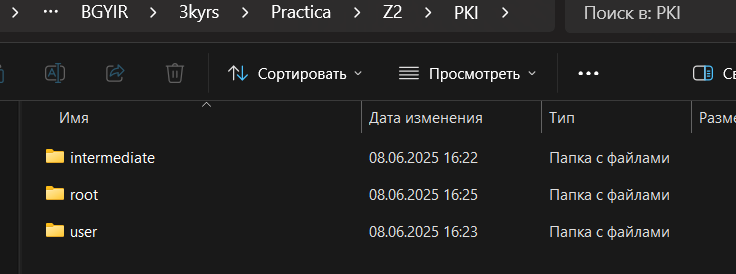
**Шаг 0. Подготовка папок**

основная структура:

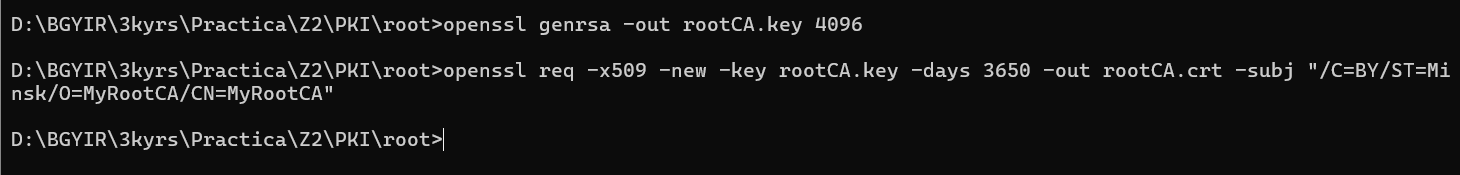
mkdir -p D:\BGYIR\3kyrs\Practica\Z2\PKI\root

mkdir -p D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate

mkdir -p D:\BGYIR\3kyrs\Practica\Z2\PKI\user



**Шаг 1. Создание Корневого удостоверяющего центра (КУЦ)**

****

каталог:

cd D:\BGYIR\3kyrs\Practica\Z2\PKI\root

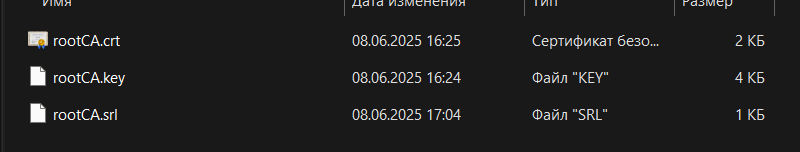
Создание закрытого ключа (4096 бит):

openssl genrsa -out rootCA.key 4096

Создание самоподписанного сертификата (10 лет):

openssl req -x509 -new -key rootCA.key -days 3650 -out rootCA.crt -subj "/C=BY/ST=Minsk/O=MyRootCA/CN=MyRootCA"

* rootCA.key — корневой закрытый ключ (нельзяя раскрывать никому)
* rootCA.crt — доверенный сертификат, которым подпишем УЦ

****

**Шаг 2. Создание Промежуточного удостоверяющего центра (УЦ)**

Создание файла intermediate\_openssl.cnf в папке intermediate со следующим содержанием:

[ req ]

distinguished\_name = req\_distinguished\_name

x509\_extensions = v3\_ca

prompt = no

[ req\_distinguished\_name ]

C = BY

ST = Minsk

O = MyIntermediateCA

CN = IntermediateCA

[ v3\_ca ]

basicConstraints = CA:TRUE

keyUsage = critical, keyCertSign, cRLSign

subjectKeyIdentifier = hash

authorityKeyIdentifier = keyid:always,issuer:always

каталог:

cd D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate

Сгенерирование ключа:

openssl genrsa -out intermediate.key 4096

Сгенерирование заявки на сертификат (CSR):

openssl req -new -key intermediate.key -out intermediate.csr -subj "/C=BY/ST=Minsk/O=MyIntermediateCA/CN=IntermediateCA"

