Интеграция Рутокен в систему шифрования VeraCrypt (TrueCrypt)

Система шифрования VeraCrypt является мультиплатформенной Open Source разработкой, основанной на коде последней версии утилиты TrueCrypt 7.1a. Аналогично своему предку, VeraCrypt позволяет шифровать разделы жесткого диска, создавать защищенные контейнеры и при этом обладает широким спектром настроек и дополнительных возможностей. Разработчики оперативно исправляют все уязвимости TrueCrypt при их обнаружении.

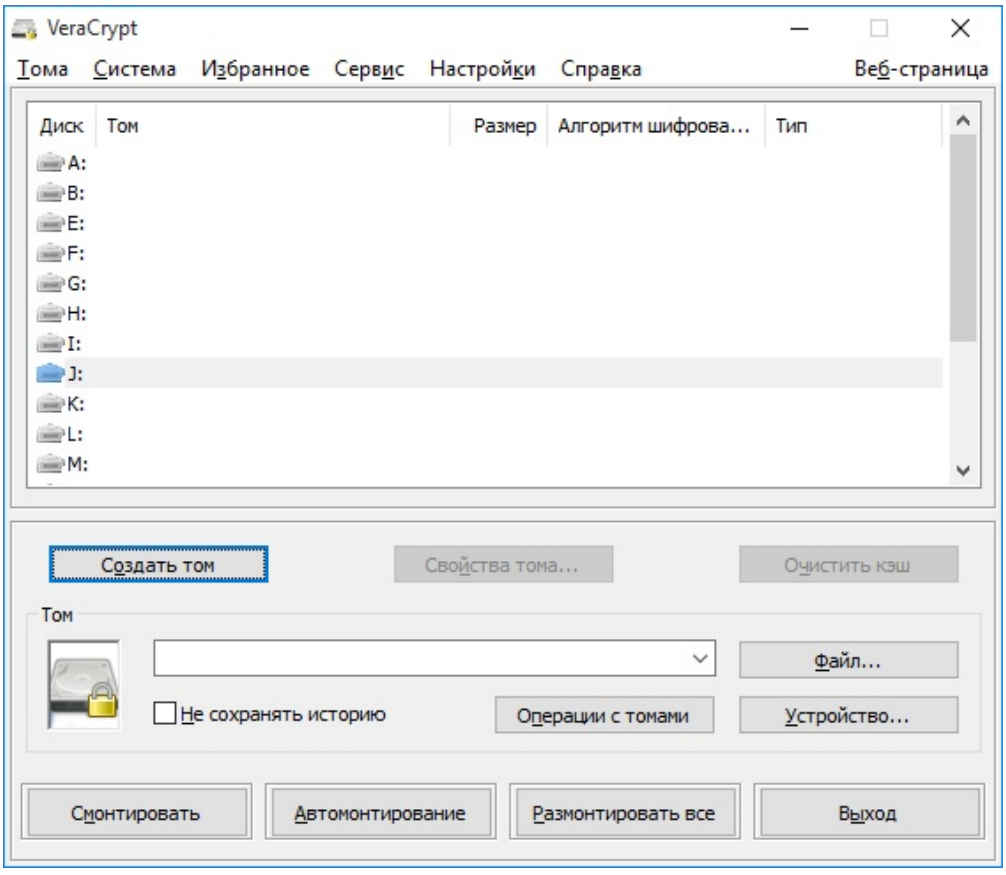
Официальный сайт: http://veracrypt.codeplex.com/

В качестве защищенного хранилища ключа для обеспечения доступа к зашифрованным контейнерам и разделам может использоваться электронный идентификатор Рутокен, что обеспечит дополнительную безопасность хранимой информации.

Поддержка устройств

Токены и смарт-карты семейств Рутокен ЭЦП и Рутокен Lite могут использоваться с VeraCrypt в ОС Windows, Linux, OS X с использованием нашей библиотеки PKCS#11.

