Утилита администрирования Рутокен (rtAdmin)

Применение

Утилита rtAdmin версия 2.0 используется для автоматизации процедур форматирования и администрирования устройств Рутокен: смены метки токена, PIN-кодов и их параметров, управления разделами Flash-памяти.

При работе с утилитой рекомендуется не подключать больше одного устройства Рутокен.

Поддерживаемые модели

- Рутокен Lite
- Рутокен ЭЦП
- Рутокен ЭЦП 2.0
- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 3000
- Рутокен ЭЦП 3.0
- Смарт-карты Рутокен ЭЦП SC
- Смарт-карты Рутокен ЭЦП 2.0
- Смарт-карты Рутокен ЭЦП 3.0 NFC
- Рутокен ЭЦП PKI
- Рутокен ЭЦП 2.0 Flash

Модель Рутокен S в новой версии rtAdmin 2.0 не поддерживается. Если требуется работа с моделью Рутокен S используйте rtAdmin 1.3 в ОС Windows.
Для работы с семейством устройств Рутокен ЭЦП в Windows XP/2003/Vista/2008 – используйте rtAdmin 1.3,

Поддерживаемые платформы

- MS Windows 11/10/8.1/8/2012/7/2008R2
- MS Windows XP/2003/Vista/2008 – только в версии rtadmin 1.3
- GNU/Linux
- macOS

Ссылки на загрузку

Для Windows

Для Linux

Для macOS

Параметры

Утилита запускается из командной строки, её параметры представлены в таблице.

№	Описание команды	Параметр командной строки	Значение по умолчанию/Примечание

1	Форматирование токена Внимание! Обращаем ваше внимание, что при форматировании **все содержимое Рутокена удаляется безвозвратно**. Если устройство имеет встроенную флеш-память, при форматировании **данные с флеш-памяти так же будут удалены безвозвратно.** Пожалуйста, перед форматированием сделайте копию важной информации!	-f	-
2	Текущий PIN-код администратора	-o [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -o
3	Текущий PIN-код пользователя	-c [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -c
4	Устанавливаемый PIN-код администратора	-a [PIN-код (≤ 32)]	87654321 Значение по умолчанию используется только при форматировании без указания параметра -a
5	Устанавливаемый PIN-код пользователя	-u [PIN-код (≤ 32)]	12345678 Значение по умолчанию используется только при форматировании без указания параметра -u
6	Устанавливаемый PIN2 (для Рутокен PINPad. Устанавливается на экране устройства)	-t	Если значение параметра не установлено, то будет использовано значение по умолчанию
7	Генерация PIN-кода администратора (используется при форматировании)	-G [длина PIN-кода (8-32)]	Генерировать PIN-код администратора установленной длины (8-32) (используется при форматировании). При использовании этого параметра параметр -u игнорируется
8	Генерация PIN-кода пользователя (используется при форматировании)	-g [длина PIN-кода (8-32)]	Генерировать PIN-код пользователя установленной длины (8-32) (используется при форматировании). При использовании этого параметра параметр -u игнорируется
9	Загрузка значений пар PIN-кодов из файла	-b [имя файла]	Файл загружается по адресу, который указан в значении параметра. В файле каждому PIN-коду соответствует отдельная строка. При использовании этого параметра параметры -a, -u, -G, -g игнорируются
10	Политика смены PIN-кода пользователя	-p [кто может менять PIN-код: 1 – администратор, 2 – пользователь, 3 – пользователь и администратор]	Значение по умолчанию - 2
11	Минимальная длина PIN-кода администратора	-M [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
12	Минимальная длина PIN-кода пользователя	-m [длина PIN-кода (6-31 для Рутокен ЭЦП и Рутокен Lite, 1 для Рутокен S)]	6
13	Максимальное количество попыток ввода PIN-кода администратора	-R [число попыток (3-10)]	10
14	Максимальное количество попыток ввода PIN-кода пользователя	-r [число попыток (1-10)]	10
15	Метка токена в кодировке Windows-1251	-L [метка токена]	Установить метку токена в кодировке Windows-1251
16	Метка токена в кодировке UTF-8	-D [метка токена]	Установить метку токена в кодировке UTF-8

