Утверждён Приказом

Генерального директора

КИТ Финанс (АО)

№23-1 от 17.05.2021 г.

Ю.А. Сычев

РЕГЛАМЕНТ

ОКАЗАНИЯ УСЛУГ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

КИТ ФИНАНС (АО)

Санкт-Петербург, 2021 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 соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

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

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

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

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 (далее – 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.

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 функции по созданию и выдаче сертификатов ключей проверки электронных подписей и иные функции удостоверяющего центра 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 электронных подписей, 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 Предмет регулирования

1.1.1 Настоящий Регламент оказания услуг Удостоверяющего центра КИТ Финанс (АО) (далее – Регламент) определяет порядок реализации функций и исполнения обязанностей Удостоверяющего центра КИТ Финанс (АО) (далее – Общества).

1.1.2 Предметом регулирования настоящего Регламента являются условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, а также правила пользования услугами Удостоверяющего центра.

1.1.3 Нормы, содержащиеся в Регламенте, обязательны для всех Заявителей, обратившихся за получением сертификатов ключей проверки усиленной неквалифицированной или усиленной квалифицированной электронной подписи.

1.1.4 Настоящий 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.

1.1.5 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.

1.1.6 Настоящий Регламент располагается в информационно-телекоммуникационной сети Интернет по адресу: https://brokerkf.ru/doc/uc/reglament_uc.pdf.

1.2 Сведения об Удостоверяющем центре

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

1.2.2 Реквизиты Удостоверяющего центра:

ОГРН: 1167847466742 ИНН: 7840060671

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

1.2.3 Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании:

- Свидетельства об аккредитации Удостоверяющего центра № 716/1 от 06.09.2018 г., выданного Министерством связи и массовых коммуникаций Российской Федерации;
- Лицензии Управления Федеральной службы безопасности Российской Федерации по городу Санкт-Петербургу и Ленинградской области 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).

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

1.2.5 График работы: пн. – пт.: 9:00 – 18:00 (время московское), сб. – вс.: выходной

1.3 Порядок информирования о предоставлении услуг Удостоверяющего центра

1.3.1 Информирование о предоставлении услуг Удостоверяющего центра осуществляется следующими способами:

- по номеру телефона: 812-332-32-66, 8-800-700-00-55
- по адресу электронной почты: uc@brokerkf.ru
- путем опубликования информации на сайте Удостоверяющего центра https://brokerkf.ru/certificate-authority/.

1.3.2 Заявители вправе получить информацию по вопросам предоставления услуг Удостоверяющего центр, обратившись в Удостоверяющий центра одним из указанных в п. 1.3.1 настоящего Регламента способов, либо самостоятельно ознакомившись с информацией, размещенной на сайте Удостоверяющего центра.

1.4 Стоимость услуг Удостоверяющего центра

1.4.1 Услуги удостоверяющего центра могут оказываться на платной основе.

1.4.2 Сроки, порядок расчётов и тарифы за оказание услуг Удостоверяющего центра публикуются на сайте Удостоверяющего центра.

1.4.3 Сроки и порядок расчётов за оказание услуг Удостоверяющего центра могут быть изменены по согласованию с Заявителем.

1.4.4 Размер платы за услуги Удостоверяющего центра не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ).

2.1 Удостоверяющий центр предоставляет услуги по изготовлению и выдаче Сертификатов для усиленной неквалифицированной электронной подписи и усиленной квалифицированной электронной подписи, а также услуги, связанные с использованием средств электронной подписи.

2.2 Деятельность Удостоверяющего центра направлена на достижение следующих целей:

2.2.1 Обеспечение юридически значимого документооборота при обмене электронными документами между Обществом и участниками системы электронного документооборота Общества;

2.2.2 Обеспечение юридически значимого документооборота при обмене электронными документами между Владельцами сертификатов и другими участниками электронного взаимодействия;

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

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

2.3 Функции Удостоверяющего центра:

2.3.1 Создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов Заявителям (Владельцам сертификатов) при условии установления личности получателя Сертификата (Заявителя) либо полномочия лица, выступающего от имени Заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с п. 4 ч. 4 ст.8 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

2.3.2 Осуществление подтверждения владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения Сертификата;

2.3.3 Установление сроков действия Сертификатов.