Подписание её корневым центром:

openssl x509 -req -in intermediate.csr ^

-CA D:\BGYIR\3kyrs\Practica\Z2\PKI\root\rootCA.crt ^

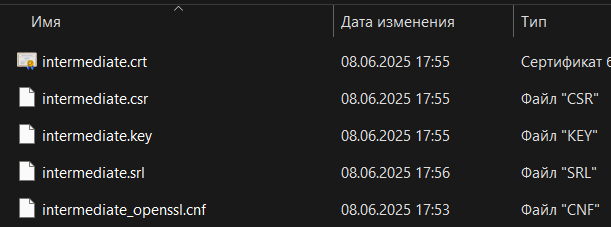
-CAkey D:\BGYIR\3kyrs\Practica\Z2\PKI\root\rootCA.key ^

-CAcreateserial ^

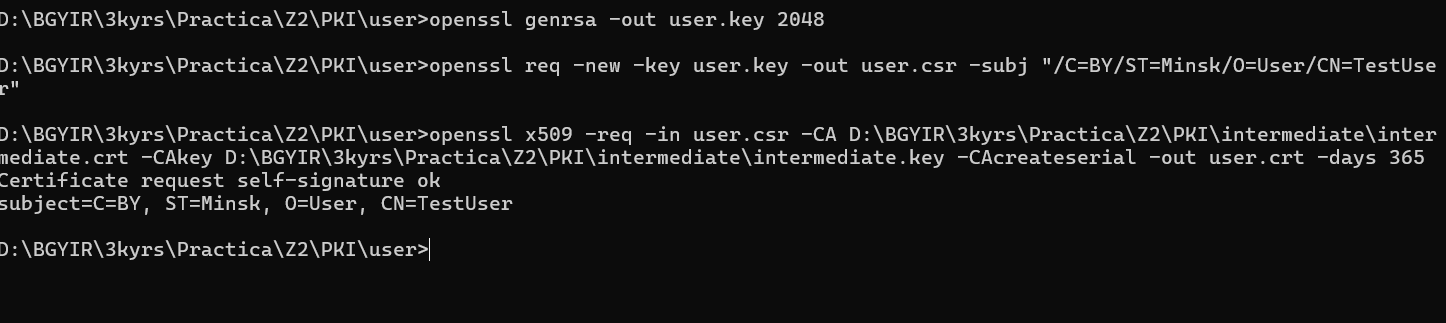
-out intermediate.crt -days 1825 ^

-extfile intermediate\_openssl.cnf -extensions v3\_ca

* intermediate.crt — сертификат промежуточного УЦ, выданный КУЦ
* intermediate.key — ключ УЦ
* intermediate.csr — заявка
* rootCA.srl — сгенерированный серийный номер



**Шаг 3. Создание пользователя (РЦ или клиента)**

****

каталог:

cd D:\BGYIR\3kyrs\Practica\Z2\PKI\user

Сгенерирование закрытого ключа:

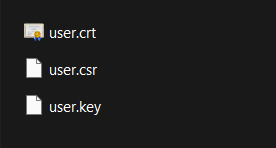
openssl genrsa -out user.key 2048

Сгенерирование заявки на сертификат:

openssl req -new -key user.key -out user.csr -subj "/C=BY/ST=Minsk/O=User/CN=TestUser"

Подписание её промежуточным УЦ:

openssl x509 -req -in user.csr -CA D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate\intermediate.crt -CAkey D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate\intermediate.key -CAcreateserial -out user.crt -days 365

* user.crt — выданный сертификат клиента
* user.key — его ключ
* user.csr — заявка
* intermediate.srl — серийный номер, выданный промежуточным центром
* 

**Проверка цепочки доверия**

Создание файла chain.pem:

type D:\BGYIR\3kyrs\Practica\Z2\PKI\user\user.crt D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate\intermediate.crt D:\BGYIR\3kyrs\Practica\Z2\PKI\root\rootCA.crt > chain.pem

Проверка:

openssl verify -CAfile D:\BGYIR\3kyrs\Practica\Z2\PKI\root\rootCA.crt -untrusted D:\BGYIR\3kyrs\Practica\Z2\PKI\intermediate\intermediate.crt D:\BGYIR\3kyrs\Practica\Z2\PKI\user\user.crt

