SSL 证书 - IBM

证书安装指南

webnic
accelerate your business

请选择您的版本

IBM AS 400 / iSeries 伺服器 SSL 安装指南

IBM HTTP Server IKEYMAN 界面 SSL 安装说明

IBM WebSphere IKEYMAN 界面 SSL 安装指南

使用命令行界面安装 IBM WebSphere SSL 证书

IBM AS 400 / iSeries 伺服器 SSL 安装指南

步骤 1：下载 Intermediate CA 证书

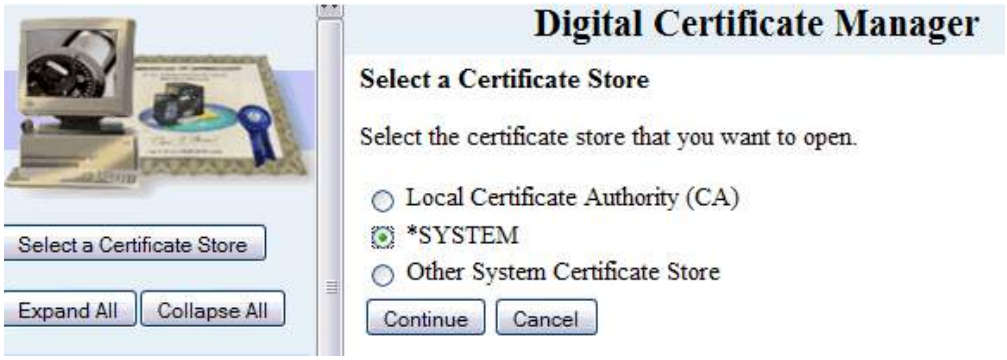
1. 通过此链接下载 Intermediate CA 证书。

   选择和你的 SSL 证书适合的 Intermediate CA 证书。

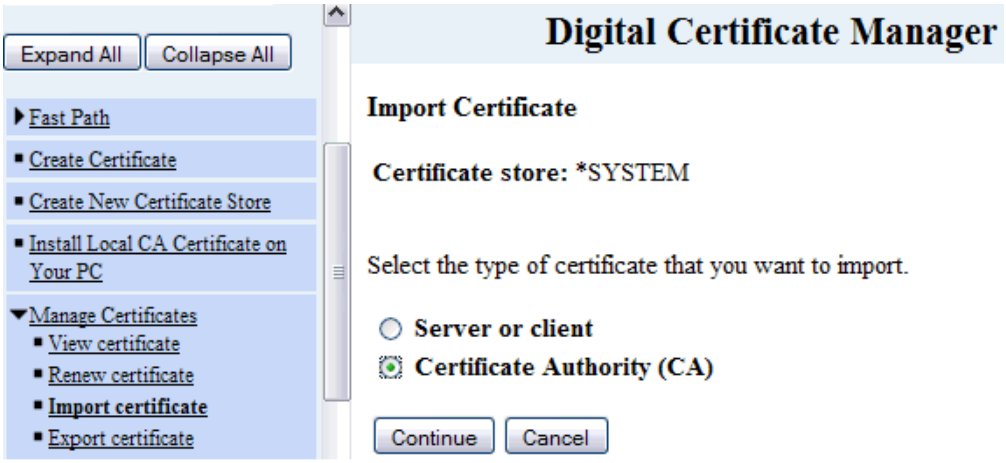
2. 复制 Intermediate CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 intermediate.txt.

步骤 2：安装 Intermediate CA 证书

1. 启动 Digital Certificate Management (DCM)。
2. 从导航面板中，点击 Select a Certificate store > 选择 *System

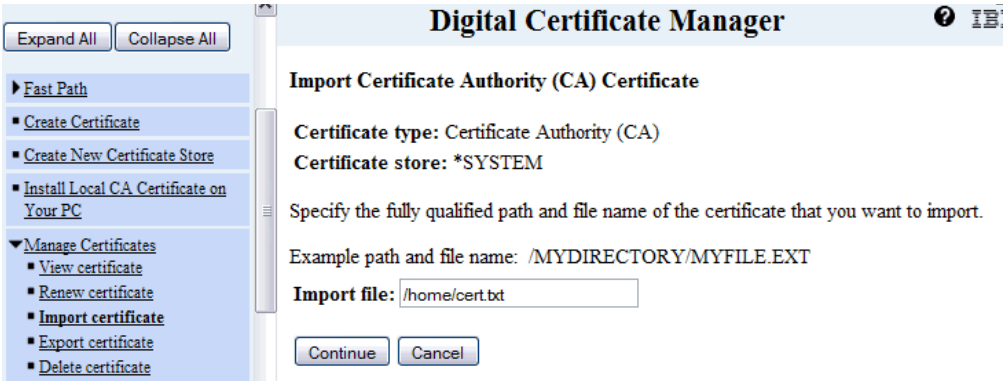


3. 输入证书密码 > 点击 Continue。
4. 从导航面板 选择 Manage Certificate。
5. 从列表中，选择 Import Certificate > Certificate Authority (CA) > 点击 Continue。



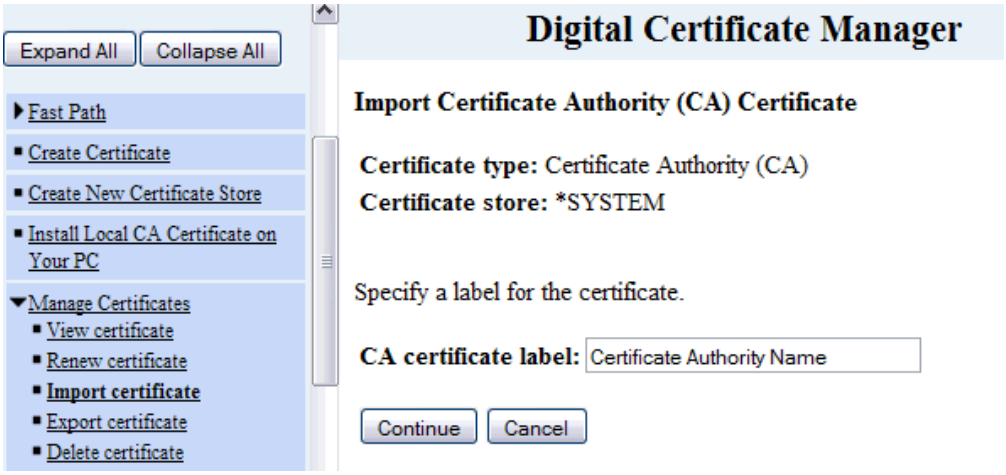
6. 下一步，输入 Intermediate CA 证书文件所在的路径及文件名称。

   例：如果文件是储存在 /home 目录，而 Intermediate CA 证书文件名是 Intermediate.txt，你应输入 /home/intermediate.txt。



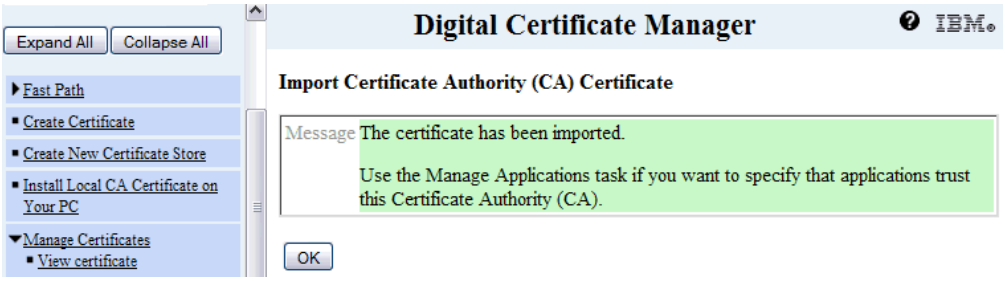
7. 点击**继续**。

8. 创建 CA 证书标签。



9. 点击**继续**。

10. 系统将提示 Intermediate CA 已被导入。点击 **OK**。



步骤 3：获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

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

   [加密数据]

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

3. 把证书存档为 filename.txt 文档。

步骤 4：安装 SSL 证书

1. 启动 Digital Certificate Manager （DCM）。
2. 从导航面板中，点击 Select a Certificate Store > 选择 *SYSTEM。
3. 输入密码，点击继续。
4. 从导航面板，选择 Manager Certificates。
5. 选择 Import Certificate > 选择 Server or Client。
6. 选择证书后完成安装。
7. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。

IBM HTTP Server IKEYMAN 界面 SSL 安装说明

因证书签名算法升级，目前证书均需要使用 SHA-256 算法签发。IBM Http Server 8.5 之前版本不支持 SHA-256 算法，无法加载使用 SHA-256 算法证书生成的 kdb 文件。如需配置 SHA-256 算法证书，请升级 IHS 到 8.5 或以上版本。

步骤 1：创建证书请求

1. 运行 ikeyman

IBM Http Server 附带 I Key Manager 工具，可用于管理 IHS 的证书密钥文件。

IBM HTTP Server V6.1 版本不支持创建 2048 位证书请求，请使用 IHS7 或以上版本自带的 I Key Manager 工具来创建证书申请。选“**Start Key Management Utility**”，运行 I Key Manager

2. 创建密钥库文件

密钥库类型选择“**CMS**”

