

Начало работы со смарт-картой Рутокен ЭЦП 3.0 NFC

- Общая информация
- Работа со смарт-картой на компьютере
 - В ОС Windows
 - Изменение PIN-кода
 - Просмотр сведений об устройстве
 - Просмотр версии установленного комплекта драйверов Рутокен
 - Выбор криптопровайдера, используемого по умолчанию, для устройства Рутокен
 - Выбор метода генерации ключевых пар RSA
 - Выбор настроек для PIN-кода
 - Указание имени устройства Рутокен
 - Разблокировка Администратором PIN-кода Пользователя
 - Форматирование Рутокена
 - В ОС семейства GNU/Linux
 - Проверка корректности подключения считывателя для смарт-карт к компьютеру
 - Установка дополнительного программного обеспечения
 - Проверка работы Рутокен ЭЦП 3.0 NFC в системе
 - Изменение PIN-кода Пользователя
 - В macOS
 - Проверка корректности подключения считывателя для смарт-карт к компьютеру
 - Определение названия модели смарт-карты
 - Проверка работы смарт-карты в системе
 - Изменение PIN-кода смарт-карты
- Работа со смарт-картой на мобильном устройстве
 - В ОС Android
 - Установка приложения Панель управления Рутокен на Android
 - Подключение Рутокена
 - Работа с приложением Панель управления Рутокен
 - Изменение PIN-кода
 - Изменение метки устройства Рутокен
 - Разблокировка PIN-кода
 - В iOS
- Технические характеристики смарт-карты Рутокен ЭЦП 3.0 NFC

Общая информация

Смарт-карта Рутокен ЭЦП 3.0 NFC — это устройство, для формирования и безопасного хранения электронной подписи, а также двухфакторной аутентификации.

Она выглядит следующим образом:



Со смарт-картой можно работать, как на компьютере, так и на мобильном устройстве.

Для работы со смарт-картой:

- на компьютере. Необходим контактный или бесконтактный считыватель для смарт-карт;
- на мобильном устройстве. Необходимо, чтобы мобильное устройство было оборудовано специальным NFC-модулем (это можно проверить в описании его параметров).

Для смарт-карты заданы два PIN-кода: PIN-код Пользователя и PIN-код Администратора.

По умолчанию значение PIN-кода Пользователя — 12345678, а PIN-кода Администратора — 87654321.

При первом использовании смарт-карты PIN-коды необходимо изменить.

В инструкции описаны процедуры работы со смарт-картой Рутокен ЭЦП 3.0 NFC в различных мобильных и настольных ОС, а именно:

- в ОС Windows;
- в ОС семейства GNU/Linux;
- в macOS;
- в ОС Android;
- в iOS.

Работа со смарт-картой на компьютере

Для подключения смарт-карты к компьютеру:

1. Если считыватель контактный, то вставьте в него смарт-карту.
2. Если считыватель бесконтактный, то приложите к нему смарт-карту.
3. Подключите считыватель к USB-порту компьютера. Если смарт-карта подключена корректно, то на считывателе начнет светиться индикатор. Если смарт-карта подключена некорректно, то индикатор на считывателе может мигать или не светиться (зависит от модели считывателя).

В ОС Windows

Изменение PIN-кода

Перед началом работы со смарт-картой необходимо изменить ее PIN-коды. Чтобы их изменить, загрузите и установите [Комплект драйверов Рутокен](#).

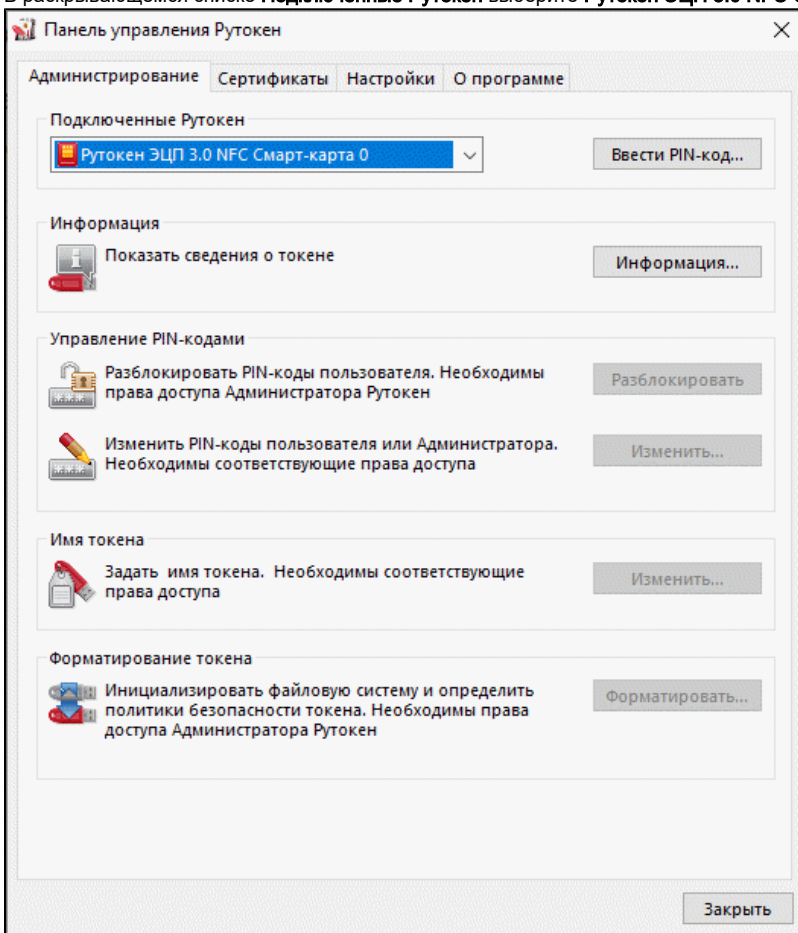
После установки комплекта драйверов на компьютере появится специальная программа для обслуживания устройств Рутокен — Панель управления Рутокен.

Для того, чтобы изменить PIN-код Пользователя или Администратора:

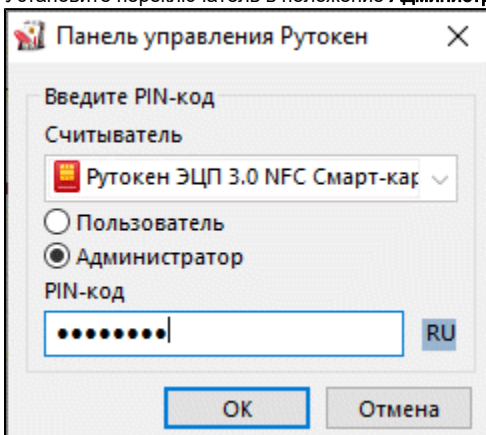
1. Откройте **Панель управления Рутокен**.



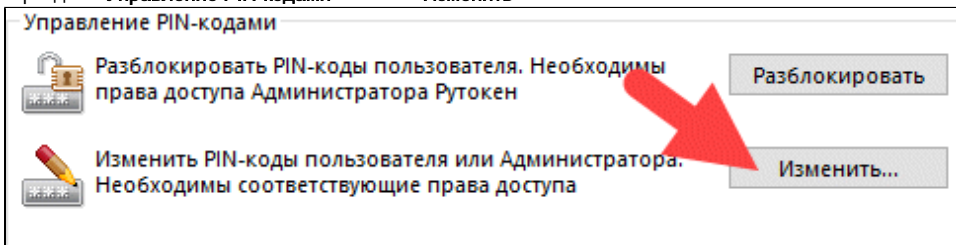
2. В раскрывающемся списке **Подключенные Рутокен** выберите **Рутокен ЭЦП 3.0 NFC Смарт-карта**.



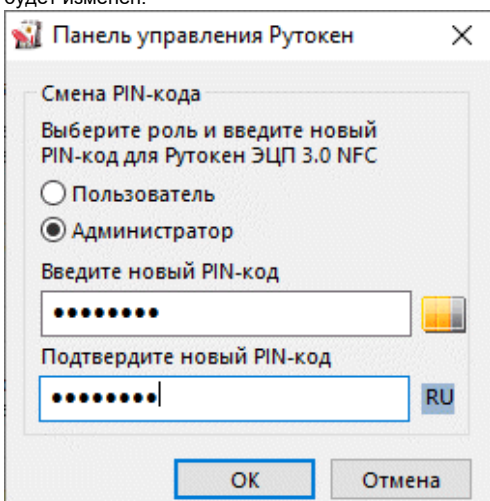
3. Нажмите **Ввести PIN-код**.
4. Установите переключатель в положение **Администратор**, введите PIN-код Администратора и нажмите **ОК**.



5. В разделе **Управление PIN-кодами** нажмите **Изменить**.



6. Установите переключатель в необходимое положение, введите два раза новый PIN-код и нажмите **ОК**. В результате выбранный PIN-код будет изменен.



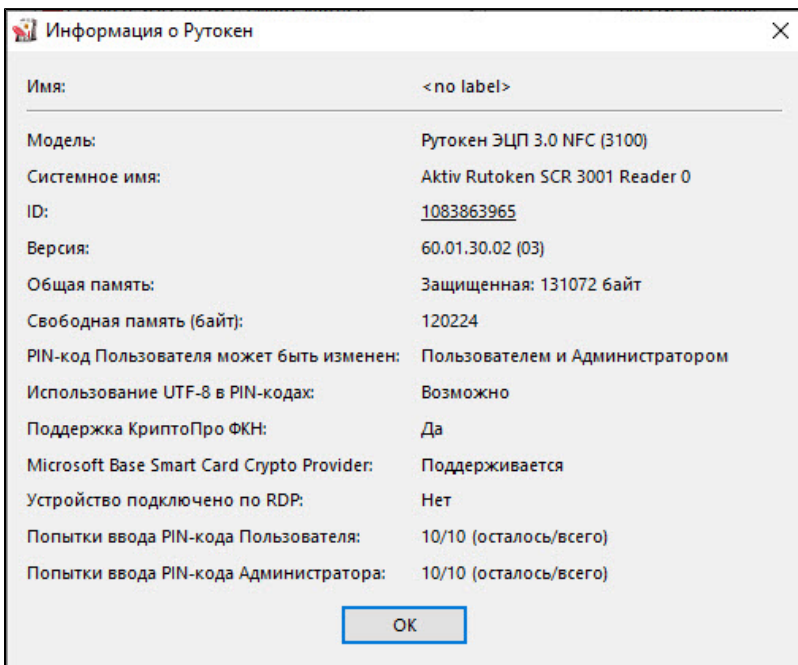
Просмотр сведений об устройстве

В Панели управления Рутокен можно узнать следующую информацию об устройстве:

- наименование модели;
- уникальный цифровой идентификатор;
- версию прошивки и флаги состояния;
- общий объем памяти;
- объем свободной памяти;
- политику для смены PIN-кода Пользователя;
- возможность использования UTF-8 в PIN-кодах;
- возможность работы с КриптоПро Рутокен CSP по защищенному каналу ФКН;
- подключено ли оно по RDP.

