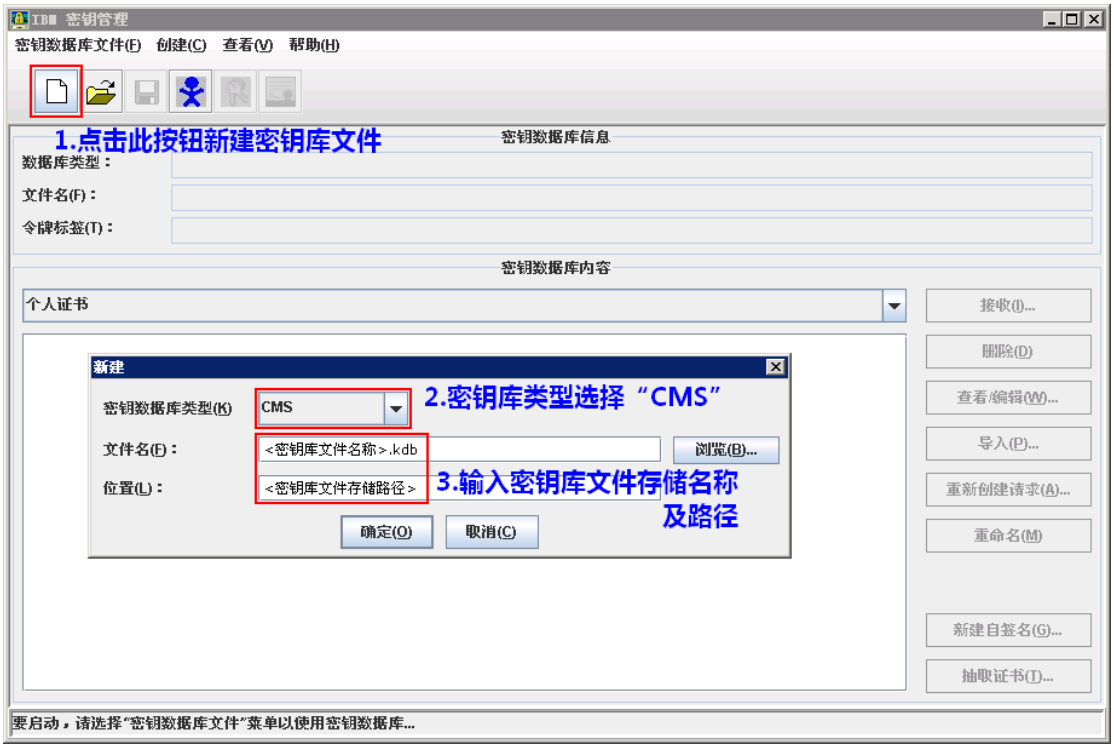
目录

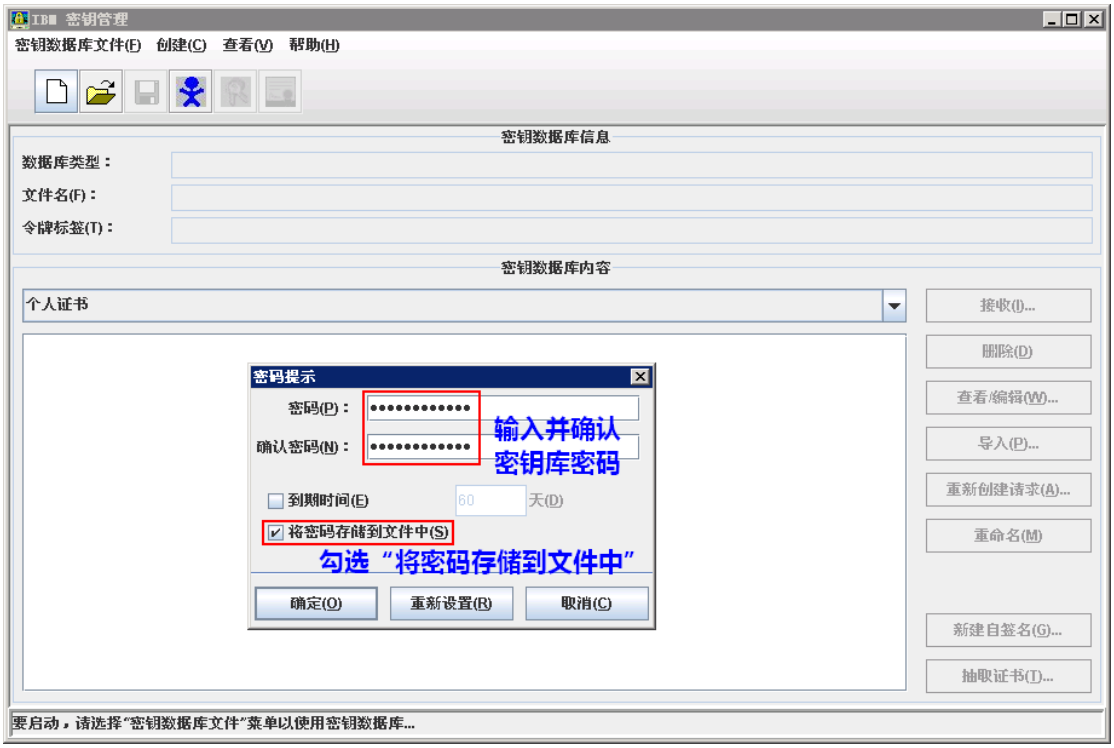
一、 生成证书请求

1. 打开 IBM Key Management Utility 证书工具(iKeyman)

