Мобильная квалифицированная ЭП «перевернет» банкинг

Фото: Safetech

Дарья Верестникова, директор по развитию продуктов компания SafeTech, рассказала «Банковскому обозрению», когда «умрут» СМС в финансовой сфере, что придет им на смену и в чем здесь интерес банков

Текст:
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Дарья, самым запоминающимся на конференции «Удаленная идентификация. Новые правовые реалии и возможности для банков» стало выступление представителя вашей компании. Почему?
— Мы говорили не только о технологиях мобильной электронной подписи (ЭП), но и о связанных с ними новых бизнес-возможностях для банков. Распространение digital привело к существенному развитию банковских сервисов, но появились и новые риски, поскольку развитие технологий ЭП и подтверждения в digital отставало от эволюции самих систем ДБО. В частности, обычная СМС — простая ЭП. Уровень ее защищенности соответствует названию. Перехват СМС и подмена SIM-карты — это реальные угрозы. Неслучайно судебная практика сейчас такова, что суды квалифицируют СМС как неперсонифицированное средство подписи, поскольку невозможно однозначно заявлять, что конкретный клиент ее получил и применил к конкретному платежу. Доступ к коду в СМС имеет и банк, который сформировал этот код, и оператор сотовой связи, не говоря уже о злоумышленниках.

— СМС небезопасно. Какие существуют альтернативы?
— Исторически для защиты транзакций используют одноразовые пароли в СМС (простая ЭП), а также ключи на USB-токенах и смарт-картах (усиленная ЭП). Между тем рынок сейчас развивается таким образом, что можно смело прогнозировать: СМС в финансовой сфере «умрут» в перспективе двух лет, поэтому продолжение их использования — однозначно тупиковый путь. Чуть дольше «продержится» передача одноразовых паролей через PUSH-уведомления, но больше в сфере обслуживания физлиц. Одноразовые пароли для юрлиц — это очень большой финансовый риск. В любом случае «перебивать вручную» их неудобно, не говоря уже о безопасности.

Взамен мы предлагаем использовать усиленную ЭП на мобильном устройстве — наше решение PayControl. Оно обеспечивает высокий уровень безопасности и юридическую значимость. Для клиента все выглядит очень просто. Созданная операция приходит клиенту в мобильное приложение с реквизитами и вложенными документами. Клиент проверяет операцию, после чего «прикладывает пальчик» в TouchID или вводит пинкод и нажимает кнопку «Подписать». Время на подтверждение такой операции — от трех секунд.

PayControl полностью блокирует распространенные атаки на клиентов систем ДБО, таких как перевыпуск SIM-карты, фишинг, подмена документа и др. Подпись транзакции «привязана» к реквизитам платежа и к мобильному устройству пользователя — попытки воспроизведения на другом устройстве ни к чему не приводят. Решение может быть полностью встроено в приложение мобильного банкинга. Поддерживаются мобильные платформы iOS (8.0+) и Android (4.0+). ЭП при этом формируется буквально «в пару касаний», что резко повышает удобство использования.

Нам удалось создать два варианта мобильной подписи: «облегченную» версию с неквалифицированной ЭП (для физических лиц и мелких юридических лиц), а также сертифицированный вариант облачной подписи, на которую буквально месяц назад было получено положительное заключение ФСБ России.

— Почему в «биометрических» поправках к Закону № 482-ФЗ оставлена возможность простой ЭП для аутентификации физических лиц?

— Изначально в Законе было предусмотрено использование только квалифицированной ЭП. Но на тот момент не было сертифицированных средств электронной подписи, которые подходили бы для массового рынка по таким критериям, как легкость распространения и мобильность использования, что могло негативно повлиять на результаты всего проекта. Юридическим лицам теоретически можно было бы выдать даже привычные всем USB-токены, но для физлиц это невозможно. Поэтому в последней редакции вынуждены были указать простую ЭП для физлиц. Изменения вызвали недоумение у специалистов по ИБ, но на тот момент поправки были «вынужденным» шагом, потому что не было сертифицированных облачных и мобильных решений. Теперь они у нас есть, и уже сейчас их можно использовать.

— Как же появилась квалифицированная ЭП в смартфоне?

— 14 февраля 2018 года было получено положительное заключение ФСБ России на решение КриптоПро DSS с модулем аутентификации myDSS, которое представляет собой совместную разработку компаний «КриптоПро» и SafeTech. Мы более двух лет вели разработку и сертификацию совместного решения, и на данный момент можно смело утверждать, что КриптоПро myDSS — это абсолютно уникальный на рынке продукт, настоящий прорыв в сфере информационной безопасности.

Серверная часть решения может быть как развернута в IT-инфраструктуре самого банка, так и использоваться по модели SaaS из облака «КриптоПро», что актуально для относительно небольших организаций. Безопасность платформы обеспечивается использованием сертифицированных аппаратных решений КриптоПро HSM, давно зарекомендовавших себя на рынке.

Квалифицированная ЭП позволяет предоставить клиенту банка новые удаленные сервисы, которые были невозможны ранее. Плюс к этому myDSS прекрасно ложится в популярную концепцию удаленной биометрической идентификации.

— Вы упомянули о новых возможностях, расскажите о них подробнее.

— Компания SafeTech «раскачивает» рынок уже более трех лет, с самого появления PayControl. За это время мы прошли путь от недопонимания до крайней заинтересованности банков и страховых компаний. Поэтому можем говорить не просто о «потенциальных» новых возможностях, а о «реальных» бизнес-кейсах. Сейчас у нас шесть проектов в банках из топ-10 на разных стадиях реализации и с различными нетривиальными кейсами помимо уже «классической» замены СМС.

Так, в одном из банков решение выходит на этап промышленной эксплуатации в версии для private-банкинга. Представьте себе: клиент позвонил персональному менеджеру и попросил перевести деньги водителю. Менеджер в фоновом режиме исполняет перевод. Ранее зачастую здесь возникали ошибки, и деньги уходили не туда. Решение PayControl, встроенное в приложение Private-банкинга, обеспечивает подтверждение перевода на смартфоне самим клиентом при нажатии кнопки «Подтвердить» или «Отвергнуть».

Сейчас прорабатываем варианты использования PayControl взамен 3-D Secure. Если раньше при оплате в Интернет-магазине использовались только СМС-подтверждения, то теперь клиенту в мобильное приложение приходит уведомление с кнопкой подтверждения. Также мы прорабатываем варианты с аутентификацией в банкоматах. В этом случае можно будет не иметь при себе карту или иметь виртуальную карту, но получать доступ к наличным деньгам при помощи мобильного приложения.

Одним из интереснейших и очень востребованных кейсов является «Безбумажный офис», когда клиент не подписывает бумаги, а подтверждает их юридически значимой электронной подписью на своем мобильном телефоне или планшете банка. Сейчас это особенно востребовано в кредитовании и страховании.

Подводя итоги, можно утверждать, что PayControl реализует массу полезных функций, позволяющих отказаться от СМС и сократить за счет этого затраты на услуги операторов связи, отказаться от аппаратных устройств и «пластика», минимизировать фрод, пополнить информацию о клиентах для маркетологов банка, что может привести к реальному «взрыву» на рынке digital. Б.О