

# CSR 生成與憑證安裝指南 適用於 PLESK

 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

網路伊文	Q。搜索中	11 <del>93</del> . 27 - 2	음 調路中文 ~ (2)	ssl.net-chinese.tw ② ② Powered BY Plesk
□ 網站與域名		へ 顕示更少		() 資料庫
◎ 郵件	📑 主機存取	● 主機設定	꼗 PHP 設定 (v7.2.34)	📔 傳出郵件控制
② 應用程式	PHP Composer	G SSL/TLS 證書	☆ 應用程式	G SSL憑證購買
口 文件	<b>S</b>	未被保護的域名	<b>*</b>	🚥 域名註冊
	── 檔案管理員	網站統計	₩a 網站統計 SSL/TLS	🚯 WordPress
<u>」」</u> 統計	🟴 DNS設定	🔀 郵件帳戶	🙀 郵件設定	🧭 Speed Kit
台 帳戶	< ▲ 傳出資訊的限制	有密碼保護的目錄	網站複製	
🛛 SEO Toolkit		•		資源使用量 ^
WordPress	目話	advisor	TmunifyAV	磁碟空間: 0%
	ն 輕鬆架站	🧭 Speed Kit	Google PageSpeed	已用 0 MB (共計 10 GB)
	M DNSSEC	🙊 Mail log	en Brenne.	流臺: 0% 已用 0 MB/月 (共計 20 GB/月)
		plesk.com	集思廣益 (EN) Cookie	

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。



Q 搜索中	음 調路中文 → ② ssl.	net-chinese.tw & ? plesk
#站舆城名 > ssl.net-chinese.tw > SSL/TLS 證書 > ssl.net-chinese.tw 的 SSL/TLS 證書		
▲ 您的城名未使用有效的 SSL/TLS 證書保護安全。訂購或上傳一個證書以保護您城名	3的安全。	上傳證書 (.pem 文件)
Basic protection for a personal website	^	如果您已經簽發了證書,您可以 在這裡上傳它。
RapidSSL is one of the cheapest certificates provided by DigiCert CA Plugin. A reasonable choice if you need only encryption, but not extended validation. 顧示詳情 即刻開買	技術基於 RapidSSL.	選擇所購買證書的.pem 檔並將 它上傳至您的伺服器。將會把證 書自動地分配給域名。
Business-level protection for a company website	^	高級設定
GeoTrust True BusinessID OV certificate. Strong business-level SSL. Recommended for websites that process confidential or transactional information (for example, e-commerce websites). This certificate shows	技術基於 Geo <b>Trust® 6</b>	

# 三、點選「添加 SSL/TLS 證書」

Q。搜索中	
ssl.net-chinese.tw 的 SSL/TLS 證書	
如果您在該伺服器上創建了證書簽名請求且收到了證書文件,請在此處上傅它。如果您想 證,請點按 <b>添加 SSL/TLS 證書</b> .	要上傳證書和在其它伺服器上生成的私密金鑰對,或生成自簽章憑
給域名添加 SSL/TLS 證書後,需要在網站主機設定中啟用 SSL/TLS 支援並選擇該證書:網	站與域名 > 主機設定(該域名)/> 安全。
在此處上傳證書	
< 證書 (*.crt) * 選擇檔案 沒有選擇檔案	
上傳證書	
☆ ふ如 SSL/TLS 證書     ☆ 保護 Web 郵箱的安全     ☆ 保護郵箱的安全     ☆ 保護	State C.
未找到項目。	
plesk.com  集思廣益 (EN)   C	ookie

安

### 三、依下圖範例使用英文填入相應的資料(比特請選擇 2048)

### 添加 SSL/TLS 證書

證書名稱 *	網站用憑證(2021)				
設定					
使用該表格生成證書請求,從提供商	3購買證書,或者生成自簽章憑證。				
一個請求是包含有關您在表格中指定的域名資訊的 CSR 檔。您可以將此請求發給憑證授權,他們即可為您頒發證書。然後您可以用以下的上傳表格將其上 傳。					
自簽章憑證是由其創建者簽發的身份 全性不高。	d證書。如果您使用此類證書,表示您自己要核實您網站的身份。儘管自簽章憑證允許使用 SSL/TLS,但其可信度低,多				
比特*	2048 🗸				
國家 *	Taiwan 🗸				
省/市/自治區*	Taiwan				
地址(市) *	Taipei City				
組織名稱(公司) *	Net-Chinese Co.,Ltd				
組織部門/分部名稱	Product Dept.				
域名 *	ssl.net-chinese.tw				
電子郵件 *	service@net-chinese.com.tw				
請求自簽名					

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

網站與域名 > ssl.net-chinese.tw 的 SSL/TLS 證書 ✓ 信息: SSL/TLS 證書已簽發。若要令其運行工作,請分配證書以保護域名、郵件或 web 郵箱的安全。 如果您在該伺服器上創建了證書簽名請求且收到了證書文件,請在此處上傳它。如果您想要上傳證書和在其它伺服器上生成的私密金鑰對,或生成自簽章憑 證,請點按添加 SSL/TLS 證書. 給域名添加 SSL/TLS 證書後,需要在網站主機設定中啟用 SSL/TLS 支援並選擇該證書:網站與域名 > 主機設定(該域名)/> 安全。 在此處上傳證書 選擇檔案 沒有選擇檔案 語書 (\*.crt) \* < 上傳證書 Q 🕂 添加 SSL/TLS 證書 🕅 保護 Web 郵箱的安全 🕥 保護郵箱的安全 🔀 移除 條目共計1 每頁顯示條目: 10 25 100 所有 🗌 R K С А 名稱↑ 已使用 網站用憑證(2021) 🔎 🔳 🔳 0 🤳 條目共計1 每頁顯示條目: 10 25 100 所有 plesk.com 集思廣益(EN) Cookie

