1. Создайте центр сертификации: (скриншоты в отчет)
   - имя УЦ сделайте по своим инициалам "ФИО" латинскими буквами
   - создать каталог для УЦ "ФИО_CA"

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

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

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

   - создать каталог для сертификатов созданных УЦ (certs_db)

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

   - создайте пустой файл Index.db для базы данных УЦ

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

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

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

   - создайте пустой файл .rand для для хранения случайной последовательности

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

   - создать файл для хранения серийного номера сертификатов (serial)

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

   - 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
     ```

- в сертификат должен добавляться URL на СОС

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

- 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>
```

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

```
default_days = 189
```

- срок действия СОС (суток) = последние 2 цифры из номера зачетки

```
default_crl_days = 89
```

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

```
9

Шестнадцатеричная система - 9.
```

- задать функцию хеширования по умолчанию SHA512

```
default_md = sha512
```

- 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/
```

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

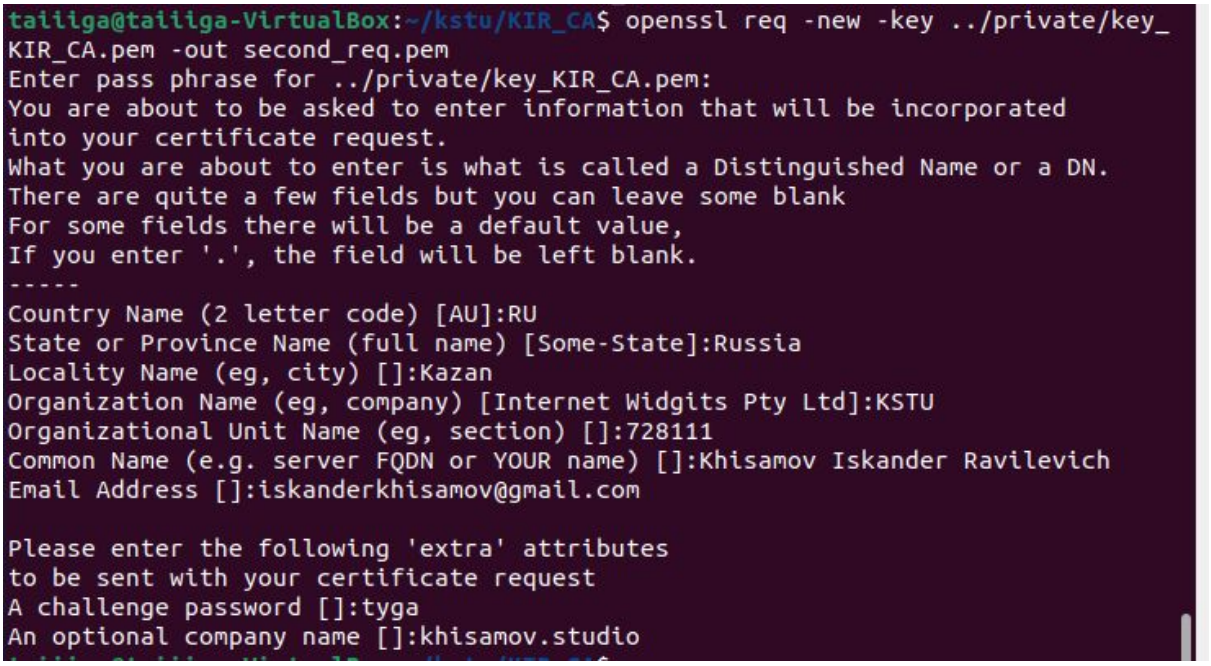
```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl req -config KIR_CA.conf -new
-sha512 -key ../private/key_KIR_CA.pem -out KIR_CA.crt
Enter pass phrase for ../private/key_KIR_CA.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are 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]:
```

