## 中華電信通用憑證管理中心 (PublicCA)

Windows IIS 系列 SSL 憑證請求檔製作與安裝手冊附錄 聲明:本說明文件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。本說明文件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

停用 SSLv2、SSLv3	2
Windows Server 2003 IIS 6	2
Windows Server 2008 IIS 7	7
Windows Server 2012 IIS 8	13
更換 SHA256 憑證	17
Windows Server 2003 IIS 6	17
Windows Server 2008 IIS 7	
Windows Server 2012 IIS 8	51

## 停用 SSLv2、SSLv3

Windows Server 2003 IIS 6

一、開啟登錄檔編輯程式,依照以下路徑找到 SSL2.0。

HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvi ders\SCHANNEL\Protocols\SSL 2.0



二、找到SSL 2.0下,「Server」的機碼,並點選之。

若無「Server」的機碼,請在 SSL2.0 資料夾上按右鍵→新增→機碼,然後 輸入「Server」。



三、接著在右邊的畫面下按右鍵→新增→DWORD值,然後輸入「Enabled」,並確 認資料欄位值為「0x00000000(0)」,若不是,請手動將值改為0。



四、依照以下路徑找到 SSL3.0。

HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvi ders\SCHANNEL\Protocols\SSL 3.0

🎻 登錄編輯程式			
檔案(F) 編輯(E) 檢視(V) 我的最	逶(A) 說明(H)		
Protocols	▲ 名稱	類型	資料
🛉 💼 PCT 1.0	••••• (預設値)	REG_SZ	(數值未設定)
□			
Client			
Server			
WDigest			
Server Applications			
ServiceCurrent			
ServiceGroupOrder			
🗄 🚞 ServiceProvider			
🖻 🚞 Session Manager			
Setup			
E IIImage			
E SystemResources			
+ I rimal Server			
	卢		_
我的電腦\HKEY_LOCAL_MACHINE\	SYSTEM/CurrentControlSet/Co	ontrol\SecurityProviders\S(	CHANNEL \Protocols\SSL

五、找到 SSL 3.0 下,「Server」的機碼,並點選之。

若無「Server」的機碼,請在 SSL3.0 資料夾上按右鍵→新增→機碼,然後 輸入「Server」。

💣 登錄編輯程式				
檔案(F) 編輯(E) 檢視(V) 我的最	愛( <u>A</u>	) 説明(出)		
E- Protocols		名稱	類型	資料
		••••] (預設値)	REG_SZ	(數值未設定)
Glimt				
Server )				
Server Applications				
ServiceCurrent				
ServiceGroupOrder				
Service Honorer				
E Stillmage				
+ SystemResources				
Terminal Server				
TimeZoneInformation	τI			
		•		Þ
我的電腦\HKEY_LOCAL_MACHINE	SYSTI	EM/CurrentControlSet/Co	ntrol\SecurityProviders\SC	HANNEL Protocols SSL

六、接著在右邊的畫面下按右鍵→新增→DWORD 值,然後輸入「Enabled」,並確 認資料欄位值為「0x00000000(0)」,若不是,請手動將值改為0。



七、重新啟動電腦。啟動完成後,可以使用測試工具(註1、註2)進行檢測, 看 SSL 2.0、SSL3.0 是否已停用。

註1:例如行政院國家資通安全會報技服中心網頁 http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh 有介紹 兩種檢測伺服器端 SSL 協定的工具:(1) TestSSLServer (http://www.bolet.org/TestSSLServer/) 與(2) QUALYS SSL LABS SSL Server Test 檢測工具(https://www.ssllabs.com/ssltest/index.html, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協 定,因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點, 弱點編號 CVE-2014-3566 (POODLE),故建議不要使用 SSL V3 協定,請改用 TLS 最新協定。

註2:

- (1)若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <u>https://zmap.io/sslv3/browsers.html</u>之英文說明
- (2)請超連結至 <u>https://dev.ssllabs.com/ssltest/viewMyClient.html</u>可檢測您用戶端
   之瀏覽器是否已經停用 SSL V3。
- (3)若是 I.E. 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選 使用 SSL V3 與使用 SSL V2,或參考下圖設定(取材自行政院國家資通 安全會報技服中心網頁

http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh)



一、開啟登錄檔編輯程式,依照以下路徑找到 SSL2.0。

HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvider s\SCHANNEL\Protocols\SSL 2.0



二、在 SSL2.0 資料夾上按右鍵→新增→機碼,然後輸入「Server」。



公 登錄編輯程式				
檔案(F) 編輯(E) 檢視(V) 我的最愛	(A) 說明(H)			
📄 📲 SecurityProviders 📃	名稱	類型	資料	
		REG_SZ	(數值未設定)	
🖻 🤚 Schannel				
Ciphers				
CipherSuites				
🖻 🖳 🕒 Protocols				
🖻 🖳 🔛 SSL 2.0				
Client				
Server				
WDigest				
ServiceCurrent				
ServiceGroupUrder				
E Servicerrovider				
+ Session Manager				
±				
±				
Storage				
Systeminiormation				
	•		•	
電腦\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\新模				

三、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值,然後輸入「Enabled」,並確認資料欄位值為「0x00000000(0)」,若不是,請 手動將值改為0。



🚮 登錄編輯程式					
檔案(F) 編輯(E) 檢視(V) 我的最	愛(A) 說明(H)				
📄 🦺 SecurityProviders	▲ 名稱	類型	資料		
SaslProfiles	(損該1)	REG_SZ	(數值未設定)		
📄 🤚 Schannel	🛛 🌔 🎎 Enabled	REG_DWORD (	0x00000000 (0)		
Ciphers					
CipherSuites					
Hashes					
KeyExchangeAlgorithn	a				
E					
□					
Client Server					
WDigest					
🚽 🖳 📔 ServiceGroupOrder					
📄 🕀 퉲 ServiceProvider					
📄 🗄 퉬 Session Manager					
🗄 🖶 퉲 SNMP					
🗄 🕀 StillImage					
Storage					
SystemInformation	-				
			Þ		
電腦\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Serv 📈					

四、依照以下路徑找到 SSL3.0

### HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvider s\SCHANNEL\Protocols\SSL 3.0

若無 SSL3.0,請找到以下路徑,自行新增 SSL3.0 機碼。

# HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvider

### s\SCHANNEL\Protocols\



五、在 SSL3.0 資料夾上按右鍵→新增→機碼,然後輸入「Server」。



六、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值,然 後輸入「Enabled」,並確認資料欄位值為「0x00000000(0)」,若不是, 請手動將值改為0。



七、重新啟動電腦。啟動完成後,使用可以測試工具(註1、註2)進行檢測, 看 SSL 2.0、SSL3.0 是否已停用。

註 1:例如行政院國家資通安全會報技服中心網頁 <u>http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh</u>有介紹兩種檢 測伺服器端 SSL 協定的工具:(1) TestSSLServer (<u>http://www.bolet.org/TestSSLServer/</u>) (2) QUALYS SSL LABS SSL Server Test 檢測工具(<u>https://www.ssllabs.com/ssltest/index.html</u>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定,因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點,弱點編號 CVE-2014-3566 (POODLE),故建議不要使用 SSL V3 協定,請改用 TLS 最新 協定。

註2:

- (1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <u>https://zmap.io/sslv3/browsers.html</u>之英文說明
- (2)請超連結至<u>https://dev.ssllabs.com/ssltest/viewMyClient.html</u>可檢測您用戶端 之瀏覽器是否已經停用 SSL V3。
- (3)若是 I.E.瀏覽器可於工具列->網際網路選項->進階->安全性取消勾 選使用 SSL V3 與使用 SSL V2,或參考下圖設定(取材自行政院國家資 通安全會報技服中心網頁

http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh)



- 一、經測試, IIS8 SSL2.0 預設是關閉的, 若您的 SSL2.0 是開啟的, 您可以依照以下關閉 SSL 3.0 的作法來關閉 SSL2.0。
- 二、開啟登錄檔編輯程式,依照以下路徑找到 Protocols。

### HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProvider s\SCHANNEL\Protocols\

在 Protocols 的機碼上,按下右鍵→新增→機碼,然後輸入「SSL 3.0」。







三、在 SSL3.0 資料夾上按右鍵→新增→機碼,然後輸入「Server」。

四、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值,然後輸入「Enabled」,並確認資料欄位值為「0x00000000(0)」,若不是,請手動將值改為0。