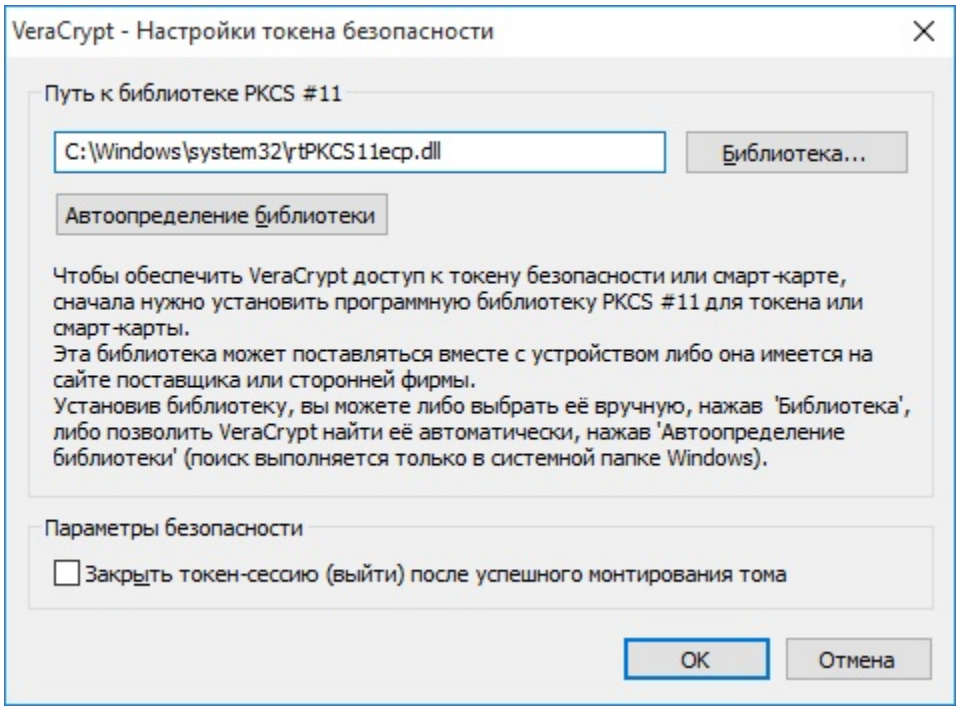
Работа Рутокен S с VeraCrypt в ОС Windows также обеспечивается нашей библиотекой. В Linux и OS X токены Рутокен S поддерживаются проектом OpenSC.



Настройка доступа к контейнерам с помощью токена (для Windows, Linux, OS X)

1) Установите драйвера Рутокен для Windows с нашего сайта. Если вы используете Linux или OS X, то вам необходимо скачать библиотеку PKCS#11 с нашего сайта.

