SSL 伺服器數位憑證 IIS 6.0 操作手冊



臺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:V5.1 文件編號:MNT-03-071 生效日期:110 年 8 月 10 日

目 錄

1.目的	1
2.範圍	2
3.参考資料	3
4.定義	4
5.作業程序	5
5.1 產生「憑證請求檔(CSR)」	5
5.2 將製作好的憑證請求檔(CSR)上傳	14
5.3 下載已核發憑證	20
5.4 安裝根憑證	23
5.5 安裝中繼憑證	27
5.6 安裝伺服器憑證	
5.7 檢視憑證是否安裝成功	34
5.8 匯出憑證(備份)	
5.9 匯入憑證(還原)	40
5.10 更新 SSL 憑證	48
5.11 新增憑證管理單元	55
6.常見問題	59
7.附件	60

本資料為臺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. 介紹 IIS 6.0 網頁伺服器之憑證請求檔產製步驟及 SSL 伺服器數位憑證 安裝說明。
- 1.2. 符合本公司資訊安全政策之規範。

本資料為臺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,

2.範圍

魚。

本資料為臺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,

3.参考資料

魚。

本資料為臺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.定義

無。

本資料為臺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.作業程序

5.1 產生「憑證請求檔(CSR)」

※如申請站台已安裝SSL憑證(非首次申請),請參照5.10章節進行憑證更新!
※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!
※憑證請求檔(CSR)產生後,不可點選刪除擱置要求,否則憑證將無法安裝!
5.1.1 執行網際網路資訊服務(IIS)管理員

點選桌面左下角開始→程式集(或所有程式)→系統管理員→執行網際 網路資訊服務(IIS)管理員。在欲安裝 SSL 憑證的站台上按滑鼠右鍵→內 容→目錄安全設定→點選伺服器憑證。(若找不到 IIS 管理員或 Internet Information Services 請先以 Windows2003 原版光碟安裝此功能後,再 執行此步驟)

20249346	иттр 横栖	l f		Ĩ	ACD MET	1
網站	效能	ISAPI 篩選器	主目錄	文件	目錄安全語	設定
驗證及?	存取控制 格用匿名存耳 證方法。	汉,並編輯這個資源	· 和功驗	扁鞋(<u>E)</u>]		
- TP (立址)	万細域名稲限制				1	
6	使用 IP 位址 或拒絕到這個	或網際網路網域名和 固資源的存取。	講來授予 4	扁輯(1)	1	
安全通	訊————————————————————————————————————					
Ŭ	當存取這個貨 9 用用戶端憑言	資源時使用安全通訊 費。		器憑證(≦) 見愿證(⊻) 編輯(D)		
<i>n</i>					4	
		確	定 取注	肖 (用(4) 🚺 👪	明

5.1.2 Web 伺服器憑證精	- <u></u>	
點選下一步。		
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	
	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(下一步(下一步(下一步(丁))	取消
5.1.3 準備產生憑證請求	檔(1)	
點選建立新憑證→黑	占選下一步。	
IIS 憲證精靈		×
伺服器憑證 這些是指派憑證到網站的:	方法。	
請選取您想要用於此網站的	的方法:	
(● 建立新憑證(C) ●)		
○ 指派已有的憑證(公。		
○ 從金鑰管理員備份檔案	₩ ●	
C 從 .pfx 檔案匯入憑證()	a)	
○ 從遠端伺服器網站複製	l或移動憑證到此網站(Y)	
	\sim	
	\sim	
		The sets
		取消

SSL 伺服器數位憑證 IIS 6.0 操作手册

5.1.4 準備產生憑證請求檔(2)

點選準備要求,但於稍後傳送→點選下一步。

IIS 憲證精畫	×
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 ○ 立即傳送要求到線上換覺授權(3) 	
<上一步(B) 下一步(B) 取消	肖

5.1.5 輸入憑證資訊(1)

5.1.5.1 名稱:出現在憑證管理清單中的名稱,可自由設定。

請填入較有意義之文字。

5.1.5.2 位元長度:請選擇 2048 位元長度。點選下一步。

IIS 憲證精靈	2
名 額及安全設定 您的新憑證必須有名稱及特定的	应元長度。
請輸入新憑證名稱。它應是個容 2 新 0.0	易參考且記憶的名稱。
伯爾(<u>他</u>). 復設的網站	
加密金鑰的位元長度決定了憑證 越好。不過長度越大也會導致速 位元長度(出): 2048	的加密金鑰強度。位元長度越大,安全性也就 度越慢。 <
□ 請選取此憑證的 1024 2048 4096 8192 16384	¥(CSP)@)
	<上一步(B) 下一步(A) > 取消

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。	
請輸入新憑證名稱。它應是個容易參考且記憶的名稱。 名稱(M):	
加密金鑰的位式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(出):	
□ 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(D) 取	(消

5.1.6 輸入憑證資訊(2)

以下欄位會出現在憑證內容之中,請小心填寫!各欄位說明如下:

5.1.6.1 公司:公司名稱,可使用縮寫,必須以英文方式填寫!

(如:臺灣網路認證股份有限公司為TWCA)

5.1.6.2 單位:使用該憑證之單位名稱。必須以英文方式填寫!

(如:系統部為 SYSTEM)

設定完成後→點選下一步。

IS 憲證精畫
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,請與憑證授權單位的網站聯絡。 公司(Q): TWCA 單位(U):
SWSTEM -
<上一步(B) (下一步(M) > 取消

5.1.7 輸入憑證資訊(3)

一般名稱:貴公司欲加密的網站名稱(如:www.twca.com.tw,不必加 http://

<u>或 https://)</u>

設定完成後→點選下一步。

IIS	憲設精査 🗾 🗾 🗾
惣	網站的一般名稱 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,請用有效的 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。
1	一般名稱(C):
\langle	www.twca.com.tw
-	<上一步(B) 下一步(B) 下

5.1.8 輸入憑證資訊(4)
5.1.8.1 國家(地區):選擇國家簡稱,如:TW(台灣)
5.1.8.2 州/省:國家全名,<u>必須以英文方式填寫</u>!(如:TAIWAN)
5.1.8.3 城市/位置:城市全名,<u>必須以英文方式填寫</u>!(如:TAIPEI)
設定完成後→點選下一步。

IIS 憲憲精畫	×
地理資訊 此憑證授權單位要求下列地理的資訊。	
國家 (地區)(∑): IW (台湾) ▼	
省/州③: TAIWAN	J
城市/位置①: TAIPEI	.
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@(下一步@)>	取消

5.1.9 指定執行出之憑證申請檔(CSR)檔案存放路徑。

如:C:\certreq.txt

設定完成後→點選下一步。

IIS 憑證精靈	×
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(四):	
z.\certreg.txt 瀏覽(R)	
<上一步B) 下一步D)> 取消	

5.1.10 確認憑證資訊(1)

