中華電信 HiPKI 憑證管理中心（OVTLSCA）

Apache SSL 憑證請求檔製作與憑證安裝手冊

本手冊適用於 Apache+mod_ssl 環境下之 SSL 伺服器軟體憑證安裝，Apache Server 可執行於 Unix like 的平台上(例如:Linux)或是 Windows 平台，請依照您的作業系統選擇適當的手冊參考。本手冊的安裝程序，已經在 Apache 2.4.12 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 憑證請求檔製作手冊

一、製作憑證請求檔

1. 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

2. 請執行以下指令來產生金鑰，金鑰會產生在當前的目錄下

   $ sudo 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。

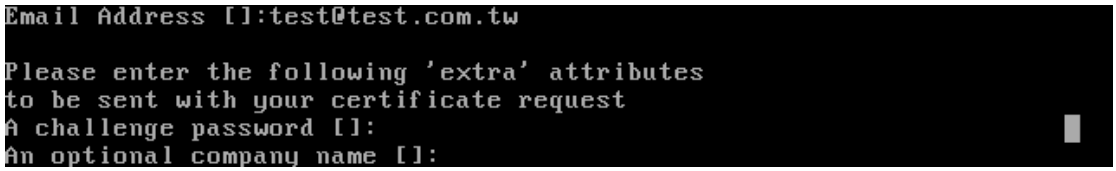
```
[root@Franklin bin]# openssl
OpenSSL> exit
[root@Franklin bin]# openssl genrsa -des3 -out server.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++++
.....................++++++
e is 65537 (0x10001)
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[root@Franklin bin]# _
```

3. 執行完畢後，會產生金鑰檔案，檔名為 server.key，請您將此檔案與密碼**備份或是妥善保存**。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，需要重新提出申請並廢止舊憑證。

4. 請執行以下指令，以產生憑證請求檔

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

```
[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
```



請先輸入剛才設定的私密金鑰密碼，接著依照畫面填入所需資料：

Country Name:	填入 TW
State or Province Name:	不需要填，按 Enter 跳過
Locality Name:	城市(ex: Taipei City)
Organization Name:	組織名稱(ex: Chunghwa Telecom Co., Ltd.)
Organization Unit Name:	單位名稱(ex: Information Department)
Common Name:	網站名稱(ex: www.test.com.tw)
Email Address:	可不填，按 Enter 跳過
A challenge password:	不需要填，按 Enter 跳過
An optional company name:	不需要填，按 Enter 跳過

二、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信公開金鑰基礎建設服務網站（https://chtca.hinet.net/）依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

補充說明 1: 中華電信公開金鑰基礎建設服務之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

Linux Apache 憑證安裝手冊

一、下載憑證串鏈，包含 3 張憑證，分別是(1) HiPKI Root CA - G1(ePKI Root 簽發給中華電信 HIPKI 憑證管理中心憑證)、(2)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(3)OV TLS CA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 HRCA 根憑證(檔名為 HRCA_b64.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。

   若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。

   HiPKI Root CA - G1(ePKI Root 簽發給中華電信 HIPKI 憑證管理中心憑證)**需另行至** https://eca.hinet.net/download/eCA1-to-HRCA1.crt **下載**

2. 從網站 https://chtca.hinet.net/index.html → 儲存庫 → Root CA 憑證、憑證廢止清冊及其相關資訊：

   根憑證：

   https://eca.hinet.net/repository-h/download/HRCA_b64.crt

   eCA-G1 簽發 HiPKI RCA-G1 交互憑證 (RSA 4096 w/SHA-256)

   從網站 https://chtca.hinet.net/index.html → 儲存庫 → 交互 CA 憑證、下屬 CA 憑證及其相關資訊：

   中繼憑證 1：

   https://eca.hinet.net/download/eCA1-to-HRCA1.crt

   HiPKI OV TLS CA-G1 憑證 (RSA 4096 w/SHA-256)

   中繼憑證 2：

   https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

   SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，進行 SSL 憑證下載。

   若您是中華電信之員工，負責管理單位之伺服器，請至 https://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

二、SSL 憑證安裝

1. 將 server.key、eCA1-to-HRCA1.crt、OVTLSCA1_b64.crt、SSL 伺服器憑證(檔名為 32 個英數字.cer)移到特定資料夾(ex: /etc/ssl/webssl/)，以方便管理
2. 修改 httpd-ssl.conf (檔案可能位置為<apache 安裝路徑>/conf/extra/httpd-ssl.conf)
3. command line 切換至特定資料夾(ex: /etc/ssl/webssl/)，將 eCA1-to-HRCA1.crt 併入 OVTLSCA1_b64.crt 憑證中。

