При переходе на электронный документооборот встает вопрос авторства документа, достоверности и защиты от искажений.

Наиболее удобным средством защиты электронных документов от искажений, позволяющим при этом однозначно идентифицировать отправителя, сообщения, является электронная цифровая подпись (ЭЦП).

Банк России и другие банки Российской Федерации эффективно используют ЭЦП для осуществления своих операций путем пересылки банковских электронных документов по корпоративным и общедоступным телекоммуникационным сетям.

10 января 2002 года был принят Федеральный Закон «Об электронной цифровой подписи», вступивший в силу с 22 января текущего года, который закладывает основы решения проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными документами, при соблюдении которых электронная цифровая подпись признается юридически равнозначной собственноручной подписи человека в документе на бумажном носителе.

Федеральный Закон «Об электронной цифровой подписи» определяет условия использования ЭЦП в электронных документах органами государственной власти и государственными организациями, а также юридическими и физическими лицами, при соблюдении которых:

- средства создания подписи признаются надежными;

- сама ЭЦП признается достоверной, а ее подделка или фальсификация подписанных данных могут быть точно установлены;
- предоставляются юридические гарантии безопасности передачи информации по открытым телекоммуникационным каналам;

- соблюдаются правовые нормы, содержащие требования к письменной форме документа;
- сохраняются все традиционные процессуальные функции подписи, в том числе удостоверение полномочий подписавшей стороны, установление подписавшего лица и содержания сообщения, а также роль подписи в качестве судебного доказательства;

-обеспечивается охрана персональной информации.

В Законе устанавливаются права и обязанности обладателя электронной цифровой подписи. В соответствии с законом владельцем сертификата ключа подписи (обладателем электронной цифровой подписи) является физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись электронных документах (подписывать электронные документы).

Владелец сертификата ключа подписи обязан:

- Хранить в тайне закрытый ключ электронной цифровой подписи;

- Не использовать для электронной цифровой подписи открытые и закрытые ключи электронной цифровой подписи, если ему известно, что эти ключи используются или использовались ранее;

- Немедленно требовать приостановления действия сертификата ключа подписи при наличии оснований полагать, что тайна закрытого ключа электронной цифровой подписи нарушена.

Согласно ст. 6 данного Закона сертификат ключа подписи должен содержать следующие сведения:

Уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;

Фамилия, имя, отчество владельца сертификата ключа подписи или псевдоним владельца; Открытый ключ электронной цифровой подписи;

Наименование и место нахождения удостоверяющего центра, выдавшего сертификат ключа подписи;

Сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.
Таким образом электронный документ (любой документ, хранящийся на компьютере, будь то письмо, финансовый документ, чертеж, изображение, контракт и т.д.) подписанный ЭЦП при соблюдении условий, обговоренных в законе, может быть использован в финансовых отношениях и в судебном

разбирательстве, что значительно расширяет область применения электронных документов.

Использование ЭЦП позволит: значительно сократить время, затрачиваемое на оформление сделки и обмен документацией; усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов; гарантировать достоверность документации; минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена; построить корпоративную систему обмена документами.

Электронная цифровая подпись функционирует на основе криптоалгоритмов с асимметричными (открытыми) ключами и инфраструктуры открытых ключей. Проблема традиционных алгоритмов шифрования с симметричными ключами заключается в том, что шифрование и дешифрование происходит при помощи одного и того же ключа. В связи с этим возникает вопрос об обмене ключами. Для того чтобы произвести защищенный обмен информацией, пользователям необходимо обменятся ключами, при чем использовать для этого обмена альтернативные средства передачи информации, поскольку при обмене нешифрованной информацией по электронной почте высока вероятность дискредитации ключа. Идеальным, с точки зрения безопасности, вариантом представляется личный обмен ключевыми носителями, однако он является наиболее ресурсоемким. В криптосистемах на основе асимметричных ключей для шифрования и дешифрования используется пара ключей – секретный и публичный ключи, уникальные для каждого пользователя, и цифровой сертификат. Цифровой сертификат представляет собой расширение открытого ключа, включающего не только сам ключ, но и дополнительную информацию, описывающую принадлежность ключа, время использования, доступные криптосистемы, название удостоверяющего центра и т.д.

Для реализации подобного взаимодействия используются специальные структуры, удостоверяющие центры. Их основная функция – распространение публичных и секретных ключей пользователей, а также верификация сертификатов. Удостоверяющие центры могут объединяться в цепочки. Вышестоящий (корневой) удостоверяющий центр может выдать сертификат и права на выдачу ключей нижестоящему центру. Тот, в свою очередь, может выдать права еще другому нижестоящему центру и так далее, при чем, сертификат, выданный одним из центров, может быть верифицирован любым из серверов в цепочке. Таким образом существует возможность установить центр распространения секретных ключей в непосредственной близости от пользователя,

что решает проблему дискредитации ключа при передаче по сетям связи.

В случае с ЭЦП процесс обмена сообщением выглядит следующим образом:

- отправитель получает у удостоверяющего центра секретный ключ;
- используя этот ключ, формирует электронную цифровую подпись и отправляет письмо;

- получатель при помощи публичного (общедоступного) ключа и цифрового сертификата, полученного у удостоверяющего центра, устанавливает авторство документа и отсутствие искажений.

Как видно из схемы обмена, на удостоверяющих центрах лежит огромная ответственность, поскольку именно они отвечают за надежность функционирования всей инфраструктуры открытых ключей.

Цифровая подпись обеспечивает:

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

- Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной.

- Невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

- Предприятиям и коммерческим организациям сдачу финансовой отчетности в государственные учреждения в электронном виде;
- Организацию юридически значимого электронного документооборота.

Возможные атаки на ЭЦП таковы:

- Подделка подписи. Получение фальшивой подписи, не имея секретного ключа — задача практически нерешаемая даже для очень слабых шифров и хэшей.
- 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 Plain Text — файла, чаще всего в формате

DOC или HTML. Если у фальшивого набора байт и произойдет коллизия с хешем исходного документа, то должны выполниться 3 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 соответствующий 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.

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.

Получение двух документов с одинаковой подписью (коллизия второго рода)

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хеширования MD5.

- Социальные атаки. Социальные атаки направлены на «слабое звено» криптосистемы — человека. 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.

Электронная цифровая подпись является наиболее перспективным и широко используемым в мире способом защиты электронных документов от подделки и обеспечивает высокую достоверность сообщения. Законы Российской Федерации дают возможность использования систем ЭЦП для обмена финансовыми и другими критическими для делопроизводства документами. Существует возможность использования в системах ЭЦП сертифицированных ФАПСИ средств, что дает возможность обмена документами, подписанными ЭЦП с органами государственной власти. Основной проблемой широкого использования ЭЦП является отсутствие официальных государственных удостоверяющих центров или

признанных де-факто2 коммерческих, реализующих инфраструктуру открытых ключей на основе отечественных алгоритмов. Для организации корпоративной системы ЭЦП они не требуются, но если в будущем вы планируете выйти на публичный уровень, сертификат корневого удостоверяющего центра вашей компании должен быть выдан публичным удостоверяющим центром.

Электронная цифровая подпись - эффективное решение для всех, кто не хочет ждать прихода фельдъегерской или 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.

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.