

# CSR 生成與憑證安裝指南 適用於 Windows

網路中文 网路中文 Net-Chinese Net-Chinesisch Net-chino Нетто-китайски ネット-チャイニーズ 네 - 중국

# 生成 CSR 憑證請求檔

本章節將開始帶您操作如何使用 IIS 網站伺服器產生申請憑證時必要的 CSR(Certificeate Signing Request) 文件。

節

#### 一、至 IIS 首頁中找尋「伺服器憑證」並點擊進入



「伺服器憑證」的圖示會位在 IIS 的左側樹狀結構中,寫著您電腦主機名稱的那一個部份。

如果您找不到的IIS的話,可以透過Windows的搜尋功能中輸入「IIS」或「Internet Information Services」進行查找。

Internet Information Services (III) 管理員 <th>二、點選石構</th> <th>剿動作中的「建立憑證要求」</th> <th></th>	二、點選石構	剿動作中的「建立憑證要求」	
●     ●<	<b>8</b>	Internet Information Services (IIS) 管理員	_ <b>D</b> X
<ul> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	€ • WINSRV2012	•	🖸 🛛 🟠 🕡 🗸
●         ●	檔案(F) 檢視(V) 說明(H)		
就结	(個典(F) (資稅(V) 詳明(H)	● 印服器憑證         少的地可用來要求及管理網頁伺服器可與針對 SSL 設定的網旋指配使用的憑證。         ● 運話:       ● ● 登行台         ● ● 登行台       發行者         ● 目標       ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	國人         建立憑證要求         完成憑證要求         建立局我簽署憑證         設口已更新憑證的自動重新繁結         ② 說明
	就緒		• <u>1</u> .:

#### 三、填寫 CSR 資料

hinese Co.,Ltd
icts Dept.
i City
n

依上圖指示,在一般名稱中輸入不含「http//」的網址,如果您的主機名稱是 www 則請輸入 「www. 你的域名. 域名後綴」,若為其他子域名申請,則請帶入該子域名的主機名稱。如 果您申請的是通用型憑證,則請輸入「\*. 你的域名. 域名後綴」。例如:\*.net-chinese.tw

另外,組織為必填欄位、縣市建議填您所在縣市即可,省份帶入 Taiwan 即可。

最後,建議您全程以英文填寫,填寫完後請按「下一步」。

#### 四、選擇密碼編譯服務提供者及位元長度

要求憑證	?	×
<b>密碼編譯服務提供者內容</b>		
攫取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度越大。安全性 越高。不過,位元長度較大可能會降低效能。	沋	
密碼編譯服務提供者(S):		
Microsoft RSA SChannel Cryptographic Provider		
位元長度(B):		
2048 v		
上一步(P) 下一步(N) 完成(F)	取消	

在密碼編譯服務提供者中有兩個選項,預設值為「Microsoft RSA SChannel Cryptographic Provider」,請維持這個選項,不需要更動。位元長度請用下拉式選單選擇「2048」,確認無誤後請點擊「下一步」。

#### 五、請選擇 CSR 的儲存路徑後點擊完成

要求憑證	?	x
<b>檔案名稱</b>		
指定憑證要求的檔案名稱。這項資訊可傳送給憑證授權單位做為簽署之用。		
指定憑證要求的檔案名稱(R):		
C:\Users\Administrator\Desktop\ServerCSR.txt		
<b>上一步(P)</b> 下一步(N) 完成(F)	取消	

在這邊會讓您選擇您要將 CSR 檔案給儲存在那裡,您可以點選右邊的「…」按鈕後選擇儲存 路徑,選擇好之後按下「完成」。

CSR 檔案在 Windows 中是以.txt 文本格式進行儲存。

#### 六、到您儲存的路徑找尋 CSR 檔案並開啟它

ServerCSR - 記事本	_		2	x
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)				
BEGIN NEW CERTIFICATE REQUEST				^
MIIEeTCCA2ECAQAwgYgxCzAJBgNVBAYTA1RXMQ8wDQYDVQQIDAZUYWJ BgNVBA oWC1Ebo YB1 o SBDo YEEUErwCgVDVOOKDBNOZYO+O2bo brv/gZSE	.3Y¥4x	FDAS	5	
MRcwFQYDVQQLDA5Qcm9kdWN0cvBEZXB0L iEbMBkGA1UEAwwSc3NsLm	51dC1i	aG1u	1	
ZXN1LnR3MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApb0	ZN8N¥	Ūi7∈	9	
HT/7x0QZUQxGxGFyeXDqVDvYwJAjHKXYAs2Iq5Jr/7kkea+hPsW6y8c	x 1MKU	laBNz	-	
A66VCGyaAInYhggqUCBUsUzipWF1YN/MqUCjCQjaPS/f12ID/wA0UM)	nPXcs	LZQY V1H:		
Z+InfRab i5Z9hvoZcvVIISZGeaVW5VRCaIpPTI1d2fZ+BxGSaQII7vCi(	Jan 120 JepPT1	vımj EfhC		
LgAtRmrEeuGWBgdkgfnmSKfvujEHvdJ4WghAbfG1q10+WXY1GL4LQEH	DVNoR	Y9ip	, ,	
BqrUmX5YDwIDAQABoIIBqTAaBgorBgEEAYI3DQIDMQwWCjYuMi45MjA	wLjIw	RQYJ		
KwYBBAGCNxUUMTgwNgIBBQwKV21uU3J2MjAxMgwYV010U1JWMjAxM1x	BZG1p	bml z		≡
AHIAbwBzAG8AZgBOACAAIIgBTAEEAIABTAEMAaABbAG4AbgB1AGwATAE	) areur Sdahta	.aQDj .eQBu	) 7	
AHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByAwEAMIH	PBgkq	hkiG	,	
9w0BCQ4xgcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCs	GAQUF	BwME	}	
MHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb	3DQME	AgIA	4	
ZOMEAOUWBWYFKW4DAgcwCgYIKoZIbycNAwcwHOYDVR00BBYEFPgmij	uldgig ZyVnIn	nkgc KmUr		
qaaREXjsQRkqMAOGCSqGSIb3DQEBBQUAA4IBAQAqj1Zr2N1GUmzDXw0	ArN6I	LY19	)	
MmFnL1GFza5qpih6DpD4Z3r9AUee4X7bD92L0xDFJ99sTkRL2PwHDa	mUxEQ	S2vZ	;	
6SQMA6FVf4vDcSvhbTzQtGhH0kSsiOdN/pH1RzCLKqqVjKPUwqK1Yap	)000jq	ısIgU	J	
vdbzirvbuviryczotkicałr4xgErkxKKiq5KAZuzcUUHWVMxEeVGUN 5rin4eumai3I6kU5i44e0NVLiDuCivZTfuaXEgtEV0tykztyKSIXu05	'ðsrkg 67076	idqz iWa3	2	
k8FOHTn/+ESLOmfmemMaXSBZ7cvOXsh3iv4H4mZX1LY8NOtB+LucR	uDRck	ിലർഗ	,	
,				~
			>	зł

當您開啟儲存的 CSR 檔案後,您就可以到網路中文網站進行送件了。

Windows 平台生成的 CSR 有一個與其他平台非常不同的點在於「Windows 的私密金鑰不會匯出 供管理員存取」。

所以您無法在 Windows 的主機中找到與存取您的私密金鑰,從產出、匯入憑證到繫結,您 完全都不會接觸到私密金鑰,若您有要將 Windows 憑證移機到其他平台進行佈署的需求, 我們將會在後面的說明帶您操作。



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匯入到您的 IIS 中。與其他平台 很不一樣的地方在於,它有三種方式可以匯入憑證,將在本章之中各別和您說明

#### 在本章節您可以學習三種憑證匯入方法:

- A. 使用 IIS 完成憑證請求方式匯入憑證
- B. 使用 MMC(主控台)方式匯入憑證
- C. 使用 IIS 的「匯入」方式匯入 .PFX 格式的憑證

#### 三種匯入方式有什麼樣的不同?

- ◆ 收到的憑證只有一個 .cer 格式的憑證:選擇 A
- ◆ 收到的憑證有數個憑證(網站憑證、中繼憑證及根憑證): 選擇 B
- ◆ 其他 Windows 匯出的憑證,或是原部署於其他作業系統 (如 Linux) 移裝, 且有私密金鑰檔的時候:選擇 C。

會有這樣的分別,主要是因為,在 Linux 系統中,通常會使用 Open SSL 利用演算機制去產生私密金鑰,再由私密金鑰去產生一組與之配對的公鑰,即 CSR, 而使用者再利用這個 CSR 送交給憑證發行機構進行簽署,簽署完成後再將簽署 過的公鑰交給您。這就是您拿到的終端憑證。

這就像是,CSR 其實只是一張上面寫了您網域、公司的空白執照,但是這空白的執照並沒有獲得第三方認可,因此不具效力,而送交第三方公證機構簽署或 是蓋印章的執照,才具有公信力。

而 Windows Internet Information 的機制下生成 CSR, 會將其金鑰留在生成的主機裡面,並不會匯出給使用者,也許是基於資訊安全考量。(就算是開放系統, 您也不應該隨意將私密金鑰交給第三方)。

在一些特殊的情況之下(例如您同時有 Windows 系統的網頁主機及 Linux 的網 頁主機),會需要做多重部署的情況。這時您需要將運行在 Linux 或開放式傳統 的憑證同時一併部署於 Windows(通常是通用型憑證或是多域名型憑證),就會 需要將憑證、信任鏈(中繼憑證/根憑證)與終端憑證轉換成 PKCS#12 文件格 式以對其中的憑證、私密金鑰以再加密的方式包覆起來 - PFX 格式即為 PKCS#12 的文件格式。

在這樣的方式之下,您就必須以.PFX 格式將原先部署於開放式系統主機上的憑證匯入 Windows。

#### A、 使用 IIS 完成憑證請求方式匯入憑證

#### 使用對象:

- 1. 以 Windows Internet Information Services 依照第一章的方式產生 CSR 的使 用者。
- 2. 在遞交資料時的伺服器選擇 Internet Information Services 或 IIS 5.0 及 later 版本的使用者。
- 3. 收到的憑證是上游廠商以.cer 給您的憑證。

## 一、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

□來源: Sectigo Certification Authority <noreply@sectigo.com> 收信: 標題: ORDER #434539327 - Your PositiveSSL Certificate for ssl.net-ch 日期: Wed, 06 Jan 2021 14:19:09 標籤: Jimmy, 已處理 附檔(1): ■ ssl.net-chinese t</noreply@sectigo.com>	🕒 💼 🛥 🚥
w.zip	<u></u> 純文字 HTML
COMODO Creating Trust Online	▲ 
Your PositiveSSL Certificate for ssl.net-chinese.tw i	s attached!
Dear @net-chinese.com.tw,	
Thank you for placing your order. We are pleased to announce that issued.	t your PositiveSSL Certificate for ssl.ne
To help reduce domain name mismatch warnings, we have also inc certificate.	cluded the domain name www.ssl.net-c
We strongly recommend that you click here for instructions to configured correctly.	ensure that your certificate is installed
Attached to this small you should find a rin file containing:	
	注人 (Sactiga/Camada)

#### 曾將憑證以 ZIP 壓縮福的万式附件給甲請人 (Sectigo/Com

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)

€ 🗇 ד ↑ 🎴	o « ssl_	net-chinese 🕨 ssl_net-chines	e_tw ∨ Ċ	搜尋 ssl_net-chinese	tw 🔎
숨 我的最愛	^	名稱	修改日期	類型	大小
📜 下載	=	🔄 ssl_net-chinese_tw.cer	21/1/2021 14:12	安全性憑證	8 KB