2.3.4 Аннулирование выданных Удостоверяющим центром Сертификатов.

2.3.5 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.

2.3.6 Ведение Реестра выданных и аннулированных Удостоверяющим центром Сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных Удостоверяющим центром Сертификатах и информацию о датах прекращения действия или аннулирования Сертификатов и об основаниях таких прекращения или аннулирования.

2.3.7 Установление порядка ведения Реестра сертификатов, не являющихся квалифицированными, и порядка доступа к нему, а также обеспечение доступа лиц к информации, содержащейся в Реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет"

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

2.3.9 Проверка уникальности ключей проверки электронной подписи в Реестре сертификатов.

2.3.10 Осуществление по обращениям участников электронного взаимодействия проверки электронных подписей.

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

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

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

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

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

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1 Удостоверяющий центр обязан:

3.1.1 Информировать Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

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 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.

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 Обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей, при необходимости обеспечить уничтожение ключей электронных подписей в максимально короткие сроки.

3.1.7 Отказать Заявителю в создании Сертификата в случае, если не было подтверждено, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения Сертификата.

3.1.8 Отказать Заявителю в создании Сертификата в случае отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения Сертификата.

3.1.9 Не указывать в создаваемом им Сертификате ключ проверки электронной подписи, который содержится в Сертификате, выданном этому Удостоверяющему центру любым другим удостоверяющим центром.

3.1.10 Вносить информацию о выданном Сертификате в Реестр сертификатов не позднее указанной в нём даты начала действия такого сертификата.

3.1.11 Вносить информацию о прекращении действия Сертификата в Реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие Сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

3.1.12 Хранить в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации следующую, следующую информацию:

- реквизиты основного документа, удостоверяющего личность Владельца квалифицированного сертификата - физического лица;
- сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени Заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
- сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия Владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях Владельца квалифицированного сертификата включена в квалифицированный сертификат.

Хранение указанной в настоящем пункте информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.1.13 Для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном Удостоверяющему центру головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. Удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания Сертификатов, не являющихся квалифицированными сертификатами

3.1.14 Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к Реестру квалифицированных сертификатов этого аккредитованного удостоверяющего центра в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

3.1.15 В случае принятия решения о прекращении своей деятельности:

- сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;
- передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным Удостоверяющим центром квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре. Ключи электронной подписи, хранимые аккредитованным Удостоверяющим центром по поручению Владельцев квалифицированных сертификатов электронной подписи, подлежат уничтожению в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности.

3.1.16 В случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам уведомить об этом в письменной форме Владельцев сертификатов, которые выданы этим Удостоверяющим центром и срок действия которых не истек. Удостоверяющий центр должен направить уведомление не менее чем за один месяц до даты прекращения деятельности Удостоверяющего центра.

3.1.17 В случае прекращения деятельности Удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме Владельцев сертификатов, которые выданы этим Удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций.

3.1.18 Обязан выполнять настоящий Регламент оказания услуг Удостоверяющего центра КИТ Финанс (АО) в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с требованиями Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с действующем законодательством Российской Федерации об электронной подписи.

3.1.19 Не наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени такого аккредитованного Удостоверяющего центра.

3.1.20 Выдавать квалифицированный сертификат в форме, требования к которой устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности по согласованию с уполномоченным федеральным органом.

3.1.21 При выдаче квалифицированного сертификата в порядке, установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», идентифицировать Заявителя - физическое лицо, обратившееся в Удостоверяющий центр за получением квалифицированного сертификата.

3.1.22 Получить от лица, выступающего от имени Заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

3.1.23 С использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных Заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

3.1.24 При получении квалифицированного сертификата Заявителем ознакомить Заявителя (Владельца сертификата) с информацией, содержащейся в квалифицированном сертификате. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление Заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

3.1.25 Одновременно с выдачей квалифицированного сертификата должен предоставить Владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

3.1.26 При выдаче квалифицированного сертификата направлять в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

3.1.27 При выдаче квалифицированного сертификата Удостоверяющий центр по желанию Владельца квалифицированного сертификата безвозмездно осуществлять его регистрацию в единой системе идентификации и аутентификации с проведением идентификации Владельца при его личном присутствии.

