АО «Интерфакс»

Регламент применения электронной подписи в Едином федеральном реестре сведений о фактах деятельности юридических лиц (версия 1.3 от 16 мая 2018 года)

Москва, 2018 г

ИСТОРИЯ ИЗМЕНЕНИЙ

Дата	Версия	Описание	Автор
16.05.2018	1.3	В раздел 7 добавлен пункт о подписи сведений о файлах документов, прикрепленных к сообщению	Адашев Дмитрий

Содержание

1. Общие положения

Настоящий Регламент устанавливает порядок применения электронной подписи при осуществлении информационного обмена электронными документами Пользователями Реестра с Единым федеральным реестром сведений о фактах деятельности юридических лиц и его неотъемлемой частью - Единым федеральным реестром сведений о банкротстве.

2. Термины и определения

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;

Сертификат ключа проверки электронной подписи (сертификат) – 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;

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) - сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом такого удостоверяющего центра;

Удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон об электронной подписи);

Аккредитованный удостоверяющий центр - удостоверяющий центр, признанный органом исполнительной власти, уполномоченным в сфере использования электронной подписи, соответствующим требованиям Закона об электронной подписи;

Авторизованный удостоверяющий центр – аккредитованный удостоверяющий центр, прошедший процедуру подтверждения соответствия требованиям к удостоверяющим центрам согласно Требованиям к удостоверяющим центрам, оказывающим услуги по созданию и управлению сертификатами ключей проверки электронных подписей пользователей Единого федерального реестра сведений о фактах деятельности юридических лиц, и оказывающий услуги по созданию и управлению сертификатами ключей проверки электронных подписей Пользователей Реестра в соответствии с требованиями настоящего Регламента;

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Законом об электронной подписи порядке выдан сертификат ключа проверки электронной подписи.

Единый федеральный реестр сведений о фактах деятельности юридических лиц (Реестр) – государственный информационный ресурс, находящийся в федеральной собственности, содержащий сведения о фактах деятельности юридических лиц в соответствии с законодательством о государственной регистрации юридических лиц и индивидуальных предпринимателей;

Единый федеральный реестр сведений о банкротстве (ЕФРСБ) - государственный информационный ресурс, находящийся в федеральной

собственности, содержащий сведения о несостоятельности (банкротстве) в соответствии с законодательством о несостоятельности (банкротстве), и являющийся неотъемлемой частью Реестра;

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи;

Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам;

Оператор Реестра – юридическое лицо, определяемое в соответствии с законодательством и осуществляющее формирование и обеспечение технического и организационного функционирования Реестра;

Организатор сети Удостоверяющих центров (Организатор сети) – юридическое лицо, привлекаемое Оператором Реестра в целях проверки Удостоверяющих центров на соответствие Требованиям к удостоверяющим центрам, оказывающим услуги по созданию и управлению сертификатами ключей проверки электронных подписей пользователей Единого федерального реестра сведений о фактах деятельности юридических лиц, и осуществления контроля за деятельностью авторизованных удостоверяющих центров;

Реестр сертификатов ключей проверки электронных подписей пользователей Единого федерального реестра сведений о фактах деятельности юридических лиц (Реестр сертификатов Пользователей) – информационный ресурс, включающий в себя сертификаты ключей проверки электронных подписей Пользователей Единого федерального реестра сведений о фактах деятельности юридических лиц, изготовленные авторизованными удостоверяющими центрами. Порядок ведения Реестра сертификатов Пользователей устанавливается Оператором Реестра;

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

Подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе;

Пользователь Реестра – физическое лицо, являющееся уполномоченным представителем Участника информационного обмена и наделенное полномочиями по совершению действий в рамках информационного обмена с Реестром;

Актуальный список аннулированных квалифицированных сертификатов

(список аннулированных сертификатов) - список аннулированных сертификатов, срок действия которого уже наступил и не истек на момент обращения к нему;

Список аннулированных сертификатов - электронный документ с электронной подписью удостоверяющего центра, представляющий собой список уникальных номеров сертификатов ключей проверки электронной подписи, действие которых на определенный момент было прекращено удостоверяющим центром до истечения срока их действия. Список аннулированных сертификатов имеет определенный срок действия, устанавливаемый удостоверяющим центром;

Средство 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;

Участник информационного обмена – лицо, размещающее сведения в Реестре.

