МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

НГТУ
НЭТИ | **Факультет прикладной математики и информатики**

Кафедра прикладной математики

Практическое задание № 3

по дисциплине «Основы криптографии»

ЭЛЕМЕНТАРНЫЕ МЕТОДЫ ШИФРОВАНИЯ

Группа ПМ-91 ЗАТОЛОЦКАЯ ЮЛИЯ

БАРСУКОВА НАТАЛЬЯ

ЧЕРНИКОВ ДАНИИЛ

Преподаватель СТУПАКОВ ИЛЬЯ МИХАЙЛОВИЧ

Новосибирск, 2021

Цель: научиться работе с криптографическими сертификатами и изучить использование OpenSSL для их создания.

Часть 1:

Пункт 1.

Запрос

req -new -config ca.conf -x509 -out ca.crt -keyout=ca.key

ca.conf:

```
[ req ]
default_bits = 2048
distinguished_name = req_distinguished_name
x509_extensions = v3_ca

[ req_distinguished_name ]
countryName = Country Name
countryName_default = RU
countryName_min = 2
countryName_max = 2

localityName = Locality Name
localityName_default = Novosibirsk

organizationName = organization Name
organizationName_default = Novosibirsk State Technical University

commonName = Common Name
commonName_max = 64

[ v3_ca ]
basicConstraints=critical, CA:TRUE, pathlen:1
keyUsage=critical, keyCertSign
```

