Квалифицированная электронная подпись на мобильном устройстве.

Как технологиям взлететь и подняться под «облака»?

Подступиться к решению задачи реализации электронной подписи в «облаке» множество компаний пыталось с 2010—2011 года. В то время активно развивался проект «электронного правительства». Специалисты и пользователи услуг не без оснований ожидали, что большинство сервисов в этом проекте удастся реализовать в «облаке», что откроет возможности предоставления простых и удобных услуг, основанных, в том числе, на «облачной» электронной подписи, и для других проектов и областей жизни российского общества. Тем не менее, по разным причинам, электронное правительство было реализовано без электронной подписи в «облаке», и компания «Ростелеком» по-прежнему предлагает корпоративным и частным пользователям Госуслуг всем привычные токены. А между тем, технологии, которые все-таки могут обеспечить «взлет» идеи электронной подписи в «облаке», уже существуют и успешно внедряются.

Что такое электронная подпись и зачем ей нужно в «облако»?

Электронная подпись все больше входит в повседневную жизнь граждан и юридических лиц. По законодательству РФ (Федеральный закон от 06 апреля 2011 года №63-ФЗ «Об электронной подписи») электронная подпись является полноценной заменой рукописной подписи и обладает полной юридической силой. Обычным гражданам электронная подпись обеспечивает удаленное взаимодействие через Интернет с государственными структурами, учебными и медицинскими учреждениями. Компаниям и организациям она позволяет участвовать в электронных торгах, организовать юридически-значимый электронный документооборот, сдавать в электронном виде отчетность в контролирующие органы власти.

Традиционными и надежными носителями ключей электронной подписи являются электронные ключи — токен или смарт-карта — которые, будучи сертифицированными криптографическими средствами, должны подлежать строгому учету и выдаваться в строгом соответствии с правилами и требованиями регуляторов отрасли. При этом в среде заинтересованных специалистов неоднократно высказывалось смелое предположение, что если бы удалось найти другое решение и совсем избавиться от токенов, перейти на какую-нибудь «более простую для пользова-

>>info

В самом общем смысле электронная подпись является результатом криптографического преобразования электронного документа с использованием так называемого «ключа электронной подписи». Она позволяет однозначно определить лицо, подписавшее электронный документ, а также обнаружить факт внесения в него изменений уже после момента подписания. Создается электронная подпись с использованием так называемых «средств электронной подписи», которые могут быть сертифицированными (это является обязательным условием для формирования квалифицированной электронной подписью) или несертифицированными (используются для неквалифицированной электронной подписи).

С определенной долей упрощения можно говорить, что безопасность электронной подписи и сервисов, предоставляемых на ее основе, базируется на том, что ключи электронной подписи хранятся в секрете, в защищенном виде, и что каждый пользователь ответственно хранит ключ своей подписи и не допускает инцидентов. И поэтому, криптографические алгоритмы и протоколы, а также основанные на них программные и программно-аппаратные решения для формирования электронной подписи обеспечивают с использованием этих ключей требуемые свойства информации: целостность, достоверность, аутентичность (подлинность, неотказуемость).

Павел Мельниченко
Технический директор
SafeTech

Денис Калемберг
Генеральный директор
SafeTech

теля» технологию хранения ключей подписи, то количество юридических лиц и граждан, использующих электронную подпись, существенно бы увеличилось. В этой связи переход на «облачное» хранение ключей подписи давно представлялся экспертам перспективным решением. Эта идея постепенно становилась еще более актуальной по мере все более широкого распространения среди частных и корпоративных пользователей смартфонов и планшетных компьютеров, так как подключить к ним токен или смарт-карту — задача далеко нетривиальная. «Облачное» хранение ключей подписи представлялось весьма удобным решением для поклонников работы и получения информационных сервисов непосредственно на мобильных устройствах без дополнительных считывающих устройств — токенов и смарт-карт.

