SSL 伺服器數位憑證 IIS 6.0

伺服器操作手册



台灣網路認證股份有限公司 TAIWAN-CA. Inc. 台北市100 延平南路 85 號 10 樓 電話:02-2370-8886 傳真:02-2370-0728 www.twca.com.tw

機密等級:公開 版本:V3.0 文件編號:MNT-03-071 生效日期: 2005 年 11 月 14 日

目 錄

1.目的	1
2.参考資料	2
3.定義	3
4.作業程序	4
4.1 如何產生「憑證申請檔(CSR)」?	4
4.2 如何將製作好的憑證申請檔(CSR)上傳?	7
4.3 下載已核發憑證作業	8
4.4 如何安裝自我憑證?	12
4.5 如何安裝中繼憑證?	14
4.6 如何備份憑證(匯出)?	16
4.7 如何復原憑證(匯入)?	20
4.8 如何啟動 SSL 模式?	24
4.9 如何更新 SSL 憑證?	26
5.附件	27

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉 變成任何其他形式使用。

1.目的

- 1.1. 主要介紹 SSL 伺服器數位憑證 IIS 6.0 伺服器之憑證申請檔產製步驟及 憑證安裝說明。
- 1.2. 符合本公司資訊安全政策之規範。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。

2.參考資料

無。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。

3.定義

魚。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。

4.作業程序

4.1 如何產生「憑證申請檔(CSR)」?

※在產生的過程中,所有需要填入的資料,請務必以英文方式填寫!

4.1.1「開始」→「程式集」→「系統管理員」→「網際網路資訊服務(IIS)管 理員」畫面中在欲執行 SSL 模式的站臺上按右鍵→「內容」→「目錄安全 設定」→「伺服器憑證」,以啟始 Web 伺服器憑證精靈→「下一步」。



4.1.2 準備產生憑證請求檔,「建立新憑證」→「下一步」→「準備要求,但稍
 後傳送」→「下一步」。

■ 計算 211	IIS 懇證精畫 ×
伺服器 熟證 這些是指派憑證到網站的方法。	爰選或立即要求 您可以先準備稍後才傳送的要求,或您可以立即傳送它。
ま28日-4258-8日4-41-(2)とかたは ● 建立新馬證(○)。 > 3日40日 (月1)の品面(血)	您想要先準備指後傳送的憑證要求,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
 ○ 從金鑰管理員備份檔案匯入憑書(20)。 ○ 從 pfx 檔案匯入憑證(20)。 	
○ 從遠端伺服器網站複製或移動憑證到北網站(型)	
<上一步⊕ 下一步 ₪ > 取消	<上一步促【下一步⑪〉> 取消

4.1.3 輸入憑證資訊

4.1.3.1 名稱:出現在憑證管理清單中的名稱,填入較有意義之文字,<u>需</u> 以英文方式填寫!位元長度:若要申請 40 位元 SSL 憑證,請選擇 512; 若要申請 128 位元 SSL 憑證,則選擇 1024。

(及完全語名	
物的新憑證必須有名稱及特定的()	立元長度。
請輸入新憑證名稱。它應是個容易	易參考且記憶的名稱。
呂稱(<u>M</u>):	
營運網站	
	2215 ·
1024 • 512	

4.1.3.2 以下三個欄位將會出現在憑證內容之中,請慎填!各欄位說明如下:

公司:公司名稱,需以英文方式填寫!。(如:TWCA)

單位:使用該憑證之單位名稱,需以英文方式填寫!(如:IT)

公用名稱:網站名稱(如:www.taica.com.tw),即申請同意書上之 Common

拉桥 盡	IIS 透透精靈
司資訊 您的憑證中必須有您的公司的資訊,這些資訊用來區別您的及其他的公司。	您站台的公用名稿 您的 Web 站台的公用名稿是一個完全合格的網域名稱。
諸邊敗救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 若齋進一步資訊,諸與憑證授權的 Web 站台聯絡。	諸為您的站台輸入公用名稱。若伺服器在 Internet,諸用有效的 DNS 名稱。若 伺服器在 internet,建議您用電腦的 NetBIOS 名稱。 如果變更公用名稱,您將需要取得新的感識。
公司(1):	公用名稱(C)
line .	www.tsice.com.tv/
單位(1):	
T I	

Name 欄位內容!

