Digital

Правильный вход

построение систем аутентификации в современных реалиях

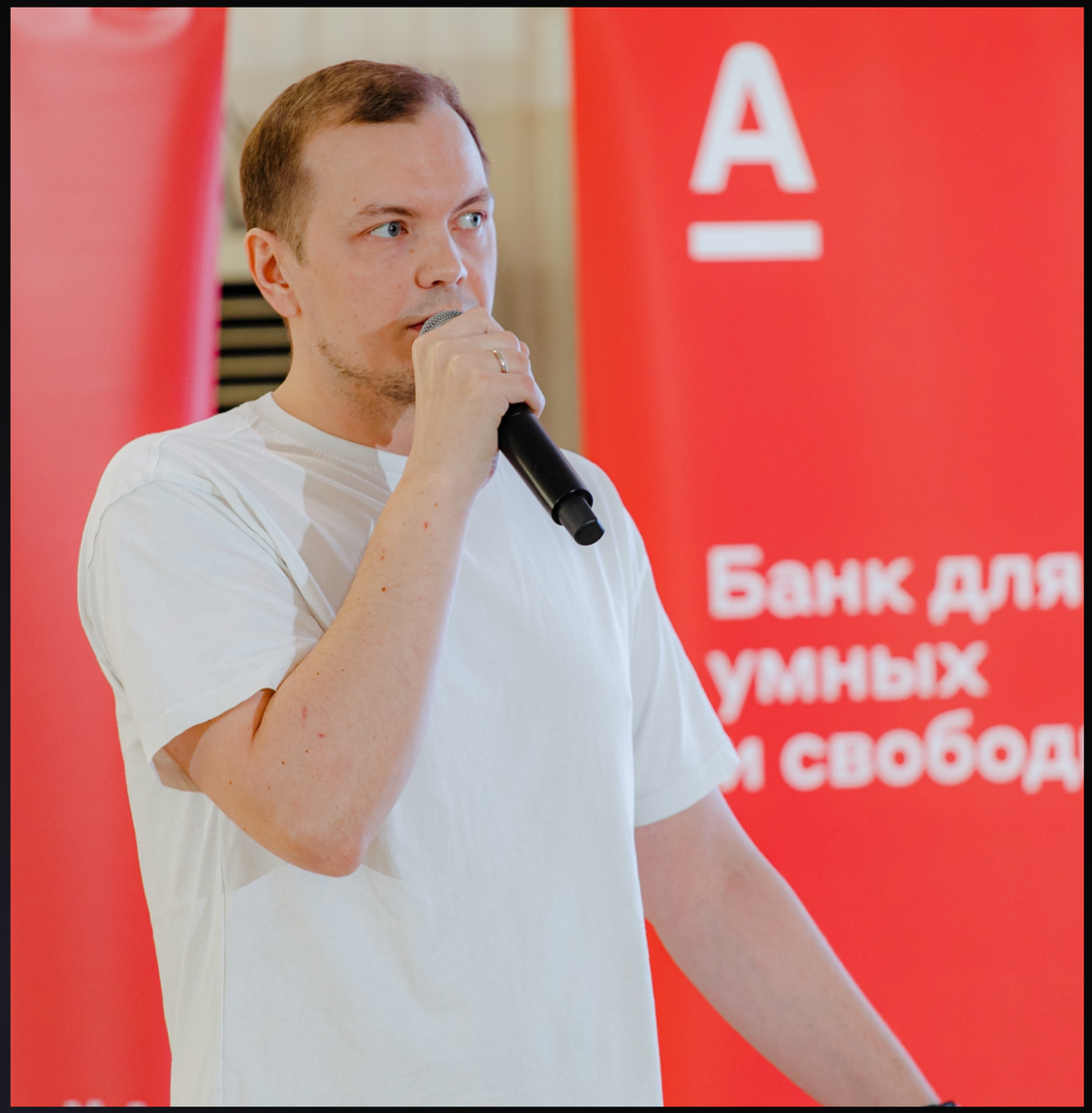
Дмитрий Корнеев / 27 июля 2023

A Digital

Дмитрий Корнеев

Senior Product Owner, Альфа-Банк

- Более 10 лет в IT-разработке
- 5 лет в построении систем аутентификации и передачи данных
- СберБизнес ID
- Alfa ID



A Digital

О чём разговор?

