КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-05 34 06 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 4.0

Программа генерации ключей mkkey. Руководство по использованию

СЕИУ.00009-05 34 06
Листов 13

Литера О

2022

Аннотация

Настоящий документ содержит руководство по использованию программы mkkey из состава «МагПро КриптоПакет» 4.0.

Содержание

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа mkkey из комплекта «МагПро КриптоПакет» 4.0 выполняет создание закрытых ключей для использования в программном комплексе «МагПро КриптоПакет» 4.0, в том числе создание ключей на аппаратных носителях.

Программа позволяет создавать ключи на устройстве «Вьюга», в файловой системе устройства «Рутокен», а также в неизвлекаемой памяти любого сертифицированного устройства, предоставляющего интерфейс PKCS#11 («Рутокен ЭЦП», «JaCarta» и др.).

Программа не формирует заявки на получение сертификата. Для формирования заявок необходимо использовать команду req утилиты openssl.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 УСЛОВИЯ РАБОТЫ ПРОГРАММЫ

Для запроса пароля к ключевому контейнеру и сообщения пользователю о необходимых действиях с аппаратными устройствами программа использует текстовый интерфейс.

Задание режимов работы (например, параметры алгоритмов и набор генерируемых ключей) выполняется с помощью опций командной строки.

Программа предназначена для работы в следующих операционных системах:

Windows 8.1/10;
Windows Server 2012/2016/2019;
Debian GNU/Linux 9(stretch)/10(buster)/11(bullseye);
Ubuntu 14.04, 16.04, 18.04, 20.04;
Linux Mint 19.x, 20.x, Linux Mint Debian Edition 4;
RedHat Enterprise Linux 7, 8;
CentOS 7, 8;
SUSE Linux 12, 15;
OpenSUSE 15.1, 15.2;
EMIAS OS 1.0, 2.0;
Дистрибутивы Альт на базе платформ 8 и 9, включая Альт Сервер, Альт Рабочая станция, Альт Рабочая станция К, Альт Образование, Альт 8 СП, Sipmly Linux;
МСВСфера Сервер 7.3, МСВСфера АРМ 7.3;
Гослинукс IC6;
РЕД ОС 7.2, 7.3;
Rosa Enterprise Desktop (RED) X4;
Rosa Enterprise Linux Server (RELS) 7.3;
Rosa Enterprise Linux Desktop (RELD) 7.3;
РОСА КОБАЛЬТ;
Astra Linux Special Edition Смоленск 1.6 aka исп.1, 1.7;
Astra Linux Special Edition Новороссийск;
Astra Linux Common Edition 2.12;
Numa Edge 1.0;
FreeBSD 12.x, 13.x;
MacOS 10.15, 11;
Sun Solaris 10, 11;
OpenWRT 19.07, 21.02.

Для хранения закрыты ключей могу использоваться

- файловая система компьютера;
- любой аппаратный ключевой носитель, предоставляющий интерфейс PKCS#11 («Рутокен ЭЦП», «JaCarta» и им подобные);
- устройство «Рутокен» с хранением ключей в файловой системе токена;
- устройсво «Вьюга».

В будущем может быть добавлена поддержка и других устройств.

Из-за ошибки в системных библиотеках возможны проблемы с созданием ключей на аппаратных токенах в операционных системах SUSE Linux, ROSA RED и Альт.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 ФУНКЦИИ ПРОГРАММЫ

Программа предоставляет удобный пользовательский интерфейс для выполнения операций по созданию закрытых ключей и ключей подписи и их записи на ключевой носитель, а также формирования файла инициализации программного датчика случайных чисел.

Программа не выполняет указанные операции самостоятельно, а лишь обеспечивает взаимодействие с пользователем. Для формирования ключей вызывается утилита openssl.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 4.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 4.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 4.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Правила пользования» (СЕИУ.00009–05 94).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

Программа устанавливается и настраивается автоматически при установке утилиты openssl (см. «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-05 34 03).

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

6 ИСПОЛЬЗОВАНИЕ ПРОГРАММЫ

6.1 Формат запуска программы

Формат запуска программы:

```
mkkey [опции]
```

По умолчанию (если не указаны опции) программа выводит краткую справку об опциях.

6.2 Опции

```
-V                - отобразить номер версии программы
-a                - алгоритм ключа, по умолчанию gost2012_256
-n                - не шифровать ключ
-p <параметр>     - набор параметров для ключа (умолчание - A)
-w <имя файла>    - файл, в который будет записан закрытый ключ
-t <носитель>     - записать ключ(и) на носитель указанного типа
                    поддерживаются носители: VJUGA, RUTOKEN, PKCS11

Только для носителя VJUGA:
 -s <параметр>  - набор параметров для ключа подписи (умолчание - A)
 -x <параметр>  - набор параметров для ключа шифрования (умолчание - XA)

Только для носителя RUTOKEN:
 -k <id>        - идентификатор ключа
 -P             - защищать ключ PIN-кодом

Только для носителей PKCS11:
 -k <id>        - идентификатор ключа
```

6.3 Выбор алгоритма

Программа mkkey предоставляет возможность создания ключей подписи и обмена для алгоритма ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 (последний - только для целей совместимости с предыдущими версиями).

6.4 Ввод пароля

Для отказа от зашифрования ключевых контейнеров на пароле необходимо при запуске программы указать опцию -n.

Если опция -n при запуске программы не была указана, перед инициализацией ДСЧ программа требует дважды ввести пароль для защиты ключевых контейнеров длиной от 6 до 32 символов.

