IBM HTTP Server SSL 证书部署指南

沃通电子认证服务有限公司

WoTrus CA Limited

目　　录

一、　安装 SSL 证书的环境.....3
1.1 SSL 证书安装环境简介.....3
1.2 网络环境要求.....3
二、　SSL 证书的安装.....3
2.1 获取 SSL 证书.....3
2.2 转换证书格式.....4
2.3 安装证书.....8
三、　SSL 证书的备份.....8
四、　SSL 证书的恢复.....9

技术支持联系方式

技术支持邮箱：supp3@wotrus.com

技术支持热线电话：18822828659 / 0755-26027827

技术支持网页：https://bbs.wosign.com

公司官网地址：https://www.wosign.com

一、 安装 SSL 证书的环境

1.1 SSL 证书安装环境简介

IBM HTTP Server 系统一套

SSL 证书一张（备注：本指南使用 test.wosign.com 域名 SSL 证书进行操作,通用其它版本证书）

1.2 网络环境要求

请确保站点是一个合法可访问的域名地址，可以正常通过 http://XXX 进行正常访问。

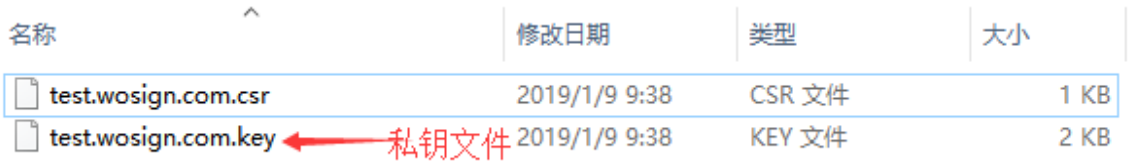
二、 SSL 证书的安装

2.1 获取 SSL 证书

成功在沃通申请证书后，会得到一个.zip 压缩包文件，解压后得到四个文件夹(见图 1)，不同服务器或设备要求不同的格式，IBM HTTP Server 需要用到 OtherServer 里面的证书文件，如图 1：

图 1

私钥 key 文件，需要找到生成 CSR 时保存的两个文件，如下图(若创建 CSR 时选择一键生成 CSR，私钥文件为当时浏览器自动下载的.key 文件)



2.2 转换证书格式

IHS 服务器要求的证书格式类型为 KDB，需要通过 IBM IKeyMan 工具转换,证书的格式转换分为以下两步：

1、 将 crt+key 文件转换为 JKS

转换工具下载：https://download.wotrus.com/wotrus/wosigncode.exe

转换步骤：运行下载的证书转换工具，选择“证书”-“转换证书格式”，证书源格式选择“PEM”，目标格式选择“JKS”，证书文件选择 OtherServer 中的 domain.com.crt 文件，私钥文件选择创建 CSR 时保存的.key 文件，私钥密码默认留空，JKS 密码自行设置，但注意保存该密码，后续过程需要用到，点击“转换”后，输入名称，选择路径，将 JKS 证书保存到指定位置，具体可参考下图：

2、 将 JKS 转换为 KDB

转换所需工具：IHS 自带的 IKeyMan 工具(版本要求 7.0 以上)

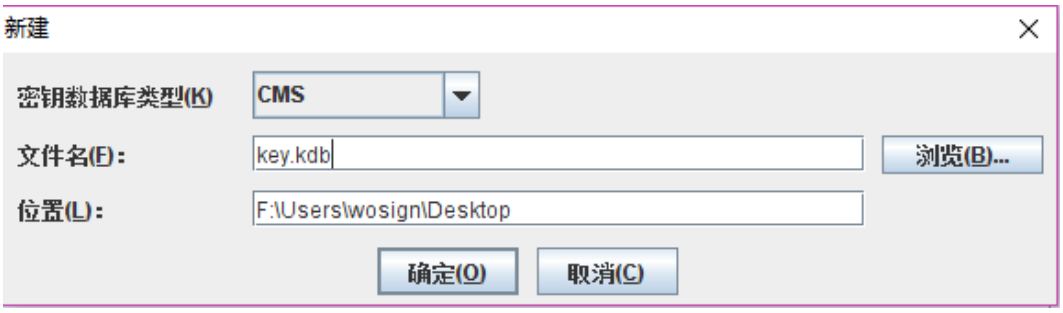
转换步骤：

1)、运行 IKeyMan(以 Windows 为例)

