

CSR 生成與憑證安裝指南 適用於 Apache

網路中文

网路中文

Net-Chinese

Net-Chinesisch

Net-chinois

Net-chino

Нетто-китайски

ネット-チャイニーズ

넷 - 중국

ةين يصل ا يفاص



目錄

Chapter 1 確認 Apache 版本與配置檔

- 1-1 | Apache 簡介4
- 1-2 | 查詢 Apache 的版本4
- 1-3 | 查看您的 httpd.conf 設定檔4
- 1-4 | 如果您有使用虛擬站台 <VirtualHost> 請一併檢查5
- 1-5 | SSL 相關路徑資訊的關鍵字5
- 1-6 | 如果您需要尋求協助...5
- 1-7 | 設定完成後需要重啟伺服器5

Chapter 2 產生私密金鑰與憑證請求檔 (CSR)

- 2-1 | 取得 OpenSSL.....6
- 2-2 | 使用 OpenSSL 產生私密金鑰與憑證請求檔6
- 2-3 | 查看 CSR 與 KEY.....7

Chapter 3 遞交資料與驗證

- 3-1 | 至網路中文遞交 CSR 文件以申請憑證8
- 3-2 | 進行域名驗證13
- 3-3 | 進行驗證方式的更換19
- 3-4 | 組織驗證與電話驗證 (OV/EV 限定).....20

Chapter 4 取得憑證

- 4-1 | 取得憑證22

Chapter 5 安裝憑證

- 5-1 | 查找憑證所在位置 (Linux 版 Apache).....24
- 5-2 | 查找憑證所在位置 (Windows 版 Apache).....25

附錄 A：Apache 發行版預設框架26

附錄 B：將憑證合併成集成 Bundle 檔案29

附錄 C：各品牌發行之中繼憑證 / 根憑證下載來源30

附錄 D：將憑證轉換為 PFX 格式或將 PFX 格式的憑證解離31

附錄 E：於 Windows 上安裝 OpenSSL.....32

Chapter 1 確認 Apache 版本與配置檔

1-1 | Apache 簡介

Apache HTTP Server(簡稱 Apache) 是 Apache 軟體基金會的一個開放原碼的網頁伺服器軟體，可以在大多數的作業系統中運行，由於跨平台和安全性，被廣泛的使用，是最流行的網頁伺服器之一。

我該如何查詢我的配置

由於 Apache 可在多數的作業系統中運行，尤其是 UNIX 與 Linux 作業系統，因為開源的特性，使得 Linux 共有許多種的版本與分支，這也使得 Apache 的配置會隨著版本與分支而有所不同，而 Apache 的安裝檔來源又分為下列兩種。

- 使用源碼包以進行安裝。
- 使用軟體包管理工具進行安裝 (CentOS/RHEL/Fedora 使用 Yum、Ubuntu 使用 apt-get 方式等等)

除了 Linux 分支不同以外，這兩種不同的安裝方式所產生的配置上也會有所不同，您可以在附錄 A 依照您的作業系統來查看您的 Apache 配置。另外，如果您的預設配置並沒有 SSL Config 相關的配置檔的話，您可能需要額外加裝 mod_ssl 模組來擴充您的 Apache 功能，使其支援 SSL。

請注意：

雖然主要的 Apache HTTP Server 文件中的範例假定您使用的是從 apache.org 分發的標準文件配置，但許多第三方的分發伺服器會更改配置以符合本地策略，這可能會使遵循範例和查詢各種重要的文件變得困難。

1-2 | 查詢 Apache 的版本

您可以使用下列的指令碼來查詢目前您所使用的 Apache 版本，可以幫助您判斷。

- **Windows :** httpd -v
- **Linux :** apachectl -v

1-3 | 查看您的 httpd.conf 設定檔

請依照本說明書的附錄 A 查找您的 httpd.conf 檔案 (Debian 及 Ubuntu 用戶請搜尋 apache2.conf)，在這裡是 Apache 的總設定檔，如果您安裝的 Apache 是有 SSL_Config 設定檔的，請依附錄查詢 SSL_Config 的位置找到相關設定檔。若您的 Apache 是沒有 SSL_Config 的，則在 httpd.conf 設定檔中查詢附加模組設定，通常可能會在 `<IfModule></IfModule>` 之中，如下範例：

```
<IfModule>
Include conf/ssl.conf
</IfModule>
```

這樣，您可以在您的 conf 資料夾下找到您 SSL 的 conf 設定檔。

另外，您必須在 Listen 中再加入 Port 443 的開啟，這個 Port 是為了 SSL 安全連線通道開的。

例如：Listen 443

如果您的相關設定前面有加上 "#" 代表註解，需要取消掉才能使設定正常運作。

1-4 | 如果您有使用虛擬站台 <VirtualHost> 請一併檢查

有時候，為了業務需要，特定客戶會使用虛擬站台 (VirtualHost)，這是為了能讓一台主機上能夠運行多個網站，當您找不到 SSL 相關設定時，不妨來這裡看看，也許相關設定值會寫在這裡，有關於虛擬站台的區塊通常如下顯示：

```
<VirtualHost xxx.xxx.xxx.xxx:443>
  ServerName www.mydomain.com
  DocumentRoot /xxx/xxx
  ServerAdmin admin@example.com
  ErrorLog /xxx/xxxx/logs/error_log
</VirtualHost>
```

在 <VirtualHost></VirtualHost> 的區塊中，如果有發現 SSL 設定相關的關鍵字，則代表這個虛擬站台擁有各別的 SSL 設定，相關的關鍵字可以在下一節發現，以下是將 SSL 設定檔寫在虛擬站台設定的例子：

```
<VirtualHost xxx.xxx.xxx.xxx:443>
  ServerAdmin admin@example.com
  DocumentRoot /var/www/
  ServerName www.mydomain.com
  ErrorLog /www/home/logs/error_log
  SSLEngine On
  SSLCertificateFile /etc/ssl/netc_com_tw.crt
  SSLCertificateKeyFile /etc/ssl/netc_com_tw.key
  SSLCertificateChainFile /etc/ssl/ca_bundle.crt
</VirtualHost>
```

1-5 | SSL 相關路徑資訊的關鍵字

本節說明 SSL 相關的關鍵字，有了以下關鍵敘述，您就可以掌握憑證粗略的放置位置。

SSLEngine On	用來表示啟用 SSL
SSLCertificateFile	用來表示網站憑證檔的放置路徑，例如：/etc/ssl/netc_com_tw.crt
SSLCertificateKeyFile	用來表示網站私密金鑰的放置路徑，例如：/etc/ssl/netc_com_tw.key
SSLCertificateChainFile	用來表示中繼憑證、根憑證等信任鏈，例如：/etc/ssl/ca_bundle.crt

1-6 | 如果您需要尋求協助...

由於 Apache 是一套開源的網頁伺服器軟體，針對不同的作業系統以及不同的分支，皆擁有不同的設定與路徑，所以實際的設定將會以您實際使用的作業系統為主 (包含各配置檔的路徑)。您可以在附錄 A 查找您作業系統的基本配置路徑。

如果您需要我們協助，請您提供下列資訊：

- 使用的作業系統 (包含版本)
- 主要配置檔 (httpd.conf/apache2.conf)
- SSL 相關配置檔 (httpd-ssl.conf/ssl.conf)
- 虛擬主機配置檔 (httpd-vhosts.conf)

1-7 | 設定完成後需要重啟伺服器

當您安裝完相關配置時，請使用啟動指令將伺服器重新啟動，相關的設定才會生效

Chapter 2 產生私密金鑰與憑證請求檔 (CSR)

2-1 | 取得 OpenSSL

在大多數的 Linux 環境中，作業系統已預裝了 OpenSSL(也包含 MacOS，因為它本來就是基於 UNIX 而開發的系統)，Windows 的使用者若要使用 OpenSSL，則必須安裝 Win32 包的 OpenSSL。Win32 版本的 OpenSSL 請查閱下方連結：

- Win32/Win64 OpenSSL 安裝檔：<https://slproweb.com/products/Win32OpenSSL.html>

如果 Linux 的使用者發現在系統上並沒有安裝，請使用作業系統的 yum(Fedora/CentOS/RHEL) 或是 apt-get(Debian/Ubuntu) 指令來取得並進行安裝，或是從 OpenSSL 的官方網站取得原始碼進行編譯。

- OpenSSL 官方網站：<http://www.openssl.org>

2-2 | 使用 OpenSSL 產生私密金鑰與憑證請求檔

通常，在使用 OpenSSL 來產生私密金鑰或憑證請求檔的環境下，都是使用命令列或是命令提示字元，也因此，在這裡的所有操作，全部都是輸入指令來完成產生的步驟，同時會帶入許多的參數。以下是產出的指令：

```
openssl req -new -newkey rsa:2048 -nodes -keyout name.key -out name.csr
```

指令參數說明

- **req** 用來做為對 OpenSSL 請求的參數
- **-new** 用來請求新的 csr 憑證請求檔
- **-newkey** 用來請求新的私密金鑰
- **rsa:2048** 指定請求的私密金鑰指定為使用 RSA 加密演算法，並將金鑰長度指定為 2048bit
- **-nodes** 不使用 DES 加密演算法對私密金鑰進行加密，若不加入此參數將會對金鑰加密 (不建議)
- **-keyout** 輸出私密金鑰名稱
- **-out** 輸出 CSR 憑證請求檔的名稱

在輸入上述指令後，會出來以下資訊，請依照相關指示輸入

- **Country NAME** 請使用符合 ISO3166 的規範輸入國名縮寫，如台灣請輸入 TW
- **State or Province Name** 請輸入完整的省 / 州名，勿使用縮寫，台灣的話請輸入 Taiwan
- **Locality Name** 請輸入城市名稱，勿使用縮寫，例如：Taipei City
- **Organization** 請輸入公司法定名稱，若名稱中有 & 等特殊符號，請使用 and 代替
- **Organization Unit Name** 部門或組織單位的名稱，如行銷部：Marketing Dept.
- **Common Name** 即網域名稱，請輸入 www.mydomain.com；如果您購買的是通用型憑證，則請輸入星號，例如：*.mydomain.com