- 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:
```

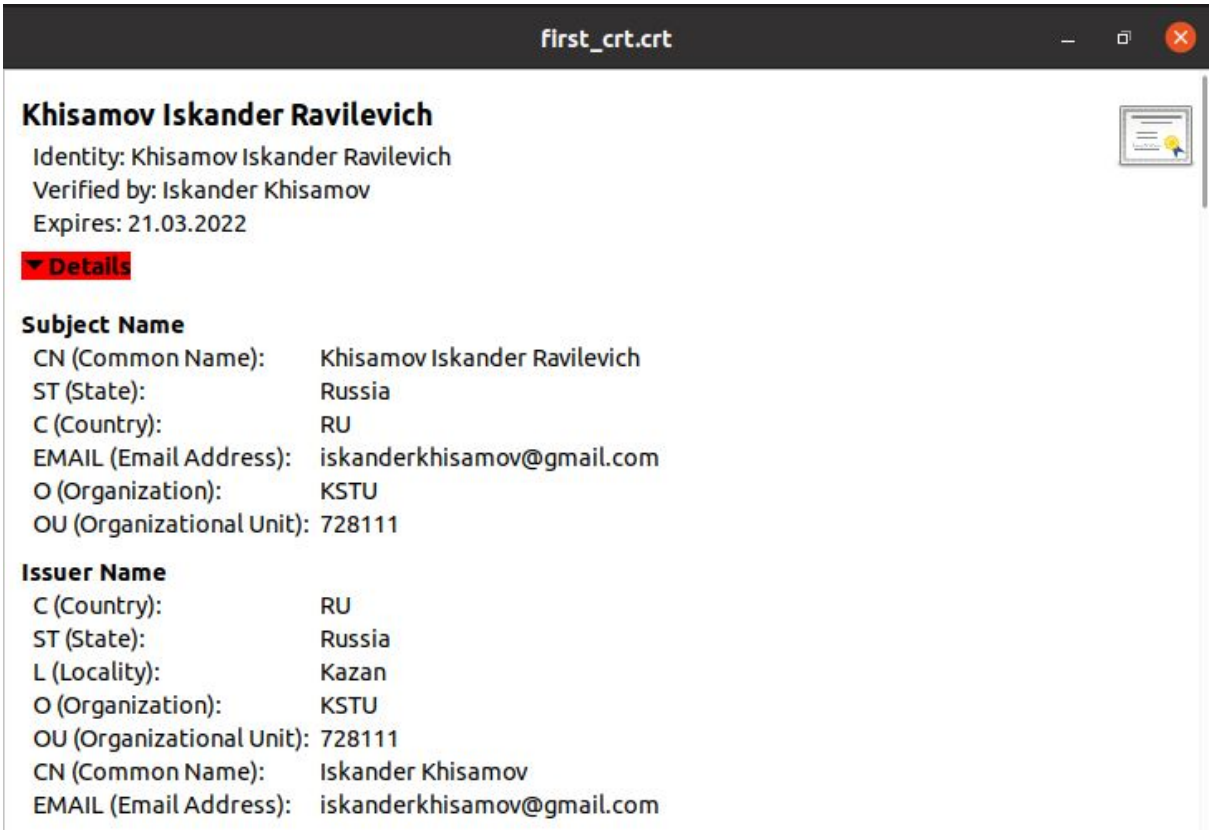
2. Создайте для двух пользователей два запроса на сертификат, добавьте свои ФИО как владельца сертификата. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl req -new -key ../private/key_
KIR_CA.pem -out first_req.pem
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) [AU]:RU
State or Province Name (full name) [Some-State]:Russia
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
```



