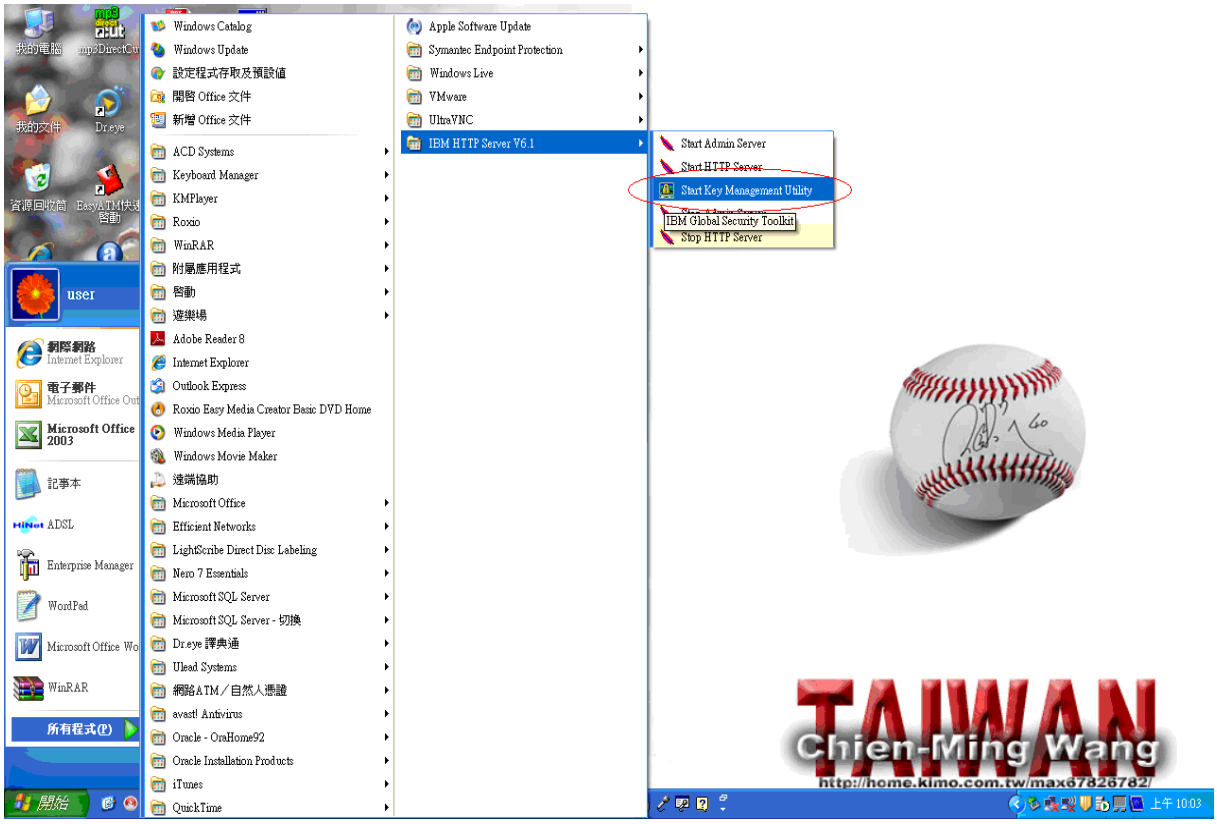
# 中華電信通用憑證管理中心(PublicCA)