或者，您可以使用另外一種方式，直接生成的時候就宣告包含下列資訊：

```
openssl req -new -newkey rsa:2048 -nodes -keyout name.key -out name.csr -subj "/C=TW/ST=Taiwan/L=Taipei City/O=Net-Chinese Co.,Ltd/OU=Product Dept./CN=www.net-chinese.com.tw"
```

指令參數說明

- **-subj** **CSR 附加主旨**
- **C** **國家名稱縮寫**
- **ST** **省 / 州**
- **L** **城市**
- **O** **組織名稱**
- **OU** **部門名稱**
- **CN** **此憑證請求要頒發憑證的主要域名，若為通用型請以 "*" 符號表示。**

請注意：

上述指令的 **[]**、**[/]** 及 **[=]** 符號，請勿省略。

接著，您就可以找尋您的 CSR 與私密金鑰，在您未指定輸出路徑的話，則應會在您的系統根目錄中取得。

2-3 | 查看 CSR 與 KEY

當您執行此操作後，您會得到一組 CSR 與私密金鑰，其編碼都為 PEM 格式編碼，您可以依照頭尾的標籤來判斷，判斷的準則您可以參考下列說明：

以標籤來判斷產出檔案內容	
CSR 憑證請求檔	-----BEGIN CERTIFICATE REQUEST----- -----END CERTIFICATE REQUEST-----
KEY 私密金鑰	-----BEGIN PRIVATE KEY----- -----END PRIVATE KEY-----
CRT 憑證檔案	-----BEGIN CERTIFICATE----- -----END CERTIFICATE-----

建議您在向網路中文提交資料時，請確認您提交的資料是 CSR 憑證請求檔，相關的文件透過文字編輯器查看標頭即可得知該文件是屬於何種文件。

貼心提醒：

您的私密金鑰為憑證配對重要憑據，請妥善留存，若遺失可能會造成憑證無法安裝配對及造成您的資安疑慮。

Chapter 3 遞交資料與驗證

3-1 | 至網路中文遞交 CSR 文件以申請憑證

當您取得 CSR 與私密金鑰時，這時候就必須登入網路中文網站以進行遞交憑證，本章節將教您如何遞件。

3-1-1 我該在哪裡找到我剛剛購買的憑證？

當您購買 SSL 之後，您可以在以下三種方式找到您剛才購買的憑證並進行遞交。

1. 透過待開通服務找到購買的商品

在「收合選單」中的「待開通服務」中找到剛才購買的憑證，並點選裡面有一個「點擊進行設定」的按鈕。

訂單編號	服務種類	產品名稱
1309643	域名加值服務	
1419992	SSL數位憑證	單域名專業!

2. 透過首頁的帳號點選「SSL 憑證管理」

當您在「收合選單」之外時，您可以點選購物車圖示旁邊的小人頭中的「SSL 憑證管理」，就能到達收合選單中的「SSL 憑證」，接著您就參考方法 3。

19 分27秒後登出 | netcpmnc | 0

網路中文

弱點掃描 | SSL憑證 | 雲端服務 | 品牌保護 | SEO服務 | 常見

帳戶管理
訂單管理
域名管理
主機空間管理
SSL憑證管理
價格一覽表
域名歸戶作業
登出

系統安全性升級公告

信箱驗證及密碼重設作業。
常見問題

晚上八點來電：02-2531-9696

3-1-3 檢查資訊並選擇伺服器與驗證方式

在您於上一個步驟點選「驗證 CSR」按鈕後，系統會反解並列出您的 CSR 詳細資訊，請注意域名或組織與其他資訊的內容是否正確，並依據您的伺服器選擇，以及選擇您所想要的驗證方式。

單域名專業型(銅牌級)(新申請) - www.net-chinese.com.tw

CSR詳細資訊 編輯

域名: www.net-chinese.com.tw
組織: Net-Chinese Co.,Ltd
組織部門: Product Dept.
地區: Taipei City
省或州: Taiwan
國家: TW

CSR文件下載

選擇網頁伺服器軟體與驗證方式:

選擇伺服器軟體

Apache + OpenSSL

選擇驗證方式

Email

選擇驗證的信箱地址

service@net-chinese.com.tw

填寫組織資訊(英文填寫):

*公司正式英文名稱

Email
CNAME
HTTPCSRHASH

目前，在 SSL 方面，提供三種域名驗證方式。

- **Email 驗證**：使用 Email 方式寄送帶有驗證碼的電子郵件，將驗證碼貼於指定網頁即完成驗證。
- **CNAME 驗證**：使用 DNS 管理功能新增相關 CNAME 值以進行驗證，使用此方式需擁有 DNS 實際控制權。
- **HTTPCSRHASH 驗證**：使用驗證檔方式將驗證檔放置網站主機指定路徑中，使用此方式需擁有主機實際控制權限，並且能上傳檔案至主機上。

驗證相關教學請參照：<https://www.net-chinese.com.tw/nc/index.php/MenuLink/Index/SSLValidation>

請注意：

1. 由於歐盟國家頒布了個人資料保護相關法規，您的信箱有可能將不會在 WHOIS 中被揭露，如果遇到這種情況，而您又擁有相同域名的電子郵件信箱，則您可以透過建立臨時性的管理員信箱以接收驗證信。
2. 使用 CNAME 驗證方式進行驗證時，請確定您有新增 DNS 記錄的權限，各家的 DNS 界面操作，請洽詢 DNS 服務代管業者。記錄的生效速度取決於 DNS 更新的速度。
3. HTTPCSRHASH 驗證不適用於通用型憑證與多域名型憑證中附掛域名的驗證。

選擇驗證的信箱地址

service@net-chinese.com.tw

service@net-chinese.com.tw
admin@www.net-chinese.com.tw
administrator@www.net-chinese.com.tw
hostmaster@www.net-chinese.com.tw
postmaster@www.net-chinese.com.tw
webmaster@www.net-chinese.com.tw
admin@net-chinese.com.tw
administrator@net-chinese.com.tw
hostmaster@net-chinese.com.tw
postmaster@net-chinese.com.tw
webmaster@net-chinese.com.tw

當您使用 Email 驗證時，卻發現無法使用 WHOIS 信箱時，如果您有建立與申請憑證時的主要域名相同域名信箱的權限時，這裡提供 5 個可以被用做 Email 信箱的管理員帳號，您可以依據您的需求來建立。

- admin
- administrator
- hostmaster
- postmaster
- webmaster

3-1-4 填寫組織相關資訊 (組織驗證 OV/ 延伸驗證 EV 必要)

當您購買的是屬於組織驗證 (OV) 型或是延伸驗證 (EV) 型的憑證，則發證機構將會對您的公司或組織進行必要的徵信與查核，為了審查順利，請盡可能的在此填寫的資訊與您公司的所登記設立的資訊相同，以免造成審查不通過及延誤查證。


填寫組織資訊(英文填寫):

*公司正式英文名稱

Net-Chinese Co.,Ltd

公司統一編號

70535344

經營別名(DBA) 

鄧白氏環球編碼(D-U-N-S) 

65-771-2279

部門名稱

Product Dept.

*公司主要電話

+886-2-25319696

傳真

886225319522

請務必輸入國碼、區碼與電話號碼

*所在地址

12F.,No.46,Zhongshan N. Rd, Sec. 2, Zhongshan Dist

*城市或所在區域

Taipei City

*省或州

Taiwan

*國家

台灣

*郵遞區號

10448

上述的資訊，有紅色星號的欄位為必要填寫的欄位，且建議使用英文填寫相關資訊，鄧白氏環球編碼 (DUNS) 為第三方的公證機構，發證機構會優先使用這資料庫的資訊進行查核，如果您知道您的鄧白氏環球編碼，請在此填上。傳真欄位現階段不支援國際碼【+】符號與連字號【-】號，如果您填寫此欄位，必須捨棄。

當您發現您現在公司的資訊與鄧白氏環球編碼不符合，請聯繫美商鄧白氏股份有限公司台灣分公司詢問修改事宜。您可以透過以下的連結查詢您的鄧白氏號碼：

- D&B UPIK：<https://www.dnb.com/de-de/upik-en/>

3-1-5 填寫管理人資訊

在管理人資訊的欄位中你將需要填寫管理人資訊，通常此管理人也會是憑證申請者的資訊，憑證也將會寄到管理人的信箱，如無特別需求，技術人可以與管理相符。

填寫聯繫人資料(英文填寫):

管理人資料		技術人資料	
<input checked="" type="checkbox"/> 同管理人資料			
*職稱 Coordinator	組織名稱	*職稱 Coordinator	組織名稱
*名字 Jimmy	*姓氏 Chang	*名字 Jimmy	*姓氏 Chang
*電話 +886-2-25319696	傳真 +886225319522	*電話 +886-2-25319696	傳真 +886225319522
<small>請務必輸入國碼、區碼與電話號碼</small>		<small>請務必輸入國碼、區碼與電話號碼</small>	
郵編 10448	城市 Taipei City	郵編 10448	城市 Taipei City
地址 12F, No.46, Zhongshan N. Rd., Sec. 2, Zhongshan Dist		地址 12F, No.46, Zhongshan N. Rd., Sec. 2, Zhongshan Dist	
*電子信箱 pm@net-chinese.com.tw		*電子信箱 pm@net-chinese.com.tw	
地區 Taiwan	國家 Taiwan	地區 Taiwan	國家 Taiwan

 傳真 只許為數字

清除重填

確認申請

當資料確認無誤後，請點選「確認申請」以送出訂單。

單域名專業型(銅牌級)(新申請) - www.net-chinese.com.tw



成功

關閉

至此，憑證申請流程已全數完成

3-2 | 進行域名驗證

憑證的審驗階段會依據不同的驗證類型而有不同的驗證方式，其分類上大致上可以分成：

由申請客戶主動發起的驗證

- 域名驗證 (Domain Control Validation)

