Identity Blitz

Сервер аутентификации Blitz Identity Provider

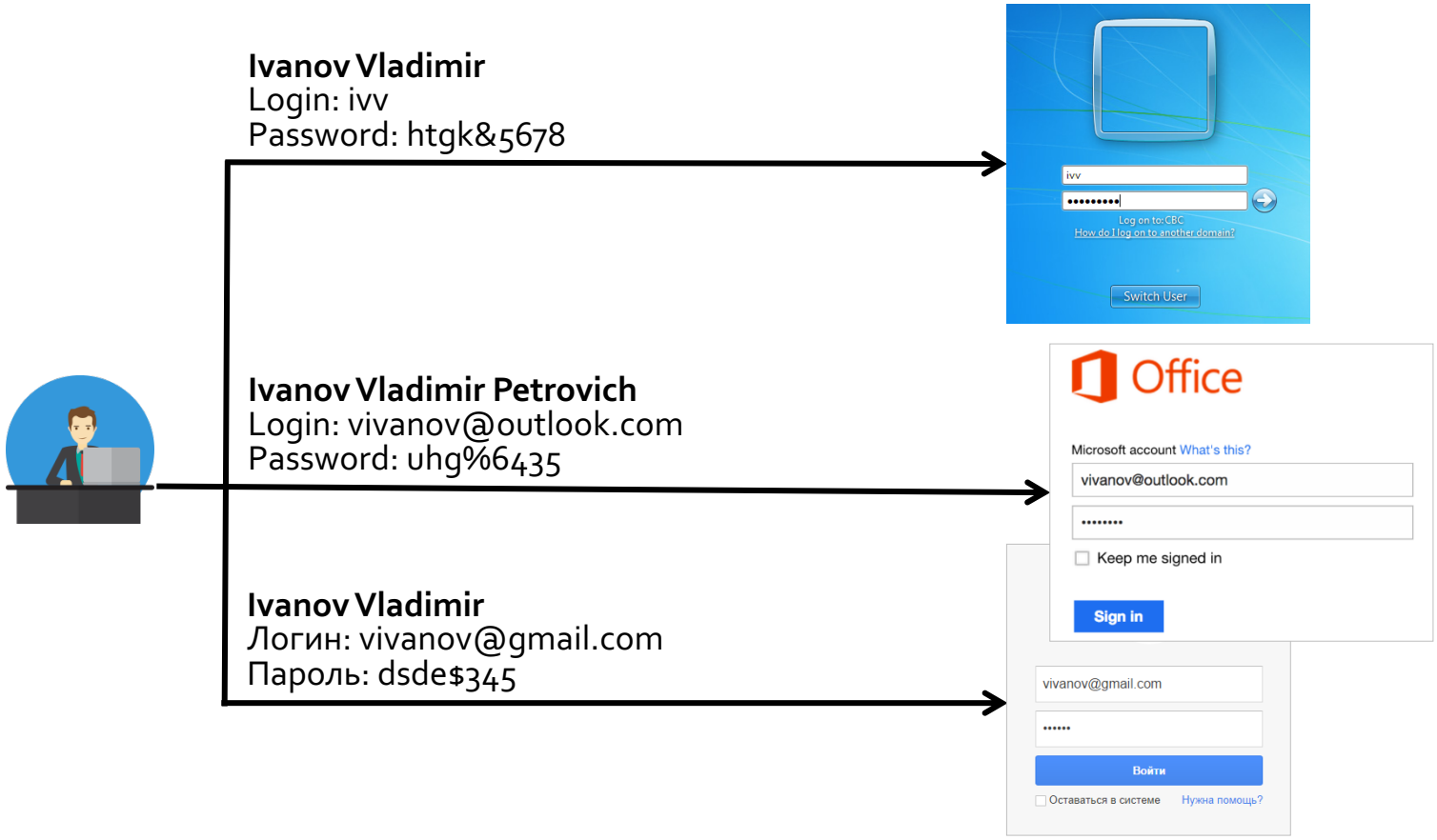
Скажите нет парольному хаосу

РЕАК СОФТ

Содержание

1) **Проблема**
2) Решение
3) О компании

Парольный хаос



Обычный сотрудник имеет в среднем не менее 3 учетных записей от приложений компании. Некоторым же приходится помнить более 10 паролей от рабочих учетных записей (DTI survey 2006)

Слабая защищенность учетных записей

Хорошие пароли трудно запомнить,
пароли можно украсть или подобрать

Не все механизмы аутентификации в разных приложениях достаточно безопасны. Сделанное «плохо» приложение компрометирует пароли и несет угрозу безопасности

При доступе к «облачным» / «внешним» сервисам пароли покидают организацию

36% экспертов по ИБ считают, что атаки фишинга будут наиболее значимой киберугрозой в ближайшие три года (Ponemon Institute Research Report 2015)

