介绍

CA(certification authority)，功能包括：证书发放、证书更新、证书撤销和证书验证

> 验签过程

1. 生成请求文件
2. CA核查申请者身份的真实性
3. CA使用根证书私钥加密请求文件（生成证书）
4. 把证书发放给申请者

术语

术语	解释
PKIX	Public Key Infrastructure for X.509 Certificates（公钥基础设施工作小组）
IETF	Internet Engineering Task Force（互联网工程任务组）
X.509	密码学里公钥证书的格式**标准**，应用在TLS/SSL在内的众多Internet协议里，还有非在线应用场景，如电子签名
PKCS	Public-Key Cryptography Standards，RSA实验室与其它安全厂商为了促进公钥密码发展而制定的一系列标准
PFX	公钥加密技术12号标准（Public Key Cryptography Standards #12，PKCS#12）,可包含公钥、私钥和证书，以二进制形式存储，通常包含密码保护，后缀名pfx/p12。
RCA	root certification authority（根证书颁发机构）
ICA	intermediate certification authority（中间证书颁发机构）

X.509文件编码

编码（也用于扩展名）	解释
.DER	Distinguished Encoding Rules。用于二进制编码的证书
.PEM	Privacy Enhanced Mail。用于ASCII编码(Base64)的各种X.509 v3证书。文件开始由一行"-----begin ..."开始。它是openssl默认的信息存放方式

X.509文件扩展名

扩展名	解释
.CRT	用于证书（只存放公钥），linux常用这种格式，证书可以是DER编码的，也可以是PEM编码的
.CER	用于证书（只存放公钥），微软系统用的格式，相同编码的时候可以安全的与CRT互相转换
.KEY	用于PCSK#8的公钥和私钥，可以是DER编的，也可以是PEM编码的。一般用来以PEM编码格式存储私钥
.pfx/.p12	微软用来存储公钥、私钥和证书制定的一个可移植格式，以二进制形式存储
.jks	Java Key Store，包含key文件和crt文件，应用在基于java的web如服务器如tomcat，weblogic
.csr	证书请求文件（certificate signing request），生成X.509证书之前，需要用户提交证书申请文件，再由CA机构签发证书

搭建CA认证

确认openssl已安装

```
rpm -qf `which openssl`
```

配置为CA认证中心

配置文件中还有ca存放的目录，私钥公钥文件名等一系列的配置

```
vim /etc/pki/tls/openssl.cnf
# 以前是false，改成true
basicConstraints=CA:TRUE
policy=policy_anything
```

创建一个CA密钥对

没有任何机构可以给根CA颁发证书，所以只能采用CA自己给自己颁发证书的方式，可以通过CA命令直接快速创建公钥和私钥。可以通过CA指令快速创建：

```
/etc/pki/tls/misc/CA -newca
```

```
#生产完的公钥
/etc/pki/CA/cacert.pem
#生成完的私钥
/etc/pki/CA/private/cakey.pem
```

也可以用openssl命令，手动创建证书：

```
#创建证书数据库列表文件
touch /etc/pki/CA/index.txt
# 指定第一个颁发证书的序列号
echo 'EBED18FAEA312048' > serial
#生成私钥文件(-des3表示用密码保护该私钥文件)
(umask 066;openssl genrsa -out /etc/pki/CA/private/cakey.pem -des3 2048)
#生成自签证书
openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -days 3650 -out
/etc/pki/CA/cacert.pem
```

创建二级CA

目前一般RCA只给ICA颁发证书，ICA才进行颁发服务器证书。如果本地为了方便，可以直接用RCA给服务器颁发证书，忽略此步骤

```
#创建证书数据库列表文件
touch /etc/pki/CA/index.txt
# 指定第一个颁发证书的序列号
echo 'ECED18FAEA311010' > serial
#生成私钥文件(-des3表示用密码保护该私钥文件)
(umask 066;openssl genrsa -out /etc/pki/CA/private/cakey.pem -des3 2048)
#申请者根据私钥创建csr
openssl req -new -key /etc/pki/CA/private/cakey.pem -out /etc/pki/CA/ica.csr
#rca给ica签发证书
openssl ca -in /etc/pki/CA/csr/ica.csr -out /etc/pki/CA/certs/ica.pem -days 3650
#ica机器上重命名
mv ica.pem cacert.pem
```

