ГАЗПРОМБАНК

Аутентификация и электронная подпись

Горленко С.А.

Предпосылки

Цифровая трансформация общества

Электронные сервисы повсеместно интегрировались в нашу жизнь. Высокая конкуренция между смежными сервисами

Легкий клиентский опыт

Низкий уровень киберграмотности массового потребителя. Сложился стереотип защищённости, отсутствия существенных последствий при взломе и легкости восстановление аутентификационных данных

Опыт применения ЭП

В основном применяется в системах ДБО как частном случае ЭДО. Культура использования ЭП физическими лицами не развита, отсутствует понимание тяжести возможных последствий при компрометации ключей ЭП

Развитие цифровых гос. сервисов

Развитие электронных сервисов приводит к повышению значимости действий в цифровой среде и увеличению тяжести последствий при компрометации (например, резонансные случаи переоформления недвижимости).
Примеры:

- эксперимент правительства – ЭП в трудовых договорах;
- ЭП на портале ФНС;
- ЕСИА.

Преимущества облачной ЭП

Препятствия распространению применения «классической» ЭП

- Частая потеря и компрометация ключей ЭП как следствие низкой киберграмотности физических лиц и отношения к ключам ЭП как учётным данным интернет магазина
- Высокая стоимость обслуживания и логистики (выпуск, плановый и не плановый перевыпуск)

Решение Использование облачного хранилища ключей ЭП

Безопасность

Приемлемый уровень защищенности использования ЭП при низком уровне киберграмотности подписанта за счет использования защищенного облачного хранилища и усиленной аутентификации физических лиц при доступе к ключам ЭП

Простота и мобильность

Простота использования в повседневных операциях влияет на положительный клиентский опыт – увеличивает прибыль Банка.

Повышение мобильности руководителей за счет сохранения контроля и возможности совершения юридически значимых действий с использованием облачной ЭП в любое время и месте, в том числе за рубежом (нет проблем с трансграничной передачей ключей ЭП и СКЗИ)

Возможность применения облачной ЭП

Правовая база

ФЗ от 27.12.2019 N 476-ФЗ «О внесении изменений в федеральный закон «Об электронной подписи» …» расширил возможности по применению облачной ЭП:

- устанавливает возможность УЦ по хранению ключей ЭП субъектов и созданию ЭП с использованием этих ключей по поручению владельцев соответствующих сертификатов ЭП;
- устанавливает возможность УЦ по удаленной идентификации субъектов при выдаче сертификатов ЭП.

Технологии

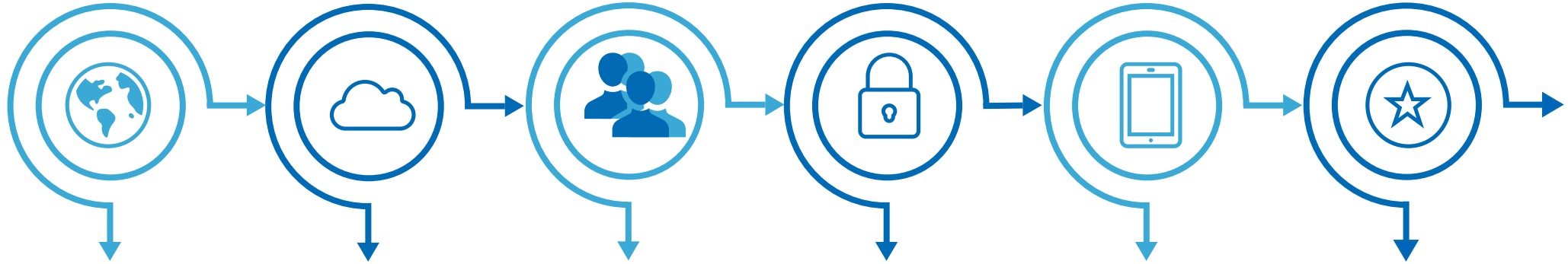
На рынке представлено решение, обеспечивающее возможность реализации облачной ЭП - ПАК «КриптоПро DSS».

