網路中文
www.net-chinese.com.tw

# CSR 生成與憑證安裝指南
# 適用於 PLESK




2022 年 4 月更新 二版

章節 1

# 生成CSR憑證請求檔及私密金鑰

本章節將開始帶您操作如何使用產生申請憑證時必要的 CSR(Certificeate Signing Request) 文件及私密金鑰 (Private Key)，幫助您生成憑證必要文件。

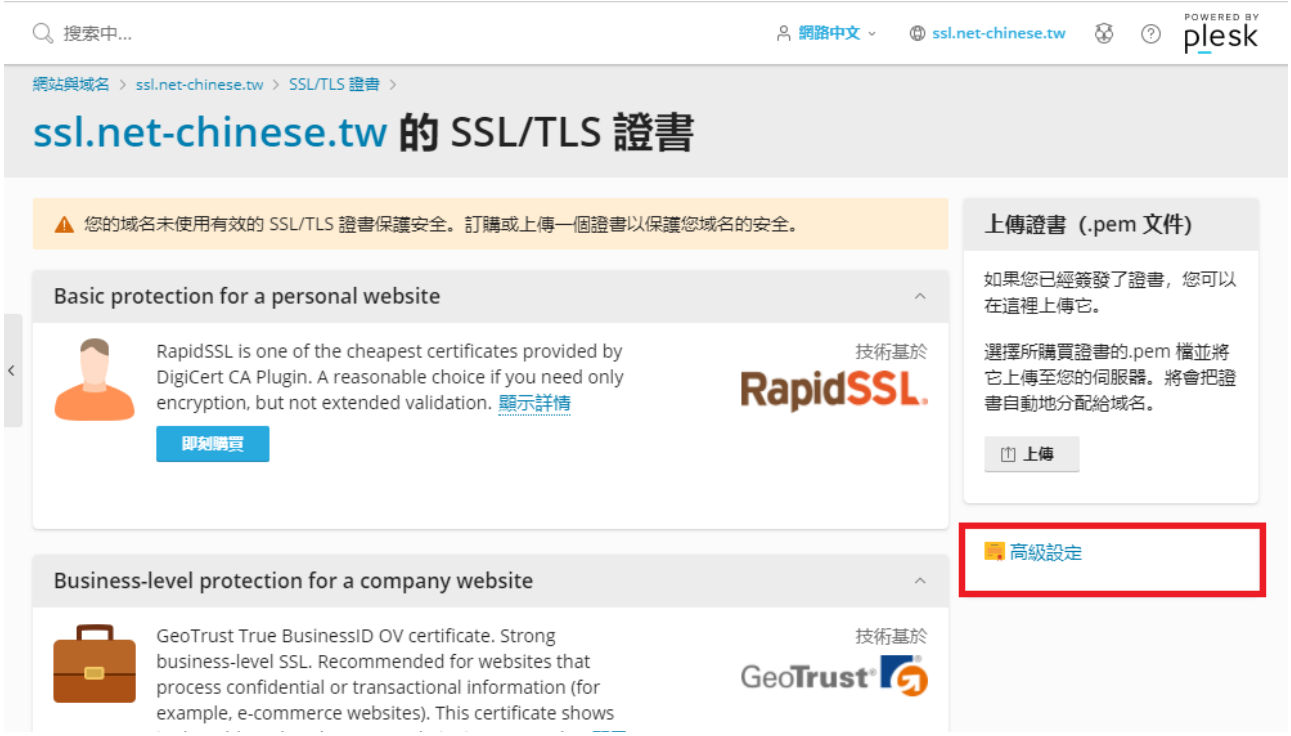
## 一、至「網站與域名」中，點選「SSL/TLS 證書」圖示


Plesk 是一個虛擬主機管理平台，系統會提供您各種有關於站台的操作，所以要進入管理平台，您必須具備管理員權限的帳號與密碼。若您沒有管理權限的帳號密碼，請向您的主機商或是資訊人員取得相關必要資訊。

若您是向網路中文購買的各式雲端服務主機 ( 基本型 / 進階型 / 商務型 /Mail)，則請至您的網路中文帳號主要信箱中收取「雲端服務啟用通知信」，裡面會附上您的帳號與密碼。

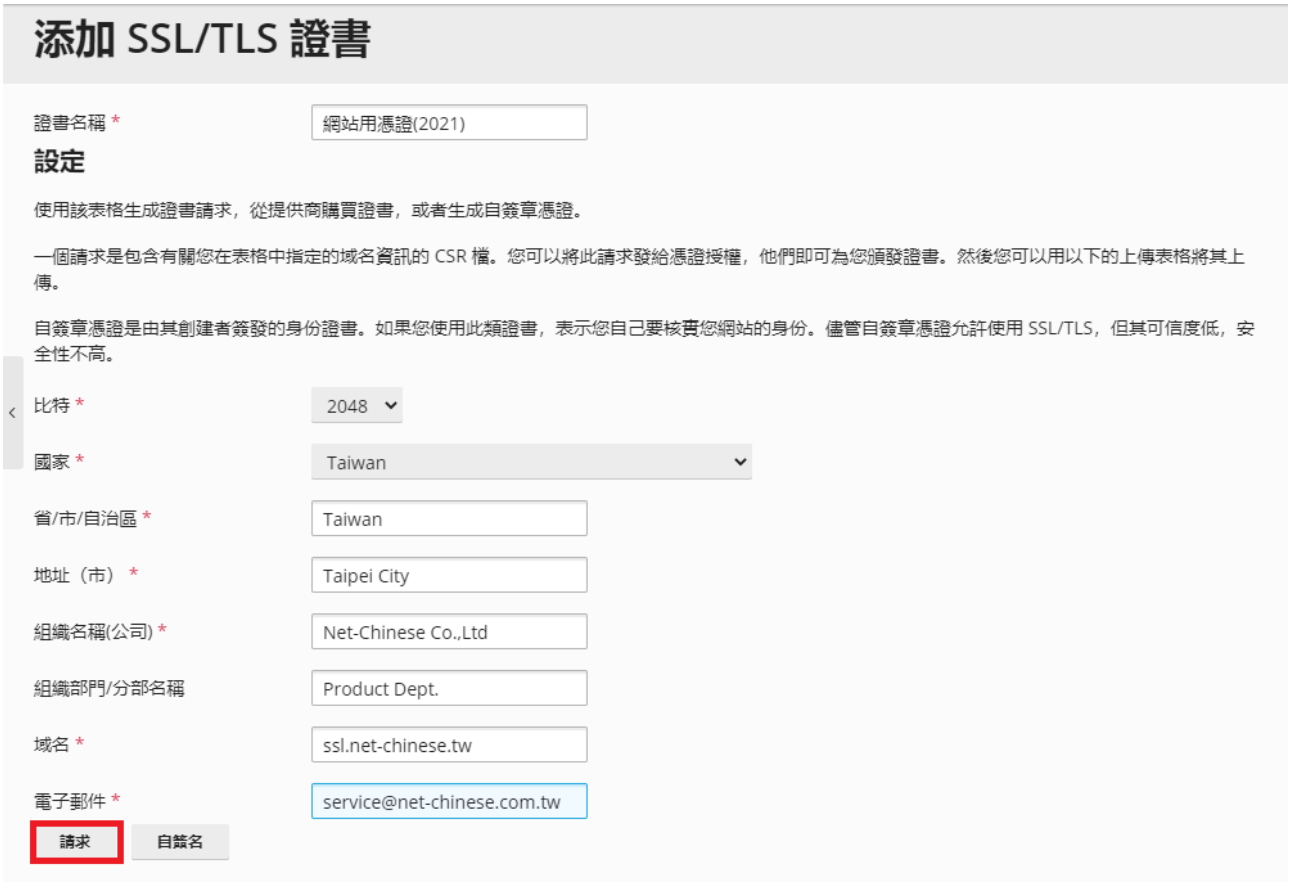
在製作 CSR 方面，Plesk 平台有著非常優秀的性能，生成憑證請求檔亦十分方便，如果您是新申請用戶，建議您可以直接透過平台內的方式進行生成私密金鑰與 CSR 檔案；若您原本就有數位憑證的用戶，亦可以利用匯入的方式將既有憑證匯入。