## IBM HTTP Server SSL 憑證請求檔製作與 SSL 憑證安裝手冊



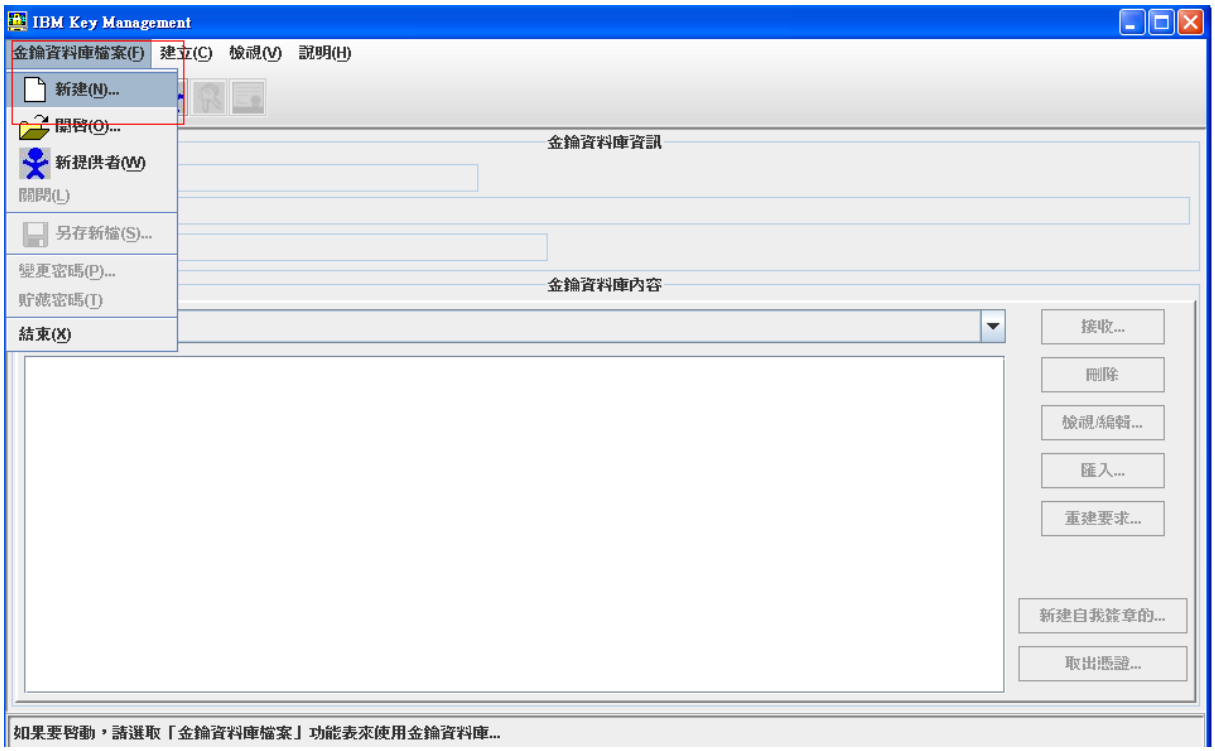
## 1. 產生「憑證請求檔」

「開始」→「程式集」→「IBM HTTP Server V6.1」→「Start Key Management Utility」



## 2. 啟動 IBM Key Management(IBM Server 的金鑰管理程式)

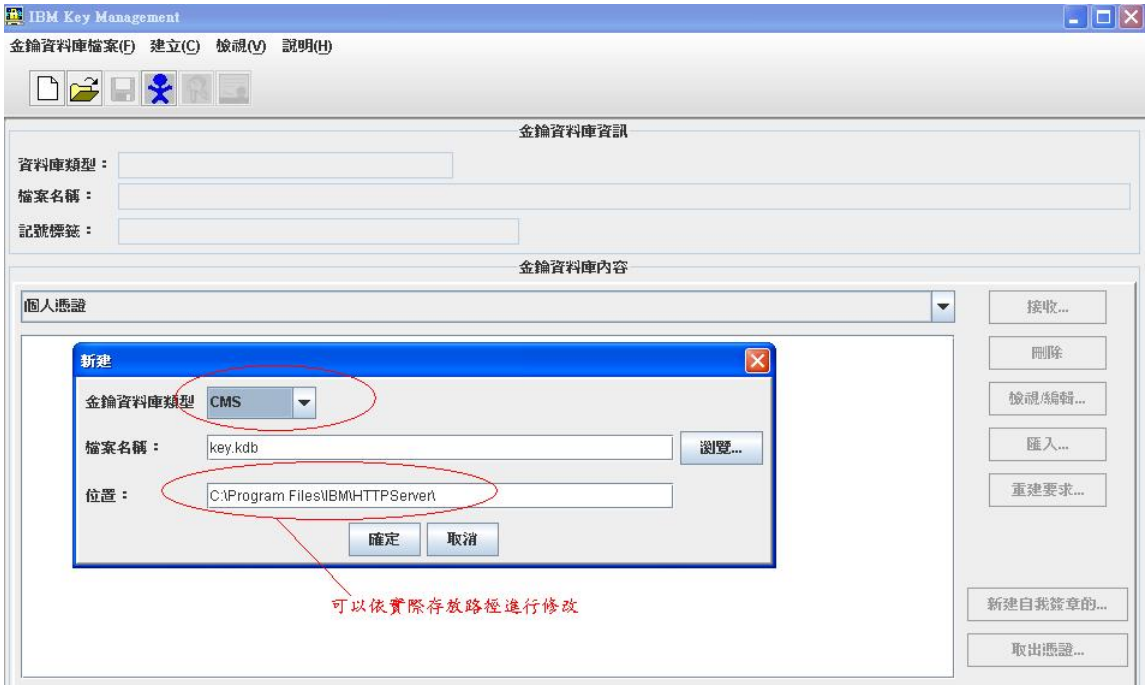
2-1 建立新的金鑰資料庫 :「金鑰檔案資料庫」→「新建」




2-2 選擇資料庫型態：『CMS』

檔案名稱：key.kdb (預設值)