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

網站與域名 > ssl.net-chinese.tw > SSL/TLS 證書 >

#### 更改 SSL/TLS 證書 網站用憑證(2021) 的屬性

證書名稱 \*

網站用憑證(2021)

#### 重命名

設定

使用該表格生成證書請求,從提供商購買證書,或者生成自簽章憑證。

一個請求是包含有關您在表格中指定的域名資訊的 CSR 檔。您可以將此請求發給憑證授權,他們即可為您頒發證書。然後您可以用以下的上傳表格將其上 傳。

自簽章憑證是由其創建者簽發的身份證書。如果您使用此類證書,表示您自己要核實您網站的身份。儘管自簽章憑證允許使用 SSL/TLS,但其可信度低,安 全性不高。

比特	2048
國家	Taiwan
省/市/自治區	Taiwan
地址(市)	Taipei City
組織名稱(公司)	Net-Chinese Co.,Ltd
組織部門/分部名稱	Product Dept.
域名	ssl.net-chinese.tw
電子郵件	service@net-chinese.com.tw

CSR

#### ---BEGIN CERTIFICATE REQUEST----

MIIC+DCCAeACAQAwgbIxCzAJBgNVBAYTAlRXMQ8wDQYDVQQIDAZUYWl3YW4xFDAS  ${\tt BgNVBAcMC1RhaXBlaSBDaXR5MRwwGgYDVQQKDBNOZXQtQ2hpbmVzZSBDby4sTHRk}$ MRYwFAYDVQQLDA1Qcm9kdWN0IER1cHQuMRswGQYDVQQDDBJzc2wubmV0LWNoaW51 c2UudHcxKTAnBgkqhkiG9w0BCQEWGnNlcnZpY2VAbmV0LWNoaW5lc2UuY29tLnR3 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw7HlPyRhph5Smay0diub X+XS737HKPD1b8Y/iznk1U5sHIjIqwEUL+jPkb9g/CnzPEcMzz5eJRc5AfR7qfLq 1NMgLYmQSNHoMlCAQBGp1X9sWge0djt0u/UWrUONvd1jslhhe1YEfSLRBRwUBAtM GORjj/yc/ceDQLsgU/z0kj/Ent7U1eVvUACL1bYJu49B4TVTC1u9XqiWE1bhEtV0 xEhVY2zTrpvE8jBwCAKAPETs5BGb2SsHP8VusKMYOre4LOcfpiHR/9NF8aG8HNmc Fs50HFdPcUVfciR5u739yo+5eDkryI9f0M8EM+fWnkZ970zVVGFigqI42Ml9Rk6C ZwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAFNTBWrdlRS/ygQxdBN6LK+M66SF SKMXj1bifEnWfwHGj4RX3ZJ9zN2MfJpAMo2+EQGMvBOzqh7KTm8+PUoIWJxVgdv0 Ni5UM1HPapSX9HtzzgtLMJvw8N2WBfn0f7nq9ZhXJL3xhVFKPp05h2alWvr77bmr wxnIrXc/Mldg22nP0JWu/FTwzGfs5Wpbjzp/Oq1zawmUI9HO3dBFsPoMO2fwamTK rcTSegZ+G169opFCCElCCFkQ8wgG73tJLzpwL4E34XN73jb68gus/2aSUe7A2YBE Mjq3HOQAigSaMeetG90zzekEWCc4MmwbP3qmMCuHim3V2gWfimGBq/eJbQg= ----END CERTIFICATE REQUEST-----

#### 私密金鑰 (\*.key)

-----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDDseU/JGGmHlKZ rLR2K5tf5dLvfsco8PVvxj+LOeTVTmwciMirARQv6M+Rv2D8KfM8RwzPPl4lFzkB 9Hup8urU0yAtiZBI0egyUIBAEanVf2xaB7R2O3S79RatQ4293WOyWGF7VgR9ItEF HBQEC0wY5GOP/Jz9x4NAuyBT/PSSP8Se3tTV5W9QAIvVtgm7j0HhNVMLW71eqJYT VuES1XTESFVjbNOum8TyMHAIAoA8ROzkEZvZKwc/xW6woxg6t7gs5x+mIdH/00Xx obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7l4O5vIj184zwQz59aeRn3s7NVUYWKCojjY yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfuqe+QkeqyV3XIPKXRL9pFliUm yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZxT84qWpSNlpdzhaEfYEF9v

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。



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。



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),您曾在甲請憑證時填寫 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)

- I 🎝	<b>-</b> =	ssl_net-chinese_tw							-		×
檔案	常用	共用 檢視									~ ?
★ 釘選到[ 快速存取]	複製	<ul> <li>         前下         減 前下         減製路徑         前上         前上捷徑     </li> </ul>	<b>修</b> 至	複製到	× ⊪⊮	重新命名	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	>	[] 開啟 → ]) 編輯 ] 優程記錄	計 全選 計 全部 <sup>2</sup> □ 全部 <sup>2</sup> □ 反向	不選 異擇
	剪	貼簿		組合	合管理		新增		開啟	選取	
← → ヾ ↑ 📙 « 下載 > ssl_net-chi		,	ٽ v	Q	搜尋 ssl_net-cl	ninese_tw					
名稱		^		修改日期	玥		類型	7	כי]י		
📄 ssl_net-chinese_tw.ca-bundle 🙀 ssl_net-chinese_tw.crt		2019/3, 2021/1,	/12 上午 /6 上午	12:00 12:00	CA-BUNDLE 札 安全性憑證	當案	5 KB 3 KB				

#### SSL/TLS 數位憑證安裝教學 Plesk 虛擬主機管理系統



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。

🗐 另存新檔		×
$\leftarrow \rightarrow \checkmark \uparrow$	> 本機 > 下載 > ssl_net-chinese_tw	⑦ 没 授尋 ssl_net-chinese_tw
組合管理 ▼	新増資料夾	≣≕ ◄ ?
<ul> <li>≱ 快速存取</li> <li>■ 桌面</li> <li>↓ 下載</li> <li>○件</li> </ul>	▲ 名稱 Ssl_net-chinese_tw.ca-bundle 家sl_net-chinese_tw.crt	修改日期         類型           2019/3/12 上午 12:00         CA-BUNDLE 檔案           2021/1/6 上午 12:00         安全性憑證
□□ □□ 檔案名稱( 存檔類型	(N):         mycertificate.crt           (T):         所有檔案 (*.*)	> ~ ~
∧ 陽藏資料夾	編碼(E): UTF-8	✓ 存檔(S) 取消



5 個項目

....

SSL/TLS 數位憑證安裝教學 Plesk 虛擬主機管理系統

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)

#### 上傳證書文件

使用該表格以組成檔形式上傳證書的組成部分。

證書 (*.crt) *
--------------

上傳證書

選擇檔案沒有選擇檔案

選擇檔案 沒有選擇檔案

#### 以文本形式上傳證書

使用該表格以文本形式上傳證書的組成部分。複製檔內容並貼上到相應的欄位。

	證書 (*.crt) *	
<		
	CA 證書 (*-ca.crt)	
	上傳證書	

### 四、將憑證給放入後按下「上傳證書」

使用該表格以組成檔形式上傳證書	的組成部分。
證書 (*.crt) *	選擇檔案 ssl_net-chinese_tw.crt
CA 證書 (*-ca.crt)	選擇檔案 My_CA_Bundle-ca.crt
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)

#### 上傳證書文件

使用該表格以組成檔形式上傳證書的組成部分。

證書 (*.crt) *	選擇檔案沒有選擇檔案
CA 證書 (*-ca.crt)	選擇檔案 沒有選擇檔案
上傳證書	
以文本形式上傳證書	

使用該表格以文本形式上傳證書的組成部分。複製檔內容並貼上到相應的欄位。

證書 (*.crt) *	
<	
CA 證書 (*-ca.crt)	
上傳證書	

### 六、使用記事本或文本工具開啟 .crt 檔案

🧾 開啟			×
← → · ↑ 🔒 « 434	539327 → CER - CRT Files 🗸 🗸	ひ  ノ の  授 尋 CER	- CRT Files
組合管理 ▼ 新増資料夾	i de la companya de l		
synology_dsm 🔺	名稱 ^	修改日期	類型
<ul> <li>OneDrive</li> </ul>	🔄 AAACertificateServices.crt	2021/1/7 下午 06:32	安全性憑證
-1-100	My_CA_Bundle.ca-bundle	2021/1/7 下午 06:32	CA-BUNDLE 檔案
💻 本機	🔄 SectigoRSADomainValidationSecureS	2021/1/7 下午 06:32	安全性憑證
🔰 3D 物件	🔄 ssl_net-chinese_tw.crt	2021/1/7 下午 06:32	安全性憑證
🚽 iso映像檔資源庫	🔄 USERTrustRSAAAACA.crt	2021/1/7 下午 06:32	安全性憑證
🕹 🗸 🗸	C		>
檔案名種	稱(N): ssl_net-chinese_tw.crt	→ 所有檔案 (*.*)	~
	編碼(E): 自動偵測	文字文件(*.txt)	