注意：请选中“**将密码存储到文件**”选项，此选项将把密码加密保存到扩展名为**.sth** 的文件中。IHS 启动时，会自动从该.sth 文件中读取密码，如果不选择此项启动 HTTP SERVER 时会报错。

3. 生成证书请求

IHS6 下的 ikeyman 最高支持 1024 位密钥，目前所有服务器要求 2048 位密钥。使用 IHS7 版 ikeyman 创建的含 2048 位密钥的密钥库文件，在 IHS6 下仍可以正常应用。

导出证书签名请求文件 certreq.arm，并稍后发送给天威诚信，等待证书的签发。

步骤 2：导入服务器证书

1. 获取并导入 CA 证书

将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容分别粘贴到记事本文本文件中。

证书正文的例子：

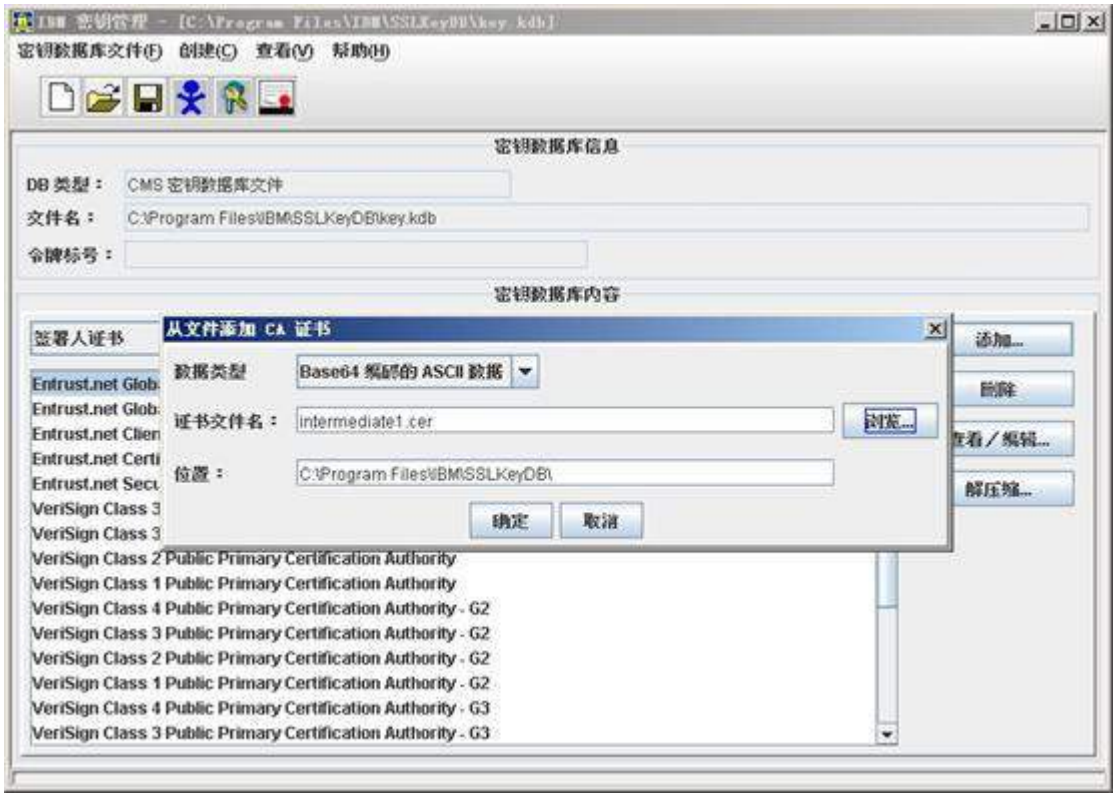
-----BEGIN CERTIFICATE-----

[加密数据]

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

修改文件扩展名，保存为 intermediate1.cer 和 intermediate2.cer 文件(如果只有一中级证书，则只需要保存安装一张中级证书)。

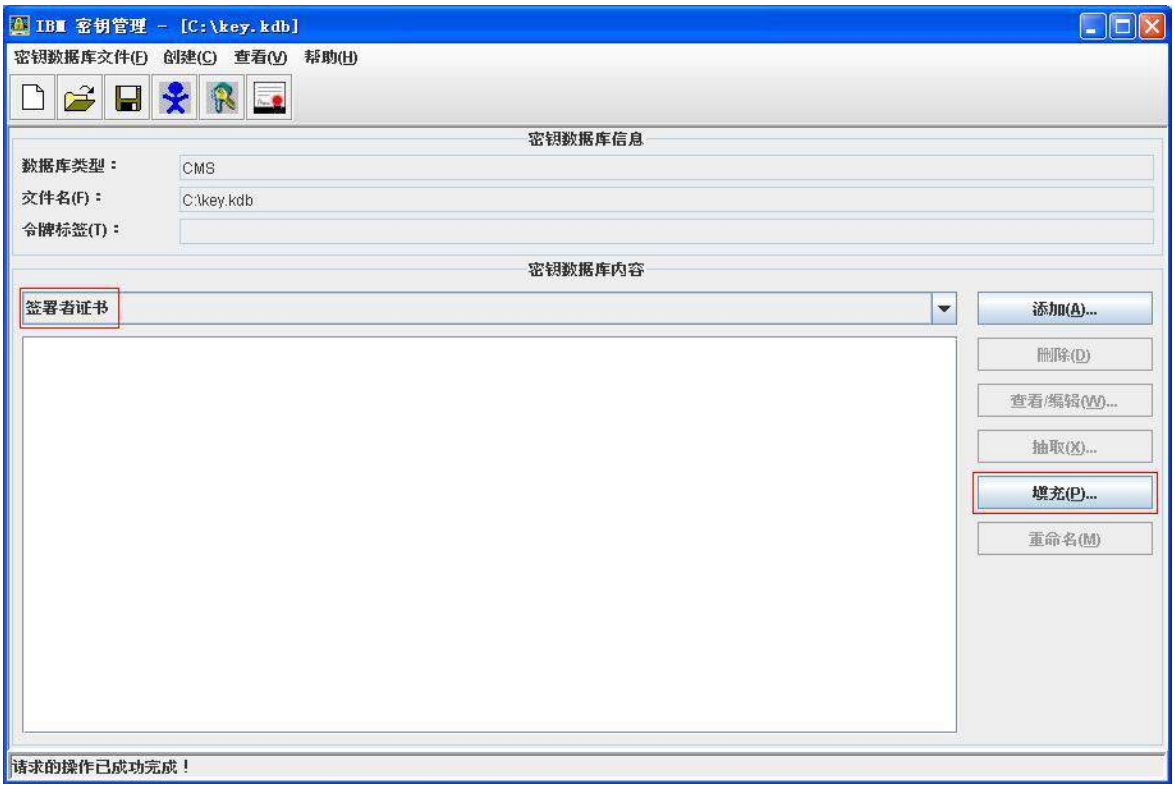
运行 ikeyman 并打开您的 kdb 文件，切换到“签署人证书”视图，并选择“添加”

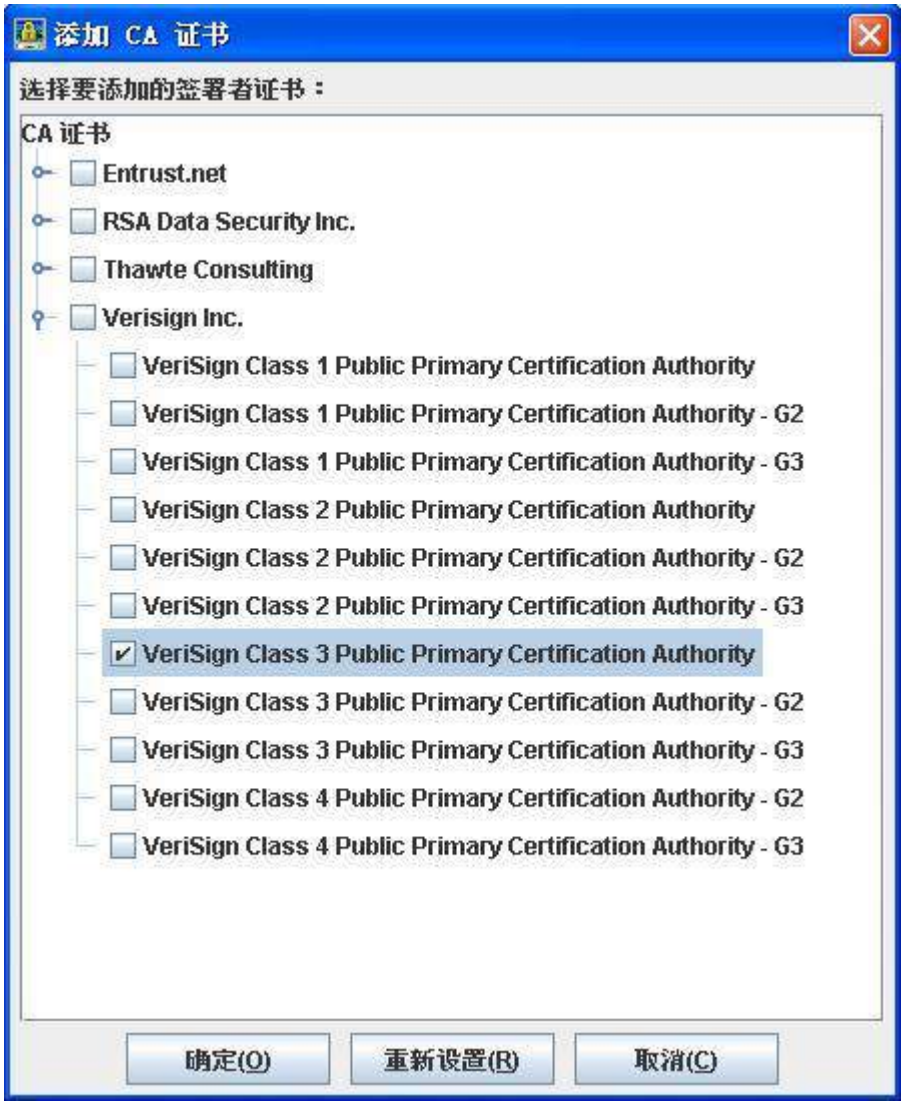


分别添加两张中级 CA 证书，并输入证书的标号

2.　　填充根证书

IHS7 版 ikeyman 创建的 kdb 文件默认不包含服务器证书的根证书，需要使用 IHS7 版 ikeyman 打开生成的 kdb 文件，切换到“**签署人证书**”选项中，选择“**填充**”模式，将 VeriSign 服务器证书的“**VeriSign Class 3 Public Primary Certificate Authority**”的根证书填充到 kdb 格式证书密钥库文件中。





