OZON tech

OzonID. Повышаем комфорт пользователей, снижая затраты компании

Долгополов Денис
Android Dev

AGENDA

01 **Пару слов об авторизации**

02 **Виды авторизации**

- Логин + пароль
- OTP
- MobileID
- Внешние сервисы
- Cross-app
- InstantLogin
- Биометрия
- Доверенное устройство
- Мультиаккаунт

03 **Трудности упаковки в SDK**

04 **Зачем нам зоопарк**

ozontech

01

Пару слов об авторизации

Самый общий флоу

Родился

Свидетельство о рождении

Паспорт

Мы сейчас здесь

Купил сим-карту

Авторизовался в Ozon

Цель авторизации

Доверие =
Общие секреты

А что после секрета?

01 Пользователь вводит номер телефона

02 Бэк отправляет SMS-код

03 Юзер вводит код из SMS

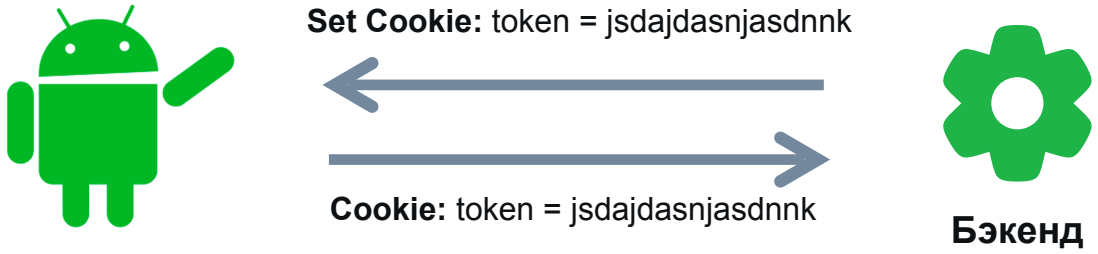
04 Бек проверяет код

05 **Код правильный**

06 Отдаём пользователю **токен**

Токен?

Это уникальная строка, которую знает только пользователь и бэк



token = 12345.8b1CorlJVOLKYbk.010624

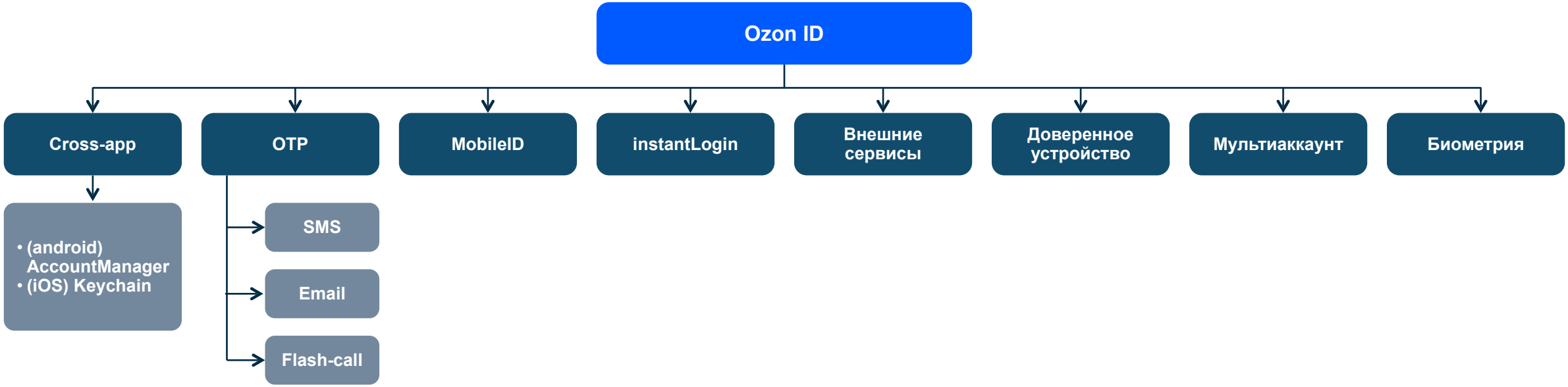
- 12345 — userId
- 8b1CorlJVOLKYbk — JWT-строка
- 010624 — дополнительный параметр


