КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-04 31 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 3.0

Описание применения

СЕИУ.00009-04 31
Листов 13

Литера О

2018

Аннотация

Настоящий документ содержит общее описание программного комплекса «МагПро КриптоПакет» 3.0.

Содержание

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

1 НАЗНАЧЕНИЕ СКЗИ МАГПРО КРИПТОПАКЕТ

Основное назначение СКЗИ «МагПро КриптоПакет» 3.0 — обеспечение криптографической защиты информации при сетевом взаимодействии. СКЗИ позволяет защищать как конкретные соединения, такие как подключение к веб-серверу или RDP-соединение (эту задачу решают исполнения №№ 5 и 6), так и сетевой трафик целиком путем организации виртуальной частной сети (исполнения №№ 7 и 8). Исполнения №№ 3 и 4 позволяют также организовать криптографическую защиту (шифрование, подпись, имитозащита) на уровне отдельных файлов.

Исполнения №№ 1 и 2 обеспечивают возможность использования российских криптоалгоритмов при работе с приложениями, рассчитанными на использование библиотеки OpenSSL, такими как

- www–сервер Apache
- Почтовые сервера Postfix и Dovecot
- Сервер каталогов OpenLDAP
- Текстовый веб-браузер lynx
- Интерпретатор tcltls
- Утилита wget
- Почтовые программы mutt и pine
- Программа мгновенных сообщений jabberd
- и др.

Однако следует иметь ввиду, что для этих приложений необходимо проведение отдельных сертификационных испытаний.

Также СКЗИ во всех исполнениях обеспечивает возможность управления ключевой системой: создания криптографических ключей и выпуск сертификатов для целей использования прочими компонентами СКЗИ.

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

2 УСЛОВИЯ РАБОТЫ СКЗИ «МАГПРО КРИПТОПАКЕТ»

«МагПро КриптоПакет» 3.0 поставляется в собранном виде для работы на аппаратных платформах Intel (архитектуры x86 и x86_64) и UltraSparc в операционных системах:

Windows 7 SP1/8.1/10;
Windows Server 2008R2 SP1/2012/2012R2/2016
Debian GNU/Linux 7(wheezy)/8(jessie)/stretch;
Linux Mint 17.x, 18.x, Linux Mint Debian Edition 2
Ubuntu 14.04, 16.04;
RedHat Enterprise Linux 6, 7;
CentOS 6, 7;
SUSE Linux 11, 12;
OpenSUSE 42.2, 42.3;
OS EMIAS 1.0;
Альт Линукс 6, 7, 8;
МСВСфера Сервер 6.3, МСВСфера АРМ 6.3;
Атликс 3.1;
Гослинукс ІС4;
FreeBSD 10.x, 11.x;
Oracle Solaris 10, 11;
MacOS 10.12;
Rosa Enterprise Desktop (RED) X2, X3;
Rosa Enterprise Linux Server (RELS) 6, 7; РОСА КОБАЛЬТ 1.0;
Astra Linux Special Edition РУСБ.10015-07.

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

3 Обеспечение информационной безопасности при использовании «МагПро КриптоПакет» 3.0

Надежная криптографическая защита данных при использовании «МагПро КриптоПакет» 3.0 обеспечивается только в том случае, если эксплуатация «МагПро КриптоПакет» 3.0 осуществляется в строгом соответствии с требованиями документа «Средство криптографической защиты информации «МагПро КриптоПакет» 3.0. Правила пользования» (СЕИУ.СЕИУ.00009–04 94).

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

4 ПОДДЕРЖИВАЕМЫЕ АЛГОРИТМЫ ГОСТ И СТАНДАРТЫ ПО ИХ ИСПОЛЬЗОВАНИЮ

«МагПро КриптоПакет» 3.0 реализует криптографические алгоритмы, соответствующие российским стандартам ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 (последние два используются для совместимости с предыдущими версиями «МагПро КриптоПакет»), а также рекомендациям по стандартизации «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».

Наборы параметров для этих алгоритмов соответствуют рекомендациям по стандартизации «Информационная технология. Криптографическая защита информации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89» и «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов», а также RFC 4357 (для совместимости с предыдущими версиями).

Поддерживаемые форматы закрытых ключей соответствуют рекомендация по стандартизации «Информационная технология. Криптографическая защита информации. Контейнер хранения ключей» и «Информационная технология. Криптографическая защита информации. Транспортный ключевой контейнер».

Сертификаты и списки отзывов реализованы в соответствии с RFC 5280 и технической спецификацией «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 3411 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509»

Поддерживаемые форматы защищенных сообщений соответствуют RFC 5751, использование российских алгоритмов в этих форматах соответствует рекомендациям по стандартизации «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 И ГОСТ Р 34.10 в криптографических сообщениях формата CMS».

