Без росчерка пера

Поскольку электронной цифровой подписи, электронным платежным системам и юридически значимому электронному документообороту государство уделяет повышенное внимание, отечественные разработчики продолжают совершенствовать свои решения и расширять линейки продуктов, предназначенные для использования электронной подписи. При этом учитываются такие тенденции ИТ, как облака и мобильность.

Сергей Орлов

Изменение законодательства и требований по сертификации, реализация проектов «Электронное правительство» и «Портал государственных услуг», развитие дистанционного банковского обслуживания и интернет-банкинга, поиск возможностей для определения ответственности в киберпространстве — все это способствует не только повышенному интересу к программно-аппаратным решениям, совмещающим удобство использования и усиленную защиту, но и пониманию участниками рынка необходимости и важности средств цифровой подписи.

Электронная подпись (ЭП) предназначена для защиты электронного документа. Она формируется в результате криптографических операций с использованием закрытого ключа, позволяет идентифицировать владельца сертификата ключа подписи и гарантирует целостность документа. Присоединяемая к электронному сообщению ЭП дает получателю возможность узнать, является ли отправитель сообщения тем, за кого себя выдает. Нередко для формирования электронной цифровой подписи применяют аппаратные устройства — USB-токены или смарт-карты. При использовании токенов и смарт-карт закрытый ключ подписи не покидает пределов данных устройств, что исключает возможность компрометации ключа.

Применение цифровой подписи обеспечивается инфраструктурой открытых ключей (Public Key Infrastructure, PKI). Основным компонентом PKI является удостоверяющий центр (см. Рисунок 1), который отвечает за выдачу ключей и гарантирует подлинность сертификатов, подтверждающих соответствие между открытым ключом и информацией о владельце ключа. Это могут быть корпоративные цифровые сертификаты или сертификаты государственного образца для физических лиц, например для применения в облачном сервисе. Надежное и безопасное хранение последних на данный момент обеспечивается только одним способом — с помощью смарт-карт и токенов, уверены в компании «Актив».

Между тем разработчики предлагают различные компоненты для встраивания криптографических функций в Web-приложения — например, SDK и плагины к браузерам с программным интерфейсом доступа к криптографическим функциям. Считается, что с их помощью можно реализовывать функции цифровой подписи, отличающиеся высоким уровнем безопасности. Средства цифровой подписи предоставляются и в виде онлайновых сервисов.

ДЛЯ ЧЕГО И КОМУ НУЖНА ЭП?

Насколько же востребованы в России неквалифицированная (для нее нет жесткой законодательной регламентации) и квалифицированная ЭП? По мнению Алексея Сабанова, заместителя генерального директора компании «Аладдин Р.Д.», к типовым примерам применения в России неквалифицированной электронной подписи можно отнести практически все процессы, не связанные с государственными органами и соответствующими требованиями законодательства. Причем из-за необходимости проведения весьма затратных мероприятий по распространению средств квалифицированной ЭП крупные предприятия занижают соответствующие требования, доводя их до уровня неквалифицированной ЭП.

Наиболее массовыми и яркими примерами использования неквалифицированной ЭП являются электронные торговые площадки по проведению госзакупок согласно Федеральному закону РФ № 44-ФЗ и системы дистанционного банковского обслуживания, рассказывает Юрий Маслов, коммерческий директор компании «КриптоПро», отмечая, однако, что по целому ряду причин массовой потребности в неквалифицированной электронной подписи на рынке пока нет. По усло-

Иллюстрация Натальи Левшиной

виям ее использования такая подпись близка к электронно-цифровой подписи, а последней за десятилетие законного существования так и не удалось завоевать популярность. Поэтому не стоит ждать массового распространения неквалифицированной ЭП. В то же время расширяется сфера добровольного применения квалифицированной электронной подписи. Это связано с тем, что риски ее использования существенно ниже.

Характерно, что юридическая значимость электронного документа не зависит от вида электронной подписи — квалифицированной или неквалифицированной. Юридическую силу он получает при наличии любой разрешенной для него электронной подписи. Однако, как и при использовании собственноручной подписи, применение электронной подписи несет с собой ряд рисков. Как и обычную подпись, электронную можно подделать или отказаться от нее. Соответственно, существует вероятность того, что электронный документ, удостоверенный ЭП, не будет принят в качестве доказательства. При использовании усиленной квалифицированной ЭП эта вероятность значительно меньше, чем в случае усиленной неквалифицированной ЭП, и просто ничтожна по сравнению с использованием простой ЭП, поясняет Юрий Маслов.

