Настройка двухфакторной аутентификации в macOS Catalina и новее

Общая информация

Инструкция применима к macOS Catalina и новее.

Для аутентификации в macOS могут использоваться:

- Рутокен ЭЦП PKI;
- Рутокен ЭЦП 2.0 2000;
- Рутокен ЭЦП 2.0 Flash
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 2.0 3000;
- Рутокен ЭЦП 3.0;
- Рутокен 2151;
- Смарт-карта Рутокен ЭЦП 2.0;
- Смарт-карта Рутокен ЭЦП 3.0 NFC;
- Рутокен ЭЦП 2.0 Bluetooth (при подключении по USB-кабелю).

Для аутентификации в системе macOS используются ключевая пара и сертификат RSA.

Перед настройкой двухфакторной аутентификации необходимо установить специальное приложение и проверить наличие ключевой пары и сертификата.

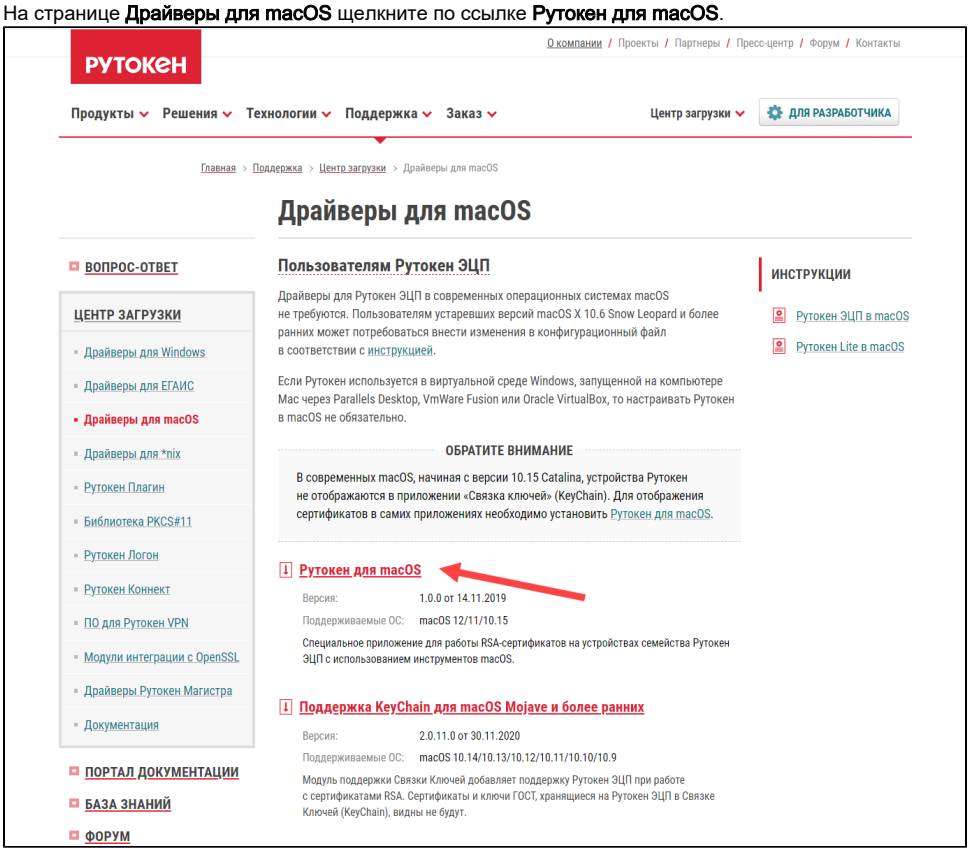
Установка приложения "Рутокен для macOS"

Приложение "Рутокен для macOS" необходимо для настройки двухфакторной аутентификации в macOS с использованием сертификатов, записанных на устройствах семейства Рутокен.

