# 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



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。**
- 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 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
```

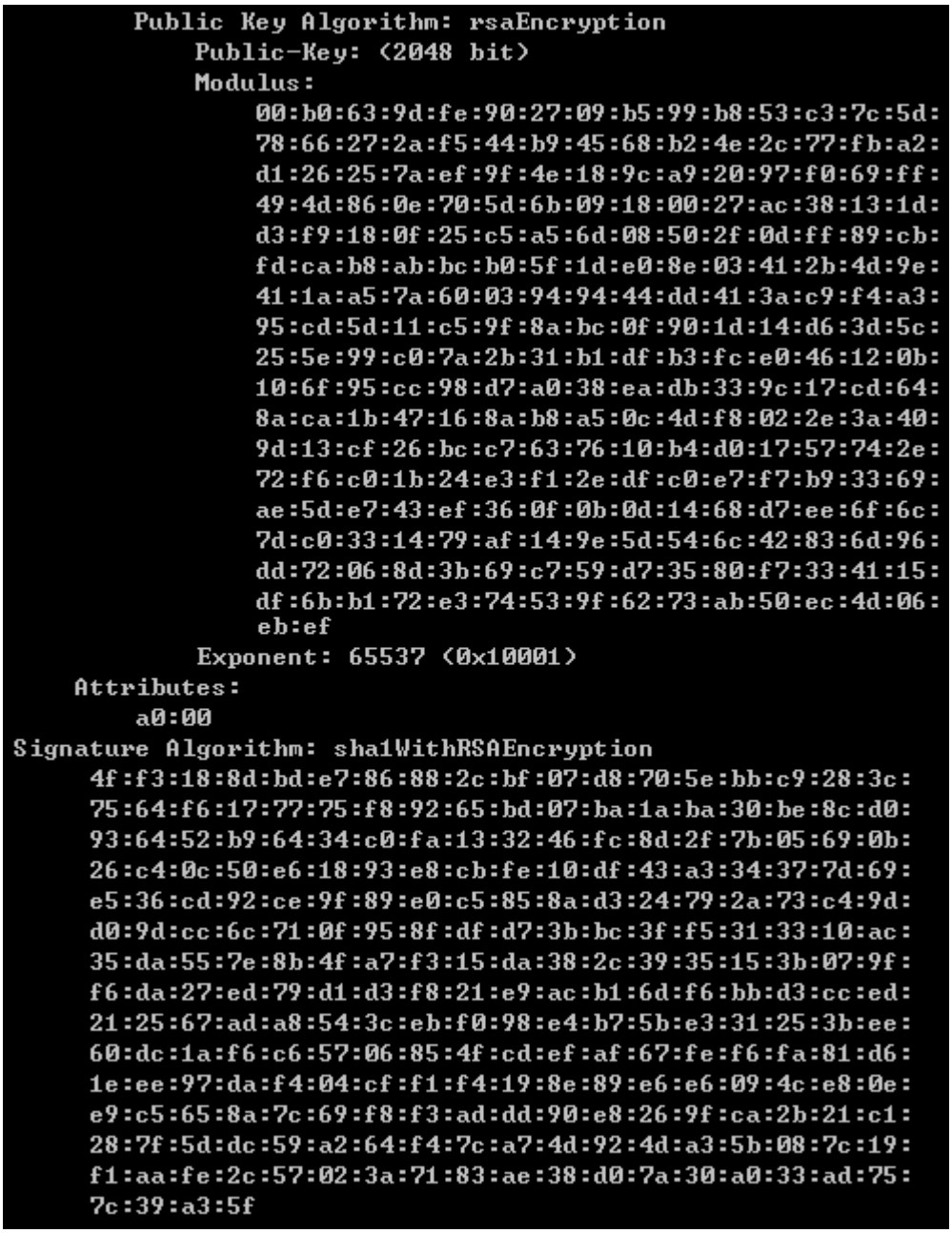
```
Email Address []:test@test.com.tw

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 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 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)。

