

电子证书(伺服器)用户指南

Microsoft IIS 5.0 / 6.0 适用

仅适用于 SHA-1 电子证书 (伺服器)

修订日期: 2014年12月

目錄

A.	电子证书(伺服器)申请人指引	2
	新申请	3
	续期申请	4
B.	产生证书签署要求(CSR)	5
	建立新伺服器证书	7
	更新目前的伺服器证书	
C.	提交证书签署要求(CSR)	16
D.	安装香港邮政根源证书	20
	安装 "Hongkong Post e-Cert CA 1 - 10" 根源证书	23
	安装"Hongkong Post Root CA 1"根源证书	
E.	安装伺服器证书	
F.	备份密码匙	
	在 IIS 5.0 上备份密码匙	
	在 IIS 6.0 上备份密码匙	40
G.	还原密码匙	45
	在 IIS 5.0 上还原密码匙	45
	在 IIS 6.0 上还原密码匙	51

A. 电子证书(伺服器)申请人指引

香港邮政核证机关在收到及批核电子证书(伺服器)申请后,会向申请人(即获授权代表)发出主旨为"Submission of Certificate Signing Request (CSR)"的电邮,要求申请人到香港邮政核证机关的网站提交 CSR。

本用户指南旨在提供参考给电子证书(伺服器)申请人如何在 Windows 2000 / 2003 上的 Microsoft IIS 5.0 / 6.0 产生配对密码匙和证书签署要求(CSR)的详细步骤。包含公匙的 CSR 将会提交到香港邮政核证机关以作证书签署。

如阁下在证书签发后遗失密码匙,您将不能安装或使用该证书。因此强烈建议阁下于提交证书签署要求(CSR)前及完成安装伺服器证书后均为密码匙进行备份。有关备份及还原密码匙的方法,请参阅以下部分的详细步骤:

F.	备份密码匙	35
G.	还原密码匙	45

新申请

如阁下是首次申请电子证书(伺服器),请参阅以下部分的详细步骤:

B.	产生证书签署要求(CSR)	5
	建立新伺服器证书	7
C.	提交证书签署要求(CSR)	16
D.	安装香港邮政根源证书	20
	安装"Hongkong Post e-Cert CA 1 - 10"根源证书	23
	安装"Hongkong Post Root CA 1"根源证书	26
E.	安装伺服器证书	29

续期申请

如阁下正更新目前伺服器上的电子证书(伺服器),请参阅以下部分的详细步骤:

B.	产生证书签署要求(CSR)	5
	更新目前的伺服器证书	13
C.	提交证书签署要求(CSR)	16
E.	安装伺服器证书	

B. 产生证书签署要求(CSR)

- 按 [开始] > [所有程式] / [程式集] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] / [Internet 服务管理员]來启动网际网路资讯服务 (IIS) 管理员。
- 2. 在 [网际网路资讯服务 (IIS) 管理员] / [Internet Information Services]视 窗内,展开[网站]及选择您的网站,以滑鼠右键按一下,然后按[内容]。

🐚 網際網路資訊服務 (IIS) 管理員		_ 🗆 🗵
🗐 檔案(F) 執行(A) 檢視(V) 視窗(<u>₩)</u> 說明(<u>H</u>)	_ ð ×
	፻ 🖬 💂 ▶ ■ 🗉	
 ● 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	A稱 iisstart.htm pagemor.gif () () 朝窗(W) M) E) L)	· 北次
。 爲目前的選取項目開啓內容		

3. 在[目錄安全设定]索引标签内,按一下[伺服器凭证]。

預設的網站 內容	<u>? ×</u>
網站 效能 ISAPI 篩選器 目錄安全設定 HTTP 標頭	主目錄 文件
- 驗證及存取控制	
资用运行行取,亚编辑运回直录印3號 證方法。	[[[]][[]][[]][[]][[]][[]][[]][[]][[]][
□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。	<u>,</u>
	编輯①
安全通訊	
當存取這個資源時使用安全通訊亚書> 	伺服器憑證(3)
	檢視憑證(型)
	編輯(D)
確定 取消	套用(<u>A</u>) 說明

建立新伺服器证书

注意:如阁下正更新目前的伺服器证书,请跳到步骤14。

4. 在[网页伺服器凭证精靈]内,按[下一步]继续。

教迎使用網頁伺服器憑證精霊。 🛛 🔀		
	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。	
	諸按 [下一步] 來繼續。	
	<上一步图 下一步 (17).3 取消	

5. 选择[建立新凭证], 然后按[下一步]。

IIS 憑證積量	×
伺服器整證 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:	
● 建立新憑證(C)。	
○ 指派已有的憑證(点)。	
○ 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(?)	
<上一步(B) (下一步(M)>)	取消

6. 选择[准备要求,但于稍后传送],然后按[下一步]。

IIS 憑證精靈	×
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(P) ○ 立即傳送要求到線上憑證授權(3) 	
<上一步(B) 下一步(B) 下一步(B))]]	取消

输入新凭证名称 (或接受预设) 及选择 2048 作为密码匙的[位元长 度], 然后按[下一步]。

注意:小于 2048 位元的密码匙或未能提供足够保密程度,相反大于 2048 位元有可能与某些浏览器不兼容。建议选择长度为 2048 位元的密码匙,从而提供较佳的保密程度。

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):	
<u> </u>	
加密金鑰的位元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): 2048 🔽 🔽	
□ 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(A) > 取	消

8. 输入您的公司名称及单位,然后按[下一步]。

IIS 憑着蓋	×
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,諸與憑證授權單位的網站聯絡。	
公司(<u>O</u>):	
My Organization	
單位(U):	
My Organizational Unit	
<上一步⊞ 下一步刨>	取消

9. 输入您网站的一般名称(即伺服器名称), 然后按[下一步]。

注意:若申请电子证书(伺服器)"多域版",请在「一般名称」一欄中, 输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同 的登记伺服器名称。而「电子证书主体别名内的额外伺服器名称」,则无需 在产生证书签署要求(*CSR*)过程中输入,香港邮政核证机关系统 在签发证 书时,会根据申请表格所申请的资料自动填写。

若申请电子证书(伺服器) "通用版",请在「一般名称」一欄中, 输入与申请表格中所填写的「有通配符的电子证书伺服器名称」相同的 登记伺服器名称(伺服器名称的最左部份需包括有通配符「*」的部 份)。例如 *.myserver.com。

IIS 憲證精畫
您有我的一般名稱 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,諸用有效的 DNS 名稱。 若伺服器在近端内部網路上,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。
一般名稱(<u>C</u>):
www.myserver.com
< 上一步 (B) 下一步 (M) > 取消

