API 技術客服
使用 Openssl 製作憑證請求檔手冊

目錄

使用 Openssl 製作憑證請求檔手冊

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 以後

(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。

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。

```
[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]# _
```

(4) 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到憑證請求檔中，不過經濟部工商憑證管理中心網站非 IC 卡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。

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
```

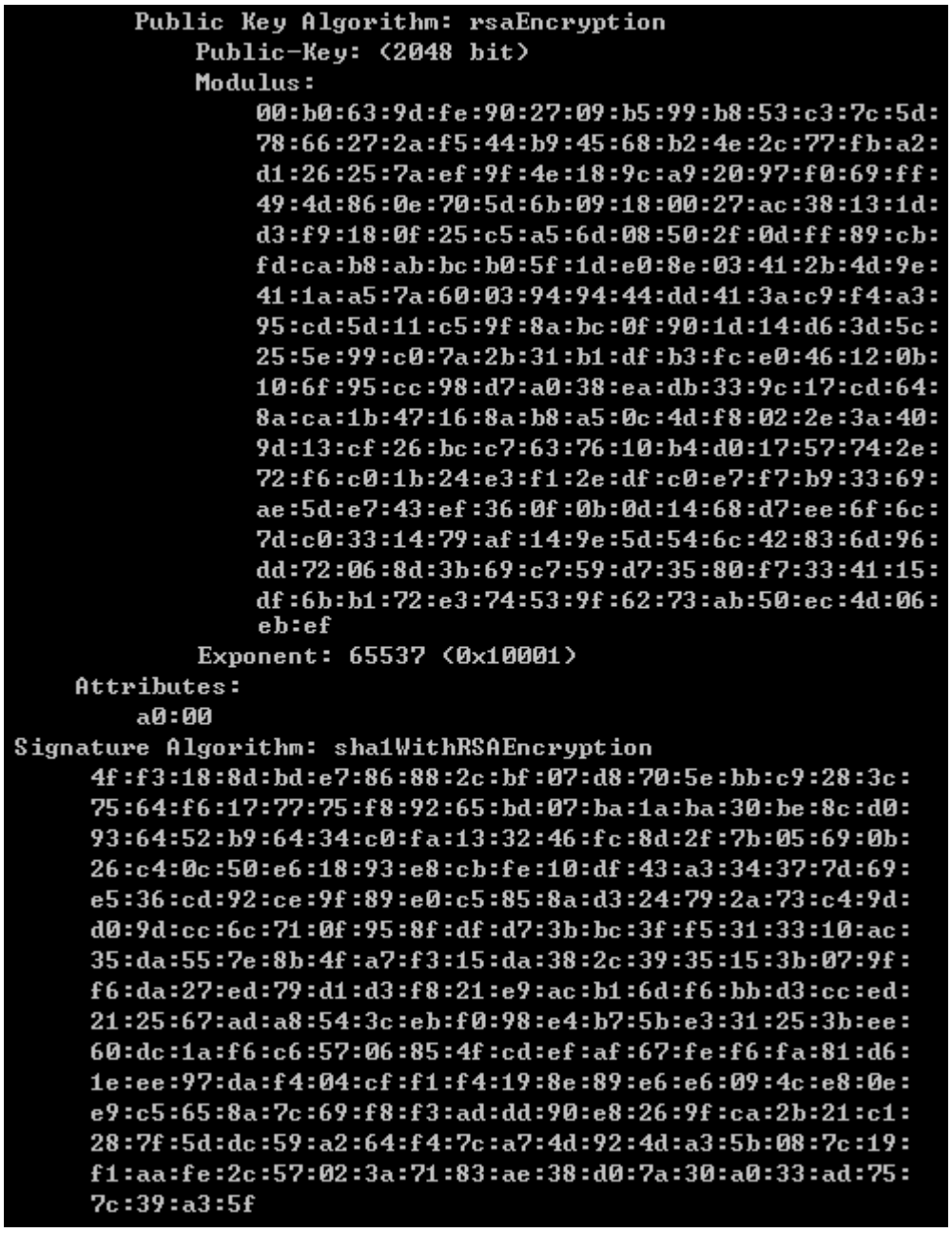
```
Email Address []:test@test.com.tw

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

(5) 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:



二、將憑證請求檔存到儲存媒體，完成製作憑證請求檔動作。

請將產生的憑證請求檔(certreq.txt) 複製並妥善保管，至經濟部工商憑證管理中心（http://moeaca.nat.gov.tw/nonic.html）依照網頁說明申請非 IC 卡類憑證。