中華電信通用憑證管理中心 (PublicCA)

Windows IIS 6.0 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,若因參考本說明文件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 6.0 SSL 憑證請求檔製作手冊	2
從未安裝過憑證的伺服器產生憑證請求檔操作步驟	2
已安裝過憑證的伺服器產生憑證請求檔操作步驟	10
Windows IIS 6.0 SSL 憑證安裝操作手冊	46
安裝根憑證(eCA)及中繼憑證(PublicCA)	46
從未安裝過憑證的伺服器,安裝憑證操作步驟	64
已安裝過憑證的伺服器,安裝憑證操作步驟	73
附件一:單一 IP 多網域憑證安裝步驟	91

Windows IIS 6.0 SSL 憑證請求檔製作手冊

從未安裝過憑證的伺服器產生憑證請求檔操作步驟

一、將「網際網路資訊服務(IIS)管理員」開啟。

				-9	[設定物的伺服器] 糕羹
我的電腦					[EXACASED] MIRE Framework 1 1 設定
				9 <u>66</u>	Microsoft NET Framework 1.1 at the
1 10 10 10 10 10 10 10 10 10 10 10 10 10				902 Alba	Microsoft NET Framework 1.1 相靈
- Total - Contract - C				9	1711年版初 の数学社会を考め
網路上的芳鄰				5	分配式幅柔系統
				9	本機安全性原則
				1	争件假視器
2				ୁ ଜନ୍ମ	服撈
資源回收筒		a de se		8	双能
		ä	HP Network Config Utility		授權
			Windows Card Space		終端機伺服器授權 (5)))((1))(1))
			Windows防火牆		終端機服務設定
Internet			工作列和 [開始] 功能表	ť	終端機服務管理員
Administrator		T	已儲存的使用者名稱和密碼	P	資料來源 (ODBC)
		3	日期和時間	2	路由及遠端存取
管理您的伺服器	👽 我的電腦		可攜式媒體裝置	8	電腦管理
		9	印表機和傳真	1	管理您的伺服器
高大 命令提示字元	控制台(C)	2	地區及語言選項	2	網路会載中簽署理員
_	■ 系統管理工具 ト		字型 🤇	1	網際網路資訊服務 (IIS) 管理員
○ Windows 檔案總管		2	目動更新		· · · · · · · · · · · · · · · · · · ·
~	○ 印衣(限和))等具			8	歩き受権単位
	2) 説明及支援(II)	-70	系統管理工具 ▶	5	
10 10 10 10 10 10 10 10 10 10 10 10 10 1		3	市油品兴致位相機 ▶		
Microsoft Baseline Security	▶ 搜尋(2)	*	授權		
🍯 Analyzer 2.2	🖅 執行(R)		排走的工作 ▶		
			新唱歌杨乐程式 *////FERD		
1000 1000年1月	👶 Windows安全性(W)	- 32 - 25	新唱健電		
			宿 <u>眠</u> 2011年1987年		
一個一彩炳儀服務管理員			資料火選項		
💦 網際網路資訊服務 (IIS) 管		() ()	遊戲控制器		
理員		100	電視選視		
		-	電話和數據機選項		
		-	新期167連線 メ回約24回02/28175		
「「「「「「「」」」」」		2	啊呀~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
WINIE AND .		33	前日		
	💋 登出(L) 🚺 關機(U)	0	\$P\$10次百訊版道 \$P\$10		
			雑金		
2		3	網小		

二、產生憑證請求檔

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

🐚 網際網路資訊服務 (IIS) 令	行建員			
🛐 檔案(F) 執行(A) 檢視(V) 視窗(W) 説明(H)			_ 8 ×
	a B. 12 m 12 i k	■ II		
	2 G 10 00 00 00 00	認徳		
□ 🗊 TRUSTPAY (本機電腦)	aspnet_client	1 001E	10000	
🖻 📁 應用程式集區	📄 iisstart_20030221.htm			
日 🔛 税股的抵抗	pagerror.gif			
+ / 約頁服務延伸	查看(E)			
F	開啓舊檔(0)			
	使用櫂限(1) 御師(10)			
_				
	皆町③)			
	呼血(L) 暫停(A)			
	新音(M) →			
	從這裡新增視窗(W)			
	重新命名(<u>M</u>)			
-	重新整理(F)			
	匯出清單(L)			
	內容(<u>R</u>)			
	說明(<u>H</u>)			
爲目前的選取項目開啓內容對語	5方塊。			

接著將頁面切到「目錄安全設定」頁面。

在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

預設的網站 內容 ? ×
HTTP 標頭 自訂錯誤 ASP NET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定
驗證及存取控制 格用匿名存取,並編輯這個資源的驗 證方法。
□ IP 位址及網域名稱限制
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
編輯①
安全通訊
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 「日服器憑證③…
核成功的言葉(⊻)
編輯(D)
確定 取消 雲用(益) 説明

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,以滑鼠按下「下一步」 按鈕,開始製作 Windows 2003 IIS 6.0 伺服器憑證請求檔。



接著畫面會到「伺服器憑證」視窗,以滑鼠點選「建立新憑證(C)」,接著 以滑鼠按下「下一步」按鈕。

IIS 憲證精畫	×
伺服器赛题 這些是指派憑證到網站的方法。	
 諸選取您想要用於此網站的方法: 建立新憑證(C)。 指派已有的憑證(A)。 從金鑰管理員備份檔案匯入憑證(O)。 從.pfx檔案匯入憑證(M) 	
○ 從遠端伺服器網站複製或移動憑證到此網站(型)	
<上一步图(下一步 四))	取消

接著畫面會到「延遲或立即要求」視窗,以滑鼠點選「準備要求,但稍後再 傳送(P)」,接著以滑鼠按下「下一步」按鈕。

IIS 憲諸憲 ×
延遅或立即要求 您可以先準備稍後才傳送的要求,或您可以立即傳送它。
您想要先準備稍後傳送的憑證要求,或您想要立即傳送要求到線上憑證授權?
• 準備要求,但於稍後傳送 [2]
C 立即傳送要求到線上德證授權(2)
<上一步B) 下一步M> 取消

接著畫面會到「名稱及安全設定」視窗,以滑鼠點選「名稱(M)」欄位後並 輸入網站名稱,接著以滑鼠點選「位元長度(H)」為「2048」bits 後,接著 以滑鼠按下「下一步」按鈕。

IIS 憲證精畫 🛛 🗙 🗙 🗙 🗙 🗙 🗙 🗙 🗙 🗙 🗙 🗶 🗶 🗶 🗶 🗶 🗶
名稱及安全設定 您的新憑證必須有名稱及特定的位元長度。
諸輸入新憑證名稱。它應是個容易參考且記憶的名稱。
名積40. publicca.hinet.net
加密金鑰的位元長度決定了憑證的加密金鑰強度。位元長度越大,安全性也就 越好。不過長度越大也會導致速度越慢。
位元長度(田): 2048
□ 諸選取此憑證的密碼編譯服務提供者(CSP)(P)
<上一步(B) 下一步(B)

接著畫面會到「公司資訊」視窗,以滑鼠點選「公司(0)」欄位後並輸入組 織名稱或公司名稱,接著以滑鼠點選「單位(U)」欄位後並輸入組織或公司 的單位名稱,接著以滑鼠按下「下一步」按鈕。

★ 計算 211
公司資訊 您的憑證中必須有您公司的資訊,這些資訊將用來區別您的及其他的公司。
諸選取或輸入您的公司名稱及單位。通常這是您公司及部門的正式名稱。
右需進一步資訊,諸與您證授權単位的網站聯絡。
公司(○): 中華電信股份有限公司數據通信分公司
單位(四).
<上一步(B) 下一步(B) 取消

接著畫面會到「您站台的一般名稱」視窗,以滑鼠點選「一般名稱(C)」欄 位後並輸入一般名稱(即站台的網址「Domain Name」),接著以滑鼠按下「下 一步」按鈕。

IIS 憲諸憲 III III III III III III III III III
您 網站的一 後名 稱 您的網站的一般名稱是一個完全符合規定的網域名稱。
諸為您的網站輸入一般名稱。若伺服器在網際網路上,諸用有效的 DNS 名稱。 若伺服器在近端內部網路上,您也許想用電腦的 NetBIOS 名稱。
如果變更一般名稱,您將需要取得新的憑證。
策名稱(C): publicca.hinet.net
<上一步(B) 下一步(B) 取消

接著畫面會到「地理資訊」視窗,接著以滑鼠點選「國家(地區)(C)」,以 滑鼠點選「TW(台灣)」,接著以滑鼠點選「州/省(S)」欄位後依照所在地輸 入正確的州/省名稱,如圖為輸入「空白」或輸入「臺灣省」亦可,接著以 滑鼠點選「城市/位置(L)」欄位後依照所在地輸入正確的城市名稱,如圖為 輸入「臺北市」,接著以滑鼠按下「下一步」按鈕。

III 憲語結畫	×
地理資訊 此憑證授權單位要求下列地理的資訊。	>
國家 (地區)(C): I₩ (台湾) 省/州 (S):	
▼ 城市位置(L):	
▲ 「「「「「「「「」」」 「「「」」 「「」」 「「」」 「「」」 「「」」	
必須剩人[目/刑]和[級印位],須為正式有機且不可召獲差。	
<u>《上一步图】[下一步(N)》]</u> 取消	

接著畫面會到「憑證要求檔案名稱」視窗,接著以滑鼠點選「檔案名稱(F)」 欄位後並輸入路徑及要存的檔案名稱。如下圖所示,通常都是依照如下圖之 預設值路徑及檔案名稱存放,接著以滑鼠按下「下一步」按鈕。

and a set of the set	×
憲證要求檔案名稱 將以您所指定檔名的文字檔案儲存您的憑證要求。	
諸輸入檔案名稱給憑證要求。	
和来在#E	瀏覽(R)
<u>〈上一步®) (下一;</u>	步(N) > 取消

接著畫面會到「要求的檔案摘要」視窗,檢視剛才各步驟所設定的值是否無

誤。如果沒有問題,接著以滑鼠按下「下一步」按鈕。

王 王 王 王 王 王 王
要求的檔案摘要 您已經選擇建立要求檔案。
若要建立下列要求,請按 [下一步]。
檔案名稱: c:\certreq.txt
您的要求包含下列資訊:
發給 好記的名稱 國家地區 城市 公司 單位 如 防 和 如 如 如 如 如 如 如 如 如 一 如 一 如 一 一 如 一 一 一 一 一 一 一 一 一 一 一 一 一
<上一步图(下一步图)) 取消

接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成結束製作憑證請求檔動作。



三、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。

		_		-9	殿定你的伺服哭! 烤索
我的電腦					Microsoft NET Engraved 1 1 25
				9 <u>72</u>	Microsoft NET Emmeuork 1.1 #=
				9 <u>6</u> 2	Microsoft NET Framework 1.1 相靈
- 30				9	元件版初 八教一社会安玄(法
網路上的芳鄰				-5 P	プ取み備系が続
				لو .	平侯女王任原则
					争件做祝辞
				% स्व	J版7分
資源回收筒		a des			22.112
		a	HP Network Config Utility	100 100	没程
			Windows Card Space	P	終端機伺服器授權 (1))))))))))))))))))))))))))))))))))))
		1	Windows防火牆		終端機服務設定
Internet			工作列和 [開始] 功能表	ť	終端機服務管理員
Administrator		33	已儲存的使用者名稱和密碼	ø	資料來源 (ODBC)
		3	日期和時間	9	路由及遠端存取
管理 管理 您的 伺服 異	😡 我的電腦		可攜式媒體裝置	9	電腦管理
		8	印表機和傳眞	1	管理您的伺服器
□□□ ☆☆根示字示	📝 控制台(C) 🌖 🔹 🕨	9	地區及語言選項	Ø	細胞負載平衡管理員
	◎滴 系統管理工具	i 🖾	字型 🤇	۹	網際網路資訊服務 (IIS) 管理員 🌙
C Hindows 按案编符		1	自動更新	Ø	速漏桌面
	🥥 印表機和傳眞	<u>X</u> 1	ज्य के में कि		憑證授權單位
(PPP)		-	系統管理工具	5	叢集系統管理員
記事本	∭ 就明友文援(Ⅱ)	5	帝 備 器 央 數 位 相 機	Τ	
	🔎 捜尋(8)	P	授權		
Analyzer 2.2		1	排定的工作		
	₹ <u></u> +¥(1) (<u>C</u>)	0	新增或移除程式		
💦 磁碟重組工具	④ Windows安全性(W)	*	新增硬體		
		Ö	滑鼠		
終端機服務管理員			資料夾選項		
		>	遊戲控制器		
🧊 網際網路資訊服務 (IIS) 管 理昌		-	電源選項		
		b	電話和數據機選項		
		E.	網路連線		
		ø	網際網路選項		
所有程式(2) ▶		1	語音		
		Ø,	聲音及音訊裝置		
	💋 登出し) 🔟 關機(1)) 👗	鍵盤		
▶ 開始 🙈 🔞		8	顯示		
		9.			

一、將「網際網路資訊服務(IIS)管理員」開啟。

二、將私密金鑰及憑證匯出備份。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

著 (211) 務課網路資訊服務 (115) 管	理員			_ 🗆 🗵
🐚 檔案 Œ 執行 (A) 檢視 (V) 視窗(₩) 説明(H)			_ 8 ×
← → 1 1 1 × 1 2) 🗟 😫 💵 💂 🕨 🗉	L II		
	注: ① ② ● ● ● <th>II</th> <th></th> <th></th>	II		
。 爲目前的選取項目開啓內容對話:	, 方塊。			

接著將頁面切到「目錄安全設定」頁面,在「目錄安全設定」頁面,以滑鼠按下「檢視憑證」按鈕。

預設的網站 內容 ? ×
HTTP標頭 自訂錯誤 ASP_NET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定
驗證及存取控制 啓用匿名存取,並編輯這個資源的驗 證方法。
- IP 位址及網域名稱限制
↓ 使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
編輯①
安全通訊
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 檢視憑證(V)
編輯(D)
確定 取消 套用(点) 説明

將目前線上金鑰及憑證進行備份。憑證視窗如下出現有「這個憑證有一個對

應的私密金鑰」,代表這張憑證的私密金鑰跟憑證皆有存在。接著切「詳細 資料」頁面,並點選「複製到檔案」按鈕。

潇潇				?	×
(般	憑證路徑			1
	🧱 憲證資言	Ą			
	這個憑證的使用	目目的如下:		-	
	• 確保遠端	電腦的識別			
	• 向遠端電	腦證明您的身分			
	登 給:	publicca.hinet.net			
	登 行者:	Public Certification Authority			
	有效期白	2013/12/22 31 2016/12/22			
	🌮 這個憑證有	i一個對應的私密金鑰。			
			發行者聲明(8)	
			確	Ê	

憲證		? ×
一般 詳細資料 過證路	徑	
願示(S): 「そ部、		
Weeking (Weeking)		
欄位	值	
	₩3	
	02 9d 11 81 c3 8b fe ad 7d 15	
	sha1RSA	
1 2 發行者	Public Certification Authority,	
	2013年12月22日 下午 05:12:06	
一 一 有效期到	2016年12月22日 下午 05:12:06	
三主體	publicca.hinet.net,政府網路處	-
	DOM 20040 TO:2-1	- 1
		_
		<u> </u>
	編輯內容(四) 🥻 [複製到檔案(C	<u>)</u>
		定
	NEE	~

接著出現「憑證匯出精靈」,「匯出私密金鑰」頁面選擇「是,匯出私密金 鑰」後,以滑鼠按下「下一步」按鈕。

憲證匯出精畫	×
匯出私密金鑰 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?	
 ○ 提,匯出私密金鑰(Y) ○ 否,不要匯出私密金鑰(Q) 	
	_
<上一步B) (下一步M)> 取消	

接著出現「匯出檔案格式」頁面,選擇「個人資訊交換 - PKCS #12

(.PFX)(P)」,並勾選「啓用加強保護(需要 IE 5.0 或 NT 4.0 SP4 以上的 版本)(E)」,接著以滑鼠按下「下一步」按鈕。



接著出現「密碼」頁面,輸入保護私密金鑰的密碼。請務必記住此密碼,到 時需要將金鑰刪除產製新金鑰後需要將原來私密金鑰及憑證匯回時,就要輸 入此密碼。輸入密碼完成後,接著以滑鼠按下「下一步」按鈕。

