CES571S - L3 - MD5 Collision

467261 - Yifu Wang

2018 - 11 - 30

1 Becoming a Certificate Authority

Generating.

```
root@LunaEx:~# git clone https://github.com/Luna1996/demoCA.git
Cloning into 'demoCA'...
remote: Enumerating objects: 5, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 5 (delta 0), reused 5 (delta 0), pack-reused 0
Unpacking objects: 100% (5/5), done.
root@LunaEx:~# ls
E81CSE503.pem  demoCA
root@LunaEx:~# openssl req -new -x509 -keyout ca.key -out ca.crt -config ./demoCA/openssl.cnf
Generating a 2048 bit RSA private key
..........................+++
.......................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:Beijing
Locality Name (eg, city) []:Beijing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WYF
Organizational Unit Name (eg, section) []:WYF
Common Name (e.g. server FQDN or YOUR name) []:WangYifu
Email Address []:yifu.w@wustl.edu
root@LunaEx:~#
```

ca.key

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIyxWbUJO3scMCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECDB4xXyIzwRRBIIEyG05ectZNvbb
HXRNBs96koDI3Tv0g8UimYYa2c8ne0I0JL+Ses/1JYHLYwgVv1TIxtY8Zjr+qGLx
dbsXPv8gsCTr88Qrek2wr1Z1+1C3H9avfKLI0Izo8MDMA+YZQpnnPn/rkCbvwL01
MWnGfZVpHqZZICzDi1Ggx+iJwaDNf5xf8qHnzIc0Li18hMwamRJjcTF9OwNnum9o
WUbwS7E1x/d6vciR2aQxaeOJMGmjkbnTnG5IPUuob4NIr3EVNnU0Ss3wMG+EssnH
fbWXMc1MXW++1cTKx0uio2qN4gSi/kS85qLVpHPI1r0JSIQtKDwhYR6ZNpZvFG7Z
360KV8X37uAOxy/rVU2eHezdvMKSiV8mfIm8aJuXBYQ31OHz1WVF6L1NODr4e7o7
U7sd8p9uM1h18vfUKqcr+1+oeT5NK+MKv5wWUoNKCYWKMe+NeH1u6IP/aY/Dskjs
LNCYt8qaPZGZG/IUISRt2vmNeWfNO4jsNPMSMCKkBeNFtrTmbAp6tqAADG5VHQuo
Tskka9TKb92W1Wof3U4cRShLZ8TLBbgarY5gWMtCsNQzVH6rKKS4Aks1UKib73ge
kZ4uQFMOUgiW9Hi8w8bFe10uwt0e5SOF4xe1Sg1G0x5OPNtp8WzH9PUTJYmca2v6
a+EqsASUmnGTv4RDQwDBiyCKW2ENvvkb5qTy1bQSqng6q4uRC0X7T4WhgstKYf9I
gpLbQGAHh9k4HQAhHPpOJdFs3W15AkpeMvH3srpM0FmndyjUc4GrQbaDyOjCWc1G
zK9BNK7TezkhRiZZB0A6NjC5kH5SexyCFnMg/MIOPjUQryRKzN1gOfTeLd1DsVJf
YOafjdDNbcs1tsTP2XK/MI8dpaF2VHMU9bx2jqcIcfrAja54r99G5BpdFFQr06z0
S4mXqGkAw/E5gh+2XTkU6dupIQ6S1zrzzDg6TKkOUT1OZwm5VZi+ctjw0WMzFNBI
g405+HcyXwOPxw+MPWpOptWa1mmaIDx8X/Rx7/bSDRcS43OfA3vH1sQKNLUsych2
