## 中華電信通用憑證管理中心 (PublicCA)

Windows IIS 7.0 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 7.0 SSL 憑證請求檔製作手冊	2
Windows IIS 7.0 SSL 憑證安裝操作手冊	5
附件一:設定 SSL 安全通道的加密強度	19
附件二:單一 IP,多站台啟用 SSL	28

## Windows IIS 7.0 SSL 憑證請求檔製作手冊

一、點選「開始」「系統管理工具」「Internet Information Services (IIS)
 管理員」

- 何服器管理員			X
檔案(F) 執行(A) 檢視(V) 說明(H)			
🧇 🔿 🔁 🚾 🛛 😰			
<ul> <li>Internet Explorer</li> <li>Windows Update</li> <li>Windows 運路人</li> <li>Extras 及升級</li> <li>新給管理工具</li> </ul>		的網頁應用程式基礎結構。	
🚡 附屬應用程式	user		-
■ 取動	文件		
	電腦		
	網路	SCSI 較動器	
	控制台	<ul> <li>Windows Server Backup</li> <li>工作排程器</li> </ul>	
	糸統管理工具 ▶	▲ 元件服務	
	說明及支援		
		一 共用與存放管理	
	執行	→ 安全性設定精靈	
		10.服菇官注意 27. 条统设定	
		▲ 事件檢視器	
		▲ 目有進階安全性的 Windows 防火牆	
▲ 上一頁			-
開始搜尋	<b>○ ● →</b>	記憶體診斷工具	
	蹤器 🛛 🚠 伺服器管	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	🔤 🏚 🕞 🦙 下午 01:20

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」



三、點選「建立憑證要求」

🍹 Internet Information Services (IIS) 管理	뤚	_ 8 ×
🌀 🕥 📲 🕨 WIN-GIGVLP9ICXU 🔸		🖸 🗠 🟠 I 🖉 🗸
檔案(F) 檢視(V) 說明(H)		
<ul> <li>建結網頁</li> <li>● WIN-GIGVLP9ICXU (WIN-GIGVLP9ICXU (WIN-GIGVLP9ICXU))</li> <li>● 應用程式集區</li> <li>● ● ◎ 站台</li> </ul>	<ul> <li>● 同服器憑證</li> <li>些功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站路能使用的憑證。</li> <li>▲稱 ▲ 發行給</li> <li>▲</li> <li>● 發行給</li> </ul>	<ul> <li>勤作</li> <li>匯入</li> <li>建立憑證要求</li> <li>建立網域憑證</li> <li>建立自我簽署憑證</li> <li>② 說明 線上說明</li> </ul>

四、輸入以下所有欄位資料,輸入完成後點點選「下一步」

要求憑證 分辨名稱屬	性	<u>? x</u>
指定憑證的必要資訊。省( 一般名稱(M): 組織(O): 組織單位(U): 縣市/位置(L) 省份(S): 國家 (地區)(R):	份及縣市/位置必須指定成正式名稱,而且不能包含縮寫。 www.test.com.tw CHT ValueAdd Taipei none TW ▼	
	上一步(P) 下一步(N) 完成(F) <b>取</b>	び肖

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	<u>? ×</u>
<b>密碼編譯服務提供者內容</b>	
選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度 越大,安全性就越高。不過,位元長度較大可能會降低效能。 密碼編譯服務提供者(S): Microsoft RSA SChannel Cryptographic Provider ● 位元長度(B): 2048	
上一步(P) 下一步(N) 完成(F) 取	消

六、指定要儲存憑證請求檔檔案名稱與存放位置,確認後點選「完成」。

要求憑證		<u>? ×</u>
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。	
指定憑證要求的檔案名稱(R):		
C:\certreq.txt		
	上一步(P) 下一步(A) 完成(P	7) 取消

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 7.0 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。
  - 2. 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、點選「開始」→「系統管理工具」→「Internet Information Services (IIS) 管理員」。

🛼 伺服器管理員			
檔案(F) 執行(A) 檢視(V) 說明(H)			
🗢 🔿   🖄 📰 🛛 🚺			
<ul> <li>Internet Explorer</li> <li>Windows Update</li> <li>Windows 連絡人</li> <li>Extras 及升級</li> </ul>	<u>r</u>	的網頁應用程式基礎結構。	
퉬 系統管理工具 퉬 附屬應用程式	user		-
▶ 散動 ▶ 維護	文件		
	電腦	<ul> <li>終端機服務</li> <li>▶</li> <li>▶</li> <li>Particular</li> <li>Particular<td># </td></li></ul>	# 
	網路	★ KCSI 取動器	
	控制台	<ul> <li>Windows Server Backup</li> <li></li></ul>	
	条統管理工具 ▶	🧆 元件服務 🞯 可靠性和效能監視器	
	說明及支援	→ 本機安全性原則 分 共用與存放管理	
	執行	3. 5 km/km/km/km/km/km/km/km/km/km/km/km/km/k	
		🚽 存放裝置總管 📑 伺服器管理員	
		☑ 糸統設定	
◆ 上一頁		■ 具有進階安全性的 Windows防火牆 ③ 服務	•
開始搜尋	0	■ 記憶體診斷工具	
🥂開始 🛛 🏭 💻 🔰 🗔 關機事件追	蹤器 🛛 🛓 伺服器管	≦ 資料來源 (ODBC) ▲ 電腦管理	📄 🕡 🌔 🚺

四、點選主機連線預設名稱,再點選畫面右邊「伺服器憑證」。



五、點選「完成憑證要求」。

🍹 Internet Information Services (IIS) 管理	員	_ 8 ×
🚱 💿 📲 🕨 WIN-GIGVLP9ICXU 🕨		🖸 🗠 🟠 I 🖓 🗸
檔案(F) 檢視(V) 說明(H)		
→       →       ●	<ul> <li>● 同服器憑證</li> <li>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。</li> <li>2稱 ▲ 發行給</li> </ul>	卸作         唯之         建立過滤還要求         完成憑證要求         建立網域憑證         建立自我簽署憑證         ② 說明         線上說明
就緒		) 🗃 😨 🗧

