模組相關使用手冊，適度調整 SSL 伺服軟體憑證安裝步驟。
以下為 Lighttpd+mod_ssl 環境下之 SSL 伺服軟體憑證安裝程序，整個安裝程序包含 4 個部份：

一、 產製 eCA自簽憑證及Public CA憑證之憑證串鏈
二、 產製沒有加密過的server key
三、 產製包含Key和SSL 伺服軟體憑證的PEM檔案
四、 在Lighttpd Server設定SSL
五、 重啟Lighttpd Server

一、產製 eCA 自簽憑證及 Public CA 憑證之憑證串鏈

當您向 Public CA 申請的 SSL 伺服軟體憑證經審核通過並簽發之後，您可先不用急著設定所申請的 SSL 伺服軟體憑證,而必須先取得 eCA 自簽憑證、Public CA 憑證，並製作出 eCA 自簽憑證及 Public CA 憑證之憑證串鏈，且在 Lighttpd Server 上設定此憑證串鏈。

1. 下載憑證串鏈
   包含 3 張憑證，分別是
   (1)eCA 根憑證
   - ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證

   (2)PublicCA 中繼憑證
   - 中華電信通用憑證管理中心自身憑證

   (3)PublicCA 簽發給用戶的 SSL 伺服器憑證(在三、產製包含 Key 和

SSL 伺服軟體憑證的 PEM 檔案會用到）

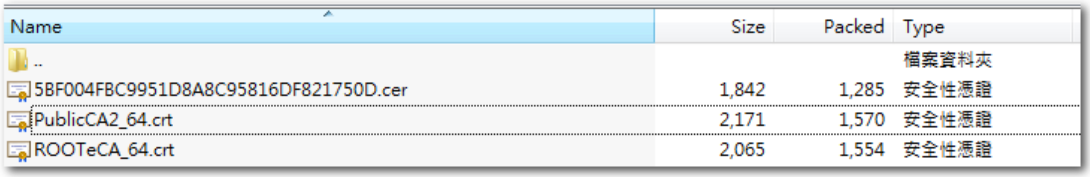
可採以下兩種方式之一取得:

- 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(若為 SHA1 憑證串鏈，檔名為 PublicCA_64.crt；若為 SHA256 憑證串鏈，檔名為 PublicCA2_64.crt)與 用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。
  若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單 「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證 串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。
- 從網站查詢與下載：
  - eCA 憑證
    - http://eca.hinet.net/download/ROOTeCA_64.crt
  - PublicCA憑證
    - http://publicca.hinet.net/CHTM/download/PublicCA_64.crt
  - PublicCA G2憑證
    - http://publicca.hinet.net/CHTM/download/PublicCA2_64.crt
  - SSL 憑證下載
    - 您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，進行 SSL 憑證下載。

      註：PublicCA 網站 http://publicca.hinet.net/
    - 若您是中華電信之員工，負責管理單位之伺服器，請至 http://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證(請選擇 Based 64 格式)。
      (註：使用 IE 下載.crt 格式的憑證時，IE 會將副檔名.crt 改為.cer， 但編碼格式還是屬於 Base64)

2. 登入 Lighttpd Server 機器（註：您登入的帳號必須具有 root 或 Lighttpd 管理員的權限）
3. 以下範例，以 SHA1 安裝為安裝範例
   上傳上述 3 個憑證檔案至 Lighttpd Server（可選擇上傳至 home 資料夾）
   - eCA 根憑證
     - ROOTeCA_64.crt
   - PublicCA 中繼憑證
     - PublicCA_64.crt
   - 用戶的 SSL 伺服器憑證

- ***xxxxxx…(32 個英數字)***.cer -> 為您的 SSL 憑證檔名，會與範例不一樣



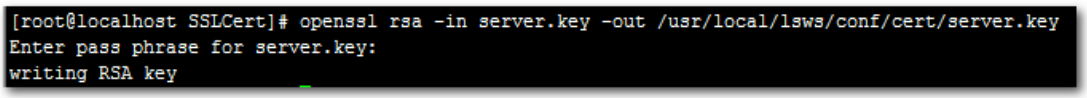
Name	Size	Packed	Type
..			檔案資料夾
5BF004FBC9951D8A8C95816DF821750D.cer	1,842	1,285	安全性憑證
PublicCA2_64.crt	2,171	1,570	安全性憑證
ROOTeCA_64.crt	2,065	1,554	安全性憑證

4. 產製 CA 憑證串列並複製 CA 憑證串列至 Lighttpd 目錄下
（註：以下%符號表示 Shell 的 prompt，不是命令的一部分）
% cat PublicCA_64.crt ROOTeCA_64.crt >
/etc/lighttpd/caChain.crt

（/etc/lighttpd 為 Lighttpd Server 的目錄，若您的 Lighttpd Server 不在此位置，請自行更改）

二、產製沒有加密過的 server key

因為 Lighttpd 規定只能放沒有加密過的 server key
(註:
http://redmine.lighttpd.net/projects/lighttpd/wiki/Docs_SSL#SSL-passwords)，所以我們需要將先前拿來產製 CSR 的 server.key，移除其密碼加密，並且將 output 指定在 Lighttpd server 資料夾下面:
% openssl rsa -in server.key -out server_no_pwd.key



```
[root@localhost SSLCert]# openssl rsa -in server.key -out /usr/local/lsws/conf/cert/server.key
Enter pass phrase for server.key:
writing RSA key
```

三、產製包含 Key 和 SSL 伺服軟體憑證的 PEM 檔案

產製包含 Key 和 SSL 伺服軟體憑證的 PEM 檔案並指定 output 至 Lighttpd 目錄下:
% cat server_no_pwd.key ***xxxxxx…(32 個英數字)***.cer >
/etc/lighttpd/server.pem
註1. ***xxxxxx…(32 個英數字)***.cer（為您的 SSL 憑證檔名，會與範例不一樣）
註2. /etc/lighttpd 為 Lighttpd Server 的目錄，若您的 Lighttpd Server 不在此位置，請自行更改

四、在 Lighttpd Server 設定 SSL

% vi /etc/lighttpd/lighttpd.conf

```
$SERVER["socket"] == "Lighttpd-Server-IP:443" {
ssl.engine = "enable"
ssl.pemfile = "/etc/lighttpd/server.pem"
ssl.ca-file ="/etc/lighttpd/caChain.crt"
server.name = "www.example.com"
server.document-root = "/srv/www/vhosts/example.com/www/"
}
```

註: ***Lighttpd-Server-IP*** 是您的 Lighttpd Server IP

五、重啟 Lighttpd Server

```
% service lighttpd restart
```

附件一.　更換 SHA256 憑證

- 適用於申請時，有同時取得 SHA1、SHA256 憑證，或是憑證在效期內，經由審驗人員再次核發 SHA256 憑證者
- 有關國際間漸進淘汰SHA1 憑證轉移至SHA256 憑證細節，請參與本管理中心網站之問與答之金鑰長度與演算法 (https://publicca.hinet.net/SSL-08-06.htm)
- 安裝步驟
  - 產製 CA 憑證串列並複製 CA 憑證串列至 Lighttpd 目錄下
  - 產製包含 Key 和 SSL 伺服軟體憑證的 PEM 檔案
    - 產製包含 Key 和 SSL 伺服軟體憑證的 PEM 檔案並指定 output 至 Lighttpd 目錄下:
    - % cat server_no_pwd.key ***xxxxxx…(32 個英數字)***.cer > /etc/lighttpd/server.pem
  - 重啟 Lighttpd Server
    - service lighttpd restart