Содержание:

Введение

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 позволяющей идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе. Электронная цифровая

подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;

- подтверждение подлинности электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

При этом электронной документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

В скором будущем заключение договора будет возможно в электронной форме, который будет иметь такую же юридическую силу, как и письменный документ. Для этого он должен иметь механизм электронной цифровой подписи, подтверждаемый сертификатом. Владелец сертификата ключа подписи владеет закрытым ключом электронной цифровой подписи, что позволяет ему с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы). Для того, чтобы электронный документ могли открыть и другие пользователи, разработана система открытого ключа электронной подписи.

Для того, чтобы иметь возможность скреплять электронный документ механизмом электронной цифровой подписи, необходимо обратиться в удостоверяющий центр за получением сертификата ключа подписи. Сертификат ключа подписи должен

быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи. Удостоверяющий центр по закону должен подтверждать подлинность открытого ключа электронной цифровой подписи.

Основные положения

Общая суть электронной подписи заключается в том, что с помощью криптографической хэш-функции вычисляется относительно короткая строка символов фиксированной длины (хэш).

Затем этот хэш шифруется закрытым ключом владельца, а результатом является подпись документа. Подпись прикладывается к документу, таким образом получается подписанный документ.

Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным.

При ведении деловой переписки, при заключении контрактов подпись ответственного лица является непременным атрибутом документа, преследующим несколько целей:

- гарантирование истинности письма путем сличения подписи с имеющимся образцом;

- гарантирование авторства документа (с юридической точки зрения).

Выполнение данных требований основывается на следующих свойствах подписи:

- с помощью подписи получателю документа можно доказать, что она принадлежит подписывающему;

- подпись неподделываема; то есть служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто иной;

- подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно;

- документ с подписью является неизменяемым;

- подпись неоспорима;

- любое лицо, владеющее образцом подписи может удостоверится, что документ подписан владельцем подписи.

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа.

Таким средством является электронно-цифровая подпись (ЭЦП), которая сохранила основные свойства обычной подписи.

Существует несколько методов построения ЭЦП, а именно:

- шифрование электронного документа (ЭД) на основе симметричных алгоритмов.

Данная схема предусматривает наличие в системе третьего лица-арбитра, пользующегося доверием обеих сторон. Авторизацией документа в данной схеме является сам факт шифрования ЭД секретным ключом и передачи его арбитру;

- использование ассиметричных алгоритмов шифрования. Фактом подписания документа является шифрование его на секретном ключе отправителя;

- развитием предыдущей идеи стала наиболее распространенная схема ЭЦП - шифрование окончательного результата обработки ЭД хеш-функцией при помощи ассиметричного алгоритма.

Появление этих разновидностей обусловлено разнообразием задач, решаемых с помощью электронных технологий передачи и обработки электронных документов.

При генерации ЭЦП используются параметры трех групп:

- общие параметры;

- секретный ключ;

- открытый ключ.

Атаки на электронную цифровую подпись

Стойкость большинства схем ЭЦП зависит от стойкости ассиметричных алгоритмов шифрования и хэш-функций.

Существует следующая классификация атак на схемы ЭЦП:

1. Атака с известным открытым ключом:

Атака с известными подписанными сообщениями - противник, кроме открытого ключа имеет и набор подписанных сообщений.

Простая атака с выбором подписанных сообщений - противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения;

2. Направленная атака с выбором сообщения;

3. Адаптивная атака с выбором сообщения.

Каждая атака преследует определенную цель, которые можно разделить на несколько классов:

1. Полное раскрытие. Противник находит секретный ключ пользователя.

2. Универсальная подделка. Противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП.

3. Селективная подделка. Подделка подписи под выбранным сообщением.

4. Экзистенциальная подделка. Подделка подписи хотя бы для одного случайно выбранного сообщения.

На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя:

- Отказ одного из участников авторства документа;

- Модификация принятого электронного документа;

- Подделка документа;

- Навязывание сообщений в процессе передачи - противник перехватывает обмен сообщениями и модифицирует их.

Так же существуют нарушения, от которых невозможно оградить систему обмена сообщениями - это повтор передачи сообщения и фальсификация времени отправления сообщения. Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений.

Средства работы с электронной цифровой подписью

PGP. Наиболее известный - это пакет PGP (Pretty Good Privacy) - (www.pgpi.org), без сомнений являющийся на сегодня самым распространенным программным продуктом, позволяющим использовать современные надежные криптографические алгоритмы для защиты информации в персональных компьютерах.

К основным преимуществам данного пакета, выделяющим его среди других аналогичных продуктов следует отнести следующие:

Открытость. Исходный код всех версий программ PGP доступен в открытом виде. Любой эксперт может убедиться в том, что в программе эффективно реализованы криптоалгоритмы. Так как сам способ реализации известных алгоритмов был доступен специалистам, то открытость повлекла за собой и другое преимущество - эффективность программного кода.

Стойкость. Для реализации основных функций использованы лучшие (по крайней мере на начало 90-х) из известных алгоритмов, при этом допуская использование достаточно большой длины ключа для надежной защиты данных

Бесплатность. Готовые базовые продукты PGP (равно как и исходные тексты программ) доступны в Интернете в частности на официальном сайте PGP Inc. (www.pgpi.org).

Поддержка как централизованной (через серверы ключей) так и децентрализованной (через «сеть доверия») модели распределения открытых ключей.

Удобство программного интерфейса. PGP изначально создавалась как продукт для широкого круга пользователей, поэтому освоение основных приемов работы отнимает всего несколько часов.

GNU Privacy Guard (GnuPG)

GnuPG (www.gnupg.org) - полная и свободно распространяемая замена для пакета PGP. Этот пакет не использует патентованный алгоритм IDEA, и поэтому может быть использован без каких-нибудь ограничений. GnuPG соответсвует стандарту RFC2440 (OpenPGP).

Криптон

Пакет программ Криптон (www.ancud.ru) предназначен для использования электронной цифровой подписи (ЭЦП) электронных документов.

В стандартной поставке для хранения файлов открытых ключей используются дискеты. Помимо дискет, пакет Криптон дает возможность использования всех типов ключевых носителей (смарт-карт, электронных таблеток Touch Memory и др.).

Заключение

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 2013 г. N 63-ФЗ "Об электронной подписи" и определяет ЭП так:

- "электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию".

После становления ЭП 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 ЭП, особенности её использования в сферах государственного управления и в корпоративной информационной системе.

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.

Список использованной литературы

1. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года №1-ФЗ .
2. Электронная подпись и шифрование // МО ПНИЭИ .
3. Современные криптографические методы защиты информации - системы с открытым ключом .
4. «Юридическая сила электронных документов» О. Беззубцев 5.« Некоторые вопросы правового обеспечения использования ЭЦП» Беззубцев О.А., Мартынов В.Н., Мартынов В.М.
5. 6.«Информатика для юристов и экономистов» Под ред. С.В. Симоновича. СПб.: Питер, 2002.
6. 7.«Электронный документ» А. Марченко.

7. 8.«Законодательное регулирование правового статуса ЭЦП. Основные положения» Ткачев А.В
8. 9.«Юридический справочник руководителя»2008 г.