

政府憑證管理中心(GCA) Apache SSL憑證請求檔製作與憑證安裝手冊

聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請政府憑證管理中心（GCA）之 SSL 伺服器軟體憑證用戶參考，若因參考本手冊所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

本手冊適用於 Apache Server 環境下之 SSL 伺服器軟體憑證安裝
本手冊的安裝程序，已經在 Apache_2.2.29 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 伺服器軟體憑證安裝步驟。

目錄

Linux Apache SSL 憑證請求檔製作手冊	2
Linux Apache SSL 憑證安裝操作手冊	5
Windows Apache SSL 憑證請求檔製作手冊	8
Windows Apache SSL 憑證安裝操作手冊	12
附件一：設定 SSL 安全通道的加密強度.....	17
附件二：停用 SSLv3.0.....	18

Linux Apache SSL 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 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 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 TLS 通訊模式時, 皆會用到。

```
[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) 再次提醒您請將 server.key 檔案進行備份。若是在提出憑證申請後私密金鑰遺失, 核發下來的憑證將會無法使用, 需要重新提出申請與廢止憑證。
- (6) 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 GCA 網站 SSL 憑證申請頁

面只會擷取憑證請求檔中的公開金鑰數值，並不會使用以下憑證主體資訊，而是以您在 GCA 網站填寫之申請書內容進行身分審驗。

Country Name : TW

State or Province Name : 不需輸入，按 enter 鍵略過

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，多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主)

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]:
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 []:
```

