06.04.2011 № 63-ФЗ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ЭЛЕКТРОННОЙ ПОДПИСИ

Принят
Государственной Думой
25 марта 2011 года

Одобрен
Советом Федерации
30 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, в том числе в случаях, установленных другими федеральными законами.

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, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним

нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее — уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

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, 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 настоящим Федеральным законом;

8) аккредитация удостоверяющего центра — признание соответствия удостоверяющего центра требованиям настоящего Федерального закона;

8.1) аккредитация доверенной третьей стороны — признание уполномоченным федеральным органом соответствия юридического лица требованиям настоящего Федерального закона к доверенной третьей стороне;

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, индивидуальные предприниматели, 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, созданного 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;

16) заявитель — коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее — нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата;

17) доверенная третья сторона — юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные настоящим Федеральным законом;

18) средства доверенной третьей стороны — программные и (или) аппаратные средства, используемые для оказания услуг доверенной третьей стороной, прошедшие процедуру подтверждения соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

19) метка доверенного времени — достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая и проверяемая доверенной третьей стороной, удостоверяющим центром или оператором информационной системы и полученная в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

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, имеющие 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, и может применяться в любых правоотношениях в соответствии с законодательством Российской Федерации, 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, нормативными актами Центрального банка Российской Федерации (далее — нормативные правовые акты) или соглашением между участниками электронного взаимодействия, в том числе правилами платежных систем (далее — соглашения 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.

3.1. Если федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами предусмотрено, что документ должен подписываться несколькими лицами, электронный документ должен быть подписан лицами (уполномоченными должностными лицами органа, организации), изготовившими этот документ, тем видом подписи, который установлен законодательством Российской Федерации для подписания изготовленного электронного документа электронной подписью.

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. Исключение составляют случаи, когда в состав пакета электронных документов лицом, подписавшим пакет, включены электронные документы,

созданные иными лицами (органами, организациями) и подписанные ими тем видом электронной подписи, который установлен законодательством Российской Федерации для подписания таких документов. В этих случаях электронный документ, входящий в пакет, считается подписанным лицом, первоначально создавшим такой электронный документ, тем видом электронной подписи, которым этот документ был подписан при создании, вне зависимости от того, каким видом электронной подписи 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, с учетом части 3 настоящей статьи.

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.

3. Признание электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами, соответствующими признакам усиленной электронной подписи, и их применение в правоотношениях в соответствии с законодательством Российской Федерации осуществляются в случаях, установленных международными договорами Российской Федерации. Такие электронные подписи признаются действительными в случае подтверждения соответствия их требованиям указанных международных договоров аккредитованной доверенной третьей стороной, аккредитованным удостоверяющим центром, иным лицом, уполномоченными на это международным договором Российской Федерации, с учетом настоящего Федерального закона.

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, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы,

и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений;

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

3) осуществляет аккредитацию доверенных третьих сторон, проводит проверки соблюдения доверенными третьими сторонами требований, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в порядке, установленном уполномоченным федеральным органом, и в случае выявления несоблюдения этих требований выдает предписания об устранении выявленных нарушений.

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;

1.1) наименования, адреса аккредитованных доверенных третьих сторон;

2) реестр выданных уполномоченным федеральным органом квалифицированных сертификатов;

3) перечень удостоверяющих центров, аккредитация которых досрочно прекращена;

4) перечень аккредитованных удостоверяющих центров, аккредитация которых приостановлена;

5) перечень аккредитованных удостоверяющих центров, деятельность которых прекращена;

5.1) перечень доверенных третьих сторон, аккредитация которых досрочно прекращена;

5.2) перечень аккредитованных доверенных третьих сторон, аккредитация которых приостановлена;

5.3) перечень аккредитованных доверенных третьих сторон, деятельность которых прекращена;

6) реестры выданных аккредитованными удостоверяющими центрами 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 выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов и иной информации в уполномоченный федеральный орган в случае прекращения деятельности аккредитованного удостоверяющего центра;

2) порядок формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов, а также предоставления информации из таких реестров, включая требования к формату предоставления такой информации;

3) правила аккредитации удостоверяющих центров, доверенных третьих сторон, порядок проверки соблюдения аккредитованными удостоверяющими центрами, аккредитованными доверенными третьими сторонами требований, которые установлены настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, в том числе требований, на соответствие которым эти удостоверяющие центры, доверенные третьи стороны были аккредитованы;

