

# 中華電信通用憑證管理中心(PublicCA)

## IBM HTTP Server 憑證請求檔製作與憑證安裝手冊

聲明：本說明文件之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本說明文件所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本說明文件所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

本說明書的申請程序，已經在 Windows 系統 + IBM HTTP Server 7.0 測試過，您所使用的版本或環境可能與本版本有所差異，若是如此則請參考您的 HTTP Server 相關使用手冊，適度調整申請步驟。

### 目錄

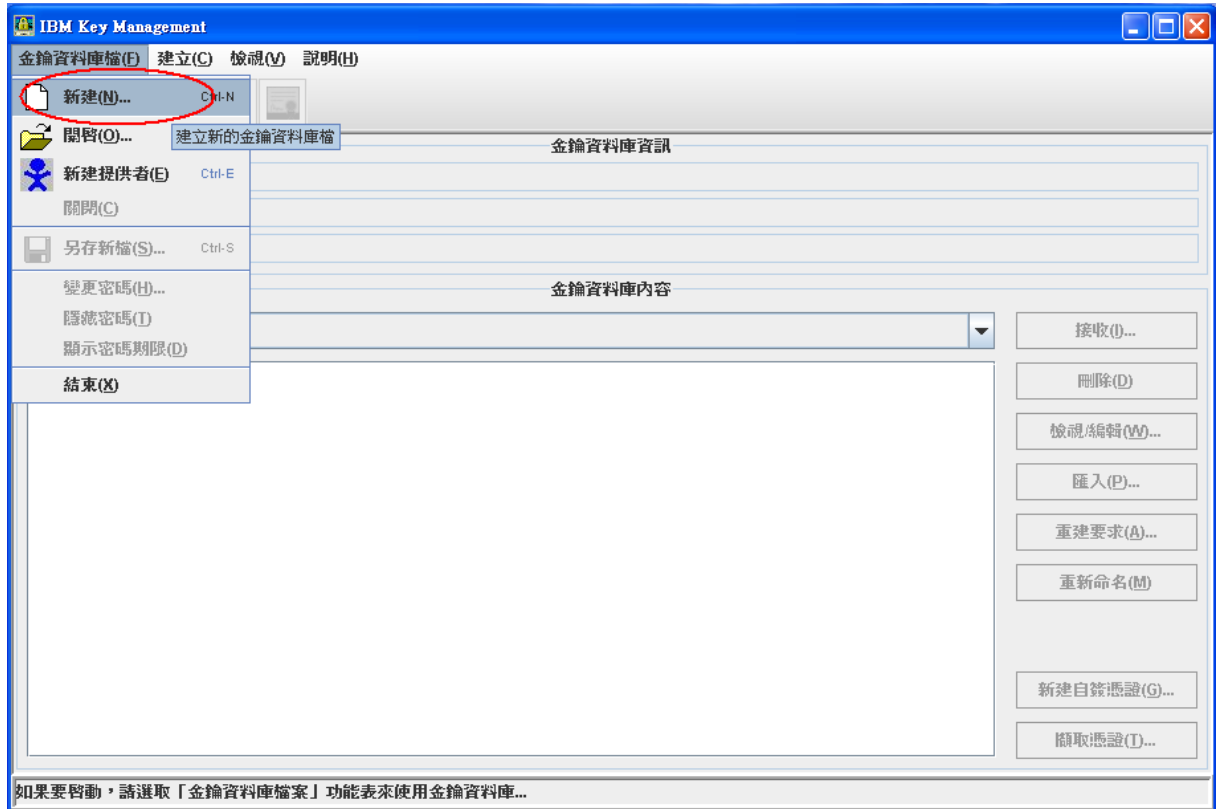
IBM HTTP Server SSL 憑證請求檔製作手冊 .....	2
IBM HTTP Server SSL 憑證安裝操作手冊 .....	6