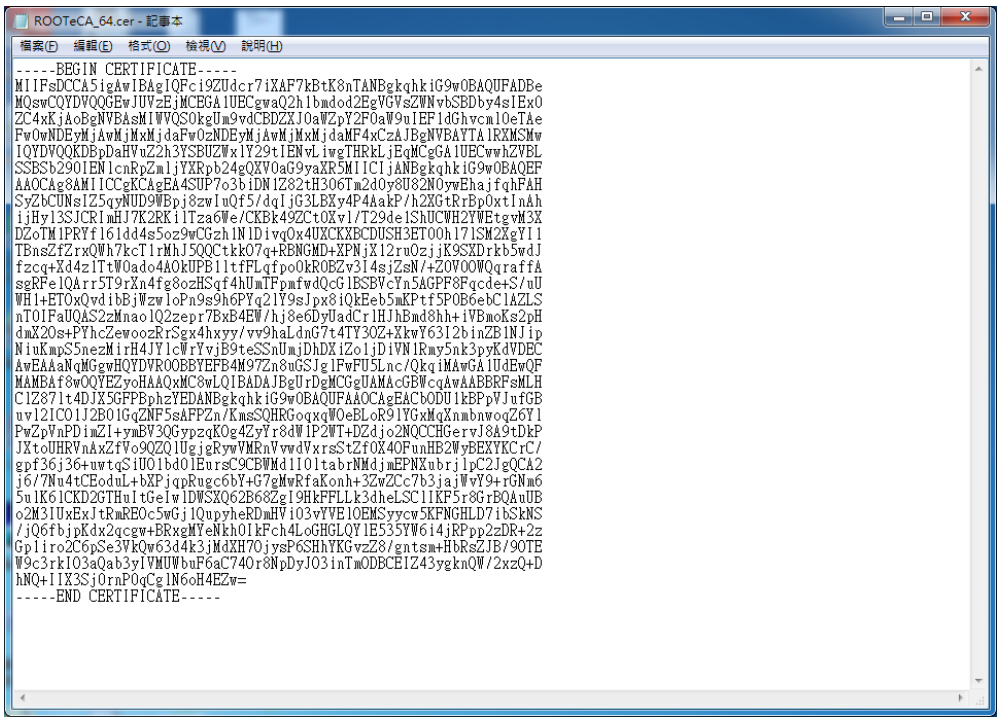
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。

(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

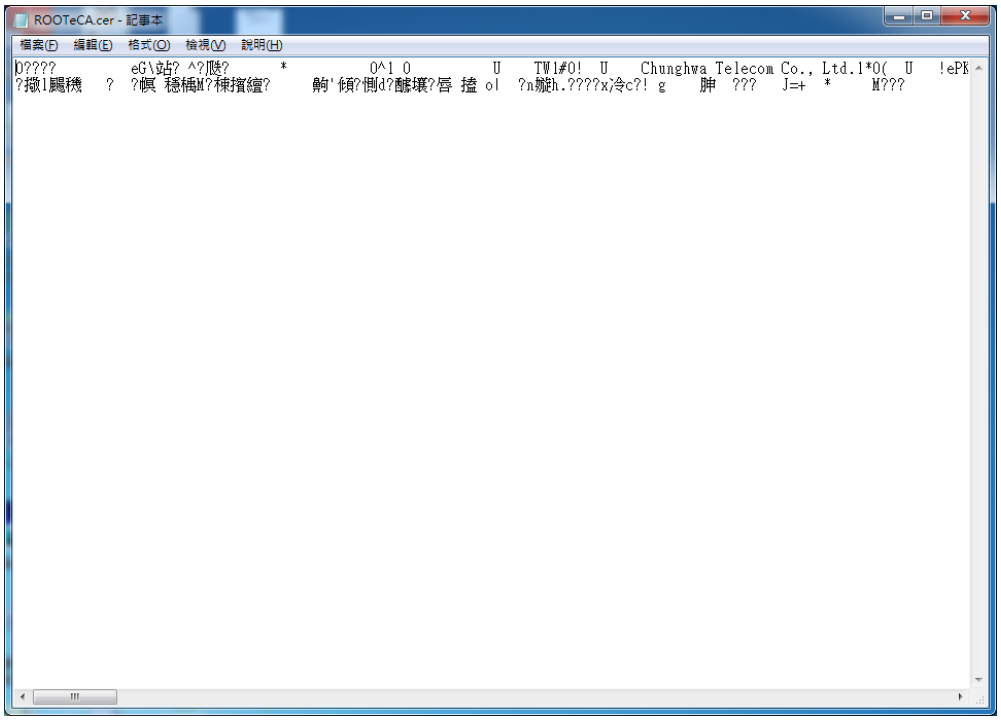
**$** openssl x509 -in server.cer -inform DER -out server.crt。

