# Практическая работа 1

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

За выполнение обязательной части - 12 баллов.

**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  
...

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 Request:

Data:

Version: 1 (0x0)

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

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus: ...

Exponent: ...

Attributes:

Requested Extensions:

X509v3 Key Usage:

Digital Signature

X509v3 Extended Key Usage:

TLS Web Client Authentication

X509v3 Basic Constraints:

CA:FALSE

Signature Algorithm: sha256WithRSAEncryption

...

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

…

1. Все подготовленные конфиги и полученные расшифровки добавить в отчет.

**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.

Запрос можно сделать с помощью утилиты Curl:

curl https://istupakov.ddns.net:4006/api/csr -F file=@client.csr --cacert cryptolab-ca.crt -v

Файл cryptolab-ca.crt:

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

MIIFIzCCBAugAwIBAgIUO/5hOVy0eOjeHoFRdcBGwxqnO7UwDQYJKoZIhvcNAQEL

BQAwga4xCzAJBgNVBAYTAlJVMRQwEgYDVQQHDAtOb3Zvc2liaXJzazEvMC0GA1UE

CgwmTm92b3NpYmlyc2sgU3RhdGUgVGVjaG5pY2FsIFVuaXZlcnNpdHkxPDA6BgNV

BAsMM0ZhY3VsdHkgb2YgQXBwbGllZCBNYXRoZW1hdGljcyBhbmQgQ29tcHV0ZXIg

U2NpZW5jZTEaMBgGA1UEAwwRQ3J5cHRvTGFiIFJvb3QgQ0EwHhcNMjQwODMxMTYw

ODQ2WhcNMzQwODI5MTYwODQ2WjCBrjELMAkGA1UEBhMCUlUxFDASBgNVBAcMC05v

dm9zaWJpcnNrMS8wLQYDVQQKDCZOb3Zvc2liaXJzayBTdGF0ZSBUZWNobmljYWwg

VW5pdmVyc2l0eTE8MDoGA1UECwwzRmFjdWx0eSBvZiBBcHBsaWVkIE1hdGhlbWF0

aWNzIGFuZCBDb21wdXRlciBTY2llbmNlMRowGAYDVQQDDBFDcnlwdG9MYWIgUm9v

dCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRNhpOaHJlMU4I

uriDlpjCeXklFJkByZ7yEdAS367mBLlUxFfibK5B/ApopXk/szjsMr0yqQmt2tsa

JvdD4gsXd9NXaUxTvsqbRwBKe0Xovw0UXO+whPBcz6QDydA/fH4xvBfbWDEMlQCF

Dte9JfRTEnGYUyZOG+/I/Bh5LhsODG4scZw9axcJAQvHkSterHOxK9Xr5dGGN0zC

7fUoIVtGRcW2JOCA3mZZTzuYlNXDFjNMfLBo/rjFhC/Q9+jwy9sA46lTThQIcwET

dHIkxAj/7cGoqKqOJ0Ic6e40JvpYNga2CfvMOXXaWajv6qsLtwrPS2SHMpR8Ilrh

fojpC5cCAwEAAaOCATUwggExMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFPuw

lHXfk1fyof8CUdqleaHTsxnFMIHuBgNVHSMEgeYwgeOAFPuwlHXfk1fyof8CUdql

eaHTsxnFoYG0pIGxMIGuMQswCQYDVQQGEwJSVTEUMBIGA1UEBwwLTm92b3NpYmly

c2sxLzAtBgNVBAoMJk5vdm9zaWJpcnNrIFN0YXRlIFRlY2huaWNhbCBVbml2ZXJz

aXR5MTwwOgYDVQQLDDNGYWN1bHR5IG9mIEFwcGxpZWQgTWF0aGVtYXRpY3MgYW5k

IENvbXB1dGVyIFNjaWVuY2UxGjAYBgNVBAMMEUNyeXB0b0xhYiBSb290IENBghQ7

/mE5XLR46N4egVF1wEbDGqc7tTAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQEL

BQADggEBAKdZjOqmyH+JWugjAeky1Spz06wNCOqqrBkGaHPHNRSOUBnR3/ssMbaF

BfXt0SdbiPqwJz/lJ4akWazezQK4K7faOQF3RA3xwxJ9UxnSQYpJFkUiCdwYy1pH

f5FaYNh2dfbPwPunZdj5GwEiuzaId5dukp70HcqY35/CsFfTm4cvSfhVt6mmG/AA

tlOVa+LQi3FmdLgUmGSr5w4iwvT2maHwzHLq3C747j0bhBTyBlBm/Vicyp+ynCk1

propHicvbPdocpCTGjs1E8CUltQn2OjARYtu0ohl2EgpkFW1MKqKD1d5Xw3jpXFa

HL5ddAhO3hpJJqi2YInbCPq6RNIjq3Q=

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

*Если curl возвращает ошибку, попробуйте использовать более свежую версию.*

1. Подойти к преподавателю и попросить подписать ваш запрос.
2. Скачать подписанный сертификат, вставить в отчет его адрес и расшифровку.
3. (*дополнительно, +5 баллов*) Изучить как работает отзыв сертификатов. Продемонстрировать проверку, что полученный сертификат корректен и не отозван.

**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.
2. Привести результаты запросов с сертификатами из части 1.3 и из части 2 в отчете, в том числе ссылку на отправленное сообщение (возвращается в Location Header).
3. (*дополнительно, +3 балла*) Продемонстрировать доступ в чат из браузера на ПК и телефоне.