|  |  |  |
| --- | --- | --- |
|  | | |
| Федеральное государственное бюджетное  образовательное учреждение высшего образования «Новосибирский государственный технический университет» | | |
|  | | |
| Кафедра прикладной математики | | |
| Практическое задание № 3 | | |
| по дисциплине «Основы криптографии» | | |
| **Создание криптографический сертификатов при помощи Open SSL** | | |
|  | | |
|  |  |  |
| Группа ПМ-01 | будник светлана |
|  | самсонов семён |
|  |  |
|  |  |
| Преподаватель | Ступаков илья михайлович |
|  |  |
|  |  |
| Новосибирск, 2022 | | |

# Цель работы

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

# Задание

**Часть 1.** Работа с OpenSSL

1. Создать корневой сертификат с помощью OpenSSL (openssl req -new -config ca.conf -x509 -out ca.crt -keyout=ca.key), подготовив конфиг:

Текст конфигурационного файла ca.conf:

[ req ]

prompt = no ## для того, чтобы брать значения сразу с полей конфиг-файла

distinguished\_name = req\_distinguished\_name

x509\_extensions = v3

[ req\_distinguished\_name ]

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

commonName = Master Sertificate

[ v3 ]

keyUsage = critical,Certificate Sign

basicConstraints = critical,CA:TRUE,pathlen:1

Вызов команды для создания корневого сертификата с приватным ключом:

(в качестве PEM pass phrase использовалась фраза hello)

**> openssl req -new -config ca.conf -x509 -out ca.crt -keyout ca.key //создание сертификата**

Generating a RSA private key

.................................................................................................................+++++

...+++++

writing new private key to 'ca.key'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

-----

Результат вызова команды:

**> Get-ChildItem**

Directory: C:\Semen\work\Учёба\Для НГТУ\3 курс\5 семестр\Криптография\3

лаба\1 часть

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a--- 30.10.2022 20:30 981 1.1.txt

-a--- 30.10.2022 20:27 446 ca.conf

-a--- 30.10.2022 20:27 1306 ca.crt

-a--- 30.10.2022 20:27 1854 ca.key

**> openssl x509 -in ca.crt -text -noout //расшифровка сертификата**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

6c:1c:d3:5c:04:03:d8:f7:9b:ad:25:04:c2:f6:26:92:86:6f:f6:f5

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Master Sertificate

Validity

Not Before: Oct 30 13:27:42 2022 GMT

Not After : Nov 29 13:27:42 2022 GMT

Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Master Sertificate

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:b0:13:d2:9d:05:d8:77:a0:d0:43:5d:59:a9:ef:

39:45:00:95:fe:37:bf:47:04:ed:22:6b:93:97:08:

44:4f:42:00:0b:b8:a5:54:fd:10:5e:a1:86:02:ea:

5a:5b:5a:52:47:b0:ee:01:a5:b0:65:fc:6f:af:0e:

a9:ab:88:79:b3:20:19:04:aa:37:c4:65:54:42:24:

c4:2a:93:4b:9b:58:bf:f1:0d:a5:02:06:e8:c4:aa:

2e:38:94:8d:77:d8:9c:25:b7:a5:99:0f:ae:70:8f:

e1:16:d1:7a:74:fb:e9:ed:9d:22:32:fc:03:ea:ba:

01:30:27:7b:a7:1e:cf:9d:18:f2:60:a5:01:8f:73:

8f:b9:ba:48:5c:a9:a2:ab:1e:62:bd:3f:82:f4:ef:

4e:88:f6:4e:4e:7d:0d:47:d1:68:76:1e:36:78:2a:

91:75:d2:85:b3:5e:4d:80:93:fc:80:a2:05:5f:93:

ee:d9:14:f2:42:42:b3:10:ad:7a:5e:18:4d:60:51:

ac:5e:61:ff:4a:6f:26:d1:51:7a:33:6d:04:f8:e7:

c0:cb:9d:a4:41:06:22:42:84:84:f3:c6:f0:55:34:

fd:d7:6d:ce:8d:1b:65:b9:2a:22:97:aa:58:c0:4c:

c3:4c:af:91:28:e3:f7:aa:13:8a:f3:08:48:0b:52:

b0:e1

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Certificate Sign

X509v3 Basic Constraints: critical

CA:TRUE, pathlen:1

Signature Algorithm: sha256WithRSAEncryption

24:dd:20:51:c1:c9:b2:13:a2:ed:e1:eb:58:d7:54:45:29:b2:

ff:4b:81:26:53:b8:3f:2d:00:af:29:17:e0:5f:ce:08:92:31:

6b:a7:29:f7:f6:f1:76:ea:66:f7:45:5a:a1:52:da:78:7b:a3:

0b:63:1a:84:5a:1f:ed:ab:76:fa:6b:7d:bf:89:8c:d2:bc:89:

cb:7a:42:bc:a0:55:65:2c:4b:81:71:62:76:32:d1:39:78:b0:

84:64:77:c4:9f:82:b5:00:1a:56:ee:00:28:23:7f:71:ab:71:

51:74:02:55:e0:83:f9:f3:02:8b:87:5a:04:25:a9:3a:98:73:

7d:4e:84:ae:e3:b2:50:a1:40:c6:bb:5b:70:d8:96:7f:18:53:

6a:56:0b:7a:43:92:6b:2d:7a:c0:a3:8c:48:ee:6e:41:21:72:

3d:73:f4:bf:97:60:02:ff:5e:52:99:06:f4:8e:47:e5:74:00:

6f:4c:30:de:5b:c5:70:e0:86:9d:11:74:80:0d:f7:18:35:62:

49:71:c6:91:51:d3:5e:13:00:8b:a7:23:ae:19:cd:2f:8b:51:

de:58:e6:b2:da:5a:0a:a6:a2:a4:89:4a:96:c9:c8:63:cb:9a:

3a:be:7f:18:b6:17:33:2a:9b:f8:16:a2:ef:a8:7b:33:74:32:

e1:1f:e6:39

1. 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:

Текст конфигурационного файла client.conf:

[ req ]

prompt = no

distinguished\_name = req\_distinguished\_name

x509\_extensions = x509\_ext # расширения для формата x509v3

req\_extensions = req\_ext # расширения для запроса на подпись

[ req\_distinguished\_name ]

commonName = Budnik Svetlana, Samsonov Semyon

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

[ req\_ext ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:FALSE

[ x509\_ext ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:FALSE

Вызов команды для создания запроса клиентского сертификата с приватным ключом:

(в качестве PEM pass phrase использовалась фраза hello)

> openssl req -new -config .\client.conf -out client.csr -keyout client.key

Generating a RSA private key

...............+++++

............+++++

writing new private key to 'client.key'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

-----

Результат вызова команды:

> Get-ChildItem

Directory: C:\Semen\work\Учёба\Для НГТУ\3 курс\5 семестр\Криптография\3

лаба\1 часть

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a--- 30.10.2022 21:35 5176 1.1.txt

-a--- 30.10.2022 21:36 5207 1.2.txt

-a--- 30.10.2022 21:06 554 ca.conf

-a--- 30.10.2022 20:27 1306 ca.crt

-a--- 30.10.2022 20:27 1854 ca.key

-a--- 30.10.2022 21:34 637 client.conf

-a--- 30.10.2022 21:31 1119 client.csr

-a--- 30.10.2022 21:31 1854 client.key

**> openssl req -in .\client.csr -text -noout //вывод запроса документа**

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = "Budnik Svetlana, Samsonov Semyon", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:bd:79:4c:fd:42:76:1d:52:a1:2e:1a:e2:df:cd:

45:64:5b:08:da:a3:71:25:d8:a3:52:6d:af:76:4c:

65:05:ba:42:56:01:03:81:fe:77:d5:51:3d:5c:43:

34:76:bf:84:f3:af:13:60:4b:47:8b:c1:c6:f9:4c:

9d:e4:56:ed:f2:65:a3:ad:93:d9:76:e5:af:61:ed:

69:9d:b7:ed:de:b1:21:37:f5:cb:c2:f5:7e:4d:2a:

bc:73:45:29:d6:c8:71:64:43:ec:ab:56:37:7f:85:

ef:03:fa:92:f8:f4:b4:27:8b:a8:19:d3:6d:f0:d2:

22:a2:bd:a3:a0:dd:78:d5:a5:50:c5:5a:8a:c1:79:

31:f1:51:e3:56:90:f1:30:13:74:25:8e:00:96:13:

cd:32:f1:b6:56:00:b8:b5:b8:1f:2a:26:82:59:c5:

a5:74:7c:3f:75:cb:d0:33:43:ed:43:b7:5b:a4:14:

82:fc:ed:4a:5f:49:60:18:1f:91:ed:33:44:c6:b2:

ad:61:ac:f9:1f:8a:4b:5c:5c:b8:d9:35:84:bd:a9:

82:62:66:0e:bc:7e:58:73:fb:0f:cb:26:40:46:ca:

62:56:3b:69:78:6a:62:5f:66:c0:cf:6a:a2:2a:69:

f6:a3:66:dd:22:73:e6:ce:23:7d:b6:00:12:82:73:

94:97

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

ad:07:1d:d7:b1:c9:8f:be:9b:21:86:1f:36:4e:18:1d:1c:20:

a2:aa:de:7c:c8:16:87:94:d4:db:2a:7a:ee:56:3f:34:57:f0:

8a:19:01:3c:00:0e:54:82:09:5a:2a:1b:e0:28:d8:97:ff:62:

fd:6f:47:2c:8a:1f:88:f0:27:8c:4f:da:3f:ee:d9:c9:fe:90:

e8:a1:33:e7:2d:aa:91:bd:50:62:42:11:eb:a3:a7:52:8d:8d:

ea:4c:62:93:c2:14:76:90:24:a5:2d:92:b1:1c:f5:b5:da:d3:

98:0b:bc:9c:1b:7f:92:c9:40:aa:a6:da:24:6b:35:2a:d8:d0:

6e:f5:89:e3:ee:ea:e8:fa:02:c6:49:3c:66:58:dd:0b:3a:d0:

33:74:f9:d7:14:83:33:4d:21:91:f3:79:b4:82:2f:8b:44:b9:

47:52:4d:03:99:e2:39:0c:c3:ba:29:7a:c5:db:99:da:df:7a:

80:b3:9d:7b:b9:9f:2c:a4:a6:06:66:9a:7d:8a:a5:c1:90:ce:

eb:e2:ac:e5:47:39:7b:e0:e2:0b:e5:fd:ff:de:17:76:ff:71:

6a:9b:c9:7a:68:f3:4f:a9:71:cb:89:46:6d:ec:03:52:0b:70:

a4:a8:3d:2d:82:84:03:e7:4b:1f:f9:41:1b:d4:34:df:58:aa:

ab:bd:b8:ca

1. 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:

Текст конфигурационного файла client.conf:

[ req ]

prompt = no

distinguished\_name = req\_distinguished\_name

x509\_extensions = x509\_ext # расширения для формата x509v3

req\_extensions = req\_ext # расширения для запроса на подпись

[ req\_distinguished\_name ]

commonName = Budnik Svetlana, Samsonov Semyon

countryName = RU

localityName = Novosibirsk

organizationName = Novosibirsk State Technical University

[ req\_ext ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:FALSE

[ x509\_ext ]

keyUsage = digitalSignature

extendedKeyUsage = clientAuth

basicConstraints = CA:FALSE

Вызов команды для подписи запроса клиента корневым ключом:

(в качестве pass phrase использовалась фраза hello)

**openssl x509 -req -extfile client.conf -extensions x509\_ext -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out client.crt**

Signature ok

subject=CN = "Budnik Svetlana, Samsonov Semyon", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Getting CA Private Key

Enter pass phrase for ca.key:

Результат вызова команды:

> Get-ChildItem

Directory: C:\Semen\work\Учёба\Для НГТУ\3 курс\5 семестр\Криптография\3

лаба\1 часть

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a--- 30.10.2022 21:35 5176 1.1.txt

-a--- 31.10.2022 0:23 5408 1.2.txt

-a--- 31.10.2022 0:24 5418 1.3.txt

-a--- 30.10.2022 21:06 554 ca.conf

-a--- 30.10.2022 20:27 1306 ca.crt

-a--- 30.10.2022 20:27 1854 ca.key

-a--- 31.10.2022 0:21 775 client.conf

-a--- 31.10.2022 0:22 1334 client.crt

-a--- 31.10.2022 0:11 1119 client.csr

-a--- 31.10.2022 0:11 1854 client.key

**> openssl x509 -in client.crt -text -noout //вывод сертификата**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

5e:68:1c:28:6d:f1:c0:66:17:e6:4f:e8:8a:90:3a:85:87:88:e7:88

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = Master Sertificate

Validity

Not Before: Oct 30 17:22:05 2022 GMT

Not After : Nov 29 17:22:05 2022 GMT

Subject: CN = "Budnik Svetlana, Samsonov Semyon", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:cb:68:53:98:e0:bc:3b:6a:d7:a8:9a:da:e4:e8:

41:3b:e7:7a:44:e5:c9:e9:23:8a:86:e1:97:e5:64:

f0:b5:66:f1:ea:29:37:c9:93:5a:c7:78:4b:17:1a:

60:d8:83:dc:64:ee:af:6d:4a:8d:10:23:13:d6:23:

90:02:16:eb:25:4b:39:d2:f4:52:7d:80:b4:37:06:

a7:dc:67:89:10:a1:00:1c:e4:2c:37:31:d4:0a:3f:

6d:07:7d:94:b9:ee:00:ab:14:56:ab:c4:73:37:e7:

65:7f:99:67:2f:f8:f0:73:10:5c:0d:54:d0:9b:e0:

ce:b9:26:bc:f3:c0:b6:ad:80:53:c3:94:50:36:f7:

d4:28:1a:a7:e0:fe:18:ca:4c:6a:33:97:00:8a:bf:

94:e2:2a:f2:74:b6:80:8c:a5:10:8e:65:14:4e:a4:

fe:b6:b6:25:03:bb:7a:65:87:7c:59:db:4e:9f:5d:

e4:29:44:35:a5:9f:5f:a0:2e:d6:3d:f0:ee:dc:ea:

cc:d7:fe:cb:bf:f9:77:b6:0e:60:9a:73:86:0b:a6:

c0:45:4c:e1:2c:d4:9c:1d:23:03:5b:6b:a5:1c:20:

85:d9:4e:bb:62:c5:a0:22:e1:0d:4e:d2:39:0b:4e:

36:02:e8:40:db:e5:d0:e3:65:65:a3:2f:51:5e:5c:

d6:f7

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

a4:aa:be:26:e1:95:ad:d6:84:01:d9:1a:16:e8:1c:4d:14:ac:

15:d0:55:b0:76:34:b6:e1:a4:ff:6f:bb:f1:67:98:42:d9:88:

ea:6e:2f:c4:c5:20:77:4c:d3:03:cb:dd:f4:42:39:74:01:3c:

a7:8b:8c:a7:8e:31:aa:29:a1:ca:88:20:87:ad:c2:03:45:51:

4a:85:ae:f4:94:eb:e5:61:31:90:2b:87:3b:c6:55:20:c2:83:

f2:45:05:9f:82:53:93:ff:af:23:ef:39:60:ff:c8:66:fc:4f:

49:f5:ff:3d:86:6b:3e:56:15:a9:78:25:5c:1a:25:14:d3:2d:

fc:56:62:03:c4:a2:95:b4:18:33:01:d7:c8:f3:bb:a0:e1:37:

68:db:09:89:a4:67:46:77:c6:a1:50:d9:ea:c7:e8:59:d5:e2:

18:db:cd:75:76:4d:83:3e:ea:c9:94:2a:51:6c:e8:23:df:4d:

9c:f2:0d:b9:53:ed:fd:68:3e:5b:ba:df:96:83:b9:a0:98:3e:

7b:85:41:9b:83:d7:a5:98:07:46:24:15:07:08:8a:35:9c:9f:

99:ff:ec:12:2a:d0:be:11:ef:c2:ed:39:4a:c0:63:2a:dc:33:

c1:7d:95:d1:fb:1e:8b:c6:d6:7b:af:9a:65:ed:66:2a:ba:71:

0d:42:12:cd

**Часть 2.** Подписать сертификат у преподавателя

1. Загрузить файл запроса сертификата методом POST на адрес https://istupakov.ddns.net:4203/api/csr. Запомнить полученный в ответ в Location Header адрес для скачивания сертификата.

Запрос можно сделать с помощью утилиты Curl:

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

Файл cryptolab-ca.crt:

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

MIIDnjCCAoagAwIBAgIULYKD9cyU791JU+gx3wNqkGLC9pEwDQYJKoZIhvcNAQEL

BQAwdTELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEfMB0GA1UE

AwwWQ3J5cHRvTGFiIDIwMjIgUm9vdCBDQTAeFw0yMjEwMjAxNDUzNTRaFw0yMzEw

MjAxNDUzNTRaMHUxCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2liaXJzazEv

MC0GA1UECgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZlcnNpdHkx

HzAdBgNVBAMMFkNyeXB0b0xhYiAyMDIyIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEB

AQUAA4IBDwAwggEKAoIBAQCwiP2x1wyiOrQhwKzNW7r7TcgdM9blX6dIfzbM9HTt

nQBGHNp89EZLE0RF9h5vz/qql1MRp9EmoYdmLBRE5M+A2kPF47sH/INSBhacFaCx

A/cwmTDNex6FZGPxsDPu7EEISZ5RRpIiW/PjsyZkfiNyIJdHL3XiRcdwkBKtbQ1d

H0AJjWCr+TJ8kVSOnWsc/8OnjYQiDWjBcZev9uyGd18AbPUmElct9rXqvJ2P8YCN

sJxq0qbxw9l0UT/1Fr7QfBMpLXxJt2xOc1m9hiJNdM6gQwKGEZSI64u7kHGCEpz9

Y6XswSpo/ZSEQioTw13uPw2E6NSO2u+aViUz9kP1r6y1AgMBAAGjJjAkMA4GA1Ud

DwEB/wQEAwICBDASBgNVHRMBAf8ECDAGAQH/AgEBMA0GCSqGSIb3DQEBCwUAA4IB

AQCrf3tvgcSc4pwrP0Plc6Z+1Ij265+SoAKygMSw95J+Wd3BcCA857EALuJ1hay9

95p/bQBnOUr7CMr3SMssz7EgwtWYCZ43pyb+m5mcJG+prH5IPPDlsDvG5G9HLjlv

XQ0PVasYXBq9Ta2wu7UpTlYqJbei6s4ik8brkY4MhnoO0PYXIA1qxelOoLf+3liR

oShTB70epto976cePabvLVEDkN+8gB7uGAOj+GeA1EbNZhGvhNrWURCfmnhY7a/H

xsEBVbWB4QVnZiSeKXzXYjTD6SolNY6DZeYx0UwrUdEg9LTG0ZChrRJ9nERJ6FJK

nyA+yo0mP2CN1LBcvyuyWIvL

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

1. Скачать подписанный сертификат, вставить в отчет его адрес и расшифровку.

Результат работы команды:

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

\* Trying 217.71.129.139:4203...

\* TCP\_NODELAY set

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

\* ALPN, offering h2

\* ALPN, offering http/1.1

\* successfully set certificate verify locations:

\* CAfile: ./cryptolab-ca.crt

CApath: /etc/ssl/certs

\* 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 2022 Server

\* start date: Oct 20 14:56:34 2022 GMT

\* expire date: Oct 20 14:56:34 2023 GMT

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

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab 2022 Root CA

\* SSL certificate verify ok.

\* Using HTTP2, server supports multi-use

\* 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 0x557332b077c0)

> POST /api/csr HTTP/2

> Host: istupakov.ddns.net:4203

> user-agent: curl/7.68.0

> accept: \*/\*

> content-length: 1321

> content-type: multipart/form-data; boundary=------------------------51a2a5ef8f1b6597

>

\* 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

\* Connection state changed (MAX\_CONCURRENT\_STREAMS == 100)!

< HTTP/2 202

< content-type: application/json; charset=utf-8

< date: Wed, 16 Nov 2022 08:59:05 GMT

< server: Kestrel

< location: https://istupakov.ddns.net:4203/api/csr/8f7d574f-09c5-4f0a-a512-7fcc3803317a

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

<

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

{"id":"8f7d574f-09c5-4f0a-a512-7fcc3803317a","subject":"CN = \"Budnik Svetlana, Samsonov Semyon\", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University","timestamp":"2022-11-16T08:59:05.9746371Z"}

Подписанный сертификат:

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

MIIDsTCCApmgAwIBAgIUFofvYtS9wARu9cFljwaepVjlf/QwDQYJKoZIhvcNAQEL

BQAwdTELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05vdm9zaWJpcnNrMS8wLQYDVQQK

DCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwgVW5pdmVyc2l0eTEfMB0GA1UE

AwwWQ3J5cHRvTGFiIDIwMjIgUm9vdCBDQTAeFw0yMjExMTYwOTE1MTVaFw0yMzEx

MTYwOTE1MTVaMH8xKTAnBgNVBAMMIEJ1ZG5payBTdmV0bGFuYSwgU2Ftc29ub3Yg

U2VteW9uMQswCQYDVQQGEwJSVTEUMBIGA1UEBwwLTm92b3NpYmlyc2sxLzAtBgNV

BAoMJk5vdm9zaWJpcnNrIFN0YXRlIFRlY2huaWNhbCBVbml2ZXJzaXR5MIIBIjAN

BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy2hTmOC8O2rXqJra5OhBO+d6ROXJ

6SOKhuGX5WTwtWbx6ik3yZNax3hLFxpg2IPcZO6vbUqNECMT1iOQAhbrJUs50vRS

fYC0Nwan3GeJEKEAHOQsNzHUCj9tB32Uue4AqxRWq8RzN+dlf5lnL/jwcxBcDVTQ

m+DOuSa888C2rYBTw5RQNvfUKBqn4P4YykxqM5cAir+U4irydLaAjKUQjmUUTqT+

trYlA7t6ZYd8WdtOn13kKUQ1pZ9foC7WPfDu3OrM1/7Lv/l3tg5gmnOGC6bARUzh

LNScHSMDW2ulHCCF2U67YsWgIuENTtI5C042AuhA2+XQ42Vloy9RXlzW9wIDAQAB

oy8wLTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIHgDATBgNVHSUEDDAKBggrBgEFBQcD

AjANBgkqhkiG9w0BAQsFAAOCAQEAYs2aGl/Unm5m56q/yZ0TvZzpVm63fXv3Gpt0

3YfTN22KDE/P1jH/FiKuyLlLPKg1FXf27X/TB4BOQRmOY444UAqIzXCKJZXR4PFz

8FWdtQir4et4J3lv17p+W8CWBfvCVcHsWu1zvSD8e7icwUBFh9EsC9u5p6NnE7qL

RlhPU/kO3yeMfL+7EN/zSYiBd/uik6r6U1EcZhM9PBi/O/uvUFewpqzTa0H/hfUc

y1LV4Re086Rel0afKuC48VWmkMjneJfK0jj0/zAN2PuHoVYNforiGYrnAfdhtjHt

pvCENUyC/RX+JN9ql4vSS6hzfW/ZAz0b5YsNAFVGJ9WejrpYIg==

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

Расшифровка подписанного сертификата:

openssl x509 -in client.crt -text -noout

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

16:87:ef:62:d4:bd:c0:04:6e:f5:c1:65:8f:06:9e:a5:58:e5:7f:f4

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = CryptoLab 2022 Root CA

Validity

Not Before: Nov 16 09:15:15 2022 GMT

Not After : Nov 16 09:15:15 2023 GMT

Subject: CN = "Budnik Svetlana, Samsonov Semyon", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:cb:68:53:98:e0:bc:3b:6a:d7:a8:9a:da:e4:e8:

41:3b:e7:7a:44:e5:c9:e9:23:8a:86:e1:97:e5:64:

f0:b5:66:f1:ea:29:37:c9:93:5a:c7:78:4b:17:1a:

60:d8:83:dc:64:ee:af:6d:4a:8d:10:23:13:d6:23:

90:02:16:eb:25:4b:39:d2:f4:52:7d:80:b4:37:06:

a7:dc:67:89:10:a1:00:1c:e4:2c:37:31:d4:0a:3f:

6d:07:7d:94:b9:ee:00:ab:14:56:ab:c4:73:37:e7:

65:7f:99:67:2f:f8:f0:73:10:5c:0d:54:d0:9b:e0:

ce:b9:26:bc:f3:c0:b6:ad:80:53:c3:94:50:36:f7:

d4:28:1a:a7:e0:fe:18:ca:4c:6a:33:97:00:8a:bf:

94:e2:2a:f2:74:b6:80:8c:a5:10:8e:65:14:4e:a4:

fe:b6:b6:25:03:bb:7a:65:87:7c:59:db:4e:9f:5d:

e4:29:44:35:a5:9f:5f:a0:2e:d6:3d:f0:ee:dc:ea:

cc:d7:fe:cb:bf:f9:77:b6:0e:60:9a:73:86:0b:a6:

c0:45:4c:e1:2c:d4:9c:1d:23:03:5b:6b:a5:1c:20:

85:d9:4e:bb:62:c5:a0:22:e1:0d:4e:d2:39:0b:4e:

36:02:e8:40:db:e5:d0:e3:65:65:a3:2f:51:5e:5c:

d6:f7

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

62:cd:9a:1a:5f:d4:9e:6e:66:e7:aa:bf:c9:9d:13:bd:9c:e9:

56:6e:b7:7d:7b:f7:1a:9b:74:dd:87:d3:37:6d:8a:0c:4f:cf:

d6:31:ff:16:22:ae:c8:b9:4b:3c:a8:35:15:77:f6:ed:7f:d3:

07:80:4e:41:19:8e:63:8e:38:50:0a:88:cd:70:8a:25:95:d1:

e0:f1:73:f0:55:9d:b5:08:ab:e1:eb:78:27:79:6f:d7:ba:7e:

5b:c0:96:05:fb:c2:55:c1:ec:5a:ed:73:bd:20:fc:7b:b8:9c:

c1:40:45:87:d1:2c:0b:db:b9:a7:a3:67:13:ba:8b:46:58:4f:

53:f9:0e:df:27:8c:7c:bf:bb:10:df:f3:49:88:81:77:fb:a2:

93:aa:fa:53:51:1c:66:13:3d:3c:18:bf:3b:fb:af:50:57:b0:

a6:ac:d3:6b:41:ff:85:f5:1c:cb:52:d5:e1:17:b4:f3:a4:5e:

97:46:9f:2a:e0:b8:f1:55:a6:90:c8:e7:78:97:ca:d2:38:f4:

ff:30:0d:d8:fb:87:a1:56:0d:7e:8a:e2:19:8a:e7:01:f7:61:

b6:31:ed:a6:f0:84:35:4c:82:fd:15:fe:24:df:6a:97:8b:d2:

4b:a8:73:7d:6f:d9:03:3d:1b:e5:8b:0d:00:55:46:27:d5:9e:

8e:ba:58:22

**Часть 3.** Работа с TLS

1. Отправить от вашей бригады некоторое сообщение в чат. Для этого необходимо отправить POST запрос на адрес https://istupakov.ddns.net:4203/api/chat/message в теле которого, будет строка с сообщением (тело запроса должно быть в формате JSON, запрос можно сделать с помощью утилиты Curl). Для аутентификации в чате необходимо использовать полученные ранее сертификаты.

Отправка сообщения в чат, используя самоподписанный сертификат клиента

Результат работы команды:

curl -H "Content-Type: application/json" --cert client-selfsigned.crt --key client.key --cacert cryptolab-ca.crt --data '{"Prodam garage"}' https://istupakov.ddns.net:4203/api/chat/message -v

\* Trying 217.71.129.139:4203...

\* TCP\_NODELAY set

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

\* ALPN, offering h2

\* ALPN, offering http/1.1

Enter PEM pass phrase:

\* successfully set certificate verify locations:

\* CAfile: cryptolab-ca.crt

CApath: /etc/ssl/certs

\* 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 2022 Server

\* start date: Oct 20 14:56:34 2022 GMT

\* expire date: Oct 20 14:56:34 2023 GMT

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

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab 2022 Root CA

\* SSL certificate verify ok.

\* Using HTTP2, server supports multi-use

\* 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 0x55eaa461c7c0)

> POST /api/chat/message HTTP/2

> Host: istupakov.ddns.net:4203

> user-agent: curl/7.68.0

> accept: \*/\*

> content-type: application/json

> content-length: 17

>

\* 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

\* Empty reply from server

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

**curl: (52) Empty reply from server**

1. Привести результаты запросов с сертификатами из части 1 и из части 2 в отчете, в том числе ссылку на отправленное сообщение (возвращается в Location Header).

Отправка сообщения в чат с подписанным преподавателем сертификатом

Результат работы команды:

curl -H "Content-Type: application/json" --cert client.crt --key client.key --cacert cryptolab-ca.crt --data '"Prodam garage"' https://istupakov.ddns.net:4203/api/chat/message -v

\* Trying 217.71.129.139:4203...