进入 iKeyman 界面，新建密钥库文件，如下图：



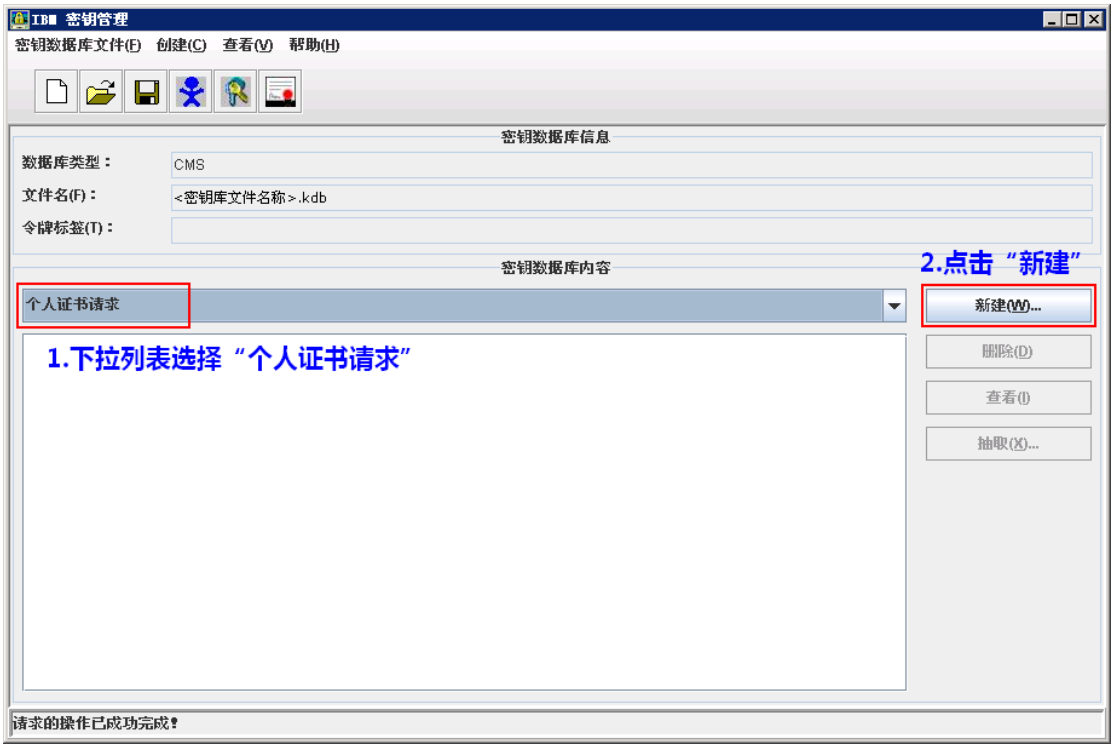
图表一



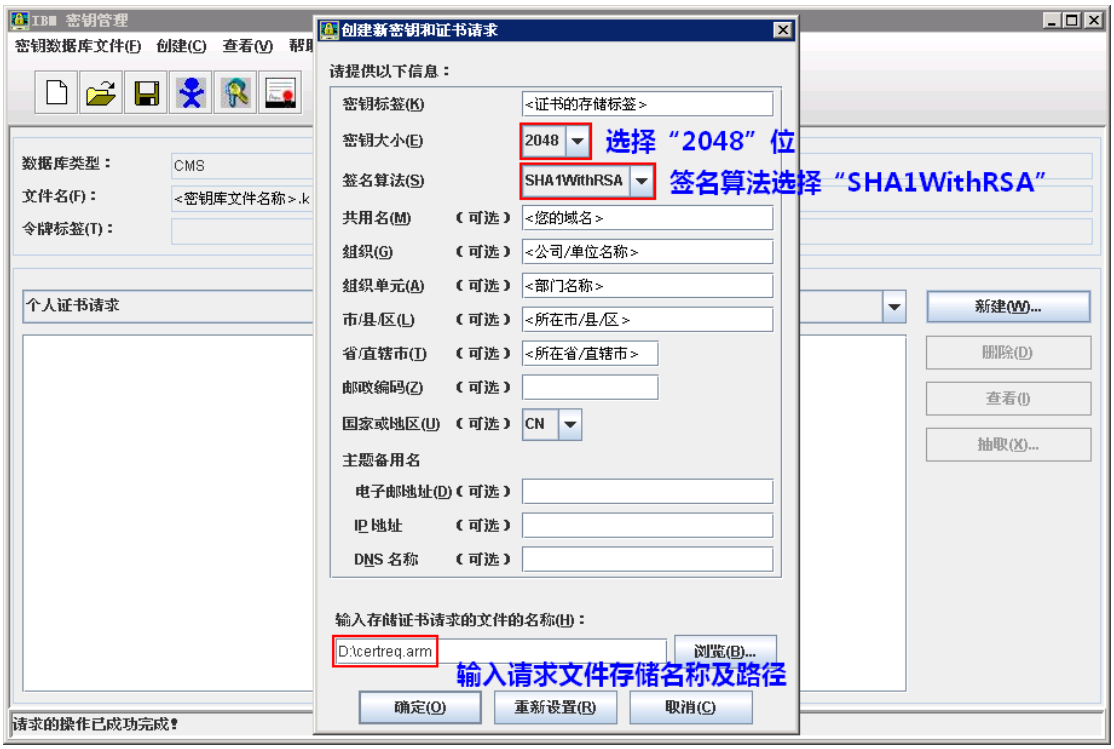
图表二

2. 创建证书申请

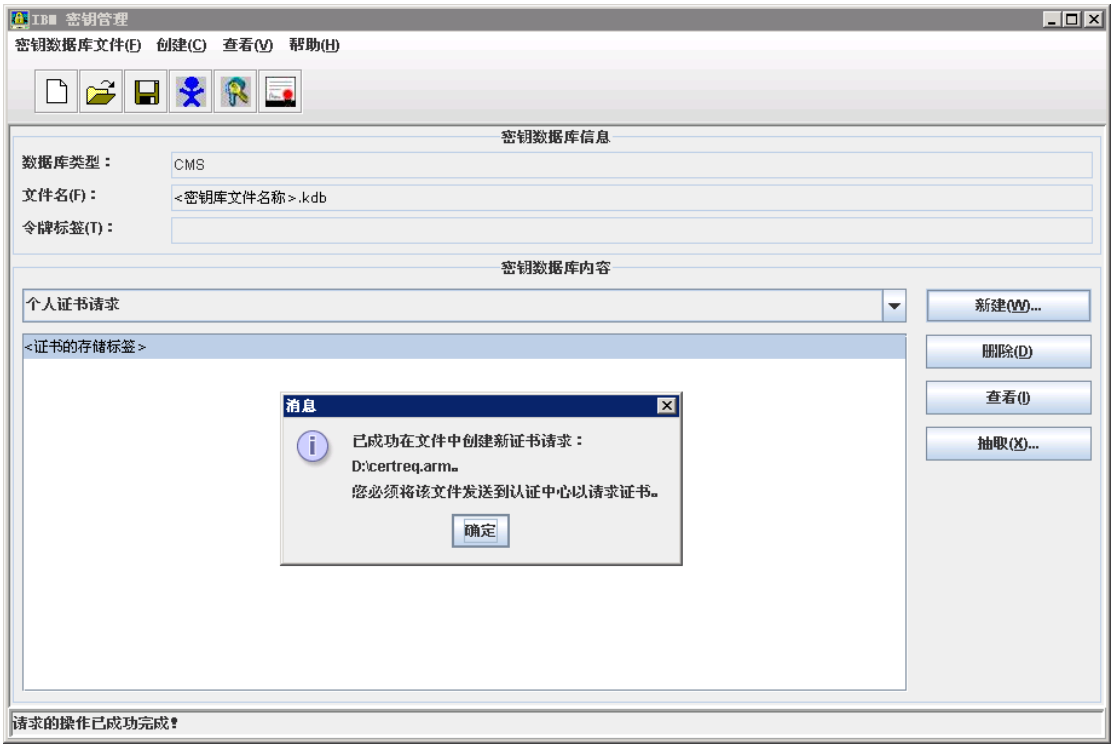
选择“个人证书请求”栏目，并点击“新建”按钮，如下图步骤进行操作：


IBM 密钥管理
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)
密钥数据库信息
数据库类型：
CMS
文件名(F)：
<密钥库文件名称>.kdb
令牌标签(T)：
密钥数据库内容
个人证书请求
新建(W)...
删除(D)
查看(I)
抽取(X)...
2.点击“新建”
1.下拉列表选择“个人证书请求”
请求的操作已成功完成。

图表三


创建新密钥和证书请求
请提供以下信息：
密钥标签(K)
<证书的存储标签>
密钥大小(E)
2048
选择“2048”位
签名算法(S)
SHA1WithRSA
签名算法选择“SHA1WithRSA”
共用名(M) (可选) <您的域名>
组织(G) (可选) <公司/单位名称>
组织单元(A) (可选) <部门名称>
市/县/区(L) (可选) <所在市/县/区>
省/直辖市(T) (可选) <所在省/直辖市>
邮政编码(Z) (可选)
国家或地区(U) (可选) CN
主题备用名
电子邮件地址(D) (可选)
IP 地址 (可选)
DNS 名称 (可选)
输入存储证书请求的文件的名称(H)：
D:\certreq.arm
浏览(B)...
输入请求文件存储名称及路径
确定(O)
重新设置(R)
取消(C)