(7) 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
Public-Key: (2048 bit)
Modulus:
 00:b0:63:9d:fe:90:27:09:b5:99:b8:53:c3:7c:5d:
 78:66:27:2a:f5:44:b9:45:68:b2:4e:2c:77:fb:a2:
 d1:26:25:7a:ef:9f:4e:18:9c:a9:20:97:f0:69:ff:
 49:4d:86:0e:70:5d:6b:09:18:00:27:ac:38:13:1d:
 d3:f9:18:0f:25:c5:a5:6d:08:50:2f:0d:ff:89:cb:
 fd:ca:b8:ab:bc:b0:5f:1d:e0:8e:03:41:2b:4d:9e:
 41:1a:a5:7a:60:03:94:94:44:dd:41:3a:c9:f4:a3:
 95:cd:5d:11:c5:9f:8a:bc:0f:90:1d:14:d6:3d:5c:
 25:5e:99:c0:7a:2b:31:b1:df:b3:fc:e0:46:12:0b:
 10:6f:95:cc:98:d7:a0:38:ea:db:33:9c:17:cd:64:
 8a:ca:1b:47:16:8a:b8:a5:0c:4d:f8:02:2e:3a:40:
 9d:13:cf:26:bc:c7:63:76:10:b4:d0:17:57:74:2e:
 72:f6:c0:1b:24:e3:f1:2e:df:c0:e7:f7:b9:33:69:
 ae:5d:e7:43:ef:36:0f:0b:0d:14:68:d7:ee:6f:6c:
 7d:c0:33:14:79:af:14:9e:5d:54:6c:42:83:6d:96:
 dd:72:06:8d:3b:69:c7:59:d7:35:80:f7:33:41:15:
 df:6b:b1:72:e3:74:53:9f:62:73:ab:50:ec:4d:06:
 eb:ef
Exponent: 65537 (0x10001)
Attributes:
  a0:00
Signature Algorithm: sha1WithRSAEncryption
 4f:f3:18:8d:bd:e7:86:88:2c:bf:07:d8:70:5e:bb:c9:28:3c:
 75:64:f6:17:77:75:f8:92:65:bd:07:ba:1a:ba:30:be:8c:d0:
 93:64:52:b9:64:34:c0:fa:13:32:46:fc:8d:2f:7b:05:69:0b:
 26:c4:0c:50:e6:18:93:e8:cb:fe:10:df:43:a3:34:37:7d:69:
 e5:36:cd:92:ce:9f:89:e0:c5:85:8a:d3:24:79:2a:73:c4:9d:
 d0:9d:cc:6c:71:0f:95:8f:df:d7:3b:bc:3f:f5:31:33:10:ac:
 35:da:55:7e:8b:4f:a7:f3:15:da:38:2c:39:35:15:3b:07:9f:
 f6:da:27:ed:79:d1:d3:f8:21:e9:ac:b1:6d:f6:bb:d3:cc:ed:
 21:25:67:ad:a8:54:3c:eb:f0:98:e4:b7:5b:e3:31:25:3b:ee:
 60:dc:1a:f6:c6:57:06:85:4f:cd:ef:af:67:fe:f6:fa:81:d6:
 1e:ee:97:da:f4:04:cf:f1:f4:19:8e:89:e6:e6:09:4c:e8:0e:
 e9:c5:65:8a:7c:69:f8:f3:ad:dd:90:e8:26:9f:ca:2b:21:c1:
 28:7f:5d:dc:59:a2:64:f4:7c:a7:4d:92:4d:a3:5b:08:7c:19:
 f1:aa:fe:2c:57:02:3a:71:83:ae:38:d0:7a:30:a0:33:ad:75:
 7c:39:a3:5f
```

二、將憑證請求檔存放到方便存取的目錄，完成製作憑證請求檔動作。

三、請至 GCA 網站(<http://gca.nat.gov.tw>)進行 SSL 憑證申請作業。

Linux Apache SSL 憑證安裝操作手冊

一、取得 GRCA 及 GCA 之憑證串鏈

當您向 GCA 申請的 SSL 伺服器軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服器軟體憑證，而必須先取得 GRCA 及 GCA 之憑證串鏈，並在 Apache Server 上安裝 GRCA 及 GCA 之憑證串鏈，這樣您接下來安裝的 SSL 伺服器軟體憑證才會正常運作。如果您以前曾經在同一部 Apache Server 上成功安裝過 GRCA 及 GCA 之憑證串鏈，則您可以跳過步驟一和二，直接進行 SSL 伺服器應用軟體憑證的安裝。

- (1) 請至GCA網站下載已經製作好的憑證串鏈檔案，格式為PEM編碼，下載網址為http://gca.nat.gov.tw/download/GRCA1_5_GCA2.zip
- (2) 將下載的GRCA1_5_GCA2.zip解壓縮得到GRCA1_5_GCA2.crt

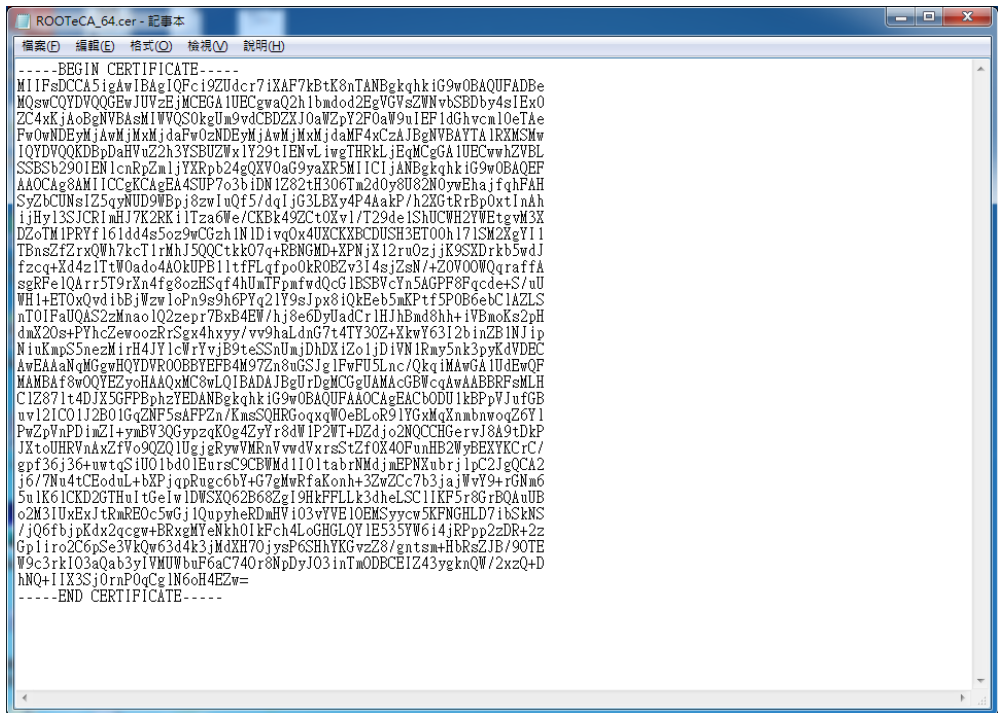
二、安裝 GRCA 及 GCA 之憑證串鏈與 SSL 憑證

- (1) 請確定已下載簽發之 SSL 伺服器軟體憑證(*.cer)。
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。
- (2) 執行以下命令將SSL伺服器軟體憑證由DER編碼格式轉換成PEM編碼格式

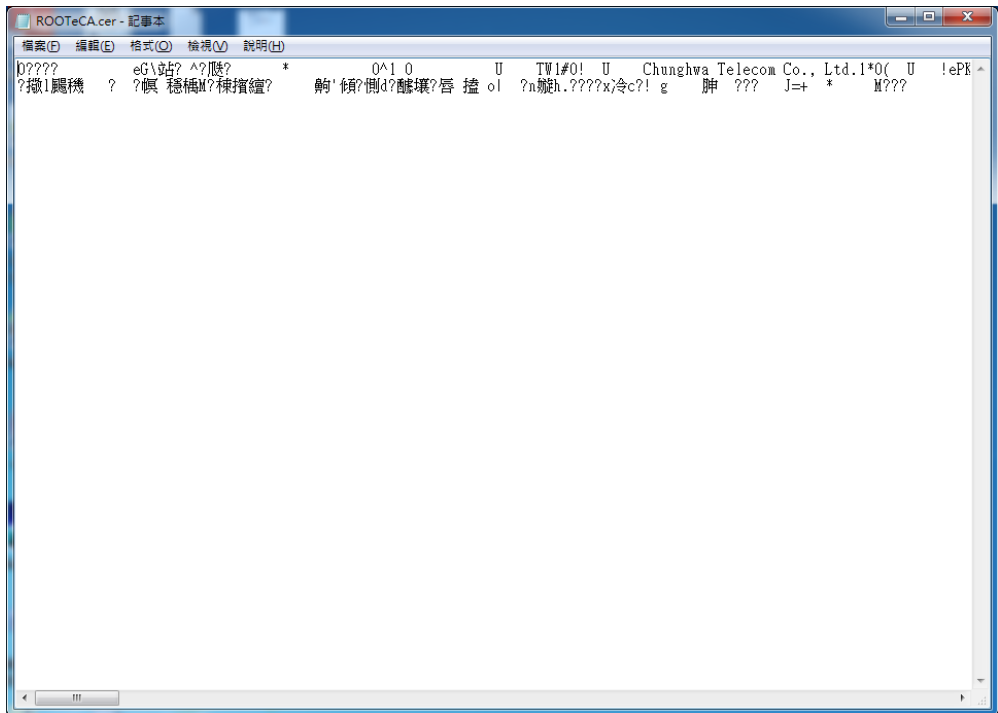
```
$ openssl x509 -in server.cer -inform DER -out server.crt。
```

如何確認憑證編碼格式：請利用文字編輯器將憑證檔案開啟，根據出現的畫面來判別憑證編碼格式。

PEM 編碼格式：



DER 編碼格式：



(3) 若 Apache 版本 < **2.4.8**，請參考以下步驟操作

- 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為 <apache 安裝路徑>\conf\extra\ 目錄下。

- 修改以下三個參數並存檔

SSLCertificateFile：伺服器憑證(*.cert)檔案路徑

SSLCertificateKeyFile：私密金鑰檔案路徑

SSLCertificateChainFile：GRCA1_5_GCA2.crt 檔案路徑

請注意這把 SSL Server 私密金鑰必須是當初您用來產生憑證請求檔 (Certificate Signing Request, CSR) 所對應的同一把私密金鑰，否則將無法成功建立 SSL 連線。

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on
```

```
SSLCertificateFile "/export/httpd-2.2.29/certs/server.crt"
SSLCertificateKeyFile "/export/httpd-2.2.29/certs/server.key"
SSLCertificateChainFile "/export/httpd-2.2.29/certs/GRCA1_5_GCA2.crt"
```