Для отмены ввода пароля следует ввести пустой пароль, т.е. нажать Enter, не вводя никаких символов.

В пароле могут быть использованы как символы ASCII, так и русские буквы. Русские буквы интерпретируются как имеющие кодировку UTF-8, что соответствует рекомендациям PKCS#5.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Следует обратить внимание, что OpenSSL и большая часть приложений, её использующих, не производит никаких преобразований кодировки пароля. Поэтому ключи, защищенные паролем, состоящим из русских букв, могут быть использованы с командно-строчной утилитой openssl и большинством приложений библиотеки OpenSSL только при запуске последних в локали UTF-8.

6.5 Создание контейнеров на аппаратном носителе

6.5.1 Выбор аппаратного носителя

Ключевые контейнеры на аппаратных носителях создаются в тех случаях, если указана опция -t со значением VJUGA, RUTOKEN или PKCS11. Запись ключевых контейнеров производится на соответствующее устройство.

Не предполагается работа с несколькими устройствами одного типа одновременно.

6.5.2 Создание ключей на устройстве «Вьюга»

Устройство «Вьюга» позволяет хранить только два ключа и только длины 256 бит (хранение ключей для алгоритма ГОСТ Р 34.10-2012 512 бит на устройстве «Вьюга» не поддерживается).

При создании ключей на устройстве «Вьюга» всегда создаётся два ключа - ключ подписи и ключ шифрования. По умолчанию эти ключи имеют параметры шифрования A и XA. Альтернативные параметры могут быть указаны с помощью опций -s и -x, например:

```
mkkey -t VJUGA -s C -x XB
```

6.5.3 Создание ключей в файловой системе устройства «Рутокен»

Устройство «Рутокен» позволяет хранить несколько ключей в пределах доступной памяти устройства. Каждому ключу назначается идентификатор – десятичное число в интервале от 1 до 65535, этот идентификатор выбирается пользователем при создании ключа и указывается в параметре -k, например:

```
mkkey -t RUTOKEN -k 20
```

В этом случае будет создан ключ с идентификатором 20, при дальнейшей работе с этим ключом (например, с помощью утилиты openssl) следует использовать его спецификацию: RUTOKEN:20

Если на токене уже имеется ключ с указанным идентификатором, вновь созданный ключ заменит старый.

Для защиты ключа PIN-кодом следует использовать опцию -P. В этом случае для чтения ключа с устройства будет требоваться ввод PIN-кода пользователя.

6.5.4 Создание ключей в неизвлекаемой памяти устройства с интерфейсом PKCS#11

Программа позволяет создавать ключи в неизвлекаемой памяти любого устройства с интерфейсом PKCS#11 («Рутокен ЭЦП», «JaCarta» и пр.), однако в системе должна быть установлена библиотека, предоставляющая интерфейс PKCS#11 для конкретного устройства (поставляется вместе с устройством), а для того, чтобы программа нашла эту библиотеку, должна быть установлена переменная окружения `PKCS11_LIBNAME`, значением которой должен быть полный путь к этой библиотеке (допустимо указывать только короткое имя библиотеки, если библиотека может быть найдена по стандартным алгоритмам операционной системы). Для устройства «Рутокен ЭЦП» переменную окружения можно не выставлять.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Каждому ключу назначается идентификатор, этот идентификатор выбирается пользователем при создании ключа и указывается в параметре -k, например:

```
mkkey -t PKCS11 -k 20
```

В этом случае будет создан ключ с идентификатором 20, при дальнейшей работе с этим ключом (например, с помощью утилиты openssl) следует использовать его спецификацию: RUTOKEN:20

Если на токене уже имеется ключ с указанным идентификатором, вновь созданный ключ заменит старый.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

7 СОЗДАНИЕ ЗАЯВОК НА ПОЛУЧЕНИЕ СЕРТИФИКАТА

7.1 Краткие сведения о команде *req* утилиты openssl

Программа mkkey создает только закрытый ключ.

Для получения сертификата на соответствующий открытый ключ необходимо сформировать заявку на ключ с помощью команды *req* утилиты openssl.

Внимание. На каждый ключ создаётся отдельная заявка.

Команда *req* позволяет вводить информацию, которая должна содержаться в заявке, с клавиатуры, либо считывать её из конфигурационного файла.

Если в полях сертификата должны присутствовать русские буквы, вводить информацию с клавиатуры следует в кодировке utf-8.

Формат вызова команды *req* при использовании PKCS#8-контейнеров (содержащихся в файлах):

```
openssl req -new [-config файл-конфигурации] -key файл-pkcs8\
 -out имя-файла-заявки
```

Формат вызова команды *req* при использовании аппаратного контейнера:

```
openssl req -new [-config файл-конфигурации] -key спецификация-ключа \
 -keyform ENGINE -engine cryptocom -out имя-файла-заявки
```

Спецификация ключа, хранящегося в аппаратном контейнере, может быть одной из перечисленных:

Ключ подписи на устройстве Вьюга:

```
VJUGA.S
```

Ключ шифрования на устройстве Вьюга:

```
VJUGA.X
```

Ключ в файловой системе устройства «Рутокен» с идентификатором <id>:

```
RUTOKEN:<id>
```

Ключ в неизвлекаемой памяти устройства PKCS#11 с идентификатором <id>:

```
PKCS11:<id>
```

Более подробная информация по ключам команды *req* приведена в документе «Средство криптографической защиты информации «МагПро КриптоПакет» 4.0. Утилита openssl. Руководство по использованию», СЕИУ.00009-05 34 03.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения