政府伺服器數位憑證管理中心(GTLSCA)

Windows IIS 8.0 SSL 憑證請求檔製作與憑證安裝手冊

聲明:本手冊之智慧財產權為中華電信股份有限公司(以下簡稱本公司)所有, 本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享 供申請 SSL 伺服軟體憑證用戶參考,若因參考本手冊所敘述的程序而引起的任 何損害,本公司不負任何損害賠償責任。

目錄

Windows IIS 8.0 SSL 憑證請求檔製作手冊	2
Windows IIS 8.0 SSL 憑證安裝操作手冊	6
附件一:停用 SSLv2、SSLv3	19

Windows IIS 8.0 SSL 憑證請求檔製作手冊

V }	Internet Information Servid s (IIS) 管理員	
€ SIN-8IHG1LIL8	3C6 🕨	🕶 🖂 🟠 🔞 🕶
檔案(F) 檢視(V) 說明(H)		
建编 《●・ ● ● ② 起始網頁 《●・ ● ◎ 記始網頁 《●● WIN-8H611LBC6 (WIN-8H ● ◎ 開程式集區 》 ● ◎ 始台 》 《 ● ● ◎ 始台 》 》 》 》 书台 》 》 ● ● ◎ 第一日 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	WIN-8IHG1LIL8C6 首頁 時選誌 第8至(G) B S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S S </th <th>動作 管理伺服器 2 重新設動 > 設動 ● 停止 検視使用程式集區 検視送台 ● 取得新的網頁平台元件 ● 説明 線上説明</th>	動作 管理伺服器 2 重新設動 > 設動 ● 停止 検視使用程式集區 検視送台 ● 取得新的網頁平台元件 ● 説明 線上説明
就緒		Sec. 1

一、 開啟「Internet Information Services (IIS)管理員」

二、 點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站), 再點選畫面 右邊「伺服器憑證」兩下。

Internet Information Servid、s (IIS) 管理員	_ 0 ×
€ WIN-8HG1LL8C6 >	🔛 🖂 🟠 🕡 -
檔案(F) 檢視(V) 說明(H)	
1 1<	數件 普理伺服器 ② 重新設動 欲勁 ● 停止 検視應用程式集區 検視活台 ③ ● 取得新的網頁平台元件 ● 説明 規計説明
就编	•

三、 點選「建立憑證要求」

() () <t< th=""><th>B</th><th>Inte</th><th>ernet Information Services</th><th>(IIS) 管理員</th><th></th><th>_ 0 ×</th></t<>	B	Inte	ernet Information Services	(IIS) 管理員		_ 0 ×
 ● 編視 ● 設場() ● 副目の 器源 語 ● 副目の 器源 語 ● 副目の 需要 菜及 智慧病育 回知 器 可用計 對 SL 設定的現法 指配使用的 語。 ● 副目示 要求及智慧病育 回知 器 可用 ● 第 空 () ● 全部展示()) 部組 法 沒有分組 ● ● 副目示 要求及智慧病育 ● 第 行為 ● 副子() ● 目の 需要 書。 ● 副目示 要求及智慧病育 ● 第 行為 ● 副子() ● 目の 需要 書。 ● 副目示 要求及智慧病育 ● 第 行為 ● 副目示 要求及智慧病育 回知 ● 第 定用 ● ● 目示 要求 和 ● ● ■ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	WIN-8IHG1LIL8	C6 🕨				😐 🖂 🕜 -
建設 ● (1)	檔案(E) 檢視(V) 說明(H)					
Image: Name (Amplitude) Name (Amplitude)	連線 ● ・ ● ● ● ● ● ● ● E 姓始銀頁 ▲ ● WIN-8HrG1LIBC6 (WIN-8Hr ● ● ● B 印程式集區 ▲ ● ● Default Web Site	● 印服器憑證 此功能可用來要求及管理網頁伺 時選器: ● 名稱	服器可與針對 SSL 設定的網站描記 ▼ 移至(G) ~ (金) 全部顯示(A) 酸行給	使用的憑證。 聲組依據: 沒有分組 。 發行者	到期日	數作 僅入 建立德國要求 完成急醒要求 建立信载委署憑證 建立自我签署憑證 ② 說明 線上說明
W		■ 切能做优 ₩ 内容做視				A =1
	玩着					V

