Одной из актуальных проблем в настоящее время в мире является проблема информационной безопасности

Это 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 электронной цифровой подписи

Электронная цифровая подпись (далее - ЭЦП) -- реквизит электронного документа, позволяющий установить отсутствие искажения информации 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 закрытого ключа ЭЦП.

Виды электронной цифровой подписи

Существует 3 вида ЭЦП:

1. Присоединенная электронная цифровая подпись. В случае создания присоединенной подписи создается новый файл ЭЦП, в который помещаются данные подписываемого файла.

Достоинства присоединенной подписи: простота дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле, файл можно копировать, пересылать и т.п.

Недостаток: без использования средств СКЗИ (средства криптографической защиты информации) уже нельзя прочесть и использовать содержимое файла.

2. Отсоединенная электронная цифровая подпись. При создании отсоединенной подписи файл подписи создается отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется.

Достоинство: подписанный файл можно читать, не прибегая к СКЗИ.

Недостаток отсоединенной подписи: необходимость хранения подписанной информации в виде нескольких файлов.

3. Электронная цифровая подпись внутри данных (Наиболее распространена). Применение ЭЦП этого вида существенно зависит от приложения, которое их использует.

Недостаток: вне приложения, создавшего ЭЦП, без знания структуры его данных проверить подлинность частей данных, подписанных ЭЦП затруднительно.

Предназначение и преимущества электронной цифровой подписи

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

- контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему.

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

- невозможность отказа от авторства. 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.

- доказательное подтверждение авторства документа. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец пары ключей может доказать своё авторство подписи под

документом. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

- значительное сокращение времени, затрачиваемое на оформление сделки и обмен документацией;

- совершенствование и уменьшение стоимости процедуры подготовки, доставки, учета и хранения документов;

- строительство корпоративной системы обмена документами;

- выбор наиболее выгодного ценового предложения товаров и услуг на электронных торгах, аукционах и тендерах;

- взаимоотношения с населением, организациями и властными структурами на современной основе, более эффективно, с наименьшими издержками;

- расширение географии бизнеса, совершая в удаленном режиме экономические операции с партнерами из любых регионов России.

Принцип работы электронной цифровой подписи

1. Каждому пользователю, участвующему в обмене электронными документами, генерируются уникальные секретный и открытый криптографические ключи. Секретный (закрытый) ключ является элементом, с помощью которого производится шифрование документов и формируется электронно-цифровая подпись. Секретный 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 всех, с кем он собирается обмениваться подписанными документами. Кроме того, дубликат открытого ключа направляется в Удостоверяющий Центр, где создана библиотека открытых ключей ЭЦП. В библиотеке Центра обеспечивается регистрация и надежное хранение открытых.

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 вышеизложенного можно сделать вывод, что электронная цифровая подпись - 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 - создание бумажной копии для подписи - пересылка бумажной копии с подписью - рассмотрение бумажной копии - перенос ее в электронном виде на компьютер" уходит в прошлое. А значит использование электронной цифровой подписи полезно, удобно и безопасно.

Список используемых источников

http://www.mtron.ru

http://www.ucnbs.ru/about/

http://www.documoborot.ru

http://www.digitalsign.ru

http://iecp.ru/

http://www.ekey.ru/

http://www.garant.ru/