政府伺服器數位憑證管理中心(GTLSCA) 金鑰對未改變,僅更換TLS 憑證操作手冊

中華民國 113 年 5 月

目錄

網站伺服器	: IIS	3
網站伺服器	: Apache	19
網站伺服器	: Tomcat	23

網站伺服器: IIS

1. 開啟「Internet Information Services (IIS)管理員」,點選主機連線預設名稱,再 點選畫面右邊「伺服器憑證」。



2. 點選「完成憑證要求」。(請確認原憑證是否已安裝於同一台伺服器裡。)

💐 Internet Information Services (I	IS) 管理員		-	- 🗆	×
← → ● DESKTOP-JUE	DB30K 🕨			🐱 🖂	• 🕥
檔案(E) 檢視(⊻) 說明(H)					
建線 ◎ DESKTOP-JUDB30K (DESK ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	● 印服器憑證 此功能可用來要求及管理網頁伺服器可 證・ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	興針對 SSL 設定的網站搭配使用的憑 至(G) ~ (G) 全部顯示(A)) 。 發行給 renew.test.gov.tw	動作 建立憑證要求 完成憑證要求 建立細ば憑證 建立自我簽署憑! 愈用己更新憑證 2 説明	2	
就緒					• 1 .:

3. 選擇新的 TLS 憑證,並輸入好記的名稱。

完成憑證要求	?	×
指定憑證授權單位回應 [1]		
藉由攝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。		
含有憑證授權単位回應的補業名稱(K):		
C:\Users\t \(new)/308A0D289D/5E9D5t		
好記的名稱()):		
renew.test.gov.tw_new		
響取新馮譜的馮譜儲 左區(S) ·		
	En XH	
7年人上	取洞	

4. 按「確定」,出現完成憑證要求的畫面,多一條新憑證列表。

Internet Information Services (IIS) 管理員		– 🗆 X
← → ● DESKTOP-JU	DB30K 🕨		😰 🖂 🚱 🗸
檔案(E) 檢視(V) 說明(H)			
福案(P) 檢視(M) 說明(H) 連線 ② DESKTOP-JUDB30K (DESK → @ 應用程式集區 > - @ 站台	● 同服器憑證 此功能可用來要求及管理網頁伺服器可 證。	與針對 SSL 設定的網站搭配使用的憑 至(g) ~ 😡 全部顯示(A) 安 發行給 renew.test.gov.tw renew.test.gov.tw	堕入 建立憑證要求 完成憑證要求 建立網城憑證 建立目我簽署憑證 檢視 運出 更新 ※ 移除 愈用已更新憑證的自動重新數結 ② 說明
		>	
< > > 就緒	间 切龍儀視 🚾 内容磁視		• <u>•</u>

5. 點選要安裝的站台,本手冊以(Default Web Site)進行說明,選擇「繫結」。

📬 Internet Information Services (IIS)	管理員					- 0	×
← → WIN-U1LEEOI8L7E → 站台 → Default Web Site →						🕶 🖄	• 100 -
檔案(F) 檢視(V) 說明(H)							
Impact (F) (發信(V) 說明(H) 連續 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Def	fault Wel	b Site 首 • ♥ 移至(SSL 設定 預設文件 愛編	頁 G) → 要求歸選 模組 瀏覽目錄	~ ~	動作 瀏覽 編輯權限 壁鏡線 繁積 圖 基本設定 檢視應用程式 檢視應知錄 管理網站 ② 重新設動 ● 飲動 ● 停止 瀏覽 *80 (http) 進階設定 設定 限制 ② 説明	O O
	🗊 功能檢視 [合容檢視					<i>Q</i> -
玩精							0

6. 選擇已存在的 https 443 連接埠,點選「編輯」。

站台繫結	? ×
類型 主機名稱 連接埠 IP 位址 製結資訊 http 80 * https 443 *	新增(A) 編輯(E) 移除(R)
	瀏覽(<u>B</u>)
	關閉(<u>C</u>)

