

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**.

РУТОКЕН

О компании / Проекты / Партнеры / Пресс-центр / Форум / Контакты

Продукты ▾ Решения ▾ Технологии ▾ Поддержка ▾ Заказы ▾

Центр загрузки ▾ [ДЛЯ РАЗРАБОТЧИКА](#)

Главная > Поддержка > Центр загрузки > Драйверы для macOS

Драйверы для macOS

ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- Драйверы для Windows
- Драйверы для ЕГАИС
- Драйверы для macOS**
- Драйверы для *nix
- Рутокен Плагин
- Библиотека PKCS#11
- Рутокен Логон
- Рутокен Коннект
- ПО для Рутокен VPN
- Модули интеграции с OpenSSL
- Драйверы Рутокен Магистра
- Документация

ПОРТАЛ ДОКУМЕНТАЦИИ

БАЗА ЗНАНИЙ

ФОРУМ

Пользователям Рутокен ЭЦП

Драйверы для Рутокен ЭЦП в современных операционных системах macOS не требуются. Пользователям устаревших версий macOS X 10.6 Snow Leopard и более ранних может потребоваться внести изменения в конфигурационный файл в соответствии с [инструкцией](#).

Если Рутокен используется в виртуальной среде Windows, запущенной на компьютере Mac через Parallels Desktop, VmWare Fusion или Oracle VirtualBox, то настраивать Рутокен в macOS не обязательно.

ОБРАТИТЕ ВНИМАНИЕ

В современных macOS, начиная с версии 10.15 Catalina, устройства Рутокен не отображаются в приложении «Связка ключей» (KeyChain). Для отображения сертификатов в самих приложениях необходимо установить [Рутокен для macOS](#).

Рутокен для macOS

Версия: 1.0.0 от 14.11.2019

Поддерживаемые ОС: macOS 12/11/10.15

Специальное приложение для работы RSA-сертификатов на устройствах семейства Рутокен ЭЦП с использованием инструментов macOS.

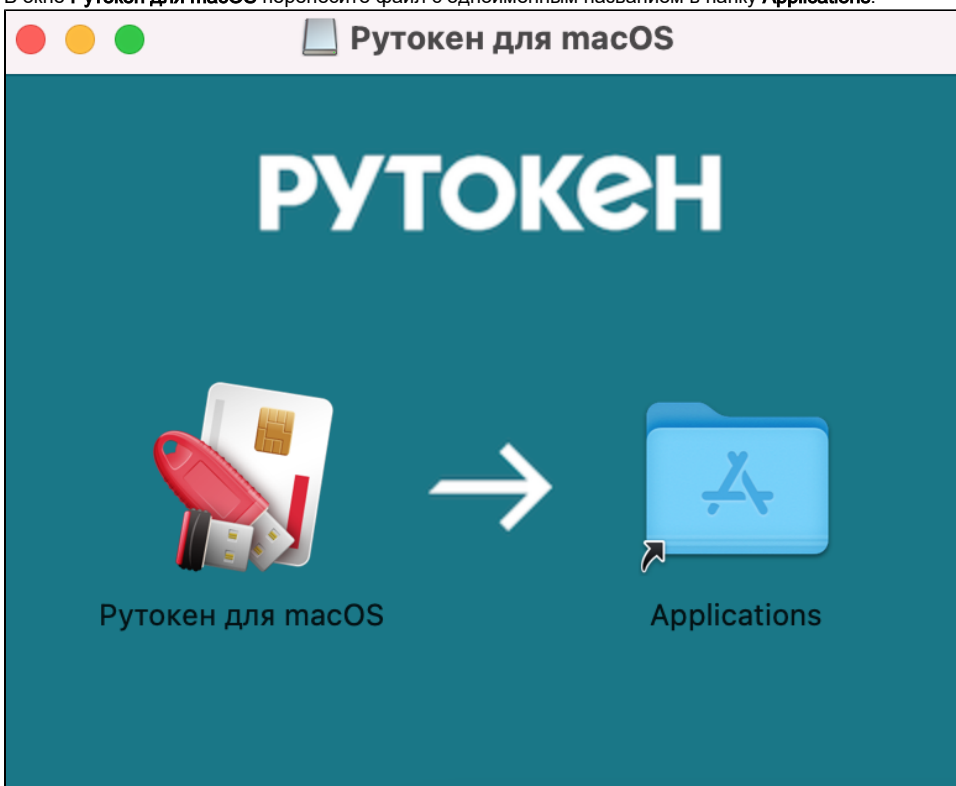
Поддержка KeyChain для macOS Mojave и более ранних

