

Установка и настройка OpenSSL для работы с rtengine 0.7.x

ВНИМАНИЕ! Используйте OpenSSL версии 1.1.0 или новее

1. Загрузите модуль интеграции (rtengine) в составе Комплекта разработчика Рутокен с нашего [сайта](#).
2. Загрузите и установите библиотеку PKCS#11 с нашего [сайта](#).
3. Установить OpenSSL 1.1.0 или новее.
4. Модифицируем конфигурационный файл OpenSSL (для Linux: /usr/lib/ssl/openssl.cnf , в Windows файл находится в директории установки OpenSSL). Добавляем следующую информацию в начало файла:

```
openssl_conf = openssl_def
```

и в конец файла:

```
[ openssl_def ]

engines = engine_section

[ engine_section ]

rtengine = gost_section

[ gost_section ]

dynamic_path = /path/to/librtengine.so

MODULE_PATH = /path/to/librtpkcs11ecp.so

RAND_TOKEN = pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP

default_algorithms = CIPHERS, DIGEST, PKEY, RAND
```

dynamic_path — путь до библиотеки rtengine.

MODULE_PATH — путь до библиотеки librtpkcs11ecp.

RAND_TOKEN — идентификатор токена откуда будет браться энтропия (в формате [pkcs11 uri](#).)

Возможные компоненты идентификатора:

```
manufacturer: ID ;

model: ;

serial: ;

token: ( "label").
```

Работа с rtengine без токена



Для того, чтобы шифровать и выписывать ГОСТ сертификаты с помощью rtengine без подключенного Рутокена необходимо:

1. Убрать из конфигурационного файла секцию **RAND_TOKEN**, чтобы энтропия не бралась с Рутокена.
2. Убрать опцию **RAND** из **default_algorithms**.

Для систем на базе Windows все аналогично.

5. Создайте переменную среды OPENSSL_CONF, записав туда путь до конфигурационного файла.

Для Linux, например, выполните, запустив bash :

```
export OPENSSL_CONF=/path/to/openssl.cnf
```

Для Windows, запустив cmd:

```
set OPENSSL_CONF=C:\path\to\openssl.cnf
```

Пример конфигурационного файла OpenSSL

```
#    rtengine

openssl_conf = openssl_def

[ openssl_def ]

engines = engine_section

[ engine_section ]

rtengine = gost_section

[ gost_section ]

dynamic_path = /path/to/librtengine.so

MODULE_PATH = /path/to/librtpkcs11ecp.so

RAND_TOKEN = pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP;serial=2adc8d87

default_algorithms = CIPHERS, DIGEST, PKEY, RAND

#

[ req ]

prompt = no

distinguished_name = req_distinguished_name

req_extensions = ext

#

[ req_distinguished_name ]

countryName = RU

commonName = Ivanov

emailAddress = ivanov@mail.ru

stateOrProvinceName = Moscow

#

[ ext ]

subjectSignTool = ASN1:FORMAT:UTF8,UTF8String: \" 2.0\"

extendedKeyUsage=emailProtection

keyUsage=digitalSignature,nonRepudiation,keyEncipherment,dataEncipherment

#

[ ca ]
```

```
default_ca = CA_default

[ CA_default ]

dir = ./demoCA #

database = $dir/index.txt

new_certs_dir = $dir/newcerts # ,

certificate = $dir/cacert.pem #

serial = $dir/serial

private_key = $dir/private/cakey.pem #

RANDFILE = $dir/private/.rand

default_days = 365 #

default_crl_days = 30

default_md = md_gost12_256 #

policy = policy_any

email_in_dn = no

name_opt = ca_default

cert_opt = ca_default

copy_extensions = copy


#

[ policy_any ]

countryName = supplied

stateOrProvinceName = optional

organizationName = optional

organizationalUnitName = optional

commonName = supplied

emailAddress = optional
```