## 二、點選「高級設定」




## 三、點選「添加 SSL/TLS 證書」

# 三、依下圖範例使用英文填入相應的資料 ( 比特請選擇 2048)




在這個欄位中，您可以給您的證書一個名稱，您可以給它一個好記的名稱，或是使用域名做為名稱。

接著，請在下拉選單中，在比特 ( 位元長度 ) 中，選擇 2048 位元；國家欄位用下拉式選單選擇您所在的國家或地區即可。

在省 / 市 / 自治區內，請依照您的所在地填入，如果您在台灣，則填入 Taiwan 即可；地址欄位僅需要填入公司或組織的所在縣市即可，不需要填寫完整地址。

組織名稱 ( 公司 )，為一個必要填寫的欄位，所以請用英文填入您的組織名稱或公司名稱。

域名 ( 主要名稱 )，請用不含「http://」開頭的主機名稱 + 域名名稱填入

電子郵件欄位則填入承辦人或是公司 / 組織的公開信箱即可。

上述資料，建議您全程使用英文填寫，避免使用中文字元及特殊字元 ( 您可以使用 and 取代 &)，如果您是申請組織驗證型的憑證，將會有效的供審核人員加速審核。

以上資訊填寫完了，請按一下『請求』按鍵以生成 CSR 與私密金鑰。

## 四、生成完成後點選名稱以查看資訊


在上面的圖示上，您可以看到四個圖示，分別是 R、K、C、A，已有提供者會以較為深色的顏色表示，尚未提供者會以較為淡色的圖示表示。或者，您也可以將滑鼠游標移至圖示上面，Plesk 會告訴您目前該項目是否提供。

- R(Request - 請求檔 ) - 在使用 Plesk 生成 CSR 時，則必定會有請求檔 ( 自簽發不會產生 )，若您是自有憑證，且採用外部匯入的情況時，則 R 欄的信封圖示會以淡色表示。

- K(Key - 私密金鑰 ) - 在使用 Plesk 生成 CSR 時，因為 CSR 與私鑰必然是成對配對，所以一定會產生私鑰，若您是自有憑證，且採外部匯入時，則必須要準備與之配對的私密金鑰才能使憑證產生作用。若未匯入私密金鑰，則 K 欄的鑰匙圖示會以淡色表示。

- C(Certificate - 憑證檔 ) - 在您獲得了發證機構頒發的憑證之後，則會有一個憑證檔 ( 不管是以 .crt 檔案表示或是以純文字格式表示。您必須將其匯入主機。若您未匯入憑證檔，則 C 欄的憑證圖示會以淡色表示。

- A(Authority - 信任鏈 ) - 這個項目是由憑證頒發機構所簽署的根憑證、中繼憑證所組成的信任鏈，以讓您的憑證可以透過信任鏈查詢頒發來源。若您的憑證是由第三方的機構頒發的，則憑證頒發機構會提供根憑證與中繼憑證供您匯入。若您未匯入信任鏈檔案，則 A 欄的圖示會以淡色表示。( 自簽發憑證不會產生 )

右邊的「已使用」即代表目前這張憑證繫結了幾個站台，關於繫結的部份，請查詢第 3 章。

# 五、捲動捲軸以查看 CSR 與私密金鑰


在進入查看頁面後，往下卷動卷軸則可以查看您的 CSR 憑證請求檔及私密金鑰，您只需要把 CSR 整段複製 ( 包含 -----BEGIN CERTIFICATE REQUEST----- 及 -----END CERTIFICATE REQUEST----- 段落 - 上圖紅框表示處 )，即可到憑證遞送頁面進行申請遞送。

