网络安全与管理——SSL_CA的使用

软件92-易俊泉-2194411245

1 实验要求

① 创建一个自签名的根证书颁发机构。

② 创建web服务器的私钥和公钥，输入证书信息，产生“证书签名请求(csr)”。

③ 生成用户证书并进行签名。

④ 将私钥、签名密钥与CA的公钥一起打包到一个文件中。

2 实验原理

2.1 ssl概述

SSL协议最先由netscape公司提出，包括sslv2和sslv3两个版本。当前形成标准的为了tls协议(rfc2246规范)和DTLS（rfc4347，用于支持UDP协议）。sslv3和tls协议大致一样，只是有一些细微的差别。实际应用中，用的最多的为sslv3。

SSL协议能够保证通信双方的信道安全。它能提供数据加密、身份认证以及消息完整性保护，另外SSL协议还支持数据压缩。

SSL协议通过客户端和服务端握手来协商各种算法和密钥。

2.2 openssl简介

openssl是一个功能丰富且自包含的开源安全工具箱。它提供的主要功能有：SSL协议实现(包括SSLv2、SSLv3和TLSv1)、大量软算法(对称/非对称/摘要)、大数运算、非对称算法密钥生成、ASN.1编解码库、证书请求(PKCS10)编解码、数字证书编解码、CRL编解码、OCSP协议、数字证书验证、PKCS7标准实现和PKCS12个人数字证书格式实现等功能。

openssl采用C语言作为开发语言，这使得它具有优秀的跨平台性能。openssl支持Linux、UNIX、windows、Mac等平台。

2.3 证书申请

生成X509数字证书前，一般先由用户提交证书申请文件，然后由CA来签发证书。大致过程如下：

① 用户生成自己的公私钥对；

② 构造自己的证书申请文件，符合PKCS#10标准。该文件主要包括了用户信息、公钥以及一些可选的属性信息，并用自己的私钥给该内容签名；

③ 用户将证书申请文件提交给CA；

④ CA验证签名，提取用户信息，并加上其他信息（比如颁发者等信息），用CA的私钥签发数字证书；

X509证书申请的格式标准为pkcs#10和rfc2314。

3 实验步骤

3.1 创建自签名根CA密钥

运行脚本./new-root-ca.sh，产生CA密钥（私钥）ca.key。输入身份信息，产生自签名证书ca.crt

自签名SSL证书是指用户自己利用工具创建的证书，而不是通过受信任的CA机构签发.

其中`Enter pass phrase for ca.key:yjqlovemhy`

```
root@hspEdu01 /u/l/ssl.ca-0.1# ./new-root-ca.sh
No Root CA key round. Generating one
Generating RSA private key, 1024 bit long modulus
.........................++++++
............++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:

Self-sign the root CA...
Enter pass phrase for ca.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) [MY]:CN
State or Province Name (full name) [Perak]:ShanXi
Locality Name (eg, city) [Sitiawan]:XiAn
Organization Name (eg, company) [My Directory Sdn Bhd]:XiAn JiaoTong
University
Organizational Unit Name (eg, section) [Certification Services
Division]:XJTU
Common Name (eg, MD Root CA) []:MD Root CA
Email Address []:XJTU@163.com

```

产生密钥文件`ca.key`:

```
[root@localhost ssl.ca-0.1]# cat ca.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,26B4E4F966062B51

ur0MSp/bd+tNiQp2hByHhrIPXNbCQtSUWtYxcaRVSPiIneQUZfa04RPd2v9CDrgd
gcDlTjF6vUfXhqJRFghGy16ayriqOyqLDrQwQ+4d6yC/K8F0AWDp1eWKiYB5uopI
u2JeOedsnYvju4w8vr/7TqGTqChq1sEDky6LEhOr36qjBoMqhdb1UeJ1Yf4H4OH7
```

```
Bt4uD+ddhZMr87mmHLShDrs1OvxqfK1pEdAjTFr1Mk/RD/z/FcrZF3rRfWcXpsLe
cxQVLRHBHVVhr5uQC9g2INBWocmtt/m28eweRLuD2/gObQH9CZuc5+Y8WyawnlYU
LXxf5dnIyI4eC7vfKconBQnueikpz2sW3W8Ejsqu1K5TVhErlPZ50/9eir2Rn9rA
D9zahmhOzBNaAElNZMTUlxL2v9tDmwm9h1fZsn1K/dSN/AB6jmUjLV26PGhOWNpE
TPzuovp2O0MSfR/98l+IbXNM8XBCaF9Gt/nqb5xTtqLJDTEk20RIIl4BFsEoHkIX
y5w/n6E8G/cSw/rWTJg4KiymW1xsmACJV197dYZauhN72T+7eBN6n96Pncx2z9Nw
R2gTRvq576Za6teki6APt7PQQy091xW1N/FUEClXsqVAhxypeoaKw6iPwiPL7dof
d9HVl6IJZR+Y6fvTysSgJUCMmiLhC0IcamH8dfd0NAk1i6Ph1orntwEWnqoaFJJz
178MsgSvPAlQ6R61s94NuovaIUM8NmAsyQQZBSDlC3JRhOzZa/u19/CjAAWiq4Q9
xRlhbbkmbZdVX2Pn2u+K358yxZQmomXaV1F56sGYAE3TR+iEDc4K1A==
-----END RSA PRIVATE KEY-----
```