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：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 EECDH+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 >= **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
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。

# Windows Apache SSL 憑證請求檔製作手冊

一、產生憑證請求檔

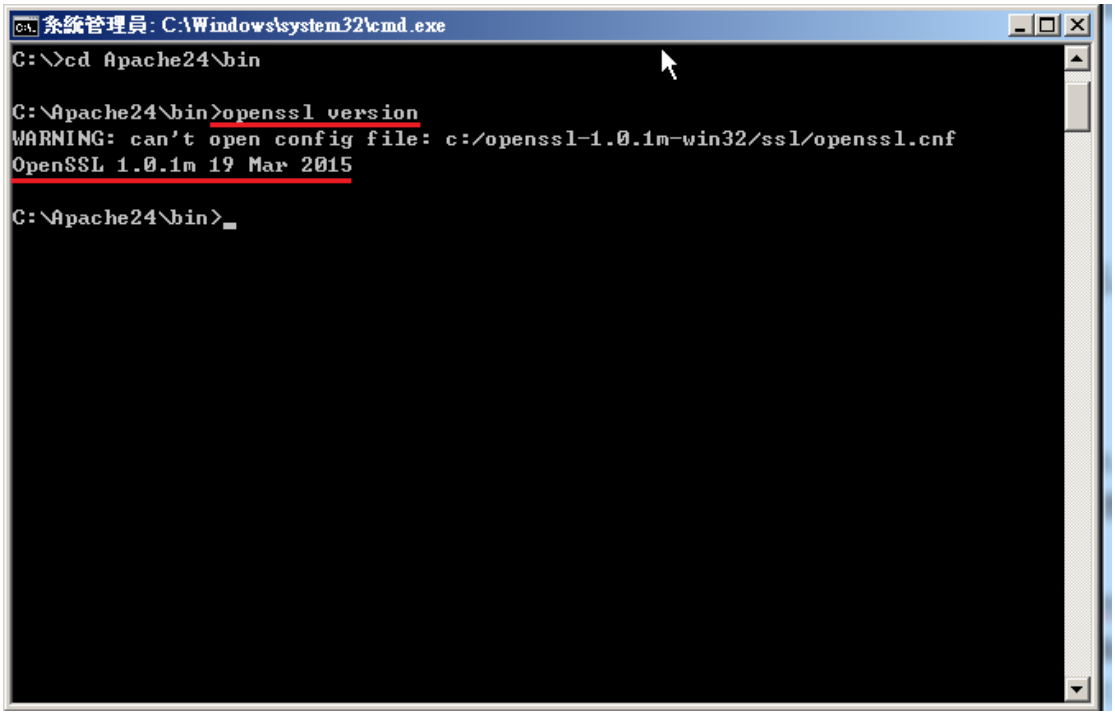
(1) 產生憑證請求檔（Certificate Signing Request file,簡稱 CSR 檔）需使用 OpenSSL 工具，此工具通常安裝在 <apache 安裝目錄>/bin 目錄下，會包含一個 openssl.exe 檔案。