7. 1	重新選擇	要安裝	在此站台	分新的	TLS 憑證。	(其餘設定を	皆不需變動)
------	------	-----	------	-----	---------	--------	--------

編輯站台繫結				?	×
類型(I): https 〜	IP 位址([): 全部未指派		連接埠(<u>O</u>): ✓ 443		
主機名稱(<u>H</u>):					
□ 需要伺服器名稱指詞	<u>₩(N)</u>				
renew.test.gov.tw_ne	W	~	選取(L)	檢視(⊻)]
			確定	取消	

- ◆ 若因遠端連線匯入無法成功,可改下方操作方式。
- 1. 請將原憑證備份匯出。
 - (1) 開啟「Internet Information Services (IIS)管理員」。

在左邊點選主機名稱,再點選畫面右邊的「伺服器憑證」。

🍓 Internet Information Services (IIS) 管理員	– 0 ×
	😨 🗟 🏠 🔞 -
檔案(F) 檢視(V) 說明(H)	
連線 ・・ ・ ・ ・・ ・	 動作 管理伺服器 重新飲動 飲動 ● 貸止 檢視遮用程式集區 檢視站台 ● 取得新的網頁平台元件 (?) 說明
就緒	6

(2) 先點選要匯出的憑證,然後按下右邊畫面的「匯出」,依據匯出憑證的 視窗填上路徑與密碼(此組密碼若忘記了,將會無法使用匯出的憑證 檔)。到此,憑證備份完成。

📬 Internet Information Services (IIS)	管理員		– 0 ×
← → ♥IN-U1LEEOI8	L7E 🕨		🔛 📧 🟠 🔞 •
檔案(F) 檢視(V) 說明(H)			
福案(F) 檢視(V) 說明(H) 連線 ● 世始網頁 ● WIN-U1LEEOI8L7E (WIN-U) ● 應用程式集區 ● 6 站台 > ● Default Web Site	 同服器憑 此功能可用來要求及管求 使用的憑證・ ・ ・<td>證 重網頁伺服器可與針對 SSL 設定的網站搭配 ▼ ▼ 移至(G) ~ 發行給 www.test.com.tw</td><td>堕入 建立憑證要求 完成憑證要求 建立自我簽署憑證 建立自我簽署憑證 發標 更新 更新 文陽除 愈用已更新憑證的自動重新繫結 診明</td>	證 重網頁伺服器可與針對 SSL 設定的網站搭配 ▼ ▼ 移至(G) ~ 發行給 www.test.com.tw	堕入 建立憑證要求 完成憑證要求 建立自我簽署憑證 建立自我簽署憑證 發標 更新 更新 文陽除 愈用已更新憑證的自動重新繫結 診明
	< () () () () () () () () () () () () () (28	
▲ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★			G

🍓 Internet Information Services (IIS) 管理員	— 0 X
	🔤 📧 🟠 🔞 -
檔案(F) 檢視(V) 說明(H)	
連線 ●	動作 僅入 建立愿證要求 完成憑證要求 建立信载簽署憑證 建立目载簽署憑證 機視 運出 更新 ※ 移除 歐用已更新憑證的自動重新繫結 ② 說明
就緒	6

2. 將匯出的 PFX 檔匯入至其他有安裝 IIS 的電腦(請利用 mmc 匯入方式)。

(1) 「開始」→「輸入 mma	:」,按下「Enter」	」°	
本機			
最佳比對			
mmc			
命 动行命令			
	_n 13		
mmc			
= 2 m @ =	- 1		
(2) 選擇「提安」」「新揃	/ 救 除 よ 入 ナ 答 理	留元。	
	初示职人民官理		Tanan Anna 1
🖀 主控台1 - [主控台根目錄]		2-	×
🚟 檔案(F) 動作(A) 檢視(V) 我的最要	5(O) 視窗(W) 說明	(H)	_ & ×
◆ 開新檔案(N)	Ctrl+N		
□ 開馭(O) (甘方(C)	Ctrl+O		動作
品(4) 另存新檔(A)	可顯示		主控台根目錄 🔺
新增/移除资本人式管理第元(M)	Ctrl+M		其他動作 ▶
選項(P)	Currin		
1 secol msc			
(注意(2))			
變更使用者及/或嵌入式管理單元主控台的選	項。		