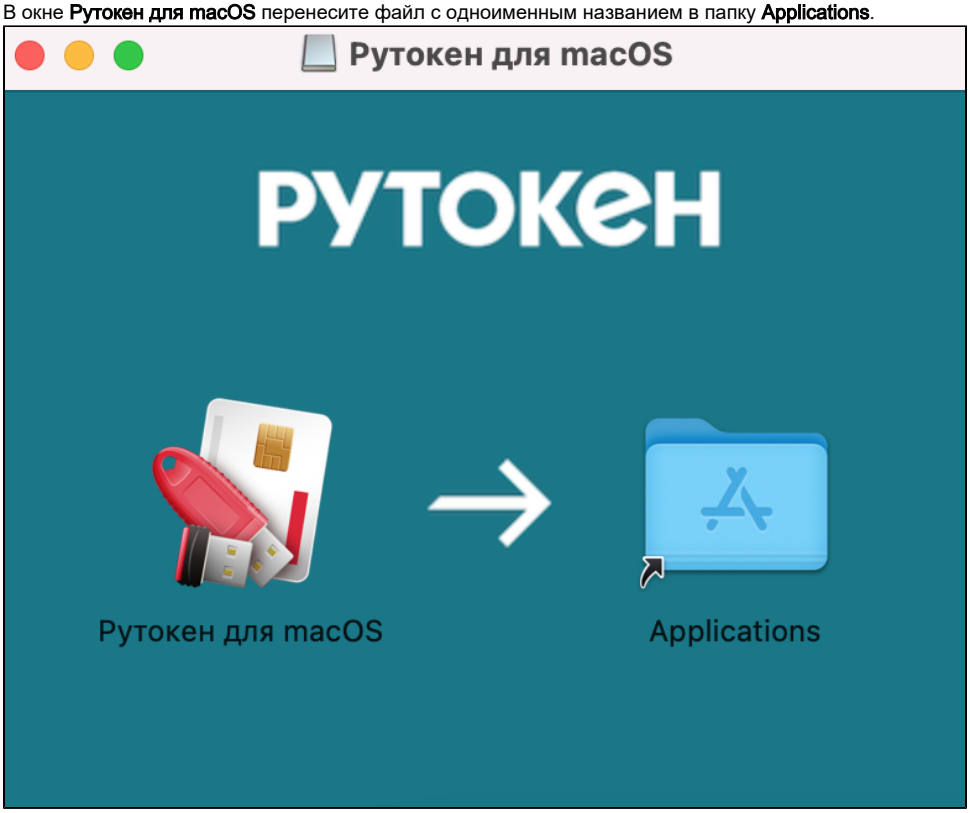
Чтобы установить это приложение:

1. Перейдите на страницу:
   https://www.rutoken.ru/support/download/mac/

2. На странице **Драйверы для macOS** щелкните по ссылке **Рутокен для macOS**.