   Windows 執行以下指令:

   type eCA1-to-HRCA1.crt >> OVTLSCA1_b64.crt

   Linux 執行以下指令:

   cat eCA1-to-HRCA1.crt >> OVTLSCA1_b64.crt
4. 修改以下三個參數並存檔

   SSLCertificateFile：**伺服器憑證**檔案路徑及檔案名稱

   SSLCertificateKeyFile：**私密金鑰**檔案路徑及檔案名稱

   SSLCertificateChainFile：**中繼憑證**檔案路徑及檔案名稱 (步驟 3 所產生的 OVTLSCA1_b64.crt)

   ※ **請注意這個 SSLCertificateKeyFile 所指向的金鑰必須是當初您用來產生憑證請求檔(CSR 檔)的同一個金鑰，否則將無法成功建立 SSL。**
5. 重新啟動 Apache

   /usr/local/apache/bin/apachectl stop

   /usr/local/apache/bin/apachectl start
6. 成功後，請以 https 連線試試加密通道。

   ※ **依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。**

   ※ **與您系統連線的 Client 端(還沒信賴 HRCA 的 Server、裝置或 Browser)需要安裝 HRCA 根憑證。**

   Android：請升級至最新版，推薦使用 Chrome，並開啟自動更新

   iOS：請升級至最新版

   或是 Server 端改安裝以下憑證鏈

   根憑證：

   https://eca.hinet.net/download/ROOTeCA_64.crt

   中繼憑證 1：

   https://eca.hinet.net/download/eCA1-to-HRCA1.crt

   中繼憑證 2：

   https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

三、安裝 SSL 安全認證標章

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

Windows Apache 憑證請求檔製作手冊

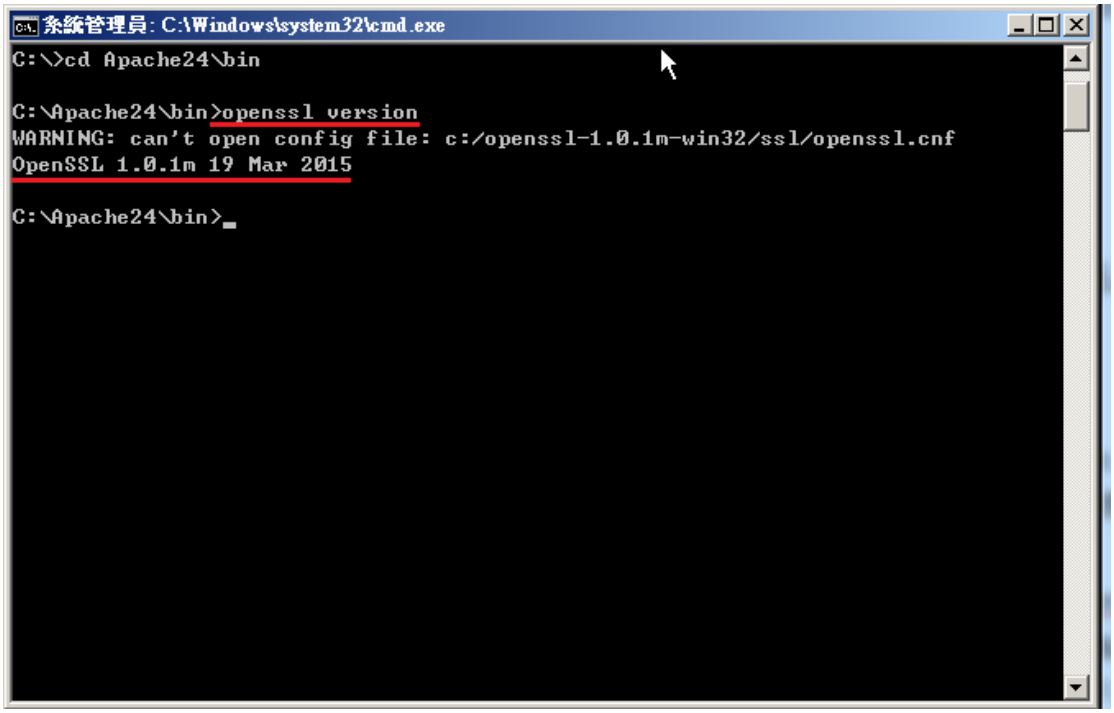
一、製作憑證請求檔

1. 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



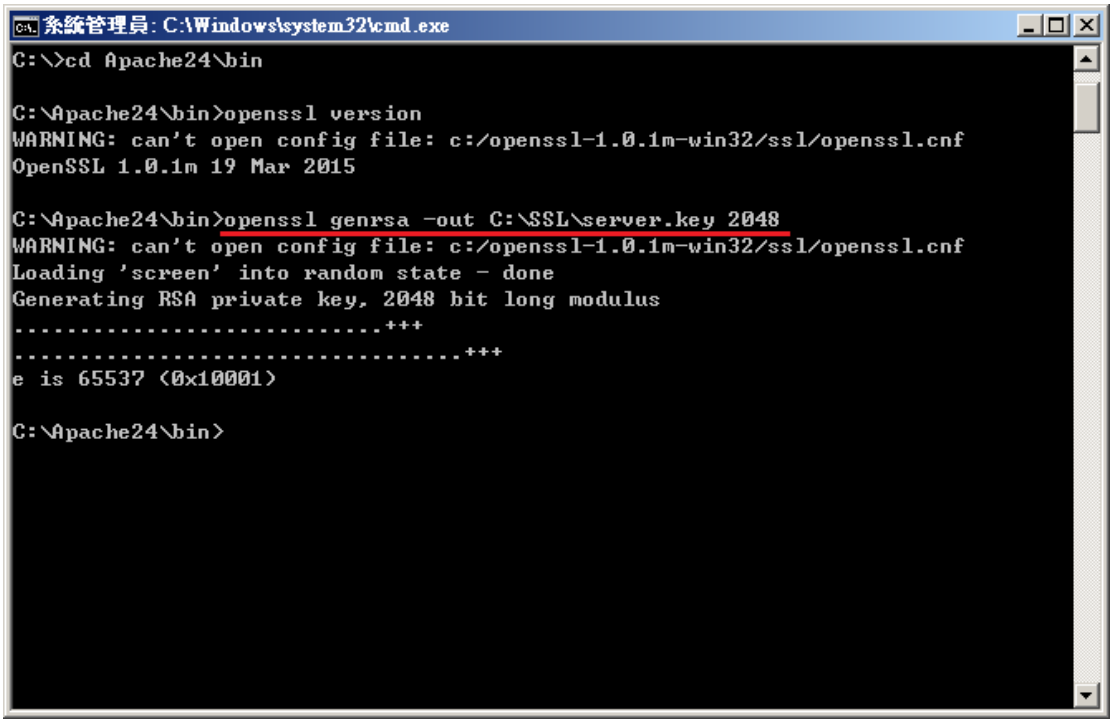
2. 請執行以下指令來產生金鑰，金鑰會產生在當前的目錄下

   $ 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。

   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**)



