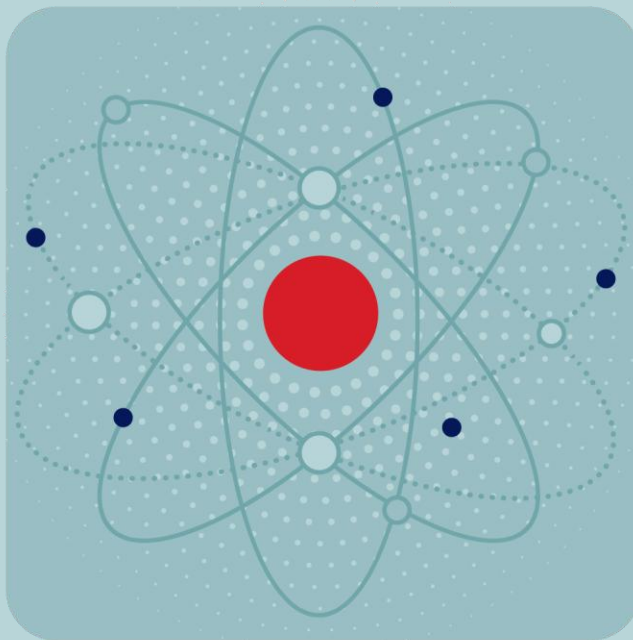


ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН

ЦАЧ

ТЕХНОЛОГИИ
ДОВЕРИЯ



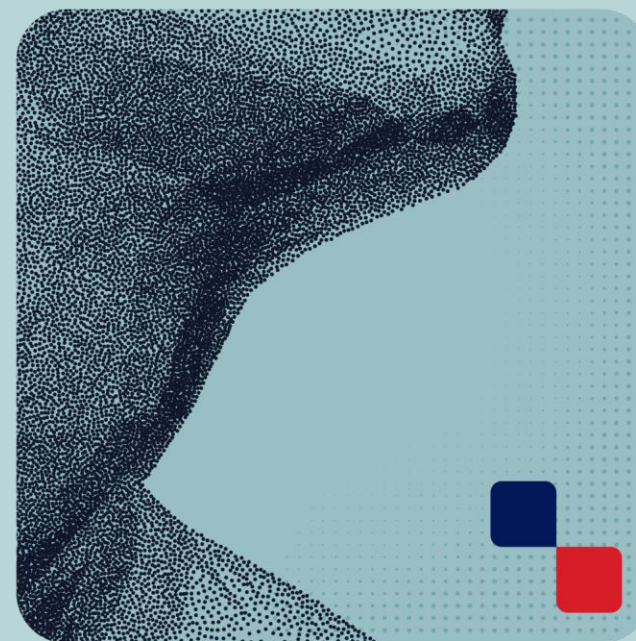
КОМПАНИЯ
ПРАКТИВ



Некастодиальное хранение криптоактивов

**Павел
Анфимов**

Заместитель директора
по управлению продуктами Рутoken,
Компания «Актив»



Какие бывают криптокошельки



Владение криптоактивом =
владение закрытым ключом

Где хранится закрытый ключ?