Основные компоненты решения:

- КриптоПро DSS – ядро системы, обеспечивающее предоставление сервисов создания пользователей, ключей, ЭП и т.д.;
- КриптоПро HSM – обеспечивает защищенное хранение ключей ЭП владельцев сертификатов ЭП в неизвлекаемом виде;
- КриптоПро MyDSS – обеспечивает усиленную аутентификацию владельцев сертификатов ЭП с использованием векторов аутентификации при получении распоряжений на подписание, а также визуализацию подписываемого документа.

Облачная электронная подпись на базе ПАК «КриптоПро DSS»

Удобно, современно, безопасно, технологично



Из любой точки планеты

Удалённая биометрическая идентификация и получение КЭП без посещения офиса

Работа в облаках

Работает в Интернет и мобильном банкинге, системах ЭДО, виртуальных рабочих средах

Для клиентов и сотрудников

Применяется для ФЛ и ЮЛ. Возможно использование для сотрудников внутри компании

Безопасно и современно

Отображение информации об ЭД. Использование современных технологий и соответствие требованиям

Удобно

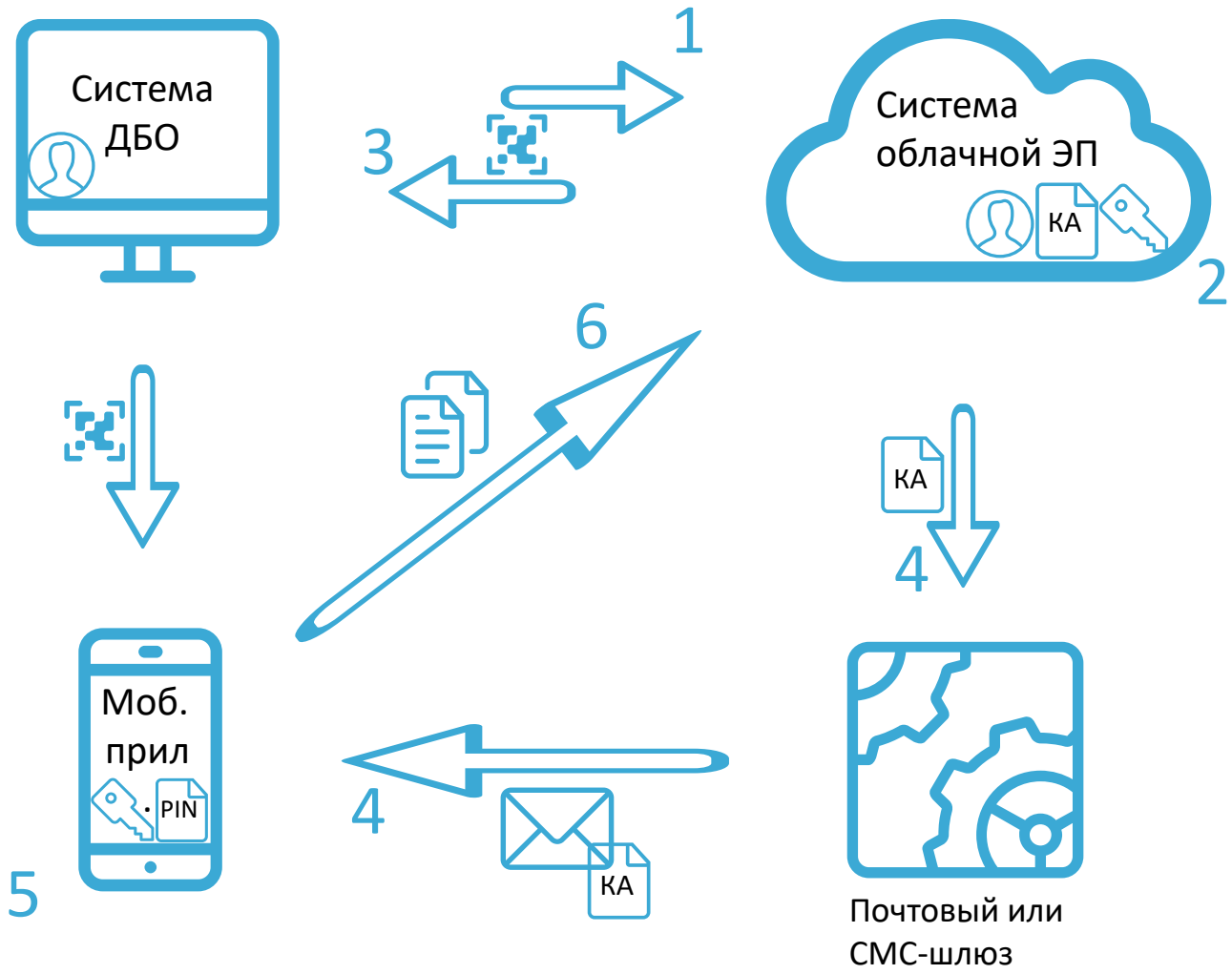
Подтверждение операций с мобильных устройств в одно нажатие. Понятный интерфейс