憲設匯出精霊	×
密碼 為了安全性,您必須使用密碼保護私密金鑰。	
輸入並確認密碼。 密碼(P):	
******** 確認密碼():	

<上一步⊕ 下一步 型> 取消	

接著出現「要匯出的檔案」頁面,點選「瀏覽」選擇存放位置,或直接在「檔

案名稱(F)」打上路徑及檔案名稱也可以。

憲證匯出精靈	×
要匯出的檔案 請指定您要匯出的檔案名稱	
檔案名稱(E): 	瀏覽(R)
	< 上一步 (B) 下一步 (D) > 取消

如果有按下「瀏覽」,則可選擇檔案路徑及輸入所要儲存的私密金鑰及憑證.pfx 檔檔名。輸入完成後,按下儲存後,接著會跳回「要匯出的檔案」 頁面,並於頁面上出現存放檔案路徑及檔案名稱。

另存新檔				? ×
儲存於①:	🞯 桌面	•	6 🖻 📂 🛙	
表最近的文件 () 点面 () 我的文件 () 我的文件 () 和 一 一 一 一 一 一 一 一 一 一 一 一 一	 □ 我的文件 □ 我的電腦 □ 網路上的芳鄰 □ 細路上的芳鄰 □ 3HD738888888.pfx 			
	檔名(N):publicca_Re	qBackup	•	儲存圖
	存檔類型(I): 個人資訊交	[换 (*.pfx)	•	

輸入完成後,接著以滑鼠按下「下一步」按鈕。

たまである。 「「「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、 「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」」では、「」
要 匯出的檔案 諸指定您要匯出的檔案名稱
檔案名稱④:
C:\Documents and Settings\Administrator\桌面\publicca_ReqBackup 瀏覽(R)
<上一步(L)下一步(L))> 取消

接著出現「完成憑證匯出精靈」頁面,按下「完成」以完成匯出私密金鑰及 憑證動作。

憲證匯出精靈		×
	完成憑證匯出精霊	
	您已經成功地完成憑證匯出精靈。	
	您已指定下列新設定:	
	檔案名稱 C:\Documents and Sett 運出金鑰 是 包含憑證路徑中的所有憑證 否 檔案格式 個人資訊交換 (*.pfx)	
	< 上一步(B) 完成 取消	-

如果匯出完成,會出現如下訊息「匯出成功」。

灧.	夏 匯出精靈	×
6	霍出成功。	
	確定	
		2

三、刪除原來的私密金鑰及憑證。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

(11) 利除網路資訊服務	管理員			
🐚 檔案(E) 執行(A) 檢討	見(V) 視窗(W) 說明(H)			_8×
⇐ ⇒ 🗈 💽 🗙 😭	0 🖻 😫 💷 💂	▶ ■ Ⅱ		
● TRUSTPAY (本機電路 ● 應用程式集區 ● 應用程式集區 ● 通過電台調整 ● 和資量部務延件	名(1) 2 3 2 3 2 3 2 3 2 3 2 3 3 2 3 <td></td> <td> 狀況</td> <td></td>		狀況	
爲目前的選取項目開啓內容對	話方塊。			

接著將頁面切到「目錄安全設定」頁面,在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

預設的網站內容 ? ×
HTTP 標頭 自訂錯誤 ASP-WET ASP-WET
驗證及存取控制 啓用匿名存取,並編輯這個資源的驗 證方法。
□ IP 位址及網域名稱限制
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
安全通訊
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 檢視憑證(Y)
編輯(D)
確定 取消 套用(益) 説明

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,按下「下一步」後, 開始刪除原來的私密金鑰及憑證。



接著出現「修改目前的憑證指派」頁面,選擇「移除目前的憑證」,接著按 下「下一步」。

	×
修改目前的憲證指派 目前安裝在此網站的憑證。	
您想要如何處理目前安裝的憑證?	
○ 更新目前的憑證(型)。	
● 移除目前的憑證 R) ● ●	
C 取代目前的應證(△)。	
○ 匯出目前的憑證到 .pfx 檔案(区)	
○ 複製或移動目前的憑證到遠端伺服器網站(C)	
<上一步@(下一步®)>	取消

接著出現「移除憑證」頁面,頁面上會顯示目前憑證的詳細資訊,請務必執 行之前的私密金鑰及憑證備份後,才可執行此步驟移除憑證,否則憑證一移 除,將無法救回,接著按下「下一步」。

IIS 憲證精靈		×
移除票證 您可以儲存此憑證且稍後在注	這個或其他伺服器重複使用此憑證。	
若要從您的伺服器移除此憑 憑證詳細資訊: 發給 發照者 到期日 使用目的 使記的名稱 國家,地區 公司 單位	證並將之儲存至稍後再使用,請按 [下一步]。 publicca.hinet.net Public Certification Authority 2016/12/22 伺服器驗證, 用戶端驗證 publicca.hinet.net TW 中華電信股份有限公司數據通信分公司 政府網路處	
	<上一步图 (下一步图)	取消

接著出現「正在完成網頁伺服器憑證精靈」頁面,按下「完成」以完成刪除

憑證動作。

IIS 憲證精靈	×
	正在完成網頁伺服器憑證精 靈
	您已經成功完成網頁伺服器憑證精靈。
	解除憑證安裝
	若要附加憑證在此電腦,諸再次啓動網頁伺服器憑證 精靈。然後,您可以建立新憑證或重複使用儲存的憑 證。
	請按 [完成] 來關閉此精靈。
	<上一步(B) 完成 取消

四、開始產製私密金鑰及憑證。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

🀚 網際網路資訊服務 (IIS) 管理	理員			
🐚 檔案EP 執行(A) 檢視(V)) 視窗(₩) 説明(出)			_ 8 ×
(= -> 🗈 💽 🗙 😭 🙆	🖹 🔮 🖬 💂 🕨 🛛	I II		
← → こ Ⅲ × ご •	注意 ② III □ ● 名額 ● ● ● ● ● ○ ● ● ● ● ○ ● ● ● ●	■ II 路径	狀況	
爲目前的選取項目開啓內容對話力	, 方塊。			

接著將頁面切到「目錄安全設定」頁面,在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

預設的網站 內容	? ×
HTTP 標頭 自訂錯誤 ASP NET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄3	全設定
驗證及存取控制 啓用匿名存取,並編輯這個資源的驗 證方法。 編輯 (E)	
IP 位址及網域名稱限制	
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。	
編輯(I)	
安全通訊	
當存取這個資源時使用安全通訊並啓 「伺服器應證[3] 用用戶端憑證。	
檢視憑證(♡)	
·····································	
確定 取消 套用(点)	說明

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,以滑鼠按下「下一步」 按鈕,開始製作 Windows 2003 IIS 6.0 伺服器憑證請求檔。



接著畫面會到「伺服器憑證」視窗,以滑鼠點選「建立新憑證」,接著以滑 鼠按下「下一步」按鈕。

IIS 憲證精畫 X
伺服器憲證 這些是指派憑證到網站的方法。
諸選取您想要用於此網站的方法: ○ 建立新馮锴(○)。
○ 從金鏞管理貝彌衍檔案匯入應證(U)。 ○ 從 .pfx 檔案匯入憑證(M)
○ 從遠端伺服器網站複製或移動憑證到此網站(型)

接著畫面會到「延遲或立即要求」視窗,以滑鼠點選「準備要求,但稍後再 傳送(P)」,接著以滑鼠按下「下一步」按鈕。

★ 211
延遅或立即要求 您可以先準備稍後才傳送的要求,或您可以立即傳送它。
您想要先準備稍後傳送的憑證要求,或您想要立即傳送要求到線上憑證授權?
 準備要求,但於稍後傳送① ① 立即傳送要求到線上憑證授權③
<上一步(B) (下一步(M) > 取消

接著畫面會到「名稱及安全設定」視窗,以滑鼠點選「名稱(M)」欄位後並 輸入網站名稱,接著以滑鼠點選「位元長度(H)」為「2048」bits 後,接著 以滑鼠按下「下一步」按鈕。

IIS 畫諸靈靈 III III III III III III III III III
名稱及安全設定 您的新憑證必須有名稱及特定的位元長度。
請輸入新憑證名稱。它應是個容易參考且記憶的名稱。 名稱AD
publicca.hinet.net
加密金鑰的位元長度決定了憑證的加密金鑰強度。位元長度越大,安全性也就 越好。不過長度越大也會導致速度越慢。
位元長度(田): 2048
□ 諸選取此憑證的密碼編譯服務提供者(CSP)(P)
<上一步(B) (下一步(M) > 取消

接著畫面會到「公司資訊」視窗,以滑鼠點選「公司(0)」欄位後並輸入組 織名稱或公司名稱,接著以滑鼠點選「單位(U)」欄位後並輸入組織或公司 的單位名稱,接著以滑鼠按下「下一步」按鈕。

IIS 憑證精畫 X
公司資訊 您的憑證中必須有您公司的資訊,這些資訊將用來區別您的及其他的公司。
諸選取或輸入您的公司名稱及單位。通常這是您公司及部門的正式名稱。
若需進一步資訊,諸與憑證授權單位的網站聯絡。
◇司②
政府網路處
<上一步图 下一步图 取消

接著畫面會到「您網站的一般名稱」視窗,以滑鼠點選「一般名稱(C)」欄 位後並輸入一般名稱(即網站的網址「Domain Name」),接著以滑鼠按下「下

一步」按鈕。

IIS 憲證精畫 X
您 網站的一 後名 稱 您的網站的一般名稱是一個完全符合規定的網域名稱。
諸為您的網站輸入一般名稱。若伺服器在網際網路上,諸用有效的 DNS 名稱。 若伺服器在近端內部網路上,您也許想用電腦的 NetBIOS 名稱。
如果變更一般名稱,您將需要取得新的憑證。
一般名新(2):
publicca.hinet.net
<上一步 B(下一步 D) 取消

接著畫面會到「地理資訊」視窗,接著以滑鼠點選「國家(地區)(C)」,以 滑鼠點選「TW(台灣)」,接著以滑鼠點選「州/省(S)」欄位後依照所在地輸 入正確的州/省名稱,如圖為輸入「空白」或輸入「臺灣省」亦可,接著以 滑鼠點選「城市/位置(L)」欄位後依照所在地輸入正確的城市名稱,如圖為 輸入「臺北市」,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精畫 🛛 🗙
地理資訊 此憑證授權單位要求下列地理的資訊。
国家(地區)(C): 【W(台灣) ▼ 省/州 ©:
臺北市
必須輸入 [省/州] 和 [城市/位置],須爲正式名稱且不可含縮寫。
< 上一步 (B) (下一步 (B)) 取消
h + h - h - h = h + h + h + h + h + h + h + h + h +

接著畫面會到「憑證要求檔案名稱」視窗,接著以滑鼠點選「檔案名稱(F)」

欄位後並輸入路徑及要存的檔案名稱,如下圖所示,通常都是依照如下圖之 預設值路徑及檔案名稱存放,接著以滑鼠按下「下一步」按鈕。

IIS 憲諸憲	×
憲證要求檔案名稱 將以您所指定檔名的文字檔案儲存您的憑證要求。	
諸輸入檔案名稱給憑證要求。	
檔案名稱(17):	
e-Vcentreg.txt	瀏覽(<u>R</u>)
< 上一步 (B) (下一2	步(N)> 取消

接著畫面會到「要求的檔案摘要」視窗,檢視剛才各步驟所設定的值是否無 誤,如果沒有問題,接著以滑鼠按下「下一步」按鈕。

IIS 憑證精靈	×
要求的檔案摘要 您已經選擇建立要求檔案。	
若要建立下列要求,請按 []	
檔案名稱: c:\certreq.txt	
您的要求包含下列資訊:	
發給 好記的名稱 國家/地區 城市 公司 單位	publicca.hinet.net publicca.hinet.net TW 臺北市 中華電信股份有限公司數據通信分公司 政府網路處
	<上一步图 下一步图 取消

接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成結束製作憑證請求檔動作。



五、備份產製私密金鑰及憑證請求檔後的私密金鑰及憑證檔。 點選「開始」→「執行」

Administrator		
管理您的伺服器	😏 我的電腦	
□ 命令提示字元	☑ 控制台(C) ▶	
 ₩indows 檔案總管	 	
13事本	(2) 說明及支援(出)	
Microsoft Baseline Security Analyzer 2.2	<u>── 搜尋(3)</u>	
日本 磁碟重組工具	👸 Windows安全性(W)	】 開啓程式、資料夾、文件或網站。
於 義 終 端 機 服 務 管 理 員		
新際網路資訊服務 (IIS) 管 理員		
所有程式(P) ▶		
\frown	💋 登出(L) 🚺 關機(U)	
受開始 🥑 🕖		

執行 ? ×
剩入程式、資料夾、文件或網際網路資源的名稱, Mindows會自動開啓。
確定 取消 瀏覽(B)

於「開啟(0)」欄位輸入 mmc 後,按下「確定」按鈕。

於主控台點選「檔案」→「新增/移除嵌入式管理單元」。	
----------------------------	--

m 王 至 台 1						
檔案(乎)執行(Δ) 檢視(♥) 我的最愛(0)	視窗(型) 説明(出)				
開新檔案(N)	Ctrl+N					
開啓舊檔(<u>O</u>)	Ctrl+O					
儲存③	Ctrl+S					
另存新檔(A)				-		
(新增移除嵌入式管理單元	(M)) Ctrl+M		這個橄視沒有項目可顧	小。		
選項(P)						
1 C:\WINDOWS\\inetsrv\ii	s.msc					
2 C:\WINDOWS\\services.;	msc					
<u>3</u> C:\WINDOWS\\compmg	mt.msc					
4 C:\WINDOWS\system32\d:	frg.msc					
結束(X)						
		-				
, 讓您能夠從嵌入式管理單元:	」 主控台中新增或移称	除嵌入式管理單元。				
					1 10	

接著出現「新增/移除嵌入式管理單元」畫面,點選「新增」按鈕。

新增用各條嵌入式管理單元	? ×
獨立 〕延伸	
用這個畫面從主控台中新增或移除獨立的嵌入式管理單元。	
嵌入式管理單元 新增到心:	
_ t###	
1#1/2	
新增D 移除(R) 關於(B)	
	j

接著出現「新增獨立嵌入式管理單元」畫面,於「可用的獨立嵌入式管理單元」點選「憑證」項目後,按下「新增」按鈕。

新增獨立嵌入式管理單元	?×
可用的獨立嵌入式管理單元:	
嵌入式管理單元	廠商 ▲
▲ 💱磁碟重組工具	Microsoft Corp, Executi
一	Microsoft and VERITA
💿 網址連結	Microsoft Corporation
📄 衛 網際網路資訊服務 (IIS) 管理員	Microsoft Corporation
🥏 網際網路驗證服務 (IAS)	Microsoft Corporation
<u> 词 </u>	Microsoft Corporation
	Microsoft Corporation
國際證授權單位	Microsoft Corporation
🙀 🙀 憑證範本	Microsoft Corporation 🚽
1	<u> </u>
- 描述	或服務的憑證存放內容。
	新增创 關閉(C)
	確定 取消

接著出現「憑證嵌入式管理單元」畫面,於「這個嵌入式管理單元將自動管 理下列帳戶的憑證:」點選「電腦帳戶」後,點選「下一步」按鈕。

憲設嵌入式管理軍元	×
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)	
○ 服務帳戶(S)	
● 電腦帳戶 <u>C</u>	
	-
<上一步四(下一步四)> 取消	

接著出現「選擇電腦」畫面,於「這個嵌入式管理單元將自動管理:」點選「本機電腦(執行這個主控台的電腦)(L)」後,點選「完成」按鈕。

選擇電腦		×
韩骝摆你更岁,武帝理智	一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
一這個飲人式官理里工發		
・ 本機電腦 (執行這個	1主控合的電腦)(L):	
○ 另一台電腦(▲):	瀏覽(民)	
□ 允許對選取的電腦 (\W)	進行從命令列所啓動的變更。這只在您儲存主控台後才能適用	
	<上一步(B) 完成 取消	