124



Какие бывают криптокошельки



Кастодиальное хранение

- ✓ Ключ хранит биржа (банк) и дает доступ к нему



Облачное хранение
ключа электронной
подписи

Некастодиальное хранение

- ✓ Ключ хранит сам пользователь



Классическое
хранение ключа
электронной подписи

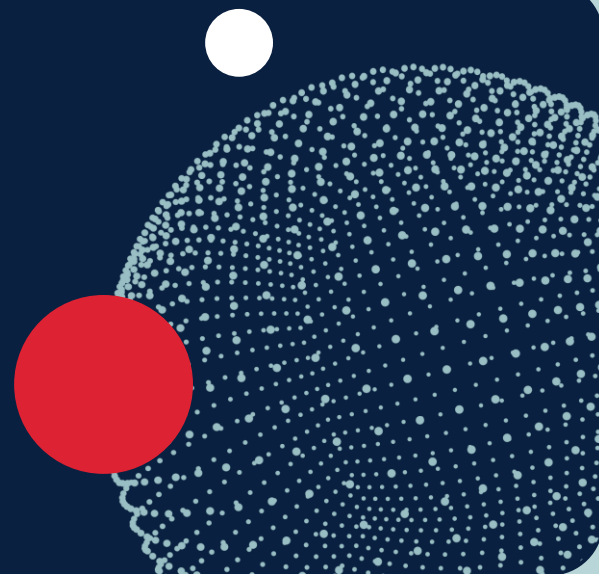
Безопасность криптоактивов



Некастодиальное хранилище
закрытого ключа —
криптокошелек

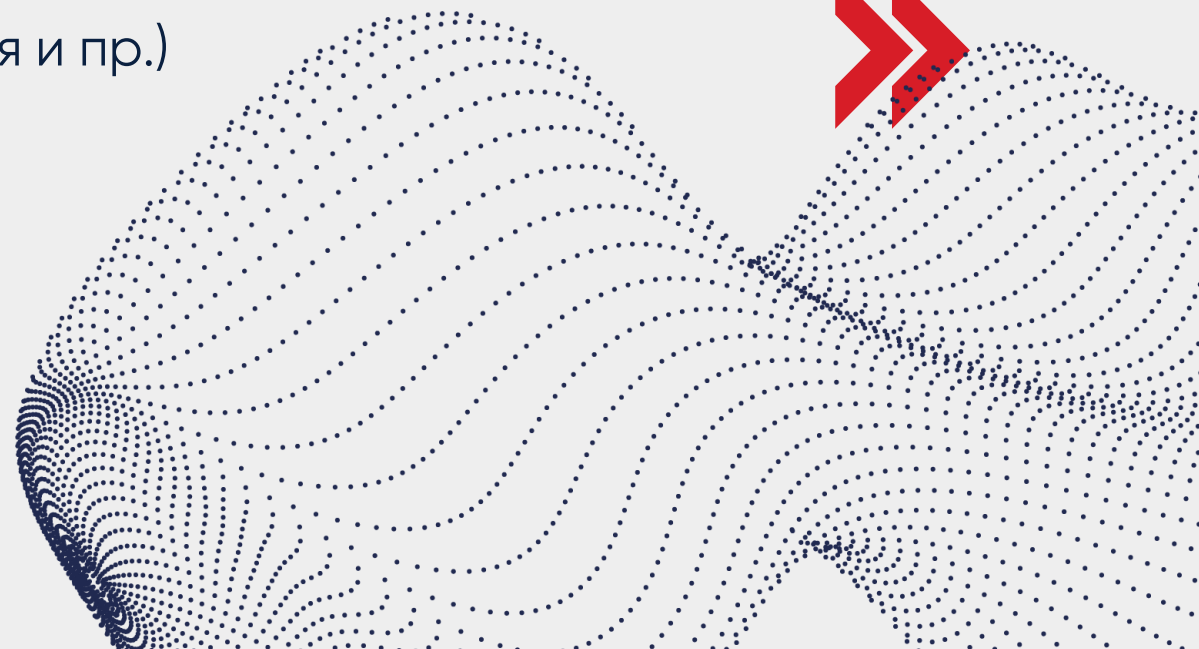


Безопасность закрытого ключа —
это условие того, что активы не будут
потеряны в результате атаки
злоумышленников или утраты
самого ключа



Требования к некастодиальному криптокошельку

- ✓ Отчуждаемое устройство (для хранения отдельно от компьютера)
- ✓ Защита от взлома
- ✓ Криптографическое вычисление эл. подписи на борту
- ✓ Защита от НСД (ПИН-код, биометрия и пр.)
- ✓ Удобство в использовании