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

#### 上傳證書文件

使用該表格以組成檔形式上傳證書的組成部分。

證書 (*.crt) *	選擇檔案 沒有選擇檔案		
CA 證書 (*-ca.crt)	選擇檔案 沒有選擇 🥘 ssl_net-chinese_tw.crt - 記事本	-	>
上傳證書			
以文本形式上傳證書	MIIFyjCCELKgdwIBAgIQcK8vgp9bBDU9G51N/eYcfTANBgkqhkiG9w0BAQsFADCB izELWAkGA1UEBhMCR0IxGzAZBeNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlciEOMA4G		
使用該表格以文本形式上傳證書的	組成部分。複製檔内容在MHU2FsZm9yZDEYMBYGAIUEChMPU2VjdG1nbyBMaW1pdGVkMTcwNQYDVQQD 組成部分。複製檔内容 EySTZWNOaWdwIFJTQSBEb21haW4gVmFsaWRhdG1wbiBTZWN1cmUgU2VydmVyIENB MB4XDT1xMDEwNzAwMDAwMFoXDT1yMDEwNilzNTk10VowHTEbMBkGA1UEAxMSc3Ns		
證書 (*.crt) *	BEGIN CERTIFIL m51dC1 jaG1uZXN1L nR3M1 IB1 jANBgkqhkiG9w0BAQEFAAOCAQ8AM1 IBCgKCAQEA		
<	jzELMAKGAIUEBMKCROPECM2Z5EIRc5AfR7qfLqINMgLYmQSNHoMICAQBGpIX9sWgeOdjtOu/UWrUOWvdIj AluEBvMHU2=z7mgvZnkslhkelYEfSLRERwUBAtMGORij/vc/ceDOLsgU/z0ki/Ent701eVvUACL1bYJu49B		
	EySTZWW0aWdyIFJTQS(4TVTC1u9XqiWE1bhEtV0xEhVY2zTrpvE8jBwCAKAPETsSBGb2SsHP8VusKMY0re4		
	Lm51dC1jaG1uZWILm 70zVVGFigq142M19R6CZWIDAQABo4ICKTCCAoOWHWYDWR0jBBgwFoAUjYxexFSt		
	w7H1PyRhph55may@di.10.522v3liwaRukdW1eEwiQ1DVR00BD1EFGW0QfW9kQ2500Cce7kD110057mA46 PEcMzz5eJRc5AfR7qfA1UdDwEB/wQEAwIFoDAMBgNVHRMB4f8EAjAAMB0GA1UdJQQWMBQGCCGGAQUFBwMB		
	slhhelYEFSLRBRwUBA BggTbgEFbQCDAJBJbgNVH5AEQJBAMDQGJ9S0AQQBSJEBAgIHMCUVIWTIKWTBBQUH ATVICUV9vgHEIbbET AgEWF2h0dHB2018vc2VjdGlnby5jb20vQlBTMAgGBmeBDAECATCBhAYIKwYBBQUH		
	LOCEPTHE/9NF8aG8HWZ29SU0FEb21haW5WYWxpZGF0aW9uU2VjdXJ1U2VydmVyQ0EuY3J0MCMGCCsGAQUF		
	70zVVGF1gq142M19RkBzABhhdodHRwOi8vb2NzcC5zZWNOaWdvLmNvbTA1BgNVHREELjAsghJzc2wubmV0 iuF36Zv5mwXhuAGNYeLWNoaW51c2UudHeCFnd3dv5zc2wubmV0LWNoaW51c2UudHcwggEDBgorBgEEAdZ5		
	A1UdDwE8/wQEAwIFoDAgQCBIH0BIHxA08AdQBGpVXrdfqRIDC1oolp9PN9ESxBdL79SbiFq/L8cP5tRwAA BegrBgEFB0cDA18JBgdX7bcC00tAAAFAwBGWE0CIC1G1wSIXoo7wpxC0rSUrk1pVBKUZ6ay/npifX3tib3		
	AgEWF2h0dHBz018vc2lA iAV rDeH2 jgz+5sG4k i461dCZM4+050Q5084e+Z/d+qe0QB2AN+1Xqtogk8fbK3u		
	Z29SU0FEb21hawSWYnthi/TSxRC6Nhu5NSKJS7Z6/75+gwea0CIQDUHHAb8ek+RD0PMk8L77/0wAarIKGI		
	BzABhhdodHRwOi8vb21VKNZ5h19yon5MUANBgKqnK1G9WUBAUSFAAUCAQEAUHIIVmXkJujaeUjCWV6WbUtm LWNoaW51c2UudHecFn2EgrxMcf635SF18J+Cktzf0w11cECMPdL74j/MadfDifkmwDOA/CU3ur2DJN9CaD		
			>
	第1列,第28行 100% Unix (LF) AiAVrDeH2jgz+5sG4k1++0±002000+c+±2/01400002±HiT±AqC0002±HiT±AqC000x00	UTF-8	_

# 八、確認貼入後按「上傳證書」

BgEFBQcwAYYYAHR0cDovL29jc3AuY29tb2RvY2EuY29tMA0GCSqGSIb3DQEBDAUA A4IBAQAYh1HcdCE9nIrgJ7cz0C7M7PDmy14R3iJvm3WOnnL+5Nb+qh+cli3vA0p+ rvSNb3I8QzvAP+u431yqqcau8vzY7qN7Q/aGMnwU4M309z/+3ri0ivCR1v79Q2R+ /czSAe9ffgZGC1CKxO/WIu6pKJmBHaIKU4MiRTOok3JMrO668QavHHxW/BBC5gA CiIDEOUMsfnNkjc27Tvx5Dq2+UUTJnWvu6rvP3t309LEApE96QDTF1w52z97GA1F z20F1i9d31kWT29RvdVFGD/tSo70BmF0Ixa1DVBzJ0RHfxBdiSprhTEUxOipakyA vGp427h/jnZymQvg/teRCBaho1+V ----END CERTIFICATE-----

#### -----BEGIN CERTIFICATE-----

MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb MBkGA1UECAwSR3J1YXR1ciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow GAYDVQQKDBFDb21vZG8gQ0EgTG1taXR1ZDEhMB8GA1UEAwwYQUFBIEN1cnRpZmlj YXR1IFN1cnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE BwwHU2FsZm9yZDEaMBgGA1UECgwRQ29tb2RvIENBIExpbW10ZWQxITAFBgNVBAMM GEFBQSBDZXJ0aWZpY2F0ZSBTZXJ2aWN1czCCASIwDQYJKoZIhvcNAQEBBQADggEP ADCCAQoCggEBAL5AnfRu4ep2hxxNRUSOvkbIgwadwSr+GB+05AL686tdUIoWMQua BtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe 3M/vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4 YgNW8IoaE+oxox6gmf049vYnM1hvB/VruPsUK6+3qszWY19zjNoFmag4qMsXeDZR rOme9Hg6jc8P2ULimAyrL58OAd7vn51J8S3frHRNG5i1R8X1KdH5kBjHYpy+g8cm ez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQU oBEKIz6W8Qfs4q8p74K1f9AwpLQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQF MAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20v QUFBQ2VydG1maWNhdGVTZXJ2aWN1cy5jcmwwNqA0oDKGMGh0dHA6Ly9jcmwuY29t b2RvLm51dC9BQUFDZXJ0aWZpY2F0ZVN1cnZpY2VzLmNybDANBgkqhkiG9w0BAQUF AAOCAQEACFb8AvCb6P+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm713sAg9g1o1Q GE8mTgHj5rCl7r+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLz Rt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BsW0/8tqt1bgT2 G9w84FoVxp7Z8V1IMCF1A2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs10UIJqsi 12D4kF501KKaU73yqWjgom7C12yxow+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3 smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==

