Инструкция
по изготовлению ключевой информации с использованием средства криптографической защиты информации «Модуль генерации ключей - 3»

В настоящем документе описана процедура по изготовлению ключевой информации с использованием средства криптографической защиты информации «Модуль генерации ключей - 3».

Содержание

Обозначения и сокращения

Сокращение	Расшифровка сокращения
МГК	Модуль генерации ключей
ОМНИ	Отчуждаемый машинный носитель информации
ПЭВМ	Персональная электронно-вычислительная машина
СКЗИ	Средство криптографической защиты информации
ТШ КБР	Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России
УЦ	Управляющий центр на базе СКЗИ «СКАД Сигнатура»

Термины и определения

Термин	Определение
Ключевая информация	Закрытые и открытые ключи, ключи шифрования, ключи ЭП, сертификаты ключей и другая вспомогательная технологическая информация, необходимая для обеспечения процессов изготовления, эксплуатации и управления криптографическими ключами

1. Общие сведения

В настоящем документе приведено описание генерации закрытого ключа и запроса на получение сертификата с использованием средства криптографической защиты информации «Модуль генерации ключей - 3». СКЗИ «МГК-3» распространяется Банком России совместно с СКЗИ «DiSec-W».

Клиент Банка России руководствуется нормативными документами Банка России и эксплуатационной документацией на СКЗИ при работе с ключевой информацией.

2. Установка СКЗИ «МГК-3»

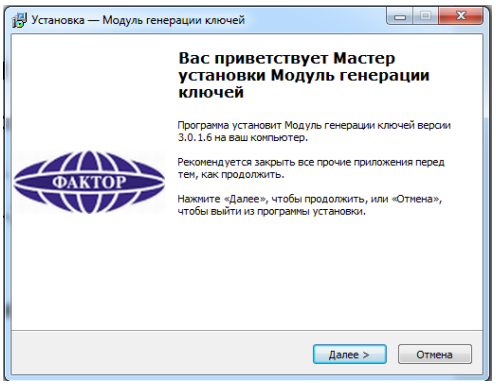
Установка СКЗИ «Модуль генерации ключей «МГК-3»» выполняется на отдельную ПЭВМ, соответствующую требованиям документа «Правила пользования» из состава дистрибутивного комплекта СКЗИ «МГК-3».

Для инсталляции СКЗИ «МГК-3» пользователь должен обладать правами администратора ОС Windows.

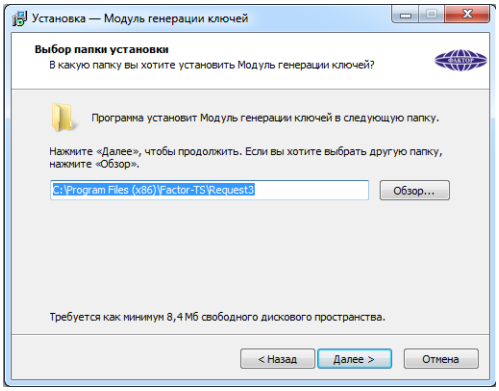
Установка СКЗИ «МГК-3» осуществляется путем запуска файла инсталляции ..\КС1-2\setup.exe, находящегося на установочном диске из состава дистрибутивного пакета.

В ходе установки инсталлятор потребует повышение прав, необходимо нажать «ОК».

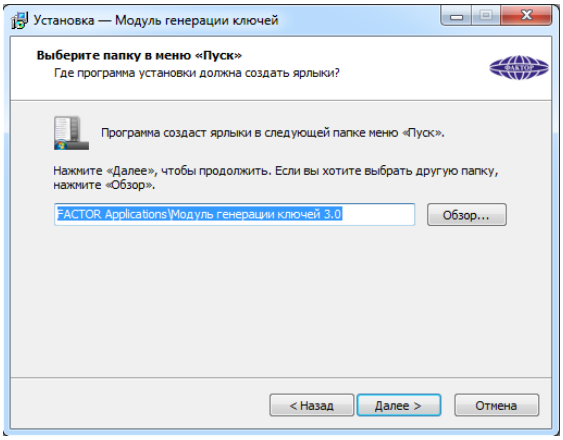
Для продолжения установки нажать «Далее».