Версия: 2.0.11.0 от 30.11.2020

Поддерживаемые ОС: macOS 10.14/10.13/10.12/10.11/10.10/10.9

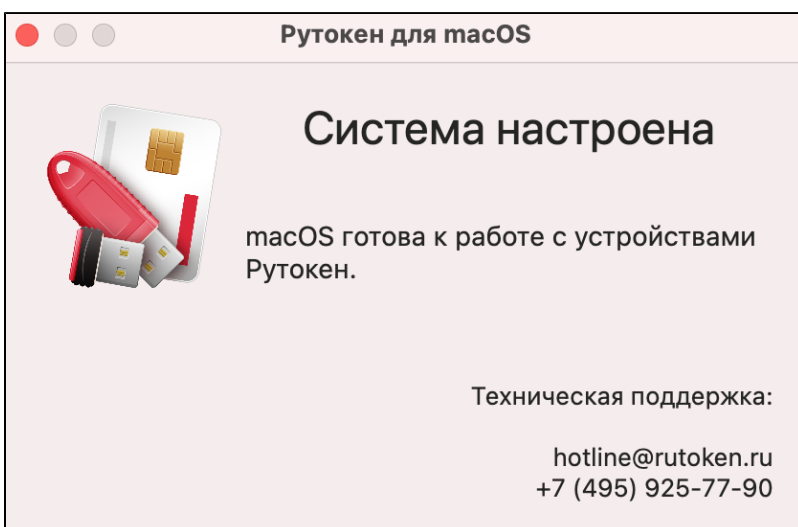
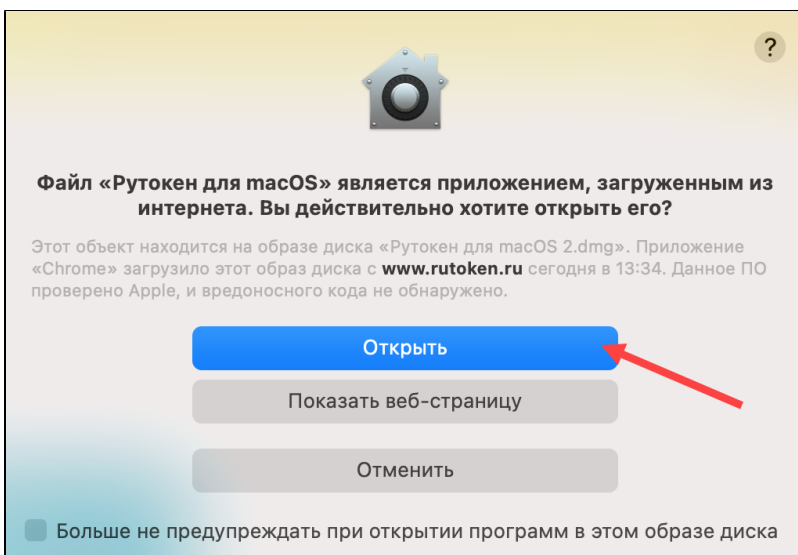
Модуль поддержки Связки Ключей добавляет поддержку Рутокен ЭЦП при работе с сертификатами RSA. Сертификаты и ключи ГОСТ, хранящиеся на Рутокен ЭЦП в Связке Ключей (KeyChain), видны не будут.

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.

