# 政府憑證管理中心(GCA) SSL 憑證串鍊設定說明

# 國家發展委員會 中華民國 106 年 8 月

目錄

一、前言	3
二、安裝方式	4
(一)網站伺服器: Windows IIS 7	4
(二)網站伺服器: Windows IIS 8	15
(三)網站伺服器:Apache	25
(四)網站伺服器:Tomcat	
三、憑證串鍊檢測方式	32

## 一、前言

- 本本文件係針對機關網站已導入 HTTPS 機制(先前已安裝過 GCA SSL 憑證)的網站伺服器參考操作使用,請依照貴機關網 路伺服器版本執行安裝設定。
- ➤ 若貴機關網站尚未導入 HTTPS 機制,則不須重新安裝設定。

# 二、安裝方式

### (一)網站伺服器: Windows IIS 7

1. 請先點選「開始」→輸入「mmc」→按下「Enter」。



🚟主接台1 - [主接台)	根目錄]					IX
🚠 檔案(F) 🛛 執行(A)	檢視(♡)	我的最愛(0)	視窗(₩)	說明(H)	_ 8	×
	? 📊					
📔 主控台根目錄	名稱				 動作	
		這個檢測	視沒有項目で	可顯示。	主控台根目錄	•
					其他動作	►
	1					

2. 選擇「新增/移除嵌入式管理單元」。

屬主接台1 - [主接台根目錄]	
☐ 檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(F	) _8×
↓ 開新檔案(N) Ctdl+N	
■ 開設售檔(O)… Ctd+O (独友(Y) Ct+L()	動作
協計(%)     この目前       另存新檔(A)     沒有項目可顯示。	主控台根目錄 ▲
新增移除嵌入式管理單元(M) Ctrl+M	其他動作 ▶
選項(r)	
1 servermanager.ms:	
2 C:\Windows\\devmgmt.msc	
3 C:\Windows\system32\gpedit.msc	
結束(X)	

3. 接著點選「憑證」→「新增」。

新增或移降嵌入式管理軍 您可以為這個主控台從您 元。對於可延伸的嵌入式	元 約電腦上可以使用的 管理單元,您可以設	教入式管理單元中選擇一些嵌入去 定啟用哪些延伸。	× 管理單元,並且設定所選擇的嵌入式管理單
可用的嵌入式管理單元(%): 嵌入式管理單元	廠商    ▲	選取的嵌入式管理 🧰 主控台根目錄	單元(E): 編輯延伸(X)
<ul> <li>終端機服務管理員</li> <li>評組原則物件編輯器</li> <li>要若留理員</li> <li>資料夾</li> <li>路由及遠端存取</li> <li>電腦管理</li> <li>電腦管理</li> <li>電話語音</li> <li>網址連結</li> <li>網路存取保護 (NAP</li> </ul>	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft A Microsoft A Microsoft Cor Microsoft Cor Microsoft Cor	新增(A) >	移除(R) 往上移(U) 往下移(D) <b>進階(V)</b>
描述: 憑證嵌入式管理單元讓您	瀏覽電腦或服務的憑	遺存放內容。	確定 取消

選擇「電腦帳戶」→「下一步」→「完成」。

<b>憑證嵌入式管理單元</b>	x
這個軟人式管理単元將目動管理下列根戶的感證:	
○ 我的使用者帳戶(M)	
C 服務時間()	
<ul> <li>○ 電腦帳戶(C)</li> </ul>	
<上一步四(下一步の)> 取消	

選擇電腦	×
諸選擇您要嵌入式管理單元管理的電腦。	
	1
● 本機電腦(L): (執行這個主控台的電腦)	
○ 另一台電腦(A): 瀏覽(R)	
□ 九許對選取的電腦進行從命令列所啟動的變更。這只在您儲存主控台後才能適用 (₩)	
	]
	_
<上一步(L) 完成 取消	

# 最後按下「確定」。

<ul> <li>表入式管理單元</li> <li>終端機服務管理員</li> <li>詳組原則物件編輯器</li> <li>装置管理員</li> <li>資料夾</li> <li>資料</li> <li>電腦管理</li> <li>電話語音</li> <li>網站存取保護 (NAP</li> <li>透端桌面</li> <li>憑證</li> </ul>	厳商 Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Q Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	新增(A) >	■主控台根目錄 → 憑證 (本様電腦)	編輯延伸(X) 移除(R) 往上移(U) 往下移(D)
---	--	---------	------------------------	--------------------------------