→點選下一步。

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

IIS 憲證精靈		×
要求的檔案摘要 您已經選擇建立要求檔	家。	
若要建立下列要求,諸	波 [下一步]。	
檔案名稱: c:/certreq.tx	t	
您的要求包含下列資訊	l:	
發給 好記的名稱 國家地區 州/市 公司 單位	www.twca.com.tw test TW TAIWAN TAIPEI TWCA SYSTEM	
	<上一步图 (下-	一步(10)。 取消

本資料為臺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。

5.1.11 確認憑證資訊(2)

點選完成,「憑證請求檔(CSR)」產生完成。

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。建立了憑證 🛌 要求且儲存到檔案:	
	c:/certreq.txt	
	諸傳送或電子郵件此檔案到您的憑證授權,它將傳送給您含您的新憑證的回應檔案。請重新啓動此 送給您含您的新憑證的回應檔案。請重新啓動此 精靈來附加此新憑證到您的伺服器。	
	諸按 [完成] 來關閉此精靈。	
	<上一步(B) 完成 取消	

5.1.12 完成之憑證請求檔內容如下

🐻 certreq.txt - 記事本	
檔案(F) 編輯(E) 格式(Q) 檢視(Y) 說明(H)	
BEGIN NEW CERTIFICATE REQUEST	*
MIIESTCCAZECAQAwaTELMAkGA1UEBhMCVFcxDzANBgNVBAgTB1RBSVdBTjEPM	A ØG 📃
A1UEBxMGVEFJUEVJMQ0wCwYDVQQKEwRUV0NBMQ8wDQYDVQQLEwZTWVNURU0xGI	DAW
BgNVBAMTD3d3dy50d2NhLmNvbS50dzCCASIwDQYJKoZIhvcNAQEBBQADggEPAI	DCC
AQoCggEBAK4es248f2Wxi20fzolIU0SkfFHzePxgwOBB1XneYDgWRu0A1hm0x	Wyq
p/iZi66S00fnpgJC18D0A/kv/ntVY0WWHxMqh0B8H5IDTfBZqXw8lv92tAJRL	E+J
epwoCBbDoRZrG3Y4H/zRx7UoWcMPoDgXNoLDay44WcYgBcEy1015xCnqBPz1o	rGw
mZcyS4jDio1XM1gnw6sqFZYiQy4WyZUkH6Z1LhS8c5HGGsHIhBjk1F9OaCOm3	gZU
IUXiFga5SsRmF6hEegWRSYv6Z5Rn9Z6gfz8kGSfQjrz9Y1SnarQdFAoFdCi2QI	FEg
4010tH+mGhzgKKycAQ2B0LIfbxL18r0CAwEAAaCCAZkwGgYKKwYBBAGCNw0CA	ZEM
Fgo1LjIuMzc5MC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQEAwIE8	DBE
BgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDA0BggqhkiG9w0DBAICA	IAW
BwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR01BAwwCgYIKwYBBQUHAwEwgf0GC:	isG
AQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBA	CAA
UWBDAGgAYQBUAG4AZQBSACAAQWByAHkAcAB0AG8AZWByAGEAcABoAGkAYwAgAI	FAA
CGBNAHAAAABKAGNACGOBIQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAA
<u>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</u>	AAA
	AAA
AAAAAAAAAAAAAAAABOGCSqGSIb3DQEBBQUAA4IBAQALh7hQDvCrMHGuuOoO+dT2f.	JKC
DA3u1DMDuWhyG1xhdw8cEKB5m4rwEGKD61J1uFy8y4vFYKyVyk1mwUKkWKDdg	Zew
4CU4cu170tW2oUpzA3S50ArqkU273bnB8UFjU2PJmdshavYCepUM2cHFGsbUD	FNg
+1yjp4/qMjS9v+BUIPvx9xP9K8xod/82qL3SJUSI1Dw8jm/aBJ4WIxn2x1Lv+i	A5H
Ha+PbyH1+wF1H2eF7vcvp6jw1au9vcowownGgcHuqr3tsP1zyNvytj81ccJvEv	YVS
END MEW GERIIFIGHIE REQUESI	-
1	► //.

本資料為臺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。

5.2 將製作好的憑證請求檔(CSR)上傳

5.2.1 連接 TWCA 網站(1)

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

點選憑證服務,點選 SSL 憑證。



5.2.2 連接 TWCA 網站(2)

點選申請憑證。

※如申請 EV SSL 伺服器憑證,請點選 EV SSL 憑證。

双 透記旅程 TWCA - 臺灣網路 → ×	
SSL憑證	^
中請憑證	
EV SSL憑證	
申請憲證	
■ 財團法人金融聯合徵信中心加密檔案傳輸作業	
申請/増購憑證 憑證更新 憑證廃止 聯絡人異動 晶片卡解鎖 網站密碼重設	
■財金代繳代發憑證	
申請/培購憑證 憑證更新 憑證廢止 聯絡人異動 線上品片卡解鏡 網站密碼重設	▲ 柳葉花门

5.2.3 連接 TWCA 網站(3)

將瀏覽器視窗畫面往下拉,上傳 CSR。

上傳憑證請求檔(CSR)
請依據適用之『憑證操作手冊』產生憑證請求檔(CSR),手冊取得請來電02-2370-8886#9 洽詢。
產生憑證請求檔(CSR)後
請將CSR以純文字的方式儲存成為檔案(建議檔案名稱為Certreq.txt)後,請以純ASCII的文字编輯器(如記事本
來開啟此檔。注意不要使用文書處理軟體(如WORD)開啟,因為它們會額外插入文字的格式指令及控制字元。
• 傳送憑證申請檔 (CSR)
以下為CSR檔案的內容範例: —— BEGIN NEW CERTIFICATE REQUEST ——
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U
ECBMGVEFJV0FOMQ8wDQYDVQQHEwZUQUIXQU4xDjAMB
gNVBfwefEg,uhYUGJ84DWgbyGYGYVQQLEwJJVDEcMBoGA1U
EAxMTbGFiMzAwLnRhaWNhLmNvbS50dzBcMA0GCSqGSIb3D
QEBAQUAA0sAMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ
giJfHCa2diLHQq69SMUmLXNdnaVQnl4pkgPo1qNvKv0TKR7tac
LnfjmWxuUHUHUulihihiluHLUIHUILHhkiG9w0BAQQFAANBAIIG
5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD
duwd01q42V5xCmasPCImklri1TX4BYr5qzY=END NEW CERTIFICATE REQUEST
請將CSR檔案中的內容複製到下方的空欄中,注意複製的範圍應包括「BEGIN NEW CERTIFICATE
REOUEST 到「END NEW CERTIFICATE REOUEST」的宣告文字。

