Приложение № 5 к Агентскому договору
№ ДВ-2020/19 от «01» июня 2020 г.
(в ред. ДС №1 от 01.07.2020)

РЕГЛАМЕНТ
Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»
(порядок реализации функций аккредитованного
удостоверяющего центра и исполнения его обязанностей)

1. ОПРЕДЕЛЕНИЯ

1.1. Понятия и термины гражданского, налогового законодательства, законодательства в сфере электронной подписи, других отраслей законодательства Российской Федерации, используемые в настоящем Регламенте, применяются в том значении, в каком они используются в этих отраслях законодательства, федеральных законах, если иное не предусмотрено настоящим Регламентом.

1.2. В настоящем Регламенте используются следующие термины с соответствующими определениями:

1.2.1. **Бланк сертификата ключа проверки электронной подписи (бланк сертификата)** – документ на бумажном носителе или электронный документ, содержательная часть которого соответствует содержательной части сертификата ключа проверки электронной подписи.

1.2.2. **Владелец сертификата ключа проверки электронной подписи (владелец сертификата)** – лицо, которому в установленном Федеральным законом от 6 апреля 2011 №63-ФЗ «Об электронной подписи» и настоящим Регламентом порядке выдан сертификат ключа проверки электронной подписи.

1.2.3. **Внеплановая смена ключей ЭП (сертификата)** – замена ключей ЭП (сертификата) в связи с компрометацией, изменением информации, внесенной в сертификат, или после окончания срока их действия.

1.2.4. **Доверенное лицо УЦ** – физическое лицо, юридическое лицо или индивидуальный предприниматель, наделенные УЦ полномочиями по вручению сертификатов от имени УЦ, и исполняющие свои обязанности в соответствии с требованиями настоящего Регламента. Доверенным лицом УЦ могут стать лица, с которыми УЦ заключит соответствующий договор. Порядок заключения договора определяется по взаимному соглашению сторон и не является предметом регулирования Регламента.

1.2.5. **Единая система идентификации и аутентификации** - федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации, и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

1.2.6. **Запрос сертификата** - электронный документ, содержащий ключ проверки ЭП с параметрами алгоритма, сведения о владельце ключа проверки ЭП и дополнительные данные о владельце ключа проверки ЭП.

1.2.7. **Заявитель** – юридическое лицо независимо от организационно – правовой формы, физическое лицо или иной хозяйствующий субъект (в том числе индивидуальный предприниматель, адвокат, нотариус и т.д.), обращающиеся в УЦ для получения квалифицированного сертификата. После создания сертификата заявитель становится владельцем сертификата.

1.2.8. **Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат, сертификат)** – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 №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.

1.2.9. **Ключ проверки электронной подписи (ключ проверки ЭП)** – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

1.2.10. **Ключ электронной подписи (ключ ЭП)** – уникальная последовательность символов, предназначенная для создания электронной подписи.

1.2.11. **Ключ электронной подписи Удостоверяющего центра (ключ ЭП УЦ)** - ключ ЭП, использующийся УЦ для создания сертификатов ключей проверки ЭП и списков отозванных сертификатов.

1.2.12. **Компрометация ключа ЭП** - утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации (утеря носителя ключа ЭП или ключа ЭП (стирание, уничтожение с физического носителя), физическая порча носителя ключа ЭП, получение к ключу ЭП доступа третьих лиц, передача ключа ЭП по открытым каналам связи, например, по электронной почте, и прочее).

1.2.13. **Общество** - Общество с ограниченной ответственностью «ЭТП ГПБ Консалтинг» (ООО «ЭТП ГПБ Консалтинг»), ОГРН 5167746487651, ИНН 7728356929.

1.2.14. **Оператор Удостоверяющего центра (оператор УЦ)** – работник УЦ, наделенный полномочиями по осуществлению действий по регистрации, управлению и выдаче сертификатов ключей проверки ЭП, иными функциями и полномочиями, указанными в Регламенте.

1.2.15. **Плановая смена ключей ЭП/сертификата** - замена ключей ЭП или сертификата ключа проверки ЭП до окончания срока их действия.

1.2.16. **Рабочий день Удостоверяющего центра (рабочий день УЦ)** – промежуток времени с 09:00 по 18:00 по московскому времени, за исключением выходных и праздничных дней согласно законодательству Российской Федерации.

1.2.17. **Регламент Удостоверяющего центра (Регламент)** – настоящий Регламент, предусматривающий порядок реализации функций аккредитованного УЦ и исполнения его обязанностей, включая права, обязанности, ответственность Сторон Регламента, принятые форматы данных, основные организационно-технические мероприятия, направленные на обеспечение безопасной работы УЦ.

1.2.18. **Реестр сертификатов ключей проверки электронных подписей (реестр сертификатов)** – реестр выданных и аннулированных УЦ квалифицированных сертификатов ключей проверки ЭП, в том числе включающий в себя информацию, содержащуюся в выданных УЦ сертификатах, и информацию о датах прекращения действия или аннулирования сертификатов, а также об основаниях прекращения действия или аннулирования сертификатов.

1.2.19. **Реестр УЦ** - набор документов УЦ в электронной и/или бумажной форме, включающий следующую информацию:

- реестр заявлений на создание и выдачу сертификата ключа проверки электронной подписи;
- реестр заявлений на создание сертификата ключа проверки электронной подписи для сервера;
- реестр доверенностей на представителя индивидуального предпринимателя или юридического лица, данные которого указываются в сертификате;
- реестр доверенностей на вручение и получение документов в УЦ ООО «ЭТП ГПБ Консалтинг» представителем индивидуального предпринимателя или юридического лица;
- реестр заявлений на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр изготовленных списков отозванных сертификатов.