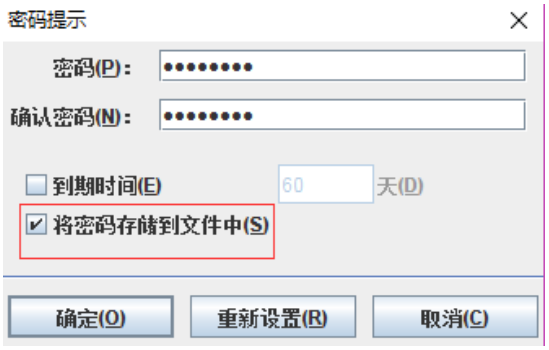
在开始菜单中，找到“IBM HTTP Server V7.0”-“Start Key Management Utility”，运行 IBM 密钥管理工具

2)、创建 KDB 文件

在打开的 IBM 密钥管理工具中，点击创建新密钥数据库文件，密钥数据库类型选择 CMS 并选择密钥保存路径。



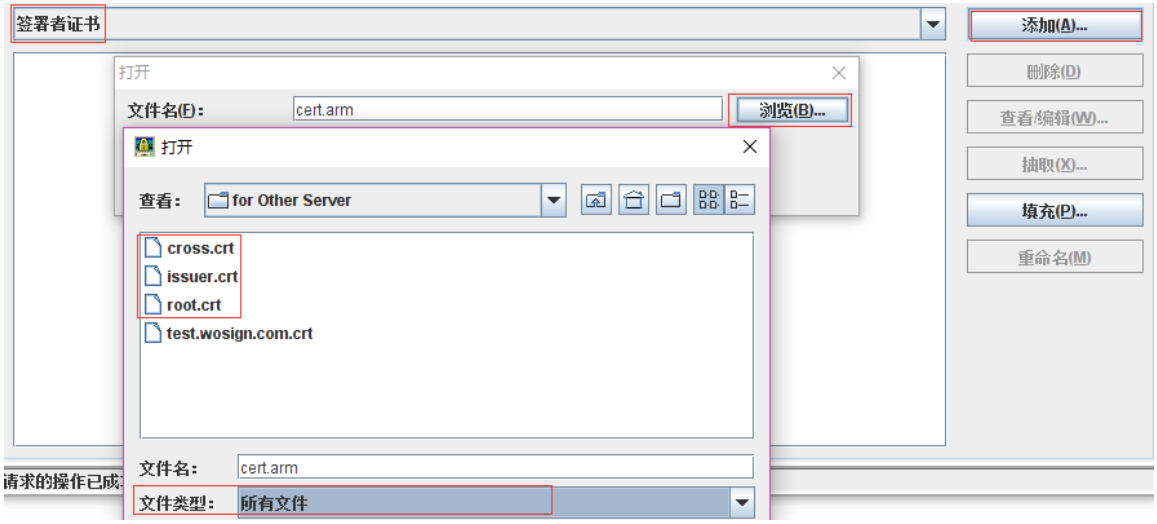
注意：请选中“将密码存储到文件”选项，此选项将把密码加密保存到扩展名为.sth 的文件中。IHS 启动时，会自动从该.sth 文件中读取密码，如果不选择此项启动 IHS 时会报错。

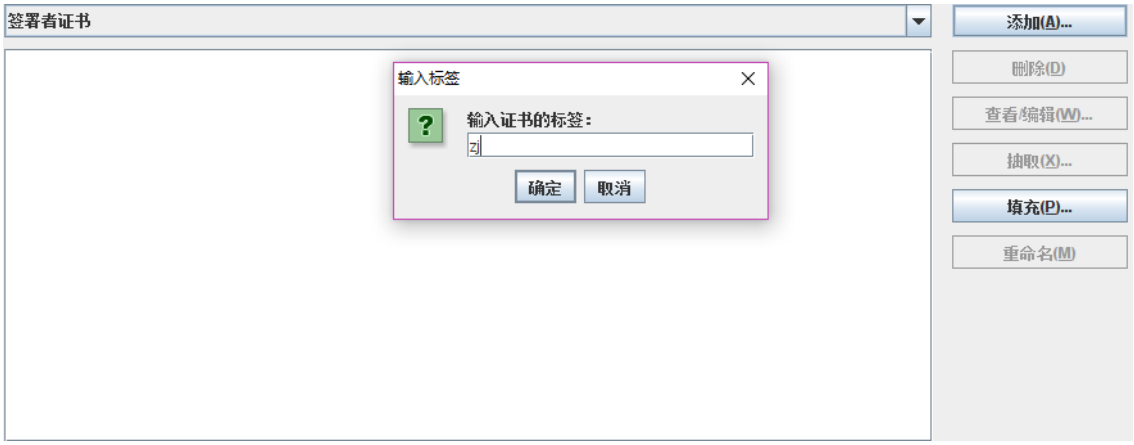


创建密钥库成功后，会在对应的目录下生成三个文件：

3)、导入签署者证书(证书链)