4. 删除已經無用之 GRCA2 憑證

檢查信賴的根憑證中是否有 GRCA2 的憑證(到期日為

2037/12/31),若有請刪除。

-	主接台	1 - [主接台	根目錄/憑言	<b>遼 (本機電腦)</b> \	信任的根憑	<b>遺授權\</b> 憑護	2]		
-	檔案(F	) 執行(A)	檢視(♥)	我的最愛(0)	視窗(₩)	說明(H)			_ 8 ×
		2 🗖   🐇	' 🖷   🗙	🗟 🛛 🖬					
	主控台	根目錄	發給 ▲			發行者		動作	
	📮 憑調	證 (本機電脂 /用 -	Class 3	Public Primary C	Certification	Class 3 Publi	ic Primary Certif	憑證	•
L	-	迴入 信任的根憑		Public Frimary C zht (c) 1997 Miej	.eruncanon msoft Com	Class 3 Publi Conversibilit (c	c Frimary Certif	其他動	」作 ▶
		🗋 憑證		oot Certification .	Authority	ePKI Root C	ertification Aut	選擇的項目	a 🔺
	F 📫	企業信任	🔄 Microse	ft Authenticode (	(tm) Root A	Microsoft Au	uthenticode		
	± _	中磁速度均受信任的支	<b>Govern</b>	ment Root Certif	ication Aut	Government	Root Certificati	具把動	lπ⊨ ►
1	+	沒有信任的	Microst	oft Authenticode( oft Root in dia di	(tm) Root A	Microsoft Au	uthenticode(tm). 201. 9 uthority		
	+ 🚞	第三方根温		oft Root Certifica	y te Authority	Microsoft Ro	oot Certificate A		
	+ 📄	受信任的/ 馮證註冊型	👼 NO LIA	BILITY ACCER	PTED, (c)9	NO LIABILI	ITY ACCEPTEI		
	÷ 📑	智慧卡信伯	🔄 Thawte	Timestamping C	A	Thawte Time	estamping CA		
┛			•				<u> </u>		

5. 檢查中繼憑證授權單位中是否有 GRCA 的自發憑證(到期日為

2032/12/5),若有請刪除。

6. 請至下列網址下載2張自發憑證

第1張 GRCA 自發憑證(GRCA1 簽 GRCA1.5) http://grca.nat.gov.tw/repository/Certs/GRCA1\_to\_GRCA1\_5.cer 第2張 GRCA 自發憑證(GRCA1.5 簽 GRCA2)

http://grca.nat.gov.tw/repository/Certs/GRCA1\_5\_to\_GRCA2.cer

 7. 匯入第1張自發憑證。在「中繼憑證授權」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\憑證]	
🚠 檔案(F) 執行(A) 檢視(∀) ま	的最愛(O) 視窗(₩) 說明(H)	_ & ×
🗢 🔿 📶 📅 📋 🧔 😼	? 🖬	
📔 主控台根目錄	發給 ▲   發行者	動作
□ 🗊 憑證 (本機電腦)	🔄 Microsoft Windows Hardware Com Microsof	tR) 摄输
	Public Certification Authority ePKI Ro	ot C
🗆 📒 信仕的根徳證授曜	Root Agency Root Ag	enc] 具把動作 ▶
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	🔄 VeriSign Class 1 CA Individual Su Class 1 P	ubl
□ □ □ 正未信任	🔄 VeriSign Class 2 CA - Individual S Class 2 P	ubl
日 — 干酪炒起了个推	www.verisign.com/CPS Incorp.by Class 3 P	ubl
📑 😇 所有工作(K)	匯入(1)	
王 📔 沒有信 🔞 襪(V)	,	
田 🦲 第三月 👋 這裡新煙湖窗	141)	
📘 🗉 🧮 憑證訂 🛛 新工作台檢視(T)		
■ 🔛 🎬 智慧   🔢 🗠 🔛		
第二に)		
里利楚理(1) 医山注盟の		
		_
包含可以在這個項由工報们的BUTF。		

# 出現以下畫面後,點選「下一步」→「下一步」→「完成」。



入檔案	
指定您想要随人的檔案。	
檔案合稱[[]]:	
E.VGRCA1_to_GRCA1_5.cer	[ 瀏覽 <u>R</u> )]
請注意: 您可以將數個憑證用以下的	的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX, P	12)
密碼編譯訊息語法標準 - PKCS #	7 認證 (.p7b)
Microsoft 序列憑證存放 (.sst)	
入了解憑證檔案格式	
	<上一步(B)   下一步(N) >   取消
主人精靈	
<b>建人精靈</b> 證存放區	
主人精密 證存放區 憑證存放區是用來存放憑證的系統區	矗域。
<b>送存放區</b> 透音放區是用來存放憑證的系統區	聶域。
上人構整 證存放區 憑證存放區是用來存放憑證的系統區 Windows會自動選擇一個憑證存放區	區域。 區,您也可以為憑證指定存放位置。
主人構築  建存放區  憑證存放區是用來存放憑證的系統  Windows會自動選擇一個憑證存放區	區域。 亟,您也可以為憑證指定存放位置。 ■ 方物原 (11)
■人構築 建存放區 憑證存放區是用來存放憑證的系統 Windows會自動選擇一個憑證存放 ○ 自動根據憑證類型來選取憑證 ○ 酸的有調發短 1000000000000000000000000000000000000	區域。 區,您也可以為憑證指定存放位置。 覺存放區(U)
■ 人構築 選存放區 憑證存放區是用來存放憑證的系統區 Windows會自動選擇一個憑證存放區 ○ 自動根據憑證類型來選取憑證 ● 解所有憑證放入以下的存放區 週週五故區。	區域。 區,您也可以為憑證指定存放位置。 覺存放區(U) <u>〔(P)</u>
<ul> <li>▶ 人構築</li> <li>※ 證存放區</li> <li>● 憑證存放區是用來存放憑證的系統區</li> <li>● Windows 會自動選擇一個憑證存放區</li> <li>● 簡動根據憑證類型來選取憑證</li> <li>● 將所有憑證放入以下的存放區</li> <li>憑證存放區:</li> </ul>	區域。 亟,您也可以為憑證指定存放位置。 聲存放區(U) ፪(P)
<ul> <li>▲ 人 構 密</li> <li>(2) 建存放區</li> <li>● 憑證存放區是用來存放憑證的系統區</li> <li>● Windows 會自動選擇一個憑證存放區</li> <li>● ○ 自動根據憑證類型來選取憑證</li> <li>● 第所有憑證放入以下的存放區</li> <li>憑證存放區:</li> <li>□ 中繼憑證授權</li> </ul>	區域。 區,您也可以為憑證指定存放位置。 發存放區(U) 區(P) 圖(R)
<ul> <li>■人構築</li> <li>■遊存放區</li> <li>● 憑證存放區是用來存放憑證的系統區</li> <li>○ 剛動根據憑證類型來選取憑證</li> <li>○ 簡動根據憑證類型來選取憑證</li> <li>○ 將所有憑證放入以下的存放區</li> <li>憑證存放區:</li> <li>□中繼憑證授權</li> </ul>	區域。 區,您也可以為憑證指定存放位置。 聲存放區(U) ⑤(P)
<ul> <li>■ 人構築</li> <li>● 適合放區</li> <li>● 過動器揮一個憑證存放區</li> <li>● 自動根據憑證類型來選取憑證</li> <li>● 將所有憑證放入以下的存放區</li> <li>● 避視振盪證授權</li> </ul>	區域。 區,您也可以為憑證指定存放位置。 證存放區(U) 區(P) ————————————————————————————————————
<ul> <li>▶ 送存放區</li> <li>&gt; 還存放區是用來存放憑證的系統區</li> <li>○ 副動根據憑證類型來選取憑證</li> <li>○ 副動根據憑證類型來選取憑證</li> <li>○ 將所有憑證放入以下的存放區</li> <li>憑證存放區:</li> <li>□ 中繼憑證授權</li> </ul>	區域。 區,您也可以為憑證指定存放位置。 登存放區(U) 區(P) 
<ul> <li>▶ 法 書 2 (1)</li> <li>▶ 3 (1)</li> <li>▶ 4 (1)</li> <li>▶ 4 (1)</li> <li>▶ 5 (1)</li> <li>▶ 6 (1)</li> <li>▶ 7 (1</li></ul>	區域。 亟,您也可以為憑證指定存放位置。 聲存放區(U) ≦(P) 