回到「新增獨立嵌入式管理單元」畫面,點選「關閉」按鈕。

加宕的球联入共管理工		? ×
新增獨立嵌入式管理軍元		? ×
可用的獨立嵌入式管理單元:		
嵌入式管理單元	廠商	
警磁碟重組工具	Microsoft Corp, Executi	
当磁碟管理	Microsoft and VERITA	
◎ 網址連結	Microsoft Corporation	
🖣 網際網路資訊服務 (IIS) 管理員	- Microsoft Corporation	
● 網際網路驗證服務 (IAS)	Microsoft Corporation	
▲ 读端点面	- Microsoft Corporation	
	- Microsoft Corporation	
▲ 過過 ● 過調授權單位	Microsoft Corporation	
· · · · · · · · · · · · · · · · · · ·	Microsoft Corporation	
		-
描述- 憑證嵌入式管理單元讓您瀏覽電腦或	服務的憑證存放內容。	
	〔新增(Δ) ↓ 關閉(△	
		取消
回「蛇崎/牧队史、七竺田男;	二	它协会
到"利增/移除散八式官埕单/	し」 童 町 , 粘 迭 , 確	上, 大 」 按對
行增/移除嵌入式管理軍元		? ×
獨立 延伸		
		1
用這個畫面從主控台中新增或移除獨立	Z的嵌入式管理單元。	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到(3):	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②:	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: □ 振證 (本機電腦)	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 ☐ 主控台根目錄 新增到②: ☞ 憑證 (本機電腦)	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到◎: ∰憑證 (本機電腦)	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 憑證 (本機電腦)	Σ的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: □ 憑證 (本機電腦)	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ∰ 憑證 (本機電腦)	Z的嵌入式管理單元。 ▼	
 用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 主控台根目錄 ● 憑證 (本機電腦) 	Z的嵌入式管理單元。 ▼	
 用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 正控台根目錄 ● 正證 (本機電腦) 	Σ的嵌入式管理單元。 ▼	
 用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 → 主控台根目錄 新增到②: 	Σ的嵌入式管理單元。 ▼	
 用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 憑證 (本機電腦) 描述 	Σ的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 违控台根目錄 ● 通憑證 (本機電腦) ● 描述	Z的嵌入式管理單元。 ▼	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 正控台根目錄 ● 正控台根目錄 ● 正理台根目錄	Z的嵌入式管理單元。 ▼	
 用這個童面從主控台中新增或移除獨立 嵌入式管理單元 → 主控台根目錄 新增到③: 過應證(本機電腦) 描述 描述 新增(四)	∑的嵌入式管理單元。	
用這個畫面從主控台中新增或移除獨立 嵌入式管理單元 新增到②: ● 正控台根目錄 ● 正控台根目錄 ● 描述 ● 描述 ● 新增② ● 移除④ ● 開訪	Z的嵌入式管理單元。 ▼ ▼	

於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「憑證註冊要

求」→「憑證」找到產生憑證請求檔的憑證及私密金鑰,以滑鼠右鍵點選該 「憑證請求檔的私密金鑰及憑證」,接著點選「所有工作(K)」→「匯出」。

* 主接台1			
檔案(乎)執行(Δ) 檢視(∀) 我的最愛(○) 視窗(₩)	說明(出)		
┣————————————————————————————————————			
○主控台根目錄	2017年1月11日1日11日11日11日11日11日11日11日11日11日11日11日	到期日 預5	
● 「」 「」 」 「」 」 」 「」 」 」 「」 」 」 「」 」 」 」		2014/12/23 《至	
□ 信任的根憑證授權	所有工作(K) ▶ 開啓		
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	煎下(1) 羅出		
□□□ 受信任的發行者	複製①		
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	刪除①		
□□□ 受信任的人	内容(<u>R</u>)		
	說明(出)		

接著出現「憑證匯出精靈」畫面,於「歡迎使用憑證匯出精靈」點選「下一 步」按鈕。



接著出現「憑證匯出精靈」,「匯出私密鑰」頁面選擇「是,匯出私密金鑰

(Y)」後,以滑鼠按下「下一步」按鈕。

憲證匯出精霊	×
匯出私密金鑰 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?	
 ● 提,匯出私密金鑰(型) ○ 否,不要匯出私密金鑰(型) 	
	_
<上一步回(下一步10)> 取消	

接著出現「匯出檔案格式」頁面,選擇「個人資訊交換 - PKCS #12 (.PFX)(P)」,並勾選「啓用加強保護(需要 IE 5.0 或 NT 4.0 SP4 以上的 版本)(E)」,接著以滑鼠按下「下一步」按鈕。

「 記録 正 出 精 霊
匯出檔案格式 憑證可以用多種檔案格式匯出。
諸選取您想要使用的格式 :
€ DER 編碼二位元 X.509 (CER)(D)
C 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)
✓ 啓用加強保護 (需要 IE 5.0 或 NT 4.0 SP4 以上的版本)(E)
□ 如果匯出成功的話就刪除私密金鑰(匹)
<上一步图 下一步创 > 取消

接著出現「密碼」頁面,輸入保護私密金鑰的密碼。請務必記住此密碼,到時需要將金鑰刪除產製新金鑰後需要將原來私密金鑰及憑證匯回時就要輸

入此密碼。輸入密碼完成後,接著以滑鼠按下「下一步」按鈕。

憲證匯出精霊	×
密碼 為了安全性,您必須使用密碼保護私密金鑰。	
輸入並確認密碼。 密碼(P): *******	
· 確認密碼(C): ********	
<上一步@(下一步₪)> 取消	

接著出現「要匯出的檔案」頁面,點選「瀏覽」選擇存放位置,或直接在檔案名稱打上路徑及檔案名稱也可以。

憲證匯出精靈 要匯出的檔案 諸指定您要匯出的檔案名稱	×
檔案名稱(E): 	瀏覽 <u>R</u>)
	< 上一步 图 下一步 图 > 取消

如果有按下「瀏覽」,則可選擇檔案路徑及輸入所要儲存的私密金鑰及憑證.pfx 檔檔名。輸入完成後,按下「儲存」後,接著會跳回「要匯出的檔案」頁面,並於頁面上出現存放檔案路徑及檔案名稱。

另存新檔		? ×
儲存於①:	: 📝 桌面 💽 🕜 😥 🖽 -	
 我最近的交件 () 我最近的交件 () 承面 () 我的交件 () 我的交件 () 我的電腦 () 我的電腦 () 我的電腦 	 ● 我的交件 ● 我的電腦 ● 網路上的芳鄰 ● 13HD73888888.pfx 	
術路上的方琳	構成 (M). 「The Bay	¥777
	T∰ 石 (型): [publicca_ReqBackup] [] 存檔類型(I): 個人資訊交換 (*.pfx)	取消

輸入完成後,接著以滑鼠按下「下一步」按鈕。

×

接著出現「完成匯出精靈」頁面,按下「完成」以完成匯出私密金鑰及憑證 動作。

憲證匯出精靈		×
	完成憑證匯出精霊	
	您已經成功地完成憑證匯出精靈。	
	您已指定下列新設定:	
	檔案名稱 進出金鑰 包含憑證路徑中的所有憑證 檔案格式 個人資訊交換 (*.pfx)	
	I	
	<上─步(B) 完成 取消	

如果匯出完成,會出現如下訊息「匯出成功」。

瀌.	愛匯出精靈	×
6	霍出成功。	
	·····	ส

六、刪除憑證請求檔擱置要求,與將原來備份的私密金鑰及憑證檔(.pfx 檔)匯入。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

「 箱案(D) 執行(山) 核規(Y) 親窗(Y) 説明(H) (* →) 1 (* →)
← → こ 回 × □ 2 回 × □ 2 □ 2 □ 2 □ 2 □ 2 □ 1 □ #約(#約6)資訊服務 ● 新聞
 ● 新院報告資訊服務 ● spinet_client ● spi
目前(2) 停止(2) 暫停(2) 暫停(2) 新增(2) > 放視(2) > 從這種新婚親窗(20) 國際(20) 國際(20) 重新範察理(20) 重新範案理(20) 正 預容(20) 夏明(20)

接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

預設的網站內容 ? ×
HTTP 標頭 自訂錯誤 ASP MET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定
驗證及存取控制 格用匿名存取,並編輯這個資源的驗 證方法。 編輯 <u>進</u>)
IP 位址及網域名稱限制 使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。 編輯①…
安全通訊 當存取這個資源時使用安全通訊並啓 用用戶端憑證。 後戚思思(20) 編輯(D)

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,以滑鼠按下「下一步」 按鈕,開始刪除憑證請求檔擱置要求。
歡迎使用網頁伺服器憑證精霊。							
	歡迎使用網頁伺服器憑證精 靈						
	此精靈將協助您建立及管理用在介於伺服器及 用戶端安全網頁通訊間的伺服器憑證。						
	您的網頁伺服器狀態: 您有擱置的憑證要求。憑證精靈將協助您處理 憑證授權的回應或移除擱置要求。						
	諸按 [下一步] 來繼續。						
	<上一步(B) 下一步(B) 取消						

接著畫面會到「擱置的憑證要求」視窗,以滑鼠點選「刪除擱置要求(D)」, 接著以滑鼠按下「下一步」按鈕。

IIS 憲證精畫	×
蜀置的憑證要求 擱置的憑證要求是指憑證授權未回應的要求。	
有擱置的憑證要求。您要如何處理?	
○ 處理擱置要求及安裝憑證 (2)	
● 刪除擱置要求①	
<上一步(B) (下一步(B) >	取消

接著畫面會到「請按「下一步」來刪除要求。」視窗,接著以滑鼠按下「下一步」按鈕。



接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成刪除憑證擱置要動作。



回到「預設的網站」「內容」畫面,接著再按下「伺服器憑證」按鈕。

預設的網站內容 ?>
HTTP 標頭 自訂錯誤 ASP.NET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定
驗證及存取控制 移用匿名存取,並編輯這個資源的驗 證方法。
□ IP 位址及網域名稱限制
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
編輯①
安全通訊
當存取這個資源時使用安全通訊並啓 (同服器應證 ©)
校視憑證(2)
編輯(D)
確定 取消 套用(益) 説明

再次開啟「歡迎使用網頁伺服器憑證精靈」視窗畫面,以滑鼠按下「下一步」 按鈕,開始匯入原先備份的私密金鑰及憑證(.pfx 檔)。



接著畫面會到「伺服器憑證」視窗,以滑鼠點選「從.pfx 檔案匯入憑證」, 接著以滑鼠按下「下一步」按鈕。

★ 211 金融 211 金融 211
伺服器 熟證 這些是指派憑證到網站的方法。
諸選取您想要用於此網站的方法:
○ 建立新憑證(C)。
○指派已有的憑證(A)。
○ 從金鑰管理員備份檔案匯入憑證(Q)。
○ 従.pfx 檔案進人應證(M)
○ 從遠端伺服器網站複製或移動憑證到此網站(型)
<上一步(B) 下一步(B) 取消

接著出現「匯入檔案」頁面,點選「瀏覽」選擇存放位置,或直接在檔案名稱打上路徑及檔案名稱也可以。

IIS 憲證精畫 🛛 🗙
匯入憲證 您可以從.PFX 檔匯入憑證。
請輸入包含憑證的檔案名稱及路徑。
路徑及檔案名稱(P):
e:*.pfx (瀏覽(R))
指定在匯入後,匯入的憑證是否應標示為可匯出。將憑證標示為可匯出將具有 較高的安全風險,不過,它可允許憑證匯出到檔案進行備份。
□ 將憑證標示爲可匯出(M)

按下「瀏覽」,則可選擇檔案路徑及選擇私密金鑰及憑證.pfx 檔檔名。選 擇完成後,按下「開啟」後,接著會跳回「匯入憑證」頁面,並於頁面上出 現私密金鑰及憑證.pfx 檔檔案路徑及檔案名稱。

開啓	?	×
查詢(I)	- 🕼 🖉 🕜 😥 🔽	
我最近的文件	 → 我的文件 → 我的電腦 → 網路上的芳盤 → 13HD738888888.pfx 	
<u>桌面</u>	publices_ReqDacKup.pfx	
び 我的文件		
我的電腦		
網路上的芳鄰		
	檔名(M): 13HD738888888.pfx	₽

輸入完成後,並勾選「將憑證標示為可匯出(M)」,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精畫 X
随入悪意 您可以從.PFX 檔匯入憑證。
請輸入包含憑證的檔案名稱及路徑。 路徑及檔案名稱(P)
C:\Documents and Settings\Administrator\桌面\13HD738888888.pfx 瀏覽化
指定在匯入後,匯 <u>入的憑證是否應標示為可匯出。將憑證標示為可匯出將具有</u> 較高的安全風險,不過,它可允許憑證匯出到檔案進行備份。
▶ 將憑證標示為可雖出(M)
<上一步(B) 下一步(B) 取消

接著出現「匯入憑證密碼」頁面,輸入保護私密金鑰的密碼。

IIS 憲證精畫	×
匯入燕證密碼 您必須提供密碼以匯入憑證。	
諸爲您想要匯入的憑證輸入密碼。	
密語 ().	
1	<上一步(B) 下一步(B) 取消

接著出現「SSL連接埠」頁面,並設定「這個網站應該使用的SSL連接埠(L)」, 請依網站需求自行設定,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精畫		×
SSL 連接埠 為這個網站指定 SSL 連接埠。		
浸伺網站應該使用的 SSL 連接埠(止):		
	\sim	
	<上─毋個) 下─毋個>	取消

接著出現「已匯入憑證的摘要」頁面,確認憑證內容無誤後,接著以滑鼠按 下「下一步」按鈕。



接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成匯入私密金鑰及憑證.pfx 檔動作。



透過瀏覽器連線測試網頁 https 是否連線正常。



檢查 SSL 憑證串鏈是否正常。

🖉 https://publicca.hinet.n	et/index.html - Microsoft Internet Explorer	
檔案(F) 編輯(E) 檢視(
	21 🕜 入 授琴 🛠 抜印段変 🕙 🕗 • 🚱 🔄	秋五 油结 >>
тачи (2) 💽 Апрелирионсса.	unetnevindex.rumi	
It's Work.	般 詳細資料 振盪路徑 一般 詳細資料 振盪路径 ● ● 融品 ●	
	登行者: Public Certification Authority 有效期自 2013/12/22 列 2016/12/22 医簧键微微	*
) ② 完成		A K K K K K K K K K K K K K K K K K K K
		- 111
 https://publicea.hinet.n 檔案(P) 編輯(E) 檢視((A) 上一頁 · (A) · (A) 	eVindex.html - Microsoft Internet Explorer V) 我的最愛(A) 工具(I) 說明(H) A) 🔥 搜尋 👷 我的最爱 🏈 🔗 📚 🚍	
 ▶ https://publicca.hinet.n 檔案① 編輯 ② 核視(▲ 上一頁 · ○ · × 綱壮 ② 營 https://publicca.hinet.n 	et/index.html - Microsoft Internet Explorer ② 我的最爱④ 工具① 說明⑪ ② 忝 │ ♪ 搜尋 ☆ 我的最爱 ④ │ @ + ॆ 毫 唇 hinet.net/index.html	× × ▼ ▶ 移至 連結 ≫
★ https://publicca.hinet.n 檔案 ① 編輯 ② 校硯(③ 上一頁 → ④ → ▲ 網址 ② ≧ https://publicca.] It's Work.	et/index.html - Microsoft Internet Explorer ② 我的最愛 ④ 工具 ① 説明 ④ ② ♪ 搜尋 ☆ 我的最爱 ④ @ ~ 》 ② ② Thet net/index.html	- · · · · · · · · · · · · · · · · · · ·
★ https://publicca.hinet.m 檔案① 編輯② 校硯(④ 上一頁 · ④ · ▼ 〕 網址① ● https://publicca.] It's Work.	et/index.html - Microsoft Internet Explorer ① 我的最愛 ④ 工具 ① 説明 ④ P 搜尋 ◆ 我的最爱 ④ P ▲ ■ Primet net/index html	- · · · · · · · · · · · · · · · · · · ·

以上動作即完成 Windows 2003 IIS 6.0 重新產製金鑰及憑證請求檔動作, 並還原原先的 SSL 私密金鑰及憑證動作。

Windows IIS 6.0 SSL 憑證安裝操作手冊

安裝根憑證(eCA)及中繼憑證(PublicCA)

