中華電信通用憑證管理中心 (PublicCA)

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

Windows IIS 8.0 SSL 憑證請求檔製作手冊

ー、 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。

	V	Internet Information Servi认s (IIS) 管理員	_ 0 ×
# 進代() 設現(+) # 進代() 設現(+) # 進代() 設現(+) # 進代() 設用(-) # 進代() 設用(-) # 進代() ご () # 進代() # 進代() ご () # 進代() ご	€ S WIN-8IHG1LIL8	C6 >	🕶 🛛 🔓 🕡 🕶
日本 WIN-88HG1LL8C6 首頁 ● 登班編集 ● 修正 ● 登田電式集集 ● 修正 ● 登田電式集集 ● 修正 ● 登 常星 ● 修正 ● 登 常星 ● 修正 ● 第 ● ● ● ● 第 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	檔案(F) 檢視(V) 說明(H)		
	福雲(F) 檢視(V) 說明(H) 建築 ④ · □ 1 ● ● ● · □ 1 ● ● ● · □ 1 ● ● ● · □ 1 ● ● ● · □ ● □ ● ● · □ ● □ ● ● · □ ● □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ □ ● ● · □ ● <p< th=""><th></th><th>動作 管理伺服器 ◆ 重新設動 ● 設動 ● 停止 按視應用程式集區 按視應用程式集區 接視站台 ● 取得新的網頁平台元件 ● 説明 線上說明 #上說明</th></p<>		動作 管理伺服器 ◆ 重新設動 ● 設動 ● 停止 按視應用程式集區 按視應用程式集區 接視站台 ● 取得新的網頁平台元件 ● 説明 線上說明 #上說明
	★ # # # # # # # # # # # # # # # # # # #		G E

三、 點選「建立憑證要求」

2	Inte	rnet Information Services	(IIS) 管理員		_ 0 ×
WIN-8IHG1LIL80	26 🕨				😉 🛛 🟠 I 🕑 🗸
檔案(F) 檢視(V) 說明(H)					
檔案(E) 檢視(公) 說明(H) 連續 ④, - [] (二) (多, →] 起始術頁 → [] 一句 起始術頁 → [] 一句 起始/頁 → [] 一句 近台 → [] 一句 近台 → [] Default Web Site	● 印服器憑證 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 ▼ 移至(⑤) ~ √ 全部顯示(Δ) 發行給	使用的憑證。 群組依據 沒有分組 • 發行者	到期日	M作 運入 建立意趣要求 現或意理要求 建立自我簽署應證 説明 線上說明
< <u>Ⅲ</u> >」 就結	< 回 功能檢視 💦 内容檢視	11		>	43

四、 輸入以下所有欄位資料,輸入完成後請點選「下一步」

	要求憑證	? X
分辨名稱屬性 (二)		
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,而且不能包含縮寫。	
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)	取消

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。請注意依照國際密碼學趨勢,請使用 RSA 2048 位元(含)以上金鑰長度。

要求憑證	? X
密碼編譯服務提供者內容	
選取率碼編譯服務提供者及位元長度。加密金銷的位元長度會決定憑證的加密強度。位元長 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):	度越大,安全性就
上一步(P) 下一步(N) 完	3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」。
此時憑證請求檔製作完成,使用憑證請求檔至中華電信通用憑證管理中心申

請SSL憑證。

要求憑證	? X
檔案名稱	
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。	
指正态超要次的储装否确(K): C:\certreq.txt	
	取消
	n//m

七、此時憑證請求檔(certreq.txt)製作完成,使用憑證請求檔至中華電信 通用憑證管理中心網站(http://publicca.hinet.net/)依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者,請從企業入口網站 電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

Windows IIS 8.0 SSL 憑證安裝操作手冊

- 一、 下載憑證串鏈,包含3張憑證,分別是(1)eCA 根憑證(ePKI Root CA 憑證,也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證 (中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺 服器憑證,可採以下兩種方式之一取得:
 - 您若是本公司之客戶,技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮 檔,解壓縮後包括3個檔案,分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.crt)與用 戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成,此為憑證序號)。 若是中華電信之所屬單位,於經審驗核准申請之電子表單的資訊表單 「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方,可以下載憑證 串鏈壓縮檔,解壓縮後可以取得憑證串鏈3個檔案。
 - 從網站查詢與下載:
 eCA 憑證:

http://epki.com.tw/download/ROOTeCA_64.crt

PublicCA G2 憑證: <u>http://epki.com.tw/download/PublicCA2_64.crt</u> SSL 憑證下載:您若是本公司之客戶,請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」,進行 SSL 憑證下載。 若您是中華電信之員工,負責管理單位之伺服器,請至 http://chtra.cht.com.tw/ 點選「憑證與卡片作業」,再點選「憑證查 詢」,下載 SSL 憑證。