<上一步圆(下一步图)>

取消

憑證匯入精靈		×
	完成憑證匯入精靈	
	按一下 [完成],即匯入憑證。 您已指定下列新設定:	
	使用者選取的憑證存放區 中維憑證授權 內容 憑證 檔案名稱 E:\GRCA1_to_GRCA1_5.ce	
	<上一步 B 完成 取消	

8. 匯入第2張自發憑證。在「中繼憑證授權」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\憑證]		>	×
🚟 檔案(F) 執行(A) 檢視(V) 劧	ຳ的最愛(O) 視窗(₩) 說明(H)		_82	<
🗢 🔿 🖄 📅 📋 🚨 😸 🗌	? 📊			
📔 主控台根目錄	發給 ▲	發行者	動作	=
□ □ □ 憑證 (本機電腦)	Microsoft Windows Hardware Com	Microsoft R	憑證 4	•
□ □ 10/2 □ □ 10/2 □ □ 10/2 □ □ 10/2 □ □ 10/2 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Root Agency	Root Agenc	其他動作 🛛	۶
■ 憑證	🧊 VeriSign Class 1 CA Individual Su	Class 1 Publ		
■ □ 企業信任	🔄 VeriSign Class 2 CA - Individual S	Class 2 Publ		
日	🔄 www.verisign.com/CPS Incorp.by	Class 3 Publ		
<ul> <li>受信式</li> <li>所有工作(K)</li> <li>受信式</li> <li>旅方信</li> <li>歳視(♡)</li> <li>従這裡新増視窗(</li> <li>① 憑證註</li> <li>新工作台檢視(T)</li> <li>① 智慧</li> <li>貼上(P)</li> <li>重新整理(P)</li> </ul>	▶ 匯入(I) (W) 			
進出清單(L)           說明(H)		Þ		
包含可以在這個項日工教IJBymyF。				

依照上述匯入第1張 GRCA 自發憑證的步驟, 匯入第2張自發憑

證。

<b>善證匯入精靈</b>	×
<b>匯入檔案</b> 指定您想要匯入的檔案。	
檔案名稱(2).	
E:VGRCA1_5_to_GRCA2.cer	
請注意: 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 ( PEX_P12)	
密碼編譯訊息語法標準 - PKCS #7 認證 (.p7b)	
Microsoft 序列憑證存放 (.sst)	
深入了解 <u>憑證檔案格式</u>	
<上一步(B) 下一步(A) > 取消	

匯入完成後的中繼授權單位只會有下圖中的3張憑證。

搹 主控台1 - [主控台根目鏡	(基礎電話)(中盤連選授権)(準約)	ĝ]			
🚠 檔案(F) 執行(A) 檢視	(Y) 我的最愛(○) 視窗(₩) 說明()	Ð			_ 8 ×
🧇 🔿 🙍 📅 📋 🧔	😹 🛛 📅				
1 主控台根目錄	彩给 🔺	登行者	到期日	動作	
<ul> <li>              E控台根目錄</li></ul>	Bite A Government Root Certification Aut Government Root Certification Aut Microsoft Windows Hardware Com Root Agency VeriSign Class 1 CA Individual Su VeriSign Class 2 CA - Individual Su Www.verisign.com/CPS Incorp.by 政府憑證管理中心.	送行主 Government Root Certification Autho Government Root Certification Autho Microsoft Root Authority Root Agency Class 1 Public Primary Certification A Class 2 Public Primary Certification A Government Root Certification Autho	④目目日 2020/7/19 2020/7/19 2002/12/31 2004/1/1 2008/5/13 2004/1/7 2004/1.8 2033/1/31	<b>動作</b> <u> </u> <u> </u> <u> </u> <u> </u>	•
✓ ▶ 中繼憑證授權 存放包含 8 個憑	<u>∢</u>		Þ		