(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

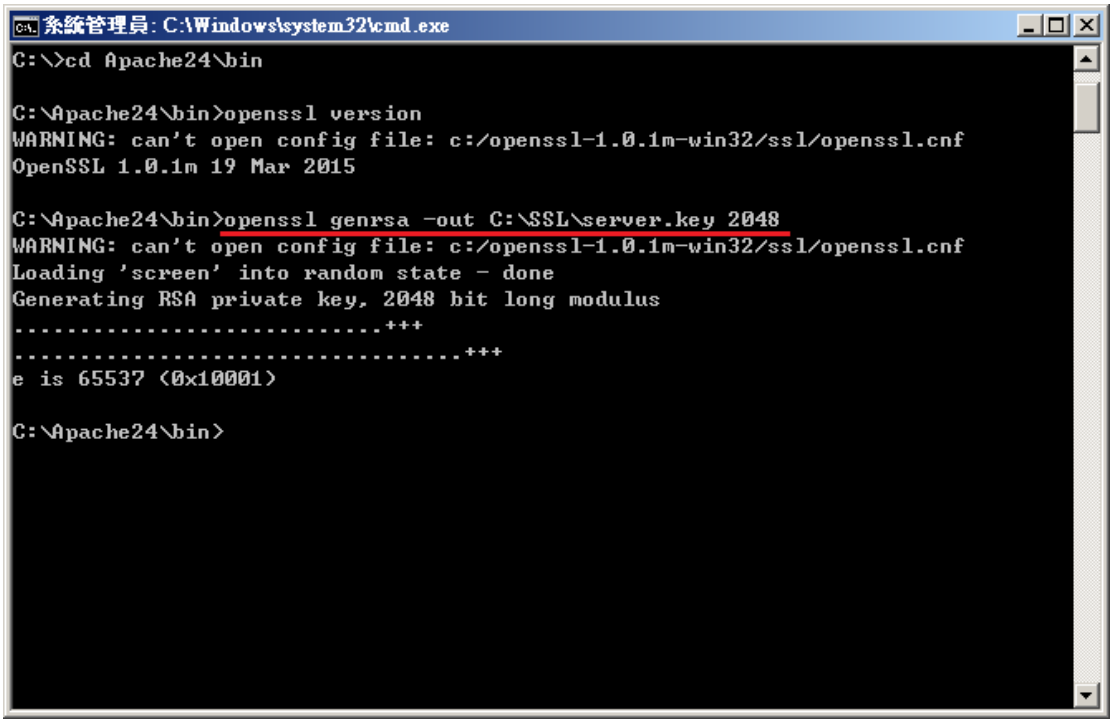
修復版本：1.0.1g / 1.0.2-beta2 以後




(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。**
- 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。