图表四

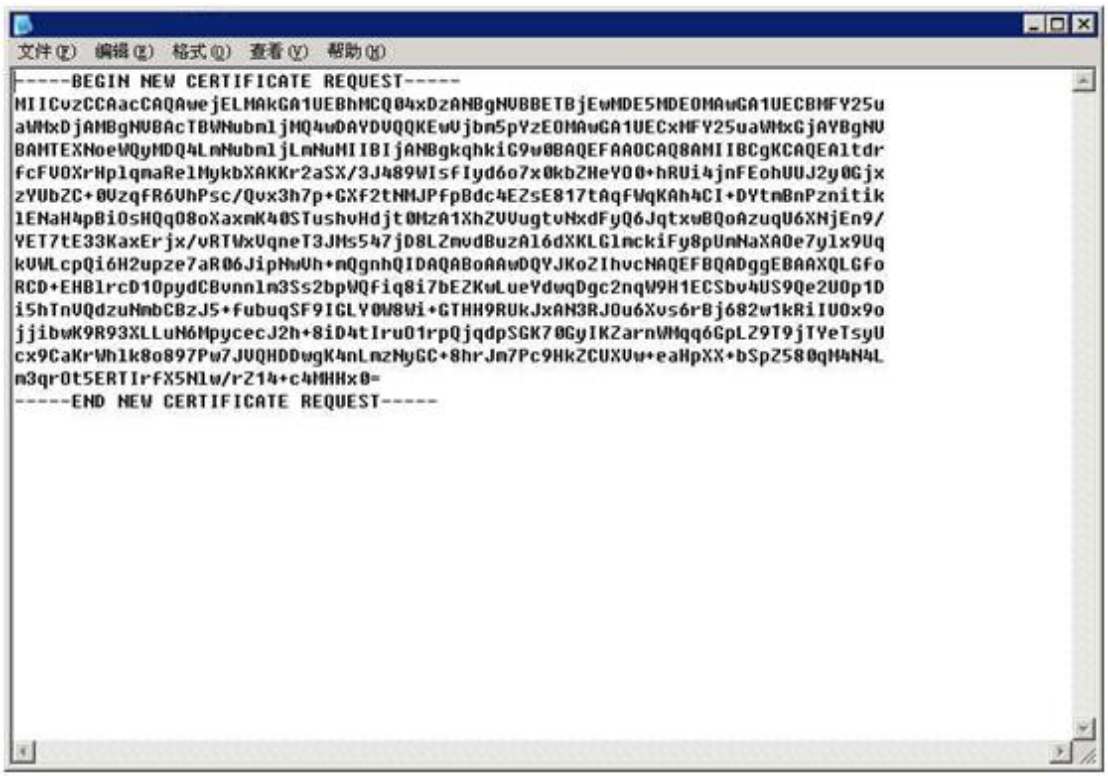


图表五

3. 查看证书请求文件

生成的证书请求文件应如下图所示：

该文件可使用记事本工具打开，所显示内容如下图所示：


文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvzCCAacCAQAwejELMAkGA1UEBhMCQ04xDzANBgNVBBETBjEwMDE5MDEOMAwGA1UECBMFY25u
aWMxDjAMBgNVBAcTBWNubmljMQ4wDAYDVQQKEwVjbm5pYzEOMAwGA1UECxMFY25uaWMxGjAYBgNV
BAMTEXNoeWQyMDQ4LmNubmljLmNuMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1tdr
fcFVOXrHplqmaRelMykbXAKKr2aSX/3J489WIsfIyd6o7x0kbZHeYO0+hRUi4jnFEohUUJ2y0Gjx
zYUbZC+0VzqFR6VhPsc/Qvx3h7p+GXf2tNMJPfpBdc4EZsE817tAqfWqKAh4CI+DYtmBnPznitik
1ENaH4pBiOsHQqO8oXaxmK40STushvHdjt0MzA1XhZVVugtvNxdFyQ6JqtxwBQoAzuqU6XNjEn9/
YET7tE33KaxErjx/vRTWxVqneT3JMs547jD8LZmvdBuzAl6dXKLGlmckiFy8pUmNaXAOe7ylx9Uq
kVWLcpQi6H2upze7aR06JipNwVh+mQgnhQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAAXQLGfo
RCD+EHBlrcD1OpydCBvnnlm3Ss2bpWQfiq8i7bEZKwLueYdvqDgc2nqW9H1ECSbv4US9Qe2UOp1D
i5hTnVQdzuNmbCBzJ5+fubuqSF9IGLY0W8Wi+GTHH9RUkJxAN3RJOu6Xvs6rBj682w1kRiIUOx9o
jjibwK9R93XLLuN6MpycecJ2h+8iD4tIruO1rpQjqdpSGK70GyIKZarnWMqq6GpLZ9T9jTYeTsyU
cx9CaKrWh1k8o897Pw7JVQHDDvgK4nLmzNyGC+8hrJm7Pc9HkZCUXVw+eaHpXX+bSpZ580qM4N4L
m3qr0t5ERTIrfX5N1w/rZ14+c4MHHx0=
-----END NEW CERTIFICATE REQUEST-----

图表六

二、 下载服务器证书

1. 准备下载证书所需信息

参考号与授权码：参考号与授权码是下载证书的密码凭证。当申请的证书通过审核时，用户将接收到由 CNNIC 发送的通过审批的电子邮件通知，该邮件中含有 16 位的参考号与授权码信息,其中参考号与授权码的前 13 位为明文显示，后 3 位为密文显示。审核员会以邮件通知的方式发送后三位的明文显示。

2. 下载证书

登录 CNNIC 官网，进入 CNNIC 服务器证书下载中心页面：

http://www.cnnic.net.cn/jczyfw/fwqzs/fwqzsxzzx/

点击相应的链接进入到证书下载页面，如下图所示：

图表七　可信服务器证书下载页面

根据网页上的提示输入“参考号”和“授权码”，将证书请求文件中除去头尾“-----BEGIN NEW CERTIFICATE REQUEST-----”和“-----END NEW CERTIFICATE REQUEST-----”的中间部分内容复制到 CSR 文本框中。结果如下所示：

图表八　填入收到的参考号和授权码以及生成的 CSR

点击“下载”，如果参考号、授权码和证书请求文件均无问题，则显示页面如下所示。

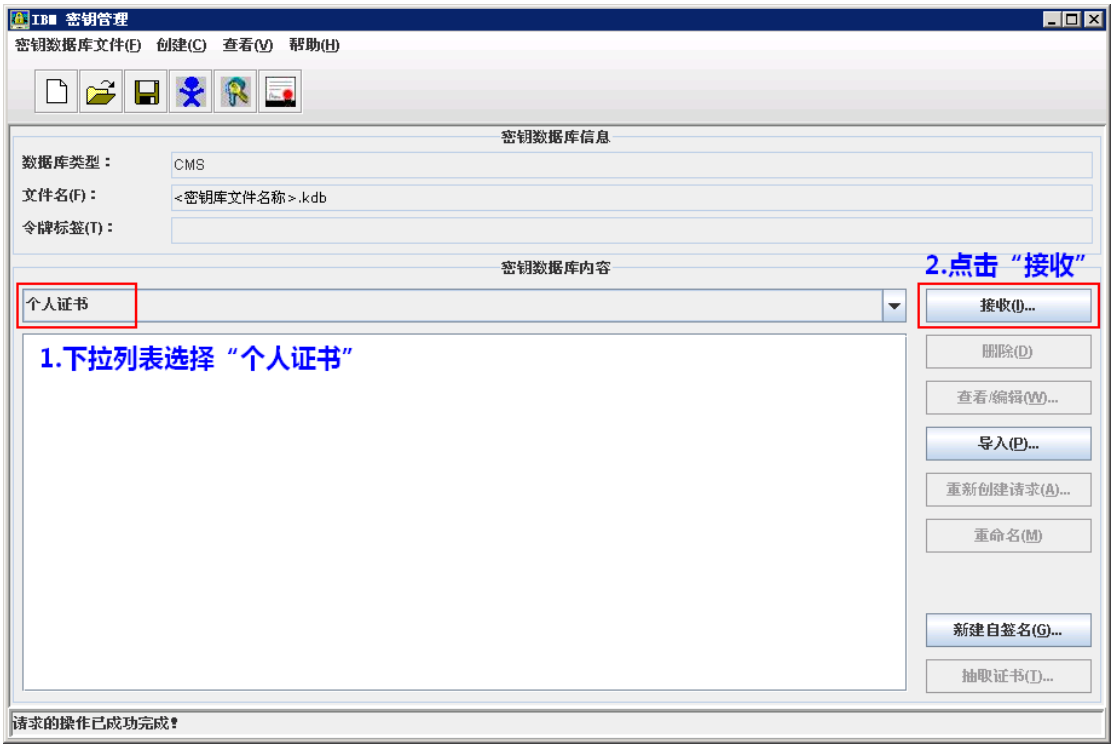
图表九　生成证书

请按页面提示将文本框中的内容拷贝下来，粘贴到一个文本文档中保存，为文件起一个方便记忆的名字，以.cer 为后缀。您也可以直接点击保存，自动下载一个名为 WebCert.cer 的文件，该文件即为申请的证书。请妥善保存该文件，如果该证书丢失，就必须进行证书补发操作，此操作可能会有相应费用产生。