9. 請重新繫結(Binding),進入編輯站台繫結後,請先選擇「未選

取」,之後再選原本的 SSL 憑證並按確定。

💱 Internet Information Service	es (III) 管理員	_ B ×
	71∀JUKVM → 站台 → Default Web Site →	🗾 🖸 🐼 🟠 I 🔞 🗸
檔案(F) 檢視(V) 說明(H)		
(福亮 (F) (秋代(V) 說明(H) 連結 2 · [2] [5] 2 · [2] [5] [5] [5] [5] [5] [5] [5] [5] [5] [5	Default Web Site 首頁         詳細依錄: 區域         評価         IS         Coi HTTP 回應標 HTTP 重新導 IP-4 位址及 ISAPI 篩邊器 MIME 類型         SSL 設定         URL Revoite         資料(原則)         Nota Table	bbf: 》 激發 編編編編版
	Kitps 443 *     Kitps     Kitps	<ul> <li>潮覽 %80 (http)</li> <li>潮覽 *443 (https)</li> <li>連階設定</li> <li>設定</li> <li>失敗要求的追蹤</li> </ul>



10. 若重新繫結後依然沒有更新為5層憑證串鍊,請將主機重開機。

### (二)網站伺服器: Windows IIS 8

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

Ĩ	7	rhā eļ s				전 2 방송에 다른				
				系統管理	里員: Wir	ndows PowerShell		_	. 🗆 X	
資)	Windows Power	Shell著作權	(C) 2012 Micros	oft Corporat	ion. 著作	乍權所有,並保留一切權利	利。		^	
	PS C:\Users\A PS C:\Users\A	dministraton dministrator	mmc							
		<b>a</b>			主控	台1 - [主控台根目錄]		_		
G		🚰 檔案(F)	動作(A) 檢視(V)	我的最愛(O)	視窗(W)	說明(H)			_ & ×	
ſ		📔 主控台根目	目録 名種	l				動作		
Ľ					這個	固檢視沒有項目可顯示。		主控台根目	目録 ▲	
my								其他動作	∎ ▶	19
										물건 다니 아버
	微軟新注音 半									
								W	indows Sen	ver 2012 Standard
	-									Build 9200
	-( ≥								- 18 19 (	2013/7/11 2013/7/11

2. 選擇「新增/移除嵌入式管理單元」。

	主控台1 - [主控台根目]	錄] Land Land Land Land Land Land Land Land
🚟 檔案(F) 動作(A) 檢視(V) 我的最愛(O)	視窗(W) 說明(H)	_ 8 ×
↓ 開新檔案(N)	Ctrl+N	
<b>開</b> 啟(O)	Ctrl+O	動作
儲存(S)	Ctrl+S 沒有項目可顯示	。 主控台根目錄 ▲
另存新檔(A)		
新増/移除嵌入式管理單元(M)	Ctrl+M	
選項(P)		
1 C:\Windows\system32\compmgmt		
結束(X)		
開啟一個現存的主控台。		

3. 接著點選「憑證」→「新增」。

您可以為這個主控台從您的電 》式等田第一,你可以認定的	腦上可以使用的嵌入 田哪些延伸。	式智	新増或移除嵌入式管理單元 理單元中選擇一些嵌入式管理單元	,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):			躍取的毒 λ <del>ず</del> 等 理	留元(F)·	
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				
🛃 授權管理員	Microsoft Corp				L13(U)
🧾 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 舆 V				
2 網址連結	Microsoft Corp				
🤇 🗊 憑證 🔹 🔵	Microsoft Corp	$\overline{\mathbf{v}}$			進階(V)
描述: 憑證嵌入式管理單元讓您瀏覽	電腦或服務的憑證符	₹放[	[內容。		
					唯正 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: ④ 我的使用者帳戶(M) ④ <u>服務帳</u> 戶(C) ● 電腦帳戶(C)	
< 上一步(B) (下一步(N) > 取消	
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理: ● 本機電腦 (執行這個主控台的電腦)(L): ○ 另一台電腦(A):	

最後按下「確定」。

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       受權管理員       詳組原則物件編輯器       長置管理員       資料夾       各曲及遭       置       電器       電	廠商 Microsoft Corp Microsoft Corp	III	新增(A) >	編輯延伸(∞) 移除(R) 上移(U) 下移(D)
網址連結 憑證	Microsoft Corp Microsoft Corp	~		進階(V)