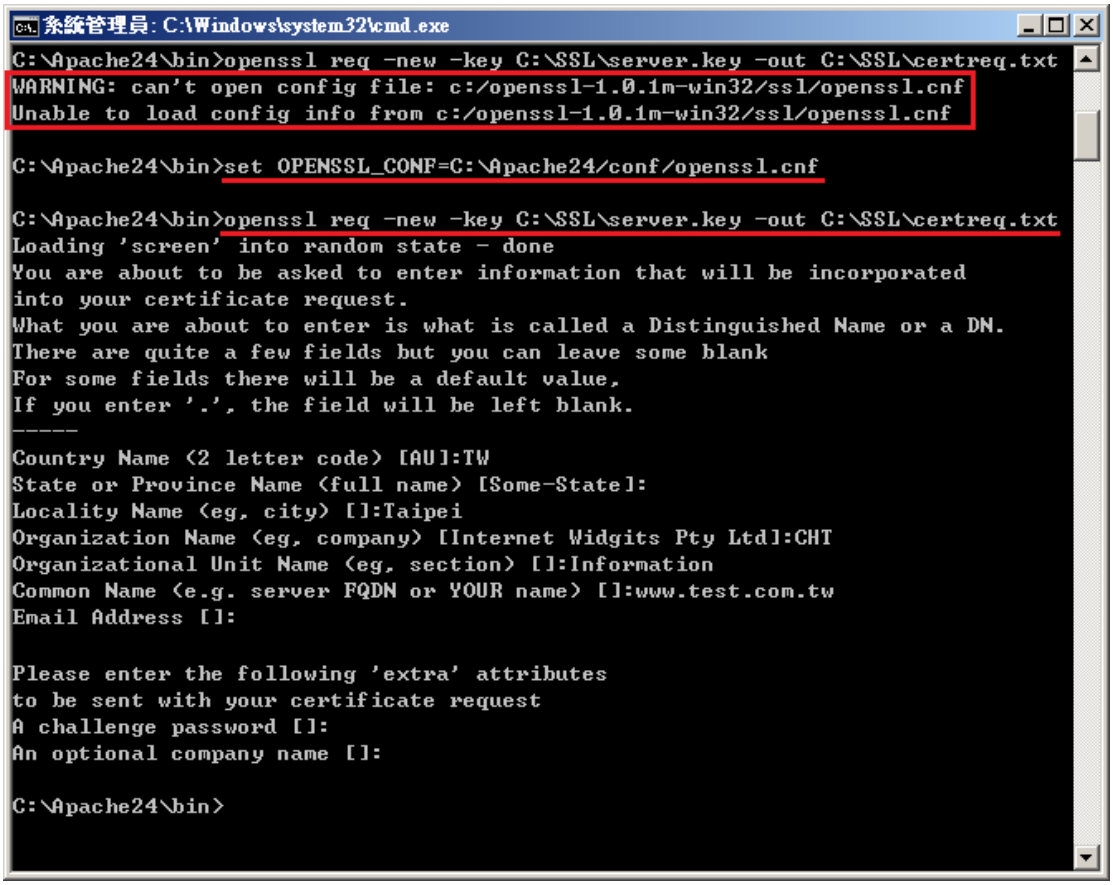
Country Name：TW
State or Province Name：不需輸入，按 enter 鍵略過
Locality Name：城市(如：Taipei)
Organization Name：組織名稱(如：CHT)
Organizational Unit Name：單位名稱(如:Information)

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




(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 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 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)。

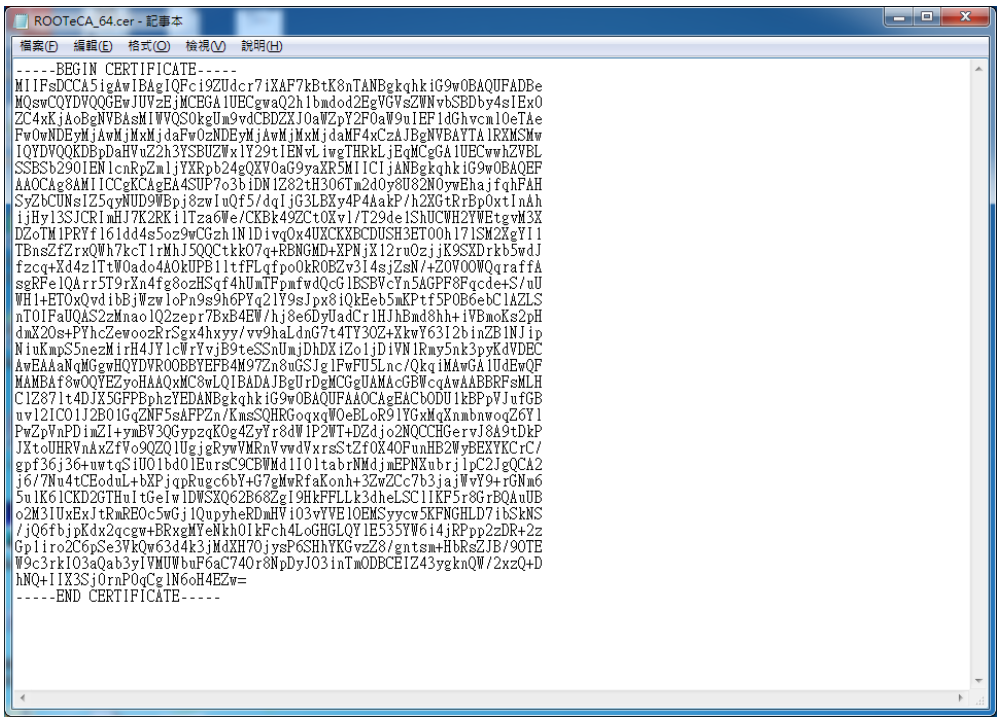
註：以下步驟假設您下載之 SSL 憑證之檔名已經改名為 server.cer，如果您並非使用這個檔名，請自行調整下面的步驟內容。