四、 輸入以下所有欄位資料,輸入完成後請點選「下一步」,多網域憑證申 請填一個代表網站名稱即可,實際憑證核發資料是以申請書填寫為主。

	要求憑證	? X
分辨名稱屬性		
指定憑證的必要資訊・省份及縣	市/位置必須指定成正式名稱,而且不能包含編寫。	
一般名稱(M):	www.test.com.tw	
組織(O):	中華電信股份有限公司數據分公司	
組織單位(U):	政府網路處	
縣市/位置(L)		
省份(S):	none	
國家 (地區)(R):	TW v	
	上一步(P) 下一步(N) 完成(F) 即	调

五、 選擇密碼編譯服務提供者『Microsoft RSA SChannel Cryptographic Provider』,金鑰長度選擇 『2048』位元。

要求憑證	?	x
密碼編譯服務提供者內容		
選取容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,安全性認 越高。不過,位元長度較大可能會降低效能。 密碼編譯服務提供者(S): Microsoft RSA SChannel Cryptographic Provider ▼ 位元長度(B): 2048	£	
上一步(P) (下一步(N) 完成(F)	取消	

六、 指定儲存憑證請求檔的檔案名稱與存放位置,確認後請點選「完成」。

要求憑證	?	x
▲案名稱		
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:\certreq.txt		
上一步(P) 下一步(N) 完成(F)	取消	

七、此時憑證請求檔(certreq.txt)製作完成,使用憑證請求檔至憑證管理中心 (https://gca.nat.gov.tw)申請 SSL 憑證。

Windows IIS 8.0 SSL 憑證安裝操作手冊



一、開啟「Internet Information Services (IIS)管理員」。

二、點選主機連線預設名稱,再點選畫面右邊「伺服器憑證」。

「 Internet Information Servi な s (IIS) 管理員	_ 0 ×
S S SINGLILL&C6 →	- O 🗟 🖾 🔁
檔案(F) 檢視(V) 說明(H)	
	動作 管理伺服器 ② 重新数動 ● 旋動 ● 停止 位視應用程式集區 検視站台 ● 取得新的網頁平台元件 ② 説明 總上說明
	•=

三、點選「完成憑證要求」。

● WIN-8H4G1LLEG ● ● WIN-8H4G1LLEG ● 事業(D) 結構(D) 影明(D) ● ● <th>6]</th> <th>Internet I</th> <th>nformation Services (IIS) 管理員</th> <th></th> <th>_ 0 ×</th>	6]	Internet I	nformation Services (IIS) 管理員		_ 0 ×
 第集(① 触視① 説明(①) 第集(② 使用 (○) (N)-8h ● ① Bright (○) (N)-8h ● ② Default Web Site ● ② Default Web Site ● ② Default Web Site ● ③ Default Web Site ● ○ Default Web Site ● ○ Default Web Site ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	€ WIN-8IHG1LIL8	3C6 •			🎂 🖂 🏠 🕡 🕶
	檔案(E) 檢視(⊻) 說明(H)				
就繪	連接 ● ● <	・ ●	#針野 SSL 設定的網站描配使用的憑證。 (① ~ 🔂 全部顯示(Δ) ■ 野組依據: 沒有分組 會	動作 通过高程要 受)期日 通过回我猛烈 建立自我猛烈 建立目我猛烈 後日	菜 薹 薹
	就緒				e =

四、如下圖,選擇至憑證管理中心申請之 SSL 憑證,並輸入好記的名稱(一般填寫 Domain Name)。

完成憑證要求	?	x
指定憑證授權單位回應		
藉由擷取包含憑證授權單位回應的檔案,完成先前建立的憑證要求。 含有憑證授權單位回應的檔案名稱(R): [C:\Users\Administrator\Desktop\certreq.cer		
好記的名稱(V): www.test.com.tw 選取新憑證的憑證儲存區(S):		
個人 ~		
確定	取消	

五、步驟4按「確定」,出現完成憑證要求的畫面。

9	Internet Information Services (IIS) 管理員	_ D X
WIN-8IHG1LIL8	C6 •	🖸 🛛 🟠 🕡 🗸
檔案(E) 檢視(⊻) 說明(H)		
連線 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	 ● 服器憑證 此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。 ● ● 移至(G) ● ● ● ● ● ● 移至(G) ● ● ● ● ● ● ● ● ● ●	 動作 僅入 建立憑證要求 完成憑證要求 建立網域憑證 建立自我簽署憑證 檢視 度出 更新 ※ 移除 ② 說明 線上說明
< III >	🛅 功能檢視 🚰 內容檢視	
就緒		9 .:

- 六、至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案,下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip
- 七、將 GTLSCA_All.zip 解壓縮,可以得到 ROOTeCA_64.crt、

eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案。

八、接著要安裝 eCA 自發憑證及 GTLSCA 憑證。

請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。

Ĩ		이렇게 잘 물려 물려 물건을 받았다. 영영 가격 등 전에 모르는 것을 가지?		
	$\mathbf{\Sigma}$	系統管理員: Windows PowerShell	_ D X	
資源	Windows Power	·Shell著作權(C)2012 Microsoft Corporation. 著作權所有,並保留一切權利。	^	
	PS C:\Users\A PS C:\Users\A	Administratory mmc		
		· · · · · · · · · · · · · · · · · · ·	_ D X	
c		🜇 檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)	_ & ×	
F		主控台根目錄 名稱	動作	
L		這個檢視沒有項目可顯示。	主控台根目錄 ▲	
my			其他動作 ▶	
F				
L				
G				
	微軟新注音 半			
			Windows Server	2012 Standard
			• 18 Vii (b)	2013/7/11

九、選擇「新增/移除嵌入式管理單元」。

					主控台1	- [主控台根目錄]			x
	檔案(F) 動作(A) 3	檢視(V)	我的最愛(O)	視窗(W) 說	明(H)		-	5 ×
4		開新檔案(N)			Ctrl+N				
		開啟(O)			Ctrl+O		ŧ	助作	
	1	儲存(S)			Ctrl+S	沒有項目可顯示。	3	主控台根目錄	
		另存新福(A)				_		其他動作	÷
	\leq	新增/移除嵌入式	は管理単分	⊤(M)	Ctrl+M	>			
		選塤(P)				-			
	_	1 C:\Windows\s	system32	2\compmgmt					
	1	結束(X)							
開戶	如一個現	見存的主控台。							

十、接著點選「憑證」→「新增」。

			新增或移除崔	成入式管理單元		x
您可以為這個主控台從您的電 入式管理單元,您可以設定啟	腦上可以使用的嵌入 用哪些延伸。	式管	き理単元中選擇―	些嵌入式管理單元,	並且設定所選擇的嵌。	入式管理單元。對於可延伸的嵌
可用的嵌入式管理單元(S):				選取的嵌入式管理單	元(E):	
嵌入式管理單元	廠商	^		📔 主控台根目錄		編輯延伸(X)
🔐 具有進階安全性的 Win	Microsoft Corp					
🔍 服務	Microsoft Corp					移除(R)
🧾 原則結果組	Microsoft Corp					
🔕 效能監視器	Microsoft Corp					⊢終(U)
🛺 授權管理員	Microsoft Corp					1.12(0)
🧾 群組原則物件編輯器	Microsoft Corp		$ \longrightarrow $			下移(D)
🛁 裝置管理員	Microsoft Corp	0	新増(A) >	D		
📫 資料夾	Microsoft Corp					
🧕 路由及遠端存取	Microsoft Corp					
🌆 電腦管理	Microsoft Corp					
🖓 電話語音	Microsoft Corp	≡				
📄 磁碟管理	Microsoft 舆 V					
12 網址連結	Microsoft Corp					
(🗊 憑證)	Microsoft Corp	$\overline{}$				進階(V)
描述:						
憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放區內容。 						
						確定 取消

選擇「電腦帳戶」→「下一步」→「完成」。

憑證嵌入式管理單元	x
這個嵌入式管理單元將自動管理下列帳戶的憑證: ○ 我的使用者帳戶(M) ● <u>服發帳</u> 戶(S) ● 電腦帳戶(C)	
<上一步(B) 下一步(N) > 取消	

選取電腦	x
請選取您要此嵌入式管理單元管理的電腦。 □ 這個嵌入式管理單元將一直管理: ● 本機電腦 (執行這個主控台的電腦)(L):	
○ 另一台電腦(A): 瀏覽(R)	
□ 當電腦從命令列啟動時,可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)	
< 上一步(B) 完成 取]消

最後按下「確定」。

1 用时		_	選取的嵌入式管理单元(E):	
嵌入式管理單元	廠商	^	1 主控台根目錄	編輯延伸(X)
	Microsoft Corp		→ 憑證 (本機電腦)	2454 m
🔍 服務	Microsoft Corp			移除(R)
J 原則結果組	Microsoft Corp			
∑ 效能監視器	Microsoft Corp			上移(U)
20 授權管理員	Microsoft Corp			13(0)
JJ 群組原則物件編輯器	Microsoft Corp			下移(D)
🚔 裝置管理員	Microsoft Corp		新増(A) >	
🎬 資料夾	Microsoft Corp			
😐 路由及遠端存取	Microsoft Corp			
🖣 電腦管理	Microsoft Corp			
😵 電話語音	Microsoft Corp	=		
🚽 磁碟管理	Microsoft 與 V			
🖭 網址連結	Microsoft Corp			
₽ 憑證	Microsoft Corp	~		進階(V)
i述: 愚證嵌入式管理單元讓您瀏覽	記電腦或服務的憑證存	₮放	內容 •	

十一、匯入 eCA 自發憑證。在「中繼憑證授權單位」下的「憑證」按下右鍵, 選擇「所有工作」→「匯入」。

-	主控台1 - [主控台根目錄\憑證	(本機電腦)\中繼憑證授權單位'	∖憑證]	_ D X		
🚟 檔案(F) 動作(A) 檢	读視(V) 我的最愛(O) 視窗(W) 說明	(H)		_ F ×		
🗢 🄿 🖄 📰 📋	Q 📄 🛛 🖬					
■ 主控台根目錄	發給 ▲	簽發者	到期E	動作		
⊿ 🖓 ∞證 (本候电脑) ▶ 🦀 個人	Microsoft Windows Hardware	Microsoft Koot Authority	2002/	憑證 ▲		
⊿ 📔 受信任的根憑證	www.verisign.com/CPS Incorp	Class 3 Public Primary Certificati	2040/	其他動作 ▶		
● 憑證		,	(
▶ 🔜 企業信仕 ⊿ 📫 中繼馮諙授權單						
□□□ □□ 湿泡油加度温=	<u> </u>					
6 元 所	· 有工作(K) ▶ 匯入	(I)				
▶ ■ 党信任 ▲	視(∨) ▶					
▶ 🔛 第三方 🏻 從	這裡開啟新視窗(W)					
	工作台檢視(T)					
▶ □ 用尸螨						
▶ 🔛 智慧卡 🛛 🕅	出清單(L)					
▶ 🛗 信任的 🔡	(田(円)					
D Veb H	() () () ()					
< III >	<		>			
包含可以在這個項目上執行的動作。						

依照下列步驟匯入自發憑證。

◎ 參 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 ○ 目前使用者(C) ● 本機電腦(L) 	
請按 [下一步] 繼續。	
耳 (N)进一	以消

	X
중 ₩ 38 ● ● 湯證匯入精靈	
要匯入的檔案 指定您想要匯入的檔案。	
 檔客名稿(F): E:\eCA1_to_eCA2-New.crt 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) 	瀏覽(R)
④ 承 馮諮匯 λ 捨露	下一步(N) 取消 ×
憑證存放區 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) 第85方連時執入以下於方於原(D) 	
● 將所有您證及入以下的存放區(P) 憑證存放區: 中編憑證授權單位	瀏覽(R)