4. 檢查信賴的根憑證中是否有 GRCA2 的憑證(到期日為

2037/12/31),若有請刪除。

• =)	N 🛎 🔟 🤞 K					
主	空台根目錄 連時(大時要知)	教給	遊覧者 「「「」」、「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」、「」、	到期E	動作	
P	③程(华级电信)	Class 3 Public Primary Certific.	Class 3 Public Primary Certificati	2028/	憑證	-
4	🧾 受信任的根憑證	Convright (c) 1997 Microsoft .	. Copyright (c) 1997 Microsoft C	1999/	其他動作	•
Ļ	通徳度(	Government Root Certificatio	overnment Root Certification	2037/	ePKI Root Certif	-
	中端憑證授權單 安保有值任根證 受保有值代感證 受信任明的證證授 要信件論題 要信件論題 要指的 是一方明的證證 要 是一方明的證證 要 是一方明的證證 要 是一方明的證證 要 是一方明的證證 是 要 是 一 是 是 一 是 一 是 是 一 是 是 一 是 是 是 一 是 是 是 一 是 是 是 一 是 是 是 一 是 是 是 一 是 是 是 一 是 是 一 是 一 是 是 一 是 是 一 是 是 一 是 是 一 是 是 一 是 是 一 是 是 一 是 一 是 是 一 是 是 一 是 是 是 一 是 是 一 是 是 一 是 是 一 是 是 一 是 一 是 是 一 是 一 是 一 是 一 是 一 是 一 是 一 是 一 是 一 是 一 一 是 二 一 是 一 是 一 是 一 一 是 一 是 一 是 一 是 一 一 一 是 一 一 一 一 一 一 一 一 一 一 一 一 一	Microsoft Authenticode(th) R Microsoft Root Authority Microsoft Root Certificate Aut Microsoft Root Certificate Aut Microsoft Root Certificate Aut NO LIABILITY ACCEPTED, (c)9. ROOTCA/4096	<ul> <li>Microsoft Authenticode(tm) Ro, Microsoft Root Authority</li> <li>Microsoft Root Certificate Auth</li> <li>Microsoft Root Certificate Auth</li> <li>Microsoft Root Certificate Auth</li> <li>NO LIABILITY ACCEPTED, (c)97 ROOTCA/4096 Thawte Timestamping CA</li> </ul>	2000/ 2020/ 2021/ 2035/ 2036/ 2004/ 2033/ 2021/	其他動作	
		<		5		

- 檢查中繼憑證授權單位中是否有 GRCA 的自發憑證(到期日為 2032/12/5),若有請刪除。
- 6. 請至下列網址下載2張自發憑證

第1張 GRCA 自發憑證(GRCA1 簽 GRCA1.5) http://grca.nat.gov.tw/repository/Certs/GRCA1\_to\_GRCA1\_5.cer 第2張 GRCA 自發憑證(GRCA1.5 簽 GRCA2) http://grca.nat.gov.tw/repository/Certs/GRCA1\_5\_to\_GRCA2.cer

7. 匯入第1張 GRCA 自發憑證。在「中繼憑證授權單位」下的「憑

	贬 运祥 川有工作				
	主控台1 - [主控台根日錄)馮諮	(木櫟雪腦)\中繼馮諮授權單位	\馮諮1	_	D X
			(vec am ]		
猫菜(F) 動作(A)	磁((V) 我的販変(O) 倪鹼(W) 訊9	9(H)			- 18   ×
🗢 🔿 🙋 🖬 🗉					
🧰 主控台根目錄	● 一般	簽發者	到期E	動作	
⊿ 🗊 憑證 (本機電腦)	) 🔄 Microsoft Windows Hardware	. Microsoft Root Authority	2002/	馮諙	
▶ 🚞 個人	Root Agency	Root Agency	2040/	甘油香佐	
▲ 📄 受信任的根	<sup>您證</sup>    🔄 www.verisign.com/CPS Incorp	. Class 3 Public Primary Certificati	2016/	→ 把動作	•
■ 懲證 N ● 小業信任					
	權里				
□ □ □ □ ∞2202100	尚清耳				
▶ 🔛 受信任	所有工作(K) ・ 2種2	((1)			
▷ 🧰 沒有信	檢視(V) ►				
▶ 🚞 第三方	從這裡開啟新視窗(VV)				
	新工作台檢視(T)				
	生利定性(F)				
▶ 📔 信任的	進出清単(L)				
⊳ 🧰 Web ⊦	說明(H)				
< 111	> <		>		
包含可以在這個項目上調	执行的動作。			,	

證」按下右鍵,選擇「所有工作」→「匯入」。

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。	
下一步(N)	取消

	×
중 🔗 憑證匯入精靈	
要進入的檔案	
指在2018要進入的相樂。	
檔案名稱(口):	
D:\GRCA1_to_GRCA1_5.cer	瀏覽(R)
法本 海南间路路回河路田间下站路望安排车间,回望去去	
注意: 您可以將數個您證用以下的格式存放在问一個個案中:	
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
	5.0.7

중 🥩 憑證匯入精靈	X
<b>憑證存放區</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。	
○ 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: 中繼憑證授權單位	测链(R)
	/到見(∩)
	下一步(N) 取消
중 🦻 憑證匯入精靈	X
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:  使用考理取的馮謅之故區 中提馮證授權單位	
檔案名稱 D:\GRCA1_to_GRCA1_5.cer	
	]
	<u> </u>