Ограниченные возможности для контроля доступа и аудита

Приложения не всегда позволяют гибко настроить правила аутентификации в зависимости от того, кто, когда и откуда осуществляет вход

У администратора отсутствует единая картина, в какие приложения кто из пользователей и как часто входит

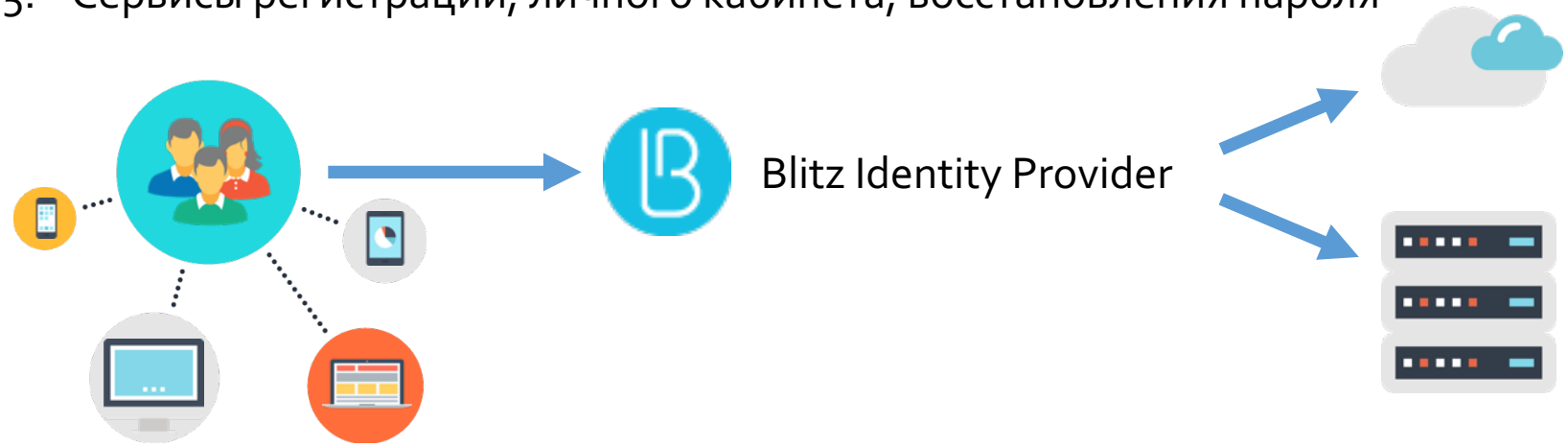
Сотрудникам другой организации, филиала или дочерней компании трудно быстро предоставить доступ к информационным ресурсам компании, не подвергаясь риску несанкционированного доступа

Содержание

1) Проблема
2) **Решение**
3) О компании

Решение – создание единого сервиса входа организации

1. Одна учетная запись для доступа ко всем приложениям компании
2. Однократность процедуры входа
3. Гибко настраиваемая двухфакторная аутентификация
4. Возможность доступа с любых устройств (PC, Apple Mac, планшет, смартфон)
5. Сервисы регистрации, личного кабинета, восстановления пароля



28% организаций в мире уже внедрили систему единого входа. 25% планируют это сделать в течение года (Deloitte security survey 2007)

Что дает Blitz Identity Provider

Blitz Identity Provider – серверное ПО, устанавливаемое на сервера компании. Пользователи могут входить в приложения компании и в SaaS-сервисы с использованием единой учётной записи пользователя и однократной аутентификации

Компаниям, уставшим от парольного хаоса

- ✓ безопасный доступ ко всем приложениям компании
- ✓ двухфакторная аутентификация при удаленном доступе (из вне сети организации)
- ✓ использование любых устройств доступа (PC, Apple Mac, смартфоны, планшеты)

Разработчикам веб-порталов

- ✓ возможность входа через аккаунты соцсетей
- ✓ самообслуживание пользователей (регистрация, личный кабинет, восстановление забытого пароля)
- ✓ гибкая настройка методов аутентификации

Разработчикам прикладного ПО

- ✓ поддержка SSO-протоколов (SAML 2.0, OAuth 2.0, OpenID Connect 1.0)
- ✓ Поддержка разнообразных методов двухфакторной аутентификации
- ✓ Настраиваемые формы регистрации и ведения личного кабинета

