

|  |  |
| --- | --- |
| Федеральное государственное бюджетное  образовательное учреждение высшего образования  «НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» | |
| Кафедра прикладной математики | |
| Практическое задание № 1 | |
| по дисциплине «Основы криптографии» | |
|  | |
|  |  |
| Группа ПМ-12 | Овчинников Иваны  Лойченко Данила  Березенцев Тимофей |
| Преподаватель | СТУПАКОВ ИЛЬЯ МИХАЙЛОВИЧ |
| Новосибирск, 2023 | |

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

# Часть 1:

1. Создать корневой сертификат с помощью OpenSSL (openssl req -new -config ca.conf -x509 -out ca.crt -keyout=ca.key), подготовив конфиг таким образом, чтобы openssl x509 -in ca.crt -text выдавал расшифровку вида:

ca.conf

[ req ]

default\_bits = 2048

distinguished\_name = req\_distinguished\_name

string\_mask = utf8only

default\_md = sha256

x509\_extensions = v3\_ca

prompt = no

[ req\_distinguished\_name ]

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

commonName = Some body once told me

[ v3\_ca ]

keyUsage = critical, keyCertSign

basicConstraints = critical, CA:true, pathlen:1

subjectKeyIdentifier = none

РАСШИФРОВКА ca.crt

> openssl x509 -in ca.crt -text

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

1e:0c:11:ae:86:ac:c2:bf:d2:07:75:e9:ac:b4:10:91:71:e2:94:cb

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Some body once told me

Validity

Not Before: Sep 30 08:53:42 2023 GMT

Not After : Oct 30 08:53:42 2023 GMT

Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Some body once told me

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:9f:42:23:03:1a:12:6e:f9:79:50:70:64:5a:ca:

0e:38:5a:5a:ea:2c:9e:53:b0:d6:fe:8a:be:0a:36:

0d:ad:84:6e:7a:b2:33:89:ed:f4:3e:e0:d6:77:6e:

b4:f9:90:93:12:0f:56:85:0c:ac:97:75:ea:2c:dc:

08:ce:c3:d2:1a:fb:07:18:72:05:f9:38:c3:a6:e0:

2c:c4:71:c2:8e:cb:a4:9b:72:d6:12:8f:f9:88:b2:

06:a4:18:de:5b:96:64:07:e7:62:37:84:69:33:06:

60:b4:52:86:70:a8:5a:a8:e3:2b:1f:4a:85:89:6e:

44:b5:f0:b0:13:d1:7c:92:87:5d:f9:0a:00:07:29:

2d:54:dc:32:8a:f0:f4:af:63:12:ec:c1:4f:a6:53:

7f:bf:87:a3:5a:d4:96:cc:79:2b:ac:01:23:2a:60:

50:48:f7:09:69:f5:be:9c:f2:d9:7d:d9:06:32:ab:

ca:97:68:f3:bd:da:7a:c5:51:a7:26:c7:f4:53:23:

10:a4:f6:03:0e:0a:8e:fd:6c:14:5a:66:56:76:f9:

1f:41:eb:11:03:69:2c:e5:30:f1:b3:75:18:63:92:

5d:b0:03:f9:31:2a:e8:02:7c:58:88:15:1e:dd:fc:

d5:83:21:0c:7c:97:c9:e2:c2:98:51:e4:6f:a4:10:

b7:c3

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Certificate Sign

X509v3 Basic Constraints: critical

CA:TRUE, pathlen:1

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

02:89:6e:ce:05:9a:e7:83:af:01:ab:61:f1:c6:9e:0d:b4:8b:

a3:ce:fe:5b:57:09:59:26:77:cc:8b:e3:d4:f4:76:77:d9:bd:

2d:09:dd:dc:1c:84:5c:be:71:91:54:b9:6b:b7:c3:45:cf:3a:

94:26:21:a2:84:2c:85:97:83:d2:22:9a:f2:98:da:0b:0c:45:

cf:77:98:be:e6:4c:1c:d3:28:83:12:92:16:5f:7f:a2:82:7b:

90:08:74:53:67:4d:6f:12:eb:99:4d:b8:e5:1b:34:95:73:6c:

a9:91:54:ab:17:4f:76:b0:9e:64:00:76:dc:10:c9:0a:4d:f1:

2c:62:da:ba:c9:3b:cf:a1:7c:ff:a0:56:d8:cf:85:ea:7a:3d:

18:f9:1e:08:d2:39:73:fd:9a:07:9d:46:e5:89:2a:91:15:6e:

9f:14:b6:9d:92:a5:7a:da:99:51:68:1a:96:20:84:f5:32:b7:

7d:84:de:53:f6:1c:1f:ea:6f:e5:d3:f1:2c:65:32:db:1e:c6:

03:d0:66:45:cb:3f:23:90:b0:8c:03:eb:33:20:59:9d:f3:f4:

3c:8d:60:0f:17:2c:d4:ce:38:91:d7:a0:d5:a9:0c:56:11:03:

04:1d:eb:46:84:22:20:3a:84:4d:ad:c0:f4:5e:d3:5d:75:5b:

ef:a1:a7:b8

-----BEGIN CERTIFICATE-----

MIIDnjCCAoagAwIBAgIUHgwRroaswr/SB3XprLQQkXHilMswDQYJKoZIhvcNAQEL

BQAwdTELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEfMB0GA1UE

AwwWU29tZSBib2R5IG9uY2UgdG9sZCBtZTAeFw0yMzA5MzAwODUzNDJaFw0yMzEw

MzAwODUzNDJaMHUxCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2liaXJzazEv

MC0GA1UECgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZlcnNpdHkx

HzAdBgNVBAMMFlNvbWUgYm9keSBvbmNlIHRvbGQgbWUwggEiMA0GCSqGSIb3DQEB

AQUAA4IBDwAwggEKAoIBAQCfQiMDGhJu+XlQcGRayg44WlrqLJ5TsNb+ir4KNg2t

hG56sjOJ7fQ+4NZ3brT5kJMSD1aFDKyXdeos3AjOw9Ia+wcYcgX5OMOm4CzEccKO

y6SbctYSj/mIsgakGN5blmQH52I3hGkzBmC0UoZwqFqo4ysfSoWJbkS18LAT0XyS

h135CgAHKS1U3DKK8PSvYxLswU+mU3+/h6Na1JbMeSusASMqYFBI9wlp9b6c8tl9

2QYyq8qXaPO92nrFUacmx/RTIxCk9gMOCo79bBRaZlZ2+R9B6xEDaSzlMPGzdRhj

kl2wA/kxKugCfFiIFR7d/NWDIQx8l8niwphR5G+kELfDAgMBAAGjJjAkMA4GA1Ud

DwEB/wQEAwICBDASBgNVHRMBAf8ECDAGAQH/AgEBMA0GCSqGSIb3DQEBCwUAA4IB

AQACiW7OBZrng68Bq2Hxxp4NtIujzv5bVwlZJnfMi+PU9HZ32b0tCd3cHIRcvnGR

VLlrt8NFzzqUJiGihCyFl4PSIprymNoLDEXPd5i+5kwc0yiDEpIWX3+ignuQCHRT

Z01vEuuZTbjlGzSVc2ypkVSrF092sJ5kAHbcEMkKTfEsYtq6yTvPoXz/oFbYz4Xq

ej0Y+R4I0jlz/ZoHnUbliSqRFW6fFLadkqV62plRaBqWIIT1Mrd9hN5T9hwf6m/l

0/EsZTLbHsYD0GZFyz8jkLCMA+szIFmd8/Q8jWAPFyzUzjiR16DVqQxWEQMEHetG

hCIgOoRNrcD0XtNddVvvoae4

-----END CERTIFICATE-----

2 .Создать запрос клиентского сертификата (файл .csr) и приватный ключ с помощью OpenSSL (openssl req -new -config client.conf -out client.csr -keyout=client.key), подготовив конфиг таким образом, чтобы openssl req -in client.csr -text выдавал расшифровку вида:

client.conf

[ req ]

prompt = no

days = 365

distinguished\_name = req\_distinguished\_name

req\_extensions = v3\_req

default\_bits = 2048

[ req\_distinguished\_name ]

commonName = Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

[ v3\_req ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:false

РАСШИФРОВКА client.csr

> openssl req -in client.csr -text

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = "Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:89:4a:0c:1a:19:a8:60:54:b1:2f:a0:69:d6:34:

79:ce:83:bf:5a:79:2b:2e:5a:f3:9b:ed:34:8e:9c:

6c:bc:b9:98:ed:b0:34:6b:2f:ce:0e:14:d1:be:5d:

38:f2:3c:04:21:0b:ba:22:f2:b5:54:25:a2:5d:8d:

11:e3:0c:f7:86:20:5e:67:ac:1b:41:c0:dc:e5:ff:

be:18:f9:84:b0:cc:c1:d6:6d:f1:8b:a7:32:1e:30:

5f:ad:e4:2a:02:0a:58:90:73:b3:e4:5c:13:74:70:

9d:de:3b:a2:d8:dd:b0:05:38:38:a5:c1:5e:a3:8c:

d6:31:8d:59:31:e1:b1:f0:2b:f6:30:ff:e3:1a:98:

74:97:74:d9:45:98:8a:56:c0:d2:b6:b1:66:d1:02:

46:fd:c1:66:18:65:6e:e4:40:1c:99:69:46:09:2f:

5e:5f:54:f4:2e:8e:11:2f:01:b1:50:a6:8c:35:30:

c4:8c:36:6d:af:36:0d:26:f7:6e:ec:53:2c:0e:32:

bd:f8:58:97:fe:87:a2:e4:d7:31:fa:4d:97:7f:39:

92:23:48:22:76:b8:cd:9e:6b:df:bb:66:d7:cc:a4:

fc:86:96:41:3d:6d:2f:45:29:04:22:4d:94:0a:53:

ee:16:93:71:f2:22:c8:a7:c0:82:9c:55:a9:c6:7b:

dd:33

Exponent: 65537 (0x10001)

Attributes:

Requested Extensions:

X509v3 Key Usage:

Digital Signature

X509v3 Extended Key Usage:

TLS Web Client Authentication

X509v3 Basic Constraints:

CA:FALSE

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

6f:e1:83:70:ae:64:03:9c:e7:3d:17:ec:3d:2f:12:49:73:e6:

32:ef:f7:1a:a7:f4:2e:b5:9a:6f:ae:1d:c6:a4:f9:3e:f0:48:

09:5a:1d:b3:e1:47:e3:0c:05:fd:f7:30:ea:c3:5b:9e:1c:97:

04:ee:d1:36:4c:5c:e4:df:ca:fb:d2:d9:15:4a:d8:fe:78:fd:

71:d3:5a:73:fb:ad:5c:68:92:4b:87:f0:f7:ce:77:f3:0e:8e:

46:4d:e5:ba:92:37:ba:ec:b2:61:23:07:fd:cc:ef:d2:5e:14:

c9:2f:53:43:c8:cf:be:5d:9b:d8:06:43:cb:58:c9:39:81:43:

0c:30:a2:a6:2d:c9:93:5a:71:7b:a6:4f:d2:58:0c:c8:75:b5:

14:97:3c:f4:b5:3d:be:6b:cc:9c:75:07:b1:34:e7:58:8d:82:

d7:cb:ca:9c:e8:6a:72:be:01:9a:c2:a9:ae:c5:10:52:5d:10:

fd:8b:df:a1:53:8d:9a:60:90:b9:14:f2:6b:84:ba:26:48:4c:

d8:6d:c4:c0:1f:41:6c:a4:28:14:8d:59:1b:ee:23:2e:5a:cc:

0e:9b:fc:4a:0c:dc:dc:3b:32:33:cf:aa:f4:7e:06:ea:a8:8b:

ee:e6:cd:39:e2:bb:ce:d8:05:eb:b3:84:99:6a:e2:ff:c3:ea:

5d:c2:59:29

-----BEGIN CERTIFICATE REQUEST-----

MIIDEjCCAfoCAQAwgY4xODA2BgNVBAMML092Y2hpbm5pa292IEkuUiwgTG95Y2hl

bmtvIEQuUywgQmVyZXplbnRzZXYgVC5EMQswCQYDVQQGEwJSVTEUMBIGA1UEBwwL

Tm92b3NpYmlyc2sxLzAtBgNVBAoMJk5vdm9zaWJpcnNrIFN0YXRlIFRlY2huaWNh

bCBVbml2ZXJzaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAiUoM

GhmoYFSxL6Bp1jR5zoO/WnkrLlrzm+00jpxsvLmY7bA0ay/ODhTRvl048jwEIQu6

IvK1VCWiXY0R4wz3hiBeZ6wbQcDc5f++GPmEsMzB1m3xi6cyHjBfreQqAgpYkHOz

5FwTdHCd3jui2N2wBTg4pcFeo4zWMY1ZMeGx8Cv2MP/jGph0l3TZRZiKVsDStrFm

0QJG/cFmGGVu5EAcmWlGCS9eX1T0Lo4RLwGxUKaMNTDEjDZtrzYNJvdu7FMsDjK9

+FiX/oei5Ncx+k2XfzmSI0gidrjNnmvfu2bXzKT8hpZBPW0vRSkEIk2UClPuFpNx

8iLIp8CCnFWpxnvdMwIDAQABoD4wPAYJKoZIhvcNAQkOMS8wLTALBgNVHQ8EBAMC

B4AwEwYDVR0lBAwwCgYIKwYBBQUHAwIwCQYDVR0TBAIwADANBgkqhkiG9w0BAQsF

AAOCAQEAb+GDcK5kA5znPRfsPS8SSXPmMu/3Gqf0LrWab64dxqT5PvBICVods+FH

4wwF/fcw6sNbnhyXBO7RNkxc5N/K+9LZFUrY/nj9cdNac/utXGiSS4fw98538w6O

Rk3lupI3uuyyYSMH/czv0l4UyS9TQ8jPvl2b2AZDy1jJOYFDDDCipi3Jk1pxe6ZP

0lgMyHW1FJc89LU9vmvMnHUHsTTnWI2C18vKnOhqcr4BmsKprsUQUl0Q/YvfoVON

mmCQuRTya4S6JkhM2G3EwB9BbKQoFI1ZG+4jLlrMDpv8Sgzc3DsyM8+q9H4G6qiL

7ubNOeK7ztgF67OEmWri/8PqXcJZKQ==

-----END CERTIFICATE REQUEST-----

3. Создать запрошенный сертификат, подписав его с помощью корневого (openssl x509 -req -extfile client.conf -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt -extensions v3), подготовив конфиг таким образом, чтобы openssl x509 -in client.crt -text выдавал расшифровку вида:

client.conf

[ req ]

prompt = no

days = 365

distinguished\_name = req\_distinguished\_name

req\_extensions = v3\_req

default\_bits = 2048

[ req\_distinguished\_name ]

commonName = Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

[ v3\_req ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:false

[ v3 ]

basicConstraints = CA:false

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

subjectKeyIdentifier = none

authorityKeyIdentifier = none

Расшифровка client.crt

> openssl x509 -in client.crt -text

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

09:78:4b:bf:b4:f3:76:21:08:36:d7:36:cb:41:8d:e3:9a:9b:f2:04

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Some body once told me

Validity

Not Before: Oct 4 09:04:05 2023 GMT

Not After : Nov 3 09:04:05 2023 GMT

Subject: CN = "Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:89:4a:0c:1a:19:a8:60:54:b1:2f:a0:69:d6:34:

79:ce:83:bf:5a:79:2b:2e:5a:f3:9b:ed:34:8e:9c:

6c:bc:b9:98:ed:b0:34:6b:2f:ce:0e:14:d1:be:5d:

38:f2:3c:04:21:0b:ba:22:f2:b5:54:25:a2:5d:8d:

11:e3:0c:f7:86:20:5e:67:ac:1b:41:c0:dc:e5:ff:

be:18:f9:84:b0:cc:c1:d6:6d:f1:8b:a7:32:1e:30:

5f:ad:e4:2a:02:0a:58:90:73:b3:e4:5c:13:74:70:

9d:de:3b:a2:d8:dd:b0:05:38:38:a5:c1:5e:a3:8c:

d6:31:8d:59:31:e1:b1:f0:2b:f6:30:ff:e3:1a:98:

74:97:74:d9:45:98:8a:56:c0:d2:b6:b1:66:d1:02:

46:fd:c1:66:18:65:6e:e4:40:1c:99:69:46:09:2f:

5e:5f:54:f4:2e:8e:11:2f:01:b1:50:a6:8c:35:30:

c4:8c:36:6d:af:36:0d:26:f7:6e:ec:53:2c:0e:32:

bd:f8:58:97:fe:87:a2:e4:d7:31:fa:4d:97:7f:39:

92:23:48:22:76:b8:cd:9e:6b:df:bb:66:d7:cc:a4:

fc:86:96:41:3d:6d:2f:45:29:04:22:4d:94:0a:53:

ee:16:93:71:f2:22:c8:a7:c0:82:9c:55:a9:c6:7b:

dd:33

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Key Usage:

Digital Signature

X509v3 Extended Key Usage:

TLS Web Client Authentication

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

56:02:c3:48:0f:54:b5:da:86:c6:be:66:f7:45:b8:3b:e7:54:

f2:11:4d:1c:61:46:c6:9c:9b:81:e2:79:e8:67:88:d3:13:47:

56:89:35:f5:49:91:a8:ef:f1:1e:88:5b:99:20:a5:ad:75:35:

6d:10:2e:7e:40:16:a1:5b:24:ba:19:de:02:72:79:f6:87:8e:

10:3f:4b:5d:c8:ef:b9:20:a3:4a:1e:f8:2b:16:75:12:60:9a:

62:66:47:16:57:bf:e2:0d:37:a2:15:d9:21:de:02:bb:df:f8:

dc:04:99:24:cb:57:4a:2a:b9:56:a5:8b:c9:d5:92:c2:91:76:

46:93:f5:9c:e4:57:38:14:f8:17:2e:df:b9:14:d1:f1:cf:e7:

02:57:2d:d9:ae:a0:a8:e4:0b:10:ee:e9:04:43:82:92:56:74:

ee:82:29:40:7f:e3:79:bf:86:a5:b3:52:b9:37:83:04:c4:ff:

33:cd:9b:10:7e:64:66:bb:d3:41:dc:34:ff:30:72:a5:69:59:

84:00:fb:d7:77:8d:12:3e:79:64:f5:6d:bf:66:b9:2a:6d:c7:

ff:88:48:d3:ae:d3:2a:eb:f6:2d:83:08:92:11:34:69:64:1e:

52:95:39:52:87:4f:96:a4:51:b5:cb:77:59:7c:56:77:84:c4:

51:03:53:5f

-----BEGIN CERTIFICATE-----

MIIDwTCCAqmgAwIBAgIUCXhLv7TzdiEINtc2y0GN45qb8gQwDQYJKoZIhvcNAQEL

BQAwdTELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEfMB0GA1UE

AwwWU29tZSBib2R5IG9uY2UgdG9sZCBtZTAeFw0yMzEwMDQwOTA0MDVaFw0yMzEx

MDMwOTA0MDVaMIGOMTgwNgYDVQQDDC9PdmNoaW5uaWtvdiBJLlIsIExveWNoZW5r

byBELlMsIEJlcmV6ZW50c2V2IFQuRDELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05v

dm9zaWJpcnNrMS8wLQYDVQQKDCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwg

VW5pdmVyc2l0eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIlKDBoZ

qGBUsS+gadY0ec6Dv1p5Ky5a85vtNI6cbLy5mO2wNGsvzg4U0b5dOPI8BCELuiLy

tVQlol2NEeMM94YgXmesG0HA3OX/vhj5hLDMwdZt8YunMh4wX63kKgIKWJBzs+Rc

E3Rwnd47otjdsAU4OKXBXqOM1jGNWTHhsfAr9jD/4xqYdJd02UWYilbA0raxZtEC

Rv3BZhhlbuRAHJlpRgkvXl9U9C6OES8BsVCmjDUwxIw2ba82DSb3buxTLA4yvfhY

l/6HouTXMfpNl385kiNIIna4zZ5r37tm18yk/IaWQT1tL0UpBCJNlApT7haTcfIi

yKfAgpxVqcZ73TMCAwEAAaMvMC0wCQYDVR0TBAIwADALBgNVHQ8EBAMCB4AwEwYD

VR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBAFYCw0gPVLXahsa+

ZvdFuDvnVPIRTRxhRsacm4HieehniNMTR1aJNfVJkajv8R6IW5kgpa11NW0QLn5A

FqFbJLoZ3gJyefaHjhA/S13I77kgo0oe+CsWdRJgmmJmRxZXv+INN6IV2SHeArvf

+NwEmSTLV0oquVali8nVksKRdkaT9ZzkVzgU+Bcu37kU0fHP5wJXLdmuoKjkCxDu

6QRDgpJWdO6CKUB/43m/hqWzUrk3gwTE/zPNmxB+ZGa700HcNP8wcqVpWYQA+9d3

jRI+eWT1bb9muSptx/+ISNOu0yrr9i2DCJIRNGlkHlKVOVKHT5akUbXLd1l8VneE

xFEDU18=

-----END CERTIFICATE-----

**Часть 2:**

1) curl https://istupakov.ddns.net:4203/api/csr -F file=@client.csr --cacert cryptolab-ca.crt -v

\* Trying 217.71.129.139:4203...