由驗證機構主動發起的驗證

- 組織驗證 (Organization Validation)
- 電話驗證 (Callback Validation)

在這裡，我們先說明在遞件時選擇的驗證方式，是屬於驗證的第一環 - 域名驗證的部份，這個部份的驗證首先是要確認受驗證人確實擁有域名的所有權或控制權。在先前提到 SSL 使用三種方式進行驗證即屬域名驗證，大概可以概分以下三類：

- 電子郵件驗證：以電子郵件寄送驗證碼或連結供申請人完成驗證。
- 驗證檔驗證：使用 CSR 解碼的資訊以 MD5 及 SHA 演算法產生唯一值以供驗證資訊是否正確。
- DNS 驗證
 - CNAME 驗證：使用 DNS 新建 CNAME 記錄並置入 MD5 與 SHA 演算法產生的值以供查驗。
 - TXT 驗證：使用 TXT 記錄並置入 CA 給予的驗證值。

3-2-1 使用 Email 驗證 (Sectigo)

當您選擇使用了 Email 方式以進行驗證，您將會收到一封來自於 CA 頒發的信件，不同的品牌與其憑證頒發機構寄信的內容有可能會有所差異，但大致上都是點擊連結即完成，或還需要輸入驗證碼等後續動作的分別。在此，我們以 Sectigo 品牌的驗證信進行範例說明，因為它是最受歡迎的憑證品牌。

SECTIGO | Order Verification

Domain Control Validation for: www.net-chinese.com.tw

Dear service@net-chinese.com.tw,

We have received the request to issue an SSL certificate for:
 Domain(s): www.net-chinese.com.tw
 Subject: Net-Chinese Co.,Ltd
 12F, No. 46, Zhongshan N. Rd, Sec. 2, Zhongshan Dist
 Taipei City
 Taiwan
 Taiwan

This order was placed by a person whose email address is pm@net-chinese.com.tw

To complete the domain control validation for this certificate, please click [here](#) ← 點擊此處可以開啟驗證頁面
 and enter the following "validation code" (please make sure the reference number mentioned in this email subject matches the one you will see when entering the validation code):

[wDTfUsPAh9GuljMo3tNtwEXRX*amRuGc](#) ← 驗證碼在此

*****PLEASE NOTE CHOOSING THE OPTION BELOW WILL REJECT THE CERTIFICATE*****
 If neither you nor a trusted colleague made this request for a certificate then you can reject it by browsing to [Reject](#) ← 不要點選這裡，會拒絕驗證。

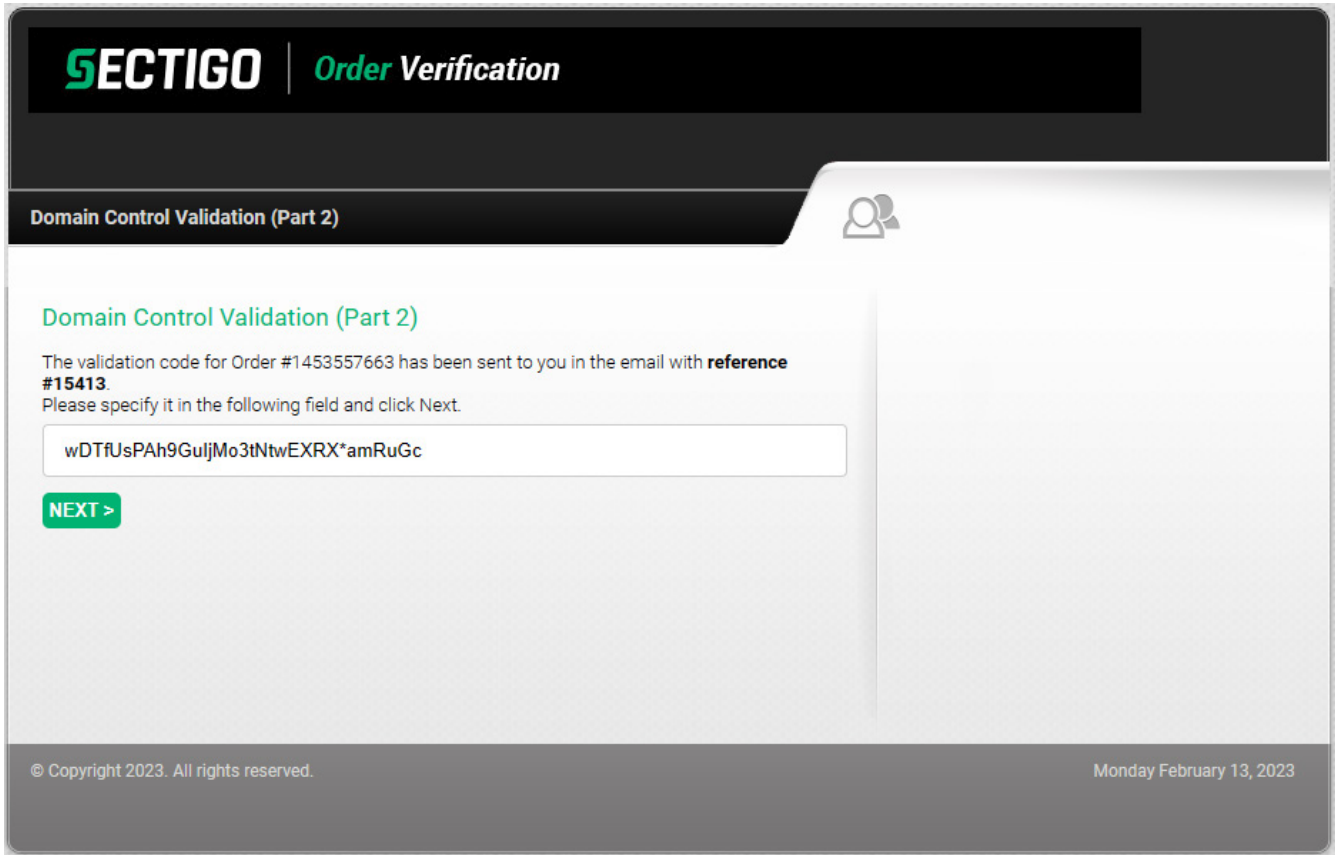
Thank you for being a valued Sectigo customer.

[visit our website](#)
[get support](#)

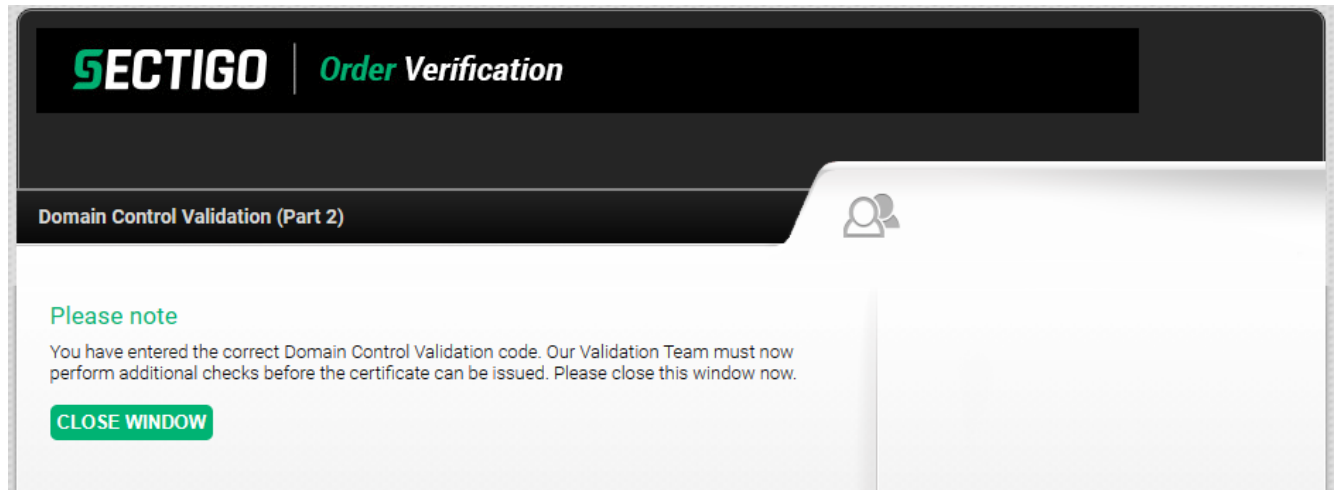
Copyright © Sectigo Limited, All rights reserved.

在您收到驗證信之後，裡面會載名您的管理人信箱，以及域名，如果是 OV/EV 型的憑證還會列有公司名稱、地址等資訊，以及驗證連結與驗證碼，請參照上面圖片的說明，複製驗證碼並貼上連結。如果您從未自行或委託他人申請 SSL 憑證，那麼在您可以選擇拒絕驗證。

如果您對驗證信點選「拒絕驗證」，那就不能再對此憑證進行驗證，須先進行辦理退貨事宜以重新購買與送件。；當您超過退貨期限後進行了憑證重置或重發證的階段，如果再點選拒絕驗證，將會無法對該憑證進行後續操作，網路中文將不受理該張訂單的退款，請特別謹慎操作。



點開驗證頁面連結，並將驗證信中隨附的驗證碼給貼入後，並按下「Next」。



驗證完成，您可以點選「Close Window」以關閉視窗。

使用 Email 驗證 (DigiCert/Thawte/GeoTrust)

對於 DigiCert 體系的憑證而言，可能不會第一時間以 E-Mail 的方式寄送給您，這個牽涉到憑證頒發機構的作業流程，對於 DigiCert 的品牌而言，在他們的作業上還是習慣先以電話進行照會，會詢問您是否有申請憑證。並且以人工的方式寄 / 補發驗證信。

這邊的範例以 Thawte 品牌示範他們的驗證信與驗證方式供您參考，由於 GeoTrust 也是隸屬於 DigiCert 的子品牌，同時也使用相同的系統，所以其他品牌的 Email 驗證信應不至於相差太大。

Hello,

We've received a request to add this domain to a Thawte account for use with a certificate.