(4) 若 Apache 版本 \geq 2.4.8，請參考以下步驟操作

- cat server.crt GRCA1_5_GCA2.crt > server-chain.crt
- mv server-chain.crt server.crt (此 crt 檔案經由修改已經包含完整憑證串錄)
- 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為 <apache 安裝路徑>\conf\extra\ 目錄下。
- 修改以下 2 個參數並存檔

SSLCertificateFile：伺服器憑證(*.crt)檔案路徑

SSLCertificateKeyFile：私密金鑰檔案路徑

請注意這把 SSL Server 私密金鑰必須是當初您用來產生憑證請求檔 (Certificate Signing Request, CSR) 所對應的同一把私密金鑰，否則將無法成功建立 SSL 連線。

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on
```

```
SSLCertificateFile "/export/httpd-2. /certs/server.crt"
SSLCertificateKeyFile "/export/httpd-2. /certs/server.key"
```

- (5) 重新啟動 Apache
- (6) 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。
- (7) 成功後，請以 https 連線測試 SSL 加密通道。

Windows Apache SSL 憑證請求檔製作手冊

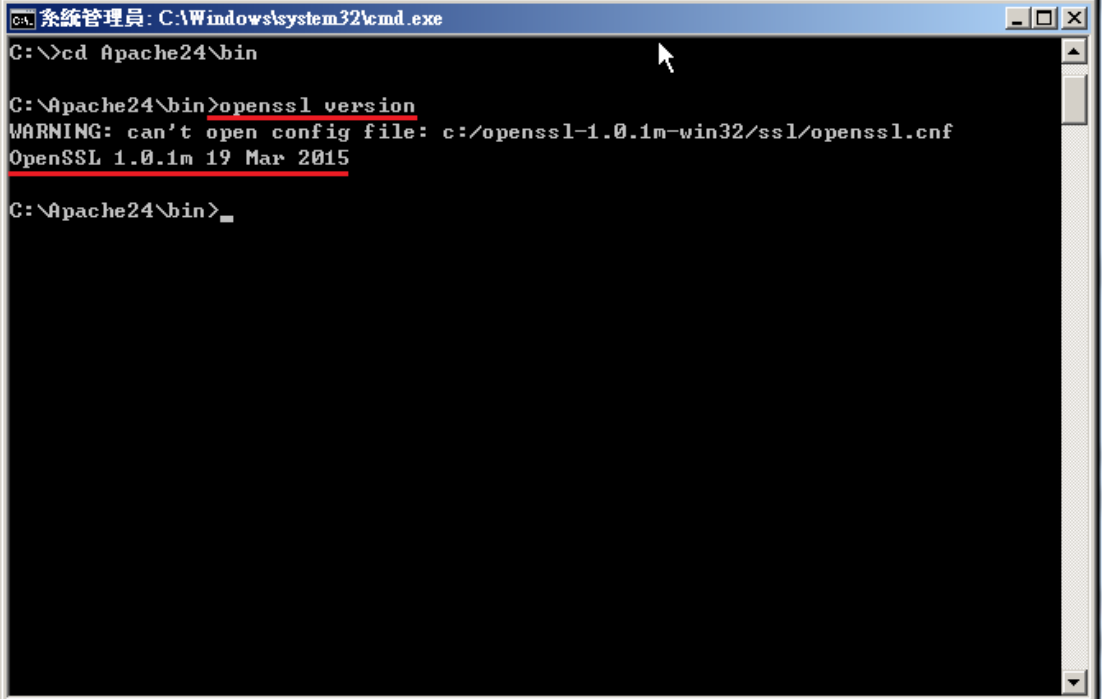
一、產生憑證請求檔

- (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 <apache 安裝目錄>/bin 目錄下, 會包含一個 openssl.exe 檔案。
- (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



```
系統管理員: C:\Windows\system32\cmd.exe
C:\>\cd apache24\bin

C:\Apache24\bin>openssl version
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
OpenSSL 1.0.1m 19 Mar 2015

C:\Apache24\bin>_
```

- (3) 因 Windows 系統下的 Apache 無法詢問私密金鑰密碼, 故產生不加密之 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 -out <server.key 儲存路徑> 2048


```
系統管理員: C:\Windows\system32\cmd.exe
C:\>cd apache24\bin

C:\Apache24\bin>openssl version
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
OpenSSL 1.0.1m 19 Mar 2015

