SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

О создании квалифицированной облачной подписи в рамках эксперимента по Постановлению Правительства №1104 от 29.10.2016

Иван Андреевич Янсон
бизнес-партнер по информационной безопасности ПАО Сбербанк

Рейтинг Doing Business

"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)

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

SCST

Указ от 07.05.2012 N 596

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.

Рейтинг Doing Business

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.

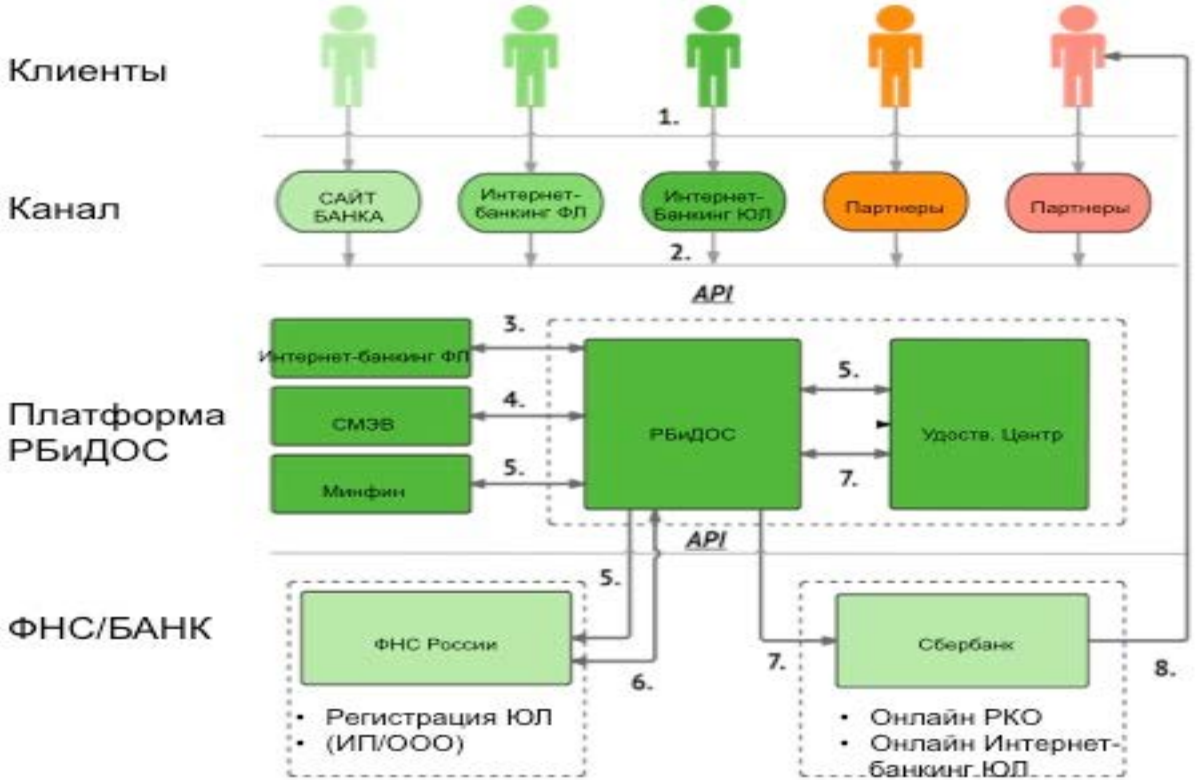
Регистрация предприятий, Россия

~ 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

Схема сервиса регистрации и открытия счетов ЮЛ и ИП



1. Клиент заходит на одну из площадок, интегрированную с РБиДОС
2. Площадка через API передает рег. данные в РБиДОС платформу
3. Подтверждение паспортных данных через Интернет-банкинг ФЛ
4. Сверка со СМЭВ загруженных пользователем данных
5. Формирование пакета уставных документов , оплата госпошлины, выпуск и подписание ЭЦП Физ лица и отправка по API в ФНС России
6. Получение от ФНС подтверждения о регистрации ЮЛ
7. Формирование и отправка в Банк пакета документов на дистанционное открытие счета, выпуск и подписание ЭЦП Юр. Лица
8. Получение клиентом от банка электронного письма с номером счета и доступом в Интернет-банкинге ЮЛ

50% клиентов открывают бизнес и расчетный счет дистанционно

SCST

129-ФЗ и 115-ФЗ Регистрация ЮЛ и ИП, 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….»

