政府伺服器數位憑證管理中心(GTLSCA)

Apache SSL 憑證請求檔製作與憑證安裝手冊

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 與 Apache 2.4.39 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 伺服軟體憑證安裝步驟。

目錄

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。**

(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，不過憑證管理中心網站 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，而是以您在憑證管理中心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 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]:
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
```

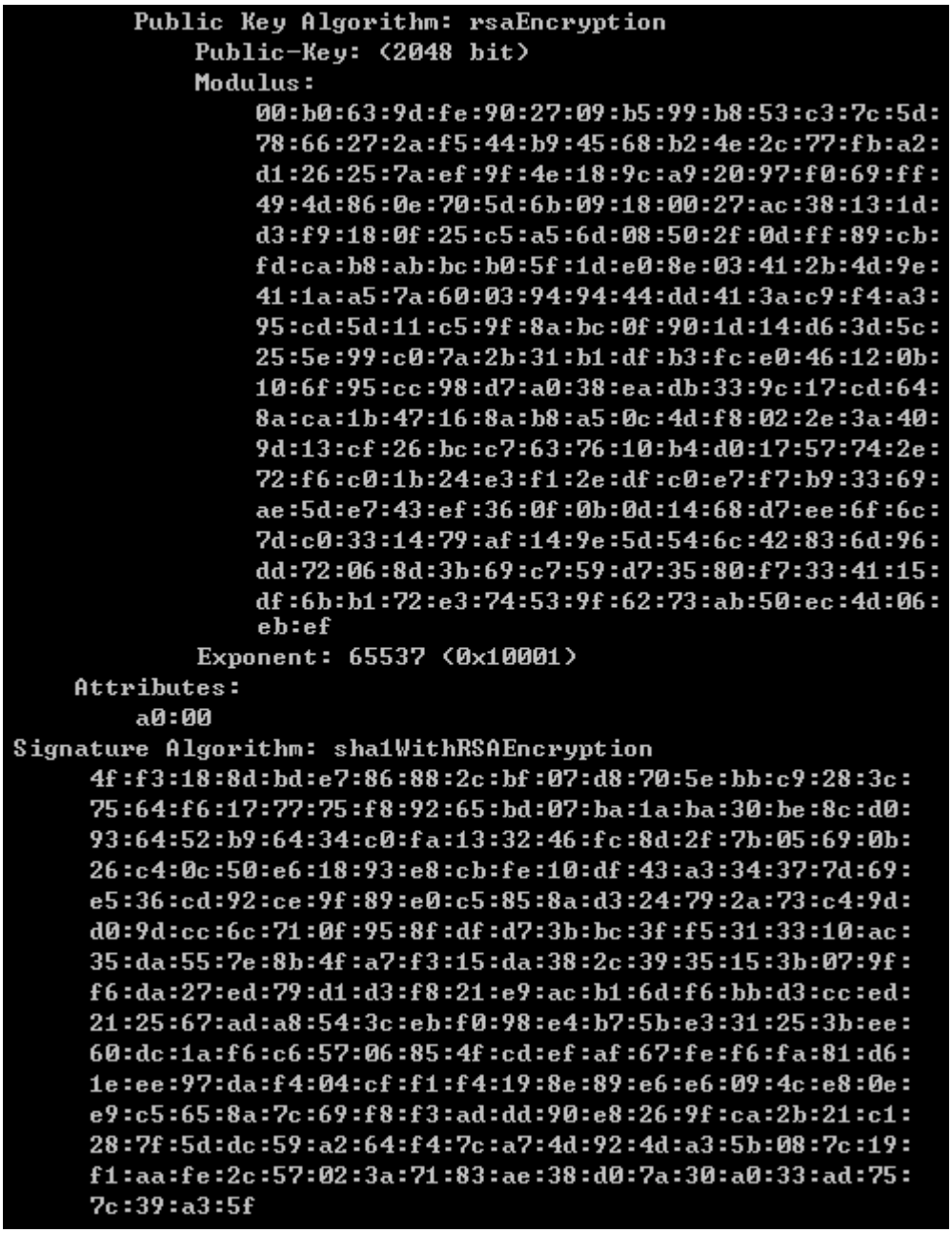
```
Email Address []:test@test.com.tw

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:



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、請至憑證管理中心網站(https://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 eCA 及 GTLSCA 之憑證串鏈

當您申請的 SSL 伺服軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服軟體憑證，而必須先取得對應之憑證串鏈，並在 Apache Server 上安裝該憑證串鏈，這樣您接下來安裝的 SSL 伺服軟體憑證才能正常運作。

(1) 請至GTLSCA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https://gtlsca.nat.gov.tw/download/eCA1_GTLSCA.zip

