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

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；

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

二、生成证书请求

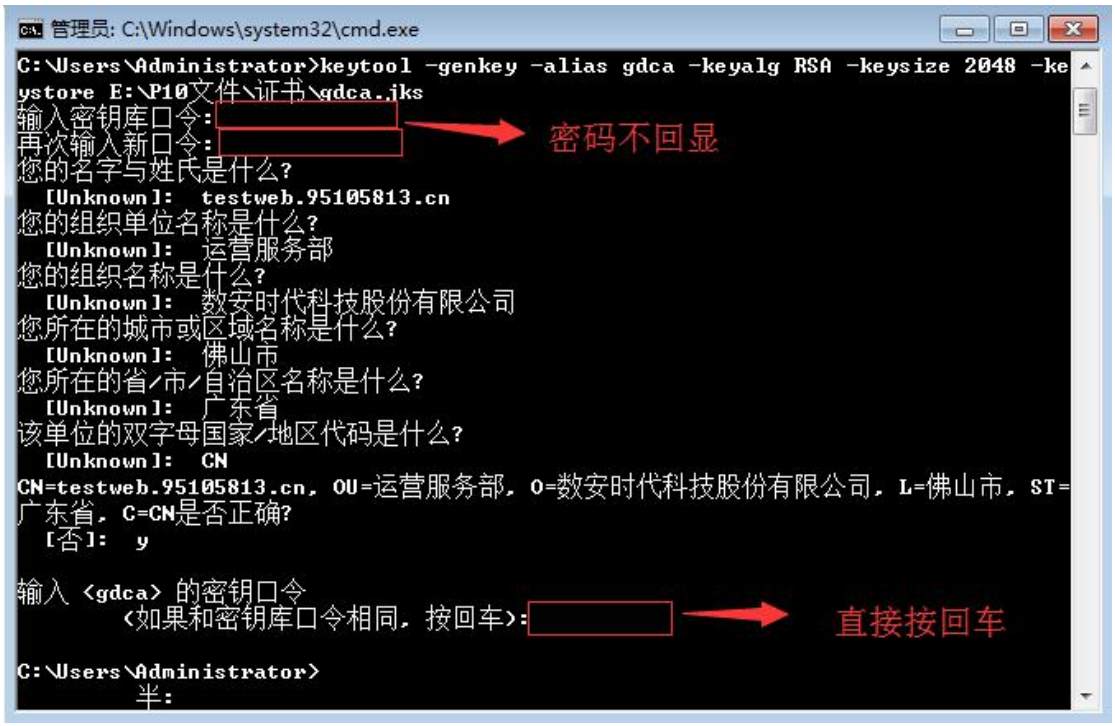
1. 安装 JDK&JBoss（仅针对没有安装的用户）

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:\gdca.jks**



（JDK 6 及以上版本，密码输入时不会回显）

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

（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

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

3. 生成证书请求文件(CSR)

keytool -certreq -alias gdca -sigalg SHA256withRSA -file D:\certreq.csr -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

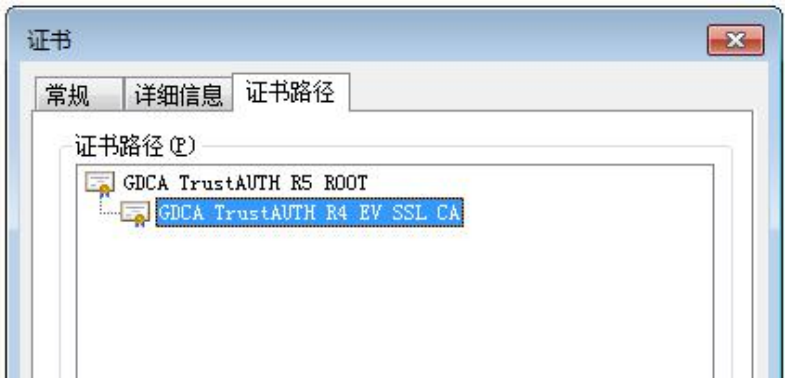
地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

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）

GDCA_TrustAUTH_R4_OV_SSL_CA.cer：

GDCA_TrustAUTH_R4_EV_SSL_CA.cer:

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813



2) 从 GDCA 官网下载

用户可以访问 GDCA 官网

https://www.gdca.com.cn/customer_service/knowledge_universe/ca_cq/

下载服务器证书的根证书和 CA 证书,如下图所示：

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

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

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.cer
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, 2, 3, **4** [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

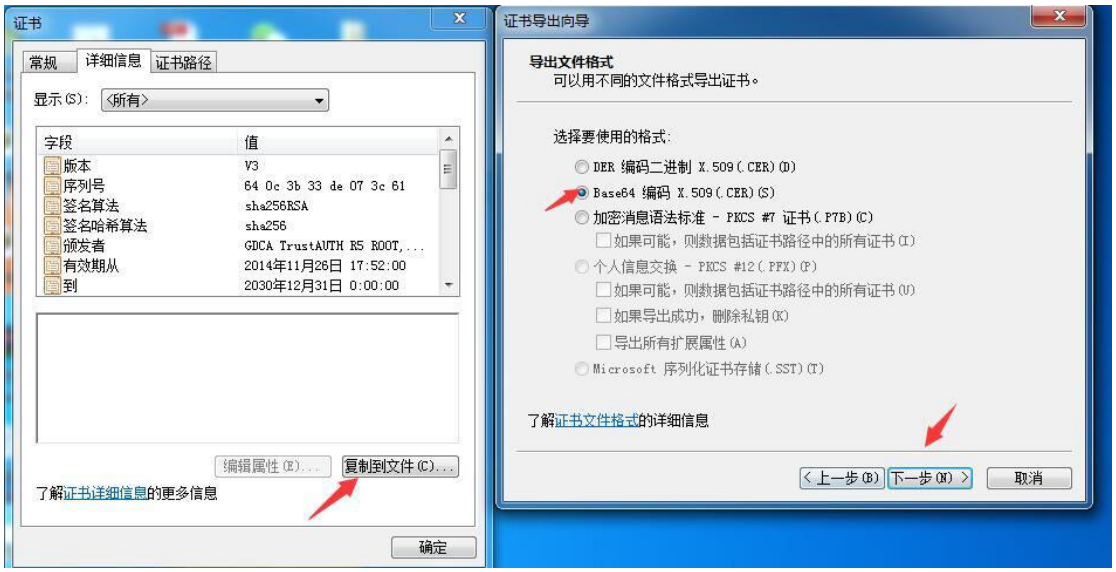
为保证您的证书能够正常使用，需要为浏览器下载并安装CA根证书，这样你的浏览器才能信任由GDCA签发的所有证书（下载后双击证书文件进行安装）。

34 项，显示 31 到34.[首页/前一页] 1, 2, 3, **4** [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

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813

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：



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。

地址：广州市东风中路 448 号成悦大厦 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）：95105813