

Утверждён Приказом
Генерального директора
КИТ Финанс (АО)
№ 5 от 16.01.2019 г.

Ю. Лазаренко

Ю.А. Лазаренко

**РЕГЛАМЕНТ
ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
КИТ ФИНАНС (АО)**

Санкт-Петербург, 2019 г.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте используются основные термины, определенные в статье 2 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями), а также термины, определенные в Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом Федерального Агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152.

Аккредитация удостоверяющего центра – признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Заявитель – лицо, обратившееся в Удостоверяющий центр за получением сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

Квалифицированная электронная подпись – 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 Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Неквалифицированная электронная подпись – 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.

Подтверждение владения ключом электронной подписи – получение удостоверяющим центром 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.

Реестр сертификатов – реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных 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.

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

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.

Удостоверяющий Центр КИТ Финанс (АО) (Удостоверяющий центр) – структурное подразделение КИТ Финанс (АО), осуществляющее выполнение функций Удостоверяющего центра по изготовлению и управлению Сертификатами, получившее аккредитацию в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Уполномоченное лицо Удостоверяющего центра КИТ Финанс (АО) – сотрудник удостоверяющего центра КИТ Финанс (АО), наделённый полномочиями по заверению сертификатов ключей проверки электронной подписи, проверке достоверности документов и сведений и проведению идентификации заявителей.

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.

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1 Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра КИТ Финанс (АО) (далее – Общества). Нормы, содержащиеся в Регламенте, обязательны для всех Заявителей обратившихся за получением сертификатов ключей проверки, усиленной неквалифицированной или усиленной квалифицированной электронной подписи.

1.2 Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании Свидетельства об аккредитации Удостоверяющего центра № 716/1 от 06.09.2018 г., выданного Минкомсвязи России (федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи) и лицензии, выданной Управлением Федеральной службы безопасности Российской Федерации по городу Санкт-Петербургу и Ленинградской области. Данные лицензии Удостоверяющего центра:

ЛСЗ № 0001029 Рег. № 1176Н от 21 августа 2018 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания 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 или индивидуального предпринимателя).

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности»: работы, предусмотренные пунктами 12, 13, 14, 15, 20, 21, 22, 23, 24, 25, 26, 28 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утверждённому постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

Для обеспечения своей деятельности Удостоверяющий центр использует сертифицированные в соответствии с действующим законодательством Российской Федерации средства криптографической защиты информации.

1.3 Статус Удостоверяющего центра, при обеспечении функционирования корпоративных информационных систем, определяется соглашением участников этих систем.

1.4 Реквизиты Удостоверяющего центра:

Почтовый адрес: 191119, г. Санкт-Петербург, ул. Марата, дом 69-71, лит. А

Адрес электронной почты: uc@brokerkf.ru

Контактные телефоны: 611-00-00 (добавочный: 44019, 44114, 44582).

График работы: пн. – пт.: с 9:00 – 18:00, сб. – вс.: выходной.

Адрес сайта Удостоверяющего центра: https://brokerkf.ru/soprovozhdenie_klientov/technical-support/electronic-signature/.

1.5 Получение информации о оказываемых услугах Удостоверяющего центра доступно по указанным реквизитам.

1.6 Услуги удостоверяющего центра могут оказываться на платной основе, сроки, порядок расчётов и тарифы за оказание услуг Удостоверяющего центра публикуются на сайте Общества.

1.7 Настоящий Регламент располагается по электронному адресу в сети Интернет: http://brokerkf.ru/doc/uc/reglament_uc.pdf.

2. СВЕДЕНИЯ ОБ УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ И ОКАЗЫВАЕМЫХ УСЛУГАХ

2.1 Удостоверяющий центр КИТ Финанс (АО) является структурным подразделением Общества.

2.2 Удостоверяющий центр предоставляет услуги по изготовлению и выдаче сертификатов ключей проверки электронной подписи для усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи, а также услуги, связанные с использованием средств электронной подписи.

2.3 Деятельность Удостоверяющего центра направлена на достижение следующих целей:

2.3.1 Обеспечение юридически значимого документооборота при обмене электронными документами между Обществом и Участниками системы электронного документооборота Общества;

2.3.2 Обеспечение юридически значимого документооборота при обмене электронными документами между владельцами сертификатов ключей проверки электронной подписи и другими участниками электронного взаимодействия;

2.3.3 Обеспечение надлежащего использования средств криптографической защиты информации в соответствии с требованиями законодательства Российской Федерации;

2.3.4 Обеспечение безопасности информации с использованием средств криптографической защиты информации в информационных системах Общества, а также при передаче информации по незащищенным каналам связи за пределы информационных систем Общества.

2.4 Функции Удостоверяющего центра:

2.4.1 Создание сертификатов ключей проверки электронных подписей и выдача сертификатов Заявителям (Владельцам сертификатов).

2.4.2 Установление сроков действия сертификатов ключей проверки электронных подписей.

2.4.3 Аннулирование выданных Удостоверяющим центром сертификатов ключей проверки электронных подписей.

2.4.4 Выдача по обращению Заявителей средств электронной подписи, содержащих 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.

2.4.5 Ведение Реестра сертификатов.

2.4.6 Создание по обращениям Заявителей ключей электронных подписей и ключей проверки электронных подписей.

2.4.7 Проверка уникальности ключей проверки электронной подписи в Реестре сертификатов.

2.4.8 Осуществление подтверждения владения ключом электронной подписи, подтверждения владения сертификатом ключа электронной подписи, соответствующего ключу проверки электронной подписи, указанному заявителем для получения сертификата.

2.4.9 Обеспечение условий, необходимых для признания юридической значимости электронных документов, подписанных электронной подписью.

2.4.10 Участие в работе технической (экспертной) комиссии при рассмотрении конфликтных ситуаций, осуществление проверки электронных подписей по обращениям участников электронного взаимодействия.