Order info:

Domain name: net-chinese.com.tw

Account ID: 1432822

Order number: 366681453

Ordered on: 17 Feb 2023

Certificate type: OV

Organization name: Net-Chinese Co.,Ltd

What's next?

Before we can issue your certificate, approve the request to verify that you control net-chinese.com.tw.

View the details and complete the request here (link is valid for 30 days):

<https://dcv.thawte.com/link/domain-control-validation/?t=r7x86zh91qflsk3zv6g5tz9rrnz2143c&o=367842477>

Contact us if you have questions or need to reject the request here:

<https://www.thawte.com/about/contact/>

Support ID: 7597-3862-9751-5512

Thank you,

Thawte Customer Support

<https://www.thawte.com/about/contact/>

在您收到由憑證頒發機構發的驗證信後，裡面會有一個連結，請將之複製並貼上瀏覽器，此連結有效期限為 30 天，所以請您盡早作業。



Language ▾

Approve domain control validation request

Review the details and complete the verification request. We can issue certificates for **net-chinese.com.tw** after your approval.

Domain Details		
Domain name net-chinese.com.tw	Domain validation expiration date N/A	Organization Net-Chinese Co.,Ltd 12F, No.46, Zhongshan N. Rd., Sec. 2,Zhongshan Dist Taipei City, TAIWAN 10448 TW
Account ID 1432822	Organization Contact Jimmy Chang	

Approve domain control validation request

I confirm that I am the contact for the domain referenced above. I confirm and agree that:

1. Jimmy Chang (account #1432822) has the authority to apply for certificates for this domain on behalf of Net-Chinese Co.,Ltd (domain #).
2. Net-Chinese Co.,Ltd has the right to use and obtain certificates for the domain listed above as well as any subdomains of the listed domain.
3. Thawte may rely on this authorization for any subsequent certificate renewals or any orders placed by Net-Chinese Co.,Ltd until this authorization is revoked by written notice sent to Thawte (Attention Legal), 2801 North Thanksgiving Way, Suite 500, Lehi UT, 84043 USA.
4. I will promptly notify Thawte if this authorization is revoked or if a domain name listed above is transferred to a 3rd party.
5. Thawte may periodically reconfirm the control over the domain name(s) and approval of the corresponding certificate(s) using a reconfirmation email sent to the domain contact.

Approve Request ← 批准請求鍵

隨後，點選圖中的「批准請求鍵」以進行驗證。



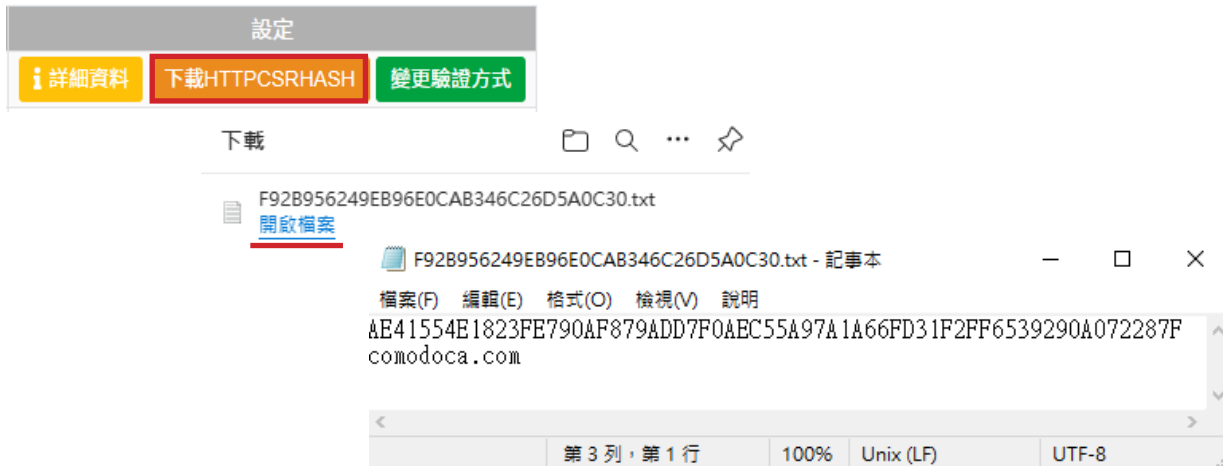
Language ▾

Thank you! We'll continue to work on your request and notify you about further updates.

當您看到了此訊息，恭喜您，您已經完成了 DigiCert 系列品牌的域名驗證。

3-2-2 使用 HTTPCSRHASH 驗證

當您選擇使用 HTTPCSRHASH 驗證時，您會從網路中文下載一個 TXT 驗證檔，或是由網路中文發送原廠給予的驗證檔，您需要將其放置在網站伺服器上面，但請注意，不同品牌的憑證會有不同的內文與檔名命名方式，但無論內文或檔名是什麼，您都不應該去任意更動取得的文件內容。



那當您取得了驗證檔，應該放在哪裡呢？依照憑證發證機構的指示，您應該將憑證檔您網站的根目錄為起點的相對路徑 `/root/.well-known/pki-validation` 之下。

請注意：

1. `root` 在此是代表您的網站根目錄，如果您是使用 Apache 系統，請依照附錄 A 查詢該系統或版本預配置的 `DocumentRoot` 位置；如果您使用的是 IIS 的使用者，通常會將 `C:\inetpub\wwwroot` 設為網站根目錄。
2. 如果您有使用虛擬站台 (VirtualHost) 的配置，則根目錄依照各別配置為主。
3. 如果您的根目錄下面沒有 `【.well-known】` 與 `【pki-validation】` 資料夾，請自行建立。
4. 如果您是在 Windows 環境下使用 Apache，那在圖型化介面下無法建立以 `."` 為開頭的資料夾，建議您在命令提示字元下以 `【mkdir .well-known】` 指令建立資料夾。
5. 如果您沒有新建一個主機名為空白的裸域 A 記錄指向站台，您可能會無法使用驗證檔驗證。
6. 依據 2021 年的新政策，當您購買的憑證若是 `【通用型憑證】`，您將無法使用驗證檔方式進行驗證；如果您是購買 `【多域名型憑證】`，則您將無法對附掛於主要頒發對象的域名使用驗證檔方式驗證，僅主要域名 (CSR CommonName) 可使用。

在您放置完成之後，您應該在瀏覽器上使用絕對路徑的方式檢查驗證文件是否能被開啟，以確認能讓外界進行存取，存取的路徑如下：`http(s):// 您申請頒發憑證的不含 www 的域名/.well-known/pki-validation/ 驗證檔名.txt`

例如：`https://net-chinese.com.tw/.well-known/pki-validation/F92B956249EB96E0CAB346C26D5A0C30.txt`

接下來，等候約一個工作天，讓發證機構進行排程驗證即可。

3-2-3 使用 DNS 驗證 (CNAME)

當您欲使用 DNS-CNAME 驗證的選項，請優先確認您有 DNS 的實際控制權，能夠新增 / 刪除 DNS 記錄的權限。否則，您應該將設定的工作交由相關人員執行，並提供它們需要賦與的值。

您可以在網路中文 >> 收合選單中的【SSL 憑證總覽】中，找到目前驗證中的憑證，點選【下載 CNAME】並取得相關資訊。

設定

詳細資料
下載CNAME
變更驗證方式

CNAMEAuthName _F92B956249EB96E0CAB346C26D5A0C30.

CNAMEAuthValue AE41554E1823FE790AF879ADD7F0AEC5.5A97A1A66FD31F2FF6539290A072287F.comodoca.com

確定

然後，在您的 DNS 代管服務提供商的介面上，新增一筆 CNAME 記錄，將 CNAME 別名分別填入別名 (Alias) 與指向目標 (Point to/target/value)。

我們將在下方列出幾種可能的設定，具體的設定與限制，還是要向您的服務提供商詢問，或查詢相關使用者手冊。

請注意：以下別名與指向位置的值僅是範例，請勿完全照抄。實際填寫值以系統給予的值為主。

Windows Server DNS

若您是使用 Windows Server 的 DNS 伺服器，請依照右邊的指示設定相關值。

別名： _F92B956249EB96E0CAB346C26D5A0C30
完整網域名稱 (FQDN)： _F92B956249EB96E0CAB346C26D5A0C30.net-chinese.com.tw
目標主機完整網域名稱 (FQDN)： AE41554E1823FE790AF879ADD7F0AEC5.5A97A1A66FD31F2FF6539290A0722B7F.comodoca.com

網路中文代管 DNS

若您是使用網路中文的代管 DNS，請依照右邊的指示設定相關值。

記錄類型： CNAME
主機名稱 / 別名： _F92B956249EB96E0CAB346C26D5A0C30
IP/ 域名： AE41554E1823FE790AF879ADD7F0AEC5.5A97A1A66FD31F2FF6539290A0722B7F.comodoca.com

CloudFlare

若您是使用 CloudFlare 的代管 DNS，請依照右邊的指示設定相關值。

類型 (TYPE)： CNAME
名稱 (Name)： _F92B956249EB96E0CAB346C26D5A0C30.net-chinese.com.tw
目標 (Target)： AE41554E1823FE790AF879ADD7F0AEC5.5A97A1A66FD31F2FF6539290A0722B7F.comodoca.com

BIND

若您是使用 BIND DNS Server，您需要修改您的 BIND 設定檔與 Zone File。

_F92B956249EB96E0CAB346C26D5A0C30.net-chinese.com.tw IN CNAME
 AE41554E1823FE790AF879ADD7F0AEC5.5A97A1A66FD31F2FF6539290A0722B7F.comodoca.com