\* Connected to istupakov.ddns.net (217.71.129.139) port 4203 (#0)

\* schannel: disabled automatic use of client certificate

\* ALPN: offers http/1.1

\* schannel: added 1 certificate(s) from CA file 'cryptolab-ca.crt'

\* schannel: connection hostname (istupakov.ddns.net) validated against certificate name (istupakov.ddns.net)

\* ALPN: server accepted http/1.1

\* using HTTP/1.1

> POST /api/csr HTTP/1.1

> Host: istupakov.ddns.net:4203

> User-Agent: curl/8.0.1

> Accept: \*/\*

> Content-Length: 1364

> Content-Type: multipart/form-data; boundary=------------------------a89ed3e86bcb7b2e

>

\* We are completely uploaded and fine

< HTTP/1.1 202 Accepted

< Content-Type: application/json; charset=utf-8

< Date: Wed, 04 Oct 2023 09:09:15 GMT

< Server: Kestrel

< Location: https://istupakov.ddns.net:4203/api/csr/ac119848-e680-4eca-87d1-2ea724655943

< Transfer-Encoding: chunked

< Strict-Transport-Security: max-age=2592000

<

{"id":"ac119848-e680-4eca-87d1-2ea724655943","subject":"CN = \"Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D\", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University","timestamp":"2023-10-04T09:09:16.2652603Z"}\* Connection #0 to host istupakov.ddns.net left intact

2) Подойти к преподавателю и попросить подписать ваш запрос.

3) openssl x509 -in SignedCRT.crt -text

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

68:75:7e:3f:50:88:20:bb:33:84:2c:2d:fa:ea:80:66:ad:80:e6:9a

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = CryptoLab Root CA

Validity

Not Before: Oct 4 09:16:43 2023 GMT

Not After : Oct 3 09:16:43 2024 GMT

Subject: CN = "Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:89:4a:0c:1a:19:a8:60:54:b1:2f:a0:69:d6:34:

79:ce:83:bf:5a:79:2b:2e:5a:f3:9b:ed:34:8e:9c:

6c:bc:b9:98:ed:b0:34:6b:2f:ce:0e:14:d1:be:5d:

38:f2:3c:04:21:0b:ba:22:f2:b5:54:25:a2:5d:8d:

11:e3:0c:f7:86:20:5e:67:ac:1b:41:c0:dc:e5:ff:

be:18:f9:84:b0:cc:c1:d6:6d:f1:8b:a7:32:1e:30:

5f:ad:e4:2a:02:0a:58:90:73:b3:e4:5c:13:74:70:

9d:de:3b:a2:d8:dd:b0:05:38:38:a5:c1:5e:a3:8c:

d6:31:8d:59:31:e1:b1:f0:2b:f6:30:ff:e3:1a:98:

74:97:74:d9:45:98:8a:56:c0:d2:b6:b1:66:d1:02:

46:fd:c1:66:18:65:6e:e4:40:1c:99:69:46:09:2f:

5e:5f:54:f4:2e:8e:11:2f:01:b1:50:a6:8c:35:30:

c4:8c:36:6d:af:36:0d:26:f7:6e:ec:53:2c:0e:32:

bd:f8:58:97:fe:87:a2:e4:d7:31:fa:4d:97:7f:39:

92:23:48:22:76:b8:cd:9e:6b:df:bb:66:d7:cc:a4:

fc:86:96:41:3d:6d:2f:45:29:04:22:4d:94:0a:53:

ee:16:93:71:f2:22:c8:a7:c0:82:9c:55:a9:c6:7b:

dd:33

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Key Identifier:

F5:AD:C7:C4:8B:CB:F7:B1:20:9C:FA:5E:5C:96:66:6D:AD:63:92:AB

X509v3 Authority Key Identifier:

keyid:FF:63:D1:82:FB:64:0B:24:FC:D3:B6:01:24:A1:0C:8B:54:40:C3:29

DirName:/C=RU/L=Novosibirsk/O=Novosibirsk State Technical University/CN=CryptoLab Root CA

serial:46:81:D2:1A:25:3A:5C:43:FD:43:7D:48:8F:65:8D:24:09:BF:2E:CE

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment

X509v3 Extended Key Usage: critical

TLS Web Client Authentication

X509v3 CRL Distribution Points:

Full Name:

URI:http://istupakov.ddns.net:4185/cryptolab.crl.pem

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

87:53:a3:22:19:35:19:1d:47:ca:1f:06:53:08:3d:aa:3e:3f:

d6:d4:35:ce:ee:57:39:57:16:3c:e8:6b:27:d2:c7:88:e6:54:

a8:9f:0d:ed:45:8c:c5:52:9f:33:8b:fe:8e:4d:3b:f1:6e:9d:

c6:91:3d:1a:9c:c4:fc:e5:d8:df:3a:ca:df:bc:59:9e:5d:8d:

c3:08:62:5b:40:8f:26:2f:7a:bc:41:f4:99:61:5a:fd:54:e8:

04:6e:02:9b:39:0d:46:d3:4c:6f:58:aa:be:2a:b6:00:ca:7f:

cb:cd:58:6a:37:93:2f:7c:d2:51:fc:94:2f:c3:dd:e5:8d:a3:

a7:bb:31:d2:5c:40:5b:61:a1:29:0d:03:ac:1c:1b:d5:ae:f2:

29:a5:f5:cc:f7:f4:6a:68:b4:3f:20:e1:c7:4e:cf:11:f2:1a:

9c:5a:f5:91:b5:67:8d:9a:ef:be:b1:57:8f:a4:64:6e:b8:09:

e2:3f:d3:65:67:e5:1c:c1:21:06:33:7a:99:c9:3a:33:90:16:

11:08:d2:85:22:58:2b:a4:c9:08:68:0b:54:ed:3a:dd:ca:d5:

65:c6:bc:e8:6b:da:2f:12:5a:f9:c9:07:15:c8:9b:a0:ee:e8:

fc:b4:7a:93:b9:d2:a2:35:f9:c1:0b:b6:b9:f5:0f:5b:1a:5e:

a5:50:b7:84

-----BEGIN CERTIFICATE-----

MIIE2zCCA8OgAwIBAgIUaHV+P1CIILszhCwt+uqAZq2A5powDQYJKoZIhvcNAQEL

BQAwcDELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEaMBgGA1UE

AwwRQ3J5cHRvTGFiIFJvb3QgQ0EwHhcNMjMxMDA0MDkxNjQzWhcNMjQxMDAzMDkx

NjQzWjCBjjE4MDYGA1UEAwwvT3ZjaGlubmlrb3YgSS5SLCBMb3ljaGVua28gRC5T

LCBCZXJlemVudHNldiBULkQxCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2li

aXJzazEvMC0GA1UECgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZl

cnNpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCJSgwaGahgVLEv

oGnWNHnOg79aeSsuWvOb7TSOnGy8uZjtsDRrL84OFNG+XTjyPAQhC7oi8rVUJaJd

jRHjDPeGIF5nrBtBwNzl/74Y+YSwzMHWbfGLpzIeMF+t5CoCCliQc7PkXBN0cJ3e

O6LY3bAFODilwV6jjNYxjVkx4bHwK/Yw/+MamHSXdNlFmIpWwNK2sWbRAkb9wWYY

ZW7kQByZaUYJL15fVPQujhEvAbFQpow1MMSMNm2vNg0m927sUywOMr34WJf+h6Lk

1zH6TZd/OZIjSCJ2uM2ea9+7ZtfMpPyGlkE9bS9FKQQiTZQKU+4Wk3HyIsinwIKc

VanGe90zAgMBAAGjggFMMIIBSDAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBT1rcfE

i8v3sSCc+l5clmZtrWOSqzCBrQYDVR0jBIGlMIGigBT/Y9GC+2QLJPzTtgEkoQyL

VEDDKaF0pHIwcDELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8w

LQYDVQQKDCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEa

MBgGA1UEAwwRQ3J5cHRvTGFiIFJvb3QgQ0GCFEaB0holOlxD/UN9SI9ljSQJvy7O

MA4GA1UdDwEB/wQEAwIF4DAWBgNVHSUBAf8EDDAKBggrBgEFBQcDAjBBBgNVHR8E

OjA4MDagNKAyhjBodHRwOi8vaXN0dXBha292LmRkbnMubmV0OjQxODUvY3J5cHRv

bGFiLmNybC5wZW0wDQYJKoZIhvcNAQELBQADggEBAIdToyIZNRkdR8ofBlMIPao+

P9bUNc7uVzlXFjzoayfSx4jmVKifDe1FjMVSnzOL/o5NO/FuncaRPRqcxPzl2N86

yt+8WZ5djcMIYltAjyYverxB9JlhWv1U6ARuAps5DUbTTG9Yqr4qtgDKf8vNWGo3

ky980lH8lC/D3eWNo6e7MdJcQFthoSkNA6wcG9Wu8iml9cz39GpotD8g4cdOzxHy

Gpxa9ZG1Z42a776xV4+kZG64CeI/02Vn5RzBIQYzepnJOjOQFhEI0oUiWCukyQho

C1TtOt3K1WXGvOhr2i8SWvnJBxXIm6Du6Py0epO50qI1+cELtrn1D1saXqVQt4Q=

-----END CERTIFICATE-----

**Часть 3:**

1) Запрос с сертификатом из 1 части

curl -X POST https://istupakov.ddns.net:4203/api/chat/message -H 'Content-Type: application/json' -d "\"Ovchinnikov Loychenko Berezencev\" " --cert client.crt --key client.key --cacert cryptolab-ca.crt -v

Note: Unnecessary use of -X or --request, POST is already inferred.

\* Trying 217.71.129.139:4203...

\* Connected to istupakov.ddns.net (217.71.129.139) port 4203 (#0)

\* ALPN, offering h2

\* ALPN, offering http/1.1

Enter PEM pass phrase:

\* CAfile: cryptolab-ca.crt

\* CApath: /etc/ssl/certs

\* 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: Sep 16 09:40:52 2023 GMT

\* expire date: Jun 11 09:40:52 2026 GMT

\* subjectAltName: host "istupakov.ddns.net" matched cert's "istupakov.ddns.net"

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab Root 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 0x559f04a14560)

\* TLSv1.2 (OUT), TLS header, Supplemental data (23):

> POST /api/chat/message HTTP/2

> Host: istupakov.ddns.net:4203

> user-agent: curl/7.81.0

> accept: \*/\*

> content-type: application/json

> content-length: 35

>

\* TLSv1.2 (OUT), TLS header, Supplemental data (23):

\* We are completely uploaded and fine

\* 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):

\* TLSv1.3 (OUT), TLS alert, decode error (562):

\* OpenSSL SSL\_read: error:0A000126:SSL routines::unexpected eof while reading, errno 0

\* Failed receiving HTTP2 data

\* OpenSSL SSL\_write: SSL\_ERROR\_SYSCALL, errno 0

\* Failed sending HTTP2 data

\* Connection #0 to host istupakov.ddns.net left intact

curl: (56) OpenSSL SSL\_read: error:0A000126:SSL routines::unexpected eof while reading, errno 0

2) Запрос с сертификатом подписанным у преподавателя

curl -X POST https://istupakov.ddns.net:4203/api/chat/message -H 'Content-Type: application/json' -d "\"Ovchinnikov Loychenko Berezencev\" " --cert SignedCRT.crt --key client.key --cacert cryptolab-ca.crt -v

Note: Unnecessary use of -X or --request, POST is already inferred.

\* Trying 217.71.129.139:4203...

\* Connected to istupakov.ddns.net (217.71.129.139) port 4203 (#0)

\* ALPN, offering h2

\* ALPN, offering http/1.1

Enter PEM pass phrase:

\* CAfile: cryptolab-ca.crt

\* CApath: /etc/ssl/certs

\* 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: Sep 16 09:40:52 2023 GMT

\* expire date: Jun 11 09:40:52 2026 GMT

\* subjectAltName: host "istupakov.ddns.net" matched cert's "istupakov.ddns.net"

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab Root 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 0x55f5ff3a0560)

\* TLSv1.2 (OUT), TLS header, Supplemental data (23):

> POST /api/chat/message HTTP/2

> Host: istupakov.ddns.net:4203

> user-agent: curl/7.81.0

> accept: \*/\*

> content-type: application/json

> content-length: 35

>

\* TLSv1.2 (OUT), TLS header, Supplemental data (23):

\* We are completely uploaded and fine

\* 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 (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: Wed, 04 Oct 2023 10:12:01 GMT

< server: Kestrel

< location: https://istupakov.ddns.net:4203/chat/message/8605206f-33f4-4304-943d-f1979ab4d3b8

< strict-transport-security: max-age=2592000

<

\* TLSv1.2 (IN), TLS header, Supplemental data (23):

\* Connection #0 to host istupakov.ddns.net left intact

{"message":"Ovchinnikov Loychenko Berezencev","user":"O=Novosibirsk State Technical University, L=Novosibirsk, C=RU, CN=\"Ovchinnikov I.R, Loychenko D.S, Berezentsev T.D\"","timestamp":"2023-10-04T10:12

# 3)

