SSL 數位憑證 IIS6 憑證安裝說明





106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

### 【版權及商標聲明】

本文件由 Cloudmax 匯智製作,並保留所有權利。

文件提供之安裝步驟僅供參考,詳細狀況依伺服器版本或所在網路環境、架構而有些微差 別,請依實際狀況或系統提供商資訊為準,若於安裝上有任何問題可與我們聯繫,將有專員 引導您排除障礙。

本文件所引用之各商標及商品名稱分屬其合法註冊公司所有,絕無侵權之意,特此聲明。

### 【有限擔保責任聲明】

Cloudmax 匯智盡力製作本說明文件其正確性,但不擔保本文件無任何瑕疵,亦不為使用本 說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。若對本文件有任何疑問與建 議,可利用下方資訊與我們聯繫:

電話:+886-2-2718-7200

傳真:+886-2-2718-1922

信箱:service@cloudmax.com.tw



 • 25 號 3 樓
 t. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-1922
 f. +886-2-2718-1922
 106073, Taiwan (R.O.C.)

# 目錄

— 、	選擇產生 CSR 檔案方式1
	1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用)1
	2. 透過 IIS 伺服器產生 (申請 GlobalSign 使用)2
_`	安裝前注意事項6
$\equiv$	數位憑證安裝前準備確認事項7
四、	選擇安裝方式9
	1. CSR 透過線上 OpenSSL 生成 (操作僅限申請 GeoTrust)9
	2. CSR 透過 IIS 伺服器產生13
	3. 匯入中繼憑證檔案15
五、	檢查憑證安裝是否正確21
六、	備份數位憑證



 匯智 資訊股份有限公司

 106073 台北市大安區仁愛路四段 25 號 3 樓
 t. +886-2-2718-7200

 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City

 106073, Taiwan (R.O.C.)

# 一、選擇產生 CSR 檔案方式

CSR 檔案為提供給憑證中心驗證的檔案,透過此 CSR 檔案憑證中心將會簽發 CER 檔案; 而產生 CSR 檔案的同時會一併會產出 KEY 檔案,而這三個檔案為互相匹配憑證才可正常運行。

## 1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用)

若您為申請 GeoTrust 的憑證,我們建議您可以直接使用我們的 OpenSSL 線上產生工具, 來快速產生 CSR 檔,並且將所產生出來的 CSR 檔案提交給匯智,一併產出的 KRY 檔案請 您務必儲存,以利後續憑證安裝過程順利。

GeoTrust 線上生成 CSR 工具:

http://geotrust.cloudmax.com.tw/OpenSSL/CreateCSR.asp

1



 • 25 號 3 樓
 t. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-1922
 f. +886-2-2718-1922
 106073, Taiwan (R.O.C.)

## 2. 透過 IIS 伺服器產生 (申請 GlobalSign 使用)

若您為申請 GlobalSign 的憑證,我們建議您直接於 IIS 伺服器上產生 CSR 的資訊,產生的

步驟如下表:

1.

進入 IIS 系統 · 針對要置入憑證的網站點選滑鼠右鍵/屬性

🥘 Internet 信息服务(	IIS)管理器			_ 🗆 🗙
⑤ 文件(E) 操作(A)	查看(V) 窗口	コ( <u>W)</u> 帮助(H)		_ 8 ×
(+ -> 🗈 🖬 🗡		월 🖬   是   ▶ ■		
Mainternet 信息服务 □ JDTSERVER003( □ JDTSERVER003( □ JDTSERVER003) □ DTSERVER003( □ DTSERVER003( □ DTSERVER003) □ DTSERVER003( □ DTSERVER03( □ DTSERVER03(	本地计算机) 资源管理器( 打开( <u>O</u> ) 权限(I) 浏览(B)	名称 aspnet_client iisstart.htm pagerror.gif E)	路径	状况
	启动(5) 停止(P) 暂停(A) 新建(N)			
	所有任务(K) 查看(V) 从这里创建1			
	删除( <u>D</u> ) 重命名( <u>M</u> ) 刷新(E) 导出列表(L)			
	属性( <u>R</u> ) 帮助( <u>H</u> )			
	舌框。	,		

