«Мобильная» электронная подпись

Как предоставлять удалённо любые услуги и выдать КЭП каждому жителю страны?

Дарья Верестникова,
коммерческий директор
компании SafeTech

С самого начала 2019 года в среде специалистов в области информационных технологий, а также представителей бизнес-подразделений, ответственных за дистанционные сервисы и электронный документооборот, возник повышенный интерес к мобильной аутентификации и подписи в смартфоне.

Это и понятно: в настоящее время возможность полноценной работы на мобильных устройствах, включая формирование подписи, стала неотъемлемым требованием к информационным системам и сервисам. Об особенностях «мобильной» подписи, её внедрении и перспективах использования мы поговорили с Дарьей Верестниковой, коммерческим директором компании SafeTech.

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

Вся жизнь современного человека неуклонно переходит в «цифровое» пространство. И проявляется это не только в социальных сетях, играх и развлечениях. Люди получают возможность удалённо 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 пройти процедуру аутентификации (показать и доказать то, кем он является), а также подтвердить своё волеизъявление (сообщить и подтвердить то, что конкретно он хотел бы сделать). Самые современные инструменты решения первой задачи предоставляет Единая биометрическая система (ЕБС), а для решения второй задачи, по-прежнему, лучше всего подходит электронная подпись (ЭП), реализация которой на мобильных устройствах и стала требованием времени.

Конечно же, любая электронная подпись 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 для смартфона или планшета. Классическим примером являются SMS-коды и USB-токены. Первые – абсолютно небезопасны и дороги, имеют низкий уровень юридической значимости, вторые – имеют не всегда достаточную мобильность и, к сожалению, ряд ограничений с точки зрения удобства использования.

Дарья, а в чём проблемы кодов, передаваемых пользователю в SMS или PUSH?

Привычная для всех SMS-ка имеет целый ряд ограничений, начиная с того, что она никак не гарантирует ни целостность, ни авторство «подписываемого» с её помощью документа. Она говорит лишь то, что кто-то, что-то, когда-то подтвердил. И если эти «кто-то» и «что-то» совпали с действительностью – это большое везение! Например, российская судебная практика сейчас всё чаще сводится к признаю SMS «неперсонифицированным» средством подтверждения. Помимо этого, использование SMS стало ещё и дорогим!

Это привело к тому, что бизнес-подразделения банков и компаний, оказывающих услуги через Digital-каналы, стали искать выход и начали использовать Push-коды. На первый взгляд, это казалось оптимальным, и все повсеместно начали переходить на эту технологию. На ваш смартфон пришло Push-уведомление, содержащее код для подтверждения операции, и вам даже не нужно его подставлять в интерфейс мобильного приложения – он сам «подставится» и подтвердит транзакцию. Удобно? Да! Но вот безопасно ли? Конечно нет! Эксперты в области безопасности называют такой вариант «профанация электронной подписи». Почему они так говорят? На сервере прикладной системы «сгенерировался» какой-то одноразовый пароль (OTP), он как-то был передан клиенту на смартфон, как-то сам за клиента «подставился» в интерфейс и сам «подписал» транзакцию. «Страшный сон» любого специалиста ИБ.

Также существует ещё и проблема социальной инженерии, и сколько бы банки не предупреждали пользователей об опасности, всё чаще мы слышим истории про то, как мошенник «выудил» у клиента код подтверждения и похитил деньги. Почему же так происходит? Потому что невозможно в одной SMS уместить все реквизиты платежа, чтобы человек сам видел, куда в действительности будут отправлены его деньги. Поэтому вопрос обеспечения безопасности транзакций по-прежнему остаётся сложным, и его необходимо решать комплексно.

Но ещё хуже, что находятся банки, которые вообще перестали предусматривать какие бы то ни было процедуры подтверждения операций. То есть вы просто отправляете платёж, и для его проведения «подставляется» некий ID установленной сессии, даже без SMS и Push-кодов! Конечно же, такое «подтверждение транзакций» совсем не подходит для развития дистанционных услуг.

