SSL 證書 - IBM

證書安裝指南

webnic
accelerate your business

請選擇您的版本

IBM AS 400 / iSeries 伺服器 SSL 安裝指南

IBM HTTP Server IKEYMAN 界面 SSL 安裝說明

IBM WebSphere IKEYMAN 界面 SSL 安裝指南

使用命令行界面安裝 IBM WebSphere SSL 證書

IBM AS 400 / iSeries 伺服器 SSL 安裝指南

步驟 1：下載 Intermediate CA 證書

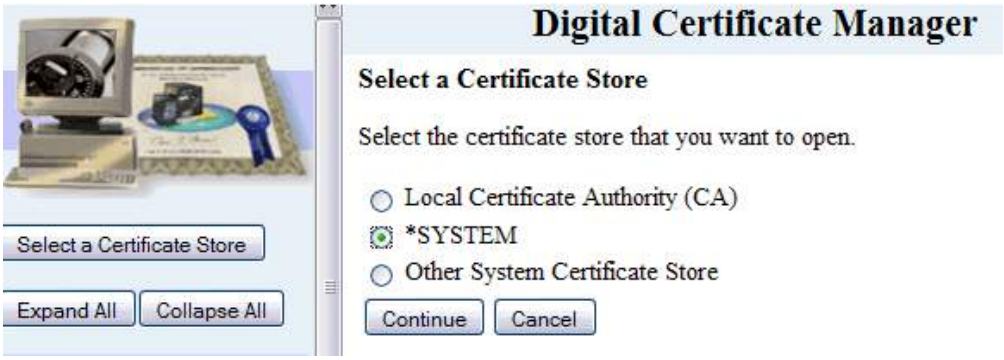
1. 通過此鏈接下載 Intermediate CA 證書。

   選擇和你的 SSL 證書適合的 Intermediate CA 證書。

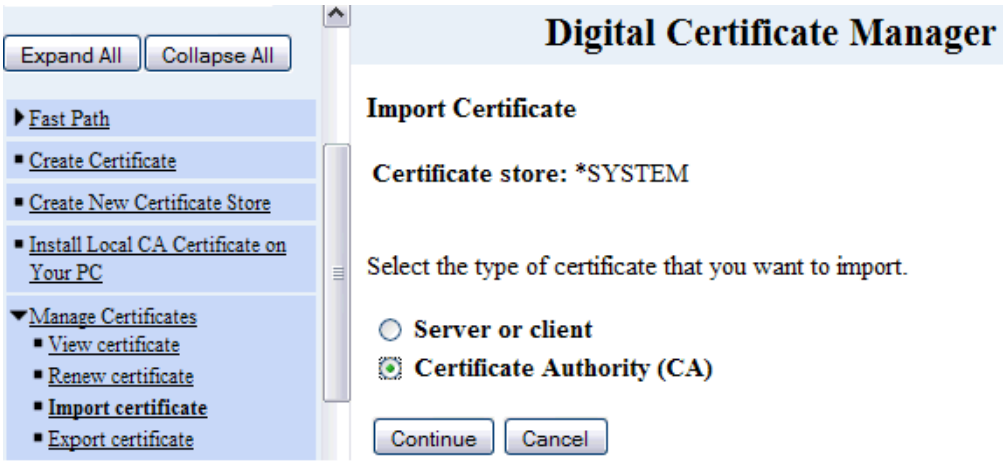
2. 複製 Intermediate CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.txt.

步驟 2：安裝 Intermediate CA 證書

1. 啟動 Digital Certificate Management (DCM)。
2. 從導航面板中，點擊 Select a Certificate store > 選擇 *System

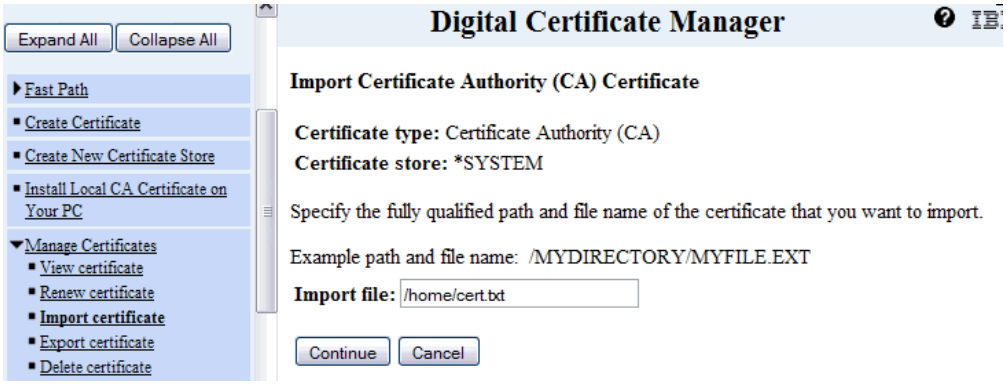


3. 輸入證書密碼 > 點擊 Continue。
4. 從導航面板 選擇 Manage Certificate。
5. 從列表中，選擇 Import Certificate > Certificate Authority (CA) > 點擊 Continue。



6. 下一步，輸入 Intermediate CA 證書文件所在的路徑及文件名稱。

   例：如果文件是儲存在 /home 目錄，而 Intermediate CA 證書文件名是 Intermediate.txt，你應輸入 **/home/intermediate.txt**。

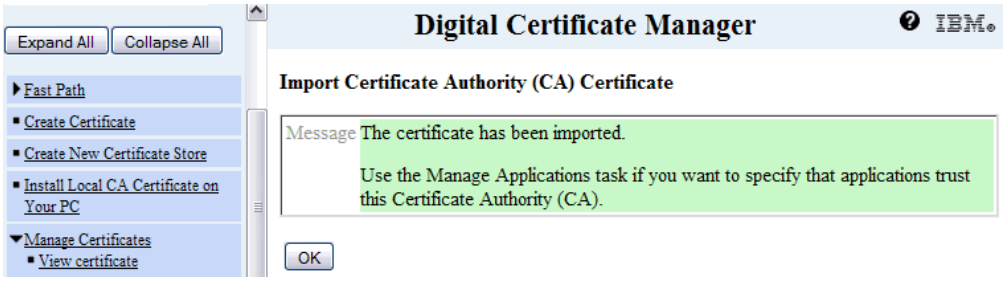


7. **點擊繼續**。

8. 創建 CA 證書標籤。

9. 點擊**繼續**。

10. 系統將提示 Intermediate CA 已被導入。點擊 **OK**。



步驟 3：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。

2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

   證書正文的例子：

   -----BEGIN CERTIFICATE-----

[加密數據]

-----END CERTIFICATE-----

3. 把證書存檔為 filename.txt 文檔。

步驟 4：安裝 SSL 證書

1. 啟動 Digital Certificate Manager （DCM）。

2. 從導航面板中，點擊 Select a Certificate Store > 選擇 *SYSTEM。

3. 輸入密碼，點擊**繼續**。

4. 從導航面板，選擇 Manager Certificates。

5. 選擇 Import Certificate > 選擇 Server or Client。

6. 選擇證書後完成安裝。

7. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

IBM HTTP Server IKEYMAN 界面 SSL 安裝說明

因證書籤名算法升級，目前證書均需要使用 SHA-256 算法簽發。 IBM Http Server 8.5 之前版本不支持 SHA-256 算法，無法加載使用 SHA-256 算法證書生成的 kdb 文件。如需配置 SHA-256 算法證書，請升級 IHS 到 8.5 或以上版本。

步驟 1：創建證書請求

1. 運行 ikeyman

IBM Http Server 附帶 I Key Manager 工具，可用於管理 IHS 的證書密鑰文件。 IBM HTTP Server V6.1 版本不支持創建 2048 位證書請求，請使用 IHS7 或以上版本自帶的 I Key Manager 工具來創建證書申請。選“**Start Key Management Utility**”，運行 I Key Manager

2. 創建密鑰庫文件

密鑰庫類型選擇“CMS”

注意：請選中“將密碼存儲到文件”選項，此選項將把密碼加密保存到擴展名為.sth 的文件中。 IHS 啟動時，會自動從該.sth 文件中讀取密碼，如果不選擇此項啟動 HTTP SERVER 時會報錯。

3. 生成證書請求

IHS6 下的 ikeyman 最高支持 1024 位密鑰，目前所有服務器要求 2048 位密鑰。使用 IHS7 版 ikeyman 創建的含 2048 位密鑰的密鑰庫文件，在 IHS6 下仍可以正常應用。

