SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

Варианты реализации дистанционной подписи в рамках эксперимента по Постановлению Правительства №1104 от 29.10.2016

Александр Владимирович Бродский
Управляющий директор
Департамент 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

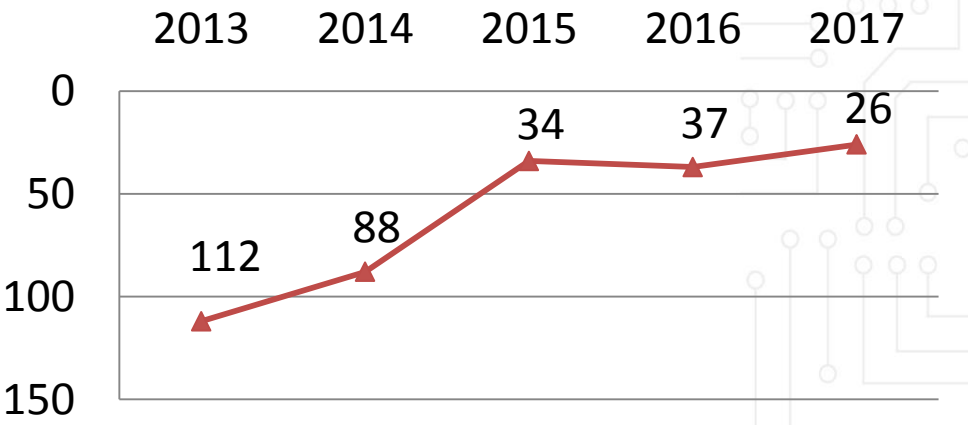
Рейтинг Doing Business

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 занимает 26е место**. Необходимо скорейшее дальнейшее улучшение данного индикатора для достижения запланированного суммарного показателя к 2018 г.

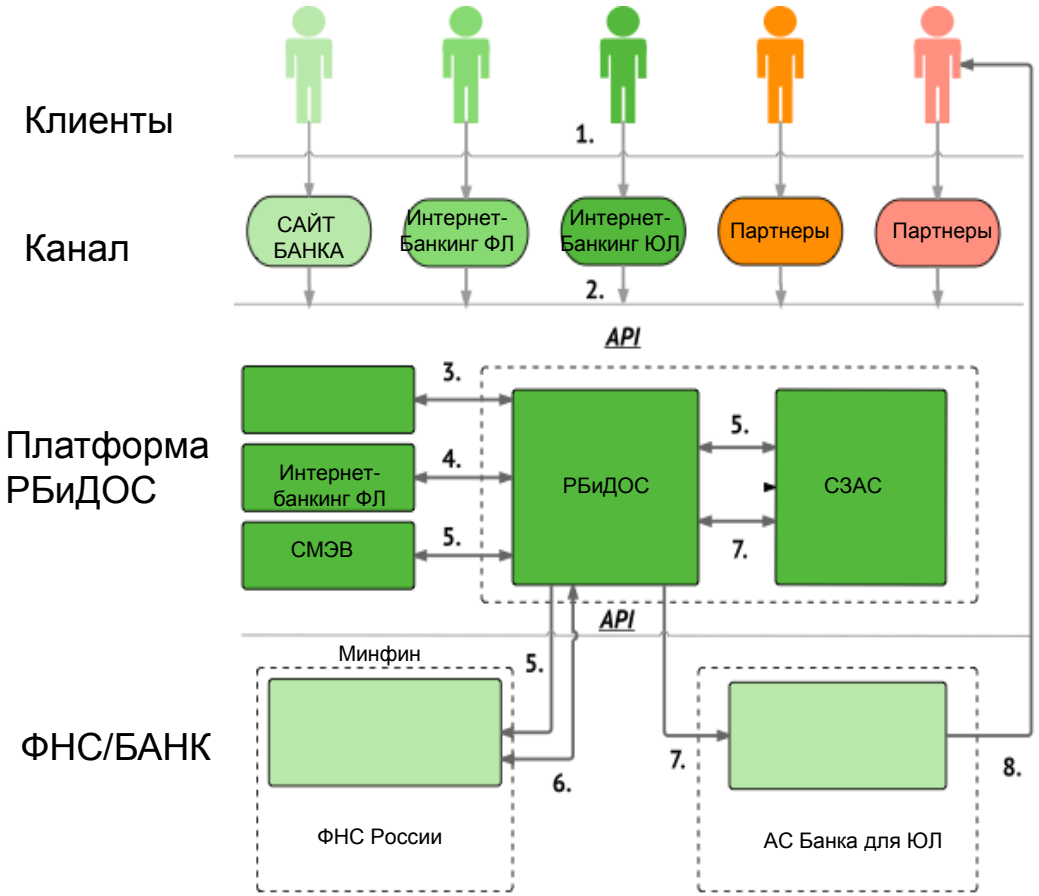
Регистрация предприятий, Россия



~ 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

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 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

- Регистрация ЮЛ
- (ИП/ООО)

- РКО ЮЛ
- Интернет-банкинг ЮЛ

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).

