Криптографическая аутентификация

 вконтакте

 безымянные

Наша команда

Всеволод Деткин
Backend-разработчик

Даниил Неслуховский
Frontend-разработчик

Егор Алтынов
Data Scientist

Пётр Ильин
Backend-разработчик

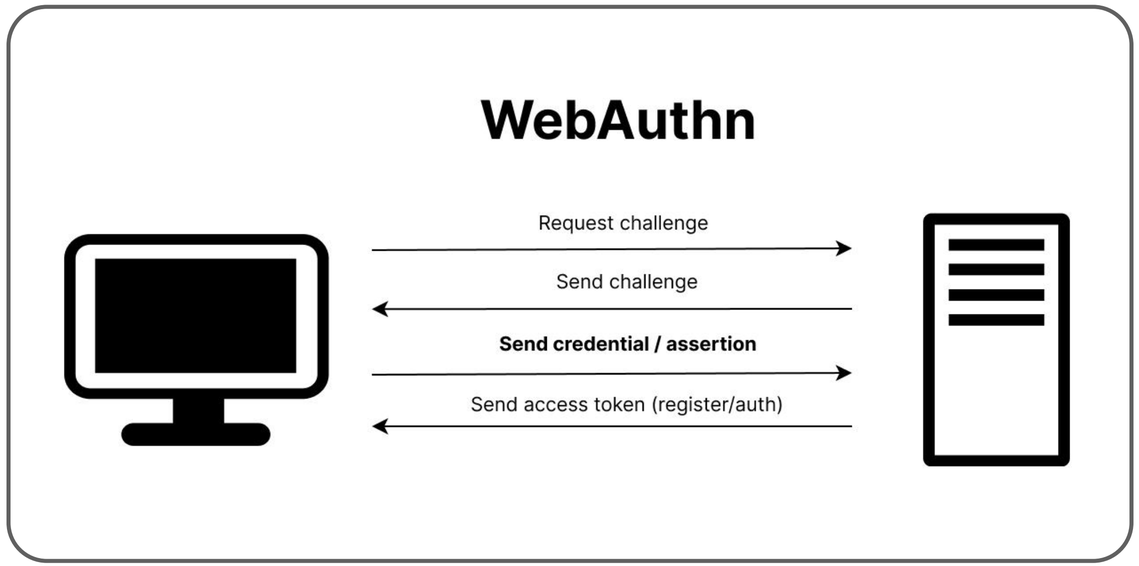
вконтакте

безымянные

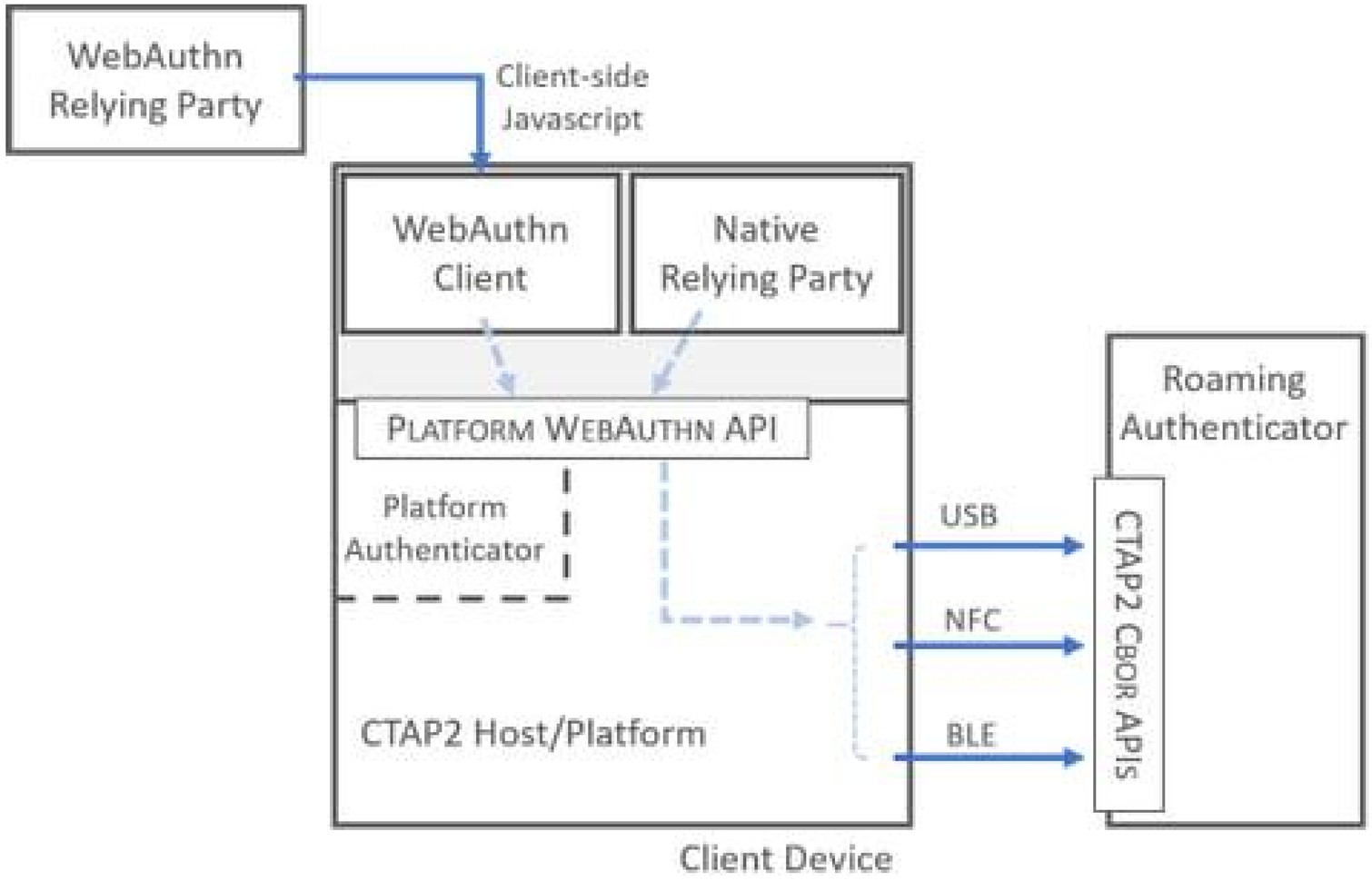
Проблематика

По стандарту WebAuthn все сгенерированные профили (пары ключей) сохраняются в статичном приватном хранилище на определенном устройстве, из-за чего процесс копирования профилей между устройствами является крайне проблематичным.

Необходимо продумать решение, которое позволило бы хранить ключи в облаке и синхронизировать их для пользователя.