На самом деле сама по себе идея хранения ключа электронной подписи пользователя в «облаке», в каком-то суперзащищенном месте, например, в HSM (Hardware Security Module или как его еще называют в «аппаратном модуле безопасности») или где-то еще — эта идея далеко не нова. Более того, в корпоративной среде это довольно распространенная практика, поскольку опыт использования HSM для хранения закрытых ключей пользователей в корпоративной инфраструктуре насчитывает уже почти десять лет. Таким образом, переход к этой технологии хранения ключей в масштабах публичных сервисов давно рассматривался как один из сложных, но, тем не менее, потенциально возможных вариантов. И в этом отношении оставался только один краеугольный вопрос безопасности: «каким образом конкретный пользователь-обладатель ключа электронной подписи, хранящегося в «облаке», будет получать доступ к этому ключу»?

Доступ к «облаку» — какой вариант выбрать?

Одной из первых, еще в 2011—2012 году, свои «облачные» технологии электронной подписи предложила компания КриптоПро. Это был сервис КриптоПро DSS (Digital Signature Server), основанный на использовании для хранения ключей электронной подписи решения КриптоПро HSM. В качестве способа доступа к ключам пользователей было предложено на выбор сразу несколько вариантов: многоразовый пароль, одноразовый пароль, аутентификация с использованием токена, подключаемого к компьютеру.

Первый вариант — многоразовый пароль — означает, что для того, чтобы что-то подписать в «облаке» КриптоПро DSS, пользователю необходимо в этом «облаке» сначала аутентифицироваться с использованием пароля. И в этом отношении пользователь получает все прелести, связанные с использованием многоразового пароля: о недостаточности уровня безопасности многоразовых паролей говорят все эксперты по безопасности уже не один десяток лет, что доказывают множество инцидентов с украденными базами паролей и часто весьма простыми способами эти пароли угадать или украсть.

Второй вариант — одноразовый пароль — предусматривает передачу одноразовой последовательности символов для аутентификации пользователя в «облаке» через SMS или ее генерацию OTP-токеном (One Time Password). Наиболее значимым недостатком одноразовых паролей является отсутствие их привязки к операции, которая с их помощью подтверждается. То есть одноразовый пароль может подтвердить любую, даже созданную злоумышленником, операцию. Этот факт породил большое количество мошеннических схем по «выведыванию» этих паролей у пользователей — от поддельных сайтов и приложений (фишинг) до социальной инженерии (выведывание кодов при личном общении). Привязка к реквизитам возможна при отправке кода через SMS, но этот канал уже давно показал свою полную несостоятельность для передачи кодов подтверждения (то есть одноразовых паролей), так как SMS может быть перехвачено десятком разных способов, самый простой из которых — приложение-троян для смартфона.

Третий вариант — аутентификация в КриптоПро DSS с использованием электронного ключа (токена

или смарт-карты), который подключается к компьютеру пользователя. Безусловно, это наиболее безопасный и привычный вариант двухфакторной аутентификации и допуска к информационным ресурсам и сервисам. Но, с другой стороны, если у пользователя есть токен, то зачем ему «облако» КриптоПро DSS с ключами электронной подписи? Устанавливаем на компьютер криптопровайдер и пользователь получает возможность спокойно работать! Более того, в ряде случаев подписание документов электронной подписью возможно и в самом токене, что является одной из лучших практик в индустрии безопасности. Т. е. вся идея простоты и доступности электронной подписи в «облаке» убивается этим вариантом на корню.

При анализе особенностей использования того или иного способа получения доступа к ключам электронной подписи «в облаке» следует учитывать, что электронная подпись, как правило, принимается каким-то юридически-значимым действием (услугой или сервисом). И ее востребованность обусловлена высоким уровнем безопасности, который обеспечивается за счет хранения в тайне ключа подписи и стойких криптографических алгоритмов. А если для доступа к ключу используется один из методов аутентификации (многоразовый пароль, одноразовый пароль, SMS и пр.), то получается, что свойства безопасности самой электронной подписи подменяются свойствами безопасности используемого механизма аутентификации. Поскольку безопасность всей системы определяется безопасностью ее самого «слабого звена», то система электронной подписи в целом не может быть более безопасной, чем, например, пароль доступа к ключам подписи. На практике это может означать, что получение злоумышленником пароля позволит ему подписывать от имени легального пользователя любые документы, что для реализации сервисов «облачной подписи» с юридически-значимыми последствиями является совершенно недопустимым.