2.4.11 Взаимодействие с уполномоченным федеральным органом исполнительной власти в области использования шифровальных (криптографических) средств.

2.4.12 Поддержание работоспособности программных и технических средств Удостоверяющего центра, а также восстановление работоспособности после аварийных сбоев.

2.4.13 Осуществление иной, связанной с использованием электронной подписи, деятельности.

2.5 Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, в том числе материальный, причиненный третьим лицам в результате:

2.5.1 Неисполнения или ненадлежащего исполнения условий Регламента.

2.5.2 Неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

2.6 Удостоверяющий центр не несет ответственности за последствия, возникшие в результате нарушения участниками электронного документооборота положений настоящего Регламента.

2.7 Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством Российской Федерации. В случае прекращения функционирования Удостоверяющий центр обязан:

2.7.1 Сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности.

2.7.2 Передать в уполномоченный федеральный орган в установленном законодательством Российской Федерации порядке реестр выданных аккредитованным удостоверяющим центром квалифицированных сертификатов.

2.7.3 Передать на хранение в уполномоченный федеральный орган в установленном законодательством Российской Федерации порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

2.8 Настоящий Регламент оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее – Регламент, определяет условия Договора об электронном документообороте, заключенного Обществом с юридическими и физическими лицами, а также с индивидуальными предпринимателями, присоединившимися к Договору об электронном документообороте на условиях, зафиксированных в настоящем Регламенте. Договор об электронном документообороте не является публичным договором в смысле статьи 426 Гражданского кодекса РФ. Общество вправе по своему усмотрению отказать в заключении Договора об электронном документообороте без объяснения причин такого отказа.

2.9 Присоединение к настоящему Регламенту (заключение Договора об электронном документообороте) производится в порядке, определенном ст.428 Гражданского кодекса Российской Федерации путем передачи Обществу письменного Заявления о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО) по формам Приложений №№ 2, 3, 4.

Договор об электронном документообороте считается заключенным с момента регистрации заявления о присоединении, если иное не предусмотрено настоящим Регламентом.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1 Удостоверяющий центр обязан:

3.1.1 Информировать в письменной форме Заявителей об условиях и о порядке использования ключей электронной подписи и средств электронной подписи, о рисках, связанных с применением электронной подписи, и о мерах, необходимых для обеспечения безопасности ключей электронной подписи и их проверки.

3.1.2 Вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;

3.1.3 Обеспечивать актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.1.4 Обеспечивать и 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.

3.1.5 Обеспечивать доступность реестра сертификатов в информационно-телекоммуникационной сети «Интернет» в любое время, за исключением периодов планового или внепланового технического обслуживания.

3.1.6 Предоставить информацию, содержащуюся в реестре сертификатов Удостоверяющего центра по средствам почтового отправления либо с использованием информационно-телекоммуникационной сети «Интернет» в течении двадцати четырёх часов, с момента поступления запроса, способом, указанным в запросе.

3.1.7 Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронной подписи, при необходимости обеспечить уничтожение ключей электронной подписи в максимально короткие сроки.

3.1.8 Направлять в единую систему идентификации и аутентификации сведения о лице, получившем сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им сертификате.

3.1.9 По желанию заявителя, получившего сертификат, безвозмездно осуществить регистрацию указанного заявителя в единой системе идентификации и аутентификации.

3.1.10 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.

3.1.11 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.

3.1.12 Соблюдать срок действия ключей электронной подписи Удостоверяющего центра, используемых для подписания создаваемых сертификатов, распределяя сроки их действия так, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

3.1.13 Нести ответственность в соответствии с законодательством Российской Федерации за вред, причиненный третьим лицам.

3.2 Удостоверяющий центр имеет право:

3.2.1 Отказать Заявителю в регистрации в Удостоверяющем центре и выдаче сертификата, в случае непредставления необходимых документов либо их ненадлежащего оформления;

3.2.2 Отказать в изготовлении Сертификата в случае, если используемое Заявителем средство для формирования запроса на создание Сертификата средство криптографической защиты информации не поддерживается Удостоверяющим центром.

3.2.3 Отказать Владельцу сертификата в отзыве Сертификата, в случае непредставления необходимых документов, предоставлении документов не в полном объеме, предоставлении документов, вызывающих сомнение в их подлинности.

3.2.4 Запрашивать документы, для подтверждения информации у Заявителей, при изготовлении и выдаче Сертификатов.

3.2.5 Аннулировать сертификат в случае вступления в силу решения суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

3.2.6 В одностороннем порядке аннулировать действие Сертификатов в случае:

- наличия у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата;
- невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи;
- появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включенной в выданный сертификат;
- если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

3.2.7 Запрашивать и получать из государственных информационных ресурсов:

- выписку из единого государственного реестра юридических лиц в отношении Заявителя - юридического лица;
- выписку из единого государственного реестра индивидуальных предпринимателей в отношении Заявителя - индивидуального предпринимателя;
- выписку из единого государственного реестра налогоплательщиков в отношении Заявителя - иностранной организации;
- подтверждение соответствия указанных данных фамильно-именной группы и СНИЛС.

3.2.8 Запрашивать дополнительные документы, для подтверждения информации у Заявителей, при изготовлении и выдаче Сертификатов, в случае возникновения противоречий между сведениями, представленными Заявителем и сведениями полученными Удостоверяющим центром из государственных информационных ресурсов.

3.2.9 Не принимать от заявителя документы, не соответствующие требованиям законодательства Российской Федерации.

3.3 Владелец сертификата обязан:

3.3.1 Обеспечивать конфиденциальность ключа электронной подписи и не допускать использование принадлежащего ему ключа электронной подписи без его согласия.

3.3.2 Уведомлять Удостоверяющий центр и иных участников электронного документооборота о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

3.3.3 Хранить в тайне свой ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

3.3.4 Использовать ключи ЭП только во время осуществления электронного документооборота. После окончания использования отключать (отсоединять) ключевой носитель от персонального компьютера или иного аппаратно-программного средства, применяемого для использования электронного документооборота;

3.3.5 Применять для формирования электронной подписи только действующий ключ электронной подписи.

3.3.6 Не применять свой ключ электронной подписи, если Владельцу сертификата стало известно, что этот ключ используется или использовался ранее другими лицами.

3.3.7 Применять ключ электронной подписи только в соответствии с областями использования, указанными в соответствующем данному ключу Сертификате.

3.3.8 Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) действия Сертификата в случае потери, раскрытия, искажения ключа электронной подписи, а также в случае если Владельцу сертификата стало известно, что этот ключ используется или использовался ранее другими лицами.

3.3.9 Не использовать ключ электронной подписи, связанный с Сертификатом, заявление на приостановку действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановку действия Сертификата до момента официального уведомления о приостановке Сертификата.

3.3.10 Не использовать ключ электронной подписи, связанный с Сертификатом, который аннулирован (отозван) или действие его приостановлено;

3.3.11 Не использовать ключ электронной подписи до предоставления Удостоверяющему центру подписанной копии Сертификата, соответствующего данному ключу электронной подписи.

3.3.12 В случае несоблюдения указанных выше мер по обеспечению безопасности, владелец сертификата несет риск любых вызванных таким несоблюдением неблагоприятных последствий и убытков, в том числе связанных с несанкционированным завладением Ключами ЭП третьими лицами и их использованием в системе электронного документооборота от лица владельца ключей ЭП.

3.4 Владелец сертификата имеет право:

3.4.1 Получить реестр аннулированных сертификатов, изготовленный Удостоверяющим центром.

3.4.2 Применять Сертификат для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в Сертификате.

3.4.3 Обратиться в Удостоверяющий центр с запросом на создание Сертификата.

3.4.4 Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) или приостановление действия Сертификата, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.

3.4.5 Обратиться в Удостоверяющий центр с заявлением на возобновление действия Сертификата, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи и срока, на который действие Сертификата было приостановлено.

3.4.6 Обратиться в Удостоверяющий центр за получением информации о действительности Сертификата на определенный момент времени.

3.4.7 Обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием Сертификата, изданного Удостоверяющим центром.

3.4.8 Применять реестр аннулированных сертификатов Удостоверяющего центра для подтверждения действительности своего Сертификата.

4. ПОРЯДОК ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1 Удостоверяющий центр оказывает услуги по созданию сертификатов ключей проверки электронной подписи только после:

4.1.1 присоединения Заявителей к Правилам электронного документооборота КИТ Финанс (АО) в порядке, установленном указанными Правилами электронного документооборота – для Заявителей, у которых заключен договор на брокерское обслуживание с Обществом;

4.1.2 присоединения Заявителей к настоящему Регламенту в порядке, установленном пп. 2.8-2.9. настоящего Регламента - в случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом.

4.2 При обращении в Удостоверяющий центр для получения сертификатов ключей проверки электронной подписи для усиленной квалифицированной электронной подписи Заявитель обязан предоставить следующие документы либо их надлежащим образом заверенные копии и сведения:

4.2.1 запрос на создание квалифицированного сертификата ключа проверки электронной подписи;

4.2.2 основной документ, удостоверяющий личность;

4.2.3 номер страхового свидетельства государственного пенсионного страхования Заявителя - физического лица (СНИЛС);

4.2.4 идентификационный номер налогоплательщика Заявителя - физического лица;

4.2.5 основной государственный регистрационный номер Заявителя - юридического лица;

4.2.6 основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя Заявителя - индивидуального предпринимателя;

4.2.7 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;

4.2.8 вид на жительство или нотариально заверенный перевод документа, удостоверяющего личность иностранного гражданина, если владельцем сертификата ключа проверки электронной подписи является иностранный гражданин;

4.2.9 доверенность или иной документ, подтверждающий право Заявителя действовать от имени других лиц;

4.2.10 согласие на обработку персональных данных.

4.3 При обращении в Удостоверяющий центр для получения сертификатов ключей проверки электронной подписи для усиленной неквалифицированной электронной подписи Заявитель обязан присоединиться к правилам электронного документооборота КИТ Финанс (АО) и предоставить следующие документы либо их надлежащим образом заверенные копии и сведения:

4.3.1 запрос на создание сертификата ключа проверки электронной подписи;

4.3.2 доверенность или иной документ, подтверждающий право Заявителя действовать от имени других лиц.

4.4 Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 4.2.5-4.2.7 настоящего Регламента.

4.5 Создание ключей Электронной подписи.

4.5.1 Процедура создания ключа электронной подписи и ключа проверки электронной подписи выполняется Заявителями, имеющими договор на брокерское обслуживание с Обществом, самостоятельно с помощью сертифицированных средств электронной подписи, предоставляемых Удостоверяющим центром.

4.5.2 Заявители, имеющие договор на брокерское обслуживание с Обществом, по умолчанию, формируют ключи электронной подписи, для использования в торговых системах и СЭД Общества, в формате «СКЗИ Крипто-КОМ» на указанный носитель.

4.5.3 В случае формирования ключей электронной подписи посредством Web-интерфейса, запрос на создание Сертификата автоматически поступает в Удостоверяющий центр, в случае формирования ключей электронной подписи посредством специализированного программного обеспечения (сертифицированного СКЗИ), Заявитель самостоятельно предоставляет запрос на создание Сертификата в электронной форме в Удостоверяющий центр, в случае формирования ключей электронной подписи в офисе Общества выполняется сотрудниками Удостоверяющего центра с использованием аттестованного АРМ.

