SSL 伺服器數位憑證
IBM HTTP Server 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：V1.1
文件編號：MNT-03-076
生效日期：101 年 9 月 27 日

目　　錄

1. 目的

1.1. 介紹 IBM HTTP Server 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。

2.參考資料

無。

3.定義

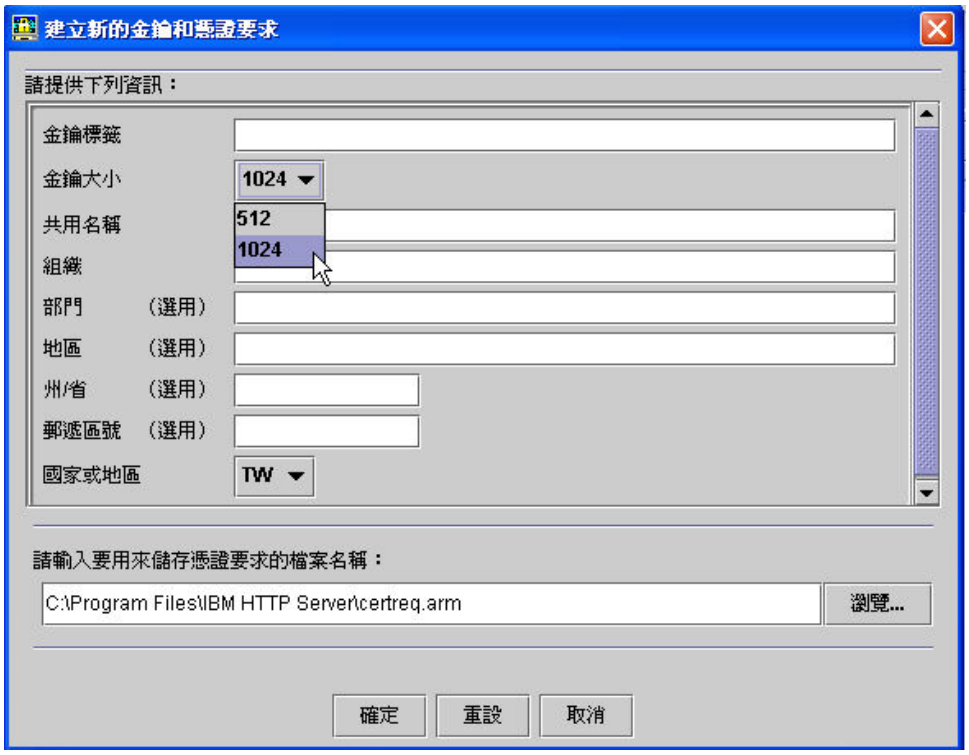
無。

4.作業程序

4.1 升級 GSKit 版本

※由於IHS6.0預設無法產生2048金鑰長度CSR，建議升級為IHS7.0以上版本，或在原IHS6.0架構，參照以下IBM官方技術說明作法，下載FIX檔修復。

4.1.1 IHS6.0 預設只能產生 1024 位元金鑰長度 CSR

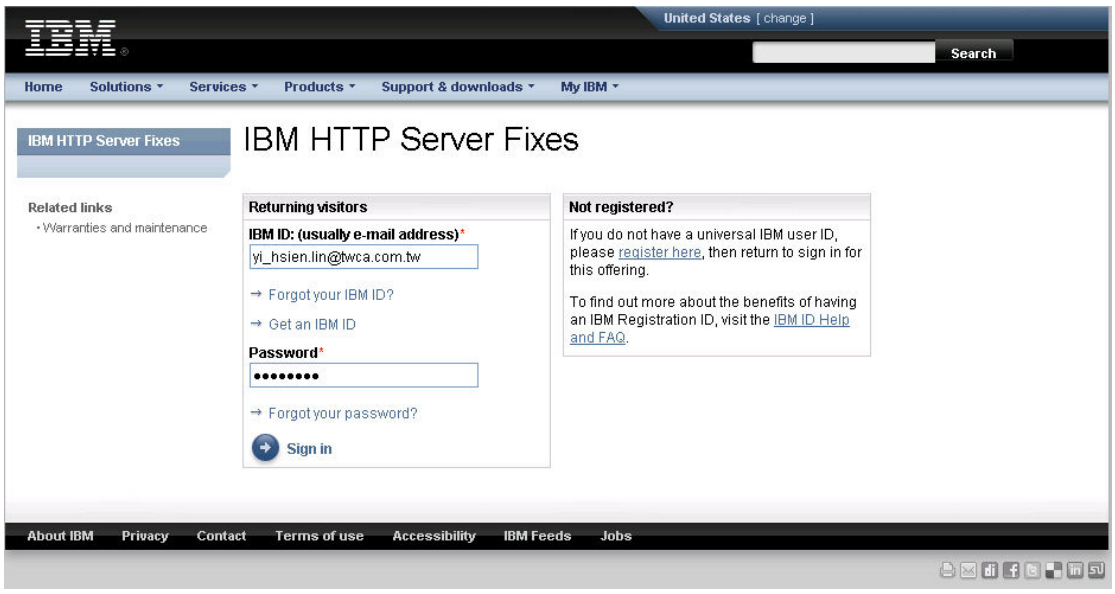


4.1.2 IBM 官方技術說明連結

http://www-01.ibm.com/support/docview.wss?uid=swg21421447

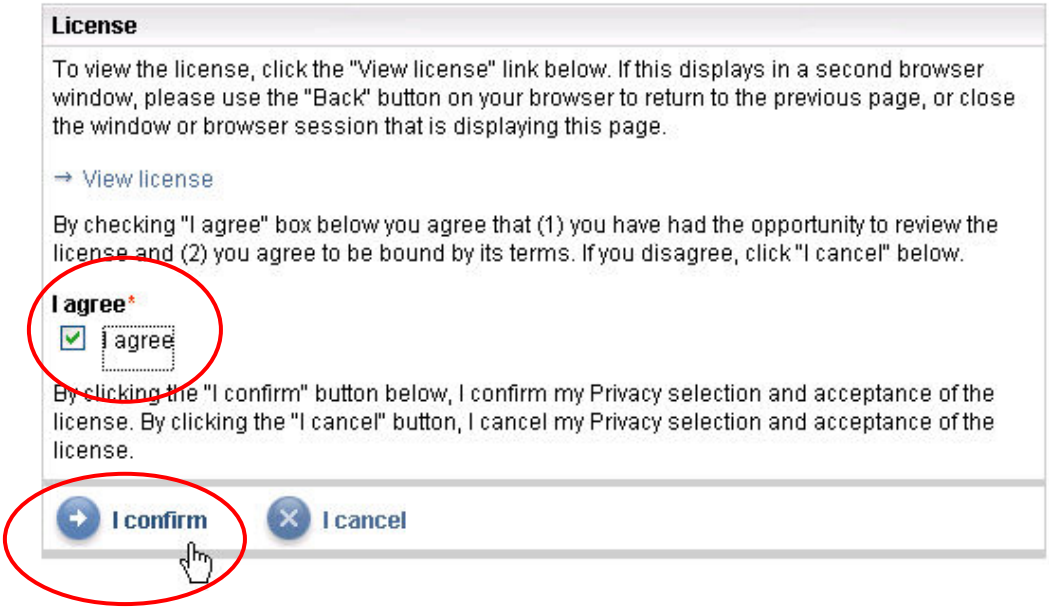
4.1.3 點選「IBM HTTP Server Fixes」連結

4.1.4 於 IBM 官網註冊一免費帳號，並輸入帳號(郵件地址)及密碼，點選「Sign in」登入

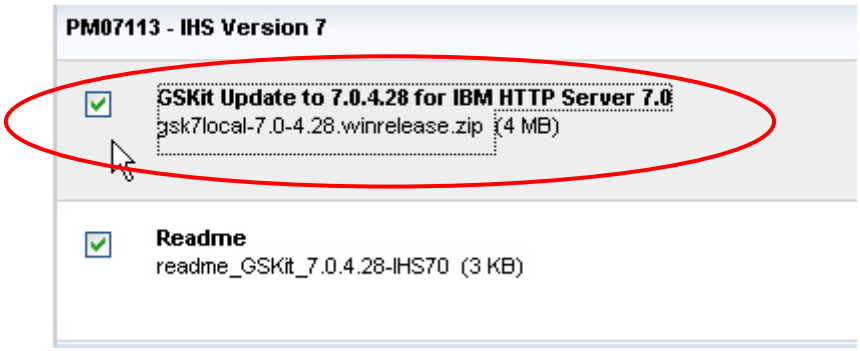


4.1.5 選擇 Windows 2000、Windows NT 版本，點選「Continue」

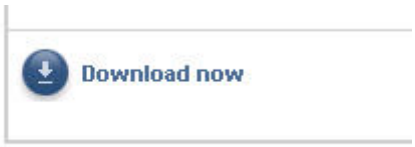
4.1.6 勾選「I agree」，點選「I confirm」



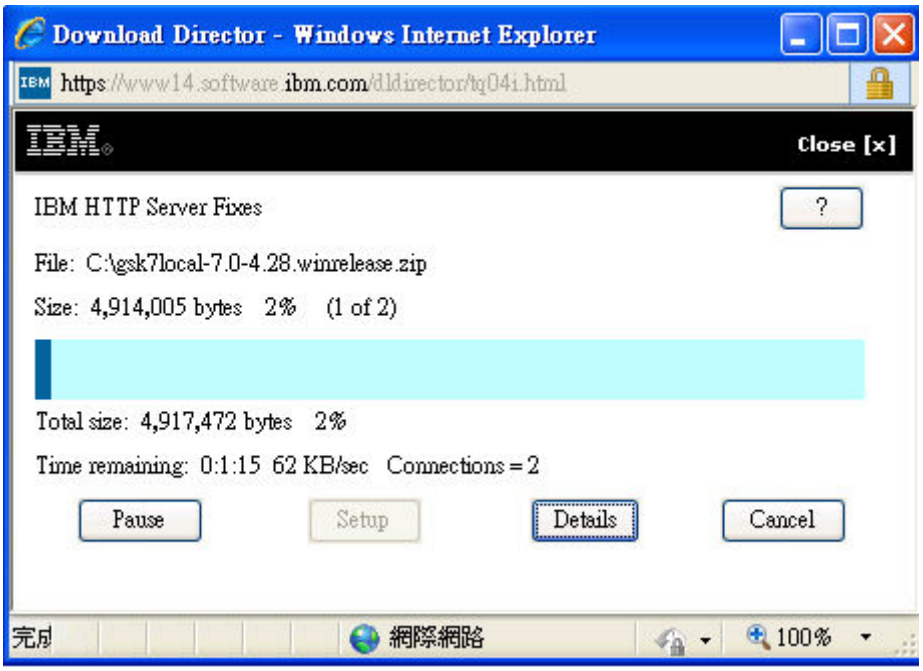
4.1.7 下拉選單，找到「gsk7local-7.0-4.28.winrelease.zip」修正檔並勾選



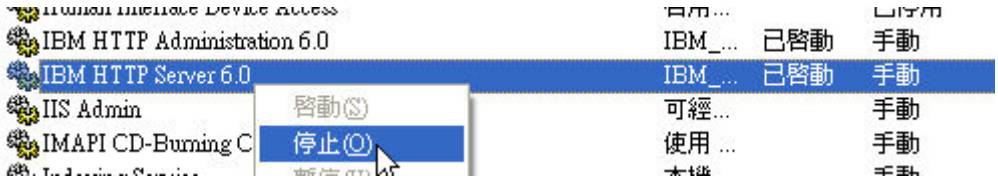
4.1.8 點選「Download now」



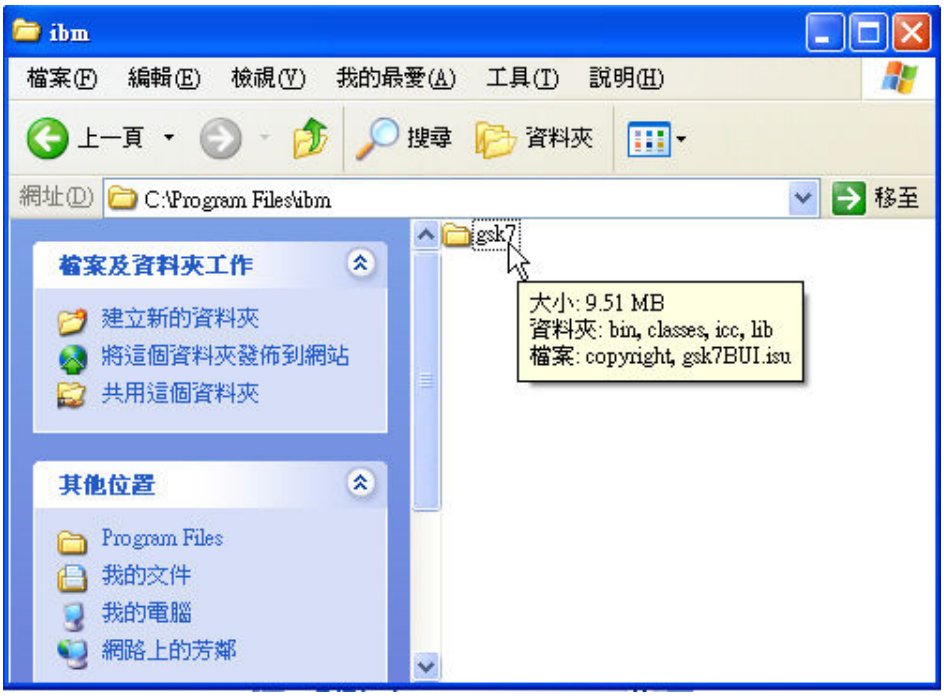
4.1.9 啟動 IBM 下載程式，選擇存放路徑，開始下載選擇檔案



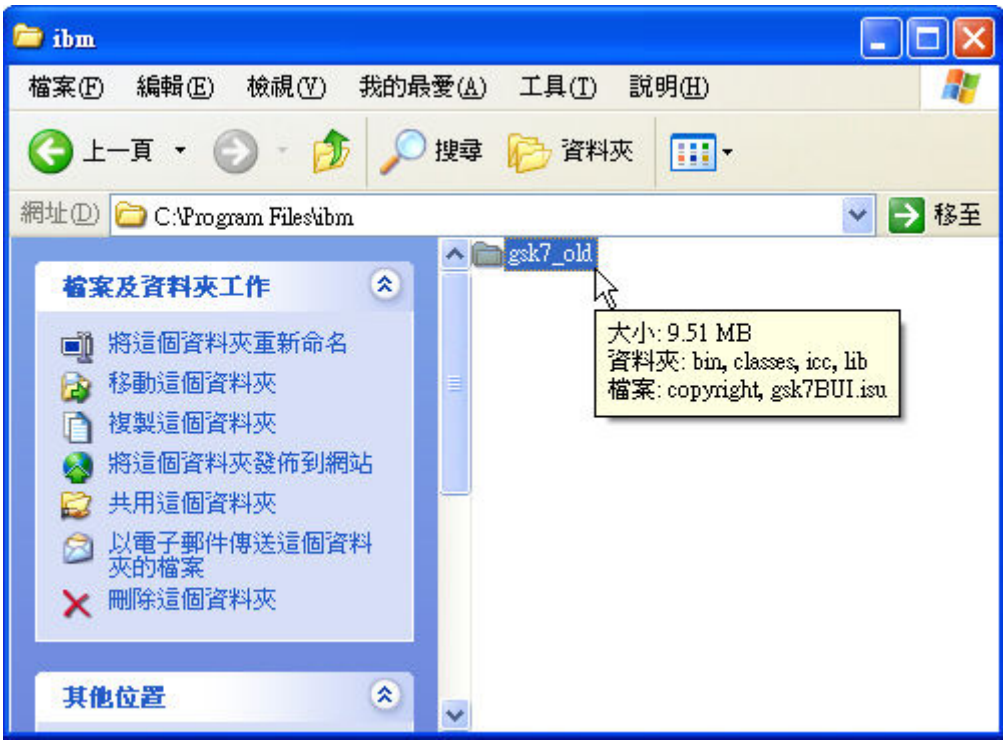
4.1.10 開始升級 GSKit 版本，請先停止 IBM HTTP Server 6.0 服務