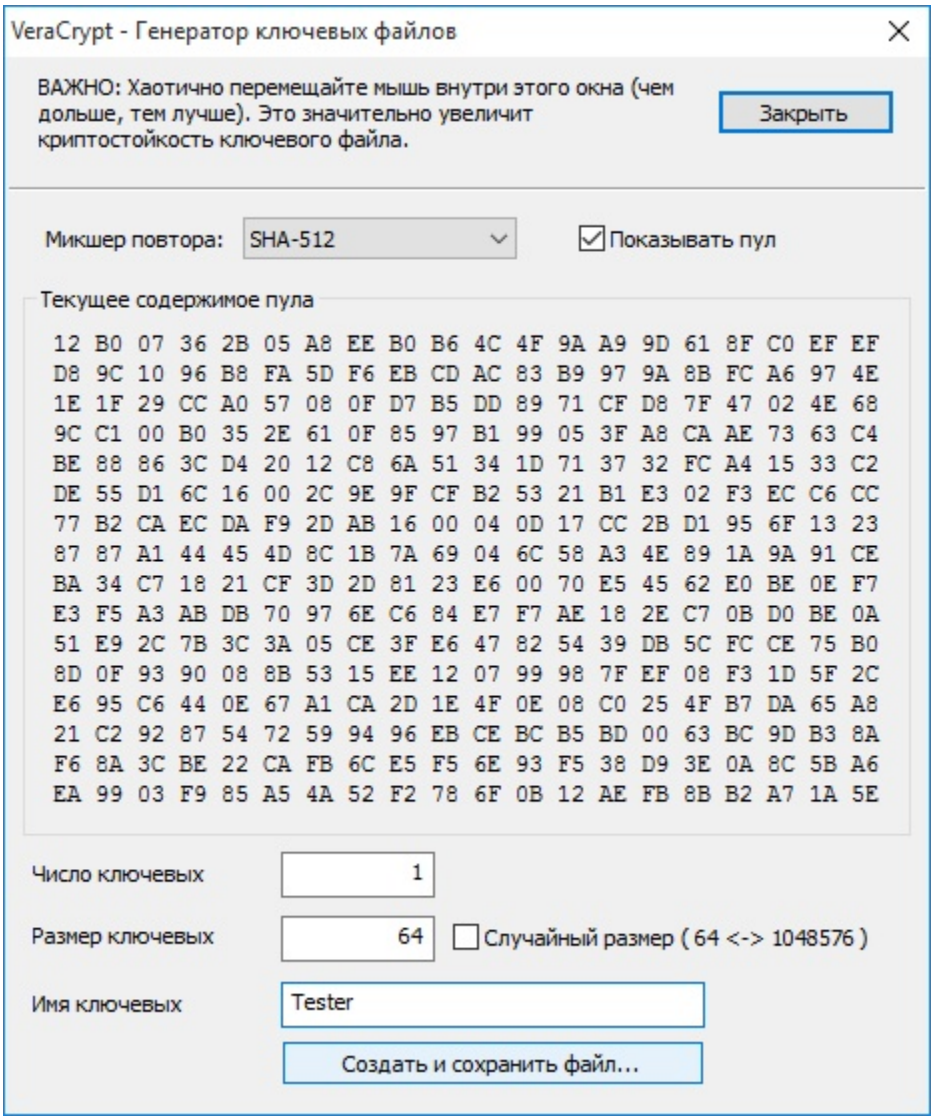
2) Необходимо указать библиотеку, для работы с токенами/смарт-картами: "Настройка -> Токены безопасности..."



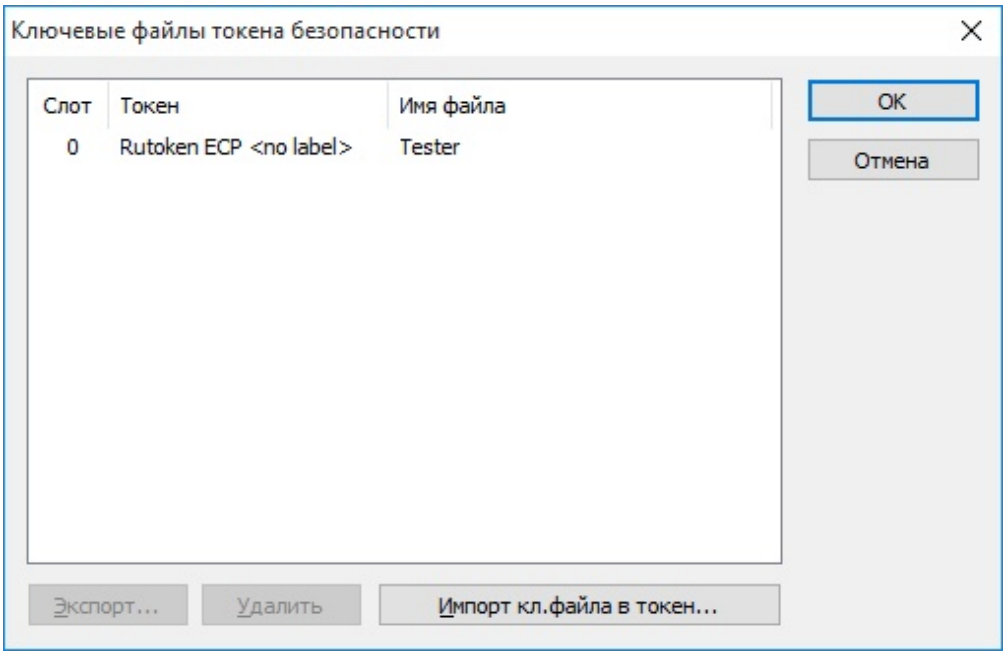
В Windows, если библиотека не указана, можно воспользоваться "Автоопределением библиотеки". Необходимая библиотека rtPKCS11ecp.dll или rtPKCS11.dll (для Рутокен S) обычно располагается в директории C:\Windows\System32