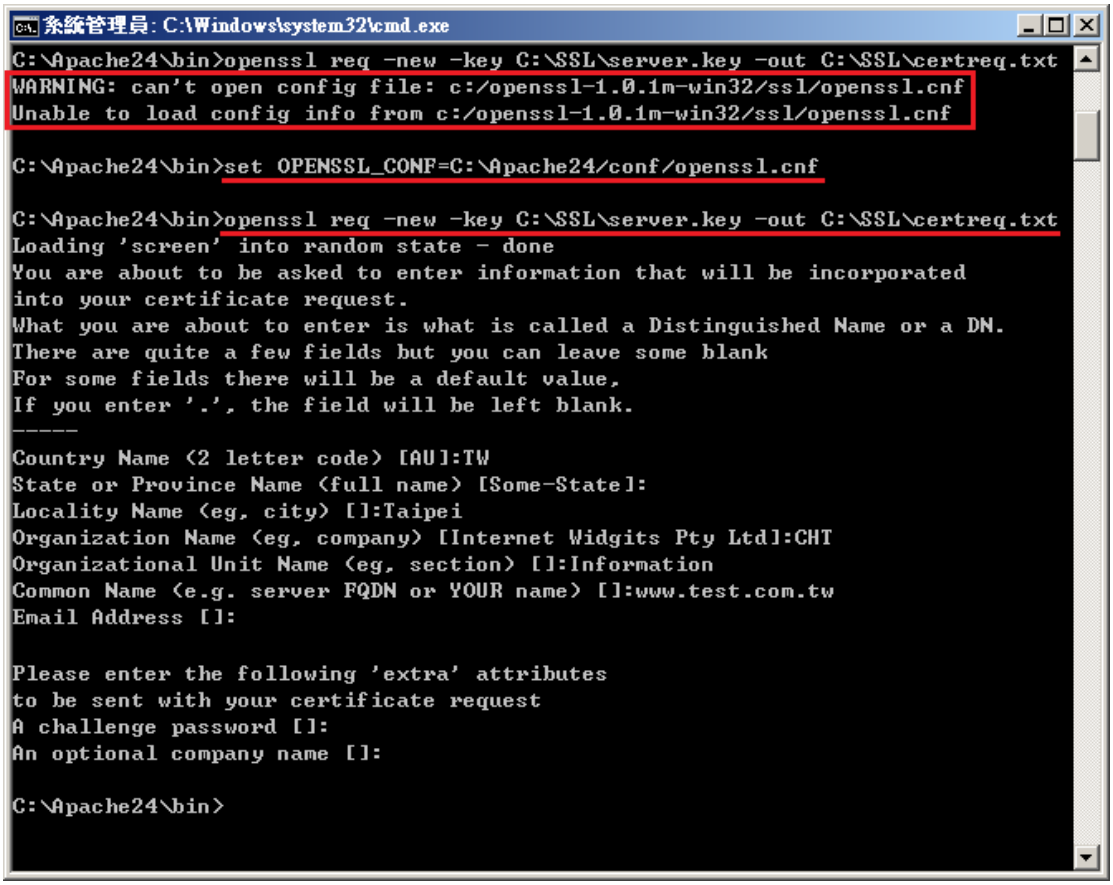
3. 執行完畢後，會產生金鑰檔案，檔名為 server.key，請您將此檔案與密碼**備份或是妥善保存**。若是在提出憑證申請後，金鑰遺失，核發下來的憑證將會無法使用，需要重新提出申請並廢止舊憑證。

4. 請執行以下指令，以產生憑證請求檔

請先找出 Apache 安裝目錄下的 openssl.cnf

$ set OPENSSL_CONF=<openssl.cnf 所在路徑>

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



依照畫面填入所需資料：

Country Name:	填入 TW
State or Province Name:	不需要填，按 Enter 跳過
Locality Name:	城市(ex: Taipei City)
Organization Name:	組織名稱(ex: Chunghwa Telecom Co., Ltd.)
Organization Unit Name:	單位名稱(ex: Information Department)
Common Name:	網域名稱(ex: www.test.com.tw)
Email Address:	可不填，按 Enter 跳過
A challenge password:	不需要填，按 Enter 跳過
An optional company name:	不需要填，按 Enter 跳過

二、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信公開金鑰基礎建設服務網站（https://chtca.hinet.net/）依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

補充說明 1: 中華電信公開金鑰基礎建設服務之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

Windows Apache 憑證安裝手冊

一、下載憑證串鏈，包含 3 張憑證，分別是(1)HRCA 根憑證(HiPKI Root CA 憑證，也就是中華電信 HIPKI 憑證管理中心自簽憑證)、(2)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(3)OV TLS CA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 HRCA 根憑證(檔名為 HRCA_b64.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。

   若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。

   HiPKI Root CA - G1(ePKI Root 簽發給中華電信 HIPKI 憑證管理中心憑證)需另行至 https://eca.hinet.net/download/eCA1-to-HRCA1.crt 下載

2. 從網站 https://chtca.hinet.net/index.html → 儲存庫 → Root CA 憑證、憑證廢止清冊及其相關資訊：

   根憑證：

   https://eca.hinet.net/repository-h/download/HRCA_b64.crt

   eCA-G1 簽發 HiPKI RCA-G1 交互憑證 (RSA 4096 w/SHA-256)

   從網站 https://chtca.hinet.net/index.html → 儲存庫 → 交互 CA 憑證、下屬 CA 憑證及其相關資訊：

   中繼憑證 1：

   https://eca.hinet.net/download/eCA1-to-HRCA1.crt

   HiPKI OV TLS CA-G1 憑證 (RSA 4096 w/SHA-256)

   中繼憑證 2：

   https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

   SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，進行 SSL 憑證下載。

   若您是中華電信之員工，負責管理單位之伺服器，請至 https://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