Для просмотра сведений об устройстве Рутокен:

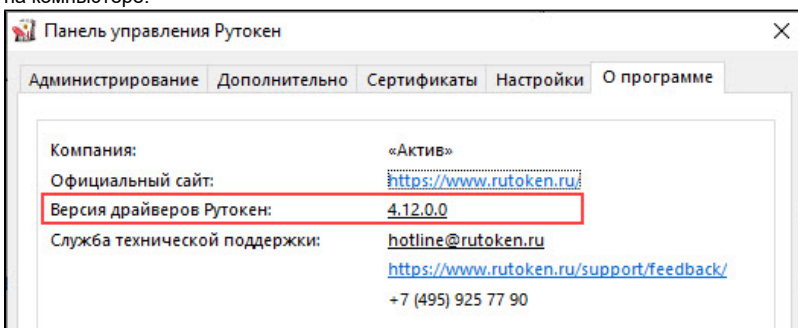
1. Откройте **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите **Рутокен ЭЦП 3.0 NFC Смарт-карта**.
3. В разделе **Информация** нажмите на одноименную кнопку. Откроется окно **Информация о Рутокен**, в этом окне указана вся необходимая информация об устройстве.



Просмотр версии установленного комплекта драйверов Рутокен

Для просмотра версии установленного комплекта драйверов:

1. Откройте **Панель управления Рутокен**.
2. Перейдите на вкладку **О программе**. В поле **Версия драйверов Рутокен** указан номер версии комплекта драйверов, который установлен на компьютере.



Выбор криптопровайдера, используемого по умолчанию, для устройства Рутокен

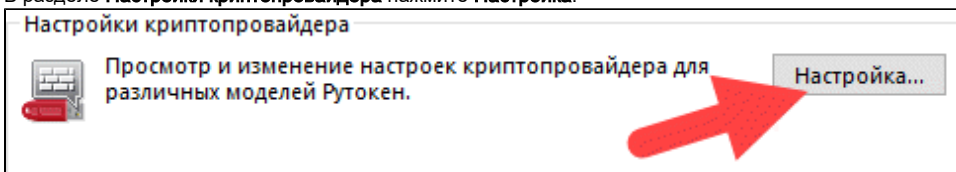
Криптопровайдер — это динамически подключаемая библиотека, реализующая криптографические функции со стандартизированным интерфейсом.

У каждого криптопровайдера могут быть собственные наборы алгоритмов и собственные требования к формату ключей и сертификатов.

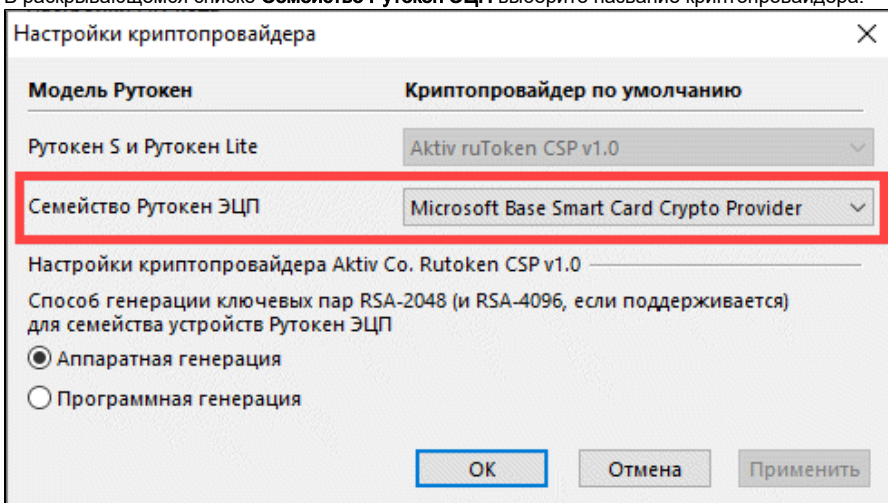
Чтобы выбрать криптопровайдера, который будет использоваться для Рутокена по умолчанию:

1. Открой **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.

3. В разделе **Настройки криптопровайдера** нажмите **Настройка**.



4. В раскрывающемся списке **Семейство Рутокен ЭЦП** выберите название криптопровайдера.

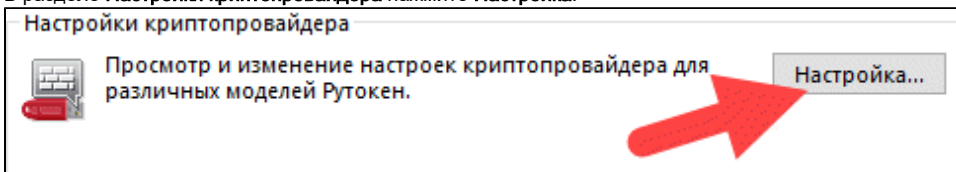


5. Чтобы применить изменения и продолжить работу с настройками нажмите **Применить**.
6. Чтобы подтвердить выбор криптопровайдера нажмите **ОК**.
7. В окне с запросом на разрешение внесения изменений на компьютере нажмите **Да**.

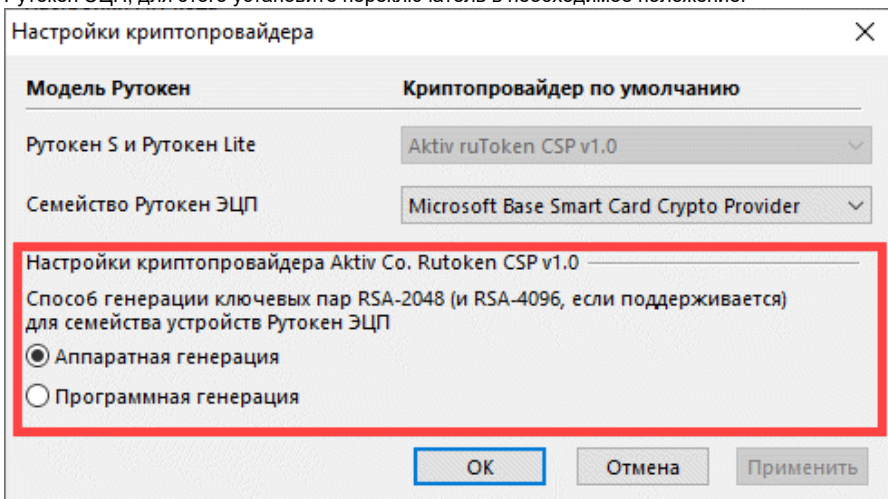
Выбор метода генерации ключевых пар RSA

Чтобы выбрать криптопровайдера для генерации ключевых пар RSA:

1. Откройте **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. В разделе **Настройки криптопровайдера** нажмите **Настройка**.



4. В разделе **Настройки криптопровайдера Aktiv Co. Rutoken CSP v1.0** выберите способ генерации ключевых пар RSA 2048 бит для Рутокен ЭЦП, для этого установите переключатель в необходимое положение.



5. Чтобы применить изменения и продолжить работу с настройками, нажмите **Применить**.
6. Чтобы подтвердить выбор криптопровайдера, нажмите **ОК**.

7. В окне с запросом на разрешение внесения изменений на компьютере нажмите **Да**.

Выбор настроек для PIN-кода

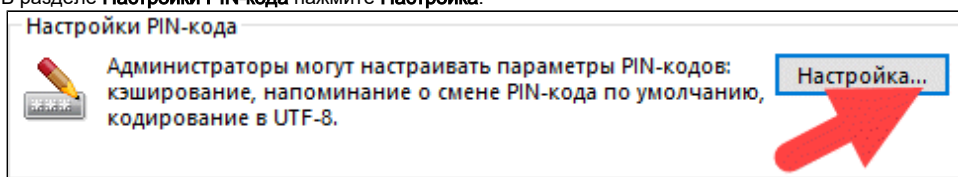
В Панели управления Рутокен можно задать настройки для PIN-кодов. Перечень настроек указан в таблице 1.

Таблица 1

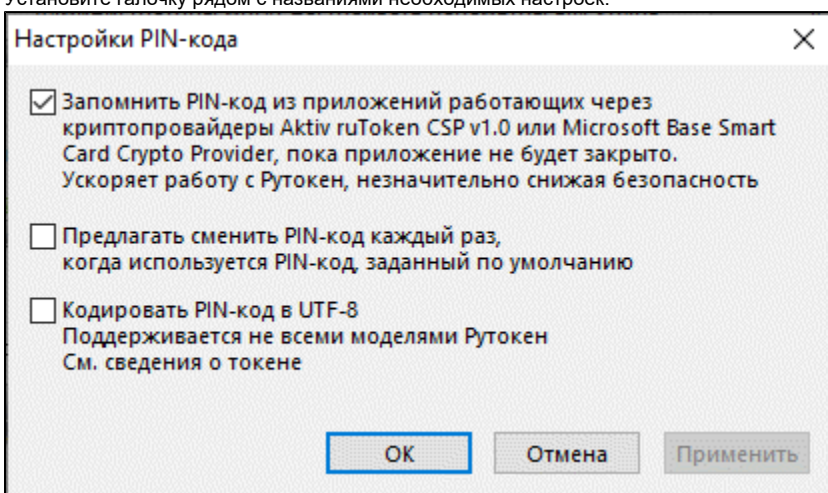
Настройка	Результат выбора настройки
Запомнить PIN-код из приложения...	PIN-код Пользователя вводится один раз при первом использовании устройства Рутокен в приложении. Эта настройка позволяет уменьшить количество вводов PIN-кода в прикладных приложениях за счет кратковременного хранения их криптопровайдером в зашифрованной памяти. Не следует использовать данную настройку, если нет уверенности в безопасности компьютера.
Предлагать сменить PIN-код каждый раз...	Каждый раз после ввода PIN-кода на экране отображается сообщение с предложением изменить PIN-код (если пользователь не изменил PIN-код, установленный по умолчанию).
Кодирование PIN-кода в UTF-8...	PIN-код может состоять из кириллических символов. Эта настройка позволяет безопасно использовать PIN-коды, содержащие кириллические символы.

