SCS SBER CYBER SECURITY

Практика применения удаленной электронной подписи в РФ. Риски «безоблачного» будущего

А.И. Качалин

Управляющий директор
Управление криптографии, аутентификации и идентификации
ПАО Сбербанк

2021: 10 лет великой облачной развилке

Какая сейчас есть подпись:

– Дистанционная

Какой должна стать подпись:

– Дистанционная (облачная)
– Мобильная
– ПЭП ЕПГУ
– Биометрия
– УНЭП, квази-УКЭП на ЕПГУ

Технологическая реализация:

– Криптопровайдеры
– TPM
– Аппаратные криптографические токены – smart-карты, USB-токены, HSM
– SIM-карты
– Server Side Signature (подпись на сервере)

Нет полностью легитимных сервисов мобильной и удаленной подписи для всех сценариев

Выбор любого из (всех) вариантов лучше, чем отсутствие решения

Низкое проникновение технологии

Попытка внедрения заменителей (ПЭП, биометрия)

Риски мошенничества при реализации сервисов и услуг (в т.ч. УЦ)

Введение ограничений, централизация (сокращение АУЦ, «единые платформы»)

Мировая тенденция: получение госуслуг через коммерческие каналы*

Коммерческие организации могут подавать заявления на юридически значимые государственные услуги и вносить запись в информационные реестры

Жизненные ситуации

- Подача налоговой декларации
- Регистрация бизнеса
- Запись медицинских данных
- Запись образовательных данных
- Чтение медицинской истории
- Чтение образовательных данных
- Проверка налогового статуса
- Данные об автомобиле
- Детали о собственности

рынок ЭП 14.1 млрд дол. к 2026 году**

Госуслуги

важность которых определяется коммерческим клиентским путем, **отдаются на реализацию бизнесу**

Бухгалтерские, налоговые агентства, банки, агентства по бизнес-обслуживанию, образовательные и медицинские учреждения, страховые фирмы, автодилеры, риелторы и пр.

* McKinsey, 2021.
** MarketsandMarkets, 2020.

Мировая практика применения электронной подписи

SCS SBER CYBER SECURITY

Случаи применения подписи		Частотность сценария / жизненной ситуации использования ЭП[1]	Бразилия	ОАЭ	Эстония	Казахстан	Швеция	UK	Австралия	Беларусь
Общие	Коммерческие соглашения[2]		ES ✓	ES ✓	ES ✓	ES ✓	ES ✓	ES ✓	ES ✓	ES
	HR-документы[3]		ES ✓	ES ✓	ES ✓	ES	ES ✓	ES ✓	ES ✓	ES
	Лицензионные соглашения на ПО		ES ✓	ES ✓	ES ✓	ES	ES ✓	ES	ES ✓	ES
	Договоры аренды, лизинга		ES	Руч.	ES ✓	QES	ES ✓	ES ✓	ES ✓	ES
	Подача заявлений для получения госуслуг		ES	ES ✓	ES ✓	ES	ES ✓	ES ✓	ES ✓	ES ✓
	Пользовательские, клиентские соглашения		ES	ES ✓	ES ✓	ES ✓	ES ✓	ES ✓	ES ✓	ES
Высокорисковые регулируемые случаи	Нотариально заверенные документы		Руч.	Руч.	Руч.	QES	Руч.	QES	Руч.	QES[5]
	Передача, покупка недвиж. имущества		Руч.	Руч.	Руч.	Руч.	QES	QES	QES	Руч.
	Брачные соглашения		Руч.	Руч.	QES	QES	QES	QES	QES	Руч.
	Наследование		Руч.	Руч.	Руч.	QES	Руч.	QES	QES	Руч.
	Трудовые договоры		Руч.	Руч.[4]	QES	QES	ES	ES ✓	ES ✓	Руч.
	Учредительные документы		Руч.	Руч.	Руч.	Руч.	Руч.	Руч.	QES	QES[5]
	Передача или залог акций		Руч.	Руч.	Руч.	Руч.	Руч.	Руч.	QES	Руч.
	Трансфер интеллектуальной собств.		Руч.	Руч.	Руч.	Руч.	QES	QES	Руч.	Руч.
	Права на использование интеллектуальной собственности		Руч.	ES ✓	ES ✓	QES	ES ✓	ES ✓	ES ✓	Руч.
	Использование товарных знаков		Руч.	ES ✓	Руч.	QES	ES ✓	ES ✓	ES	Руч.

Частота использования, кол-во подписей в течение жизнь

Руч. — Требуется ручная подпись

QES — Требуется квалифицированная эл. подпись

ES — Достаточно усиленной или простой электронной подписи

✓ — Чаще достаточно только SES (простая электронная подпись)

1 В среднем по рассмотренным странам
2 Коммерческие соглашения – например, заказы на закупку, подтверждения заказов, счета-фактуры, соглашения о продаже, соглашения о предоставлении услуг, соглашение о неразглашении
3 HR-документы – соглашения о неразглашении информации, уведомления о конфиденциальности, документы о льготах и другие документы, подписываемые новыми сотрудниками
4 Кроме трудовых договоров, которые необходимо подать в органы власти ОАЭ
5 С копией в бумажном виде с ручной подписью

Сценарий «Приобретение автомобиля» согласно принципам «Невидимого государства»

Для обеспечения высокого качества клиентского опыта страны-пионеры реализуют принцип невидимого государства

- Государственные сервисы
- Сервисы частных провайдеров

Сценарий «Приобретение автомобиля»

«Взгляд государства»

Регистрация транспортного средства

Оформление парковки

«Взгляд пользователя»

Выбор автомобиля

Получение кредита на покупку автомобиля

Покупка автомобиля

Регистрация транспортного средства

Прохождение техосмотра

Оформление страховки

Покупка аксессуаров для автомобиля

Оформление разрешения на парковку

Приобретение транспондера и пополнение лицевого счета для проезда по платным трассам

Мой автомобиль

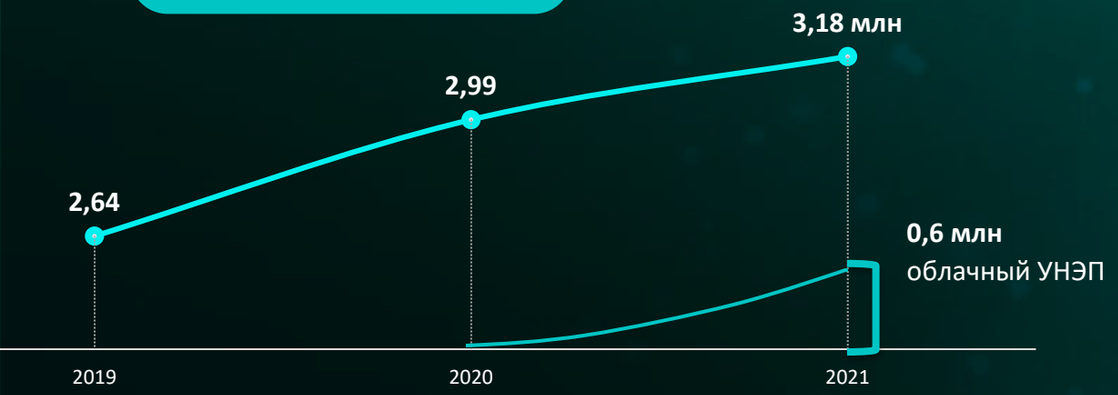
Принцип «Невидимого государства»

Встраивание государственных сервисов в коммерческие платформы, для обеспечения наилучшего пользовательского опыта

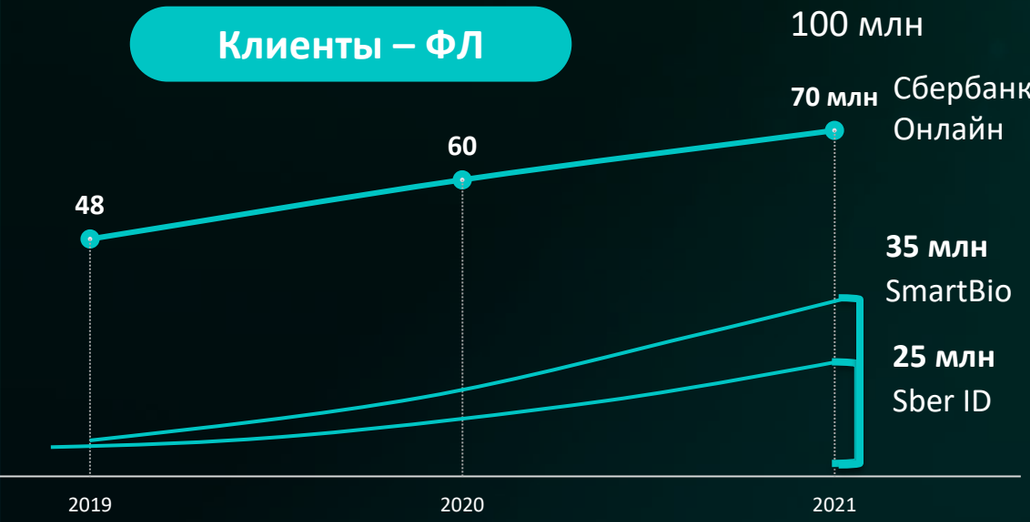
ЭП в удаленных каналах обслуживания

SCS SBER CYBER SECURITY

Клиенты – ЮЛ

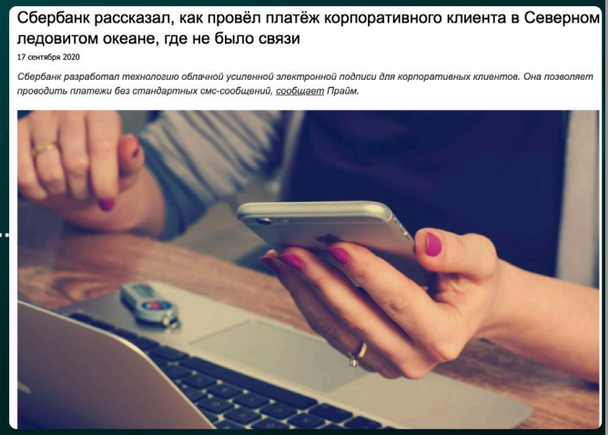


Клиенты – ФЛ



Юридические лица:

- Высокая доля клиентов в дистанционных каналах обслуживания
- Высокий потенциал проникновения электронной подписи
- Сохранить существующий уровень взаимодействия в дистанционных каналах
- Потребность в мобильности руководителей


Сбербанк рассказал, как провёл платёж корпоративного клиента в Северном ледовитом океане, где не было связи

17 сентября 2020

Сбербанк разработал технологию облачной усиленной электронной подписи для корпоративных клиентов. Она позволяет проводить платежи без стандартных смс-сообщений, сообщает Прайм.

Физические лица:

- Высокая доля клиентов в дистанционных каналах
- Высокая потребность в выполнении юридически значимых действий, в том числе с государственными органами (нужна УКЭП)
- Полностью дистанционное обслуживание клиентов
- Выполнение phygital-операций

Тенденции регулирования: ограничения и нагрузка на бизнес

	Было 2011-2020	**Стало** 2021	**Тенденция**
УКЭП Доверенный инструмент, аккредитованные операторы	**≈ 500** комм. УЦ **5** подзаконных НПА **2** регулятора Минцифры, ФСБ	**3** гос. УЦ **≈20** комм. УЦ **> 30** подзаконных НПА **5** регуляторов Минцифры, ФСБ, ЦБ, ФНС, Казначейство	Гос. монополизация УЦ и платформ подписания ФНС, ПЭП ЕСИА, ЕЦПП Необоснованное вмешательство в бизнес-взаимоотношения Не оценивается стоимость реализации мер, оценка эффекта
УНЭП Гибкий инструмент, правилами и рисками управляет бизнес		Вводится регулирование УНЭП (476-ФЗ)	
ПЭП Компонент бизнес-системы (логин / пароль)		Требования по защите каналов (для выдачи УНЭП) (476-ФЗ)	

Риск разрушения работающего, отрегулированного сегмента (ЭП)

Переход на отечественные решения и сервисы после апробации в государственных системах и сервисах

«DDoS» систем доверия: синтетическая цифровая личность

Синтетическая цифровая личность (СЦЛ) – цифровая личность, создаваемая злоумышленником, с использованием как реальной, так и вымышленной информации для совершения мошеннических действий в отношении физических, юридических лиц или органов государственной власти

Методы создания цифровой личности:

- Фабрикации личности – личность создается на основании полностью вымышленных данных без использования реальных ПДн
- Модификация личности – личность создается путем клонирования существующей личности с внесением небольших изменений
- Компиляция личности – личность создается из комбинации реальных и вымышленных ПДн

Создание вымышленных атрибутов цифровой личности (примеры):

- Генерация комплекса атрибутов цифровой личности ФИО, идентификаторы, адрес, биографические и контактные данные и прочее (https://www.fakenamegenerator.com/advanced.php)
- Генерация идентификаторов ИНН, ОГРН, КПП, СНИЛС и других по известному алгоритму (http://mellarius.ru/random-inn)
- DeepFake - Генерация фото, видео, голоса, отпечатков пальцев нейросетевыми алгоритмами (https://thispersondoesnotexist.com)

Доступность методов генерации атрибутов цифровой личности позволяет быстро создавать цифровые личности в больших количествах для совершения противоправных действий массового характера

Попытки реализации угроз – вопрос времени

SCS SBER CYBER SECURITY

Сейчас:

85 млн в ЕПГУ/ЕСИА
160 тыс. в ЕБС
1 млн УКЭП ФЛ
Пилотные фин.сервисы

ЧТО ПОД РИСКОМ?

Будет (ЕЦКИ, СЭР-2030):

100 млн в ЕПГУ/ЕСИА
20 млн в ЕБС
70 млн ЭП
Все массовые комм. и гос. сервисы

УГРОЗЫ

ДЛЯ ГОСУДАРСТВА

Нанесение финансового ущерба
- Неправомерное получение выплат, пособий, компенсаций на СЦЛ
- Отмывание денег и уклонение от уплаты налогов через сделки с СЦЛ

Нарушение / приостановка деятельности
- Массовая регистрация заявок, жалоб и обращений от СЦЛ

Нанесение ущерба репутации
- Влияние на новостную повестку, создание искусственного ажиотажа множеством синтетических личностей
- Снижения доверия к государственной системе цифровой идентификации из-за СЦЛ

Влияние на политическое устройство
- Участие СЦЛ в голосованиях, референдумах, петициях

ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ

Нанесение финансового ущерба
- Оформление невозвратных кредитов, займов, рассрочек
- Трудоустройство «мертвых душ»
- Мошенничество при договорных отношениях с СЦЛ или юр.лицом,

Нарушение / приостановка деятельности
- Массовая регистрация заказов / обращений от СЦЛ
- Массовые регистрация жалоб в проверяющие органы от СЦЛ

Нанесение ущерба репутации
- Массовая публикация негативных отзывов
- Ассоциация юр.лица с негативным или нежелательным контекстом через ассоциацию с СЦЛ

ДЛЯ ФИЗИЧЕСКИХ ЛИЦ

Нанесение финансового ущерба
- Мошенничество при сделках с СЦЛ или юр.лицами, зарегистрированными на СЦЛ.
- Получение услуг, имущества или денежных выплат, предназначенных реальной личности, СЦЛ на правах представителя («синтетические родственники»)

Нанесение ущерба репутации
- Ассоциация физ.лица с негативным или нежелательным контекстом через ассоциацию с СЦЛ

Риски стратегии «единственной платформы» ЭП

SCS SBER CYBER SECURITY

Бизнес	• Невозможность обеспечить бесшовный клиентский путь в рамках жизненной ситуации • Дискриминация доступа к государственным сервисам прочих платформ • Дополнительная нагрузка на бизнес – тарифы платформы-монополиста • Отсутствие альтернатив
Технологии	• Усложнение клиентского пути, дополнительные ограничения по устройствам и ПО пользователей • Отсутствие равных условий по качеству сервиса, скорости обновлений • Требования к платформе – 99,99% uptime, зависимость от СМЭВ, ЕСИА, ЕБС. Отказ (недоступность) любого из указанных компонентов является критичным
Кибербезопасность	• Единая система обработки конфиденциальной информации (банковской и коммерческой тайны), персональных данных клиентов • Взрывной рост попыток мошеннических действий, рисков утечки информации • Сложность организации процесса реагирования на инциденты и расследования (распределен между цепочкой сервисов)
Развитие ЭП	• Использование одного решения. Переход от рынка к заказной разработке • Монополия, снижение скорости развития, рост технологического отставания, прекращение развития иных технологических решений и сервисов, коллективов

Направления развития рынка ЭП и технологий

Выполнение планов развития и <u>контроль выполнения</u>:

- выполнение положений стратегии Цифровой трансформации СЭР-2030, в том числе принципов концепции ЕЦКИ
- увеличение количества государственных и коммерческих сервисов, использующих ЭП
- увеличение использования ЭП как органичный результат востребованности технологии бизнесом и гражданами

Потребность в регулировании:

- нормативно предусмотреть способы прохождения аккредитации УЦ в целях легитимизации применения существующих средств дистанционной подписи
- определить требования к применению технологий мобильной подписи для всех участников рынка
- закрепить на законодательном уровне равные возможности доступа всем участникам рынка к государственным сервисам для реализации коммерческих сервисов, в состав которых входят государственные услуги
- обеспечить возможность реализации бесшовного клиентского пути – связывание КомID и ЕСИА-ID, для реализации коммерческих сервисов, в состав которых входят государственные услуги
- избегать внесения точечных поправок в отраслевые нормативные правовые акты (ФЗ о дистанционном заключении договоров связи, ипотеке и т.п.), разрешающих в коммерческих правоотношениях отдельные сценарии использования «подмены», установленных на уровне действующей нормативной правовой базы, криптографических технологий ЭП иными менее надежными технологиями

Распределенное развитие сервисов ЭП позволит расширить базу пользователей, увеличить количество подключенных сервисов при контролируемом уровне риска

SCS SBER CYBER SECURITY

Практика применения удаленной электронной подписи в РФ. Риски «безоблачного» будущего

А.И. Качалин

Управляющий директор
Управление криптографии, аутентификации и идентификации
ПАО Сбербанк