Рутокен ЭЦП в операционных системах macOS

- Общая информация
- Определение названия модели USB-токена
- Проверка корректности подключения считывателя для смарт-карт к компьютеру
- Определение названия модели смарт-карты
- Проверка работы Рутокен ЭЦП в системе
- Проверка наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП
    - Начиная с версии 10.15
    - До версии 10.15
- Проверка наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП
- Изменение PIN-кода Рутокен ЭЦП
- Решение проблем с Рутокен ЭЦП в системе

Общая информация

Устройства семейства Рутокен ЭЦП используются для безопасного хранения и предъявления персональной информации: ключей шифрования, сертификатов, лицензий, удостоверений и других данных.

Для работы с USB-токеном подключите его к USB-порту компьютера.

Для работы со смарт-картой вставьте ее в считыватель для смарт-карт и подключите считыватель к USB-порту компьютера.

Чтобы проверить корректность работы Рутокен ЭЦП в операционных системах macOS необходимо выполнить действия, указанные в данной инструкции.

Если вы используете для устройства стандартный PIN-код (12345678), то рекомендуется его изменить на более сложный.

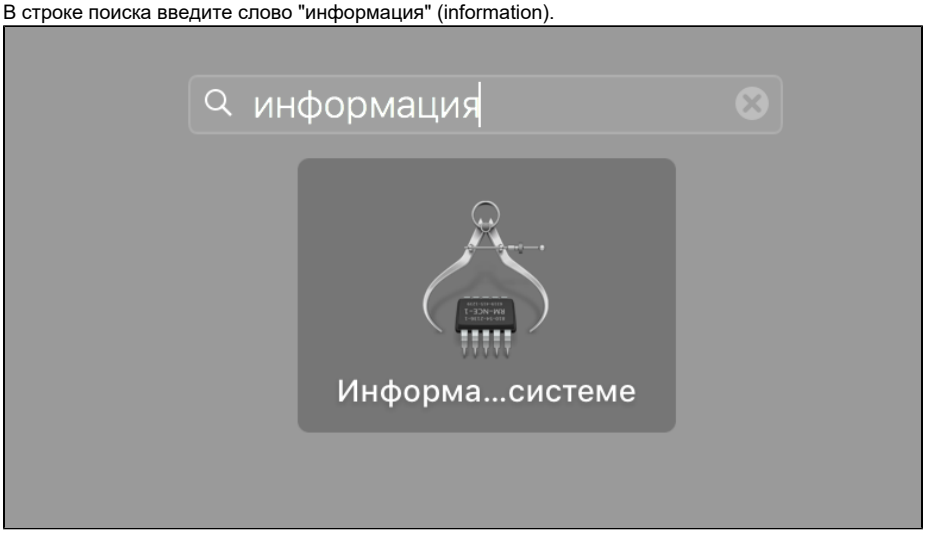
Определение названия модели USB-токена

Если вы работаете со смарт-картой, то выполнять процедуру, описанную в этом разделе, не надо.

Для определения названия модели USB-токена:

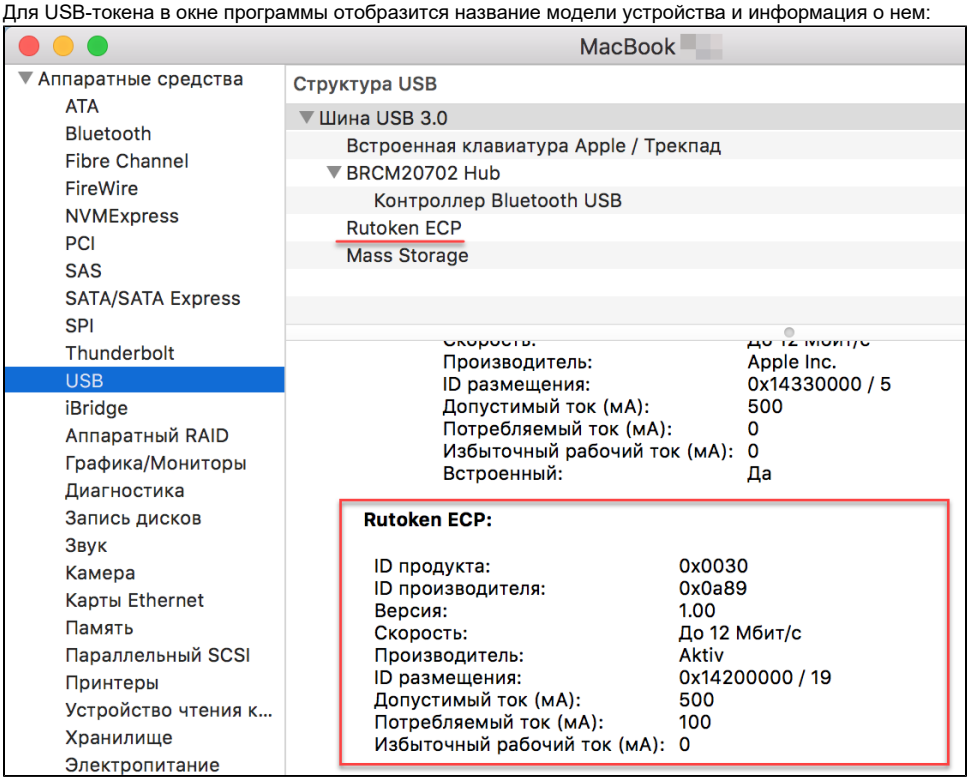
1. Подключите USB-токен к компьютеру
2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "информация" (information).



4. Откройте программу **Информация о системе (System Information)**.

5. На боковой панели окна программы выберите пункт **USB**.
6. Для USB-токена в окне программы отобразится название модели устройства и информация о нем:



Проверка корректности подключения считывателя для смарт-карт к компьютеру

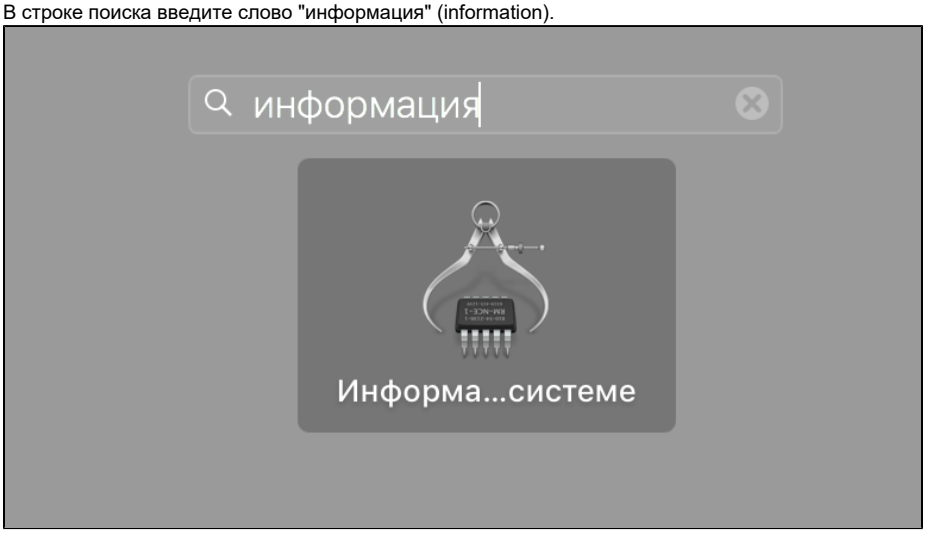
Если вы работаете с USB-токеном, то выполнять процедуру, описанную в этом разделе, не надо.

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

1. Подключите считыватель для смарт-карт к компьютеру и вставьте в него смарт-карту

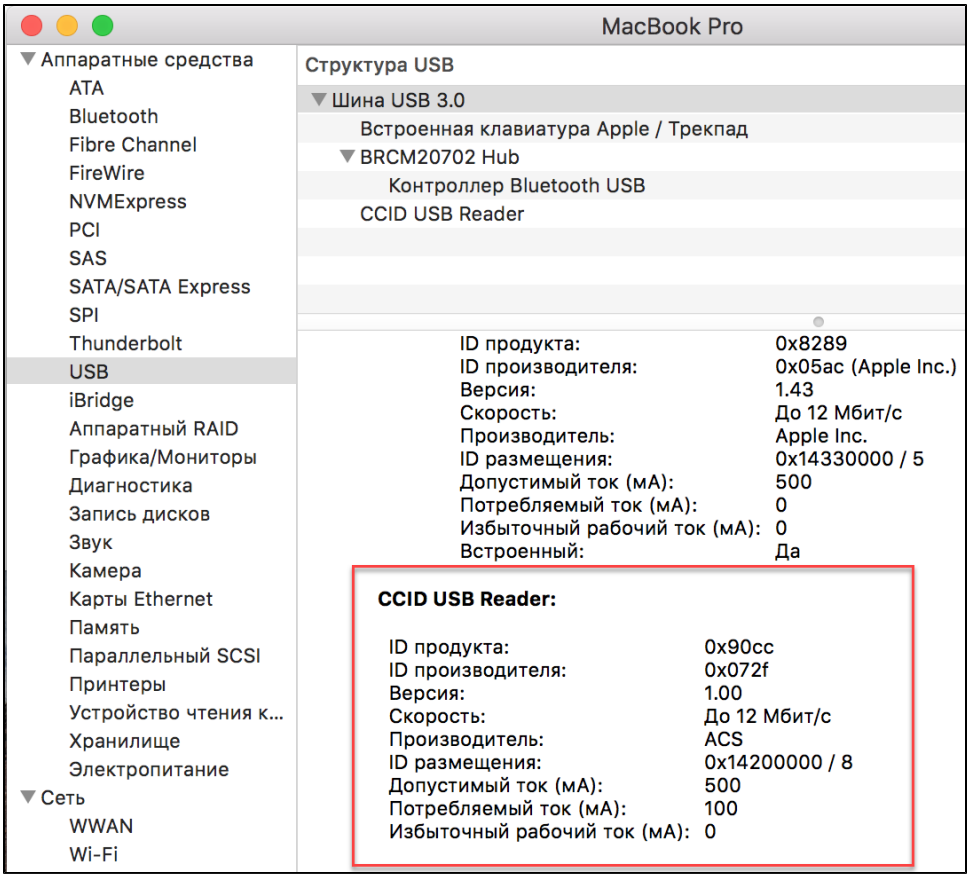
2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "информация" (information).



4. Откройте программу **Информация о системе (System Information)**.

5. На боковой панели окна программы выберите пункт **USB**.
6. 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

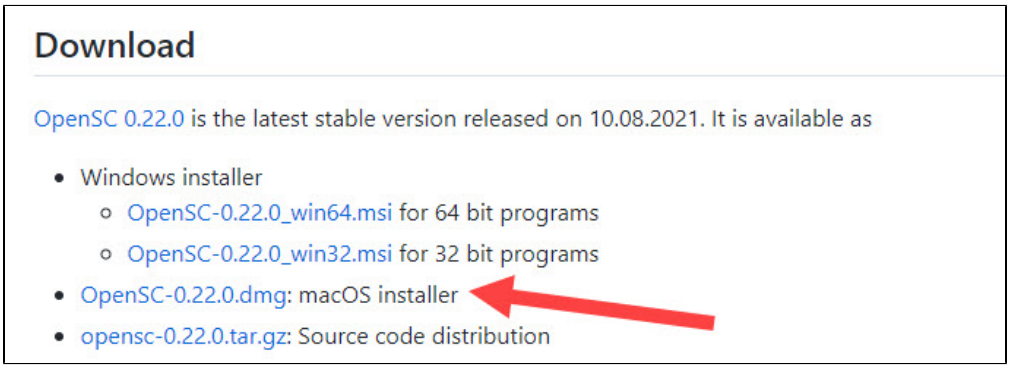
Если вы работаете с USB-токеном, то выполнять процедуру, описанную в этом разделе, не надо.

Перед запуском процесса определения названия модели смарт-карты:

- загрузите и установите пакет **OpenSC**;
- загрузите и установите библиотеку **PKCS#11**;
- определите путь до библиотеки **librtpkcs11ecp.dylib**.

Актуальная версия установочного пакета OpenSC доступна по ссылке:

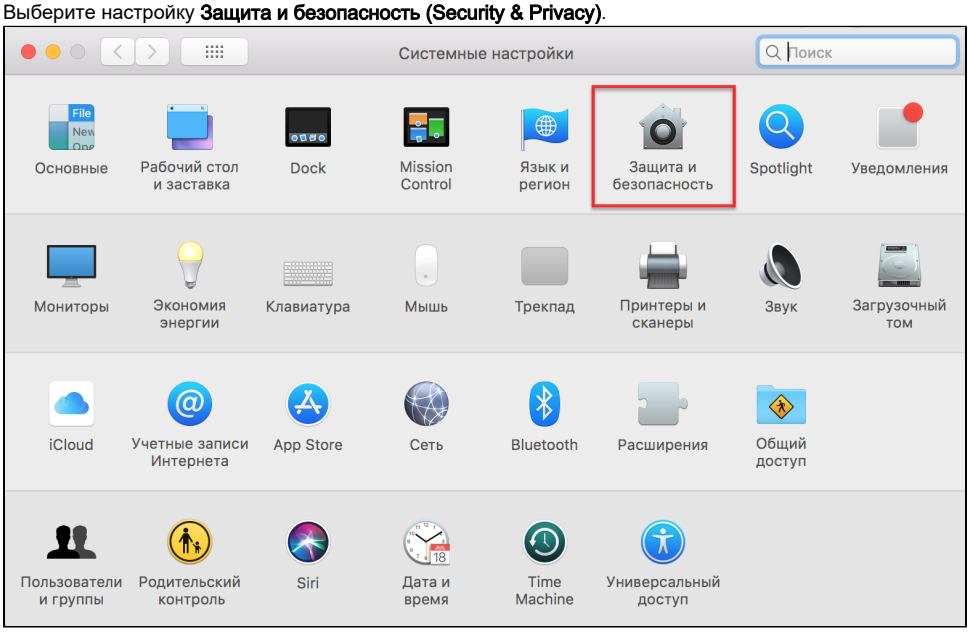
https://github.com/OpenSC/OpenSC/wiki



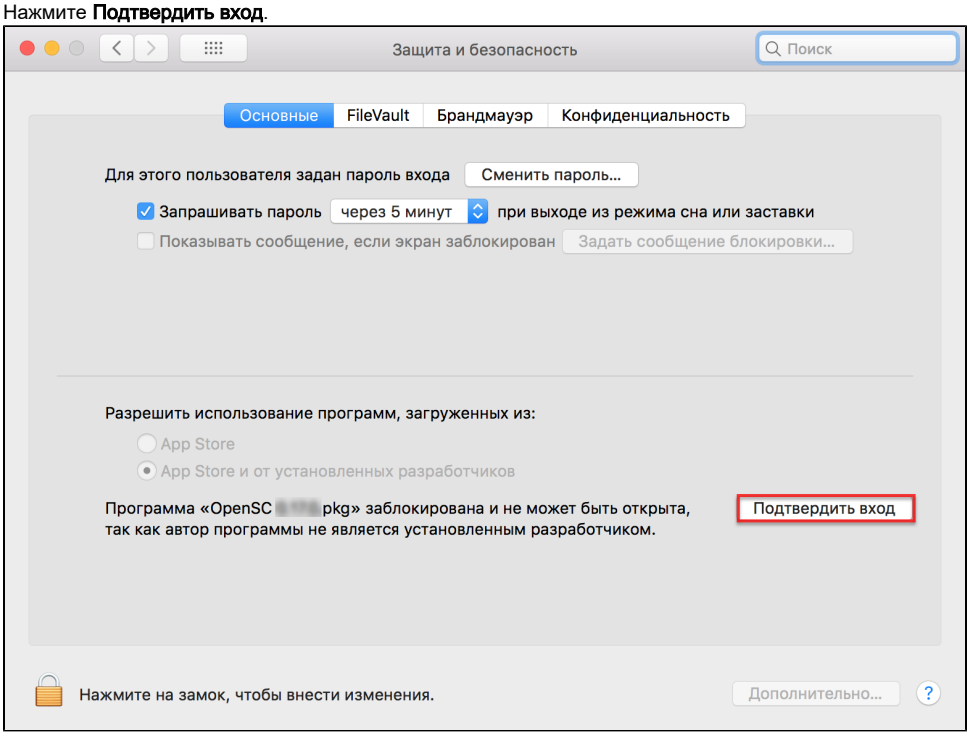
Для установки пакета OpenSC:

1. Запустите программу установки пакета OpenSC.
2. В окне с уведомлением о том, что автор программы является неустановленным разработчиком нажмите **OK**.

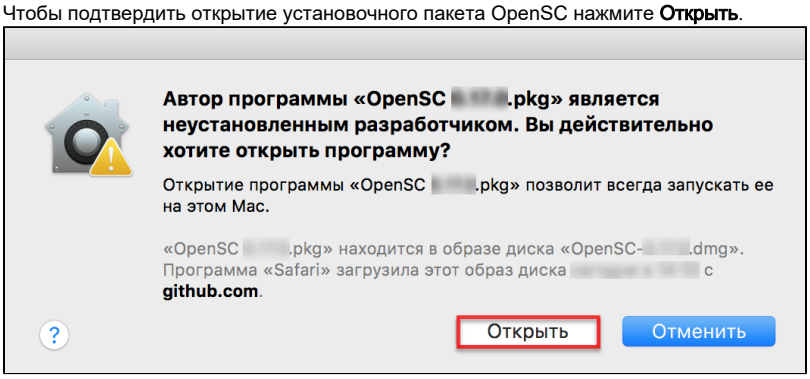
3. Выберите в меню **Apple** ( ) пункт **Системные настройки (System Preferences)**.
4. Выберите настройку **Защита и безопасность (Security & Privacy)**.



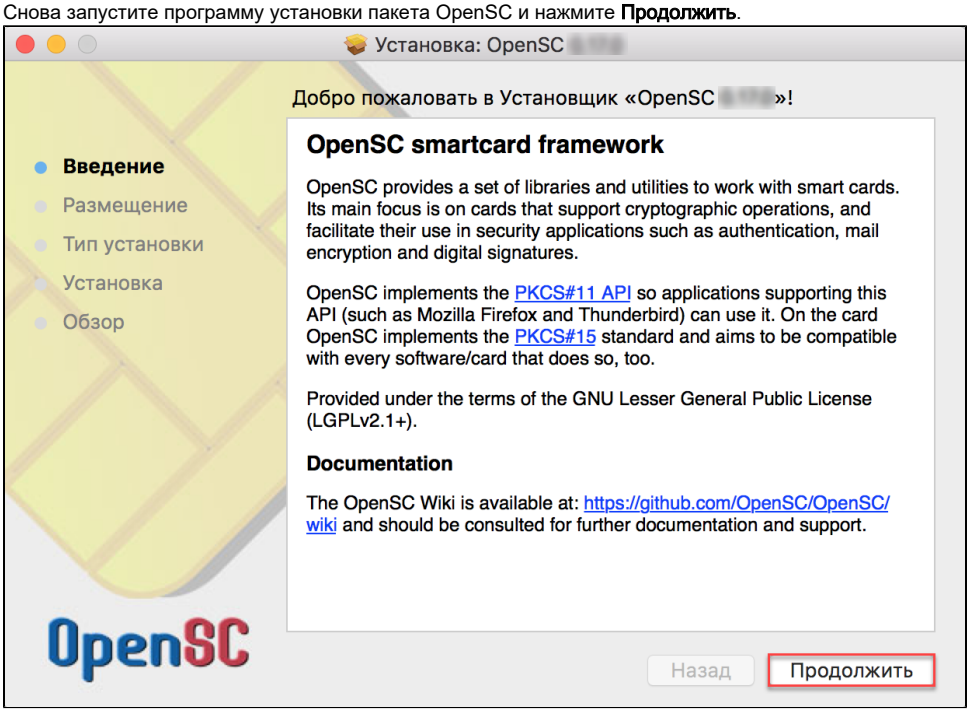
5. Нажмите **Подтвердить вход**.



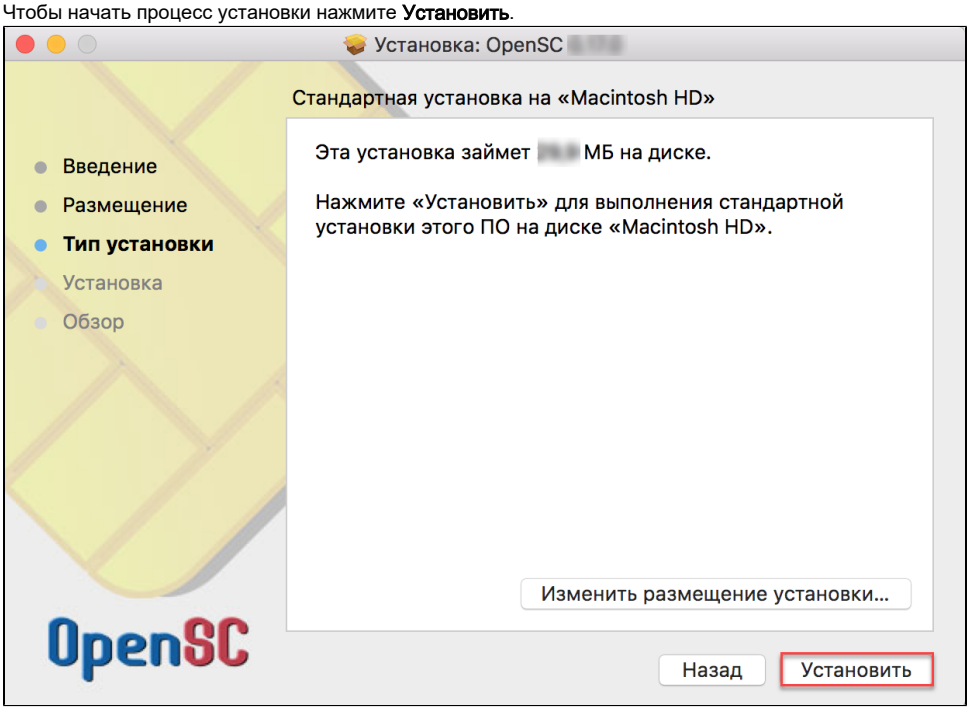
6. Чтобы подтвердить открытие установочного пакета OpenSC нажмите **Открыть**.



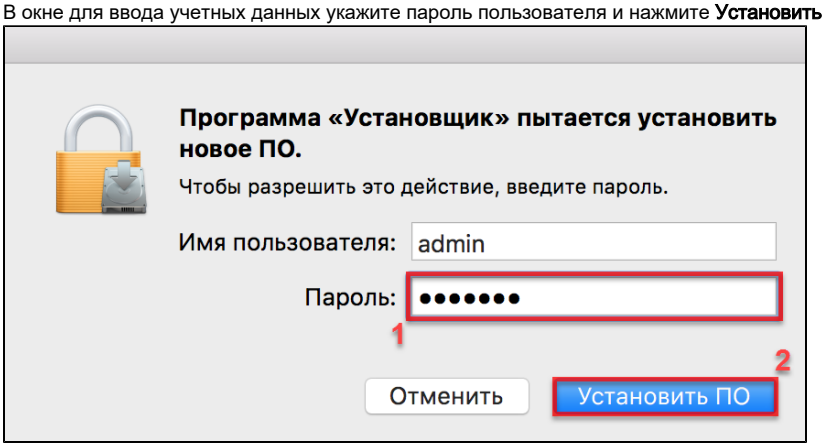
7. Снова запустите программу установки пакета OpenSC и нажмите **Продолжить**.



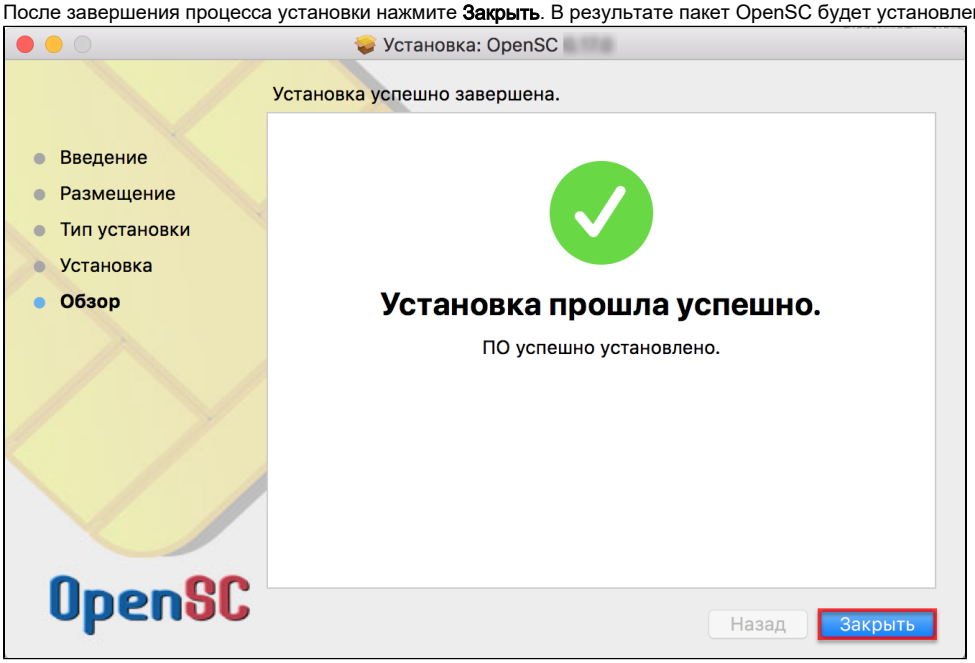
8. Чтобы начать процесс установки нажмите **Установить**.



9. В окне для ввода учетных данных укажите пароль пользователя и нажмите **Установить ПО**.

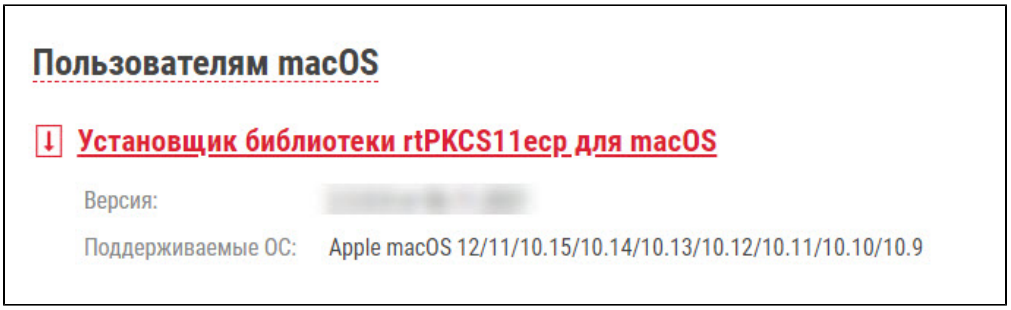


10. После завершения процесса установки нажмите **Закрыть**. В результате пакет OpenSC будет установлен.



11. Если после установки пакета необходимо остановить установщик, то нажмите **Остановить**.

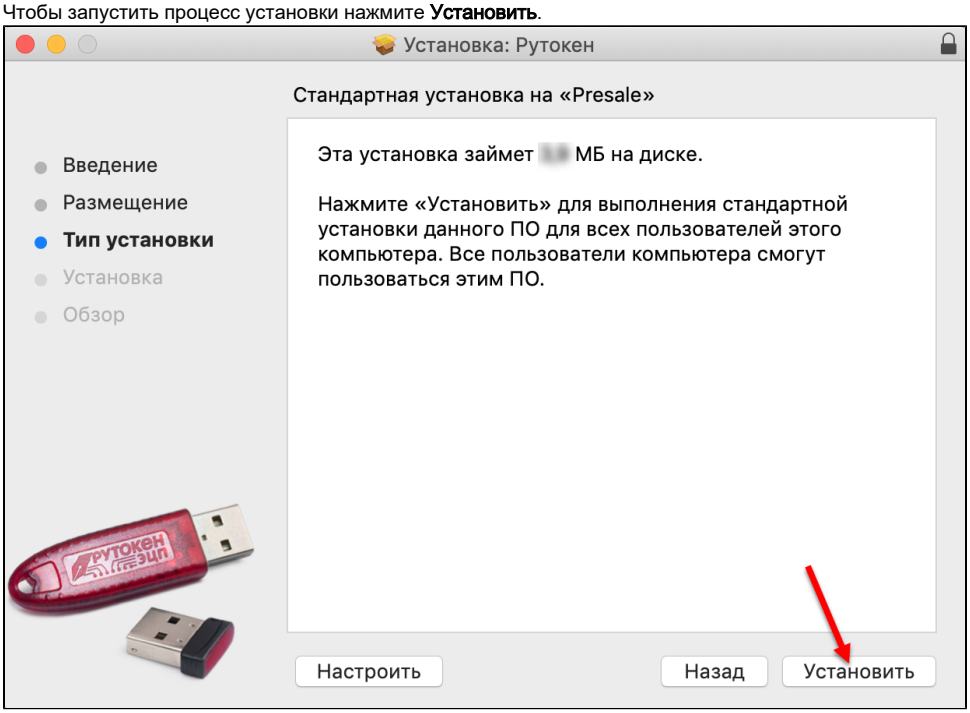
Для того чтобы загрузить библиотеку PKCS#11 перейдите по указанной ссылке и выберите необходимую версию:
https://www.rutoken.ru/support/download/pkcs/



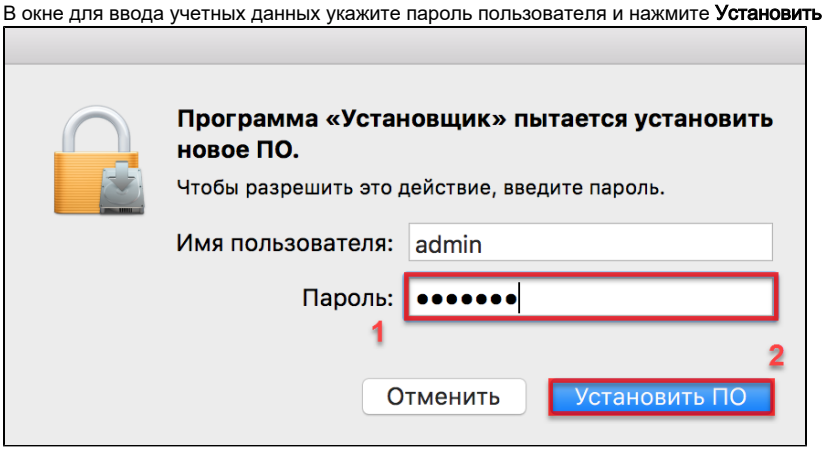
Для установки библиотеки PKCS#11:

1. Запустите программу установки библиотеки PKCS#11 и нажмите **Продолжить**.

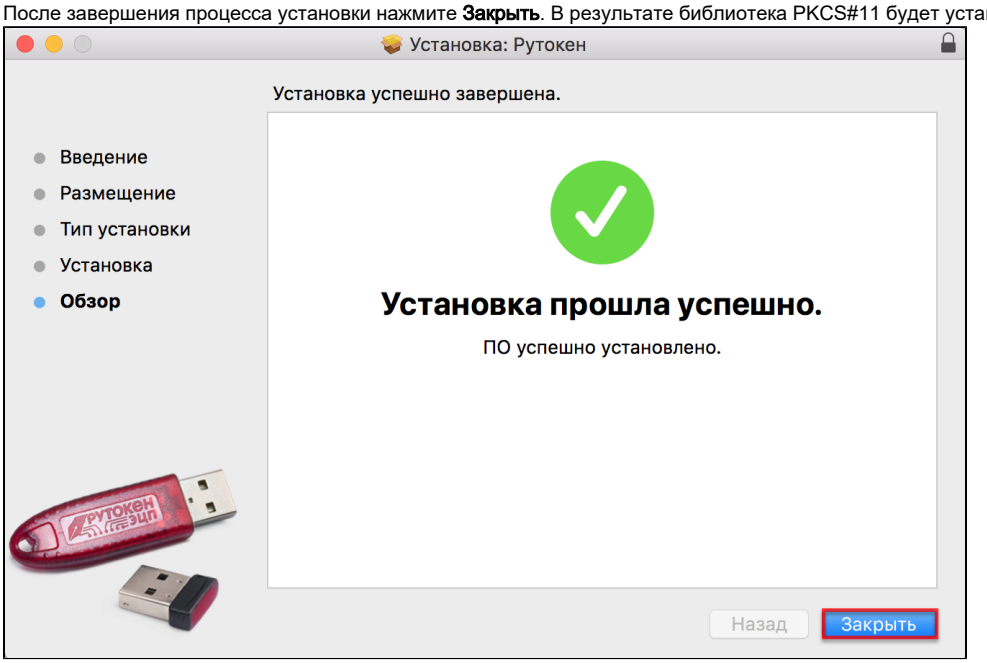
2. Чтобы запустить процесс установки нажмите **Установить**.



3. В окне для ввода учетных данных укажите пароль пользователя и нажмите **Установить ПО**.



4. После завершения процесса установки нажмите **Закрыть**. В результате библиотека PKCS#11 будет установлена.

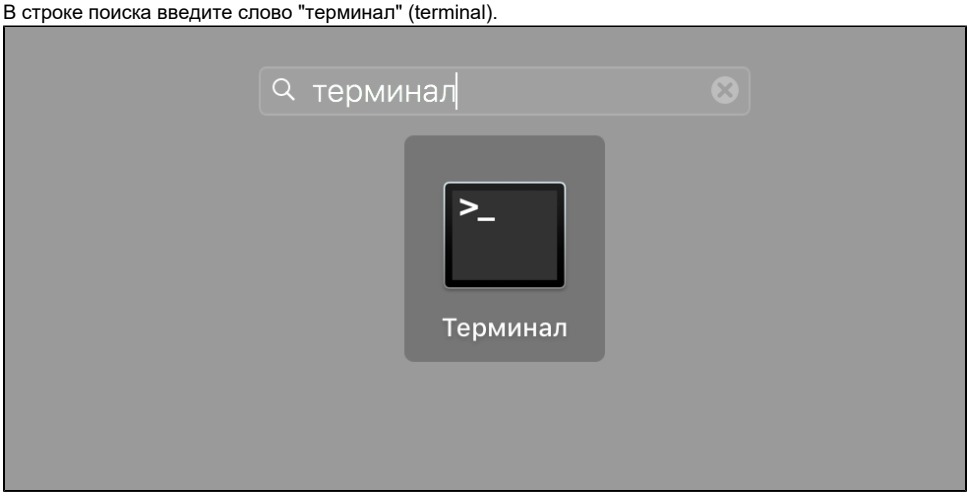


5. Если после установки библиотеки необходимо остановить установщик, то нажмите **Остановить**.

Для того чтобы определить путь до библиотеки librtpkcs11ecp.dylib:

1. Откройте программу **Launchpad**.

2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал (Terminal)**.

4. Введите команду:

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

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

```
android-cb449385bb8d1615:~ admin$ sudo find /usr -name librtpkcs11ecp.dylib
Password:
/usr/local/lib/pkcs11/librtpkcs11ecp.dylib
/usr/local/lib/librtpkcs11ecp.dylib
```

Чтобы **определить название модели смарт-карты** введите команду:

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

A — путь до библиотеки librtpkcs11ecp.dylib.

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

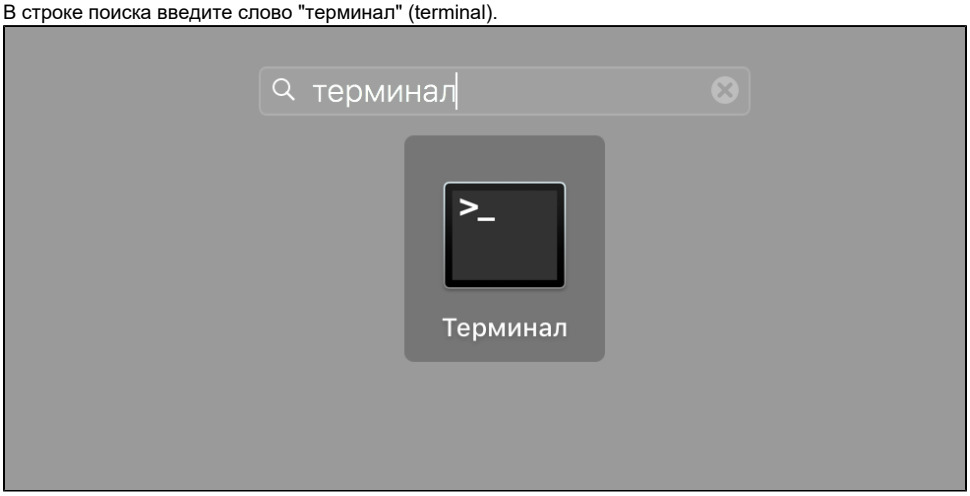
```
android-cb449385bb8d1615:~ admin$ pkcs11-tool --module /usr/local/lib/librtpkcs11ecp.dylib -T
Available slots:
Slot 0 (0x0): ACS ACR 38U-CCID
  token label        : Rutoken ECP <no label>
  token manufacturer : Aktiv Co.
  token model        : Rutoken ECP SC
  token flags        : login required, rng, SO PIN to be changed, token initialized, PIN initialized, user PIN to be changed
  hardware version   : 54.2
  firmware version   : 18.0
  serial num         : 332882eb
  pin min/max        : 6/32
```

Проверка работы Рутокен ЭЦП в системе

Для проверки работы Рутокен ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "терминал" (terminal).

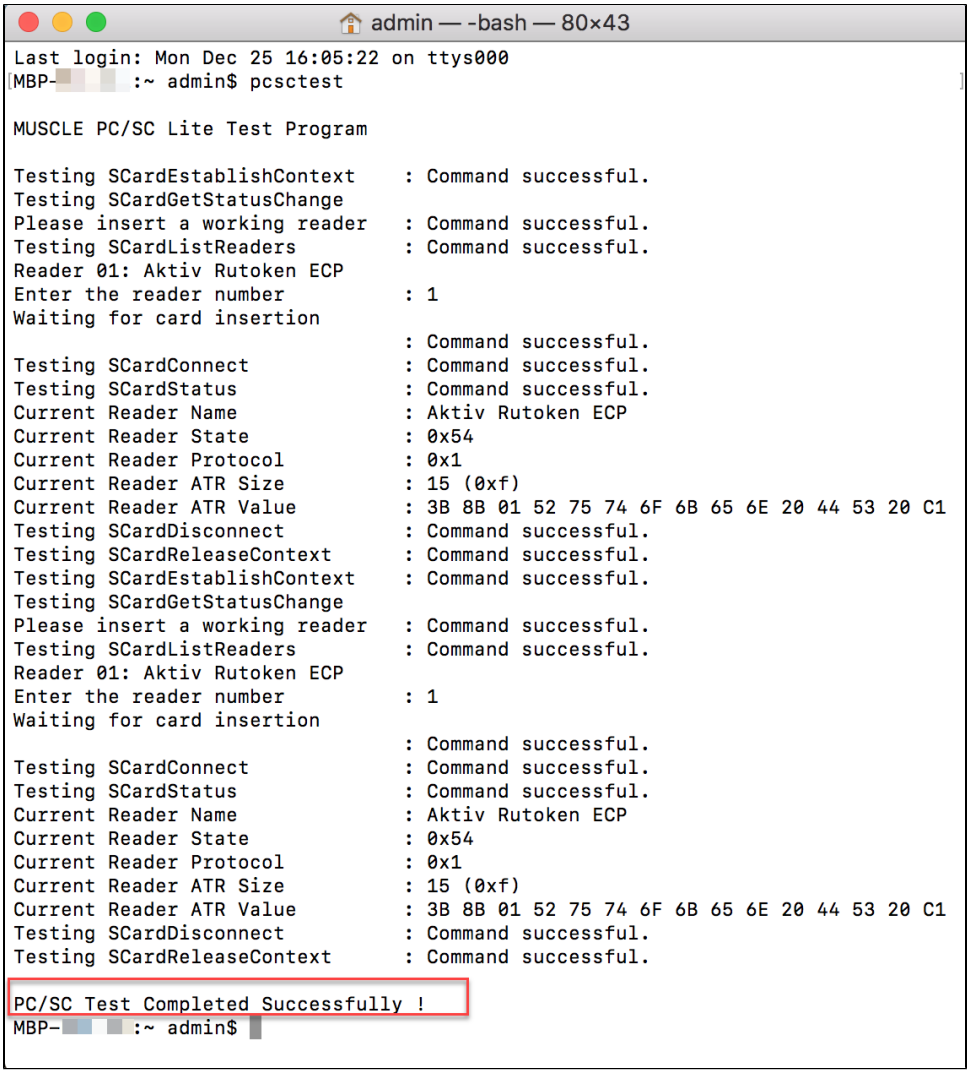


4. Откройте **Терминал (Terminal)**.

5. Введите команду:

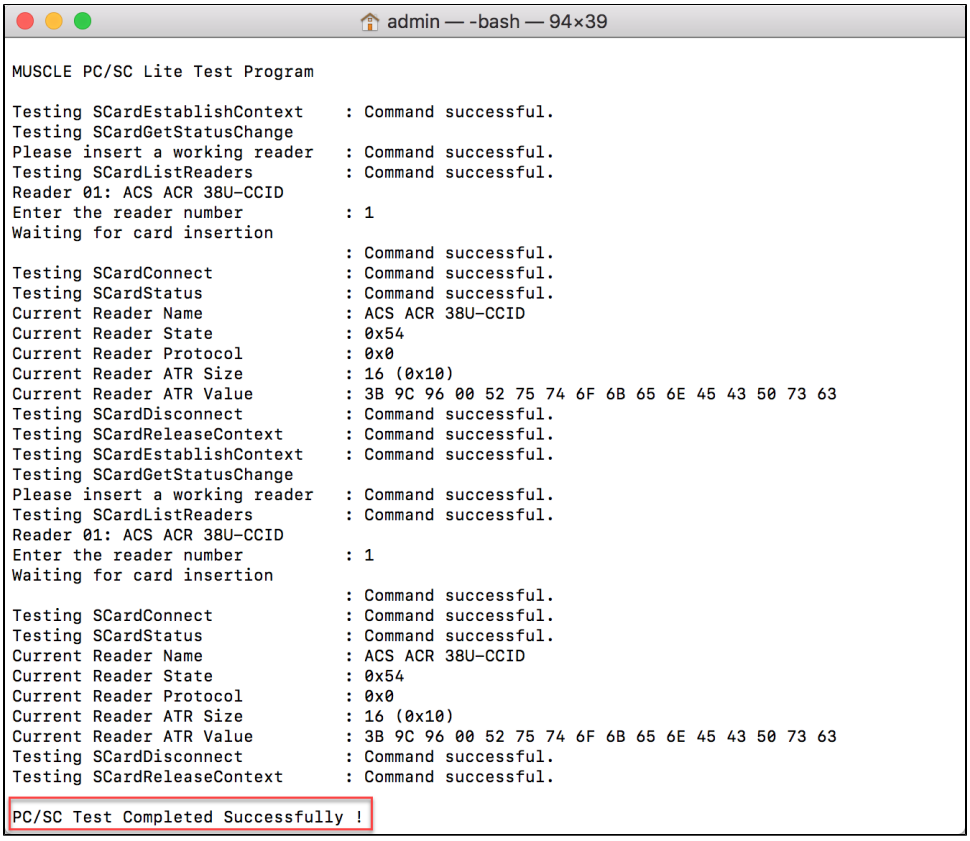
```
pcsctest
```

6. Нажмите **Enter** и введите цифру "1".
7. Нажмите **Enter** и введите цифру "1".
8. Нажмите **Enter**.
9. Если отобразилось следующее сообщение:
   Для USB-токена:



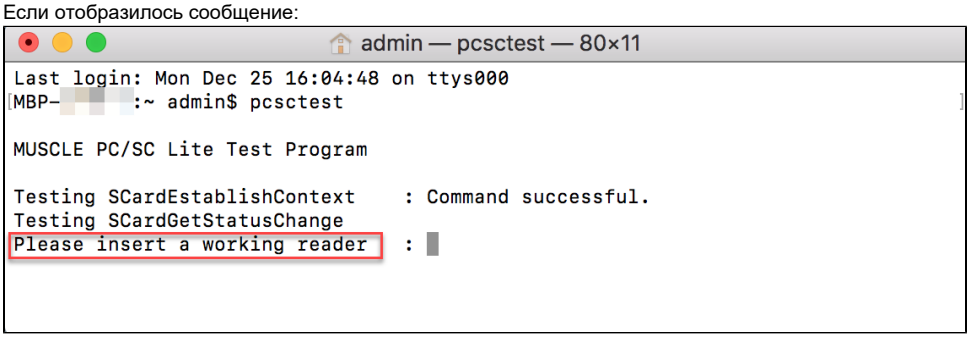
Значит USB-токен работает.

Для смарт-карты:



Значит смарт-карта работает.

10. Если отобразилось сообщение:



Значит Рутокен ЭЦП не работает. Для решения данной проблемы перейдите в раздел Решение проблем с Рутокен ЭЦП в системе.

Проверка наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП

Процесс проверки наличия RSA сертификатов изменился в операционной системе с версии 10.15.

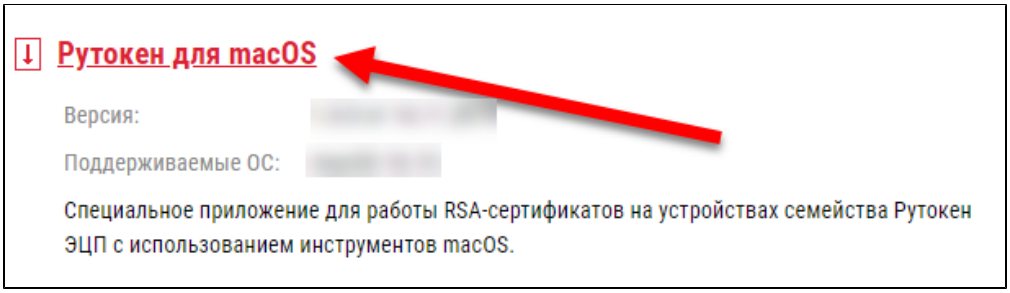
В первом подразделе описан текущий процесс проверки, а во втором — тот, что был раньше.

Начиная с версии 10.15

Перед проверкой наличия RSA сертификатов с ключевыми парами на Рутокен ЭЦП загрузите и установите на компьютер специальное приложение для работы с RSA-сертификатами.

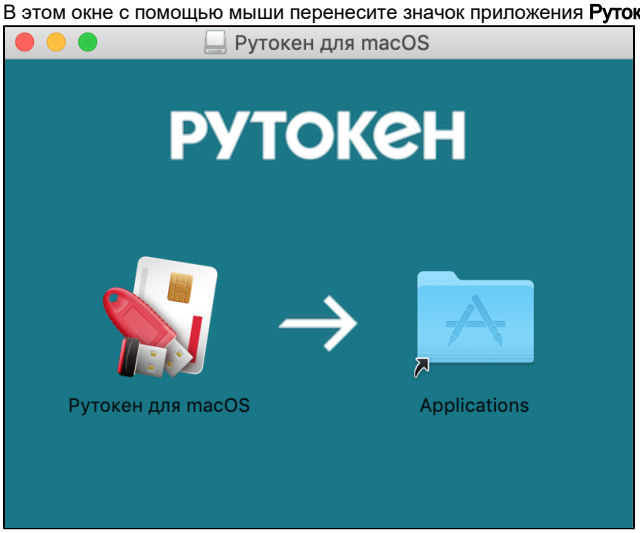
Для того чтобы загрузить это приложение перейдите по указанной ссылке:

https://www.rutoken.ru/support/download/drivers-for-mac/

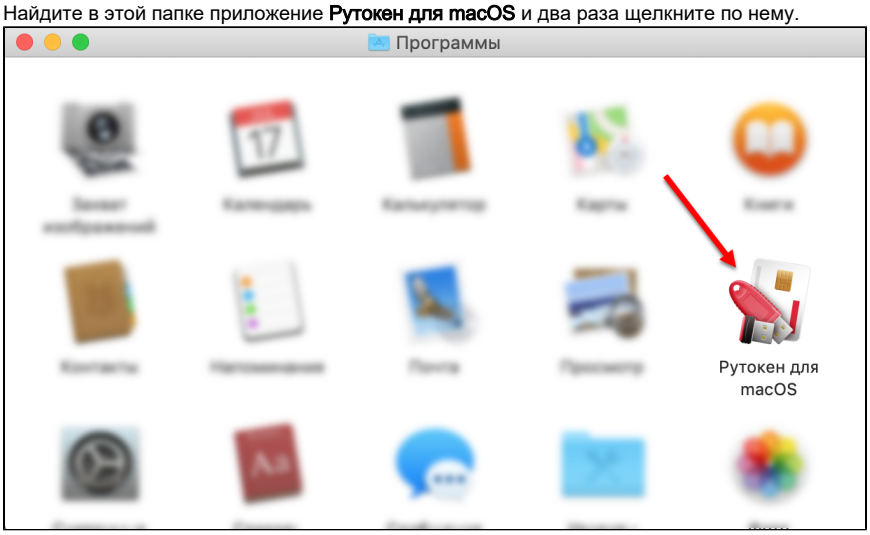


Для **установки приложения**:

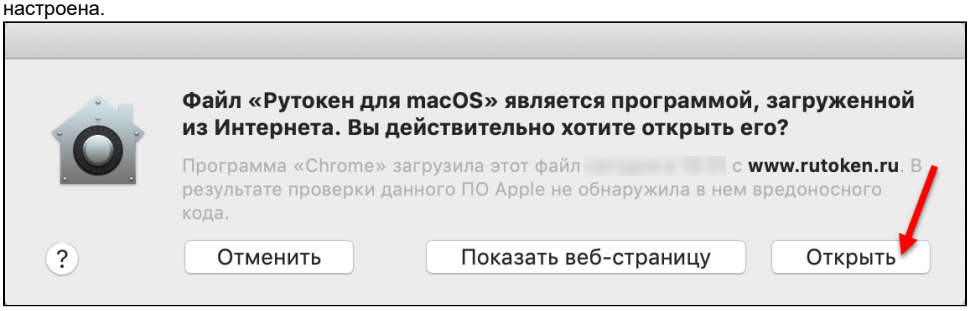
1. Запустите программу установки. На экране отобразится окно **Рутокен для macOS**.
2. В этом окне с помощью мыши перенесите значок приложения **Рутокен для macOS** в папку **Applications**.

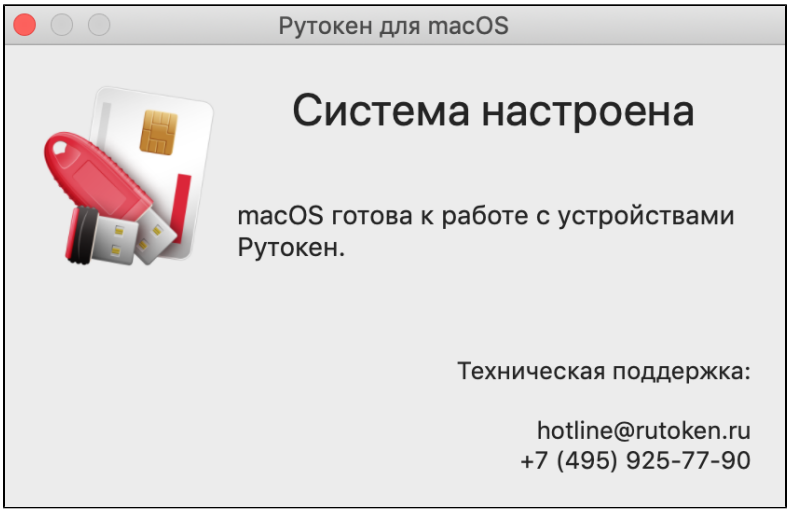


3. В окне **Рутокен для macOS** два раза щелкните по папке **Applications**. Откроется папка **Программы**.
4. Найдите в этой папке приложение **Рутокен для macOS** и два раза щелкните по нему.



5. Чтобы подтвердить открытие приложения, нажмите **Открыть**. В результате на экране отобразится уведомление о том, что система настроена.



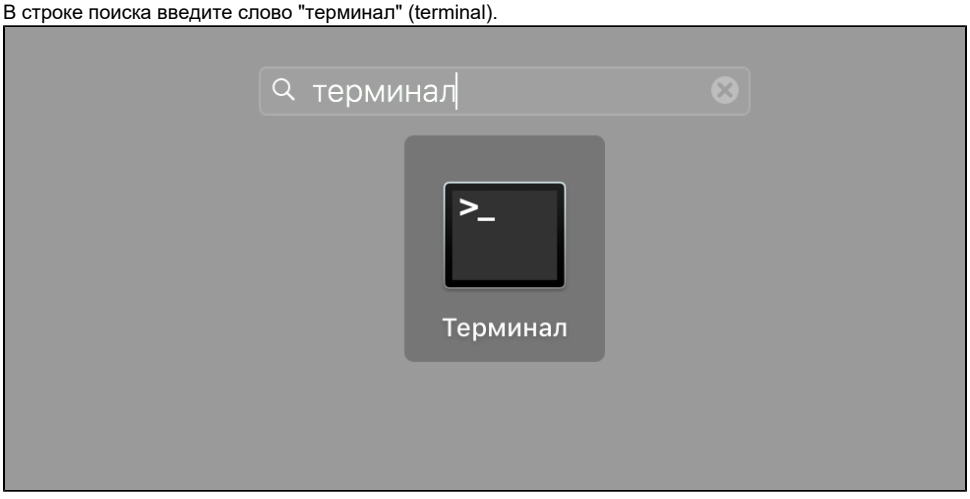


6. Закройте окно с этим уведомлением и окно Рутокен для macOS.

Для проверки наличия RSA сертификатов с ключевыми парами RSA на Рутокен ЭЦП:

1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "терминал" (terminal).

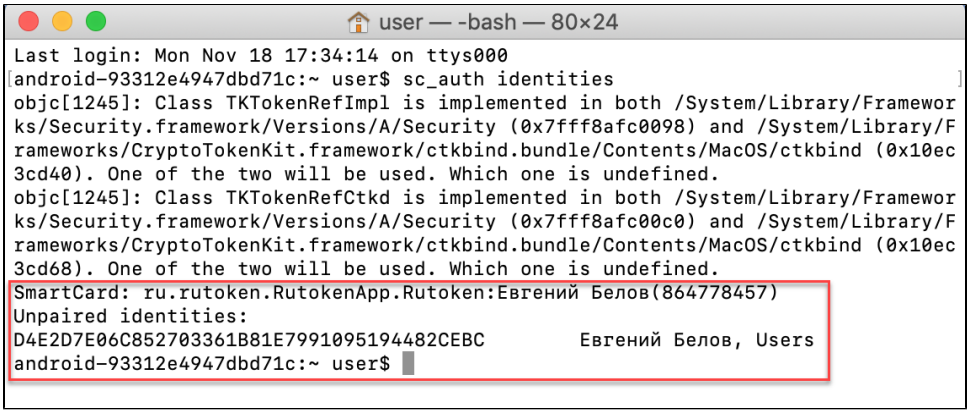


4. Откройте **Терминал (Terminal)**.

5. Введите команду:

```
sc_auth identities
```

В результате в окне Терминала отобразится информация обо всех RSA-сертификатах с ключевыми парами RSA, хранящихся на устройстве Рутокен ЭЦП.

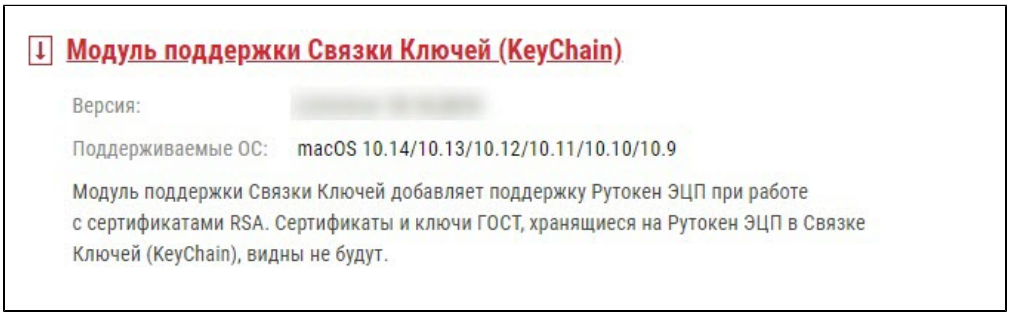


До версии 10.15

Перед запуском процесса проверки наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП загрузите и установите на компьютер модуль поддержки Связка Ключей (KeyChain).

Для того чтобы загрузить данный модуль поддержки перейдите по указанной ссылке и выберите необходимую версию модуля:

https://www.rutoken.ru/support/download/drivers-for-mac/



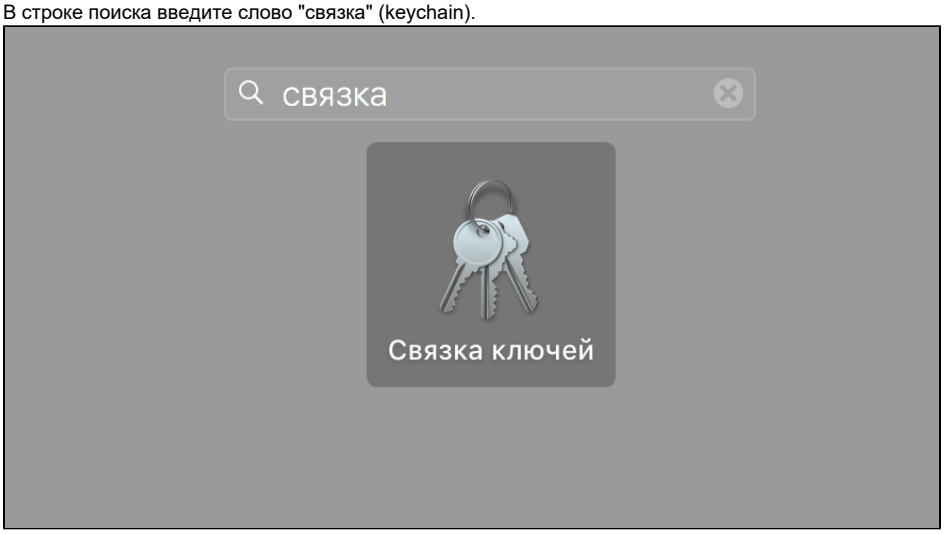
Для установки модуля поддержки Связки Ключей (KeyChain) запустите программу установки модуля и следуйте инструкциям, отображающимся на экране.

После установки модуля перезагрузите систему.

Для проверки наличия RSA сертификатов и ключевых пар RSA на Рутокен ЭЦП:

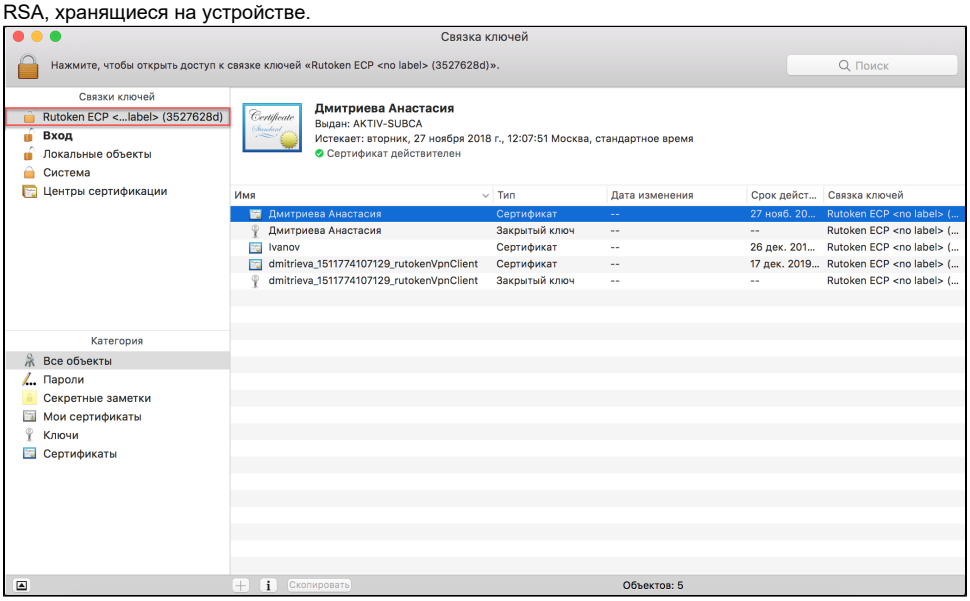
1. Подключите устройство к компьютеру.
2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "связка" (keychain).

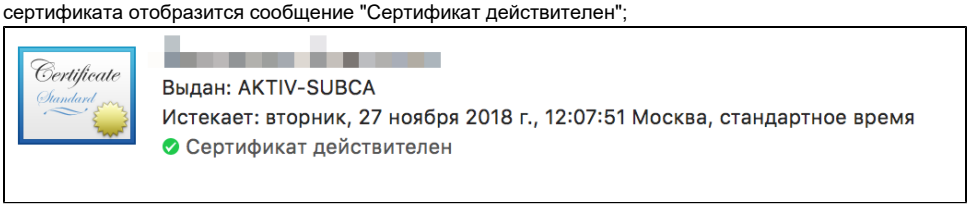


4. Откройте программу **Связка ключей (Keychain Access)**.

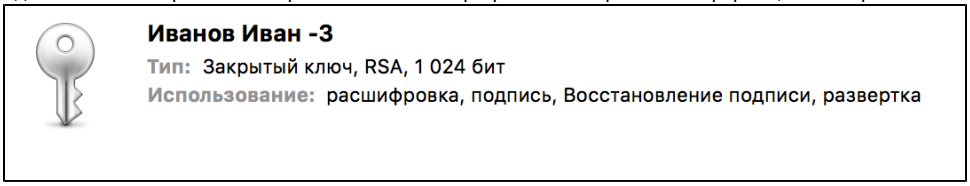
5. В боковой панели окна программы выберите название устройства. В окне программы отобразятся RSA сертификаты и ключевые пары RSA, хранящиеся на устройстве.



6. Щелкните левой кнопкой мыши в строке с необходимым RSA сертификатом или ключевой парой RSA.
 - для RSA сертификата в верхней части окна программы отобразится информация о выбранном сертификате. У действительного сертификата отобразится сообщение "Сертификат действителен";

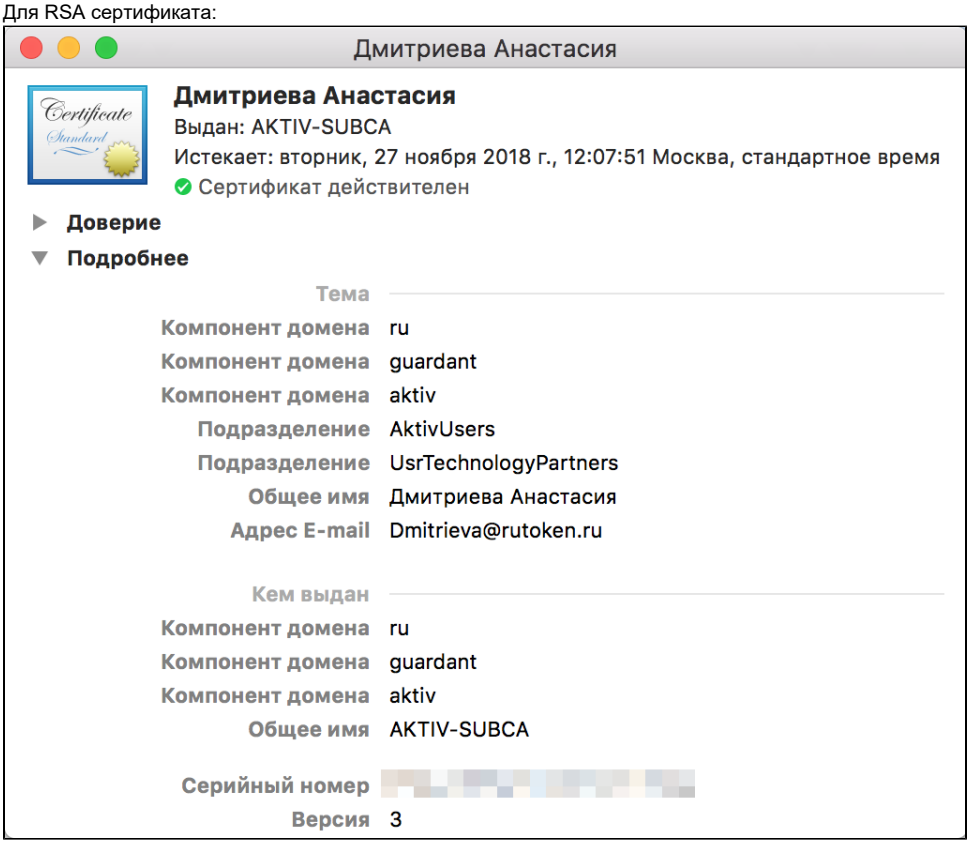


- для ключевой пары RSA в верхней части окна программы отобразится информация о выбранной ключевой паре.

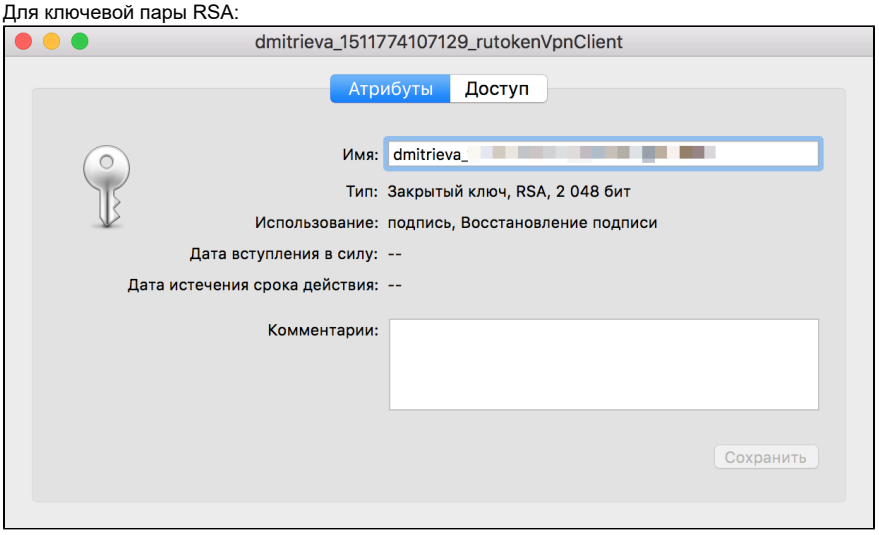


Чтобы открыть RSA сертификат или ключевую пару RSA щелкните два раза по строке с именем необходимого объекта. В результате

откроется окно с полной информацией о нем.
Для RSA сертификата:



Для ключевой пары RSA:



Если для Рутокен ЭЦП вы используете стандартный PIN-код (12345678), то следует его изменить на более сложный.

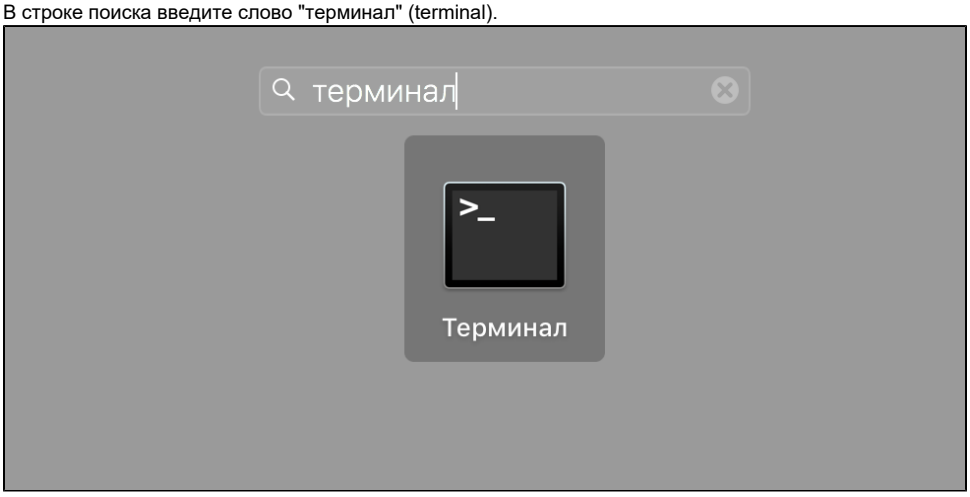
Проверка наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП

Для проверки наличия ГОСТ сертификатов и ключевых пар ГОСТ на Рутокен ЭЦП:

1. Подключите устройство к компьютеру.

2. Откройте программу **Launchpad**.

3. В строке поиска введите слово "терминал" (terminal).

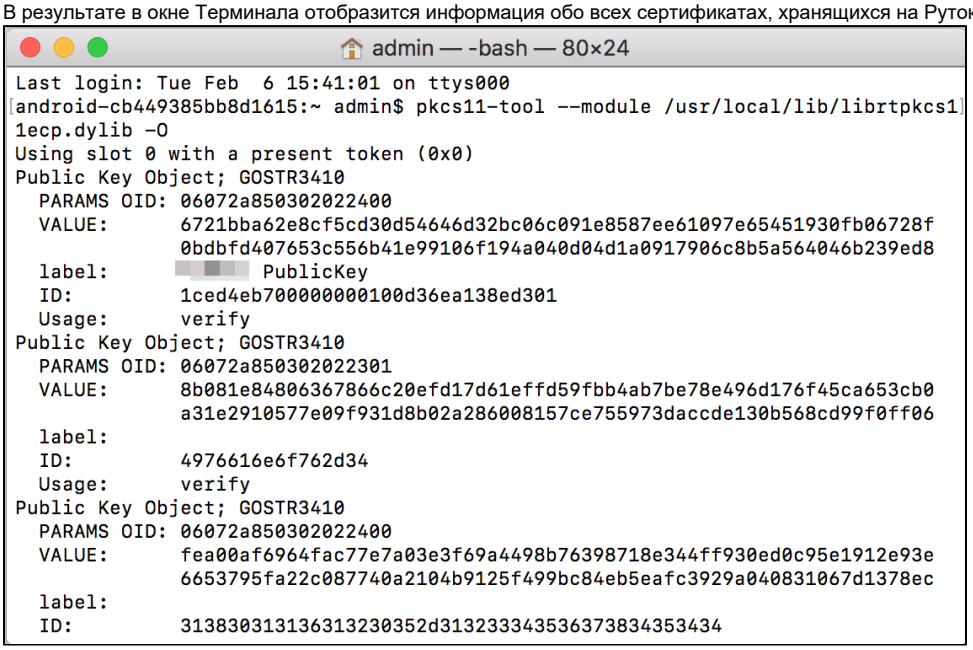


4. Откройте **Терминал (Terminal)**.

5. Введите команду:

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

A — путь до библиотеки librtpkcs11ecp.dylib.
В результате в окне Терминала отобразится информация обо всех сертификатах, хранящихся на Рутокен ЭЦП.



Чтобы открыть сертификат или ключевую пару скопируйте ID необходимого объекта и введите команду:

```
pkcs11-tool --module {A} -r -y cert --id {B} | openssl x509 -inform der -text
```

A — путь до библиотеки librtpkcs11ecp.dylib.

B — ID сертификата.

В результате в окне Терминала отобразится полная информация об указанном объекте.

Чтобы скопировать сертификат в файл введите команду:

```
pkcs11-tool --module {A} -r -y cert --id {B} > ./{C}
```

A — путь до библиотеки librtpkcs11ecp.dylib.
B — ID сертификата.
C — имя файла.

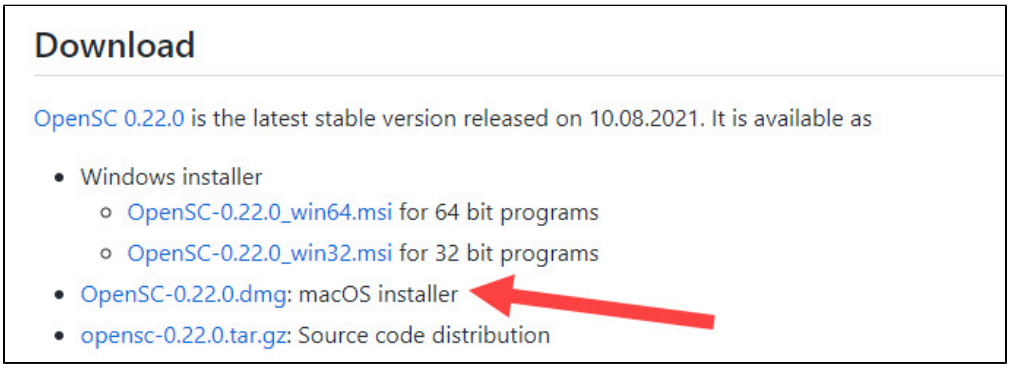
Изменение PIN-кода Рутокен ЭЦП

Перед запуском процесса смены PIN-кода устройства:

- загрузите и установите пакет OpenSC;
- загрузите и установите библиотеку PKCS#11;
- определите путь до библиотеки librtpkcs11ecp.dylib.

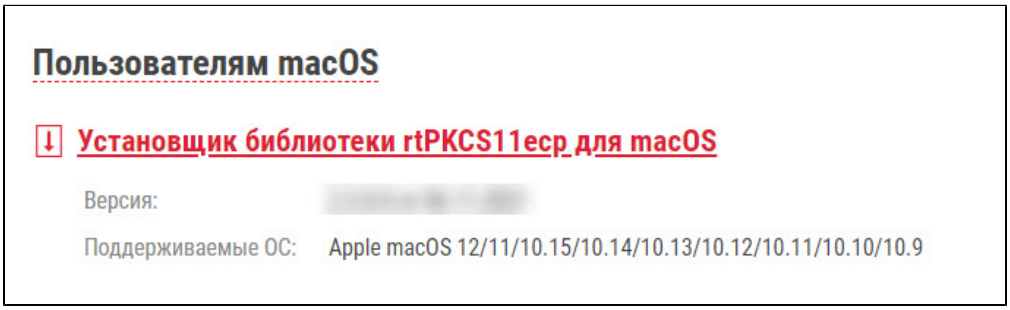
Для того чтобы загрузить установочный пакет OpenSC перейдите по указанной ссылке и выберите необходимую версию:

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



Для установки пакета OpenSC запустите программу установки пакета и следуйте инструкциям, отображающимся на экране.

Для того чтобы загрузить библиотеку PKCS#11 перейдите по указанной ссылке и выберите необходимую версию:
https://www.rutoken.ru/support/download/pkcs/

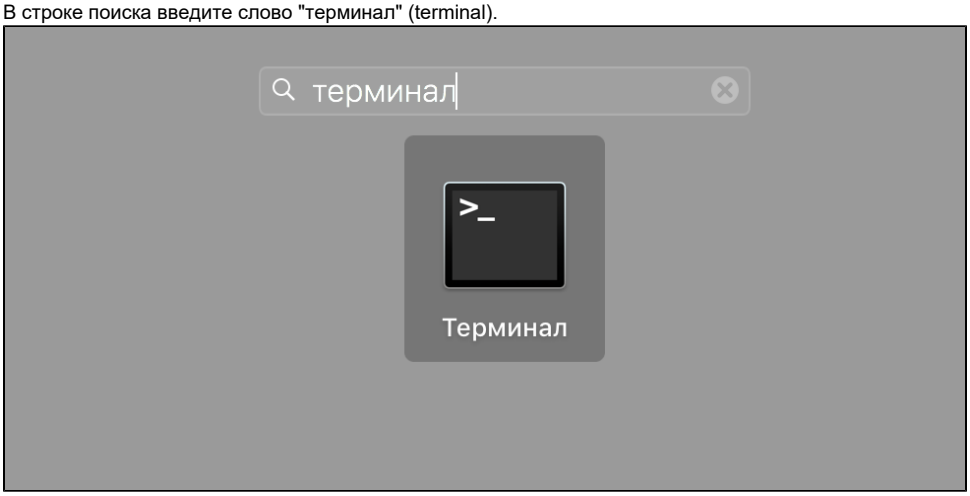


Для установки библиотеки PKCS#11 запустите программу установки библиотеки и следуйте инструкциям, отображающимся на экране.

Для того чтобы определить путь до библиотеки librtpkcs11ecp.dylib:

1. Откройте программу **Launchpad**.

2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал (Terminal)**.

4. Введите команду:

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

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

```
android-cb449385bb8d1615:~ admin$ sudo find /usr -name librtpkcs11ecp.dylib
Password:
/usr/local/lib/pkcs11/librtpkcs11ecp.dylib
/usr/local/lib/librtpkcs11ecp.dylib
```

Для изменения PIN-кода введите команду:

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

A — путь до библиотеки librtpkcs11ecp.dylib.
B — текущий PIN-код устройства.
C — новый PIN-код устройства.

```
android-cb449385bb8d1615:~ admin$ pkcs11-tool --module /usr/local/lib/librtpkcs11ecp.dylib --l
ogin --pin 12345678 --change-pin --new-pin 123456
Using slot 0 with a present token (0x0)
PIN successfully changed
```

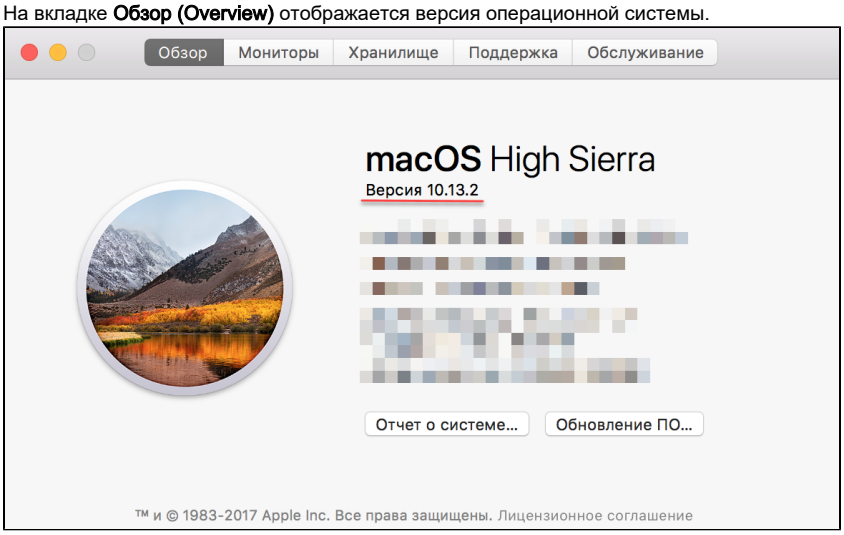
В результате PIN-код устройства будет изменен.

Решение проблем с Рутокен ЭЦП в системе

Для начала определите версию операционной системы, которую вы используете. Для этого:

1. Выберите в меню «Apple» ( ) пункт «Об этом Mac» (About This Mac).

2. На вкладке **Обзор (Overview)** отображается версия операционной системы.



Если вы используете версию 10.7 и выше, то устройство семейства Рутокен ЭЦП должно определяться системой автоматически. В таком случае проверьте корректно ли подключено устройство к компьютеру и снова повторите процедуру Проверка работы Рутокен ЭЦП в системе.

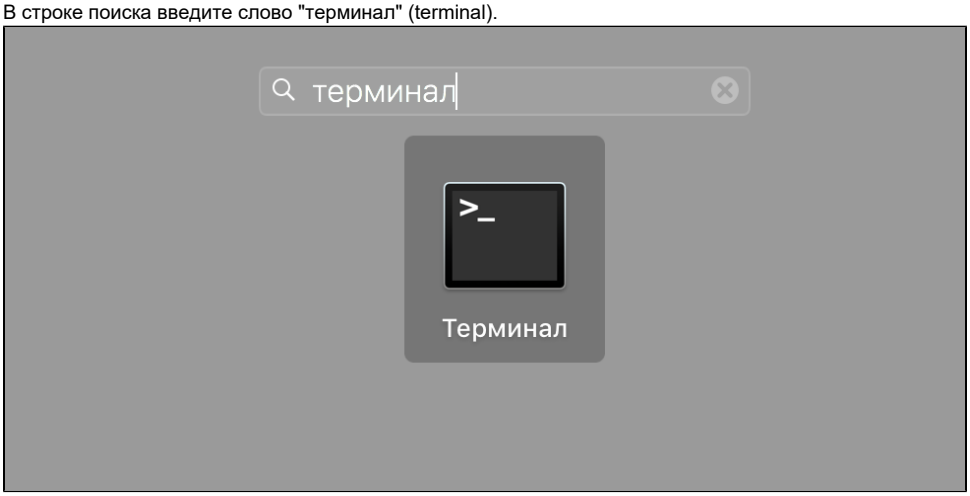
Если вы используете версию ниже чем 10.7, то необходимо изменить конфигурационный файл и перезагрузить систему.

Будьте очень внимательны при работе с конфигурационным файлом info.plist

Для изменения конфигурационного файла:

1. Откройте программу **Launchpad**.

2. В строке поиска введите слово "терминал" (terminal).



3. Откройте **Терминал (Terminal)**.
4. Откройте конфигурационный файл. Для этого введите команду:

```
sudo nano /usr/libexec/SmartCardServices/drivers/ifd-ccid.bundle
/Contents/Info.plist
```

5. В конфигурационный файл добавьте следующие строки:

a. в массив <key>ifdVendorID</key> строку <string>0x0A89</string>;
b. в массив <key>ifdProductID</key> строку <string>0x0030</string>.
c. в массив <key>ifdFriendlyName</key> строку <string>Aktiv Rutoken ECP</string>.

6. Перезагрузите систему.

После этого снова проверьте работу устройства в системе, а именно повторите процедуру Проверка работы Рутокен ЭЦП в системе.