(2) 將下載的eCA1_GTLSCA.zip解壓縮得到eCA1_GTLSCA.crt

二、安裝 eCA 及 GTLSCA 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)。

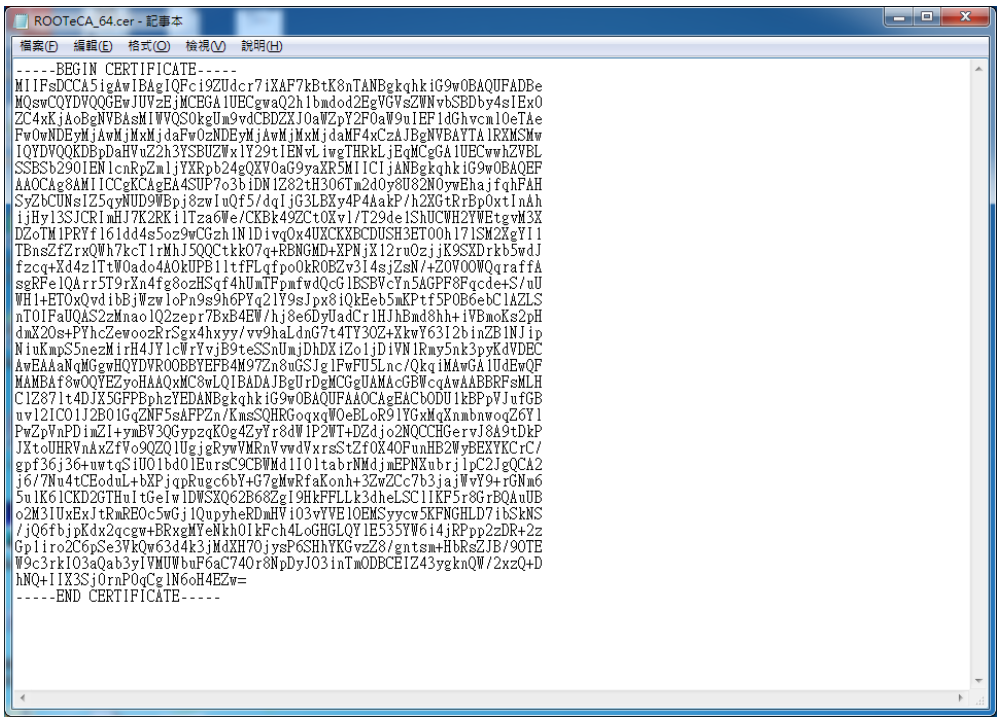
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。

(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

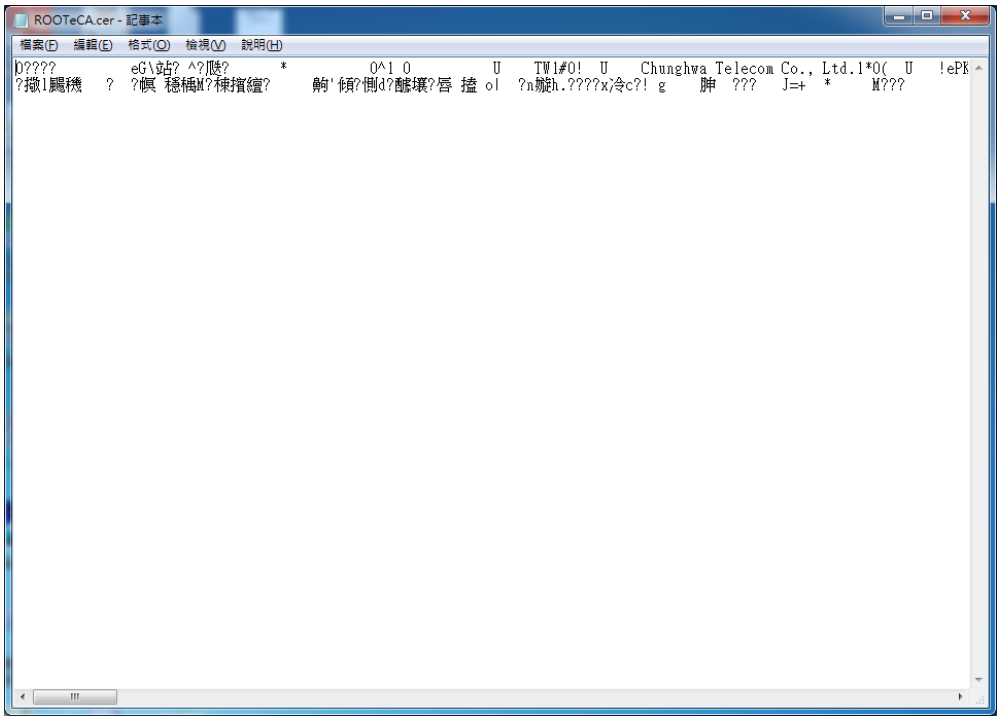
$ openssl x509 -in server.cer -inform DER -out server.crt。