2

於目錄安全性中點選伺服器憑證





106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

3 選擇新建憑證

IIS 证书向导	×
<b>服务器证书</b> 以下是为网站分配证书的方法。	
选择此网站使用的方法: ⑦ 新建证书 ① . ⑦ 分配现有证书 ④ . ⑦ 从恋钥管理器备份文件导入证书 ② . ⑦ 从 .pfx 文件导入证书 ③ . ⑦ 将远程服务器站点的证书复制或移动到此站点 ① .	
< 上一歩 (2) 下一歩 (2) >	

4

輸入您容易記憶的名稱(建議直接輸入網域)

特別留意:密鑰長度目前憑證中心僅頒發 2048 的憑證資訊。

IIS	<b>业</b> 书内书	
4	3条和安全性设置 新证书必须具有名称和特定的位长。	>
	输入新证书的名称。此名称应易于引用和记忆。	
	globalsign. com	
ļ.	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 低。	
1	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 低。 位长 (近): 2048	
	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 位长 (d): 2048 [] 选择证书的加密服务提供程序 (CSP) (g)	
	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 位长 (L): 2048 「选择证书的加密服务提供程序 (CSP) (L)	
	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 位长 (U): 2048 [7] 选择证书的加密服务提供程序 (CSP) (P)	
1	密钥的位长决定了证书的加密程度。位长越长,安全性越高。然而,位长过长将使性能降低。 位长 创: 2048 厂 选择证书的加密服务提供程序 (CSP) ①	



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da'an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

### 依照您的實際狀況,填入申請單位與部門名稱

IIS 证书向导	×
<b>单位信息</b> 证书必须包含您单位的相关信息,以便与其他单位的证书区分开。	
选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。	1
如需详细信息,请参阅证书颁发机构的网站。	
单位 @):	
GlobalSign China Co., Ltd.	
<b>部</b> 门 (1):	
IT Dept.	
<上一步®) (下一步®) (下一步®) (下一步®)	取消

#### 6

5

### 憑證申請的網域名稱

15 矿书向导	×
<b>站点公用名称</b> 站点公用名称是其完全合格的域名。	<b>E</b>
输入站点的公用名称。如果服务器位于 Internet 上,应使用有效的 位于 Intranet 上,可以使用计算机的 NetBIOS 名。	)DWS 名。如果服务器
如果公用名称发生变化,则需要获取新证书。	
公用名称 (C):	
cn.globalsign.com	
< 上一步 (8) 「	下一步(11) > 取消



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da'an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

7

依照您的伺服器所在地而填寫資訊

115 证书 <b>肖</b> 导	×
<b>境理信息</b> 证书颁发机构要求下列地理信息。	
国家(地区)(2):	
(中国) -	
省/自治区(2):	
Shanghai	•
市县 (L):	
Shanghai	•
Shanghai 省/自治区和市县必须是完整的官方名称,且不能包含缩写。	•
< 上一步 @) (下一步 @)	<u>》</u> 取消

8

確認 CSR 產出位置

书请求文件名		18
以指定的文件名将证书请求保存	子为艾本文件。	Ű.
输入证书请求的文件名。		
文件名 (E):		
c:\certreq.txt		浏览( <u>R</u> )

\*若透過 IIS 產生 CSR 檔案,KEY 檔案將會直接儲存於此 IIS 伺服器中。



 匯智 資訊股份有限公司

 106073 台北市大安區仁愛路四段 25 號 3 樓
 t. +886-2-2718-7200

 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City

 106073, Taiwan (R.O.C.)

# 二、安裝前注意事項

數位憑證是由私密金鑰(private key)與公開金鑰(public key)兩個部分組成,在進行安裝

及使用數位憑證前,須將私密金鑰與公開金鑰檔案放置於伺服器可讀取之儲存區中。

依伺服器網路環境不同而實際需求各異,以下列出安裝時常見忽略的狀況:

·伺服器是否正常連上 Internet?

·HTTPS 協定之通訊埠是否開啟1?

·部分狀況下,伺服器需要額外的固定 IP<sup>2</sup>支援;此時需調整網址之 A 紀錄<sup>3</sup>。

·與伺服器串連的網路設備通訊埠的狀態是否設定完成4?

若無法確認網路環境,或您非相關設備或服務的權限擁有者,應與設備、系統所屬管理員或

該服務、設備提供商諮詢及確認。

安裝過程中,因操作錯誤或其他不可預期因素,可能導致系統資料異常、毀損,請在系統更 動前,將重要系統及資料進行備份。

<sup>&</sup>lt;sup>1</sup> HTTPS 協定預設使用 Port 443,但使用者可依實際狀況進行調整。

<sup>&</sup>lt;sup>2</sup>多個網站共用同一台伺服器的情況下(如虛擬主機),需要利用額外的固定 IP 以解決通訊埠不足的問題。

<sup>&</sup>lt;sup>3</sup> 須注意您是否擁有修改 DNS(Domain Name Service) Server 權限,且 DNS 紀錄修改需要生效時間。

<sup>&</sup>lt;sup>4</sup> 例如防火牆、負載平衡裝置、代理伺服器等,可能須調整規則、開啟通訊埠,甚至部分設備也需要安裝、支援數位憑證。



 匯智 資訊股份有限公司

 106073 台北市大安區仁愛路四段 25 號 3 樓
 t. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-1922

 106073, Taiwan (R.O.C.)

# 三、數位憑證安裝前準備確認事項

憑證核發成功後,指定的 Email 信箱將可收到國外認證中心發的英文通知信與匯智的中文通

知信,而信中將會提供憑證中心所簽屬的 CER 檔案與憑證中繼憑證檔案,這些資訊將以純

文字的方式來顯示,請您進行以下的動作確認所頒發的憑證資訊是否正確。

# 1 請協助查看憑證資訊檔案文本資料中



2

請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-

----』)



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

3 開啟純文字檔案,貼上您所複製的資訊



- 4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer) · 所見的圖示將會變成 📭
- 5 請點擊憑證檔案,確認憑證網域、簽發者單位、有效期間是否為正常資訊



# 四、選擇安裝方式

上述的憑證資訊確認完畢後,我們即將開始要把憑證安裝於伺服器當中,於第一大項時,我 們有介紹兩種因申請不同憑證廠商而建議的生成方式,請參考以下的資訊來完成憑證安裝動 作。

# 1. CSR 透過線上 OpenSSL 生成 (操作僅限申請 GeoTrust)

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)以及 KEY 的文本資訊(當時透過 OpenSSL 或是線上生成工具時一併產生的 KEY 檔案),請準備好兩項的資訊, 連入 Geotrust PFX 線上合成工具,並且依照網頁指示完成 PFX 檔案的匯出。

GeoTrust PFX 線上合成工具:http://geotrust.cloudmax.com.tw/OpenSSL/CreatePFX.asp

\* 僅限申請 GeoTrust 憑證適用,因線上合成工具會一併合成 GeoTrust 對應的中繼憑證。



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.

進入 IIS 系統,針對要置入憑證的網站點選滑鼠右鍵/屬性

🐚 Internet 信息服务(II	5)管理器					- 🗆 ×
⑤ 文件(E) 操作(A) ∃	査看(⊻) 窗口	( <u>W</u> ) 帮助(	(H)			_ 8 ×
🗢 🤿 🗈 💽 🗙	1 d B	2 🖪 🖇				
🐚 Internet 信息服务		名称		路径	状况	
□ 刘 DOTSERVER003(本 〒	地计算机)	🥥 aspnet_c	:lient fm			
白 一 网站		pagerror	.gif			
世 💓 🔤 🔤 🗄	资源管理器(E	)				
	打开( <u>0</u> ) 权限(I)					
	浏览(B)					
	启动(5)					
	停止( <u>P</u> ) 暂停(A)					
-	新建(N)	•				
	所有任务(K)	•				
	查看(⊻)	•				
	从这里创建窗					
	删除( <u>D</u> ) 素会名(M)					
	里印·石(凹) 刷新(F)					
	导出列表(L)					
	属性( <u>R</u> )					
	帮助(H)					E
打开当前选择的属性对话	E.					

2

於目錄安全性中點選伺服器憑證





106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da'an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

#### 選擇從 .PFX 文件導入憑證

IIS 憑證精靈	×
<b>伺服器蒸查</b> 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:	
C 建立新憑證(C)。	
○指派已有的憑證(▲)。	
C 從金鑰管理員備份檔案匯入憑證(O)。	
● 従_pfx 檔案匯人態證(M)	
() 從速碼同服器網站復興或移動遷證到此網站(型)	
<u>_&lt;上一步</u> 图】	下一步创> 取消