4.5.4 В случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом, процедура создания ключей электронной подписи выполняется сотрудниками Удостоверяющего центра

в офисе Общества, с использованием аттестованного АРМ, на основании заранее полученного заявления о присоединении к Регламенту, с указанием всех параметров ключа электронной подписи и оплаченного счёта, в соответствии с тарифами, опубликованными на сайте Общества. Созданные ключи записываются на ключевой носитель, приобретенный участником электронного взаимодействия в соответствии с заявлением или предоставляемый самим заявителем.

4.5.5 Предоставляемый Заявителем ключевой носитель должен иметь поддерживаемый тип устройства, не содержать никакой информации (инициализирован), ключевые носители, не удовлетворяющие указанным требованиям, для записи ключевой информации могут не приниматься.

4.5.6 Порядок смены ключей электронной подписи владельца сертификата осуществляется по заявлению владельца о смене ключа электронной подписи.

4.5.7 Заявление о смене ключа электронной подписи может быть подано как в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, так и на бумажном носителе.

4.5.8 В заявлении указывается причина смены ключа электронной подписи (компрометация, угроза компрометации и др.), какой ключ электронной подписи и какого владельца подлежит смене.

4.5.9 Порядок смены ключей электронной подписи Удостоверяющего центра осуществляется в соответствии с технической документацией разработчика.

4.5.10 Плановая смена ключей электронной подписи Удостоверяющего центра выполняется не позднее, чем за 1 год до окончания периода действия рабочего ключа электронной подписи.

4.5.11 Внеплановая смена ключей электронной подписи Удостоверяющего центра выполняется в случае компрометации или угрозы компрометации ключа электронной подписи.

4.5.12 При внеплановой смене ключа электронной подписи Удостоверяющего центра прекращается действие всех сертификатов, подписанных скомпрометированным ключом, новые сертификаты создаются безвозмездно.

4.5.13 Информация о факте компрометации ключей Удостоверяющего центра размещается на главной странице сайта Общества <http://www.brokerkf.ru>, владельцы сертификатов оповещаются о компрометации путем рассылки по электронной почте и посредством систем электронного документооборота.

4.5.14 Информация о новом сертификате УЦ размещается в разделе Удостоверяющего центра сайта Общества.

4.6 Создание Сертификата.

4.6.1 Уполномоченное лицо Удостоверяющего центра при получении запроса на создание Сертификата от заявителя, имеющего договор на брокерское обслуживание с Обществом, производит сравнение данных, указанных в запросе, с информацией, содержащейся в учётной системе Общества.

4.6.2 Запрос на создание сертификата может быть подан как в форме электронного документа, так и на бумажном носителе.

4.6.3 При принятии положительного решения Уполномоченное лицо Удостоверяющего центра изготавливает Сертификат не позднее 3-х рабочих дней, следующих за рабочим днем, в течение которого был получен запрос.

4.6.4 После изготовления Сертификата, Уполномоченное лицо Удостоверяющего центра передаёт копию Сертификата в электронном виде на авторизованный адрес электронной почты Заявителя или оригинал Сертификата при личном обращении Заявителя.

4.6.5 При получении Сертификата Заявителю необходимо распечатать полученный документ, подписать и передать 2 экземпляра Сертификата в Удостоверяющий центр.

4.6.6 При плановой смене Сертификата в рамках ЭДО с Обществом документы в Общество можно передать без визита в офис через Личный кабинет, подписав действующим ключом электронной подписи.

4.6.7 В случае отказа в изготовлении Сертификата Заявитель уведомляется об этом с указанием причины отказа.

4.6.8 Заявителям, имеющим договор на брокерское обслуживание с Обществом, выпуск сертификатов ключа проверки электронной подписи для работы в сторонних системах электронного документооборота осуществляется на платной основе, в соответствии с тарифами, опубликованными на сайте Общества.

4.6.9 В случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом, процедура создания сертификата ключа проверки электронной подписи выполняется сотрудниками Удостоверяющего центра в офисе Общества, на основании заранее полученного заявления о

присоединении к Регламенту, с указанием всех параметров сертификата ключа проверки электронной подписи и оплаченного счёта, в соответствии с тарифами, опубликованными на сайте Общества. Созданные сертификаты записываются на ключевой носитель, приобретенный участником электронного взаимодействия в соответствии с заявлением или предоставляемый самим заявителем.

4.6.10 При личном обращении в офис Общества Заявителям выдаются записанные на ключевой носитель сертификат ключа проверки электронной подписи, соответствующий ключу электронной подписи, копия сертификата ключа проверки электронной подписи на бумажном носителе.

4.6.11 При выдаче сертификата, личность заявителя устанавливается по основному документу удостоверяющего личность, в соответствии с законодательством Российской Федерации.

4.7 Аннулирование (отзыв) сертификата ключа проверки электронной подписи.

4.7.1 Удостоверяющий центр аннулирует Сертификат ключа проверки электронной подписи в следующих случаях:

- по истечении срока действия;
- по заявлению Владельца Сертификата на прекращение действия Сертификата;
- в случае прекращения деятельности Удостоверяющего центра без передачи его функций другим лицам;
- при компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

4.7.2 Удостоверяющий центр признает сертификат аннулированным, если:

- не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате;
- вступило в силу решение суда, которым установлено, что сертификат содержит недостоверную информацию;

4.7.3 Фактом уведомления Владельца Сертификата об аннулировании Сертификата является публикация Удостоверяющим центром обновленного актуального Реестра аннулированных сертификатов.

4.7.4 Информация о прекращении действия Сертификата вносится в Реестр выданных Сертификатов в течение тридцати минут после поступления в Удостоверяющий центр заявления Владельца Сертификата на аннулирование (отзыв) Сертификата. Действие Сертификата прекращается с момента начала использования Реестра аннулированных сертификатов, в который внесён этот Сертификат.

