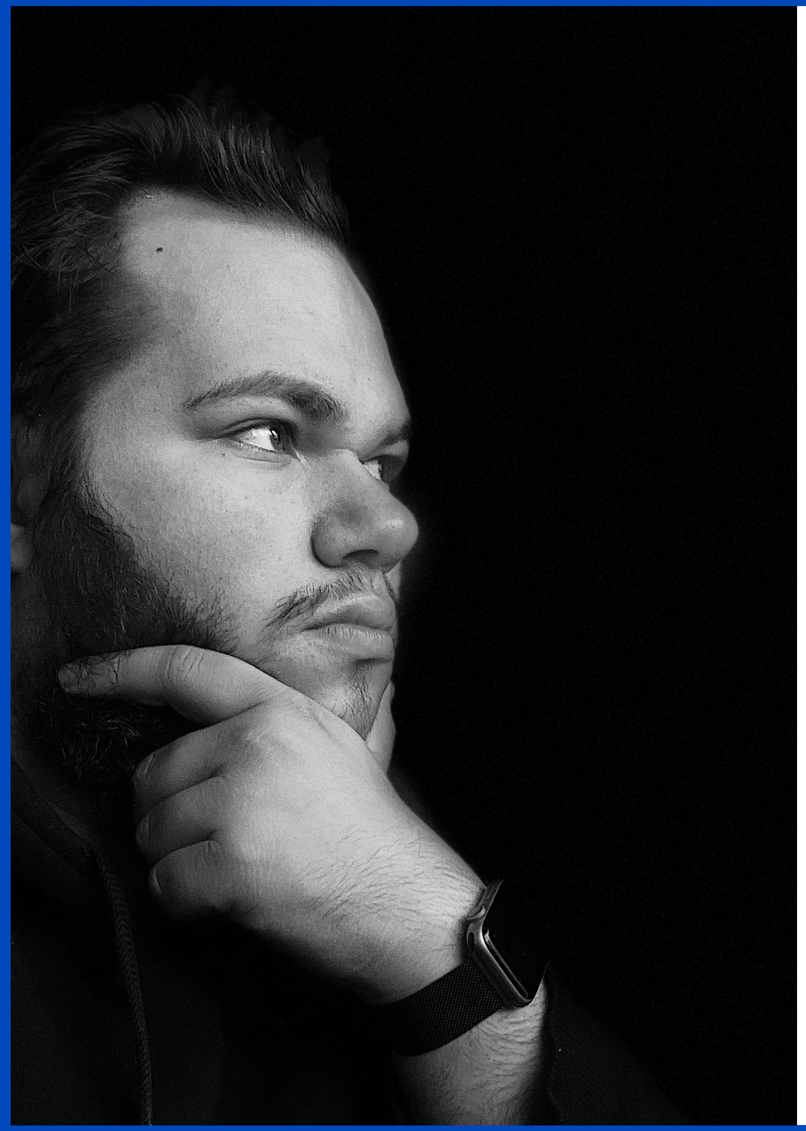
аспирити

best practices **локальной аутентификации** на Flutter

Павел
Гершевич

Head of Mobile Dev
Flutter Tech Lead

аспирити



- 10 лет в мобильной разработке
- На Flutter с 2018
- 20+ проектов

аспирити

№1
в проектировании и разработке корпоративных решений

Учим студентов в самом крупном ВУЗе в Сибири

Работаем с клиентами из 10 стран

О чем поговорим

Для чего и как внедрять локальную аутентификацию

Посмотрим особенности для Flutter и React Native

Посмотрим на алгоритм локальной аутентификации

01

уязвимости, от которых поможет

Несанкционированный доступ к данным

- Подделка аутентификации устройства (подмена биометрии
- Обход аутентификации устройства
- Права superuser

Получение данных из KeyChain / KeyStore зная или обойдя их защиту

Неправильное использование хранилища

- Неавторизованный доступ через биометрию
- Неправильное использование KeyChain, что может привести к сохранению в незащищенное хранилище

Попадание в приложение или использование “защищенных” данных

Одно из решений защиты - локальная аутентификация

Какие данные мы можем использовать для ЛА?