«Секрет»
Токен
Добавляем токен к каждому https-запросу

02

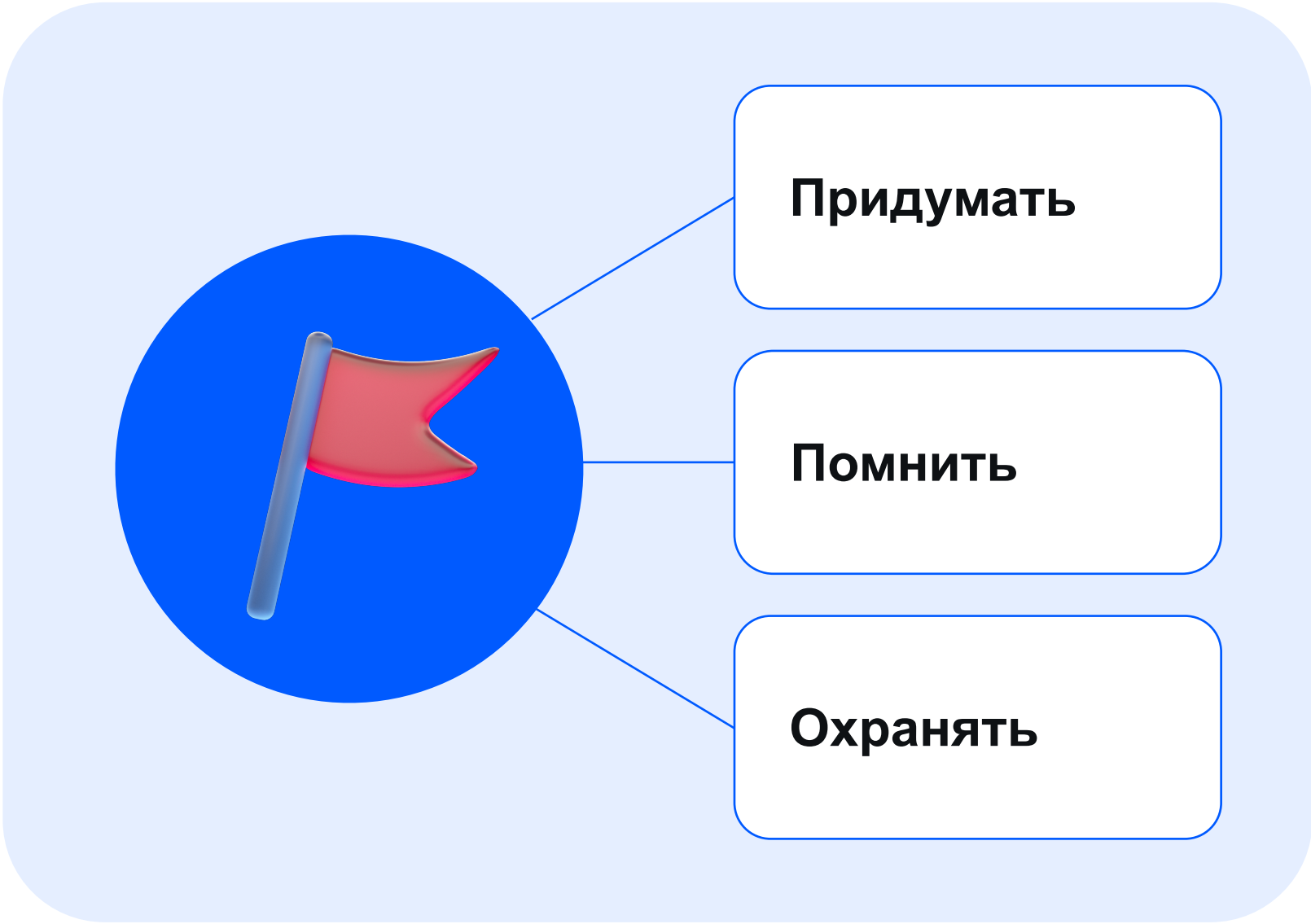
Виды авторизации

Виды авторизации



Логин + Пароль

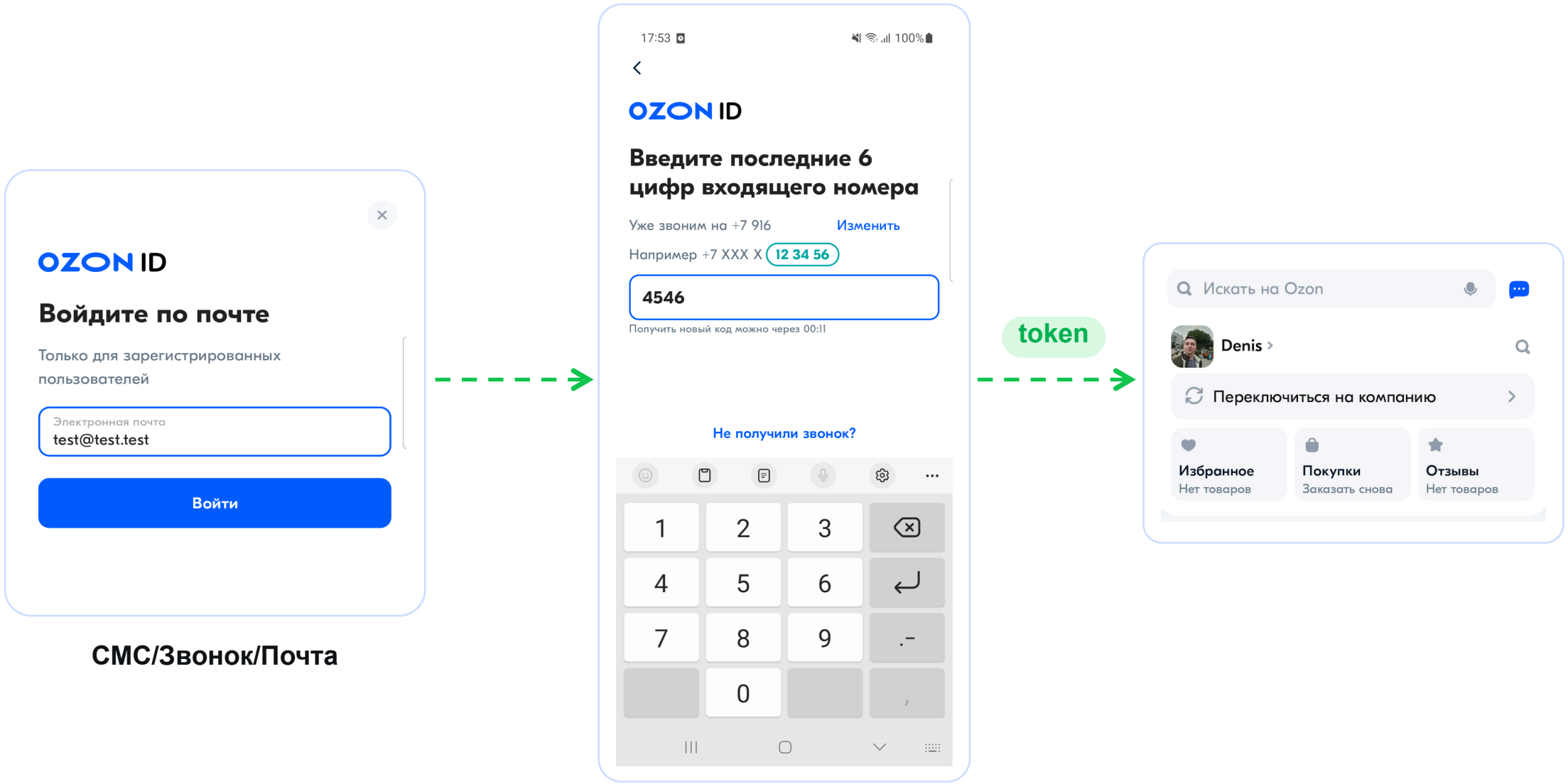
Нужно:



Что есть у всех?

OTP (One-Time Password)

OTP (One-Time Password)



СМС/Звонок/Почта

OTP (One-Time Password)

Несколько уровней защиты

СМС/Звонок

- Почта – менее надёжно

СМС + Почта

СМС + Почта + Пин-код банка

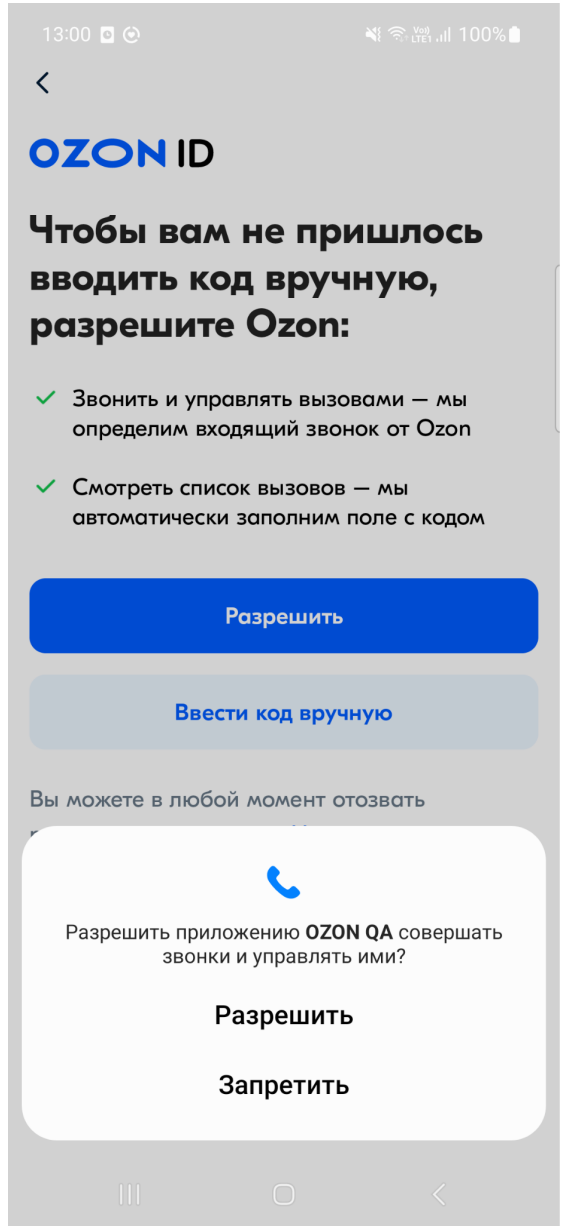
OTP (One-Time Password)

Автоматическое чтение кода

- **В конце СМС добавлен хэш-код**
  - Хэш-код создаётся на основе подписи приложения
- **Временное ограничение – несколько минут**