4.7.5 Аннулирование (отзыв) Сертификата осуществляется по заявлению его владельца, подающемуся в Удостоверяющий центр в электронной или бумажной форме, в соответствии с Приложением 5 настоящего Регламента.

4.7.6 Аннулирование (отзыв) Сертификата осуществляется после подтверждения полномочий владельца сертификата или доверенного лица.

4.7.7 Аннулирование (отзыв) Сертификата осуществляется в течение тридцати минут рабочего дня, в котором было зарегистрировано заявление в Удостоверяющем центре.

4.8 Приостановление действия Сертификата ключа проверки электронной подписи.

4.8.1 Приостановление действия Сертификата осуществляется по заявлению его владельца, подающемуся в Удостоверяющий центр в устной, электронной или бумажной форме, а также по решению Удостоверяющего центра в случаях, определенных настоящим Регламентом.

4.8.2 Если в течение срока приостановления действия Сертификата действие этого Сертификата не будет возобновлено, то Сертификат аннулируется (отзывается) Удостоверяющим центром.

4.8.3 В случае отказа в приостановлении действия Сертификата Владелец Сертификата уведомляется об этом с указанием причины отклонения заявления.

4.8.4 При принятии положительного решения Уполномоченное лицо Удостоверяющего центра приостанавливает действие Сертификата.

4.9 Возобновление действия Сертификата ключа проверки электронной подписи.

4.9.1 Возобновление действия Сертификата может быть осуществлено исключительно в период приостановления действия Сертификата.

4.9.2 Возобновление действия Сертификата и официальное уведомление Владельца о возобновлении действия Сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было принято заявление Удостоверяющим центром.

4.9.3 Возобновление действия Сертификата осуществляется на основании заявления в электронной или бумажной форме.

4.10 Ведение реестра сертификатов Удостоверяющего центра.

4.10.1 Реестр сертификатов Удостоверяющего центра ведётся в формате электронной базы данных.

4.10.2 Информация о истечении срока действия сертификата вносится в базу данных автоматически.

4.10.3 Доступ к реестру сертификатов обеспечивается круглосуточно, за исключением периодов планового или внепланового обслуживания.

4.10.4 Информирование о плановом или внеплановом обслуживании осуществляется путём публикации информации на сайте Общества.

4.11 Представление Сертификатов, находящихся в Реестре Удостоверяющего центра.

4.11.1 Представление Сертификата, находящегося в Реестре Удостоверяющего центра, осуществляется на основании запроса в свободной форме с указанием информации, позволяющей идентифицировать Сертификат в Реестре выданных Сертификатов, и цели, для достижения которой должен быть представлен Сертификат. Сертификат представляется в электронном виде.

4.11.2 Срок предоставления Удостоверяющим центром Сертификата составляет три дня с момента получения Удостоверяющим центром соответствующего запроса.

5. ПОДТВЕРЖДЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1 Удостоверяющим центром Общества, предоставляется услуга по проверке электронной подписи в электронных документах.

5.2 Подтверждение электронной подписи осуществляется на основании Заявления.

5.3 К заявлению прилагаются следующие файлы:

- файл содержащий подписанный электронной подписью документ или два файла, подписанный документ и файл содержащий значение электронной подписи;
- файл сертификата, с использованием которого необходимо проверить подлинность электронного документа;
- файл сертификата Удостоверяющего центра, выдавшего сертификат автора электронной подписи;
- файл реестра аннулированных сертификатов, актуальный на день подачи заявления.

5.4 Процедура проверки всех сертификатов осуществляется уполномоченными сотрудниками Удостоверяющего центра, с использованием сертифицированных СКЗИ.

5.5 Стоимость услуги проверки электронной подписи может осуществляться на платной основе, в зависимости от типа запроса.

5.6 Подтверждение подлинности электронной подписи Удостоверяющего центра также может осуществляться в соответствии с «Порядком разрешения конфликтных ситуаций КИТ Финанс (АО) (Приложение № 1)».

6. ДОПОЛНИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1 Срок действия ключа проверки электронной подписи участника электронного документооборота устанавливается равным сроку действия сертификата ключа проверки электронной подписи и составляет 12 месяцев.

6.2 Смена ключей проверки электронной подписи и Сертификатов производится в связи с истечением установленного срока их действия.

6.3 Реестр аннулированных сертификатов обновляется Удостоверяющим центром не реже 1 (одного) раза в сутки, исключая выходные и праздничные дни, в том числе и в случае отсутствия изменений в реестре.

7. ПРОЧИЕ УСЛОВИЯ

7.1 Конфиденциальность

7.1.1 Удостоверяющий центр обеспечивает конфиденциальность персональных данных, вносимых в Реестр Сертификатов.

7.1.2 Заявители и/или их уполномоченные представители представляют Удостоверяющему центру письменное согласие на обработку принадлежащих им персональных данных, которые будут внесены Удостоверяющим центром в Сертификат.

7.2 Прекращение оказания услуг Удостоверяющим центром.

7.2.1 Прекращение деятельности Удостоверяющего Центра может быть осуществлено на основании решения Общества и в порядке, установленном внутренними документами Общества и законодательством Российской Федерации.

7.2.2 В случае прекращения деятельности Удостоверяющего Центра все Сертификаты, выданные Удостоверяющим Центром, аннулируются.

7.3 Хранение Сертификатов в Удостоверяющем центре.

7.3.1 Хранение в Удостоверяющем центре всех выданных Сертификатов осуществляется постоянно в форме электронных документов.

8. СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

8.1 Инженерно-технические меры защиты информации.

8.1.1 Сервер Удостоверяющего центра размещен в серверном помещении. Рабочие станции Уполномоченных лиц Удостоверяющего центра размещены согласно схеме организации рабочих мест персонала Общества.

8.1.2 Антивирусная защита сервера Удостоверяющего центра и рабочих станций Уполномоченных лиц Удостоверяющего центра проводится в рамках общекорпоративной антивирусной системы.