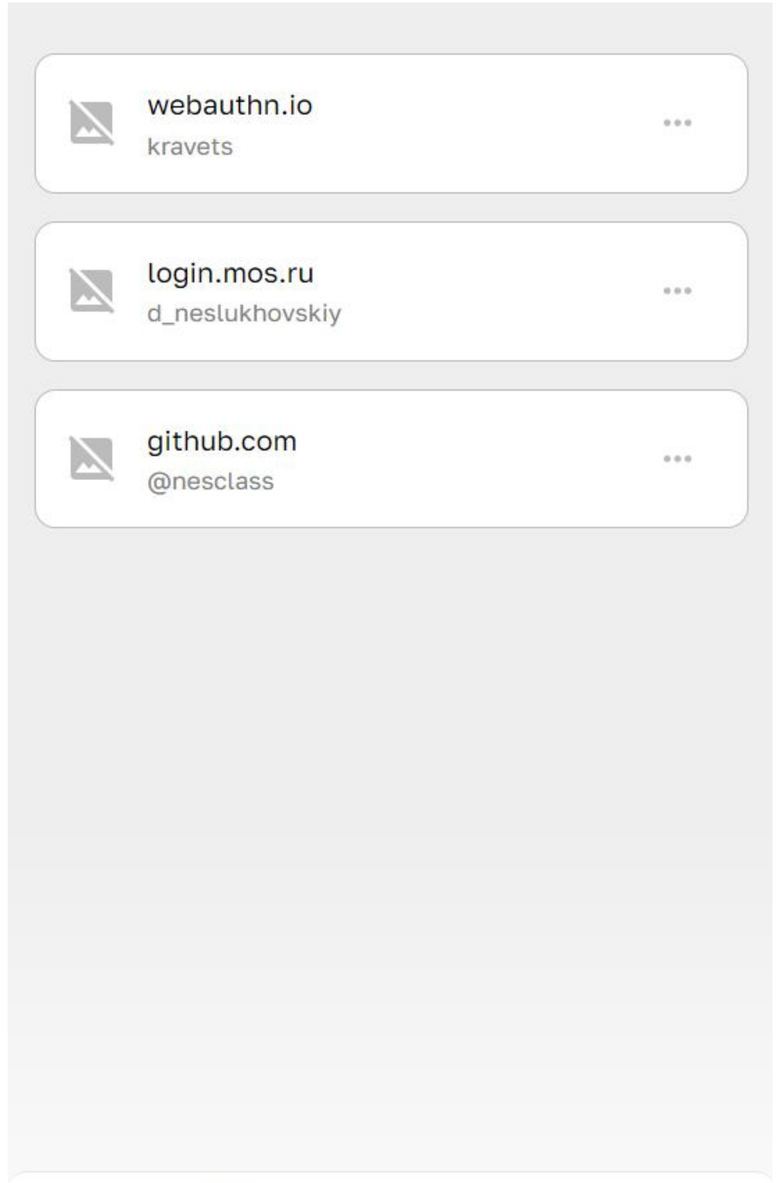
Тонкости реализации WebAuthn



Решение

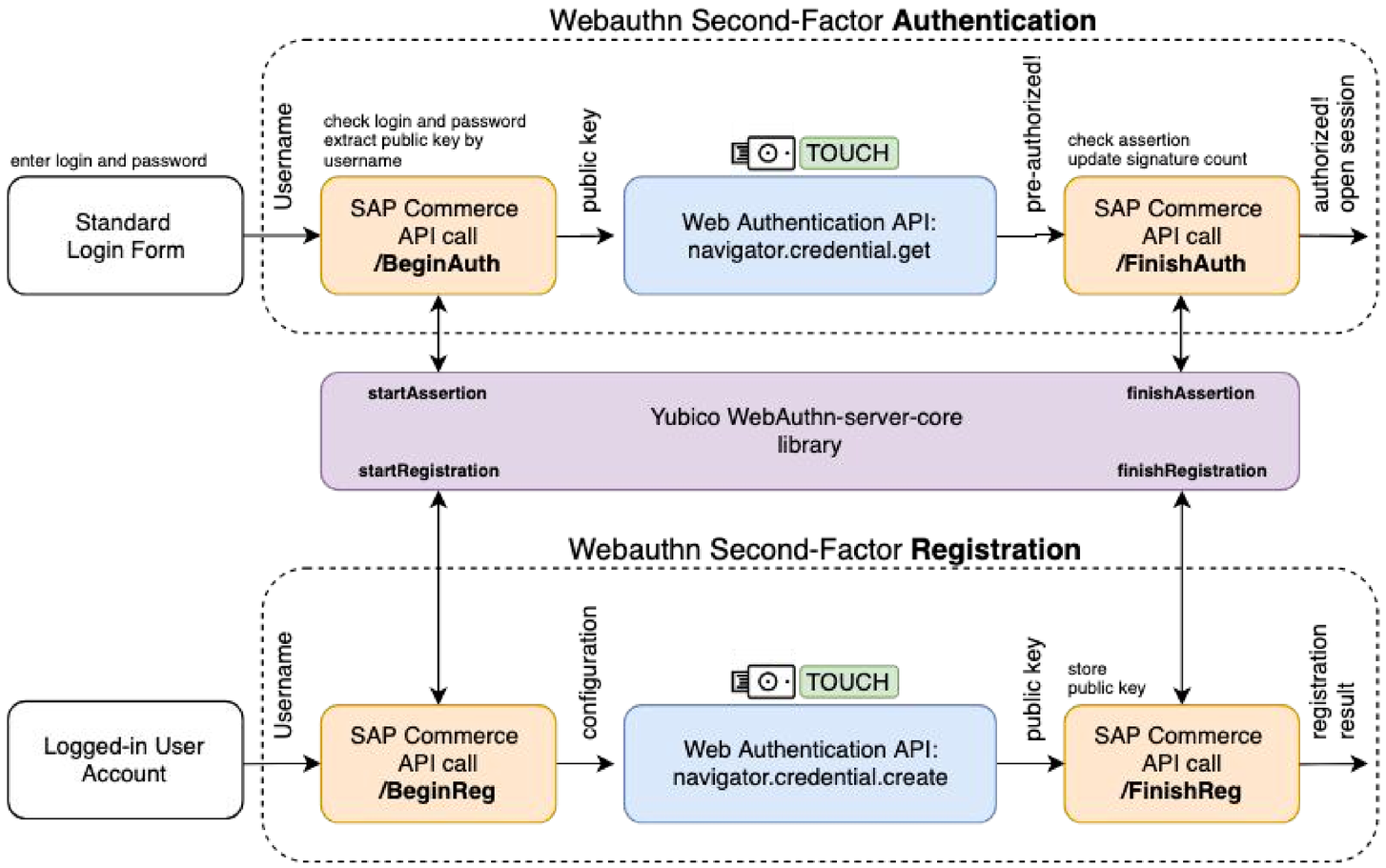
Мы разработали MVP-приложения
для операционной системы Windows,
которое эмулирует USB FIDO2 носитель
по CTAP-протоколу через USB/IP-сервер
со вшитым контролируемым реестром ключей.