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(*.crt)檔案路徑

  SSLCertificateKeyFile：私密金鑰檔案路徑

  SSLCertificateChainFile：eCA1_GTLSCA.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 -TLSv1 -TLSv1.1
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on

SSLCertificateFile "/export/httpd-2.2.29/conf/sslcerts/gca_server.crt"
SSLCertificateKeyFile "/export/httpd-2.2.29/conf/sslcerts/gca_server.key"
SSLCertificateChainFile "/export/httpd-2.2.29/conf/sslcerts/eCA1_GTLSCA.crt"
```

(4) 若 Apache 版本 >= **2.4.8**，請參考以下步驟操作

- cat server.crt eCA1_GTLSCA.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鍊)
- 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 -TLSv1 -TLSv1.1
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on

SSLCertificateFile "/export/httpd-2.    /conf/sslcerts/server.crt"
SSLCertificateKeyFile "/export/httpd-2.    /conf/sslcerts/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

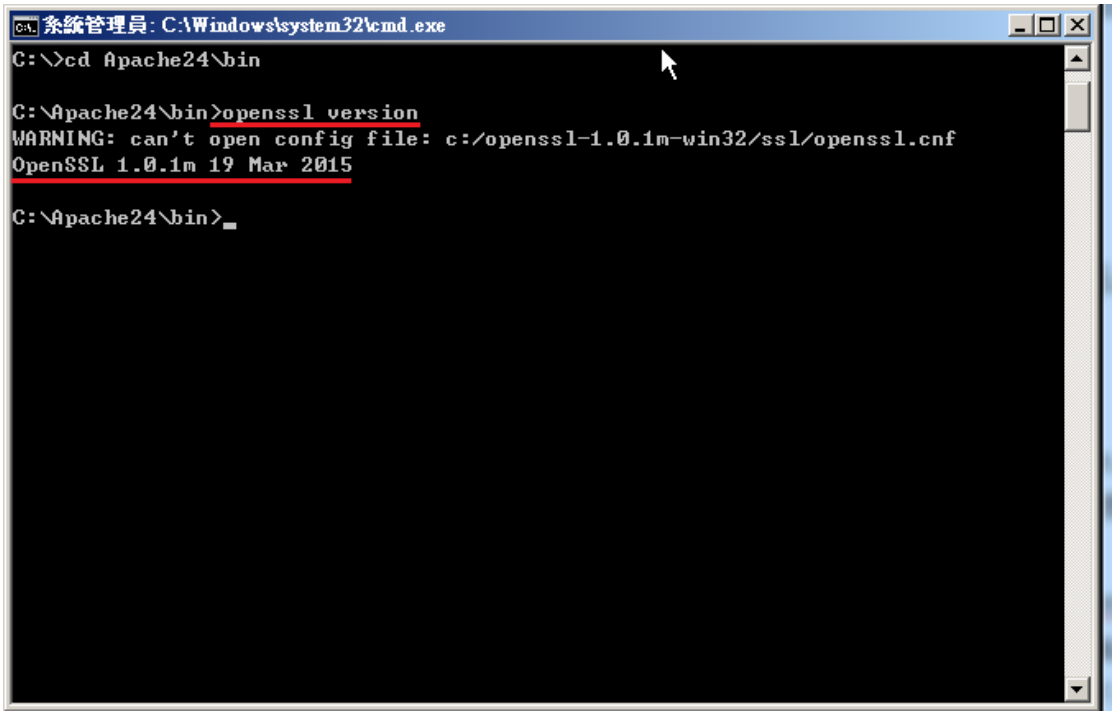
(1) 產生憑證請求檔（Certificate Signing Request file,簡稱 CSR 檔）需使用 OpenSSL 工具，此工具通常安裝在 <apache 安裝目錄>/bin 目錄下，會包含一個 openssl.exe 檔案。

(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

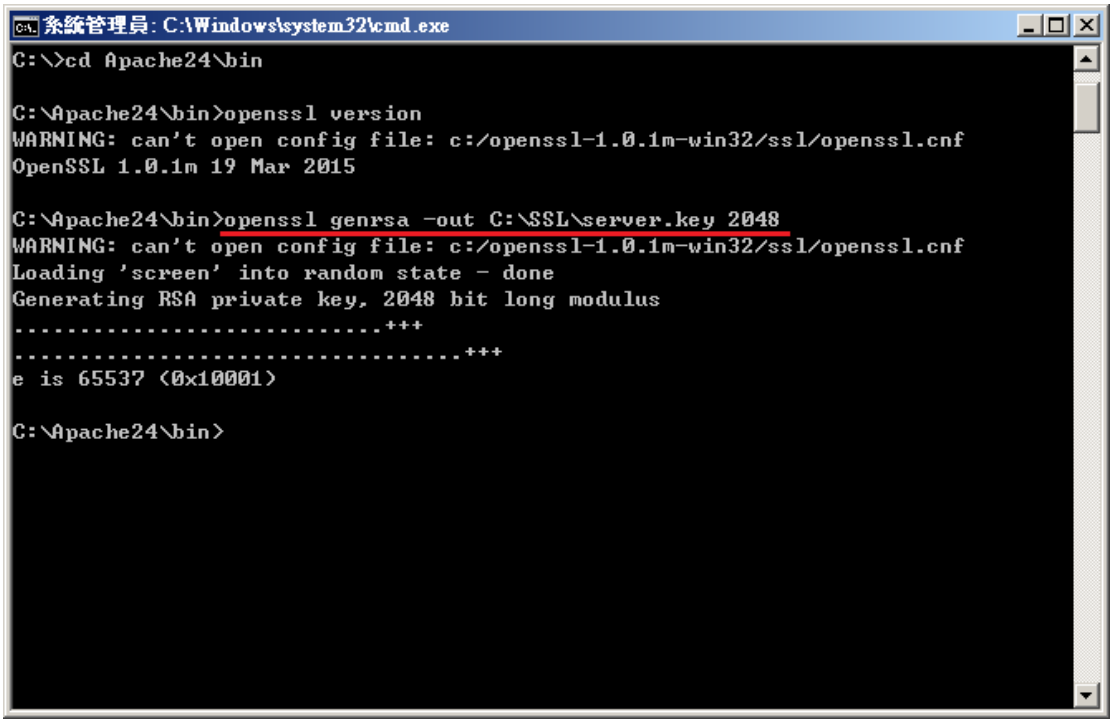
修復版本：1.0.1g / 1.0.2-beta2 以後



(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



- **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。**

(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，不過憑證管理中心網站 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，而是以您在憑證管理中心網站填寫之申請書內容進行身分審驗。

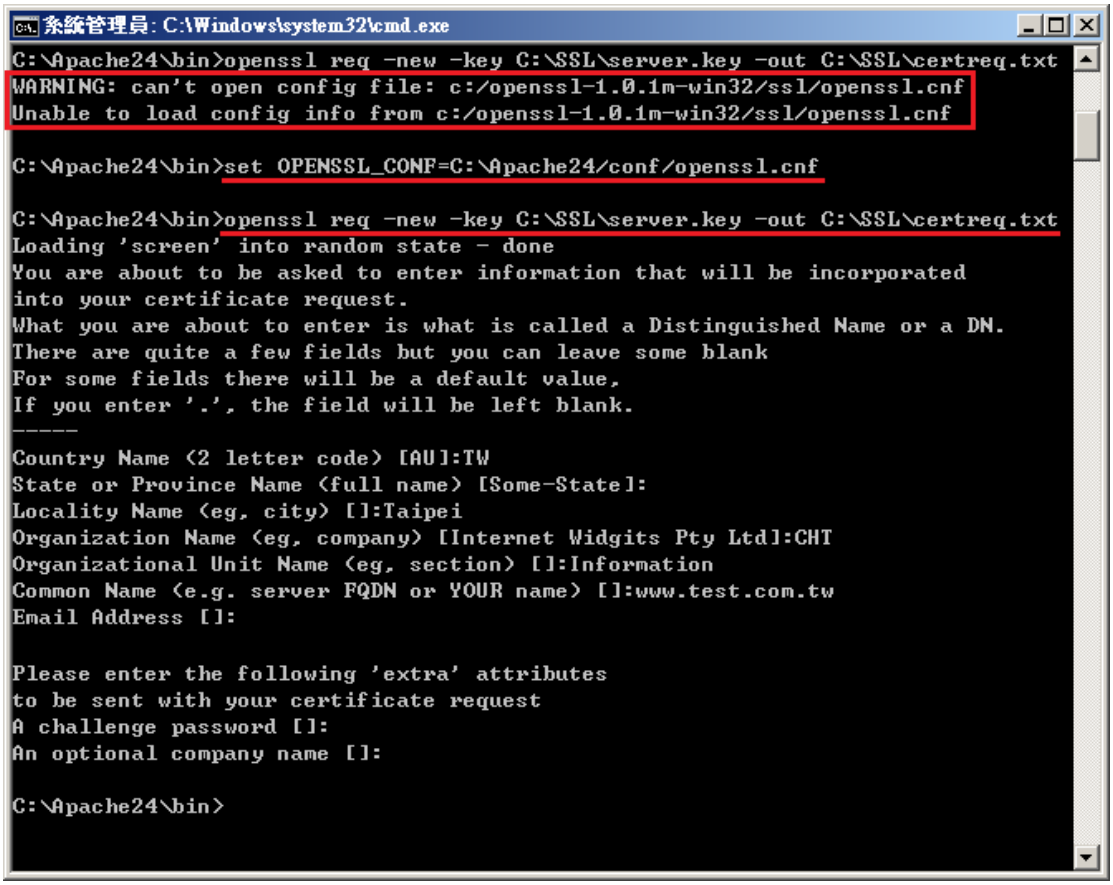