導出證書籤名請求文件 certreq.arm，並稍後發送給天威誠信，等待證書的簽發。

步驟 2：導入服務器證書

1. 獲取並導入 CA 證書

將證書籤發郵件中的從 BEGIN 到 END 結束的兩張中級 CA 證書內容分別粘貼到記事本文

本文件中。

證書正文的例子：

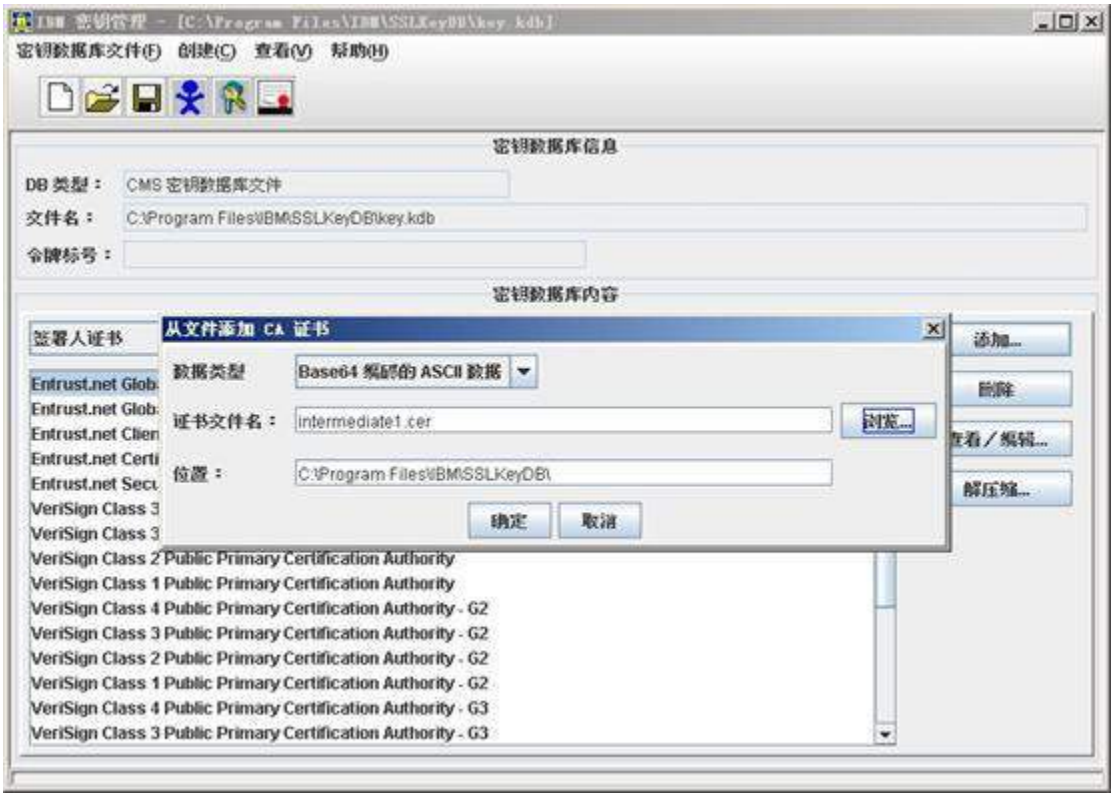
-----BEGIN CERTIFICATE-----

[加密數據]

-----END CERTIFICATE-----

修改文件擴展名，保存為 intermediate1.cer 和 intermediate2.cer 文件(如果只有一中級證書，則只需要保存安裝一張中級證書)。

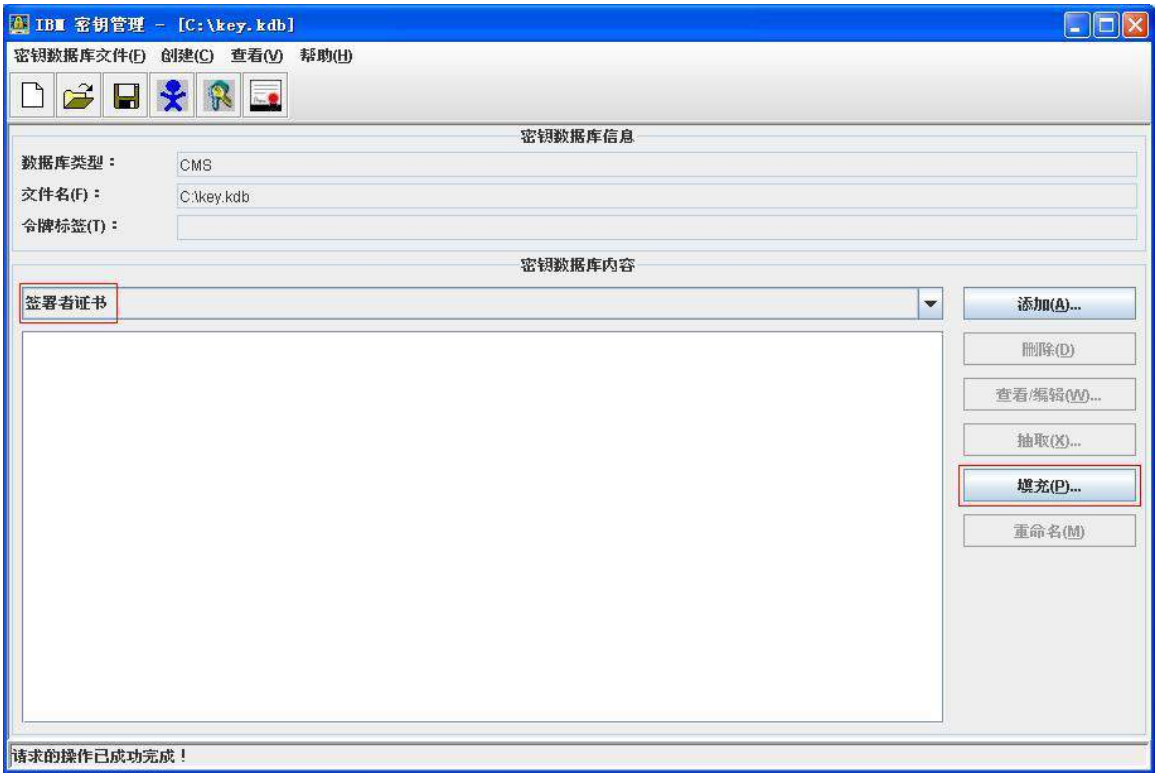
運行 ikeyman 並打開您的 kdb 文件，切換到“簽署人證書”視圖，並選擇“添加”

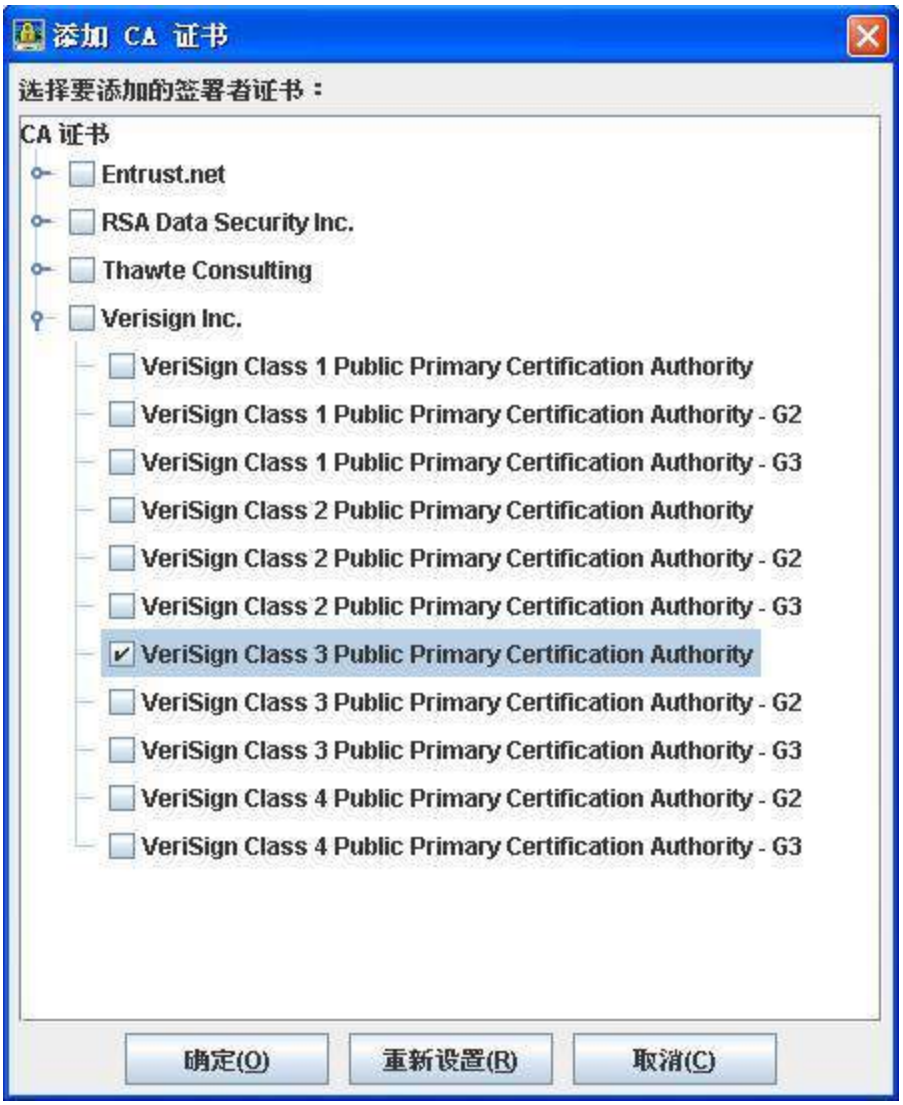


分別添加兩張中級 CA 證書，並輸入證書的標號

2. 填充根證書

IHS7 版 ikeyman 創建的 kdb 文件默認不包含服務器證書的根證書，需要使用 IHS7 版 ikeyman 打開生成的 kdb 文件，切換到“**簽署人證書**”選項中，選擇“**填充**”模式，將 VeriSign 服務器證書的“**VeriSign Class 3 Public Primary Certificate Authority**”的根證書填充到 kdb 格式證書密鑰庫文件中。