4) требования к порядку реализации функций аккредитованного удостоверяющего центра, аккредитованной доверенной третьей стороны и исполнения их обязанностей, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности;

5) формат электронной подписи, обязательный для реализации всеми средствами электронной подписи, по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности;

6) требования к порядку действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи, а также при приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях;

7) по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности перечень угроз безопасности, актуальных при идентификации заявителя — физического лица в аккредитованном удостоверяющем центре, выдаче квалифицированного сертификата без его личного присутствия с применением информационных технологий путем предоставления сведений из единой системы идентификации и аутентификации и единой информационной системы персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным

биометрическим персональным данным гражданина Российской Федерации (далее — единая биометрическая система), а также хранении и использовании ключа электронной подписи в аккредитованном удостоверяющем центре.

5. Федеральный орган исполнительной власти в области обеспечения безопасности:

1) по согласованию с уполномоченным федеральным органом устанавливает требования к форме квалифицированного сертификата и правила подтверждения владения ключом электронной подписи;

2) устанавливает требования к средствам электронной подписи, средствам удостоверяющего центра, за исключением указанных в пункте 2.1 настоящей части, и средствам доверенной третьей стороны, включая требования к используемым доверенной третьей стороной средствам электронной подписи;

2.1) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра, применяемым для реализации функций, предусмотренных частью 2.2 статьи 15 настоящего Федерального закона, включающие в себя в том числе требования по:

а) хранению ключей квалифицированной электронной подписи и автоматическому созданию такой подписи с их использованием по поручению соответствующих владельцев квалифицированных сертификатов;

б) аутентификации владельцев квалифицированных сертификатов, по поручению которых аккредитованный удостоверяющий центр создает и проверяет квалифицированную электронную подпись;

в) защите информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и аккредитованным удостоверяющим центром, осуществляющим создание и проверку квалифицированной электронной подписи по поручению такого владельца;

г) доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной электронной подписи;

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

4) осуществляет подтверждение соответствия средств доверенной третьей стороны 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

1. 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, имеющие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

2. Участники электронного взаимодействия не вправе устанавливать иные, за исключением предусмотренных настоящим Федеральным законом, ограничения признания усиленной квалифицированной электронной подписи. Нарушение запрета на ограничение или отказ от признания электронных документов, подписанных квалифицированной электронной подписью, соответствующей предъявляемым к ней требованиям, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, а также нарушение запрета операторами государственных и муниципальных информационных систем, информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования на предъявление требований о наличии в квалифицированном сертификате информации, не являющейся обязательной в соответствии с настоящим Федеральным законом и принимаемыми в соответствии с ним нормативными правовыми актами, по любым причинам, кроме предусмотренных настоящим Федеральным законом, не допускается.

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, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом, и с использованием квалифицированного сертификата лица, подписавшего электронный документ;

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;

3) позволяют создать электронную подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

2. При создании электронной подписи средства электронной подписи должны:

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

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 самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью, включая визуализацию данной электронной подписи, содержащую информацию о том, что такой документ подписан электронной подписью, а также о номере, владельце и периоде действия сертификата ключа проверки электронной подписи;

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), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 настоящего Федерального закона;

1.1) осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

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 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;

5) отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

6) отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;

7) незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением сторон, или возникновения у аккредитованного удостоверяющего

центра обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи (при осуществлении аккредитованным удостоверяющим центром деятельности, предусмотренной частью 2.2 статьи 15 настоящего Федерального закона).

2.1. Удостоверяющему центру запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

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 приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра. При совершении порученных удостоверяющим центром действий доверенное лицо обязано идентифицировать заявителя при его личном присутствии.

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 настоящим Федеральным законом и иными 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) уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;

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) уникальный 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 (в том числе в квалифицированном сертификате), 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. При этом распорядительным актом юридического лица определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи 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. В случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи 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, является руководитель юридического лица. В случае возложения федеральным законом полномочий по исполнению государственных функций на конкретное должностное лицо ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при исполнении государственных функций является это должностное лицо.

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.

6.1. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

1) не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

3) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

7. Информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 настоящей статьи, или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

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. Аккредитованными удостоверяющими центрами являются удостоверяющие центры, получившие аккредитацию, а также удостоверяющий центр федерального органа исполнительной власти, уполномоченного

на осуществление государственной регистрации юридических лиц, удостоверяющий центр федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, и удостоверяющий центр Центрального банка Российской Федерации. Данные удостоверяющие центры обязаны 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 от имени юридических лиц, государственных органов, органов местного самоуправления, 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.

