МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

НГТУ  НЭТИ

Кафедра прикладной математики

Лабораторная работа № 3

по дисциплине «Основы криптографии»

Место для ввода текста.

Группа	ПМ-93, ПМ-92
Бригада	29
	ИВАНОВ ВЛАДИСЛАВ
	ОБЕРШТ ЕЛЕНА
Преподаватели	СТУПАКОВ И.М.
Дата	14.12.2021

Новосибирск

Задание

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:

```
~/Documents/lab3 openssl req -new -config ca.conf -x509 -out ca.crt -keyout=ca.key -days 90
Generating a RSA private key
.................................+++++
.....................................................................................................+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:
Locality Name (eg, city) []:Novosibirsk
Organization Name(eg, org) []:NSTU
Common Name (eg, YOUR name) []:Vladislav, Helen
~/Documents/lab3
```

```
~/Documents/lab3 openssl x509 -in ca.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3e:b1:97:02:79:12:59:86:a5:a1:fd:7c:67:72:42:ce:75:03:52:3b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RU, L = Novosibirsk, O = NSTU, CN = "Vladislav, Helen"
        Validity
            Not Before: Dec  9 12:21:08 2021 GMT
            Not After : Mar  9 12:21:08 2022 GMT
        Subject: C = RU, L = Novosibirsk, O = NSTU, CN = "Vladislav, Helen"
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b2:8f:d1:f7:57:13:2a:e7:d5:56:5a:57:98:98:
                    22:e8:4b:13:8c:be:37:b6:65:79:a1:c9:79:b6:3e:
                    27:86:30:a4:b2:48:74:97:db:95:b5:61:5c:5b:40:
```

```
                    7d:55:dd:b8:82:79:a0:4e:b4:d3:5f:59:19:fa:5d:
                    34:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:1
    Signature Algorithm: sha256WithRSAEncryption
         80:0d:1d:5f:5a:f5:f4:ce:47:28:86:8f:79:d3:64:8a:6d:1d:
         fb:30:85:36:df:23:5a:72:2a:ef:cf:5f:96:30:4f:e9:11:0f:
         d0:00:4e:42:95:07:45:86:78:f0:f0:f3:83:b6:9d:4a:d6:61:
         06:60:03:51:1e:b7:99:ce:91:6c:fb:ac:7c:52:cd:f5:f3:aa:
         f0:33:09:54:7b:26:04:51:6c:ea:d4:6e:f2:4b:07:1a:4e:d4:
         f1:2c:23:64:7f:53:07:7e:2b:14:a7:4e:54:bc:6b:c6:d8:50:
         c5:79:71:78:35:2f:7f:10:87:12:6e:5b:fd:cb:12:34:6d:55:
         96:83:13:19:d9:f3:c5:c6:dc:6a:73:53:ca:9d:ef:7e:13:05:
         05:e8:76:6c:3d:7c:37:5d:ee:37:ba:e1:03:86:c6:ac:0f:fb:
         4b:4f:6e:8f:4b:fe:cd:22:56:ff:fc:a5:e7:d4:4f:87:9c:0f:
         d0:6a:30:91:f1:07:9c:28:a8:95:72:2d:50:85:35:8a:bd:c9:
         6a:e1:80:e8:7b:e4:3e:cc:43:fe:d4:7a:94:af:3b:0b:bc:dd:
         aa:5b:7b:2e:0d:f4:6a:1f:75:40:fe:1b:1d:8c:ab:a1:8c:7e:
         e1:52:ac:fa:c5:27:17:3d:4a:1f:af:b0:b4:c5:2a:f5:71:10:
         72:7c:c3:3b
-----BEGIN CERTIFICATE-----
MIIDTjCCAjagAwIBAgIUPrGXAnkSWYalof18Z3JCznUDUjswDQYJKoZIhvcNAQEL
```

Конфиг:

```
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_ca

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = RU
countryName_min = 2
countryName_max = 2
localityName = Locality Name (eg, city)
organizationName = Organization Name(eg, org)
commonName = Common Name (eg, YOUR name)
commonName_max = 64

[ v3_req ]
keyUsage = digitalSignature, nonRepudiation

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

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:

```
~/Documents/lab3 openssl req -new -config client.conf -out client.csr -keyout=client.key -days 90
Ignoring -days; not generating a certificate
Generating a RSA private key
..............+++++
..+++++
writing new private key to 'client.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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.
-----
Common Name (eg, YOUR name) []:Vladislav, Helen
Country Name (2 letter code) [RU]:
Locality Name (eg, city) []:Novosibirsk
Organization Name(eg, org) []:NSTU
~/Documents/lab3
```

```
~/Documents/lab3 openssl req -in client.csr -text
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = "Vladislav, Helen", C = RU, L = Novosibirsk, O = NSTU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bf:21:eb:ff:1e:a2:4f:31:d7:fa:22:0d:72:a0:
                    82:0e:e4:18:72:79:39:b4:f8:ef:21:47:11:a5:1f:
                       fc:42:9c:4d:6d:fd:a7:a2:4e:33:d6:79:97:00:2e:
                       a1:9d
                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
         ac:92:ab:c2:78:ae:4d:ba:e6:4e:56:b3:27:19:d3:2c:80:18:
         74:20:38:6b:63:ae:99:20:9f:3f:78:26:48:63:4b:f4:21:2b:
         ce:10:87:ca:90:ec:88:4c:cf:2f:e1:f5:b3:80:8c:e8:2e:ea:
         63:af:c9:0a:02:b6:04:82:1a:31:3c:7a:32:fa:76:53:6c:7f:
         7c:63:b8:5a:1c:ac:5b:26:82:ec:77:77:9d:ea:1c:84:96:8e:
         b7:d5:16:a8:50:54:c5:f9:99:87:f4:16:8b:85:98:d9:29:9f:
         72:74:29:5e:31:a1:ad:be:94:57:6b:4e:fc:0c:41:96:f9:56:
         19:a6:c0:86:d1:22:b9:c1:d3:f6:66:e7:e2:29:5a:fc:63:47:
         95:8f:f3:eb:09:44:f6:30:08:25:54:c4:41:98:9e:91:45:cf:
         af:2c:93:51:95:f9:00:8b:8e:d9:ce:7c:69:3e:2d:94:b7:45:
         b8:f2:cb:53:dc:47:46:c3:8c:a7:7b:84:0a:fd:59:79:4d:41:
         1f:d5:2d:74:43:b7:b1:5c:58:c1:e8:a6:62:d5:43:25:ae:f1:
         14:fb:45:fb:7e:ed:aa:00:d0:b2:40:73:1c:17:b1:39:bd:a6:
         80:26:9b:4d:5f:d8:30:1d:ad:9c:e1:26:bf:13:fc:c6:ad:69:
         74:87:ab:46
-----BEGIN CERTIFICATE REQUEST-----
MIIC0DCCAbgCAQAwTTEZMBcGA1UEAwwQVmxhZGlzbGF2LCBIZWxlbjELMAkGA1UE
```

```
 [ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_ca

[ req_distinguished_name ]
commonName = Common Name (eg, YOUR name)
countryName = Country Name (2 letter code)
countryName_min = 2
countryName_max = 2
countryName_default = RU
localityName = Locality Name (eg, city)
organizationName = Organization Name(eg, org)
commonName_max = 64

[ v3_req ]
keyUsage = digitalSignature
extendedKeyUsage = clientAuth
basicConstraints = CA:FALSE

[ v3_ca ]
keyUsage=digitalSignature
```

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), подготовив конфиг таким образом, чтобы openssl x509 -in client.crt -text выдавал расшифровку:

```
~/Documents/lab3 openssl x509 -req -extfile client.conf -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
 client.crt -extensions v3_req -days 90
Signature ok
subject=CN = "Vladislav, Helen", C = RU, L = Novosibirsk, O = NSTU
Getting CA Private Key
Enter pass phrase for ca.key:
~/Documents/lab3
```