六、選擇至憑證管理中心申請之 SSL 憑證,並輸入好記名稱(一般填寫 Domain Name)。

= Internet Informa	HOD 761A1C62 (112) 星话首			
G 🖸 🔋 🕨	WIN-GIGVLP9ICXU >			
檔案(F) 檢視(∀)	說明(H)			
連線 </td <td>ニの進設す☆ 開設蒼嶺 (◆ ● ◆ 電腦 ◆</td> <td>本機磁碟機 (C:) ↓</td> <td>▼ ∰</td> <td>2 V V V V V V V V V V V V V V V V V V V</td>	ニの進設す☆ 開設蒼嶺 (◆ ● ◆ 電腦 ◆	本機磁碟機 (C:) ↓	▼ ∰	2 V V V V V V V V V V V V V V V V V V V
□····································	● 組合管理 マ 📗 檢視	見 🔻 📑 新増資料夾		0
🗄 😔 Defau	最愛的連結 三 点面 1 電腦	名稱 A V	修改日期  - 類型 2010/3/27 下午1 檔案資料夾 2010/3/28 上午1 檔案資料夾 2010/3/27 上午0 檔案資料夾	_   •   大小 _   •   標註
	<ul> <li>■ 文件</li> <li>■ 圖片</li> <li>● 音樂</li> </ul>	₩ PerfLogs ₩ Program Files ₩ Windows ₩ 使用者	2008/1/19 下午 0 檔案資料夾 2010/3/27 上午 1 檔案資料夾 2010/3/27 上午 0 檔案資料夾 2010/3/27 上午 1 檔案資料夾	
	<ul> <li>♂ 最近的變更</li> <li></li></ul>	www.test.com.tw.	2010/3/28 上午 1 安全性憑證	2 KB
۲ ۲۰۰۶	· 資料夾 <b>へ</b> 檔案名和	▲ 解(N): www.test.com.tw	▼ *.cer 開設舊檔(0)	▶  

完成憑證要求	? ×
指定憑證授權單位回應	
藉由擷取包含憑證授權單位回應的檔案,完成先前建立的憑證要求。	
含有憑證授權單位回應的檔案名稱(R):	
C:/www.test.com.tw.cer.cer	
好記的名稱(Y):	
www.test.com.tw	
確定	取消

七、步驟4按「確定」,出現完成憑證要求的畫面。

🐂 Internet Information Servic	es (IIS) 管理員	
🚱 💽 📲 🕨 WIN-GIGV	VLP9ICXU 🕨	🗾 🖸 🔛 🏠 l 🕐 👻
檔案(F) 檢視(∀) 說明(H)		
連線 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	<ul> <li>         ・ の服器憑證         ・         ・         ・</li></ul>	<ul> <li>▶</li> <li>● 匯入</li> <li>建立憑證要求</li> <li>完成憑證要求</li> <li>建立網域憑證</li> <li>建立自我簽署憑證</li> <li>檢視</li> <li>理出</li> <li>更新</li> <li>※ 移除</li> <li>② 說明</li> <li>線上說明</li> </ul>
就緒		<b>1</b> .:

八、接著要安裝 eCA 及 PublicCA 憑證。 請先點選「開始」→輸入「mmc」→按下「Enter」。

程式集 mmc.exe 檔案	
🍌 ММС	Administrator
	文件
	電腦
	網路
	控制台
	糸統管理工具 ▶
	說明及支援
	執行
₽ 搜尋每個地方	
▶ 搜尋網際網路	
mmc	0

🚟主接台1 - [主接台4	根目錄]					Ľ
\overline 🚠 檔案(F) 🛛 執行(A)	檢視(\)	我的最愛(0)	視窗(₩)	說明(H)	_ 5	×
	? 📊					
📔 主控台根目錄	名稱				動作	
		這個檢測	視沒有項目	可顯示。	主控台根目錄	•
					其他動作	×
					J	

九、選擇「新增/移除嵌入式管理單元」。

🚟主控台1 - [主控台根目錄]					l ×
🚠 檔案(F) 執行(A) 檢視(∀) 🤅	我的最愛(O)	視窗(₩)	說明(H)	_ 5	×
🕼 開新檔案(N)	Ctrl+N				
■ 開散舊檔(0)	Ctrl+O			動作	
I語仔(A) 另存新檔(A)	Ctrl+S	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	5		其他動作	►
選項(r)	_				
1 servermanager.msc					
2 C:\Windows\\devmgmt.msc 3 C:\Windows\system 32\spedit m	er.				
ジャンパン1100 100 500 100 2 gpool 10 10 10 10 10 10 10 10 10 10 10 10 10					
īrā					
」 	新增或移除嵌	入式管理單	1元。	I	

十、接著點選「憑證」→「新增」。

新增或移除嵌入式管理單	元			×
您可以為這個主控台從您約 元。對於可延伸的嵌入式	的電腦上可以使用的嵌 管理單元,您可以設定¥	入式管理單元中 改用哪些延伸。	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
可用的嵌入式管理單元(%)	:	選	教的嵌入式管理單元(E):	
嵌入式管理單元	廠商 ▲		1 主控台根目錄	編輯延伸(X)
🦳 🚞 終端機服務管理員	Microsoft Cor			\$200.00
📃 群組原則物件編輯器	Microsoft Cor			1步时(氏)
🚽 🛁 裝置管理員	Microsoft Cor			
1 2 資料夾	Microsoft Cor			往上移(U)
路由及遠端存取     日本     日本	Microsoft Cor			往下我们)
🚽 🌆 電腦管理	Microsoft Cor	新增(A) > 🚺		12 (19/0)
	Microsoft Cor 🔪 –			
🔜 🚘 磁碟管理	Microsoft 與			
📄 📄 網址連結	Microsoft Cor			
📄 🧾 網路存取保護 (NAP	Microsoft Cor			
臺遠端桌面	Microsoft Cor			
🌔 🗊 憑證 🔹 🔵	Microsoft Cor			348-1716-2223
	<b>_</b>			
描述:				
	瀏覽電腦或服務的憑證	存放內容。		
				確定 取消

