БЕЗБУМАЖНЫЙ ОФИС И ПОДПИСЬ В СМАРТФОНЕ

КАК УПРОСТИТЬ ЖИЗНЬ КЛИЕНТУ, СНИЗИТЬ РИСКИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И ИЗБАВИТЬСЯ ОТ БУМАГ?

Беседовал: Дмитрий Груцо

Дарья ВЕРЕСТНИКОВА, коммерческий директор компании SafeTech

Последний год у всех банков постоянно возникают схожие вопросы, касающиеся стратегического развития цифровых каналов:

- **Как подписывать договоры с клиентами без бумаги, надежно и юридически значимо?**
- **Как снизить риски социальной инженерии?**
- **Как упростить работу клиентов в онлайне, сохранив при этом безопасность?**

А главное, как все это реализовать с использованием мобильных телефонов?

Так появилась большая востребованность в технологиях мобильной аутентификации и подписи в смартфоне.

В настоящее время возможность полноценной работы на мобильных устройствах, включая формирование подписи, стала неотъемлемым требованием к информационным системам и сервисам. Об особенностях «мобильной» подписи, безбумажных офисах и решении проблем социальной инженерии мы поговорили с Дарьей ВЕРЕСТНИКОВОЙ, коммерческим директором компании SafeTech.

NBJ: Дарья, расскажите, пожалуйста, зачем нужны средства электронной подписи в банках, и какие тенденции в их развитии сейчас существуют?

Д. ВЕРЕСТНИКОВА: Большинство банковских сервисов уже давно перешли в «мобильное» пространство. Люди получают возможность удаленно совершать различные действия, делать покупки и получать услуги. И неважно, кто является клиентом прикладной системы – организация или человек, работа на мобильном устройстве стала обычным делом. При этом, как и на стационарных компьютерах, мобильному пользователю также необходимо подтвердить не только свою личность, но и совершаемое действие. Для решения этой задачи лучше всего подходит электронная подпись (ЭП), реализация которой на мобильных устройствах и стала требованием времени.

Конечно же, технология электронной подписи должна быть:

- безопасной;
- удобной;
- юридически значимой;
- не очень дорогой.

Вроде бы очевидно, но тем не менее эти факторы не всегда просто собрать в одном решении, которое вдобавок работало бы на смартфоне или планшете. Классическим примером являются SMS-коды и USB-токены. Первые – абсолютно небезопасны и дороги, несут юридические риски, вторые – не обеспечивают достаточную мобильность и, к сожалению, имеют ряд ограничений с точки зрения цены и удобства использования.

NBJ: Дарья, а в чем проблемы кодов, передаваемых пользователю в SMS или PUSH?

Д. ВЕРЕСТНИКОВА: Привычный для всех SMS-код имеет целый ряд ограничений, начиная с того, что он никак не гарантирует ни целостность, ни авторство «подписываемого» с его помощью документа. Код подтверждает лишь то, что кто-то что-то когда-то совершил. И если эти «кто-то» и «что-то» совпали с действительностью – это большое везение! Например, судебная практика в России сейчас все чаще сводится к признаю SMS «неперсонифицированным» средством подтверждения. Помимо этого, использование SMS стало еще и дорогим!

Удорожание SMS привело к тому, что банки начали использовать PUSH-коды. На первый взгляд, это казалось оптимальным, и многие перешли на эту технологию. Эксперты в области безопасности называют такой вариант «профанацией электронной подписи». На сервере прикладной системы «сгенерировался» какой-то одноразовый пароль (OTP), он как-то был передан клиенту на смартфон, иногда даже сам за клиента «подставился» в интерфейс и сам «подписал» транзакцию. «Страшный сон» любого специалиста ИБ. И это мы еще не коснулись проблемы социальной инженерии.

NBJ: Расскажите подробнее о проблемах социальной инженерии, и как с ними бороться?

Д. ВЕРЕСТНИКОВА: Это очень серьезная проблема, которая настигла, прежде всего, простых граждан. Сколько бы банки ни предупреждали пользователей об опасности, все чаще мы слышим истории про то, как мошенник «выудил» у клиента код подтверждения и похитил деньги. Существует несколько наиболее массовых сценариев хищений, в которых клиента просят сообщить присланный код подтверждения.

