Электро́нная цифрова́я по́дпись(ЭЦП)— реквизит электронного документа, предназначенный для защиты данного **электронного документа** от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивает не отказуемость подписавшегося .

Составные части ЭЦП.

Схема электронной подписи обычно включает в себя:

· алгоритм генерации ключевых пар пользователя;

· функцию вычисления подписи;

· функцию проверки подписи.

Функция вычисления подписи на основе документа и секретного ключа пользователя вычисляет собственно подпись. В зависимости от алгоритма функция вычисления подписи может быть детерминированной или вероятностной. Детерминированные функции всегда вычисляют одинаковую подпись по одинаковым входным данным. Вероятностные функции вносят в подпись элемент случайности, что усиливает криптостойкость алгоритмов ЭЦП. Однако, для вероятностных схем необходим надёжный источник случайности (либо аппаратный генератор шума, либо криптографически надёжный генератор псевдослучайных бит),что усложняет реализацию.

В настоящее время детерминированные схемы практически не используются. Даже в изначально детерминированные алгоритмы сейчас внесены модификации, превращающие их в вероятностные (так, в алгоритм подписи RSA вторая версия стандарта PKCS#1добавила предварительное преобразование данных (OAEP), включающее в себя, среди прочего, зашумление).

Функция проверки подписи проверяет, соответствует ли данная подпись данному документу и открытому ключу пользователя. Открытый ключ пользователя

доступен всем, так что любой может проверить подпись под данным документом.

Поскольку подписываемые документы — переменной (и достаточно большой) длины, в схемах ЭЦП зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭЦП, поэтому в схеме может быть использована любая надёжная хэш-функция.

Алгоритмы ЭЦП делятся на два больших класса: обычные цифровые подписи и цифровые подписи с восстановлением документа. Обычные цифровые подписи необходимо пристыковывать к подписываемому документу. К этому классу относятся, например, алгоритмы, основанные на эллиптических кривых (ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002).Цифровые подписи с восстановлением документа содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и тело документа. К этому классу относится один из самых популярных алгоритмов —RSA.

Следует различать электронную цифровую подпись и код аутентичности сообщения, несмотря на схожесть решаемых задач (обеспечение целостности документа и неотказуемости авторства). Алгоритмы ЭЦП относятся к классу асимметричных алгоритмов, в то время как коды аутентичности вычисляются по симметричным схемам .

Назначение ЭЦП.

Электронная цифровая подпись может иметь следующее назначение:

· Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» ит. 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 хешированияMD5.

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.

2. Преимущества использования электронной цифровой подписи

Применение ЭЦП имеет следующие преимущества:

· Конфиденциальность: электронной цифровой подписи (ЭЦП) безошибочно указывает на аутентичность и уникальность своего автора; ЭЦП не поддается подделке или переносу с документа на документ; ЭЦП защищает подписанный документ от подделки, а также от изменения или искажения содержащейся в нем информации; ЭЦП несет принцип неотречения, что предотвращает отказ

· Снижение в несколько раз материальных и технических затрат налогоплательщика

· Не требуется наличия у налогоплательщика специалистов, владеющих знаниями и навыками формирования отчетности в электронном виде

· Приоритетность сдачи отчетности в электронном виде

· Экономия времени, сил и нервов, так как не требуется посещения налогового органа при сдаче отчетности

· Возможность предоставления отчетности вплоть до 24 часов последнего дня сдачи отчетности

· Прохождение первичного камерального контроля, что исключает наличие арифметических и логических ошибок, использование контрольных соотношений, которые используют в налоговых органах при проведении камеральных проверок

· Возможность оперативного обновления форматов представления документов в электронном виде по телекоммуникационным каналам связи (в случае изменения форм налоговых деклараций и иных документов, служащих основанием для исчисления и у платы налогов, и бухгалтерской отчетности или введения новых форм деклараций налогоплательщик автоматически получает возможность обновления версий форматов)

· Возможность получения выписки (отправив информацию в налоговый орган в электронном виде по телекоммуникационным каналам связи, налогоплательщик имеет возможность получить выписку о выполнении обязательств перед бюджетом)

· Подтверждение доставки отчетности (налоговый орган высылает квитанцию о приеме налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи)

· Оперативное информирование о действующих налогах и сборах, законодательстве (о налогах и сборах и принятых в соответствии с ним нормативных правовых актах и других).

