Identity Blitz

RISSPA
be professional

Семинар «Безопасная разработка и защита приложений»

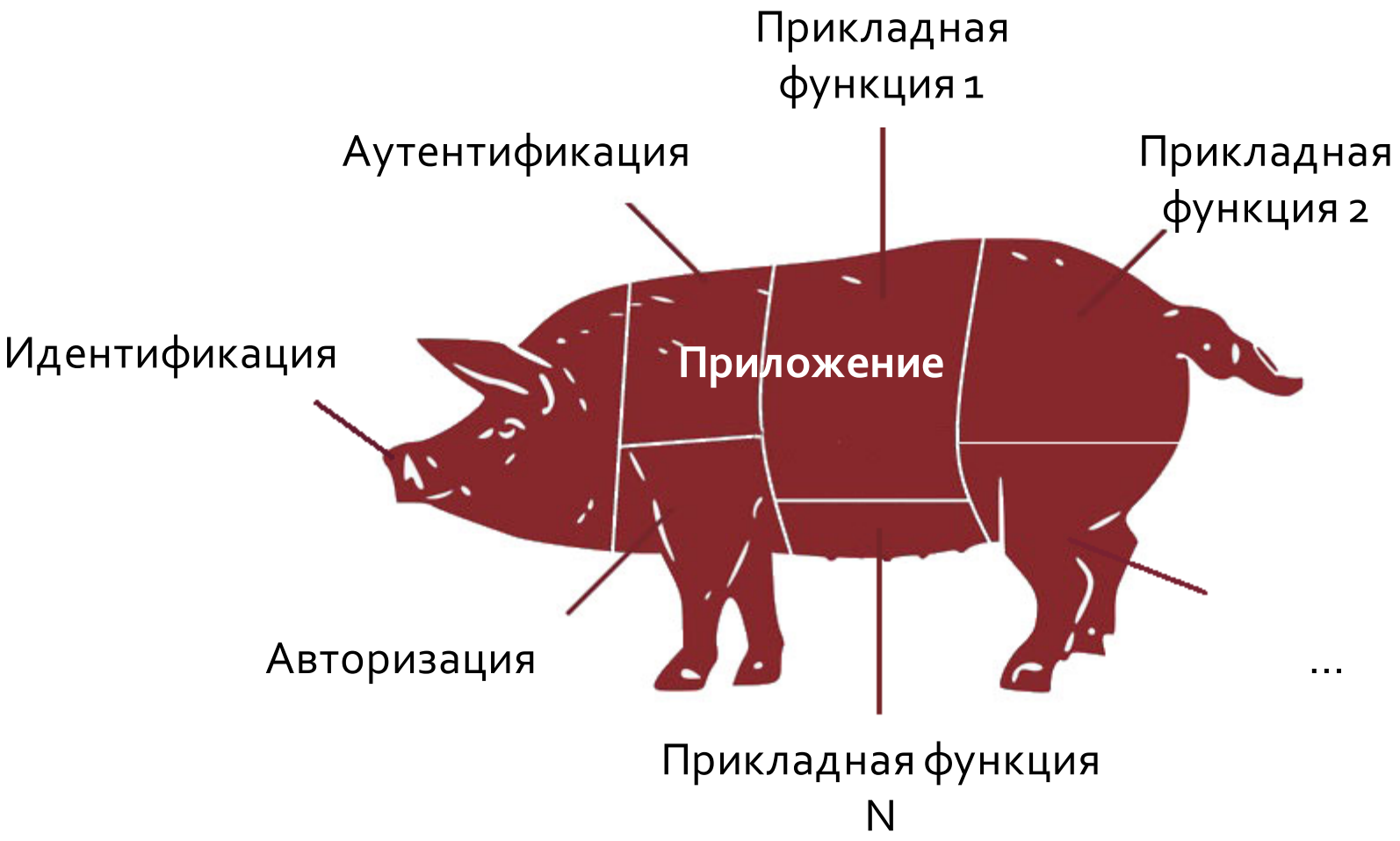
Идентификация, аутентификация, авторизация – встроенные функции приложений или задачи специализированного сервиса организации?

Михаил Ванин, генеральный директор ООО «РЕАК СОФТ»

mvanin@reaxoft.ru

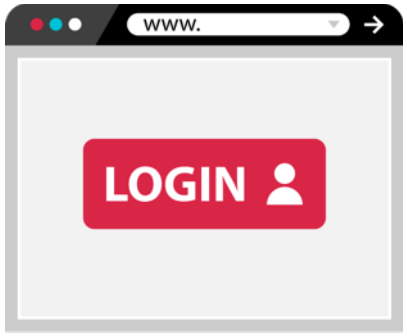
РЕАК СОФТ

Функции приложения



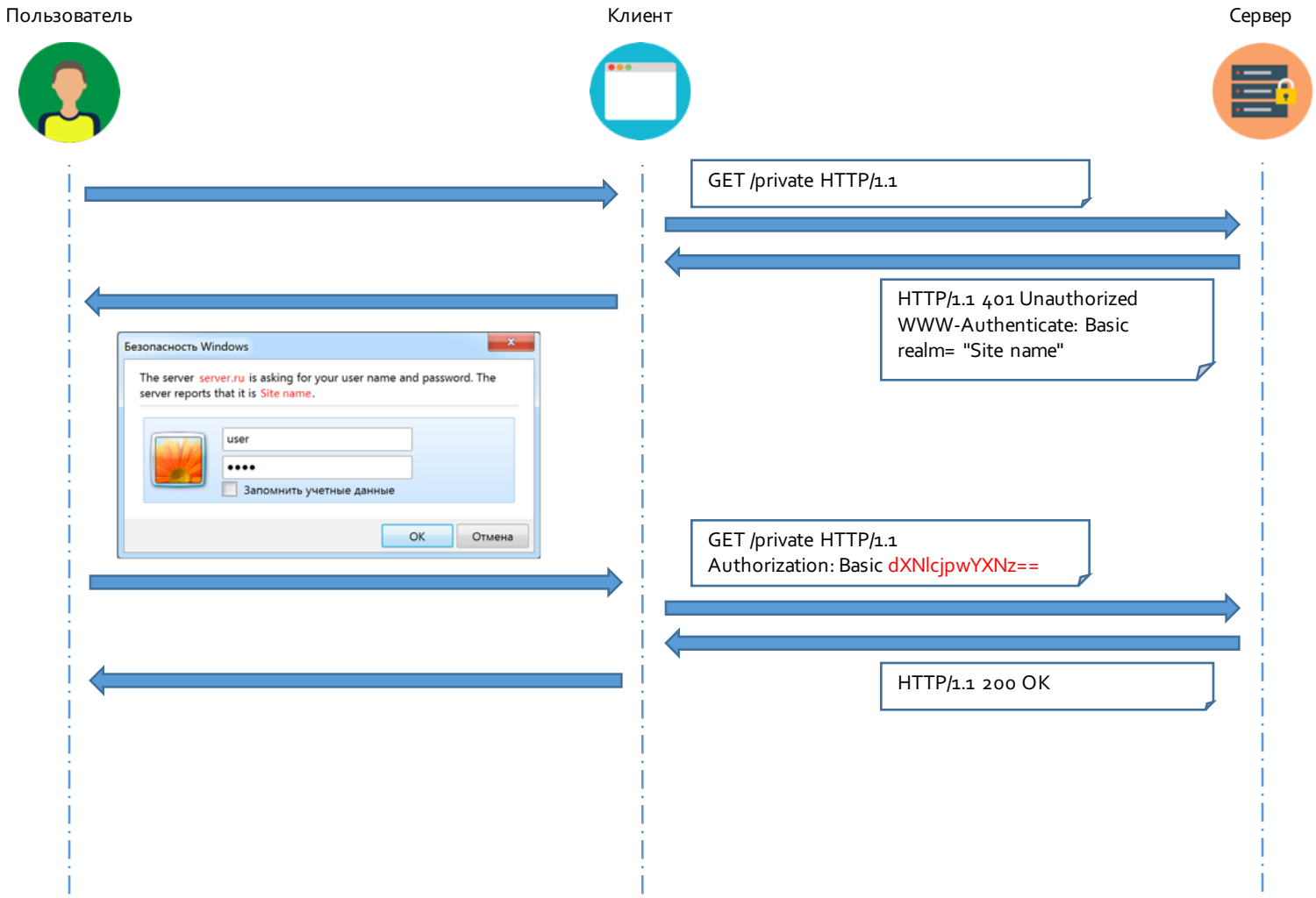
Возможные варианты реализации в приложении парольной аутентификации