選擇「電腦帳戶」→「下一步」→「完成」。

憑證嵌入式管理單 <b>元</b>	×
這個裝入式給理單是將自動給理式利潤目的憑證。	
< 上一步(B, 下一步(N) > 取)月	

<ul> <li>諸選擇您要嵌入式管理單元幣自動管理.</li> <li>本機電腦(L):(執行這個主控台的電腦)</li> <li>另一台電腦(A):</li> <li>九許對證取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>人許對證取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>人許對證取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>人許對證取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>人許對證取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>(W)</li> <li>(M)</li> <li>(M)</li> <li>(M)</li> <li>(M)</li> <li>(M)</li> </ul>	瀏覽(R) 諸存主控台後才能遍用
諸選擇您要嵌入式管理單元管理的電腦。 這個嵌入式管理單元將自動管理 ● 本機電腦(L): (執行這個主控台的電腦) ● 另一台電腦(A): ■ 允許對選取的電腦進行從命令列所啟動的變更。這只在您 (W) ▲ 上一步化 (W) 上許對選取的電腦進行從命令列所啟動的變更。這只在您 (W) ▲ 上一步化 《 大子子書 》 《 大子書 》 《 大子書 》 》 》 》 》 》 》 》 》 》 》 》 》	瀏覽(R) 諸存主控台後才能適用
這個嵌入式管理單元將自動管理:         ● 本機電腦(L):(執行這個主控台的電腦)         ● 另一台電腦(A):         ● 九許對選取的電腦進行從命令列所啟動的變更。這只在您(W)         ● 九許對選取的電腦進行從命令列所啟動的變更。這只在您(W)         ▲ 大書生         ● 文格件嵌入式管理 元         ● 雪松市動家管理員         ● 新出原則物件編輯器         ● 加速のお代 Cor         ● 新出原則物件編輯器         ● 新出原則物件編輯器         ● 加速のお代 Cor         ● 新出原則物件編輯器         ● 新出原則物件編輯器         ● 新出原則物件編輯器         ● 新出原則物件編輯器         ● 新出原則物件編輯器         ● 新出原則物件编辑器         ● 新出原則物件編輯器         ● 新出原目 ● 「読得對素	瀏覽(R) 諸存主控台後才能遍用
<ul> <li>本機電腦(L):(執行這個主控台的電腦)</li> <li>另一台電腦(A):</li> <li>九許對選取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>(W)</li> <li>(W)</li> <li>(W)</li> <li>(W)</li> <li>(W)</li> <li>(W)</li> <li>(A)</li> <li>(A)</li></ul>	瀏覽(R) 諸存主控台後才能適用
<ul> <li>○ 另一台電腦(A):</li> <li>□ 九許對選取的電腦進行從命令列所啟動的變更。這只在您(W)</li> <li>▲ 上一步(C)</li> <li>《(W)</li> <li>(W)</li> <li>《(W)</li> <li>(W)</li> <li>(W</li></ul>	瀏覽(R) 諸存主控台後才能適用
<ul> <li>今一音电脑(A):</li> <li>              九許對選取的電腦進行從命令列所啟動的變更。這只在您 (W)      </li> <li>             太許對選取的電腦進行從命令列所啟動的變更。這只在您 (W)      </li> <li>             太上一步(低)         </li> <li>             後按下「確定」。      </li> <li>             我安藤太式管理單元。</li> <li>             新聞の運用的嵌入式管理單元中選擇一些嵌入式 "對於可延伸的嵌入式管理單元。您可以設定散用哪些延伸。      </li> <li>             新聞の運用的嵌入式管理單元。</li> <li>             新聞の運用的嵌入式管理單元。</li> </ul> <li>             新聞の運用の嵌入式管理單元。</li> <li>             新聞の運用の嵌入式管理單元。</li> <li>             新聞の運用の嵌入式管理單元。</li> <li>             新聞の運用の嵌入式管理單元。</li> <li>             新聞の運用の嵌入式管理單元。</li> <li>             Waresoft Cor 新課 原則物件編輯器             Microsoft Cor 資 對政             Microsoft Cor      </li>	潮覚(R)…」 諸存主控台後才能適用
■ 允許對選取的電腦進行從命令列所啟動的變更。這只在忽 (W) 《上一步(W) 後按下「確定」。 <b>主次8時家人式管理單元</b> 可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式。 <b>許然可延伸的嵌入式管理單元</b> ,您可以設定啟用哪些延伸。 用的嵌入式管理單元(S): 家商高 發端機服務管理員 Microsoft Cor 影響對來 Microsoft Cor	諸存主控台後才能適用
《上一步低》          後按下「確定」。         第380年後人式管理單元。         第380年後人式管理單元。         第380年後人式管理單元。         第380年後人式管理單元。         第380年後人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総人式管理單元。         第40年の総合式管理員         第40年の第二日         第40年の第二日         第40年の第二日         第40年の総合式管理員         第40年の後端長期         第40年の後端長期         第40年の後端長期         第40年の後端長期         第40年の後端長期         第40年の時代についけてい。         第40年の時代にのいけてい。         第40年の時代にのいけてい。         第40年の時代の前代のの。         第40年の時代の前代のの。         第40年の時代の前代のの。         第40年の時代の前代のの。         第40年の時代の前代のの。         第40年の時代の前代のの。         第40年の時代の前代のの。	
《上一步低)     《上一步低)     《上一步低)     《     《技安下「確定」。     《     《     《     》     《     》     《     》     《     》     》     》     》     》     》     》     》     》     》     》     》     》     》     》     《     》      》     》     》     》     》     》      》     》      》     》     》     》        》      》      》      》      》      》      》      》      》      》      》      》      》      》      》	
《 上一步代文》          後 按 下 「 確 定 」。         \$5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳入式管理單元         ?5.86時歳人式管理單元         ?5.86時歳人式管理單元         》         *2.365項運         》         *2.365項運         ※該端機服務管理員         Microsoft Cor         》 詳組原則物件編輯器         Microsoft Cor         》 詳料政         Microsoft Cor         》 資料政       Microsoft Cor         》 路由及為常理算       Microsoft Cor         》 路由 政務端常長期       Microsoft Cor         》 路由 政務端常長期       Microsoft Cor	
《上一步(正)     《     《 按下「 確 定 」。     《     》      》      》     》     》     》      》     》      》     》     》      》      》      》      》      》      》      》	