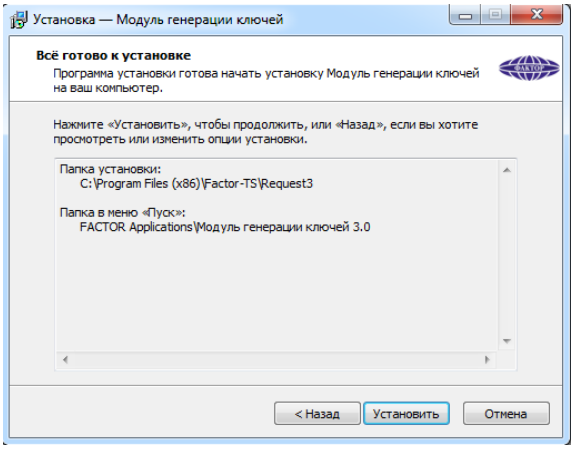
Путь установки, не изменять. Для продолжения установки нажать «Далее».



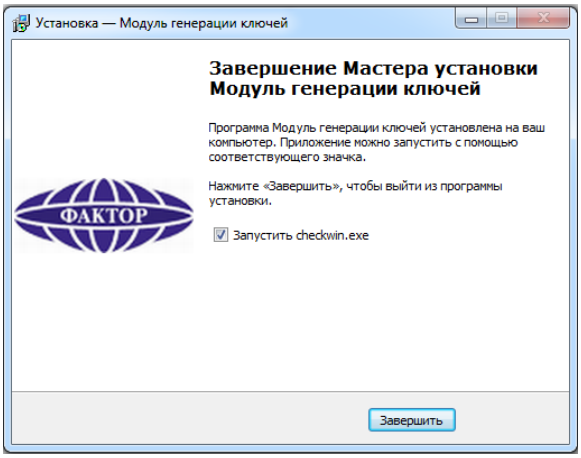
Для продолжения установки необходимо нажать «Далее».



Для продолжения установки нажать «Установить».

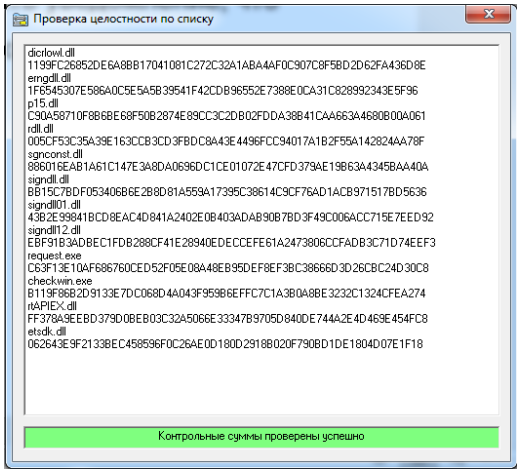


Для продолжения установки нажать «Завершить».



Если программа установилась корректно, в окне «Проверка целостности по списку» будет выдано уведомление «Контрольные суммы проверены успешно».

Установка СКЗИ «МГК-3» выполнена. Для завершения необходимо закрыть окно нажав красный крест в верхнем правом углу.

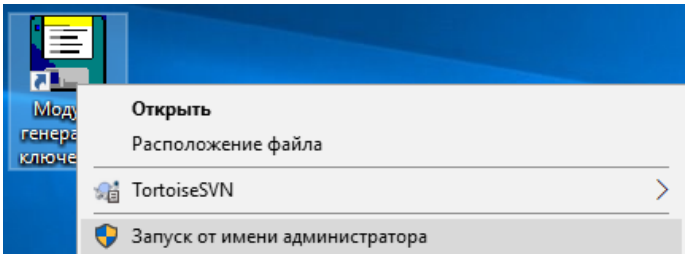


Если будет обнаружено несовпадение, то программа укажет файл, для которого имеет место ошибка контрольной суммы. В этом случае требуется обязательная замена программного обеспечения.

