SSL 同时被 2 个专栏收录 0 订阅 4 篇文章 订阅专

注：本实验在fedora 24下，openssl1.1.0

初始化

```
rm -rf /etc/pki/CA/*.old
touch /etc/pki/CA/index.txt

touch /etc/pki/CA/index.txt.attr
echo "unique_subject = no" > index.txt.attr

echo 01 > /etc/pki/CA/serial
echo 02 > /etc/pki/CA/serial
rm -rf keys
mkdir keys
```

生成根CA并自签（Common Name填RootCA）

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

生成二级CA（Common Name填SecondCA）

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

- **生成三级CA（Common Name填ThirdCA）**

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

- **使用三级CA签发服务器证书**

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

注：

指定证书数据内容

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

去掉key加密的输入提示：

```
去掉 -des3
```

don't ask question

```
-batch
```

---

crt转pem格式

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

吊销证书（作废证书）

首先

```
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时其时很少用到该命令，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：

```
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：

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

还可以添加-crldays和-crlhours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：

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


The_Hungry_Brain
码龄9年 暂无认证
99 原创 13万+ 周排名 112万+ 总排名 27万+ 访问 等级
3263 积分 105 粉丝 148 获赞 14 评论 508 收藏
私信 关注

搜博主文章

最新评论
VS 2015 正确设置DLL路径的方法
Z - C: 好的，谢谢
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
linxizi0622: 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？

强烈不推荐 不推荐 一般般 推荐 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　艾小小雨的博客 1210
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…

单机使用Openssl搭建CA并生成证书和CRL（woindows、linux）　shuizhongmose的专栏 1153
参考文档：https://blog.csdn.net/miouqi/article/details/75268402 安装 windows去openssl官网下载安装包，然后将openssl的路径添加到环境变量PATH下…

python openssl 读取 crl 吊销 证书　1710
import OpenSSL fp = open('/Users/heyong/Downloads/DZCACrl20130502.crl', 'r') crl = "".join(fp.readlines()) crl_object = OpenSSL.crypto.load_crl(Ope…

The_Hungry_Brain　关注　5　1　14　专栏目录