

Создание гражданином запроса на выпуск ОУ-сертификата с алгоритмами шифрования ГОСТ

1. Создайте конфигурационный файл `mydomain.cnf` и заполните его согласно примеру:

```
openssl_conf = openssl_init

[ openssl_init ]
stbl_section = stable_section

[ req ]
distinguished_name = req_distinguished_name
req_extensions = v3_req
x509_extensions = v3_req
prompt = no
string_mask = utf8only
utf8 = yes

[ req_distinguished_name ]
CN = mydomain.ru
SN = Иванов
GN = Иван Иванович
C = RU
SNILS = 12345678901
INN = 123456789012

[ v3_req ]
keyUsage = digitalSignature, keyEncipherment, keyAgreement
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = DNS:mydomain.ru
certificatePolicies = 1.2.643.2.25.1.14.2, 1.2.643.100.113.1,
1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4,
1.2.643.100.113.5
subjectSignTool = HSM

[ stable_section ]
SNILS = min:11,max:11,mask:NUMERICSTRING,flags:nomask
INN = min:12,max:12,mask:NUMERICSTRING,flags:nomask
```

2. Замените значения внутри файла на ваши:

- C — двухсимвольный код страны согласно ГОСТ 7.67-2003, для России — RU
- SN — фамилия, указанная в вашем профиле на Госуслугах. Обязательно заполнение русскими буквами. Пример верной записи: Иванов
- GN — имя и отчество, указанные в вашем профиле на Госуслугах. Отчество — при наличии. Обязательно заполнение русскими буквами. Пример верной записи с отчеством: Иван Иванович. Пример верной записи при отсутствии отчества: Иван

- INN — ИНН, указанный в вашем профиле на Госуслугах. Состоит из 12 цифр
 - SNILS — СНИЛС, указанный в вашем профиле на Госуслугах. Состоит из 11 цифр
 - CN — имя домена, на который оформляется TLS-сертификат, например mydomain.ru. Для доменных имён, состоящих из русских букв, укажите значение, конвертированное с помощью [метода punycode](#), например xn--i1afg.xn--d1acufc.xn--p1ai
 - keyUsage — расширение, определяющее назначение ключа. В запросе обязательно должны присутствовать значения digitalSignature, keyEncipherment и keyAgreement, иные не допускаются
 - extendedKeyUsage — расширение, определяющее расширенное назначение ключа. В запросе обязательно должны присутствовать значения serverAuth и clientAuth, иные не допускаются
 - subjectAltName — расширение, определяющее альтернативное имя субъекта — DNS-имя. В запросе обязательно должно быть указано хотя бы одно значение расширения, определяющее альтернативное имя субъекта — DNS-имя, равное указанному в CN. Значения типа WildCard допускаются только образованные от основного доменного имени, указанного в CN (*.mydomain.ru). Допускается до 99 альтернативных имён субъекта. Примеры верных записей: DNS:*.mydomain.ru, DNS:www.mydomain.ru
 - certificatePolicies — политики, в соответствии с которыми должен использоваться сертификат. В запросе обязательно должна быть указана политика 1.2.643.2.25.1.14.2 и любые комбинации политик в зависимости от класса средства криптографической защиты информации (СКЗИ): СКЗИ класса КС1 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1, СКЗИ класса КС2 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1, 1.2.643.100.113.2, СКЗИ класса КС3 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, СКЗИ класса КВ1 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4, СКЗИ класса КВ2 — 1.2.643.2.25.1.14.2, 1.2.643.100.113.1, 1.2.643.100.113.2, 1.2.643.100.113.3, 1.2.643.100.113.4, 1.2.643.100.113.5
 - subjectSignTool — СКЗИ владельца сертификата
3. Установите приложение OpenSSL, пакет gost-engine и откройте командную строку
 4. Для создания запроса в командной строке введите команду: `$ openssl req -out mydomain.p10 -outform DER -new -newkey gost2012_512 -pkeyopt paramset:A -nodes -keyout newkey.key -config mydomain.cnf`
 5. Замените значения внутри команды на ваши:
 - mydomain.p10 — имя файла запроса, который будет создан при выполнении команды из п. 4
 - newkey.key — имя файла закрытого ключа, который будет создан при выполнении команды из п. 4
 - gost2012_512 — алгоритм с длиной закрытого ключа. В команде обязательно должен быть указан любой из алгоритмов: gost2012_256 — соответствует идентификатору id-tc26-gost3410-12-256 для алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256 бит, gost2012_512 — соответствует id-tc26-gost3410-12-512 для алгоритма подписи ГОСТ Р 34.10-2012 с ключом 512 бит

– pkeyopt paramset — набор параметров закрытого ключа. В команде обязательно должен быть указан любой из параметров в зависимости от алгоритма с длиной закрытого ключа: для gost2012_256 — XA, который соответствует id-GostR3410-2001-CryptoPro-XchA-ParamSet, для gost2012_512 — A соответствует id-tc26-gost-3410-12-512-paramSetA, B соответствует id-tc26-gost-3410-12-512-paramSetB

```
administrator@astra:~$ openssl req -out mydomain.p10 -outform DER -new -newkey gost2012_512 -pkeyopt paramset:A -nodes -keyout newkey.key -config mydomain.cnf
Generating a GOST2012_512 private key
writing new private key to 'newkey.key'
-----
```

6. Проверьте созданный запрос с помощью команды: `$ openssl req -in mydomain.p10 -inform DER -noout -text -nameopt utf8 -config mydomain.cnf`

```
administrator@astra:~$ openssl req -in mydomain.p10 -inform DER -noout -text -nameopt utf8 -config mydomain.cnf
Certificate Request:
  Data:
    Version: 1 (0x0)
    Subject: CN=mydomain.ru, SN=Иванов, GN=Иван Иванович, C=RU, SNILS=12345678901, INN=123456789012
    Subject Public Key Info:
      Public Key Algorithm: GOST R 34.10-2012 with 512 bit modulus
```