Благо, регулятор отрасли старается задавать правильный вектор обеспечения безопасности удалённых пользователей. В частности, Положение Банка России от 17 апреля 2019 г. N 683-П «Об установлении обязательных для кредитных организаций требований...» значительно повышает уровень безопасности транзакций, требуя от банков находить такие способы подтверждения, которые бы смогли обеспечить контроль целостности и авторства подписываемого документа. На данный момент это делает такие небезопасные способы подтверждения, как SMS и Push, неприменимыми при работе в дистанционных каналах.

Дарья, расскажите, пожалуйста, что такое подпись в смартфоне? Чем она отличается от «обычной», и в чём преимущество её использования для клиента?

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 её использовании обеспечивается эффективное противостояние наиболее распространённым атакам на клиентов систем ЭДО («перевыпуск» SIM-карты, фишинг, подмена документа, социальная инженерия и т.д.). Главный принцип – клиент видит реквизиты платежа на своём смартфоне и подтверждает их одним нажатием кнопки.

Сценарий работы пользователя очень прост:

- Информация о об операции приходит непосредственно в мобильное приложение банка. Клиент проверяет информацию и подтверждает её буквально «одним касанием» к экрану. Волеизъявление клиента (действие, электронный документ, финансовая транзакция) подписывается в смартфоне и передаётся 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 своём смартфоне. На основе полученных данных на смартфоне генерируется «усиленный» код, которым клиент подтверждает свой платёж в Интернет-банке.
- В основе PayControl лежит ассиметричная криптография. Закрытый ключ «рождается», «живёт» 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 или другого провайдера услуг.

Решение PayControl может быть полностью встроено в мобильное приложение банка. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, ключ клиента, момент времени и «отпечаток» смартфона пользователя. Даже если предположить, что злоумышленник как-то получит доступ к подписи, то он никак не сможет её использовать для другой операции, на другом устройстве, в другое время.

У Вас есть совместная разработка с Компанией «КриптоПро» под названием «myDSS». В чём отличие этого решения?

Нам удалось предложить рынку два решения для формирования «мобильной» подписи: «облегчённую» версию, основанную на неГОСТ-овых криптоалгоритмах, которое идеально подходит для обслуживания физических и небольших юридических лиц, а также «самое полновесное» решение, востребованное в тех областях, где необходима квалифицированная электронная подпись (КЭП).

Решение для формирования КЭП называется «КриптоПро 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 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 отчётности, 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.

Судя по тому, как Вы рассказываете, использование PayControl и myDSS выглядит для клиента очень просто. Разве может быть безопасность такой простой и почему это так сложно повторить?

Вы даже не представляете, насколько важный вопрос поднимаете! Очень часто, когда мы представляем свои технологии, возникает две типовые реакции потенциальных партнёров и заказчиков. Сначала говорят: «Это выглядит слишком просто, чтобы быть безопасным», а по мере ознакомления продолжают: «Действительно, очень простое решение – мы и сами такое же напишем за 2 недели».

Скажем честно, первая реакция нам даже нравится, она говорит об успешности наших разработчиков. Обычно безопасность накладывает свои ограничения, и удобство использования системы снижается. Есть даже расхожий стереотип, что «безопасность удобной быть не может». Тем не менее наши технологии разрабатывались с целью сделать работу пользователей и безопасной, и удобной. Для этого были затрачены отдельные усилия, и теперь простота использо-

вания наших решений – это конкурентное преимущество, которое выходит за рамки вопросов безопасности и вызывает неподдельный интерес со стороны бизнес-подразделений банков и компаний, оказывающих услуги через Интернет.

Фразы «напишем сами за 2 недели» говорят исключительно о поверхностном погружении в проблематику, поскольку кажется, что если выглядит просто для пользователя, то и сделать аналогичное решение не составит особого труда. Это глубоко ошибочное мнение. Специалисты, делающие такие заявления лишь по результатам первичного ознакомления с PayControl, вряд ли учитывают всю проблему целиком. За 2 недели нельзя даже сделать «видимость» PayControl, а уж разработать полноценное средство подписи – тем более. Поэтому я всегда призываю бизнес-подразделения и ИТ-подразделения банков смотреть «под капот». Не всё, что выглядит просто, является безопасным. Не всё, что выглядит как PayControl, позволит обеспечить ту же защиту дистанционных каналов. Если к вам приходит какой-либо разработчик и говорит, что сам произведёт похожее решение за короткий срок – не верьте сразу! Посмотрите внимательнее, отдайте это предложение на экспертизу своим специалистам по ИБ, отдайте своим юристам, посмотрите, как это будет работать в вашей инфраструктуре, соберите экспертное мнение. Обязательно! В платформе PayControl реализована полноценная электронная подпись на базе симметричной или ассиметричной криптографии, обеспечивается контроль целостности, контроль авторства и многое другое. Эта «простая» вроде бы технология лежит в основе решения MyDSS для мобильной аутентификации и формирования подписи с использованием «ГОСТ-овой» криптографии, которое имеет сертификат соответствия ФСБ России и досконально проверялось регулирующим органом.

Дарья, сейчас активно обсуждается Положение Банка России от 17 апреля 2019 г. N 683-П. Насколько PayControl «подходит» под данное постановление?

Выполнение требований этого Положения на данный момент вызывает много вопросов. Банки скрупулёзно анализируют и сами требования, и степень их выполнения в своих дистанционных каналах. В соответствии с пунктом 5.1., например: «Кредитные организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом». Решение PayControl, в частности, обеспечивает контроль целостности и авторства документа или транзакции. Выработка ЭП осуществляется с использованием закрытых ключей пользователей в их смартфоне на основе данных транзакции, значения времени и других опциональных параметров. При внесении изменений в подписываемые данные значение электронной подписи изменится. «Уполномоченное лицо» однозначно определяется соответствующим ему ключом и набором уникальных опциональных признаков, таких как отпечаток мобильного устройства.

Часто можно услышать, что PayControl не имеет аналогов. В чём уникальность?

PayControl – это платформа мобильной аутентификации и электронной подписи. Уже сейчас это не просто «подписалка», это действительно воплощение нового класса систем. Мы ещё 3 года назад говорили о том, что все «традиционные» и устаревшие способы аутентификации отойдут на второй план. Сейчас всё так и происходит. Теперь мы вновь смотрим на несколько лет вперёд 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 ещё 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 её 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 PayControl – это новый класс систем обеспечения безопасности транзакций, которые мы сейчас выводим на рынок, они будут развиваться в ближайшие несколько лет.

Дарья, Вы упомянули о биометрической и адаптивной аутентификации в PayControl. Расскажите, пожалуйста, об этих возможностях подробнее.

Постараюсь пояснить на примере. Если раньше смена номера телефона или самого мобильного устройства и, как следствие, смена ключа электронной подписи, словом, любая «высокорисковая» операция требовала жёсткого контроля и визита в офис банка с «физическим» подписанием бумаг, то сейчас это не требуется. Теперь в момент первичной регистрации с клиента «снимаются» биометрические данные, которые «складываются» в банк, и при каждой «высокорисковой» операции будет запрашиваться дополнительная идентификация, чтобы на всякий случай проверить клиента: он ли это совершает операцию или нет? Это и есть использование «дополнительных факторов биометрической аутентификации».

