УТВЕРЖДЕНО

АКСФ.501490.008 90

ПАК АУТЕНТИФИКАЦИ И БЕЗОПАСНОГО ХРАНЕНИЯ ИНФОРМАЦИИ «РУТОКЕН» V. 4

Руководство администратора

АКСФ.501490.008 90

Листов 21

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

2021

Аннотация

Настоящий документ предназначен для администраторов, осуществляющих эксплуатацию программно-аппаратного комплекса «Рутокен» версии 4 (далее ПАК «Рутокен» v. 4). В настоящем документе приведены общие сведения, описание архитектуры ПАК «Рутокен» v. 4, а также функции администратора ПАК.

Содержание

1. ОБЩИЕ СВЕДЕНИЯ

В состав ПАК «Рутокен» v. 4 входит электронный идентификаторв в форм-факторе USB-токена, смарт-карты или карты micro SD. ПАК «Рутокен» v. 4» предназначен для выполнения функций по защите информации, а именно: хранение ключевой и управление доступом к ключевой информации. Обеспечивает контроль доступа к компьютеру, поддержку любого числа пользователей (владельцев ПАК «Рутокен» v. 4) на одном компьютере, безопасное хранение в одном устройстве большого количества данных: файлов, ключей шифрования, цифровых сертификатов

ПАК «Рутокен» v. 4 может быть использован в приложениях, где прежде использовались пароли при доступе к БД, Web-серверам, VPN-сетям и security-ориентированным приложениям на программно-аппаратную аутентификацию, обеспечивает надежность и безопасность процесса аутентификации.

Электронные идентификаторы ПАК «Рутокен» v. 4 представляют собой комбинацию активного и пассивного устройств аутентификации, в зависимости от задачи. Они предоставляют вычислительную платформу, на которой информация может храниться и обрабатываться безопасно.

Информация, хранящаяся в памяти электронных идентификаторов, может быть организована таким образом, чтобы доступ к ней полностью контролировался его владельцем или поставщиком приложений

Ключи и PIN-коды хранятся в памяти электронного идентификатора в специальных объектах файловой системы, доступ к этим объектам имеет только сам электронный идентификатор.

Функции ПАК «Рутокен» v. 4

- Хранение паролей для доступа к системам, сетям и т.п.;
- Хранение ключей шифрование и ключей электронной подписи;

- Хранение ключей для целей аутентификации;
- Безопасное хранение информации;
- Управление доступом к информации и ключам, хранящимся на электронном идентификаторе.

2. СТРУКТУРА ПАК «РУТОКЕН» V. 4

В состав ПАК «Рутокен» v. 4 входит

- электронный идентификатор Рутокен, представленный следующими моделями:

– Рутокен ЭЦП SC;

– Рутокен ЭЦП 2.0 2100;

– Рутокен ЭЦП 2.0;

– Рутокен ЭЦП 2.0 micro;

– Рутокен ЭЦП, PKI версия;

– Рутокен ЭЦП micro, PKI версия;

– Рутокен ЭЦП 2.0 Flash;

– Рутокен Lite SD;

– «Rutoken Lite» (Рутокен Lite);

– «Rutoken S» (Рутокен S).

В состав программного обеспечения входят следующие файлы:

- cryptoki.h,
- pkcs11f.h,
- pkcs11.h,
- pkcs11t.h,
- rtpkcs11f.h,
- rtpkcs11.h,
- rtpkcs11t.h
- pki-core-cpp.h
- libpki-core.so
- rtAdmin
- librtpkcs11ecp.so
- rtDrivers.exe
- rtAdmin.exe

- RutokenPlugin.msi
- rtDrivers.x86.msi
- rtpkcs11ecp.dll
- rtDrivers.x64.msi

2.1 Архитектура ПАК «Рутокен» v. 4

Архитектура ПАК «Рутокен» v. 4 была разработана в соответствии с требованиями индустриального стандарта PC/SC. В ней можно выделить четыре уровня:

- Аппаратный уровень. Самый нижний уровень представлен физическими устройствами: непосредственно электронным идентификатором и оборудованием ПЭВМ. Взаимодействие между токеном и хост-контроллером осуществляется по протоколу USB Control Transfer Protocol, который использует Vendor Specific Requests (VSR). Основным аппаратным элементом Рутокен является защищенный микроконтроллер, реализующий поддержку файловой системы и команд по ISO 7816. В зависимости от физического интерфейса подключения, микроконтроллером реализуются функции интерфейса USB, ISO 7816-3, а также другие функции.
- Интерфейс низкого уровня, включающий средства операционной системы. Над аппаратным уровнем находится интерфейс, обеспечивающий представление Рутокен интерфейсам более высокого уровня в качестве смарт-карты, вставленной в ридер. Интерфейс образуется взаимодействием между CCID-драйвером и системным программным обеспечением, реализующим интерфейс PC/SC. Взаимодействие интерфейса низкого уровня с интерфейсом аппаратного уровня происходит путем передачи однозначно определенных команд с использованием Transport Protocol Data Units (TPDU) по протоколам T=0 и T=1.