5.2.4 貼上憑證請求檔

開啟在 5.1 章節產生的憑證請求檔,利用全選後複製貼上的方式(CSR 檔 案內容包含-----BEGIN CERTIFICATE REQUEST-----、----END CERTIFICATE REQUEST-----),將製作好之憑證請求檔(CSR)內容貼 到申請欄位中→選擇繼續。

1		
	以下為USK檔条的內容較例, ——BEGIN NEW CERTIFICATE REQUEST——	
	MIIRIDCRSMIRADRdwdswcdadadde Smannagara	
	ECRWGAF1A0F0W68mD6ADA66HFm7n6ntx0fatx0fawr	
	gNVBfwefEg,uhYUGJ84DWgbyGYGYVQQLEwJJVDEcMBoGA1U	
	EAxMTbGFiMzAwLnRhaWNhLmNvbS50dzBcMA0GCSqGSIb3D	
	QEBAQUAA0sAMEgCQQDYdmR9MVXzUClzOE6wW0ggZRpZ	
	giJfHCa2diLHQq69SMUmLXNdnaVQnl4pkgPo1qNvKv0TKR7tac	
	LnfjmWxuUHUHUulihihiluHLUIHUILHhkiG9w0BAQQFAANBAIIG	
	5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD	
	duwd01q42V5xCmasPCImkIri1TX4BYr5qzY=END NEW CERTIFICATE REQUEST	
	請將CSR檔案中的內容複製到下方的空欄中,注意複製的範圍應包括「BEGIN NEW CERTIFICATE	
	REQUEST」到「END NEW CERTIFICATE REQUEST」的宣告文字。	
	แห่งกรรณระหภาพกายนายแห่งกายกายแห่งกายกายกายกายกายกายกายกายกายกายกายกายกายก	
	bgQWBBSR+R1sSSU/V/Z0Im68RkMAVeAP8DANBgkqhkiG9w0BAQUFAAOCAQEAZaCM	
	2Kk7q+NgpSIUj9kyT41MZJ6rKQo1vgrM30wArJystvirASXJKZHszeVPT5FER5a0	
	Q/Zm35L6mE9iUy3OR8/cbqQsvTXeeZb464uvK56FD1f7F9GqRSFLVrdKP8TGxTEc	
	D2vkD75Y6t/BLBeaxNSDf6wjaaWIYwmKOi90jv47fS9L6JgaXCloZZA8rVUDdh5k	
	jkYoBCl7J2cwKdyRvY5/uiqNGfrHqPdo4RtvTlbgQa7v7p5xTZKuWguf3B6oNPKA	
	odqB6O227bwFsy7W8fpmKgJECS0J0bc+fUUiXudC7m4wREDG8BmiABP3y8b7xrtw	
	we4hPuT0NcvMzHzqtw==	-
	END NEW CERTIFICATE REQUEST	1
	法按下「缵德」按纽以通送屮CCD,並缵德社皿程序。	
	ロリコス I ···································	
	鐵續重設	

本資料為臺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。

5.2.5 再次檢視上傳之憑證請求檔案內容

證作業 ×				
	IWCA			
安田	中口 网络上海索针皿夯料			
谷川				
The tens of pro	保密說明			
	申請憑證 您在此頁面所輸入的所有資料,傳送	至本公司時均受SSL安全機制保護, 並無外洩之虞, 請放心		
	源證發止 以下所有欄位皆為必填,並請注意以	半形文字輸入		
	^{漫論搜尋} 檢查CSR內容		\frown	
	解說		您的CSR內容	
	一般名稱:此名稱所代表的網站之多	安全性,將由此SSL伺服器憑證所保護	www.twca.com.tw	
	組織單位:這是一個可以用來區分組	追鱵部門的欄位	TWCA	
	組織:即貴公司的名稱		SYSTEM	
(城市/位置:即貴公司進行商業行為	時的所在[例: Taipei]	TAIPEI	
1.1.1	州/省: 即 貴公司進行商業行為的州	N/省所在地.請不要用缩寫的地名填寫此欄位[例: Taiwan]	TAIWAN	1
	國別:此欄係以ISO組織的國家代码	馬來表示. 舉例來說, TW代表台灣, US代表美國	TW	
	CCD A the E OF (hite)		2010	

5.2.6 設定通行密碼及選擇身分審驗方式

5.2.6.1 請自行設定通行密碼,該密碼請牢記,如您需要廢止憑證時,必須輸入此通行密碼。

請輸入通行密碼

通行密碼 此密碼是廢止憑證所需,	建立通行密碼	

5.2.6.2 為符合 SSL 憑證國際審放標準,將審驗網域所有權者請您選擇以下一種審驗方式:

一、EMAIL 驗證:將會自動帶出網域註冊之 EAMIL 或者請選擇 admin@網域、administrator@網域、webmaster@網域、hostmaster@ 網域、postmaster@網域此六個 EMAIL 任一個 EMAIL 皆可進行身分 驗證作業,選擇送出後系統將會寄出驗證信,請務必至該信箱完成驗 證作業

二、檔案驗證:請您填入收取該檔案收件人 EMAIL,您將在此 EMAIL 收到一附件檔案,請您依照信件說明將檔案放入,完成後請通知我們進 行檔案驗證作業。

三、電話驗證:網域所有權人的資料可公開查詢到才能使用電話驗證,

本資料為臺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。

請您選擇進行電話驗證的時段,我們將依照您所選擇的去電驗證。

網域所有權

	為符合SSL憑證國際審放標準,將審驗網域所有權請您選擇以下一種審驗方式。			
	● 網域所有權EMAIL驗證:點選確認後,糸統將會自動寄出驗證信,諸用戶務必至該信箱收信並點擊確認即可。			
	◉ maintain@twca.com.tw (網域註冊資料來源由WHOIS取得)			
	或諸選擇			
	admin@twca.com.tw			
	administrator@twca.com.tw			
细博管理者	webmaster@twca.com.tw			
11 J-04 E -T E	hostmaster@twca.com.tw			
	ostmaster@twca.com.tw			
	────────────────────────────────────			
	諸您填入接收電子信箱:maintain@twca.com.tw ,將郵寄檔案及說明給您。			
	◎ 電話驗證:我們將以電話驗證方式確認網域所有權			
	請您留下方便聯絡的時間: 🖲 皆可 🔍 上午時段 🔍 下午時段			

5.2.6.3 填寫表單編號,並確認以上表單內容輸入正確後,按繼續送出申

請。

確認以上所輸入的資料正確後,請輸入表單編號,按"繼續"送出申請

表單編號 請輸入憑證申請單 <mark>右上角</mark> 的表單編號	若未填過憑證申請單,諸線上登打憑證表單線上作業輸入
請按一下"繼續"按鈕以送出註冊資料,完成註冊程序。	繼續