## 二、回到「伺服器憑證」中點選「完成憑證請求」

<b>\$</b>						Internet I	nformation	n Services (IIS)	管理員						_ 🗆 X
$\bigcirc$	9	WINSRV2012	2 🔸											2	• 🕥 🏠 🛛 •
檔案(F)	檢視(V)	說明(H)													
連線				伺服哭馮	部								動作		
😪 - 🔡	🖄   😪			비민지지 취취 개당	( nH								E	覆入	
⊿ • WI	后網貝 NSRV201	2 (WINSRV201	此功制	11可用來要求及管	理網頁伺服	8器可與針對 SSL	設定的網站搭	記使用的憑證。						建立憑證要求 白成馮證要求	
	應用程式 站台	集區	篩選		-	💎 移至(G) → 🖕	計全部顯示(A)	│群組依據: 沒有	分組	•				建立網域憑證	
			名稱	•		發行給		發行者		到	朝日	憑調	Ŗ	建立自我簽署	憑證
													100	釣用己更新憑 <sup>結</sup>	證的自動重新繫
													2	說明	
			<			Ш						>			
<	ш	>	111 功能	「 内容検	視										
就緒															€ <u>1</u> .:
=、	記	宁夕	摇的	1住大	囸										
— `			ドサナ		٣										
							完成憑	證要求					?	x	
				170 4rd 145 88 A											
	ſ		指定憑	證授權单(	山回爐										
		藉由擷取自	回合憑證	授權單位回	應的檔署	<b>案</b> ,完成先前	前建立的憑	證要求。							
		人士证约的			17 XX (D)										
		百角浓疸的	叉催 早11	凹燃的個条	石侢(K)					_					
		i\Certificat	te\ssl_n	et-chinese_	tw\ssl_r	net-chinese	_tw\ssl_ne	et-chinese_tw	/.cer						
		好記的名稱	≣(Y):												
		cel not chi		1											
		ssiner-chi	nese.tw	4											
		鼝取新憑護	的憑謂	儲存區(S):											
							<b>*</b>								
											確定		取消	á	

選好憑證後,您可以給他一個好記的名稱(這邊以站台主機名稱命名為例),憑證儲存區若您是以 Administrator 身份的話可以選個人,或是以本機為主的 Web Hosting,比較不易受執行身份影響,設定無誤後按請「確定」。

## B、 以 MMC( 主控台 ) 的方式匯入憑證

#### 使用對象:

- 1. 以 Windows Internet Information Services 依照第一章的方式產生 CSR 的使用者。
- 2. 在遞交資料時的伺服器選擇非 Internet Information Services 或 IIS 5.0 及 later 版本的使用者。
- 3. 收到的憑證是上游廠商以文本格式或是 .crt 格式給您的憑證。

#### -、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



#### 以文字格式的方式做為憑證檔案寄送給申請人

在大多數的情況之下,發證機構將會以文字格式做為終端憑證寄送給客戶。而並不會包含中繼憑證 (Intermediate) 及根憑證 (Root)。而中繼憑證與根憑證將會以公開方式放在發證機構供有需要的使用者下載。

如果您有需要,您可自行至發證機構網站下載。

Image: ServerCSR - 記事本   Image: Im	x
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)	
BEGIN NEW CERTIFICATE REQUEST	^
MIIEeTCCA2ECAQAwgYgxCzAJBgNVBAYTA1RXMQ8wDQYDVQQIDAZUYW13YW4xFDAS	S
BgNVBAcMC1RhaXB1aSBDaXR5MRwwGgYDVQQKDBNUZXQtQ2hpbmVzZSBDby4s1HRk	2
MRCWFQIDYQQLDASQCM9KQWNUCYDEZADULJEDMDKGAIUEAWWSCSNSLMDIQUIJaGIU ZYNIL pR2WIIRI;ANBg/gab/;CQm0BAOFFAAOCAOSAWIIRCgKCAOFAabcZNSNWU;Zg	1
HT /7x007U0xGxGExceXDaVDxYwIA jHKXYAc2Ia5Ir /7kkca+bPcW6x2ox1MKUaBNz	; ,
A6BVCGvaAInYhgggOCBOsOzipWF1YN/MgOCiCQiaPS/fI2TD7wAoOMYnPXcsLZQY	;
h4rmKTZYLPhgb6fKQLgMo5PYCyfTXMPPvnhB+1IhJDHIoOc+aWPGWSEai1ZO/1M	i
Z+JofRabj5Z9hyoZcyVUSZGeqVW5VRCqIpPTI1d2fZ+BxGSqQU7vCiCgpPT1EfhC	
LgAtRmrEeuGWBgdkgfnmSKfvujEHvdJ4WghAbfG1q10+WXY1GL4LQEKDVNoRY9ip	>
BqrUmX5YDwIDAQABoIIBqTAaBgorBgEEAYI3DQIDMQwWCjYuMi45MjAwLjIwRQYJ	
KwYBBAGCNxUUMTgwNgIBBQwKV21uU3J2MjAxMgwYV010U1JWMjAxM1xBZG1pbm1z	≡
dHJhdb99DAtJbmVUIWdyLmV42IDyDgorDgEEAYI3UQ10MWQwYgIDAK5aAEUAaQDj	]
ARIADWDZAGOALGDUAGAAUGDIAEEAIADIAEMAAADRAG4ADGDIAGWAIADDARIAEWDV AHOAbwBaaHIAYOBwaGaabaOBiaCaaUiaBwaGQadaBaaCaabaaGOaZOBwawFaMIHPBacabaa	2
9w0BCQ4ygcEwgb4wDgYDVR0PAQH/BAQDAgTwMBMGA1UdIQQMMAcGCCsGAQIFBwMF	, ,
MHgGCSaGSIb3DQEIDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCaGSIb3DQMEAgIA	Ĺ
gDALBg1ghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAF1AwQBAjALBg1ghkgE	}
ZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR00BBYEFPgmuiZxVpJpKmUr	
qaaREXjsQRkqMA0GCSqGSIb3DQEBBQUAA4IBAQAqj1Zr2N1GUmzDXwCArN6ILY19	)
MmFnL1GFza5qpih6DpD4Z3r9AUee4X7bD92L0xDFJ99sTkRL2PwHDa1mUxEQS2v2	
bSQMAbFVf4vDcSvbbIzQtGhHUkSsiUdN/pHIKzCLKqqVjKPUwqKIYapUUUjqsIgU	J
vaozirvouviruczolikicanr4xgErkxRAIqoRAzuzcuUnwVMXEeVGUNW8SFKgIdqz	
2297724878878777878787878787878787878787878	
KOLONIN, BELORERENERRANDE, COMBINITY HIMERIEI ONO DE EUCLURICE	$\sim$
<	≥ <sub></sub>

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	X
⊛ ⊚ - ↑ 퉬	。≪ ssl_net-chinese ▶ ssl_net-chinese_tw v C [搜尋 ssl_net-chine	se_tw 🔎
組合管理 ▼ 新増]	資料夾	:= 👻 🔞
☆ 我的最愛	▲ 名稱 ▲ 修改日期 到	領型
🚺 下載	□ ssl_net-chinese_tw.cer 2021/1/21下午 0 多	安全性憑證
■ 桌面	=	
圖 嵌虹的位置		
🖳 本機		
		>
檔案名稱(N):	ssl_net-chinese_tw.crt	~
存檔類型(T):	所有檔案 (*.*)	~
▲ 陽藏資料夾	編碼(E): ANSI V 存檔(S)	取消



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。

# 二、在搜尋輸入「MMC」開啟主控台



## 三、在 MMC 點選「檔案」下面的「新增 / 移除嵌入式管理單元」

			主控台1 - [主控台根目錄]	_ <b>D</b> X
	檔案	(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(	<i>り</i>	_ & ×
¢		開新檔案(N) Ctrl+N		
		開啟(O) Ctrl+O	稱 動作	
		儲存(S) Ctrl+S	這個檢視沒有項目可顯示・主控台根目	錄 🔺
		另存新福(A)	其他動作	•
		新増/移除嵌入式管理單元(M) Ctrl+M		
		建坝(P)		
		取如使用過的備業		
		結束(X)		
讓魚	論調	從嵌入式管理單元主控台中新增或移除嵌入式管理	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	