Использование встроенных возможностей браузеров и протокола HTTP



Создание в приложении формы парольной аутентификации

HTTP Basic парольная аутентификация

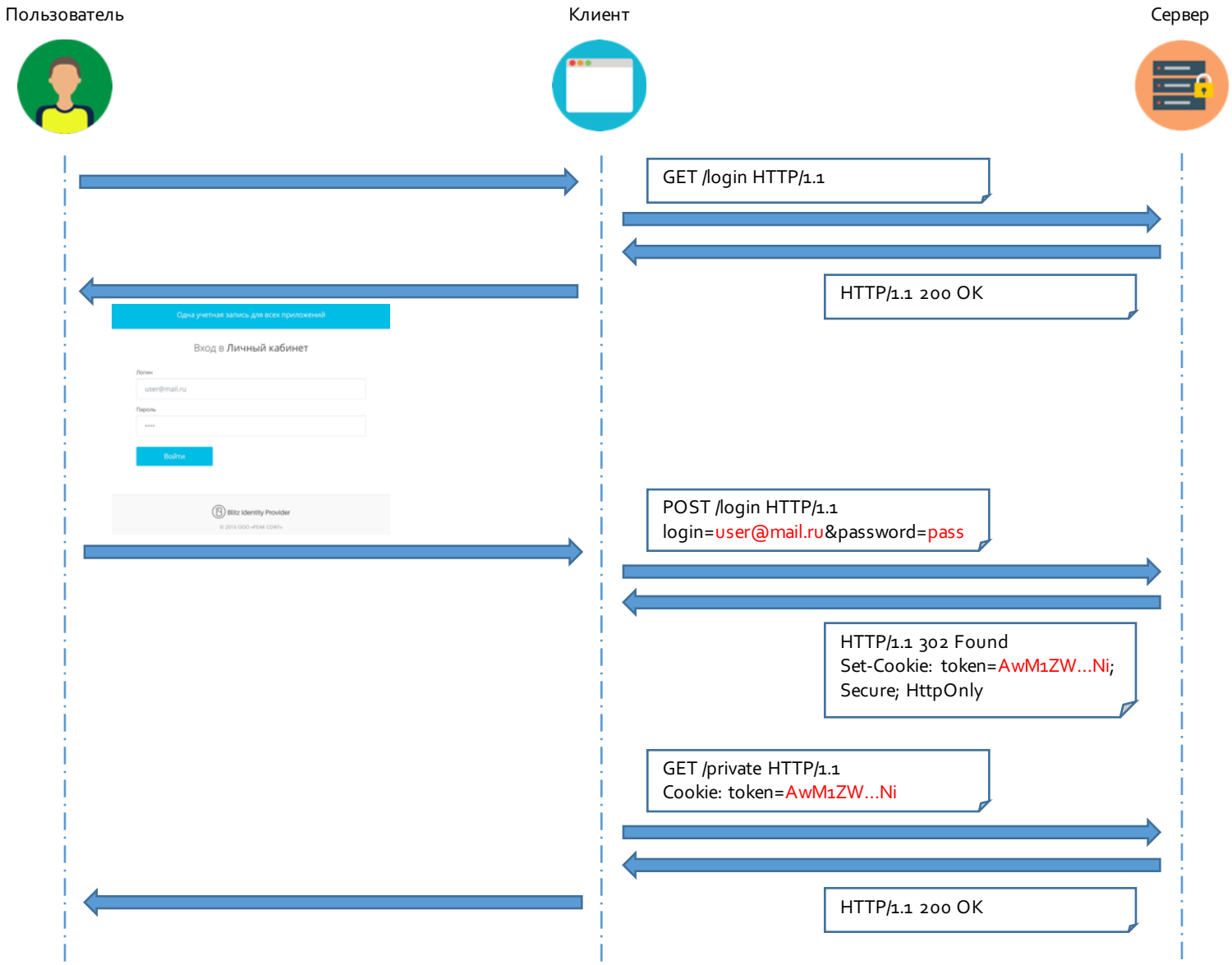


* base64encode("user:pass")="dXNlcjpwYXNz"

Другие виды HTTP аутентификации

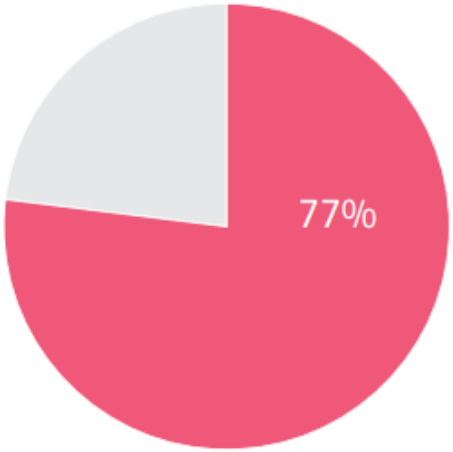
1. Digest
2. NTLM (Windows Authentication)
3. Negotiate

Аутентификация с использованием формы

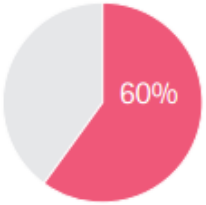


Пользователи не доверяют паролям

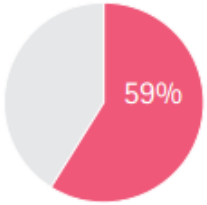
Я нуждаюсь в альтернативе логинам/паролям для своей защиты в Интернете



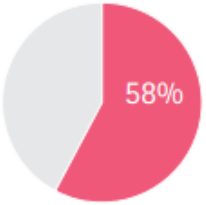
Логины и пароли громоздки в использовании



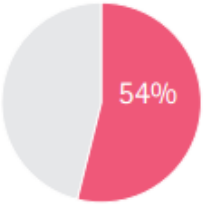
В следующем году я бы использовал уникальный чип в моем телефоне/ПК для своей защиты в Интернете



В следующем году я бы использовал биометрию для своей защиты в Интернете



Я знаю не менее одной альтернативы логину/паролю для своей защиты в Интернете



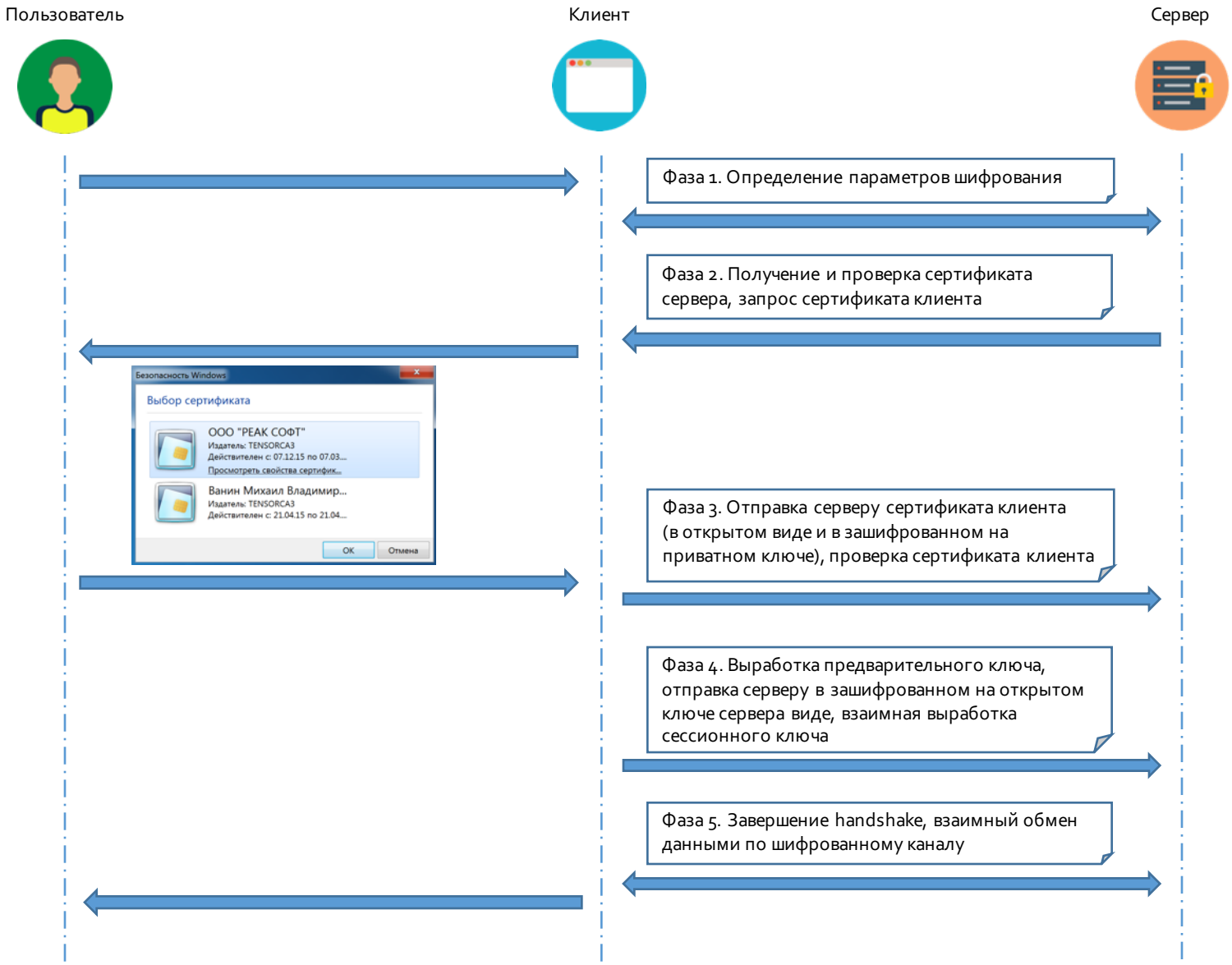
Источник: 2015 Accenture Digital Consumer Survey