五、重新啟動電腦。啟動完成後,使用可以測試工具(註1、註2)進行檢測, 看 SSL 2.0、SSL3.0 是否已停用。

註 1:例如行政院國家資通安全會報技服中心網頁 <u>http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh</u>有介紹兩種檢 測伺服器端 SSL 協定的工具:(1) TestSSLServer (<u>http://www.bolet.org/TestSSLServer/</u>) (2) QUALYS SSL LABS SSL Server Test 檢測工具(<u>https://www.ssllabs.com/ssltest/index.html</u>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定,因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點,弱點編號 CVE-2014-3566 (POODLE),故建議不要使用 SSL V3 協定,請改用 TLS 最新 協定。

註2:

- (1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <u>https://zmap.io/sslv3/browsers.html</u>之英文說明
- (2)請超連結至<u>https://dev.ssllabs.com/ssltest/viewMyClient.html</u>可檢測您用戶端 之瀏覽器是否已經停用 SSL V3。
- (3)若是 I.E.瀏覽器可於工具列->網際網路選項->進階->安全性取消勾 選使用 SSL V3 與使用 SSL V2,或參考下圖設定(取材自行政院國家資 通安全會報技服中心網頁

http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh)



## 更換 SHA256 憑證

Windows Server 2003 IIS 6

- 一、適用於申請時,有同時取得 SHA1、SHA256 憑證。或是憑證再效期內,經由 審驗人員再次核發 SHA256 憑證者。
- 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、需要先備妥 OpenSSL 軟體,或是找尋已安裝 OpenSSL 軟體的主機,後續將 會使用到。

Windows 版 OpenSSL 軟體連結,可以只安裝「light」的版本即可: <u>https://www.openssl.org/related/binaries.html</u>

四、由於 Windows Server 2003 預設並不支援 SHA256 憑證,請依照您的需求參考以下連結,進行更新。

http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx

五、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。
開啟 IIS 管理員,並對著安裝憑證的站台點選右鍵→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(1	D 説明(H)			_ <del>8</del> ×
← → 🗈 🖬 🗙 🗃 🗔 🛱	皇   ▶ ■			
▲ 開際網路資訊服務 ● ● Wh63D1FZIPKECF (本機 ● 應用程式集區 ● 應用程式集區 ● multic 中國要求 一個的 一個的 一個的 一個的 一個的 一個的 一個的 一個的	路徑	状	· 況	

憲證匯出精靈		×
	歡迎使用憑證匯出精霊	
	這個精靈將協助您從憑證存放區將憑證、憑證信任 清單及憑證撤銷清單複製到您的磁碟中。	
	憑證由憑證授權單位簽發,能識別您的身分,並包含 用來保護資料或建立安全性網路連線的資訊。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(B) 下一步(B) 取消	_
憑證匯出精靈		×
禁證匯出精量 匯出私密金鑰 您可以選擇將私密金鑰與	憑證─起匯出。	×
<ul> <li>無證匯出精靈</li> <li>匯出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下	×
<ul> <li>無證匯出精靈</li> <li>匯出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> <li>您想將私密金鑰與憑證</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起 <u>匯</u> 出?	×
<ul> <li>無證匯出精靈</li> <li>匯出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> <li>您想將私密金鑰與憑證一</li> <li>運,匯出私密金鋪</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出?	×
<ul> <li>○ 否,不要進出私室</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ☆ 錀 ②	×
<ul> <li>○ 否,不要進出私室</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ☆金鑰②	×
<ul> <li>基證匯出精量</li> <li>通出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> <li>您想將私密金鑰與憑證</li> <li>● 是,匯出私密金鋪</li> <li>● 否,不要匯出私密</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ☆金鑰②	×
<ul> <li>○ 否,不要谁出私室</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ☆金鑰②	×
<ul> <li>歴出私密金鑰</li> <li>歴出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> <li>您想將私密金鑰與憑證</li> <li>● 是,匯出私密金鋪</li> <li>● 否,不要匯出私密</li> </ul>	憑證一起匯出。 。如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ☆金鑰②	×
<ul> <li>歴出私密金鑰</li> <li>歴出私密金鑰</li> <li>您可以選擇將私密金鑰與</li> <li>私密金鑰受到密碼的保護</li> <li>一頁輸入密碼。</li> <li>您想將私密金鑰與憑證</li> <li>① 徑, 隆田私密金鑰</li> <li>① 否,不要隆出私密</li> </ul>	憑證一起匯出。 • 如果您要將私密金鑰與憑證一起匯出,您必須在下 起匯出? ○ ○ ○ ○ ○ ○ ★ (四) 下一毋(四) 下一毋(四) 面消	



憲證匯出精靈	×
<b>要匯出的檔案</b> 請指定您要匯出的檔案名稱	
檔案名稱(E):	
C:\sha1_bak.pfx	瀏覽(R)
	《上一步图 下一步四) 取消
憲證匯出精霊	×
	名成憑證匯出精靈。 四已經成功地完成憑證匯出精靈。 四已指定下列新設定: 描葉名稱
	<上一步(B) 完成 取消
意意匯出精畫 × 匯出成功。 確定	

六、開啟「命令提示字元」,進入安裝 OpenSSL 目錄下的 bin 資料夾。



七、由 pfx 檔案分離出私密金鑰。

執行以下指令,並輸入從 IIS 匯出 pfx 時的密碼:

openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>



八、將私密金鑰與SHA256 憑證重新合併成 pfx 檔案 執行以下指令,並輸入兩次 pfx 檔案匯出密碼: openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path>



X

九、移除 SHA1 憑證,並匯入 SHA256 憑證。

回到IIS管	·理貞,並點選「伺服器憑證」			
🧯 網際網路資訊服	務 (IIS) 管理員			_ 6
🌀 檔案 🕑 🛛 執行 🛅	酿的相站 內容	?×		_15
⇐ ⇒   🗈 💽	網站 效能 ISAPI 篩選器 主目錄	文件		
衛 網際網路資訊	目錄安全設定 HTTP 標頭 自訂	錯誤 狀況	]	
⊡~氦D1F2 ⊡~─── 應用程;	驗證及存取控制 於田厝名存取,並編輯這個咨询的驗			
□─────────────────────────────────────				
- ja mul				
	II 位址发網域名補限制			
	或拒絕到這個資源的存取。			
	編輯①			
	女主通訊 當存取這個資源時使用安全通訊並啓 (2010年10月17日)			
		<u></u>		
	確定した消しを用(か)			
	NER			
•				

ITTO the mark い 明い 肥 「 /つ 町 町 ) 睡 いが







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,請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。	
	諸按 [完成] 來關閉此精靈。	
	< 上一步 B) <b>完成</b> 取消	

十、匯入 SHA256 憑證

🧯 網際網路資訊 🖩	務 (IIS) 管理員		
🍯 檔案 🕑 🛛 執行	預設的網站 內容	<u>? ×</u>	_ B ×
<ul> <li>← →</li> <li>●</li> <li>●<td>- 網站 効能 ISAPI 篩選器 主 目錄安全設定 HTTP 標頭  </td><td>目錄 文件  </td><td>況 (</td></li></ul>	- 網站 効能 ISAPI 篩選器 主 目錄安全設定 HTTP 標頭	目錄 文件	況 (
□ ● ● <i>● 應用程</i> □ ● ● <i>■ 應用程</i> 一 ● <i>● 網站</i> 1 0 0 <i>預</i> 1 mu 1 mu 1 mu	驗證及存取控制	编輯(2)	
⊡- 🍎 網頁服	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(])	
	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。	D服器應證©) 按關應證(型) 編輯(型)	
	確定   取消   要	用(Δ)   説明	







IIS 憲證精靈	×
<b>匯入燕證密碼</b> 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。 密碼(P):	
	<上─步B(下─步M)> 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(止):		
	<上一步图 下一步图 >	取消



IIS 憑證精靈		×
	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。	
	目前已安裝憑證在此電腦。	
	如果您將來需要更新,取代,或刪除此新憑證,諸再 次使用精靈。	
	要關閉這個精靈,諸按 [完成]。	
	<上一步但( <b>完成</b> ) 取消	

十一、 匯入 PublicCA G2 憑證(若曾經匯入過,可以略過此步驟)。 PublicCA G2 憑證:<u>http://publicca.hinet.net/CHTM/download/PublicCA2\_64.crt</u>