4.1.3.3 以下三個欄位亦會出現在憑證內容之中,請慎填!各欄位說明如下:

國家/區域:兩碼之國碼,<u>需以英文方式填寫</u>!(如:臺灣為TW)

州/省:國家全名,<u>需以英文方式填寫</u>!(如: Taiwan)

城市/位置:城市全名,<u>需以英文方式填寫</u>!(如: Taipei)

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。

ad 17 22		
1理資訊 此憑證受權要求下列地理(的資訊。	
國家(地區)(C):		
州/省(S):		
Taiwan		-
城市/位置(上):		
Taipei		-
必須輸入 [州/省] 和 [城市	尬置],正式名稱不可含縮寫。	

4.1.3.4 指定執行出之憑證申請檔(CSR)檔案存放路徑。(如:D:\SSL\certreq.txt)

IIS 憑證楮靈
慧證要求檔案名稱 將以您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(1):
D:\SSL\certreq.txt 瀏覽(R)
<上一步(B) 下一步(D) 取消

4.1.3.5 伺服器憑證精靈會將前幾個步驟所設定的憑證申請檔內容,供使用者再

次確認設定內容。請先確認畫面所列出之內容是否皆為英文方式書寫且



正確無誤→「下一步」→「完成」。

4.1.3.6 完成之憑證請求檔內容如下。

----BEGIN NEW CERTIFICATE REQUEST---MIIDAjCCAmsCAQAwbTEWMBQGA1UEAxMNMTkyLjE20C4wLjEwMjEUMBIGA1UECxML SURMZW9uIFR1c3QxDjAMBgNUBAoTBURhaWNhMQ8wDQYDVQQHEwZUYW1wZWkxDzAN BgNVBAgTB1RhaXdhbjELMAkGA1UEBhMCVFcwgZ8wDQYJKoZIhvcNAQEBBQADgYØA MĪGJAoGBAKNXzRByH5zCa8vN1/bd47VaxAD68DVV8CDMTYh7SBXZBueØCs3Hv+Fo rf1HMQEd2cjm/bKvRjKk/LrGXAYHDrLBXJtLrgDi7rjXn+C6Z31dPEbUWvWnLw3t KeXSH8wa6aaIC2ApEUA+Z07Q0BIZGeeilie14DUBb4JUXe6wZIYrAgMBAAGgggFT MBoGCisGAQQBgjcNagMxDBYKNS4wLjIx0TUuMjA1BgorBgEEAYI3AgEOMScwJTAO BgNUHQ8BAF8EBANCBPAwEwYDUR0IBAwwCgYIKwYBBQUHAwEwgF0GCisGAQQBgjcN AgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgA YQBuAG4AZQBsACAAQwByAHkAcABØAG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYA aQBKAGUAcgOBiQAgdwtlPabCtPlfjfzHtSbBt/b6Jwj0AXTsDaesxyUjwlNxcENE oBaREDcuhxJ+/SNAjK1Pd6vR4dU0LXdmF0pUh0Lp16yHMrZgBUV4YmzU+g6dXuNU o3NjeIpScstRhbLOvOnHWbdhj+stOCO+Pzr5Ftln/Z3s1KzKxEjNjz+AdQAAAAAA AAAAMAOGCSqGSIb3DQEBBQUAA4GBAFikYzMbP0b/vz+NTOE118+GixDF1qQx5VF6 t1wBDLL58I3U+knb6bEfa4NVQSvW6QfkEDC62mY71e5hhVhjjzAUWtz2dDdaWdWK OK8hexLEuTxQJObqrDDPa1xcyXJT41un1/sZ+TRfjN01EBPJ104bJ11C/gzSUMzJ iAWYz1Ka -- END NEW CERTIFICATE REQUEST-----

4.2 如何將製作好的憑證申請檔(CSR)上傳?

4.2.1 連接至本公司首頁 <u>http://www.twca.com.tw</u>。

- 4.2.2 點選「SSL 伺服器憑證」→「憑證申請」→「憑證申請」。 - **-** × A Teica 臺灣網路認識 - Microsoft Internet Explorer 檔案(F) 編輯(E) 核規(Y) 我的最愛(A) 工具(T) 說明(E) Q 图 资 搜尋 我的最爱 媒體 記錄 到印 11 網址① 🕘 http://www.taica.com.tw/ 連結 💩 Hotmail 的発費電子郵件 💩 Windows Media 😸 Windows 😸 自訂連編 TAICA 台灣認證 安全認識標度 SSL伺服器憑證 金融EDI 檔案下載 **F**全等級測試 憑證申請 線上研討會 網路銀行 (網際網路) 網路信用卡 HOME 網路下單 客戸服務 聯外通道 ENGLISH 新手上路 影音介紹 臺灣網路認證股份有限公司 TAIWAN-CA. COM. /apply.htm
- 4.2.3 選擇「步驟四 傳送憑證請求檔與線上填寫註冊資料