(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

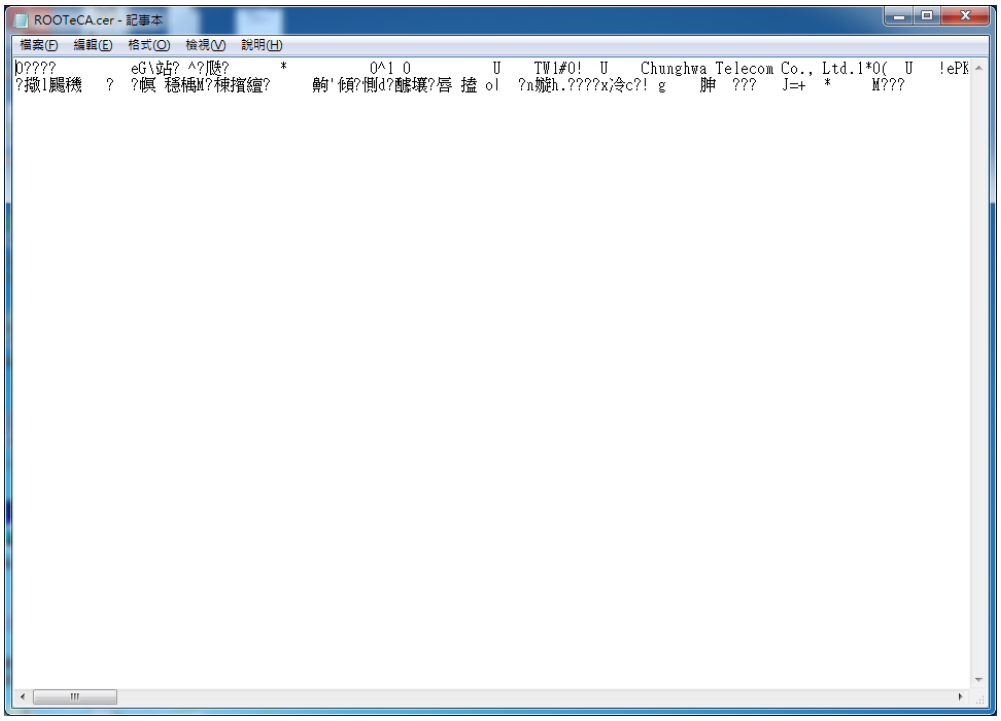
**$** openssl x509 -in server.cer -inform DER -out server.crt。