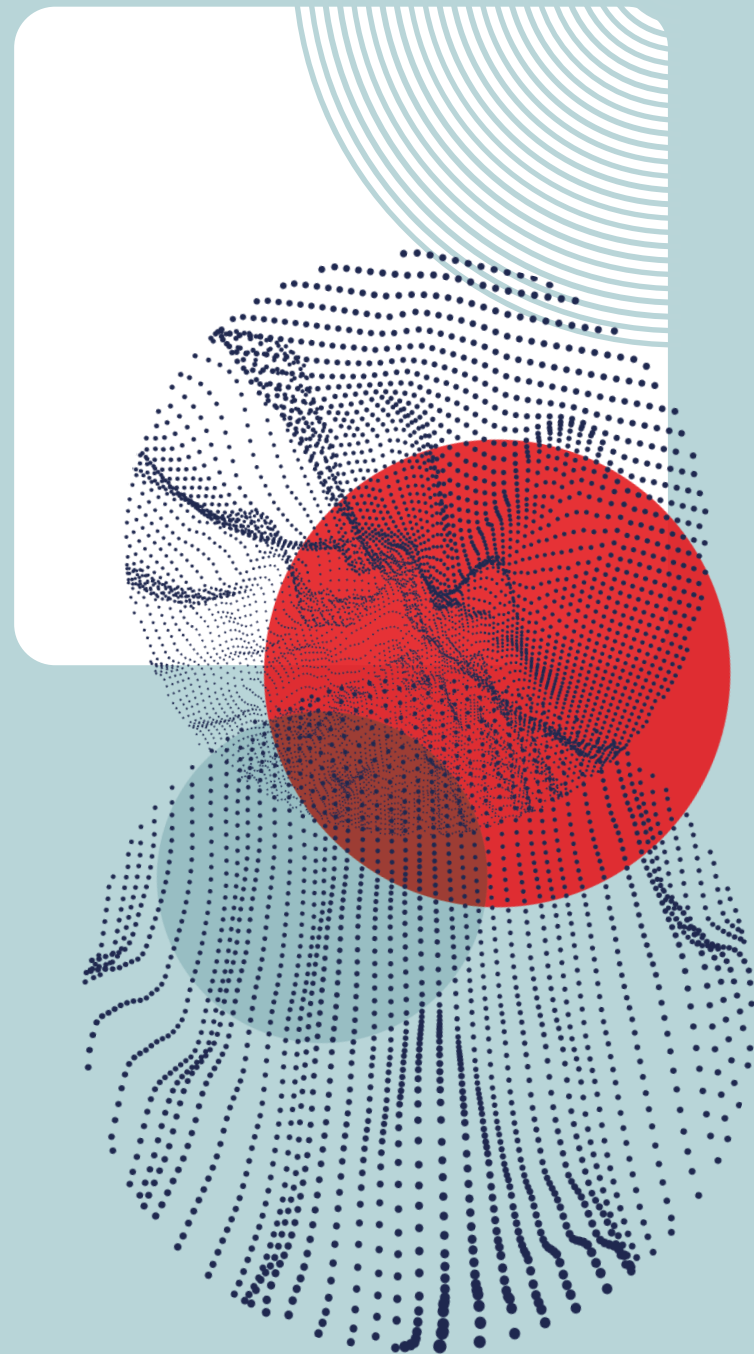


Сходства криптокошелька и средства электронной подписи

Свойства	Средство ЭП	Криптокошелек
Подпись на борту	да	да
Неизвлекаемое хранение закрытого ключа	частично	да*
Физическое подтверждение операций	частично	да
Форм-фактор USB/NFC-устройства	да	да
Доверие к производителю	да	да