此步驟為該伺服器網站從未安裝根憑證(eCA)及中繼憑證(PublicCA)才需執行。

- 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。
 - 2. 從網站查詢與下載:

eCA 憑證:

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

PublicCA G2 憑證:

http://epki.com.tw/download/PublicCA2_64.crt

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、點選「開始」→「執行」



(0)」欄位輸入mmc後,按下「確定」按鈕。

A行 ?×
新入程式、資料夾、文件或網際網路資源的名稱, Windows 命自動問題。
確定 取消 瀏覽图…

於主控台點選「檔案」→「新增/移除嵌入式管理單元」。

1 主控台1								
檔案(F)執行(A)	檢視(♡)	我的最愛(0)	視窗(₩)	說明(H)				
開新檔案(N)		Ctrl+N						
開啓舊檔(O)		Ctrl+O						[
(語仔(3) (月) (4)		Ctrl+S						
*****					這個檢視沒有項目可國	 ■示。		
新增格除嵌入式	管理单元(图	1) Utrl+M						
1 C:\WINDOWS\	\unetsrv\us.n	nsc o						
3 C:\WINDOWS\	.vcompmgmt	t.msc						
4 C:\WINDOWS\sy	/stem32\dfrg	g.msc						
T								
讓您能夠從嵌入式管	理單元主持	空台中新增或移	除嵌入式管	理單元。				

接著出現「新增/移除嵌入式管理單元」畫面,點選「新增」按鈕。

新增/移除嵌入式管理單元	? ×
獨立 延伸	
用這個畫面從主控台中新增或移除	獨立的嵌入式管理單元。
嵌入式管理單元 🔄 主控台根目	錄 🔄 💼
141/1	
	關於(3)

接著出現「新增獨立嵌入式管理單元」畫面,於「可用的獨立嵌入式管理 單元」點選「憑證」項目後,按下「新增」按鈕。

Ð	/碧獨立嵌入式管理軍 元	? ×
	可用的獨立嵌入式管理單元:	
	嵌入式管理單元	廠商 ▲
	💕 磁碟重組工具	Microsoft Corp, Executi
	過磁碟管理	Microsoft and VERITA
	🗿 網址連結	Microsoft Corporation
	🖣 網際網路資訊服務 (IIS) 管理員	Microsoft Corporation
	🧇網際網路驗證服務 (IAS)	Microsoft Corporation
	<u> </u>	Microsoft Corporation
C	「「「「「「「」」」	Microsoft Corporation
	医热 起授權單位	Microsoft Corporation
	1200 - 医静脉	Microsoft Corporation 🚽
		新增(A) 關閉(C)

接著出現「憑證嵌入式管理單元」畫面,於「這個嵌入式管理單元將自動 管理下列帳戶的憑證:」點選「電腦帳戶」後,點選「下一步」按鈕。

憲證嵌入式管理軍 元	×
這個歌人式管理單元將目動管理下列帳戶的憑證:	
○ 我的使用者帳戶(M)	
○ 服務帳戶(S)	
	_
<上一步(L) 下一步(L) 取消	

接著出現「選擇電腦」畫面,於「這個嵌入式管理單元將自動管理:」點選「本機電腦(執行這個主控台的電腦)(L)」後,點選「完成」按鈕。



回到「新增獨立嵌入式管理單元」畫面,點選「關閉」按鈕。

新增獨立嵌入式管理軍元		? ×
可用的獨立嵌入式管理單元:		
嵌入式管理單元	廠商	
警磁碟重組工具	Microsoft Corp, Executi	
一 磁碟管理	Microsoft and VERITA	
💿 網址連結	Microsoft Corporation	
🛛 🖣 網際網路資訊服務 (IIS) 管理員	Microsoft Corporation	
🗌 🧇 網際網路驗證服務 (IAS)	Microsoft Corporation	
	Microsoft Corporation	
· · · · · · · · · · · · · · · · · · ·	Microsoft Corporation	
🙆 憑證授權單位	Microsoft Corporation	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Microsoft Corporation	Ţ
, 描述 憑證嵌入式管理單元讓您瀏覽電腦或服	3務的憑證存放內容。 	
	新增(A) 關閉(C	\supset

回到「新增/移除嵌入式管理單元」畫面,點選「確定」按鈕。

新碧/移除嵌入式管理單元 ? 🛛
獨立 延伸
用這個畫面從主控台中新增或移除獨立的嵌入式管理單元。
嵌入式管理單元 新增到⑥:
_
描述
新增①
確定取消

於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「信任的根 憑證授權」→「憑證」→「所有工作(K)」→「匯入(I)」。

🌇 主控台1 - [主控台根目錄\憑詞	證 (本機電腦)\信任的根憑證授權\憑]]			_ 🗆 🗙
猫 檔案 (F) 執行 (▲) 檢視 (V)	我的最愛(Q) 視窗(₩) 說明(H)				_ 8 ×
	} 😰 💵				
□ 主控台根目錄	發給 △	發行者	到期日	預定目的	好記▲
□ 🗐 憑證 (本機電腦)	ABA.ECOM Root CA	ABA.ECOM Root CA	2009/7/9	安全電子郵件,伺服	DST (
• • • • • • • • • • • • • • • • • • •	🔤 Autoridad Certificadora de la Asoci	Autoridad Certificadora de la Asociaci	2009/6/28	安全電子郵件,伺服	Autor
(二) 信任的根憑證授權)	🔤 Autoridad Certificadora del Colegi	Autoridad Certificadora del Colegio N	2009/6/29	安全電子郵件,伺服…	Autor
○ 振音	K) SELO	Baltimore EZ by DST	2009/7/3	安全電子郵件,伺服…	DST
		Belgacom E-Trust Primary CA	2010/1/21	安全電子郵件,伺服…	Belga
田─────────────────────────────────────	 SecureNet CA Class A 	C&W HKT SecureNet CA Class A	2009/10/15	安全電子郵件,伺服…	CWF
	曾視窗(W) SecureNet CA Class B	C&W HKT SecureNet CA Class B	2009/10/15	安全電子郵件,伺服…	CWF
	SecureNet CA Root	C&W HKT SecureNet CA Root	2010/10/15	安全電子郵件,伺服…	CWF
日本 二 第二万位 新工作合物	窥視①… SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	2009/10/15	安全電子郵件,伺服…	CWF
	F) Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/26	安全電子郵件,伺服…	Certis
□ □ SPC	L) Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/26	安全電子郵件,伺服…	Certis
	utoridade Certificadora	Certisign Autoridade Certificadora A	2018/6/26	安全電子郵件,伺服…	Certis
說明(<u>H</u>)	utoridade Certificadora	Certisign Autoridade Certificadora A	2018/7/9	安全電子郵件,伺服…	Certis
	🔛 Class 1 Primary CA	Class 1 Primary CA	2020/7/6	安全電子郵件,伺服…	CertP
	🔤 Class 1 Public Primary Certification	Class 1 Public Primary Certification A	2028/8/1	安全電子郵件,用戶…	VeriS
	🔤 Class 1 Public Primary Certification	Class 1 Public Primary Certification A	2020/1/7	安全電子郵件,用戶…	VeriS
	🔤 Class 2 Primary CA	Class 2 Primary CA	2019/7/6	安全電子郵件,伺服…	CertP
	🔤 Class 2 Public Primary Certification	Class 2 Public Primary Certification A	2004/1/7	安全電子郵件,用戶…	VeriS
	🔤 Class 2 Public Primary Certification	Class 2 Public Primary Certification A	2028/8/1	安全電子郵件,用戶…	VeriS
	🔛 Class 3 Primary CA	Class 3 Primary CA	2019/7/6	安全電子郵件,伺服…	CertP
	🔤 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	2028/8/1	安全電子郵件,用戶…	VeriS
	🔤 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	2004/1/7	安全電子郵件,用戶…	VeriS
	🔤 Class 3P Primary CA	Class 3P Primary CA	2019/7/6	安全電子郵件,伺服…	CertP
	🔛 Class 3TS Primary CA	Class 3TS Primary CA	2019/7/6	安全電子郵件,伺服…	CertP
	🔤 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	1999/12/30	時間戳記	Miere
	🔤 Deutsche Telekom Root CA 1	Deutsche Telekom Root CA 1	2019/7/9	安全電子郵件,伺服…	Deuts
	🔤 Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	2019/7/9	安全電子郵件,伺服…	Deuts
	🔤 DST (ANX Network) CA	DST (ANX Network) CA	2018/12/9	安全電子郵件,伺服	DST 💌
	 				
將新憑證加入存放					

接著出現「憑證匯入精靈」畫面,於「歡迎使用憑證匯入精靈」點選「下

一步」按鈕。

憲證匯入精靈	×
数辺(使用憑證匯入精霊
這個精調	霻將協助您將憑證、憑證信任諸單及憑證撤銷 巍碟複製到憑證存放區。
振設由) 用來保護 放區是)	愚證授權單位簽發,能識別您的身分,並包含 獲資料或建立安全性的網路連線資訊。憑證存 用來存放憑證的系統區域。
諸按「	一步] 繼續。
	<上一步(B)(下一步(M))) 取消

接著出現「匯入檔案」畫面,點選「瀏覽」選擇存放位置,或直接在檔案 名稱打上路徑及檔案名稱也可以。

匯入精	盖
匯入檔 3 指定	案 您想要匯入的檔案。
檔案	名稱(F):
I	瀏覽(R))
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	副人資訊交換- PKCS #12 (.PFX,.P12)
끃	?碼編譯訊息語法標準 - PKCS #7 認證 (.p7b)
М	licrosoft 序列憑證存放 (.sst)
	<上一步(B) 下一步(N) > 取消

如果有按下「瀏覽」,則可選擇要匯入的檔案路徑及所要選取的根憑證檔 名「ROOTeCA_64.crt」。選取完成後,按下開啟後,接著會跳回「匯入檔 案」頁面,並於頁面上出現要匯入的檔案路徑及檔案名稱,並點選「下一 步」按鈕。

憲證匯入精畫	×
匯入檔案 指定您想要匯入的檔案。	
檔案名稱(E): C:\Documents and Settings\Administrator\点面\ROOTeCA_64.crt [瀏覽(R)]	
諸注意: 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 認證 (.p7b)	
Microsoft 序列憑證存放 (.sst)	
<上一步(B) 下一步(B) 下一步(B) 取消	

接著出現「憑證存放區」畫面,點選「將所有憑證放入以下的存放區(P)」 點選「瀏覽」按鈕。

無證匯入精畫 🛛 🛛 🛛 🛛 🛛
憲證存放區 憑證存放區是用來存放憑證的系統區域。
Windows 會自動選擇一個憑證存放區,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: 信任的根憑證授權
<上一步圆 下一步创 > 取消
妾著出現「選擇憑證存放區」畫面,先點選「顯示實體存放區(S)」,選擇

按者出現"選擇認證仔放區」畫面,元點選「顯不員體仔放區(S)」,選择「「信任的根憑證授權」→「本機電腦」後,並點選「確定」按鈕。

憑證匯入楮霊	د	<
憲證存放區 憑證存放圖	選擇憲證存放區 ? 🔀	
₩indows 會 ⓒ 自動 ⓒ 將所 憑證 信任	選取您要使用的憑證存放區(C)	
	< 上一步 (B) 下一步 (M) > 取消	

回到「憑證存放區」畫面後,以滑鼠按下「下一步」按鈕。

憲證存放區
憑證存放區是用來存放憑證的系統區域。
Windows會自動選擇一個憑證存放區,您也可以爲憑證指定存放位置。
○ 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)
· · · · · · · · · · · · · · · · · · ·
信任的根憑證授權(本機電腦) 創覽(衣)]

接著出現「完成憑證匯入精靈」頁面,按下「完成」以完成 eCA 根憑證匯入動作。

憲證匯入精靈		×
	完成憑證匯入精霊	
	您已經成功地完成憑證匯入精靈。	
	您已指定下列新設定:	
	使用者選取的憑證存放區 內容 檔案名稱 C:\Documents and Settings\/	
	< 上一步 (B) 完成 取消	

按下完成後,如有出現類似以下訊息,	則直接按下「是」,即可匯入完成。
-------------------	------------------

安全在答	
	您正要從憑證授權單位 (CA) 安裝憑證,該憑證授權單位聲稱代表:
	ePKI Root Certification Authority
	Windows 無法確認憑證確實是從 "ePKI Root Certification Authority" 來的。您應該連絡 "ePKI Root Certification Authority" 以確認 它的來源。 下列數字在這個過程中將可以協助您:
	憑證指紋 (sha1): 5825B6CB 84152731 5CCC6DF0 55731CF5 DBD5E4FF
	警告: 如果您安裝這個根憑證,Windows 將自動信任任何由這個 CA 所發行的憑證。使用未經確認的憑證指紋來安裝憑證將會有安 全性的風險。如果您按 [是],表示您認可這個風險。
	您想要安裝這個憑證嗎?
	是四一百四二

匯入完成,會出現如下訊息「匯入執行成功」訊息。

憲證匯入	精靈	×
i	匯入執行	亍成功。
	確定	

匯入完成後,請在「信任的根憑證授權」→「憑證」以滑鼠按下右鍵,點 選「重新整理」。

🌇 主控台1 - [主控台根目錄\憲	證 (本機電腦)\信任的根憲證授權\憑	2)				x
🜇 檔案(E) 執行(A) 檢視(V)	我的最愛(Q) 視窗(W) 說明(H)				_ 8	×
	3 🕄 🖬					
主控台根目錄	■ 離給 /	發行者	到期日	福定日的	好記的名種 批	.
- 🗊 憑證 (本機電腦)	ABA.ECOM Root CA	ABA.ECOM Root CA	2009/7/9	安全電子郵件,伺服	DST (ABA ECOM) CA	<u> </u>
□ 🗄 💼 個人	🔤 Autoridad Certificadora de la Asoci	Autoridad Certificadora de la Asociaci	2009/6/28	安全電子郵件,伺服	Autoridad Certificado	1
🕞 📄 信任的根憑證授權	Autoridad Certificadora del Colegi	Autoridad Certificadora del Colegio N	2009/6/29	安全電子郵件,伺服	Autoridad Certificado	
「「「「「「「」」」	re EZ by DST	Baltimore EZ by DST	2009/7/3	安全電子郵件,伺服	DST (Baltimore EZ)	
由···································	m E-Trust Primary CA	Belgacom E-Trust Primary CA	2010/1/21	安全電子郵件,伺服	Belgacom E-Trust Pri	
□ □ □ 中繼憑証 檢視(♡)	KT SecureNet CA Class A	C&W HKT SecureNet CA Class A	2009/10/15	安全電子郵件,伺服	CW HKT SecureNet	
田 🔲 受信任的 從這裡新增調	見窗(W) KT SecureNet CA Class B	C&W HKT SecureNet CA Class B	2009/10/15	安全電子郵件,伺服	CW HKT SecureNet	
	KT SecureNet CA Root	C&W HKT SecureNet CA Root	2010/10/15	安全電子郵件,伺服	CW HKT SecureNet	-
□□□ 弗二万根 新工作合做品	R(1) KT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	2009/10/15	安全電子郵件,伺服	CW HKT SecureNet	
	n - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/26	安全電子郵件,伺服	Certisign Autoridade	
	n - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/26	安全電子郵件,伺服	Certisign Autoridade	
	n Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/6/26	安全電子郵件,伺服	Certisign Autoridade	
說明(<u>H</u>)	n Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/7/9	安全電子郵件,伺服	Certisign Autoridade	
	🔤 Class 1 Primary CA	Class 1 Primary CA	2020/7/6	安全電子郵件,伺服	CertPlus Class 1 Prim	
	🔤 Class 1 Public Primary Certification	Class 1 Public Primary Certification A	2028/8/1	安全電子郵件,用戶	VeriSign Class 1 Publi	
	🔤 Class 1 Public Primary Certification	Class 1 Public Primary Certification A	2020/1/7	安全電子郵件,用戶	VeriSign Class 1 Prim	
	🔤 Class 2 Primary CA	Class 2 Primary CA	2019/7/6	安全電子郵件,伺服	CertPlus Class 2 Prim	
	🔤 Class 2 Public Primary Certification	Class 2 Public Primary Certification A	2004/1/7	安全電子郵件,用戶	VeriSign Class 2 Prim	
	🔤 Class 2 Public Primary Certification	Class 2 Public Primary Certification A	2028/8/1	安全電子郵件,用戶	VeriSign Class 2 Publi	
	🔤 Class 3 Primary CA	Class 3 Primary CA	2019/7/6	安全電子郵件,伺服	CertPlus Class 3 Prim	
	🔤 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	2028/8/1	安全電子郵件,用戶	VeriSign Class 3 Publi	
	🔤 Class 3 Public Primary Certification	Class 3 Public Primary Certification A	2004/1/7	安全電子郵件,用戶	VeriSign Class 3 Prim	
	🔤 Class 3P Primary CA	Class 3P Primary CA	2019/7/6	安全電子郵件,伺服	CertPlus Class 3P Pri	
	🔤 Class 3TS Primary CA	Class 3TS Primary CA	2019/7/6	安全電子郵件,伺服	CertPlus Class 3 TS Pri	
	🔤 Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	1999/12/30	時間戳記	Microsoft Timestamp	
	🔤 Deutsche Telekom Root CA 1	Deutsche Telekom Root CA 1	2019/7/9	安全電子郵件,伺服…	Deutsche Telekom Ro	
	🔤 Deutsche Telekom Root CA 2	Deutsche Telekom Root CA 2	2019/7/9	安全電子郵件,伺服	Deutsche Telekom Ro	
	DST (ANX Network) CA	DST (ANX Network) CA	2018/12/9	安全電子郵件,伺服	DST (ANX Network)	-
Ⅰ ►	•				Þ	
重新整理目前的選取項目。						