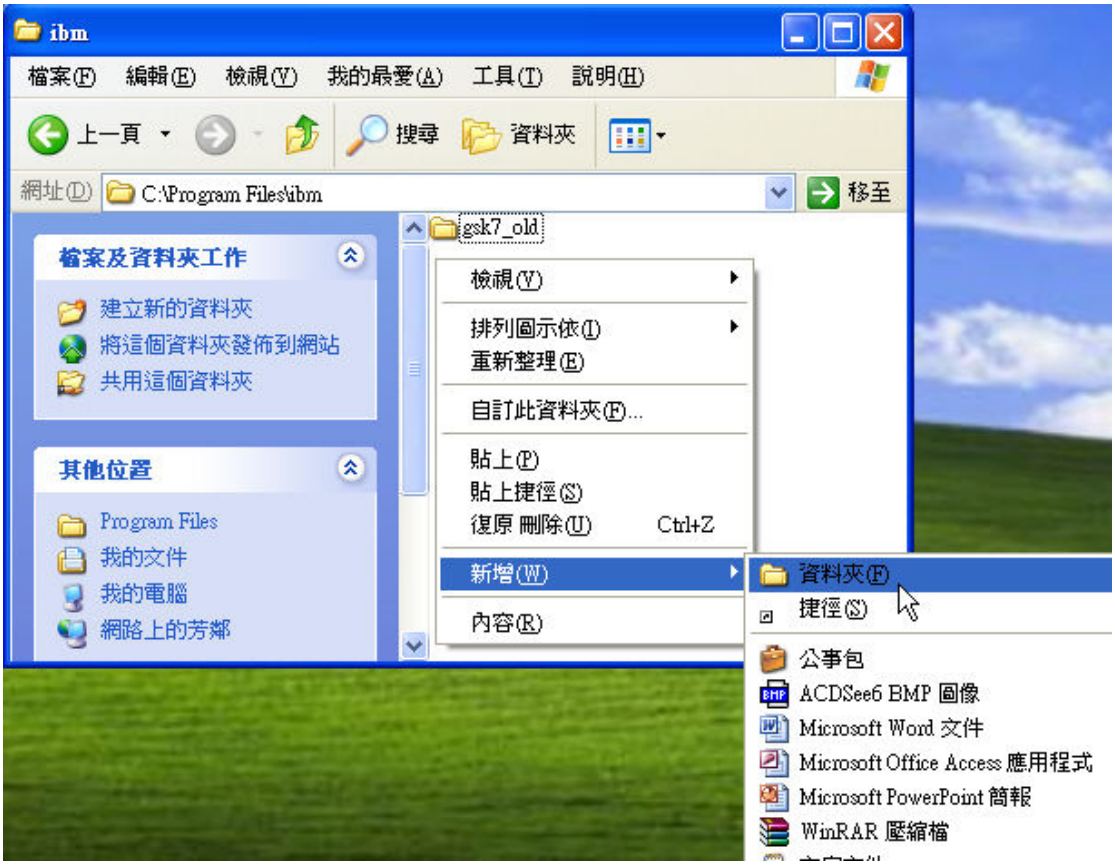
4.1.11 進入 gsk7 所在路徑，預設安裝路徑為 C:\Program Files\ibm



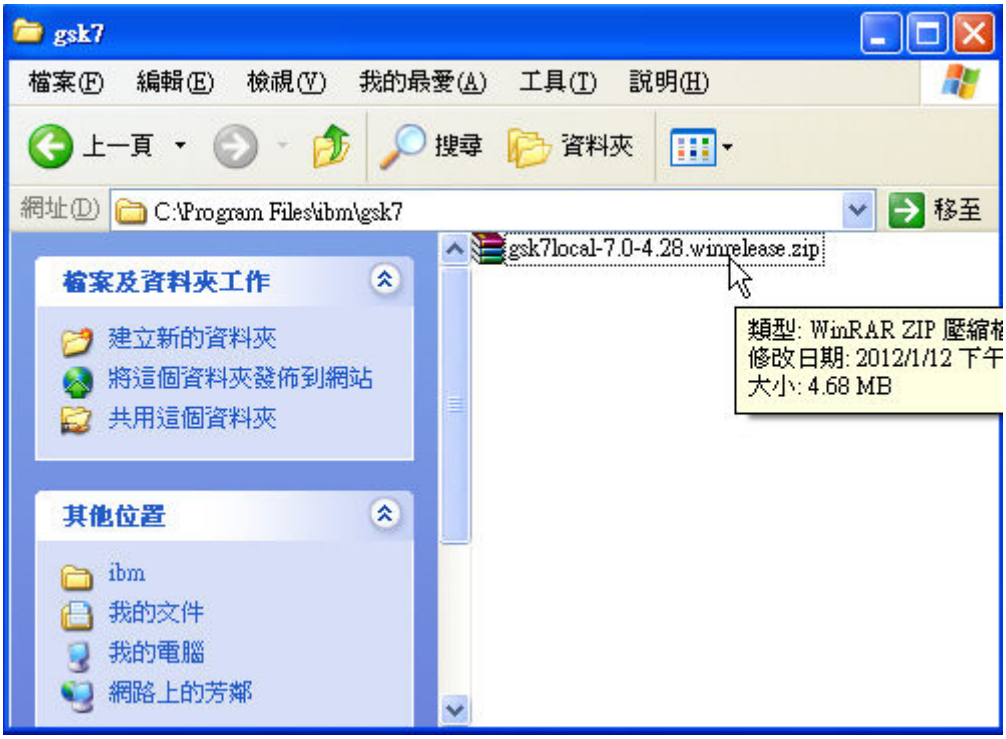
4.1.12 重新命名 gsk7 資料夾名稱，例如更名為 gsk7_old



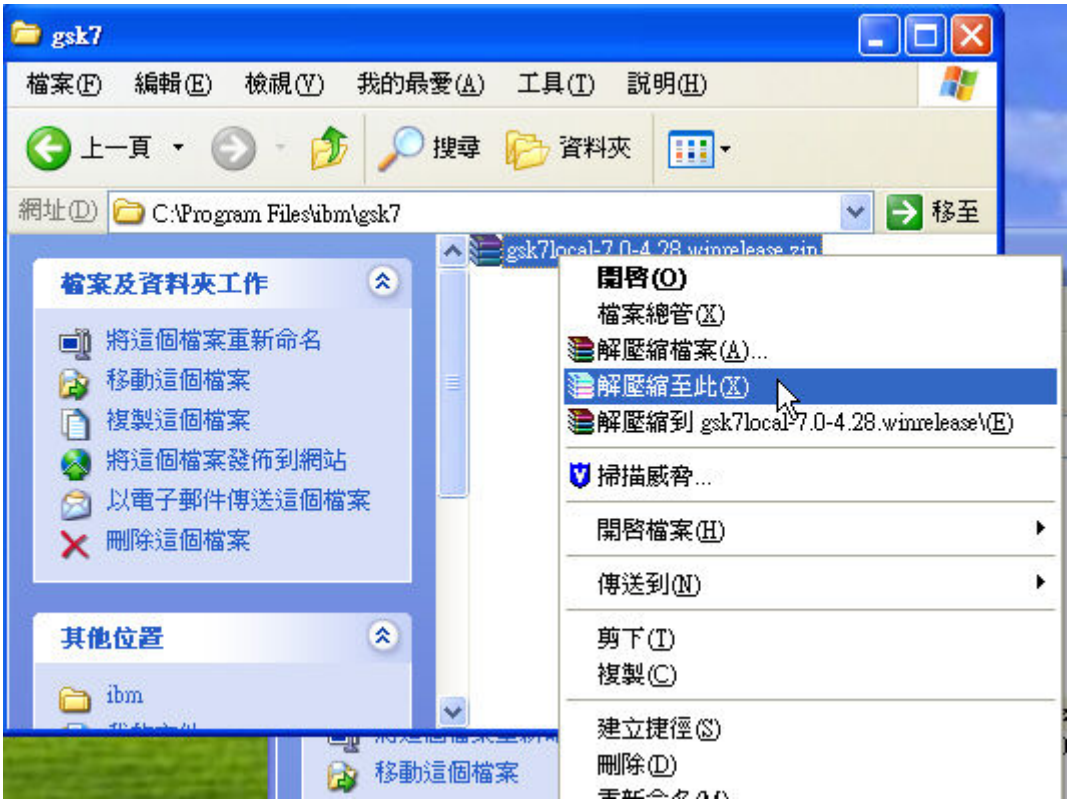
4.1.13 新增一資料夾，並重新命名為 gsk7



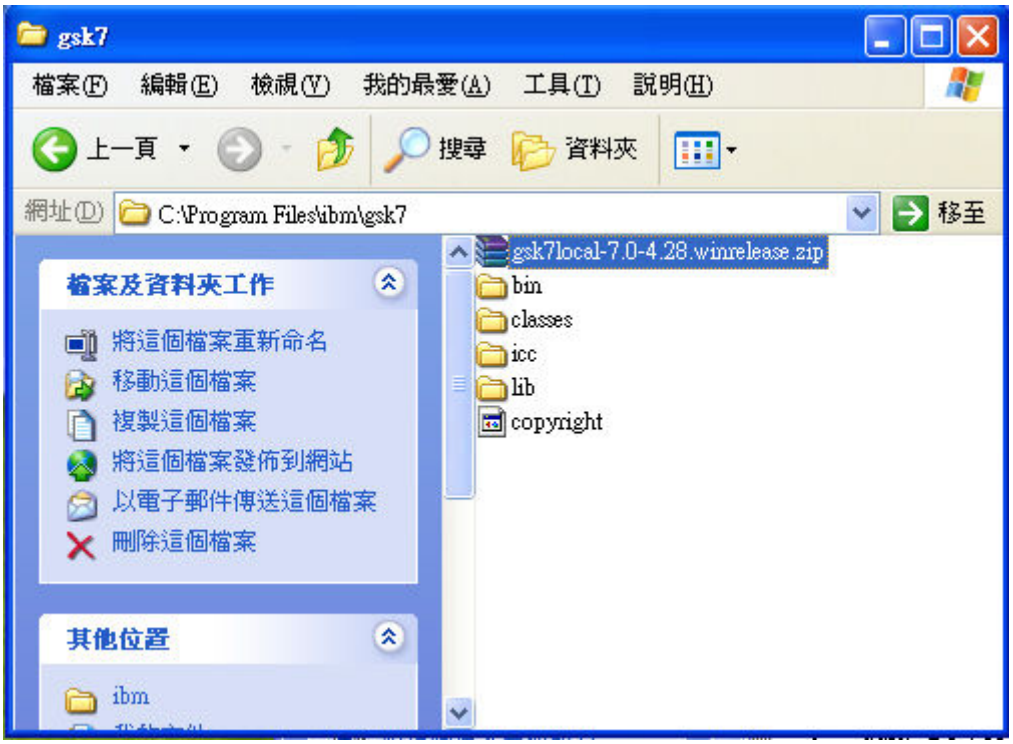
4.1.14 將 GSKit7 修補程式 gsk7local-7.0-4.28.winrelease.zip 置於 gsk7 資料夾內



4.1.15 將檔案解壓縮至 gsk7 資料夾內

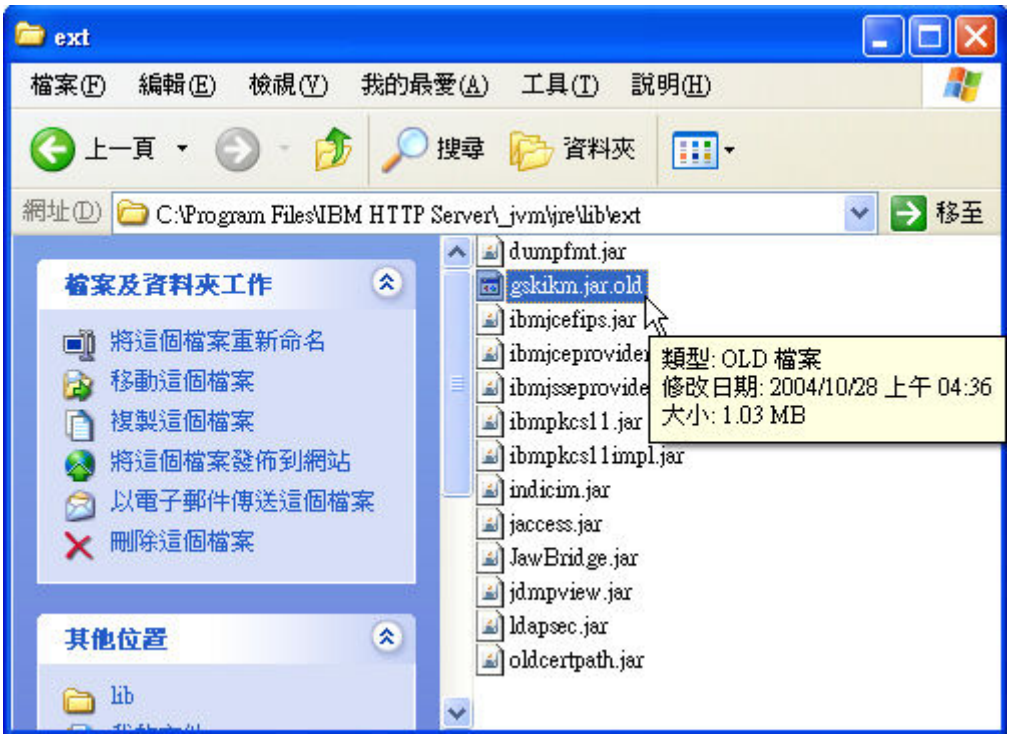


4.1.16 解壓縮後結果



4.1.17 重新更名 gskikm.jar(預設安裝路徑為 C:\Program Files\IBM HTTP Server_jvm\jre\lib\ext)

4.1.18 例如更名為 gskikm.jar.old



4.1.19 重新啟動 IBM HTTP Server6.0 服務

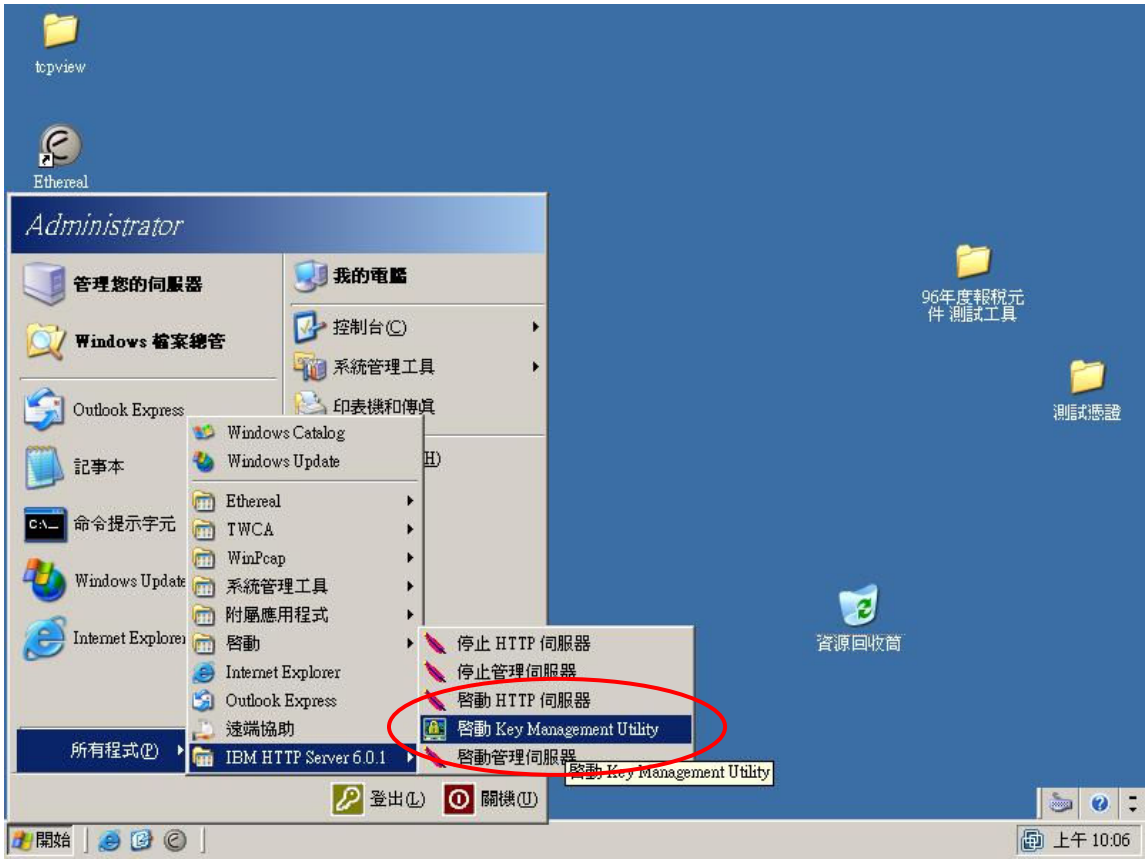
4.1.5 修復 GSKit 後，IHS6.0 可產生 2048 位元金鑰長度 CSR