Сертификат для усиленной квалифицированной ЭП должен быть изготовлен аккредитованным в Минкомсвязи России удостоверяющим центром, то есть сертификат ключа проверки электронной подписи должен быть квалифицированным. Это одно из обязательных условий ее использования. В частности, важным фактором распространения средств ЭП с использованием мобильных устройств на российском рынке является техническая готовность удостоверяющих центров выдавать такие средства.

По словам Алексея Сабанова, согласно требованиям Федерального закона № 63-ФЗ квалифицированной может быть только усиленная подпись. Суть «усиления» ЭП по отношению к простой подписи состоит в том, что должна использоваться асимметричная криптография и обеспечиваться идентификация владельца ЭП с некоторым уровнем достоверности. «Понятие юридической силы электронного документа пока не

Рисунок 1. Аккредитованные российские удостоверяющие центры выдают электронные подписи поставщикам госзаказа для работы на федеральных торговых площадках, а также на любых коммерческих. Сертификат ключа подписи вносится в единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров Российской Федерации.

закреплено в законах, но, очевидно, должны обязательно предоставляться такие сервисы безопасности, как идентификация подписанта, целостность документа или сообщения и неотказуемость. Соответственно, ЭП должна быть как минимум усиленной. Целостность обеспечивается ЭП, неотказуемость — аутентификацией

Электронная подпись стремится в «облака»

КРИПТО ПРО

Нет ничего удивительного в том, что в последние годы так резко возрос спрос на решения, позволяющие использовать электронную подпись (ЭП) на мобильных устройствах. Ведь уже трудно себе представить человека, который бы не пользовался смартфоном или планшетным компьютером. Причем пользовался не только для того, чтобы скоротать время в очереди или в метро, включив одну из казуальных игр, но и для работы — например, используя систему дистанционного банковского обслуживания или корпоративную систему документооборота.

В то же время вопрос использования ЭП на этих устройствах долгое время оставался без ответа. Дело в том, что средства криптографической защиты информации (СКЗИ), реализующие ЭП, относятся к товарам двойного назначения, на экспорт которых наложены существенные ограничения. А размещая то или иное приложение, содержащее в своем составе СКЗИ, в одном из интернет-магазинов приложений (iTunes AppStore, Google Play, Windows Store), разработчик по сути осуществляет экспорт СКЗИ, поскольку серверы, на которых хостятся эти интернет-магазины расположены за пределами Российской Федерации.

Для решения этой проблемы 3 года назад нами была начата разработка решения «КриптоПро DSS», предназначенного для централизованного защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию ЭП в интересах пользователей при взаимодействии с программно-аппаратным криптографическим модулем (ПАКМ) «КриптоПро HSM». Данное решение поддерживает все основные форматы документов, может быть легко интегрировано с любыми прикладными системами (например, корпоративными системами документооборота) и решениями для обеспечения многофакторной аутентификации пользователей при доступе к закрытым ключам. Самой же главной же особенностью данного решения является отсутствие необходимости установки СКЗИ на клиентской стороне (будь то настольный ПК, планшет или смартфон) — ведь такая установка зачастую вызывает определенные трудности у простого пользователя, еще более усугубляющиеся в случае с мобильными устройствами. В настоящее время это единственное на рынке решение для создания как корпоративных, так и публичных сервисов «облачной» ЭП.

В части сертификации данного решения мы также проделали большую работу. Так, в июне этого года нами был получен сертификат ФСБ России, удостоверяющий, что ПАКМ «КриптоПро HSM», используемый в составе решения на базе «КриптоПро DSS», соответствует требованиям к средствам ЭП. Сам же «КриптоПро DSS» в настоящее время находится в процессе сертификации в ФСБ России, по окончании которого решение на базе «КриптоПро DSS» сможет быть использовано и для создания усиленной квалифицированной ЭП.

Алексей Голдбергс, заместитель технического директора по развитию продуктов ООО «КРИПТО-ПРО»

Реклама

подписанта, использованием усиленной ЭП и наличием системы ведения и заверения записей действий подписанта, — подчеркивает он. — Что касается аутентификации, все зависит от того, кто и как организует процессы аутентификации. В принципе, для обеспечения юридической силы вполне достаточно корректно построенной двухфакторной аутентификации. Заявляемая многофакторная аутентификация в абсолютном большинстве случаев является двухфакторной. Кроме того, до сих пор существует путаница в понятиях "идентификация" и "аутентификация", которая будет снята, скорее всего, после принятия федерального закона, где они четко разграничены. Ведь разобрались же участники электронного взаимодействия с видами ЭП».

Если говорить о средствах ЭП с использованием мобильных устройств, то их распространение на российском рынке зависит в первую очередь от изменений законодательства и нормативной базы, желания операторов мобильной связи и готовности их инфраструктуры открытых ключей (так называемой доверенной платформы).

ПОДПИСЬ В ОБЛАКАХ

С развитием массовых систем электронного документооборота, участниками которых являются разные юридические лица и граждане, все большую актуальность приобретает задача по предоставлению средств создания и применения электронной подписи в виде онлайновых сервисов, считает Юрий Маслов: «Это связано и с тем, что существенно понижаются требования к квалификации владельцев электронной подписи и стоимости владения средствами ЭП. Спрос рождает предложение — за последний год на российском рынке появилось свыше 10 операторов онлайновых сервисов для использования ЭП, в то время как в прошлом году не было ни одного».

Например, для автоматизации подписи, обмена и хранения электронных документов предлагается онлайновый сервис eSign-PRO (*http://www.esign-pro.ru*). Все регистрируемые в нем электронные документы защищаются цифровой подписью, причем ее формирование и проверка осуществляются на стороне клиента с помощью криптоплагина eSign Crypto Plugin, который устанавливается при первом доступе к порталу. Сервис eSign-PRO поддерживается инфраструктурой открытых ключей на базе удостоверяющего центра e-Notary, аккредитованного ФНС России и принадлежащего компании «Сигнал-КОМ», но могут применяться сертификаты, выпущенные другим удостоверяющим центром.

Как подчеркивают разработчики, данный сервис соответствует требованиям закона «Об электронной подписи» (№ 63-ФЗ) и использует средства криптографической защиты «КриптоКОМ 3.2», сертифицированные ФСБ России. Предусматривается возможность хранения ключевой информации на различных носителях, включая USB-токены.

«В соответствии с общемировой тенденцией развития информационных технологий, все большее внимание уделяется облачным технологиям применения и использования электронной подписи в системах электронного документооборота, — рассказывает Юрий Маслов. — Наша компания уже разработала и подала на сертификацию в ФСБ России программно-аппаратный комплекс "КриптоПро DSS", в котором реализована облачная технология применения ЭП».

«Возможно, для операций с низким уровнем рисков такие сервисы смогут быть востребованы, — считает Алексей Сабанов. — Однако средства ЭП и особенно закрытый ключ должны контролироваться владельцем. И это требование закреплено не только в законе № 63-ФЗ, но и в законах всех развитых стран. Наряду с идентификацией и аутентификацией факт единоличного управления владельцем своим закрытым ключом является основой доверия к применению ЭП».

НА ПУТИ К ЗРЕЛОСТИ

Насколько зрелыми, практичными и удобными являются технологии установления подлинности отправителя? По мнению Алексея Сабанова, подлинность подписи должна подкрепляться предъявлением дополнительных требований и их неукоснительным соблюдением. Первичная идентификация владельца ЭП может считаться относительно надежной только для сотрудников организаций с добротно построенной кадровой службой. Чтобы организовать удаленное электронное взаимодействие, систему первичной идентификации клиентов и трансляции доверия к полученной идентификации другому предприятию надо создавать в тесном взаимодействии с государством. Предложения некоторых удостоверяющих центров, выдающих сертификат ключа проверки подписи по Интернету через два часа после запроса, порождают недоверие ко всей системе аккредитованных УЦ. Инфраструктура, в которую входят почти 400 УЦ, создана, но реального доверия к аккредитованным УЦ и заверенным ими документам пока нет.

Тем временам требования к средствам ЭП растут, скоро на рынке останутся только законченные, надежные и удобные для пользователей средства ЭП. «Наша компания предлагает широкий спектр продуктов и решений. Мы много вкладываем в инновационные решения и формируем на них спрос, — рассказывает Алексей Сабанов. — В частности, компания "Аладдин Р.Д." разработала линейку продуктов JaCarta для строгой аутентификации, формирования усиленной квалифицированной электронной подписи и безопасного хранения ключей и цифровых сертификатов. Все новые продукты и решения компании основаны на единой технологической платформе с одноименным названием, что позволяет использовать все преимущества и функциональные возможности в различных отраслях, включая кредитно-финансовый сектор, телекоммуникации, медицину и прочие направления деятельности».

Устройства семейства JaCarta ГОСТ имеют аппаратную реализацию российских криптоалгоритмов и сертифицированы ФСБ РФ как персональные средства электронной подписи по КС1 и КС2. Они могут применяться для аутентификации с использованием механизмов электронной подписи, формирования электронной подписи на документах, подтверждения различных операций в информационных системах и при работе с облачными сервисами.

В данных устройствах российские криптоалгоритмы реализованы на уровне микропроцессора, при этом используется схема работы с неизвлекаемым закрытым ключом подписи. Такой подход исключает возможность хищения закрытого ключа подписи, а электронная подпись генерируется внутри устройства. Содержащиеся в JaCarta ГОСТ ключи и сертификаты могут применяться для строгой двухфакторной аутентификации и формирования усиленной квалифицированной электронной подписи сразу в нескольких информационных системах, функционирующих в рамках одной или нескольких инфраструктур PKI.

В продуктах линейки «Рутокен» (см. Рисунок 2) с двухфакторной аутентификацией (устройство и PIN-код) микропроцессоры осуществляют генерацию ключевых пар и формирование и проверку электронной подписи (алгоритм ГОСТ Р 34.10-2001), а защищенные микроконтроллеры имеют энергонезависимую память для хранения пользовательских дан-

ных. На базе данных устройств можно создавать специализированные программно-аппаратные решения. В отличие от продуктов, использующих Java, микропрограмма в «Рутокен» реализована на компилируемом языке. По мнению разработчиков из компании «Актив», это дает больше возможностей для оптимизации ПО.

Предлагаемый этой же компанией плагин для браузеров (для его установки не требуются права администратора) умеет работать с USB-токеном и имеет программный интерфейс доступа к криптографическим функциям. Плагин позволяет интегрировать «Рутокен» с системами дистанционного банковского обслуживания и электронного документооборота.

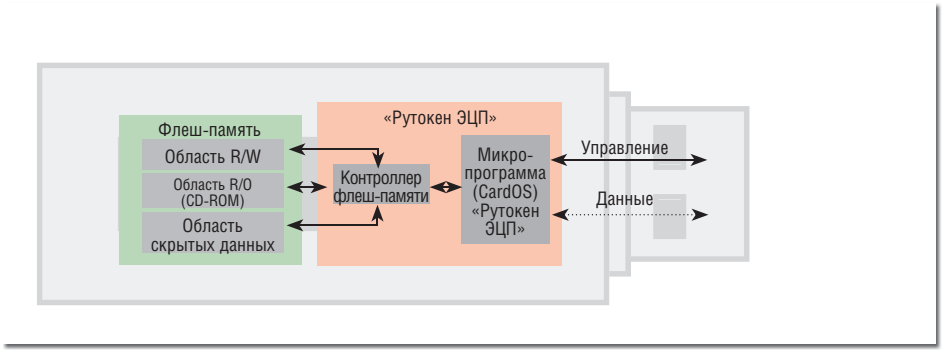

Рисунок 2. Устройство «Рутокен ЭЦП» представляет собой криптографический USB-токен, дополненный управляемой флеш-памятью емкостью от 4 до 64 Гбайт, которую можно использовать для хранения дистрибутива программного обеспечения, автоматического запуска приложений при подключении токена или доверенной загрузки операционной системы. Устройство имеет сертификат ФСБ о соответствии требованиям, предъявляемым к СКЗИ по классу КС2 и к средствам ЭП согласно Федеральному закону № 63-ФЗ «Об электронной подписи».

ЭП И МОБИЛЬНОСТЬ

В сентябре компания «Актив» начала массовые продажи «Рутокен ЭЦП Bluetooth» (см. Рисунок 3). Эти устройства для аутентификации и применения технологии электронной подписи можно подключить через USB-порт к ПК и ноутбукам на базе ОС Windows, Linux и OS X и использовать — благодаря поддержке Bluetooth — на мобильных устройствах, работающих под управлением операционных систем Android и iOS. «Рутокен ЭЦП Bluetooth» создан с учетом строгих государственных требований в области информационной безопасности, поддерживает российские стандарты электронной подписи, шифрования и хеширования. Криптографические операции выполняются внутри самого токена, к тому же для его использования специальных знаний не требуется: достаточно подключить токен к компьютеру или установить соединение с мобильным устройством через Bluetooth. Предусмотрено шифрование канала Bluetooth по ГОСТ 28147-89.

В октябре компании «Актив» и «Аванпост» (российский разработчик систем идентификации и управления доступом к информационным ресурсам предприятия — IDM), объявили о совместимости программного комплекса «Avanpost 4.0» со всей линейкой электронных ключей «Рутокен», включая модели «Рутокен ЭЦП».