Country Name：TW
State or Province Name：不需輸入，按 enter 鍵略過
Locality Name：城市(如：Taipei)
Organization Name：組織名稱(如：CHT)
Organizational Unit Name：單位名稱(如:Information)

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



(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:

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、請至憑證管理中心網站(https://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 eCA 及 GTLSCA 憑證之憑證串鏈

當您申請的 SSL 伺服軟體憑證經審核通過並簽發之後，您可先不用急著安裝所申請的 SSL 伺服軟體憑證，而必須先取得對應之憑證串鏈，並在 Apache Server 上安裝該憑證串鏈，這樣您接下來安裝的 SSL 伺服軟體憑證才能正常運作。

(1) 請至GTLSCA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https://gtlsca.nat.gov.tw/download/eCA1_GTLSCA.zip

(2) 將下載的eCA1_GTLSCA.zip解壓縮得到eCA1_GTLSCA.crt

二、安裝 eCA 及 GTLSCA 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)。

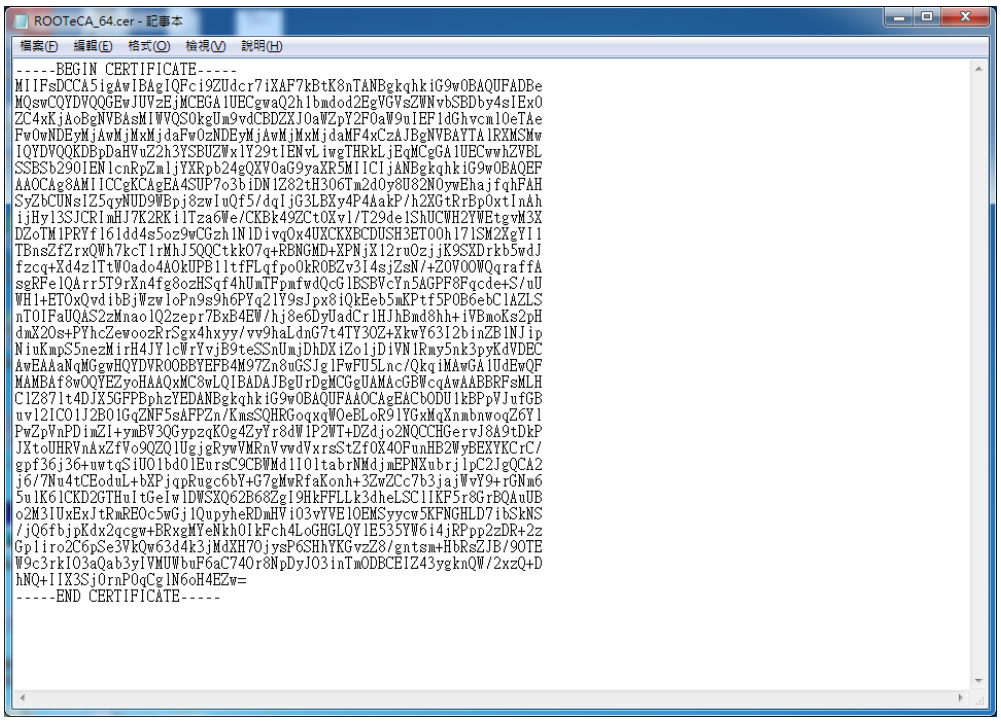
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。

(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

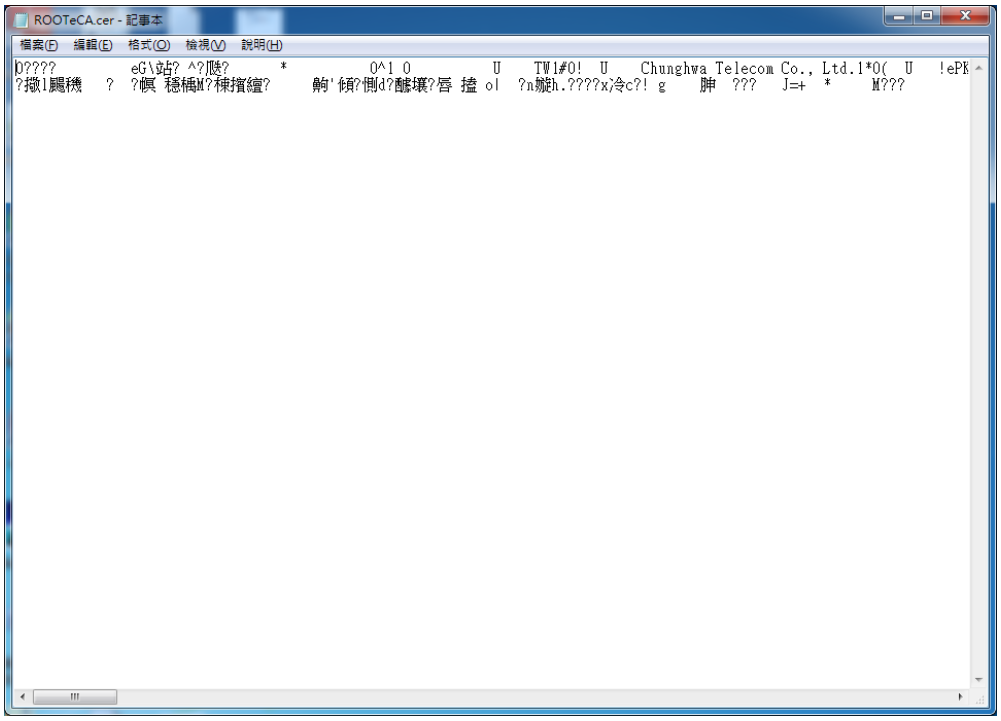
$ openssl x509 -in server.cer -inform DER -out server.crt。

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(*.crt)檔案路徑

  SSLCertificateKeyFile：私密金鑰檔案路徑

  SSLCertificateChainFile：eCA1_GTLSCA.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 -TLSv1 -TLSv1.1
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on

SSLCertificateFile "/export/httpd-2.2.29/conf/sslcerts/gca_server.crt"
SSLCertificateKeyFile "/export/httpd-2.2.29/conf/sslcerts/gca_server.key"
SSLCertificateChainFile "/export/httpd-2.2.29/conf/sslcerts/eCA1_GTLSCA.crt"
```