檢查一下,找到「ePKI Root Certification Authority」且看到憑證到期 日為 2034/12/19 即是 eCA 憑證有匯入成功。

🌇 主控台1 - [主控台根目錄\漂	證 (本機電腦)\信任的根憑證授權\憑]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]			_ 🗆 >
	我的最愛(<u>()</u> 親窗(<u>W</u>) 説明(<u>H</u>)				_ 8 ×
				· 第一日 45	175365 /2 #F
□ 土控首恨日球 ● 周 馮逵 /★掸蚕 III)	Bar Antipart Cartification Authority	酸17-合	到期日 2024/12/10	「現た日的」	好記的名稱 秋 4
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	E Houris from Cartificate Authority	Fourifax Secure Contification Authority	2034/12/13	安全電子郵件 伺服	Fauifax Secure Certifi
□ □ □ 信任的根憑證授權	Equifax Secure eBusiness CA-1	Fourifax Secure eBusiness CA-1	2020/6/20	安全電子郵件,伺服	Equifax Secure eBusi
	Equifax Secure eBusiness CA-2	Equifax Secure eBusiness CA-7	2020/0/20	安全電子郵件 伺服	Equifax Secure eBusi
□ □ □ 企業信任	Equifax Secure Global eBusiness C	Equifax Secure Global eBusiness CA-1	2020/6/20	安全電子郵件,伺服	Equifax Secure Globa
□… 📄 中繼憑證授權	Ellinet International Root CA	Ellnet International Root CA	2018/10/2	安全雷子郵件, 伺服	EIInet International R
	FESTE, Public Notary Certs	FESTE, Public Notary Certs	2020/1/1	安全電子郵件,伺服	FESTE, Public Notary
	FESTE, Verified Certs	FESTE, Verified Certs	2020/1/1	安全電子郵件,伺服	FESTE. Verified Certs
田 🛄 受信任的發行者	First Data Digital Certificates Inc. C	First Data Digital Certificates Inc. Cert	2019/7/3	伺服器驗證 用戶端…	First Data Digital Certi
□ □ 沒有信任的您證	FNMT Clase 2 CA	FNMT Clase 2 CA	2019/3/18	安全電子郵件,伺服	Fabrica Nacional de
田一〇 第二万秋源語技権単位	🔤 GlobalSign Root CA	GlobalSign Root CA	2014/1/28	安全電子郵件,伺服	GlobalSign Root CA
	🔤 G TE Cyber Trust Global Root	GTE CyberTrust Global Root	2018/8/13	安全電子郵件,用戶	GTE CyberTrust Glob
H- SPC	🔤 G TE Cyber Trust Root	GTE CyberTrust Root	2004/4/3	安全電子郵件,用戶	GTE CyberTrust Root
	🔤 GTE CyberTrust Root	GTE CyberTrust Root	2006/2/23	安全電子郵件,用戶…	GTE CyberTrust Root
	🔤 http://www.valicert.com/	http://www.valicert.com/	2019/6/25	安全電子郵件,伺服	ValiCert Class 1 Polic
	🔤 http://www.valicert.com/	http://www.valicert.com/	2019/6/25	安全電子郵件,伺服…	ValiCert Class 3 Polic
	E http://www.valicert.com/	http://www.valicert.com/	2019/6/25	安全電子郵件,伺服…	ValiCert Class 2 Polic
	IPS SERVIDORES	IPS SERVIDORES	2009/12/29	安全電子郵件,伺服…	IPS SERVIDORES
	🔤 Microsoft Authenticode(tm) Root A	Microsoft Authenticode(tm) Root Aut	1999/12/31	安全電子郵件,代碼	Microsoft Authentico
	🔤 Microsoft Root Authority	Microsoft Root Authority	2020/12/30	<全部>	Microsoft Root Autho
	Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	2021/5/9	<全部>	Microsoft Root Certifi
	🔤 NetLock Expressz (Class C) Tanusit	NetLock Expressz (Class C) Tanusitva	2019/2/20	伺服器驗證,用戶端…	NetLock Expressz (Cl
	🔤 NetLock Kozjegyzoi (Class A) Tan	NetLock Kozjegyzoi (Class A) Tanusit	2019/2/19	伺服器驗證,用戶端…	NetLock Kozjegyzoi (
	NetLock Uzleti (Class B) Tanusitva	NetLock Uzleti (Class B) Tanusitvany	2019/2/20	伺服器驗證,用戶端…	NetLock Uzleti (Class
	NO LIABILITY ACCEPTED, (c)9	NO LIABILITY ACCEPTED, (c)97	2004/1/7	時間戳記	VeriSign Time Stampi
	PTT Post Root CA	PTT Post Root CA	2019/6/26	安全電子郵件,伺服	KeyMail PTT Post Ro
	🔛 Saunalahden Serveri CA	Saunalahden Serveri CA	2019/6/25	安全電子郵件,伺服…	Saunalahden Serveri
	Saunalahden Serveri CA	Saunalahden Serveri CA	2019/6/25	安全電子郵件,伺服	Saunalahden Serveri
信任的根憑證授權 存放包含 104 (固憑證。				

四、於主控台視窗點選「主控台根目錄」→「憑證(本機電腦)」→「中繼憑證 授權」→「憑證」→「所有工作(K)」→「匯入(I)」。

論:主接台1 - 「主接台根目錄/善證 (本機面臨)\中盤善證授權(善證)					
* 檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 説明(H)					_ 181 ×1
〕主控台根目錄 登給 △	發行者	到期日	預定目的	好記的名稱	狀態
- 憑證 (本機電腦) Microsoft Windows Hardware Com.	Microsoft Root Authority	2002/12/30	代碼簽署, Windows	<無>	
	Root Agency	2039/12/31	《全部》	<#>	
E VenSign Class 1 CA Individual Su	Class I Public Primary Certification A	2008/5/12	<至前>	<無>	
□ 中繼張證授權 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Class 2 Public Primary Certification A	2004/1/0	<王市> 2.16.040.1.112722.1	<無>	
□ ● 憑證撤銷者單	Class 5 Fublic Filmary Certification A	2004/1/7	2.10.040.1.113733.1	<##>	
□ □ □ = 第二月10					
田· 🗀 憑證註冊 新工作台檢視(I)					
· ···································					
至初 <u>定</u> 在(1) 陳出港留(1.)					
記明(<u>出</u>)					
					Þ
將新憑證加入存放					

接著出現「憑證匯入精靈」畫面,於「歡迎使用憑證匯入精靈」點選「下 一步」按鈕。



接著出現「匯入檔案」畫面,點選瀏覽選擇存放位置,或直接在檔案名稱 打上路徑及檔案名稱也可以。

憲證匯入括 畫	×
匯入檔案 指定您想要匯入的檔案。	
檔案名稱(F): 瀏覽(R)	
諸注意: 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 認證 (.p7b)	
Microsoft 序列憑證存放 (.sst)	
	_

如果有按下「瀏覽」,則可選擇要匯入的檔案路徑及中繼憑證檔檔名 (PublicCA_64.crt)。選取完成後,按下「開啟」後,接著會跳回「匯入檔 案」頁面,並於頁面上出現要匯入的檔案路徑及檔案名稱。

開啓		? ×
查詢(]):	: 📝 桌面 💽 🕄 🗇 📂 🛄 -	
	 □ 我的文件 □ 我的電腦 	
我最近的文件	■ 網路上的芳鄰	
	1-11D79888888 cer	
🔰 🕻	PublicCA_64.cr	
点面	ROOTECA_64.crt	
>		
我的文件		
我的電腦		
		
網路上的芳鄰		
	檔名(N): PublicCA_64.crt I	開啓②
	檔案類型(I): X.509 憑證 (*.cer;*.crt) ▼	現以7月

選取完成後,接著以滑鼠按下「下一步」按鈕。

慧證匯入精畫	×
匯入檔案 指定您想要匯入的檔案。	
檔案名種(E): C:\Documents and Settings\Administrator\点面\PublicCA_64.crt 题覽(R)]	
諸注意: 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 (.PFA,.P12) 密碼編譯訊息語法標準 - PKCS #7 認證 (.p7b)	
Microsoft 序列憑證存放 (.sst)	
<上一步(L) 下一步(L) > 取消	

接著出現「憑證存放區」畫面,點選「將所有憑證放入以下的存放區(P)」 點選「瀏覽」按鈕。

意識匯入精畫
憲證存放區 憑證存放區是用來存放憑證的系統區域。
Windows會自動選擇一個憑證存放區,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:
中繼憑證授權 (瀏覽(R))
< 上一步(B) 下一步(M) > 取消
·

接著出現「選擇憑證存放區」畫面,先點選「顯示實體存放區(S)」,選擇 「中繼憑證授權」→「本機電腦」後,並點選「確定」按鈕。



回到「憑證存放區」畫面後,以滑鼠按下「下一步」按鈕。

憲證匯入精畫 ×
憲證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 會自動選擇一個憑證存放區,您也可以爲憑證指定存放位置。
○ 自動根據過過類型來選取憑證存放區(U)
第所有憑證放入以下的存放區(P)
恶音存放 區。
中繼憑證授權体機電腦 創覽 (2))
< 上一步(B) 下一步(N) >

接著出現「完成憑證匯入精靈」頁面,按下「完成」以完成 PublicCA 中 繼憑證匯入動作。

憲證匯入精靈		×
	完成憑證匯入精霊	
	您已經成功地完成憑證匯入精靈。	
	您已指定下列新設定:	
a state of the second	使用者選取的憑證存放圖。中繼憑證授權、本機電腦	
	内容 透證 檔案名稱 C:\Documents and Settings\/	
	< 上一步 (B) 完成 取消	

匯入完成,會出現如下訊息「匯入執行成功」訊息。



匯入完成後,請在「中繼憑證授權憑證」→「憑證」以滑鼠按下右鍵,點 選「重新整理」。

🎦 主控台1 - [主控台根目錄\憲	證 (本機電腦)\中繼憑證授權\憑證]					
🌇 檔案(E) 執行(A) 檢視(V)	我的最愛⊙) 視窗(₩) 説明(出)					_ 8 ×
	3 😰 🖬					
] 主控台根目錄	發給 △	發行者	到期日 預定目	的 英	記的名稱	狀態
- 🗐 憑證 (本機電腦)	🔤 Microsoft Windows Hardware Com	Microsoft Root Authority	2002/12/30 代碼簽	署, Windows 👒	無>	
● ● 個人	Root Agency	Root Agency	2039/12/31 <全部>	<	無 >	
□ □ 信任的根憑證授權	🔛 VeriSign Class 1 CA Individual Su	Class 1 Public Primary Certification A	2008/5/12 《全部》	<	無 >	
□ □ 企業信任	🔛 VeriSign Class 2 CA - Individual S	Class 2 Public Primary Certification A	2004/1/6 <全部>	<	無 >	
 ● 中總憑證授權 ● 透證數消清單 ● 愛信任的發行者 ● 沒有信任的感證 ● 沒有信任的感證 ● 愛信任的人 ● 愛信任的人 ● 愛信任的人 ● 愛信任的人 ● 愛信任的人 	www.venisign.com/CPS Incorp.by	Class 3 Public Primary Certification A 所有工作(公) ・ 重新整理(P) 暨出情望台 檢視(Y) ・ 排列圖示① ・ 對齊圖示(E) 說明(任)	2004/1/7 2.16.84	0.1.113733.1 <	無>	
▲ ▲ 本 ★ <p< td=""><td>×</td><td></td><td></td><td></td><td></td><td>×</td></p<>	×					×

檢查一下,找到「Public Certification Authority」且看到憑證到期日為 2027/5/15 即是 PublicCA 中繼憑證有匯入成功。

🌇 主控台1 - [主控台根目錄\憑證 (本機電腦)\中繼	(憲證授權)憲證]					_ 🗆 🗵
窗 檔案 E 執行 (A) 檢視 (V) 我的最愛 (O) 視	窗(W) 説明(H)					_ 8 ×
〕主控台根目錄 發給 △		發行者	到期日	預定目的	好記的名稱	狀態
👘 憑證 (本機電腦) 🔤 Microsoft Window	we Herdware Com	Misresoft Root Authority	2002/12/30	代碼簽署,Windows	<無>	
■ ■ 個人	on Authority	ePKI Root Certification Authority	2027/5/15	<全部>	<無>	
□□ 信任的根戀證授權 🔤 Root Agenuy		Reet Agency	2039/12/31	<全部>	<無>	
■ 原證 🔤 VeniSign Class 1 (CA Individual Su	Class 1 Public Primary Certification A	2008/5/12	<全部>	<無>	
世世世王第18日世 🔤 VenSign Class 2 (CA - Individual S	Class 2 Public Primary Certification A	2004/1/6	<全部>	<無>	
日一回 中枢認識技術種 🔤 www.verisign.com	n/CPS Incorp.by	Class 3 Public Primary Certification A	2004/1/7	2.16.840.1.113733.1	<無>	
日 一 受信任的發行者						
□ □ 2月信任的憑證						
□ □ 第三方根憑證授權單位						
□□□□ 受信任的人						
□ 💼 憑證註冊要求						
i in the sec						
						Þ
中繼憑證授權 存放包含 6 個憑證。						

回到「主控台」頁面,點選「檔案」→「結束」,以結束「主控台」。

1	主控台1	- [主控台	限目錄\憑	證 (本機電腦) \/	中繼憑證授	権\憑證]						_ 🗆 🗵
°B	檔案①	執行(<u>A</u>)	檢視(型)	我的最愛(0)	視窗(₩)	說明(<u>H</u>)						_ 8 ×
4	開新権	諸案(N)		Ctrl+N								
E	開啓翻	[檔(0)		Ctrl+O			發行者	到期日	預定目的		好記的名稱	狀態
-6	(語仔)(a) 	5) 54時(4)		C#I+S	dows Hardy	vare Com	Microsoft Root Authority	2002/12/30	代碼簽署,₩	indows	<無>	
	2213789	i'i⊞ (<u>∆</u>)			ation Autho	rity	ePKI Root Certification Authority	2027/5/15	<全部>		<無> 	
Ē	新增用	3除嵌入式 、	管理單元()	₫) Ctrl+M	1 CA Indiv	vidual Su	Class 1 Public Primary Certification A	2008/5/12	< ± m> < 全部>		<無> <無>	
E	进归(世	o			2 CA - Ind	ividual S	Class 2 Public Primary Certification A	2004/1/6	<全部>		<無>	
	<u>1</u> C:\W	INDOWS'	\inetsrv\iis.r	nsc	com/CPS Ir	orp.by	Class 3 Public Primary Certification A	2004/1/7	2.16.840.1.11	3733.1	<無>	
	2 C:\W	INDOWS\	.\services.m:	9C								
E	<u>3</u> C:1W	UNDOWS\	.vcompmgm vstem 32Vd fr	a.msc ø msc								
	laborto a		,	P								
	結束(2	() ()										
G	- 📄 SPC											
◀			<u> </u>	•								Þ
結	東程式並 掛	标使用者	諸存文件。									