1.2.20. **Сайт УЦ** – официальная страница УЦ, размещенная в сети Интернет по адресу: https://ca.etpgpb.ru и содержащая информацию об УЦ, об услугах УЦ и их стоимости, инструкции и пояснения для заявителей и владельцев сертификатов, другую

информацию, необходимую к опубликованию в соответствии с порядком реализации функций УЦ и исполнения его обязанностей.

1.2.21. **Сертификат ключа проверки электронной подписи (сертификат, сертификат ЭП, квалифицированный сертификат)** - электронный документ или документ на бумажном носителе, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП. Формат сертификата ключа проверки ЭП, создаваемого УЦ ООО «ЭТП ГПБ Консалтинг», соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 г. N 795 "Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи" и рекомендациям IETF RFC 5280.

1.2.22. **Сертификат ключа проверки электронной подписи Удостоверяющего центра (сертификат ЭП УЦ)** - сертификат ключа проверки ЭП, использующийся для проверки УЦ в созданных им сертификатах ключей проверки ЭП и списка отозванных сертификатов.

1.2.23. **Система межведомственного электронного взаимодействия** – инфраструктура, обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

1.2.24. **Список отозванных сертификатов** – электронный документ с электронной подписью УЦ, включающий в себя список серийных номеров сертификатов ключей проверки ЭП, которые на определенный момент времени были аннулированы или прекратили свое действие.

1.2.25. **Средства электронной подписи (средства ЭП)** – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП, и соответствующие требованиям к средствам электронной подписи, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра». УЦ ООО «ЭТП ГПБ Консалтинг» поддерживает использование сертифицированных средств ЭП производства ООО «КРИПТО-ПРО».

1.2.26. **Средства УЦ** - программное и (или) аппаратное средство, используемое УЦ для выполнения своих функций и соответствующее требованиям к средствам удостоверяющего центра, утверждённым Приказом ФСБ России от 29.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра».

1.2.27. **Стороны Регламента (Стороны)** – юридическое или физическое лицо, индивидуальный предприниматель, присоединившиеся к Регламенту в установленном Регламентом порядке и признающие его требования.

1.2.28. **Удостоверяющий центр** – структурное подразделение Общества, осуществляющее функции по созданию, управлению и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом.

1.2.29. **Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ)** – физическое лицо, являющееся работником ООО «ЭТП ГПБ Консалтинг» и наделенное полномочиями по заверению бланков сертификатов, иных документов ООО «ЭТП ГПБ Консалтинг», а также иными полномочиями согласно настоящего Регламента.

1.2.30. **Федеральный закон** - Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

1.2.31. **Формат сертификата ключа проверки электронной подписи (списка отозванных сертификатов)** – упорядоченный набор допустимых полей данных сертификата ключа проверки ЭП (списка отозванных сертификатов).

1.2.32. **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.

1.2.33. **Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

1.3. Регламент содержит также иные определения, которые используются в значениях, раскрытых в соответствующих разделах Регламента.

2. СОКРАЩЕНИЯ

2.1. **ЕСИА** - Единая система идентификации и аутентификации.

2.2. **СМЭВ** – Система межведомственного электронного взаимодействия.

2.3. **СОС** – список отозванных сертификатов.

2.4. **УЦ** – Удостоверяющий центр.

2.5. **ЭП** – электронная подпись.

2.6. Регламент содержит также иные сокращения, которые используются в значениях, раскрытых в соответствующих разделах Регламента.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Предмет регулирования

3.1.1. Настоящий Регламент определяет порядок изготовления (создания), управления и использования квалифицированных сертификатов ключей проверки ЭП и выполнения целевых функций УЦ в соответствии с Федеральным законом.

3.1.2. Действие Регламента распространяется на заявителей, владельцев сертификатов (представителей заявителя/владельца сертификата), определенных Доверенным лицом УЦ, на Доверенное лицо УЦ, заключившее с Удостоверяющим центром Агентский договор № ДВ-2020/19 от «01» июня 2020 г.

3.1.3. Фактом присоединения к настоящему Регламенту является факт регистрации предоставленного в УЦ заявления на создание и выдачу сертификата ключа проверки электронной подписи (по форме Приложения № 1 к настоящему Регламенту). Дата регистрации заявления на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи (по форме Приложения № 1 к настоящему Регламенту) УЦ или Доверенным лицом УЦ является датой присоединения к Регламенту.

3.1.4. Лицо, присоединившееся к Регламенту, является Стороной Регламента, что влечет обязанность соблюдать его требования.

3.1.5. Факт присоединения лица к Регламенту означает полное принятие им условий Регламента и всех его приложений в редакции, действующей на дату акцепта оферты. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями Регламента.

3.1.6. Внесение изменений (дополнений) в Регламент, а также в приложения к нему, производится УЦ в одностороннем порядке посредством утверждения новой редакции Регламента.

3.1.7. Изменения, вносимые УЦ в Регламент, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечению 5 (Пяти) календарных дней с даты их публикации на сайте УЦ. Изменения (дополнения), вносимые УЦ в Регламент в связи с изменениями законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных актов.

3.2. Сведения об Удостоверяющем центре

3.2.1. Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации в соответствии с законодательством Российской Федерации, Уставом и иными локальными нормативными актами Общества.

3.2.2. Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей осуществляет деятельность на основании:

- лицензии ЛСЗ №0016562 от 24.09.2019 г., выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России;

- свидетельства об аккредитации УЦ №775 от 03.10.2017 г., выданное Министерством связи и массовых коммуникаций Российской Федерации.

Актуальная информация о наличии лицензий и свидетельств УЦ размещается на сайте УЦ.

3.2.3. Контактная информация:

Юридический адрес: 117342, г. Москва, ул. Миклухо-Маклая, д. 40, этаж 1, помещение IV, комната 20.