3. Выпустите два сертификата по этим запросам. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ sudo openssl ca -config KIR_CA.conf -
extensions CA_CLIENT_extensions -days 366 -notext -md sha512 -in first_req.pem
-out first_crt.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:'Russia'
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 21 15:43:48 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
```



first_crt.crt

Issued Certificate

Version:	3
Serial Number:	09
Not Valid Before:	2021-03-20
Not Valid After:	2022-03-21

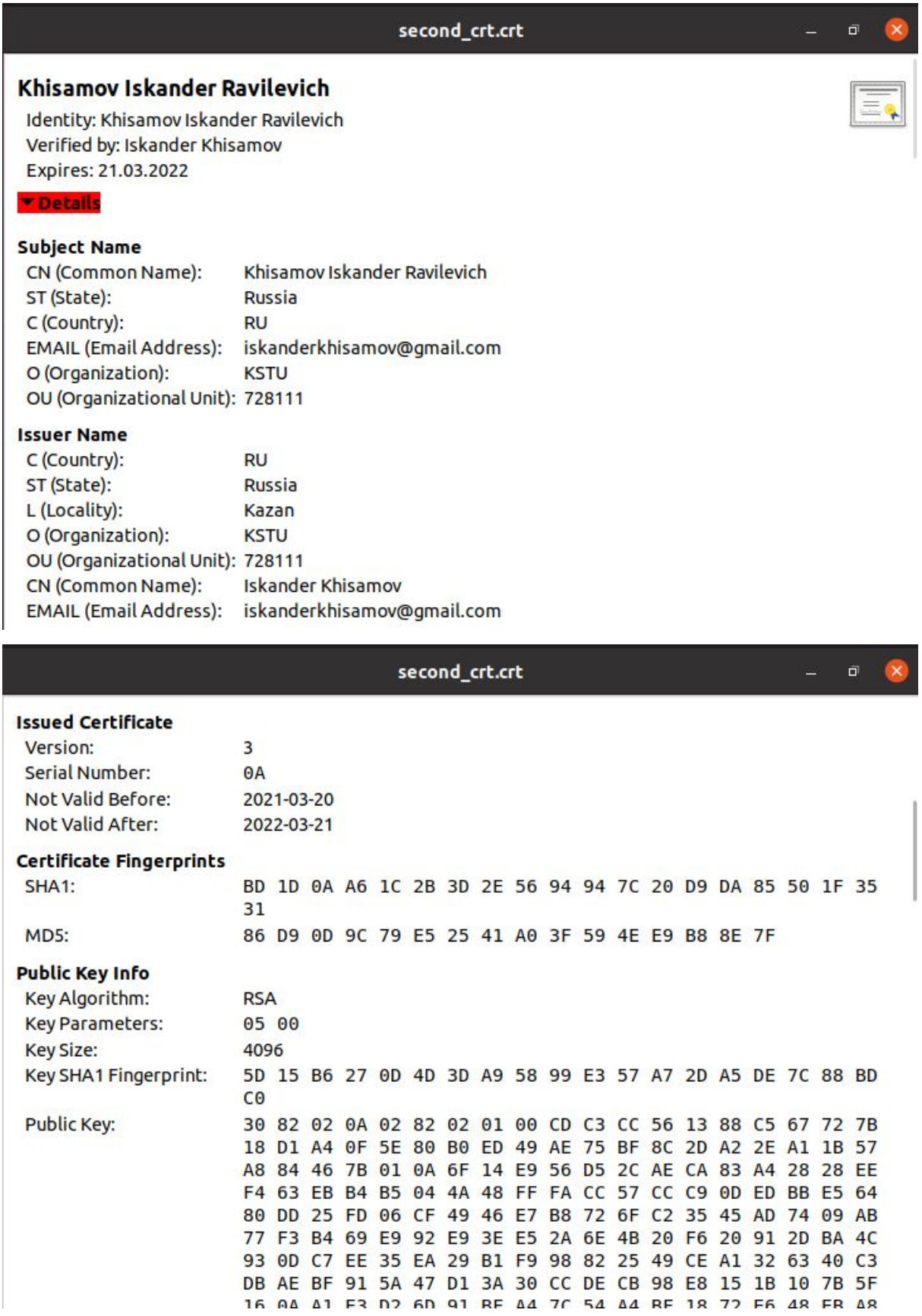
Certificate Fingerprints

SHA1:	CF EE C4 50 02 BE 6A 88 7D AF 3F EB 01 C9 E7 5E 91 97 A5 6C
MD5:	7E 59 5C 31 8A ED C0 7B 19 04 B5 87 9A BC 8B 59

Public Key Info

Key Algorithm:	RSA
Key Parameters:	05 00
Key Size:	4096
Key SHA1 Fingerprint:	5D 15 B6 27 0D 4D 3D A9 58 99 E3 57 A7 2D A5 DE 7C 88 BD C0
Public Key:	30 82 02 0A 02 82 02 01 00 CD C3 CC 56 13 88 C5 67 72 7B 18 D1 A4 0F 5E 80 B0 ED 49 AE 75 BF 8C 2D A2 2E A1 1B 57 A8 84 46 7B 01 0A 6F 14 E9 56 D5 2C AE CA 83 A4 28 28 EE F4 63 EB B4 B5 04 4A 48 FF FA CC 57 CC C9 0D ED BB E5 64 80 DD 25 FD 06 CF 49 46 E7 B8 72 6F C2 35 45 AD 74 09 AB 77 F3 B4 69 E9 92 E9 3E E5 2A 6E 4B 20 F6 20 91 2D BA 4C 93 0D C7 EE 35 EA 29 B1 F9 98 82 25 49 CE A1 32 63 40 C3 DB AE BF 91 5A 47 D1 3A 30 CC DE CB 98 E8 15 1B 10 7B 5F 16 0A A1 E3 D2 6D 91 BF A4 7C 54 A4 BF 18 72 E6 48 EB A8

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ sudo openssl ca -config KIR_CA.conf -
extensions CA_CLIENT_extensions -days 366 -notext -md sha512 -in second_req.pem
 -out second_crt.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:'Russia'
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 21 15:45:03 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
```