- 二、 有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節,請參閱問與 答之金鑰長度與演算法(https://publicca.hinet.net/SSL-08-06.htm)
- 三、 開啟「Internet Information Services (IIS)管理員」。

8	Internet Information Servi 🛵 (IIS) 管理員	_ 0 ×
🕞 🕥 🥞 🛉 WIN-8IHG1LIL	306 •	
檔案(F) 檢視(V) 說明(H)		
福案(F) 檢視(V) 說明(H) 遵總 ④ ● 圖 創創 後。 ● 题始振頁 ④ ● WIN-8iHG1LL8C6 (WIN-8iF) ● 適 始台	WIN-8IHG1LIL8C6 首頁 #選號	動作 管理伺服器 重新設動 取動 停止 被視意用程式集區 技視站会 取得新的網頁平台元件 2 取得新的網頁平台元件 2 設用 線上說明
< III >	□ 功能檢視 🜊 內害檢視	
就緒		•

四、 點選主機連線預設名稱,再點選畫面右邊「伺服器憑證」。

🛐 Internet Information Servid is (IIS) 管理員	_ 0 ×
Image: State of the state o	🛂 🖂 🟠 🔞 🗸
榴寗(F) 檢視(V) 說明(H)	
	動作 管理伺服器 重新設動 原則 停止 被視應用程式集區 被視應用程式集區 機械站台 取得新的網頁平台元件 説明 線上說明
就緒	6=

五、 點選「完成憑證要求」。

8	Internet Information Services (IIS) 管理員	_ 🗗 X
€ S WIN-8IHG1LIL8	C6 •	🔤 🖾 🟠 🔞 🔻
檔案(E) 檢視(V) 說明(H)		
連線 ②	 ● 同服器憑證 此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站指配使用的憑證。 ● ● 修至(⑤) ● ● 全部顯示(△) ● 詳細依據: 沒有分组 ● 名稱 ● 發行給 發行者 到期日 	動作 僅人 建立香證要求 完成潘證要求 建立網域潘證 建立目気簽署憑證 ② 説明 線上説明
	< III)	
< III >	THE NUMERAL OF A DECEMBER OF A	6 =
阮緒		*

六、如下圖,選擇存放由中華電信通用憑證管理中心所簽發之 SSL 憑證的位置,並輸入好記名稱(一般填寫 Domain Name)。

完成憑證要求	?	х	
指定憑證授權單位回應			
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。 合有憑證授權單位回產的檔案名稱(R): C:\Users\Administrator\Desktop\certreq.cer … 好記的名稱(M): www.test.com.tw 選取新憑證的憑證儲存區(S): 個人			
確定	取消		

七、 步驟4按「確定」,出現完成憑證要求的畫面。

V]	Internet Information Services (IIS) 管理員	_ _ ×
WIN-8IHG1LIL8	C6 🕨	ど 🐼 🚱 🗸
檔案(E) 檢視(V) 說明(H)		
連線 ● ● ● 記始網頁 ● ● WIN-8IHG1LL8C6 (WIN-8IH ● @ 應用程式集區 ▲ - ● 站台 ▷ • ● Default Web Site	● D R 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。	動作 運立憑證要求 完成憑證要求 建立自我蓋署憑證 建立自我蓋署憑證 檢視 運出 東新 ※ 移除 (2) 說明 線上說明
	🋅 功能檢視 🔁 內容檢視	6ª .
0%57E		*il .:

- 八、 接著要安裝 eCA 及 PublicCA 憑證。
 - 請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。

	系統管理員: Windows PowerShell	
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	dministratory mmc	
	a 主控台1 - [主控台根目錄]	
c	🬇 檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)	_ # ×
	☐ 主控台根目錄 名稱	動作
	這個檢視沒有項目可顯示。	主控台根目錄 ▲
۲.		其他動作 ▶
微軟新注音 半		
		Windows Server 2012 Sta Build
L(D) 🗃 🙆 🐧 📮	▲ 😼 🕼 🌜 英 斗 1 2013/

