CIS / № 1 (23) / 2023 / www.cis.ru

Электронная подпись

Когда безопасность дороже времени?

Валерия Валетина
Менеджер по работе с корпоративными клиентами «Актив», Рутокен

Любое решение для обеспечения информационной безопасности не может быть одновременно максимально простым и максимально защищённым: чем-то приходится поступаться.

Вот, например, личный смартфон. Вряд ли информация на нём (контакты, файлы и фотографии) настолько интересна для посторонних людей, чтобы требовать использования сложных и дорогих способов защиты (со смартфонами знаменитостей дело обстоит совершенно иначе, но давайте трезво оценивать собственную значимость). К тому же большинство ставит удобство превыше всего и информацию в памяти смартфонов никак не защищает. Меньшинство обходится простой встроенной биометрией (лицо, рисунок, радужки глаз, отпечатки пальцев). А по-настоящему надёжный пароль устанавливают единицы (которым есть что терять).

Иная ситуация сложилась с дверными замками. Несмотря на то, что уже несколько лет существуют электронные устройства, которые издалека узнают смартфон хозяина и сами распахивают перед ним дверь, все устанавливают старые добрые стальные замки с ключами (да не один, а даже два или три). Ключи неудобные и тяжёлые, их всюду нужно носить с собой, да ещё тратить время на открывание замка, но всё равно в данном случае безопасность важнее.

А как обстоит дело с электронной подписью, столь важным атрибутом современной цифровой среды? Технология это новая (по сравнению с используемой на протяжении веков обычной подписью на бумаге), для большинства непонятная и даже внушающая опасение. Поэтому в российском законодательстве установлены строгие требования к программному обеспечению, используемому для создания электронной подписи, аккредитованным удостоверяющим центрам, выдающим сертификаты ключей её проверки и так далее. Кроме того, для защиты электронной подписи российскими разработчиками были созданы USB-токены и смарт-карты с криптографическим ядром, позволяющие использовать неизвлекаемые ключи.

Что такое неизвлекаемые ключи электронной подписи и в чём их преимущества

Ключ электронной подписи – это числовая последовательность, никак не привязанная к своему владельцу, поэтому ключ очень просто скопировать. А любой, у кого есть ключ, может подписывать с его помощью электронные документы от имени и без ведома законного владельца. Единственный способ защитить ключ от копирования – обеспечить защищённое хранение. Для этого есть несколько способов:

1. Ключи помещаем в реестр или в файл, а защищаем встроенными средствами операционной системы. У этого способа два недостатка. Во-первых, недостаточная мобильность: чтобы подписать документы на другом ПК, ключ нужно будет копировать. А во-вторых, нужно будет очень хорошо защитить саму операционную систему. Ведь если злоумышленник подсмотрит (или перехватит) пароль, то ничто не помешает ему завладеть ключом. Вывод: если на ПК используется двухфакторная аутентификация, то можно выбрать и такой способ, но лучше не стоит.
2. Ключи копируем на флэш-накопитель. Теперь подписывать можно с любого ПК, к которому подключена флэшка. Только вот сам накопитель никак не защищён. Его нужно хранить в сейфе, а компьютер, на котором происходит подписание, стоит проверять на наличие вирусов. Ведь какой-нибудь «троян» способен запросто украсть ключ. Вывод: флэш-накопитель – самый неудачный вариант, крайне не рекомендуется.
3. Ключи помещаем на специальный физический носитель – смарт-карту или USB-токен в защищённую область памяти. Для доступа к ключам необходимо ввести PIN-код. Для вычисления электронной подписи используется специальное программное обеспечение, установленное на ПК. Таким образом, каждый раз при подписании электронных документов ключ электронной подписи передаётся в память рабочего компьютера. Но существует программное обеспечение, позволяющее злоумышленнику извлечь и скопировать ключ. Для этого нужно подсмотреть PIN-код и на время получить доступ к токену.
4. Ключи электронной подписи создаются и хранятся в памяти криптографического токена, а значит, необходимость передавать ключи на ПК отпадает. Следовательно, такие ключи можно объявить неизвлекаемыми. Способа достать неизвлекаемый ключ из памяти токена (и скопировать его) не существует.