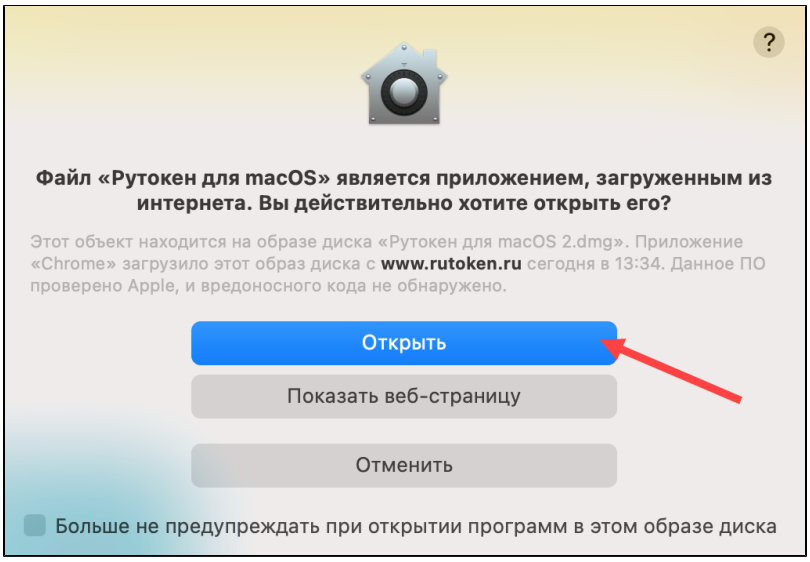


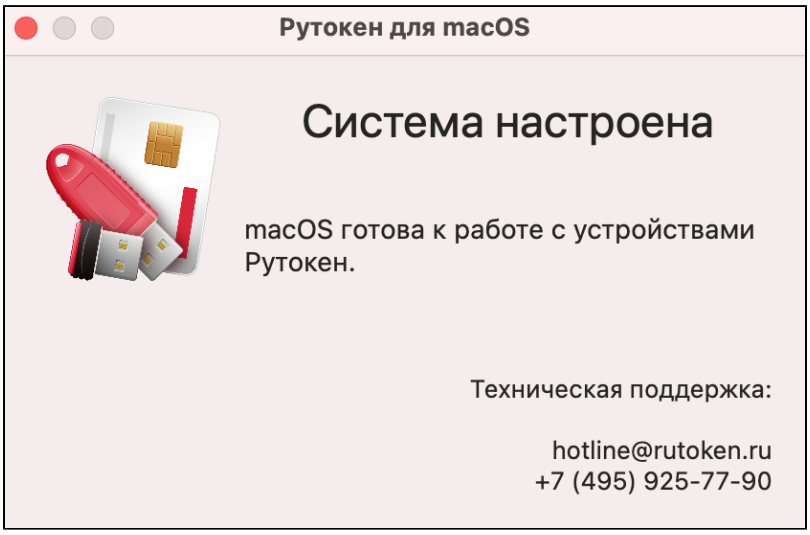
3. Загрузите приложение.
4. Перейдите в папку **Загрузки**.
5. Дважды щелкните по названию файла **Рутокен для macOS**.
6. В окне **Рутокен для macOS** перенесите файл с одноименным названием в папку **Applications**.



7. Перейдите в **Launchpad** и дважды щелкните по названию приложения **Рутокен для macOS**.
8. В окне с подтверждением открытия приложения нажмите **Открыть**. В результате приложение Рутокен для macOS добавит возможность аутентификации по сертификату в систему.

После установки приложения обязательно перезагрузите компьютер.

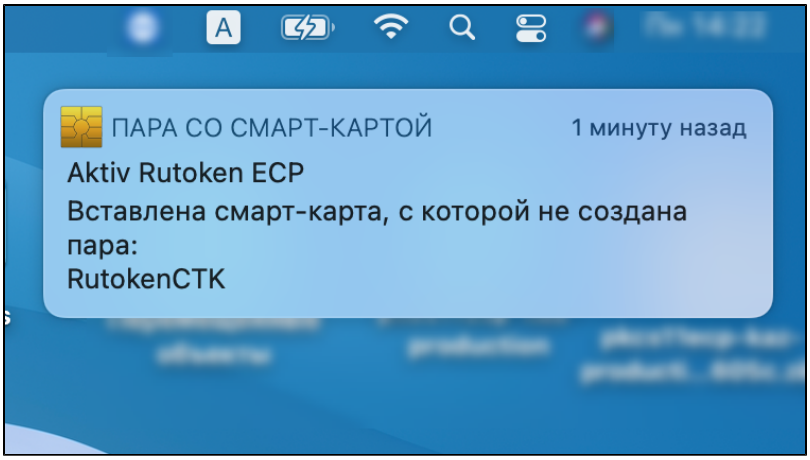




Далее проверьте наличие ключевой пары и сертификата RSA на Рутокене.

Проверка наличия ключевой пары и сертификата RSA

Чтобы проверить наличие ключевой пары и сертификата RSA, подключите Рутокен к компьютеру. Если на экране отобразилось уведомление о том, что вставлена смарт-карта, с которой не создана пара RutokenCTK, значит сертификат есть.



В таком случае необходимо выполнить только специальную настройку, которая описана в соответствующем разделе.

Генерация ключевой пары и выписывание сертификата RSA

Сгенерировать ключевую пару и выписать сертификат можно на специальном сервисе ra.rutoken.ru.

Для работы с этим сервисом вам необходимо загрузить и установить Рутокен Плагин. Его актуальная версия расположена на странице:

https://www.rutoken.ru/support/download/rutoken-plugin/

в разделе **Пользователям macOS**.



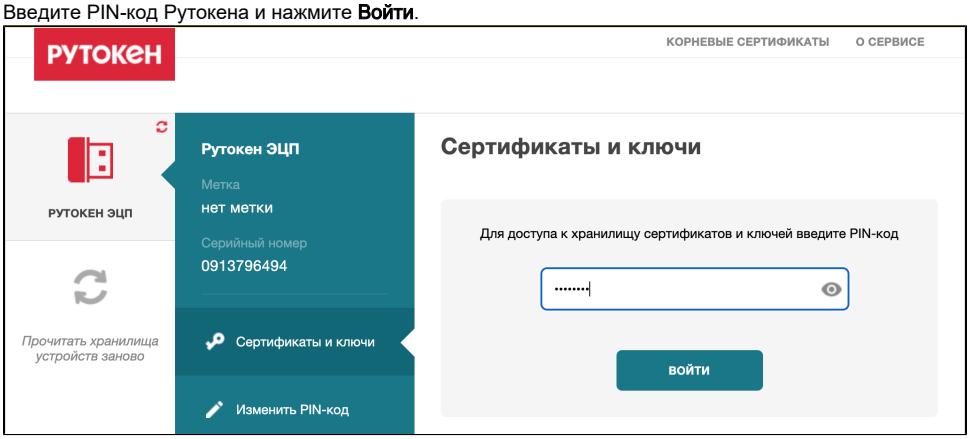
Процедура загрузки и установки описана в инструкции.