 选择 "HK (香港特别行政区)" 作为[国家(地区)], 输入 "Hong Kong" 作为[省/州]/[州/省] 及[城市/位置], 然后按[下一步]。

IIS 憑意精靈	×
地理資訊 此憑證授權單位要求下列地理的資訊。	
國家 (地區)(C): HK (香港特別行政區 ▼	
省/州 ③): Hong Kong	•
城市/位置(L):	
Hong Kong	-
必須輸入 [省/州] 和 [城市/位置],須為正式名稱且不可含縮寫。	
< 上一步图 下一步砚 >	取消

11. 输入凭证要求的档案名称,然后按[下一步]。

IIS 憲證精畫	×
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(F):	
c:/certreg.txt	瀏覽(<u>R</u>)
<上一步B) [下一:	步(N)> 取消

12. 按[下一步]。

注意:请确定于「发给」一欄显示正确的登记域名(即伺服器名称)及「国家(地区)」一欄显示「HK」。

IIS 憑證精靈		×
要求的檔案摘要 您已經選擇建立要求檔案。		
若要建立下列要求,請按[下	一步]。	
檔案名稱: c:\certreq.txt		
您的要求包含下列資訊:		
發給 好記的名稱 國家/地區 州 / 省 城市 公司 單位	www.myserver.com 預設的網站 HK Hong Kong Hong Kong My Organization My Organizational Unit	
	<上一步(B) (下一步(M))>	取消

13. 按[完成]來关闭精靈。

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:/certreg.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。 諸重新啓動此 送給您含您的新憑證的回應檔案。 諸重新啓動此 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	

更新目前的伺服器证书



14. 在[网页伺服器凭证精靈]内,按[下一步]继续。

15. 选择[更新目前的凭证], 然后按[下一步]。

IIS 憲證精畫	×
修改目前的憲證指派 目前安裝在此網站的憑證。	
您想要如何處理目前安裝的憑證?	
○ 更新目前的憑證(W)。	
○ 移除目前的憑證(图)。	
○ 取代目前的憑證(点)。	
○ 匯出目前的憑證到 .pfx 檔案(盔)	
○ 複製或移動目前的憑證到遠端伺服器網站(C)	
<上一步(B) 下一步(A) >	取消

16. 选择[准备要求, 但于稍后传送] / [准备要求, 但稍后再传送], 然后按[下 一步]。



17. 输入凭证要求的档案名称, 然后按[下一步]。

IIS 憲憲精靈	×
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。	
請輸入檔案名稱給憑證要求。	
檔案名稱(F):	
s:\certreg.bxt 瀏覽(R)	
<上一步(B) 下一步(N) >	取消

18. 按[下一步]。

注意:请确定于「发给」一欄显示正确的登记域名(即伺服器名称)及「国家(地区)」一欄显示「HK」。

IIS 憲證精靈		×
要求檔案摘要 您已經選擇建立要求檔案。		
若要建立下列要求,請按 [下	`一步]。	
檔案名稱: c:\certreq.txt		
您的要求包含下列資訊:		
發給 好記的名稱 國家地區 公司 單位	www.myserver.com 預設的網站 HK Hongkong Post e-Cert (Server) 0000812107	
	<上一步图 下一步 (下一步 (1) >)	取消

19. 按[完成]來关闭精靈。

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楮靈。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。 諸重新啓動此 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	

C. 提交证书签署要求(CSR)

1. 在香港邮政核证机关发出主旨为 "Submission of Certificate Signing Request (CSR)" 的电邮内按一下超連结以連线至香港邮政核证机关的 网站。



 输入[伺服器名称],印于密码信封面的[參考编号](九位數字)及印于密码 信封内的[电子证书密码](十六位數字),然后按[提交]。

そ Hongkong Post e-Cert 香港郵政電子核證	The solution for e-Security	
		▲ 歡迎自製電子證書
		電子證書 (伺服器)
	登記人在本表格內提供的個人資料, 香定, 要求查詢及更正其個人資料。登記 郵政個人資料(私隱)政策整明及收集個/	港郵政將會用作處理有關的申請事宜。登記人有權根據【個人資料(私膳)條例】的規 人查閱資料的權利,包括獲取在本表格內所提供有關的個人資料。其他詳情,請參閱香港 人資料整明。
Hongkong Post		
香港郵政 Linking people Delivering business	伺服器名稱: www.myserver.c	om
集心剤 単白機	請填寫以下有關電子證書密碼信封的資	资料 :
	参考編號:	000214379
	(印於密碼信封面;九位數字)	
	電子證書密碼:	•••••
	(十六位數字密碼內的空白地方無須填寫))
		[提交] (重設)
		1
	2007 © 重要告示 私隱政策	

 按[提交]确认申请资料。(如发现资料不正确,请聯络香港邮政核证机 关。)

そ Hongkong Post e-Cert 香港郵政電子核證	The solution	for e-Security		
• e : m m e	<u>A</u> A A	## #1	X迎自製電子證書 子證書(伺服器)	_
Exercise and the second		登記人資料 伺服器名稱: 翰外伺服器名稱: 翰外伺服器名稱數里: 證書類型: 機構名稱: 部門名稱 / 分行名稱: 商業登記證: 公司註冊證 / 公司登記證: 其他註冊證明文件: 有關所申請的電子證書的資料 有效期 (月):	www.myserver.com www.myserver2.com 1 電子證書(伺服器)"多域版" My Organization 1234567890123456 12345678	
		此頁用以確認申請資料,如以上資 [提交]	料正確,請按[提交] 鍵繼續: 拒絕 返回上頁	

4. 用文字编辑器(例如:记事本)开启早前产生的证书签署要求(CSR)及复制全部内容包括 "-----BEGIN NEW CERTIFICATE REQUEST-----"及 "-----END NEW CERTIFICATE REQUEST-----"。(您可參考 B 部的步骤 11 或步骤 17 的凭证要求档案的位置。)

D certreg - 記事本		X
檔案(F) 編輯(E) 格式(O) 檢視(Y) 說明(H)		
BEGIN NEW CERTIFICATE REQUEST MIIDZZCCATACAQAwgYsxCZAJBGNVBAYTAKhLMRIWEAYDVQQIEw]Ib25nIEtvbmcX EjAQBgNvBACTCUhvbmcgS29uZZEYMBYGA1UEChMPTxkgT3JnYw5pemF0aw9uMR&w HQYDVQLEXZNeSBPcmdhbml6YxRpb25hbCBvbmlOMRkwFwYDVQQDExB3d3cubX1z ZXJ2ZXIuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnaFeC/NK7uHak 6NoLDn1avj9p4Gk3uRKESYS9GJJ3R5z167oNUh3ohZEF+LRKW20jDQvDN4X3UcM2 p]3NBG/vJpv30P2Nx/pg3MKo24CZsmJIDJQLMawNEKDZ9VgL86aSFN2F+gFbjY6Z 3nRM4FW89FCPDK+dxXl5iHHv10MniwUDAQABOIIBmTAaBgorBgEEAYI3DQIDMQwW CjUUMi4ZNZkwLjIwewYKKWYBBAGCNWIBDjFtMGswDgYDVR0PAQH/BAQDAgTMMEQG CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvCNAWICAgCAMA4GCCqGSIb3DQMEAgIAgDAH BgUrDgMCBZAKBggqhkiG9w0DBZATBgNVHSUEDDAKBggrBgEFBQCDATCB/QYKKwYB BAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBZAG8AZgB0ACAAUgBTAEEAIABT AEMAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		
	>	11 ×