Электронная подпись на мобильном устройстве. Проблемы и положительный опыт

В дальнейшем предпринималось еще много серьезных и довольно успешных попыток предложить технологии и реализовать масштабные проекты с использованием «облачной» электронной подписи. Это были и операторы мобильной связи, и крупные международные компании, такие как, например, Gemalto. Но одним из самых успешных стал опыт финской компании Valimo, которая наряду с оператором мобильной связи EMT (в настоящее время Telia Eesti) стала активным участником успешно реализованного в Эстонии проекта мобильной идентификации Mobil-ID. К слову сказать, проект Mobil-ID, будучи полноценной мобильной альтернативой знаменитой Универсальной Электронной Карты Эстонии (ID-карты), предоставил гражданам возможности не совсем «облачной» электронной подписи. Решение позволило абонентам, используя свои мобильные устройства и специальные возможности SIM-карты, подписывать электронные документы и подтверждать запросы на услуги электронного правительства. То есть средством электронной подписи стала SIM-карта, а решение в общем предоставляет сервисы по формированию подписи путем взаимодействия с определенным абонентом.

Эти технологии пытались адаптировать для России сразу несколько известных на рынке компаний, но дальше всех продвинулась компания «Аладдин Р.Д.». Разработчик средств аутентификации и формирования электронной подписи успешно прошел путь до апробации технологии в «МегаФоне» и в МТС, но, к сожалению, проект не был запущен в масштабах страны. В чем, на наш взгляд, заключаются причины, не позволившие реализовать перспективный проект?

Во-первых, SIM-карты уже не были «обычными симками», а ввиду усложнения решаемых задач и требований к ним, они становились в несколько раз дороже. По некоторым данным, стоимость увеличивалась до 10 раз, и кто-то должен был компенсировать эти затраты. Для сравнения: положительный опыт Эстонии во многом был связан с тем, что в проекте Mobil-ID движущей силой выступил сотовый оператор с государственным участием, который мог позволить себе пойти на дополнительные затраты и координацию своих действий с другими операторами. А в России для реализации схожего проекта необходимо было координировать усилия и разделять расходы уже 4-х крупнейших операторов мобильной связи. При этом сами решения — приложения идентификации пользователя и формирования его электронной подписи — необходимо было инсталлировать на SIM-картах абонентов всех операторов по всей стране, что многократно усложняло вопросы производства SIM-карт и вопросы их логистики в масштабах России, которая имеет многократно бОльшее население, чем Эстония.

Во-вторых, возник очень сложный организационный вопрос первичной идентификации граждан, которые получают SIM-карты с электронной подписью. В настоящее время с определенными оговорками любой из нас может купить SIM-карту для себя, для членов своей семьи, друзей, но если бы этот проект стартовал, то операторов бы строго обязали проводить первичную идентификацию (например, так, как это сейчас делают банки по Федеральному закону от 07 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступ-

>>info

Активная фаза проекта Универсальной Электронной Карты в Эстонии началась в 2000 году. К окончанию 2011 года уже более 1,1 млн граждан Эстонии (на тот момент из 1,6 млн жителей) получили пластиковые идентификационные документы (ID-карты), оснащенные почти двумя десятками элементов безопасности: смарт-карточный чип, микропечать, голограмма и прочее. На микросхеме смарт-карты было установлено идентификационное приложение, требующее от пользователя при взаимодействии через Интернет с информационными системами электронного правительства ввода PIN-кода, а также приложение электронной подписи — со своим отдельным PIN-кодом. Благодаря этому ID-карта стала полноценным средством идентификации человека, на которой хранятся и личные данные гражданина страны, и ключ электронной подписи. Ограничением стала лишь необходимость использовать персональный компьютер или ноутбук, а также считывающее устройство для ID-карты.

В 2007 году в Эстонии стартовал проект Mobil-ID, инициатором которого стал оператор мобильной связи EMT (сейчас Telia Eesti). Идея проекта Mobil-ID заключалась в записи упомянутых приложений идентификации гражданина и его электронной подписи на SIM-карту мобильного оператора. Таким образом, пользователь Mobil-ID получил возможность идентифицировать себя с помощью мобильного телефона, причем для этого уже не требовалось считывающее устройство для ID-карты.