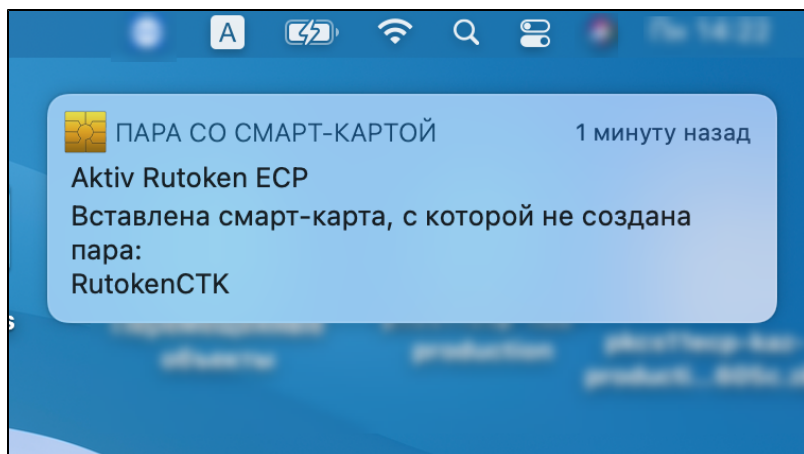
После установки приложения обязательно перезагрузите компьютер.



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**.

Пользователям macOS

↓

Рутокен Плагин для macOS

Версия:	4.5.6.0 от 12.08.2021
Браузеры:	Mozilla Firefox, Google Chrome, Opera, Спутник, Яндекс.Браузер
Поддерживаемые ОС:	Apple macOS 12/11/10.15/10.14/10.13/10.12/10.11/10.10/10.9

Процедура загрузки и установки описана в [инструкции](#).

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

Чтобы сгенерировать 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**.

РУТОКЕН

КОРНЕВЫЕ СЕРТИФИКАТЫ О СЕРВИСЕ

Рутокен ЭЦП

Метка
нет метки

Серийный номер
0913796494

Прочитать хранилища устройств заново

Сертификаты и ключи

Изменить PIN-код

Сертификаты и ключи

Для доступа к хранилищу сертификатов и ключей введите PIN-код

.....

ВОЙТИ

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

РУТОКЕН

КОРНЕВЫЕ СЕРТИФИКАТЫ О СЕРВИСЕ

Рутокен ЭЦП

Метка
нет метки

Серийный номер
0913796494

Прочитать хранилища устройств заново

Сертификаты и ключи

Изменить PIN-код

ДОБАВИТЬ К КЛЮЧАМ СЕРТИФИКАТ

ДОБАВИТЬ КОРНЕВОЙ СЕРТИФИКАТ

Соответствие найдется автоматически

+ СОЗДАТЬ КЛЮЧ

Рутокен придуман для хранения ключей и сертификатов. Начните с создания ключа, если вы тут впервые: это первый шаг к получению сертификата.

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

Прочитать хранилища устройств заново

Сертификаты и ключи

Изменить PIN-код

автоматически присвоен ключам во время генерации

Маркер

ООО Рога и Копыта

Допустимы: латинский алфавит, цифры и символы "+" и "/"

Тип

☒ Обычные

☐ Только для подписи журнала

Алгоритм

☐ ГОСТ Р 34.10-2012 256-бит — используется в ЕГАИС

☐ ГОСТ Р 34.10-2012 512-бит

1 ☒ RSA

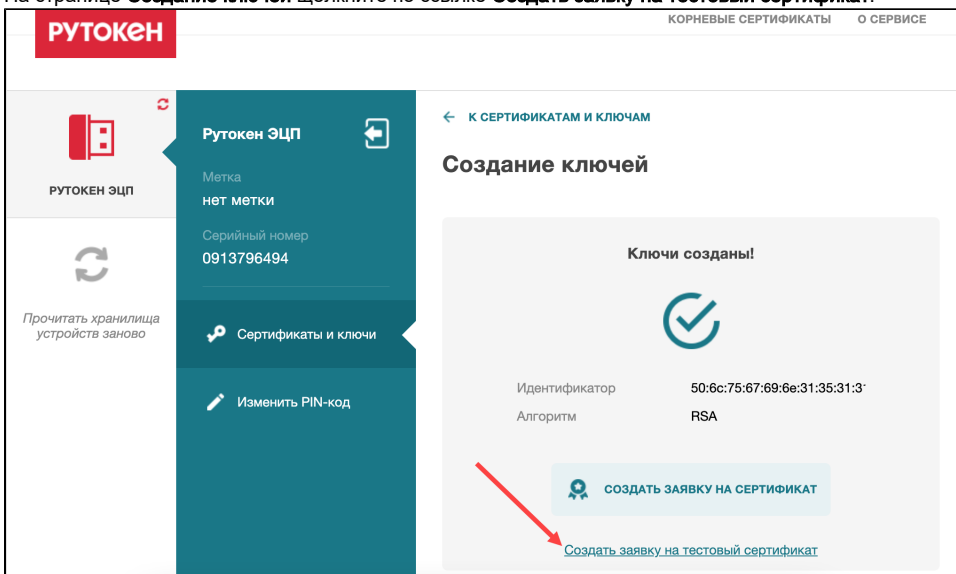
☐ ГОСТ Р 34.10-2001 — выводится из эксплуатации

