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。

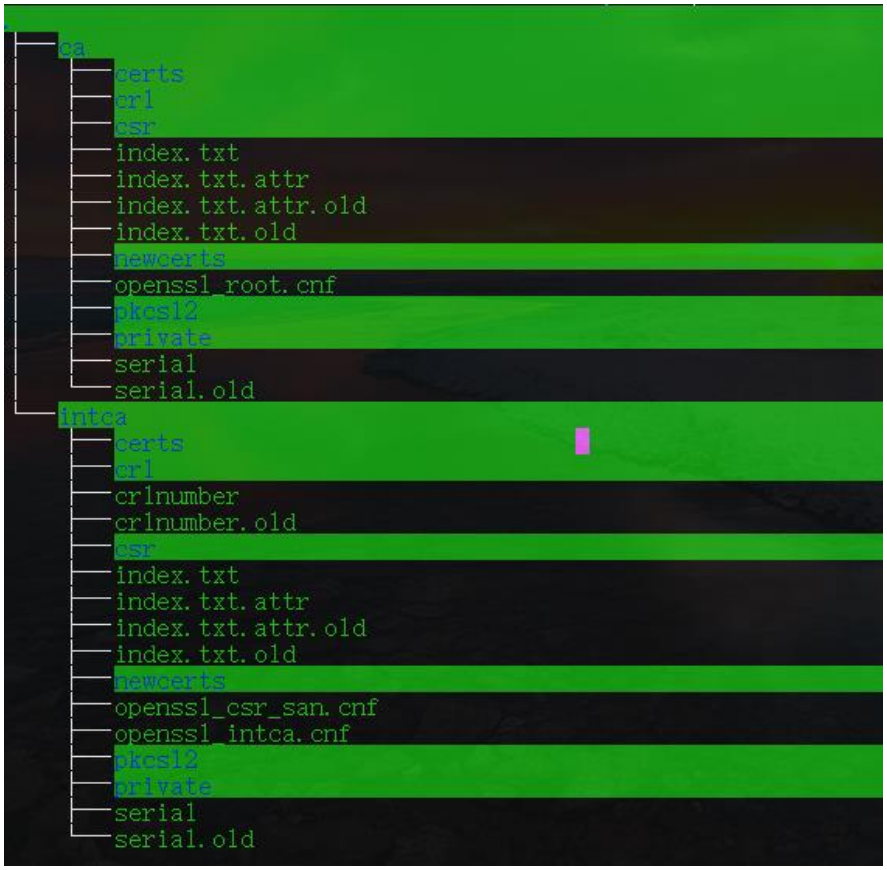
二. 脚本说明

脚本主要分为三个部分

1. gen_ca.sh

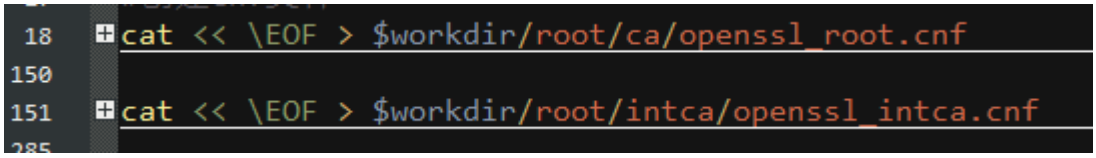
用于生成证书工作目录，并按照 cnf 配置文件中的配置，创建 CA 和中间证书。

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。）：



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。

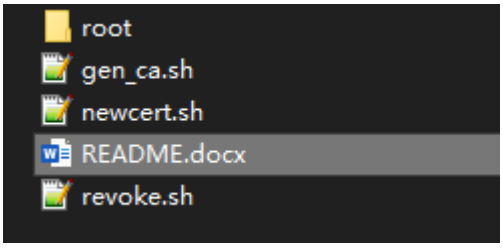
生成服务器证书的时候，可以按照提示，输入多个 SAN（Subject Alternative Name）。建议使用 FQDN 名称，可使用通配符，也可以使用 IP。

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

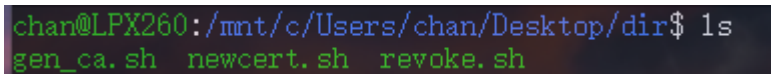
脚本为配套使用，所有脚本需要和 root 目录同级。



运行时，路径需要和和 root 同级。

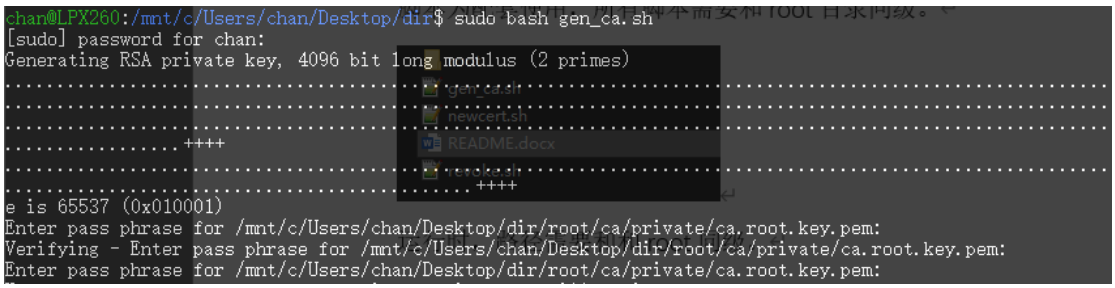
四. 使用示例

1. 创建工作目录/CA/IntCA

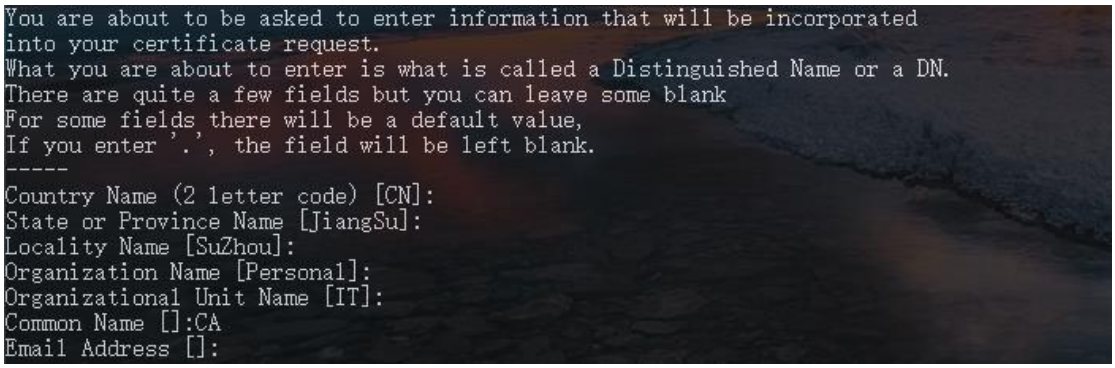


使用 root 权限运行 gen_ca.sh

输入 CA 私钥密码(3 遍)

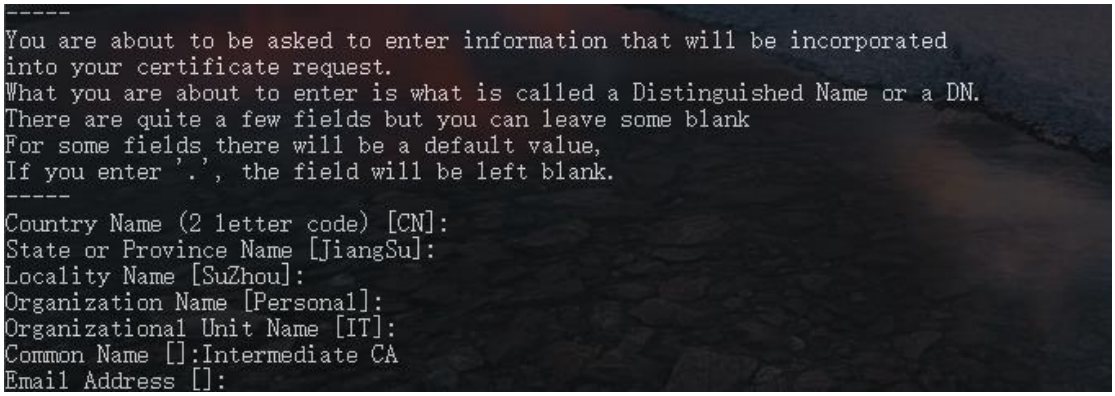


确认证书 Subject，这里会默认填入 openssl_root.cnf 里面的 defaults。可以手动修改。

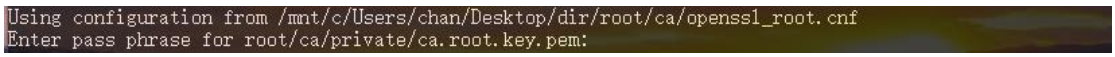


输入 IntermediateCA 的私钥密码

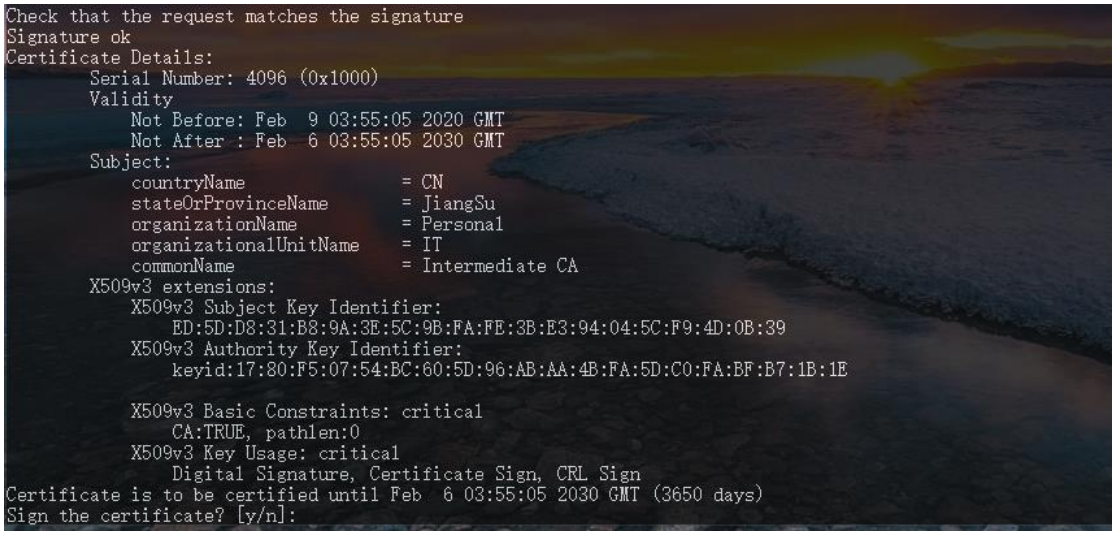
输入 Intermediate CA 的 Subject 信息



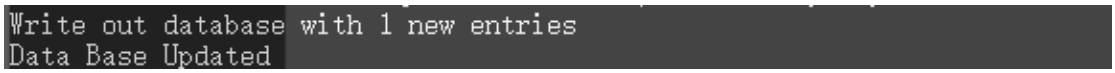
输入 CA 私钥的密码



两次 y 确认使用 CA 签发中间证书 IntmediateCA



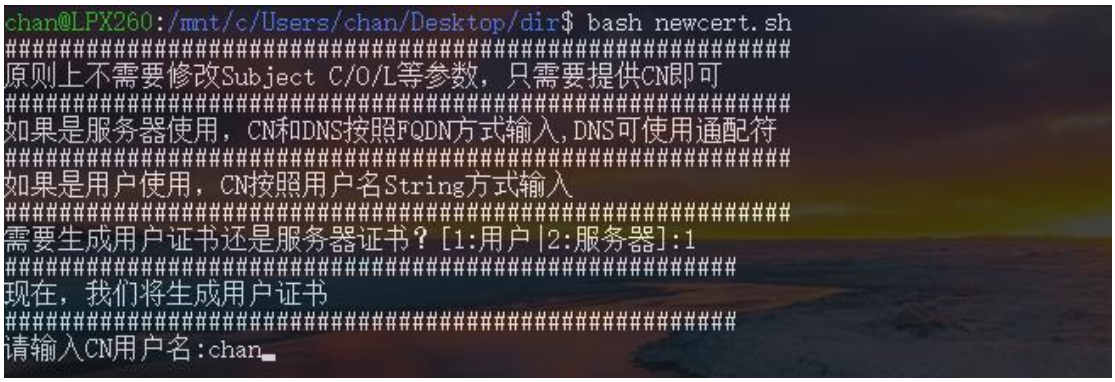
提示成功



