SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

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

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.

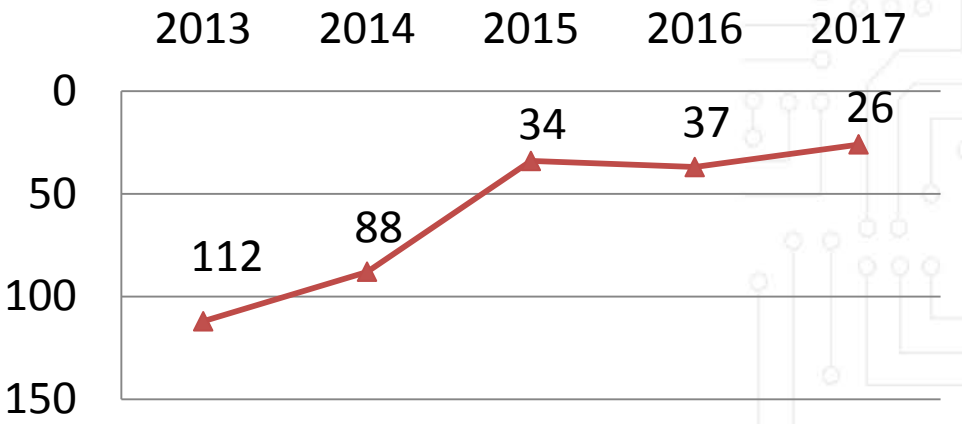
Рейтинг Doing Business

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 **в 2017 году Россия заняла 26е 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

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

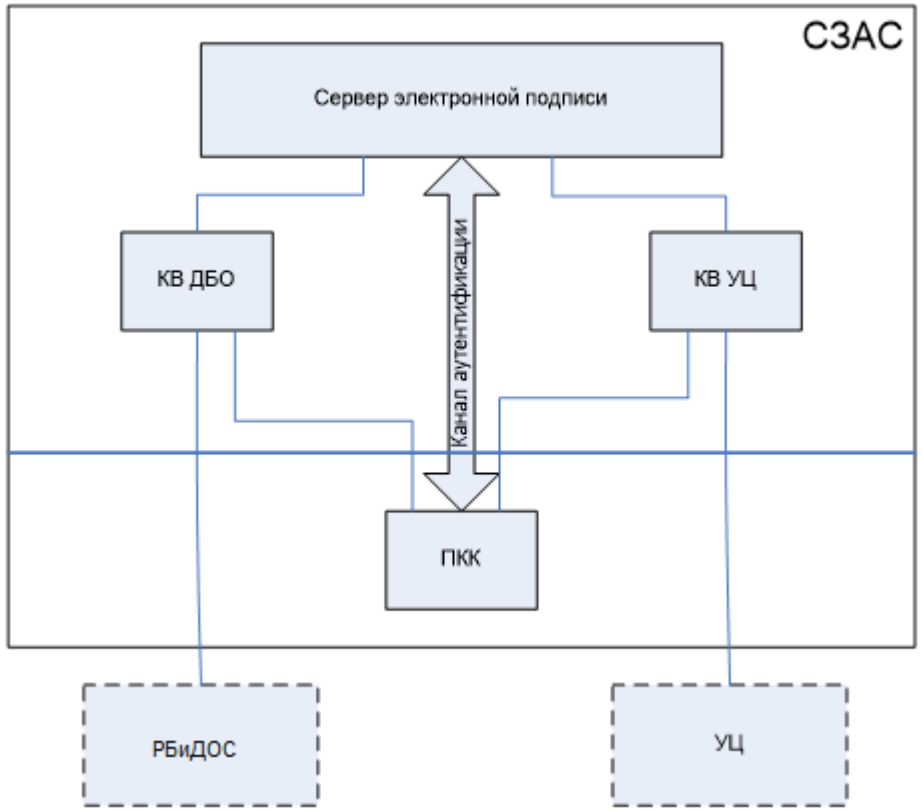
Реализуется с помощью:
Специализированной защищенной автоматизированной системы (СЗАС), предназначенной для **централизованного создания и хранения ключей усиленной квалифицированной электронной подписи**, а также их **дистанционного** применения владельцами квалифицированных сертификатов ключа проверки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

SCST

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

Постановление Правительства №1104 от 29.10.2016

Требования безопасности ФСБ согласно Постановлению Правительства предъявляются к:

а) к средствам и порядку **хранения ключей** усиленной квалифицированной электронной подписи (УКЭП);

б) к средствам и порядку **дистанционной идентификации (аутентификации**) владельцев квалифицированных сертификатов ключа проверки электронной подписи (КСКПЭП);

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

г) к средствам и порядку **доказательства неотказуемости владельцев КСКПЭП от поручения** на автоматизированное создание аккредитованным УЦ УКЭП таких владельцев;

д) к средствам и порядку **автоматизированного создания УКЭП,** используемым аккредитованным УЦ в целях создания УКЭП владельцев КСКПЭП по их поручению, полученному дистанционно.

Таким образом, требования предъявляются к СЭП, ПКК, каналу аутентификации, защите каналов между клиентом и компонентами СЗАС

