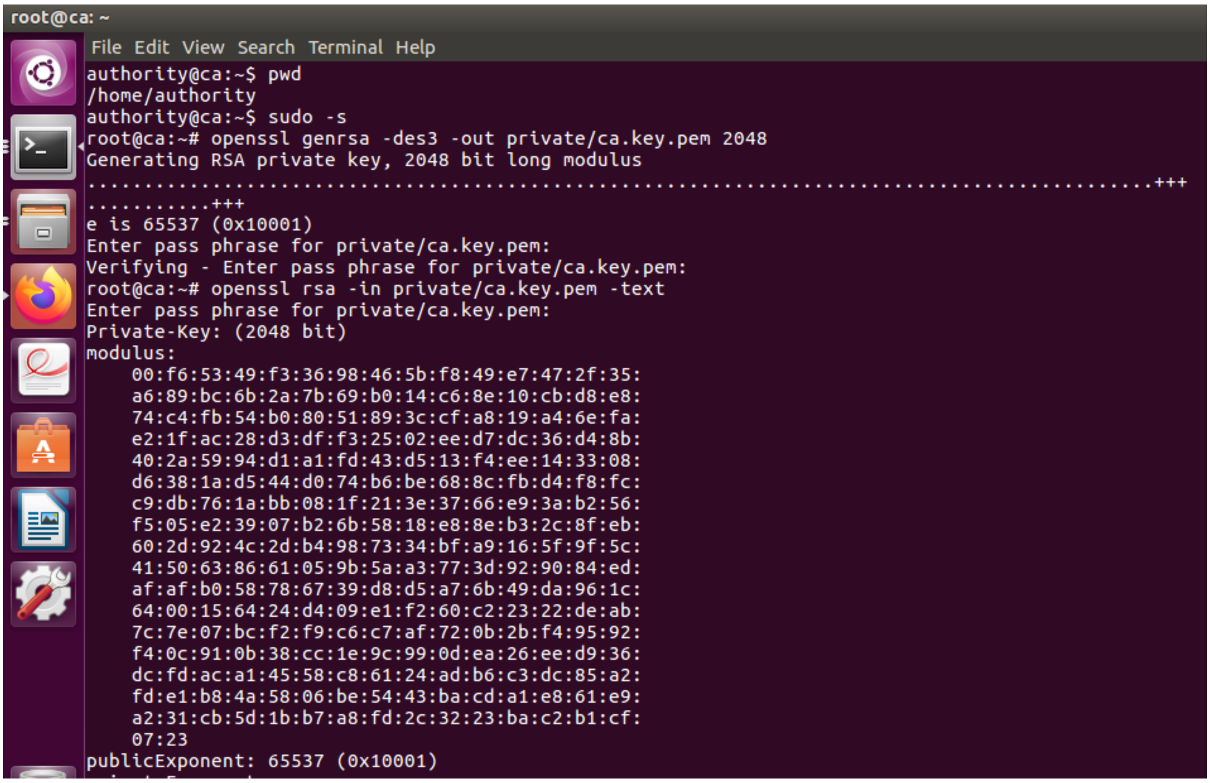
Electronic Certificate Lab

Malshani RANCHA GODAGE

Generate private and public key pair for Certification Authority computer by running the command “openssl genrsa -des3 -out private/ca.key.pem 2048” in the /home/authority directory. Before generate I entered to administrative mode. Then I entered the command “openssl rsa -in private/ca.key.pem -text” to access the keys.

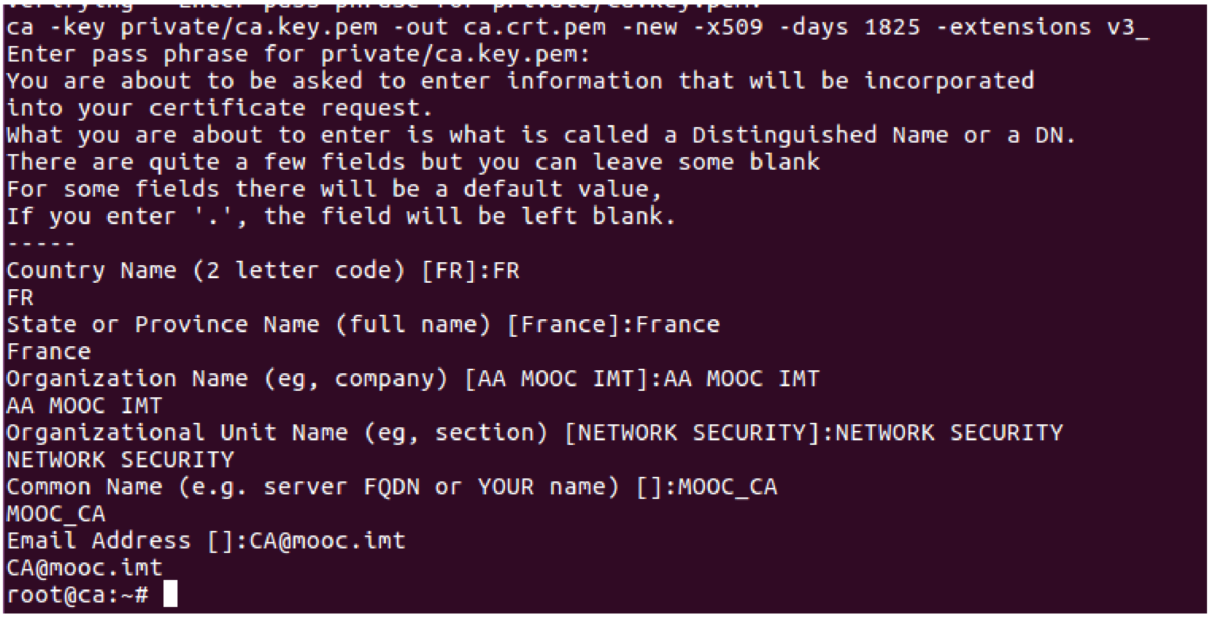


```
authority@ca:~$ pwd
/home/authority
authority@ca:~$ sudo -s
root@ca:~# openssl genrsa -des3 -out private/ca.key.pem 2048
Generating RSA private key, 2048 bit long modulus
..............................................................................................+++
...........+++
e is 65537 (0x10001)
Enter pass phrase for private/ca.key.pem:
Verifying - Enter pass phrase for private/ca.key.pem:
root@ca:~# openssl rsa -in private/ca.key.pem -text
Enter pass phrase for private/ca.key.pem:
Private-Key: (2048 bit)
modulus:
    00:f6:53:49:f3:36:98:46:5b:f8:49:e7:47:2f:35:
    a6:89:bc:6b:2a:7b:69:b0:14:c6:8e:10:cb:d8:e8:
    74:c4:fb:54:b0:80:51:89:3c:cf:a8:19:a4:6e:fa:
    e2:1f:ac:28:d3:df:f3:25:02:ee:d7:dc:36:d4:8b:
    40:2a:59:94:d1:a1:fd:43:d5:13:f4:ee:14:33:08:
    d6:38:1a:d5:44:d0:74:b6:be:68:8c:fb:d4:f8:fc:
    c9:db:76:1a:bb:08:1f:21:3e:37:66:e9:3a:b2:56:
    f5:05:e2:39:07:b2:6b:58:18:e8:8e:b3:2c:8f:eb:
    60:2d:92:4c:2d:b4:98:73:34:bf:a9:16:5f:9f:5c:
    41:50:63:86:61:05:9b:5a:a3:77:3d:92:90:84:ed:
    af:af:b0:58:78:67:39:d8:d5:a7:6b:49:da:96:1c:
    64:00:15:64:24:d4:09:e1:f2:60:c2:23:22:de:ab:
    7c:7e:07:bc:f2:f9:c6:c7:af:72:0b:2b:f4:95:92:
    f4:0c:91:0b:38:cc:1e:9c:99:0d:ea:26:ee:d9:36:
    dc:fd:ac:a1:45:58:c8:61:24:ad:b6:c3:dc:85:a2:
    fd:e1:b8:4a:58:06:be:54:43:ba:cd:a1:e8:61:e9:
    a2:31:cb:5d:1b:b7:a8:fd:2c:32:23:ba:c2:b1:cf:
    07:23
publicExponent: 65537 (0x10001)
```