Постановление Правительства №1104 от 29.10.2016

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

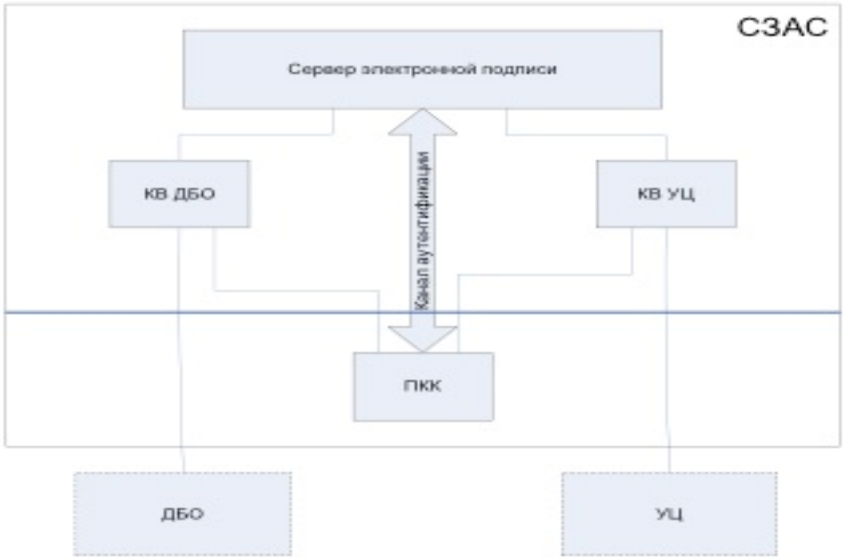
Реализуется с помощью:

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).

Структура специализированной защищенной АС (СЗАС)



Состав СЗАС

- КВ УЦ - Компонент взаимодействия с УЦ
- КВ ДБО - Компонент взаимодействия с ДБО
- СЭП - Сервер электронной подписи
- ПКК – Программный компонент клиента Банка
- РБиДОС это система дистанционной регистрации бизнеса и открытия счетов

Функции компонент схемы

- Клиент через систему ДБО направляет запросы на регистрацию бизнеса и открытие счетов. Кроме того, система ДБО взаимодействует с ФНС для регистрации ЮЛ и ИП и АС Банка для открытия счетов
- Активация облачной подписи клиента производится с ПКК через канал аутентификации
- Хранение ключей ЭП и выработка ЭП от ЭД выполняется в СЭП

Постановление Правительства №1104 от 29.10.2016

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);

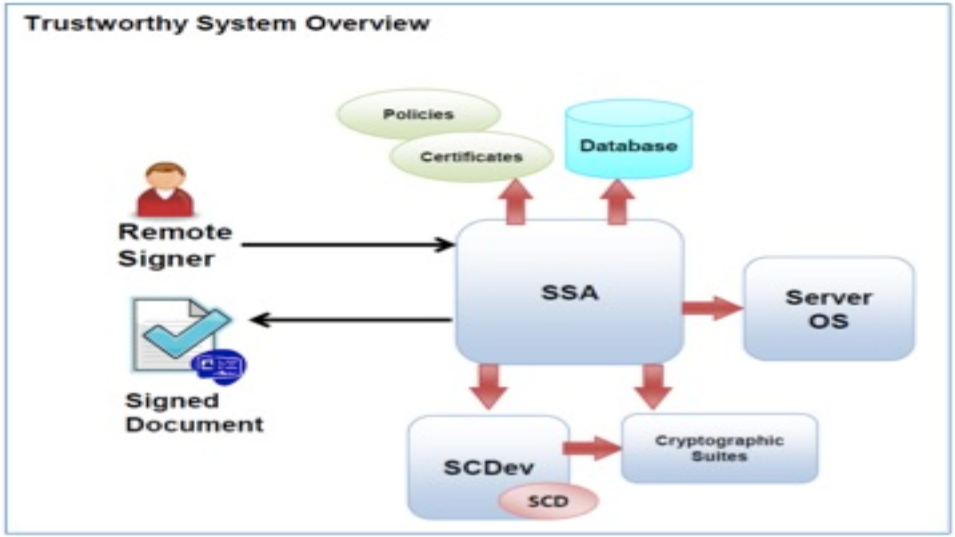
в) средствам и порядку **защиты информации, передаваемой по каналу дистанционного** взаимодействия между владельцами КСКПЭП и аккредитованным УЦ;