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.

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	• 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»	Клиенту выдается SIM-карта с установленной СКЗИ и пакетом услуг	• Перспектива использования SIM-карты в госуслугах	• Визит в офис • Длительность вывода продукта на рынок • Не существует оборудование HSM нужного класса КА • Низкая клиентоотдача
«Токен»	Типовая схема без ОЭП	• 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	• 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
«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	• Риск подмены документов/получения доступа к ОЭП/фальсификации данных

Регистрация бизнеса и дистанционное открытие счета: индикаторы решений

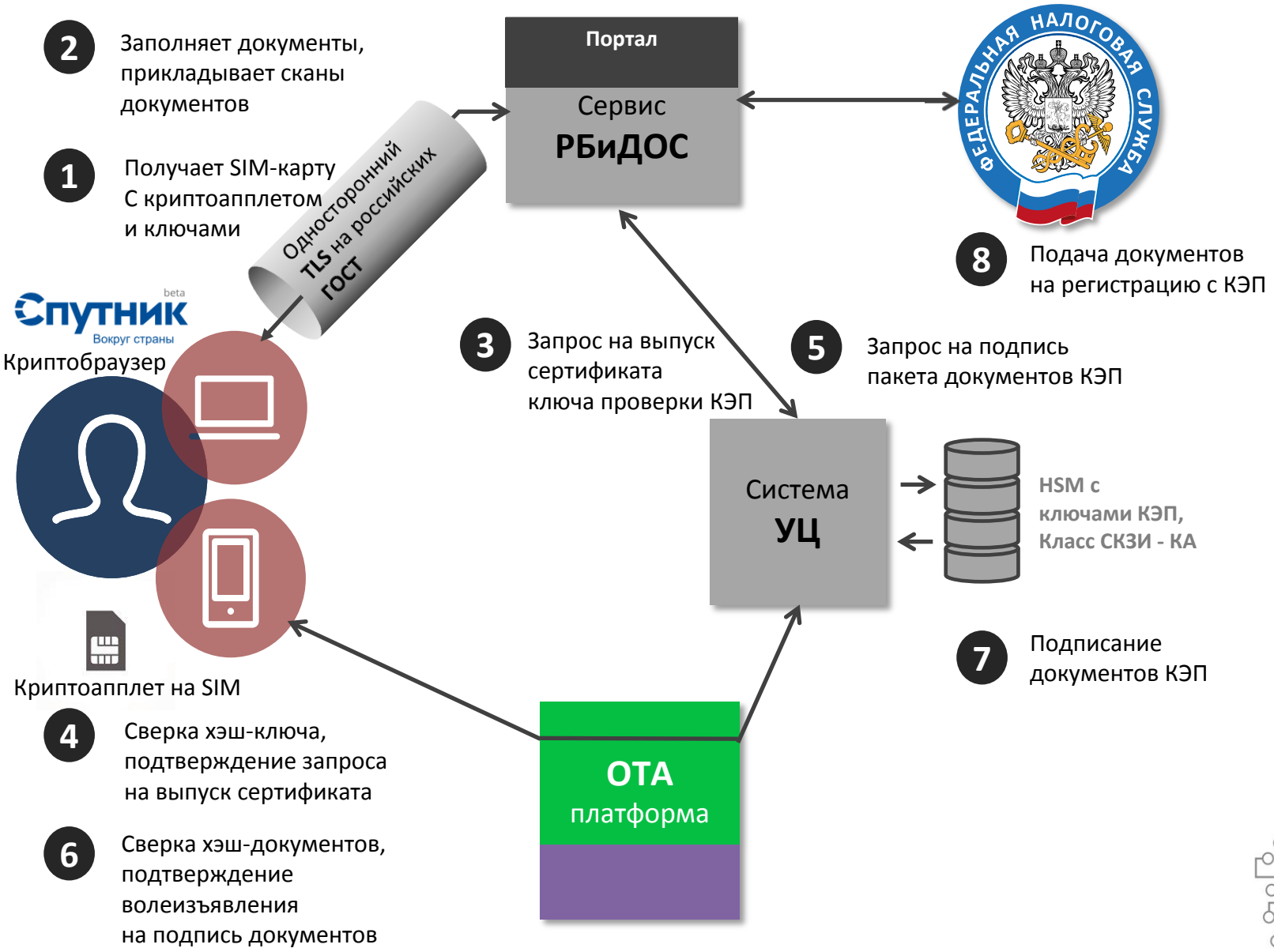
Схема	Проникновение	Юзабилити	Эффективность	Time-to-market	Безопасность	Перспективность
«Спец.Браузер»	1%					
«SIM-карта»	1%					
«Токен»	1%					
«Мобильное приложение + ПВДНП»	5%					
«Биометрия»	10%					
«Идентификация через Интернет-банкинг ФЛ»	18%					