3. 获取并导入服务器证书

将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容粘贴到记事本等文本编辑器中，保存为 server.cer 文件 。

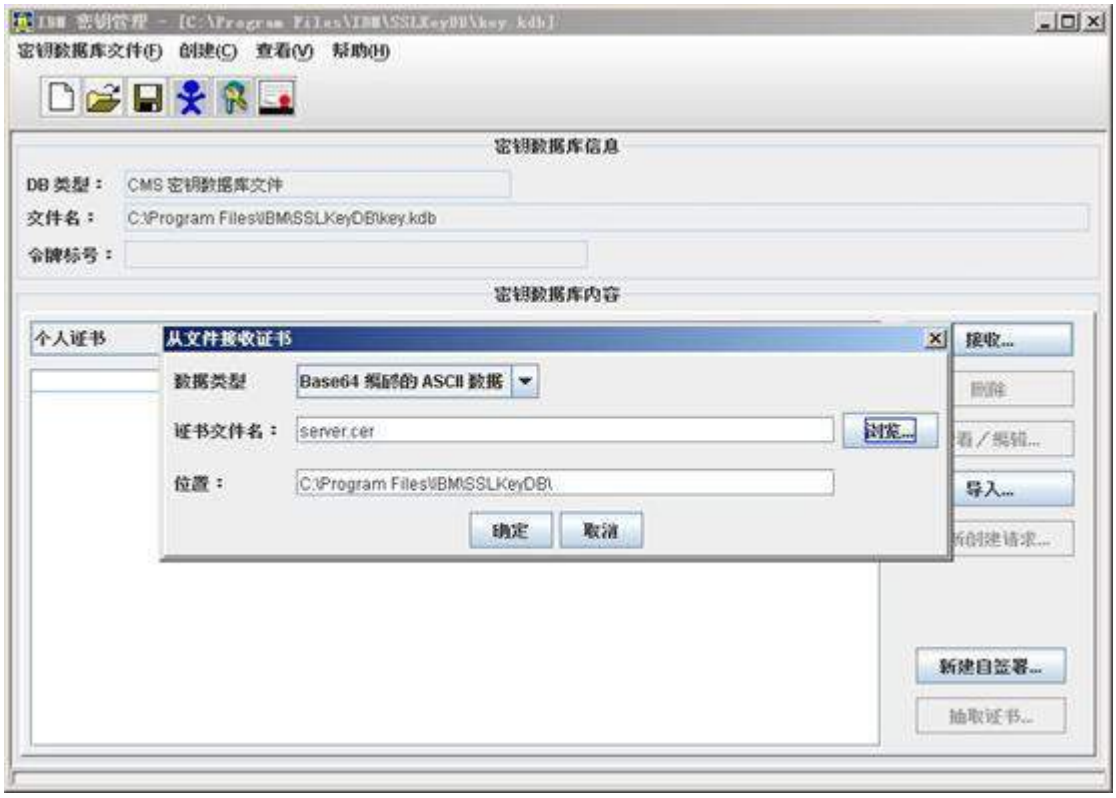
证书正文的例子：

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

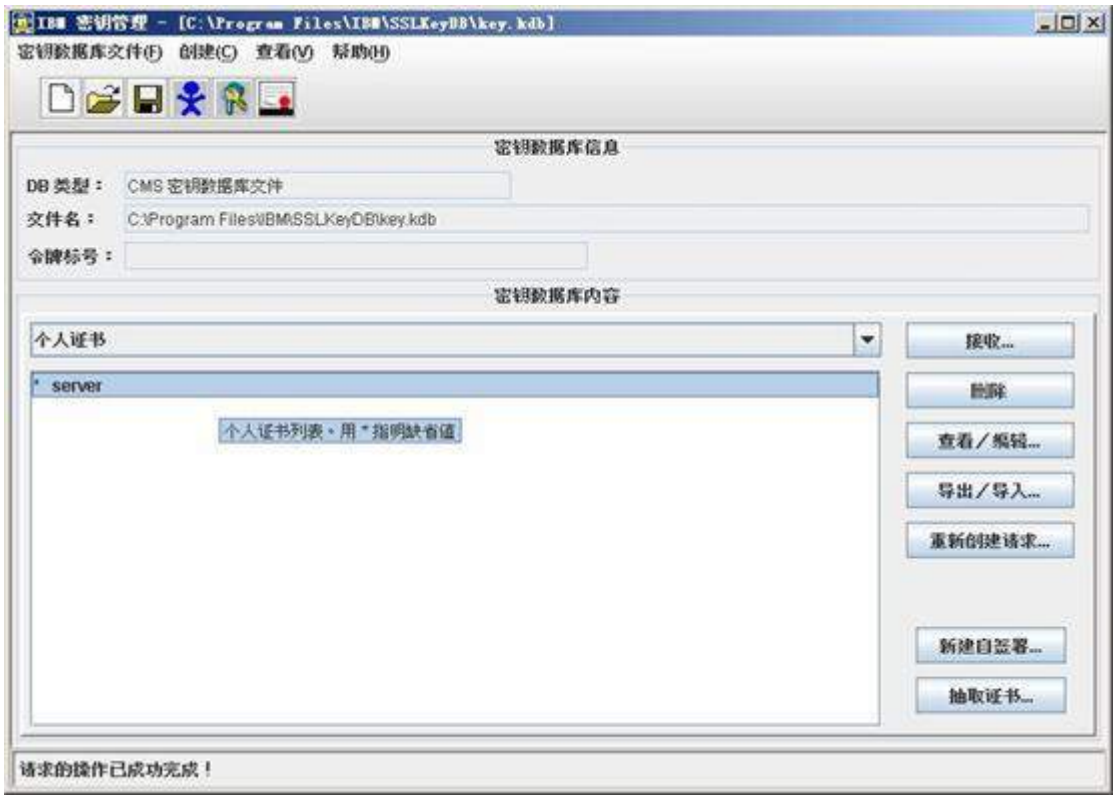
[加密数据]