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：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 EECDH+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 >= **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  AAOCAQ8AMIIBCgKCAQEA36nu2MtLzMzB1Of7lCqnV2VC/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 GTAXMBUGB2CGdgFkAgExCgYIYIZ2AWQDAwEwYgGA1UdHwSBgDB+MD2gO6A5hjdo
21 dHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9HQ0E0L0NSTDIvQ1JMXzAw
22 MDEuY3JsMD2gO6A5hjdodHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9H
23 Q0E0L0NSTDIvY29tcGxldGUuY3JsMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggr
24 BgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAs71WC1KbhEmLBKu5HmUpHARv5lVa
25 rGusMOPNlBiKwLnfIP9WgcEzwInHdlC8YYEzWYM5K6qagP1spWhzA4rGIg4660ZO
26 z91Sk6sqE1hhYza/BnYlpvz63y8XjCUAOw0WWpbKpCJWGeuTg7FaN2ZpQs4POMbU
27 36aernb1KLTIFOQUFmfklmUiHNKe3+g03xTINzyZ+lJCRtk6frG1CyqqO7h0d2Zc
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。

```
iHgCOkChSiqpSJL5/42dl5yYc/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/
MQswCQYDVQQGEwJUVzEwMC4GA1UECgwnR292ZXJubWVudCBSb290IENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5MB4XDTEzMDEzMTAzMjIzNFoXDTMzMDEzMTAzMjIzNFow
RDELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCeihjOaUv+mZojEhMB8GA1UECwwY5pS/
5bqc5oaR6K2J566h55CG5Lit5b+DMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAtX7xPZUtp5iBGQvqYghJUoLeyCJJoaTcc1bcOGHij64WUBYpDu8KKEQK
R1y3zjcDXrLcZX483tmNs92DXSNuBH1x+we1aFyuLpKQVCji97ys3KeMxAEcaXqo
8cZu8nY3g//zkvX80G4RoCyDR86Z420R3mb0GlVw/9TEK8+oduZqAArEdfionpbE
K5zZ/8qaaHafgqMBQGuzfccDKLoWRcTzu3S0IvOpVU6pcB0rJOtc4F7c16tQdXfo
a8sjfcveKKbUQF6AklwugRufHdLqEVpOiGRcDPaHtT6SHJ7D/t+A/rAXMPidcksQ
rea/E+5+lehqEMHSA/gSLa9Ph+/gDQIDAQABo4IBIDCCARwwHwYDVR0jBBgwFoAU
lWcd4Jx6LJzLxZjnHQcmKobsdM0wHQYDVR0OBBYEFNEYZ8NX/hKakWtfXzHqPsKE
n/u9MA4GA1UdDwEB/wQEAwIBBjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8vZ3Jj
YS5uYXQuZ292LnR3L3JlcG9zaXRvcnkvQ1JMMi9DQS5jcmwwVgYIKwYBBQUHAQEE
SjBIMEYGCCsGAQUFBzAChjpodHRwOi8vZ3JjYS5uYXQuZ292LnR3L3JlcG9zaXRv
cnkvQ2VydHMvSXNzdWVkVG9UaGlzQ0EucDdiMBIGA1UdEwEB/wQIMAYBAf8CAQAw
HgYDVR0gBBcwFTAJBgdghnZlAAMDMAgGBmeBDAECAjANBgkqhkiG9w0BAQsFAAOC
AgEAs3KvqDSIq6GERR/SonDfYnrpF/IdZLM9gBfsIIafNeeWjFCIuC5Ah7LEIhZY
PP/D8y00OCRlZ7GoY4JZIvTFA1fb2umEmKC/ssCwQdUxyd52JfbqBL5N0cP2eU1x
lZG8d1z8uIq7ItyfO5ML1eAboYMHsO7c10pLmtufZj8VZ4zp4DTRxVzROPKwlIbR
QSKNlymWgAop+Eg9b40lfBMBxFppb3R4IZpijCpy0RbPOzvtmDpen3WZmJ+vsCqc
08b8JqDeRG5zQI1sIeV15qqGZuV8oL5gFi4niltkLNS3fGYAr4+LXVojMWIO/Noe
Ji+i3AtfhnN/w3Ixzhxi39pN+hYzFGtsZNioUC2MQexFJS+AQ4s8D41cRCMwovfi
0erTbWKhTPoQXirUDV/ZSUjUlLDbXzdiUB+mxWd2k16HYcvMFUevxbNzJAxP355T
q9tliZpM/7MVq0/Bw4SGxxQRQF1uVQjMBtEsRYHKVZ1IBBJVOe8jZhc81Sw3jDmm
Ttyjx1o2m8VVImsiIP2iPI3hlw/UCwCGRg5xvqqW72w2niT9pXdvZowBVbhP24wt
umuA45M5h4UNZRNo4/NG3UwS9eLKtfB06YFf3DcBban/Drf8LX8OGvF++Im3SeGJ
6zhUlYOVJcTHpR6TToXoKzvuzegRL2vQ4k22B++JtOQgsAg=
-----END CERTIFICATE-----

subject=/C=TW/O=Government Root Certification Authority
issuer=/C=TW/CN=Government Root Certification Authority - G1.5
-----BEGIN CERTIFICATE-----
MIIGcTCCBFmgAwIBAgIRAKOUO28QJlHOulORI3SaKiowDQYJKoZIhvcNAQELBQAw
WjELMAkGA1UEBhMCVFcxEjAQBgNVBAoMCeihjOaUv+mZojE3MDUGA1UEAwwuR292
ZXJubWVudCBSb290IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzEuNTAeFw0x
NzA3MTkwMjUxNDhaFw0yMDA3MTkwMjUxNDhaMD8xCzAJBgNVBAYTAlRXMTAwLgYD
VQQKDCdHb3Zlcm5tZW50IFJvb3QgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwggIi
MA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC2/5c8gb4BWCQnr44BK9ZykjAy
```