C:\Apache24\bin>openssl genrsa -out C:\SSL\server.key 2048
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

C:\Apache24\bin>
```

- 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**。若是在提出憑證申請後，金鑰遺失，核發下來的憑證將會無法使用，需要重新提出申請與廢止憑證。
- (5) 產生憑證請求檔

\$ openssl req -new -key <server.key 路徑> -out <certreq.txt 儲存路徑>

- 若您在執行此指令時遇到「**WARNING: can't open config file...**」的訊息，請先找出 Apache 安裝目錄下的 openssl.cnf，然後執行以下環境變數設定後，在執行產製憑證請求檔指令
set OPENSSL_CONF=<openssl.cnf 所在路徑>

請輸入憑證主體資訊到憑證請求檔中，不過 GCA 網站 SSL 憑證申請頁面只會擷取憑證請求檔中的公開金鑰數值，並不會使用以下憑證主體資訊，而是以您在 GCA 網站填寫之申請書內容進行身分審驗。

Country Name : TW

State or Province Name : 不需輸入，按 enter 鍵略過

Locality Name : 城市(如：Taipei)

Organization Name : 組織名稱(如：CHT)

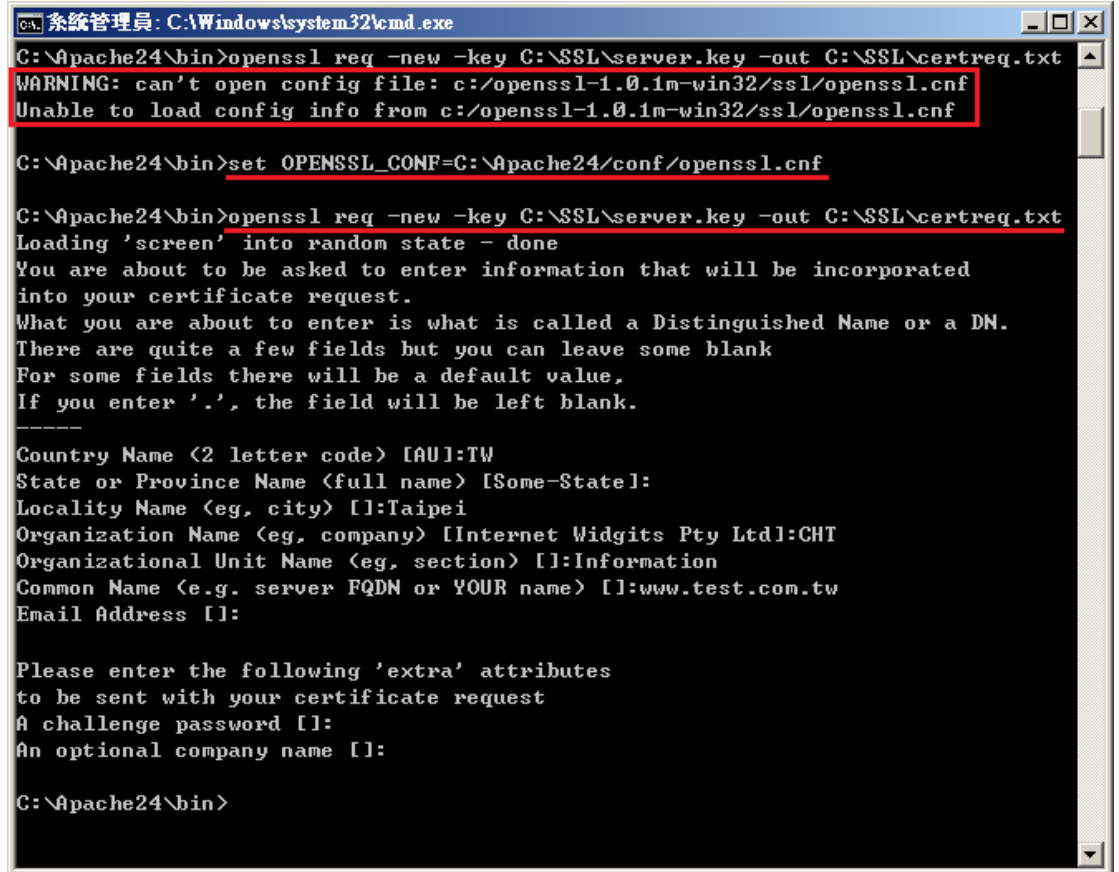
Organizational Unit Name : 單位名稱(如:Information)

Common name：網站名稱(如：www.abc.com.tw，多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主)

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

A challenge password：不需輸入，按 enter 鍵略過

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



```
CA 系統管理員: C:\Windows\system32\cmd.exe
C:\Apache24\bin>openssl req -new -key C:\SSL\server.key -out C:\SSL\certreq.txt
WARNING: can't open config file: c:/openssl-1.0.1m-win32/ssl/openssl.cnf
Unable to load config info from c:/openssl-1.0.1m-win32/ssl/openssl.cnf

C:\Apache24\bin>set OPENSSL_CONF=C:\Apache24\conf\openssl.cnf

C:\Apache24\bin>openssl req -new -key C:\SSL\server.key -out C:\SSL\certreq.txt
Loading 'screen' into random state - done
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 DN.
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) [AU]:TW
State or Province Name (full name) [Some-Statel]:
Locality Name (eg, city) []:Taipei
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CHT
Organizational Unit Name (eg, section) []:Information
Common Name (e.g. server FQDN or YOUR name) []:www.test.com.tw
Email Address []:

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

C:\Apache24\bin>
```

(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 所在路徑>

請求檔內容範例如下:

```
系統管理員: C:\Windows\system32\cmd.exe
C:\Apache24\bin>openssl req -noout -text -in C:\SSL\certreq.txt
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=TW, ST=Some-State, L=Taipei, O=CHT, OU=Information, CN=www.test.com.tw
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:bb:12:9c:9a:6b:ae:cd:d5:66:4f:18:3a:fe:a6:
      b4:75:b2:d5:46:c5:75:36:8b:6d:e9:46:52:fb:3b:
      8a:b3:a7:76:e5:1f:39:e8:20:33:4a:d5:d0:4a:f1:
      b8:09:5b:57:6d:bb:90:69:45:62:08:35:12:81:ae:
      e1:0c:2f:00:0a:e4:6b:27:01:80:37:fd:61:a1:c0:
      f0:dc:53:05:25:e0:22:90:19:a6:c9:3e:75:d1:b4:
      63:cd:82:aa:fa:d9:ab:5e:38:58:81:3f:66:54:64:
      8b:0c:c4:4e:67:b8:2e:4c:62:19:82:af:73:7b:f4:
      6c:b4:a1:9c:b5:6c:01:f8:6f:fa:01:58:45:e4:36:
      f1:1b:7d:cb:60:c2:17:1f:38:41:31:5d:2a:e5:23:
      4e:45:17:f8:67:b7:8c:d1:55:66:71:89:4f:87:91:
      17:d1:5c:61:b0:5b:40:1a:2c:23:fd:f1:83:ad:f9:
      2e:77:4c:66:f8:35:e6:fc:30:ec:13:21:bd:f9:88:
      6e:77:7b:32:b2:28:00:b5:b9:75:56:75:be:60:35:
      14:66:05:21:36:2f:3d:6c:02:6a:f4:c2:17:17:38:
      3f:ec:87:51:3c:47:82:0f:21:63:61:82:3c:bb:ee:
      30:f9:7a:6c:ee:21:ed:90:9e:0b:4e:4b:19:92:db:
      31:a3
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: sha1WithRSAEncryption
    40:c4:47:4b:1a:00:dc:77:7f:7f:f3:9a:07:78:b0:2a:a5:5e:
    d9:90:bc:ec:1e:ba:80:5b:2d:56:b9:0c:dc:d6:76:68:a0:92:
    64:83:41:92:21:89:b1:b3:17:7e:2b:a5:3d:5d:98:c7:5f:9a:
    68:f2:0a:e6:82:62:b9:86:0e:77:48:78:dc:94:31:d4:71:e0:
    3c:72:31:11:6b:c0:59:93:c4:18:88:e7:87:b5:a6:ee:69:1c:
    06:ba:23:dd:f1:fe:d1:7d:ff:ef:97:b0:47:7e:f6:5c:f8:ce:
    ab:fb:2c:33:7c:d9:fb:82:f2:06:84:fb:51:58:83:f3:c6:fe:
    a4:ae:c9:7a:e6:05:b6:b0:48:30:07:fb:ef:27:b2:47:26:41:
    35:e2:68:e3:c4:35:c9:72:dd:0d:f1:2c:93:bf:46:f8:b9:39:
    28:15:eb:2f:19:8b:f8:71:23:3c:5e:dd:a1:19:63:f7:ca:2c:
    e6:4b:6b:d2:02:77:2b:5f:a0:8b:3b:b9:57:a7:5e:05:6c:c3:
    f5:b4:7c:2a:a4:89:db:bf:f1:01:80:63:e7:a0:6e:a5:8d:d1:
    4f:09:ef:17:70:25:3c:46:3a:30:14:86:b4:31:d0:85:f4:3b:
    25:9a:19:e4:d2:68:3b:2d:dd:54:e7:e5:24:e7:fd:61:6d:c9:
    f3:30:1c:4c
C:\Apache24\bin>
```

- 二、將憑證請求檔存放到方便存取的目錄，完成製作憑證請求檔動作。
- 三、請至 GCA 網站(<http://gca.nat.gov.tw>)進行 SSL 憑證申請作業

Windows Apache SSL 憑證安裝操作手冊

一、取得 GRCA 及 GCA 憑證之憑證串鏈

當您向 GCA 申請的 SSL 伺服器軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服器軟體憑證，而必須先取得 GRCA 及 GCA 之憑證串鏈，並在 Apache Server 上安裝 GRCA 及 GCA 之憑證串鏈，這樣您接下來安裝的 SSL 伺服器軟體憑證才會正常運作。如果您以前曾經在同一部 Apache Server 上成功安裝過 GRCA 及 GCA 之憑證串鏈，則您可以跳過步驟一和二，直接進行 SSL 伺服器應用軟體憑證的安裝。

- (1) 請至GCA網站下載已經製作好的憑證串鏈檔案，格式為PEM編碼，下載網址為http://gca.nat.gov.tw/download/GRCA1_5_GCA2.zip
- (2) 將下載的GRCA1_5_GCA2.zip解壓縮得到GRCA1_5_GCA2.crt

二、安裝 GRCA 及 GCA 之憑證串鏈與 SSL 憑證

- (1) 請確定已下載簽發之 SSL 伺服器軟體憑證(*.cer)。
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。
- (2) 執行以下命令將 SSL 伺服器軟體憑證由 DER 編碼格式轉換成 PEM 編碼格式

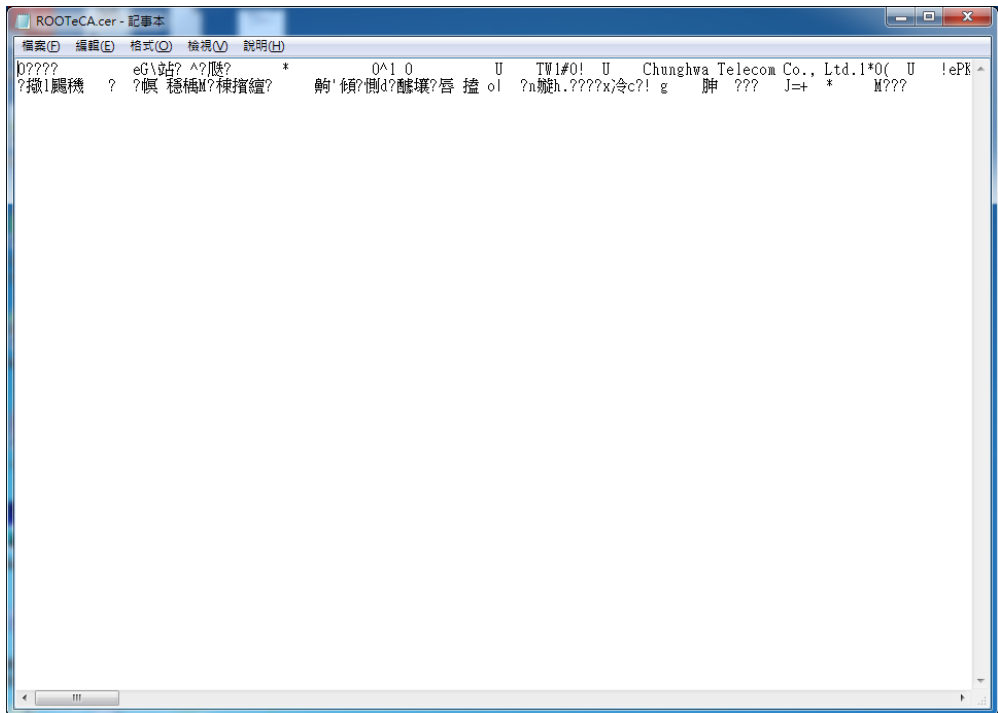
```
$ openssl x509 -in server.cer -inform DER -out server.crt。
```

如何確認憑證編碼格式：請利用文字編輯器將憑證檔案開啟，根據出現的畫面來判別憑證編碼格式。

PEM 編碼格式：



DER 編碼格式：



(3) 若 Apache 版本 < **2.4.8**，請參考以下步驟操作

- 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為 <apache 安裝路徑>\conf\extra\ 目錄下。
- 修改以下三個參數並存檔
 - SSLCertificateFile：伺服器憑證(*.cert)檔案路徑
 - SSLCertificateKeyFile：私密金鑰檔案路徑
 - SSLCertificateChainFile：GRCA1_5_GCA2.crt 檔案路徑

請注意這把 SSL Server 私密金鑰必須是當初您用來產生憑證請求檔 (Certificate Signing Request, CSR) 所對應的同一把私密金鑰，否則將無法成功建立 SSL 連線。

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite EEC DH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on
```

```
SSLCertificateFile "/export/httpd-2.2.29/certs/server.crt"
SSLCertificateKeyFile "/export/httpd-2.2.29/certs/server.key"
SSLCertificateChainFile "/export/httpd-2.2.29/certs/GRCA1_5_GCA2.crt"
```

