Федеральный закон “Об электронной подписи”/ N 63-ФЗ от 06.04.2011/

6 апреля 2011 года N 63-ФЗ

Принят Государственной Думой25 марта 2011 года

Одобрен Советом Федерации30 марта 2011 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует 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.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - 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;

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, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра 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 настоящим 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 или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом;

8) аккредитация удостоверяющего центра - признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего 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.

Статья 3. Правовое регулирование отношений в области использования электронных подписей

1. Отношения в области использования электронных подписей регулируются настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также соглашениями между участниками электронного взаимодействия. Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Виды электронных подписей, используемых органами исполнительной власти и органами местного самоуправления, порядок их использования, а также требования об обеспечении совместимости средств электронных подписей при организации электронного взаимодействия указанных органов между собой устанавливает Правительство Российской Федерации.

Статья 4. Принципы использования электронной подписи

Принципами использования электронной подписи являются:

1) право участников электронного взаимодействия использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

2) возможность использования участниками электронного взаимодействия по своему усмотрению любой информационной технологии и (или) технических средств, позволяющих выполнить требования настоящего Федерального закона применительно к использованию конкретных видов электронных подписей;

3) недопустимость признания электронной подписи и (или) подписанного ею электронного документа не имеющими юридической силы только на основании того, что такая электронная подпись создана не собственноручно, а с использованием средств электронной подписи для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Статья 5. Виды электронных подписей

1. Видами электронных подписей, отношения в области использования которых регулируются настоящим Федеральным законом, являются простая электронная подпись и усиленная электронная подпись. Различаются усиленная неквалифицированная электронная подпись (далее - неквалифицированная электронная подпись) и усиленная квалифицированная электронная подпись (далее - квалифицированная электронная подпись).

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

3. 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.

4. 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, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

5. При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом, может быть обеспечено без использования сертификата ключа проверки электронной подписи.

Статья 6. Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

1. Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе.

2. Информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям статьи 9 настоящего Федерального закона.

3. Если в соответствии с федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или обычаем делового оборота документ должен быть заверен печатью, электронный документ, подписанный усиленной электронной подписью и признаваемый равнозначным документу на бумажном носителе, подписанному

собственноручной подписью, признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью и заверенному печатью. Федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия могут быть предусмотрены дополнительные требования к электронному документу в целях признания его равнозначным документу на бумажном носителе, заверенному печатью.

4. Одной электронной подписью могут быть подписаны несколько связанных между собой электронных документов (пакет электронных документов). При подписании электронной подписью пакета электронных документов каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью того вида, которой подписан пакет электронных документов.

Статья 7. Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами

1. Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.

2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права.

Статья 8. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи

1. Уполномоченный федеральный орган определяется Правительством Российской Федерации.

2. Уполномоченный федеральный орган:

1) осуществляет аккредитацию удостоверяющих центров, проводит проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены настоящим Федеральным законом и на соответствие которым эти удостоверяющие центры были аккредитованы, и в случае выявления их несоблюдения выдает предписания об устранении выявленных нарушений;

2) осуществляет функции головного удостоверяющего центра в отношении аккредитованных удостоверяющих центров.

3. Уполномоченный федеральный орган обязан обеспечить хранение следующей указанной в настоящей части информации и круглосуточный беспрепятственный доступ к ней с использованием информационно-

телекоммуникационных сетей:

1) наименования, адреса аккредитованных удостоверяющих центров;

2) реестр выданных и аннулированных уполномоченным федеральным органом квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых аннулирована;

4) перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

6) реестры квалифицированных сертификатов, переданные в уполномоченный федеральный орган в соответствии со статьей 15 настоящего Федерального закона.

4. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, устанавливает:

1) порядок передачи реестров квалифицированных сертификатов и иной информации в уполномоченный федеральный орган в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) порядок формирования и ведения реестров квалифицированных сертификатов, а также предоставления информации из таких реестров;

3) правила аккредитации удостоверяющих центров, порядок проверки соблюдения аккредитованными удостоверяющими центрами требований, которые установлены настоящим Федеральным законом и на соответствие которым эти удостоверяющие центры были аккредитованы.

5. Федеральный орган исполнительной власти в области обеспечения безопасности:

1) устанавливает требования к форме квалифицированного сертификата;

2) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Федеральным законом, и публикует перечень таких средств.

Статья 9. Использование простой электронной подписи

1. Электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий:

1) простая электронная подпись содержится в самом электронном документе;

2) ключ простой электронной подписи применяется в соответствии с правилами, установленными оператором информационной системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ.

2. Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать, в частности:

1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;

2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

3. К отношениям, связанным с использованием простой электронной подписи, в том числе с созданием и использованием ключа простой электронной подписи, не применяются правила, установленные статьями 10 - 18 настоящего Федерального закона.

4. Использование простой электронной подписи для подписания электронных документов, содержащих сведения, составляющие государственную тайну, или в информационной системе, содержащей сведения, составляющие государственную тайну, не допускается.

Статья 10. Обязанности участников электронного взаимодействия при использовании усиленных электронных подписей

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны:

1) обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

2) уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

3) не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с

настоящим Федеральным законом.

Статья 11. Признание квалифицированной электронной подписи

Квалифицированная электронная подпись признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий:

1) квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата;

2) квалифицированный сертификат действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

3) имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом проверка осуществляется с использованием средств электронной подписи, получивших подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

4) квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

Статья 12. Средства электронной подписи

1. Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

2. При создании электронной подписи средства электронной подписи должны:

1) показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;

2) создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной

подписи;

3) однозначно показывать, что электронная подпись создана.

3. При проверке электронной подписи средства электронной подписи должны:

1) показывать содержание электронного документа, подписанного электронной подписью;

2) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

3) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

4. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих сведения, составляющие государственную тайну, или предназначенные для использования в информационной системе, содержащей сведения, составляющие государственную тайну, подлежат подтверждению соответствия обязательным требованиям по защите сведений соответствующей степени секретности в соответствии с законодательством Российской Федерации. Средства электронной подписи, предназначенные для создания электронных подписей в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

5. Требования частей 2 и 3 настоящей статьи не применяются к средствам электронной подписи, используемым для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе.

Статья 13. Удостоверяющий центр

1. Удостоверяющий центр:

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям);

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует выданные этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

5) ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или

аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

6) устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

10) осуществляет иную связанную с использованием электронной подписи деятельность.

2. Удостоверяющий центр обязан:

1) информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

2) обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

3) предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

4) обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

3. Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

1) неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг удостоверяющим центром;

2) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных настоящим Федеральным законом.

4. Удостоверяющий центр вправе наделить третьих лиц (далее - доверенные лица) полномочиями по созданию и выдаче сертификатов ключей проверки электронных подписей от имени удостоверяющего центра, подписываемых электронной подписью, основанной на сертификате ключа проверки электронной подписи, выданном доверенному лицу этим удостоверяющим

центром.

5. Удостоверяющий центр, указанный в части 4 настоящей статьи, по отношению к доверенным лицам является головным удостоверяющим центром и выполняет следующие функции:

1) осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных доверенными лицами сертификатах ключей проверки электронных подписей;

2) обеспечивает электронное взаимодействие доверенных лиц между собой, а также доверенных лиц с удостоверяющим центром.

6. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами. В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена. В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

7. Порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, определенных настоящей статьей, устанавливается удостоверяющим центром самостоятельно, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия.

8. Договор об оказании услуг удостоверяющим центром, осуществляющим свою деятельность в отношении неограниченного круга лиц с использованием информационной системы общего пользования, является публичным договором.

Статья 14. Сертификат ключа проверки электронной подписи

1. Удостоверяющий центр осуществляет создание и выдачу сертификата ключа проверки электронной подписи на основании соглашения между удостоверяющим центром и заявителем.

2. Сертификат ключа проверки электронной подписи должен содержать

следующую информацию:

1) даты начала и окончания срока его действия;

2) фамилия, имя и отчество (если имеется) - для физических лиц, наименование и место нахождения - для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

3) ключ проверки электронной подписи;

4) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

5) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи;

6) иная информация, предусмотренная частью 2 статьи 17 настоящего Федерального закона, - для квалифицированного сертификата.

3. В случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата ключа проверки электронной подписи наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в сертификате ключа проверки электронной подписи, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами. Владельцем такого сертификата ключа проверки электронной подписи признается юридическое лицо, информация о котором содержится в таком сертификате.

4. Удостоверяющий центр вправе выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе. Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную удостоверяющим центром.