2.1. Аккредитованный удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. Аккредитованному удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.

2.2. Удостоверяющий центр, аккредитованный в соответствии с требованиями части 3.1 статьи 16 настоящего Федерального закона, а также удостоверяющий центр федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, удостоверяющий центр федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, и удостоверяющий центр Центрального банка Российской Федерации по поручению владельца квалифицированного сертификата вправе осуществлять:

1) хранение ключа электронной подписи, ключ проверки которой содержится в квалифицированном сертификате с обеспечением его защиты от компрометации и (или) несанкционированного использования, в том числе создание при помощи указанного ключа подписи по поручению владельца квалифицированного сертификата с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с пунктом 2.1 части 5 статьи 8 настоящего Федерального закона;

2) информирование владельца квалифицированного сертификата об использовании указанного ключа электронной подписи и предоставление по требованию владельца квалифицированного сертификата истории использования указанного ключа электронной подписи.

2.3. Требования к форме указанного в пункте 1 части 2.2 настоящей статьи поручения владельца квалифицированного сертификата, порядку передачи поручения владельца квалифицированного сертификата аккредитованному удостоверяющему центру, в том числе с учетом возможности осуществления процедуры дополнительной аутентификации владельца квалифицированного сертификата путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы, а также к правилам хранения указанного поручения устанавливаются уполномоченным федеральным органом по согласованию с федеральным органом исполнительной власти в области обеспечения безопасности.

3. Аккредитованный удостоверяющий центр обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов этого аккредитованного удостоверяющего центра 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 выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре. Ключи электронной подписи, хранимые аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи, подлежат уничтожению

в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности.

5. Аккредитованный удостоверяющий центр обязан выполнять порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленный таким аккредитованным удостоверяющим центром в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с настоящим Федеральным законом и иными нормативными правовыми актами, принимаемыми в соответствии с настоящим Федеральным законом.

6. Аккредитованный удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени такого аккредитованного удостоверяющего центра.

6.1. Удостоверяющий центр федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, вправе наделить доверенных лиц полномочиями на прием заявлений о получении квалифицированного сертификата юридического лица и выполнение требований статьи 18 настоящего Федерального закона от имени удостоверяющего центра федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, на создание ключа электронной подписи (при условии исключения возможности доступа работников таких доверенных лиц к ключам электронных подписей заявителей), а также на хранение ключей квалифицированных электронных подписей для дистанционного использования и на создание при помощи указанных ключей электронных подписей для электронных документов. При вручении созданного удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, квалифицированного сертификата указанное доверенное лицо обязано установить личность владельца сертификата (заявителя) в соответствии с порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленным федеральным органом исполнительной власти, уполномоченным на осуществление государственной регистрации юридических лиц, с учетом требований, предусмотренных пунктом 4 части 4 статьи 8 настоящего Федерального закона. Доверенные лица, указанные в настоящей части, в установленном Правительством Российской Федерации порядке определяются федеральным органом исполнительной власти, уполномоченным на осуществление государственной регистрации юридических лиц, из числа удостоверяющих центров, получивших аккредитацию в соответствии с частями 3 и 3.1 статьи 16 настоящего Федерального закона, при условии их соответствия дополнительным требованиям, установленным Правительством Российской Федерации, и организационно—техническим требованиям в области информационной безопасности, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

6.2. Аккредитованные удостоверяющие центры, являющиеся удостоверяющим центром федерального органа исполнительной власти, уполномоченного на осуществление государственной регистрации юридических лиц, удостоверяющим центром федерального органа исполнительной власти, уполномоченного на правоприменительные функции по обеспечению исполнения федерального бюджета, казначейскому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации, и удостоверяющим центром Центрального банка Российской Федерации, должны соответствовать требованиям, предусмотренным пунктами 1.1, 3 — 5, 7 части 3, пунктом 2 части 3.1 статьи 16 настоящего Федерального закона. Уполномоченный федеральный орган совместно с федеральным органом исполнительной власти в области обеспечения безопасности в порядке, установленном статьей 16.1 настоящего Федерального закона, осуществляет проверки соблюдения аккредитованными удостоверяющими центрами, указанными в настоящей части, требований, предусмотренных настоящим Федеральным законом. В рамках проведения таких проверок не могут быть осуществлены приостановка, прекращение аккредитации таких удостоверяющих центров.