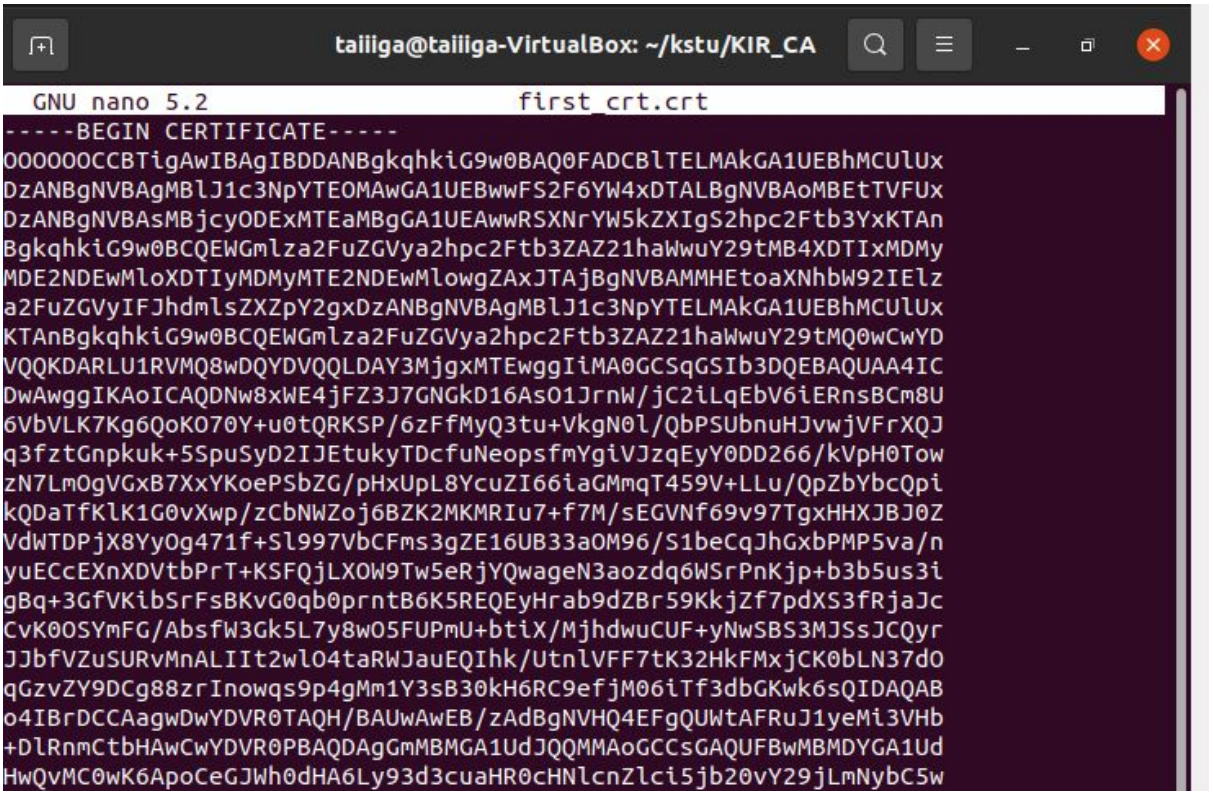


4. Проверьте подлинность одного сертификата с помощью сертификата УЦ. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -modulus -in firs
t_crt.crt | openssl md5
(stdin)= b287e25fbac6340226d8b072e012ba69
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -modulus -in KIR_
CA.crt | openssl md5
(stdin)= b287e25fbac6340226d8b072e012ba69
```

5. Измените информацию в сертификате. (скриншоты в отчет)

