Электронная подпись

Электронная подпись в России впервые появилась в январе 2002 года вместе с принятием первого закона «Об электронной цифровой подписи» (1-ФЗ). Затем, спустя 9 лет, в апреле 2011 появился новый закон «Об электронной подписи» (63-ФЗ).

Закон, регулирующий отношения в области использования **электронных подписей** при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами - **Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ.**

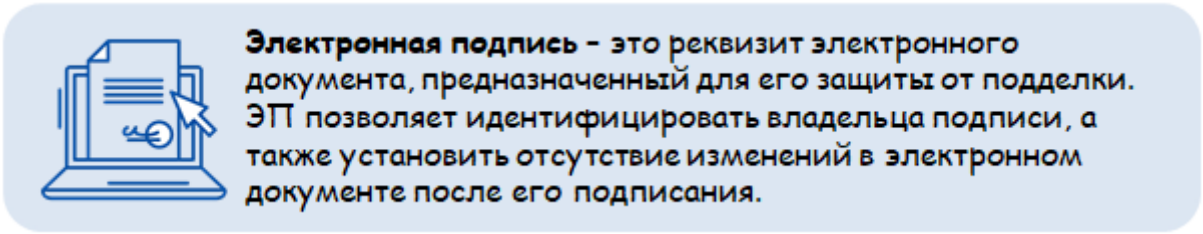
ФЗ "Об электронной подписи"

Основные понятия

Рано или поздно организация начинает задумываться о переходе на электронный документооборот и внедрении электронной подписи (ЭП). Некоторые внедряют ЭП как дань моде, другие – потому что так требует законодательство, а третьи потому что проанализировали бизнес-процессы, взвесили риски и затраты и определили, для чего это необходимо.

1) **электронная подпись** (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

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



2) **сертификат ключа проверки электронной подписи** - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

3) **квалифицированный сертификат ключа проверки электронной подписи** (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный

аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган);

4) **владелец сертификата ключа проверки электронной подписи** - лицо, которому в установленном Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

5) **ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи;

6) **ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи);

7) **удостоверяющий центр** - юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом;

8) **аккредитация удостоверяющего центра** - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона;

9) **средства электронной подписи** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

10) **средства удостоверяющего центра** - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра;

11) **участники электронного взаимодействия** - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане;

12) **корпоративная информационная система** - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц;

13) **информационная система общего пользования** - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано;

14) **вручение сертификата ключа проверки электронной подписи** - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу;

15) **подтверждение владения ключом электронной подписи** - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Виды электронных подписей

Видами электронных подписей являются:

- простая электронная подпись
- усиленная электронная подпись.

Различаются *усиленная:*

1. усиленная неквалифицированная электронная подпись
2. усиленная квалифицированная электронная подпись

Простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.

Неквалифицированной электронной подписью является электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Согласно законодательству *РФ, квалифицированная электронная подпись — это эквивалент подписи, проставляемой «от руки», обладающий полной юридической силой.*

При использовании **неквалифицированной электронной подписи** сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Возможности электронной подписи для физических лиц: обеспечивает удаленное взаимодействие с государственными, учебными, медицинскими и прочими информационными системами через интернет.

Возможности электронной подписи для юридических лиц: электронная подпись дает допуск к участию в электронных торгах, позволяет организовать юридически-значимый электронный документооборот (ЭДО) и сдачу электронной отчетности в контролирующие органы власти.

Квалифицированная подпись

Универсальный вариант — квалифицированная подпись. Именно ее наличие в первую очередь проверяют в государственных органах.

	Простая ЭП	Неквалифицированная ЭП	Квалифицированная ЭП
Внешние и внутренние электронные документы	+	+	+
Документооборот с физическими лицами	+	+	+
Арбитражный суд	+	+	+
Госуслуги	+		+
Контролирующие органы (ФНС, ПФР, ФСС)			+
Электронные торги			+

Такая подпись подойдет для счетов-фактур и налоговой. По закону электронные счета-фактуры можно подписывать только такой подписью. Стоит квалифицированный сертификат от 1000 руб., купить его можно только в удостоверяющем центре, входящем в зону доверия ФНС.

Каждый год сертификат квалифицированной подписи необходимо обновлять, что добавляет забот: надо следить за сроком действия и вовремя заказывать перевыпуск.

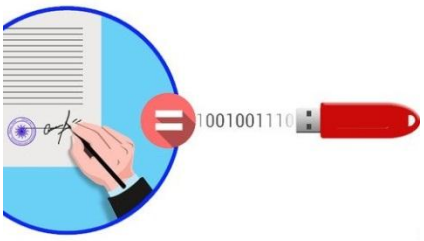
Для работы с квалифицированной подписью надо установить специальную программу — средство криптозащиты информации. Программа крепит электронную подпись на документ и проверяет подписи других участников обмена.

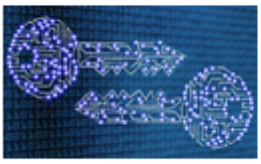
Можно выбрать платную программу («Криптопро ЦСП») или бесплатную («Випнет ЦСП» - ViPNet CSP). Функционально они почти не отличаются, но с бесплатной могут возникнуть проблемы совместимости. Платная стоит около 1000 руб., ежегодная оплата сертификата электронной подписи еще около 1000 руб.

Некоторые используют облачную электронную подпись, для нее не надо устанавливать программу криптозащиты. Облачная подпись хранится в сервисе обмена, и каждый раз, когда вы подписываете документ, вам на телефон приходит смс с подтверждением действия. Такой сертификат дешевле и удобнее в использовании, но менее безопасен, чем программа криптозащиты.