Чтобы выбрать настройки для PIN-кода:

1. Откройте **Панель управления Рутокен**.
2. Перейдите на вкладку **Настройки**.
3. В разделе **Настройки PIN-кода** нажмите **Настройка...**.



4. Установите галочку рядом с названиями необходимых настроек.



5. Чтобы применить изменения и продолжить работу с настройками нажмите **Применить**.
6. Чтобы подтвердить выбор настроек нажмите **ОК**.
7. В окне с запросом на разрешение внесения изменений на компьютере нажмите **Да**.

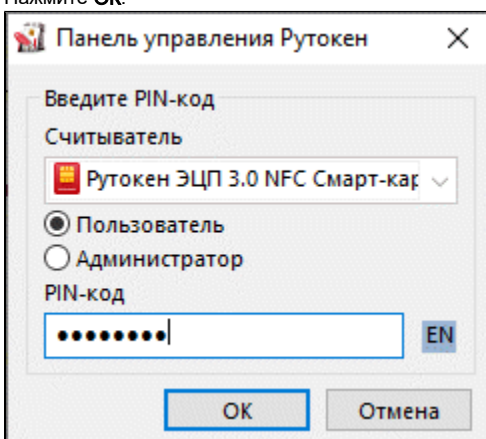
Указание имени устройства Рутокен

Для того чтобы различать устройства Рутокен между собой следует задать имя каждому устройству. Оно не всегда будет отображаться в сторонних приложениях.

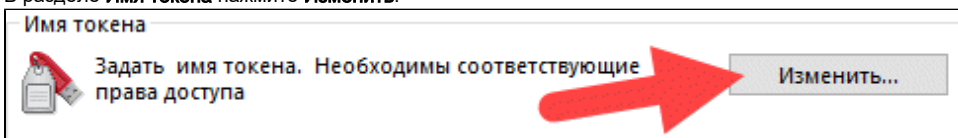
Рекомендуется указать имя и фамилию владельца устройства или краткое наименование области применения устройства.

Для указания имени устройства Рутокен:

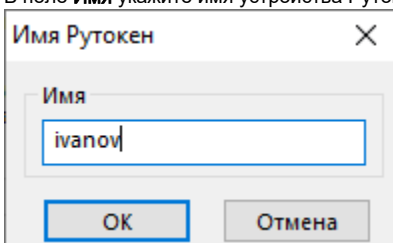
1. Откройте **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите **Рутокен ЭЦП 3.0 NFC Smart-карта**.
3. Нажмите **Ввести PIN-код**.
4. Установите переключатель в положение **Пользователь**.
5. Введите PIN-код Пользователя.
6. Нажмите **ОК**.



7. В разделе **Имя токена** нажмите **Изменить**.



8. В поле **Имя** укажите имя устройства Рутокен.



9. Нажмите **ОК**.

Разблокировка Администратором PIN-кода Пользователя

PIN-код Пользователя блокируется в том случае, если пользователь несколько раз подряд ввел его с ошибкой.

PIN-код Пользователя можно разблокировать только, если знаешь PIN-код Администратора.

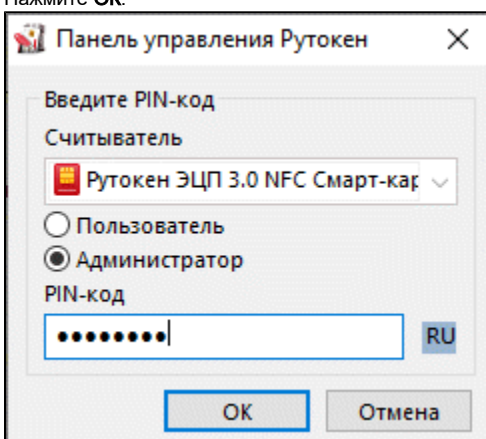
После того как PIN-код Пользователя будет разблокирован, счетчик неудачных попыток аутентификации примет исходное значение.

После разблокировки PIN-код Пользователя не изменится.

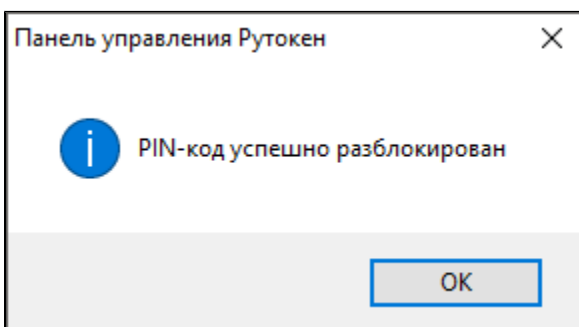
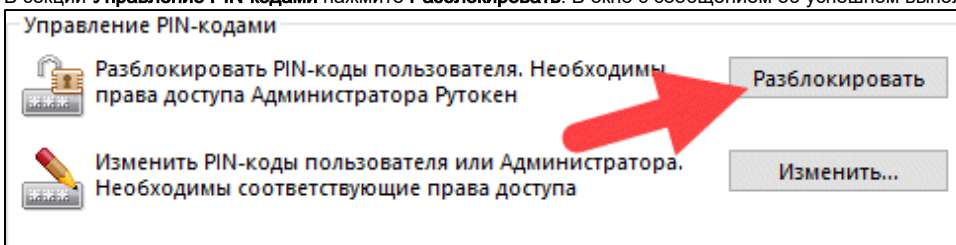
Для того чтобы разблокировать PIN-код Пользователя:

1. Откройте **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите **Рутокен ЭЦП 3.0 NFC Smart-карта**.
3. Нажмите **Ввести PIN-код**.
4. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.

5. Нажмите **OK**.



6. В секции **Управление PIN-кодами** нажмите **Разблокировать**. В окне с сообщением об успешном выполнении операции нажмите **OK**.



В результате PIN-код Пользователя будет разблокирован.

Форматирование Рутокена

В ходе форматирования устройства все, созданные на нем объекты удалятся. Также при форматировании задаются новые значения PIN-кодов или выбираются значения, используемые по умолчанию.

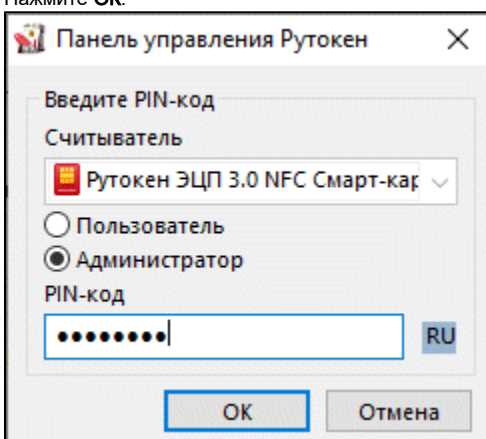
Если пользователь исчерпал все попытки ввода PIN-кода Администратора, то существует возможность вернуть устройство в заводское состояние. Для такого форматирования ввод PIN-кода Администратора не требуется.

При форматировании устройства Рутокен все данные на нем, в том числе ключи и сертификаты, будут удалены безвозвратно. В процессе форматирования не следует отключать устройство Рутокен от компьютера, так как это может привести к его поломке.

Для запуска процесса форматирования устройства Рутокен:

1. Откройте **Панель управления Рутокен**.
2. В раскрывающемся списке **Подключенные Рутокен** выберите **Рутокен ЭЦП 3.0 NFC Смарт-карта**.
3. Нажмите **Ввести PIN-код**.
4. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.

5. Нажмите **OK**.