九、 選擇「新增/移除嵌入式管理單元」。

					主控	台1 -	·[主控台根目錄]	_ D X
	檔案	(F) 動作(A)	檢視(V)	我的最愛(O)	視窗(W)	說明	1(H)	_ & ×
4		開新檔案(N)			Ctrl+	N		
		開啟(O)			Ctrl+	0		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)				_		其他動作 ▶
	\leq	新增/移除嵌 <i>入</i>	、式管理單分	τ(M)	Ctrl+	М	>	
	_	選填(P)						
		1 C:\Window	s\system3	2\compmgmt				
		結束(X)						
開創	一個	現存的主控台	•					,

十、 接著點選「憑證」→「新增」。

嵌入式管理單元	廠商 ^ Microsoft Corp	×	📓 主控台根目錄	編輯延伸(X)			
。服務	Microsoft Corp			移除(R)			
∬ 原則結果組	Microsoft Corp						
120 效能監視器	Microsoft Corp			- 緑石の			
20 授權管理員	Microsoft Corp			上修(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) >	D				
²¹ 資料夾	Microsoft Corp	\sim	ſ				
9 路由及遠端存取	Microsoft Corp						
■ 電腦管理	Microsoft Corp						
電話語音	Microsoft Corp						
2 磁碟管理	Microsoft 與 V						
12] 網北連結	Microsoft Corp						
al <mark>憑證</mark>	Microsoft Corp	-		進階(V)			
★ Machine Coopen ↓ 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。							

	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 ○ 我的使用者帳戶(M) ○ 服務帳戶(S) ④ 電腦帳戶(C)	帳戶的憑證:	
	< 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 □ 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 ○ 另一台電腦(A): □ 當電腦從命令列啟動時,可以	電腦。 1腦)(L): 瀏覽(R) 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)]

最後按下「確定」。

▶ 具有進階安全性的 Win… 服務	Microsoft Corp		同 馮證 (木櫟雷際)	
▲服務 了 医即4+ 用 4日	Microsoft Corr			
P (F B)(4+ FB 40	microsoft corp			移除(R)
」「尽則結米祖	Microsoft Corp			
〕 效能監視器	Microsoft Corp			上较小小
■授權管理員	Microsoft Corp			上核(0)
] 群組原則物件編輯器	Microsoft Corp			下移(D)
副裝置管理員	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			
劉網址連結	Microsoft Corp			
- 憑證	Microsoft Corp	-		進階(V)

十一、 先匯入根憑證。在「信任的根憑證授權」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)\受信任的根憑證授權單	〖位\憑證] 🛛 🗕 🗖 🗙
福案(F) 動作(A) 檢視(V) 我的最爱(O) 視察 ◆ ➡ 2 記 自 Q → 2 記	5(\V) 說明(H)	_ <i>E</i> ×
▲ □ 通信 日 日 日 ● □ 個人 □ Class 3 Public Primar ▲ □ 受信任的根憑證 □ Class 3 Public Primar □ ○ ○ ○ ● □ 受信 ○ ○ ● □ 中 ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● □ ● ● ● ● ● ● <	登録者 y Certific Class 3 Public Primary Certificati y Certific Class 3 Public Primary Certificati licrosoft Copyright (c) 1997 Microsoft C 正 正 Microsoft Copyright (c) 1997 Microsoft C 正 不thenticode(tm) Ro Root Authority Microsoft Root Certificate Auth ficate Aut Microsoft Root Certificate Auth ROOTCA/4096 ROOTCA/4096 rg CA Thawte Timestamping CA	到期E 2028/ 2004/ 1999/ 2000/ 2020/ 2020/ 2021/ 2035/ 2036/ 2004/ 2033/ 2021/
包含可以在這個項目上執行的動作。		

十二、 依照下圖步驟匯入根憑證。

	x
◎ 🦻 憑證匯入精靈	
物油片中准改研】转录	
歡迎使用憑證進入補靈	
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。	
● 本機電腦(L)	
韩按 [下—牛] 维结。	
arg IX [1' 2/] Hearing *	
下一步(N) 取	溑
	x
📀 🔄 憑證匯入精靈	
要匯入的檔案	
指定您想要匯入的檔案。	
提 定 会研旧!	
C:\ROOTeCA_64.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)	
次) 了 经准想提安终于	
本八丁 <u>群////////////////////////////////////</u>	