(3) 點選「憑證」→「新增」

人式管理單元	廠商	^	111 主控台根目錄	編輯延伸(X)
且有谁踏安全性的 Win	Microsoft Corp			
服務	Microsoft Corp			移除(R)
原則結果組	Microsoft Corp			
效能監視器	Microsoft Corp			上移(1)
授權管理員	Microsoft Corp			10(0)
群組原則物件編輯器	Microsoft Corp			下移(D)
裝置管理員	Microsoft Corp		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 舆 V			
细址連結	Microsoft Corp			
憑證	Microsoft Corp	~		進階(V)
:				

(4) 「電腦帳戶」→「下一步」→「完成」。

選取電腦		×
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	音理:	
◉ 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	

(5) 「確定」。



(6) 點選到個人下的憑證,按下右鍵「所有工作」→「匯入」



(7) 選擇之前備份的憑證檔,輸入密碼來執行匯入動作。

÷ .	ቓ 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 [卜一步] 羅續。
	下一步(N) 取減
← 4	☞ 憑證匯入精靈
_	要匯入的檔案 指定您想要匯入的檔案。

描安之瑶(D	
™#RDRep D:\gcara.pfx	瀏覽(<u>R</u>)
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)	

(8)	輸入匯出時設定之密碼	以及勾選	「將這個金鑰設成可匯出」	0
-----	------------	------	--------------	---

← 🖉 憑證匯入績靈
私密金鑰保護 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(1): ■ 啟用強式私密金鑰保護。如果您敵用這個選項,每次私密金鑰被應用程式使用。系統 便會通知您(E)
 ▶ 調道個金鑰設成可匯出,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
← 🦻 憑證匯入精靈
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) ● 將所有憑證放入以下的存放區(P) 馮證左放區・
個人 瀏覽(R)
下一步(N) 取消

← 🛃 憑證匯入精靈			
完成憑證匯入精靈			
按一下 [完成],即可匯入》	長證。		
您已指定下列設定: 使用者攫取的憑證存放區 內容 權安全稱	個人 PFX Dàgcara pfy		
177 (FT 976 HH)	D. (gedia.pix		
		完成D	取消
憑證匯入精靈 ×			
〔 匯入執行成功。			
確定			

- 3. 於 IIS 完成註冊要求, 匯入新憑證。
 - (1) 開啟「Internet Information Services (IIS)管理員」,點選主機連線預設名稱,再點選畫面右邊「伺服器憑證」。

📬 Internet Information Services (IIS)	管理員	- 0 X
← → WIN-U1LEEOI8	.7E 🕨	🔛 🖄 🔞 🔹
檔案(F) 檢視(V) 說明(H)		
建線	 WIN-U1LEEOI8L7E 首頁 · ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	動作 各理伺服器 重新設動 敵動 停止 検視應用程式集區 検視站台 取得新的網頁平台元件 ② 説明
就緒		61

(2) 點選「完成憑證要求」。

💐 Internet Information Services (I	IIS) 管理員		– 🗆 X
← → ● DESKTOP-JUI	DB30K >		🔤 🖂 🟠 🔞 🗸
檔案(E) 檢視(⊻) 說明(H)			
 ■ ● ●	 ・ 一日服器 憑證 ・ 単語 ・ 単語 ・ 単語 ・ 単語 ・ 単称 ・ 単称 ・ 単称 ・ ・ ・	與針對 SSL 設定的網站描配使用的憑 至④ ~	動作 運立憑證要求 完成憑證要求 建立启我簽署憑證 設用己更新憑證的自動重新繫結 ② 說明
就緒			¶1.:

(3) 選擇新的 TLS 憑證,並輸入好記的名稱。

完成憑證要求	?	×
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\(\(new)7368A6D289D75E9D58		
好記的名稱(V): renew.test.gov.tw_new 選取新憑證的憑證儲存區(S): 個人 V		
確定	取消	

