**Электронная подпись в облаках и на земле**

Маслов Юрий Геннадьевич, коммерческий директор ООО «КРИПТО-ПРО»

Многообразие видов электронных подписей, введённых в оборот Федеральным законом от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи», ввело некоторое смущение (лучше назвать плюрализм) в ума людей как в толковании сферы их применения, так и в технологии их реализации.

В своём докладе я постараюсь провести некоторый анализ понятия и видов электронных подписей, который, смею надеяться, положит плюрализм на фактическую основу.

Для начала важно понять, что неправильно говорить о том, что разные виды электронной подписи имеют разную юридическую силу. Это в корне неправильно! Электронная подпись, вне зависимости от её вида, обеспечивает равнозначность электронного документа, подписанного электронной подписью, бумажному документу, подписанному собственноручной подписью. А следовательно и правовые последствия от факта подписания электронного документа одинаковы для всех видов подписи.

Правда стоит отметить, что есть ограничения на применимость тех или иных видов электронной подписи для тех или иных видов документов, используемых в тех или иных отношениях. Например, простая электронная подпись неприменима для подписания документов, которые в соответствии с правилами документооборота заверяются оттиском печати. А для заверения электронных счетов-фактур по закону нужно использовать исключительно усиленную квалифицированную электронную подпись.

Так же между видами электронной подписи есть и существенное различие. В первую очередь это относится к презумпции действительности электронной подписи и основаниям её недействительности. Напомню, что презумпция — это положения, устанавливающие наличность фактов или событий без полного доказательства их существования. А так же договоримся, что под действительной электронной подписью будем понимать такую электронную подпись в электронном документе, которая создана и используется в соответствии с установленными нормами права Российской Федерации, воплощает подлинное волеизъявление её создателя. Как видим, понятие действительности электронной подписи мы отличаем от действия электронного документа и его эффективности. Действие электронного документа зависит от вступления его в силу, срока, прекращения и других условий, в то время как действительность электронной подписи определяется нормами законодательства РФ.

В соответствии с нормами Федерального закона от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи» только для одного вида электронной подписи, а именно для квалифицированной электронной подписи, установлена презумпция действительности. В соответствии с ней действительность квалифицированной электронной подписи является нормальным состоянием этого вида электронной подписи. И наоборот, недействительность квалифицированной электронной подписи должна быть установлена исключительно в судебном порядке.

Для остальных видов электронной подписи (простой и неквалифицированной) действует презумпция относительной недействительности (оспоримость). Это означает, что действительность зависит от наличия согласия сторон к использованию данного вида электронной подписи данным способом и отсутствия оспаривания одной из сторон как самой электронной подписи так и самого согласия сторон.

Исходя из описанных выше презумпций относительно видов электронной подписи, существенно отличается и технология их реализации, технология применения электронных подписей.

Для квалифицированной электронной подписи применима любая технология, отвечающая требованиям ФСБ России. Почему ФСБ России, а не Минкомсвязи России? Потому, что ФСБ России является регулятором в области криптографических средств защиты информации, к которым относятся и средства квалифицированной электронной подписи. Что значит «отвечающая требованиям ФСБ России»? Это означает, что не только сами средства электронной подписи являются сертифицированными ФСБ России, но и технология использования этих средств одобрена ФСБ России (отвечает условиям эксплуатации сертифицированных средств электронной подписи). Таким образом, если условия эксплуатации сертифицированных средств электронной подписи не полно или не чётко изложены в эксплуатационной документации на сертифицированное средство электронной подписи, или эти условия не могут быть однозначно интерпретированы всеми специалистами (экспертами) в области криптографических средств, то крайне необходимо письменно обращаться в ФСБ России и получать письменные разъяснения от ФСБ России о допустимости конкретных условий использования конкретных средств электронной подписи. В противном случае, можете появиться риск оспаривания действительности квалифицированной электронной подписи в судебном порядке.

Ввиду наличия презумпции относительной действительности простой и неквалифицированной электронной подписи, необходимо обеспечить доказуемость действительности электронной подписи, что очень сильно зависит от технологии реализации. Например, для технологии, использующей сертификаты ключей проверки электронных подписей и криптографические средства электронной подписи, условия действительности неквалифицированной электронной подписи будут выглядеть следующим образом:

1. электронная подпись однозначно определяет лицо, являющееся подписантом, если одновременно выполнены следующие условия:
   a. имеется положительный результат проверки электронной подписи с использованием средства электронной подписи, соответствующего условиям установленным соглашением или оператором информационной системы, и сертификата ключа проверки электронной подписи лица, являющегося подписантом;
   b. сертификат ключа проверки электронной подписи изготовлен удостоверяющим центром, соответствующего условиям установленным соглашением или оператором информационной системы;
   c. удостоверяющий центр имеет доказательства владения лицом, являющимся подписантом, данного сертификата ключа проверки электронной подписи.
2. ключ электронной подписи являлся конфиденциальным на момент создания электронной подписи, если одновременно выполнены следующие условия:

a. сертификат ключа проверки электронной подписи лица, являющегося подписантом, не является аннулированным и действие его не прекращено на момент создания электронной подписи или на момент проверки электронной подписи;
b. сертификат ключа проверки электронной подписи удостоверяющего центра, с использованием которого удостоверяющий центр подписал сертификат ключа проверки электронной подписи лица, являющегося подписантом, не является аннулированным и действие его не прекращено на момент создания электронной подписи или на момент проверки электронной подписи;
c. информация об аннулированных и прекративших своё действие сертификатах ключа проверки электронной подписи является доступной и актуальной на момент создания электронной подписи или на момент проверки электронной подписи.