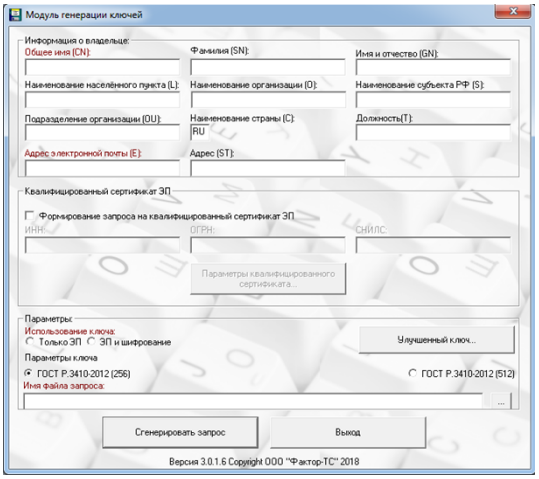
3 Настройка СКЗИ «МГК-3»

Первый запуск СКЗИ «МГК-3» должен выполняться от имени администратора.

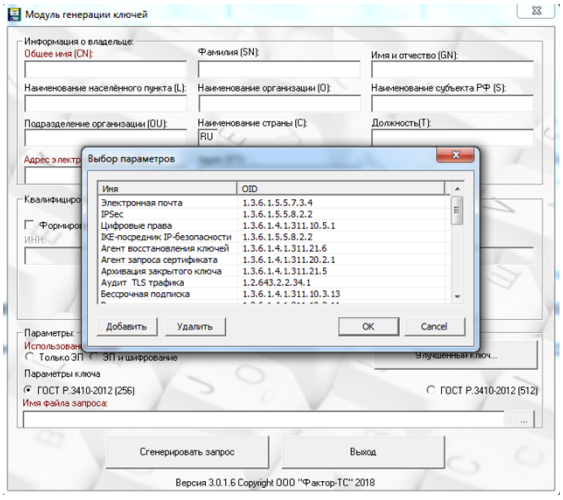
Нажать правой кнопкой мыши по ярлыку и выбрать «*Запуск от имени администратора*».



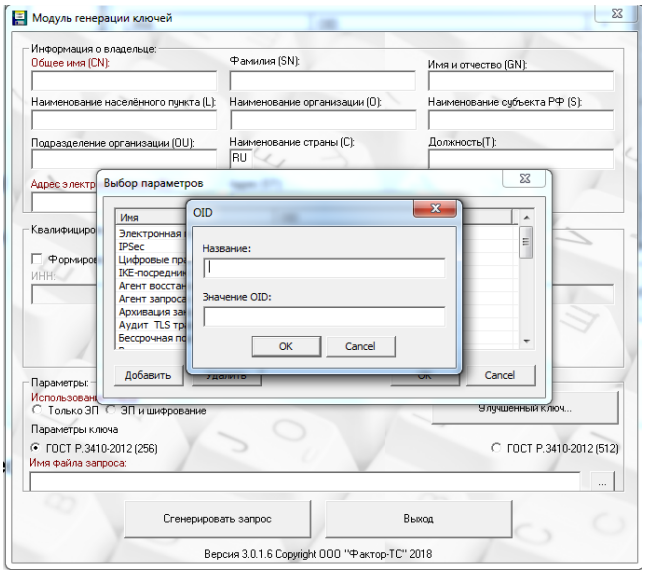
После запуска программы на экран будет выведено главное окно «Модуль генерации ключей» с формой, содержащей поля, необходимые для заполнения при формировании ключей и запросов на сертификаты.



Нажать на кнопку «Улучшенный ключ». После этого откроется дополнительное окно.