Сервис ra.rutoken.ru работает в браузерах: Google Chrome, Яндекс. Браузере, Mozilla Firefox, Opera и Спутнике.

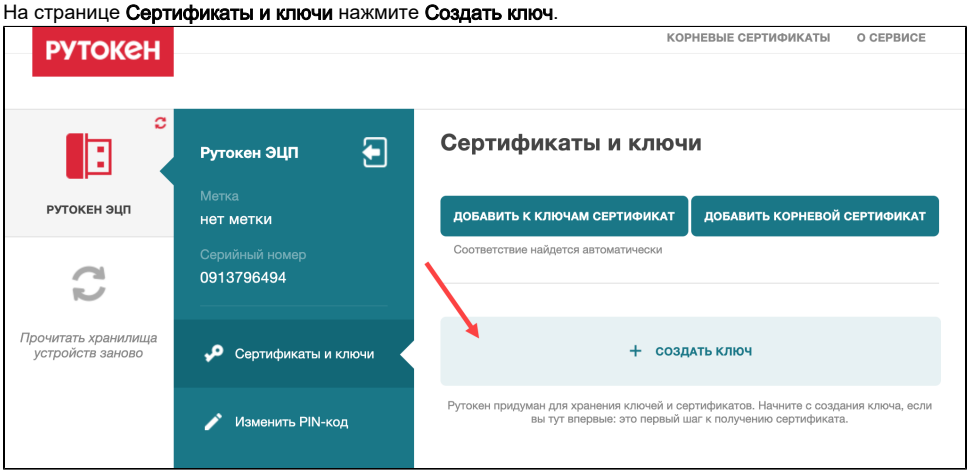
Чтобы снегерировать ключевую пару и выписать сертификат RSA:

1. Перейдите на страницу:
   https://ra.rutoken.ru/
2. Подключите Рутокен к компьютеру.

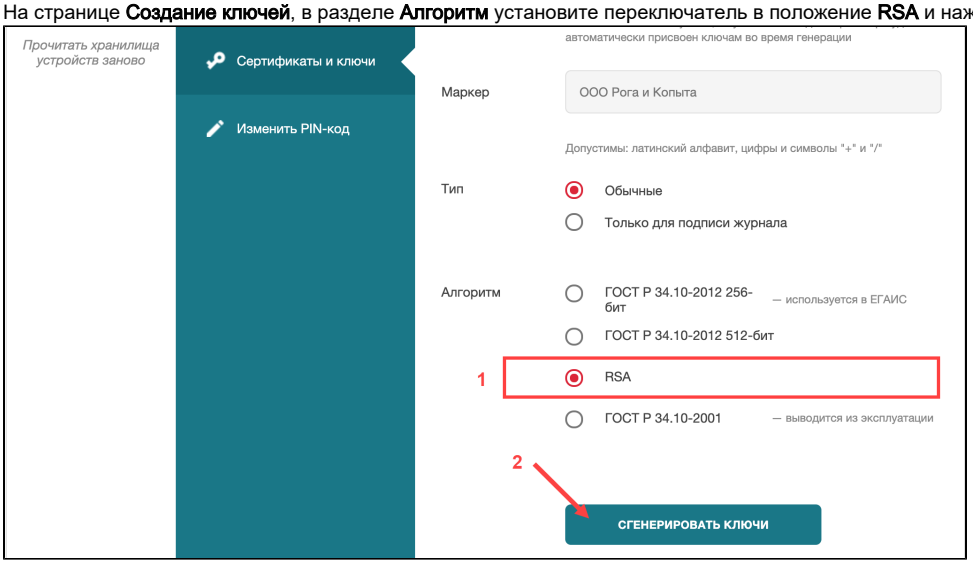
3. Введите PIN-код Рутокена и нажмите **Войти**.



4. На странице **Сертификаты и ключи** нажмите **Создать ключ**.

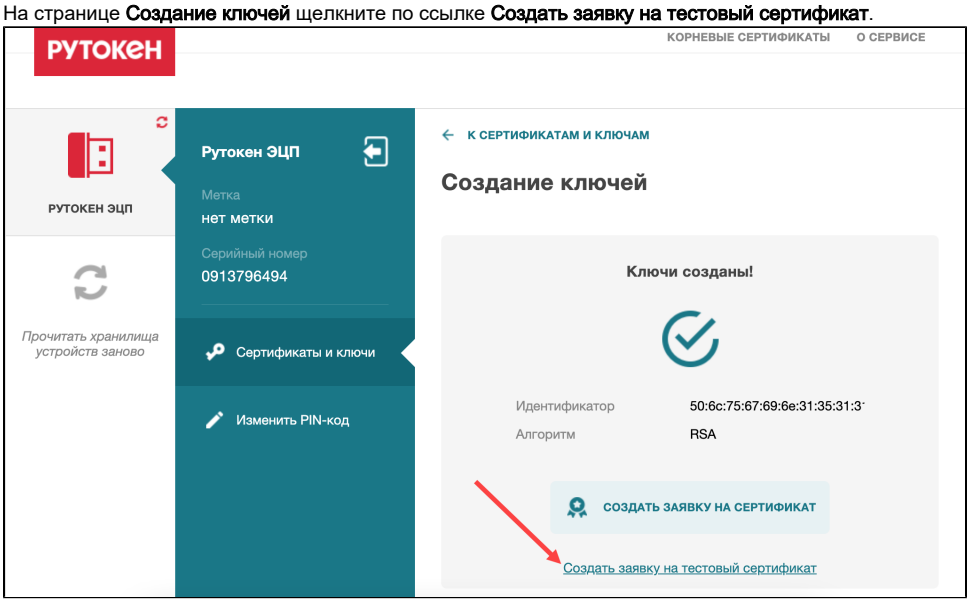


5. На странице **Создание ключей**, в разделе **Алгоритм** установите переключатель в положение **RSA** и нажмите **Сгенерировать ключи**.



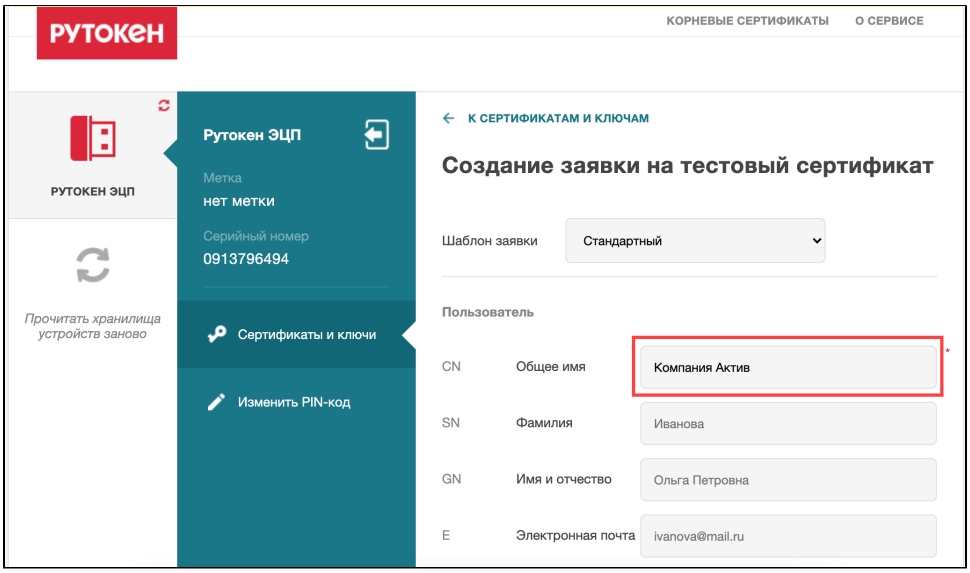
Генерация ключевой пары может занять 20-30 секунд. Дождитесь окончания этого процесса.

6. На странице **Создание ключей** щелкните по ссылке **Создать заявку на тестовый сертификат**.