Administrator				
管理您的伺服器	😡 我的電腦			
妏 Windows 檔案總管		•		
	👘 系統管理工具	•		
CA 前令従不子元	😂 印表機和傳真			
13事本	說明及支援(出)			
	≫ 搜尋⊗			
$\langle$	177 執行 R)			
	🖉 登出(L) 🚺	闢機(U)		
🥂 開始 🛛 🥭 🕑 👘 網際	網路資訊服務 (IIS)			
執行		<u>?</u> ×	1	
	· 婆豹本,立任武卿	怒媚败恣酒的之摇,		
	自動開啓。	까케이지의 14 신자비가 14 14 -		
開啓(0): ( 「「「」」」		•		
$\sim$				
	確定 取消	瀏覽(B)		
IT and the				
₩ 王控合1 横安(A) 検視(	♡) 我的最愛(∩) (	遺齋(W) 覚明(H)		
開新檔案(N)	Ctrl+N			
開啓舊檔( <u>()</u>	Ctrl+O			
1819(2) 另存新檔( <u>A)</u>	CEIHS			
新增移除嵌入式管理單:	元(M) Ctrl+M	這個檢視沒有項目可顯示。		
選項(!)				
<u>1</u> C:\WINDOWS\\inetsrv 2 C:\WINDOWS\system 32	Viis.msc Vifrg msc			
		,	, ""	

新增市移除嵌入式管理單元	? ×
獨立  延伸	
請使用這個畫面從主控台新增或移除獨立的嵌入式管理單元。	
將嵌入式管理單元 🔂 主控台根目錄	
描述	
[新增四]] 移除(R) 關於(B)	
	(文)消



憲證嵌入式管理單元	X
這個嵌入式管理單元將自動管理下列帳戶的憑證:	
○ 我的使用者帳戶(M)	
●電腦帳戶〇	
<上一步B(下一步M)> 取消	
深 標志 16	
選擇電腦	×
選擇電腦 諸選擇您要嵌入式管理單元管理的電腦。	×
選擇電腦 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幣自動管理: ○ 本機電腦 (執行這個主控合的電腦)(1);	×
選擇電腦 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管理的電腦。 ○ 本機電腦 (執行這個主控台的電腦)(L): ○ 呆一台電幣(A):	×
選擇電腦 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管理的電腦。 ○ 萍機電腦 (執行這個主控台的電腦)(L): ○ 另一台電腦(Δ): ○ 另一台電腦(Δ): ○ 另一台電腦(Δ): ○ 日本物動素素問題集合(4) へん 見ば(日本) 台湾東一法日本物動素素的(4) 中的資源。	×
選擇電醫 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幣自動管理: ○ 本機電腦(執行這個主控台的電腦)(L): ○ 另一台電腦( <u>A</u> ): ○ 另一台電腦( <u>A</u> ): □ 允許對選取的電腦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 ( <u>W</u> )	×
<ul> <li>選擇電監</li> <li>諸選擇您要嵌入式管理單元管理的電腦。</li> <li>這個嵌入式管理單元幣自動管理:</li> <li>○ 萍機電腦(執行這個主控台的電腦)(L):</li> <li>○ 另一台電腦(<u>A</u>):</li> <li>○ 另一台電腦(<u>A</u>):</li> <li>□ 尤許對選取的電腦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 (W)</li> </ul>	×
選擇電監 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幣自動管理: ○ 萍機電腦(執行這個主控合的電腦)(L): ○ 另一台電腦(Δ): □ 先許對選取的電腦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 (W)	
選择電監 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幣自動管理: ○ 萍機電腦(執行這個主控音的電腦)(L): ○ 另一台電腦( <u>A</u> ): ○ 另一台電腦( <u>A</u> ): □ 允許對選取的電腦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 (W)	×
選擇電腦         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管理的電腦()         • 本機電腦(執行這個主控台的電腦)(L):         • 牙一台電腦(A):         ⑦覽(R)         ● 九計對選取的電腦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 (W)	×
選擇電腦 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培申動管理: • 本機電腦(執行這個主控台的電腦)(L): • 另一台電腦(A): ① 另一台電腦(A): ① 允許對選取的電腦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 (W)	×
選擇電醫 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: ● 萍機電腦(執行這個主控台的電腦)(L): ● 另一台電腦( <u>A</u> ): □ 先許對選取的電腦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 (W)	×
選擇電腦       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幣自動管理:       李機電腦(執行這個主控音的電腦)(L):       予一台電腦(Δ):       ⑦厚(L)       九許對選取的電腦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 (W)	

新增獨立嵌入式管理軍元		<u>?</u> ×
可用的獨立嵌入式管理單元:		
嵌入式管理單元	廠商	
🖓 電話語音	Microsoft Corporation	
🛛 👺 磁碟重組工具	Microsoft Corp, Executi	
→ 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	
國 憑證授權單位	Microsoft Corporation	
🙀 憑證 範本	Microsoft Corporation	-
111.54		_
振設嵌入式管理單元讓您瀏覽電腦或朋	服務的憑證存放內容。	
	$\sim$	-
	新理(4) 闘闘(	c) )
La construction de la construction		

新增用各除嵌入式管理單元	? ×
獨立 〕延伸	
請使用這個畫面從主控台新增或移除獨立的嵌入式管理單元。	
將嵌入式管理單元 🦳 主控合根目錄	
●● 「「」「「」」「「」」「「」」「」「」「」」「」「」「」」「」」「」」「」」「	
└ 描述	
· · · · · · · · · · · · · · · · · · ·	
MEAC 7	

注意 主 接 台 1		
檔案正子 執行(▲) 檢視(♥)	我的最愛(Q) 視窗(W) 說明(H)	
← → 🗈 💽 💼 🛃	毘   😫	
🚡 主控台根目錄\憑證 (本機	電腦)\中繼憲證授權(憑證	
主控台根目錄     一一一個人     一一一個人     一一一個人     一一一信任的根憑證授權     一一一企業信任     一一一一次有信     一一一没有信     一一一沒有信     一一一沒有信     一一一沒有信     一一一沒有信     一一一次有信     一一一次有信     一一一家證註     一一一家證註     一一一家證註     一一一家證註     王ナ     一一家證註     王十二章     五新整理     匯出諸單     隆出活單	<ul> <li> 發給 △ Government Root Certification Aut Government Root Certification Aut Government Root Certification Aut Government Root Certification Aut Microsoft Windows Hardware Com Microsoft Windows Hardware Com Microsoft Root A Public Certification Authority Public Certification Authority Root Agency Koot Agency Class 1 Public Pr Class 3 Public Pr States 1 CA Individual Sub Class 3 Public Pr States 1 CA Individual Sub Class 3 Public Pr States 2 Public Pr States 1 CA Individual Sub Class 3 Public Pr States 2 Public Pr Government Root States 2 Public Pr States 2 Pub</li></ul>	It Certification . It Certification . Iuthority ication Authori imary Certificat imary Certificat imary Certificat ot Certification . ot Certification .
<u> </u>		
<u> </u>		
意識唯人精量	<b>歡迎使用憑證匯入精霊</b> 這個精靈將協助您將憑證、憑證信任清單及憑 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, 用來保護資料或建立安全性的網路連線資訊。 放區是用來存放憑證的系統區域。 諸按 [下一步] 繼續。	≥ 遺撤銷 並包含 應證存
	<上一步( <b>下一步</b> 図)	取消

<b>證匯入精靈</b>	×
<b>匯入檔案</b> 华定你想更陈入的档案。	
檔案名稱(F):	
C:\PublicCA2_64.cer	D
請注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:	
個人資訊交換- PKCS #12 (.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(N) > ) 取	[] [] [] [] [] [] [] [] [] [] [] [] [] [
匯入精靈	×
<b>制設存放區</b> 進設方於原見用本方於進設的系体原因。	
思證任成會是用來任成思證的系統會學。	
Windows 會白勳選擇一個憑證存故區,您也可以聲憑證指定存於位置。	
○ 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(民)	
	 形像 【
	K7B

