

АО «СИГНАЛ-КОМ»

ПРОГРАММНЫЙ МОДУЛЬ  
«SIGNAL-COM GOST ENGINE»

Версия 1.2

Руководство системного программиста

ШКНР.00065-01 32 01

Листов 19

## СОДЕРЖАНИЕ

Содержание .....	2
Аннотация.....	3
1. Общие сведения .....	4
1.1. Сокращения .....	4
1.2. Термины и определения .....	4
1.3. Назначение программы .....	5
2. Структура программы .....	6
3. Настройка программы .....	7
3.1. Установка на ОС семейства Linux.....	7
3.2. Установка на ОС семейства Windows.....	8
3.3. Настройка файла конфигурации openssl.cnf.....	8
4. Проверка программы.....	10
4.1. Проверка загрузки модуля .....	10
4.2. Проверка наличия TLS криптонаборов ГОСТ .....	10
5. Примеры использования .....	11
5.1. Генерация ключей .....	11
5.2. Режим сервера TLS .....	11
5.3. Режим клиента TLS.....	12
5.4. Создание электронной подписи CMS .....	12
5.5. Проверка электронной подписи подписи CMS.....	13
5.6. Зашифрование данных по протоколу CMS .....	13
5.7. Расшифрование данных по протоколу CMS .....	14
6. Дополнительные возможности.....	15
7. Сообщения системному программисту .....	16
Литература.....	18

### **АННОТАЦИЯ**

Настоящий документ содержит руководство по установке и настройке программного модуля, предназначенного для интеграции средства криптографической защиты информации «Крипто-КОМ 3.5» и программной библиотеки OpenSSL 3.0.

## **1. ОБЩИЕ СВЕДЕНИЯ**

### **1.1. Сокращения**

В документе использованы следующие сокращения:

ДСЧ – датчик случайных чисел;

ОС – операционная система;

ПО – программное обеспечение;

ППО – прикладное программное обеспечение;

СКЗИ – средство криптографической защиты информации;

УЦ – удостоверяющий центр;

ЭП – электронная подпись;

PSE – personal security environment;

RFC – request for comments.

### **1.2. Термины и определения**

В настоящем руководстве используются следующие термины:

- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- сертификат ключа проверки электронной подписи – документ в электронном виде или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
- средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;
- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;
- электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме

(подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

### **1.3. Назначение программы**

Программный модуль «Signal-COM GOST Engine» предназначен для интеграции средства криптографической защиты информации «Крипто-КОМ 3.5» и программной библиотеки OpenSSL 3.0.

Программный модуль «Signal-COM GOST Engine» позволяет использовать российские алгоритмы электронной подписи и шифрования в криптографических протоколах TLS [12] и CMS [11], реализованных в библиотеке OpenSSL.

Модуль «Signal-COM GOST Engine» взаимодействует с СКЗИ «Крипто-КОМ 3.5», в котором реализованы следующие криптографические стандарты:

- ГОСТ Р 34.10-2012;
- ГОСТ Р 34.11-2012;
- ГОСТ Р 34.12-2015;
- ГОСТ Р 34.13-2015;
- ГОСТ 28147-89.

Модуль «Signal-COM GOST Engine» предназначен для работы в среде операционных систем Windows и Linux.

## **2. СТРУКТУРА ПРОГРАММЫ**

Модуль «Signal-COM GOST Engine» выполнен в виде библиотеки динамической компоновки scgost.dll (для Windows) или разделяемой библиотеки libscgost.so (для Linux).

### 3. НАСТРОЙКА ПРОГРАММЫ

Для установки модуля «Signal-COM GOST Engine» необходимо использовать инсталляционный диск для соответствующей ОС.

Инсталляционный диск содержит следующие каталоги и файлы:

- readme – файл с описанием дистрибутива;
- bin – каталог с бинарными файлами;
- test/gost2012 - каталог с тестовыми ключами и сертификатами;
- test/pse - каталог с тестовым PSE;
- test/config/openssl.cnf – пример файла конфигурации.