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

切换到“个人证书”视图，选择“接收”，选择并导入您的服务器证书文件。

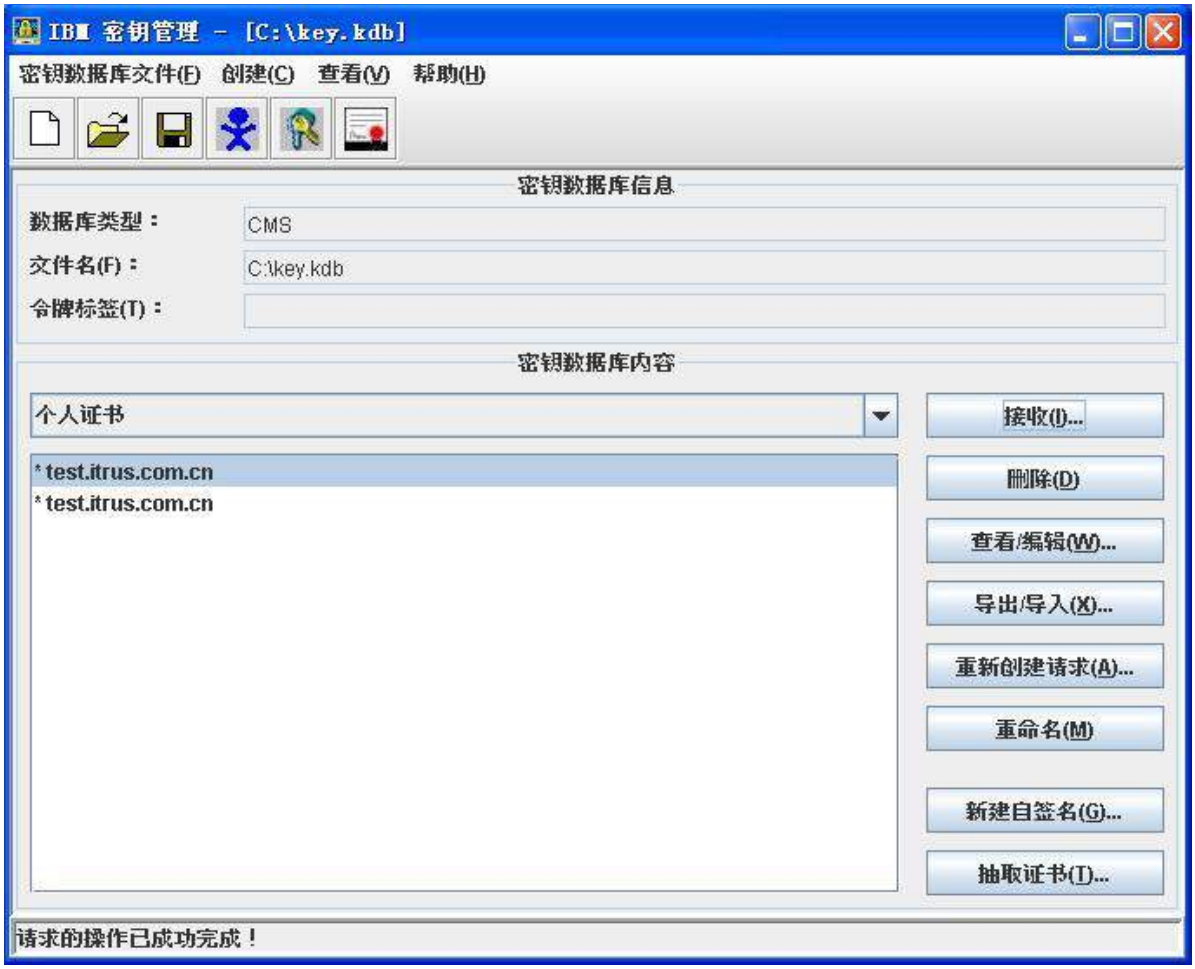


导入证书成功



IHS7 版本 I Key Manager 的 bug 问题处理

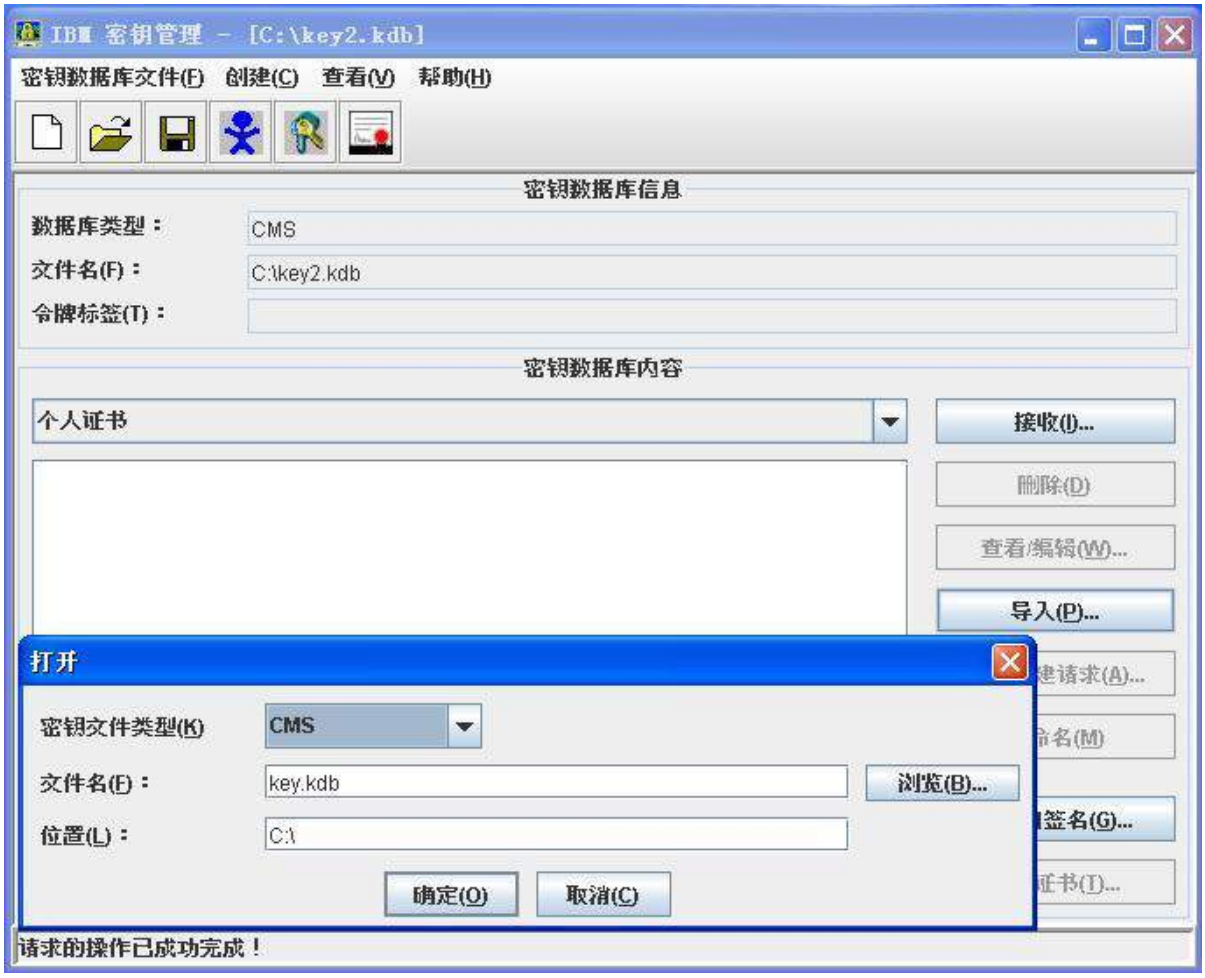
在 IHS7 版 I Key Man 中接收服务器证书后，可能在“个人证书”中同时出现两个完全相同的服务器证书项的 bug 问题。此模式下的 kdb 文件，在 Windows 平台下的 IHS 中应用不受影响，但在 Unix/Linux 平台下，大部分 IHS 将无法加载该 kdb 文件。因此，需要通过新建一个空的 kdb 文件，并将您存在 bug 问题的 kdb 文件中，“个人证书”下存储的“test.itrus.com.cn”的服务器证书迁移到新建的空 kdb 文件中。IHS7 bug 示例图：



新建空的 CMS 格式 kdb 文件，设置文件名与原 kdb 文件名不同。

注意：请选中“将密码存储到文件”选项，此选项将把密码加密保存到扩展名为.sth 的文件中。IHS 启动时，会自动从该.sth 文件中读取密码，如果不选择此项启动 HTTP SERVER 时会报错。

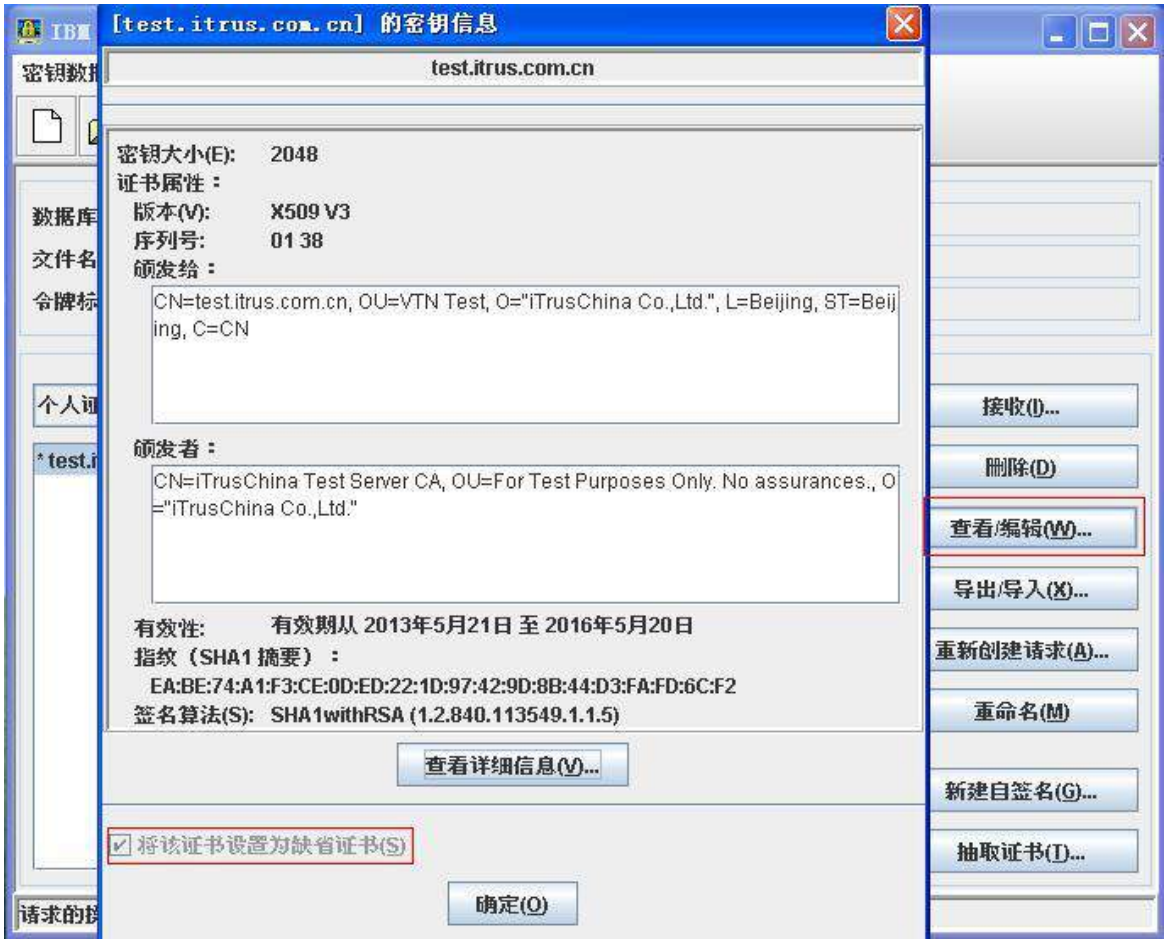
请留意点击“确定”后是否生成.sth 文件。部分版本 ikeyman 存在环境兼容 bug，虽已勾选“将密码存储到文件”，但无法生成.sth 的密码存储文件。在新建的 kdb 文件中，切换到“个人证书”选项卡，选择“导入”。选择密钥文件类型为 CMS，并选中您存在 bug 问题的 key.kdb 文件。