Q1: Is it possible to access to that key? Explain.

Yes because “openssl rsa -in private/ca.key.pem –text” command shows elements of keys I just generated.

Then I created certificate for Certificate Authority computer by “openssl req -config openssl.cnf -new -x509 -days 1825 -extensions v3_ca -key private/ca.key.pem -out ca.crt.pem”. I filled field names for country, state, organization, common name and email. Then I listed the files and found out ca.cert.pem.

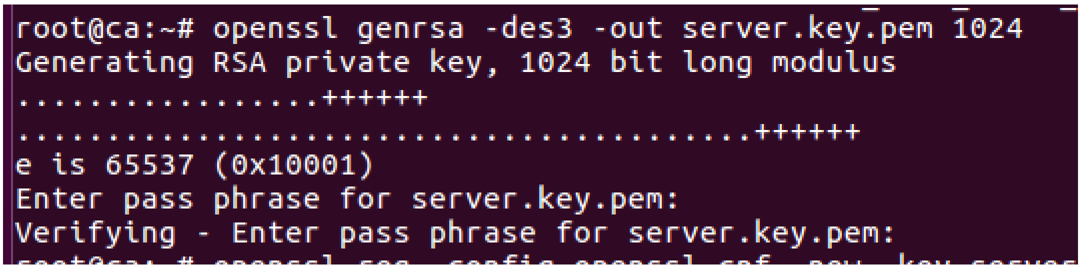


```
Verifying - Enter pass phrase for private/ca.key.pem:
ca -key private/ca.key.pem -out ca.crt.pem -new -x509 -days 1825 -extensions v3_
Enter pass phrase for private/ca.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about 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) [FR]:FR
FR
State or Province Name (full name) [France]:France
France
Organization Name (eg, company) [AA MOOC IMT]:AA MOOC IMT
AA MOOC IMT
Organizational Unit Name (eg, section) [NETWORK SECURITY]:NETWORK SECURITY
NETWORK SECURITY
Common Name (e.g. server FQDN or YOUR name) []:MOOC_CA
MOOC_CA
Email Address []:CA@mooc.imt
CA@mooc.imt
root@ca:~# 
```

Q2: Why do you need to enter a passphrase when executing that command?

a) To prove that we own the private key used.

Then I generated private and public key pairs for Server computer.

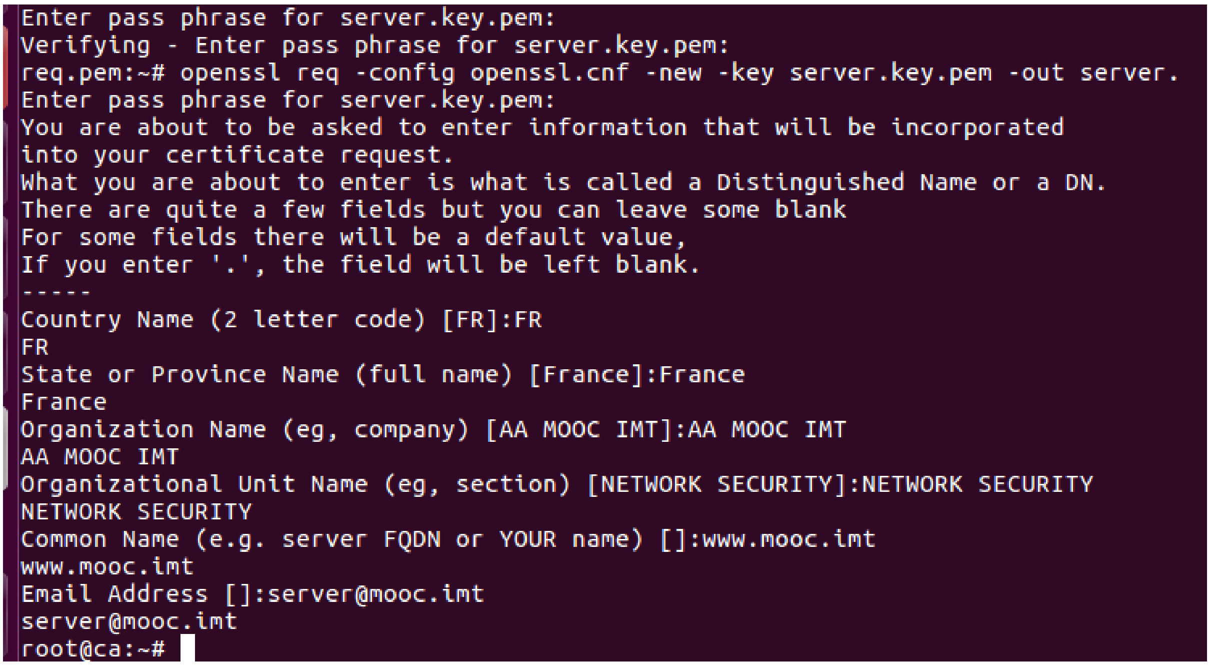


```
root@ca:~# openssl genrsa -des3 -out server.key.pem 1024
Generating RSA private key, 1024 bit long modulus
.................++++++
..........................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key.pem:
Verifying - Enter pass phrase for server.key.pem:
root@ca:~# openssl req -config openssl.cnf -new -key server
```

Q3: What does parameter 1024 means in the previous command?

a) Number of bits of the key pair

Then I generated certificate “server.cert.pem” for Server computer by entering “# openssl ca -config openssl.cnf -in server.req.pem -out server.crt.pem -extensions server” command.