产生自签名证书文件`ca.crt`：

```
[root@localhost ssl.ca-0.1]# cat ca.crt
-----BEGIN CERTIFICATE-----
MIIC1DCCAj2gAwIBAgIJAJ2o/f8qIV9RMA0GCSqGSIb3DQEBBQUAMIGRMQswCQYD
VQQGEwJDTjEPMA0GA1UECBMGU2hhblhpMQ0wCwYDVQQHEwRYaUFuMSEwHwYDVQQK
ExhYaUFuIEppYW90b25nIFVuaXZlcnNpdHkxDTALBgNVBAsTBFhKVFUxEzARBgNV
BAMTCk1EIFJPT1QgQ0ExGzAZBgkqhkiG9w0BCQEWDHhqdHVAMTYzLmNvbTAeFw0y
MjA2MDcxNjAwMTBaFw0zMjA2MDQxNjAwMTBaMIGRMQswCQYDVQQGEwJDTjEPMA0G
A1UECBMGU2hhblhpMQ0wCwYDVQQHEwRYaUFuMSEwHwYDVQQKExhYaUFuIEppYW90
b25nIFVuaXZlcnNpdHkxDTALBgNVBAsTBFhKVFUxEzARBgNVBAMTCk1EIFJPT1Qg
Q0ExGzAZBgkqhkiG9w0BCQEWDHhqdHVAMTYzLmNvbTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAwlVcUH5WmnB5n70EjguZMe03PIu1tnPoVsZHDl8GYNl2HsVz
B04Pj7Cc6ONxX+o4aMqGXcXumwyqLX59w9aUvxmLjyHbEz1Oga7+vSnFahXVcx67
fYO3i1YBBA2MvEG7WesXZVo8ftsOpmyqHOX85h/JC+ZW2X9CR1NpqLdS5xECAwEA
AaMyMDAwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUsdqZ7dfhXZBryRRWcv3O
W/8lZQEwDQYJKoZIhvcNAQEFBQADgYEAJH6Kq5w1Tkwe2RXcPHni4ThVSV1ay+BA
IrFGKGLDu+jFZA/j0Qh90+zeJydyFoLcUgbBBtAHgI104wowTx5KuD3200AK/oxi
yLPUHuERFam/LdXAAdUH3CMnQSOo9PChBDcJGipjgncC2QFJMqweEs1vh7+QyOvF
kEMYRaC1a7A=
-----END CERTIFICATE-----
```

3.2 创建服务器证书

使用`/new-server-cert.sh www.yjqlovemhy.com`命令，产生服务器密钥；输入身份信息，产生证书签名请求文件

```
root@hspEdu01 /u/l/ssl.ca-0.1# ./new-server-cert.sh www.yjqlovemhy.com
No www.yjqlovemhy.com.key round. Generating one
Generating RSA private key, 1024 bit long modulus
...++++++
..........++++++
e is 65537 (0x10001)

Fill in certificate data
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) [MY]:CN
State or Province Name (full name) [Perak]:ShanXi
Locality Name (eg, city) [Sitiawan]:XiAn
Organization Name (eg, company) [My Directory Sdn Bhd]:shiji
Organizational Unit Name (eg, section) [Secure Web Server]:sj
Common Name (eg, www.domain.com) []:www.yjqlovemhy.com
Email Address []:yjqlovemhy@163.com

You may now run ./sign-server-cert.sh to get it signed
```

