Содержание:

Введение

Электронная подпись предназначена для защиты электронного документа, передаваемого посредством различных сред или хранящегося в цифровом виде, от подделки и является атрибутом электронного документа. Она получается в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяет идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе.

Электронная цифровая подпись (ЭЦП) – это программно-криптографическое средство, которое обеспечивает:

- Проверку целостности документов;
- Конфиденциальность документов;
- Установление лица, отправившего документ

Электронная подпись 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.

Электронный документ

- это любой документ, созданный при помощи компьютерных технологий и хранящийся на носителях информации, обрабатываемых при помощи компьютерной техники, будь то письмо, контракт или финансовый документ, схема, чертеж, рисунок или фотография.

Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

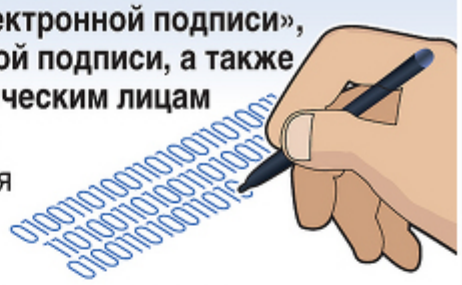
- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждение подлинности электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Схема принципа действия ЭП

ЗАКОН ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

Госдума приняла базовый закон «Об электронной подписи», который расширяет понятие электронной подписи, а также позволяет использовать ее юридическим лицам

Кроме того, закон регулирует работу и аккредитацию центров удостоверения электронной подписи, ее выдачу, проверку и удаление



ПРИНЦИП ДЕЙСТВИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Подготовка ключей

Закрытый ключ — *Остаётся у владельца подписи*

Программно-технический комплекс

Открытый ключ — *Передаётся адресату*

Хеш-функция *(Идентификатор документа, математически рассчитываемый на основании текста самого документа, позволяющий сравнивать документ на соответствие)*

Подписание

- Электронный документ
- Создание хеш-функции
- Шифрование хеш-функции закрытым ключом
- Создание электронной подписи
- Соединение подписи с документом

Проверка

- Подписанный электронный документ, переданный адресату
- Считывание документа
- Создание хеш-функции
- Расшифровка хеш-функции открытым ключом
- Восстановление хеш-функции
- Сравнение хеш-функций, если они одинаковые, электронная подпись верна

Источник: uc.credos.ru

ТАСС Телеком · ИТАР-ТАСС

Преимущества использования ЭП

Использование ЭП позволяет:

- 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.

Подделать ЭП 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 ЭП 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

Как происходит подписание документа с помощью ЭЦП?

Подпись ставят не на сам документ, а на его хэш. Хэш - это сжатая версия документа. Он нужен, потому что электронные документы весят достаточно много, поэтому на их шифрование уходило бы достаточно много времени. Для вычисления хэша применяют криптографические хэш-функции. Это гарантия того, что любые изменения в документе при проверке подписи будут выявлены.

Преимущество хэш-функций

- Быстрое формирование и подпись из-за меньшего объема информации.

- Хэш-функция позволяет не делить объемный текст на блоки и не терять их порядок.

После того, как получен хэш документа, отправитель шифрует информацию при помощи закрытого ключа. У отправителя документа и его получателя есть два ключа: закрытый и открытый. Оба хранят свои ключи у себя, но закрытый нельзя передавать никому, а открытый можно передавать любому. Закрытый ключ применяется отправителем для шифрования, а открытый ключ использует получатель для расшифровки данных. Благодаря такой схеме можно легко обмениваться секретной информацией с разными получателями с минимальным риском потери информации. Если только получатель не потерял собственный ключ или не передал в руки злоумышленников.

Зашифрованный закрытым ключом хэш отправляется получателю вместе с сертификатом. Сертификат вручает аккредитованный центр сертификации ключей. АЦСК проверяет принадлежность открытого ключа получателю. Открытый ключ находится в сертификате и известен владельцу и получателю.

Получатель расшифровывает документ с помощью открытого ключа. Узнать, подлинна ли электронная подпись возможно:

- С помощью программного обеспечения.
- На сайте госуслуг.
- Самостоятельно, по значению хеш-функций. Суть проверки - сравнить хэш документа и расшифрованную подпись, и если они совпадают, значит подпись верна.

Как формируется Электронная цифровая подпись

Личный ключ ЭЦП формируется на основании абсолютно случайных

чисел, генерируемых датчиком случайных чисел, а открытый — вычисляется из личного ключа ЭЦП таким образом, чтобы получить второй из первого было невозможно.

Кроме того, закрытый ключ ЭЦП представляет собой уникальную

последовательность символов длиной 264 бита, которая предназначена для создания ЭЦП в электронных документах. Работает личный ключ только в паре с

открытым ключом.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Открытый ключ содержится в Сертификате открытого ключа, и подтверждает принадлежность открытого ключа ЭЦП определенному лицу.

