госуслуги

Создание организацией запроса на выпуск OV-сертификата с алгоритмами шифрования ГОСТ

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

```
openssl_conf = openssl_init

[ openssl_init ]
oid_section = new_oids
stbl_section = stable_section

[ new_oids ]
INNLE = 1.2.643.100.4

[ 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
O = Наименование организации
C = RU
ST = 77 г.Москва
L = г. Москва
streetAddress = ул. Примерная, д. 1
INNLE = 1234567890
OGRN = 1234567890123

[ 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 ]
INNLE = min:10,max:10,mask:NUMERICSTRING,flags:nomask
OGRN = min:13,max:13,mask:NUMERICSTRING,flags:nomask
```

2. Замените значения внутри файла на ваши:

– C — двухсимвольный код страны согласно ГОСТу 7.67-2003, для России — RU

– ST — двухсимвольный код и наименование субъекта РФ по адресу регистрации организации. Допускается заполнение латинскими или русскими буквами. Примеры

верных записей: 55 Murmansk region, 22 Altai Territory, 55 Мурманская область, 22 Алтайский край

– L — наименование населённого пункта по адресу регистрации организации. Допускается заполнение латинскими или русскими буквами. Примеры верных записей: Moscow, г. Москва

– streetAddress — адрес места регистрации организации, включая наименование улицы, номер дома, корпуса, строения, квартиры, помещения. Допускается заполнение латинскими или русскими буквами. Примеры верных записей: Primernaya street, building 1, ул. Примерная, д. 1

– O — официальное название организации. Допускается заполнение латинскими или русскими буквами. Примеры верных записей: Test Organization, Наименование организации

– INNLE — ИНН организации, указанный в её профиле на Госуслугах. Состоит из 10 цифр

– OGRN — ОГРН организации, указанный в её профиле на Госуслугах. Состоит из 13 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--j1ail.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 -newke
y 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, O=Наименование организации, C=RU, ST=77 г.Мо
сква, L=г. Москва, street=ул. Примерная, д. 1, INNLE=1234567890, OGRN=1234567
890123
        Subject Public Key Info:
            Public Key Algorithm: GOST R 34.10-2012 with 512 bit modulus
```