《 本 准 裕 际 】 # 录	x
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。	
○ 自動根據憑證蘋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: 受信任的根憑證授權單位	
深入了解透證存放區	
下一步(N) 取	消
	x
④ 参 憑證匯入精靈	x
중 參 憑證匯入精靈	X
중 ● 憑證匯入精靈	X
중 委 憑證匯入精靈 定成憑證匯入精靈 按一下 [完成],即可匯入憑證。	X
 중 差 憑證匯入精靈 完成憑證匯入精靈 按-下[完成],即可匯入憑證・ 	X
중 夢 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圖 受信任的根憑證授權單位	X
 중 差 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 受信任的根憑證授權單位 內容 憑證 提定名經 	X
 ● 夢 憑證匯入精靈 定成憑證匯入精靈 按一下 [完成],即可匯入憑證。 您已指定下列設定: 使用看選取的憑證存放區 受信任的根憑證授權單位 內容 憑證 橫案名稱 C:\ROOTeCA_64.cer (只不知道:) 	X
 ● 源證匯入精靈 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: 使用者鑑取的憑證存放區 受信任的根憑證授權單位 內容 憑證 檔案名稱 C:\ROOTeCA_64.cer 	X
 ● 憑證匯入精盤 完成憑證匯入精盤 皮一下[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 受信任的根憑證授權單位 內容 憑證 檔案名稱 C:\ROOTeCA_64.cer 	X
 ● 源證匯入精靈 安広馮證歴入精靈 按一下[完成],即可匯入憑證 坡一下[完成],即可匯入憑證 悠辺 使用書選取的憑證存放區 受信任的根憑證授權單位 内容 憑證 欄裏名稱 C:\ROOTeCA_64.cer 	X
 ● 憑證 法證理入精盤 定成憑證 歴入精盤 按一下 [完成],即可匯入憑證。 吃已指定下列設定: 使用者聲取的憑證存放區 受信任的根憑證授權單位 內容 憑證 檔案名稱 C:\ROOTeCA_64.cer 	
 ● 法設置人精整 た成憑證匯入精整 按一下 (完成],即可匯入憑證 安信任的根憑證授權單位 內容	
 ● 振鶴匯人精盤	X
 ● 振台区入精盤 定成馮台区入精盤 皮市下(完成),即可匯入憑證・ 佐田指定下列設定: 使用音選取的憑證存放圖 受信任的根憑證授權單位 内容 憑證 福案名稱 C\ROOTeCA_64.cer 	X



十三、 匯入成功後,可以看到 eCA 的根憑證。

🚡 ±i	空台1 - [主控台根目錄\憑證 (本	機電腦)\受信任的根憑證授權單	월位∖慿	證] ×
 福案(F) 動作(A) 機能 ● ● 2 〒 & ● 主控台根目錄 △ □ 憑證 (本機電腦) ▷ □ 個人 △ □ 憑證 (本機電腦) ▷ □ 個人 ○ 宣信任的根憑證: ○ 公案信任 	R(V) 我的最愛(O) 視窗(W) 說明 文字 (A) 我的最愛(O) 視窗(W) 說明 文字 (A) 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和 和	成电加八文 III エリルズ 認由 文 作 4 (H) 登録者 Class 3 Public Primary Certificati Class 3 Public Primary Certificati Copyright (c) 1997 Microsoft C PKI Root Certification Authority	到期E 2028/ 2004/ 1999/ 2034/	■ 動作 憑證 私 其他動作 ● KI Root Certif ▲
 ▶ <u>①</u> 企業信任 ▶ <u>○</u> 中繼憑證授權單, ▶ <u>○</u> 受信信的就證 ▶ <u>○</u> 算三方根憑證 ▶ <u>○</u> 受信任的人 ▶ <u>○</u> 要信任的人 ▶ <u>○</u> 用戶端驗證茲發: ▶ <u>○</u> 想慧卡信任根目: ▶ <u>○</u> 信任的裝置 ▶ <u>○</u> Web Hosting 	Microsoft Authenticode(tm) R Microsoft Root Authority Microsoft Root Certificate Aut Microsoft Root Certificate Aut Microsoft Root Certificate Aut NO LIABILITY ACCEPTED, (c)9 ROOTCA/4096 Thawte Timestamping CA	Microsoft Authenticode(tm) Ro Microsoft Root Authority Microsoft Root Certificate Auth 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 →
受信任的根憑證授權單位 存於			>	