证书签名请求文件`www.yjqlovemhy.com.csr`中的信息如下：

```
[root@localhost ssl.ca-0.1]# cat www.yjqlovemhy.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIB/TCCAWYCAQAwgYoxCzAJBgNVBAYTAkNOMQ8wDQYDVQQIEwZTaGFuWGkxDTAL
BgNVBAcTBFhpQW4xDjAMBgNVBAoTBVNoaUppMQswCQYDVQQLEwJTSjEbMBkGA1UE
AxMSd3d3LnlqcWxvdmVtaHkuY29tMSEwHwYJKoZIhvcNAQkBFhJ5anFsb3ZlbWh5
QDE2My5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAM09Ynu/2TzFVg0v
+lu/bDPfSWJ5Fg/ajq94PZya7LpxwwZIEyusdjw7J4pwFyehrAPxmyiLI5g16peG
t+/jUi3Ai+X8uWqgsFiFQpKoBSW+UnguJMhZlyuzlysvjUEB8nTWpG6Sl3KPneOp
ElymrSO3i47ZnbGFtEBRb5VO27lvAgMBAAGgMjAwBgkqhkiG9w0BCQ4xIzAhMBEG
CWCGSAGG+EIBAQQEAwIGQDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3DQEBBQUAA4GB
AIQrp/fe+gIsqWp8eYjJtzBoQynwF8hbHMzSHe2SiUO1Wj7GwwIWJQJpYvbX1vNj
ClF0QKFkPdGf/JUMv48EzkBehQVhtP8+Ewr95Z53LzUmAZ3Ocd2X1Ob6R1w8KdNh
NJqR5Q3s5Vync5xk6RhWtUF5V3uynIr8TuWNPGGoM0aK
-----END CERTIFICATE REQUEST-----
```

3.3 签署服务器证书

使用`./sign-server-cert.sh  www.yjqlovemhy.com`，CA给服务器www.yjqlovemhy.com颁发证书。

```
[root@localhost ssl.ca-0.1]# ./sign-server-cert.sh  www.yjqlovemhy.com
CA signing: www.yjqlovemhy.com.csr -> www.yjqlovemhy.com.crt:
Using configuration from ca.config
Enter pass phrase for ./ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'ShanXi'
```

```
localityName          :PRINTABLE:'XiAn'
organizationName      :PRINTABLE:'ShiJi'
organizationalUnitName:PRINTABLE:'SJ'
commonName            :PRINTABLE:'www.yjqlovemhy.com'
emailAddress          :IA5STRING:'yjqlovemhy@163.com'
Certificate is to be certified until Jun  7 16:02:27 2023 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
CA verifying: www.yjqlovemhy.com.crt <-> CA cert
www.yjqlovemhy.com.crt: OK
```