3-3 | 進行驗證方式的更換

如果您選擇了三種憑證驗證方式之一，因為某些方式不合使用，必須進行更換。網路中文也可以提供您中途更換域名驗證方式，變換的方式如下：

收合選單

帳戶管理

域名管理

主機空間

SSL憑證

價格一覽表

SSL憑證總覽

已核發憑證 | 未完成憑證 | 已過期憑證

立即結帳 (0) 搜尋 清單下載

貼心小叮嚀：

1. 多年限SSL憑證需於每年進行更新，使用中憑證到期前30天將會以信件通知您更新憑證
2. 點選更新憑證按鈕後須重新進行遞交資料、驗證流程並須等待憑證商重新核發憑證

名稱	憑證類型	狀態	年限	憑證到期日	訂單到期日	設定
1 www.net-chinese.com.tw	單域名專業型(銅牌級)	驗證中	1	0000-00-00	0000-00-00	詳細資料 重發驗證信 變更驗證方式
2 netchost.tw	單域名進階型(白金級)	待核發	1	0000-00-00	0000-00-00	遞交資料

在驗證中的憑證中點選【變更驗證方式】，然後選擇其他種您想要使用的驗證方式以進行變更。具體的值或設定方式，請依照前面的相關章節進行設定或是套用變更。

變更驗證方式

選擇驗證方式

HTTPCSRHASH

Email

CNAME

HTTPCSRHASH

PREAL 取消

當選擇好欲變更的驗證方式後，請點選「確定」，當您看到「變更完成」後，即代表驗證方式已套用新款驗證方式。



變更完成

確定

3-4 | 組織驗證與電話驗證 (OV/EV 限定)

當您正在進行域名驗證的時候，同時間憑證頒發機構也正在透過第三方的公正機構網站 (例如：鄧白氏、國貿局或是其他第三方機構或網站) 正在對您提供的組織資訊是否與註冊資訊相符。這個部份所需要的時間原則上並不會超過 7 個工作天，當然若您的資料有誤，要進行更改後再驗證，則時程有可能將會延長。

然而，憑證的頒發，是需要滿足以下三個條件才會正式發證，所以憑證頒發的時長也取決於資料的正確性。

- 1. 域名控制驗證 (由客戶端設定，發證機構端驗證)
- 2. 組織基本公開訊息資料查核驗證 (發證機構端作業)

在上述兩個步驟完成驗證之後，才會進入到下一個步驟

※ 電話驗證

電話驗證可能會是由系統撥號，告知您驗證碼；也可能在 Email 上面附上電話驗證的驗證碼，再於網頁上填入驗證碼的半自動流程，或是由驗證單位親自打電話向您進行真人通話與查核，也許會向您詢問一些簡單的問題。當然，在您接獲驗證電話前，應該會寄發相關的信件知會您或與您排定時間。

以下是一個以郵件發送驗證碼的範例：



在您點開驗證頁面時，同時也將驗證碼貼入即可以完成驗證。

SECTIGO | Order Verification

Certificate Request Verification

English

We verified the following email address for your organisation *****@net-chinese.com.tw**

If the email address is incorrect, please click the following link to provide the correct one: [Correct Email for Verification](#)

By entering your details below, you confirm that the above-mentioned email address belongs to you and you have the authority to represent **Net-Chinese Co.,Ltd**

Title

First name

Surname

Complete Email Verification

To complete email verification, please enter the 6 digit verification code we delivered to you.

Email Verification Code

Submit

© Copyright 2023. All rights reserved. Wednesday February 15, 2023

填入您的職稱、姓名、與驗證碼後，按下【Submit】即可以等待發證。

Thank you

Thank you for completing the Certificate Request Verification process. Please feel free to close this Window now.

Close Window

驗證完成，您可以關閉視窗，等候憑證寄送。

Chapter 4 取得憑證

4-1 | 取得憑證

當您完成驗證後，您將會取得由 CA 頒發的憑證。至於各廠牌的憑證在頒發的方式也許會有不同，這邊將會列幾種常見的憑證組合格式：

以 ZIP 壓縮檔格式頒發的形式

Sectigo 憑證 - 由原廠供應

- **www_yourdomain_com_tw.crt**：網站終端憑證
- **AAACertificateServices.crt**：根憑證
- **USERTrustRSAAAACA.crt**：交叉簽署憑證
- **SectigoRSA(Domain/Organization/Extended)Validation.crt**：中繼憑證

Sectigo 憑證 - 由合作夥伴供應

- **CER - CRT Files** (為 x.509 格式的憑證)
 - **www_yourdomain_com_tw.crt or 1455134046.crt**：網站終端憑證，單域名以網址命名，多域名以訂單號命名。
 - **AAACertificateServices.crt**：根憑證。
 - **USERTrustRSAAAACA.crt**：交叉簽署憑證。
 - **SectigoRSA(Domain/Organization/Extended)Validation.crt**：中繼憑證。
 - **My_CA_Bundle.ca-bundle**：信任鏈 Bundle(將中繼憑證 / 交叉簽署憑證 / 根憑證) 打包的檔案。
- **PKCS7 File**
 - **PKCS7.p7b**：為 PKCS7 編碼的憑證檔。
- **Plain Text Files** (為 x.509 格式的文字版)
 - **www_yourdomain_com_tw.txt or 1455134046.txt**：網站終端憑證文字版，單域名以網址命名，多域名以訂單號命名。
 - **AAACertificateServices.txt**：根憑證文字版
 - **USERTrustRSAAAACA.txt**：交叉簽署憑證文字版
 - **SectigoRSA(Domain/Organization/Extended)Validation.txt**：中繼憑證文字版
 - **CA Bundle.txt**：信任鏈 Bundle 文字版 (將中繼憑證 / 交叉簽署憑證 / 根憑證) 打包的檔案。
- **!PRIVATE KEY INFO!.txt** (私鑰資訊說明與宣告文件)
- **Choosing the Right Files to Install.txt** (憑證格式說明與安裝適用文件)

Chapter 5 安裝憑證

5-1 | 查找憑證所在位置 (Linux 版 Apache)

您可以使用下面這一組命令，找到憑證放置的路徑，至於憑證的配置檔，需要請您參考附錄 A，因為不同的作業系統、不同的檔案來源安裝包，所預設安裝的位置不一樣。以下，將以 CentOS 的設定與配置查找檔案：

```
grep -i -r "SSLCertificateFile" /var/httpd/
```

請注意：

`/var/httpd/` 需要替換成您的 Apache 安裝目錄

接著，系統就會回饋給您檔案的放置資訊，像下面：

```
/etc/httpd/conf.d/ssl.conf:# Point SSLCertificateFile at a PEM encoded certificate. If
/etc/httpd/conf.d/ssl.conf:SSLCertificateFile /etc/pki/tls/certs/localhost.crt
/etc/httpd/conf.d/ssl.conf:# the referenced file can be the same as SSLCertificateFile
```

由此系統的回傳資訊可得知憑證資訊的放置路徑在 `/etc/pki/tls/certs/localhost.crt`，而位於 `/etc/httpd/conf.d/ssl.conf` 的檔案中則有包含 "SSLCertificateFile" 的資訊；同理，您也能使用 `grep` 指令找到其他的資訊，例如 "SSLCertificateKeyFile" (私密金鑰)，或 "SSLCertificateChainFile" (由根憑證與中繼憑證合起來的信任鏈檔案)。

然後，再執行下列命令用來檢查 Apache 設定檔是否有錯誤。

執行設定檔測試

```
apachectl configtest
```

當系統回應您 `Syntax OK`，代表您的語法設定正確，如果不是這個訊息內容，請您重新檢查設定檔的內容。

重新啟動 Apache 服務

```
apachectl restart
```

請注意，執行檔測試與 Apache 服務重啟，這邊用的指令是 `apachectl`，指令的方面可能會隨著系統有所不同，建議您可以參看配置表。

5-2 | 查找憑證所在位置 (Windows 版 Apache)

Windows 版與 Linux 不同之處在於，它擁有圖形化的介面，所以您可以直接在 Windows 上直接查閱 conf 資料夾中的各配置檔，主要還是建議先從兩個檔案查起：

- conf\extra\httpd-ssl.conf
- conf\extra\httpd-vhosts.conf (使用虛擬主機配置)

如果您是全新的 Apache，建議您先用記事本開啟 conf\httpd.conf 的檔案，然後使用尋找 (Ctrl+F)，找尋這一串指令【LoadModule ssl_module modules/mod_ssl.so】，並把前面的 # 標記給取消，才表示該指令敘述是實際可運用的而非註解。

之後，您必須再 httpd.conf 文件中額外搜尋文字【httpd-ssl.conf】，然後於 #Include conf/extra/httpd-ssl.conf 中，將其 # 取消，代表 httpd-ssl.conf 的配置檔會額外被引入使用，並於修改完成後，儲存 httpd.conf 檔案。

請注意：

無論在 Windows 還是 Linux 環境，當指令前面有 # 符號時，代表它是一個註解，是一段不會被執行的指令。

當文件設定完成之後，您就可以依照相關配置檔，找尋 "SSLCertificateFile"、"SSLCertificateKeyFile" 與 "SSLCertificateChainFile" 敘述的憑證位置，並將其替換後，修改檔案名。

重新啟動 Apache 服務

您可以使用三種方式來重啟 Apache 服務：

1. 在搜尋列打「服務」或是「開始→Windows 系統管理工具→服務」，開啟服務視窗後，找尋 Apache，並將其啟動。
2. 在 CMD 命令提示字元，先將目錄轉換至 bin，再輸入 httpd 以進行啟動。
3. 在工具列也許會有 Apache 的控制面板，可以在上面點滑鼠右鍵以進行啟用

附錄 A : Apache 發行版預設框架

Apache httpd 2.0 預設框架 (apache.org 源碼包)

```

ServerRoot :           /usr/local/apache2
DocumentRoot :        /usr/local/apache2/htdocs
Apache Config File    /usr/local/apache2/conf/httpd.conf
SSL config :          /usr/local/apache2/conf/ssl.conf
ErrorLog :            /usr/local/apache2/logs/error_log
AccessLog :           /usr/local/apache2/logs/access_log
cgi-bin :             /usr/local/apache2/cgi-bin
binaries (apachectl) : /usr/local/apache2/bin
start / stop :        /usr/local/apache2/bin/apachectl
                        (start|stop|graceful|configtest)