#### 四、在「新增 / 移除嵌入式管理單元」中選擇「憑證」後按「新增」



#### 五、在嵌入式管理單元選擇管理「電腦帳戶」的憑證。



## 六、在嵌入式管理單元管理的電腦中選擇「本機電腦」後按「完成」

		選取	電腦	
請選取您要此嵌入	入式管理單元管理的電	間間。		
~這個蟲入式管理	8留元赼—百答珊·			
● 本機電腦 (	執行這個主控台的電腦	窗)(L):		
○ 另一台電腦	ắ(A):			瀏覽(R)
🗌 當電腦從商	8令列啟動時,可以對	İ這台電腦進行	變更。這只有在您儲存主	控台之後才適用(W)
			< 上一步(B)	完成 取消
~ 가까 수지 않은 지금 !		rm == — 杰	- →四《父 网上审公 「丁寸	
		<b>理單元無</b> 新増或移除制		
在認選取 您可以為這個主控台從您的問 人式管理單元,您可以設定的	的嵌入式管 翻上可以使用的嵌入式管	<b>理單元無</b> 新増或移除敏 <sup>該理單元中選擇一</sup>	<b>民誤後點擊「確</b> 入式管理單元 些嵌入式管理單元,並且設定所	定し 「選擇的嵌入式管理単元・對於可延伸的行
在認選取 您可以為這個主控台從您的關 入式管理單元,您可以設定的 可用的嵌入式管理單元(S):	的嵌入式管 電腦上可以使用的嵌入式電 取用哪些延伸・	<b>理單元無</b> 新增或移除制 <sup>該理單元中選擇一</sup>	<b>民 設後 點擊 「確</b> 入式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E):	定し 所選擇的嵌入式管理單元・對於可延伸的
★ 確認選取 您可以為這個主控台從您的問入式管理單元,您可以設定的 成式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元		<b>理單元無</b> 新増或移除敏 <sup>訪理單元中選擇一</sup>	其設後點擊「確 人式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): □ 主控台根目錄 □ 正空的(大概要○)	<b>に定」</b> 所選擇的嵌入式管理単元。對於可延伸的 編輯延伸(X)
★ 確認選取 您可以為這個主控台從您的調 入管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一般及式管理單元 ※ 具有進階安全性的 Win ◎ 服務	的嵌入式管 電腦上可以使用的嵌入式管 軟用哪些延伸。 旅商 ^ . Microsoft Corp Microsoft Corp	<b>理單元無</b> 新増或移除的 <sup>翻單單元中選擇一:</sup>	其設後點擊「確 人式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 「愛 憑證 (本機電腦)	「選擇的嵌入式管理單元・對於可延伸的計 編輯延伸(♡ 移除(R)
★ 確認選取 您可以為這個主控台從您的習 べ式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一員有進階安全性的 Win ○ 服務 ■ 原則結果組	的嵌入式管	<b>理單元無</b> 新増或移除制 <sup>奮理單元中選擇一:</sup>	其設後點擊「確 入式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 ■ 憑證(本機電腦)	F選擇的嵌入式管理単元。對於可延伸的 編輯延伸(X) 移除(R)
★ 確認選取 您可以為這個主控台從您的聞 入式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一,服務 圓,原則結果組 ○,效能監視器	的嵌入式管 電腦上可以使用的嵌入式智 数用哪些延伸。 旅商 へ Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	<b>理單元無</b> 新増或移除制 <sup>諸理單元中選擇一:</sup>	ま設後點擊「確   大式管理單元   些嵌入式管理單元,並且設定所   選取的嵌入式管理單元(E):   雪主控台根目錄   「● 法控台根目錄   「● 法控台根目錄   「● 憑證(本機電腦)	「選擇的嵌入式管理單元。對於可延伸的 編輯延伸(X) 移除(R) 上稼(U)
○ 確認選取 您可以為這個主控台從您的聞 入式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一員有進階安全性的Win 服務 I 原則結果組 ② 效能監視器 I 原則結果組 ③ 效能監視器 I 原則結果組 ③ 2 課題理目目目的 (5000)	的嵌入式管	<b>理單元無</b> 新増或移除的 部理單元中選擇一	<ul> <li> <b>法設後點擊「確</b> (入式管理單元         ) 並且設定所 世嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): <sup>●</sup> 主控台根目錄 「● 速控台根目錄         (本機電腦)         </li> </ul>	F選擇的嵌入式管理單元・對於可延伸的 編輯延伸(X) 移除(R) 上移(U)
★ 確認選取 您可以為這個主控台從您的習 べ了管理單元,您可以設定的 可的嵌入式管理單元(S): 嵌入式管理單元 一個的嵌入式管理單元(S): 一個的設定(S): 一個的記(S): 一個的記(S): 一個的記(S): 一個的記(S): 一個說(S): 一個的記(S): 一個說(S): (S)	的嵌入式管	<b>理單元無</b> 新増或移除的 部理單元中選擇一	<ul> <li>其時後點擊「確</li> <li>入式管理單元</li> <li>些嵌入式管理單元,並且設定所</li> <li>選取的嵌入式管理單元(E):</li> <li>■主控台根目錄</li> <li>◎ 憑證(本機電腦)</li> </ul>	F選擇的嵌入式管理単元。對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
★ 確認選取 如可以為這個主控台從您的調 入若理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一員有進階安全性的Win 如能監視器 原則結果組 如就監視器 過授權管理員 員群組原則物件編輯器 過裝置管理員 資料夾	的嵌入式管	<b>理單元無</b> 新増或移除的 <sup>諸理單元中選擇一:</sup>		新選擇的嵌入式管理單元・對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
○ 確認選取 您可以為這個主控台從您的聞入式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一, 服務 算, 原則結果組 一, 服務 算, 原則結果組 一, 一, 一	的嵌入式管	<b>理單元無</b> 新増或移除的 <sup>話理單元中選擇一:</sup>	其設後點擊「確 人式管理單元,並且設定所 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 承證(本機電腦)	F 選擇的嵌入式管理單元・對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
★ 確認選取 ※可以為這個主控台從您的習入式管理單元,您可以設定的 ○可用的嵌入式管理單元(S): 嵌入式管理單元(S): 嵌入式管理單元(S): 嵌入式管理單元(S): ※ 具有進階安全性的 Win ※ 服務 ፪ 原則結果組 ※ 效能監視器 2 詳細原則物件編輯器 3 詳細原則 3 詳細原則物件編輯器 3 詳細原則物件編輯器 3 詳細原則	的嵌入式管	<b>理單元無</b> 新増或移除的 部理單元中選擇一:	★ 誤後點擊「確 人式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ● 主控台根目錄 ● 憑證 (本機電腦)	F選擇的嵌入式管理單元。對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
<ul> <li>○ 確認選取</li> <li>※可以為這個主控台從您的電入式管理單元,您可以設定。</li> <li>○ 功管理單元,您可以設定。</li> <li>○ 可以設定。</li> <li>○ 可以設定。</li> <li>○ 政能管理單元(S):</li> <li>○ 政能監視器</li> <li>○ 政能監視器</li> <li>○ 政能監管理員</li> <li>○ 詳細原則結果組</li> <li>◎ 詳細原則約件編輯器</li> <li>○ 該點式管理員</li> <li>○ 該點式臺端存取</li> <li>○ 電話語音</li> </ul>	的嵌入式管	<b>理單元無</b> 新増或移除的 <sup>諸理單元中選擇一:</sup>	其設後點擊「確 入式管理單元,並且設定所 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 ₪憑證(本機電腦)	F 定 た よ が の に 、 の が の び の の の の の の の の の の の の の
★ 確認選取 您可以為這個主控台從您的聞入式管理單元,您可以為這個主控合從您的聞入式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 ● 具有進階安全性的Win ● 服務 ■ 原則結果組 ● 效能監視器 2 詳組原則物件編輯器 ● 詳細原則物件編輯器 ● 資料夾 ● 路由及遠端存取 ● 電話語音 ● 磁碟管理 ● 電話語音 ● 磁碟管理	的嵌入式管 電腦上可以使用的嵌入式電 取用哪些延伸。 旅用哪些延伸。	<b>理單元無</b> 新増或移除的 <sup>諸理單元中選擇一:</sup>	其時後點擊「確 人式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 ● 憑證(本機電腦)	F 選擇的嵌入式管理單元・對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
★ 確認選取 您可以為這個主控台從您的習 入式管理單元,您可以設定的 可用的嵌入式管理單元(S): 嵌入式管理單元 一個具有進階安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路安全性的Win 個具有進路空全性的Win 個具有進路空全性的Win 個具有進路空全性的Win 個具有進路空全性的Win 個具有進路空全性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的Win 個具有進路空空性的 個子。 個子。 個子。 個子。 個子。 個子。 個子。 個子。 個子。 個子。	的嵌入式管	<b>理單元無</b> 新増或移除的 部理單元中選擇一:	★ 誤後點擊「確 人式管理單元 些嵌入式管理單元,並且設定所 選取的嵌入式管理單元(E): ■ 主控台根目錄 ☞ 憑證 (本機電腦)	F選擇的嵌入式管理單元。對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D)
★ 確認選取 您可以為這個主控台從您的聞人式管理單元,您可以為這個主控合從您的聞人式管理單元,您可以設定的可用的嵌入式管理單元(S): 或入式管理單元 分式管理單元 一,而的嵌入式管理單元(S): 一,而不可以設定的 一,而不可。 一,而不可 , 一,而不可。 一,而不可 一,而不可。 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一,而不可 一, 一,而不可 一, 一, 一, 一, 一, 一, 一, 一, 一, 一, 一, 一, 一,	的嵌入式管	<b>理單元無</b> 新増或移除的 <sup>舒理單元中選擇一:</sup>	其設後點擊「確 人式管理單元,並且設定所 進政的嵌入式管理單元(E): ■ 主控台根目錄 ⑦ 憑證(本機電腦)	F選擇的嵌入式管理單元・對於可延伸的 編輯延伸(×) 移除(R) 上移(U) 下移(D) <u>進階(V)</u>
<ul> <li>本 確認選取</li> <li>您可以為這個主控台從您的智人式管理單元,您可以設定的可用的嵌入式管理單元(S):</li> <li>廠入式管理單元(S):</li> <li>廠入式管理單元(S):</li> <li>廠入式管理單元(S):</li> <li>廠及式管理單元</li> <li>一 資為進階安全性的Win</li> <li>※ 原則結果組</li> <li>※ 效能監管理員</li> <li>劉 群組原曾理員</li> <li>一 資路出話管理</li> <li>※ 電話語音</li> <li>※ 磁型</li> <li>※ 電話語音</li> <li>※ 磁型</li> <li>※ 範述:</li> </ul>	的嵌入式管	<b>理單元魚</b> 新増或移除的 部理單元中選擇一:	其設後點擊「確 入式管理單元,並且設定所 選取的嵌入式管理單元(E): ● 主控台根目錄 ☞ 憑證(本機電腦)	F選擇的嵌入式管理単元。對於可延伸的報告
本 確認選取 您可以為這個主控台從您的電人式管理單元,您可以設定的可用的嵌入式管理單元(S): 嵌入式管理單元 ● 具有進階安全性的Win ● 服務 』原則結果組 ● 效能監視器 」原則結果組 ● 数點點 ● 教出及遺端存取 』 帮出及遺端存取 』 電話語管理 ● 電話語管理 ● 網話語管理 ● 網話語管理 ● 網話語管理 ● 電話語管理 ● 網話語管理 ● 電話語管理 ● 網話語管理 ● 調響	br	<b>理單元魚</b> 新増或移除的 <sup>舒理單元中選擇一:</sup>	其設後點擊「確 人式管理單元,並且設定所 進政的嵌入式管理單元(E): ● 主控台根目錄 ⑦ 憑證(本機電腦)	F 選擇的嵌入式管理單元・對於可延伸的 編輯延伸(べ) 移除(R) 上移(U) 下移(D) <u>進階(M)</u>
★ 在意思選取 您可以為這個主控台從您的電入式管理單元,您可以設定。 可用的嵌入式管理單元(S): 取入式管理單元(S): 取入式管理單元(S): 取入式管理單元(S): 取入式管理單元(S): 取為工管理單元(S): 取為工管理單元(S): 取為工管理單元(S): 取為工管理單元(S): 取為工管理單元(S): 對相思管理具具 算器由及遠端存取 影電話語音 磁域址建結 國 電話語管理 梁 總型 該述:	的嵌入式管	<b>理單元魚</b> 新増或移除的 部理單元中選擇一:	其時後點擊「確 人式管理單元,並且設定所 些嵌入式管理單元,並且設定所 運取的嵌入式管理單元(E): ● 主控台根目錄 ● 憑證(本機電腦)	F選擇的嵌入式管理單元。對於可延伸的 編輯延伸(X) 移除(R) 上移(U) 下移(D) 進階(V)
<b>在 認選取</b> 您可以為這個主控台從您的電入式管理單元,您可以設定的可用的嵌入式管理單元(S): 嵌入式管理單元(S): 嵌入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 廠入式管理單元(S): 國上總 國上 國 <	的嵌入式管 離上可以使用的嵌入式 離面 小 小 心 がはrosoft Corp Microsoft Corp	<b>理單元余</b> 新増或移除的 <sup>諸理單元中選擇一:</sup>	其法後點學「確 人式管理單元,並且設定所 選取的嵌入式管理單元(E): ■主控台根目錄 ■洒證(本機電腦)	F選擇的嵌入式管理單元・對於可延伸的 編輯延伸(べ) 修除(R) 上移(U) 下移(D) 進階(V)

# 八、 在憑證樹的「個人」資料夾中按滑鼠右鍵選「所有工作」 匯入

<b>-</b>		主控台1 - [主控台根目録\憑證 (本機電腦)\個人]	_ 🗆 X
搹 檔案(F) 重	动作(A) 檢視(V) 我的最愛(O)	視窗(₩) 説明(H)	_ 8 ×
(= =) 2	T 📋 🖬 🖬 🔳 🖬		
主控台根目:	錄物件類型	動作	
▲ 憑證 (本	機電腦)	這個檢視沒有項目可顧示。 個人	
	■ 封憑證(N)	其他動作	•
	6 月41日 (4 ) M	■ 幸珍馮諳(N)	
	檢視(\) ▶	華公共演講(R)	
	從這裡開啟新視窗(W)	匯入()	
Þ 🛄 1	新工作台檢視(T)	進階操作(A) ▶	
	重新整理(F)		
Þ 🧰	匯出清單(L)		
	說明(H)		
▶ 🧰 信任	的裝置		
⊳ 📔 Weł	b Hosting		
將憑證新增到存			
<u> </u>			
ገነ ነ	<b>∀「瀏覓」</b> 】	医择網站您寇旳米源路倥俊按 「 ト 一 歹 」	
			Y
		la de la constante de la const	
	🙆 🌽 馮諮匯λ	特面	
	要匯入的檔案		
	指定你相	目要匯入的檔案。	
	JH AL ASA		
			-
	檔案名科	爯(F):	
	icate\4	41089325\441089325\CER - CRT Files\ssl net-chinese tw.crt 瀏覽(R)	
	注意: 您	『可以將數個憑證用以下的格式存放在同一個檔案中:	
	個人	資訊父換- PKCS #12 (.PFX,.P12)	
	<b></b> 家種	组課訊 自語法 / / / / / / / / / / / / / / / / / / /	
	Micr	osoft 序列憑證存放區 (.SST)	
			_
		下一步(N) 取消	