5. 在方格内贴上内容,然后按[提交]。

そ Hongkong Post e-Cert 香港郵政電子核證	The solution for e-S	Security	
·►■■■■	<u>A</u> A A	歡迎自製電子證書 電子證書(伺服器)	~
	諸注意,由20 有RSA密碼匙長 詳情請參關有[12年12月1日起,香港郵政核證機關只會簽發RSA密碼匙長度為2048位元的電子證書 1度為2048位元的「簽發電子證書要求」(Certificate Signing Request, CSR) 朝公告。	(伺服器)。只 才會被接受。
Flongkong Post 香港學政	請複製「簽發i 面的方格中,	電子資書要求」(Certificate Signing Request, CSR)(已被base64 编碼的PH 並按[提交]建題鏡。	CCS#10)於下
Linking people bitmenting balances (# 40 per people people (# 20 people		<pre>MIICUDCCAACACAQAevczELAAkcALUEBhACSExexEjAQBqNVBAgTCUhvbmcg529u2zES MIICuDCCAACACAQAevczELAAkcALUEBhACSExexEjAQBqNVBAgTCUhvbmcg529u2zES BMGGAUEBANSG9u2yELAStMSEHWVDVQCKEAkJDnRlcmSldCSqCSED3DQEB AQUAAHBDwAwqgEKAoIBAQDWOGFUJKqhNuWerAMwdfkLSdJoqXzHJ05zqn/ CTWCQwTOID9FfHbe-domEKLN97a9t+17KV01q3CVESW7/LIQ0H1dKW3KEBXsR LX8-pirXC/e/rwLGA9NVJACjXV3082K02BmzjrgKBtzpVF/h2ppdFyfMnRVHcBR HxcaEnxsucrg/9KEteBPVH/pVDINGCL2X1z858aC2EC1c2CK/jqdCNkE+W6N+ 7fIm9XnzIrgKFV6DAX7/Txt9OThXK1PIa61YQRROASm2hascfkwUEc207peKx2zd LWWPAITvezId89E9jY5J4pJvBnQDF71EVc30FL8wgf6PAgHBAAGADANBgkqhhiG HNPC0+bwL9mZmFB2pppB0GWtwjfCHUBCxXcUhhNc220KKJNwh59fcrcsc3cV 2epNrEtDH1BP2rJoSINDW4UA32drGD/dun1NYf1HUKWT27j517TinmmMNEg7qv5 nlc/MQ63PxLuGJ7r2pc1Tvc2pSFuw5zv6XBWxG51sz7thgLkeqS3pFa+2ghEVsht</pre>	

6. 按[接受证书]确认接受此证书。

				2321014
sieke '	AAA	款迎自製電子證書 電子證書(伺服器)		
	以下為你的電子道書內的資料:-			
ERTIZEN	用戶資料			
*********	個服器名稱 T	www.myserver.com		
	额外得脂器名稱:	www.myserver2.com		
1000	機構名稱 :	My Organization		
	分行/部門名稱:			
Della perde beleving berten	商業臺記證:	1234567890123456		
	公司註冊證 / 公司登記證 1	12345678		
	其他赶南遍明文件 :			
	其他資料(香港蘇政核證機關系統產生)			
	型記人參考編號:	0000821066		
	過書類型 :	Hongkong Post e-Cert (Ser	(ver)	
	發行機關:	Hongkong Post e-Cert CA 1	1 - 10	
	遊畫序號 1	2E4591		
	還書有效日期 :	27/04/2013 to 27/04/2014		
	請該[推奨]確認接受上述讀書,並同意香	潜都政根據電子交易條例的規定將該證書於儲存庫公	4 -	
	(注意: 委選解政政集你的個人資料,只) 及更正你的個人資料。)	會用於處理你的電子語書申請事宜。你有權根據個人家	昇料(私種)幹例的規定・要求査)	51
	接受通知	不接受	101.00	

- 7. 分别下载以下证书:
 - Hongkong Post e-Cert (Server)
 - Hongkong Post e-Cert CA 1 10
 - Hongkong Post Root CA 1

注意: 您也可以从搜寻及下载证书网页下载您的电子证书(伺服器)。 http://www.hongkongpost.gov.hk/sc

注意:如 "Hongkong Post e-Cert CA 1 - 10" 根源证书 及 "Hongkong Post Root CA 1" 根源证书已安装于伺服器上,您只需下载 "Hongkong Post e-Cert (Server)" 证书。



D. 安装香港邮政根源证书

 按 [开始] > [执行], 然后输入 "mmc"及按[确定] 來启动 Microsoft Management Console (MMC), 然后从[档案]选单中选取[新增/移除嵌入 式管理单元]。

論主接台 1	l						[<u> </u>
檔案任	執行(<u>A</u>)	檢視(♡)	我的最愛(①)	視窗(₩)	説明(H)			
開新檔案	案(N)		Ctrl+N					
開啓舊相	當(()		Ctrl+O					
儲存(5)	۳ /۵۵		Ctrl+S					
	≝(<u>A</u>)			咽检想沒有	·····································	 		
新增移	除嵌入式管	管理單元()	<u>1</u>) Ctrl+M		2月1日11月11~			
選項(Ľ). 								
最近使用	用過的檔案	2						
結束(X)								
				-				
讓您能夠從	É嵌入式管	理單元主	空台中新增或移	3除嵌				

2. 按[新增]。

新增/移除嵌入式管理單元		? ×
獨立 延伸		
用這個畫面從主控台中新增或移除獨立的嵌入式管理單元。		
嵌入式管理單元 新增到心:	•	
描述		
	Į	友消

3. 选择[凭证], 然后按[新增]。

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 ▲
警磁碟重組工具	Microsoft Corp, Executi
武 御 磁 碟 管理 日	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
· · · · · · · · · · · · · · · · · · ·	Microsoft Corporation
- 🙀 憑證範本	Microsoft Corporation 🚽
, +#\$\$#	
遇證嵌入式管理單元讓您瀏覽電腦或朋	员務的憑證存放內容。
[新增(A) 關閉(C)