位置：C:\Program Files\IBM\HTTPServer

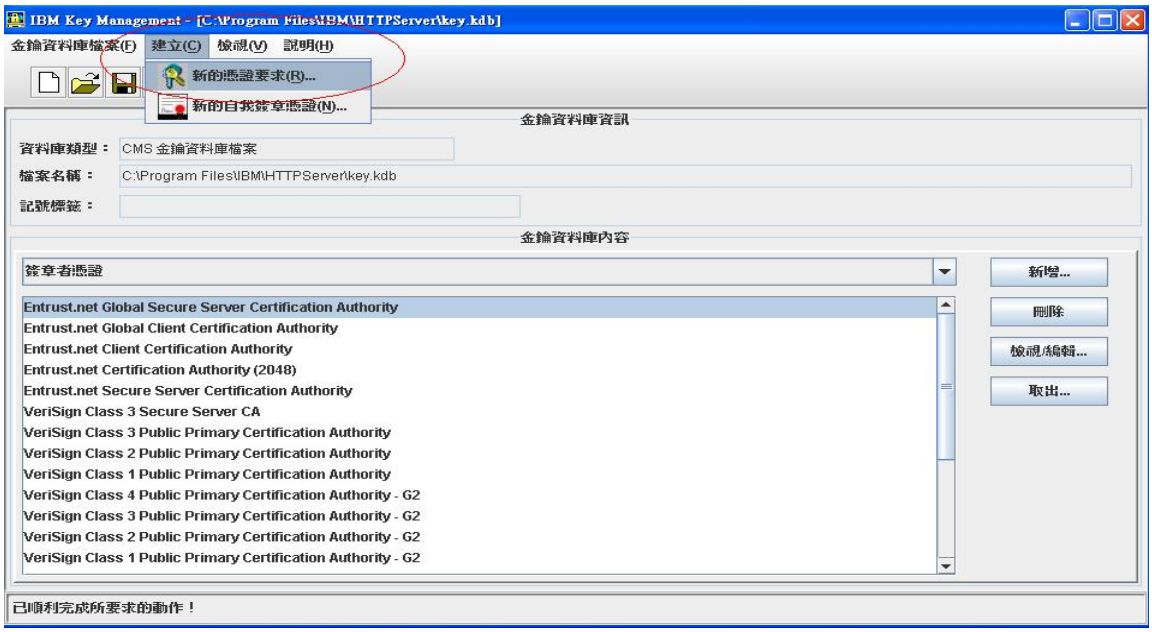


2-3 設定金鑰資料庫密碼

說明: 密碼至少取用 6 個字元，並避免使用一般可以取得的資訊所組成。例如：生日、姓名或身分證字號等……


## 3. 建立新憑證

「建立」→「新的憑證要求」



3-1 輸入憑證相關資訊，輸入完後按→「確定」

各欄位說明如下：(建議以下欄位必須使用英文填寫)

(1) 金鑰標籤：可以自行訂定。

(2) 金鑰大小：此處以選擇 『1024』爲例。

(3) 共用名稱：網站名稱 (使用 Domain Name，非 URL)

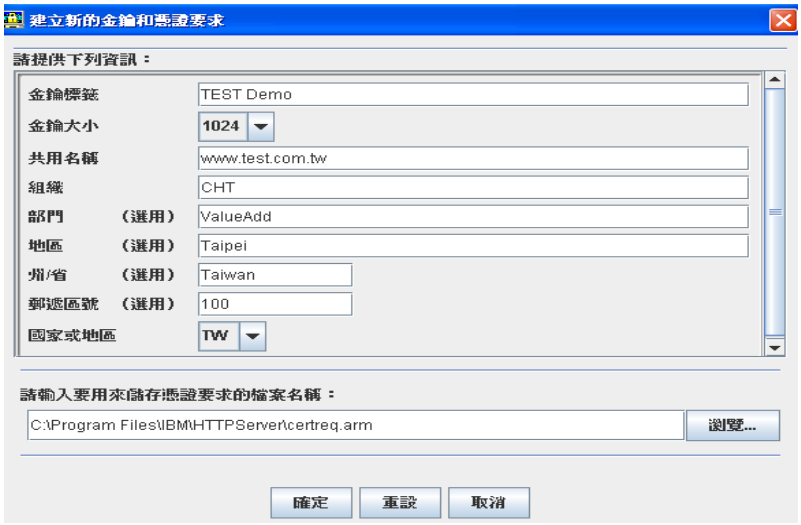
(4) 組織：使用憑證之組織 (例如：CHT)

(5) 部門：使用憑證組織之單位(例如: ValueAdd (加值處))

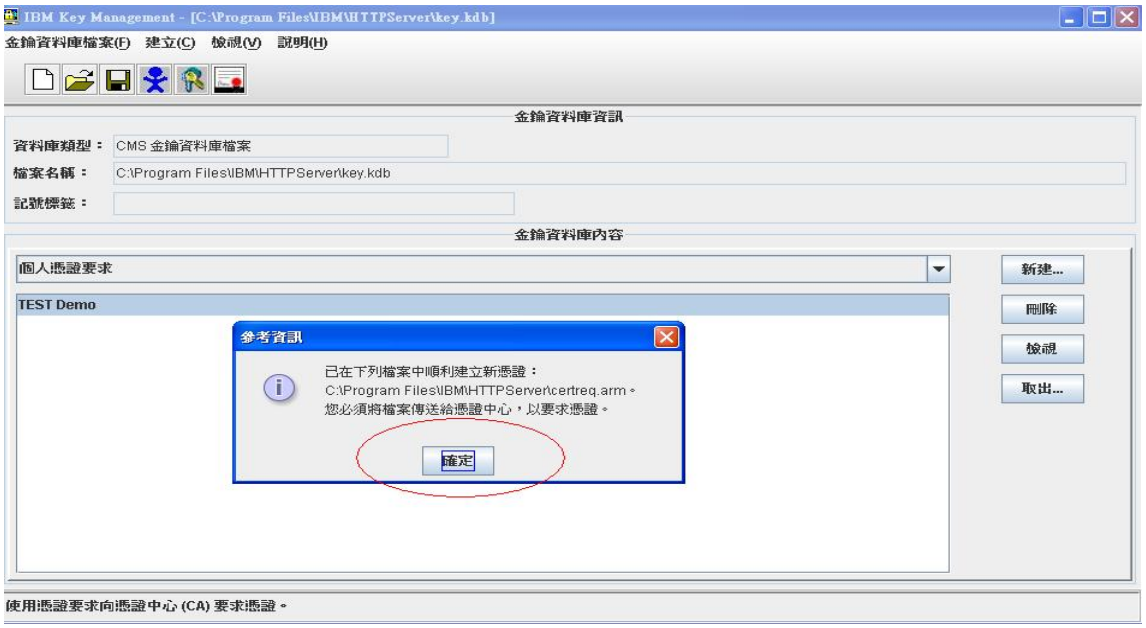
(6) 地區：城市名稱 (例如: Taipei )