понедельник, 22 янв. • 09:41

Код: 662478 — для входа на Ozon.
Никому не сообщайте. 7V+3dmscp

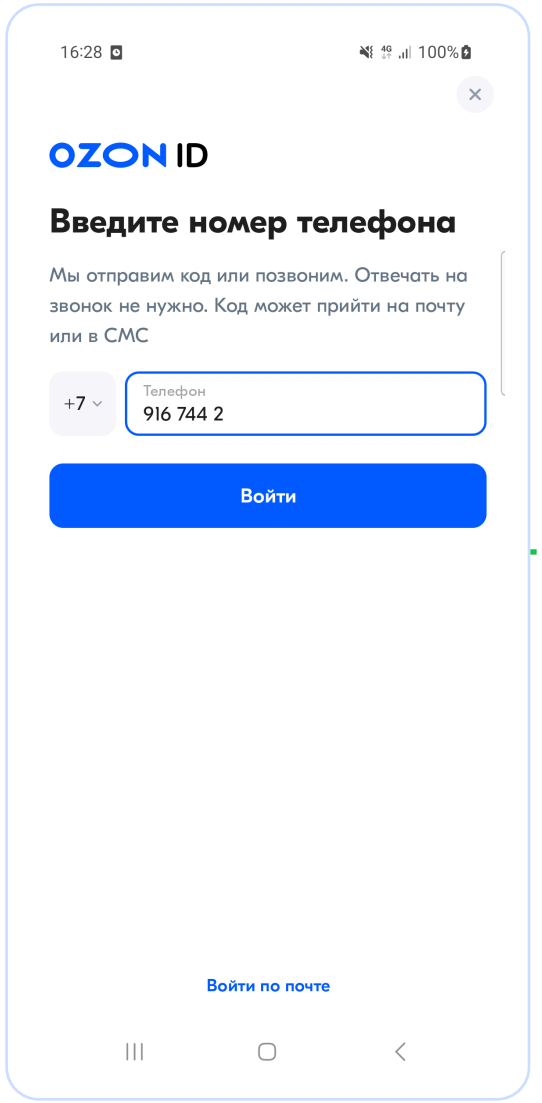


Можем упростить?

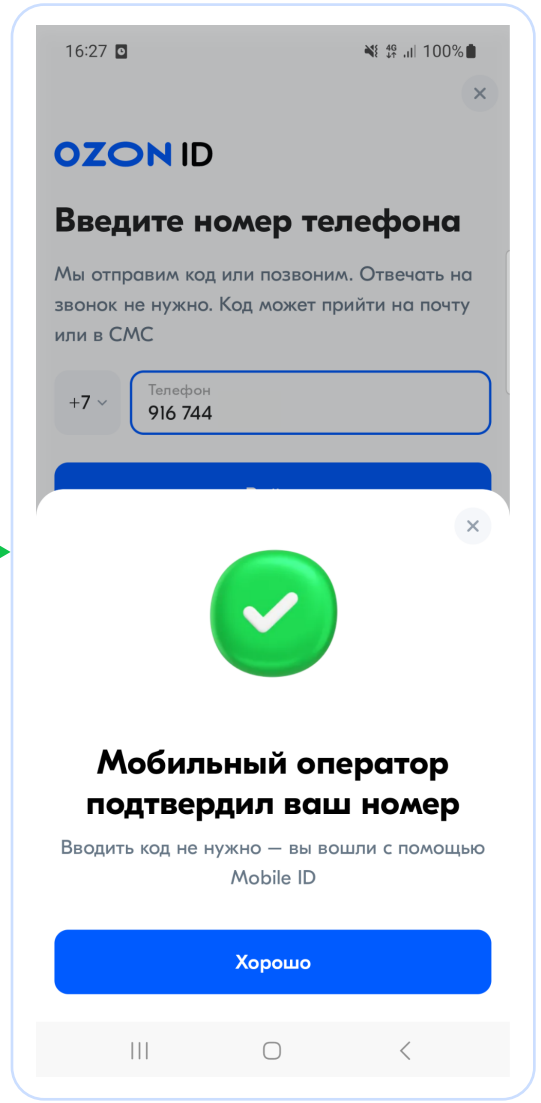
MobileID

MobileID

Ввёл номер телефона



Готово



Подробнее о MobileID

Ввёл номер телефона

- симка вставлена в телефон
- подключен к моб. интернету
- не в роуминге
- подходящий оператор

Запрос к оператору по мобильному интернету

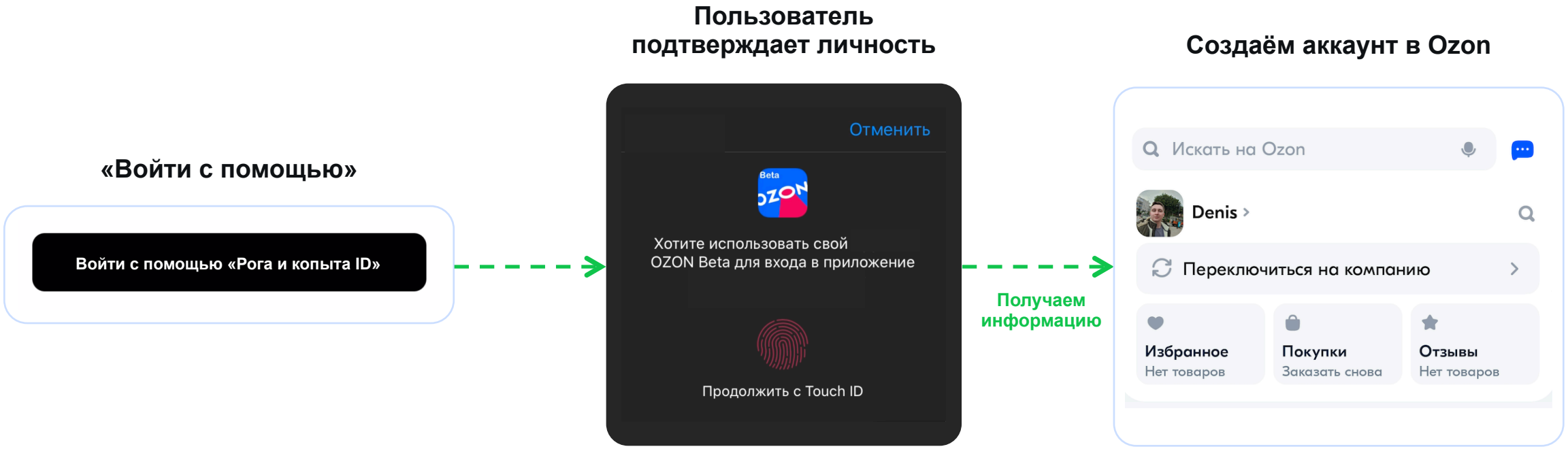
Оператор оповещает Бэкенд Ozon, что всё ок

Бекенд Ozon оповещает приложение, что всё ок

Пользователь доверят кому-то, кроме нас?