Для Linux и OS X вы указываете путь к скачанной вами библиотеки PKCS#11 (например, /usr/lib/librtpkcs11ecp.so).

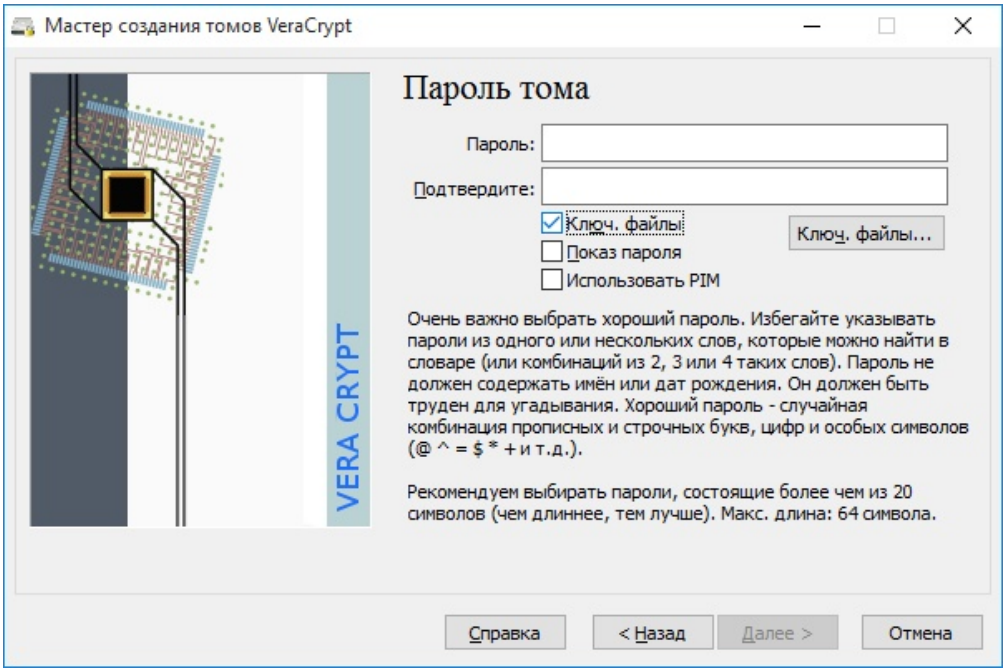
3) Сгенерируйте ключ: "Сервис -> Генератор ключевых файлов". Задайте имя файла и сохраните его в удобном месте.



