**信息安全综合实验报告**

**Lab1私有CA证书签发的简单实现**

**信安法 2013484 张世伟**

1. **实验目的**
   1. 熟悉Openssl工具的使用
   2. 搭建私有CA并生成根证书
   3. 完成证书签发、吊销流程的简单实现
2. **实验原理**
   1. **PKI的基本组成**
   2. 公钥证书（PKC， Public Key Certificate）

PKI的基本部件，由可信实体签名的电子记录，记录将公钥和密钥（公私钥对）所有者的身份捆绑在一起。

* 1. 证书作废列表（CRL，Certificate Revocation List）

证书作废列表通常由同一个可信发证实体签名。当公钥的所有者丢失私钥，或者改换名称时，需要将原有证书作废并更新证书作废列表。

* 1. 证书存档（Repository）

是存放公钥证书和作废证书列表的电子站点。

* 1. 认证机构（CA，Certificate Authority）

一个可信实体，发放和作废公钥证书，并对作废证书列表签名。

* 1. 注册机构（RA，Registration Authority）

一个可选PKI实体，与CA分开，不对数字证书或证书作废列表签名，而是负责记录和验证部分或所有有关信息（特别是主体的身份）的证书管理机构。

* 1. 署名用户（Subscriber）

作为主体署名证书并依据策略使用证书和密钥的实体。

* 1. 依赖方（Relying Party）

一个接收包括证书和签名信息的人或机构，利用证书提供的公钥验证其有效性，与持证人建立保密通信。依赖方与署名用户统称最终用户（End-User）。

* 1. 策略管理机构（PMA，Policy Management Authority）

监督证书策略的产生和更新，管理PKI证书策略。

* 1. **PKI的主要运行流程**

①署名用户向RA提出数字证书申请

②RA对署名用户进行身份确认

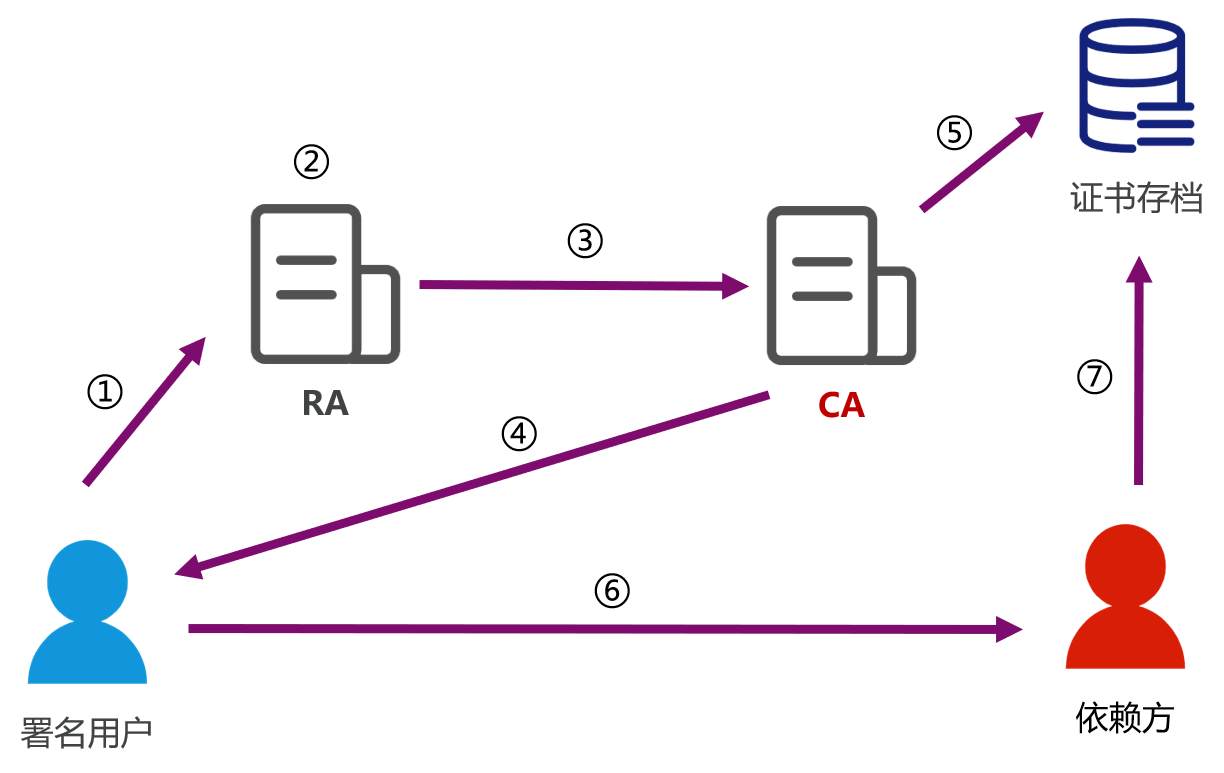
③RA向CA提出发行申请

④CA对署名用户发行证书

⑤CA在证书存档里公开发行的证书及作废列表

⑥署名用户和依赖方通信

⑦依赖方通过证书存档来检验证书的有效性，然后利用公钥来验证电子签名、进行数据加密等



* 1. **CA的职责**
* 接收证书申请请求
* 用自己的私钥签发证书
* 接收证书查询请求
* 接收证书作废请求
* 提供证书作废列表

1. **实验环境**

Ubuntu20.04操作系统 + OpenSSL 1.0.2

