华南理工大学

《PKI 原理与技术》课程实验报告

实验题目：CA 证书的签发与认证

姓名：李鹏　　学号：201630610571

班级：16 信息安全　　组别：

合作者：

指导教师：徐玲玲

实验概述

【实验目的及要求】

实验目的：

学会签发根 CA 证书，使用根 CA 证书签发下级证书。

实验要求：

利用 OpenSSL 提供的命令行工具实现：

1. 生成根 CA 密钥对、生成自签名的根 CA 证书；
2. 生成普通个人用户的密钥对，并生成证书请求；
3. 以 CA 管理员的角色，给上一步生成的证书请求签发个人证书。

【实验环境】

Linux 内核 2.6 及以上，安装有 OpenSSL。

实验内容

【实验过程】

一.安装 openssl

```
root@cslp:/var/MyCA# openssl version
OpenSSL 1.1.0g  2 Nov 2017
```

二.OpenSSL 建立自己的 CA

1. 环境准备

```
wuyulp@cslp:/var$ sudo mkdir MyCA
[sudo] password for wuyulp:
wuyulp@cslp:/var$ cd MyCA/
wuyulp@cslp:/var/MyCA$ mkdir certs private
mkdir: cannot create directory ‘certs’: Permission denied
mkdir: cannot create directory ‘private’: Permission denied
wuyulp@cslp:/var/MyCA$ sudo mkdir certs private
wuyulp@cslp:/var/MyCA$ ls
certs  private
wuyulp@cslp:/var/MyCA$ chmod g-rwx,o-rwx private
chmod: changing permissions of 'private': Operation not permitted
wuyulp@cslp:/var/MyCA$ sudo su
root@cslp:/var/MyCA# chomd g-rwx,o-rwx private
Command 'chomd' not found, did you mean:

  command 'chmod' from deb coreutils

Try: apt install <deb name>
root@cslp:/var/MyCA# chmod g-rwx,o-rwx private
root@cslp:/var/MyCA# echo "01" >serial
root@cslp:/var/MyCA# touch index.txt
root@cslp:/var/MyCA# ls
certs  index.txt  private  serial
```

```
root@cslp:/var/MyCA# vim openssl.cnf
root@cslp:/var/MyCA# cat openssl.cnf
[ ca ]
default_ca = myca
[ myca ]
dir = /var/MyCA
certificate = $dir/cacert.pem
database = $dir/index.txt
new_certs_dir = $dir/certs
private_key = $dir/private/cakey.pem
serial = $dir/serial
default_crl_days= 7
default_days = 365
default_md = md5
policy = myca_policy
x509_extensions = certificate_extensions
[ myca_policy ]
commonName = supplied
stateOrProvinceName = supplied
countryName = supplied
emailAddress = supplied
organizationName= supplied
organizationalUnitName = optional
[ certificate_extensions ]
basicConstraints= CA:false
[ req ]
default_bits = 2048
default_keyfile = /var/MyCA/private/cakey.pem
default_md = md5
prompt = no
distinguished_name = root_ca_distinguished_name
x509_extensions = root_ca_extensions
[ root_ca_distinguished_name ]
commonName = My Test CA
stateOrProvinceName = HZ
countryName = CN
emailAddress = test@cert.com
```

2. 生成根证书

```
root@cslp:/var/MyCA# openssl req -new -x509 -keyout ca.key -out ca.crt -config o
penssl.cnf
Generating a 2048 bit RSA private key
.........+++
.....................................................................
.....................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
root@cslp:/var/MyCA# ls
ca.crt  ca.key  certs  index.txt  openssl.cnf  private  serial
```

三. 生成普通个人用户的密钥对,并生成证书请求

1. 生成普通个人用户的密钥对(key 文件)

```
root@cslp:/var/MyCA# openssl genrsa -des3 -out client.key 1024
Generating RSA private key, 1024 bit long modulus
..............++++++
..............++++++
e is 65537 (0x010001)
Enter pass phrase for client.key:
Verifying - Enter pass phrase for client.key:
root@cslp:/var/MyCA# ls
ca.crt  ca.key  certs  client.key  index.txt  openssl.cnf  private  serial
```

2. 生成普通个人用户的证书请求

```
root@cslp:/var/MyCA# openssl req -new -key client.key -out client.csr
Enter pass phrase for client.key:
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) [AU]:CN
State or Province Name (full name) [Some-State]:GD
Locality Name (eg, city) []:GZ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SCUT
Organizational Unit Name (eg, section) []:TANGLAB
Common Name (e.g. server FQDN or YOUR name) []:scut.tanglab.tang
Email Address []:12345@126.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:qwer
An optional company name []:tanglab
root@cslp:/var/MyCA# ls
ca.crt  certs       client.key  openssl.cnf  serial
ca.key  client.csr  index.txt   private
```

四. 以 CA 管理员身份给普通用户请求签发个人证书

1. 给普通用户签发证书

```
root@cslp:/var/MyCA# openssl ca -in client.csr -out client.crt -cert ca.crt -key
file ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Can't open /var/MyCA/index.txt.attr for reading, No such file or directory
139831024574912:error:02001002:system library:fopen:No such file or directory:..
/crypto/bio/bss_file.c:74:fopen('/var/MyCA/index.txt.attr','r')
139831024574912:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/
bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :ASN.1 12:'GD'
localityName          :ASN.1 12:'GZ'
organizationName      :ASN.1 12:'SCUT'
organizationalUnitName:ASN.1 12:'TANGLAB'
commonName            :ASN.1 12:'scut.tanglab.tang'
emailAddress          :IA5STRING:'12345@126.com'
Certificate is to be certified until May  7 01:45:15 2020 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
```

2. 验证生成的证书

```
root@cslp:/var/MyCA# openssl version
OpenSSL 1.1.0g  2 Nov 2017
```

小结

以前只是掌握了证书,CA,普通用户等相关的理论概念,这次通过 linux 的 openssl 命令行工具实践了公钥私钥对,证书的生成以及证书请求的生成与签发.加深了对整个 PKI 体系的理解,并学会了一定的应用.

指导教师评语及成绩

评语：

成绩：　　指导教师签名：

批阅日期：