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

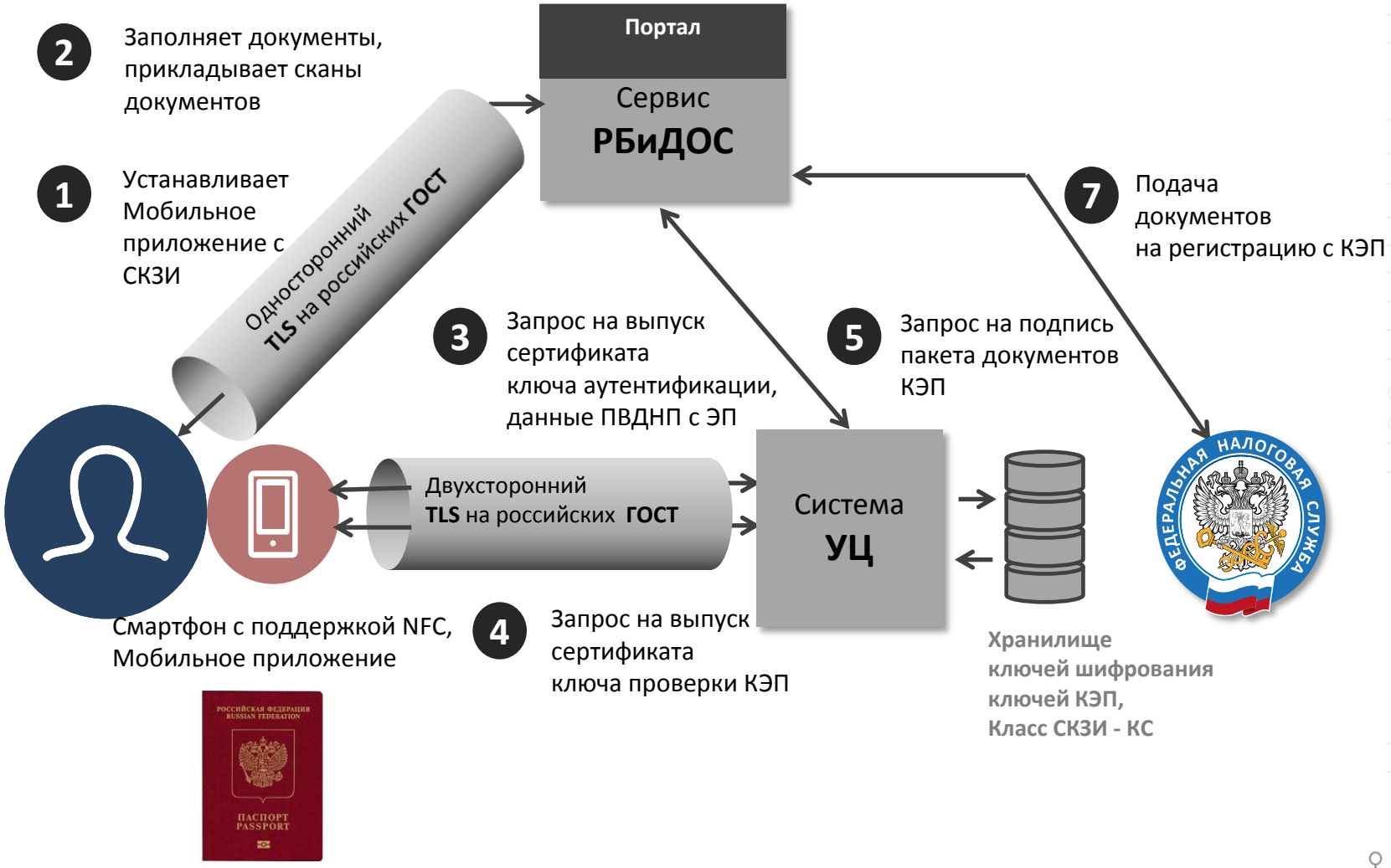
SCST

Схема «SIM-карта»

