Электронная подпись (ЭП), **Электронная цифровая подпись** (ЭЦП), **Цифровая подпись** (ЦП) позволяет подтвердить авторство электронного документа. Это может быть и реальное лицо, или, например,

аккаунт в криптовалютной системе. Подпись связана как с автором, так и с самим документом с помощью криптографических методов, и не может быть подделана с помощью обычного копирования.

Электронная цифровая подпись (ЭЦП)- это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Основные принципы

Широко применяемая в настоящее время технология электронной подписи основана на асимметричном шифровании с открытым ключом и опирается на следующие принципы:

- Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. Механизм генерации ключей строго определён и является общеизвестным. При этом каждому открытому ключу соответствует определённый закрытый ключ. Если, например, Иван Иванов публикует свой открытый ключ, то можно быть уверенным, что соответствующий закрытый ключ есть только у него.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение закрытым ключом так, чтобы расшифровать его можно было только открытым ключом. Механизм шифрования является общеизвестным.
- Если электронный документ поддается расшифровке с помощью открытого ключа, то можно быть уверенным, что он был зашифрован с помощью уникального закрытого ключа. Если документ расшифрован с помощью

открытого ключа Ивана Иванова, то это подтверждает его авторство: зашифровать данный документ мог только Иванов, т.к. он является единственным обладателем закрытого ключа.

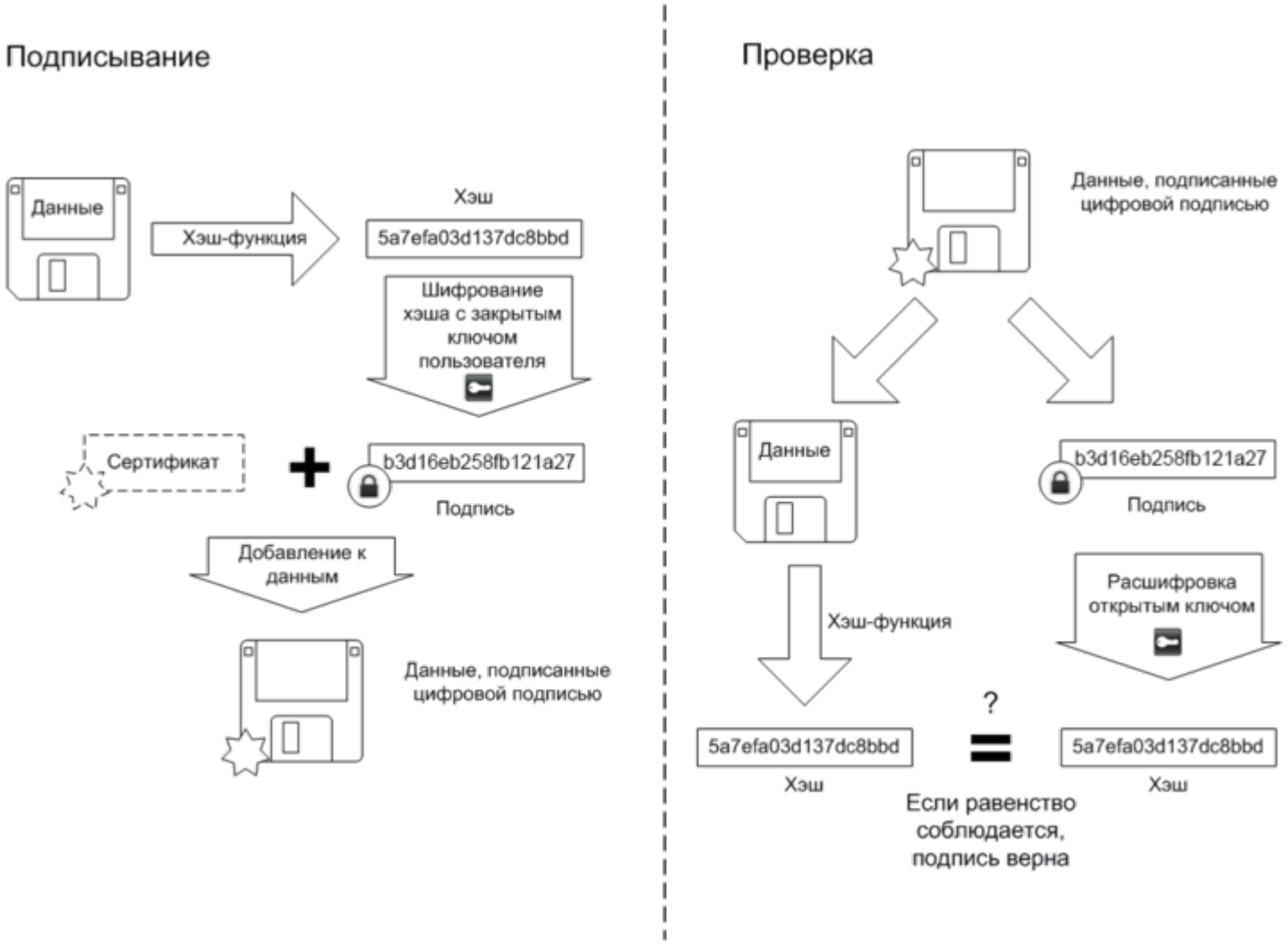
Однако шифровать весь документ было бы неудобно, поэтому шифруется только его хеш — небольшой объём данных, жёстко привязанный к документу с помощью математических преобразований и идентифицирующий его. Шифрованный хеш и является электронной подписью.