Панель управления Рутокен

Введите PIN-код

Считыватель

Рутокен ЭЦП 3.0 NFC Смарт-карт

☐ Пользователь

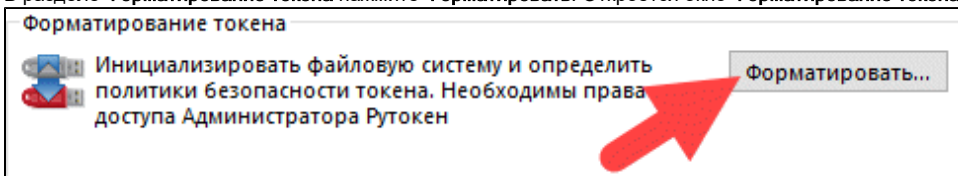
☒ Администратор

PIN-код

..... RU

OK Отмена

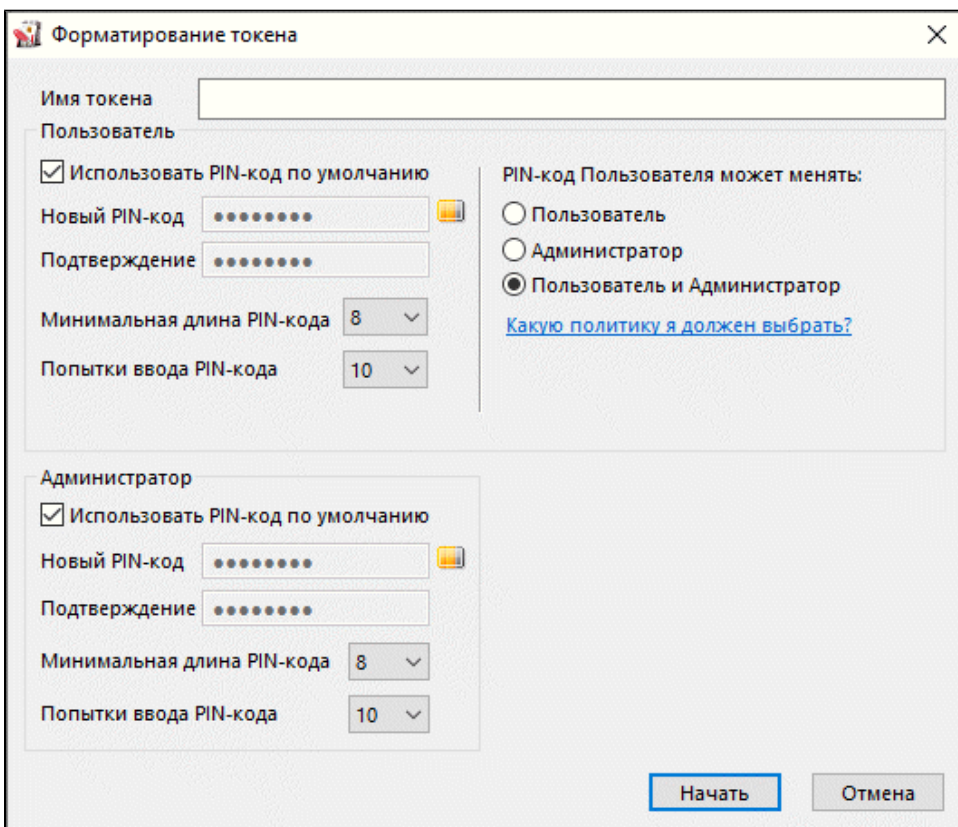
6. В разделе **Форматирование токена** нажмите **Форматировать**. Откроется окно **Форматирование токена**.



Форматирование токена

Инициализировать файловую систему и определить политики безопасности токена. Необходимы права доступа Администратора Рутокен

Форматировать...



Форматирование токена

Имя токена

Пользователь

☒ Использовать PIN-код по умолчанию

Новый PIN-код

Подтверждение

Минимальная длина PIN-кода 8

Попытки ввода PIN-кода 10

PIN-код Пользователя может менять:

☐ Пользователь

☐ Администратор

☒ Пользователь и Администратор

[Какую политику я должен выбрать?](#)

Администратор

☒ Использовать PIN-код по умолчанию

Новый PIN-код

Подтверждение

Минимальная длина PIN-кода 8

Попытки ввода PIN-кода 10

Начать Отмена

7. В поле **Имя токена** введите имя устройства Рутокен.

8. В разделе **PIN-код Пользователя может менять** установите переключатель в необходимое положение.

PIN-код Пользователя может менять:

☐ Пользователь

☐ Администратор

☒ Пользователь и Администратор

[Какую политику я должен выбрать?](#)

9. В разделе **Пользователь** укажите новый PIN-код Пользователя или установите галочку **Использовать PIN-код по умолчанию**.
10. В раскрывающемся списке **Минимальная длина PIN-кода** выберите необходимое значение.
11. В раскрывающемся списке **Попытки ввода PIN-кода** выберите необходимое значение.

Пользователь

☒ Использовать PIN-код по умолчанию

Новый PIN-код

Подтверждение

Минимальная длина PIN-кода

Попытки ввода PIN-кода

12. В разделе **Администратор** укажите новый PIN-код Администратора или установите галочку **Использовать PIN-код по умолчанию**.
13. В раскрывающемся списке **Минимальная длина PIN-кода** выберите необходимое значение.
14. В раскрывающемся списке **Попытки ввода PIN-кода** выберите необходимое значение.

Администратор

☒ Использовать PIN-код по умолчанию

Новый PIN-код

Подтверждение

Минимальная длина PIN-кода

Попытки ввода PIN-кода

15. Нажмите **Начать**.
16. В окне с предупреждением об удалении всех данных на устройстве Рутокен нажмите **ОК**.

Панель управления Рутокен

 **ВНИМАНИЕ!** Все данные на Рутокен будут уничтожены! Начать форматирование?

17. Дождитесь окончания процесса форматирования.

Рутокен форматируется

Внимание! Не отключайте Рутокен, пока процесс не завершится

18. В окне с сообщением об успешном форматировании устройства Рутокен нажмите **ОК**.

В ОС семейства GNU/Linux

Проверка корректности подключения считывателя для смарт-карт к компьютеру

Первым делом подключите считыватель для смарт-карт к компьютеру и вставьте в него смарт-карту.

Для проверки корректности подключения считывателя для смарт-карт к компьютеру введите команду:

`lsusb`

В результате в окне Терминала отобразится название модели считывателя для смарт-карт:

```
dm18@ubuntu:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 08e6:3437 Gemalto (was Gemplus) GemPC Twin SmartCard Reader
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
dm18@ubuntu:~$
```

Это означает, что считыватель для смарт-карт подключен корректно.

Определить название смарт-карты и выполнить дальнейшие действия данной инструкции невозможно без предварительной установки дополнительного программного обеспечения.

Установка дополнительного программного обеспечения

В deb-based и rpm-based системах используются разные команды. Список систем указан в таблице 1.

Таблица 1. Список операционных систем GNU/Linux

deb-based	rpm-based
Debian, Ubuntu, Linux Mint,	RedHat, CentOS, Fedora, ALT Linux,
Astra Linux	ROSA Linux, МСВС, ГосЛинукс, РЕД ОС

Для выполнения действий данной инструкции необходимо установить следующее программное обеспечение:

в **deb-based** системах это обычно:

- библиотека libccid не ниже 1.4.2;
- пакеты libpcsc-lite1 и pcscd;
- pcsc-tools.

в **rpm-based** системах это обычно:

- ccid не ниже 1.4.2;
- pcsc-lite;
- pcsc-tools.

в **ALT Linux** это обычно:

- pcsc-lite-ccid;
- libpcsc-lite;
- pcsc-tools.

Также для всех типов операционных систем необходимо установить библиотеку OpenSC.

Перед установкой библиотек и пакетов **проверьте их наличие в системе**. Для этого введите команду:

В **deb-based** системах:

`dpkg -s libccid libpcsc-lite1 pcscd pcsc-tools opensc`

Если библиотека или пакет уже установлены в системе, то в разделе **Status** отобразится сообщение "install ok installed".

В разделе **Version** отобразится версия указанной библиотеки или пакета (версия библиотеки libccid должна быть выше чем 1.4.2).

В **rpm-based** системах:

```
sudo rpm -q ccid pcsc-lite pcsc-tools opensc
```

Если библиотека или пакет уже установлены в системе, то на экране отобразятся их названия и номера версий (версия библиотеки ccid должна быть выше чем 1.4.2).

В **ALT Linux**:

```
sudo rpm -q pcsc-lite-ccid libpcsc-lite pcsc-tools opensc
```

Если у вас нет доступа к команде sudo, то используйте команду su.

Если библиотек и пакетов еще нет на компьютере, то необходимо их установить.

Для **установки пакетов и библиотек**:

В **deb-based** системах введите команду:

```
sudo apt-get install libccid pcscd libpcsc-lite pcsc-tools opensc
```

В **rpm-based** системах (кроме ALT Linux) введите команду:

```
sudo yum install ccid pcsc-lite pcsc-tools opensc
```

В **ALT Linux** введите команду:

```
sudo apt-get install pcsc-lite-ccid libpcsc-lite pcsc-tools opensc
```

Если у вас нет доступа к команде sudo, то используйте команду su.

Проверка работы Рутокен ЭЦП 3.0 NFC в системе

Для проверки работы смарт-карты:

1. Подключите ее к компьютеру.
2. Введите команду:

```
pcsc_scan
```

3. Если отобразилось следующее сообщение:

```
user@ubuntu:~$ pcsc_scan
Using reader plug'n play mechanism
Scanning present readers...
0: Gemalto PC Twin Reader (3629CED3) 00 00

Fri Nov 13 08:50:20 2020
Reader 0: Gemalto PC Twin Reader (3629CED3) 00 00
Event number: 0
Card state: Card inserted,
ATR: 3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43 50 73 63 C0

ATR: 3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43 50 73 63 C0
+ TS = 3B --> Direct Convention
+ T0 = 9C, Y(1): 1001, K: 12 (historical bytes)
+ TA(1) = 97 --> F1=512, D1=64, 8 cycles/ETU
500000 bits/s at 4 MHz, fMax for F1 = 5 MHz => 625000 bits/s
TD(1) = 80 --> Y(i+1) = 1000, Protocol T = 0
-----
TD(2) = 11 --> Y(i+1) = 0001, Protocol T = 1
-----
TA(3) = 40 --> IFSC: 64
+ Historical bytes: 52 75 74 6F 6B 65 6E 45 43 50 73 63
Category indicator byte: 52 (proprietary format)
+ TCK = C0 (correct checksum)

Possibly identified card (using /usr/share/pcsc/smartcard_list.txt):
NONE

Updating /home/user/.cache/smartcard_list.txt using http://ludovic.rousseau.free.fr/softwares/pcsc-tools/smartcard_list.txt

Possibly identified card (using /home/user/.cache/smartcard_list.txt):
3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43 50 73 63 C0
Aktiv Rutoken ECP 3.0 NFC (PKI)
https://www.rutoken.ru/products/all/rutoken-ecp-nfc/
```

Значит смарт-карта работает корректно.

Изменение PIN-кода Пользователя

Перед запуском процесса смены PIN-кода установите библиотеку PKCS#11 и определите путь до библиотеки libtpkcs11ecp.so.

Для того чтобы загрузить библиотеку PKCS#11:

1. Определите разрядность используемой системы:

```
uname -p
```

Если в результате выполнения команды отобразилась строка подобная "i686", то система является 32-разрядной.

Если в результате выполнения команды отобразилась строка подобная "x86_64", то система является 64-разрядной.