Поддержка разнообразных методов аутентификации

Парольная аутентификация

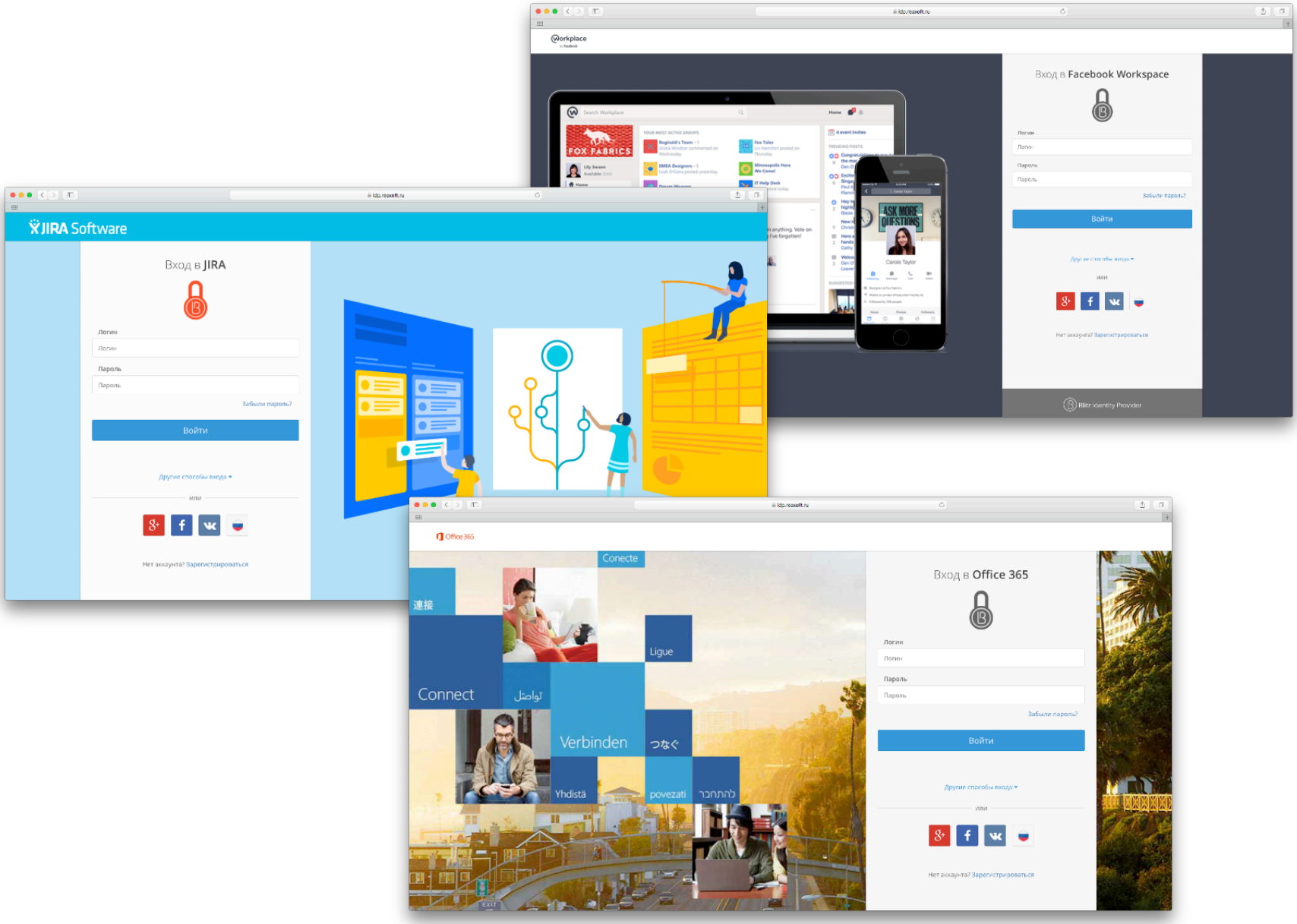
Вход через аккаунт в соцсетях и в госуслугах

Интегрированная в ОС аутентификация
(сквозная идентификация по результатам входа в домен)

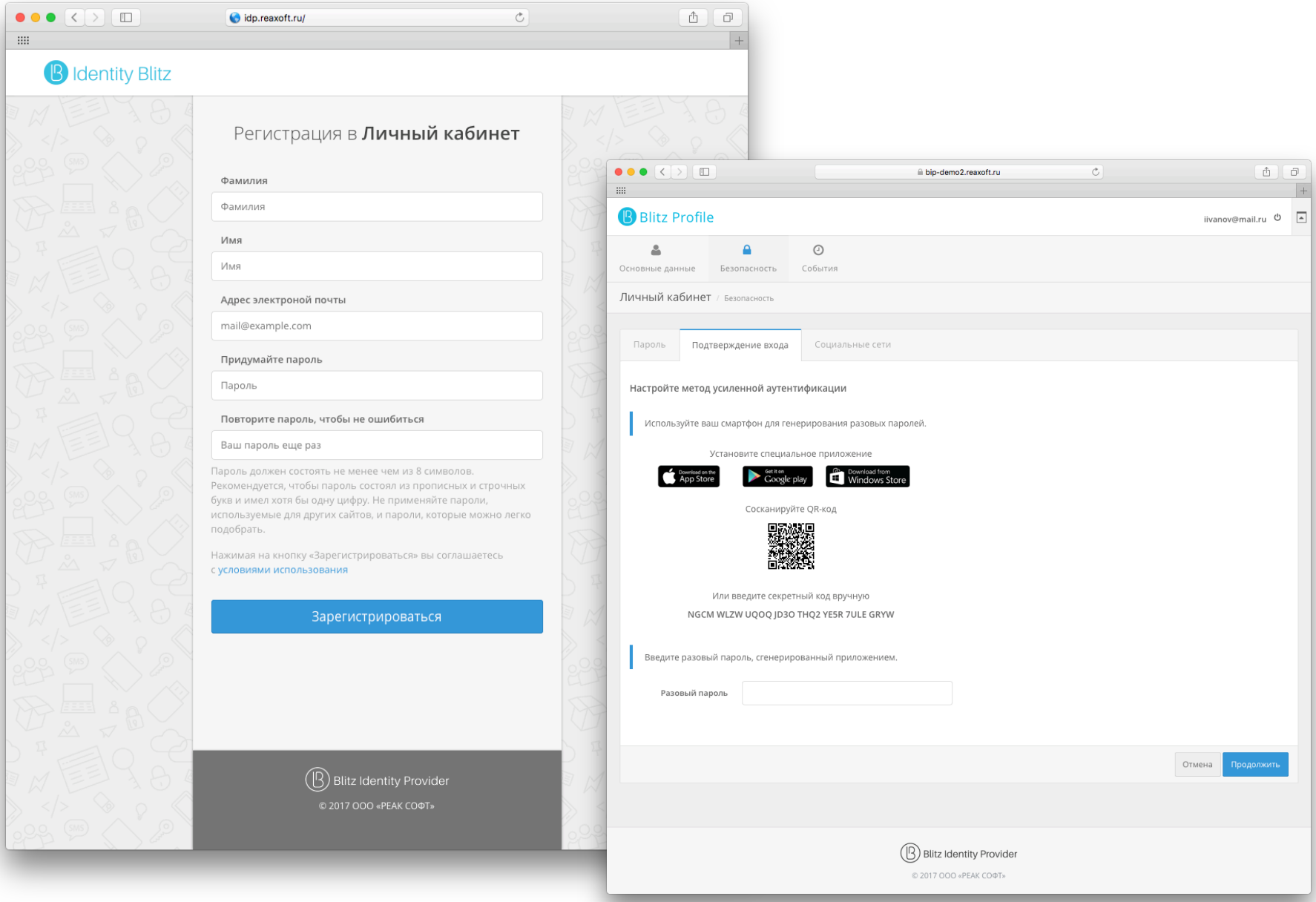
Усиленная аутентификация
(проверка 2 фактора в дополнении к паролю)

Строгая аутентификация
(проверка электронной подписи)

Настраиваемый внешний вид пользовательского интерфейса



Конфигурируемые сервисы самообслуживания

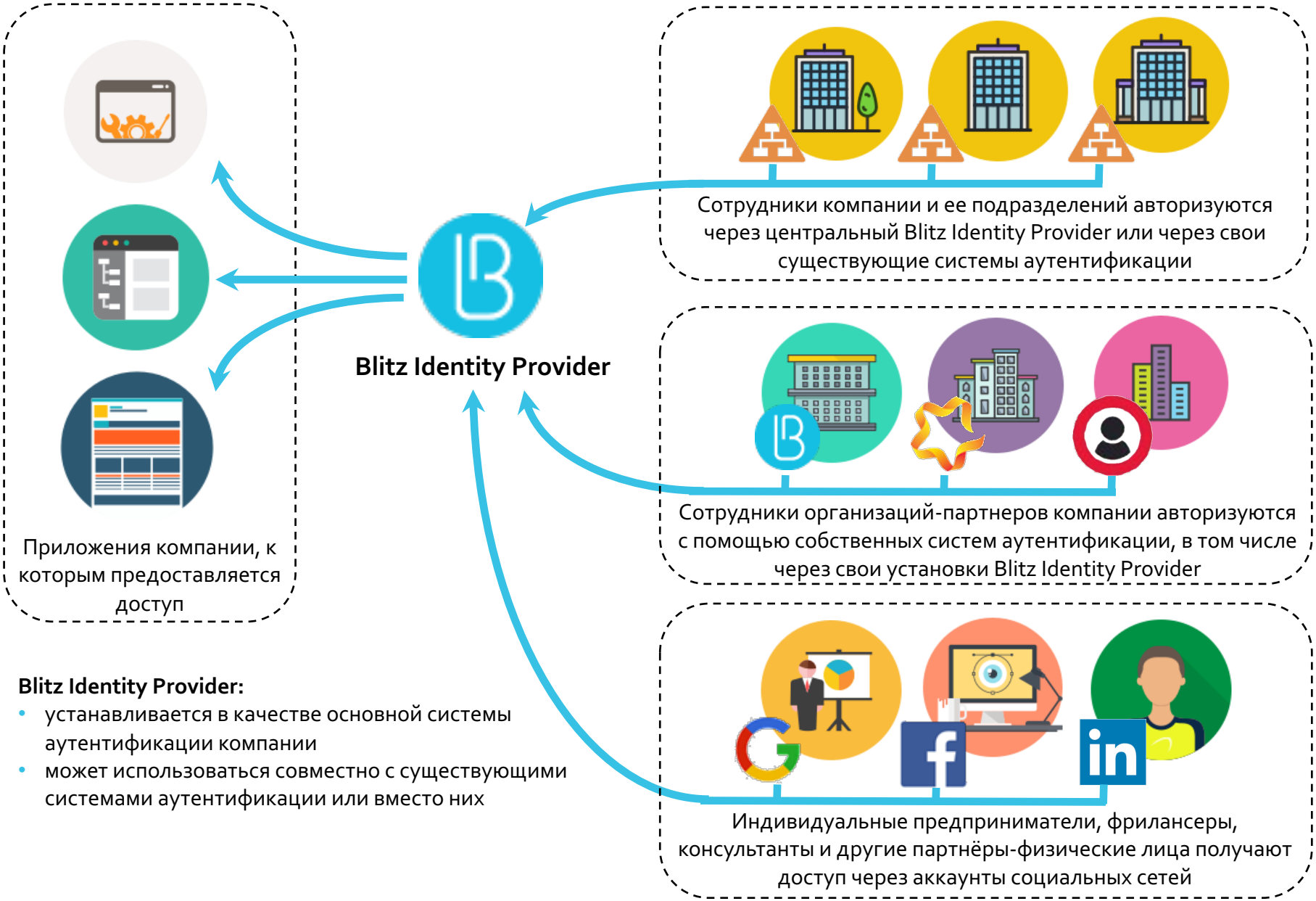


Гибкие процедуры входа

Функциональные возможности Blitz Identity Provider

Предоставляемые способы идентификации и аутентификации	1) 2) 3) 4) 5) 6)	Логин/пароль Смарт карта / USB-токен с электронной подписью Аппаратные брелоки (HOTP/TOTP/OCRA) Программные TOTP-брелоки (Google Authenticator, Яндекс.Ключ, Authy и им подобные) SMS-коды push-аутентификация на мобильное приложение
Поддержка внешних систем идентификации	1) 2) 3) 4) 5)	Вход через социальные сети (Google / VK / Facebook) Вход через gosuslugi (ЕСИА) Вход через установку Blitz Identity Provider другой организации (федерация) Вход с использованием Kerberos-сервера Вход с использованием совместимого TLS/SSL-шлюза или VPN-шлюза
Способы подключения приложений	1) 2) 3)	SAML 1.0/1.1/2.0 OpenID Connect 1.0 (OIDC) / OAuth 2.0 через веб-прокси с пробросом логина/пароля в форму входа веб-приложения
Подключение к внешним хранилищам учетных записей и паролей	1) 2) 3)	MS Active Directory / Samba4 LDAP-совместимый сервер Произвольное хранилище (через коннектор-обертку)
Сервисы самообслуживания пользователей	1) 2) 3)	Самостоятельная регистрация пользователя Самостоятельное восстановление забытого пароля Личный кабинет настроек безопасности (возможность вести данные в аккаунте, менять пароль, настраивать двухфакторную аутентификацию, смотреть события безопасности и список используемых устройств доступа)
Прочее	1) 2) 3) 4) 5) 6)	Веб-консоль администрирования сервиса аутентификации и пользователей Настраиваемый внешний вид страниц входа Протоколирование событий доступа и аудит Гибкая настройка правил контроля доступа при входе в приложения Высокая производительность при развертывании на скромных аппаратных ресурсах Высокая надежность при развертывании в кластере

Пример использования в компании с построением «сетей доверия»



Blitz Identity Provider:

- устанавливается в качестве основной системы аутентификации компании
- может использоваться совместно с существующими системами аутентификации или вместо них

Кому будет полезен Blitz Identity Provider?

Федеральные и региональные органы власти

- ✓ Построение региональной системы единого входа для доступа пользователей к региональным сервисам (Госуслуги, ЖКХ, форумы, сайты региональных компаний) и получение большего контроля, нежели чем все системы подключать к ЕСИА
- ✓ Унификация доступа сотрудников региональных и муниципальных властей, а также совместное использование региональных систем сотрудниками разных ведомств

Коммерческие компании – заводы, телеком, банки, торговые сети, интернет-порталы, страховые компании

- ✓ Имеют несколько приложений (веб-приложения, мобильные приложения) с разными системами входа и учетными записями. Желают унифицировать вход и навести порядок
- ✓ Компании ведут интернет-бизнес. Хотят предоставить пользователям удобные средства регистрации аккаунтов, входа, восстановления забытого пароля, защиты аккаунтов
- ✓ Хотят развивать в организации ИТ-архитектуру предприятия. Создавать сервисы и повторно их использовать. Хорошее начало – единый сервис доступа организации

Корпорации, холдинги, управляющие компании

- ✓ Имеют холдинговую или филиальную структуру. В результате слияний и поглощений внутри много баз учетных записей и разрозненных сервисов входа. Нуждаются в унификации доступа, что дает также возможность предоставлять сотрудникам доступ к общим приложениям корпорации или получать совместный доступ к системам различных филиалов

ВУЗы

- ✓ Унифицировать доступ абитуриентов, студентов, преподавателей, администрации к приложениям в гетерогенной среде

Преимущества Blitz Identity Provider

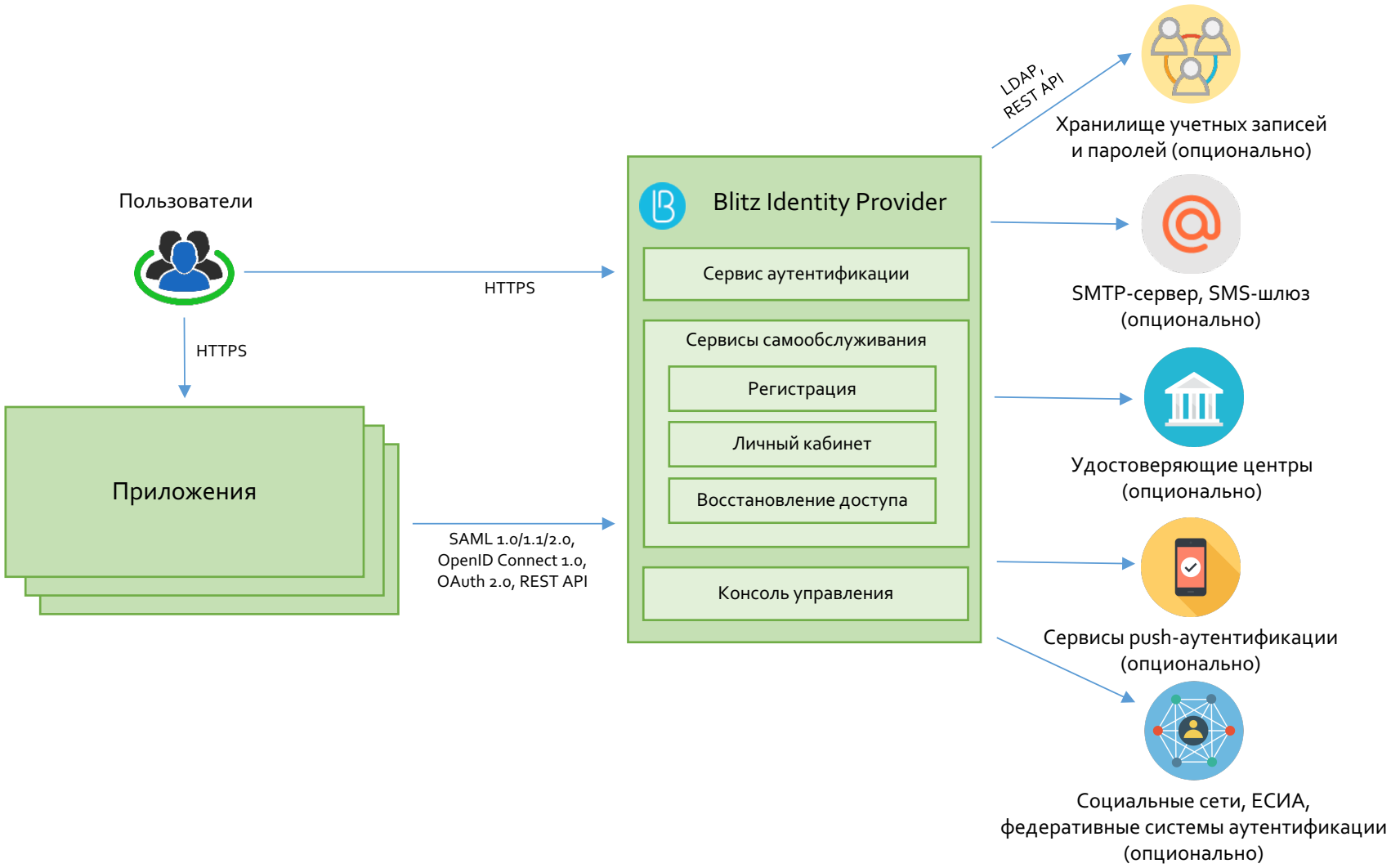
Локализация в РФ

- ✓ Поддерживает все популярные в РФ средства аутентификации и криптопровайдеры
- ✓ Включен в единый реестр российских программ для ЭВМ
- ✓ Поддерживает возможность входа через ЕСИА и через популярные в РФ соцсети
- ✓ Русский язык интерфейса, документации
- ✓ Цена не привязана к курсу доллара

Функциональные

- ✓ Простота настройки через веб-консоль администратора, простота интеграции в существующую ИТ-инфраструктуру (подключение к существующим базам пользователей, поддержка существующих средств аутентификации)
- ✓ Большой выбор доступных методов аутентификации, простая настройка
- ✓ Кроссплатформенность. Серверное ПО работает как в Windows, так и в Linux. Пользователи могут использовать любые устройства доступа (ПК, Apple Mac, планшеты, смартфоны)
- ✓ Возможность объединять установки Blitz Identity Provider в федерацию. Предоставление доступа к приложениям компании сотрудникам контрагентов, заказчиков, госорганов

Схема взаимодействия Blitz Identity Provider



Как устроен Blitz Identity Provider

Веб-приложения

- **Сервис аутентификации**
- **Регистрация пользователя**
- **Личный кабинет**
- **Восстановление доступа**
- **Консоль управления**

Слой «Веб»

Фреймворк Bootstrap

Утилиты

Blitz Smart Card Plugin

Слой «Сервисы»

SAML 2.0
Поставщик идентификации

Simple
Blitz Web Gate

OAuth 2.0 / OpenID Connect 1.0
OIDC поставщик идентификации
OAuth Authorization Endpoint сервис
OAuth Token Endpoint сервис
Сервис проверки маркера безопасности

REST API
поставщик ресурсов (сведений о пользователе)
сервис регистрации пользователя
сервис изменения атрибутов пользователя
сервис редактирования настроек авторизации

Identity Brokering

Social Login

ЕСИА

Федерация с Blitz IDP

Слой «Бизнес-логика»

Java, Scala, play, JS, Blitz BDK

Слой «Серверный кэш»

Memcached

Слой «Хранение»

Хранение событий безопасности и иных данных

MapDB или Couchbase

Хранение учетных записей

LDAP или Внешняя БД

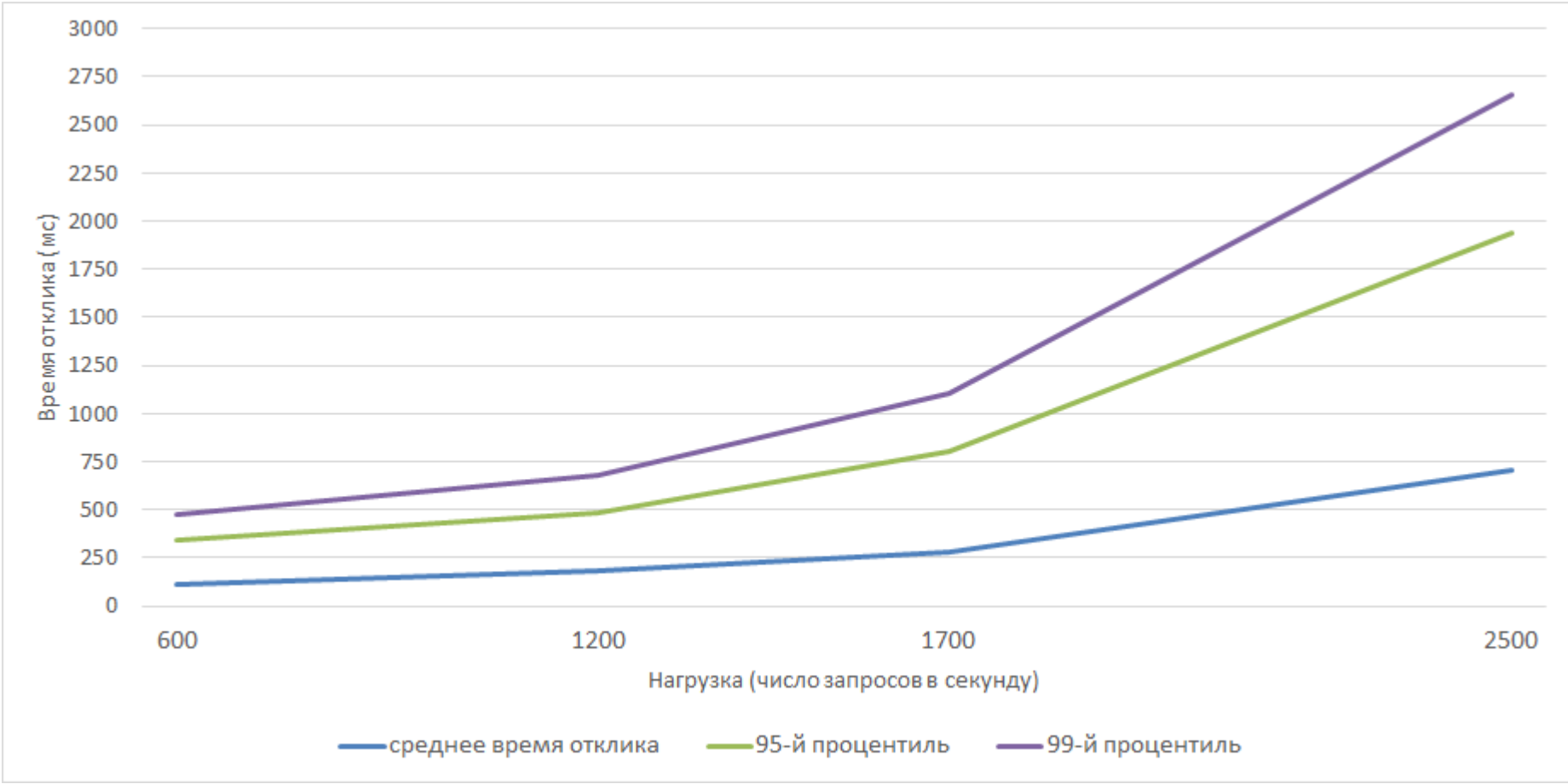
Слой «Объекты»