	<b>;擊憑證進人精靈的</b> 對詁框「確認」按鈕	
	主控台1 - [主控台根目錄\憑證 (本機電腦)\個人]	_ 🗆 X
福案(F) 動作(A) 檢視(V) 我 ◆ ➡ 2 〒 □ □ 0 ➡	我的最爱(O) 視蜜(W) 說明(H) 【□ 1000 1000 1000 1000 1000 1000 1000 1	_ <i>E</i> ×
<ul> <li>◆●◆ ② 〒 □ ○ ●</li> <li>● 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</li></ul>	●       ●         ●       ● <td< td=""><td></td></td<>	
個人 在放原並去句含馮證。		

在匯入憑證後,您必須按右鍵將之重新整理,已匯入的憑證就會在裡面。 但請注意,用 MMC 主控台方式匯入的終端憑證,此時是不可以用在網站繫結的,您在 IIS 會看不到這張憑證。您必須將金鑰進行指派給憑證(憑證旁邊會有金鑰圖示)

發給  ▼	簽發者	到期日	使用目的
🔄 ssl.net-chinese.tw	Sectigo RSA Domain Validation	2022/1/22	伺服器驗證, 用戶端
1	未將金鑰與憑證進行關聯時的狀	態	
發給  ▼	簽發者	到期日	使用目的

發給	簽發者	到期日	使用目的
🛱 ssl.net-chinese.tw	Sectigo RSA Domain Validation	2022/1/22	伺服器驗證, 用戶端

已將金鑰指派給憑證時的狀態





#### 一二、 在搜尋輸入「CMD」或「命令提示字元」開啟主控台



#### 一三、 輸入以下指令讓憑證與私密金鑰相關聯

#### 主控台

certutil -repairstore my "SerialNumber"

SerialNumber 是您在步驟 11 查看的憑證序號

#### 指令實際執行結果



一四、	<b>淮</b> ,	入中約	繼憑證 -	在中繼憑證	授權單	單位 \ 憑	證下按右	鍵匯入
<b>-</b>			主控台1 - [	[主控台根目錄\憑證 (本機電腦	)\中繼憑證授相	權單位\憑證]		_ 🗆 X
🚟 檔案(F) 動作	F(A) 檢視(V) 我i	的最愛(O) 視	l窗(W) 說明(H)					_ & ×
🗢 🔿 🔽 🗖	1 🗟 🗟	2 🗖						· · · · · · · · · · · · · · · · · · ·
📔 主控台根目錄		發給	•	簽發者	到期日	使用目的	動作	
⊿ 🗊 憑證 (本機	電腦)	www.veri	sign.com/CPS Incorp	Class 3 Public Primary Certificati	2016/10/25	伺服器驗證,用戶端	憑證	<b></b>
		USERTru	st RSA Certification A	AAA Certificate Services	2029/1/1	<全部>	其他動作	۱.
▷ □ 支信任 ▷ □ 文信任	时依您超过催单业 任	Sectigo F	RSA Domain Validati	USERTrust RSA Certification Aut	2031/1/1	伺服器驗證,用戶端		
▲ 🗎 中編憑	」 語授權單位	Root Age	ency	Root Agency	2040/1/1	<注部>		
	<u>-</u> 		t windows Hardware ificata Soniicae	AAA Costificate Services	2002/12/31	程式碼發著, VVINDO 田氏時輪路 紀式碑		
	8	Car Cert	TEL D	Add Certificate Services	2023/1/1	/四/一/呵叔道,/孟少/吻…		
<b>↓</b> ● ● ●	所有⊥作(K)	,	№ 人(I)	1				
27 没有	檢視(∨)	•						
	從這裡開啟新視調	韽(W)						
	新工作台檢視(T)							
▷ 📔 遠如	重新整理(F)							
▶ 🔛 憑證	匯出清單(L)							
▶ 📫 信任	說明(H)		-					
þ 🚞 Web F	losting							

一五、 選擇中繼憑證存放位置為本機電腦

◎ 🥏 憑證匯入精靈	×
歡迎使用憑證匯入精靈	
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。	
憑證由憑證授權單位簽發,能識別您的身分,並包含用來保護資料或建立安全網路連線的資 訊,憑證存放區是用來存放憑證的系統區域。	
─存放位置 〇 目前使用者(C)	
<ul> <li>◎ 本機電腦(L)</li> <li>請按 [下一步] 繼續。</li> </ul>	
下一步(N) 取	(消

一六、 選擇中繼憑證來源路徑後進行下一步

€ 🦻 🤅	慿證匯入精靈 	
要	匯入的檔案	
	指定您想要匯入的檔案。	
	檔案名稱(F):	_
	5\CER - CRT Files\SectigoRSADomainValidationSecureServerCA.crt 瀏覽(R)	
	注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:	
	個人資訊交換- PKCS #12 (.PFXP12)	
	密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)	
	Microsoft 序列憑證存放區 (.SST)	
	下一步(N)	取消
彈	ा □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	取消
逻	下-步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」並 <sup>憑證存放區是用來存放憑證的系統區域,</sup>	<sup>取消</sup> 進行下
選	下-步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」並 <sup>憑證存放區是用來存放憑證的系統區域,</sup>	<sup>取消</sup>
選	下一步(N) <b>選擇中繼憑證存放區為「中繼憑證授權單位」並</b> 透證存放區是用來存放憑證的系統區域。 Windows 可自動導取憑證存放區,你也可以為憑證指定存放位置。	<sub>取消</sub>
選	下一步(N) <b>選擇中繼憑證存放區為「中繼憑證授權單位」並</b> 憑證存放區是用來存放憑證的系統區域。 Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。	<sub>取消</sub> 進行下
選	下一步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」並 憑證存放區是用來存放憑證的系統區域。 Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。 〇 自動根據憑證類型來選取憑證存放區(U)	取消 進行下
選	下一步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」並 憑證存放區是用來存放憑證的系統區域。 Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。 〇 自動根據憑證類型來選取憑證存放區(U) ④ 將所有憑證放入以下的存放區(P)	<sub>取消</sub>
選	下一步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」並 應證存放區是用來存放憑證的系統區域。 Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。 () 自動根據憑證類型來選取憑證存放區(U) @ 將所有憑證放入以下的存放區(P) 透證存放區:	<b>取消</b> <b>進行下</b>
選	下一步(N) <b>医存 加                                   </b>	<b>取消</b> <b>進行下</b>
選	下一步(N) 選擇中繼憑證存放區為「中繼憑證授權單位」が 應證存放區是用來存放憑證的系統區域。 Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。 () 自動根據憑證類型來選取憑證存放區(U) ⑧ 將所有憑證放入以下的存放區(P) 憑證存放區: 中繼憑證授權單位	<sub>取消</sub> 進行下
選	F 一步(N)     法     医     医     医     医     医     医     医     医     酸     医     酸     医     酸     医     酸     的     酸     酸     酸     的     的     和     题     的     和     题     的     和     题     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和     的     和      的     和      的      和      的      和       和       和        和         和	取消 ■
選		取消 ■
選		<b>取</b> 満 <b>進行下</b>
選	正	<b>取消</b> <b>進行下</b>
選	F 一步(N)	取消
選		

一八、 點擊完成

€ ∌ 慿	證匯入精靈			x	
5	記成憑證匯入精靈				
技	:一下 [完成],即可匯入憑;	B •			
也 ;	记指定下列設定: 使用者攫取的憑證存放區 內容 檔案名稱	中繼憑證授權單位 憑證 C:\Users\Administrator\Desk	top\Certificate\441089	9325\441089	
	¢	ш		>	
九、點	擊憑證匯入精	<b>埥靈的對話框「</b> 碍	<sup></sup> 確認」按鈕	F)	
	主控台1 - [ 的最愛(O) 視窗(W) 說明(H)	主控台根目錄\憑證 (本機電腦)\中繼憑	[證授權單位\憑證]	L	_ & ×
🗢 🔿 🙇 📰 📋 🙆 📄					
<ul> <li>主控合視目錄</li> <li>ご 法證 (本機電腦)</li> <li>○ 個人</li> <li>○ 受信任的根憑證授權單位</li> <li>○ 企業信任</li> <li>○ 要信任的報行者</li> <li>○ 受信任的發行者</li> <li>○ 受信任的發行者</li> <li>○ 受信任的發行者</li> <li>○ 受信任的發行者</li> <li>○ 受信任的人</li> <li>○ 第三方根憑證授權單位</li> <li>○ 受信任的人</li> <li>○ 第三方根憑證授權單位</li> <li>○ 當購真面</li> <li>○ 證購真</li> <li>○ 證購真</li> <li>○ 智慧卡信任根目錄</li> <li>○ 信任的裝置</li> <li>▷ ○ Web Hosting</li> </ul>		登發書    到期日 Class 3 Public Primary Certificati AAA Certificate Services    2031/1/ USERTrust RSA Certification Aut  2031/1/ Rotter	使用目的 (1 < 全部> (1 < 全部> (1 の服器驗證,用戶端) (1 の服器驗證,用戶端) (1 < 全部> (2)31 程式碼接電,Windo) (1 用戶端驗證,程式碼)	作 <u>長證</u> 其他動作	<b>A</b> 7