Протокол TLS реализован в соответствии с RFC 2246, 4346, 5246 и рекомендациями по стандартизации «Информационная технология. Криптографическая защита информации. Использование набором алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».

Протокол OCSP реализован в соответствии с RFC 6960.

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

5 СОСТАВ СКЗИ МАГПРО КРИПТОПАКЕТ

СКЗИ «МагПро КриптоПакет» 3.0 может поставляться в 8 исполнениях.

В состав исполнений №№ 1 и 2 входят криптографические библиотеки

- Библиотека реализации базовых криптографических функций форматов X509 и PKCS#7 libcrypto (для ОС Windows – libeay32.dll);
- Библиотека реализации протокола TLS libssl (для ОС Windows – ssleay32.dll);
- Библиотека реализации алгоритмов ГОСТ libcryptocom (для ОС Windows – cryptocom.dll).

В состав исполнений № 3 (соответствует классу КС1) и № 4 (соответствует классу КС2) дополнительно входит

- Утилита openssl, реализующая доступ к основной функциональности библиотек из командной строки.

В состав исполнений № 5 (соответствует классу КС1) и № 6 (соответствует классу КС2) дополнительно входит

- Средство защиты доступа к сетевым ресурсам «КриптоТуннель» (исполнения №№ 5 и 6).

В состав исполнений № 7 (соответствует классу КС1) и № 8 (соответствует классу КС2) дополнительно входит

- Виртуальная частная сеть «OpenVPN-ГОСТ» (исполнения №№ 7 и 8).

Кроме того, в состав всех исполнений входят:

- Программа создания файла инициализации программного ДСЧ mkseed и программа создания ключей mkkey;
- Средство контроля целостности integrity и программа расчета хэш-сумм gost12sum);
- Скрипты для управления сертификатами и заявками.

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

6 СОВМЕСТИМОСТЬ МАГПРО КРИПТОПАКЕТ И OPENSSL

«МагПро КриптоПакет» 3.0 полностью совместим с OpenSSL 1.0.2.

Для использования российских алгоритмов необходимо подгрузить библиотеку libcryptocom (в случае ОС Windows – cryptocom.dll) с помощью конфигурационного файла или с помощью средств конфигурирования приложения, если оно не считывает конфигурационный файл OpenSSL.

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

7 УПРАВЛЕНИЕ КЛЮЧАМИ В «МагПро КриптоПакет» 3.0

7.1 Создание ключей

1. Создать ключи для нужного алгоритма ГОСТ. Это можно сделать двумя способами:
   – с помощью команды **genpkey** утилиты `openssl`;
   – с помощью программы **mkkey**, входящей в состав СКЗИ.
   Оба варианта позволяют использовать как аппаратный, так и программный датчик случайных чисел, однако если ключи создаются с помощью команды **genpkey** утилиты `openssl` с использованием программного датчика случайных чисел, этот датчик должен быть предварительно проинициализирован программной **mkseed**.
2. Сформировать заявку на регистрацию ключей с помощью команды req утилиты openssl.
3. Отправить заявку в удостоверяющий центр и получить сертификат на ключ.

7.2 Использование ключей при работе с приложениями

1. Использовать ключи в соответствии с требованиями приложений.
2. При выполнении операций электронной подписи явно указывать используемые алгоритмы не нужно, так как алгоритм подписи определяется по сертификату, а алгоритм хэширования однозначно определяется алгоритмом подписи.
   При выполнении операций зашифрования, как правило требуется явное указание алгоритма шифрования gost89.
3. При конфигурировании сервера TLS необходимо явное указание криптонабора GOST2012-GOST8912-GOST8912 или GOST2001-GOST89-GOST89 (последний – только для совместимости со старыми версиями).

7.3 Окончание работы с ключами

Когда работа с ключами по какой-то причине окончена (истечение срока действия, компрометация и т.д.), необходимо удалить закрытые ключи с помощью программы mkkey.

7.4 Возможные датчики случайных чисел

«МагПро КриптоПакет» 3.0 может использовать как программный, так и аппаратные датчики случайных чисел.

Аппаратные ДСЧ входят в состав изделий «Аккорд» (ACCORD), «Соболь» (SOBOL), «АПМДЗ-И/М2» (KRAFTWAY) и «Вьюга» (VJUGA).

