

# 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** 

©2004-2017 沃通电子认证服务有限公司 WoTrus CA Limited All Rights Reserved

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502

电话: 0755-86008688 网站: www.wosign.com



目 录

<i>—</i> `,	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
<u> </u>	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	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

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



# 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:

	修改日期	类型	大小
ApacheServer	2023/10/23 12:09	文件夹	
NginxServer	沃通0街1023支:0井	文件夹	
OtherServer	2023/10/23 12:09	文件夹	
	2023/10/23 12:09	文件夹	
📓 README.txt	2023/10/23 12:09	TXT 文件	1 KB
	图 1		
名称 ^	修改日期	类型	大小
🔄 cross.crt	2023/3/31 16:34	安全证书	2 KB
🔄 intermediate.crt	2023/3/31 16:34	安全证书	3 KB
🔄 root.crt	2023/3/31 16:34	安全证书	2 KB
🔄 test.wosign.com.crt	2023/3/31 16:34	安全证书	3 KB

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)



名称 ^	修改日期	类型	大小
📋 test.wosign.com.csr	2019/1/9 9:38	CSR 文件	1 KB
🗋 test.wosign.com.key <del>🛶 — 私</del> 钥文件	2019/1/9 9:38	KEY 文件	2 KB

### 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: <u>https://download.wotrus.com/wotrus/wosigncode.exe</u>

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:

お格式 〇 5	安装证书 🗌 创	建SPC/证书链		在以下文本	·框中粘贴证书内	容(PEM格式):		
	DER OPFX O	JKS						
	DER OPFX 🧿	JKS (别名:1)						
OtherSe	erver中domain.	com.crt 🛛 🛎	起译					
创建C	SR时保存.key文	t件 ü	起译					
设	置JKS保护密码							
	+++1/4							
	转换							
	時格式 : : ・ PEM ・ ・ PEM ・ の の の の の の の に の 。 ・ : ・ ・ : ・ ・ : ・ : ・ ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : : ・ ・ ・ ・ ・ ・ ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ ・ ・ ・ ・ : ・ : ・ : ・ : ・ : ・ : ・ : ・ ・ : ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	<ul> <li>b推式 安装证书 创</li> <li>PEM DER PFX </li> <li>PEM DER PFX </li> <li>OtherServer中domain.</li> <li>创建CSR时保存.key文</li> <li>设置JKS保护密码</li> </ul>	<ul> <li>・ 安装证书 创建SPC/证书链</li> <li>・ PEM DER PFX JKS</li> <li>・ PEM DER PFX ・ JKS(別名:1)</li> <li>・ OtherServer中domain.com.crt 芝 创建CSR时保存.key文件 芝</li> <li>・ 设置JKS保护密码</li> </ul>	<ul> <li>・ 安装证书 创建SPC/证书链</li> <li>・ PEM DER PFX JKS</li> <li>・ PEM DER PFX ・ JKS (別名:1)</li> <li>・ OtherServer中domain.com.crt 选择</li> <li>・ 创建CSR时保存.key文件 选择</li> <li>・ 设置JKS保护密码</li> </ul>	<ul> <li>市格式 会装证书 创建SPC/证书链</li> <li>● PEM ● DER ● PFX ● JKS</li> <li>● PEM ● DER ● PFX ● JKS (別名:1)</li> <li>OtherServer中domain.com.crt 选择</li> <li>创建CSR时保存.key文件 选择</li> <li>设置JKS保护密码</li> </ul>	<ul> <li>● 在以下文本框中粘贴证书内</li> <li>● 在以下文本框中粘贴证书内</li> <li>● PEM ● DER ● PFX ● JKS</li> <li>● PEM ● DER ● PFX ● JKS (創名:1)</li> <li>● OtherServer中domain.com.crt 选择</li> <li>● 创建CSR时保存.key文件 选择</li> <li>● 设置JKS保护密码</li> </ul>	<ul> <li>● 在以下文本框中粘贴证书内容(PEM格式):</li> <li>● PEM ● DER ● PFX ● JKS</li> <li>● PEM ● DER ● PFX ● JKS (創名:1)</li> <li>● OtherServer中domain.com.crt 选择</li> <li>创建CSR时保存.key文件 选择</li> <li>设置JKS保护密码</li> </ul>	<ul> <li>● 在以下文本框中粘贴证书内容(PEM格式):</li> <li>● PEM ● DER ● PFX ● JKS</li> <li>● PEM ● DER ● PFX ● JKS (剧答:1)</li> <li>● OtherServer中domain.com.crt 选择</li> <li>● 创建CSR时保存.key文件 选择</li> <li>● 设置JKS保护密码</li> </ul>



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。

	🌉 IBM 密钥管理	
	密钥数据库文件(E) 创建(C) 查看(V) 帮助(E)	
新建		×
密钥数据库类型(K)	CMS 💌	
文件名(E):	key.kdb	浏览(B)
位置(L):	F:\Users\wosign\Desktop	
	确定( <u>O</u> ) 取消( <u>C</u> )	

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。

密码提示		×
密码(P):	•••••	
确认密码(N): 🔹	•••••	
到期时间(E)	60	天(D)
☑ 将密码存储到	文件中(S)	
确定(0)	重新设置(R)	取消( <u>C</u> )

创建密钥库成功后,会在对应的目录下生成三个文件:



	修改日期	类型	大小
📄 key.kdb	2021/9/7 星期二	KDB 文件	1 KB
🗋 key.rdb	2021/9/7 星期二	RDB 文件	1 KB
🗋 key.sth	2021/9/7 星期二	STH 文件	1 KB

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)

签署者证书			-	添加(A)
3	打开	X		删除(D)
	文件名(E):	cert.arm 浏览(B)		查看/编辑(₩)
	🌆 打开	×		抽职( <u>X</u> )
	查看: 📑	or Other Server		填充(P)
	Cross.crt	gn.com.crt	[	重命名(M)
	文件名:	cert.arm		
请求的操作已成:	文件类型:	所有文件		
签署者证书			•	添加( <u>A</u> )
				删除(D)
		? 输入证书的标签:		查看/编辑(W)
				抽取(X)
		确定		填充(P)
				重命名(M)

#### 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。



·····································		•	接收(!)
打开		×	删除(D)
密钥文件类型(	JKS		查看/编辑(W)
文件名(5):	key.jks	浏览(B)	导入(P)
位置(L):	F:\Users\wosignp\Desktop\\		重新创建请求(
	确定(O) 取消(C)		重命名(M)
			新建自签名(G
			抽取证书(1)。

密钥数据库内容	
个人证书	接收()
	删除(D)
密码提示 × · · · · · · · · · · · · · · · · · ·	查看/编辑(W)
	导入(P)
确定( <u>O</u> ) 重新设置( <u>R</u> ) 取消( <u>C</u> )	重新创建请求(A)
	重命名(M)
	新建自签名(G)
	抽取证书(工)…

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)。

	密钥数据库内容			
个人证书			-	接收(!)
	更改标签 您想在完成导入过程之前更改这些标签吗? 选择要更改的标签(S): 1 \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\ \$\	× 确定(0) 取消(C)		<ul> <li>圖除D</li> <li>查看總續(W)</li> <li>每入(P)</li> <li>重新创建请求(A)</li> <li>重命名(M)</li> </ul>
	test.wosign.com			新建日登名(O)… 抽取证书(I)…

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



mischape series Graets		1	
) 🚄 🖬 😤 🕻	[test.wosign.com] 的密钥信息 X		
	test.wosign.com	-	
数据库类型: CMS 文件名(F): F:\Use	· 签钥大小(E): 2048 · 证书报性: · 班书版性: · 新东水V··· X509 V3		
2 16 19 22 (17 -	序列号: 00 CE 3D C5 7C E7 58 26 6D 49 84 64 42 E6 0A EABB 额发给:		
个人证书 rest.wosign.com	CN=	-	接收() 冊除(D)
	酸炭者: CN="WoTrus OV Server CA [Run by the Issuer]", O=WoTrus CA Limited, C=CN		查看/编辑(W)
			导出/导入(X) 重新创建请求(A)
	有效性: 有效规从2021年7月7日至2022年7月8日 指放(SHA1 拖要): 7/C5DFF80E14562557883:97:71:22:58:AAF3:8A:40:7CFD 签名算法(S): 1.2340.113549.1.1.11		重命名(M)
	查看详细信息①		新建自签名(G)
	✓ 将该证书设置为缺省证书(S)		<b>抽取证书(I)</b>

## 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

地址:中国深圳市南山区南海大道 1057 号科技大厦二期 A 座 502



# 四、 SSL 证书的恢复

重复 2.3 操作即可。