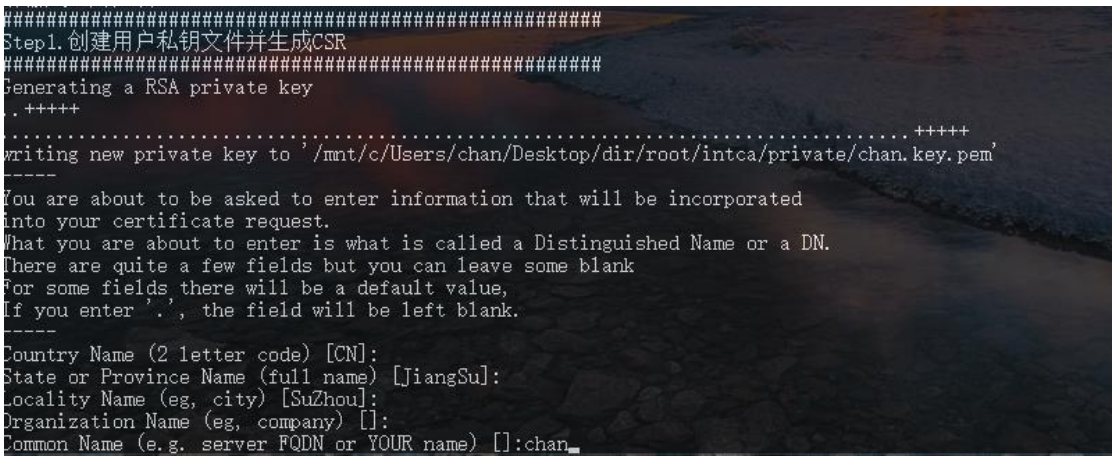
查看目录

2. 生成用户证书

bash newcert.sh

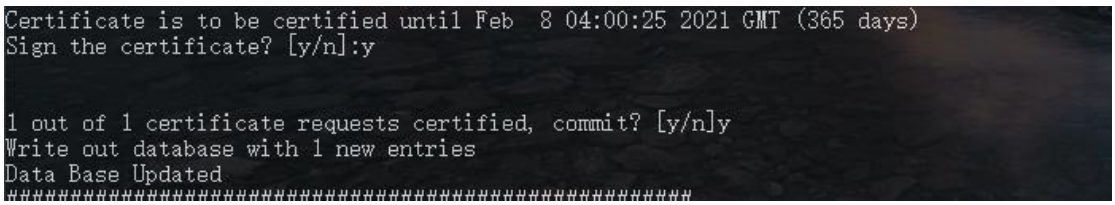


CN 输入用户名，其他默认

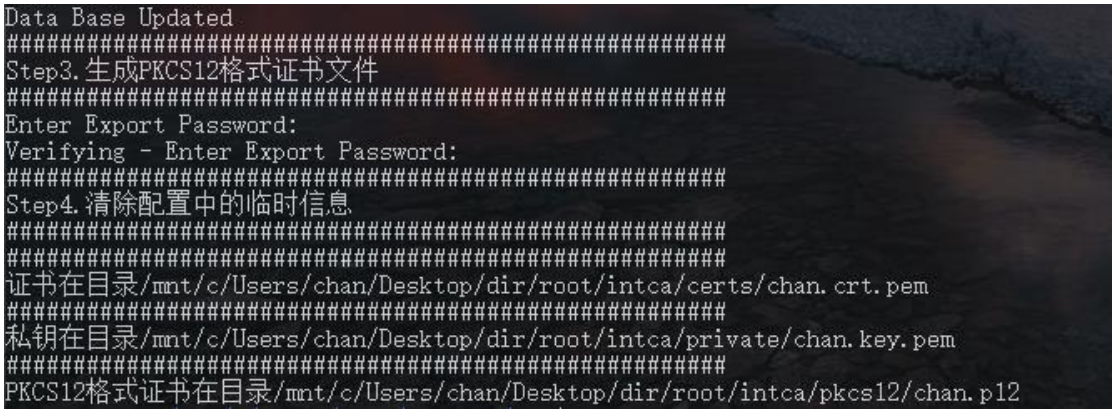


使用 IntCA 签发用户证书，输入 IntCA 的私钥密码

确认证书信息，按 2 次 y



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



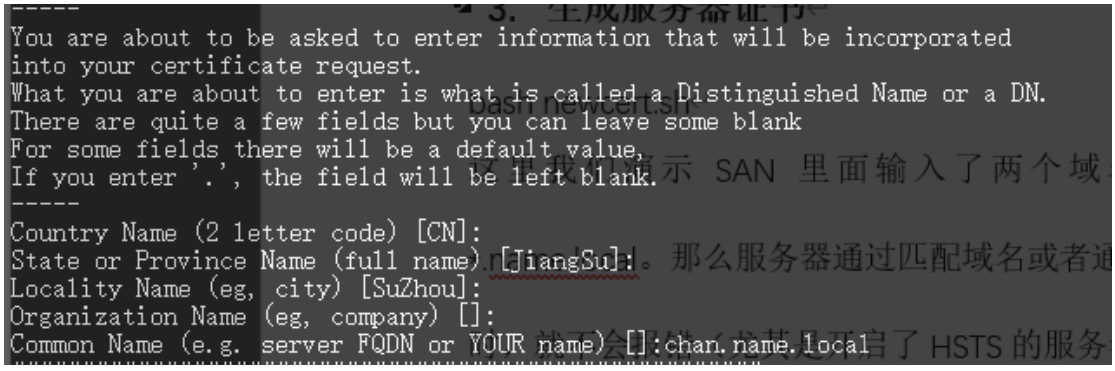
查看生成的证书

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）。

同样的，输入 Subject 里面的 CN，生成 CSR