Расшифровка: x509 -in ca.crt -text

```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         2d:4e:1e:75:fe:4e:80:ed:cf:db:3e:19:97:4a:8d:a0:1c:a3:c3:a2
      Signature Algorithm: sha256WithRSAEncryption
      Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Daniil Chern and
Julia zat\1B[D\1B[Z\1B[C\1B[C
      Validity
         Not Before: Dec  2 16:32:00 2021 GMT
         Not After : Jan  1 16:32:00 2022 GMT
      Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Daniil Chern
and Julia zat\1B[D\1B[Z\1B[C\1B[C
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
               00:c3:bf:53:d1:0e:13:23:ea:fe:d1:c4:2b:2b:f8:
               98:a5:3a:a5:86:70:76:06:cc:b2:b5:42:63:5b:ce:
```

```
                17:37:c8:d0:79:0f:6b:5c:92:e4:41:71:5e:6d:62:
                c5:23:cb:02:3c:3d:81:c3:c3:73:f6:30:79:35:b5:
                e1:fd:cb:8e:d9:62:bd:09:15:59:c6:df:7d:e0:82:
                59:6e:b7:aa:92:1f:33:45:50:aa:04:a8:d7:02:bc:
                06:20:d0:92:ba:82:1a:ff:3a:19:88:2f:5d:c0:0d:
                0e:19:dd:0f:0f:11:60:23:63:ae:a4:5d:cb:7a:f3:
                a3:b3:25:88:2a:4f:fa:e3:b5:45:8f:25:ab:33:b3:
                ef:a7:e5:5a:c5:ea:0f:97:ab:2b:db:b5:ac:d6:7a:
                1b:0d:0a:ab:c6:9a:34:be:51:58:e8:c1:07:69:0e:
                e8:63:76:55:19:32:dd:19:aa:23:53:cd:62:3d:58:
                7f:c3:c7:fc:50:d0:ab:7a:9d:8f:1a:35:e2:1d:98:
                1b:7d:94:cb:fd:05:87:7c:5a:eb:8f:2f:5c:fc:a2:
                c2:79:ba:9e:fd:47:e1:77:bf:ea:c0:cf:f4:cf:4c:
                e7:26:0f:e4:b3:60:2b:13:1e:30:e6:39:24:13:8f:
                f2:02:ec:49:c9:47:77:b3:ae:0b:15:9a:ed:cc:0d:
                59:4f
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
            X509v3 Key Usage: critical
                Certificate Sign
    Signature Algorithm: sha256WithRSAEncryption
        09:91:50:19:7d:de:84:56:46:67:da:73:18:0c:db:ae:56:f6:
        80:c8:8f:c2:33:04:1e:47:0f:e5:15:b3:ab:83:63:2e:0a:e1:
        1f:ec:01:ca:9c:1c:e0:6f:a0:5d:e5:58:73:4e:26:79:f7:98:
        ff:cb:ca:60:17:8d:1a:66:de:cf:5f:24:1f:92:3b:cc:26:25:
        9b:e7:92:e3:75:72:49:51:ae:6e:32:10:87:7f:1c:8a:d8:93:
        38:32:81:90:c5:e5:31:10:34:17:fe:77:c2:a0:84:d0:cd:df:
        57:51:8d:71:ad:27:e3:e3:03:3c:38:71:1c:04:9d:44:76:98:
        bf:d2:41:af:4d:a8:a5:b7:25:1b:f3:76:0d:f4:d1:70:14:46:
        cd:7d:63:f9:5a:de:38:0d:34:1e:c7:c6:67:ce:30:ee:37:ee:
        e7:72:71:db:9a:35:50:31:6b:8d:1e:3f:45:c8:46:51:32:5d:
        45:04:8f:45:1b:cc:2a:ba:f8:2e:c2:e7:bb:e2:b4:77:15:1b:
        49:3c:3e:87:e3:2d:a6:09:49:84:e2:71:f3:63:aa:36:e9:52:
        45:18:c2:ce:59:8b:a5:3f:01:2a:6b:ec:04:f2:77:b8:6f:ef:
        36:3e:5e:1c:3c:a0:42:f4:29:ec:d6:54:ed:cb:99:4b:c4:2a:
        63:58:35:98
-----BEGIN CERTIFICATE-----
MIIDwDCCAqigAwIBAgIULU4edf5OgO3P2z4Zl0qNoByjw6IwDQYJKoZIhvcNAQEL
BQAwgYUxCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2liaXJzazEvMC0GA1UE
CgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZlcnNpdHkxLzAtBgNV
BAMMJkRhbmlpbCBDaGVybiBhbmQgSnVsaWEgemF0G1tEG1taG1tDG1tDMB4XDTIx
MTIwMjE2MzIwMFoXDTIyMDEwMTE2MzIwMFowgYUxCzAJBgNVBAYTAlJVMRQwEgYD
VQQHDAtOb3Zvc2liaXJzazEvMC0GA1UECgwmTm92b3NpYmlyc2sgU3RhdGUgVGVj
aG5pY2FsIFVuaXZlcnNpdHkxLzAtBgNVBAMMJkRhbmlpbCBDaGVybiBhbmQgSnVs
aWEgemF0G1tEG1taG1tDG1tDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAw79T0Q4TI+r+0cQrK/iYpTqlhnB2BsyytUJjW84XN8jQeQ9rXJLkQXFebWLF
I8sCPD2Bw8Nz9jB5NbXh/cuO2WK9CRVZxt994IJZbreqkh8zRVCqBKjXArwGINCS
uoIa/zoZiC9dwA0OGd0PDxFgI2OupF3LevOjsyWIKk/647VFjyWrM7Pvp+VaxeoP
l6sr27Ws1nobDQqrxpo0vlFY6MEHaQ7oY3ZVGTLdGaojU81iPVh/w8f8UNCrep2P
GjXiHZgbfZTL/QWHfFrrjy9c/KLCebqe/Ufhd7/qwM/0z0znJg/ks2ArEx4w5jkk
E4/yAuxJyUd3s64LFZrtzA1ZTwIDAQABoyYwJDASBgNVHRMBAf8ECDAGAQH/AgEB
MA4GA1UdDwEB/wQEAwICBDANBgkqhkiG9w0BAQsFAAOCAQEACZFQGX3ehFZGZ9pz
```

GAzbrlb2gMiPwjMEHkcP5RWzq4NjLgrhH+wBypwc4G+gXeVYc04mefeY/8vKYBeN
Gmbez18kH5I7zCYlm+eS43VySVGubjIQh38citiTODKBkMXlMRA0F/53wqCE0M3f
V1GNca0n4+MDPDhxHASdRHaYv9JBr02opbclG/N2DfTRcBRGzX1j+VreOA00HsfG
Z84w7jfu53Jx25o1UDFrjR4/RchGUTJdRQSPRRvMKrr4LsLnu+K0dxUbSTw+h+Mt
pglJhOJx82OqNulSRRjCzlmLpT8BKmvsBPJ3uG/vNj5eHDygQvQp7NZU7cuZS8Qq
Y1g1mA==
-----END CERTIFICATE-----

Пункт 2.