可见，证书颁发成功。

`www.yjqlovemhy.com.crt` 文件信息如下：

```
[root@localhost ssl.ca-0.1]# cat www.yjqlovemhy.com.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CN, ST=ShanXi, L=XiAn, O=XiAn Jiaotong University,
OU=XJTU, CN=MD ROOT CA/emailAddress=xjtu@163.com
        Validity
            Not Before: Jun  7 16:02:27 2022 GMT
            Not After : Jun  7 16:02:27 2023 GMT
        Subject: C=CN, ST=ShanXi, L=XiAn, O=ShiJi, OU=SJ,
CN=www.yjqlovemhy.com/emailAddress=yjqlovemhy@163.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:cd:3d:62:7b:bf:d9:3c:c5:56:0d:2f:fa:5b:bf:
                    6c:33:df:49:62:79:16:0f:da:8e:af:78:3d:9c:9a:
                    ec:ba:71:c3:06:48:13:2b:ac:76:3c:3b:27:8a:70:
                    17:27:a1:ac:03:f1:9b:28:8b:23:98:35:ea:97:86:
                    b7:ef:e3:52:2d:c0:8b:e5:fc:b9:6a:a0:b0:58:85:
                    42:92:a8:05:25:be:52:78:2e:24:c8:59:97:2b:b3:
                    97:2b:2f:8d:41:01:f2:74:d6:a4:6e:92:97:72:8f:
                    9d:e3:a9:12:5c:a6:ad:23:b7:8b:8e:d9:9d:b1:85:
                    b4:40:51:6f:95:4e:db:b9:6f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
```

```
keyid:B1:DA:99:ED:D7:E1:5D:90:6B:C9:14:56:72:FD:CE:5B:FF:25:65:01

            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication, Microsoft Server Gated Crypto, Netscape Server Gated Crypto
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
        c1:d1:f2:a6:31:45:f7:03:2e:23:6a:64:5c:42:f0:5e:e6:7e:
        c6:83:21:e6:c5:59:21:84:32:02:e9:55:2a:ca:6a:7c:51:24:
        0f:4f:29:92:f4:7d:05:f9:e7:c3:5c:8f:e2:28:fd:69:08:ac:
        a4:fa:06:eb:b4:09:f3:c6:e9:ca:ad:b5:56:d7:f0:02:6d:25:
        e4:6d:52:d3:98:20:a9:29:5e:16:70:ab:51:a9:2b:10:d4:7e:
        ee:08:e8:c8:da:b4:86:28:d3:c4:42:cd:2b:20:85:95:f1:15:
        b3:b5:fa:d4:22:6c:25:a6:a0:ee:26:07:95:a1:94:58:ee:36:
        08:83
-----BEGIN CERTIFICATE-----
MIIC+jCCAmOgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBkTELMAkGA1UEBhMCQ04x
DzANBgNVBAgTBlNoYW5YaTENMAsGA1UEBxMEWGlBbjEhMB8GA1UEChMYWGlBbiBK
aWFvdG9uZyBVbml2ZXJzaXR5MQ0wCwYDVQQLEwRYSlRVMRMwEQYDVQQDEwpNRCBS
T09UIENBMRswGQYJKoZIhvcNAQkBFgx4anR1QDE2My5jb20wHhcNMjIwNjA3MTYw
MjI3WhcNMjMwNjA3MTYwMjI3WjCBijELMAkGA1UEBhMCQ04xDzANBgNVBAgTBlNo
YW5YaTENMAsGA1UEBxMEWGlBbjEOMAwGA1UEChMFU2hpSmkxCzAJBgNVBAsTAlNK
MRswGQYDVQQDExJ3d3cueWpxbG92ZW1oeS5jb20xITAfBgkqhkiG9w0BCQEWEnlq
cWxvdmVtaHlAMTYzLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAzT1i
e7/ZPMVWDS/6W79sM99JYnkWD9qOr3g9nJrsunHDBkgTK6x2PDsninAXJ6GsA/Gb
KIsjmDXql4a37+NSLcCL5fy5aqCwWIVCkqgFJb5SeC4kyFmXK7OXKy+NQQHydNak
bpKXco+d46kSXKatI7eLjtmdsYW0QFFvlU7buW8CAwEAAaNnMGUwHwYDVR0jBBgw
FoAUsdqZ7dfhXZBryRRWcv3OW/8lZQEwNAYDVR0lBC0wKwYIKwYBBQUHAwEGCCsG
AQUFBwMCBgorBgEEAYI3CgMDBglghkgBhvhCBAEwDAYDVR0TAQH/BAIwADANBgkq
hkiG9w0BAQQFAAOBgQDB0fKmMUX3Ay4jamRcQvBe5n7GgyHmxVkhhDIC6VUqymp8
USQPTymS9H0F+efDXI/iKP1pCKyk+gbrtAnzxunKrbVW1/ACbSXkbVLTmCCpKV4W
cKtRqSsQ1H7uCOjI2rSGKNPEQs0rIIWV8RWztfrUImwlpqDuJgeVoZRY7jYIgw==
-----END CERTIFICATE-----
```

3.4 创建用户证书

使用`./new-user-cert.sh  yjq@www.yjqlovemhy.com`创建用户密钥和产生证书签名请求文件。

```
[root@localhost ssl.ca-0.1]#  ./new-user-cert.sh  yjq@www.yjqlovemhy.com
Fill in certificate data
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.
-----
Common Name (eg, John Doe) []:YiJunQuan
Email Address []:18813517223@163.com

You may now run ./sign-user-cert.sh to get it signed

```

3.5 签署用户证书

使用`./sign-user-cert.sh  yjq@www.yjqlovemhy.com`，给用户yjq颁发证书。

```
[root@localhost ssl.ca-0.1]# ./sign-user-cert.sh  yjq@www.yjqlovemhy.com
CA signing: yjq@www.yjqlovemhy.com.csr -> yjq@www.yjqlovemhy.com.crt:
Using configuration from ca.config
Enter pass phrase for ./ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :PRINTABLE:'YiJunQuan'
emailAddress          :IA5STRING:'18813517223@163.com'
Certificate is to be certified until Jun  7 16:11:32 2023 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
CA verifying: yjq@www.yjqlovemhy.com.crt <-> CA cert
yjq@www.yjqlovemhy.com.crt: OK