17	Конвертация в UTF-8 (флаг для параметров, связанных с PIN-кодами)	-U	По умолчанию PIN-коды не конвертируются в UTF-8
18	Ограничение количества выполняемых итераций до одной	-q	-
19	Используемая библиотека PKCS#11	-z [путь к библиотеке]	rtPKCS11.dll
20	Путь к конфигурационному файлу	-n [путь к файлу]	-
21	Протоколирование	-l [путь к файлу лога]	Путь: каталог, в котором лежит утилита. Имя файла: rtadmin.exe.log
22	Разблокировка PIN-кода пользователя и локальных PIN-кодов	-P -o [PIN-код администратора (≤ 32)]	Идентификатор локального пользователя указывать не нужно. Разблокировать локальные PIN-коды и PIN-код пользователя. Для использования этого параметра необходим логин с текущим PIN-кодом администратора
23	Установить SM mode (только для Bluetooth токена)	-s	[Пароли: (1 - опциональный пароль), (2 - 1 пароль), (3 - 6 паролей)] [Режим: (caps - только заглавные буквы), (digits - заглавные буквы и цифры)]
24	Исключенные токены при поточном форматировании	-E [серийные номера токенов в формате: 0x46bc3390 или 932436970]	В качестве разделителя серийных номеров использовать пробел. Также можно использовать опцию -E на каждый серийный номер
25	Показать возможные параметры и примеры	-h, --help	-
32	Запрос PIN-кода Рутокена из стандартного потока ввода в маскированном виде	-I *(i в верхнем регистре)* <вместо значений PIN задавать stdin>	Если аргумент флагов -u, -c, -o, -a равен "stdin", то этот PIN-код будет браться из стандартного потока ввода Примеры: 1) Смена PIN-кода Пользователя: rtadmin -I -u stdin -o stdin 2) Разблокировка PIN-кода Пользователя: rtadmin -I -P -o stdin
33	Выбор Рутокена, с котором производится работа, по серийному номеру	-S <серийный номер Рутокена в hex>	Необходим, когда хотим производить работу с конкретным Рутокеном, а не со всеми. Пример: -S 3a7d6e32 -S 3A7D6E32
34	Получение расширенных политик PIN-кодов	--show-expp	Устройства Рутокен ЭЦП 3.0 поддерживают работу с расширенными политиками PIN-кодов Пользователя. Опция --show-expp позволяет получить текущее состояние этих политик

35	Установка расширенных политик PIN-кодов	--set-expp [Использование: --set-expp (pin_policy_opt1) (value1) (pin_policy_opt2) (value2) ...] pin_policy_opts: • MinPinLength – Минимальная длина PIN-кода: <значение заданное при форматировании> - 31 символ • PinHistoryDepth – Глубина истории PIN-кодов Пользователя: 0-10 • AllowDefaultPinUsage – Разрешить использование PIN-кода по умолчанию: true/false • PinContainsDigit – PIN-код содержит цифры: true/false • PinContainsUpperLetter – PIN-код содержит прописные буквы: true/false • PinContainsLowerLetter – PIN-код содержит строчные буквы: true/false • PinContainsSpecChar – PIN-код содержит спец. символы. chars: true/false • RestrictOneCharPin – Запретить PIN-код из повторяющегося символа: true /false • AllowChangePinPolicy – Разрешить Администратору менять политики PIN-кодов: true /false • RemovePinPolicyAfterFormat – Удалять политики PIN-кодов при форматировании: true/false	Устройства Рутокен ЭЦП 3.0 поддерживают работу с расширенными политиками PIN-кодов Пользователя. Опция --set-expp позволяет устанавливать политики PIN-кодов

26	Просмотр информации о подключенном Рутокене	-T	Вывод информации в о подключённом устройстве в виде:
			
			`: dec`
			`: Rutoken ECP\ Rutoken lite`
			`: dec /dec (/)`
			`PIN- : dec/dec (/)`
			`PIN- : dec/dec (/)`
			`PIN- : dec/dec (/)`
			`PIN- : dec/dec (/)`

27	Показать версию приложения	-v, --version	-

Параметры для управления флеш-памятью (Рутокен Flash)			
27	Разбиение Flash-памяти на разделы (форматирование) Внимание! Форматирование удалит всю информацию с Flash-памяти. Сделайте копию важной информации - после форматирования ее будет невозможно восстановить.	-F [идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный пользователь] [права доступа: ro, rw, hi, cd]	1 весь объем (1DDC сейчас) a rw Один параметр используется для одного раздела. Чтобы создать много разделов используется последовательность команд -F. Для создания раздела необходим PIN-код администратора. Если он не указан, то будет использован PIN-код по умолчанию

