IBM HTTP Server (IHS 服务器)

SSL 证书安装文档

沃通电子认证服务有限公司

WoTrus CA Limited

目录

技术支持联系方式

技术支持邮箱：support@wosign.com

技术支持热线电话：0755-26027828 / 0755-26027859 / 0755-26027827

技术支持论坛：https://bbs.wosign.com

公司官网地址：https://www.wosign.com

一、 获取 SSL 证书

从沃通完成 SSL 证书申请后，将会得到一个私钥 key 文件(创建 CSR 时保存)和一个 domain.com_sha256.zip 的压缩包文件，解压会得到三个子压缩包，IHS 服务器需要用到 for Nginx.zip 中的.crt 文件和私钥.key 文件。

二、 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：

2.1 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 for Nginx.zip 解压出来的.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：

2.2 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：

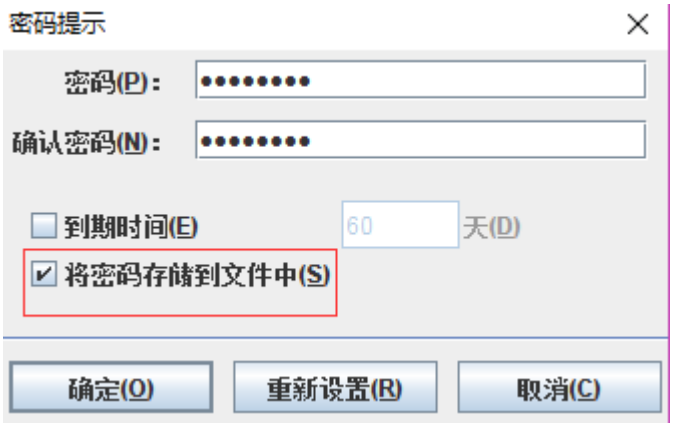
1）运行 IKeyMan(以 Windows 为例)

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。

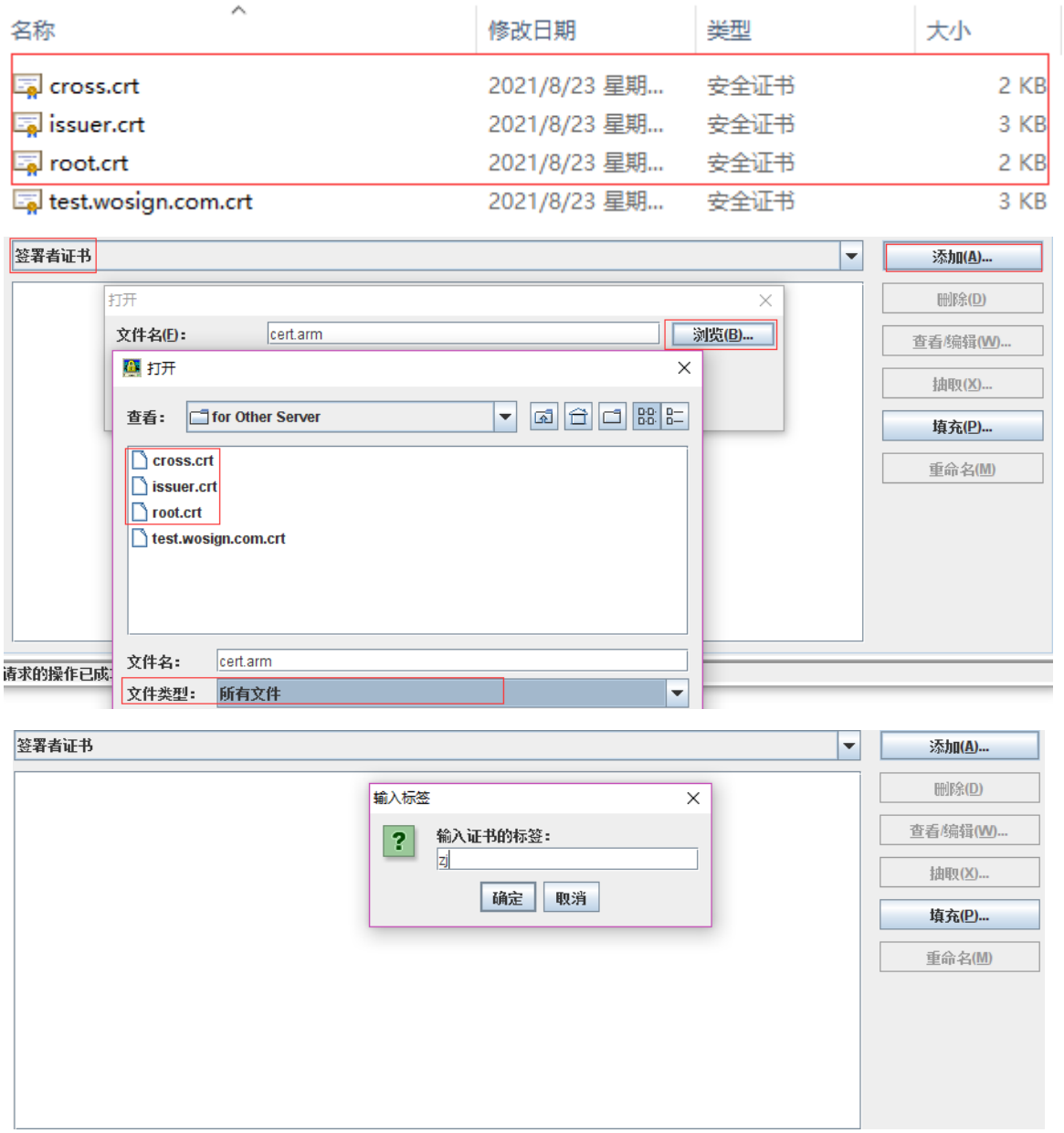
注意：请选中“将密码存储到文件”选项，此选项将把密码加密保存到扩展名为.sth 的文件中。IHS 启动时，会自动从该.sth 文件中读取密码，如果不选择此项启动 IHS 时会报错。