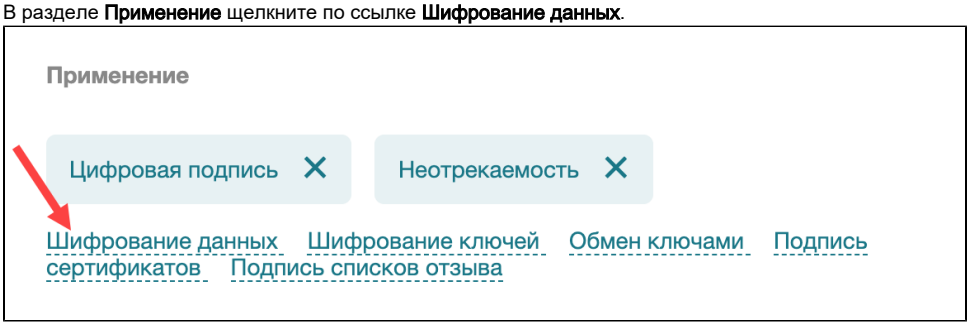


7. На странице **Создание заявки на тестовый сертификат**, в разделе **Пользователь** в поле **Общее имя** введите необходимое значение.

   Запомните значение, которое вы ввели в поле **Общее имя**, оно вам пригодится при настройке аутентификации.



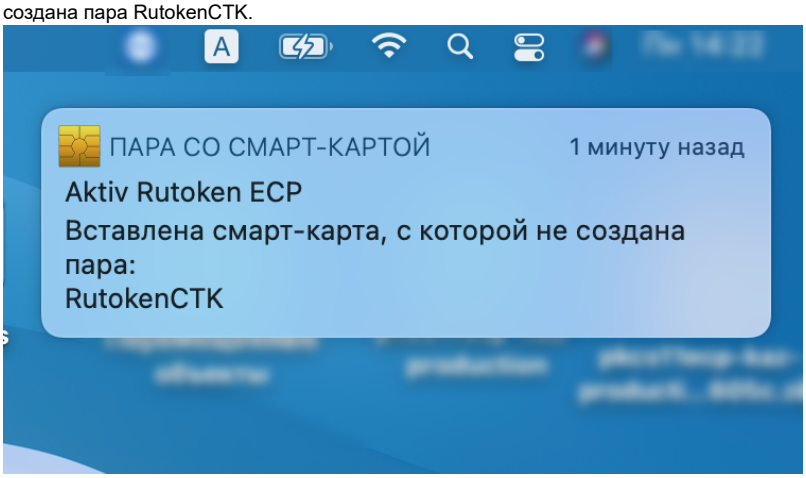
8. При необходимости на этой странице введите другие данные пользователя.
9. В разделе **Применение** щелкните по ссылке **Шифрование данных**.



10. В разделе **Дополнительное применение** щелкните по ссылке **Аутентификация клиента**.
11. Нажмите **Создать запрос**. В результате на Рутокене будет создан сертификат RSA.
    После этого настройте аутентификацию по сертификату в системе.

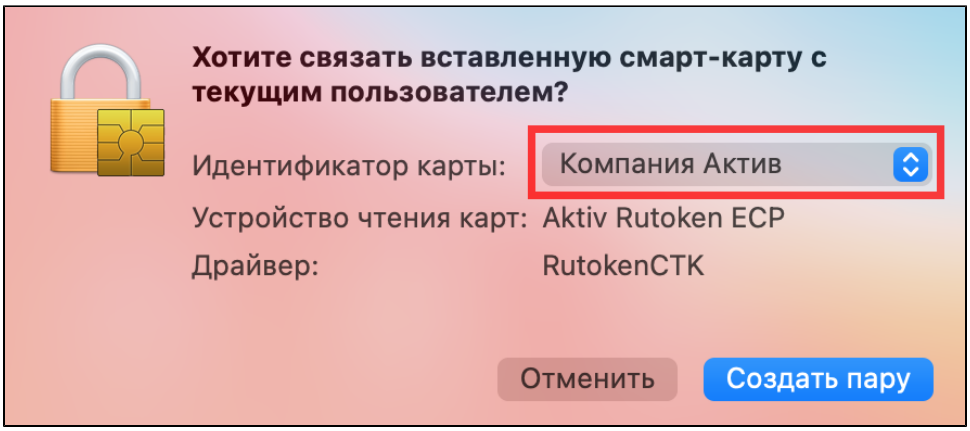
Настойка аутентификации

Чтобы настроить аутентификацию в системе по сертификату, сохраненному на Рутокене:
1. Подключите Рутокен к компьютеру. В правом верхнем углу отобразится уведомление о том, что вставлена смарт-карта, с которой не создана пара RutokenCTK.