-----END CERTIFICATE-----

### 九、確認提示

#### 網站與域名 >

### ssl.net-chinese.tw 的 SSL/TLS 證書

	✓ 信息: SSL/TLS 證書已被成功更新。									
1	—————————————————————————————————————									
1	給域名添加 SSL/TLS 證書後,需要在網站主機設定中啟用 SSL/TLS 支援並選擇該證書 <b>:網站與域名 &gt; 主機設定</b> (該域名)/> <b>安全。</b>									
	在山	L處.	上傳	證書	t					
<	證書 (*.crt) * 選擇檔案 沒有選擇檔案									
						上傅證書				
	÷	添加。	SSL/TL	S 證書		⑦ 保護 Web 郵箱的安全 ◎ 保護郵箱的安全 ※ 移除	Q			
	條目共	喆1					每頁顧示條目: 10 25 100 所有			
		R	к	C	А	名稱↑	已使用			
			P	5		網站用憑證(2021)	0 🖡			
	條目共	打 1					每頁顯示條目: 10 25 100 所有			
	plesk.com 年思慶益 (FN) Cookie									

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。



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。

搜索中		合 調路	中文 × 🕲 ssl.net-chinese.tw 🚷 🤅
網站審計評分: 84 / 100	任務:9/9	)	2 備份管理員
	∧ 顯示更少		■ 資料庫
📑 主機存取	● 主機設定	应 PHP 設定 (v7.2.34)	📔 傳出郵件控制
PHP Composer	G SSL/TLS 證書	☆ 應用程式	🧾 SSL憑證購買
	未被保護的域名	×	🚥 域名註冊
── 檔案管理員	網站統計	<mark>↓</mark> 細站統計 SSL/TLS	🚯 WordPress
<b>P</b> DNS設定	🔀 郵件帳戶	郵件設定	🧭 Speed Kit
🖌 傳出資訊的限制	🗧 有密碼保護的目錄	1 網站複製	次还在田目
日誌	advisor	🚯 ImunifyAV	貧
			磁碟空間: 0%
100 輕鬆架站	💉 Speed Kit	Google PageSpeed	ご用 0 MB (共計 10 GB)
M DNSSEC	💼 Mail log		D) (共計 20 GB/月)

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

Q。搜索中	
您可在此配置網站主機設定並選携	星網站可用的功能。
主機類型	網站
網站狀態	活動 [更改]
文檔根目錄	
偏好域名	○ www.ssl.net-chinese.tw
	○ ssl.net-chinese.tw
	◎ 無
	選擇將要通過 SEO 安全 HTTP 301 重定向將網站訪客重定向到的 URL(有或無 www. 首碼)。
安全	
要保證您網站的交易安全,可使用 SSL/TLS 證書,最後在下面選擇語	fl SSL/TLS 協定,該協定可加密所有資料並通過安全的連接來傳輸資料。要啟用 SSL/TLS 支援,請在網站上安裝 證書。
SSL/TLS 支援	◇ 啟用
SEO 安全 301 永久重定向(從 HTTP 到 HTTPS)	● 停用
證書	網站用憑證(2021)(ssl.net-chinese.tw) 💙
	網站用慿證(2021)(ssl.net-chinese.tw)
網站腳本和統計	Default Certificate (自簽)(其他庫)
	未選定

指定可田 Web 伺服簫解釋、執行或處理的程式設計相指令碼語言。 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	
SEO 安全 301 永久重定向(從 HTTP 到 HTTPS)	●停用	管理員未開放主機管理權限
證書	網站用憑證(2021) (ssl.net-chinese.tw) ∨	
✔ SSL/TLS 支援		
□ SEO 安全 301 永久重定向(公	는 HTTP 到 HTTPS)	管理員有開放主機管理權限
證書	網站用憑證(2021)(ssl.net-chinese.tw)	

### 三、選取好憑證後,請點選「應用」

	Q、搜索中		음 <b>網路中文</b>	<ul> <li>Ssl.net-chinese.tw</li> </ul>	8	?
	SSL/TLS 支援	◇ 啟用				
	SEO 安全 301 永久重定向(從 HTTP 到 HTTPS)	● 停用				
	證書	網站用憑證(2021) (ssl.net-chinese.tw) 🗸				
	網站腳本和統計					
	指定可由 web 伺服器解釋、執行或	成處理的程式設計和指令碼語言。				
>	PHP支援 (PHP 版本         7.2.34           注意更改 PHP 處理常式類型可能會中斷           瞭解如何選擇最適合的 PHP 設定	<ul> <li>, 運行 PHP 以 FPM 應用程式 </li> <li>)</li> <li>(該網站上現有 PHP 腳本的運行。</li> </ul>				
	CGI支援	📀 啟用 (cgi-bin目録位於www-root)				
	FastCGI 支援	◇ 啟用				
	Webalizer 👻 網站統計 (使用您	的 FTP 用戶名和密碼對您的網站統計存取權限加以	以保護 ☑)			
	自訂錯誤文檔	✓ 啟用				
		確定 應用 取消				

