Содержание:

Назначение и применение ЭЦП

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.

Все эти свойства ЭЦП позволяют использовать её для следующих целей:

- Декларирование товаров и услуг (таможенные декларации)
- Регистрация сделок по объектам недвижимости
- Использование в банковских системах
- Электронная торговля и госзаказы
- Контроль исполнения государственного бюджета
- В системах обращения к органам власти

- Для обязательной отчетности перед государственными учреждениями
- Организация юридически значимого электронного документооборота
- В расчетных и трейдинговых системах

История возникновения

В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «**электронная цифровая подпись**», хотя они всего лишь предполагали, что схемы ЭЦП могут существовать.

В 1977 году, Рональд Ривест, Ади Шамир и Леонард Адлеман разработали криптографический алгоритм RSA, который без дополнительных модификаций можно использовать для создания примитивных цифровых подписей.

Вскоре после RSA были разработаны другие **ЭЦП**, такие как алгоритмы цифровой подписи Рабина, Меркле.

В 1984 году Шафи Гольдвассер, Сильвио Микали и Рональд 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.

В 1994 году Главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации был разработан первый российский стандарт **ЭЦП** — ГОСТ Р 34.10-94, основанный на вычислениях в группе точек эллиптической кривой и на хеш-функции, описанной в ГОСТ Р 34.11-94.

В 2002 году для обеспечения большей криптостойкости алгоритма взамен ГОСТ Р 34.10-94 был введен стандарт ГОСТ Р 34.10-2001. В соответствии с этим стандартом термины «**электронная цифровая подпись**» и «**цифровая подпись**» являются синонимами.

Алгоритмы

Существует несколько схем построения **цифровой подписи**:

- На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы **ЭЦП** наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем. Их появление обусловлено разнообразием задач, решаемых с помощью **ЭЦП**.

Использование хеш-функций

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах **ЭЦП** зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма **ЭЦП**, поэтому в схеме может быть использована любая надёжная хэш-функция.

Использование хэш-функций даёт следующие преимущества:

- **Вычислительная сложность**. Обычно хеш цифрового документа делается во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хеша являются более быстрыми, чем алгоритмы **ЭЦП**. Поэтому формировать хэш документ и подписывать его получается намного быстрее, чем подписывать сам документ.
- **Совместимость**. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хеш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.
- **Целостность**. Без использования хеш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения **ЭЦП**. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Стоит заметить, что использование хеш-функции не обязательно при цифровой подписи, а сама функция не является частью алгоритма **ЭЦП**, поэтому хеш-функция может использоваться любая или не использоваться вообще.

В большинстве ранних систем **ЭЦП** использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы к атакам с использованием открытого ключа (см. ниже), так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст. Чтобы избежать этого, вместе с цифровой подписью используется хеш-функция, то есть, вычисление подписи осуществляется не относительно самого документа, а относительно его хеша. В этом случае в результате верификации можно получить только хеш исходного текста, следовательно, если используемая хеш-функция криптографически стойкая, то получить исходный текст будет вычислительно сложно, а значит атака такого типа становится невозможной.

Симметричная схема

Симметричные схемы **ЭЦП** менее распространены чем асимметричные, так как после появления концепции цифровой подписи не удалось реализовать эффективные алгоритмы подписи, основанные на известных в то время симметричных шифрах. Первыми, кто обратил внимание на возможность симметричной схемы цифровой подписи, были основоположники самого понятия **ЭЦП** Диффи и Хеллман, которые опубликовали описание алгоритма подписи одного бита с помощью блочного шифра. Асимметричные схемы **цифровой подписи** опираются на вычислительно сложные задачи, сложность которых еще не доказана, поэтому невозможно определить, будут ли эти схемы сломаны в ближайшее время, как это произошло со схемой, основанной на задаче об укладке ранца. Также для увеличения криптостойкости нужно увеличивать длину ключей, что приводит к необходимости переписывать программы, реализующие асимметричные схемы, и в некоторых случаях перепроектировать аппаратуру. Симметричные схемы основаны на хорошо изученных блочных шифрах.

В связи с этим симметричные схемы имеют следующие преимущества:

- Стойкость симметричных схем **ЭЦП** вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.