3.1.28 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.

3.2 Удостоверяющий центр имеет право:

3.2.1 Наделить третьих лиц полномочиями по приему заявлений на выдачу Сертификатов, а также вручению Сертификатов от имени Удостоверяющего центра.

3.2.2 Выдавать Сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе.

3.2.3 Отказать Заявителю в регистрации в Удостоверяющем центре и выдаче Сертификата в случае непредставления необходимых документов либо их ненадлежащего оформления, предоставлении документов не в полном объёме или вызывающих сомнение в их подлинности.

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

3.2.5 Отказать в изготовлении Сертификата в случае невыполнения Заявителем обязанностей, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами и настоящим Регламентом.

3.2.6 Отказать в изготовлении Сертификата, если предоставленные Заявителем сведения не прошли проверку в соответствии с пп. 2.2-2.3 ст. 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

3.2.7 Отказать в выдаче Сертификата в случае, если Заявитель – физическое лицо или Уполномоченный представитель Заявителя не предоставил письменного согласия на обработку своих персональных данных.

3.2.8 Аннулировать Сертификат Владельца, если Удостоверяющему центру стало известно, что Владелец сертификата не владеет ключом электронной подписи, соответствующему ключу проверки электронной подписи, указанному в таком Сертификате.

3.2.9 Аннулировать Сертификат в случае вступления в силу решения суда, которым, в частности, установлено, что Сертификат содержит недостоверную информацию.

3.2.10 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.

3.2.11 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.

3.2.12 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.

3.2.13 Не принимать от Заявителя документы, не соответствующие требованиям законодательства Российской Федерации.

3.3 Ответственность Удостоверяющего центра

3.3.1 Удостоверяющий центр (работники Удостоверяющего центра, доверенные лица и их работники) несёт гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

3.3.2 Удостоверяющий центр в соответствии с законодательством Российской Федерации несёт ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющего центра;

- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных действующим законодательством и настоящим Регламентом.

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

3.3.4 Удостоверяющий центр не несет ответственность за невозможность использования Сертификата в случае если такая невозможность возникла после создания Сертификата и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

3.4 Заявитель обязан:

3.4.1 Предоставить в Удостоверяющий центр документы, предусмотренные Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами и настоящим Регламентом.

3.4.2 Присоединиться к настоящему Регламенту (заключить Договор об электронном документообороте), предоставив подписанное Заявление о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО).

3.4.3 Предоставить в Удостоверяющий центр документы, содержащую актуальную и достоверную информацию и оформленные надлежащим образом.

3.4.4 Своевременно произвести оплату услуг по созданию и выдаче Сертификата.

3.5 Владелец сертификата обязан:

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

3.5.2 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.

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

3.5.4 Использовать ключи электронной подписи 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;

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

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

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

3.5.8 Не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр для прекращения действия Сертификата в случае потери, раскрытия, искажения ключа электронной подписи, а также при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

3.5.9 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.

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

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

3.5.12 Предоставлять в Удостоверяющий центр только достоверную информацию.

3.5.13 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 электронной подписи третьими лицами и их использованием в системе электронного документооборота от лица владельца ключей электронной подписи.

3.6 Владелец сертификата имеет право:

3.6.1 Получить реестр аннулированных Сертификатов, изготовленный Удостоверяющим центром.

3.6.2 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.

3.6.3 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.

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

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

3.6.6 Применять реестр аннулированных Сертификатов Удостоверяющего центра для подтверждения действительности своего Сертификата.

3.6.7 Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию Сертификата на бумажном носителе, заверенную удостоверяющим центром.

4. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

4.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей

4.1.1 Порядок создания ключей электронных подписей и ключей проверки электронных подписей Удостоверяющий центр оказывает услуги по созданию Сертификатов только после:

- 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;

- присоединения Заявителей к настоящему Регламенту в порядке, установленном пп. 1.1.4-1.1.5 настоящего Регламента - в случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом.

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется одним из следующих способов:

1) Заявители, имеющие договор на брокерское обслуживание с Обществом, создают ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. N 173 "О внесении изменений в некоторые нормативные правовые акты ФСБ России" (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350).

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

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,

2) В случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом Удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи для Заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)".

В случае отсутствия у Заявителя договора на брокерское обслуживание с Обществом процедура создания ключа электронной подписи и ключа проверки электронной подписи выполняется на основании заранее полученного заявления о присоединении к настоящему Регламенту с указанием всех параметров ключа электронной подписи и оплаченного счёта в соответствии с тарифами, опубликованными на сайте Удостоверяющего центра. Созданные ключи записываются на ключевой носитель, приобретенный участником электронного взаимодействия в соответствии с Заявлением или предоставляемый самим Заявителем.

Предоставляемый Заявителем ключевой носитель должен иметь поддерживаемый тип устройства, не содержать никакой информации (инициализирован). Удостоверяющий центр имеет право не принимать для записи ключевой информации ключевые носители, не удовлетворяющие указанным требованиям.

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона "Об электронной подписи" создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также необходимость выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для Заявителя.

4.1.2 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, порядок информирования Владельцев сертификатов об осуществлении такой смены

Плановая смена ключей электронной подписи Удостоверяющего Центра выполняется в период действия ключа электронной подписи Удостоверяющего центра.

Плановая смена ключей электронной подписи производится по следующим основаниям:

- истечение срока действия ключа электронной подписи;

- переход на использование новых стандартов электронной подписи и функции хеширования в соответствии с требованиями, установленными органом исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей электронной подписи осуществляется в течение одного рабочего дня в следующем порядке:

1. Уполномоченное лицо Удостоверяющего центра формирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
2. В случае создания Удостоверяющим центром ключа электронной подписи для подписания от своего имени неквалифицированных сертификатов Уполномоченное лицо Удостоверяющего центра изготавливает Сертификат и подписывает его созданным ключом электронной подписи.
3. В случае создания Удостоверяющим центром Ключа электронной подписи для подписания от своего имени квалифицированных сертификатов Уполномоченное лицо направляет соответствующее заявление и запрос на Сертификат в головной удостоверяющий центр, функции которого осуществляет уполномоченный федеральный орган. Головной удостоверяющий центр создаёт квалифицированный сертификат и вручает его Удостоверяющему центру.

Информирование Владельцев сертификатов об осуществлении смены ключа электронной подписи Удостоверяющего центра производится посредством размещения на сайте Удостоверяющего центра соответствующей информации с возможностью скачивания нового Сертификата, как доверенного способа его получения.

4.1.3 Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности

Внеплановая смена ключей электронной подписи производится по следующим основаниям:

- нарушение конфиденциальности ключа электронной подписи
- угроза нарушения конфиденциальности такого ключа электронной подписи.

Процедура внеплановой смены ключей Удостоверяющего центра осуществляется в порядке, предусмотренным для процедуры плановой смены ключей Удостоверяющего центра.

Одновременно со сменой такого ключа электронной подписи прекращается действие всех Сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих Сертификатах в реестр сертификатов.

Информирование Владельцев сертификатов об осуществлении смены ключа электронной подписи Удостоверяющего центра производится посредством размещения на сайте Удостоверяющего центра соответствующей информации с возможностью скачивания нового Сертификата, как доверенного способа его получения.

К случаям нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра относятся события, включая, но не ограничиваясь:

- потеря/хищение ключевого носителя
- несанкционированный доступ к месту хранения ключевого носителя
- нарушение правил хранения ключевого носителя.

К угрозам нарушения конфиденциальности ключа электронной подписи относятся следующие виды угроз:

- угрозы, вызванные действиями работников Удостоверяющего центра
- угрозы, вызванные действиями внешних нарушителей
- угрозы, вызванные стихийными явлениями или объективными физическими процессами.