- PIN-код из 4, 5 и более цифр
- Пароль
- Биометрические данные

02

правила, которые мы вывели

Правило №1
Не использовать биометрию без fallback

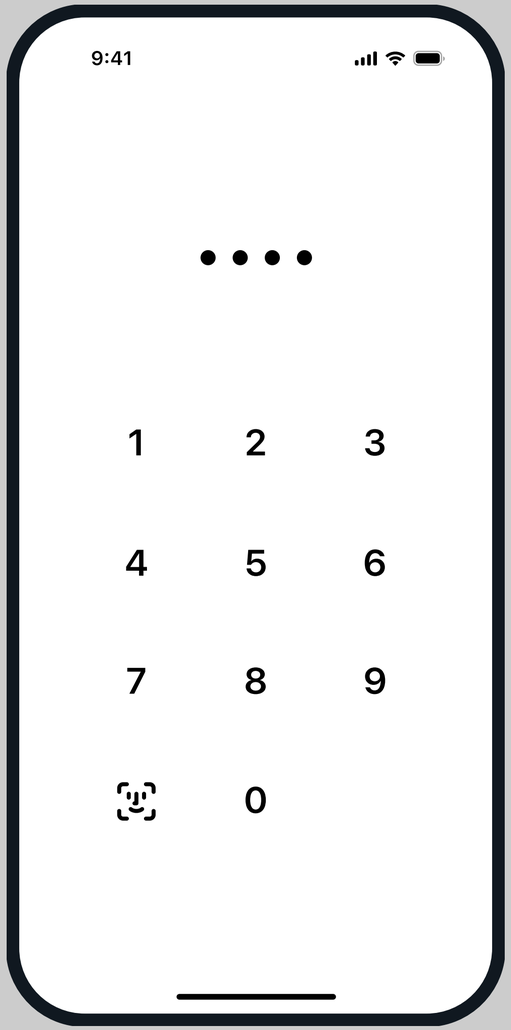
- Множество неверных вводов
- Может не сработать у пользователя
- Может физически сломаться сенсор

Правило №2 Использовать PIN, а не пароль

- PIN короче и его проще запомнить
- В идеальном мире, пароль обрабатывается на сервере
- Работу с PIN в некоторых случаях проще прописать

Правило №2
Использовать PIN, а не пароль

PIN проще подобрать,
так как для 4 цифр всего
10000 вариантов



Использовать кнопки, а не клавиатуру

- Своеобразная защита от брутфорса
- Проще реализовать

Правило №4
Никто не должен знать PIN

- Злоумышленник узнает PIN только через человеческий фактор
- Труднее взломать приложение

Правило №5 Храним только шифрованный refresh token

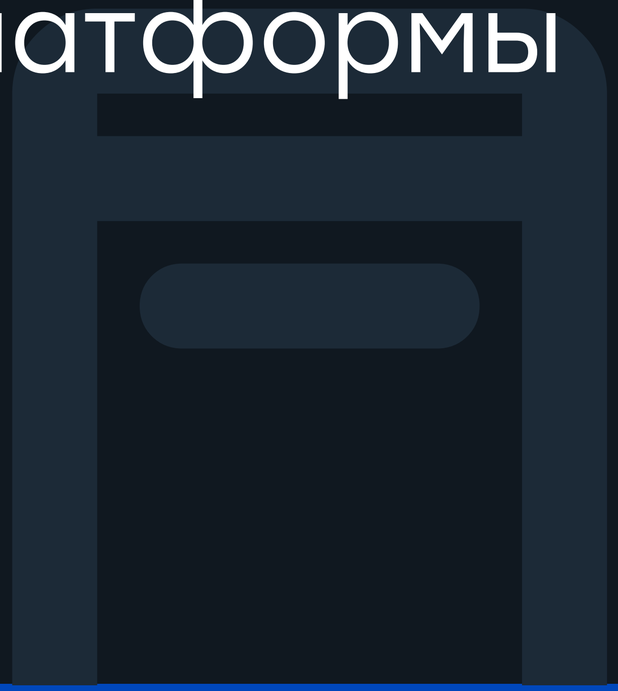
- Шифруем PIN-кодом
- Двойной токен - дополнительная защита
- KeyStore и KeyChain не на столько надежны, как кажутся