(4) 按「確定」,出現完成憑證要求的畫面,多一條新憑證列表。(請重新 整理確認憑證沒有消失,將憑證點2下開啟確認是否有其對應的私 鑰。)

💐 Internet Information Services (I	IIS) 管理員		- 🗆 X
← → ● DESKTOP-JUI	DB30K 🕨		😰 🖂 🟠 🔞 🗸
檔案(E) 檢視(⊻) 說明(H)			
福案(P) 檢視(V) 說明(H) 連線 ② DESKTOP-JUDB30K (DESK) → ③ 随用程式集區 > → ④ 站台	● ・ の服器憑 の服器源 の の の の の の の の の の の の の	[與針對 SSL 設定的網站描配使用的憑 至(⑤) - √ 全部顯示(Δ) / 發行給 renew.test.gov.tw renew.test.gov.tw	國人 建立憑證要求 完成憑證要求 建立自我簽署憑證 險視 夏世 政規 更新 教除 愈用己更新憑證的自動重新繁結 诊
		>	
< > > 就緒	□目 初尾俄倪 ₩ 四音傑虎		

- 將與私鑰結合的新憑證匯出並匯入至原主機,於 IIS 站台繫結選取新憑證即 可。
 - (1) 匯出新憑證請參考第1點操作步驟(p.7至 p.8)
 - (2) 匯入新憑證請參考第2點操作步驟(p.9至 p.14)
 - (3) 至原主機開啟「Internet Information Services (IIS)管理員」, 點選要安裝的站台,本手冊以(Default Web Site)進行說明,選擇「繫結」。

lnternet Information Services (IIS)	管理員			- 0	×
← → WIN-U1LEEOI8I	.7E 🕨 站台 🕨 Defaul	t Web Site 🔸		🔯 🗵 🟠	•
檔案(F) 檢視(V) 說明(H)					
連線 <	Default \	Web Site 首	頁	動作	
→ ● 型店相員 WIN-U1LEEOI8L7E (WIN-U) ◎ 應用程式集區 → ◎ 站台 > ● Default Web Site	師選器: ⅡS HTTP 回應標 MIME 事 項	 ▼ 移至 ● ●<!--</th--><th>(G) ▼ ▲ ●<!--</th--><th> ▲ 編輯催侬 ● 经最优合 ● 菱结 ● 基本設定 檢視應用程式 檢視感樹目錄 </th><th></th></th>	(G) ▼ ▲ ● </th <th> ▲ 編輯催侬 ● 经最优合 ● 菱结 ● 基本設定 檢視應用程式 檢視感樹目錄 </th> <th></th>	 ▲ 編輯催侬 ● 经最优合 ● 菱结 ● 基本設定 檢視應用程式 檢視感樹目錄 	
	記錄 處理常3 應	式對 預設文件	模組	管理網站 ご 重新啟動 ● 啟動	۲
	■●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	〕 父 頁 聖 編	瀏覽目錄	● 使止 激覽網站 ● 瀏覽 *-80 (http) 進階設定	
	€ ● ●			設定 限制	
<>	🔟 功能檢視 💦 內容檢	視			
就緒					6

(4) 選擇已存在的 https 443 連接埠,點選「編輯」。

¢	占台繫結						?	×
	類型	主機名稱	連接埠	IP 位址	繫結資訊		新増(<u>A</u>)	
	http		80	÷			絙 訳(F)	
	https		443	÷			₩ ₩ #4(Ľ)	
							移除(<u>R</u>)	
							瀏覽(B)	
							關閉(<u>C</u>)	

(5) 重新選擇要安裝在此站台新的 TLS 憑證。

編輯站台繫結				?	×
類型①: https ∨	IP 位址([): 全部未指派		連接埠(<u>O</u>): ✓ 443]	
主機名稱(<u>H</u>):					
□ 需要伺服器名稱指:	汞(<u>N</u>)				
ssi 馮暾(E)· renew.test.gov.tw_ne	ew	~	選取(上)	檢視Ѹ	
			確定	取消	