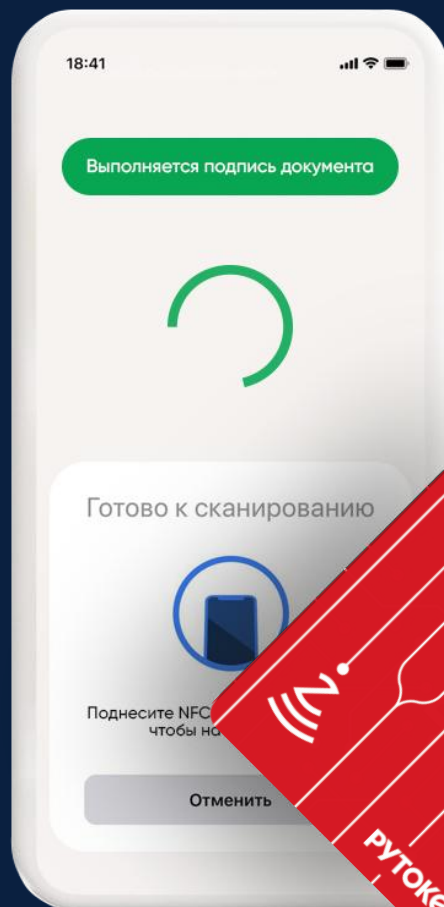
Чего не хватало в устройствах Рутокен ЭЦП 3.0

- ✓ Поддержки специальной эллиптической кривой EdDSA (Ed25519)
- ✓ Экспорта мнемонической фразы после генерации закрытого ключа согласно BIP39
- ✓ Импорта ключа по мнемонической фразе согласно BIP39
- ✓ Поддержки новых функций в API



Первый российский аппаратный **криптокошелёк**

Безопасно

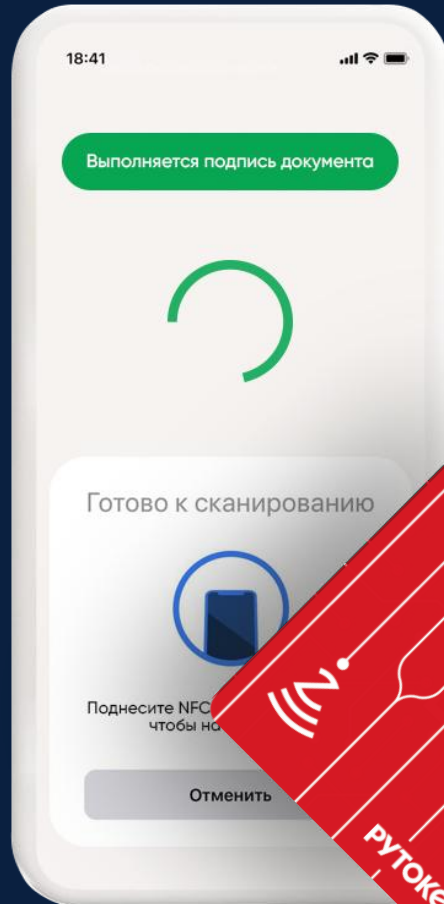


- ✓ Активы защищены от кражи
- ✓ Закрытый ключ не хранится на ПК
- ✓ Защищенный микрочип (Secure Element)