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 СЭП, ПКК, каналу аутентификации, защите каналов между клиентом и компонентами СЗАС

Европейский опыт применения «облачной» ЭП (1/5)



SSA – Server Signing Application

SCDev – Signature Creation Device

SCD – Signature Creation Data (обычно это закрытые ключи ЭП)

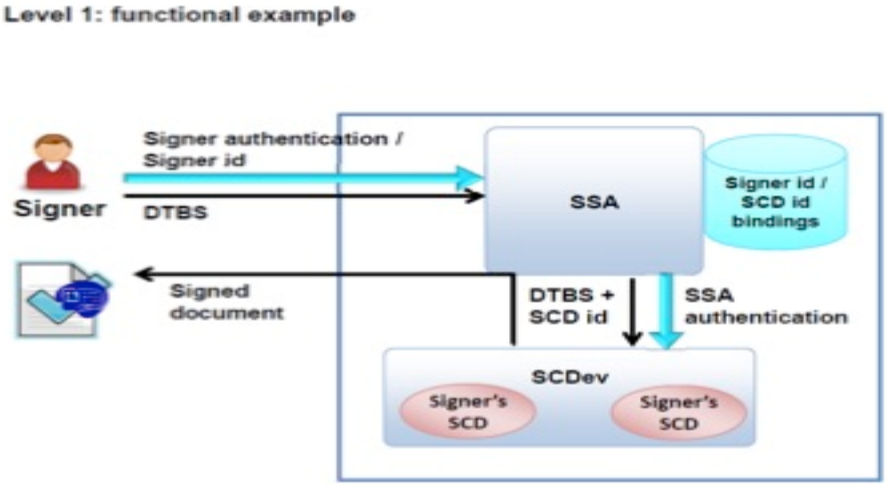
В октябре 2013 года Европейский Комитет по Стандартизации (CEN) одобрил техническую спецификацию Security Requirements for Trustworthy Systems supporting Server Signing; DIN CEN/TS 419241, SPEC 91126, в декабре 2016 года была утверждена новая редакция спецификации

В сентябре 2014 года в силу вступило новое Постановление Европарламента №910/2014 (eIDAS), которое заменяет директиву 1999 года №1999/93/EC, разрешает хранение и использование ключа квалифицированной ЭП на сервере аккредитованного поставщика доверенных услуг, так называемого TSP (Trust Service Provider), например, аккредитованного УЦ

Европейский опыт применения «облачной» ЭП (2/5)

Согласно Директиве 1999/93/EC одним из свойств усиленной электронной подписи является то, что она формируется с помощью средств, которые находятся исключительно под собственным контролем владельца подписи

Поэтому спецификация DIN CEN/TS 419241 для случая серверной электронной подписи также требует соблюдения указанного свойства и выделяет два уровня исключительного собственного контроля подписи:



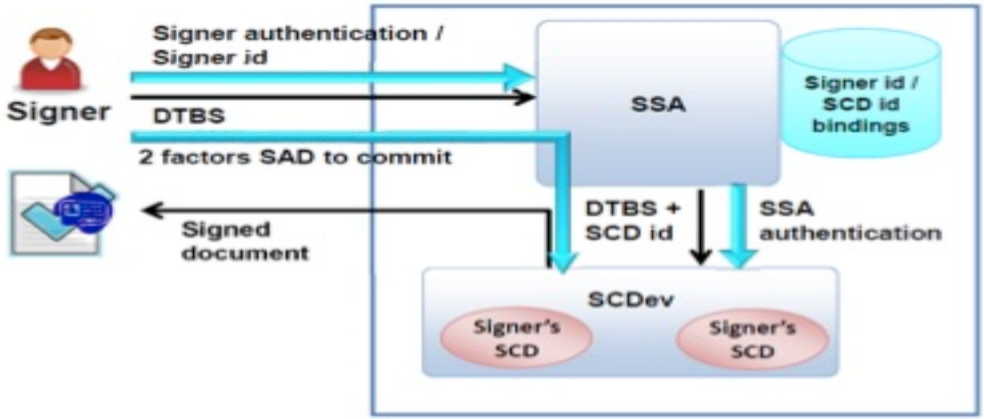
Уровень 1. Дистанционная аутентификация подписанта осуществляется приложением серверной подписи