網站伺服器:Apache

1. 將憑證由 DER 格式轉換為 Base64 格式。

(1)	點選憑證	檔案後,選擇詳細資料。
憑證		×
一般	詳細資料	憑證路徑
	📮 憑證資訊	R
ž	這個憑證的使用 ●確保遠端 ●向遠端電」 ●2.16.886.1	相目的如下: 電腦的識別 腦證明您的身分 01.0.3.3
	發給:	gcaweb.nat.gov.tw
	簽發者:	政府憑證管理中心
	有效期自	2014/ 1/ 17 39 2017/ 1/ 17
深入	、了解 <u>憑證</u>	安裝憑證O 簽發者聲明(3)
		確定

(2) 選擇複製到檔案。

憑證	×
一般 詳細資料 憑證路徑	
顯示(3): << 全部>	
欄位	值
□□版本 □□序號	V3 00 æ 3b 14 63 94 84 8d 61 3c ■
自一般早通 昇法 「日」 後章 雑湊演算法 「日」 後發者	sha256KSA sha256 政府憑證管理中心,行政院,…
有效期自 「同有效期到	2014年1月17日上午 09:54:41 2017年1月17日上午 09:54:41 👻
深入了解些證詳細資料	編輯內容④ 複製到檔案①
	確定

(3) 點選下一步。

憑證匯出精靈					
	歡迎使用憑證匯出精靈				
	這個精靈將協助您從憑證存放區將憑證、憑證信任 清單及憑證撒銷清單複製到您的磁碟中。				
	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。				
	<上一步(B) 下一步(A) > 取消				
(4) 選擇 Base64 編碼	, °				
憑證匯出精靈					
匯出檔案格式 憑證可以用多種檔案	格式匯出。				
法婴页你相要传用的	枚式·				
	市				
● Base-64 編碼 X	.509 (CER)				
◎ 加密編譯訊息詞	語法標準 - PKCS #7 憑證 (.P7B)(<u>C</u>)				
□ 如果可能的	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	● 個人資訊交換 - PKCS #12 (.PFX)(型)				
	 」如果可能的話,包含您證路徑中的所有您證(U) □ 加里薩史成功即刪除私変全論(K) 				
○ Microsoft 序列	馬證存放 (.sst)(I)				
深入了解 <u>憑證檔案格式</u>					
	<上一步(B)下一步(N)> 取消				

(5) 輸入檔案名稱。

憑證匯出精靈	×
要匯出的檔案 諸指定您要匯出的檔案名稱	
檔案名稱(F): gcaweb	瀏覽(R)
	<上一步(B)下一步(N)> 取消

- (6) 完成轉換。
- 2. 以文字編輯器開啟 Base64 格式憑證, 並與原憑證設定檔中的 TLS 憑證更換。
 - (1) 若 Apache 版本 < 2.4.8, 請參考以下步驟操作
 - 利用文字編輯器開啟 httpd-ssl.conf,檔案可能位置為<apache 安裝路徑>\conf\extra\ 目錄下。
 修改以下參數並存檔 SSLCertificateFile:伺服器憑證(*.crt)檔案
 路徑。
 - (2) 若 Apache 版本 >= 2.4.8, 請參考以下步驟操作
 - 利用文字編輯器開啟 httpd-ssl.conf,檔案可能位置為<apache
 安裝路徑>\conf\extra\ 目錄下。
 - ii. 利用文字編輯器開啟原指定的憑證檔(範例為 sever.crt),SSLCertificateFile 參數指定之位址。

```
SSLCertificateFile "/export/httpd-2. /certs/gca_server.crt"
SSLCertificateKeyFile "/export/httpd-2. /certs/gca_server.key"
```