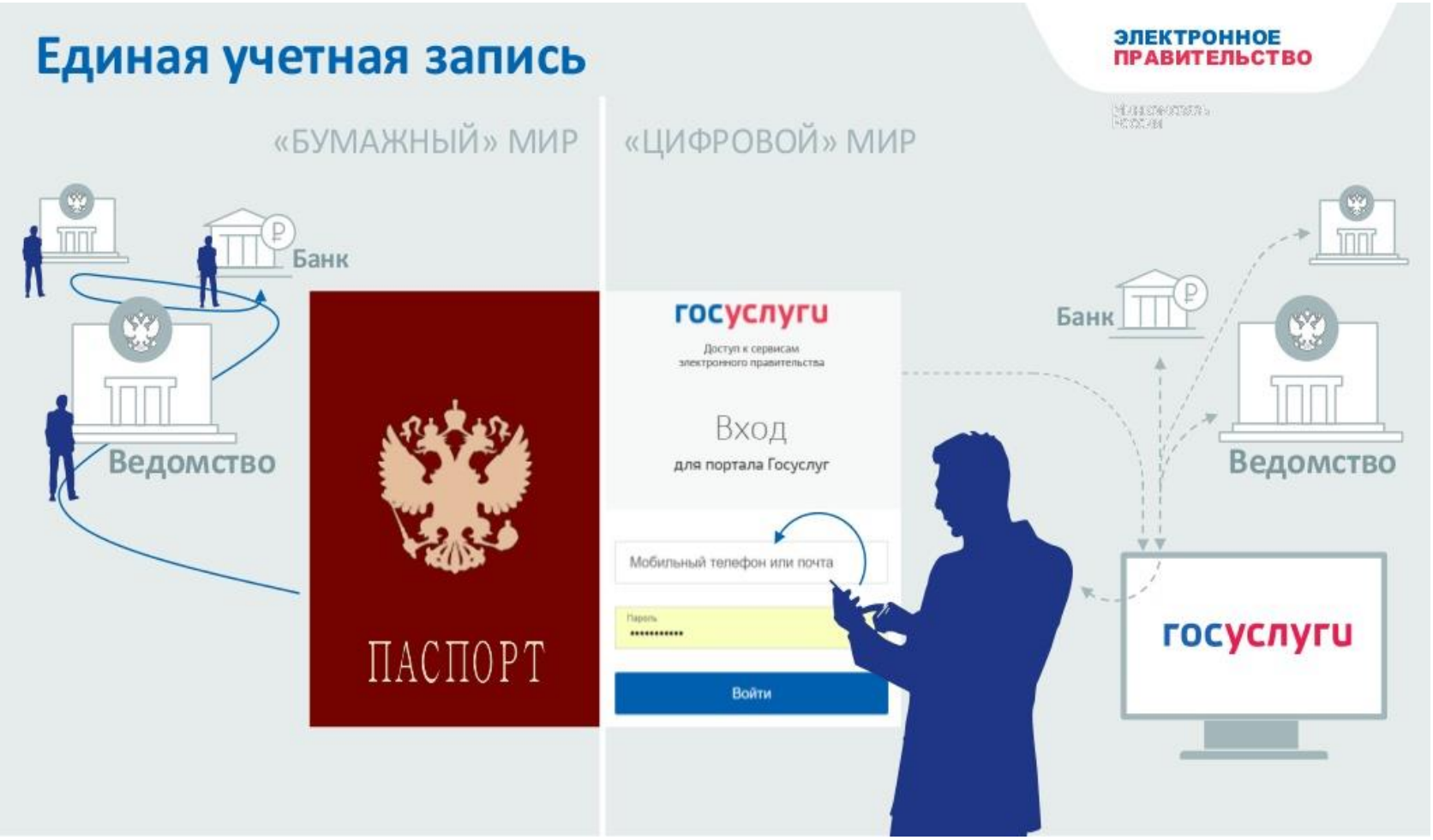


Криптобраузер Спутник существует для ОС Windows (XP, 7, 8, 10); MacOS, Android, iOS – 4Q2017