SCST

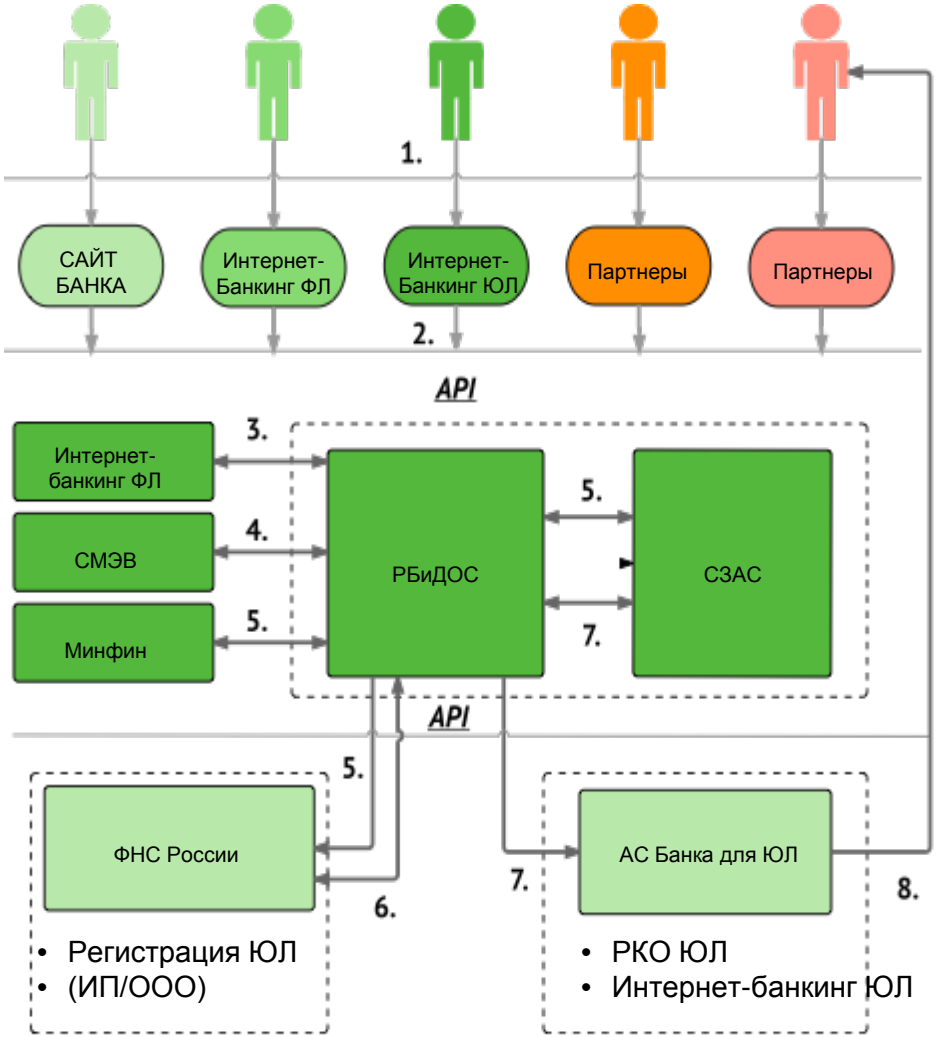
Схема сервиса регистрации и открытия счетов ЮЛ и ИП

Клиенты

Канал

Платформа РБиДОС

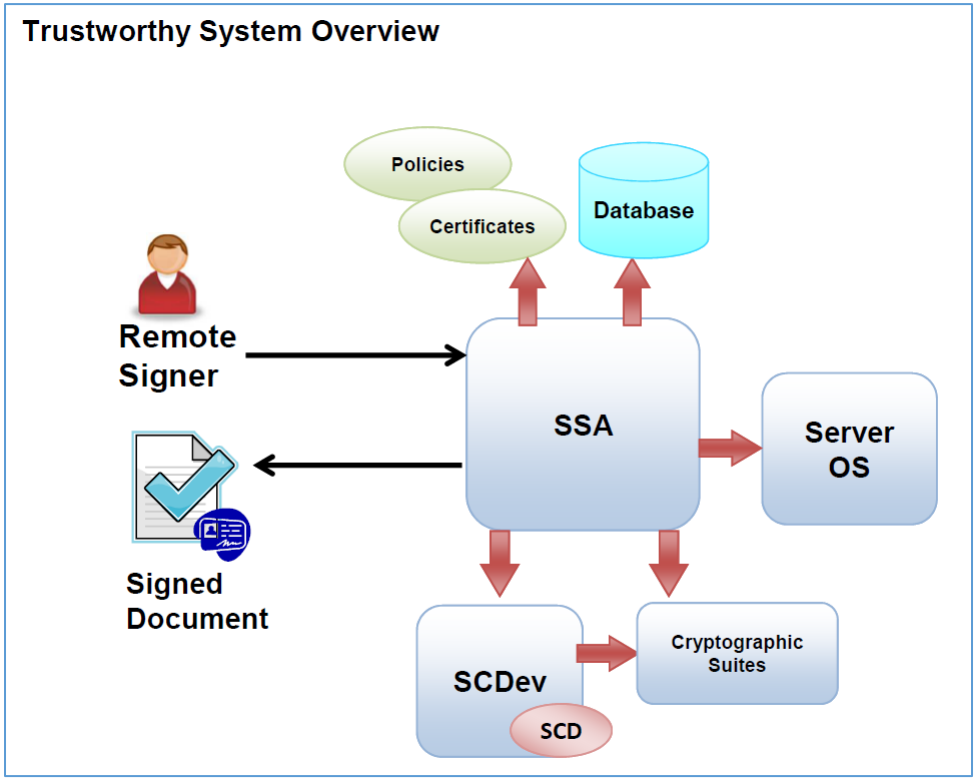
ФНС/БАНК



1. Клиент заходит на одну из площадок, интегрированную с РБиДОС
2. Площадка через API передает рег. данные в РБиДОС платформу
3. Подтверждение паспортных данных и идентификация ФЛ через АС Банка (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-банкинг ЮЛ

SCST

Европейский опыт применения «облачной» ЭП.