iwkbEWJ3EK92cNV4kjb/1RBLCpHXbx5FyRPXHu3xIYmAckG4NT7zSYCyHOaVRg5b
TbYsU17UC0P/wGvXh4ewftOFwZxQ2A6YjY40jbGcK2zefeTFYY8ymZiGsn4P5O3Q
VeeNBk+PYmuZi1hft9Pp91Hk/DaZvWKtpky61kzeGNG1AiIryE8uuZNBaDJMyEvX
g/SobKvd0MdNpmEAOA2Rf19OP0cQFIfbT174LYmT9jEXQMtthTrV3+PuZUWAMIuY
0HaZicMPEkguB7SJziX+pCX2znTdKV8p2DotHJ9rn4O7g5mvU8HOprt1UL/imYmH
8Sx4vvha4E7M7Sin7ZJJkKnUGbcs7Me4VYfqfU5bKt06MFcij+pKfJDFrw6aBUbR
1bTiW5QeXwSqd09ES0RBkW1091rWy4KhxkdnbfmEWvu85wAXWZp/cAvKhu8kxVN2
1QCkL5wEuHb5bnk2xsmQd47R0LUmHSxj/6/utDBeAaYQmkaxopb4YTtg4VT8UPdr
ayvXtr3Kw6fCmSNVfFUt7NSxCfaEMNkGkRbZP4DK+6HukPm05Qt7BodcPGYf8Ys2
iOAOHMzdMC4XmKmUjHFWig==
-----END ENCRYPTED PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIID2jCCAsKgAwIBAgIJAPNtiDc1hLheMA0GCSqGSIb3DQEBCwUAMIGBMQswCQYD
VQQGEwJDTjEQMA4GA1UECAwHQmVpamluZzEQMA4GA1UEBwwHQmVpamluZzEMMAoG
A1UECgwDV11GMQwwCgYDVQQLDANXUYxETAPBgNVBAMMCFdhbmdZaWZ1MR8wHQYJ
KoZIhvcNAQkBFhB5aWZ1LndAd3VzdGwuZWR1MB4XDTE4MTIwMTA0MjQ1MFoXDTE4
MTIzMTA0MjQ1MFowgYExCzAJBgNVBAYTAkNOMRAwDgYDVQQIDAdCZW1qaW5nMRAw
DgYDVQQHDAdCZW1qaW5nMQwwCgYDVQQKDANXU1YxDDAKBgNVBAsMA1dZRjERMA8G
A1UEAwwIV2FuZ11pZnUxHzAdBgkqhkiG9w0BCQEWEH1pZnUud0B3dXN0bC51ZHUw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJNyLsrwv7mjODR16zy+EP
b20R1Qy8kYXQz64GcT1ZhA001baq9S39I7cGgCwCkL0BN1qEPYaBPreYAansVGEW
511//Nk5DnhDhR/teGRR42V0KMsJIwAIz90K4UxuwdhYe1088k8BsBIRq1m0grpv
FV/Zg/but2evCOwHtNs3ta3WwO+oyrSFGjFVjSAQJDz/khIcDbYTIGvfW5o9UQJX
8oKzKRCWdPzr19Sh5CdJXOdVsZ1ayOzCfNDzmzJRiC6SUpP8MJm4ZM/YXZUHvMiK
+O/EbL+n8IM6Z2KGmhxqy28kVXVfxnD+hXdWNPRbCC3yFB9MWWhYGozSpWk1vhRv
AgMBAAGjUzBRMB0GA1UdDgQWBBQpZ0PSuvma20xph03VZC1pKu/+NjAfBgNVHSME
GDAWgBQpZ0PSuvma20xph03VZC1pKu/+NjAPBgNVHRMBAf8EBTADAQH/MA0GCSqG
SIb3DQEBCwUAA4IBAQCpegLgJITIKSKABTNxSfgDkETSroimuazbT6ejT0gy+rc3
5yCqMg2zG9iO+mu2X6cU3ptmncm4ufYHXcMLxyCJ5zhg8vU0QVUsFVeQ+618CJ3p
sOw9kiEgYFd1WnSxbSIf2NR3GaxrMUc5xkMfcE8wjp26tZ1OqYLLgdGK2kTDIb1y
vQr8rndWcp7PgcH9WngaYdOTLTt7vQyVONq6n21jGzZmyUx4ZL571ELjyENX1DLC
z1NZYjsuPGppCVb4a2m1KfVcvIZV0OVttS9rhUMSVIx9r1zEiMMb5CdUcExyzI7p
NPSzuYOz1zNszAnpmgbn01/cU8zxIVpX0oryJEUZ
-----END CERTIFICATE-----