Повышение надежности аутентификации

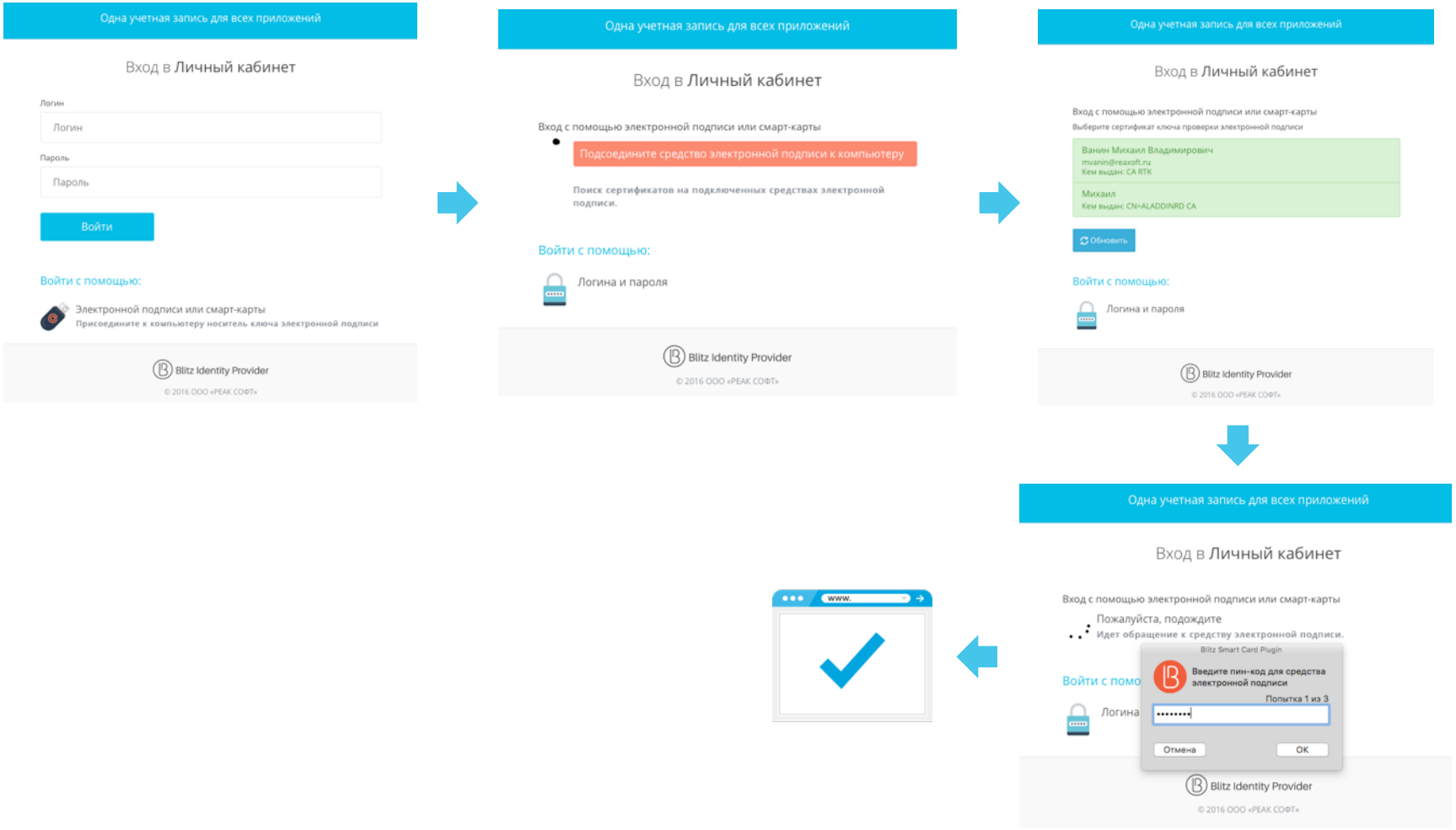
Строгая аутентификация (криптографические средства и электронная подпись)

Усиленная аутентификация (усиление парольной аутентификацией – проверка 2 фактора)

Строгая аутентификация с использованием TLS/SSL Handshake



Строгая аутентификация с использованием формы аутентификации



Для возможности взаимодействия веб-браузера с USB-токеном / смарт-картой необходим браузерный плагин

Критерии выбора плагина

1. **Поддержка различных ОС и браузеров**
   - Поддерживается ли Google Chrome? Или работа только через NPAPI?
   - Поддерживаются ли Linux и Mac OS X последних версий, и какие их браузеры?
2. **Поддержка средств электронной подписи различных производителей**
   - Поддерживаются ли смарт-карты и токены только одного производителя или разных?
   - Обеспечивается ли поддержка только в Windows или и в других ОС?
3. **Уровень технической поддержки производителя плагина**
   - Имеет ли разработчик плагина обязательства по технической поддержке и SLA?
4. **Безопасность плагина**
   - Не помещает ли плагин в ОС корневые доверенные сертификаты?
   - Не требует ли плагин ввода пользователем ПИН-кода в веб-страницы браузера?

Примеры плагинов

1. КриптоПро ЭЦП Browser plug-in
2. Aladdin JC-WebClient
3. Рутокен Плагин
4. Плагин портала государственных услуг
5. Blitz Smart Card Plugin

Варианты усиленной аутентификации

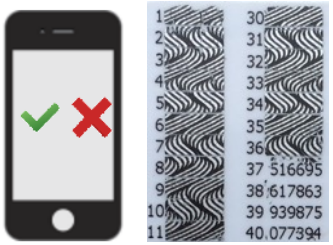
SMS-коды

Email-коды

HOTP-устройства

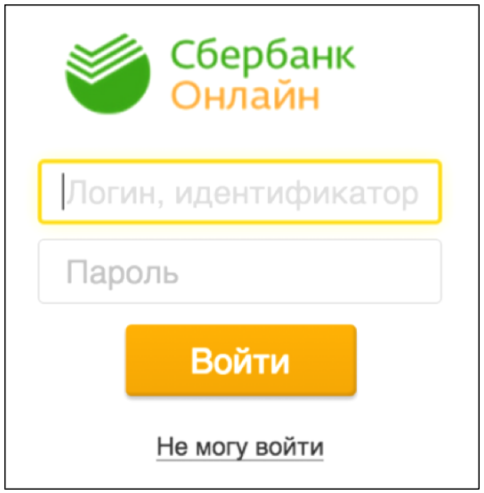
TOTP-устройства

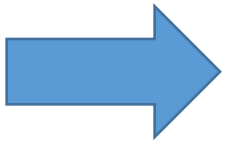
U2F-устройства

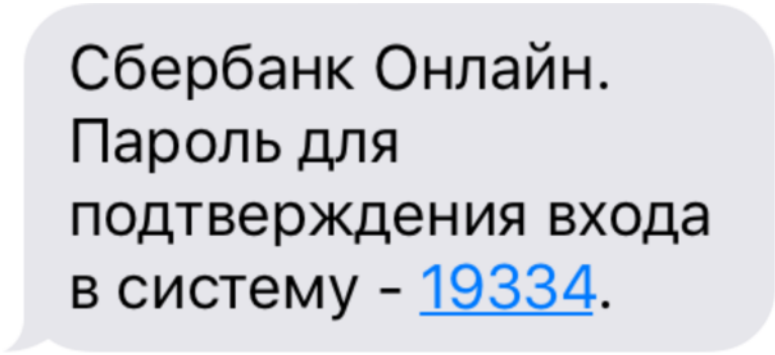


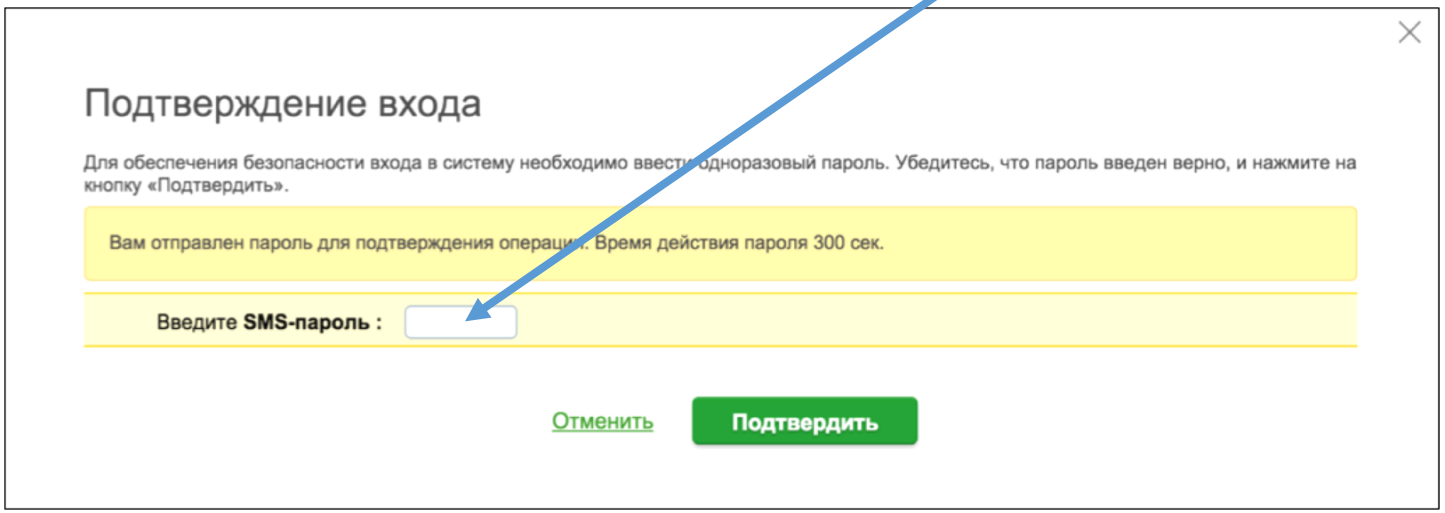
Иные способы

Отправка одноразового пароля по SMS / email









Разновидности HOTP-устройств

С LCD-дисплеем
(код вводит пользователь)

USB HID устройство
(само впечатывает код)

Комбинированное

RFC4226 «HOTP: An HMAC-Based One-Time Password Algorithm»

Примеры файлов описаний HOTP-устройств

Y000000273.xml

```xml
<?xml version="1.0" encoding="utf-8"?>
<Tokens>
  <Token serial="AN064433">
    <CaseModel>5</CaseModel>
    <Model>517</Model>
    <ProductionDate>03/19/2014</ProductionDate>
    <ProductName>eTPass 6.20</ProductName>
    <Applications>
      <Application ConnectorID="{a61c4073-2fc8-4170-99d1-9f5b70a2cec6}">
        <Seed>8ccd232e654561a4d4f77361111d161e3d60a99e</Seed>
        <MovingFactor>1</MovingFactor>
      </Application>
    </Applications>
  </Token>
</Tokens>
```

Пример файла для Aladdin eToken Pass

test.csv

```
LOGGING START,29.02.2016 19:09
OATH-HOTP,29.02.2016 19:09,1,,,1fae82de3e5e8bc0bd3386355cbac644f0c5cac3,,,0,0,0,6,0,0,0,0,0,0,0
3021021,,0,0ed62c725c43b8009f2a75ced7a0c646ab37cc34,000000000000,2016-02-29T19:13:49,
```