7. Аккредитованный удостоверяющий центр (работник аккредитованного удостоверяющего центра, доверенные лица и их работники) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

8. Аккредитованный удостоверяющий центр на безвозмездной основе обеспечивает физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», для проведения идентификации физических лиц в аккредитованном удостоверяющем центре на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети «Интернет».

Статья 16. Аккредитация удостоверяющего центра

1. Аккредитация удостоверяющих центров осуществляется в два этапа в отношении удостоверяющих центров, являющихся юридическими лицами.

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

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

1) минимальный размер собственных средств (капитала) составляет не менее чем один миллиард рублей либо пятьсот миллионов рублей при наличии не менее чем в трех четвертях субъектов Российской Федерации одного или более филиала или представительства удостоверяющего центра;

1.1) наличие лицензии на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица);

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 100 миллионов рублей и 500 тысяч рублей за каждое место осуществления лицензируемого вида деятельности, указанное в лицензии федерального органа исполнительной власти в области обеспечения безопасности, выданной удостоверяющему центру в соответствии с пунктом 1 части 1 статьи 12 Федерального закона от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности», если количество таких мест превышает десять, но не более 200 миллионов рублей. Если количество мест осуществления указанного лицензируемого вида деятельности не превышает десять, финансовое обеспечение ответственности составляет 100 миллионов рублей;

3) наличие права собственности на аппаратные средства электронной подписи и средства удостоверяющего центра, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, и наличие права использования программных средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, на законных основаниях;

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

4.1) соответствие требованиям к деловой репутации руководителя и учредителей (участников) удостоверяющего центра, имеющих право прямо или косвенно либо совместно с иными лицами, связанными с ними договорами доверительного управления имуществом, и (или) простого товарищества, и (или) поручения, и (или) корпоративным договором, и (или) иным соглашением, предметом которого является осуществление прав, удостоверенных акциями (долями), распоряжаться более 10 процентами акций (долей), составляющих уставный капитал удостоверяющего центра, установленным правительственной комиссией, указанной в части 5.1 настоящей статьи;

5) наличие у удостоверяющего центра, претендующего на получение аккредитации, порядка реализации функций удостоверяющего центра и исполнения его обязанностей, установленного удостоверяющим центром в соответствии с утвержденными федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, а также с настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами;

6) в отношении удостоверяющего центра, претендующего на получение аккредитации, не была досрочно прекращена его аккредитация в течение трех лет до подачи заявления;

7) лицо, имеющее право в соответствии с законодательством Российской Федерации действовать от имени удостоверяющего центра без доверенности, не является лицом, имевшим право в соответствии с законодательством Российской Федерации действовать без доверенности от имени удостоверяющего центра, аккредитация которого была досрочно прекращена, в течение трех лет до подачи заявления.

3.1. Для осуществления хранения ключа электронной подписи в соответствии с частью 2.2 статьи 15 настоящего Федерального закона аккредитация удостоверяющего центра осуществляется при условии выполнения им следующих дополнительных требований:

1) наличие финансового обеспечения ответственности за убытки, причиненные в случае компрометации и (или) несанкционированного использования ключей электронной подписи, хранение которых осуществляет аккредитованный удостоверяющий центр по поручению их владельцев, за исключением случаев наличия вины владельца квалифицированного сертификата, в сумме не менее 200 миллионов рублей, а также 500 тысяч рублей за каждое место осуществления лицензируемого вида деятельности, непосредственно связанного с созданием сертификатов ключей проверки электронной подписи, указанное в лицензии федерального органа исполнительной власти в области обеспечения безопасности, выданной удостоверяющему центру в соответствии с пунктом 1 части 1 статьи 12 Федерального закона от 4 мая 2011 года № 99-ФЗ «О лицензировании отдельных

видов деятельности», если количество таких мест превышает десять, но не более 300 миллионов рублей. Если количество мест осуществления указанного лицензируемого вида деятельности не превышает десять, финансовое обеспечение ответственности составляет 200 миллионов рублей;

2) наличие в собственности удостоверяющего центра и применение им средств, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, которые обеспечивают:

а) хранение ключей квалифицированных электронных подписей и автоматическое создание таких подписей с использованием данных ключей по поручению соответствующих владельцев квалифицированных сертификатов;

б) аутентификацию владельцев квалифицированных сертификатов, по поручению которых аккредитованный удостоверяющий центр создает и проверяет квалифицированную электронную подпись;

в) защиту информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и аккредитованным удостоверяющим центром, осуществляющим создание и проверку квалифицированной электронной подписи по поручению такого владельца;

г) доказательства невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной 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 наличие документа, подтверждающего соответствие таких средств установленным требованиям, на основании информации, полученной от федерального органа исполнительной власти в области обеспечения безопасности, с использованием единой системы межведомственного электронного взаимодействия.