Самый распространенный кейс – звонок якобы из службы безопасности банка.

Жертве сообщают, что ее счета подвергаются атаке и для отмены операции необходимо срочно сообщить код из SMS или PUSH. Или звонок из кредитного отдела банка для погашения задолженности. Таким образом, продиктовать мошеннику код в условиях стрессовой ситуации может даже очень осторожный клиент.

Почему же так происходит? В одной SMS и PUSH невозможно уместить все реквизиты платежа, чтобы человек сам видел, куда в действительности будут отправлены его деньги. Естественно, нужно работать с клиентами в части просвещения, но первоочередная задача – дать клиенту возможность обратить внимание на подозрительные действия мошенника без возможности сообщить вовне какой-либо код.

Поэтому вопрос обеспечения безопасности транзакций по-прежнему остается сложным, и его необходимо решать комплексно. В частности, мобильная аутентификация и подпись в смартфоне реализована таким образом, что там нет никаких кодов подтверждения, которые можно было бы кому-то сообщить, но есть полное отображение реквизитов операции и гарантия того, что именно эта операция будет исполнена на конкретном телефоне клиента.

NBJ: Дарья, расскажите, пожалуйста, что такое подпись в смартфоне? Чем она отличается от обычной, и в чем преимущество ее использования для клиента?

Д. ВЕРЕСТНИКОВА: Несколько лет назад мы представили рынку подпись в смартфоне PayControl, призванную закрывать все риски, существующие в SMS- и PUSH-подтверждениях, и позволяющую «превратить» мобильное устройство в аналог USB-токена с таким же высоким уровнем безопасности и очень простым пользовательским сценарием.

Сейчас PayControl – это полноценная платформа мобильной аутентификации и электронной подписи. При ее использовании обеспечивается эффективное противостояние наиболее распространенным атакам на клиентов систем ЭДО («перевыпуск» SIM-карты, фишинг, подмена документа, социальная инженерия и т. д.). Главный принцип – клиент видит реквизиты платежа на своем смартфоне и подтверждает их одним нажатием кнопки.

Сценарий работы пользователя очень прост:

- Клиент создает операцию в любом цифровом канале (мобильный банк, интернет-банк, платежная система и т.д.).
- Информация о об операции приходит непосредственно в мобильное приложение банка. Клиент проверяет информацию и подтверждает ее буквально «одним касанием» экрана. Волеизъявление клиента (действие, электронный документ, финансовая транзакция) подписывается в смартфоне и передается в прикладную систему.
- Если на смартфоне пользователя доступ к сети Интернет отсутствует (при нахождении, например, в роуминге, на промышленной территории, на складе, в подвале, и прочее), то в интерфейсе Интернет-банка генерируется QR-код, отражающий детали конкретной операции, который пользователь сканирует в мобильном приложении на своем смартфоне. На основе полученных данных на смартфоне генерируется «усиленный» код, которым клиент подтверждает свой платеж в Интернет-банке.

Если углубиться немного в технику, то хотелось бы отметить, что в основе PayControl лежит ассиметричная криптография. Закрытый ключ «рождается», «живет» и «умирает» в конкретном смартфоне – попытки воспроизведения ключа на другом устройстве ни к чему не приводят. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, ключ клиента, момент времени и «отпечаток» смартфона пользователя. Решение PayControl может быть полностью встроено в мобильное приложение банка. Даже если предположить, что злоумышленник как-то получит доступ к подписи, то он никак не сможет ее использовать для другой операции, на другом устройстве, в другое время.

NBJ: Получается, рынок ориентирован на мобильных пользователей, а как быть с классическими пользователями Интернет-банка?

Д. ВЕРЕСТНИКОВА: Конечно, концепция Mobile First – это тренд, но мы никогда не забываем о других каналах. Например, чтобы PayControl подписал на смартфоне документ, абсолютно не имеет значения,

в каком канале он был создан. Это может быть не только мобильный банк, но и Интернет-банк, отделение операциониста и даже банкомат. Важно то, что информация о совершенной операции приходит прямо в смартфон клиента, где он проверяет детали операции, подписывает полноценной электронной подписью.

NBJ: Мы слышали, вы создали возможность альтернативного входа в Интернет-банк через мобильное приложение без логина и пароля, и даже Markswebb высоко оценил нововведение?