# IBM HTTP Server SSL 憑證請求檔製作手冊

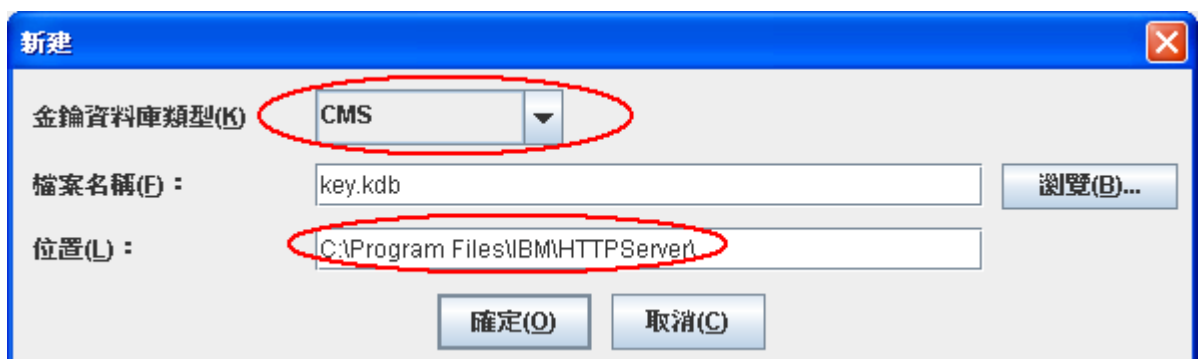
## 一、啟動Start Key Management Utility

「開始」→「程式集」→「IBM HTTP Server 7.0」→「Start Key Management Utility」。

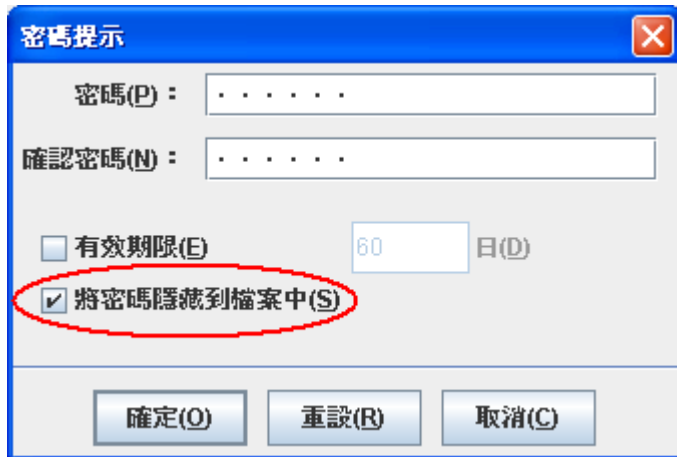
## 二、點選「金鑰資料庫檔」→「新建」。



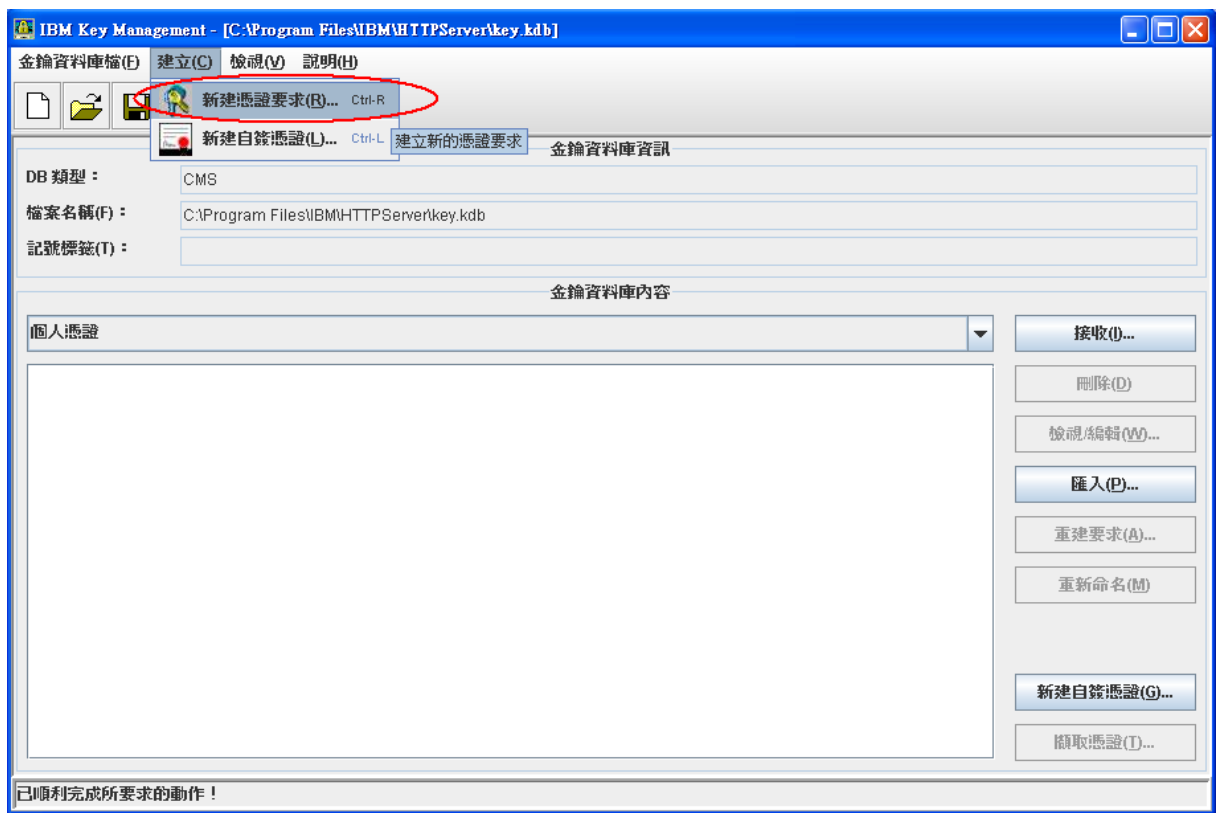
## 三、選取「金鑰資料庫類型」與「位置」。



## 四、輸入保護密碼後按下「確定」。



五、選擇「建立」→「新建憑證要求」。



六、依序將資料填入

金鑰標籤：名稱

金鑰大小：選擇「2048」（請注意依照國際密碼學趨勢，請使用2048位元(含)以上金鑰長度。）

簽章演算法：選擇「SHA1WithRSA」

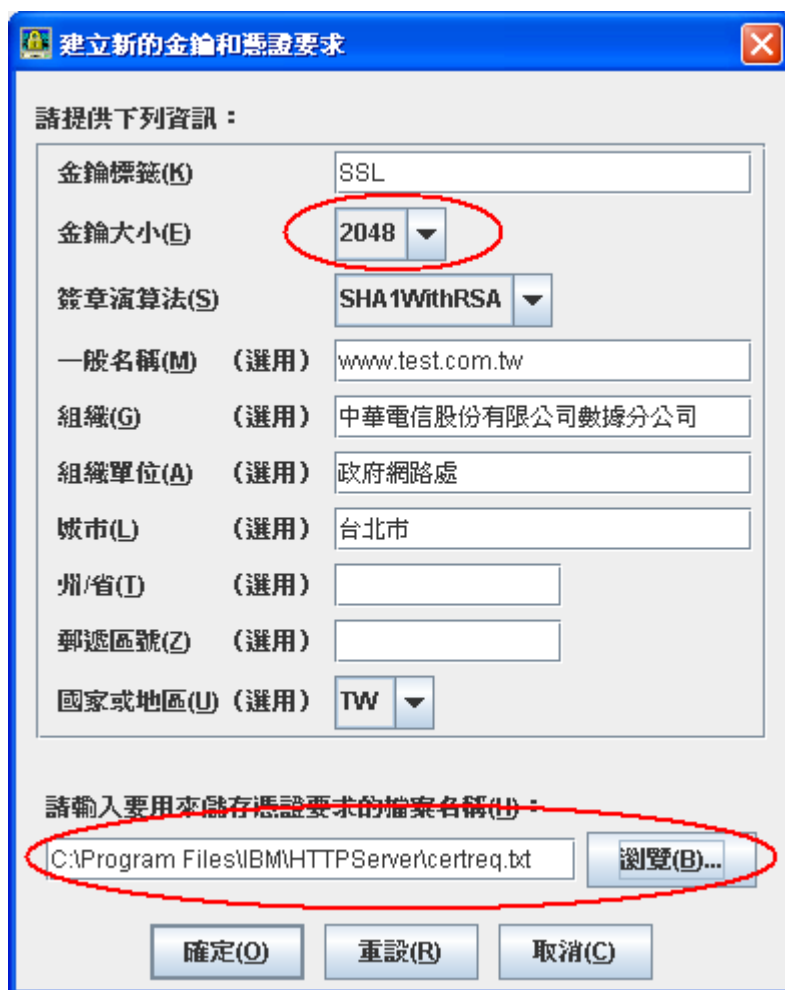
一般名稱：填入網域名稱

組織：公司名稱

組織單位：組織單位

國家或地區：選擇「TW」

檔案名稱請儲存為：certreq.txt



建立新的金鑰和憑證要求

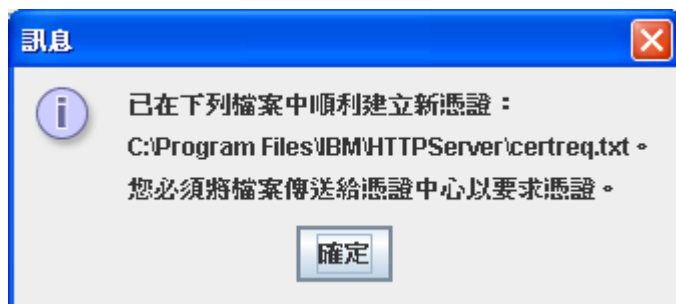
請提供下列資訊：

金鑰標籤(K)		SSL
金鑰大小(E)		2048
簽章演算法(S)		SHA1WithRSA
一般名稱(M)	(選用)	www.test.com.tw
組織(G)	(選用)	中華電信股份有限公司數據分公司
組織單位(A)	(選用)	政府網路處
城市(L)	(選用)	台北市
州/省(D)	(選用)	
郵遞區號(Z)	(選用)	
國家或地區(U)	(選用)	TW

請輸入要用來儲存憑證要求的檔案名稱(F)：

C:\Program Files\IBM\HTTPServer\certreq.txt 瀏覽(B)...

確定(O) 重設(R) 取消(C)



- 七、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請SSL憑證 (以文字編輯器如記事本開啟憑證請求檔，全選及複製檔案內容，將憑證請求檔貼上SSL憑證申請網頁之表單。)。若屬於中華電信公司各單位申請SSL憑證者，請從企業入口網站電子表單之資訊表單IS14-伺服器應用軟體憑證申請/異動單提出申請。
- 八、補充說明 1: 中華電信通用憑證管理中心之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於步驟六所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準而記載於所簽發的SSL憑證裡面的欄位[如憑證主體名稱(Subject Name)或憑證主體別名

(Subject Alternative Name)等欄位]。

九、補充說明2:若您是申請多網域SSL憑證或萬用網域SSL憑證，僅需要產生1個憑證請求檔（產生憑證請求檔之過程就是幫您的伺服器產製1對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會包含客戶之組織身分、完全吻合網域名稱與公開金鑰在憑證內。後續先安裝SSL憑證串鏈在產生憑證請求檔之站台，再將私密金鑰與憑證備份匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱caservice@cht.com.tw詢問，不需要每個網站站台都分別產生憑證請求檔。）

## IBM HTTP Server SSL 憑證安裝操作手冊

一、下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA\_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2\_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。

若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。

2. 從網站查詢與下載：

eCA憑證：

[http://epki.com.tw/download/ROOTeCA\\_64.crt](http://epki.com.tw/download/ROOTeCA_64.crt)