本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

4.2.4 用複製貼上的方式,將製作好之憑證申請檔(CSR)內容貼到申請欄位中→

選擇「繼續」。					
🖉 Taica 臺灣網路認證 - Microsoft Internet Explorer					
檔案(E) 編輯(E) 檢視(V) 我的最愛(A) 工具(I) 說明	1 H)				
				- 📃 🖸	à
エー頁 停止 単利型社 首頁 15 網址(D) 創 http://www.taica.com.tw/	144 9730 949 <u>98</u> 98 82	3L/AX 3591T	7 (L) 19644	2324 IC	▼ 208至
連結 《Hotmail 的免費電子郵件 《Windows Media 《W.	indows 🙆自訂連結				
	以下寫CSR檔案的同	内容範例:			
	BEGIN NEW CE	RTIFICATE REOL	IEST		
台灣認證	MIIBJDCBzwIBADB	qMQswCQYDVQ	QGEwJUVzEPM.	A0GA1U	
	ECBMGGZRDGSQD	SFesGwZUDWgrz	grhgzhrreXQU4x	DjAMB	
STEREOF P	gNVBAoTBVRBSUN E AwMThCEiMTAWL	VBMQswCQYDV(QULEWIJVDEcM	BoGAIU	
	gilfHCa2diLHOa69S	MUmLXNdnaVO	nl4pkgPolaNvKv	0TKR7tac	
	Lnfjm Wxu6pAgMBA	AGiG9w0BAQQI	AANBAIlGzBUI	KGyYGY	
	5vczs+LzMPlclybw	TE4784HIZUbibZl	hXNg6L90H09CI	HpDXD	
	duwd01q42V5xCmas	SPCIMEINITX4BY	T5qZY=		
改版公告	BND NEW CERT				
線上研討會	御行台 · ある口 (***) - ***			A.	
	周年前、中国人でした。員	r I			
	請將CSR檔案中的]容複製到			
HOME	右邊的空欄中,注	意複製的			
客戸服務	111国際包括 " PECIN NEW				
Bit of Line int	CERTIFICATE REC	JEST"			
	到				
	"END NEW CEI	TIFICATE			
	REQUEST"				
	100百日父子。			-	
		4			
	請按一下"繼續"按	以便送出	181405 05-2	K (
	CSR,並繼續註冊	序	282394 ¥ .4	*	_
					<u> </u>
管 完成					● 網際網路
:#A-開始 🖄 📶 🛋 🔼 🔂 心体性原。 🖉 30 電調	○ 田小宮戶幅 ▲1	aica 杏 👉 Thomas	w Wintermet In	105 hmp -	1844 🗸 🖬 🚾 🔍 🦣 🥢 🚟 🛛 a M 11-25

4.2.5 再次檢視上傳之憑證申請檔案內容。

🛃 Taica 臺灣網路認證 -	Microsoft Internet Ex	olowe													_ # X
檔案(E) 續輯(E) 核	(現代) 我的最爱(D II (脱机田												10
± – π • , , , , , , , , , , , , , , , , , , ,	· () ·	理道見	0	我的最爱	() ##	C) #151	5. ##	्र मुख्य	医	•		86 ICQ			
病社(1) 📄 http://www.	taica.com.tw/									_				×	<i>€</i> 8至
連結 🐑 Hotmail 的発動	2電子郵件 🍓 Wi	adows Media	👌 Wiadow	1 🐑 eit	連結										
TAICA															-
台灣認證			線上	:填寫	窮註冊	ŀ資	料								
安全認證標章															
	保密說明: 您在此頁!	面所輸入的	所有資料	以,值没;	至本公司[诗均受	SSL安全	機制保計	ε,						
	並無外洩	と虞,請放	¢.	1 147403											
			木	è杏CS	R內容										
改版公告				<u>, 11.00</u>											
10 LUT210		解	1 說				您的	JCSR	內容						-
	一般名稱:														
HOME	此名稱所代表的 保護。	的網站之安全	全性・將	由此SSL作	可服器透验)所 w	rww.taica.c	om.tw							
客戸服務	紙鐵:														
聯外通道	即 貴公司的	白稿。				Т	WCA								
	組織單位:														
	這是一個可以用	非來區分組 結	机合成产5 合约	欄位。		C	s								
	城市/位置:														
	即 貴公司進行	f 開業行為A	9所在。	[例:Tai	pei]	ta	arpei								
						-				-					
	州/省:													-	*
● 元店 ■●問題 100 114 =	100 100 100 400	w (23.20 a	- 100	DAGST.	Tairs #	é Th		Married 1	9/105 hor	. [Clearter		i i i i i i i i i i i i i i i i i i i	896 2071 -	M 11/26

- 4.2.6使用視窗右方式下拉移動方式,將申請之伺服器與聯絡資料填入適當欄 位(聯絡資料欄位請務必與申請同意書所填內容相符)。
- 4.3 下載已核發憑證作業
 - 4.3.1 若上傳之 CSR 及相關聯絡資料經過審驗通過,將會由系統自動發送伺服 器憑證下載通知給相關聯絡人。其中技術聯絡人所收到的通知含有憑證檔 案及安全標章之附檔及安裝說明:
 - ※ ServerCert.crt →伺服器憑證檔。
 - ※ TaiCASecureCA_Prod.crt (或 EntrustCA_Prod.crt)→中繼憑證檔。
 - ※ mark1.gif、mark2.gif、mark3.gif →認證標章圖形檔。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。