Выгодно

Не требует покупки физических носителей для ключей ЭП и их доставки пользователю

Как получить облачную ЭП

Регистрация пользователя облачной ЭП



1 **Запрос на регистрацию пользователя**

Из системы ДБО в систему облачной ЭП направляется информация о новом пользователе

2 **Регистрация нового пользователя**

В системе облачной ЭП регистрируется новый пользователь, для которого формируется вектор аутентификации (ВА) и соответствующий код активации (КА)

3 **Отправка QR-кода**

ВА передается в виде QR-кода пользователю (через ДБО, по электронной почте или в печатном виде)

4 **Отправка кода активации**

КА отправляется на электронную почту или по СМС на зарегистрированный номер мобильного телефона

5 **Установка вектора аутентификации**

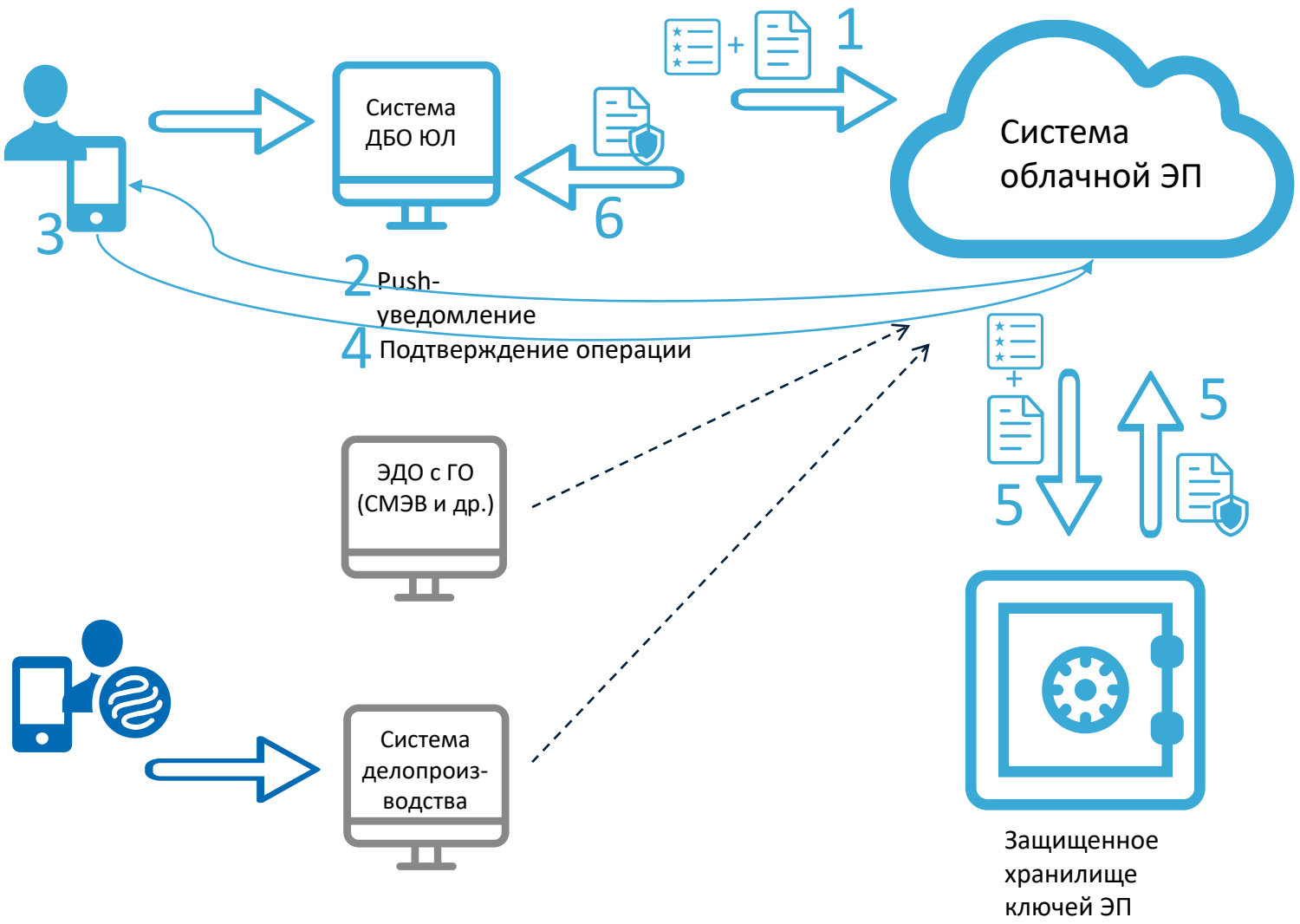
Пользователь сканирует QR-код, вводит КА и устанавливает PIN-код или биометрическую защиту (Face ID/Touch ID) на ВА