Использовать электронную цифровую подпись может любой человек, не зависимо от уровня владения персональным компьютером, образования и рода занятий.

Как отмечалось выше ЭЦП - это часть электронного документа, а фактически - обычный файл, полученный в результате криптографического преобразования документа.

При использовании ЭЦП гарантируется следующее. Во-первых, то, что документ не изменился в процессе пересылки. Если после подписания цифровой подписью документ был искажен, это выяснится при проверке открытым ключом. Во-вторых - гарантируется однозначная идентификация отправителя. В случае с обычной подписью это можно сделать, например, сравнив с подписью в паспорте.

Электронная подпись основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой

подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы.

Для каждого абонента генерируется пара ключей: секретный и открытый.

Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Для хранения закрытого ключа используют:

- USB-накопители,
- дискеты,
- считыватель для ключей,
- защищенную память компьютера
- смарт-карты, пластиковой карты с микросхемой, на которых можно хранить информацию.

Три вида электронной подписи

Электронные подписи разделяются законом 2011 г. на три вида.

- Простые подписи создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания.
- Усиленная неквалифицированная подпись создана с использованием криптографических средств и позволяет определить не только автора документа, но проверить его на наличие изменений. Для создания таких подписей может использоваться сертификат неаккредитованного центра, можно также вообще обойтись без сертификата, если технические средства позволяют выполнить требования закона.

- Усиленная квалифицированная подпись является разновидностью усиленных, она имеет сертификат от аккредитованного центра и создана с помощью подтвержденных ФСБ средств.

Кому необходима электронная подпись

Для некоторых категорий лиц квалифицированная электронная подпись — необходимость для сдачи отчётности в ФНС, ПФР и ФСС. При количестве сотрудников в компании, превышающем определённое число, отчётность нужно сдавать только в электронной форме.

Отчётность только в электронном виде сдают:

- В ФНС — компании с численностью сотрудников более 100 человек, а также все плательщики НДС;
- ПФР и ФСС — компании с численностью сотрудников более 25 человек.

В остальных случаях компании имеют право выбирать — отчёты на бумаге или в электронной форме. Но преимущества сдачи отчётности, заверенной электронной подписью, через интернет очевидны: не нужно стоять в очередях и даже покидать рабочее место, отчёты будут доставлены мгновенно и гарантированно. Электронная сдача отчётности экономит время, бумагу и предотвращает непредвиденные ситуации, связанные с возможной утерей или задержкой попадания документа в контролирующий орган. Еще одно важно преимущество электронной отчётности заключается в возможности использования электронных документов при разборе спорных ситуаций с контролирующими органами, с подтверждениями оператора как третьей стороны.

Также КЭП необходима предпринимателям, обязанным по закону перейти на онлайн-кассы. В этом случае электронная подпись нужна для регистрации онлайн-ККТ в Федеральной налоговой службе и для заключения договора с оператором фискальных данных.

Юридические лица, ведущие деятельность в форме акционерного общества, обязаны раскрывать в интернете сведения о своей деятельности на сайте Единого федерального реестра сведений о фактах деятельности юридических лиц (ЕФРСФДЮЛ). Для раскрытия сведений нужна электронная подпись.

Электронная подпись необходима государственным и муниципальным организациям для проведения закупок по 44-ФЗ.

Как используют электронную подпись

Даже если в использовании электронной подписи нет законодательной необходимости, она может упростить ведение бизнеса и решение повседневных вопросов гражданина. Рассмотрим подробнее основные сферы применения ЭП.

Электронный документооборот

Электронная подпись необходима при работе в системах электронного документооборота для обмена письмами и документами различного формата. Электронный документооборот делает взаимодействие значительно быстрее,

проще и надёжнее, а также избавляет от проблем, связанных с хранением большого количества бумаг. ЭДО можно организовать внутри организации и с другими компаниями. Возможность шифрования передаваемых электронных документов обеспечивает абсолютно конфиденциальную деловую переписку контрагентов.

Электронная отчётность

Помимо вышеперечисленных ситуаций, в которых отчётность возможна только в электронном виде, можно в добровольной форме перейти на электронные отчёты в ФНС, Росстат, ФСС, ПФР и другие контролирующие организации. Для этого тоже понадобится квалифицированная электронная подпись.

Участие в электронных торгах

Для участия в торгах на федеральных и коммерческих электронных торговых площадках необходимо получить сертификат ключа проверки электронной подписи. В электронных торгах могут участвовать физические и юридические лица.

Доступ к информационным государственным системам

Госуслуги и прочие государственные порталы требуют обязательного наличия электронной подписи, благодаря которой можно удалённо оплачивать штрафы, подавать заявления на регистрацию бизнеса, записываться на прием к врачу.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

- https://ecm-journal.ru
- https://prezi.com
- https://iitrust.ru
- https://www.1-ofd.ru
- http://www.tadviser.ru