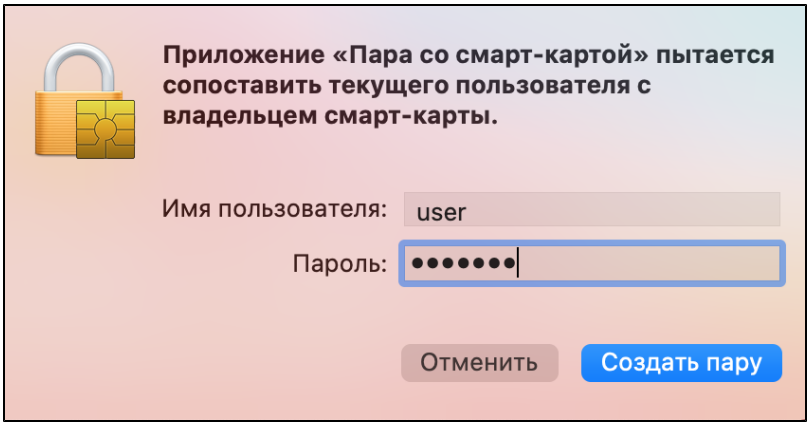


2. Щелкните по этому уведомлению.
3. В раскрывающемся списке выберите необходимый идентификатор и нажмите **Создать пару**.

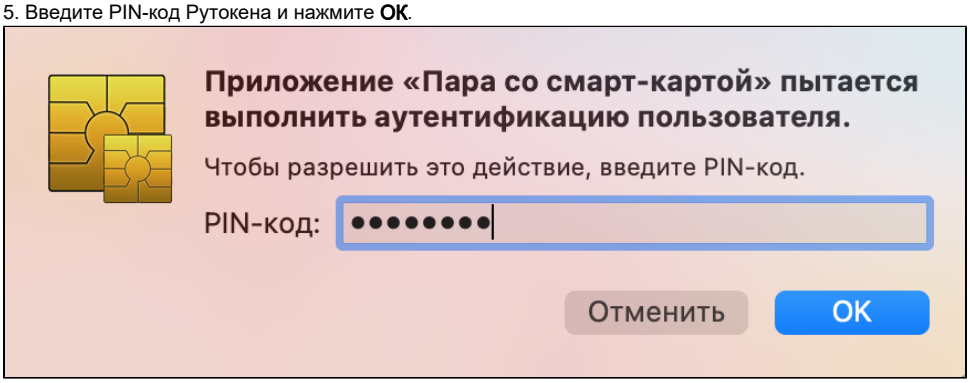
Идентификатор — это значение, которое вы вводили при создании заявки на тестовый сертификат в поле **Общее имя**.



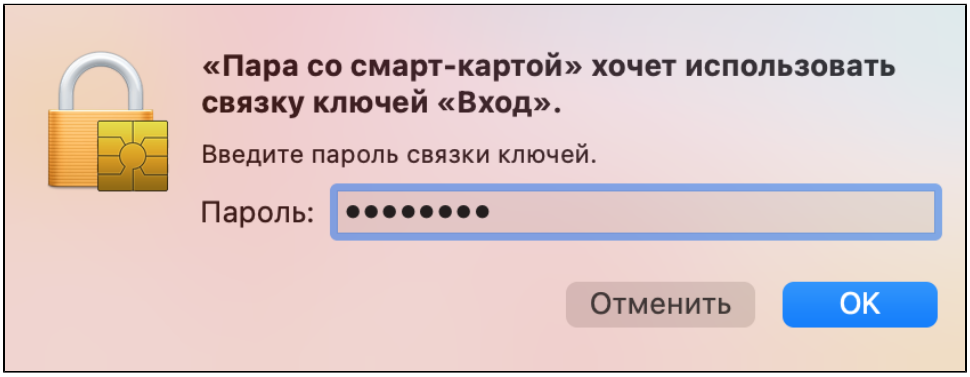
4. Введите пароль аккаунта пользователя и нажмите **Создать пару**.



5. Введите PIN-код Рутокена и нажмите **OK**.



6. Введите пароль от связки ключей и нажмите **OK**.



В результате аутентификация будет настроена, и при входе в систему вы будете подключать Рутокен и вводить его PIN-код.