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: 使用者選取的應證存放圖 中語 內容	■。 継憑證授權 證
	· 個菜名稱 C:	PublicCA2_54.cer
	<上────────────────────────────────────	完成取消
憲證匯入精霊		
(1) 匯入執行成功。		
確定		
清主接台1		
	的最愛( <u>()</u> 親窗( <u>W</u> ) 説明( <u>H</u> )	
	r B. 2	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
1 土壤古像日球、急波(平陽电)	■八甲基常起文作に常設 ※ ^	
□ 🔄 💬 憑證 (本機電腦)	Government Root Certification Aut	Government Root Certification ,
	Government Root Certification Aut	Government Root Certification .
┃	Microsoft Windows Hardware Com	Microsoft Root Authority
	Public Certification Automity	ePKI Root Certification Authori
	Root Amney	Root Agency
┃	VeriSign Class 1 CA Individual Sub	Class 1 Public Primary Certificat
□ □ □ 沒有信任的憑證	VeriSign Class 2 CA - Individual Su	Class 2 Public Primary Certificat
┃	当www.vensign.com/CPS Incorp.by 副政府馮鹮答理由心。	Class 3 Public Primary Certificat
<ul> <li>□···□ 受信任的人</li> <li>□··□ 憑證註冊要求</li> <li>□··□ SPC</li> </ul>	■政府憑證管理中心	Government Root Certification
		F
中繼憑證授權 存放包含 11 個憑證	•	
		,

十二、 檢視 SHA256 憑證,並以瀏覽器檢視網頁是否正常運作。 回到 IIS 管理員,並點選「檢視憑證」

🧯 網際網路資訊 🖩	務 (IIS) 管理員			_ 8 ×
🌀 檔案 🕑 🛛 執行	預設的網站 內容	<u>? ×</u>		_ <b>8</b> ×
◆ → È I 約除網路資訊 ● ● Wh-63DIF ● ● 應用程: ● ● 網站 100 mul	網站         效能         ISAPI 篩選器         主目錄         文           目錄安全設定         HTIP 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。		<b>:</b> 決兄	
— 会 muł ⊡- <mark>)</mark> 網頁服	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。 			
	女主通訊 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(2) 編輯(2)			
	確定 取消 裏用(点)	〕 說明		
4				

憲副		? ×
[	般 詳細資料 愚證路徑	1
	馬賓盧廣	
	這個憑證的使用目的如下:	-
	● 所有應用程式原則	
		- 1
	<b>登給:</b> www.test.com.tw	
	登行者: Public Certification Authority - G2	
	- <b>右☆期白</b> 20152246 <b>20</b> 20202246	
	10月11日11日11日11日11日11日11日11日11日11日11日11日11日	
	28-6元中4年8日月 / m.	
	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	
	·····································	
_		2

- 一、適用於申請時,有同時取得 SHA1、SHA256 憑證。或是憑證在效期內,經由 審驗人員再次核發 SHA256 憑證者。
- 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、需要先備妥 OpenSSL 軟體,或是找尋已安裝 OpenSSL 軟體的主機,後續將 會使用到。

Windows 版 OpenSSL 軟體連結,可以只安裝「light」的版本即可: <u>https://www.openssl.org/related/binaries.html</u>

四、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。

開啟 IIS 管理員,點選「伺服器憑證」



於要匯出的憑證右鍵→匯出

匯出憑證					? ×
匯出到(E):					
C:\sha1_bak.pfx					
密碼(P):					
確認密碼(M):					
$\sim$	-			The SNP	
		唯疋	_0_	取)月	

五、開啟「命令提示字元」,進入安裝 OpenSSL 目錄下的 bin 資料夾。 請依實際安裝路徑做調整



六、由 pfx 檔案分離出私密金鑰。

執行以下指令,並輸入從 IIS 匯出 pfx 時的密碼:

openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>



七、將私密金鑰與 SHA256 憑證重新合併成 pfx 檔案 執行以下指令,並輸入兩次 pfx 檔案匯出密碼: openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path> -name <alias name>



#### 八、匯入 SHA256 憑證。



重新回到 IIS 管理員,並點選「匯入」

匯入憑證		? ×	
馮證 <b>檔案 (</b> ufx)(C):			
Cásha2 halt afu			
C.wnaz_bak.prx			
密碼(P):			
(		_	
□ · · · · · · · · · · · · · · · · · · ·			
Internet Information Services (IIS	5) 管理員		
S S WIN-R8R71VJUK	.VM >		🔄 🖸 🖾 🔛 🖸 🖸
檔案(F) 檢視(∀) 說明(H)			
連線	▲ 「「「「「「「」」」 「「」」 「「」 「」 「」 「」 「」 「」 「」 「		動作
🔍 - 📃 🖄 😽			匯入
	此功能可用來要求及管理網百信	T服器可與針對 SSL 設定的網站搭配	建立憑證要求
□ Y WIN-R8K71YJUKYM (WIN-R8	使用的憑證。		完成憑證要求
	_名稱 ▲	發行給	· · · · · · · · · · · · · · · · · · ·
	4chain	www.4chain.com.tw	》年上江前94%(20) 起
	ErrorSubjectAltName	169.254.255.161	建立自我簽署憑證
	iis_multidomain	www.test1.com.tw	檢視
	IP	169.254.255.161	陈史
	new4chain	www.new4cnain.com	
	www.test.com.tw/	www.test.com.tw/	史新
	www.test.com/w/122.htm	www.test.com.tw/123.htm	★ 移除
	www.test.com.tw-SHA256	www.test.com.tw	🔞 說明
	WWW.WIN2000.COM.IW	WWW.WIN2008.COM.TW	線上說明
	•	F	
			1
	📰 功能檢視 🜈 內容檢視		
就緒			6
🥂開始 🛛 🚠 📰 🏉 👋 🛛 💱 Int	ernet Information Servi		😢 🛱 🚰 🌄 🕢 🗊 🕼 下午 02:25

九、匯入 PublicCA G2 憑證(若曾經匯入過,可以略過此步驟)。 PublicCA G2 憑證:<u>http://publicca.hinet.net/CHTM/download/PublicCA2\_64.crt</u>

程式集		
mmc.exe	8	
	Administrator	
	文件	
	电脑	
	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		
	<u>○</u>	
—————————————————————————————————————	mation Servi	
嘉主接台1 - [主接台根目錄]		
🧧 檔案(F) 執行(A) 檢視(V) 我的最愛(C	) 視窗(₩) 說明(H)	X
< 開新檔案(№) Ctd+№	I	
開設告檔(0) Ctrl+C (は友(5)) Ctrl+S		動作
另存新檔(A)	≷有項目可顯示。	主控台根目錄 🔺
新增移除嵌入式管理單元(M) Ctd+h 選項(r)	4	其他動作  ▶
1 ServerManager.msc		
2 C:\Windows\\certmgr.msc		
3 C:\Windows\\services.msc 4 C:\Windows\System32\comeyn msc		
(注重(X)		
1		1

新增或移除嵌入式管理單	元		×
您可以為這個主控台從您。 元。對於可延伸的嵌入式。	的電腦上可以使用的嵌入 管理單元,您可以設定剧	、式管理單元中選擇一些嵌入式管理單元,並且 如用哪些延伸。	設定所選擇的嵌入式管理單
可用的嵌入式管理單元(%)	:	選取的嵌入式管理單元(E):	
嵌入式管理單元	廠商   ▲	1 主控台根目錄	
🧧 終端機服務管理員	Microsoft Cor		1000 m
🔢 群組原則物件編輯器	Microsoft Cor		移床(尺)
🛁 裝置管理員	Microsoft Cor		
📔 資料夾	Microsoft Cor		往上移(U)
<u> </u> 路由及遠端存取	Microsoft Cor		往下移の)
電腦管理	Microsoft Cor 🌈 👔	新增(A) > 🚺	12 1 10 (07)
1 の 電話語音	Microsoft Cor		
■ 磁碟管理	Microsoft 與		
○ 網址建結	Microsoft Cor		
■ 調路仔収保護 (NAP… 「毎 はまま」	Microsoft Cor		
	Microsoft Cor		
	Microsoft Cor		進階(V)
描述:			
憑證嵌人式管理單元讓您	瀏覽電腦或服務的憑證在	字放内容。	
1			
		Γ	確定取消
准备出工业处理现二			
急波嵌入內官理里兀			
這個嵌入式管理單	元將自動管理下列帷	夏戶的憑證:	
○ 我的使用者帳月	≠(M)		
○ 服務幅戶(S)			
(• 電腦帳尸(C)	<b>)</b>		
		$\sim$	
		<上一步(L) 下一步(N) >	1) 取消

