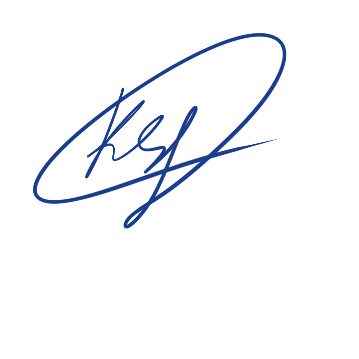
**Федеральное государственное бюджетное образовательное учреждение высшего образования "Белгородский государственный технологический университет им. В.Г. Шухова"**

Кафедра программного обеспечения вычислительной техники и автоматизированных систем.

**Лабораторная работа №5**

Инфраструктура открытых ключей.

Выполнил:

Студент группы КБ-211

Коренев Д.Н.

Принял:

Смакаев А.В.

Оглавление

[Оглавление 2](#_Toc185562146)

[Задание 3](#_Toc185562147)

[Вывод 11](#_Toc185562148)

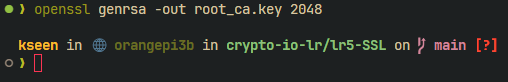
*Цель работы:* ознакомиться с принципами работы инфраструктуры открытых ключей, методами ее работы, хранения ключей и форматом сертификатов X.509. Разработать консольное приложение, работающее со встроенным в операционную систему хранилищем сертификатов.

Задание

1. Сгенерировать самоподписанный сертификат CA. В качестве CN указываем 127.0.0.1, остальные данные можно указать вымышленные
   * вариант с openssl описан [в статье на habr](https://habr.com/ru/articles/671730/)
   * вариант с CA Smallstep описан [в статье на habr](https://habr.com/ru/articles/671730/)

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание  
Рисунок 1. Версия OpenSSL.

  
Рисунок 2. Для нашего CA генерируем приватный ключ 2048-бит RSA.

Вывод команды с рисунка 2:

-----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDJIkktS7QEwSgg

nSoXV0+sDAU4ZjkPgt5XhH4794Atbk3WpyxtYtbk1h2KFGNyW5Cqe5RqExuEufLm

7osf9mThtB019hDb1ZZGQTzZQrWhmncu191mFi/4sc38vd80s0CioQ+i234P/XdN

UQE6XZQ3kTidAv4BAinx9CBNQNsf/mSPNMwqgNzzyPIbf+o+j5rwD9cLTQFu3jQt

wySgu/aQvraMam67q5CMezPdAPuU+7wUkUzgb2wY3DRCMQ8Zsq2+Wg3pNJbx6wOU

05esrrH8lORowqVSmJE/bvVopft60bbrM2GzfjRnqhKpchFdJ/QOj1u49+rwNioD

C25YDJ9zAgMBAAECggEAY8VDIVnlEVqzSgJMB8oCtmg8Cq8CbQRQwH7zk1GBXofR

ysGgUx5tVJQ1kPHuJqLvDvJAO6IAy4TlzdHUZ2V0w1TyDHtj/3hik7T2txrVODWE

G1Nu+p3U6/tfH5kb6Gtmi4VzWSihztK/ZDXjcw1KYYoC2DfMwblODzw27btXNvW7

snduxOxPq6ZsNtjz6OydyRJUzL0OnlyJiO+alUXXE9n5Z5HMCpcI+7n1Gv9kiRAe

ZeZGWOZv4QXW6jDvlB7aTcX1ZiBUSoU+bHAnJWgULxWukMJ0nsrVQ4jPKrauxIek

rT6x+KXZIpyS6nOVDujyOMWwAhN83iINMab4QV0tqQKBgQDqrqb1VszA49p/r7Ul

puRI1caK2A9gRp0drKOPsTqjJHX0C41eajqK0AsHAXCxXV/VtLOkW4UCTnWFH8Qd

sz0Hb2iLIct8M1liMvapOy2s1s5dT2R9l9quFDw3/Cr52Ud6O9HA3bjw34q9A38C

shuqXSXuNXxjtkY7m6ByRHtXvQKBgQDbZ36fkS1WK5Y4K2IbTV3sEnU5VvAlqYhc

7q7+FIFYw7WOIc5RQhHD15U4JoDuEj79dIgg9kY3/rkeDs+NY/vG242AEcIV9S8S

EIEnkfpHU1sGRdALavWLrW4cJxzyWC77n/Wt+axFZPjKmoz/IqJA4CIluLAx6A5p

bO/TDeTu7wKBgDesJQlQhRRBOWVPDn8XH1Kz+/yWEte5CK6wdMCyv4FSNfUmBGxg

cPDbN7J6wfwhdYmh63fTCjOo3zIsff65tYGdCUTwSHB3Uf38rw0ob8Zv0tbJ7cHp

k0P2ou55EMzioZU6uaCyOJxTu3rpaGkATZXVsRjYcWDKLdEYMzDIVCZVAoGAcRM1

vycjJnXwRaKWPVvyO+iHYbXcroxhKwQYS/plb0nuGAJ0Qoy6eyRwUzAE4q2kqRuV

zOcf6VvuK/+WGFifOi2ND6QXUxm52KWI6svhIUFkeCciwb+uLP6E8R13Xa71B9m4

1KEIl/sh/ckJQbSnyqe48ZfttsrSIqNyNmPCySECgYEAt3SQUZZ3aajOjhYQCJzb

XNUhIdqicZWwG2EU5T8tlrY15MMuaiV22y/mnYVIVNhYd6Pk6DqoO58wr0oXoKO4

1fqN4pVm/vqrAN9/pDu3LFCozjbMKzUD7cka8fRs8tdwEMujNd63bAbxVzEK9Yi1

UacIOm9spQeenHl9Xwmvamk=

-----END PRIVATE KEY-----

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание  
Рисунок 3. Далее для нашего CA генерируем X.509 сертификат на 365 дней (root\_ca.crt) и подписываем его приватным ключом (root\_ca.key).

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

76:c6:83:1e:8f:db:d3:ed:c5:d5:85:38:f5:23:8b:f2:fa:5c:4e:4d

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, ST = Samarskaya oblast, L = Samara, O = Kerasi, OU = Home, CN = LCL, emailAddress = ex@mail.ru

Validity

Not Before: Dec 20 00:30:52 2024 GMT

Not After : Dec 20 00:30:52 2025 GMT

Subject: C = RU, ST = Samarskaya oblast, L = Samara, O = Kerasi, OU = Home, CN = LCL, emailAddress = ex@mail.ru

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c9:22:49:2d:4b:b4:04:c1:28:20:9d:2a:17:57:

4f:ac:0c:05:38:66:39:0f:82:de:57:84:7e:3b:f7:

80:2d:6e:4d:d6:a7:2c:6d:62:d6:e4:d6:1d:8a:14:

63:72:5b:90:aa:7b:94:6a:13:1b:84:b9:f2:e6:ee:

8b:1f:f6:64:e1:b4:1d:35:f6:10:db:d5:96:46:41:

3c:d9:42:b5:a1:9a:77:2e:d7:dd:66:16:2f:f8:b1:

cd:fc:bd:df:34:b3:40:a2:a1:0f:a2:db:7e:0f:fd:

77:4d:51:01:3a:5d:94:37:91:38:9d:02:fe:01:02:

29:f1:f4:20:4d:40:db:1f:fe:64:8f:34:cc:2a:80:

dc:f3:c8:f2:1b:7f:ea:3e:8f:9a:f0:0f:d7:0b:4d:

01:6e:de:34:2d:c3:24:a0:bb:f6:90:be:b6:8c:6a:

6e:bb:ab:90:8c:7b:33:dd:00:fb:94:fb:bc:14:91:

4c:e0:6f:6c:18:dc:34:42:31:0f:19:b2:ad:be:5a:

0d:e9:34:96:f1:eb:03:94:d3:97:ac:ae:b1:fc:94:

e4:68:c2:a5:52:98:91:3f:6e:f5:68:a5:fb:7a:d1:

b6:eb:33:61:b3:7e:34:67:aa:12:a9:72:11:5d:27:

f4:0e:8f:5b:b8:f7:ea:f0:36:2a:03:0b:6e:58:0c:

9f:73

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

70:91:B1:C8:AF:8C:5D:C3:09:7A:3C:D7:56:7C:3C:DB:1C:01:3D:B6

X509v3 Authority Key Identifier:

70:91:B1:C8:AF:8C:5D:C3:09:7A:3C:D7:56:7C:3C:DB:1C:01:3D:B6

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

83:1e:99:d9:56:0d:62:87:63:21:e1:c6:4e:fa:28:1f:c4:72:

6d:b8:5c:8a:59:56:2d:e3:68:be:2f:8a:4b:fd:70:a4:db:50:

ae:f0:6e:a6:b2:d6:94:7a:ef:e2:d6:4b:fd:45:1f:04:3d:3b:

df:da:aa:a4:93:67:d8:67:a5:04:d8:f9:c7:54:7b:24:a5:9d:

ef:a3:14:bc:ff:de:86:83:9b:51:81:3b:41:0d:c6:16:5b:1c:

33:ed:71:fc:08:0f:44:f2:7d:7b:62:93:7a:47:b4:63:6d:19:

11:6e:9e:0b:61:55:b5:2a:6c:65:bd:fd:f4:1a:72:cb:46:9e:

4c:9f:c8:56:36:7f:c4:2e:68:72:6e:86:e0:54:e5:dc:17:21:

1c:a3:6f:23:4f:a7:3d:62:05:a1:f7:1f:a3:40:45:b9:91:75:

87:cb:3e:f3:05:00:af:95:f7:27:01:10:3b:9d:0e:91:2a:b4:

26:15:29:b1:3a:0d:7c:30:2c:58:23:d0:2b:fa:4f:b4:2b:18:

18:29:b3:94:44:52:89:07:51:c6:4c:88:e6:63:99:30:c3:ff:

1d:e8:19:9b:2e:12:97:a6:b5:88:fb:78:c5:fc:4f:b1:6e:3f:

5e:f2:1a:34:10:f6:85:84:4e:fa:1c:f5:b6:3e:c1:2f:45:6a:

00:40:af:89

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

MIID6TCCAtGgAwIBAgIUdsaDHo/b0+3F1YU49SOL8vpcTk0wDQYJKoZIhvcNAQEL

BQAwgYMxCzAJBgNVBAYTAlJVMRowGAYDVQQIDBFTYW1hcnNrYXlhIG9ibGFzdDEP

MA0GA1UEBwwGU2FtYXJhMQ8wDQYDVQQKDAZLZXJhc2kxDTALBgNVBAsMBEhvbWUx

DDAKBgNVBAMMA0xDTDEZMBcGCSqGSIb3DQEJARYKZXhAbWFpbC5ydTAeFw0yNDEy

MjAwMDMwNTJaFw0yNTEyMjAwMDMwNTJaMIGDMQswCQYDVQQGEwJSVTEaMBgGA1UE

CAwRU2FtYXJza2F5YSBvYmxhc3QxDzANBgNVBAcMBlNhbWFyYTEPMA0GA1UECgwG

S2VyYXNpMQ0wCwYDVQQLDARIb21lMQwwCgYDVQQDDANMQ0wxGTAXBgkqhkiG9w0B

CQEWCmV4QG1haWwucnUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJ

IkktS7QEwSggnSoXV0+sDAU4ZjkPgt5XhH4794Atbk3WpyxtYtbk1h2KFGNyW5Cq

e5RqExuEufLm7osf9mThtB019hDb1ZZGQTzZQrWhmncu191mFi/4sc38vd80s0Ci

oQ+i234P/XdNUQE6XZQ3kTidAv4BAinx9CBNQNsf/mSPNMwqgNzzyPIbf+o+j5rw

D9cLTQFu3jQtwySgu/aQvraMam67q5CMezPdAPuU+7wUkUzgb2wY3DRCMQ8Zsq2+

Wg3pNJbx6wOU05esrrH8lORowqVSmJE/bvVopft60bbrM2GzfjRnqhKpchFdJ/QO

j1u49+rwNioDC25YDJ9zAgMBAAGjUzBRMB0GA1UdDgQWBBRwkbHIr4xdwwl6PNdW

fDzbHAE9tjAfBgNVHSMEGDAWgBRwkbHIr4xdwwl6PNdWfDzbHAE9tjAPBgNVHRMB

Af8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCDHpnZVg1ih2Mh4cZO+igfxHJt