3. 獲取並導入服務器證書

將證書籤發郵件中的從 BEGIN 到 END 結束的服務器證書內容粘貼到記事本等文本編輯器中，保存為 server.cer 文件 。

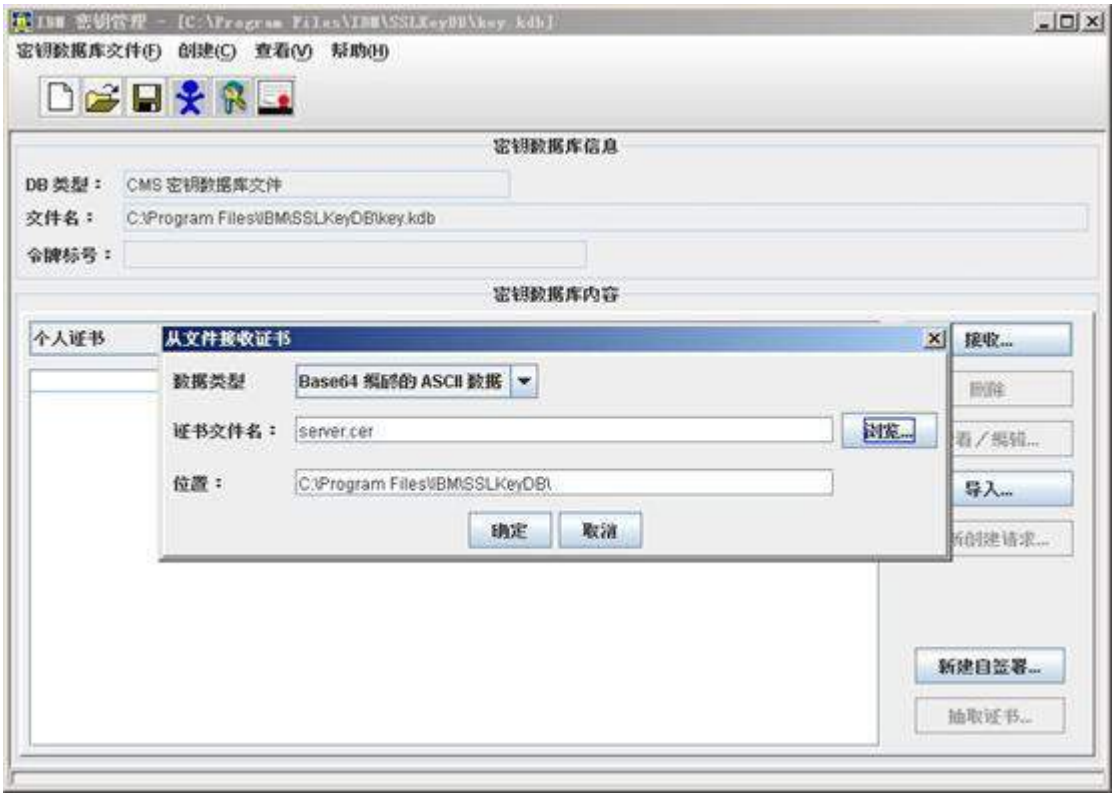
證書正文的例子：

-----BEGIN CERTIFICATE-----

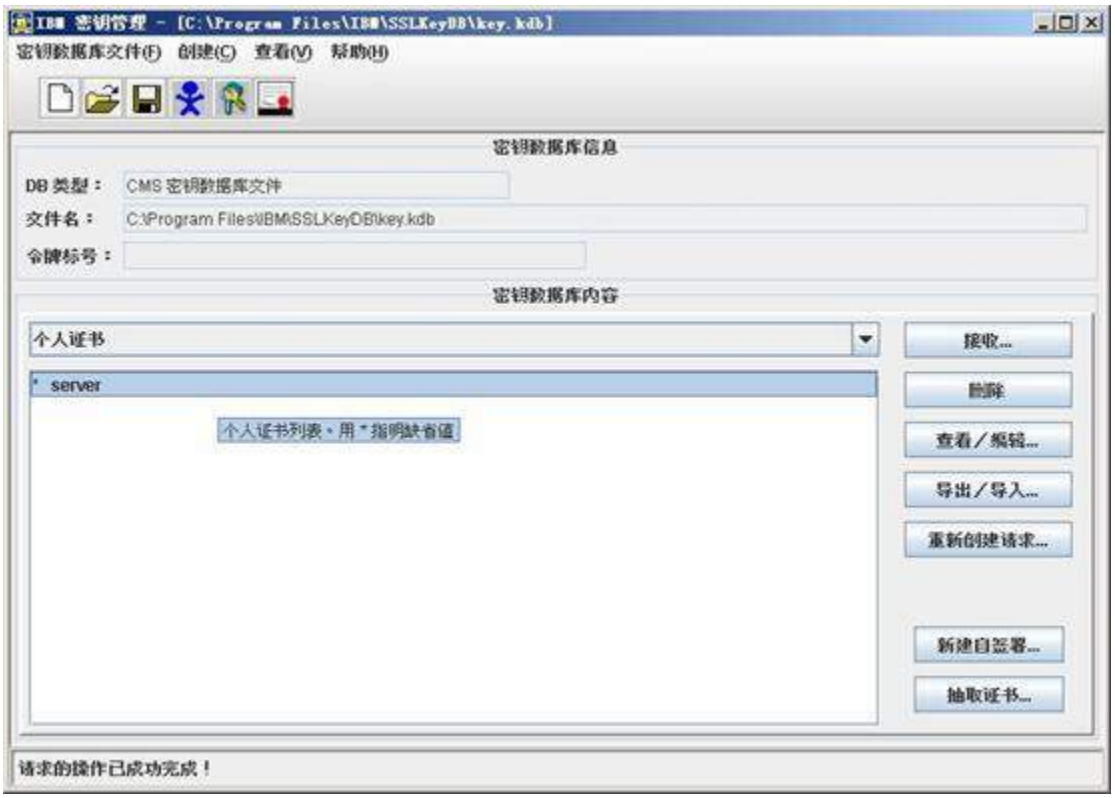
[加密數據]

-----END CERTIFICATE-----

切換到“個人證書”視圖，選擇“接收”，選擇並導入您的服務器證書文件。

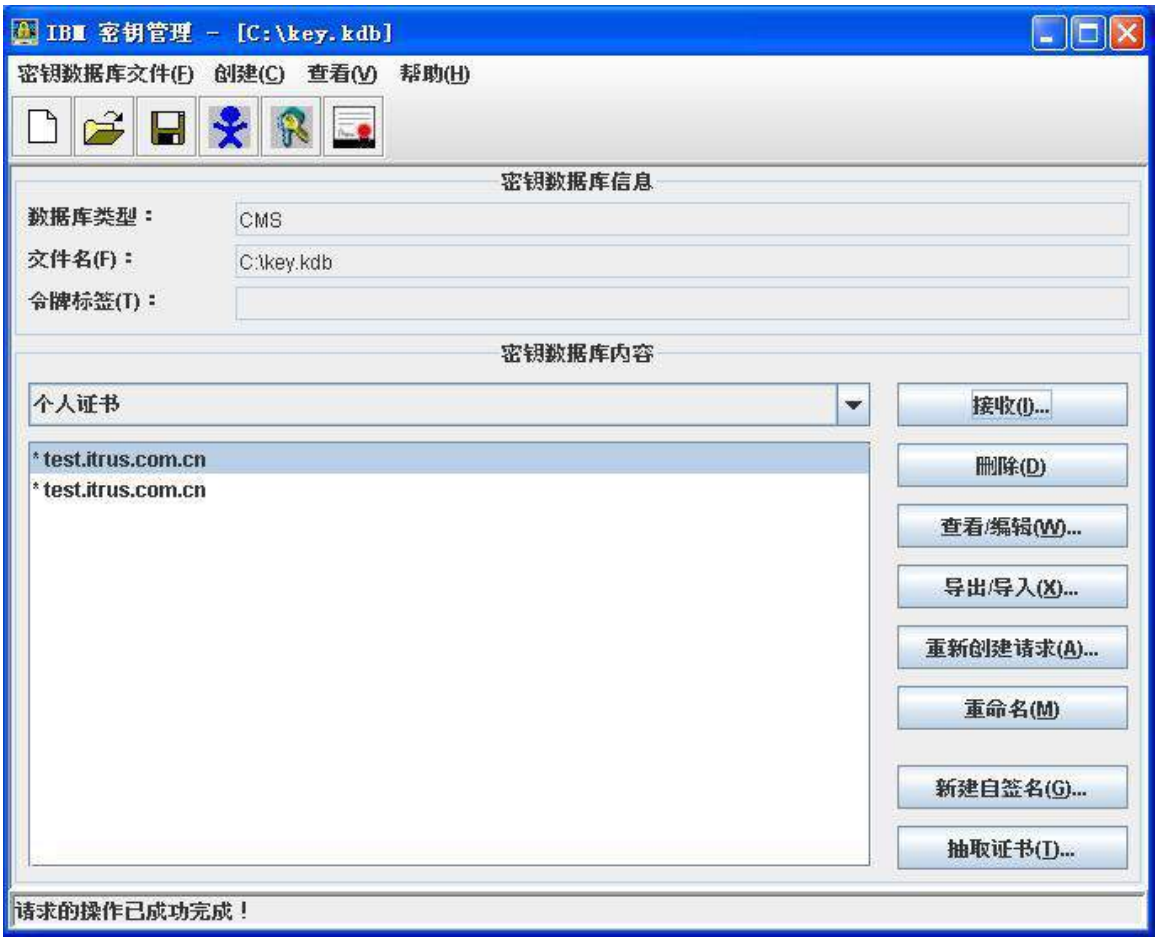


導入證書成功



IHS7 版本 I Key Manager 的 bug 問題處理

在 IHS7 版 I Key Man 中接收服務器證書後，可能在“個人證書”中同時出現兩個完全相同的服務器證書項的 bug 問題。此模式下的 kdb 文件，在 Windows 平台下的 IHS 中應用不受影響，但在 Unix/Linux 平台下，大部分 IHS 將無法加載該 kdb 文件。因此，需要通過新建一個空的 kdb 文件，並將您存在 bug 問題的 kdb 文件中，“個人證書”下存儲的“test.itrus.com.cn”的服務器證書遷移到新建的空 kdb 文件中。 IHS7 bug 示例圖：