- Что такое «ВХОД»?
- Обзор основных решений
- Основные сложности реальной практики
- Роль государства
- Best-practice оптимальных решений
- Текущие функциональные возможности
- Перспективы развития

A Digital

Что такое «ВХОД»

- Идентификация. **Я – Вася**
- Аутентификация. **То, что знает или есть только у Васи**
- Авторизация. **Вася может следующее:...**
- Верификация. **Вася доказал то, что он – Вася**
- Single Sign-On. **Я – Вася везде, и все это знают**

A Digital

Что такое единый ID?

Единая учётная запись пользователя,
используемая для регистрации и входа
в продукты и сервисы компании и партнёров

Продукт, упрощающий жизнь клиента
в цифровой среде

Возможность вывести продукты за контур компании

A Digital

Зачем нужен единый ID?

- ✓ Бесшовная аутентификация пользователей в различных сервисах
- ✓ Унификация пользовательского опыта
- ✓ Сбор юридически значимых согласий пользователей
- ✓ Сбор данных о пользователях
- ✓ Передача партнёрам информации о пользователях
- ✓ Продуктовый энейблер
- ✓ Бординг не-клиентов и апсейл продуктов
- ✓ Экономия от разработки и поддержки единого сервиса для разных потребителей

A Digital

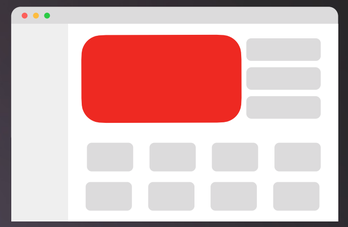
Сценарий

Первый вход в сервис

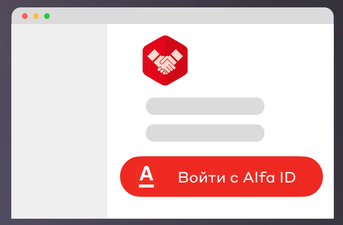
Клиенты банка

Не-клиенты банка

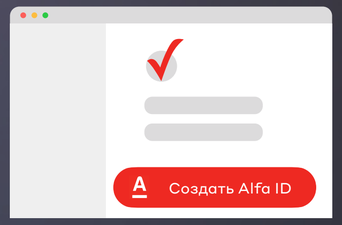
Переход из банка



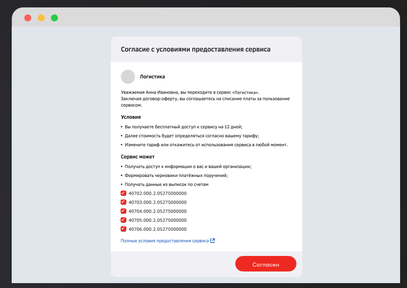
Переход с:
- сайта сервиса
- ЛК ID



Регистрация ID



Страница Согласия



Получение партнёром данных о пользователе

Бесшовный вход в сервис

A Digital

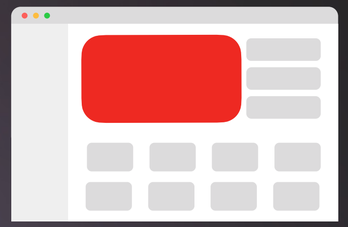
Сценарий

Активный пользователь

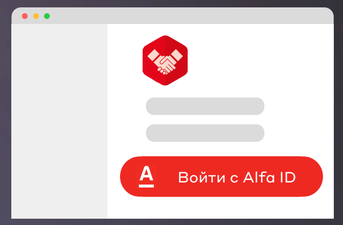
Клиенты банка

Не-клиенты банка

Переход из банка



Переход с:
- сайта сервиса
- ЛК ID



Бесшовный вход в сервис

A Digital

Обзор основных решений

A Digital

Обзор основных решений

Банковская авторизация

Логин/пароль

2-факторная аутентификация

Вход по номеру карты

УКЭП

Защищенный канал обмена данными

1st-gen ID

oAuth 2.0 + OIDC

KYC как актив

Легитимные согласия на передачу ПДн

Передача расширенных данных профиля

Аутентификация по номеру телефона

2nd-gen ID

Кросс-девайсная аутентификация (QR)