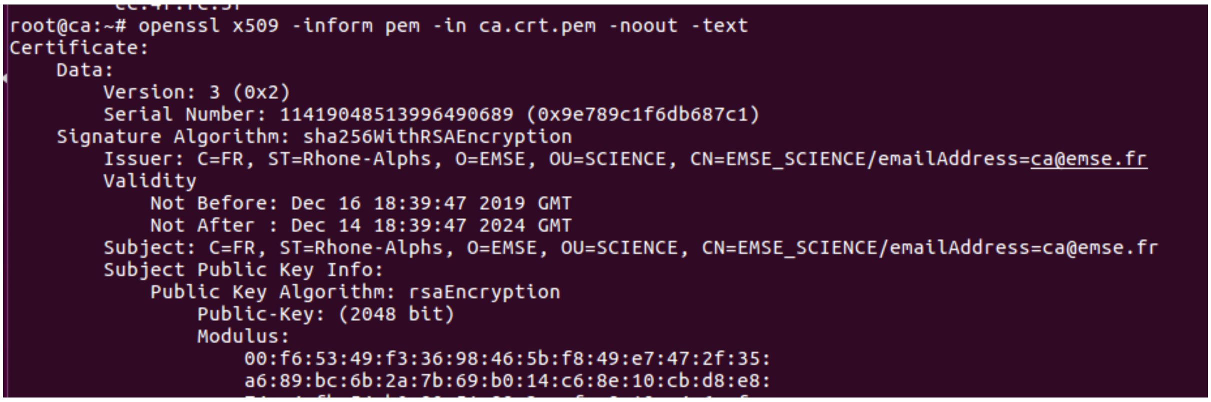


```
Enter pass phrase for server.key.pem:
Verifying - Enter pass phrase for server.key.pem:
req.pem:~# openssl req -config openssl.cnf -new -key server.key.pem -out server.
Enter pass phrase for server.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate 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) [FR]:FR
FR
State or Province Name (full name) [France]:France
France
Organization Name (eg, company) [AA MOOC IMT]:AA MOOC IMT
AA MOOC IMT
Organizational Unit Name (eg, section) [NETWORK SECURITY]:NETWORK SECURITY
NETWORK SECURITY
Common Name (e.g. server FQDN or YOUR name) []:www.mooc.imt
www.mooc.imt
Email Address []:server@mooc.imt
server@mooc.imt
root@ca:~# 
```

Q4: Which elements can be found in an electronic certificate of a machine?

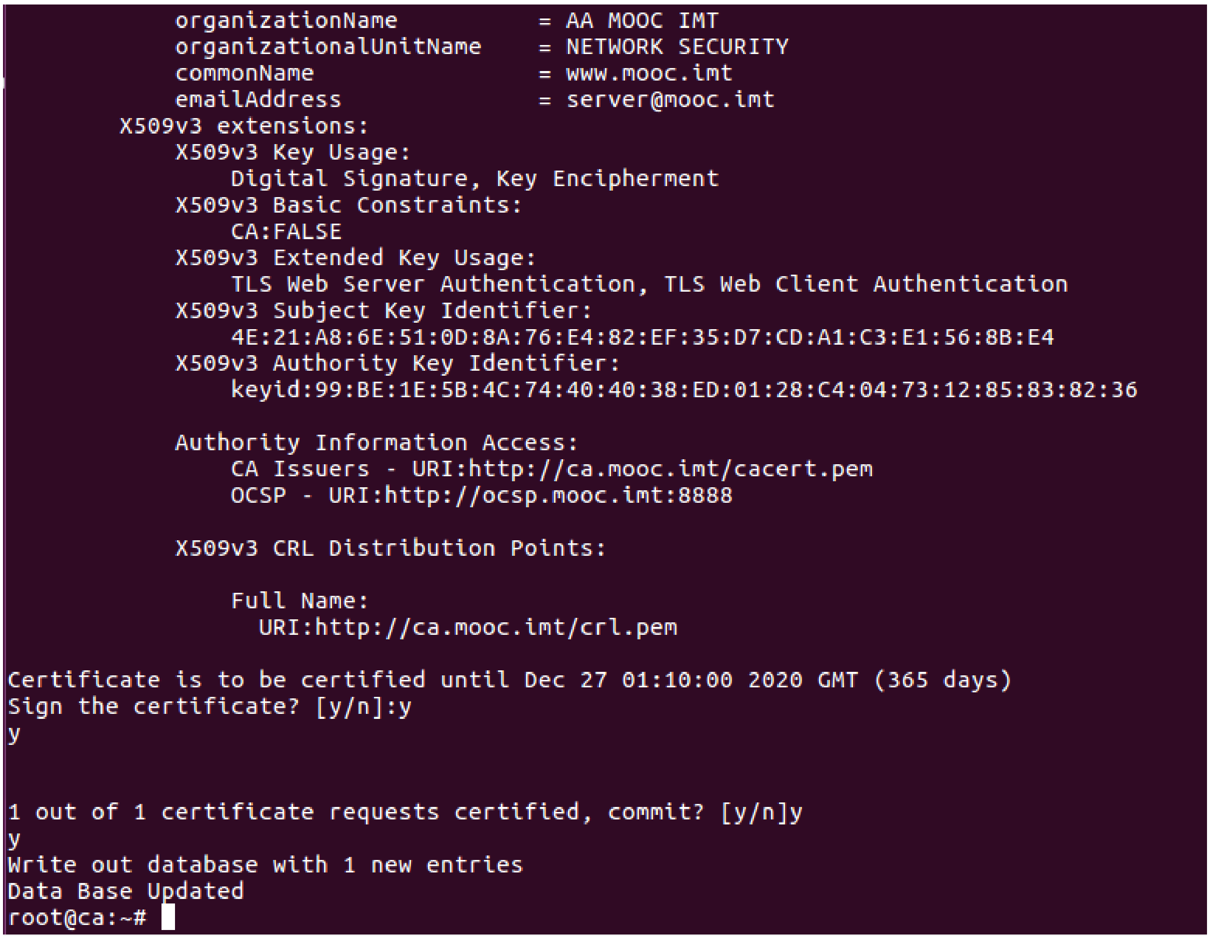
a) The name, URL of the machine. YES
c) The signature of a third party (certification authority). YES
d) The validity period of the certificate. YES