Внешние сервисы

Внешние сервисы



Общий принцип

01

Пользователь выбирает сервис, в котором уже авторизован

02

Пользователь видит список, какие данные сервис передаст Ozon

03

Ozon получает токен, по которому может запросить данные о юзере

04

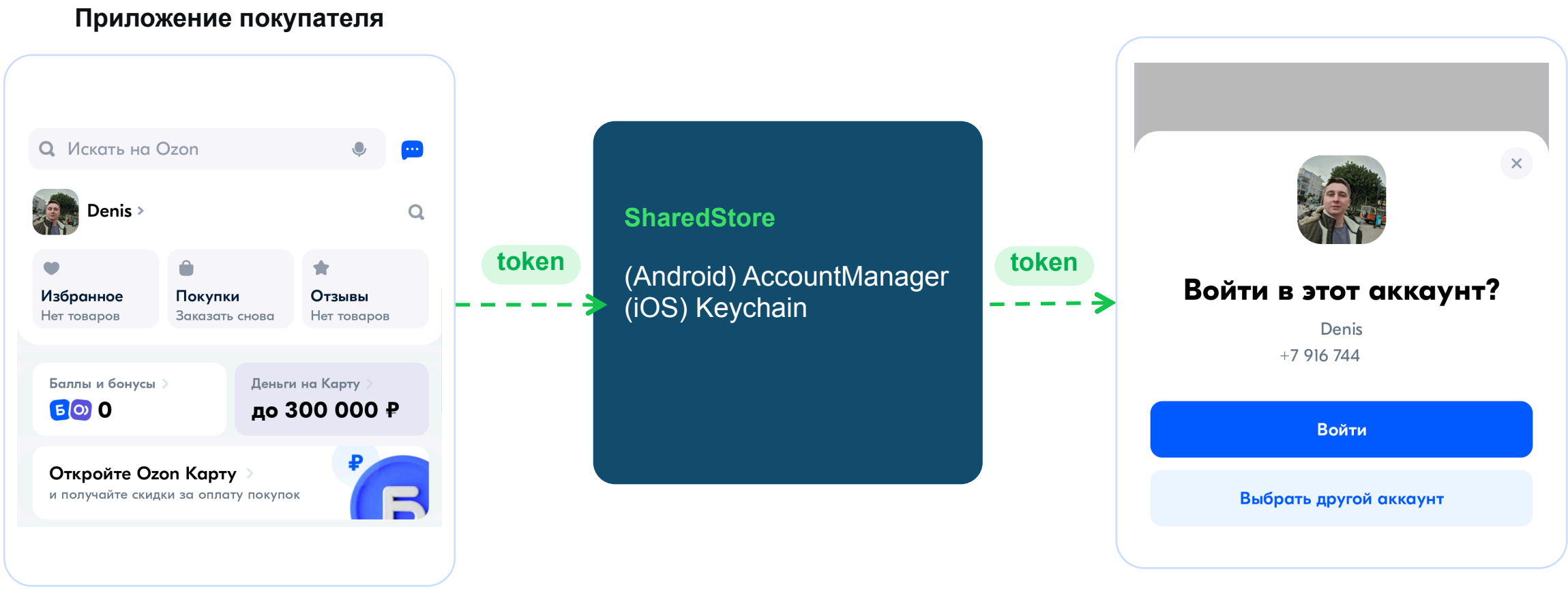
Ozon создаёт юзера по телефону/почте

ozontech

Пользователь любит нашу экосистему?

Cross-app

Cross-app


Приложение покупателя
Искать на Ozon
Denis
Избранное
Нет товаров
Покупки
Заказать снова
Отзывы
Нет товаров
Баллы и бонусы
0
Деньги на Карту
до 300 000 ₽
Откройте Ozon Карту
и получайте скидки за оплату покупок
token
SharedStore
(Android) AccountManager
(iOS) Keychain
token
Войти в этот аккаунт?
Denis
+7 916 744
Войти
Выбрать другой аккаунт

Условия работы Cross-app

Одинаковая подпись

- **(android)** нужно учитывать, что некоторые магазины могут переподписывать apk
- **(ios)** один аккаунт разработчика

Совместимая версия SDK

- Первое приложение **шлёт** токен
- Второе **принимает**

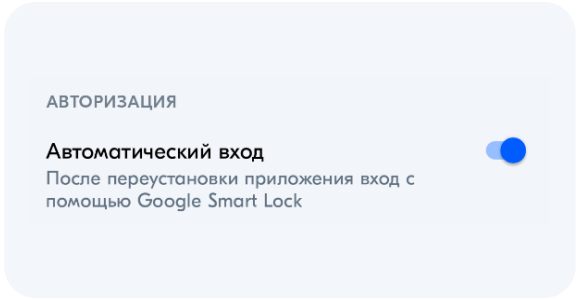
```
// A

val accountManager = AccountManager.get(application)
val newAccount = Account(accountName, ACCOUNT_TYPE)
accountManager.addAccountExplicitly(newAccount)

accountManager.setUserData(account, "token", "sddzx...ccxz")


// B

val token = accountManager.getUserData(account, "token")
api.auth(token)
```

Пользователь собирается **удалить** приложение?

