КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-03 34 06 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
МагПро КриптоПакет вер. 2.1

Программа создания закрытых ключей mkkey.
Руководство оператора

СЕИУ.00009-03 34 06
Листов 10

Литера О

2015

Инв.№ подл.	Подп. и дата	Взам. инв.№	Инв. № дубл.	Подп. и дата

Аннотация

Настоящий документ содержит руководство оператора для работы с программой mkkey из состава СКЗИ «МагПро КриптоПакет».

Содержание

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

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

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

Поддерживатюся аппаратные носители Вьюга, Rutoken S, Rutoken ЭЦП.

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

Программа также может создавать файл начального заполнения датчика случайных чисел, необходимый в случае использования программного ДСЧ.

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

2 УСЛОВИЯ РАБОТЫ ПРОГРАММЫ

Программа mkkey предназначена для работы в следующих операционных системах:

Windows XP/Vista/7
Windows Server 2003/2008 Debian GNU/Linux lenny/squeeze/wheezy;
Ubuntu 8.04, 10.04, 12.04;
AltLinux 5.0, 6.0, ИВК-Кольчуга;
Red Hat Enterprise Linux 4, 5, 6;
CentOS 4, 5, 6;
Fedora 17;
МСВСфера 5.2, 5.4;
SUSE Linux 10, 11;
Mandriva PowerPack 2008.1, 2009.1, 2010.1, 2010.2, 2011.1, Mandriva Flash 2008.1, 2009.1, 2010.1, 2010.2, 2011.1, Mandriva Corporate Server 4 update 3, Server 5;
FreeBSD 7.x, 8.x, 9.x, а также версия на основе OpenSSL 1.0.0;
Sun Solaris 9, 10, а также версия на основе OpenSSL 1.0.0.

Для инициализации клавиатурного ДСЧ, 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.

Ключевые контейнеры на аппаратных устройствах создаются и защищаются средствами криптоядра «МагПро».

Ключевые контейнеры в PKCS#8-файлах шифруются алгоритмом ГОСТ 28147-89 в режиме гаммирования с обратной связью, ключом, полученным из пароля с помощью алгоритма PBKDF PKCS-5 v.2. При выводе ключа из пароля используется HMAC ГОСТ Р 34.11-94.

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

3 ЗАПУСК ПРОГРАММЫ

3.1 Формат запуска программы

Формат запуска программы:

```
mkkey [опции]
```

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

3.2 Опции

```
-V              - отобразить номер версии программы
-r [имя файла] - запись файла инициализации программного ДСЧ
                  если имя файла не указано, будет использован файл
  /home/abra/.magprocryptopack/random_seed

-a              - алгоритм ключа, по умолчанию GOST2001
-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
-y              - удалить ключ(и) с аппаратного носителя
-c <имя файла> - использовать файл конфигурации openssl
-K <имя файла> - использовать ключ из указанного файла (DER-формат)

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 <номер>     - идентификационный номер ключа
 -P             - защищать ключ PIN-кодом
 -l             - отобразить список ключей на токене
```

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

4 ВЫПОЛНЕНИЕ ПРОГРАММЫ

4.1 Выбор алгоритма

Программа mkkey предоставляет возможность создания ключей подписи и обмена для алгоритма ГОСТ Р 34.10-2001 (gost2001).

4.2 Выбор файла заполнения ДСЧ

При создании ключей с использованием клавиатурного ДСЧ программа выполняет инициализацию файла начального заполнения ДСЧ, что позволяет дальнейшую эксплуатацию OpenSSL с выбранным ДСЧ.

Если в момент запуска программы не указан параметр опции -r, то создается файл начального заполнения с умолчательным именем:

В ОС Windows — `%APPDATA%\MagProCryptoPack\random_seed`

В POSIX-системах — `$HOME/.magprocryptopack/random_seed`

В случае использования клавиатурного ДСЧ также возможно явное указание имени файла заполнения. Имя файла заполнения указывается в качестве значения параметра -r.

4.3 Инициализация ДСЧ

В случае использования клавиатурного датчика случайных чисел программа предлагает пользователю последовательно вводить с клавиатуры указанные символы: заглавные и строчные латинские буквы и цифры. Для ввода заглавных букв используйте клавишу Shift. В начале каждой строки приглашения ввода символов в скобках выводится количество введенных символов и общее количество требуемых символов, разделенных косой чертой. В случае некорректного ввода количество требуемых символов увеличивается.

4.4 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-ти символов 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. 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.

4.5 Создание контейнеров на аппаратном носителе

4.5.1 Выбор аппаратного носителя

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

Не предполагается работа с несколькими устройствами одного типа одновременно.

Для удаления ключей с аппаратного носителя необходимо указать тип носителя (опция -t) и опцию -y. Для носителя RUTOKEN дополнительно требуется указать идентификационный номер ключа, который должен быть удален.

4.5.2 Работа с ключами на устройстве Вьюга

Устройство Вьюга позволяет хранить только два ключа.

При создании ключей на устройстве Вьюга вседа создается 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
```

Для удаления ключей с устройства Вьюга следует использовать опцию -y. Память устройства очищается полностью, т.е. удаляются оба ключа.

```
mkkey -t VJUGA -y
```

4.5.3 Работа с ключами на устройстве Rutoken

Устройство Rutoken позволяет хранить несколько ключей в пределах доступной памяти устройства. Каждому ключу назначается десятичное число в интервале от 1 до 65535 - идентификационный номер. При создании ключа требуется указать идентификационный номер, который будет назначен создаваемому ключу, 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.S

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.

Для просмотра ключей, записанных на токен, используется опция -l:

```
mkkey -t RUTOKEN -l
```

Для удаления ключа с токена слеудет использовать опцию -y, указав при этом идентификатор ключа, например:

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

5 СОЗДАНИЕ ЗАЯВОК НА ПОЛУЧЕНИЕ СЕРТИФИКАТА

5.1 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 создается 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 на устройстве Rutoken с идентификатором <номер>:

```
RUTOKEN:<номер>.S
```

Более подробная информация по ключам команды *req* приведена в соответствующей странице руководства по программе openssl.

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