4

3

選找到剛剛所合成完畢的 PFX 檔案資訊,同時將此 PFX 檔案設定為可匯出

IIS 责意精量	X
<b>隆入蒸設</b> 您可以從 PFX 襠匯入憑證。	
諸輸入包含憑證的檔案名稱及路徑。 路徑及檔案名稱(P):	0
C:\Documents and Settings\Administrator\桌面\wis-	ajorkxg6pi_w3% 瀏覽(R)
指定在匯入後,匯入的應證是否應標示為可匯出 較高的安全風險,不過,它可允許應證匯出到格 「將憑證標示為可匯出(M)	a。將憑證標示為可匯出將具有 案進行備份。
	0
<u>&lt;</u> ±-	-步图 下



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da'an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

#### 5

HTTPS 預設使用 443 port,請依照實際狀況來進行設定

畫諸鑑選 2II	×
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(止):	
	上一步图 下一步图

憑證安裝完成,您可以直接跳到 五、檢查憑證安裝是否正確



 • 25 號 3 樓
 t. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-1922
 f. +886-2-2718-1922
 106073, Taiwan (R.O.C.)

### 2. CSR 透過 IIS 伺服器產生

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件),因您的 CSR 由 IIS 伺服器直接產生,所以 KEY 檔案將會直接保留再 IIS 中,請您依照以下的步驟將簽發下 來的 CER 資訊匯入 IIS 伺服器:

# 1 點選當時執行的站台/內容

<b>復 何際何</b> 路資。	R服務 (IIS) 管理員		
🌀 檔案(E) 🕏	行(A) 檢視(Y) 親窗(W) 説明(H)		_8×
🗢 🔿 🔁 🗉	I 🗙 🗗 🖸 🖳 😫 🖳 🕨	■ 11	
	R服務 2 RX 3 GOF1 (本株 室式集画 部dex.html 室看(2) 開始系統(2) 使用確認(2) 避難(2)	路徑	#X%
	容新(3) 停止(2) 暫停(2) 新增(2) 所有工作(2)		
	校視(型) ▶ 従這裡新増視窗( <u>Ψ</u> )		
▲ 開啓目前選擇的	開除① 重新命名(M) 重新整理(P) 匯出清單①	<u> </u>	<b>)</b>
0	内容(R)		
	<b>呪</b> 朔( <u>H</u> )		
2		<u> </u>	

- 目錄安全設定 / 伺服器憑證

ssl.wis.com.t	w 內容			?	×
網站 目錄3		ISAPI 篩選器 HTTP 標	子   主目: 頭	錄 │ 文件 自訂錯誤	
験證及存り	取控制 啓用匿名存取 證方法。	,並編輯這個資源		編輯(正)	
	網域名稱限制 使用 IP 位址或 或拒絕到這個貨	網際網路網域名書 資源的存取。	ı	編輯(])	
一安全通訊	當存取這個資源 用用戶端憑證	原時使用安全通訊 。		₩器態證©)] 親憑證(Y) 編輯(D)	
	<b>œ</b>	定 _ 取消	1 _ 套用	(A)   説明	



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

#### 3 處理擱置要求及安裝憑證

<b>畫諸憲選 211</b>	×
<b>蜀<b>置的燕證要求</b> 擱置的應證要求是指憑證授權未回應的要求。</b>	
有擱置的憑證要求。您要如何處理?	
☞ 處理擱置要求及安裝憑證 (2)	
<上一步④ 下一步(U) >	取消

4

### 找尋 3. 數位憑證安裝前準備確認事項 所儲存的 CER 檔案 (副檔名為.cer)



#### 5

### HTTPS 預設使用 443 port · 請依照實際狀況來進行設定

IIS 憲證格畫	×
SSL 連接埠 黨這個網站指定 SSL 連接埠。	
這個網站應該使用的 SSL 連接埠(L):	
	步10) > 取消



### 3. 匯入中繼憑證檔案

※ 若您的憑證是使用線上合成的方式匯入,可直接跳過此步驟。

電腦運算能力於近十年內大幅提升,為確保憑證用戶網路資料傳輸安全,各大憑證中心於 2010 年起開始做根憑證 1024 升級為 2048 位元的作業,而舊的瀏覽器因缺少 2048 位元的 根憑證資料,所以需要利用中繼憑證來進行交互驗證,確保於舊版本瀏覽器使用 HTTPS 連 線時,不會出現錯誤或警告訊息,請您依照以下的步驟來完成中繼憑證匯入動作:

1 請協助查看憑證資訊檔案文本資料中「中繼憑證」



z 請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END

CERTIFICATE-----』)

3 開啟純文字檔案·貼上您所複製的資訊



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922



4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer),所見的圖示將會變成

-

開始 > 執行(R), 輸入"mmc"

6

7

5

於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元

檔案①	執行(点)	檢視(型)	我的最爱(0)
間新楷	END		Ctrl+N
開啓護	HTO)		Ctrl+O
儲存© 另存新	D i榆()		Ctrl+S
新增用 通項在	3除嵌入式 )	管理單元企	D Cul+M
1C:\W	INDOWS'.	\inetsrv\iis.r	nac
2 C \W	INDOWS'.	.\compmgm	t.mac
a source			

點選『新增』·然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/新

增



106073 台北市大安區仁愛路四段 25 號 3 樓 <sup>t.</sup> 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

t. +886-2-2718-7200
f. +886-2-2718-1922

請使用這個畫面從主控台新增或移時獨	可用的海立徐人式管理單元:	1.000000	
將後入或管理單元 🔁 主疫台根目錄 加入 (G):	<ul> <li>※入式管理單元</li> <li>◆ 電話語音</li> <li>◆ 相撲道出工具</li> <li>● 新球準約結済訊服務(IIS)管理員</li> <li>◆ 新球準約結済訊服務(IAS)</li> <li>◆ 新球準約結接服務(IAS)</li> <li>◆ 新球準約結接線路路(IAS)</li> <li>● 新球準約</li> <li>● 新球準約</li> <li>● 新球準約</li> <li>● 新球準約</li> </ul>	解決のの行くCorporation Microsoft Corp, Exsection Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation Microsoft Corporation	
描述 新增(D)	描述 恭媛嵌入式管理單元線包造發電腦或	服務的應證存放內容 ·	

8

選擇『電腦帳戶』 然後『下一步』





106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da'an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

選擇『本機電腦(執行這個主控台的電腦)』,然後完成

<ul> <li>(*)</li></ul>	國主控合的電腦)(1)	12/09 (D)
□ 九許對選取的電影 (型)	識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

10

9

完成後,在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示,點

選『確定』完成憑證管理單元新增程序

The part of the second second second	可用的漂立嵌入式装建算示		
國使用這國黨面從主致目對電影特許導 將於人式管理單元 至 主控台根目錄 加入(3)	<ul> <li>● 電話語量第二</li> <li>● 電話語音</li> <li>● 網球運輸工具</li> <li>● 網球運輸</li> <li>● 網球運輸</li> <li>● 網球運輸結論服務 (IIS) 管理員</li> <li>● 網球網結論證服務 (IAS)</li> <li>● 網球網結論證服務 (IAS)</li> <li>● 週球機能資訊服務 (IS)</li> <li>● 週球機能資訊服務 (IS)</li> </ul>	旅行のの行 Corporation Microsoft Corporation	
- 構造 新聞の二	推进 参加收入式管理單元線並設置電磁域	服務的泰雄存放内容。	2



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

11

開啟憑證主控台,在『中繼憑證授權』點選右鍵,『所有工作 > 匯入』。系統執行

憑證匯入精靈歡迎畫面後,『下一步』

************************************	(很電腦)\中醫憑證授	ŧ		
主控台根目錄 ● ● ● 個人 ● ● 個人 ● ● 信任的根憑證 ● ● 企業信任	尋找憑證(1)	0		物件類型 一 憑證撤銷清單 一 憑證
□ 憑證	所有工作低)	•	尋找憑證(	N
<ul> <li>■ ○ 沒有信任的愚</li> <li>■ ○ 第三方根憑證</li> </ul>	檢視(⊻) 従這裡新增親窗(₩)	·	匯入①	
□ □ ▽信比的人	新工作台檢視(I)			
⊕- 🧰 SPC	重新整理(E) 匯出清單(L)			
	說明田			

12

, 用『瀏覽』選擇下載的中繼憑證檔案位置·然後點選『下一步』

檔案名稱(E):			_
C:\Documents and	Settings/Administrator/J#	(fili)/cert.cer	瀏覽(R)
請注意: 您可以將	數圖憑證用以下的格式	式存放在同一個檔案	ф: <b>Т</b>
個人資訊交換-	PKCS #12 (PFX, P12)		
密碼編譯訊息圖	法標準 - PKCS #7 12	₫ (p7b)	
Microsoft 序列目	體存放 (.sst)		



