[openssl建立多级CA签发证书](http://blog.chinaunix.net/uid-20553497-id-3163297.html)

平时我们自己签发CA证书再签发服务器证书的场景其实都非常简单。浏览器把自签CA导入后，就可以信任由这个CA直接签发的服务器证书。  
  
    但是实际上网站使用的证书肯定都不是由根CA直接签发的，比如  
[](http://blog.chinaunix.net/attachment/201204/6/20553497_1333693513CImM.png)   
  
淘宝登陆服务器使用的证书。  
  
我之前是自己写了脚本由自签CA直接签发服务器证书，为了真清楚的理解一下证书链的作用就直接使用openssl先签发2层的子CA，再由子CA去签发服务器证书。  
手动签发证书的脚本如下：  
生成自签CA

**点击(此处)折叠或打开**

1. # cat makerootca.sh
2. #!/bin/bash
3. DIR=/root/ssl.test2
4. mkdir -p $DIR/demoCA/{private,newcerts}
5. touch $DIR/demoCA/index.txt
6. echo 01 > $DIR/demoCA/serial
7. openssl genrsa -des3 -out $DIR/demoCA/private/cakey.pem 2048
8. openssl req -new -x509 -days 3650 -key $DIR/demoCA/private/cakey.pem -out $DIR/demoCA/careq.pem

签发二级CA的脚本

**点击(此处)折叠或打开**

1. # cat no2domain.sh
2. #!/bin/bash
3. NAME=$1
4. DIR=$(pwd)/autoget
5. openssl genrsa -des3 -out $DIR/$NAME.key 2048
6. openssl rsa -in $DIR/$NAME.key -out $DIR/$NAME.key
7. openssl req -new -days 3650 -key $DIR/$NAME.key -out $DIR/$NAME.csr
8. openssl ca -extensions v3\_ca -in $DIR/$NAME.csr -config ./openssl.cnf -days 3000 -out $DIR/$NAME.crt -cert $DIR/../demoCA/careq.pem -keyfile $DIR/../demoCA/private/cakey.pem

    sh no2domain.sh  no2

签发三级CA的脚本

**点击(此处)折叠或打开**

1. # cat no3domain.sh
2. #!/bin/bash
3. [ $# -ne 1 ] && echo "$0 NAME" && exit
4. NAME=$1
5. DIR=$(pwd)/autoget
6. openssl genrsa -des3 -out $DIR/$NAME.key 2048
7. openssl rsa -in $DIR/$NAME.key -out $DIR/$NAME.key
8. openssl req -new -days 3650 -key $DIR/$NAME.key -out $DIR/$NAME.csr
9. openssl ca -in $DIR/$NAME.csr -extensions v3\_ca -config ./openssl.cnf -days 3000 -out $DIR/$NAME.crt -cert $DIR/no2.crt -keyfile $DIR/no2.key

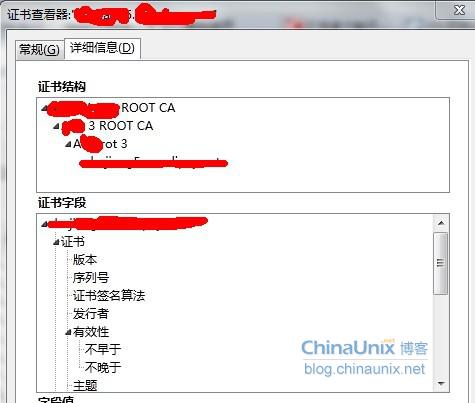
       sh no3domain.sh  no3

由三级CA签发服务器证书的脚本

**点击(此处)折叠或打开**

1. # cat no4domain.sh
2. #!/bin/bash
3. [ $# -ne 1 ] && echo "$0 NAME" && exit
4. NAME=$1
5. DIR=$(pwd)/autoget
6. openssl genrsa -des3 -out $DIR/$NAME.key 2048
7. openssl rsa -in $DIR/$NAME.key -out $DIR/$NAME.key
8. openssl req -new -days 3650 -key $DIR/$NAME.key -out $DIR/$NAME.csr
9. openssl ca -in $DIR/$NAME.csr -config ./openssl.cnf -days 3000 -out $DIR/$NAME.crt -cert $DIR/no3.crt -keyfile $DIR/no3.key

     sh no4domain.sh my.domain.net

当我们把使用三级CA签发的服务器证书配置在nginx 上时，在已经导入根CA的浏览器上肯定是会遇到证书报警的，然后依次把三级CA(no3.crt  )和二级CA(no2.crt)追加到服务器证书后面，浏览器ssl链接成功，点击证书查看如下图：  
[](http://blog.chinaunix.net/attachment/201204/6/20553497_1333694049g3W3.jpg)  
  
  
  
  
  
  
http://blog.chinaunix.net/uid-20553497-id-3163297.html