4.1. К заявлению для аккредитации удостоверяющего центра в целях осуществления хранения ключей электронных подписей в соответствии с частью 2.2 статьи 15 настоящего Федерального закона прилагаются документы, подтверждающие соответствие удостоверяющего центра требованиям, установленным частью 3.1 настоящей статьи. При направлении заявления аккредитация удостоверяющего центра может осуществляться как на соответствие только требованиям, установленным частью 3.1 настоящей статьи (при условии наличия действующей аккредитации на соответствие части

3 настоящей статьи), так и на соответствие требованиям частей 3 и 3.1 настоящей статьи одновременно.

5. В срок, не превышающий тридцати календарных дней со дня приема заявления удостоверяющего центра, уполномоченный федеральный орган на основании представленных документов принимает решение о соответствии удостоверяющего центра требованиям, установленным пунктами 1—4, 5—7 части 3 и (или) частью 3.1 настоящей статьи, или об отказе в его аккредитации.

5.1. В случае принятия решения о соответствии удостоверяющего центра требованиям, установленным пунктами 1 — 4, 5 — 7 части 3 и (или) частью 3.1 настоящей статьи, уполномоченный федеральный орган в срок, не превышающий десяти календарных дней со дня принятия решения, предусмотренного частью 5 настоящей статьи, направляет соответствующее заключение в правительственную комиссию, уполномоченную на принятие решения об аккредитации удостоверяющих центров (далее — правительственная комиссия). Положение о правительственной комиссии, ее состав и порядок принятия ею решений утверждаются Правительством Российской Федерации. При утверждении состава правительственной комиссии должно быть предусмотрено, что не менее 30 процентов членов правительственной комиссии должны быть представителями автономной некоммерческой организации, на которую в соответствии с решением Правительства Российской Федерации возложены функции по мониторингу развития цифровой экономики и цифровых технологий и формированию прогнозов развития цифровой экономики и цифровых технологий. При утверждении порядка деятельности правительственной комиссии к ее компетенции должно быть отнесено в том числе принятие на основе заключений уполномоченного федерального органа решений об аккредитации удостоверяющих центров, у которых руководители и учредители (участники) имеют право прямо или косвенно либо совместно с иными лицами, связанными с ними договорами доверительного управления имуществом, и (или) простого товарищества, и (или) поручения, и (или) корпоративным договором, и (или) иным соглашением, предметом которого является осуществление прав, удостоверенных акциями (долями), распоряжаться более 10 процентами акций (долей), составляющих уставный капитал данных удостоверяющих центров, и соответствуют высоким требованиям к деловой репутации.

5.2. Правительственная комиссия рассматривает представленные документы и в течение двадцати рабочих дней принимает решение об аккредитации удостоверяющего центра (в случае его соответствия пункту 4.1 части 3 настоящей статьи) или отказе в аккредитации.

5.3. В случае принятия решения об аккредитации удостоверяющего центра уполномоченный федеральный орган в срок, не превышающий пяти календарных дней со дня принятия решения об аккредитации, направляет уведомление удостоверяющему центру о принятом решении и вносит соответствующую информацию в перечень аккредитованных удостоверяющих центров, после чего удостоверяющий центр считается аккредитованным удостоверяющим центром. Аккредитованный удостоверяющий центр обязан осуществить присоединение

информационной системы, обеспечивающей реализацию функций аккредитованного удостоверяющего центра (далее — присоединение аккредитованного удостоверяющего центра), к информационно-технологической и коммуникационной инфраструктуре в порядке, установленном в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее — инфраструктура). После присоединения аккредитованного удостоверяющего центра к инфраструктуре уполномоченный федеральный орган выдает аккредитованному удостоверяющему центру квалифицированный сертификат, созданный с использованием средств головного удостоверяющего центра. 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 в удостоверяющий центр уведомление о принятом решении с указанием причин отказа.

6. Основаниями для отказа в аккредитации удостоверяющего центра являются его несоответствие требованиям, установленным частями 3 и (или) 3.1 настоящей статьи, несоответствие иным требованиям настоящего Федерального закона, а также наличие в представленных им документах недостоверной информации. При этом отказ в аккредитации удостоверяющего центра на соответствие требованиям части 3.1 настоящей статьи не приостанавливает действие аккредитации удостоверяющего центра на соответствие требованиям части 3 настоящей статьи.