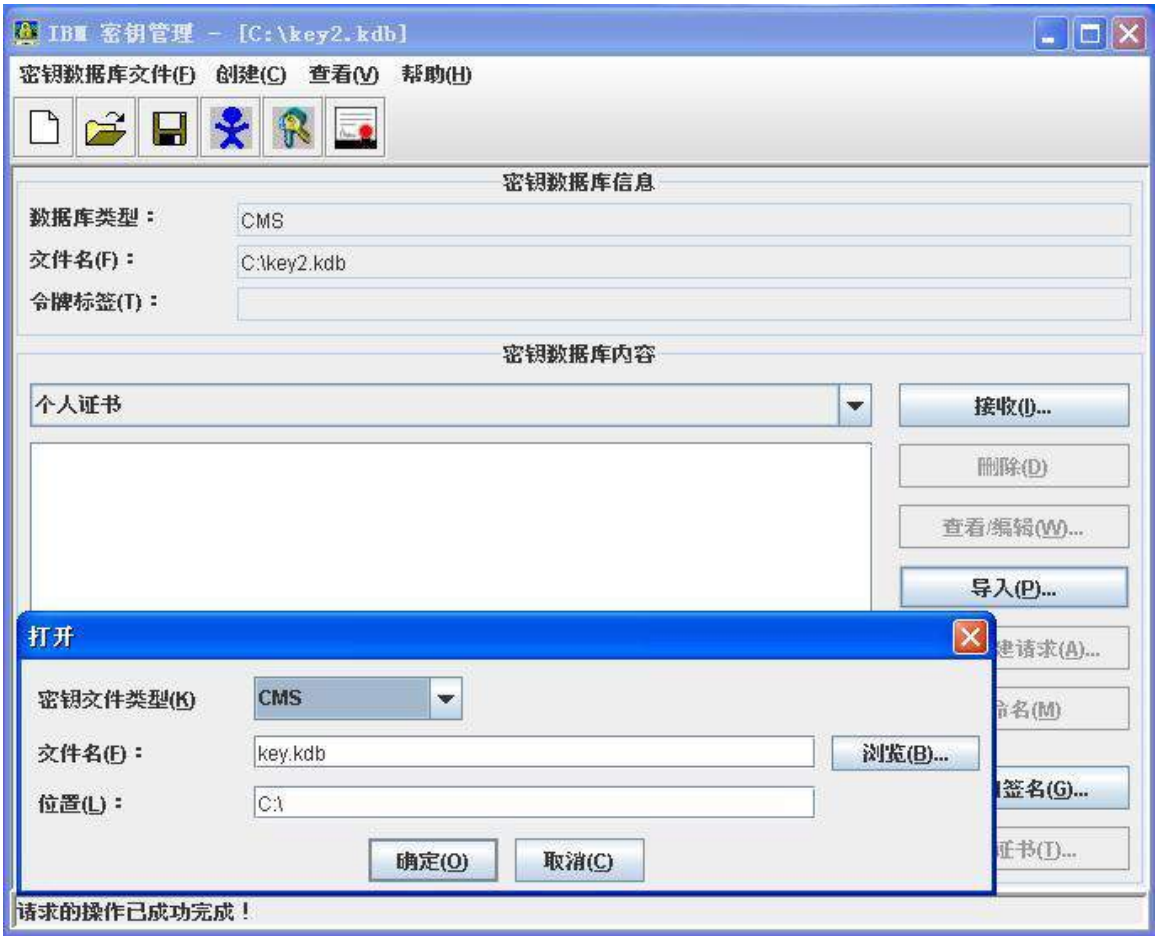


新建空的 CMS 格式 kdb 文件，設置文件名與原 kdb 文件名不同。

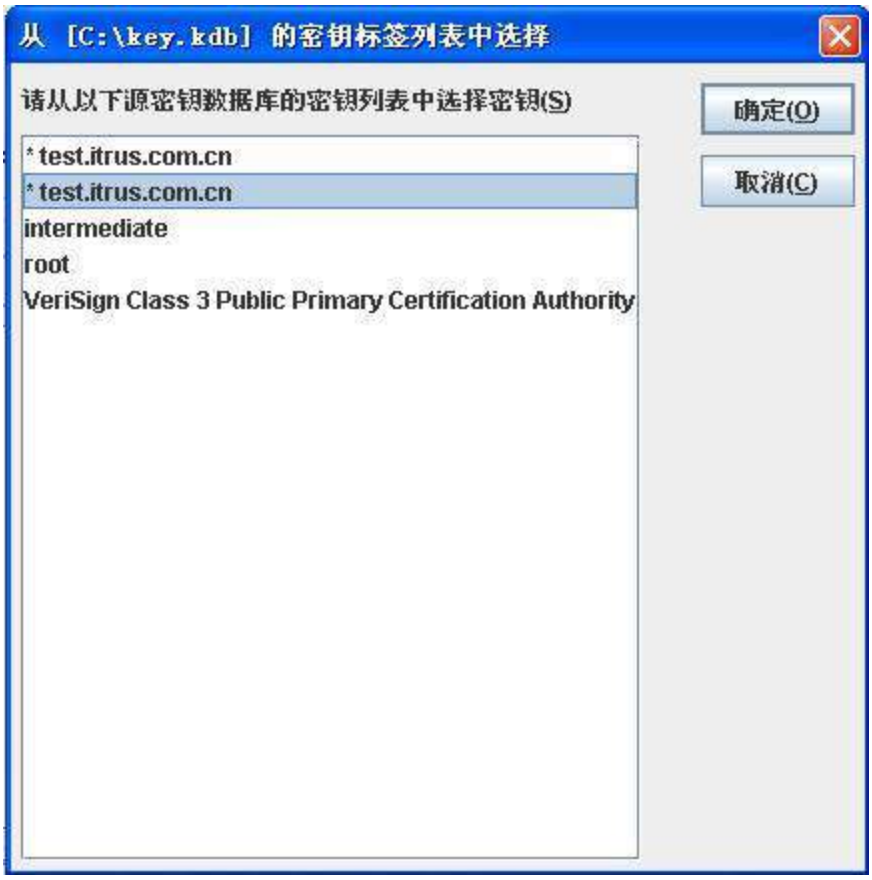
注意：請選中“**將密碼存儲到文件**”選項，此選項將把密碼加密保存到擴展名為.sth 的文件中。 IHS 啟動時，會自動從該.sth 文件中讀取密碼，如果不選擇此項啟動 HTTP SERVER 時會報錯。

請留意點擊“確定”後是否生成.sth 文件。部分版本 ikeyman 存在環境兼容 bug，雖已勾選“將密碼存儲到文件”，但無法生成.sth 的密碼存儲文件。在新建的 kdb 文件中，

切換到“個人證書”選項卡，選擇“導入”。選擇密鑰文件類型為 CMS，並選中您存在 bug 問題的 key.kdb 文件。

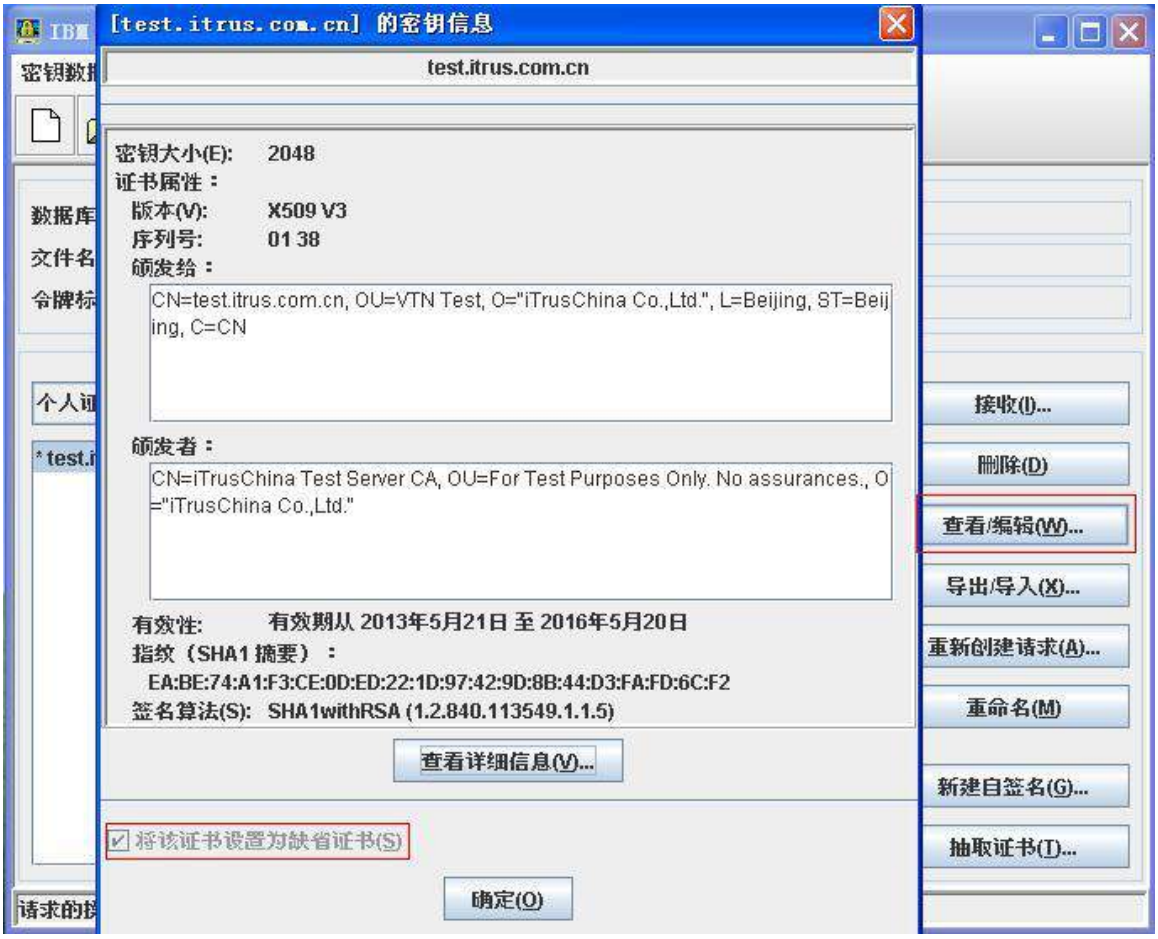


選擇將您原 kdb 文件中的任意一個“個人證書”導入到新的 kdb 文件中。



選擇導入完成之後，請確認檢查證書已被設置為缺省證書，並確保“簽署人證書”中同時已包含所有必需的 CA 證書（包含兩張中級 CA 及一張 root 證書）。

確認新建的 kdb 文件中“簽署人證書”完整，與之前製作的 kdb 文件包含的簽署人證書相同。 “個人證書”中不存在重複的證書項目即可。



確認證書成功遷移到新的 kdb 文件中後，可保留新的 kdb 文件，並刪除存在 bug 的 kdb 文件。

步驟 3：安裝服務器證書

打開 IHS 安裝目錄下 conf 目錄中的 httpd.conf 文件，在所有已存在的 Load Module 條目下方添加如下條目以加載 IBM SSL 模塊 LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

在 httpd.conf 文件結尾處添加如下內容：

```
<IfModule mod_ibm_ssl.c>
  Listen 0.0.0.0:443
  <VirtualHost *:443>
   SSLEnable
   SSLProtocolDisable SSLv2 SSLv3
   SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA
   SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA
   SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA
  </VirtualHost>
</IfModule>
SSLDisable
KeyFile "C:\Program Files\IBM\SSLKeyDB\key.kdb"
```

保存退出，並重啟 IHS。

完成 HIS 的設置後，您還需要登錄 Websphere 控制台，檢查“環境”=“虛擬主機”檢查配置中 default_host 或您自定義的虛擬主機項，“主機別名”下，是否已正確啟用 443 端口。

步驟 4：服務器證書的備份及恢復

在您成功的安裝和配置了服務器證書之後，請務必依據下面的操作流程，備份好您的服務器證書，以防證書丟失給您帶來不便。

1. 服務器證書的備份

備份服務器證書密鑰庫文件 key.kdb、key.rdb、key.sth 即可完成服務器證書的備份操作。

2. 服務器證書的恢復

請參照服務器證書配置部分，將服務器證書密鑰文件恢復到您的服務器上，並修改配置文件，恢復服務器證書的應用。

IBM WebSphere IKEYMAN 界面 SSL 安装指南

步驟 1：下載中級 CA 證書

1. 通過此鏈接下載中級 CA 證書。

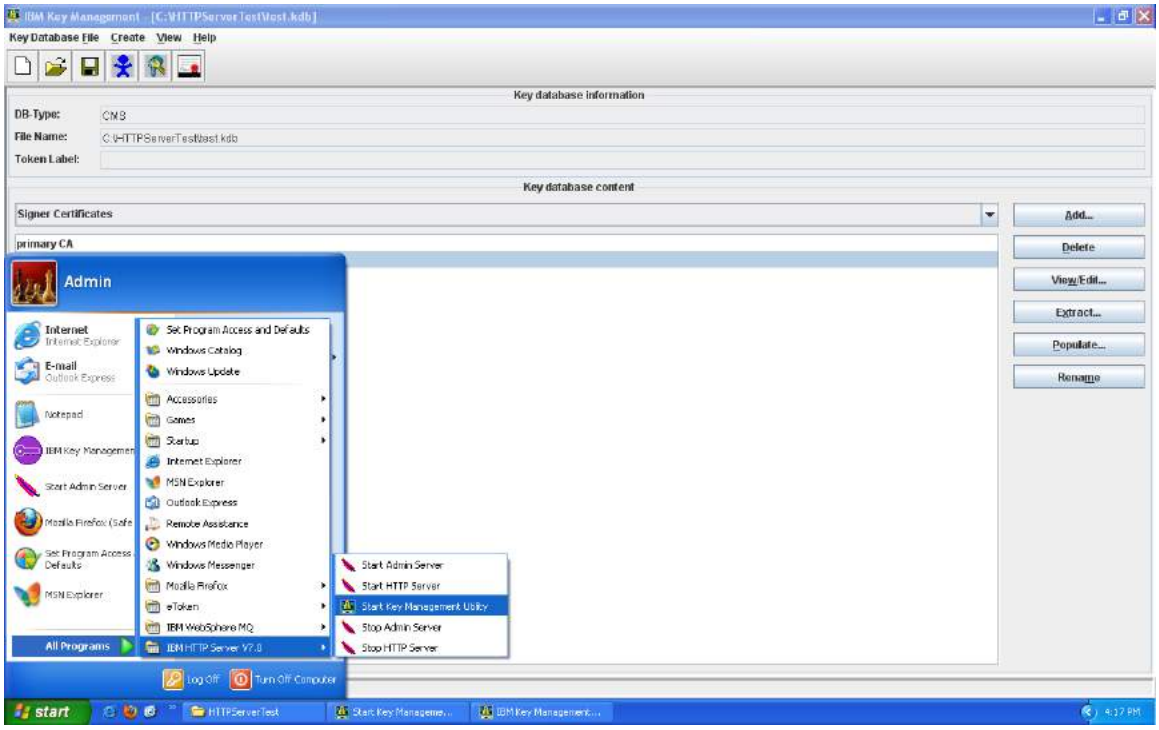
選擇和你的 SSL 證書適合的中級 CA 證書。

2. 複製中級 CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 intermediate.cer.