(7) 州/省：國家全名 (例如: Taiwan)

(8)請輸入要用來儲存憑證要求的檔案名稱：(例如：C:\Program Files\IBM\HTTPServer\certreq.arm)，此「憑證要求」亦即一般所稱的憑證請求檔(CSR)



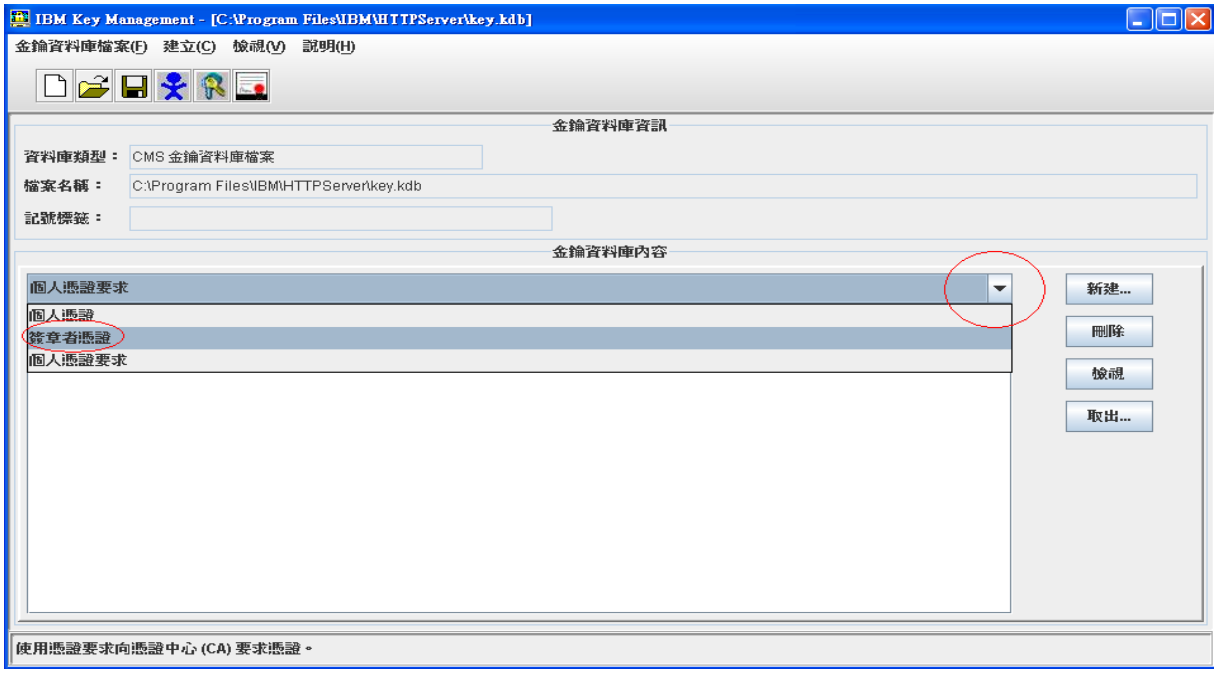

3-2 憑證請求檔製作完成，請至中華電信通用憑證管理中心申請憑證。



## 4. 新增簽章憑證

4-1 連線至 http://publicca.hinet.net/SSL-07.htm 下載Root CA憑證與中繼憑證(Based 64編碼)