```

给用户颁布的证书`yjq@www.yjqlovemhy.com.crt`如下：

```
[root@localhost ssl.ca-0.1]# cat yjq@www.yjqlovemhy.com.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CN, ST=ShanXi, L=XiAn, O=XiAn Jiaotong University,
OU=XJTU, CN=MD ROOT CA/emailAddress=xjtu@163.com
        Validity
            Not Before: Jun  7 16:11:32 2022 GMT
            Not After : Jun  7 16:11:32 2023 GMT
        Subject: CN=YiJunQuan/emailAddress=18813517223@163.com

```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c3:cd:2c:ae:b3:a8:ac:3b:7e:dc:3a:48:00:3a:
                    16:e0:99:0b:f4:93:44:1a:35:c1:97:89:2a:55:34:
                    d9:d4:2b:8b:a3:c5:64:24:05:cf:55:b2:2a:62:b4:
                    5d:1a:f7:f6:fa:ca:00:9f:9b:30:12:6f:7a:f0:4c:
                    72:99:86:71:84:77:42:61:a7:e0:2f:d4:2b:5b:c0:
                    13:23:68:77:51:06:9a:2d:7e:13:de:39:89:d7:e0:
                    bc:97:35:10:90:c0:99:90:c5:e9:df:83:49:41:49:
                    c0:81:2c:6d:d7:99:00:17:15:8c:fa:21:66:d2:f9:
                    3d:cd:81:6f:3d:2e:7f:47:a9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:18813517223@163.com
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:

keyid:B1:DA:99:ED:D7:E1:5D:90:6B:C9:14:56:72:FD:CE:5B:FF:25:65:01

            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
    Signature Algorithm: md5WithRSAEncryption
        08:1f:cf:fe:ed:07:b3:40:94:41:6e:e6:45:50:0c:df:ea:43:
        f4:f0:de:8f:9d:5d:36:b8:75:4b:7c:d6:26:4d:f9:21:20:58:
        52:4e:f9:5e:3f:4f:8c:da:4c:c4:8c:cf:39:fb:9f:c6:3d:4a:
        a1:f9:fe:fd:b7:59:bc:ea:df:8a:f7:73:be:23:0e:a6:6d:b1:
        2e:7c:77:3a:b2:e4:8b:85:b1:00:97:61:f1:a4:26:78:91:dd:
        a9:13:fd:ad:bb:eb:53:67:2d:45:a3:74:de:6b:9e:fa:84:a2:
        a2:0d:b8:29:4a:ac:24:10:d8:40:ec:f2:4d:1a:0d:4d:35:20:
        a7:ec
-----BEGIN CERTIFICATE-----
MIICsDCCAhmgAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBkTELMAkGA1UEBhMCQ04x
DzANBgNVBAgTBlNoYW5YaTENMAsGA1UEBxMEWGlBbjEhMB8GA1UEChMYWGlBbiBK
aWFvdG9uZyBVbml2ZXJzaXR5MQ0wCwYDVQQLEwRYSlRVMRMwEQYDVQQDEwpNRCBS
T09UIENBMRswGQYJKoZIhvcNAQkBFgx4anR1QDE2My5jb20wHhcNMjIwNjA3MTYx
MTMyWhcNMjMwNjA3MTYxMTMyWjA4MRIwEAYDVQQDEwlZaUp1blF1YW4xIjAgBgkq
hkiG9w0BCQEWEzE4ODEzNTE3MjIzQDE2My5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAMPNLK6zqKw7ftw6SAA6FuCZC/STRBo1wZeJKlU02dQri6PFZCQF
z1WyKmK0XRr39vrKAJ+bMBJvevBMcpmGcYR3QmGn4C/UK1vAEyNod1EGmi1+E945
idfgvJc1EJDAmZDF6d+DSUFJwIEsbdeZABcVjPohZtL5Pc2Bbz0uf0epAgMBAAGj
cDBuMB4GA1UdEQQXMBWBEzE4ODEzNTE3MjIzQDE2My5jb20wDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAWgBSx2pnt1+FdkGvJFFZy/c5b/yVlATAdBgNVHSUEFjAUBggr
BgEFBQcDAgYIKwYBBQUHAwQwDQYJKoZIhvcNAQEEBQADgYEACB/P/u0Hs0CUQW7m
RVAM3+pD9PDej51dNrh1S3zWJk35ISBYUk75Xj9PjNpMxIzPOfufxj1Kofn+/bdZ
```

```
vOrfivdzviMOpm2xLnx3OrLki4WxAJdh8aQmeJHdqRP9rbvrU2ctRaN03mue+oSi
og24KUqsJBDYQOzyTRoNTTUgp+w=
-----END CERTIFICATE-----
```

3.6 将用户证书打包到一个pkcs12文件中。

使用`./p12.sh yjq@www.yjqlovemhy.com`将用户证书打包到一个pkcs12文件中

