Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

По дисциплине «КМЗИ»

Тема: “Сертификаты X.509 и инфраструктура открытых ключей”

Выполнил:

Студент 3 курса

Группы ИИ-21

Кирилович А. А.

Проверила:

Хацкевич А.С.

Брест 2023

Цель:Создать программу, которая создание сертификатов X.509

**C:\D>openssl genpkey -algorithm ED25519 -out root\_keypair.pem -quiet**

**C:\D>openssl pkey -in root\_keypair.pem -noout -text**

ED25519 Private-Key:

priv:

9e:2f:7b:34:61:38:ad:e1:40:39:36:3f:cb:a6:93:

f6:37:3f:98:2c:e4:7f:2c:1d:5c:11:47:04:0f:3d:

42:70

pub:

1d:ed:5c:d8:d1:a8:9c:1a:ac:2e:a0:59:93:11:24:

4a:c1:58:06:96:28:ab:6b:9a:0c:fc:a7:fc:e7:57:

6a:8c

**C:\D>openssl req -new -subj "/CN=Root CA" -addext "basicConstraints=critical,CA:TRUE" -key root\_keypair.pem -out root\_csr.pem**

**C:\D>openssl req -in root\_csr.pem -noout -text**

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = Root CA

Subject Public Key Info:

Public Key Algorithm: ED25519

ED25519 Public-Key:

pub:

1d:ed:5c:d8:d1:a8:9c:1a:ac:2e:a0:59:93:11:24:

4a:c1:58:06:96:28:ab:6b:9a:0c:fc:a7:fc:e7:57:

6a:8c

Attributes:

Requested Extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: ED25519

Signature Value:

9d:11:26:dd:93:03:3e:53:3c:f9:13:7c:46:c0:da:30:25:11:

07:a8:91:8d:06:6e:92:10:e4:d5:5c:ef:d8:81:c7:b8:c9:d8:

13:71:24:ca:6a:a3:1b:da:fd:ba:64:ec:a6:ce:5e:8b:7b:fc:

99:cb:19:aa:48:fa:e5:8a:38:03

**C:\D>openssl x509 -req -in root\_csr.pem -copy\_extensions copyall -signkey root\_keypair.pem -days 7 -out root\_cert.pem**

Certificate request self-signature ok

subject=CN = Root CA

**C:\D>openssl x509 -in root\_cert.pem -noout -text -quiet**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

55:98:b8:0d:3d:7d:c9:d4:67:cb:86:05:d6:84:99:51:52:64:82:19

Signature Algorithm: ED25519

Issuer: CN = Root CA

Validity

Not Before: Nov 21 09:02:56 2023 GMT

Not After : Nov 28 09:02:56 2023 GMT

Subject: CN = Root CA

Subject Public Key Info:

Public Key Algorithm: ED25519

ED25519 Public-Key:

pub:

1d:ed:5c:d8:d1:a8:9c:1a:ac:2e:a0:59:93:11:24:

4a:c1:58:06:96:28:ab:6b:9a:0c:fc:a7:fc:e7:57:

6a:8c

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

09:AC:BF:78:11:E3:1D:CA:A7:2E:7C:EB:F6:45:D0:1D:3C:1E:3E:32

Signature Algorithm: ED25519

Signature Value:

82:76:7b:60:7c:ce:e9:bf:7d:65:55:a5:c4:cc:76:d2:01:3a:

51:d7:c9:79:70:4d:0f:7f:fe:06:75:20:40:81:8d:aa:0c:cd:

b1:12:52:3f:f8:ef:b7:73:c9:6e:cf:7f:f2:6a:33:bf:4d:ee:

4b:d9:2a:b9:7c:c8:00:2b:d4:08

**C:\D>openssl genpkey -algorithm ED25519 -out intermediate\_keypair.pem -quiet**

**C:\D>openssl req -new -subj "/CN=Intermediate CA" -addext "basicConstraints=critical,CA:TRUE" -key intermediate\_keypair.pem -out intermediate\_csr.pem**

**C:\D>openssl x509 -req -in intermediate\_csr.pem -copy\_extensions copyall -CA root\_cert.pem -CAkey root\_keypair.pem -days 7 -out intermediate\_cert.pem**