4. 选择[电脑帐户],然后按[下一步]。

憲證嵌入式管理單元
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)
○ 服務帳戶(3)
·
<上一步(B) 下一步(M) > 取消

5. 选择[本机电脑], 然后按[完成]。

選擇	a a construction of the second se	×
	 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):]
	 ○ 另一音电脑(型): □ 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 (₩) 	
	<上一步(B) 完成 取消	

关闭[新增独立嵌入式管理单元]对话框,然后按[确定]关闭[新增/移除嵌入式管理单元]对话框。

安装 "Hongkong Post e-Cert CA 1 - 10" 根源证书

 展开[中继凭证授权]及以滑鼠右键按一下[凭证],然后选择[所有工作]> [汇入]。

🚡 主接台1 - [主接台根目錄\憲式	(本機電腦)\中繼憲證授權\憲證]			<u>_ 8 ×</u>
🚡 檔案(E) 執行(A) 檢視(V)	我的最愛(O) 視窗(W) 說明(H)			_ 8 ×
	😫 💵			
📄 主控台根目錄	● 發給 △	發行者	到期日	
🖻 👹 憑證 (本機電腦)	🔛 Microsoft Windows Hardware Com	Microsoft Root Authority	2002/12/31	代碼簽署, Windows
⊡… 🧰 個人	🔛 Root Agency	Root Agency	2040/1/1	<全部>
🗈 🧰 信任的根憑證授權	📴 VeriSign Class 1 CA Individual Su	Class 1 Public Primary Certification A	2008/5/13	<全部>
□ □ □ 企業信任	📴 VeriSign Class 2 CA - Individual S	Class 2 Public Primary Certification A	2004/1/7	<全部>
□…□□ 中繼憑證授權	🔤 www.verisign.com/CPS Incorp.by	Class 3 Public Primary Certification A	2004/1/8	2.16.840.1.113733.1
四一 受信任的 所有工作低) ▶ 匯入①…			
● ② 沒有信任 檢訊 △				
田 二 第三方根 公司相关的	泪窍(W)			
⊡… 📄 SPC 新工作台檢	視(<u>T</u>)			
重新整理(F)				
)			
說明(<u>H</u>)				
收新课题加入方施				
カマカリに含意なカリノヘキナルス		J		

8. 在[凭证汇入精靈]内,按[下一步]继续。

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。	
	《上一步图】 下一步四) 取消	

 按[浏览]指定早前于 C 部的步骤 7 下载的 "Hongkong Post e-Cert CA 1 -10" 根源证书 (ecert_ca_1-10_pem.crt), 然后按[下一步]。

檔案名稱(E):			
C:\ecert_ca_1-10_p	em.crt		[瀏覽(R)]
諸注意: 您可以將	數個憑證用以下的	的格式存放在同一個格	當案中:
個人資訊交換-	PKCS #12 (PFX, 1	P12)	
密碼編譯訊息器	唔法標準 - PKCS #	7 認證 (.p7b)	
Microsoft 序列遗	题證存放 (.sst)		

10. 选择[将所有凭证放入以下的存放区], 然后按[下一步]。

燕殼匯入精畫	×
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,您也可以為憑證指定存放位置。 ○ 自動根據憑證類型來選取憑證存放區(U) • 蔣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®…	
 <上一步(B) 下一步(D) > 取消	

11. 按[完成]來关闭精靈。

燕證匯入精靈	Contraction of the local division of the loc	×
	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:	
•	使用者進取的憑藏存放區 中總憑證授權 內容 憑證 檔案名稱 C:Vecert_ca_1-10_pem.c	rt
	<上一步(B) 完成] 取	

12. 按[确定]來完成。





图表 1: "Hongkong Post e-Cert CA 1 - 10" 根源证书已成功安装

安装 "Hongkong Post Root CA 1" 根源证书

展开[信任的根凭证授权]及以滑鼠右键按一下[凭证],然后选择[所有工作]>[汇入]。

🚡 主接台1 - [主接台	台根目錄\憑證	(本機電腦))\信任的根憲證授權\憑證]		<u>_ 8 ×</u>
🚡 檔案 🕑 執行 (A) 檢視(V)	我的最愛(0)	→ 視窗(W) 説明(H)			_ 8 ×
← → 🗈 💽	• D	😫 💷				
📄 主控台根目錄		登給 △		發行者	到期日	預定目的▲
📋 🗐 憑證 (本機電)	186)	🔛 ABA.E0	COM Root CA	ABA.ECOM Root CA	2009/7/10	安全電子郵件,1
🗄 💼 個人 🛛 🔛 Autoridad Certificadora de la Aso		ad Certificadora de la Asoci	Autoridad Certificadora de la Asociaci	2009/6/29	安全電子郵件,1	
□ □ □ 信任的根	🖻 🚞 信任的根憑證授權 🛛 🔛		ad Certificadora del Colegi	Autoridad Certificadora del Colegio N	2009/6/30	安全電子郵件,1
	筋有手作が		NE J (T)	Baltimore EZ by DST	2009/7/4	安全電子郵件,1
			JCA	Belgacom E-Trust Primary CA	2010/1/21	安全電子郵件,1
□ 田…□□ 甲羅您護	檢視(?)	×	AT SecureNet CA Class A	C&W HKT SecureNet CA Class A	2009/10/16	安全電子郵件,1
□□□ 文信性的	從這裡新增調	視窗(W	KT SecureNet CA Class B	C&W HKT SecureNet CA Class B	2009/10/16	安全電子郵件,一
1111	*****		KT SecureNet CA Root	C&W HKT SecureNet CA Root	2010/10/16	安全電子郵件,1
□□□□ 第二刀心 □□□□ 受信任的。	新工作合版	硯(山)	KT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Root	2009/10/16	安全電子郵件,1
	重新整理(F)		n - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/27	安全電子郵件,1
	TTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTTT		n - Autoridade Certificador	Certisign - Autoridade Certificadora	2018/6/27	安全電子郵件,1
			n Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/6/27	安全電子郵件,1
	説明(H)		n Autoridade Certificadora	Certisign Autoridade Certificadora A	2018/7/10	安全電子郵件,1
		Class 1	Primary CA	Class 1 Primary CA	2020/7/7	安全電子郵件,1
		Class 1	Public Primary Certification	Class 1 Public Primary Certification A	2028/8/2	安全電子郵件,
		Class 1	Public Primary Certification	Class 1 Public Primary Certification A	2020/1/8	安全電子郵件,)
		Class 2	Primary CA	Class 2 Primary CA	2019/7/7	安全電子郵件,1
		Class 2	Public Primary Certification	Class 2 Public Primary Certification A	2004/1/8	安全電子郵件,)
		Class 2	Public Primary Certification	Class 2 Public Primary Certification A	2028/8/2	安全電子郵件,
		Class 3	Primary CA	Class 3 Primary CA	2019/7/7	安全電子郵件,1
		Class 3	Public Primary Certification	Class 3 Public Primary Certification A	2028/8/2	安全電子郵件,
		Class 3	Public Primary Certification	Class 3 Public Primary Certification A	2004/1/8	安全電子郵件,)
		Class 3H	Primary CA	Class 3P Primary CA	2019/7/7	安全電子郵件,1
		Class 31	IS Primary CA	Class 3TS Primary CA	2019/7/7	安全電子郵件,1
		Copyrig	zht (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	1999/12/31	時間戳記
		Deutsch	e Telekom Root CA 1	Deutsche Telekom Root CA 1	2019/7/10	安全電子郵件,1
						•
將新憑證加入存放						