Биометрия

Работа с не-клиентами

Кастоимизация и вариативность способов и факторов аутентификации для разных сценариев

Управление пользователями настройками своей аутентификации

next-gen ID

PassKeys

Аутентификация по web3-токену

Готовые SDK для интеграций с партнёрами

Безопасная аутентифкация без участия пользователя (фоновая)

Мы примерно тут

A Digital

Обзор основных решений

		A			ВТБ	Я	G		
Банковская авторизация	Логин/пароль	✅	✅	✅	✅	✅	✅	✅	✅
	2-факторная аутентификация	✅	✅	✅	✅	✅	✅	✅	✅
	Вход по номеру карты	✅	⛔	✅	✅	⛔	⛔	⛔	⛔
	УКЭП	✅	⛔	✅	✅	⛔	⛔	⛔	⛔
1st-gen ID	oAuth 2.0 + OIDC	✅	✅	✅	✅	✅	✅	✅	✅
	Профиль клиента (включая KYC)	✅	✅	✅	⛔	✅	✅	✅	✅
	Расширенный профиль	✅	✅	✅	⛔	✅	✅	✅	✅
	Аутентификация по номеру телефона	✅	✅	✅	✅	✅	✅	✅	✅
2nd-gen ID	QR-аутентификация	✅	⛔	✅	✅	✅	✅	✅	⛔
	Биометрия (браузер)	✅	⛔	⛔	✅	⛔	✅	✅	✅
	Работа с не-клиентами	⛔	⛔	✅	✅	✅	✅	✅	✅
	Единая УЗ ЮЛ/ФЛ	⛔	✅	⛔	⛔	✅	✅	✅	✅
next-gen ID	Дополнительные беспарольные способы аутентификации	✅	⛔	✅	✅	✅	✅	✅	✅
	Web3 ID	⛔	⛔	⛔	⛔	⛔	✅	✅	⛔

A Digital

Основные сложности реальной практики

- ✓ Высокая стоимость и сроки доработок смежных ядровых систем
- ✓ «Зоопарк» старых систем аутенитфикации в эксплуатации
- ✓ Проприетарные решения существующего ИТ-ландшафта
- ✓ Взаимоисключающие требования заказчиков
- ✓ Долгосрочное бюджетирование проекта
- ✓ Сложность в понимании самой технологии безопасной аутентификации
- ✓ Низкий уровень актуальности данных о клиентах
- ✓ «Дорогие» риски нарушения регуляторных норм при высокой зарегулированности

A Digital

Роль государства

- ✓ **115-ФЗ** «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»
- ✓ **152-ФЗ** «О персональных данных»
- ✓ **63-ФЗ** «Об электронной подписи»
- ✓ **149-ФЗ** «Об информации, информационных технологиях и о защите информации»
- ✓ **126-ФЗ** «О связи»

➡ **Обязательная регуляторная составляющая постоянно растёт**

➡ **С одной стороны, государство заботится о безопасности граждан в условиях динамически развивающихся цифровых угроз**

➡ **С другой стороны, намечается тенденция к переходу от регулирующей модели к контролирующей**