步驟 2：安裝中級 CA 證書

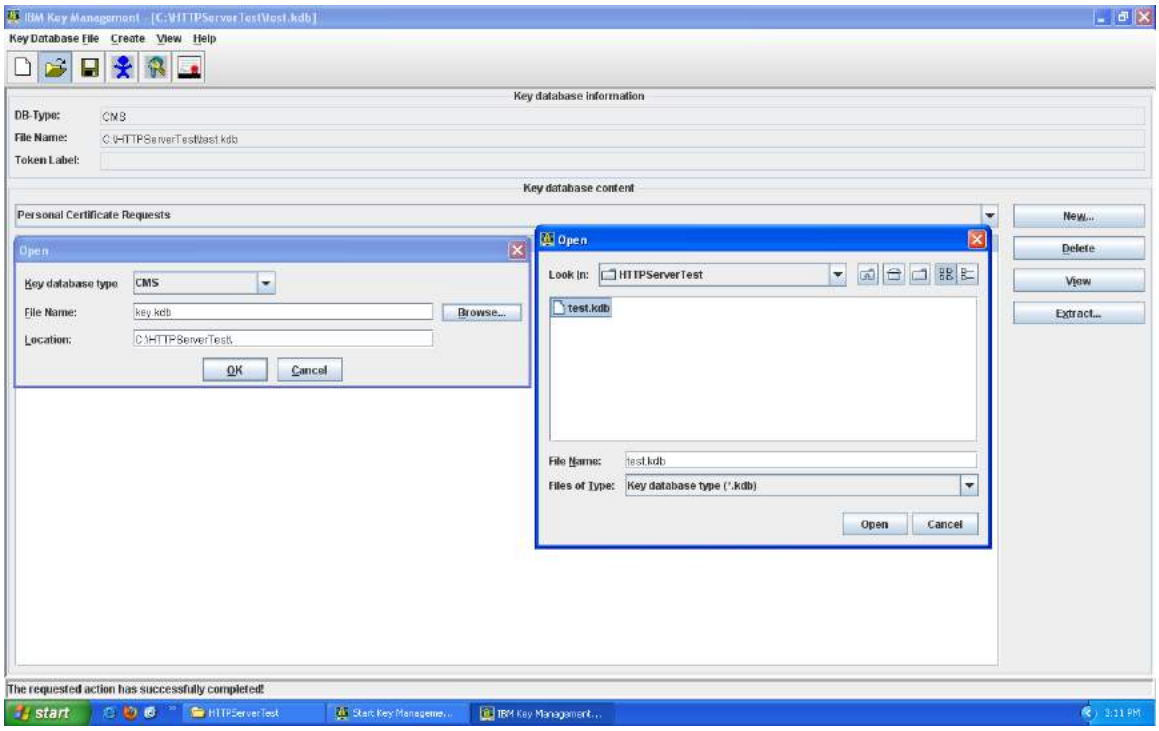
1. 開啟 Key Management Utility (iKeyman)：

Windows 界面：在開始界面，點擊 Start Key Management Utility

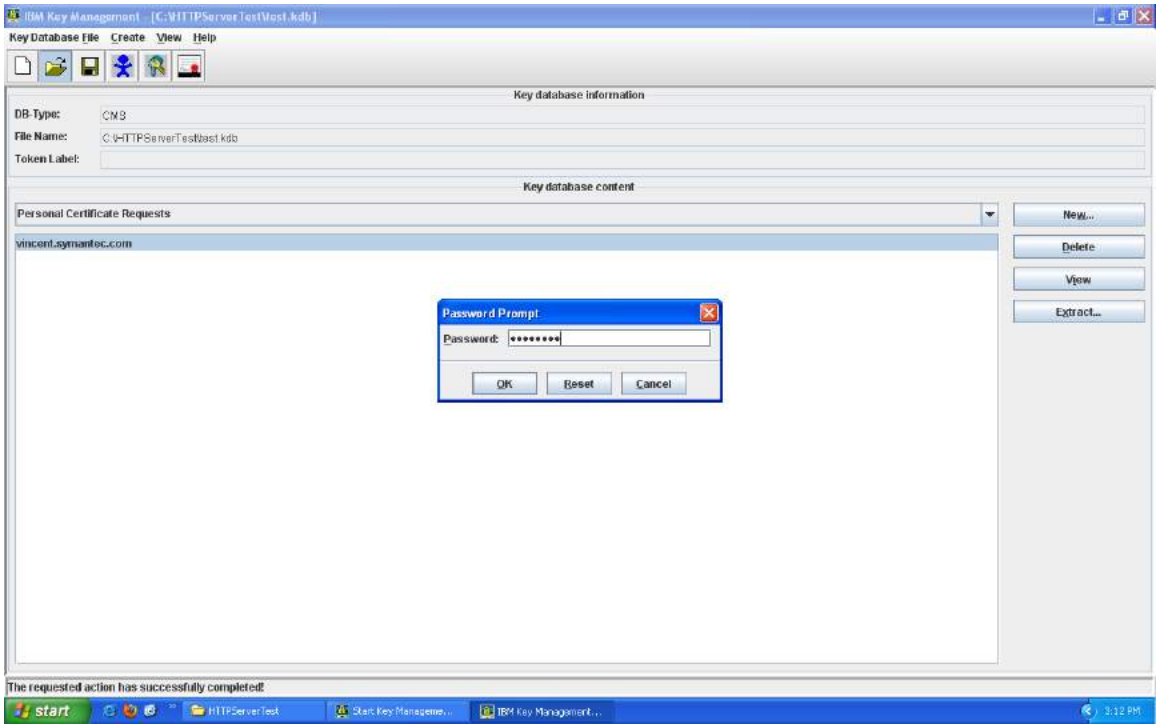


AIX, Linux 或 Solaris: 在命令行里輸入 ikeyman

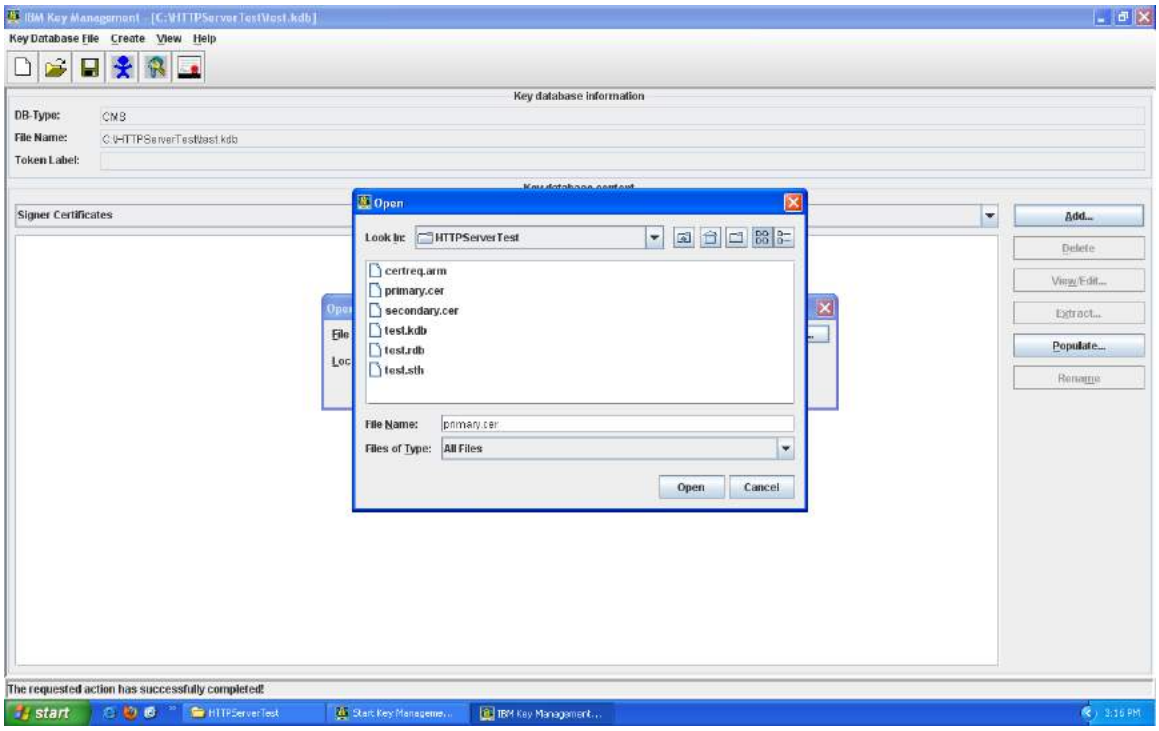
2. 打開生成 CSR 的密鑰數據庫文件。



3. 輸入密碼後點擊 OK。

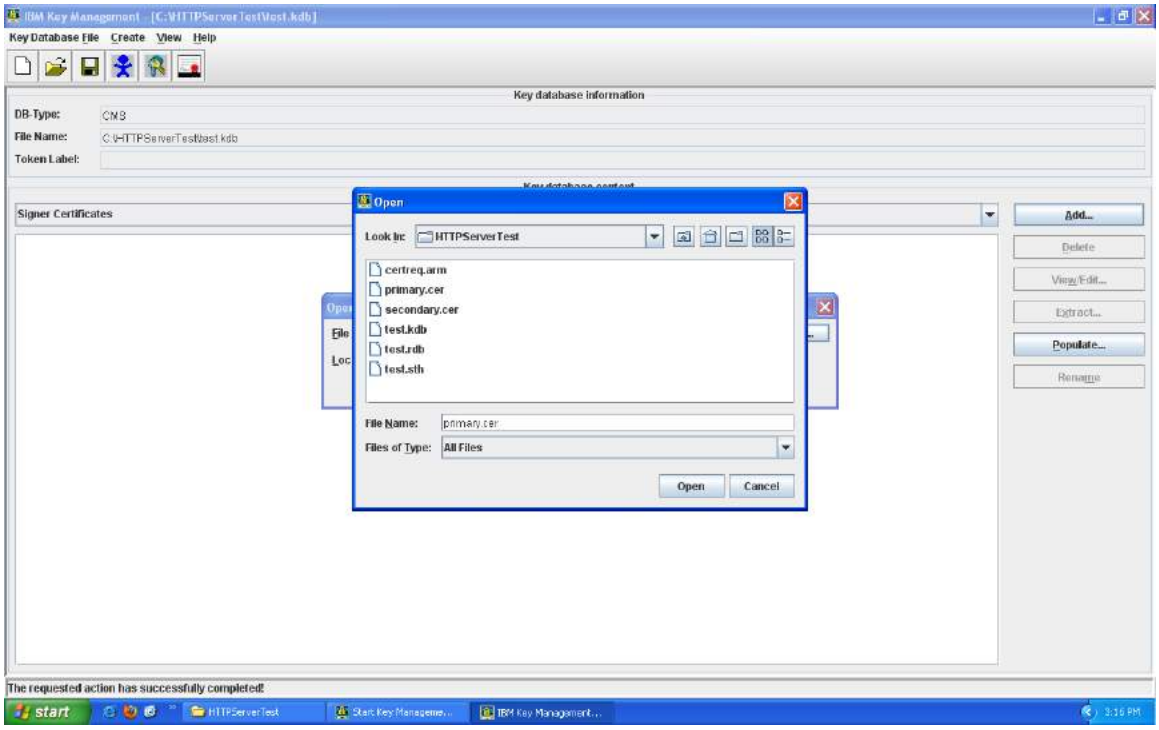


4. 選擇 Signer Certificate，點擊**添加**。



5. 點擊 Files of Type 然後選擇 **All Files**。

6. 輸入 **Intermediate.cer** 證書的路徑。



7. 點擊 OK。

8. 輸入證書的標籤，如：Intermediate CA

步驟 3：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。

2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

-----BEGIN CERTIFICATE-----

[加密數據]

