Содержание

1. Введение

2. Назначение и применение электронной подписи

3. Общая схема

4. Защищенность

5. Этапы становления ЭЦП в России

6. Использование ЭЦП в России

7. Использование ЭЦП в других странах

8. Алгоритмы

9. Симметричная схема

10. Ассиметричная схема

11. Использование хэш-функций

12. Управление ключами

13. Заключение

Введение

Информационные технологии шагают по планете. Сейчас сложно найти организацию, предприятие или фирму, офис которой не освещали бы экраны мониторов. Печатные машинки ушли в прошлое, уступив место компьютерам. Секретари хранят подготовленные шаблоны документов и перед распечаткой лишь подставляют нужные данные вместо того, чтобы всякий раз «отстукивать» полный текст. В то же самое время исследования, которые были проведены в странах с развитой информационной инфраструктурой, показали не уменьшение, а, наоборот, увеличение расхода бумаги. И дело не только в том, что современные принтеры в случае небольшой опечатки, допущенной сотрудником в тексте договора или платежного документа, позволяют производить макулатуру со скоростью от 12 листов в минуту. Ведь документ можно было бы вообще не распечатывать, ошибку исправить прямо в файле и передать партнерам или банку файл с конкретным документом — и никакой бумаги. Прочитать документ можно и с экрана монитора. Однако, ведя дела таким образом, можно попасть в ситуацию, когда недобросовестный партнер исправит в подготовленном договоре сумму сделки и предъявит этот файл как исходный со всеми печатями и подписями.

Говорят, что в старые времена разрубали монету и давали по одной половинке двум гонцам. Даже если они не были знакомы между собой, при встрече они могли сложить имеющиеся у них части монеты и убедиться, что служат общему делу. Предположим, что кто-то хочет передать вам конфиденциальное сообщение таким образом, чтобы прочесть его мог только адресат. В этом случае ему достаточно узнать ваш открытый ключ, а потом выполнить шифрование сообщения с его помощью. Полученный шифротекст может быть передан вам по открытым каналам связи. Для проверки подлинности предъявляются шифротекст, открытый ключ и исходный текст. Во-первых, по исходному тексту тем же самым способом вычисляется шифр - преобразование, во-вторых, шифротекст расшифровывается с помощью открытого ключа. Если оба результата идентичны — значит, текст не претерпел изменений. . Этот факт позволяет использовать его в качестве личной подписи владельца секретного ключа под файлом с текстом документа — электронной цифровой подписи.

Назначение и применение цифровой электронной подписи

Электронная подпись предназначена для идентификации лица, подписавшего электронный документ. Кроме этого, использование электронной подписи позволяет осуществить:

1. 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.
2. Защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев.
3. 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.
4. 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.

Все эти свойства ЭП позволяют использовать её для следующих целей:

1. Декларирование товаров и услуг (таможенные декларации)
2. Регистрация сделок по объектам недвижимости
3. Использование в банковских системах
4. Электронная торговля и госзаказы
5. Контроль исполнения государственного бюджета
6. В системах обращения к органам власти
7. Для обязательной отчетности перед государственными учреждениями

Защищенность

Цифровая подпись обеспечивает:

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

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

3) 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.

4)Предприятиям и коммерческим организациям сдачу финансовой отчетности в государственные учреждения в электронном виде;

5)Организацию юридически значимого электронного документооборота;

Возможны следующие угрозы цифровой подписи:

1) Злоумышленник может попытаться подделать подпись для выбранного им документа.

2)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 собой осмысленный текст; Текст документа оформлен по установленной форме.

3)Документы редко оформляют в виде Plain Text — файла, чаще всего в формате DOC или HTML.

Использование ЭЦП в России

После становления ЭЦП при использовании в электронном документообороте между кредитными организациями и кредитными бюро в 2005 году активно стала развиваться инфраструктура электронного ДОУ между налоговыми органами и налогоплательщиками. Начал работать приказ Министерства по налогам и сборам Российской Федерации от 2 апреля 2002 г. N БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи». Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи определяет общие принципы организации информационного обмена при представлении налогоплательщиками налоговой декларации в электронном виде по телекоммуникационным каналам связи.

В Законе РФ от10.01.2002 № 1-ФЗ «ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ» прописаны условия использования электронной цифровой подписи, особенности ее использования в сферах государственного управления и в корпоративной информационной системе. Благодаря электронной цифровой подписи теперь, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете, через «Системы электронной торговли», обмениваясь с контрагентами необходимыми документами в электронном виде, подписанными ЭЦП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.

В Москве в рамках реализации ГЦП (Городской целевой программы) "Электронная Москва" был образован Уполномоченный удостоверяющий Центр ОАО "Электронная Москва" (<http://www.uc-em.ru>) для решения задач координации работ и привлечения инвестиций при выполнении Городской целевой программы.

Заключение

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр на основании государственной лицензии. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Федеральный закон от 10.01.2002 N 1-ФЗ «Об электронной цифровой подписи» Еще до вступления в силу этого закона термин "электронная цифровая подпись" содержится более чем в полусотне нормативных актов, но лишь этот закон содержит комплексную правовую базу для широкого ее использования в предпринимательской деятельности и развития электронной коммерции в нашей стране. В соответствии с Законом владельцем может быть только физическое лицо. Такой подход принят и в европейском законодательстве. Естественно, как и в случае с собственноручной подписью, физическое лицо может действовать от имени юридического лица, но на такое полномочие обязательно должно быть указано в сертификате ключа подписи. В законодательстве других стран, например США, допускается принадлежность электронной подписи не только физическим, но и юридическим лицам. "Американский" подход неудачен, поскольку при этом возрастает вероятность несанкционированного использования электронной подписи юридического лица, при котором сложно установить конкретное физическое лицо, осуществившее подписание электронного документа.