4-2 點選「簽章者憑證」

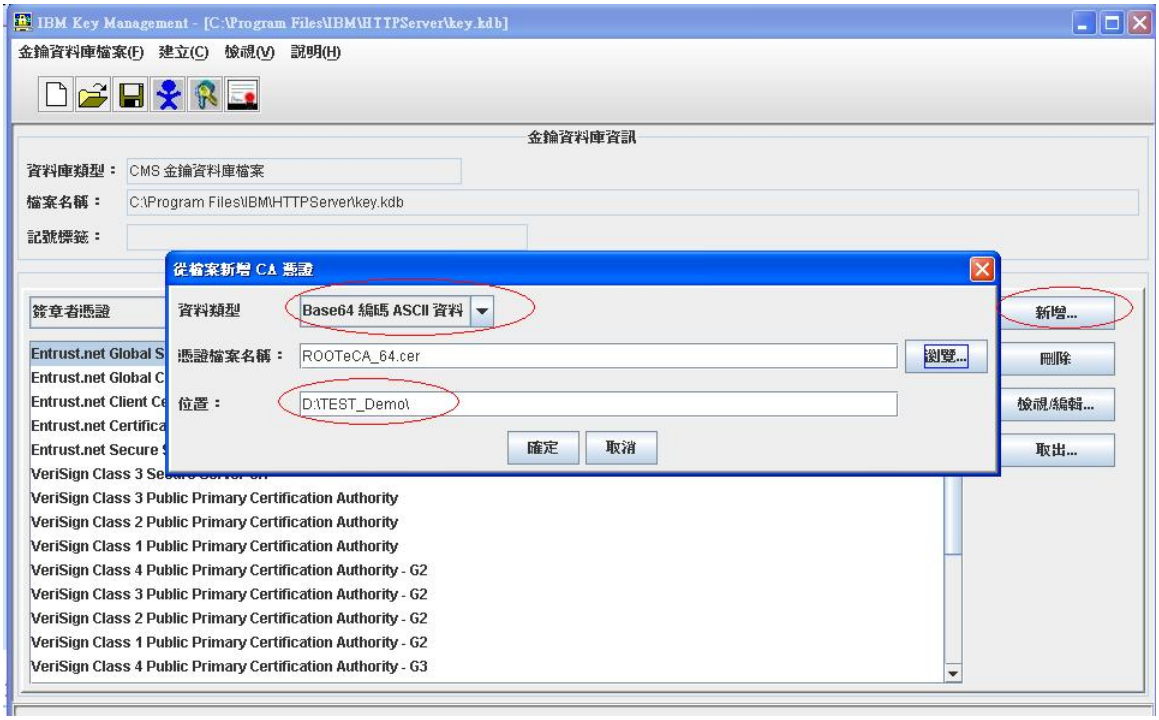


4-3 安裝 ePKI Root CA 憑證檔案→「新增」

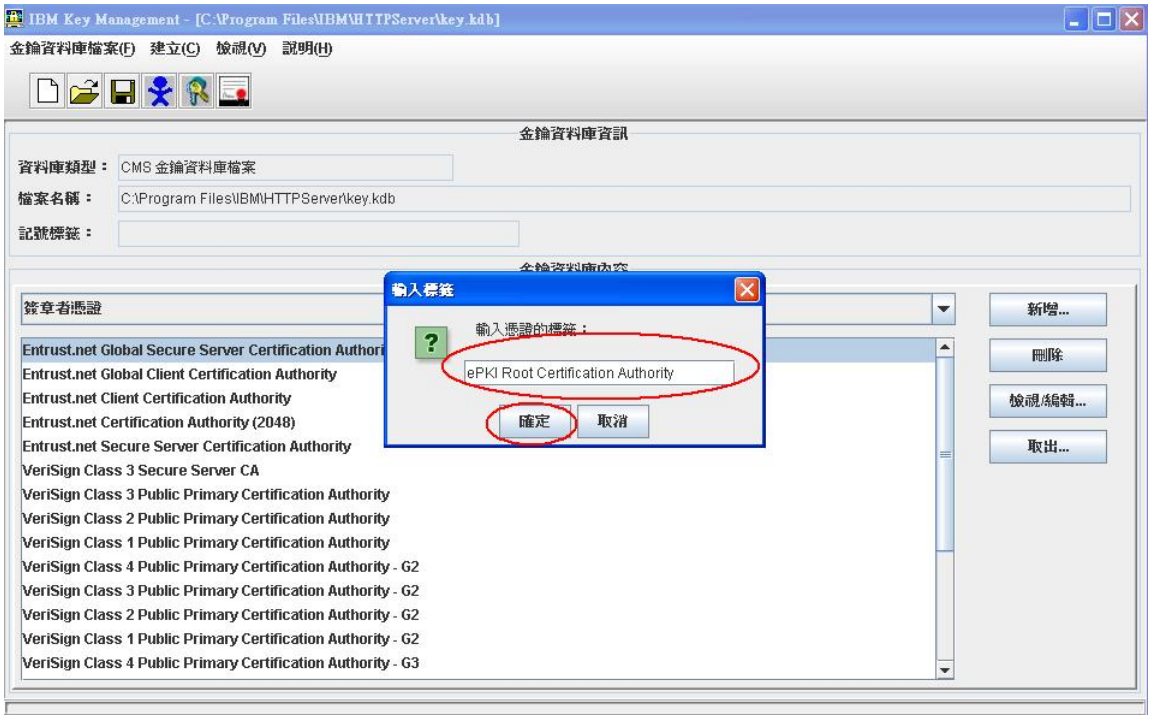
資料型態：Base64 編碼 ASCII 資料

憑證檔案名稱：ROOTeCA_64.cer

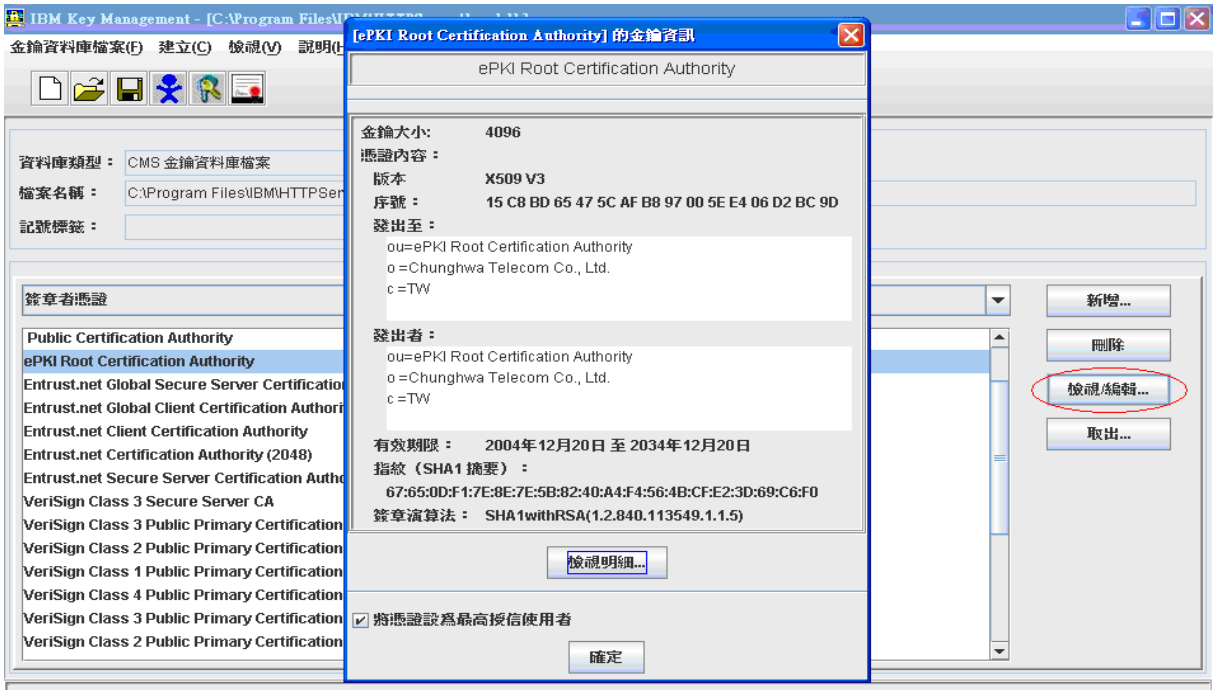
位置： D:\TEST_Demo\ → 請依實際存放路徑存檔




