



openssl创建根证书并用根证书创建子证书

原创 小丶二 linux 2018/04/10 18:25 阅读量 2.2K



本文被收录于专区
程序人生

进入专区参与更多专题讨论

```
// 根证书私钥 ca.key (无密码去掉-des3)
openssl genrsa -des3 -out ca.key 1024

// 生成公钥
openssl rsa -in cakey.crt -pubout -out capubkey.crt

// 根证书请求 ca.csr
openssl req -sha256 -new -key ca.key -out ca.csr

// 使用私钥和证书请求签发根证书 ca.crt
openssl req -x509 -days 1024 -key ca.key -in ca.csr > ca.crt
或
openssl x509 -req -in request.csr -out cert.cer -signkey private.key -days 365

// 生成v3证书
openssl x509 -req -extfile /etc/pki/tls/openssl.cnf -extensions v3_req -in req.csr -out cert.cer -signkey pr

// 生成p12证书
openssl pkcs12 -export -in child.cer -inkey child.key -password pass:111111 -out child.p12

// 生成带CA的p12证书
openssl pkcs12 -export -in server.pem -inkey server.key -certfile ca.pem -password pass:111111 -out server.p1

// 解析p12证书
openssl pkcs12 -in client.p12 -password pass:11111111 -nodes

// 然后使用上面1、2命令创建server.csr、server.key

// 使用根证书签发证书
openssl x509 -req -in server.csr -out server.crt -signkey server.key -CA ca.crt -CAkey ca.key -CAcreateserial

// 将密钥和证书合并,将crt文件内容追加到server.key内容后面
cp server.key server.pem
cat server.crt >> server.pem

// 检测证书是否根证书签发
openssl verify -CAfile 根证书.crt 用户证书.crt
openssl verify -CAfile 根证书.crt -verbose 用户证书.crt

// 验证crl文件
openssl crl -in server.crl -CAfile root.cer -noout
// 返回Error getting CRL issuer certificate 或 verify OK
```



关注 私信 提问

文章 67 经验值 175 粉丝 1 关注 0

作者的专辑

全部

其它 (1)
shell (1)
英语 (1)
C语言 (10)

原创计划

立即入驻

自媒体入驻开源社区，
获百万流量，打造个人技术品牌



推荐关注

换一批



yokol
文章 56 访问 7.8W



wphmoon
文章 37 访问 16.7W



暗中观察
文章 175 访问 54.5W



jump--jump
文章 37 访问 9.3W



雪饼
文章 62 访问 529.4W



打赏



0 评论



0 收藏



0 赞



分享

```
// 吊销证书server.crt
openssl ca -revoke server.crt -cert ca.crt -keyfile ca.key

// 生成crl吊销证书文件
openssl ca -gencrl -out ca.crl -cert ca.crt -keyfile ca.key

// 查看crl文件内容
openssl crl -in client.crl -text -noout

// crl文件der转pem
openssl crl -in server.der -inform der -outform pem -out server.pem

// 生成证书链文件
openssl crl2pkcs7 -certfile root01.pem -certfile root02.pem -outform PEM -out root.p7b -nocrl

// 查看证书信息
openssl x509 此处省略10000字。。。静静往下看↓↓↓

// 打印证书请求信息
openssl req -in cert.pem -noout -text

// 打印出证书的内容:
openssl x509 -in cert.pem -noout -text

// 打印出证书的系列号
openssl x509 -in cert.pem -noout -serial

// 打印出证书的拥有者名字
openssl x509 -in cert.pem -noout -subject

// 打印证书颁发者
openssl x509 -in ca.crt -noout -issuer

// 以RFC2253规定的格式打印出证书的拥有者名字
openssl x509 -in cert.pem -noout -subject -nameopt RFC2253

// 在支持UTF8的终端一行过打印出证书的拥有者名字
openssl x509 -in cert.pem -noout -subject -nameopt oneline -nameopt -escmsb

// 打印出证书的MD5特征参数
openssl x509 -in cert.pem -noout -fingerprint

// 打印出证书的SHA特征参数
openssl x509 -sha1 -in cert.pem -noout -fingerprint

// 把PEM格式的证书转化成DER格式
openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER

// 把der格式的证书链转为pem格式
openssl pkcs7 -inform der -in safaricom_b2c.p7b -out safaricom_b2c_readable.p7b

// 把p7b转换成cer格式
openssl pkcs7 -print_certs -in chain.p7b -out chain.cer

// 把一个证书转化成CSR
openssl x509 -x509toreq -in cert.pem -out req.pem -signkey key.pem

// 给一个CSR进行处理, 颁发签名证书, 增加CA扩展项
openssl x509 -req -in careq.pem -extfile openssl.cnf -extensions v3_ca -signkey key.pem -out cacert.pem

// 给一个CSR签名, 增加用户证书扩展项
openssl x509 -req -in req.pem -extfile openssl.cnf -extensions v3_usr -CA cacert.pem -CAkey key.pem -CAcreate

// 取证书请求文件的MD5
openssl req -modulus -in req.csr | grep Modulus | openssl md5

// 取证书公钥MD5
cat ecpubkey.pem | openssl md5
```

```
// 取证书私钥MD5
openssl rsa -noout -modulus -in private.key | openssl md5
```

openssl

© 著作权归作者所有

举报



打赏



0 赞



0 收藏



分享

作者的其它热门文章

[php 实现RSA加密解密](#)

[php 实现AES加密](#)

[mysql数据库出现ERROR 1 \(HY000\): Can't create/write to file '/tmp/#sql_a019_0.MYT'](#)

[select选择已选中的option不触发onchange事件的解决办法](#)



OSCHINA 社区

关于我们
联系我们
加入我们
合作伙伴
Open API

在线工具

Gitee.com
企业研发管理
CopyCat-代码克隆检测
实用在线工具
[国家反诈中心APP下载](#)

活动

源创计划
月度评选
“交个朋友”计划

QQ群



530688128

公众号



视频号



OSCHINA APP

聚合全网技术文章，根据你
的阅读喜好进行个性推荐

下载 APP

©OSCHINA(OSChina.NET) 工信部 开源软件推进联盟 指定官方社区

深圳市奥思网络科技有限公司版权所有 粤ICP备12009483号