uFyKWVYt42i+L4pL/XCk21Cu8G6mstaUeu/i1kv9RR8EPTvf2qqkk2fYZ6UE2PnH

VHskpZ3voxS8/96Gg5tRgTtBDcYWWxwz7XH8CA9E8n17YpN6R7RjbRkRbp4LYVW1

Kmxlvf30GnLLRp5Mn8hWNn/ELmhybobgVOXcFyEco28jT6c9YgWh9x+jQEW5kXWH

yz7zBQCvlfcnARA7nQ6RKrQmFSmxOg18MCxYI9Ar+k+0KxgYKbOURFKJB1HGTIjm

Y5kww/8d6BmbLhKXprWI+3jF/E+xbj9e8ho0EPaFhE76HPW2PsEvRWoAQK+J

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

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание  
Рисунок 4. Генерируем ключи для сервера.

-----BEGIN PRIVATE KEY-----

MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCdh6XIMXUiZfaa

5K/WjApepgcQC9qqwbx2EXaB6PvXceobYSJKPxujWR+XgLlGXvVSUcgkIwZjC540

39fe+p45GkOVpz4PRSl/e8ilU5jaa1wTL8FRJWdCOquOmGDGwhCMnmO2M9yvv2MQ

5HgNlU7uCjTW/Iww4AWxRQj/8FH+VCi/IMFFfvfzCEvyIV+uQ3zfykOHOiRvOKfz

F+PaWmNfiENnt2tEoAKObex/T1eOgmQbsMcP17vYJJ/dvf7RLx79EQDeA1r08Zvt

w/wVsgIHBtq1yyAqJMc7dRIGunld1m30APkP10HlnALKXB70r/cmv9RXk4/a8ooe

GVD5Uxy7AgMBAAECggEAAVB4BTsuAc/dk0R3l+l3NK71JCC7l4a74c60StH80YfC

LxRL/iT+QApAUm1HUagwXjPcem2B+7v4rlkOKtTm33PlC6lnjsBCLMdSanHpUCxq

vXMKjXjFOC8Ku2SkehDbpOPonqtagTgUxYSCelDvZadw8jimzfzKHCtTr3770CY0

Po3Y7BWBeZ3CgQRExB/XgsEABgUxenUKvqsVC/WLhAVjhltL6tUsfiDIhrnnMNYR

+v0sReo3SMqTiw+l9udPapCTT/1h7cYUD5uHfb+M1paHXfPmvJCPCxzmKCJog3b8

/sI5XT8/Ze1zFpALpyD63FdN/fnxYEL9QDleeOwRwQKBgQDcGK2lpLWZwsxSG1FX

Q7R9qzqPh4kXI7pCkX3/7jlRBB0TGwE7tNpQ8lzx/5i+yZX1OTMSGp47VZnPukPa

bXC3Z3dEKdTiosA5MwI7RJCikElloMz/Ox1h87OtGwKb110d8GpM03eVdDFGxL0M

YoCHEzw1gjSpAIk/aoj1NChBCwKBgQC3OinxVj1O3mFfucxjnuWv5dr/LcCkliif

8hGAvihvEoVul8wn0q3aAzef5uLU6Wm1vT7xH+F8GwvfqiEVJkimARkjoDFRM6oQ

2gkmqAFDHwTULX5GK3kQyY+8FHdT8LPmguySo9XqESMYhz6G4Ormv+nm5SHHq5wV

UqRB+klBEQKBgB1/FS6Az3Gm4JkUXidSxIqe+v8nS+EVAa5QL1GwTHAmG/tmgBjP

WP7GLFymQ4M2Ium1W7nOZWxQQYfMT7GjPxrlO9+ft48T/qzrwB3PR47xxVRgY3jF