#### 3.1. Установка на ОС семейства Linux

Установка модуля «Signal-COM GOST Engine» на ОС семейства Linux выполняется в следующем порядке:

- установить пакет openssl версии не ниже 3.0.0 с помощью системного менеджера установки или путём сборки из исходного кода;
- распаковать архив с дистрибутивом «Signal-COM GOST Engine» в любой каталог;
- скопировать библиотеку libscgost.so в каталог динамических модулей расширения openssl (например, /usr/local/lib64/engines-3);
- распаковать архив с дистрибутивом СКЗИ «Крипто-КОМ 3.5» в любой каталог;
- скопировать библиотеку libccom.so в каталог динамических модулей расширения openssl (например, /usr/local/lib64/engines-3).

Пример сборки из исходного кода на CentOS:

```
yum install perl-IPC-Cmdperl-Test-Simple

cd /usr/src
wget https://www.openssl.org/source/openssl-3.0.7.tar.gz
tar -zxf openssl-3.0.7.tar.gz
rm openssl-3.0.7.tar.gz

cd /usr/src/openssl-3.0.7
./config
make
make test
make install
```

### 3.2. Установка на ОС семейства Windows

Установка модуля «Signal-COM GOST Engine» на ОС семейства Windows выполняется в следующем порядке:

- установить собранные бинарные файлы openssl версии не ниже 3.0.0 из рекомендуемых источников или сборкой из исходного кода.
- распаковать архив с дистрибутивом «Signal-COM GOST Engine» в любой каталог;
- скопировать библиотеку scgost.dll в каталог динамических модулей расширения openssl (например, C:/Program Files/OpenSSL/lib/engines-3);
- распаковать архив с дистрибутивом СКЗИ «Крипто-КОМ 3.5» в любой каталог;
- скопировать библиотеку scom.dll в каталог динамических модулей расширения openssl (например, C:/Program Files/OpenSSL/lib/engines-3).

Рекомендуемые источники для установки бинарных файлов openssl:

- <https://wiki.openssl.org/index.php/Binaries>
- <https://kb.firedaemon.com/support/solutions/articles/4000121705-openssl-3-0-and-1-1-1-binary-distributions-for-microsoft-windows>

Рекомендации по сборке openssl из исходного кода:

- [https://wiki.openssl.org/index.php/Compilation\\_and\\_Installation#Windows](https://wiki.openssl.org/index.php/Compilation_and_Installation#Windows)
- <https://web.archive.org/web/20161123004257/http://developer.covenanteyes.com/building-openssl-for-visual-studio/>

### 3.3. Настройка файла конфигурации openssl.cnf

Для настройки модуля «Signal-COM GOST Engine» необходимо выполнить следующие действия:

Для подключения модуля к openssl добавить в файл конфигурации:

dynamic\_path - путь к модулю в каталоге динамических модулей openssl.

PSE\_PATH – путь к ключевому контейнеру СКЗИ «Крипто-КОМ».

Пример для ОС семейства Linux:

```
openssl_conf = openssl_def
...
```



```
[openssl_def]  
engines = engine_section
```

```
[engine_section]  
scgost = scgost_section
```

```
[scgost_section]  
engine_id = scgost  
dynamic_path = /usr/local/lib64/engines-3/libscgost.so  
PSE_PATH = /home/user/pse  
default_algorithms = ALL
```

#### 4. ПРОВЕРКА ПРОГРАММЫ

Проверка работоспособности модуля «Signal-COM GOST Engine» может быть выполнена следующим образом:

##### 4.1. Проверка загрузки модуля

Выполнить команду:

```
openssl engine
```

При нормальной работе вывод будет содержать:

```
(scgost) Signal-COM GOST engine
```