6 **Завершение регистрации пользователя**

Мобильное приложение отправляет в систему облачной ЭП сообщение об успешной регистрации устройства пользователя и отпечаток данного устройства

Применение облачной ЭП в Банке

Подтверждение подписания ЭД с мобильного устройства



1 Передача документа на подпись

В ДБО пользователь инициирует подписание ЭД. ЭД с сертификатом и параметрами ЭП направляется в систему облачной ЭП

2 Формирование и отправка запроса на подтверждение подписания документа

Система облачной ЭП формирует запрос на подтверждение подписания ЭД, включающий основные параметры ЭД. Запрос направляется в МП в виде push-уведомления

3 Подтверждение подписания документа

Пользователь подтверждает запрос подписания ЭД в МП. МП передает в систему облачной ЭП хеш, вычисленный от подтверждаемой операции с использованием ВА

4 Проверка корректности подтверждения

Система облачной ЭП проверяет полученное из МП подтверждение подписания ЭД (повторяет вычисления, выполненные в МП)

5 Передача документа на подписание

Система облачной ЭП обращается к защищенному хранилищу ключей для подписания ЭД

6 Подписание документа и передача его в ДБО

Подписанный ЭД возвращается в систему ДБО

Выводы

Несмотря на то, что мобильное устройство пользователя не является доверенной средой, используемая технология доступа к ключам ЭП, минимизирует угрозу компрометации ключей ЭП до приемлемого уровня

Использование облачного хранилища ключей ЭП позволяет оптимизировать процессы, связанные с обслуживанием сертификатов, и минимизировать затраты на логистику

Технология облачной ЭП позволяет интегрировать усиленную ЭП в те клиентские каналы обслуживания, где ранее использование усиленной ЭП не представлялось возможным из-за специфики бизнес-процессов (например, обслуживание массового сегмента физ. лиц), а также улучшить клиентский опыт в традиционных каналах

Существует высокий потенциал для использования инфраструктуры облачной ЭП для внутренних целей, не связанных с обслуживанием клиентов – облачная ЭП во внутренних системах документооборота и делопроизводства, отказ от ключей, подключаемых к серверам и т.п.