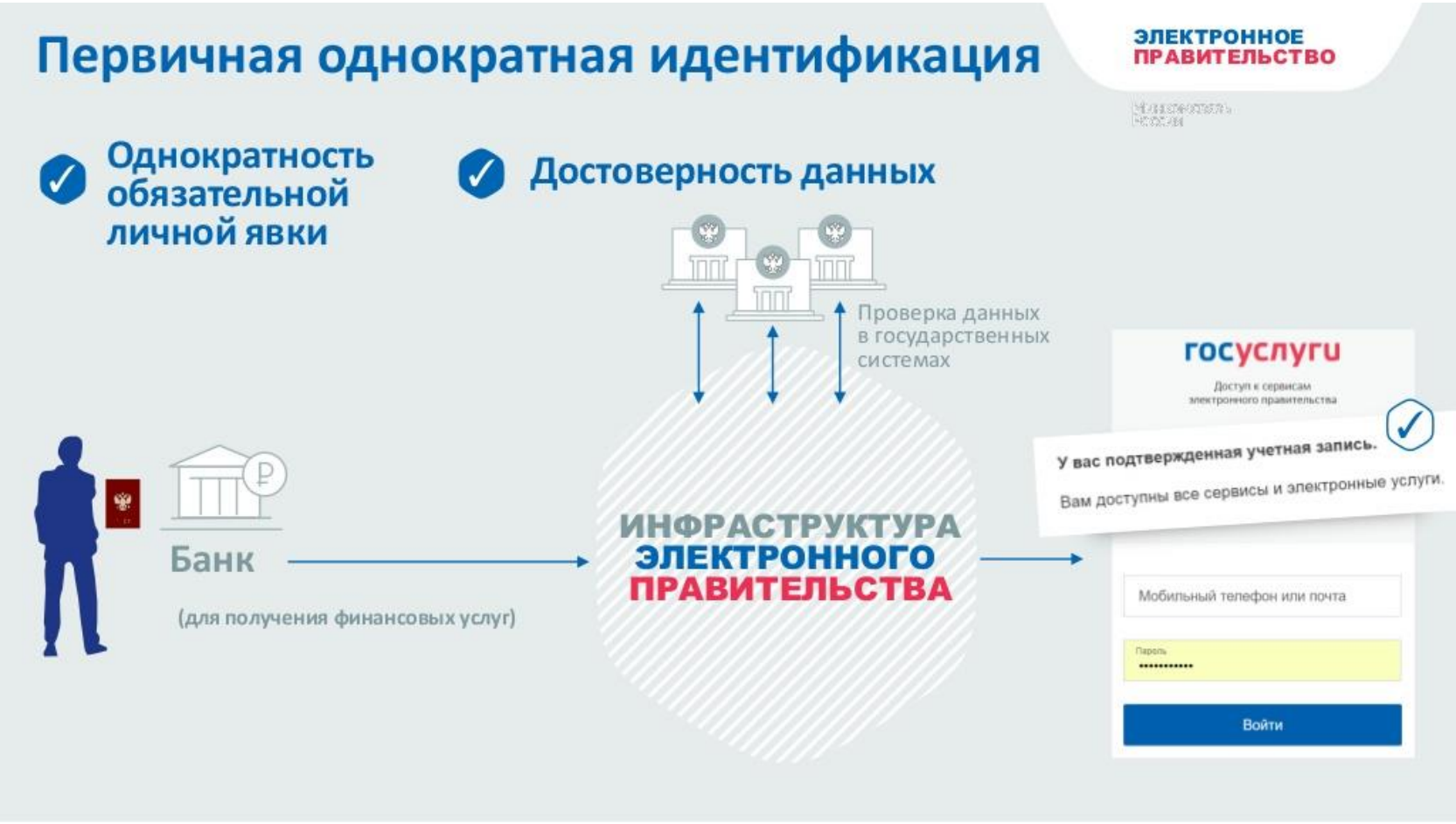
Схема «Мобильное приложение + ПВДНП»



Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (1/3)



Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (2/3)

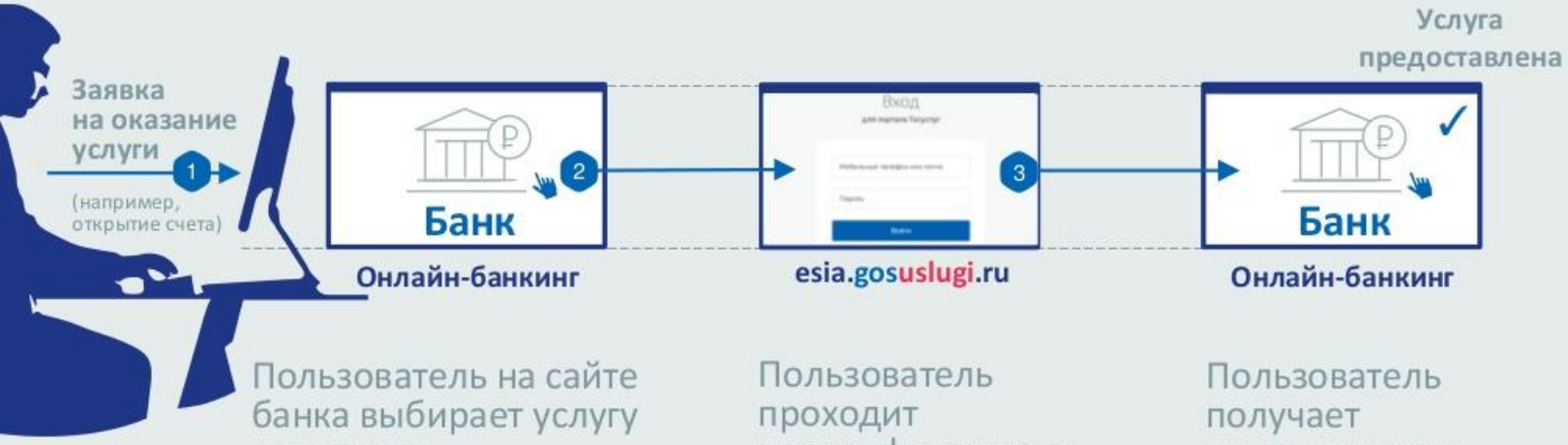


Пилот ЦБ РФ и Минкомсвязи по удаленной идентификации (3/3)