Пример файла для YubiKey

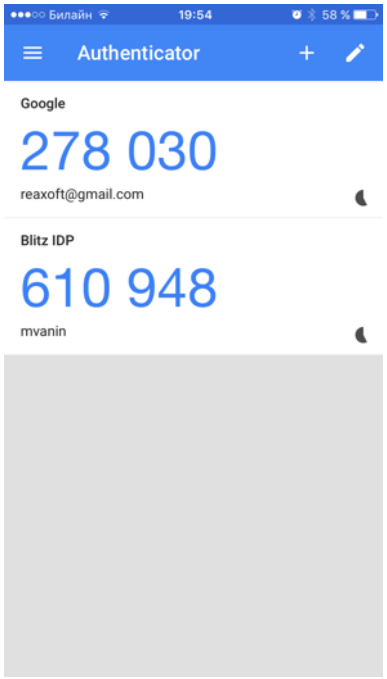
reaxoft-display-cards.pskc

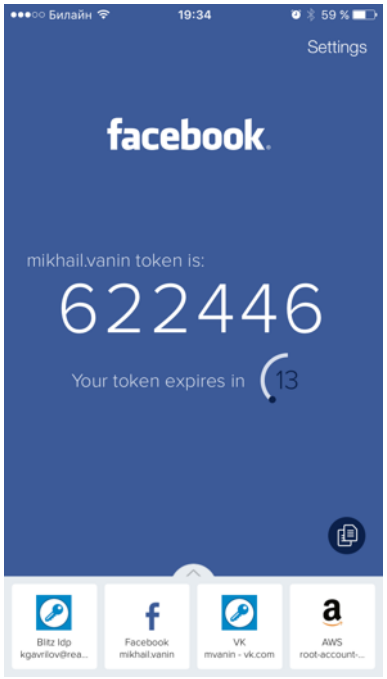
```xml
<?xml version="1.0" encoding="UTF-8"?>
<KeyContainer Version="1.0"
              Id="NIDS_749A0BA4"
              xmlns="urn:ietf:params:xml:ns:keyprov:pskc"
              xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
              xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionKey>
        <ds:KeyName>Pre-shared-key</ds:KeyName>
    </EncryptionKey>
    <MACMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1">
        <MACKey>
            <xenc:EncryptionMethod
            Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <xenc:CipherData>
                <xenc:CipherValue>
                SMdFc0ddvs8XQumhYlAGjZyViTskZYDZ/BVcuThE8azEz798ZCJ2njhanHL3kzvX<
                /xenc:CipherValue>
            </xenc:CipherData>
        </MACKey>
    </MACMethod>
  <KeyPackage>
    <DeviceInfo>
      <Manufacturer>NagraID Security</Manufacturer>
      <SerialNo>MC-00007568</SerialNo>
      <Model>306ES</Model>
      <IssueNo>1F0C0A547841081719</IssueNo>
    </DeviceInfo>
    <Key Id="1F0C0A547841081719"
        Algorithm="urn:ietf:params:xml:ns:keyprov:pskc:cap">
    <AlgorithmParameters>
        <ResponseFormat Length="6" Encoding="DECIMAL"/>
    </AlgorithmParameters>
      <Data>
        <Secret>
          <EncryptedValue>
            <xenc:EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <xenc:CipherData>
              <xenc:CipherValue>
              sBEGfpWsZso3Bo42W6yGxi0FrFHuAYVv3403WqTooTPHf4I8q7haPgaML1hebqqo<
              /xenc:CipherValue>
            </xenc:CipherData>
          </EncryptedValue>
          <ValueMAC>Y4nHXzEQ1KDsbjJn1H6VXve3KNE=</ValueMAC>
        </Secret>
        <Counter>
          <PlainValue>0</PlainValue>
        </Counter>
      </Data>
    </Key>
```

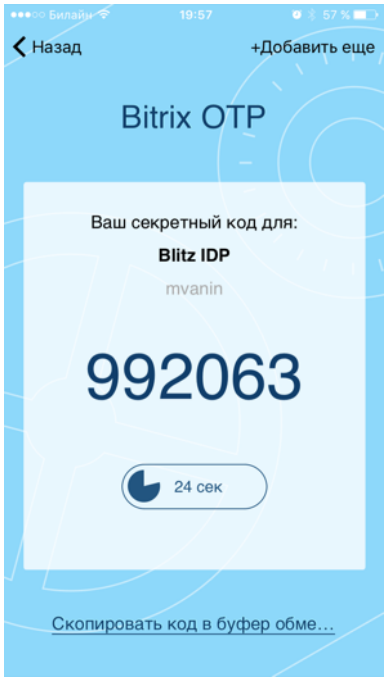
Пример файла для NagraID Security Display Card

Существует большое разнообразие формата файлов, описывающих HOTP-устройства

Примеры TOTP мобильных приложений







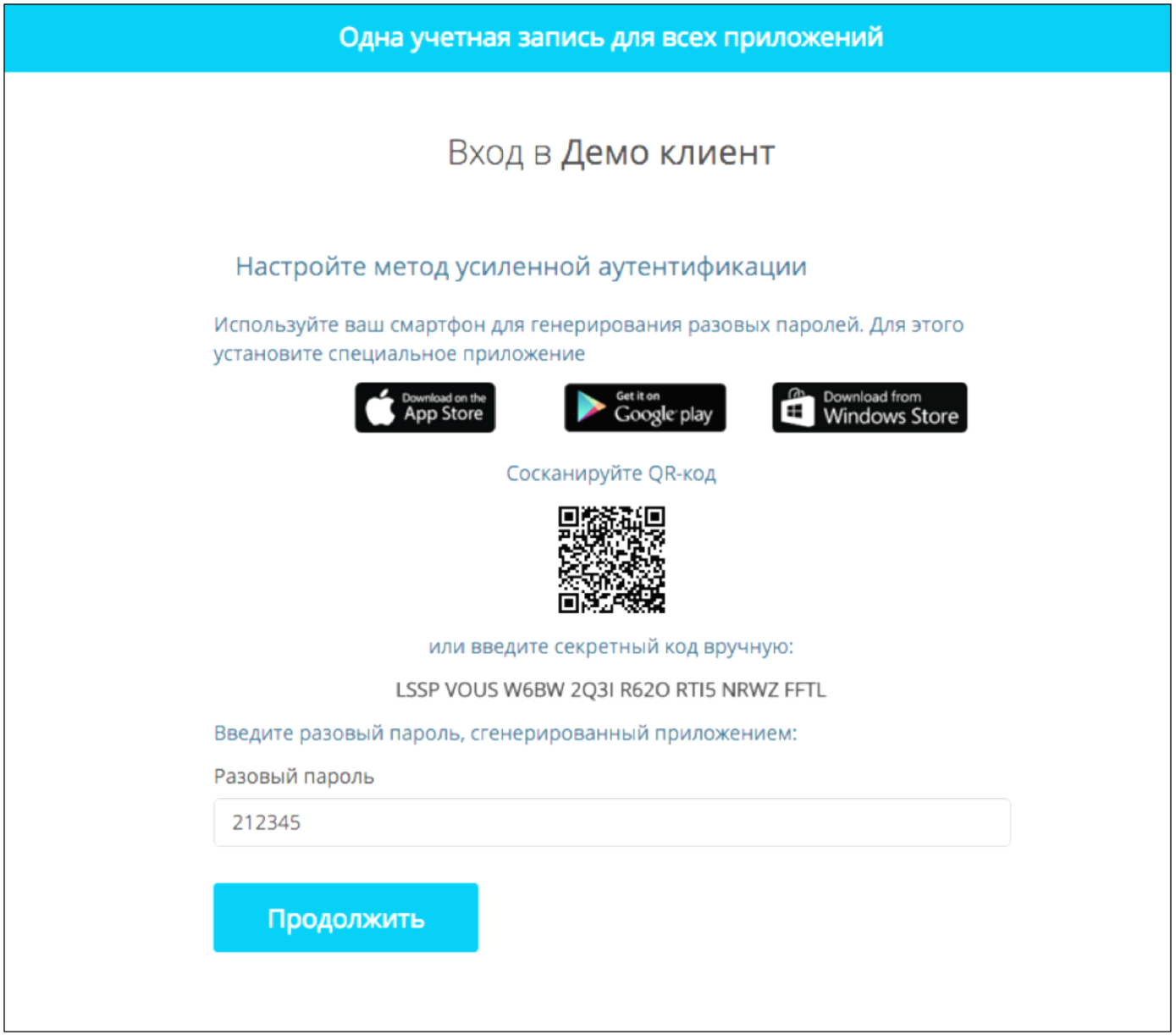
Google Authenticator
(наиболее известный)

Authy
(наиболее функциональный)

Bitrix24 OTP
(сделан компанией из РФ)

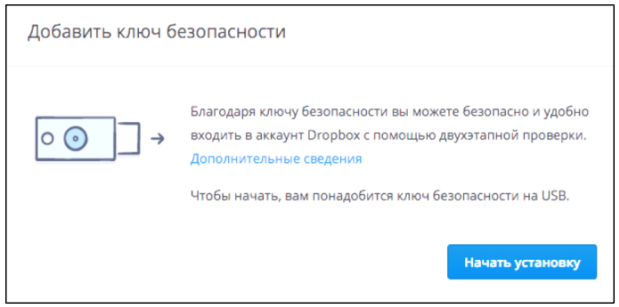
RFC6238 «TOTP: Time-Based One-Time Password Algorithm»

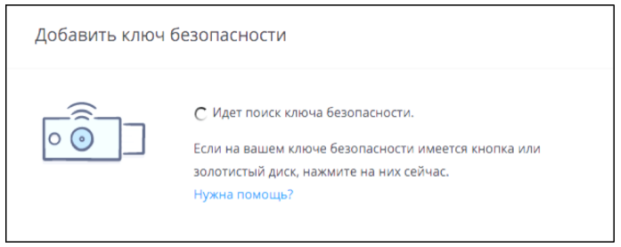
Пример окна настройки TOTP пользователем

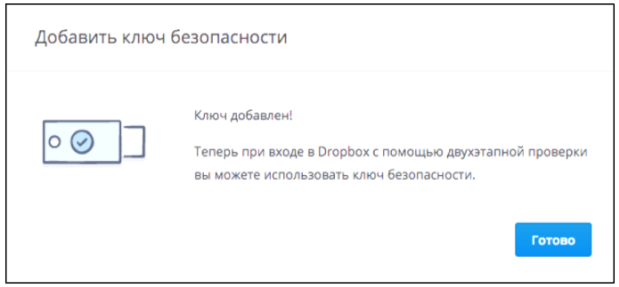


FIDO U2F устройство (Universal 2nd Factor)

Регистрация устройства







Проверка при входе

Еще разработчики беспокоятся о …

Регистрация и администрирование учетных записей

Регистрация событий входа/выхода

Отчеты о событиях входа

Информирование пользователей о событиях входа

Применение парольных политик

Сервисы самостоятельного восстановления пароля

Сервисы смены пароля, управления аутентификаторами

Сервисы выхода из приложений

А правильно ли разработчики поступают, когда создают все эти функции безопасности в своем приложении?

