КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-01 31 - ЛУ

Подп. и дата | Инв. № дубл. | Взам. инв.№ | Подп. и дата | Инв.№ подп.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
МагПро КриптоПакет вер. 1.0

Описание применения

СЕИУ.00009-01 31
Листов 14

Литера О

2006

Аннотация

Настоящий документ содержит общее описание программного комплекса СКЗИ «МагПро КриптоПакет», предоставляющего возможность использовать российские криптографические алгоритмы при работе с приложениями, рассчитанными на использование OpenSource–библиотеки OpenSSL.

Содержание

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

1 НАЗНАЧЕНИЕ СКЗИ МАГПРО КРИПТОПАКЕТ

Основное назначение СКЗИ СКЗИ «МагПро КриптоПакет» — возможность использования российских криптоалгоритмов при работе с приложениями, рассчитанными на использование библиотеки OpenSSL.

OpenSSL — широко распространенная свободно распространяемая (OpenSource) криптобиблиотека, доступная практически для всех операционных систем. Она используется во множестве программных приложений, в том числе:

- www–сервер Apache
- Почтовые сервера Postfix и Courier
- Сервер каталогов OpenLDAP
- Виртуальная локальная сеть OpenVPN
- Серверное приложение stunnel
- lynx
- tcltls
- wget
- Почтовая программа mutt
- pine
- jabberd

Как и библиотека OpenSSL, СКЗИ «МагПро КриптоПакет» обеспечивает в этих приложениях следующую функциональность:

- Создание защищенных TCP-соединений с использованием протокола TLS;
- Обработка защищенных сообщений электронной почты в форматах S/MIME и PKCS#7;
- Работа с сертификатами ключей в формате X509 и заявками на сертификаты в формате PKCS#10;
- Проверка статуса сертификатов с использованием протокола OCSP.

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

2 СОСТАВ СКЗИ МАГПРО КРИПТОПАКЕТ

В состав СКЗИ «МагПро КриптоПакет» входят:

1. Библиотека реализации базовых криптографических функций форматов X509 и PKCS#7 libcrypto;
2. Библиотека реализации протокола TLS libssl;
3. Библиотека реализации алгоритмов ГОСТ libcryptocom;
4. Утилита openssl, реализующая доступ к основной функциональности библиотек из командной строки;
5. Программа создания закрытых ключей mkkey;
6. Программа удаления закрытых ключей wipekey;
7. Комплект заголовочных файлов для компиляции приложением с использованием библиотек комплекса;
8. Скрипты для управления сертификатами и заявками;
9. Датчик случайных чисел yarrowd.

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

3 СОВМЕСТИМОСТЬ МАГПРО КРИПТОПАКЕТ И OpenSSL

3.1 Совместимость с OpenSSL 0.9.8

Библиотеки СКЗИ «МагПро КриптоПакет» совместимы с OpenSSL 0.9.8 на уровне исходных текстов, т.е. приложение, использующее опубликованный API OpenSSL, может быть скомпилировано с использованием ПК СКЗИ «МагПро КриптоПакет». Бинарной совместимости нет, поэтому для использования ПК СКЗИ «МагПро КриптоПакет» приложения обязательно должны быть перекомпилированы.

3.2 Функциональность, предоставляемая библиотеками СКЗИ «МагПро КриптоПакет»

По умолчанию библиотеки libcrypto и libssl из ПК СКЗИ «МагПро КриптоПакет» предоставляют функциональность, полностью идентичную оригинальной OpenSSL. Для использования российских алгоритмов необходимо подгрузить библиотеку libcryptocom с помощью конфигурационного файла библиотеки libcrypto или с помощью средств конфигурирования приложения, если оно не считывает конфигурационный файл библиотеки libcrypto.

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

4 УПРАВЛЕНИЕ КЛЮЧАМИ В МАГПРО КРИПТОПАКЕТ

4.1 Создание ключей

1. Создать ключи для нужного алгоритма ГОСТ.
   (1.1) В **ознакомительной версии** МагПро КриптоПакет:
   - Для создания ключей используется команда **req** утилиты `openssl`.
   - Для создания ключей команда req использует собственный ДСЧ OpenSSL.
   - Команда req дает возможность записывать созданные ключи только в файловые контейнеры. Запись ключей в аппаратные контейнеры с помощью команды req невозможна.
   - Можно создавать ключи непосредственно вместе с заявкой, с использованием опции `-newkey` команды req.