Адаптивная аутентификация – следующий шаг в развитии систем ДБО. Расскажу о ней на примере трёх сценариев подтверждения операций. Первый сценарий. Если проводится априори «хорошая» транзакция, например «типовая» или часто проводимая клиентом, то она подписывается без дополнительного подтверждения. Если транзакция так же «хороша», но по каким-то причинам требуется дополнительное

подтверждение (может быть актуально для юридических лиц), тогда это можно реализовать с помощью второго сценария, например дополнительного подтверждения Face ID или Touch ID. И третий сценарий – если операция очень рисковая или «Scoring» (интегральный показатель надёжности, выявленный антифрод-системой) у неё откровенно не заслуживает доверия, то проведение транзакции потребует формирования полноценной электронной подписи, причём пароль на использование ключа этой подписи задаётся в соответствии с очень жёсткими требованиями, так называемый «длинный пароль» – под стать риску этой операции. Таким образом мы закрываем риск того, что кто-то возьмёт ваше мобильное устройство, приложит ваш «пьяный палец» и похитит ваши средства.

Итак, когда мы анализируем поведение клиента в цифровом канале и решаем, можно или нельзя доверять его действиям, а затем в зависимости от результатов анализа просим его подписать транзакции различными способами, это и составляет суть адаптивной аутентификации. Тем не менее большинство бизнес-подразделений банков стремятся исключить запрос дополнительного подтверждения у физических лиц. Как это можно реализовать? Мы считаем, что это возможно только в интеграции с антифрод-системой. Если антифрод-система выдаёт свою оценку («Scoring»), которая подтверждает доверие этому человеку или этой операции, то возможно подписать эту операцию клиента или документ в автоматическом режиме. Причём это будет именно подпись, не подстановка какого-то непонятного идентификатора, а полноценная подпись. Только в таком случае мы можем быть уверенными, что противодействуем наиболее частым атакам злоумышленников.

Насколько это совместимо с использованием ЕБС?

Мы часто слышим про единую биометрическую систему. На использование ЕБС возлагают большие надежды. В банковской среде можно услышать даже такие «восторженные» ожидания: «У нас же есть Единая Биометрическая Система, теперь пользователям будет очень удобно – лицо приложил, и всё!» Особенность ЕБС на данный момент в том, что в составе этой системы нет средств электронной подписи. Поэтому возможности использования такой системы для подтверждения волеизъявления клиентов в настоящее время весьма ограничены. Как правило, речь идёт о предоставлении банкам возможности удалённой идентификации физических лиц с последующим удалённым открытием счёта. Но для того, чтобы дать даже такую возможность юридическим или физическим лицам проводить значимые транзакции, подписывать юридически значимые электронные документы и полноценно взаимодействовать с государством, нужна квалифицированная электронная подпись.

Многие эксперты предлагают использовать ЕБС для удалённой идентификации пользователей при выдаче квалифицированной электронной подписи. Сейчас по требованиям законодательства эта идентификация должна проходить очно, но уже есть соответствующие законопроекты. Когда мы технологически и законодательно придём к тому, что у каждого пользователя будет возможность получить на свой смартфон инструменты формирования квалифицированной электронной подписи удалённо, то использование ЕБС станет массовым, а удалённое получение цифровых услуг – действительно удалённым.

Какие ещё услуги банков становятся возможными на основе квалифицированной электронной подписи со смартфона?

Мы уже запустили ряд абсолютно новых удалённых услуг. Например, онлайн регистрация бизнеса с открытием расчётного счёта. Банк один раз встречается с клиентом, пока тот ещё «физик», выдаёт 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 расчётного счёта, доступа в ДБО, для подписи документа – для чего угодно! С помощью этой же подписи он может отправить документы 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: удалённая регистрация бизнеса, сдача налоговой отчётности, 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 днём появляется всё больше и больше. Если у нас совместно с регулятором отрасли, совместно с удостоверяющими центрами, совместно с ведущими производителями криптографических решений в России получится предоставить банкам технологии, которые помогут жителям страны экономить время, деньги, силы, то таких проектов станет ещё 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 удалённо брать кредиты и подписывать трудовые договоры, но и расписываться о получении стола из «Икеи» прямо со смартфона без использования бумаги!

SafeTech
SAFETY TECHNOLOGIES

SafeTech *– российский разработчик инновационных решений для защиты систем дистанционного банкинга и электронного документооборота.*

www.safe-tech.ru