Запрос

req -new -config client.conf -out client.csr -keyout=client.key

client.conf:

```
[ req ]
distinguished_name = req_distinguished_name
req_extensions = v3_req

[ req_distinguished_name ]
commonName = common Name

countryName = country Name
countryName_default = RU
countryName_min = 2
countryName_max = 2

localityName = locality Name
localityName_default = Novosibirsk

organizationName = organization Name
organizationName_default = Novosibirsk State Technical University

[ v3_req ]
keyUsage = digitalSignature, nonRepudiation
extendedKeyUsage = clientAuth
basicConstraints = CA:false
```

Расшифровка: req -in client.csr -text

```
Certificate Request:
   Data:
      Version: 1 (0x0)
      Subject: CN = "Chernikov D.S., Zatolockaya J.A., Barsukova N.I.", C = RU, L = Novosibirsk, O =
Novosibirsk State Technical University
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
               00:ce:15:2a:08:aa:5e:80:b7:f2:02:bd:43:cb:34:
               a8:aa:77:2e:79:c1:66:ed:b0:9a:1c:b6:2f:4d:30:
               bd:84:31:62:55:b2:09:77:64:ac:61:43:95:67:94:
               67:21:f1:f9:40:37:18:76:4c:4c:41:69:bc:2a:de:
               2c:33:fb:35:98:47:6c:9f:82:0c:11:dc:19:a4:e9:
               f3:f4:40:a2:21:10:da:98:3b:28:08:99:6d:f1:cb:
               5e:10:43:f4:72:7b:4b:60:87:a6:84:5e:72:20:4c:
               c7:b2:fa:36:e7:4a:59:9f:d0:14:9b:bc:c7:c1:7a:
```

```
                2f:44:0d:a9:b7:74:26:2f:25:a0:96:6d:f4:eb:94:
                d9:2f:34:63:56:28:41:2c:e3:83:c3:f8:6f:09:85:
                70:61:dd:4d:e4:dd:63:98:22:78:55:00:2f:a3:7d:
                f2:9c:75:41:21:11:cd:bd:91:59:ab:55:81:57:72:
                4a:9e:1d:d1:6e:b9:ae:98:db:84:0b:98:ab:6d:44:
                42:09:bd:b3:63:ea:df:86:54:47:a1:50:0e:a7:f5:
                45:e8:94:a5:db:6f:6b:93:a8:25:29:c7:4a:00:d7:
                a4:80:3a:90:00:f2:1f:9b:f5:fe:9f:0b:6e:ba:f1:
                6a:10:9a:ba:60:73:a0:96:2e:78:b5:de:0d:f7:7d:
                c0:d5
            Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
          X509v3 Key Usage:
            Digital Signature, Non Repudiation
          X509v3 Extended Key Usage:
            TLS Web Client Authentication
          X509v3 Basic Constraints:
            CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
        9d:a1:f3:34:dc:24:71:db:ef:61:b4:c5:a1:c4:09:18:3f:ec:
        43:ce:89:48:43:ab:cf:1c:cf:60:a7:d2:3e:3e:ac:f6:f7:cd:
        1e:b0:bf:d9:33:d7:8c:87:20:3f:cb:e0:ea:e5:2e:47:9e:d0:
        43:0b:ad:6a:0c:e7:a9:22:2f:5d:73:b5:99:fa:37:01:e6:2a:
        a9:79:32:31:13:07:09:cf:1e:28:9c:8e:8f:27:9b:a2:6b:fe:
        2e:c6:d6:6f:a3:67:07:00:96:c7:3f:d3:76:23:8a:36:8c:6a:
        73:82:f6:7e:54:94:10:c3:49:1f:9a:c8:9e:ca:aa:88:0b:17:
        fb:92:8e:fa:62:3e:30:93:27:71:25:de:d4:84:fe:4a:4a:30:
        06:3e:a8:1c:cb:53:cd:94:21:b0:c6:28:4a:1f:79:9a:fd:4b:
        71:68:b9:74:15:11:44:8f:3b:58:44:f2:7c:5d:2b:16:81:32:
        a8:f1:04:0d:6e:99:83:4d:4e:eb:bc:1d:bc:87:07:d8:60:11:
        c5:88:bf:8a:fc:42:45:10:ac:2a:a8:7e:61:57:3b:41:f7:bc:
        e2:3c:61:1d:6d:0f:89:81:c2:1c:2b:d3:47:2c:4e:d6:d9:41:
        75:12:ec:0c:60:70:88:dc:8f:ae:67:e5:fd:0e:a7:2b:62:ce:
        6d:ba:4a:91
-----BEGIN CERTIFICATE REQUEST-----
MIIDEzCCAfsCAQAwgY8xOTA3BgNVBAMMMENoZXJuaWtvdiBElIMuLCBaYXRvbG9j
a2F5YSBKLkEuLCBCYXJzdWtvdmEgTi5JLjELMAkGA1UEBhMCUlUxFDASBgNVBAcM
C05vdm9zaWJpcnNrMS8wLQYDVQQKDCZOb3Zvc2liXJzayBTdGF0ZSBUZWNobmlj
YWwgVW5pdmVyc2l0eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM4V
KgiqXoC38gK9Q8s0qKp3LnnBZu2wmhy2L00wvYQxYlWyCXdkrGFDlWeUZyHx+UA3
GHZMTEFpvCreLDP7NZhHbJ+CDBHcGaTp8/RAoiEQ2pg7KAiZbfHLXhBD9HJ7S2CH
poReciBMx7L6NudKWZ/QFJu8x8F6L0QNqbd0Ji8loJZt9OuU2S80Y1YoQSzjg8P4
bwmFcGHdTeTdY5gieFUAL6N98px1QSERzb2RWatVgVdySp4d0W65rpjbhAuYq21E
Qgm9s2Pq34ZUR6FQDqf1ReiUpdtva5OoJSnHSgDXpIA6kADyH5v1/p8LbrrxahCa
umBzoJYueLXeDfd9wNUCAwEAAaA+MDwGCSqGSIb3DQEJDjEvMC0wCwYDVR0PBAQD
AgbAMBMGA1UdJQQMMAoGCCsGAQUFBwMCMAkGA1UdEwQCMAAwDQYJKoZIhvcNAQEL
BQADggEBAJ2h8zTcJHHb72G0xaHECRg/7EPOiUhDq88cz2Cn0j4+rPb3zR6wv9kz
14yHID/L4OrlLkee0EMLrWoM56kiL11ztZn6NwHmKql5MjETBwnPHiicjo8nm6Jr
/i7G1m+jZwcAlsc/03YjijaManOC9n5UlBDDSR+ayJ7KqogLF/uSjvpiPjCTJ3El
3tSE/kpKMAY+qBzLU82UIbDGKEofeZr9S3FouXQVEUSPO1hE8nxdKxaBMqjxBA1u
mYNNTuu8HbyHB9hgEcWIv4r8QkUQrCqofmFXO0H3vOI8YR1tD4mBwhwr00csTtbZ
QXUS7AxgcIjcj65n5f0Opytizm26SpE=
-----END CERTIFICATE REQUEST-----
```