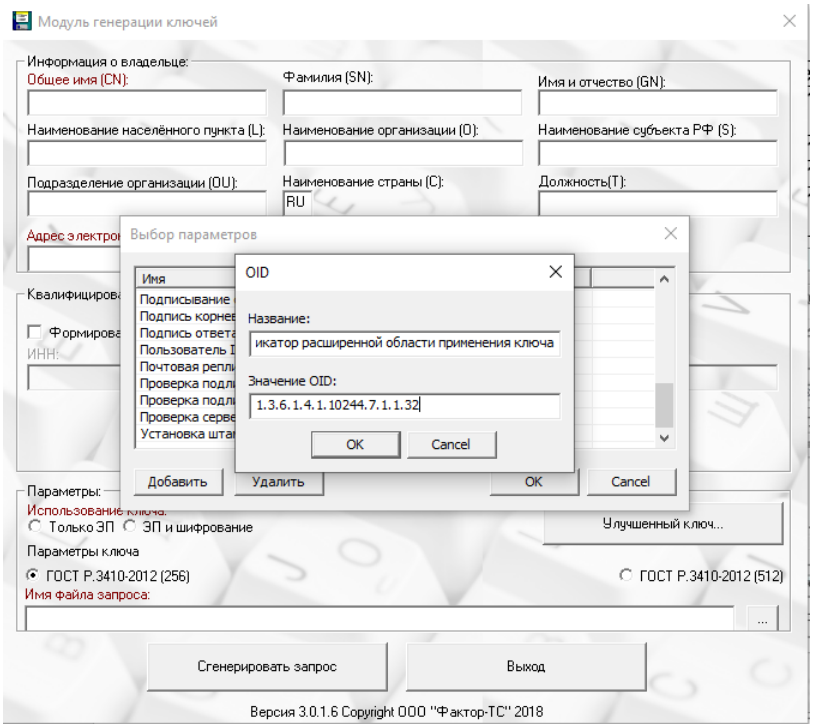


Нажать кнопку «Добавить».

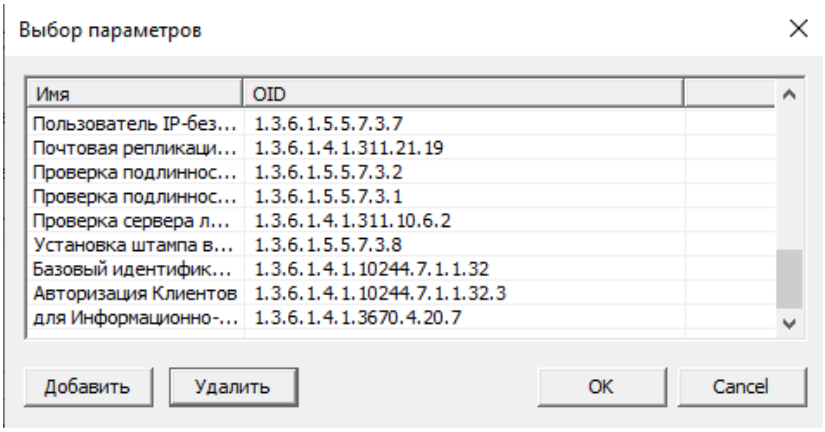


Заполнить поля OID следующими значениями:

Название (Имя)	Значение OID
Базовый идентификатор расширенной области применения ключа	1.3.6.1.4.1.10244.7.1.1.32
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3
Авторизация АРМ КПКИ	1.3.6.1.4.1.10244.7.1.1.32.5
для Информационно-аналитических и статистических систем Банка России	1.3.6.1.4.1.3670.4.20.7
IKE-посредник IP-безопасности	1.3.6.1.5.5.8.2.2



По окончании добавления всех OID необходимо убедиться, что добавление OID выполнено успешно.

