Содержание:

Введение

Сегодня сложно найти специалиста в области информатизации или телекоммуникаций, который бы не знал, что такое электронная цифровая подпись (ЭЦП). Однако мало кто осознает, что само по себе использование этой технологии только создает предпосылки для организации юридически значимого электронного документооборота. Точно так же как технология производства бумаги или авторучек - это лишь возможность организовать традиционный бумажный документооборот. Что необходимо предпринять, чтобы обмен электронными документами с ЭЦП стал столь же привычным, как и документами на бумажном носителе? Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющей идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе. Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий: сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;-подтверждена подлинностью электронной цифровой подписи в электронном документе; электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи. При этом электронной документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи. В скором будущем заключение договора будет возможно в электронной форме, который будет иметь такую же юридическую силу, как и письменный документ. Для этого он должен иметь механизм электронной цифровой подписи, подтверждаемый сертификатом. Владелец сертификата ключа подписи владеет закрытым ключом электронной цифровой подписи, что позволяет ему с помощью

средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы). Для того, чтобы электронный документ могли открыть и другие пользователи, разработана система открытого ключа электронной подписи. Для того, чтобы иметь возможность скреплять электронный документ механизмом электронной цифровой подписи, необходимо обратиться в удостоверяющий центр за получением сертификата ключа подписи. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи. Первый в России такой удостоверяющий центр запущен в сентябре 2002 г. Российским НИИ развития общих сетей (РосНИИРОС). Удостоверяющий центр по закону должен подтверждать подлинность открытого ключа электронной цифровой подписи.

Основные положения

Электронная цифровая подпись Хэш-функция защищаемого электронного документа представляет собой уникальное число, получаемое из исходного документа путем его преобразования с помощью сложного, но известного алгоритма (хэш-функции). Хэш-функция чувствительна к всевозможным искажениям исходного электронного документа, то есть изменение (искажение) хотя бы одного знака в исходном документе приводит в среднем к искажению половины знаков хэш-значения. Кроме того, она устроена таким образом, что, во-первых, по хэш-значению документа нельзя восстановить исходный электронный документ, а во-вторых, практически невозможно отыскать два различных электронных документа, которые обладали бы одним и тем же хэш-значением. Схема формирования электронной цифровой подписи под электронным документом его создателем (отправителем) предусматривает вычисление хэш-функции этого документа и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования и является значение ЭЦП как реквизит электронного документа, которое пересылается получателю вместе с этим документом. Таким образом, электронная цифровая подпись жестко увязывает содержание документа и секретный ключ для формирования ЭЦП и делает невозможным изменение документа без нарушения подлинности данной подписи. Функции ЭЦП: Поскольку электронная цифровая подпись - средство защиты информации, предоставляющее возможность контроля целостности и подтверждения подлинности электронного документа, то ЭЦП должна обеспечивать выполнение следующих основных функций: подтверждать, что

подписывающее лицо сознательно подписало электронный документ; подтверждать, что документ подписало именно подписывающее лицо и только оно; ЭЦП должна существенно зависеть от подписываемого документа, в том числе от имеющихся в нем отметок времени; подписывающее лицо не должно иметь возможности отказаться впоследствии от факта подписи электронного документа. Общая суть электронной подписи заключается в следующем: с помощью криптографической хэш-функции вычисляется относительно короткая строка символов фиксированной длины (хэш). Затем этот хэш шифруется закрытым ключом владельца - результатом является подпись документа. Подпись прикладывается к документу. В результате этого получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным. При ведении деловой переписки, при заключении контрактов подпись ответственного лица является непременным атрибутом документа, преследующим несколько целей: гарантирование истинности письма путем сличения подписи с имеющимся образцом и гарантирование авторства документа (с юридической точки зрения).Выполнение данных требований основывается на следующих свойствах подписи: подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему; подпись неподделываема, то есть служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ; подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно; документ с подписью является неизменяемым; подпись неоспорима; любое лицо, владеющее образцом подписи, может удостоверится, что документ подписан владельцем подписи. Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является электронно-цифровая подпись (ЭЦП), которая сохранила основные свойства обычной подписи.
Методы построения ЭЦП: шифрование электронного документа на основе симметричных алгоритмов. Данная схема предусматривает наличие в системе третьего лица - арбитра, пользующегося доверием обеих сторон. Авторизацией документа в данной схеме является сам факт шифрования электронного документа секретным ключом и передачи его арбитру. использование ассиметричных алгоритмов шифрования. Фактом подписания документа является шифрование его