2

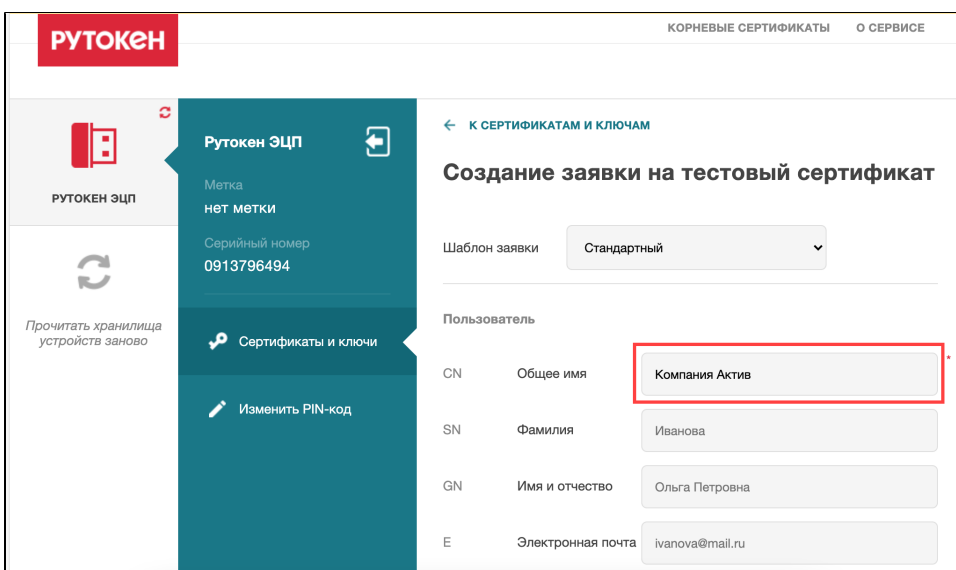
СГЕНЕРИРОВАТЬ КЛЮЧИ

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

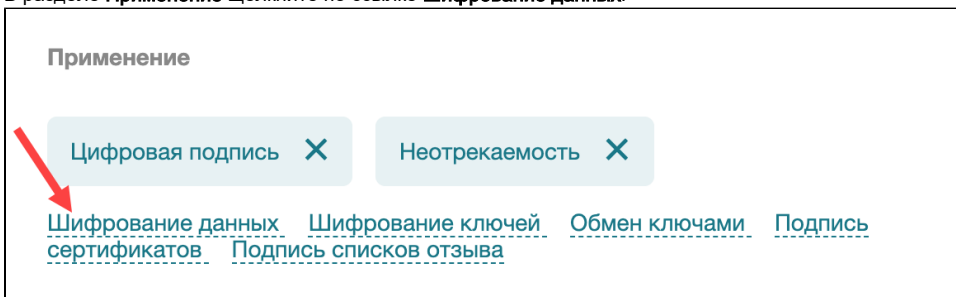
6. На странице **Создание ключей** щелкните по ссылке **Создать заявку на тестовый сертификат**.



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**.