Пункт 3.
Создание запрошенного сертификата.

```
OpenSSL> x509 -req -extfile client.conf -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt
Signature ok
subject=CN = "Chernikov D.S., Zatolockaya J.A., Barsukova N.I.", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University
Getting CA Private Key
34359836736:error:08064066:object identifier routines:OBJ_create:oid exists:crypto/objects/obj_dat.c:698:
Enter pass phrase for ca.key:
```

Расшифровка запрошенного сертификата: x509 -in client.crt -text

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      3e:27:bd:61:35:c9:9e:31:bd:8b:7f:90:45:f4:d5:00:68:33:0e:4f
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Daniil Chern and Julia zat\1B[D\1B[Z\1B[C\1B[C
    Validity
      Not Before: Dec 2 16:59:43 2021 GMT
      Not After : Jan 1 16:59:43 2022 GMT
    Subject: CN = "Chernikov D.S., Zatolockaya J.A., Barsukova N.I.", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (2048 bit)
        Modulus:
          00:ce:15:2a:08:aa:5e:80:b7:f2:02:bd:43:cb:34:
          a8:aa:77:2e:79:c1:66:ed:b0:9a:1c:b6:2f:4d:30:
          bd:84:31:62:55:b2:09:77:64:ac:61:43:95:67:94:
          67:21:f1:f9:40:37:18:76:4c:4c:41:69:bc:2a:de:
          2c:33:fb:35:98:47:6c:9f:82:0c:11:dc:19:a4:e9:
          f3:f4:40:a2:21:10:da:98:3b:28:08:99:6d:f1:cb:
          5e:10:43:f4:72:7b:4b:60:87:a6:84:5e:72:20:4c:
          c7:b2:fa:36:e7:4a:59:9f:d0:14:9b:bc:c7:c1:7a:
          2f:44:0d:a9:b7:74:26:2f:25:a0:96:6d:f4:eb:94:
          d9:2f:34:63:56:28:41:2c:e3:83:c3:f8:6f:09:85:
          70:61:dd:4d:e4:dd:63:98:22:78:55:00:2f:a3:7d:
          f2:9c:75:41:21:11:cd:bd:91:59:ab:55:81:57:72:
          4a:9e:1d:d1:6e:b9:ae:98:db:84:0b:98:ab:6d:44:
          42:09:bd:b3:63:ea:df:86:54:47:a1:50:0e:a7:f5:
          45:e8:94:a5:db:6f:6b:93:a8:25:29:c7:4a:00:d7:
          a4:80:3a:90:00:f2:1f:9b:f5:fe:9f:0b:6e:ba:f1:
          6a:10:9a:ba:60:73:a0:96:2e:78:b5:de:0d:f7:7d:
          c0:d5
        Exponent: 65537 (0x10001)
  Signature Algorithm: sha256WithRSAEncryption
    70:c9:25:cf:b5:67:d4:2d:d4:10:fd:2e:cf:5a:6c:ea:0f:c4:
    84:4a:d3:53:be:c3:13:04:9e:8b:d3:96:da:5b:fc:e0:c1:e6:
    b4:11:c7:cf:46:48:87:6e:e8:4c:26:09:0b:35:69:68:28:86:
    7c:48:57:6e:3c:3f:1e:c1:95:33:82:88:09:c5:9b:fd:4e:26:
    67:6e:72:9d:dd:11:dc:6b:3c:0b:b2:0f:b4:e8:d9:f2:15:49:

```
        84:74:38:42:70:b0:3c:1d:9e:f7:e7:d3:15:ca:70:6e:57:86:
        1b:a1:61:46:eb:ac:ba:dd:02:2c:37:b6:fe:dc:67:c2:8b:93:
        4d:b2:c7:29:31:9d:89:55:67:32:f9:c0:fe:e8:82:36:64:86:
        08:32:c0:4d:dc:ae:b1:d6:da:aa:2f:3b:0a:d3:4d:16:c5:da:
        35:7d:b9:ec:b3:06:f0:a2:7f:6c:46:c1:9d:68:44:73:b2:17:
        86:f7:41:31:51:23:77:d4:c5:dd:73:85:d6:9c:67:07:d6:95:
        b4:80:9d:29:38:84:4e:40:11:d3:66:5a:bb:f1:19:83:46:45:
        25:b9:6f:21:ab:d5:75:a2:58:78:63:af:f5:88:62:21:f0:10:
        16:2f:84:21:54:e7:12:fe:c4:b9:57:37:c7:bb:90:25:8e:92:
        d3:f0:76:31
    -----BEGIN CERTIFICATE-----
    MIIDojCCAoqgAwIBAgIUPie9YTXJnjG9i3+QRfTVAGgzDk8wDQYJKoZIhvcNAQEL
    BQAwgYUxCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2liaXJzazEvMC0GA1UE
    CgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZlcnNpdHkxLzAtBgNV
    BAMMJkRhbmlpbCBDaGVybiBhbmQgSnVsaWEgemF0G1tEG1taG1tDG1tDMB4XDTIx
    MTIwMjE2NTk0M1oXDTIyMDEwMTE2NTk0M1owgY8xOTA3BgNVBAMMMENoZXJuaWtv
    diBELlMuLCBaYXRvbG9ja2F5YSBKLkEuLCBCYXJzdWtvdmEgTi5JLjELMAkGA1UE
    BhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQKDCZOb3Zvc2liaXJz
    ayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTCCASIwDQYJKoZIhvcNAQEBBQAD
    ggEPADCCAQoCggEBAM4VKgiqXoC38gK9Q8s0qKp3LnnBZu2wmhy2L00wvYQxYlWy
    CXdkrGFDlWeUZyHx+UA3GHZMTEFpvCreLDP7NZhHbJ+CDBHcGaTp8/RAoiEQ2pg7
    KAiZbfHLXhBD9HJ7S2CHpoReciBMx7L6NudKWZ/QFJu8x8F6L0QNqbd0Ji8loJZt
    9OuU2S80Y1YoQSzjg8P4bwmFcGHdTeTdY5gieFUAL6N98px1QSERzb2RWatVgVdy
    Sp4d0W65rpjbhAuYq21EQgm9s2Pq34ZUR6FQDqf1ReiUpdtva5OoJSnHSgDXpIA6
    kADyH5v1/p8LbrrxahCaumBzoJYueLXeDfd9wNUCAwEAATANBgkqhkiG9w0BAQsF
    AAOCAQEAcMklz7Vn1C3UEP0uz1ps6g/EhErTU77DEwSei9OW2lv84MHmtBHHz0ZI
    h27oTCYJCzVpaCiGfEhXbjw/HsGVM4KICcWb/U4mZ25ynd0R3Gs8C7IPtOjZ8hVJ
    hHQ4QnCwPB2e9+fTFcpwbleGG6FhRuusut0CLDe2/txnwouTTbLHKTGdiVVnMvnA
    /uiCNmSGCDLATdyusdbaqi87CtNNFsXaNX257LMG8KJ/bEbBnWhEc7IXhvdBMVEj
    d9TF3XOF1pxnB9aVtICdKTiETkAR02Zau/EZg0ZFJblvIavVdaJYeGOv9YhiIfAQ
    Fi+EIVTnEv7EuVc3x7uQJY6S0/B2MQ==
    -----END CERTIFICATE-----
```