4-3-1 輸入 Root CA 憑證說明文字 → ePKI Root Certificate Authority→「確定 」



4-3-2 Root CA 憑證安裝完成→檢視憑證資訊.參考下圖

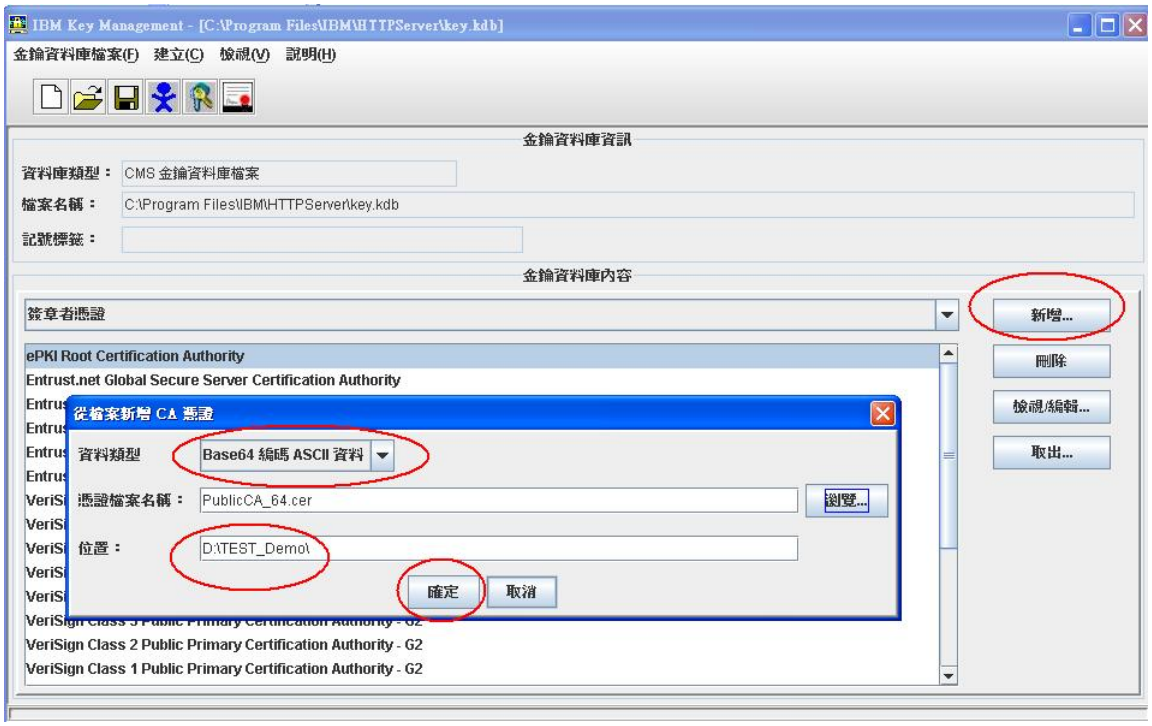


4-4 安裝中繼憑證

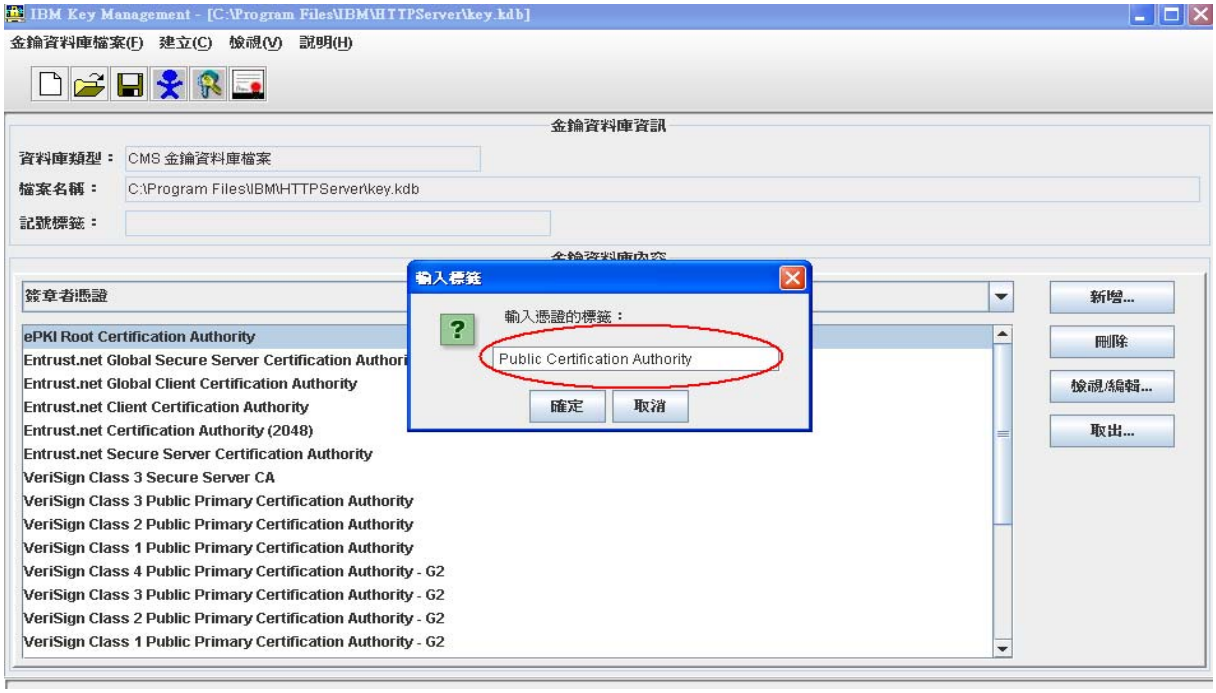
資料型態：Base64 編碼 ASCII 資料

憑證檔案名稱：PublicCA_64.cer