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
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

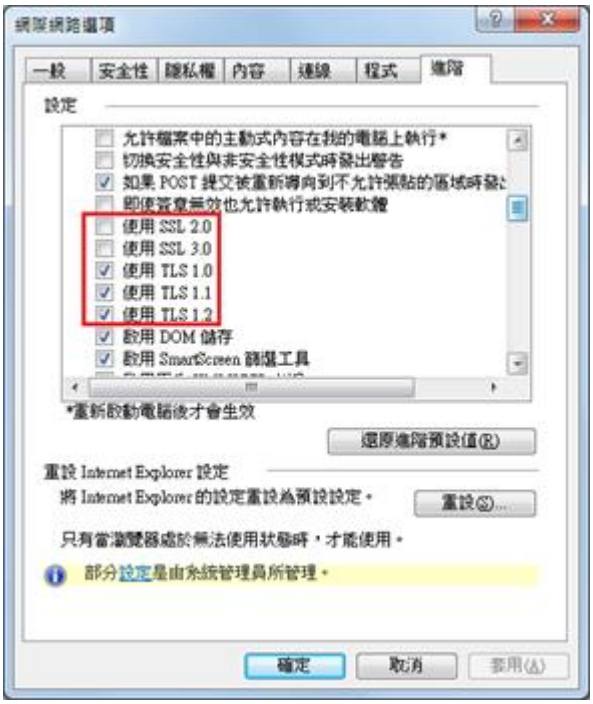
- OpenSSL 1.0.1j 版本有針對 POODLE 弱點進行修補，您可選擇同時更新 OpenSSL 版本與停用 SSLv3.0，或是直接停用 SSLv3.0。
- 先開啟 http.conf 或是 http-ssl.conf 檔案，並找到 “SSLProtocol all -SSLv2”，其意思為所有 SSL 通訊協定，扣除 SSLv2.0。因此，若要停用 SSLv3.0，只要將上述改為 “SSLProtocol all -SSLv2 -SSLv3”，重新啟動 Apache 即可。

```
#   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/sslv3/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）


網際網路選項
一般
安全性
隱私權
內容
連線
程式
進階
設定
允許檔案中的主動式內容在我的電腦上執行*
切換安全性與非安全性模式時發出警告
如果 POST 提交被重新導向到不允許張貼的區域時發出
即使簽章無效也允許執行或安裝軟體
使用 SSL 2.0
使用 SSL 3.0
使用 TLS 1.0
使用 TLS 1.1
使用 TLS 1.2
啟用 DOM 儲存
啟用 SmartScreen 篩選工具
*重新啟動電腦後才會生效
還原進階預設值(R)
重設 Internet Explorer 設定
將 Internet Explorer 的設定重設為預設設定。
重設(S)...
只有當瀏覽器處於無法使用狀態時，才能使用。
部分設定是由系統管理員所管理。
確定
取消
套用(A)