

<b>README .....</b>	<b>1</b>
一. 前言: .....	1
二. 脚本说明 .....	1
1. gen_ca.sh .....	1
2. newcert.sh.....	3
3. revoke.sh.....	3
三. 注意事项 .....	4
四. 使用示例 .....	4
1. 创建工作目录/CA/IntCA.....	4
2. 生成用户证书 .....	6
3. 生成服务器证书.....	8
4. 吊销证书 .....	9

# README

## 一. 前言：

一直以来断断续续地研究证书和其配置管理机制，但是由于使用不多，虽然也写过一些文档，总是忘记地比较快。最近因有朋友沟通中提到需要使用证书做 SSLVPN 认证，再次翻出原来的文档，发现每次都手动去敲太过繁琐，效率也太低了。所以折腾了几天，做了这几个脚本。

通过这几个脚本，可以实现证书工作目录地生成/新证书（服务器/用户）签发以及证书吊销操作。

脚本使用 OpenSSL 实现。使用脚本前，建议提前了解下 openssl 的知识。CSDN 上面有相关的信息。

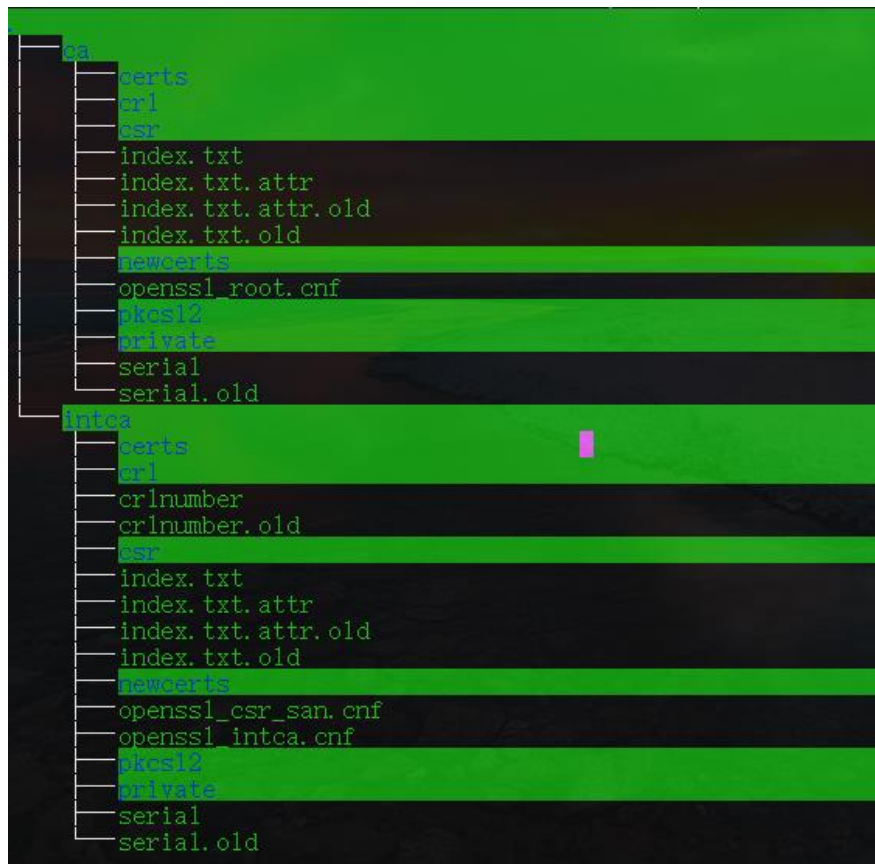
## 二. 脚本说明

脚本主要分为三个部分

### 1. gen\_ca.sh

用于生成证书工作目录，并按照 cnf 配置文件中的配置，创建 CA 和中间证书。

## 1.1 生成的工作目录如下：



## 1.2 cnf 配置文件

配置文件内容在下面的代码块，可以按照使用需求自行修改（实际上 default 参数只是在证书生成的时候帮你自动填写上回车即可使用，使用过程中细心点，可以发现是能够手动修改的。）：

```
18  + cat << \EOF > $workdir/root/ca/openssl_root.cnf
150
151  + cat << \EOF > $workdir/root/intca/openssl_intca.cnf
285
```

