Содержание:

1.

Введение

В наше время мало кто разбирается что такое электронная цифровая подпись. Данная технология ЭЦП дает организациям юридически значимый электронный документооборот.

Электронная цифровая подпись (ЭЦП) – это реквизит электронного документооборота. ЭЦП предназначена для защиты электронного контента от подделки. По своей сути ЭЦП относительно равна обычной подписи на бумажном документе при соблюдении нескольких условий:

- сертификат ключа (ЭЦП) не утратил свою актуальность (то есть срок действия не закончился) на момент подписания электронного документа;
- подтверждена подлинность ЭЦП в электронном документе;
- ЭЦП используется только по требованиям, которые указаны в сертификате;

Возможно, в скором будущем подписание договоров или каких-либо других документов будет иметь такую же юридическую силу, как и обычный письменный вариант документа. Для такого документа будет обязателен подтверждающий сертификат ЭЦП.

Для того чтобы производить электронный документооборот с ЭЦП нужно обратиться в удостоверяющую организацию, за получением сертификата ЭЦП. Такая организация должна внести данный сертификат в реестр сертификатов ключей и подписей не позднее даты активации сертификата, в противном случае сертификат будет не действителен. Первая такая удостоверяющая организация в России была запущена в 2002 году Российским НИИ развития общих сетей (РосНИИРОС).

1.

Основные положения

Хэш-функция защищаемого электронного документа (контента) представляется как уникальное число, изменение хоть одного знака такого числа, привод к искажению половины знаков хэш-функции. Формирование ЭЦП в электронном документе (контенте) тоже предусматривает уникальный номер хэш-функции, который шифрует значения посредствам секретного электронного ключа отправителя.

Следовательно, ЭЦП защищает содержание документа и секретный ключ и делает невозможным редактирование электронного документа без нарушения данной ЭЦП.

Функции электронной цифровой подписи (ЭЦП):

- Подтверждение, что подписывающее лицо самостоятельно и сознательно подписало электронный документ (контент).
- Защита от неактуальности. Подписывающее лицо не может отказаться после подписания от факта подписи электронного документа по средствам ЭЦП.
- ЭЦП зависит от документа и отметок времени имеющихся в нем.
- Подтверждение, того, что документ подписало именно подписывающее лицо.

Общая концепция ЭЦП складывается в следующем: что с помощью криптографической хэш-функции вычисляется уникальная строка символов. Далее этот хэш шифруется ключом владельца. Подпись прикладывается к электронному документу (контенту), в результате чего появляется подписанный электронный документ. Для желающих лиц установить подлинность документа, используют расшифровку подписи открытым ключом владельца и также определяется хэш этого же электронного документа. Электронный документ (контент) является подлинным, если хэш совпадает с расшифровкой из подписи.

Методы построения электронной цифровой подписи:

- схема ЭЦП заключается в том, что хэш-функцией при помощи ассиметричного алгоритма производиться шифрование окончательного результат обработки электронного документа.

- актуальным подтверждением подписания электронных документов является шифрование его с помощью секретного ключа отправителе и записи документа на него.
- Авторизацией электронного документа является факт шифрования его секретным ключом отправителя и передача его арбитру.

При генерации ЭЦП используются три группы параметров:

- Общие параметры
- Секретный ключ
- Открытый ключ

1.

Атаки на ЭЦП

Стойкость к атакам большинства схем электронных цифровых подписей во многом зависят от ассиметричных алгоритмов шифрования и хэш-функций.

Классификация атак на ЭЦП:

- Атака известным открытым ключом
- Атака с выбором сообщения
- Адаптивная атака с выбором сообщения
- Полное вскрытие – хакер (противник) смог найти секретный ключ пользователя
- Подделка подписи под выбранным сообщением (селективная подделка)
- Подделка подписи для одного из выбранных сообщений (экзистенциальная подделка)

На практике применение электронной цифровой подписи помогает выяснить множество нарушений таких, как подделка электронного документа отказ одного из участника от авторства электронного документа, модификация и редактирование уже принятого электронного документа.

1.

Средства работы с ЭЦП

Самый известный способ – это пакет PGP (Pretty Good Privacy), позволяющий использовать лучшие криптографические алгоритмы для защиты данных на персональных компьютерах пользователей. Про пакет PGP:

Открытость. Исходный код PGP открыт для редактирования, он не заблокирован. Любой программист может самостоятельно убедиться в том, что алгоритмы работаю эффективно.

Стойкость. Для реализации программы используются только актуальные и надежные алгоритмы. Используется достаточно большой уникальный код для большей защиты.

Бесплатность. Программное обеспечение PGP доступно на официальном сайте совершенно бесплатно PGP Ink.

Удобство программного интерфейса. Интерфейс программы создавался для использования большого количества пользователей. Следовательно, для этого был создан достаточно большой и понятный интерфейс.

Еще один пакет программного обеспечения ЭЦП – это Криптон. Криптон тоже предназначен для использования электронной цифровой подписи в электронном документообороте. Для хранения секретных ключей программа использует все типы носителей, существующие на данный момент.

1.

Заключение

В скором будущем, когда все компании перейдут полностью на электронный документооборот без электронной цифровой подписи обойтись, будет невозможно. Несколько аспектов, а именно плюсов ЭЦП:

- Удостоверение источника электронного документа
- Защита от изменений и модерации электронного документа
- Невозможность отказа от авторских прав

1.

Источники

2. Электронная подпись — Википедия (wikipedia.org)

3. Электронно-цифровая подпись (ЭЦП): виды подписей и область их применения (audit-it.ru)
4. Что такое электронная подпись: как получить и для чего нужна - Сбербанк (sberbank.ru)
5. Электронная подпись (ЭЦП): что это такое, для чего нужна и как ее получить физическим и юридическим лицам (timeweb.com)
6. Что такое электронная цифровая подпись (ЭЦП) | Инфотекс Траст (iitrust.ru)
7. Электронная цифровая подпись (allbest.ru)
8. Реферат: Электронно-цифровая подпись как средство защиты электронного документа - BestReferat.ru
9. Электронная подпись: зачем она нужна, как получить ЭП физическому и юридическому лицам, ИП (tinkoff.ru)