CA颁发证书

申请者创建证书申请文件

```
#申请者创建私钥
(umask 066;openssl genrsa -out /etc/pki/tls/private/app.key 2048)
```

```
#申请者根据私钥创建csr
openssl req -new -key /etc/pki/tls/private/app.key -out /etc/pki/tls/app.csr
```

CA机构创建domain.ext

需要指定extfile，subjectAltName指定可以使用的域名，如果有多个域名可以继续往后面加DNS.2=。泛域名证书格式为：*.xxx.com

```
# vim domain.ext
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName=@SubjectAlternativeName
[ SubjectAlternativeName ]
DNS.1=apps-uat3.cimbbank.com.ph
```

CA机构签发证书

```
#将证书申请文件发送给ca机构后，ca机构在他们的机器上签发证书
openssl ca -in /etc/pki/CA/app.csr -out /etc/pki/CA/certs/app.crt -days 3650 -extfile domain.txt
#crt转pem
openssl x509 -in apps-uat3.crt -out apps-uat3-pubkey.pem
#cer转crt
openssl x509 -inform PEM -in apps-uat3.cer -out apps-uat3.crt
```

制作证书链

一般来说，根证书颁发机构（RCA）不会直接颁发服务器证书（SC），它只负责给中间证书颁发机构(ICA)颁发证书，ICA再颁发服务器证书。但是目前操作系统一般只存放了RCA的根证书，没有ICA的证书。因此，在拿到签发后的证书后，一般需要自己制作证书链，把ICA的证书包含进来

```
-----BEGIN CERTIFICATE-----
server的证书
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ica的证书
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
自己搭建的CA，把root CA证书也放进来
-----END CERTIFICATE-----
```

证书越靠上级的放越后面，自己签发的证书为了保证证书链完整性，最好把RCA的证书也丢到证书链的最后面

服务端配置

服务端需要用到自己的私钥文件、CA签发的证书文件(crt)。

nginx

```
server {
  listen       443 ssl;
  ssl_certificate /etc/nginx/conf.d/ssl/cimbbank.com.ph.crt;
  ssl_certificate_key /etc/nginx/conf.d/ssl/cimbbank.com.ph.key;
  ssl_session_timeout 5m;
  ssl_protocols SSLv2 SSLv3 TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers HIGH:!aNULL:!MD5:!EXPORT56:!EXP;
  ssl_prefer_server_ciphers on;
}
```

客户端

浏览器

浏览器访问网站前，需要将CA认证中心的公钥导入到受信任的根证书颁发机构后，它签发的所有证书就会被浏览器信任。windows电脑上，需要将之前CA机器上生成的cacert.pem，重命名为cacert.crt文件，双击后，根据向导选择导入至受信任的根证书颁发机构。

linux服务器

方法一

```
#将ca公钥文件追加到ca-bundle.crt
cat cacert.pem >> /etc/pki/tls/certs/ca-bundle.crt
```

方法二

```
yum install -y ca-certificates
#2.将公钥cacert.pem文件拷贝至这个目录
cp cacert.pem /etc/pki/ca-trust/source/anchors/
#3.更新cacert
```

```
update-ca-trust
```

附录

常用指令

```
#linux查看某个网站的证书，bengin end的部分
openssl s_client -showcerts -connect apps-uat3.cimbbank.com.ph:443
#查看证书的内容
openssl x509 -in cimbbank.com.ph.crt -noout -text
#cer crt互转，默认-inform -outform是PEM编码格式，如果是DER格式，则需要指定
openssl x509 -inform PEM -in apps-uat3.cer -out apps-uat3.crt
#key转pem，个人感觉没必要转，直接改后缀就好。ng要求的key就是pem编码格式
openssl rsa -in cimbbank.com.ph.key -out cimbbank.com.ph.pem
```

更多证书类型转换，可以参考：https://www.chinassl.net/ssltools/convert-ssl-commands.html