ТЕХНОЛОГИЧЕСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН DAY

ТЕХНОЛОГИИ ДОВЕРИЯ

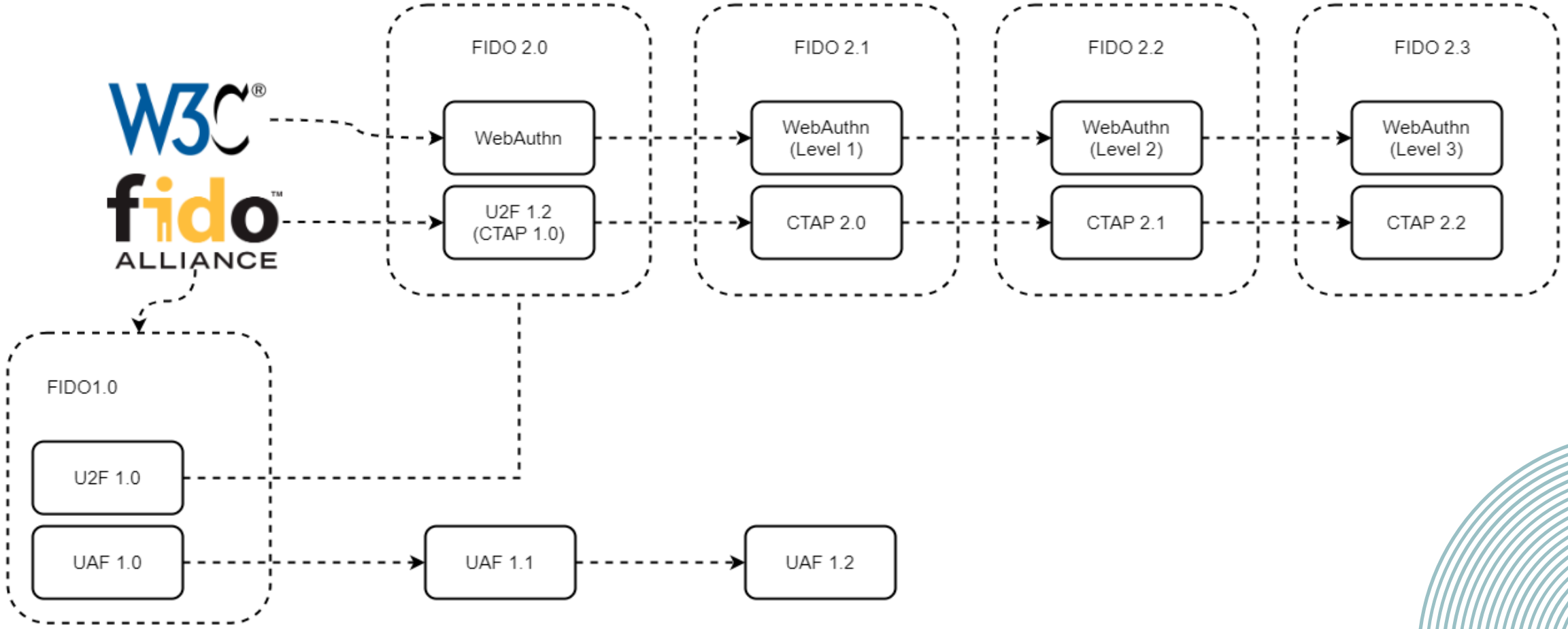
КОМПАНИЯ АКТИВ

Возможности использования технологии FIDO2

Татьяна Калужнина

эксперт и разработчик ОС Рутокен, Компания «Актив»

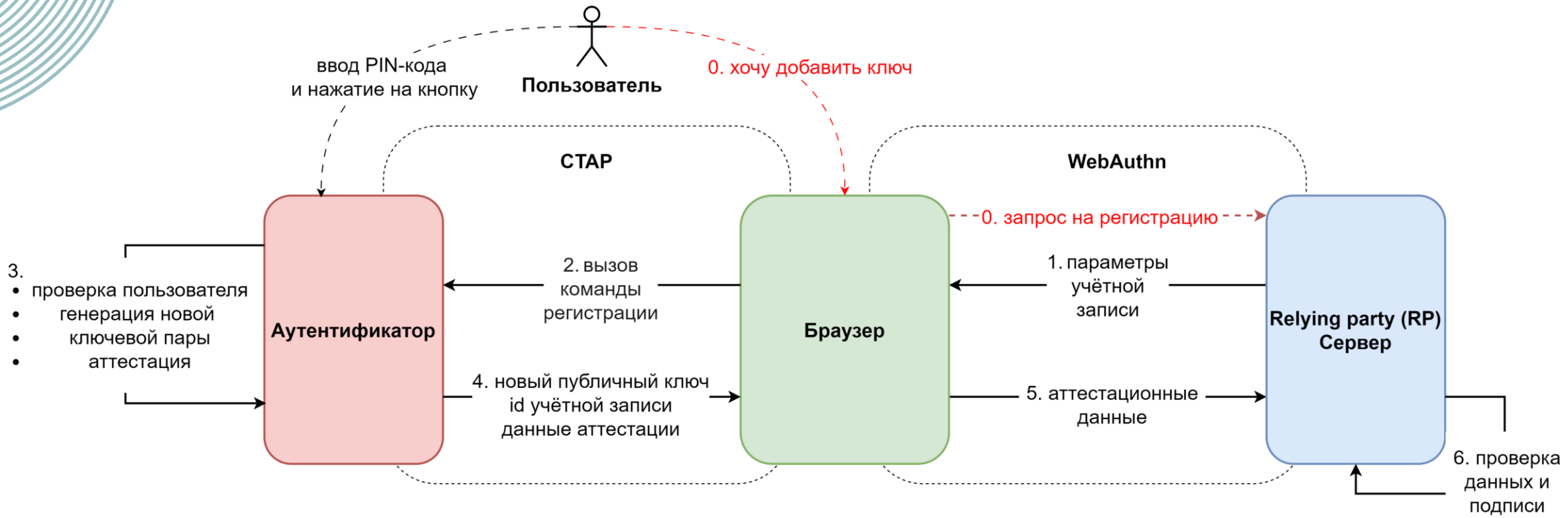
FIDO2 = WebAuthn + CTAP



FIDO2 это:

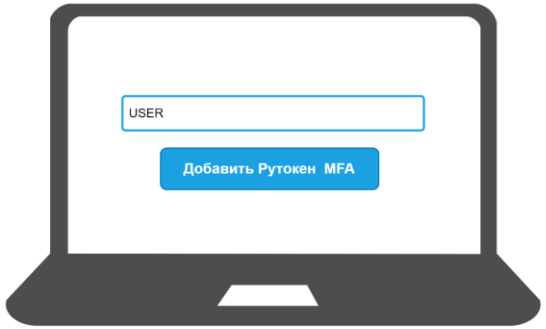
- Безопасность
- Удобство
- Масштабируемость
- Расширяемость

Регистрация



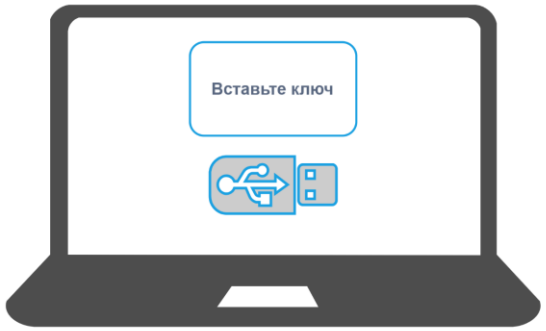
Регистрация

1



Добавьте аутентификатор

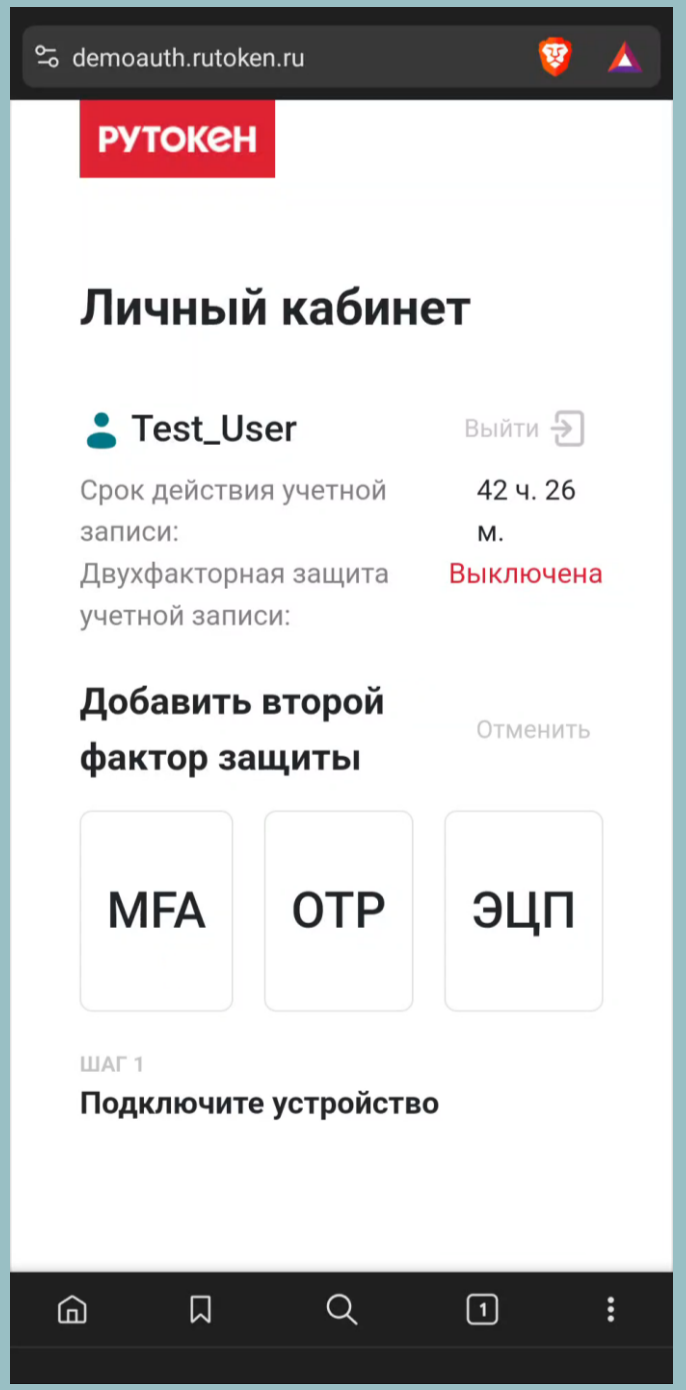
2



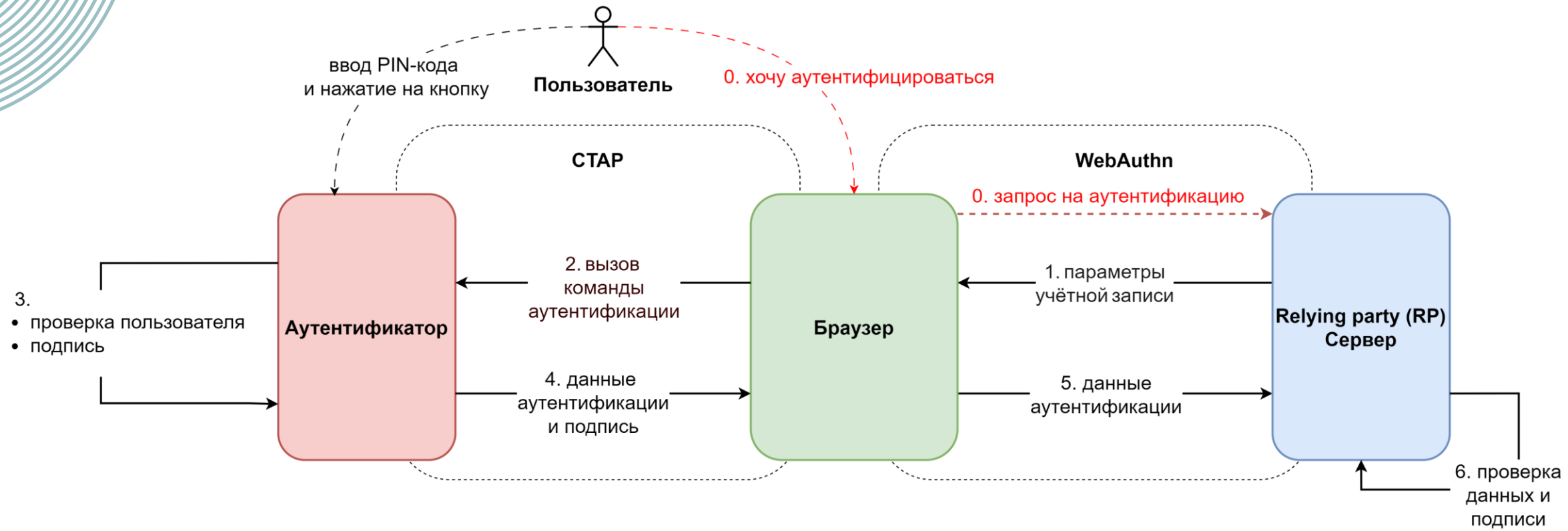
Вставьте ключ, введите PIN-код и нажмите на кнопку