章節 2

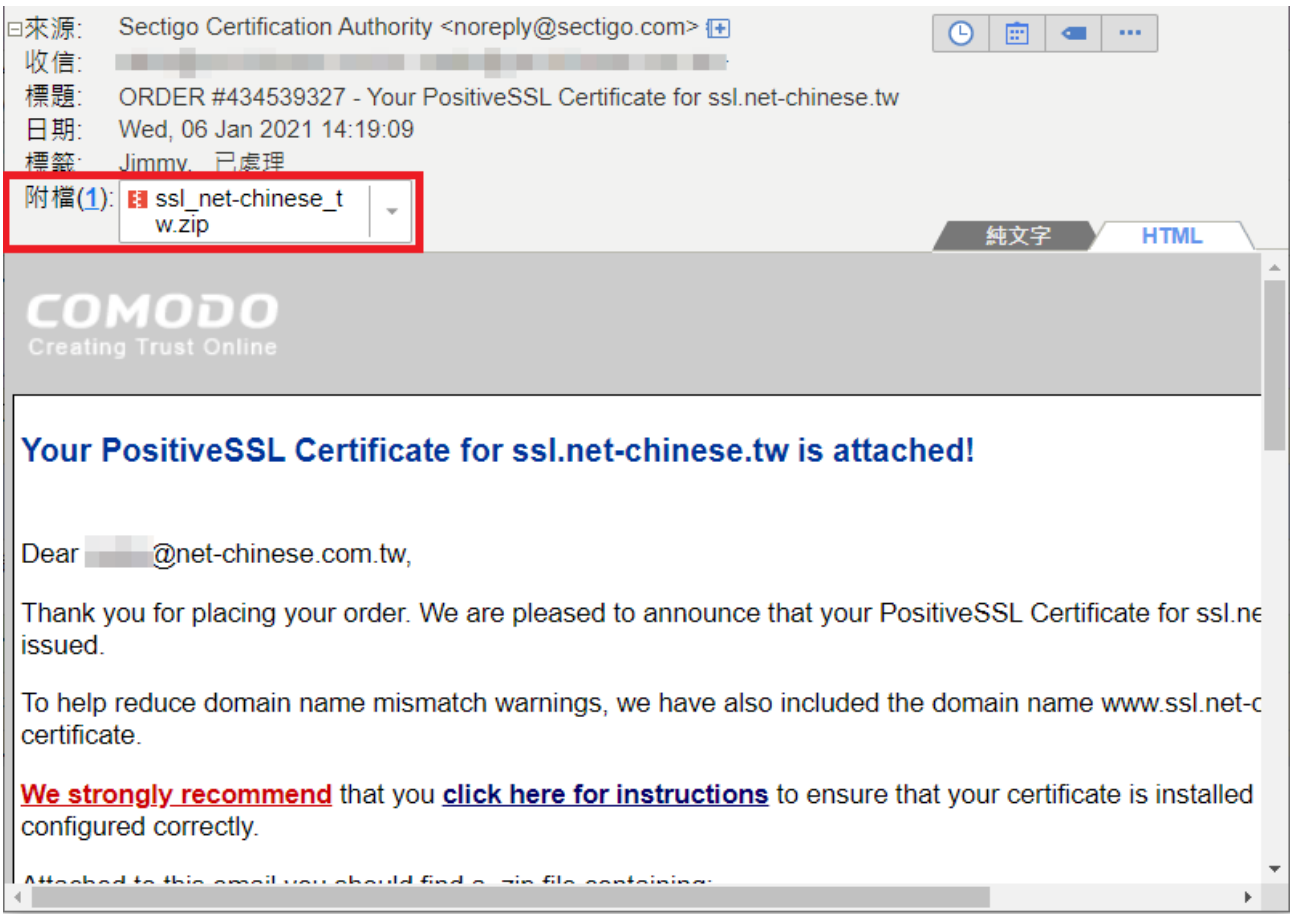
# 在您的 Plesk 中匯入與安裝數位憑證

本章節將帶您操作在您取得憑證後，如何將憑證與中繼憑證透過 Plesk 匯入您的虛擬主機中。

## 一、點選「SSL/TLS」證書圖示→「高級設定」→「憑證名稱」


在您已經收到了憑證，準備將其匯入主機時。請您參照第 1 章生成 CSR 的路徑找到 SSL/TLS 證書的清單列表。

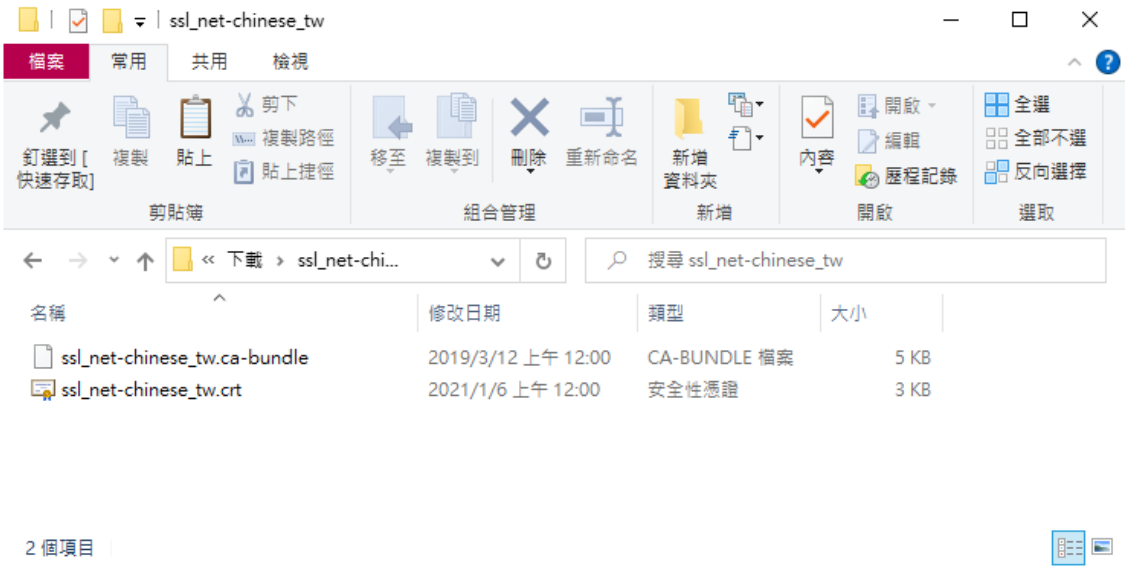
# 二、查看您申請憑證時填入的管理人信箱是否收到發證機構來信

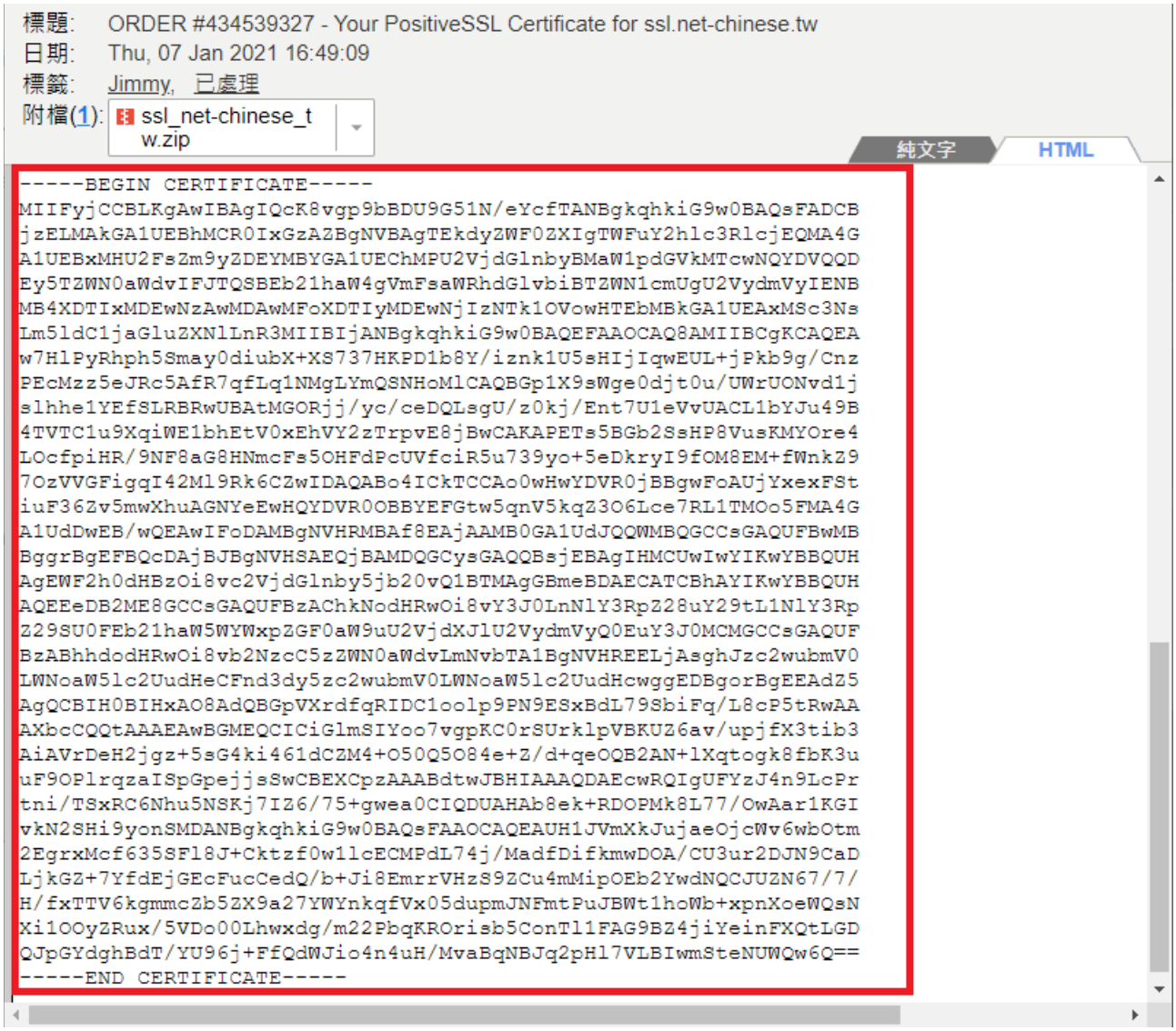



通常在您完成發證機構所要求的驗證程序後 ( 域名驗證 / 組織驗證 )，您會在申請憑證時填寫的管理人信箱收到信件，寄信的內容會依照各家發證機構不同而有不同方式的形式表現，但大致上可以分為兩種類型：

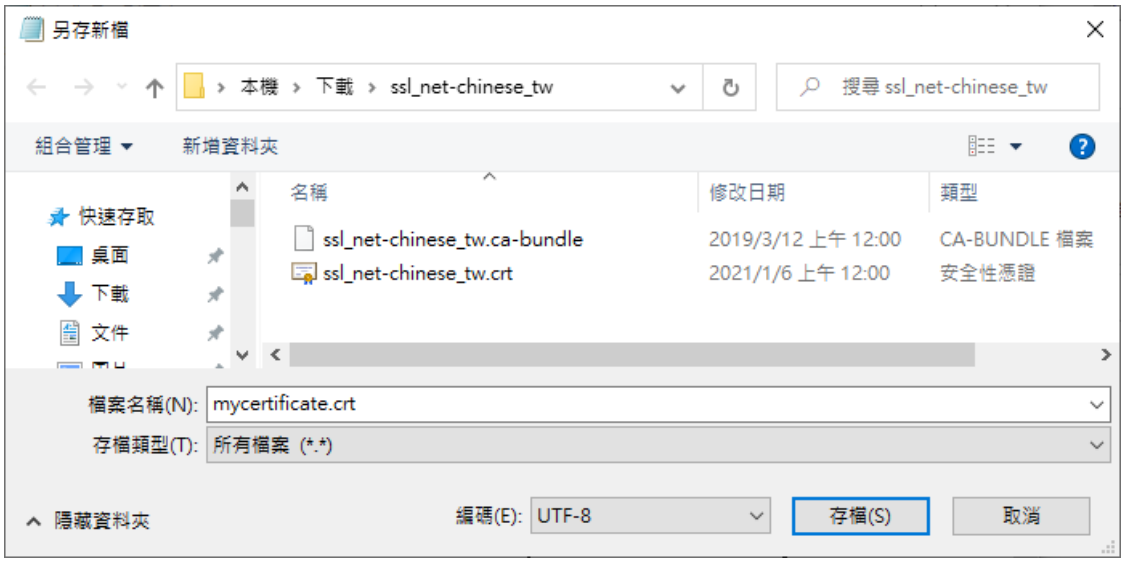
1. 以附件檔夾帶憑證檔案，以壓縮格式寄送 ( 如 .zip 檔 )
2. 以文本格式記出，以文字方式表示。

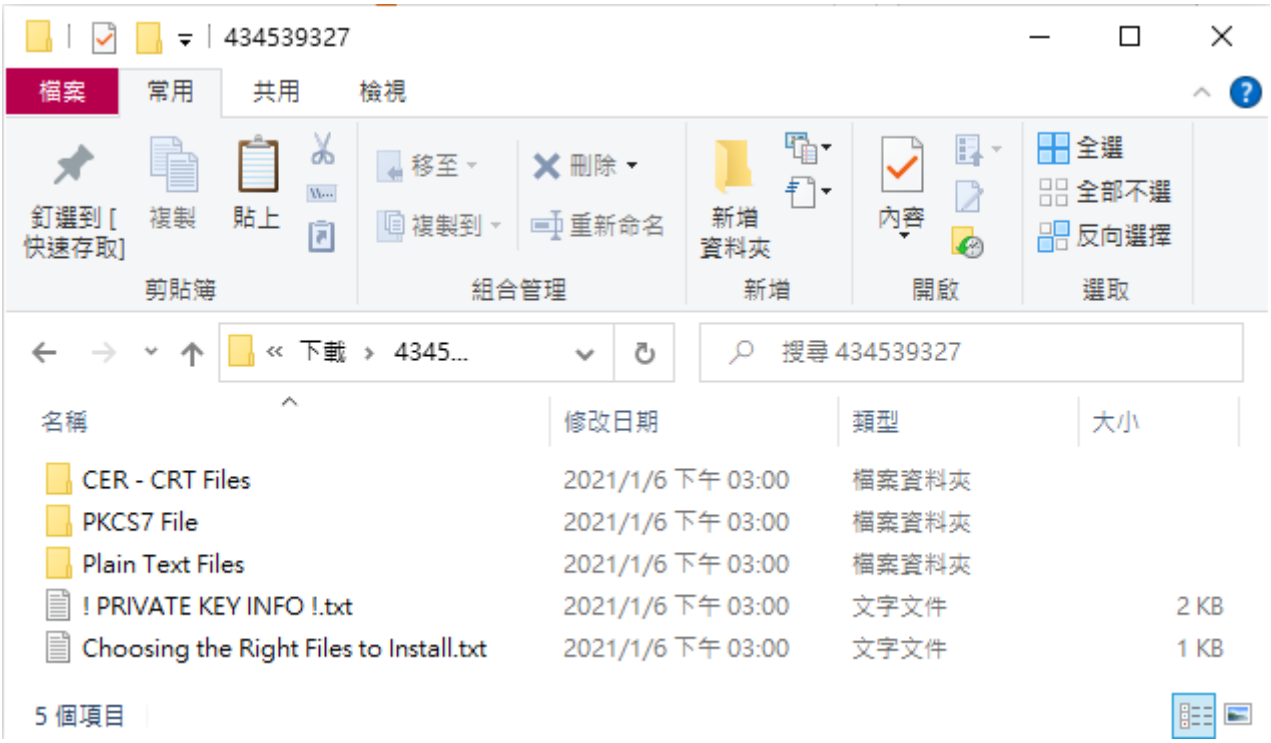
以附件檔夾帶的憑證檔，有時會有較為簡化的方式做附件，如您選擇的伺服器是 Apache 就會給你一個 Bundle 檔 ( 根憑證與中繼憑證信任鏈 ) 和一個網站憑證檔，如果是 IIS 可能就會給你一個 .cer 格式的檔案，如果是 Other 類型可能就會給你完整的根憑證、中繼憑證及網站憑證檔案。( 如下圖 )