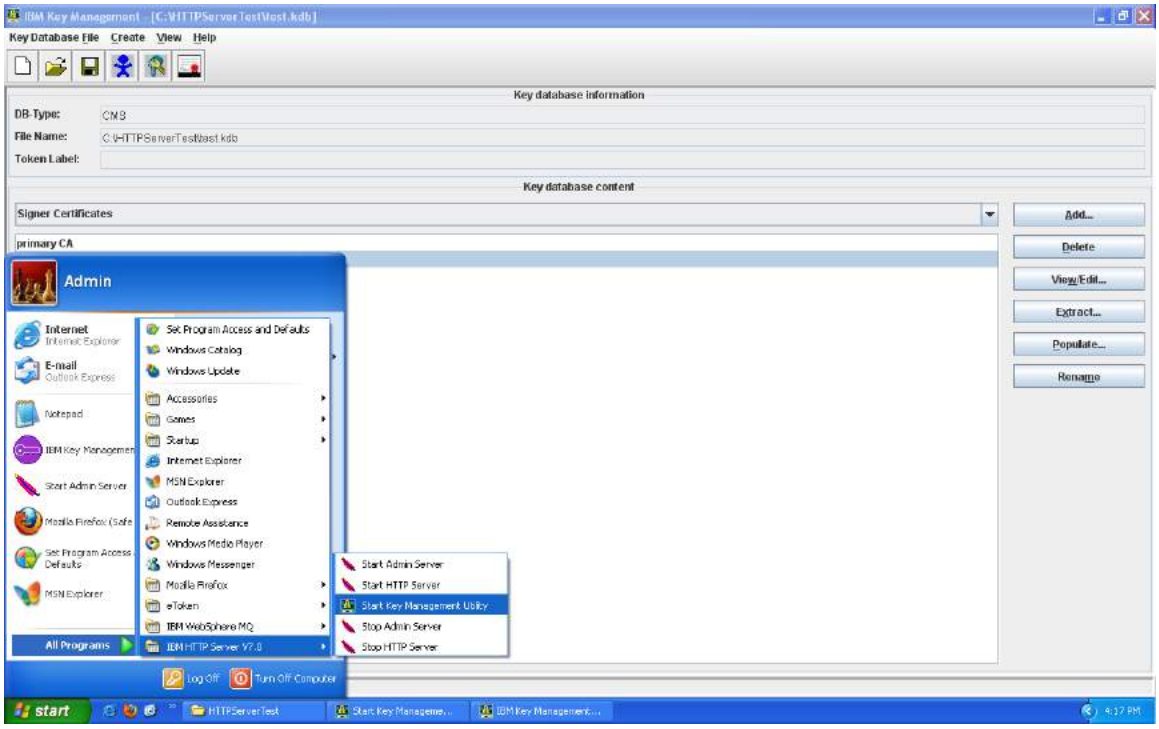
-----END CERTIFICATE-----

3. 把證書存檔為 filename.cer 文檔。

步驟 4：安裝 SSL 證書

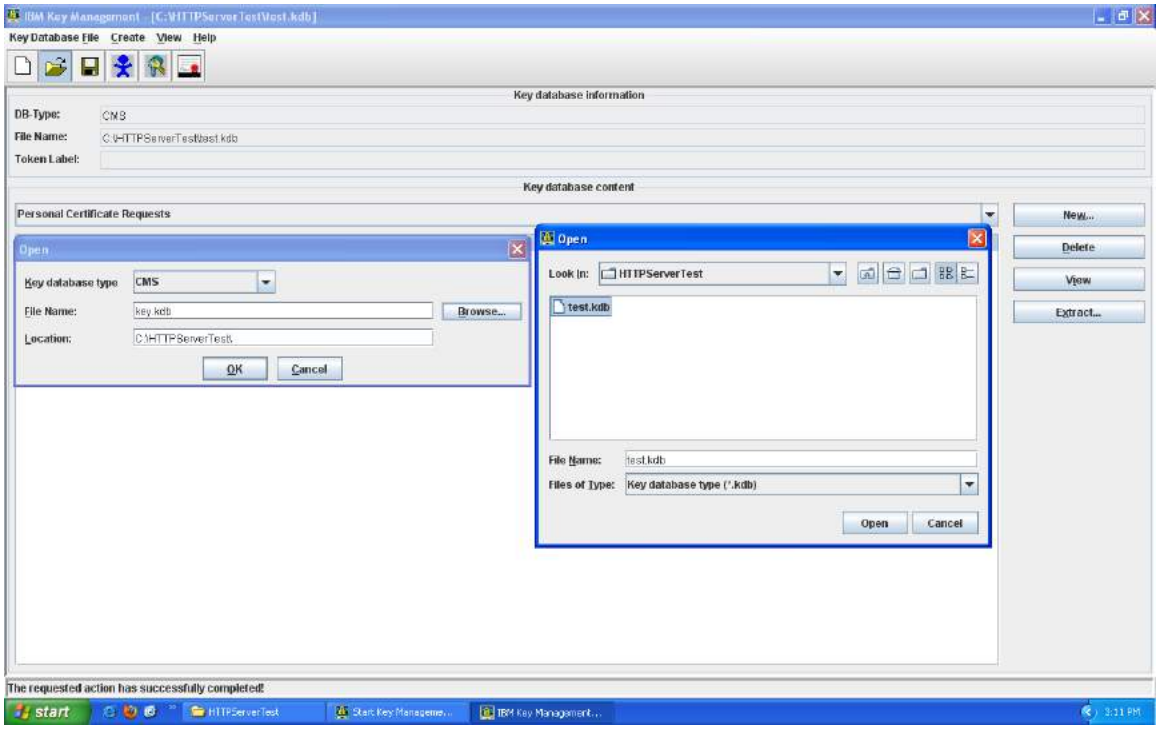
1. 開啟 Key Management Utility (iKeyman)：

Windows 界面：在開始界面，點擊 Start Key Management Utility



AIX, Linux 或 Solaris: 在命令行里輸入 ikeyman

2. 在 Key Database File 目錄裡點擊 **Open**。點擊 **Key database type**，然後選擇 **CMS**。

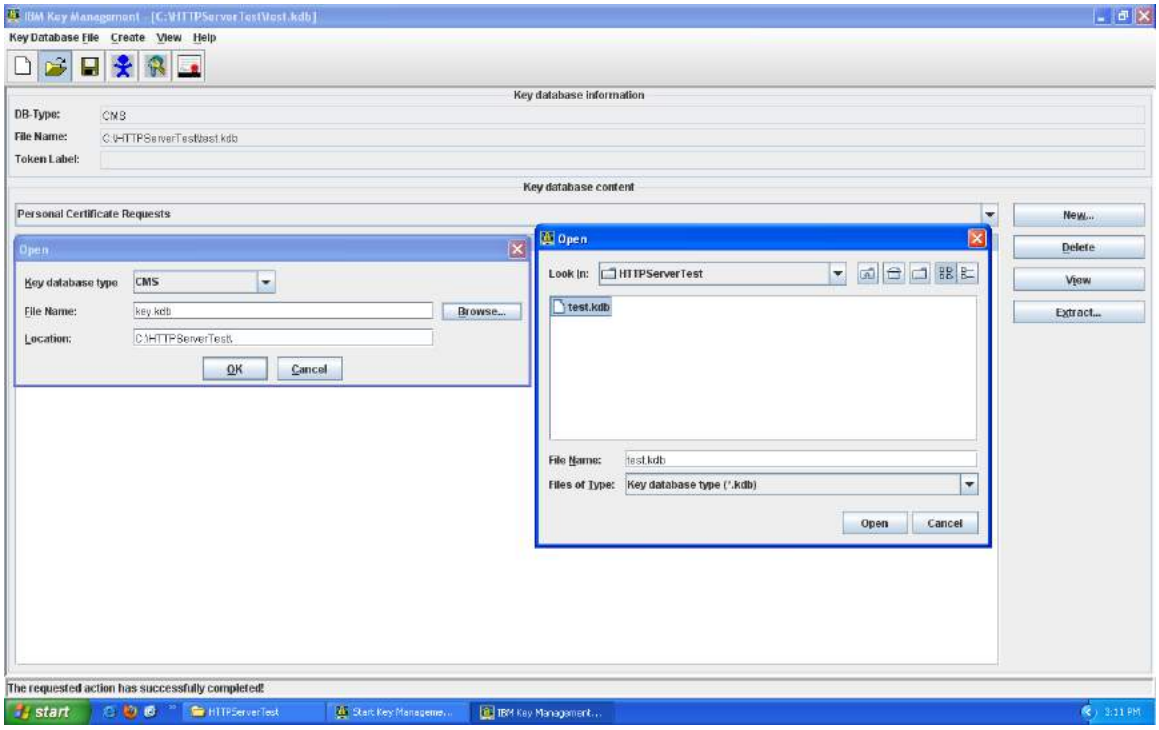


3. 點擊 **Browse**，瀏覽至儲存 Key Database 文件的目錄。

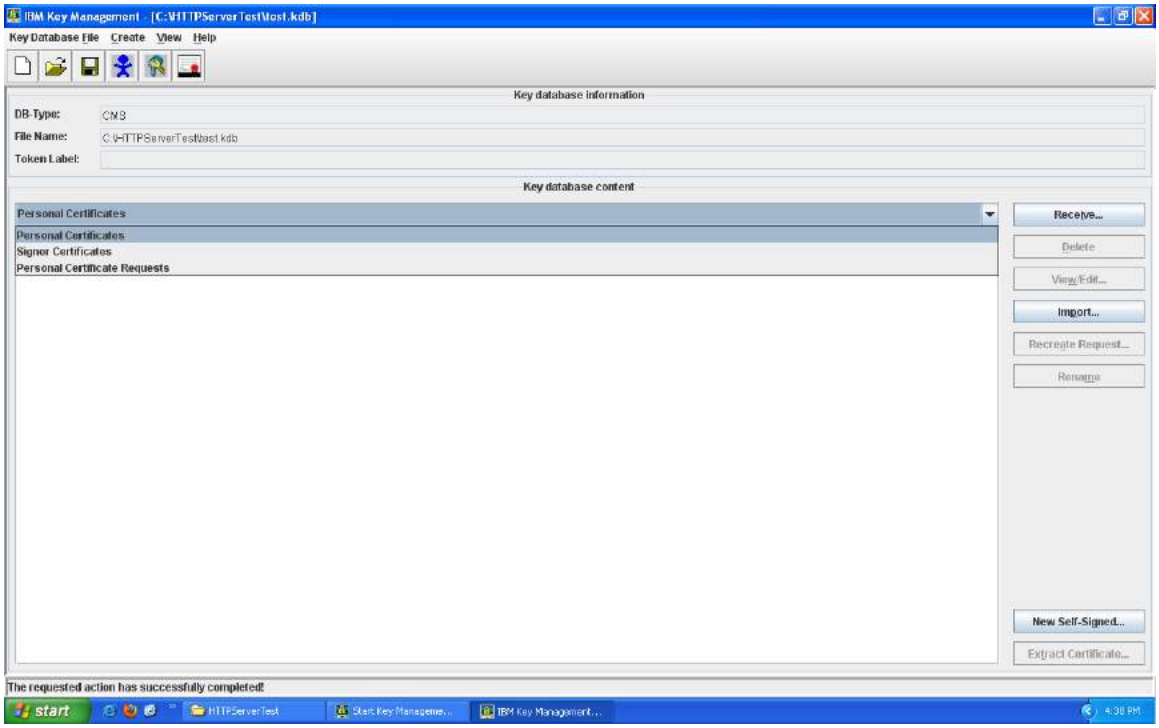
4. 選擇你要添加至證書的密鑰數據庫文件，例：**key.kdb**。

5. 點擊**開啟**。

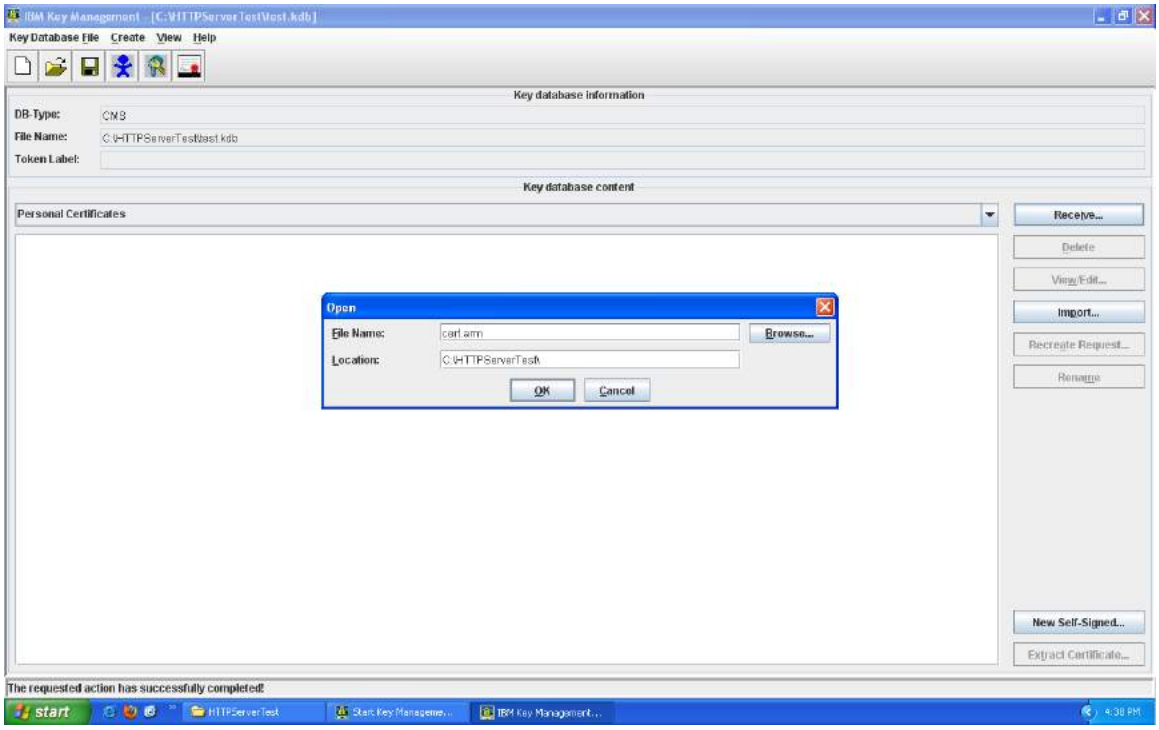
6. 在密碼提示窗口，輸入你在創建密鑰數據庫時所使用的密碼，然後點擊 OK。



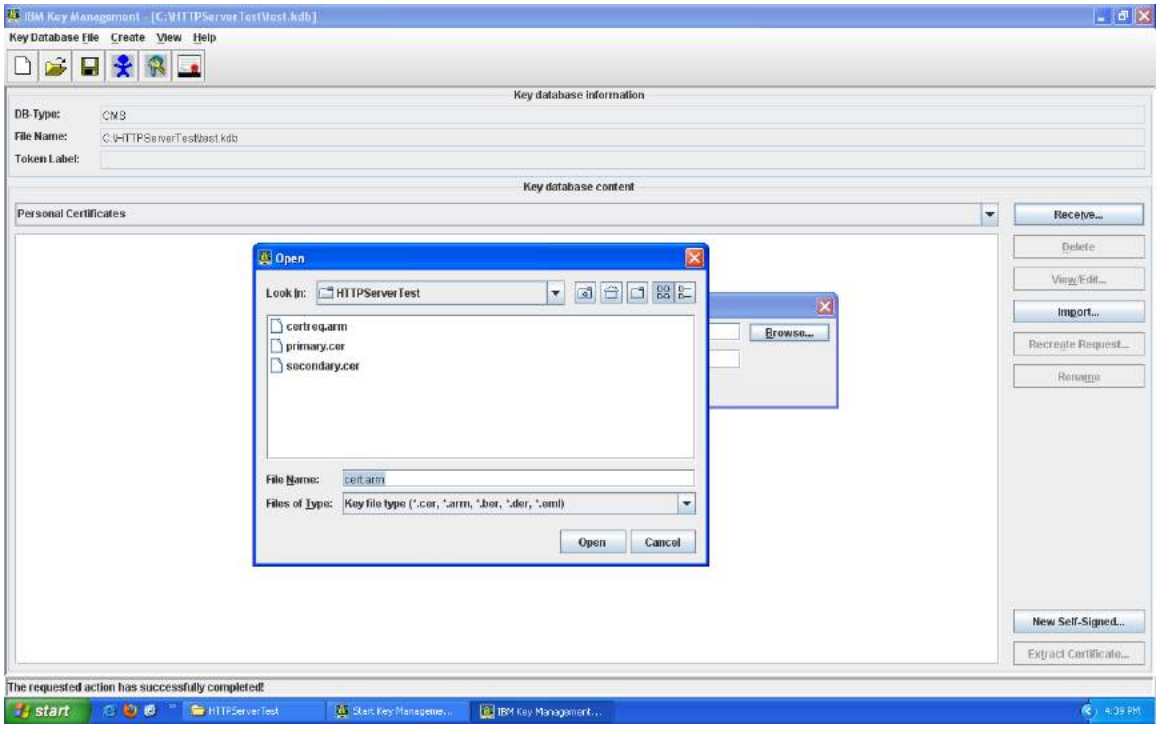
7. 選擇 Personal Certificates view。



8. 點擊 Receive。



9. 點擊 **Browse** 選擇證書的名稱和路徑。



10. 點擊 **OK**。

11. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

使用命令行界面安装 IBM WebSphere SSL 證書

步驟 1：下載中級 CA 證書

1. 通過此鏈接下載中級 CA 證書。

   選擇和你的 SSL 證書適合的中級 CA 證書。

2. 複製中級 CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為

   intermediate.cer.

步驟 2：安裝中級 CA 證書

1. 運行以下命令把 intermediate.cer 加入到密鑰數據庫：

UNIX

gsk7cmd -cert -add -db filename -pw password -label label -file filename -format ascii

Windows

runmqckm -cert -add -db filename -pw password -extensionel -file filename -format ascii

- **-db filename** 是 CMS 密鑰數據庫的全文件名，例：dbkey.kdb

- **-pw password** 是.cms 擴展的 CMS 密鑰數據庫的密碼