Д. ВЕРЕСТНИКОВА: Совершенно верно. Совсем недавно с одним из банков из «топ 5» мы запустили самый масштабный проект для физических лиц, где реализовали не только подпись операций, но и вход в Интернет-банк через смартфон. Зачем? 70% пользователей мобильных приложений не помнит логин/пароль от Интернет-банка, а иногда появляется необходимость провести работу именно за компьютером, в спокойной размеренной обстановке. Что делать с такими клиентами?

На экране Интернет-банка вместо окна с логином и паролем отображается QR-код. Вы открываете мобильное приложение банка, подносите телефон к экрану, считываете QR-код, и Интернет-банк автоматически «проваливается» в личный кабинет! Ничего проще и быстрее и придумать нельзя

NBJ: А работает ли то же самое для банкоматов без пластика?

Д. ВЕРЕСТНИКОВА: Безусловно, аналогичную функциональность можно реализовать и для банкоматов. И для этого вам не требуется внедрять в банкоматы NFC – нужно лишь обновить ПО. На экране, по аналогии с Интернет-банком, появится QR-код, который клиент сканирует своим смартфоном и получает доступ к банкомату. Все действия в банкомате, будь то перевод или снятие наличных, клиент подпишет при помощи смартфона. Банк может даже выдать клиенту виртуальную карту, с которой клиент сможет снимать денежные средства и распоряжаться ими, не имея вообще пластикового аналога на руках.

И все это благодаря полноценной электронной подписи, которая формируется в мобильном устройстве клиента и может однозначно указать на конкретного пользователя и совершенное им действие и подписать любой тип волеизъявления.

NBJ: Получается, что мы можем не только заменить коды подтверждения и вход в Интернет-банк, но и решить одну из наболевших проблем – организацию безбумажного офиса и подпись договоров клиентами без бумаг?

Д. ВЕРЕСТНИКОВА: Конечно! Ваши клиенты смогут прямо со своего мобильного телефона подписывать любые договоры, которые раньше приходилось подписывать в офисе руками: от открытия новых счетов и карт, до оформления депозитов и кредитов. И это будет абсолютно безопасно и юридически значимо.

Банки тратят огромные средства на печать, подписание, хранение и логистику документов. Безбумажный документооборот значительно сокращает затраты Банка на коммуникацию с клиентами. И это намного проще, чем приходить в офис. А что клиенту еще нужно, если это экономит его время? Он навсегда останется с любимым банком.

Помимо ваших текущих клиентов, банки могут обслуживать клиентов без бумаг и в офисах. Клиенты будут работать на планшетах банков, где им при визите будет выдаваться временная электронная подпись для совершения операций в отделении. Все документы клиент будет подписывать не на бумаге, а на планшете, «тапая» по экрану. Перед уходом временная ЭП удалится, и клиент спокойно покинет отделение. Все подписанные электронные документы банк может направить клиенту в удобном виде, хоть на почту, и не переживать

за печать, хранение и логистику бумажных версий.

NBJ: Это действительно здорово! Насколько нам известно, у вас есть совместная разработка с компанией «КриптоПро» под названием «myDSS». В чем отличие этого решения?

Д. ВЕРЕСТНИКОВА: Нам удалось предложить рынку два решения для формирования «мобильной» подписи: «облегченную» версию, которая идеально подходит для обслуживания физических и юридических лиц, а также «полновесное» решение, востребованное в тех областях, где необходима квалифицированная электронная подпись (КЭП)

Решение для формирования КЭП называется myDSS и представляет собой совместную разработку компаний «КриптоПро» и SafeTech на базе программно-аппаратного комплекса облачной электронной подписи «КриптоПро DSS» и платформы PayControl. В прошлом году, 10 августа, на это решение был получен сертификат ФСБ России, и, по нашему мнению и мнению наших клиентов, – это настоящий прорыв для всего рынка информационной безопасности и цифровой экономики нашей страны.