4.2 產生「憑證請求檔(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！

4.2.1 啟動 IKEYMAN（IKEYMAN 是 IBM HTTP SERVER 的憑證管理程式）

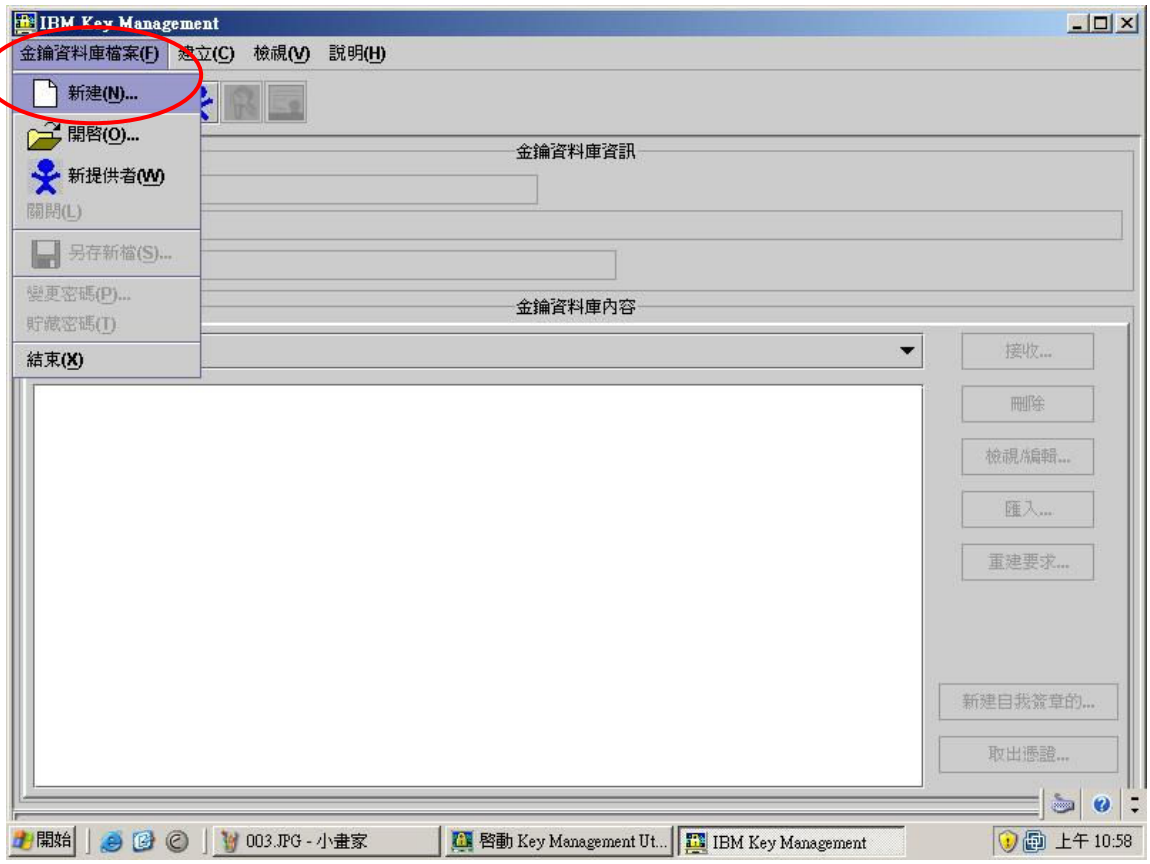
點選桌面左下角開始→程式集(或所有程式)→IBM HTTP Server 6.0.1→啟動 Key Management Utitlity。



4.2.2 建立新的金鑰資料庫

金鑰資料庫是伺服器用來儲存一或多個密碼組合與認證的檔案。您可將某個金鑰資料庫用於所有的密碼組合及認證，或建立多個資料庫。

金鑰資料庫檔案→新建→金鑰資料庫類型。

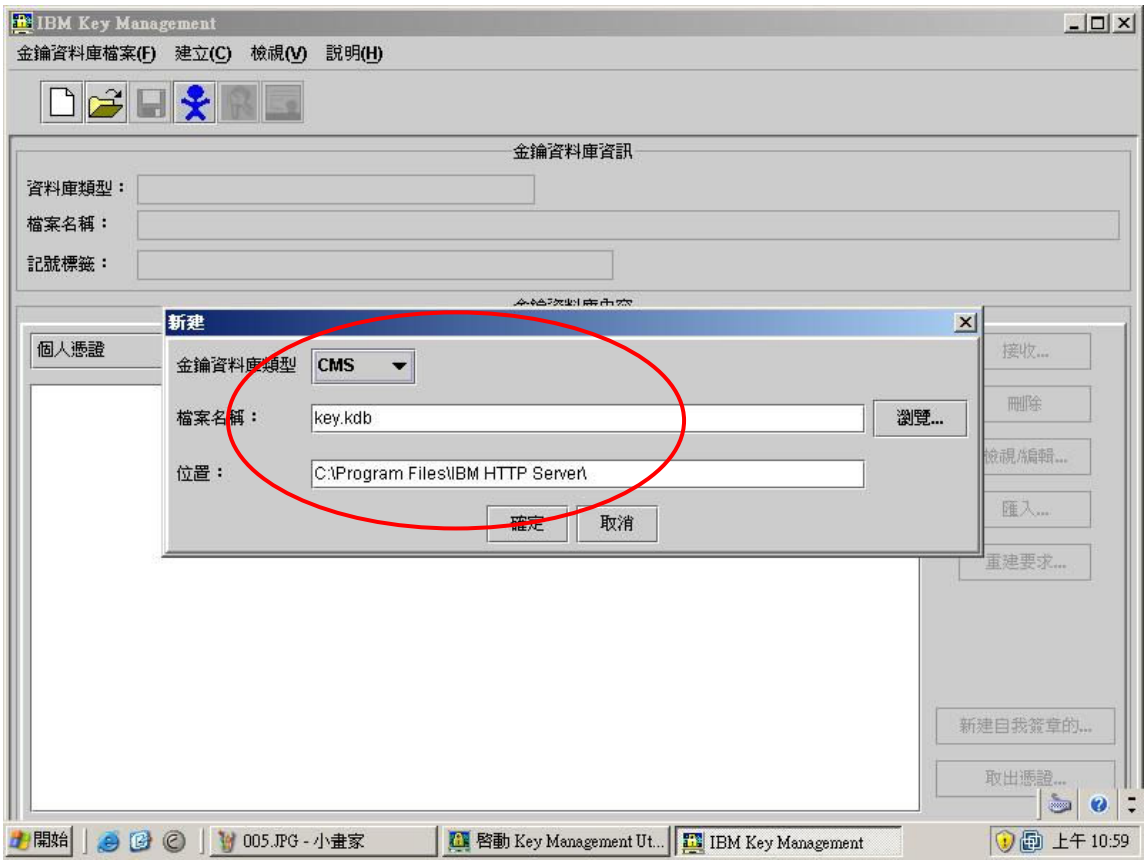


說明：

金鑰資料庫類型：請選擇 CMS

路徑：C:\Progran Files\IBM HTTP Server

檔名：key.kdb（副檔名 KDB 為預設值）



4.2.3 設定金鑰資料庫密碼

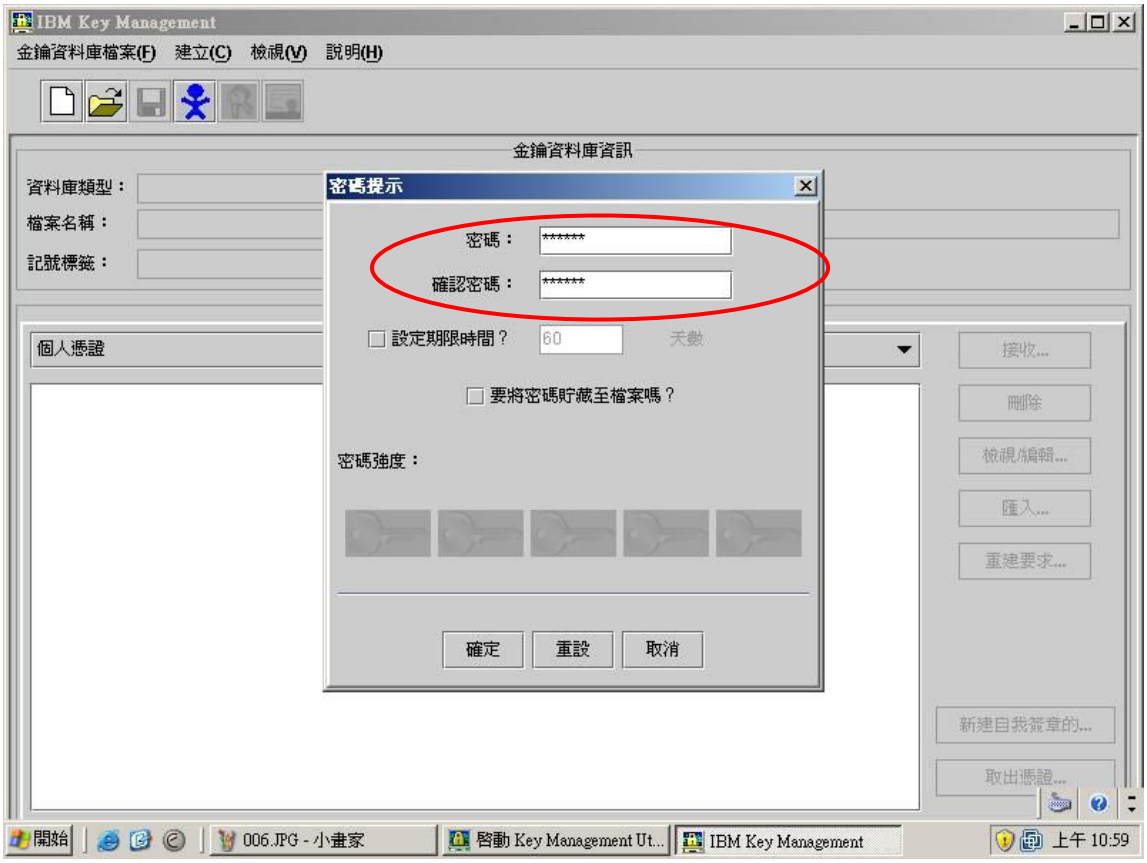
當您建立新的金鑰資料庫時，您會指定金鑰資料庫密碼。這個密碼非常重要，因為他會保護專屬密碼。專屬密碼是唯一可以簽認文件或將公用密碼加密之訊息解密的密碼，最好是能常常變更金鑰資料庫的密碼。

指定密碼時請遵循下列指示：

（1） 通行碼必須是英文字母（含大小寫）、數字或特殊字元

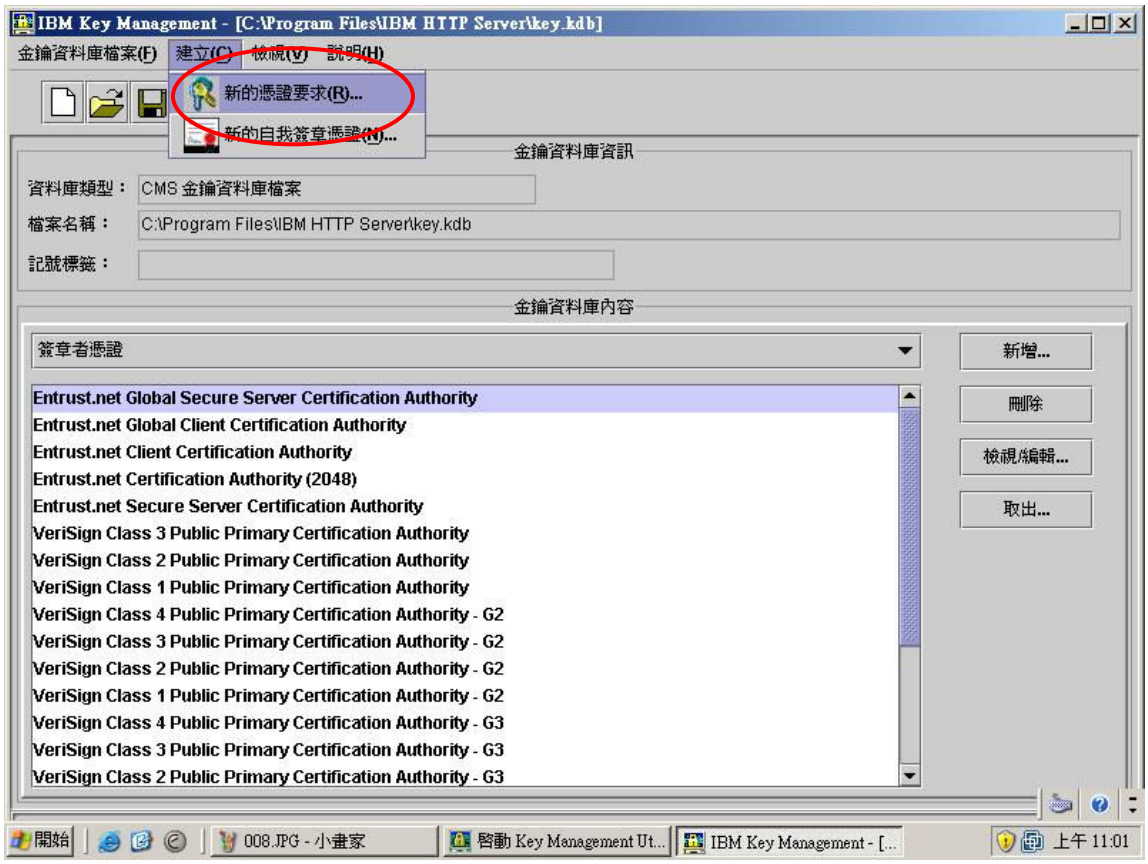
（2） 通行碼至少必須為六個字元，並且至少包含二個非連續的號碼。確定通行碼不是由一般可取得的資訊所組成；例如，關於您自己、配偶或子女的姓名字首及生日。

（3） 隱藏通行碼。



4.2.4 建立新憑證

建立➔新的憑證要求。



4.2.5 輸入憑證相關資訊

以下欄位會出現在憑證內容之中，全部都需要，且必須以英文填寫，請小心填寫！各欄位說明如下：

(1) 金鑰標籤：可自訂，要用來識別資料庫中的密碼及認證的說明備註。

(2) 金鑰大小：請選擇 **2048** 位元長度。

(3) **共用名稱：網站名稱(如：www.twca.com.tw，不必加 http://或 https://)**

(4) 組織：使用該憑證之組織或公司名稱。(如：TWCA)

(5) 部門（選用）：使用該憑證之單位名稱。(如： SYSTEM)