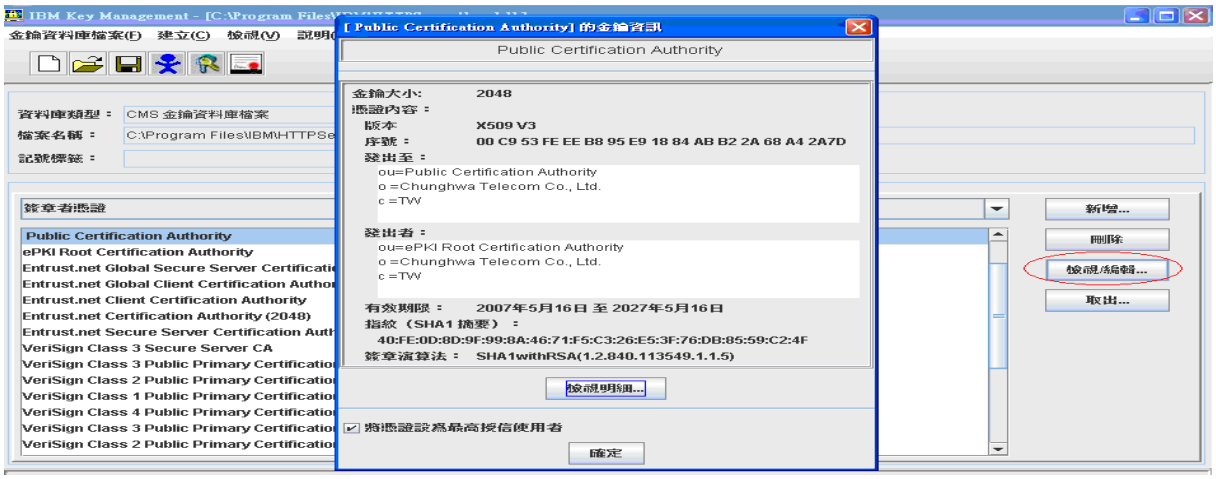
位置： D:\TEST_Demo\ → 依實際存放路徑



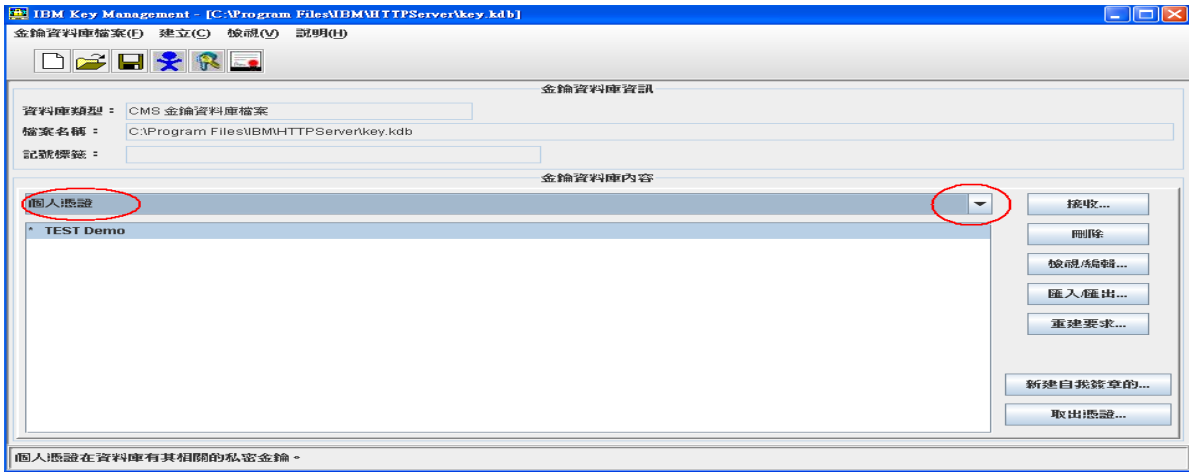

4-4-1 輸入中繼憑證說明文字 → Public Certification Authority→「確定 」



4-4-2 中繼憑證安裝完成→檢視憑證資訊.參考下圖




4-5 安裝個人憑證→點選「個人憑證」