- Интерфейсы высокого уровня. Самый высокий уровень сформирован из реализаций различных стандартов (PKCS #11) и API (Microsoft Crypto API, Microsoft Crypto Next Generation Key Storage Provider (minidriver)), которые могут взаимодействовать с интерфейсами низкого уровня и оперировать или не оперировать понятием «смарт-карта». Сообщение с интерфейсами более низких уровней происходит путем вызовов однозначно определенных интерфейсных функций и их трансформацией в APDU на среднем уровне.

3. УСТАНОВКА И НАСТРОЙКА ПАК «РУТОКЕН» V.4

3.1 Установка ПАК «Рутокен» v. 4

1. Для работы с программным обеспечением ПАК «Рутокен» v. 4 необходимо перенести файлы, входящие в состав программного обеспечения ПАК «Рутокен» v. 4 в одну директорию ПЭВМ пользователя. В случае работы с ОС Windows следует установить драйверы ПАК «Рутокен» v. 4 путем запуска исполняемого файла rtDrivers.exe.

   В случае работы с ОС Linux отдельной установки драйверов не требуется.

2. При необходимости следует перезагрузить компьютер.
3. Подсоедините электронный идентификатор к свободному USB-порту или вставьте в карт-ридер.
4. Произведите установку прикладного ПО, следуя инструкции разработчиков.

3.2 Настройка ПАК «Рутокен» v. 4

Для выполнения функций форматирования, настроек PIN-кодов и прав доступа в ОС Windows используется Панель управления Рутокен, ярлык которой появится в меню Пуск после установки программного обеспечения. Для работы в ОС Linux используется консольная утилита rtAdmin. Также консольная утилита rtAdmin.exe может использоваться и на ОС Windows.

1. После установки программного обеспечения в соответсвии с п. 3.1 администратору следует изменить PIN-код администратора по умолчанию – на всех электронных идентификаторах изначально установлен PIN-код 87654321. Длина нового PIN-кода администратора не может иметь длину менее 6 символов.

При работе на ОС Windows для этого необходимо открыть Панель управления Рутокен, ярлык которой появится на рабочем столе после установки, открыть вкладку **Администрирование**, нажать кнопку **Ввести PIN-код**, отметить пункт **Администратор**, ввести PIN-код по умолчанию, нажать **ОК**. Затем следует нажать кнопку **Изменить…**, отметить пункт **Администратор**, ввести новый PIN-код, нажать **ОК**.

При работе на ОС Linux следует в командной строке запустить утилиту rtAdmin с параметрами

```
>rtAdmin –o 87654321 –a  pin-admin
```

где pin-admin новый PIN-код администратора.

2. По умолчанию пользователь имеет возможность смены PIN-кода пользователя. При необходимости администратор может отформатировать идентификатор пользователя, дав право изменять PIN-код пользователя

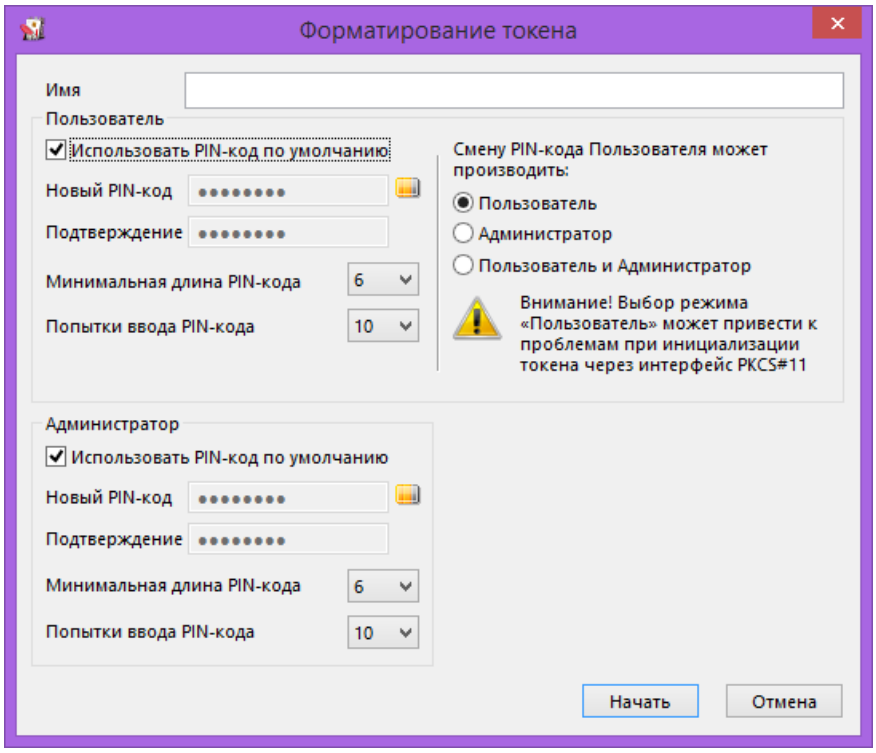
    - только администратору
    - только пользователю
    - и администратору, и пользователю.