```
~/Documents/lab3 openssl x509 -in client.crt -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:96:36:95:98:fc:b1:51:9a:14:2b:38:2f:8c:2b:a3:f6:a0:9b:c8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = RU, L = Novosibirsk, O = NSTU, CN = "Vladislav, Helen"
        Validity
            Not Before: Dec  9 12:38:13 2021 GMT
            Not After : Mar  9 12:38:13 2022 GMT
        Subject: CN = "Vladislav, Helen", C = RU, L = Novosibirsk, O = NSTU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bf:21:eb:ff:1e:a2:4f:31:d7:fa:22:0d:72:a0:
                    82:0e:e4:18:72:79:39:b4:f8:ef:21:47:11:a5:1f:
```

```
                fc:42:9c:4d:6d:fd:a7:a2:4e:33:d6:79:97:00:2e:
                a1:9d
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Basic Constraints:
                CA:FALSE
    Signature Algorithm: sha256WithRSAEncryption
         8c:dd:db:86:28:95:15:a1:90:af:83:8c:48:79:9b:b2:bd:3e:
         e3:6f:95:3c:62:c3:cb:fd:19:9e:34:9a:91:e6:5e:f9:18:83:
         55:ca:6e:ff:fb:e8:16:e4:84:6c:b7:8d:dc:1f:c8:b9:e8:b5:
         43:4f:e6:05:6f:1a:df:cd:ae:fe:bf:b1:bd:8c:f2:9d:67:35:
         22:7d:fe:83:a2:39:5e:32:cf:65:74:d1:48:5d:a4:87:55:be:
         db:5d:1a:34:91:a8:45:1f:b7:8d:64:8b:26:e8:28:a9:6b:ca:
         cc:df:b7:19:f4:31:60:1d:14:7e:58:19:4f:38:95:43:e0:1a:
         4e:36:06:99:39:9b:9d:5e:bc:d7:28:25:c4:31:9c:6f:3e:07:
         41:12:ca:4c:96:51:0f:7c:b0:a9:b5:dd:ed:34:a7:ba:7b:fc:
         30:2d:9e:6b:f1:6f:65:f9:d7:a5:30:9a:85:7e:13:6a:9d:25:
         42:00:b4:34:27:ec:9a:2a:02:7d:45:f3:fb:da:7b:dc:d6:d4:
         5f:75:c4:fd:ea:a4:37:d0:03:ff:dd:24:23:cd:f4:50:90:24:
         5d:c0:4c:13:dd:96:9a:0b:33:94:5a:84:3c:f3:dc:64:c6:68:
         45:c2:97:61:3e:c3:c3:4a:fc:52:85:2c:0d:51:5a:a3:54:1a:
         87:77:a0:2a
-----BEGIN CERTIFICATE-----
MIIDVzCCAj+gAwIBAgIUFZY2lZj8sVGaFCs4L4wro/agm8gwDQYJKoZIhvcNAQEL
```

4. Подписать сертификат у преподавателя
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.