```

Apache httpd 2.2 預設框架 (apache.org 源碼包)

```

ServerRoot :           /usr/local/apache2
DocumentRoot :        /usr/local/apache2/htdocs
Apache Config File    /usr/local/apache2/conf/httpd.conf
Other Config Files    /usr/local/apache2/conf/extra/
SSL config Files      /usr/local/apache2/conf/extra/httpd-ssl.conf
ErrorLog :            /usr/local/apache2/logs/error_log
AccessLog :           /usr/local/apache2/logs/access_log
cgi-bin :             /usr/local/apache2/cgi-bin
binaries (apachectl) : /usr/local/apache2/bin
start / stop :        /usr/local/apache2/bin/apachectl
                        (start|restart|gracefull|graceful-stopstop|graceful|configtest)

```

Apache httpd 2.4 預設框架 (apache.org 源碼包)

```

ServerRoot :           /usr/local/apache2
DocumentRoot :        /usr/local/apache2/htdocs
Apache Config File    /usr/local/apache2/conf/httpd.conf
Other Config Files    /usr/local/apache2/conf/extra/
SSL config Files      /usr/local/apache2/conf/extra/httpd-ssl.conf
ErrorLog :            /usr/local/apache2/logs/error_log
AccessLog :           /usr/local/apache2/logs/access_log
cgi-bin :             /usr/local/apache2/cgi-bin
binaries (apachectl) : /usr/local/apache2/bin
start / stop :        /usr/local/apache2/bin/apachectl
                        (start|restart|gracefull|graceful-stopstop|graceful|configtest)

```

Debian, Ubuntu (Apache httpd 2.x)

```

ServerRoot :           /etc/apache2
DocumentRoot :         /var/www
Apache Config File :   /etc/apache2/apache2.conf
                       /etc/apache2/ports.conf
Default VHost Config : /etc/apache2/sites-available/default, /etc/apache2/sites-enabled/000-default
Module Locations :     /etc/apache2/sites-available, /etc/apache2/mods-enabled
ErrorLog :             /var/log/apache2/error.log
AccessLog :           /var/log/apache2/access.log
cgi-bin :             /usr/lib/cgi-bin
binaries (apachectl) : /usr/sbin
start / stop :        /etc/init.d/apahce2
                       (start|stop|restart|reload|force-reload|start-htcacheclean|stop-htcacheclean)

```

Fedora Core, CentOS, RHEL

```

ServerRoot :           /etc/httpd
Primary Config File :  /etc/httpd/conf/httpd.conf
Other Config Files :  /etc/httpd/conf.d
Module Locations :    /usr/lib/httpd/modules
DocumentRoot :        /var/www/html
ErrorLog :            /var/log/httpd/error_log
AccessLog :           /var/log/httpd/access_log
cgi-bin :             /var/www/cgi-bin (empty and disabled by default)
runtime directory :   /etc/httpd/run
start / stop :        /sbin/service httpd
                       {start|stop|restart|condrestart|reload|status|fullstatus|graceful|help|configtest}

```

RedHat 9.0 及更早版本

```

ServerRoot :           /etc/httpd
Primary Config File :  /etc/httpd/conf/httpd.conf
DocumentRoot :        /var/www/html
ErrorLog :            /var/log/httpd/error_log
AccessLog :           /var/log/httpd/access_log
cgi-bin :             /var/www/cgi-bin (empty and disabled by default)
binary :              /usr/sbin/httpd
start/stop :          /sbin/service httpd
                       {start|stop|restart|condrestart|reload|status|fullstatus|graceful|help|configtest}

```

Mac OSX (Leopard, Apache httpd 2.2) :

```

ServerRoot :           /usr
Primary Config File :  /etc/apache2/httpd.conf
DocumentRoot :        /Library/WebServer/Documents
ErrorLog :             /var/log/apache2/error_log
AccessLog :           /var/log/apache2/access_log
cgi-bin :              /Library/WebServer/CGI-Executables (empty by default)
binary :              /usr/sbin/httpd
start/stop            /usr/sbin/apachectl
                     (start|stop|restart|fullstatus|status|gracefull|graceful-stop|configtest|help)

```

FreeBSD 6.1 (Apache httpd 2.0)

```

ServerRoot           /usr/local
Config File          /usr/local/etc/apache2/httpd.conf
DocumentRoot        /usr/local/www/data
ErrorLog             /var/log/httpd-error.log
AccessLog            /var/log/httpd-error.log
cgi-bin              /usr/local/www/cgi-bin
binaries (apachectl) /usr/local/sbin
start/stop           /usr/local/etc/rc.d/apache2.sh [fast|force|one]
                     (start|restart|stop|reload|configtest|rcvar)
/etc/rc.conf variables apache2_enable="YES"

```

Win32 (Apache httpd 2.2)

```

ServerRoot :          "C:/Program Files/Apache Software Foundation/Apache2.2"
Config File :         "C:/Program Files/Apache Software Foundation/Apache2.2/conf/httpd.conf"
DocumentRoot :       "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"
ErrorLog :            "C:/Program Files/Apache Software Foundation/Apache2.2/logs/error.log"
AccessLog :           "C:/Program Files/Apache Software Foundation/Apache2.2/logs/access.log"
cgi-bin :             "C:/Program Files/Apache Software Foundation/Apache2.2/cgi-bin"
binaries (apachectl) : "C:/Program Files/Apache Software Foundation/Apache2.2/bin"

```

附錄 B：將憑證合併成集成 Bundle 檔案

當憑證有的時候要將中繼憑證與根憑證給集成為一個信任鏈檔案，基本上可以透過指令來將三個檔案合併成一個，但在進行這類合併的作業之前，您需要先了解附件的檔案：

Sectigo

- **www_yourdomain_com_tw.crt**：網站終端憑證
- **AAACertificateServices.crt**：根憑證
- **USERTrustRSAAAACA.crt**：交叉簽署憑證
- **SectigoRSA(Domain/Organization/Extended)Validation.crt**：中繼憑證

DigiCert (Thawte/GeoTrust/DigiCert)

- **www_yourdomain_com.cer Or star_tatung_com.cer**：網站憑證
- **DigiCertCA.cer**：中繼憑證
- **TrustedRoot.cer**：根憑證

GlobalSign

- **CEXXXXXXXXXXXXX.crt**：網站憑證 (XX 代表英文或數字所組成的訂單號碼)
- **GSXXXXXXXXXXXXX.crt**：中繼憑證 (中繼憑證以 GS 開頭)
- **Root-RX.crt**：根憑證 (可能因不同分類分為 R1/R3/R6 等等)

好的，無論您取得的所有憑證 (不管是壓縮檔隨附的，或是從發證機構下載的) 為何副檔名，都不重要，因為這些名字可以依照您的喜好做更名，您只需要知道哪些憑證代表什麼就好，接下來，這邊將進行指令的示範，您可以在 Linux 環境或是 Windows 的命令提示字元中，將檔案合併成信任鏈的集成 Bundle 檔。

Linux

```
cat FileName1.crt FileName2.crt FileName3.crt > OutputFileName.ca-bundle
```

Windows or DOS

```
copy FileName1.crt + FileName2.crt + FileName3.crt OutputFileName.ca-bundle
```

- **FileName** - 原始檔案名稱
- **OutputFileName** - 輸出儲存的自定義檔案名稱
- **ca-bundle** - 為集成檔，是否需要另外再補 .crt 副檔名讓它成為 x.509 格式的憑證則依據個人需求決定。

請注意：
請依照實際的檔案名稱代入，勿直接照抄輸入 "FileName"

在執行上述指令時，建議將檔案放置同一資料夾下，並將當前路徑指定到憑證檔所在路徑下再執行。

附錄 C：各品牌發行之中繼憑證 / 根憑證下載來源

Sectigo

中繼與根憑證：<https://support.sectigo.com/articles/Knowledge/Sectigo-Intermediate-Certificates>

Sectigo 的憑證是將中繼、根憑證打包成一個 ZIP 檔，您可以在上述的連結下載您所需要的中繼、根憑證以便使用。

DigiCert(Thawte/GeoTrust/DigiCert)

根憑證：<https://www.digicert.com/kb/digicert-root-certificates.htm>

中繼憑證：<https://www.digicert.com/kb/digicert-root-certificates.htm#intermediates>

交叉簽署憑證：<https://www.digicert.com/kb/digicert-root-certificates.htm#cross-signed>

因為 Thawte、GeoTrust、DigiCert(包含前身 Symantec) 的憑證，均為 DigiCert 的子品牌，所以也使用同一套體系的頒發平台進行頒發，所以在根憑證與中繼憑證上，均相容於 DigiCert。故購買 DigiCert 品牌的憑證，不論是何種子品牌，均可以共通使用。

GlobalSign

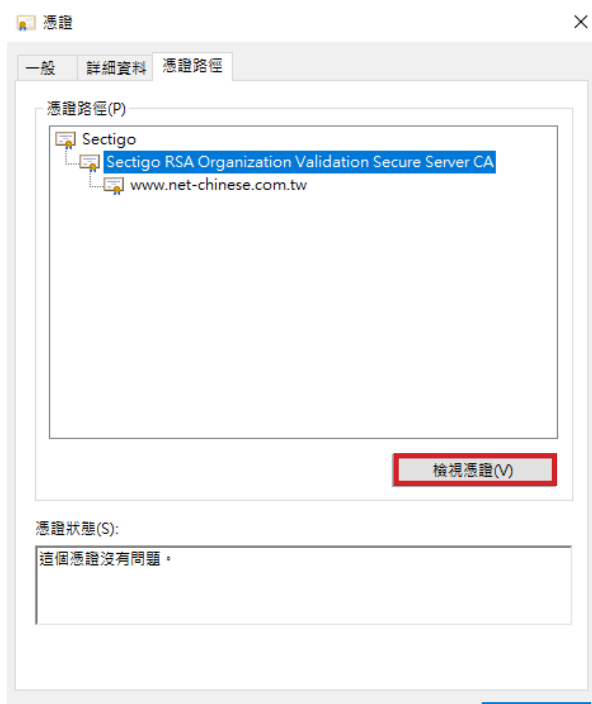
根憑證：<https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates>