Выбирая предложенные решения, очень важно понимать, что различным сегментам клиентов и наборам сервисов необходим разный уровень безопасности и юридической значимости. Например, при дистанционном обслуживании физлиц или небольшого бизнеса простой или усиленной неквалифицированной подписи может быть вполне достаточно, но для предприятий с государственным участием или тех, кто взаимодействует с госструктурами (сдача налоговой отчетности, регистрация юридических лиц и прочее), необходимо использовать сертифицированные средства электронной подписи и усиленную квалифицированную электронную подпись. Именно поэтому мы постарались одним решением закрыть все категории клиентов.

NBJ: Какие еще услуги банков становятся возможными на основе квалифицированной электронной подписи со смартфона?

Д. ВЕРЕСТНИКОВА: Мы уже запустили с банками ряд абсолютно новых удаленных услуг. Например, онлайн регистрация бизнеса с открытием расчетного счета. Банк один раз встречается с клиентом, пока тот еще «физик», выдает ему квалифицированную электронную подпись для смартфона, при помощи которой он подписывает все документы в налоговую на открытие бизнеса и «превращается» в «юрика». Ему перевыпускают ключ электронной подписи уже на юридическое лицо, он использует эту электронную подпись для открытия расчетного счета, доступа в ДБО, для подписи документа – для чего угодно! С помощью этой же подписи он может отправить отчетность в налоговую, этой же подписью может пользоваться на Госуслугах – где угодно! И вот этот идеальный «сквозной процесс», когда банк один раз посмотрел на клиента и предоставил ему все возможные сервисы, сейчас и реализуется.

На рынке уже представлены такие сервисы: удаленная регистрация бизнеса, сдача налоговой отчетности, система дистанционного банковского обслуживания, торги и Госзакупки прямо с мобильного телефона. Физические лица могут зарегистрировать недвижимость в Росреестре без необходимости установки дополнительного ПО и получения аппаратных средств ЭП.

Таких проектов с каждым днем появляется все больше и больше. Если у нас совместно с регулятором отрасли, совместно с удостоверяющими центрами, с ведущими производителями криптографических решений в России получится предоставить банкам технологии, которые помогут жителям страны экономить время, деньги, силы, то таких проектов станет еще больше, и мы сможем «оКЭПить» каждого жителя страны, чтобы он стал полноценным участником безопасного электронного взаимодействия. Если мы не будем сбавлять темп, через несколько лет каждый житель страны сможет не только удаленно брать кредиты и подписывать трудовые договоры, но и расписываться о получении стола из «Икеи» прямо со смартфона без использования бумаги!

NBJ: Мобильная аутентификация – это действительно тренд. Сколько сейчас банков уже использует эту технологию, и в какую сторону движется ее развитие?

Д. ВЕРЕСТНИКОВА: Очень много. Было инициировано более 50 проектов только за последний год. Такие уважаемые и крупные банки, как Сбербанк, ВТБ, Альфа-Банк, РСХБ, Промсвязьбанк и многие другие уже сотрудничают с нами в части мобильной аутентификации. Мы, будучи компанией – резидентом «Сколково», постоянно развиваем продукты и технологии. Уже сейчас это не просто «подписалка», это действительно воплощение нового класса систем. Мы еще 3 года назад говорили о том, что все «традиционные» и устаревшие способы аутентификации отойдут на второй план. Сейчас все так и происходит. Теперь мы вновь смотрим на несколько лет вперед и прекрасно понимаем, что «подписалки» даже с инновационными методами подписи скоро вновь окажется для заказчиков недостаточно. Поэтому мы активно развиваем решение, проводим интеграцию с различными системами обеспечения безопасности, в частности с биометрическими системами аутентификации и антифрод-системами. Это необходимо, например, для предоставления банкам возможности «адаптивной аутентификации», а также возможности еще большего повышения уровня безопасности и удобства для клиента. Интеграция с биометрическими системами позволит добавить дополнительные факторы аутентификации при совершении так называемых «высокорисковых» операций, а использование передовых антифрод-систем позволит «на лету», в момент совершения операции, оценивать риск ее подписи и работы пользователя на конкретном мобильном устройстве.

Таким образом, PayControl – это действительно полноценная платформа, которая позволит банкам, как кубики, собирать те функциональные возможности, которые им необходимо получить. Поэтому мы и говорим, что это – новый класс систем обеспечения безопасности транзакций, которые мы сейчас выводим на рынок, они будут «взрывать» его в ближайшие несколько лет. NBJ