※ 請確實將伺服器憑證檔及中繼憑證檔安裝於伺服器中。

- 4.3.2 若因為貴公司之 mail server 設定,導致無法順利取得附件之憑證檔案, 請依照下列步驟,下載相關檔案。
- 4.3.3 下載伺服器憑證:
 - 4.3.3.1 先連至本公司首頁 (<u>http://www.twca.com.tw</u>)。
 - 4.3.3.2 點選 SSL 伺服器憑證。
 - 4.3.3.3 點選 憑證申請。



4.3.3.4 點選 憑證搜尋。



4.3.3.5 輸入申請之 DNS 位址填寫當初所申請的憑證之網站名稱,如 www.abc.com.tw (注意,大小寫需一致),輸入完成後,按下搜尋鍵

●憑證搜尋	3. 2. 8. 20	SSL憑證申請
請輸 以打	入網站名稱(Comr 製尋TaiCA SSL伺用	non Name) 服器憑證
~~~	24 mer 100 m	1/2 U 70 122
網站名稱:		
	搜尋重設	

4.3.3.6 點選 下載憑證。

aica.com.tw 定1	28位元伺服器憑證
解說	内容
一般名稱	www.taica.com.tw
憑證狀態	有效
有效期限	2002-10-04 15:32:13.0 2003-10-28 08:00:00.0
憑證等級	TaiCA Secure Server
憑證內容	Country = TW State = TAIWAN Locality = TAIPEI Organization = TaiCA Organizational Unit = TaiCA Common Name = www.taica.com.tw
憑證序號	1033716735
憑證擁有者	台灣網路認證

4.3.4 下載中繼憑證。

下載網址: https://ssl.taica.com.tw/cacert/taicasecureca_prod.crt

- 4.3.5 安裝安全認證標章,認證標章(markl.gif, mark2.gif, mark3.gif):(請 依貴公司需求選擇適合之圖檔)。
  - 4.3.5.1 先連至本公司首頁(<u>http://www.twca.com.tw</u>)。
  - 4.3.5.2 點選 產品服務。
  - 4.3.5.3 點選 SSL 伺服器憑證。
  - 4.3.5.4 點選 產品介紹。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。



4.3.5.6 請依貴公司需求選擇適合之圖檔規格。



4.3.5	.7 按滑鼠右鉤	建→選 另存	圖片。	)		
档案图 績	瞬间 植桃豆 林桃田 林的极爱山	) 工具① 脱钙图				
G 1-A	· 🕑 · 🖹 🗟 🏠	🔎 線像 🤺 彩的晶素	😵 1482 🔞	ð 🔊 🎍 🖃 📮	ety	
總生(1) 👩	http://www.tesa.com.tw/IM&0E43	tig elhtém_J3				👱 🛃 移至 🗵
Google -	<u> </u>	🕅 Search Heb 🔹 🧔 🗗	10 blocket	AntoFil 💽 Options 🥒		
msn ^M •	×	Search · Z Highlight	V Options	Pop-up: Blocked (0) *	🖂 Hotnail 🛛 🏭 Me	mager [ 2 My M2N
	開帯場応(2) 在紙供置限帯連約(1) 另平目標(2) 男子目標(2) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子医外体支置外(1) 男子母の(1) 男子母の(1) 男子母の(1) 男子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1) 子母の(1)					

4.3.5.8請在 貴公司的網頁上加上本公司認證標章及以下超連結語法,以便 讓使用者查詢 貴公司憑證狀態

<A target=new href="https://ssl.taica.com.tw/servlet/ShowServerCertInfo?DNS=申請之DNS位

址 ">

<img src="/mark.gif" tppabs="/mark.gif" border="0">

</A>

其中 src="/mark.gif"這一段,請依 貴公司的狀況調整路徑名

- 4.4 如何安裝自我憑證?
  - 4.4.1 請先將自 CA 取得的自我憑證檔(ServerCert.crt)儲存於硬碟中。
  - 4.4.2 使用憑證精靈,將伺服器憑證匯入「網際網路資訊服務(IIS)管理員」畫面中在欲執行 SSL 模式的站臺上按右鍵→「內容」→「目錄安全設定」→「伺服器憑證」,以啟始網頁伺服器憑證精靈→「下一步」。

twca (已停止) Å	內容			3	? ×	3
網站	效能	ISAPI 篩選器	主目錄	文件		歌迎使用網頁伺服器應設精靈。
目錄安 驗證及存取 ● P 位址及網	全設定 │ 控制 啓用匿名存取, 證方法。 域名稱限制 使用 IP 位址或 或拒絕到這個習	HTTP 標頭 並編輯這個資源的驗 網際網路網域名稱來授 環的存取。	) 〔 <u></u> 予	自訂錯誤 (在)		<b>歡迎使用網頁伺服器憑證精</b> 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簡的伺服器憑證。 您的網頁伺服器狀態: 您有類還的同能器要求。"感聲描靈將協助您處理