本資料為臺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,

5.2.7 送出後等待 CA 系統簽發憑證

CSR 上傳完成後,近日會完成驗證(以下畫面為選擇電話驗證的顯示結

果),憑證簽發後會以 Email 通知業務及技術聯絡人(TWCA SSL 伺服器數

位憑證下載通知),憑證亦可以在 TWCA 網站搜尋及下載。



本資料為臺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,

5.3 下載已核發憑證

1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經審驗通過,將會寄送「SSL 伺服器數位憑證 下載通知」電子郵件給相關聯絡人,郵件內容包含附件憑證鏈壓縮檔(cert.zip) 及 TWCA SSL 動態認證標章之安裝說明與標章圖檔連結。

將附件憑證鏈壓縮檔 Cert.zip 解壓縮後,可得到三個憑證鏈檔。

※內容及憑證用途如下圖所式:

cert	
-	根憑證檔
-	伺服器憑證檔
-	中繼憑證檔
	cert →

2 檔案下載說明

如果因為貴公司之 mail server 設定,導致無法順利取得附件憑證鏈壓縮檔案, 請依照下列步驟,利用本公司網站憑證搜尋功能,下載憑證鏈壓縮檔。

本資料為臺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,



5.3.3 輸入申請之網站名稱

在網站名稱中輸入憑證申請單上填寫之網站名稱(Common Name),如

www.twca.com.tw (注意,大小寫需一致,不必加 http://或 https://),輸

入完成後,按下搜尋鍵。

				– 🗅 ×
🕞) 🛞 🙋 https://ssl2.twca.com.tw/NCWebSSl	L/search.htm?dns=&Submit=%B7j%B4M	- 🗎 C	搜尋	P • 🖓 🕁 🕲 🤤
🐹 憑證服務 TWCA - 臺灣網路認 🧔 SSL憑證作業	ŧ×∎.			
				/
-				
客服專區	🔍 查詢用戶憑證			
Service	請輸入網站名稱(Common Name)以搜尋TWC	A SSL伺服器憑證		
The new HP helitiog explain vestimistic delivers the proves and graphics performance of a vestimization with the				
申請憑證	網站名稱 www.twca.com	.tw		
憑證廢止	Commonwanie (@guwww.twca	.com.tw)		
憑證搜尋	搜尋			請輸人網站名稱
1000				
				~

本資料為臺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,

5.3.4 下載憑證鏈壓縮檔

確認憑證相關資訊與申請相符後點選下載→憑證鏈,另開檔案下載視窗,按下另存新檔,儲存憑證鏈壓縮檔 cert.zip。



接下來無論憑證需要裝到哪一台伺服器,都一定要將核發下來的憑證,在先前 建立憑證要求的伺服器上安裝,如果您的網站並非建在這台伺服器,還是需要 先在這台伺服器安裝好,之後再參考 5.8 章節從這台伺服器匯出憑證,及 5.9 章節,將憑證匯入到您的網站伺服器。

5.4 安裝根憑證

5.4.1 儲存根憑證

請參照 5.3 章節相關步驟,將根憑證檔 (root.cer) 儲存於電腦中可存取 位置。

本資料為臺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。

5.4.2 新增憑證管理單元

請參照 5.11 章節新增憑證管理單元。

5.4.3 安裝根憑證(1)

點選展開主控台根目錄內的憑證(本機電腦)→信任的根憑證授權→於 憑證上按滑鼠右鍵選所有工作→點選匯入。

1根目錄		發行者	到期日	預定目的	好記的名稱
證 (本機電腦)	ABA.ECOM Root CA	ABA ECOM Root CA	2009/7/10	安全電子郵件,用戶	DST (ABA.ECOM) CA
1個人	🔤 Ald Trust External CA Root	Add Trust External CA Root	2020/5/30	伺服器驗證,用戶端	USER Trust
「11的根患證授權	🔤 Autoridat. Certificadora de la Asoci	Autoridad Certificadora de la Asociaci	2009/6/29	安全電子郵件,伺服	Autoridad Certificadora d
● 所有工作(K) ▶	M Qertificadora del Colegi	Autoridad Certificadora del Colegio N	2009/6/30	安全電子郵件,伺服	Autoridad Certificadora d
	CyberTrust Root	Baltimore CyberTrust Root	2025/5/13	伺服器驗證,安全電	Baltimore CyberTrust Ro
中和1 检視(Ⅴ) ▶	E Baltimore EZ by DST	Baltimore EZ by DST	2009/7/4	安全電子郵件,伺服	DST (Baltimore EZ) CA
又信に 没有方 從這裡新增視窗(W)	🔄 Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	2010/1/21	安全電子郵件,伺服	Belgacom E-Trust Prima
	🔤 C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	2009/10/16	安全電子郵件,伺服	CW HKT SecureNet CA
ホーノ 新工1F日1徴税(山) 受信化	🔤 C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class B	2009/10/16	安全電子郵件,伺服	CW HKT SecureNet CA
其他/ 重新整理(F)	🔤 C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	2010/10/16	安全電子郵件,伺服	CW HKT SecureNet CA
McAfe 匯出清單(L)	🔤 C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	2009/10/16	安全電子郵件,伺服	CW HKT SecureNet CA
	CA 1	CA 1	2019/3/11	安全電子郵件,伺服	ViaCode Certification A
SPC 説明(H)	🔤 Certiposte Classe A Personne	Certiposte Classe A Personne	2018/6/24	安全電子郵件,伺服	Certiposte Editeur
	🔤 Certiposte Serveur	Certiposte Serveur	2018/6/24	安全電子郵件,伺服	Certiposte Serveur
	🔤 Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/27	安全電子郵件,伺服	Certisign Autoridade Ce
	🔤 Certisign - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/27	安全電子郵件,伺服	Certisign Autoridade Ce
	🔤 Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/6/27	安全電子郵件,伺服	Certisign Autoridade Ce
	🔤 Certisign Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/7/10	安全電子郵件,伺服	Certisign Autoridade Ce
	Class 1 Primary CA	Class 1 Primary CA	2020/7/7	安全電子郵件,伺服	CertPlus Class 1 Primary
	Class 1 Public Primary Cartification	Class 1 Public Primary Cartification 4	2028/8/2	实补需子配件 田丘	VariSim Class 1 Public

5.4.4 安裝根憑證(2)

啟動歡迎使用憑證	匯入精靈→點選下一步。
燕證匯入精靈	
	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(B) (下一步(B) 取消

5.4.5 安裝根憑證(3)

點選瀏覽,指定根憑證檔存放位置→點選下一步。

本資料為臺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。

憲證匯入精畫 🛛 🔀
匯入檔案 指定您想要匯入的檔案。
檔案名稱(正):
C:\root.cer
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)
<上一步图 下一步创 > 取消

5.4.6 安裝根憑證(4)

按預設點選將所有憑證放入以下的存放區→憑證存放區→信任的根憑證 授權→點選下一步。

進入 相	f畫
憲證 存: 逓證	放區 控放區是用來存放憑證的系統區域。
Win	dows 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。
	」目動根據應證類型來選取應證存放區(U) 一次所有應證於人以下的定於區(P)
	透證存放區:
	信任的根憑證授權 瀏覽(R)
	(上一步图) 下一步图 取消

