

image not found or type unknown



Сейчас сложно обнаружить профессионала по части информатизации или телекоммуникаций, который бы не знал, что такое электрическая числовая подпись (ЭЦП). Впрочем мало кто осознает, что само подходящее применение данной схемы исключительно создает предпосылки для организации де-юре необходимого электрического документооборота. Точно так же как технологии бумаги или авторучек - это лишь вероятность организовать установленный бумажный документооборот. Что необходимо предпринять, дабы перевод электронными документами с ЭЦП стал в такой же степени привычным, будто и документами на бумажном носителе?

Электрическая числовая закорючка - атрибут электрического документа, приготовленный для защиты предоставленного электрического документа через подделки, произведенный в результате шифровального переустройства информации с употреблением закрытого ключа электронной цифровой подписи и позволяющей идентифицировать собственника сертификата ключа подписи, а да определить неимение искажений информации в электрическом документе. Электрическая числовая закорючка в электрическом документе равнозначна собственноручной подписи в документе для бумажном носителе при одновременном следованье последующих условий:

документ ключа подписи, относящийся к этой электрической цифровой подписи, не потерял множеству (действует) для пункт проверки или на пункт подписания электрического документа присутствие доказательств, устанавливающих пункт подписания; -подтверждена подлинностью электрической цифровой подписи в электрическом документе;

электронная числовая подпись используется в соответствии со сведениями, подтвержденными в сертификате ключа подписи.

Хэш-функция защищаемого электронного документа представляет собой уникальное число, получаемое из исходного документа путем его преобразования с помощью сложного, но известного алгоритма (хэш-функции).

Хэш-функция чувствительна к всевозможным искажениям исходного электронного документа, то есть изменение (искажение) хотя бы одного знака в исходном

документе приводит в среднем к искажению половины знаков хэш-значения. Кроме того, она устроена таким образом, что, во-первых, по хэш-значению документа нельзя восстановить исходный электронный документ, а во-вторых, практически невозможно отыскать два различных электронных документа, которые обладали бы одним и тем же хэш-значением.

Схема формирования электронной цифровой подписи под электронным документом его создателем (отправителем) предусматривает вычисление хэш-функции этого документа и шифрование этого значения посредством секретного ключа отправителя.

Результатом шифрования и является значение ЭЦП как реквизит электронного документа, которое пересылается получателю вместе с этим документом.

Таким образом, электронная цифровая подпись жестко увязывает содержание документа и секретный ключ для формирования ЭЦП и делает невозможным изменение документа без нарушения подлинности данной подписи.

Заключение

Электронная цифровая подпись может использоваться в нескольких ипостасях. Закон «Об ЭЦП» определяет условия применения ЭЦП как ответственной подписи в документе, аналога собственноручной подписи и печати. Подобным образом ЭЦП используется в системах электронного документооборота различного назначения (организационно-распорядительного, кадрового, законодательного, торгово-промышленного и прочего). Однако область применения ЭЦП не ограничивается приведенными областями. Сама по себе, электронная цифровая подпись - великолепный механизм обеспечения целостности и подтверждения авторства и актуальности любых данных, представленных в электронном виде.

Электронная подпись поможет проверить целостность электронного письма (e-Mail) и убедиться в надёжности отправителя, однозначно определит автора статьи, опубликованной в Интернете, и укажет дату публикации, позволит написать собственное мнение о прочитанном документе в Microsoft Word и прикрепить его в виде «стикера» к файлу, не «испортив» сам файл своими пометками, при этом надёжно привязав такой «стикер» к текущему содержимому документа (при изменении текста документа «стикер» сразу обнаружит, что документ изменялся), оставит «визитную карточку» о действиях, совершённых в электронном мире, подтвердит полномочия и т.п.

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.

Список использованной литературы

1. Федеральный закон «Об электронной цифровой подписи» от 10 января
2. «Некоторые вопросы правового обеспечения использования ЭЦП» Беззубцев О.А., Мартынов В.Н., Мартынов В.М.
3. «Информатика для юристов и экономистов» Под ред. С.В. Симоновича. СПб.: Питер, 2002.
4. «Электронный документ» А. Марченко.
5. «Законодательное регулирование правового статуса ЭЦП. Основные положения» Ткачев А.В
6. «Юридический справочник руководителя» 2008 г.