输入 IntCA 私钥的密码，签发证书

生成完毕，按照提示找到对应目录

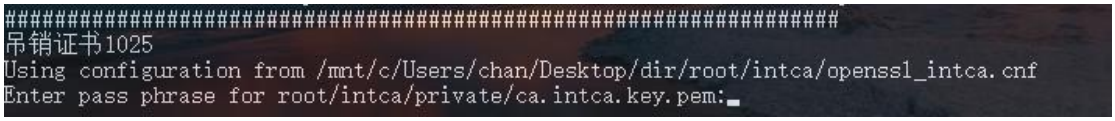
查看证书

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

根据显示的证书信息，确认吊销证书无误

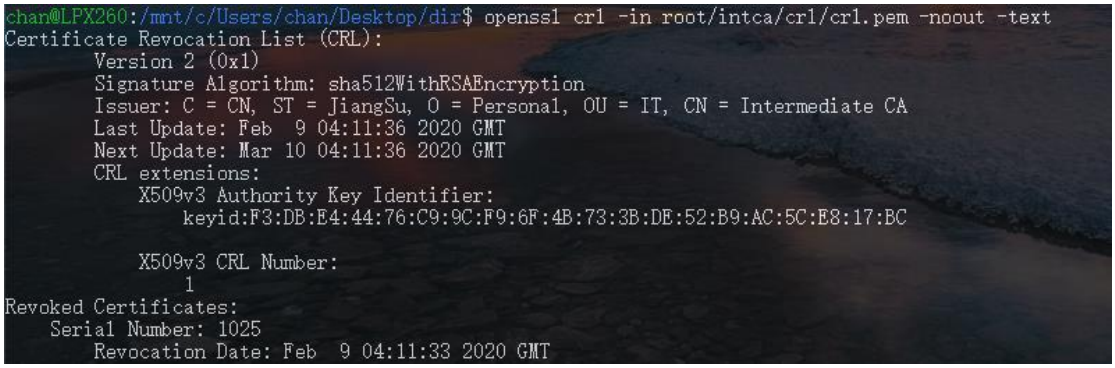
输入 IntCA 私钥密码，确认吊销



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



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

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。