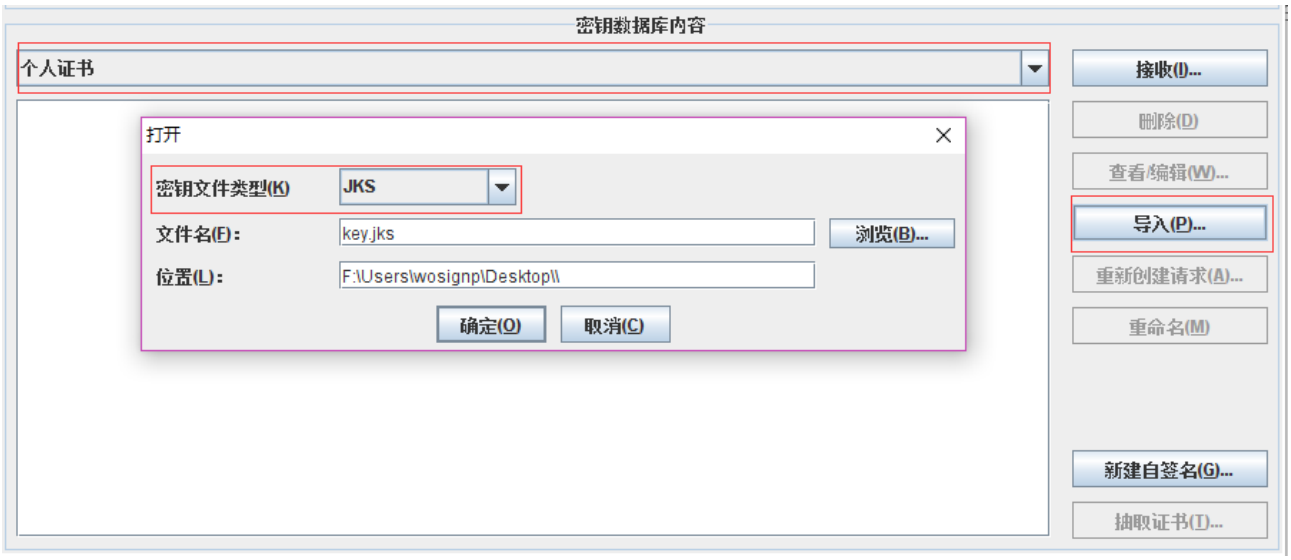
密钥数据库文件创建完成后，点击”签署者证书”-“添加”，依次将 OtherServe 中的 intermediate.crt、cross.crt、root.crt 文件导入签署者证书(标签可自定义，不重复即可)

