

注：本实验在fedora 24下，openssl1.1.0

初始化

```
1 rm -rf /etc/pki/CA/*_old
2 touch /etc/pki/CA/index.txt
3
4 touch /etc/pki/CA/index.txt.attr
5 echo "unique_subject = no" > index.txt.attr
6
7 echo 01 > /etc/pki/CA/serial
8 echo 02 > /etc/pki/CA/serial
9 rm -rf keys
10 mkdir keys
```

生成根CA并自签 (Common Name填RootCA)

```
1 openssl genrsa -des3 -out keys/RootCA.key 2048
2 openssl req -new -x509 -days 3650 -key keys/RootCA.key -out keys/RootCA.crt
```

生成二级CA (Common Name填SecondCA)

```
1 openssl genrsa -des3 -out keys/secondCA.key 2048
2 openssl rsa -in keys/secondCA.key -out keys/secondCA.key
3 openssl req -new -days 3650 -key keys/secondCA.key -out keys/secondCA.csr
4 openssl ca -extensions v3_ca -in keys/secondCA.csr -config /etc/pki/tls/openssl.cnf -days 3650 -out keys/secondCA.crt
```

生成三级CA (Common Name填ThirdCA)

```
1 openssl genrsa -des3 -out keys/thirdCA.key 2048
2 openssl rsa -in keys/thirdCA.key -out keys/thirdCA.key
3 openssl req -new -days 3650 -key keys/thirdCA.key -out keys/thirdCA.csr
4 openssl ca -extensions v3_ca -in keys/thirdCA.csr -config /etc/pki/tls/openssl.cnf -days 3650 -out keys/thirdCA.crt
```

使用三级CA签发服务器证书

```
1 openssl genrsa -des3 -out keys/server.key 2048
2 openssl rsa -in keys/server.key -out keys/server.key
3 openssl req -new -days 3650 -key keys/server.key -out keys/server.csr
4 openssl ca -in keys/server.csr -config /etc/pki/tls/openssl.cnf -days 3650 -out keys/server.crt -cert keys/thirdCA.crt
```

注：

指定证书数据内容

```
1 -subj /C=CN/ST=Guangdong/L=Shenzhen/O=PAX/OU=Common Software/CN=Server CA/emailAddress=qiaoje@paxsz.com
```

去掉key加密的输入提示：

```
1 去掉 -des3
```

don't ask question

```
1 -batch
```

certpem格式

```
1 openssl x509 -in mycert.crt -out mycert.pem -outform PEM
```

吊销证书 (作废证书)

首先

```
1 echo 00 > /etc/pki/CA/crlnumber
```

一般由于用户私钥泄露等情况才需要吊销一个未过期的证书。(当然我们用本测试CA时其很少用到该命令,除非专门用于测试吊销证书的情况)  
假设需要被吊销的证书文件为client.pem,则执行以下命令吊销证书:

```
1 openssl ca -revoke client.pem -cert RootCA.pem -keyfile RootCA.key -config /etc/pki/tls/openssl.cnf
```

生成证书吊销列表文件 (CRL)

准备公开被吊销的证书列表时,可以生成证书吊销列表 (CRL),执行命令如下:

```
1 openssl ca -gencrl -out client.crl -cert RootCA.pem -keyfile RootCA.key -config /etc/pki/tls/openssl.cnf
```

还可以添加 -cridays和 -crhours参数来说明下一个吊销列表将在多少天后 (或多少小时候)发布。

可以用以下命令检查client.crl的内容:

```
1 openssl crl -in client.crl -text -noout
```

Spring中的@Transactional事物回滚实例源码

openssl生成证书及吊销列表

一,先来讲讲基本概念. 证书分类:按类型可以分为CA证书和用户证书,我们说的root也是特殊的CA证书. 用户证书又可以按照用途分类,放在...

优质评论可以帮作者获得更高权重

Levi\_Mavin: WeiSont\_Ross: 楼主你好,我想问一下,如何给证书添加CRL发点,比如修改配置文件或者添加参数 这样能实现吗? 2年前 回复

证书介绍及openssl生成证书和吊销列表\_xmayyang的专栏

证书介绍及openssl生成证书和吊销列表 转自http://www.manimcode.com/info-detail-1062882.html 一,先来讲讲基本概念. 证书分类:按类型可以分为CA证...

证书吊销列表CRL的使用\_果他爹的学习笔记

证书吊销列表CRL的使用 吊销证书命令openssl ca -revoke xxx.pem 生成吊销证书列表openssl ca -gencrl -out xxx.crl apache 中的使用 设置/usr/local/...