8. 匯入第2張自發憑證。在「中繼憑證授權」下的「憑證」按下右

鍵,選擇「所有工作」→「匯入」。

<b>-</b>	主控台1 - [主控台根目錄\憑證	(本機電腦)\中繼憑證授權單位	∖憑證]	_ 🗆 🗙
🚟 檔案(F) 動作(A) 檢	≷視(V) 我的最愛(O) 視窗(W) 說明	i(H)		_ & ×
🗢 🔿 🖄 🖬 📋	Q 🔒 🛿 🖬			
主控台根目錄	● 一	簽發者	到期E	動作
⊿ ♀️ 忽證 (平徳电順)	Microsoft Windows Hardware	Microsoft Root Authority	2002/	憑證 ▲
▶ 🔜 個八	Root Agency	Root Agency	2040/	其他動作 ▶
	www.verisign.com/CPS Incorp	Class 3 Public Primary Certificati	2016/	
▶ 🖀 企業信任				
⊿ 📔 中繼憑證授權單	L.			
	B			
	有工1F(K)	.(1)		
▶ 📔 沒有信 🛛 檢	視(V)			
▶ 📔 第三方 🛛 從	這裡開啟新視窗(W)			
▶ 📔 受信任	工作会檢損(T)			
	新整理(F)			
	出清單(L)			
	明(H)			
< III >	< III		>	
包含可以在這個項目上執行	的動作。			

依照上述匯入第1張 GRCA 自發憑證的步驟, 匯入第2張自發憑

證。

(人) 🖕 准認庭 ) 結示	X
♥ ☞ 漆磁進八病蓋	
要匯入的檔案 指定您想要匯入的檔案。	
檔案名稱(F): D:\GRCA1_5_to_GRCA2.cer	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

# 匯入完成後的中繼授權單位只會有下圖中的3張憑證。

<b>a</b>	主控台1 - [主控台根目錄	\憑證 (本機電腦)\中繼憑證授權	輩單位\憑證]		- • ×
🚟 檔案(F) 動作(A) 檢視(V) 我的	5最愛(O) 視窗(W) 說明(H)				_ & ×
🗢 🧼 🙇 📰 📋 🙆 🔒 👔					
●         ●	建築(の) 税差(W) 証何(f) 可 登録 本 に Government Root Certification Authority. に Government Root Certification Authority. に Government Root Certification Authority. に 同ののの ののの ののの ののの ののの ののの ののの	家設書               Government Root Certification             Government Root Certification             Microsoft Root Authority             Root Agency             Class 3 Public Primary Certificati             Government Root Certification	<ul> <li>到明日 使用</li> <li>2020/7/19 &lt;全</li> <li>2020/7/19 &lt;全</li> <li>2020/7/19 &lt;</li> <li>2002/12/31 </li> <li>2016/10/25 伺服</li> <li>2013/1/31 &lt;</li> </ul>	H目的 動作 悪部> 調み 構造 其他動作 部 系 器 新 N 器 動能 第 一 一 一 一 一 一 一 一 一 一 一 一 一	, p
	<				

9. 請重新繫結(Binding),進入編輯站台繫結後,請先選擇「未選

取」	,之後再選	原本的	SSL	憑證並按確定	0
----	-------	-----	-----	--------	---

10. 若重新繫結後依然沒有更新為5層憑證串鍊,請將主機重開機。

### (三)網站伺服器: Apache

請至 GCA 網站下載已經製作好的憑證串鏈檔案,格式為 PEM 編
 碼,下載網址為

http://gca.nat.gov.tw/download/GRCA1\_5\_GCA2.zip •

- 2. 將下載的GRCA1\_5\_GCA2.zip解壓縮得到GRCA1\_5\_GCA2.crt。
- 3. 若 Apache 版本 < 2.4.8, 請參考以下步驟操作
  - (1)將GRCA1\_5\_GCA2.crt放置於Apache Server存放憑證的目錄
     中,舊的憑證串鍊檔案(NewWithOld\_GCA2.crt)可刪除。
  - (2)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
     SSLCertificateChainFile:GRCA1\_5\_GCA2.crt 檔案路徑。
  - (3) 若在 httpd-ssl.conf 找不到 SSLCertificateChainFile 參數,則 請確認私密金鑰檔案路徑設定的 conf 檔案為何(ex: httpd.conf, httpd-vhosts.conf),此參數會與私密金鑰放在同一設定檔中。
- 4. 若 Apache 版本 >= 2.4.8, 請參考以下步驟操作
  - (1) 將 GRCA1\_5\_GCA2.crt 使用文字編輯軟體開啟,複製全部的 內容。
  - (2) 用文字编輯軟體開啟目前已經安裝的網站 SSL 憑證,檔案路

徑為 SSLCertificateFile 參數指定之位址,以下為範例。

SSLCertificateFile "/export/httpd-2. /certs/gca server.crt" SSLCertificateKeyFile "/export/httpd-2. /certs/gca server.key"