14. 在[凭证汇入精靈]内,按[下一步]继续。

憑證匯入精靈		×
	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(1) 取消	

 按[浏览]指定早前于 C 部的步骤 7 下载的 "Hongkong Post Root CA 1" 根源证书 (ecert_ca_1_pem.crt), 然后按[下一步]。

檔案名稱(E):			
C:\ecert_ca_1_pem	.crt		劉覽(<u>R</u>)
諸注意:您可以將	數圖憑證用以下的	的格式存放在同一個橋	[案中:
個人資訊交換-1	PKCS #12 (PFX, P	12)	
密碼編譯訊息語	F法標準 - PKCS#	7 認證 (.p7b)	
Microsoft 序列過	體存放 (.sst)		

16. 选择[将所有凭证放入以下的存放区], 然后按[下一步]。

燕證匯入楮畫	x
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,您也可以為憑證指定存放位置。 〇 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: 信任的根憑證授權 瀏覽(R) 	
<上一步(B) 下一步(M) > 取消	

17. 按[完成]來关闭精靈。

燕 波隆入 桥靈		×
	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: 使用資源取到該證確成圖 內容 檔案名稱 C\ecert_ca_1_pem.crt	-
	▲上一步(B) 完成 取消	

18. 按[确定]來完成。



🚡 主控台1 - [主控台根目錄/憑證	(本機電腦)\信任的根憲證授權\憲證]		_ 8 ×
📸 檔案(E) 執行(<u>A</u>) 檢視(V)	我的最愛(◯) 視窗(Ლ) 説明(⊞)			_ 5 ×
← → 🗈 💽 🐰 🖻 🗙 (S B S .			
📄 主控台根目錄	發給 △	發行者	到期日	預定目的▲
🗄 👹 憑證 (本機電腦)	🔤 Equifax Secure eBusiness CA-2	Equifax Secure eBusiness CA-2	2019/6/23	安全電子郵件,1
直…(□□ 個人	🔛 Equifax Secure Global eBusiness C	Equifax Secure Global eBusiness CA-1	2020/6/21	安全電子郵件,1
🖻 📄 信任的根憑證授權	🖼 EUnet International Root CA	EUnet International Root CA	2018/10/2	安全電子郵件,1
	🔤 FESTE, Public Notary Certs	FESTE, Public Notary Certs	2020/1/2	安全電子郵件,1
	🖼 FESTE, Verified Certs	FESTE, Verified Certs	2020/1/2	安全電子郵件,1
田一旦 甲繼徳證授權	🔛 First Data Digital Certificates Inc. C	First Data Digital Certificates Inc. Cert	2019/7/4	伺服器驗證,用)
田二国 文信仕的幾行者	🖼 FNMT Clase 2 CA	FNMT Clase 2 CA	2019/3/18	安全電子郵件,1
出一 2 後有信性別您證	🖼 GlobalSign Root CA	GlobalSign Root CA	2014/1/28	安全電子郵件,1
田一四 第二万限思想反推单位	🖼 GTE CyberTrust Global Root	GTE CyberTrust Global Root	2018/8/14	安全電子郵件,
	🖼 GTE CyberTrust Root	GTE CyberTrust Root	2004/4/4	安全電子郵件,厂
	FieldTE CuberTrast Poot	GTE CuberTract Poot	2006/2/24	空谷蚕之配件(
	🔤 Hongkong Post Root CA 1	Hongkong Post Root CA 1	2023/5/15	<全部>
	Bith://www.valicert.com/	http://www.yalicert.com/	2019/6/26	安全雷子郵件。(
	122 http://www.valicert.com/	http://www.valicer.com/	2019/6/26	安全電子郵件,1
	🔤 http://www.valicert.com/	http://www.valicer.com/	2019/6/26	安全電子郵件,1
	E IPS SERVIDORES	IPS SERVIDORES	2009/12/30	安全電子郵件, ——
	🔤 Microsoft Authenticode (tm) Root A	Microsoft Authent ode (tm) Root Aut	2000/1/1	安全電子郵件,
	🔤 Microsoft Root Authority	Microsoft Root A ority	2020/12/31	<全部>
o IL Cyber Hast Root	O IL Cyberriastice	7. 2000	2127	XIBIRI
Hongkong Post Root CA 1	Hongkong Post Root	CA 1 2023	/5/15	<全部>
http://www.valicert.com/	http://www.yalicert.co	2019 / mr	16/26	安全雷子郵件
	NO LIABILITY ACCEPTED, (c)9	NO LIABILITY ACCEPTED, (c)97	2004/1/8	時間戳記
	🔛 PTT Post Root CA	PTT Post Root CA	2019/6/26	安全電子郵件,1
	🔛 Saunalahden Serveri CA	Saunalahden Serveri CA	2019/6/26	安全電子郵件,1
	🔛 Saunalahden Serveri CA	Saunalahden Serveri CA	2019/6/26	安全電子郵件, (一)
	17			
, 信任的根憑證授權 存放包令 104 個調	,			

图表 2: "Hongkong Post Root CA 1" 根源证书已成功安装

- E. 安装伺服器证书
 - 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] / [Internet 服务管理员] 來启动网际网路资讯服务 (IIS) 管理 员。
 - 2. 在 [网际网路资讯服务 (IIS) 管理员] / [Internet Information Services]视 窗内,展开[网站]及选择您的网站,以滑鼠右键按一下,然后按[内容]。



3. 在[目錄安全设定]索引标签内,按一下[伺服器凭证]。

預設的網站 內容	<u>? ×</u>
網站 效能 ISAPI 篩選器 目錄安全設定 HTTP 標頭	主目錄 文件 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。	[]
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 或拒絕到這個答應的存取。	₹
安全通訊 當存取這個資源時使用安全通訊並書 用用戶端憑證。	伺服器憑證③ 依視憑證(∑)