2 Creating a Certificate for SEEDPKILab2018.com

2.1 Generate public/private key pair

```
root@LunaEx:~# openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:bd:be:20:74:5d:ce:48:81:bb:dd:d0:25:bd:83:
    aa:50:da:57:56:a0:a5:7f:a6:af:7e:87:71:3d:49:
    ec:4a:9c:f7:e8:be:61:6f:ae:83:40:90:b8:8e:4b:
    53:03:00:70:5a:54:8e:c2:c9:ba:7b:be:c9:67:c2:
    88:ea:04:c9:56:f7:01:db:7b:d5:85:3a:53:e7:33:
    9b:ac:3d:8d:5b:de:81:62:c2:bd:23:ec:5a:8d:ec:
    72:38:94:ab:39:91:bf:88:bf:68:d4:81:80:76:64:
    ad:1e:a2:05:db:10:84:3b:d5:66:0b:ee:57:65:9b:
    0c:8d:8a:11:10:4f:13:f8:bf
publicExponent: 65537 (0x10001)
privateExponent:
    00:a1:81:7c:4e:90:aa:4d:bd:60:13:e6:60:b9:77:
    a1:39:41:20:a6:74:07:6b:28:8e:a8:bc:d0:fe:c2:
    35:87:2d:25:37:cf:15:50:e2:d2:85:da:a9:bd:35:
    10:6b:b5:ab:ec:b7:9c:ec:e0:99:03:4b:da:53:9f:
    9a:ba:d7:68:28:4e:c5:83:dc:65:dc:a5:a5:51:dc:
    1c:22:05:31:6f:2a:e0:f4:26:99:bb:7a:1f:6b:ad:
    9b:18:2c:3f:77:c7:2d:d2:d5:cf:2c:df:c1:4d:b2:
    50:fa:22:ca:b2:10:93:ce:31:6b:cf:58:83:d6:da:
    57:58:c0:da:60:eb:57:18:c1
prime1:
    00:e0:65:37:0e:b1:62:b9:e8:f6:ee:fd:85:de:46:
    41:b2:98:51:f1:27:cb:7b:af:c3:d8:46:43:f7:43:
    cc:01:1a:46:0c:95:85:26:51:c0:82:fa:16:f6:d3:
    9e:f8:c3:ab:d7:60:26:e1:44:23:ea:88:eb:be:3c:
    e4:fa:40:1e:db
prime2:
    00:d8:77:7a:03:95:50:f6:d8:4f:17:5c:1c:99:b5:
    83:d9:3b:6a:e0:b8:07:9d:f5:2e:19:47:cb:50:d2:
    80:5e:49:48:ff:1b:1b:be:18:82:c2:ae:d3:01:44:
    20:df:97:4d:7b:21:c1:a3:cd:e8:98:66:e8:81:2d:
    43:7f:be:b8:ed
exponent1:
    7a:8d:ac:f9:40:56:2c:35:19:10:43:b4:66:46:36:
    c1:64:c1:74:15:08:e4:3f:85:95:cc:22:78:9c:35:
    81:f0:a8:8b:5c:ea:00:98:ab:ac:9d:0c:07:b8:62:
    5d:78:f8:94:43:76:58:97:8f:8a:1b:47:ad:79:b2:
    91:1e:8d:fb
exponent2:
    2c:c7:42:59:3d:69:1b:37:11:dd:5e:33:98:64:61:
    1a:ed:dc:a5:11:cc:99:93:5f:6e:e1:58:20:a6:fa:
    e1:06:3d:f0:6f:b6:24:73:c3:90:ec:43:3f:ee:cc:
    f2:13:c5:76:64:3c:3f:5b:57:f3:36:ce:7f:f2:52:
    15:39:e9:dd
coefficient:
    3f:d3:2a:b6:90:55:8a:a2:73:73:de:59:8f:a4:40:
    80:ac:c7:7d:73:a8:8c:da:2e:fc:59:1a:bb:6d:0e:
    a2:c6:3b:b2:da:a1:5b:de:2d:ea:a4:42:cf:90:f6:
    03:3c:d5:a9:f3:f7:f5:57:25:83:dd:1f:ed:c0:d9:
    69:ca:65:63
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC9viB0Xc5Igbvd0CW9g6pQ2ldWoKV/pq9+h3E9SexKnPfovmFv
roNAkLiOS1MDAHBaVI7Cybp7vslnwojqBMlW9wHbe9WFOlPnM5usPY1b3oFiwr0j
7FqN7HI4lKs5kb+Iv2jUgYB2ZK0eogXbEIQ71WYL7ldlmwyNihEQTxP4vwIDAQAB
AoGBAKGBfE6Qgk29YBPmYLl3oTlBIKZ0B2sojgi80P7CNYctJTfPFVDi0oXaqb01
```

