ООО «Интерфакс - ЦРКИ»

Регламент применения электронной подписи при организации электронного взаимодействия между Распространителем информации и Субъектами раскрытия информации

(действует с 1 сентября 2024 года, версия 1.3)

Москва

2024

Содержание

1. Общие положения

Настоящий Регламент устанавливает порядок применения электронной подписи при организации электронного взаимодействия между Распространителем информации – Обществом с ограниченной ответственностью «Интерфакс – Центр раскрытия корпоративной информации» и Субъектами раскрытия информации.

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, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон об электронной подписи) 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, и являющийся в связи с этим официальным документом;

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 Законом об электронной подписи;

Аккредитованный удостоверяющий центр - удостоверяющий центр, признанный соответствующим требованиям Закона об электронной подписи;

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

Центр раскрытия корпоративной информации, ЦРКИ - сетевое издание «Центр раскрытия корпоративной информации» (свидетельство о регистрации СМИ ЭЛ № ФС77-64320 выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) «25» декабря 2015 года). Доменное имя сайта в сети Интернет: E-DISCLOSURE.RU;

Распространитель информации, Агентство - общество с ограниченной ответственностью «Интерфакс – Центр раскрытия корпоративной информации» (ООО «Интерфакс - ЦРКИ»), являющееся редакцией ЦРКИ и аккредитованное на проведение действий по раскрытию информации о ценных бумагах и об иных финансовых инструментах на основании решения Банка России от «27» октября 2016 г. № РБ-52-5/1557;

Субъект раскрытия информации - лицо, которое в соответствии с требованиями законодательства Российской Федерации раскрывает информацию в Ленте новостей и (или) на странице Распространителя информации в сети

Интернет;

Пользователь ЦРКИ – физическое лицо, являющееся уполномоченным представителем Субъекта раскрытия информации и наделенное полномочиями по совершению действий, направленных на раскрытие информации в Ленте новостей и (или) на странице Распространителя информации в сети Интернет;

Публичная информация - информация о ценных бумагах и об иных финансовых инструментах, иная информация, предоставленная Субъектами раскрытия информации, которая в соответствии с требованиями федеральных законов и принятых в соответствии с ними нормативных правовых актов, а также нормативных актов Банка России, регулирующих объем, порядок и сроки раскрытия информации эмитентами ценных бумаг, и раскрытия информации, связанной с деятельностью акционерных инвестиционных фондов и управляющих компаний паевых инвестиционных фондов, должна быть раскрыта в Ленте новостей и (или) на странице Распространителя информации в сети Интернет;

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;

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;

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;

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;

Иные термины, используемые в настоящем Регламенте, трактуются в соответствии с законодательством Российской Федерации, нормативными правовыми актами Банка России и Техническими условиями осуществления Распространителем информации действий по раскрытию информации о ценных бумагах и об иных финансовых инструментах, согласованными с Банком России (далее - *Технические условия*).

3. Изменение (дополнение) Регламента

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

Уведомление о внесении изменений (дополнений) в настоящий Регламент осуществляется Распространителем информации путем размещения указанных изменений (дополнений) на сайте Распространителя информации по адресу: https://www.e-disclosure.ru/ за пять дней до их вступления в силу.

4. Условия допуска Пользователя ЦРКИ к направлению Публичной информации в Агентство

Пользователь ЦРКИ допускается к направлению Публичной информации Распространителю информации при наличии у него квалифицированного сертификата, выданного аккредитованным удостоверяющим центром и отвечающего требованиям, установленным статьей 17 Закона об электронной подписи, при выполнении одного из следующих условий:

1) Пользователь является лицом, имеющим право действовать от имени Субъекта раскрытия информации без доверенности;

2) Пользователь уполномочен на взаимодействие с Распространителем информации на основе машиночитаемой доверенности, соответствующей единому формату (версия 003), разработанному Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации. Такая машиночитаемая доверенность должна содержать полномочие на совершение действий, направленных на раскрытие информации в Ленте новостей и на странице Распространителя информации в сети Интернет, а также такая машиночитаемая доверенность должна быть доступна в «Едином блокчейн хранилище машиночитаемых доверенностей (МЧД) - распределенном реестре ФНС России».

5. Порядок использования электронной подписи при направлении Публичной информации в Агентство

Субъекты раскрытия информации при направлении Публичной информации Распространителю информации обязаны использовать квалифицированные сертификаты ключей подписей, выданные аккредитованными удостоверяющими центрами, соответствующие требованиям, установленным статьей 17 Закона об электронной подписи.

Использование квалифицированной электронной подписи при направлении Публичной информации в Агентство осуществляется в соответствии с требованиями, установленными Законом об электронной подписи, Техническими условиями и настоящим Регламентом.

Подписанные квалифицированной электронной подписью электронные документы, публикуемые Субъектами раскрытия информации в Ленте новостей и (или) на странице Распространителя информации в сети Интернет, проходят процедуру проверки электронной подписи.

При направлении Публичной информации в Агентство обработке подлежат электронные документы, которые подписаны квалифицированной электронной подписью Субъекта раскрытия информации, признанной действительной.