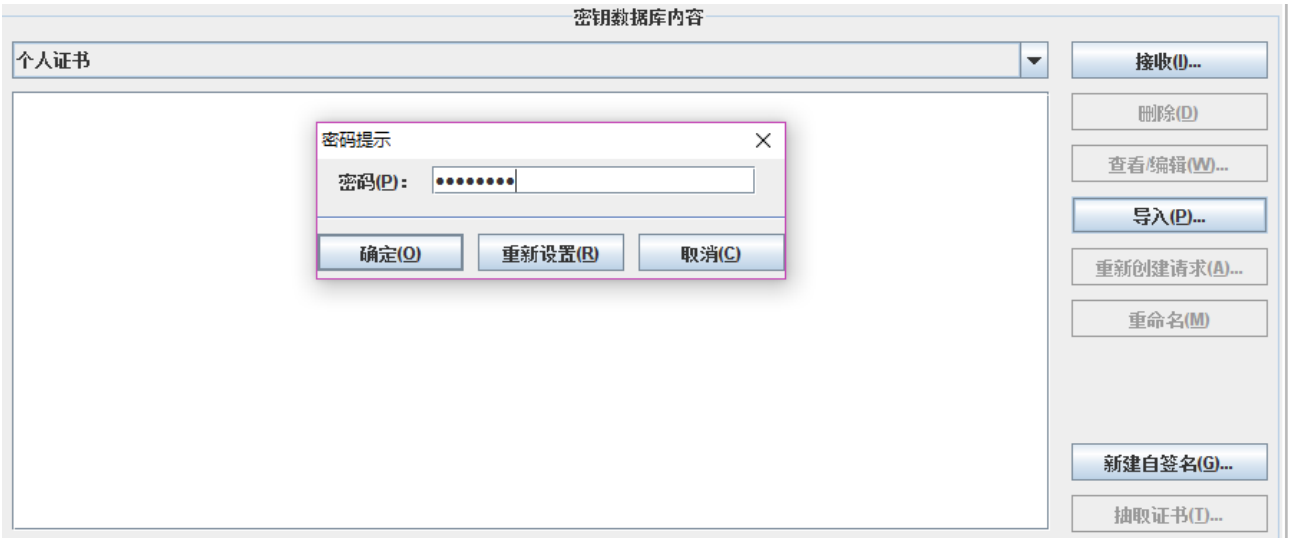




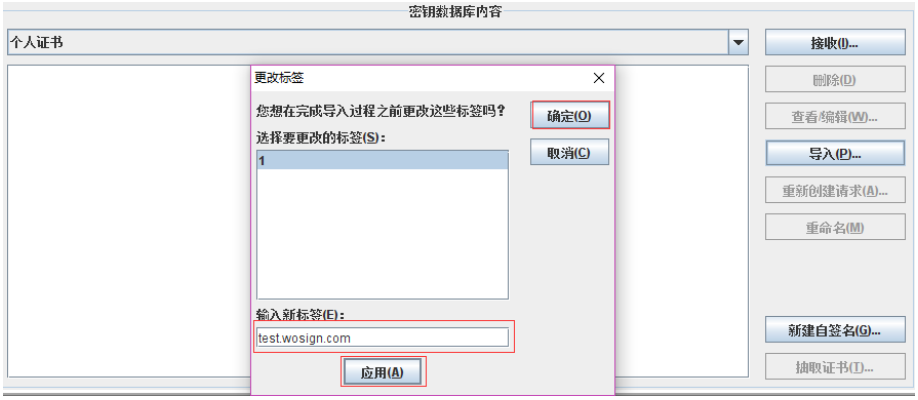
4)、导入 JKS 文件

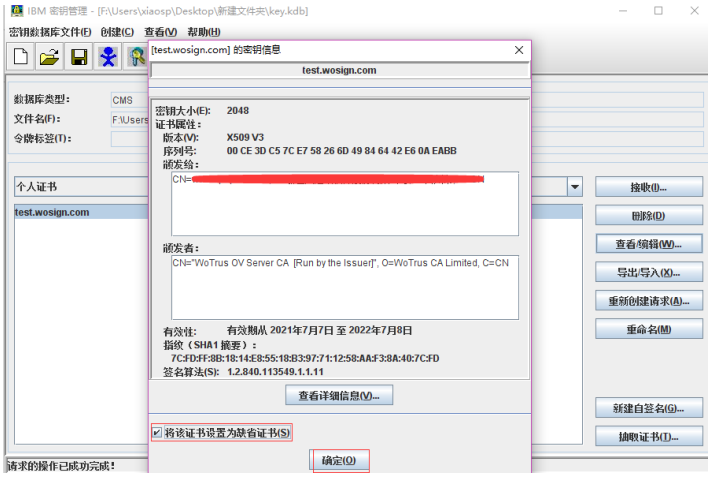
签署者证书导入完成后，回到“个人证书”，“导入”，选择之前步骤合成的 JKS 文件，输入设置的 JKS 密码。





输入 JKS 保护密码，点击确定，在新标签中输入证书域名或别名，点击“应用”、“确定”，在个人证书中将会看到对应的证书，点击”查看/编辑”，可将证书设置为缺省证书(默认证书)。





2.3 安装证书

在 IBM HTTP Server 下，找到 httpd.conf 文件，修改证书相关配置。

1)、启用 SSL 模块(去掉#注释)

LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

2)、添加 SSL 配置

Listen 443
<VirtualHost *:443>
ServerName www.domain.com
SSLEnable
SSLClientAuth None
<Directory “/opt/IBM/HttpServer/htdocs2">
Options Indexes
AllowOverride None
Require all granted
</Directory>
DocumentRoot “/opt/IBM/HttpServer/htdocs2"
DirectoryIndex index2.html
</VirtualHost>
SSLDisable KeyFile “/opt/IBM/HttpServer/conf/key.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000

三、 SSL 证书的备份

请保存好收到的证书压缩包文件及自己生成 csr 一起的.key 文件，以防丢失

四、 SSL 证书的恢复

重复 2.3 操作即可。