Актуальные вопросы
доверия к PKI и неактуальному Закону № 63-ФЗ

Сергей МУРУГОВ,
генеральной директор ООО «Топ Кросс»

Как известно, Российская Федерация давно является участником Таможенного Союза, который, в свою очередь, уже успел трансформироваться в Евразийский Экономический Союз (ЕАЭС). Поэтому, наверное, пора серьезно задуматься о переводе трансграничных транзакций во взаимной и внешней торговле в правовое поле. Более того, товарооборот РФ далеко не ограничивается странами ЕАЭС, в идеале уже сегодня необходимо предусматривать использование в ближайшем будущем механизмов, гарантирующих законность и прозрачность транзакций, например при торговле со странами ЕС. Однако ситуация такова, что проблемы с применением электронной подписи остаются не только в международном обмене, но даже на внутреннем российском рынке.

Организация доверенного электронного экономического пространства имеет множество аспектов и немало проблем. В данной статье рассмотрим только одну из них – Закон № 63-ФЗ от 8.04.2011 «Об электронной подписи», проанализировав отдельные его положения. Что касается трансграничных транзакций, то эксперты признают лучшим вариант, когда каждая из сторон работает по правилам своей, локальной юрисдикции, проверяя подписи партнерской стороны, работающей в чужой юрисдикции. И эффективность российского законодательства в лице Закона № 63-ФЗ – первая проблема, с которой мы сталкиваемся. Посмотрим на данный Закон со стороны не удостоверяющих центров, а собственно бизнеса и попытаемся понять, почему Закон так и не заработал. На наш взгляд, основная причина в том, что применение его крайне некомфортно и рискованно для реального бизнеса. Заставить им пользоваться можно только путем законодательного принуждения – посредством других, подзаконных нормативно-правовых актов. Попытаемся разобраться, почему так произошло.

Разрешение передачи закрытого ключа PKI

Прежде всего следует отметить, что применение норм Закона в его нынешнем виде и их техническая реализация вовсе не так безопасны, как многие уверяют. Дело в том, что в PKI авторство (даже без учета проблем, связанных с идентификацией субъекта) и неотрекаемость от подписи обеспечиваются исключительно через единоличное владение – управление собственным закрытым ключом. После того как закрытый ключ переходит в другие руки (не важно, обеспечено требование «конфиденциальности» такой передачи или нет), технически становится просто невозможно определить, кто именно выработал подпись – сам владелец сертификата или другое лицо. Печальные последствия законодательного «разрешения передачи закрытого ключа» усугубляются еще и тем, что средства подписи (сертифицированные, между прочим) не обязаны обеспечивать неизвлекаемость закрытого ключа из своего хранилища. Говоря простым языком, закрытый ключ можно скопировать штатными средствами и впоследствии использовать копию (или копии) наравне с оригиналом. Напомним, в других странах передача закрытого ключа запрещена, а его незаконное использование карается весьма сурово, включая уголовную ответственность. Невозможно понять, зачем норму по передаче ключей вообще вложили в Закон, ведь она сама по себе совершенно нелогична. Здесь уместно провести аналогию с обыкновенной жизнью: получая деньги за товарища по работе, никто не подделывает его подпись в зарплатной ведомости, а ставит свою подпись с указанием доверенности. В случае реализации действующей редакции Закона № 63-ФЗ для бизнеса появляется огромный риск того, что партнер запросто может «пойти в отказ»

от договоренностей и втянуть бизнес в судебные тяжбы.

Сертификат юрлица

Сертификат юридического лица (не путать с европейской электронной печатью) – придумка Закона, заслуживающая отдельного рассмотрения. Напомним, что сертификат выдается на год, при том что генерального директора компании можно сменить за пять рабочих дней. Поддержка актуальности полномочий гендиректора в сертификате возложена на самого гендиректора, а он в ряде случаев может быть заинтересован в том, чтобы эту актуальность не поддерживать. Таким образом, мы получаем риски по оспариванию сделок, заключенных не уполномоченным на это лицом. Исходная причина: сертификат юрлица, используемый как инструмент для подтверждения полномочий, на самом деле плохо к этому назначению приспособлен. Та же самая задача совсем по-другому решается, например в Беларуси, где формула доверия к полномочиям выглядит следующим образом:
сертификат физического лица + самоактуализируемый токен полномочий = безопасный аналог российского сертификата юрлица.

В результате применения этих инструментов тот, кто их предъявил, становится гендиректором, главным бухгалтером и т. д. – как на бумаге. Попутно напомним, что в техническом плане реализация подобной схемы не представляет сложности – в РФ такие технические решения (инфраструктура управления привилегиями – PMI) давно имеются.

Электронная подпись втридорога

Использовать российскую электронную подпись на практике дорого. Во-первых, специальные сертификаты юрлица (за отдельные деньги) необходимо получать фактически под каждое назначение – ПФР, Росреестр,

Электронная торговая площадка. Во-вторых, средства подписи влекут денежные расходы, причем многократные, с периодом последующей покупки равным сроку действия сертификата ФСБ (а вот, например, в Польше удостоверяющий центр обязан бесплатно обеспечивать пользователей средством подписи). В-третьих, ежегодные затраты на российские сертификаты неадекватно велики. Так, одной компании сертификат для ЭТП обошелся более чем в 10 тыс. руб. в год (для сравнения: в ЕС стоимость сертификата составляет примерно 20 евро на три года).

Недосказанности и неоднозначные трактовки

Закон № 63-ФЗ изобилует недосказанностями и неоднозначными трактовками. Перечислим некоторые, самые очевидные.

1. Статья 6 декларирует, что ЭП равнозначна собственноручной подписи (включая и иностранную), но на практике это не работает. Любой бизнес в итоге замыкается на фискальные органы, а там включаются их собственные приказы, правила, регламенты, зачастую весьма непрозрачные и нелогичные. Появляются требования к конкретному виду подписи, ведомственные форматы документов, сообщений, форм представления самой электронной подписи. Например, электронные счета-фактуры: оказывается, счетами-фактурами можно обмениваться между контрагентами только через посредника в виде специального оператора и, разумеется, за деньги. Кроме того, бизнес должен самостоятельно хранить архивы электронных счетов-фактур. Если вспомнить, что ЭП имеет срок действительности равный сроку действия сертификата автора подписи, то возникает вопрос: как обеспечить доверие к ЭП после прекращения действия сертификата автора подписи? Что делать бизнесу, куда бежать, кому платить, чтобы не влететь на риски по непризнанию НДС?
2. Статья 14 п. 7 Закона гласит, что «информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена УЦ в реестр сертификатов

в течение одного рабочего дня». При этом нигде не сказано, кто отвечает за возможные убытки бизнеса в период от момента обращения в УЦ до фактического отзыва сертификата.

3. Статья 17 п. 7: «ограничения использования квалифицированного сертификата…» – неплохо было бы понять, что означает это самое ограничение, какие ограничения бывают и как это технически указывается в сертификате, в каком атрибуте или расширении и на основании какой технической спецификации? Другими словами: норма есть, а как ею корректно пользоваться?

> Бизнесу хотелось бы иметь не просто работающую инфраструктуру и средства идентификации и аутентификации для дистанционного взаимодействия.

4. В статье 7 п. 1 сказано, что «электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона». Кроме этого пункта ни в Законе, ни в одном подзаконном нормативно-правовом акте не говорится, как это реализовать технически и на основании чего этой реализации обязаны верить ФНС, ФТС и т. д. Ситуация такова, что возможность заключения международного е-договора продекларирована, и это вводит бизнес в заблуждение. Фактически существует огромный риск, что международный электронный договор, подписанный ЭП, не признают основанием для перевода денег за рубеж и российская сторона окажется лицом, замешанным в незаконном выводе денег из страны или ввозе/вывозе контрабанды.

О перспективах УЦ

Если бизнес опять не обманут в ожиданиях (как это уже было с универсальной электронной картой) и ФМС действительно начнет выпускать электронные удостоверения личности (е-паспорта), то для рынка УЦ останется только ниша сертификатов юрлица. По объему это всего 2–3 млн сертификатов в год, а то и в три года (сертифицированные средства, работающие с трехлетними сертификатами, уже давно есть на нашем рынке), обработать такой объем технически способен один удостоверяющий центр. В этой ситуации удостоверяющим центрам, чтобы сохранить свой бизнес, придется тянуть деньги из реального сектора экономики: за счет коротеньких по сроку жизни сертификатов, отдельных сертификатов различного назначения и тому подобных ухищрений, не имеющих никакой практической ценности ни для бизнеса, ни для потребителя.

Идеальным выходом для бизнеса было бы развитие событий по сценарию хотя бы той же Беларуси: сертификаты физлиц от ФМС и токены привилегий, которые могут (и должны) выпускать профильные ведомства, отвечающие за эти привилегия-полномочия по закону. Точно так, как они это делают и сейчас на бумаге. Например, ФНС: выписка из ЕГРЮЛ определяет полномочия гендиректора, останется только оформить такую выписку в виде электронной самоактуализированной сущности – и задачка решена.

Ожидания бизнеса

Бизнесу хотелось бы иметь не просто работающую инфраструктуру (один УЦ или миллион – бизнесу без разницы) и средства идентификации и аутентификации для дистанционного взаимодействия. Бизнес ожидает однозначно определенные, узаконенные базовые правила – примитивы более высокого уровня абстракции, чем просто электронная подпись. Это «штампы времени», «электронные выписки», «е-архивы», «доверенные средства доставки», «защищенные веб-сервисы», «сервисы валидации», «сервисы атрибутирования» – все то, что перечислено в пунктах раздела о доверенных сервисах новых европейских правил образца 2014 г. В ЕС поняли две главные вещи. Во-первых, сама по себе ЭЦП никому не нужна – необходимы инфраструктура ее использования, доверенные сервисы, из которых, как из кирпичей, можно построить ИС, автоматизирующую доверенным и, самое главное, законным образом процессы в реальном бизнесе. Во-вторых, необходимо создать правовые основы использования электронной подписи, одинаково работающие во всех странах ЕС. Вот поэтому и была отменена морально устаревшая Директива ЕС о подписи. Кстати, во многом Закон № 63-ФЗ списывали именно с этой отмененной Директивы. Следуя логике, Закон следует не исправлять и не дополнять, а отменить как не оправдавший ожидания и написать новый закон, вобрав все самое лучшее и нацеленное на результаты, главный из которых – комфорт и выгода для бизнеса. ■