Прекращение действия сертификата, выданного Субъекту раскрытия информации, осуществляется в обязательном порядке при прекращении полномочий Пользователя ЦРКИ, указанного в качестве владельца сертификата наряду с наименованием Субъекта раскрытия информации, а также в случае компрометации принадлежащего владельцу сертификата ключа электронной подписи.

Субъект раскрытия информации в случае компрометации принадлежащего ему ключа электронной подписи незамедлительно извещает об этом аккредитованный удостоверяющий центр для прекращения действия сертификата ключа проверки электронной подписи, соответствующего этому ключу электронной подписи.

При прекращении полномочий Пользователя ЦРКИ по осуществлению действий, направленных на раскрытие информации, от имени Субъекта раскрытия информации последний незамедлительно извещает об этом аккредитованный удостоверяющий центр для прекращения действия сертификата, выданного указанному Пользователю ЦРКИ, а в случае, если взаимодействие с Распространителем информации осуществлялось на основании машиночитаемой доверенности - Субъект раскрытия информации незамедлительно формирует заявление об отмене доверенности согласно требованиям Постановления Правительства РФ от 21.02.2022 г. N 223 "Об утверждении организационно-технических требований к порядку хранения, использования и отмены указанных в статьях 17.2 и 17.3 Федерального закона "Об электронной подписи" доверенностей".

В случае возникновения обстоятельств, не позволяющих Субъекту раскрытия информации (Пользователю ЦРКИ) правомерно использовать квалифицированную электронную подпись и средства электронной подписи при осуществлении информационного обмена с Агентством, Субъект раскрытия информации обязан незамедлительно (не позднее одного рабочего дня со дня наступления таких обстоятельств) уведомить об этих обстоятельствах аккредитованный удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения его действия.

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

Электронный документ, подписанный квалифицированной электронной подписью Пользователя ЦРКИ, 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 Субъекта раскрытия информации 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 Субъектами раскрытия информации, должны иметь документальное подтверждение соответствия 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 Субъектов раскрытия информации, которые должны быть подписаны электронной подписью при направлении в Агентство, определяется нормативными правовыми актами Банка России и Техническими условиями.

Формирование электронного документа осуществляется с учетом следующих требований:

- создание электронных документов осуществляется уполномоченными лицами;

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 аккредитованным 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.

7. Порядок применения и проверки электронной подписи

Применение электронной подписи при подписании электронного документа Субъекта раскрытия информации осуществляется с использованием применяемого сертифицированного средства электронной подписи и программного обеспечения ЦРКИ.

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

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

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.

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 ЦРКИ, осуществляется согласительной комиссией (далее также - Комиссия). При возникновении разногласий Субъект раскрытия информации, заявляющий о разногласиях (сторона-инициатор), обязан направить Распространителю информации 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 Распространитель информации формирует согласительную комиссию, в которую входят:

- представитель Распространителя информации – председатель комиссии;
- представитель стороны-инициатора – член комиссии;
- представитель стороны-ответчика - член комиссии.

В качестве специалиста при разрешении конфликтных ситуаций, определенных настоящим разделом, может привлекаться представитель аккредитованного 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 Распространителя информации. 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;

- федеральных законов и иных нормативных правовых актов, на основании которых заявляется требование;
- перечня прилагаемых к заявлению (уведомлению) о разногласии документов, составляющих доказательную базу.

В 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 Распространителя информации, стороны-инициатора, стороны-ответчика.

9. Разграничение ответственности

Субъекты раскрытия информации:

- 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 Технические условия при направлении Публичной информации в Агентство, а также требования эксплуатационной документации на средство электронной подписи.

Распространитель информации не несет ответственности за какой-либо ущерб, потери и прочие убытки, которые понес Субъект раскрытия информации по причине ненадлежащего исполнения настоящего Регламента, несоблюдения руководств и инструкций, касающихся работы Субъекта раскрытия информации, применения электронной подписи и машиночитаемых доверенностей.

Распространитель информации не несет ответственности за какой-либо ущерб, потери и прочие убытки, которые понес Субъект раскрытия информации по причине ненадлежащих действий или бездействия Удостоверяющего центра, включая ненадлежащую проверку правомочий Пользователя ЦРКИ обращаться в Удостоверяющий центр за получением квалифицированного сертификата от имени Субъекта раскрытия информации, несвоевременное уведомление Распространителя информации об обновлении списка аннулированных сертификатов или несвоевременное обновление такого списка, выдачу сертификатов ключей проверки электронной подписи, не соответствующих требованиям настоящего Регламента.

Ответственность за реальный ущерб, который понес Субъект раскрытия информации по причине ненадлежащих действий или бездействия Удостоверяющего центра, включая ненадлежащую проверку правомочий Пользователя ЦРКИ обращаться в Удостоверяющий центр за получением квалифицированного сертификата от имени Субъекта раскрытия информации, несвоевременное уведомление Распространителя информации об обновлении списка аннулированных сертификатов или несвоевременное обновление такого списка, выдачу сертификатов ключей проверки электронных подписей, не соответствующих требованиям настоящего Регламента, несет соответствующий удостоверяющий центр.