В приведённых выше условиях не указано ещё условие целостности электронного документа после подписания.

В случае, когда не обеспечено доказуемость хотя бы одного из условий, то можно говорить о недействительности электронной подписи.

Как мы видим, действительность электронной подписи есть величина (состояние) которая может изменяться во времени. Для юридически значимого электронного документооборота, необходимо, что бы состояние действительности электронной подписи было неизменяемым (действительным) с момента создания электронной подписи и до окончания срока хранения или срока исковой давности электронного документа.

Обеспечение такого состояния действительности электронной подписи является комплексной задачей, в которой существенную роль играет и техническая составляющая реализации электронной подписи и организационное обеспечения применения электронной подписи.

В последние годы наблюдается активный всплеск интереса к так называемой «облачной» электронной подписи. Эта технология подразумевает минимизацию (вплоть до полного отсутствия) криптографических преобразований по созданию и проверке электронной подписи на рабочем месте клиента (на компьютере, планшете и т.д.) и перенос этих операций на некую серверную часть, в облако.

Повышение интереса к облачной ЭП связано не только с существенным уменьшением цены владения электронной подписи в системе электронного документооборота (ЭДО), но и с возрастанием числа так называемых открытых систем ЭДО, не внутрикорпоративных. А в открытых системах ЭДО всё труднее и всё дороже обеспечить безопасную среду функционирования криптосредства на рабочем месте пользователя системы ЭДО. Это не только ведёт к существенному удорожанию цены электронной подписи (обучение пользователей, закупка, внедрение и эксплуатация системы защиты рабочего места пользователей и т.д.). Одним из существенных препятствий по внедрению массовых систем ЭДО с квалифицированной ЭП является соблюдение используемых платформ (ОС) соответствующих допустимым к сертифицированному средству электронной подписи. Производители ОС меняют платформы с частотой, за которой не успевают разработчики СКЗИ и регулятор.

Что хорошего даёт облачная ЭП?

Предоставляет возможность создавать электронную подпись без всякого программного обеспечения, аппаратных средств и ключей, установленных на стороне клиента.

Обеспечивается доступ отовсюду через браузер, что даёт полную мобильность и отсутствие риска потери ключей, смарт-карты и др.

Ключи порождаются, хранятся и управляются централизовано на сервере подписи, где обеспечено безопасное окружение.

Причём дело перешло от теоретического интереса к практическому применению.

Например, в облачная ЭП применяется в Лёгкой версии Бухгалтерии.Контур на основе системы «КлаудКрипт».

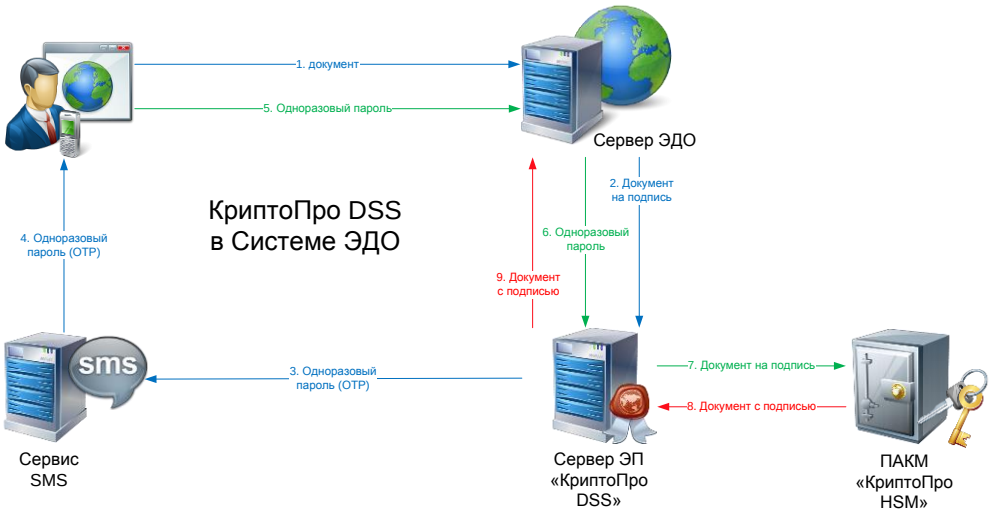
Или в интернет-бухгалтерии «Моё дело» на основе сервиса «Калуги Астрал». Аналогичное решение есть и у Компании Тензор и у Такскома.