(4) 若 Apache 版本 >= **2.4.8**，請參考以下步驟操作

- 將 eCA1_GTLSCA.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白行，貼上步驟(1)複製的憑證串鍊內容，可參考下圖。

```
1  -----BEGIN CERTIFICATE-----
2  MIIFNzCCBB+gAwIBAgIQboDPTayQ/0nvVYN0jC89TzANBgkqhkiG9w0BAQsFADBE
3  MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQLDBjmlL/l
4  upzmhpHorYnnrqHnkIbkuK3lv4MwHhcNMTUwNjI2MDcyOTEzWhcNMTgwNjI2MDcy
5  OTEzWjB4MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQL
6  DBjmlL/lupzmhpHorYnnrqHnkIbkuK3lv4MxFzAVBgNVBAMTDmdjYS5uYXQuZ292
7  LnR3MRkwFwYDVQQFExAwMDAwMDAwMDEwMDI0OTMxMIIBIjANBgkqhkiG9w0BAQEF
8  AAOCAQ8AMIIBCgKCAQEA36nu2MtLzMzB1Of71CqnV2VC/qpwk8Yh/nbYXJ/KCkB0
9  raDPxAD5IjJYHkAR5RcwkbdCEXyEylfsBmoqikpT8NLRJQZKBmc0cciltIeFRZWX
10 ymNhEBkmMo3jhK2r/3o1WLIcnoAIrSifLBC0TAR3xjzHQ1xIG4/FkC89APo0PZNR
11 Beo8h67YSgnGbSA/1fG/KCKCc3dbzKi4PADffrvUzmpIvIsm1MTxo028TT/BkrP2
12 LpxLr8p6+fc7s7b7mcr1nLBLETGAT+/tGIn+v1T14DnrK/0kbjUiyTlOkr1q8bYO
13 Vc4Znr7+lf8Vt6jYlBFDEdr5SJBIZD/cMgjUChTzrwIDAQABo4IB7zCCAeswHwYD
14 VR0jBBgwFoAU0Rhnw1f+EpqRa19fMeo+woSH+70wHQYDVR0OBBYEFIFlLP6lDPXX
15 psjH64JagS2rR1ZZMIGYBggrBgEFBQcBAQSBizCBiDBFBggrBgEFBQcwAoY5aHR0
16 cDovL2djYS5uYXQuZ292LnR3L3JlcG9zaXRvcnkvQ2VydHMvSXNzdWVkVG9UaGlz
17 Q0EucDdiMD8GCCsGAQUFBzABhjNodHRwOi8vZ2NhLm5hdC5nb3YudHcvY2dpLWJp
18 bi9PQ1NQMi9vY3NwX3NlcnZlci5leGUwDgYDVR0PAQH/BAQDAgWgMBQGA1UdIAQN
19 MAswCQYHYIZ2ZQADAzAZBgNVHREEEjAQgg5nY2EubmF0Lmdvdi50dzAgBgNVHQkE
20 GTAXMBUGB2CGdgFkAgExCgYIYIZ2AWQDAwEwgYgGA1UdHwSBgDB+MD2gO6A5hjdo
21 dHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9HQ0E0L0NSTDIvQ1JMXzAw
22 MDEuY3JsMD2gO6A5hjdodHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9H
23 Q0E0L0NSTDIvY29tcGxldGUuY3JsMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggr
24 BgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAs71WC1KbhEmLBKu5HmUpHARv5lVa
25 rGusMOPNlBiKwLnfIP9WgcEzwInHdlC8YYEzWYM5K6qagP1spWhzA4rGIg4660ZO
26 z91Sk6sqE1hhYza/BnYlpvz63y8XjCUAOw0WWpbKpCJWGeuTg7FaN2ZpQs4POMbU
27 36aernb1KLTIFOQUFmfklmUiHNKe3+g03xTINzyZ+1JCRtk6frG1CyqqO7h0d2Zc
28 iHgCOkChSiqpSJL5/42dl5yYc/W9eU4gFfSdvC0f1OHb8cCspbmtTI6RWnU5UoY8
29 aJofnhLb1x/k8GwgizPvQk7axgOFaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA==
30 -----END CERTIFICATE-----
31
32 與END CERTIFICATE間隔一空白行，貼上複製的憑證串鍊內容
```

- 貼上後之檔案範例如下圖。

```
9KmS6KznEVKBRq7/w3SouQznO0wRGcS8TxOSvIkWfMDmeU2O8lkvqMmDLbiLxpya
W4cljrcgcgMqe3JzJSbN5rZBqgnQseAnV0HktCrs9MDig3Sd7yLpSrgLJIdlPvnI
vA==
-----END CERTIFICATE-----
```