28	Изменение прав доступа	-C [идентификатор раздела (1-8)] [новые права доступа: ro, rw, hi, cd] [долговременность: p - постоянное изменение, t - временное]	Для изменения прав используется PIN-код владельца раздела. Если PIN-код не указан, а владельцем раздела является администратор или пользователь, то будет использован PIN-код по умолчанию. Если владельцем раздела является локальный пользователь, а его PIN-код не был указан с использованием команды -O, то произойдет ошибка
29	Получение информации о размере Flash-памяти и атрибутах разделов	-i [a - атрибуты всех разделов] [1-8 - атрибуты конкретного раздела] [sz - объем памяти] Формат ответа – аналогично п. 27 Разбиение Flash-памяти на разделы (форматирование): [идентификатор раздела (1-8)] [размер в Мб] [владелец: a - администратор, u - пользователь, l3-l9 - локальный пользователь] [права доступа: ro, rw, hi, cd]	sz
Параметры для управления локальными пользователями			
30	Устанавливаемый PIN-код локального пользователя	-B [идентификатор локального пользователя (l3-l9)] [PIN-код]	-
31	Текущий PIN-код пользователя	-O [идентификатор локального пользователя (l3-l9)] [PIN-код]	Если PIN-код для данного пользователя не определен, текущий PIN-код указывать не нужно

При необходимости параметры командной строки могут быть переданы с помощью конфигурационного файла.

В случае отсутствия заданных PIN-кодов при форматировании устанавливаются PIN-коды по умолчанию.

Утилита является циклической и после выполнения заданных действий на подключенном токене ожидает подключения следующего.

Форматирование

Утилита предоставляет пользователю возможность поточного форматирования токенов:

1. Пользователь запускает утилиту, установив предварительно необходимые настройки в конфигурационном файле или задав опции в командной строке.
2. Утилита форматирует обнаруженные токены, заносит результаты в лог-файл, ждет подключения следующего токена или команды прекращения работы (например, по нажатию на клавишу Enter).
3. Результаты форматирования пишутся в лог.

Пользователь может запустить форматирование токенов с автоматической генерацией PIN-кода заданной длины, для этого он устанавливает соответствующую опцию в конфигурационном файле.

Пользователь может задать дефолтные значения PIN-кодов, тогда все токены будут иметь одинаковые PIN-коды.

Пользователь может задавать PIN-коды или генерировать их автоматически в кодировке UTF-8, установив соответствующую опцию в конфигурационном файле.

Пользователь может использовать заранее сгенерированные сторонними утилитами PIN-коды. Для этого в настройках он указывает файл, в котором хранится список сгенерированных PIN-кодов с символом перевода строки в качестве разделителя. PIN-коды должны быть записаны парами, например:

```
userpin
adminpin
userpin2
adminpin2
...
```

Смена PIN-кода

В зависимости от политик смены PIN-кода, указанных при форматировании, PIN-код пользователя могут изменить пользователь и(или) администратор.

Результаты смены PIN-кодов пишутся в лог. Если авторизоваться не удается, в лог-файл пишется ошибка. Поточная смена PIN-кодов не прерывается.

Пользователь может запустить смену PIN-кодов с автоматической генерацией новых PIN-кодов заданной длины, для этого он устанавливает соответствующий параметр. Пользователь может задать дефолтные значения PIN-кодов, тогда все токены будут иметь одинаковые PIN-коды.

Пользователь может задавать PIN-коды или генерировать их автоматически в кодировке UTF-8, установив соответствующую опцию в конфигурационном файле.

Пользователь может использовать заранее сгенерированные сторонними утилитами PIN-коды. Для этого в настройках он указывает файл, в котором хранится список сгенерированных PIN-кодов с символом перевода строки в качестве разделителя. PIN-коды должны быть записаны парами, например:

```
userpin
adminpin
userpin2
adminpin2
...
```

Протоколирование работы в лог-файл

Лог-файл представляет собой файл со строками следующего содержания:

1. В случае форматирования

ID токена	Результат форматирования	PIN-код администратора	PIN-код пользователя
В шестнадцатеричном и десятичном виде	Format Passed/ Failed	PIN-код администратора, который был установлен при форматировании	PIN-код пользователя, который был установлен при форматировании

2. В случае смены PIN-кода

ID токена	Результат смены PIN-кодов	PIN-код	PIN-код
В шестнадцатеричном и десятичном виде	Admin/User/Local user pin change Failed/Passed	Старый PIN-код	Новый PIN-код