then I created certificate for server www.mooc.imt

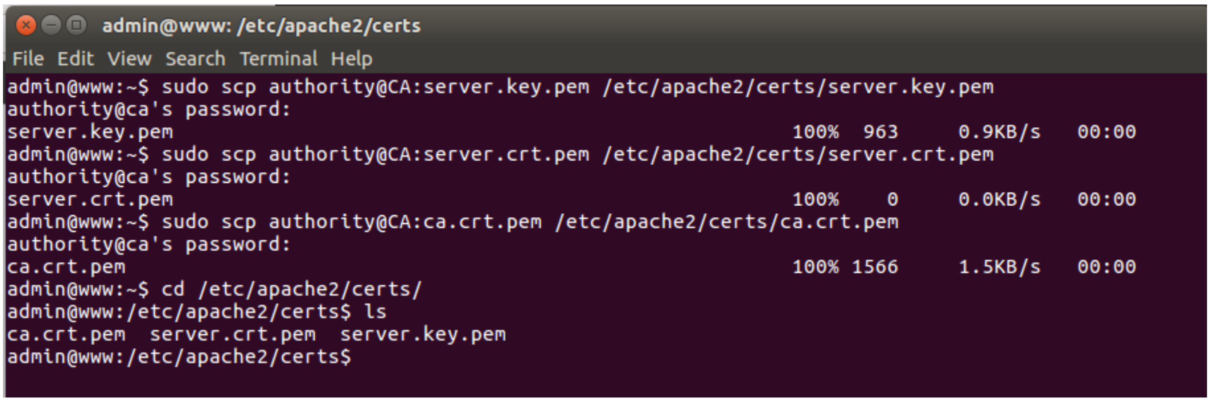


```
root@ca:~# openssl x509 -inform pem -in ca.crt.pem -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11419048513996490689 (0x9e789c1f6db687c1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, ST=Rhone-Alphs, O=EMSE, OU=SCIENCE, CN=EMSE_SCIENCE/emailAddress=ca@emse.fr
        Validity
            Not Before: Dec 16 18:39:47 2019 GMT
            Not After : Dec 14 18:39:47 2024 GMT
        Subject: C=FR, ST=Rhone-Alphs, O=EMSE, OU=SCIENCE, CN=EMSE_SCIENCE/emailAddress=ca@emse.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f6:53:49:f3:36:98:46:5b:f8:49:e7:47:2f:35:
                    a6:89:bc:6b:2a:7b:69:b0:14:c6:8e:10:cb:d8:e8:
```

Then I copied the server's certificate, private key as well as the CA certificate which can be found in machine CA in the machine hosting to the Server computer.



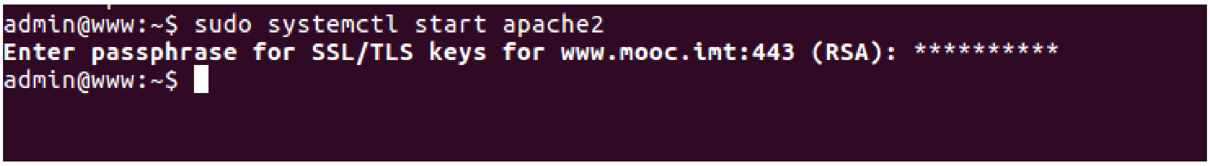
```
            organizationName          = AA MOOC IMT
            organizationalUnitName    = NETWORK SECURITY
            commonName                = www.mooc.imt
            emailAddress              = server@mooc.imt
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Subject Key Identifier:
                4E:21:A8:6E:51:0D:8A:76:E4:82:EF:35:D7:CD:A1:C3:E1:56:8B:E4
            X509v3 Authority Key Identifier:
                keyid:99:BE:1E:5B:4C:74:40:40:38:ED:01:28:C4:04:73:12:85:83:82:36

            Authority Information Access:
                CA Issuers - URI:http://ca.mooc.imt/cacert.pem
                OCSP - URI:http://ocsp.mooc.imt:8888

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://ca.mooc.imt/crl.pem

Certificate is to be certified until Dec 27 01:10:00 2020 GMT (365 days)
Sign the certificate? [y/n]:y
y


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



admin@www: /etc/apache2/certs
File Edit View Search Terminal Help

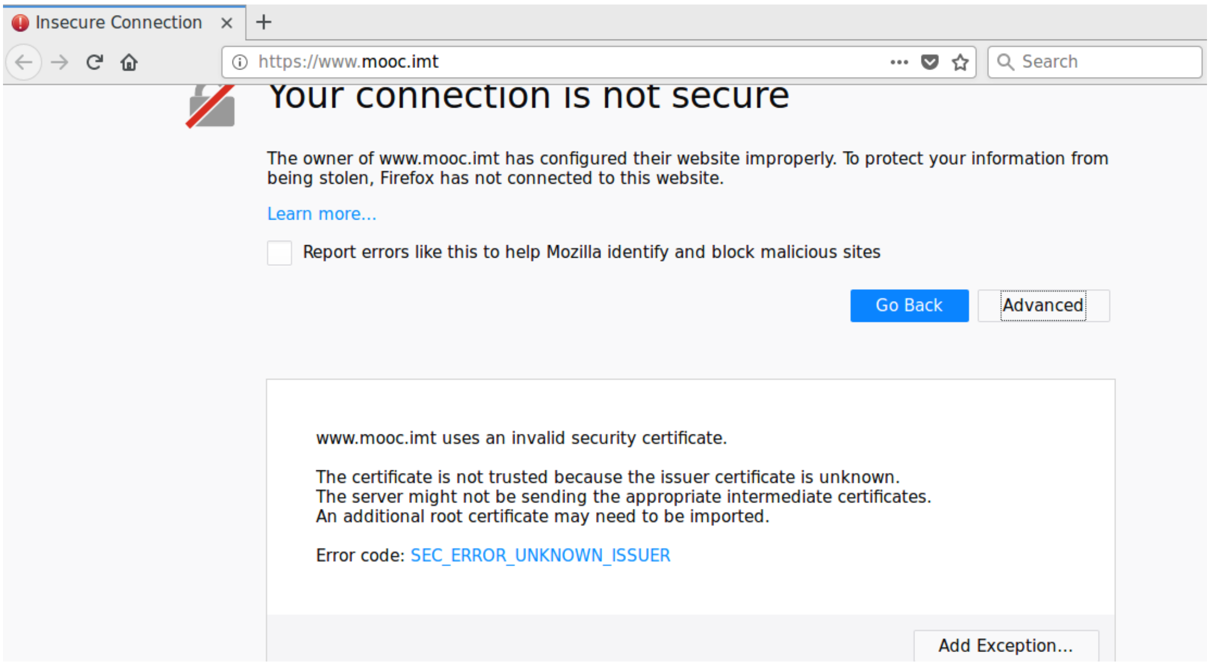
```
admin@www:~$ sudo scp authority@CA:server.key.pem /etc/apache2/certs/server.key.pem
authority@ca's password:
server.key.pem                                    100%  963     0.9KB/s   00:00
admin@www:~$ sudo scp authority@CA:server.crt.pem /etc/apache2/certs/server.crt.pem
authority@ca's password:
server.crt.pem                                    100%    0     0.0KB/s   00:00
admin@www:~$ sudo scp authority@CA:ca.crt.pem /etc/apache2/certs/ca.crt.pem
authority@ca's password:
ca.crt.pem                                        100% 1566     1.5KB/s   00:00
admin@www:~$ cd /etc/apache2/certs/
admin@www:/etc/apache2/certs$ ls
ca.crt.pem  server.crt.pem  server.key.pem
admin@www:/etc/apache2/certs$
```

All three files are copied perfectly, so I launched web service on machine WWW.