2. Перейдите по указанной ссылке, выберите необходимую версию, загрузите и установите ее:

<https://www.rutoken.ru/support/download/pkcs/>

Для того чтобы определить путь до библиотеки librtpkcs11ecp.so введите команду:

```
find /usr/*(lib|lib64) -name librtpkcs11ecp.so
```

```
dm18@ubuntu:~$ find /usr/*(lib|lib64) -name librtpkcs11ecp.so
/usr/lib/librtpkcs11ecp.so
dm18@ubuntu:~$
```

Для изменения PIN-кода введите команду:

```
pkcs11-tool --module {A} --login --pin {B} --change-pin --new-pin {C}
```

A — путь до библиотеки librtpkcs11ecp.so.

B — текущий PIN-код устройства.

C — новый PIN-код устройства.

В результате PIN-код устройства будет изменен.

В macOS

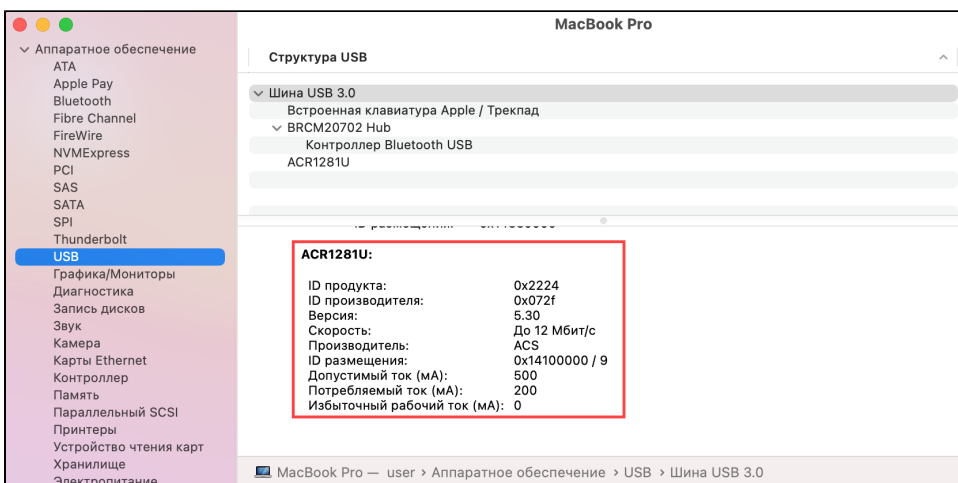
Проверка корректности подключения считывателя для смарт-карт к компьютеру

Для проверки корректности подключения считывателя для смарт-карт к компьютеру:

1. Подключите считыватель для смарт-карт к компьютеру и вставьте в него смарт-карту
2. Откройте программу **Информация о системе (System Information)**.



3. На боковой панели окна программы выберите пункт **USB**.
4. Для считывателя в окне программы отобразится название модели считывателя и информация о нем.



Это означает, что считыватель для смарт-карт подключен корректно.

Определение названия модели смарт-карты

Перед запуском процесса определения названия модели смарт-карты:

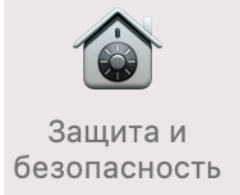
- загрузите и установите пакет **OpenSC**;
- загрузите и установите приложение **Рутокен для macOS**;
- определите путь до библиотеки **libtpkcs11esc.dylib**.

Актуальная версия установочного пакета OpenSC доступна по ссылке:

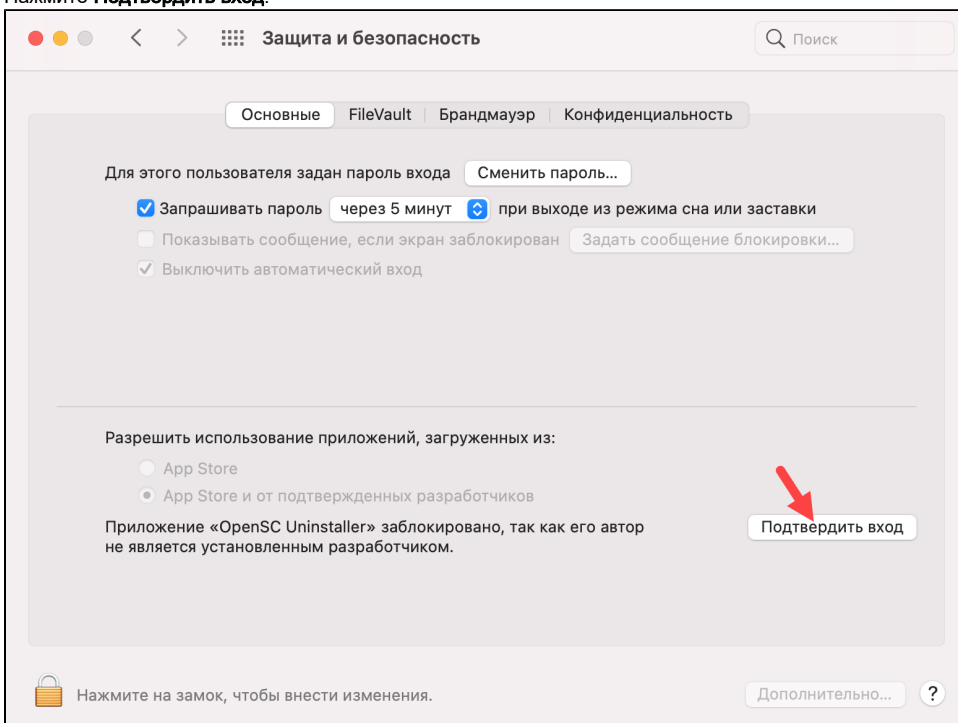
<https://github.com/OpenSC/OpenSC/wiki>

Для установки пакета **OpenSC**:

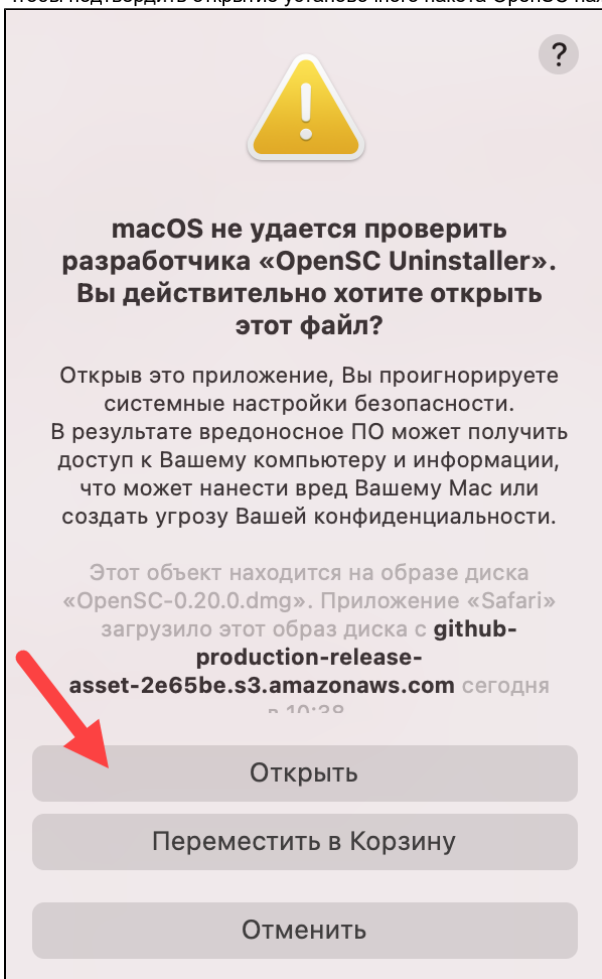
1. Запустите программу установки пакета OpenSC.
2. В окне с уведомлением о том, что автор программы является неустановленным разработчиком нажмите **Отменить**.
3. Выберите в меню **Apple** () пункт **Системные настройки (System Preferences)**.
4. Выберите настройку **Защита и безопасность (Security & Privacy)**.



5. Нажмите **Подтвердить вход**.



6. Чтобы подтвердить открытие установочного пакета OpenSC нажмите **Открыть**.



7. Снова запустите программу установки пакета OpenSC и нажмите **Продолжить**.
8. Чтобы начать процесс установки нажмите **Установить**.
9. В окне для ввода учетных данных укажите пароль пользователя и нажмите **Установить ПО**.
10. После завершения процесса установки нажмите **Заккрыть**. В результате пакет OpenSC будет установлен.
11. Если после установки пакета необходимо остановить установщик, то нажмите **Остановить**.

Для того чтобы загрузить приложение **Рутокен для macOS** перейдите по указанной ссылке:

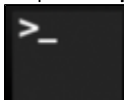
<https://www.rutoken.ru/support/download/mac/>



Для установки приложения Рутокен для macOS, в окне **Рутокен для macOS** перетащите значок **Рутокен для macOS** в папку **Application**.

Для того чтобы определить путь до библиотеки `librtpkcs11ecp.dylib`:

1. Откройте **Терминал (Terminal)**.



2. Введите команду:

```
sudo find /usr -name librtpkcs11ecp.dylib
```

3. Нажмите **Enter**. В результате в окне Терминала отобразится путь до библиотеки librtpkcs11ecp.dylib.

```
Last login: [REDACTED]
user@MacBook-Pro-user ~ % sudo find /usr -name librtpkcs11ecp.dylib
Password:
/usr/local/lib/librtpkcs11ecp.dylib
user@MacBook-Pro-user ~ %
```

Чтобы **определить название модели смарт-карты**, подключите ее к компьютеру и введите команду:

```
pkcs11-tool --module {A} -T
```

A — путь до библиотеки librtpkcs11ecp.dylib.

В разделе **token model** отобразится название модели смарт-карты.

```
[user@MacBook-Pro-user ~ % pkcs11-tool --module /usr/local/lib/librtpkcs11ecp.dylib -T
Available slots:
Slot 0 (0x0): Aktiv Rutoken ECP
token label      : Rutoken ECP <no label>
token manufacturer : Aktiv Co.
token model      : Rutoken ECP
token flags      : login required, rng, SO PIN to be changed, token initialized, PIN
initialized, user PIN to be changed
hardware version  : 20.5
firmware version  : 23.2
serial num       : 3b9a5e04
pin min/max      : 8/32
user@MacBook-Pro-user ~ %
```

Проверка работы смарт-карты в системе

Для проверки работы Рутокен ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте **Терминал (Terminal)**.