3. Вступление в силу Регламента. Изменение (дополнение) Регламента

Настоящий Регламент вступает со дня его опубликования на сайте Оператора Реестра по адресу: http://www.fedresurs.ru/.

Действие настоящего Регламента распространяется на информационный обмен электронными документами Участниками информационного обмена с Единым федеральным реестром сведений о фактах деятельности юридических лиц с 1 января 2013 года.

Действие настоящего Регламента распространяется на информационный обмен электронными документами Участниками информационного обмена с ЕФРСБ с 1 июля 2013 года. До 01 июля 2013 года информационный обмен электронными документами Участниками информационного обмена с ЕФРСБ осуществляется в соответствии с Регламентом применения электронной цифровой подписи в Едином федеральном информационном ресурсе сведений о банкротстве.

Внесение изменений (дополнений) в настоящий Регламент, включая приложения к нему, производится Оператором Реестра в одностороннем порядке.

Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется Оператором Реестра путем размещения указанных изменений (дополнений) на сайте Оператора Реестра по адресу: http://www.fedresurs.ru/ за десять дней до их вступления в силу.

4. Условия допуска пользователя к информационному обмену с Реестром

Пользователь Реестра допускается к информационному обмену с Реестром при наличии у него квалифицированного сертификата, выданного авторизованным удостоверяющим центром и отвечающего требованиям, установленным Приложением № 1 к настоящему Регламенту.

5. Порядок использования электронной подписи при информационном обмене с Реестром

Участники информационного обмена при размещении сведений в Реестре обязаны использовать квалифицированные сертификаты ключей подписей, выданные авторизованными удостоверяющими центрами, соответствующие структуре, указанной в Приложении № 1 к настоящему Регламенту, и внесенные Организатором сети в Реестр сертификатов Пользователей.

Использование квалифицированной электронной подписи при информационном обмене электронными документами с Реестром осуществляется в соответствии с требованиями, установленными Законом об электронной подписи и настоящим Регламентом.

Подписанные квалифицированной электронной подписью электронные документы, размещаемые Участниками информационного обмена в Реестре, проходят процедуру проверки электронной подписи.

При информационном обмене с Реестром обработке подлежат электронные документы, которые подписаны квалифицированной электронной подписью Участника информационного обмена, признанной действительной.

Прекращение действия сертификата, выданного Участнику информационного обмена на имя Пользователя Реестра, осуществляется в обязательном порядке при прекращении полномочий Пользователя Реестра, а также в случае компрометации принадлежащего Пользователю Реестра ключа электронной подписи.

Участник информационного обмена в случае компрометации принадлежащего ему ключа электронной подписи незамедлительно извещает об этом авторизованный удостоверяющий центр для прекращения действия сертификата ключа проверки электронной подписи, соответствующего этому ключу электронной подписи.

При прекращении полномочий Пользователя Реестра по подписанию документов в электронной форме от имени Участника информационного обмена последний незамедлительно извещает об этом авторизованный удостоверяющий центр для прекращения действия сертификата, выданного указанному Пользователю Реестра.

В случае возникновения обстоятельств, не позволяющих Участнику информационного обмена (Пользователю Реестра) правомерно использовать квалифицированную электронную подпись и средства электронной подписи при осуществлении информационного обмена с Реестром, Участник информационного обмена обязан незамедлительно (не позднее одного рабочего дня со дня наступления таких обстоятельств) уведомить об этих обстоятельствах авторизованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения его действия.

