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-23

Романюк А. П.

Проверила:

Хацкевич А.С.

Брест 2024

Цель:Создать программу, которая создание сертификатов X.509

**D:\progr\github\University\KMZI\II\lab6>openssl genpkey -algorithm ED448 -out root\_keypair.pem**

**D:\progr\github\University\KMZI\II\lab6>openssl pkey -in root\_keypair.pem -noout -text**

ED448 Private-Key:

priv:

c8:c5:c6:60:a3:b4:0b:57:11:b2:9f:7a:d0:3a:65:

79:4a:03:9f:2f:ad:e5:e9:9b:da:27:5b:b6:97:be:

f4:15:01:2e:46:c1:99:51:3b:4b:58:1d:f5:25:1f:

02:63:a5:9a:0f:28:ad:ec:f1:65:b4:ff

pub:

fb:f3:76:a2:2d:ea:c0:fe:20:bb:3f:59:2b:b4:e1:

c2:40:1a:08:54:97:dd:52:f0:99:e0:3a:07:f8:77:

8d:39:6a:79:1f:1a:95:c2:de:54:c4:89:2a:e8:e3

**D:\progr\github\University\KMZI\II\lab6>openssl req -new -subj "/CN=Root CA" -addext "basicConstraints=critical,CA:TRUE" -key root\_keypair.pem -out root\_csr.pem**

**D:\progr\github\University\KMZI\II\lab6>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: ED448

ED448 Public-Key:

pub:

fb:f3:76:a2:2d:ea:c0:fe:20:bb:3f:59:2b:b4:e1:

c2:40:1a:08:54:97:dd:52:f0:99:e0:3a:07:f8:77:

8d:39:6a:79:1f:1a:95:c2:de:54:c4:89:2a:e8:e3:

60:8d:03:19:d6:25:1b:9b:1e:cd:00:80

Attributes:

Requested Extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: ED448

Signature Value:

a1:4c:5e:81:3a:88:f3:cc:6f:8b:86:05:4d:d6:9e:91:f4:53:

a4:50:c5:57:f9:e0:63:37:e3:d0:78:80:06:9a:05:ee:12:5d:

73:a4:8f:94:8b:f6:9e:04:1c:d5:38:2e:ce:34:20:f9:ea:ff:

a7:3a:00:9a:55:02:b8:d2:31:e7:ab:48:15:3b:64:9a:54:b9

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -req -in root\_csr.pem -copy\_extensions copyall -key root\_keypair.pem -days 3650 -out root\_cert.pem**

Certificate request self-signature ok

subject=CN=Root CA

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -in root\_cert.pem -noout -text**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

4c:9c:81:77:4d:0c:3a:f2:7a:2e:4e:72:53:3c:a5:d9:f3:bd:c2:bd

Signature Algorithm: ED448

Issuer: CN=Root CA

Validity

Not Before: Nov 26 11:22:52 2024 GMT

Not After : Nov 24 11:22:52 2034 GMT

Subject: CN=Root CA

Subject Public Key Info:

Public Key Algorithm: ED448

ED448 Public-Key:

pub:

fb:f3:76:a2:2d:ea:c0:fe:20:bb:3f:59:2b:b4:e1:

c2:40:1a:08:54:97:dd:52:f0:99:e0:3a:07:f8:77:

8d:39:6a:79:1f:1a:95:c2:de:54:c4:89:2a:e8:e3:

60:8d:03:19:d6:25:1b:9b:1e:cd:00:80

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

BE:0A:A4:D6:1F:AC:B6:D1:88:F5:E9:62:29:CB:24:B3:29:9E:E7:4C

Signature Algorithm: ED448

Signature Value:

f9:d9:9d:cf:26:94:46:a9:43:f6:18:41:bc:70:b6:16:e6:4a:

44:56:c6:3b:cc:ac:1d:16:55:1c:cf:58:11:b1:2c:0a:37:97

7d:42:ef:a8:e8:65:35:38:86:8a:cf:e7:a9:9a:78:63:96:a5:

2c:b9:2e:20:47:3d:3d:45:21:10:94:96:09:e0:03:dc:78:95:

3a:0a:e8:da:2c:00

**D:\progr\github\University\KMZI\II\lab6>openssl genpkey -algorithm ED448 -out intermediate\_keypair.pem**

**D:\progr\github\University\KMZI\II\lab6>openssl req -new -subj "/CN=Intermediate CA" -addext "basicConstraints=critical,CA:TRUE" -key intermediate\_keypair.pem -out intermediate\_csr.pem**

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -req -in intermediate\_csr.pem -copy\_extensions copyall -CA root\_cert.pem -CAkey root\_keypair.pem -days 3650 -out intermediate\_cert.pem**

Certificate request self-signature ok

subject=CN=Intermediate CA

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -in intermediate\_cert.pem -noout -text**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

a6:24:df:5d:21:98:dc:93:b6:d3:9f:dc:5f:3d:7b:7f:ba:4e:09

Signature Algorithm: ED448

Issuer: CN=Root CA

Validity

Not Before: Nov 26 11:29:00 2024 GMT

Not After : Nov 24 11:29:00 2034 GMT

Subject: CN=Intermediate CA

Subject Public Key Info:

Public Key Algorithm: ED448

ED448 Public-Key:

pub:

8c:6e:e7:31:33:90:53:a6:3f:88:9b:78:c4:4f:17:

86:ef:78:ea:fa:28:65:27:72:17:3e:dc:b0:b3:b5

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Subject Key Identifier:

86:08:E3:FB:CB:F4:09:A7:BA:EA:1A:2C:58:BC:DE:9F:00:10:71:DA

X509v3 Authority Key Identifier:

BE:0A:A4:D6:1F:AC:B6:D1:88:F5:E9:62:29:CB:24:B3:29:9E:E7:4C

Signature Algorithm: ED448

Signature Value:

fd:44:85:ca:6e:26:60:8c:02:ce:9a:2b:c7:fd:c6:54:ec:ba:

90:81:10:5c:e7:16:25:e1:04:db:30:5e:ca:27:46:8a:e9:23:

f4:bb:02:b2:d8:95:28:3e:ba:31:3b:4f:b7:fa:a9:ed:24:1

**D:\progr\github\University\KMZI\II\lab6>openssl genpkey -algorithm ED448 -out leaf\_keypair.pem**

**D:\progr\github\University\KMZI\II\lab6>openssl req -new -subj "/CN=Leaf" -addext "basicConstraints=critical,CA:FALSE" -key leaf\_keypair.pem -out leaf\_csr.pem**

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -req -in leaf\_csr.pem -copy\_extensions copyall -CA intermediate\_cert.pem -CAkey intermediate\_keypair.pem -days 3650 -out leaf\_cert.pem**

Certificate request self-signature ok

subject=CN=Leaf

**D:\progr\github\University\KMZI\II\lab6>openssl x509 -in leaf\_cert.pem -noout -text**

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

35:e7:5c:37:a5:d1:57:fe:dd:d9:9b:2f:6b:9e:87:bd:47:92:fe:a5

Signature Algorithm: ED448

Issuer: CN=Intermediate CA

Validity

Not Before: Nov 26 11:34:55 2024 GMT

Not After : Nov 24 11:34:55 2034 GMT

Subject: CN=Leaf

Subject Public Key Info:

Public Key Algorithm: ED448

ED448 Public-Key:

pub:

7b:eb:c3:11:35:bf:23:f3:00:3e:e1:2d:aa:e0:fb:

a3:42:78:b6:3a:c0:1c:ed:07:3d:c9:b8:f5:5c:07

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:FALSE

X509v3 Subject Key Identifier:

80:D6:FB:45:92:D7:A4:BC:A1:59:C8:08:25:87:F6:43:99:D3:BF:F7

X509v3 Authority Key Identifier:

86:08:E3:FB:CB:F4:09:A7:BA:EA:1A:2C:58:BC:DE:9F:00:10:71:DA

Signature Algorithm: ED448

Signature Value:

81:3a:7a:e6:41:e5:50:d5:19:39:37:8e:7d:5c:41:36:83:b8:

83:2f:75:7f:86:bc:14:99:dc:62:c9:f6:f1:2c:5c:dc:15:c8:

80:93:a5:dc:60:bd:bc:7e:27:89:39:5a:96:62:4a:21:cd

**D:\progr\github\University\KMZI\II\lab6>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.