3. Введите команду:

```
pcscctest
```

4. Нажмите **Enter** и введите цифру "1".
5. Нажмите **Enter** и введите цифру "1".
6. Нажмите **Enter**.

7. Если отобразилось следующее сообщение:

```
user — -zsh — 80x24
50 73 63 C0
Testing SCardDisconnect      : Command successful.
Testing SCardReleaseContext   : Command successful.
Testing SCardEstablishContext : Command successful.
Testing SCardGetStatusChange
Please insert a working reader : Command successful.
Testing SCardListReaders      : Command successful.
Reader 01: Gemalto PC Twin Reader
Enter the reader number      : 1
Waiting for card insertion

Testing SCardConnect          : Command successful.
Testing SCardStatus            : Command successful.
Current Reader Name           : Gemalto PC Twin Reader
Current Reader State           : 0x54
Current Reader Protocol        : 0x1
Current Reader ATR Size        : 19 (0x13)
Current Reader ATR Value       : 3B 9C 97 80 11 40 52 75 74 6F 6B 65 6E 45 43
50 73 63 C0
Testing SCardDisconnect      : Command successful.
Testing SCardReleaseContext   : Command successful.

PC/SC Test Completed Successfully !
user@MacBook-Pro-user ~ %
```

Значит смарт-карта работает.

Изменение PIN-кода смарт-карты

Для изменения PIN-кода введите команду:

```
pkcs11-tool --module {A} --login --pin {B} --change-pin --new-pin {C}
```

A — путь до библиотеки libtpkcs11ecp.dylib.

B — текущий PIN-код устройства.

C — новый PIN-код устройства.

```
Last login: Sat Nov 7 12:08:06 on ttys000
user@MacBook-Pro-user ~ % pkcs11-tool --module /usr/local/lib/libtpkcs11ecp.dylib ]
--login --pin 12345678 --change-pin --new-pin 87654321
Using slot 0 with a present token (0x0)
PIN successfully changed
user@MacBook-Pro-user ~ %
```

В результате PIN-код устройства будет изменен.

Работа со смарт-картой на мобильном устройстве

В ОС Android

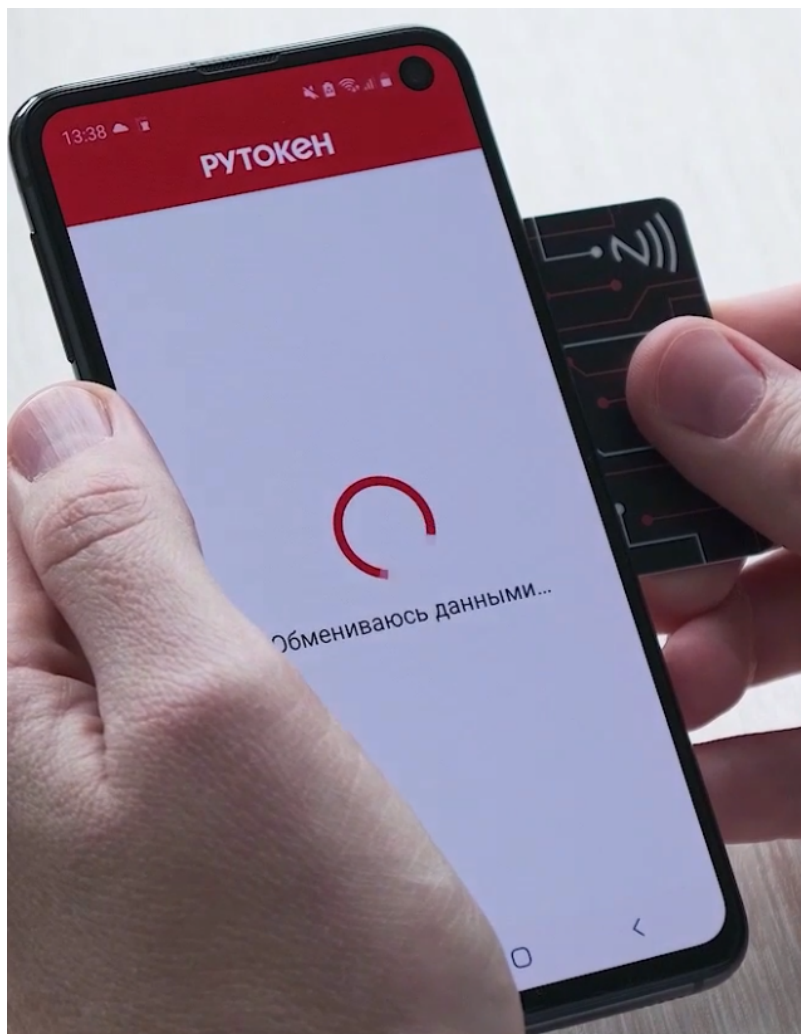
Работа со смарт-картой возможна, если выполняются два условия:



- у мобильного устройства есть NFC-модуль;
- на мобильном устройстве включена функция NFC.

При работе со смарт-картой на мобильном устройстве отображается специальное окно с сообщением, которое предупреждает, что карту необходимо приложить.

Смарт-карта прикладывается к мобильному устройству следующим образом:



Смарт-карту необходимо держать так до того момента, пока на экране смартфона отобразится сообщение о том, что работа с картой NFC завершена.

Установка приложения Панель управления Рутокен на Android

Приложение Панель управления Рутокен дает возможность:

- просматривать информацию о подключенных устройствах Рутокен;
- изменять PIN-коды и метки устройств.

Для установки приложения Панель управления Рутокен:

1. Запустите **Google Play Маркет** на устройстве.
2. В строке поиска введите название приложения и нажмите **ENTER**.
3. Выберите **Панель управления Рутокен** в списке результатов поиска. Откроется страница с подробными сведениями о приложении.



4. Нажмите **Установить**.
5. Ознакомьтесь со списком прав, которые необходимы приложению.
6. Если вы согласны предоставить приложению требуемые права, нажмите **Принять**. Начнется загрузка и установка приложения.
7. Если вы не согласны предоставить приложению требуемые права, нажмите **Назад**. В этом случае установка приложения будет отменена.

Подключение Рутокена

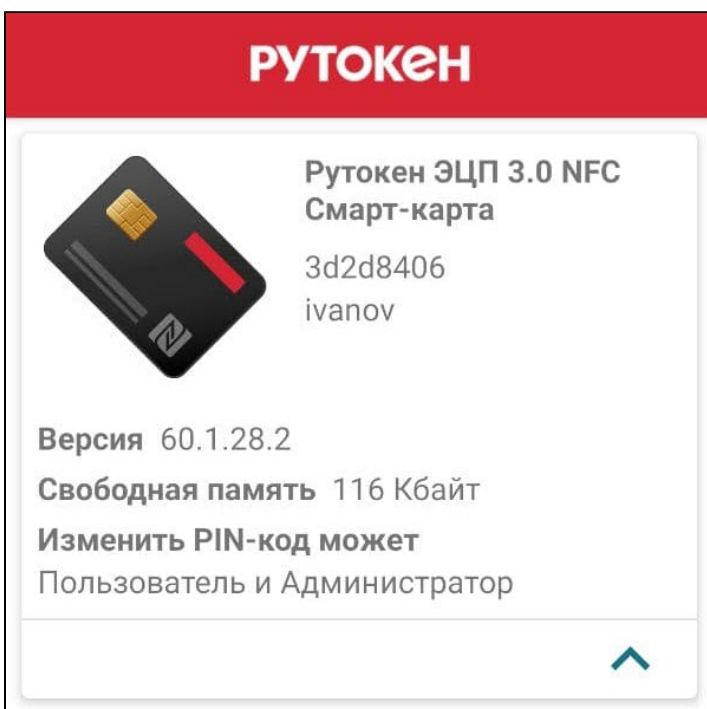
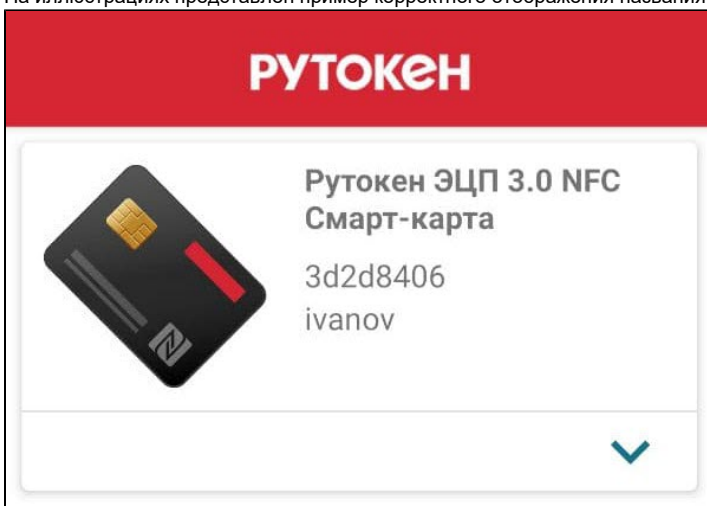
Для подключения дуальной смарт-карты с поддержкой NFC необходимо мобильное устройство с NFC-модулем.

Для проверки отображения названия дуальной смарт-карты в приложении Панель управления Рутокен:

1. Запустите приложение **Панель управления Рутокен**.



2. Приложите Рутокен ЭЦП 3.0 NFC к мобильному устройству.
3. В окне приложения, в карточке устройства нажмите на стрелочку. Откроется окно с основной информацией о смарт-карте. На иллюстрациях представлен пример корректного отображения названия смарт-карты и информации о ней.



Работа с приложением Панель управления Рутокен

Изменение PIN-кода

Для изменения PIN-кода Пользователя или Администратора в приложении Панель управления Рутокен:

1. Подключите смарт-карту к устройству на Android.
2. Запустите приложение **Панель управления Рутокен**.



3. Нажмите на карточку устройства.