```
-----BEGIN CERTIFICATE-----
MIIHUDCCBTigAwIBAgIBCzANBgkqhkiG9w0BAQ0FADCBlTELMAkGA1UEBhMCUlUx
DzANBgNVBAgMBlJ1c3NpYTEOMAwGA1UEBwwFS2F6YW4xDTALBgNVBAoMBEtTVFUx
DzANBgNVBAsMBjcyODExMTEaMBgGA1UEAwwRSXNrYW5kZXIgS2hpc2Ftb3YxKTAn
BgkqhkiG9w0BCQEWGmlza2FuZGVya2hpc2Ftb3ZAZ21haWwuY29tMB4XDTIxMDMy
MDE2MzkxNloXDTIyMDMyMTE2MzkxNlowgZAxJTAjBgNVBAMMHEtoaXNhbW92IElz
a2FuZGVyIFJhdmlsZXZpY2gxDzANBgNVBAgMBlJ1c3NpYTELMAkGA1UEBhMCUlUx
KTAnBgkqhkiG9w0BCQEWGmlza2FuZGVya2hpc2Ftb3ZAZ21haWwuY29tMQ0wCwYD
VQQKDARLU1RVMQ8wDQYDVQQLDAY3MjgxMTEwggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQDNw8xWE4jFZ3J7GNGkD16AsO1JrnW/jC2iLqEbV6iERnsBCm8U
6VbVLK7Kg6QoKO70Y+u0tQRKSP/6zFfMyQ3tu+VkgN0l/QbPSUbnuHJvwjVFrXQJ
q3fztGnpkuk+5SpuSyD2IJEtukyTDcfuNeopsfmYgiVJzqEyY0DD266/kVpH0Tow
zN7LmOgVGxB7XxYKoePSbZG/pHxUpL8YcuZI66iaGMmqT459V+LLu/QpZbYbcQpi
kQDaTfKlK1G0vXwp/zCbNWZoj6BZK2MKMRIu7+f7M/sEGVNf69v97TgxHHXJBJ0Z
VdWTDPjX8YyOg471f+Sl997VbCFms3gZE16UB33aOM96/S1beCqJhGxbPMP5va/n
yuECcEXnXDVtbPrT+KSFQjLXOW9Tw5eRjYQwageN3aozdq6WSrPnKjp+b3b5us3i
gBq+3GfVKibSrFsBKvG0qb0prntB6K5REQEyHrab9dZBr59KkjZf7pdXS3fRjaJc
CvK0OSYmFG/AbsfW3Gk5L7y8wO5FUPmU+btiX/MjhdwuCUF+yNwSBS3MJSsJCQyr
JJbfVZuSURvMnALIIt2wlO4taRWJauEQIhk/UtnlVFF7tK32HkFMxjCK0bLN37dO
qGzvZY9DCg88zrInowqs9p4gMm1Y3sB30kH6RC9efjM06iTf3dbGKwk6sQIDAQAB
o4IBrDCCAagwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUWtAFRuJ1yeMi3VHb
+DlRnmCtbHAwCwYDVR0PBAQDAgGmMBMGA1UdJQQMMAoGCCsGAQUFBwMBMDYGA1Ud
HwQvMC0wK6ApoCeGJWh0dHA6Ly93d3cuaHR0cHNlcnZlci5jb20vY29jLmNybC5w
ZW0wQwYDVR0RBDwwOoIbU3BhcmtsaW5nIEludGVybWlkaWF0ZSBDQSAxghtTcGFy
a2xpbmcgQ0EgSW50ZXJtaWRpYXRlIDEwgdYGCCsGAQUFBwEBBIHJMIHGMDgGCCsG
AQUFBzAChixodHRwOi8vcGtpLnNwYXJrbGluZ2NhLmNvbS9TcGFya2xpbmdSb290
```



6. Проверьте подлинность измененного сертификата. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -modulus -in KIR_
CA.crt | openssl md5
(stdin)= b287e25fbac6340226d8b072e012ba69
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -modulus -in firs
t_crt.crt | openssl md5
unable to load certificate
140685021889856:error:0D07207B:asn1 encoding routines:ASN1_get_object:header to
o long:../crypto/asn1/asn1_lib.c:101:
140685021889856:error:0D068066:asn1 encoding routines:asn1_check_tlen:bad objec
t header:../crypto/asn1/tasn_dec.c:1137:
140685021889856:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:neste
d asn1 error:../crypto/asn1/tasn_dec.c:309:Type=X509
140685021889856:error:0906700D:PEM routines:PEM_ASN1_read_bio:ASN1 lib:../crypt
o/pem/pem_oth.c:33:
(stdin)= d41d8cd98f00b204e9800998ecf8427e
```

