Настройка двухфакторной аутентификации в macOS Catalina и Big Sur

Обеспечение поддержки входа в macOS по токену или смарт-карте Рутокен

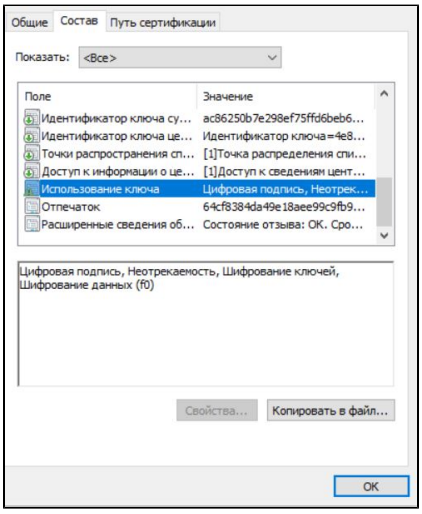
В качестве примера настраивается аутентификация для учетной записи *user* сертификатом *Шавровой Ксении.*

Инструкция применима к macOS версии 10.15 Catalina

Предварительная подготовка.

Для аутентификации в системе используется сертификат RSA (1024 бит или больше), выписанный на Рутокен ЭЦП 2.0.

Обратите внимание, что в области применения сертификата должно быть также указано Цифровая подпись, Шифрование данных и Шифрование ключей.



Также вам понадобится корневой сертификат (в виде .cer файла). Для аутентификации в macOS может использоваться любое из следующих устройств:

- Рутокен ЭЦП 2.0
- Рутокен ЭЦП PKI
- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 3000
- Смарт-карты Рутокен ЭЦП SC
- Смарт-карты Рутокен ЭЦП 2.0
- Рутокен ЭЦП 2.0 Bluetooth (при подключении по USB-кабелю)

Начиная с macOS 10.15 Catalina был компанией Apple был изменен механизм работы с токенами. Теперь сертификаты с токенов в "Связке ключей (KeyChain)" больше не видны.

Настройка аутентификации

1. Установите на компьютер под управлением macOS программу "Рутокен для macOS".

После установки этой программы сертификаты с устройства Рутокен смогут использоваться внутри приложений, которые обновили механизм работы с токенами для macOS Catalina.

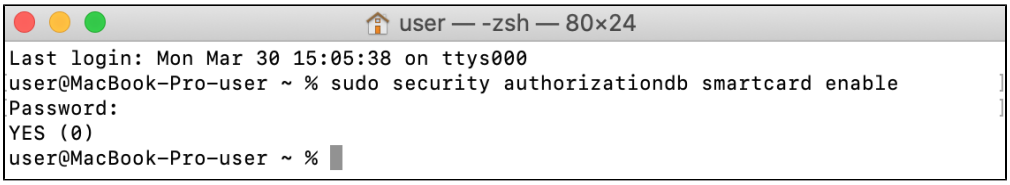
2. Перезагрузите компьютер

3. Подключите Рутокен с сертификатом

4. Операции по настройки аутентификации будут производиться через "Терминал" (Terminal), его можно найти в "Программы"/"Утилиты" (Applications/Utilities).

5. Первоначально необходимо активировать возможность аутентификации по смарт-картам с помощью команды:

```
sudo security authorizationdb smartcard enable
```

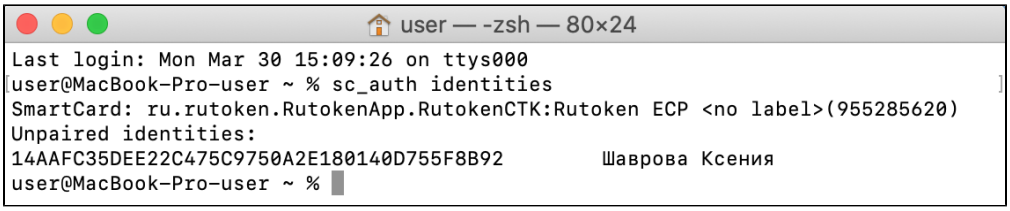


В случае успешного выполнения, команда возвращает YES (0)

6. Далее нужно определить хэш сертификата:

```
sc_auth identities
```

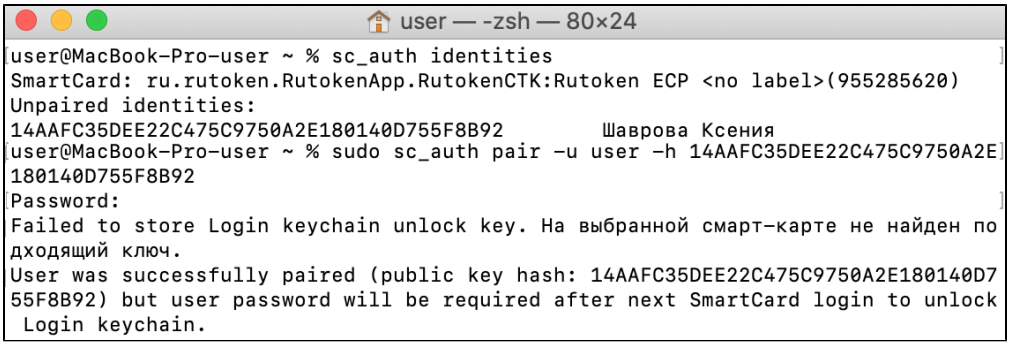
Будет выведен список сертификатов и соответствующих им хешей, в нашем случае он один:



7. Свяжем пользователя с приватным ключом на токене по хешу сертификата, выполнив

```
sudo sc_auth pair -u user -h hash
```

Где в качестве *hash* используется хеш сертификата, находящегося на токене. Его можно скопировать любым удобным способом из выдачи предыдущей команды. В качестве *user* нужно использовать имя вашего пользователя (в данном случае - *user*):



Проверить корректность привязки можно с помощью команды:

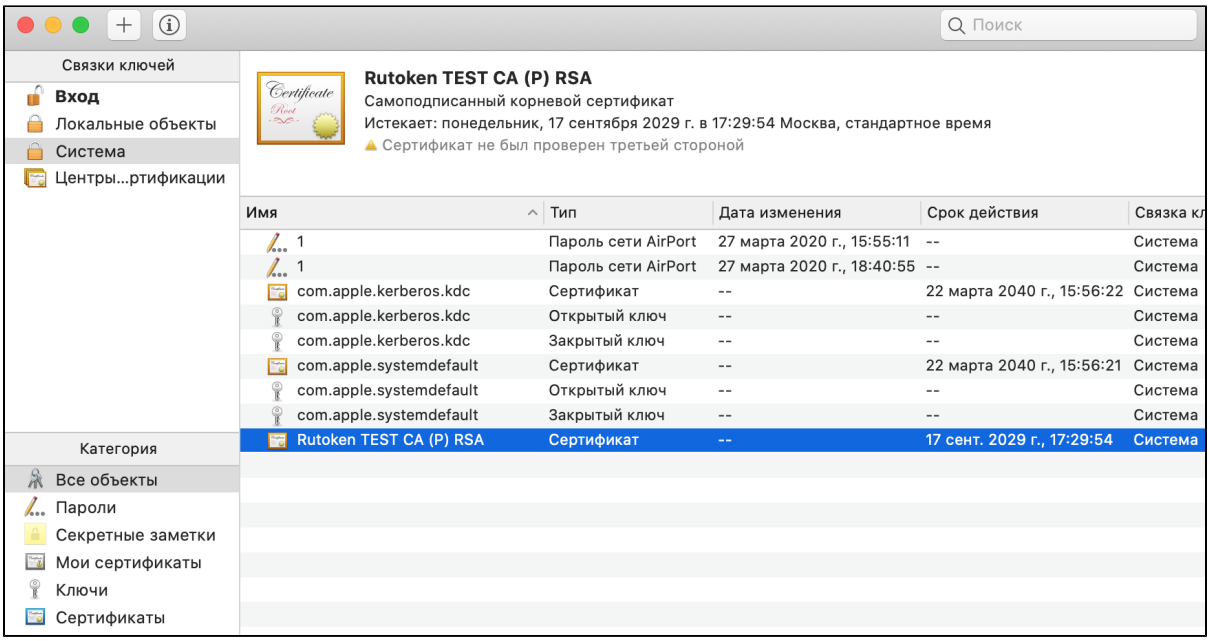
```
sc_auth list -u user
```

Команда должна вернуть указанный нами хеш.

8. Также необходимо сделать установку для пользователя _securityagent

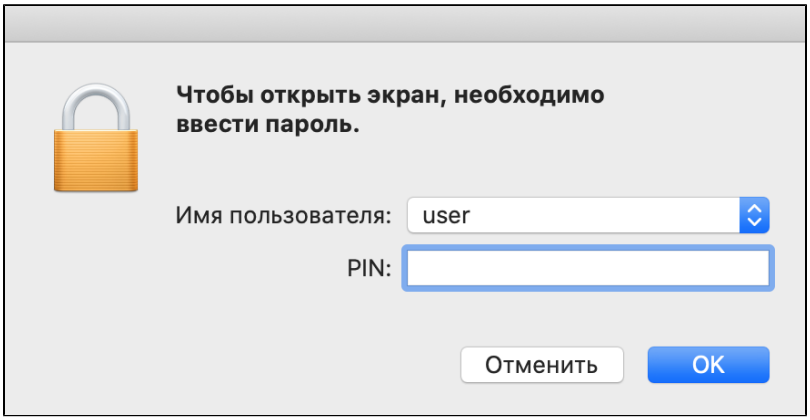
```
cd /Applications/\ \ macOS.app/Contents/PlugIns
sudo launchctl asuser _securityagent pluginkit -a "RutokenCTK.appex"
```

9. В "Связке ключей" (Keychain) необходимо разместить корневой сертификат в связке "Система" (System). Сделать это можно перетащив сертификат в окошко связки "Система".



10. Для проверки корректности работы аутентификации извлечем токен Рутокен и перезагрузим систему.

Первоначально мы увидим стандартный запрос пароля, однако с подключением токена вместо "пароль" в окошке ввода появится "PIN".



*Если аутентификация по смарт-карте невозможна после включения/перезагрузки, ознакомьтесь с инструкцией.