    Также при форматировании администратор может задать имя электронному идентификатору.

    В ОС Windows для форматирования и изменения настроек прав смены PIN-кода необходимо в Панели управления Рутокен открыть вкладку **Администрирование**, нажать кнопку **Форматировать…** . В отрывшемся окне отметить, кто может производить смену PIN-кода пользователя, нажать **Начать**.

    В ОС Linux для форматирования запускается утилита rtAdmin с параметрами

Команда	**Параметр команд-ной строки**	**Значение**
Форматирование	-f	-
Политика смены PIN-кода пользователя	-p	1- администратор 2 – пользователь 3 – пользователь и администратор



3. Настройка минимальной длины PIN-кода

Для настройки минимальной длины PIN-кода в ОС Windwos необходимо в Панели управления Рутокен открыть вкладку **Администрирование**, нажать кнопку **Форматировать…** . В отрывшемся окне в поле **Минимальная длина PIN-кода** указывается требуемое значение.

В ОС Linux для настройки минимальной длины требуется отформатировать идентификатор при помощи утилиты rtAdmin с параметрами

Команда	**Параметр командной строки**	**Значение**
Форматирование	-f	-
Минимальная длина PIN-кода администратора	-M	От 6 до 31
Минимальная длина PIN-кода пользователя	-m	От 6 до 31

4. Ограничение количества последовательных неуспешных попыток ввода PIN-кода.

   Для установления ограничения количества последовательных неуспешных попыток ввода PIN-кода пользователя или администратора в ОС Windows необходимо в Панели управления Рутокен открыть вкладку **Администрирование**, нажать кнопку **Форматировать…** . В отрывшемся окне в поле **Попытки ввода PIN-кода** указывается требуемое значение.

   В ОС Linux следует в командной строке запустить утилиту rtAdmin с параметрами

Команда	**Параметр командной строки**	**Значение**
Форматирование	-f	-
Максимальное коли-	-R	От 3 до 10

чество попыток ввода PIN-кода администратора		
Максимальное количество попыток ввода PIN-кода пользователя	-r	От 1 до 10

В случае превышения максимального количества попыток ввода PIN-кода электронный идентификатор блокируется.

Если устройство заблокировано пользователем, оно должно быть передано администратору. Администратор имеет возможность разблокировать идентификатор. В ОС Windows в Панели управления Рутокен необходимо открыть вкладку **Администрирование** и нажать кнопку **Разблокировать**.

В ОС Linux необходимо в командной строке запустить утилиту rtAdmin и выполнить форматирование устройства, установив PIN-код пользователя по умолчанию командой.

```
>rtadmin.exe -f -q
```

В случае блокировки устройства администратором оно должно быть передано производителю для низкоуровнего форматирования.

4. АВАРИЙНЫЕ СИТУАЦИИ

№ п/п	Нештатная ситуация	Действия при нештатной ситуации
1.	Выход электронного идентификатора из строя	Необходимо сообщить администратору безопасности о выходе из строя аппаратного модуля и обеспечить его доставку администратору безопасности для выяснения причин выхода из строя.
2.	Отказы в работе программных средств вследствие случайного или умышленного их повреждения.	При отказах в работе программных средств, в следствии случайного или умышленного их повреждения, лицо, ответственное за безопасность функционирования программных и аппаратных средств, обязано произвести служебное расследование по данному факту с целью установления причины отказа и восстановления правильной работы программных средств в установленном порядке.
3.	Ошибка: Неправильный пин-код	Нужно повторить ввод пин-кода, однако после третей неудачной попытки пин-код блокируется

5. ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

При возникновении вопросов, на которые вам не удалось найти ответ в этом документе, рекомендуем обратиться к следующим дополнительным источникам информации:

- **WWW:** http://www.rutoken.ru

  Web-сайт разработчика содержит большой объем справочной информации об электронных идентификаторах Рутокен.

- Форум: http://forum.rutoken.ru

  Форум содержит ответы на часто задаваемые вопросы. Кроме того, здесь Вы можете задать свой вопрос разработчикам.

- **Служба технической поддержки:**

  www: http://www.rutoken.ru/support/feedback/

  email: hotline@rutoken.ru

  тел.: +7(495)925-77-90