4. Чтобы открыть меню, нажмите в правом верхнем углу на значок
5. Выберите пункт меню **Сменить PIN-код**. В приложении отобразится окно для ввода нового PIN-кода.
6. Перейдите на вкладку **Пользователь** (для ввода нового PIN-кода Пользователя) или **Администратор** (для ввода нового PIN-кода Администратора).
7. Введите текущий PIN-код.
8. Два раза новый PIN-код

9. Нажмите **ОК**.

Изменение метки устройства Рутокен

Для изменения метки устройства:

1. Подключите Рутокен к устройству на Android.
2. Запустите приложение **Панель управления Рутокен**.

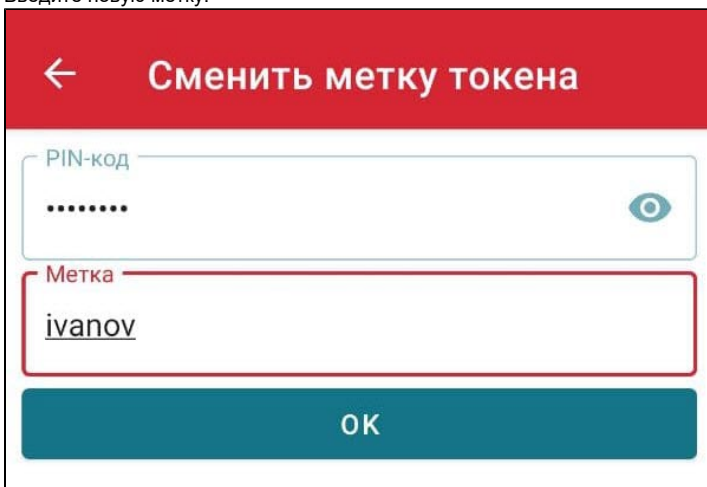


3. Нажмите на карточку устройства.



4. Чтобы открыть меню, нажмите в правом верхнем углу на значок
5. Выберите пункт меню **Сменить метку токена**. В приложении отобразится окно для ввода PIN-кода Пользователя и новой метки.
6. Введите PIN-код Пользователя.

7. Введите новую метку.



8. Нажмите **ОК**.

Разблокировка PIN-кода

Для разблокировки PIN-кода Пользователя:

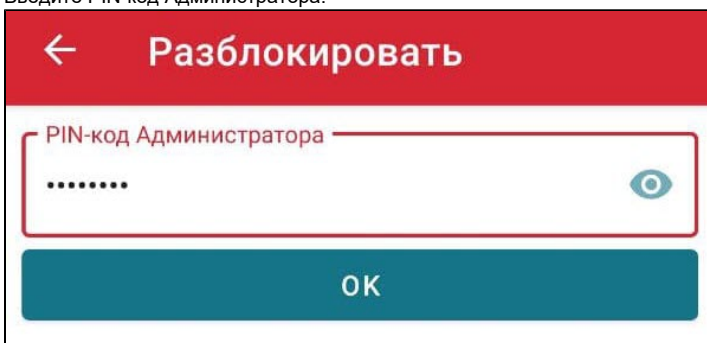
1. Подключите Рутокен к устройству на Android.
2. Запустите приложение **Панель управления Рутокен**.



3. Нажмите на карточку устройства.



4. Чтобы открыть меню нажмите в правом верхнем углу на значок.
5. Выберите пункт меню **Разблокировать**. В приложении отобразится окно для ввода PIN-кода Администратора и кнопка для разблокировки PIN-кода Пользователя.
6. Введите PIN-код Администратора.



7. Нажмите **ОК**.

В iOS

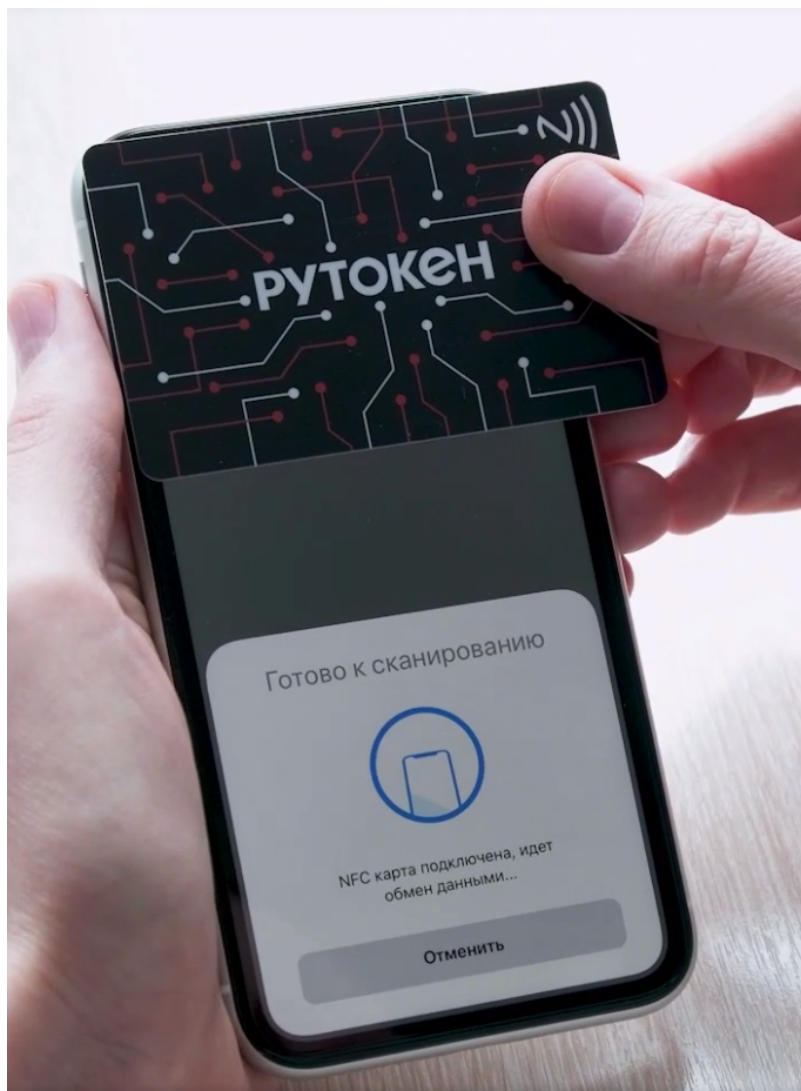
Работа со смарт-картой возможна если соблюдаются два условия:



- версия iOS от 13 и выше;
- у вас одна из следующих моделей iPhone: XR; XS; 11; 11 Pro; 11 Pro Max; 12; 12 mini; 12 Pro; 12 Pro Max.

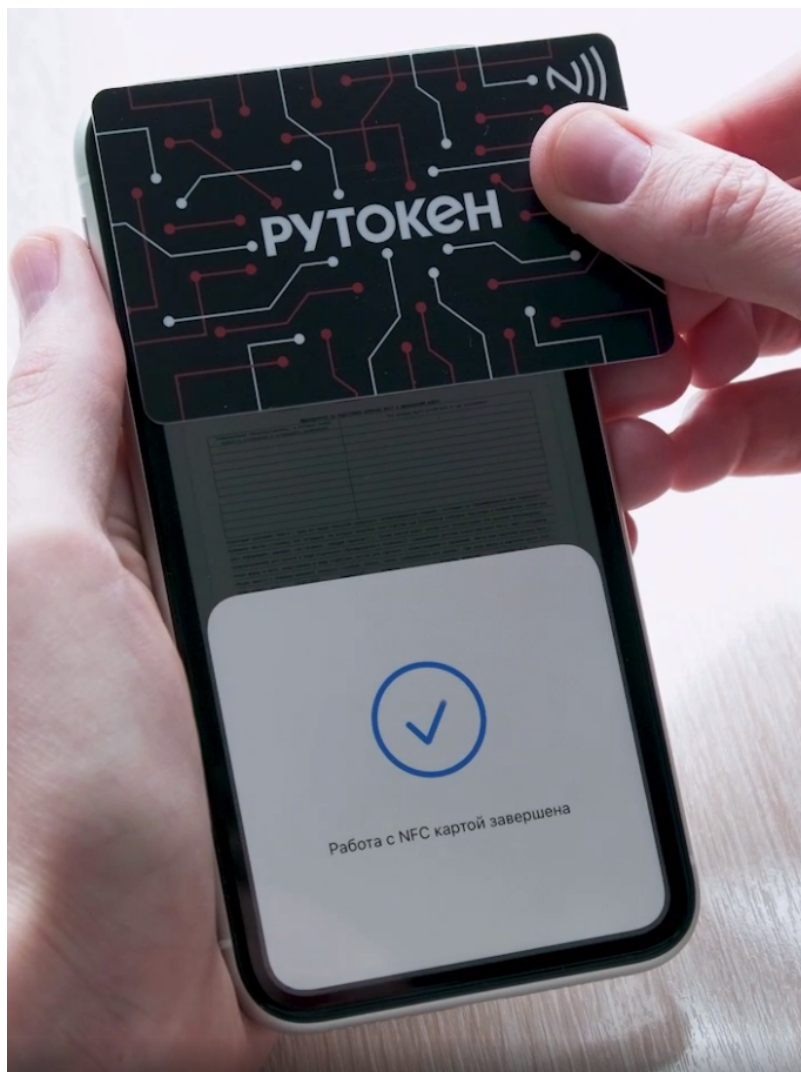
При работе со смарт-картой на мобильном устройстве отображается специальное окно с сообщением, которое предупреждает, что карту необходимо приложить.

Смарт-карта прикладывается к мобильному устройству следующим образом:



Верхняя часть смартфона должна находиться в нескольких миллиметрах от смарт-карты.

Смарт-карту необходимо держать так до того момента, пока на экране смартфона отобразится сообщение о том, что работа с картой NFC завершена:



Процесс подписания документа в приложении состоит из следующих шагов:

1. Откройте приложение, в котором необходимо подписать документ.
2. Откройте документ.

3. Нажмите Подписать.