选择将您原 kdb 文件中的任意一个“个人证书”导入到新的 kdb 文件中。

选择导入完成之后，请确认检查证书已被设置为缺省证书，并确保“签署人证书”中同时已包含所有必需的 CA 证书（包含两张中级 CA 及一张 root 证书）。

确认新建的 kdb 文件中“签署人证书”完整，与之前制作的 kdb 文件包含的签署人证书相同。“个人证书”中不存在重复的证书项目即可。



确认证书成功迁移到新的 kdb 文件中后，可保留新的 kdb 文件，并删除存在 bug 的 kdb 文件。

步骤 3：安装服务器证书

打开 IHS 安装目录下 conf 目录中的 httpd.conf 文件，在所有已存在的 Load Module 条目下方添加如下条目以加载 IBM SSL 模
块 LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

在 httpd.conf 文件结尾处添加如下内容：

```
<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，并重启 IHS。

完成 HIS 的设置后，您还需要登录 Websphere 控制台，检查“环境”=“虚拟主机”检查配置中 default_host 或您自定义的虚拟主机项，“主机别名”下，是否已正确启用 443 端口。

步骤 4：服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。

1. 服务器证书的备份

备份服务器证书密钥库文件 key.kdb、key.rdb、key.sth 即可完成服务器证书的备份操作。

2. 服务器证书的恢复

请参照服务器证书配置部分，将服务器证书密钥文件恢复到您的服务器上，并修改配置文件，恢复服务器证书的应用。

IBM WebSphere IKEYMAN 界面 SSL 安装指南

步骤 1：下载中级 CA 证书

1. 通过此链接下载中级 CA 证书。

   选择和你的 SSL 证书适合的中级 CA 证书。

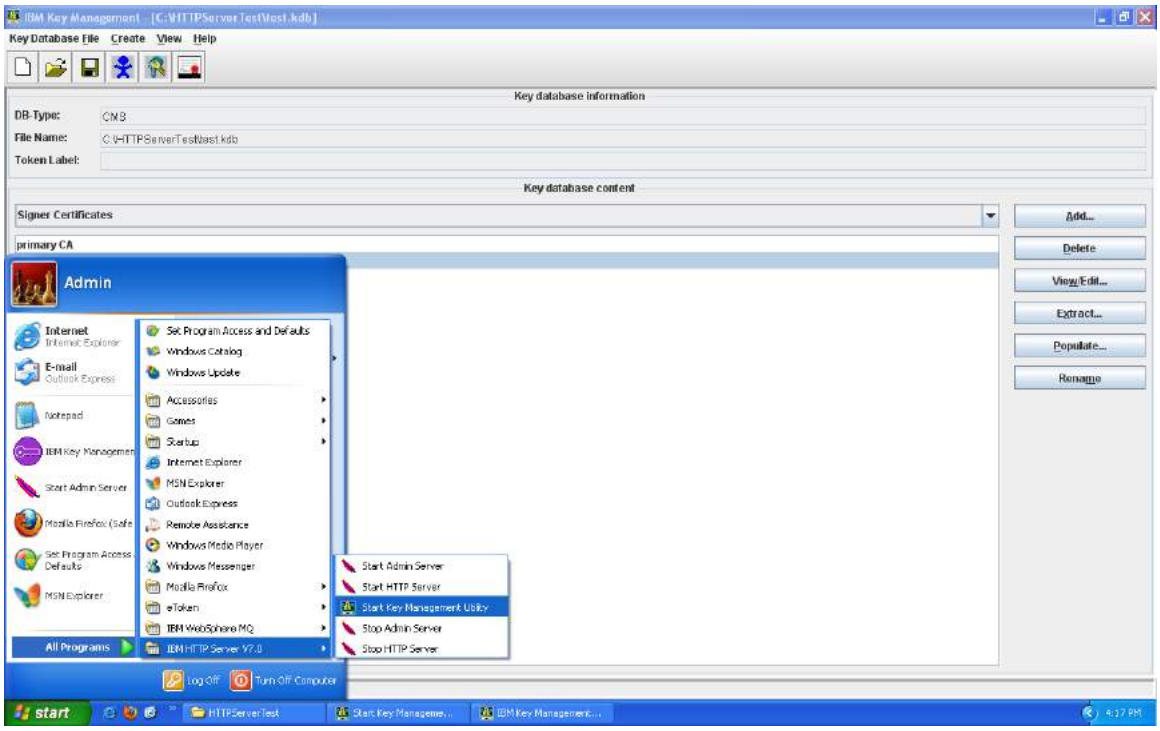
2. 复制中级 CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为