- **-label** 是附加到證書的密鑰標籤，例：”ibmwebspheremqqmname”
- **-file filename** 是中級 CA 證書的全文件名，例：intermediate.cer
- **-format ascii** 代表證書的格式。可把數值更換為 Base64-encoded ASCII。默認是 ascii。

步驟 3：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

-----BEGIN CERTIFICATE-----

[加密數據]

-----END CERTIFICATE-----

3. 把證書存檔為 **filename.cer** 文檔。

步驟 4：安裝 SSL 證書

1. 使用以下命令行把證書安裝至 iKeycmd（以 UNIX 命令行）：

UNIX

gsk7cmd -cert -receive -file filename -db filename -pw password -format ascii

Windows

runmqckm -cert -receive -file filename -db filename -pw password -format asci

- **-db filename** 是 CMS 密鑰數據庫的全文件名，例：dbkey.kdb
- **-pw password** 是.cms 擴展的 CMS 密鑰數據庫的密碼
- **-label** 是附加到證書的密鑰標籤，例：”ibmwebspheremqqmname”
- **-file filename** 是中級 CA 證書的全文件名，例：intermediate.cer
- **-format ascii** 代表證書的格式。可把數值更換為 Base64-encoded ASCII。默認是 ascii。

步驟 5：提取 SSL 證書

1. 運行以下命令行提取 iKeyman 裡的證書。

UNIX

gsk7cmd -cert -extract -db filename -pw password -label label -target filename -format ascii

Windows

runmqckm -cert -extract -db filename -pw password -label label -target filename -format ascii

- **-db filename** 是 CMS 密鑰數據庫的全文件名，例：dbkey.kdb
- **-pw password** 是.cms 擴展的 CMS 密鑰數據庫的密碼
- **-label** 是證書的標籤
- **-target filename** 是目標文件的名稱
- **-format ascii** 代表證書的格式。可把數值更換為 Base64-encoded ASCII。默認是 ascii。

2. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。