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 и иных принимаемых в соответствии с настоящим Федеральным законом нормативных правовых актов, в том числе требований, на соответствие которым эти удостоверяющие центры были аккредитованы, в течение всего срока их аккредитации. В случае выявления несоблюдения аккредитованным удостоверяющим центром указанных требований должностное лицо уполномоченного федерального органа обязано 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 досрочно прекращает аккредитацию удостоверяющего центра, а в случае, если удостоверяющий центр аккредитован в соответствии с требованиями частей 3 и 3.1 настоящей статьи, его аккредитации прекращаются одновременно.

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

Статья 16.1. Федеральный государственный надзор в сфере электронной подписи

1. Федеральный государственный надзор в сфере электронной подписи осуществляется уполномоченным федеральным органом.

2. Предметом федерального государственного надзора в сфере электронной подписи является соблюдение аккредитованными удостоверяющими центрами, доверенными третьими сторонами требований настоящего Федерального закона и иных принимаемых в соответствии с ним нормативных правовых актов.

3. Федеральный государственный надзор в сфере электронной подписи осуществляется в соответствии с требованиями Федерального закона от 26 декабря 2008 года № 294—ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» с учетом особенностей организации и проведения проверок, установленных настоящей статьей.

4. Плановые проверки аккредитованных удостоверяющих центров, доверенных третьих сторон при осуществлении федерального государственного надзора в сфере электронной подписи не проводятся.

5. Внеплановые проверки аккредитованных удостоверяющих центров, доверенных третьих сторон проводятся по основаниям, указанным в части 2 статьи 10 Федерального закона от 26 декабря 2008 года № 294—ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», а также на основании мотивированного представления должностного лица уполномоченного федерального органа по результатам анализа результатов мероприятий по контролю без взаимодействия с аккредитованными удостоверяющими центрами, доверенными третьими сторонами, рассмотрения или предварительной проверки обращений о нарушениях требований настоящего Федерального закона и иных принимаемых в соответствии с ним нормативных правовых актов, допущенных аккредитованными удостоверяющими центрами, доверенными третьими сторонами, которые поступили в уполномоченный федеральный орган от федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, иных государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, органов государственных внебюджетных фондов, юридических и физических лиц.

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, отчество (если имеется) владельца квалифицированного сертификата — для физического лица, не являющегося индивидуальным предпринимателем, либо фамилия, имя, отчество (если имеется) и основной государственный регистрационный номер индивидуального предпринимателя владельца квалифицированного сертификата — для физического лица, являющегося индивидуальным предпринимателем, либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата — для российского юридического лица, либо наименование, место нахождения владельца квалифицированного сертификата, а также идентификационный номер налогоплательщика (при наличии) — для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);

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

4) уникальный 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) идентификатор, однозначно указывающий на то, что идентификация заявителя при выдаче сертификата ключа проверки электронной подписи проводилась либо при его личном присутствии, либо без его личного присутствия одним из способов, указанных в абзаце первом пункта 1 части 1 статьи 18 настоящего Федерального закона.

2.1. Операторы государственных и муниципальных информационных систем, а также информационных систем, использование которых предусмотрено

нормативными правовыми актами, или информационных систем общего пользования не вправе требовать наличие в квалифицированном сертификате информации, не являющейся обязательной в соответствии с настоящим Федеральным законом и принимаемыми в соответствии с ним иными нормативными правовыми актами.

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 по согласованию с уполномоченным федеральным органом.

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

6. Владелец квалифицированного сертификата обязан 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.

Статья 18. Выдача квалифицированного сертификата

1. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

1) в порядке, установленном настоящим Федеральным законом, идентифицировать заявителя — физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя — гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом

от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации. Устанавливаются:

а) в отношении физического лица — фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

б) в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, — наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица;

в) для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, — наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано;

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

3) в установленном порядке идентифицировать заявителя — физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата). Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя — гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149—ФЗ «Об информации, информационных технологиях и о защите информации»;

4) предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети «Интернет»), и указать страницу сайта в информационно-телекоммуникационной сети «Интернет», с которой безвозмездно предоставляются эти средства. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

1.1. Подтверждение достоверности сведений, перечисленных в пунктах 1 и 2 части 1 настоящей статьи, осуществляется одним из следующих способов:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием единой системы идентификации и аутентификации.