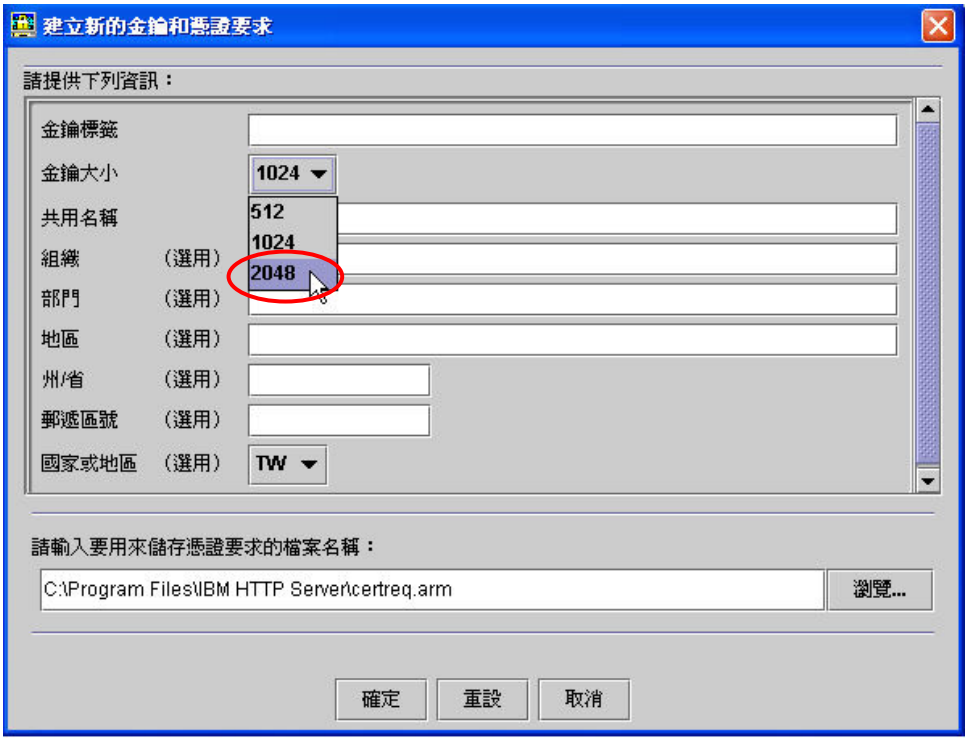
(6) 地區（選用）：城市全名（如：Taipei）

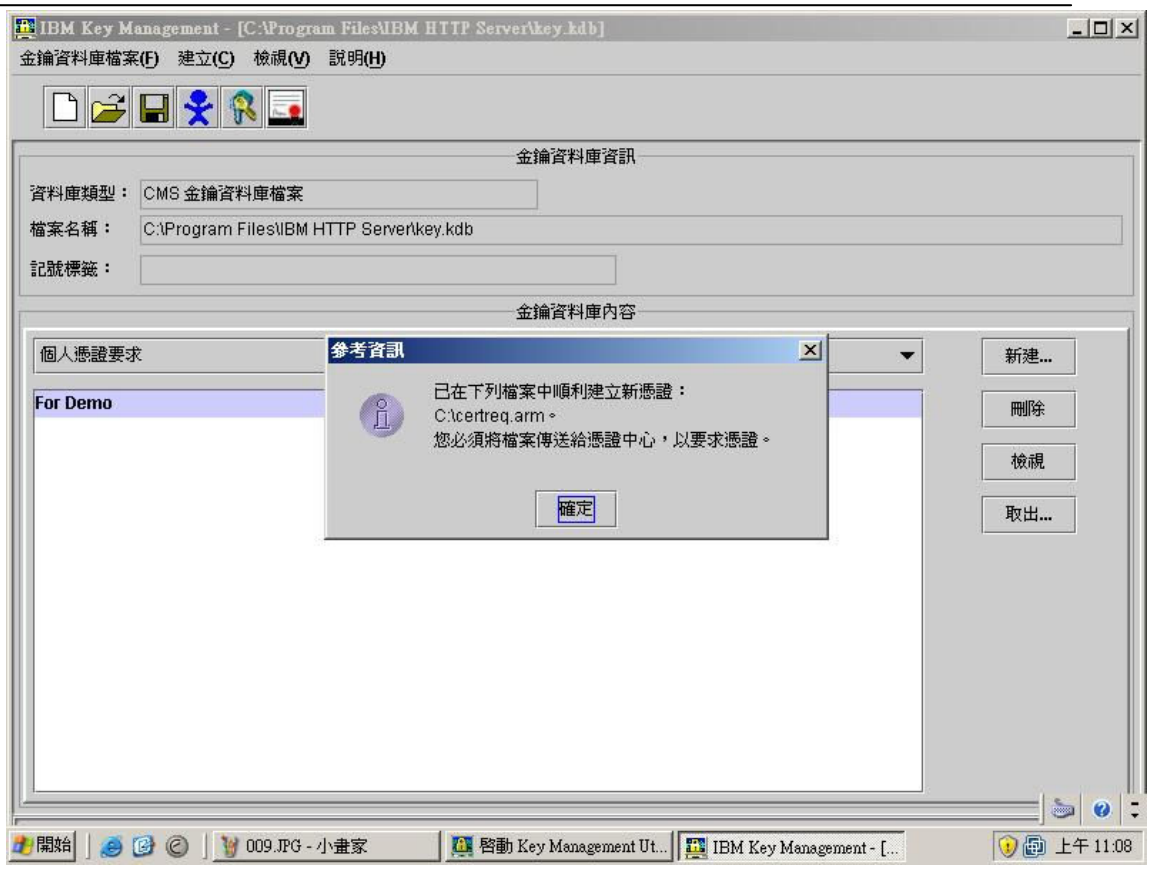
(7) 州／省（選用）：國家全名（如：Taiwan）

(8) 郵遞區號：聯絡地址的郵遞區號。

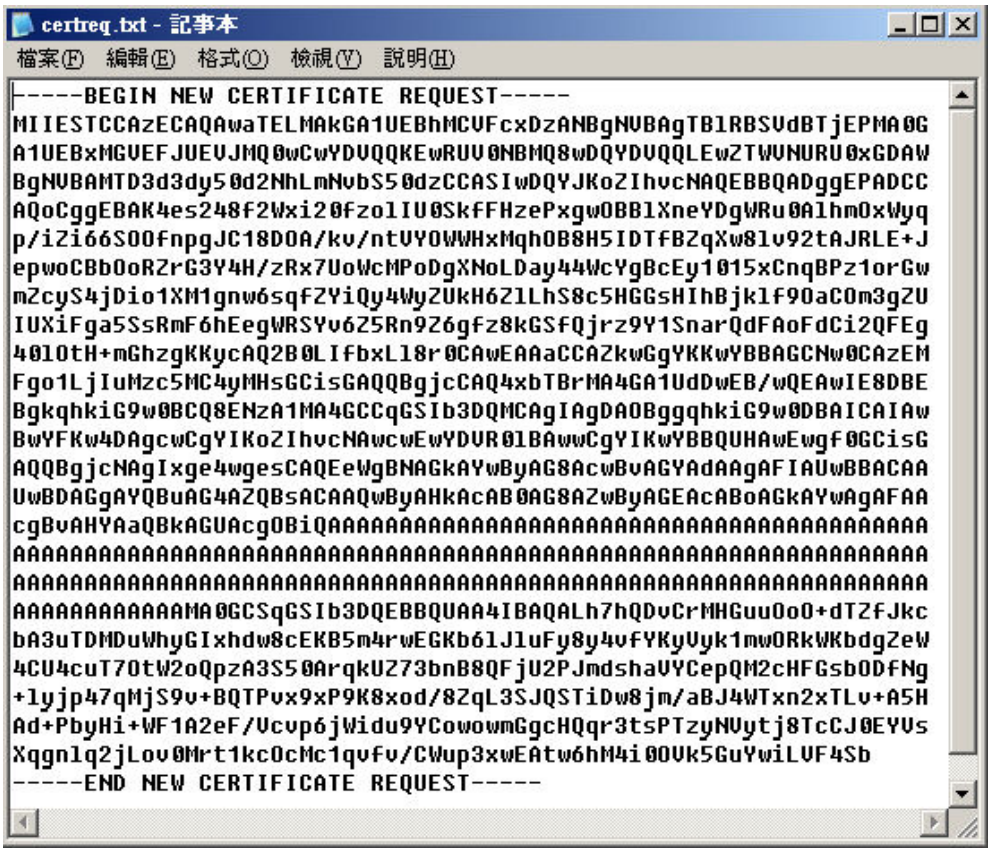
(9) 國家或地區：兩碼之國碼（如：臺灣為 TW）

(10) 請輸入要用來儲存憑證要求的檔案名稱：(如：C:\certreq.arm)





4.2.6 利用記事本開啟憑証請求檔 CSR，內容範例如下圖所示。



4.3 將製作好的憑證請求檔(CSR)上傳

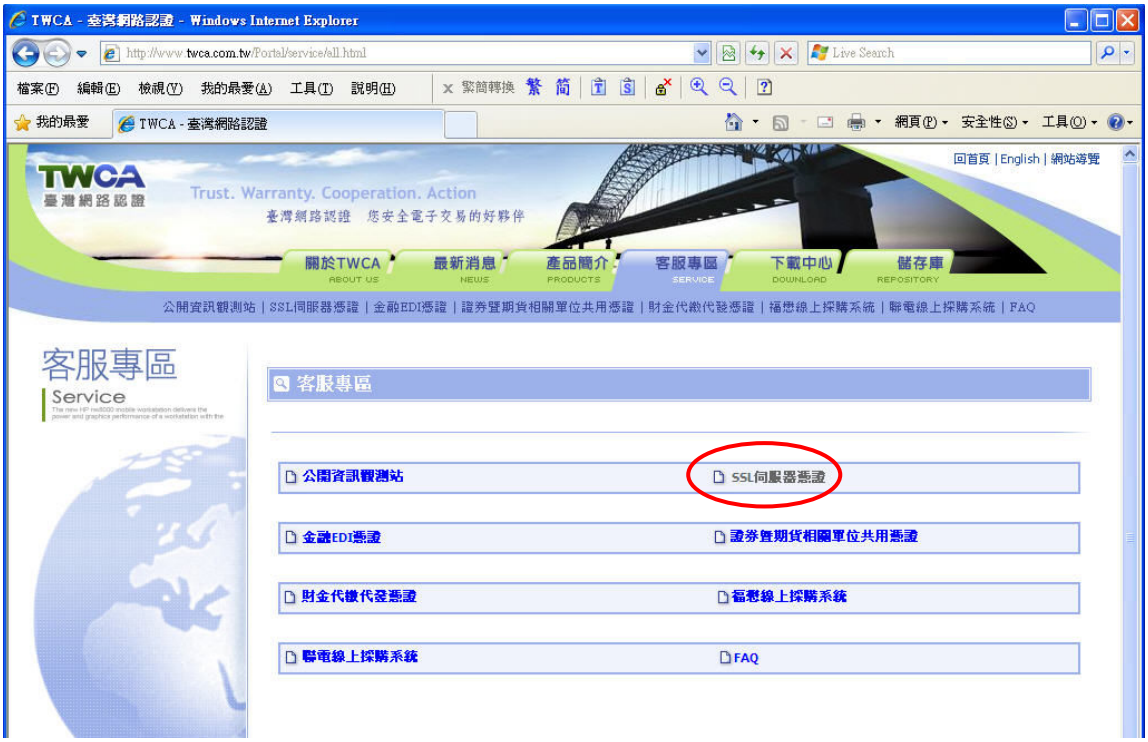
4.3.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw

點選右上方圖示憑證申請展期或註銷請由此進入。

4.3.2 連接 TWCA 網站(2)

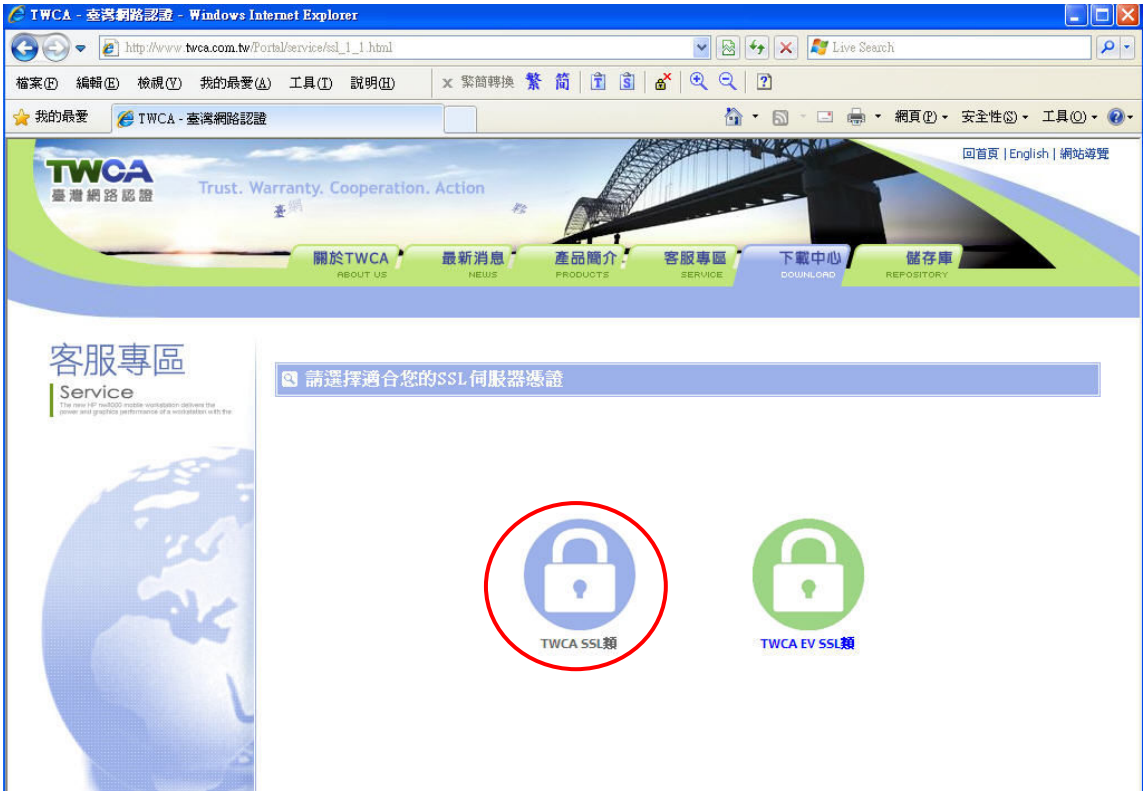
點選 SSL 伺服器憑證。



4.3.3 連接 TWCA 網站(3)