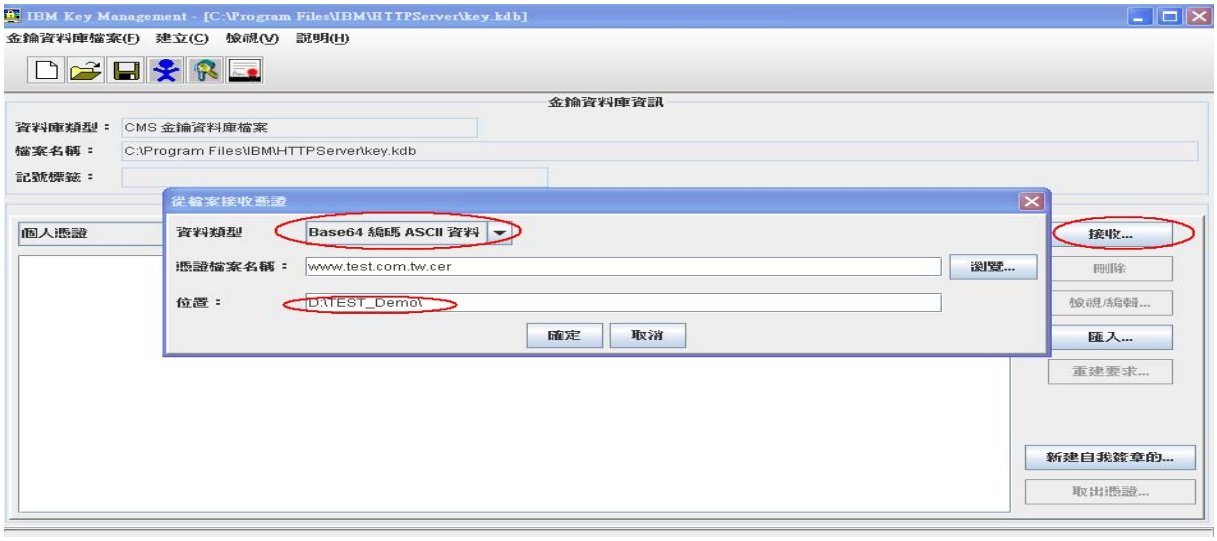


4-5-1 安裝個人憑證→「接收」

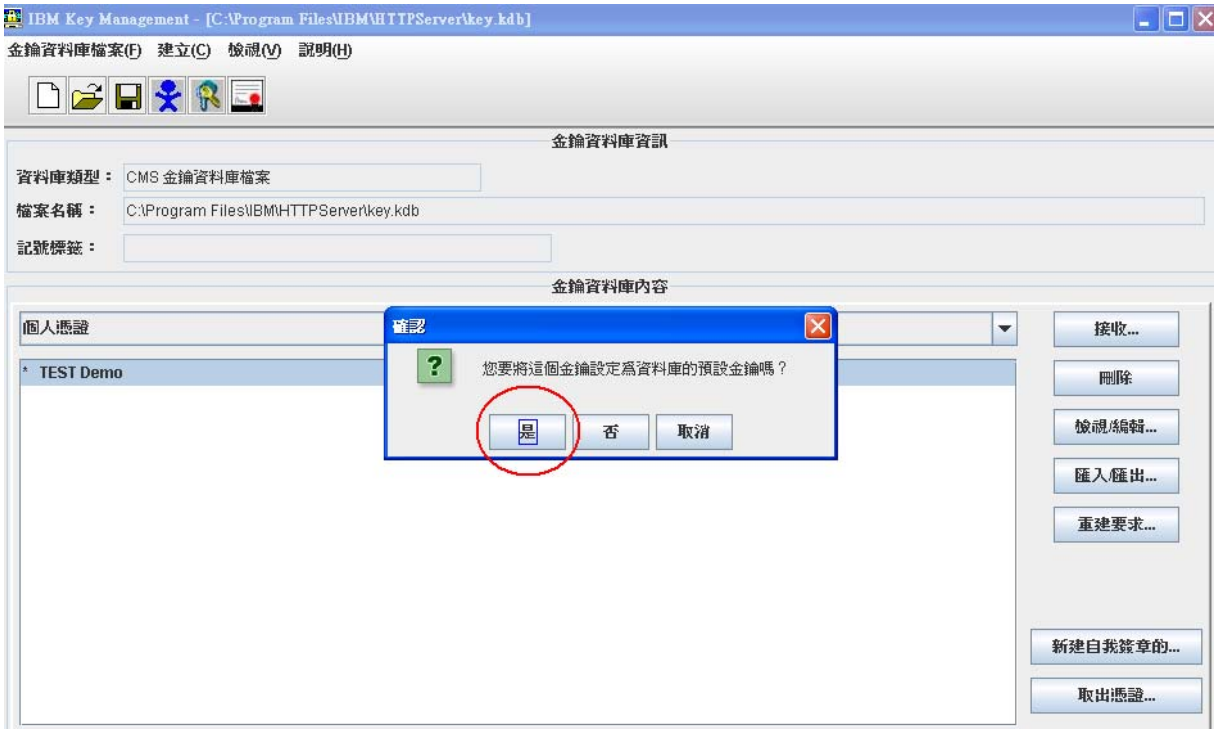
資料型態：Base64 編碼 ASCII 資料

憑證檔案名稱：www.test.com.tw.cer

位置： D:\TEST_Demo\ → 依實際存放路徑




4-5-2 設定爲預設金鑰→ 請選「是」



4-5-3 個人憑證安裝完成→「確定」→檢視憑證資訊.參考下圖


5. 安裝完成