5.4.7 安裝根憑證(5)

點選完成

本資料為臺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。

SSL 伺服器數位憑證 IIS 6.0 操作手册

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 信任的根憑證授權 內容 憑證 檔案名稱 C.voot.cer	
	<上一步(B) 完成 取消	

5.4.8 完成根憑證安裝



本資料為臺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,

5.5 安裝中繼憑證

5.5.1 儲存中繼憑證

請參照 5.3 章節相關步驟,將中繼憑證檔(uca.cer)儲存於電腦中可存 取位置。

5.5.2 新增憑證管理單元

請參照 5.11 章節新增憑證管理單元。

5.5.3 安裝中繼憑證(1)

點選展開主控台根目錄內的憑證(本機電腦)→中繼憑證授權→於憑證 上按滑鼠右鍵選所有工作→點選匯入。

🌇 主控台根目錄/憑證 (本機電腦)\中繼憑證)	技種法證					
📄 主控台根目錄	發給 ∧	發行者	到期日	預定目的	好記的名稱	~
🖻 🐻 憑證 (本機電腦)	🖼 GlobalSign Root CA	Root SGC Authority	2014/1/28	1.3.6.1.4.1.311.10.3	<無>	
■ 🛄 個人	🖼 GTE CyberTrust Root	Root SGC Authority	2006/2/23	1.3.6.1.4.1.311.10.3	<無>	
■ ■ 信任的根態證授權	🔤 Microsoft Windows Hardware Com	Microsoft Root Authority	2002/12/31	代碼簽署,Windows	<無>	
	📔 🔤 Microsoft Windows Hardware Com	Microsoft Root Authority	2002/12/31	代碼簽署,Windows	<無>	
	SGC Authority	Root SGC Authority	2010/1/1	伺服器驗證,1.3.6.1	<無>	
心理和明何単	MSN Content Authentication CA	MSN Content PCA	2017/2/10	代碼簽署,時間戳記	<無>	
日本 受信日 所有工作(区) ・	匯入① ntent Authentication CA	MSN Content PCA	2010/2/25	代碼簽署,時間戳記	<無>	=
2 2 2 有信 检理(17) →	MSN Content PCA	Microsoft Root Certificate Authority	2017/2/10	《全部》	<無>	=
	Root Agency	Root Agency	2040/1/1	<全部>	<無>	
■ 受信任	📔 🔤 SecureNet CA SGC Root	Root SGC Authority	2009/10/16	1.3.6.1.4.1.311.10.3	<無>	
🗉 🧰 其他人 新工作台檢視(I)	🔛 TaiCA Information Policy CA	TaiCA Secure Root	2013/3/19	<全部>	<無>	
● ● 憑證註	🔛 TaiCA Information User CA	TaiCA Information Policy CA	2013/3/19	<全部>	<無>	
	🔛 Thawte Premium Server CA	Root SGC Authority	2004/7/17	1.3.6.1.4.1.311.10.3	<無>	
進出清萆(止)	🔛 Thawte Server CA	Root SGC Authority	2004/7/17	1.3.6.1.4.1.311.10.3	<無>	
説明(H)	TWCAOA	TWCAOA	2027/7/13	《全部》	<無>	_
	🔛 TWCAWLAN	TWCAWLAN	2032/5/23	<全部>	<無>	
	🔛 TWCAWLAN	TWCAWLAN	2032/5/23	《全部》	<無>	
	🔛 TWCAWLAN	TWCAWLAN	2032/5/23	<全部>	<無>	
	🔛 TWCAWLAN	TWCAWLAN	2032/7/13	<全部>	<無>	
	TIMC 6 IMT 6 M	TIMCAINTAM	20122/5/22	~~	<u>∼</u> ∰~	×
						/
將新憑證加入存放						

5.5.4 安裝中繼憑證(2)

啟動歡迎使用憑證匯入精靈→點選下一步。



5.5.5 安裝中繼憑證(3)

本資料為臺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。

點選瀏覽,指定中繼憑證檔存放位置→點選下一步。
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):
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 #/認證 (.p/b)
MILTOSOTT FF Y DESED 17 DQ (.SSI)
< <u> < </u>
5.5.6 安裝中繼憑證(4)
按預設點選將所有憑證放入以下的存放區→憑證存放區→中繼憑證授
→ 點選下一步。
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。
透露在放區:
中繼憑證授權 瀏覽 (R)
<上一步(B) 下一步(B) 取消

5.5.7 安裝中繼憑證(5) 點選完成。	
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 中繼憑證授權 內容 憑證 檔案名稱 C:\uca.cer
558 中土山磁馮城穴排	<上一步(B) 完成 取消
3.3.0 元成 半 極 忽 證 女 农	



5.6 安裝伺服器憑證

5.6.1 儲存伺服器憑證檔

請參照 5.3 章節相關步驟,將伺服器憑證檔 (server.cer) 儲存於電腦中可存取位置。

5.6.2 執行網際網路資訊服務(IIS)管理員

點選桌面左下角開始→程式集→系統管理員→執行網際網路資訊服務 (IIS)管理員。在 5.1 章節產生憑證申請檔(CSR)的站台上按滑鼠右鍵→點 選內容→目錄安全設定→點選伺服器憑證。

網站	11F 惊頭 效能	ISAPI 舘	□=]3 選器 ┃	暗誤 主目錄	 文件	A.S. NEI 目錄安全設	定
驗證及存	取控制 啓用匿名存 證方法。	取,並編輯這	個資源的點	¢	輯(正)		
IP 位址及	網域名稱限制						
8	使用 IP 位址 或拒絕到這	或網際網路約 固資源的存取	罔域名稱來 ₹。	授予 	輪報①		
安全通訊							
-	當存取這個 用用戶端憑	資源時使用多 證。	全通訊並帮		器憑證(S) 記愿證(Y) 諸報(D)		
						_	



5.6.4 安裝伺服器憑證(2)

點選	瀏覽	,	指	定	到取	得的	server	.cer	檔	案→	下	一步	0
----	----	---	---	---	----	----	--------	------	---	----	---	----	---

IIS 憲證精靈	
虚理 翻置要求 藉由擷取含憑證授權回應的檔案來處理憑證擱置要求。	
請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):	\frown
C:\server.cer	(瀏覽·R)
	Į
<上一步图 [下一	步图> 取消

本資料為臺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 bouring is the availability property of TWCA and shall not be distributed

5.6.5 安裝伺服器憑證(3)

請先設定 SSL 連接埠,預設值為 443 →下一步。

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

5.6.6 安裝伺服器憑證(4)