Instant Login

Instant Login

Включили SmartLock



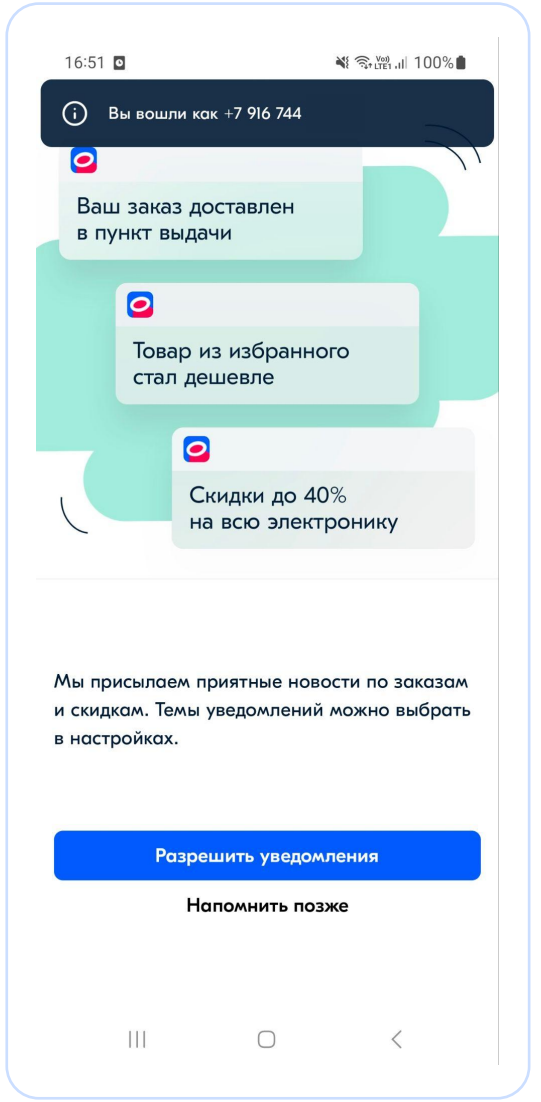
Сохранили секрет в Google Account

Психанул и удалил приложение

Вернулся

Восстановили секрет

Автоматически авторизовали



Instant Login

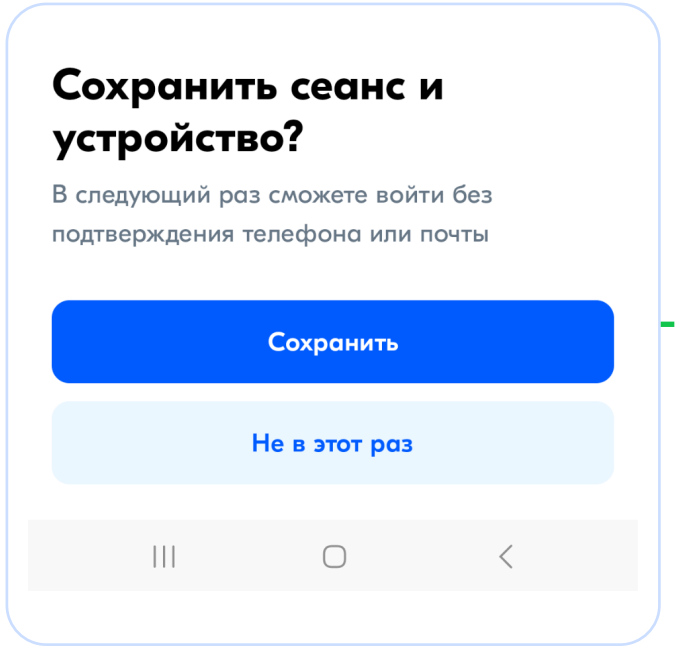
```
val client = Credentials.getClient(application, options)

if (userEnableSmartLock) {
        val token = api.generateUserToken()
        client.saveCredential(token)
}


// Юзер удалил приложение 😡
// …
// Юзер вернулся 😊


val userData = client.request(options)
val token = api.authUser(userData.token)
```

Пользователь вышел, но собирался вернуться?

Доверенное устройство

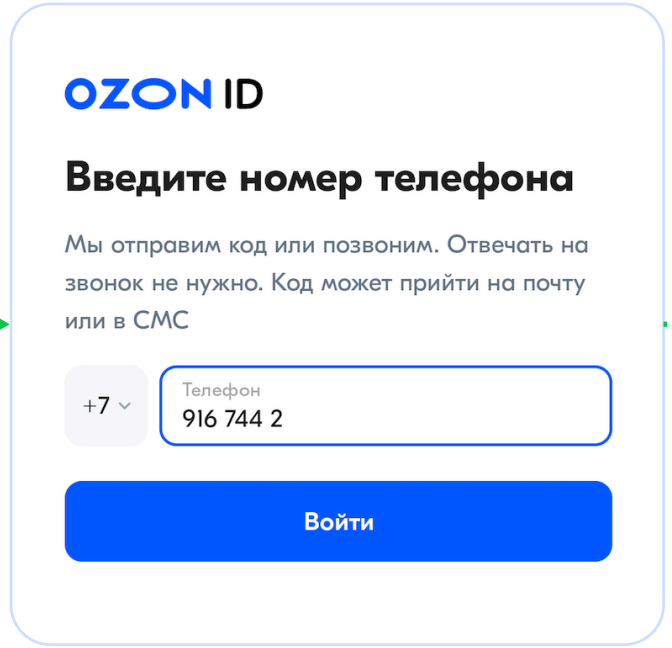
Доверенное устройство

При логауте спрашиваем, запомнить ли сеанс



Запоминаем устройство

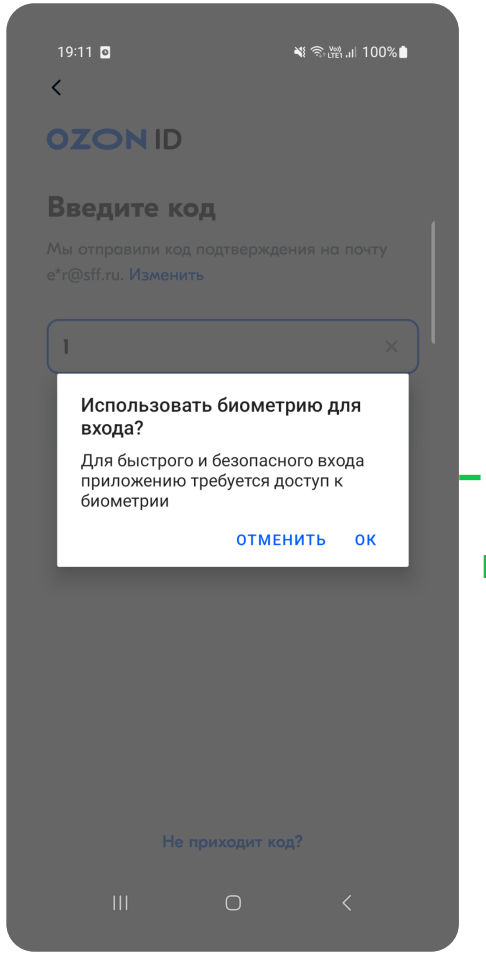
При авторизации бэкенд узнает пользователя по устройству