3

Успешная регистрация!

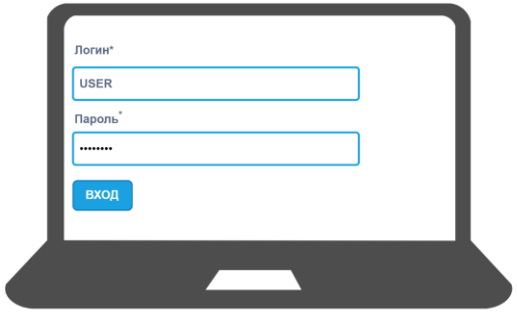


Аутентификация



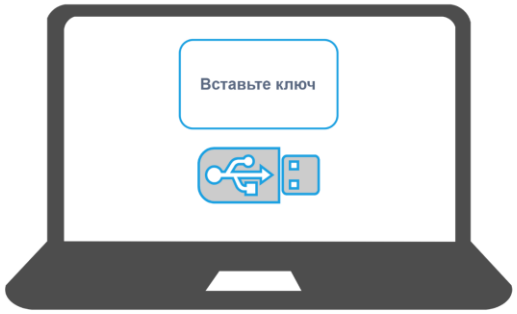
Второй фактор

1



Введите имя и пароль

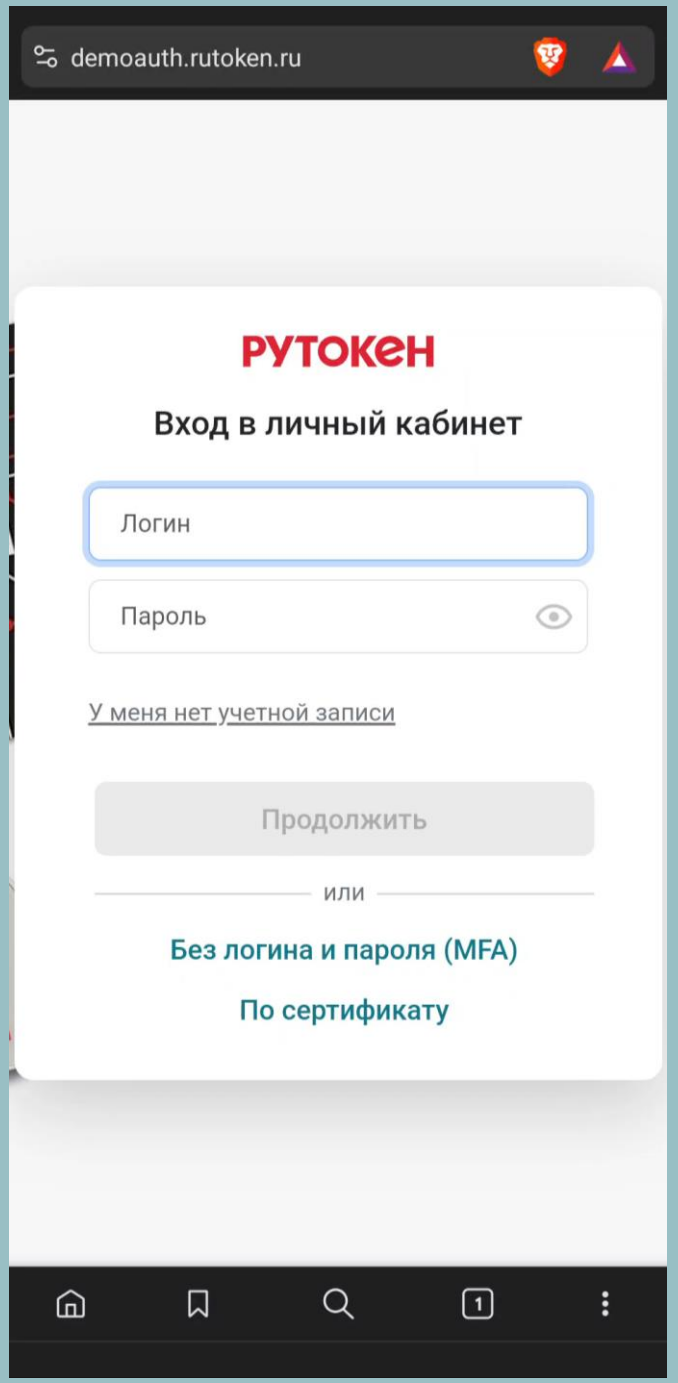
2



Вставьте ключ, введите PIN-код и нажмите на кнопку

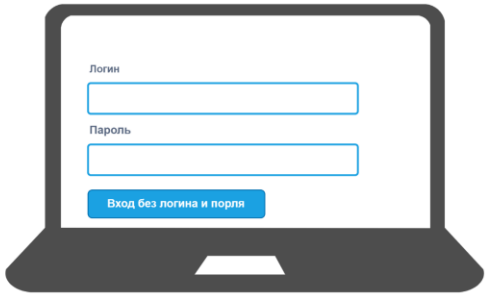
3

Успешная аутентификация!



