Кафедра защиты информации

Нормативное регулирование в области ЭЦП

Табаков Кирилл Викторович гр.116

МФТИ 2005

Содержание:

Введение

Общие тенденции

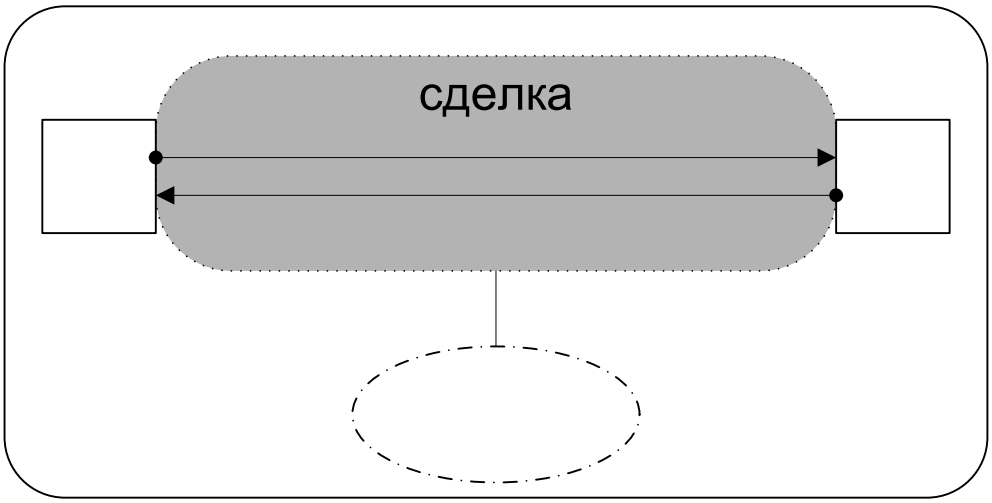
В связи с все более усложняющимися отношениями между людьми стало необходимо осуществление взаимодействия между двумя людьми, минуя личные контакты. Методами такого виртуального контакта были посредники, тайники, телефон, Интернет. В век информации и организаций на первый план выходит Интернет. Во-первых, он позволяет быстро и вне зависимости от местоположения людей осуществлять отношения между ними. Во-вторых, заменяет истинный объект отношения на электронное описание его, над которым и совершается сделка.

Всё это приводит к заметному возрастанию активности в области осуществления электронных сделок. Но следствием усложнения и ускорения отношений возникает необходимость защиты достоверности этих сделок. В Интернете выдать себя за другое лицо или подать объект, который существует только на бумаге, гораздо легче, чем при реальном контакте между сторонами, вступающими в отношение.

Т.о. появление новых технологий в аспекте скорости и простоты заметно облегчают деятельность, а в аспекте защиты достоверности также заметно усложняют. В данной статье рассматривается методы удостоверения электронных документов, используя ЭЦП.

Схема использования ЭЦП

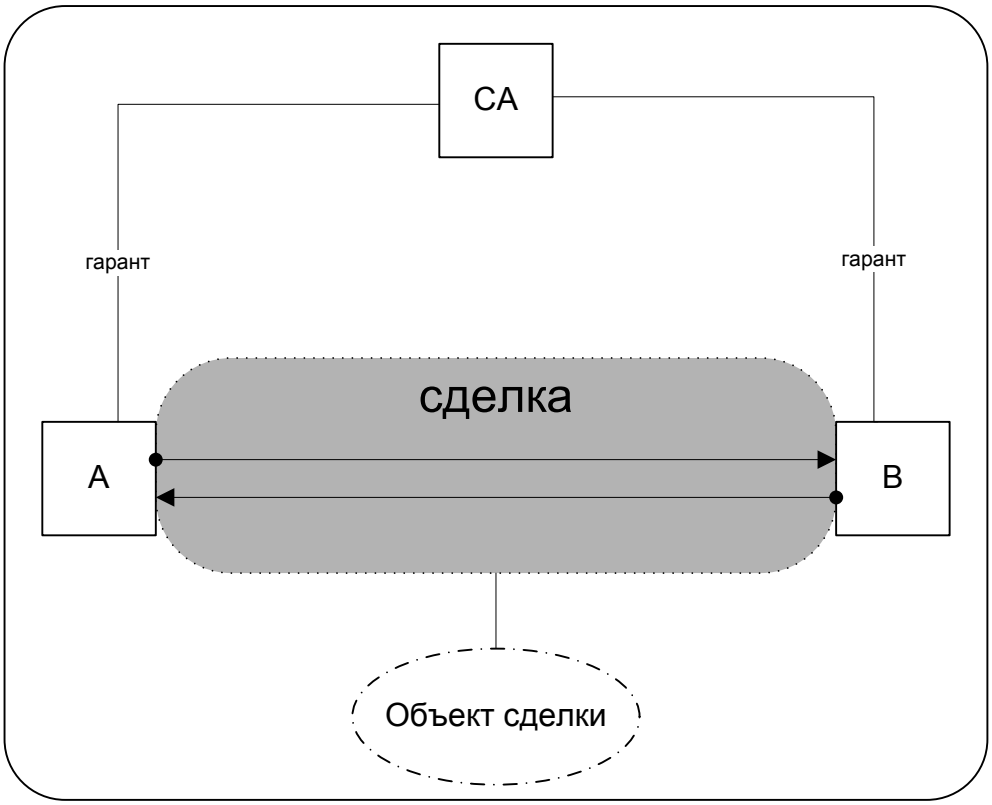
Для начала надо рассмотреть схему отношения между двумя субъектами «А» и «Б».



