一、生成自签名证书

1.生成私钥(.key)

```
openssl genrsa -out ca.key 2048
```

2.基于私钥（.key）创建证书签名请求（.csr）

```
openssl req -new -key ca.key -out ca.csr -subj
"/C=CN/ST=shanghai/L=shanghai/O=example/OU=it/CN=domain1/CN=domain2"
```

具体各参数说明：

C-----国家（Country Name）
ST----省份（State or Province Name）
L----城市（Locality Name）
O----公司（Organization Name）
OU----部门（Organizational Unit Name）
CN----产品名（Common Name）
emailAddress----邮箱（Email Address）

3.使用自己的私钥（.key）签署自己的证书签名请求（.csr），生成自签名证书（.crt）

```
openssl x509 -req -in ca.csr -out ca.crt -signkey ca.key -days 1
```

> 对于这条命令，要注意以下几点：
>
> 1. 这个命令是`openssl x509`，`-req`是参数，和前面生成证书签名请求的`openssl req`命令不同。
> 2. `-signkey my.key`配置清晰地表明使用自己的私钥进行签名。

二、生成私有CA签发的证书

> 与生成自签名证书不同地方在于，生成自签名证书场景下只有一个参与方，请求证书和签发证书都是自己，而生成私有CA证书的场景里开始涉及两个角色了：
>
> 签发证书的一方：CA（主要牵涉的是CA私钥和根证书）
> 请求签发证书的一方：如服务器
> 为了变于区别，我们把它相关的文件分别用ca和server加以区别

1.生成Server端私钥（server.key）和证书签名请求（server.csr）

```
openssl genrsa -out server.key 2048
```

```
openssl req -new -key server.key -out server.csr -subj
"/C=CN/ST=shanghai/L=shanghai/O=example/OU=it/CN=domain3/CN=domain4"
```

2.使用CA证书（ca.crt）与密钥（ca.key）签署服务器的证书签名请求（server.csr），生成私有CA签名的服务器证书（server.crt）

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 1
```

3.验证server.crt是否真得是由ca签发的：

```
openssl verify -CAfile ca.crt server.crt
```

出现“OK”则表示验证成功。

备注：证书核验出错: error 18 at 0 depth lookup:self signed certificate
检查客户端、服务端证书是否可用的时候提示这个报错
注意 服务端证书、客户端证书、根证书， 三者的CN(Common Name)**不可以一样**，否则会有这个报错。

三、搭建C-S模型验证证书的方法：

1.证书生成

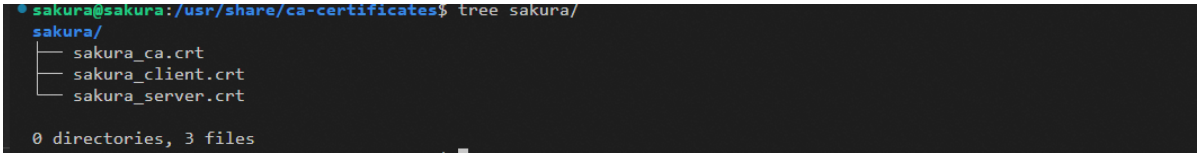
```
### 生成自签名证书
openssl genrsa -out ca.key 2048
openssl req -new -key ca.key -out ca.csr -subj "/C=CN/ST=shanghai/L=shanghai/O=example/OU=it/CN=domain1/CN=domain2"
openssl x509 -req -in ca.csr -out ca.crt -signkey ca.key -days 7

### 生成私有CA签发的证书（server）
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr -subj "/C=CN/ST=shanghai/L=shanghai/O=example/OU=it/CN=domain3/CN=domain4"
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 7

### 生成私有CA签发的证书（client）
openssl genrsa -out client.key 2048
openssl req -new -key client.key -out client.csr -subj "/C=CN/ST=shanghai/L=shanghai/O=example/OU=it/CN=domain3/CN=domain4"
openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -days 7
```

四、安装证书

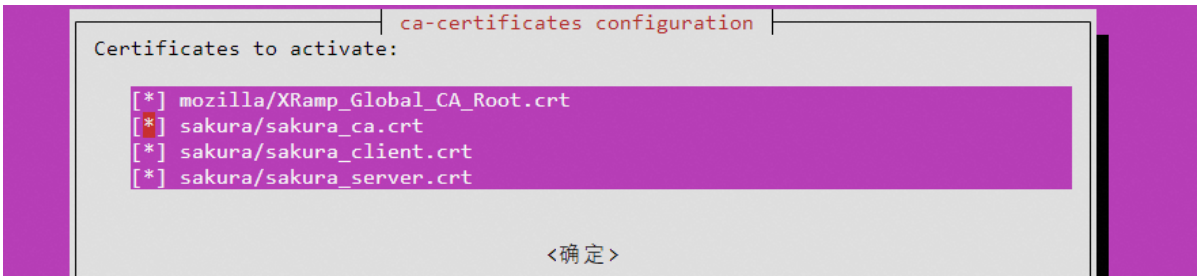
1.将证书拷贝到/usr/share/ca-certificates/目录下



2.安装证书

```
sudo dpkg-reconfigure ca-certificates
```

> 在弹出的界面内按空格选择需要安装的证书，之后回车进行安装即可。




```
sakura@sakura:/usr/share/ca-certificates$ sudo dpkg-reconfigure ca-certificates
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
正在处理用于 ca-certificates (20211016~20.04.1) 的触发器 ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...

done.
done.
```

3.查看已安装的证书

```
sakura@sakura:/etc/ssl/certs$ ls -hl sakura_*
lrwxrwxrwx 1 root root 47 Apr 20 14:58 sakura_ca.pem -> /usr/share/ca-certificates/sakura/sakura_ca.crt
lrwxrwxrwx 1 root root 51 Apr 20 14:58 sakura_client.pem -> /usr/share/ca-certificates/sakura/sakura_client.crt
lrwxrwxrwx 1 root root 51 Apr 20 14:58 sakura_server.pem -> /usr/share/ca-certificates/sakura/sakura_server.crt
```