SSA – Server Signing Application

SCDev- Signature Creation Device

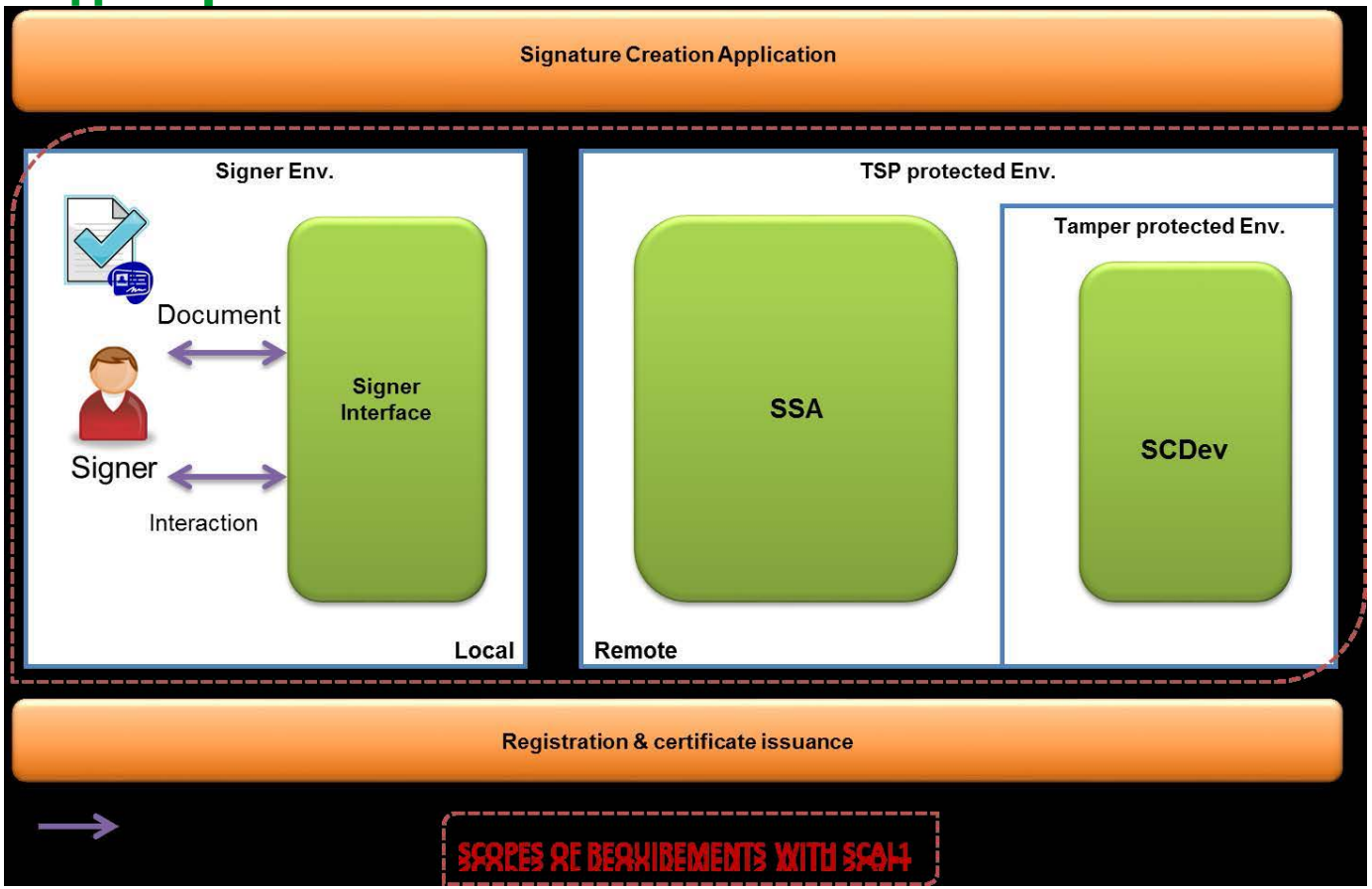
SCD – Signature Creation Data (обычно это закрытые ключи ЭП)

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.

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 вместо спецификации был утвержден Стандарт EN 419241-1, Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements, который вводит понятие двух ***уровней уверенности в единоличном контроле (sole control assurance level - SCAL)*** *владельцем ключей*

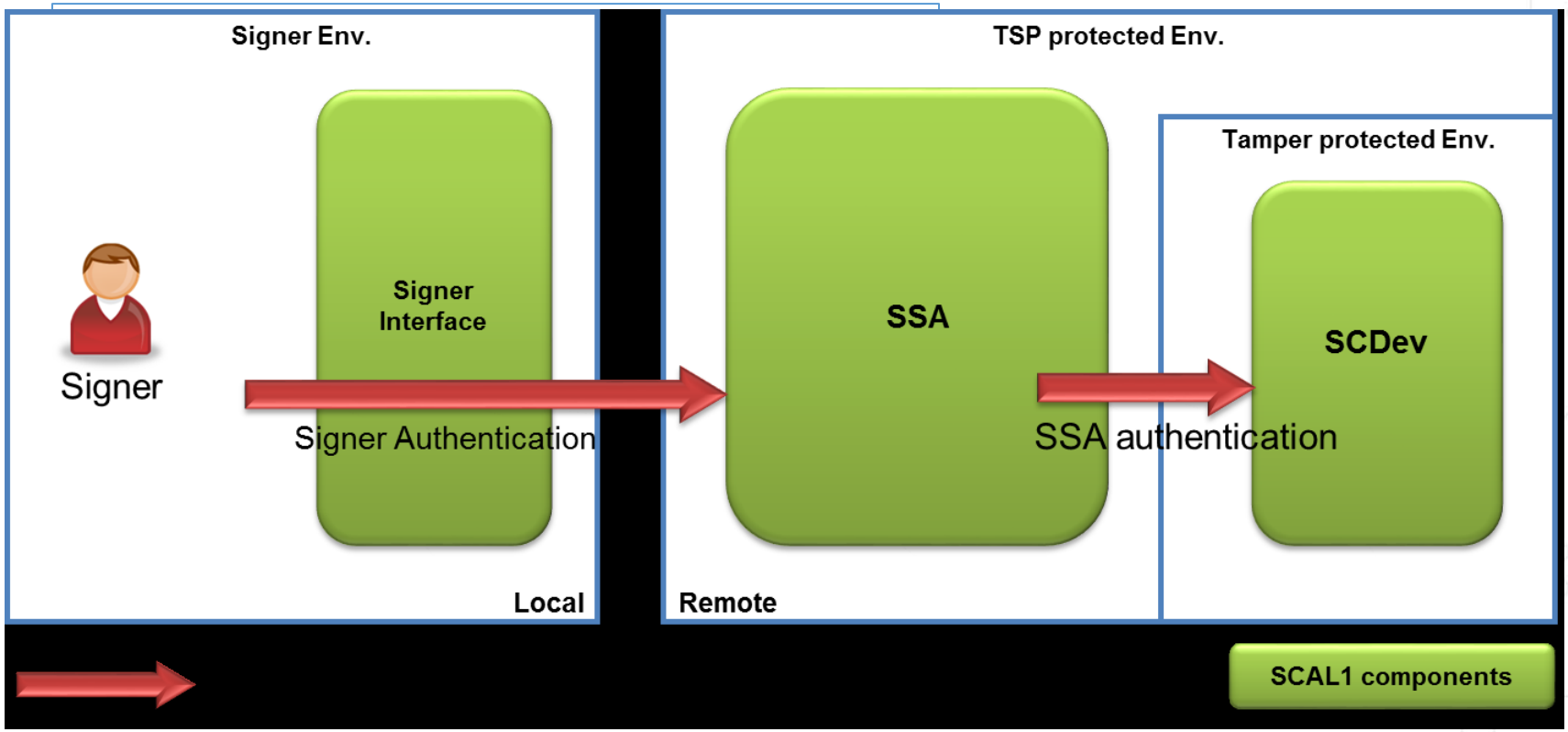
Европейский опыт применения «облачной» ЭП. Уровень доверия 1.