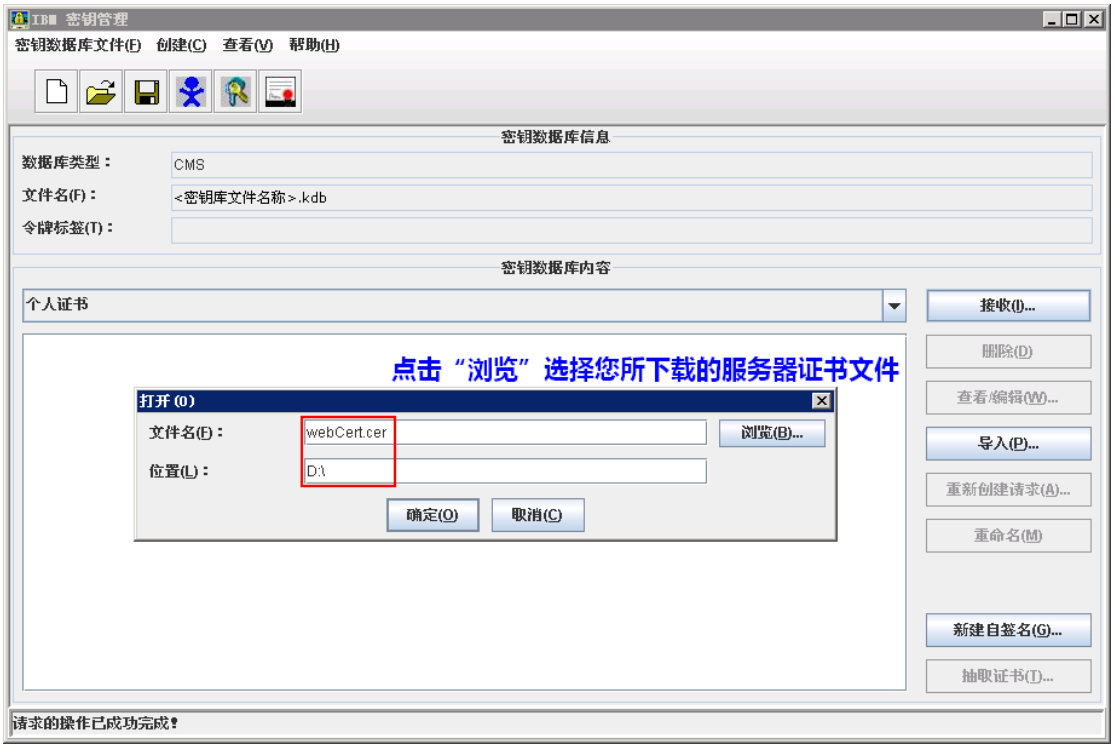
三、 安装服务器证书

1. 完成证书申请

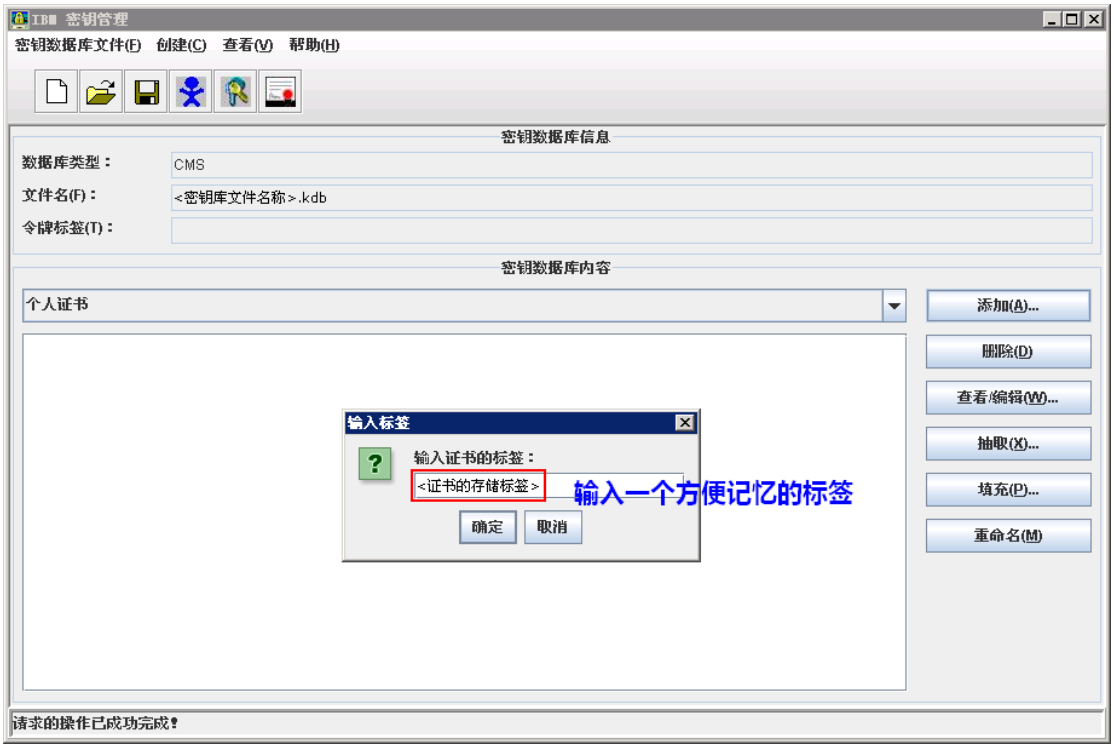
进入 iKeyman 界面，选择“个人证书”栏目，如下图步骤完成证书申请。



图表十


密钥管理
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)
密钥数据库信息
数据库类型：
CMS
文件名(F)：
<密钥库文件名称>.kdb
令牌标签(T)：
密钥数据库内容
个人证书
接收(I)...
删除(D)
查看/编辑(W)...
导入(P)...
重新创建请求(A)...
重命名(M)
新建自签名(G)...
抽取证书(T)...
点击“浏览”选择您所下载的服务器证书文件
打开 (0)
文件名(F)：
webCert.cer
浏览(B)...
位置(L)：
D:\
确定(O)
取消(C)
请求的操作已成功完成。