二〇、 匯之	入根》	ふうしょう あうしょう ひちょう しんしょう しんしょう しんしょう しんしょう しんしん しんしょう しんしょう しんしん しんしょう しんしょ しんしょ	受信任的憑	證授權	<b>輩單位 \</b> 3	憑證下	匯入
-		主控台1 - [主持	空台根目錄\憑證 (本機電腦)\受	信任的根憑證	授權單位\憑證]		_ 🗆 X
🔜 檔案(F) 動作(A) 檢視(V) 我的	的最愛(O) 視窗	ā(W) 說明(H)					_ & ×
	- <b>-</b>	•	答發者	到期日	使用目的	thu∉	
⊿ 🗊 憑證 (本機電腦)	VeriSign Cl	lass 3 Public Primar	VeriSign Class 3 Public Primary	2036/7/17	用戶端驗證,程式改	進路	
↓ □ 個人	USERTrust	RSA Certification A	USERTrust RSA Certification Aut	2038/1/19	用戶端驗證,程式码		-
受信任的根憑證授權單位	TWCA Roo	ot Certification Auth	TWCA Root Certification Author	2030/12/31	用戶端驗證,程式研	具他動作	•
	· •	躍入の	nawte Timestamping CA	2021/1/1	時間戳記		
	· ·	EE/(()	arfield Class 2 Certification Au	2034/6/30	用戶端驗證,程式和		
→ □ 平準/ 檢視(V)	+	CA	SecureTrust CA	2030/1/1	用戶端驗證,程式和		
▶ 2 5 6 0 2 6 0 2 6 1 1 1 1	見窗(VV)	Y ACCEPTED, (c)9	NO LIABILITY ACCEPTED, (c)97	2004/1/8	時間戳記		
▶ 😁 第二, 新工作台檢視(1	T)	oot Certificate Aut	Microsoft Root Certificate Auth	2036/3/23	<全部>		
		oot Certificate Aut	Microsoft Root Certificate Auth	2035/6/24	<全部>		
		oot Certificate Aut	Microsoft Root Certificate Auth	2021/5/10	<全部>		
▷ 📫 遠端貞 🚈 // // // // // // // // // // // // //		oot Authority	Microsoft Root Authority	2020/12/31	<全部>		
▶ 🧰 憑證記 🛛 說明(H)		uthenticode(tm) R	Microsoft Authenticode(tm) Ro	2000/1/1	安全電子郵件,程式		
▶ 🧰 智慧卡信仕根目録	Co Daddy	Root Certificate Au	Go Daddy Root Certificate Auth	2038/1/1	用戶端驗證,程式研		
▶ 🚞 信任的裝置	🔄 Go Daddy	Class 2 Certificatio	Go Daddy Class 2 Certification	2034/6/30	用戶端驗證,程式4≡		
Web Hosting	🔄 🔄 GlobalSigr	n Root CA	GlobalSign Root CA	2028/1/28	用戶端驗證,程式和		
	GlobalSigr	n	GlobalSign	2029/3/18	用戶端驗證,程式和		
	GlobalSigr	n	GlobalSign	2021/12/15	用戶端驗證,程式研		
	ePKI Root 🛛	Certification Author	ePKI Root Certification Authorit	2037/12/31	用戶端驗證,程式研		
	🔄 ePKI Root (	Certification Author	ePKI Root Certification Authority	2034/12/20	用戶端驗證,程式和		
	Entrust Roo	ot Certification Aut	Entrust Root Certification Autho	2030/12/8	用戶端驗證,程式研		
	🔄 DST Root (	CA X3	DST Root CA X3	2021/9/30	用戶端驗證, 文件劉		
	🔄 DigiCert Hi	igh Assurance EV R	DigiCert High Assurance EV Ro	2031/11/10	用戶端驗證,程式和		
	🔄 🔄 DigiCert Gl	lobal Root G2	DigiCert Global Root G2	2038/1/15	用戶端驗證,程式和		
	🔄 🗔 DigiCert G	lobal Root CA	DigiCert Global Root CA	2031/11/10	用戶端驗證,程式研		
	🔄 🔄 DigiCert As	ssured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	用戶端驗證,程式和		
	Copyright	(c) 1997 Microsoft	Copyright (c) 1997 Microsoft C	1999/12/31	時間戳記		
	🔄 🔄 Class 3 Pub	olic Primary Certific	Class 3 Public Primary Certificati	2028/8/2	用戶端驗證,程式码		
	🔄 🔄 Certum CA	к.	Certum CA	2027/6/11	用戶端驗證,程式码		
	🔄 🔄 Baltimore (	CyberTrust Root	Baltimore CyberTrust Root	2025/5/13	用戶端驗證,程式码		
	AddTrust E	xternal CA Root	AddTrust External CA Root	2020/5/30	用戶端驗證,程式到❤>		
將憑證新增到存放區	p					,	

根憑證的匯入其步驟與匯入中繼憑證的步驟 15-19 雷同,唯憑證存放區域不一樣,但存放區 應是與您選擇之憑證樹下存放區的資料夾雷同,故不再贅述步驟。

若有必要,請在「第三方根憑證授權單位 \ 憑證」下一併匯入根憑證。

「受信任的根憑證授權單位」與「第三方根憑證授權單位」的差別,依據微軟的說明其差異 性如下:

#### 受信任的根憑證授權

隱含的信任憑證授權單位。包括所有在[第三方根憑證授權單位]存放檔中的憑證,以及來自您的組織及 Microsoft 的根憑證。

如果您是系統管理員,而且想要將協力廠商憑證授權單位授予的憑證新增至此存放區中,以供 Windows Server 2003 Active Directory 網域中的所有電腦使用,則可使用[群組原則]將受信任的根憑證分送到您的組織中。如需相關資訊,請參閱信任的根憑證授權 原則

#### 第三方根憑證授權單位

此受信任根憑證是指來自 Microsoft 或您組織以外的憑證授權單位。

有關於各品牌中繼憑證與根憑證資訊,請參閱附錄資料。

#### C、 使用「匯入」方法將 PFX 格式憑證匯入 IIS 或 MMC

#### 使用對象:

- 1. 原先以 Linux 或其他開放平台生成 CSR 與私密金鑰的使用者。
- 2. 購買了多域名型憑證或是通用型憑證且有混合佈署的使用者。
- 3. 有做混合系統部署或是 Web Farm 等多主機負載平衡的使用者。

## 將 PFX 格式憑證匯入 IIS

## 一、打開 IIS 並點選「伺服器憑證」後,按下動作欄的「匯入」

<b>8</b> ]	Internet Information Services (IIS) 管理員	_ <b>D</b> X
		😰 🛛 🟠 I 🕖 🗸
檔案(F) 檢視(V) 說明(H)		
建築           ●         ●	<ul> <li>● 印服器憑證</li> <li>此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站描配使用的憑證。</li> <li>● ● 移至(G) ● ● 全部顯示(A) ■ 群相依據: 憑證儲存區 ●</li> <li>● ● 各至(G) ● ● 全部顯示(A) ■ 群相依據: 憑證儲存區 ●</li> <li>● ● 各至(G) ● ● 全部顯示(A) ■ 群相依據: 憑證儲存區 ●</li> <li>● ● 各至(G) ● ● 全部顯示(A) ■ 報信</li> </ul>	b/r           僅入           建立透證要求           完成憑證要求           建立自我簽署憑證           設印己更新憑證的自動重新繁 這           ? 說明
就緒		Sec. 19

#### 什麼是 PFX 格式?

在密碼學之中, PKCS#12 定義了一種存檔格式,通常用它來打包一個私密金鑰 及有關的 X.509(PEM 格式) 憑證,或者是信任鏈的全部項目。

一個 PKCS#12 格式文件通常是被加密的,同時又單獨存在(存檔文件格式)。所以可以用一個容器的概念去理解它 - 一個裡面放了憑證與金鑰,且上了密碼鎖的箱子。

常用的副檔名格式為 .P12、.PFX。

可以透過 OpenSSL 的指令對 PFX 文件進行打包、拆包的轉換工作。

## 二、選取憑證來源並輸入密碼,選擇憑證儲存區後,按下「確定」。

匯入憑證 ? ×
憑證檔案 (.pfx)(C):
Iministrator\Desktop\Certificate\webcertificate.pfx
密碼(P):
選取憑證儲存區(S):
個人 🗸
✔ 允許匯出此憑證(A)
確定 取消

小提醒:

如果未來還有想要在這台主機上匯出憑證時,請記得勾選「允許匯出此憑證」

## 三、若是在這邊有看到憑證,即代表憑證匯入成功。

<b>8</b> ]	Internet Information Services (IIS) 管理員	_ <b>D</b> X
		🎦 🛛 🟠 🔞 -
檔案(F) 檢視(V) 說明(H)		
(目典(F) 性优(V) 武明(H)       遵總     ● <td>● 加路憑證</td> <td>國入           建立憑證要求           完成憑證要求           建立領域憑證           建立自我簽書憑證           檢視           選出           要新           ※ 移除           歐用已更新憑證的自動重新繫結           20</td>	● 加路憑證	國入           建立憑證要求           完成憑證要求           建立領域憑證           建立自我簽書憑證           檢視           選出           要新           ※ 移除           歐用已更新憑證的自動重新繫結           20
就緒		€1.:

## 將 PFX 格式憑證匯入 MMC 一、 在憑證樹的「個人」資料夾中按滑鼠右鍵選「所有工作」 匯入

福宾(F) 動作(A) 檢視(V) 我的最愛(O) 視蜜(W) 說明(H)	_ <b>D</b> X
	_ & ×
道個檢視沒有項目可顯示・	· ·
● ● ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○	,
▶ 10     ★ 10 ± 1 + 0 ⊈     ★ 10 ± 1 + 0 ⊈       ▶ 10     ★ 横視(V)     ▶         要求新憑證(R)	
▶ 🖆 從這裡關啟新視窗(W) <b>匯入()</b>	
▶ <mark>新</mark> 工作台檢視(T) 進階操作(A) ▶	
▶ C2 / 重新整理(F) ▶ C2 / 面中注意(1)	
▶ 3 信任的装置	
▶ 🞽 Web Hosting	
將憑證新增到存放區	
一、'坎「瀏覽」 選擇細趾馮證的本酒,無誤後'块「下——先」。	
_ * 孩 · 澍見」送洋禍如忽竝的木麻 / 無砆反孩 ·   * 少」 *	
📀 🍠 憑證匯入精靈	
要匯入的檔案	
<b>要匯入的檔案</b> 指定您想要匯入的檔案。	
要匯入的檔案 指定您想要匯入的檔案。	
<b>要匯入的檔案</b> 指定您想要匯入的檔案。 	
要匯入的檔案 指定您想要匯入的檔案。 	
要匯入的檔案 指定您想要匯入的檔案。 檔案名稱(F): C\Users\Administrator\Desktop\Certificate\webcertificate pfx	
要匯入的檔案 指定您想要匯入的檔案。 檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx 瀏覽(R)	
要匯入的檔案 指定您想要匯入的檔案。 檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx 瀏覽(R)	
要匯入的檔案 指定您想要匯入的檔案。 檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx 瀏覽(R) 注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:	
要匯入的檔案 指定您想要匯入的檔案。 檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx 瀏覽(R) 注意: 您可以將數個憑證用以下的格式存放在同一個檔案中: 個人資訊交換- PKCS #12 (.PFX,.P12)	
要匯入的檔案 指定您想要匯入的檔案。	
要匯入的檔案 指定您想要匯入的檔案。	
要匯入的檔案 指定您想要匯入的檔案。          檔案名稱(F):       C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx       瀏覽(R)         注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:       個人資訊交換-PKCS #12 (.PFX,.P12)         密碼編譯訊息語法標準-PKCS #7 憑證 (.P7B)       Microsoft 序列憑證存放區 (.SST)	
<ul> <li>要匯入的檔案</li> <li>指定您想要匯入的檔案。</li> <li>檔案名稱(F): <ul> <li>C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx</li> <li>瀏覽(R)</li> </ul> </li> <li>注意: 您可以將數個憑證用以下的格式存放在同一個檔案中: <ul> <li>個人資訊交換-PKCS #12 (.PFX,.P12)</li> <li>密碼編譯訊息語法標準-PKCS #7 憑證 (.P7B)</li> <li>Microsoft 序列憑證存放區 (.SST)</li> </ul> </li> </ul>	
要匯人的檔案 指定您想要匯人的檔案。           檔案名稱(F):         C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx         瀏覽(R)           注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:         個人資訊交換-PKCS #12 (.PFX,.P12)         密碼編譯訊息語法標準-PKCS #7 憑證 (.P7B)           Microsoft 序列憑證存放區 (.SST)         Microsoft 序列憑證存放區 (.SST)	
#庭您想要匯入的檔案。     描定您想要匯入的檔案。 檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx	
<b>要匹人的檔案</b> 指定您想要匯人的檔案。	
理定您想要匯人的檔案。   描定您想要匯人的檔案。   信案名稱(F):   C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx   瀏覽(R)   注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:   個人資訊交換-PKCS #12 (.PFX,.P12)   密碼編譯訊息語法標準-PKCS #7 憑證 (.P7B)   Microsoft 序列憑證存放區 (.SST)	
医型子科学校会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社	
歴史的檔案 指定您想要匯人的檔案。                健案名稱(F):             C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx	
要匹入的檔案 指定您想要匯入的檔案。           檔案名稱(F):         ①\Users\Administrator\Desktop\Certificate\webcertificate.pfx         瀏覽(R)           注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:         個人資訊交換- PKCS #12 (.PFX,.P12)         密碼編譯訊息話法種進- PKCS #7 憑證 (.P7B)           Microsoft 序列憑證存放區 (.SST)         Microsoft 序列憑證存放區 (.SST)	
医型 加速	
<section-header>     box 2005 2005 2005 2005 2005 2005 2005 200</section-header>	