- **Приложения**
- **Аутентификаторы**
- **Пользователи**
- **Устройства**
- **Атрибуты**
- **Разрешения**
- **События безопасности**

Операционная система

Windows или Linux

Производительность обработки запросов аутентификации



При тестировании Blitz Identity Provider был развернут на 2 серверах конфигурации 2 Core CPU, 2 Gb RAM.
https://identityblitz.ru/products/blitz-identity-provider/performance/

Содержание

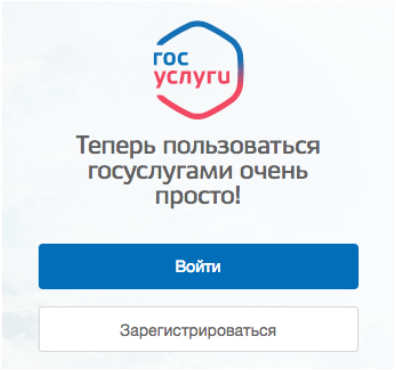
1) Проблема
2) Решение
3) **О компании**

Основные проекты РЕАК СОФТ

2014 – 2015

Развитие и техническая поддержка ПО Единой системы идентификации и аутентификации (https://esia.gosuslugi.ru, ЕСИА)

- 50 млн пользователей
- 1500 подключенных систем
- 20 тыс. центров регистрации
- более 1 млн аутентификаций в сутки



Рыбаков фонд

2016

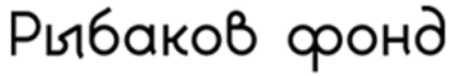
На основе Blitz Identity Provider построена единая система аутентификации UNID RF в Рыбаков Фонде. Используется 10 интернет-проектами фонда для регистрации и аутентификации пользователей

2017

Аутентификация с помощью средства электронной подписи на сайте fedresurs.ru во всех популярных браузерах и ОС

интерфакс
INTERFAX

Компании, которые используют ПО РЕАК СОФТ



Партнёры РЕАК СОФТ

AT Consulting

РТ ЛАБС

ПРОГРЕСС

ИНФОТЕКС ТРАСТ

AXOFT

Эшелон
комплексная безопасность

taskdata
Заставьте данные работать на Вас

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

ТНБ NST
Технологии Национальной Безопасности

REDSYS

Что дальше

1. Загрузите пробную версию Blitz Identity Provider
   https://identityblitz.ru/products/blitz-identity-provider/download/
2. Ознакомьтесь с документацией Blitz Identity Provider и видеороликами:

   https://identityblitz.ru/products/blitz-identity-provider/documentation/

   https://www.youtube.com/channel/UCArUq-fI73Ebn33NKxeVgzg
3. Свяжитесь с нами, мы с удовольствием ответим на ваши вопросы.

https://identityblitz.ru