十四、 第二步,匯入中繼憑證。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)			_ & ×
🗢 🔿 🙍 📰 📋 🧟 😽 🚺 🥽				
□ 主控台根目錄 發給 ▲	簽發者	到期E	動作	
▲ 彙 憑證 (本機電腦) ▶ ■ 個人	ware Microsoft Root Authority	2002/	憑證	•
✓ I I I I I I I I I I I I I I I I I I I	corp Class 3 Public Primary Certificati	2040/	其他動作	•
▶ ■ 正未信は ⊿ 👕 中編憑證授權單				
── 憑證撤銷清旦				
○ 通道 所有工作(K)	匯入(1)			
▷ 2 2 1 C 2 2 7 C 2 7				
▷ III 第三方 從這裡開啟新視窗(W)				
▶ _ 受信仕 ▶ 😁 用戶端 新工作台檢視(T)				
▷ 🖸 憑證註 重新整理(F)				
▶ 🚰 智慧卡 匯出清單(L)				
▷				
包含可以在這個項目上執行的動作。				

依照上述匯入 eCA 根憑證的步驟,匯入 PublicCA G2 中繼憑證。

		x
중 🥭 憑證匯入精靈		
要匯入的檔案 指定您想要匯入的檔案。		
檔案名稱(F); C:\PublicCA2_64.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)		
深入了解 <u>憑證檔案格式</u>		
	下一步(N) 取》	肖

成功匯入後,可以看到 PublicCA G2 的中繼憑證。

-	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]	_ _ ×
🚟 檔案(F) 動作(A) 檢視(V)	我的最愛(O) 視窗(W) 說明(H)			_ & ×
🗢 🔿 🙋 🖬 🔏 🖬 🔰	🕻 🗊 🔒 🖬			
🧾 主控台根目錄	發給▲	簽發者	到期日	動作
⊿ 🗊 憑證 (本機電腦)	Microsoft Windows Hardware C	Microsoft Root Authority	2002/12/31	馮謟▲
▶	Public Certification Authority - G2	ePKI Root Certification Authority	2034/12/11	其他動作 ▶
☐ 憑證 ▶ ● ☆ 業信任	www.verisign.com/CPS Incorp.b	Class 3 Public Primary Certificati	2016/10/25	Public Certification 🔺
₽ == ±未信亡 ■ = 中継憑證授權單位 ■ 憑證撤銷清單 ■ 憑證				其他動作 ▶
 ▶ ²¹ 受信任的發行者 ▶ ²¹ 沒有信任的憑證 ▶ ²¹ 第三方根憑證授權單¹ 				
▶ 🧰 受信任的人 ▶ 🚰 受信任的人				
▶ 🧰 憑證註冊要求				
▶ III 信任的裝置 ▶ III Web Hosting				
< III >	< 111		>	
中繼憑證授權單位存放區包含4	個憑證。			

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)。

8]	Internet Information Services (IIS) 管理員	
WIN-8IHG1LIL	8C6 → 站台 → Default Web Site →	🖸 🛛 🔂 🕡 🕶
檔案(E) 檢視(V) 說明(H)		
建線 ● ▼ ■ 2 2 2 2 2 2 2 2 2 2	● Default Web Site 首頁 師選器: • ▼ 移至④ • IS • ▼ 移至⑤ • IS • ▼ 移至⑤ • HTTP 回應標 MIME 類型 SSL 設定 項 ● ● ●	動作 ● ▲ 編輯權限 ● ●
< <u>III</u> >	夏水町/温 記録 記録 選進市 3(5) 度 運 運 預設文件 模組 輸出快取處 理 通 運 通 夏 運	▶ 啟動 ● 停止 瀏覽網站 ● 瀏覽 *:80 (http) 進階設定 設定 限制 ♀ 說明 ♥
就緒		1 .:

			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)
						》管(B)
						12132 (9)
						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 馮瓚(P):		
www.test.com.tw	✓ 選取(L)	檢視(V) 取消

+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。 +七、 安裝 SSL 安全認證標章:

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文 的 SSL 安全認證標章安裝說明,將網站 SSL 安全認證標章安裝成功,網友可 瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁,參考從企業入口網站的電子表單之資 訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案 中的 SSLSealispec.txt,將網站 SSL 安全認證標章安裝成功。