接著會跳出「您要將主控台設定值儲存到主控台1嗎?」訊息,點選「否」, 結束「主控台」。

☆ 主党△1 「主党△担日鎮」	· · · · · · · · · · · · · · · · · · ·						
	3 🗳 💵						
1 主控台根目錄	2226 △	發行者	到期日 預	定目的	好記的名稱	狀態	
- 🗐 憑證 (本機電腦)	Microsoft Windows Hardware Com	Microsoft Root Authority	2002/12/30 代	碼簽署, Windows	<無>		
● ● 佐氏的根連環探護	Public Certification Authority	ePKI Root Certification Authority	2027/5/15 <1	全部>	<無>		
1111111111111111111111111111111111111	Root Agency	Root Agency	2039/12/31 <3	全部>	<無>		
日… 🔄 止未行に	VenSign Class 1 CA Individual Su	Class 1 Public Primary Certification A	2008/5/12 <3	全部> > #7	<無>		
□□□ 〒● 徳忠忠文作	VenSign Class 2 CA - Individual S	Class 2 Public Primary Certification A	2004/1/6 <3	全部>	<#*>		
→ 活動	www.vensign.com/CPS Incorp.by	Class 3 Public Primary Certification A	2004/17/ 2.1	16.840.1.113733.1	<無>		
□ 📄 受信任的發行者							
🗄 📄 沒有信任的憑證							
🗉 🧰 第三方根憑證授權單位			-				
□ □ 受信任的人	Micro	soft Management Console	×				
田…■ 您證註冊要求							
	L	您要將主控台設定值儲存到 主控	台1嗎?				
		是(Y) (否(N)) 取消					
					-		
	<u></u>					<u> </u>	

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

六、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。



一、將「網際網路資訊服務(IIS)管理員」開啟。

二、安裝 SSL 憑證

於之前申請憑證網站的站台上按滑鼠右鍵點選「內容」。

🐚 網際網路資訊服務 (IIS) 管理員				_ 🗆 🗙
🐚 檔案 (F) 執行 (A) 檢視 (V) 視	[窗(₩) 説明(H)			_ Ð ×
← → 🗈 🖬 🗙 📽 🖻 😫	😫 💵 💂 🕨 🔳	II		
	Market Contract Contr	····· 路徑	<u> </u>	
爲目前的選取項目開啓內容對話方塊。				

接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

預設的網站 內容 ?
HTTP 標頭 自訂錯誤 ASP_NET
網站 效能 ISAPI 篩選器 主目錄 文件 (目錄安全設定)

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,以滑鼠按下「下一步」

按鈕,開始安裝 Windows 2003 IIS 6.0 伺服器憑證。



接著畫面會到「擱置的憑證要求」視窗,點選「處理擱置要求及安裝憑證(P)」, 以滑鼠按下「下一步」按鈕,開始安裝 Windows 2003 IIS 6.0 伺服器憑證。

IIS 憲證精畫 X X X X X X X X X X X X X X X X X X X
對置的憑證要求 擱置的憑證要求是指憑證授權未回應的要求。
有擱置的馮證要求 您要如何處理? • <u>處理擱置要求及安裝憑證</u> • 励除擱置要求②
<上一步B(下一步M)> 取消

接著畫面會到「處理擱置要求」視窗,點選「瀏覽」選擇存放位置,或直接 在「路徑及檔案名稱(P)」欄位打上路徑及檔案名稱也可以。

■ 計畫: ● 目書: ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
虚理國置要求 藉由擷取含憑證授權回應的檔案來處理憑證擱置要求。
諸輸入含憑證授權回應檔案的路徑及檔名。
路徑及檔案名稱(2):
5:*.cer (瀏覽(R))
<u><上一步(B)</u> 下一步(M) > 取消

如果有按下「瀏覽」,則可選擇檔案路徑及輸入所要開啟的 SSL 伺服器憑證.cer 檔檔名(中華電信通用憑證管理中心(PublicCA)核發的伺服器 SSL 憑證檔名類似 00HD73000000.cer)。輸入完成後,按下「開啟」後,接著 會跳回「處理擱置要求」頁面,並於頁面上出現存放檔案路徑及檔案名稱。

開啓						? ×
查詢(]):	🞯 桌面			•) 🕸 📂 [
	→ 我的文件 → 我的電腦	- 407				
戎猿近的文件	13HD73888	888.cer				
<u>桌面</u> 合						
我的文件						
我的電腦						
網路上的芳鄰						
	檔名(N):	13HD73888	888.cer		•	開啓回
	1111来现空(1):)恋證幅菜(≁.cer)		_	-4X7H

開啟完成後,接著以滑鼠按下「下一步」按鈕。

王 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新
虚理國置要求 藉由擷取含憑證授權回應的檔案來處理憑證擱置要求。
諸輸入含憑證授權回應檔案的路徑及檔名。
路徑及極基条轄住)
C:\Documents and Settings\Administrator\桌面\13HD738888888.cer 瀏覽(R)
<上一步GU 下一步(U) 取消

接著出現「SSL連接埠」頁面,並設定「這個網站應該使用的SSL連接埠(L)」, 請依網站需求自行設定,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精靈	×
SSL 連接埠 為這個網站指定 SSL 連接埠。	
這個網站應該使用的 SSL 連接埠(L):	
	<上一步(B) (下一步(B)) 取消

接著出現「憑證摘要」頁面,確認憑證內容無誤後,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精靈	X		
您已經選擇從回應檔案安 憑證摘要			
若要安裝下列憑證,請打	皮[下一步]。		
檔案名稱: C:\	Documents and Settings\Administrator\13HD73888888.cer		
憑證詳細資訊: 發給 者 到期日 使用目的 好記的名稱 國家司 單位	publicca.hinet.net Public Certification Authority 2016/12/22 伺服器驗證,用戶端驗證 publicca.hinet.net TW 中華電信股份有限公司數據通信分公司 政府網路處		
<上一步(B) 下一步(B) 取消			

接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成匯入憑證.cer 檔動作。



三、透過瀏覽器連線測試網頁 https 是否連線正常。



檢查 SSL 憑證串鏈是否正常。

🍘 https://publicca	a.hinet.net/index.html - Microsoft Internet Explorer	
檔案(E) 編輯(E)) 檢視(Y) 我的最愛(A) 工具(I) 説明(H)	A.
④ 上一頁 → ④	- 🗷 😰 🏠 🔎 搜尋 🧙 裁的最愛 🕢 🔗 - 😓 🚍	
網址① 🕘 https://	/publicca.hinet.net/index.html	▼ ● 移至 連結 ※
It's Work.	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	<u> </u>
	一般 詳細資料 憲證路徑	
	•確保遠端電腦的識別	
	登箱: publicca.hinet.net	
	登行者 : Public Certification Authority	
	有效期自 2013/12/22 到 2016/12/22	
	· · · · · · · · · · · · · · · · · · ·	
	確定	
(二)		✓ ✓ ✓
🍘 https://publicc	a hinet.net/index.html - Microsoft Internet Explorer	-
https://publicca 檔案(P) 編輯(E)	a. hinet. net/index. html - Microsoft Internet Explorer) 檢視(ツ) 我的最愛(A) 工具(T) 說明(H)	_ D × //
 ▲ https://publicc. 檔案匠 編輯匠 ④ 上一頁 → ④ 毎日の ● 	a.hinet.net/index.html - Microsoft Internet Explorer) 檢視(Y) 我的最愛(A) 工具(I) 說明(H) ▼ 图 ② 《 P 搜尋 会我的最爱 经 A S 등	
 https://publice 檔案① 編輯⑥ 上一頁 · ④ 網址② ● https:// 	a. hinet. net/index. html - Microsoft Internet Explorer) 檢視(♡) 我的最愛(A) 工具(I) 説明(II) - ▲ ② 《A 夕 搜尋 ☆ 我的最爱 《 ② - ③ 云 //publicca.hinet.net/index.html	_□×
 https://publice 植案(P) 編輯(E) 上一頁 ・ (D) 網址(D) 新ttps:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer	_□× ♪ ● 移至 連結 ≫
 https://publicc: 檔案(P) 編輯(E) 上一頁 ・ 〇 網址(D) (通) https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer) 檢視(♡)	_□×
 https://publice 植案(E) 編輯(E) 上一頁 、 (2) 網址(D) (2) https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer) 核親(♡ 我的最愛(A) 工具(T) 説明(E) ~ ▲ ② ⑦ ② ⑫ ⑦ 搜尋 ⑦ 我的最爱 ⑧ ◎ ~ ॆ 毫 /publicea. hinet. net/index. html	_□× ▲ ▲ ▲ ▲ ▲
 https://publicc: 檔案(P 編輯(E) 上一頁 · ○ 網址(D) (通) https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer) 校根(Y) 获的最爱(A) 工具(T) 説明(H) ~ ▲ ② 《A 》 搜尋 ☆ 我的最爱 ④ ② - ③ 毫 /publicca. hinet net/index. html	_□×
 https://publice 植案(E) 編輯(E) 上一頁 - ○ 網址(D) ④ https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer ● 檢視(♡)	_□×
 https://publicc: 位案で 編輯(E) 上一頁 · ○ 網址(D) (利用) https:// It's Work. 	a. hinet.net/index.html - Microsoft Internet Explorer) 校硯(Y)	_□×
 https://publice 植案(E) 編輯(E) 上一頁 、 ② 網址(D) ④ https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer ● 核銀(♡) 我的最愛(a) 工具(T) 說明(E) ~ N ② ⑦ ♪ 搜尋 ☆ 我的最爱 ④ ② ~ ③ 副 //publicca. hinet. net/index. html	× ♪ ♪ 移至 連結 >> ♪
 https://publice 植案(P) 編輯(E) 一頁 ~ 〇 網址(D) @ https:// It's Work. 	a. hinet.net/index.html - Microsoft Internet Explorer	_□×
 https://publice 植案(E) 編輯(E) 上一頁 、 ② 網址(D) ④ https:// It's Work. 	a. hinet. net/index. html - Microsoft Internet Explorer ● 校硯(♡) 供的最愛(Δ) 工具(T) 説明(H) P ● ② ⑦ ② ② ② ③ ③ ③ ③ /publicca. hinet.net/index. html	× ♪ ♪ 移至 連結 >>
 https://publice 植案① 編輯② 上一頁 ~ ② 網址② ② https:// It's Work. 	a. hinet.net/index.html - Microsoft Internet Explorer	▲□× ● 移至 連結 >>
 https://publice 植案(E) 編輯(E) 上一頁 、 ② 網址(D) ④ https:// It's Work. 	a. kinet.net/index.html - Microsoft Internet Explorer ☆ 校硯(Y) 鉄的最愛(A) 工具(T) 説明(H) ~ N ② ⑦ ♪ 建尋 ☆ 鉄的最愛 ④ ② ~ ③ ③ /publicca.hinet.net/index.html	× ♪ 予 移至 連結 ≫
 https://publice 植案(P) 編輯(E) 上一頁 ~ ② 網址(D) @ https:// It's Work. 	a. hinet.net/index.html - Microsoft Internet Explorer ● 依根(Y) 我的最要(A) 工具(T) 說明(H) P N 使 按母 会 我的最爱 ② ③ - ③ 毫 /yublicca.hinet.net/index.html	▲□× ● 移至 連結 >>
 https://publice: 檔案(P) 編輯(E) 上一頁 ~ 〇 網址(D) (利用) https:// It's Work. 	a kinet net/index html - Microsoft Internet Explorer	▲□× ▲ ● 移至 連結 >>
 https://publice 植案(P) 編輯(E) 上一頁 ~ ② 網址(D) @ https:// It's Work. 	A kinet net/index.html - Microsoft Internet Explorer ☆ 松硯 (Y) 我的最爱 (A) 工具 (T) 説明 (A) ② ③ ④ ● 複 ② ③ ● ③ ③ /yublicca.hinet.net/index.html	▲□× ● 移至連結 >>
 https://publice: 檔案(P) 編輯(E) 上一頁 ~ 〇 網址(D) (和) https:// It's Work. 	A hinet net/index.html - Microsoft Internet Explorer	▲□× ● 移至 連結 >

🛎 https://publicca.hinet.net/index.html - Microsoft Internet Explorer	. 🗆 🗙
檔案 E 編輯 E 檢視 Y 我的最愛 (A) 工具 I 說明 (H)	-
③ 上一頁 → ③ → 🖹 👔 🏠 🔑 搜尋 👷 裁的最爱 🤣 😥 - 😓 🚍	
網址 ① 🙆 https://publicca.hinet.net/index.html 💽 🄁 移至 🔅	連結 »
It's Work.	*
一般 詳細資料 想證路徑 ■ PKI Root Certification Authority ■ Public Certification Authority ■ publices hinet net 校调:問證(①)	
憑證狀態(3): 這個憑證沒有問題。	
確定	-
▶ ● 完成	

四、依照您的網路架構,您可能需要於防火牆開啟對應 https 的 port。
已安裝過憑證的伺服器,安裝憑證操作步驟

一、將憑證核發的伺服器 SSL 憑證轉換成 P7B 格式的憑證檔。 在 Microsoft Windows 作業系統下,將中華電信通用憑證管理中心 PublicCA 核發的憑證 00HD73000000. cer 以滑鼠點兩下打開。

13HD73888889.cer	2013/12/23 下午 03:25	安全性憑證	5 KB
憑證		×	
一般詳細資料憑證路	<u>2</u>		
[] 憑證資訊			
這個憑證的使用目的如	۱۴ :		
	规则 购自分		
· · · · · · · · · · · · · · · · · · ·	a.hinet.net		
资發者: Public	Certification Authority		
有效期自 2013/	12/ 23 39] 2016/ 12/ 2:	3	
	安裝憑證(I) 簽發	彗聲明(S)	
深入了解聽證			
		確定	

切換至「詳細資料」頁面。

-般 詳細資料 濃證路徑 額示(S): <全部>	•	
欄位	值	
III版本 III序號	V3 00 8e 4d a9 d3 1c 6d 05 eb 96	=
竇簽章演算法	sha1RSA	
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	shal Bublic Contification Anthonia	
[] 煎發者 [] 有效期白	Public Certification Authority, 2013年12月23日下午 03:25:27	
一 有效期到	2016年12月23日下午 03:25:27	-
	編輯內容(E) 複製到檔案(C))
罙入了解 <u>憑證詳細資料</u>		

接著出現「憑證匯出精靈」畫面,於「歡迎使用憑證匯出精靈」點選「下一步」按鈕。



接著出現「匯出檔案格式」畫面,點選「加密編譯訊息語法標準 - PKCS #7

憑證 (. P7B)(C)」,並勾選「如果可能的話,包含憑證路徑中的所有憑證(I)」, 以滑鼠點選「下一步」按鈕。

· 法證匯出精靈· · · · · · · · · · · · · · · · · · ·
匯出檔案格式 憑證可以用多種檔案格式匯出。
諸選取您想要使用的格式:
◎ DER 編碼二位元 X.509 (.CER)(D)
○ Base-64 約4.509 (.CER)(第)
◎ 加密編譯訊息語法標準 - 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 (.PPA)(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)
□ 匯出所有延伸內容(A)
○ Microsoft 序列憑證存放 (.sst)(T)
深入了解 <u>憑證檔案格式</u>
<上一步(LL)下一步(N)> 取消

接著出現「要匯出的檔案」畫面,點選「瀏覽」選擇存放位置,或直接在檔案名稱打上路徑及檔案名稱也可以。

憑證匯出精靈	X
要匯出的檔案 諸指定您要匯出的檔案名稱	
檔案名稱(F):	》覽R)
	<上一步(周) 下一步(ℕ) > 取消

如果有按下「瀏覽」,則可選擇要匯出的檔案路徑及要匯出核發的伺服器 SSL 憑證檔檔名(.P7B)。輸入完成,按下儲存後,接著會跳回「要匯出的檔案」

頁面,並於頁面上出現要儲存的檔案路徑及檔案名稱,並點選「下一步」按 鈕。

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). C:\OpenSSL-Win32\bin\13HD73888889.p7b	瀏覽(R)
	T-+-ML Brit
	1. 52 (M) × 4X/M