```
[root@localhost ssl.ca-0.1]# ./p12.sh yjq@www.yjqlovemhy.com
Enter Export Password:
Verifying - Enter Export Password:

The certificate for yjq@www.yjqlovemhy.com has been collected into a pkcs12 file.
You can download to your browser and import it.

```

`yjq@www.yjqlovemhy.com.p12`中的信息如下

```
[root@localhost ssl.ca-0.1]# vim yjq@www.yjqlovemhy.com.p12

0<82>
×^B^A^C0<82>
<9d>^F  *<86>H<86>÷^M^A^G^A <82>
<8e>^D<82>
<8a>0<82>
<86>0<82>^G^_^F *<86>H<86>÷^M^A^G^F <82>^G^P0<82>^G^L^B^A^@0<82>^G^E^F  *<86>H<86>÷^M^A^G^A0^\^F
*<86>H<86>÷^M^A^L^A^F0^N^D^HýpÞy! ª<8f>^B^B^H^@<80>
<82>^FØ<9e>¾^SÒYþs¾[âùOH¶^Z¤výùÖ<91><9a>4^E<95><9a>¯Nö³c^X!^S.Ý×^Vÿ<8a>ê;^E-^T^HÜÀÈø^\<84>d·^OÉ6^Eß^SÌIC<8c>äë<8a>^X}Þ<8d>L¬&^HSÔ/Ô§q<99>88ìCó\^ZT$ãcÐ-°N4UG<9c>Ú<90>Ïª]!    kë·?
êÛ#G¤@^LLl¼©^S^E<86>ñ<ñO<80>mP¥>Àb¦^HVøú¿'<80>úKFßÕoHÏL^Eô<9e>Û{/[Ö+^M^G<Êc¿`¨»0®YØ¹~u^F84¡^?<94><9f>"Ý«oA<80>BùÒ2*<81>|{¯ê<92>F
<\NÇ^Ftr•ê<95>§^^½Q@     aõuÄh°<9c>^\G^G2bU     Ö}¡¿?
%^B1<94>ÑÏè¢<87>¨ÞÄ2#Íf<8b>´{0 G<94>ßM^F<9f>ÉèPZÀv_2EQ <84>
<8e>0ÌBAÖ<9a>;oÃo^F»¥h¶G1ïÑ»åÝv^Ws^U)^H]^FG¶à<99>]<95>'Â°^CõÄÈ)<9f>l^L<9e>^?
<96>D*^M<9d>>^X\õ<9e>^]ò¼^A^B»{ÂV^[#½Èaû<94>HfY^K}
Í¯ã<91>Í¨]U<8c>m<8a>u._^Kµ^T4^Qw^R*¤o!¤ÎZR¹G^G¼¾ j¿Öfà °KØ<90><83>
<87>/^SgÊ,b^<95>óªÚ^_iwÁÄX<9c>©^Q^ClÐo<85>^L½<9e>FV<8e>x^Z$<9f>f¶^OßzÜÝ$O°2à
ñ&R+^GØ^E±ô^Xuá^Gø^L<8e><98>ÆþG,d@•i^Uµ^G¼^^e¶QñK^Av<81>i°tôÿ¸jK<95>IÞ<84>
<85>^^L~<9a>Å^Yõ9<9e>^C¾<82>aÐ<8b>^\<87>I7¿ê<95>^P<9c>U<8f>X<85>Éóæ<9e>
<96>ñ}ï^O<83><87>ÐïUûéÆ<90>¢[`ðû§¨¤^S<ËiòK^RQÙ^D<82>oþ:
<9e>ì<96>õ¢^H<98>Q¢<83>×^RèV«R£<87>ãísdü<89>Oÿ¼®"Ü¼<96>`tæM"^WtÝ"z±<84>¼#^Bô
<8f>Îùh1Uëææa¬¹p§eø:Ïµ^QÌp8±`lâT_÷Mê8^^ÿ<91>_'³_N^A×ÂÁ`
gyÙ<97>^P^T¾ÍÓäf<9a>ø«´^_^A»ß^GðÔt´^G^^êu;<91>nõ¥>å)[<9b>M6     âëÁ^QÉUh<8e>
^L*<9f>¦<8e>^W<80>a^\ùý9øef¶<8f>[
```