Беспарольная аутентификация

1



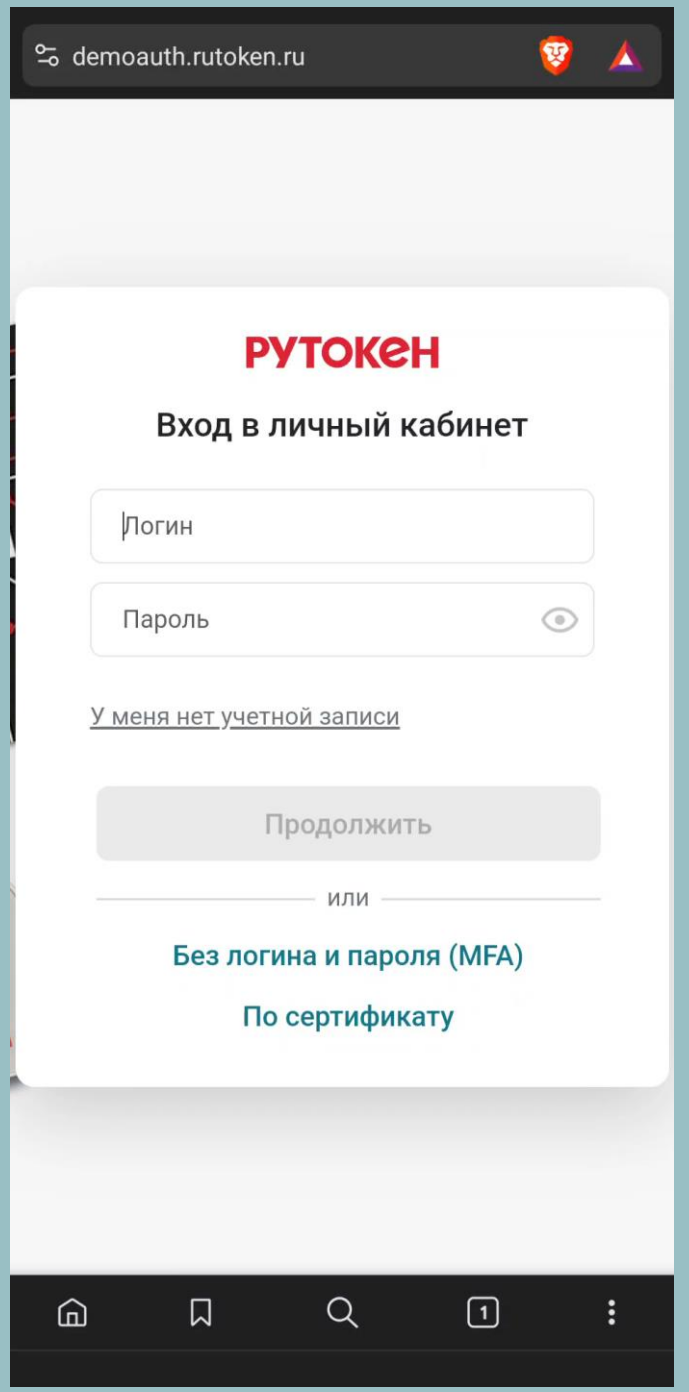
Выберите вход без логина и пароля

2

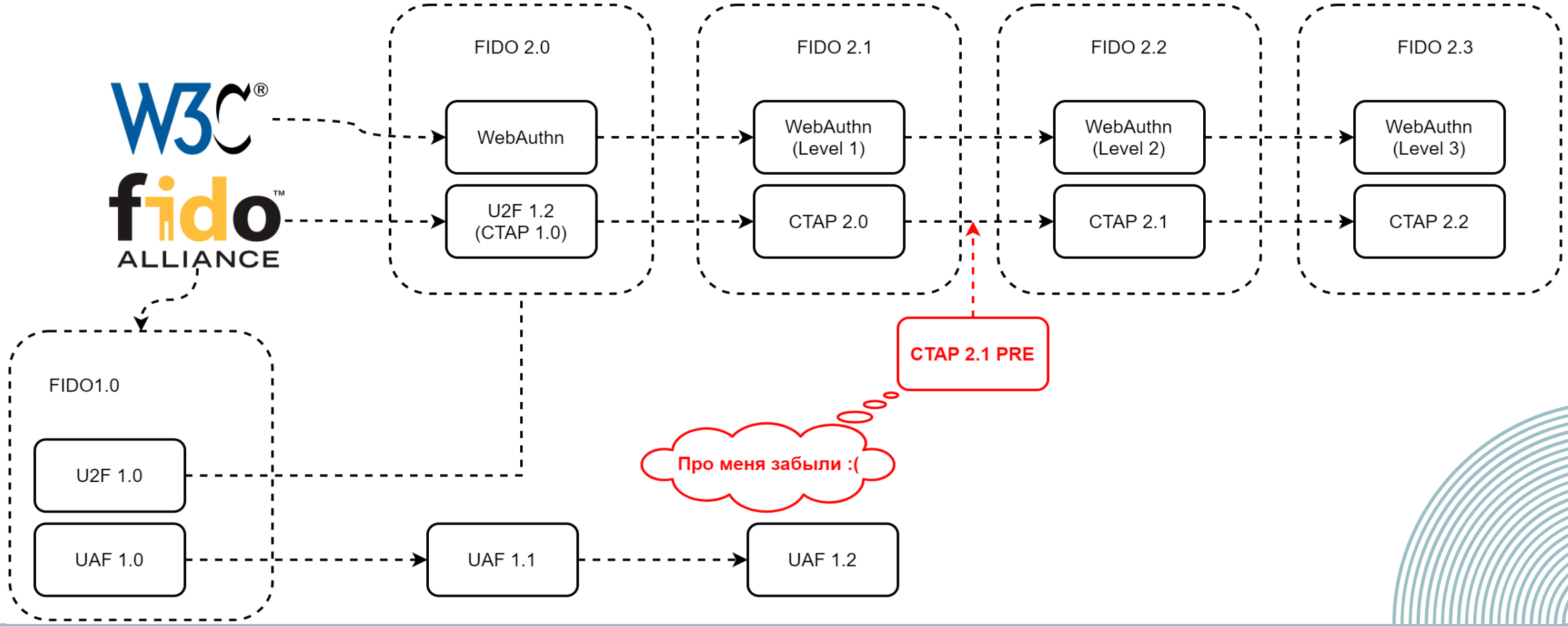
Вставьте ключ, введите PIN-код и нажмите на кнопку