《 上一步(正) 後 按 下 「 確 定 」。 第380時載入式管理單元 第380時載入式管理單元,您可以使用的嵌入式管理單元中選擇一些嵌入式 第40時載入式管理單元,您可以設定啟用哪些延伸。 第40時載入式管理單元(您): 第410時載入式管理單元(您): 第410時期物件編輯器 Microsoft Cor 新指面原則物件編輯器 Microsoft Cor 新指面見為能異常理員 Microsoft Cor 新指面見為能異常理員 Microsoft Cor 新指面見為能異常理員 Microsoft Cor 新指面見書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書書	
<ul> <li>&lt; 上一步(正)</li> <li>後 按 下 「 確 定 」。</li> <li></li> <li><b>今式移降祓入式管理單元</b> <li>「可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式     <li>· 對於可延伸的嵌入式管理單元,您可以設定啟用哪些延伸。     <li>用的嵌入式管理單元(您):     </li> <li>※對於可延伸的嵌入式管理單元(您):     <li>※ 對於可延伸的嵌入式管理單元(您):     <li>※ 對紙原則物件編輯器 Microsoft Cor     <li>※ 對組原則物件編輯器 Microsoft Cor     </li> </li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	
《上一步现金》     《上一步现金》     《 按下「 確 定 」。     《     》      》     》     》     》     》     》      》     》     》      》     》      》     》      》     》     》     》      》     》     》     》     》      》      》     》      》	
《 上一步 (正)     》 (□)     《 上一步 (正)     》 (□)     》 (□)     》 (□)     》 (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)     □ (□)	
《 上一步(正) 後 按 下 「 確 定 」。 第388年後入式管理單元 第388年後、人式管理單元,您可以使用的嵌入式管理單元中選擇一些嵌入式 第38年月前、您可以設定啟用哪些延伸。 第48年月前、您可以設定啟用哪些延伸。 第48年月前、您可以能定啟用哪些延伸。 第48年月前、您可以能定啟用。 第48年月前、您認知此是一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個	
《 上一步(上) 後 按 下 「 確 定 」。 管式移除嵌入式管理單元 可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式 第一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個一個	
後 按 下 「 確 定 」。 <b> </b>	完成    取消
後按下「 確 定」。 <b>学或移除嵌入式管理單元</b> 可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式 。對於可延伸的嵌入式管理單元,您可以設定散用哪些延伸。 用的嵌入式管理單元(S): 蒸入式管理單元(S): 蒸入式管理單元(S): 蒸入式管理單元(S): 蒸入式管理單元(S): 蒸入式管理單元(S): 蒸入式管理單元(S): 二 整式機關務管理員 影端機服務管理員 影端機服務管理員 影icrosoft Cor 量 裝置管理員 Microsoft Cor 量 資料來 所以為這個主控台根目錄 量 主控台根目錄 量 主控台根目錄 量 二 影響。 影響。 影響。 影響。 影響。 影響。 影響。 影響。	
B或移時嵌入式管理單元 可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式 。對於可延伸的嵌入式管理單元,您可以設定散用哪些延伸。 用的嵌入式管理單元(您): 蒸入式管理單元 廠商 於端機服務管理員 Microsoft Cor 影群組原則物件編輯器 Microsoft Cor 影群組原則物件編輯器 Microsoft Cor 資料來 Microsoft Cor 資料來 Microsoft Cor 資料來 Microsoft Cor	
<ul> <li>可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式</li> <li>對於可延伸的嵌入式管理單元,您可以設定散用哪些延伸。</li> <li>用的嵌入式管理單元(次):</li> <li>選取的嵌入式管理</li> <li>蒸入式管理單元</li> <li>廠商</li> <li>蒸入式管理單元</li> <li>廠商</li> <li>整約</li> <li>経済機服務管理員</li> <li>Microsoft Cor</li> <li>新指原則物件編輯器</li> <li>Microsoft Cor</li> <li>新指原則物件編輯器</li> <li>Microsoft Cor</li> <li>新指原則物件編輯器</li> <li>Microsoft Cor</li> <li>資料夾</li> <li>Microsoft Cor</li> <li>資料</li> </ul>	
の以為這個主律合花怒的電腦上可以使用的軟人式管理單元中選择一些軟人式 ・對於可延伸的嵌入式管理單元。然可以設定散用哪些延伸。 用的嵌入式管理單元(%): 蒸入式管理單元 整商 全 整約講機服務管理員 新在rosoft Cor 量、群組原則物件編輯器 新在rosoft Cor 量、酸當管理員 新在rosoft Cor 量、資料來 新在rosoft Cor 電 資料來 新在rosoft Cor 電 資料來 新在rosoft Cor 電 資料來	
用的嵌入式管理單元(\$): 選取的嵌入式管理]	
款入式管理單元     廠商     ▲       診端機服務管理員     Microsoft Cor       評組原則物件編輯器     Microsoft Cor       詳細原則物件編輯器     Microsoft Cor       書裝置管理員     Microsoft Cor       資 済料夾     Microsoft Cor       資 溶料夾     Microsoft Cor       資 溶料夾     Microsoft Cor       資 溶料夾     Microsoft Cor	理單元,並且設定所選擇的嵌入式管理
<ul> <li>診端機服務管理員 Microsoft Cor</li> <li>詳組原則物件編輯器 Microsoft Cor</li> <li>装置管理員 Microsoft Cor</li> <li>資料夾 Microsoft Cor</li> <li>資料夾 Microsoft Cor</li> <li>資料夾 Microsoft Cor</li> <li>資料夾 Microsoft Cor</li> </ul>	9理單元,並且設定所選擇的嵌入式管理 元(E):
新田原則物件編輯器 Microsoft Cor 電装置管理員 Microsoft Cor 資料夾 Microsoft Cor 電路出発達端存取 Microsoft Cor	9理單元,並且設定所選擇的嵌入式管理 元(E): 編輯延伸(X)
当時世界は でのでは、 でのでは、 でのでは、 でのでは、 でのでは、 でのでは、 でのでは、 でのでのでのでのでのでは、 でのでのでのでは、 でのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでの	理單元,並且設定所選擇的嵌入式管理 元(E): 脳) <u> 全別を</u> クロン
	P理單元,並且設定所選擇的嵌入式管理 元(E): 脳) 移除(R)
	P理單元,並且設定所選擇的嵌入式管理 元(E): 脳) 移除(R) (たいなかの)
	7理單元,並且設定所選擇的嵌入式管理 元(E):
電話を空 Microsoft Cor 新増(A) >	7理單元,並且設定所選擇的嵌入式管理 元(E): 腦) <sup>[</sup> 編輯延伸(X) 形(R) (在上移(D) (在下移(D)
· 磁碟管理 Microsoft 與 …	7理單元,並且設定所選擇的嵌入式管理 元(E): 脳) 「編輯延伸(X) 「移除(R) 往上移(0) 往下移(D)
會網址連結 Microsoft Cor	7理單元,並且設定所選擇的嵌入式管理 元(E): 腦)
圖 網路存取保護 (NAP Microsoft Cor	F理單元,並且設定所選擇的嵌入式管理 元(E): (E): (編輯延伸(X) (移除(R)) (往上移(D)) (往下移(D))
多速端兵面 Microsoft Cor	P理單元,並且設定所選擇的嵌入式管理 元(E): (E): (編輯延伸(X) (部) (部) (部) (部) (部) (部) (部) (部)
₽憑證 Microsoft Cor	P理單元,並且設定所選擇的嵌入式管理 元(E): (E): (語) (名味(C)) (名味称(D) (名下称(D))