##### 4.2. Проверка наличия TLS криптонаборов ГОСТ

Выполнить команду:

```
openssl ciphers
```

При нормальной работе вывод будет включать поддерживаемые в протоколе TLS криптонаборы ГОСТ:

```
GOST2012-MAGMA-MAGMAOMAC  
GOST2012-KUZNYECHIK-KUZNYECHIKOMAC  
LEGACY-GOST2012-GOST8912-GOST8912  
IANA-GOST2012-GOST8912-GOST8912
```

## 5. ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

### 5.1. Генерация ключей

Использовать команду openssl:

```
openssl genpkey -algorithm [algorithm_name] -pkeyopt paramset:[paramset_value] -out  
[key_file_name]
```

со следующими значениями опций:

- [algorithm\_name] - название алгоритма из списка:
  - gost2012\_256 - ГОСТ Р 34.10-2012 (256 бит)
  - gost2012\_512 - ГОСТ Р 34.10-2012 (512 бит)
- [paramset\_value] - параметр эллиптической кривой из списка:
  - TCA - tc26\_gost\_3410\_2012\_256\_paramSetA (gost2012\_256)
  - TCB - tc26\_gost\_3410\_2012\_256\_paramSetB (gost2012\_256)
  - TCC - tc26\_gost\_3410\_2012\_256\_paramSetC (gost2012\_256)
  - TCD - tc26\_gost\_3410\_2012\_256\_paramSetD (gost2012\_256)
  - A - tc26\_gost\_3410\_2012\_512\_paramSetA (gost2012\_512)
  - B - tc26\_gost\_3410\_2012\_512\_paramSetB (gost2012\_512)
  - C - tc26\_gost\_3410\_2012\_512\_paramSetC (gost2012\_512)
  - A - GostR3410\_2001\_CryptoPro\_A\_ParamSet (gost2012\_256)
  - B - GostR3410\_2001\_CryptoPro\_B\_ParamSet (gost2012\_256)
  - C - GostR3410\_2001\_CryptoPro\_C\_ParamSet (gost2012\_256)
  - XA - GostR3410\_2001\_CryptoPro\_XchA\_ParamSet (gost2012\_256)
  - XB - GostR3410\_2001\_CryptoPro\_XchB\_ParamSet (gost2012\_256)
- [key\_file\_name] – имя файла со сгенерированным ключом

Пример генерации ключа и создания запроса на сертификат:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCA -out gost_2012_256.key  
openssl req -new -key gost_2012_256.key -out gost_2012_256.pem
```

### 5.2. Режим сервера TLS

Использовать команду openssl:

```
openssl s_server -CAfile [ca_cert_file_name] -key [server_key_file_name] -cert  
[server_cert_file_name] -accept [port] -www -tls1_2
```

со следующими значениями опций:

- [ca\_cert\_file\_name] – имя файла с сертификатом УЦ
- [server\_key\_file\_name] – имя файла с ключем сервера
- [server\_cert\_file\_name] – имя файла с сертификатом сервера
- [port] – порт сервера

Пример сервера TLS:

```
openssl s_server -CAfile test/gost2012/256/cacert.pem -key test/gost2012/256/server.p8 -cert  
test/gost2012/256/server.cer -accept 4433 -www -tls1_2 -security_debug_verbose -msg -  
legacy_renegotiation -client_renegotiation
```

### 5.3. Режим клиента TLS

Использовать команду openssl:

```
openssl s_client -connect [ip_address]:[port] -CAfile [ca_cert_file_name] -key  
[client_key_file_name] -cert [client_cert_file_name] -tls1_2 -cipher [cipher_suite_name]
```

со следующими значениями опций:

- [ip\_address] – IP адрес сервера
- [port] – порт сервера
- [ca\_cert\_file\_name] – имя файла с сертификатом УЦ
- [client\_key\_file\_name] – имя файла с ключем клиента
- [client\_cert\_file\_name] – имя файла с сертификатом клиента
- [cipher\_suite\_name] – имя криптонабора из списка:
  - GOST2012-MAGMA-MAGMAOMAC
  - GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
  - LEGACY-GOST2012-GOST8912-GOST8912
  - IANA-GOST2012-GOST8912-GOST8912

Пример клиента TLS:

```
openssl s_client -connect 127.0.0.1:4433 -CAfile test/gost2012/256/cacert.pem -key  
test/gost2012/256/client.p8 -cert test/gost2012/256/client.cer -security_debug_verbose -msg -  
tls1_2 -cipher GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
```

### 5.4. Создание электронной подписи CMS

Использовать команду openssl:

```
openssl cms -sign -binary -in [file_name] -out [sgn_file_name] -signer [sgn_cert_file_name] -  
inkey [sgn_key_file_name]
```

со следующими значениями опций:

- [file\_name] – имя файла с данными для подписания
- [sgn\_file\_name] – имя файла с подписанными данными

- [sgn\_cert\_file\_name] – имя файла с сертификатом подписания
- [sgn\_key\_file\_name] – имя файла с ключом подписания

Пример подписания:

```
openssl cms -sign -binary -in data -out msg-sgn-256.txt -signer test/gost2012/256/client.cer -inkey test/gost2012/256/client.p8
```

## 5.5. Проверка электронной подписи подписи CMS

Использовать команду openssl:

```
openssl cms -verify -binary -CAfile [ca_cert_file_name] -in [sgn_file_name] -out [verify_file_name] -signer [sgn_cert_file_name] -purpose any
```

со следующими значениями опций:

- [ca\_cert\_file\_name] – имя файла с сертификатом УЦ
- [sgn\_file\_name] – имя файла с подписанными данными
- [verify\_file\_name] – имя файла с данными после проверки подписи
- [sgn\_cert\_file\_name] – имя файла с сертификатом подписания

Пример проверки подписи:

```
openssl cms -verify -binary -CAfile test/gost2012/256/cacert.pem -in msg-sgn-256.txt -out msg-sgnverify-256.txt -signer test/gost2012/256/client.cer -purpose any
```

## 5.6. Зашифрование данных по протоколу CMS

Использовать команду openssl:

```
openssl cms -encrypt -outform DER -[enc_algorithm_name] -in [file_name] -out [enc_file_name] -recip [enc_cert_file_name]
```

со следующими значениями опций:

- [enc\_algorithm\_name] – имя алгоритма шифрования из списка:
  - magma-ctr-ascpkm - ГОСТ Р 34.12-2015 (шифр «Магма») в режиме CTR-АСРКМ
  - magma-ctr-ascpkm-омас - ГОСТ Р 34.12-2015 (шифр «Магма») в режиме CTR-АСРКМ-ОМАС
  - kuznyechik-ctr-ascpkm - ГОСТ Р 34.12-2015 (шифр «Кузнечик») в режиме CTR-АСРКМ
  - kuznyechik-ctr-ascpkm-омас - ГОСТ Р 34.12-2015 (шифр «Кузнечик») в режиме CTR-АСРКМ-ОМАС
  - gost89 - ГОСТ 28147-89 в режиме гаммирования с обратной связью
- [file\_name] – имя файла с данными для зашифрования
- [enc\_file\_name] – имя файла с зашифрованными данными

- [enc\_cert\_file\_name] – имя файла с сертификатом получателя

Пример зашифрования:

```
openssl cms -encrypt -outform DER -kuznyechik-ctr-acpkm-omac -in data -out msg-enc-256-kuz-ctracpkm-omac.txt -recip test/gost2012/256/client.cer
```

## 5.7. Расшифрование данных по протоколу CMS

Использовать команду openssl:

```
openssl cms -decrypt -binary -inform DER -in [enc_file_name] -out [dec_file_name] -recip [enc_cert_file_name] -inkey [enc_key_file_name]
```

со следующими значениями опций:

- [enc\_file\_name] – имя файла с зашифрованными данными
- [dec\_file\_name] – имя файла с расшифрованными данными
- [enc\_cert\_file\_name] – имя файла с сертификатом получателя
- [enc\_key\_file\_name] – имя файла с закрытым ключом получателя

Пример расшифрования:

```
openssl cms -decrypt -binary -inform DER -in msg-enc-256-kuz-ctracpkm-omac.txt -out msg-dec-256-kuz-ctracpkm-omac.txt -recip test/gost2012/256/client.cer -inkey test/gost2012/256/client.p8
```

## **6. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ**

Полный список команд openssl приведен в документации

<https://www.openssl.org/docs/man3.0/man1/>

## 7. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

При использовании модуля «Signal-COM GOST Engine» системному программисту в консоль (стандартный поток вывода) могут выводиться следующие сообщения:

- "bad key parameters format" – неправильный формат параметров ключа
- "bad mac" – неправильный MAC
- "bad order" – неправильный порядок
- "bad pkey parameters format" – неправильный формат параметров закрытого ключа
- "cannot pack ephemeral key" – невозможно упаковать эфемерный ключ
- "cannot unpack ephemeral key" – невозможно распаковать эфемерный ключ
- "cipher not found" – реализация алгоритма шифрования не найдена
- "ctrl call failed" – ошибка в управляющей функции обратного вызова
- "error computing export keys" – ошибка вычисления экспортируемых ключей
- "error computing shared key" – ошибка вычисления общего ключа
- "error parsing key transport info" – ошибка представления информации транспорта ключа
- "error point mul" – ошибка умножения точки эллиптической кривой
- "incompatible algorithms" – несовместимые алгоритмы
- "incompatible peer key" – несовместимый открытый ключ
- "invalid cipher" – неправильный алгоритм шифрования
- "invalid cipher params" – неправильные параметры алгоритма шифрования
- "invalid cipher param oid" – неправильный идентификатор параметров алгоритма шифрования шифра
- "invalid digest type" – неправильный тип дайджеста
- "invalid iv length" – неправильная длина вектора инициализации
- "invalid mac key length" – неправильная длина ключа MAC
- "invalid mac key size" – неправильная длина ключа MAC
- "invalid mac params" – неправильные параметры вычисления MAC
- "invalid mac size" – неправильный размер MAC
- "invalid paramset" – неправильный набор параметров эллиптической кривой
- "key is not initialized" – ключ не инициализирован
- "key parameters missing" – отсутствуют параметры ключа



"mac key not set" – не задан ключ вычисления MAC

"no parameters set" – не заданы параметры ключа

"no peer key" – отсутствует открытый ключ

"public key undefined" – не задан открытый ключ

"rng error" – ошибка ДСЧ

"signature mismatch" – подпись не действительна

"ukm not set" – не задан ключевой материал пользователя

"unsupported cipher ctl command" – команда управления алгоритма шифрования не поддерживается

"unsupported parameter set" – набор параметров не поддерживается

### ЛИТЕРАТУРА

1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
3. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры, 2015.
4. ГОСТ Р 34.13-2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, 2015.
5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
6. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008.
7. ITU-T Recommendation X.509, «Information Technology - Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks», August 2005.
8. D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008.
9. PKCS #8: Private-Key Information Syntax Standard. Version 1.2, November 1993.
10. Р 1323565.1.023-2018 «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509», Рекомендации по стандартизации, 2018.
11. Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений,

защищенных криптографическими методами», Рекомендации по стандартизации, 2019.

12. Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)», Рекомендации по стандартизации, 2020.
13. МР 26.2.002-2018. «Параметры эллиптических кривых для криптографических алгоритмов и протоколов». Методические рекомендации ТК 26, 2018.
14. СКЗИ «Крипто-КОМ 3.5». Формуляр. ШКНР.00064-01 30 01.
15. СКЗИ «Крипто-КОМ 3.5». Правила пользования. ШКНР.00064-01 90 02.
16. СКЗИ «Крипто-КОМ 3.5». Подсистема управления ключевой информацией. Общее описание. ШКНР.00064-01 31 01.