   intermediate.cer.

步骤 2：安装中级 CA 证书

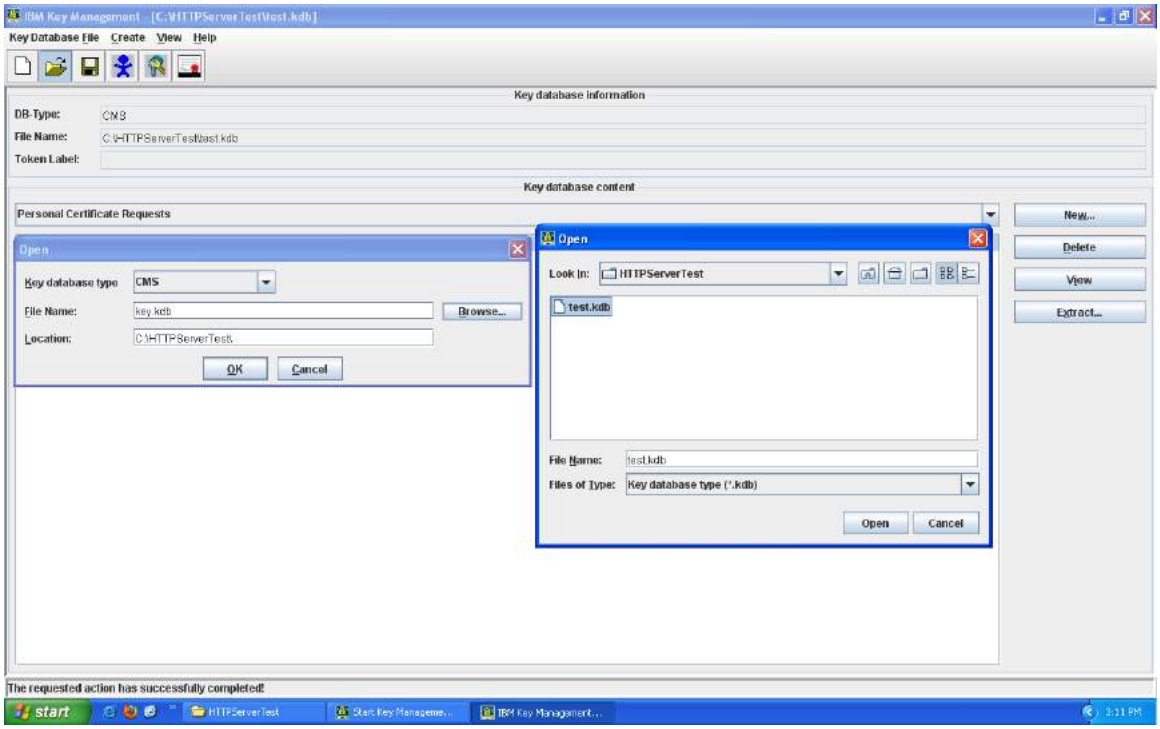
1. 开启 Key Management Utility (iKeyman)：

Windows 界面：在开始界面，点击 Start Key Management Utility

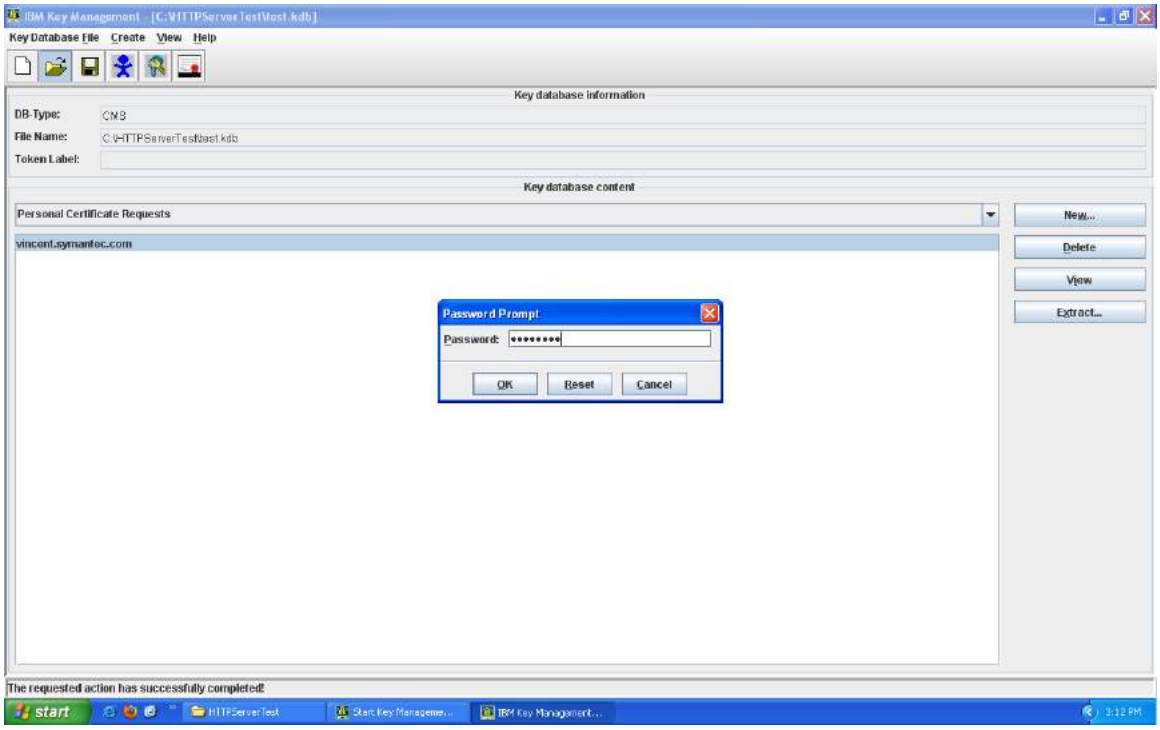


AIX, Linux 或 Solaris: 在命令行里输入 ikeyman

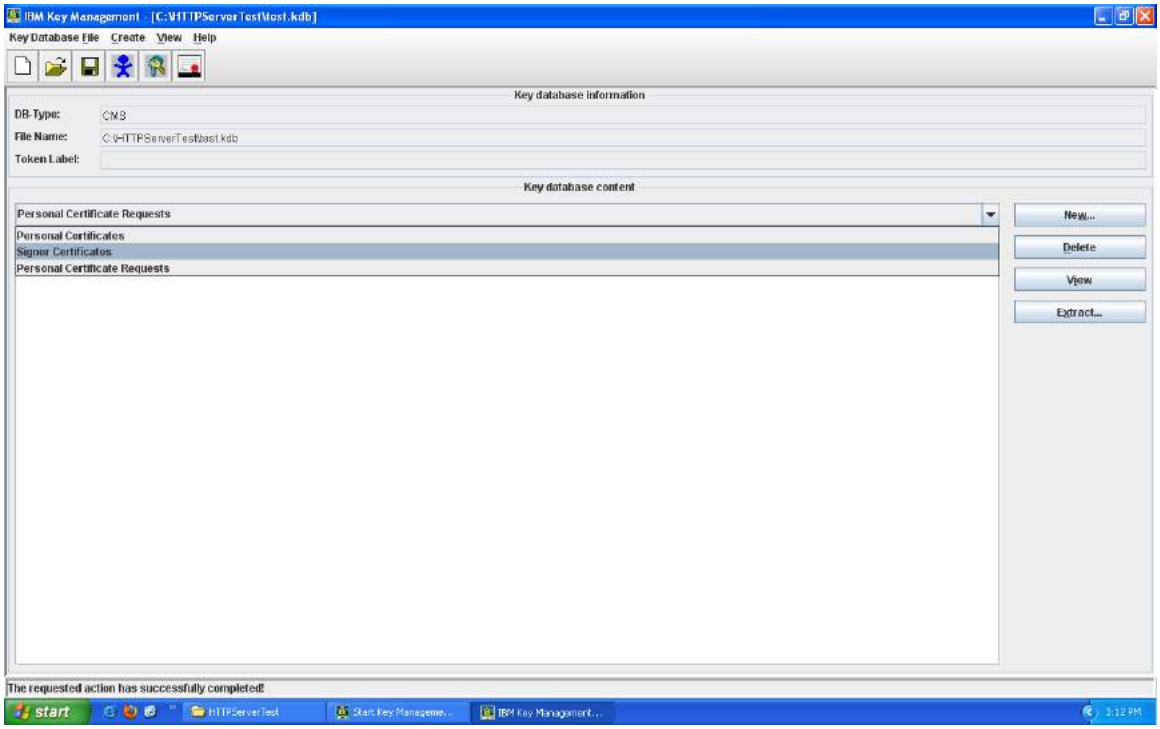
2. 打开生成 CSR 的密钥数据库文件。



3. 输入密码后点击 OK。

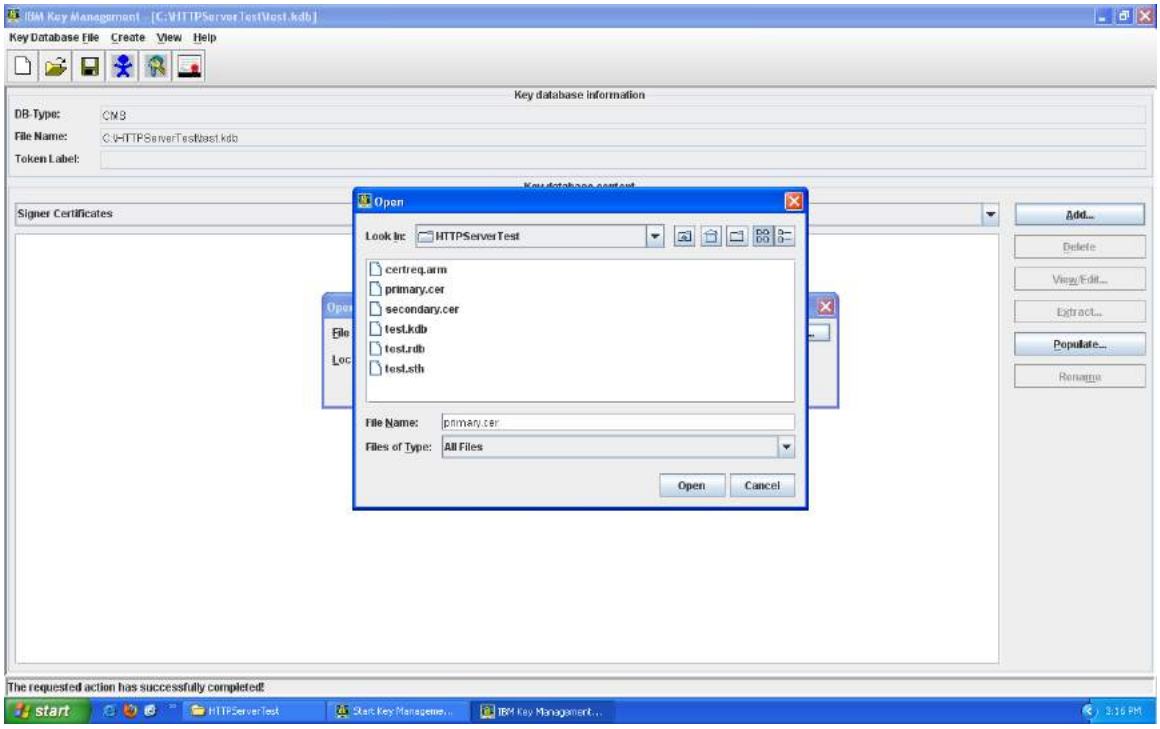


4. 选择 Signer Certificate，点击**添加**。



5. 点击 Files of Type 然后选择 **All Files**。

6. 输入 **Intermediate.cer** 证书的路径。



7. 点击 OK。

8. 输入证书的标签，如：Intermediate CA

步骤 3：获取 SSL 证书

4. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。

5. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

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

   [加密数据]

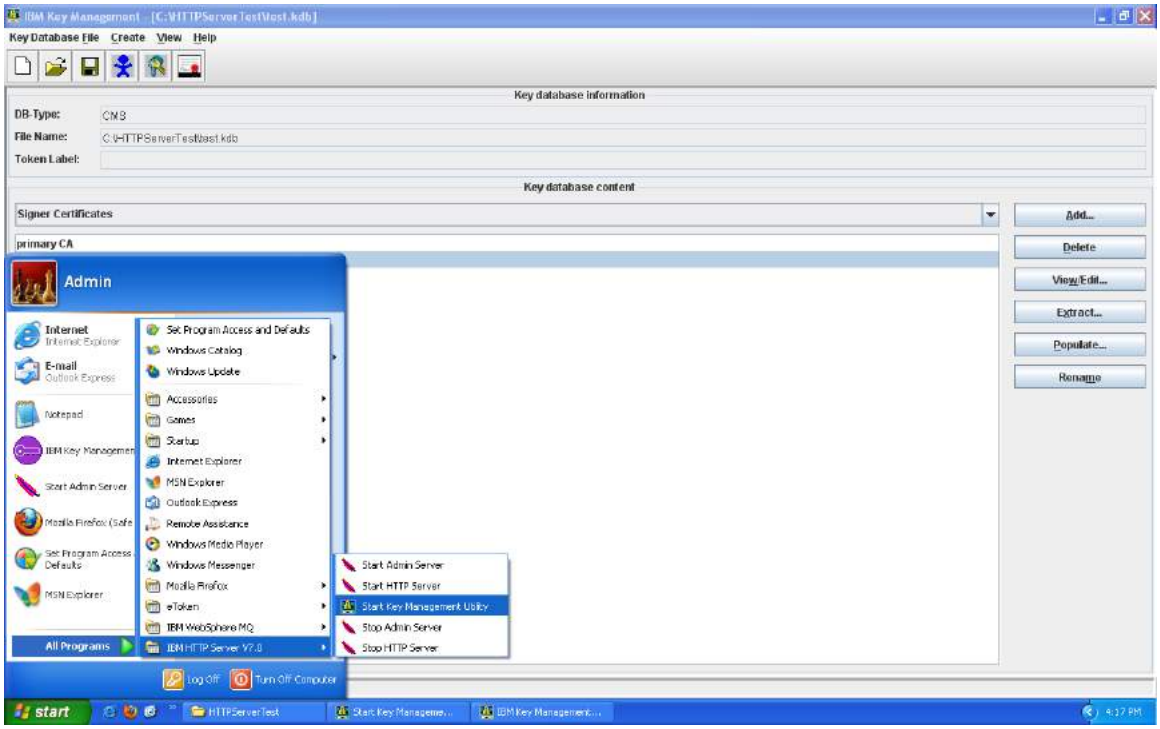
   -----END CERTIFICATE-----

6. 把证书存档为 filename.cer 文档。

步骤 4：安装 SSL 证书

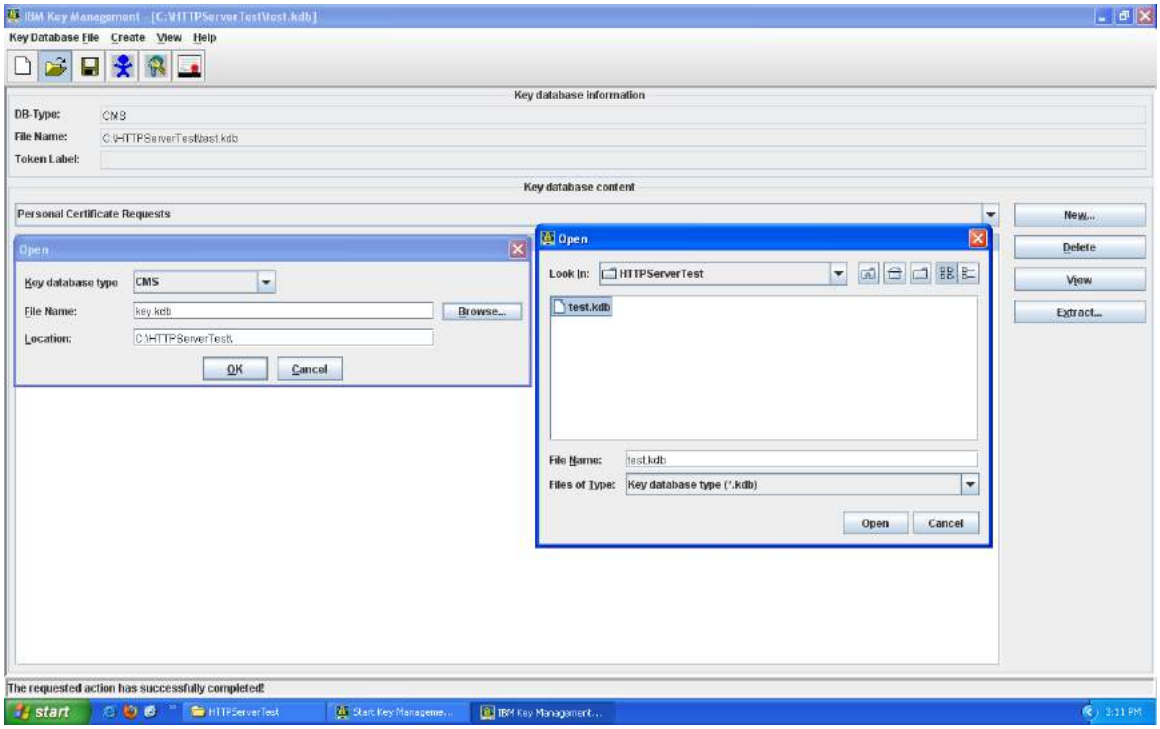
1. 开启 Key Management Utility (iKeyman)：

Windows 界面：在开始界面，点击 Start Key Management Utility