JF/vOCI333ahOzJ6+NQI9xrJcp0oWqmhPdZcZpJJO+N2Ve5wyaAK+GYXAoGAPSHw

4I6vgeL8hh3NredUJy3/tWgkgEWBZGw1nsjTYMvDLTUEbr0COF0ecAFu6S6/kF2F

5JmIeAnmGkf/JblSP+DZ7GMEUV11fo3gw78GPMjaqZhMK0lR6WH2zP/fGGiU/XHt

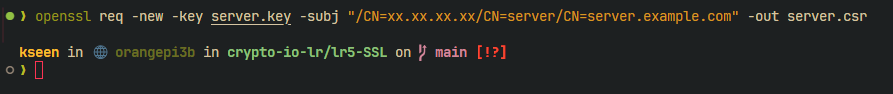
ULfNJX12QjbNi977QOYDOoB0ltQRDaQ3HbROQKECgYAyezTFF7pUUJv3ejXCLYNL

zEqtxWcfA4WOKSpCzLYbBw06xBlgvMbwopw7HfhjNFdBc9hjTqESTA3VyNpbbVKv

9iW0flQzfByVP8JbIO1jRvmSTHZQSENujt2RXzeaCAAMqA7szRL7dR3sWrtvgM5h

ryBU/E/3RQuY8kw9R/z3wA==

-----END PRIVATE KEY-----

  
Рисунок 5. Создаем запрос на сертификат для сервера.

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = xx.xx.xx.xx, CN = server, CN = server.example.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:9d:87:a5:c8:31:75:22:65:f6:9a:e4:af:d6:8c:

0a:5e:a6:07:10:0b:da:aa:c1:bc:76:11:76:81:e8:

fb:d7:71:ea:1b:61:22:4a:3f:1b:a3:59:1f:97:80:

b9:46:5e:f5:52:51:c8:24:23:06:63:0b:9e:34:df:

d7:de:fa:9e:39:1a:43:95:a7:3e:0f:45:29:7f:7b:

c8:a5:53:98:da:6b:5c:13:2f:c1:51:25:67:42:3a:

ab:8e:98:60:c6:c2:10:8c:9e:63:b6:33:dc:af:bf:

63:10:e4:78:0d:95:4e:ee:0a:34:d6:fc:8c:30:e0:

05:b1:45:08:ff:f0:51:fe:54:28:bf:20:c1:45:7e:

f7:f3:08:4b:f2:21:5f:ae:43:7c:df:ca:43:87:3a:

24:6f:38:a7:f3:17:e3:da:5a:63:5f:88:43:67:b7:

6b:44:a0:02:8e:6d:ec:7f:4f:57:8e:82:64:1b:b0:

c7:0f:d7:bb:d8:24:9f:dd:bd:fe:d1:2f:1e:fd:11:

00:de:03:5a:f4:f1:9b:ed:c3:fc:15:b2:02:07:06:

da:b5:cb:20:2a:24:c7:3b:75:12:06:ba:79:5d:d6:

6d:f4:00:f9:0f:d7:41:e5:9c:02:ca:5c:1e:f4:af:

f7:26:bf:d4:57:93:8f:da:f2:8a:1e:19:50:f9:53:

1c:bb

Exponent: 65537 (0x10001)

Attributes:

(none)

Requested Extensions:

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

0d:6c:72:71:6b:5a:2b:32:df:a2:3c:39:f6:01:6e:12:88:33:

d6:fe:3b:fa:fe:ec:90:ba:a8:13:d2:a6:14:06:ea:f5:32:3e:

0c:b3:54:82:5e:38:01:d6:61:f8:5e:89:c5:e4:ae:4e:97:d8:

68:5b:c8:d8:07:af:e2:c5:17:7a:ad:4f:c7:64:a0:2f:99:a2:

d9:6b:2d:0d:05:82:09:77:dc:27:66:d9:ad:dc:e4:19:c4:25:

32:ec:78:fd:68:9c:2f:c2:3f:26:8b:62:2e:32:e3:ab:48:90:

ff:e2:e3:eb:a6:f1:e7:dc:7d:9f:38:b0:29:16:42:10:7e:b0:

cc:67:62:0e:01:27:bb:a7:8f:20:db:43:65:ae:b0:50:d2:80:

07:70:33:72:ae:f5:02:5b:a6:01:58:80:26:bd:d9:00:5c:08:

80:aa:55:0c:0e:9c:b1:ad:17:ef:46:38:26:40:bb:51:87:ab:

da:cb:d9:49:f7:cd:54:5a:8a:67:40:6a:b6:60:15:47:bf:74:

91:26:0d:bd:9d:b8:34:af:2a:aa:87:8a:95:d9:47:5c:99:6b:

7d:5f:9a:84:2f:29:6f:f1:70:c4:b6:48:ce:6c:c2:95:f3:2b:

49:e1:98:4b:2c:1a:e4:13:a9:43:9a:79:96:0b:f1:cc:4c:0f:

9c:8b:21:4e

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

MIICiTCCAXECAQAwRDEUMBIGA1UEAwwLeHgueHgueHgueHgxDzANBgNVBAMMBnNl

cnZlcjEbMBkGA1UEAwwSc2VydmVyLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0B

AQEFAAOCAQ8AMIIBCgKCAQEAnYelyDF1ImX2muSv1owKXqYHEAvaqsG8dhF2gej7

13HqG2EiSj8bo1kfl4C5Rl71UlHIJCMGYwueNN/X3vqeORpDlac+D0Upf3vIpVOY

2mtcEy/BUSVnQjqrjphgxsIQjJ5jtjPcr79jEOR4DZVO7go01vyMMOAFsUUI//BR

/lQovyDBRX738whL8iFfrkN838pDhzokbzin8xfj2lpjX4hDZ7drRKACjm3sf09X

joJkG7DHD9e72CSf3b3+0S8e/REA3gNa9PGb7cP8FbICBwbatcsgKiTHO3USBrp5

XdZt9AD5D9dB5ZwCylwe9K/3Jr/UV5OP2vKKHhlQ+VMcuwIDAQABoAAwDQYJKoZI

hvcNAQELBQADggEBAA1scnFrWisy36I8OfYBbhKIM9b+O/r+7JC6qBPSphQG6vUy

PgyzVIJeOAHWYfheicXkrk6X2GhbyNgHr+LFF3qtT8dkoC+ZotlrLQ0Fggl33Cdm

2a3c5BnEJTLseP1onC/CPyaLYi4y46tIkP/i4+um8efcfZ84sCkWQhB+sMxnYg4B

J7unjyDbQ2WusFDSgAdwM3Ku9QJbpgFYgCa92QBcCICqVQwOnLGtF+9GOCZAu1GH

q9rL2Un3zVRaimdAarZgFUe/dJEmDb2duDSvKqqHipXZR1yZa31fmoQvKW/xcMS2

SM5swpXzK0nhmEssGuQTqUOaeZYL8cxMD5yLIU4=

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

Содержимое openssl.cnf:

[SAN]

subjectAltName = @alt\_names

[alt\_names]

IP.1 = 127.0.0.1

IP.2 = 10.18.18.35

DNS.1 = localhost

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание  
Рисунок 6. Генерируем сертификат X.509 (server.crt) на 365 дней для HTTPS сервера и подписываем его приватным ключом CA (root\_ca.key).