PublicCA G2憑證：

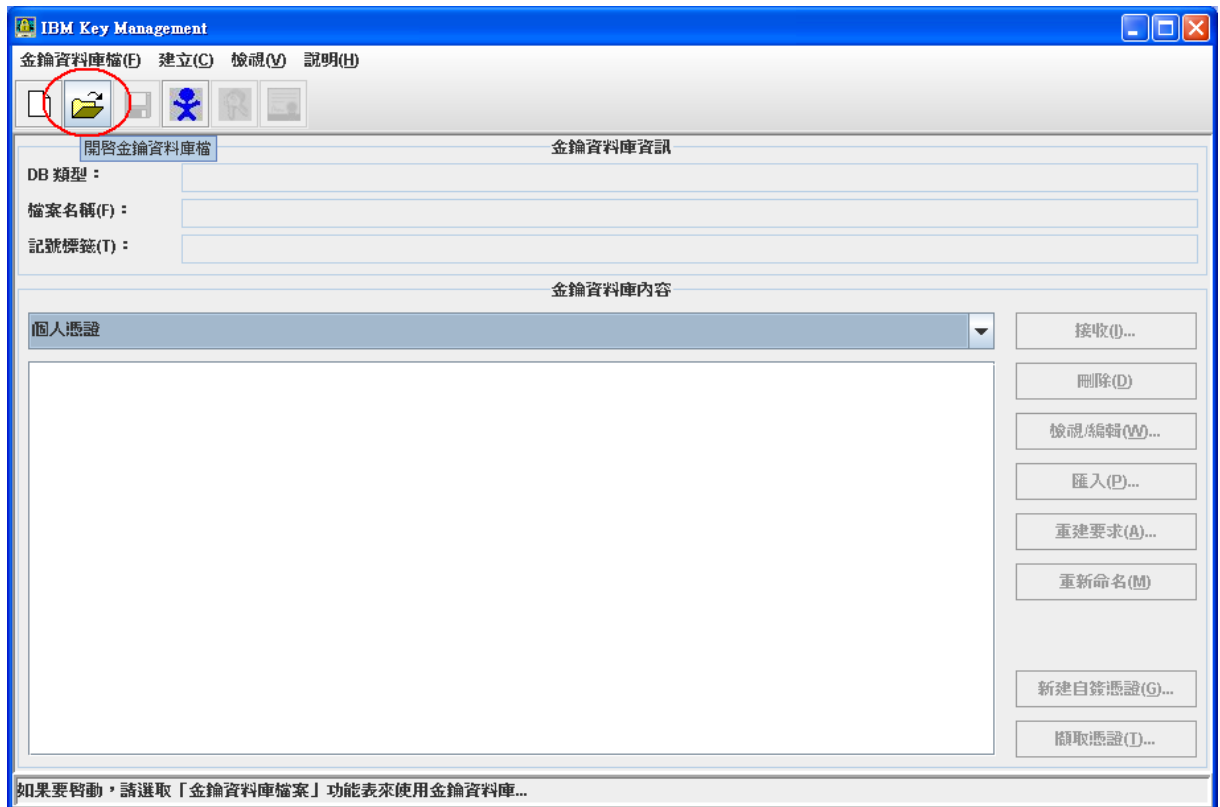
[http://epki.com.tw/download/PublicCA2\\_64.crt](http://epki.com.tw/download/PublicCA2_64.crt)

SSL憑證下載：您若是本公司之客戶，請至PublicCA網站點選「SSL憑證服務」再點選「SSL憑證查詢及下載」，進行SSL憑證下載。

若您是中華電信之員工，負責管理單位之伺服器，請至

<http://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載SSL憑證。

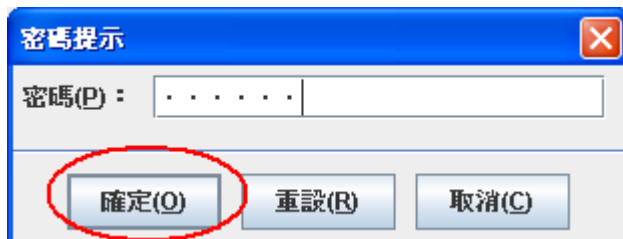
二、開啟Start Key Management Utility後，點選「開啟舊檔」。