3

Успешная аутентификация!

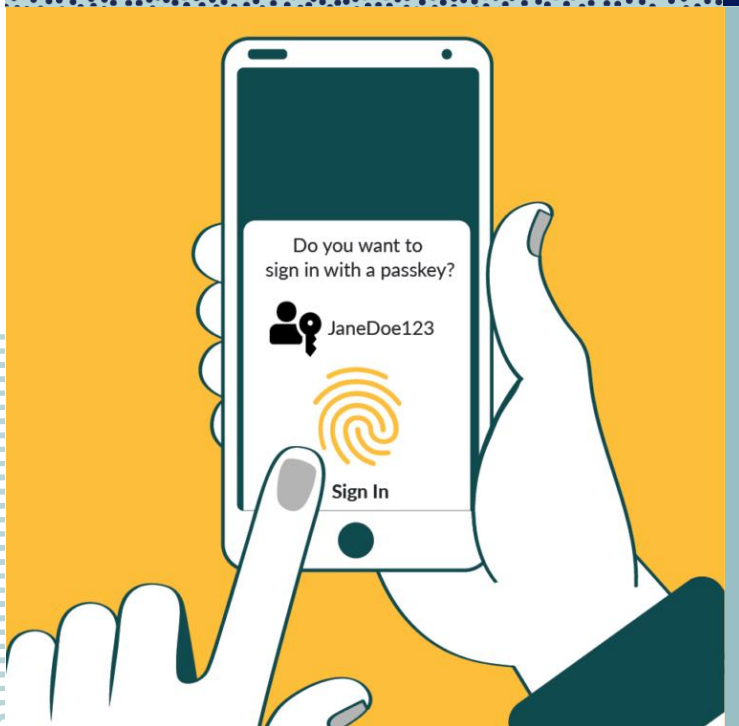


Возможность управления учётными данными

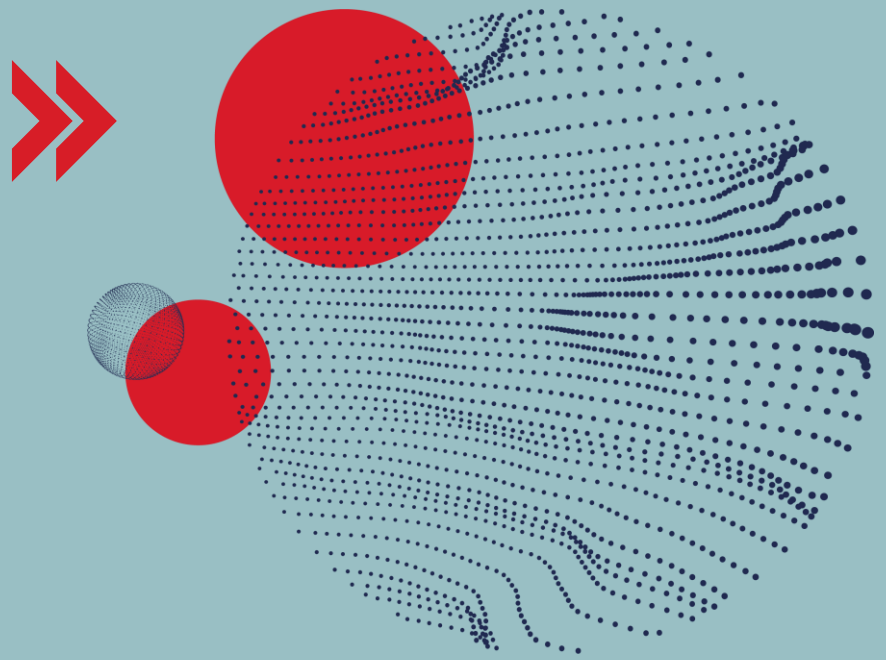


Что такое Passkey?

- Технология основана на WebAuthn.
- Вход с использованием того же процесса, который применяется для разблокировки своего устройства (скан лица, отпечаток пальца, PIN-код от экрана блокировки).



