|  |  |  |
| --- | --- | --- |
|  | | |
| Федеральное государственное бюджетное  образовательное учреждение высшего образования «Новосибирский государственный технический университет» | | |
|  | | |
| Кафедра прикладной математики | | |
| Лабораторная работа № 1 | | |
| по дисциплине «Основы криптографии» | | |
| **Работа с криптографическими сертификатами** | | |
|  | | |
|  | Бригада 6 | Замятин Артём |
| Группа ПМ-25 | выходцев александр |
|  |  |
|  |  |
|  |  |
|  |  |
| Преподаватель | ступаков илья михайлович |
|  |  |
| Новосибирск, 2024 | | |

1. **Цель работы**

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

1. **Ход работы**

**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 таким образом, чтобы openssl x509 -in ca.crt -text выдавал расшифровку вида:**

Certificate:

    Data:

        Version: 3 (0x2)

        Serial Number: ...

    Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <Some name>

        Validity

            Not Before: ...

            Not After : ...

        Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <Some name>

        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                Public-Key: (2048 bit)

                Modulus: ...

                Exponent: ...

        X509v3 extensions:

            X509v3 Key Usage: critical

                Certificate Sign

            X509v3 Basic Constraints: critical

                CA:TRUE, pathlen:1

    Signature Algorithm: sha256WithRSAEncryption  
...

Мы подготовили конфиг на основе которого был создан сертификат, соответствующий заданию.

Текст конфига:

[ req ]

distinguished\_name = Brigada6

default\_bits = 2048

default\_md = sha256

x509\_extensions = v3\_ca

prompt = no

[ Brigada6 ]

C = RU

L = Novosibirsk

O = Novosibirsk State Technical University

CN = Brigada6

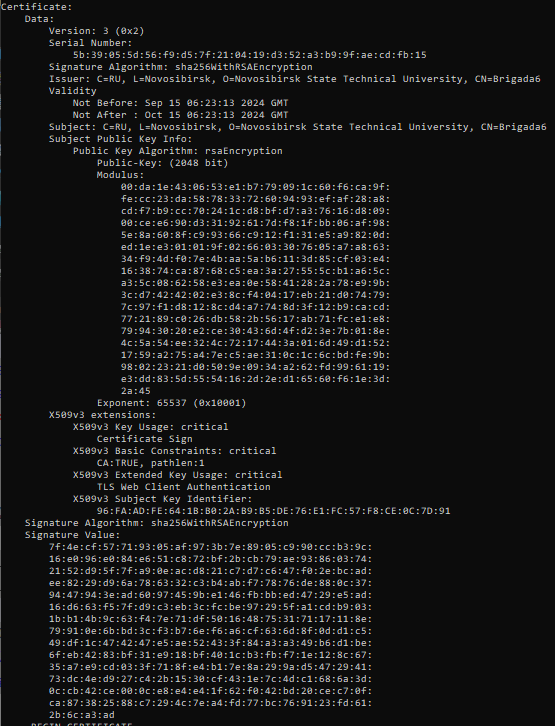
[ v3\_ca ]

keyUsage = critical, keyCertSign

basicConstraints = critical, CA:true, pathlen:1

extendedKeyUsage = critical, TLS Web Client Authentication

Результат:



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 таким образом, чтобы openssl req -in client.csr -text выдавал расшифровку вида:**

Certificate:

    Data:

        Version: 3 (0x2)

        Serial Number: ...

    Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <Some name>

        Validity

            Not Before: ...

            Not After : ...

        Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <ФИО 1, ФИО 2, ...>

        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                Public-Key: (2048 bit)

                Modulus: ...

                Exponent: ...

        X509v3 extensions:

            X509v3 Basic Constraints:

                CA:FALSE

            X509v3 Key Usage:

                Digital Signature

            X509v3 Extended Key Usage:

                TLS Web Client Authentication

    Signature Algorithm: sha256WithRSAEncryption

…

Текст конфига:  
[ req ]

distinguished\_name = Brigada6

default\_bits = 2048

default\_md = sha256

req\_extensions = v3\_req

prompt = no

[ Brigada6 ]