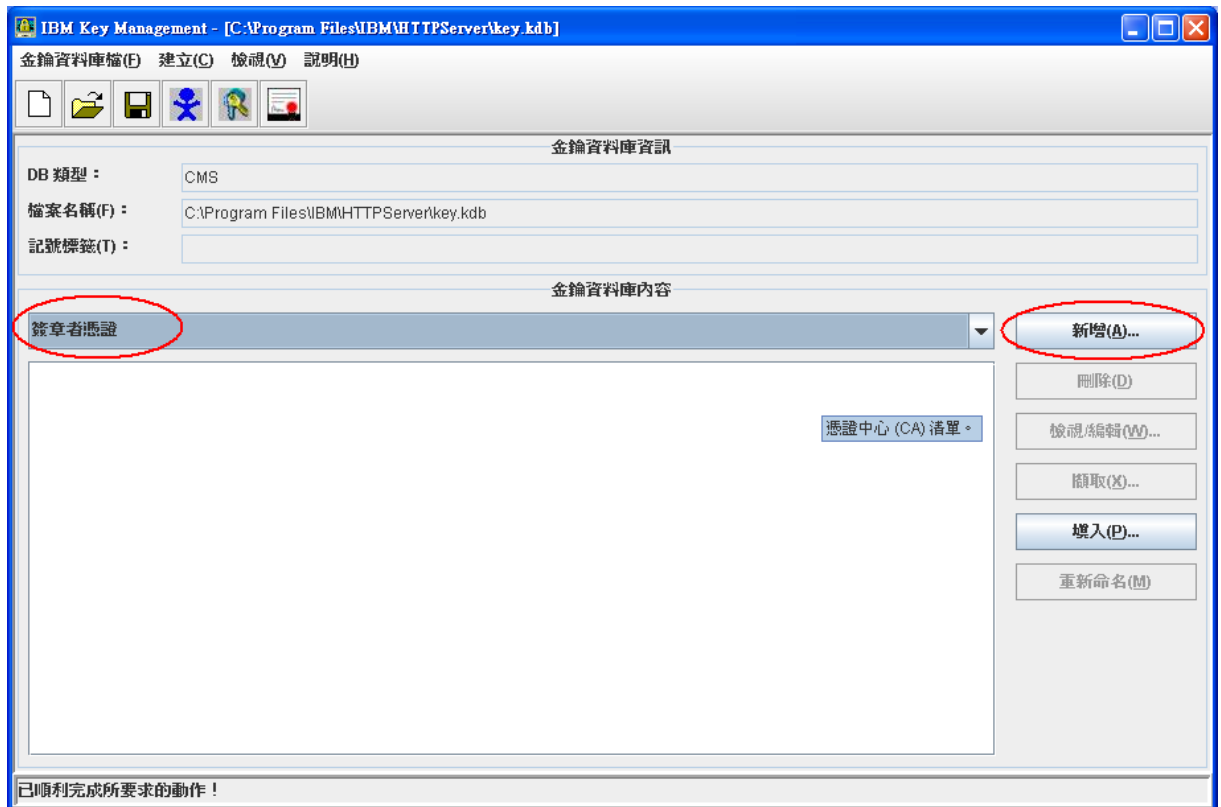
三、選擇之前存放金鑰庫的位置後按下「確定」。



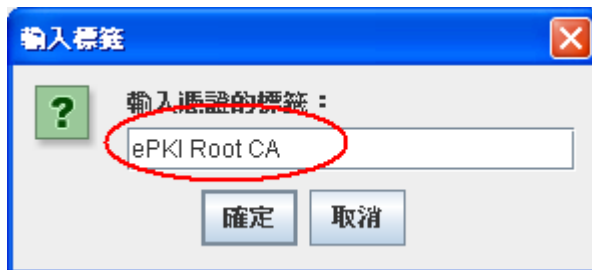
四、輸入之前的保護密碼後按下「確定」。



五、在下拉選單中選擇「簽章者憑證」，然後點選，「新增」。



六、利用「瀏覽」選取ROOTeCA\_64.crt。



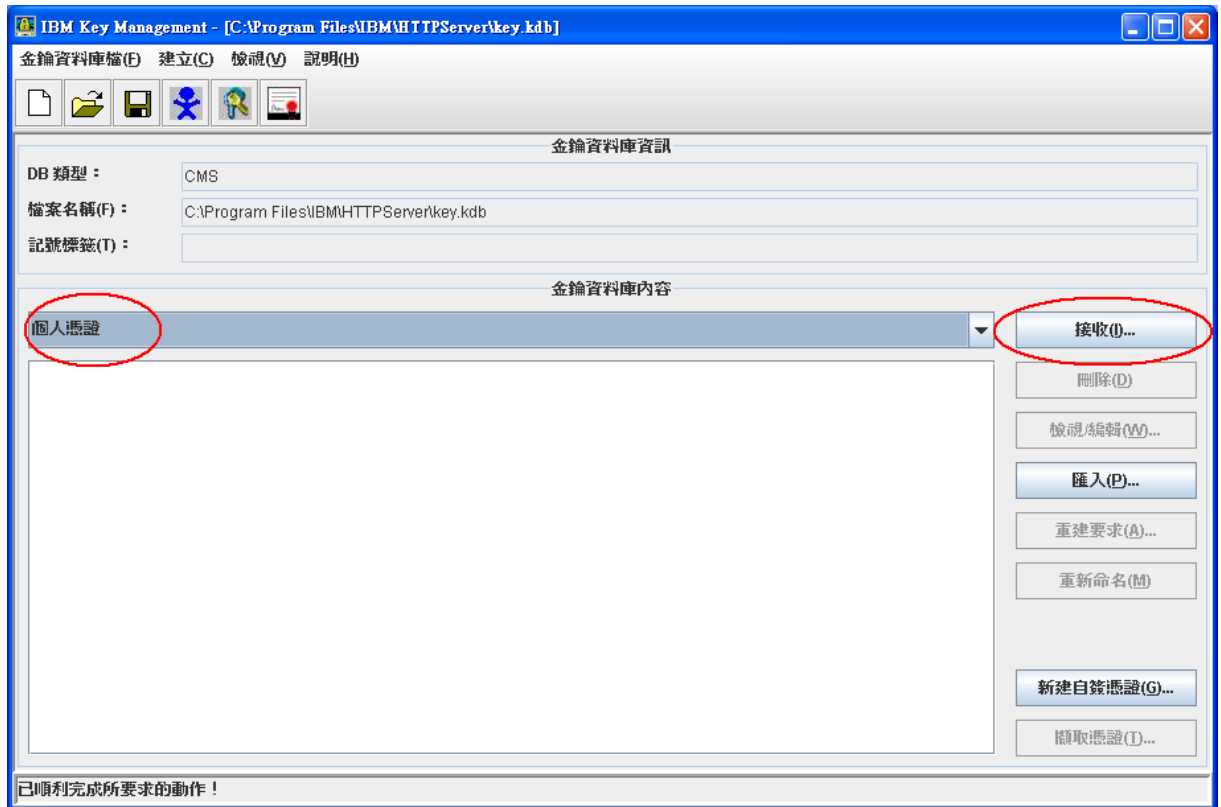
七、依照上述相同的步驟將PublicCA2\_64.crt新增至金鑰資料庫。







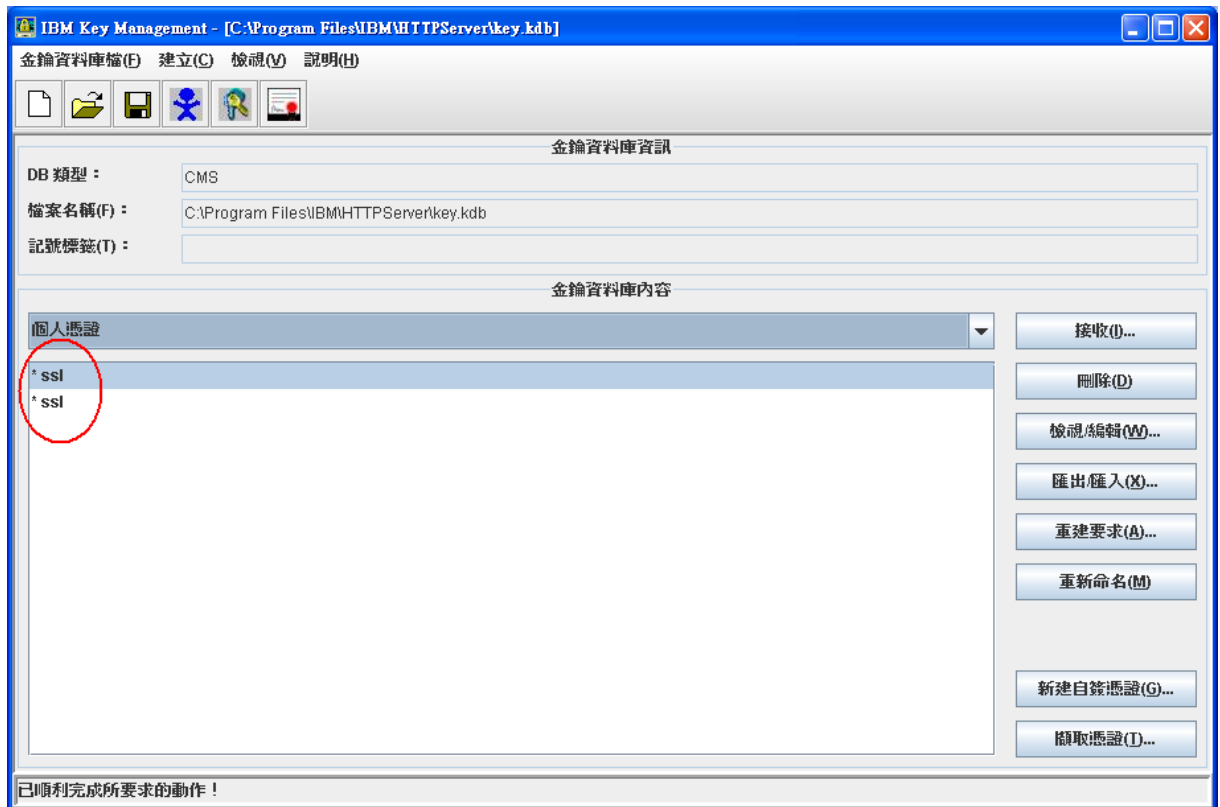