```
k3XË    <99>É+@<94>&[<82>È¦c¥¿ê^T\,ñÄq[²@§WÝÒ^?å¤cÃNÄ;4Y»þ^?ýÎ/
ÐÎ2ÉóÏ^R=¸.2µ<81>s\
ò[_FB^Sñõà<99>^B<98><93><8c>^T^RZ^L_ìm÷<9f>®+
<82>nC<8e>^W¼ÆÅiRÞ^Kßp^Yå2O<8d>Q<80>
<83>ç_<99>é^N±ä@^Q×=¶<87>÷ãw(¨^Q#ÄT<8c>Ü<83>^?Ë@<9a>ÁÇßy+V²GÁ^@°]
<8b>^\^@ÝYçS<92>VÚ¦-¤^UãáêÕê^_õ5ö^QÑ<89>Xzvã7,Á^?
DÏ¹>Å'íã$fSZJ•ò^\^YI<89>æ'KO(P6C<82><95>^?jÊ<88>Tÿ<94>^L¦¿¤õüÌPÏx*½^_
t<81><92>^[ûl¥
¤x<9d>çó<94>%^LªµB^KÍôhl|^©ÀÑú~#<8b><8a>?%<87>°^[<8f>ú^V?
Y§ÞÚncÜÇ¿<86>Ýðü<8a>V^B^_¥E<8d>ÞJ!<80>
<88>Â¾4ü3ÉÌÄ•Â¸1¶«G<91>ð¢<9c>a|^T^HAñ^XÀÞ<8c>íö[+^Z{Â<9c>¼·<8a>±ì"X
ëÑ•¹Þ^U+<84>^GÀY^N<9a>7ÿPQ=Õ¸^U<9f>K_3ê¸f3^K^D7^\<81>©Û»³Ix^G¼Äì^?Å|¡Ë<98>M
# ÁüóECl~EôPz<9a>qÎú¨¼<96>Ìÿ2¸|<93>T^Ce^U¥ËÄï0;^]7ÈJ
D@¢Êð÷^[<,Î£~^QmôAO¿ô<8b>¼Õøs<9b><91>»~
<81>Õ<81>^N§ô6¯^WÛGo<91>×o6<8c>^@©f^H^BOã<9f>P¡±{É^÷«^AeRàêlàn?
ß^H^H^Bµj¨ã¶'C^MöÀ4õ+¦Î}<82>'Ï<93>Æ¿M
U¿<95>å <9c>¯|ÔS^N <83>$é<82>þ^]K\\øÈ¤^N´<8e>È»<99>2¿|&"Ò/Ôò,<99>D*^\^?
@ß\^^¾}^A÷^KéäT<86>^LOÒkÈú¦ßjÐ°äeìÕ÷^GxÌ9|<9a>
[&c3µ^\&ZÇ•¢<86>¿µÌ`ò<84>o^T^E9.ÌÍÑ<8b><8d>^PÉ^È§zï^E^QË<93><8f>6N^M<9f>
<86>^H×Ç<9c>èàà¥=jâ[p^SMt%ólÞ0^O2<8f>µ^Q^E•\c¼Æ^W  uþ*ûR·¿þP*
<9c>iSÄ=ÆmØÚ§Æg<8d>f_y<94>ç<93>Ä^Ok^V~XuOmñ)ì¦¯ú<8f>~/ó<83>EÝ<8a><84>
<9c>ÕÂ^Hëµ*Üg¢ô<92>•TÝl»Eõ,9´?8'^Q<8d>^A?+^N±æ²^WwþÎÿ^F<89><9c>^D¡d6â´mËç,?
^Aéçy|'U<97>^CAn!Û^]ðr^Gý^DaXÒ¢¥<83><87>¶Úñ^O^[o^[
Ê<92>['<90>áÃ»þ0Ãô^RåCZN!¥p<9e>«G´^R¦B{.1±¿<92>^C^KÍªÓõ~Å<94>Ö^DQ¡<98>80Ó|¸
d^Z<8c>^M<99>h^CKsÕ~Êúñ¹e7^Y¹Àë;EûÏÁÛ@<86>ÑÊ^E^W,D¨2^]1^EIôY¥2ÕYoTõÍvg^T^A:ÿ
'^K<8a>'<93>æ4<95>wê]j<8b>^^kÅÌT^V^_A¾^C]<95><8c>m1%<81>¿<90>Ç<80>^SßõÆz+)ä;
<88>¢ì7^EäAãúæ^åEDi(§VeX^S<88>0<82>^C_^F    *<86>H<86>÷^M^A^G^A
<82>^CP^D<82>^CL0<82>^CH0<82>^CD^F^K*<86>H<86>÷^M^A^L
^A^B <82>^B¦0<82>^B¢0^\^F
*<86>H<86>÷^M^A^L^A^C0^N^D^H[2<<83>ñ|^C^V^B^B^H^@^D<82>^B<80>
[^X^KÓjÄ<89>¶z<80>-<84>öÀm_ý_¿&H®×ú(^B<86>R°N&cmb×Åõ^^\U^Uÿo*R¼yÔiá°wÏï.·K}
<¯^V/îÏ^S#]¦Èì»<95>~•<8f>#«+C2<8a>+îïÛQ<81>è<80>ùQí^\¯<9e>^GwÚvo^N^G«¤
{<8c>CÕ^?Î•7/Ú0¨¸Ê¸^^äóÊá^Ys^D v^Nì<9c>V ÿþ<97>^Ze<8e>«^?^[>
<84>¸Ì^_Ùª^UÄÁ)÷]´^^<92>é<98><80><89>Ç^VW¬A»<98>ýwW2\
¥p^KÀî3ò¿9ÒÆ=úC@Ëý<84>¥^S²<86><97>À¼<91>OÝ¾'^Q¨ü©HÊ^MsR(¬<8e>O^V
(üÖC<8e>¾<91>eè<97>ûÆ¸^AÎBïOo#¯à¿°»YåãÉÈÈ¦<8e>2ÀÖ^Qq^?<84>4^E\-
^S<9a>û^<95>®'(<8b>ïóD$`0b,N<9b>%ÞzG}
è¶ò<88>ðÛ^@ÚY×<<8c>.§ý•òm^B<94>â",x<88>zÿ <9b>^P×ÎÿbðÖ·FÌüJ¯ù<97>
[·ª<83>¿ß^T.h£»_Âu·<89>ÌäÜs9Æ_e^[kÂ^[u`•Å[^Q<85>^RÀà´^A?q73½Hä^XwS<83>
´ªð,ü^@xøíBD÷êa<8a>^AâRÁó4Ê<9f>^B^BÄwhaä<87>
<8b>V^XSs^U^Ud»3¨îl<83>tv²(°G`I°-
<81>^Nµ¹w>êÉ2<88>¥ÚÇjÓ¼<95>^[cî@<83>P<9b>55*{<9c>¸^K<84>iö^H^Q<98>â$ç7?
<8b>"|ÔÌÄ5åöE¤ú2^]3Îb¿Ô^0V*ÈÂ/T<9c>ÈÍïþ=åk<84>Ô^W;î^V<81>?
<8d>#ñ<8a>ÿv&^D¢^_zÓbæj;Âræ<92>|<9b>•Åi^LÈÿ£$E¶zÄ3BdÔÁ@¸^T°^?
ª^E·^K<ê"^QÃ<9c>ËÏ<9b>~$¶säË<88>
<unÐ^X<90>©dxw¯ô^F3t^S{ôoàtÃ^0|^_÷ç<8d>JÈ^AªyõÑ°~w<8b>^Z^?%²0Ø
```