Биометрия

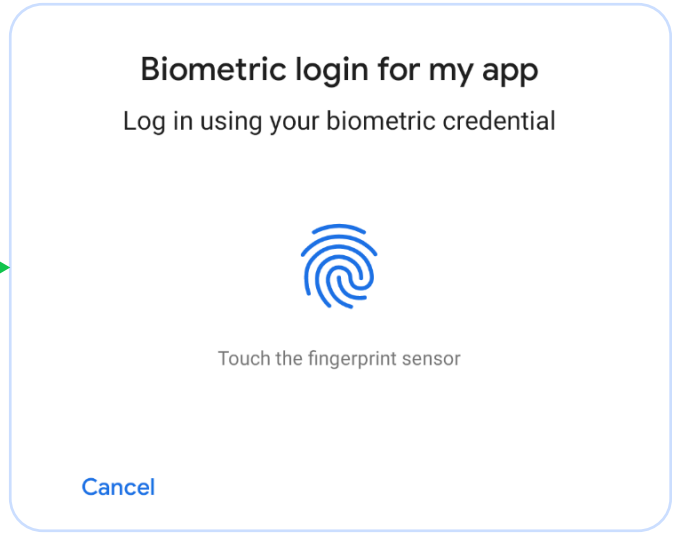
Биометрия

После логина просим включить биометрию



Запоминаем на бэке biometryToken и deviceID

При следующей авторизации предлагаем войти по биометрии

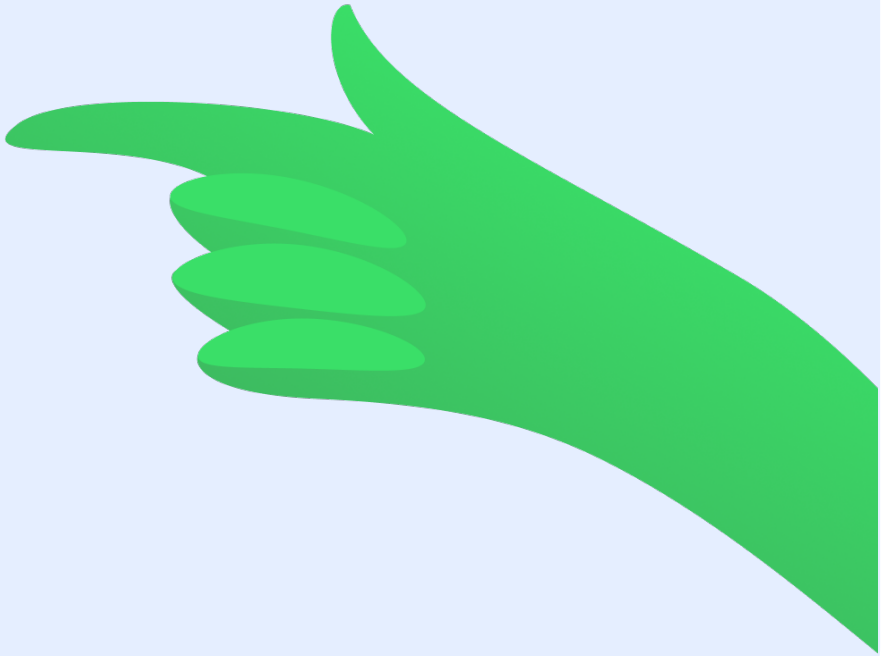


Проверяем biometryToken и deviceID

Интересные факты

Автоматическое чтение кода

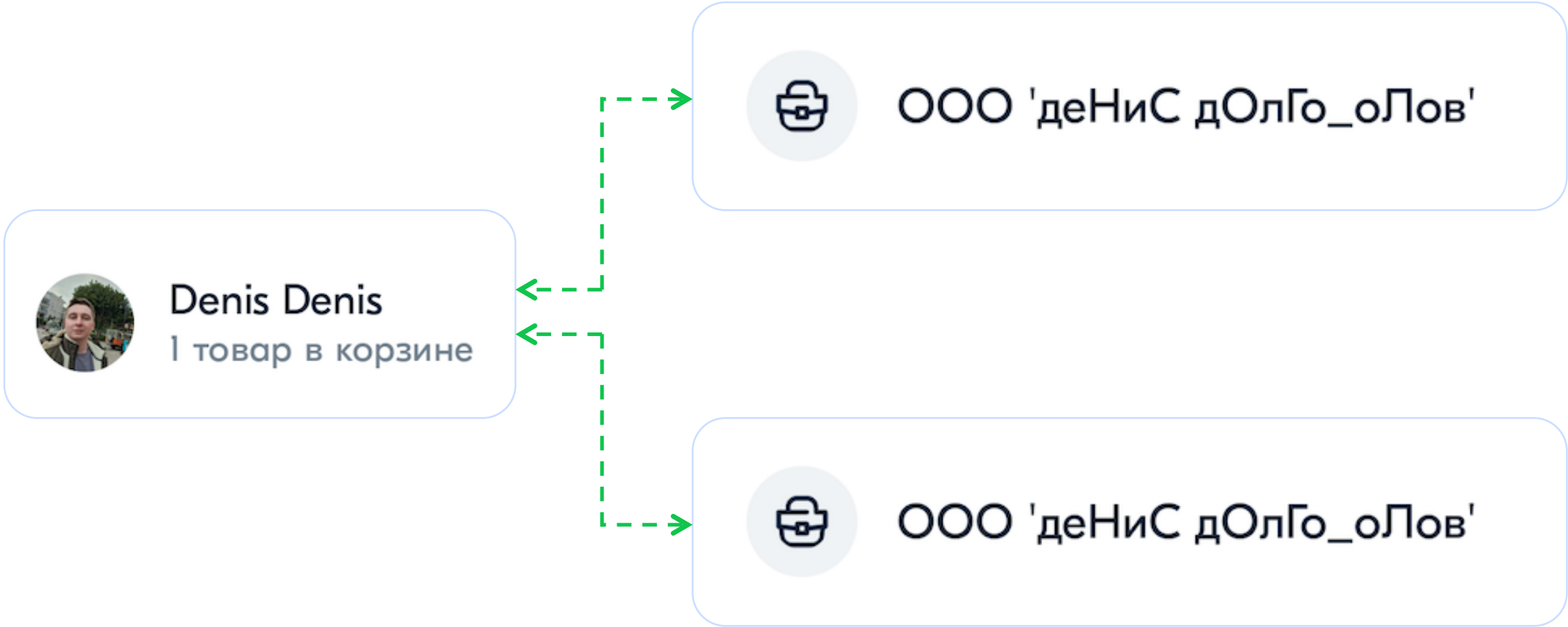
- Пользователь добавит новый отпечаток – нужно заново попросить его включить вход по биометрии
- Разные устройства – разные степени защиты по биометрии
  - Самый надежный – **вход по отпечатку**



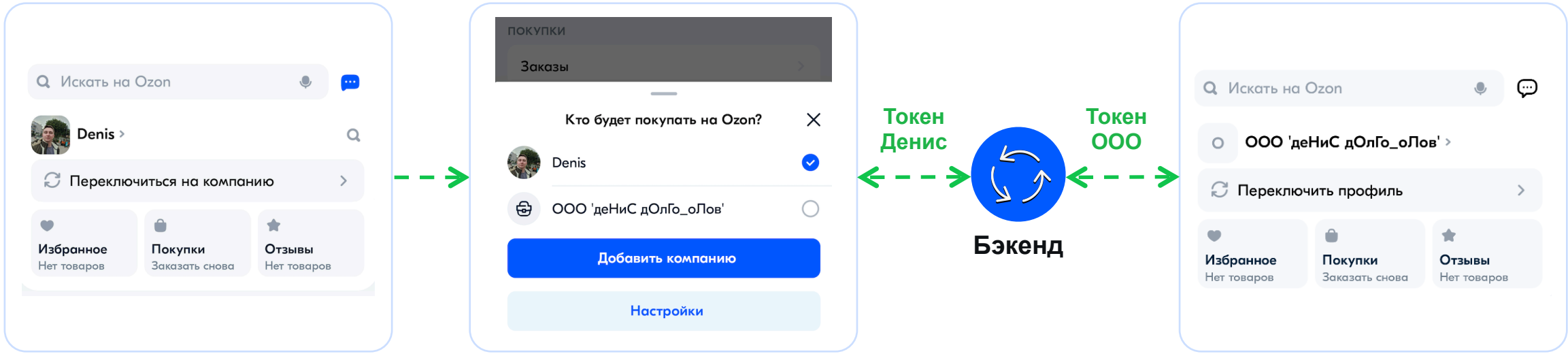
У пользователя есть несколько личностей?