Компания КРИПТО-ПРО тоже сделала такое решение под названием «КриптоПро DSS».

Общее у всех описанных выше решений одно – все они основаны на использовании ПАКМ «КриптоПро HSM» и все они не удовлетворяют требованиям ФСБ России как средства применения квалифицированной электронной подписи.

Для того, что бы понять и аргументировать это утверждение, постараюсь пояснить на примере реализации в виде «КриптоПро DSS».

Архитектура «КриптоПро DSS» на примере аутентификации «OTP по SMS» показана на рисунке ниже:




КриптоПро DSS предназначен для централизованного, защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи в интересах пользователей.

КриптоПро DSS обеспечивает:

- Создание электронной подписи под любым электронным документом.
- Широкий охват платформ и устройств, с которых пользователь может работать с КриптоПро DSS.
- Отсутствие необходимости установки клиентской части. Необходим лишь веб-браузер.
- Снижение риска компрометации ключей пользователей за счёт их централизованного защищённого хранения.
- Снижение стоимости развертывания и владения инфраструктурой ЭП, т.к. нет необходимости установки средства ЭП на каждое рабочее место пользователя, а управление всей инфраструктурой сосредоточено на одном сервере.
- Лёгкость встраивания функций создания ЭП в прикладные системы за счёт простых интерфейсов автоматизации на базе стандартных средств протокола HTTP и веб-сервисов.
- Возможность применения различных схем аутентификации пользователя для доступа к его ключам.

Помимо перечисленных возможностей сервера электронной подписи КриптоПро DSS дополнительно может выполняться проверка электронной

подписи, которая как и в случае с СЭП КриптоПро DSS не требует установки специального программного обеспечения. Для этой цели доступен сервис проверки электронной подписи КриптоПро SVS.

***КриптоПро DSS*** предоставляет пользователям интерактивный веб-интерфейс для управления криптографическими ключами и создания ЭП в документе, который пользователь загружает на ***КриптоПро DSS***. Таким образом, для работы с ***КриптоПро DSS*** пользователю необходим только браузер, никаких СКЗИ или средств электронной подписи устанавливать не нужно. Благодаря этому, использовать функции ***КриптоПро DSS*** можно с любого устройства с любой аппаратной платформой с любой операционной системой, где есть браузер.

Ключи пользователей хранятся в защищённом модуле ***КриптоПро HSM***, сертифицированный ФСБ Росси по классу защиты КВ2. Каждый пользователь получает доступ к своим ключам после прохождения процедуры надёжной аутентификации на ***КриптоПро DSS***.

В зависимости от настройки, ***КриптоПро DSS*** может реализовывать следующие способы аутентификации пользователя:

- классическая однофакторная аутентификация по логину и паролю;
- двухфакторная аутентификация с дополнительным вводом одноразового пароля, доставляемого пользователю через SMS (OTP-via-SMS);
- строгая криптографическая аутентификация с предъявлением сертификата клиента/пользователя;
- подключаемые модули, реализующие произвольные схемы аутентификации.

Кроме того, КриптоПро DSS может требовать подтверждения каждой операции подписания с помощью одноразового пароля, отправляемого через SMS.

***КриптоПро DSS*** предоставляет интерфейсы автоматизации, которые позволяют интегрировать использование ЭП в другие бизнес-процессы. Например, с веб-портала на определённом этапе, когда необходимо подписать документ, пользователь может быть автоматически перенаправлен на ЭП, где он интерактивно осуществит подписание документа и автоматически будет перенаправлен обратно с уже подписанным документом. Также при

необходимости приложение может автоматически подписать документ на ЭП от имени пользователя, запросив у него только аутентификационные данные.

Для повышения производительности и отказоустойчивости сервера электронной подписи может использоваться как вертикальное (увеличение производительности каждого сервера путем наращивания вычислительной мощности), так и горизонтальное (увеличение количества серверов и балансировка сетевой нагрузки) масштабирование.

Как мы видим, система безопасности применения электронной подписи смещается с безопасной эксплуатации средства электронной подписи (в данном случае ПАКМ «КриптоПро HSM», сертифицированный ФСБ России по классу КВ2) на систему безопасной и однозначной аутентификации пользователей (владельцев ключей) на сервере «КриптоПро DSS». А эта система не является частью ПАКМ «КриптоПро HSM» и не описана в эксплуатационной документации на «КриптоПро HSM» и, следовательно, не одобрена ФСБ России.

Для того, что бы утверждать о применении квалифицированной электронной подписи в облачной технологии, нужно иметь одобрение ФСБ России на всю реализацию этой технологии. Одобрение может быть выражено в форме наличия сертификата соответствия на «КриптоПро DSS» или в форме заключения о контроле встраивания ПАКМ «КриптоПро HSM» в сервер «КриптоПро DSS». Компания КРИПТО-ПРО идёт вторым путём…