



SCS SBERBANK
CYBER
SECURITY



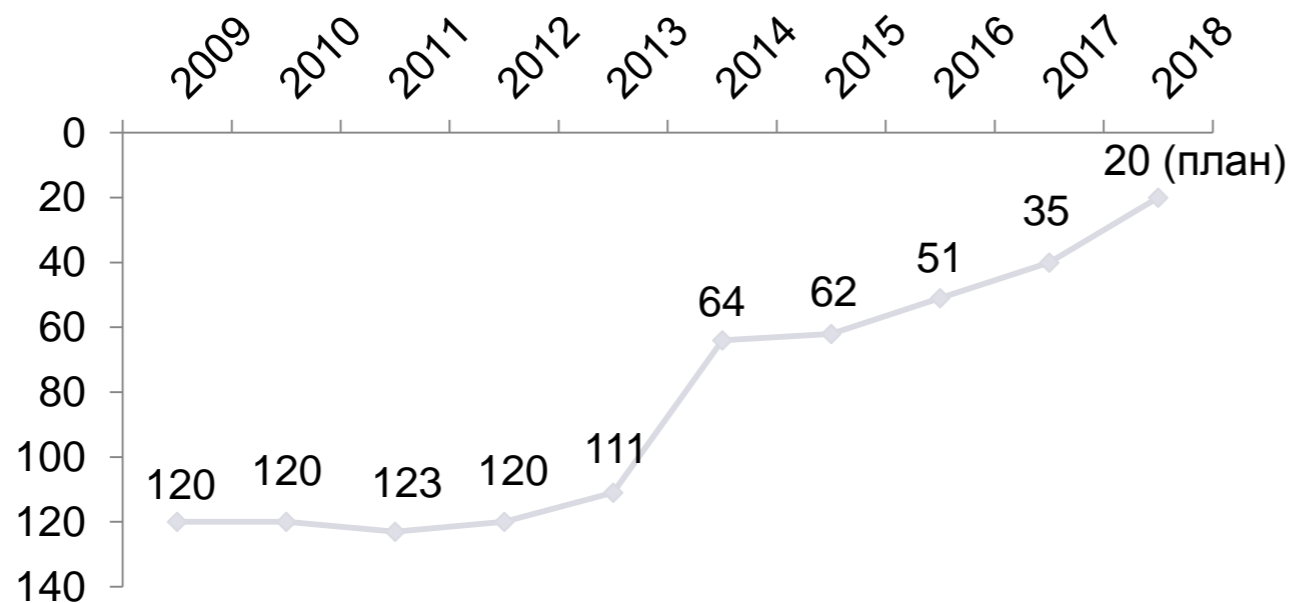
**Практика применения средств
электронной подписи в
проекте по дистанционной
регистрации бизнеса и
открытию счетов по
ПП№1104 от 29.10.2016**



"Предлагаю запустить масштабную программу развития экономики нового технологического направления, так называемой цифровой экономики. В ее реализации будем опираться именно на российские компании, на исследовательские и инжиниринговые центры страны. Это вопрос национальной безопасности и технологической независимости страны»

(Послание В.В. Путина Федеральному собранию, 2016)

Россия в Рейтинге

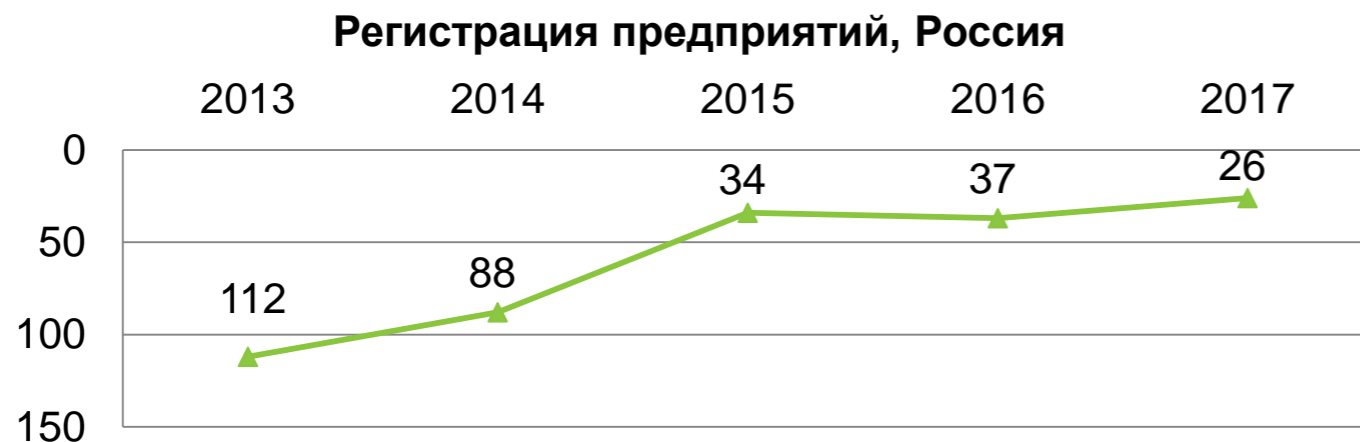


Майскими указами 2012 года президент РФ Владимир Путин поставил задачу достижения 20-й строчки рейтинга Doing Business к 2018 году.

Рейтинг составляется на основании 10 индикаторов регулирования предпринимательской деятельности:

1. Регистрация предприятий
2. Получение разрешений на строительство
3. Подключение к системе электроснабжения
4. Регистрация собственности
5. Кредитование
6. Защита инвесторов
7. Налогообложение
8. Международная торговля
9. Обеспечение исполнения контрактов
10. Ликвидация предприятий

По показателю «регистрация предприятий» к 2017 г. Россия должна занять 26 место. Необходимо скорейшее дальнейшее улучшение данного индикатора для достижения запланированного суммарного показателя к 2018 г.



~ 60% стартапов в мире открываются с участием российских инвесторов. Из них только 3 тыс. в России (0,5%).
Прежде всего это связано со сложной регистрацией бизнеса, открытием счетов и трудностях при ведении платежной международной деятельности в России

Один из важнейших критериев – возможность выполнить все online, без физического визита

Цель эксперимента: обеспечение дистанционного направления электронных документов для государственной регистрации юридических лиц и индивидуальных предпринимателей, а также открытие им счетов в кредитных организациях

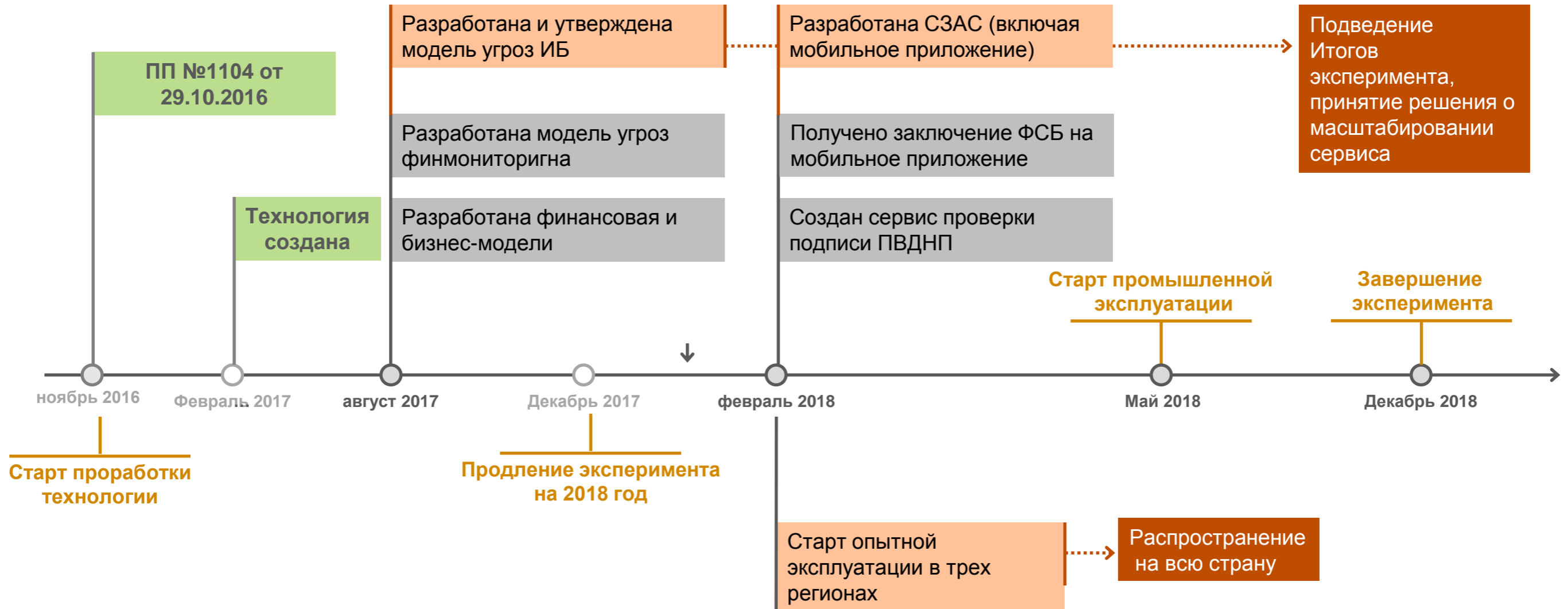
Реализуется с помощью:

Специализированной защищенной автоматизированной системы (СЗАС), предназначенной для **централизованного создания и хранения ключей усиленной квалифицированной электронной подписи**, а также их **дистанционного** применения владельцами квалифицированных сертификатов ключа проверки электронной подписи

Задачи перед участниками эксперимента:

- Разработать модель угроз информационной безопасности СЗАС (Сбербанк, ВТБ);
- Разработать финансовую модель и бизнес-модели направления ЭД для государственной регистрации ЮЛ и ИП и открытия им счетов в кредитных организациях посредством использования СЗАС (Сбербанк, ВТБ);
- На основе модели угроз информационной безопасности разработать и утвердить временные (на период эксперимента) требования к СЗАС (ФСБ России);
- Создать автоматизированную систему в соответствии с временными требованиями, утвержденными ФСБ РФ (Сбербанк, ВТБ);
- Обеспечить эксплуатацию СЗАС в соответствии с законодательством РФ и временными требованиями, утвержденными ФСБ РФ (Сбербанк, ВТБ);
- Провести оценку результатов эксперимента и представить соответствующий доклад в Правительство Российской Федерации с необходимыми предложениями (Минкомсвязи совместно с другими ведомствами, Сбербанком и ВТБ).

» Дорожная карта эксперимента по ПП №1104 (проект РБидОС)



Разработка Модели угроз и требований ФСБ к СЗАС:

- Разработана Модель угроз для СЗАС
- На основании Модели угроз ФСБ разработаны Временные требования к СЗАС

Разработка технологии:

- Компанией Инфотекс создано криптографическое мобильное приложение (программный компонент клиента) для формирования КЭП и аутентификации клиента по протоколу NFC по загранпаспорту с чипом.
- Компанией ФГБУ НИИ Восход создан сервис по проверке электронной подписи под блоком данных, считанных с чипа загранпаспорта

Оценка соответствия компонент СЗАС:

- Проведены сертификационные исследования мобильного приложения, получено положительное заключение ФСБ
- Сформирована разработчиками и специализированными испытательными организациями декларация соответствия СЗАС Временным требованиям ФСБ (на период опытной эксплуатации)

Запуск эксплуатации технологии

- Принято решение о продлении эксперимента на 2018 год
- Получено разрешение ФСБ на проведение опытной эксплуатации СЗАС с 15.02.2018 на трех регионах
- Планируется начать с конца мая промышленную эксплуатацию СЗАС во всех регионах Российской Федерации



Регистрация ИП

Регистрация ООО

Вопрос-Ответ

Обратная связь

Зарегистрируйте ваш бизнес и откройте счет в ПАО Сбербанк онлайн

Заполнение документов на регистрацию бизнеса и открытие расчетного
счета занимает в среднем 25 минут

Открыть ИП

Открыть ООО



Наши партнеры объединились, чтобы вам было проще начать бизнес

Что для этого нужно?



Чтобы отправить эту заявку вам должно быть от 19 лет.



Вы должны быть клиентом ПАО Сбербанк.



Паспорт гражданина РФ.



Биометрический загранпаспорт, выпущенный не ранее 2009.



Android-смартфон версии 5.0 или выше с функцией NFC

[Модели с NFC](#) ↗



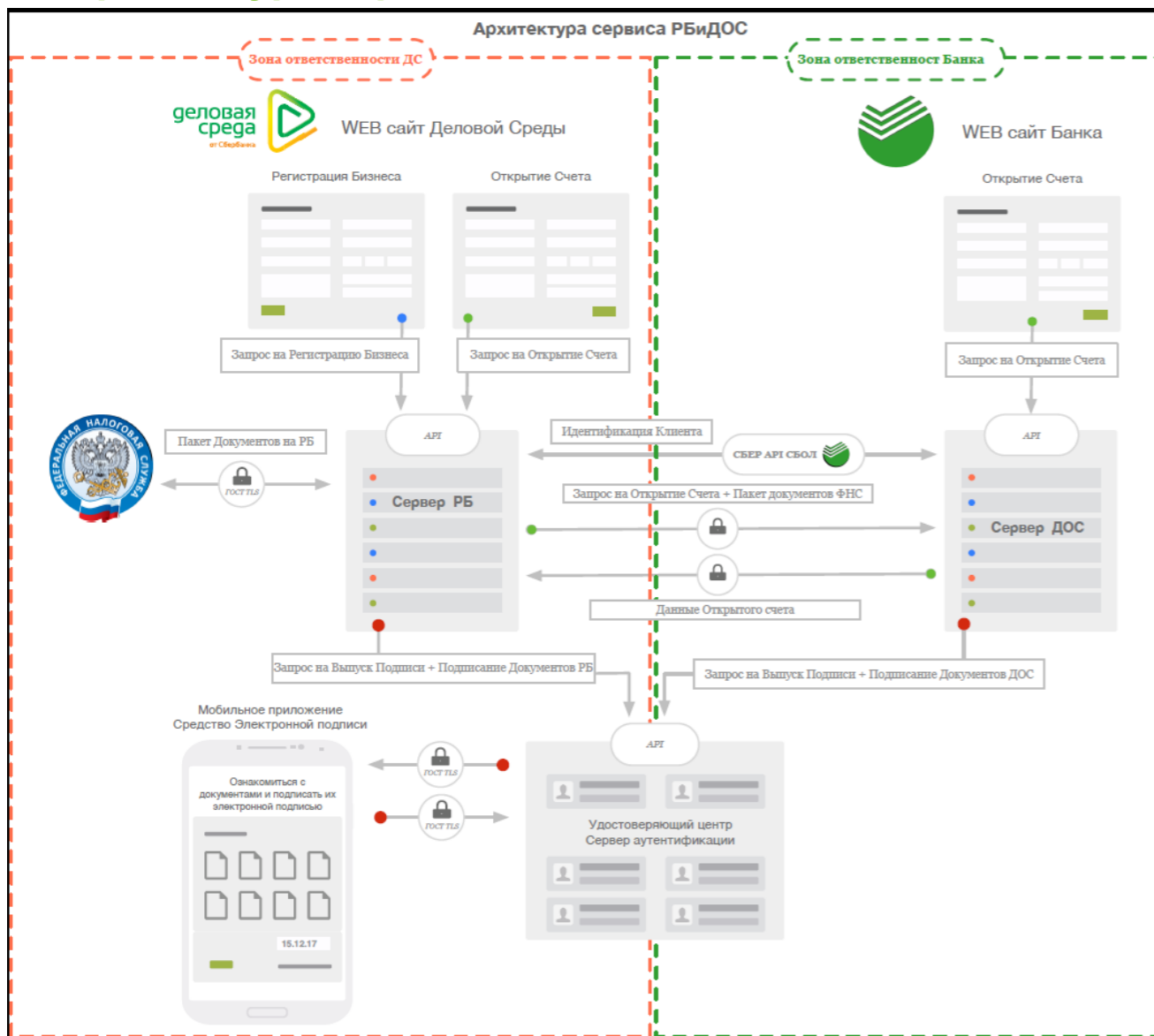
СНИЛС.

Регистрация ИП или ООО с одним учредителем



- + не требуется личный визит в Банк и Федеральную Налоговую Службу
- + электронная подпись без ключевого носителя, хранится в памяти смартфона
- + сервис бесплатен для Клиента при условии открытия счета в ПАО Сбербанк
- + специальный тариф «Легкий старт» без ежемесячной абонентской платы

Архитектура сервиса РБидОС и основные шаги клиента



Как это работает ?

- Шаг 1**
Выберите форму регистрации
- Шаг 2**
Введите и подтвердите персональные данные
- Шаг 3**
Заполните формы на регистрацию бизнеса и открытие счета
- Шаг 4**
Оплатите государственную пошлину онлайн
- Шаг 5**
Получите электронную подпись и подпишите документы, установив мобильное приложение
- Поздравляем! Ваш бизнес зарегистрирован и открыт счет в ПАО Сбербанк



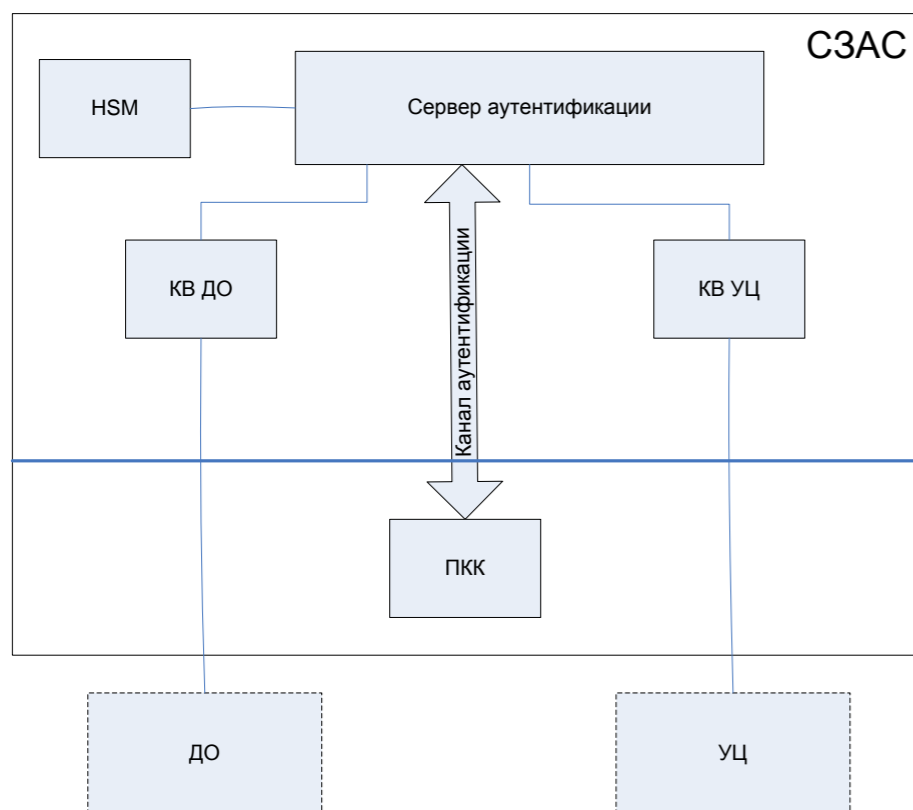
Структура СЗАС

Состав СЗАС

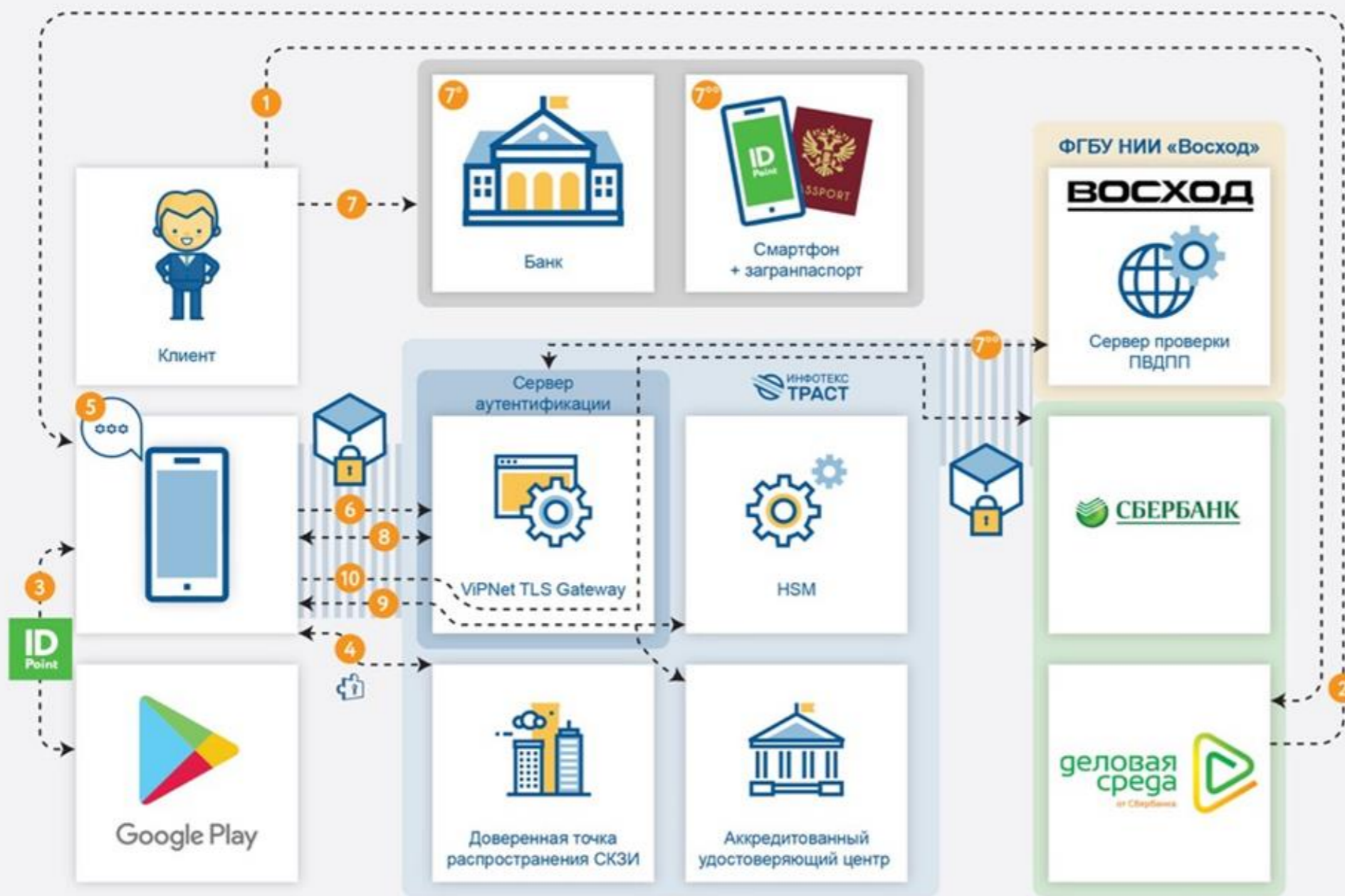
- КВ УЦ - Компонент взаимодействия с УЦ
- КВ ДО - Компонент взаимодействия с системами дистанционного обслуживания (ДО)
- СА - Сервер аутентификации
- ПКК – Программный компонент клиента (мобильное приложение)
- РБидОС это система дистанционной регистрации бизнеса и открытия счетов

Функции компонент схемы

- Клиент через систему ДО направляет запросы на регистрацию бизнеса и открытие счетов. Кроме того, система ДО взаимодействует с ФНС для регистрации ЮЛ и ИП и АС Банка для открытия счетов
- Подпись клиента хранится в ПКК в зашифрованном виде, ее активация производится с ПКК через канал аутентификации
- На аппаратном модуле HSM хранятся ключи шифрования, на которых зашифрованы ключи подписи клиента. Ключи шифрования защищены паролем.



» Схема работы клиента с СЗАС



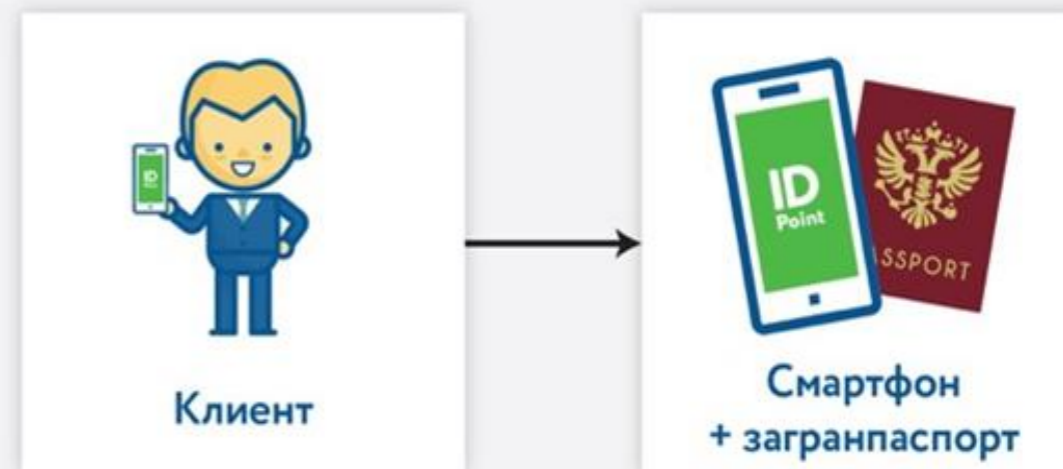
- 1 Ввод необходимых данных на сайте «Деловой среды»
- 2 СМС-сообщение со ссылкой на скачивание приложения и идентификацию клиента
- 3 Скачивание приложения IdPoint
- 4 Догрузка криптобиблиотеки, контроль целостности, учет СКЗИ
- 5 Формирование стойкого пароля
- 6 Установление одностороннего TLS, генерация запроса на клиентский TLS-сертификат
- 7 Аутентификация (7° – очная / 7°° – ПВДНП), выпуск TLS-сертификата
- 8 Установление двухстороннего TLS-канала
- 9 Формирование запроса и выпуск сертификата КЭП клиента
- 10 Подпись документов КЭП клиента

Очная верификация клиента



- 1 Установка приложения, формирование ключей и запросов
- 2 Личный визит в банк
- 3 Верификация личности сотрудником банка и подтверждение корректности запроса на сертификат ЭП
- 4 Создание сертификата аутентификации
- 5 Создание квалифицированного сертификата

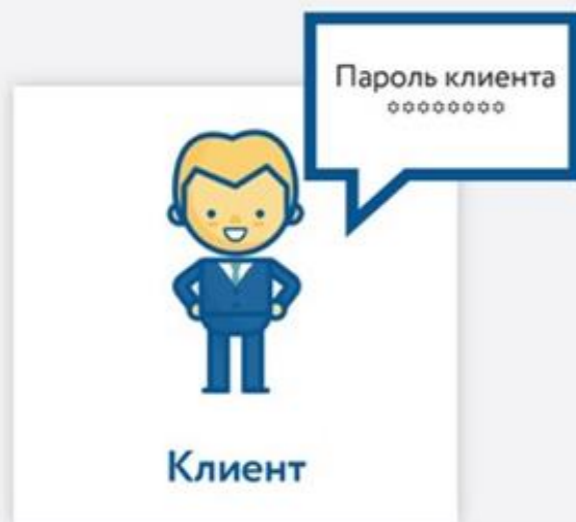
Удаленная верификация клиента



- 1 Установка приложения, формирование ключей и запросов
- 2 Считывание информации заграничного паспорта с помощью смартфона
- 3 Проверка данных клиента
- 4 Создание сертификата аутентификации
- 5 Создание квалифицированного сертификата

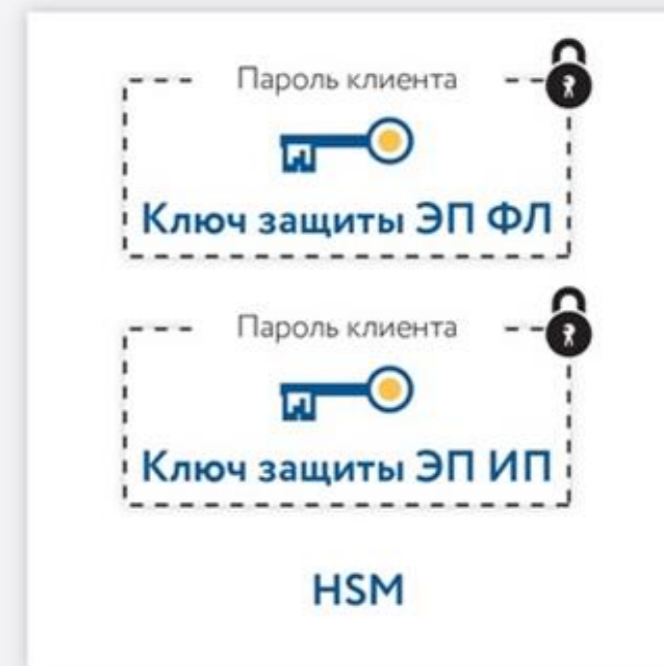
»» Временные требования к СЗАС: защита ключей

Не допускается хранение ключей ЭП и ключей аутентификации без их предварительного шифрования (которое должно осуществляться встроенной функцией ПКК). При этом должно быть реализовано:

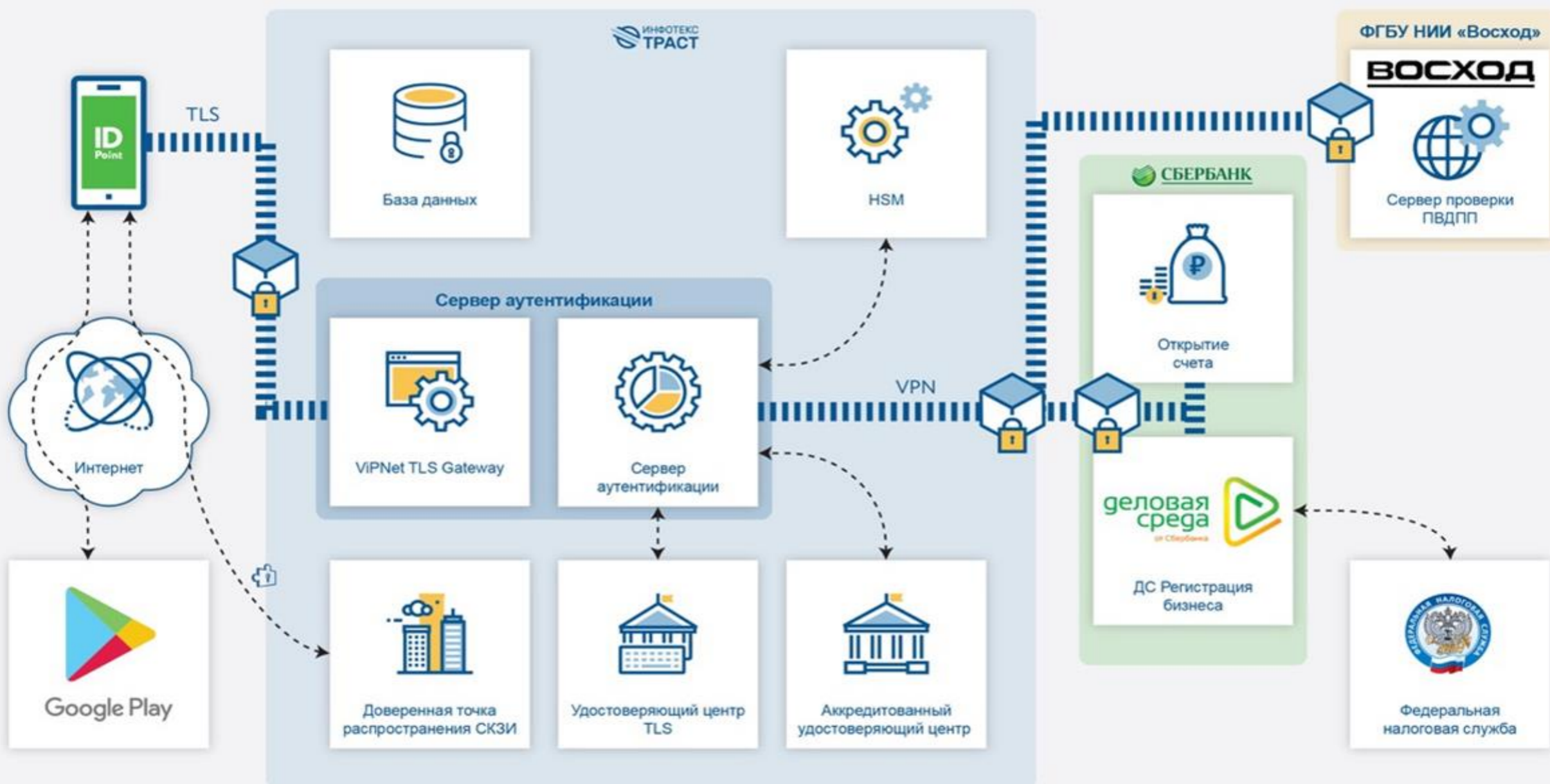


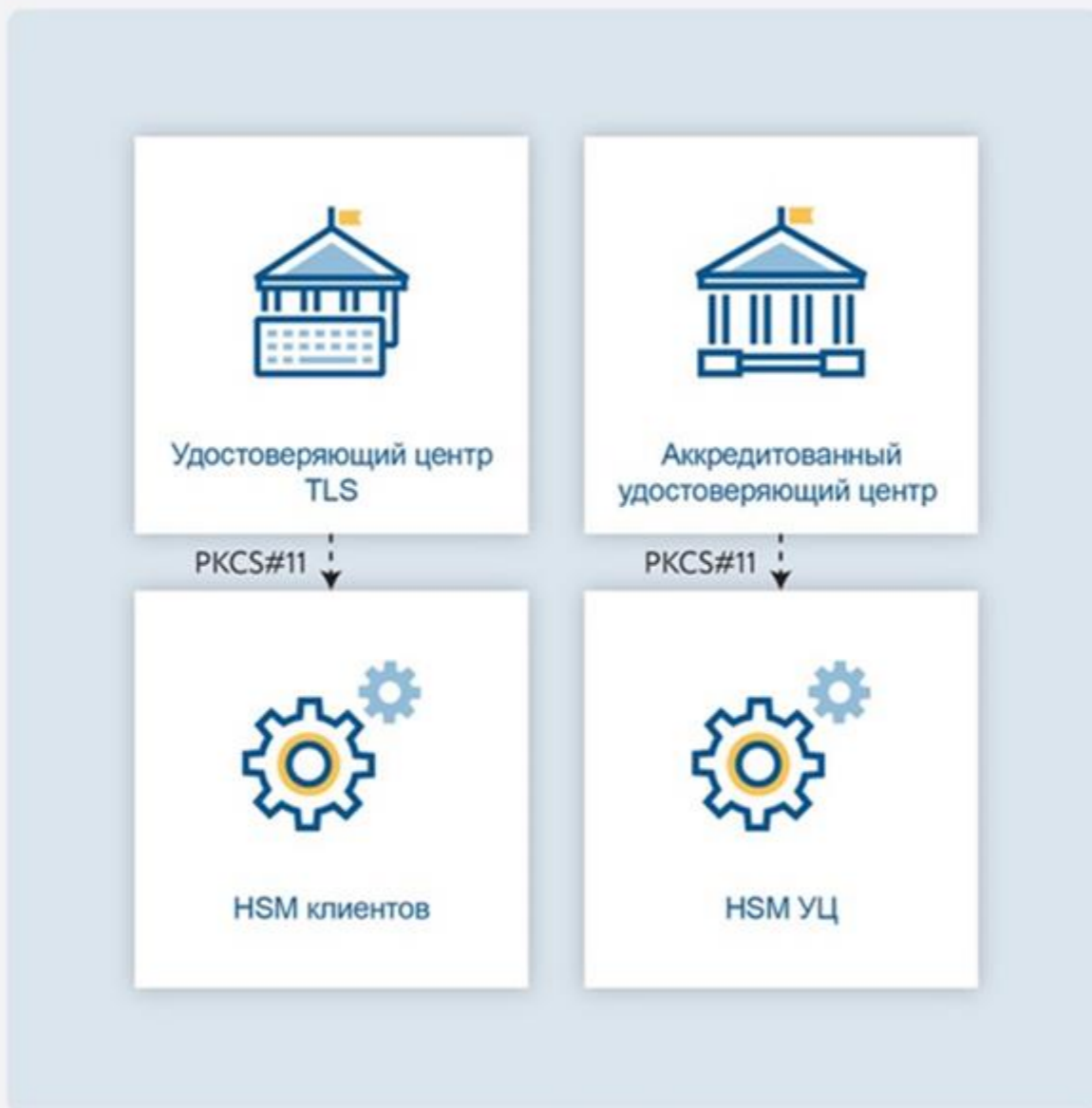
Мобильное приложение

- ❑ Шифрование ключа ЭП на ключе защиты посредством применения алгоритма шифрования в соответствии с ГОСТ 28147-89;
- ❑ Хранение зашифрованного на пароле ключа защиты ключа ЭП в HSM.



»» Схема серверных компонентов СЗАС





Средства удостоверяющего центра:

- ✓ ViPNet Удостоверяющий центр, сертификат соответствия № СФ/128-2932 (УЦ), класс КСЗ
- ✓ хранение ключей Удостоверяющего центра в ViPNet HSM
- ✓ поддержка алгоритмов ГОСТ Р 34.10-2001/2012
- ✓ поддержка политик разграничения доступа

Временные требования:

- ✓ Ключи ЭП, используемые для подписи квалифицированных сертификатов и списков уникальных номеров квалифицированных сертификатов, действие которых на определенный момент было прекращено УЦ до истечения срока их действия, должны создаваться и храниться посредством ПАКМ HSM УЦ в зашифрованном на ключе защиты, формируемом по схеме разделения секрета 3 из 5, виде.
- ✓ Ключ ЭП, используемый для подписания сертификатов открытых ключей аутентификации, в УЦ должен создаваться и храниться посредством ПАКМ HSM клиентов в зашифрованном на ключе защиты, формируемом по схеме секрета 3 из 5, виде.



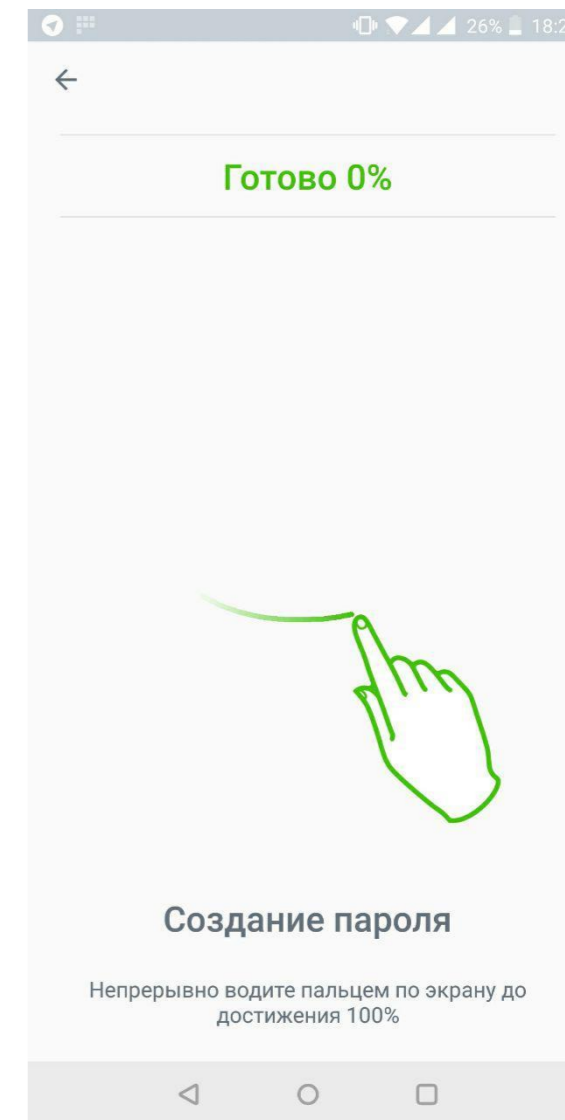
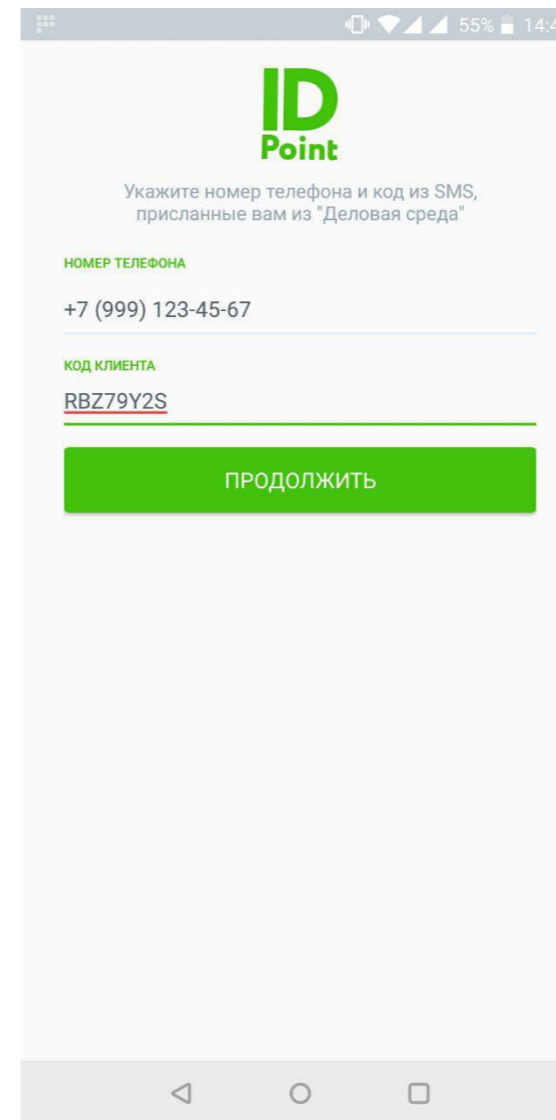
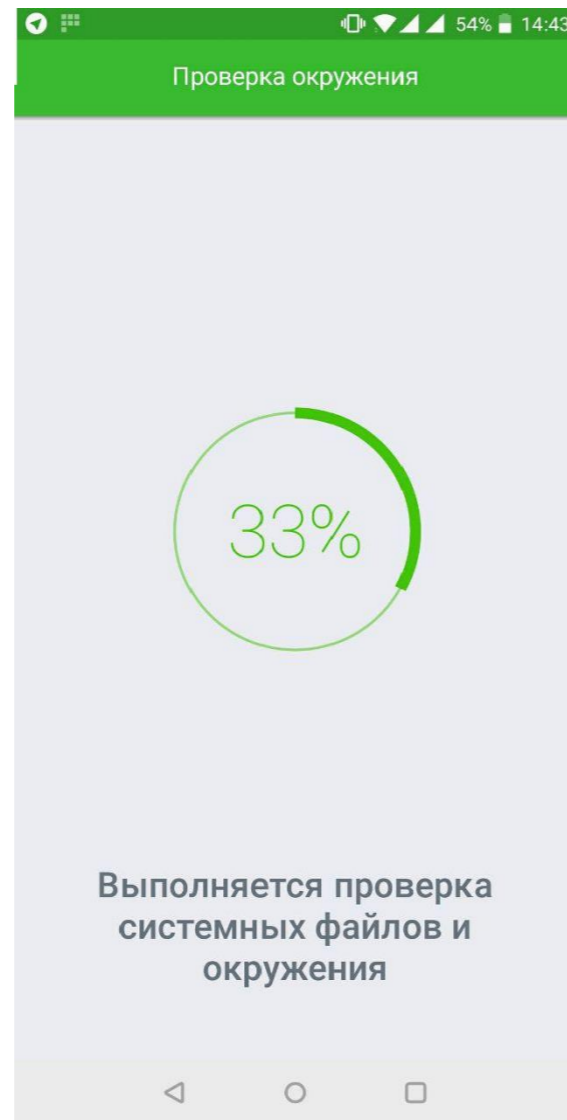
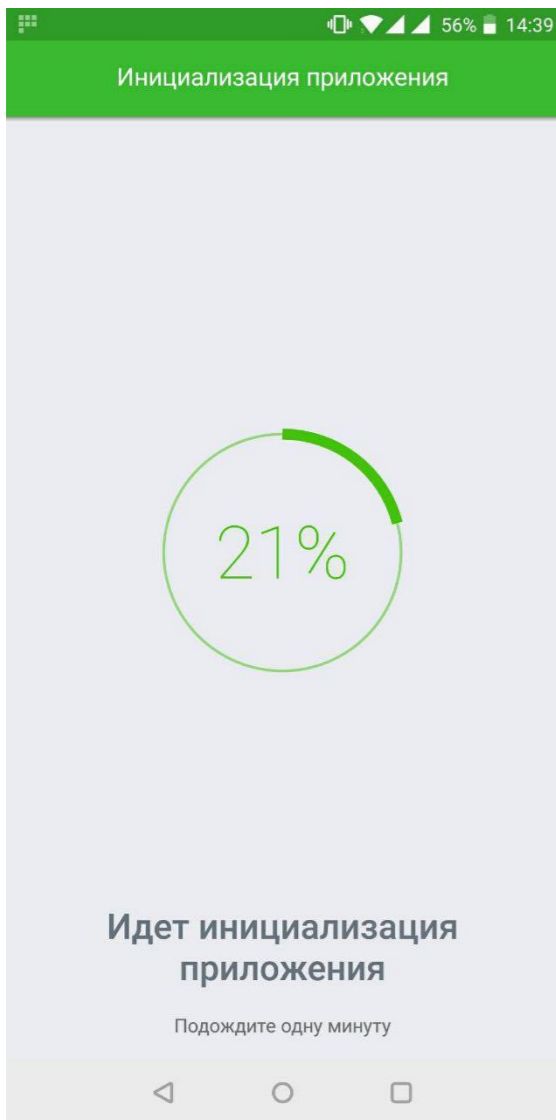
ПАК ViPNet Coordinator KB:

- ✓ СКЗИ класса KB2
- ✓ МСЭ 4 класса по требованиям ФСБ

Временные требования:

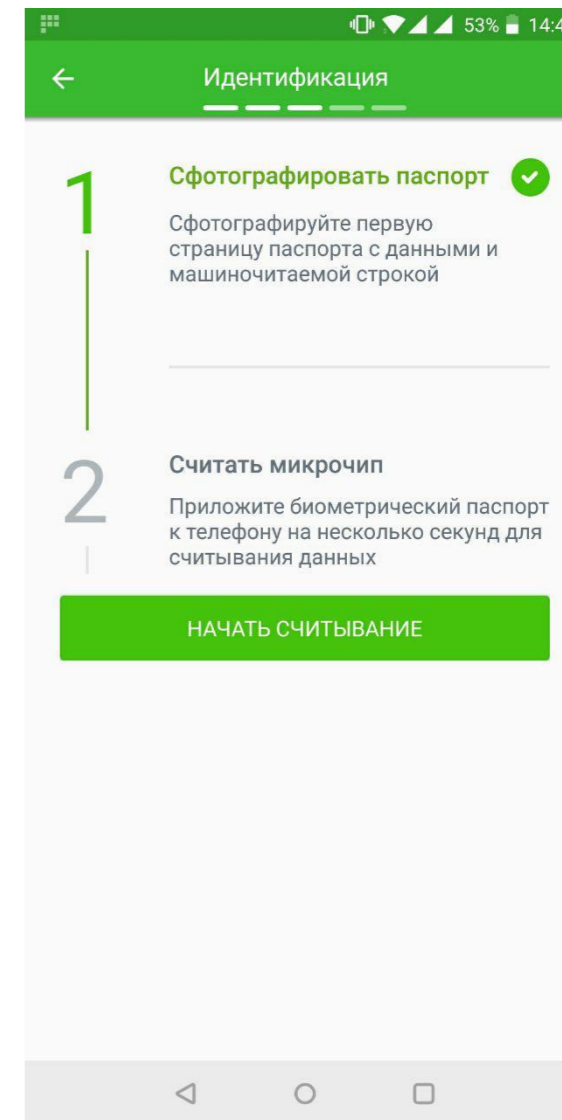
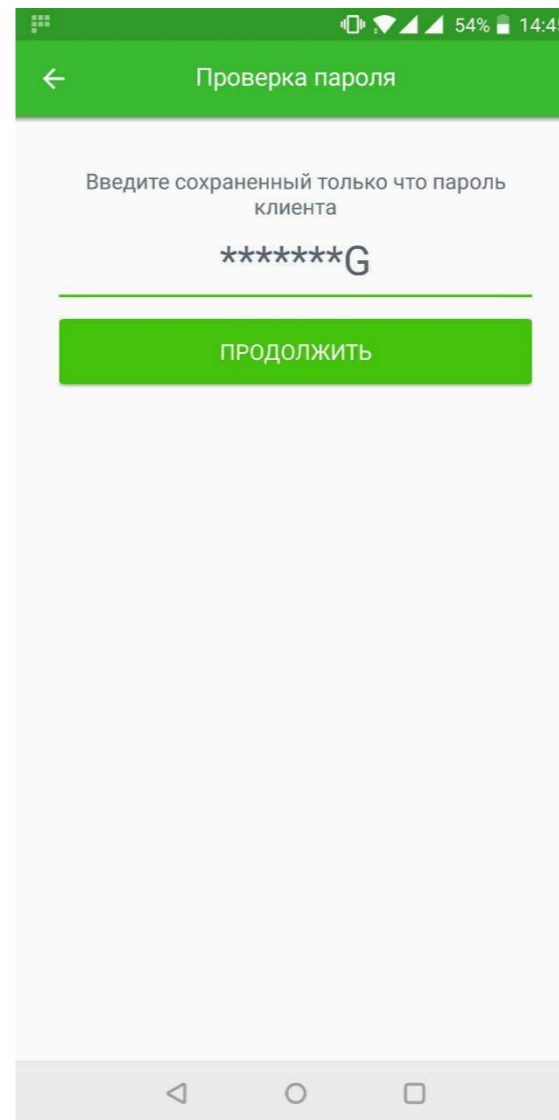
- ✓ При организации сетевого взаимодействия СК СЗАС между собой в случае их размещения в разных контролируемых зонах, каналы связи (сети связи) между этими компонентами должны быть защищены с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже KB, либо быть выделенными в соответствии с Федеральным законом от 07.07.2003 № 126-ФЗ «О связи».

- ✓ Для ограничения возможностей по построению каналов атак на СА, сервер БД, сервер передачи электронных документов участников эксперимента, сервер проверки электронной подписи и ДТР ПКК (далее – серверные компоненты СЗАС, СК СЗАС) с использованием каналов связи должны применяться межсетевые экраны уровня веб-сервера (тип «Г»), сертифицированные на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. № 9, по 1, 2, 3 или 4 классу защиты.
- ✓ Для обеспечения обнаружения компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации должны применяться средства антивирусной защиты, сертифицированные на соответствие Требованиям к средствам антивирусной защиты, утвержденным приказом ФСТЭК России от 20 марта 2012 г. № 28, по 1, 2, 3 или 4 классу защиты.
- ✓ Для обнаружения вторжений, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на средства защиты информации и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также для реагирования на эти действия (предотвращение этих действий) должны применяться системы обнаружения вторжений, сертифицированные на соответствие Требованиям к системам обнаружения вторжений, утвержденным приказом ФСТЭК России от 6 декабря 2011 г. № 638, по 1, 2, 3 или 4 классу защиты.



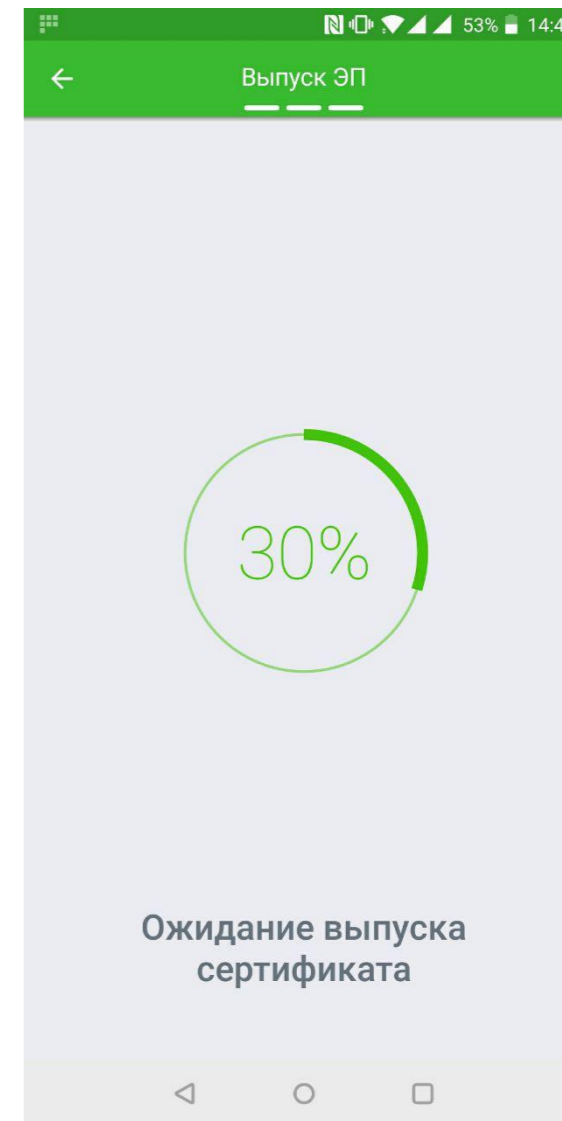
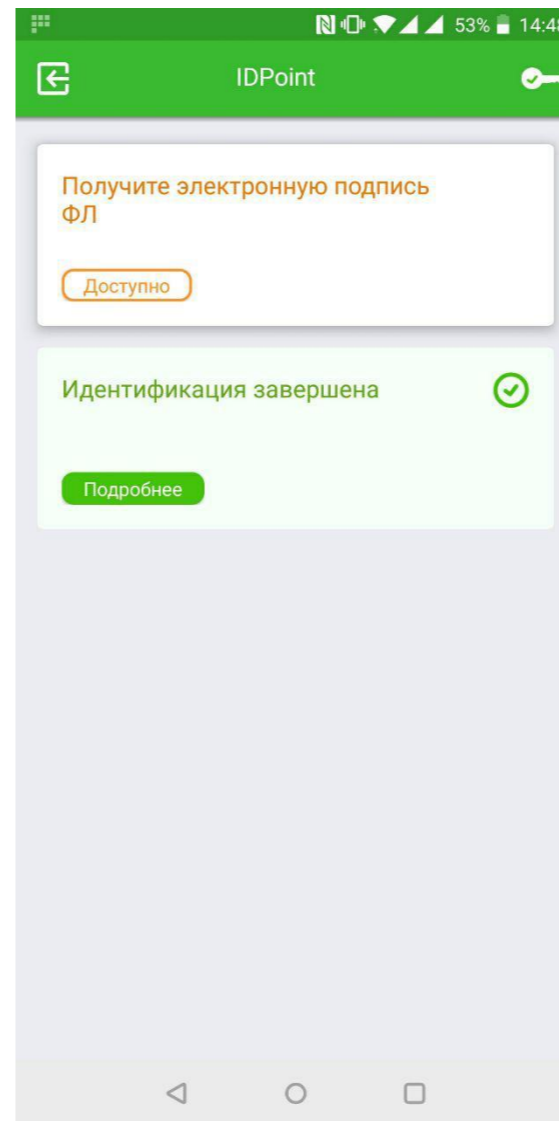
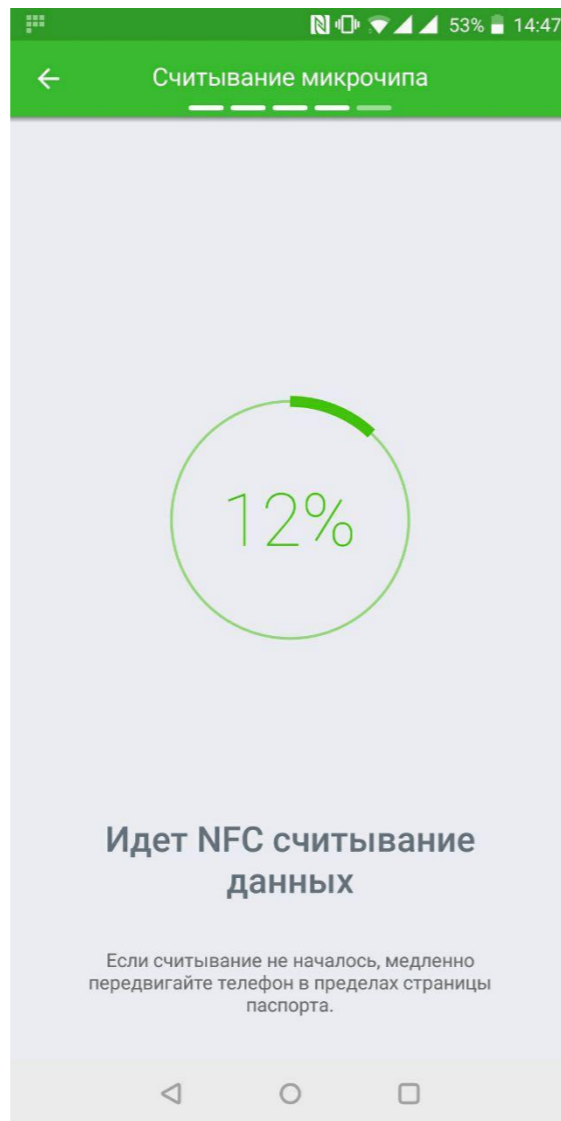
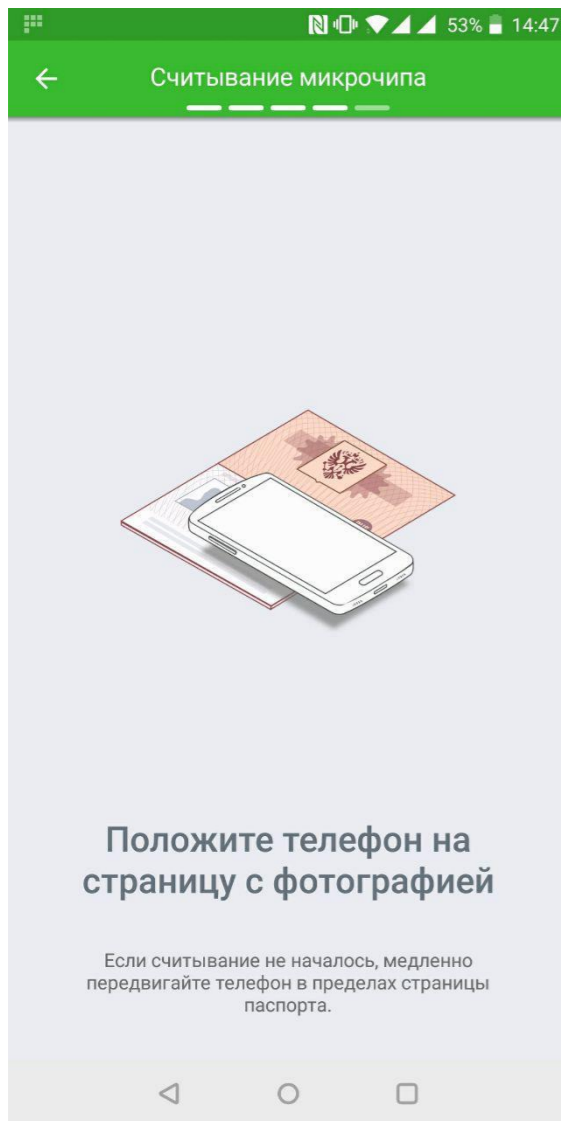


Мобильное приложение в РБидОС. Формирование пароля к ключам клиента





Мобильное приложение в РБидОС. Завершение идентификации с помощью ПВДНП.





Мобильное приложение в РБидОС. Выпуск сертификата и подпись заявления на регистрацию бизнеса.



Данные сертификата

Версия
3

Серийный номер
01 d3 9f 40 75 93 2f e0 00 00 21 29 10 ef 00 02

Имя издателя
O=Открытое Акционерное Общество "ИнфоТекС Интернет Трест"
STREET=Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
C=RU
E=SupportIT@infotecs.ru
CN=ОАО "ИИТ"
INN=007743020560
OGRN=1027739113049
S=77 г. Москва
L=Москва

Период действия

Не ранее
06.02.2018 14:48

Не позднее

С данными ознакомлен

ПРОДОЛЖИТЬ

IDPoint

Зарегистрируйте бизнес

Доступно

Подпись ФЛ получена ✓

Подробнее

Идентификация завершена ✓

Подробнее

Документы на подпись

60%

Загрузка документов

Документы на подпись

Дата документа: 07.11.2017
ФИО Индивидуального предпринимателя: ИВАНОВ ИВАН ИВАНОВИЧ
Дата рождения: 12.03.1991
Место рождения: МОСКВА
Адрес места проживания: 141308, Р-Н СЕРГИЕВО-ПОСАДСКИЙ, 50 СЕРГИЕВ ПОСАД, УЛ 1-Я ЛЕСНАЯ, ДОМ 1, КОРПУС 16, КВАРТИРА 58
Удостоверение личности: 45 11 069181, выдан: ОВД ПВО

Заявление.xml

Заявление
в государственной регистрации физического лица
в качестве индивидуального предпринимателя

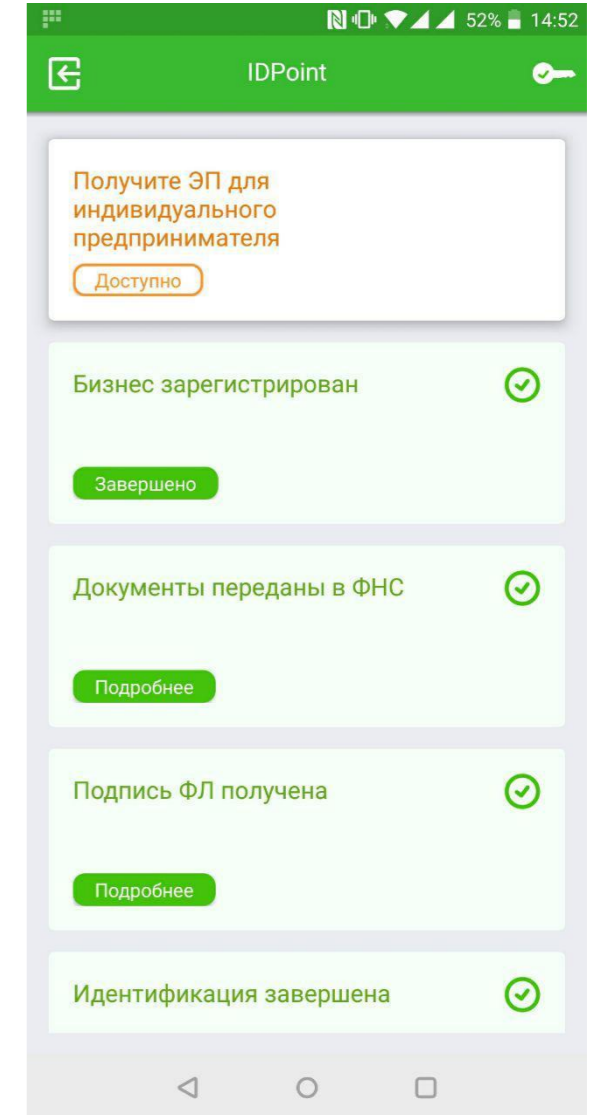
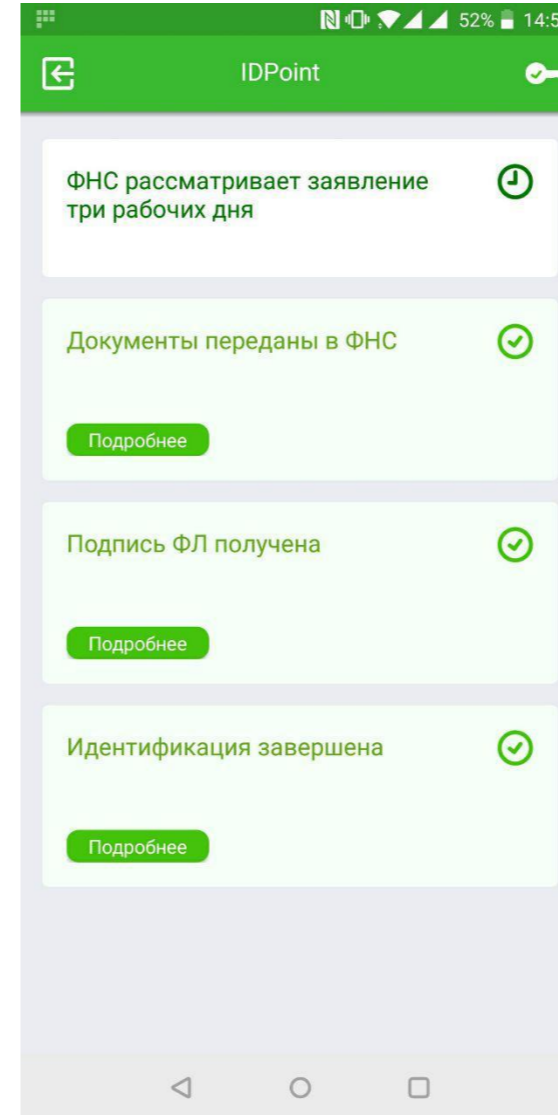
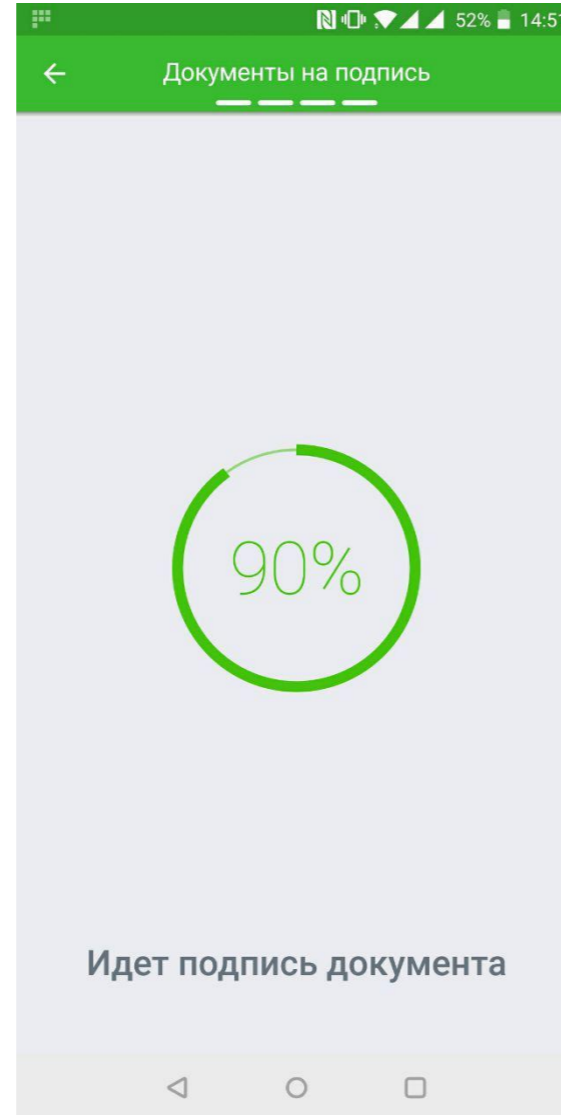
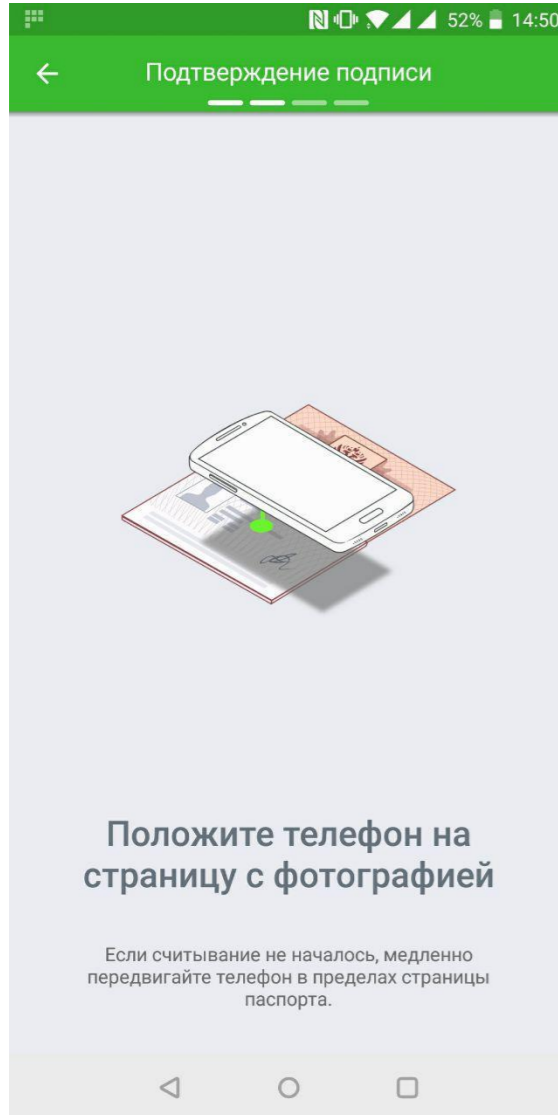
1. Фамилия, имя, отчество физического лица
1.1. Имя россиянина
1.1.1 Фамилия **Иванов**

Заявление на регистрацию.tif

ПОДПИСАТЬ

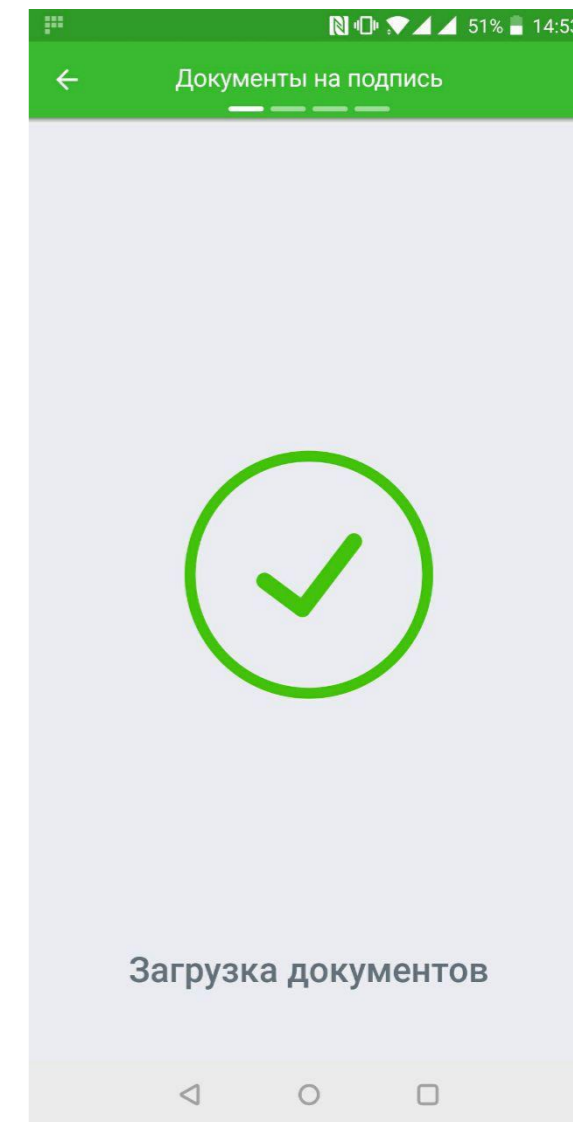
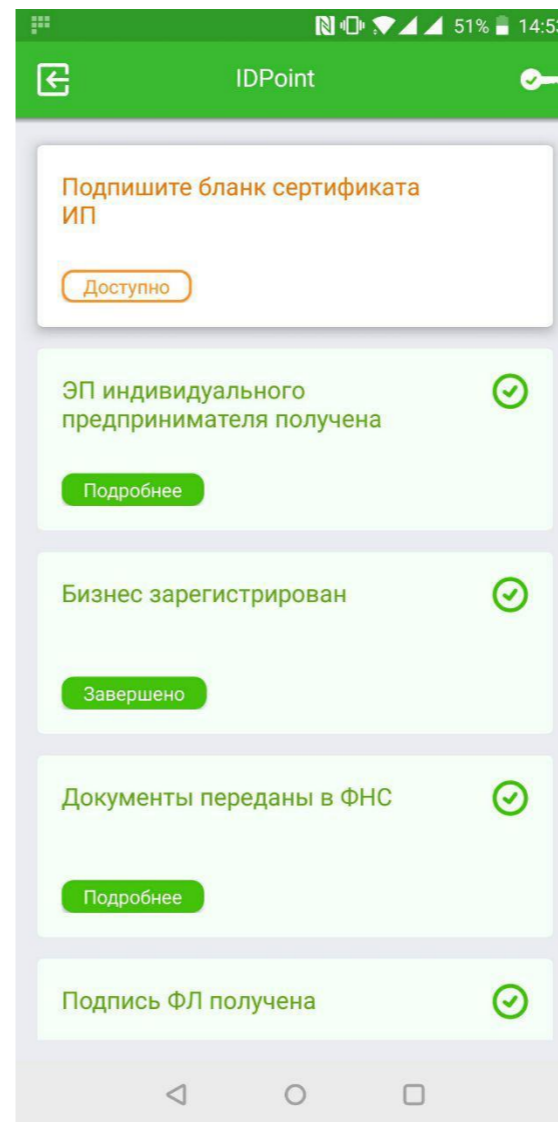
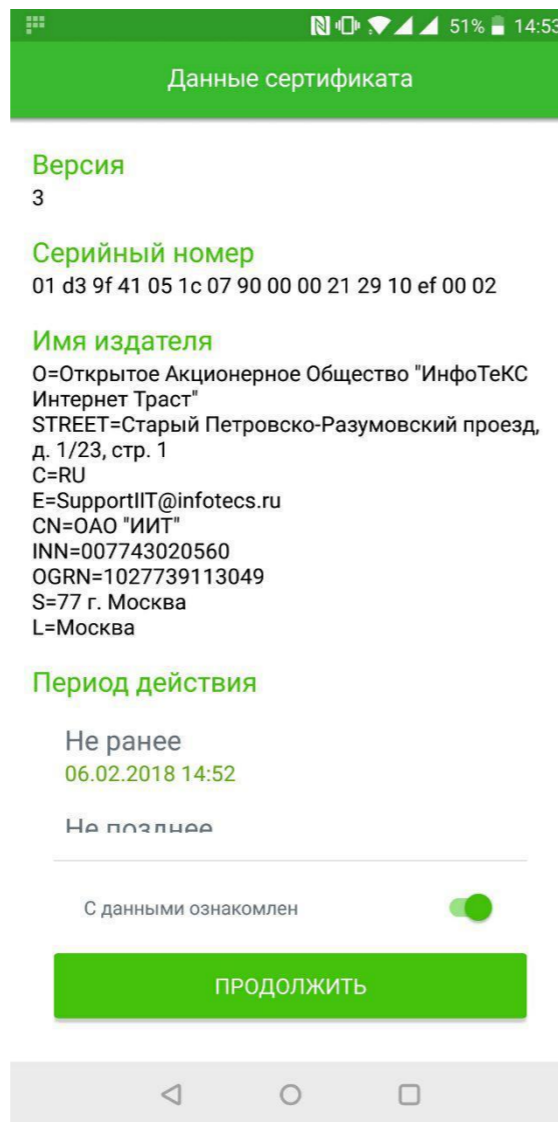
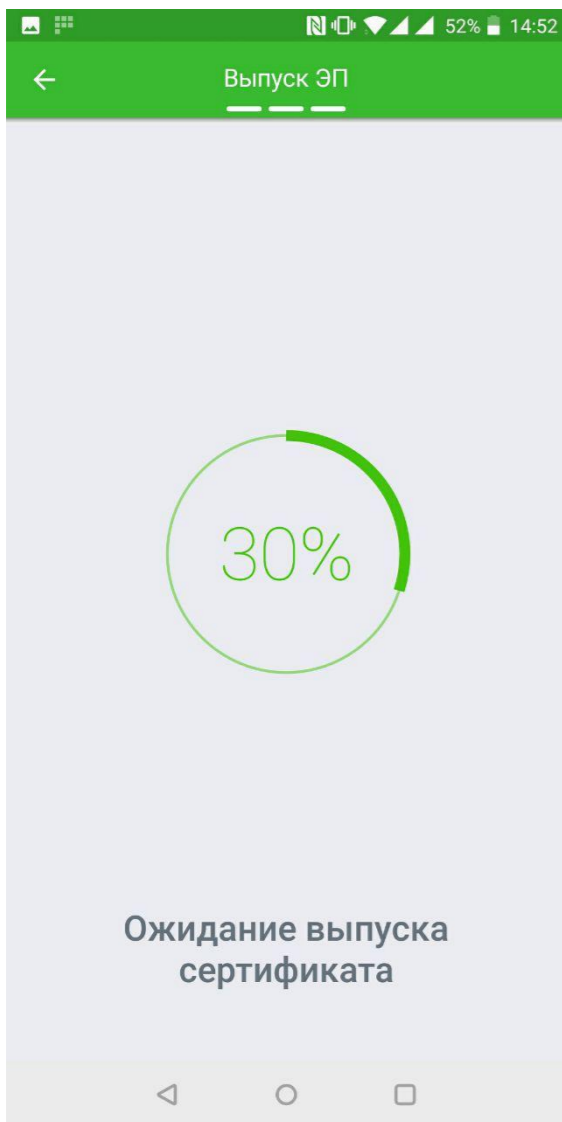


Мобильное приложение в РБидОС. Подтверждение подписи заявления на регистрацию бизнеса в ФНС с помощью ПВДНП.



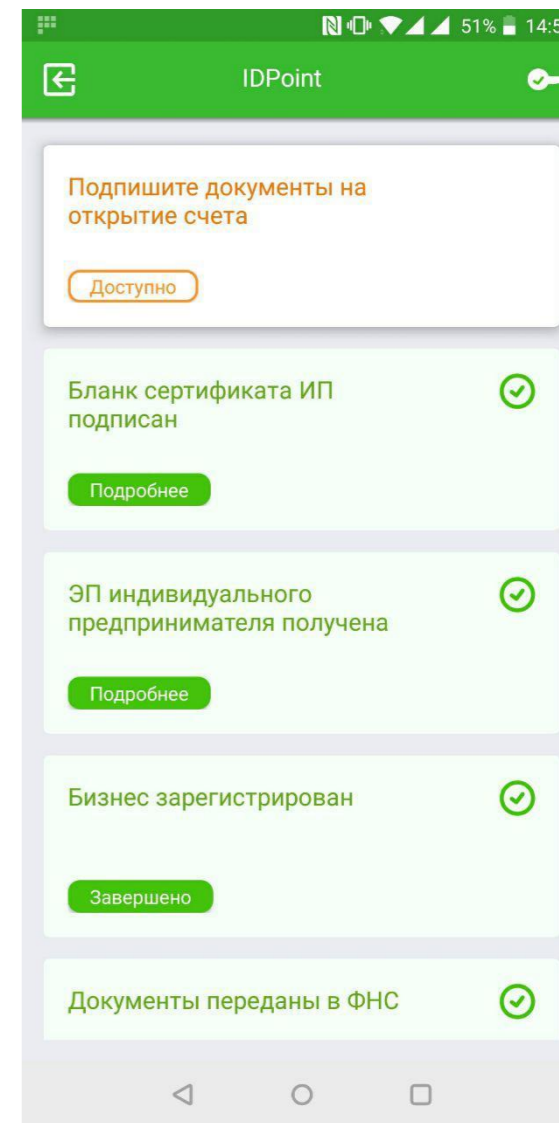
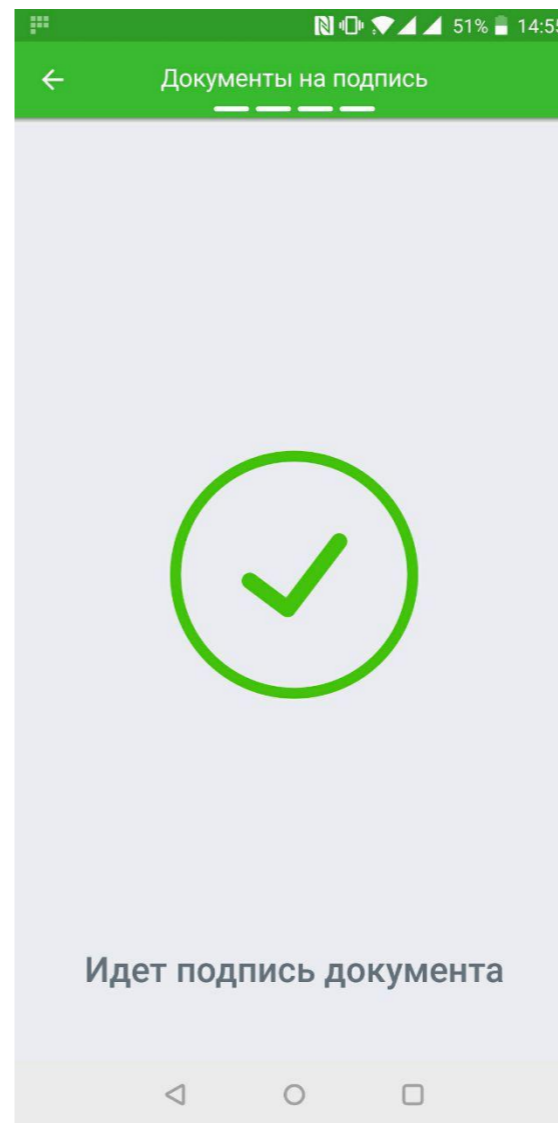
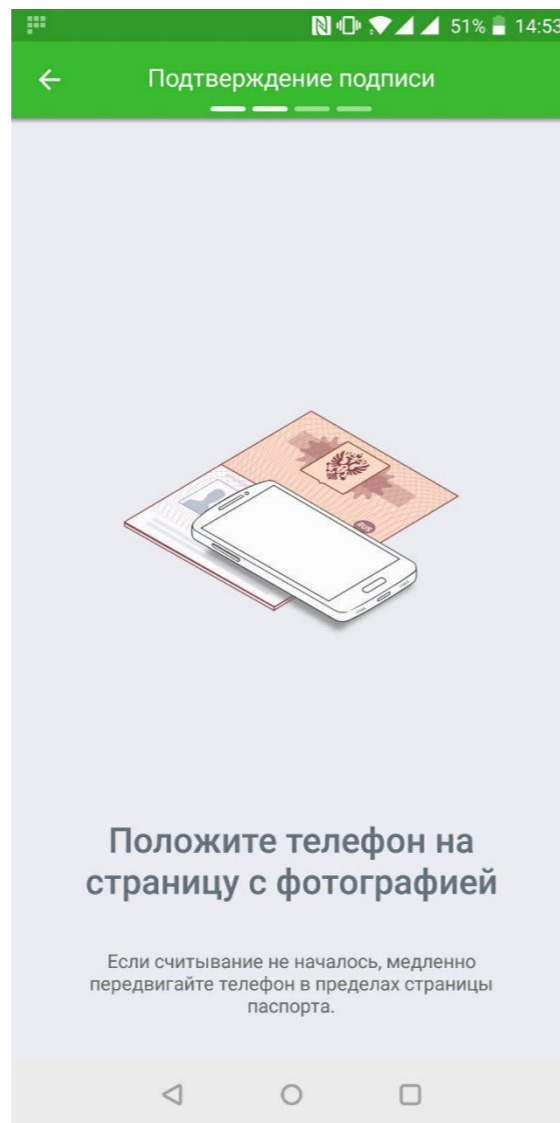


Мобильное приложение в РБидОС. Формирование сертификата Индивидуального предпринимателя.



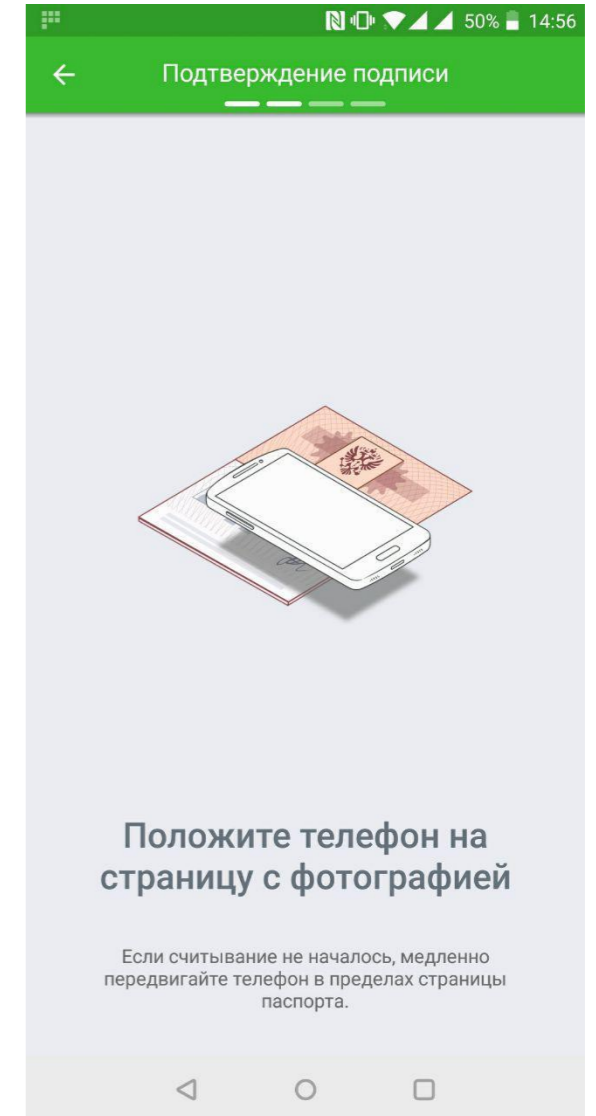
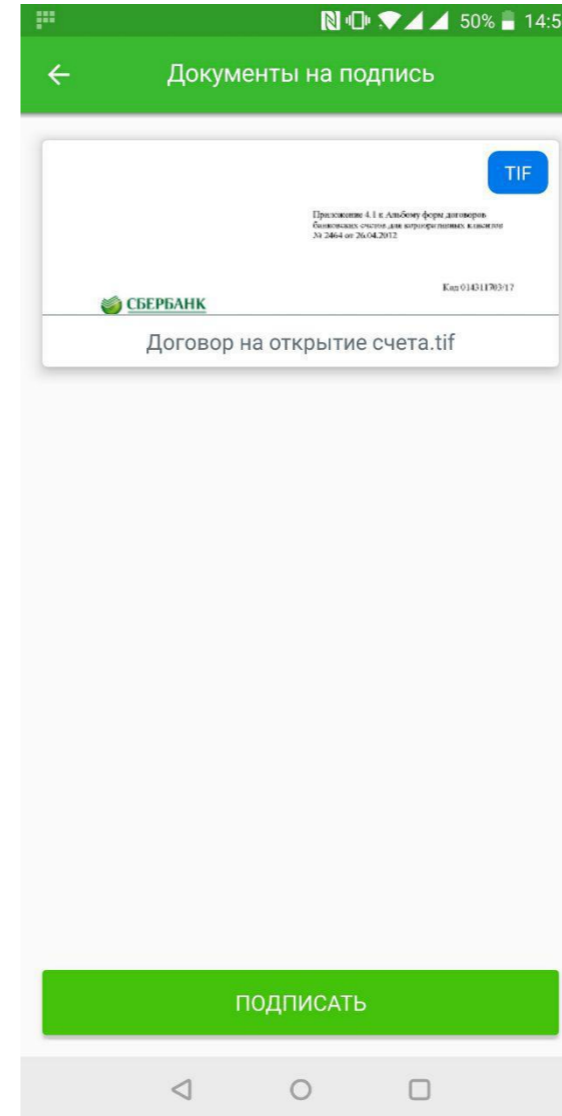
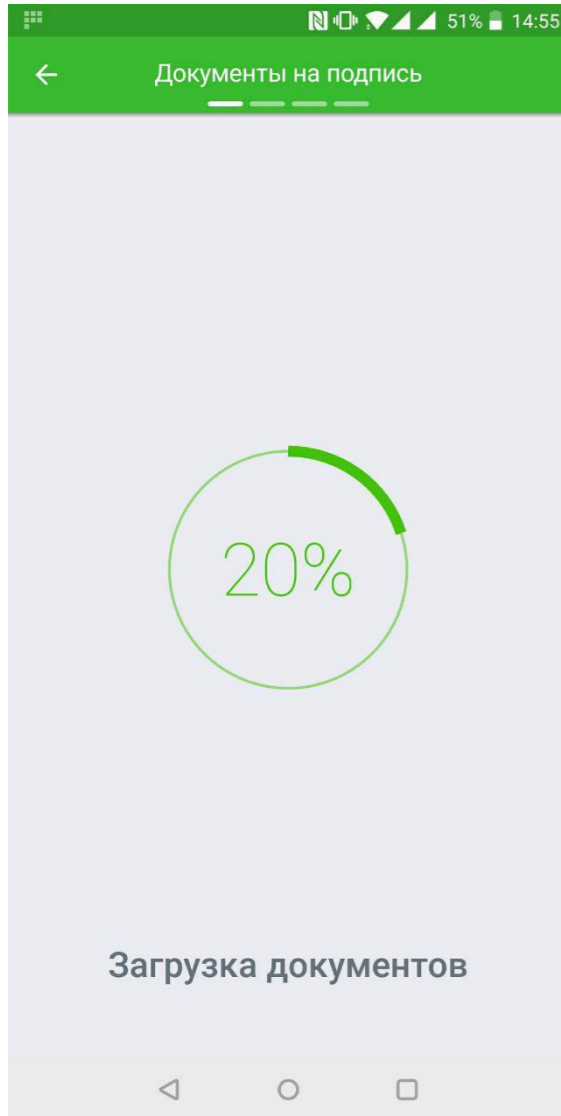


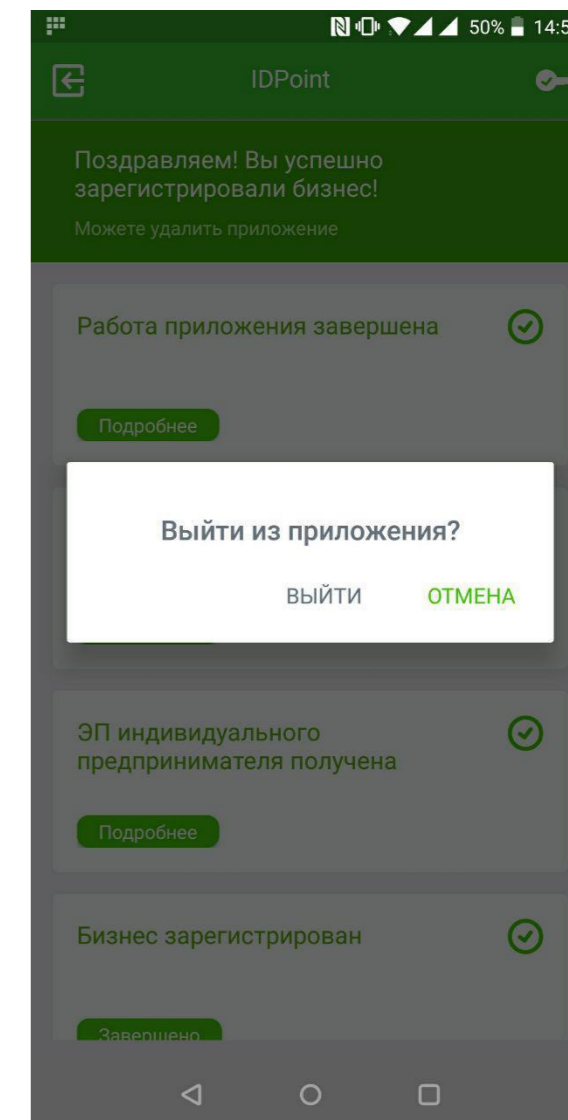
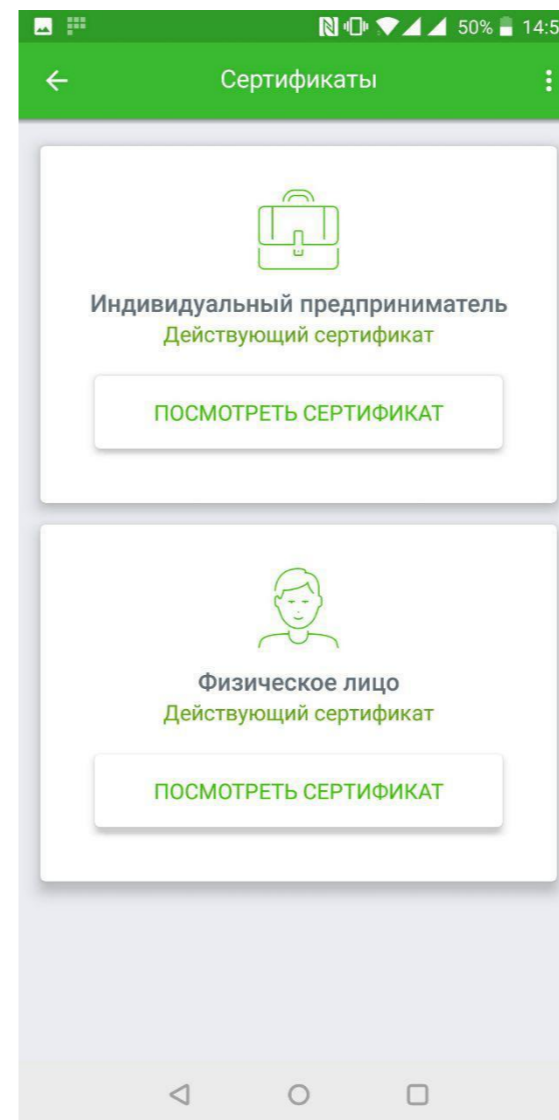
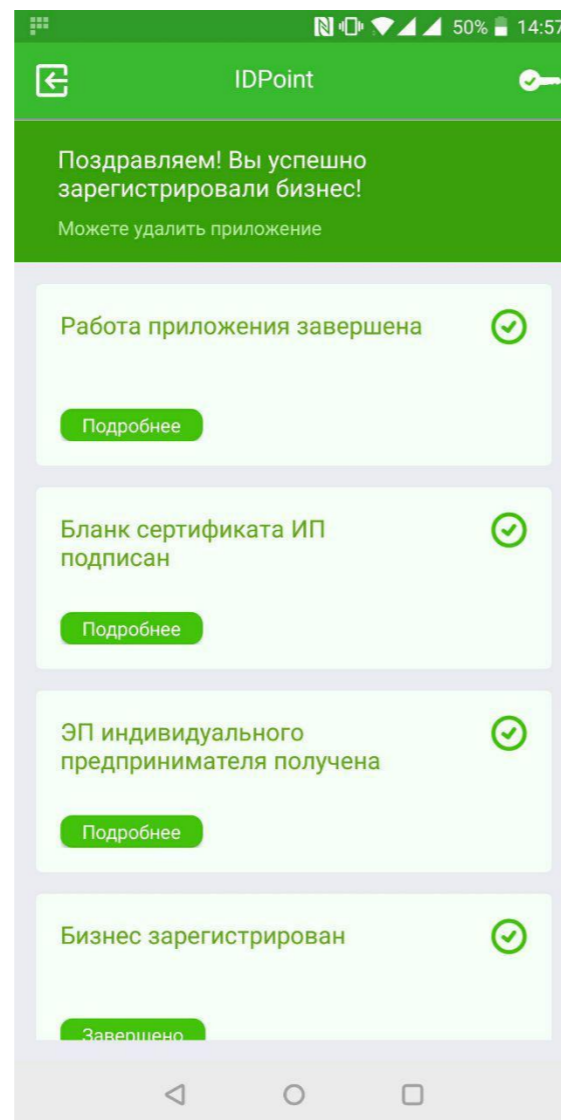
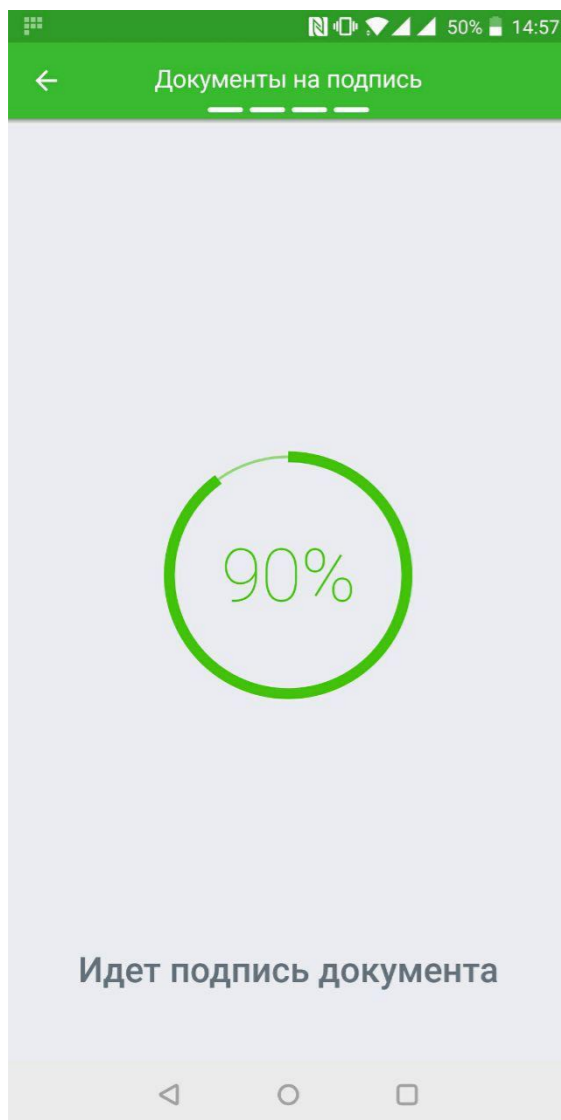
Мобильное приложение в РБидОС. Подпись сертификата ИП подписью ФЛ с подтверждением ПВДНП.

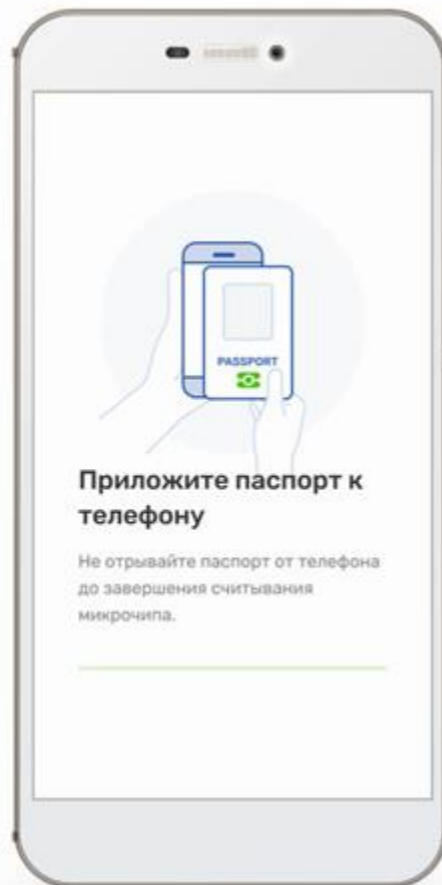




Мобильное приложение в РБидОС. Подпись договора на открытие счета с подтверждением ПВДНП.







Спасибо за внимание!

Иван Андреевич Янсон
бизнес-партнер по информационной безопасности
Департамент безопасности ПАО
Сбербанк
IAYanson@sberbank.ru

Указ Президента РФ от 07.05.2012 N 596 "О долгосрочной государственной экономической политике"

В целях повышения темпов и обеспечения устойчивости экономического роста, увеличения реальных доходов граждан Российской Федерации, достижения технологического лидерства российской экономики постановляю:

1. Правительству Российской Федерации принять меры, направленные на достижение следующих показателей:

а) создание и модернизация 25 млн высокопроизводительных рабочих мест к 2020 году;

б) увеличение объема инвестиций не менее чем до 25 процентов внутреннего валового продукта к 2015 году и до 27 процентов - к 2018 году;

в) увеличение доли продукции высокотехнологичных и наукоемких отраслей экономики в валовом внутреннем продукте к 2018 году в 1,3 раза относительно уровня 2011 года;

г) увеличение производительности труда к 2018 году в 1,5 раза относительно уровня 2011 года;

д) повышение позиции Российской Федерации в рейтинге Всемирного банка по условиям ведения бизнеса со 120-й в 2011 году до 50-й - в 2015 году и до 20-й - в 2018 году.

» Приложение 2. Нормативная база, позволяющая дистанционно выполнять регистрацию бизнеса и открытие счетов.

"О государственной регистрации юридических лиц и индивидуальных предпринимателей" от 08.08.2001 N 129-ФЗ

Статья 9. Порядок представления документов при государственной регистрации

«1. В регистрирующий орган документы могут быть направлены ...направлены в форме электронных документов, **подписанных электронной подписью**, с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети Интернет.....

1.2. Необходимые для государственной регистрации заявление, уведомление или сообщение представляются в регистрирующий орган....и удостоверяются подписью заявителя, подлинность которой должна быть засвидетельствована в нотариальном порядке,Свидетельствование в нотариальном порядке подписи заявителя на представляемых при государственной регистрации заявлении, уведомлении или сообщении не требуется в случае:

...направления документов в регистрирующий орган в порядке, установленном пунктом 1 настоящей статьи, в форме электронных документов, **подписанных усиленной квалифицированной электронной подписью заявителя.»**

"О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ:

Пункт 5 статьи 7 от 07.08.2001 №115-ФЗ. «При этом предусмотренный настоящим пунктом запрет на открытие кредитной организацией счета (вклада) клиента без личного присутствия открывающего счет (вклад) физического лица или представителя клиента не применяется в случае, **если данный клиент ранее был идентифицирован этой же кредитной организацией при личном присутствии физического лица либо при личном присутствии представителя клиента....»**



Требования безопасности ФСБ согласно Постановлению Правительства предъявляются к:

- а) средствам и порядку **хранения ключей** усиленной квалифицированной электронной подписи (УКЭП);
- б) средствам и порядку **дистанционной идентификации (аутентификации)** владельцев квалифицированных сертификатов ключа проверки электронной подписи (КСКПЭП);
- в) средствам и порядку **защиты информации, передаваемой по каналу дистанционного** взаимодействия между владельцами КСКПЭП и аккредитованным УЦ;
- г) средствам и порядку **доказательства неотказуемости владельцев КСКПЭП от поручения** на автоматизированное создание аккредитованным УЦ УКЭП таких владельцев;
- д) средствам и порядку **автоматизированного создания УКЭП**, используемым аккредитованным УЦ в целях создания УКЭП владельцев КСКПЭП по их поручению, полученному дистанционно.

Другими словами, требования предъявляются к СА, ПКК, каналу аутентификации, защите каналов между клиентом и компонентами СЗАС