Passkey



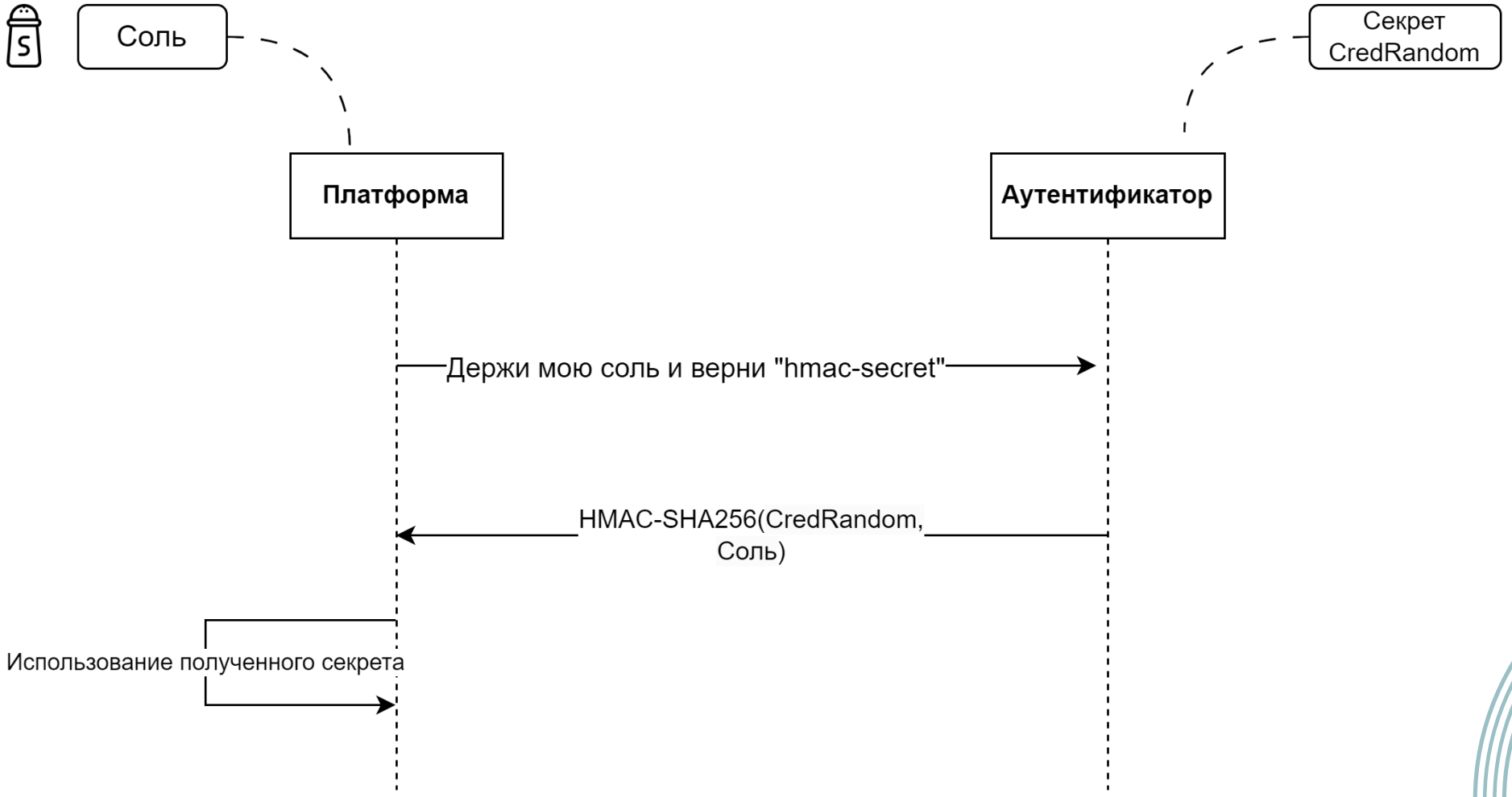
Регистрация:

- Генерация ключевой пары
- **А)** Хранение приватного ключа на устройстве (discoverable credential)
  - Использует место на устройстве
- **Б)** Хранение на веб-сайте
  - Шифрование приватного ключа на мастер ключе
  - **-** Невозможен сценарий passwordless
  - **+** Безграничное хранилище
- Веб-сайт хранит публичный ключ

Аутентификация:

- Генерация подписи с помощью приватного ключа
- Проверка подписи веб-сайтом с помощью сохраненного открытого ключа

Расширение “hmac-secret ”



