中華電信通用憑證管理中心(PublicCA)

Lighttpd 伺服器憑證請求檔製作手冊

一、產生憑證請求檔

(1) 產生憑證請求檔（Certificate Signing Request file，簡稱 CSR 檔）
需使用 openssl 工具，此工具通常安裝在 /usr/local/ssl/bin 目錄下(可以使用 $ find / -name openssl -print 指令找到您安裝的目錄，請確定您已經安裝成功再執行下列指令。)

(2) 開始前，請確認您 OpenSSL 的版本沒有受到 Heartbleed Bug 的影響，您可輸入以下指令來確認您 OpenSSL 的版本。若您的版本有 Heartbleed Bug，建議先升級到修復版本，再執行以下操作。
$ openssl version
影響範圍：1.0.1 ~ 1.0.1f / 1.0.2-beta ~ 1.0.2-beta1
修復版本：1.0.1g / 1.0.2-beta2

(3) 產生以 3-DES 加密，PEM 格式的私密金鑰(長度需為 RSA 2048 位元)
執行 openssl 程式如下：
$ openssl genrsa -des3 -out server.key 2048

- 若您的 SSL 憑證即將到期，需更新憑證，建議可以另開一個新的資料夾，並在此資料夾下執行上述指令，以避免線上使用的 server.key 被覆蓋。
- 依照國際密碼學規範，請使用 RSA 2048 位元(含)以上金鑰長度。

(4) 執行完畢後會產生私密金鑰檔案，檔名為 server.key，請您將此檔案備份，執行過程會要求您輸入密碼(pass phrase)
Enter PEM pass phase:
一定要牢記此密碼，日後每次啟動 SSL 通訊模式時均會用到。

```
[root@Franklin bin]# openssl
OpenSSL> exit
[root@Franklin bin]# openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++++
.....................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[root@Franklin bin]# _
```

(5) 產生憑證請求檔

$ openssl req -new -key server.key -out certreq.txt

執行過程會要求輸入密碼，完畢後會產生憑證請求檔，檔名為 certreq.txt

請輸入憑證主體資訊放入憑證申請求檔中，不過 PublicCA 網站 SSL 憑證申請頁面只會擷取憑證請求檔的公開金鑰數值，並不會使用以下憑證主體資訊，而是以您在 PublicA 網頁投單所登打之組織與網站名稱資訊為準進行身分審驗。

Country Name：TW

State or Province Name：

Locality Name：城市(如：Taipei)

Organization Name：組織名稱(如：CHT)

Organizational Unit Name：單位名稱(如:Information)

Common name：網站名稱(如：www.abc.com.tw)

Email address：伺服器管理者電子郵件 (如:abc@abc.com.tw)

challenge password：不需輸入，按 enter 鍵略過

optional company name：不需輸入，按 enter 鍵略過

```
[root@Franklin bin]# openssl req -new -key server.key -out certreq.txt
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporate
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
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) [GB]:TW
State or Province Name (full name) [Berkshire]:Taiwan
Locality Name (eg, city) [Newbury]:Taipei
Organization Name (eg, company) [My Company Ltd]:CHT
Organizational Unit Name (eg, section) []:Information
Common Name (eg, your name or your server's hostname) []:www.abc.com.tw
```

```
Email Address []:test@test.com.tw

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

(6) 檢視憑證請求檔

您可使用下面指令檢視您所產生的憑證請求檔

$openssl req -noout -text -in certreq.txt

請求檔內容範例如下:

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=TW, L=Taipei, O=CHT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c5:c9:4b:1b:c3:7f:30:65:4c:2b:52:3c:22:9a:
                    ef:68:97:9b:9e:64:03:f5:7a:9c:ee:b9:1c:0b:a8:
                    51:8b:8b:20:81:68:2d:45:de:d5:36:f3:98:bb:ed:
                    a4:6f:cc:a3:44:97:b6:a3:18:e3:08:07:67:6d:97:
                    82:52:89:8c:1c:1a:9b:c5:0c:de:32:36:37:ee:e1:
                    b1:e1:05:7c:c8:e9:e5:8e:39:3a:9d:16:e2:b6:0f:
                    86:21:46:20:80:9a:b3:a3:82:c6:85:6b:87:00:74:
                    d9:f0:76:9a:36:6f:a8:d4:23:7f:bf:a9:e5:6c:d4:
                    77:10:f7:84:f9:12:92:1b:5f:80:6a:a9:7e:dd:32:
                    30:cf:4c:e0:32:a3:62:e9:ab:94:8e:82:37:84:42:
                    bb:17:24:90:42:2f:9c:0c:dc:a7:57:74:1e:6c:9c:
                    22:cd:61:1d:23:ff:e1:ab:66:2c:6b:b7:83:ec:d8:
                    4e:de:c5:a0:c6:a3:a2:d9:5f:6f:a4:47:dc:de:e6:
                    a9:9b:c6:35:b4:87:17:58:18:28:0a:ae:87:1b:d9:
                    ba:9a:86:73:c4:c2:59:2e:97:50:c4:5a:75:a5:18:
                    43:ef:36:9a:b1:82:b9:1f:ed:f8:51:53:9e:55:0c:
                    dd:92:c4:a2:84:8a:4d:59:8b:1c:66:e2:62:bd:02:
                    04:9b
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        ad:03:70:a8:eb:2b:09:8b:84:3f:c3:73:7d:93:c2:e1:58:06:
        7f:65:e5:73:9e:ab:fb:bc:ae:46:50:e4:1f:de:4c:06:13:27:
        41:04:ab:c0:1e:f7:f1:58:d4:42:de:5f:d2:7d:f6:d8:da:16:
        fe:45:b5:48:22:60:4a:58:3b:78:54:74:39:ac:93:3e:dc:08:
        b5:2a:8f:62:c3:30:f1:e3:4d:4a:1f:3f:cd:7b:7b:a4:e8:45:
        f8:f1:ff:9f:8e:a1:dd:fa:97:df:83:a5:e7:af:0b:11:80:dd:
        b4:ed:00:d4:8a:5e:17:39:c4:82:59:b6:3e:6b:83:f5:dd:e3:
        28:a9:61:dc:e6:8d:bc:8c:ee:63:68:3e:13:65:40:a5:43:b9:
        d0:e1:a7:6b:7c:c4:8e:92:fd:d5:1c:79:59:29:25:50:c5:1b:
        af:bf:c7:56:b8:d4:68:fb:9b:5b:e7:dc:b2:f8:5d:ea:55:8f:
        c7:4c:9c:75:66:84:1f:f4:f3:c8:6f:12:31:9d:67:22:4a:23:
        03:d0:d0:aa:18:ef:6d:2c:37:49:dc:1e:a9:33:f3:9e:aa:2e:
        45:98:08:12:de:1e:a1:59:3e:0f:88:e2:91:7c:a6:41:37:cb:
        90:ab:5e:a8:4e:56:cd:4c:67:f5:1d:74:84:3b:db:0c:c8:f6:
        89:29:bb:d3
```

二、將憑證請求檔存到儲存媒體，完成製作憑證請求檔動作。

三、請將產生的憑證請求檔(certreq.txt) 複製至中華電信通用憑證管理中心網站 （http://publicca.hinet.net/）依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。