(3) 在開啟之 SSL 憑證檔案最後面間隔一空白行,貼上步驟(1)複

製的憑證串鍊內容,可參考下圖。

1 ----BEGIN CERTIFICATE----MIIFNzCCBB+gAwIBAgIQboDPTayQ/0nvVYN0jC89TzANBgkqhkiG9w0BAQsFADBE 2 3 MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQLDBjmlL/1 upzmhpHorYnnrgHnkIbkuK31v4MwHhcNMTUwNjI2MDcyOTEzWhcNMTgwNjI2MDcy 4 OTEzWjB4MQswCQYDVQQGEwJUVzESMBAGA1UECgwJ6KGM5pS/6ZmiMSEwHwYDVQQL 5 6 DBjmlL/lupzmhpHorYnnrqHnkIbkuK31v4MxFzAVBgNVBAMTDmdjYS5uYXQuZ292 7 LnR3MRkwFwYDVQQFExAwMDAwMDAwMDEwMDI00TMxMIIBIjANBgkqhkiG9w0BAQEF 8 AAOCAQ8AMIIBCgKCAQEA36nu2MtLzMzB10f71CqnV2VC/qpwk8Yh/nbYXJ/KCkB0 9 raDPxAD5IjJYHkAR5RcwkbdCEXyEylfsBmoqikpT8NLRJQZKBmc0cciltIeFRZWX 10 ymNhEBkmMo3jhK2r/3o1WLIcnoAIrSifLBC0TAR3xjzHQ1xIG4/FkC89APo0PZNR 11 Beo8h67YSqnGbSA/1fG/KCKCc3dbzKi4PADffrvUzmpIvIsm1MTxo028TT/BkrP2 LpxLr8p6+fc7s7b7mcr1nLBLETGAT+/tGIn+v1T14DnrK/0kbjUiyTl0kr1q8bY0 12 13 Vc4Znr7+1f8Vt6jYlBFDEdr5SJBIZD/cMgjUChTzrwIDAQABo4IB7zCCAeswHwYD 14 VR0jBBgwFoAU0Rhnw1f+EpqRa19fMeo+woSH+70wHQYDVR00BBYEFIF1LP61DPXX 15 psjH64JagS2rR1ZZMIGYBggrBgEFBQcBAQSBizCBiDBFBggrBgEFBQcwAoY5aHR0 16 cDovL2djYS5uYXQuZ292LnR3L3J1cG9zaXRvcnkvQ2VydHMvSXNzdWVkVG9UaG1z 17 Q0EucDdiMD8GCCsGAQUFBzABhjNodHRwOi8vZ2NhLm5hdC5nb3YudHcvY2dpLWJp 18 bi9PQ1NQMi9vY3NwX3NlcnZlci5leGUwDgYDVR0PAQH/BAQDAgWgMBQGA1UdIAQN 19 MAswCQYHYIZ2ZQADAzAZBgNVHREEEjAQgg5nY2EubmF0Lmdvdi50dzAgBgNVHQkE GTAXMBUGB2CGdgFkAgExCgYIYIZ2AWQDAwEwgYgGA1UdHwSBgDB+MD2gO6A5hjdo 20 21 dHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9yeS9HQ0E0L0NSTDIvQ1JMXzAw 22 MDEuY3JsMD2q06A5hjdodHRwOi8vZ2NhLm5hdC5nb3YudHcvcmVwb3NpdG9veS9H 23 Q0E0L0NSTDIvY29tcGxldGUuY3JsMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggr 24 BgEFBQcDAjANBgkqhkiG9w0BAQsFAAOCAQEAs71WC1KbhEmLBKu5HmUpHARv51Va 25 rGusMOPN1BiKwLnfIP9WgcEzwInHdlC8YYEzWYM5K6qagP1spWhzA4rGIg4660Z0 26 z91Sk6sqE1hhYza/BnY1pvz63y8XjCUAOw0WWpbKpCJWGeuTg7FaN2ZpQs4POMbU 27 36aernb1KLTIF0QUFmfklmUiHNKe3+g03xTINzyZ+1JCRtk6frG1Cyqq07h0d2Zc 28 iHgCOkChSiqpSJL5/42d15yYc/W9eU4gFfSdvC0f10Hb8cCspbmtTI6RWnU5UoY8 29 aJofnhLb1x/k8GwgizPvQk7axg0FaU7WYkvb9a9nFbNUPGdTw4v2+aQ0iA== 30 ----END CERTIFICATE-----31 與END CERTIFICATE間隔一空白行,貼上複製的憑證串鍊內容

(4) 貼上後之檔案範例如下圖。



(5) 將修改後的 SSL 憑證檔案存檔,檔案放置路徑跟原本

SSLCertificateFile 參數相同,此SSL 檔案經由修改已經包含

憑證串鍊。

(6) 檢查 conf 檔案中是否有 SSLCertificateChainFile 參數, 若有

請註解該行(前方加上#)。

5. 重新啟動 Apache Server。

#### (四)網站伺服器:Tomcat

下列步驟兩個%中間之路徑或名稱,請依照實際主機環境進行調整。

- 請先將原本的 keystore 檔案備份,避免之後操作錯誤造成私密金 鑰遺失。
- 2. 打斷原本 keystore 中之憑證串鍊,步驟如下。
  - (1) 將 keystore 轉換為 pfx 檔案

keytool -importkeystore -srckeystore %keystoreFile% -destkeystore %pfxFile% -srcstoretype jks -deststoretype PKCS12 -srcalias %aliasName% -destalias %aliasName%

(2) 從 pfx 檔案中分離私密金鑰(.key)

openssl pkcs12 -in %pfxFile% -nocerts -nodes -out %server.key%

(3) 利用私密金鑰產生 CSR 檔案

openssl req -new -key % server.key% -out % server.csr%

(4) 利用 OpenSSL 與私密金鑰產生自簽憑證

openssl x509 -req -days 7305 -sha1 -extfile openssl.cfg -extensions v3\_ca -signkey %server.key% -in %server.csr% -out %server.cer%

(5) 將自簽憑證匯入原本的 Keystore 中,以打斷原本的憑證串鍊

keytool -import -keystore %keystoreFile% -alias %private key entry% -file %server.cer%