8.1.3 Резервное копирование сервера Удостоверяющего центра проводится в рамках общекорпоративной системы архивирования данных.

8.1.4 Физический доступ в помещения.

8.1.4.1. Серверное помещение Удостоверяющего центра оборудовано системой контроля доступа электромеханического типа и оборудовано механическими замками.

8.1.5 Электроснабжение и кондиционирование воздуха в помещениях.

8.1.5.1. Технические средства Удостоверяющего центра подключены к электрической сети гарантированного электроснабжения.

8.1.5.2. Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.

8.1.5.3. Серверное помещение Удостоверяющего центра оборудовано системой пожарной сигнализации и дымоудаления.

8.2 Программно-аппаратные меры защиты информации.

8.2.1 Организация доступа к техническим средствам Удостоверяющего центра.

8.2.1.1 Сервер Удостоверяющего центра и рабочие места Уполномоченных лиц Удостоверяющего центра защищаются от несанкционированного доступа средствами операционной системы.

8.2.1.2 Доступ системных администраторов общесистемного программного обеспечения серверов Удостоверяющего центра для выполнения регламентных работ осуществляется в присутствии Уполномоченного лица Удостоверяющего центра.

8.2.1.3 База данных Удостоверяющего центра ограничена по доступу средствами парольной защиты и контроля портов.

8.2.2 Защита внешних сетевых соединений.

8.2.2.1 Защита программно-технических средств обеспечения деятельности Удостоверяющего центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования, сертифицированных ФСТЭК России средств межсетевое экранирования.

8.2.3 Организационные меры защиты информации.

8.2.3.1 Уполномоченные лица Удостоверяющего центра работают под индивидуальными учётными записями.

8.2.3.2 Уполномоченные лица Удостоверяющего Центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 5 лет.

9. ПОРЯДОК ИЗМЕНЕНИЯ РЕГЛАМЕНТА И ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ РЕГЛАМЕНТА (ДОГОВОРА ОБ ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ).

9.1. Общество имеет право вносить изменения в настоящий Регламент в одностороннем порядке, о чем Общество обязано сообщить не позднее, чем за 5 (Пять) календарных дней до даты введения в действие изменений путем размещения указанных изменений и дополнений на официальном сайте Общества в Интернет.

9.2. Изменения и дополнения, вносимые Обществом в Регламент в связи с изменением законодательства Российской Федерации, считаются вступившими в силу одновременно с вступлением в силу таких документов (изменений в таких документах).

9.3. Настоящий Регламент (Договор об электронном документообороте) действует до заявления одной из Сторон о прекращении Договора электронного документооборота. Такое заявление одна Сторона должна направить другой не позднее, чем за 30 (Тридцать) дней до предполагаемой даты прекращения.

9.4. Прекращение действия настоящего Регламента (Договора об электронном документообороте) не влияет на юридическую силу и действительность электронных документов, которые были созданы до прекращения действия Регламента.

Порядок разрешения конфликтных ситуаций КИТ Финанс (АО)

Настоящий Порядок разрешения конфликтных ситуаций КИТ Финанс (АО) (далее Порядок) определяет процесс разрешения конфликтных ситуаций, возникающих при использовании системы электронного документооборота КИТ Финанс (АО) (далее Общество).

1. Возникновение конфликтных ситуаций

1.1. В связи с осуществлением электронного документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах средств электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- не подтверждение подлинности электронных документов средствами проверки электронной подписи получателем;
- оспаривание факта формирования электронного документа;
- оспаривание факта идентификации (аутентификации) Владельца ключа электронной подписи, подписавшего документ;
- заявление Участника системы электронного документооборота об искажении электронного документа;
- оспаривание факта отправления и/или доставки электронного документа;
- оспаривание времени отправления и/или доставки электронного документа;
- иные случаи возникновения конфликтных ситуаций, связанных с функционированием системы электронного документооборота.

1.2. Конфликтная ситуация возникает также в случае, если Участник системы электронного документооборота:

- высказывает недоверие к составу и формату электронных документов, хранящихся в локальном архиве рабочего места Участника системы электронного документооборота;
- высказывает недоверие к программному обеспечению, функционирующему на его рабочем месте.

2. Уведомление о конфликтной ситуации

2.1. В случае возникновения конфликтной ситуации Сторона, предполагающая возникновение конфликтной ситуации, должна незамедлительно, но не позднее 3 (Трех) рабочих дней после возникновения конфликтной ситуации, направить уведомление о конфликтной ситуации другой Стороне.

2.2. Уведомление о предполагаемом наличии конфликтной ситуации должно содержать информацию о существовании конфликтной ситуации и обстоятельствах, которые, по мнению уведомителя, свидетельствуют о наличии конфликтной ситуации. В Уведомлении должны быть указаны фамилия, имя и отчество, должность, контактные телефоны, факс, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

2.3. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее 3 (Трех) рабочих дней, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить уведомителю информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

2.4. Общество в случае выявления предполагаемого наличия конфликтной ситуации с Участником системы электронного документооборота имеет право до разрешения конфликтной ситуации приостановить электронный документооборот с данным Участником.

3. Разрешение конфликтной ситуации в рабочем порядке

3.1. Конфликтная ситуация признается разрешенной в рабочем порядке в случае, если уведомитель удовлетворен информацией, полученной от Стороны, которой было направлено уведомление и в течение 3 (Трёх) рабочих дней, следующих за днем получения такой информации, не поступило письменного заявления о рассмотрении конфликтной ситуации технической комиссией.

3.2. В случае если уведомитель не удовлетворен информацией, полученной от Стороны, которой направлялось уведомление, для рассмотрения конфликтной ситуации формируется техническая комиссия.

4. Формирование технической комиссии, ее состав

4.1. Не позднее чем на следующий рабочий день после того, как принято решение о необходимости сформировать техническую комиссию, или не позднее, чем на пятый рабочий день после получения уведомления о конфликтной ситуации, в случае, если конфликтная ситуация не была урегулирована в рабочем порядке, техническая комиссия должна быть сформирована.

4.2. Если Общество и Участник системы электронного документооборота, являющиеся сторонами в конфликтной ситуации, не договорятся об ином, в состав технической комиссии входит равное количество, но не менее чем по одному уполномоченному представителю каждой из конфликтующих Сторон, в состав комиссии могут также включаться эксперты – представители разработчиков средств криптографической защиты информации.

4.3. Лица, входящие в состав технической комиссии, должны обладать необходимыми знаниями в области построения систем криптозащиты и работы компьютерных информационных систем.

4.4. Право представлять в технической комиссии Участника системы электронного документооборота или Общество должно подтверждаться доверенностью, оформленной надлежащим образом.

4.5. По инициативе любой из Сторон к работе технической комиссии для проведения технической экспертизы могут привлекаться независимые эксперты, с необходимым знаниями в области построения систем криптозащиты.

4.6. Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

5. Компетенция и полномочия технической комиссии

5.1. Сформированная техническая комиссия при рассмотрении конфликтной ситуации устанавливает на технологическом уровне наличие или отсутствие фактических обстоятельств, свидетельствующих о факте и времени составления и/или отправки электронного документа, его подлинности, а также о подписании электронного документа конкретной электронной подписью, аутентичности отправленного документа полученному.

5.2. Техническая комиссия вправе рассматривать любые иные технические вопросы, необходимые, по мнению технической комиссии, для выяснения причин и последствий возникновения конфликтной ситуации.

5.3. Техническая комиссия не вправе давать правовую или какую-либо иную оценку установленных ею фактов.

6. Базовая процедура работы технической комиссии

6.1. Порядок и процедура работы технической комиссии устанавливаются ее членами индивидуально для каждого случая.

6.2. Базовая процедура работы технической комиссии в случае разбора конфликтной ситуации с электронным документом, подписанным усиленной квалифицированной электронной подписью, состоит из следующих действий:

- Устанавливается принадлежность ключа электронной подписи, использованного при формировании электронной подписи оспариваемого электронного документа, Участнику системы электронного документооборота.

- Устанавливается действительность Сертификата ключа проверки электронной подписи Участника системы электронного документооборота, использованного при формировании электронной подписи оспариваемого электронного документа.

- Устанавливается подтверждение соответствия электронной подписи оспариваемого электронного документа электронной подписи Участника системы электронного документооборота, путем использования специальных сертифицированных средств электронной подписи, установленных на аттестованном по требованиям безопасности информации автоматизированном рабочем месте «АРМ-РКС».

- Протокол проверки электронной подписи распечатывается и подписывается всеми членами технической комиссии.

7. Протокол работы технической комиссии

7.1. Все действия, предпринимаемые технической комиссией для выяснения фактических обстоятельств, а также выводы, сделанные технической комиссией, заносятся в Протокол работы технической комиссии. Протокол работы технической комиссии должен содержать следующие данные:

- состав технической комиссии с указанием сведений о квалификации каждого из членов технической комиссии;
- краткое изложение обстоятельств возникшей конфликтной ситуации;
- мероприятия, проводимые технической комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты, времени и места их проведения;
- выводы, к которым пришла техническая комиссия в результате проведенных мероприятий;
- подписи всех членов технической комиссии.

7.2. В случае если мнение члена (или членов) технической комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов технической комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами комиссии), чье особое мнение отражает соответствующая запись.

7.3. Протокол составляется в одном подлинном экземпляре на бумажном носителе, который находится на хранении в Обществе. По требованию Участника системы электронного документооборота или любого из членов технической комиссии, им может быть выдана заверенная Обществом копия Протокола.

8. Акт по итогам работы технической комиссии

8.1. По итогам работы технической комиссии составляется Акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии Акт должен также содержать следующие данные:

- состав технической комиссии;
- дату и место составления Акта;
- даты и время начала и окончания работы технической комиссии;
- краткий перечень мероприятий, проведенных технической комиссией;
- подписи членов технической комиссии;
- указание на особое мнение члена (или членов технической комиссии), в случае наличия такового.

8.2. Количество экземпляров Акта устанавливается технической комиссией, по одному экземпляру которого передается каждой Стороне конфликтной ситуации.

8.3. К Акту может прилагаться особое мнение члена (или членов технической комиссии), не согласных с выводами технической комиссии, указанными в Акте. Особое мнение составляется в произвольной форме в таком же количестве подлинных экземпляров, что и Акт, и составляет приложение к Акту.

9. Претензионный и судебный порядок урегулирования конфликтной ситуации

9.1. Все споры и разногласия, которые могут возникнуть в связи с применением, нарушением, толкованием настоящего Порядка, признанием недействительными настоящего Порядка или их части, Стороны будут стремиться разрешить, используя механизмы согласительного урегулирования споров и разногласий.

9.2. В случае, если конфликтная ситуация не урегулирована в результате работы технической комиссии, либо в иной ситуации, если Участник системы электронного документооборота считает, что его права при осуществлении электронного документооборота были нарушены, он обязан направить Обществу претензию.

9.3. В случае недостижения согласия между Сторонами в результате исполнения обязательного рабочего и претензионного порядка разрешения возникающих споров и разногласий, все споры, связанные с заключением, обстоятельствами исполнения, нарушениями, расторжением и признанием недействительным электронного документа или норм настоящего Порядка подлежат рассмотрению в суде в соответствии с правилами о подсудности по месту нахождения Общества.

**Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ
Финанс (АО) физических лиц**

Настоящим _____ (далее – Заявитель)

*(ФИО полностью)**(паспортные данные, место регистрации)*

заявляет о своем полном и безусловном присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее также Компания, и обязуется соблюдать его условия и положения.

