КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-01 34 04 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
МагПро КриптоПакет вер. 1.0

Дополнительные скрипты к OpenSSL. Руководство оператора

СЕИУ.00009-01 34 04
Листов 8

Литера О

2006

Аннотация

Настоящий документ содержит руководство оператора для работы с дополнительными скриптами для библитеки OpenSSL из состава СКЗИ «МагПро КриптоПакет».

Содержание

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

1 СКРИПТ MKREQ

1.1 Описание

Скрипт mkreq создает закрытый ключ и заявку на сертификат, которая отсылается в удостоверяющий центр для получения сертификата. Сертификаты используются для аутентификации TLS-серверов и клиентов и для защиты (подписи и/или шифрования) электронной почты с использованием протокола S/MIME.

Этот скрипт предоставляет простой и удобный способ создавать заявки на сертификаты для большинства рядовых случаев. Если необходим какой-то необычный сертификат, следует воспользоваться непосредственно командой req утилиты openssl.

Первый аргумент этого скрипта — тип сертификата (серверный, клиентский или S/MIME).

Второй аргумент — наименование сущности, которая аутентифицируется с помощью этого сертификата. Для серверных сертификатов наименование должно представлять собой полное и корректное доменное имя сервера, для клиентских и S/MIME сертификатов это обычно личное имя владельца сертификата.

Опции позволяют указать дополнительную информацию о владельце сертификата, такие как наименование организации, ее местонахождение и т.д., а также некоторые технические свойства сертификата.

Как правило, скрипт создает два файла: `name.key` — файл, содержащий закрытый ключ (если не используется уже существующий закрытый ключ) и `name.req` — файл, содержащий заявку на сертификат. Закрытый ключ должен храниться у владельца сертификата, а заявку на сертификат следует отправить в удостоверяющий центр для подписания и создания сертификата.

Скрипт также поддерживает создание заявок на сертификаты для уже существующих закрытых ключей (в том числе хранящихся на аппаратных устройствах), созданных при помощи утилиты mkkey из состава МагПро КриптоПакет.

1.2 Формат запуска скрипта

mkreq type name [options]

1.3 Опции

Команда	**Расшифровка**	**Описание**
–email	Адрес электронной почты	Устанавливает значение поля сертификата emailAddress. По умолчанию устанавливается в значение электронного почтового адреса текущего пользователя, который создается из логина пользователя и содержания файла `/etc/mailname`. Если файл `/etc/mailname` не существует (в ОС Debian это значит, что почтовый агент не установлен), эта опцию необходимо указывать.

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

Команда	Расшифровка	Описание
–country	Код страны	Устанавливает значение поля сертификата country. По умолчанию — RU
–org	Наименование организации	Устанавливает наименование организации. Если опция не указана, используется умолчательное значение из файла `openssl.cnf`.
–unit	Наименование подразделения организации	Устанавливает наименование подразделения организации. Если опция не указана, используется умолчательное значение из файла `openssl.cnf`.
–loc	Местоположение	Устанавливает местоположение (например, город). Если опция не указана, используется умолчательное значение из файла `openssl.cnf`.
–sign-only	Только подпись	Устанавливает назначение сертификата только для цифровой подписи. Эту опцию следует использовать только для создания S/MIME-сертификатов.
–encrypt-only	Только шифрование	Устанавливает назначение сертификата только для шифрования. Эту опцию следует использовать только для создания S/MIME-сертификатов.
–rsa[size]	Алгоритм RSA	Создать ключевую пару для алгоритма RSA (по умолчанию создается ключевая пара для алгоритма ГОСТ Р 34.10-2001). Необязательный аргумент size может иметь значения 512, 1024 или 2048 и определяет размер ключа RSA в битах. По умолчанию 2048.
–nopass	Не запрашивать пароль	Не запрашивать пароль для защиты закрытого ключа и не зашифровывать ключ с помощью алгоритма шифрования PKCS#5 на парольной основе.

Команда	Расшифровка	Описание
–key filename	Создать заявку для существующего ключа	Создает заявку на сертификат для уже существующего ключа. Если имя ключевого файла начинается с ACCORD или SOBOL, предполагается, что это наименование аппаратного устройства, поддерживаемого в МагПро КриптоПакет. Если необходимо использовать файл, наименование которого начинается с этих слов (в регистре заглавных букв), следует указать путь к файлу, например `./ACCORD.key`. Опции –rsa и –nopass при использовании этой опции не оказывают влияния.

2 СКРИПТ INSTALLCADATA

2.1 Описание

Устанавливает корневые сертификаты удостоверяющих центров и списки отзыва сертификатов в каталог сертификатов OpenSSL.

Это вспомогательный скрипт, который делает сертификаты удостоверяющих центров и списки отзыва сертификатов доступными для функции проверки сертификатов библиотеки OpenSSL.

Скрипт просматривает каждый файл, указанный в командной строке, и проверяет, содержит ли файл сертификат или список отзыва сертификатов, и копирует его в каталог сертификатов OpenSSL, переименовывая их в соответствии с указанным значением поля distinguished name сертификата удостоверяющего центра, с суффиксом -root.pem или -crl.pem.

Когда все указанные файлы скопированы, вызывается команда `c_rehash` для создания необходимых символических ссылок.

2.2 Формат вызова скрипта

installcadata files...

2.3 Переменные среды

`SSL_CERTS_DIR` — указывает неумолчательное расположение хранилища сертификатов. Если эта переменная не установлена, используется значение по умолчанию, компилированное в бинарном коде 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