Первый уровень (SCAL1) характеризуется следующими условиями:

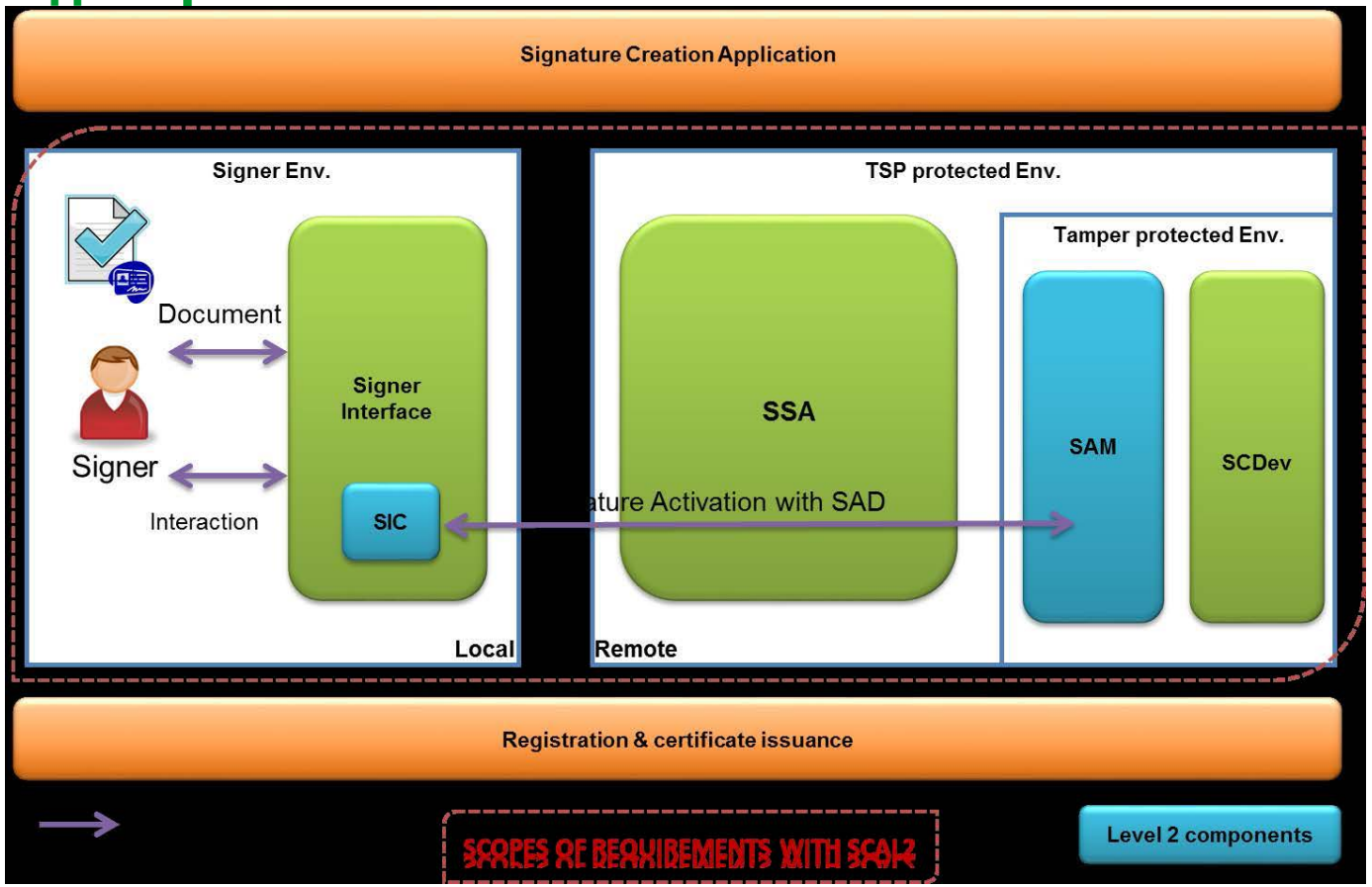
- *Уровень уверенности в том, что ключи используются под единоличным контролем владельца, низкий.*
- *Использование ключей ЭП происходит при условии аутентификации подписанта серверным приложением подписи SSA*
- *Не ожидается, что выполняются требования по единоличному контролю, которые применяются к локально используемым устройствам формирования подписи*

Европейский опыт применения «облачной» ЭП. Уровень доверия 1.



- Для обеспечения большего удобства и гибкости ключи подписи могут формироваться, храниться и использоваться вне криптографического модуля (смарт-карты или HSM). Но все же рекомендуется использовать ключи в защищенной от изменений и копирования среде (например, в HSM)
- Если ключи ЭП хранятся в виде файлов, то должна быть обеспечена их защита от удаления и модификации
- Приложение SSA должно сопоставлять ключи ЭП их владельцам (то есть после аутентификации владелец ключа может использовать только свой ключ ЭП)

Европейский опыт применения «облачной» ЭП. Уровень доверия 2.



Второй уровень (SCAL2) характеризуется следующими условиями:

- *Уровень уверенности в том, что ключи используются под единоличным контролем владельца, высокий.*
- *Использование ключей ЭП происходит при условии аутентификации подписанта с помощью **модуля SAM, аутентификационных данных SAD, с использованием протокола аутентификации SAP***
- *Уровень уверенности в единоличном контроле должен быть таким же, как в случае локально используемых устройств формирования подписи*

Европейский опыт применения «облачной» ЭП. Понятия SAM, SAD, SAP, SIC.

