Содержание:

Электронная цифровая подпись

Для общего понимания что же такое электронная подпись, разберем его точное определение.

Электронная подпись (ЭП) — 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.

Где же применяется эта цифровая электронная подпись? И её назначение?

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

1. **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.
2. **Защиту от изменений (подделки) документа**: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
3. **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.
4. **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

Теперь рассмотрим немного истории возникновения эдектронной подписи.

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. См. Криптосистема Голдвассера-Микали.

На каких алгоритмах построена ЭП?

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.

Возможно ли подделать?

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

И конечно это такое же нарушение как и подделк обычной подписи.

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:

1. Документ представляет из себя осмысленный текст.
2. Текст документа оформлен по установленной форме.
3. 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:

1. Случайный набор байт должен подойти под сложно структурированный формат файла.
2. То, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме.
3. 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.