5. Сертификат ключа проверки электронной подписи действует с момента его выдачи, если иная дата начала действия такого сертификата не указана в самом сертификате ключа проверки электронной подписи. Информация о сертификате ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

6. Сертификат ключа проверки электронной подписи прекращает свое действие:

1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

4) в иных случаях, установленных настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

7. Информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов в течение одного рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение действия сертификата ключа проверки электронной подписи. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

8. В течение не более чем одного рабочего дня удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи путем внесения записи о его аннулировании в реестр сертификатов по решению суда, вступившему в законную силу, в частности если решением суда установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

9. Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

Статья 15. Аккредитованный удостоверяющий центр

1. Удостоверяющий центр, получивший аккредитацию, является аккредитованным удостоверяющим центром. Аккредитованный удостоверяющий центр обязан хранить следующую информацию:

1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата

действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

2. Аккредитованный удостоверяющий центр должен хранить информацию, указанную в части 1 настоящей статьи, в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3. Аккредитованный удостоверяющий центр обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей к выданным этим удостоверяющим центром квалифицированным сертификатам и к актуальному списку аннулированных квалифицированных сертификатов в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

4. В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

2) передать в уполномоченный федеральный орган в установленном порядке реестр квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

Статья 16. Аккредитация удостоверяющего центра

1. Аккредитация удостоверяющих центров осуществляется уполномоченным федеральным органом в отношении удостоверяющих центров, являющихся российскими или иностранными юридическими лицами.

2. Аккредитация удостоверяющего центра осуществляется на добровольной основе. Аккредитация удостоверяющего центра осуществляется на срок пять лет, если более короткий срок не указан в заявлении удостоверяющего центра.

3. Аккредитация удостоверяющего центра осуществляется при условии выполнения им следующих требований:

1) стоимость чистых активов удостоверяющего центра составляет не менее чем один миллион рублей;

2) наличие финансового обеспечения ответственности за убытки, причиненные третьим лицам вследствие их доверия к информации, указанной в сертификате ключа проверки электронной подписи, выданном таким удостоверяющим центром, или информации, содержащейся в реестре сертификатов, который ведет такой удостоверяющий центр, в сумме не менее

чем полтора миллиона рублей;

3) наличие средств электронной подписи и средств удостоверяющего центра, получивших подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

4) наличие в штате удостоверяющего центра не менее двух работников, непосредственно осуществляющих деятельность по созданию и выдаче сертификатов ключей проверки электронных подписей, имеющих высшее профессиональное образование в области информационных технологий или информационной безопасности либо высшее или среднее профессиональное образование с последующим прохождением переподготовки или повышения квалификации по вопросам использования электронной подписи.

4. Аккредитация удостоверяющего центра осуществляется на основании его заявления, подаваемого в уполномоченный федеральный орган. К заявлению прилагаются документы, подтверждающие соответствие удостоверяющего центра требованиям, установленным частью 3 настоящей статьи. Удостоверяющий центр вправе не представлять документ, подтверждающий соответствие имеющихся у него средств электронной подписи и средств удостоверяющего центра требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, если такой документ или содержащиеся в нем сведения находятся в распоряжении федерального органа исполнительной власти в области обеспечения безопасности. В этом случае уполномоченный федеральный орган самостоятельно проверяет получение подтверждения соответствия таких средств установленным требованиям на основании информации, полученной от федерального органа исполнительной власти в области обеспечения безопасности.

5. В срок, не превышающий тридцати календарных дней со дня приема заявления удостоверяющего центра, уполномоченный федеральный орган на основании представленных документов принимает решение об аккредитации удостоверяющего центра или об отказе в его аккредитации. В случае принятия решения об аккредитации удостоверяющего центра уполномоченный федеральный орган в срок, не превышающий десяти дней со дня принятия решения об аккредитации, уведомляет удостоверяющий центр о принятом решении и выдает свидетельство об аккредитации по установленной форме. Одновременно с выдачей свидетельства об аккредитации уполномоченный федеральный орган выдает аккредитованному удостоверяющему центру квалифицированный сертификат, созданный с использованием средств головного удостоверяющего центра, функции которого осуществляет уполномоченный федеральный орган. В случае принятия решения об отказе в аккредитации удостоверяющего центра уполномоченный федеральный орган в срок, не превышающий десяти календарных дней со дня принятия решения об отказе в аккредитации, направляет или вручает удостоверяющему центру уведомление о принятом решении с указанием причин отказа в форме документа на бумажном носителе.

6. Основанием для отказа в аккредитации удостоверяющего центра является его несоответствие требованиям, установленным частью 3 настоящей статьи, или наличие в представленных им документах недостоверной информации.