Типичная организация

Пользователи устали от парольного хаоса

Я не хочу запоминать много паролей от своих рабочих учетных записей.

И мне не нравится, что при смене пароля в каждом приложении свои правила его задания.

Мне не нравится, что когда переключаюсь между приложениями, то у меня каждый раз просят вновь ввести логин и пароль.

И что мешает сделать, чтобы экраны входа выглядели одинаково?

Я редко использовала приложение и забыла от него пароль.

И как мне его теперь восстановить?

Беспорядок с входом в приложения беспокоит и администраторов ИБ

Чем больше приложений со своей системой входа, тем чаще инциденты «забыл пароль». Пора что-то с этим предпринять

Я не могу гибко настроить в приложениях правила аутентификации.

Придется довольствоваться парольной аутентификацией

Пользователи не могут быстро усвоить новые пароли. Внедрение новых приложений происходит медленно

При внедрении нового приложения мне нужно готовить для него учетные записи, давать доступы, выдавать пользователям пароли. На это я трачу свои время и энергию

Беспорядок с входом в приложения беспокоит и администраторов

Я не уверен, что все эти механизмы аутентификации в разных приложениях безопасны. Сделанное «плохо» приложение компрометирует пароли и несет угрозу безопасности

У меня нет единой картины, в какие приложения кто из пользователей и как часто ходит

Пользователи выбирают ненадежные пароли. Вход не защищен. Парольные политики не эффективны

Организациям нужен единый сервис доступа

Пользователь с использованием любого устройства единожды проходит идентификацию и аутентификацию

Получает доступ к разрешенным приложениям как внутри, так и вне организации

Преимущества использования единого сервиса

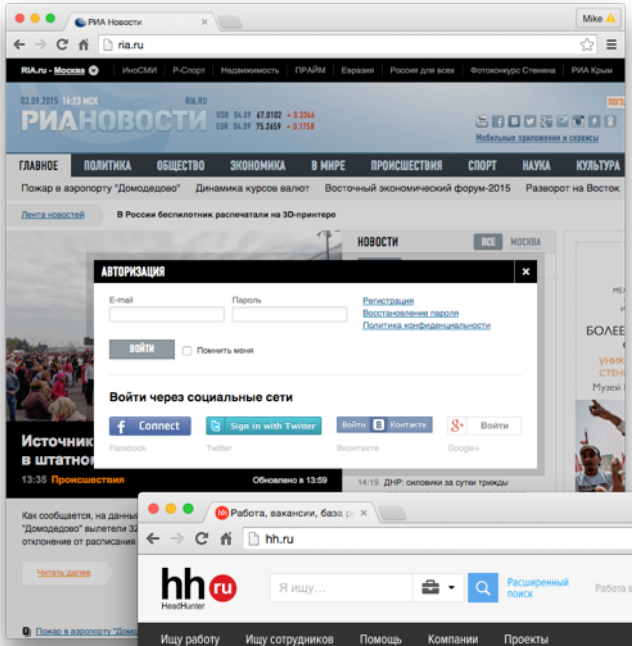
Пользователям:

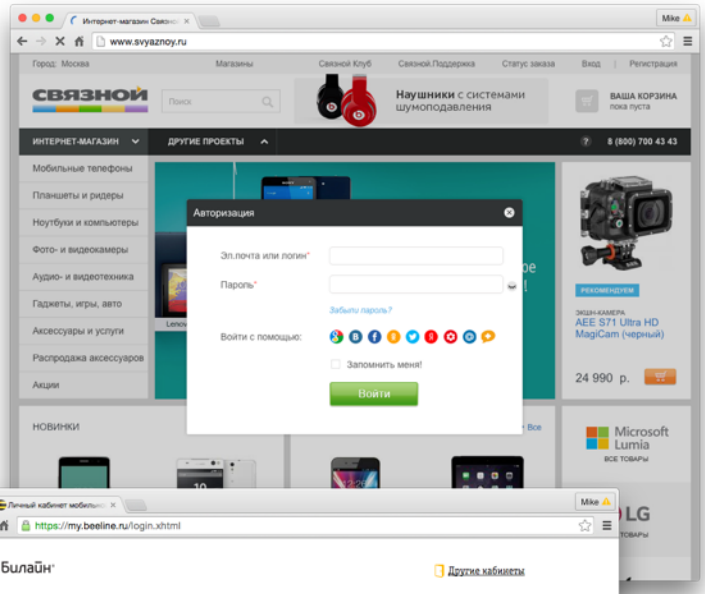
1) используя всего одну учётную запись пользователь получает доступ ко всем приложениям организации. Пользователи избавлены от необходимости помнить много логинов и паролей
2) используют надежные методы двухфакторной аутентификации
3) имеют средства для самостоятельного контроля событий безопасности, связанных с входом/выходом в приложения

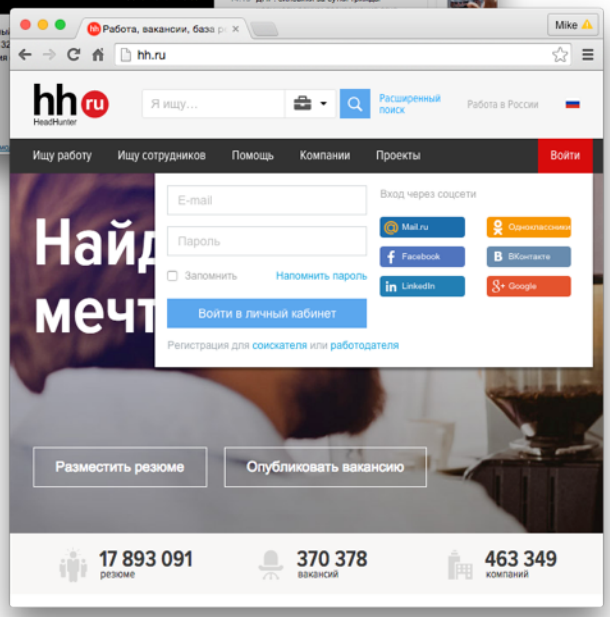
Владельцам/администраторам:

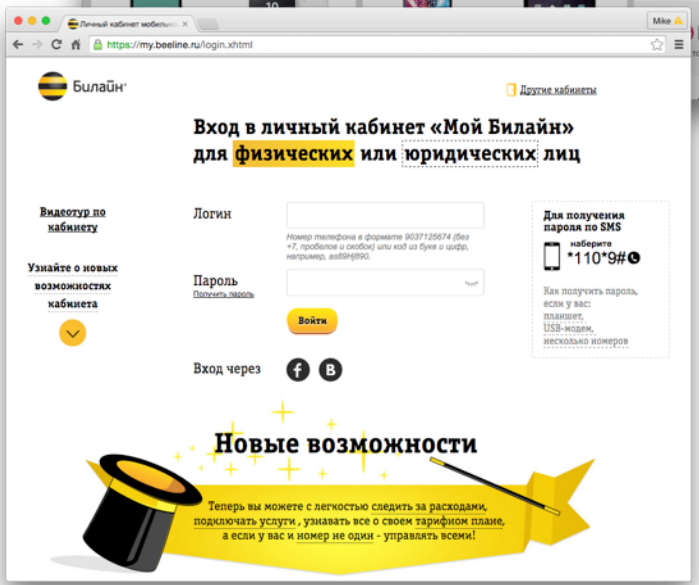
1) централизуют управление аутентификацией, снижают эксплуатационные затраты
2) внедрение новых приложений происходит быстрее – не нужно раздавать пользователям логины и пароли
3) увеличивают безопасность
4) снижают зависимость от поставщиков решений по аутентификации. Легко можно заменять поставщиков смарт-карт/токенов
5) с меньшими затратами добиваются соответствия нормативным требованиям по ИБ