Почтовый адрес: 117342, г. Москва, ул. Миклухо-Маклая, д. 40, этаж 1, помещение IV, комната 20.

Адрес осуществления деятельности: 117418, г. Москва, Якиманская наб., д.2.

Телефон технической поддержки и для справок: +7 (800) 100-65-49.

Круглосуточный многоканальный номер телефона: +7 (800) 100-65-49.

Адрес сайта: https://ca.etpgpb.ru

Адрес электронной почты: ca@etpgpb.ru

3.2.4. График работы:

День недели	Время работы (время Московское)
Понедельник - пятница	с 9:00 до 18:00
Суббота, Воскресенье, праздничные дни	Выходной

3.2.5. Реквизиты:

ИНН/КПП	7728356929/772801001
ОГРН	5167746487651
р/счет	40702810000000002041
Банк	Банк ГПБ (АО) г. Москва
к/счет	30101810200000000823
БИК	044525823

3.2.6. По вопросам предоставления услуг УЦ заинтересованные лица получают информацию в следующем порядке:

- на сайте УЦ путем самостоятельного ознакомления с размещенной информацией;

- по номеру телефона технической поддержки и для справок путем консультации со специалистами УЦ в режиме реального времени;

- по круглосуточному многоканальному номеру телефона справок путем консультации со специалистами УЦ в режиме реального времени;

- через форму обратной связи на сайте УЦ путём оставления заявки на консультацию;

- по адресу электронной почты путем отправки сообщения с вопросами в адрес УЦ.

3.3. Стоимость услуг. Сроки и порядок расчётов.

3.3.1. Стоимость услуг по выдаче сертификата определяется Доверенным лицом УЦ при обращении заявителя к нему.

3.3.2. УЦ обязуется оказать услуги Стороне, присоединившейся к настоящему Регламенту, в течение 3 (трех) рабочих дней со дня предоставления в УЦ регистрационной и идентифицирующей информации (документов) в объеме, определенном настоящим Регламентом, на условиях Регламента.

4. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ ФУНКЦИЙ

4.1. Создание и выдача квалифицированных сертификатов в электронной форме лицам, обратившимся за их получением (заявителям), при условии установления личности заявителя либо полномочия лица, выступающего от его имени по обращению за получением данного сертификата с учетом требований, установленных статей 18 Федерального закона.

4.2. Подтверждение владения получателем сертификата (заявителем) ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения сертификата.

4.3. Установление сроков действия сертификатов.

4.4. Аннулирование выданных сертификатов.

4.5. Выдача по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП заявителем.

4.6. Ведение реестра сертификатов.

4.7. Создание ключей ЭП и ключей проверки ЭП по обращениям заявителей.

4.8. Проверка уникальности ключей проверки ЭП в реестре сертификатов.

4.9. Обеспечение доступа лиц к информации, содержащейся в реестре сертификатов (к Списку отозванных сертификатов), в том числе с использованием сети Интернет.

4.10. Осуществление по обращениям участников электронного взаимодействия проверки электронных подписей.

4.11. Предоставление информации, содержащейся в реестре сертификатов, в том числе информации об аннулировании сертификата ключа ЭП.

4.12. Предоставление прав использования программ для ЭВМ, необходимых для управления сертификатом.

4.13. УЦ оказывает иные услуги, предусмотренные Федеральным законом, в соответствии с настоящим Регламентом и иными внутренними документами УЦ.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Удостоверяющий центр имеет право

5.1.1. Запрашивать у заявителя документы для подтверждения информации, содержащейся в заявлении на создание и выдачу сертификата.

5.1.2. Запросить сведения у операторов базовых государственных информационных ресурсов с использованием СМЭВ для проверки достоверности документов и сведений, представляемых заявителями при подаче заявлений на создание и выдачу сертификата.

5.1.3. Запросить у заявителя дополнительные документы, подтверждающие достоверность представленных им сведений в случае наличия противоречий между сведениями, представленными заявителем, и сведениями, полученными УЦ из государственных информационных ресурсов.

5.1.4. Не принимать от заявителя документы, не соответствующих требованиям действующих нормативных правовых актов Российской Федерации.

5.1.5. Отказать в регистрации заявления на создание и выдачу сертификата в случае ненадлежащего его оформления и/или непредставления документов, указанных в Регламенте.

5.1.6. Отказать в прекращении действия сертификата владельцу сертификата в случае ненадлежащего оформления соответствующего заявления на прекращение действия сертификата.

5.1.7. Отказать в прекращении действия сертификата владельцу сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям или истек установленный срок действия ключа ЭП, соответствующего сертификату.

5.1.8. В одностороннем порядке вносить изменения в Регламент.

5.1.9. Выпускать дополнительные инструкции и положения, регламентирующие процедуры, связанные с получением и применением сертификатов.

5.1.10. В одностороннем порядке без заявления владельца сертификата прекратить или приостановить действие сертификата с обязательным уведомлением владельца сертификата, действие которого прекращено, и указанием обоснованных причин (например, в случае наличия у УЦ достоверных сведений о нарушении конфиденциальности ключа ЭП владельца сертификата, невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области ЭП, а также в случае появления у УЦ 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 данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке, а также в иных случаях, предусмотренных настоящим Регламентом).

5.1.11. В одностороннем порядке прекратить действие Регламента в отношении Стороны, присоединившейся к Регламенту, уведомив соответствующую Сторону за 5 (пять) рабочих дней до дня аннулирования сертификата, владельцем которого является указанная Сторона.

5.1.12. Наделить третьих лиц (далее – Доверенные лица УЦ) полномочиями по вручению сертификатов, выпущенных УЦ, а также полномочиями по установлению личности получателя сертификата на основании заключенного договора между УЦ и Доверенным лицом УЦ.

