Электронная Цифровая Подпись

Электронная подпись – что это?

Электронная подпись (ЭП) — информация в электронной форме, присоединенная к другой информации в электронной форме (электронный документ) или иным образом связанная с такой информацией. Используется для определения лица, подписавшего информацию (электронный документ).

Электронная подпись представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭП и проверить принадлежность подписи владельцу сертификата ключа ЭП. Значение реквизита получается в результате криптографического преобразования информации с использованием *закрытого ключа ЭП*.

Назначение и применение ЭП

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Использование электронной 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.

Назначение и применение ЭП

Использование электронной подписи позволяет осуществить:

- 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.

История возникновения ЭП

- 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.

ЭП в России

- 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.
- В 2002 году для обеспечения большей криптостойкости алгоритма взамен ГОСТ Р 34.10-94 был введен стандарт ГОСТ Р 34.10-2001, основанный на вычислениях в группе точек

эллиптической кривой. В соответствии с этим стандартом, термины «электронная цифровая подпись» и «цифровая подпись» являются синонимами.

Виды ЭП в РФ

Федеральный закон РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» устанавливает следующие виды ЭП:

- Простая электронная подпись (ПЭП);
- Усиленная неквалифицированная электронная подпись (НЭП);
- Усиленная квалифицированная электронная подпись (КЭП).

Виды ЭП в РФ

Простая электронная подпись:

Создается с помощью кодов, паролей и других инструментов. Эти средства защиты позволяют идентифицировать автора подписанного документа. Важным свойством простой электронной подписи является отсутствие возможности проверить документ на предмет наличия изменений с момента подписания.

Усиленная неквалифицированная подпись:

Создается с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений.

Простые и усиленные неквалифицированные подписи заменяют подписанный бумажный документ в случаях, оговоренных законом или по согласию сторон. Усиленная подпись также может рассматриваться как аналог документа с печатью.

Виды ЭП в РФ

Усиленная квалифицированная подпись:

Усиленная подпись должна обязательно иметь сертификат аккредитованного Удостоверяющего центра. Эта подпись заменяет бумажные документы во всех случаях, за исключением тех, когда закон требует наличия исключительно документа на бумаге. С помощью таких подписей можно организовать юридически значимый электронный документооборот с партнерскими компаниями, органами государственной власти и внебюджетными фондами.

Активное развитие новых сервисов на основе применения квалифицированной электронной подписи ожидается в ближайшей перспективе. Организация юридически значимого электронного документооборота позволит ускорить процедуру обмена документами и сэкономить значительные денежные и трудовые ресурсы.

Удостоверяющий центр

При использовании асимметричного криптографического преобразования возникает задача обеспечения совместного использования зашифрованной информации, связанная с **управлением ключами.** Для решения этой трудоемкой задачи создаются специальные удостоверяющие центры.

Удостоверяющий центр – это юридическое лицо, согласно Закону «Об электронной подписи» выполняющее следующие функции:

- изготовление сертификатов ключей подписей;
- создание (генерация) ключей электронных цифровых подписей по обращению клиентов с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;
- приостановка и возобновление действия сертификатов ключей подписей, а также их аннулирование;

Удостоверяющий центр

- ведение реестра сертификатов ключей подписей, обеспечение его актуальности и возможности свободного доступа к нему клиентов;
- проверка уникальности открытых ключей электронных цифровых подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдача сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществление по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;
- предоставление клиентам иных связанных с использованием электронных цифровых подписей услуги.

Удостоверяющий центр

Применение КЭП

- Электронная отчетность:

  В контролирующие органы и внебюджетные фонды, ФНС, ПФР, ФСС, Росстат.
- Электронные торги:

  На федеральных (при размещение госзаказа) и коммерческих электронных торговых площадках.
- Счета-фактуры:

  В электронном виде.
- Обмен документами:

  Заверенными электронной подписью, при взаимодействии организаций (договоры, акты).
- Арбитражный процесс:

  При банкротстве организаций и продаже имущества при помощи арбитражных управляющих.

Алгоритмы построения ЦЭП

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 ЭП 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 ЭП.

Использование хеш-функций

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хеш. Для вычисления хэша используются криптографические хеш-функции. Хеш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хеш-функция.

Использование хеш-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 ЭП. Поэтому формировать хэш документа и подписывать его получается намного быстрее, чем подписывать сам документ.

Использование хеш-функций

Использование хеш-функций даёт следующие преимущества:

- 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 ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Функция не является частью алгоритма ЭП, поэтому хеш-функция может использоваться любая или не использоваться вообще.

Симметричная схема

Симметричные схемы ЭП 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 ЭП 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. Симметричные схемы основаны на хорошо изученных блочных шифрах.

Симметричная схема

Симметричные схемы имеют следующие преимущества:

- Стойкость симметричных схем ЭП 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 ЭП 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.