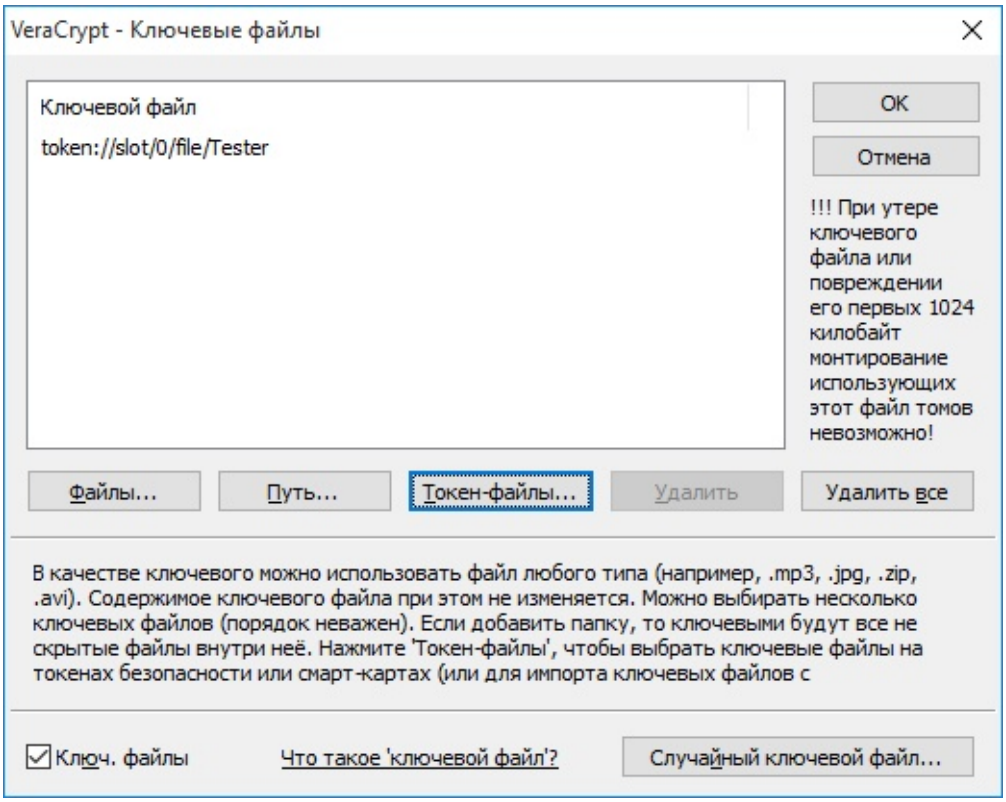
4) Разместите ключ на токене/смарт-карте: "Сервис -> Ключевые файлы токена безопасности... -> Импорт ключевого файла в токен". Вам потребуется ввести пин-код устройства. После размещения ключа на токене его необходимо удалить с компьютера.



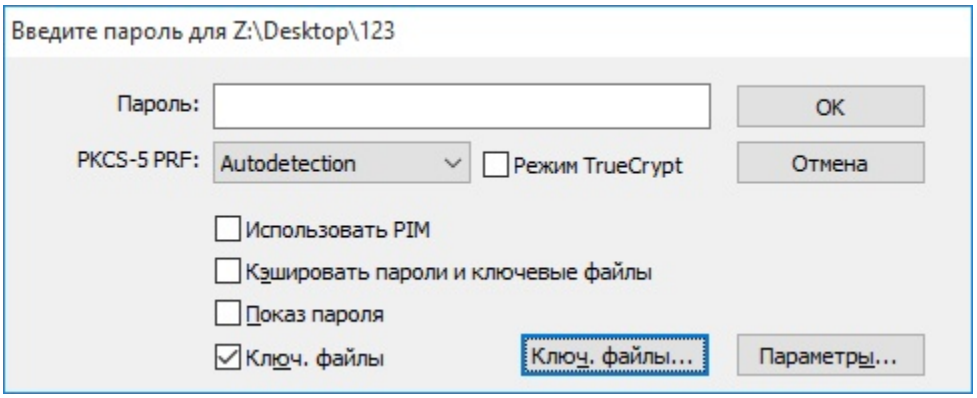
5) Создайте раздел, выбрав использование ключей: "Тома -> Создание нового тома". Укажите необходимые параметры для создаваемого раздела. На этапе указания пароля тома укажите использование ключевого файла.



Зайдите в "Ключ. файлы -> Токен-файлы" и укажите ключ на токене, который вы разместили в п.4.



Теперь для того, чтобы получить доступ к созданному зашифрованному разделу, вам будет необходимо подключить токен и использовать размещенный на нем ключ.



В случае возникновения вопросов по конфигурации VeraCrypt ответы на них можно найти в документации на официальном сайте: http://veracrypt.codeplex.com/documentation