**Default Subject 配置如下：**

openssl\_root.cnf（运行 gen\_ca.sh 会用到，该配置影响 CA 和 IntermediateCA）

```
95 # Optionally, specify some defaults.
96 countryName_default           = CN
97 stateOrProvinceName_default  = JiangSu
98 localityName_default         = SuZhou
99 0.organizationName_default    = Personal
100 organizationalUnitName_default = IT
101 #emailAddress_default         = [your email address]
```

openssl\_intca.cnf（该配置会影响后面的用户证书和服务器证书）

```
230 # Optionally, specify some defaults.
231 countryName_default           = CN
232 stateOrProvinceName_default  = JiangSu
233 localityName_default         = SuZhou
234 0.organizationName_default    = Personal
235 organizationalUnitName_default = IT
236 #emailAddress_default         = [Your email address]
```

## 2. newcert.sh

用于生成用户和服务器证书，其中在生成用户证书的时候，会同时生成 pkcs12 格式的证书文件（包含密钥）。

生成用户证书的时候，Subject 和 CN 为用户名，其他按照默认。

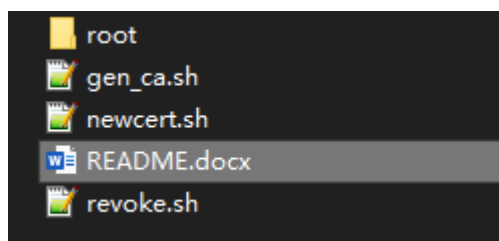
生成服务器证书的时候，可以按照提示，输入多个 SAN（Subject Alternative Name）。建议使用 FQDN 名称，可使用通配符，也可以使用 IP。

## 3. revoke.sh

用于证书的吊销，按照提示输入证书 CN 即可。

### 三. 注意事项

脚本为配套使用，所有脚本需要和 root 目录同级。



运行时，路径需要和和 root 同级。

```
chan@LPX260:/mnt/c/工具/CertificateAuthority$ ls
README.docx  gen_ca.sh  newcert.sh  revoke.sh  root
```

### 四. 使用示例

#### 1. 创建工作目录/CA/IntCA

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ ls
gen_ca.sh  newcert.sh  revoke.sh
```

使用 root 权限运行 gen\_ca.sh

输入 CA 私钥密码(3 遍)

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ sudo bash gen_ca.sh
[sudo] password for chan:
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
++++
.....
e is 65537 (0x010001)
Enter pass phrase for /mnt/c/Users/chan/Desktop/dir/root/ca/private/ca.root.key.pem:
Verifying - Enter pass phrase for /mnt/c/Users/chan/Desktop/dir/root/ca/private/ca.root.key.pem:
Enter pass phrase for /mnt/c/Users/chan/Desktop/dir/root/ca/private/ca.root.key.pem:
```

确认证书 Subject, 这里会默认填入 openssl\_root.cnf 里面的 defaults。

可以手动修改。

```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name [JiangSu]:
Locality Name [SuZhou]:
Organization Name [Personal]:
Organizational Unit Name [IT]:
Common Name []:CA
Email Address []:

```

输入 IntermediateCA 的私钥密码

```

Generating a RSA private key
.....
writing new private key to '/mnt/c/Users/chan/Desktop/dir/root/intca/private/ca.intca.key.pem'
Enter PEM pass phrase: 输入 IntermediateCA 的私钥密码
Verifying - Enter PEM pass phrase:

```

输入 Intermediate CA 的 Subject 信息

```

-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name [JiangSu]:
Locality Name [SuZhou]:
Organization Name [Personal]:
Organizational Unit Name [IT]:
Common Name []:Intermediate CA
Email Address []:

```

输入 CA 私钥的密码

```

Using configuration from /mnt/c/Users/chan/Desktop/dir/root/ca/openssl1_root.cnf
Enter pass phrase for root/ca/private/ca.root.key.pem:

```

两次 y 确认使用 CA 签发中间证书 IntmediateCA

```

Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: Feb  9 03:55:05 2020 GMT
    Not After : Feb  6 03:55:05 2030 GMT
  Subject:
    countryName           = CN
    stateOrProvinceName   = JiangSu
    organizationName       = Personal
    organizationalUnitName = IT
    commonName             = Intermediate CA
  X509v3 extensions:
    X509v3 Subject Key Identifier:
      ED:5D:D8:31:B8:9A:3E:5C:9B:FA:FE:3B:E3:94:04:5C:F9:4D:0B:39
    X509v3 Authority Key Identifier:
      keyid:17:80:F5:07:54:BC:60:5D:96:AB:AA:4B:FA:5D:C0:FA:BF:B7:1B:1E

    X509v3 Basic Constraints: critical
      CA:TRUE, pathlen:0
    X509v3 Key Usage: critical
      Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Feb  6 03:55:05 2030 GMT (3650 days)
Sign the certificate? [y/n]:

```

提示成功

```

Write out database with 1 new entries
Data Base Updated

```

查看目录

```

chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ ls root/ca/certs/
ca.root.crt.pem
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ ls root/intca/certs/
ca.chain.crt.pem  ca.intca.crt.pem

```

## 2. 生成用户证书

bash newcert.sh

```

chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ bash newcert.sh
#####
原则上不需要修改Subject C/O/L等参数，只需要提供CN即可
#####
如果是服务器使用，CN和DNS按照FQDN方式输入，DNS可使用通配符
#####
如果是用户使用，CN按照用户名String方式输入
#####
需要生成用户证书还是服务器证书？[1:用户 2:服务器]:1
#####
现在，我们将生成用户证书
#####
请输入CN用户名:chan_

```

CN 输入用户名，其他默认



```
#####
Step1. 创建用户私钥文件并生成CSR
#####
Generating a RSA private key
..+++++
.....+++++
writing new private key to '/mnt/c/Users/chan/Desktop/dir/root/intca/private/chan.key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [JiangSu]:
Locality Name (eg, city) [SuZhou]:
Organization Name (eg, company) []:
Common Name (e.g. server FQDN or YOUR name) []:chan_
```

使用 IntCA 签发用户证书，输入 IntCA 的私钥密码

```
#####
Step2. 使用中间证书签发用户CSR
#####
Using configuration from /mnt/c/Users/chan/Desktop/dir/root/intca/openssl_intca.cnf
Enter pass phrase for root/intca/private/ca.intca.key.pem: _
```

确认证书信息，按 2 次 y

```
Certificate is to be certified until Feb  8 04:00:25 2021 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
#####
```

最后会导出 pkcs12 格式的证书，输入导出密码用于保护证书和私钥

```
Data Base Updated
#####
Step3. 生成PKCS12格式证书文件
#####
Enter Export Password:
Verifying - Enter Export Password:
#####
Step4. 清除配置中的临时信息
#####
证书在目录/mnt/c/Users/chan/Desktop/dir/root/intca/certs/chan.crt.pem
#####
私钥在目录/mnt/c/Users/chan/Desktop/dir/root/intca/private/chan.key.pem
#####
PKCS12格式证书在目录/mnt/c/Users/chan/Desktop/dir/root/intca/pkcs12/chan.p12
```

查看生成的证书



```

chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ tree root/intca/pkcs12/
root/intca/pkcs12/
├── chan.p12
└── chan.txt

0 directories, 2 files
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ tree root/intca/certs/
root/intca/certs/
├── ca.chain.crt.pem
├── ca.intca.crt.pem
└── chan.crt.pem