Такое решение легко портируется на другие
операционные системы, и работает без лишних
тягот и компромиссов для пользователя в
живых браузерах без поднастроек.

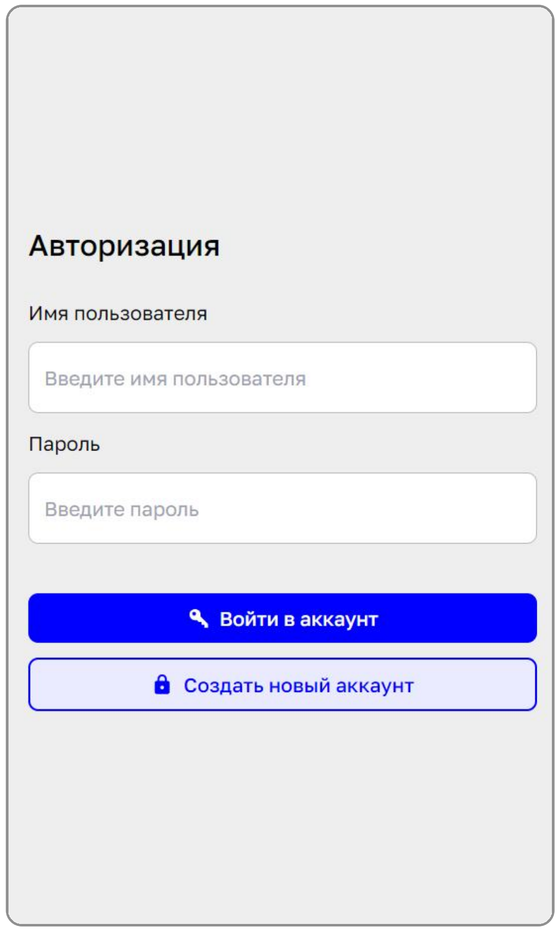


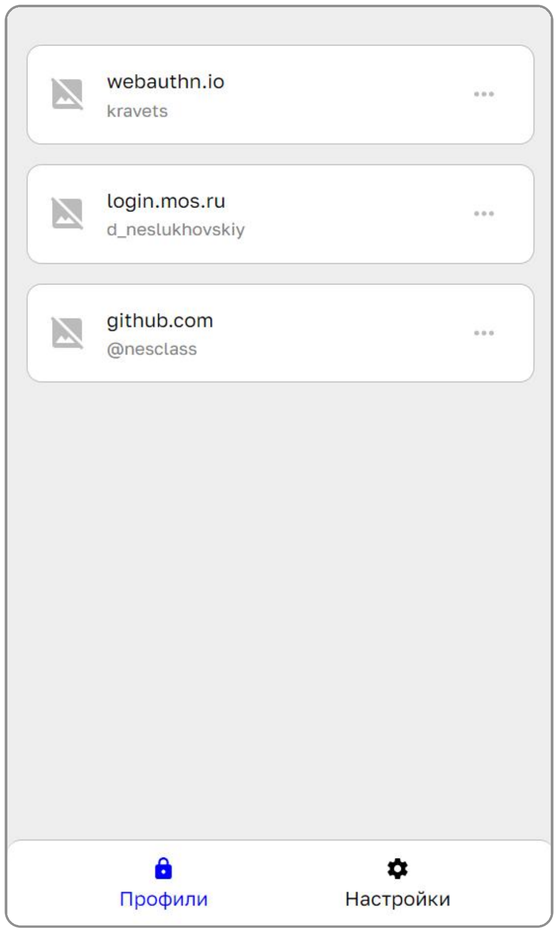
вконтакте

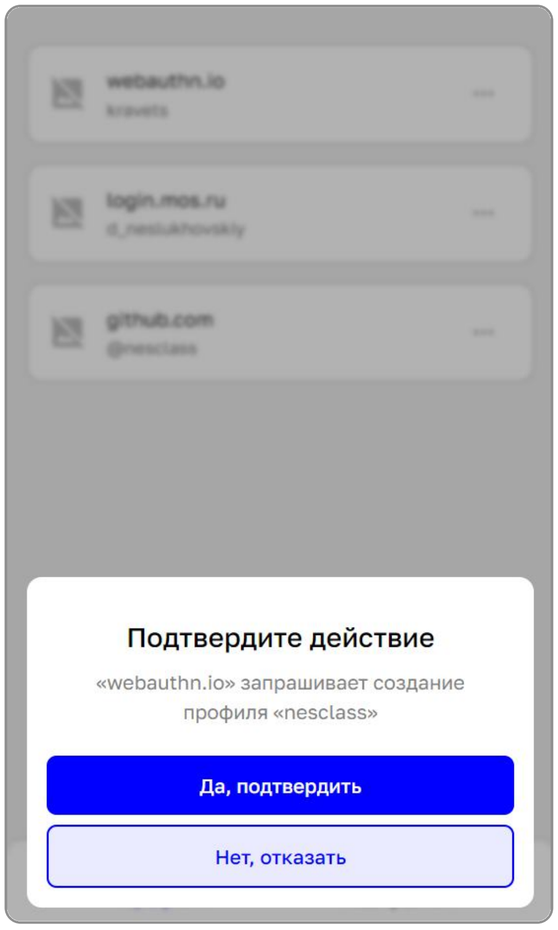
Как это работает?

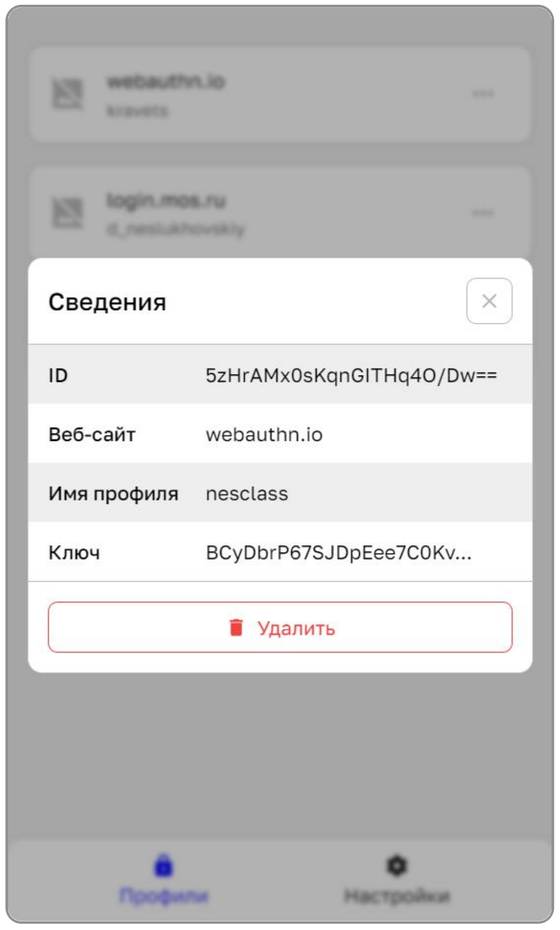


А как выглядит на практике?









вконтакте

безымянные

Архитектура решения

Что ещё можно улучшить?

1. Портировать приложение на Linux и Mac OS средствами Wales
2. Придумать алгоритм для подписи криптоконтейнера с участием пользователя
3. Сделать восстановление аккаунта с обнулением реестра ключей

Спасибо за внимание!

Ссылка на телеграм-канал

team_noname

Ссылка на исходный код

noname-to/nuclear-linker