중 🦻 憑證匯入精靈	×
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 中繼憑證授權單位	
内容 憑證 描字名紙 Ebec A1 to aCA2 Navy set	
TII 完全時 E.\eCAT_t0_eCA2-New.crt	
	元成(F) 取消

十二、匯入GTLSCA憑證。在「中繼憑證授權單位」下的「憑證」按下右鍵, 選擇「所有工作」→「匯入」。

≧ 主控台1 - [主控台根目錄\憑證 (本機電腦)\中繼憑證授權單位\	憑證]	_ D X
🚟 檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)		_ 8 ×
☐ 主控台根目錄 發給 ▲ 簽發者	到期E	動作
▲ 🖗 憑證 (本機電腦) 🔤 Microsoft Windows Hardware Microsoft Root Authority	2002/	憑證 ▲
▶ 🧧 個人 🔤 Root Agency Root Agency	2040/	其他動作 ▶
4 - 文庫正知知惑題: A www.verisign.com/CPS Incorp Class 3 Public Primary Certificati	2016/	C C Notation 11
▶ <mark>□</mark> 企業信任		
⊿ 🦀 中繼憑證授權單/		
🤗 憑證撤銷清耳		
● 所有工作(K) → 匯入(D		
▶ <u>夏</u> 信田 ▶ [●] 沒有信 檢視(V) ▶		
▶ 📫 第三方 從這裡閩啟新視廠(W)		
▶ <u>●</u> 憑證鈕 重新整理(F)		
▶ G Web H 說明(H)		
	>	
包含可以在這個項目上執行的動作。		

×
要 匯入的檔案 指定您想要匯入的檔案。
相多名稱(D) E:\GTLSCA.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 (.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)
下一步(N) 取消

成功匯入後,可以看到 GTLSCA 的憑證。

-	主控台1 - [主控台根目錄\憑證	(本機電腦)\中繼憑證授權單位	\憑證]	_	D X	
□ 檔案(P) 動作(A) 檢視(V) 我的最愛(Q) 視窗(W) 說明(H)						
🗢 🄿 🖄 🖬 📋	ù 📾 🛛 🔽 🗖					
■ 主控台根目錄	發給	簽發者	到期E	動作		
⊿ 🙀 惣誼 (平傍竜脑) ▷ 🦳 個人	Ender PKI Root Certification Author	ePKI Root Certification Authority	2034/	憑證	-	
▶ 🧾 受信任的根憑證:	Root Agency	Root Agency	2040/	其他動作	•	
▶ 🔛 企業信任	www.verisign.com/CPS Incorp	Class 3 Public Primary Certificati	2016/			
▲ 一 千遍忽臣过催年	広 政府伺服器數位憑證管理中心	ePKI Root Certification Authorit	2031/			
▶ 🔜 受信性的毁打者 ▶ 🎬 沒有信任的憑證						
▶ 📔 第三方根憑證授;						
▷						
▷ 🛄 遠端桌面						
▶ 🚆 智慧卡信任根目:						
▷ 🔲 间江时装直 ▷ 🚆 Web Hosting						
Windows Live II						
< III >	< III		>			
中編憑證授權單位 存放區包含 5 個憑證。						