2. При обращении в аккредитованный удостоверяющий центр заявитель представляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) основной документ, удостоверяющий личность;

2) страховой номер индивидуального лицевого счета заявителя — физического лица;

3) идентификационный номер налогоплательщика заявителя — физического лица;

4) основной государственный регистрационный номер заявителя — юридического лица;

5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя — индивидуального предпринимателя;

6) номер свидетельства о постановке на учет в налоговом органе заявителя — иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя — иностранной организации;

7) документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени государственного органа или органа местного самоуправления.

2.1. Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 2 — 6 части 2 настоящей статьи.

2.2. Аккредитованный удостоверяющий центр должен с использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 настоящей статьи. Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 настоящего Федерального закона аккредитованный удостоверяющий центр запрашивает и получает из государственных информационных ресурсов:

1) выписку из единого государственного реестра юридических лиц в отношении заявителя — юридического лица;

2) выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя — индивидуального предпринимателя;

3) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя — иностранной организации.

2.3. В случае, если полученные в соответствии с частью 2.2 настоящей статьи сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и аккредитованным удостоверяющим центром идентифицирован заявитель, аккредитованный удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае, а также в случаях, установленных пунктами 5 и 6 части 2 статьи 13 настоящего Федерального закона, аккредитованный удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

3. При получении квалифицированного сертификата заявителем он должен быть ознакомлен аккредитованным удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя — физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной

подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

3.1. Квалифицированный сертификат выдается аккредитованным удостоверяющим центром на безвозмездной основе или за установленную удостоверяющим центром плату при условии, что размер такой платы не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

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

5. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

Статья 18.1. Доверенная третья сторона

1. Доверенная третья сторона оказывает услуги:

1) по подтверждению действительности электронных подписей, используемых при подписании электронного документа, в том числе установлению фактов того, что соответствующие сертификаты действительны на определенный момент времени, созданы и выданы аккредитованными удостоверяющими центрами, аккредитация которых действительна на день выдачи этих сертификатов;

2) по проверке соответствия всех квалифицированных сертификатов, используемых при подписании электронного документа, требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами;

3) по проверке полномочий участников электронного взаимодействия;

4) по созданию и подписанию квалифицированной электронной подписью доверенной третьей стороны квитанции с результатом проверки квалифицированной электронной подписи в электронном документе с достоверной информацией о моменте ее подписания;

5) по хранению данных, в том числе документированию выполняемых доверенной третьей стороной операций.

2. Доверенная третья сторона обеспечивает конфиденциальность, целостность и доступность информации при ее обработке и хранении, а также при ее передаче с использованием информационно-телекоммуникационных технологий.

3. Доверенная третья сторона несет гражданско-правовую и (или) административную ответственность в соответствии с международными договорами Российской Федерации, законодательством Российской Федерации за неисполнение обязанностей, установленных настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также за нарушение порядка реализации функций доверенной третьей стороны и исполнения ее обязанностей.

4. Информационные системы доверенной третьей стороны, предназначенные для реализации услуг доверенной третьей стороны, присоединяются к информационно-технологической и коммуникационной инфраструктуре в порядке, установленном в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Статья 18.2. Аккредитация доверенной третьей стороны

1. Аккредитация доверенной третьей стороны осуществляется на добровольной основе на срок три года, если более короткий срок не указан в заявлении доверенной третьей стороны.

2. Аккредитация доверенной третьей стороны осуществляется при условии выполнения следующих требований:

1) в отношении юридического лица, предполагающего оказывать услуги доверенной третьей стороны, не проводится процедура ликвидации, отсутствует решение (определение) арбитражного суда о введении процедуры банкротства в соответствии с законодательством Российской Федерации о банкротстве, отсутствуют сведения в реестрах недобросовестных поставщиков, ведение которых осуществляется в соответствии с законодательством Российской Федерации;

2) минимальный размер собственных средств (капитала) составляет не менее чем один миллиард рублей либо 500 миллионов рублей при наличии не менее чем в трех четвертях субъектов Российской Федерации одного или более филиала, или представительства доверенной третьей стороны;

3) наличие финансового обеспечения гражданской ответственности юридического лица, предполагающего оказывать услуги доверенной третьей стороны, за ущерб, причиненный третьим лицам вследствие оказания таких услуг ненадлежащего качества, размер которого определяется Правительством Российской Федерации;

4) наличие у юридического лица, предполагающего оказывать услуги доверенной третьей стороны, средств доверенной третьей стороны и средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности в соответствии с пунктом 2 части 5 статьи 8 настоящего Федерального закона;

5) доверенная третья сторона, претендующая на получение аккредитации, не была включена в перечень, предусмотренный пунктом 5.1 части 3 статьи 8 настоящего Федерального закона, в течение трех лет до подачи заявления;

6) лицо, имеющее право в соответствии с законодательством Российской Федерации действовать от имени доверенной третьей стороны без доверенности, не является лицом, имевшим право действовать без доверенности от имени доверенной третьей стороны или удостоверяющего центра, аккредитация которых была досрочно прекращена, в течение трех лет до подачи заявления.