3. Использование ЭЦП вмире

Система электронных подписей широко используется в Эстонской Республике, где введена программа ID-карт, которыми снабжены 3/4 населения страны.

При помощи электронной подписи в марте 2007 года были проведены выборы в местный парламент— Рийгикогу. При голосовании электронную подпись использовали 400 000 человек.

Кроме того, при помощи электронной подписи можно отправить налоговую декларацию, таможенную декларацию, различные анкеты как в местные

самоуправления, так и в государственные органы.

В крупных городах при помощи ID-карты возможна покупка месячных автобусных билетов.

Все это осуществляется через центральный гражданский портал Eesti.ee. Эстонская ID-карта является обязательной для всех жителей с 15 лет, проживающих временно или постоянно на территории Эстонии .

4. Правовые основы и особенности использования ЭЦП в Украине

Внедрение на Украине системы формальных процедур документооборота, соответствующей международным, ив особенности европейским, стандартам, которая бы, не теряя своей юридической надежности, отличалась гибкостью, универсальностью, удобством, является крайне необходимым. Причем не только для контрагентов в банковских или коммерческих операциях, с чем чаще всего ассоциируется использование элекронной цифровой подписи (ЭЦП). Ведь речь идет не только о сфере хозяйственного права. ЭЦП —одно из потенциальных средств осуществления правоотношений, которые традиционно относятся к предмету регулирования административного права.

Однако опыт некоторых стран СНГ доказывает, что с принятием законодательных актов, определяющих статус ЭЦП, нередко возникали разнообразные коллизии, препятствующие реализации этих актов. Сравнивая положения Федерального закона Российской Федерации «Об электронной цифровой подписи» (далее — Закон РФ), подписанного Президентом РФ в январе 2002 года, и проекта Закона Украины «Об электронной цифровой подписи»(далее — законопроект), и имея при этом представление о структуре государственного аппарата на Украине (в частности, центральных органов исполнительной власти), можно предположить, что подобная перспектива вполне возможна.

Законопроект об ЭЦП

В целом законопроект довольно сбалансирован и преимущественно сориентирован на международные и европейские стандарты систем коммуникаций. Как позитив мы воспринимаем предусмотренную в законопроекте альтернативу для пользователей в порядке использования цифровой подписи (речь не идет о государственном секторе).

Законы об ЭЦП приняты в Германии, Австрии, Франции, Индии, Ирландии, Республике Корея, Литве, Польше, Финляндии, Эстонии, России, Таиланде и т.п. Подобные законы действуют даже в странах, где существовали стойкие традиции договорной юрисдикции, диспозитивности в регулировании хозяйственной деятельности между контрагентами, например, в Великобритании и США. Закон об электронном документообороте принятии в Беларуси.

Конечно, в каждом государстве установлен свой более или менее либеральный подход к регулированию порядка использования криптографических (технологических) средств [1].

Использование ЭЦП в системе B2B-Украина позволяет:

· **приравнять по юридической значимости** электронные документы, используемые в Системе, к традиционным бумажным документам;

· организаторам процедур – подписывать ЭЦП объявление конкурсов, аукционов и размещение объявлений;

· организаторам конкурсов – заверять загружаемую в Систему конкурсную документацию;

· участникам конкурсов – заверять загружаемые в Систему конкурсные заявки;

· использовать для обеспечения конкурсных заявок Электронную Банковскую Гарантию;

· подписывать ставки на аукционах и подачу предложений в объявлениях;

· оптимизировать процедуру подготовки, учета и хранения документов;

· обеспечить целостность и подлинность электронных документов;

· **обеспечить однозначное установление авторства документов**, используемых в торгах;

· **исключить возможность подделки подписи и подписанных документов**;

· уменьшить число конфликтных ситуаций, возникающих при некорректной отправке конкурсных заявок и файлов с ценами для переторжки.

Защита электронного документа в Системе обеспечивает:

· подтверждение того, что документ исходит от конкретного пользователя Системы (подтверждение авторства документа);

· проверку подлинности и целостности документа;

· предотвращение несанкционированного доступа к документу в процессе информационного обмена;

· идентификацию пользователя Системы, подписавшего электронный документ.