DV 中繼憑證：<https://support.globalsign.com/ca-certificates/intermediate-certificates/domainssl-intermediate-certificates>

OV 中繼憑證：<https://support.globalsign.com/ca-certificates/intermediate-certificates/organizationsssl-intermediate-certificates>

EV 中繼憑證：<https://support.globalsign.com/ca-certificates/intermediate-certificates/extendedssl-intermediate-certificates>

如何查看我的根憑證與中繼憑證



在 X.509 的視窗之中，可以點選頁籤『憑證路徑』，查看此張憑證信任鏈的中繼憑證與根憑證，您可以點選『檢視憑證』以進行查看。

而在 Linux 的環境之下，可以使用下列語法以進行憑證查詢
`$openssl verify -untrusted < 中繼憑證 > < 網站憑證 >`

若為相匹配的憑證，則會回傳您 OK 的訊息，若為不相符的中繼憑證，則會回傳您 verification failed 的訊息。

什麼時候我需要額外下載憑證？

中繼憑證做為根憑證的替身，因為根憑證一般而言受到發證機構的嚴密保護，以避免失竊與竄改，引發終端憑證的信任問題。因此，利用中繼憑證做為一個 Proxy 代理，以確保根憑證的私密金鑰絕對無法被存取。因此，所有的終端憑證皆由中繼憑證簽發而成。

如果您不和核發的終端憑證一同安裝中繼憑證，有可能會無法建立信任鏈，將會使訪客存取時收到「這個安全性憑證是由您尚未信任的公司所發出」。但有些 CA 在發證時並不會發中繼與根憑證，需要由您親自下載並透過憑證路徑進行查詢。

附錄 D：將憑證轉換為 PFX 格式或將 PFX 格式的憑證解離

將 PEM 編碼轉換為 PFX

1. 將憑證檔案與私密金鑰檔案 (.crt 檔案與 .key 檔案) 在相同的工作路徑之下
2. 輸入以下的指令

```
openssl pkcs12 -export -in <Cert Path and FileName> -inkey <Key Path and FileName> -out <CustomName.pfx> -certfile <TrustChain Path and FileName> -password pass: <Password>
```

注意：上述指令中，紅色的字請依照您實際的環境與檔案路徑進行填寫

參數詳解：

- pkcs12 -export：將憑證匯出為 pkcs12 的編碼格式 (即 PFX)
- -in <Cert Path and FileName>：請依照所在環境輸入憑證檔路徑與檔案。例如 C:\certfile\mysite.crt 或 /etc/cert/mysite.crt
- -inkey <Key Path and FileName>：請依照所在環境輸入私鑰檔路徑與檔案。例如 C:\certfile\private.key 或 /etc/cert/private.key
- -out <CustomName.pfx>：為您要命名的 PFX 憑證檔名，請依自己喜好自訂。
- -certfile <TrustChain Path and FileName>：請依照信任鏈 (由中繼憑證與根憑證 Bundle 在一起的憑證檔) 所在環境輸入信任鏈憑證檔路徑與檔案。
- -password pass: <Password>：自定密碼，為設定匯入時要求的密碼，通常在 Windows 作業系統匯入 PFX 憑證時會要求密碼。

將 PFX 編碼轉換為 PEM

請確定你的來源環境在匯出時是否已經包含了憑證檔、私密金鑰、信任鏈。然後，執行下列指令。

```
openssl pkcs12 -in <FilePath and Name.pfx> -out <CustomName.pem> -nodes -password pass:<Password>
```

參數詳解：

- pkcs12 -in <File Path and Name.pfx>：原始檔案的檔名
- -out <CustomName.pem>：為您要輸出的檔案名字，您可以依照自己想要的檔案格式輸出為 .pem/.txt 或 .crt
- -nodes：代表不對輸出的檔案額外進行 3DES-CBC 演算法加密
- -password pass:<Password>：為當初建立 PFX 類型憑證定義的密碼，必須輸入才能正確轉換。

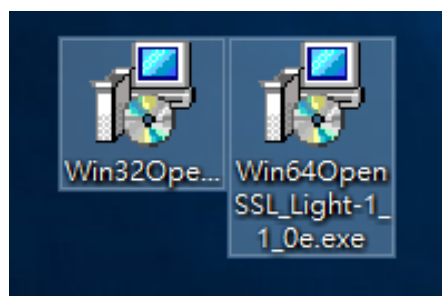
附錄 E：於 Windows 上安裝 OpenSSL

取得 Win32/64 版的 OpenSSL

一般而言，OpenSSL 套件預設在 Linux 之中，如果您今天希望在 Windows 作業系統中使用 OpenSSL，那麼您必須下載包裝成可供 Windows 執行的 OpenSSL。您可以在下列的網址中下載到屬於您作業系統版本的 OpenSSL。

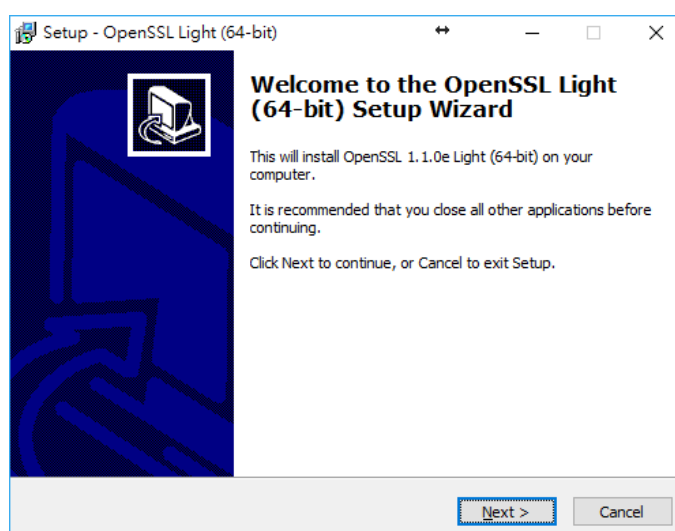
取得網址：<https://slproweb.com/products/Win32OpenSSL.html>

右圖是下載回來的 MSI 或 EXE 安裝檔，請確認您的作業系統是 32 位元或 64 位元，就可以選擇相對應的安裝程式來進行安裝。若是 32 位元就選擇 Win32 或 x86；而 64 位元就選擇 Win64 檔案來進行安裝。



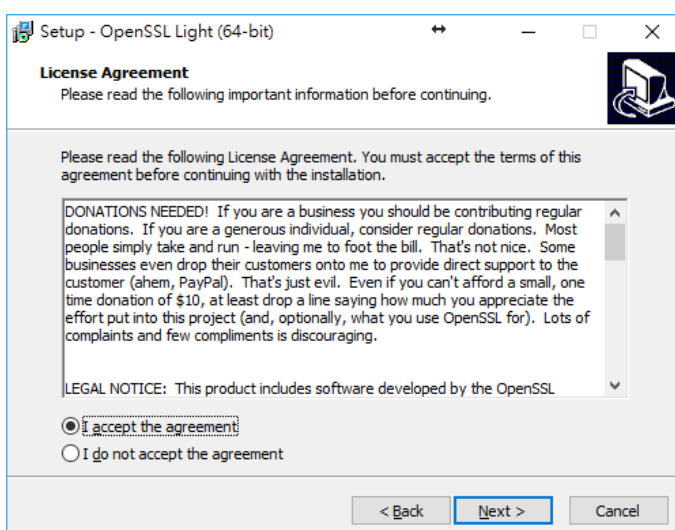
安裝順序：

1. 在這裡點選 **Next>** 以進行到下一個視窗

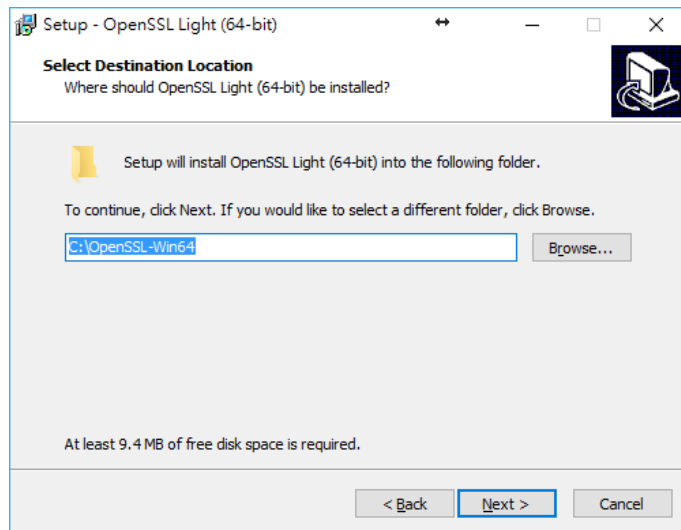


2. 為版權協議頁面，若沒有任何疑問。

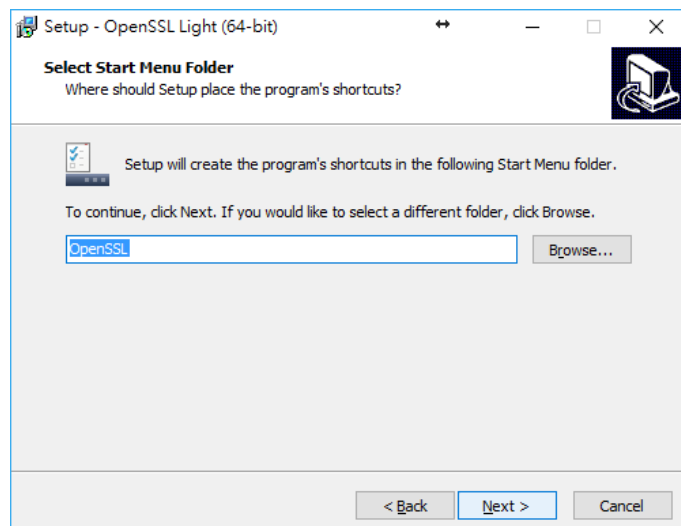
請點擊 "I accept the agreement" 後，點擊 **Next>**