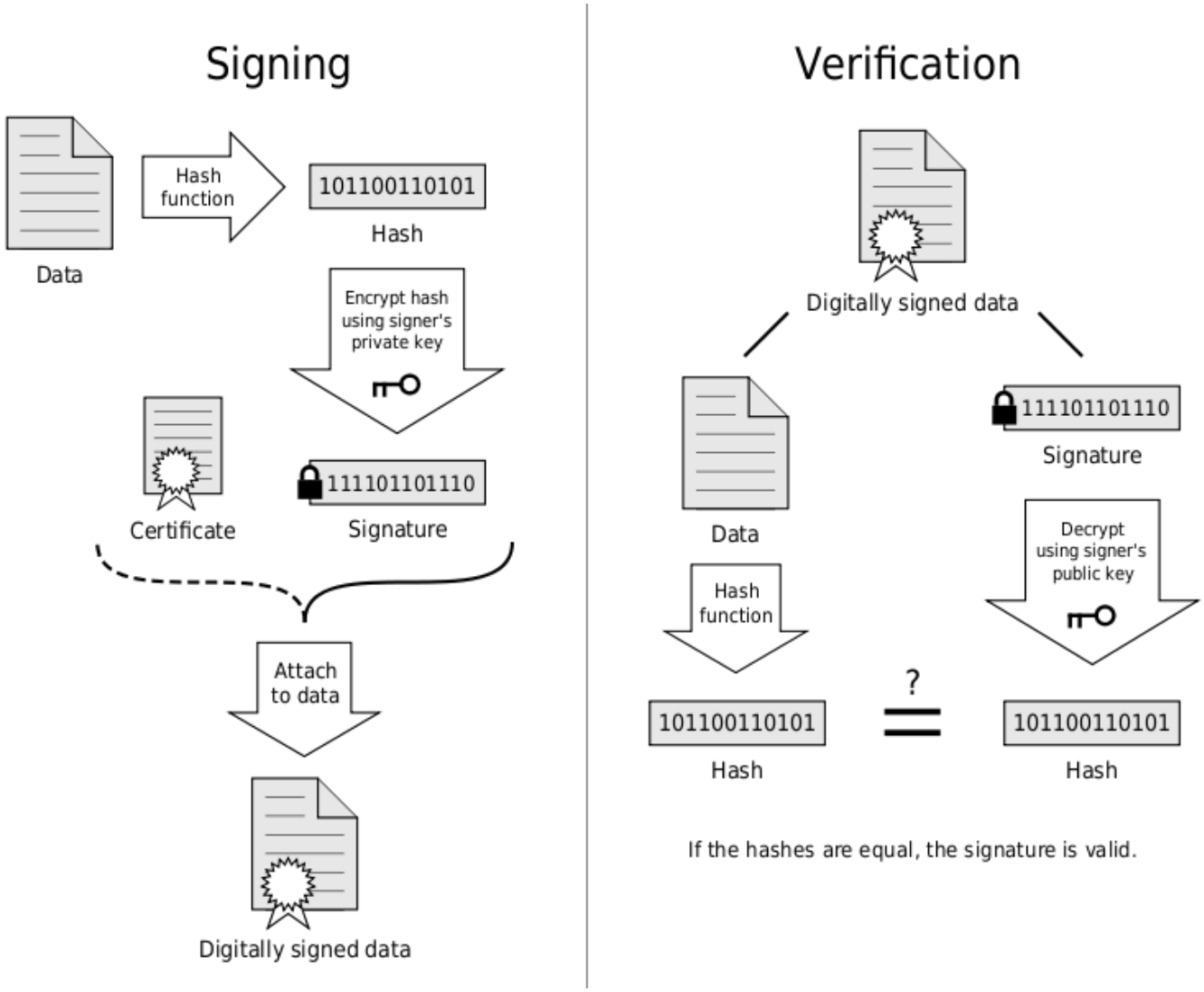
- Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных **ЭЦП** есть и ряд недостатков:

- Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.
- Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Из-за рассмотренных недостатков симметричная схема **ЭЦП** Диффи-Хелмана не применяется, а используется её модификация, разработанная Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объема вычислений. Для преодоления проблемы «одноразовости» ключей используется генерация отдельных ключей из главного ключа.

Асимметричная схема



Схема, поясняющая алгоритмы подписи и проверки

Асимметричные схемы **ЭЦП** относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых зашифрование производится с помощью открытого ключа, а расшифрование — с помощью закрытого, в схемах цифровой подписи подписывание производится с применением закрытого ключа, а проверка — с применением открытого.

Общепризнанная схема цифровой подписи охватывает три процесса:

- **Генерация ключевой пары**. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.
- **Формирование подписи**. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.

- **Проверка (верификация) подписи**. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

- Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
- Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

Следует отличать **электронную цифровую подпись** от кода аутентичности сообщения (MAC).

Виды асимметричных алгоритмов ЭЦП

Как было сказано выше, чтобы применение **ЭЦП** имело смысл, необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

Обеспечение этого во всех асимметричных алгоритмах цифровой подписи опирается на следующие вычислительные задачи:

- Задачу **дискретного логарифмирования** (EGSA)
- Задачу **факторизации**, то есть разложения числа на простые множители (RSA)

Вычисления тоже могут производиться двумя способами: на базе математического аппарата эллиптических кривых (ГОСТ Р 34.10-2001) и на базе полей Галуа (DSA). В настоящее время самые быстрые алгоритмы дискретного логарифмирования и факторизации являются субэкспоненциальными. Принадлежность самих задач к классу NP-полных не доказана.

Алгоритмы **ЭЦП** подразделяются на обычные цифровые подписи и на цифровые подписи с восстановлением документа. При верификации цифровых подписей с восстановлением документа тело документа восстанавливается автоматически, его не нужно прикреплять к подписи. Обычные цифровые подписи требуют присоединение документа к подписи. Ясно, что все алгоритмы, подписывающие хеш документа, относятся к обычным **ЭЦП**. К **ЭЦП** с восстановлением документа относится, в частности, RSA.

Схемы цифровой подписи могут быть одноразовыми и многоразовыми. В одноразовых схемах после проверки подлинности подписи необходимо провести замену ключей, в многоразовых схемах это делать не требуется.

Также алгоритмы **ЭЦП** делятся на детерминированные и вероятностные. Детерминированные **ЭЦП** при одинаковых входных данных вычисляют одинаковую подпись. Реализация вероятностных алгоритмов более сложна, так как требует надежный источник энтропии, но при одинаковых входных данных подписи могут быть различны, что увеличивает криптостойкость. В настоящее время многие детерминированные схемы модифицированы в вероятностные.

В некоторых случаях, таких как потоковая передача данных, алгоритмы **ЭЦП** могут оказаться слишком медленными. В таких случаях применяется быстрая цифровая подпись. Ускорение подписи достигается алгоритмами с меньшим количеством модульных вычислений и переходом к принципиально другим методам расчета.

Перечень алгоритмов ЭЦП

Асимметричные схемы:

- FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
- Схема Эль-Гамаля
- Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
- Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001
- Схема Диффи-Лампорта
- Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
- Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99
- Схема Шнорра
- Pointcheval-Stern signature algorithm
- Вероятностная схема подписи Рабина
- Схема BLS (Boneh-Lynn-Shacham)
- Схема GMR (Goldwasser-Micali-Rivest)

На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям:

- Групповая цифровая подпись
- Неоспоримая цифровая подпись
- «Слепая» цифровая подпись и справедливая «слепая» подпись
- Конфиденциальная цифровая подпись
- Цифровая подпись с доказуемостью подделки
- Доверенная цифровая подпись

Подделка подписей

Анализ возможностей подделки подписей называется криптоанализ. Попытку сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».

Модели атак и их возможные результаты

В своей работе Гольдвассер, Микали и Ривест описывают следующие модели атак, которые актуальны и в настоящее время:

- **Атака с использованием открытого ключа**. Криптоаналитик обладает только открытым ключом.
- **Атака на основе известных сообщений**. Противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им.
- **Адаптивная атака на основе выбранных сообщений**. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.

Также в работе описана классификация возможных результатов атак:

- **Полный взлом цифровой подписи**. Получение закрытого ключа, что означает полный взлом алгоритма.
- **Универсальная подделка цифровой подписи**. Нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа.

- **Выборочная подделка цифровой подписи**. Возможность подделывать подписи для документов, выбранных криптоаналитиком.
- **Экзистенциальная подделка цифровой подписи**. Возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком.