Фактически, использование активных криптографических средств электронной подписи (токенов и смарт-карт) – единственный по-настоящему надёжный способ защиты ключей электронной подписи от злоумышленников. Почему же он не используется в 100% случаев?

1. Токены с криптографическим процессором стоят немного дороже токенов без оного. И уж, конечно, дороже обычных флэшек.
2. При выдаче ключей Удостоверяющие центры иногда рассказывают об опасностях, подстерегающих владельцев ключей, и о способах защиты. В результате пользователи зачастую выбирают более понятную им флэшку, чем совершенно незнакомый токен.

Виды электронной подписи: простая, усиленная и квалифицированная

Федеральный закон «Об электронной подписи» № 63-ФЗ говорит нам, что существует три вида электронной подписи:

- **простая,** которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определённым лицом;
- **неквалифицированная,** полученная в результате криптографического преобразования информации с использованием ключа электронной подписи;
- **квалифицированная,** соответствующая всем признакам неквалифицированной электронной подписи, причём ключ проверки электронной подписи указан в квалифицированном сертификате (выданном

аккредитованным Удостоверяющим центром), а для создания и проверки используются сертифицированные средства.

Для непосвящённых звучит не совсем понятно, поэтому поясним попроще.

Простой подписью пользовался каждый из нас. Она применяется, например, в системах дистанционного банковского обслуживания, когда клиент банка пишет SMS для перевода денег или выполняет оплату в личном кабинете, предварительно введя пароль.

Плюс у простой подписи один (причём следующий из её названия) – простота реализации. А вот всё остальное – минусы. Дело в том, что поскольку у простой подписи нет единого вида и принципа формирования, то, с одной стороны, человеку бывает сложно осознать тот факт, что он что-то подписал, а с другой – владельцу подписанного документа бывает непросто доказать факт подписания. Обычно для этой цели используют журналы информационных систем, подтверждающие отправку SMS или аутентификацию пользователя.

Для использования простой подписи (как и для неквалифицированной) обязательно подписание регламента электронного документооборота, где (среди прочего) как раз и сказано, как будет проходить подписание и проверяться подпись. Составить правильный регламент не очень просто (особенно для простой подписи), юридические ошибки позволят оспорить факт подписания в суде. Именно поэтому для получения доступа к личному кабинету на сайте банка необходимо подписывать такие толстые соглашения.

Неквалифицированная подпись представляет собой цифровую последовательность, вычисленную с помощью специальных алгоритмов на основе исходного документа и ключей электронной подписи. Для проверки электронной подписи используется сертификат ключей её проверки. При этом участники электронного документооборота вольны выбирать, какие именно алгоритмы использовать, с помощью чего создавать ключи и сертификаты. То есть, в отличие от простой подписи, есть понятные правила подписания и проверки, и главное – сторонам договориться и подписать регламент. Именно неквалифицированная подпись используется, например, в системах дистанционного банковского обслуживания юридических лиц.

Квалифицированная подпись во многом похожа на неквалифицированную, но есть два исключения. Во-первых, всё строго регламентировано. Криптографические алгоритмы – только ГОСТ. Программные и аппаратные средства криптографической защиты информации (СКЗИ) – только сертифицированные. Сертификаты проверки электронной подписи – только выданные аккредитованными государством Удостоверяющими центрами.

Но зато (и это, во-вторых) квалифицированная электронная подпись полностью аналогична (равнозначна) собственноручной на бумажном носителе и может использоваться без предварительного подписания соглашений и регламентов.

Но и в этой свободе есть минус. Если злоумышленник украдёт ключ квалифицированной электронной подписи, то сможет подписать всё, что захочет. Поэтому ключ и должен храниться на токене и быть неизвлекаемым.