Мультиаккаунт

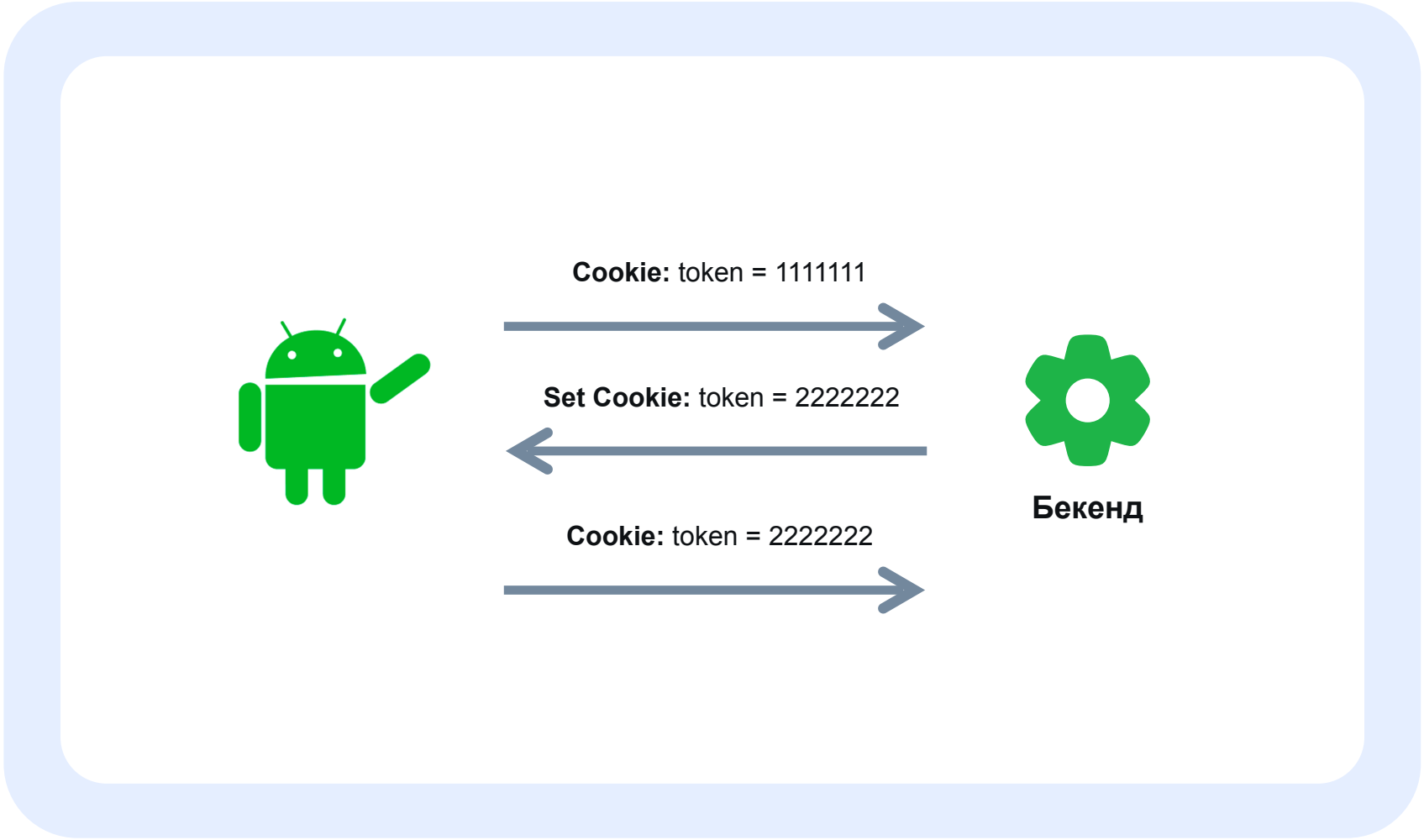
Один человек – несколько юрлиц



Один человек – несколько юрлиц



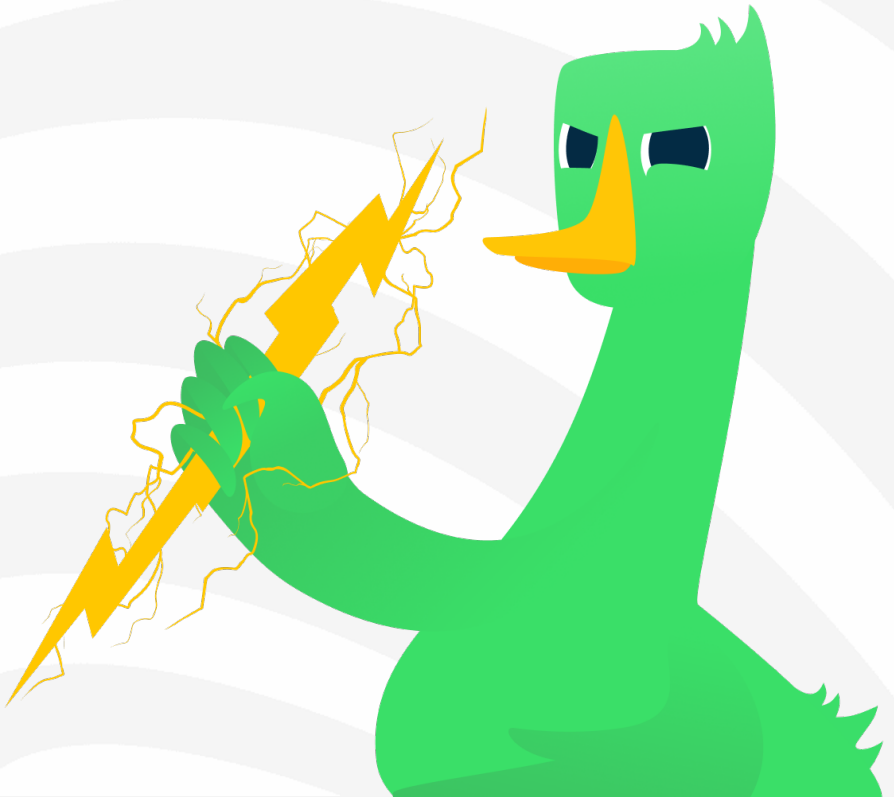
Один человек – несколько юр. лиц



03

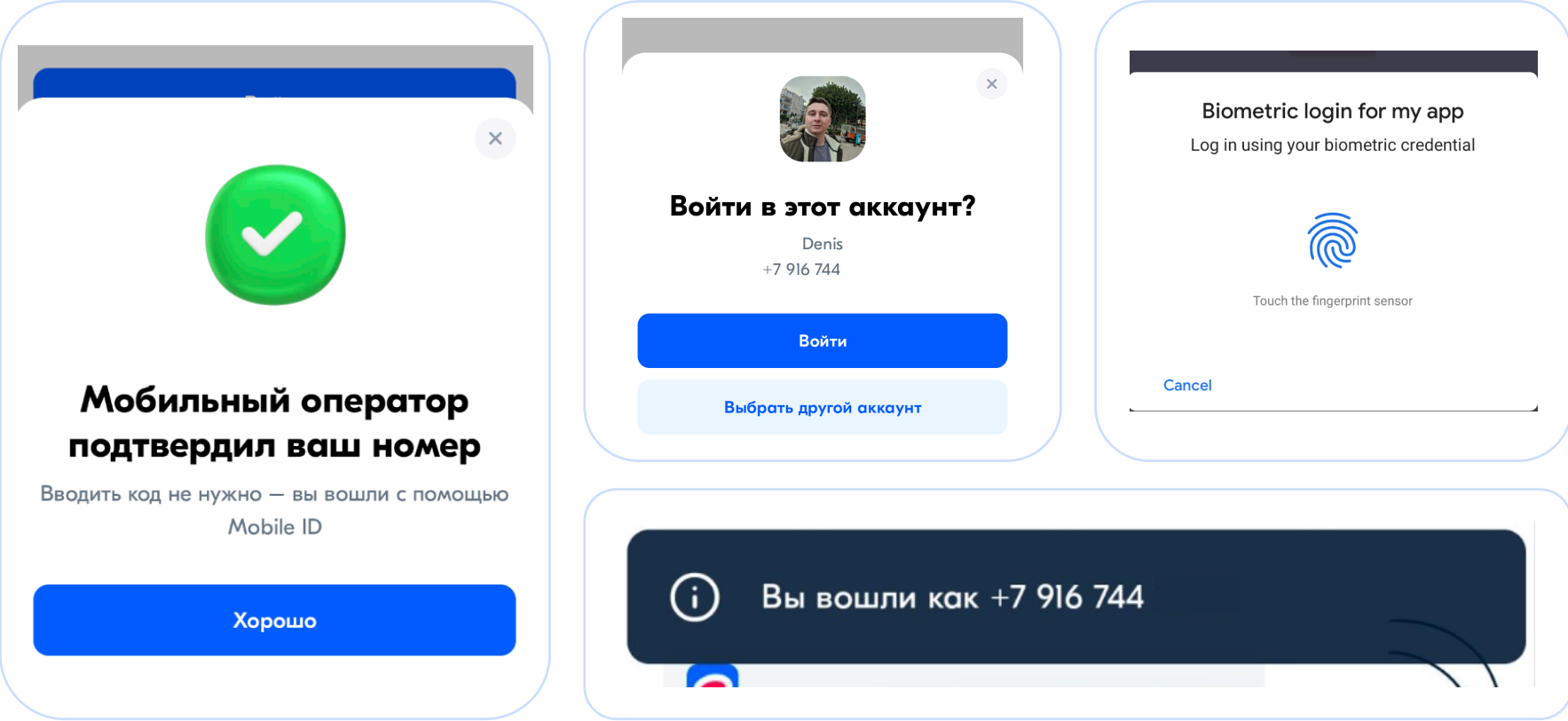
Трудности упаковки в SDK

Поставляем auth в 10 приложений



Трудность #1 😡

Шторки нужно разруливать между собой



Трудность #2 😡

Не все можно упаковать в SDK

- **(android)** приложение игнорирует network-security-config из sdk
- **(ios)** нельзя поддержать диплинки

sdk-network-security-config
+
app-network-security-config
=
app-network-security-config