3. В случае форматирования Flash-памяти

ID токена	Результат форматирования	ID раздела	Объем раздела	Владелец раздела	Права доступа
В шестнадцатеричном и десятичном виде	Volume create Passed/ Failed	ID созданного раздела (01-08)	Объем раздела в Мб	a / u / l3-l9	ro / rw / hi / cd

4. В случае изменения атрибутов разделов Flash-памяти

ID токена	Результат	ID раздела	Новые права доступа	Долговременность изменения прав

В шестнадцатеричном и десятичном виде	Volume access mode change Passed/ Failed	ID изменяемого раздела (01-08)	ro / rw / hi / cd	p / t

5. В случае получения информации об атрибутах разделов Flash-памяти

ID токена	Результат	ID раздела	Объем раздела	Владелец раздела	Права доступа
В шестнадцатеричном и десятичном виде	Getting volume info Passed/ Failed	ID изменяемого раздела (01-08)	Объем раздела в Мб	a / u / l3-l9	ro / rw / hi / cd

Пользователь может задавать имя лог-файла и его расположение. По умолчанию файл лежит в папке с утилитой и называется rtadmin.exe.log.

Если при повторном запуске утилиты пользователь не указал новое имя лог-файла, то старый файл дополняется.

Примеры использования

1. Отформатировать один токен с параметрами по умолчанию (для поточного выполнения убрать флаг -q)

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

2. Отформатировать токен, задав имя токена `RutokenLabel`, PIN-код пользователя `123456789` и PIN-код администратора `987654321`.

```
rtadmin.exe -f -L RutokenLabel -u 123456789 -a 987654321 -q
```

3. Отформатировать токен с использование конфигурационного файла, задав имя токена `RutokenLabel`, PIN-код пользователя `123456789` и PIN-код администратора `987654321`.
   Создаем в папке с утилитой конфигурационный файл с именем conf.txt со следующим содержимым:

   conf.txt

   ```
   rtadmin -f -L RutokenLabel -u 123456789 -a 987654321 -q
   ```

   Запускаем утилиту с указанным именем конфигурационного файла в командной строке:

   ```
   rtadmin.exe -n conf.txt
   ```

4. Отформатировать токен, сменив политику смены PIN-кода только пользователем, максимальное количество попыток ввода PIN-кода пользователя `10`, а PIN-код администратора `3`.

   ```
   rtadmin.exe -f -p 2 -r 10 -R 3 -q
   ```

5. Отформатировать токен, задав минимальную длину PIN-кода пользователя `8` и сам PIN-код `12345678`, PIN-код администратора `9` и сам PIN-код `987654321`.

   ```
   rtadmin.exe -f -m 8 -u 12345678 -M 9 -a 987654321 -q
   ```

6. Разбить память на 1 раздел со следующими атрибутами: владелец - пользователь, права - для чтения и записи, объем раздела - весь (Для Рутокен Flash 4ГБ). PIN-код администратора указан по умолчанию.

   ```
   rtadmin.exe -F 1 3783 u rw -q -a 87654321
   ```

7. Разбить память на 4 раздела со следующими атрибутами:
   первый: владелец - пользователь, права - для чтения и записи, объем раздела - 945 Мб;
   второй: владелец - пользователь, права - только для чтения, объем раздела - 946 Мб;
   третий: владелец - пользователь, права - cd-rom раздел, объем раздела - 946 Мб;
   четвертый: владелец - администратор, права - скрытый раздел, объем раздела - 946 Мб. PIN-код администратора указан по умолчанию.

```
rtadmin.exe -F 1 945 u rw -F 2 946 u ro -F 3 946 u cd -F 4 946 a hi -q -a 87654321
```

8. Изменить права доступа первого раздела на "только для чтения". Владельцем является пользователь, PIN-код указан по умолчанию.

```
rtadmin.exe -C 1 ro p -q -u 12345678
```

9. Получение PIN-кода Пользователя и Администратора из стандартного потока ввода, при форматировании одного Рутокена.

```
rtadmin.exe -f -q -I -u stdin -a stdin
```

10. Форматирование PIN-кода с серийным номером 3ca76d25.

```
rtadmin.exe -f -S 3ca76d25 -q
```

11. Установка расширенных политик PIN-кодов: PIN-код должен содержать цифру, минимальная длина PIN-кода: 8.

```
rtadmin.exe  --set-expp PinContainsDigit true MinPinLength 8
```