AIX, Linux 或 Solaris: 在命令行里输入 ikeyman

2. 在 Key Database File 目录里点击 Open。点击 Key database type，然后选择 CMS。

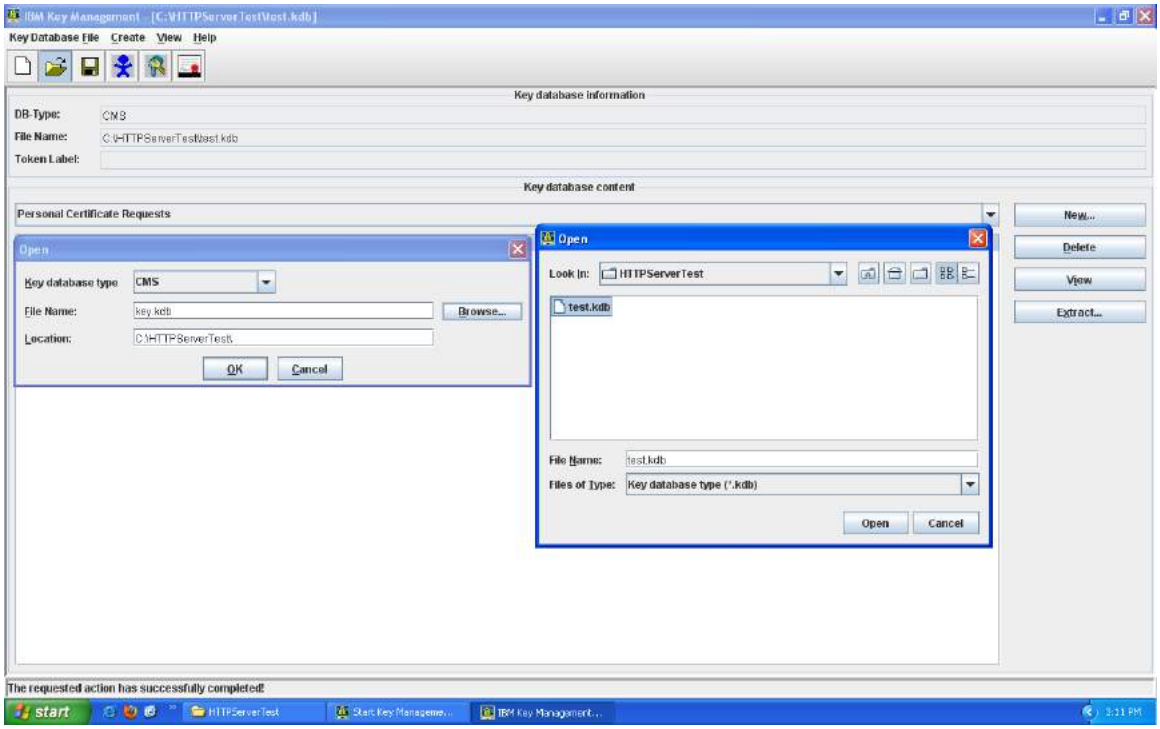


3. 点击 Browse，浏览至储存 Key Database 文件的目录。

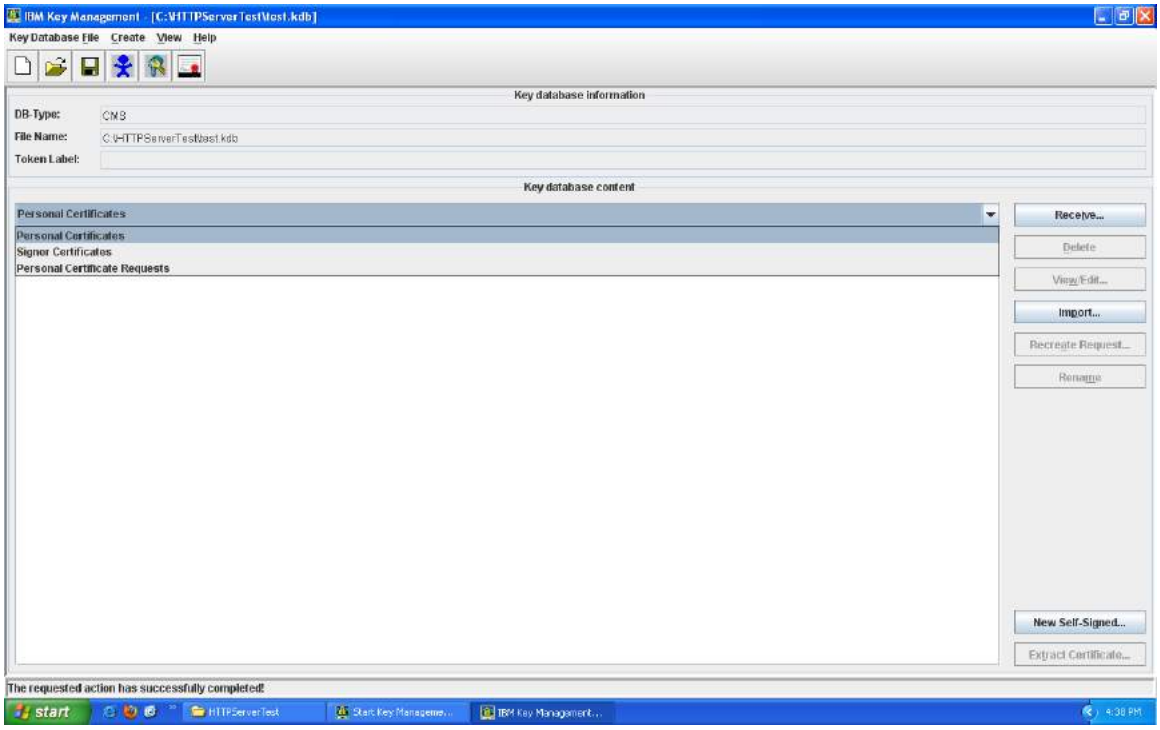
4. 选择你要添加至证书的密钥数据库文件，例：key.kdb。

5. 点击开启。

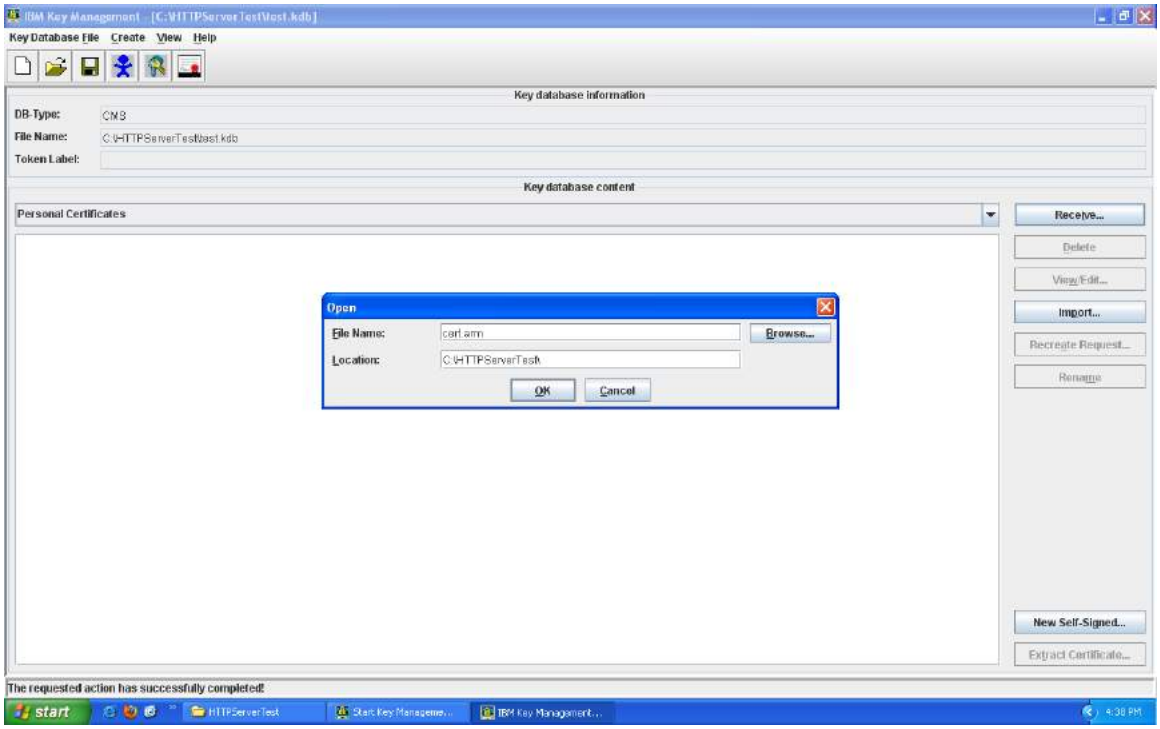
6. 在密码提示窗口，输入你在创建密钥数据库时所使用的密码，然后点击 OK。



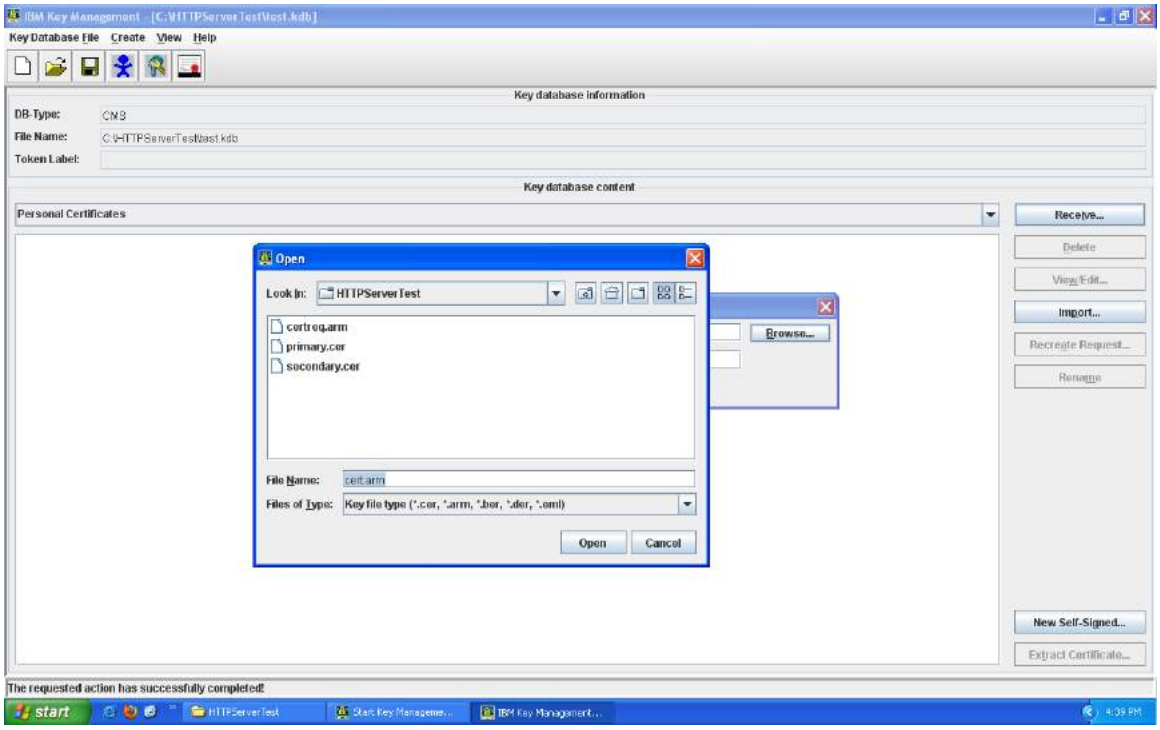
7. 选择 Personal Certificates view。



8. 点击 Receive。



9. 点击 Browse 选择证书的名称和路径。



10. 点击 OK。

11. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。

使用命令行界面安装 IBM WebSphere SSL 证书

步骤 1：下载中级 CA 证书

3. 通过此链接下载中级 CA 证书。

   选择和你的 SSL 证书适合的中级 CA 证书。

4. 复制中级 CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为

   intermediate.cer.

步骤 2：安装中级 CA 证书

1. 运行以下命令把 intermediate.cer 加入到密钥数据库：

   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 密钥数据库的全文件名，例：dbkey.kdb
- -pw password 是.cms 扩展的 CMS 密钥数据库的密码
- -label 是附加到证书的密钥标签，例：”ibmwebspheremqqmname”

- -file filename 是中级 CA 证书的全文件名，例：intermediate.cer
- -format ascii 代表证书的格式。可把数值更换为 Base64-encoded ASCII。默认是 ascii。

步骤 3：获取 SSL 证书

7. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
8. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

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

   [加密数据]

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

9. 把证书存档为 filename.cer 文档。

步骤 4：安装 SSL 证书

1. 使用以下命令行把证书安装至 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 密钥数据库的全文件名，例：dbkey.kdb
- -pw password 是.cms 扩展的 CMS 密钥数据库的密码
- -label 是附加到证书的密钥标签，例：”ibmwebspheremqqmname”
- -file filename 是中级 CA 证书的全文件名，例：intermediate.cer
- -format ascii 代表证书的格式。可把数值更换为 Base64-encoded ASCII。默认是 ascii。

步骤 5：提取 SSL 证书

1. 运行以下命令行提取 iKeyman 里的证书。

   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 密钥数据库的全文件名，例：dbkey.kdb
   - -pw password 是.cms 扩展的 CMS 密钥数据库的密码
   - -label 是证书的标签
   - -target filename 是目标文件的名称
   - -format ascii 代表证书的格式。可把数值更换为 Base64-encoded ASCII。默认是 ascii。

2. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。