6. Условия равнозначности электронного документа, подписанного квалифицированной электронной подписью Пользователя Реестра, документу на бумажном носителе, подписанному собственноручной подписью.

Электронный документ, подписанный квалифицированной электронной подписью Пользователя Реестра, признанной действительной в соответствии с настоящим Регламентом, имеет такую же юридическую силу, как и подписанный собственноручной подписью документ на бумажном носителе, в том числе заверенный оттиском печати соответствующего лица, и влечет предусмотренные для указанного документа правовые последствия.

Наличие в электронном документе действительной квалифицированной электронной подписи Пользователя Реестра означает, что документ направлен от имени владельца сертификата ключа проверки электронной подписи, а сведения, содержащиеся в электронном документе, являются подлинными и достоверными.

Средства электронной подписи, применяемые Участниками информационного обмена, должны иметь документ, подтверждающий соответствие требованиям, установленным пунктом 2 части 5 статьи 8 Закона об электронной подписи (далее – сертифицированные средства электронной подписи).

Порядок формирования и проверки электронной подписи должен соответствовать следующим основным требованиям:

- формирование электронной подписи должно осуществляться только с использованием действующего ключа электронной подписи;
- формирование и проверка электронной подписи электронного документа осуществляется с использованием Сертифицированного средства электронной подписи;

Перечень электронных документов, которые в рамках Реестра должны быть подписаны электронной подписью, определяется нормативными правовыми актами.

Формирование электронного документа осуществляется с учетом следующих требований:

- создание электронных документов осуществляется уполномоченными лицами;
- сертификат ключа проверки электронной подписи должен содержать ограничения, определяющие право владельца данного сертификата формировать электронную подпись в отношении данного типа электронных документов.

В настоящем Регламенте предъявляются следующие требования к применению электронной подписи:

1) сертификат ключа проверки электронной подписи является действительным на определенный момент времени (действительный сертификат), если:
    - сертификат ключа проверки электронной подписи создан авторизованным удостоверяющим центром;
    - срок действия сертификата ключа проверки электронной подписи наступил на момент подписания электронного документа;
    - срок действия сертификата ключа проверки электронной подписи не истек на момент подписания электронного документа;
    - серийный номер сертификата ключа проверки электронной подписи отсутствует в актуальном списке аннулированных сертификатов;
2) электронная подпись признается действительной при одновременном выполнении следующих условий:
    - 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;
    - имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания;
    - квалифицированная электронная подпись используется с учетом ограничений, содержащихся в квалифицированном сертификате лица, подписывающего электронный документ (если такие ограничения установлены).

7. Порядок применения и проверки электронной подписи

Применение электронной подписи при аутентификации Участника информационного обмена, а также при подписании электронного документа осуществляется с использованием применяемого сертифицированного средства электронной подписи и программного обеспечения Реестра.

Формирование электронной подписи может быть осуществлено только владельцем сертификата ключа подписи (Пользователем Реестра).

Проверка электронной подписи осуществляется с использованием применяемого сертифицированного средства электронной подписи и программного обеспечения Реестра.

Обработка подписанного электронной подписью электронного документа осуществляется только после положительного результата проверки выполнения условий признания электронного документа равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Если к публикуемому в Едином федеральном реестре сведений о фактах деятельности юридических лиц (или его неотъемлемой части − Едином федеральном реестре сведений о банкротстве) сообщению или отчету прикреплен файл документа, то при успешном подписании электронной подписью сообщения/отчета, также подписываются сведения о прикрепленном файле. Сведения о файле генерируются в результате выполнения хэш-функции по алгоритму ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». Полученные сведения включаются во внутреннюю структуру данных сообщения/отчета, подписанных электронной подписью.