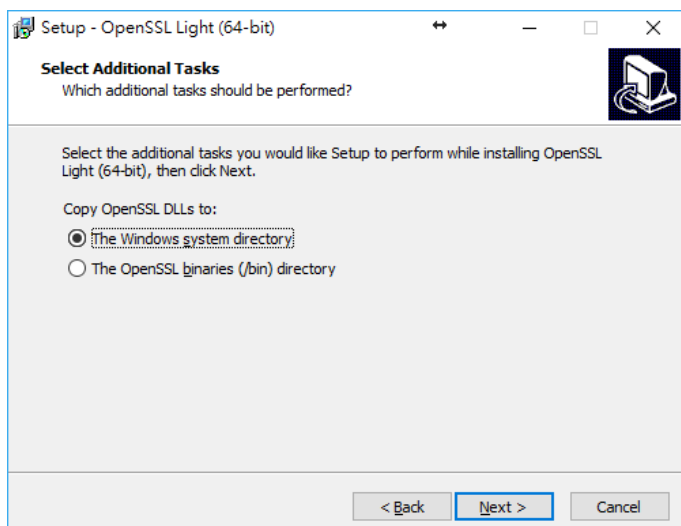
3. 選擇欲安裝的路徑，若沒有疑問請點選 **Next >**



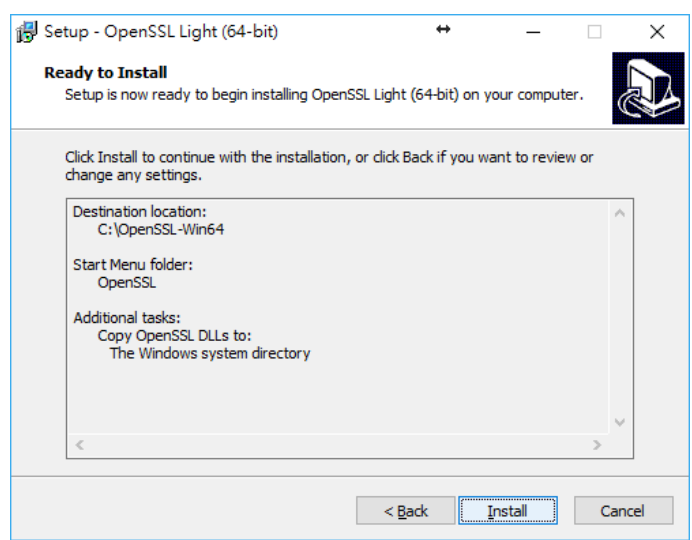
4. 選擇是否將 OpenSSL 加入至開始功能表，若沒有疑問請點選 **Next >**



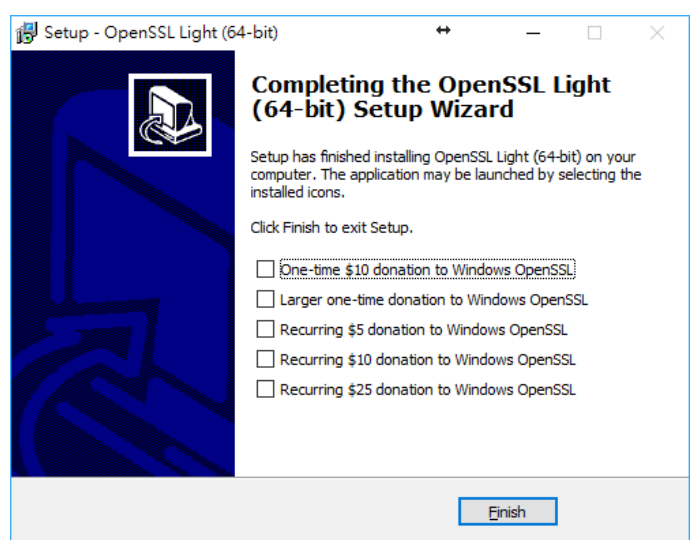
5. 選擇您想在安裝 OpenSSL 輕量版時的額外位置，如無特別需求，可直接選擇 "The windows system directory"。



6. 再次確認前面的選項沒有疑問，就可以按下 Install 以開始進行 OpenSSL 的安裝。

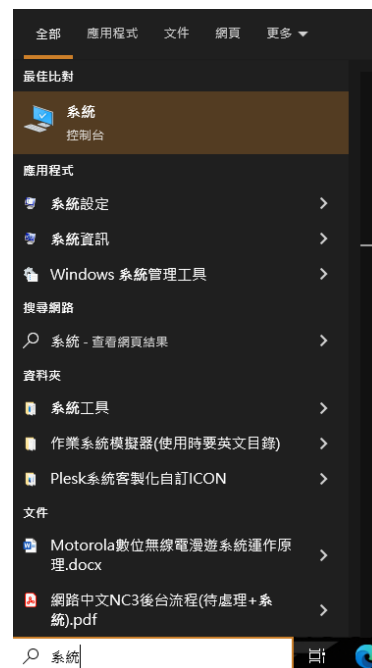


7. 裝完成後，系統會問你要不要對將 OpenSSL 開發成 Windows 安裝包的開發團隊進行讚助，如無意願的話，請點選 Finish。

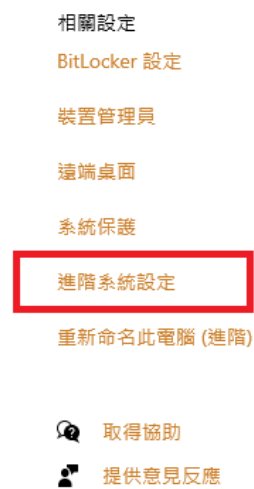


環境變數設定：

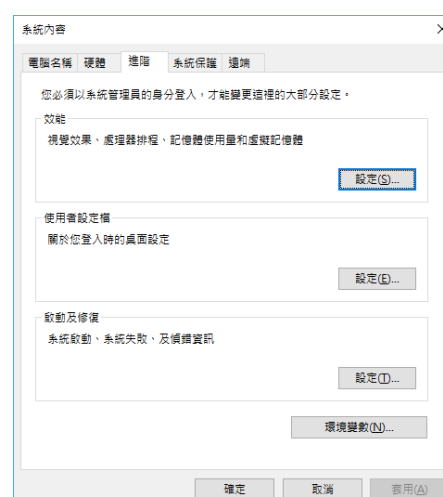
1. 首先，在桌面上的工作列搜尋欄上面輸入「系統」後，接著就會出現候選選項（如右圖）



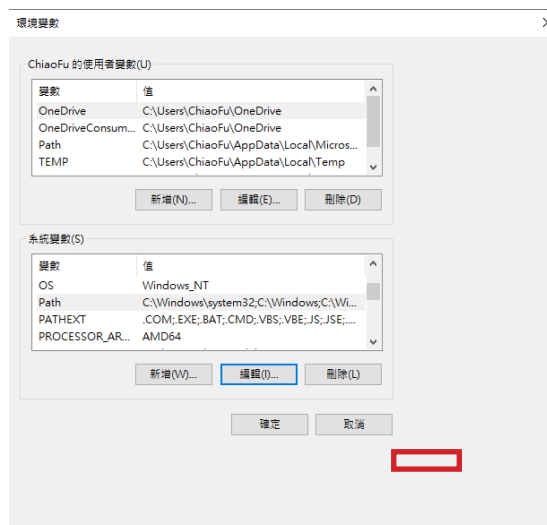
2. 接著就會看到「進階系統設定」。



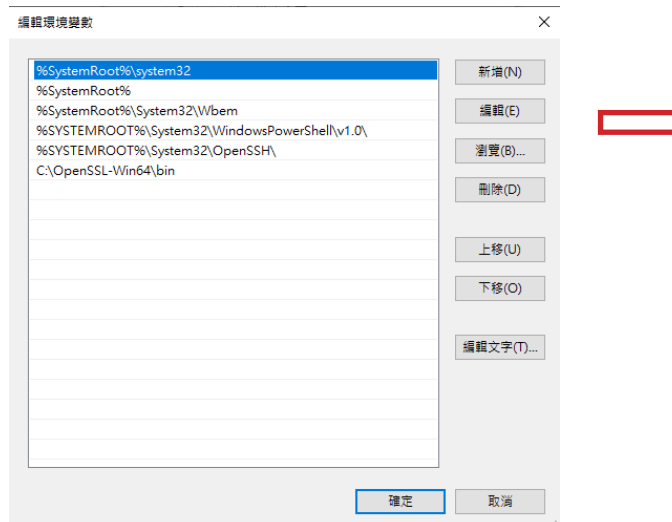
3. 在「進階」頁籤中，點選最下方的「環境變數」



4. 於下方的「系統變數」中找尋變數項目為 "Path" 之後，請點選「編輯」。



5. 點選「新增」後，將 OpenSSL 安裝的實際路徑下層的 bin 資料夾給指定進來。如不知道安裝路徑，您可以透過「瀏覽」進行搜尋並指定，設定完之後點選「確定」



6. 進行測試：在搜尋列上輸入「cmd」或「命令提示字元」叫出來後，輸入指令「openssl version」。若有顯示目前 OpenSSL 的版本號，即意味著安裝成功。

您可以在命令提示字元中執行常見以 OpenSSL 命令為首的相關指令 (例如私鑰生成、CSR 生成…等)，產出的檔案會放在 C:\使用者\使用者名稱 的資料夾下面。

```

命令提示字元
Microsoft Windows [版本 10.0.19045.2728]
(c) Microsoft Corporation. 著作權所有，並保留一切權利。
C:\Users\ChiaoFu>openssl version
OpenSSL 3.1.0 14 Mar 2023 (Library: OpenSSL 3.1.0 14 Mar 2023)
C:\Users\ChiaoFu>

```