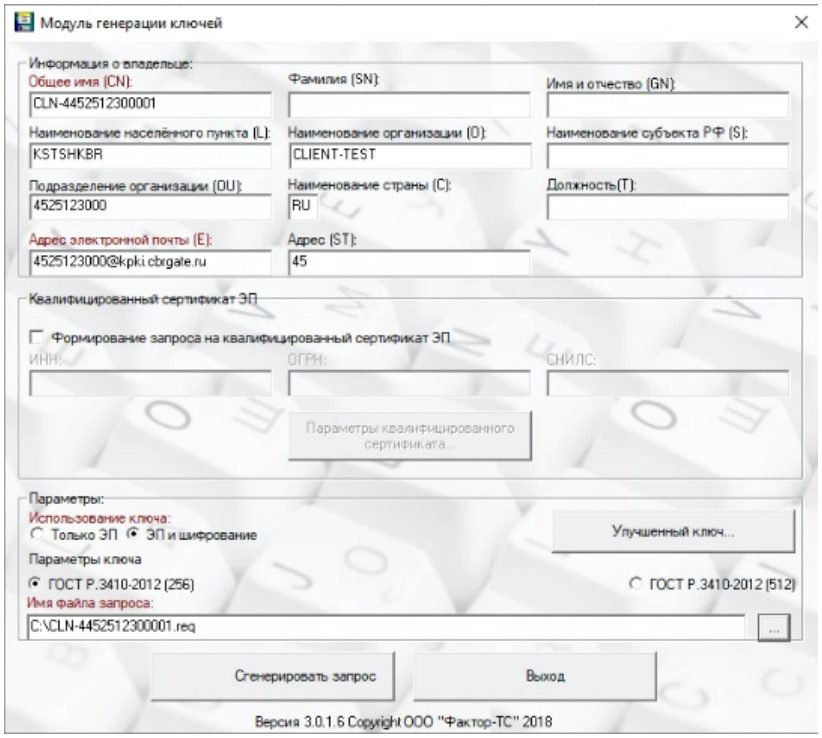


Дополнительные OID добавлены. Нажать кнопку «Cancel».

4. Изготовление ключевой информации

В качестве ключевого носителя для хранения закрытого ключа допускается применять любой носитель, разрешенный к использованию в соответствии с эксплуатационной документацией на СКЗИ «МГК-3».

Для генерации закрытого ключа и запроса на получение сертификата, требуется заполнить поля согласно данным, полученным из Банка России. Пример заполнения полей приведен ниже.

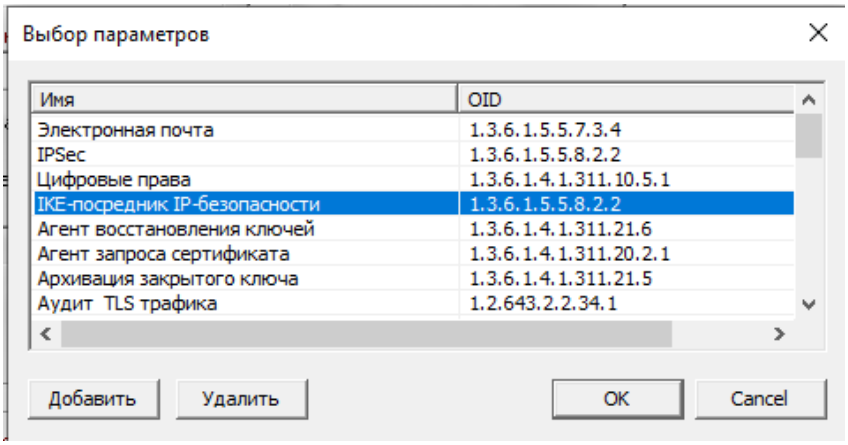


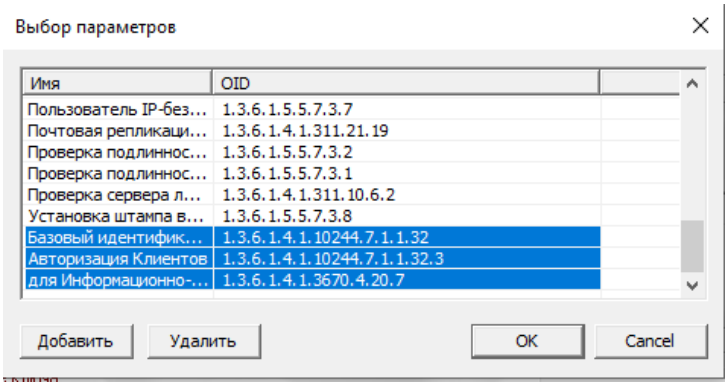
В поле «Использование ключа» выбрать «ЭП и Шифрование».

Нажать  и указать место сохранения расположение файла запрос.

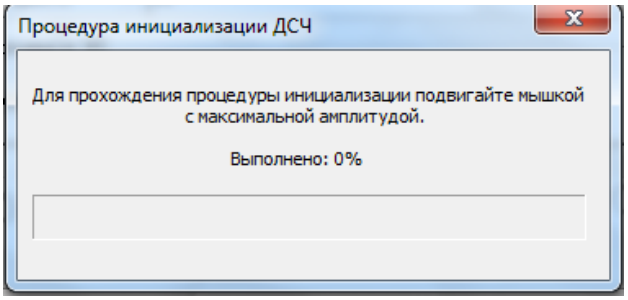
Нажать на кнопку «Улучшенный ключ» и с помощью зажатой кнопки «CTRL» и левой кнопки мыши выбрать следующие пять OID и нажать «ОК»:

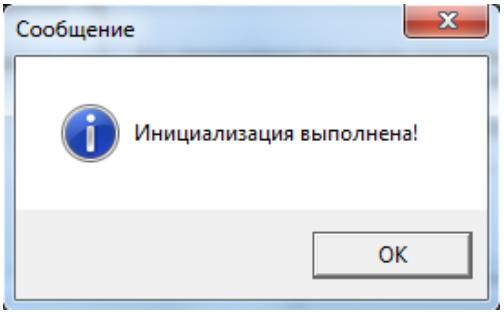
Название (Имя)	Значение OID
Базовый идентификатор расширенной области применения ключа	1.3.6.1.4.1.10244.7.1.1.32
Авторизация Клиентов	1.3.6.1.4.1.10244.7.1.1.32.3
Авторизация АРМ КПКИ	1.3.6.1.4.1.10244.7.1.1.32.5
для Информационно-аналитических и статистических систем Банка России	1.3.6.1.4.1.3670.4.20.7
IKE-посредник IP-безопасности	1.3.6.1.5.5.8.2.2





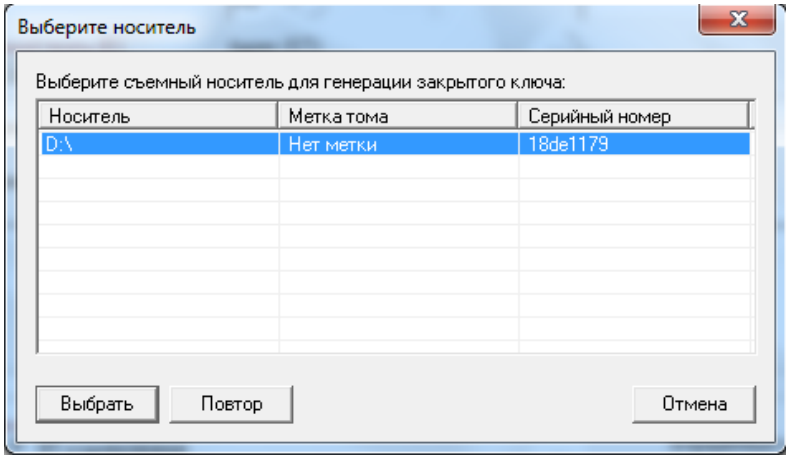
Нажать кнопку «Сгенерировать запрос». После нажатия появится генератор датчика случайных чисел (ДСЧ), где следует с максимальной амплитудой водить мышкой от края до края монитора для его заполнения.





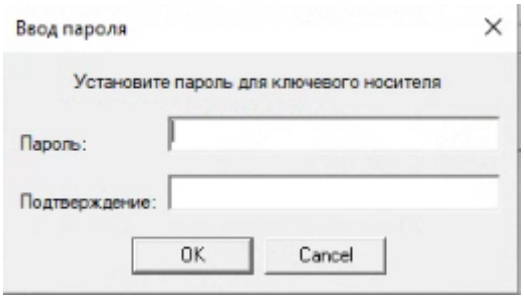
Следует указать ОМНИ, на который будет выполнена загрузка закрытого ключа.

При использовании в качестве ключевого носителя USB-flash выбрать носитель для сохранения закрытого ключа, нажать кнопку «Выбрать».

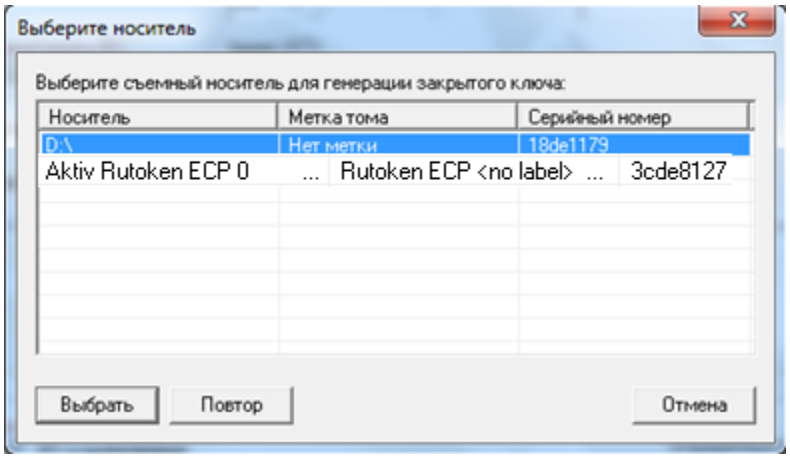


Будет предложено вести пароль для закрытого ключа.