8. Порядок разрешения конфликтных ситуаций, связанных с применением электронной подписи

8.1. Общие положения

Разрешение конфликтных ситуаций, связанных с подтверждением авторства и неизменности электронного документа, подписанного электронной подписью, возникающих при информационном обмене с Реестром, осуществляется согласительной комиссией (далее также - Комиссия). При возникновении разногласий Участник информационного обмена, заявляющий о разногласиях (сторона-инициатор), обязан направить Оператору Реестра заявление о разногласиях, возникших при обмене (в связи с обменом) и применением электронных документов, подписанное уполномоченным должностным лицом, с подробным изложением причин разногласий и предложением создать согласительную комиссию по ее разрешению.

По заявлению о разногласиях Оператор Реестра формирует согласительную комиссию, в которую входят:

- представитель Оператора Реестра – председатель комиссии;
- представитель стороны-инициатора – член комиссии;
- представитель стороны-ответчика член комиссии.

В качестве специалиста при разрешении конфликтных ситуаций, определенных настоящим разделом, привлекается представитель авторизованного удостоверяющего центра, создавшего сертификат ключа проверки электронной подписи, соответствующего ключу электронной подписи, который использовался при подписании электронного документа.

В качестве эксперта при разрешении конфликтных ситуаций, определенных настоящим разделом, могут привлекаться иные лица, обладающие необходимыми специальными знаниями.

До начала работы согласительной комиссии стороне - инициатору рекомендуется убедиться в целостности установленного на его технических средствах программного обеспечения, в том числе средства электронной подписи, а также отсутствии несанкционированных действий со стороны третьих лиц.

Комиссия осуществляет свою деятельность по месторасположению Оператора Реестра. Язык работы согласительной комиссии – русский.

8.2. Документы, предоставляемые инициатором

Сторона-инициатор представляет заявление о разногласии (уведомление о возникших разногласиях) с указанием:

- даты подачи и номера заявления (уведомления);
- информации, идентифицирующей инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования;

- обоснованного расчета заявленных требований;
- федеральные законы и иные нормативные правовые акты, на основании которых заявляется требование;
- перечня прилагаемых к заявлению (уведомлению) о разногласии документов, составляющие доказательную базу.
- состав документов, предоставляемых стороной-инициатором, должны быть включены:
- файл, содержащий электронный документ с электронной подписью, либо файл, содержащий электронный документ, и файл, содержащий электронную подпись этого документа;
- файл, содержащий сертификат ключа проверки электронной подписи, соответствующий электронной подписи.

8.3. Порядок работы согласительной комиссии

Сторона-ответчик обязана в период работы комиссии представить стороне-инициатору и Комиссии возражения по каждому требованию, изложенному в заявлении о разногласиях.

В возражениях ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы Комиссии.

Любая сторона в ходе работы Комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставление документов, вещественных или иных доказательств в устанавливаемый комиссией срок.

Рассмотрение конфликтной ситуации производится на основании всех представленных документов и иных доказательств.

В том случае, если обстоятельства, имеющие значение для принятия решения по делу и связанные с подтверждением подлинности электронной подписи в электронном документе, могут быть исследованы только на основе применения специальных знаний, комиссия вправе назначить экспертизу.

Экспертиза может быть назначена Комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.

8.4. Оформление результатов работы согласительной комиссии

По итогам работы согласительной комиссии составляется акт, в котором указываются:

- состав комиссии;
- дата и место составления акта;
- дата и время начала и окончания работы Комиссии;
- перечень мероприятий, проведенных Комиссией;

- краткое изложение доводов стороны-инициатора и стороны ответчика;
- краткое изложение заключения специалиста;
- краткое изложение выводов эксперта, если для разрешения конфликтной ситуации привлекался эксперт;
- выводы согласительной комиссии;
- собственноручные подписи членов Комиссии;
- указание на особое мнение члена (или членов Комиссии), в случае наличия такового.

Акт составляется в 3-х экземплярах и предоставляется по одному экземпляру для Оператора Реестра, стороны-инициатора, стороны-ответчика.