<ul> <li>本機電腦(L):</li> </ul>	(執行這個主控台	(的電腦)	<b>S</b>			
<ul> <li>- 日本市場(4)</li> </ul>		(47-6/6/		3	alera l	
				//	#1.5-5 (4.5) ····	
□ 九許對選取的 (₩)	的電腦進行從命令	列所散動的	變更。這只在您( 	諸存主控台後	才能適用	
			《上一步四	完成	取消	
			<上─步@	完成	取消	
或移除嵌入式管理軍			< 上─步Œ	完成	取消	- ]
或移除嵌入式管理軍	元	21-+		完成	取消	-
或移除嵌入式管理軍 可以為這個主控台從您 。對於可延伸的嵌入式	<b>元</b> 的電腦上可以使用的 管理單元,您可以設分	发入式 <b>管理單</b> 元 定散用哪些延伸	<上一步(正) 亡中選擇一些嵌入式管 ♥ •	完成	<b>取消</b> 设定所選擇的嵌入式	-   
<b>或移除嵌入式管理單</b> 可以為這個主控台從您 。對於可延伸的嵌入式 目的嵌入式管理單元(S)	元 的電腦上可以使用的 管理單元,您可以設立 :	於入式管理單元 定散用哪些延何	<上一步(正) 在中選擇一些嵌入式管理單 選取的嵌入式管理單	完成 奇理單元,並且言 元(E):	<b>取消</b> 设定所選擇的嵌入式	-   
<b>或移除嵌入式管理單</b> 可以為這個主控台從您 。對於可延伸的嵌入式 目的嵌入式管理單元(S) 入式管理單元	元 的電腦上可以使用的 管理單元,您可以設定 : 廠商	於入式管理單元 2112日明哪些延伸	<上一步(正) 在中選擇一些嵌入式管 建取的嵌入式管理單 一 主控台根目錄	完成 <sup>会理單元,並且論</sup> 元(E):	取消 改定所選擇的嵌入式 編輯延伸(X	_ 】 】 】
<b>或移除嵌入式管理單</b> 可以為這個主控台從您 。對於可延伸的嵌入式 目的嵌入式管理單元(S) (入式管理單元 	元 的電腦上可以使用的 管理單元,您可以設立 : <u>廠商</u> Microsoft Cor	款入式管理單元 2敗用哪些延作	< 上一步(正 上一步(正 上中選擇一些嵌入式管 地 建取的嵌入式管理單 ■ 主控台根目錄 □ 二 主控台根目錄 □ 二 二 二 二 二 一 二 一 一 一 一 一 一 一 一 一 一 一 一	完成 管理單元,並且言 (元(E): 腦)	取消 設定所選擇的嵌入式 編輯延伸(X 系除(R)	-      )
<b>或移除嵌入式管理單</b> 可以為這個主控台從您 對於可延伸的嵌入式 問的嵌入式管理單元(S) 記式管理單元 終端機服務管理員 群組原則物件編輯器	元 的電腦上可以使用的 管理單元,您可以設力 : <u>廠商 ▲</u> Microsoft Cor Microsoft Cor Microsoft Cor	₭入式 <b>管理單</b> 元 定散用哪些延作	< 上一步(正 亡中選擇一些嵌入式管 建取的嵌入式管理單 ■ 主控台根目錄 □ 憑證 (本機電	完成 管理單元,並且言 元(E): 腦)	<b>取消</b> 取消   数定所選擇的嵌入式   编輯延伸(X   移除(R)	-      )
或移除嵌入式管理軍 可以為這個主控台從您 對於可延伸的嵌入式 問的嵌入式管理單元(3) 入式管理單元 終端機服務管理員 群組原則物件編輯器 裝置管理員 容料來	<b>元</b> 的電腦上可以使用的 管理單元,您可以設力 : Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	款入式管理單元 定啟用哪些延伸	< 上一步(正 亡中選擇一些嵌入式管 建取的嵌入式管理單 ■ 主控台根目錄 □ 漂 濃 (本機電	完成 管理單元,並且調 元(E): 腦)	<b>取消</b> 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上我(II	-           
或移除嵌入式管理單 可以為這個主控台從您 對於可延伸的嵌入式 問的嵌入式管理單元(3) (入式管理單元 各端 機服務管理員 帮組原則物件編輯器 裝置管理員 資料來 (路中及读端存取	<b>元</b> 的電腦上可以使用的 管理單元,您可以設定 : <u>厳商</u> ▲ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	₭入式管理單元 定啟用哪些延伸	< 上一步(正 亡中選擇一些嵌入式管 灣。 選取的嵌入式管理單 ■主控台根目錄 □ 主控台根目錄 □ 憑證 (本機電	完成 管理單元,並且言 (元(E): 腦)	<b>取消</b> 股消 股消 股定所選擇的嵌入式 後定所選擇的嵌入式 後定所選擇的嵌入式 後定所選擇的嵌入式 後定所選擇的嵌入式 後定所選擇的嵌入式	- 【 】 )… )
或移除嵌入式管理單 可以為這個主控台從您 對於可延伸的嵌入式 開的嵌入式管理單元 終端機服務管理員 詳組原則物件編輯器 裝置管理員 資料來 路由及遠端存取 軍腦管理	元 的電腦上可以使用的 管理單元,您可以設定 : <u>厳商</u> ▲ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	於入式管理單元 定啟用哪些延伸	< 上一步(正 亡中選擇一些嵌入式管 ₱。 選取的嵌入式管理單 ■主控台根目錄 □ 主控台根目錄 □ 二 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	完成 奇理單元,並且言 (元(E): 腦)	<b>取消</b> 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(0) 往下移(0)	- 【 】 〕 〕 〕
或移除嵌入式管理單 可以為這個主控台從您 ○對於可延伸的嵌入式 問的嵌入式管理單元(2) (2) (2) (2) (2) (2) (2) (2) (2) (2)	元 的電腦上可以使用的 管理單元,您可以設定 : <u>厳商</u> ▲ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	₭入式管理單元 定設用哪些延伸 新増(A) >	< 上一步(正 亡中選擇一些嵌入式管 ■・ 選取的嵌入式管理單 ■主控台根目錄 □ 主控台根目錄 □ 二 推電	完成 奇理單元,並且言 (元(E): 腦)	取消 设定所選擇的嵌入式	- 【 】 )… )
或移除嵌入式管理單 可以為這個主控台從您 對於可延伸的嵌入式 開的嵌入式管理單元(S) (入式管理單元 (S) (大式管理單元) (S) (大式管理單元) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S	元 的電腦上可以使用的 管理單元,您可以設定 : <u>厳商</u> ▲ Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	於入式管理單元 定 散用哪些延伸 新増(A) >	< 上一步(正 中選擇一些嵌入式管 ● 2 2 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3	完成 <sup> 許理單元,並且該 :元(E): 腦)</sup>	取消 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(D)	- 【管 )
或移除嵌入式管理單 可以為這個主控台從忽 對於可延伸的嵌入式 明的嵌入式管理單元(3) 以式管理單元 終端機服務管理員 群組原則物件編輯器 裝置管理員 資料夾 略由及遠端存取 電話語音 磁碟管理 網址連結	元 的電腦上可以使用的 管理單元,您可以設定 : 厳商 Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	於入式管理單元 該用哪些延何   新増(A) >	< 上一步(正 中選擇一些嵌入式管理單 ■ 主控台根目錄 □ 主控台根目錄	完成 辞理單元,並且言 (元(E): 腦)	取消 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(D)	- 【 】 )… )
或移時嵌入式管理單 可以為這個主控台從您。 對於可延伸的嵌入式 開的嵌入式管理單元(%) 又式管理單元 終端機服務管理員 群組原則物件編輯器 裝置管理員 資料夾 略由及遠端存取 電腦管理 電話語音 磁碟管理 網址連結 網路存取保護(NAP	元 的電腦上可以使用的 管理單元,您可以設定 : 厳商 Microsoft Cor Microsoft Cor	於入式管理單元 定敵用哪些延何 新増(A) >	< 上一步(正 中選擇一些嵌入式管理單 ■ 主控台根目錄 □ 主控台根目錄 □ 二 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	完成 奇理單元,並且言 元(E): 腦)	取消 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(D)	- 【 】 】 】 】
式移除嵌入式管理單 可以為這個主控台從您 對於可延伸的嵌入式 用的嵌入式管理單元(3) (入式管理單元 線端機服務管理員 群組原則物件編輯器 裝置管理員 資料夾 路由及遠端存取 電腦管理 電話語音 磁碟管理 網路存取保護 (NAP 發端端点面	元 的電腦上可以使用的報 管理單元,您可以設定 : 颜商  ▲ Microsoft Cor Microsoft Cor		< 上一步(正 中選擇一些嵌入式管理單 選取的嵌入式管理單 ■ 主控台根目錄 □ 二 注控台根目錄 □ 二 二 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	完成 奇理單元,並且詞 元(E): 腦)	取消 设定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(D)	
或移降嵌入式管理單 可以為這個主控台從您 。對於可延伸的嵌入式 問的嵌入式管理單元(ぷ) ?入式管理單元 終端機服務管理員 帮組原則物件編輯器 裝置管理員 資料夾 略由及遠端存取 電腦管理 國點管理 網址連結 網路存取保護(№AP 遠端桌面 憑證	元 的電腦上可以使用的損 管理單元,您可以設況 : 廠商 Microsoft Cor Microsoft Cor	嵌入式管理單元 定敵用哪些延伸 新増(Δ)>	< 上一步(正 中選擇一些嵌入式管 建取的嵌入式管理單 ■ 主控台根目錄 ■ 法控台根目錄 ■ 憑證 (本機電	完成 管理單元,並且記 元(E): 腦)	取消 設定所選擇的嵌入式 編輯延伸(X 移除(R) 往上移(D) 往下移(D)	
或移除嵌入式管理單 可以為這個主控台從您。 對於可延伸的嵌入式 目的嵌入式管理單元(ぷ) (入式管理單元 終端機服務管理員 脊紺原則物件編輯器 裝置管理員 資料夾 略由及遠端存取 電腦管理 爾址連結 網路存取保護(MAP 透端桌面 憑證	元 的電腦上可以使用的損 管理單元,您可以設定 : 廠商 Microsoft Cor Microsoft Cor	嵌入式管理單元 差散用哪些延伸 新増(Δ)>	< 上一步(正 中選擇一些嵌入式管理 選取的嵌入式管理單 ■ 主控台根目錄 ■ 法控台根目錄 ■ 法控台根目錄	完成 <sup>各理</sup> 單元,並且 元(E): 腦)	取消 設定所選擇的嵌入式	