Ясно, что самой «опасной» атакой является адаптивная атака на основе выбранных сообщений, и при анализе алгоритмов **ЭЦП** на криптостойкость нужно рассматривать именно ее (если нет каких-либо особых условий).

При безошибочной реализации современных алгоритмов **ЭЦП** получение закрытого ключа алгоритма является практически невозможной задачей из-за вычислительной сложности задач, на которых **ЭЦП** построена. Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго рода. Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода — выборочной. С учетом применения хеш-функций, нахождение коллизий для алгоритма подписи эквивалентно нахождению коллизий для самих хеш-функций.

Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

- Документ представляет из себя осмысленный текст.
- Текст документа оформлен по установленной форме.
- Документы редко оформляют в виде Plain Text — файла, чаще всего в формате DOC или HTML.

Если у фальшивого набора байт и произойдет коллизия с хешем исходного документа, то должны выполниться 3 следующих условия:

- Случайный набор байт должен подойти под сложно структурированный формат файла.
- То, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме.
- Текст должен быть осмысленным, грамотным и соответствующий теме документа.

Впрочем, во многих структурированных наборах данных можно вставить произвольные данные в некоторые служебные поля, не изменив вид документа для пользователя. Именно этим пользуются злоумышленники, подделывая документы.

Вероятность подобного происшествия также ничтожно мала. Можно считать, что на практике такого случиться не может даже с ненадёжными хеш-функциями, так как документы обычно большого объёма — килобайты.

Получение двух документов с одинаковой подписью (коллизия второго рода)

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хеширования MD5.

Социальные атаки

Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами.

- 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 на свой собственный, выдавая себя за него.

Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

Управление ключами

Управление открытыми ключами

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭЦП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя, защитить эти ключи от подмены злоумышленником, а также организовать отзыв ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями.

Центр сертификации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзыв истекших и компрометированных сертификатов и ведет базы выданных и отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

Хранение закрытого ключа

Смарт-карта и USB-брелоки eToken

Закрытый ключ является наиболее уязвимым компонентом всей криптосистемы цифровой подписи. Злоумышленник, укравший закрытый ключ пользователя, может создать действительную цифровую подпись любого электронного документа от лица этого пользователя. Поэтому особое внимание нужно уделять способу хранения закрытого ключа. Пользователь может хранить закрытый ключ на своем персональном компьютере, защитив его с помощью пароля. Однако такой способ хранения имеет ряд недостатков, в частности, защищенность ключа полностью зависит от защищенности компьютера, и пользователь может подписывать документы только на этом компьютере.

В настоящее время существуют следующие устройства хранения закрытого ключа:

- Дискеты
- Смарт-карты
- USB-брелок
- Таблетки Touch-Memory

Кража или потеря одного из таких устройств хранения может быть легко замечена пользователем, после чего соответствующий сертификат может быть немедленно отозван.

Наиболее защищенный способ хранения закрытого ключа — хранение на смарт-карте. Для того, чтобы использовать смарт-карту, пользователю необходимо не только её иметь, но и ввести PIN-код, то есть, получается двухфакторная аутентификация. После этого подписываемый документ или его хэш передается в карту, её процессор осуществляет подписывание хеша и передает подпись обратно. В процессе формирования подписи таким способом не происходит копирования закрытого ключа, поэтому все время существует только единственная копия ключа. Кроме того, произвести копирование информации со смарт-карты сложнее, чем с других устройств хранения.

В соответствии с законом «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ», ответственность за хранение закрытого ключа владелец несет сам.

Использование ЭЦП

В России

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи», ст. 3 и определяет ЭЦП так:

«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 позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе»

После становления ЭЦП при использовании в электронном документообороте между кредитными организациями и кредитными бюро в 2005 году активно стала развиваться инфраструктура электронного документооборота между налоговыми органами и налогоплательщиками. Начал работать приказ Министерства по налогам и сборам РФ от 2 апреля 2002 г. N БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи». Он определяет общие принципы информационного обмена при представлении налоговой декларации в электронном виде по телекоммуникационным каналам связи.

В Законе РФ от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» прописаны условия использования ЭЦП, особенности её использования в сферах государственного управления и в корпоративной информационной системе.

Благодаря ЭЦП теперь, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете, через «Системы электронной торговли», обмениваясь с контрагентами необходимыми документами в электронном виде, подписанными ЭЦП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.