тема

Электронно- цифровая подпись

Подготовила

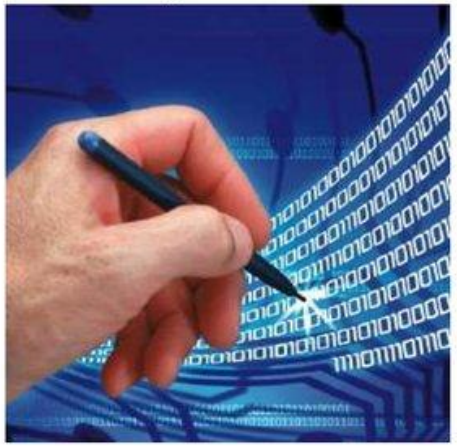
Россель Диана группа Ш-11


Подпись
ЭЦП

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*.



следующие типы хранилищ:

- - *файловая система* - при выборе данного пункта ключи и регистрационные свидетельства будут храниться на Вашем персональном компьютере в виде файлов;
- - *Kaztoken* - при выборе данного носителя ключи и регистрационные свидетельства будут храниться на внешнем защищённом носителе ключевой информации, защищённых при помощи пин-кода;
- - *E-Token* – при выборе данного пункта ключи и регистрационные свидетельства будут храниться на внешнем защищённом носителе ключевой информации, защищённые при помощи пин-кода. Преимуществом данного места хранения заключается невозможность копирования закрытых ключей, недостатком необходимость приобретать носитель.
- - *AKEY* – при выборе данного пункта ключи и регистрационные свидетельства будут храниться на внешнем защищённом носителе ключевой информации, защищённые при помощи пин-кода. Преимуществом данного места хранения заключается невозможность копирования закрытых ключей, недостатком необходимость приобретать носитель.
- - *JaCarta* – при выборе данного пункта ключи и регистрационные свидетельства будут храниться на внешнем защищённом носителе ключевой информации, защищённые при помощи пин-кода. Преимуществом данного места хранения заключается невозможность копирования закрытых ключей, недостатком - необходимость приобретать картридер для считывания.
- - *ЭЦП на sim-карте* - при выборе данного носителя ключи и регистрационные свидетельства будут храниться на sim-карте вашего телефона. Приобрести соответствующую sim-карту можно в отделах продаж операторов сотовой связи.
- - *удостоверения личности* - для записи ЭЦП на чип удостоверения личности (для физических лиц) необходимо обратиться в ближайший отдел НАО «Государственная корпорация «Правительство для граждан» (ЦОН), предъявив удостоверение личности. Для дальнейшей работы с ЭЦП, записанной на удостоверении личности необходимо приобрести картридер. Подробнее об этом вы можете узнать на этой странице.

Процедура подачи онлайн-заявки на выпуск ЭЦП состоит из четырех шагов:

- Шаг 1 - Изучение инструкции и установка ПО
- Шаг 2 - Подача онлайн-заявки
- Шаг 3 - Подтверждение онлайн-заявки в НАО ГК "Правительство для граждан"
- Шаг 4 - Установка регистрационных свидетельств НУЦ РК.

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[Прим. 1]. Механизм шифрования является общеизвестным.
- Если электронный документ поддается расшифровке с помощью открытого ключа[Прим. 2], 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.

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.[1]
- 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.[2]
- 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 (Криптосистема Гольдвассер — Микали).

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 хеша используются криптографические хеш-функции, что гарантирует выявление изменений документа при проверке подписи. 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 хеш документа 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 ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.
- Использование хеш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭП, поэтому хеш-функция может использоваться любая или не использоваться вообще.
- В большинстве ранних систем ЭП использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы для атак с использованием открытого ключа (см. ниже), так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст.[5] 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 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.[1] Асимметричные схемы цифровой подписи опираются на вычислительно сложные задачи, сложность которых ещё 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.[4] Симметричные схемы основаны на хорошо изученных блочных шифрах.
- В связи с этим 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.
- 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 объёма вычислений. Для преодоления проблемы «одноразовости» ключей используется генерация отдельных ключей из главного ключа

Перечень алгоритмов ЭП

- 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 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012 (основан на сложности вычисления дискретного логарифма в группе точек эллиптической кривой)
- Евразийский союз: ГОСТ 34.310-2004[8] полностью идентичен российскому стандарту ГОСТ Р 34.10-2001
- Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
- Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 (в настоящее время не действует), СТБ 34.101.45-2013
- Схема Шнорра
- Pointcheval-Stern signature algorithm
- Вероятностная схема подписи Рабина
- Схема BLS (Boneh-Lynn-Shacham)
- Схема DLR (Donna-Lynn-Rivest)
- Схема GMR (Goldwasser-Micali-Rivest)

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.

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 txt-файла, чаще всего в формате DOC или HTML.
- Если у фальшивого набора байт и произойдет коллизия с хешем исходного документа, то должны выполниться три 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 соответствующим 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. Некоторые форматы подписи даже защищают целостность текста, но не служебных полей.[9]
- 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.

Социальные атаки

- Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами[11].
- 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

СПАСИБО ЗА ВНИМАНИЕ!