八、在下拉選單中選擇「個人憑證」，然後點選，「接收…」。



九、利用「瀏覽」選取由中華電信通用憑證管理中心所簽發的SSL憑證。



十、安裝成功後，可看到下圖出現之前憑證請求檔所設定的「金鑰標籤」。



十一、 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

十二、 請安裝 SSL 安全認證標章：

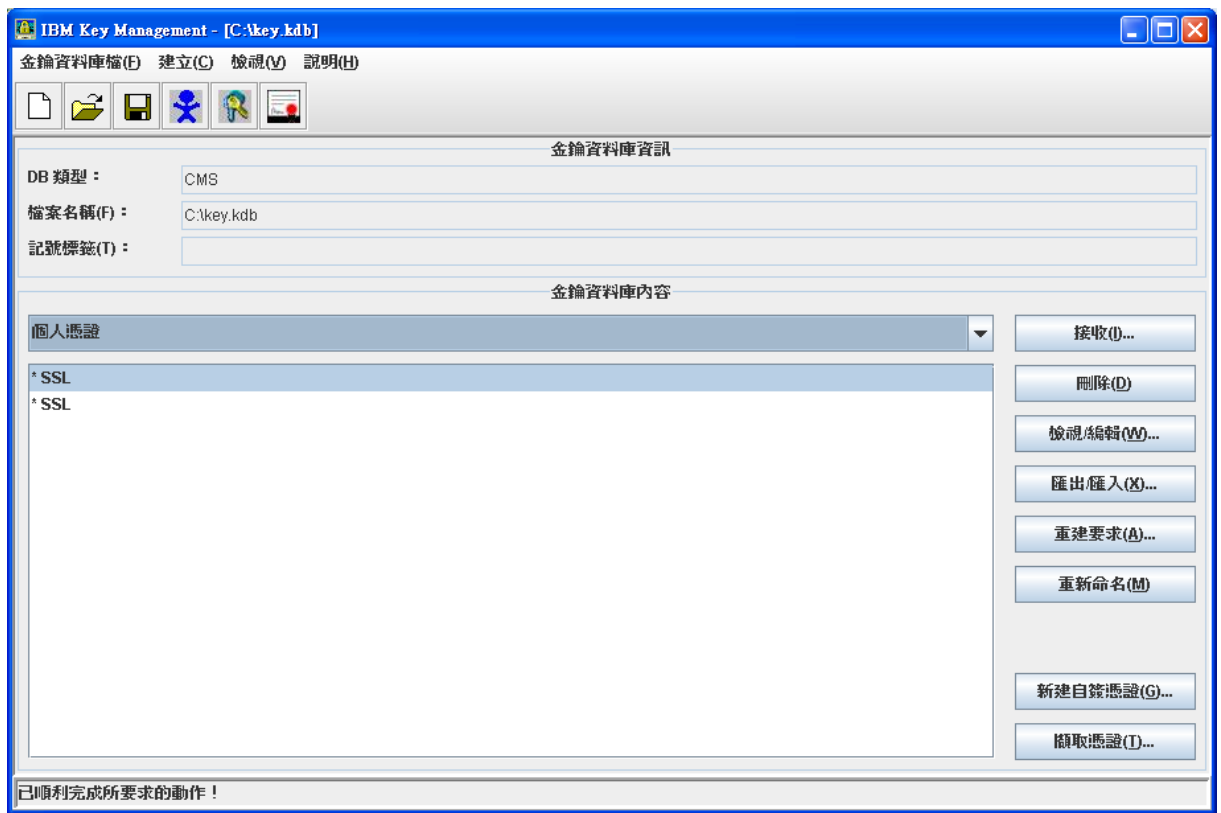
請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。您也可參考