接著出現「完成憑證匯出精靈」頁面,按下「完成」以完成伺服器 SSL 憑證檔 (.P7B)匯出動作。

憑證匯出精靈		X
	完成憑證匯出精靈	
	您已經成功地完成憑證 匯出 精 你已指定下列新設定:	·查。
	芯口指定 17月前 設定。 檔案名稱 匯出金鑰 包含憑證路徑中的所有憑證 檔案格式	C:\OpenSSL-Win32\bi 否 是 加密編譯訊息標準語
	< III	4
	《上一步砚】	完成 取消

匯出完成,會出現如下訊息「匯出成功」訊息。

	完成憑證匯出精靈	
	您已經成功地完成憑證匯出精 您已指定下列新設定:	ञ. ·
(BI	檔案名稱 匯出金鑰 包含憑證路徑中的所有憑證 橫案格式 聲匯出精靈	C:\OpenSSL-Win32\bi 否 是 加密編譯訊息標準語
E	匪 出成功。	Þ
L	<u>確定</u> (上一步(B)	

二、使用 OpenSSL 將產製請求檔匯出的金鑰及憑證取出金鑰,及與新核發的憑證 結合為. pfx 檔。

接著使用 Windows OpenSSL 將產製請求檔匯出的金鑰及憑證取出金鑰,此時 會需要匯出私密金鑰及憑證檔. pfx 檔的密碼。 指令: openssl pkcs12 -in filename.pfx -out filename.pem 範例: openssl pkcs12 -in publicca_ReqBackup.pfx -out publicca_ReqBackup.pem

指令:

openssl rsa -in filename.pem –out filename.key 範例: openssl rsa -in publicca_ReqBackup.pem –out publicca_ReqBackup.key



將上面所匯出的憑證檔(.P7B)檔案轉成 Base64 格式。

指令:

openssl pkcs7 -in filename.p7b inform DER -print_certs -out filename.pem 範例:

openssl pkcs7 -in 13HD73888889.p7b inform DER –print_certs –out 13HD73888889.pem

將取出的請求檔金鑰與新核發憑證結合為私密金鑰及憑證檔.pfx 檔, 並設定好密碼。

指令:

openssl pkcs12 -export -in filename.pem -inkey filename.key –out filename.pfx 範例:

openssl pkcs12 -export -in 13HD73888889.pem -inkey publicca_ReqBackup.key -out publicca_ReqBackup.pfx



三、移除舊私密金鑰及憑證,及將結合後的私密金鑰及憑證匯入要安裝的 Windows 2003 IIS 6.0 伺服器。



將「網際網路資訊服務(IIS)管理員」開啟。

於要申請憑證網站的站台上按滑鼠右鍵點選「內容」。

🀚 網際網路資訊服務 (IIS) 管理員			
🐚 檔案(E) 執行(Δ) 檢視(V) 視窗(W) 說明(H)			_ & ×
	▶ ■ Ⅱ		
● ●	下 路徑 itm	狀況	
客日前的避斯道日期愍 <u>肉</u> 恋耕 <u>新</u> 古神。			
(简单的1000000000000000000000000000000000000			J.

接著將頁面切到「目錄安全設定」頁面。在「目錄安全設定」頁面,以滑鼠按下「伺服器憑證」按鈕。

顧設的網站 內容 ? ×
HTTP 標頭 自訂錯誤 ASP NET
──網站 │ 效能 │ ISAPI 篩選器 │ 主目錄 │ 文件 ──目錄安全設定 〉
驗證及存取控制 啓用匿名存取,並編輯這個資源的驗 證方法。
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
安全通訊
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 檢視憑證(V)
編輯(D)
確定 取消 雲用(益) 説明

接著畫面會到「歡迎使用網頁伺服器憑證精靈」視窗,以滑鼠按下「下一步」 按鈕,開始安裝 Windows 2003 IIS 6.0 伺服器憑證。



接著出現「修改目前的憑證指派」頁面,選擇「移除目前的憑證」,接著按 下「下一步」。

王 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新 新
修改目前的憲證指派 目前安裝在此網站的憑證。
您想要如何處理目前安裝的憑證?
○ 更新目前的憑證(₩)。
● 移除目前的應證(R)。
C 取代目前的應證(△)。
○ 匯出目前的憑證到 .pfx 檔案(ऱ)
○ 複製或移動目前的憑證到遠端伺服器網站(C)
<上一步图(下一步图)> 取消

接著出現「移除憑證」頁面,頁面上會顯示目前憑證的詳細資訊,請務必執 行之前的私密金鑰及憑證備份後,才可執行此步驟移除憑證,否則憑證一移 除,將無法救回,接著按下「下一步」。



接著出現「正在完成網頁伺服器憑證精靈」頁面,按下「完成」以完成刪除 憑證動作。



回到「預設的網站」「內容」畫面,接著再按下「伺服器憑證」按鈕。

預設的網站 內容 ? ×
HTTP 標頭 自訂錯誤 ASP NET 網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定
驗證及存取控制 啓用匿名存取,並編輯這個資源的驗 證方法。 編輯(E)
IP 位址及網域名稱限制 使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。
編輯① 安全通訊
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 檢視應證(2) 編輯(1)
確定 取消 套用(点) 説明

再次開啟「歡迎使用網頁伺服器憑證精靈」視窗畫面,以滑鼠按下「下一步」 按鈕,開始匯入「產製請求檔匯出的金鑰及憑證所取出金鑰與新核發的憑證 結合的.pfx 檔」。



接著畫面會到「伺服器憑證」視窗,以滑鼠點選「從.pfx 檔案匯入憑證(M)」, 接著以滑鼠按下「下一步」按鈕。

X 量材電気 211
伺服器整整 這些是指派憑證到網站的方法。
諸選取您想要用於此網站的方法:
 ○ 従金鑰管理員備份檔案匯入憑證(①)。 ○ 従 pfx 檔案匯人憑證(M)
○ 從遠端伺服器網站複製或移動憑證到此網站(型)
<上─步(B) 下─步(B) 取消 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

接著出現「匯入檔案」頁面,點選「瀏覽」選擇存放位置,或直接在檔案名稱打上路徑及檔案名稱也可以。

★ 211
隆入憲證 您可以從.PFX 檔匯入憑證。
請輸入包含憑證的檔案名稱及路徑。
路徑及檔案名稱(P):
■ 23% pfx (瀏覽 R))
指定在匯入後,匯入的憑證是否應標示為可匯出。將憑證標示為可匯出將具有 較高的安全風險,不過,它可允許憑證匯出到檔案進行備份。 □ 將憑證標示為可匯出(M)
<上一步(B) 下一步(A) > 取消

按下「瀏覽」,則可選擇檔案路徑及選擇私密金鑰與憑證.pfx 檔檔名。選 擇完成後,按下「開啟」後,接著會跳回「匯入憑證」頁面,並於頁面上出

開啓						? ×
查詢(]):	🞯 桌面		-] 🕝 🖄	• 🖽	
ました 我最近的文件 で 点面 の 文件	● 我的文件 ● 我的電腦 ● 網路上的芳約 ● 15ftD738888 ● publicca_Req	f 38.pfx Backup.pfx				
我的電腦 (1) 網路上的芳鄰						
	檔名(N):	publicca_ReqF PFX 檔 (*.pfx	Backup.pfx			開啓()) 取消

現私密金鑰及憑證.pfx 檔檔案路徑及檔案名稱。

輸入完成後,並勾選「將憑證標示為可匯出(M)」,接著以滑鼠按下「下一步」按鈕。

■ 計畫書 211
匯入憲證 您可以從.PFX 檔匯入憑證。
諸輸入包含憑證的檔案名稱及路徑。 路徑及檔案名稱A
C:\Documents and Settings\Administrator\桌面\publicca_ReqBackup. 》瀏覽(R)
指定在匯入後,匯入的憑證是否應標示為可匯出。將憑證標示為可匯出將具有 較高的安全風險,不過,它可允許憑證匯出到檔案進行備份。 ————————————————————
▼ 將违證標示為可匯出(M)
<上一步(B) (下一步(M)> 取消

接著出現「匯入憑證密碼」頁面,輸入保護私密金鑰的密碼。

IIS 憲證精靈		×
匯入燕證密碼 您必須提供密碼以匯入憑證。		
諸為您想要匯入的憑證輸入密碼。		

	<上一步围 下一步10 >	取消

接著出現「SSL連接埠」頁面,並設定「這個網站應該使用的SSL連接埠(L)」, 請依網站需求自行設定,接著以滑鼠按下「下一步」按鈕。

IIS 憲證精畫		×
SSL 連接埠 爲這個網站指定 SSL 連接埠。		
适面網站應該使用的 SSL 連接埠(止):		
	<上一步()下一步(Q)>)	取消

接著出現「已匯入憑證的摘要」頁面,確認憑證內容無誤後,接著以滑鼠按 下「下一步」按鈕。



接著畫面會到「正在完成網頁伺服器憑證精靈」視窗,按下「完成」後,即 完成匯入私密金鑰及憑證.pfx 檔動作。



透過瀏覽器連線測試網頁 https 是否連線正常。

🖉 about:blank - Microsoft Internet Explore	Ħ	_ 🗆 🗙
檔案(E) 編輯(E) 檢視(Y) 我的最愛(A)	工具(I) 說明(H)	1
③ 上一頁 → ⊙ → 🖹 🔰 🏠 🔎 搜尋	📩 我的最爱 🛛 🙆 - 💺 🕞	
網址D 🔊 https://publicca.hinet.net/index.html	<u> </u>	🔁 移至 連結 »
	(1) 您即將透過安全性連線檢視畫面。	
	《一》網路上的任何人,都無法查閱您和這個網站交換的 任何資訊。	
	□ 以後不顯示這個警告(1)	
	「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	
		-
🛃 完成	一 () () () () () () () () () (祭網路 //
-		
https://publicca.hinet.net/index.html - M	icrosoft Internet Explorer	
★ https://publicca.hinet.net/index.html - M 檔案 (L) 編輯 (L) 被視(V) 我的最愛(L)	icrosoft Internet Explorer 工具① 説明任 	_
 ▶ https://publicca.hinet.net/index.html - M 檔案 (P) 編輯 (E) 被視 (V) 我的最愛 (A) ○ 上一頁 + ○ + ▲ ② ☆ / 伊尋 網址(D) ⑧ https://publicca.hinet.net/index.html 	icrosoft Internet Explorer 工具① 説明⑪ <mark>会我的最爱 ❷</mark> ❷- ॆ ■	_□× <i>靴</i> ● 移至 連結 ≫
 https://publicca.hinet.net/index.html - M 檔案(P) 編輯(E) 校親(Y) 我的最愛(A) 上一頁 + 〇 + 王 ② ふ ク 提尋 網址(D) 圖 https://publicca.hinet.net/index.html 	icrosoft Internet Explorer 工具① 説明① 会 我的最愛 ② ② - ③ IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	_ □ × 》 移至 連結 »
 https://publicca.hinet.net/index.html - M 檔案 (上) 編輯 (正) 故親 (平) 我的最愛 (金) 上一頁 - 〇 - 王 (金) (二) 提尋 網址 (四) (金) https://publicca.hinet.net/index.html It's Work. 	icrosoft Internet Explorer 工具① 説明① ☆ 我的最爱 ② ② - 📚 🚍	_□X 】 ● 移至 連結 >
 https://publicca.hinet.net/index.html - M 檔案(E) 線輯(E) 校親(Y) 我的最愛(A) 上一頁 - 〇 - 区 〇 〇 / 建尋 網址(D) 〇 https://publicca.hinet.net/index.html It's Work. 	icrosoft Internet Explorer 工具① 説明①	_□×
 https://publicca.hinet.net/index.html - M 檔案 (上) 編輯 (正) 彼視 (①) 我的最愛(点) 上一頁 - 〇 - 区 (2) (小) 伊建 網址(①) (1) https://publicca.hinet.net/index.html It's Work. 	iicrosoft Internet Explorer 工具① 説明任) ☆ 我的最爱 ④ 🔗 - 🚴 🚍	_□×
★ https://publicca.hinet.net/index.html - M 檔案 (上) 編輯 (上) 依親 (① 我的最愛 (▲)) 上一頁 - ○ - ○ ② ⑦ ② ⑦ 2 提尋 網址 (①) ⑥ https://publicca.hinet.net/index.html It's Work.	icrosoft Internet Explorer 工具① 説明④ ☆ 我的最爱 ❷ ❷ ● 疑 ₪ ▼	_□× 》 ● 移至 連結 ≫
https://publicca.hinet.net/index.html - M 檔案E 編輯E 被視() 我的最愛() 上一頁 - 〇 - 図 ② ふ シ 捜尋 網址印 @ https://publicca.hinet.net/index.html It's Work. Internet Explorer Microsoft I	iterosoft Internet Explorer 工具① 説明① ☆ 我的最愛 ④ ② - ऄ I ☑ ✓ Internet Explorer 的增強式安全性設定目前已經在您的伺服器上啓用了。此	_□×
https://publicca.hinet.net/index.html - M 檔案E 編輯E 被視() 我的最愛() こ上一頁 - こ - こ こ こ へ 児母 網址() 資 https://publicca.hinet.net/index.html It's Work.	iterosoft Internet Explorer 工具① 説明④ ☆ 我的最愛 ② ② ・ ③ ₪ ✓	_□× ♪ ● 移至 連結 >
https://publicca.hinet.net/index.html - M 檔案(P) 編輯(E) 核視(Y) 我的最愛(A) 上一頁 - 〇 - 王 ② ふ ♪ 搜尋 網址(D) 資 https://publicca.hinet.net/index.html It's Work. Internet Explorer 反全性響 確認示,	icrosoft Internet Explorer 工具① 説明④ ☆ 裁的最愛 ② ② ・ ③ ■ ✓	_□× 】 ● 移至 連結 ≫
★ https://publicca.hinet.net/index.html - M 檔案 E 編輯 E 檢視 ① 我的最愛 (A) ● 上一頁 - ○ - ■ ② ⑦ ♪ 搜尋 網址 ① ④ https://publicca.hinet.net/index.html It's Work.	Iternet Explorer 工具①<説明④	_□× ♪ ● 移至 連結 >>
★ https://publicca.hinet.net/index.html - M 檔案 医 編輯 医 被視 ⑦ 我的最愛 ④ ● 上一頁 - ○ - ≥ ② ⑦ ♪ 搜尋 網址 ① ⑧ https://publicca.hinet.net/index.html It's Work.	icrosoft Internet Explorer 工具① 説明④ ☆ 我的最爱 ② ② ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	_□× ♪ ● 移至 連結 >>
 ▲ https://publicca.hinet.net/index.html - M 檔案 (E) 編輯 (E) 核視 (Y) 我的最愛(A) 上一頁 - ○ - ○ ○ 梁 (A) > 搜尋 網址(D) @ https://publicca.hinet.net/index.html It's Work. 	iterosoft Internet Explorer 工具① 説明④ ☆ 我的最愛 ④ ◎・ 》 ■ ✓	_□× ♪ 移至 連結 > ▲
★ https://publicca.hinet.net/index.html - M 檔案 匠 編輯 匠 檢視 ① 我的最愛 ④ ▲ 上一頁 ~ ② ~ 값 ② ⑦ ♪ 搜尋 網址 ① ④ https://publicca.hinet.net/index.html It's Work. It's Work. Internet Explorer ※ 盤 / / / / / / / / / / / / / / / / / /	iterosoft Internet Explorer 工具① 説明田 ☆ 我的最愛 ④ ②- ③ ■ ✓ Internet Explorer 的増強式安全性設定目前已經在您的伺服器上啓用了。此 達式等級可以降低受到危險網站內容攻擊的風險,可是它可能妨礙網站正 並限制存取網路資源。 要顯示這個訊息① Explorer 的增強式安全性設定的詳細資訊 確定	 □ × ♪ 秒 秒 秒 ● ●
★ https://publicca.hinet.net/index.html - M 檔案 ① 編輯 ② 被視 ② 我的最愛 ④ ● 上一頁 ~ ③ ~ ≥ ② ⑦ ♪ 搜尋 網址 ② 圖 https://publicca.hinet.net/index.html It's Work.	iterosoft Internet Explorer I具① 説明④ ☆ 我的最爱 ② ③- ◎ ■ Internet Explorer 的増強式安全性設定目前已經在您的伺服器上啓用了。此 建式等級可以降低受到危險網站內容攻擊的風險,可是它可能妨礙網站正 並限制存取網路資源。 	 _□ × ♪ 移至 連結 >
 ▲ https://publicca.hinet.net/index.html - M 檔案 (E) 編輯 (E) 檢視 (Y) 我的最愛(A) ○ 上一頁 - ○ - ○ ○ ○ ○ ○ ○ ○ ○ 伊建章 網址(D) ④ https://publicca.hinet.net/index.html It's Work. 	正具① 説明④ ☆ 我的最愛 ④ ◎・ ◎ ■ ● ◎・ ◎ ■ ●	 ■ × ● ●
★ https://publicca.hinet.net/index.html - M 檔案 匠 編輯 匠 檢視 ① 我的最愛 ④ ▲ 上一頁 ~ ② ~ 값 ② ⑦ ♪ 搜尋 網址 ① ④ https://publicca.hinet.net/index.html It's Work. It's Work. Internet Explorer ※ 登書 增調示 ? · · · · · · · · · · · · · · · · · · ·	iterosoft Internet Explorer 工具① 説明④ ☆ 我的最愛 ② ② ● ● ● ■ ● ■ witermet Explorer 的増強式安全性設定目前已經在您的伺服器上啓用了。此 培式等級可以降低受到危險網站內容攻擊的風險,可是它可能妨礙網站正 並限制存取網路資源。 要顯示這個訊息① Explorer 的增強式安全性設定的詳細資訊 確定	 _□× ♪ 秒 秒 秒 秒 0 0
★ https://publicca.hinet.net/index.html - M 檔案 ① 編輯 ② 故親 ③ 我的最愛 ④ ● 上一頁 - ○ - ▲ ② ⑦ ♪ 搜尋 網址 ② ● https://publicca.hinet.net/index.html It's Work.	iterosoft Internet Explorer I具① 説明④ ☆ 我的最爱 ② ③- ◎ ■ ■ (*) internet Explorer 的増強式安全性設定目前已經在您的伺服器上啓用了。此 達式等級可以降低受到危險網站內容攻擊的風險,可是它可能妨礙網站正 並限制存取網路資源。 要顯示這個訊意① Explorer 的増強式安全性設定的詳細資訊 確定	 ▲ ▲ ● ●
★ https://publicca.hinet.net/index.html - M 檔案匠 編輯 函 被視 ⑦ 我的最愛 ④ ● 上一頁 ~ ○ ~ ≥ ② ⑦ ♪ 搜尋 網址 ① ● https://publicca.hinet.net/index.html It's Work.	正具① 説明④ ☆ 我的最愛 ④ ○・ ▷ □ ○ ★ ● </td <td> ■ ● ●</td>	 ■ ● ●
★ https://publicca.hinet.net/index.html - M 檔案匠 編輯匠 被視() 我的最愛() 上一頁 - ○ - ≥ ② ⑦ ♪ 搜尋 網址() 圖 https://publicca.hinet.net/index.html It's Work.	正具① 説明④ ★教的最愛 	 □ × ● 移至 連結 >>