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。

IS 憲證精靈	
您已經選擇從回盟 憑證摘要	檔案安装読書・
若要安裝下列調	證,請按[下一步]。
檔案名稱:	D:\TWCA\SSL\测試憑證申請與畫面\IIS60\ServerCert.crt
憑證詳細資訊: 發發期日 好記。 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	192.168.0.89 TaiCA Secure CA -Evaluation Only 2006/09/04 TASO20-3 TW Taiwan Taipei TWCA IT
	<上一步(B) 下一步(B) 取消

5.6.7 安裝伺服器憑證(5)

點選完成,完成伺服器憑證安裝。

- 5.7 檢視憑證是否安裝成功
 - 5.7.1 新增憑證管理單元

請參照 5.11 章節新增憑證管理單元。

5.7.2 新增憑證管理單元

點選展開主控台根目錄內的憑證(本機電腦)→個人→憑證。查看右側 欄位是否顯示已安裝之伺服器憑證。若無,代表憑證並未安裝成功,請參 照 5.6 章節安裝伺服器憑證。若有,請點選開啟該張憑證。

福主整台1	
檔案① 執行(4) 檢視(7) 我的最愛(2) 親窗(22) 說明(4)	
日本日本日本 日本日本日本 日本日本日本 日本日本日本 日本 日本 日本 日本	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
田 🖻 受信任的人	
随人存放包含 個感識。	

5.7.2.1 一般欄位:請確認有效期起迄時間是否正確,

並於下方顯示這個憑證有一個對應的私密金鑰。

	? ×
一般)詳細資料 憑證路徑	1
馬首電機 🔛	
這個派證的使用目的如下: ·確保遠端電腦的證別	
*諸參照憑證受權敘述中的詳細資訊。	
登給 : www.twca.com.tw	-
登行者 : 『WCA Secure CA	
有效期自 2011/5/3 到 2014/5/3	
🌮 這個憑證有一個對應的私密金鑰。	
经行者举明	2
 	定

本資料為臺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。

5.7.2.2 憑證路徑欄位:請確認憑證鏈是否正確,且憑證狀態顯示這個憑證

Baltimore CyberTrust Root	
	検用振動の
	1双形兄招咒言臣(<u>平</u>)

<u>没有問題</u>,可確認憑證已安裝成功。

5.8 匯出憑證(備份)

5.8.1 新增憑證管理單元

請參照 5.11 章節新增憑證管理單元。

5.8.2 匯出憑證(1)

點選展開主控台根目錄內的憑證(本機電腦)→個人→憑證,在欲匯出 的伺服器憑證上按右鍵所有工作→點選匯出。

音主控台1		
檔案 (上) 執行(▲) 檢視(⊻) 我的最愛(2) 親留	£(Ψ) 説明(E)	
匯出憑證		
5.8.3 匯出憑證(2)		

本資料為臺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, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

第36頁

SSL 伺服器數位憑證 IIS 6.0 操作手册

5.8.6 匯出憑證(5)

設定匯出資料的保護密碼→點選下一步。(請務必記住此密碼,匯入憑證 時需使用)

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(2):	
**** 確認密碼(_):	

<上一步(B) 下一步(B) 取消	

5.8.7 匯出憑證(6)

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

建匯出精靈	
要匯出的檔案 諸指定您要匯出的檔案名稱	
檔案名稱(E):	
D.\TWCA\SSL\測試憑證申請與畫面\US60\US60.pfx 瀏覽(R).	2
	TL-Adv
<u>《上一步图】(下一步(1))</u>	取消

本資料為臺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,

5.8.8	完成匯出憑證(備份	;)

點選完成。

憑證匯出精靈		×
	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 DATWCANSLAIII訊應 健出金鑰 是 包含憑證路徑中的所有憑證 是 檔案格式 個人資訊交換 (*.pfx)	
	<上一步(B) 完成 取消	

5.9 匯入憑證(還原)

5.9.1 新增憑證管理單元

請參照 5.11 章節新增憑證管理單元。

5.9.2 匯入憑證(1)

點選展開主控台根目錄內的憑證(本機電腦)→個人,按滑鼠右鍵→所 有工作→點選匯入。

☆主接台1		×
檔案(E) 執行(A) 檢視(V) 我的最愛(O) 視窗(U)	D 説明(H)	
主控台根目錄\憲證 (本機電腦)\個人		
日 主控合根日球 物件類型		
	這個檢視沒有項目可顯示。	
● 信任的規念證授権		
日 二 正未行に		
田 💼 受信任的發行者	尋找憑證(N)	
■ ○ 第三方根憑證授權單位	所有工作(些) ▶ 尋找憑證(型)	
	重新整理EP 匯入(1)	
E _ SPC	檢視(⊻) →	
	排列圖示① ▶	
	對齊圖示(E)	
個人在防范中旬今碼證。	說明(出)	

5.9.3 匯入憑證(2)	
啟動歡迎使用憑證匯入精靈	→點選下一步。

憲證匯入精靈		×
	歡迎使用憑證匯入精霊	
	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。	
	請按 [下一步] 繼續。	
	<上一步(B) (下一步(B)) 取消	

本資料為臺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。

SSL 伺服器數位憑證 IIS 6.0 操作手册

5.9.4 匯入憑證(3)	
點選瀏覽。	
憲證匯入精畫	X
羅入緯案	
指定您想要匯入的檔案。	
	_
· · · · · · · · · · · · · · · · · · ·	
副夏区	
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進 - PKCS #7 認證 (π7h)	
Microsoft 医利振鹉方的 (set)	
MILIOSOT /T/ 1/2/2017/1X (.880)	
	-

5.9.5 匯入憑證(4)

指定到當初匯出備份的檔案(*.PFX)→點選開啟。

閒容					<u>? ×</u>
查詢(]):	🞯 桌面		•	3 🔊 📂	
 我最近的交件 () ()	→ 我的交件				
我的電腦 () 網路上的芳鄰	檔名(N): 檔案類型(T):	 個人資訊交換 (*pfx;*p12)	•	開啓(1) 取消

SSL 伺服器數位憑證 IIS 6.0 操作手册

入精靈 ↓ 檔案 指定您想要匯入的檔案。			
檔案名稱(E):			
D:\TWCA\SSL\测試憑證申詞	諸與畫面VIIS60\Te	st.pfx	瀏覽(R)
請注意: 您可以將數個憑證	用以下的格式存放	收在同一個檔案中:	
個人資訊交換-PKCS #12	2 (.PFX, P12)		
密碼編譯訊息語法標準·	- PKCS #7 認證 (.p	7Ъ)	
Microsoft 序列憑證存放	(.sst)		

5.9.7 匯入憑證(6)