```
admin@www:~$ sudo systemctl start apache2
Enter passphrase for SSL/TLS keys for www.mooc.imt:443 (RSA): **********
admin@www:~$
```

Then I run Firefox in brest computer by typing the command firefox &. Then I entered https://www.mooc.imt in the url field and found out following message.



Your connection is not secure

The owner of www.mooc.imt has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

www.mooc.imt uses an invalid security certificate.

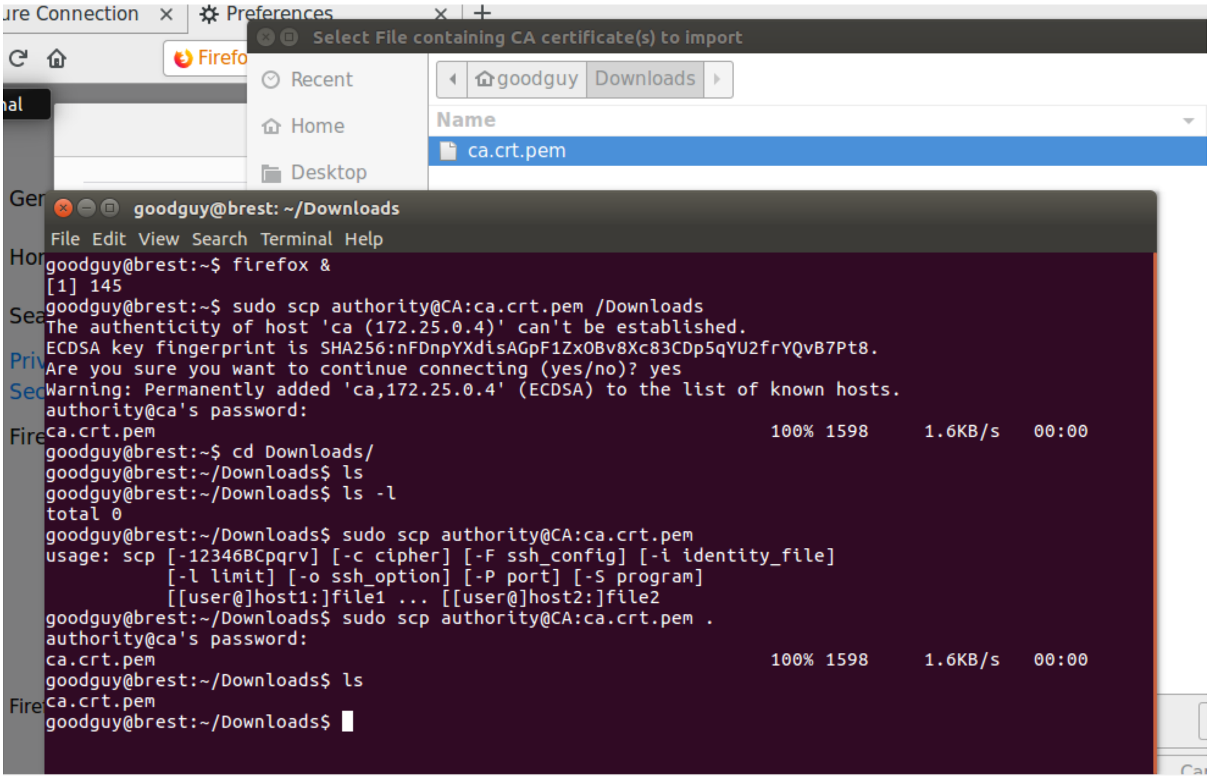
The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Q5: What is the meaning of these alerts ?

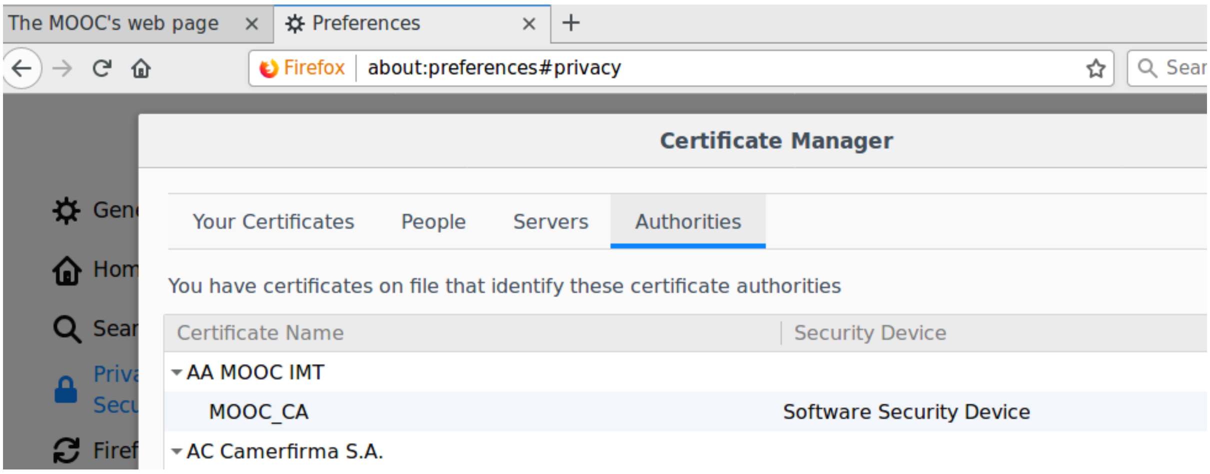
c) The certificate can not be verified. RIGHT

No downloaded the certificate to Downloads folder of Brest computer and imported it into firefox browser.


ure Connection
Preferences
Select File containing CA certificate(s) to import
Recent
Home
Desktop
goodguy
Downloads
Name
ca.crt.pem
goodguy@brest: ~/Downloads
File Edit View Search Terminal Help