如果今天收到的憑證是以文字格式的話，我們可以利用記事本軟體，將憑證給複製 ( 需要包含 -----BEGIN CERTIFICATE----- 及 -----END CERTIFICATE----- 貼入空白的記事本。然後選擇「另存新檔」存檔案時一樣要選擇「所有檔案 (*.*)」，然後檔名您可以自訂，並在檔名最後加上副檔名 (.crt)，編碼的話選擇 ASCII 或是 UTF-8 都可以。






如果您是在網路中文下載的憑證，或是由網中客服寄發給您的憑證，解壓縮之後，您也許會看到的內容如上，以下將針對各資料夾與內容物進行說明。

- CER - CRT Files - 以副檔名為 .CRT 格式的憑證檔案，內含網站憑證、根憑證、中繼憑證。

  Sectigo(COMODO) 品牌
  - xxx_xxx_xx.crt 是網站憑證，其中 xx 會是您的域名。
  - AAA Certificate Service.crt (AddTrust) 為 Sectigo 品牌的根憑證。
  - USERTrustRSAAddTrust.crt 為 Sectigo 品牌的互簽憑證。
  - SectigoRSA(Domain/Organization/Extended)ValidationSecureServerCA.crt 為 Sectigo 品牌的中繼憑證。
  - My_CA_Bundle.ca-bundle 為根憑證、互簽憑證及中繼憑證的三合一信任鏈憑證。

  非 Sectigo 品牌

  未必會有附上中繼憑證及根憑證，但我們可以從關鍵字中查詢。
  - 有 Root 字樣 - 根憑證。
  - 有 Intermediate 字樣 - 中繼憑證。
- PKCS7 File - 加密訊息語法標準檔，用來使用對訊息簽章或加解密，Microsoft Windows 系統、AZURE 雲端服務及 JAVA Tomcat 有機會用到，該檔案只會包含憑證與中繼憑證。
- Plain Text Files - 為 CER - CRT Files 中憑證的純文字文件，您可以利用另存新檔方式儲存成 .crt 格式。
- !PRIVATE KEY INFO !.txt - 憑證檔不含私密金鑰指南及宣告。
- Choosing the Right Files to Install.txt - 用來告知您各資料夾的內容物檔案。

請注意，其內容物會因為您所選擇的品牌、驗證方式而有不同。

## 三、將卷軸拉至憑證上傳處 ( 透過憑證檔上傳 )


## 四、將憑證給放入後按下「上傳證書」

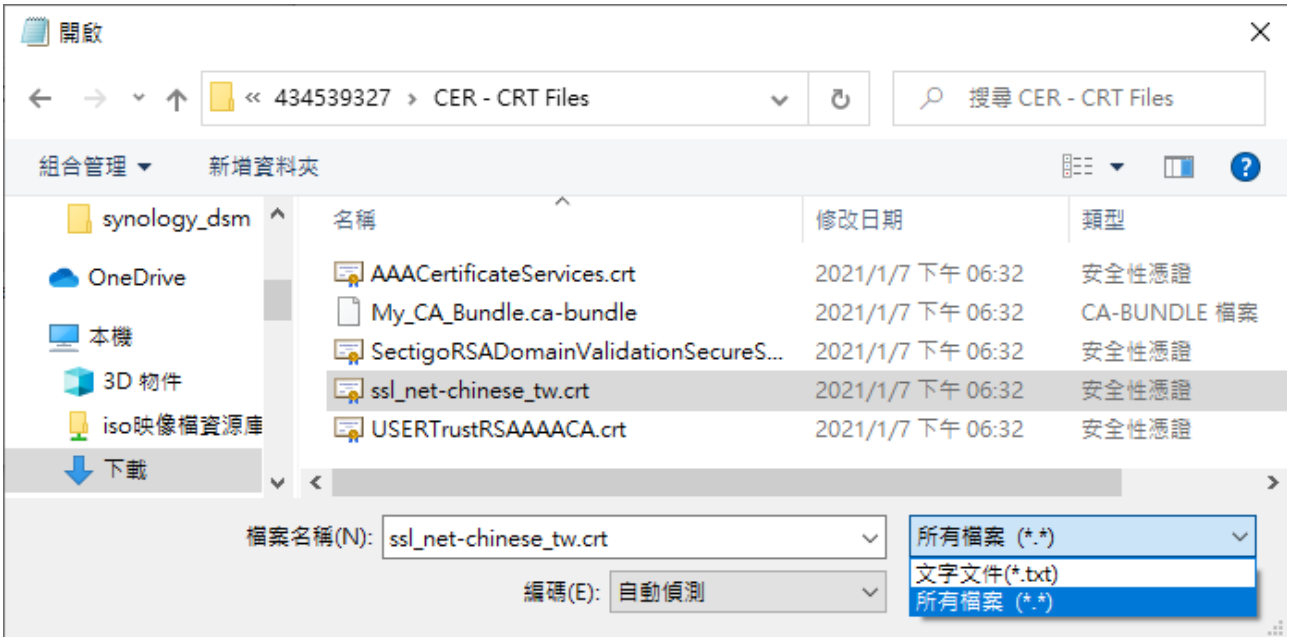

**小提醒：**

上圖提到的 CA 證書 (*-ca.crt)

在本章第 2 點的時候有提到，憑證頒發機構寄給您的憑證中，也許含有信任鏈憑證 (Bundle 檔 )，您這裡可以將 xxx.ca-bundle 檔改成 -ca.crt 後，再行上傳即可。