на секретном ключе отправителя. схема ЭЦП - шифрование окончательного результата обработки электронного документа хеш-функцией при помощи ассиметричного алгоритма. Появление этих разновидностей обусловлено разнообразием задач, решаемых с помощью электронных технологий передачи и обработки электронных документов. При генерации ЭЦП используются параметры трех групп: общие параметры секретный ключ открытый ключ Отечественным стандартом на процедуры выработки и проверки ЭЦП является ГОСТ Р 34.10-94.

Понятие электронной цифровой подписи

Электронная цифровая подпись (далее - ЭЦП) -- реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП.

История развития и распространения электронной цифровой подписи

За рубежом:

1976 год Американские математики У. Диффи и М.Э. Хеллмэн опубликовали работу под названием "Новые направления в криптографии", которая существенно повлияла на дальнейшее развитие криптографии и, в частности, привела к появлению такого понятия, как "цифровая подпись".

1977 год Был разработан первый криптографический алгоритм - RSA.

1981 год Был разработан алгоритм DSA в 1981 г. и с тех пор используется как стандарт США для электронной цифровой подписи.

1984 год Разработана криптосистема - Схема Эль-Гамаля, лежит в основе стандартов электронной цифровой подписи в США и России.

1984 год Ш. Гольдвассер, С. Микали и Р. Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны

модели атак на алгоритмы ЭЦП, а также предложена схема GMR, отвечающая описанным требованиям.

1991 год Национальный институт стандартизации и технологий (NIST) США опубликовал стандарт на ЭЦП DSS (Digital Signature Standard).

1993 год Метод RSA был обнародован и принят в качестве стандарта. RSA можно применять как для шифрования/расшифрования, так и для генерации/проверки электронно-цифровой подписи.

1997 год В Германии был принят Закон "Об электронной цифровой подписи".

2003 год Верховной Радой Украины приняты законы “Об электронных документах и электронном документообороте” и “Об электронной цифровой подписи”.

В России:

1993 год Разработка отечественного закона об электронной цифровой подписи (ЭЦП).

1994 год Был принят первый отечественный стандарт в области ЭЦП -- ГОСТ Р34.10 -- 94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

1999 год Министерство Российской Федерации по связи и информатизации организовало разработку проекта федерального закона «Об электронной цифровой подписи», который создает правовые основы формирования надежной инфраструктуры, включающей удостоверяющие центры.

2001 год Правительство одобрило законопроект "Об электронной цифровой подписи".

2002 год Принятый новый стандарт на ЭЦП: ГОСТ Р 34.10-2001 «Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

2002 год Принят Федеральный закона «Об электронной цифровой подписи», который создал основу для использования электронного документа и электронной цифровой подписи.

6 апреля 2011 года президент России Дмитрий Медведев подписал закон «Об электронной подписи» (ЭП), одобренный Госдумой и Советом Федерации в марте.

Глава российского правительства Дмитрий Медведев подписал в начале 2013 года постановление №33, описывающее порядок использования «простой электронной подписи» при оказании государственных и муниципальных услуг в дополнение к уже используемой усиленной ЭП.

Виды электронной цифровой подписи

Существует 3 вида ЭЦП:

1. Присоединенная электронная цифровая подпись. В случае создания присоединенной подписи создается новый файл ЭЦП, в который помещаются данные подписываемого файла.

Достоинства присоединенной подписи: простота дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле, файл можно копировать, пересылать и т.п.

Недостаток: без использования средств СКЗИ (средства криптографической защиты информации) уже нельзя прочесть и использовать содержимое файла.

2. Отсоединенная электронная цифровая подпись. При создании отсоединенной подписи файл подписи создается отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется.

Достоинство: подписанный файл можно читать, не прибегая к СКЗИ.

Недостаток отсоединенной подписи: необходимость хранения подписанной информации в виде нескольких файлов.