Уровень 2. Дистанционная аутентификация подписанта осуществляется устройством формирования подписи, с помощью средств активации подписи (Signer'r activation data). При этом должна использоваться многофакторная аутентификация (как минимум, двухфакторная)

SCST

Европейский опыт применения «облачной» ЭП (3/5)

На уровне 2 исключительного собственного контроля подписи требование мультифакторной аутентификации может быть реализовано разными способами:



Вариант 2.1: Мультифакторная аутентификация применяется между подписантом и устройством создания подписи (SCDev) с использованием данных активации подписи (SAD) (см. схему данного варианта на рисунке)

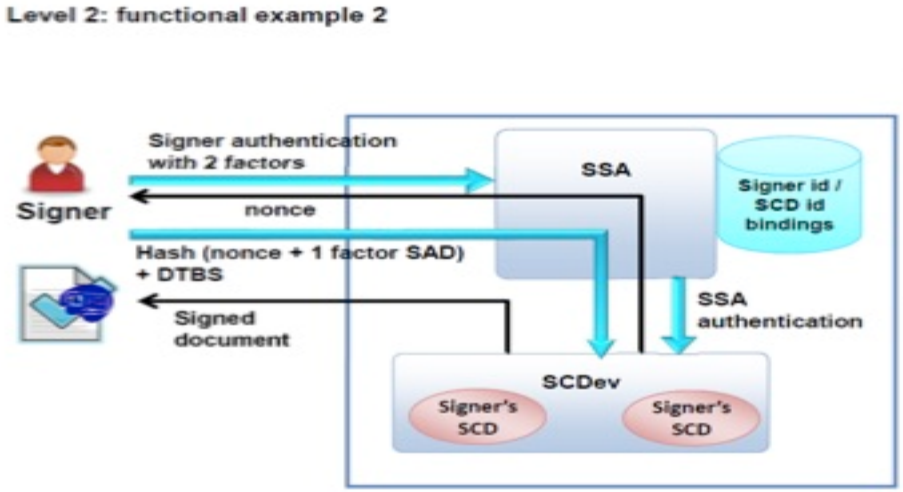
Вариант 2.2: Мультифакторная аутентификация между подписантом и устройством аутентификации, которое далее извлекает и передает данные активации подписи и передает их на устройство создания подписи

Вариант 2.3: Мультифакторная аутентификация происходит между подписантом и приложением серверной подписи, а затем подписант по защищенном каналу передает данные активации подписи на устройство формирования подписи

Европейский опыт применения «облачной» ЭП (4/5)

Пример **варианта 2.3:** Мультифакторная аутентификация происходит между подписантом и приложением серверной подписи, а затем подписант по защищенном каналу передает данные активации подписи на устройство формирования подписи

Такой вариант дает определенную свободу, так как мультифакторную аутентификацию можно не реализовывать в устройстве генерации подписи.



Отметим, что уровень 1 допустим только для усиленной подписи, если же мы говорим о квалифицированной подписи, то здесь Спецификация DIN CEN/TS 419241 требует обязательного выполнения уровня 2 требований к аутентификации

Европейский опыт применения «облачной» ЭП (5/5)

Испания: Компания Izenpe создана в 2003 году Правительством Страны Басков, является аккредитованным УЦ и может выдавать квалифицированные сертификаты ЭП. По данным на весну 2013 года, Izenpe выпустила около 350 тыс. квалифицированных сертификатов, из которых 30 тыс. «в облаке». Ключи ЭП хранятся в специализированном аппаратном криптографическом модуле HSM.