Часть 2:

1. Загрузить файл запроса сертификата методом POST на адрес https://istupakov.ddns.net:4559/api/csr. Запомнить полученный в ответ в Location Header адрес для скачивания сертификата.

```
curl https://istupakov.ddns.net:4559/api/csr -F file=@client.csr --
cacert cryptolab-ca.crt -v

*   Trying 217.71.129.139:4559...
* Connected to istupakov.ddns.net (217.71.129.139) port 4559 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: cryptolab-ca.crt
*  CApath: none
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
```

```
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
* Server certificate:
*  subject: C=RU; L=Novosibirsk; O=Novosibirsk State Technical Uni-
versity; CN=CryptoLab Server
*  start date: Oct 14 15:12:52 2021 GMT
*  expire date: Oct 14 15:12:52 2022 GMT
*  subjectAltName: host "istupakov.ddns.net" matched cert's "istupa-
kov.ddns.net"
*  issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical Uni-
versity; CN=CryptoLab CA
*  SSL certificate verify ok.
* Using HTTP2, server supports multiplexing
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after
upgrade: len=0
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* Using Stream ID: 1 (easy handle 0x1bf7bba0f10)
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
> POST /api/csr HTTP/2
> Host: istupakov.ddns.net:4559
> user-agent: curl/7.80.0
> accept: */*
> content-length: 1345
> content-type: multipart/form-data; boundary=----------------------
---ab711b790417c6ed
>
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* We are completely uploaded and fine
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
< HTTP/2 202
< content-type: application/json; charset=utf-8
< date: Thu, 02 Dec 2021 18:06:22 GMT
```

```
< server: Kestrel
< location: https://istupakov.ddns.net:4559/api/csr/074ed8a7-a883-
45eb-beb1-701cd5105b1d
< strict-transport-security: max-age=2592000
<
{"id":"074ed8a7-a883-45eb-beb1-701cd5105b1d","subject":"CN = \"Cher-
nikov D.S., Zatolockaya J.A., Barsukova N.I.\", C = RU, L = Novosi-
birsk, O = Novosibirsk State Technical University","timestamp":"2021-
12-02T18:06:22.9790762Z"}* TLSv1.2 (IN), TLS header, Supplemental
data (23):
* Connection #0 to host istupakov.ddns.net left intact
```