(4) 若 Apache 版本 $\geq 2.4.8$ ，請參考以下步驟操作

- 將 GRCA1_5_GCA2.crt 使用文字編輯軟體開啟，複製全部的內容。
- 用文字編輯軟體開啟 SSL 憑證
- 在開啟之 SSL 憑證檔案最後面間隔一空空白行，貼上步驟(1)複製的憑證串錄內容，可參考下圖。

```
1 -----BEGIN CERTIFICATE-----
2 MIIIFNzCCBB+gAwIBAgIQboDPTayQ/0nvVYN0jC89TzANBgkqhkiG9w0BAQsFADBE
3 MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQLEDBjmlL/1
4 upzmqhpHorYnnrqHnkIbkuK31v4MwHhcNMTUwNjI2MDcyOTEzWbcNMTgwNjI2MDcy
5 OTEzWjB4MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQLE
6 DBjmlL/lupzmqhpHorYnnrqHnkIbkuK31v4MwFzAVBqNVBAMTDmdjYS5uYXQuZ292
7 LnR3MRkwFwYDVQQFEwAwMDAwMDAwMDEwMDI0OTMxMIIIBIjANBgkqhkiG9w0BAQEF
8 AAOCAQ8AMIIBCgKCAQEAE36nu2MtLzMzB1Of71CqnV2VC/qpwk8Yh/nbYXJ/KCkBO
9 raDPxAD5IjJYHkAR5RcwkbdcEXyEylfsBmoqikpT8NLRJQZKBmc0cciltIeFRZWX
10 ymNhEBkmMo3jhK2r/3o1WLIcnoA1rSifLBC0TAR3xjzHQ1xIG4/FkC89APo0PZNR
11 Beo8h67YSgnGbSA/1fG/KCKCc3dbzKi4PADffrvUzmpIvIsm1MTxo028TT/BkrP2
12 LpxLr8p6+fc7s7b7mcr1nLBLETGAT+/tGIn+v1T14DnrK/0kbjUiyTlOkrlq8bYO
13 Vc4Znr7+1f8Vt6jY1BFDEdr5SJBIZD/cMgjUChTzrwIDAQABo4IB7zCCAesHwYD
14 VR0jBBgwFoAU0Rhnw1f+EpgRa19fMeo+woSH+70wHQYDVRO0BBYEFIF1LP61DPXX
15 psjH64JagS2rR1ZZMIGYBgggrBgEFBQcBAQSBizCBiDBFBgggrBgEFBQcwoAoY5aHR0
16 cDovL2djYS5uYXQuZ292LnR3L3JlcG9zaXRvcnkVQ2VydHMvSXNzdWVkbG9UaGlz
17 Q0EucDdiMD8GCCsGAQUFBzABhjnNodHRwOi8vZ2NhLm5hdC5nb3YudHcvY2dpLWJp
18 bi9PQ1NQMi9vY3NwX3NlcnZlc15leGUwDgYDVRO0PAQH/BAQDAgWgMBQGA1UdIAQN
19 MAswCQYHYIIZ2ZQADAZAZBgNVHREEEjAqgg5nY2EubmF0Lmdvdi50dzAgBgNVHQkE
20 GTAXMBUGB2CGdgFkAgExCgYIYIIZ2AWQDAwEwgYgGA1UdHwSBgDB+MD2gO6A5hjdO
21 dHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9HQ0E0L0NSTDIVq1JMXzAw
22 MDEuY3JsMD2gO6A5hjdodHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9H
23 Q0E0L0NSTDIVY29tcGxldGUuY3JsMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggr
24 BgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAs71WC1KbhEmLBKu5HmUpHARv51Va
25 rGusMOPN1BiKwLnfIP9WgcEzwInHdlC8YEEzWYM5K6qagP1spWhzA4rGIg4660ZO
26 z91Sk6sqE1hhYza/BnYlpvz63y8XjCUA0w0WWpbKpCJWGeuTg7FaN2ZpQs4POMbU
27 36aernb1KLTIFoQUFmfklmUiHNKe3+g03xTINzyZ+1JCRtk6frG1Cyqq07h0d2Zc
28 iHgCokChSiqpSjL5/42dl5yYc/W9eU4gFfSdvC0f1OHb8cCspbmtTI6RWnU5UoY8
29 aJofnhLb1x/k8GwgizPvQk7axgOfaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA==
30 -----END CERTIFICATE-----
```