Как выглядит ЭП

Сама по себе подпись является не предметом, а результатом криптографических преобразований подписываемого документа, и ее нельзя «физически» выдать на каком-либо носителе (токене, smart-карте и т.д.). Также ее нельзя увидеть, в прямом значении этого слова; она не похожа на росчерк пера либо фигурный оттиск.





Криптографическое преобразование — это зашифровка, которая построена на использующем секретный ключ алгоритме.

Процесс восстановления исходных данных после криптографического преобразования без данного ключа, по мнению специалистов, должен занять большее время, чем срок актуальности извлекаемой информации.

Flash-носитель — это компактный носитель данных, в состав которого входит flash-память и адаптер (usb-флешка).

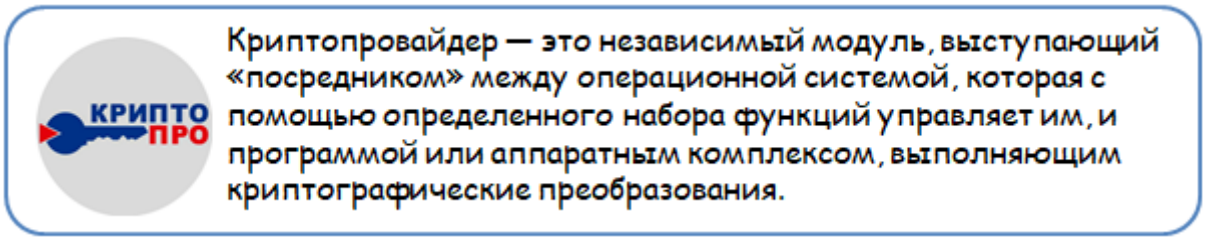
Токен — это устройство, корпус которого аналогичен корпусу usb-флешки, но карта памяти защищена паролем. На токене записана информация для создания ЭП. Для работы с ним необходимо подключение к usb-разъему компьютера и введения пароля.

Smart-карта — это пластиковая карта, позволяющая проводить криптографические операции за счет встроенной в нее микросхемы.

Sim-карта с чипом — это карта мобильного оператора, снабженная специальным чипом, на которую на этапе производства безопасным образом устанавливается java-приложение, расширяющее ее функциональность.

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».



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 ЭП, который выпускает удостоверяющий центр (УЦ). Его назначение — связать обезличенный набор байт «открытого» ключа с личностью владельца электронной подписи (человеком или организацией).

В самом простом представлении **механизм ЭП работает следующим образом.** Выделяется удостоверяющий центр (подразделение или внешняя организация), который с помощью специализированного программного обеспечения генерирует так называемые «сертификаты ключей» для каждого пользователя. Ключ ЭП – это уникальная последовательность символов. Он состоит из закрытого ключа (он доступен только своему владельцу, с его помощью владелец может подписать документ ЭП) и открытого ключа (он доступен всем, с его помощью можно определить, кто и когда подписал электронный документ).

При использовании **ECM-системы** все «сложности», с которыми может столкнуться пользователь, скрываются. Пользователь, как правило, должен просто выбрать нужную функцию: «Подписать документ» (документ, подписанный ЭП, будет одновременно закрыт для изменений) или «Получить информацию о подписях».

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.

Следовательно, если говорят, что «клиенту выдана электронная подпись» это значит:

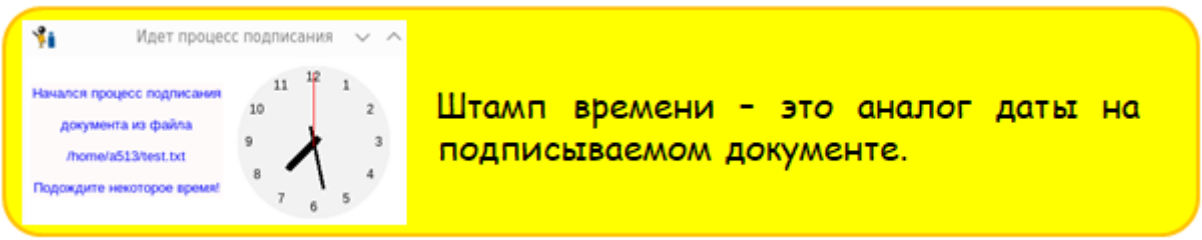
- Клиент приобрел средство электронной подписи.
- Он получил «открытый» и «закрытый» ключ, с помощью которых формируется и проверяется ЭЦП.
- УЦ выдал клиенту сертификат, подтверждающий, что «открытый» ключ из ключевой пары принадлежит именно этому человеку.

Вопрос безопасности

Требуемые 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.

Хранение электронных документов

Срок действия сертификата электронной подписи составляет один год, а, например, бухгалтерские документы, необходимо хранить пять лет. Но даже после истечения срока действия сертификата, документ не потеряет юридической силы, так как в момент подписания ставится штамп времени.



Штамп времени подтверждает, что сертификат электронной подписи был действителен на момент подписания документа. Так, в момент подписания документа проставляется штамп времени и результат проверки сертификата.

Подтвердить тот факт, что на момент подписания сертификат был действующим, можно также, обратившись к списку отозванных сертификатов на сайте удостоверяющего центра.

Непосредственно хранение электронных документов можно организовать, по крайней мере, двумя способами:

- локальное хранение (документы хранятся на локальных серверах вашей компании, например, в СЭД);
- хранение в облаке (документы хранятся на серверах компании, услугами которой вы воспользовались).

Услуги электронного архивирования предлагают операторы ЭДО.