\* TCP\_NODELAY set

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

\* ALPN, offering h2

\* ALPN, offering http/1.1

Enter PEM pass phrase:

\* successfully set certificate verify locations:

\* CAfile: cryptolab-ca.crt

CApath: /etc/ssl/certs

\* 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 2022 Server

\* start date: Oct 20 14:56:34 2022 GMT

\* expire date: Oct 20 14:56:34 2023 GMT

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

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; CN=CryptoLab 2022 Root CA

\* SSL certificate verify ok.

\* Using HTTP2, server supports multi-use

\* 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 0x560f5e7e17c0)

> POST /api/chat/message HTTP/2

> Host: istupakov.ddns.net:4203

> user-agent: curl/7.68.0

> accept: \*/\*

> content-type: application/json

> content-length: 15

>

\* 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

\* Connection state changed (MAX\_CONCURRENT\_STREAMS == 100)!

< HTTP/2 201

< content-type: application/json; charset=utf-8

< date: Wed, 16 Nov 2022 09:38:26 GMT

< server: Kestrel

< location: https://istupakov.ddns.net:4203/chat/message/23f96e34-4924-41bd-8cff-c718a27bef8d

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

<

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

{"message":"Prodam garage","user":"O=Novosibirsk State Technical University, L=Novosibirsk, C=RU, CN=\"Budnik Svetlana, Samsonov Semyon\"","timestamp":"2022-11-16T09:38:27.0536652Z","id":"23f96e34-4924-41bd-8cff-c718a27bef8d"}

1. (дополнительно, +2 балла) Продемонстрировать доступ в чат из браузера на ПК.

Чтобы браузер смог зайти на чат сервер, необходимо сгенерировать сертификат обмена личной информации p12, для этого воспользуемся командой:

> openssl pkcs12 -export -out client.p12 -inkey .\client.key -in .\client.crt -certfile .\cryptolab-ca.crt

Enter pass phrase for .\client.key: [hello]

Enter Export Password: [hello]

Verifying - Enter Export Password: [hello]

> Get-ChildItem

Directory: C:\Semen\work\Учёба\Для НГТУ\3 курс\5 семестр\Криптография\3 лаба\4 часть (доп)

Mode LastWriteTime Length Name

---- ------------- ------ ----

-a--- 16.11.2022 18:38 257 4.1.txt

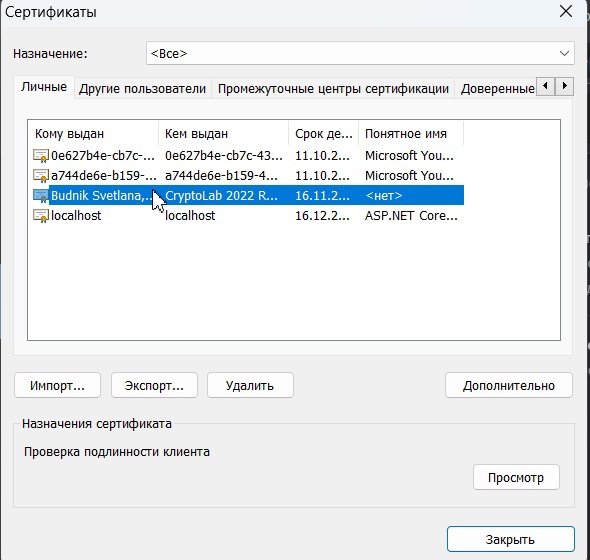
-a--- 16.11.2022 16:17 1362 client.crt

-a--- 31.10.2022 0:11 1854 client.key

-a--- 16.11.2022 18:39 3525 client.p12

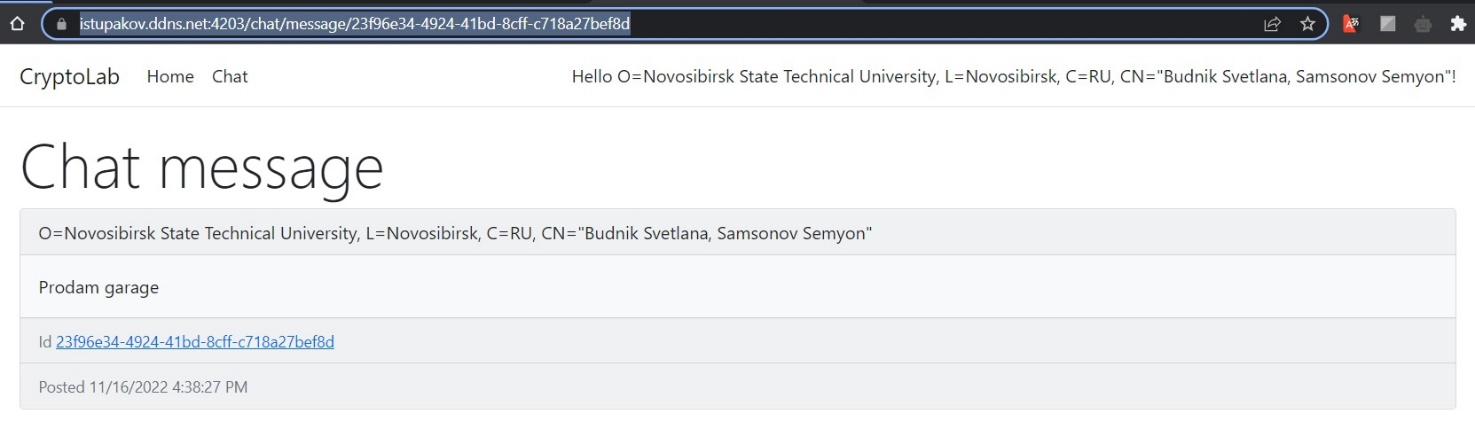
-a--- 16.11.2022 15:54 1314 cryptolab-ca.crt