31 與END CERTIFICATE間隔一空空白行，貼上複製的憑證串錄內容
32

- 貼上後之檔案範例如下圖。

```
iHgCokChSiqpsJL5/42d15yYc/W9eU4gFfSdvC0f1OHb8cCspbmtTI6RWnU5UoY8
aJofnhLb1x/k8GwgizPvQk7axgOFaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA==
-----END CERTIFICATE-----
```

原本SSL憑證之內容

```
subject=/C=TW/O=\xE8\xA1\x8C\xE6\x94\xBF\xE9\x99\xA2/OU=\xE6\x94\xBF\xE5\xBA\x9C\xE6\x
issuer=/C=TW/O=Government Root Certification Authority
-----BEGIN CERTIFICATE-----
MIIFLzCCAxegAwIBAgIQMe5Y77XBpI+a7fR13bilwTANBgkqhkiG9w0BAQsFADA/
AQswCQYDVQQGEwJUVzEwMC4GA1UECgwnR292ZXJubWVudCBSb290IENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5SMB4XDTEzMTAzMjIzNFoXDTMzMDEzMTAzMjIzNFow
RDELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCEihjOaUv+mZojEhMB8GA1UECwwY5pS/
5bqc5oaR6K2J566h55CG5Lit5b+DMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAtX7xPZUtp5iBGQvqYghJUoLeyCJJoatcc1bc0GHij64WUBYPdu8KKEQK
R1y3zjcDXrLcZX483tmNs92DXSNuBHlx+welaFyuLpKQVCji97ys3KeMxAcaxQo
3cZu8nY3g//zkvX80G4RoCyDR86Z420R3mb0G1Vw/9TEK8+oduZqAArEdfionpbE
K5zZ/8qaaHafggMBQGuzfccDKLoWRcTzu3S0IvOpVU6pcB0rJOtc4F7c16tQdXfo
a8sjfcveKKbUQF6AklwugRufHdLqEVpOiGRcDPAhtT6SHJ7D/t+A/rAXMPidcksQ
rea/E+5+lehqEMHSA/gSLa9Ph+/gDQIDAQABo4IBIDCCARwHwYDVR0jBBgwFoAU
lWcd4Jx6LJzLxZjnHQcmKobsdM0wHQYDVR0OBBYEFNEY28NX/hKakWtfxZhgPseK
n/u9MA4GA1UdDwEB/wQEAwIBBjA+BgNVHR8ENzA1MD0gMaAvh1lodHRwOi8vZ3Jj
fS5uYXQuZ292LnR3L3JlcG9zaXRvcnkQ1JMMi9DQ55jcmwvVgYIKwYBBQUHAQEE
B3BIMEYGCsGAQUFBzACHjpodHRwOi8vZ3JjY55uYXQuZ292LnR3L3JlcG9zaXRv
cnkvQ2VydHMvSXNzdWVvKVG9UaG1zQ0EucDdiMBIGA1UdEwEB/wQIMAYBAf8CAQAw
HgYDVR0gBBcwFTAJBgdghnZ1AAMDMAgGBmeBDAECAjANBgkqhkiG9w0BAQsFAAOC
AgEAs3KvqDSIq6GERR/SonDfYnrpF/IdZLM9gBfsIIafNeeWjFCiUC5Ah7LEIhZY
PP/D8y00OCR1Z7GoY4JZIVTFA1fb2umEmKC/ssCwQdUxyd52JfbqBL5N0cP2eU1x
LZG8d1z8uIq7ItYfO5ML1eAboYMHsO7c1OpLmtufZj8VZ4zp4DTRxVzROPKw1IbR
QSKNlymWgAop+Eg9b401fBMBxPppb3R4IZpijCpy0RbPozvtmDpen3WzmJ+vsCq
08b8JqDeRG5zQI1sIeV15qqGZuV8oL5gFi4niltkLNS3fGYAr4+LXVojMWIO/Noe
Ji+i3AtfhnN/w3Ixxhxi39pN+hYzFGtsZNIoUC2MQexFJS+AQ4s8D41cRCMwovfi
DerTbWKhTPOQXirUDV/ZSUjULDbXzdiUB+mxWd2k16HYcvMFUevxbNzJAXP355T
q9tliZpM/7MVq0/Bw4SGxxQRQFluVQjMBtEsRYHKVZ1IBBJVOe8jZhc81Sw3jDmm
Ttyjx1o2m8VVImSiIP2iPI3hlw/UCwCGRg5xvqqW72w2niT9pXdvZowBVbhP24wt
amuA45M5h4UNZRNo4/NG3UwS9eLkTfB06YFf3DcBban/Drf8LX8OGvF++Im3SeGJ
6zhU1YOvJcTHPr6TToXoKzvuzegRL2vQ4k22B++JtOQgsAg=
-----END CERTIFICATE-----
```