🚟主控台1 - [主控台	根目錄\憑證 (本機	憲電腦)\中総憑言	[授權\憑證]		_ 🗆 🗵
\overline 🚠 檔案(F) 🛛 執行(A)	檢視(V) 我的₽	最愛(O) 視窗(W	) 說明(H)		_ 8 ×
🗢 🔿 🖄 📅 🗈	] 🛛 😹 🛛 🖓	DI			
主控台根目錄 通 憑證 (本機電腦) ■ 個人 ■ 信任的根憑證 ■ 企業管住 ■ 空作情 所有 ■ 受信情 依視 ■ 受信情 日 ■ 読證 ■ 受信情 日 ■ 読書 ■ 受信者 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	發給     GCA2     GRCA2     GRCA2	lows Hardware Cor tion Authority 1 CA Individual Su 匯入(1)	發行者 GRCA2 GRCA a Microsoft Root Author ePKI Root Certification Root Agency Class 1 Public Primary Class 2 Public Primary Class 3 Public Primary	itty n Auti Certif Certif	▲ D作 ►
[23] 四字可以在建個項目上:	轵1丁比更1作。 				

急避难入有釜		의
	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撒鎖 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(B <b>(下一步(N)</b> ) 取消	

<b>5 證</b> 匯入精靈		×
匯入檔案		
指定您想要匯入的檔案。		
		_
檔案名稱(F):	VOLUME AN	
C:PublicCA2_64.cer	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)		
深入了解 <u>憑證檔案格式</u>		
		_
	<上一步(E) 下一步(N)> 取消	1
5. 遺殖入精靈		×
些 <b>設</b> 種入精靈 		×
些 <b>設                                    </b>	•	×
<b>些說難入精靈</b> <b>憑證存放區</b> 憑證存放區是用來存放憑證的系統區域	•	×
告說 随入 精泰 憑證存放區 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。	×
些說 随入 精泰 憑 波存放 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。	×
<ul> <li></li></ul>	。 您也可以為憑證指定存放位置。 故區(U)	×
<ul> <li>基邊住入 精靈</li> <li>基邊存放區</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證猶知來選取憑證存,</li> <li>第所有憑證放入以下的存放區(P)</li> <li>運送互致性。</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U) ▶	×
<ul> <li>基邊住入 精靈</li> <li>基邊存放區</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>① 自動根據憑證類型來選取憑證存;</li> <li>④ 將所有憑證放入以下的存放區(?)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U)	×
<ul> <li>些違狂入精靈</li> <li>&gt; 憑證存放區</li> <li>&gt; 憑證存放區是用來存放憑證的系統區域</li> <li>○ 附前dows 會自動選擇一個憑證存放區,</li> <li>○ 自動根據憑證類型來選取憑證存,</li> <li>○ 自動根據憑證類型來選取憑證存,</li> <li>○ 將所有憑證放入以下的存放區(?)</li> <li>&gt; 憑證存放區:</li> <li>□ 中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U)	×
<ul> <li>基邊住入 精靈</li> <li>基邊存放區</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證猶知來選取憑證存,</li> <li>節將所有憑證放入以下的存放區(P)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U) ┣️	×
<ul> <li>基證在入構整</li> <li>基證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證類型來選取憑證存;</li> <li>第所有憑證放入以下的存放區(P)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U) 》 瀏覽(R)…	×
<ul> <li>基邊住入 積極</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證類型來選取憑證存,</li> <li>自動根據憑證類型來選取憑證存,</li> <li>密新所有憑證放入以下的存放區(?)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U) 》 瀏覽(R)	×
<ul> <li>法設在入積蒸</li> <li>通過存放區</li> <li>通過存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證猶型來選取憑證存,</li> <li>第所有憑證放入以下的存放區(?)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 故區(U) 》 瀏覽(R)	×
<ul> <li>基證存放區</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證類型來選取憑證存</li> <li>衛筋所有憑證放入以下的存放區(P)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	。 您也可以為憑證指定存放位置。 效區(U)	×
<ul> <li>基證存放區</li> <li>憑證存放區是用來存放憑證的系統區域</li> <li>Windows 會自動選擇一個憑證存放區,</li> <li>自動根據憑證類型來選取憑證存;</li> <li>將所有憑證放入以下的存放區(?)</li> <li>憑證存放區:</li> <li>中繼憑證授權</li> </ul>	☆ 您也可以為憑證指定存放位置。 放區(U) 瀏覽(R)	×
些波旺入转数          邁波在入转数         邁波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,         ● 自動根據憑證類型來選取憑證存,         ● 自動根據憑證類型來選取憑證存,         ● 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	◎ 您也可以為憑證指定存放位置。 放區(U) 瀏覽(R)	×

憑證匯入精靈			×
	完成憑證匯入精靈		
- Contraction of the Contraction	按一下 [完成],即匯入憑證	•	
	您已指定下列新設定·		
	使用者選取的憑證存放區	中繼憑證授權	
	▲ 内容 檔案名稱	憑證 C\PublicCA2 f4 cer	
		$\frown$	-
	<u> &lt; 上一步(B)</u>	完成    取消	
憑證匯入精靈	×		
(1) 匯入執行成功。			
藤定			
喜主控台1 - [主控台根目錄)	憑證 (本機電腦)\中繼憑證授	[權]]]]	
🚠 檔案(F) 執行(A) 檢視(N	₩) 我的最愛(0) 視窗(\\)	說明(H)	_ 8 ×
🗢 🔿   🚈 📰 🕹 👘	🗙 🗈 🗟 🔽 📊		
主控台根目錄 發給	*	發行者	動作
🗊 憑證 (本機電腦)   🔄 GCA	A2	GRCA2	憑證 ▲
<ul> <li>□ □ □</li> <li>□ □<th>zaz rosoft Windows Hardware Com</th><th>Microsoft Root Authority</th><th>其他動作 ▶</th></li></ul>	zaz rosoft Windows Hardware Com	Microsoft Root Authority	其他動作 ▶
■ ■ □ 企業信任	lie Certification Authority	ePKI Root Certification Auth	Public Certifi 🔺
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	lic Certification Authority - G2	ePKI Root Certification Auth Root Agency	其他動作 ▶
	iSign Class 1 CA Individual Su	Class 1 Public Primary Certif	
Ⅱ Ⅲ	Sign Class 2 CA - Individual S	Class 2 Public Primary Certif	
🗉 🧰 第三方根憑證1 🔤 ₩₩₩	w.verisign.com/CPS Incorp.by	Class 3 Public Primary Certif	
□ 🔲 党信任的人			
田 🧰 智慧卡信任根			
			1