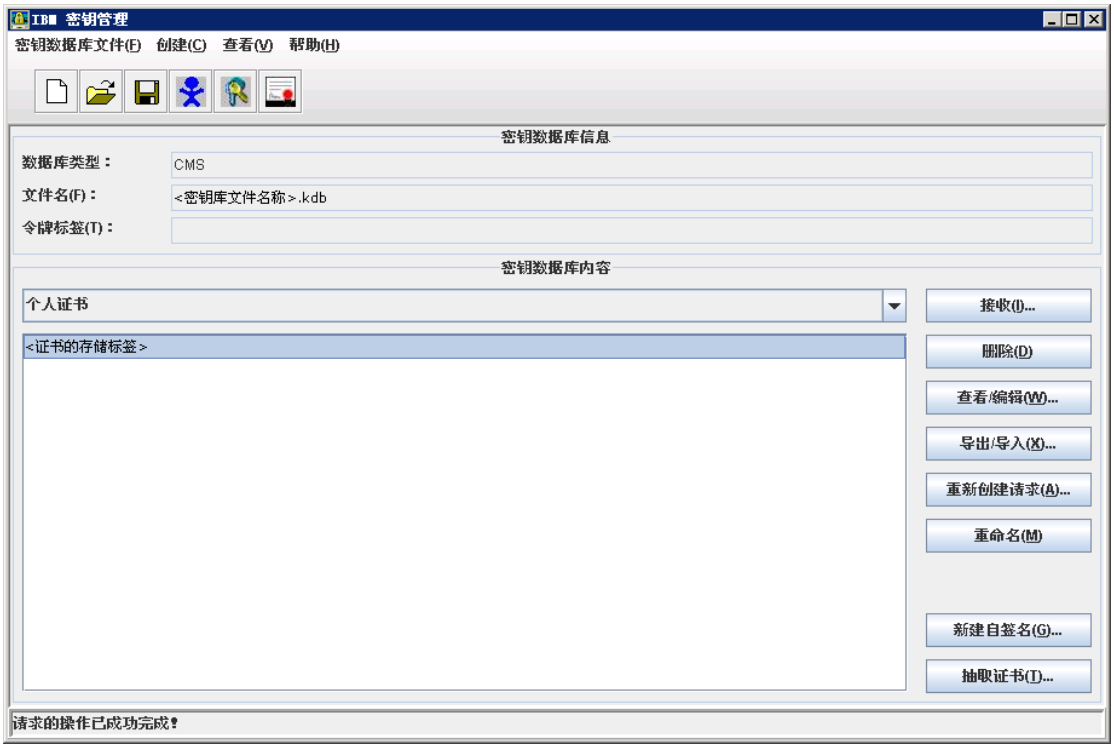
图表十一


密钥管理
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)
密钥数据库信息
数据库类型：
CMS
文件名(F)：
<密钥库文件名称>.kdb
令牌标签(T)：
密钥数据库内容
个人证书
添加(A)...
删除(D)
查看/编辑(W)...
抽取(X)...
填充(P)...
重命名(M)
输入标签
输入证书的标签：
<证书的存储标签>
输入一个方便记忆的标签
确定
取消
请求的操作已成功完成。

图表十二

2. 查看证书列表

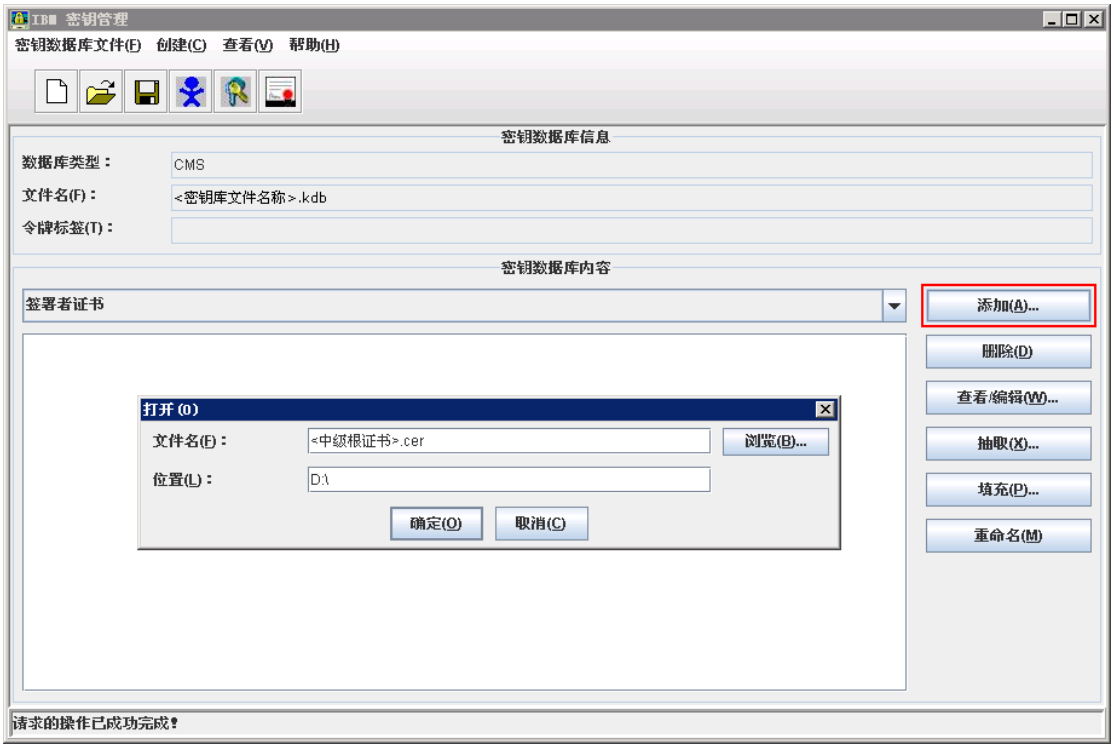
完成证书申请后，该证书会在个人证书列表中出现，以<证书的存储标签>标识，如下图所示：