A Digital

Best-practice оптимальных решений

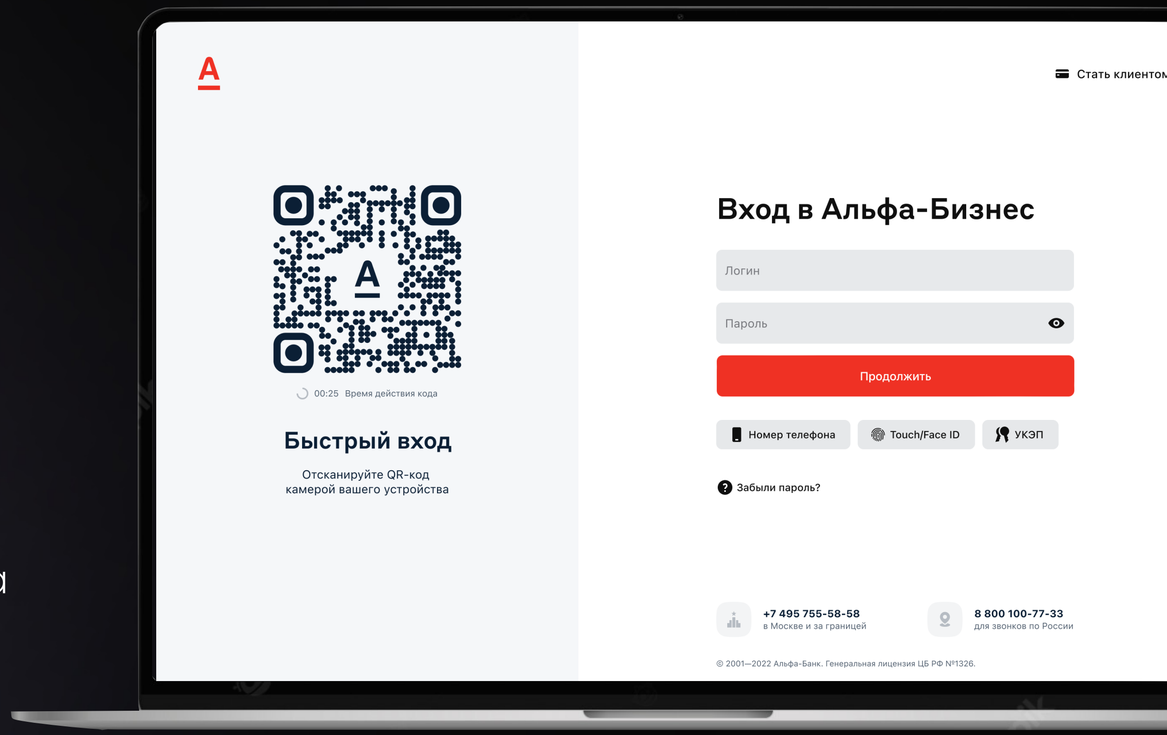
- Микро-сервисная модель + оркестратор
- RESTFUL-архитектура
- Соответствие отраслевому стандарту oAuth 2.0 + OIDC
- Mobile-first
- Максимизация использования биометрии
- Диверсификация способов для подписи согласий (СМС, УКЭП, ГосКлюч)
- Двухсторонний обмен данными между банком и партнёрами
- Поддержка интеграций со сторонними Auth-провайдерами (другими ID)
- Поддержка разных средств защиты информации: SSL, ПАК ФПСУ-IP

A Digital

Текущие функциональные возможности

- ✓ Аутентификация пользователей с помощью:
  - ✓ Логин + пароль
  - ✓ Номер телефона + код из СМС
  - ✓ Номер карты + пароль / код из СМС
  - ✓ QR (на компьютере с помощью МП)
  - ✓ Push-уведомление на другое устройство
  - ✓ Одноразовая ссылка на e-mail
  - ✓ Биометрический слепок пользователя
  - ✓ УКЭП ФНС

- ✓ Настраиваемая многофакторная аутентификация (СМС, код, auth-приложение)
- ✓ Кастомизация сценариев на уровне партнёра и/или клиента
- ✓ Сбор юридически значимых согласий пользователей
- ✓ Передача информации о пользователя
- ✓ Регистрация учётной записи не-клиента
- ✓ Удаленная верификация УЗ с помощью ЕСИА с ЕБС



A Digital

Перспективы развития

- ✓ ЕСИА как обязательная система
- ✓ ID банков и бигтехов в синергии с ЕСИА
- ✓ Рост актуальности информации о пользователях
- ✓ Беспарольная аутентификация
- ✓ Фоновая аутентификация
- ✓ Web3 auth (блокчейн)
- ✓ Новые законы о запрете иностранной почты ⚡

A Digital

СПАСИБО!

Дмитрий Корнеев / 27 июля 2023