Signer's interaction component (Компонент взаимодействия подписанта)

- Компонент взаимодействия подписанта это программное обеспечение или аппаратное средство, которое функционирует на устройствах подписанта и находится под его единоличным контролем.
- Использование этой компоненты является существенной составляющей протокола активации подписи SAP, а также процесса формирования электронной подписи устройством создания подписи SCDev.
- Компонента SIC всегда используется для аутентификации подписанта или/и для создания данных для активации подписи SAD
- SIC может сам использоваться для формирования SAD
- SIC может использоваться для аутентификации подписанта и для последующей идентификации подписанта в процессе формирования данных для активации подписи SAD
- Компонента SIC может быть, например, следующим:
  - -приложением, функционирующим в браузере,
  - -мобильным приложением , выполняющимся в смартфоне или на планшете
  - -безопасным элементом мобильного телефона (например, SIM картой, получающей SMS-сообщения)
  - - криптографическим устройстом, которым владеет подписант (токены, смарт-карты и т.п.)
- Компонента SIC обеспечивает связь между подписантом и операцией подписи посредством протокола активации подписи SAP

Signature activation module (Модуль активации подписи)

- Модуль активации подписи SAM это программное обеспечение, которое обепечивает высокий уровень уверенности в том, что ключи подписи находятся под единоличным контролем подписанта
- Модуль активации подписи SAM должен использоваться в защищенной от изменений среде
- Если модуль активации подписи SAM используется не в защищенной среде устройства пормирования подписи SCDev, то тогда для их взаимодействия следует использовать защищенный канал.

Европейский опыт применения «облачной» ЭП. Понятия SAM, SAD, SAP, SIC.

Signature activation data (данные для активации подписи)

- SAD могут быть либо множеством данных, либо результатом криптографических преобразований
- SAD могут быть сформированы внутри SIC, либо удаленно с помощью SIC под контролем его владельца
- SAD с высокой степенью уверенности должны быть взаимосвязаны:
  - с подписываемыми данными,
  - с аутентифицированным пользователем,
  - с выбранным ключом подписи
- В случае, если аутентификация подписанта происходит до формирования и передачи SAD, то должна выполняться проверка того, что SAD исходят именно от этого подписанта.

Signature activation protocol (протокол активации подписи)

- SAP должен обеспечивать безопасное дистанционное формирование электронной подписи криптографическим модулем от имени подписанта
- SAP это протокол, с помощью которого подписант (посредством своей компоненты взаимодействия SIC) и сервер дистанционной подписи TW4S взаимодействуют для того, чтобы сформировать данные для активации подписи SAD
- SAP должен обеспечивать как минимум следующее:
  - Аутентификацию подписанта при использовании ключа ЭП,
  - Аутентификацию запроса на формирование подписи с помощью тех или иных активационных данных SAD,
  - Проверку валидности и активности ключа ЭП,
  - Безопасную передачу всех элементов данных активации подписи SAD,
  - Проверку наличия действующего сертификата ключа ЭП.

SCST

Европейский опыт применения «облачной» ЭП. Понятия SAM, SAD, SAP, SIC.

Signature creation device (SCDev)(Устройство формирования подписи)

- Устройство формирования подписи SCDev обеспечивает конфиденциальность и целостность ключей ЭП.
- SCDev может содержать несколько ключей подписи как для одного подписанта, так и многих подписантов. В случае, если SCDev содержит разные ключи для одного или нескольких подписантов, то должно быть реализовано разграничение доступа к этим ключам ЭП.
- Ключи подписи должны быть однозначно сопоставлены с их владельцами с помощью протокола активации подписи SAP. Ключи подписи не должны использоваться, если не было произведено волеизъявление их владельцев.
- SCDev может активироваться одним SSA для уровня SCAL1. В случае уровня SCAL2 устройство SCDev участвует в протоколе SAP и обеспечивает то, что операция подписи находится под контролем легитимного подписанта. При этом SSA взаимодействует с SCDev через модуль активации SAM, который проверяет активационные данные SAD, чтобы активировать соответствующие ключи подписи.
- Для активации ключей ЭП могут применяться несколько разных протоколов SAP и видов активационных данных SAD. Однако, при этом ключу подписи должны быть сопоставлен только один протокол SAD и один механизм (вид) SAP.
- Аутентификация подписанта может быть произведена на заданный период времени или на заданное число операций подписи. Но SAD должны вычисляться для каждой операции подписи. SAD могут быть связаны с конкретными данными для подписи, например, для целей пакетной подписи документов.
- Устройство формирования подписи SCDev должно иметь оценочный уровень доверия EAL 4 или выше согласно ISO/IEC 15408 и удовлетворять требованиям стандартов ISO/IEC 19790 или FIPS PUB 140-2 по уровню 3.
- SCDev перед началом создания ключей подписи должно быть инициализировано с помощью технических процедур, которые требуют участия минимум двух разных специалистов.

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 КА - Сложность установки для клиента - Загрузка ресурсов офисов - Требует техподдержки клиентов
«SIM-карта»/«SIM-карта с КЭП»	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 - Не существует оборудование HSM нужного класса КА - 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 сэлфи с последующим сравнением со скан-копией паспорта	- Удобство - Инновационность	- Визит в офис - Сложность доработок - Не согласована ФСБ
«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 клиентоотдачи - 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 с аутентификационной ЭП»	1%					
«SIM-карта с ЭП»	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

