Содержание:

Введение

Одной из проблем в наше время является проблема информационной безопасности. Это можно объясняется тем, что информационные технологии коренным образом изменили нашу жизнь. Уже сейчас факты свидетельствуют: большая часть оборота информации и документов теперь осуществляется в электронном виде. Технология же электронной подписи способна еще более расширить возможности электронного документооборота, обезопасить его, распространить его на все сферы общественной жизни, способствовать развитию доступных для всех возможностей электронного бизнеса. В странах, где законодательно закреплено понятие электронной подписи, не выходя из дома или офиса, возможно безопасно и гарантированно совершать любые сделки; отстаивать свои права в органах правопорядка, ведя переписку по электронной почте; декларировать свои доходы в налоговых органах.

Понятие ЭЦП

Электронная цифровая подпись – это реквизит электронного документа, позволяющий установить отсутствие каких-то
недочетов в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается
в результате криптографического преобразования информации с использованием закрыт

Виды электронной цифровой подписи.

Существует 3 вида ЭЦП:

1. Присоединенная ЭЦП. В случае создании присоединенной новой подписи создается новый файл ЭЦП, в который помещаются данные о том, кто его подписал. Достоинства присоединенной подписи: простота использования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле, который можно копировать, пересылать и т.п. Недостаток: без использования средств СКЗИ (средства криптографической защиты информации) уже нельзя прочесть и использовать содержимое файла.
2. Отсоединенная ЭЦП. При создании отсоединенной подписи сам подписываемый файл никак не изменяется, а создается отдельно от подписываемого файла. Достоинство: подписанный файл можно читать, не использую СКЗИ. Недостаток отсоединенной подписи: необходимость хранения в виде нескольких файлов.
3. ЭЦП внутри данных (Наиболее распространена). Применение ЭЦП этого вида очень зависит от приложения, которое его использует. Недостаток: вне приложения, создавшего ЭЦП, без понимания структуры его данных проверить ненастоящие фрагменты данных , подписанных ЭЦП затруднительно.

Предназначение и преимущества ЭЦП

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

1)Контроль целостности документа: при любом попытки изменить или даже случайном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного документа и соответствует лишь оригиналу (точнее ему же).

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

3) Отказ от авторства невозможна. 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. (Из 3 пункта о отказ от авторства невозможна) То владелец пары ключей может доказать своё авторство подписи под документом. Конечно, зависит от определения документа, могут быть подписаны такие поля, как «автор», «внесённые изменения» и т. д.

5) Ускоряет оформление сделки и обмен документацией;

6) Совершенствование и уменьшение стоимости процедуры подготовки, доставки, учета и хранения документов;

7)Создание корпоративной системы обмена документами;

8)Наиболее выгодного выбор ценового предложения товаров и услуг на электронных торгах и т.п.

9) Взаимоотношения с населением, организациями и властными структурами на современной основе, более эффективно, с наименьшими издержками;

10) Улучшение географии бизнеса, совершая в удаленном режиме экономические операции с деловыми партнерами из любых регионов .

Принцип работы электронной цифровой подписи

1. Каждому пользователю, который участвует в обмене электронными документами, создается особый секретный и открытый криптографические ключи. Секретный (закрытый) ключ является элементом, с помощью которого производится шифрование документов и формируется электронно-цифровая подпись. Так же этот ключ является собственностью пользователя, и держится в секрете от других пользователей. Открытый ключ используется для проверки ЭЦП получаемых документов-файлов. Владелец должен обеспечить наличие своего открытого ключа у всехс кем он со Кроме того, дубликат открытого ключа направляется в Удостоверяющий Центр, где создана библиотека открытых ключей ЭЦП. В библиотеке Центра обеспечивается регистрация и надежное хранение открытых ключей.
2. Пользователь генерирует для документа электронную цифровую подпись. При этом на основе секретного ключа ЭЦП и содержимого документа путем криптографического преобразования вырабатывается некоторая символьная последовательность, которая и является электронно-цифровой подписью данного пользователя для конкретного документа. Эта символьная последовательность сохраняется в отдельном файле. В подпись записывается: дата формирования подписи; информация о лице, сформировавшем подпись; имя файла открытого ключа подписи.
3. Пользователь, получивший подписанный документ и имеющий открытый ключ

ЭЦП отправителя на основании текста документа и открытого ключа отправителя выполняет обратное криптографическое преобразование, обеспечивающее проверку электронной цифровой подписи отправителя. Если ЭЦП под документом верна, то это значит, что документ действительно подписан отправителем и в текст документа не внесено никаких изменений.

Заключение

Из всего выше озвученного можно сделать вывод, что электронная цифровая подпись – это эффективное решение для всех, кто не хочет ждать прихода курьерской почты за многие сотни километров, чтобы проверить подлинность полученной информации или подтвердить заключение сделки. Документы могут быть подписаны цифровой подписью и переданы к месту назначения в течение нескольких секунд. Все участники электронного обмена документами получают равные возможности независимо от их удаленности друг от друга. Подделать ЭЦП невозможно - это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи. С использованием ЭЦП работа по схеме "разработка проекта в электронном виде и т.д. уходит в прошлое. А значит использование электронной цифровой подписи полезно, удобно и безопасно.

Список используемой литературы

http://www.documoborot.ru

http://www.digitalsign.ru

http://iecp.ru/

http://www.ekey.ru/

http://www.garant.ru/