В настоящее время Mobil-ID представляет собой услугу Telia Eesti — полноценное цифровое удостоверение личности в личном смартфоне (https://www.telia.ee/era/mobiil/lisateenused/mobiil-id). Сертификаты Mobil-ID выдает Департамент полиции и пограничной охраны Эстонии, поэтому аналогично ID-карте услуга Mobiil-ID позволяет осуществлять различные электронные транзакции, получать услуги электронного правительства, заключать договоры, подписывать документы электронной подписью и голосовать на выборах. Услуга доступна пользователям как в Эстонии, так и за ее пределами, и, хотя она и не являлась полноценной «облачной», тем не менее, до недавнего времени оставалась единственной возможностью для осуществления электронных операций на смартфоне или планшете.

ным путем, и финансированию терроризма»). Соответственно расходы и трудоемкость бизнес-процессов операторов сразу же существенно возросли бы.

И, в-третьих, возник извечный вопрос «Зачем?». Какие такие Госуслуги и сервисы коммерческих компаний, оказываемые исключительно на базе электронной подписи, были готовы к предложению физическим и юридическим лицам в России? На тот момент, к сожалению, такие услуги еще не были представлены, поэтому критической необходимости старта проекта еще не было.

В настоящее время продолжается попытка реализации «облачной» подписи с использованием SIM-карт, анонсированная компанией «1С». Технологии, лежащие в основе этого проекта, были кратко представлены, главным образом, российским финансовым институтам (в рамках Уральского форума «Информационная безопасность финансовой сферы» 2017 года). Сейчас информации о ходе данного проекта очень немного и только время покажет, оправдаются ли ожидания пользователей о получении «облачной» подписи с использованием SIM-карт от компании «1С».

Еще одной заслуживающей внимание перспективной попыткой реализации «облачной» подписи для доступа с мобильных устройств стал собственный проект компании «МегаФон». В этом проекте оператор предлагал компромиссное решение: для хранения ключей электронной подписи использовать HSM, а для обеспечения пользователям доступа к своим ключам подписи — клиентскую часть на основе специализированного апплета на SIM-карте, который генерировал простые одноразовые пароли.

С одной стороны, преимущества предложенного решения были очевидны: нет необходимости производить на SIM-карте сложные криптографические операции, и, соответственно, не потребовались более сложные и дорогие SIM-карты с интегрированными криптографическими сопроцессорами. Бюджет такого проекта был бы уже более реальным. Но с другой стороны, для доступа к ключам подписи опять предлагались одноразовые пароли, которые в прошлом генерировались на OTP-токенах. Эти одноразовые пароли просто были перенесены на SIM-карту со всеми своими недостатками и ограничениями. Таким образом, снова безопасность всей системы электронной подписи подменялась бы безопасностью пароля доступа к ключу подписи, и она не была бы безопаснее или удобнее в использовании простого одноразового пароля.

Чего сейчас рынок ждет от электронной подписи?

В настоящее время на рынке наблюдается очередной всплеск интереса к «облачной» электронной под-

>>info

Что имеется ввиду, когда говорится, что «клиенту выдана электронная подпись»? Каждый специалист скажет, что сама по себе подпись является результатом криптографических преобразований подписываемой информации, и подпись нельзя выдать на Flash-носителе, токене или смарт-карте. И уж совсем точно это не есть просто средство подписи — непосредственное техническое средство для формирования электронных подписей документов. Так как же правильно использовать термин, который, как и в других специфических областях, стал профессиональным жаргоном?

Итак, электронная подпись, выданная конкретному клиенту, подразумевает наличие трех составляющих:

Первое — это средство электронной подписи. То есть непосредственно техническое средство, реализующее набор криптографических алгоритмов и функций. Например, это может быть криптопровайдер (КриптоПро CSP, ViPNet CSP), самостоятельный токен (Рутокен ЭЦП, JaCarta ГОСТ) или «облако».

Второе — это ключевая пара, сформированная средством электронной подписи. Один из ключей в этой паре — ключ электронной подписи (его еще иногда называют закрытым ключом), который используется выработки подписи. В самом общем случае, закрытый ключ может храниться в различных местах: на компьютере (хоть это и весьма небезопасно), на флэшке (тоже небезопасно), на токене (уже лучше, но небезопасно), на токене/смарт-карте в неизвлекаемом виде (наиболее безопасный вариант). Второй из ключей – открытый, ключ проверки электронной подписи. Он необходим, чтобы любой желающий мог проверить корректность электронной подписи. Этот ключ не является секретом, но однозначно привязан к закрытому ключу.

Третье — это сертификат ключа проверки электронной подписи, который формируется Удостоверяющим Центром. Зачем нужен сертификат? Когда человек с помощью имеющегося средства электронной подписи генерирует ключевую пару, то физически она будет представлять собой два обезличенных набора байт. И когда человек передает кому-либо открытый ключ для последующей проверки электронной подписи, то всегда возникает риск того, что этот открытый ключ (обезличенный набор байт) в процессе передачи будет кем-то подменен. И, соответственно, злоумышленник, который подменил этот открытый ключ на свой, сможет выдавать себя за подписанта, просто перехватывая сообщения, изменяя их и ставя свою электронную подпись. Чтобы такого не происходило, необходимо обезличенный набор байт открытого ключа связать с личностью конкретного клиента, с определенным человеком или организацией. И это как раз делают Удостоверяющие Центры (УЦ). То есть человек или представитель организации приходит в Удостоверяющий Центр, показывает свой паспорт и говорит: «Вот я, Иван Иванов, вот мой ключ проверки электронной подписи. Выдайте мне, пожалуйста, документ, что этот открытый ключ принадлежит мне — Ивану Иванову». И вот этот документ и есть сертификат. И за него, за его корректность отвечает Удостоверяющий Центр. УЦ несет ответственность (финансовую и административную) за сертификаты, которые он выпускает. И если в какой-то сделке появится сертификат ключа проверки, выданный на имя Ивана Иванова, но с открытым ключом, не принадлежащим Ивану Иванову, УЦ будет нести ответственность по этой сделке. Причем ответственность, как прописано в законодательстве, около 50 млн рублей. Это весьма серьезная финансовая ответственность. То есть УЦ — это такая организационная единица, которая занимается сопоставлением открытых ключей и личностей в физическом мире.

В соответствии с законодательством РФ, различают «сертификат ключа проверки электронной подписи» и «квалифицированный сертификат ключа проверки электронной подписи» (квалифицированный сертификат), первый из них выдается Удостоверяющим Центром, а второй — аккредитованным в соответствии с законодательством РФ Удостоверяющим Центром. Важно понимать, что сам по себе ключ проверки электронной подписи (открытый ключ) есть понятие техническое, в то время как сертификат открытого ключа и Удостоверяющий Центр — это понятие организационное.

Таким образом, когда мы говорим, что человеку «выдана электронная подпись», то имеем ввиду, что:

- Ему выдано средство подписи.
- У него есть ключевая пара: открытый и закрытый ключ, с помощью которых формируется и проверяется электронная подпись.
- Удостоверяющим Центром ему выдан сертификат на открытый ключ, то есть УЦ проверил, что соответствующий открытый ключ из ключевой пары на самом деле принадлежит этому человеку.

И применительно к «облачной» электронной подписи, когда мы говорим, что человеку выдана «облачная» электронная подпись, то это значит, что человеку в «облаке» сформировали ключевую пару, удостоверились, что открытый ключ на самом деле принадлежит этому человеку, выпустили соответствующий сертификат, и этому человеку выдали средство для доступа к его ключам в облаке.

писи. Примечательно, что этот интерес предопределен сугубо практическими задачами бизнеса.

Одной из таких задач является так называемая «одноразовая подпись». Во многих областях сейчас требуется поставить квалифицированную электронную подпись однократно и решения для формирования такой «одноразовой подписи» (без использования ключей подписи еще раз) чрезвычайно востребованы. Очевидно, что «классические» варианты выдачи клиентам электронной подписи не совсем подходят — сроки и стоимость выдачи токена или смарт-карты, развертывания криптопровайдера на компьютере клиента, формирования ключей подписи, выдачи сертификата — все это для одной-единственной подписи слишком сложно, дорого и долго. В таких условиях предложение «облачной» подписи представляется весьма подходящим выбором.

Показательным примером являются сделки с недвижимостью. В частности, многие компании-застройщики и торговцы недвижимостью осуществляют работу с клиентами неким стандартным общепринятым образом: к ним приходит клиент, и, чтобы зарегистрировать сделку в Федеральной службе государственной регистрации, кадастра и картографии (Росреестре) необходимо собрать установленный пакет документов, сходить в этот Росреестр, сдать эти документы для регистрации, а потом совершить еще один визит и получить соответствующее свидетельство на регистрацию права собственности. Примечательно, что уже сейчас все это можно сделать в электронном виде, по крайней мере, информационные системы и процессы Россреестра это позволяют. Для того чтобы это сделать, нужна лишь квалифицированная электронная подпись участников сделки, которой клиент и застройщик подпишут сформированный пакет документов. И клиенту эта операция нужна всего один раз. Разумеется, компании-застройщики и торговцы недвижимостью, а также другие игроки рынка, в бизнесе которых необходима «одноразовая» электронная подпись клиента, не будут строить систему для формирования подписи в своей инфраструктуре. Они воспользуются услугами, которые, кстати говоря, уже пытаются предлагать некоторые компании.

Другой задачей бизнеса является уход в мобильность. Ни для кого не секрет, что привязанность пользователя к рабочему месту с персональным компьютером семимильными шагами уходит за горизонт. Появляется все больше сценариев использования сервисов, предполагающих работу на персональном мобильном устройстве: обычно это мобильный телефон или может быть планшет.

Системы принятия решений коллегиальных органов, документооборот, дистанционное банковское обслуживание, управление компанией, электронные торги — эти и многие другие сервисы требуют все меньшего времени реакции и бóльшей мобильности.

Бизнес, предоставляющий эти сервисы, не может не ответить на эти требования. И используемые средства электронной подписи должны также им отвечать. А традиционные средства, такие как криптопровайдеры и токены, не имеют возможности работать на мобильных устройствах. И «облачные» технологии как раз решают эту задачу.

Подпись документов как услуга — профессиональный блеф или реальный сервис?

Итак, в чем состоит смысл сервиса однократной квалифицированной электронной подписи? Когда клиент приходит оформлять сделку, при наличии у него квалифицированной электронной подписи можно было бы собрать и отправить документы, например, как в примере с недвижимостью, в Россреестр в электронном виде. И больше никому никуда не ходить. Это удобно, но клиенту нужно предоставить квалифицированную электронную подпись, а где же ее взять для однократной подписи? И вот в последнее время появились компании, как правило, являющиеся Удостоверяющими Центрами, которые предлагают клиентам за небольшие деньги однократную, да еще и «облачную» подпись. «Мы сделаем квалифицированную электронную подпись за Вас», — говорят такие компании. То есть некая организация по запросу клиента у себя генерирует для него ключевую пару, здесь же, в своем Удостоверяющем Центре, выпускает для него сертификат, берет у этого человека собранный набор документов, подписывает от его имени, а самому клиенту возвращает уже подписанный набор документов. Конечно же, для решения конкретной задачи удобно. Но вот можно ли считать такую услугу легитимной?

В теории, в идеальных условиях, наверное, это может рассматриваться как однократная услуга. Но с юридической точки зрения, с точки зрения здравого смысла и самих принципов электронной подписи, закрепленных № 63-ФЗ «Об электронной подписи», не все так гладко. Судите сами: какая-то организация с непонятными для конкретного человека правами, генерирует ему ключ электронной подписи, на имя этого человека выпускает квалифицированный сертификат открытого ключа. В итоге получаем полный набор для формирования электронной подписи, которая по своей юридической значимости является заменой собственной рукописной подписи. С помощью ключа электронной подписи можно подписать любые документы и оформить любые распоряжения, которые государственные органы должны воспринять как руководство к действию, так как уже выпущен и может быть предоставлен сертификат открытого ключа. Распоряжения могут быть любые, вплоть до смены имени

и фамилии. Парадокс ситуации заключается в том, что человек, воспользовавшись таким сервисом, это никаким образом уже не контролирует!

Конечно же, юридические соглашения между клиентом и компанией, которые заключаются для оказания таких услуг, могут быть любые: доверенность на формирование электронной подписи, поручение, договор. Компании, предоставляющие эти услуги, очень разные, и у них могут быть разные юридические конструкции, в том числе и хорошо продуманные, предоставляющие определенную гарантию безопасности и качества сервиса. Тем не менее, с точки зрения здравого смысла, с точки зрения принципов электронной подписи, услуги в таком виде не совсем корректны. В нашем примере регистрации прав собственности на объект недвижимости ничто не мешает этой же компании сначала зарегистрировать права собственности на клиента, а потом следующим пакетом отправить заявление на перерегистрацию этого права собственности на совершенно другое юридическое или физическое лицо. Схем для мошенничества огромное количество: у них есть сертификат, у них есть ключ электронной подписи, у них есть все реквизиты на сам объект недвижимости. И им ничего не мешает воспользоваться этими средствами, и никто это не проконтролирует и не изменит.

Некоторые сервисные компании идут дальше, хотя и предоставляют похожую схему. Они также генерируют у себя ключи электронной подписи своих клиентов, используют развитую и более надежную систему управления процессом оказания таких услуг однократной электронной подписи, но подтверждение на подписание документов клиента производится через SMS. По этой причине, как мы выяснили ранее, всю эту систему в полной мере нельзя считать квалифицированным средством подписи. Компании очень убедительно объясняют, что они купили сертифицированный HSM, показывают на него бумагу: «Вот мы пользуемся сертифицированным средством и подтверждаем операции с помощью SMS». Но почему же дальше как пользоваться этим сертифицированным HSM никто уже не читает? Между тем в «Правилах пользования…», которые являются неотъемлемой частью сертификата регулятора отрасли, написано, что для обеспечения доступа к HSM со стороны пользователя для подписи документов, необходимо устанавливать набор программного обеспечения, устанавливать зашифрованный защищенный канал, и так

>>info

К сожалению, прецедент использования сервисной компанией ключа электронной подписи и сертификата за своего клиента был. Все начиналось логично и правильно: зарегистрирован и аккредитован Удостоверяющий Центр, выпущен набор сертификатов на вполне реальных существующих физических лиц, которым оказывались услуги «однократной» электронной подписи. Но в последующем у клиента увели объект недвижимости стоимостью несколько сотен миллионов рублей. Ничего не подозревающий собственник пришел выполнять операции со своей недвижимостью, но выяснил, что она уже очень давно ему не принадлежит: через несколько лиц были перерегистрированы права собственности и конечный покупатель был вполне добропорядочным. Скандал был очень большой. В том числе этот инцидент положил начало, так сказать, *«зачистке» удостоверяющих центров*.

Схема, когда человек не может контролировать свое средство подписи, потенциально несет в себе риск большого количества мошенничества. Пусть даже не компания, которая оказывает услугу, пусть это будет неблагонадежный сотрудник, например, просто операционист, но мошенничество от этого не станет менее значимым. Так, объект недвижимости в Москве стоимостью несколько десятков миллионов рублей — это половина или даже вся сумма заработка среднестатистического сотрудника за всю его трудовую жизнь. Поэтому неблагонадежные сотрудники могут решить так: «уведем этот объект недвижимости, а потом гори оно все огнем!». Таким образом, схема оказания услуг однократной подписи сама по себе потенциально несет возможности мошенничества. Конечно же, не факт, что эти возможности обязательно реализуются, но они есть, причем совершенно реальные.

Итак, получается, что схемы оказания услуг однократной подписи находятся на грани легальности и нелегальности. Они могут использоваться до тех пор, пока кто-то не копнул глубже. В 2016 году был большой скандал с одним очень крупным банком, который тоже заявил, что они используют «облачную» квалифицированную подпись с доступом по СМС. Как только это все вскрылось, то банк потрясла череда проверок со стороны регуляторов, в частности, со стороны федеральной службы безопасности России. И очень быстро предложения банка этих услуг для клиентов завершились и больше уже не возобновлялись. Кстати говоря, подрядчиком банка по этим работам была одна из самых известных компаний — операторов электронной отчетности, один из крупнейших и признанных клиентами удостоверяющих центров в стране.

далее, и так далее. Потому что HSM является не «железкой» для использования произвольными удаленными пользователями, а средством для выполнения набора конкретных операций внутри конкретной организации, где есть возможность построения защищенного канала непосредственно к этой «железке».

КриптоПро myDSS. Квалифицированная электронная подпись в смартфоне

Возвращаясь к рассмотренным вариантам доступа к ключам электронной подписи в «облаке», попытаемся подвести некоторые итоги и расскажем о комплексном решении КриптоПро myDSS. Компания SafeTech специализируется на системах подтверждения транзакций и документов, особенно в банковской области, которая всегда была на острие атак злоумышленников, и на острие технологий противодействия этим атакам. Такая специализация позволила компании разработать собственное решение PayControl (http://www.safe-tech.ru/content/products/paycontrol), которое позволяет безопасно с помощью мобильного телефона подтверждать выполнение операций и подписывать документы: будь то платежные документы, операции входа на порталы или другие информационные ресурсы и сервисы.

Партнерское взаимодействие с компанией КриптоПро позволило нам найти устойчивую нишу для комплексного решения: в «облачный» сервис КриптоПро DSS был внедрен метод формирования подтверждений на подписание на основе технологий PayControl. Совместное решение использует передовые технологии «облачного» управления ключами и функциями электронной подписи и имеет безопасный, мобильный и удобный способ доступа к функциям подписания. В комплексном решении для того, чтобы «облако» (серверная часть) выполнило подписание, ему необходима санкция на выполнение этого действия. Санкция зависит от четырех составляющих: времени, содержания подписываемого документа, уникальных признаков смартфона, а также уникального ключа, который хранится в смартфоне пользователя в защищенной области. Конечно же, это далеко не схема одноразового или многоразового пароля, здесь не используются SMS, которые сами по себе небезопасны — это существенно более безопасная технология подтверждения транзакций и документов. И она реализована в форме мобильного приложения для современных мобильных платформ.

Разработав и задокументировав схему совместной работы, компании КриптоПро и SafeTech реализовали ее и представили решение на сертификацию в Федеральную службу безопасности Российской Федерации. В настоящий момент можно аргументированно утверждать, что комплексное решение КриптоПро myDSS (http://www.safe-tech.ru/content/products/mydss) в целом, включая серверную часть (в которой в HSM хранятся ключи электронной подписи), систему управления процессами формирования подписи на стороне сервера, приложение для смартфона (которое визуализирует пользователю подписываемый документ и вырабатывает санкции на подписание), а также каналы взаимодействия клиентской и серверной частей с реализованными способами защиты этого канала — все это комплексное решение является полноценным средством электронной подписи. То есть, с определенной долей упрощения можно будет сказать, что КриптоПро myDSS — это большой токен.

В настоящее время никого уже не удивить тенденцией перехода в мобильность, отказа от некогда традиционных «железок» и других устройств для аутентификации пользователей и формирования электронной подписи. Многие пользователи привычно работают с планшетов и смартфонов, к которым просто так невозможно подключить токены и смарт-карты. Кроме того, участники рынка и сами пользователи признали, что SMS-сообщения как средство подтверждения транзакций и документов стали далеко не так безопасны и недопустимо дороги. По этой причине все стали обращать внимание на технологии «облачной» подписи и безопасные технологии доступа к ключам этой подписи. В этом смысле появление на рынке решения КриптоПро myDSS как нельзя кстати. В настоящий момент компания КриптоПро ведет активную работу по сертификации решения в ФСБ России, уже получен сертификат на серверную часть решения КриптоПро DSS, на очереди сертификация уже всего решения в целом.

Развитие технологий «облачной» подписи и технологий безопасного доступа к ключам электронной подписи прошло довольно длительный процесс становления. Это был не простой путь, а, как это часто бывает, путь, пройденный методом проб и ошибок Выработанное к настоящему времени решение, действительно, позволяет пользователям отказаться от установки на компьютере криптосредств, отказаться от покупки токенов и привязки к своему непосредственному рабочему месту. Сейчас действительно можно очень просто и удобно ставить квалифицированную электронную подпись со своего смартфона, получая доступ в любом месте и в любое время. Уже можно подписывать своей электронной подписью любые документы, причем с сохранением всех свойств безопасности, а также, что называется, подписывать со всеми удобствами.

Подготовлено с использованием публикаций авторов на Едином портале электронной подписи (http://www.iecp.ru).