```
goodguy@brest:~$ firefox &
[1] 145
goodguy@brest:~$ sudo scp authority@CA:ca.crt.pem /Downloads
The authenticity of host 'ca (172.25.0.4)' can't be established.
ECDSA key fingerprint is SHA256:nFDnpYXdisAGpF1ZxOBv8Xc83CDp5qYU2frYQvB7Pt8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ca,172.25.0.4' (ECDSA) to the list of known hosts.
authority@ca's password:
ca.crt.pem                                    100% 1598     1.6KB/s   00:00
goodguy@brest:~$ cd Downloads/
goodguy@brest:~/Downloads$ ls
goodguy@brest:~/Downloads$ ls -l
total 0
goodguy@brest:~/Downloads$ sudo scp authority@CA:ca.crt.pem
usage: scp [-12346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program]
           [[user@]host1:]file1 ... [[user@]host2:]file2
goodguy@brest:~/Downloads$ sudo scp authority@CA:ca.crt.pem .
authority@ca's password:
ca.crt.pem                                    100% 1598     1.6KB/s   00:00
goodguy@brest:~/Downloads$ ls
ca.crt.pem
goodguy@brest:~/Downloads$ 
```

Once I added the certificate, I could visit the web page. I added the certificate to Marseille computer too.



Certificate Manager

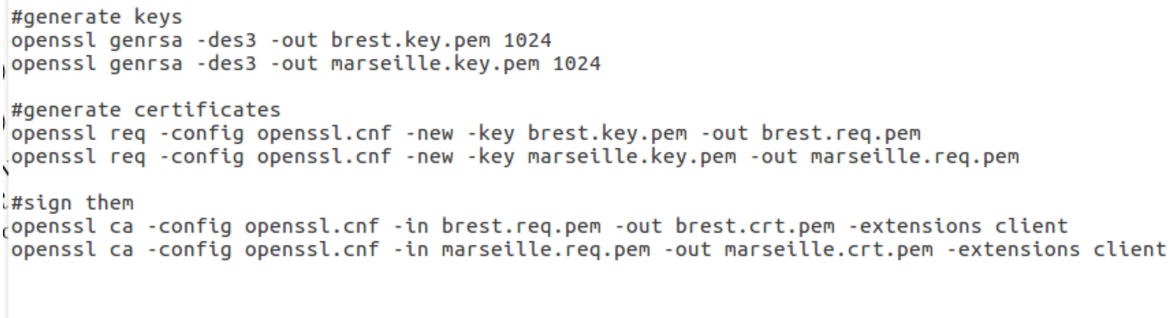
You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AA MOOC IMT	
MOOC_CA	Software Security Device
AC Camerfirma S.A.	

Q6: What can you deduce?

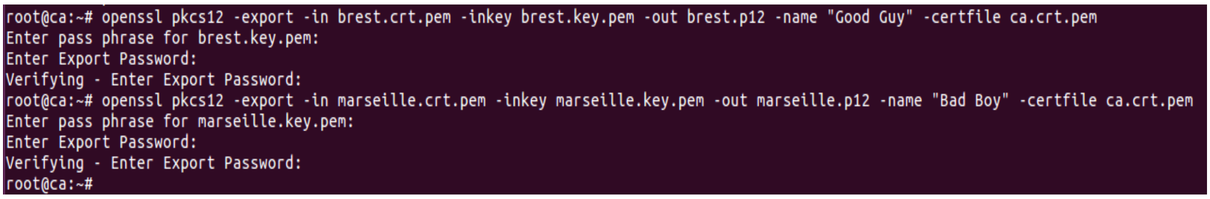
c) My browser is able to check the server's certificate as it owns the server's certificate

Then I generate continue the same process for brest and Marseille computers with following commands and by entering the necessary details.



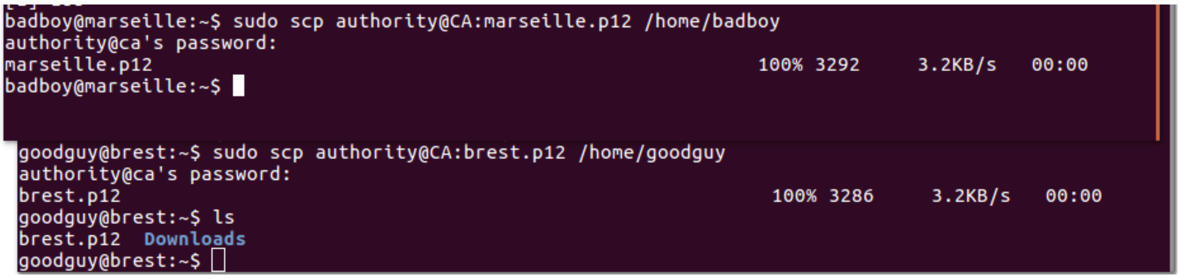
```
#generate keys
openssl genrsa -des3 -out brest.key.pem 1024
openssl genrsa -des3 -out marseille.key.pem 1024

#generate certificates
openssl req -config openssl.cnf -new -key brest.key.pem -out brest.req.pem
openssl req -config openssl.cnf -new -key marseille.key.pem -out marseille.req.pem

#sign them
openssl ca -config openssl.cnf -in brest.req.pem -out brest.crt.pem -extensions client
openssl ca -config openssl.cnf -in marseille.req.pem -out marseille.crt.pem -extensions client
```

Before add these certificates and private keys to the browser I'm going to put them in a secure container as a PKCS#12 format file.