Норвегия: Национальная система аутентификации и облачной подписи, управляемая консорциумом норвежских банков, называется BankID. Запущена на массовом рынке в 2005 году. В BankID выпущено более трёх миллионов сертификатов (более половины населения). Около 600 тыс. пользователей используют BankID через мобильное приложение на смартфоне. Ключи хранятся в аппаратном криптографическом модуле HSM. BankID является распределённой системой со множеством точек входа. Издателями квалифицированных сертификатов являются банки.

Австрия: Облачная система квалифицированной подписи запущена в 2009 году, управляется аккредитованным УЦ, принадлежащим правительству Австрии. Для доступа к ключу используется двухфакторная аутентификация: номер телефона и пароль как первый фактор, а также одноразовый пароль, отправляемый в SMS-сообщении, в качестве второго фактора. Ключи ЭП хранятся в HSM.

Италия: Создателем и оператором системы квалифицированной облачной подписи выступает частная компания Itagile, которая является аккредитованным УЦ. В системе выпущено более 200 тыс. сертификатов. Ключи хранятся в HSM. Итальянский уполномоченный орган, ответственный за сертификацию средств квалифицированной ЭП сертифицировал данное решение на соответствие требованиям стандарта CEN/TS 419241.

Источник: http://www.cryptopro.ru/blog/2015/07/22/elektronnaya-podpis-v-oblake-evropeiskii-opyt

Схемы технологии защиты сервиса «облачной» электронной подписи

Вариант схемы	Описание	За	Против
«Спец.Браузер»	Клиент в офисе получает спец. Браузер и контейнер с ключами	• Высокий уровень защиты • Согласована ФСБ	• Визит в офис • Высокая стоимость реализации • Не существует оборудование HSM нужного класса КА1 • Сложность установки для клиента • Загрузка ресурсов офисов • Требует техподдержки клиентов
«SIM-карта»	Клиенту выдается SIM-карта с установленной СКЗИ и пакетом услуг	• Перспектива использования SIM-карты в госуслугах, согласована ФСБ	• Визит в офис • Длительность вывода продукта на рынок • Низкая клиентоотдача
«Токен»	Типовая схема без ОЭП	• Согласована ФСБ • Проверенная схема работы • Регламентированный процесс	• Визит в офис • Не работает с мобильными устройствами • Сложность установки для клиента • Загрузка ресурсов офиса • Требует техподдержки клиентов
«Мобильное приложение + ПВДНП»	Клиент использует мобильное приложение, идентификация осуществляется по ПВДНП	• Визит в офис не требуется • Согласована ФСБ	• Низкая клиентоотдача (не все имеют ПВДНП и смартфон с NFC)
«Биометрия»	Использование отпечатка пальца, сэлфи с последующим сравнением со скан-копией паспорта,...	• Удобство • Инновационность	• Сложность доработок • Не согласована ФСБ • Визит в офис • Экспертно - высокий уровень отказов
«Идентификация через Интернет-банкинг для ФЛ»	Идентификация клиента производится путем входа в Интернет-банкинг для ФЛ	• Визит в офис не требуется • Высокий уровень готовности к запуску сервиса • Высокий уровень востребованности • Работает и на ПК, и на мобильных устройствах	• Не согласована ФСБ • Риск подмены документов/получения доступа к ОЭП/фальсификации данных

Регистрация бизнеса и дистанционное открытие счета: индикаторы решений

Схема	Проникновение	Юзабилити	Эффективность	Time-to-market	Безопасность	Перспективность
«Спец.Браузер»	1%					
«SIM-карта»	1%					
«Токен»	1%					
«Мобильное приложение + ПВДНП»	5%					
«Биометрия»	10%					
«Идентификация через Интернет-банкинг ФЛ»	18%					

Не согласована ФСБ

Легенда:

Проникновение – доля клиентов, зарегистрировавших бизнес, потенциально воспользовавшаяся сервисом РБиДОС
Юзабилити – удобство использования сервиса, включая визиты в банк/УЦ
Эффективность – оценка стоимости реализации и поддержки сервиса к отдаче от привлечения клиентов
Безопасность – уровень защищенности каналов и согласование схемы ФСБ
Перспективность – возможность развития схемы работы с ОЭП на прочие (гос)услуги для корп. клиентов