```

### 3. 生成服务器证书

bash newcert.sh

这里我们演示 SAN 里面输入了两个域名:chan.name.local 和 \*.name.local。那么服务器通过匹配域名或者通配符域名的 URL 访问时,就不会报错(尤其是开启了 HSTS 的服务器)。

```

#####
需要生成用户证书还是服务器证书? [1:用户|2:服务器]:2
#####
现在我们将生成服务器证书
#####
请输入服务器FQDN(建议)或IP地址:chan.name.local
#####
接下来请留意是否需要为服务器证书添加可选名称(域名/IP/通配符)
#####
是否需要添加可选DNS名称? [Y/N]:y
请输入证书可选DNS名称:*.name.local
#####
是否需要添加可选DNS名称? [Y/N]:n
#####

```

同样的,输入 Subject 里面的 CN,生成 CSR

```

-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [JiangSu]:
Locality Name (eg, city) [SuZhou]:
Organization Name (eg, company) []:
Common Name (e.g. server FQDN or YOUR name) [chan.name.local]:
-----

```

输入 IntCA 私钥的密码，签发证书

```
#####
Stap2. 使用中间证书签发服务器CSR
#####
Using configuration from /mnt/c/Users/chan/Desktop/dir/root/intca/openssl_intca.cnf
Enter pass phrase for root/intca/private/ca.intca.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
```

生成完毕，按照提示找到对应目录

```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
#####
清理配置文件中的临时信息
#####
证书在目录:/mnt/c/Users/chan/Desktop/dir/root/intca/certs/chan.name.local.crt.pem
#####
私钥在目录:/mnt/c/Users/chan/Desktop/dir/root/intca/private/chan.name.local.key.pem
#####
```

查看证书

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ tree root/intca/certs/
root/intca/certs/
├── ca.chain.crt.pem
├── ca.intca.crt.pem
├── chan.crt.pem
└── chan.name.local.crt.pem
```

## 4. 吊销证书

上面服务器证书签发错误或者丢失了，我们可以吊销证书

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ bash revoke.sh
#####
目前脚本每次只能吊销一个证书
#####
请输入需要吊销的证书CN名称[证书默认都在intca/certs目录下]:chan.name.local
#####
crlnumber文件不存在，创建文件
#####
serial=1025 subject=C = CN, ST = JiangSu, L = SuZhou, CN = chan.name.local
请再次确认证书信息是否无误[Y:确认 N:取消]y
```

根据显示的证书信息，确认吊销证书无误

输入 IntCA 私钥密码，确认吊销

```
#####
吊销证书1025
Using configuration from /mnt/c/Users/chan/Desktop/dir/root/intca/openssl_intca.cnf
Enter pass phrase for root/intca/private/ca.intca.key.pem: _
```

再次输入 IntCA 私钥密码，更新 CRL 列表

查看吊销列表或者 index

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

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ openssl crl -in root/intca/crl/crl.pem -noout -text
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha512WithRSAEncryption
  Issuer: C = CN, ST = JiangSu, O = Personal, OU = IT, CN = Intermediate CA
  Last Update: Feb  9 04:11:36 2020 GMT
  Next Update: Mar 10 04:11:36 2020 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:F3:DB:E4:44:76:C9:9C:F9:6F:4B:73:3B:DE:52:B9:AC:5C:E8:17:BC

    X509v3 CRL Number:
      1
  Revoked Certificates:
    Serial Number: 1025
    Revocation Date: Feb  9 04:11:33 2020 GMT
```

cat root/intca/index.txt,前面带有 R 字样，说明已经吊销

```
chan@LPX260:/mnt/c/Users/chan/Desktop/dir$ cat root/intca/index.txt
V      210208040025Z      1024      unknown /C=CN/ST=JiangSu/L=SuZhou/CN=chan
R      210208040731Z      200209041133Z      1025      unknown /C=CN/ST=JiangSu/L=SuZhou/CN=chan.name.local
```

吊销列表 crl.pem 可以通过脚本或者其他形式定期更新到用户设备上。

注意，如果 crl 不更新到设备，设备还是会认为原有证书是可信。