Первый российский аппаратный **криптокошелек**

Удобно 



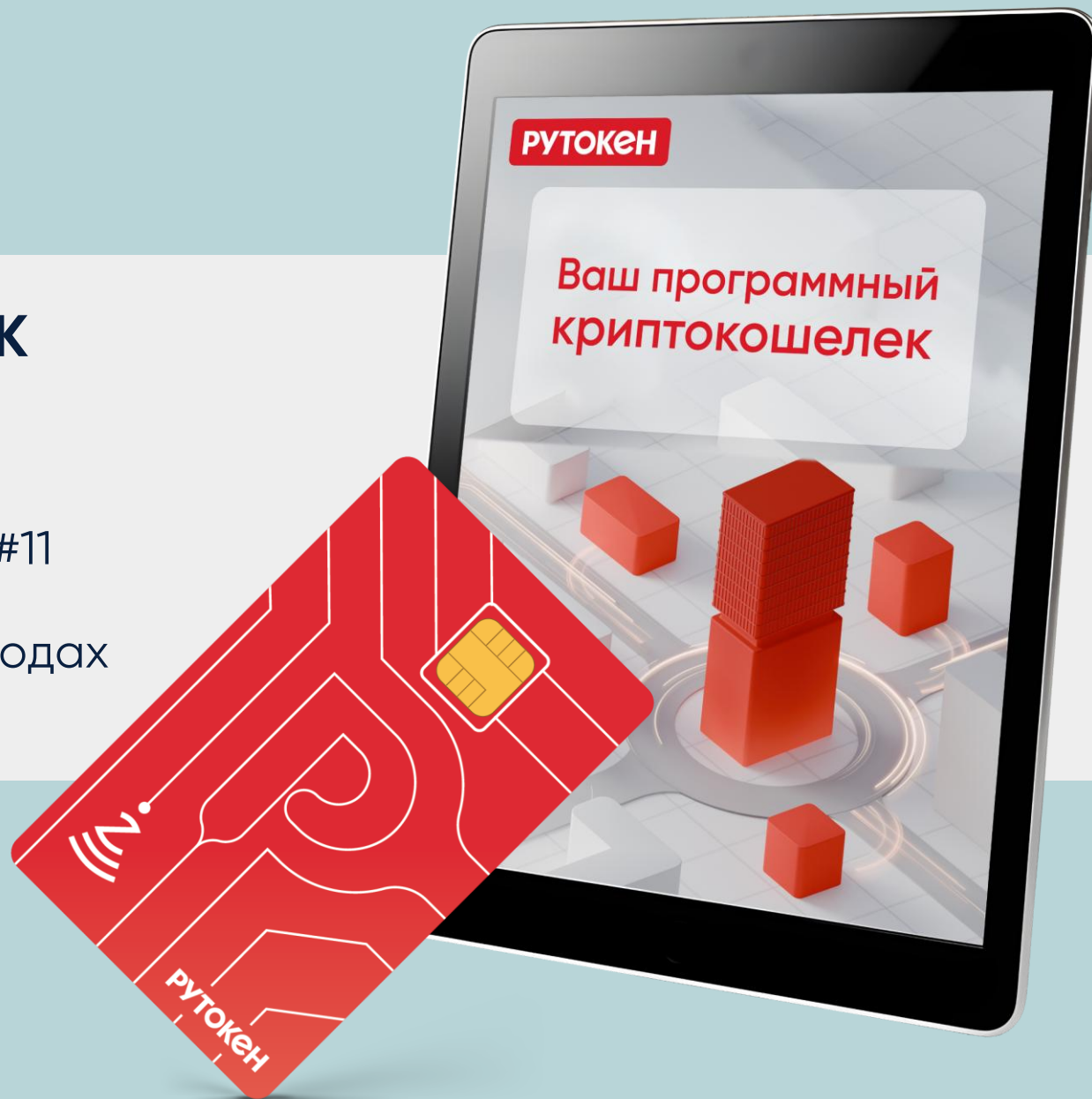
- ✓ Подписание транзакций путем прикладывания карты к мобильному устройству
- ✓ Поддержка сетей Bitcoin, Ethereum, TON, Solana, TRON



Архитектура решения

Рутокен КriptoКошелек SDK

- ✓ Специальная смарт-карта
- ✓ Специальная библиотека PKCS#11
- ✓ Демо-приложения в исходных кодах



Расширяем список внедрений



Новость

Компании «Актив» и «Пульсар» подписали соглашение о научно-техническом партнерстве



Новость

Сбер впервые выдал обеспеченный криптовалютой кредит



Внедрение

Интеграция с платформой Цифровое казначейство от Web3Tech





Павел
Анфимов

Заместитель директора
по управлению продуктами
Рутокен,
Компания «Актив»



panfimov@rutoken.ru
info@rutoken.ru



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



+7 495 925-77-90
+7 926 586-90-96