安全通訊	當存取這個資源 用用戶端憑證。	原時使用安全通訊並啓	編	╋① 應證③ 證④		Instatus (Telus Julio Symplemine) Extension 話技 [下一步] 來繼續。
		定 取消	套用( <u>A</u> )			<上─步四】 <b>下──步(0)</b> > 取消

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

4.4.3「處理擱置要求及安裝憑證」→「下一步」→指定到取得的Server_Cert.crt 檔案→「下一步」。

IIS 憑證精靈	IIS 憑證精靈	×
<b>蜀道的燕證要求</b> 擱置的憑證要求是指憑證授權未回應的要求。	<b>處理調整要求</b> 藉由顯取含憑證授權回應的檔案來處理感證機證要求。	
有關語的振識要求。想想要名應做? (7) 這理關證要求及妥疑感證(1)	請輸入含透過授權回應檔案的路徑及檔名。 路徑及檔案名稱(2):	
○ 風除腸蓋要求①・	C.\Server_Cert.crt #38(@)	ן
<上-步@	-#0.)	取清

4.4.4 請先設定 SSL 連接埠為 443 → 「下一步」。

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

4.4.5 **請先確認畫面所列出之內容是否為提出申請憑證之內容**→「下一步」→ 「完成」。

IIS 憲證精畫 X	董務儀器 211
<b>惣已経選擇從日塵槍案安裝懸證。</b> 憑證摘要	正在完成網頁伺服器憑證精 靈
王軍伝統工和機器・試合「ビーゼ」 「「「」」」 「「」」 「「」」 「「」」 「」」 「」」	您已經成功完成網頁伺服器憑證褚靈。 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 次使用稽靈。 諸按 [完成] 來關閉此稽靈。
<上一步®】 (T-步圆) (T-丁) (T-丁) (T-丁) (T-丁) (T-丁) (T-T) (	「たまた」、元成一 取消

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

### 4.5 如何安裝中繼憑證?

4.5.1 將臺灣網路認證公司的憑證(TaiCASecureCA_Prod.crt)儲存於硬碟中,使 用檔案總管尋找到儲存的檔案,選擇此憑證檔案按滑鼠右鍵,選擇「安 裝憑證」。



4.5.2 將出現使用憑證匯入精靈的畫面,請選擇「下一步」。

憑證匯入精靈		×
	歡迎使用憑證匯入精霊	
	這個精靈協助您將憑證、憑證信任清單及憑證廢止清 單從磁碟複製到憑證存放區。	
	憑證是經由憑證授權單位簽發,能確認您的身分並包 含用於保護資料或建立安全的網路連線資訊。憑證存 放區是用來存放憑證的系統區域。	
	請按 [下一步] 繼續。	
	<上一步(B) [下一步(B)] 取消	

4.5.3「將所有憑證放入以下的存放區」→「瀏覽」。



### 4.5.4 勾選「顯示實體存放區」。

選擇憑證存放區	<u>? ×</u>
選取您要使用憑證存放區。	
■ 田	
□ □ □ 中繼憑證授權   □ □ □ □ □ □ □	
▶ 顯示實體存放區(3)	
確定	取消

4.5.5 點選並開啟「中繼憑證授權」→「本機電腦」→「確定」。

選擇憑證存放區	?×
選取您要使用憑證存放區。	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
	<b>_</b>
▶ 顧示實體存放區(3)	
( 確定 取)	肖

4.5.6 點選「下一步」。



4.5.7 點選「完成」。

憑證匯入精靈	x
	完成憑證匯入精霊
	您已經成功地完成憑證匯入精靈。
	您已指定以下新的設定: [/本田老際兩份連款支持原一中機連款採練支援素的]
	使用有通知的認識行成 一千種認識的 化中域电脑 质容
	$\frown$
	<上一步(B) 瓦爾 取消

4.5.8 完成畫面。

憑證匯入精	靈
<b>i</b>	匯入執行成功。
	確定

4.6 如何備份憑證(匯出)?

4.6.1 由「開始」→「執行」→開啟 MMC ,執行「主控台」。

執行		?
	請輸入程式、資料夾、交 Windows會自動開啓。	[件或 Internet 資源的名稱,
開啓(0):	mme	
	確定	取消 瀏覽(B)

4.6.2 進入主控台後,選擇「新增/移除嵌入式管理單元」。



本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。



4.6.4「電腦帳戶」→「下一步」→「本機電腦(執行這個主控台的電腦)」→「完 成」。



新增纬3除嵌入式管理單元 獨立 擴充 諸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 「」 一 主控台根目錄 「」 一 透證 (本機電腦)	?★ 新增獨立嵌入式管理單元 可用的獨立缺入式管理單元	? ×
	<ul> <li>○ 沖市街街並家へ為管理単元.</li> <li>● 連結到 Web 位址</li> <li>● 連結到 Web 位址</li> <li>● 詳組原則</li> <li>● 資料液</li> <li>● 電腦管理</li> <li>● 電腦管理</li> <li>● 磁路管理</li> <li>● 磁路管理</li> <li>● 磁路管理</li> <li>● 磁路管理</li> <li>● 磁路管理</li> <li>● 磁路管理</li> </ul>	