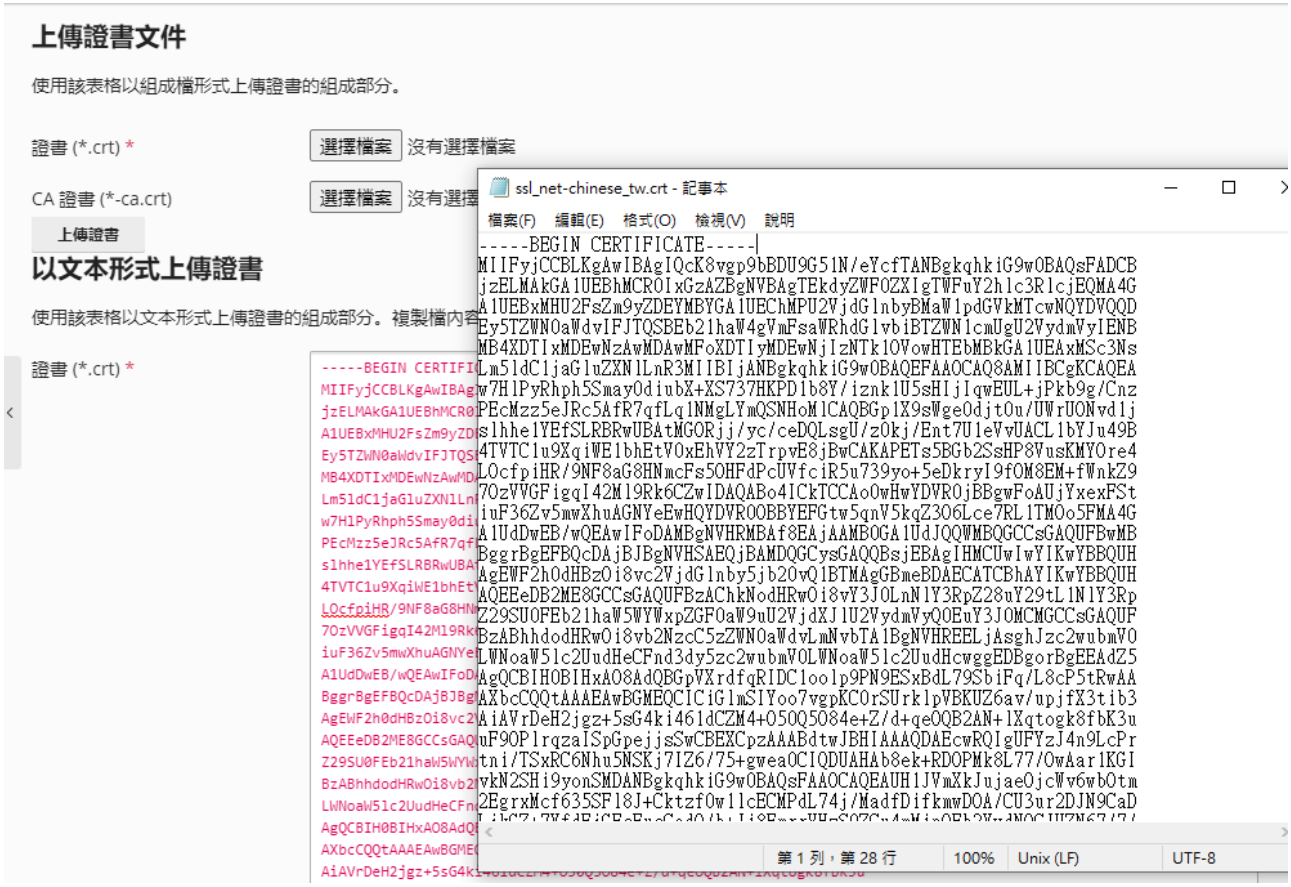
## 五、將卷軸拉至憑證上傳處（透過純文字格式上傳）


## 六、使用記事本或文本工具開啟 .crt 檔案

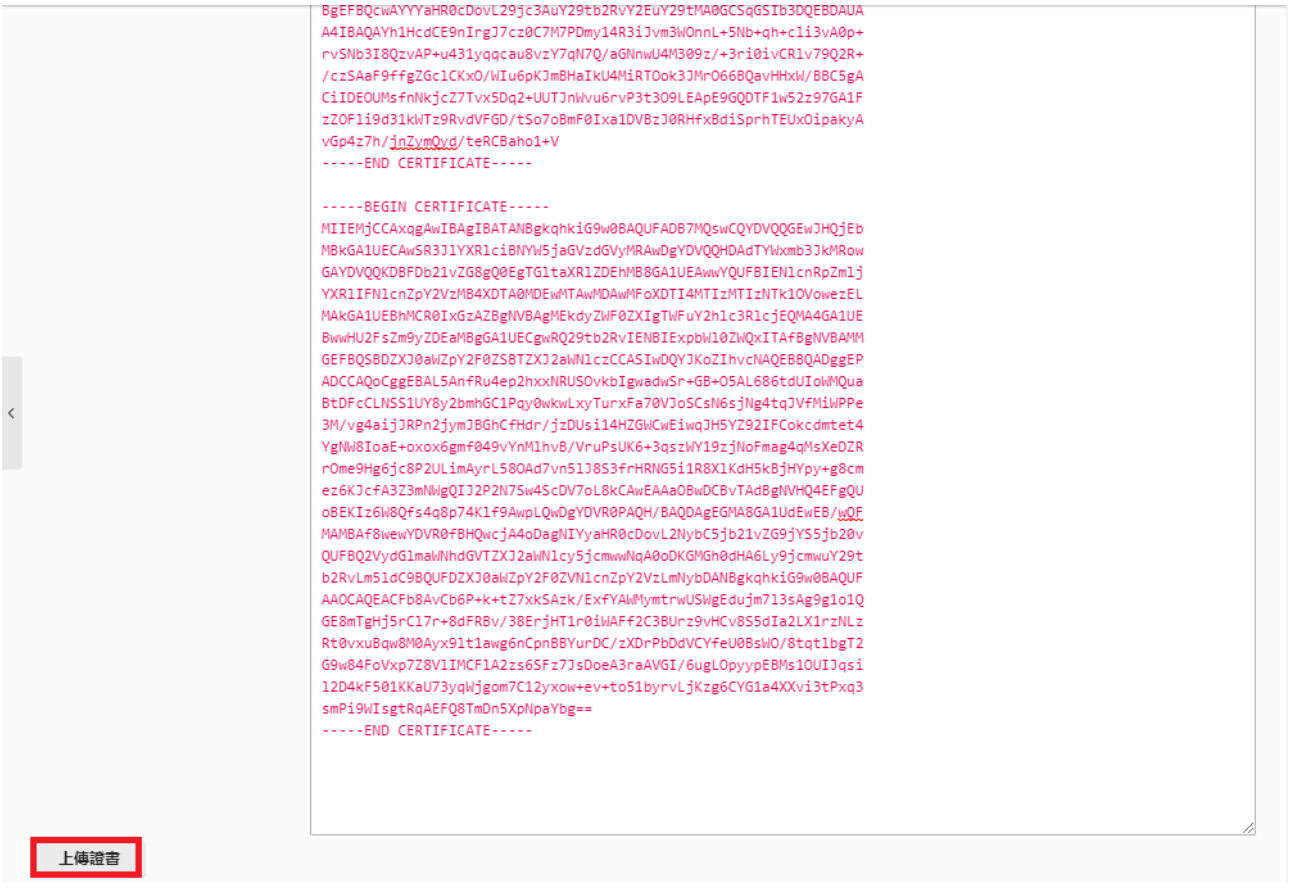



您可以在「透過憑證檔上傳」或「透過純文字格式上傳」兩種方式中擇一使用，但使用純文字格式上傳的時候，需要將「文字文件 (*.txt)」旁邊的小箭頭下拉選擇「所有檔案 (*.*)」，才能看得到 .crt 檔案喔。

# 七、 將文本格式的憑證貼入欄位




# 八、確認貼入後按「上傳證書」



# 九、 確認提示


當憑證已放入後，您會在上面看到綠色的提示，提醒您的憑證已成功匯入，而 RKCA 的圖示也看得出來憑證已放入。

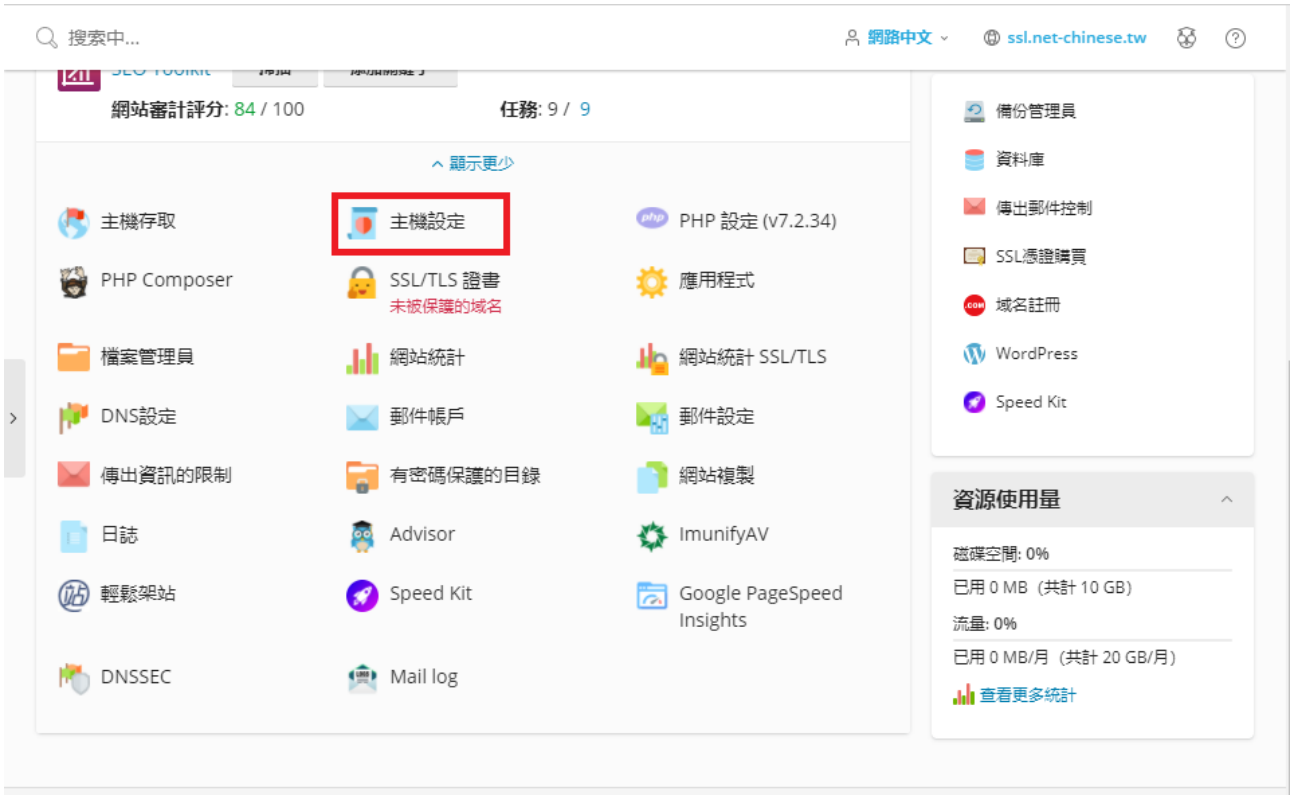
恭喜您，您已完成了憑證匯入的作業。

章節 3

# 將已裝好的憑證與站台繫結

本章節將帶領您操作如何將已匯入主機的憑證給繫結到您的站台上，讓您的網頁可以正常的使用 SSL 憑證。

## 一、點選「網站與域名」選單裡的「主機設定」




在 Plesk 中，主機設定是負責網站起始設定的重要位置，包括網站根目錄的設定、SSL 憑證的設定、強制導轉的設定等等。

# 二、將卷軸拉到「安全」項目並在「證書」項下拉清單選擇憑證


您可以在「安全」項目下面的「證書」一項中選擇你要的憑證。

此外，在「SSL/TLS」支援中顯示的是『啟用』代表您的主機是支援 SSL/TLS 的，如果顯示為停用，則聯絡您的網站管理員或主機提供商。倘若您的主機提供商有下放權限給您，則您直接將其打勾即可。

