Электронная подпись – это не предмет, который можно взять в руки, а реквизит документа, позволяющий подтвердить принадлежность ЭЦП ее владельцу, а также зафиксировать состояние информации/данных (наличие, либо отсутствие изменений) в электронном документе с момента его подписания.

Согласно законодательству РФ, квалифицированная электронная подпись — это эквивалент подписи, проставляемой «от руки», обладающий полной юридической силой. Помимо квалифицированной в России представлены еще два вида ЭЦП:

— неквалифицированная — обеспечивает юридическую значимость документа, но только после заключения дополнительных соглашений между подписантами о правилах применения и признания ЭЦП, позволяет подтвердить авторство документа и проконтролировать его неизменность после подписания,

— простая — не придает подписанному документу юридическую значимость до заключения дополнительных соглашений между подписантами о правилах применения и признания ЭЦП и без соблюдении законодательно закрепленных условий по ее использованию (простая электронная подпись должна содержаться в самом документе, ее ключ применяться в соответствии с требованиями информационной системы, где она используется, и прочее согласно ФЗ-63, ст.9), не гарантирует его неизменность с момента подписания, позволяет подтвердить авторство. Ее применение не допускается в случаях, связанных с государственной тайной.

Возможности электронной подписи

Физическим лицам ЭЦП обеспечивает удаленное взаимодействие с государственными, учебными, медицинскими и прочими информационными системами через интернет.

Юридическим лицам электронная подпись дает допуск к участию в электронных торгах, позволяет организовать юридически-значимый электронный документооборот (ЭДО) и сдачу электронной отчетности в контролирующие органы власти.

Возможности, которые предоставляет ЭЦП пользователям, сделали ее важной составляющей повседневной жизни и рядовых граждан, и представителей компаний.

Выданная электронная подпись состоит из 3 элементов:

1 – средство электронной подписи, то есть необходимое для реализации набора криптографических алгоритмов и функций техническое средство. Это может быть либо устанавливаемый на компьютер криптопровайдер (КриптоПро CSP, ViPNet CSP), либо самостоятельный токен со встроенным криптопровайдером (Рутокен ЭЦП, JaCarta ГОСТ), либо «электронное облако». Подробнее прочитать о технологиях ЭЦП, связанных с использованием «электронного облака», можно будет в следующей статье Единого портала Электронной подписи.

Криптопровайдер — это независимый модуль, выступающий «посредником» между операционной системой, которая с помощью определенного набора функций управляет им, и программой или аппаратным комплексом, выполняющим криптографические преобразования.

Важно: токен и средство квалифицированной ЭЦП на нем должны быть сертифицированы ФСБ РФ в соответствии с требованиями федерального закона № 63.

2 – ключевая пара, которая представляет из себя два обезличенных набора байт, сформированных средством электронной подписи. Первый из них – ключ электронной подписи, который называют «закрытым». Он используется для формирования самой подписи и должен храниться в секрете. Размещение «закрытого» ключа на компьютере и flash-носителе крайне небезопасно, на токене — отчасти небезопасно, на токене/smart-карте/sim-карте в неизвлекаемом виде — наиболее безопасно. Второй — ключ проверки электронной подписи, который называют «открытым». Он не содержится в тайне, однозначно привязан к «закрытому» ключу и необходим, чтобы любой желающий мог проверить корректность электронной подписи.

3 – сертификат ключа проверки ЭЦП, который выпускает удостоверяющий центр (УЦ). Его назначение — связать обезличенный набор байт «открытого» ключа с личностью владельца электронной подписи (человеком или организацией). На практике это выглядит следующим образом: например, Иван Иванович Иванов (физическое лицо) приходит в удостоверяющий центр, предъявляет паспорт, а УЦ выдает ему сертификат, подтверждающий, что заявленный «открытый» ключ

принадлежит именно Ивану Ивановичу Иванову. Это необходимо для предотвращения мошеннической схемы, во время развертывания которой злоумышленник в процессе передачи «открытого» кода может перехватить его и подменить своим. Таким образом, преступник получит возможность выдавать себя за подписанта. В дальнейшем, перехватывая сообщения и внося изменения, он сможет подтверждать их своей ЭЦП. Именно поэтому роль сертификата ключа проверки электронной подписи крайне важна, и за его корректность несет финансовую и административную ответственность удостоверяющий центр.

В соответствии с законодательством РФ различают:

— «сертификат ключа проверки электронной подписи» формируется для неквалифицированной ЭЦП и может быть выдан удостоверяющим центром;

— «квалифицированный сертификат ключа проверки электронной подписи» формируется для квалифицированной ЭЦП и может быть выдан только аккредитованным Министерством связи и массовых коммуникаций УЦ.

Условно можно обозначить, что ключи проверки электронной подписи (наборы байт) — понятия технические, а сертификат «открытого» ключа и удостоверяющий центр — понятия организационные. Ведь УЦ представляет собой структурную единицу, которая отвечает за сопоставление «открытых» ключей и их владельцев в рамках их финансово-хозяйственной деятельности.

Подводя итог вышеизложенному, фраза «клиенту выдана электронная подпись» состоит из трех слагаемых:

Клиент приобрел средство электронной подписи.

Он получил «открытый» и «закрытый» ключ, с помощью которых формируется и проверяется ЭЦП.

УЦ выдал клиенту сертификат, подтверждающий, что «открытый» ключ из ключевой пары принадлежит именно этому человеку.

ребуемые свойства подписываемых документов:

целостность;

достоверность;

аутентичность (подлинность; «неотрекаемость» от авторства информации).

Их обеспечивают криптографические алгоритмы и протоколы, а также основанные на них программные и программно-аппаратные решения для формирования электронной подписи.

С определенной долей упрощения можно говорить, что безопасность электронной подписи и сервисов, предоставляемых на ее основе, базируется на том, что «закрытые» ключи электронной подписи хранятся в секрете, в защищенном виде, и что каждый пользователь ответственно хранит их и не допускает инцидентов.