66C3D0547928C572E1DC9505F9FEA38094F67C5F

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

76:c6:83:1e:8f:db:d3:ed:c5:d5:85:38:f5:23:8b:f2:fa:5c:4e:4d

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = RU, ST = Samarskaya oblast, L = Samara, O = Kerasi, OU = Home, CN = LCL, emailAddress = ex@mail.ru

Validity

Not Before: Dec 20 00:30:52 2024 GMT

Not After : Dec 20 00:30:52 2025 GMT

Subject: C = RU, ST = Samarskaya oblast, L = Samara, O = Kerasi, OU = Home, CN = LCL, emailAddress = ex@mail.ru

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c9:22:49:2d:4b:b4:04:c1:28:20:9d:2a:17:57:

4f:ac:0c:05:38:66:39:0f:82:de:57:84:7e:3b:f7:

80:2d:6e:4d:d6:a7:2c:6d:62:d6:e4:d6:1d:8a:14:

63:72:5b:90:aa:7b:94:6a:13:1b:84:b9:f2:e6:ee:

8b:1f:f6:64:e1:b4:1d:35:f6:10:db:d5:96:46:41:

3c:d9:42:b5:a1:9a:77:2e:d7:dd:66:16:2f:f8:b1:

cd:fc:bd:df:34:b3:40:a2:a1:0f:a2:db:7e:0f:fd:

77:4d:51:01:3a:5d:94:37:91:38:9d:02:fe:01:02:

29:f1:f4:20:4d:40:db:1f:fe:64:8f:34:cc:2a:80:

dc:f3:c8:f2:1b:7f:ea:3e:8f:9a:f0:0f:d7:0b:4d:

01:6e:de:34:2d:c3:24:a0:bb:f6:90:be:b6:8c:6a:

6e:bb:ab:90:8c:7b:33:dd:00:fb:94:fb:bc:14:91:

4c:e0:6f:6c:18:dc:34:42:31:0f:19:b2:ad:be:5a:

0d:e9:34:96:f1:eb:03:94:d3:97:ac:ae:b1:fc:94:

e4:68:c2:a5:52:98:91:3f:6e:f5:68:a5:fb:7a:d1:

b6:eb:33:61:b3:7e:34:67:aa:12:a9:72:11:5d:27:

f4:0e:8f:5b:b8:f7:ea:f0:36:2a:03:0b:6e:58:0c:

9f:73

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

70:91:B1:C8:AF:8C:5D:C3:09:7A:3C:D7:56:7C:3C:DB:1C:01:3D:B6

X509v3 Authority Key Identifier:

70:91:B1:C8:AF:8C:5D:C3:09:7A:3C:D7:56:7C:3C:DB:1C:01:3D:B6

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: sha256WithRSAEncryption

Signature Value:

83:1e:99:d9:56:0d:62:87:63:21:e1:c6:4e:fa:28:1f:c4:72:

6d:b8:5c:8a:59:56:2d:e3:68:be:2f:8a:4b:fd:70:a4:db:50:

ae:f0:6e:a6:b2:d6:94:7a:ef:e2:d6:4b:fd:45:1f:04:3d:3b:

df:da:aa:a4:93:67:d8:67:a5:04:d8:f9:c7:54:7b:24:a5:9d:

ef:a3:14:bc:ff:de:86:83:9b:51:81:3b:41:0d:c6:16:5b:1c:

33:ed:71:fc:08:0f:44:f2:7d:7b:62:93:7a:47:b4:63:6d:19:

11:6e:9e:0b:61:55:b5:2a:6c:65:bd:fd:f4:1a:72:cb:46:9e:

4c:9f:c8:56:36:7f:c4:2e:68:72:6e:86:e0:54:e5:dc:17:21:

1c:a3:6f:23:4f:a7:3d:62:05:a1:f7:1f:a3:40:45:b9:91:75:

87:cb:3e:f3:05:00:af:95:f7:27:01:10:3b:9d:0e:91:2a:b4:

26:15:29:b1:3a:0d:7c:30:2c:58:23:d0:2b:fa:4f:b4:2b:18:

18:29:b3:94:44:52:89:07:51:c6:4c:88:e6:63:99:30:c3:ff:

1d:e8:19:9b:2e:12:97:a6:b5:88:fb:78:c5:fc:4f:b1:6e:3f:

5e:f2:1a:34:10:f6:85:84:4e:fa:1c:f5:b6:3e:c1:2f:45:6a:

00:40:af:89

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

MIID6TCCAtGgAwIBAgIUdsaDHo/b0+3F1YU49SOL8vpcTk0wDQYJKoZIhvcNAQEL

BQAwgYMxCzAJBgNVBAYTAlJVMRowGAYDVQQIDBFTYW1hcnNrYXlhIG9ibGFzdDEP

MA0GA1UEBwwGU2FtYXJhMQ8wDQYDVQQKDAZLZXJhc2kxDTALBgNVBAsMBEhvbWUx

DDAKBgNVBAMMA0xDTDEZMBcGCSqGSIb3DQEJARYKZXhAbWFpbC5ydTAeFw0yNDEy

MjAwMDMwNTJaFw0yNTEyMjAwMDMwNTJaMIGDMQswCQYDVQQGEwJSVTEaMBgGA1UE

CAwRU2FtYXJza2F5YSBvYmxhc3QxDzANBgNVBAcMBlNhbWFyYTEPMA0GA1UECgwG

S2VyYXNpMQ0wCwYDVQQLDARIb21lMQwwCgYDVQQDDANMQ0wxGTAXBgkqhkiG9w0B

CQEWCmV4QG1haWwucnUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDJ

IkktS7QEwSggnSoXV0+sDAU4ZjkPgt5XhH4794Atbk3WpyxtYtbk1h2KFGNyW5Cq

e5RqExuEufLm7osf9mThtB019hDb1ZZGQTzZQrWhmncu191mFi/4sc38vd80s0Ci

oQ+i234P/XdNUQE6XZQ3kTidAv4BAinx9CBNQNsf/mSPNMwqgNzzyPIbf+o+j5rw

D9cLTQFu3jQtwySgu/aQvraMam67q5CMezPdAPuU+7wUkUzgb2wY3DRCMQ8Zsq2+

Wg3pNJbx6wOU05esrrH8lORowqVSmJE/bvVopft60bbrM2GzfjRnqhKpchFdJ/QO

j1u49+rwNioDC25YDJ9zAgMBAAGjUzBRMB0GA1UdDgQWBBRwkbHIr4xdwwl6PNdW

fDzbHAE9tjAfBgNVHSMEGDAWgBRwkbHIr4xdwwl6PNdWfDzbHAE9tjAPBgNVHRMB

Af8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCDHpnZVg1ih2Mh4cZO+igfxHJt

uFyKWVYt42i+L4pL/XCk21Cu8G6mstaUeu/i1kv9RR8EPTvf2qqkk2fYZ6UE2PnH

VHskpZ3voxS8/96Gg5tRgTtBDcYWWxwz7XH8CA9E8n17YpN6R7RjbRkRbp4LYVW1

Kmxlvf30GnLLRp5Mn8hWNn/ELmhybobgVOXcFyEco28jT6c9YgWh9x+jQEW5kXWH

yz7zBQCvlfcnARA7nQ6RKrQmFSmxOg18MCxYI9Ar+k+0KxgYKbOURFKJB1HGTIjm

Y5kww/8d6BmbLhKXprWI+3jF/E+xbj9e8ho0EPaFhE76HPW2PsEvRWoAQK+J

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

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание  
Рисунок 7. Самоподписанный корневой сертификат нашего CA (root\_ca.crt) не находится в хранилище доверительных сертификатов

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание  
Рисунок 8. После добавления сертификата, все стало нормально.

Изображение выглядит как снимок экрана, текст, программное обеспечение, компьютер

Автоматически созданное описание  
Рисунок 9. Доступ к серверу через браузер по IP.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание  
Рисунок 10. Доступ к серверу через браузер по доменному имени.

Вывод

В ходе лабораторной работы мы ознакомились с принципами работы инфраструктуры открытых ключей, методами ее работы, хранения ключей и форматом сертификатов X.509. Разрабали консольное приложение, работающее со встроенным в операционную систему хранилищем сертификатов.