### 四、待頁面出現「信息:已成功更新設定」後,點選「確定」離開

✓ 信息:已成功更新設定。

### 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。
- 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。



# 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。

-	- 、點 選「SSL/TLS」證書圖示→「高級設定」→「憑證名稱」								
	網站與域名 >								
	ssl.net-chinese.tw 的 SSL/TLS 證書								
	•								
	♂ 信息: SSL/TLS 證書已簽發。若要令其運行工作,請分配證書以保護域名、郵件或 web 郵箱的安全。								
	如果您在該伺服器上創建了證書簽名請求且收到了證書文件,請在此處上傳它。如果您想要上傳證書和在其它伺服器上生成的私密金鑰對,或生成自簽章憑 證,請點按 <b>添加 SSL/TLS 證書</b> .								
	給域名添加 SSL/TLS 證書後,需要在網站主機設定中啟用 SSL/TLS 支援並選擇該證書 <b>:網站與域名 &gt; 主機設定</b> (該域名)/> <b>安全。</b>								
	在此處上傳證書								
<	證書 (*.crt) * 選擇檔案 沒有選擇檔案								
	上傳證書								
	☆    ☆    加 SSL/TLS    證書     │								
	條目共計 1 每頁顯示條目: 10 25 100 所有								
	□ R K C A 名稱↑								
	🗌 💌 🔑 🗐 鋼站用憑證(2021) 0 🖡								
	條目共計1 每頁顯示條目:10 25 100 所有								
	plesk.com  集思廣益 (EN)   Cookie								

#### 二、將卷軸捲動至私密金鑰處

#### 私密金鑰 (\*.key)

----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDDseU/JGGmHlKZ rLR2K5tf5dLvfsco8PVvxj+LOeTVTmwciMirARQv6M+Rv2D8KfM8RwzPP141FzkB 9Hup8urU0yAtiZBI0egyUIBAEanVf2xaB7R203S79RatQ4293W0yWGF7VgR9ItEF HBOEC0wY5GOP/Jz9x4NAuvBT/PSSP8Se3tTV5W9OAIvVtgm7i0HhNVMLW71eaJYT VuES1XTESFVjbNOum8TvMHAIAoA8ROzkEZvZKwc/xW6woxg6t7gs5x+mIdH/00Xx obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7l40SvIj184zwQz59aeRn3s7NVUYWKCojjY yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfuqe+QkeqyV3XIPKXRL9pFliUm yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZxT84qWpSNlpdzhaEfYEF9v beOd8/yZoI9Cyac1NHqNJ7ZvypZAksNxLlgEf6JZGSWofuC8Cljg12xIvT6oy0Py E5ouZodrOj4us8ehV87eC0lVYgWdAowzbI/tYvtVKx9XuEc8GkP99i184zdygih4 EAuoCooR5nIay6luRGdXMqc4xb2xDJVu+mHSgm40utn6Dr48AuCO/0e8x19iBdDR xGjXoxMdjPeqBhcqWIDVycFZ10idkCq3woqIpEptI9kCgYEA+mXXiporWeBR5TFv 2vAi23Dd5GaH3p6C2oIfENhPcITPn9kgYH0xKxT5xLQHpUfmriLNA375mhB6oQd8 s4enkqU5NrPX5FEkup7Bl9/nj8yDZ1q6W79+gJljsy3LtqUOeMbdqBIfG14XfYDD NgfYe3n6N7cQuMJmP2RrllBUhZ0CgYEAyBK92UU/2y+VQ3/TA5DF+kzsFbEa8Io+ /RiGaG5gYHFtze5wVbzL3V4Tjlr6uXsoSoD2YlKsWRvZvYBLZYKk4hB7xBoVxZeg qbL2peomXh4M0tpNY2OonsaiG64K0/UfX1WKB5LyPwfsoPt2uW4nM6adqFKGxpxu B85kaFWJStMCgYAEAwGzDMlJBVkKjQI3xcUpMu07NxFSNcPu8ErDIFQVf2s8KmRk ZzYddJXz5NaChWZiv9f9CFkjcsQkNFSBI91Bdjg2cicxV0N5YfXEEyhIm4Q3cbKu qaDDOrHoOwGaiYZz10vUN4YcECPcNOXrxbBoOgoSPnKcIzE0Ls2yeNMB2QKBgGH3 42SvpxwSCbn6rn4RdxAgeH4KshFU8JEIYFBks+alxEnRVsp03zKvbU4IuLr4Vntc +MieiOw9WfqUBtdXCJv1zFTzHPQbUj2md2Y46L6vYkIhSUHAvAG7bAe3ym+NmOYa wbMBvoMkwzb0y2bzTFjbXlncx0gbszk5VCtOryKnAoGAOip6XojqucHD3FQMdpdj 9CTAiPSzxHpv/Y03xDaegcntND+xTlL/yAb0p2xluHX/55+jID9njMfeCmzYCn/Y