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ sudo openssl verify -CAfile KIR_CA.cr
t first_crt.crt
unable to load certificate
140034482861376:error:0D07207B:asn1 encoding routines:ASN1_get_object:header to
o long:../crypto/asn1/asn1_lib.c:101:
140034482861376:error:0D068066:asn1 encoding routines:asn1_check_tlen:bad objec
t header:../crypto/asn1/tasn_dec.c:1137:
140034482861376:error:0D07803A:asn1 encoding routines:asn1_item_embed_d2i:neste
d asn1 error:../crypto/asn1/tasn_dec.c:309:Type=X509
140034482861376:error:0906700D:PEM routines:PEM_ASN1_read_bio:ASN1 lib:../crypt
o/pem/pem_oth.c:33:
```

7. Внесите второй сертификат в COC. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl ca -config KIR_CA.conf -revok
e second_crt.crt
Using configuration from KIR_CA.conf
Enter pass phrase for ..//private/key_KIR_CA.pem:
Revoking Certificate 0A.
Data Base Updated
```

8. Сгенерируйте COC (в команде укажите через сколько дней будет выпущен следующий). (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ sudo openssl ca -config KIR_CA.conf -
gencrl -keyfile ../private/key_KIR_CA.pem -days 365 -cert KIR_CA.crt -out crl.p
em
Using configuration from KIR_CA.conf
Enter pass phrase for ../private/key_KIR_CA.pem:
```

9. Выведите информацию о COC, разберите поля. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl crl -noout -text -in crl.pem
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: C = RU, ST = Russia, L = Kazan, O = KSTU, OU = 728111, CN = Khi
samov Iskander Ravilevich, emailAddress = iskanderkhisamov@gmail.com
        Last Update: Mar 20 17:16:47 2021 GMT
        Next Update: Jun 17 17:16:47 2021 GMT
        CRL extensions:
            X509v3 CRL Number:
                4098
Revoked Certificates:
    Serial Number: 0A
        Revocation Date: Mar 20 16:49:22 2021 GMT
    Signature Algorithm: sha512WithRSAEncryption
         76:8a:c3:d8:31:e8:1c:ff:64:fa:8b:57:fd:9b:91:16:be:d9:
         bf:57:ba:55:8b:cb:80:fb:75:1a:08:75:d2:9f:d9:ba:9f:60:
         d0:8b:72:02:af:c7:8d:d0:50:76:2f:bb:6b:3b:2b:2d:0d:21:
         1e:f9:5b:ce:46:2c:64:e8:76:72:63:ca:f1:87:b6:8e:35:98:
         22:3b:44:69:8e:1f:03:42:67:2c:73:8b:16:71:0b:a2:45:10:
         f6:67:74:b7:e4:51:cc:04:cb:cd:5a:79:04:35:d4:7f:de:fb:
         b9:7c:81:40:f8:55:55:85:fc:54:fe:5b:bf:4b:da:9f:d8:3b:
         d9:ca:84:bb:f0:8a:d8:7b:fd:1e:9e:d7:d8:a9:97:ee:0b:f4:
         03:28:29:82:1b:fb:cc:41:33:db:52:81:e5:e2:ec:5b:0a:71:
         02:41:41:e5:94:15:7c:a9:c7:e1:07:4a:8b:07:0b:db:39:83:
         da:cc:ef:3c:82:19:f8:9f:2c:7e:44:a4:14:26:2f:a5:62:06:
         e0:c8:fe:14:87:4f:77:55:0a:96:c6:b5:09:c0:a5:d6:34:86:
         28:e0:83:ae:7d:95:d2:51:e5:04:01:23:82:68:f4:af:1f:fb:
         77:75:70:fb:70:f2:6b:fa:65:ef:dc:28:10:18:0f:10:bc:54:
```