4. 在[网页伺服器凭证精靈] / [Web 伺服器凭证精靈]内,按[下一步]继续。

歡迎使用網頁伺服器憑證精霊。 🛛 🔀 🔀 🛛 🔀 🛛 🔀 🛛 🔀 🛛 🔀 🛛 🔀 🛛 🛛 🛛 🛛 🛛 🛛 🖉			
	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: 您有擱置的憑證要求。憑證精靈將協助您處理 憑證授權的回應或移除擱置要求。		
	諸按 [下一步] 來繼續。		
	<上一步(B) 下一步(D) 取 消		

5. 选择[处理搁置要求及安装凭证],然后按[下一步]。

IIS 憲憲精靈	×
蜀置的燕證要求 擱置的憑證要求是指憑證授權未回應的要求。	
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(P)	
○ 刪除擱置要求(D)	
· · · · · · · · · · · · · · · · · · ·	
<u> < 上一步 (B)</u> 下一步 (<u>N</u>) >]	取消

 按[浏览]指定早前于 C 部的步骤 7 下载的 "Hongkong Post e-Cert (Server)" 证书, 然后按[下一步]。

IIS 憲證精靈	×
虚理國置要求 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):	
c:/cert0000812107.cer	(調覽(R)
<u>《上一步图】</u> 下一:	步(11) > 取消

在[这个网站应该使用的 SSL 連接埠]输入 443, 然后按[下一步]。
 (若使用 IIS 5.0, 请跳到步骤 8)

IIS 憲證精靈		×
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(L):		
	<上一步图 下一步图 >	取消

8. 按[下一步]。

IIS 憲證精靈		×
您已經選擇從回應都 憑證摘要	富家安装設。	
若要安裝下列憑言	澄,請按 [下一步]。	
檔案名稱:	c:\cert0000812107.cer	
憑證詳細資訊: 發給者 發照期日 好記家市 單位	www.myserver.com Hongkong Post e-Cert CA 1 - 10 2008/11/19 預設的網站 HK Hongkong Post e-Cert (Server) 0000812107	
	<上一步(B) 下一步(B)	取消

9. 按[完成]來关闭精靈。



10. 按[检视凭证]來检视伺服器证书。

預設的網站 內容		<u>? ×</u>
網站 效能 目錄安全設定	と ISAPI 篩選器 HTTP 標語	
- 驗證及存取控制 — 啓用置 證方法	名存取,並編輯這個資源 。	記的驗 编輯(正)
- IP 位址及網域名稱 使用 IF 、 或拒絕	限制 - 位址或網際網路網域名和 到這個資源的存取。	調來授予
安全通訊	這個資源時使用安全通訊	
	AMDIEYER -	
		育

意識 ?×
一般 詳細資料 憑證路徑
「「「「「」」 「「」」 「「」」 「」 「」」 「」 「」 「」」 「」 「」
這 個戀證的使用目的如下 :
* 7711日78年7月11年3年4月37日
*請參照憑證授權敘述中的詳細資訊。
登給 : www.myserver.com
登行者 : Hongkong Post e-Cert CA 1 - 10
有效期自 2007/11/19 到 2008/11/19
ॐ 這個憑證有一個對應的私密金鑰。
(發行者聲明③)

图表 3: "Hongkong Post e-Cert (Server)" 证书已成功安装

F. 备份密码匙

在 IIS 5.0 上备份密码匙

- 1. 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 來启动网际网路资讯服务 (IIS) 管理员。
- 2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内,展开[网站]及选择您的 网站,以滑鼠右键按一下,然后按[内容]。



3. 在[目錄安全设定]索引标签内,按一下[伺服器凭证]。

預設的網站 內容	<u>? ×</u>
網站 效能 ISAPI 篩選器 I 目錄安全設定 HTTP 標頭	主目錄 文件 自訂錯誤
驗證及存取控制 略用匿名存取,並編輯這個資源的驗 證方法。	(<u>編輯(E)</u>]
Ⅰ 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。	
	编輯()
安全通訊 當存取這個資源時使用安全通訊並書 用用戶端憑證。	伺服器憑證(S) 検視憑證(V) 編輯(D)
 確定 取消	

4. 在[网页伺服器凭证精靈]内,按[下一步]继续。

歌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: 您已在選取的伺服器安裝了憑證。憑證精靈將 協助您管理此憑證。		
	請按 [下一步] 來繼續。		
	<上一步(B) 下一步(Q) > 取消		

5. 选择[汇出目前的凭证到.pfx 档案], 然后按[下一步]。

IIS 意識精靈	×
修改目前的憲 證指派 目前安裝在此網站的憑證。	
您想要如何處理目前安裝的憑證?	
○ 更新目前的憑證(₩)。	
○ 移除目前的憑證(R)。	
○ 取代目前的憑證(<u>A</u>)。	
● 羅出目前的憑證到.pfx 檔案(区)	
○ 複製或移動目前的憑證到遠端伺服器將站(C)	
<上一步(B) 下一步(M) >	取消

6. 输入要汇出凭证的档案名称及路径,然后按[下一步]。

IIS 憲證精靈		×
匯出憲證 您可以匯出憑證到 PFX 檔案。		
請輸入要匯出憑證的檔案名稱及路徑。		
路徑及檔案名稱(P):		
C:\myserver.pfx		瀏覽(R)
	<上─毋個 下─±	步(N) > 取消

7. 输入并确认密码为汇出的.pfx 档加密。

注意:请牢记这个非常重要的密码。如果您忘记这密码,您将不能还原您的密码匙。

IIS 憑證精靈	×
憲證 密碼 您必須提供密碼以匯出憑證。	
請輸入密碼爲匯出的 .pfx 檔加密	
密碼(P):	

確認密碼(C):	

<u> <上−毋</u> 圕 下−±	步(N) > 取消

8. 按[下一步]。

IIS 憲法 結素 陸出憲法 摘要 您已選擇要匯出	下列憑證。	×
若要匯出下列憑 檔案名稱: 憑證詳細資訊: 發照對日 好記的名稱 國家市 單位	證到此檔案,請按 [下一步]。 c:\myserver.pfx www.myserver.com Hongkong Post e-Cert CA 1 2008/11/19 預設的網站 HK Hongkong Post e-Cert (Server) 0000812107	
	<上一步图 下一步 四 >	

9. 按[完成]來关闭精靈。

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。	
	憑證已匯出到檔案。	
	要關閱這個精靈,請按 [完成]。	
	<上一步(B) 完成 取消	

<u>在 IIS 6.0 上备份密码匙</u>

- 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 來启动网际网路资讯服务 (IIS) 管理员。
- 2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内,展开[网站]及选择您的 网站,以滑鼠右键按一下,然后按[内容]。