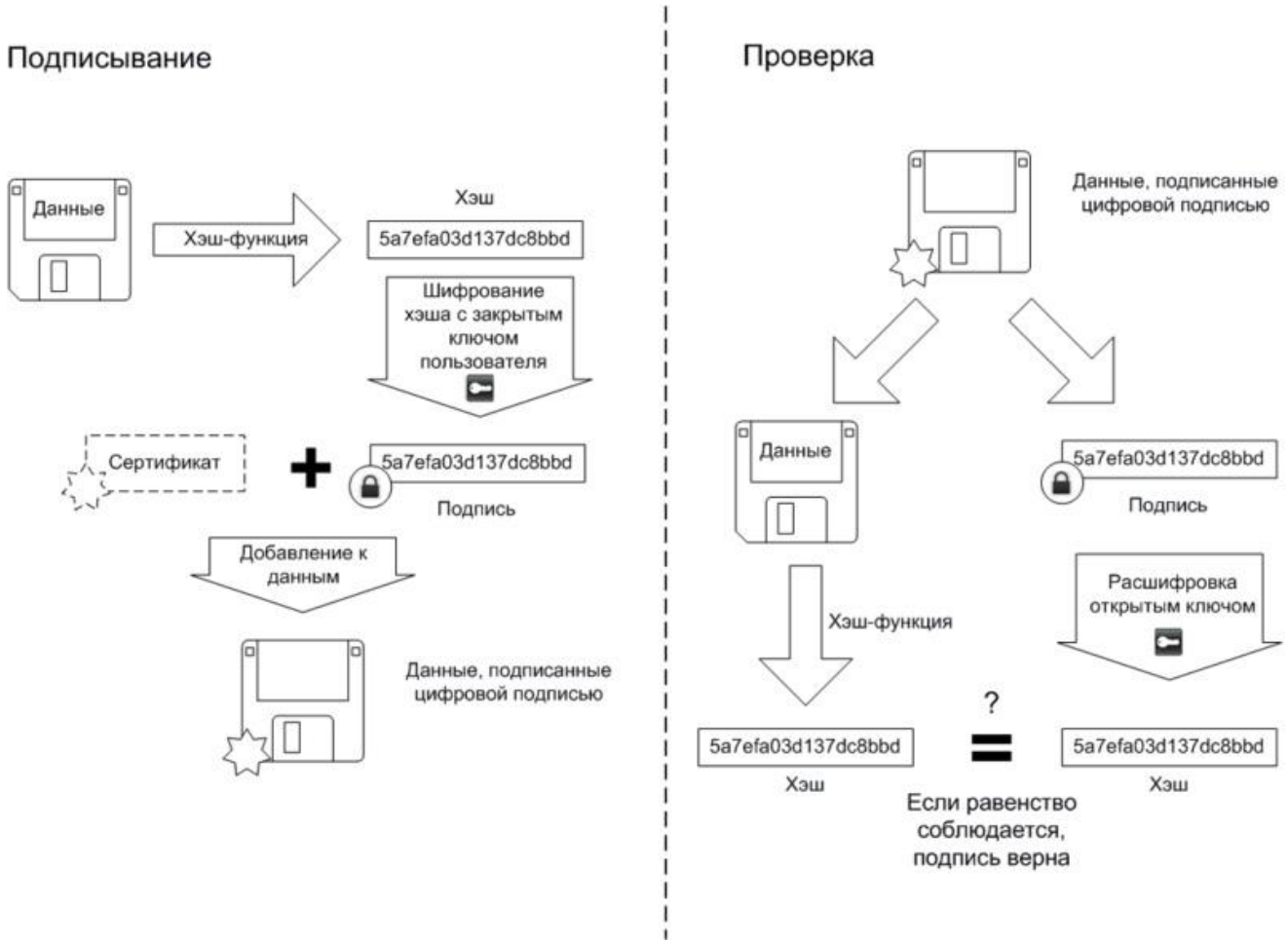
Асимметричная схема

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом. В отличие от симметричных 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.
- Формирование подписи.
- Проверка (верификация) подписи.

Алгоритмы подписи и проверки



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.

Подделка подписей

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.

Коллизия первого рода

Коллизия первого рода - подделка документа.

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.

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.

Коллизия второго рода

Коллизия второго рода - получение двух документов с одинаковой подписью.

В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим.

Управление ключами

Управление открытыми ключами

Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу.

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.

Управление ключами

Хранение закрытого ключа

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 настоящее время существуют следующие устройства хранения закрытого ключа:

Дискеты, смарт-карты, USB-брелоки, таблетки Touch-Memory.

Управление ключами

Хранение закрытого ключа

Смарт-карта и USB-брелоки

Управление ключами

Хранение закрытого ключа

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 соответствии с законом «Об электронной подписи», ответственность за хранение закрытого ключа владелец несет сам.

Использование ЭП

В России

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи».

Благодаря ЭП 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 ЭП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.

С 1 июля 2012 года Федеральный закон от 10 января 2002 г. № 1-ФЗ утратит силу, на смену ему придет Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Быстрая цифровая подпись

Быстрая цифровая подпись - вариант цифровой подписи, использующий алгоритм с гораздо меньшим (в десятки раз) числом вычислений модульной арифметики по сравнению с традиционными схемами ЭЦП. Схема быстрой электронной подписи, как и обычная, включает в себя алгоритм генерации ключевых пар пользователя, функцию вычисления подписи и функцию проверки подписи.

Применение быстрой ЭЦП

Быстрые алгоритмы цифровой подписи являются наиболее эффективными в тех случаях, когда преимущественно важна скорость получения ключа и небольшой размер подписи. Подобные требования имеют место в мобильных, сенсорных или персональных сетях (радиус которых ограничивается пределами одной комнаты) при передаче мультимедийного трафика. Использование цифровой подписи в мобильных телефонах стандарта GSM позволяет пользователям самостоятельно создавать PIN- код, а не получать его от оператора.

Реализация ускоренных алгоритмов создания ЭЦП для устройств с ограниченными ресурсами, таких как КПК, встроенные смарт-карты и мобильные телефоны, вычислительная мощность которых сильно уступает возможностям персональных компьютеров, позволит тратить меньше энергии на создание и хранение подписи и тем самым увеличит время работы устройства без подзарядки.