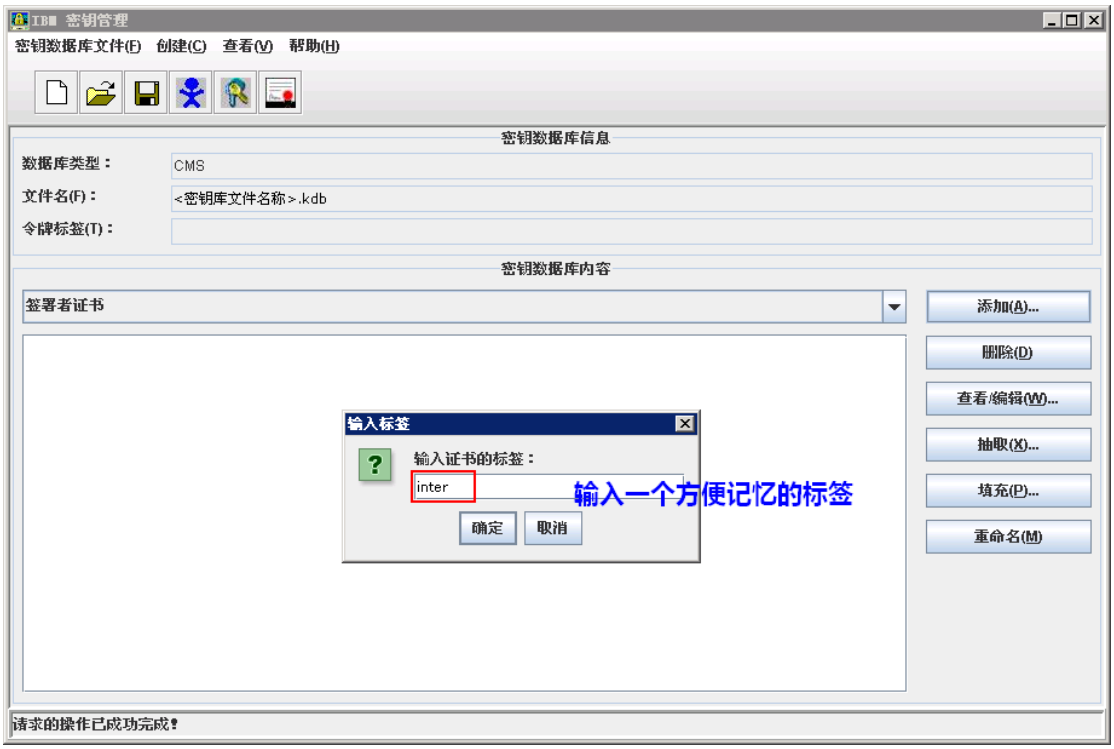
图表十三

3. 导入中级根证书

选择“签署者证书”栏目，并点击“添加”，如下图所示：


IBM 密钥管理
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)
密钥数据库信息
数据库类型：
CMS
文件名(F)：
<密钥库文件名称>.kdb
令牌标签(T)：
密钥数据库内容
签署者证书
添加(A)...
删除(D)
查看/编辑(W)...
抽取(X)...
填充(P)...
重命名(M)
打开 (0)
文件名(F)：
<中级根证书>.cer
浏览(B)...
位置(L)：
D:\
确定(O)
取消(C)
请求的操作已成功完成。

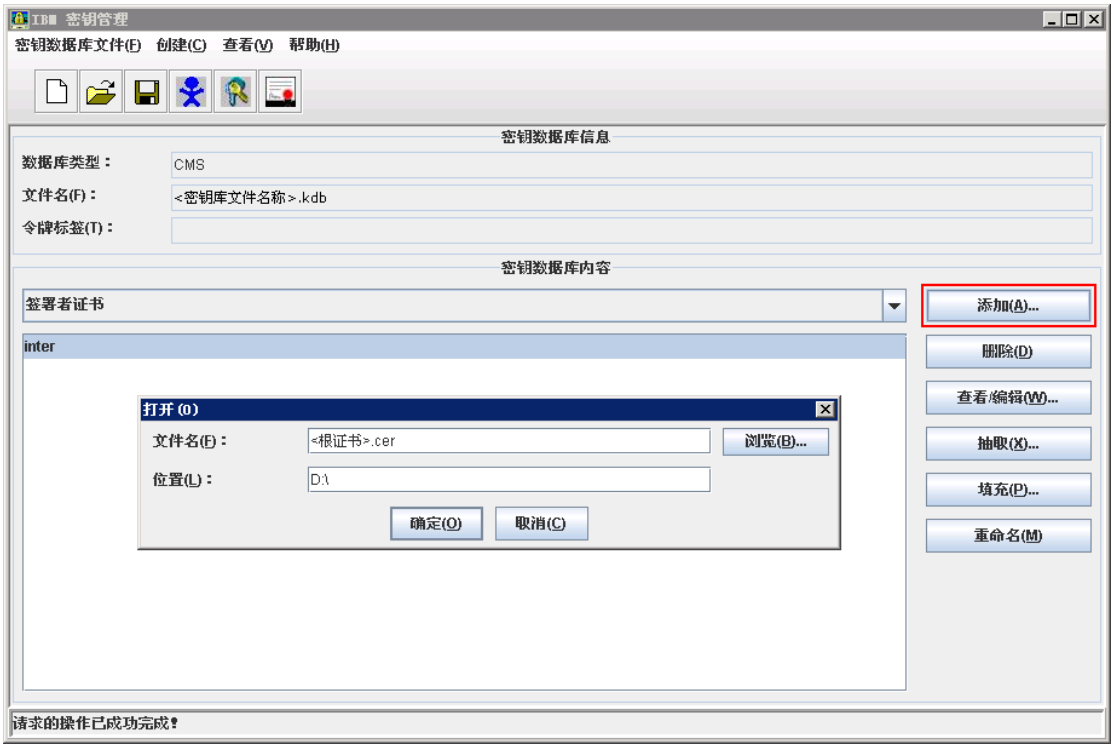
图表十四


IBM 密钥管理
密钥数据库文件(F) 创建(C) 查看(V) 帮助(H)
密钥数据库信息
数据库类型：
CMS
文件名(F)：
<密钥库文件名称>.kdb
令牌标签(T)：
密钥数据库内容
签署者证书
添加(A)...
删除(D)
查看/编辑(W)...
抽取(X)...
填充(P)...
重命名(M)
输入标签
输入证书的标签：
inter
输入一个方便记忆的标签
确定
取消
请求的操作已成功完成。