輸入匯出(備份)憑證時所設定的密碼→勾選將私密金鑰標示成可匯出 →點選下一步。

密碼 齊了維護安全性,利	私変金鑰受到來碼保護。
	はつし」 近 5 冊 人、 プリー ゆうり/16 文
詰輸入私変会論的网	宓稲隹。
密碼伊	

□ 啓用加強以来	8金鑰保護。如果您啓用這個選項,每次私密金鑰被應用程
一十/市田 王王	
式使用,系称	東會通知您(但)
式使用了系统	· 史曾通知您(E)
式使用 「茶」	東會通知想(但) 發成可匯出。這樣您將來可以進行備份或傳輸您的金編(M)
式使用 「茶」	東會通知您(但) 發成可匯出。這樣您將來可以進行備份或傳輸您的金鑰(M)
式使用 「茶」	東會通知您(在) 發成可匯出。這樣您將來可以進行備份或傳輸您的金鑰(M)
式使用 「茶」	東會通知您(E) 發成可匯出。這樣您將來可以進行備份或傳輸您的金鑰(M)

5.9.9 完成匯入憑證(還原) 點選完成。

憲 證 匯入精畫	完成憑證匯入精畫	×
	您已經成功地完成憑證匯入精靈。	
	您已指定下列新設定:	
	使用者難取的憑證存放區。個人 內容 PFX 檔案名稱 DATWCASSLA測試憑證	
		F
	<上一步(B) 完成 取消	ŧ

本資料為臺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。

5.9.10 確認伺服器憑證是否匯入成功 點選展開主控台根目錄內的憑證(本機電腦)→個人→憑證。 確認右側欄位確實顯示已匯入之伺服器憑證。

注意 主 接 台 1					- 🗆 ×
檔案 一 執行 (人) 檢視 (义) 我的最	景愛(O) 親窗(₩) 説明(H)				
← → E E % B × C	' 🗟 🖻 💷				
🎦 主控台根目錄\憑證 (本機電腦)\	國人憑證				
	發給 /	- 我们者	ZUHR C	預定目的	
	i 192.168.0.89	TaiCA Secure CA	2008/10/13	<全部>	
「日本語」					
田 二 信任的 很愿證授權					
□ □ 中繼憑證授權					
田····································					
主 第三方根憑證授權單位 東京ない					
田 🛄 文信日年97人 田 🛄 憑證註冊要求					
🕀 🧰 SPC					
	4			<u> </u>	
個人 存放包含 1 個憑證。				lie	

5.9.11 執行網際網路資訊服務(IIS)管理員

點選桌面左下角開始→程式集→系統管理員→執行網際網路資訊服務 (IIS)管理員。在欲執行 SSL 模式的站台上按右鍵→內容→目錄安全設定 →點選伺服器憑證。

F	TTP 槽面		講題	1	ASPNET
網站	2 效能 2	ISAPI 篩選器	主目錄	文件	目錄安全設定
腺證及有	F取控制 啓用匿名存取,並 調方法。	应編輯這個資源的專	^食	ŧ <u>(E)</u>]	
_ IP (守址 R	を網域タ種限制				1
8	使用 IP 位址或網 或拒絕到這個資源	際網路網域名稱來 亰的存取。	授予编	ä()	
安全通訊	、 當存取這個資源B) 用用戶端憑證。	,使用安全通訊並帮	資 何服器 校視!	憑證(S))
			編車	₿(D)	

本資料為臺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。

5.9.12 啟動伺服器憑證精靈

啟動歡迎使用網頁伺服器憑證精靈→點選下一步。

SSL 伺服器數位憑證 IIS 6.0 操作手册

5.9.14 取代目前的憑證(2)

選擇已匯入的憑證項目→點選下一步。

 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①:

 「

 (上一步(四)
 下一步(四)

 取消

SSL 伺服器數位憑證 IIS 6.0 操作手册

5.9.16 取代目前的憑證(4)

檢視已選取安裝憑證資訊→點選下一步。

5.9.18 安裝根憑證及中繼憑證

執行完以上步驟後,請參照 5.4 章節安裝根憑證及 5.5 章節安裝中繼憑證。

本資料為臺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。

5.10 更新 SSL 憑證

5.10.1 申請說明

臺灣網路認證公司會在 SSL 伺服器憑證到期前二個月發出憑證更新通 知信給 貴公司。這二個月內您隨時可以至本公司網站

https://www.twca.com.tw 下載申請表單,填寫完畢後寄回臺灣網路認證 公司,即可進行 SSL 憑證更新申請。

5.10.2 更新步驟

5.10.2.1 新增臨時站台

由於原站台上已安裝 SSL 憑證,無法比照 5.1.3 利用建立新憑證選項,

產生憑證請求檔(CSR);

故請先選用下列兩種方法,新增一臨時站台,以利後續更新作業。

※於本機 Web Server 新增臨時站台

※於另一台有安裝 IIS 服務的 Windows 主機,新增臨時站台

新增步驟如下:

5.10.2.1.1 新增臨時站台(1)

點選桌面左下角開始→程式集→系統管理員→執行網際網路資訊 服務(IIS)管理員。點選展開電腦名稱(本機電腦)→在網站上按右鍵 選擇新增→點選網站。

済訊服務 描述 (本機電腦)	識別元
新增创 ▶ 網站(<u>W</u>)… 所有工作(<u>K</u>) ▶ 網站(從檔 檢視(<u>V</u>) ▶	
從這裡新增視窗(₩) 重新整理(P) 匯出清單(L)	
內容(<u>R</u>)	
說明(H)	

5.10.2.1.2 新增臨時站台(2)

啟動歡迎使用網站建立精靈→點選下一步。

洞站建立精靈		×
	歡迎使用網站建立精靈	
PATA	此精靈將協助您在這台電腦建立新的網站。	
	如果要繼續,諸按 [下一步]。	
	<上一步图 下一步图 取消	

5.10.2.1.3 新增臨時站台(3)

說明欄位可自由設定,請填入較有意義之文字→點選下一步。

5建立精莹 站說明 描述網站來協助管理員識別它。	SW.
詰輸入網站 說明。	
說明(D):	
test	
	-

5.10.2.1.4 新增臨時站台(4)

按預設值設定→點選下一步。

(2557) 這個網站應該使用的 TCP 連接埠 (預設) [80	▼ 直:80)(<u>T</u>):
這個網站應該使用的 TCP 連接埠 (預設) 180	直: 80)(<u>T</u>):
80	
此網站的主機標頭(預設值:無)(出):	

5.10.2.1.5 新增臨時站台(5)

請自行選擇主目錄存放路徑→點選下一步。

明站主目錄	
主目錄是您的網頁內容子目錄	泉的根目錄。
請輸入您的主目錄路徑。	
路徑(P):	
D:\test	瀏覽(R)

5.10.2.1.6 新增臨時站台(6)

按預設值設定存取權限→點選下一步。

網站建立精靈 網站存取權限 設定此網站的存取權限。	×
九許下列權限:	Channa and Andrea
☑ 請取(B)	
□ 執行指令碼(例如 ASP)(S)	
厂 執行 (例如 ISAPI 應用程式或 CGI)(E)	
□ 寫入(₩)	
□ 瀏覽(0)	
若要完成精霊,諸按 [下一步]。	
《上一步图》 下一步图》	取消

5.10.2.1.7 新增臨時站台(7)

點選完成。新增臨時站台完成。

網站建立精靈		×
	您已經成功完成網站建立精 靈。	
VAN	諸按 [完成] 來屬閉這個精靈。	
	<上一步(B) 完成 取消	

5.10.2.2 產生「憑證請求檔(CSR)」

請於臨時站台,參照 5.1 章節步驟,產生憑證請求檔(CSR)。

※憑證請求檔(CSR)產生後,不可點選刪除擱置要求,否則憑證將無法安裝!