原本SSL憑證之內容

```
subject=/C=TW/O=\xE8\xA1\x8C\xE6\x94\xBF\xE9\x99\xA2/CN=\xE6\x94\xBF\xE5\xBA\x9C\xE4\xBC\x
issuer=/C=TW/O=Chunghwa Telecom Co., Ltd./CN=ePKI Root Certification Authority - G2
-----BEGIN CERTIFICATE-----
MIIGtjCCBJ6gAwIBAgIRAJltX+mt4Wzcjs2/7bFKMpUwDQYJKoZIhvcNAQELBQAw
YzELMAkGA1UEBhMCVFcxIzAhBgNVBAoMGkNodW5naHdhIFRlbGVjb20gQ28uLCBM
dGQuMS8wLQYDVQQDDCZlUEtJIFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkg
LSBHMjAeFw0xOTA3MTkwNjQ2NDVaFw0zMTA4MTkwNjQ2NDVaMFgxCzAJBgNVBAYT
AlRXMRIwEAYDVQQKDAnooYzmlL/pmaIxNTAzBgNVBAMMLOaUv+W6nOS8uuacjeWZ
qOaVuOS9jeaGkeitieeuoeeQhuS4reW/gyAtIEcxMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEAwg5R4LGoDj+mZIXmcHmRYv50ljsSLIm7EoX/KAt74uN2
yDR436V2EWkFeWhD+TS4sx2/3JCRW+KE+IX8NYBKjsWuK9OMY4Gu4FEWJpBulXCW
YjTPKyhHdEhDpxRxv9lg3Zk68XgK7j2U5sEzCPxl3QjkH7qc/Mo5BFiro8YsYAfx
gCoa/rZFEsXyZKXRJeIDw7t+iPxVy2cbQ0uNloO9670LGoOVzYVkYABv3IwZo+JR
tj+j7rLjB7xQKYmfJOA2Jc96yPm6li7zHrIQYfohGPdANmwR9opNNqYOo+LtsIYo
t3/cLp9YgAaiGdrAiKrbbEVkYH+zKzAHolf5mPBn+h3OElYfygESitWRBp2bwfOG
JwAYseTuorQHpyQpslGGcn9vcfnLhvLxa3DMrCAvSJb3SvHCyqahQz0KR0IPcu+V
LW3icaqlbJausGIGYqp8VSN6FJ0pgmYdbunBLYclv23VvjmVMl+xNJoaSFEUscmS
qA4CuYANhkWSANk8HI9rNbvmzuyWhSv7tUXY6UB67mHp4ypGcKYbXrjiKqahv6QL
UEb7S8FD7lDs75F2vMeO4O77i6joBs/L2E6WZJvSronzJCXL0IwmpYaOAsoFOf0e
GVsPBVKn+z4Bq0WA0+r7plfWofDbUGmx9Zun++rWhoDXrma+odubNlXjlRjlL3sC
AwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFHJbuqpyOO4lkCSllCL6CYjKiwr7MB0G
A1UdDgQWBBTW6y2dYf4ru3CILrgHsVmw9IMiajAOBgNVHQ8BAf8EBAMCAYYwPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovL2VjYS5oaW5ldC5uZXQvcmVwb3NpdG9yeS9D
UkwyL0NBLmNybDCBggYIKwYBBQUHAQEEdjB0MDsGCCsGAQUFBzAChi9odHRwOi8v
ZWNhLmhpbmV0Lm5ldC9yZXBvc2l0b3J5L0NlcnRzL2VDQUcyLmNydDAlBggrBgEF
BQcwAYYpaHR0cDovL29jc3AuZWNhLmhpbmV0Lm5ldC9PQlNQL29jc3BHMnNoYTIw
EgYDVR0TAQH/BAgwBgEB/wIBADAiBgNVHSAEGzAZMA0GCysGAQQBgbcjZAADMAgG
BmeBDAECAjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcN
AQELBQADggIBAEyrsJ9vUi6nEfwO0vgAoFefXpCRF+uDsmG/8F6OV9VRnbtzBwaz
HbxVmaBvDRVofLfoXWr+Nd8dd3BXVUNxemNrkZa8Hdgdv4s8yFbRs0W6fRTWkhCc
c39RpQtSeV7kyxCPlrMTYRSqCA9F+FcDMLXJIzZrzl7Tn6guIyqcfZv6sRN7CbbT
rYKSc0JX4t26WGFun2zLjzH8kxlTZ457TE4yyjlloSZdgiWL6Hz7l+nbTe6WqPVV
m4am2AAmaQaLGncsGLasl7PIHx9Nc4sy7KdOMTc5r0BPCGhAiJ6ueQ6aVd49pra7
BDIqFMA7Myy4pXRYfqFnjq9RuROWYiIluzLNUSxlaFtTMUVQnWjJxnlXlBDLX9L4
OAxTOvdbtcNNSlGK+WlcWiYdTOWF4HTu5pvdUn/+8yVE4E7MPb0vGuxv3SllQG6J
tVPuHkX6BGqRXHo253gY77HZU0g3g9qVs9UaZjWS5UTcqdgLmmOQnH7USaJ9/4rX
Ru/P8IWMPG2s6tvldRVQV5xfq2lPQ4y53ytVd0+/lp0L743+lAjnOw0I8t9QxP6c
2ti+oo43rxM8YE3etVLQBeWsmJc00GOWa/XmFACsy8Lkctx0QScAAYwCfB2accfx
j9hEXlc6MAeVUVp04YJx4dtjoIFTPIl/MFX+FkxMq4Fs6k+mxSm7tNvv
-----END CERTIFICATE-----

subject=/C=TW/O=Chunghwa Telecom Co., Ltd./CN=ePKI Root Certification Authority - G2
issuer=/C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority
-----BEGIN CERTIFICATE-----
MIIHeDCCBWCgAwIBAgIQO+7gkY6IhqlGD+iukQycujANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJUVzEjMCEGA1UECgwaQ2hlbmdod2EgVGVsZWNvbSBDby4sIEx0
```

複製貼上的憑證串鍊內容

- 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鍊。
- 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 -TLSv1 -TLSv1.1
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
SSLHonorCipherOrder on

SSLCertificateFile "/export/httpd-2.    /conf/sslcerts/server.crt"
SSLCertificateKeyFile "/export/httpd-2.    /conf/sslcerts/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、TLS 1.0 和 TLS 1.1

- 修改 SSL 設定檔(一般為 httpd-ssl.conf)，先找到 SSLProtocol 參數後，改為“SSLProtocol All -SSLv2 -SSLv3 –TLSv1 –TLSv1.1”，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 -TLSv1 -TLSv1.1

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite EECDH+AES128:EECDH+AES256:EECDH+CAMELLIA:!ECDSA:!MD5
```