```
~/Documents/lab3 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
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Request CERT (13):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Certificate (11):
* 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
* Using Stream ID: 1 (easy handle 0x558a6efcc9d0)
> POST /api/csr HTTP/2
> Host: istupakov.ddns.net:4559
> user-agent: curl/7.80.0
> accept: */*
> content-length: 1256
> content-type: multipart/form-data; boundary=------------------------c2915147a89bd910
>
* We are completely uploaded and fine
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
< HTTP/2 202
< content-type: application/json; charset=utf-8
< date: Thu, 09 Dec 2021 12:52:36 GMT
< server: Kestrel
< location: https://istupakov.ddns.net:4559/api/csr/cfa0d917-bf12-4c43-a723-0c8039a4928e
< strict-transport-security: max-age=2592000
<
* Connection #0 to host istupakov.ddns.net left intact
{"id":"cfa0d917-bf12-4c43-a723-0c8039a4928e","subject":"CN = \"Vladislav, Helen\", C = RU, L = Novosibirsk, O = NSTU","
timestamp":"2021-12-09T12:52:36.5843512Z"}%
~/Documents/lab3
```

Ссылка сертификата: https://istupakov.ddns.net:4559/api/csr/cfa0d917-bf12-4c43-a723-0c8039a4928e

Сертификат расположен в answer.crt

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

MIIDdTCCAl2gAwIBAgIUBoZ9I819dZcm7ANlNxhthA4pg0UwDQYJKoZIhvcNAQEL

BQAwazELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEVMBMGA1UE

AwwMQ3J5cHRvTGFiIENBMB4XDTIxMTIxMDA2NDQxNVoXDTIyMTIxMDA2NDQxNVow

TTEZMBcGA1UEAwwQVmxhZGlzbGF2LCBIZWxlbjELMAkGA1UEBhMCUlUxFDASBgNV

BAcMC05vdm9zaWJpcnNrMQ0wCwYDVQQKDAROU1RVMIIBIjANBgkqhkiG9w0BAQEF

AAOCAQ8AMIIBCgKCAQEAvyHr/x6iTzHX+iINcqCCDuQYcnk5tPjvIUcRpR+l3fSU

VhsSiexaSJ/7MSx5w5qVPby6n4m5dUTrqt5lPuj5X86IhltXmYk0auxprr9t57U3

yEFUbZ56k/C0YwFQ0fa9vwb7bGnuP5GyX4ohGqtNQpFrqTxI0XYSJ3PXSe3HmyNG

HQjXCf6ye0qVu1u2GdqDHtVSQDFqjd5YtkKLxhwYa9dfnvtSnMzm9hilfiSfUjT1

dIxNDytMzv1R9KvCdlUMUT++L0TF2V7TrTLe+wnMiDdYhnGXAHOq12ofJrXRzWjK

b8X/OZ5oVlbxvUfDVb38QpxNbf2nok4z1nmXAC6hnQIDAQABoy8wLTAJBgNVHRME

AjAAMAsGA1UdDwQEAwIHgDATBgNVHSUEDDAKBggrBgEFBQcDAjANBgkqhkiG9w0B

AQsFAAOCAQEAAnBGDst+HVUHy2eBLJ/h4hxAYIAzrVMglxOilBQXwd5yfsymXqE3

d8apjwHH6okOpjc1DES8j9vfxnCsnQkskVHK4AEa2J+ZDUparu/eYw+0ZVdKNtt+

1utwTWX4G2Vp5GZtpAbmAXb9Foi5YFyTI/PaFiQCridogoaMj/qd48D6FIQ3utYA

QRA66wG4FcuYOVXtRkdeHqkdOPVwuRnBxcpHEX0FixQQDQWwtmL0wm2NguB7+Z9R

llLlRHGyH7c7+U8Q4zua23Smj/G++F8kB7q5Sz+5TxEvThA+IFT3zs7YveBAsuTO

tDJTP6pJkUKfDB5mASari+Qaw61Q1jguQQ==

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

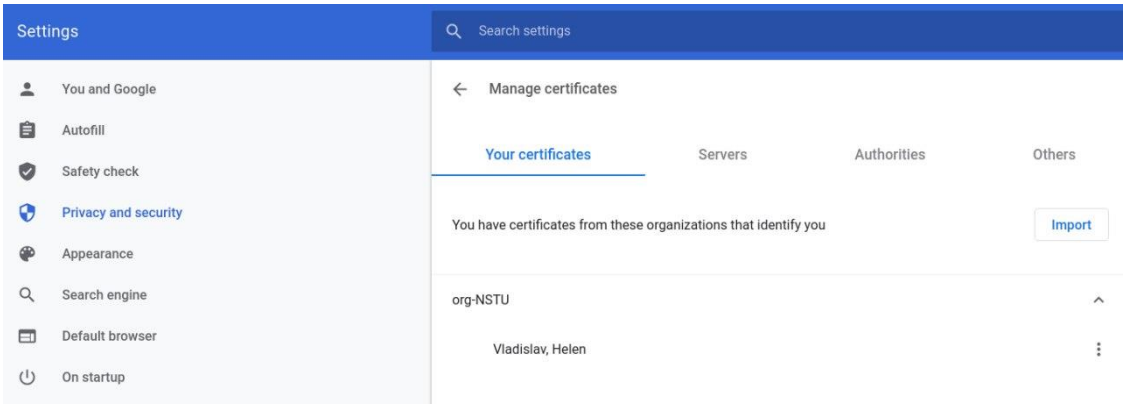
Send message “Hello World” to chat:

```
~/Documents/lab3 curl https://istupakov.ddns.net:4559/api/chat/message -d "\"Wello Horld\"" -H 'Content-Type:
 application/json' --cacert cryptolab-ca.crt -E answer.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
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Request CERT (13):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Certificate (11):
* TLSv1.3 (OUT), TLS handshake, CERT verify (15):
* 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
```

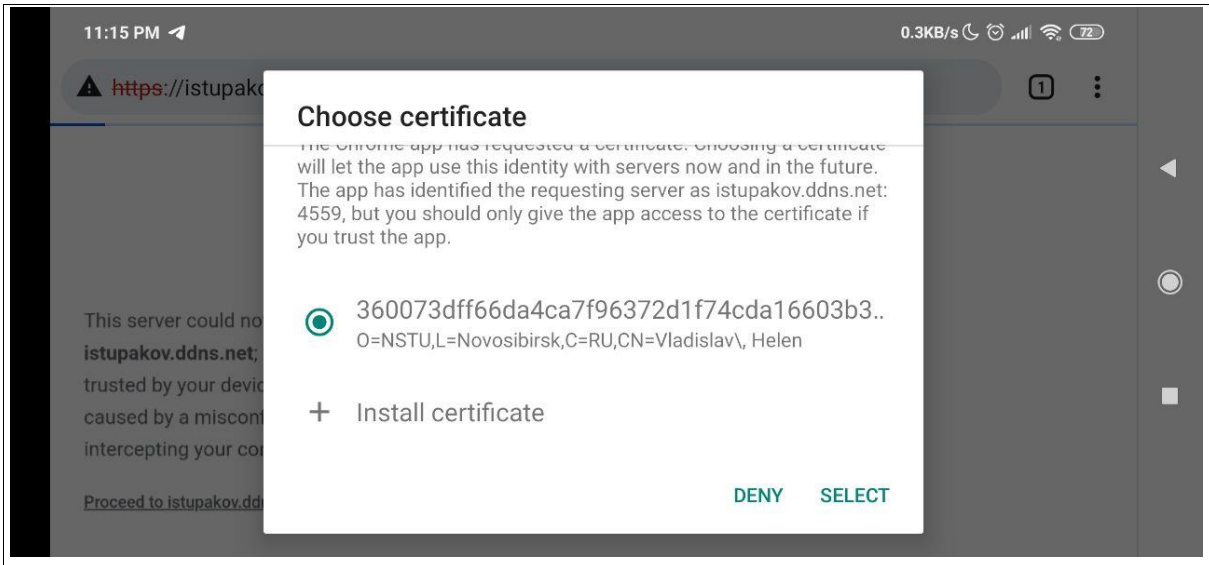
```
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x5643b3ef39d0)
> POST /api/chat/message HTTP/2
> Host: istupakov.ddns.net:4559
> user-agent: curl/7.80.0
> accept: */*
> content-type: application/json
> content-length: 13
>
* We are completely uploaded and fine
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
< HTTP/2 201
< content-type: application/json; charset=utf-8
< date: Tue, 14 Dec 2021 15:32:09 GMT
< server: Kestrel
< location: https://istupakov.ddns.net:4559/chat/message/e182fe93-c653-403a-b8bf-2f28736071ae
< strict-transport-security: max-age=2592000
<
* Connection #0 to host istupakov.ddns.net left intact
{"message":"Wello Horld","user":"O=NSTU, L=Novosibirsk, C=RU, CN=\"Vladislav, Helen\"","timestamp":"2021-12-14T1
5:32:10.1650588Z","id":"e182fe93-c653-403a-b8bf-2f28736071ae"}%