Удаленная идентификация

ЭЛЕКТРОННОЕ ПРАВИТЕЛЬСТВО

- Простота для пользователей
- Юридическая значимость



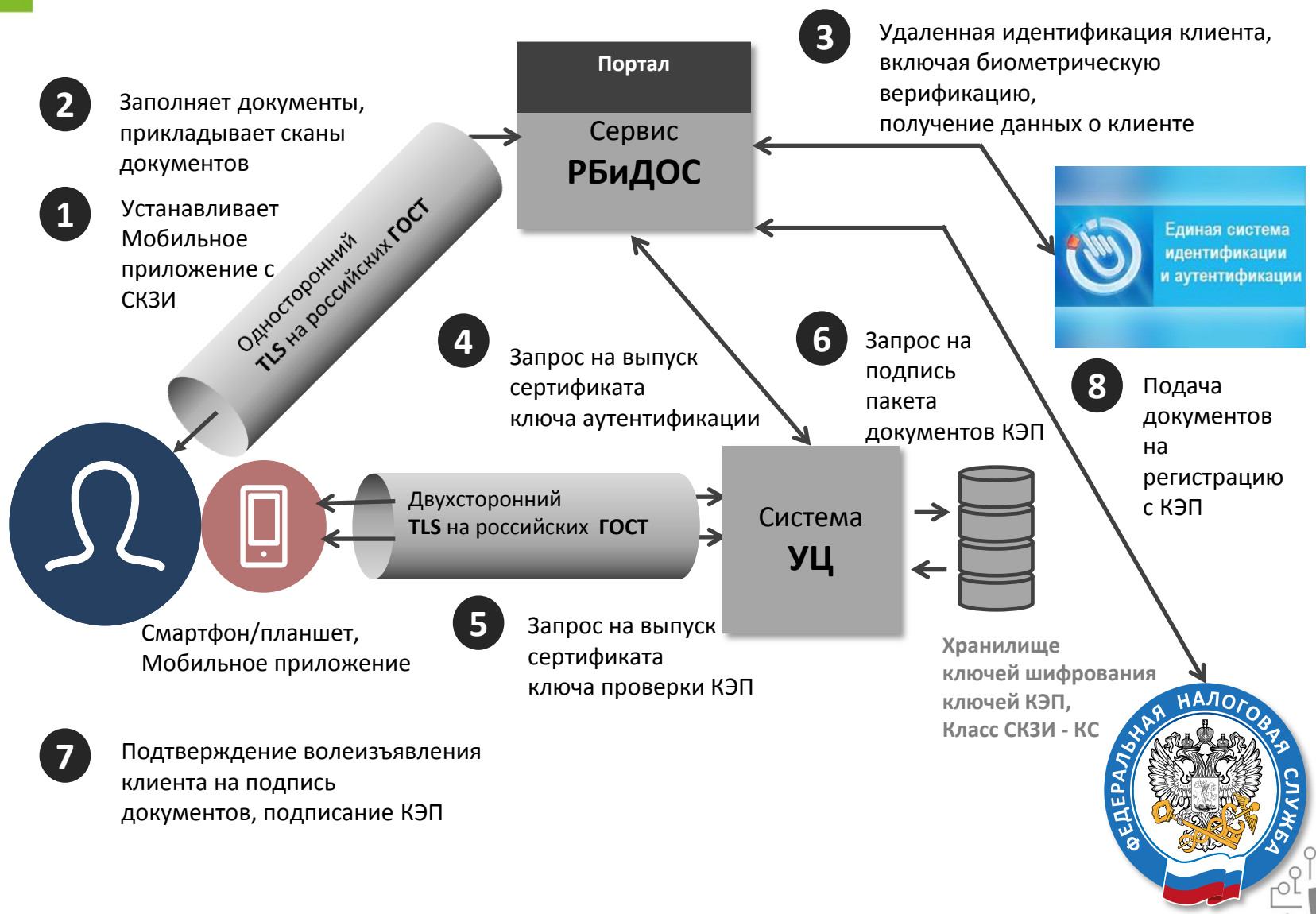
Пользователь на сайте банка выбирает услугу и получает предложение пройти идентификацию