點選 TWCA SSL 類。

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。

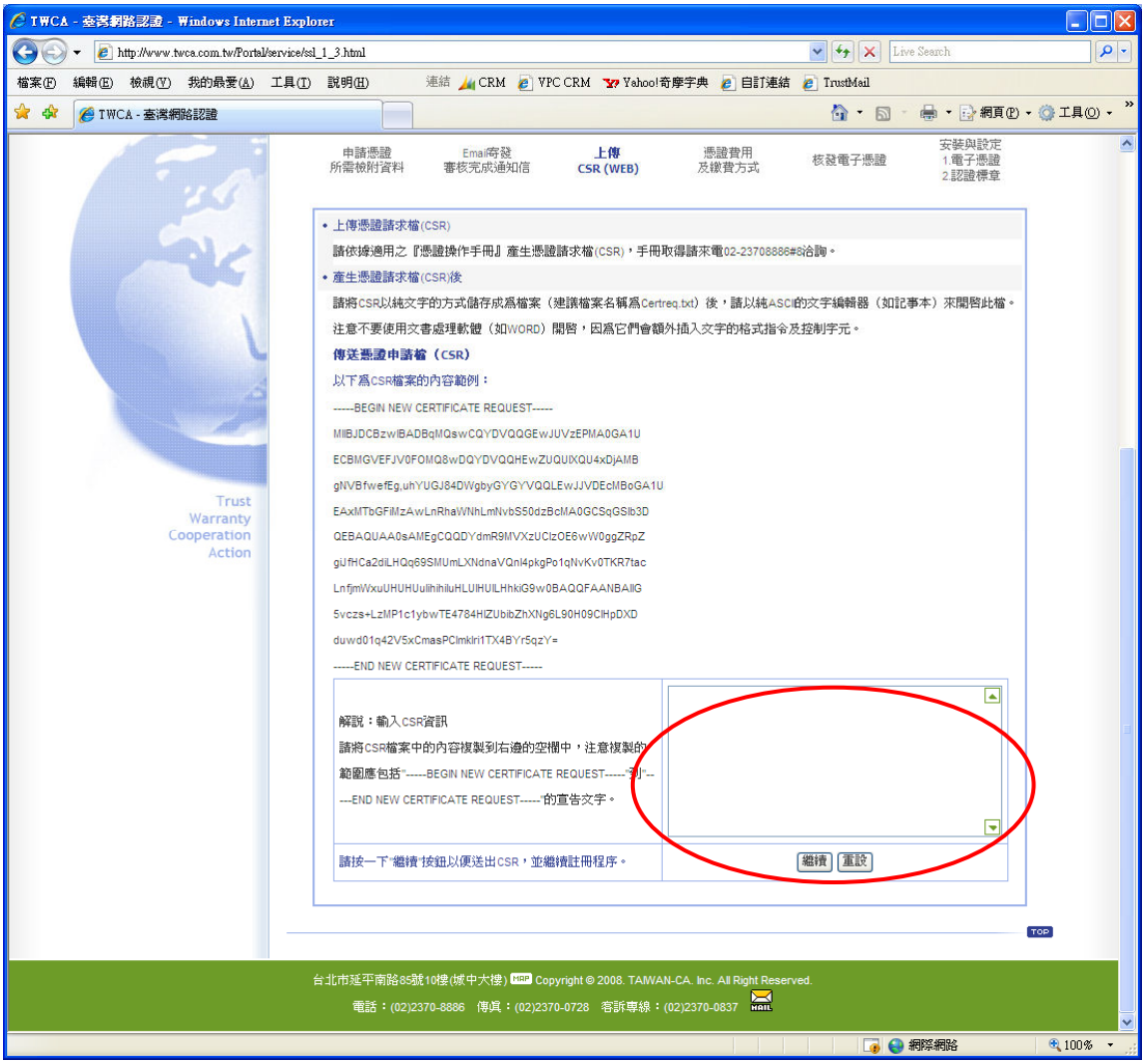


4.3.4 連接 TWCA 網站(4)

點選上傳 CSR（WEB）。

4.3.5 貼上憑證請求檔

將瀏覽器視窗畫面往下拉，開啟在 4.2 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。



4.3.6 再次檢視上傳之憑證請求檔案內容

4.3.7 填寫聯絡人基本資料

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)。

請輸入伺服器資訊

伺服器軟體廠商： 請從右邊的下拉式選單中選擇您伺服器軟體的廠商。如果不在清單中，請選擇其他。	Microsoft IIS
通行密碼：(至少六碼) 請在右邊的欄位中輸入一個您容易記憶，但不易為人所臆測的文字或片語。當您 申請、 更新或 註銷此SSL伺服器憑證時都需使用到這個通行密碼。另外，當您對本公司提出技術支援服務時，本公司亦會要求您提供此通行密碼。若有必要，請將此密碼記錄下來，並儲存在安全的地方。	輸入密碼： 再輸入一次密碼以確認：

請輸入技術聯絡人資訊

請輸入本公司寄送SSL伺服器憑證給您時的技術聯絡人資訊於下表。舉例來說，此人可以是您的網站管理者，或是您網路搬接商的技術支援人員。

請注意此人必須擁有存取您網頁伺服器的權利。本公司在發放SSL伺服器憑證以前，會先以電話與此技術聯絡人取得聯繫。

當網頁伺服器的安全出現顧慮時，此技術聯絡人有通知本公司的義務。

另若有憑證更新的訊息，本公司也會寄送給技術聯絡人及　貴公司的業務聯絡人。

姓名	
職稱	
公司	
統一編號	
通訊地址	台北市 郵遞區號：
聯絡電話	
傳真號碼	
電子郵件地址	

請輸入業務聯絡人資訊

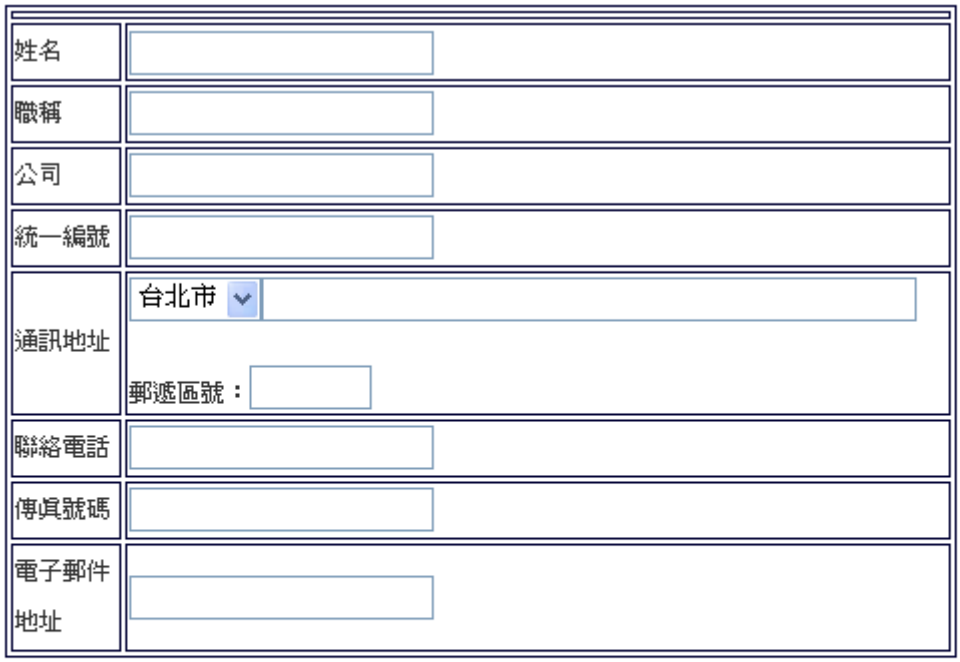
請輸入　貴公司負責SSL伺服器憑證業務聯絡人資訊於下表，並填寫本公司所要求的資訊。

舉例來說，此人可以是　貴公司的決策者或是高階的經理人。

請注意業務聯絡人必須為　貴公司組織內之一份子。本公司在發放SSL伺服器憑證以前，會先以電話與此業務聯絡人取得聯繫。

業務聯絡人與技術聯絡人不應為同一人，您應該分別指定。

另外，本公司若有更新的資料也會同時寄給上述這兩個人。



請輸入帳務聯絡人資訊

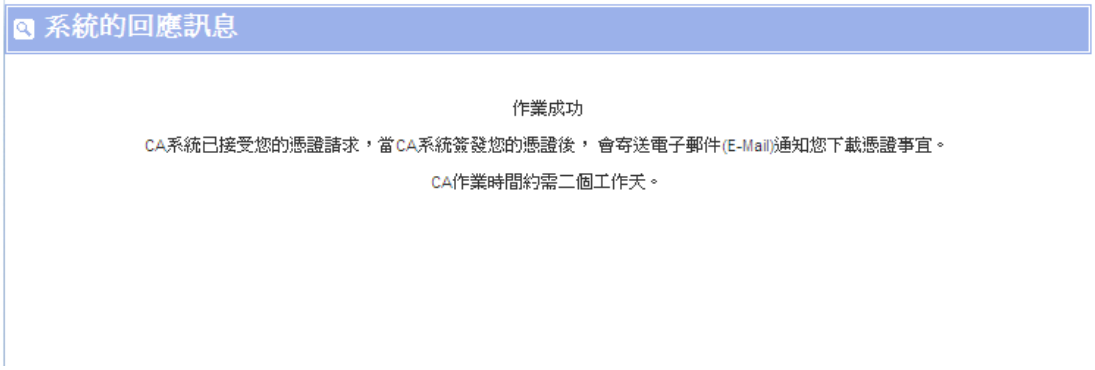
請輸入　貴公司的帳務處理聯絡人員資訊。

舉例來說，該人可以是　貴公司會計或是財務主管。

當帳單處理資料有異動時，此人有通知本公司之義務。

4.3.8 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，三個工作天內會完成資料審查作業，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。



4.4 下載已核發憑證

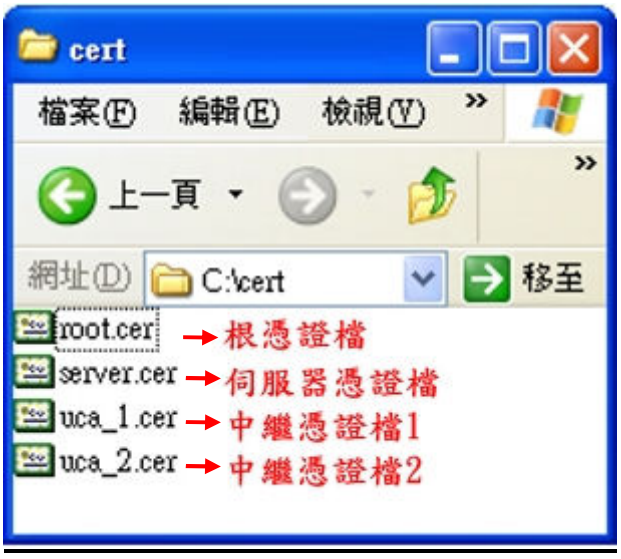
1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經過審驗通過，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，可得到三個或四個憑證鏈檔。

※如解壓縮後得到三個憑證鏈檔，內容及憑證用途如下圖所式：

※如解壓縮後得到四個憑證鏈檔，內容及憑證用途如下圖所式：



2 檔案下載說明

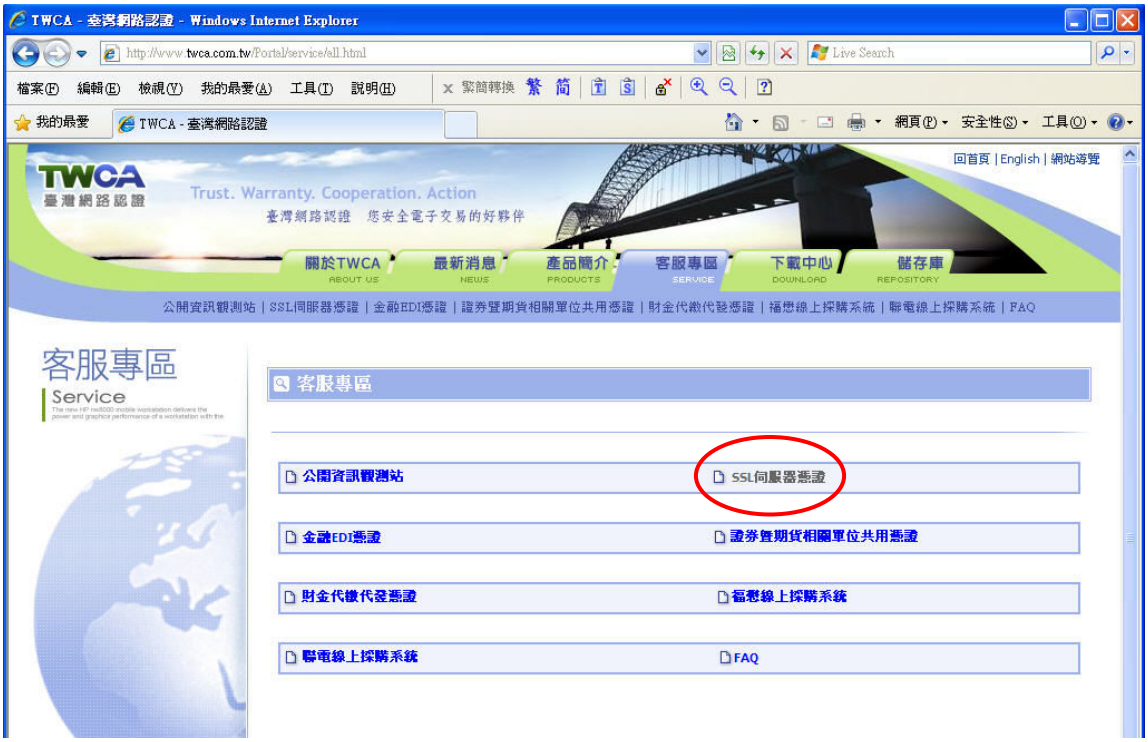
如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

4.4.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw，點選右上方憑證申請展期或註銷請由此進入。

4.4.2 連接 TWCA 網站(2)

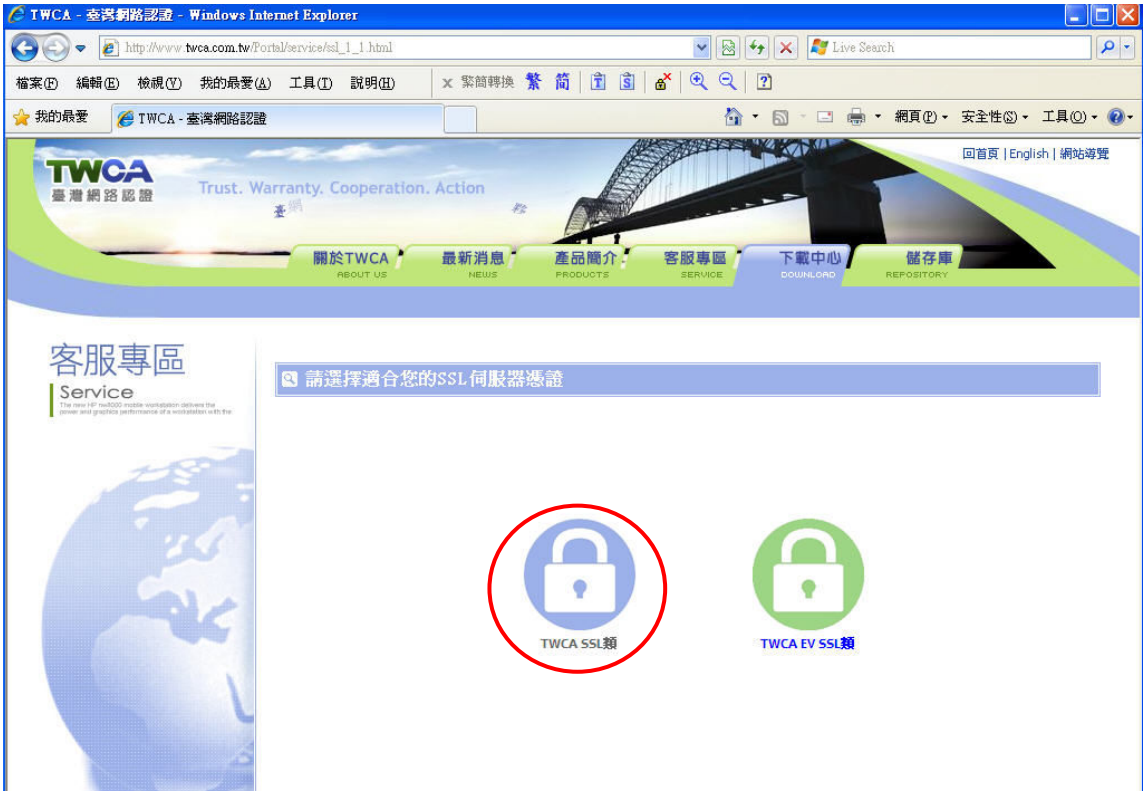
點選 SSL 伺服器憑證。



4.4.3 連接 TWCA 網站(3)

點選 TWCA SSL 類。

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。



4.4.4 連接 TWCA 網站(4)