「目前の目的では、112) 管理員				
5 檔案(F) 執行(Δ) 檢視(Y) 視窗(W) 説明(E)				_ 8 ×
← → 🗈 💽 🗙 😭	0 🖻 😫 🖬 🎍	2 ▶ ■ Ⅱ		
網際網路資訊服務 myserver (本機電腦) ・ の 應用程式集區 ・ 初站 ・ 利潤 一 利潤 一 利潤 一 利潤 一 利潤 一 利潤 一 一 利潤 一 一 利潤 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	查看(E) 開容舊檔(Q) 使用權限(L) 瀏覽(B) 容動(S) 停止(P) 暫停(A) 新增(N) 所有工作(K) 檢視(Y) 從這裡新增視窗(W) 剛除(D) 重新命名(M) 重新整理(P) 匯出諸單(L)	start.htm gerror.gif	路徑	
	前800 説明(<u>H</u>)			Þ

3. 在[目錄安全设定]索引标签内,按一下[伺服器凭证]。

預設的網站 內容	<u>? ×</u>
網站 效能 ISAPI 篩選器 I 目錄安全設定 HTTP 標頭	主目錄 文件 自訂錯誤
驗證及存取控制 略用匿名存取,並編輯這個資源的驗 證方法。	(<u>編輯(E)</u>]
Ⅰ 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。	
	编輯()
安全通訊 當存取這個資源時使用安全通訊並書 用用戶端憑證。	伺服器憑證(S) 検視憑證(V) 編輯(D)
 確定 取消	

4. 在[网页伺服器凭证精靈]内,按[下一步]继续。

歌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: 您已在選取的伺服器安裝了憑證。憑證精靈將 協助您管理此憑證。		
	請按 [下一步] 來繼續。		
	<上一步(B) 下一步(Q) > 取消		

5. 选择[汇出目前的凭证到.pfx 档案], 然后按[下一步]。

IIS 憲證精靈	×
修改目前的要證指派 目前安裝在此網站的憑證。	
您想要如何處理目前安裝的憑證?	
○ 更新目前的憑證(型)。	
○ 移除目前的憑證 R)。	
○ 取代目前的憑證(Δ)。	
● 羅出目前的憑證到.pfx 檔案(茲)	
○ 複製或移動目前的憑證到遠端伺服器網站(C)	
<上一步(B) 下一步(A) >	取消

6. 输入要汇出凭证的档案名称及路径,然后按[下一步]。

IIS 憲證精靈		×
匯出憲證 您可以匯出憑證到 PFX 檔案。		
請輸入要匯出憑證的檔案名稱及路徑。		
路徑及檔案名稱(P):		
C:\myserver.pfx		瀏覽(R)
	<上─毋個 下─±	步(N) > 取消

7. 输入并确认密码为汇出的.pfx 档加密。

注意:请牢记这个非常重要的密码。如果您忘记这密码,您将不能还原您的密码匙。

IIS 憑證精靈	×
憲證 密碼 您必須提供密碼以匯出憑證。	
請輸入密碼爲匯出的 .pfx 檔加密	
密碼(P):	

確認密碼(C):	

<u> <上−毋</u> 圕 下−±	步(N) > 取消

8. 按[下一步]。

IIS 憲法 結素 陸出憲法 摘要 您已選擇要匯出	下列憑證。	×
若要匯出下列憑 檔案名稱: 憑證詳細資訊: 發照對日 好記的名稱 國家市 單位	證到此檔案,請按 [下一步]。 c:\myserver.pfx www.myserver.com Hongkong Post e-Cert CA 1 2008/11/19 預設的網站 HK Hongkong Post e-Cert (Server) 0000812107	
	<上一步图 下一步 四 >	

9. 按[完成]來关闭精靈。

IIS 憲證精靈	<u>×</u>
	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。
	憑證已匯出到檔案。
	要關閉這個精靈,諸按 [完成]。
	<上一步(B) 完成 取消

G. 还原密码匙

<u>在 IIS 5.0 上还原密码匙</u>

 按 [开始] > [执行], 然后输入 "mmc"及按[确定] 來启动 Microsoft Management Console (MMC), 然后从[主控台]选单中选取[新增/移除嵌 入式管理单元]。

🚡 主控台1 💦 💶 🔤 💷 📃	
〕 [主控台(C)] 視窗(W)] 説明(H) □ [] [] [2] [] [] []	
開新檔案(1) Cttl+N 開啓舊檔(0) Cttl+O 儲存(2) Cttl+S 另存新檔(2) 新增移除試入式管理單元(1/1) Cttl+M 選項(1) 最近使用過的檔案 結束(2)	

11. 按[新增]。

新增移除嵌入式管理單元	Ê	?×
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 加入(S):		-
描述		
新增(D) 1	條(配) 關於(B)	
	確定	取消

12. 选择[凭证], 然后按[新增]。

新增獨立嵌入式管理單元	<u>? ×</u>
可用的獨立嵌入式管理單元:	
嵌入式管理單元	廠商▲
🔜 裝置管理員	Microsoft Corporation
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
📃 🧕 路由及遠端存取	Microsoft Corporation
電腦管理	Microsoft Corporation
🔹 🔊 電話語音	Microsoft Corporation
🛛 😻磁碟重組工具	Executive Software Inte
📄 磁碟管理	VERITAS Software Cor
	Microsoft Corporation
- 描述	
」」 「通過」 「通過」 「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	服态的漏踏左筋肉爽。
心証料////目/王年/168/心相见电脑系	MX47145/25215/0213125
<u></u>	
]	新增(A) 開閉
L	

13. 选择[电脑帐户], 然后按[下一步]。

憑證嵌入式管理單元	≤
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)	
<上一步(B) 下一步(M) > 取消	1

14. 选择[本机电脑], 然后按[完成]。

選擇電腦		×
諸選取您要嵌入式管理單元 這個嵌入式管理單元將自 ○ 本機電腦(執行這個目	進行管理的電腦。 動管理: 	
○ 另一台電腦(A):	瀏覽(3)	
🔲 允許在執行指令行時	變更選取電腦,這只能在您儲存主控台時使用(<u>W</u>)	
	<上一步(B) 完成 取消	

- 15. 关闭[新增独立嵌入式管理单元]对话框, 然后按[确定]关闭[新增/移除嵌入式管理单元]对话框。
- 16. 展开[个人]及以滑鼠右键按一下[凭证],然后选择[所有工作] > [汇入]。(如要还原凭证要求的密码匙,请展开[凭证注册要求](或于某些系统称为[REQUESTS])。)