Так что же делать? Где найти золотую середину между безопасностью и удобством? Давайте пройдёмся по типичным задачам и выясним, насколько серьёзной должна быть защита в каждом конкретном случае.

Квалифицированная электронная подпись слишком ценна, а последствия кражи ключей слишком опасны, чтобы экономить на защите. Поэтому в данном случае рекомендовано использование активных криптографических ключевых носителей (токенов), генерирующих неизвлекаемые ключи.

Если Удостоверяющий центр не хочет такие ключи создавать (или выписывать сертификат на уже созданные) – идите в другой, безопасность тут дороже времени. Если программное обеспечение для подписи электронных документов не может работать напрямую с криптографическим токеном (как, например, все токены линеек Рутокен ЭЦП), используйте криптопровайдер КриптоПро CSP 5, который умеет работать с неизвлекаемыми ключами.

Неквалифицированную электронную подпись зачастую используют не ради экономии (на поддержание собственного УЦ и выдачу сертификатов тоже тратятся ресурсы), а для того чтобы полностью контролировать процесс (например, выдавать сертификаты только проверенным контрагентам) и ради отсутствия ограничений (любое ПО, алгоритмы и пр.). К тому же необходимую для неквалифицированной электронной подписи инфраструктуру открытых ключей (PKI) можно использовать для двухфакторной аутентификации.

Итак, при выборе вида электронной подписи необходимо ответить на два главных вопроса: где хранить ключи и с помощью какого устройства подписывать. Ключи в реестре или файловой системе требуют усиленного контроля за тем, кто именно работает на ПК (что обычно решается с помощью двухфакторной аутентификации на основе токенов, но в чём же тогда экономия?), а также снижает мобильность пользователей, не позволяя им подписывать документы с любого компьютера.

Ключи на флэшках хранить можно только в том случае, если сама флэшка хранится в персональном сейфе, а во время работы владелец ни на секунду не спускает с неё глаз.

Токены были и остаются решением, специально созданным как для хранения ключей, так и для вычисления электронной подписи. Причиной их не повсеместного использования является, с одной стороны, цена (никто не любит платить за безопасность), а с другой – нежелание носить с собой и безопасно хранить ещё одну «штуковину». Кстати, те же самые токены можно использовать как для локальной, так и удалённой двухфакторной аутентификации.

Хранить ключи на смартфонах и использовать сами смартфоны для подписания можно, но только если вы уверены в отсутствии троянов и средств удалённого управления. Для персональных смартфо-

нов, используемых для множества задач с кучей установленных приложений, такое слабо достижимо (даже при наличии антивируса). Поэтому для таких целей лучше всего использовать отдельный аппарат, правда в этом случае затея становится экономически не особо привлекательной. Гораздо дешевле и удобнее для мобильной подписи использовать те же токены: как бесконтактные NFC и Bluetooth, так и контактные с интерфейсом USB Type-C. Они могут и ключи хранить, и электронную подпись вычислять вне смартфона.

При работе с **простой электронной подписью** автор рекомендует следующий подход: используйте её для работы с теми документами, оспаривание которых наименее вероятно. Например, при кадровом документообороте сотрудники вполне могут подписывать простой подписью заявление на отпуск или отчёт о командировке. Проблемы у вас могут возникнуть разве что с налоговой, но они решаются с помощью грамотно составленных регламентов.

А вот подписание простой подписью заявлений на увольнение – это уже большой риск для работодателя. Потому что сегодня человек поставит галочку, что документ он подписал, а через месяц пойдёт в суд, заявляя, что ничего не подписывал и его незаконно не допускают на рабочее место. Если выиграет, то компания заплатит и компенсацию, и штраф.

В общем, всё, как обычно. Необходимо помнить, что из триады целей «Дёшево – Удобно – Надёжно», достижимы только две. И не стоит верить на слово рекламе: всегда нужно проверять, насколько безопасно предлагаемое решение.

КОМПАНИЯ АКТИВ

Валерия Валетина
Менеджер по работе с корпоративными клиентами

«Актив», Рутокен

www.rutoken.ru