- 3. 刪除 keystore 內之前已匯入的 GRCA 及 GCA 憑證。
  - (1) 在 %JAVA\_HOME%\bin 目錄下執行

keytool -list -keystore %keystoreFile%

(2) 待出現 Enter keystore password: 請輸入密碼

(3) 將除了 PrivateKeyEntry 之外的項目都刪除(下列指令以下圖

為例,實際 alias 名稱請依據畫面顯示輸入)

keytool -delete -alias new\_with\_old -keystore %keystoreFile% keytool -delete -alias grca -keystore %keystoreFile% keytool -delete -alias gca2 -keystore %keystoreFile%



(4) 待出現 Enter keystore password: 請輸入密碼

4. 請至下列網址下載4張憑證:

GRCA1 自簽憑證

http://grca.nat.gov.tw/repository/Certs/GRCA.cer

GRCA 自發憑證(GRCA1 簽 GRCA1.5)

http://grca.nat.gov.tw/repository/Certs/GRCA1\_to\_GRCA1\_5.cer

GRCA 自發憑證(GRCA1.5 簽 GRCA2)

http://grca.nat.gov.tw/repository/Certs/GRCA1\_5\_to\_GRCA2.cer

GCA2 自簽憑證

http://gca.nat.gov.tw/repository/Certs/GCA2.cer

5. 依照下列步驟重新匯入新憑證串鍊。

### 安裝 GRCA 憑證(共3張)

(1) 在 %JAVA\_HOME%\bin 目錄下執行

keytool -import -alias grca -file D:\GRCA.cer -keystore %keystoreFile% keytool -import -alias grca2 -file D:\GRCA1\_to\_GRCA1\_5.cer -keystore %keystoreFile% keytool -import -alias grca3 -file D:\GRCA1\_5\_to\_GRCA2.cer -keystore %keystoreFile%

- (2) 待出現 Enter keystore password: 請輸入密碼
- (3) 若出現 Trust this certificate: 請翰 y

#### 安裝 GCA 憑證(共1張)

(1) 在 %JAVA\_HOME%\bin 目錄下執行

keytool -import -alias gca2 -file D:\GCA2.cer -keystore %keystoreFile%

- (2) 待出現 Enter keystore password: 請輸入密碼
- 6. 確認 PrivateKeyEntry 的 alias name。
  - 在 %JAVA\_HOME%\bin 目錄下執行 keytool -list -keystore %keystoreFile%
  - (2) 待出現 Enter keystore password: 請輸入密碼
  - (3) 找到 PrivateKeyEntry 對應的 alias name, 下圖範例為 tomcat



- 7. 匯入 SSL 伺服器應用軟體憑證。
  - (1) 在 %JAVA\_HOME% \bin 目錄下執行

keytool -import -alias %PrivateKeyEntry 的 alias name% -file

%SSL 憑證檔案所在路徑% -keystore %keystoreFile%

- (2) 待出現 Enter keystore password: 請輸入密碼
- 8. 將 Tomcat 重新啟動。

### 三、憑證串鍊檢測方式

1. 可連線到 SSL Checker 網站

(https://www.sslshopper.com/ssl-checker.html)進行憑證串鍊檢

測。

2. 正確的憑證串鍊檢測結果會類似下方截圖。



### 若憑證串鍊有錯誤,則會有紅色斷鍊,如下圖

![](_page_32_Picture_1.jpeg)

- 3. GCA SSL 5 層憑證串鍊為 GRCA1 -> GRCA1\_to\_GRCA1\_5 -> GRCA1\_5\_to\_GRCA2 -> GCA2 -> SSL,其中GRCA1為根憑證, 針對根憑證的部分,瀏覽器會自行參考自己的憑證信賴清單決定 是否信任,因此根憑證並不是 SSL 協定必須傳送的項目,故會 因為不同的檢測網站或軟體而有顯示與不顯示根憑證的差異,若 檢測結果只出現4層串鍊亦為正常現象,只要 Firefox 與 Android 手機能正常連線貴單位網站,即代表憑證串鍊安裝正確。
- 4. 亦可使用 Firefox 進行確認,詳細步驟如下

![](_page_33_Picture_0.jpeg)

![](_page_33_Figure_1.jpeg)

頁面資訊 - https://gca.nat.gov.tw/web2/index.h	ntml			
→      →				
網站: gca.nat.gov.tw				
擁有者: 這個網站沒有提供擁有者資訊。				
驗證機構: 行政院		檢視憑證 (⊻)		
隱私及歷史記錄				
我以前瀏覽過這個網站嗎?	是,來過 29 次			
此網站有在我的電腦中儲存資訊 (Cookie) 嗎 ?	否	檢視 Cookie ( <u>K</u> )		
我有在此網站儲存任何密碼嗎?	否	檢視已存密碼 (W)		
技術細節				
連線己加密(TLS_RSA_WITH_AES_128_CBC_S	HA、128 位元金鑰、TLS 1.2)			
您正在瀏覽的網頁在傳送前有經過加密。				
加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊,所以此頁面在網路上傳輸時很難會有 人看到內容。				
		說明		

δ證檢視器:「gca.nat.gov.tw」		
一般 (G) 詳細資訊 (D)		
徳證 暦級 (H)		
Taiwan GRCA	^	
Government Root Certification Authority - GL5	E	
a 政府運搬等理由心		
◎ 微證欄(位(上))		
d gca.nat.gov.tw	î	
	E	
(水本) (市時)		
不早於	-	
┃		
匯出 (公		