```
root@ca:~# openssl pkcs12 -export -in brest.crt.pem -inkey brest.key.pem -out brest.p12 -name "Good Guy" -certfile ca.crt.pem
Enter pass phrase for brest.key.pem:
Enter Export Password:
Verifying - Enter Export Password:
root@ca:~# openssl pkcs12 -export -in marseille.crt.pem -inkey marseille.key.pem -out marseille.p12 -name "Bad Boy" -certfile ca.crt.pem
Enter pass phrase for marseille.key.pem:
Enter Export Password:
Verifying - Enter Export Password:
root@ca:~#
```

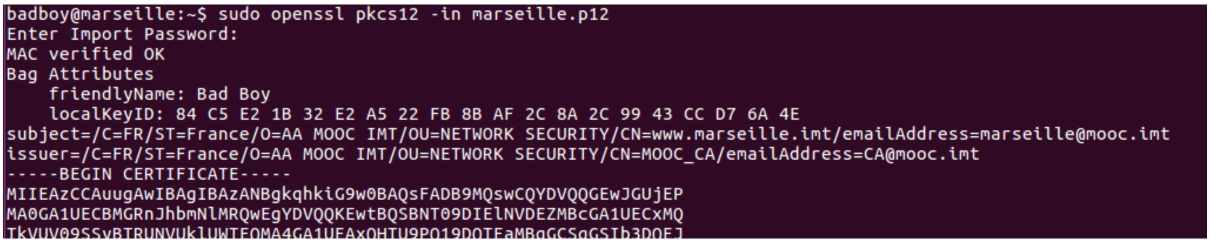
Then I copied both files into corresponding computers, by entering following commands.



```
badboy@marseille:~$ sudo scp authority@CA:marseille.p12 /home/badboy
authority@ca's password:
marseille.p12                                      100% 3292     3.2KB/s   00:00
badboy@marseille:~$
```

```
goodguy@brest:~$ sudo scp authority@CA:brest.p12 /home/goodguy
authority@ca's password:
brest.p12                                          100% 3286     3.2KB/s   00:00
goodguy@brest:~$ ls
brest.p12  Downloads
goodguy@brest:~$
```

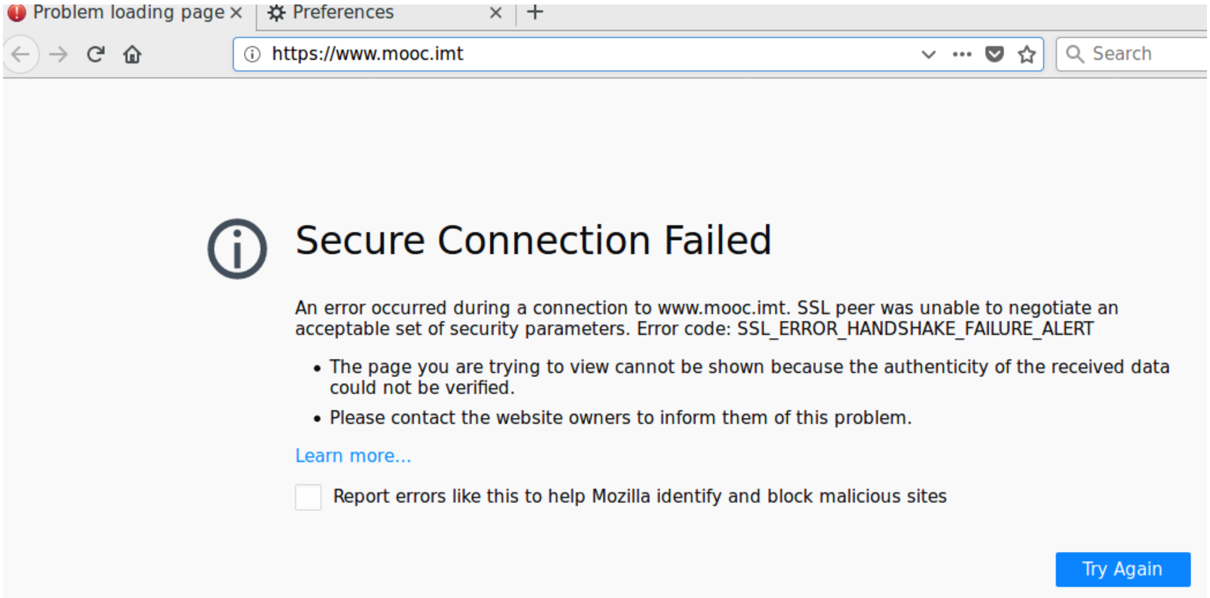
Then I viewed the content of key and certificate.