十、於站台上換上 SHA256 憑證。

點選需要更換 SHA256 憑證的站台→「繫結」

(案(F) 檢視(∀) 說明(H)		
â		動作
· 🗔 🖄 🕵	Office Default Web Site 百頁	
🖣 起始網頁		編輯權限
🍯 WIN-R8R71VJUKVM (WIN-R) 山 🔊 唯田段式住區		编辑站台
□ · · · · · · · · · · · · · · · · · · ·		
🗄 🔮 Default Web Site		□ 基本設定
± € test2	CGI HTTP 回應標 HTTP 重新導 IPv4 位址及 頭 向 網域限制	檢視應用程式
	Lidux)APPerfix End	檢視虛擬目錄
		管理網站 📀
	ISAPI 篩選器 MIME 類型 SSL 設定 URL Rewrite	😂 重新殷動
		2011711
	失敗要求的 記錄 授權規則 處理常式對	/#J夏/#986
	追蹤規則 應 	<ul> <li>○ 湖覽 *:443 (https)</li> </ul>
		· · · · · · · · · · · · · · · · · · ·
	I INCOME INCOME	失敗要求的追蹤
		限制
		20 說明
•	📰 功能檢視 💦 內容檢視	線上說明
ž		•
台繫結		? ×
類型 主機名稱	連接埠 IP 位址 緊結	新增(A)
http		(6#P.07)
https	443 * 🔿 🔍	(后本註(下)
		移除(R)
•		瀏覽(B)
		關閉( <u>C</u> )
19 シトノン 御史 6千	2	Y

连续	X
一般」詳細資料「馮譜路徑」	
	- 1
「「「」」 「「」」 「「」」 「」」 「」」 「」」 「」」 「」」 「」」	
這個憑證的使用目的如下:	-
● 所有應用程式原則 ● ■	
7866	-
Se and : www.test.com.tw	
發行者: Public Certification Authoriy - G2	
<b>有效期</b> 自 2015/2/16 到 2020/2/16	
♀」「個憑證有一個對應的私密金鑰。	
遊發者聲明(3)	
/未入了 <b>附<u>愿意</u></b>	
·	
编辑站台繁結	<u>? ×</u>
類型(T): IP 位址(I): 連接埠(O): 全部未指派 - 443	
→ 「 」 「 」 」 「 」 」 「 」 「 」 「 」 「 」 「 」 」 「 」 」 「 」 」 「 」	
SSL 憑證(S):	
www.test.com.tw-SHA256 橄視(V)	
確定 取消	肖
站台繫結	? ×
類型 主機名稱 連接埠 IP 位址 緊結	新增(A)
http 80 * https 443 *	編輯(E)
	移除(R)
	 瀏覽(B)
	限制程(〇)

十一、 以瀏覽器檢視網頁是否正常運作。

- 一、適用於申請時,有同時取得 SHA1、SHA256 憑證。或是憑證在效期內,經由 審驗人員再次核發 SHA256 憑證者。
- 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、需要先備妥 OpenSSL 軟體,或是找尋已安裝 OpenSSL 軟體的主機,後續將 會使用到。

Windows 版 OpenSSL 軟體連結,可以只安裝「light」的版本即可: <u>https://www.openssl.org/related/binaries.html</u>

四、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。

開啟 IIS 管理員,點選「伺服器憑證」

Internet Information Services (IIS) 管理員	_ <b>□</b> ×
€ VIN-8IHG1LIL8C6 →	😂 🖂 🔞 🕡 -
「 「 「 描案(E) 檢視(V) 説明(H)	
<ul> <li>●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●</li></ul>	<ul> <li>勤作</li> <li>管理伺服器</li> <li>重新設動</li> <li>該動</li> <li>停止</li> <li>檢視應用程式集區</li> <li>檢視站台</li> <li>取得新的鏡頁平台元件</li> <li>說明</li> <li>總上說明</li> </ul>
12 11 11 11 11 11 11 11 11 11 11 11 11 1	• <u>1</u> .:



匯出憑證 <b>? ×</b>	
匯出到(E):	
C:\sha1_bak.pfx	
密碼(P)	
•••••	
· 確認恋理(\\./\·	
確定 取消	

五、開啟「命令提示字元」,進入安裝 OpenSSL 目錄下的 bin 資料夾。 請依實際安裝路徑做調整



六、由 pfx 檔案分離出私密金鑰。

執行以下指令,並輸入從 IIS 匯出 pfx 時的密碼:

openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>



七、將私密金鑰與 SHA256 憑證重新合併成 pfx 檔案

執行以下指令,並輸入兩次 pfx 檔案匯出密碼:

openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path> -name <alias name>



八、匯入 SHA256 憑證。

重新回到 IIS 管理員,並點選「匯入」



匯入憑證	?	x
憑證檔案 (.pfx)(C):		
C:\sha2_bak.pfx		
密碼(P):		
•••••		
選取憑證儲存區(S):		
個人		~
✓ 允許匯出此憑證(A)		
確定	取消	

8	Internet Inf	ormation Services (IIS) 管	理員	_ <b>_</b> X
WIN-8IHG1LIL	8C6 <b>•</b>			🖅 🖂 🟠 🔞 🕶
檔案(F) 檢視(V) 說明(H)				
in anti y in soluti y in soluti y	● 印服器憑證 此功能可用來要求及管理網頁	司服器可與針對 SSL 設定的網站搭 ▼ 常 移至(G) - ☆ 全部顯示(A) 發行給 www.20170101.com.tw www.is8.multi1.com.tw www.is8.multi2.com.tw www.test.com.tw	a配使用的憑證。	堕人           建立憑證要求           完成憑證要求           建立启我簽署憑證           建立自我簽署憑證           後視           運動:           資金:           東新           ※ 移除           診明           線上説明
< III >	📰 功能檢視 🚰 內容檢視			
就緒				• <b>1</b> .:

九、匯入 PublicCA G2 憑證(若曾經匯入過,可以略過此步驟)。 PublicCA G2 憑證:<u>http://publicca.hinet.net/CHTM/download/PublicCA2\_64.crt</u>

		應	用和 nmc	呈式	"mmc	"	▶	搜 應用和 一一 一 〇 〇	子 呈式 應用程 設定 構案 Intern	) 完 et Explorer	م ×	1 0 0
					主控	台1 -	·[主控台根目錄]			_		x
檔案	(F)	動作(A)	檢視(V)	我的最愛(O)	視窗(W)	說明	1(H)				_ E	7 ×
	開新	·檔案(N)			Ctrl+	٠N						
	開啟	(O)			Ctrl+	0				動作		—
	儲存	E(S)			Ctrl	+S	2 有百日可照云。			主控台根	日錄	
	另存	新檔(A)					2月4月日日期小、			「上」王山山は	니 34.5 /도	•
$\leq$	新增 選項	/移除嵌 <i>)</i> (P)	\式管理單;	元(M)	Ctrl+	М					F	ŗ
	1 C:	Window	/s\svstem3	2\CompMamt			-					
	结束	100		- (			-					
							]					