iii. 將憑證檔內容最上面的原 TLS 憑證,更換為步驟1轉換成Base64 格式的新 TLS 憑證內容,可參考下圖。

9KmS6KznEVKBRq7/w3SouQznO0wRGcS8TxOSvIkWfMDmeU2081kvqMmDLbiLxpya W4c1jrcgcgMqe3JzJSbN5rZBqgnQseAnV0HktCrs9MDig3Sd7yLpSrgLJId1PvnI	市協告がなっていませい
vA==	史換為新的ILS憑證
END CERTIFICATE	
======================================	was/ was/ was/ was/ was/
issuer=/C=TW/O=Chunghwa Telecom Co. Ltd /CN=aDWI Doot Cartificat	tion Authority - 62
BEGIN CEDTIFICATE	cion Authority - Gz
MITGHICCRIE AVIBAGIBATIATIATIA	8
V2ELMAkGA1UEBbMCVEcxTzAbBcNVBAcMGkNodW5naHdbTER1bGV5b20c028uLCBM	
dG0uMSSwL0VDV00DDCZ1UEt.JIEJyb30g02VvdG1maWNbdG1vb1BBdXRob3JbdHkg	
LSBHM1AeFw0x0TA3MTkwN102NDVaFw0zMTA4MTkwN102NDVaMFgxCzAJBgNVBAYT	
AIRXMRTwEAYDVOOKDAnooYzml1./pmaIxNTAzBgNVBAMMLOaUv+W6nOSSuuacteWZ	
gOaVuOS91eaGkeitieeuoeeOhuS4reW/gvAtlEcxMIICI1ANBgkghkiG9w0BAOEF	
AAOCAg8AMIICCgKCAgEAwg5R4LGoDi+mZIXmcHmRYv501isSLIm7EoX/KAt74uN2	馮諮串鋪內容不動
vDR436V2EWkFeWhD+TS4sx2/3JCRW+KE+IX8NYBK1sWuK9OMY4Gu4FEWJpBu1XCW	
YjTPKyhHdEhDpxRxv91g3Zk68XgK7j2U5sEzCPx13QjkH7gc/Mo5BFiro8YsYAfx	
gCoa/rZFEsXyZKXRJeIDw7t+iPxVy2cbQ0uNlo09670LGo0V2YVkYABv3IwZo+JR	8
tj+j7rLjB7xQKYmfJOA2Jc96yPm6li7zHrIQYfohGPdANmwR9opNNgYOo+LtsIYo	
t3/cLp9YgAaiGdrAiKrbbEVkYH+zKzAHolf5mPBn+h30ElYfygESitWRBp2bwf0G	
JwAYseTuorQHpyQpslGGcn9vcfnLhvLxa3DMrCAvSJb3SvHCyqahQz0KR0IPcu+V	
LW3icaqlbJausGIGYqp8VSN6FJ0pgmYdbunBLYclv23VvjmVMl+xNJoaSFEUscmS	8
qA4CuYANhkWSANk8HI9rNbvmzuyWhSv7tUXY6UB67mHp4ypGcKYbXrjiKqahv6QL	
UEb7s8FD71Ds75F2vMeO4O7716joBs/L2E6WZJvSronzJCXL0IwmpYaOAsoFOf0e	1
GVsPBVKn+z4Bq0WA0+r7plfWofDbUGmx9Zun++rWhoDXrma+odubN1Xj1Rj1L3sC	8
AwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFHJbuqpy0041kCS11CL6CYjKiwr7MB0G	
AludDgQWBBTW6y2dYf4ru3CILrgHsVmw9IMiajAOBgNVHQ8BAf8EBAMCAYYwPAYD	
VR0fBDUwMzAxoC+gLYYraHR0cDovL2VjYS5oaW51dC5uZXQvcmVwb3NpdG9yeS9D	8
UkwyL0NBLmNybDCBggYIKwYBBQUHAQEEdjB0MDsGCCsGAQUFBzAChi9odHRw0i8v	8
ZWNhLmhpbmV0Lm5ldC9yZXBvc2l0b3J5L0NlcnRzL2VDQUcyLmNydDAlBggrBgEF	
BQcwAYYpaHR0cDovL29jc3AuZWNhLmhpbmV0Lm51dC9PQ1NQL29jc3BHMnNoYTIw	6
EgYDVR0TAQH/BAgwBgEB/wIBADA1BgNVHSAEGzAZMA0GCysGAQQBgbcjZAADMAgG	8
BmeBDAECAjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwDQYJKoZIhvcN	
AQELBQADggIBAEyrsJ9vUi6nEfwO0vgAoFefXpCRF+uDsmG/8F60V9VRnbtzBwaz	8
HbxVmaBvDRVofLfoXWr+Nd8dd3BXVUNxemNrkZa8Hdgdv4s8yFbRs0W6fRTWkhCc	3
c39RpQtSeV7kyxCPlrMTYRSqCA9F+FcDMLXJIzZrz17Tn6guIyqcfZv6sRN7CbbT	
rYKSc0JX4t26WGFun2zLjzH8kx1TZ457TE4yyj11oSZdgiWL6Hz71+nbTe6WqPVV	
m4am2AAmaQaLGncsGLas17PIHx9Nc4sy7KdOMTc5r0BPCGhAiJ6ueQ6aVd49pra7	
BDIqFMA7Myy4pXRYfqFnjq9RuROWY1IluzLNUSxlaFtTMUVQnWjJxnlXlBDLX9L4	6
OAxTOvdbtcNNS1GK+W1cWiYdTOWF4HTu5pvdUn/+8yVE4E7MPb0vGuxv3S11QG6J	
tVPuHkX6BGqRXHo253gY77HZU0g3g9qVs9Ua2jWS5UTcqdgLmmOQnH7USaJ9/4rX	
Ru/P8IWMPG2s6tv1dRVQV5xfq21PQ4y53ytVd0+/1p0L743+1AjnOw018t9QxP6c	
2t1+oo4srxM8YE3etVLQBeWsmJc00GOWa/XmFACsy8Lkctx0QScAAYwCfB2accfx	
]9nEX1c6MAeVUVpU4YJX4dtjoIFTPI1/MFX+FkxMq4Fs6k+mxSm7tNvv	
LINE VERALE AVRAG	
subject=/C=TW/O=Chunghwa Telecom Co., Ltd./CN=ePKI Root Certific	ation Authority - G2
issuer=/C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certificat	tion Authority
BEGIN CERTIFICATE	1
MIIHeDCCBWCgAwIBAgIQ0+7gkY6IhglGD+iukOvcutANBgkghkiG9w0BAOgFADBe	8
MOswCQYDVQQGEwJUVzE1MCEGA1UECgwaQ2h1bmdod2EgVGVs2WNvbSBDbv4sIEx0	(