5.10.2.3 將製作好的憑證請求檔(CSR)上傳

請參照 5.2 章節步驟,將製作好的憑證請求檔(CSR)上傳。

5.10.2.4 下載已核發憑證

請參照 5.3 章節步驟,取得或下載已核發憑證。

5.10.2.5 安裝根憑證

請參照 5.4 章節步驟,安裝根憑證。

5.10.2.6 安裝中繼憑證

請參照 5.5 章節步驟,安裝中繼憑證。

5.10.2.7 安裝伺服器憑證

請於產生憑證請求檔(CSR)的臨時站台,參照 5.6 章節步驟, 安裝伺服器憑證。

5.10.2.8 修改目前的憑證指派

※若是於本機 Web Server 新增臨時站台,執行完 5.6 章節安裝伺服器憑證後,不必匯出憑證。請您於 IIS 的網站清單中,將欲更新 SSL 憑證的站台上按右鍵→內容→目錄安全設定→點選伺服器憑證。取代目前的憑證,於憑證清單中選取憑證即可完成 SSL 憑證更新。

本資料為臺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。

SSL 伺服器數位憑證 IIS 6.0 操作手册

※若是利用另一台有安裝 IIS 服務的 Windows 主機新增臨時站台,請於該主機執行完 5.6 章節安裝伺服器憑證後,參照 5.8 章節步驟匯出憑證,將匯出之檔案(*.PFX)儲存至欲更新 SSL 憑證的 Web Server 主機上,再參照 5.9 章節將憑證匯入,將欲更新 SSL 憑證的站台上按右鍵 →內容→目錄安全設定→點選伺服器憑證,取代目前的憑證,於憑證 清單中選取憑證即可完成 SSL 憑證更新。

SSL 伺服器數位憑證 IIS 6.0 操作手册

IIS	憲證精靈			
ŋ	「用的憑證 下列 溝單包含可,	用於您的網頁伺服	器的憑證。	
	諸選取憑證			
_	發給	發照者	到期日	使用目的
	www.twca.com.t	w TWCA Secure	CA 2014/5/3	伺服器驗證,用t
	•			
			《上一步匪) 下一步四 取消

5.11 新增憑證管理單元

5.11.1 開	啟 MMC 主控台		
點選	開始→點選執行→	·輸入 mmc s	並按下確定 。
執行			? ×
	輸入程式、資料夾、 Windows 會自動開啓	文件或網際網路 。	資源的名稱,
開啓(0):	[mmc]		-
	確定	取消	瀏覽(B)

5.11.2 新增/移除嵌入式管理單元

點選檔案→點選新增/移除嵌入式管理單元。

☐ 主接台1	
【檔案 E】 執行 (A) 檢視 (V) 我的最愛 (Q) 視窗 (W) 説明 (H)	
開新檔案(N) Ctrl+N 開啓舊檔(O) Ctrl+O	
儲存(S) Ctrl+S× 另存新檔(A).	
新增修除嵌入式管理單元(M)Ctd+M 超檢視沒有項目可顯示。	
<u>1</u> C:\WINDOWS\\inetsrv\iis.msc <u>2</u> C:\WINDOWS\\compmgmt.msc <u>3</u> SQLServerManager.msc 4 C:\WINDOWS\\eventywr.msc	
讓您能夠從嵌入式管理單元主控台中新增或移除嵌////////////////////////////////////	

5.11.3 新增獨立嵌入式管理單元單元					
點選新增。					
新增相除嵌入式管理單元		? ×			
獨立 延伸	獨立 延伸				
用這個畫面從主控台中新增或移移	涂獨立的嵌入式管理單元。				
1曲火吧					
新增D 移除B)	關於(B)				
		Hirt Sale			
	唯化	4以/月			
5.11.4 新增憑證單元					
點選憑證→點選新增。					
新增獨立嵌入式管理軍元		? ×			
可用的獨立嵌入式签理開 去 。					
· · · · · · · · · · · · · · · · · · ·	廠商				
	Microsoft Corp, Execut	¥			
● ● 磁碟管理 ● ● 細い油な	Microsoft and VERITA				
▶ 約41年前 ● 網際網路咨訊服務 (US) 管理昌	Microsoft Corporation				
● 網際網路驗證服務 (IAS)	Microsoft Corporation				
通 遠端桌面	Microsoft Corporation				
	Microsoft Corporation				
國源證授權單位	Microsoft Corporation				
國 憑證範本	Microsoft Corporation	-			
,					
憑證嵌入式管理單元讓您瀏覽電腦	試服務的憑證存放內容。				
	新增(A) 闘闘	9C)			

本資料為臺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,

5.11.6 選擇本機電腦

點選本機電腦(執行這個主控台的電腦)→點選完成。

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將自動管理:	
• 本機電腦 (執行這個主控台的電腦)(L):	
○ 另一台電腦(L): 瀏覽(R)	
 □ 九許對選取的電腦進行從命令到所啓動的變更。這只在您儲存主控台後才能適用 (型) 	
<上一步(B) 完成 取消	

5.11.7 新增憑證管理單元完成

當憑證(本機電腦)新增完成後→點選關閉→點選確定。

★ 主接台1 新碧/移除嵌入式管理單元	?×	
	新增獨立嵌入式管理軍元	? ×
用這個畫面從主控台中新增或移除發展。	可用的獨立嵌入式管理單元:	
	嵌入式管理單元	廠商 ▲
嵌入式管理單元 🔄 主控台根目的		Microsoft Corp, Executi
新增到(3): 1	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Microsoft and VERITA
	● 約4224 ● 網路網路溶訊服務(US)答理品	Microsoft Corporation
	● 網際網路驗證服務 (IAS) 目空見	Microsoft Corporation
	副遠端点面	Microsoft Corporation
	國憑證	Microsoft Corporation
	國 憑證授權單位	Microsoft Corporation
	🙀 憑證範本	Microsoft Corporation
┃	」 描述 憑證嵌入式管理單元讓您瀏覽電腦或,	
		新增(山) 關閉(二)
	確定取消	

6.常見問題

6.1 請參閱 https://www.twca.com.tw/picture/file/SSL 常見技術問題手冊.pdf。

本資料為臺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,

7.附件

魚。

本資料為臺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