Сертификат подписан.
https://istupakov.ddns.net:4559/api/csr/074ed8a7-a883-45eb-beb1-701cd5105b1d

-----BEGIN CERTIFICATE-----
MIIDuDCCAqCgAwIBAgIUBoZ9I819dZcm7ANlNxhthA4pg0EwDQYJKoZIhvcNAQEL
BQAwazELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK
DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEVMBMGA1UE
AwwMQ3J5cHRvTGFiIENBMB4XDTIxMTIwMzA1Mjc0N1oXDTIyMTIwMzA1Mjc0N1ow
gY8xOTA3BgNVBAMMMENoZXJuaWtvdiBELlMuLCBaYXRvbG9ja2F5YSBKLkEuLCBC
YXJzdWtvdmEgTi5JLjELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNr
MS8wLQYDVQQKDCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0
eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM4VKgiqXoC38gK9Q8s0
qKp3LnnBZu2wmhy2L00wvYQxYlWyCXdkrGFDlWeUZyHx+UA3GHZMTEFpvCreLDP7
NZhHbJ+CDBHcGaTp8/RAoiEQ2pg7KAiZbfHLXhBD9HJ7S2CHpoReciBMx7L6NudK
WZ/QFJu8x8F6L0QNqbd0Ji8loJZt9OuU2S80Y1YoQSzjg8P4bwmFcGHdTeTdY5gi
eFUAL6N98px1QSERzb2RWatVgVdySp4d0W65rpjbhAuYq21EQgm9s2Pq34ZUR6FQ
Dqf1ReiUpdtva5OoJSnHSgDXpIA6kADyH5v1/p8LbrrxahCaumBzoJYueLXeDfd9
wNUCAwEAAaMvMC0wCQYDVR0TBAIwADALBgNVHQ8EBAMCB4AwEwYDVR0lBAwwCgYI
KwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBAKvf6E6QlVIopVePnxrlDq+iMRnI
/71g4eqz9Bz+37wFLegY/0JvlJXK4nQgH++AbRYhzP/vavtSovhz6Etk1cnmiU9r
kJpTKEhc2ivyBueT/7XHGlAKZ75v5dK5xlAx9yig6HI5VLIB9NPPTs5+xaTi5vc3
IlRGBArzzFMIVuhw0PZn6mcPksx3IoR/RZX2R7ntohg8BWp224bREljTcTuxJaqS
RGvwp6zwukzXl0O7ORWNgnBe8QwuVZn6Ql6jz8VAD0eLh4T8RZei+SEni2rOE8W1
vgfL5O2bHSUEVsQa9K/k0ti8QMUyR6gpDHHGZBRmTIpGdicUDQV4LGswvGE=
-----END CERTIFICATE-----

Часть 3:

Выполняем запрос через curl:

curl https://istupakov.ddns.net:4559/api/chat/message -d @message.json -H "Content-Type: application/json" —cacert cryptolab-ca.crt -E server.crt -v —key client.key

```
*   Trying 217.71.129.139:4559...
* Connected to istupakov.ddns.net (217.71.129.139) port 4559 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
Enter PEM pass phrase:
*  CAfile: cryptolab-ca.crt
*  CApath: none
* TLSv1.0 (OUT), TLS header, Certificate Status (22):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS header, Certificate Status (22):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS header, Finished (20):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.2 (OUT), TLS header, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, CERT verify (15):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
* Server certificate:
*  subject: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab Server
*  start date: Oct 14 15:12:52 2021 GMT
*  expire date: Oct 14 15:12:52 2022 GMT
*  subjectAltName: host "istupakov.ddns.net" matched cert's "istupakov.ddns.net"
*  issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab CA
*  SSL certificate verify ok.
* Using HTTP2, server supports multiplexing
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* Using Stream ID: 1 (easy handle 0x277941c14a0)
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
```