   (1.2) В **коммерческой версии** МагПро КриптоПакет:
   - Для создания ключей можно использовать как команду **req** утилиты `openssl`, так и программу **mkkey**, входящую в состав коммерческой версии.
   - Для создания ключей с помощью команды req в данной версии необходимо, чтобы на компьютере был установлен ДСЧ Yarrow или аппаратный ДСЧ. Программа mkkey также может использовать ДСЧ Yarrow или аппаратный ДСЧ, а также предоставляет для создания ключей встроенный клавиатурный ДСЧ, если ни Yarrow, ни аппаратного ДСЧ на компьютере не установлено.
   - Команда req дает возможность записывать созданные ключи только в файловые контейнеры. Запись ключей в аппаратные контейнеры с помощью команды req невозможна.
     Программа mkkey может записывать созданные ключи в аппаратные контейнеры.
   - Если для хранения ключей испольуются файловые контейнеры и используется ДСЧ YARROW или аппаратный ДСЧ, можно объединить шаги 1 и 2 и создавать ключи непосредственно вместе с заявкой, с использованием опции `-newkey` команды req.
   - В составе СКЗИ «МагПро КриптоПакет» для FreeBSD 4.x программа mkkey не поставляется, так как на этой платформе не поддерживаются никакие аппаратные контейнеры, а также не работает клавиатурный ДСЧ. В этих системах создание ключей возможно только с помощью команды req, как описано выше.
2. Если ключи создавались с помощью программы mkkey, формировать заявку на регистрацию ключей с помощью команды req утилиты openssl.
3. Отправить заявку в удостоверяющий центр и получить сертификат на ключ.

По умолчанию создаваемые ключи защищаются паролем, который запрашивается в процессе создания ключа. Для того чтобы создать незащищенный паролем ключ, (например, чтобы обеспечить возможность старта TLS-сервера без участия оператора) требуется указать опцию -n у mkkey или –nopass у mkreq.

Изменить пароль у ключа, хранящегося в файле, можно с помощью команды pkcs8 утилиты OpenSSL.

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

4.2 Скрипт mkreq

В составе МагПро КриптоПакет поставляется скрипт `mkreq`, который упрощает создание ключей и заявок на сертификаты.

Данный скрипт не является самостоятельной программой, а представляет собой интерфейс для команды req утилиты `openssl`.

Скрипт `mkreq` поддерживает также создание ключей с алгоритмом RSA, которые могут быть использованы в случае необходимости поддержки совместимости с зарубежными клиентами или серверами.

При использовании готового закрытого ключа скрипт `mkreq` позволяет создать заявку на сертификат ключа любого алгоритма, поддерживаемого OpenSSL.

4.3 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 щифрования gost89.
3. При конфигурировании сервера TLS необходимо явное указание поддержки шифрсьютов GOST2001-GOST89-89 или GOST94-GOST89-GOST89. СКЗИ «МагПро КриптоПакет» позволяет использовать шифрсьюты с алгоритмом RSA одновременно с шифрсьютами ГОСТ, в зависимости от поддержки ГОСТ клиентами, что позволяет одному и тому же серверу взаимодействовать как с клиентами, поддерживающими российские алгоритмы, так и с клиентами их не поддерживающими (например, зарубежными).
   Использование шифрсьютов, использующих алгоритм DSA одновременно с шифрсьютами ГОСТ, недопустимо. TLS-сервер может использовать только один серверный сертификат с одним из трех алгоритмов — DSA, ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001.
4. В некоторых серверных приложениях (например apache) существует возможность отдельной конфигурации серверных сертификатов на разных портах или разных IP-адресах. В этом случае сервер может одновременно использовать DSA и ГОСТ, если выбор между ними определяется портом или IP-адресом, на которое устанавливает соединение клиент.
5. Одновременное использование на одном порту и IP-адресе сертификатов с алгоритмом ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001 невозможно.

4.4 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 wipekey.

4.5 Возможные датчики случайных чисел и ключевые носители

СКЗИ «МагПро КриптоПакет» может использовать как программные, так и аппаратные датчики случайных чисел.

К программным ДСЧ относятся клавиатурный (KEYBOARD) и YARROW.

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

Аппаратные ДСЧ входят в состав изделий «Аккорд» (ACCORD) и «Соболь» (SOBOL). Использование ДСЧ «Аккорд» и «Соболь» возможно в том случае, если соответствующие изделия заранее установлены в компьютере.

Набор возможных ДСЧ зависит от операционной системы, в которой работает программа. Выбор ДСЧ определяет тип созданного ключевого контейнера (контейнеров).