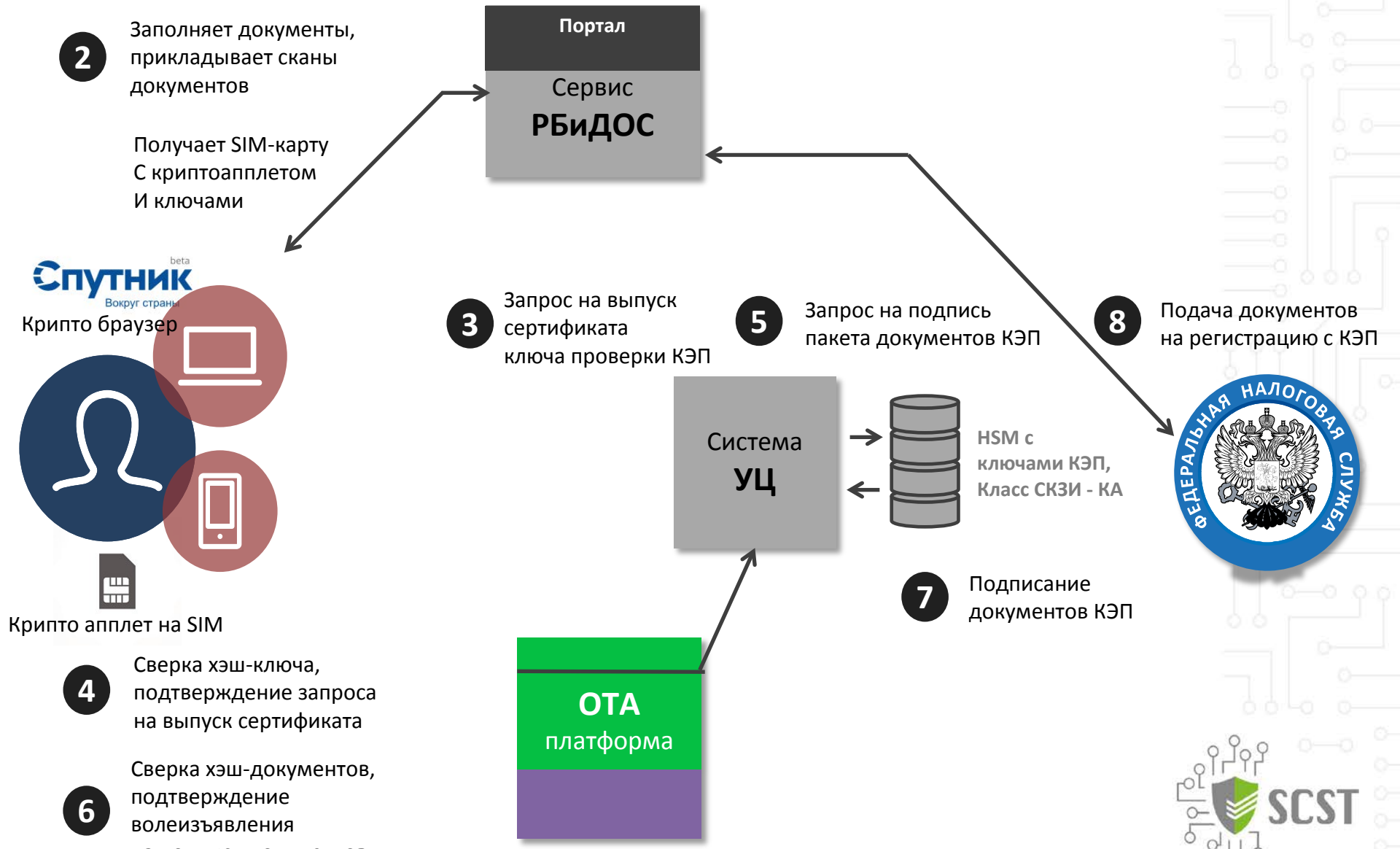
Безопасность – уровень защищенности каналов и согласование схемы ФСБ

Перспективность – возможность развития схемы работы с ОЭП на прочие (гос)услуги для корп. клиентов

Схема «Мобильное приложение + ПВДНП*»

* ПВДНП – паспортно-визовый документ нового поколения (с чипом на борту)

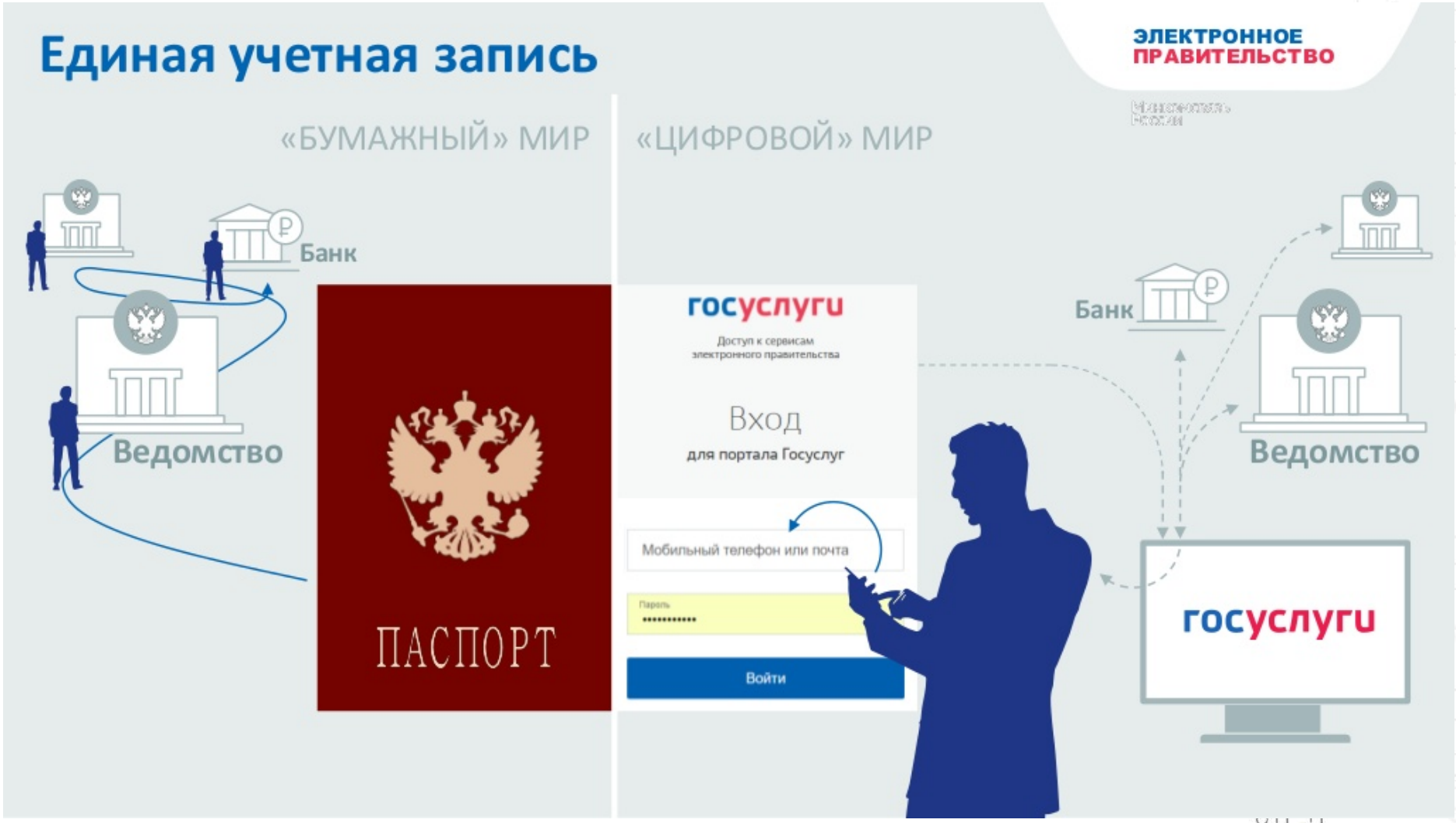
Схема «SIM-карта»