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.[4]
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Асимметричная схема



Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом.

Но в отличие от асимметричных алгоритмов шифрования, в которых шифрование производится с помощью открытого ключа, а расшифровка — с помощью закрытого (расшифровать может только знающий секрет адресат), в асимметричных схемах цифровой подписи подписание производится с применением закрытого ключа, а проверка подписи — с применением открытого (расшифровать и проверить подпись может любой адресат).

Общепризнанная схема цифровой подписи охватывает три процесса[источник не указан 1516 дней]:

- 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)

Подделка подписей

Анализ возможностей подделки подписей — задача криптоанализа. 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.

Использование ЭП

Общее назначение

Использование ЭП предполагается для осуществления следующих важных направлений в электронной экономике:

- Полный контроль целостности передаваемого электронного платежного документа: в случае любого случайного или преднамеренного изменения документа цифровая подпись станет недействительной, потому как вычисляется она по специальному алгоритму на основании исходного состояния документа и соответствует лишь ему.
- Эффективная защита от изменений (подделки) документа. ЭП даёт гарантию, что при осуществлении контроля целостности будут выявлены всякого рода подделки. Как следствие, подделывание документов становится нецелесообразным в большинстве случаев.
- Фиксирование невозможности отказа от авторства данного документа. Этот аспект вытекает из того, что вновь создать правильную электронную подпись можно лишь в случае обладания так называемым закрытым ключом, который, в свою очередь, должен быть известен только владельцу этого самого ключа (автору документа). В этом случае владелец не сможет сформировать отказ от своей подписи, а значит — от документа.
- Формирование доказательств подтверждения авторства документа: исходя из того, что создать корректную электронную подпись можно, как указывалось выше, лишь зная закрытый ключ, а он по определению должен быть известен только владельцу-автору документа, то владелец ключей может однозначно доказать своё авторство подписи под документом. Более того, в документе могут быть подписаны только отдельные поля документа, такие как «автор», «внесённые изменения», «метка времени» и т. д. То есть, может быть доказательно подтверждено авторство не на весь документ.

Перечисленные выше свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и

электронного документального и денежного обращения:

- Использование в банковских платежных системах;
- Электронная коммерция (торговля);
- Электронная регистрация сделок по объектам недвижимости;
- Таможенное декларирование товаров и услуг (таможенные декларации). Контролирующие функции исполнения государственного бюджета (если речь идет о стране) и исполнения сметных назначений и лимитов бюджетных обязательств (в данном случае если разговор идет об отрасли или о конкретном бюджетном учреждении). Управление государственными заказами;
- В электронных системах обращения граждан к органам власти, в том числе и по экономическим вопросам (в рамках таких проектов как «электронное правительство» и «электронный гражданин»);
- Формирование обязательной налоговой (фискальной), бюджетной, статистической и прочей отчетности перед государственными учреждениями и внебюджетными фондами;
- Организация юридически легитимного внутрикорпоративного, внутриотраслевого или национального электронного документооборота;
- Применение ЭЦП в различных расчетных и трейдинговых системах, а также Forex;
- Управление акционерным капиталом и долевым участием;
- ЭП является одним из ключевых компонентов сделок в криптовалютах.

Комментарии

- 1. ↑ Названия ключей открытый и закрытый — условные. Согласно алгоритму асимметричного шифровании с открытым ключом шифрующий ключ делается открытым, а дешифрующий — закрытым, чтобы обеспечить расшифровку сообщения именно получателем. В случае ЭЦП задача обратная: предоставить легкий путь дешифрации — проверки подписи, значит **дешифрующий ключ** должен быть **открытым**.
  2. ↑ И при условии, что получается осмысленный результат, а не случайный набор данных.