	新增或移	除嵌入式管理單元	x
您可以為這個主控台從您的電 入式管理單元,您可以設定顧	電腦上可以使用的嵌入式管理單元中選 效用哪些延伸。	挥一些嵌入式管理單元,並且設定所選擇的嵌,	入式管理單元。對於可延伸的嵌
可用的嵌入式管理單元(S):		選取的嵌入式管理單元(E):	
嵌入式管理單元	廠商へ	1 主控台根目錄	編輯延伸(X)
	. Microsoft Corp		5/214/D)
◎ 服務	Microsoft Corp		移际(K)
原則結果組 ▲ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★	Microsoft Corp		
◎ 災能監視薪	Microsoft Corp		上移(U)
1277年6年史	Microsoft Corp		下挖(D)
	Microsoft Corp 新增(A) >	>	下修(D)
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	Microsoft Corp		
B 路由及遠端存取	Microsoft Corp		
🌆 電腦管理	Microsoft Corp		
♣ 電話語音	Microsoft Corp 🗏		
🔄 磁碟管理	Microsoft 與 V		
20 編 <u>地</u> 連結	Microsoft Corp		No. 10
「「「「「「「」」」	Microsoft Corp		進階(V)
描述:			
馮諧嵌入式管理留元鐘你潮り	音雷腦或服務的馮證左於原內容。		
			確定 取消
	准證器	) 式管理器元	X
		八戎旨庄卑儿	
		八八百庄年九	
		八以自注单儿	
這個嵌入式管理單分	元將自動管理下列帳戶的憑證:	八以自注单儿	
這個嵌入式管理單分	·波祖·成 元將自動管理下列帳戶的憑證:	八以自注单儿	
這個嵌入式管理單元 〇 我的使用者帳戶	→ 2000 → 2000 元將自動管理下列帳戶的憑證: (M)	八以目注单儿	
這個嵌入式管理單元 〇 我的使用者帳戶	∞ ᡂ ↔ 元將自動管理下列帳戶的憑證: (M)	八以目注单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S)	∞ ᡂ ↔ 元將自動管理下列帳戶的憑證: (M)	八八百庄平儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ● 電腦帳戶(C)	∞ ᡂ ↔ 元將自動管理下列帳戶的憑證: (M)	八八百庄平儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ● 電腦帳戶(C)	∞ ᡂ ↔ 元將自動管理下列帳戶的憑證: (M)	八以目注单儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ● 電腦帳戶(C)	∞ ᡂ ↔ 元將自動管理下列帳戶的憑證: (M)	八以目注单儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ● 電腦帳戶(C)	∞ ᡂ ↔	八以目注单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 <u>服務帳戶(S)</u> ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八以目注单儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ <u>服務帳</u> 戶(S) ● 電腦帳戶(C)	- № 融 ↔ 元將自動管理下列帳戶的憑證: (M)	八,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ <u>服務帳</u> 戶(S) ● 電腦帳戶(C)	- 派祖 → K 元將自動管理下列帳戶的憑證: (M)	八,4,6,注单,1,6	
這個嵌入式管理單分 〇 我的使用者帳戶 〇 <u>服務帳戶(</u> S) ④ 電腦帳戶(C)	- 怒衄 ₩ 元將自動管理下列帳戶的憑證: (M)	八,4,6,注单,1,6	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八, 北 旨 珪 单 儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八北邑庄单儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	八, 北 旨 珪 单 儿	
這個嵌入式管理單元 〇 我的使用者帳戶 〇 服務帳戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)		
這個嵌入式管理單元 ○ 我的使用者帳戶 ○ 服務帳戶(S) ● 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)		
這個嵌入式管理單元 ② 我的使用者帳戶 ④ <u>服務帳</u> 戶(S) ④ 電腦帳戶(C)	元將自動管理下列帳戶的憑證: (M)	✓ 北 邑 珪 単 / L	▶



≧ 主控台1 - [主控台根目錄∖憑證 (本機電腦)\中繼憑證授權單位\憑證]	_ 🗆 X
🚟 檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)	_ & ×
□ 主控台根目錄 發給 ▲ 簽發者 到期E	動作
▲ 豪 憑證 (本機電腦) Government Root Certification 2032/	慿證 ▲
▶ ■ 週へ III Government Root Certificatio Government Root Certification 2032/ ▶	其他動作 ▶
▶  □企業信任	
▲ 🤇 中握憑證授權単位 Public Certification Authority PKI Root Certification Authority 2027/	
Root Agency Root Agency 2040/	
▶ 〇 沒有。 Hotan 2013/ Government Root Certification 2033/	
▶ 2月 (俄倪(V) ▶ 音第三: 公演理問盼新词案(M) Government Root Certification 2023/	
▶   留巷: [ 匯出清單(1)	
▶ <mark>□</mark> 信任( ▶ □ 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1 / 1	
	<u> </u>
<ul> <li>         参 液阻進八桿盤</li></ul>	₽ 。 客連線的資
<u>ए</u> -न	₱(N) 取消

★ 通 馮紹確 λ 結整
要匯入的檔案 指定您想要匯入的檔案。
檔案名稱(F): C:\PublicCA2_64.cer 瀏覽(R)
注意: 您可以將數個憑證用以下的格式存放在同一個檔案中: 個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B) Microsoft 序列憑證存放區 (.SST)
深入了解 <u>憑證檔案格式</u>
下一步(N) 取消
★ 參 憑證匯入精靈
★ 憑證 医入精 靈          透證存放區         憑證存放區是用來存放憑證的系統區域。
★ 憑證 医入精靈          憑證存放區         憑證存放區是用來存放憑證的系統區域。         Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。
<ul> <li>※ 憑證匯入精靈</li> <li>遊證存放區 憑證存放區是用來存放憑證的系統區域。</li> <li>Windows 可自動選取憑證存放區,您也可以為憑證指定存放位置。</li> <li>● 自動根據憑證類型來選取憑證存放區(U)</li> <li>● 能所有憑證放入以下的存放區(P)</li> <li>※部方不知:</li> </ul>
★ 感蟄医人精整          ●       ●
<ul> <li>※ ● 意識 ● 意</li></ul>
★ 多数でのである。 ◆ 多数でのである。 ◆ 多数でのである。 ◆ クリング ののである。 ◆ ののである。 ● 日本のなどのである。 ● 日本のなどのであ

	x
🖉 👼 准路陲 λ 糖露	
完成憑證匯入精靈	
按一下 [完成],即可匯入憑證。	
你已指定下列設定。	
() () () () () () () () () () () () () (	
P3日 認証 楊安文涵 C\DublicCA2.64.cer	
$\frown$	
完成(F)	取消
- 憑證匯入精靈	
(二) 匯入執行成功。	
確定	

-	主控台1 - [主控台根目錄\憑證 (2	≤機電腦)\中繼憑證授權單位\憑	[證]	_ <b>D</b> X
🚟 檔案(F) 動作(A) 檢社	見(V) 我的最愛(O) 視窗(W) 說明(H	)		_ & ×
i 🗢 🔿 🖄 🖬 🐇 🖻	🗙 🗒 🗟 🚺 🖬			
<ul> <li>              i</li></ul>		登録者 Government Root Certification Government Root Certification Microsoft Root Authority ePKI Root Certification Authority ePKI Root Certification Authority PKI Root Certification Authority Root Agency Class 3 Public Primary Certificati Government Root Certification Government Root Certification	到其 203 203 200 202 202 202 202 202 204 201 203 202	動作 憑證 ▲ 其他動作 ▶ Public Certificat ▲ 其他動作 ▶
<ul> <li>▶ 😁 智慧卡信任根目:</li> <li>▶ 😁 信任的裝置</li> <li>▶ 😁 Web Hosting</li> <li></li> <li><th>Ⅲ       含10個憑證・</th><th></th><th>&gt;</th><th></th></li></ul>	Ⅲ       含10個憑證・		>	

十、於站台上換上 SHA256 憑證。

點選需要更換 SHA256 憑證的站台→「繫結」



	站台繫結	? X
類型 主機名稱  連 http	接埠 IP 位址	新增(A) 編輯(E) 移除(R) 瀏覽(B)
		關閉(C)

	編輯站	台繋結 ? ×	<u>د</u>
類型(T): https 主機名稱(H):	IP 位址(0): ✓ 全部未指派	連接埠(O): ✓ 443	
□ 需要伺服器名稱 SSL 馮證(F): www.test.com.tw-S	指示(N) SHA256	✓ 選取(L) 檢視(V) 確定 取消	]

■ 憑證	×
一般 詳細資料 憑證路徑	
● 憑證資訊	
<ul> <li>● 所有應用程式原則</li> </ul>	
發給: www.test.com.tw	
簽發者: Public Certification Author	rity - G2
有效期自 2015/2/16 到 2020/2/16	
♀ 建個憑證有一個對應的私密金鑰。	
	簽發者聲明(S)
深入了解 <u>憑證</u>	
編輯站台繫;	結 ?
類型(T): IP 位址(I):	連接埠(O): ▼ 443
主機名稱(H):	
└」 需要伺服器名稱指示(N)	
SSL 憑證(F):	
www.test.com.tw-SHA256	❤ 選取(L) 檢視(∨)
	確定 助迷
	H≢A⊑ RX//8

			站台	鬤結		? X
類型	主機名稱	連接埠	IP位址	繫結資訊		新増(A)
http		80	*			
https		443	÷			編輯(E)
						移除(R)
						瀏覽(B)
					(	關閉(C)
						$\smile$

十一、 以瀏覽器檢視網頁是否正常運作。