Windows Server 2012/P			
WINDOWS SEIVEI ZOIZ/K	Windo	vs Serve	r 2012/R2

-	開啟			X
⊜ ⊜ ∞ ↑ 💵 •	Certificate 🕨	~ ¢	搜尋 Certificate	م
組合管理 ▼ 新増資料	科夾		: :==	• 🔲 🔞
☆ 我的最愛	名稱	修改日期	類型	大小
🚺 下載	441089325	2021/1/21 下午 0	檔案資料夾	
■ 桌面	퉬 ssl_net-chinese_tw	2021/1/21 下午 0	檔案資料夾	
週 最近的位置	🍃 webcertificate.pfx	2021/1/21 下午 0	個人資訊交換	4 KB
⊪壘 本機				
福	案名稱(N): webcertificate.pfx	<b>~</b>	個人資訊交換 (*.pfx; X.509 憑證 (*.cer;*.cr 個人資訊交換 (*.pfx; 憑證信任清單 (*.st)	*.p12) v t) *.p12)
			<ul> <li>&gt;</li></ul>	字放區 (*.sst) *.p7b)

如果在瀏覽時找不到 PFX 格式,請記得在旁邊的下拉選單選取「個人資訊交換 (\*.pfx;\*. p12)」

# 三、 輸入 PFX 密碼,如未來有匯出需求請把匯入選項中的方塊打勾

€ 🦻 慿	證匯入精靈
私密	金 <b>鑰保護</b> 為了維護安全性,私密金鑰受到密碼保護。
	請輸入私密金鑰的密碼。
	密碼(P): ●●●●●●●●
	□ 顯示密碼(D) 匯入選項(I):
	□ 啟用加強私密金鑰保護。如果您啟用這個選項,每次私密金鑰被應用程式使用,系統 便會通知您(E)
	✓將這個金鑰設成可匯出。這樣您可以在以後備份或傳輸您的金鑰(M)
	✔ 包含所有延伸內容。(A)
	下一步(N) 取消

四、選擇憑證存放區為「個人」,無誤後按「下一步」

중 🦻 憑證匯入精靈
海路方故回
憑證存放區是用來存放憑證的系統區域。 
Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。
○ 自動根據憑證類型來選取憑證存放區(U)
● 將所有憑證放入以下的存放區(P)
憑證存放區: 個人 瀏覽(R)
下一步(N) 取消
確認匯入資訊,無誤後按「完成」
完成憑證匯入精靈
按一下 [完成],即可匯入憑證。
您已指定下列設定:
使用者選取的憑證存放區 個人 內容 PFX
檔案名稱 C:\Users\Administrator\Desktop\Certificate\webcertificate.pfx

完成(F)

取消

五、

#### 六、點選「確定」結束匯入成功的對話方塊。



在這個章節中分別示範了兩種匯入憑證的方法,兩者都可以使用。主要還是看憑證發行機構 給你何種類型的憑證,還有取決於您需不需要匯入中繼憑證、根憑證等信任鏈憑證的需求。

PFX 的確是一個比較麻煩的格式,需要做拆解包的動作,這個動作需要借助一些工具來執行,將會在後面進行教學。



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、在 IIS 的「站台」圖示點右鍵選擇「編輯繫結」

<b>V</b>				Internet Informa	tion Servio	ces (IIS) 管理員			
🕞 💽 🖣 🕨 WINSRV	2012	•							
檔案(F) 檢視(V) 說明(H)	)								
建線 ◆ 日   △   ● ● 起始網頁 ▲ ● WINSRV2012 (WINSR)	V201	<b>●</b> 伺服器 此功能可用來要求及	長證 管理網頁伺服	器可與針對 SSL 設定的網	站搭配使用的	)憑證。			動作 () 建:
@ 應用程式集區		篩選器:	- 1	『移至(G) → 3 全部顧う	⊼(A) │群組依	対線:憑證儲存區 ▼			· · · · · · · · · · · · · · · · · · ·
⊿ ··•• म⊟ 		244 ●		發行給	發行	う者 しんしん しんしん しんしん しんしん しんしん しんしん しんしん しん	到期日	憑記	建:
	<u>,</u>	瀏覽 編輯權限		ssl.net-chinese.tw	Sec	tigo RSA Domain Valida	22/1/2022 7:59:59	81E	檢
	<b>P</b>								匯!
	2	新増虛擬目錄							₩ 移
		編輯繫結							) (th
		管理網站 ▶							#日 ② 論!
	<b>*</b> 2	重新整理(R)							-
	×	移除 							
		新増 FTP 發行							
		重新命名 							
		切換到內容檢視							

## 二、在站台繫結中先點「新增」

			站台	繋結	? X
類型	主機名稱	連接埠	IP位址	繫結資訊	新増(A)
http		80	*		編輯(E) 稼穡(P)
					<sup>授标(R)</sup> 瀏覽(B)
					關閉(C)

## 三、類型選擇「HTTPS」且 SSL 憑證下拉您匯入的憑證

新增站台繫結	? X
類型(T): IP 位址(0): https ✓ 全部未指派 主機名稱(H): 	連接埠(O): ✓ 443
SSL 憑證(F): ssl.net-chinese.tw	選取(L) 檢視(V) 確定 取消

在您選擇類型為https時,預設的連接埠是443,除非有特殊需求,否則無需更動連接埠號碼。若您對此做了更動,建議您在聯外路由及防火牆開通相應的連接埠接口。

如果您有多個 Virtual Host( 虛擬主機 ), 主機名稱要設定含主機名稱網址, 例如: mail.net-chinese-.tw

#### 四、確認站台繫結中已新增了 HTTPS 後關閉視窗

			站台	繋結	? X
類型	主機名稱	連接埠	IP 位址	繫結資訊	新増(A)
http		80	÷		
https		443	*		編輯(E)
					移除(R) 瀏覽(B)
					關閉(C)

## 五、重新啟動 IIS

Internet Information Services (IIS) 管理員	_ <b>_</b> ×
● WIINSRV2012 → 站台 → Default Web Site →	😉 🗠 👔 😰 🗸
檔案(F) 檢視(V) 說明(H)	
Table () 推視() 推問() Table () 推視() 推問(*) Table () 推阅(*) 推問(*) Table () 推阅(*) 推問(*) Table () 推阅(*) Table () Tabl	動作          瀏覽         編輯編現       編輯編現         編輯編現       「編輯集累         續編團用程式       後視應用程式         檢視應用程式       後視應用程式         後視應用程式       (http://www.statumerecommunity.commun
就緒	• <u>1</u> .:

# 六、開啟瀏覽器進行測試

IIS Windows Server × +	_ <b>D</b> X
← → C ▲ 不安全 ssl.net-chinese.tw	⊞ ☆ 🖰 :
Internet Information Services	
Welcome Bienvenue Tervetuloa	
גאָביד Benvenuto 軟迎 Bienvenido Hoş geldiniz ברוכים הבאים	Welkom
Bem-vindo Καλώς Vítejte ορίσατε Välkommen 환영합니다 Добро пожаловать Üdvözöljük	
双관 双관	

#### 為什麼會顯示不安全?

當您設好了繫結,也放了憑證,為什麼還是顯示不安全呢?在上一步的站台繫 結中,我們同時了保留連接埠 80 的非安全通道,及新增了 443 埠的安全通道, 所以實際上網站的運作是安全通道及非安全通道都可以開啟網頁的。我們在這 裡不建議您刪除 80 埠的非安全通道,因為您沒有辦法預期客戶會怎樣開啟您 的網頁,會建議您改用導轉的方式將其導引至安全的通道。(請參照附錄 A)

讓我們試著在網址前加入「https」看看吧。

$\leftrightarrow$ $\rightarrow$ G	٢	https://ssl.net-chinese.tw		θ	:
Winc	٢	IIS Windows Server - https://ssl.net-chinese.tw	×		
	Q	https://ssl.net-chinese.tw - Google 搜尋			

一般的網頁都會有快取 (Cache) 機制,其作用是將您瀏覽過的頁面預存在電腦中,再透過 Cookie 的方式做一些記憶,所以很多時候當您只輸入 URL 而不特別加前置的 http://或 https://時,瀏覽器都會用您過去瀏覽的經驗去連接該網站的主機。所以您必須告訴瀏覽器 說您要走的通道是加密或非加密的通道。



加入了「https://」後,是不是看到鎖頭出現了呢?這樣代表憑證設置已經完成



# 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。

#### 在 IIS 中匯出憑證

## 一、在「伺服器憑證」選擇憑證後於動作欄中選擇「匯出」

③ Internet Information Services (IIS) 管理員	_ <b>D</b> X
€ WINSRV2012 >	🔯 🖂 🏠 🕡 -
檔案(F) 檢視(V) 說明(H)	
正式     ● CHOY       ● CHOY     ● DBR 器 憑 證       ● DBR 器 憑 證     ● DBR 器 憑 證       ● DBR 器 憑 證     ● DBR 器 憑 證       ● Default Web Site     ● ● Efault Web Site       ● Default Web Site     ● ● Efault Web Site	個人           建立應證要求           完成憑證要求           建立網域憑證           建立自我簽署憑證           檢視           夏新           珍除           數用己更新憑證的自動重新繫結           說明
就維	¶.:

## 二、選定存檔的路徑並自行設定密碼

匯出憑證 <b>? ×</b>
匯出到(E):
C:\Users\Administrator\Desktop\Certificate\webce
密碼(P):
•••••
確認密碼(M):
確定 取消

## 三、到存檔路徑找尋匯出的憑證

🌆 l 💽 🚯 = l			Certificate				x
檔案 常用 :	共用	檢視					~ <b>?</b>
🔄 🕘 🔻 🚺	► Ce	rtificate 🕨		v ¢	搜尋 Certificate		Q,
🕎 我的最愛	^	名稱	修改日期		類型	大小	
🚺 下載		441089325	21/1/2021 1	4:12	檔案資料夾		
📰 桌面	≡	🚡 ssl_net-chinese_tw	21/1/2021 1	4:12	檔案資料夾		
🗐 最近的位置		溕 webcertificate.pfx	21/1/2021 1	4:55	個人資訊交換		4 KB
₂壘 本機	~						
3 個項目							:== <b>&gt;</b>

## 在 MMC 中匯出憑證

# 一、在 MMC 的「憑證 ( 本機電腦 )」中個人項下的憑證點右鍵匯出

<b>a</b>		主控台1 - [主控台	ἀ根目錄∖憑證 (本機電腦)∖個人	\馮證]	_	
🚰 檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視音	읍(W) 說明(H)					_ & ×
🗢 🔿 🙍 📰 🤞 🛍 📷						
	發給	•	簽發者	到期日 使	動作	
▲ 📦 憑證 (本機電腦) ▲ 🔗 個人	🙀 ssl.net-c	開啟(O)	ctigo RSA Domain Validation	2022/1/22  伺	憑證	<b>^</b>
□ 憑證		所有工作(K)	▶ 開啟(O)		其他動作	•
▶ 2 受信任的根憑證授權單位 ▶ 2 企業信任		剪下(T)	以新的金鑰要求憑證(Q)		ssl.net-chinese.tw	-
▶ 🔛 中繼憑證授權單位		複製(C)	以新的金鑰更新憑證(N)		其他動作	•
▶ 2 受信任的發行者 ▶ 2 没有信任的通過		刪除(D)	管理私密金鑰(M)			
▶ 🛄 沒有信任的想題 ▶ 🛄 第三方根憑證授權單位		內容(R)	進階操作(A)	•		
▶ 🥶 受信任的人		說明(H)	匯出(E)			
▶ ☐ 用戶喃眾證證錄音 ▶ ☐ 遺端桌面						
▶ 🧰 憑證註冊要求						
▶ 🔄 智慧卞信仕根目録 ▶ 🎬 信任的裝置						
⊳ 🖺 Web Hosting						
	<	ш		>		