### 三、將私密金鑰的內容複製並貼至空白記事本裡

#### ----BEGIN PRIVAIE KEY---

>

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDDseU/JGGmHlKZ rLR2K5tf5dLvfsco8PVvxj+LOeTVTmwciMirARQv6M+Rv2D8KfM8RwzPP141FzkB 9Hup8urU0yAtiZBI0egyUIBAEanVf2xaB7R2O3S79RatQ4293WOyWGF7VgR9ItEF HBQEC0wY5GOP/Jz9x4NAuyBT/PSSP8Se3tTV5W9QAIvVtgm7j0HhNVMLW71eqJYT VuES1XTESFVjbNOum8TyMHAIAoA8ROzkEZvZKwc/xW6woxg6t7gs5x+mIdH/00Xx obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7l40SvIj184zwQz59aeRn3s7NVUYWKCojjY yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfuqe+QkeqyV3XIPKXRL9pFliUm yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZxT84qWpSNlpdzhaEfYEF9v beOd8/yZoI9Cyac1NHqNJ7ZvypZAksNxLlgEf6JZGSWofuC8Cljg12xIvT6oy0Py E5ouZodrOi4us8ehV87eC0lVYgWdAowzbI/tYvtVKx9XuEc8GkP99i184zdvgih4 EAuoCooR5nIay6luRGdXMqc4xb2xDJVu+mHSgm40utn6Dr48AuCO/0e8x19iBdDR xGjXoxMdjPeqBhcqWIDVycFZ10idkCq3woqIpEptI9kCgYEA+mXXiporWeBR5TFv 2vAi23Dd5GaH3p6C2oIfENhPcITPn9kgYH0xKxTSxLQHpUfmriLNA37SmhB6oQd8 s4enkqU5NrPX5FEkup7B19/nj8yDZ1q6W79+gJljsy3LtqUOeMbdqBIfG14XfYDD NgfYe3n6N7cQuMJmP2RrllBUhZ0CgYEAyBK92UU/2y+VQ3/TA5DF+kzsFbEa8Io+ /RiGaG5gYHFtze5wVbzL3V4Tjlr6uXsoSoD2YlKsWRvZvYBLZYKk4hB7xBoVxZeg qbL2peomXh4M0tpNY2OonsaiG64K0/UfX1WKB5LyPwfsoPt2uW4nM6adqFKGxpxu B85kaFWJStMCgYAEAwGzDMlJBVkKjQI3xcUpMuO7NxFSNcPu8ErDIFQVf2s8KmRk ZzYddJXz5NaChWZiv9f9CFkjcsQkNFSBI9lBdjg2cicxV0N5YfXEEyhIm4Q3cbKu gaDDOrHoOwGaiYZz10vUN4YcECPcNOXrxbBoOgoSPnKcIzE0Ls2veNMB20KBgGH3 42SvpxwSCbn6rn4RdxAgeH4KshFU8JEIYFBks+alxEnRVsp03zKvbU4IuLr4Vntc +MieiOw9WfqUBtdXCJv1zFTzHPQbUj2md2Y46L6vYkIhSUHAvAG7bAe3ym+NmOYa wbMBvoMkwzb0y2bzTFjbXlncx0gbszk5VCtOryKnAoGAOip6XojqucHD3FQMdpdj 9CTAiPSzxHpv/Y03xDaegcntND+xTlL/yAb0p2xluHX/55+jID9njMfeCmzYCn/Y ighWCNz4Bp30KjuhBX/71QAcb+C7yUV3crPCPtOq8Yjri3KUaTdLTH6RXGiJg4Da ØsDBGeRØA58RWnNuE270TNM=

-----END PRIVATE KEY-----

★未命名 - 記事本 檔案(F) 編輯(E) 格式(O) 檢視(M) 説明 ----BEGIN PRIVATE KEY-----MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBA/ rLR2K5tf5dLvfsco8PVxj+L0eTVTmwciMirARQv6M+Rv2D8K 9Hup8urU0y4tiZBI0egyUIBAEanVf2xaB7R203S79RatQ4293 HBQEC0wY5GOP/J29x4NAuyBT/PSSP8Se3tTV5W9QAIvVtgm7j VuESIXTESFVjbN0um8TyMHAIAoA8R02kEZvZKwc/xW6woxg6t obwc2ZwWzk4cV09xRV9yJHm7vf3Kj7140SvIj184zwQz59aeR yX1GToJnAgMBAAECggEBAKc7beHAsGXqQcIrkWfnqe+QkeqyV yEK2LW3dFSg/9qnhdvrmyoK3YN31uTRPHRtrlwZLnZXT84qWp; be0d8/yZo19Cyac1NHqN17ZvypZAksNxL1gEf6JZGSW0fuC8C E5ouZodr0j4us8ehV87eC01VYgWdAowzb1/tYvtVKx9XuEc8G EAuoCooR5nIay61uRGdXMqc4xb2xDJVu+mHSgm40utn6Dr48A xGjXoxMdjPeqBhcqWIDVycFZ101dkCq3woqIpEpt19kCgYEAH 2vAi23Dd5GaH3p6C20IfENhPc1TPn9kgVH0XkxTSLQHpUfmr s4enkqU5NrPX5FEkup7B19/nj8yDZ1q6W79+gJ1jsv3LtqU0e. NgfYe3n6N7cQuMJmP2Rr11BUhZ0CgYEAyBK92UU/2y+VQ3/TA /RiGaG5gYHFtze5wVbzL3V4Tj1r6uXsoSoD2Y1KsWRvZvYBLZ qbL2peomXh4M0tpNY20onsai664K0/UfX1WKB5LyPwfsoPt2u 885kaFWJStMCgYAEAwG2DM1JBVKkj0I3xcUMu07NxFSNcPu8 ZZYdJXz5MaChWZ1v9f5FkicsQkHFSB191Bdjg2cicxW0N5Y qaDD0rHo0wGaiYZ210vUN4YcECPcN0XrxbBo0goSPnKc1zE0L 42SvpxwSCbn6rn4RdxAgeH4KshFU8JEIYFBks+a1xEnRVsp03 +Mie10w9WfqUBtdXCJv1zFTZHPQbUj2md2Y46L6vYk1hSUHAv wbMBv0Mkwzb0y2bzFfbX1ncx0gbszk5VCt0ryKnAoGA0ip6X 9CTA1FSzxHpv7Y03xDaegcntND+x11L/yAb0p2x1uHX/55+j1 ighWCNz4Bp30KjuhBX/71QAcb+C7yUW3crPCPt0q8Yjri3KUa 9DBGeR0A58RWnNuEz2Q1NM=