	▲ 以條管理 ● 憑證 描述 - 透證嵌入式管理單元讓您瀏!	VERITAS Software Cor Microsoft Corporation 更電腦或服務的憑證存放內容。 〔新檀仏〕 開閉

4.6.6 主控台中多出憑證管理項目,可在欲匯出的憑證上按右鍵執行匯出動作。

<mark>論</mark> 主控台1		
主控台(C) 視窗(₩) 説	91 🗄 🗋 🖬 🖬	
🚡 主控台根目錄 憑證 (本機)	電腦)個人)憑證	<u>-0×</u>
」執行(▲) 檢視(Ⅵ) 我的	最愛E	
⇐ ⇒   🗈 💽   🐰 🖣	a 🗙 🗗 🗟 😰	
樹狀目錄   我的最愛	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	發行者
1 主控台根目錄	192.168.0.102	Test SSL CA2
白 🔊 憑證 (本機電腦)	192.168.0.102	Test SSL CA2
白。同個人	192.168.0.102	Test SSL CA2
	192.168.0.42	Test SSL CA
⊡	192.168.0.49	For VeriSign aut
⊡ 📄 企業信任	🖭 Taica-Test	Taica-Test
🗉 🧰 中繼憑證授權	taica-w2	Test SSL CA
由 🧰 其他人	www.tai	Test SSL CA2
	所有工作(K)	開啓
E-C	剪下(I)	以新的金鑰要求憑證
	複製(C)	要求憑證並使用相同識別碼
		以新的金鑰更新憑證
進出憑證		以相同金鑰更新憑證

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

4.6.7 將出現使用憑證匯出精靈的畫面,請選擇「下一步」→「是的,匯出私 密金鑰(Y)」→「下一步」。

憑證匯出精靈		▲ 憑證確出精靈	X
	歡迎使用憑證匯出精霊	<b>匯出私密金論</b> 您可以選擇將私密金鑰與憑證一起匯出。	
	這個精靈將會從憑證存放區將憑證憑證信任清單及 憑證廢止清單複製到您的磁碟中。	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。	
I Press	憑證是經由憑證授權單位簽發,能確認您的身分並包 含用於保護資料或建立安全的網路連線資訊。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>下一步(1)</b> ) 取消		

4.6.8「個人資訊交換-PKCS#12(*. PFX)」→「啟用加強保護(需要 IE5.0 或 NT4.0 SP4 以上的版本)」→「下一步」。

諸選明	g您想要使用的格式:
C	DER encoded binary X.509 (.CER)
C	Base-64 encoded X.509 (.CER)( <u>S</u> )
C	密碼編譯訊息語法標準 - PKCS #7 憑證 (P7B)(C)
	如果可能的話,在憑證路徑中包含所有憑證①
۲	個人資訊交換 - PKCS #12 (* PFX)(2)
	如果可能的話,在憑證路徑中包含所有憑證(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(K)

4.6.9 設定匯出資料的保護密碼→「下一步」。

■人业確認密碼。 密碼(P):		
*****		
確認密碼(C):	_	
	_	

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。

4.6.10「瀏覽」→指定一個匯出檔案存放的路徑與檔名(副檔名固定為.PFX)→ 「下一步」→「完成」。



4.6.11 以上匯出動作為備份自我憑證檔與私密金鑰,請牢記匯出時設定的密碼。
4.6.12 請將下載之中繼憑證檔(TaiCASecureCA_Prod. crt),一併另行保存與備份。

4.7 如何復原憑證(匯入)?

- 4.7.1 若要執行復原(匯入)工作,亦是進入主控台,從所有工作中執行匯入功 能;如為新的伺服器設備請先執行說明 6.1 至 6.6 新增一個憑證管理 單元。
- 4.7.2 按滑鼠右鍵→「所有工作」→「匯入」→啟動憑證匯入精靈→「下一步」。

🚡 主控台1 - [主控台根目錄	>)憑證 (本機電腦)/個人/憑證]		靈	×
│ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	説明(H) 🗍 🗋 🚅		教训	使用憑證匯入精霊
」執行(A) 檢視(Ⅴ) 我的	的最愛 🕑 🔰 🗢 🔿 📘 💽 🔳			
樹狀目錄   我的最愛	發給△	發行者	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	囊位肋物熔漏器、漏器信任清留方漏器腐止清
● 主控台根目錄	= 192.168.0.102 = 192.168.0.102	Test SSL CA2 Test SSL CA2	單從磁	碟複製到憑證存放區。
□…●● 個人	192.168.0.102	Test SSL CA2	· · · · · · · · · · · · · · · · · · ·	經由憑證授權單位簽發,能確認您的身分並包
	192.168.0.42 (作(K) ▶ 要求新憑證	Test SSL CA For VeriSign auth	含用於 防腐見	保護資料或建立安全的網路運線資訊。憑證存 用來存放憑證的系統區域。