创建密钥库成功后，会在对应的目录下生成三个文件：

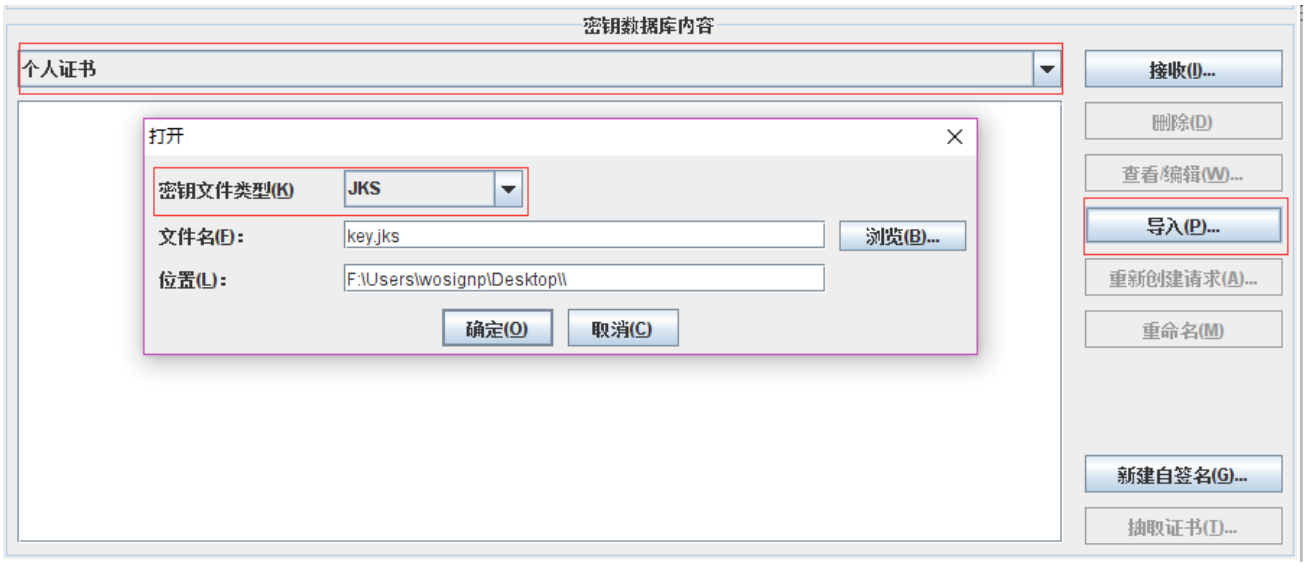
3) 导入签署者证书

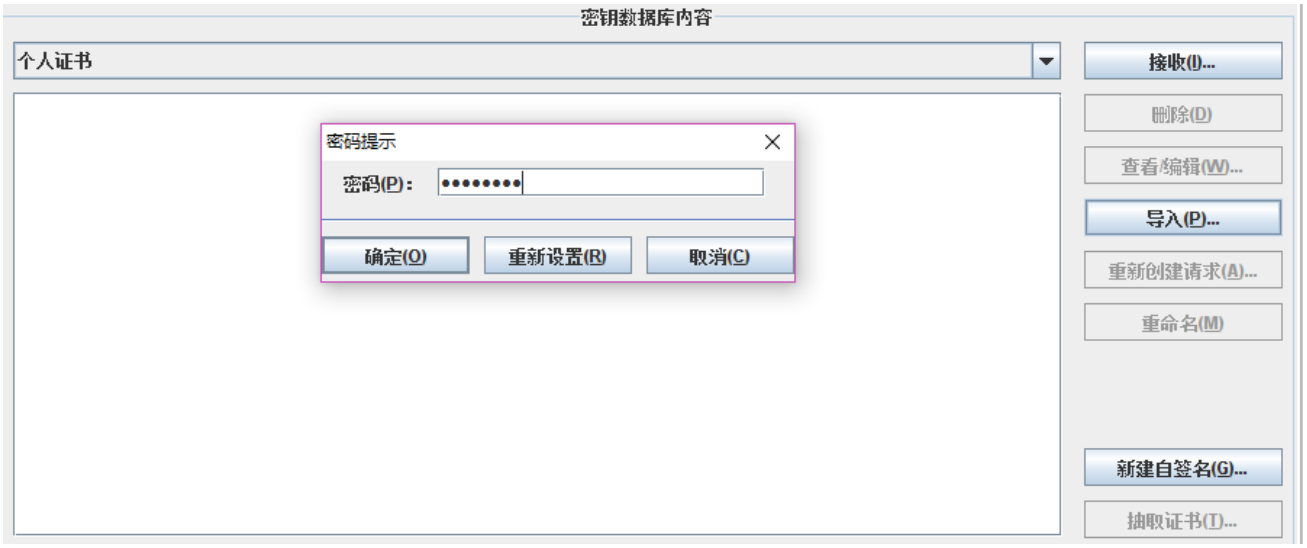
密钥数据库文件创建完成后，点击“签署者证书”-“添加”，将 for Other Server.zip 中的 issuer.crt、cross.crt、root.crt 文件依次导入签署者证书中(标签可自定义，不重复即可)。



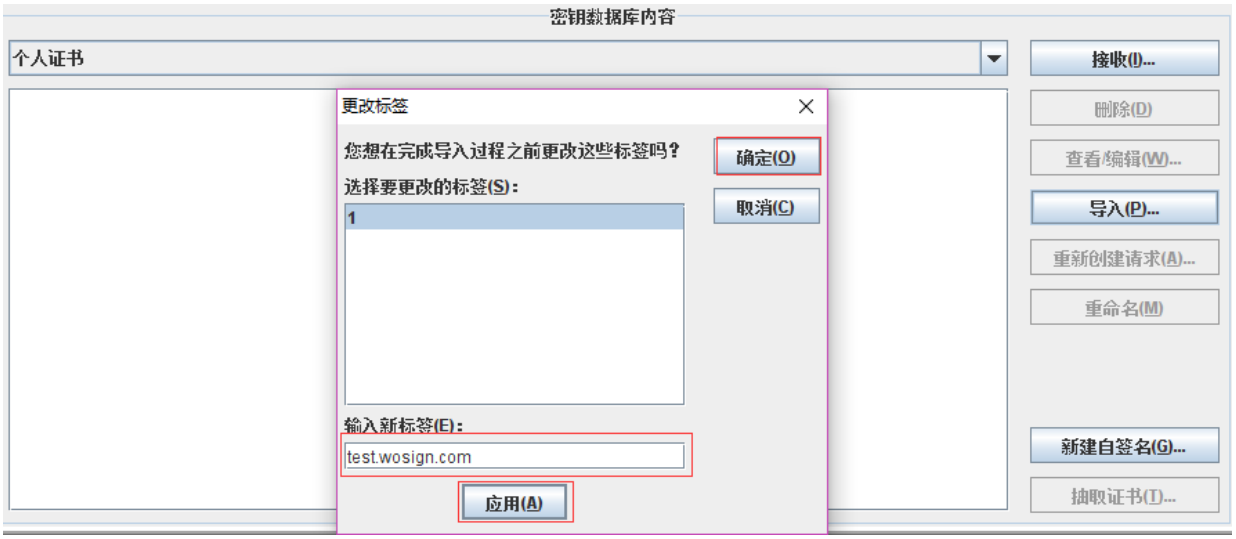
4) 导入 JKS 文件

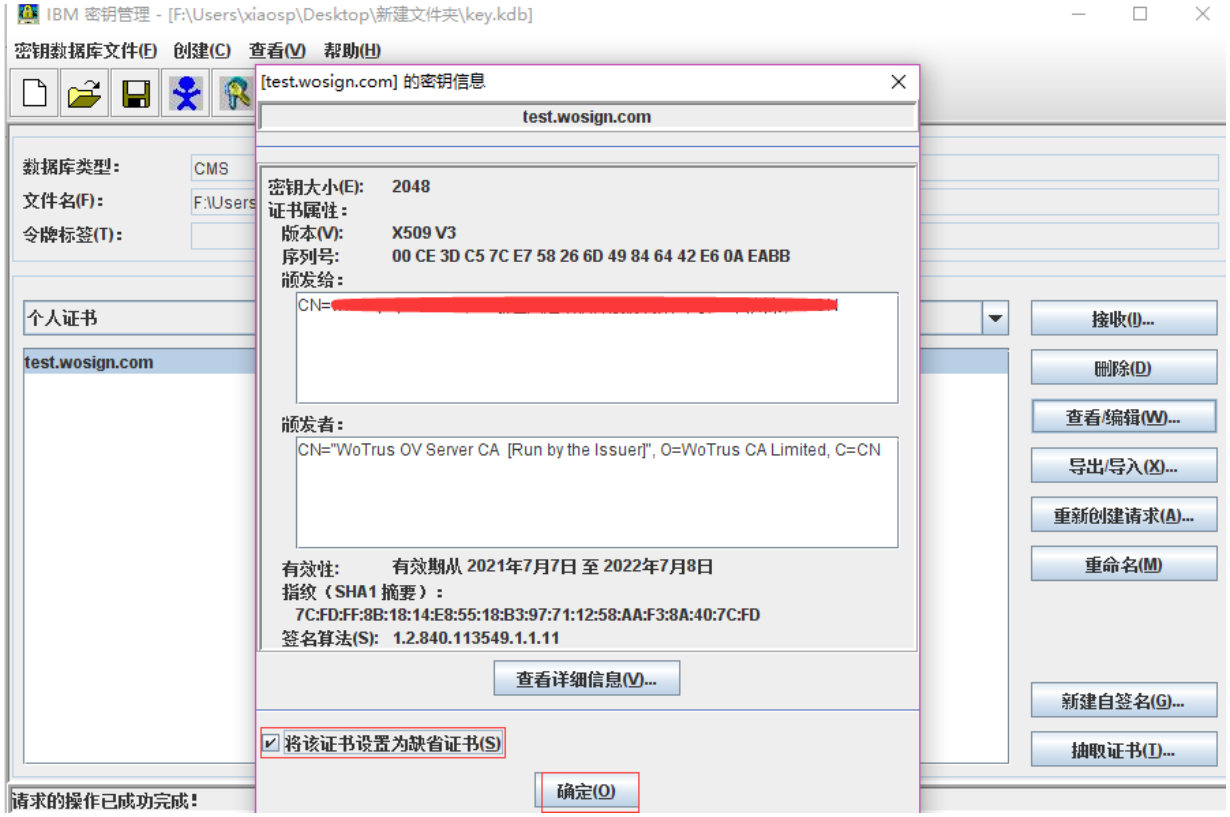
签署者证书导入完成后，回到“个人证书”，“导入”，选择之前步骤合成的 JKS 文件，输入设置的 JKS 密码。





输入密码确定后，将会弹出如下窗口，在新标签中输入证书域名或者别名，点击“应用”-“确定”，在个人证书中就可以看到对应的证书，点击“查看/编辑”，可将证书设置为缺省证书(默认证书)





三、 安装部署证书

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