<http://publicca.hinet.net/SSL-01.htm> 下方有 SSL 安全認證標章之安裝說明。

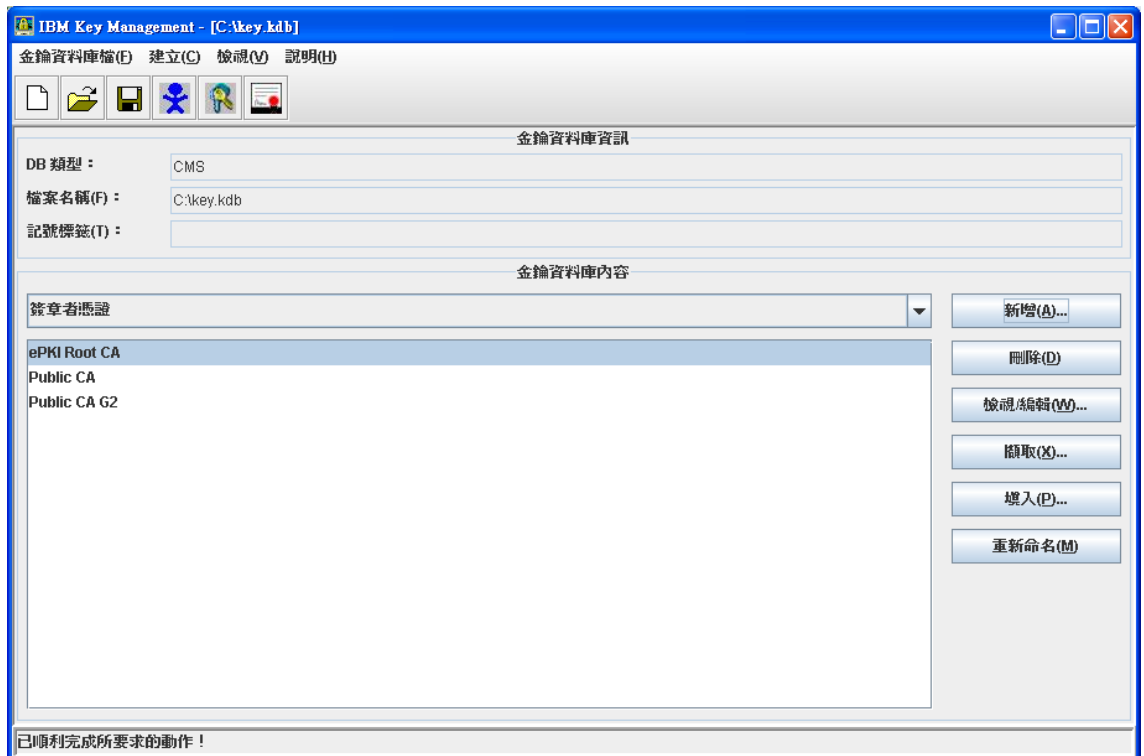
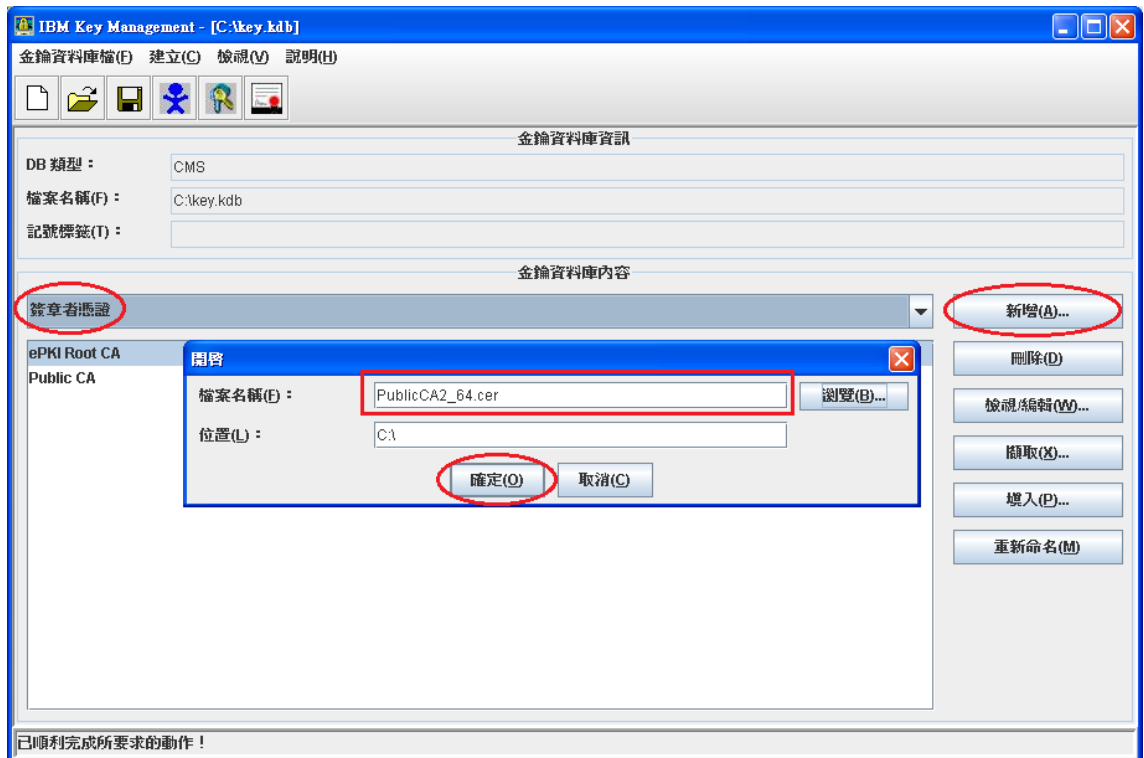
請中華電信公司負責維護網站的同仁，參考從電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSeal.spec.txt，將網站 SSL 安全認證標章安裝成功。