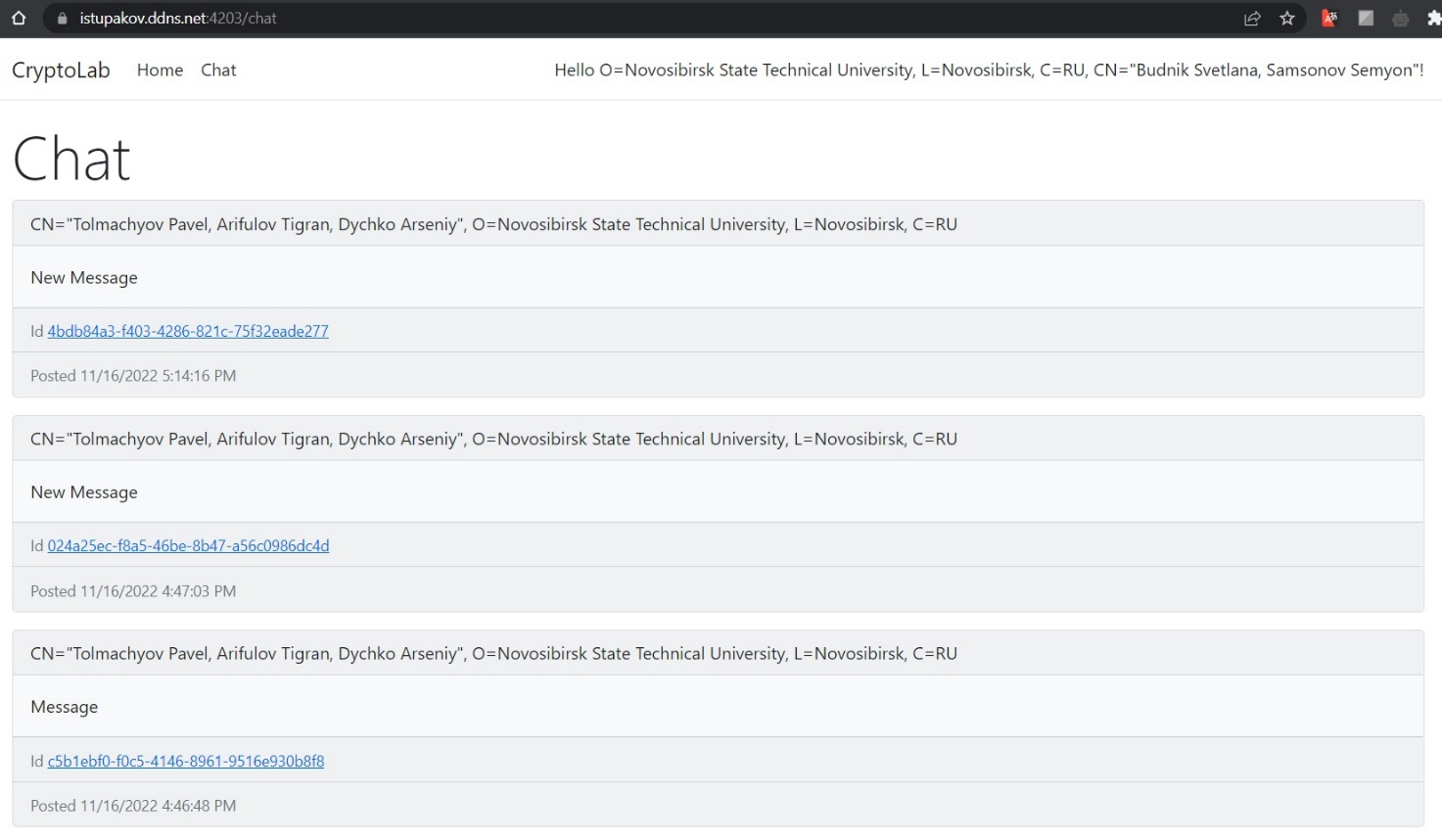
Добавляем данный сертификат в список личных сертификатов



Переходим в браузере по ссылке, выданной нам сервером на наше сообщение в чате: https://istupakov.ddns.net:4203/chat/message/23f96e34-4924-41bd-8cff-c718a27bef8d

В браузере выбираем добавленный нами сертификат, открывается страница с нашим сообщением.





1. (дополнительно, +3 балла) Продемонстрировать доступ в чат из браузера на телефоне.