1. Создайте УЦ. (скриншоты в отчет)
    a. создать каталог для УЦ "ФИО_CA"

```
taiiiga@taiiiga-VirtualBox:~/kstu$ mkdir KIR_CA
```

    b. создать каталог private, разрешить доступ к этому каталогу только одному пользователю

```
taiiiga@taiiiga-VirtualBox:~/kstu$ mkdir private
taiiiga@taiiiga-VirtualBox:~/kstu$ chmod 700 private/
```

    c. создать каталог для сертификатов созданных УЦ (certs_db)

```
taiiiga@taiiiga-VirtualBox:~/kstu$ mkdir certs_db
```

    d. создайте пустой файл Index.db для базы данных УЦ

```
taiiiga@taiiiga-VirtualBox:~/kstu$ touch Index.db
```

    e. создайте пустой файл Index.db.attr для базы данных УЦ

```
taiiiga@taiiiga-VirtualBox:~/kstu$ touch Index.db.attr
```

    f. создайте пустой файл .rand для для хранения случайной последовательности

```
taiiiga@taiiiga-VirtualBox:~/kstu$ touch .rand
```

    g. создать файл для хранения серийного номера сертификатов (serial)

```
taiiiga@taiiiga-VirtualBox:~/kstu$ touch serial
```

    h. создать файл настройки центра сертификации (ФИО_CA.conf) и настроить

```
taiiiga@taiiiga-VirtualBox:~/kstu$ touch KIR_CA.conf
```

```
dir = ../
new_certs_dir = $dir/certs_db
unique_subject = no
certificate = $dir/KIR_CA.crt
database = $dir/Index.db
private_key = $dir/private/key_KIR_CA.pem
serial = $dir/serial
default_days = 189
default_md = sha512
policy = CA_CLIENT_policy
x509_extensions = CA_CLIENT_extensions
crlnumber = $dir/crlnumber
default_crl_days = 89
```

    i. в сертификат должен добавляться URL на COC

```
[crl_section]
URI.0 = http://www.httpserver.com/crl.pem
```

j. настройте HTTP сервер, что бы отдавался СОС по этому URL

```
 GNU nano 5.2                          server.conf
<VirtualHost :80>

ServerName httpserver.com
ServerAlias www.httpserver.com
ServerAdmin webmaster@localhost
DocumentRoot /var/www/httpserver.com/
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

<VirtualHost>
```

k. срок действия сертификата (суток) = последние 3 цифры из номера зачетки

```
default_days = 189
```

l. срок действия СОС (суток) = последние 2 цифры из номера зачетки `default_crl_days = 89`

m. серийный номер первого сертификата = последняя цифра из номера зачетки в шестнадцатеричном виде

9

Шестнадцатеричная система - 9.

n. задать функцию хеширования по умолчанию SHA512

```
default_md = sha512
```

o. сгенерировать закрытый ключ (4096 бит) для УЦ (key_ФИО_CA.pem) с парольной защитой, поместить его в private

```
taiiiga@taiiiga-VirtualBox:~/kstu$ openssl genrsa -out key_KIR_CA.pem -aes-256-
cbc 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................++++
.....................................................................................
.....................................................++++
e is 65537 (0x010001)
Enter pass phrase for key_KIR_CA.pem:
Verifying - Enter pass phrase for key_KIR_CA.pem:
taiiiga@taiiiga-VirtualBox:~/kstu$ sudo mv key_KIR_CA.pem /private/
mv: cannot move 'key_KIR_CA.pem' to '/private/': Not a directory
taiiiga@taiiiga-VirtualBox:~/kstu$ sudo mv key_KIR_CA.pem private/
```

p. сгенерировать запрос на сертификат УЦ с использованием ФИО_CA.conf, добавьте свои ФИО как владельца сертификата