Два субъекта хотят заключить сделку по поводу объекта сделки. Для простоты предположим, что объект сделки находится в отношении собственности с субъектом «Б», а субъект «А» хочет стать собственником объекта сделки вместо субъекта «Б». Предположим, что обе стороны согласны на сделку. Тогда возникают следующие потребности сторон, для того чтобы заключить сделку. «А» желает убедиться, что объект сделки существует и что «Б» действительно является собственником объекта сделки. После чего происходит сделка.

Теперь, когда имеем дело с электронной сделкой, все прежние требования остаются и добавляется еще одно. «А» желает убедиться что «Б» является именно тем, за кого себя выдает. Для этого используется третий субъект сделки, который берет на себя функцию гарантирования достоверности субъекта «Б» субъекту «А».

После выяснения сути дела можно переходить к конкретно используемой схеме.



Назовем новый субъект нашей сделки «СА». И остановимся поподробнее на том, что происходит в этом случае. Рассмотрим предыдущий пример о переходе собственности на объект сделки от субъекта «Б» к субъекту «А».

«А» и «Б» находятся в отношении желания заключить сделку по поводу объекта сделки. «Б» по прежнему является собственником объекта сделки, а «А» хочет стать собственником объекта сделки. «А» и «СА» находятся в отношении: «А» является абонентом «СА» и хочет, чтобы «СА» гарантировал что, «Б» именно тот, за кого себя выдает. «Б» и «СА» находятся в отношении: «Б» является абонентом «СА», которые еще и предоставляет «Б» возможность аутентифицировать себя перед «А». Помимо этого есть необходимость заверения свершения сделки – еще один аспект отношения «А» и «Б».

Теперь можно обобщить понятие сделки, сделав её двусторонней, т.е. сливаем аспекты отношений «А» и «Б» с «СА» и получаем отношение абонента «СА» с «СА». И запишем получившееся отношение в явном виде:

1. «СА» предоставляет возможность абоненту идентифицировать себя перед другими абонентами,
2. «СА» предоставляет абоненту статус другого абонента,
3. «СА» предоставляет возможность абонентам заверять свершение сделки между двумя абонентами

Первый аспект отношения реализуется предоставлением сертификата ЭЦП всем абонентам «СА». Предоставление сертификата ЭЦП подразделяется на 3 крупные подфункции:

1. обеспечение получения сертификата,
2. обеспечение использования сертификата,
3. обеспечение аннулирования сертификата.

Под статусом абонента здесь понимается:

1. статус сертификата (действителен/недействителен),
2. полномочия подтверждать сделки данной ЭЦП.

Про третий аспект отношения следует заметить, что он реализуется ровно тем же методом, что и первый - ЭЦП.

После того, как выявлены все аспекты взаимодействия, можно приступать к анализу нормативной базы в аспекте распределению полномочий и ответственности между субъектами взаимодействия.

Анализ законодательства РФ в области ЭЦП.

Анализ нормативной базы РФ в области ЭЦП дает следующие цитаты.

«1. "Гражданский Кодекс Российской Федерации", Часть первая, Статья 160, п.2, в котором говорится: "Использование при совершении сделок ...электронно-цифровой подписи ...допускается в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон":

Часть первая, Статья 434, п.1
"Если стороны договорились заключить договор в определенной форме, он считается заключенным после придания ему условленной формы, хотя бы законом для договоров данного вида такая форма не требовалась".

Часть первая, Статья 434, п.2
"Договор в письменной форме может быть заключен ...путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору";

2. Федеральный Закон "Об информации, информатизации и защите информации", Глава 2, Статья 5, п.3
"Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования";

3. **Федеральный закон «Об электронной цифровой подписи» №1-ФЗ от 10 января 2002 года Статья 4 п.1**
"Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: сертификат ключа подписи, относящийся к электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; подтверждена подлинность электронной цифровой подписи в электронном документе; электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи."