「SEO 安全 301 永久重定向 ( 從 HTTP 到 HTTPS)」，若為啟用的狀態則代表由網站主機這邊進行強制導轉，將 HTTP 的不安全通道導轉至 HTTPS 安全通道。若為停用的狀態，則代表 HTTP 與 HTTPS 兩者皆是可以使用的。您可以請求網站管理員或是主機提供商由伺服器端幫您設置強制導轉，也可以使用 .httaccess 檔案來控制導轉 ( 後面會介紹 )。倘若您的主機提供商有下放主機控制權限給您，則您直接將其打勾即可。

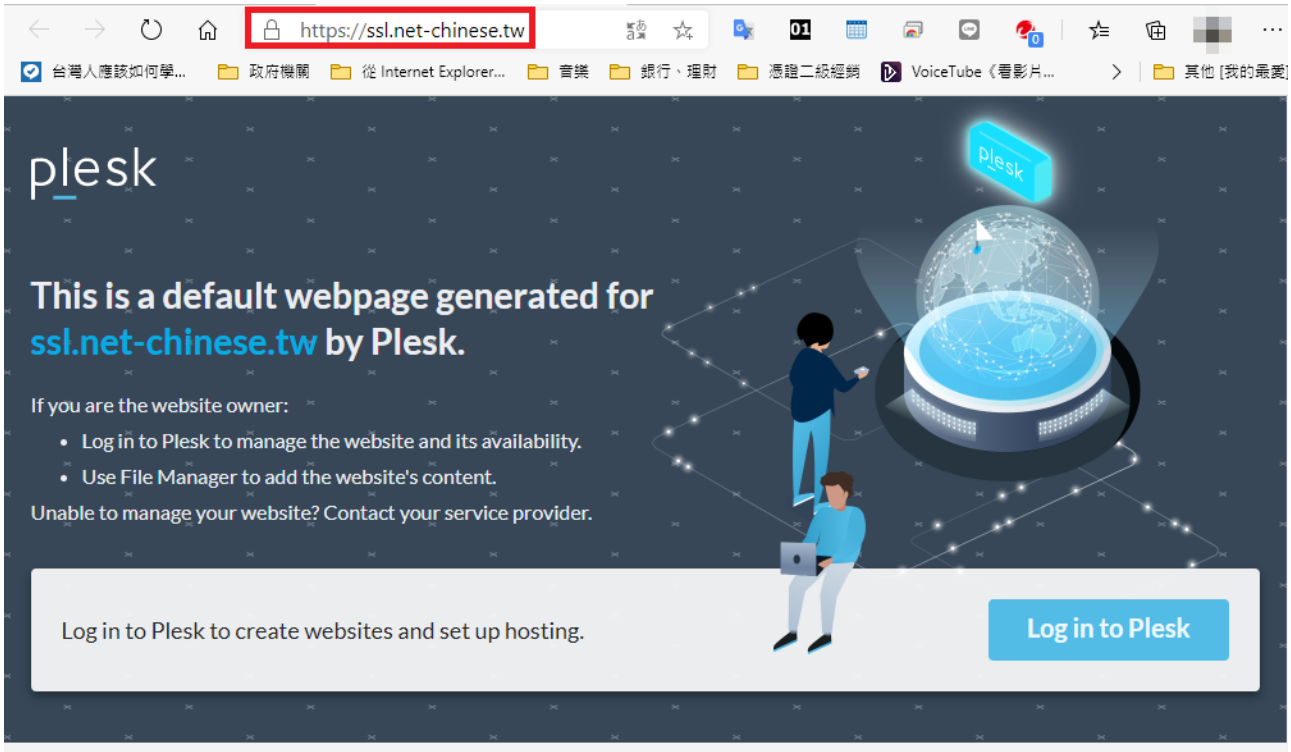
| | |
|---|---|
| SSL/TLS 支援 啟用<br>SEO 安全 301 永久重定向（從 HTTP 到 HTTPS） 停用<br>證書 網站用憑證(2021)（ssl.net-chinese.tw） | 管理員未開放主機管理權限 |

| | |
|---|---|
| ☑ SSL/TLS 支援<br>☐ SEO 安全 301 永久重定向（從 HTTP 到 HTTPS）<br>證書 網站用憑證(2021)（ssl.net-chinese.tw） | 管理員有開放主機管理權限 |

## 三、選取好憑證後，請點選「應用」


## 四、待頁面出現「信息：已成功更新設定」後，點選「確定」離開


## 五、最終畫面測試 ( 如成功會在瀏覽器網址列顯示鎖頭 )



## 六、使用 .htaccess 方式進行導轉

如果，您的主機提供商並沒有下放 Plesk 主機設定的權限給您的話。或許您可以透過考慮透過 .htaccess 檔案來將 http 轉導到 https。( 如果您沒有 .htaccess 檔案的話，則可以用記事本建立一個 )

請在你的網頁的根目錄中的 .htaccess 檔案中加入以下程式碼。
重點：如果在 .htacess 文件中有現有的程式碼，請在上面添加具有類似起始前綴的規則。

```
RewriteEngine On
RewriteCond %{SERVER_PORT} 80
RewriteRule ^(.*)$ https://www.example.com/$1 [R,L]
```

請注意：務必使用你的真實網址取代 www.example.com。

要強制一個特定的網域 (http) 來使用 https，請在你的網頁的根目錄中的 .htaccess 檔案中加入以下程式碼。

```
RewriteEngine On
RewriteCond %{HTTP_HOST} ^example.com [NC]
RewriteCond %{SERVER_PORT} 80 RewriteRule ^(.*)$ https://www.example.com/$1 [R,L]
```

務必使用你想要強制轉為 https 的網址，來取代 example.com，此外你需要用真實網址取代 www.example.com。

**補充說明：**

假使您輸入了 https 卻仍然顯示不安全，則以下提供幾點簡易的狀況排除。

1. 您的防火牆並沒有開啟通訊埠 443。
2. 您的網頁原始碼裡面有使用絕對路徑，且不安全的來源 ( 如外部圖片、影音 )，請檢查您的網頁原始碼裡面是不是有 http:// 的來源文件，若有則請您改用相對路徑，或是直接將 http 更改為 https。