```

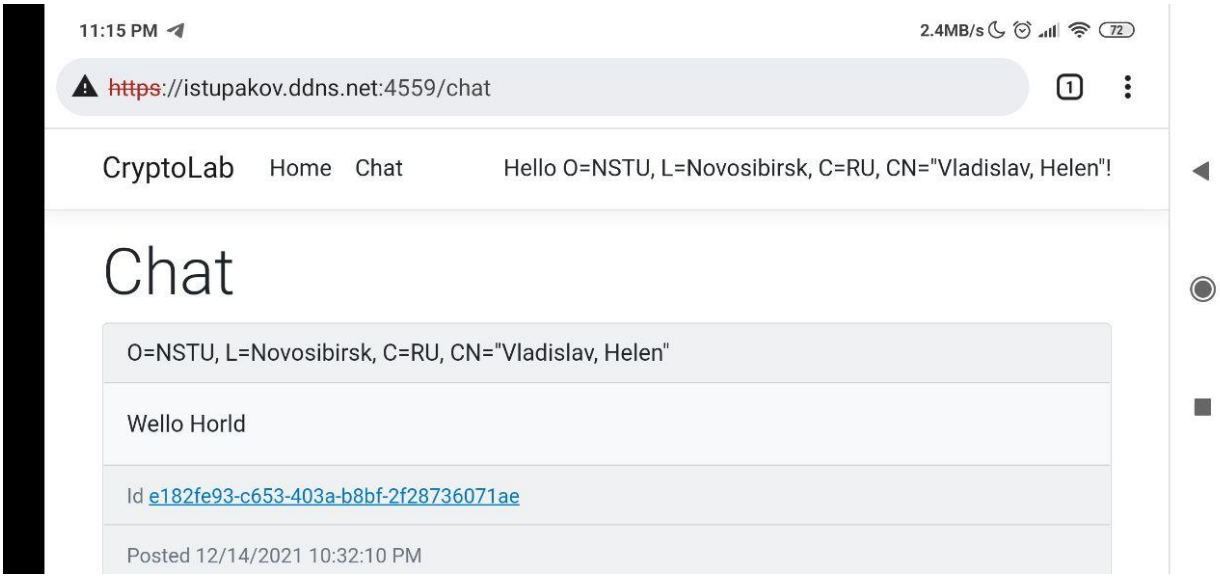
```
~/Documents/lab3 openssl pkcs12 -export -in answer.crt -inkey client.key -out exportKey.p12 -CAfile cryptolab
-ca.crt
Enter pass phrase for client.key:
Enter Export Password:
Verifying - Enter Export Password:
~/Documents/lab3 ls
answer.crt  ca.crt  ca.srl       client.crt  client.key       exportKey.p12
ca.conf     ca.key  client.conf  client.csr  cryptolab-ca.crt
~/Documents/lab3
```

Доступ из браузера:



С телефона:


11:15 PM
0.3KB/s
https://istupako
Choose certificate
will let the app use this identity with servers now and in the future.
The app has identified the requesting server as istupakov.ddns.net:
4559, but you should only give the app access to the certificate if
you trust the app.
360073dff66da4ca7f96372d1f74cda16603b3..
O=NSTU,L=Novosibirsk,C=RU,CN=Vladislav\, Helen
Install certificate
DENY
SELECT
This server could no
istupakov.ddns.net;
trusted by your devic
caused by a miscon
intercepting your co
Proceed to istupakov.dd


11:15 PM
2.4MB/s
https://istupakov.ddns.net:4559/chat
CryptoLab
Home
Chat
Hello O=NSTU, L=Novosibirsk, C=RU, CN="Vladislav, Helen"!
Chat
O=NSTU, L=Novosibirsk, C=RU, CN="Vladislav, Helen"
Wello Horld
Id e182fe93-c653-403a-b8bf-2f28736071ae
Posted 12/14/2021 10:32:10 PM