CN = Artem Zamyatin Vladislavovich, Vyxodcev Alexandr Sergeecvich

C = RU

L = Novosibirsk

O = Novosibirsk State Technical University

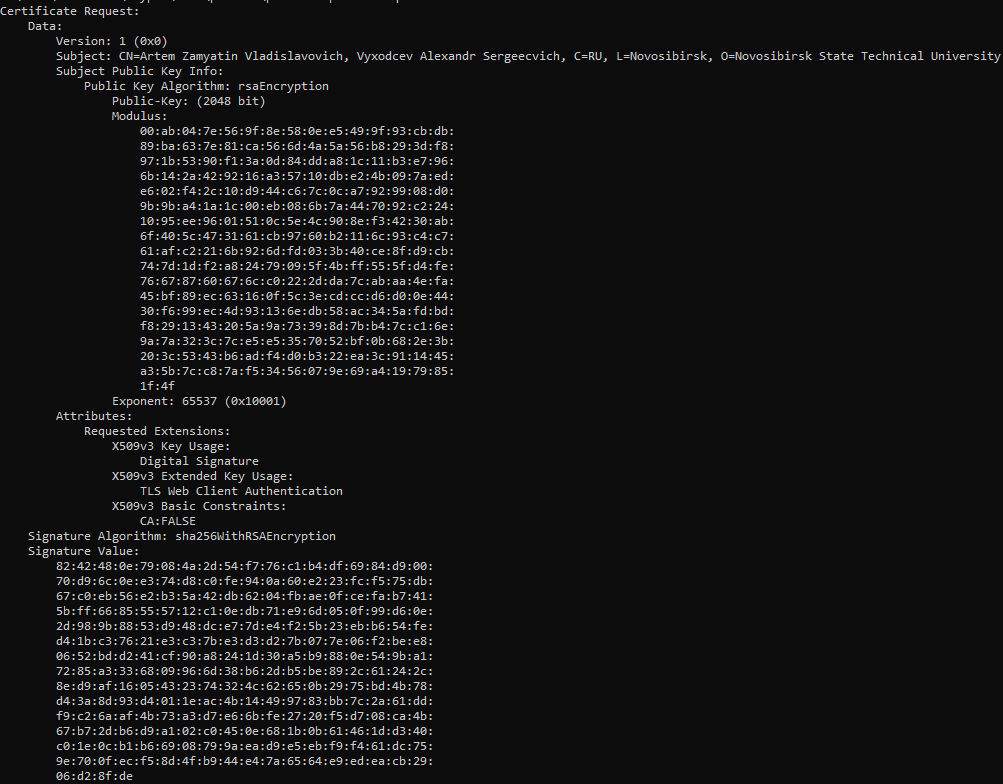
[ v3\_req ]

keyUsage = Digital Signature

extendedKeyUsage = TLS Web Client Authentication

basicConstraints = CA:FALSE

Результат:



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 таким образом, чтобы openssl x509 -in client.crt -text выдавал расшифровку вида:**

Certificate:

    Data:

        Version: 3 (0x2)

        Serial Number: ...

    Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <Some name>

        Validity

            Not Before: ...

            Not After : ...

        Subject: C = RU, L = Novosibirsk, O = Novosibirsk State Technical University, CN = <ФИО 1, ФИО 2, ...>

        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                Public-Key: (2048 bit)

                Modulus: ...

                Exponent: ...

        X509v3 extensions:

            X509v3 Basic Constraints:

                CA:FALSE

            X509v3 Key Usage:

                Digital Signature

            X509v3 Extended Key Usage:

                TLS Web Client Authentication

    Signature Algorithm: sha256WithRSAEncryption

…

Текст конфига:

[ req ]

distinguished\_name = Brigada6

default\_bits = 2048

default\_md = sha256

req\_extensions = v3\_req

prompt = no

[ Brigada6 ]

