Электронно-цифровая подпись и шифрование

Понятие электронной подписи

- **Электро́нная по́дпись (ЭП)** — информация в электронной форме, присоединенная к другой информации в электронной форме (электронный документ) или иным образом связанная с такой информацией. Используется для определения лица, подписавшего информацию (электронный документ).

- Электронно-цифровая подпись (ЭЦП) используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

- ЭЦП - это программно-криптографическое средство, которое обеспечивает:
  - проверку целостности документов;
  - конфиденциальность документов;
  - установление лица, отправившего документ

Виды электронных подписей в РФ

Федеральный закон РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» устанавливает следующие виды ЭП:

- Простая электронная подпись (ПЭП);
- Усиленная неквалифицированная электронная подпись (НЭП);
- Усиленная квалифицированная электронная подпись (КЭП).

Для чего используется электронно-цифровая подпись?

- Целью применения систем цифровой подписи является **аутентификация информации** - защита участников информационного обмена от навязывания ложной информации, установление факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений.

В чем преимущество электронной цифровой подписи?

Используя цифровую подпись, Вы можете:

- выбрать наиболее выгодное ценовое предложение товаров и услуг на электронных торгах, аукционах и тендерах;
- выстраивать взаимоотношения с населением, организациями и властными структурами на современной основе, более эффективно, с наименьшими издержками;
- расширить географию своего бизнеса, совершая в удаленном режиме экономические операции с партнерами из любых регионов России.
- внедрение электронной цифровой подписи позволяет не только значительно снизить затраты на подготовку сделок за счет проведения операций в интерактивном режиме, но и своевременно получать наиболее полную информацию, чтобы обезопасить себя от недобросовестных деловых партнеров.
- 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.

Кто может получить электронную цифровую подпись?

- Получить электронную цифровую подпись могут как физические, так и сотрудники организаций. Например:

— физические лица (граждане);
— предприятия различных организационно-правовых форм и форм собственности;
— Федеральные органы государственной власти;
— органы власти субъектов РФ;
— Муниципальные образования.

- Электронная подпись может открыть путь к более эффективному взаимодействию с властями, предприятиями и организациями всех уровней.

Каков механизм действия электронной цифровой подписи?

- Механизм действия ЭЦП прост и очень эффективен.
- По сути, электронная подпись представляет собой определенную последовательность символов, полученную за счет преобразования исходного документа специальным программным обеспечением ЭЦП.
- При пересылке происходит добавление цифровой подписи к исходному документу, в результате чего авторство и неизменность информации, содержащейся в документе, получают свое подтверждение. При внесении любых изменений в исходный документ электронная подпись сразу становится недействительной.

- Таким образом, получение ЭЦП (электронной цифровой подписи) позволяет быть уверенным в авторстве и содержании документов, которыми Вы обмениваетесь через интернет. Подделать электронную подпись невозможно. Для того чтобы подобрать подпись, потребовался бы колоссальный объем вычислений.

Алгоритм цифровой подписи

- С помощью цифровой подписи информация не шифруется и остается доступной любому пользователю, который имеет к ней доступ.
- Процесс подписания документа выглядит следующим образом.

- Шаг 1. Строится специальная функция, которая напоминает контрольную сумму — хэш-функция, она идентифицирует содержание документа.

- Шаг 2. Автор документа шифрует содержание хэш-функции своим персональным закрытым ключом. Зашифрованная хэш-функция помещается в то же сообщение, что и сам документ. Полученное таким образом сообщение может сохраняться на любом носителе или пересылаться по электронной почте. Хэш-функция имеет небольшой размер и увеличивает размер сообщения незначительно.

Что такое «сертификат ключа»? Для чего он предназначен?

- Сертификат представляет собой электронный документ, который связывает данные для проверки электронных подписей с определенным лицом, подтверждает идентичность этого лица и заверяется электронной цифровой подписью поставщика услуг - центром сертификации ключей.

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 и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный 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.

Кто занимается выдачей сертификатов электронной цифровой подписи?

- Согласно Федеральному закону об «Электронной цифровой подписи», услуги ЭЦП, в том числе и выдачу сертификатов открытых ключей, осуществляет Удостоверяющий центр.

- Удостоверяющим центром (УЦ), выдающим сертификаты ключей подписей для использования в информационных системах общего пользования, должно быть юридическое лицо, выполняющее функции, предусмотренные настоящим Федеральным законом.

- При этом удостоверяющий центр должен обладать необходимыми материальными и финансовыми возможностями, позволяющими ему нести гражданскую ответственность перед пользователями сертификатов ключей подписей за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в сертификатах ключей подписей.

Средства работы с электронной цифровой подписью

1. 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.

Средства работы с электронной цифровой подписью

2. 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).

3. 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.).

ШИФРОВАНИЕ

- Шифрова́ние — преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.
- Главный образом, шифрование служит задаче соблюдения конфиденциальности передаваемой информации.
- Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

С помощью шифрования обеспечиваются три состояния безопасности информации:

- Конфиденциальность:

Шифрование используется для сокрытия информации от неавторизованных пользователей при передаче или при хранении.

- Целостность:

Шифрование используется для предотвращения изменения информации при передаче или хранении.

- Идентифицируемость:

Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Цели шифрования

- Шифрование применяется для хранения важной информации в ненадёжных источниках и передачи её по незащищенным каналам связи. Такая передача данных представляет из себя два взаимно обратных процесса:
- Перед отправлением данных по линии связи или перед помещением на хранение они подвергаются зашифрованию.
- Для восстановления исходных данных из зашифрованных к ним применяется процедура расшифрования.

Методы шифрования

Существующие методы шифрования можно разделить на две большие группы:

- Симметричное шифрование использует один ключ для шифрования и расшифрования.
- Асимметричное шифрование использует два различных ключа для шифрования и расшифрования.

- Также шифры могут отличаться структурой шифруемой информации. Они могут либо шифровать сразу весь текст, либо шифровать его по мере поступления.

Таким образом существуют:

- Блочный шифр шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.
- Поточный шифр шифрует информацию и выдает шифротекст по мере поступления, таким образом имея возможность обрабатывать текст неограниченного размера используя фиксированный объем памяти.