4.1.4 Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Владельца сертификата

Смена ключа электронной подписи Владельца сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Смена ключа электронной подписи Владельца сертификата осуществляется по заявлению Владельца о смене ключа электронной подписи, которое может быть подано как в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, так и на бумажном носителе.

В случае, если смена ключа электронной подписи Владельца сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью Владельца сертификата.

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

Процедура выдачи Сертификата и ключа электронной подписи (при необходимости) осуществляется в соответствии со статьей 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

4.2 Процедура создания и выдачи Сертификатов

4.2.1 Порядок подачи и требования к заявлению на создание и выдачу квалифицированных сертификатов

Создание квалифицированного сертификата ключа проверки электронной подписи осуществляется на основании Заявления о присоединении к Регламенту оказания услуг Удостоверяющего центра КИТ Финанс (АО) (далее - Заявление о присоединении к Регламенту), которое может быть подано как в форме электронного документа, подписанного усиленной квалифицированной электронной подписью, так и на бумажном носителе.

Заявление о присоединении к Регламенту оформляется по формам Приложений №№ 2, 3, 4.

4.2.2 Порядок идентификации Заявителя

Идентификация Заявителя-физического лица и лица, выступающего от имени Заявителя - юридического лица осуществляется:

1. При личном присутствии:
   - гражданина Российской Федерации по основному документу, удостоверяющему личность
   - гражданина иностранного государства по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства
   - беженца, вынужденного переселенца и лица без гражданства по документу, установленному законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.
2. Без личного присутствия с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, принадлежащего лицу, личность которого устанавливается.

4.2.3 Перечень документов, запрашиваемых Удостоверяющим центром у Заявителя, для создания и выдачи квалифицированного сертификата

При обращении в Удостоверяющий центр для изготовления и выдачи квалифицированного сертификата Заявитель предоставляет документы либо их надлежащим образом заверенные копии и (или) сведения из них в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», а именно:

- основной документ, удостоверяющий личность
- страховой номер индивидуального лицевого счета заявителя - физического лица
- идентификационный номер налогоплательщика заявителя - физического лица
- основной государственный регистрационный номер заявителя - юридического лица
- основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя
- 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
- документ, подтверждающий право Заявителя действовать от имени юридического лица.

Если для подтверждения каких-либо сведений, вносимых в Сертификат, действующим законодательством или настоящим Регламентом установлена определенная форма документа, Заявитель представляет в Удостоверяющий центр документ соответствующей формы.

Все документы на иностранном языке должны иметь заверенный перевод на русский язык.

4.2.4 Порядок проверки достоверности документов и сведений, представленных Заявителем

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи». В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в Сертификат, и Удостоверяющим центром установлена личность Заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени Заявителя – юридического лица, Удостоверяющий центр осуществляет процедуру создания и выдачи Заявителю квалифицированного сертификата. В ином случае Удостоверяющий центр отказывает Заявителю в выдаче квалифицированного сертификата.

4.2.5 Порядок создания квалифицированного сертификата

Создание квалифицированного сертификата выполняется сотрудниками Удостоверяющего центра в офисе Общества на основании заранее полученного Заявления о присоединении к Регламенту с указанием всех параметров Сертификата и оплаченного счёта в соответствии с тарифами, опубликованными на сайте Удостоверяющего центра. Проводится проверка сведений, указанных в Заявлении о присоединении к Регламенту, и представленных документов. В случае подтверждения достоверности сведений Удостоверяющий центр записывает ключ электронной подписи и Сертификат на ключевой носитель, приобретенный Заявителем в соответствии с Заявлением о присоединении к Регламенту или предоставленный самим Заявителем.

Информация о Сертификате вносится в Реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

Срок действия Сертификата составляет 12 месяцев.