點選憑證搜尋。

4.4.5 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。

4.4.6 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，按下儲存，儲存憑證鏈壓縮檔 cert.zip。

4.5 安裝憑證

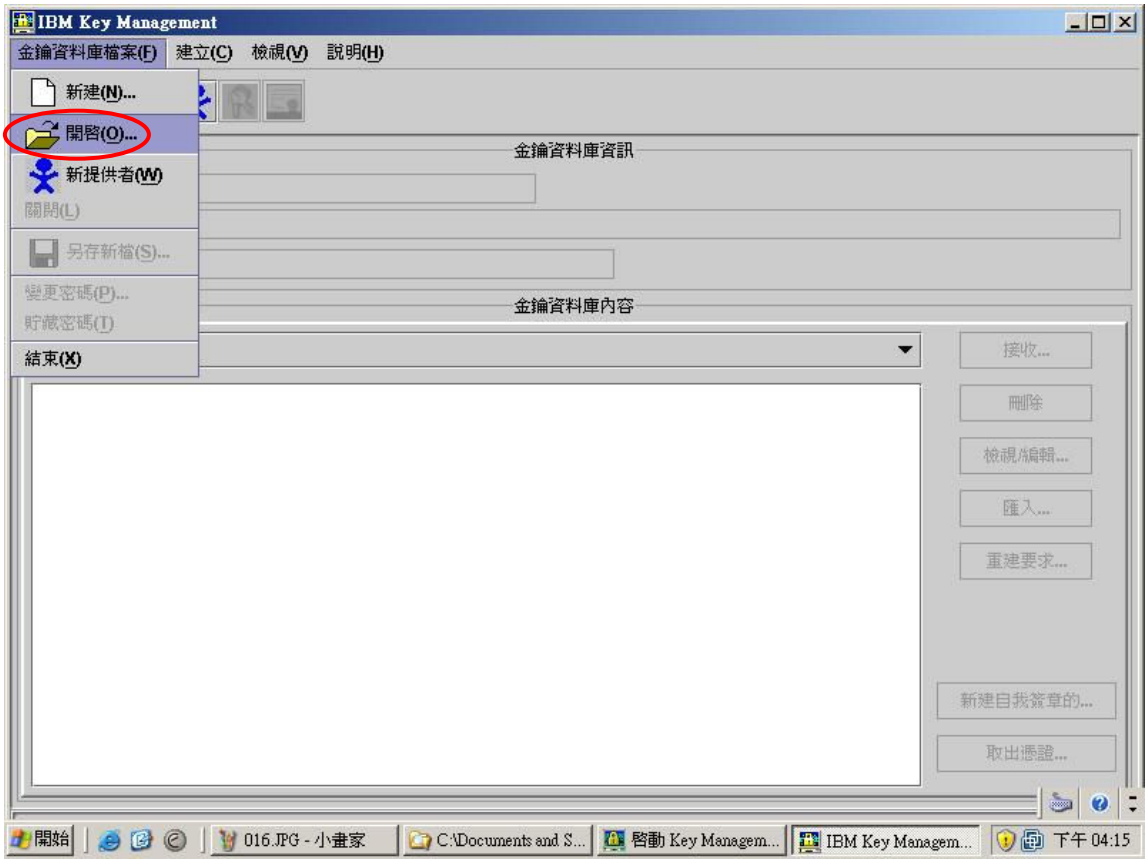
※在安裝憑證的過程中，必須依照根憑證➔中繼憑證➔自我憑證的順序安裝！

4.5.1 儲存憑證

請參照 4.4 章節相關步驟，將伺服器憑證檔（server.cer）、中繼憑證檔（uca.cer）及根憑證檔（root.cer）儲存於電腦可存取位置。

4.5.2 開啟金鑰資料庫

點選桌面左下角開始→程式集(或所有程式)→IBM HTTP Server 6.0.1→啟動 Key Management Utitlity→金鑰資料庫檔案→開啟。