3. Аккредитация доверенной третьей стороны осуществляется на основании заявления, подаваемого в уполномоченный федеральный орган. К заявлению прилагаются документы, подтверждающие соответствие доверенной третьей стороны требованиям, установленным частью 2 настоящей статьи. Доверенная третья сторона вправе не представлять документ, подтверждающий соответствие имеющихся у нее средств электронной подписи и средств доверенной третьей стороны 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 наличие документа, подтверждающего соответствие таких средств установленным требованиям, на основании информации, полученной от федерального органа исполнительной власти в области обеспечения безопасности, с использованием единой системы межведомственного электронного взаимодействия.

4. В срок, не превышающий тридцати календарных дней со дня приема заявления доверенной третьей стороны, уполномоченный федеральный орган на основании представленных документов принимает решение об аккредитации доверенной третьей стороны или об отказе в ее аккредитации.

5. В случае принятия решения об отказе в аккредитации доверенной третьей

стороны уполномоченный федеральный орган в срок, не превышающий десяти календарных дней со дня принятия решения об отказе в аккредитации, направляет доверенной третьей стороне уведомление о принятом решении с указанием причин отказа.

6. В случае принятия решения об аккредитации доверенной третьей стороны уполномоченный федеральный орган в срок, не превышающий десяти календарных дней со дня принятия решения об аккредитации, направляет уведомление доверенной третьей стороне о принятом решении и вносит информацию в перечень аккредитованных доверенных третьих сторон. После получения аккредитации аккредитованная доверенная третья сторона обязана осуществить присоединение информационной системы, обеспечивающей реализацию функций аккредитованной доверенной третьей стороны (далее — присоединение аккредитованной доверенной третьей стороны), к инфраструктуре.

7. Основаниями для отказа в аккредитации доверенной третьей стороны являются ее несоответствие требованиям, установленным частью 2 настоящей статьи, несоответствие иным требованиям настоящего Федерального закона, а также наличие в представленных ею документах недостоверной информации.

8. Аккредитованная доверенная третья сторона должна соблюдать требования, на соответствие которым она аккредитована, и требования, установленные статьей 18.1 настоящего Федерального закона, в течение всего срока ее аккредитации. В случае возникновения обстоятельств, делающих невозможным соблюдение указанных требований, аккредитованная доверенная третья сторона немедленно должна уведомить об этом в письменной форме уполномоченный федеральный орган. Уполномоченный федеральный орган вправе проводить проверки соблюдения аккредитованными доверенными третьими сторонами требований настоящего Федерального закона и иных принимаемых в соответствии с настоящим Федеральным законом нормативных правовых актов, в том числе требований, на соответствие которым эти доверенные третьи стороны были аккредитованы, в течение всего срока их аккредитации. В случае выявления по итогам внеплановых проверок несоблюдения аккредитованной доверенной третьей стороной указанных требований уполномоченный федеральный орган обязан выдать этой доверенной третьей стороне предписание об устранении нарушений в установленный срок и приостановить действие аккредитации на данный срок с внесением информации об этом в соответствующий перечень. Аккредитованная доверенная третья сторона 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 досрочно прекращает аккредитацию доверенной третьей стороны.

Статья 19. Заключительные положения

1. Сертификаты ключей подписей, выданные в соответствии с Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи», признаются квалифицированными сертификатами в соответствии с настоящим Федеральным законом.

2. Электронный документ, подписанный электронной подписью, ключ проверки которой содержится в сертификате ключа проверки электронной подписи, выданном в соответствии с порядком, ранее установленным Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи», в течение срока действия указанного сертификата, но не позднее 31 декабря 2013 года признается электронным документом, подписанным квалифицированной электронной подписью в соответствии с настоящим Федеральным законом.

3. В случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись 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 № 1—ФЗ «Об электронной цифровой подписи» (Собрание законодательства Российской Федерации, 2002, № 2, ст. 127) признать утратившим силу с 1 июля 2013 года.

Президент
Российской Федерации
Д.МЕДВЕДЕВ

Москва, Кремль

6 апреля 2011 года

№ 63-ФЗ