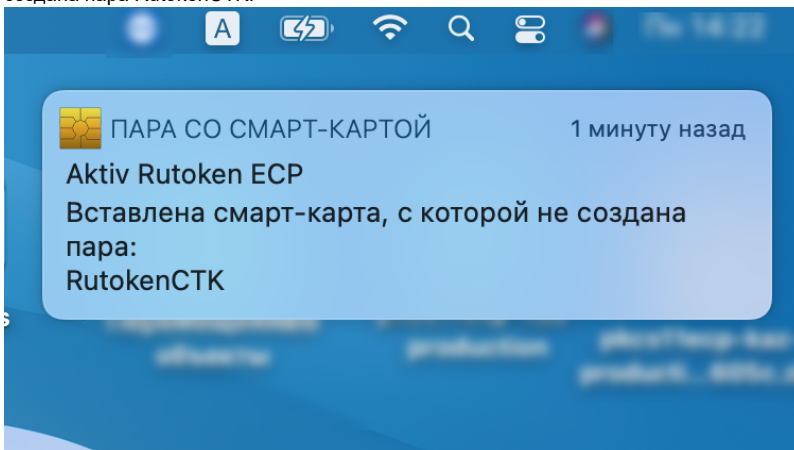


10. В разделе **Дополнительное применение** щелкните по ссылке **Аутентификация клиента**.
11. Нажмите **Создать запрос**. В результате на Рутокене будет создан сертификат RSA. После этого настройте аутентификацию по сертификату в системе.

Настройка аутентификации

Чтобы настроить аутентификацию в системе по сертификату, сохраненному на Рутокене:

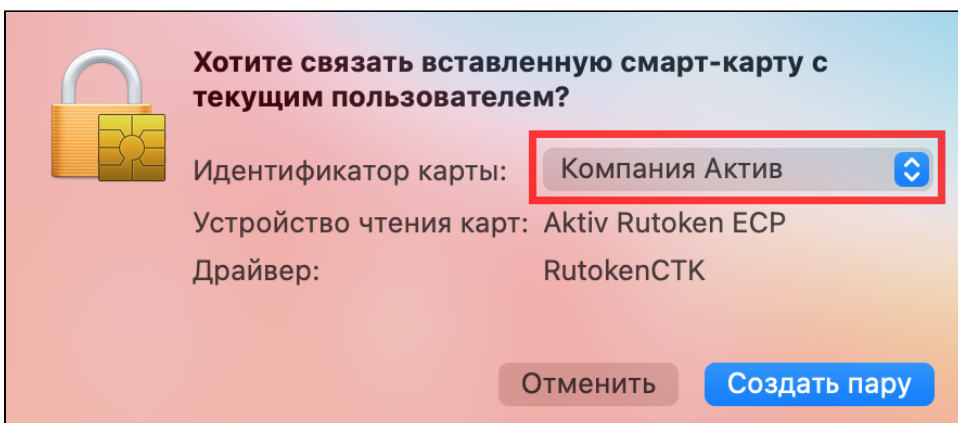
1. Подключите Рутокен к компьютеру. В правом верхнем углу отобразится уведомление о том, что вставлена смарт-карта, с которой не создана пара RutokenCTK.



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**.



Приложение «Пара со смарт-картой» пытается сопоставить текущего пользователя с владельцем смарт-карты.

Имя пользователя:

Пароль:

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



Приложение «Пара со смарт-картой» пытается выполнить аутентификацию пользователя.

Чтобы разрешить это действие, введите PIN-код.

PIN-код:

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

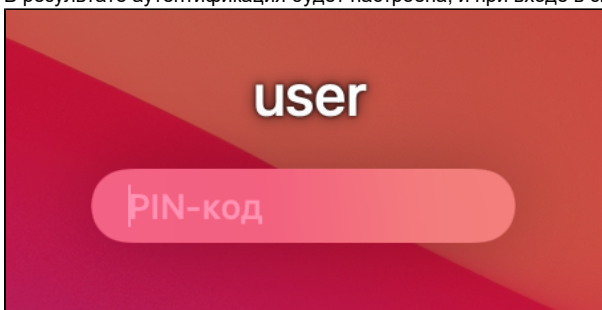


«Пара со смарт-картой» хочет использовать связку ключей «Вход».

Введите пароль связки ключей.

Пароль:

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



user

PIN-код