🚡 主控台1 - [主控台根	目錄\憑證 (本機電腦)\個人\憑證]			
│ 🏠 主控台(C) 視窗	1(W) 説明(H)			🗋 🗃 🔚 💷 🖃 🗵
」執行(▲) 檢視(♡)	我的最愛 🕑 🚽 👉 ⇒ 🗎 🖬	🔹 🔯 😫		
樹狀目錄 我的最愛	登給 △	發行者	到期日	預定目的
	所有工作(近) 要求新憑 檢規(位, 一, 一) 提入 從這裡新增視窗(四) 新工作台檢視(工) 董新整理(P) 輸出活單(し 説明(丑)			
	•			
將新憑證加入存放				

17. 在[凭证汇入精靈]内,按[下一步]继续。

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(E) 下一步(N) 取消

18. 按[浏览]指定密码匙的备份档案,然后按[下一步]。

設確入精会
要匯入的檔案 指定您想要匯入的檔案。
檔案名稱(E):
C./unyserver.pfx
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(B) 下一步(AD) > 取消

19. 输入密码匙的密码, 然后按[下一步]。

注意:为使您将來可以进行备份或传输您的密码匙,您可以将这个密码 匙设成可汇出。

憑證匯入精靈				×
密碼 资子性性实入性,利应会给买到应该的				
為」維持女王性,似名玉鏞又則名鸣的	小木:			
輸入私密金鑰的密碼。				
密碼(2):				

□ 賢用加強私密金鑰保護:如果弊	啓用這個選項,	毎次		
构密立辅放應用程码使用,系統	県曾健小心(也)			
□ 將私密金鑰標示成可匯出(M)				
	<上──步®)	下一步(N)> 取	消
		1 2/14		

20. 选择[将所有凭证放入以下的存放区], 然后按[下一步]。

● 證進人精靈 ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲
思設仔放區是用來仔放思想的系統區域。
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。
○ 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(E)
憑證存放區:
個人 瀏覽 (2)
<上一步(B) 下一步(M) > 取消

21. 按[完成]來关闭精靈。

憑證匯入精靈			×
	完成憑證匯入精霊		
	您已經成功地完成憑證匯入	精霊。	
	您已指定以下新的設定:		
	使用者選取的憑證存放區	個人	
	内谷 檔案名種	C'mvserver.pfx	
and the second second			
	J		
			_
	<上─步®)	完成 取消	

22. 按[确定]來完成。



<u>在 IIS 6.0 上还原密码匙</u>

- 按 [开始] > [所有程式] > [系统管理工具] > [网际网路资讯服务 (IIS) 管理员] 來启动网际网路资讯服务 (IIS) 管理员。
- 2. 在 [网际网路资讯服务 (IIS) 管理员] 视窗内,展开[网站]及选择您的 网站,以滑鼠右键按一下,然后按[内容]。

🀚 洞際網路資訊服務 (IIS) 管理員		
퉻 檔案(E) 執行(A) 檢視(Y) i	視窗(₩) 説明(<u>H</u>)	_ Ð ×
	≥ 😢 💷 🖳 ▶ ■ 🗉	
 網際網路資訊服務 ●●● 應用程式集區 ●●● 網站 ●●● 預設的網站 ●●● 預設的網站 ●●● 網站 ●●● 預設的網站 ●●● 預告 ●●●● 預告 ●●●● 預告 ●●●● 預告 ●●●●● 預告 ●●●●●● 預告 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	名稱 路徑 iisstart.htm pagemor.gif 舊檔(0) 權限(1) (B) (B) (C) (C) (D) (C) 命名(M) 整理(P) 清單(1) (C)	状況
。 爲目前的選取項目開啓內容		

3. 在[目錄安全设定]索引标签内,按一下[伺服器凭证]。

預設的網站 內)	容	<u>?</u> ×
網站 目錄安	│ 效能 │ ISAPI 篩選器 │ 注設定 │ HTTP 標頭	主目錄 文件 自訂錯誤
驗證及存取	救控制 啓用匿名存取,並編輯這個資源的驗 證方法。	[]
	围城名稱限制 使用 IP 位址或網際網路網域名稱來授 或損縮到這個資源的存取。	·····································
W		編輯(])
安全通訊一	當存取這個資源時使用安全通訊並書 用用戶端憑證。	(司服器憑證(፩) 檢視憑證(♡) 編輯(D)

4. 在[网页伺服器凭证精靈]内,按[下一步]继续。

歡迎使用網頁伺服器憑證精調	E •	×
	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。	
	諸按 [下一步] 來繼續。	
	<上一步(B) 下一步(M) 取消	

5. 选择[从.pfx 档案汇入凭证], 然后按[下一步]。

IIS 憑證精畫	×
伺服器赛證 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:	
○ 建立新憑證(<u>C</u>)。	
○ 指派已有的憑證(鱼)。	
○ 從金鑰管理員備份檔案匯入憑證(Q)。	
○ 從.ptx檔案進人態證(M)	
○ 從遠端伺服器網站複製或移動憑證到此網站(型)	
<上一步(B) 下一步(M) >	取消

6. 输入包含凭证的档案名称及路径,然后按[下一步]。

注意:为使您将來可以进行备份或传输您的凭证,您可以将这个凭证标示为可汇出。

IIS 憲證精畫		x
匯入憑證		
您可以從 PFX 檔匯入憑證。		Ŵ
請輸入包含憑證的檔案名稱及路徑。		
路徑及檔案名稱(2):		
c:\myserver.pfx	瀏覽(R)	
指定在匯入後,匯入的憑證是否應標示為可匯出。將憑證標示為 較高的安全風險,不過,它可允許憑證匯出到檔案進行備份。	可匯出將具有	
<上─步B 下一步	F(N) > P	刘

7. 输入凭证的密码,然后按[下一步]。

IIS 憲證精畫		×
匯入憲證密碼		
您必須提供密碼以匯人憑證。 		Ŵ
諸爲您想要匯入的憑證輸入密碼。		
密碼(P):		

	< 上一步(B) 【 下一步(R) >】	取消
		1/10

8. 在[这个网站应该使用的 SSL 連接埠]输入 443, 然后按[下一步]。

IIS 憲證精靈		×
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(L):		
	<上─毋圆 下─毋₪>	取消

9. 按[下一步]。

IIS 憲證精靈		×
已匯入憲證的摘要 您已選擇要安裝下列憑證。	•	
若要安裝下列匯入的憑證	,請按 [下一步]。	
檔案名稱: c:\mys	server.pfx	
憑證詳細資訊: 發給 發照用 好記的名稱 國家地區 公司 單位	www.myserver.com Hongkong Post e-Cert CA 1 2008/11/19 預設的網站 HK Hongkong Post e-Cert (Server) 0000812107	
	<上一步图 下一步(M)>	取消

10. 按[完成]來关闭精靈。

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。	
	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,請再 次使用精靈。	
	要關閉這個精靈,諸按 [完成]。	
	<上一步(B) 完成 取消	