“Hmac-secret” для шифрования дисков в Linux

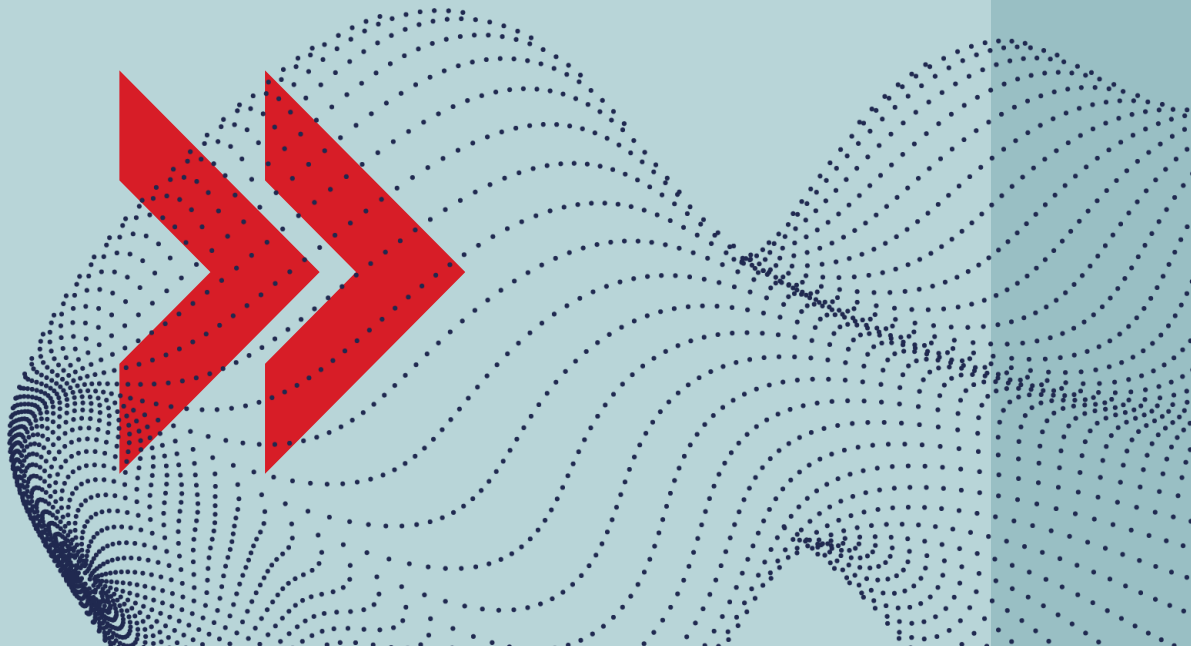
Необходима версия systemd от 248

#0 Регистрация аутентификатора

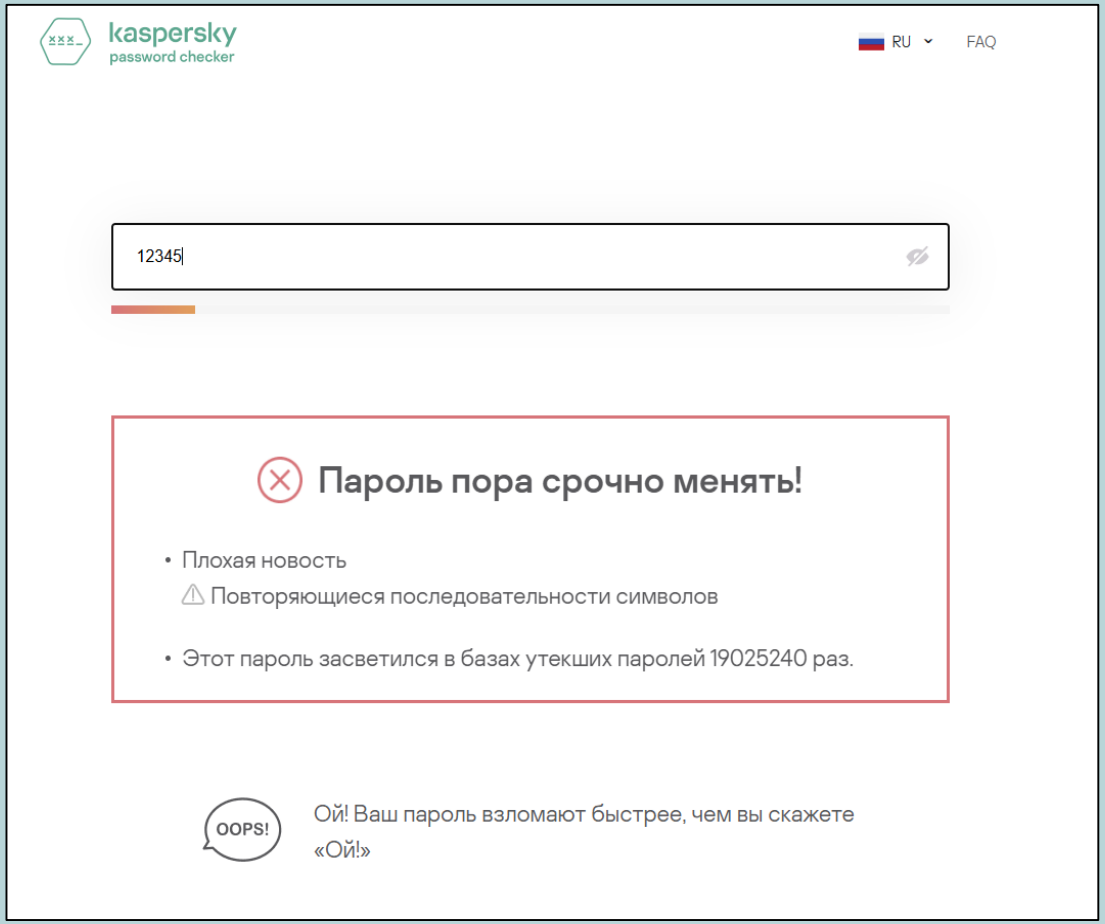
#1 При загрузке системы компонент systemd-cryptsetup ждет аутентификатор

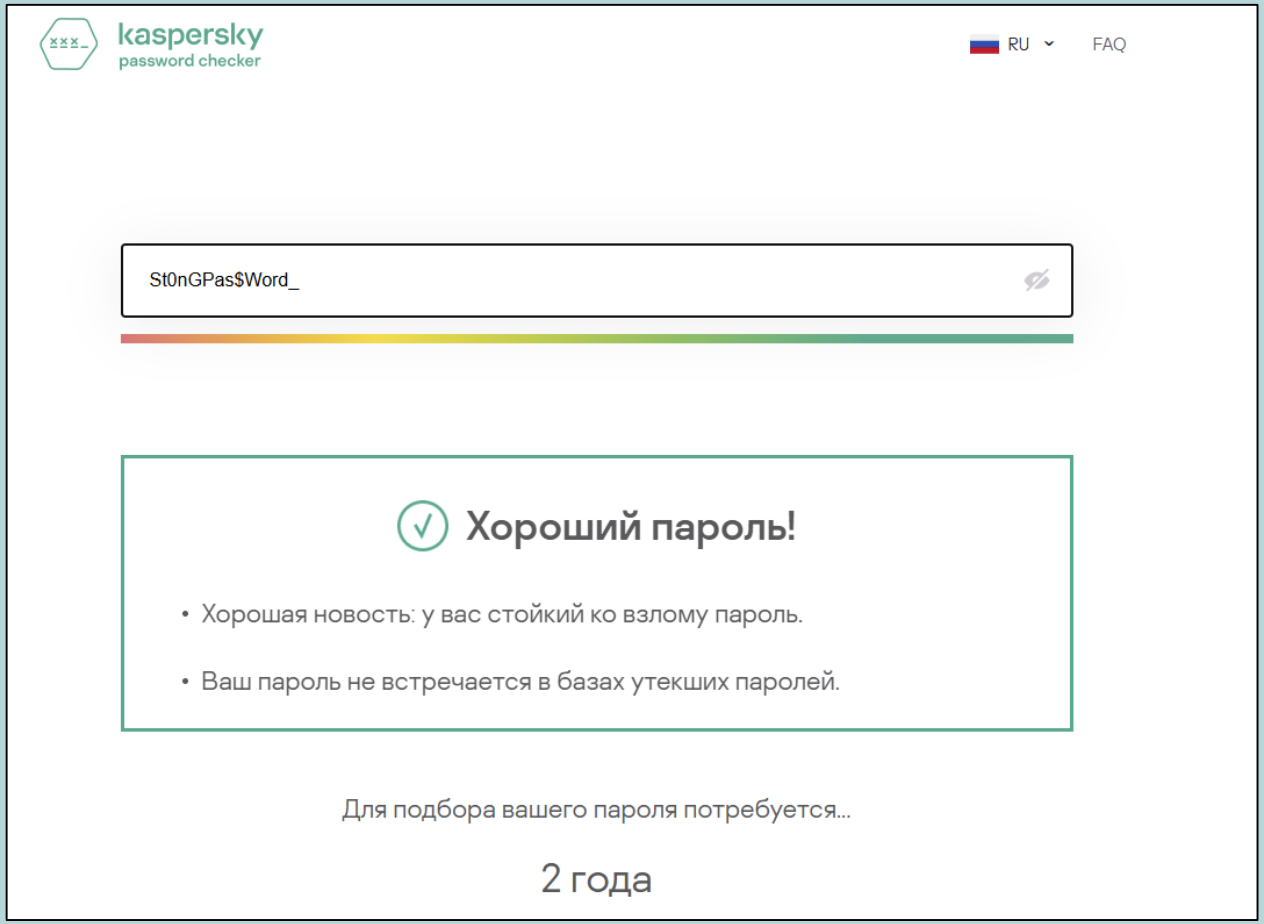
#2 Пользователь вводит PIN-код и нажимает на кнопку