二、SSL 憑證安裝

1. 將 server.key、eCA1-to-HRCA1.crt、OVTLSCA1_b64.crt、SSL 伺服器憑證(檔名為 32 個英數字.cer)移到特定資料夾(ex: C:\SSL\)，以方便管理
2. 修改 httpd-ssl.conf (檔案可能位置為 <apache 安裝路徑>/conf/extra/httpd-ssl.conf)
3. command line 切換至特定資料夾(ex: /etc/ssl/webssl/)，將 eCA1-to-HRCA1.crt 併入 OVTLSCA1_b64.crt 憑證中。

   Windows 執行以下指令:

   type eCA1-to-HRCA1.crt >> OVTLSCA1_b64.crt

   Linux 執行以下指令:

   cat eCA1-to-HRCA1.crt >> OVTLSCA1_b64.crt
4. 修改以下三個參數並存檔

   SSLCertificateFile：伺服器憑證檔案路徑及檔案名稱

   SSLCertificateKeyFile：私密金鑰檔案路徑及檔案名稱

   SSLCertificateChainFile：中繼憑證檔案路徑及檔案名稱 (步驟 3 所產生的 OVTLSCA1_b64.crt)

   ※ **請注意這個 SSLCertificateKeyFile 所指向的金鑰必須是當初您用來產生憑證請求檔(CSR 檔)的同一個金鑰，否則將無法成功建立 SSL。**

5. 重新啟動 Apache
6. 成功後，請以 https 連線試試加密通道。

※ **依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。**

※ **與您系統連線的 Client 端(還沒信賴 HRCA 的 Server、裝置或 Browser)需要安裝 HRCA 根憑證。**

Android：請升級至最新版，推薦使用 Chrome，並開啟自動更新

iOS：請升級至最新版

或是 Server 端改安裝以下憑證鏈

根憑證：

https://eca.hinet.net/download/ROOTeCA_64.crt

中繼憑證 1：

https://eca.hinet.net/download/eCA1-to-HRCA1.crt

中繼憑證 2：

https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

三、安裝 SSL 安全認證標章

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

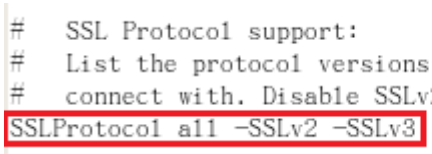
請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

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。
- OpenSSL 於 0.9.7 版開始支援 AES Cipher Suites，請透過以下指令檢查 OpenSSL 版本是否高於 0.9.7「***openssl version***」。

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。



- 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。

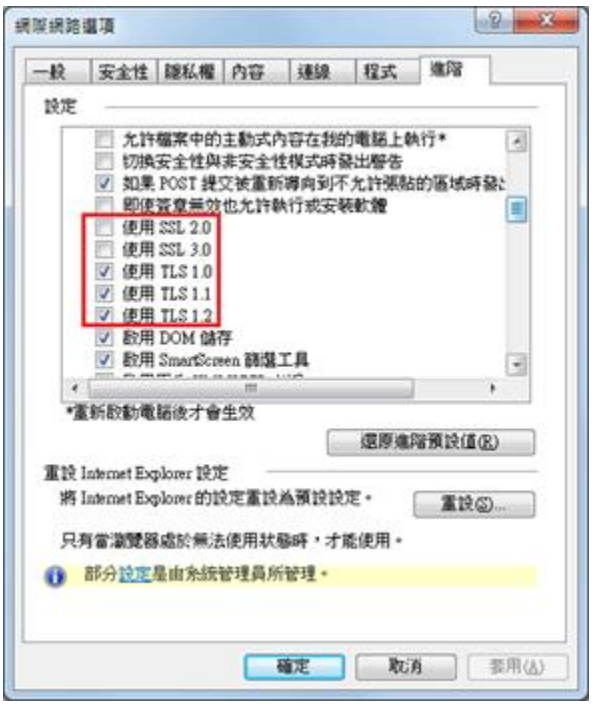
註 1:例如行政院國家資通安全會報技服中心網頁 http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh 有介紹兩種檢測伺服器端 SSL 協定的工具：(1) TestSSLServer（http://www.bolet.org/TestSSLServer/） (2) QUALYS SSL LABS SSL Server Test 檢測工具(https://www.ssllabs.com/ssltest/index.html, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定，因 2014 年 10 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 最新協定。

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 I.E.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
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)