4.2.6 Порядок выдачи квалифицированного сертификата

При выдаче квалифицированного сертификата личность Заявителя устанавливается по основному документу, удостоверяющему личность в соответствии с законодательством Российской Федерации. При личном обращении в офис Общества Заявителям выдаются записанные на ключевой носитель сертификат ключа проверки электронной подписи, соответствующего ключу электронной подписи, копия Сертификата на бумажном носителе с подтверждением ознакомления с информацией, содержащейся в Сертификате, под расписку. Одновременно с выдачей квалифицированного сертификата Владельцу квалифицированного сертификата предоставляется руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При выдаче квалифицированного сертификата Удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

4.2.7 Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром соответствующего Заявления, а также условия для срочного создания и выдачи квалифицированного сертификата Заявителю

Создание и выдача квалифицированного сертификата производятся в течение трёх рабочих дней с момента подачи Заявления о присоединении и получения сведений из государственных информационных ресурсов, при условии подтверждения всех предоставленных сведений и документов и соблюдения порядка оплаты за услуги. Срочные создание и выдача Сертификата возможны в течение двух часов с момента подачи Заявления о присоединении и получения сведений из государственных информационных ресурсов при условии подтверждения всех предоставленных сведений и оплаченного счета.

4.2.8 Порядок создания и выдачи неквалифицированных Сертификатов

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.

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

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

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.

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

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.

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

Заявителям, имеющим договор на брокерское обслуживание с Обществом, выпуск Сертификатов для работы в сторонних системах электронного документооборота осуществляется на платной основе, в соответствии с тарифами, опубликованными на сайте Общества https://brokerkf.ru/.

4.3 Подтверждение действительности электронной подписи, использованной для подписания электронных документов

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

Подтверждение электронной подписи осуществляется на основании Заявления, оформленного в свободной форме.

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.

Процедура проверки всех Сертификатов осуществляется Уполномоченными сотрудниками Удостоверяющего центра с использованием сертифицированных СКЗИ в течение десяти рабочих дней с момента поступления Заявления.

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

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

4.4 Процедуры, осуществляемые при прекращении действия и аннулирования Сертификата

4.4.1 Основания прекращения действия или аннулирования Сертификата

Сертификат прекращает свое действие в случаях, установленных статьёй 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

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 от 06.04.2011 N 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между Удостоверяющим центром и Владельцем сертификата.
- 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.

4.4.2 Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) Сертификата

Аннулирование (отзыв) Сертификата осуществляется по заявлению его Владельца, подающемуся в Удостоверяющий центр в соответствии с Приложением 5 настоящего Регламента в бумажной или электронной форме, подписанное действующей усиленной квалифицированной подписью.

Рассмотрение заявлений, в том числе представленных в электронном виде, осуществляется в течение рабочего дня Удостоверяющего центра.

Аннулирование (отзыв) Сертификата осуществляется после подтверждения полномочий Владельца сертификата или доверенного лица путем идентификации при личной явке либо проверки действительности усиленной квалифицированной электронной подписи, которой подписано заявление.

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 внесен этот Сертификат.

Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификата составляет не более двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.

4.4.3 Приостановление действия Сертификата

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.

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

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

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

4.4.4 Возобновление действия Сертификата

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

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.

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

4.5 Порядок ведения Реестра сертификатов

4.5.1 Формы ведения Реестра сертификатов

Формирование и ведение Реестра сертификатов осуществляется в порядке, установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», в течение всего срока деятельности Удостоверяющего центра. Реестр сертификатов Удостоверяющего центра ведётся в формате электронной базы данных.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов.

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

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

4.5.2 Сроки внесения информации о прекращении действия или аннулирования Сертификата в Реестр сертификатов

Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификата составляет не более двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.

Действие Сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

4.6 Порядок технического обслуживания Реестра сертификатов

Доступ к Реестру сертификатов обеспечивается круглосуточно, за исключением периодов планового или внепланового обслуживания. Плановое и внеплановое обслуживание осуществляются в максимально короткие сроки, но не должно превышать четырёх часов.

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

5. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

5.1 Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

Информирование Заявителей проводится одновременно с выдачей квалифицированного сертификата Владельцу квалифицированного сертификата посредством предоставления руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, а также путём размещения рекомендаций по соблюдению информационной безопасности на сайте Удостоверяющего центра.

