# 中華電信通用憑證管理中心(PublicCA)

# Nginx HTTP Server 伺服器 SSL 伺服軟體憑證安裝手冊



本手冊適用於 Nginx 環境下之 SSL 伺服器軟體憑證安裝，並假設 Nginx HTTP Server 係執行於 Linux。本手冊的安裝程序，已經在 Nginx-1.7.X 版本以上測試過，您所使用的版本或環境可能與 Nginx-1.7.X 版本以上有所差異，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。Nginx Server 官方網站參考 http://nginx.org/

以下為 Nginx 環境下之 SSL 伺服軟體憑證安裝程序，整個安裝程序包含 6 個部份，以 eCA (RootCA)與 Public CA(中繼 CA)的憑證串鏈為主：

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 Nginx Server 設定 SSL
五、 重啟 Nginx Server
六、 安裝 SSL 安全認證標章

## 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 Nginx HTTP 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，亦即 Public CA 之 CA 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(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 「IS14-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://epki.com.tw/download/ROOTeCA_64.crt
  - PublicCA G2憑證
    - http://epki.com.tw/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 Base 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 Base 64)

2. 登入 Nginx HTTP Server 機器 (註:您登入的帳號必須具有 root 管理員的權限)
3. 上傳上述 3 個憑證檔案至 Nginx HTTP Server (此說明環境是上傳至 /export/nginx-1.7.4/conf/Certs 資料夾)
   - eCA 根憑證
     - ROOTeCA_64.crt
   - PublicCA G2 中繼憑證
     - PublicCA2_64.crt
   - 用戶的 SSL 伺服器憑證
     - ***xxxxxx…(32 個英數字)***.cer (***xxxxxx…***.cer -> 為您的 SSL 憑證檔名,會與範例不一樣)
4. 產製可信任的 CA 憑證串列至/export/nginx-1.7.4/conf/Certs 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 >
/export/nginx-1.7.4/conf/Certs/caChain.crt
(/export/nginx-1.7.4/為 Nginx HTTP Server 的目錄，若您的 nginx Server 不在此位置，請自行更改)

## 二、產製沒有加密過的 server key

因為 Nginx HTTP Server 規定只能放沒有加密過的 server key，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 Nginx HTTP server 資料夾下面:

% openssl rsa -in server.key -out server_no_pwd.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 Nginx HTTP server 目錄下:

% cat server_no_pwd.key > /export/nginx-1.7.4/conf/Certs/server.key

% cat ***xxxxxx…***.cer PublicCA2_64.crt >
/export/nginx-1.7.4/conf/Certs/server.pem

註1. ***xxxxxx…***.cer (***xxxxxx…***.cer -> 為您的 SSL 憑證檔名(32 個英數字)，會與範例不一樣)

註2. /export/nginx-1.7.4/conf/Certs/為 Nginx HTTP Server 的憑證放置目錄，若您的 Nginx HTTP Server 不在此位置，請自行更改

## 四、在 Nginx HTTP Server 設定 SSL

% vi /export/nginx-1.7.4/conf/nginx.conf

```
# HTTPS server
server {
    listen          443 ssl;
    server_name     Nginx-Server-IP;
    ssl_certificate             /export/nginx-1.7.4/conf/Certs/Server.pem;
    ssl_certificate_key         /export/nginx-1.7.4/conf/Certs/Server.key;
    #SSL 網站服務主目錄
    root     /export/www/htdocsSSL/;
    index    index.html index.htm index.php;

    ssl_stapling on;
    ssl_stapling_verify on;
    ssl_trusted_certificate /export/nginx-1.7.4/conf/Certs/caChain.crt;

     #       ssl_session_cache       shared:SSL:1m;
     #       ssl_session_timeout     5m;
     #       ssl_ciphers     HIGH:!aNULL:!MD5;
     #       ssl_prefer_server_ciphers     on;
     #       location / {
     #            root     html;
     #            index    index.html index.htm;
     #       }
     }
```

註: ***Nginx-Server-IP*** 是您的 Nginx HTTP Server IP 或者 HostName

新增與修改 Nginx Configure 檔案，關閉有安全漏洞的 HTTPS SSLv3 協定，改採用 HTTPS TLS 通道之設定方法:

```
http {
      include           mime.types;
      default_type    application/octet-stream;

      #強制 HTTPS 服務採用 TLS 安全協定來運作
      ssl_protocols    TLSv1 TLSv1.1 TLSv1.2;
}
```

## 五、重啟 Nginx HTTP Server

nginx 啟動、停止、重啟命令

- nginx 啟動

root User 執行/export/nginx-1.7.4/sbin/nginx
(Nginx 執行主路徑，請根據自己安裝路徑實際決定)

- nginx 從容停止命令，等所有請求結束後關閉服務

ps -ef |grep nginx ➔取得{nginx 執行程序之編號}
kill -QUIT {nginx 執行程序之編號}

- nginx 快速停止命令，立刻關閉 nginx 進程

ps -ef |grep nginx ➔{nginx 執行程序之編號}
kill -TERM {nginx 執行程序之編號}

- 如果以上命令不管用，可以強制停止

kill -9 {nginx 執行程序之編號}

## 六、 安裝 SSL 安全認證標章：

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。您也可參考 http://publicca.hinet.net/SSL-01.htm 下方有 SSL 安全認證標章之安裝說明。

請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

# 附件一. 更換SHA 256憑證

- 適用於申請時，有同時取得SHA-1、SHA 256憑證，或是憑證在效期內，經由審驗人員再次核發SHA 256憑證者
- 有關國際間漸進淘汰SHA-1憑證轉移至SHA 256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憑證串鏈並複製CA憑證串列至nginx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nginx目錄下:
    - ◆ % cat server_no_pwd.key xxxxxx…(32 個英數字).cer > /export/nginx-1.7.4/conf/Certs/server.pem
  - 重啟nginx Server