十三、匯入 eCA 根憑證。在「受信任的根憑證授權單位」下的「憑證」按下右 鍵,選擇「所有工作」→「匯入」。



成功匯入後,可以看到 eCA 的根憑證。

▲ @ 憑證 (本機電腦) ▶ @ 個人 ▲ @ 受信任的根憑語: ◎ @ 微題 ▶ @ 企業信任 ▶ @ 中權憑證授權單 ▶ @ 受信任的發行書 ▶ @ 愛信任的發行者 ▶ @ 愛信任的發行者 ▶ @ 完信任的發行者 ▶ @ 完信任的表語 ▶ @ 完信任的表語 ▶ @ 完信任的表語 ▶ @ 完信任的表語 ▶ @ 完自任的人 ▶ @ 不戶端驗證登發音 ▶ @ 深證註冊要求 ▶ @ 深證註冊要求 ▶ @ Web Hosting	福寨(F) 動作(A) 檢視 ● ● ● ● ● ● ● ●	空台1 - [主控台根目錄\憑證 (本 見(V) 我的最愛(O) 視窗(W) 說明 🗙 🗐 🍛 🛛 ந 發給	機電腦)/受信任的根憑證授權員 (H) 簽發者	單位\憑 到期E	證] _ □ ×
 ▲ 企業信任 ▲ 企業信任 ▲ 中継憑證授權單 ▲ 受信任的發行者 ▲ 資有信任的憑證 ▲ 童子君憑證授 ▲ 童子君憑證授 ▲ 一 新三方君憑證授 ▲ 一 新三方君憑證 A Labert Certificate Aut ▲ Microsoft Root Certificate Aut ▲ No LIABILITY ACCEPTED, (c)97 ▲ No LiABILITY ACCEPTED, (c)97 ▲ Microsoft Root Certificate Aut ▲ Microsoft Root Certificate Aut ▲ Not	 ▲ □ 憑證 (本機電腦) ▶ □ 個人 ▲ □ 受信任的根憑證: □ 憑證 	Class 3 Public Primary Certific Class 3 Public Primary Certific Converget (e) 1007 Microsoft Provense Certification Author	Class 3 Public Primary Certificati Class 3 Public Primary Certificati Copyright (c) 1997 Microsoft C PKI Root Certification Authority	2028/ 2004/ 1999/ 2034/	憑證 ▲ 其他動作 ▶
	 ▶ ○ 企業信任 ▶ ○ 中緯憑證授權 ▶ ○ 受信任的發行者 ▶ ○ 没有三方根憑證授 ▶ ○ 第 第信任的人 ▶ ○ 第 第信任的人 ▶ ○ 第 用戶端驗證簽發 ▶ ○ 第 智慧卡信任根目: ▶ ○ 第 留慧卡信任根目: ▶ ○ 第 Web Hosting 	Microsoft Authenticode(tm) R Microsoft Root Authority Microsoft Root Certificate Aut Microsoft Root Certificate Aut Microsoft Root Certificate Aut ROO LIABILITY ACCEPTED, (c)9 ROOTCA/4096 Thawte Timestamping CA	Microsoft Authenticode(tm) Ro Microsoft Root Authority Microsoft Root Certificate Auth Microsoft Root Certificate Auth NO LIABILITY ACCEPTED, (c)97 ROOTCA/4096 Thawte Timestamping CA	2000/ 2020/ 2021/ 2035/ 2036/ 2004/ 2033/ 2021/	其他動作 →

- 十四、檢查「受信任的根憑證授權單位」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31), 若有請刪除。
- 十五、點選要安裝的站台,本手冊以(Default Web Site)進行說明,選擇「繫結」
 →新增→類型『https』、連接埠 『443』,選擇要安裝在此站台之 SSL 憑證 (www.test.com.tw)。



			站台	鬤結		? 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)
						移除(R)
						瀏覽(B)
						關閉(C)

	新增站台繫結	? X
類型(T): IP 位址(I): https ✓ 全部未指派 主機名稱(H):	連接埠(O): ✓ 443	
□ 需要伺服器名稱指示(N) SSL 馮證(F):		
www.test.com.tw	✓ 選取(L) 確定	檢視(V) 取消

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

附件一:停用 SSLv2、SSLv3

一、 經測試,IIS8 SSL2.0 預設是關閉的,若您的 SSL2.0 是開啟的,您可以 依照以下關閉 SSL 3.0 的作法來關閉 SSL2.0。

二、 開啟登錄檔編輯程式,依照以下路徑找到 Protocols。

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProvider s\SCHANNEL\Protocols\

在 Protocols 的機碼上,按下右鍵→新增→機碼,然後輸入「SSL 3.0」。





在 SSL3.0 資料夾上按右鍵→新增→機碼,然後輸入「Server」。

三、



四、 接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)
 值,然後輸入「Enabled」,並確認資料欄位值為「0x00000000(0)」,若不
 是,請手動將值改為0。





五、 重新啟動電腦。