5.2 Выдача по обращению Заявителя средств электронной подписи

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

5.3 Обеспечение актуальности информации, содержащейся в Реестре квалифицированных сертификатов, и ее защита от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов путем соблюдения сроков внесения сведений о прекращении действия и/или аннулировании Сертификатов, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий достигается путем:

- использования технических средств защиты информации;
- ограничения доступа в помещения, где размещены аппаратные средства УЦ;
- идентификации, аутентификации и разграничения доступа пользователей и обслуживающего персонала к программным средствам УЦ и защищаемой информации.

5.4 Обеспечение доступности Реестра сертификатов

Доступ к Реестру сертификатов в информационно-телекоммуникационной сети «Интернет» обеспечивается круглосуточно, за исключением периодов планового или внепланового технического обслуживания.

5.5 Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронной подписи

Процедура создания ключей электронной подписи выполняется сотрудниками Удостоверяющего центра с использованием аттестованного автоматизированного рабочего места, размещенного в помещении Общества, доступ в которое ограничен. Ключи создаются в единственном экземпляре и записываются на ключевой носитель, который передаётся Заявителю.

Одновременно с выдачей Сертификата до Владельца доводится информация о безопасном использовании средств электронной подписи.

Владелец сертификата обязан обеспечивать конфиденциальность ключа электронной подписи и не допускать использование принадлежащего ему ключа электронной подписи без его согласия.

В случае нарушения конфиденциальности ключа электронной подписи, а также в случаях наличия оснований полагать, что конфиденциальность ключа электронной подписи была нарушена, Владелец сертификата должен прекратить использование этого ключа и уведомить Удостоверяющий центр.

Удаление ключей электронной подписи производится путём форматирования ключевых носителей. Срок уничтожения Владелец сертификата устанавливает самостоятельно.

5.6 Осуществление регистрации квалифицированного сертификата и лица, которому выдан квалифицированный сертификат, в единой системе идентификации и аутентификации

В соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» при выдаче квалифицированного сертификата Удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате, а также по желанию Владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации Владельца при его личном присутствии.

5.7 Предоставление доступа к Реестру сертификатов

Удостоверяющий центр безвозмездно посредством информационно-телекоммуникационной сети "Интернет" предоставляет любому лицу доступ к информации, содержащейся в Реестре сертификатов, в том числе информацию об аннулировании или о прекращении действия Сертификата.

Перечень прекративших свое действие (аннулированных) сертификатов публикуется на сайте Удостоверяющего центра.

6. ПРОЧИЕ УСЛОВИЯ

6.1 Конфиденциальность

6.1.1 Удостоверяющий центр обеспечивает конфиденциальность персональных данных, вносимых в Реестр сертификатов.

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

6.2 Прекращение оказания услуг Удостоверяющим центром.

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

6.3 Порядок изменения Регламента и прекращения действия Регламента (Договора об электронном документообороте)

6.3.1 Общество имеет право вносить изменения в настоящий Регламент в одностороннем порядке, о чем Общество обязано сообщить не позднее, чем за пять календарных дней до даты введения в действие изменений путем размещения указанных изменений и дополнений на сайте Удостоверяющего центра.

6.3.2 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).

6.3.3 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 Тридцать календарных дней до предполагаемой даты прекращения.

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

Приложение № 1

к Регламенту оказания услуг

Удостоверяющего центра КИТ Финанс (АО)

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 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 существе 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, адрес электронной почты лица или лиц, уполномоченных вести переговоры по урегулированию конфликтной ситуации.

2.3. Сторона, которой направлено уведомление, обязана незамедлительно, однако не позднее 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 трех 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 необходимыми 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.

Приложение № 2

к Регламенту оказания услуг

Удостоверяющего центра КИТ Финанс (АО)

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):_ _____/_____

Приложение № 3

к Регламенту оказания услуг

Удостоверяющего центра КИТ Финанс (АО)

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.

Приложение № 4
к Регламенту оказания услуг
Удостоверяющего центра КИТ Финанс (АО)

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

Приложение № 5

к Регламенту оказания услуг

Удостоверяющего центра КИТ Финанс (АО)

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.