#3 Systemd-cryptsetup посылает аутентификатору соль. Получает обратно ключ и использует его для разблокировки тома. The End



Расширение “pinComplexityPolicy”

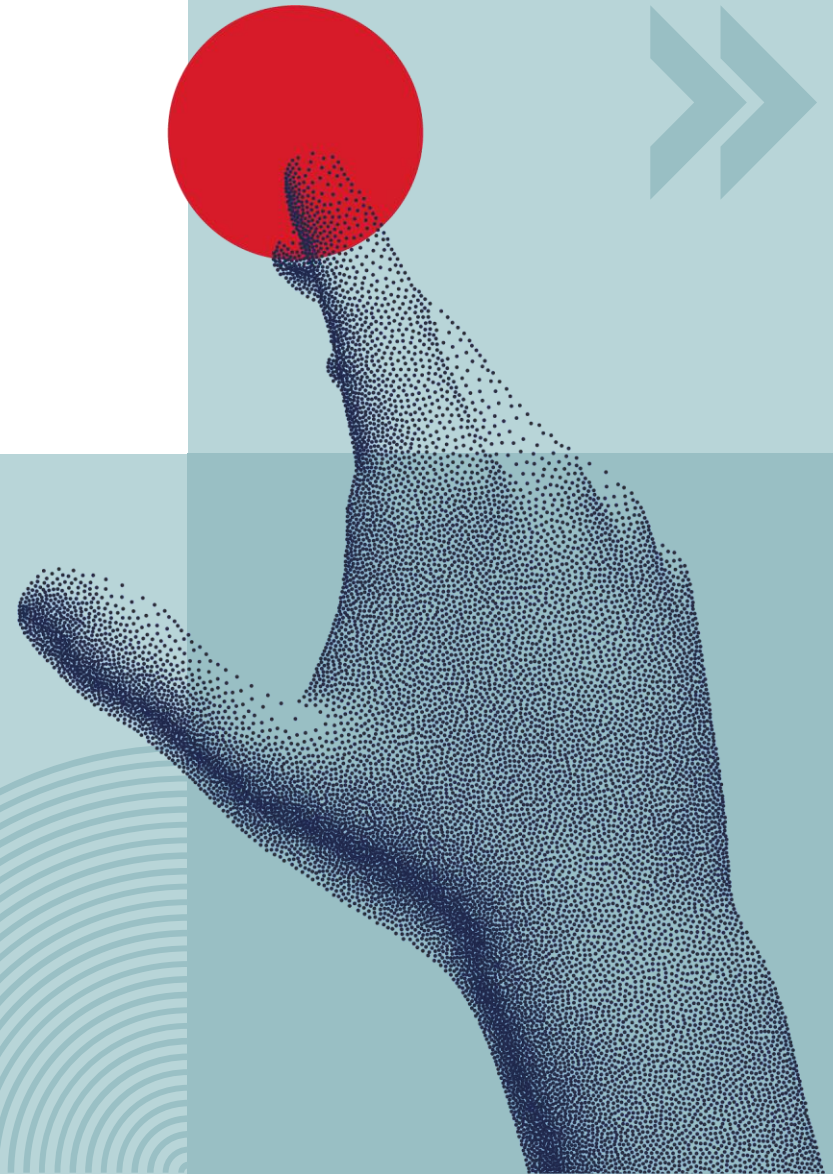




Расширение “pinComplexityPolicy”

Расширение позволяет настроить:

- минимальную длину PIN-кода
- максимальную длину PIN-кода
- требования к составу PIN-кода (например, наличие цифр, букв, специальных символов)
- требования к повторению PIN-кода (например, запрет на повторение одного и того же PIN-кода)
- требования к смене PIN-кода (например, необходимость смены PIN-кода каждые 60 дней).



Итак, что мы имеем?

#1

Повышенная безопасность, соответствующая международным стандартам и удобство использования.

#2

Привлекательный выбор для организаций и пользователей, стремящихся улучшить безопасность своих учетных записей и упростить процесс аутентификации.

#3

Активная поддержка и развитие технологии FIDO2.

КОМПАНИЯ АКТИВ

РУТОКЕН DAY

Контактная информация

Татьяна Калужнина

Эксперт
и разработчик ОС Рутокен,
Компания «Актив»

kaluzhninatatyana@rutoken.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90