章節 4

# 匯出憑證以供其他主機使用

本章節將帶領您操作如何將已匯入主機的憑證給匯出來，以便您帶著憑證至其他主機上安裝。

## 一、點選「SSL/TLS」證書圖示→「高級設定」→「憑證名稱」

# 二、將卷軸捲動至私密金鑰處

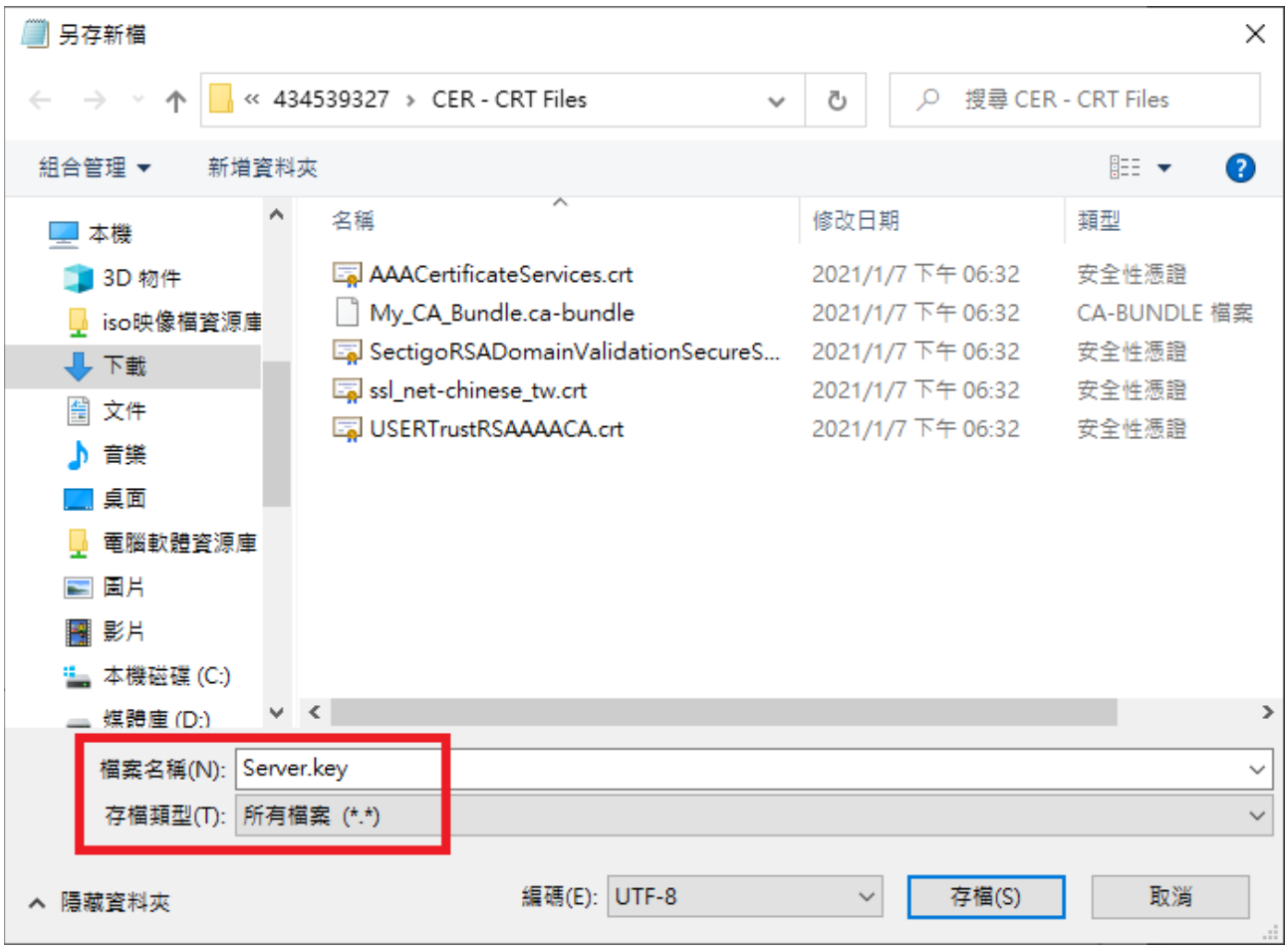
**私密金鑰 (*.key)**

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDDseU/JGGmHlKZ
rLR2K5tf5dLvfsco8PVvxj+LOeTVTmwciMirARQv6M+Rv2D8KfM8RwzPPl4lFzkB
9Hup8urU0yAtiZBI0egyUIBAEanVf2xaB7R2O3S79RatQ4293WOyWGF7VgR9ItEF
HBQEC0wY5GOP/Jz9x4NAuyBT/PSSP8Se3tTV5W9QAIvVtgm7j0HhNVMLW71eqJYT
VuES1XTESFVjbNOum8TyMHAIAoA8ROzkEZvZKwc/xW6woxg6t7gs5x+mIdH/00Xx
obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7l4OSvIj184zwQz59aeRn3s7NVUYWKCojjY
yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfuqe+QkeqyV3XIPKXRL9pFliUm
yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZxT84qWpSNlpdzhaEfYEF9v
beOd8/yZoI9Cyac1NHqNJ7ZvypZAksNxLlgEf6JZGSWofuC8Cljg12xIvT6oy0Py
E5ouZodrOj4us8ehV87eC0lVYgWdAowzbI/tYvtVKx9XuEc8GkP99i184zdygih4
EAuoCooR5nIay6luRGdXMqc4xb2xDJVu+mHSgm40utn6Dr48AuCO/0e8x19iBdDR
xGjXoxMdjPeqBhcqWIDVycFZ1OidkCq3woqIpEptI9kCgYEA+mXXiporWeBR5TFv
2vAi23Dd5GaH3p6C2oIfENhPcITPn9kgYHOxKxTSxLQHpUfmriLNA37SmhB6oQd8
s4enkqU5NrPX5FEkup7Bl9/nj8yDZ1q6W79+gJljsy3LtqUOeMbdqBIfG14XfYDD
NgfYe3n6N7cQuMJmP2RrllBUhZ0CgYEAyBK92UU/2y+VQ3/TA5DF+kzsFbEa8Io+
/RiGaG5gYHFtze5wVbzL3V4Tjlr6uXsoSoD2YlKsWRvZvYBLZYKk4hB7xBoVxZeg
qbL2peomXh4M0tpNY2OonsaiG64K0/UfX1WKB5LyPwfsoPt2uW4nM6adqFKGxpxu
B85kaFWJStMCgYAEAwGzDMlJBVkKjQI3xcUpMuO7NxFSNcPu8ErDIFQVf2s8KmRk
ZzYddJXz5NaChWZiv9f9CFkjcsQkNFSBI9lBdjg2cicxV0N5YfXEEyhIm4Q3cbKu
qaDDOrHoOwGaiYZz1OvUN4YcECPcNOXrxbBoOgoSPnKcIzE0Ls2yeNMB2QKBgGH3
42SvpxwSCbn6rn4RdxAgeH4KshFU8JEIYFBks+alxEnRVsp03zKvbU4IuLr4Vntc
+MieiOw9WfqUBtdXCJv1zFTzHPQbUj2md2Y46L6vYkIhSUHAvAG7bAe3ym+NmOYa
wbMBvoMkwzb0y2bzTFjbXlncx0gbszk5VCtOryKnAoGAOip6XojqucHD3FQMdpdj
9CTAiPSzxHpv/YO3xDaegcntND+xTlL/yAb0p2xluHX/55+jID9njMfeCmzYCn/Y
IghWCNz4Bp30KjuhBX/71QAcb+C7yUV3crPCPtOq8Yjri3KUaTdLTH6RXGiJg4Da
0sDBGeR0A58RWnNuE2ZQINM=
-----END PRIVATE KEY-----
```

# 三、將私密金鑰的內容複製並貼至空白記事本裡

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDDseU/JGGmHlKZ
rLR2K5tf5dLvfsco8PVvxj+LOeTVTmwciMirARQv6M+Rv2D8KfM8RwzPPl4lFzkB
9Hup8urU0yAtiZBI0egyUIBAEanVf2xaB7R2O3S79RatQ4293WOyWGF7VgR9ItEF
HBQEC0wY5GOP/Jz9x4NAuyBT/PSSP8Se3tTV5W9QAIvVtgm7j0HhNVMLW71eqJYT
VuES1XTESFVjbNOum8TyMHAIAoA8ROzkEZvZKwc/xW6woxg6t7gs5x+mIdH/00Xx
obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7l4OSvIj184zwQz59aeRn3s7NVUYWKCojjY
yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfuqe+QkeqyV3XIPKXRL9pFliUm
yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZxT84qWpSNlpdzhaEfYEF9v
beOd8/yZoI9Cyac1NHqNJ7ZvypZAksNxLlgEf6JZGSWofuC8Cljg12xIvT6oy0Py
E5ouZodrOj4us8ehV87eC0lVYgWdAowzbI/tYvtVKx9XuEc8GkP99i184zdygih4
EAuoCooR5nIay6luRGdXMqc4xb2xDJVu+mHSgm40utn6Dr48AuCO/0e8x19iBdDR
xGjXoxMdjPeqBhcqWIDVycFZ1OidkCq3woqIpEptI9kCgYEA+mXXiporWeBR5TFv
2vAi23Dd5GaH3p6C2oIfENhPcITPn9kgYHOxKxTSxLQHpUfmriLNA37SmhB6oQd8
s4enkqU5NrPX5FEkup7Bl9/nj8yDZ1q6W79+gJljsy3LtqUOeMbdqBIfG14XfYDD
NgfYe3n6N7cQuMJmP2RrllBUhZ0CgYEAyBK92UU/2y+VQ3/TA5DF+kzsFbEa8Io+
/RiGaG5gYHFtze5wVbzL3V4Tjlr6uXsoSoD2YlKsWRvZvYBLZYKk4hB7xBoVxZeg
qbL2peomXh4M0tpNY2OonsaiG64K0/UfX1WKB5LyPwfsoPt2uW4nM6adqFKGxpxu
B85kaFWJStMCgYAEAwGzDMlJBVkKjQI3xcUpMuO7NxFSNcPu8ErDIFQVf2s8KmRk
ZzYddJXz5NaChWZiv9f9CFkjcsQkNFSBI9lBdjg2cicxV0N5YfXEEyhIm4Q3cbKu
qaDDOrHoOwGaiYZz1OvUN4YcECPcNOXrxbBoOgoSPnKcIzE0Ls2yeNMB2QKBgGH3
42SvpxwSCbn6rn4RdxAgeH4KshFU8JEIYFBks+alxEnRVsp03zKvbU4IuLr4Vntc
+MieiOw9WfqUBtdXCJv1zFTzHPQbUj2md2Y46L6vYkIhSUHAvAG7bAe3ym+NmOYa
wbMBvoMkwzb0y2bzTFjbXlncx0gbszk5VCtOryKnAoGAOip6XojqucHD3FQMdpdj
9CTAiPSzxHpv/YO3xDaegcntND+xTlL/yAb0p2xluHX/55+jID9njMfeCmzYCn/Y
IghWCNz4Bp30KjuhBX/71QAcb+C7yUV3crPCPtOq8Yjri3KUaTdLTH6RXGiJg4Da
0sDBGeR0A58RWnNuE2ZQINM=
-----END PRIVATE KEY-----
```