複製貼上的憑證串錄內容

```
subject=/C=TW/O=Government Root Certification Authority
issuer=/C=TW/CN=Government Root Certification Authority - G1.5
-----BEGIN CERTIFICATE-----
MIIGcTCCBfmgAwIBAgIRAKOUO28QJ1H0ulORI3SaKiowDQYJKoZIhvcNAQELBQAw
NjELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCEihjOaUv+mZojE3MDUGA1UEAwuR292
ZXJubWVudCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzEuNTAeFw0x
NzA3MTkwMjUxNDhaFw0yMDA3MTkwMjUxNDhaMD8xCzAQBgNVBAYTA1RXMTAwLgYD
VQKDCdHb3Z1cm5tZW50IFJvb3QgQ2VydG1maWNndG1vbiBbBdXRob3JpdHkwgGii
AAOGCSqGSIB3DQEBAQUAA4ICDwAwggIKAoICAQC2/5c8gb4BWCQnr44BK9ZykjAy
```

- 將修改後的 SSL 憑證檔案存檔，本範例檔名為 server.crt，此 SSL 檔案經由修改已經包含完整憑證串錄。
- 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為 <apache 安裝路徑>\conf\extra\ 目錄下。
- 修改以下 2 個參數並存檔
 SSLCertificateFile：伺服器憑證(*.crt)檔案路徑
 SSLCertificateKeyFile：私密金鑰檔案路徑
 請注意這把 SSL Server 私密金鑰必須是當初您用來產生憑證請求檔 (Certificate Signing Request, CSR) 所對應的同一把私密金鑰，否則將無法成功建立 SSL 連線。

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on
```

```
SSLCertificateFile "/export/httpd-2. /certs/server.crt"
SSLCertificateKeyFile "/export/httpd-2. /certs/server.key"
```

- (5) 重新啟動 Apache
- (6) 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。
- (7) 成功後，請以 https 連線測試 SSL 加密通道。

附件一：設定 SSL 安全通道的加密強度

- Apache 使用 OpenSSL 的加密套件來做資料加密，而 Apache 加密套件的使用順序可在 http.conf 或是 http-ssl.conf 中的 SSLCipherSuite 找到。
- 預設值是「HIGH:MEDIUM:!aNULL:!MD5」，也就是加密強度「高」(HIGH encryption cipher suites, 如 AES 256 bit)、加密強度「中」(MEDIUM encryption cipher suites, 如 AES 128 bit)的順序，因此，只要 OpenSSL 有支援 AES 256 bit 的加密套件，伺服器預設就會優先使用 AES 256bit，不需要做額外設定，但需要檢查 OpenSSL 的版本。
- 更安全的方式為將欲支援的加密演算法採用正面表列的方式設定於 SSLCipherSuite。

附件二：停用 SSLv3.0

- OpenSSL 1.0.1j 版本有針對 POODLE 弱點進行修補，您可選擇同時更新 OpenSSL 版本與停用 SSLv3.0，或是直接停用 SSLv3.0。
- 先開啟 http.conf 或是 http-ssl.conf 檔案，並找到“SSLProtocol all -SSLv2”，其意思為所有 SSL 通訊協定，扣除 SSLv2.0。因此，若要停用 SSLv3.0，只要將上述改為“SSLProtocol all -SSLv2 -SSLv3”，重新啟動 Apache 即可。

```
# SSL Protocol support:
# List the protocol versions which clients are allowed to
# connect with. Disable SSLv2 by default (cf. RFC 6176).
SSLProtocol all -SSLv2 -SSLv3
```

- 啟動完成後，可使用測試工具（註 1、註 2）進行檢測，看 SSLv3.0 是否已停用。

註 1:

行政院國家資通安全會報技服中心網頁

<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh> 有介紹兩種檢測伺服器端 SSL 協定的工具：

(1) TestSSLServer (<http://www.bolet.org/TestSSLServer/>)

(2) QUALYS SSL LABS SSL Server Test 檢測工具

(<https://www.ssllabs.com/ssltest/index.html>，也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定，因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點，弱點編號 CVE-2014-3566 (POODLE)，故建議不要使用 SSL V3 協定，請改用 TLS 協定。

註 2:

(1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考

<https://zmap.io/ssl3/browsers.html> 之英文說明

(2) 請超連結至 <https://dev.ssllabs.com/ssltest/viewMyClient.html> 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。

(3) 若是 IE 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選使用 SSL V3 與使用 SSL V2，或參考下圖設定（取材自行政院國家資通安全會報技服中心網頁

<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh>)