Статья 5, п.1.
"Создание ключей электронных цифровых подписей осуществляется для использования в: информационной системе общего пользования ее участником или по его обращению удостоверяющим центром; корпоративной информационной системе в порядке, установленном в этой системе. Статус удостоверяющего центра, обеспечивающего функционирование корпоративной информационной системы, определяется ее владельцем или соглашением участников этой системы."

Статья 17, п.2.
"Порядок использование электронных цифровых подписей в корпоративной информационной системе устанавливается решением владельца корпоративной информационной системы или соглашением участников этой системы."

Статья 17, п.3.
"Содержание информации в сертификатах ключей подписи, порядок ведения реестра сертификатов ключей подписей, порядок хранения аннулированных сертификатов ключей подписей, случаи утраты указанными сертификатами юридической силы в корпоративной

информационной системе регламентируются решением владельца этой системы или соглашением участников корпоративной информационной системы."

4. Официальные материалы Высшего Арбитражного Суда РФ и СССР: Инструктивные указания Госарбитража СССР от 29 июня 1979 года №И-1-4 «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронно-вычислительной техники». Стороны по арбитражным делам в обоснование своих требований и возражений вправе представлять арбитражам документы, подготовленные с помощью электронно-вычислительной техники. Эти документы, поскольку они содержат данные об обстоятельствах, имеющих значение для дела, должны приниматься органами арбитража на общих основаниях в качестве письменных доказательств.

Письмо от 24 апреля 1992 г. № К-3/96 , согласно которого "Высший Арбитражный Суд РФ считает возможным принимать по рассматриваемым делам в качестве доказательств документы, заверенные электронной подписью печатью типа "ЛАН Крипто";

Письмо от 19 августа 1994 г № С1-7 / оп-578, где сказано: "В том случае, когда стороны изготовили и подписали договор с помощью электронно-вычислительной техники, в которой использована система цифровой (электронной) подписи, они могут представлять в арбитражный суд доказательства по спору, вытекающему из этого договора, также заверенные цифровой (электронной) подписью.

Если же между сторонами возник спор о наличии договора и других документов, подписанных цифровой (электронной) подписью, арбитражному суду следует запросить у сторон выписку из договора, в котором указана процедура порядка согласования разногласий, на какой стороне лежит бремя доказывания тех или иных фактов и достоверности подписи.

С учетом этой процедуры арбитражный суд проверяет достоверность представленных сторонами доказательств. При необходимости арбитражный суд вправе назначить экспертизу по спорному вопросу, используя при этом предусмотренную договором процедуру.

В случае отсутствия в таком договоре процедуры согласования разногласий и порядка доказывания подлинности договора и других документов, а одна из сторон оспаривает наличие подписанного договора и других документов, арбитражный суд вправе не принимать в качестве доказательств документы, подписанные цифровой (электронной) подписью.

Арбитражному суду, разрешающему подобный спор, следует оценить заключенный таким образом договор, всесторонне рассмотреть вопрос и о том, добровольно и со знанием дела стороны включили в договор процедуру рассмотрения споров и доказывания тех или иных фактов, не была ли она навязана стороне другой стороной с целью обеспечения только своих интересов и ущемления интересов другой стороны, и с учетом этой оценки вынести решение по конкретному спору".

Письмо от 7 июня 1995 года № С1 / 03-316, в котором воспроизведены положения статьи 5 федерального закона "Об информации, информатизации и защите информации" (см. выше), а также добавлено:

"Следует иметь в виду, что при соблюдении указанных условий, в том числе при подтверждении юридической силы документа электронной цифровой подписью, этот документ может признаваться в качестве доказательства по делу, рассматриваемому арбитражным судом".

В договоре между сторонами указана процедура порядка согласования и разрешения спорных вопросов. Программно-технические средства, применяемые в МИТС, позволяют

получать однозначные (бесспорные ответы) на спорные вопросы, возникающие с применением ЭЦП.

5. В качестве иллюстративных могут быть использованы материалы Арбитражного суда г. Москвы по делу № 40413 от 28 июля 1993 года и материалы Третейского суда при АО "Межбанковский финансовый дом".

6. Арбитражный процессуальный кодекс РФ от 5 мая 1995 года №70-ФЗ, Статья 60, п.1:

"Письменным доказательством являются содержащие сведения об обстоятельствах, имеющих значение для дела, акты, договоры, справки, деловая корреспонденция, иные документы и материалы, в том числе полученные посредством факсимильной, электронной или иной связи, либо иным способом, позволяющим установить достоверность документа."