1. **实验内容**
   1. **搭建私有CA**
2. 创建私有CA所需要的文件目录，保存CA的相关信息

mkdir myCA //创建CA根文件夹

cd myCA //进入CA根文件夹

mkdir newcerts private conf //创建三个文件夹，用来存放新发放证书、私钥和配置文件

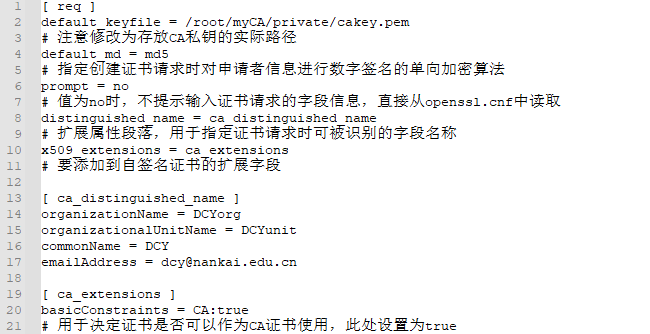
chmod g-rwx,o-rwx private //设置private文件夹的操作权限

touch index crlnumber //创建证书信息数据库、crl编号列表

echo 01 > serial //初始化证书的序列号

echo 01 > crlnumber //初始化吊销证书列表序号

1. 创建生成CA自签名证书的配置文件



1. 生成私有CA的私钥和自签名证书（根证书）

openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 2190 -config /root/myCA/conf/genca.conf

//生成x509的CA证书，过程中需要输入CA私钥的保护密码，请牢记。

//CA会按照gentestca.conf文件中配置的规则自签名生成证书

* 1. **私有CA为服务器签发证书**

1. 创建用来为其他请求签发证书的配置文件

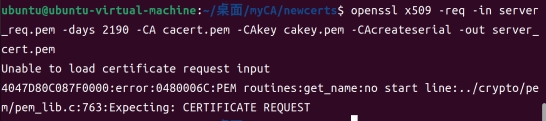


1. 模拟服务器，生成私钥与证书申请的请求文件

openssl req -newkey rsa:2048 -out server\_req.pem -outform PEM -days 2190 -config /home/ubuntu/桌面/myCA/conf/server.conf



与生成私有CA的私钥和自签名证书不同，这里的代码里没有 -x509 ，如果这里使用证书格式X.509的话，在后面生成证书时会报证书加载的error



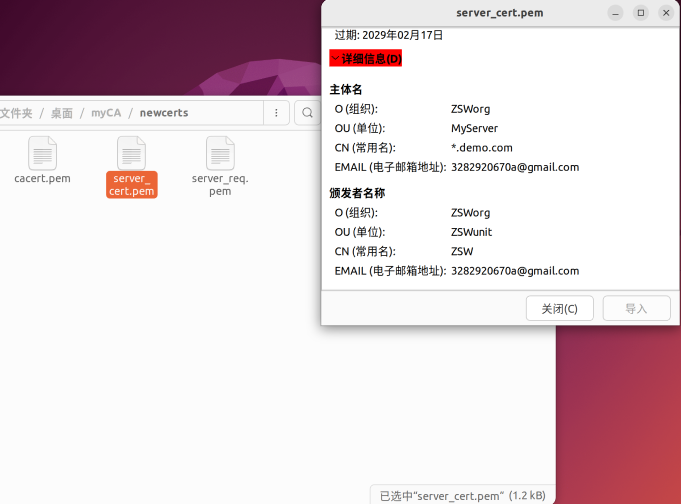
1. CA根据服务器的证书请求文件生成证书并将其返回给服务器

openssl x509 -req -in server\_req.pem -days 2190 -CA cacert.pem -CAkey /home/ubuntu/桌面/myCA/private/cakey.pem -CAcreateserial -out server\_cert.pem