```
Ì¶Ê¾ý1<81><8a>0#^F      *<86>H<86>÷^M^A ^U1^V^D^TÒ¤
±^H<8b>^^ôÿ<87>Ù<93>=Xÿñ%Iq§<8f>0c^F *<86>H<86>÷^M^A
^T1V^^T^@Y^@i^@J^@u^@n^@Q^@u^@a^@n^@/^@e^@m^@a^@i^@l^@A^@d^@d^@r^@e^@s^@s^@=
^@1^@8^@8^@1^@3^@5^@1^@7^@2^@2^@3^@@^@1^@6^@3^@.^@c^@o^@m010!0
^F^E+^N^C^B^Z^E^@^D^T!F9í<81>´s=Loz'`<8b>Ðpï
<8d>Î^D^H§<82>T<87>â"<9e>J^B^B^H^@

```

4 实验结果

使用`cat ca.db.index`，可以看到CA共颁发了两个证书：

```
[root@localhost ssl.ca-0.1]# cat ca.db.index
V   230607160227Z       01  unknown
/C=CN/ST=ShanXi/L=XiAn/O=ShiJi/OU=SJ/CN=www.yjqlovemhy.com/emailAddress=yjqlo
vemhy@163.com
V   230607161132Z       02  unknown
/CN=YiJunQuan/emailAddress=18813517223@163.com
```

实验验证成功！

> 注意：centos系统会报错，建议换一个环境。