Certificate request self-signature ok

subject=CN = Intermediate CA

**C:\D>openssl x509 -in intermediate\_cert.pem -noout -text -quiet**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

2e:0d:07:66:8f:24:b5:72:02:cb:ca:c8:0d:a9:28:0c:98:90:54:cd

Signature Algorithm: ED25519

Issuer: CN = Root CA

Validity

Not Before: Nov 21 09:02:56 2023 GMT

Not After : Nov 28 09:02:56 2023 GMT

Subject: CN = Intermediate CA

Subject Public Key Info:

Public Key Algorithm: ED25519

ED25519 Public-Key:

pub:

6c:c1:27:59:1c:67:c4:0e:19:d3:8c:01:66:e9:bf:

0d:d3:a5:01:c4:53:8b:94:45:8b:aa:93:18:cf:cb:

9b:a5

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

C3:75:5F:95:53:A6:A8:7C:03:F9:46:57:EC:61:75:90:E8:1E:65:1A

X509v3 Authority Key Identifier:

09:AC:BF:78:11:E3:1D:CA:A7:2E:7C:EB:F6:45:D0:1D:3C:1E:3E:32

Signature Algorithm: ED25519

Signature Value:

21:7e:6b:68:1b:61:e8:60:ed:a1:a7:4e:a9:a2:2c:55:8b:f8:

06:c3:b4:40:a3:c9:7b:c8:48:94:17:cc:9a:e0:44:aa:3a:69:

96:31:22:5d:53:82:a9:e2:af:81:46:54:82:af:54:33:98:28:

40:6a:3d:01:14:9d:4f:32:7e:0e

**C:\D>openssl genpkey -algorithm ED25519 -out leaf\_keypair.pem -quiet**

**C:\D>openssl req -new -subj "/CN=Leaf" -addext "basicConstraints=critical,CA:FALSE" -key** **leaf\_keypair.pem -out leaf\_csr.pem**

**C:\D>openssl x509 -req -in leaf\_csr.pem -copy\_extensions copyall -CA intermediate\_cert.pem -CAkey intermediate\_keypair.pem -days 7 -out leaf\_cert.pem**

Certificate request self-signature ok

subject=CN = Leaf

**C:\D>openssl x509 -in leaf\_cert.pem -noout -text -quiet**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

53:3f:47:96:50:ed:4d:fb:b1:f1:3d:63:97:57:1f:40:0f:62:61:2b

Signature Algorithm: ED25519

Issuer: CN = Intermediate CA

Validity

Not Before: Nov 21 09:02:57 2023 GMT

Not After : Nov 28 09:02:57 2023 GMT

Subject: CN = Leaf

Subject Public Key Info:

Public Key Algorithm: ED25519

ED25519 Public-Key:

pub:

80:00:9d:e1:c8:e0:de:0d:0a:5e:fa:e1:61:b3:35:

ad:2a:ba:4e:95:2d:68:41:3e:ab:0a:c9:0b:d0:34:

f5:78

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Key Identifier:

C5:82:46:70:F4:36:03:B6:0D:2F:83:84:74:EC:B9:FE:68:8A:36:ED

X509v3 Authority Key Identifier:

C3:75:5F:95:53:A6:A8:7C:03:F9:46:57:EC:61:75:90:E8:1E:65:1A

Signature Algorithm: ED25519

Signature Value:

95:03:f7:a8:c2:66:bf:23:82:26:61:50:70:17:bc:35:96:4f:

55:19:a3:b2:6b:7e:a3:16:25:9f:2e:43:53:f2:1c:70:d5:5c:

46:a5:9e:5a:2f:ca:dc:d1:a6:6a:f4:02:df:09:98:21:2b:ea:

7a:41:78:44:21:7b:f5:72:2b:05

**C:\D>openssl verify -verbose -show\_chain -trusted root\_cert.pem -untrusted intermediate\_cert.pem leaf\_cert.pem**

leaf\_cert.pem: OK

Chain:

depth=0: CN = Leaf (untrusted)

depth=1: CN = Intermediate CA (untrusted)

depth=2: CN = Root CA

Вывод: изучил создание сертификатов X.509 и инфраструктуру открытых ключей.