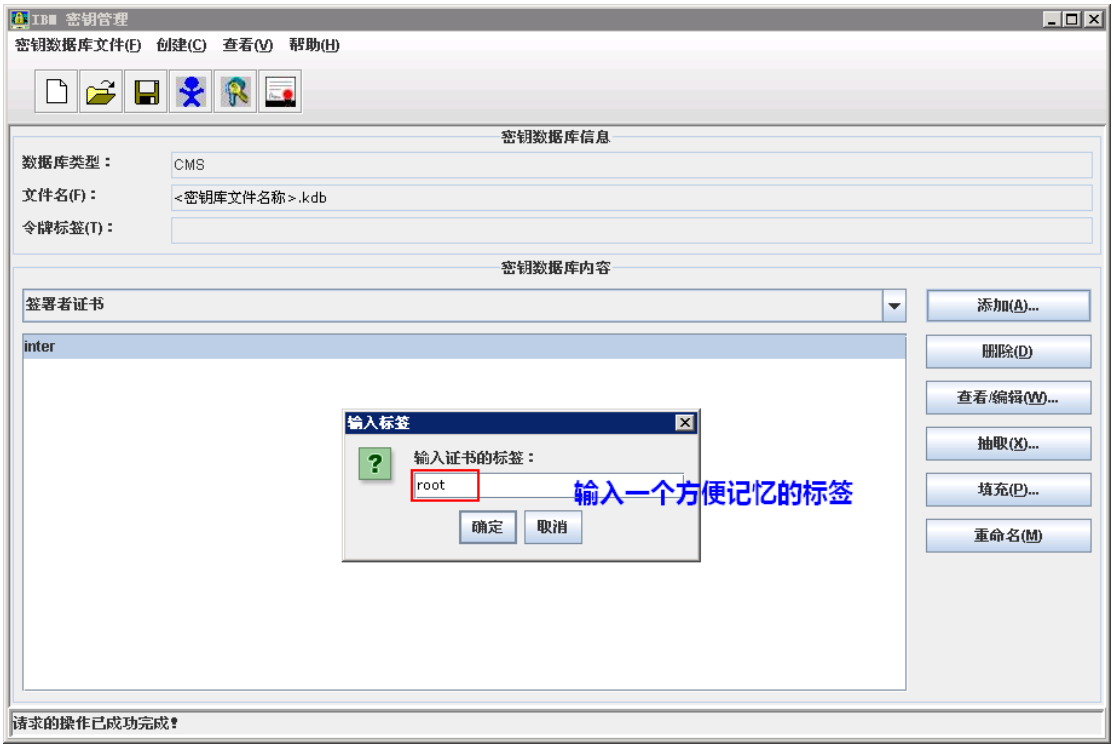
图表十五

4. 导入根证书

选择“签署者证书”栏目，并点击“添加”，如下图所示：

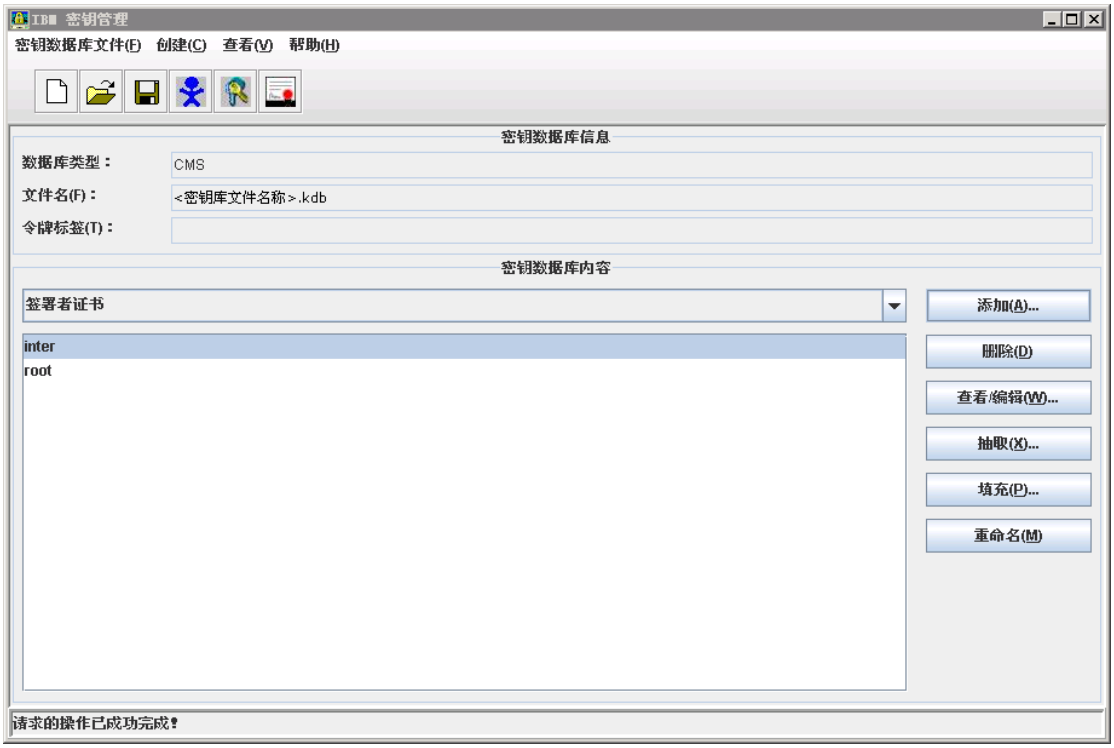


图表十六



图表十七

完成后，“签署者证书”列表应如下图所示：



图表十八

5. 修改 HTTP Server 配置文件

首先确认您的 HTTP Server 安装目录所在位置，打开该安装目录下的 conf 目录，并在 conf 目录下找到 httpd.conf 文件，这个文件就是 HTTP Server 的配置文件，您可以文本方式打开该文件并进行编辑。

打开 httpd.conf 文件找到如下段落即为配置您的服务器证书所相关的配置。

```
#LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
#Listen 0.0.0.0:443
## IPv6 support:
#Listen [::]:443
#<VirtualHost *:443>
```

```
#SSLEnable
#SSLProtocolDisable SSLv2
#</VirtualHost>
#KeyFile C:/Program Files/IBM/HTTPServer/ihsserverkey.kdb
#SSLDisable
```

找到该段落后，请参考如下所示内容修改这段配置文件。

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
#Listen [::]:443
<VirtualHost *:443>
SSLEnable
SSLProtocolDisable SSLv2
</VirtualHost>
KeyFile "<密钥库文件绝对存储路径及名称>"
SSLDisable
```

需要注意的是，记得将句首“#”号删除，否则该配置语句将被屏蔽。

6. 测试是否安装成功

重新启动您的 HTTP Server 后，在浏览器地址栏输入：https://<申请证书的域名>测试您的 SSL 证书是否安装成功，如果成功，则浏览器地址栏会显示一个安全锁标志。点击安全锁标志，可查看网站的域名证书。

四、 备份服务器证书

测试成功后请务必妥善备份您的密钥库（kdb）文件。

PS：所需备份的密钥库文件应如下图所示，后缀为 kdb：