Таблица 1. Поддерживаемые ДСЧ и ключевые контейнеры:

Тип ДСЧ	**Операционные системы**	**Тип контейнера**
ACCORD	Windows, Linux	Touch Memory на устройстве ACCORD
SOBOL	Windows	Touch Memory на устройстве SOBOL
YARROW	Windows, Linux, FreeBSD, Solaris	Файлы PKCS#8
KEYBOARD	Windows, Linux, FreeBSD[1], Solaris	Файлы PKCS#8

[1]Кроме FreeBSD 4.x

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

5 УПРАВЛЕНИЕ СЕРТИФИКАТАМИ И СПИСКАМИ ОТЗЫВА В МАГПРО КРИПТОПАКЕТ

5.1 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.

Библиотека OpenSSL 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 OpenSSL.

При запуске без параметров она производит обработку умолчательной директории с сертификатами, имя которой задано в переменой среды `SSL_CERTS_DIR` или вкомпилировано внутрь библиотеки OpenSSL.

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.

5.2 Скрипт installcadata

Для облегчения помещения в базу данных сертификатов и списков отзыва, полученных из УЦ, которые обычно имеют другую систему именования, в состав МагПро КриптоПакет включен скрипт `installcadata`, которому в качестве параметров указываются файлы сертификатов и списков отзыва и он помещает их, переименовав соответствующим образом, в директорию доверенных сертификатов УЦ, после чего запускает `c_rehash`.

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

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

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

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
```

Скрипт installcadata не обрабатывает файлов в формате, отличном от pem, и сообщает, если указанный файл не является сертификатом или списком отзыва в формате pem.

5.3 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.

Скрипт `mkreq`, входящий в состав МагПро КриптоПакет, позволяет явным образом указать все вышеперечисленные поля. Задание поля CN является обязательным, поле E-Mail, если не указано, заполняется E-Mail адресом текущего пользователя операционной системы (если его возможно определить. В противном случае требуется явное указание). Остальные поля могут быть либо указаны явно, либо берутся умолчательные значения из файла конфигурации OpenSSL.

Системным администраторам настоятельно рекомендуется после установки МагПро КриптоПакет вписать корректные для данной машины значения этих полей в файл конфигурации.

Информация об области применения ключа описывается с помощью расширений `keyUsage` и `extendedKeyUsage`. Для упрощения работы скрипт mkreq поддерживает набор предустановленных комбинаций этих расширений.

Если используется тип ключа server, создается заявка на ключ сервера TLS и используются параметры алгоритма ГОСТ Р 34.10 2001, предназначенные для ключей обмена ключами. В случае если параметры алгоритма указываются явно (например, если ключ создается отдельно

программой mkkey), при создании ключей сервера TLS следует использовать набор параметров XA или XB.

Если используется тип ключа client, создается заявка на сертификат клиента TLS. При этом следует использовать набор параметров, предназначенный для подписи (A, B или C).

Если используется тип ключа smime, создается заявка на сертификат защиты электронной подписи. Данный тип может быть уточнен указанием опций –sign-only или –encrypt-only, которые создают, соответственно, заявку на ключ только для подписи (параметры должны быть A, B или C) или только для шифрования (XA или XB). Если ни одна из этих опций не указана, создается сертификат, который предназначен для подписи (параметры A, B или C), но может быть также использован и для шифрования, поскольку ряд распространенных клиентов электронной почты, в частности Microsoft Outlook, используют для шифрования писем по умолчанию сертификат, пришедший вместе с электронной подписью соответствующего корреспондента, если его область применения это позволяет.

6 ПОДДЕРЖИВАЕМЫЕ СТАНДАРТЫ

В библиотеках ПК СКЗИ «МагПро КриптоПакет» используются криптографические алгоритмы, соответствующие российским стандартам ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94.

Наборы параметров для этих алгоритмов соответствуют RFC 4357.

Поддерживаемые форматы защищенных сообщений соответствуют RFC 3851 и 3852, использование российских алгоритмов в этих форматах соответствует RFC 4490.

Сертификаты и списки отзывов реализованы в соответствии с RFC 3280.

Упаковка открытых ключей алгоритмов ГОСТ реализована в соответствии с RFC 4491.

Протокол TLS реализован в соответствии с RFC 2246.

Протокол OCSP реализован в соответствии с RFC 2560.

После 31 декабря 2007 года алгоритм ГОСТ Р 34.10-94 должен использоваться только для проверки ранее выработанных подписей.

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