证书吊销列表 (Certificate Revocation List, CRL)

证书吊销列表 (Certificate Revocation List, CRL) 一个被签署的列表,它指定了一套证书发布者认为无效的证书.除了普通CRL外,还定义了一些特殊...

OpenSSL的CRL

2019独角兽企业重金招聘Python工程师标准>>> ...

windows下使用openssl创建多级证书链\_shuizhongmose的专栏

windows下使用openssl创建多级证书链 参考https://jamielinux.com/docs/openssl-certificate-authority/introduction.html 这篇文章很有参考价值 可以使用...

C++期末考试试卷与全部习题(含答案)

里面有两套期末考试试卷,整个C++内容的全部习题.是学生自学习和学习的好资料.全部有参考答案.

openssl生成证书(三级证书链)linux

生成思路:1.创建CA私钥(ROOT证书)2.生成CA证书请求3.CA私钥自签名CA证书并导出根证书cer4.创建中间证书私钥5.生成中间证书请求6.CA私...

openssl生成证书链多级证书

openssl生成证书链多级证书 https://www.cnblogs.com/gsls200808/p/4502944.html

openssl crl 使用方法

用途: crl工具,用于处理X.509格式的CRL文件. -inform arg 输入文件的格式. DER是DER编码的CRL对象. PEM (默认格式) 是base64编码的...

OpenSSL学习笔记——CRL

今天晚上打扑克累了,没心思学习了,所以把这一阵学的OpenSSL的CRL大概总结一下. CRL(CertificateRevocationList,证书吊销列表,是在...

利用openssl生成CA证书的方法及证书

利用openssl生成CA证书的方法及证书,根据文档可以自己生成证书.

证书吊销列表CRL解析工具 (Java)

证书吊销列表CRL解析工具 (Java)

openssl生成证书以及在tomcat下的配置

这是我自己关于学习openssl的一些心得,很初级,请大家不要见笑

No compatible source was found for this video. 解决方法

videojs播放mp4,测试代码,需要部署到服务器上(包括但不限于tomcat, iis ) 路径为test/test2.html.

证书链(The Certificate Chains)

名称解释 可选 DN (Distinguished Name) 标识名, 包含一些指定实体身份的字段,如通用名,组织等等CSR(Certificate Signing Request)数字证书签名...

The\_Hungry\_Brain

我前6年 暂无认证

99 13万+ 112万+ 27万+

原创 周排名 总排名 访问 等级

3263 105 148 14 508

积分 粉丝 获赞 评论 收藏

私信 关注

搜博文

热门文章

生成PKCS12证书,以及解析PKCS12证书 24107

HTTP2 协议规范 23492

Linux驱动开发入门——基本知识简介 22170

openssl生成证书链多级证书、证书吊销列表(CRL) 20433

VS 2015 正确设置DLL路径的方法 16619

最新评论

VS 2015 正确设置DLL路径的方法 Z - C: 好的,谢谢 22170

VS 2015 正确设置DLL路径的方法 GTMHS: 要以分号隔开,我整了半天整出来,结果加了个分号就成了

VS 2015 正确设置DLL路径的方法 GTMHS: 要以分号隔开,我整了半天整出来,结果加了个分号就成了

VS 2015 正确设置DLL路径的方法 linux20022: 谢谢大佬,我也设置成功了

VS 2015 正确设置DLL路径的方法 Z - C: 但是不知道为什么,我的项目只能添加一个.dll路径,再添加第二个时,只能重...

您愿意向朋友推荐“博客详情页”吗?

👍 👎 😐 😊 😞

强烈推荐

不推荐

一般般

排序

强烈推荐

最新文章

面试题

设备驱动程序

Go 语言

2020年: 1篇

2019年: 1篇

2018年: 14篇

2017年: 51篇

2016年: 39篇

openssl CRL证书

CRL(Certificate Revocation List) 证书撤销列表，是在证书撤销时用的。当证书因为一些原因会被CA吊销的证书。客户端拿到这个CRL后，就可以知道那些...

又小小蜀的博客 · 1210

单机使用Openssl搭建CA并生成证书和CRL ( windows、linux )

shuizhongmoe的专栏 · 1153

python openssl 读取crl吊销证书

1710

import OpenSSL (p = open("Users\heyong\Downloads\OZCA\Crl20130502.crl", "r") crl = "" join(fp.readlines()) crl\_object = OpenSSL.crypto.load(Cr...

©2021 CSDN 皮肤主题: 大白 设计师: CSDN官方博客 返回首页

关于我们 招贤纳士 广告服务 开发助手 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00

The\_Hungry\_Brain 关注

5 1 14

专栏目录