2.2   Generate a Certificate Signing Request (CSR)

```
root@LunaEx:~# openssl req -new -key server.key -out server.csr -config ./demoCA/openssl.cnf
Enter pass phrase for server.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]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2018.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:zxsaqw21
An optional company name []:
```

2.3 Generating Ceertificates

```
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2018.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:zxsaqw21
An optional company name []:
root@LunaEx:~# openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config ./demoCA/openssl.cnf
Using configuration from ./demoCA/openssl.cnf
Enter pass phrase for ca.key:
ca: ./demoCA/newcerts is not a directory
./demoCA/newcerts: No such file or directory
root@LunaEx:~# mkdir ./demoCA/newcerts
root@LunaEx: # openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config ./demoCA/openssl.cnf
Using configuration from ./demoCA/openssl.cnf
Enter pass phrase for ca.key:
Can't open ./demoCA/index.txt.attr for reading, No such file or directory
140185064968640:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:74:fopen('./de
moCA/index.txt.attr','r')
140185064968640: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 countryName field is different between
CA certificate (CN) and the request (AU)
root@LunaEx: # vim ./demoCA/openssl.cnf
root@LunaEx: # openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config ./demoCA/openssl.cnf
Using configuration from ./demoCA/openssl.cnf
Enter pass phrase for ca.key:
Can't open ./demoCA/index.txt.attr for reading, No such file or directory
140408468148672:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:74:fopen('./de
moCA/index.txt.attr','r')
140408468148672: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
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Dec  1 04:39:17 2018 GMT
            Not After : Dec  1 04:39:17 2019 GMT
        Subject:
            countryName               = AU
            stateOrProvinceName       = Some-State
            organizationName          = Internet Widgits Pty Ltd
            commonName                = SEEDPKILab2018.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                FD:23:9B:35:9F:98:20:34:8E:6E:E3:22:93:AE:58:3E:A1:E1:AC:23
            X509v3 Authority Key Identifier:
                keyid:29:67:43:D2:BA:F9:9A:DB:4C:69:87:4D:D5:64:2D:69:2A:EF:FE:36

Certificate is to be certified until Dec  1 04:39:17 2019 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
root@LunaEx: #
```

```
policy            = policy_anything

# For the CA policy
[ policy_match ]
countryName            = match
stateOrProvinceName    = match
organizationName       = match
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional

# For the 'anything' policy
# At this point in time, you must list all acceptable 'object'
# types.
[ policy_anything ]
countryName            = optional
stateOrProvinceName    = optional
localityName           = optional
organizationName       = optional
```

3 Deploying Certificate in an HTTPS Web Server

3.1 Configuring DNS

```
# This file is automatically generated by WSL based on the
# %WINDIR%\System32\drivers\etc\hosts. Modifications to thi
127.0.0.1        localhost
127.0.1.1        LunaEx.localdomain        LunaEx
127.0.0.1        SEEDPKILab2018.com
1

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

3.2 Configuring the web server

since I don't have an gui ubuntu. I moved my work to my PC.