аспирити

03 что по кросс-платформе

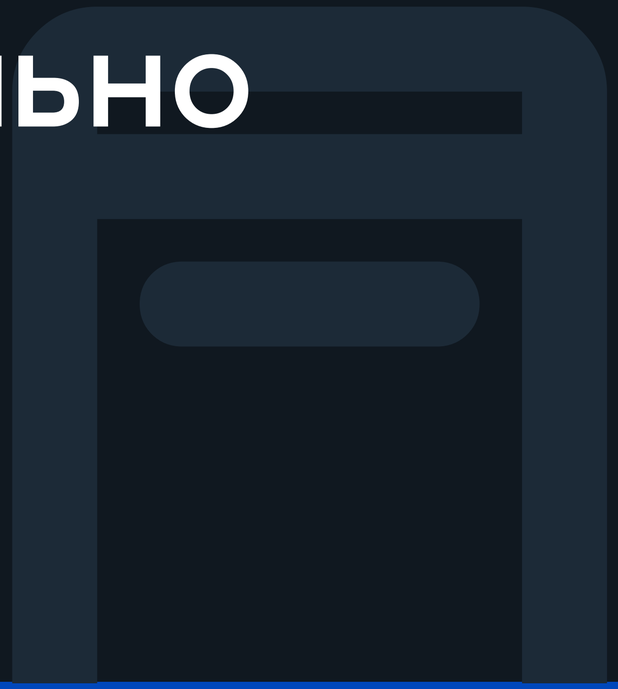
Преимущество кросс-платформы

Реверс-инжиниринг



Проблема кросс-платформы

Наличие действительно хороших библиотек для биометрии



Требования к библиотекам для работы с биометрией

Есть функция проверки на разрешение

Есть функция получения типа биометрии (отпечаток пальца / лицо)

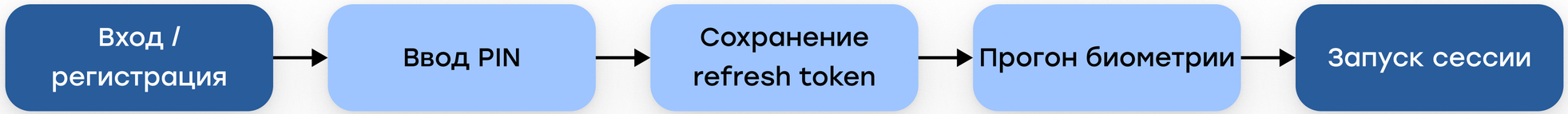
Умеет сохранять данные под биометрию

04

алгоритм локальной аутентификации

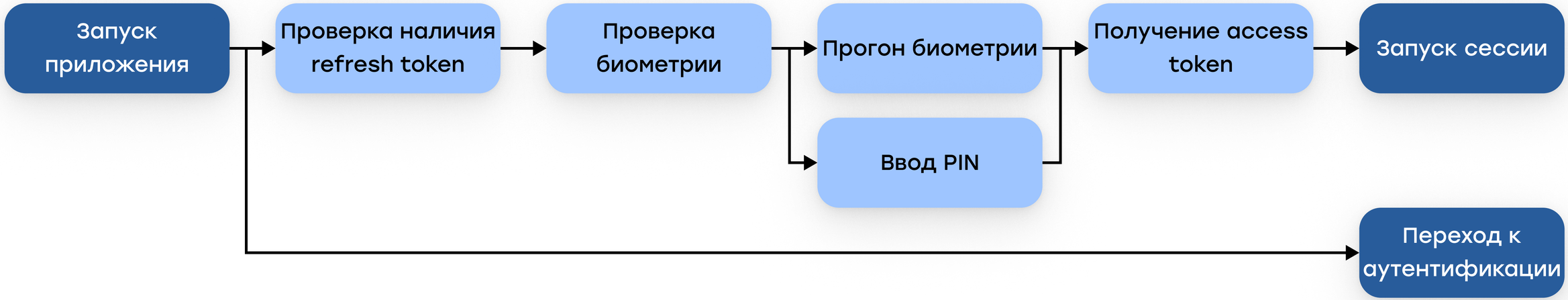
Первичная аутентификация

Первичная аутентификация



Повторная аутентификация

Повторная аутентификация



00

ИТОГИ

Итоги

- Нет “серебряной пули” для простого внедрения локальной аутентификации, особенно под кросс-платформенные приложения
- Приходится учиться на своих ошибках и составлять свои правила

Спасибо за внимание!

Telegram
@ftl_notes

GitHub
github.com/FogNature

аспирити

aspirity.ru