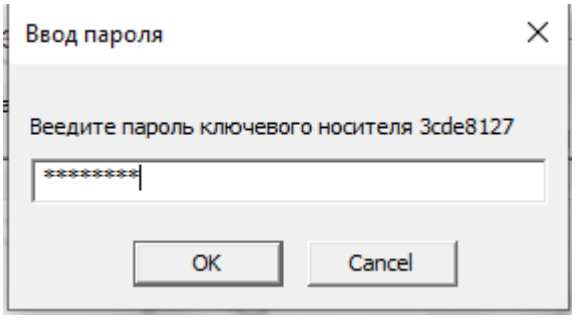
ВНИМАНИЕ! Поле «Пароль» необходимо оставить пустым и нажать кнопку «ОК».



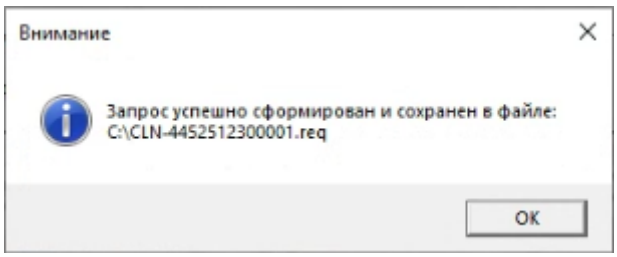
При использовании в качестве ключевого носителя Rutoken (полный перечень разрешенных ключевых носителей приведён в документации на СКЗИ «DiSec-W») выбрать носитель для сохранения закрытого ключа, нажать кнопку «Выбрать».



После этого будет предложено вести пароль для Rutoken. После ввода пароля следует нажать кнопку «Ок».



По окончании будет выдано сообщение об успешном завершении.

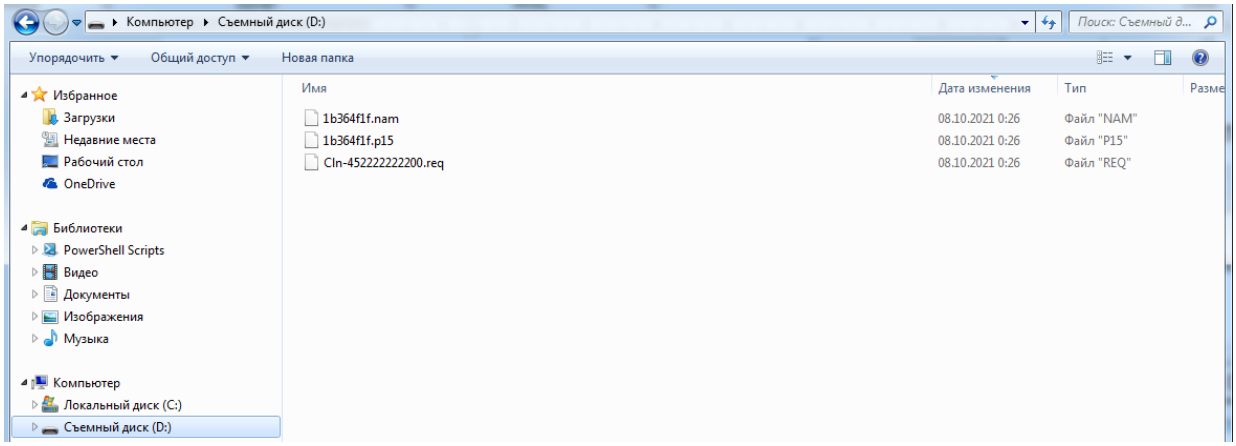


По окончании на съемном носителе будут лежать 3 файла, где:

– Файл с расширением *.nam — это отпечаток работы программы МГК;

– Файл с расширением *. p15 – это закрытый ключ;

– Файл с расширением *.req – это запрос на выдачу сертификата.