# 四、將私密金鑰檔案存檔



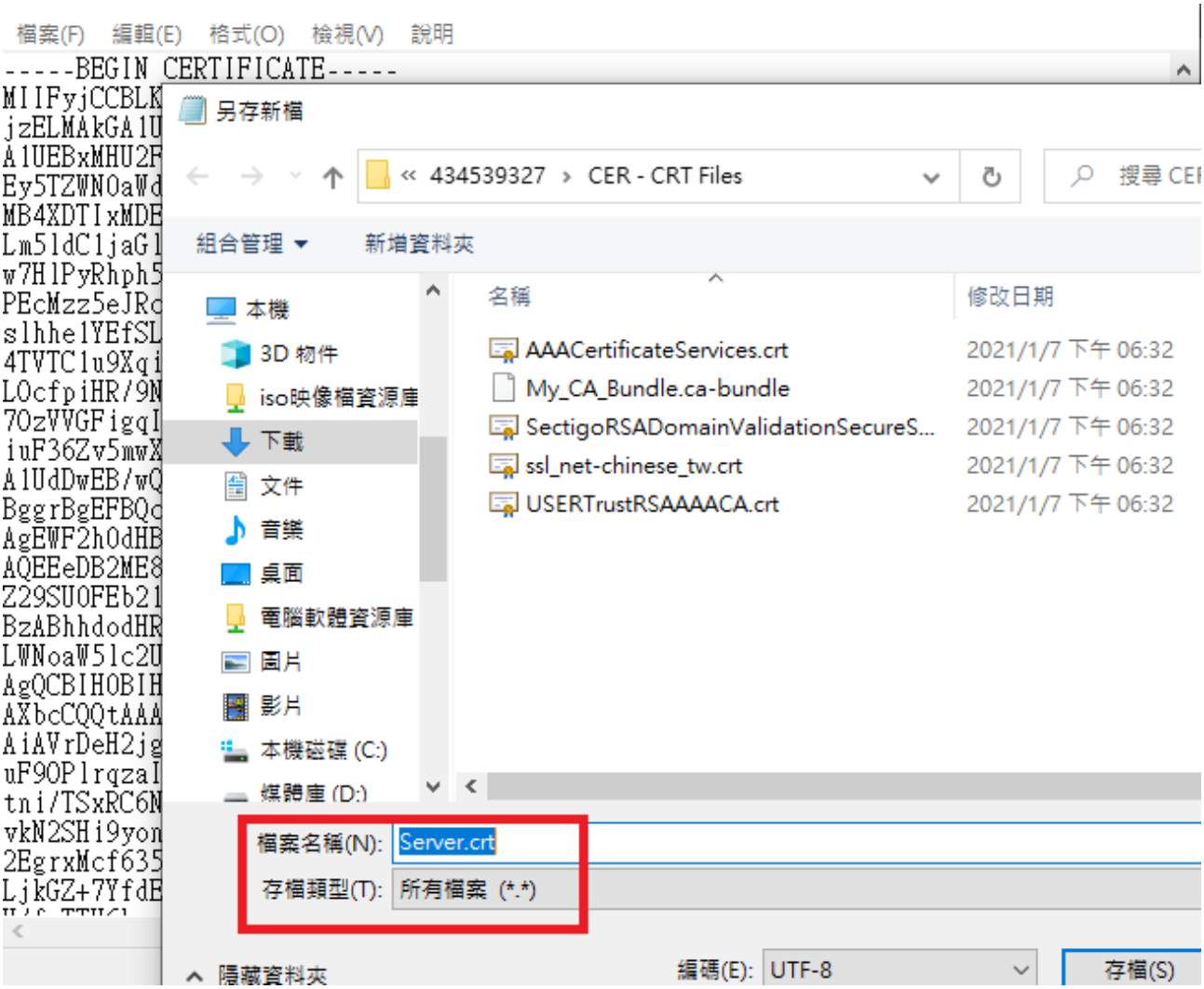

在儲存檔案時，請將存檔類型選擇「所有檔案 (*.*)」，如果未選擇，預設會是以「文字文件 (*.txt)」記事本文本格式儲存；如果是以「所有檔案 (*.*)」格式儲存，請給予一個主檔名後補上 .key 副檔名以方便存檔與辨識。

在大多數的情況下，其實儲存成文字格式或是 .key 私密金鑰檔並沒有太大的差別。因為內碼並沒有經過換算及編碼，兩者也可以用文字工具直接開啟。但若是經過編碼的 .cer/.crt/.der 憑證檔。但像憑證檔單從副檔名是無法直接判別是否經過編碼的。

所以，最好的方式就是 - 直接用記事本打開來看。

## 五、將卷軸捲動至憑證 / 中繼憑證 (-CA 證書 ) 處


## 六、分別複製並存檔



憑證儲存時，同私密金鑰儲存方式一樣，請選擇「所有檔案 (*.*)」，並給予副檔名「.crt」儲存成憑證格式即可，中繼憑證亦同。

## CSR 需要一併複製嗎？

站在資訊安全的角度來說，憑證在每年續用時，比較建議是每年重新生成私密金鑰與憑證，但若如果沒有資訊人員協助您重新生成，您還是可以以現有的 CSR 重新遞送以續用憑證。但是，建議同一組 CSR 最多不要申請超過 2 次以保護您的資訊安全。

若您要一併複制 CSR，則副檔名給予「.csr」儲存即可。

## 多機部署

以上，當您將逐一將私密金鑰、網站憑證、中繼憑證給匯出存檔後，則以該組檔案至別台主機上面進行部署安裝即可。

但是，若您要匯入的是 Microsoft Windows 主機，則必須透過 Open SSL 進行 .PFX 格式的憑證轉換，因為編碼不同不能直接匯入 (Microsoft Windows 採用 PKCS#12 格式編碼 )。

# 附錄 - 注意事項：

- **不要使用特殊字元**
  在申請伺服器憑證時，不要出現某些特殊字元，否則在您提交 CSR 後，可能會出現錯誤。這個錯誤是由於在您產生 CSR 時，輸入的資訊中包含一些特殊字元，如：(@,#,&,!, 等等，例如：您可以將 "&" 用 "and" 代替 )。

- **什麼是主要名稱 (COMMON NAME)**
  在產生 CSR 的時候，主要名稱 ( 又稱憑證名稱 /Common Name)，是一定要填寫的，但我們發現有許多的客戶常常在這個地方出現錯誤，或不符合申請規範。

  主要名稱 (Common Name) 是您的主機名稱 + 網域名稱，例如 www.net-chinese.com.tw 的伺服器憑證是頒發給某一台主機的，而不是一個域名，您的主要名稱（Common Name）必須與您要使用伺服器憑證的主機的全名完全相同，因為 www.domain.com 與 domain.com 是不同的兩台主機，除非您將兩個 A 記錄指向同一台主機。

  另外，用戶在產生 CSR 的時候，若 Domain 為 yourdomain.com 請記得產出 CSR 為 www.yourdomain.com。

  如果您今天申請的是單域名通用型域名，則主機名稱請以「*」代替，在主要名稱中輸入 *.yourdomain.com。

- **不要將 CSR 與 KEY 加密**
  有的人使用一些工具進行 CSR 與私密金鑰的生成 ( 如 OpenSSL 或是 Linux 環境 )，在產出過程中，系統會問您需不需要為 CSR 與私密金鑰加上密碼，請記得留空，不要加密。

- **請保管好您的私密金鑰**
  欲產生 CSR 檔案時，則必然會有一組私密金鑰與之相配對，私密金鑰與憑證是密不可分的。一旦您遺失了私鑰，簽發下來的憑證就無法與之配對了，此時您可能就需要重新產生新的私密金鑰與 CSR 檔案來進行重發憑證，重發憑證是否需要費用，則視發證機構的規定。

  若您有多台主機，需要將憑證佈署在多台主機上，則必須所有的主機使用同一組憑證與私密金鑰。

- **私密金鑰長度必須為 2048 位元 (bit)**
  為加強憑證安全強度，目前發證機構已不再頒發低於 2048 位元的 CSR 憑證提交資訊，所以請您在產生 CSR 時務必選擇 2048 位元的位元長度。