```
badboy@marseille:~$ sudo openssl pkcs12 -in marseille.p12
Enter Import Password:
MAC verified OK
Bag Attributes
    friendlyName: Bad Boy
    localKeyID: 84 C5 E2 1B 32 E2 A5 22 FB 8B AF 2C 8A 2C 99 43 CC D7 6A 4E
subject=/C=FR/ST=France/O=AA MOOC IMT/OU=NETWORK SECURITY/CN=www.marseille.imt/emailAddress=marseille@mooc.imt
issuer=/C=FR/ST=France/O=AA MOOC IMT/OU=NETWORK SECURITY/CN=MOOC_CA/emailAddress=CA@mooc.imt
-----BEGIN CERTIFICATE-----
MIIEAzCCAuugAwIBAgIBAzANBgkqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJGUjEP
MA0GA1UECBMGRnJhbmNlMRQwEgYDVQQKEwtBQSBNT09DIElNVDEZMBcGA1UECxMQ
TkVUV09SSyBTRUNVUklUWTEOMA4GA1UEAxOHTU9PQ19DQTEaMBgGCSqGSIb3DQEJ
```

Q7: Is the private key in cleartext? b) No

Then I updated /etc/apache2/sites-enabled/default-ssl.conf file of www computer, as described in the lab sheet with administrative permission. Then I restarted the apache server. Then I open firefox in both brest and marseile computers to access the website, they gave me an error page.



Secure Connection Failed

An error occurred during a connection to www.mooc.imt. SSL peer was unable to negotiate an acceptable set of security parameters. Error code: SSL_ERROR_HANDSHAKE_FAILURE_ALERT

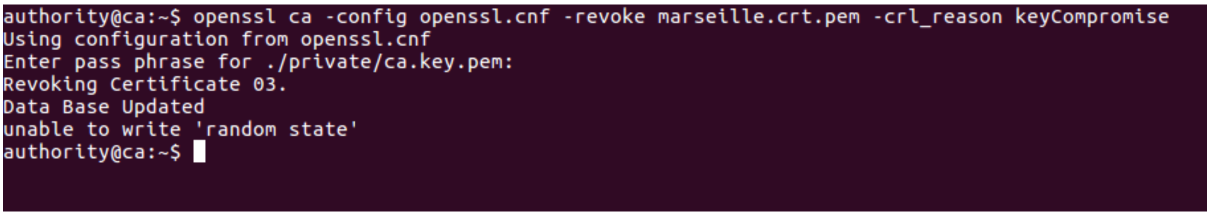
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...

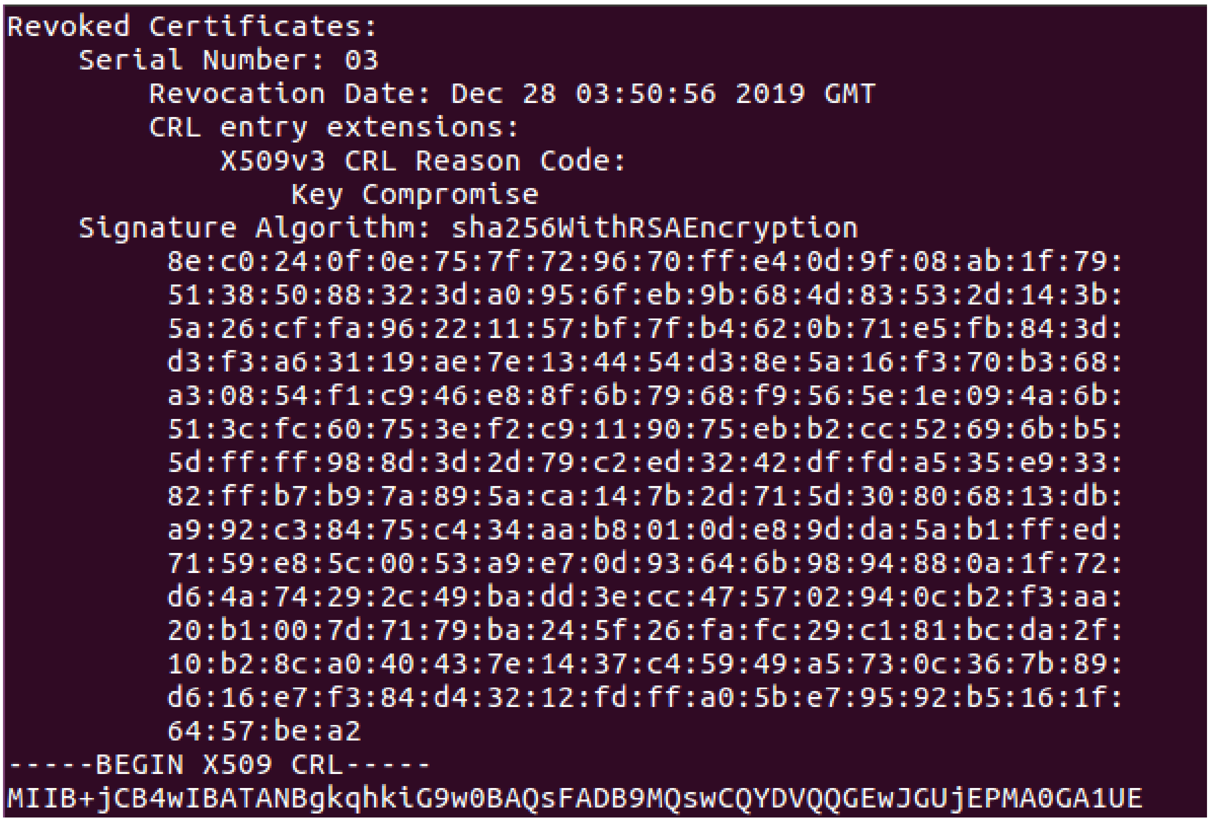
□ Report errors like this to help Mozilla identify and block malicious sites

Q9: What can be observed? a) I cannot connect

Certificate revocation for Marseille computer as follows.



```
authority@ca:~$ openssl ca -config openssl.cnf -revoke marseille.crt.pem -crl_reason keyCompromise
Using configuration from openssl.cnf
Enter pass phrase for ./private/ca.key.pem:
Revoking Certificate 03.
Data Base Updated
unable to write 'random state'
authority@ca:~$
```



```
Revoked Certificates:
    Serial Number: 03
        Revocation Date: Dec 28 03:50:56 2019 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha256WithRSAEncryption
         8e:c0:24:0f:0e:75:7f:72:96:70:ff:e4:0d:9f:08:ab:1f:79:
         51:38:50:88:32:3d:a0:95:6f:eb:9b:68:4d:83:53:2d:14:3b:
         5a:26:cf:fa:96:22:11:57:bf:7f:b4:62:0b:71:e5:fb:84:3d:
         d3:f3:a6:31:19:ae:7e:13:44:54:d3:8e:5a:16:f3:70:b3:68:
         a3:08:54:f1:c9:46:e8:8f:6b:79:68:f9:56:5e:1e:09:4a:6b:
         51:3c:fc:60:75:3e:f2:c9:11:90:75:eb:b2:cc:52:69:6b:b5:
         5d:ff:ff:98:8d:3d:2d:79:c2:ed:32:42:df:fd:a5:35:e9:33:
         82:ff:b7:b9:7a:89:5a:ca:14:7b:2d:71:5d:30:80:68:13:db:
         a9:92:c3:84:75:c4:34:aa:b8:01:0d:e8:9d:da:5a:b1:ff:ed:
         71:59:e8:5c:00:53:a9:e7:0d:93:64:6b:98:94:88:0a:1f:72:
         d6:4a:74:29:2c:49:ba:dd:3e:cc:47:57:02:94:0c:b2:f3:aa:
         20:b1:00:7d:71:79:ba:24:5f:26:fa:fc:29:c1:81:bc:da:2f:
         10:b2:8c:a0:40:43:7e:14:37:c4:59:49:a5:73:0c:36:7b:89:
         d6:16:e7:f3:84:d4:32:12:fd:ff:a0:5b:e7:95:92:b5:16:1f:
         64:57:be:a2
-----BEGIN X509 CRL-----
MIIB+jCB4wIBATANBgkqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJGUjEPMA0GA1UE
```

Q10: What is a certificate used for? c) neither to encrypt messages, nor to verify signatures.

Q11: What can you observe? c) Revoking a certificate is not immediately taken into account.

Then I edited /etc/apache2/sites-enabled/default-ssl.conf file of www computer, as described in the lab sheet with administrative permission. Then I restarted the apache server.

Q12: What can you observe ?

b) The user badboy can no longer connect ;

e) The user goodguy can still connect

f) It is required to have a copy of the revocation list.