iv. 將修改後的 TLS 憑證檔案存檔,檔案放置路徑跟原本 SSLCertificateFile 參數相同。

3. 重新啟動 Apache Server。

網站伺服器:Tomcat

- 1. 請直接於原憑證安裝的 Keystore 重新匯入新憑證即可。
 - (1) 確認 PrivateKeyEntry 的 alias name

在 %JAVA HOME%\bin 目錄下執行

keytool -list -keystore <keystore 檔案所在路徑>

- 待出現 Enter keystore password:請輸入密碼。
- 找到 PrivateKeyEntry 對應的 alias name, 範例為 tomcat



- (2) 匯入新的 TLS 伺服器應用軟體憑證。
 在 %JAVA_HOME%\bin 目錄下執行
 keytool -import -alias <PrivateKeyEntry 的alias name> -file D:\(憑證名稱cer) -keystore <keystore 檔案所在路徑>
 - 待出現 Enter keystore password:請輸入密碼。

- ◆ 若直接於 Keystore 安裝新憑證有問題,也可參考以下方式安裝新憑證。
- 先執行以下指令得到 keystore(jks 檔)裏含有私鑰(PrivateKeyEntry)的 alias name

keytool -list -keystore tomcat.jks



2. 執行以下 keytool 指令,將 JAVA Keystore (JKS) 轉檔為 PFX 檔

keytool -importkeystore -srckeystore tomcat.jks -destkeystore server.pfx srcstoretype jks -deststoretype pkcs12 -srcalias tomcat