Единый сервис доступа – это в тренде



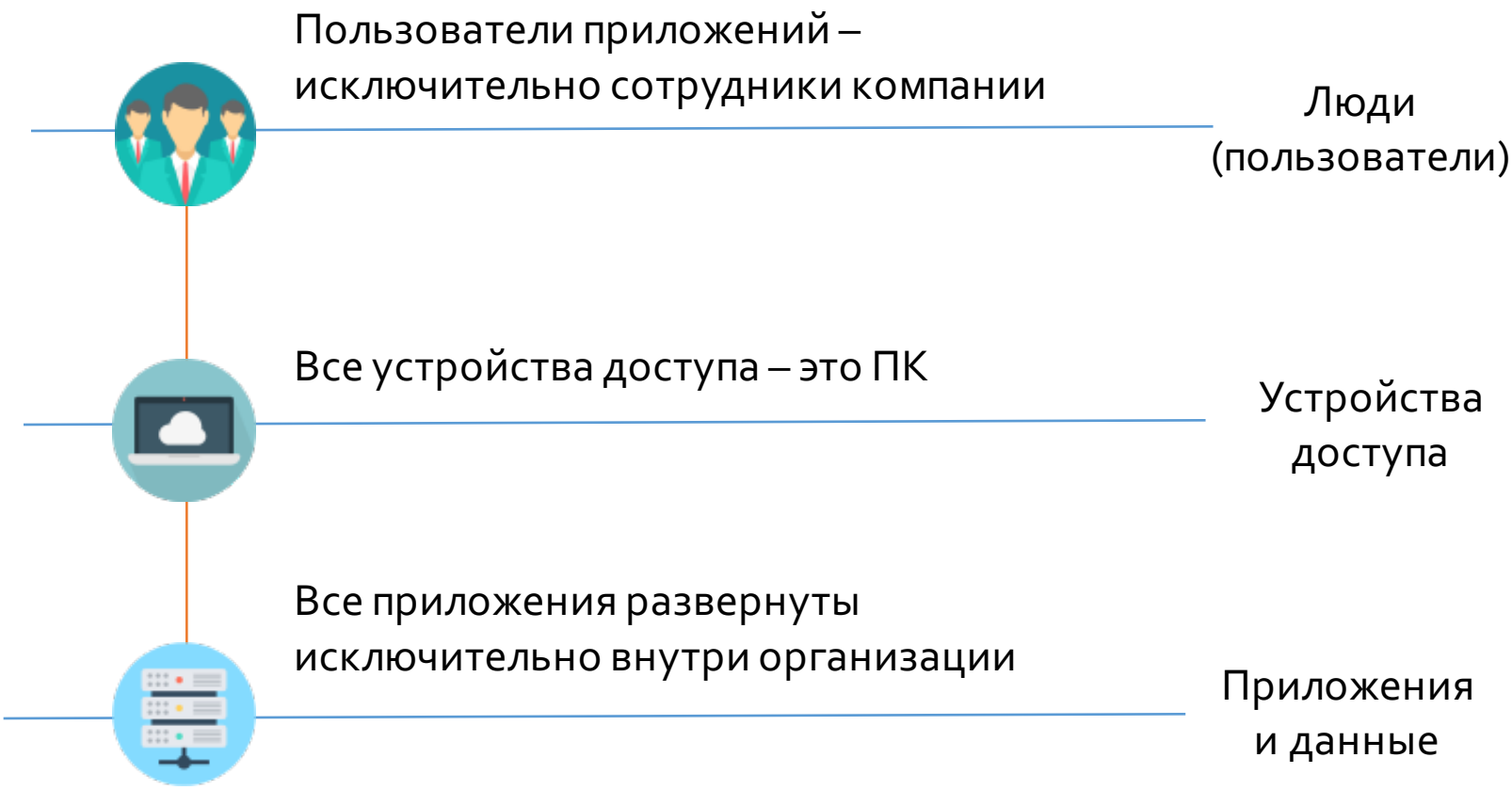






Для пользователей Интернет привычно, когда они используют любимую учетную запись соц.сети для доступа к множеству сайтов.

Эволюция условий, в которых должен функционировать единый сервис доступа

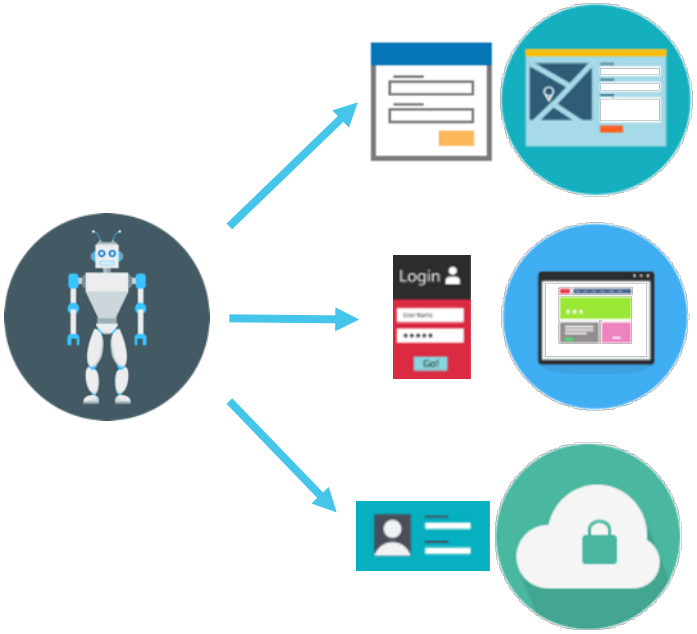


Вчерашний день

Эволюция условий, в которых должен функционировать единый сервис доступа

Сегодня и завтра

Как можно создать единый сервис доступа?



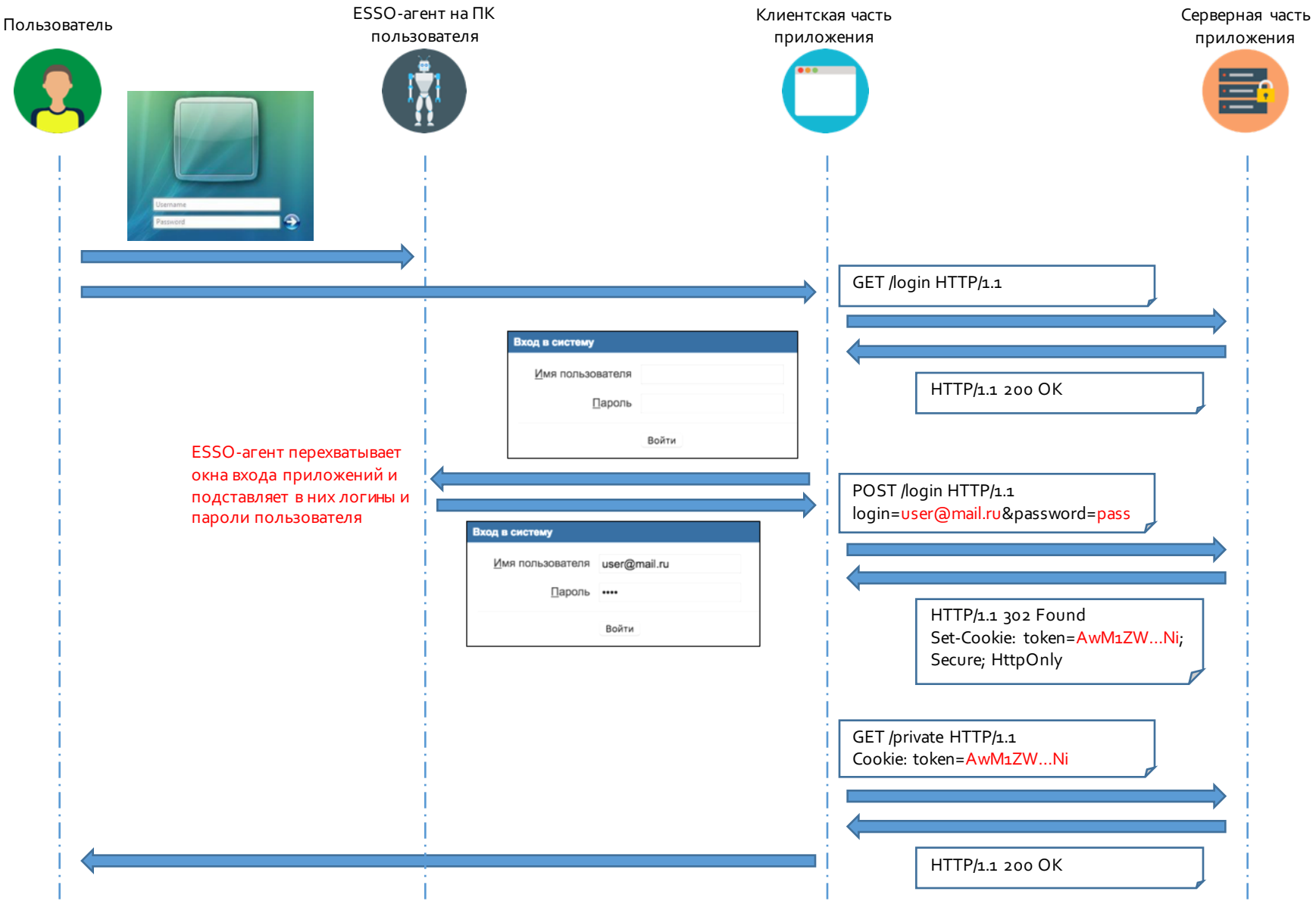
Традиционный метод

«Парольный менеджер»
(Enterprise SSO, Password Wallet)

