

数安时代科技股份有限公司

GDCA 信鉴易® SSL 服务器证书请求指南 For keytool

2015/11/23



目录

部	署前特别说明	2
生	成证书请求	.3
1.	安装 JDK&JBoss(仅针对没有安装的用户)	.3
2.	生成 keystore 文件	.3
3.	生成证书请求文件(CSR)	.5
导	入服务器证书	5
1.	获取服务器证书	.5
2.	获取根证书和 CA 证书	. 5
	1) 从邮件中获取:	. 5
	2)从 GDCA 官网下载	.7
证书	,遗失处理	.9
	部 ⁴ 1. 2. 3. 号 1. 2. 证书	 部署前特别说明 生成证书请求

一、部署前特别说明

- 1. 本文档主要描述如何通过 Keytool 产生密钥对;
- 2. 本指南在 windows 下适用 Keytool 工具方式生成证书请求文件;
- 3. 您可以使用其它方式并不要求按照本指南在 windows 下使用 Keytool 工具方式生成证书请求文件;



二、生成证书请求

1. 安装 JDK&JBoss (仅针对没有安装的用户)

安装过程比较简单,采取默认方式安装即可,如有需要可以修改安装的目录。

2. 生成 keystore 文件

生成密钥库文件 keystore.jks 需要使用 JDK 的 keytool 工具。命令行进入 JDK 或 JRE 下的 bin 目录,运行 keytool 命令(示例中粗体部分为可自定义部分, 可根据实际配置情况相应修改)。

keytool -genkey -alias **gdca** -keyalg RSA -keysize 2048 -keystore **D:\gd ca.jks**



(JDK 6 及以上版本,密码输入时不会回显)







(JDK 5版本,密码明文显示)

以上命令中,gdca为私钥别名(-alias),生成的gdca.jks文件默认放在D 盘根目录下。

注意:

- ▶ 请务必根据提示录入全部项目,并保证其准确性
- ▶ 若输出路径含有空格,需使用英文状态下的双引号括起来
- ▶ keystore 密码至少 6 个字符, 若电脑安装了 JDK 6 或以上版本, 密码输入时不会显示; 若安装了 JDK 5 版本, 密码输入时将可能出现明文显示, 请务必注意并牢记此密码, 尤其含有大小写字母的情况
- ▶ 下文涉及到 keytool 工具输入的密码均为此密码
- 如组织名称含有逗号,录入时不用输入引号,一般系统会在下面提示信息中的组织名称自动添加引号,请务必查看;如发现没有引号,请关闭命令行窗口,然后打开一个新窗口重新操作;
- ▶ 提示输入主密码时直接按回车即可,保证 keystore 密码与 gdca 主密码 一致



3. 生成证书请求文件(CSR)

keytool -certreq -alias gdca -sigalg SHA256withRSA -file D:\certreq.c
sr -keystore D:\gdca.jks



请备份密钥库文件 gdca. jks,将证书请求文件 certreq. csr 提交给 GDCA, 等待证书签发。如密钥库文件 gdca. jks 丢失,会导致证书不可用。

三、导入服务器证书

1. 获取服务器证书

在您完成申请 SSL 服务器证书的流程后,GDCA 将会在返回给您的邮件中附上 服务器证书,请留意查看申请证书时填写的邮箱。

2. 获取根证书和 CA 证书

获取根证书和 CA 证书可参考以下两种方法之一,建议优先从邮件中获取。

1) 从邮件中获取:

在您完成申请 GDCA 服务器证书的流程后,GDCA 将会在返回给您的邮件中附 上根证书 GDCA_TrustAUTH_R5_ROOT.cer 和相应的 CA 证书,请留意查看申请证书 时填写的邮箱。如果您申请的是睿信(OV) SSL 证书(Organization Validation SSL Certificate), CA 证书文件就是 GDCA_TrustAUTH_R4_OV_SSL_CA.cer;如 果您申请的是恒信企业 EV SSL 证书(Extended Validation SSL Certificate), CA 证书就是文件就是 GDCA_TrustAUTH_R4_EV_SSL_CA.cer,请确认所收到的证书

5





文件是您需要的 CA 证书。(注意: 所发至邮箱的文件是压缩文件, 里面有 3 张证

书,请确认所收到的证书文件是您需要的 CA 证书文件)

文件(F) 命令(C) 工具(S) 收藏夹(Q) 选项(N	l) 帮助(<u>H</u>)				
添加 解压到 测试 查看 删除	直找			→ 24 (R护 自)	▲ 解压格式
🗈 َ َ www.huizhou.gov.cn(1).rar\www.h	uizhou.gov.cn	- RAR 压缩文	件, 解包大小为 6,	188 字节	
名称	大小	压缩后大小	类型	修改时间	CRC32
<u>}</u> .			文件夹		
GDCA TrustAUTH R4 EV SSL_CA.cer 由视	证书 2,090	1,576	安全证书	2016/10/18 1	58479850
GDCA TrustAUTH R5 ROOT.cer	2,012	1,488	安全证书	2016/10/18 1	F8476090
I www.huizhou.gov.cn.cer	2,086	1,473	安全证书	2016/10/18 1	FBCD26

GDCA_TrustAUTH_R4_OV_SSL_CA.cer:

一一 洋细信白 证书路径	
吊规 许细信息 阻力阻住	
~ 证书路径 (P)	
🗔 GDCA TrustAUTH R5 ROOT	
GDCA TrustAUTH R4 OV SSL CA	
GDCA TrustAUTH R4 OV SSL CA	
i(
⊶ En GDCA TrustAUTH R4 OV SSL CA	
태제특징 GDCA TrustAUTH R4 OV SSL CA	

GDCA_TrustAUTH_R4_EV_SSL_CA.cer:





常规	详细信息	证书路径	
证书	·路径(2)—		
4			

2) 从 GDCA 官网下载

用户可以访问 GDCA 官网

<u>https://www.gdca.com.cn/customer_service/knowledge_universe/ca_cq/</u> 下载服务器证书的根证书和 CA 证书,如下图所示:

服务指南	>	CA证书查询				
下载中心	>	为保证您的证书能够正常使用,需要为浏览器下载并安装CA很证书,这样你的浏览器才能信任由GDCA签发的所有证书(下载后双 击正书文件进行安装)。 34 项,显示 31 到34.[<u>直刃] 卸,2_3_</u> 4 [下一页 末页]				
技术支持	>					
证书服务	~	CA名称	起始有效时间	截止有效时间	CA证书下载	
CP和CPS		GDCA TrustAUTH E4 Primer CA	2016-03-31	2030-12-31	GDCA TrustAUTH F4 Primer C4 cer	
CA证书查询			17:55:52	00:00:00		
用户证书查询		GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA TrustAUTH R4 OV SSL CA.cer	
CRL下载		GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA TrustAUTH R4 EV SSL CA.cer	
		GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07	2030-12-31	GDCA TrustAUTH R4 EV CodeSigning CA.cer	

获取第一张证书 根证书 GDCA_TrustAUTH_R5_ROOT.cer,如下图所示:





CA名称	起始有效时间	截止有效时间	CA证书下载
ROOTCA_sm2	2012-07-14 11:11:59	2042-07-07 11:11:59	社会公众应用根证书(SM2).cer
GDCA TrustAUTH E1 CA	2014-06-26 15:02:11	2034-06-21 15:02:11	广东数字证书认证中心有限公司 sm2.cer
ROOTCA_rsa	2005-08-28 16:16:16	2025-08-23 16:16:16	社会公众应用根证书(RSA).cer
GDCA TrustAUTH R2 CA	2013-12-16 14:29:40	2018-12-15 14:29:40	广东数字证书认证中心有限公司 rsa.cer
GDCA Root CA	2004-01-11 17:34:22	2024-12-11 00:00:00	GDCA Root CA.cer
GDCA Guangdong Certificate Authority	2004-01-12 10:13:07	2024-01-12 10:13:07	GDCA Guangdong Certificate Authority.ce
GDCA TrustAUTH R5 ROOT	2014-11-26 13:13:15	2040-12-31 23:59:59	GDCA TrustAUTH R5 ROOT.cer
GDCA TrustAUTH R4 SSL CA	2014-11-26 17:52:00	2030-12-31 00:00:00	GDCA TrustAUTH R4 SSL CA.cer
GDCA TrustAUTH R4 Generic CA	2016-04-07 17:58:44	2030-12-31 00:00:00	GDCA TrustAUTH R4 Generic CA.cer

获取第二张证书:

CA证书若您申请的证书是睿信(OV) SSL证书(Organization Validation SSL Certificate),下载 GDCA_TrustAUTH_R4_OV_SSL_CA.cer,如下图所示:

34 项,显示 31	到34.[首页/前一页] 1	1,234[下一页/末页]
------------	----------------	---------------

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH E4 Primer CA	2016-03-31 17:55:52	2030-12-31 00:00:00	GDCA TrustAUTH E4 Primer CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA TrustAUTH R4 OV SSL CA.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA TrustAUTH R4 EV SSL CA.cer
GDCA TrustAUTH R4 EV CodeSigning CA	2016-04-07 17:32:51	2030-12-31 00:00:00	GDCA TrustAUTH R4 EV CodeSigning CA.cer

若您申请的证书是恒信企业 EV SSL 证书 (Extended Validation SSL

Certificate),则下载 GDCA_TrustAUTH_R4_EV_SSL_CA.cer

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH E4 Primer CA	2016-03-31 17:55:52	2030-12-31 00:00:00	GDCA TrustAUTH E4 Primer CA.cer
GDCA TrustAUTH R4 OV SSL CA	2016-04-05 17:36:20	2030-12-31 00:00:00	GDCA TrustAUTH R4 OV SSL CA.cer
GDCA TrustAUTH R4 EV SSL CA	2016-04-06 11:35:09	2030-12-31 00:00:00	GDCA TrustAUTH R4 EV SSL CA.cer





从 GDCA 官网获取根证书和 CA 证书后需要转换成 Base64 编码格式,如下图 所示:

正书 💼	X	证书导出向导 ————————————————————————————————————
常规 详细信息 证书 显示 (S): <∭ (所有>	路径	导出文件格式 可以用不同的文件格式导出证书。
字段 版本 序列号 经名算法 经站哈希算法 机关发者 有效期从 到	値 V3 64 0c 3b 33 de 07 3c 61 sha25685A sha256 GDCA TrustAUTH R5 R00T, 2014年11月26日 17:52:00 2030年12月31日 0:00:00 ▼	 法择要使用的格式: ● DER 编码二进制 X.509(CER)(D) ● Base64 编码 X.509(CER)(S) ● 加密消息语法标准 - PRCS #7 证书(P7B)(C) □ 如果可能,则数据包括证书路径中的所有证书(D) ● 个人信息交换 - PRCS #12(PFX)(P) □ 如果可能,则数据包括证书路径中的所有证书(D) □ 如果可能,则数据包括证书路径中的所有证书(D) □ 如果与出成功,删除私钥(C) □ 雪出所有扩展属性(A) ● Microsoft 序列化证书存储(SST)(T)
了解证书详细信息的更多	編辑属性 (2) 夏制到文件 (C)) 信息 确定	了解证书文件格式的详细信息 (上一步 (b))下一步 (x) > 取消

四、证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件,请联系 GDCA (客服 热线 95105813)办理遗失补办业务,重新签发服务器证书。

