**实验 私有CA证书签发的简单实现**

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

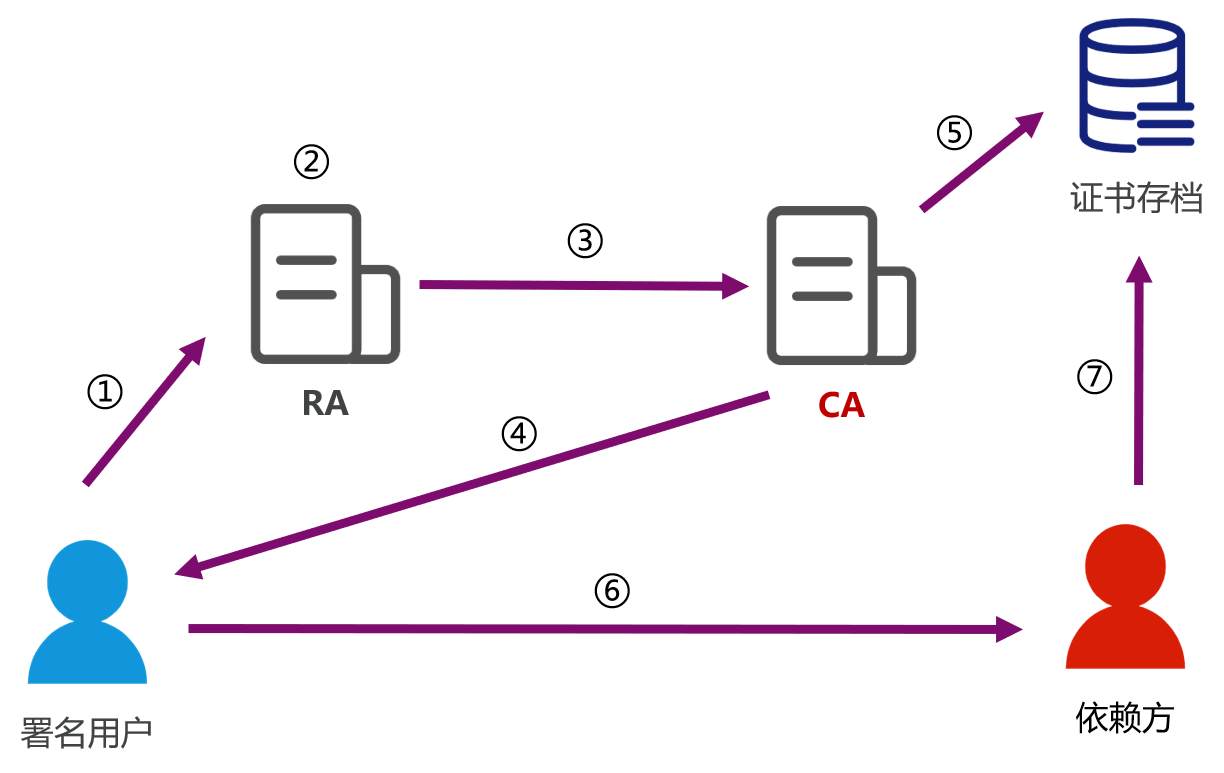
③RA向CA提出发行申请

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 1.1.1f

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 serial crlnumber //创建证书信息数据库、证书序号文件、crl序号文件

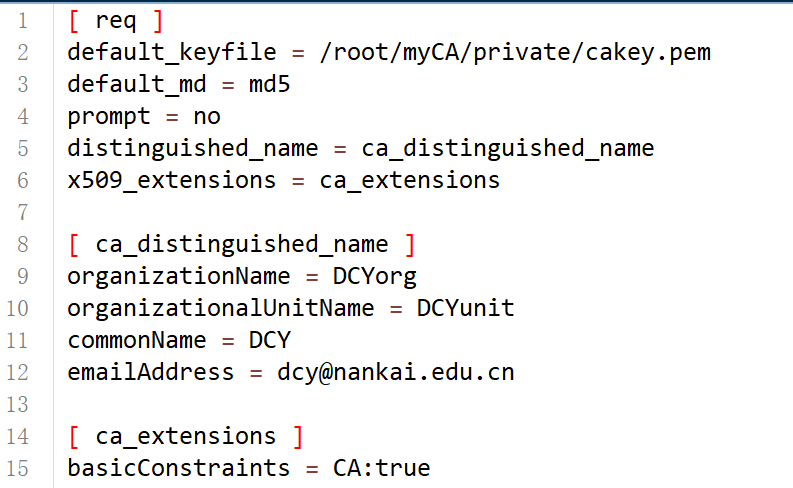
echo 01 > serial //初始化证书的序号

echo 01 > crlnumber //初始化吊销证书序号

1. 创建生成CA自签名证书的配置文件

cd conf //进入配置文件夹

vim genca.conf //创建用来生成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. 查看自签名证书

openssl x509 -in cacert.pem -text -noout //查看CA自签名证书

* 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

cd conf //再次进入配置文件夹

vim ca.conf //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

mkdir server

//在任意路径下创建服务器文件夹server

openssl req -newkey rsa:1024 -keyout server.key -out serverreq.pem -subj “/O=ServerCom/OU=ServerOU/CN=server”

//生成server的1024位私钥server.key和证书申请的请求文件serverre.pem，此时需要设置服务器的私钥保护密码，请牢记

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 ca -in serverreq.pem -out server.crt -config /root/myCA/conf/ca.conf

//向私有CA提交证书请求文件serverreq.pem，CA生成并返回证书server.crt

* 1. **私有CA为客户端签发证书**

……

* 1. **CA吊销用户证书**

1. 生成证书吊销列表（CRL）
2. 使用openssl ca指令完成用户证书吊销，将证书的序列号添加到CRL中
3. 更新并重新生成CRL

**思考：**

* CA如何验证证书的有效性？
* 需要考虑到哪些方面？

1. **实验报告**

**实验时间：**第1、2周

**报告内容：**

1. 要体现实验过程（截图）
2. 有对关键代码/指令的分析或比较详细的代码/指令注释
3. 实验心得总结

**提交方式：**通过雨课堂提交