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

8 УПРАВЛЕНИЕ СЕРТИФИКАТАМИ И СПИСКАМИ ОТЗЫВА В МАГПРО КРИПТОПАКЕТ

8.1 Управление сертификатами УЦ и списками отзыва

Для того, чтобы программы, использующие МагПро КриптоПакет, могли удостовериться в корректности сертификата, предоставленного другой стороной соединения (отправителем подписанного сообщения, сервером или клиентом TLS-соединения), необходимо, чтобы в их распоряжении была база корневых сертификатов доверенных удостоверяющих центров.

Кроме того, за исключением случаев, когда используется протокол онлайн-проверки статуса сертификатов (OCSP), необходимо наличие актуальных списков отзыва сертификатов.

В случае, если в приложении включена проверка списков отзыва, при отсутствии актуального списка отзыва УЦ, выдавшего сертификат, сертификат не будет признан корректным.

Срок действия списка отзыва обычно много меньше срока действия сертификата. Поэтому при использовании списков отзывов их необходимо регулярно обновлять.

«МагПро КриптоПакет» 3.0 поддерживает два способа хранения базы данных сертификатов удостоверяющих центров, которым соответствуют опции -CAfile и -CApath у некоторых команд утилиты openssl.

В первом случае все сертификаты и списки отзыва в формате PEM помещаются в один текстовый файл, который полностью загружается в память при старте программы.

Во втором случае каждый сертификат и список отзыва располагается в отдельных файлах. На эти файлы создаются символические ссылки с именами, сконструированными из хэш-сумм distinguished name удостоверяющих центров, что позволяет производить быстрый поиск нужного файла.

Поскольку списки отзыва публичных удостоверяющих центров могут иметь весьма большие размеры, первый способ можно рекомендовать только в случае, если доверенными являются только несколько небольших (внутрикорпоративных) УЦ.

Для создания символических ссылок используется утилита `c_rehash`, входящая в комплект «МагПро КриптоПакет» 3.0. При запуске без параметров она производит обработку умолчательной директории с сертификатами, имя которой задано в переменой среды `SSL_CERTS_DIR` или вкомпилировано внутрь библиотеки libcrypto. Если указан параметр, обрабатывается директория, заданная в качестве параметра.

Утилита `c_rehash` накладывает определенные требования на именование файлов, помещаемых в базу доверенных сертификатов. В частности, все файлы, как сертификатов, так и списков отзыва, должны иметь расширение .pem, иначе они будут проигнорированы.

В случае, если полученные сертификаты или списки отзывов не имеют формат pem, т.е. не являются текстовыми файлами, содержащими строчку

```
-----BEGIN CERTIFICATE-----
```

или

```
----BEGIN X509 CRL----
```

то, прежде чем устанавливать их в хранилище, необходимо преобразовать их в формат pem с помощью команды

```
openssl x509 -inform DER -in certificate.der -out certificate.pem
```

или

```
openssl crl -inform DER -in crl.crl -out crl.pem
```

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

8.2 Управление пользовательскими сертификатами

Для того чтобы получить пользовательский сертификат (включая сертификат TLS-сервера) необходимо создать ключевую пару (открытый и закрытый ключи), сформировать заявку на получение сертификата и отправить её в УЦ.

Заявка содержит в себе информацию о том, кому принадлежит данный ключ, и для каких целей он предназначен, и открытый ключ, и подписана с использованием закрытого ключа для той же ключевой пары.

Информация о том, кому принадлежит ключ задается в виде поля subject, представляющего собой список пар идентификатор поля - значение.

Обычно используются следующие поля:

Common Name (CN) - имя владельца сертификата. Для сертификата сервера TLS это должно быть DNS-имя сервера. Во всех остальных случаях обычно используется паспортное имя владельца.

Organization (O) - организация

Organization Unit (OU) - подразделение организации

Locality (L) - местонахождение (город)

Country (C) - страна (двухбуквенный код по ISO 630)

Email Address (E) - адрес электронной почты.

Обязательным является поле CN, но большинство удостоверяющих центров также требует обязательного указания поля Email Address.

Поля заявки могут быть либо указаны явно либо берутся умолчательные значения из файла конфигурации OpenSSL. Системным администраторам настоятельно рекомендуется после установки «МагПро КриптоПакет» 3.0 вписать корректные для данной машины значения этих полей в файл конфигурации.

8.3 Создание ключей для OpenVPN

В исполнениях №№ 7 и 8 («OpenVPN-ГОСТ»), реализующих функционал виртуальной частной сети, «МагПро КриптоПакет» 3.0 используется только для шифрования данных, нет необходимости регистрировать открытые ключи в аккредитованном удостоверяющем центре и полный набор необходимых для работы ключей и сертификатов может быть создан средствами «МагПро КриптоПакет» 3.0. В комплект поставки включается скрипт easy-gost, автоматизирующий этот процесс.

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