確定

🔵 取消

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」。

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。

<ul> <li>□ 主控台1 - [主控台根目錄\/臺證 (本穩電腦)\/信任的根臺證授權\/臺讀</li> <li>□ 檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)</li> </ul>	2]	_D×
<ul> <li>○ 主控台根目錄</li> <li>○ 個人</li> <li>○ 信任的根憑證授權</li> <li>○ 介有工作(K)</li> <li>○ 介有</li> <li>○ 受信任</li> <li>○ 受信</li> <li>○ 受信<td>發行者         Class 3 Publ         Class 3 Publ         Class 3 Publ         Class 3 Publ         Copyright (i         ePKI Root C         Government         Microsoft A:         Microsoft Ri         // Microsoft Ri         NO LIABIL         Thawte Time</td><td><b>動作</b> <b> 憑證 ▲</b> 其他動作 →</td></li></ul>	發行者         Class 3 Publ         Class 3 Publ         Class 3 Publ         Class 3 Publ         Copyright (i         ePKI Root C         Government         Microsoft A:         Microsoft Ri         // Microsoft Ri         NO LIABIL         Thawte Time	<b>動作</b> <b> 憑證 ▲</b> 其他動作 →

十二、 出現以下畫面後,點選「下一步」→「下一步」→「完成」。

憑證匯入精靈		×
	歡迎使用憑證匯入精靈	
	這個精靈將協助您將憑證、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性的網路連線資訊。憑證存 放區是用來存放憑證的系統區域。	
	諸按 [下一步] 繼續。	
		_
	<上一步(N)> 取消	

<b>登匯入精靈</b>	
<b>匯入檔案</b> 指定您想要匯入的檔案。	
檔案名稱(F):	$\frown$
C:\ROOTeCA_64.cer	( 瀏覽(R) )
	的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFXP	12)
密碼編譯訊息語法標準 - PKCS #7	
Microsoft 序列馮證存放(sst)	
涂人了解 <u>憑證福茶格式</u>	
	<上一步(4)下一步(N)> 取消
	$\sim$
國語入精靈	
憑證存放區	
憑證存放區是用來存放憑證的系統區	五域。
Windows 會自動選擇一個憑證存放區	極,您也可以為憑證指定存放位置。
<i>个</i> 。	*方协正/11\
	2170X@(U)
<ul> <li>一時所有感望放入以下的行放回 進設方版面。</li> </ul>	2(r)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	·····································
JIBITHING	780.552 (447
深入了解 <u>憑證存放區</u>	
深入了解 <u>憑證存放區</u>	
深入了解 <u>憑證存放區</u>	

憑證匯入精靈		X
	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 內容     憑證 檔案名稱	
	《上一步(1) 完成 取消	
<b>善</b> 證匯入精靈	×	
1 匯入執行成功。		
確定		

十三、 匯入成功後,可以看到 eCA 的根憑證。

臺主控台1 - [主控台根目錄\憑證(	(本機電腦)\信任的根憑證授權\憑證]		
福案(F) 執行(A) 檢視(V) 封 ◆ ⇒ 2	細田最愛(0) 視窗(₩) 説明(H) ■ ➡ ┃ <b>2</b>   ■		
<ul> <li>註控台根目錄</li> <li>□ □ 憑 憑證 (本機電腦)</li> <li>□ 個人</li> <li>□ □ 信任的根憑證授權</li> <li>□ □ 企業信任</li> <li>□ □ 企業信任</li> <li>□ □ 欠信任的發行者</li> <li>□ □ 沒有信任的憑證</li> <li>□ □ 笑信任的人</li> <li>□ □ 愛信任的人</li> <li>□ □ 愛信任的人</li> <li>□ □ 智慧卡信任根目錄</li> </ul>	議給 Class 3 Public Primary Certification Class 3 Public Primary Certification Copyright (c) 1997 Microsoft Corp. ePKI Root Certification Authority Government Root Certification Authority Microsoft Authenticode (tm) Root A Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certificate Authority NO LIABILITY ACCEPTED, (c)9 Thawte Timestamping CA	發行者 Class 3 Publ Class 3 Publ Copyright ( ePKI Root C Government Microsoft R Microsoft R Microsoft R NO LIABIL Thawte Tim	動作         通識       ▲         其他動作       ▲         身他動作       ▲
,			•

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」。

	_
☐ 檔案(F) 執行(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)	×
☐ 主控台根目錄 ● 登拾 ▲  ● 發行者 動作	_
□ 🗊 憑證 (本機電腦) 🔄 🔄 Microsoft Windows Hardware Com Microsoft R 🚛 🏭	
□ 個人 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	
□ □ 信任的根憑證授權 □ □ □ □ □ Root Agency Root Agenc; 具他動作	
📄 💭 憑證 👘 VeriSign Class 1 CA Individual Su Class 1 Publ	
王 🛄 企業信任 🔄 🔄 VeriSign Class 2 CA - Individual S Class 2 Publ	
中継徳道授権 「二 中継徳道授権 「二 中継徳がおませ」	
🔄 🚽 🚽 所有工作(K) 🔹 🕨 匯入(I)	
□ □ □ (Windows) (Wi	
🗉 🔚 憑證訂 新工作台檢視(T)	
Ⅲ 📑 智慧┤───────────	
貼上(?)	
重新整理(F)	
匯出清單(L)	
→ 合用(III)	

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

<b>憑證匯入精靈</b>	×
<b>匯入檔案</b> 指定您想要匯入的檔案。	
C:\PublicCA2_64.crt 瀏覽(R)	
個人資訊交換- PKCS #12 (.PFX,.P12)	
加密編譯訊息語法標準 - 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(N) > 取消	_

成功匯入後,可以看到 PublicCA G2 的中繼憑證。

🚟主接台1 - [主接台)	根目錄\憑證 (本機電腦)\中繼憑證授	禰單位\憑證]	
🚠 檔案(F) 🛛 執行(A)	檢視(\V) 我的最愛(O) 視窗(\V)	說明(H)	_ & ×
🗢 🔿 🔁 📅 🕹	′ 🛍 🔀 🖺 🗟 🛛 🚮		
■ 主控台根目錄	發給 ▲ ■ Microsoft Windows Hardware Com	资發者 Microsoft Poot Authority	動作
□ 🚅 證 (本1後電加	Public Certification Authority - G2	ePKI Root Certification Auth	🧾 🦄 🔺
□ 📔 受信任的者	Root Agency	Root Agency	┛ 其他動作 ▶
	🔄 www.verisign.com/CPS Incorp.by	Class 3 Public Primary Certif	Public Certif 🔺
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □			其他動作 ▶
□ 憑證撤			
Ⅲ 🧮 受信任的影			
田 🧰 沒有信任的			
田 🔛 第二万根燈			
田 🧮 憑證註冊男			
Ⅲ ■ 智慧卡信伯			
•		F	
中繼憑證授權單位 存放	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)。

📚 Internet Information Servic	:es (IIS) 答理員	
C C C C C C C C C C C C C C C C C C C	'LP9ICXU ▶ 站台 ▶ Default Web Site ▶	) 😂 📨 🔄 I 🚱 🗝
檔案(F) 檢視(V) 說明(H)		
連続 建築 地路 地路 地路 地路 地路 地路 地路 地路 地路 地路	Default Web Site 首頁 群組依據: 區域: • 圖• HS HTTP 圓應標 MIME 類型 章 主樓名稱 连接埠 IP 位址 80 *	bbft     ◎ 淵源     ◎ 漁煙4 欄段     ◎ 編輯4 欄段     ◎ 編輯4 欄段     ◎ 編輯4 欄段     ◎ 基本 該定     校視應用程式     校視應用程式     校視應用程式     校規應用在式     校規應用在式     ◆ ※ 和書表     ◎ 第一個 表
★ 新培站台索结 類型(T): IP 位址(I): ★ 新生生活	101 功能被視 40 內容機規 連接埠(0):	
Mups 生代名稱(田) SSL 憑證(S): www.test.com.tw	▼ 檢視(V) 確定 取消	

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

#### 十七、 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。

# 附件一:設定 SSL 安全通道的加密強度

IIS 7.0 預設使用 AES 128 位元來進行資料加密, 欲使用 AES 256 位元來進行資料加密的話, 可以參考以下步驟:

程式集 『gpedit.msc	
	Administrator
	文件
	電腦
	網路
	控制台
	条統管理工具 ▶
	說明及支援
	執行
	Windows 安全性
🔎 搜尋網際網路	
gpedit mscl	

一、啟動 gpedit.msc 程式

二、選擇 SSL 組態設定,對著「SSL 加密套件順序」點兩下。



三、選擇「已啟用」,並修改 SSL 加密套件的欄位。

#### 原加密套件順序:

TLS RSA WITH AES 128 CBC SHA, TLS RSA WITH AES 256 CBC S HA,TLS\_RSA\_WITH\_RC4\_128\_SHA,TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_S HA,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256,TLS\_ECDHE\_ ECDSA WITH AES 128 CBC SHA P384, TLS ECDHE ECDSA WITH A ES\_128\_CBC\_SHA\_P521,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SH A\_P256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384,TLS\_ECD HE ECDSA WITH AES 256 CBC SHA P521,TLS ECDHE RSA WITH AES\_128\_CBC\_SHA\_P256,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA \_P384,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P521,TLS\_ECDHE\_ RSA WITH AES 256 CBC SHA P256,TLS ECDHE RSA WITH AES 25 6\_CBC\_SHA\_P384,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P521,T LS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA,TLS\_DHE\_DSS\_WITH\_AES\_25 6\_CBC\_SHA,TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA,TLS\_RSA\_WI TH\_RC4\_128\_MD5,SSL\_CK\_RC4\_128\_WITH\_MD5,SSL\_CK\_DES\_192\_ED E3 CBC WITH MD5,TLS RSA WITH NULL MD5,TLS RSA WITH NU LL\_SHA

修改後的加密套件順序:

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA,TLS\_RSA\_WITH\_RC4\_128\_SHA,T LS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA,TLS\_ECDHE\_ECDSA\_WITH\_AES \_128\_CBC\_SHA\_P256,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_ P384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P521,TLS\_ECDH E\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256,TLS\_ECDHE\_ECDSA\_WITH \_AES\_256\_CBC\_SHA\_P384,TLS\_ECDHE\_ECDSA\_WITH\_AES\_256,CBC\_ SHA\_P521,TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256,TLS\_ECD HE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384,TLS\_ECDHE\_RSA\_WITH\_AE S\_128\_CBC\_SHA\_P521,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P2 56,TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384,TLS\_ECDHE\_RS A\_WITH\_AES\_256\_CBC\_SHA\_P521,TLS\_DHE\_DSS\_WITH\_AES\_128\_CB C\_SHA,TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA,TLS\_DHE\_DSS\_WIT H\_3DES\_EDE\_CBC\_SHA,TLS\_RSA\_WITH\_RC4\_128\_MD5,SSL\_CK\_RC4\_ 128\_WITH\_MD5,SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5,TLS\_RSA\_W ITH\_NULL\_MD5,TLS\_RSA\_WITH\_NULL\_SHA

SL 加密	(套件順)	茅 内容							? ×
設定	解說	1							
<u> </u>	L 加密套	件順序							
C尚: ○已 C已	未設定(C 啟用(E) 停用(D)	:)							
SSL ;	加密套件	TLS_	RSA_1	WITH_A	.ES_256	5_CE	BC_SHA	,TL:	
支援的	的作業系統	<del>ش</del> : ب	必須是	Windov	vs Vista	以	-的版本	;	
Ŀ	一個設定	E(P)	T	一個設	定(N)				
				確定			取消		套用(A)

四、開啟登錄檔編輯程式。

程式集	
💣 regedit.exe	8
	Administrator
	文件
	電腦
	網路
	控制台
	条統管理工具 ▶
	說明及支援
	<b>執</b> 行
	Windows安全性
➢ 授琴母 個 电 万	
regedit	0

五、依照下圖進行登錄檔編輯。



1 登登編輯程式			
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 說明(H)			
Mar 社主社士和社主 描葉(F) 編輯(E) 検視(V) 我的最愛(A) 說明(H)	▲ A A A A A A A A A A A A A	類型 REG_SZ REG_DWORD	資料 (數值未設定) 0×00000000 (0)
Schannel     Ciphers     Ciphers     Ciphers     NULL     Ciphers     NULL     Ciphers     NULL     Ciphers     NULL     RC2 128/128     RC4 128/128     RC4 128/128     RC4 40/128     RC4 40/128     RC4 56/128     RC4 64/128	▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ● (預該(直) ※ ■ Enabled	類型 REG_SZ REG_DWORD	資料 (數值未設定) <u>0x0000000 (0)</u>
<ul> <li>B→ Nis</li> <li>B→ NodeInterfaces</li> <li>B→ PnP</li> <li>B→ Power</li> <li>B→ Print</li> <li>PriorityControl</li> <li>ProductOptions</li> <li>B→ RtQueryRegistryConfig</li> <li>B→ SafeEloot</li> <li>B→ ScsiPort</li> <li>B→ SecurePipeServers</li> <li>B→ Schamel</li> <li>B→ Sc</li></ul>			

普登錄編輯程:	£			
檔案(F) 編輯(E	2) 檢視(V) 我的最愛(A) 說明(H)			
	<ul> <li>P- NetDiagFx</li> <li>Network</li> <li>Network</li> <li>Network</li> <li>Network</li> <li>Network</li> <li>NodeInterfaces</li> <li>Nsi</li> <li>PnP</li> <li>Power</li> <li>Print</li> <li>PriorityControl</li> <li>ProductOptions</li> <li>RtQueryRegistryConfig</li> <li>SafeBoot</li> <li>SceurePipeServers</li> <li>SceurePipeServers</li> <li>SceurePipeServers</li> <li>Schannel</li> <li>Ciphers</li> <li>DES 56/56</li> <li>NULL</li> <li>RC2 128/128</li> <li>RC4 128/128</li> <li>RC4 40/128</li> <li>RC4 56/128</li> <li>RC4 56/128</li> <li>RC4 6/128</li> </ul>	名稱 (預設值) (預設在) (注意) Enabled	類型 REG_SZ <u>REG_</u> DWORD	<u>資料</u> (數值未設定) 0x00000000 (0)
・ 登録編輯程5 當案(F) 編輯(E	✿ ) 檢視(V) 我的最愛(A) 說明(H)			
merce / mined (b	Network / Sourcest (v) 2019(11)      Network Provider      Network Provider      Nis      Network Provider      Nis      NodeInterfaces     Nis      Print     Print     Print     Print(Control     ProductOptions     RidQueryRegistryConfig     SafeBoot     SosiPort     SecurePipeServers     SecurePipeServers     SecurePipeServers     SasIProfiles     Schannel     Ciphers     Schannel     Ciphers     Ciphers     RC2 128/128     RC2 128/128     RC2 128/128     RC2 40/128     RC2 128/128     RC4 128/128     RC4 128/128     RC4 40/128	名稱 (預設值) (預設任	展EG_SZ REG_DWORD	資料 (數值未設定) 0x00000000 (0)

當 登錄編輯程式	S			
檔案(F) 編輯(E)	) 檢視(V) 我的最愛(A) 說明(H)			
100.775 ¥ 7 10.4944 ¥	Image: Construction       Image: Construction         Image: Constreaction       Image: Constreaction<	名稱 (預該值) (預該值)	X類型 REG_SZ REG_DWORD	資料 (働値未設定) 0x00000000 (0)
☆ 登録/4輯程式 檔案(F) 編輯(E)	<ul> <li>★ 様根(V) 我的最愛(A) 說明(田)</li> <li>★ MetDiagFx</li> <li>★ NetworkProvider</li> <li>★ NetworkProvider</li> <li>★ NetworkProvider</li> <li>★ NodeInterfaces</li> <li>★ NodeInterfaces</li> <li>★ Noi</li> <li>← Nai</li> <li>← PaP</li> <li>← Print</li> <li>← Print</li> <li>← Print(Decryptions)</li> <li>♥ RtQueryRegistryConfig</li> <li>♥ ScewerPipeServers</li> <li>← SecurePipeServers</li> <li>← SecurePipeServers</li> <li>← SecurePipeServers</li> <li>← ScalProfiles</li> <li>← Ciphers</li> <li>← Ciphers</li> <li>← DES 56/56</li> <li>← NULL</li> <li>← RC2 128/128</li> <li>← RC4 128/128</li> <li>← RC4 56/128</li> <li>← RC4 56/128</li> <li>← RC4 56/128</li> <li>← RC4 56/128</li> </ul>	名稱 通 (預設值) 题 Enabled	算题 REG_SZ <u>REG_DWORD</u>	資料 (數值未設定) 0×00000000 (0)