----END PRIVATE KEY----|

第28列,第26行 1009

#### 四、將私密金鑰檔案存檔

第 另存新檔         ×								
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	« 434	539327 > C	5	○ 搜尋 CER	- CRT Files			
組合管理 ▼ 新城	曾資料夾	ξ					== -	?
🔜 本機	^	名稱	^		修改日期		類型	
🔰 3D 物件		🔄 AAACer	tificateServices.crt		2021/1/7	下午 06:32	安全性憑證	
📙 iso映像檔資源	庫	My_CA	Bundle.ca-bundle		2021/1/7	下午 06:32	CA-BUNDLE	檔案
	18 C	🔄 Sectigo	RSADomainValidatior	SecureS	2021/1/7	下午 06:32	安全性憑證	
▲ 文件		🔄 ssl_net-	chinese_tw.crt		2021/1/7	下午 06:32	安全性憑證	
		🔄 USERTr	ustRSAAAACA.crt		2021/1/7	下午 06:32	安全性憑證	
27 日本								
一 天四	+							
	₽.							
■ 固月								
影片								
🏪 本機磁碟 (C:)								
媒體庫 (D:)	× ·	c						>
檔案名稱(N):	Server.	key						~
存檔類型(T):	所有檔	案 (*.*)						~
	-							
∧ 隱藏資料夾			編碼(E): UTF-8		~	存檔(S)	取消	

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

證書 (*.crt)	Ō	
BEGIN CE	ً	
MIIFyjCCBLKgA		
jzELMAkGA1UEB	ø	
A1UEBxMHU2FsZ	r5	
Ey5TZWN0aWdvI		
MB4XDTIxMDEwN	8	
Lm5ldC1jaGluZ		
w7HlPyRhph5Sm	<u>11</u>	
PEcMzz5eJRc5A		
slhhe1YEfSLRB	ø	>
4TVTC1u9XqiWE	17	
LOcfpiHR/9NF8	لتتا	
70zVVGFigqI42		
iuF36Zv5mwXhu		
A1UdDwEB/wQEA		
BggrBgEFBQcDA		
AgEWF2h0dHBzC		
AQEEeDB2ME8GC		
Z29SU0FEb21ha		
BzABhhdodHRwC		
LWNoaW5lc2Uud		
AgQCBIH0BIHxA		
AXbcCQQtAAAEA		
AiAVrDeH2jgz+		

#### CA 證書 (\*-ca.crt)

#### ----BEGIN CERTIFICATE-----

MIIGEzCCA/ugAwIBAgIQfVtRJrR2uhHbdBYLvFMNpzANBgkqhkiG9w0BAQwFADCB iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTgx MTAyMDAwMDAwWhcNMzAxMjMxMjM10TU5WjCBjzELMAkGA1UEBhMCR0IxGzAZBgNV BAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UEBxMHU2FsZm9yZDEYMBYGA1UE ChMPU2VjdGlnbyBMaW1pdGVkMTcwNQYDVQQDEy5TZWN0aWdvIFJTQSBEb21haW4g VmFsaWRhdGlvbiBTZWN1cmUgU2VydmVyIENBMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEA1nMz1tc8INAA0hdFuNY+B6I/x0HuMjDJsGz99J/LEpgPLT+N TQEMgg8Xf2Iu6bhIefsWg06t1zIlk7cHv7lQP6lMw0Aq6Tn/2YHKHxYyQdqAJrkj eocgHuP/IJo8lURvh3UGkEC0MpMWCRAIIz7S3YcPb11RFGoKacVPAXJpz9OTTG0E oKMbgn6xmrntxZ7FN3ifmgg0+1YuWMQJDgZkW7w33PGfKGioVrCSo1yfu4iYCBsk Haswha6vsC6eep3BwEIc4gLw6uBK0u+QDrTBQBbwb4VCSmT3pDCg/r8uoydajotY uK3DGReEY+1vVv2Dy2A0xHS+5p3b4eTlygxfFQIDAQABo4IBbjCCAWowHwYDVR0j BBgwFoAUU3m/WqorSs9UgOHYm8Cd8rIDZsswHQYDVR0OBBYEFI2MXsRUrYrhd+mb +ZsF4bgBjWHhMA4GA1UdDwEB/wQEAwIBhjASBgNVHRMBAf8ECDAGAQH/AgEAMB0G A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAbBgNVHSAEFDASMAYGBFUdIAAw CAYGZ4EMAQIBMFAGA1UdHwRJMEcwRaBDoEGGP2h0dHA6Ly9jcmwudXNlcnRydXN0 LmNvbS9VU0VSVHJ1c3RSU0FDZXJ0aWZpY2F0aW9uQXV0aG9yaXR5LmNybDB2Bggr BgEFBQcBAQRqMGgwPwYIKwYBBQUHMAKGM2h0dHA6Ly9jcnQudXNlcnRydXN0LmNv bS9VU0VSVHJ1c3RSU0FBZGRUcnVzdENBLmNydDAlBggrBgEFBQcwAYYZaHR0cDov L29jc3AudXNlcnRydXN0LmNvbTANBgkqhkiG9w0BAQwFAAOCAgEAMr9hvQ5Iw0/H

uF90PlrqzaISpGpejjsSwCBEXCpzAAABdtwJBHIAAAQDAEcwRQIgUFYzJ4n9LcPr

### 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。