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

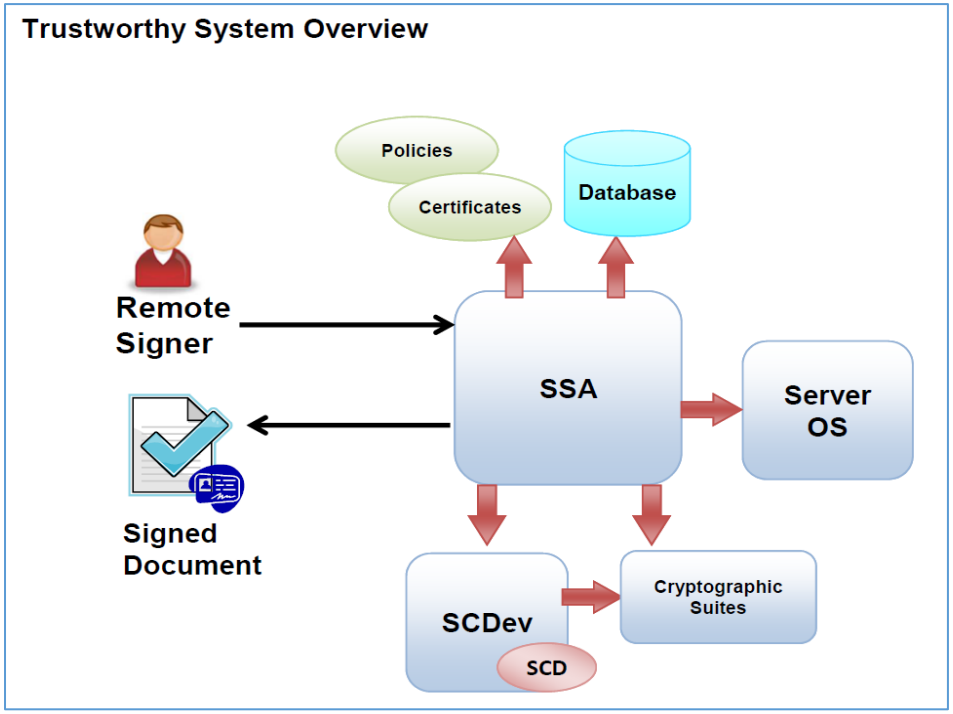
Пользователь получает интересующую финансовую услуг

SCST

Предложение Сбербанка



Европейский опыт применения «облачной» ЭП (1/4)



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

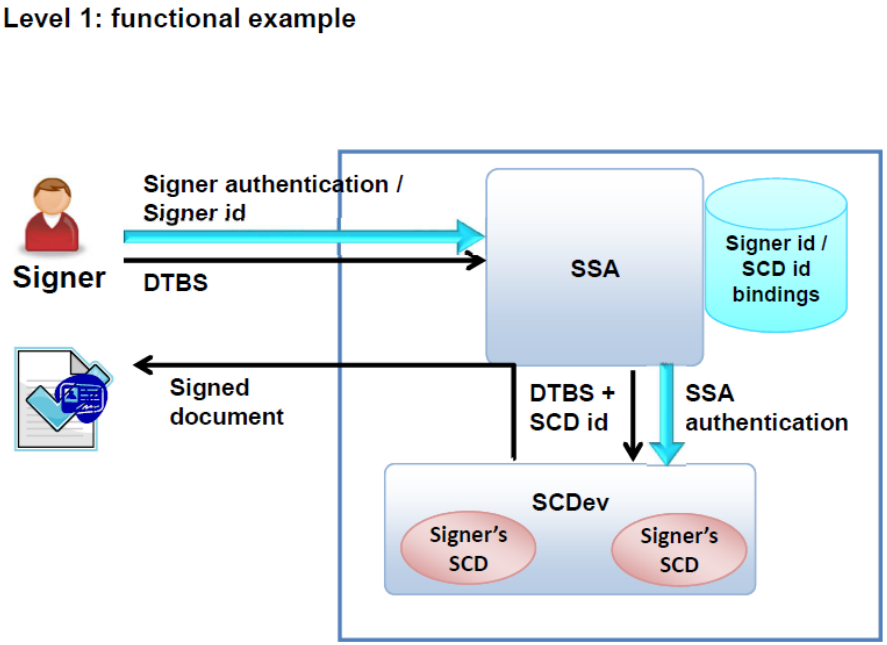
В сентябре 2014 года в силу вступило новое Постановление Европарламента №910/2014 (eIDAS), которое заменяет директиву 1999 года №1999/93/EC, разрешает хранение и использование ключа квалифицированной ЭП на сервере аккредитованного поставщика доверенных услуг, так называемого TSP (Trust Service Provider),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

