

# 中華電信通用憑證管理中心

## 伺服器軟體憑證 Apache 伺服器產生憑證請求檔說明

### 1、產生憑證請求檔

產生憑證請求檔需使用 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

- (1) 產生以 3-DES 加密，PEM 格式的私密金鑰(長度需為 1024 位元)

執行 openssl 程式如下：

```
$ openssl genrsa -des3 -out server.key 1024
```

- (2) 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 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[root@Franklin bin]# _
```

- (3) 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

您必須輸入以下資訊放入憑證申請檔中

Country Name : TW

State or Province Name : Taiwan

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 incorporated
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 []:
```

#### (4) 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:

```
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
 00:d3:90:b8:45:f5:64:89:15:0a:a4:d9:3d:fc:94:
 80:71:16:1d:e8:20:44:ab:fc:88:7e:59:fe:5c:9d:
 36:d2:df:4b:34:5b:1d:a9:e8:c9:fd:88:aa:3f:75:
 df:4a:e1:4a:f2:44:cf:e4:17:54:84:34:78:10:f8:
 22:45:e7:69:34:12:d1:66:19:48:c6:5c:3c:84:1d:
 f2:0c:9f:93:9a:c1:ef:3b:f8:7e:08:f7:de:cc:9a:
 d4:b6:bb:85:f6:d9:22:90:58:35:a6:29:3e:a2:e9:
 8d:f2:79:7d:82:08:87:77:f0:2c:f3:cb:b3:77:4d:
 81:33:6e:00:c7:1e:ad:99:d7
Exponent: 65537 (0x10001)
Attributes:
 a0:00
Signature Algorithm: md5WithRSAEncryption
9d:51:a7:cf:3b:6d:e4:b9:ad:41:1c:0c:56:16:ce:7e:85:82:
 eb:ad:7d:80:c9:ac:2b:f1:c7:df:3d:dc:15:59:f7:90:05:b5:
 64:95:e0:0c:57:5b:6d:fb:d2:2a:02:36:ce:a4:ce:77:76:67:
 81:d0:2c:a3:a9:08:aa:28:59:9a:c3:ed:80:b3:62:93:54:47:
 11:66:60:00:ee:5c:1b:65:57:28:7b:5f:00:c2:fe:df:5d:8e:
 cb:9d:87:8e:7c:1f:f2:23:07:47:6c:d1:e5:40:5b:9d:4d:59:
 b7:f9:37:5a:77:71:ee:95:0f:a6:85:5e:90:d9:23:b8:1a:e6:
 a8:a4
```

3.將憑證請求檔存到儲存媒體，連線至申請 Public CA 網站申請伺服器應用軟體憑證(SSL 類)。