用CA私钥cakey.pem为客户端的CSR文件server\_req.pem签名，并生成签名后的数字证书server\_cert.pem

  -x509: 专用于CA生成自签证书  
     -cakey: 生成请求时用到的私钥文件  
     -days n: 证书的有效期限  
     -out : 证书的保存路径

-CAcreateserial :分配序列号 01到签名证书，然后创建此序列号文件，其中包含下一个序列号 ( 02 )



* 1. **私有CA为客户端签发证书**

1. 创建用来为其他请求签发证书的配置文件



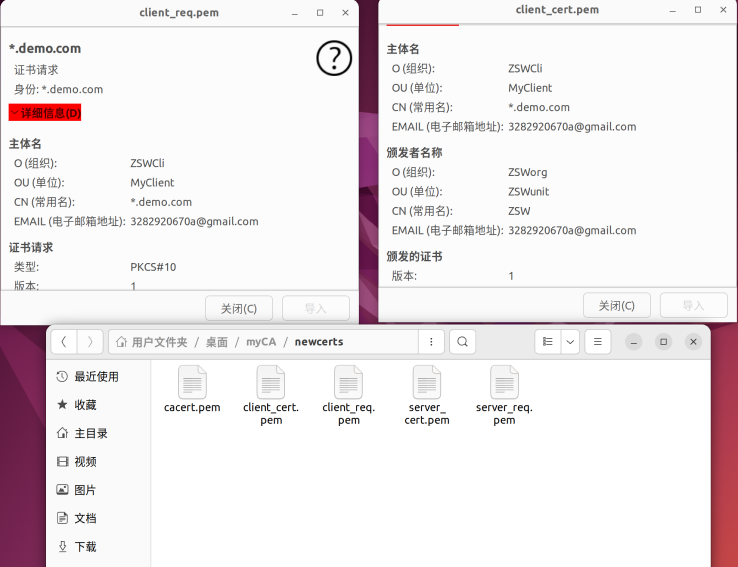
1. 模拟服务器，生成私钥与证书申请的请求文件

openssl req -newkey rsa:2048 -out client\_req.pem -outform PEM -days 2190 -config /home/ubuntu/桌面/myCA/conf/client.conf

1. CA根据服务器的证书请求文件生成证书并将其返回给服务器

openssl x509 -req -in client\_req.pem -days 2190 -CA cacert.pem -CAkey /home/ubuntu/桌面/myCA/private/cakey.pem -CAcreateserial -out client\_cert.pem

用CA私钥cakey.pem为客户端的CSR文件client\_req.pem签名，并生成签名后的数字证书client\_cert.pem



* 1. **CA吊销用户证书**

1. 找到证书对应的编号

openssl x509 -in client\_cert.pem -noout -serial -subject



1. 在存放证书的文件夹下找到编号对应的证书，对其完成吊销

openssl ca -revoke client\_cert.pem



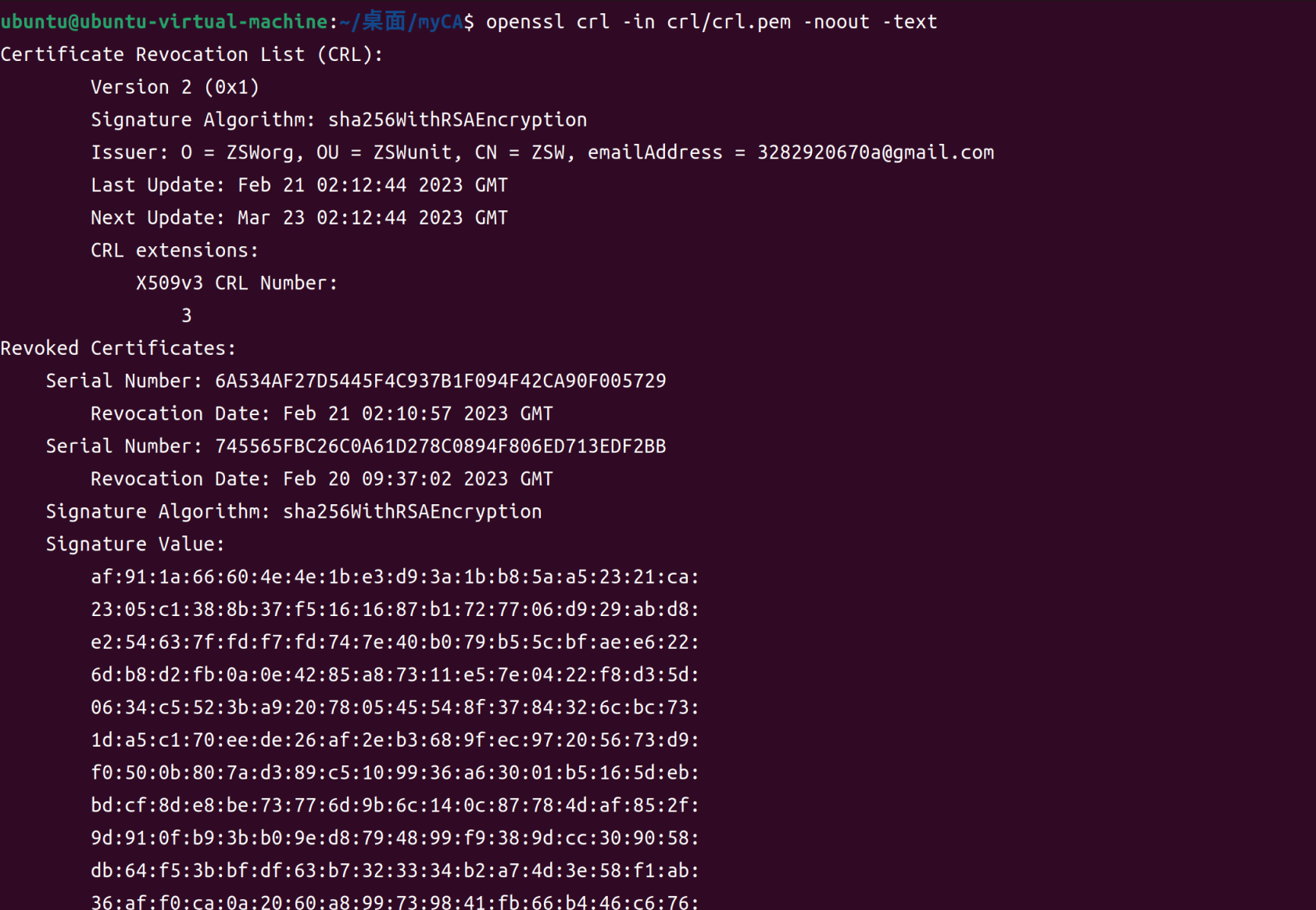
1. 更新吊销证书列表

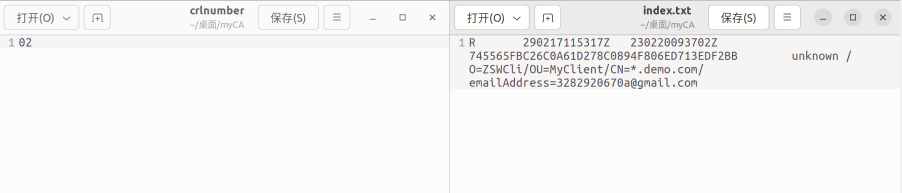
openssl ca -gencrl -out crl/crl.pem



查看吊销证书列表

openssl crl -in crl/crl.pem -noout -text





**思考：**

* CA如何验证证书的有效性？

用户A把自己的证书发送给用户B。用户B使用CA的公钥对证书的签名进行验证，由于只有CA才能生成该证书，因此只要证书验证正确，即说明证书是由CA发布的，证书中用户A的公钥是值得信赖的。用户B以后就可以使用该公钥验证用户A的签名或者进行和A进行加密通信。

* 需要考虑到哪些方面？

1. **实验总结**

**实现了PKI运行流程中的CA一些基本功能，搭建了一个私有CA，生成了密钥和根证书，模拟服务器和客户端向私有CA发送证书生成请求文件，并且生成证书，以及吊销证书，更新吊销证书列表的基本操作。主要学习了openssl的基本使用，一些基本指令的含义，CA的工作原理。**

**参考资料**

**1. <<OpenSSL CookBook>>** [**Ivan Ristić**](https://www.feistyduck.com/library/openssl-cookbook/)

**2.**  [openssl自签名ca证书,以及签发服务端/客户端证书\_bglmmz的博客-CSDN博客\_ca证书和客户端证书](https://blog.csdn.net/bglmmz/article/details/120968190)

**3.**  [使用OpenSSL自建CA及颁发证书、吊销证书\_miouqi的博客-CSDN博客\_openssl 删除证书](https://blog.csdn.net/miouqi/article/details/75268402)