```
PS D:\Code\demoCA> openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
```
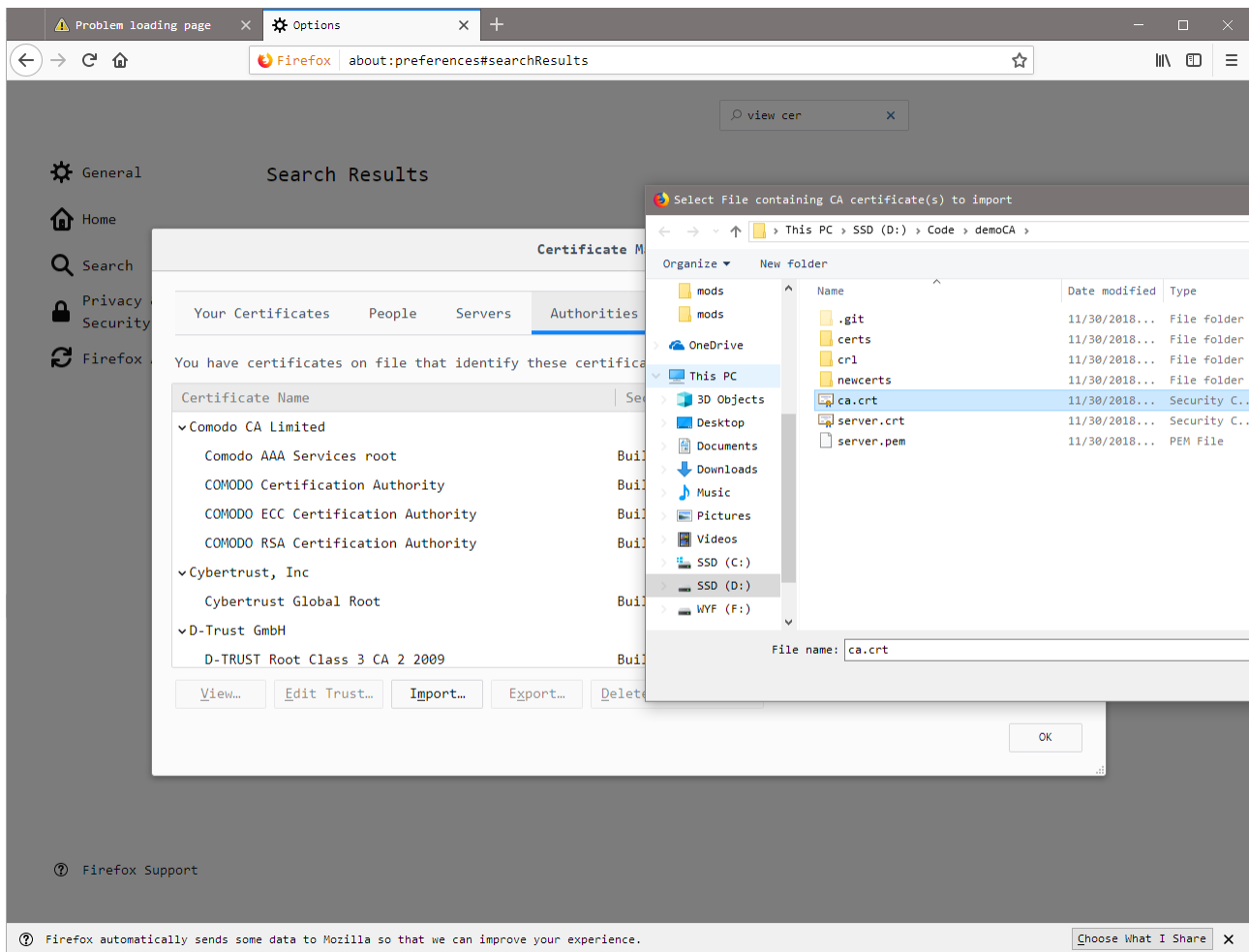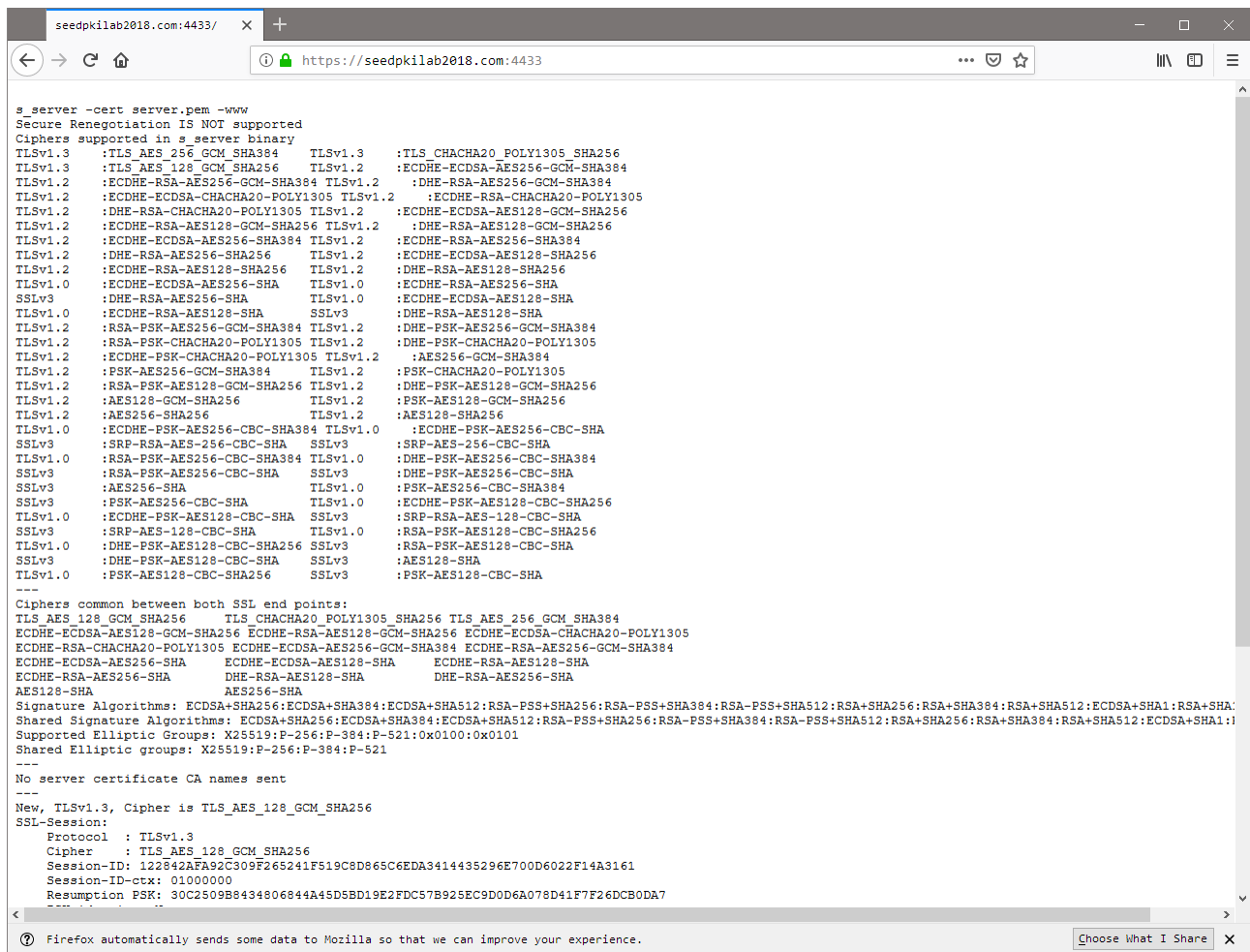
```
@echo off

echo.  >> %windir%/system32/drivers/etc/hosts
echo  127.0.0.1 SEEDPKILab2018.com    >> %windir%/system32/drivers/etc/hosts
```

3.3 Getting the browser to accept our CA certificate

3.4 Testing our HTTPS website

but when I try localhost, I can't see the page