CN = Artem Zamyatin Vladislavovich, Vyxodcev Alexandr Sergeecvich

C = RU

L = Novosibirsk

O = Novosibirsk State Technical University

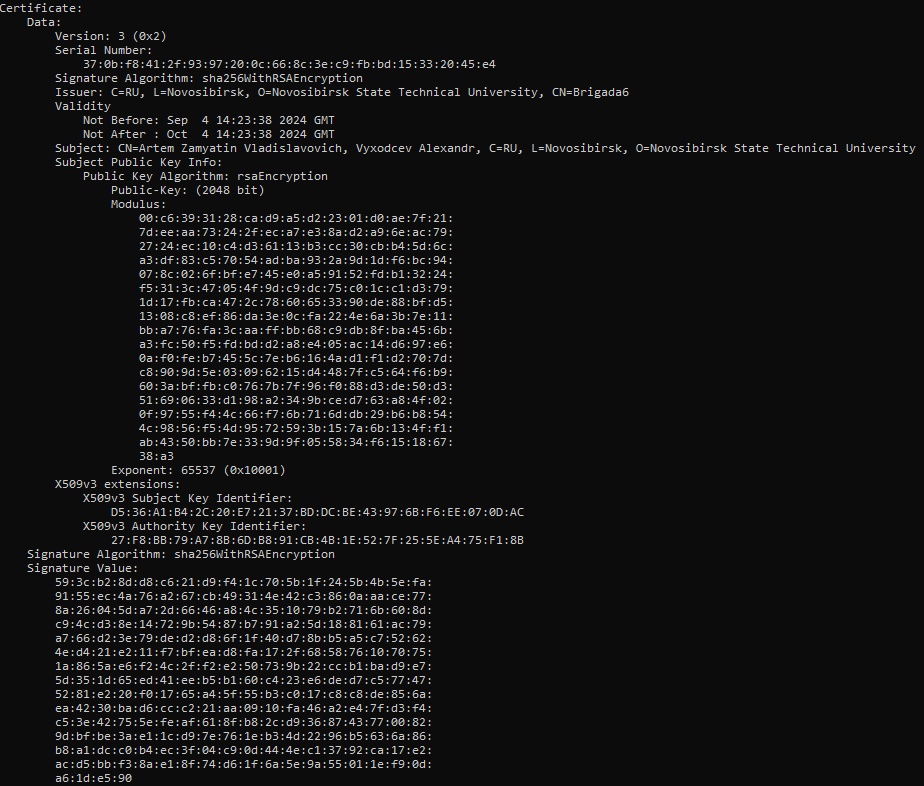
[ v3\_req ]

keyUsage = Digital Signature

extendedKeyUsage = TLS Web Client Authentication

basicConstraints = CA:FALSE

Результат:

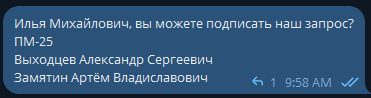


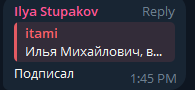
**Часть 2.** Подписать сертификат у преподавателя

1. Загрузить файл запроса сертификата методом POST на адрес https://istupakov.ddns.net:4006/api/csr.  
   Запомнить полученный в ответ в Location Header адрес для скачивания сертификата.

Загрузили файл с помощью cURL, используя команду:  
curl https://istupakov.ddns.net:4006/api/csr -F file=@client.csr --cacert cryptolab-ca.crt -v

1. **Подойти к преподавателю и попросить подписать ваш запрос.**





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

D:\unik\cripto\lab1\point 4>curl https://istupakov.ddns.net:4006/api/csr -F file=@client.csr --cacert cryptolab-ca.crt -v

\* Host istupakov.ddns.net:4006 was resolved.

\* IPv6: (none)

\* IPv4: 217.71.129.139

\* Trying 217.71.129.139:4006...

\* Connected to istupakov.ddns.net (217.71.129.139) port 4006

\* schannel: disabled automatic use of client certificate

\* ALPN: curl 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.x

> POST /api/csr HTTP/1.1

> Host: istupakov.ddns.net:4006

> User-Agent: curl/8.7.1

> Accept: \*/\*

> Content-Length: 1392

> Content-Type: multipart/form-data; boundary=------------------------5uBkxYKlA2pmgVUrEd7tPe