7. Вопрос о юридической силе «электронных документов» нашел отражение в ГОСТ 6.10.4-84 «Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения», а также в Рекомендациях РД 50-613-86 «Методические указания по внедрению и применению ГОСТ 6.10.4-84 (утв. Постановлением Госкомитета СССР по стандартам от 24 сентября 1986г. №2781).»

Вышеуказанный список цитат взят с сайта: http://www.ros-expo.com/ecp/ecpur.html.

Гражданский кодекс РФ говорит о возможности использования ЭЦП для заверения сделок между двумя сторонами по согласованию сторон. Т.е. он не накладывает никаких ограничений на распределение полномочий и ответственности между субъектами заключения электронной сделки, удостоверенной ЭЦП.

ФЗ "Об информации, информатизации и защите информации" говорит о наличии субъекта свершения сделки, который обеспечивает процедуру определения достоверности ЭЦП и гарантирует достоверность ЭЦП. Т.е. о наличии «СА» и о третьем аспекте отношения взаимодействия «СА» с абонентом «СА». Опять никаких ограничений на взаимодействие.

ФЗ «Об электронной цифровой подписи» №1-ФЗ от 10 января 2002 говорит о:

1. Правомочности ЭЦП при подтверждении заключения сделки (ЭЦП считается правомочной если она действительна, подлинна и подтверждает сделку в рамках своих полномочий),
2. Наличии «СА» (удостоверяющим центром общей или корпоративной информационной системы). Причем в случае корпоративной информационной системы следующие аспекты сертификата ЭЦП определяются владельцем информационной системы или соглашением участников:
   - порядок использование электронных цифровых подписей в корпоративной информационной системе,
   - содержание информации в сертификатах ключей подписи,
   - порядок ведения реестра сертификатов ключей подписей,
   - порядок хранения аннулированных сертификатов ключей подписей,
   - случаи утраты указанными сертификатами юридической силы в корпоративной информационной системе.

Из решений Высшего Арбитражного Суда РФ следует, что нормативная база РФ в области ЭЦП была не разработана, очень пространна и почти не указывала никаких действий для оперирования с ЭЦП до вступления в силу закона об ЭЦП. Но несмотря на вступление в силу этого закона многие аспекты оперирования с ЭЦП остаются нерегламентированными и неясными.

Заключение анализа нормативной базы РФ в области ЭЦП

Законодательная база РФ не фиксирует отношения в области ЭЦП. Устанавливает только довольно абстрактные ограничения. И по этому необходимо иметь структуру договора, которая бы давала возможность разграничения функций, полномочий и ответственности между субъектами заверения договора при помощи ЭЦП.

Концепция сертификата ЭЦП

Рассмотрим аспекты согласования «СА» с абонентом «СА»:

1. Получением абонентом сертификата ЭЦП
    a. фиксирование личной информации абонента
    b. фиксирование полномочий абонента по заверению свершения сделок ЭЦП
2. Процедура использования абонентом ЭЦП
    a. процедура использования ЭЦП для заверения свершения сделки
    b. процедура хранения абонентом секретного ключа ЭЦП
    c. процедура хранения «СА» информации об абоненте
3. Процедура аннулирования сертификата ЭЦП
    a. случаи потери ЭЦП юридической силы
    b. действия сторон в этих случаях

Для получения разнообразия оргформ реализации сертификата ЭЦП необходимо записать разнообразие значений по каждому аспекту согласования. Под значение аспекта понимается некая процедура с указанием конечных алгоритмов, действий и исполнителей этих действий и ответственности исполнителей при исполнении/неисполнении этих действий.

Заключение

В заключении следует добавить, что в сфере электронной коммерции (в которой и применяется электронная подпись) могут возникнуть неприятные ситуации, которые находятся за гранью этой концепции сертификата. К примеру, это взаимодействие двух субъектов сертификаты ЭЦП, которых выданы разными «СА». Решением этой неприятности может стать создание «СА», абонентами которого будут «СА» первого и второго из взаимодействующих субъектов, и который и будет обеспечивать сделку. А возможно и создание взаимодействия между «СА» абонентов. Как в первом, так и во втором случае существуют осложнения осуществления сделки. В первом случае подтверждающая функция ЭЦП становиться более громоздкой, а во втором случае возникает необходимость слияния баз ЭЦП двух «СА».

Несмотря на все осложнения ЭЦП является абсолютно новым методом облегчения взаимодействия между субъектами. Но этот метод остается не до конца разработанным и поэтому важную роль играет рейтинги «СА», предлагающих сертификаты «СА».

Источники:

1. http://www.ros-expo.com/ecp/ecpur.html
2. семинары по защите информации.