得到 PFX 檔案(範例為 server.pfx)後,再到有安裝 openssl 的電腦執行下面的指令,這樣就會得到私鑰 server.key

openssl pkcs12 -in server.pfx -nocerts -nodes -out server.key



4. 重新至以下連結下載憑證串鏈檔,再依後續步驟執行

https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip

5. 重新至 GCP 網站下載已簽發憑證,並命名為 install.crt,並依以下指令將 DER 格式憑證轉換為 B64 格式憑證,此處刻意將另存的 Base64 格式憑證命名為 install_B64.crt

openssl x509 -inform der -in install.crt -out install_B64.crt

6. 以文字編輯器開啟 install_B64.crt,並將憑證串鏈檔 GTLSCA_All.zip 解開之所 有憑證依下列順序以文字編輯器開啟,並全選貼至 install_B64.crt 後存檔,檔 案大小約 11kb,此時 install_B64.crt 即具備所有中繼憑證。

憑證順序由上而下為 install_B64.crt -> GTLSCA.crt -> eCA1_to_eCA2-New.crt -> ROOTeCA_64.crt

*linux: cat install_B64.crt GTLSCA.crt eCA1_to_eCA2-New.crt ROOTeCA_64.crt > server.crt, 再將 server.crt 改名為 install_B64.crt 以進行後續步驟

7. 將憑證及私鑰依以下步驟再次轉換為 pfx 格式

openssl pkcs12 -export -in install_B64.crt -inkey server.key -out install_B64.pfx

C:\Windows\System32\cmd.exe	-		×	
C:\certtemp\0616>openss1 pkcs12 -export -in install_B64.crt -inkey server.key -out : Enter Export Password: Verifying - Enter Export Password:	install_	_B64.p	fx	~
C:\certtemp\0616>				

 \sim

8. 將 pfx 轉換為 jks 格式

(1) 先以底下指令得到 pfx 檔私鑰(PrivateKeyEntry)的 alias name(下圖紅框處)

keytool -list -keystore install_B64.pfx -storetype PKCS12

	C:\Windows\System32\cmd.exe	_		×
	C:\certtemp\0616>keytool -list -keystore install_B64.pfx -storetype PKCS12 Enter keystore password: Keystore type: PKCS12 Keystore provider: SUN			
	Your keystore contains 1 entry			
(1,2022年6月16日, PrivateKeyEntry, Certificate fingerprint (SHA-256): 0F:2E:6A:62:95:FF:B5:C8:E6:87:41:06:01:DB:9E:1E:2C 6:5C:61:72:AF:D3:11:93:47:ED:AA	:FA:E3	:63:3A	:В
	Warning: <1> #4 of 4 uses the SHAlwithRSA signature algorithm which is considered a security r rithm will be disabled in a future update.	isk. T	his al	go
	C:\certtemp\0616>			
				~

(2) 依前述得到的 alias name 填入下列指令,以將 pfx 轉檔為 install.jks(alias name 為 tomcat,可自行替換)

keytool -importkeystore -srckeystore install_B64.pfx -destkeystore install.jks -

srcstoretype pkcs12 -deststoretype jks -srcalias 1 -destalias tomcat

🖬 C:\Windows\System32\cmd.exe	—		\times	
C:\certtemp\0616>keytool -importkeystore -srckeystore install_B64.pfx -destkeystore cstoretype pkcsl2 -deststoretype jks -srcalias 1 -destalias tomcat Importing keystore install_B64.pfx to install.jks Buter destination keystore password: Re-enter new password: Enter source keystore password:	install	.jks -	.sr	~
Warning: The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 w stry standard format using "keytool -importkeystore -srckeystore install.jks -destke jks -deststoretype pkcs12".	hich is ystore	an ir instal	ıdu 1.	
C:\certtemp\0616>				
				~