10. Используя COC проверьте отозванный и не отозванный сертификаты. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -text -in first_c
rt.crt
```

```
X509v3 CRL Distribution Points:

    Full Name:
      URI:http://www.httpserver.com/crl.pem
```

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -text -in second_
crt.crt
```

```
X509v3 CRL Distribution Points:

    Full Name:
      URI:http://www.httpserver.com/crl.pem
```

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -serial -in first
_crt.crt
serial=0E
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl x509 -noout -serial -in secon
d_crt.crt
serial=0F
```

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ openssl crl -noout -text -in crl.pem
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha512WithRSAEncryption
        Issuer: C = RU, ST = Russia, L = Kazan, O = KSTU, OU = 728111, CN = Khi
samov Iskander Ravilevich, emailAddress = iskanderkhisamov@gmail.com
        Last Update: Mar 20 17:26:12 2021 GMT
        Next Update: Jun 17 17:26:12 2021 GMT
        CRL extensions:
            X509v3 CRL Number:
                4099
Revoked Certificates:
    Serial Number: 0A
        Revocation Date: Mar 20 16:49:22 2021 GMT
    Serial Number: 0F
        Revocation Date: Mar 20 17:25:38 2021 GMT
```

11. Открыть сертификат любого сайта (https), разобрать всю цепочку доверия. (скриншоты в отчет)

```
taiiiga@taiiiga-VirtualBox:~/kstu/KIR_CA$ sudo openssl s_client -connect vk.com
:443
CONNECTED(00000003)
depth=2 C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign Organization Validation C
A - SHA256 - G2
verify return:1
depth=0 C = RU, ST = Saint-Petersburg, L = Saint-Petersburg, O = V Kontakte LLC
, CN = *.vk.com
verify return:1
---
Certificate chain
 0 s:C = RU, ST = Saint-Petersburg, L = Saint-Petersburg, O = V Kontakte LLC, C
N = *.vk.com
   i:C = BE, O = GlobalSign nv-sa, CN = GlobalSign Organization Validation CA -
 SHA256 - G2
 1 s:C = BE, O = GlobalSign nv-sa, CN = GlobalSign Organization Validation CA -
 SHA256 - G2
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
 2 s:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
   i:C = BE, O = GlobalSign nv-sa, OU = Root CA, CN = GlobalSign Root CA
```

Common name: *.vk.com
SANs: *.vk.com, *.vk.cc, *.vk.design, *.vk.link, *.vk.me, *.vkontakte.com, *.vkontakte.ru, *.vkpay.app, *.vkpay.io, stats.vk-portal.net, vk.cc, vk.design, vk.link, vk.me, vkontakte.com, vkontakte.ru, vkpay.app, vkpay.io, vk.com
Organization: V Kontakte LLC
Location: Saint-Petersburg, Saint-Petersburg, RU
Valid from June 9, 2020 to June 10, 2022
Serial Number: 23002c3db74fdb4508a12db8
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign Organization Validation CA - SHA256 - G2

Common name: GlobalSign Organization Validation CA - SHA256 - G2
Organization: GlobalSign nv-sa
Location: BE
Valid from February 20, 2014 to February 20, 2024
Serial Number: 040000000001444ef04247
Signature Algorithm: sha256WithRSAEncryption
Issuer: GlobalSign Root CA

Common name: GlobalSign Root CA
Organization: GlobalSign nv-sa **Org. Unit:** Root CA
Location: BE
Valid from September 1, 1998 to January 28, 2028
Serial Number: 040000000001154b5ac394
Signature Algorithm: sha1WithRSAEncryption
Issuer: GlobalSign Root CA