



# SafeShare

безопасная передача файлов  
со сквозным шифрованием

Автор: Нагребецкий Михаил

Руководитель: Коротаев Вадим

г. Омск, школа №120

# Проблема



## Мессенджеры и email

Сервер имеет доступ к содержимому файлов



## Облачные хранилища

Провайдер видит ваши данные



## Веб-сервисы передачи

Нет сквозного шифрования



## P2P (AirDrop, LocalSend)

Оба устройства должны быть онлайн одновременно

# Решение

## Zero-knowledge архитектура



Шифрование  
на устройстве



Передача  
шифртекста



Расшифровка  
на устройстве

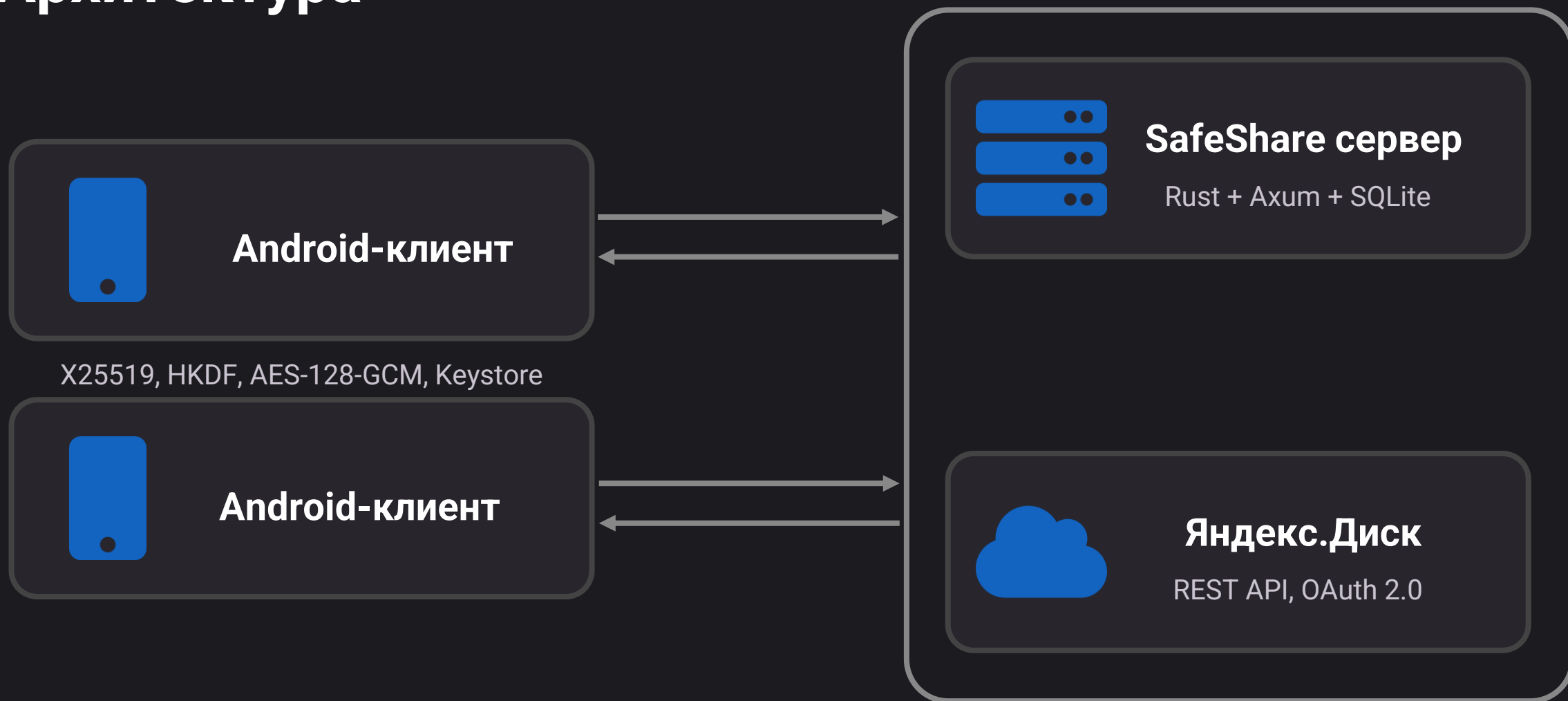
Шифрование и расшифровка – только на устройствах. Сервер никогда не видит содержимое.

# Сравнение с аналогами

| Продукт      | E2E-шифрование | Android-приложение | Self-host | Контакты |
|--------------|----------------|--------------------|-----------|----------|
| SafeShare    | ✓              | ✓                  | ✓         | ✓        |
| Firefox Send | ✓              | ✗                  | ✓         | ✗        |
| Wormhole     | ✓              | ✗                  | ✗         | ✗        |
| LocalSend    | ✓              | ✓                  | ✗         | ✗        |
| PairDrop     | ✓              | ✗                  | ✓         | ✗        |

Единственное open-source решение с нативным Android-клиентом, E2EE и подключаемыми хранилищами

# Архитектура



# Технические особенности



## Аппаратная защита ключей

Хранение в Android Keystore

Приватный ключ невозможно экспортировать



## Потоковое шифрование

AES-128-GCM блоками по 1 МБ

Без временных файлов



## Zero-knowledge сервер

Серверу недоступны:  
содержимое, ключи, имена файлов



## Pluggable storage

Простое добавление новых хранилищ

# Планы

1

## Подпись отправителя

Аутентификация через цифровую подпись на identity key

2

## Новые хранилища

Google Drive, Amazon S3, NextCloud

3

## Множественная отправка

Отправка файла сразу нескольким пользователям по одному коду

# SafeShare

Ваши файлы – только ваши

 [github.com/mihailnagr063/safeshare](https://github.com/mihailnagr063/safeshare)



Спасибо за внимание!