## 附件一：更換 SHA256 憑證

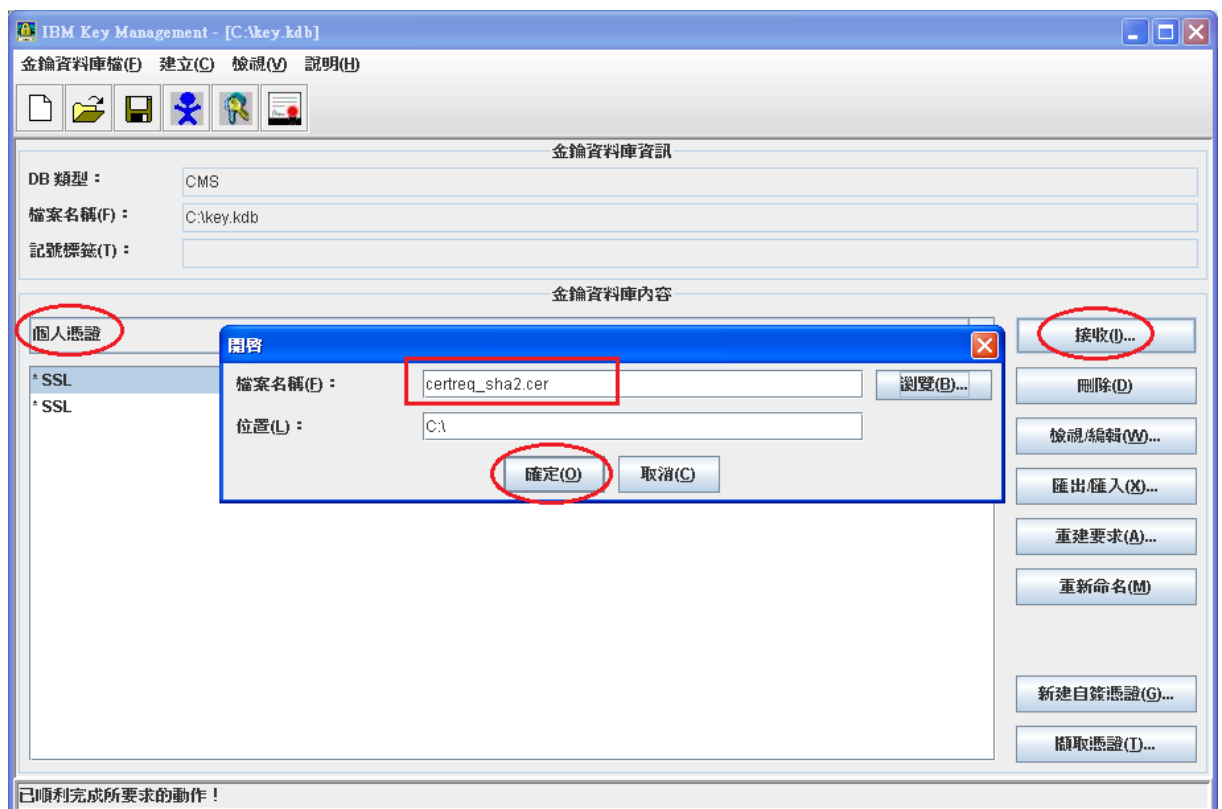
- 適用於申請時，有同時取得SHA1、SHA256憑證。或是憑證再效期內，經由審驗人員再次核發SHA256憑證者。
- 需要檔案：
  - CMS Keystore：key.kdb、key.rdb、key.sth，請複製一份到其他路徑，並使用複製的檔案進行操作。
  - PublicCA G2中繼憑證：可於zip檔中取得。
  - SHA256用戶端憑證。
- 安裝步驟：
  - 開啟 IBM Key Management，並開啟複製的 key.kdb檔案。



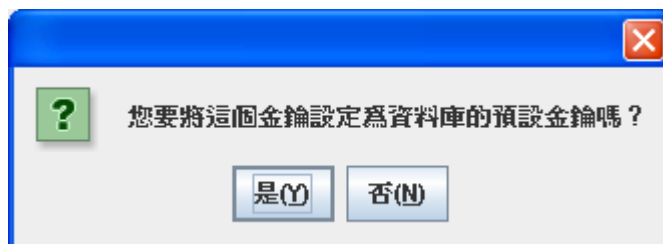
- 切換至「簽章者憑證」，並匯入 Public CA G2中繼憑證。



- 切換回「個人憑證」→「接收」→以瀏覽的方式找到SHA256的憑證。



- 待出現下圖，請點選「是」



- 請將key.kdb、key.rdb、key.sth移回原目錄，重新啟動 Server。