Подписание Заявителем настоящего Заявления и передача его Компании означает, что Заявитель ознакомился с Регламентом оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее – Регламент, определяющим условия издания криптографических ключей и сертификатов ключей проверки электронной подписи, в т.ч. рисками, связанными с использованием электронных подписей, а также обязуется соблюдать необходимые меры по обеспечению безопасности при использовании средств электронной подписи.

После подписания настоящего Заявления о присоединении Заявитель теряет право ссылаться на то, что он не ознакомился с Регламентом, либо не признаёт его условия.

Согласно условиям Регламента оказания услуг Удостоверяющего центра, КИТ Финанс (АО), прошу изготовить мне квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП) в соответствии со следующими идентификационными данными:

Область действия сертификата	
Фамилия, имя, отчество	
Дата рождения	
Паспортные данные (серия, №, кем и когда выдан, код подразделения)	
СНИЛС	
ИНН	
Адрес регистрации	
Номер телефона	
Адрес электронной почты	

С обработкой, передачей и хранением указанных мной персональных данных в целях изготовления, обслуживания и ведения реестра выданных и аннулированных сертификатов ключей проверки электронных подписей согласен.

Подпись Заявителя (уполномоченного лица): _____ / _____

Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО) индивидуального предпринимателя

Настоящим _____ (далее – Заявитель)

(ФИО индивидуального предпринимателя)

(ОГРНИП/Регистрационный номер)

– заявляет о своем полном и безусловном присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее также Компания, и обязуется соблюдать его условия и положения.

Подписание Заявителем настоящего Заявления и передача его Компании означает, что Заявитель ознакомился с Регламентом оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее – Регламент, определяющим условия издания криптографических ключей и сертификатов ключей проверки электронной подписи, в т.ч. рисками, связанными с использованием электронных подписей, а также обязуется соблюдать необходимые меры по обеспечению безопасности при использовании средств электронной подписи.

После подписания настоящего Заявления о присоединении Заявитель теряет право ссылаться на то, что он не ознакомился с Регламентом, либо не признаёт его условия.

Согласно условиям Регламента оказания услуг Удостоверяющего центра, КИТ Финанс (АО), прошу изготовить квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП) в соответствии со следующими идентификационными данными:

Область действия сертификата	
Фамилия, имя, отчество	
Дата рождения	
Паспортные данные (серия, №, кем и когда выдан, код подразделения)	
СНИЛС	
ИНН	
ОГРНИП	
Адрес регистрации	
Номер телефона	
Адрес электронной почты	

С обработкой, передачей и хранением указанных мной персональных данных в целях изготовления, обслуживания и ведения реестра выданных и аннулированных сертификатов ключей проверки электронных подписей согласен.

Подпись Заявителя (уполномоченного лица): _____ / _____

М.П.

**Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ
Финанс (АО) юридических лиц**

Настоящим _____ в лице _____

_____ далее – Заявитель)

(наименование, ФИО подписанта и на основании какого документа действует)

(ОГРН/Регистрационный номер)

– заявляет о своем полном и безусловном присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее также Компания, и обязуется соблюдать его условия и положения.

Подписание Заявителем настоящего Заявления и передача его Компании означает, что Заявитель ознакомился с Регламентом оказания услуг Удостоверяющего центра КИТ Финанс (АО), далее – Регламент, определяющим условия издания криптографических ключей и сертификатов ключей проверки электронной подписи, в т.ч. рисками, связанными с использованием электронных подписей, а также обязуется соблюдать необходимые меры по обеспечению безопасности при использовании средств электронной подписи.

После подписания настоящего Заявления о присоединении Заявитель теряет право ссылаться на то, что он не ознакомился с Регламентом, либо не признаёт его условия.

Согласно условиям Регламента оказания услуг Удостоверяющего центра, КИТ Финанс (АО), прошу изготовить квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП) в соответствии со следующими идентификационными данными:

Область действия сертификата	
Полное наименование Заявителя	
Фамилия, имя, отчество владельца сертификата	
Дата рождения	
Паспортные данные (серия, №, кем и когда выдан, код подразделения)	
СНИЛС	
ИНН	
ОГРН	
Юридический адрес	
Подразделение	
Должность	
Номер телефона	
Адрес электронной почты	

С обработкой, передачей и хранением указанных мной персональных данных в целях изготовления, обслуживания и ведения реестра выданных и аннулированных сертификатов ключей проверки электронных подписей согласен.

Подпись владельца КСКПЭП: _____ / _____

Подпись Заявителя (уполномоченного лица): _____ / _____ М.П

Заявление об аннулировании (отзыве) сертификата ключа проверки электронной подписи

" ____ " _____ 20__ г.

В соответствии с Регламентом оказания услуг УЦ КИТ Финанс (АО) прошу аннулировать и внести в реестр аннулированных сертификатов, квалифицированный сертификат ключа проверки электронной подписи (КСКПЭП), идентифицируемый перечисленными ниже параметрами:

Серийный номер КСКПЭП	ФИО Владельца КСКПЭП	Дата выдачи КСКПЭП

использовавшийся _____
(полное наименование юридического лица)

в связи с *(отметить нужное или указать иную причину)*:

- Компрометацией ключа ЭП
- Прекращением полномочий Владельца КСКПЭП
- Изменением сведений, указанных в КСКПЭП
- Физической порчей ключевого носителя
- Иное _____

Подпись Владельца КСКПЭП: _____ / _____
(подпись) (Фамилия И.О.)

Подпись руководителя:

_____ / _____
(должность) (подпись) (Фамилия И.О.)

М.П.

В настоящем документе прошито,
пронумеровано и скреплено печатью 22
(Двадцать два) листа «16» января 2019г.



Генеральный директор КИТ Финанс (АО)

Ю. А. Лазаренко

(Ю.А. Лазаренко)