5.1.13. По письменному запросу заявителя, владельца сертификата, предоставить:

- копию лицензии, выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России, заверенную подписью Уполномоченного лица УЦ и оттиском печати;
- копию свидетельства об аккредитации, выданное Министерством связи и массовых коммуникаций Российской Федерации, заверенное подписью Уполномоченного лица УЦ и оттиском печати;
- копию документа (выписку из документа) о наделении Уполномоченного лица УЦ полномочиями на подписание документов в соответствии с настоящим Регламентом, заверенную подписью Уполномоченного лица УЦ и оттиском печати.

5.2. Удостоверяющий центр обязан

5.2.1. Информировать в письменной форме заявителей об условиях и порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

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

5.2.3. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

5.2.4. Обеспечивать круглосуточную доступность реестра сертификатов в информационно-телекоммуникационной сети Интернет, за исключением периодов планового или внепланового технического обслуживания.

5.2.5. Обеспечивать конфиденциальность созданных УЦ ключей ЭП.

5.2.6. Установить личность заявителя – физического лица, обратившегося за получением квалифицированного сертификата.

5.2.7. Получить от лица, выступающего от имени заявителя – юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

5.2.8. Отказать заявителю в выдаче квалифицированного сертификата в случае, если сведения, представленные заявителем для создания квалифицированного сертификата не подтверждены сведениями, полученными из государственных информационных ресурсов, не установлена личность заявителя – физического лица или не получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением квалифицированного сертификата.

5.2.9. Хранить в форме, позволяющей проверить ее целостность и достоверность, в течение срока своей деятельности следующую информацию:

а) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата – физического лица;

б) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя – юридического лица, обращаться за получением квалифицированного сертификата;

в) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца

квалифицированного сертификата включена в квалифицированный сертификат.

5.2.10. Направлять в ЕСИА сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного УЦ).

5.2.11. По желанию лица, которому выдан квалифицированный сертификат, выраженному в устной форме при получении сертификата, безвозмездно осуществить регистрацию указанного лица в ЕСИА.

5.2.12. Отказать заявителю в создании сертификата в случае, если не было подтверждено то, что заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения сертификата.

5.2.13. Отказать заявителю в создании сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки ЭП, указанного заявителем для получения сертификата.

5.2.14. Под расписку ознакомить заявителя с информацией, содержащейся в квалифицированном сертификате.

5.2.15. Строго соблюдать срок действия ключей ЭП УЦ, используемых для подписания создаваемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие.

5.2.16. Иные обязанности УЦ определены положениями действующего законодательства Российской Федерации.

5.3. Заявитель, владелец сертификата имеет право

5.3.1. Применять сертификат УЦ для проверки электронной подписи УЦ в сертификатах, созданных УЦ.

5.3.2. Применять список отозванных сертификатов, изготовленный УЦ для установления статуса сертификатов, созданных УЦ.

5.3.3. Применять сертификат для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате.

5.3.4. Для хранения ключа ЭП применять носитель, поддерживаемый средством электронной подписи.

5.3.5. Обратиться в УЦ с заявлением на прекращение действия сертификата, владельцем которого он является, в течение срока действия соответствующего ключа ЭП.

5.3.6. Обратиться в УЦ за получением информации о статусе сертификатов и их действительности на определенный момент времени.

5.3.7. Обратиться в УЦ за подтверждением подлинности ЭП в электронном документе, сформированной с использованием сертификата, созданного УЦ.

5.3.8. Обратиться в УЦ за получением иных сопутствующих услуг, представленных с Прайс-листом (тарифами) на сайте УЦ.

5.3.9. Владелец сертификата вправе в одностороннем порядке прекратить взаимодействие с УЦ в рамках Регламента, направив в УЦ заявление на прекращение действия (аннулирования) сертификата ключа проверки электронной подписи (по форме Приложения №3 к Регламенту).

5.4. Заявитель, владелец сертификата обязан

5.4.1. Самостоятельно ознакомиться с изменениями и дополнениями Регламента, размещенными на сайте УЦ.

5.4.2. Известить УЦ об изменении сведений, включенных в квалифицированный сертификат, и подать заявление на аннулирование сертификата, содержащего недостоверные сведения.

5.4.3. Соблюдать требования по обеспечению безопасности при работе со средствами электронной подписи, в соответствии с Приложением №6 к настоящему Регламенту.

5.4.4. Хранить в тайне ключ ЭП, принимать все возможные и необходимые меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

5.4.5. Применять для формирования электронной подписи только действующий ключ ЭП.

5.4.6. Применять ключ ЭП только в соответствии с областями использования, указанными в соответствующем данному ключу сертификате (расширения Key Usage, Extended Key Usage, Application Policy сертификата).

5.4.7. Не применять ключ ЭП и немедленно обратиться в УЦ с заявлением на прекращение действия (аннулирование) сертификата ключа проверки ЭП (по форме Приложения №3 к Регламенту) в случае компрометации (потери, раскрытия, искажения) ключа ЭП, а также в случае, если пользователю УЦ стало известно, что ключ ЭП используется или использовался ранее другими лицами без согласия владельца соответствующего сертификата.

5.4.8. Не использовать ключ ЭП, связанный с сертификатом, заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи (по форме Приложения №3 к Регламенту) которого подано в УЦ, в течение времени, исчисляемого со дня регистрации заявления о прекращении действия сертификата в УЦ по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия сертификата.

5.4.9. Не использовать персональный ключ ЭП, связанный с сертификатом, действие которого прекращено.