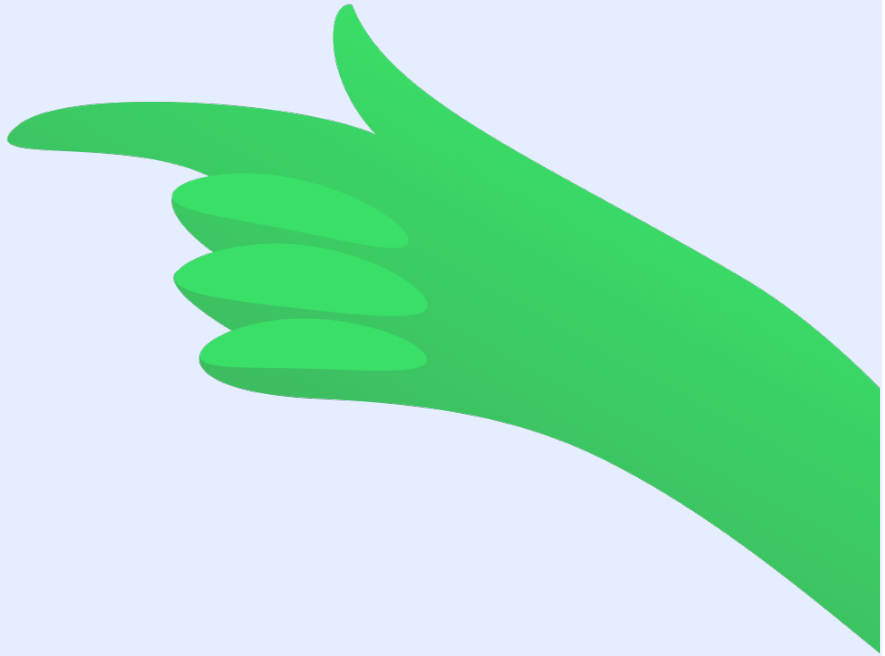
network_security_config.xml

```xml
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="false">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>

    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="false">123.ozon.ru</domain>
    </domain-config>
</network-security-config>
```

Трудность #3 😡

Не все обновляют SDK моментально

- Снизить % breaking changes → автоматически интегрировать с помощью CI
- отправлять sdk_version и включать фичи с min_sdk_version



Трудность #4 😡

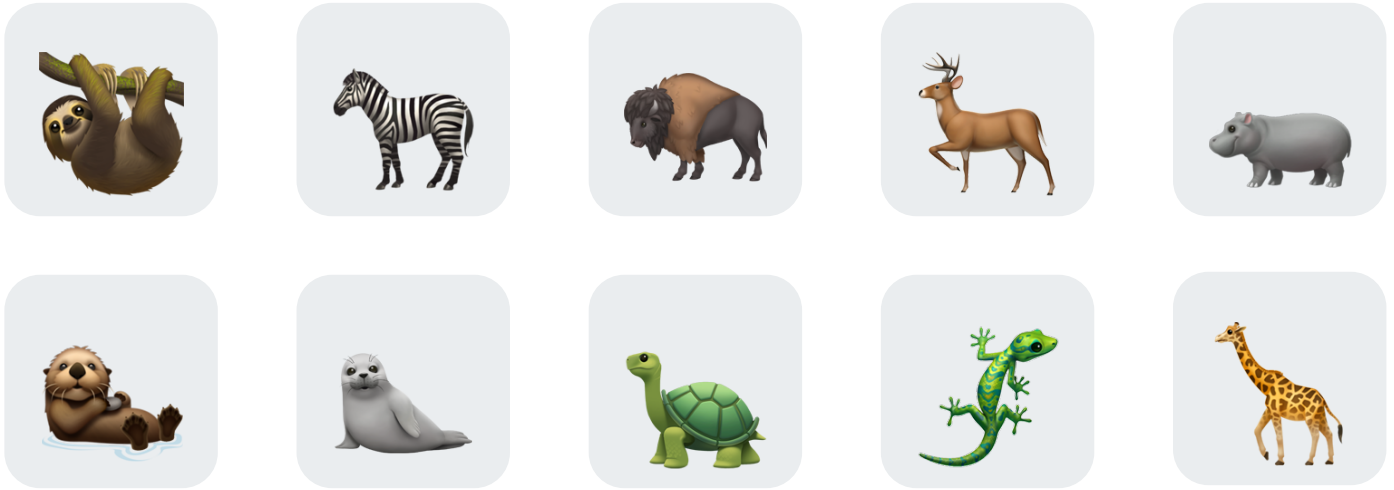
Поддержать разлогины

- Цель — **удалить токены**

Методы

- **UI**
- **Local Logout**
- **http.response.code = 401**
- **ForceLogout без UI**

А ради чего?



МИНУСЫ

Нужен штат

- dev /QA / ИБ / мониторинг

Нужно платить зарплату

ПЛЮСЫ

- Резервируемся
- Упрощаем флоу
- Повышаем конверсию
- Делаем единый SDK
- Экономим деньги 💰

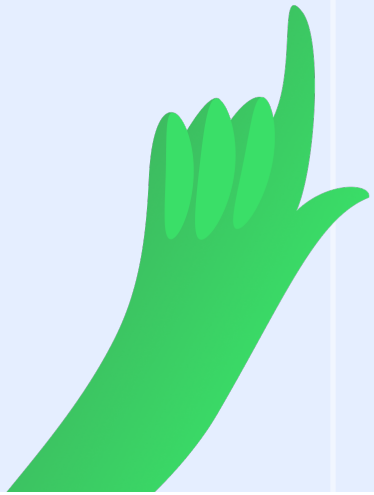
Приоритеты

Дорогие

- **SMS**

Недорогие

- **flash-call (звонки)**
- **MobileID (без ввода One-Time Password)**



Почти бесплатные

- **e-mail**

Бесплатные

- **Cross-app** (между приложениями)
- **InstantLogin** (после удаления приложения)
- **Доверенное устройство** (повторный вход)
- **Сторонние сервисы** (AppleID, Госуслуги…)
- **Мультиаккаунт (**переключение между юр. и физ. лицом)
- **Биометрия** (отпечатки пальцев)

OZON tech

Спасибо за внимание!
Вопросы?

Долгополов Денис
Android Dev
tg: @dolgopolovdenis
tg-канал: @dolgo_polo_dev
Habr: @DolgopolovDenis