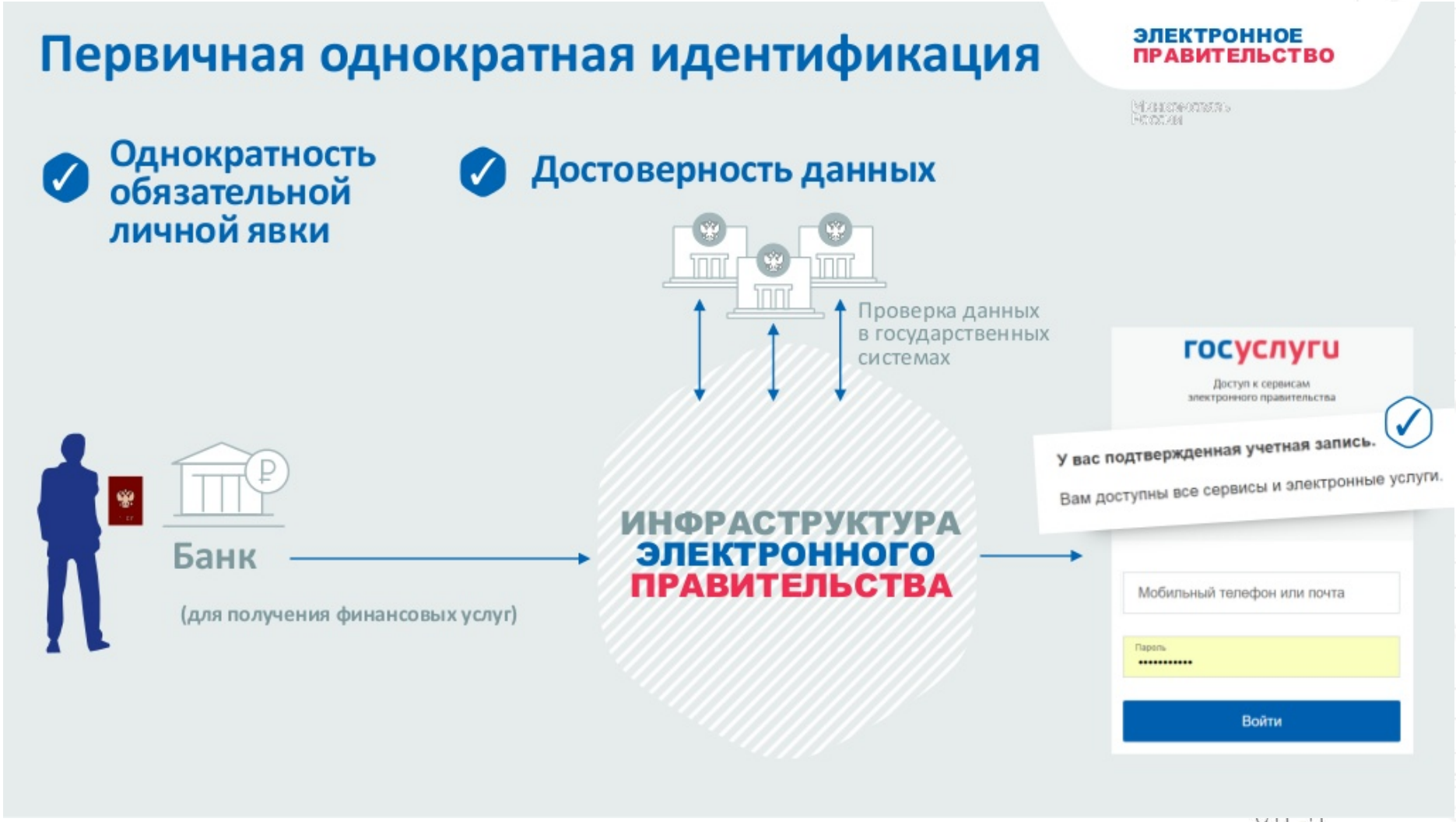
SCST

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

Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (1/5)



Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (2/5)



Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (3/5)

Удаленная идентификация (шаг 1)

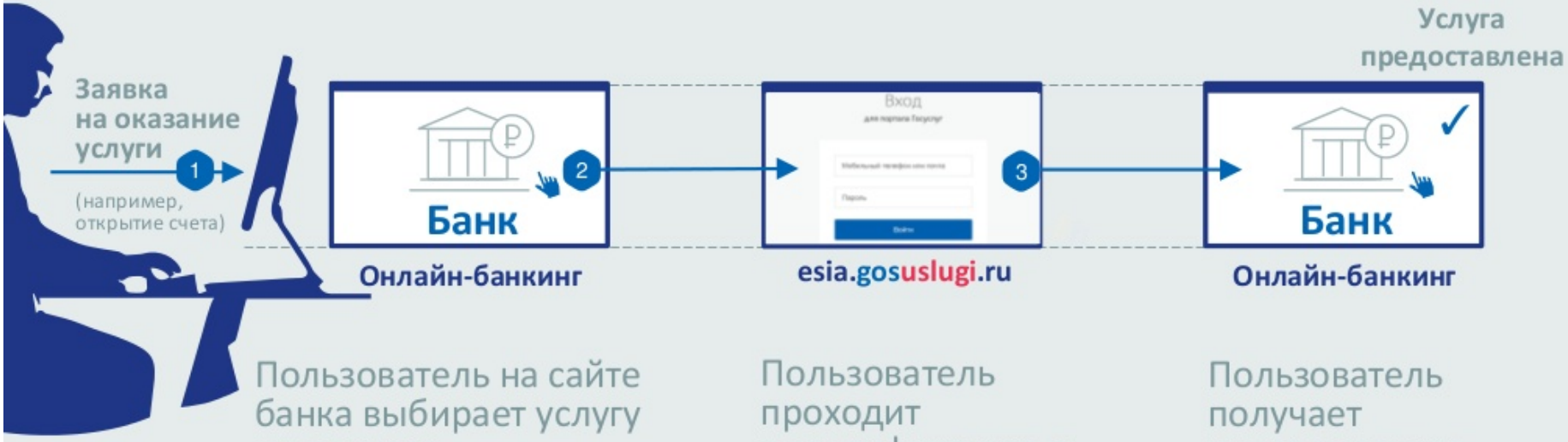
Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (4/5)

Удаленная идентификация

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО

✓ Простота для пользователей

✓ Юридическая значимость



Пользователь на сайте банка выбирает услугу и получает предложение пройти идентификацию

Пользователь проходит идентификацию в ЕСИА, в том числе биометрическую. Его данные передаются в банк.