5.4.10. В случае самостоятельного создания ключа ЭП предоставить УЦ запрос сертификата в формате PKCS #10, соответствующем ГОСТ 34.10-2012 с выполнением требований, предъявляемых к таким электронным документам используемыми УЦ средствами УЦ. Запрос сертификата должен содержать всю информацию, представляемую для включения в выдаваемый сертификат, сведения о средствах ЭП, использовавшихся для создания ключа ЭП и ключа проверки ЭП, и о средствах ЭП, с которыми будет использоваться сертификат.

5.4.11. Выполнять требования настоящего Регламента.

5.5. Ответственность Сторон

5.5.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту, Стороны несут ответственность в соответствии с законодательством Российской Федерации.

5.5.2. УЦ несет ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

5.5.3. В случае принятия решения о прекращении своей деятельности без передачи функции УЦ другим лицам сообщить об этом на сайте УЦ и в уполномоченный федеральный орган не позднее, чем за 1 (один) месяц до даты прекращения своей деятельности, и передать в уполномоченный федеральный орган Реестр выданных сертификатов.

5.5.4. Владелец сертификата принимает на себя все риски и несет ответственность за возникшие негативные последствия и убытки, в случае:

- нарушения конфиденциальности своих ключей электронной подписи;
- утери носителей ЭП;
- несвоевременного уведомления УЦ о компрометации ключа электронной подписи;
- несвоевременной смены своих ключей ЭП в случае наступления событий, влекущих компрометацию ключей ЭП;
- предоставления в УЦ недостоверной информации, устаревшей редакции документов, несвоевременного уведомления об изменениях в предоставленных в УЦ документах и данных, непредставления или несвоевременного предоставления документов, подтверждающих изменения.

5.5.5. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной своих обязательств.

5.5.6. УЦ не несет ответственность за неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту, а также за любые прямые или косвенные убытки, любую потерю прибыли, в случаях, указанных в п.5.1.53 Регламента, в том числе вызванные несанкционированным использованием ключа ЭП владельца сертификата неуполномоченными лицами.

5.5.7. УЦ не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если УЦ обоснованно полагался на сведения, предоставленные заявителем.

5.5.8. УЦ не несет ответственность за невозможность использования сертификата в случае, если такая невозможность возникла после создания сертификата и вызвана изменением требований информационных систем или законодательства Российской Федерации, иных нормативных правовых актов.

5.5.9. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием обстоятельств непреодолимой силы.

5.5.9.1. Обстоятельствами непреодолимой силы признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования аппаратно-программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Сторонами своих обязательств по настоящему Регламенту.

5.5.9.2. В случае возникновения форс-мажорных обстоятельств срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

5.5.9.3. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна незамедлительно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении обстоятельств непреодолимой силы, а также предоставить доказательства существования названных обстоятельств.

5.5.9.4. Неизвещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

5.5.9.5. В случае если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием обстоятельств непреодолимой силы и существует свыше 1 (одного) месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

6. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ

6.1. Процедура создания ключей ЭП и ключей проверки ЭП

6.1.1. Процедура создания ключей ЭП и ключей проверки ЭП для физических лиц, индивидуальных предпринимателей и юридических лиц выполняется при условии присоединения к настоящему Регламенту в порядке, определенному в п.3.1 Регламента, с учетом положений п.6.2 Регламента.

6.1.2. В случае обращения заявителя лично за получением сертификата в УЦ, оператор УЦ осуществляет формирование ключа ЭП заявителя и запись его на носитель ЭП заявителя на автоматизированном рабочем месте, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите конфиденциальной информации, размещенном в аттестованном помещении, доступ в которое ограничен, в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности России в соответствии с приказом ФСБ России от 09 февраля 2005 г. №66

«Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6.1.3. В альтернативном порядке заявитель имеет возможность самостоятельно сформировать ключ ЭП и запрос сертификата на своем персональном компьютере, используя средства УЦ, предоставляемые через функционал Личного кабинета, доступ к которому открывается на сайте УЦ после регистрации заявки на получение ЭП. Запрос сертификата передается в УЦ через функционал Личного кабинета. Порядок использования функционала Личного кабинета установлен Приложением №7 к Регламенту. Сертификат формируется УЦ только по получении запроса сертификата и прохождения процедуры идентификации лица, обратившегося за получением квалифицированного сертификата.

6.1.4. Ключ ЭП и ключ проверки ЭП создаются с использованием средства ЭП, имеющим подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

6.1.5. Процедура плановой смены ключей ЭП УЦ осуществляется в порядке, определенном внутренним регламентом исполнения плановых и внеплановых процедур УЦ, на основании наступления срока смены ключей ЭП УЦ для обеспечения непрерывности подписания сертификатов до момента их истечения. Об осуществлении такой смены владельцы сертификатов информируются на сайте УЦ путем публикации нового сертификата УЦ, соответствующего новым ключам ЭП УЦ с указанием доверенного способа получения нового сертификата УЦ.

6.1.6. В случае компрометации ключа ЭП УЦ ключ ЭП УЦ и соответствующий ему сертификат УЦ прекращают действие, владельцы сертификатов уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации ключа ЭП УЦ на сайте УЦ.

6.1.6.1. Все сертификаты, подписанные с использованием скомпрометированного ключа ЭП УЦ, считаются прекратившими действие.

6.1.6.2. После прекращения действия сертификата УЦ выполняется процедура внеплановой смены ключей ЭП УЦ. Процедура внеплановой смены ключей ЭП УЦ выполняется в порядке, определенном внутренним регламентом исполнения плановых и внеплановых процедур УЦ незамедлительно после установления факта нарушения их конфиденциальности или угрозы нарушения их конфиденциальности.