六、設定完成後,重開機,即可達到 AES 256 位元的加密效果。

頁面資訊 - https://		
→		
網站身分		
擁有者: 這個網站沒有提供擁有者資訊。		
驗證機構: Chunghwa Telecom Co., Ltd.		
<b>]</b> 為 及廢史記錄		檢視憑證 ₩
我以前有瀏覽過這個網站嗎?	否	
此網站有在我的電腦中儲存資訊 (Cookie) 嗎?	否	檢視 Cookie (K)
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		
連線已加密:高級加密(AES-256,256 bit 金譜	)	
加密使得未經許可的人非常難以破解以取得電腦關 值送與接收的答訊。	間的通訊。 所以幾乎不大 <b>有</b>	人可以 <mark>截取到您在網路上</mark>

# 附件二:單一 IP,多站台啟用 SSL

IIS7 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,即可在多個網站上啟用 443 port。

- 一、依照前述的憑證安裝步驟,先在其中一網站上安裝憑證,並以 HTTPS 測試連線是否正常。
- 二、再點選1次「繫結」,會看到主機名稱下面是空的。

📬 Internet Information Services (IIS) 管理員	_ 8 ×
G ○ WIN-R8R71VJUKVM → 站台 → test1 →	🖸 🐼 🖾 🛛 🖉 🕶
檔案(F) 檢視(∀) 說明(H)	
連絡       test1 首頁         ●       WIN-R8871VJUKVM (WIN-R8         ●       感用程式集區         ●       Sch         ●       Default Web Site         ●       best         ● <td< td=""><td>勤作</td></td<>	勤作
關閉(C)	11覽網站
應       詳細     詳細       報出快取處     錯誤網頁       選       運       通	● *80 (http) ● *80 (http) ● 潮覽 *.443 (https) 進階設定 設定 失敗要求的追蹤 限制 ② 說明 線上說明
就緒	•

三、到以下目錄:「C:\Windows\System32\inetsrv\config」,以記事本開啟 「applicatiuonHost.config」

🕌 config		<u>_8×</u>
	碟機 (C:) → Windows → System32 → inetsrv → config → 🛛 🔸 🚺 搜尋	
檔案(F) 編輯(E) 檢視(	7) 工具(T) 說明(H)	
🕒 組合管理 👻 📗 檢社	見 👻	0
	_ 名稱 ▲ 修改日期     ↓ 類型                   ↓   大小     ↓ 標記     ↓	
	Lange Constant 2013/3/18 上午 0 檔案資料夾	
	→ schema 2013/3/18 上午 0 檔案資料夾	
[ 🖹 🔤 片	administration config 2013/3/18 上午 0 CONFIG 檔案 14 KB	
📑 音樂 🔍 📢	applicationHost.config 2004/3/18下午 0 CONFIG 檔案 48 KB	
📝 最近的變更	reanection.comig 2013/3/18 上午 0 CONFIG 檔案 1 KB	
搜尋		
🔟 公用		
資料夾 🔨	x i i i i i i i i i i i i i i i i i i i	

四、找到剛剛有新增443 port 的網站後,將 domain name 加入443:之後,存 檔並關閉,如圖。

🧱 applicationHost.config - 記事本	_ 8 ×
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)	
<pre><bindings></bindings></pre>	
<pre>                                   <td></td></pre>	
<pre> </pre>	
<pre>          <logfile directory="%SystemDrive%\inetpub\logs\LogFiles" logformat="W3C"></logfile></pre>	s" />
<weblimits></weblimits>	

五、回 IIS 管理員,重新點選「繫結」,會看到主機名稱下出現之前輸入的 domain name,這樣即表示修改成功。

¥Internet Information Services (IIS) 管理員	_ 8 ×
	🖸 🖬 🖬 🕼 -
檔案(F) 檢視(∀) 說明(H)	
連線       test1 首頁         ●       WIN-RSR71VJUKVM (WIN-RS         ●       WIN-RSR71VJUKVM (WIN-RS         ●       MIN-RSR71VJUKVM (WIN-RS         ●       Default Web Site         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●       ●         ●	<ul> <li>動作</li> <li>漁覽</li> <li>編輯權限</li> <li>編輯權限</li> <li>編輯權限</li> <li>編輯權限</li> <li>編輯花台</li> <li>緊結</li> <li>又本設定</li> <li>又視應用程式</li> <li>決視虛擬目錄</li> <li>司站</li> <li>和站</li> <li>範段動</li> <li>運動</li> <li>近</li> <li>到覽 www.testl.com.tw on</li> <li>(************************************</li></ul>
使                 後組                  現                 近                 近                 近                 近                 近                 が                 近                 が <td><ul> <li>▲ *80 (nmp)</li> <li>● 瀏覽 *:443 (https)</li> <li>建階設定</li> <li>設定</li> <li>失敗要求的追蹤&lt;</li> <li>限制</li> <li>② 說明</li> <li>線上說明</li> </ul></td>	<ul> <li>▲ *80 (nmp)</li> <li>● 瀏覽 *:443 (https)</li> <li>建階設定</li> <li>設定</li> <li>失敗要求的追蹤&lt;</li> <li>限制</li> <li>② 說明</li> <li>線上說明</li> </ul>

六、接著,可以先將第2個網站新增443 port 以及掛上憑證,同樣去修改「applicatiuonHost. config」

📬 Internet Information Services (II	2) 管理員	
S S WIN-R8R71VJU	KVM ▶ 站台 ▶ test2 ▶	🖸 🐼 🖓 I 🕢 🕶
檔案(F) 檢視(V) 說明(H)		
連線 WIN-R8R71VJUKVM (WIN-R8 WIN-R8R71VJUKVM (WIN-R8 原用程式集區 中心 站台 中心 test1 中心 test1 中心 test1	test2 首頁 群組依據: 區域 • III • IIS 建立 主機名稱 連接埠 IP 位址 緊線 * 443 *	動作           ♪         瀏覽           編輯權限         編輯權限            編輯權限            編輯權限            編輯權限            編輯權限            編輯權限            編輯權限            編輯准定
	應       模組     輸出快取處     錯誤網頁     愛諭       理     童      愛諭       運ご          ご     功能檢視	<ul> <li>▲ 開設 www.issiz.com/w of *.60</li> <li>(http)</li> <li>進階設定</li> <li>設定</li> <li>失敗要求的追蹤</li> <li>限制</li> <li>② 說明</li> <li>線上說明</li> </ul>
私網		<b>•</b>



七、其他需要掛上憑證的網站依照上述步驟操作。完成後,請以HTTPS連線測試, 是否所有網站皆正常。