SCST

Европейский опыт применения «облачной» ЭП (2/4)

Согласно Директиве 1999/93/ЕС 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:



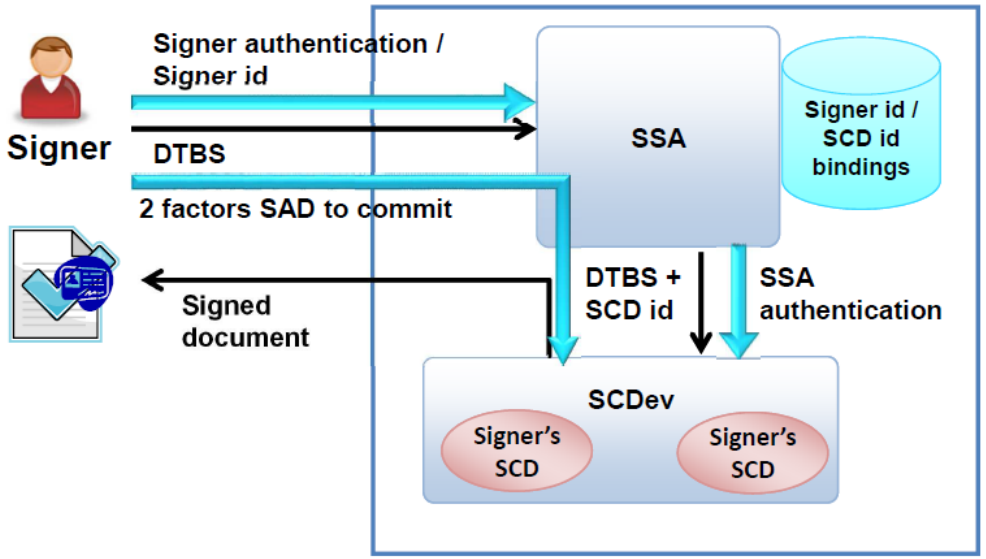
Уровень 1. Дистанционная аутентификация подписанта осуществляется приложением серверной подписи

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

SCST

Европейский опыт применения «облачной» ЭП (3/4)

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)

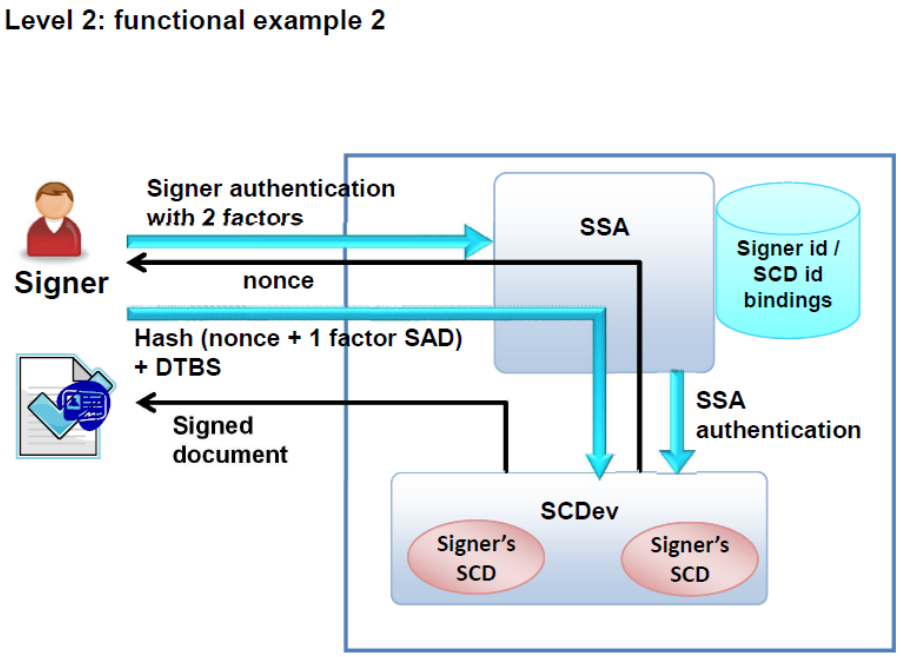
Вариант 2.2: Мультифакторная аутентификация между подписантом и устройством аутентификации, которое далее извлекает и передает данные активации подписи и передает их на устройство создания подписи

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 (4/4)

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

SBERBANK
CYBER SECURITY TEAM
SECURITY DEPARTMENT
SCST

Вопросы?

Александр Владимирович Бродский

Управляющий директор Департамента безопасности ПАО Сбербанк

AVBrodsky@sberbank.ru