6.1.6.3. Все действовавшие на момент компрометации ключа ЭП УЦ сертификаты подлежат внеплановой смене на безвозмездной основе (за счёт УЦ) на срок, указанный в поле notAfter поля Validity сертификата, подлежащего внеплановой смене с пролонгацией на срок равный времени (в днях) с момента прекращения действия и до момента выпуска нового сертификата.

6.1.7. Смена ключа ЭП владельца сертификата, осуществляется по заявлению владельца сертификата в сроки, установленные настоящим Регламентом.

6.1.7.1. Смена ключей ЭП владельца сертификата осуществляется вместе со сменой квалифицированного сертификата. В порядке плановой и внеплановой смены ключей ЭП и сертификата заявление от владельца сертификата подается по форме Приложения №1.

6.1.7.2. Плановая смена ключей ЭП и сертификата ключа проверки ЭП проводится владельцем сертификата не ранее одного календарного месяца до даты истечения действующего сертификата, указанной в поле notAfter поля Validity сертификата. Способ создания ключей ЭП при плановой смене ключей ЭП определяется владельцем сертификата по согласованию с УЦ либо с Доверенным лицом УЦ и соответствует порядку, изложенному в настоящем разделе.

6.1.7.3. Внеплановая смена ключа ЭП и ключа проверки ЭП осуществляется в следующих случаях:

- владелец сертификата не осуществил плановую смену в установленные Регламентом сроки;
- произошла компрометация ключа ЭП владельца сертификата;
- изменились сведения, включенные в сертификат;

- при компрометации ключа ЭП УЦ.

6.1.8. Способ создания ключей ЭП при внеплановой смене ключей ЭП определяется владельцем сертификата по согласованию с УЦ либо с Доверенным лицом УЦ и соответствует порядку, изложенному в настоящем разделе.

6.2. Процедура создания и выдачи квалифицированных сертификатов

6.2.1. УЦ осуществляет изготовление сертификатов ЭП физическим лицам, индивидуальным предпринимателям и представителям юридических лиц только в том случае, если указанное лицо присоединилось к Регламенту в порядке, определенному в п.3.1 Регламента.

6.2.2. Заявитель при личном прибытии в УЦ или к Доверенному лицу УЦ подаёт заявление на создание и выдачу сертификата по форме Приложения №1 к настоящему Регламенту на бумажном носителе, подписанное собственноручно, а в случае, если заявление на создание и выдачу сертификата подаётся представителем Стороны, присоединившейся к Регламенту, подписанное также и лицом, имеющим право действовать от имени Стороны, присоединившейся к Регламенту, с приложением печати (если применимо).

6.2.2.1. В заявлении на создание и выдачу сертификата по форме Приложения №1 к Регламенту должны быть указаны фамилия, имя, отчество (если имеется) владельца квалифицированного сертификата - для физического лица, не являющегося индивидуальным предпринимателем, либо фамилия, имя, отчество (если имеется) и основной государственный регистрационный номер индивидуального предпринимателя - владельца квалифицированного сертификата - для физического лица, являющегося индивидуальным предпринимателем, либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для российского юридического лица, либо наименование, место нахождения владельца квалифицированного сертификата, а также идентификационный номер налогоплательщика (при наличии) - для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации); а также страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица.

6.2.3. По прибытии заявителя (представителя заявителя) в УЦ или к Доверенному лицу УЦ, Оператор УЦ или Доверенное лицо УЦ выполняет процедуру идентификации лица, обратившегося в УЦ, путем установления его личности:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации.
- в случае отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, установление его личности осуществляется по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
- личность беженца, вынужденного переселенца или лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации, в качестве удостоверяющего личность данных категорий лиц.

6.2.4. После установления личности обратившегося лица Оператор УЦ или Доверенное лицо УЦ принимает к рассмотрению заявление на создание и выдачу сертификата по форме Приложения №1 к Регламенту и комплект подтверждающих документов либо их надлежащим образом заверенные копии.

6.2.4.1. Для определения полномочий лица, действующего от имени Стороны, присоединившейся к Регламенту, в УЦ должна быть представлена доверенность, выданная на имя лица, действующего от имени Стороны, присоединившейся к Регламенту (рекомендуемая форма доверенности - по форме

Приложения №2 Регламента) либо документ, подтверждающий полномочия лица действовать от имени Стороны, присоединившейся к Регламенту, без доверенности.

6.2.4.2. Заявителем - физическим лицом для изготовления и выдачи квалифицированного сертификата должны быть предоставлены следующие документы и сведения: документ, удостоверяющий личность; номер страхового свидетельства государственного пенсионного страхования; идентификационный номер налогоплательщика.

6.2.4.3. Заявителем – юридическим лицом для изготовления и выдачи квалифицированного сертификата должны быть предоставлены следующие документы и сведения: документ, удостоверяющий личность представителя, сведения о котором вносятся в сертификат наряду с наименованием юридического лица, номер страхового свидетельства государственного пенсионного страхования представителя; основной государственный регистрационный номер юридического лица.

6.2.4.4. Заявителем – индивидуальным предпринимателем для изготовления и выдачи квалифицированного сертификата должны быть предоставлены следующие документы и сведения: документ, удостоверяющий личность; номер страхового свидетельства государственного пенсионного страхования; основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя.

6.2.4.5. Заявителем – иностранной организацией для изготовления и выдачи квалифицированного сертификата должны быть предоставлены следующие документы и сведения: документ, удостоверяющий личность представителя, сведения о котором вносятся в сертификат наряду с наименованием иностранной организации, номер страхового свидетельства государственного пенсионного страхования представителя; 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.

6.2.4.6. В случае если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель предоставляет документ соответствующей формы.