Документ для подписи

НАРЯД-ДОПУСК № 289731931723 для работы в электроустановках

Организация: Филиал «ЗЭС» – ПАО «МЭСК»
 Подразделение: Истринский РЭС

Ответственному руководителю работ Ареškova A.C. (гр. IV) допускаящему Астахов A. B.
(фамилия, инициалы, группа) (фамилия, инициалы, группа)

Производителю работ Гурьянов A.И. наблюдающему _____
(фамилия, инициалы, группа) (фамилия, инициалы, группа)

с членами бригады Суев В. В. (гр. IV), Сокин В.И., Лексаков В. В. (гр. V), Суханов Д. В. (гр. IV), Лихоузов A.A. Ткаченко Г. М. (гр. IV), Вульга A.И., Лебедев И. A. (гр. IV), Бдин Н.М., Молчанов Д.А., Астахов A. B.
(фамилия, инициалы, группа) (фамилия, инициалы, группа)

поручается _____
(фамилия, инициалы, группа)

Работу начать: дата 14.05.2019 время 10:56 Работу закончить: дата 31.05.2019 время 10:53

Мероприятия по подготовке рабочих мест к выполнению работ

Наименование электроустановки, в которой нужно провести отключение и установить заземление	Что должно быть отключено и где заземлено
1	2

Отдельные указания: Книга – один из видов печатной продукции: неперiodическое издание, состоящее из сброшюрованных или отдельных бумажных листов (страниц) или тетрадей, на которых нанесена типографским или рукописным способом текстовая и графическая (иллюстрация) информация, имеющая, как правило, твердый переплет[1]. Также книгой может называться литературное или научное произведение, предназначенное для печати в виде отдельного сброшюрованного издания[2]. Современные детские книги-картинки могут иметь нетрадиционную форму и быть представлены в виде отдельных листов или карточек с иллюстрациями и заданиями. Листы или карточки должны быть с обложки вместе с помощью внешнего элемента (скрепки, кольца, папки, суперобложки или зажима). При этом листы и карточки могут быть

Наряд выдал: дата 15.05.2019 время 12:47 Подпись _____ Фамилия, инициалы Гурьянов A.И.
 Наряд принял по: дата _____ время _____ Подпись _____ Дата _____ время _____

Регистрация целевого инструктажа, проводимого выдающим наряд

Целевой инструктаж провел	Целевой инструктаж получил
Работник, выдавший наряд	Гурьянов A.И. (фамилия, инициалы)
	Ответственный руководитель работ (производитель работ, наблюдающий)
	Ареškova A.C. (гр. IV) (фамилия, инициалы)
	(подпись)

Разрешение на подготовку рабочих мест и на допуск к выполнению работ

Разрешение на подготовку рабочих мест и на допуск к выполнению работ выдал (должность, фамилия или подпись)	Дата, время	Подпись работника, получившего разрешение на подготовку рабочих мест и на допуск к выполнению работ
1	2	3
<u>_____</u>	<u>14.04</u>	<u>Астахов A. B.</u>
		<u>Лихоузов A.A.</u>
		<u>Сокин В.И.</u>
		<u>Лебедев И. A. (гр. IV)</u>
		<u>Суев В. В. (гр. IV)</u>
		<u>Лексаков В. В. (гр. V)</u>

Выбрать файл

Подписать

4. Введите PIN-код Пользователя и нажмите **Продолжить**.

Введите PIN-код

PIN-код

Продолжить

5. Приложите смарт-карту и дождитесь окончания процесса подписания документа. В результате документ будет подписан.

Технические характеристики смарт-карты Рутокен ЭЦП 3.0 NFC

Критерий	Характеристика смарт-карты
<i>Основные характеристики</i>	
Аппаратная часть	Защищенный микроконтроллер со встроенной энергозависимой памятью
EEPROM память	128 Кбайт
Габаритные размеры	85,6 x 53,98 x 0,76 мм
Масса	5,5 г
Поддерживаемые ОС	• Microsoft Windows 10/8.1/2019/2016/2012R2/8/2012/7/2008R2/Vista/2008 • GNU/Linux (в том числе отечественные) • Apple macOS 10.15/10.14/10.13/10.12/10.11/10.10/10.9 • Android 5 и новее • iOS 13 и новее • Аврора
<i>Поддерживаемые интерфейсы и стандарты</i>	
PKCS#11 версии 2.20, включая российский профиль (2.30 draft)	да
Microsoft Crypto API	да
PC/SC	да
Microsoft Smartcard API	да
USB CCID (работа без установки драйверов)	да
ISO/IEC 7816	• ISO/IEC 7816-3, протокол T=0 и T=1 для контактной микросхемы, • ISO 14443 (NFC) для бесконтактной микросхемы.
Криптопровайдер	собственный Crypto Service Provider

Сертификаты X.509 версии 3 на уровне программного обеспечения	да
<i>Криптографические возможности</i>	
Поддержка алгоритма ГОСТ 28147-89	да, аппаратная реализация
Поддержка алгоритма ГОСТ Р 34.12-2015 (Магма)	да, аппаратная реализация
Поддержка алгоритма ГОСТ Р 34.12-2015 (Кузнечик)	да, аппаратная реализация
Режим шифрования	- простая замена, - гаммирование, - гаммирование с обратной связью
Режим выработки имитовставки	да
Генерация ключей шифрования	да
Импорт ключей шифрования	нет
Запрет экспорта ключей шифрования	да
Поддержка алгоритма ГОСТ Р 34.10-2012	да, аппаратная реализация
Формирование и проверка ЭП	да
Генерация ключевых пар	да, с проверкой качества
Импорт ключевых пар	да, с помощью ключа эмитента
Запрет экспорта ключевых пар	да
Срок действия закрытых ключей	до 3 лет
Размер закрытого ключа	256 и 512 бит
Поддержка алгоритма ГОСТ 34.11-2012 (256 и 512 бит)	аппаратная реализация
Вычисление значения хэш-функции	да, в т. ч. с возможностью последующего формирования ЭП
Формирование и проверка ЭП	да
Генерация ключевых пар	да, с проверкой качества
Импорт ключевых пар	да
Запрет экспорта ключевых пар	да
Срок действия закрытых ключей	до 3 лет
Поддержка алгоритма ГОСТ 34.11-94	аппаратная реализация
Выработка сессионных ключей (ключей парной связи)	да - по схеме VKO GOST R 34.10-2001 согласно RFC 4357 - по схеме VKO GOST R 34.10-2012 согласно RFC 7836
Расширение по схеме EC El-Gamal	да
Поддержка алгоритма RSA	аппаратная реализация расшифрования и подписи (RSA-1024, RSA-2048, RS A-4096)
Формирование электронной подписи	да
Генерация ключевых пар	да, с проверкой качества
Импорт ключевых пар	да
Запрет экспорта ключевых пар	да

Размер ключей	до 4096 бит
Поддержка алгоритма ECDSA	да, кривые secp256k1 и secp256r1
Поддержка алгоритмов DES (3DES), AES, RC2, RC4, MD4, MD5, SHA-1, SHA-256	хранение экспортируемых ключей в EF, SHA-1, SHA-256, MD5 в PKCS#11, RC4, MD4, MD5, SHA-1, SHA-256, 3DES, AES в minidriver
Формирование электронной подписи	да
Генерация ключевых пар	да, с проверкой качества
Импорт ключевых пар	да
Работа с СКЗИ «КриптоПро 5.0» по протоколу защиты канала SESPAKE (ФКН2).	да
Сведения о сертификации	
Наличие сертификата ФСТЭК	да
Наличие сертификата ФСБ	да
Файловая система	
Файловая структура	встроенная, по стандарту ISO/IEC 7816-4
Тип размещения файловых объектов в памяти (архитектура файловой системы)	использование File Allocation Table (FAT)
Количество папок и уровень их вложенности	уровень ограничен объемом свободной памяти
Число файловых объектов внутри папки	до 255 включительно
Хранение ключевой информации	- использование файлов Rutoken Special File (RSF-файлов) для хранения ключей шифрования, сертификатов; - использование predetermined папок для хранения разных видов ключевой информации с автоматическим выбором нужной папки при создании и использовании RSF-файлов
Запрет экспорта закрытых и симметричных ключей	да
Шифрование файловой системы	да, прозрачное, алгоритм ГОСТ 28147-89, уникальный ключ шифрования для каждого экземпляра устройства
Дополнительно	использование Security Environment для удобной настройки параметров криптографических операций
Аутентификация и конфиденциальность	
Двухфакторная аутентификация	да, предъявление токена + ввод PIN-кода
Уровни доступа	- Гость - Пользователь - Администратор
Разграничение доступа к файловым объектам в соответствии с уровнем доступа	да
Ограничение числа попыток ввода PIN-кода	да, настраиваемое
Поддержка PIN-кодов	- глобальные PIN-коды: Администратора и Пользователя, - локальные PIN-коды (для защиты конкретных объектов в памяти устройства, например, контейнеров сертификатов) - Настраиваемые аппаратные политики качества PIN-кодов
Ограничение минимального размера PIN-кода	да, настраивается независимо для любого PIN-кода

Дополнительно	• поддержка комбинированной аутентификации: ○ аутентификация по глобальным PIN-кодам ○ аутентификация по глобальным PIN-кодам в сочетании с аутентификацией по локальным PIN-кодам. • возможность одновременного контроля прав доступа, заданных до 7-ю локальными PIN-кодами. • индикация факта смены глобальных PIN-кодов с умалчиваемых на оригинальные.
Возможность встраивания радиочастотной метки	да
Поддерживаемые типы меток	Работа с системами контроля и управления доступом, поддерживающими протокол NFC
<i>Встроенный контроль и индикация</i>	
Контроль целостности прошивки	да
Контроль целостности системных областей памяти	да
Проверка целостности RSF-файлов перед использованием	да
Типы счетчиков	• счетчик изменений файловой системы • счетчик изменений PIN-кодов • счетчики последовательных неудачных попыток ввода PIN-кодов • счетчик успешных операций электронной подписи
Проверка правильности функционирования криптографических алгоритмов	да
Режимы работы светодиодного индикатора	• готовность к работе • выполнение операции • нарушение в системной области памяти