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

13 選擇『將所有憑證放入以下的存放區』·憑證存放區為預設的『中繼憑證授權』·然後

『下一步』

Windows 會自動	選擇一個憑證存放	E,您也可以爲愚	體指定存放位置	•
○ 自動根據	影體類型來選取憑證	會存放區(1)		_
<ul> <li>將所有憑認</li> </ul>	量放入以下的存放	5 (P)		
憑證存放	<u>.</u>			
中継徳證	授權		3	BC(R)
			-	

憑證安裝完成,您可以直接跳到 五、檢查憑證安裝是否正確



匯智 資訊股份有限公司 106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

# 五、檢查憑證安裝是否正確

您可以透過此驗證工具來確認憑證是否已經正確掛載:

GeoTrust : http://geotrust.cloudmax.com.tw/OpenSSL/checkservercert.asp

GlobalSign : https://globalsign.ssllabs.com/

# 六、備份數位憑證

匯智數位憑證在憑證有效期間內,提供憑證重置(Reissue)與更新的服務。不過重置過程需 與新申請憑證時相同,必須再次產生私密金鑰與 CSR、驗證、簽發公開金鑰等程序後,才 可再取得憑證。將可能耽誤寶貴的系統復原時間。基於資安考量,建議系統管理者將數位憑 證進行備份。備份的方式如下:

- 1 開始 > 執行(R), 輸入"mmc"
  - \* 若已經有看到憑證項目請直接跳到本步驟 7
- 2 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元

富案①	執行(点)	檢視(型)	我的最爱(0)
間新檔	RN		Ctrl+N
開啓舊	标()		Ctrl+O
场任心	福山		CERHS
新增/档 通項@	除嵌入式	管理單元企	0 Ctrl+M
1 C:\WI	INDOWS\.	.\inetsrv\iis.n	nsc
-	MD-G HIM	A	



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

點選『新增』·然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/新

#### 增

3



#### 4







6

匯智 資訊股份有限公司

106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

5 選擇『本機電腦(執行這個主控台的電腦)』,然後完成

● 本標電腦 (執行	這個主控台的電腦)(正	E		
○ 另一台電腦(点):		7	送頭(	R)
「九許對選取的費 (型)	且腦進行從命令列所看	時間的提更・這只在您	儲存主控台後才葡	通用
		1		

完成後,在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示,點

選『確定』完成憑證管理單元新增程序



23



7

匯智 資訊股份有限公司

106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

開啟憑證主控台,點選『個人 > 憑證』,於工作室窗選定欲備份的憑證後,右鍵,

### 『所有工作 > 匯出』



於憑證精靈歡迎畫面點選『下一步>』後,選擇『是,匯出私密金鑰』,然後『下

一步』

出私密金输您可以選擇將私密金鑰與憑證一書	<b>坦</b> 匯出 ∘
私密金論受到密碼的保護。如果が 一頁輸入密碼。 忽想將私密金論與憑證一起匯出? ・ 是,匯出私密金論(文)	您要將私密金鑰與憑證一起匯出,您必須在下 ,
C 否,不要匯出私密金鑰Q	



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

9

「匯出檔案格式」預設為「個人資訊交換-PKCS#12(.PFX)(P)」,請將『如果可能的

話,包含憑證路徑中的所有憑證』

出 <b>檔案</b> 憑證可	<b>格式</b> J以用多種檔案格式匯出。
諸選取	x您想要使用的格式:
С	DER 編碼三位元 X 509 (CER)(D)
С	Base-64 編碼 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,包含憑證路徑中的所有憑證①
٩	個人資訊交換 - PKCS #12 (PFX) (P)
	▶ 如果可能的話,包含憑證路徑中的所有憑證(①)
L	✓ 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)

#### 10

# Ⅳ 用『瀏覽』指定檔案匯出位置及名稱→然後『下一步(N)』

證匯出精靈	
<b>要匯出的檔案</b> 諸指定您要匯出的檔案名稱	
描案名稱 (E)·	
C:/certification.pfx	瀏覽(E)
	· · · ·
	<u>〈上一步⊞】 【下一步₪〉</u> 取消



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

11 在憑證匯出精靈中自行設定設定 6 碼以上之保護密碼 · 『密碼(P)』及『確認密碼

(C)』欄位需相同

. L 6779	女王庄:赵妃。	电视用位响环器	创动农本细。		
輸入	並確認密碼。			_	
密	碼(里):				
1	okokokok				
碷	認密碼( <u>C</u> ):				
	otototote				
. L				_	
				· · ·	
				- A	

作視窗

<b>燕證匯出</b> 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 理出金編 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─步(E) 完成 <b>●</b> 取消