6.2.5. Надлежащим способом заверения копий документов может являться нотариальное заверение копий, заверение копий органом власти, заверение копий документов заявителем самостоятельно. При необходимости копии с документов могут быть сняты и заверены работником УЦ или Доверенным лицом УЦ.

6.2.5.1. Нотариально заверенные копии документов должны содержать штамп нотариуса «копия верна», штамп с информацией о нотариусе, должны быть заверены печатью нотариуса и иметь подпись нотариуса. Копия документа, удостоверяющего личность заявителя или его представителя предоставляется в УЦ или Доверенному лицу УЦ заверенная нотариально, совершение заверения документа, удостоверяющего личность, должно быть осуществлено не позднее 15 (пятнадцати) дней до момента подачи в УЦ или Доверенному лицу УЦ.

6.2.5.2. Копии, заверенные заявителем, могут предоставлять исключительно юридические лица и индивидуальные предприниматели, имеющие собственную печать. Совершение заверение документов должно быть осуществлено не позднее 30 (тридцати) дней до момента подачи в УЦ или Доверенному лицу УЦ. На последнем листе копии (выписки из документа) на свободном месте под текстом оформляется реквизит «Отметка о заверении копии», придающий копии документа юридическую силу и включающий: слова «Копия верна», указание о месте нахождения подлинника документа, наименование должности лица, заверившего копию, личную подпись, расшифровку подписи, дату заверения и оттиск печати. Листы многостраничных копий (выписок из документов) нумеруются, отметка о заверении копии дополняется указанием количества листов копии (выписки из документа): «Всего в копии (выписки из документа) ____ листов». Допускается заверять отметкой «Копия верна» каждый лист многостраничной копии документа.

6.2.5.3. Копии документов, заверенные органом власти, должны содержать подпись и расшифровку подписи должностного лица, их заверившего, а также печать (штамп) данного органа власти.

6.2.5.4. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

6.2.6. Документы и/или их надлежащим образом заверенные копии, представленные в УЦ для изготовления и выдачи квалифицированного сертификата, остаются на хранении в УЦ и возврату не подлежат.

6.2.7. Оператор УЦ или Доверенное лицо УЦ вправе для установления достоверности сведений, вносимых в квалифицированный сертификат, запросить у заявителя дополнительные документы и сведения.

6.2.8. Для проверки достоверности документов и сведений, представленных заявителем, Оператор УЦ или Доверенное лицо УЦ запрашивает необходимые сведения у операторов государственных информационных ресурсов с использованием СМЭВ.

6.2.9. В случае несоответствия сведений, указанных в заявлении на создание и выдачу сертификата сведениям, полученным у операторов государственных информационных ресурсов, Оператор УЦ или Доверенное лицо УЦ запрашивает у заявителя дополнительные документы, подтверждающие указанные сведения.

6.2.9.1. При несоответствии документов сведениям, полученным из государственных информационных систем или отказе заявителя представить запрошенные Оператором УЦ или Доверенным лицом УЦ документы, Оператор УЦ или Доверенное лицо УЦ вправе отказать заявителю в регистрации заявления на создание и выдачу сертификата.

6.2.9.2. В случае отказа в регистрации заявления на создание и выдачу сертификата, Оператор УЦ или Доверенное лицо УЦ уведомляет об этом заявителя с указанием причины отклонения заявления.

6.2.9.3. При изменении данных заявителя на основании предоставленных им сведений, Оператор УЦ или Доверенное лицо УЦ передает заявителю на подпись заявление на изменение учетных данных.

6.2.10. В случае достоверности сведений, указанных в заявлении и предоставленных документах, Оператор УЦ или Доверенное лицо УЦ осуществляет регистрацию заявления на создание и выдачу сертификата.

6.2.11. Формирование запроса сертификата осуществляется одновременно с изготовлением ключа ЭП в порядке, изложенном в пункте «Процедура создания ключей ЭП и ключей проверки ЭП» Регламента. На основании сформированного запроса Оператор УЦ создает сертификат с данными, указанными в заявлении и запросе сертификата. Сертификат в электронной форме записывается на ключевой носитель владельца сертификата либо Оператором УЦ, либо владельцем сертификата самостоятельно при помощи функционала Личного кабинета на сайте УЦ, в зависимости от того, какой способ формирования ключей ЭП был выбран владельцем сертификата.

6.2.12. После создания сертификата в электронной форме владельцу сертификата для ознакомления с информацией, содержащейся в сертификате, передаются два бланка сертификата. Владелец сертификата расписывается на двух экземплярах бланка сертификата, один экземпляр возвращает Оператору УЦ или Доверенному лицу УЦ. В случае, если заявитель формировал запрос сертификата самостоятельно с использованием Личного кабинета, способ передачи подписанных бланков сертификата в ознакомление владельцем сертификата устанавливается Приложением №7 Регламента.

6.2.13. При получении сертификата владелец ознакамливается под роспись с Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи (Приложение №6 к Регламенту).

6.2.14. Срок создания и выдачи сертификата не должен превышать 3 (трех) рабочих дней с момента регистрации в УЦ или у Доверенного лица УЦ соответствующего заявления (при наличии оплаты и запроса сертификата).

6.3. Подтверждение действительности электронной подписи

6.3.1. Подтверждение действительности ЭП, использованной для подписания электронных документов, созданной с использованием сертификата ЭП, выпущенным в УЦ, осуществляется на основании заявления владельца сертификата. Данное заявление оформляется по форме Приложения №4 к Регламенту на бумажном носителе, подписанное собственноручно, а в случае, если заявление на создание и выдачу сертификата подаётся представителем Стороны, присоединившейся к Регламенту, подписанное также и лицом, имеющим право действовать от имени Стороны, присоединившейся к Регламенту, с приложением печати (если применимо).