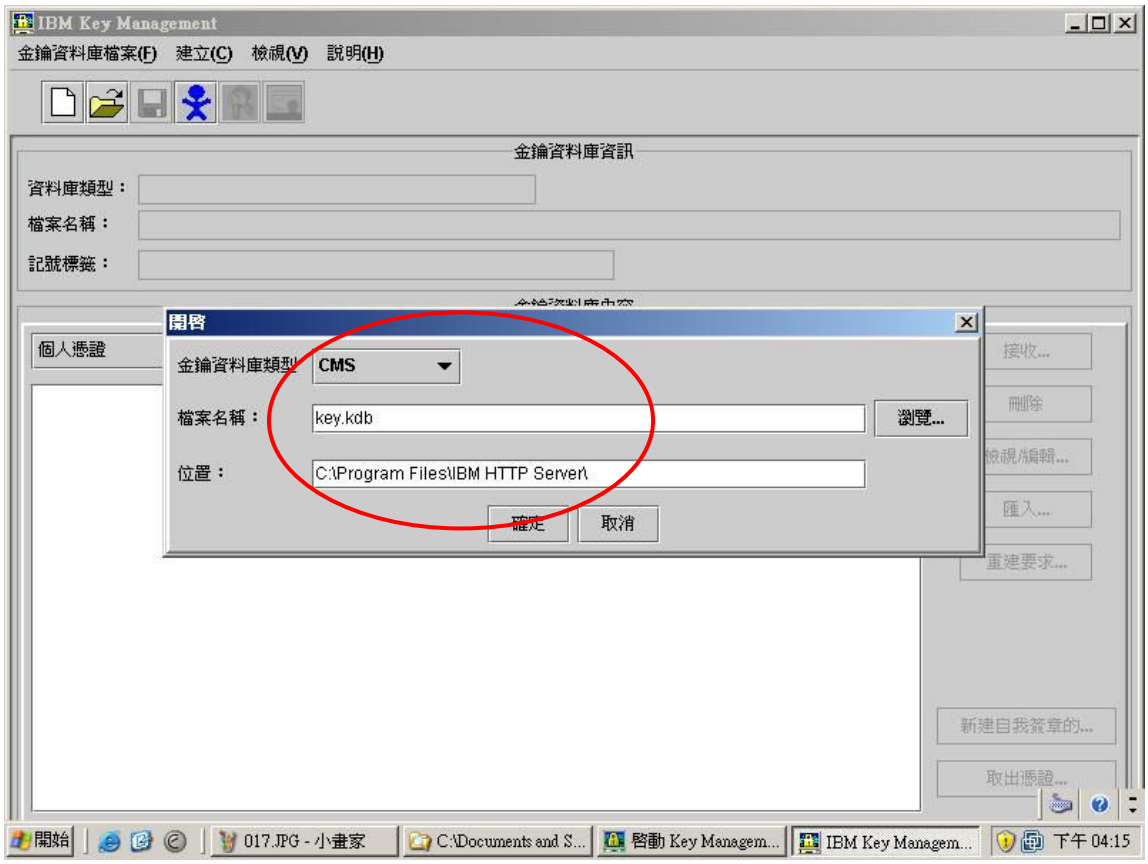


4.5.3 選擇金鑰資料庫檔案

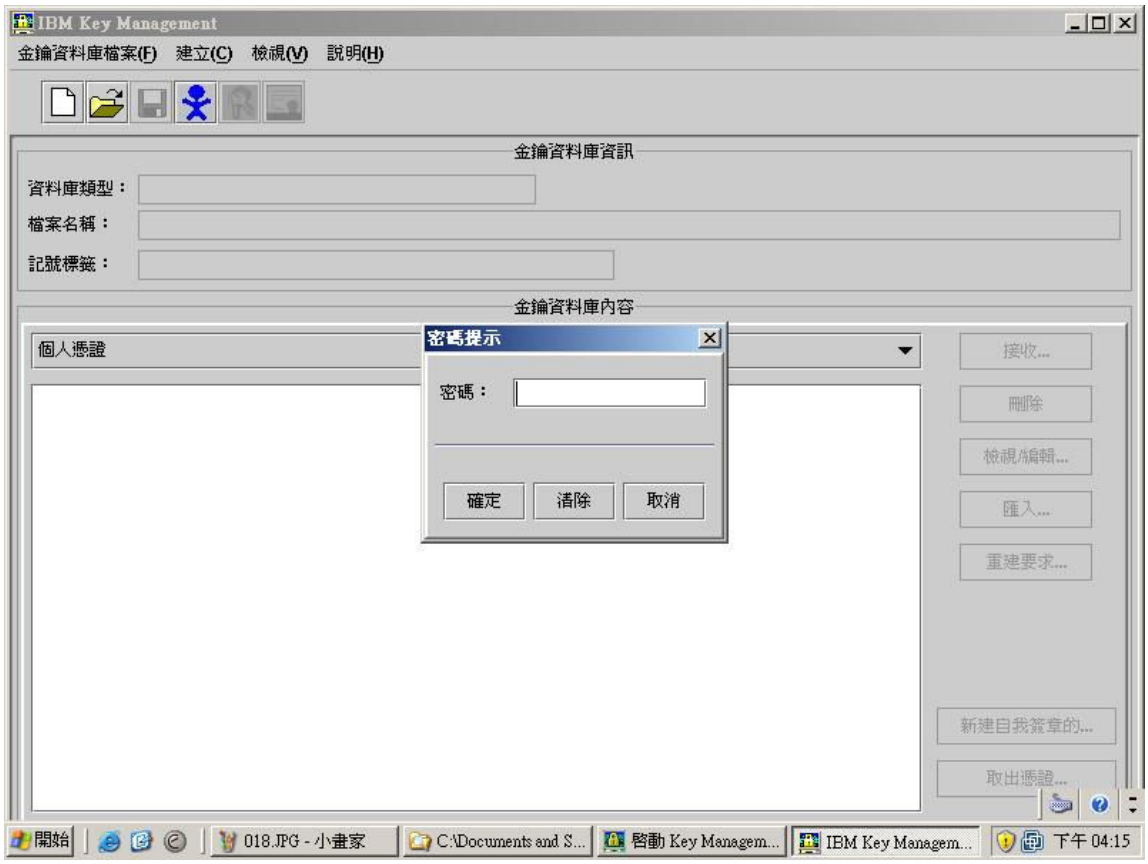
金鑰資料庫類型：請選擇 CMS

路徑：C:\Progran Files\IBM HTTP Server

檔名：key.kdb

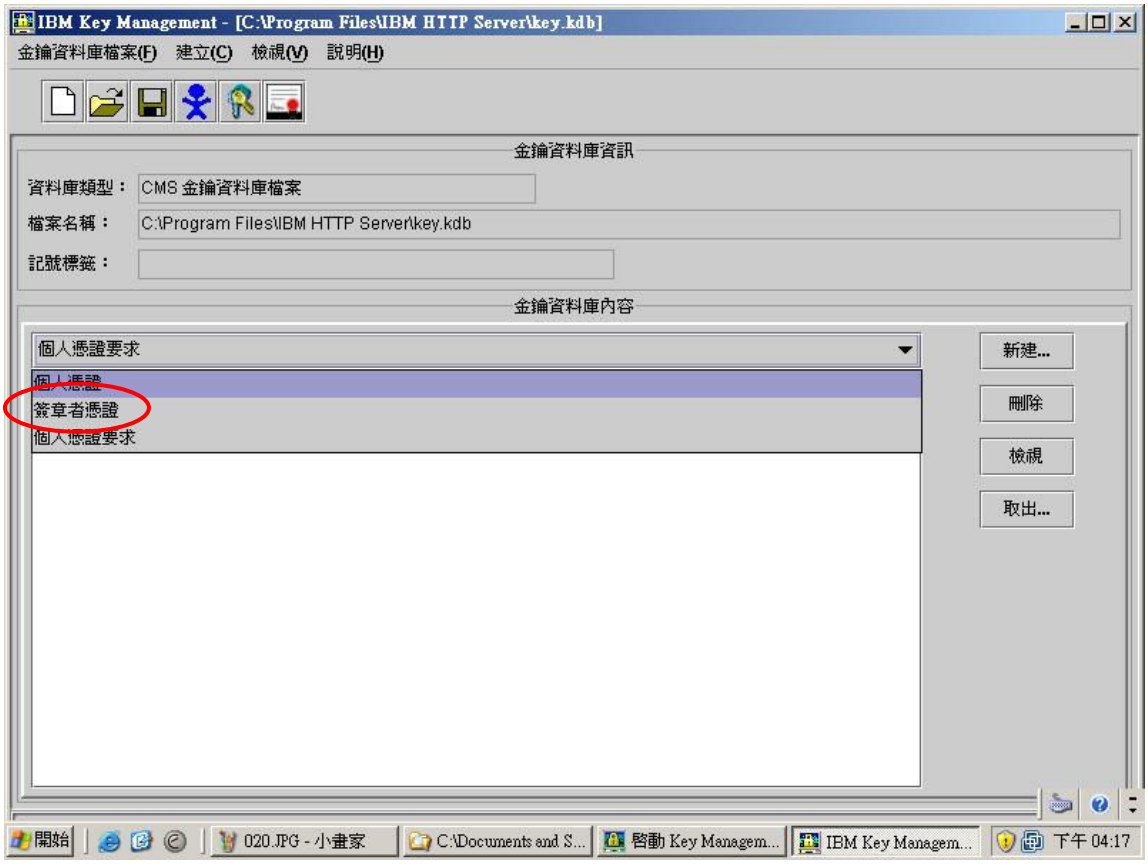


4.5.4 輸入金鑰資料庫檔案密碼



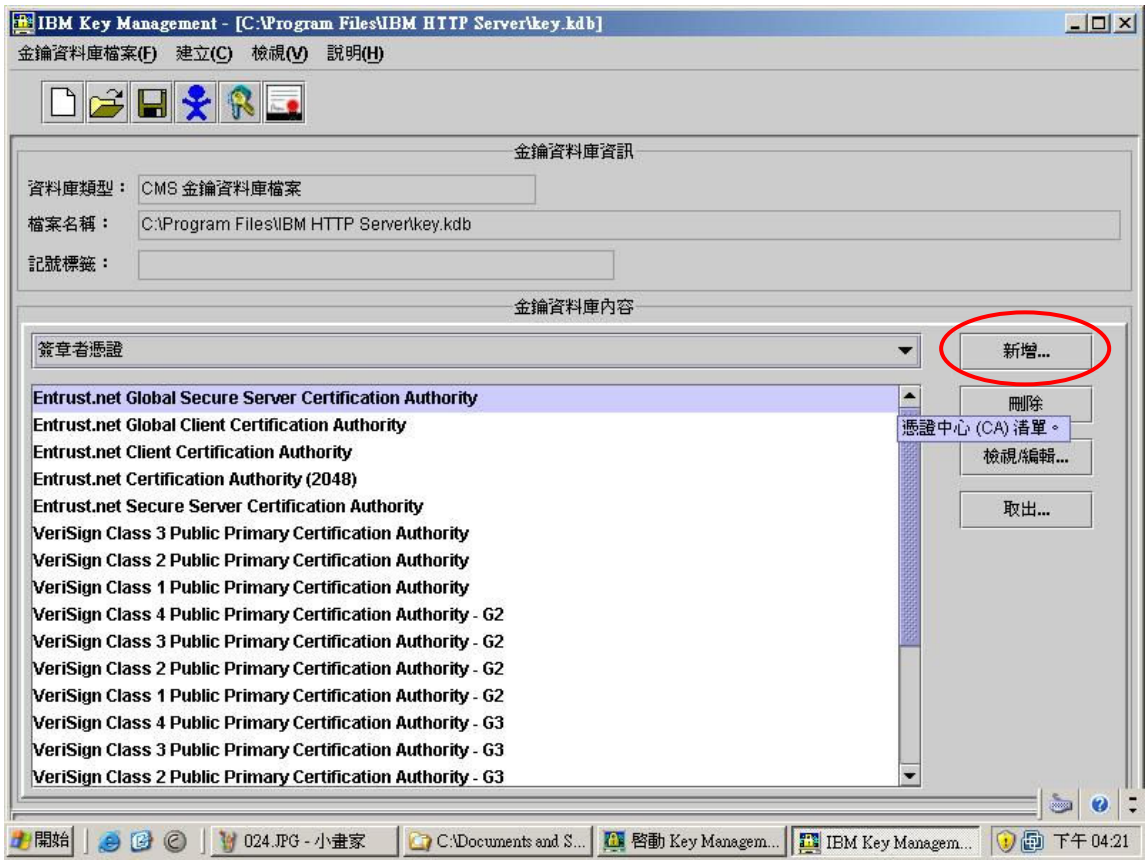
4.5.5 選擇簽章者憑證

於金鑰資料庫內容選擇簽章者憑證



4.5.6 新增簽章者憑證

點選新增

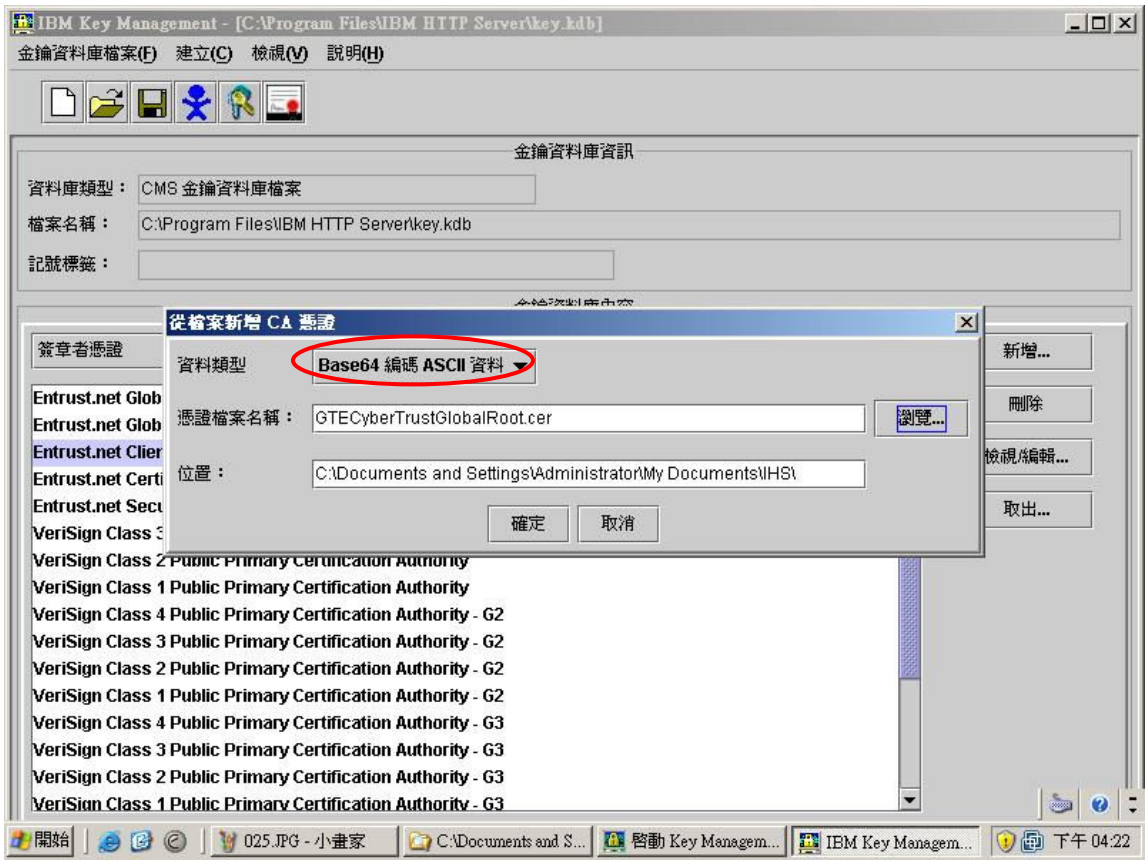


4.5.7 安裝根憑證

資料類型：Base64 編碼 ASCII 資料

憑證檔案名稱：請選擇 4.5.1 章節準備的根憑證檔案（root.cer）

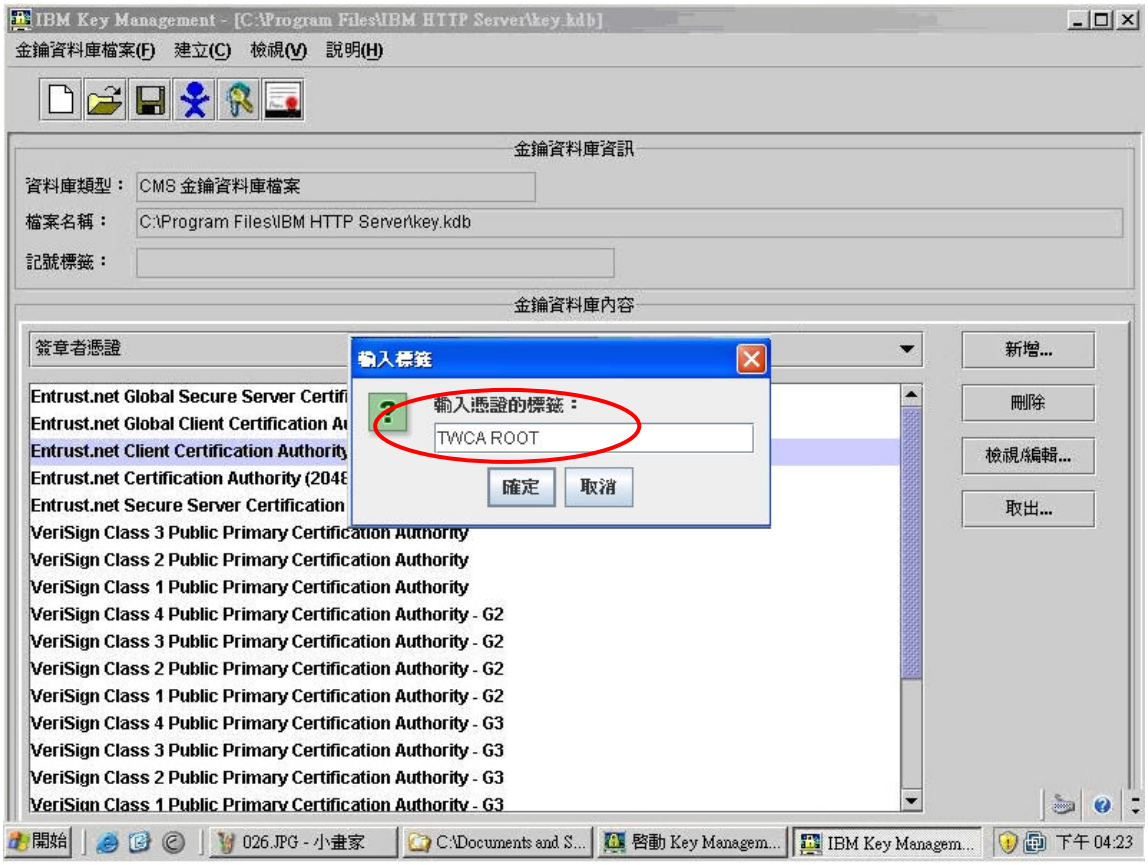
位置：請選擇 4.5.1 章節準備的根憑證檔案路徑



4.5.8 輸入根憑證說明文字

請輸入憑證標籤名稱，名稱可自訂，例如：TWCA ROOT

點選確定，完成根憑證安裝。



4.5.9 安裝中繼憑證

點選新增

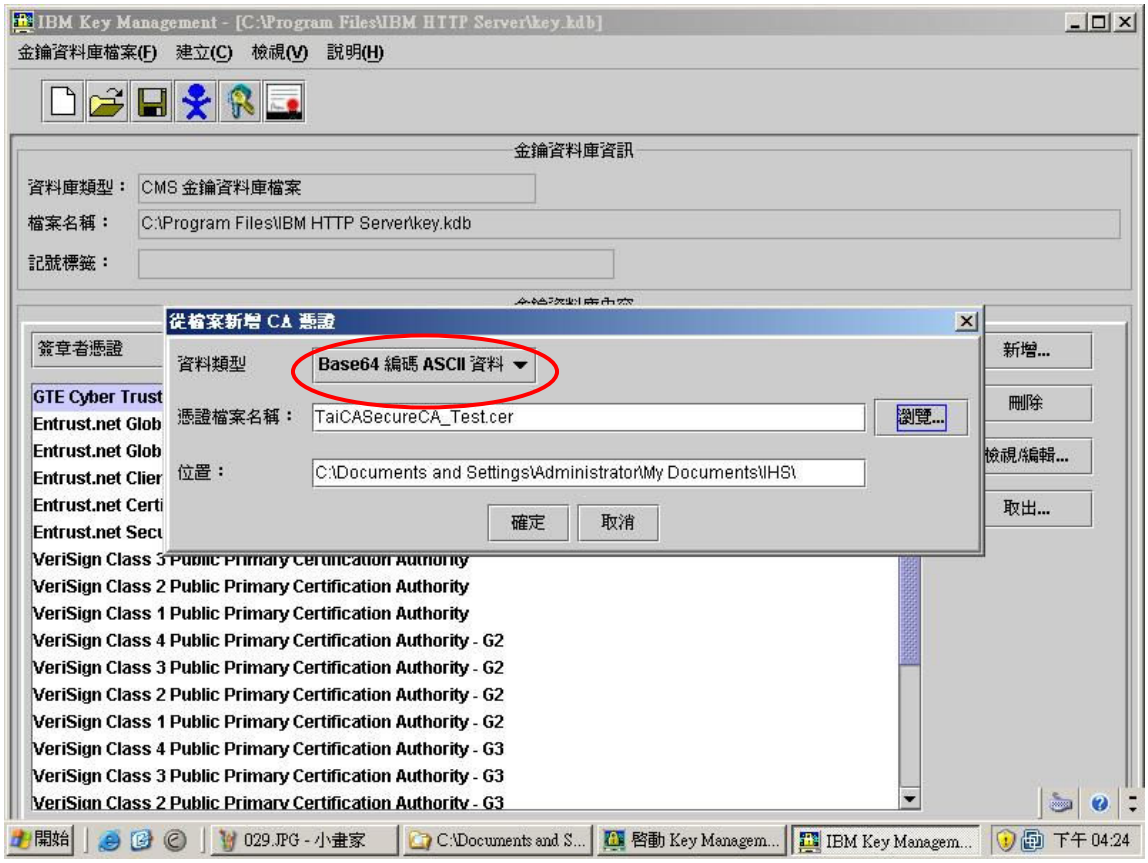
說明：

資料類型：Base64 編碼 ASCII 資料

憑證檔案名稱：請選擇 4.5.1 章節準備的中繼憑證檔案（uca.cer）

位置：請選擇 4.5.1 章節準備的中繼憑證檔案路徑

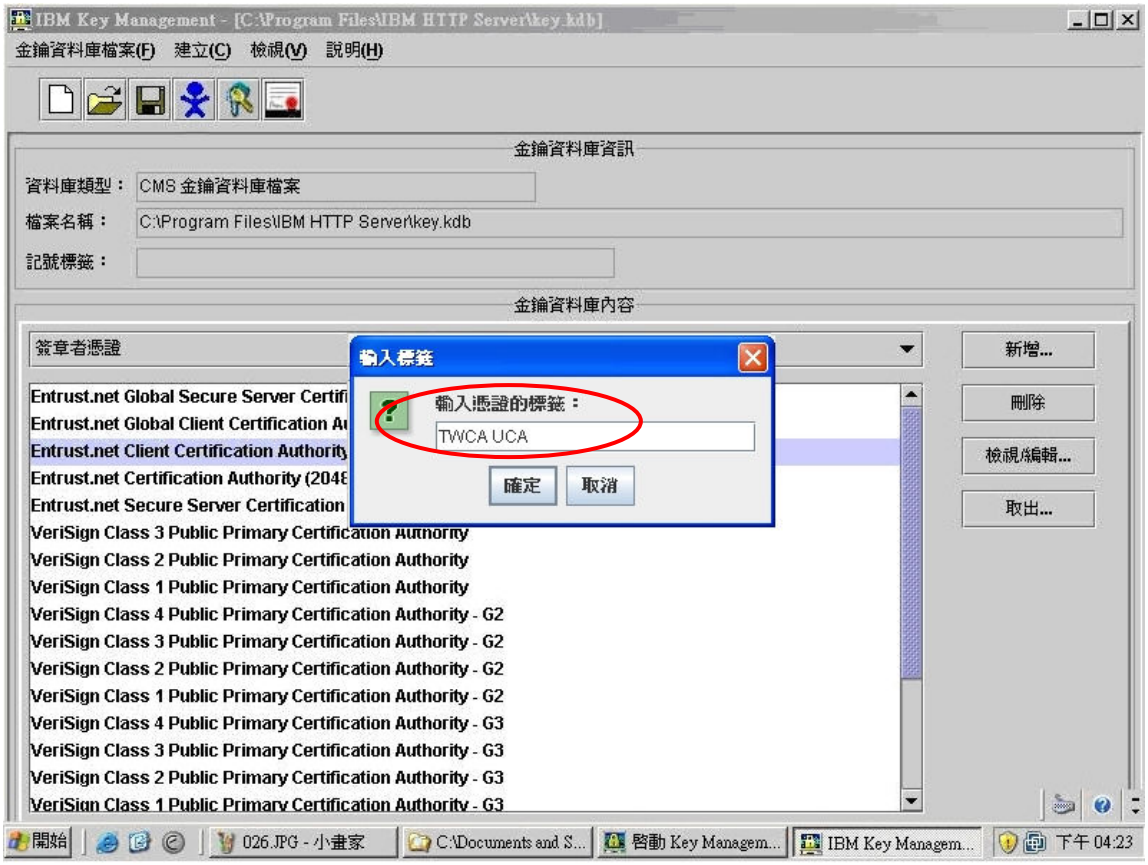
※如 4.4 章節解壓縮後得到四個憑證鍵檔，請儲存兩張中繼憑證（uca_1.cer 與 uca_2.cer）於電腦中可存取位置，並重複以下步驟安裝。