#### 二、在憑證匯出精靈中按下一步繼續。

◎ 🦻 憑證匯出精靈	X
歡迎使用憑證匯出精靈	
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從憑證存放區複製到您的磁碟中。	
憑證由憑證授權單位簽發,能識別您的身分,並包含用來保護資料或建立安全網路連線的資 訊。憑證存放區是用來存放憑證的系統區域。	
請按 [下一步] 繼續。	
下一步(N)	取消

## 三、選取「是,匯出憑證金鑰」後按「下一步」

중 🤣 憑證匯出精靈
<b>匯出私密金鑰</b> 您可以選擇將私密金鑰與憑證一起匯出。
私密金鑰受到密碼的保護。如果您要將私密金鑰與憑證一起匯出,您必須在下一頁輸入密 碼。
您想將私密金鑰與憑證一起匯出? <ul> <li>夏,匯出私密金鑰(V)</li> <li>否,不要匯出私密金鑰(O)</li> </ul>
下一步(N) 取消

## 四、選擇個人資訊交換並勾選包含路徑所有憑證及匯出延伸內容

중 🤌 憑證匯出精靈	X
匯出檔案格式 憑證可以用多種檔案格式匯出。	
請選取您想要使用的格式:	
〇 DER 編碼二位元 X.509 (.CER)(D)	
○ Base-64 編碼 X.509 (.CER)(S)	
○ 密碼編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)	
□ 如果可能的話,包含憑證路徑中的所有憑證(1)	
● 個人資訊交換 - PKCS #12 (.PFX)(P)	
✔ 如果可能的話,包含憑證路徑中的所有憑證(U)	
□ 如果匯出成功即刪除私密金鑰(K)	
✔ 匯出所有延伸內蓉(A)	
○ Microsoft 序列憑證存放區 (.SST)(T)	
	下一步(N) 取消

#### 五、設定密碼後按下「下一步」

长 🍠 憑證	· · · · · · · · · · · · · · · · · · ·
安全性為	: ;維護安全性,您必須保護安全性主體的私密金鑰,或透過密碼保護。
	] 群組或使用者名稱 (建議選項)(G)
	新T用(A) 移除(R)
V	] 密碼(P):
	· · · · · · · · · · · · · · · · · · ·
	下一步(N) 取消

## 六、點選「瀏覽」設定儲存路徑

	x
중 🥭 憑證匯出精靈	
要匯出的檔案 請指定你要匯出的檔案名稱	
檔案名稱(F):	
瀏覽(R)	-
T than	HIT SYL
	41.27月

## 七、選好路徑輸入檔名後按「存檔」

<b>E</b>	另存新檔				x
🔄 🔄 = 🕇 퉬 🕨 C	ertificate 🕨	~ ¢	搜尋 Certificate		<i>م</i>
組合管理 ▼ 新増資料水	3				0
☆ 我的最愛	名稱	修改日期	類型	大小	
<ul> <li>▶ 下載</li> <li>■ 桌面</li> <li>2 最近的位置</li> <li>● 本機</li> <li>● 細路</li> </ul>	♣ 441089325 ♣ ssl_net-chinese_tw ➡ webcertificate.pfx	2021/1/21 下午 0. 2021/1/21 下午 0. 2021/1/21 下午 0.	檔案資料夾 檔案資料夾 個人資訊交換		4 KB
-	<	III			>
檔案名稱(N): Serve 存檔類型(T): 個人]	erCert				× ×
▲ 陽藏資料夾			存檔(S)	取消	

## 八、設定好存檔檔名與路徑後按下「下一步」

€ 🦻 憑證匯出精靈	X
要匯出的檔案 請指定您要匯出的檔案名稱	
檔案名稱(F): C:\Users\Administrator\Desktop\Certificate\ServerCert.pfx	
下一步(N)	<b>权</b> 消

九、確認資訊無誤後按下「完成」

🛞 🔗 憑證匯出精靈	
完成憑證匯出精靈	
您已經成功地完成憑證匯出	1.精靈。
您已指定下列設定:	
檔案名稱	C:\Users\Administrator\Desktop\Certificate\ServerCert.pfx
匯出金鑰	是
包含憑證路徑中的所有憑	
<	III >
	完成(F) 取消

### 一〇、 按下「確定」以結束對話框

憑證匯出精靈 🗙	
匯出成功。	
確定	

#### 附錄 A- 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。

#### 附錄 B- 使用網路中文工具對 PFX 進行解離與捆包:

雖然網路中文有提供 CSR 產生工具,但基本上還是建議由主機商或是資訊人員在本機產出 CSR 與 Key 會比較好。如在生成 CSR 的章節有提到,Windows 生成時並不會把 Key 生成給資 訊人員。所以如果透過外部工具生成,還需要再捆包成 PFX 格式才能被 Windows 主機可接受。

但如果你同時擁有 Windows 主機與 Linux 主機的話,難免就會需要轉換憑證,才能將其佈署 在兩種平台機器上。這個章節就教您如何使用網路中文的工具來做憑證轉換。

在網路中文的首頁上,您可以透過以下連結開啟。

網路(史文					
服務/申請/續用▼ 加值服	務▼ SSL憑證▼ 雲端服務▼				
	SSL憑證介紹				
	SSL產品列表				
语年限異動公	立即申請				
	SSL線上工具→				
ogle規定 <mark>SSL</mark> 憑證期限不	找到適合您的SSL				
日停止販售2年期憑證 <b>。</b>	快速生成CSR文件				
	檢測CSR文件是否正確				
	SSL憑證轉檔工具				
	SSL憑證教學文件				

然後就會看到這樣的畫面,將畫面動捲動至下面



# SSL檔案格式轉換器

輕鬆轉換您的檔案格式,符合各種使用需求

如果您取得的檔案格式與主機不符,請使用此功能做格式轉換:

依照下圖格式,選擇現在格式為 PFX,欲轉換成 PEM,並放入 PFX 憑證檔,輸入密碼後就可以進行轉換。

注意:密碼必須輸入正確,否則會轉換失敗。



SSL檔案格式轉換器

輕鬆轉換您的檔案格式,符合各種使用需求

如果您取得的檔案格式與主機不符,請使用此功能做格式轉換:

現在格式: 〇 PEM 〇 DER <mark>⑨ PFX</mark> 〇 P7B
從轉換成: ● PEM ○ DER ○ PFX ○ P7B
<u>馮證權:</u>
選擇檔案 webcertificate.pfx
私鑰(Private Key):
選擇檔案 未選擇任何檔案
根憑證Root CA(非必要):
選擇檔案 未選擇任何檔案
中繼憑證Intermediate CA(非必要):
<b>選擇檔案</b> 未選擇任何檔案
<u>輸入 key 檔密碼:</u>
開始轉換

🚯 I 🕞 🕕 = I	壓縮的資料夾	IĘ	certi	ficates.zip		-	. 🗆 X
檔案 常用 共用	檢視 解壓縮						× 🕐
🔄 🔿 🔹 🕇 🚺 🕨 🕇	\$機 ▶ 下載 ▶ certificate	s.zip		~ ¢	搜尋 certificat	es.zip	Q
☆ 我的最愛	名稱	類型	壓縮大小	受密碼保護	大小	壓縮	修改日期
📜 下載	🔄 Certificate.cer	安全性憑證	2 KB	否	3 KB	29%	2021/2/24上
■ 桌面	PrivateKey.key	KEY 檔案	2 KB	否	2 KB	24%	2021/2/24 上
週 最近的位置							
/團 本機							
📬 網路							
	<		III				>
2 個項目							

如果依照第四章的方式使用 MMC 匯出所有憑證的話,則中繼憑證也會在裡面,只是需要逐一去查看內容才能辨示那些是中繼憑證或根憑證。因為相關憑證將被命名為 Certificate(1)、 Certificate(2)……等等

壓縮的資料夾工具	certificates (1).zi	p 💶 🗖 🗙
檢視 解壓縮		~ <b>(</b> ?
機 ▶ 下載 ▶ certificates (1).zip	~ ¢	搜尋 certificates (1).zip
名稱	類型	<b>壓縮大小 受密碼保護</b> :
🔄 CACertificate1.cer	安全性憑證	2 KB 否
🛱 CACertificate2.cer	安全性憑證	2 KB 否
CACertificate3.cer	安全性憑證	2 KB 否
🔄 Certificate.cer	安全性憑證	2 KB 否
PrivateKey.key	KEY 檔案	2 KB 否
	区線的資料夾工具     検視 解壓缩     解壓缩     常    「     常    和      和	屋貓的資料夾工具     certificates (1).zi       檢視     解壓縮       業 • 下載 • certificates (1).zip     v C       名稱     類型       〇 CACertificate1.cer     安全性憑證       〇 CACertificate2.cer     安全性憑證       〇 CACertificate3.cer     安全性憑證       〇 CACertificate3.cer     安全性憑證       〇 CACertificate3.cer     安全性憑證       〇 PrivateKey.key     KEY 檔案

轉換完憑證後,就會將憑證下載,此時再把他解壓縮即可得到憑證。

#### 將 PEM 格式轉換成 PFX

將您的私密金鑰及取得的憑證依照下面的圖示放置憑證檔案與私密金鑰,並設定密碼,中繼 憑證與根憑證不是必要檔案。但如果您有需要的話,也可以一併放入。

檔案副檔名建議為:.txt/.key/.crt/.cer



# SSL檔案格式轉換器

輕鬆轉換您的檔案格式,符合各種使用需求

如果您取得的檔案格式與主機不符,請使用此功能做格式轉換:

● PEM ODER OPFX OP7B
欲轉換成: ○ PEM ○ DER ● PFX ○ P7B
憑證檔: 選擇檔案 Certificate.cer
私鑰(Private Key):
選擇檔案 PrivateKey.key
根憑證Root CA(非必要):
選擇檔案 未選擇任何檔案
中繼憑證Intermediate CA(非必要):
選擇檔案 未選擇任何檔案
輸入 key 檔密碼:
開始轉換

如果在您的轉換上失敗的話,請先用記事本開啟相關檔案。檢查是不是憑證/金鑰文件檔案的內容有空格,如果有的話,請先使用 Backspace 將其空格字元取消後存檔再行轉換。