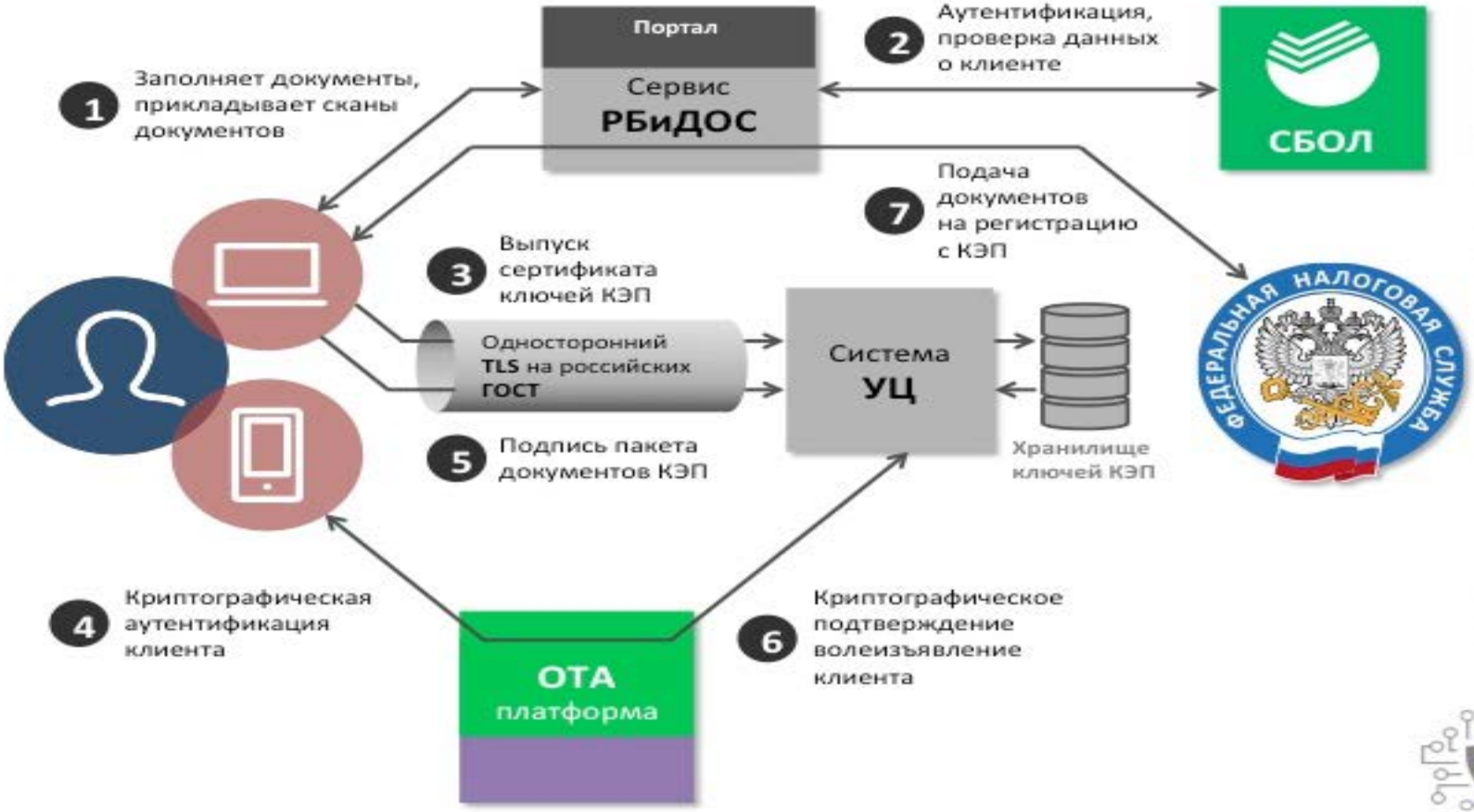
SCST

Выпуск сертификата ключа аутентификации и квалифицированного сертификата ключа проверки ЭП

Подписание документа «облачной» электронной подписью

Криптобраузер Спутник существует для ОС Windows (XP, 7, 8, 10); MacOS, Android, iOS – 4Q2017

Пример: Сервис дистанционной регистрации предприятия



SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

Спасибо за внимание!

Иван Андреевич Янсон

бизнес-партнер по информационной безопасности
Департамент безопасности ПАО Сбербанк

IAYanson@sberbank.ru