Пользователь получает интересующую финансовую услуг

SCST

Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (5/5)

Предложение Сбербанка

Регистрируется
на портале РБиДОС

Удаленная идентификация клиента,
включая биометрическую
верификацию,
получение данных о клиенте

4

Портал

Сервис
РБиДОС

3 Заполняет документы,
прикладывает сканы
документов

Устанавливает
Мобильное
приложение с
СКЗИ

5 Запрос на выпуск
сертификата
ключа аутентификации

7 Запрос на подпись
пакета документов КЭП

9 Подача документов
на регистрацию с КЭП

Смартфон/планшет,
Мобильное приложение

Двухсторонний
TLS на российских **ГОСТ**

Система
УЦ

Запрос на выпуск
сертификата
ключа проверки КЭП

**Хранилище
ключей шифрования
ключей КЭП,
Класс СКЗИ - КС**

8 Подтверждение волеизъявления
клиента на подпись
документов, подписание КЭП

ФЕДЕРАЛЬНАЯ НАЛОГОВАЯ СЛУЖБА

SCST

Проблемы первичной идентификации клиента

Проблемы первичной идентификации и распространения компоненты взаимодействия клиента

Федеральный закон № 63-ФЗ «Об электронной подписи»

1. Статья 18, часть 2: *При обращении в аккредитованный удостоверяющий центр **заявитель** указывает на ограничения использования квалифицированного сертификата (если такие ограничения им устанавливаются) и **представляет** следующие **документы либо их надлежащим образом заверенные копии** и сведения:*
   *1) **основной документ, удостоверяющий личность**;……*

Таким образом, Федеральным законом № 63-ФЗ не указано, можно ли предоставлять заявителю в Удостоверяющий центр основной документ в виде сканкопии, например, подписанной УНЭП или КЭП Также не указано может ли считаться надлежащим заверением использование УНЭП или КЭП при передаче электронных копий документов. Не описана процедура идентификации заявителя (можно ли идентифицировать по ПЭП в ДБО или в ЕСИА?)

2. Статья 18, часть 3: *При получении квалифицированного сертификата заявителем он **должен быть под расписку ознакомлен** аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате*.

Таким образом, Федеральным законом № 63-ФЗ не указано, можно ли проводить ознакомление с сертификатом с помощью электронной подписи (ПЭП, УНЭП, КЭП). В случае КЭП – можно ли заверять той самой КЭП, сертификат для которой выпущен?

Проблемы первичной идентификации клиента

Предложения по решению проблемы первичной идентификации

В целях получения УЦ возможности дистанционно формировать квалифицированные сертификаты ключей электронной подписи и ключи усиленной квалифицированной электронной подписи необходимо внести в Федеральный закон № 63-ФЗ следующие изменения:

1. Дополнить закон положениями, дающими УЦ право принимать от заявителей документы в электронном виде с использованием тех или иных видов подписи, в том числе, с помощью идентификации в ЕСИА, а также возможно, от ранее идентифицированных кредитными организациями заявителей, с помощью дистанционной идентификации в системах ДБО, либо с помощью платежных карт в устройствах самообслуживания.

2. Дополнить закон положениями, дающими УЦ право выдавать заявителям квалифицированные сертификаты дистанционно, а также дистанционно получать от заявителей подтверждения об ознакомлении с информацией, содержащейся в квалифицированном сертификате с помощью электронной подписи. В том числе, дать право подписывать ознакомление с сертификатом с помощью подписи, для которой он был выпущен.

Сходные предложения в проекте удаленной идентификации с помощью ЕСИА

Предложения о внесении изменений в Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

5.7. Кредитные организации **вправе открывать счета** (вклады) клиенту - физическому лицу **без его личного присутствия после идентификации указанного лица с использованием единой системы идентификации и аутентификации** при одновременном соблюдении следующих условий:

Получения и проверки посредством единой системы идентификации и аутентификации сведений о нем, предусмотренных абзацем вторым пункта 5.6 настоящей статьи;

подтверждения с использованием информационно-технологических элементов совпадения предоставленных биометрических персональных данных с биометрическими персональными данными, ранее полученными в соответствии с абзацами третьим и шестым пункта 5.6 настоящей статьи;

…….

Степень совпадения биометрических персональных данных, предоставляемых клиентом-физическим лицом с биометрическими персональными данными, ранее полученными в соответствии с абзацами третьим и шестым пункта 5.6 настоящей статьи, которая признается достаточной для проведения идентификации клиентов-физических лиц в соответствии с настоящим пунктом, а также порядок предоставления соответствующей информации кредитной организации, устанавливается Правительством Российской Федерации по согласованию с Центральным банком Российской Федерации.

Сходные предложения в проекте удаленной идентификации с помощью ЕСИА

……

Согласие физического лица на обработку персональных данных (включая биометрические персональные данные) для осуществления операций, предусмотренных абзацем первым настоящего пункта и договор банковского счета (вклада), **могут подписываться простой электронной подписью физического лица** - субъекта персональных данных, в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации. ***Указанное согласие и договор банковского счета (вклада), подписанные такой электронной подписью, признаются электронными документами, равнозначными документам на бумажном носителе, подписанными собственноручной подписью данного физического лица.***

Ограничения по количеству счетов (вкладов), открываемых в соответствии с настоящим пунктом одному физическому лицу, а также по сумме операций по таким счетам (вкладам), за исключением операций, совершаемых при расторжении договора банковского счета (вклада), устанавливаются Центральным банком Российской Федерации по согласованию с уполномоченным органом.

Центральный банк Российской Федерации вправе установить критерии определения кредитных организаций, которые не могут открывать счета (вклады) клиенту - физическому лицу при проведении идентификации без его личного присутствия, а также перечень таких кредитных организаций и порядок его составления.».

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