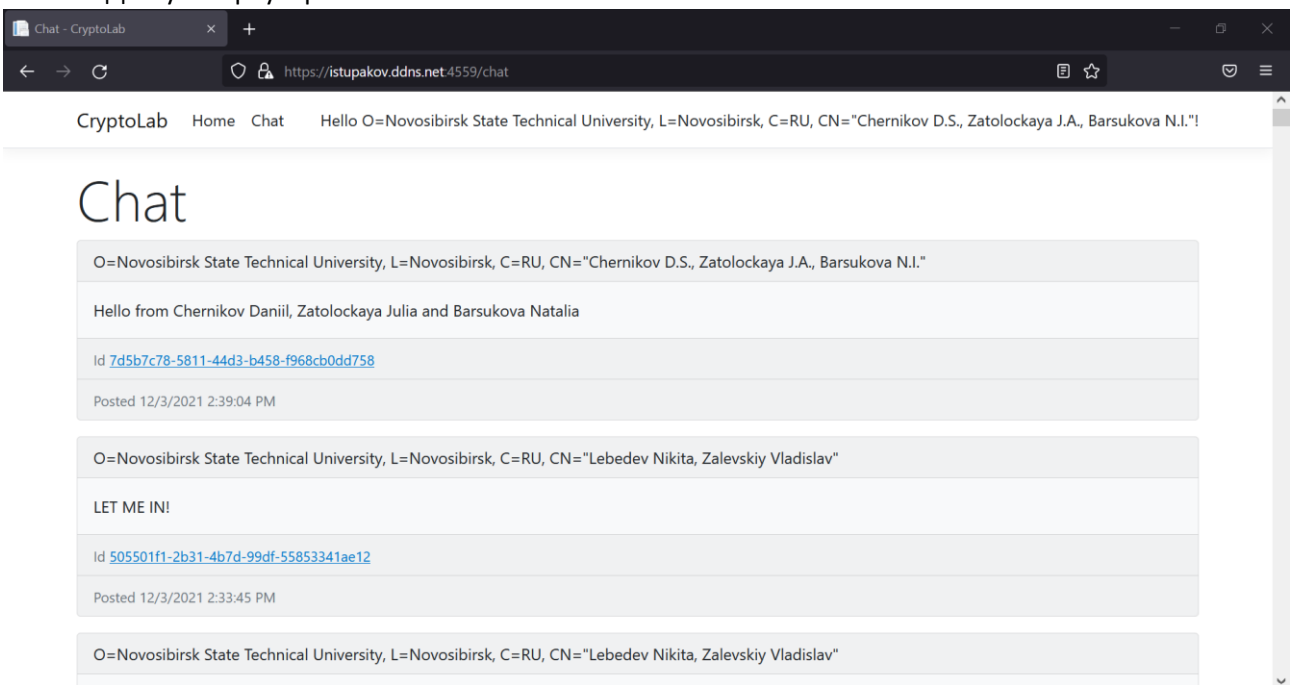
```
> POST /api/chat/message HTTP/2
> Host: istupakov.ddns.net:4559
> user-agent: curl/7.80.0
> accept: */*
> content-type: application/json
> content-length: 70
>
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* We are completely uploaded and fine
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (OUT), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
* TLSv1.2 (IN), TLS header, Supplemental data (23):
< HTTP/2 201
< content-type: application/json; charset=utf-8
< date: Fri, 03 Dec 2021 07:39:04 GMT
< server: Kestrel
< location: https://istupakov.ddns.net:4559/chat/message/7d5b7c78-5811-44d3-b458-f968cb0dd758
< strict-transport-security: max-age=2592000
<
{"message":"Hello from Chernikov Daniil, Zatolockaya Julia and Barsukova Natalia","user":"O=Novosibirsk State Technical University, L=Novosibirsk, C=RU, CN=\"Chernikov D.S., Zatolockaya J.A., Barsukova N.I.\"","timestamp":"2021-12-03T07:39:04.5914355Z","id":"7d5b7c78-5811-44d3-b458-f968cb0dd758"}* TLSv1.2 (IN), TLS header, Supplemental data (23):
* Connection #0 to host istupakov.ddns.net left intact
```

1. ссылка на сообщение:
https://istupakov.ddns.net:4559/chat/message/7d5b7c78-5811-44d3-b458-f968cb0dd758

Дополнительное задание:
Необходимо переконвертировать полученный сертификат в формат PKCS#12 и импортировать в браузер.

pkcs12 -export -in server.crt -inkey client.key -certfile cryptolab-ca.crt -name "description" -out usercert.p12

Доступ с браузера.



Доступ с браузера с телефона