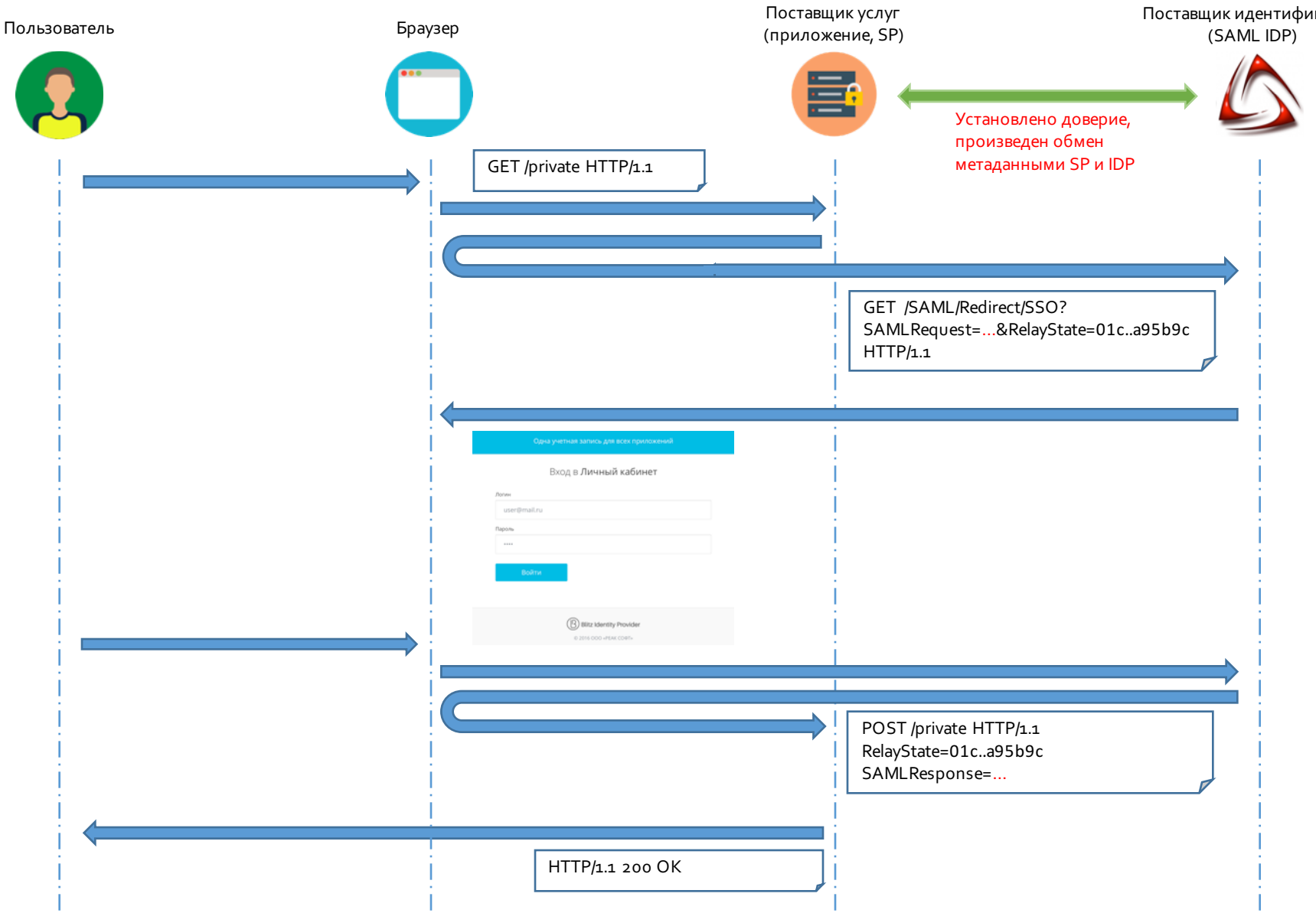
Современный метод

Identity Provider и использование протоколов федеративного доступа (SAML / WS-Federation / OAuth 2.0 + OpenID Connect)

Парольный менеджер, Enterprise Single Sign On

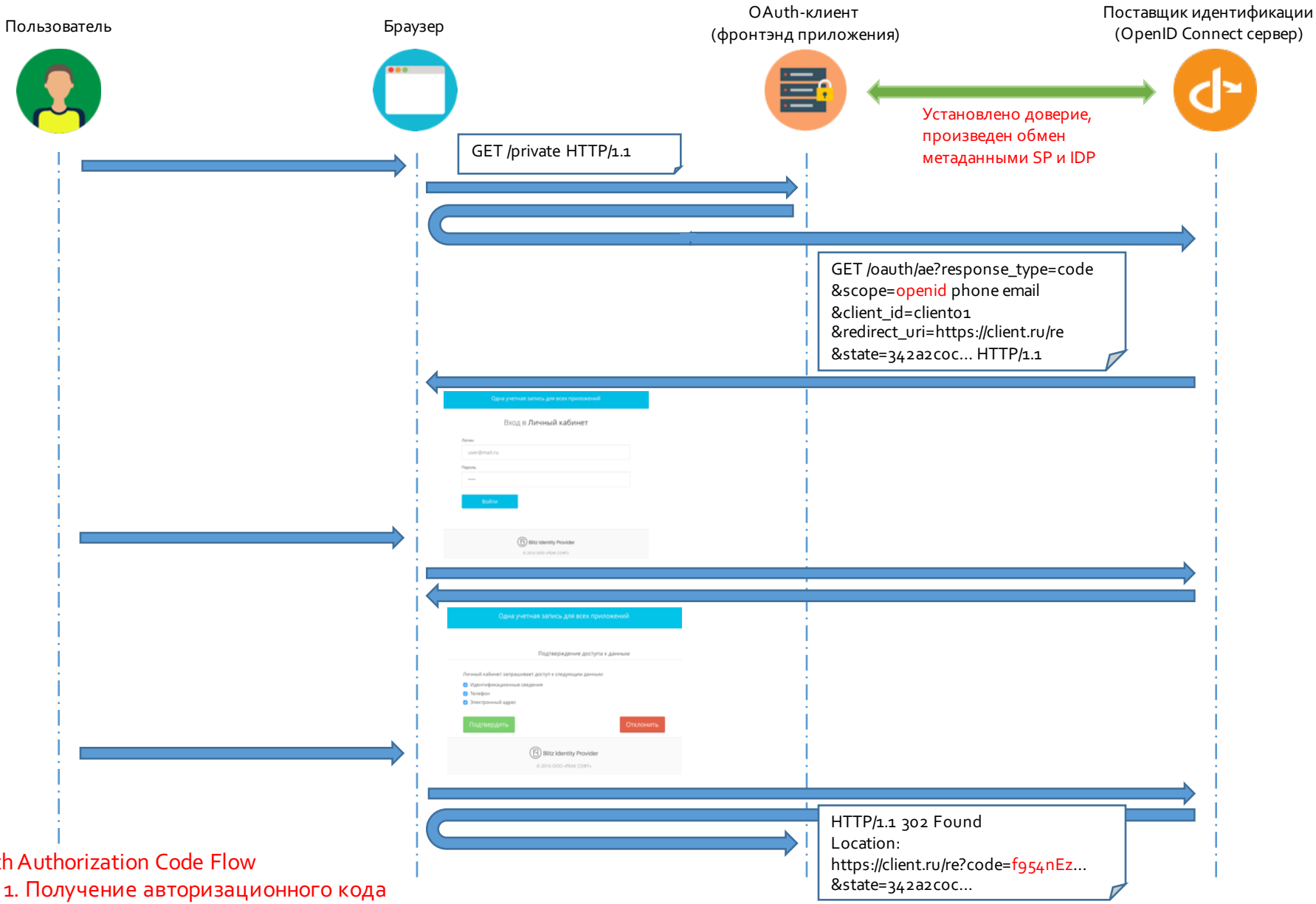


Идентификация/аутентификация с поставщиком идентификации SAML



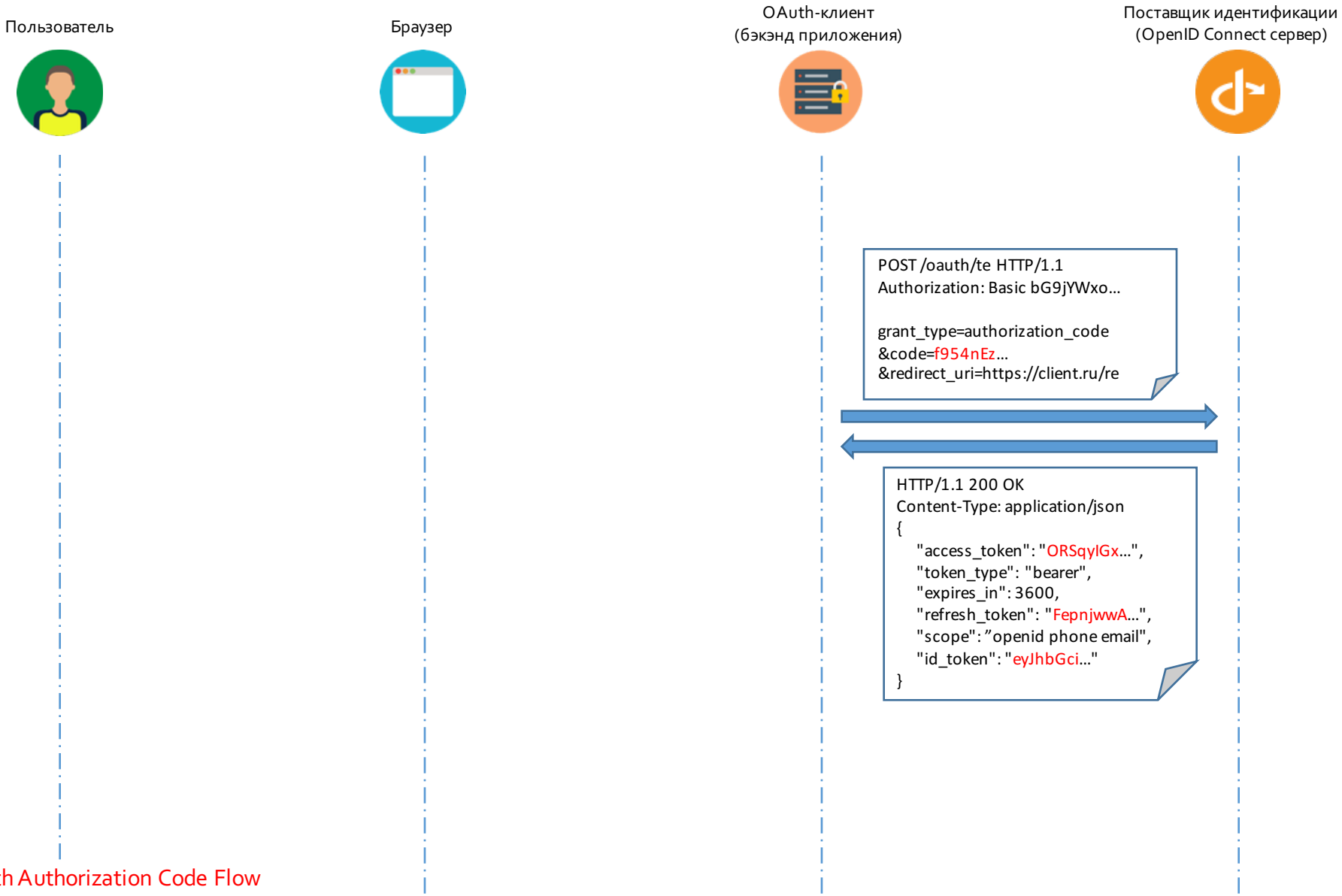
Примеры приложений, поддерживающих SAML

Идентификация/аутентификация с поставщиком идентификации OpenID Connect (OAuth 2.0)