	西	Taica-Test		
		Test SSL CA	諸按「	下一步]繼續。
田 R 新工作	告檢視( <u>T</u> )			•
正 · · · · · · · · · · · · · · · · · · ·	理E			
	[]] 單( <u>L</u> )			
	D			
•		F		<上一步(B) (下一步(B)) 取消
將新憑證加入存放				

4.7.3「瀏覽	→指定至	1 當初匯出	備份的檔案	(*, PFX)	) →「下-	-步」。
----------	------	--------	-------	----------	--------	------

檔案名稱(E):			
C:\BACKUP.PFX			(瀏覽( <u>R</u> )
建计查。你可以收	<b>曲</b> 個馮寶田以下的約日	*方防大同二個構	安山
af在息, 必可以府			1 <del>A</del> T
個人資訊父換 -	PKCS #12 (.pfx,.p12)		
密碼編譯訊息訊	晉法標準 - PKCS #7 認調	澄 (.p7b)	
Microsoft 序列調	5證存放 (.sst)		

4.7.4 輸入當初匯出備份時所設定的密碼→勾選「將私密金鑰標示成可匯出」 →「下一步」。

輸入私密金鑰的密碼。 密碼(P):
*****
啓用加強私密金鑰保護,如果您啓用這個選項,每次 私密金鑰被應用程式便用,系統便會提示您(2)
▶ 粉松老玉拥信小水可隆古(M)

4.7.5 確定選擇「將所有憑證放入以下的存放區」→存放區顯示位個人→「下 一步」→「完成」。



4.7.6 從 IIS 站台上按滑鼠右鍵→「內容」。

😋 Internet Information Ser	vices			_ 🗆 🗡
執行(▲) 檢視(型)	← ⇒ 1	😭 🗿 🖏	😫   💂   ▶ ■ ॥	
樹狀目錄	名稱		路徑	
Normation Se → ● * sumny ● ● 預設的 FTP 站 ● ● 預設的 Web P ● ● 預設 SM TP f	Type       Type </th <th>ipts Admin Samples SADC Ielp ppub ters sal.asa .gif art.asp Istart.asp Istart.asp c.gif error.gif t.gif ning.gif .gif 2000.gif</th> <th>c timetpub/scripts C:\WINDOWS\system32\inetsrv\iisadmin c:\inetpub\iissamples c:\program files\common files\system\unsadc c:\windows\help\iishelp C:\Inetpub\webpub C:\WINDOWS\web\printers</th> <th></th>	ipts Admin Samples SADC Ielp ppub ters sal.asa .gif art.asp Istart.asp Istart.asp c.gif error.gif t.gif ning.gif .gif 2000.gif	c timetpub/scripts C:\WINDOWS\system32\inetsrv\iisadmin c:\inetpub\iissamples c:\program files\common files\system\unsadc c:\windows\help\iishelp C:\Inetpub\webpub C:\WINDOWS\web\printers	
	說明( <u>H</u> )			Þ
開啓目前選擇的內容頁。				

4.7.7「目錄安全設定」→「伺服器憑證」。

設的 Web 站台		<u>?</u>
目錄安全診	「 X能 」 ISAN 前番話 」 定   HTTP 標題   自訂錯誤	○.FF │ 伺服器擴充程式
- 匿名存取及	· 驗證控制	
<b>\$</b>	啓用匿名存取,並編輯這個資源的驗證 方法。	[編輯正]]
□ □ □ □ □ □ □ □ □ □ □ □	到城名稱限制	
8	授與或拒絕以 IP 位址及 Internet 網域名稱 來存取這個資源。	
		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。	伺服器憑證③…
		檢視憑證(型)
		編輯( <u>D</u> )
	確定   取消	套用(A) <b>說明</b>

4.7.8 啟動網頁伺服器憑證精靈→「下一步」。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

20 - 1 - 2	· · · · ·	
歡迎使用網頁伺服器憑證精調	Ē•	×
	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: 您的網頁伺服器沒有安裝應證且您沒有任何擱 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) <b>下一步(B)</b> >	取消

4.7.9「指派已有的憑證」→「下一步」。

1	· · · · · · ·
	IIS 憲證精靈 🛛 🔀 🔀
	伺服器憑證
	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:
ł	◎ 建立新憑證 ②。
	○ 指派已有的應證(Δ)。
	○ 從金鑰管理員備份檔案匯入憑證(Q)。
	○ 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)
l	<上一步(B) 下一步(M) > 取消
1	

4.7.10 選擇匯入的憑證項目→「下一步」。

HS 憑證精靈				×
<b>可用的惷證</b> 下列 <b></b> 溝單包?	含可用爲您的 Web(	司服器的憑證。		
諸選取憑證:				
發給	發照者	到期日	使用目的	易記名稱
sunny	TaiCA Secure C	2004/2/2		sunny
•				
•				
		ィトーザ(B)		取消 1
		<u></u> @		

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

4.7.11 檢視已選取安裝憑證資訊→「下一步」。

	· · · · · <b>_ · · · _ ·</b>		
IS 憑證精靈			×
認證摘要 您已經選擇安裝已有的憑證			
下列憑證可用來安裝在您的	Web 伺服器。若要安裝此憑證	,請按[下一步]。	
憑證詳細資訊: 發設用者 易見名稱 國家(地區) 州城市 公單位	sunny TaiCA Secure CA - Evaluation Or 2004/2/2 sunny TW taiwan taipei taica IT	цу	
	<上一步(B)	下一步00万	取消

4.7.12「完成」。



4.7.13 執行完以上步驟後,請參照第4節說明安裝中繼憑證檔 (TaiCASecureCA_Prod. crt)。

4.8 如何啟動 SSL 模式?

4.8.1 開始→程式集→Microsoft Internet 伺服器→Internet 服務管理員畫面
 中在欲執行 SSL 模式的站臺上按右鍵→內容→目錄安全設定→選擇「安全
 通訊」中的「編輯」。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

預設的 Web 站台	ì (己停止) 內	容			<u>? ×</u>
Web站台 目錄安全討	操作員	│ 效能 HTTP 標題	ISAPI 篩選器 自訂錯誤	器 │ 主目錄 └ │ 伺服器	│ 文件 │ 掛 流程式 │
- 匿名存取及 - IP 位址及新	、驗證控制 一 啓用馬名 方法。 樹城名稱限制 授與取這個 來存取這個	取,並編輯 以IP位址) 済源。	說言個資源的驗證 Definitement網域名:		E)
- 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。			何服器憑 校視憑 編輯(	≝© ≧© ⊵	
		確定	取消	套用(4)	說明

4.8.2 在安全通訊視窗中,將「必須使用安全通道(SSL)」的選項選取,將網站 重新啟動後,使用者存取此網站或網站下目錄的檔案時,就必須使用 SSL 模式通訊。若要強迫用戶連上網站皆必須使用 128 位元之 SSL 模式的話, 則將「需要 128 位元加密」選取即可。

用尸您證 ● 略過用戶端憑證	≹(O)	
○ 接受用戶端憑證	 8( <u>A</u> )	
○ 需要用戶端憑證	۳. س	
用戶端憑證可以對; 固功能可以用來控;	應到 Windows 的使用者帳戶。這 編輯(I 則用戶端憑證對資源的存取。	<u>1</u> )

- 4.9 如何更新 SSL 憑證?
  - 4.9.1 臺灣網路認證公司所發出的 SSL 伺服器憑證效期可分為一年期及二年 期,並會在憑證到期前二個月發出憑證更新通知信給 貴公司。在這二個 月內您隨時可以至臺灣網路認證公司下載申請表單,填寫完畢後寄回台灣 網路認證公司即可進行更新申請。
  - 4.9.2 在進行更新前請記得備份您原有的 SSL 伺服器憑證。
  - 4.9.3 由於 IIS 預設的「更新憑證」功能有誤,無法產生正確的憑證申請檔, 所以更新憑證的時候,請使用同一台伺服上的其他站臺(例如:系統管理 Web站台),以產生一個新的憑證請申請檔。並依照第4.1及4.2的描述, 申請並安裝 SSL 伺服器憑證及新的臺灣網路認證公司憑證。
  - 4.9.4 安裝完伺服器憑證及中繼憑證後,回到欲更新憑證的站台,按右鍵→內 容→目錄安全設定→伺服器憑證,啟始 Web 伺服器憑證精靈後,按下「取 代目前的憑證」。

IIS 憑證精靈	IIS 憑證精靈
<b>修改目前的恶混指派</b> 目前安裝在此 web 站台的憑證。	<b>可用的萘證</b> 下列清單包含可用爲您的 Web 伺服器的憑證。
您想要如何處理目前安裝的憑證?	諸選取憑證:
○ 更新目前的憑證(₩)。	發給         發照者         到期日         使用目的         易記名額           100 160 0 100         7.004 Summer 0 0000000         100 Text
○ 1070日前的憑證( <u>山</u> )。〕	
<上一步(B)   下一步(B) >	<上一步(B) 下一步(Q) > 取消

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

## 5.附件

魚。

本資料為台灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。