Далее файл с расширением *.req необходимо отправить в регистрационный центр Банка России.

После генерации запроса на выдачу сертификата с помощью СКЗИ «МГК-3» файл *.req будет иметь следующее:

```
Subject:
    E=cln-452222222200@kpki.cbrgate.ru
    OU=4522222222
    O=CLIENT-TEST
    STREET=45
    L=KSTSHKBR
    C=RU
    CN=CLN-452222222200
…….
    Enhanced Key Usage
        IP security IKE intermediate (1.3.6.1.5.5.8.2.2)
        Unknown Key Usage (1.3.6.1.4.1.3670.4.20.7)
        Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32)
        Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.1)
```

ВНИМАНИЕ! Поле ST в СКЗИ «МГК-3» в файле *.req будет иметь поле STREET.

5. Распечатка запроса на выдачу сертификата

Для распечатки запроса необходимо выполнить следующее:

1) Открыть командную строчку с помощью команды cmd;
2) Набрать команду C:\>certutil.exe <имя запроса>.req >> %USERPROFILE%\Desktop\<имя запроса>.txt

   Для примера команда может выглядеть следующим образом:

   C:\>certutil.exe CLN-4452512300001.req >> %USERPROFILE%\Desktop\ CLN-4452512300001.txt.

   После выполнения команды на рабочем столе будет создан файл CLN-4452512300001.txt.
3) Содержимое файла CLN-4452512300001.txt использовать для оформления распечатки запроса на выдачу сертификата.

Пример запроса на выпуск сертификата ключа проверки электронной подписи

```
PKCS10 Certificate Request:
Version: 1
Subject:
    E=cln-4525555000@kpki.cbrgate.ru
    OU=4525555000
    O=CLIENT-TEST
    STREET=45
    L=KSTSHKBR
    C=RU
    CN=CLN-452555500002
  Name Hash(sha1): 9e8ecf78626ae864f52802c43c785d89bf698b76
  Name Hash(md5): 91d38b6b9b7bbb556d94e07a36f50b84
Public Key Algorithm:
    Algorithm ObjectId: 1.2.643.7.1.1.1.1
    Algorithm Parameters:
    0000  30 13 06 07 2a 85 03 02  02 23 01 06 08 2a 85 03
    0010  07 01 01 02 02
        1.2.643.2.2.35.1
        1.2.643.7.1.1.2.2
Public Key Length: 0 bits
Public Key: UnusedBits = 0
    0000  04 40 38 b9 81 d1 7a 23  30 61 f0 a8 3c 21 dc 4c
    0010  ba 90 31 62 d2 16 d4 ff  87 58 3d d2 b1 51 4c 88
    0020  ff 11 2c c5 2d 86 72 54  12 7c e9 55 a1 ee 13 bf
    0030  44 99 14 71 34 bb a5 c6  9b 9f 78 bd 5a f7 51 bb
    0040  6f da
Request Attributes: 1
  1 attributes:
  Attribute[0]: 1.3.6.1.4.1.311.2.1.14 (Certificate Extensions)
    Value[0][0], Length = 41
Certificate Extensions: 2
    2.5.29.15: Flags = 1(Critical), Length = 4
    Key Usage
        Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
    2.5.29.37: Flags = 0, Length = 26
    Enhanced Key Usage
        IP security IKE intermediate (1.3.6.1.5.5.8.2.2)
        Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32)
        Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.3)
        Unknown Key Usage (1.3.6.1.4.1.10244.7.1.1.32.5)
        Unknown Key Usage (1.3.6.1.4.1.3670.4.20.7)
Signature Algorithm:
    Algorithm ObjectId: 1.2.643.7.1.1.3.2
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  cc d5 f2 b6 bd b0 2d 9d  d4 d1 8c bc fd 6d 33 f1
    0010  03 3f 44 da 44 98 2d e6  29 54 5f 58 79 73 14 75
    0020  8f da 73 fa ab 5e b7 80  72 59 fe bc 02 8a 48 e6
    0030  65 ff 33 8e 17 26 08 d3  1d 1c cb 50 f0 2d c7 f9
Signature does not match Public key: 80070032
```

Ответственный за ключ: _____ / _____ /

Руководитель организации/центра _____ / _____ /

или его заместитель

М.П.