7. Аккредитованный удостоверяющий центр должен соблюдать требования, на соответствие которым он аккредитован, в течение всего срока его аккредитации. В случае возникновения обстоятельств, делающих невозможным соблюдение указанных требований, удостоверяющий центр немедленно должен уведомить об этом в письменной форме уполномоченный федеральный орган. Аккредитованный удостоверяющий центр при осуществлении своих функций и исполнении принятых обязательств должен соблюдать требования, установленные для удостоверяющих центров статьями 13 - 15, 17 и 18 настоящего Федерального закона. Уполномоченный федеральный орган вправе проводить проверки соблюдения аккредитованными удостоверяющими центрами требований настоящего Федерального закона в течение всего срока их аккредитации. В случае выявления несоблюдения аккредитованным удостоверяющим центром указанных требований уполномоченный федеральный орган обязан выдать этому удостоверяющему центру предписание об устранении нарушений в установленный срок и приостановить действие аккредитации на данный срок с внесением информации об этом в перечень, указанный в пункте 4 части 3 статьи 8 настоящего Федерального закона. Аккредитованный удостоверяющий центр уведомляет в письменной форме уполномоченный федеральный орган об устранении выявленных нарушений. Уполномоченный федеральный орган принимает решение о возобновлении действия аккредитации, при этом он вправе проверять фактическое устранение ранее выявленных нарушений и в случае их неустранения в установленный предписанием срок аннулирует аккредитацию удостоверяющего центра.

8. На государственные органы, органы местного самоуправления, государственные и муниципальные учреждения, осуществляющие функции удостоверяющих центров, не распространяются требования, установленные пунктами 1 и 2 части 3 настоящей статьи.

9. Головной удостоверяющий центр, функции которого осуществляет уполномоченный федеральный орган, не подлежит аккредитации в соответствии с настоящим Федеральным законом.

Статья 17. Квалифицированный сертификат

1. Квалифицированный сертификат подлежит созданию с использованием средств аккредитованного удостоверяющего центра.

2. Квалифицированный сертификат должен содержать следующую информацию:

1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;

2) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата - для физического лица либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для юридического лица;

3) страховой номер индивидуального лицевого счета владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;

4) ключ проверки электронной подписи;

5) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;

6) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;

7) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);

8) иная информация о владельце квалифицированного сертификата (по требованию заявителя).

3. Если заявителем представлены в аккредитованный удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат может быть включена информация о таких правомочиях заявителя и сроке их действия.

4. Квалифицированный сертификат выдается в форме, требования к которой устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности.

5. В случае аннулирования квалифицированного сертификата, выданного аккредитованному удостоверяющему центру, выдавшему квалифицированный сертификат заявителю, либо в случае аннулирования или истечения срока аккредитации удостоверяющего центра квалифицированный сертификат, выданный аккредитованным удостоверяющим центром заявителю, прекращает свое действие.

6. Владелец квалифицированного сертификата обязан:

1) не использовать ключ электронной подписи и немедленно обратиться в аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

2) использовать квалифицированную электронную подпись в соответствии с ограничениями, содержащимися в квалифицированном сертификате (если такие ограничения установлены).

Статья 18. Выдача квалифицированного сертификата

1. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

1) установить личность заявителя - физического лица, обратившегося к нему

за получением квалифицированного сертификата;

2) получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

2. При обращении в аккредитованный удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются) и представляет следующие документы, подтверждающие достоверность информации, предоставленной заявителем для включения в квалифицированный сертификат, либо их надлежащим образом заверенные копии:

1) основной документ, удостоверяющий личность, страховое свидетельство государственного пенсионного страхования заявителя - физического лица или учредительные документы, документ, подтверждающий факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц, и свидетельство о постановке на учет в налоговом органе заявителя - юридического лица;

2) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства (для иностранных юридических лиц);

3) доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц.

3. При получении квалифицированного сертификата заявителем он должен быть под расписку ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате.

4. Аккредитованный удостоверяющий центр одновременно с выдачей квалифицированного сертификата должен выдать владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Статья 19. Заключительные положения

1. Сертификаты ключей подписей, выданные в соответствии с Федеральным законом от 10 января 2002 года N 1-ФЗ "Об электронной цифровой подписи", признаются квалифицированными сертификатами в соответствии с настоящим Федеральным законом.

2. Электронный документ, подписанный электронной цифровой подписью до даты признания утратившим силу Федерального закона от 10 января 2002 года N 1-ФЗ "Об электронной цифровой подписи", признается электронным документом, подписанным квалифицированной электронной подписью в соответствии с настоящим Федеральным законом.

Статья 20. Вступление в силу настоящего Федерального закона

1. Настоящий Федеральный закон вступает в силу со дня его официального опубликования.

2. Федеральный закон от 10 января 2002 года N 1-ФЗ "Об электронной цифровой подписи" (Собрание законодательства Российской Федерации, 2002, N 2, ст. 127) признать утратившим силу с 1 июля 2012 года.

Президент Российской Федерации Д.МЕДВЕДЕВ

Москва, Кремль, 6 апреля 2011 года, N 63-ФЗ