3. Электронная цифровая подпись внутри данных (Наиболее распространена). Применение ЭЦП этого вида существенно зависит от приложения, которое их использует.

Недостаток: вне приложения, создавшего ЭЦП, без знания структуры его данных проверить подлинность частей данных, подписанных ЭЦП затруднительно.

Предназначение и преимущества электронной цифровой подписи

Цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ. Кроме этого, использование цифровой подписи позволяет осуществить:

- контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

- защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.

- невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.

- доказательное подтверждение авторства документа. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

- значительное сокращение времени, затрачиваемое на оформление сделки и обмен документацией;

- совершенствование и уменьшение стоимости процедуры подготовки, доставки, учета и хранения документов;

- строительство корпоративной системы обмена документами;

- выбор наиболее выгодного ценового предложения товаров и услуг на электронных торгах, аукционах и тендерах;

- взаимоотношения с населением, организациями и властными структурами на современной основе, более эффективно, с наименьшими издержками;

- расширение географии бизнеса, совершая в удаленном режиме экономические операции с партнерами из любых регионов России.

Атаки на электронную цифровую подпись

Стойкость большинства схем ЭЦП зависит от стойкости ассиметричных алгоритмов шифрования и хэш-функций. Существует следующая классификация атак на схемы ЭЦП: атака с известным открытым ключом. атака с известными подписанными сообщениями - противник, кроме открытого ключа имеет и набор подписанных сообщений. простая атака с выбором подписанных сообщений - противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения. Направленная атака с выбором сообщения Адаптивная атака с выбором сообщения. Каждая атака преследует определенную цель, которые можно разделить на несколько классов: полное раскрытие-противник находит секретный ключ пользователя. универсальная подделка-противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП. селективная подделка-подделка подписи под выбранным сообщением. экзистенциальная подделка-подделка подписи хотя бы для одного случайно выбранного сообщения. На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя: отказ одного из участников авторства документа. модификация принятого электронного документа. подделка документа. навязывание сообщений в процессе передачи - противник перехватывает обмен сообщениями и модифицирует их. Так же существуют нарушения, от которых невозможно оградить систему обмена сообщениями - это повтор передачи сообщения и фальсификация времени отправления сообщения. Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений. В развитых странах мира, в том числе и в Российской Федерации, электронная цифровая подпись широко используется в гражданском обороте. Различные банки Российской Федерации эффективно используют ЭЦП для осуществления своих операций путем пересылки банковских электронных документов по корпоративным и общедоступным телекоммуникационным сетям. Для преодоления препятствий необходимо создание унифицированных правил, при помощи которых страны могут в национальном законодательстве решить основные проблемы, связанные с юридической значимостью записей в памяти ЭВМ, письменной формой электронных данных (в том числе и документов), подписью под такими данными, оригиналом и копиями электронных данных, а также признанием в качестве судебных

доказательств электронных данных, заверенных электронной подписью.10 января 2002 года был принят Федеральный Закон «Об электронной цифровой подписи», который закладывает основы решения проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными документами, при соблюдении которых электронная цифровая подпись признается юридически равнозначной собственноручной подписи человека в документе на бумажном носителе. Федеральный Закон «Об электронной цифровой подписи» определяет условия использования ЭЦП в электронных документах органами государственной власти и государственными организациями, а также юридическими и физическими лицами, при соблюдении которых: средства создания подписи признаются надежными; сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены; предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам; соблюдаются правовые нормы, содержащие требования к письменной форме документа; сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства; обеспечивается охрана персональной информации. В Законе устанавливаются права и обязанности обладателя электронной цифровой подписи. В соответствии с законом, владельцем сертификата ключа подписи (обладателем электронной цифровой подписи) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись электронных документах (подписывать электронные документы). На владельца сертификата ключа подписи накладываются определённые обязанности, такие, как: хранение в тайне закрытого ключа электронной цифровой подписи; не использование для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее; обязанность немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена. Согласно ст. 6 данного Закона , сертификат ключа подписи должен содержать следующие сведения: уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре

удостоверяющего центра; фамилию, имя, отчество владельца сертификата ключа подписи или псевдоним владельца; открытый ключ электронной цифровой подписи; наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи; сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение. Основой для применения электронных документов, заверяемых электронной цифровой подписью, служат следующие законодательные и нормативные акты Российской Федерации: -Гражданский кодекс РФ. «Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон» (ч 1. ст.160 ГК РФ) «Договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору» (ч.1 ст.434 ГК РФ). «Договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи (п. 2 ст. 160), кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом» (ч.2 ст.847 ГК РФ). Федеральный Закон «Об информации, информатизации и защите информации». «Документ, полученный из автоматизированной информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законодательством РФ» (ст.5 ФЗ). 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. Официальные материалы Высшего Арбитражного Суда РФ Письмо от 24.04.92 № К-3/96, в соответствии с которым «Высший Арбитражный Суд РФ считает возможным принимать по рассматриваемым делам в качестве доказательств документы, заверенные электронной подписью (печатью)». В Письме от 19.08.94 № С1-7/ОП-587 указывается: «В том числе-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». Конвенция ООН «Об использовании электронных сообщений в международных договорах». Россия подписала ее в мае 2007 года, став тем самым десятой страной, признающей документы в электронной форме наравне с традиционной бумажной формой. Конвенция вступила в силу для нашей страны в декабре 2007 года . С этого момента российские компании получили право использовать электронные сообщения при работе с международными договорами.

Заключение

Самый обычный вопрос, который задаётся человеком, впервые столкнувшимся с необходимостью использования цифровой подписи, звучит примерно так: «А зачем мне вообще электронная цифровая подпись? И нужна ли?» Электронная цифровая подпись может использоваться в нескольких ипостасях. Закон «Об ЭЦП» определяет условия применения ЭЦП как ответственной подписи в документе, аналога собственноручной подписи и печати. Подобным образом ЭЦП используется в системах электронного документооборота различного назначения (организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего).Однако область применения ЭЦП не ограничивается приведенными областями. Сама по себе, электронная цифровая подпись - великолепный механизм обеспечения целостности и подтверждения авторства и актуальности любых данных, представленных в электронном виде. Электронная подпись поможет проверить целостность электронного письма (e-Mail) и убедиться в надёжности отправителя, однозначно определит автора статьи, опубликованной в Интернете, и укажет дату публикации, позволит написать собственное мнение о прочитанном документе в Microsoft Word и прикрепить его в виде «стикера» к файлу, не «испортив» сам файл своими пометками, при этом надёжно привязав такой «стикер» к текущему содержимому документа (при изменении текста документа «стикер» сразу обнаружит, что документ изменялся),оставит «визитную карточку» о действиях, совершённых в электронном мире, подтвердит полномочия и т.п. Цифровая подпись обеспечивает: Удостоверение источника документа. В зависимости от деталей определения «документа» могут быть подписаны такие поля как: автор, внесённые изменения, метка времени и т. д. Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно подпись станет недействительной.

Невозможность отказа от авторства. Так как создать корректную подпись можно лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом. Возможны следующие угрозы цифровой подписи: Злоумышленник может попытаться подделать подпись для выбранного им документа. Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. При использовании надёжной хэш-функции, вычислительно сложно создать поддельный документ с таким же хэшем, как у подлинного. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. Тем не менее, возможны ещё такие угрозы системам цифровой подписи: Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа. Злоумышленник может обманом заставить владельца подписать какой-либо документ, например используя протокол слепой подписи. Злоумышленник может подменить открытый ключ владельца (см. управление ключами) на свой собственный, выдавая себя за него.

Список использованной литературы

1. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года №1-ФЗ . Электронная подпись и шифрование // МО ПНИЭИ . Современные криптографические методы защиты информации - системы с открытым ключом . «Юридическая сила электронных документов» О. Беззубцев

2 « Некоторые вопросы правового обеспечения использования ЭЦП» Беззубцев О.А., Мартынов В.Н., Мартынов В.М.

3.«Информатика для юристов и экономистов» Под ред. С.В. Симоновича. СПб.: Питер, 2002.

4«Электронный документ» А. Марченко.

5«Законодательное регулирование правового статуса ЭЦП. Основные положения» Ткачев А.В

6«Юридический справочник руководителя»2008 г.