>

\* upload completely sent off: 1392 bytes

< HTTP/1.1 202 Accepted

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

< Date: Fri, 13 Sep 2024 02:57:26 GMT

< Server: Kestrel

**< Location: https://istupakov.ddns.net:4006/api/csr/5dc3be10-7973-4f5b-95e6-360d136798fd**

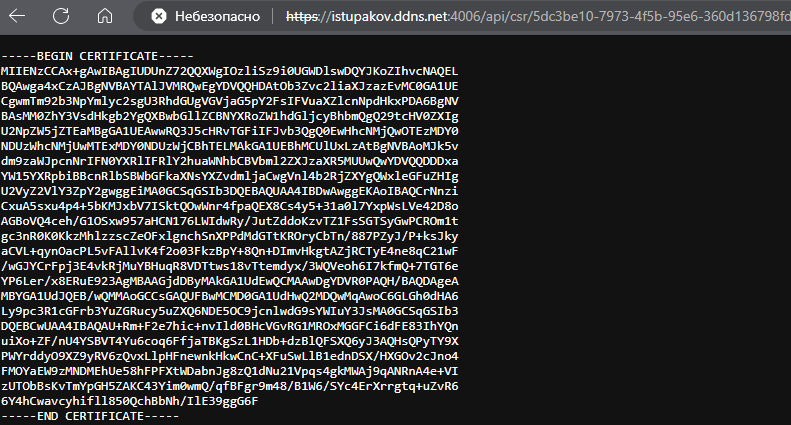
< Transfer-Encoding: chunked

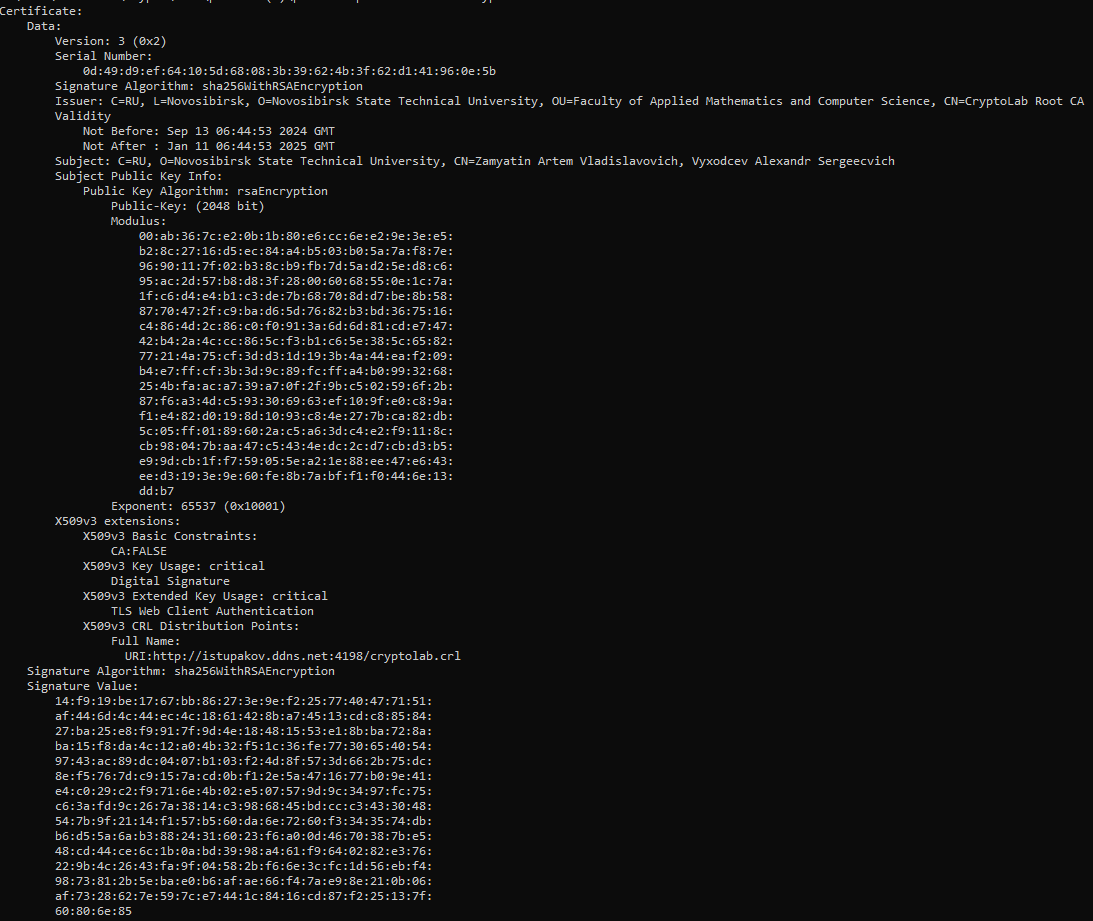
< Strict-Transport-Security: max-age=2592000

<

{"id":"5dc3be10-7973-4f5b-95e6-360d136798fd","subject":"CN = \"Zamyatin Artem Vladislavovich, Vyxodcev Alexandr Sergeecvich\", C = RU, L = Novosibirsk, O = Novosibirsk State Technical University","timestamp":"2024-09-13T02:57:26.9713581Z"}\* Connection #0 to host istupakov.ddns.net left intact

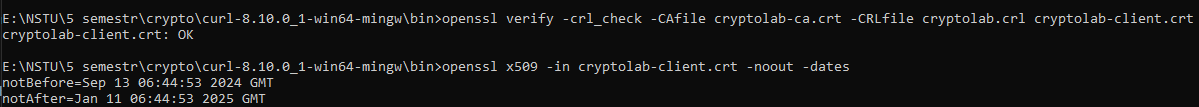
Из данного запроса нас интересует заголовок Location в котором расположена ссылка на подписанный сертификат:



Расшифровка подписанного сертификата:  
****

1. **Изучить как работает отзыв сертификатов. Продемонстрировать проверку, что полученный сертификат корректен и не отозван.**

**Отзыв сертификатов** — это процесс аннулирования цифрового сертификата до окончания его срока действия. Это означает, что сертификат больше не может считаться доверенным, даже если он формально действителен по времени.   
  
В сертификате указана ссылка на файл CRL, благодаря которой мы можем проверить полученный сертификат.

****

Вывод: Мы убедились, что сертификат действителен и не истек, используйте команду verify.

**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:4006/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.**

E:\NSTU\5 semestr\crypto\curl-8.10.0\_1-win64-mingw\bin>curl -X POST https://istupakov.ddns.net:4006/api/chat/message -H "Content-Type: application/json" -d @message.json --cert cryptolab-client.crt --key client.key --cacert cryptolab-ca.crt -v

Note: Using embedded CA bundle, for proxies (228633 bytes)

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

\* Host istupakov.ddns.net:4006 was resolved.

\* IPv6: (none)

\* IPv4: 217.71.129.139

\* Trying 217.71.129.139:4006...

\* Connected to istupakov.ddns.net () port 4006

Enter PEM pass phrase:

\* ALPN: curl offers h2,http/1.1

\* TLSv1.3 (OUT), TLS handshake, Client hello (1):

\* CAfile: cryptolab-ca.crt

\* CApath: none

\* TLSv1.3 (IN), TLS handshake, Server hello (2):

\* TLSv1.3 (IN), TLS handshake, Unknown (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 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 / [blank] / UNDEF

\* ALPN: server accepted h2

\* Server certificate:

\* subject: C=RU; O=Novosibirsk State Technical University; OU=Faculty of Applied Mathematics and Computer Science; CN=CryptoLab Server

\* start date: Sep 1 21:07:14 2024 GMT

\* expire date: Aug 30 21:07:14 2034 GMT

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

\* issuer: C=RU; L=Novosibirsk; O=Novosibirsk State Technical University; OU=Faculty of Applied Mathematics and Computer Science; CN=CryptoLab Root CA

\* SSL certificate verify ok.

\* Certificate level 0: Public key type ? (2048/112 Bits/secBits), signed using sha256WithRSAEncryption

\* Certificate level 1: Public key type ? (2048/112 Bits/secBits), signed using sha256WithRSAEncryption

\* using HTTP/2

\* [HTTP/2] [1] OPENED stream for https://istupakov.ddns.net:4006/api/chat/message

\* [HTTP/2] [1] [:method: POST]

\* [HTTP/2] [1] [:scheme: https]

\* [HTTP/2] [1] [:authority: istupakov.ddns.net:4006]

\* [HTTP/2] [1] [:path: /api/chat/message]

\* [HTTP/2] [1] [user-agent: curl/8.10.0]

\* [HTTP/2] [1] [accept: \*/\*]

\* [HTTP/2] [1] [content-type: application/json]

\* [HTTP/2] [1] [content-length: 56]

> POST /api/chat/message HTTP/2

> Host: istupakov.ddns.net:4006

> User-Agent: curl/8.10.0

> Accept: \*/\*

> Content-Type: application/json

> Content-Length: 56

>

\* upload completely sent off: 56 bytes

< HTTP/2 201

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

< date: Sun, 15 Sep 2024 07:26:41 GMT

< server: Kestrel

< location: https://istupakov.ddns.net:4006/chat/message/5570f42c-1e4c-4d75-a90d-04e550bbff98

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

<

{"message":"Hello World! From Artem Zamyatin and Vyxodcev Alexandr","user":"CN=\"Zamyatin Artem Vladislavovich, Vyxodcev Alexandr Sergeecvich\", O=Novosibirsk State Technical University, C=RU","timestamp":"2024-09-15T07:26:41.9336288Z","id":"5570f42c-1e4c-4d75-a90d-04e550bbff98"}\* Connection #0 to host istupakov.ddns.net left intact