檢查 SSL 憑證串鏈是否正常。

🛎 https://publicca.hine	et.net/index.html - Microsoft Internet Explorer	
檔案(E) 編輯(E) 檢	視(型) 我的最愛(鱼) 工具(Ⅱ) 說明(⊞)	27
④上─頁 - ● - ▼] 🔝 🐔 🔎 搜尋 👷 我的最爱 🔗 🔗 😓 🚍	
網址D) (色 https://public	a hinet.net/index.html	▼ ▶ 移至 ▶ 連結 >
It's Work.		<u> </u>
	馬資靈臺	
	這個熟證的使用目的如下:	
	◆ 確は不过逐漸電低超力/設改力/	
	登給: publicca.hinet.net	
	四行书· Dublis Cartification Anthonity	
	<u>E</u>11-<u>H</u>: Fuenc Cermication Automy	
	有效期自 2013/12/22 到 2016/12/22	
	安装港道① 登行者聲明(3)	
-]	
JE134		
🝘 https://publicca.hine	et.net/index.html - Microsoft Internet Explorer	
Attps://publicca.hine 檔案(P) 編輯(E) 檢	et.net/index.html - Microsoft Internet Explorer 視(ツ) 我的最愛(<u>A</u>) 工具(I) 説明(H)	
 ▲ https://publicca.hind 檔案 (P) 編輯 (E) 檢 ③ 上一頁 → ④ → ▲ 	et.net/index.html - Microsoft Internet Explorer 視(V) 我的最愛(A) 工具(I) 說明(H)) 😰 🏠 🔎 搜尋 🧙 我的最爱 🤣 🎯 - 😓 🚍	
 https://publicca hind 檔案E 編輯E 被 上一頁 · · · × 網址D https://publica 	et.net/index.html - Microsoft Internet Explorer 視(V) 我的最愛(A) 工具(T) 說明(H) ② ⑦ / 2 搜尋 ☆ 我的最爱 ② ② - ③ 忌 cca.hinet.net/index.html 题词 ② (X)	_□×
 https://publicca.hing 檔案(E) 編輯(E) 校 上一頁 ~ 〇 ~ 区 網址(D) (E) https://public It's Work. 	et.net/index.html - Microsoft Internet Explorer 	_□×
 https://publicca.hind 檔案(E) 編輯(E) 校 上一頁 ~ ④ ~ 区 網址(D) ⑥ https://public It's Work. 	et.net/index.html - Microsoft Internet Explorer 親(文) 我的最愛(A) 工具(T) 說明(H) ② 〈〉 〉 搜尋 〈 我的最爱 〈 〉 〉 ② cca.hinet.net/index.html 慧慧 一般 詳細資料 憑證路徑 振識路徑	_□× 》 ▼ 予移至 連結 »
 https://publicca.hind 檔案 (E) 編輯 (E) 校 上一頁 ~ 〇 ~ 区 網址 (D) (E) https://public It's Work. 	et.net/index.html - Microsoft Internet Explorer 	_□×
 https://publicca.hind 檔案(E) 編輯(E) 校 上一頁 - ③ - 区 網址(D) https://publicca.hind It's Work. 	et.net/index.html - Microsoft Internet Explorer 親(文) 我的最愛(A) 工具(T) 說明(H) P 搜尋 ☆ 我的最爱 @ @ ↓ ↓ cca.hinet.net/index.html 禁之 一般 詳細資料 憑證路徑 ● #KI Root Certification Authority ● PkII Root Certification Authority ● Public Certification Authority ● Public Certification Authority	_□× 》 ▼ 予 移至 連結 »
https://publicca.hind 檔案匠 編輯匠 被 ③上一頁 ~ ③ ~ ※ 網址① ④ https://public It's Work.	et. net/index. html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(T) 說明(H) ② 《 》 搜尋 ☆ 我的最爱 ④ ② • ③ ② sca.hinet net/index. html 集章 ? X 一般 詳細資料 憑證路徑 ◎ eFKI Root Certification Authority ◎ eFKI Root Certification Authority ◎ Public Certification Authority ◎ Public certification Authority	_□× ♪ ▼ 予移至 連結 >> ▲
 https://publicca.hind 檔案(E) 編輯(E) 校 上一頁 - ③ - 区 網址(D) 資 https://public It's Work. 	et.net/index.html - Microsoft Internet Explorer 現(文) 我的最愛(A) 工具(T) 説明(H) ② ⑦ ♪ 搜尋 ☆ 我的最爱 @ @ ♪ & Exa.hinet net/index.html	× ♪ ↓ ♪ 移至 連結 »
https://publicca.hind 檔案E 編輯E 被 ・上一頁 - ・ 、 網址D 管 https://public It's Work.	et. net/index. html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(I) 說明(H) ② 《 》 搜尋 《 我的最爱 ④ ②	× ♪ ▼ 予移至 連結 >> ▲
 https://publicca.hind 檔案(E) 線輯(E) 校 上一頁 - 〇 - 区 網址(D) 創 https://public It's Work. 	et net/index.html - Microsoft Internet Explorer 現(文) 我的最愛(A) 工具(T) 說明(H) ② ⑦ ♪ 搜尋 ☆ 我的最爱 @ ② - & 毫 Exca.hinet net/index.html 等意	× ♪ ↓ ♪ 移至 連結 »
https://publicca.hind 檔案E 編輯E 被 ・上一頁 ~ ~ ~ 網址D 資 https://public It's Work.	et net/index.html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(I) 說明(H) ② 《 》 搜尋 《 我的最爱 《 ② 《 》 ③ ② cca.hinet.net/index.html 集記 ? X - 般 詳細資料 憑證路徑 『 ##Warey Public Certification Authority 『 Public Certification Authority 『 Public Certification Authority	× ♪ ▼ ● 移至 連結 >>
 https://publicca.hind 檔案匠 編輯 (E) 校 上一頁 ~ 〇 ~ 区 網址(D) ④ https://public It's Work. 	et net/index.html - Microsoft Internet Explorer 課(♡ 我的最愛(A) 工具(T) 説明(E) ② ⑦ ₽ 搜尋 ☆ 我的最爱 @ @ • \$ 2 ***********************************	× ♪ ● 移至 連結 ≫
 https://publicca.hing 檔案(E) 線輯(E) 被 上一頁 ~ ③ ~ ※ 網址(D) 會 https://public It's Work. 	et net/index.html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(I) 説明(II) ② ② ② P 搜尋 会 我的最爱 ② ② ● ③ ② cca.hinet.net/index.html 要求 ? X - 般 詳細資料 憑證路徑 『 eFKI Root Certification Authority 『 @ Public Certification Authority 『 @ Publics hutetmet]	× ♪ ▼ 予 移至 連結 ≫
https://publicca.hind 檔案匠 編輯匠 被 ③上一頁 ~ ③ ~ 網址① ④ https://public It's Work.	et net/index.html - Microsoft Internet Explorer 現(文) 我的最愛(A) 工具(T) 説明(D) ② ⑦ ② 按尋 ☆ 我的最爱 ② ② ● ③ ② Exa.hinet net/index.html	▲
 https://publicca.hing 植家田 編輯 (E) 被 上一頁 ~ > ~ × 網址(D) (E) https://public It's Work. 	et net/index.html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(I) 説明(II) ② ② P 搜尋 会 我的最爱 ② ② ● ③ ② Exa.hinet.net/index.html 要求 2 × ● 傑 詳細資料 憑證路徑 ● eFKI Root Certification Authority ● Public Certification Authority ● Public Certification Authority ● Publices.hinet.net(I) ● With the the the the the the the the the t	▲
https://publicca.hind 檔案匠 編輯匠 被 ③上一頁 ~ ③ ~ ※ 網址① ④ https://public It's Work.	et net/index.html - Microsoft Internet Explorer 現(文) 我的最愛(山) 工具(①) 説明(①) ② ① ② 按尋 ☆ 我的最爱 ② ② ○ ③ ② ② Sca.hinet net/index.html	▲
 https://publicea.hing 植家田 編輯 (E) 被 上一頁 · · · · · 網址 (D) (A) https://public It's Work. 	et net/index.html - Microsoft Internet Explorer 現(Y) 我的最愛(A) 工具(I) 説明(II) ② ③ ♪ 搜尋 ☆ 我的最爱 ④ ② - ③ ② cca hinet net/index.html 要求	▲ 】 × ● ● 移至 連結 > ●

以上動作即完成 Windows 2003 IIS 6.0 重新產製金鑰狀況下,安裝伺服器 SSL 憑證檔動作。

四、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:單一 IP 多網域憑證安裝步驟

IIS 6 在只有一個 IP 的情況下,預設只能有一個網站使用 443 port。依照以下 步驟操作,即可在多個網站上安裝多網域憑證。

一、先在第一個站台安裝好憑證,範例使用站台為 multidomainl

二、開啟 IIS 管理員,確認站台識別元。

🍿 網際網路資訊服務 (IIS) 管理	£員			_ 🗆	×
👣 檔案(E) 執行(<u>A</u>) 檢視(V)	視窗(₩) 説明(<u>H</u>)			_ 5	×
← → 🗈 🖪 😭 🛱	😫 💂 ▶ 🔳 🗉	\frown			
 網際網路資訊服務 ♥M-63D1FZIPKECF (本機 ● ● 應用程式集區 ● ● 預支的網站 (已停. ● ● 預支的網站 (已停. ● ● 預支的網站 (已停. ● ● 預支的網站 (正停. ● ● 預支的網站 (正停. ● ● 預支的網站 (正停. ● ● 預支的網站 (正停. 	描述 愛 預設的網站 (已停止) multidomain1 multidomain2	1 1 1437980989 1437980990	<u>狀態</u> 已停止 執行中 執行中	主機標頭值 www.md1.com.tw www.md2.com.tw	
	<u>↓</u>				▶

三、開啟命令提示字元

切換至 cd C:\Inetpub\AdminScripts 目錄

執行:

cscript adsutil.vbs set /w3svc/站台識別元/SecureBindings ":443:站台1FQND"

🗈 命令提示字元	
Microsoft Windows [版本 5.2.3790]	
<c>版權所有 1985-2003 Microsoft Corp。</c>	
C:\Documents and Settings\Administrator>cd	
C:\Documents and Settings>cd	
C:∖>cd Inetpub	
C:\Inetpub>cd AdminScripts	
C:\Inetpub\AdminScripts>cscript adsutil.vbs set /w3svc/1437980989/SecureBin ":443:www.md1.com.tw" Microsoft (R) Windows Script Host Version 5.6 Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.	dings
SecureBindings : (LIST) ":443:www.md1.com.tw"	
C:\Inetpub\AdminScripts>	

四、於第2個站台安裝多網域憑證。

🌘 洞際網路資訊服務 (IIS) 管理員	Ę				_ & ×
🧐 檔案(E) 執行(<u>A</u>) 檢視(V) :	視窗(W) 說明(H)				_ 8 ×
← → 🗈 🔟 🗡 😰 💀	3 😫 是 🕨	■ II			
 網際網路資訊服務 ▼M-63D1FZIPKECF(本供 ● ● 應用程式集區 ● ● 網站 ● ● 細站 ● ● 細切 ● ● 一個 ● ● 一個 ● ● 一個 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	A稱 i isstart_htm index.htm pagerror.gif 備(①) 限(①))))))))))))))	路徑	兆大;	₽	

multidomain2 內容	? ×
網站 效能 ISAPI 篩選器 主目錄 文件 目錄安全設定 HTTP 標頭 自訂錯誤	
□ 驗證及存取控制	
啓用匿名存取,並編輯這個資源的驗 證方法。 編輯 (E)	
IP 位址及網域名稱限制	
使用 IP 位址或網際網路網域名稱來授予 或拒絕到這個資源的存取。	
安全通訊	
當存取這個資源時使用安全通訊並啓 用用戶端憑證。 校硯憑證(V)	>
編輯(D)	
歡迎使用網頁伺服器憑證精靈。	×
歡迎使用網頁伺服器憑證精 靈	È 1
此精靈將協助您建立及管理用在介於伺服器及用戶端安全網頁通訊間的伺服器憑證。	
您的網頁伺服器狀態: 您的網頁伺服器沒有安裝憑證且您沒有任何擱 置要求。憑證精靈將協助您建立此網頁伺服器 的新憑證或附加已有的憑證。	
請按 [下一步] 來繼續。	
<上一步B(下一步做)	取消





IIS 憲證精畫	×
SSL 連接埠 為這個網站指定 SSL 連接埠。	
這個網站應該使用的 SSL 連接埠(L): 1993	
<上一步图 下一步创 >	取消
IIS 巻身括業	X
憲證摘要 您已經選擇安裝已存在的憑證。	
下列憑證可用來安裝在您的網頁伺服器上。若要安裝此憑證,諸按 [下一步]。	
 憑證詳細資訊: 發給 www.md1.com.tw 發照者 Public Certification Authority 到期日 2019/3/18 好記的名稱 multidomain 國家/地區 TW 域市 Taipei 公司 中華電信股份有限公司數據分公司 單位 政府網路處 	
<上一步围(下一步10)>	取消



五、執行 SecureBindings 指令

cscript adsutil.vbs set /w3svc/站台識別元/SecureBindings ":443:站台 2FQND"



六、至此兩個站台已安裝多網域憑證,可使用瀏覽器連線試試。