9. Разграничение ответственности

Участники информационного обмена:

- сохраняют в тайне ключ своей электронной подписи;
- самостоятельно принимают решение о факте или угрозе компрометации своих ключей электронной подписи и немедленно информируют удостоверяющий центр о факте их компрометации;
- немедленно прекращают использование ключа электронной подписи в случае его компрометации;
- соблюдают правила размещения сведений в Реестре и требования эксплуатационной документации на средство электронной подписи.

Оператор Реестра не несет ответственности за какой-либо ущерб, потери и прочие убытки, которые понес Участник информационного обмена по причине ненадлежащего исполнения настоящего Регламента, несоблюдения руководств и инструкций, касающихся работы Участника информационного обмена и применения электронной подписи.

Оператор Реестра не несет ответственности за какой-либо ущерб, потери и прочие убытки, которые понес Участник информационного обмена по причине ненадлежащих действий или бездействия Удостоверяющего центра, включая ненадлежащую проверку правомочий Пользователя Реестра действовать от имени владельца сертификата ключа проверки электронной подписи, несвоевременное уведомление Оператора Реестра об обновлении списка аннулированных сертификатов или несвоевременное обновление такого списка, выдачу ключей проверки электронной подписи, не соответствующих требованиям настоящего Регламента.

Ответственность за реальный ущерб, который понес Участник информационного обмена по причине ненадлежащих действий или бездействия Удостоверяющего центра, включая ненадлежащую проверку правомочий Пользователя Реестра действовать от имени владельца сертификата ключа проверки электронной подписи, несвоевременное уведомление Оператора Реестра об обновлении списка аннулированных сертификатов или несвоевременное обновление такого списка, выдачу ключей проверки электронных подписей, не соответствующих требованиям настоящего Регламента, несет соответствующий Авторизованный удостоверяющий центр. В случае отсутствия или недостаточности для возмещения причиненного реального ущерба средств Удостоверяющего центра, субсидиарную ответственность за причиненный реальный ущерб несет Организатор сети, в размере и порядке, установленном Оператором Реестра.

Приложение 1

к Регламенту применения
электронной подписи в

Едином федеральном реестре сведений
о фактах деятельности юридических лиц

Требования к структуре сертификата ключа проверки электронной подписи Пользователя Реестра и списку аннулированных сертификатов, публикуемых авторизованным удостоверяющим центром

Сертификат ключа проверки электронной подписи Пользователя Реестра должен соответствовать требованиям, установленным в соответствии с 17 статьей Федерального закона от 6 апреля 2011 г. № 63 ФЗ "Об электронной подписи".

Состав сертификата должен соответствовать Методическим рекомендациям по составу квалифицированного сертификата ключа проверки электронной подписи, опубликованным на Портале госуслуг (http://smev.gosuslugi.ru/portal/).

Сертификат должен содержать в расширении Extended Key Usage один из объектных идентификаторов, определяющих область применения сертификата:

- Участник имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц (OID 1.3.6.1.4.1.40870.1.1.1), или
- Участник имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц (OID 1.2.643.2.64.1.1.1), или
- Участник имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц (OID 1.2.643.3.5.10.2.12), или
- Использование в Информационной системе по раскрытию существенных фактов деятельности юридических лиц (OID 1.2.643.6.3.2).

Требования к составу сертификата.

1. Юридические лица.

Сертификат выданный участнику информационного обмена – представителю юридического лица, должен содержать ОГРН и ИНН юридического лица.

2. Индивидуальные предприниматели.

Сертификат выданный участнику информационного обмена – индивидуальному предпринимателю, должен содержать ОГРНИП и ИНН индивидуального предпринимателя.

3. Физические лица.

Сертификат, выданный участнику информационного обмена - физическому лицу, должен содержать СНИЛС и ИНН физического лица.

Сертификат, выданный участнику информационного обмена - нотариусу, должен соответствовать разделу 7.1 регламента Удостоверяющего центра нотариата России по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи. (http://www.fciit.ru/files/reglament_qual.pdf)