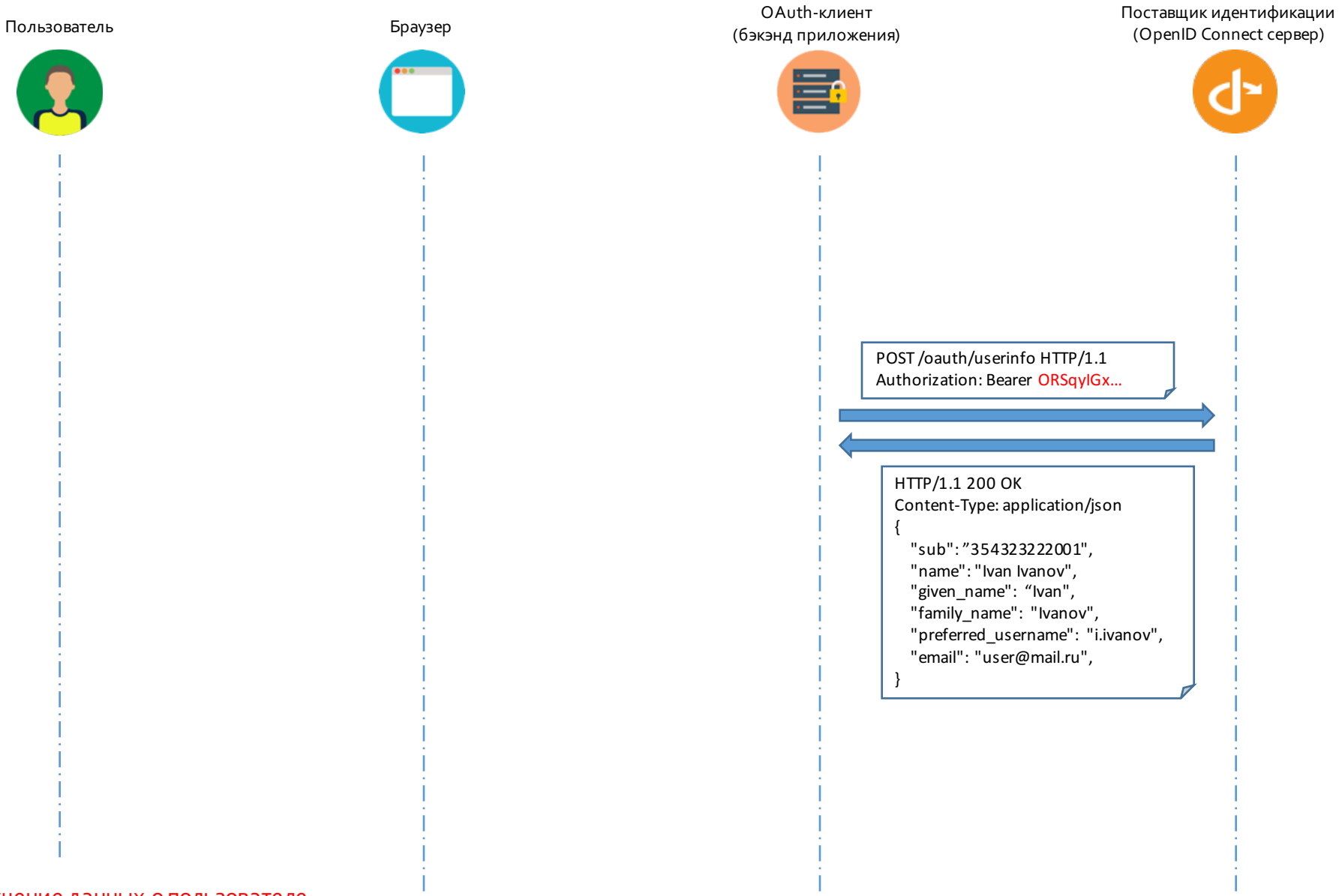
OAuth Authorization Code Flow
Фаза 1. Получение авторизационного кода

Идентификация/аутентификация с поставщиком идентификации OpenID Connect (OAuth 2.0)



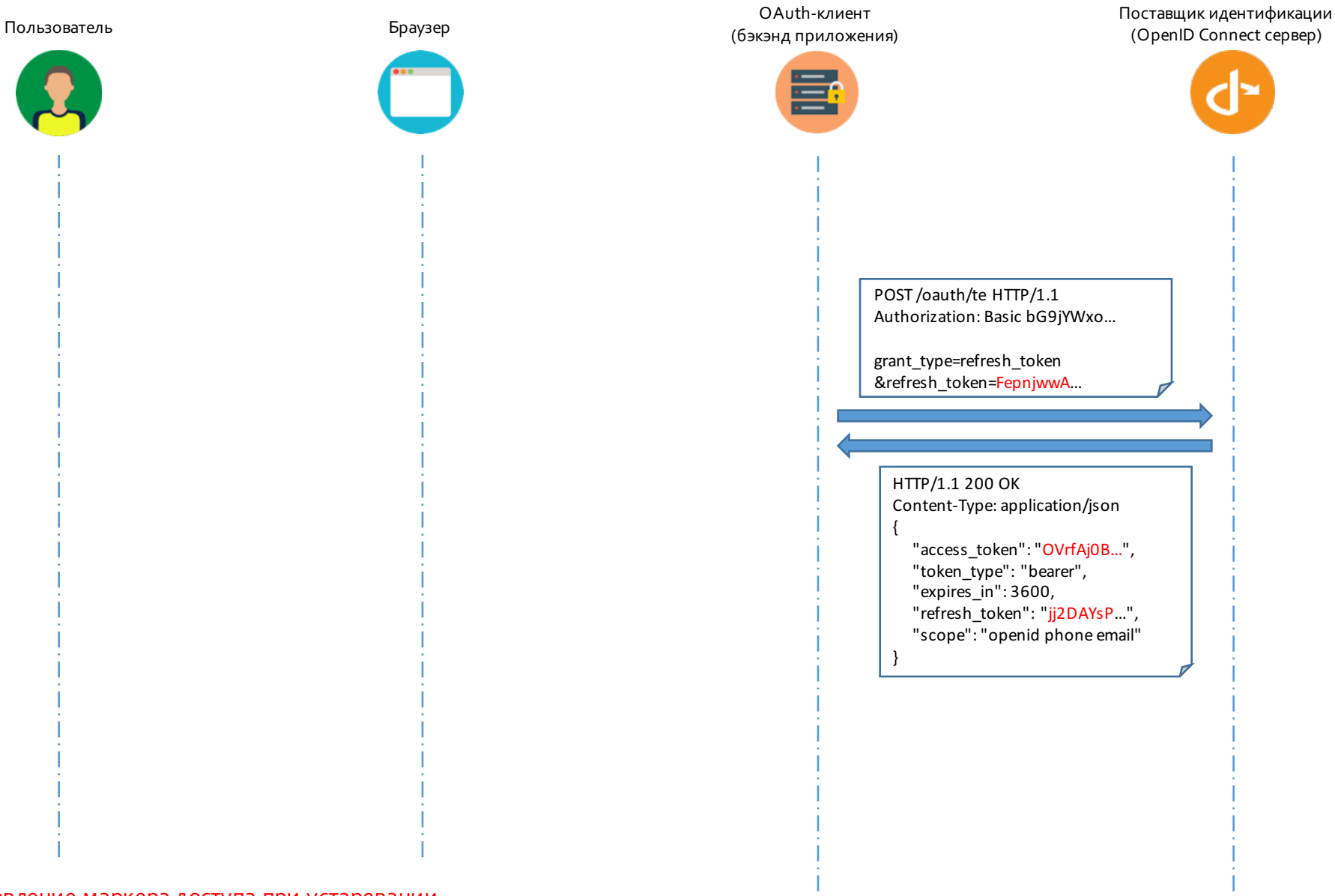
OAuth Authorization Code Flow
Фаза 2. Получение маркера доступа

Идентификация/аутентификация с поставщиком идентификации OpenID Connect (OAuth 2.0)



Получение данных о пользователе

Идентификация/аутентификация с поставщиком идентификации OpenID Connect (OAuth 2.0)



Обновление маркера доступа при устаревании

ПО для создания единого сервиса доступа

Решения крупнейших вендоров	Специализированное ПО	Облачные сервисы (IDaaS)
Oracle Access Manager Tivoli Access Manager Windows Server Active Directory ca technologies RSA Access Management	PingFederate InsightCloud PortalGuard SecureAuth SSOeasy Shibboleth OpenAM WSO2 Identity Server gluu Open-source	PingOne onelogin okta DUO Centrify welcome miniOrange covisint SailPoint

Российское ПО

Решения на основе метода «парольный менеджер»	Решения на основе протоколов федеративного доступа
INDEED ID Avanpost	Blitz Identity Provider

Заключение

1. Создание в приложении функций идентификации, аутентификации, авторизации требует усилий и компетенции
2. Результат получается лучше при решении задач идентификации, аутентификации, авторизации сторонними средствами защиты, а не путем создания встроенных функций безопасности
3. Есть большой выбор вариантов платформы для создания единого сервиса доступа. Есть несколько популярных и устоявшихся стандартов и протоколов для взаимодействия приложений и единого сервиса доступа

Материалы по теме презентации

1. Дистрибутив ПО Blitz Identity Provider для создания единого сервиса доступа (Linux/Windows) - http://identityblitz.ru/products/blitz-identity-provider/download/
2. Обзорная статья на Хабре о способах и протоколах аутентификации (Дмитрий Выростков, DataArt) - https://habrahabr.ru/company/dataart/blog/262817/
3. Мои презентации на SlideShare - http://www.slideshare.net/MikhailVanin

Пожалуйста, задавайте вопросы!

Мои контакты: Михаил Ванин, mvanin@reaxoft.ru