----BEGIN PRIVATE KEY-----MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDv0D0sTSaBF9zZ oOSOhaKuQxLCpGOnRvsmE5yz799vci1xNmdkaZOeEgk8df48wbiO5tY6HU5ZcqSv sKuSMbW4ic0DsGQMrF0fMvGs+CJuQ4O9n+ojOG70m1/Gih7AhYfKCOPRWIipNZeA 8t7At+36bfnBrYV61chy0ngPutu3L0InN/HJsqkRZ0fqeCTkWn9e76omGb05BrU6 vxhovv456x1qIkou8/oF/LvRzvLC5wdO5NAuCPweMzaS692qyXt0FIfxoFctIiXj s6M11RAK6/I3g20p+YC2IR2zFDMFNQL17I3q5S01YwYZX0FRsW2GcHufs000nwsq 51yiKW1rAgMBAAECggEBAOyecz17Ajrt6KNy9TaJhPKci64xtYIfrz7qqvt/+t5j siK6o1mYMmcNNL/LTId2PTwC1+2PbPck/wm7MA6Xrc3facHyEUXP7DIUehFI4/AX /azkVI1b7Tk9aLL1JWKgX1MiYmb1DCKpFkvNV6yfztgCGyTWgZVCpP1mXcBnhtM+ jPq0Kifo3rdX39kZAj51K1H15wBAx/uC+00N3hn5E/Kc3GkaTdLd7Ubkg1wubv/e w0K+iiQ4Zhe0JH/vouKaJy46xnAT/v0Rz0RORS+NLJ9HVQMyH4NL0U1NJaqTNoiS qJHpg004kRmUAKBGkNUE3GfWtXa7Nzu5Jadtw64mzcECgYEA9+LhC4j0xAAfsOOt bdJmQcHc5oXwg7CbwPHHX1qBGpEbisxySmL/yTn/kmbB3d3MqUvjwOdwBs22WGWS 016k0JvnwvUDTRWr685jy8ht0sSpatL/kFgD86r7EXN/rTcaJEuP4Soc7oZig8xX o+P4SMtFnPXHZJL5jqxG9zc/5j0CgYEA96m3EPYkxNtW7B1GzmoQ9ryFqgrc2802 UjptEBNoTjgWzjrIY/PwpJGENCbsOcyAz9UzPVCosJZIXyicxzHuWAWtz97VKjPF 3QIpEc5moQWSOpRXmfkz5Mzzve0Smieio+3vQt1P7nvjz103MmWPpfaga9VUv7jd o18Qe4I+hMcCgYEA4U1XUo50NbYPF1NXWFpCCT1RsEjGoEjgJWkXOs7aSvTaXTkW Hjj/Uzjc54dwZ13wZWTNZ0Jv9B79vDUETSErFVS8091F2Mb7auI2nLxZ45ZMiwOc t0jpHomkiOW5gg10PsxVxUPq63VDD5m1hRPpU089IzvUrb10CbbVAFU8Q9kCgYBi m9JmEHtHXkXXsTh2C01B1IIr2DNj2OteBiFSm0eWjUKXT1RnZ8NS4xW0Zkj8Im7P UYYbTbg8xz19mgACV+EcbvZro7+gFAkeHDQaAOJgDoXQiSvwBIci/G+4GWKkuk9J kf0H0ta+i9mCV1bD3Cg73mCwmroptA0bGNrJMmyOFQKBgDXsOt/6vnCcQvxUgrOv TMLnNACHMoX56jEL+50cVME1ga2qru61QxZ07ijon5KYHN0r0joLRBARv0J3t12z i/65aZw10FtX9RNt6bpXpet0XAIwK5/xZSh51RP1axXnN0ycv80cWzAfm3T1a0tA Igd3ZV9kOvIHUDodoGu9Dscy -----END PRIVATE KEY-----

以上圖為例,在-----BEGIN PRIVATE KEY-----本文前面有一個空格,這個空格會導致轉換失敗。而-----END PRIVATE KEY----則沒有空格,這樣的錯誤會導致轉換失敗,請特別注意。

#### 附錄 C- 使用 OEPNSSL 工具進行 PFX 憑證格式的轉換:

在 OpenSSL 環境下,輸入以下的指令列以將 PFX 轉換成 PEM

- A. 匯出檔案 (含 Key、CA 中繼憑證、CRT 憑證) openssl pkcs12 -in < 檔案名稱 .pfx> -out < 自訂名稱 .pem> -nodes -password pass:< 自 訂密碼 >
  - 1. 用記事本打開 pem 檔案
  - 2. 分別用記事本存成網站憑證、中繼憑證、KEY
- B. 匯出檔案 (只有 CRT 憑證與 CA 中繼憑證)【多了 -nokeys 參數】 openssl pkcs12 -in < 檔案名稱 .pfx> -nokeys -out < 自訂名稱 .crt> -nodes -password pass:< 自訂密碼 >
- C. 匯出檔案 (只取 Key 檔) 【多了 -nocerts 參數】 openssl pkcs12 -in < 檔案名稱 .pfx> -nocerts -out < 自訂名稱 .key> -nodes -password pass:< 自訂密碼 >

下圖為執行過程,如果覺得 PEM 不好開啟,可以輸出為.txt 檔案 (本範例使用 Mac OSX 終端機搭配 OpenSSL Command Line 指令列執行上面的類型 A 指令)

```
OpenSSL> exit
[changchiaofu@zhangqiofudeMBP ~ % clear
[changchiaofu@zhangqiofudeMBP ~ % openssl
OpenSSL> pkcs12 -in ServerCert.pfx -out cert.pem -nodes -password pass:70535344
MAC verified OK
OpenSSL>
```

經輸入指印後,會產出下面的結果,再使用文字工具將---BEGIN.....----字段的內容復製,憑 證及金鑰都會在該檔案裡面,請逐個複製。

```
Bag Attributes
       Microsoft Local Key set: <No Values>
       localKeyID: 01 00 00 00
friendlyName: {A614F1A3-8CA8-4808-89EB-0E6D19222406}
Microsoft CSP Name: Microsoft RSA <u>SChannel</u> Cryptographic Provider
Key Attributes
      X509v3 Key Usage: 10
--BEGIN PRIVATE KEY---
MIIExwIBADANBakahki69w0BAQEFAASCBKkwaaSlAqEAAoIBAQClsZk3w1ZSLt4d
P/yE5BlRDEbEYX15cOpU09iAkCMcpdqCzYirkmy/uSR5r6E+xbrLyjHUwpRoE3MD
oFUIbJoAidiGCCo4IE6zTOKlYXVg38vrQKMJCNo9L98jZMPvACjQxic9dywtlBiH
iuYDNlgs+Gpvp8pAuoyik9gLJ9Ncw8++eEH7UiEKMcig5z5pY8ZZIRgLVk7+UyNn
4mh9FpuPln2HKhlzJVRJkZ6pVblVEKoik9MiV3Z9n4HEZKpBTu8KIKCk9OUR+EIu
AC1GasR64ZYGB2SB+eZIp++6M0e90nhaCEBt8aWrU75ZdiUYvgtAOoNU2hFi2KkG
qtSZflgPAgMBAAECggEADhOnjVBAHioZkelkrcm/L0Tx7vv+A++iFaPvLageA4oN
1WpTlfGSBIWP+4wxginJGkhd5J7fVg3VwKId3a7BHd7+kTlSW1BYJbpLd+EIXg5f
AgTMyEpQC2pTJ8IHNcZESwn6o9zJcgamHgw6IGTWJ7cdiJZ8HVtIvxgJYtejiLoX
gh5PNlZf6AjuU5fN0l1yIa+wBcX79z47h01W6zPoL9N4p/aCLir33AigwA/729EM
@codIyMH1gjilmuqXcCCL14fH1ZN24vvoCTdN1p8GHbyR5ilKJjkf5NeiyJg8o0l
QPL2EX51wjaxa4KaUD0JBh5Jrk5eojriX10uQ9uLmQKBgQDiqEX0HszY34oWUMtz
eT7mmKTfytM2tLDyaB6BpqlgTS3u9gctMWGnlCd5HzywHyNgSNimHhT566Rp0pg
NHqU7sYKig0huT0FNvfzGNDL85TZDq5Jh7Kv7xoDY4EkMa4qctIFC/ulDket106c
1R93mc3DDsNGYdjYFMqc7iwqAwKBgQC7J0ku0ICe0GLgoEoZ+hcjR9xcHB90E2ZZ
7+UBqppC00fhIa3T4izzId2baM9KEfUWf72292KUbJ20czDRx0WkkgUW6DLm0lFo
ElLCsB78He2z2ezYmd568KDCgtbiNbPHeP8fAuR2trgeuXVskGpV08TZAh790cjA
hT1XycSCB0KBgQC6TrNhnMepJ0Yuva7edjU+c4T9dLS08dH5WYztg0wxSul4dZGI
lxbeNtfxUVVbfNlk2aVgcAXIgke0oEJEnh58uWBUXXG53K/6ulpJmoZWfxxE5wpg
Koi4kQOC8ZG/nI6axFYqC9WHsRs+Sjk+tPiuq0A3i7T774X85+o74JKw3QKBqQCh
VHuU+Pe37iIHRQc8h6VEq+Fione2RfEZHT6Nhig024TaRr9khnl7i7lQDTWNxBdF
sw+oWHFqWTy+Hb17SMM2cRHkIn4nECSPi0DwRwYfD+nn/rk4LLz//wqHRGXckrE0
B9ffMw4i7PeivPxmf8S6/5B+B18Rq6vNk89DC9RUxQKBq0DKJWWHALs7ZIDCmKjw
iHCndcUGauojhsTMMgvHB7aDn7lT6u6d0ZdvQaL+qgwNptzJc+shd9exWarNeWfF
d5o2pWtezVjVk+N0W9bRxo3IrVF2H0T+keGNbxsDfuJs24FviNbFa0SlpaNu/fam
s9zh/K7gDQM3czws1j3vKZ5BmA=
----END PRIVATE KEY-----
Bag Attributes
       1.3.6.1.4.1.311.17.3.75: 00 00
       localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.3.20: F8 26 BA 26 71 56 92 69 2A 65 2B A9 A6 91 11 78 EC 41 19 2A
       friendlyName: ssl.net-chinese.tw
subject=/CN=ssl.net-chinese.tw
issuer=/C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain
Validation Secure Server CA
-----BEGIN CERTIFICATE-----
```

上圖的輸出結果,在 Linux 的指令列也可以使用。 Windows 版本要使用 OPEN SSL 的話,由於 OpenSSL 官方並沒有提供 Windows 版本的安裝包,可以選擇其他開源平臺提供的工具。例如:<u>https://slproweb.com/products/Win32OpenSSL.html</u>

#### 使用 OEPNSSL 工具將 PEM 格式轉換成 PFX

- 1. 準備好憑證與 KEY(.crt 與 .key) 在工作路徑之下
- 進行合併,輸入指令碼如下
  openssl pkcs12 -export -in < 憑證絕對路徑 \ 憑證檔案 > -inkey < 私鑰絕對路徑 \ 私鑰
  檔案 > -out < 自訂名稱 .pfx> -certfile < 中繼與根憑證絕對路徑 \ 中繼憑證或根憑證 >
  -password pass:< 自定密碼 > ( 若在 openssl 環境下可以不打 openssl 敘述句 )

參數說明:

- pkcs12 -export:將憑證匯出成 pkcs12 編碼格式的 PFX 憑證檔
- -in < 憑證檔案 >: 將網站憑證放入
- -inkey < 私鑰檔案 >: 將金鑰憑證放入
- -out < 自訂名稱 .pfx>: 轉換後產出的 pfx 名稱
- -certfile < 中繼與根憑證 >: 合併入中繼憑證 (若不加可省略)
- -password pass:< 自定密碼>:為設定匯入之密碼, Windows IIS 通常會要求。(若不加可 省略)

下圖為執行過程,如果覺得 PEM 不好開啟,可以輸出為.txt 檔案 (本範例使用 Mac OSX 終端機搭配 OpenSSL Command Line 指令列執行上面的類型 A 指令)

```
changchiaofu@zhangqiofudeMBP ~ % openssl
OpenSSL> pkcs12 -export -in ssl_net-chinese_tw.crt -inkey PrivateKey.key -out IIS
Cert.pfx -certfile My_CA_Bundle.crt -password pass:70535344
OpenSSL>
```

如果您的 Windows 有安裝開源平台的 OpenSSL for Windows 的話,則請用命令提示字元完成上述的工作就可以轉換。

💽 系統管理員: 命令提;	示字元	
C:\>cd\sslwork C:\sslwork>opens lwork\ssl.keyo assword_pass:705	ssl pkcs12 -export -nodes -in C:\sslwork\webcert.crt - out C:\sslwork\win_webcert.pfx -certfile webcert_ca_bu 35344	inkey <mark>C:\ss</mark> ndle.crt -p
C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork> C:\sslwork>	-in 網站憑證 -inkey 網站私論 -out pfx格式憑證 -certifile 中繼憑證 -password pass:密碼	Ŧ