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl req -config KIR_CA.conf -new
-sha512 -key ../private/key_KIR_CA.pem -out KIR_CA.crt
Enter pass phrase for ../private/key_KIR_CA.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) [RU]:
State or Province Name [Russia]:
Locality Name [Kazan]:
Organization Name [KSTU]:
Organizational Unit Name [728111]:
Common Name []:Khisamov Iskander Ravilevich
Email Address [iskanderkhisamov@gmail.com]:
```

q. создать самоподписанный сертификат УЦ (ФИО_CA.crt) с использованием ФИО_CA.conf

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -signkey ../private/key_
KIR_CA.pem -in KIR_CA.crt -req -days 366 -out KIR_CA.crt
Signature ok
subject=C = RU, ST = Russia, L = Kazan, O = KSTU, OU = 728111, CN = Khisamov Is
kander Ravilevich, emailAddress = iskanderkhisamov@gmail.com
Getting Private key
Enter pass phrase for ../private/key_KIR_CA.pem:
```

2. Сгенерируйте ключевую пару для пользователя, создайте запрос на сертификат и выпустите сертификат. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/lab6.1$ openssl genrsa -out pkey.pem -aes-256
-cbc 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.........+++++
.....................................................................
.....................................................+++++
e is 65537 (0x010001)
Enter pass phrase for pkey.pem:
Verifying - Enter pass phrase for pkey.pem:
```

```
taiiiga@taiiiga-VirtualBox:~/kstu/lab6.1$ openssl req -new -key pkey.pem -out r
eq.pem
Enter pass phrase for pkey.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) [AU]:RU
State or Province Name (full name) [Some-State]:Tatarstan
Locality Name (eg, city) []:Kazan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:KSTU
Organizational Unit Name (eg, section) []:728111
Common Name (e.g. server FQDN or YOUR name) []:Khisamov Iskander Ravilevich
Email Address []:iskanderkhisamov@gmail.com

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

```
taiiiga@taiiiga-VirtualBox:~/kstu/lab6.1/KIR_CA$ sudo openssl ca -config KIR_CA
.conf -extensions CA_CLIENT_extensions -days 366 -notext -md sha512 -in req.pem
 -out cert.crt
Using configuration from KIR_CA.conf
Enter pass phrase for ..//private/key_KIR_CA.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'RU'
stateOrProvinceName   :ASN.1 12:'Tatarstan'
localityName          :ASN.1 12:'Kazan'
organizationName      :ASN.1 12:'KSTU'
organizationalUnitName:ASN.1 12:'728111'
commonName            :ASN.1 12:'Khisamov Iskander Ravilevich'
emailAddress          :IA5STRING:'iskanderkhisamov@gmail.com'
Certificate is to be certified until Mar 29 20:39:26 2022 GMT (366 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
```

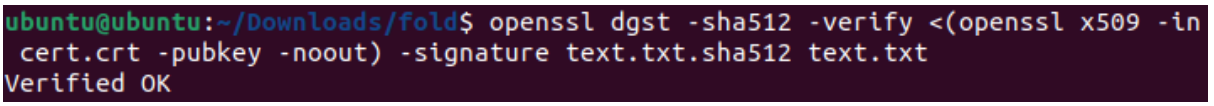
3. Создайте текстовый файл (в файле ФИО) и подпишите его, используя функцию хеширования SHA512. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/lab6.1/KIR_CA$ openssl dgst -sha512 -sign pke
y.pem -out text.txt.sha512 text.txt
Enter pass phrase for pkey.pem:
```

4. Передайте файл, подпись, сертификат пользователя и сертификат УЦ на другую виртуальную машину. (скриншоты в отчет)

```
ubuntu@ubuntu:~/Downloads/fold$ ls
cert.crt  text.txt  text.txt.sha512
```

5. Проверьте сертификат пользователя, извлеките из сертификата открытый ключ и проверьте подпись к файлу. (скриншоты в отчет)



6. Измените файл, проверьте подпись. (скриншоты в отчет)