4.5.10 輸入中繼憑證說明文字

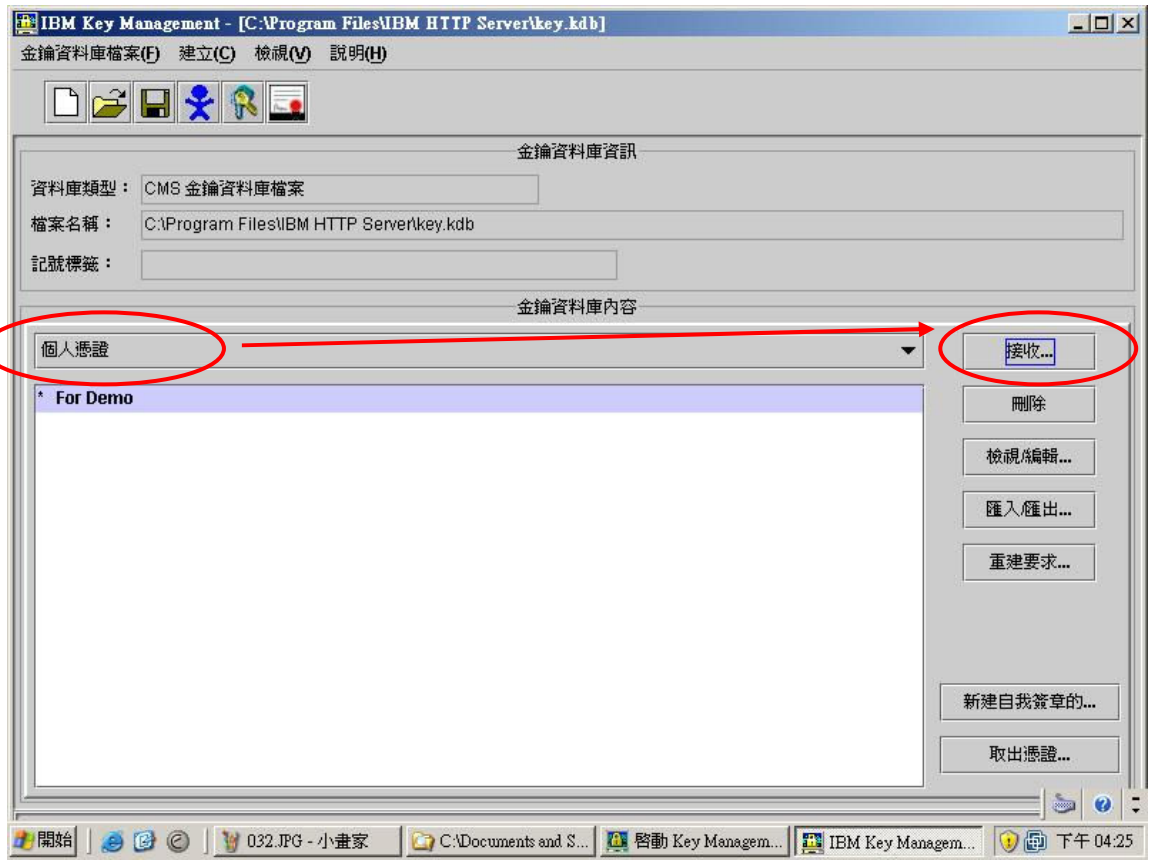
請輸入憑證標籤名稱，名稱可自訂，例如：TWCA UCA

點選確定，完成中繼憑證安裝。



4.5.10 安裝伺服器憑證

於金鑰資料庫內容選擇個人憑證→點選接收

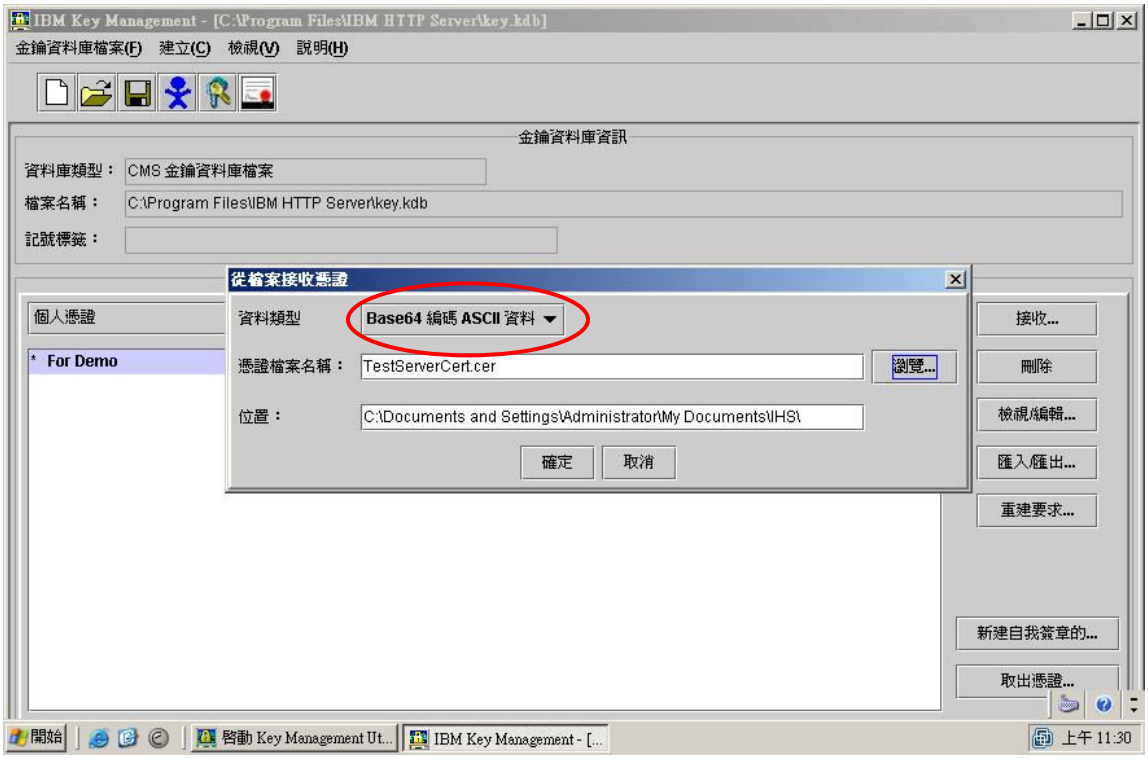


4.5.11 選擇伺服器憑證檔

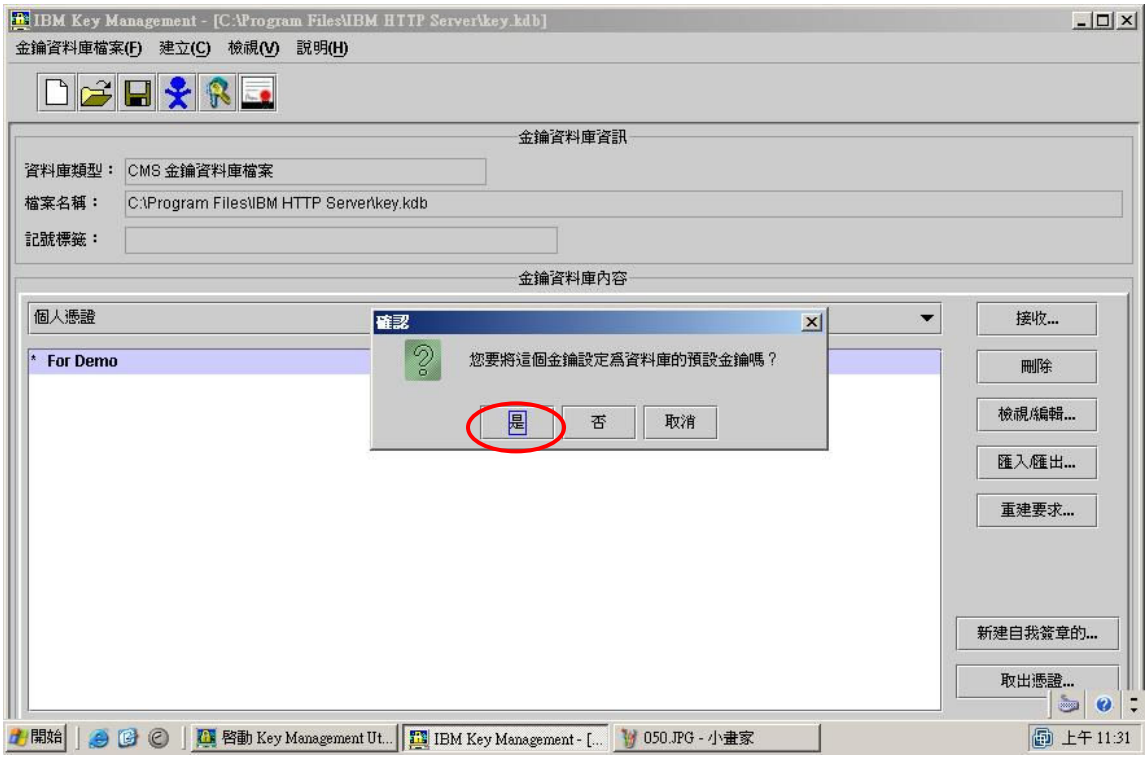
資料類型：Base64 編碼 ASCII 資料

憑證檔案名稱：請選擇 4.5.1 章節準備的伺服器憑證檔案（server.cer）

位置：請選擇 4.5.1 章節準備的伺服器憑證檔案路徑

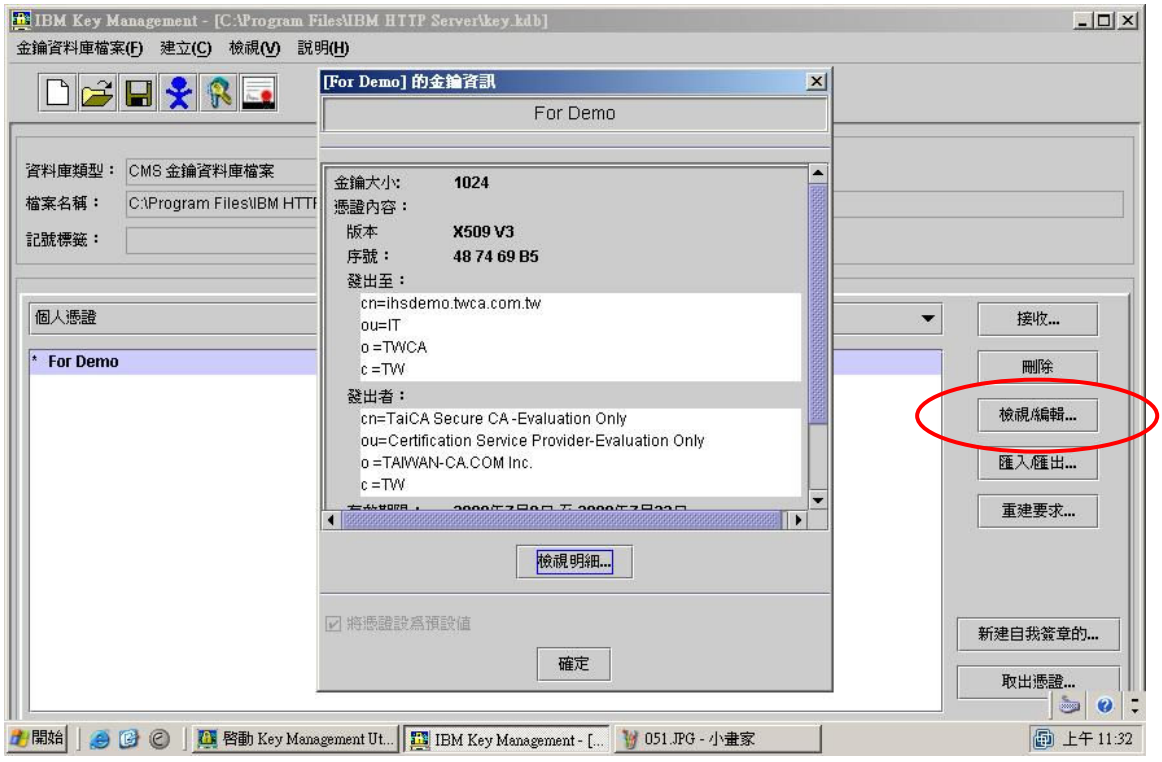


4.5.12 設定為預設金鑰



4.5.13 檢視憑證內容

點選檢視/編輯，確認憑證內容無誤。

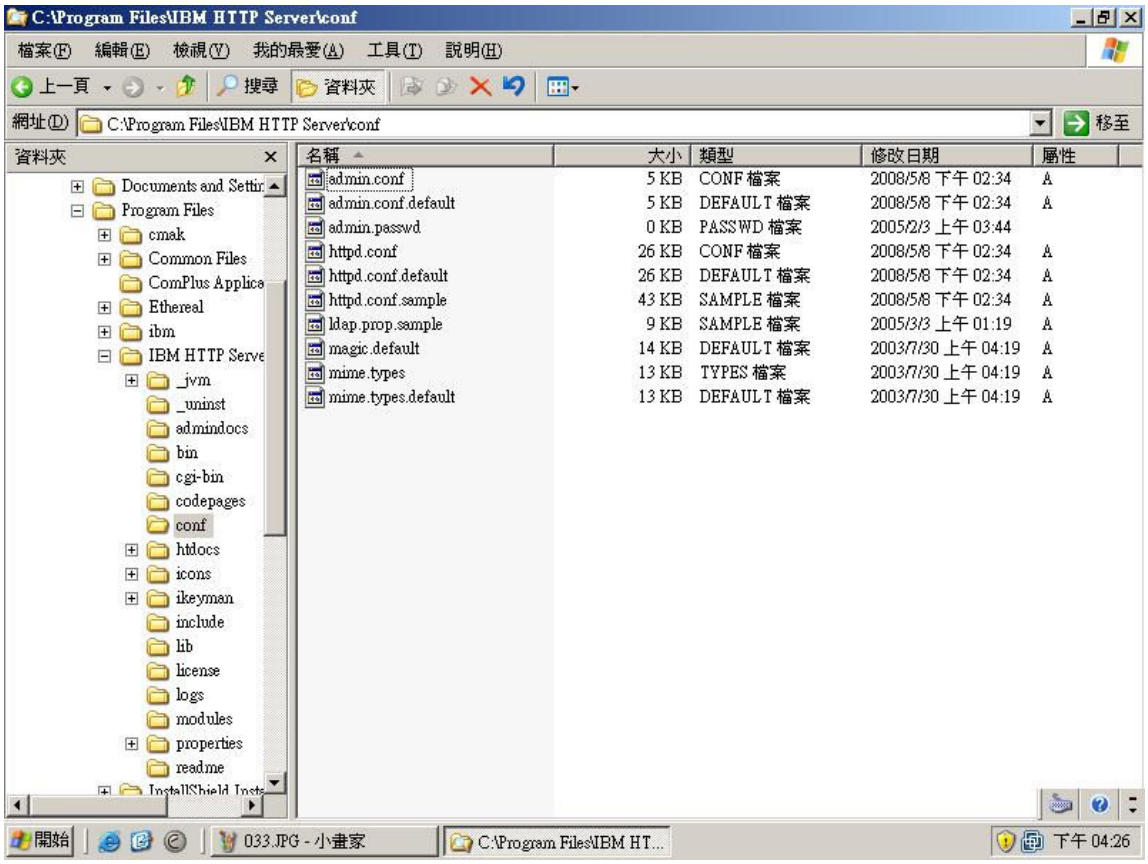


4.6 備份/還原憑證

4.6.1 進入檔案總管

由桌面→我的電腦→key.kdb 的儲存路徑

（預設值：C:\Progran Files\IBM HTTP Server）。



4.6.2 備份 key.kdb

將 key.kdb 複製到其他磁碟機或資料夾儲存。

4.6.3 還原 key.kdb

將 key.kdb 複製到 C:\Progran Files\IBM HTTP Server，並依照 4.5.2 至 4.5.4 章節步驟開啟。

4.7 設定 SSL 模式

4.7.1 停止 IBM HTTP Server 服務

※4.7.2～4.7.5 章節供首次申請 SSL 憑證設定使用，若已設定過，請直接跳至 4.7.6 章節設定。

4.7.2 變更目錄至 <IBM HTTP Server Root>>\conf 下

4.7.3 將 httpd.conf 更名成 httpd.conf.orig，httpd.conf.sample 更名成 httpd.conf

4.7.4 編輯 http.conf 並參考下列設定將其註解拿掉

LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll (Win32)
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so (UNIX)
AddModule mod_ibm_ssl.c
Listen 443
ServerName 主機名稱
<VirtualHost 申請憑證的網站名稱:443> (如：<VirtualHost www.taica.com.tw:443>)
SSLEnable
SSLClientAuth none
DocumentRoot <預設網站根目錄> (如：/usr/HTTPServer/www)
ErrorLog <error log 完整路徑> (如：/usr/HTTPServer/logs/error_log)
TransferLog <transfer log 完整路徑> (如：/usr/HTTPServer/logs/access_log)
</VirtualHost>
SSLDisable
Keyfile "憑證資料庫完整路徑" (如：drive:/IBM/IBM HTTP SERVER/ssl/keyfile.kdb)
SSLV3Timeout 1000

4.7.5 完成後，存檔離開

4.7.6 用管理者權限登入伺服器並執行 ikeyman 開啟金鑰管理工具

4.7.7 開啟 金鑰資料庫→開啟(新建)→選擇資料庫檔名(如：key.kdb)→輸入密碼後按確定

4.7.8 執行 金鑰資料庫→隱藏密碼

4.7.9 啟動 IBM HTTP Server 服務

4.8 更新 SSL 憑證

4.8.1 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 http://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。

4.8.2 更新步驟

請參照 4.2 至 4.7 章節步驟申請安裝憑證，即可完成 SSL 憑證更新。

5.附件

無。