6.3.2. Заявление должно содержать следующую информацию:

– дата и время подачи заявления;

– идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;

– время и дата формирования ЭП электронного документа;

– время и дата, на момент наступления которых требуется установить подлинность ЭП.

6.3.3. Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является носитель, содержащий:

– файл сертификата, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе;

– электронный документ – в виде одного файла, содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных.

6.3.4. УЦ обеспечивает подтверждение подлинности ЭП в электронном документе, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений Criptographic Message Syntax (CMS – стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369). Решение о соответствии электронного документа с ЭП стандарту CMS принимает УЦ. В случае, если электронный документ не соответствует стандарту CMS, УЦ отказывает заявителю в проведении процедуры подтверждения действительности ЭП.

6.3.5. Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа работников УЦ.

6.3.6. Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение УЦ. Заключение УЦ содержит:

- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- результат проверки ЭП электронного документа;
- данные, представленные комиссии для проведения проверки;
- отчет по выполненной проверке;

6.3.6.1. Отчет по выполненной проверке содержит:

а) время и место проведения проверки;

б) содержание и результаты проверки.

6.3.7. Заключение УЦ по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью УЦ. Один экземпляр заключения по выполненной проверке должен быть предоставлен заявителю – пользователю УЦ.

6.3.8. Заключение УЦ по подтверждению подлинности ЭП одного электронного документа должно быть подготовлено УЦ не позднее 3 (трех) рабочих дней с момента получения Оператором УЦ соответствующего заявления.

6.4. Процедуры, осуществляемые при прекращении действия и аннулирования квалифицированного сертификата

6.4.1. Сертификат прекращает действие в следующих случаях:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата по форме Приложения №3 к Регламенту, подаваемого в форме документа на бумажном носителе;
- в случае прекращения деятельности УЦ без перехода его функций другим лицам;

- при компрометации ключа ЭП УЦ;

- в случае прекращения действия Регламента в отношении Стороны, присоединившейся к Регламенту;

- в случае отзыва доверенности представителя Стороны, присоединившейся к Регламенту;

- в иных случаях, установленных Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или Регламентом.

6.4.2. УЦ аннулирует сертификат в следующих случаях:

- не подтверждено, что владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

- установлено, что содержащийся в таком сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате;

- вступило в силу решение суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию.

6.4.3. В случае прекращения действия сертификата по истечении установленного срока его действия временем прекращения действия сертификата признается время, хранящееся в поле notAfter поля Validity сертификата. В данном случае информация о сертификате в список отозванных сертификатов не заносится.

6.4.4. Заявление на прекращение действия сертификата оформляется владельцем сертификата по форме Приложения №3 к Регламенту на бумажном носителе, подписывается собственноручно, а в случае, если заявление на создание и выдачу сертификата подаётся представителем Стороны, присоединившейся к Регламенту, подписывается также и лицом, имеющим право действовать от имени Стороны, присоединившейся к Регламенту, с приложением печати (если применимо) и подается Оператору УЦ или Доверенному лицу УЦ при личном прибытии владельца (представителя владельца) сертификата в УЦ или к Доверенному лицу УЦ.

6.4.4.1. Подача заявления в УЦ на прекращение действия сертификата также может быть осуществлена посредством курьерской связи при представлении в УЦ доверенности на совершение указанных действий.

6.4.4.2. Оператор УЦ или Доверенное лицо УЦ удостоверяет личность заявителя в соответствии с требованиями Регламента и сверяет сведения из представленного заявления с данными владельца сертификата, хранящимися в реестрах УЦ.

6.4.4.3. При ошибках в оформлении заявления или несовпадении данных из представленного заявления с данными, хранящимися в реестре УЦ, Оператор УЦ или Доверенное лицо УЦ имеет право отказать заявителю в регистрации заявления и прекращении действия (аннулирования) сертификата или запросить дополнительные документы, подтверждающие изменение данных по своему усмотрению.

6.4.4.4. При совпадении данных из заявления со сведениями, хранящимися в реестрах УЦ, или при предоставлении владельцем сертификата документов, подтверждающих изменение данных, Оператор УЦ или Доверенное лицо УЦ регистрирует заявление на прекращение действия (аннулирования) сертификата ключа проверки ЭП. В случае, если заявление на прекращение действия (аннулирования) сертификата зарегистрировано Доверенным лицом УЦ, сведения о сертификате, подлежащем аннулированию передаются Доверенным лицом УЦ Оператору УЦ для выполнения необходимых процедур не позднее 3 (трёх) часов с момента регистрации заявления на прекращение действия (аннулирования) сертификата.

6.4.4.5. Оператор УЦ выполняет необходимые действия по аннулированию указанного в заявлении сертификата. Сведения о прекращении действия сертификата вносятся в реестр квалифицированных сертификатов.

6.4.5. Прекращение действия сертификатов Сторон, присоединившихся к Регламенту, при прекращении деятельности УЦ без перехода его функций другим лицам, осуществляется в дату, указанную в уведомлении, размещенном на сайте УЦ.

6.4.6. В случае компрометации ключа ЭП УЦ временем прекращения действия сертификатов владельцев признается время компрометации ключа ЭП УЦ, фиксирующееся в реестре УЦ.

6.4.7. Прекращение действия сертификата Стороны при прекращении действия Регламента осуществляется УЦ в дату, указанную в уведомлении УЦ, направленному Стороне, в отношении которой прекращается действие Регламента.

6.4.8. Прекращение действия сертификата представителя Стороны, присоединившейся к Регламенту, на основании отзыва доверенности ее представителя, осуществляется при получении УЦ официального письма, адресованного в УЦ, составленного в произвольной форме на бумажном носителе от Стороны, присоединившейся к Регламенту, с указанием реквизитов доверенности и ФИО представителя, чья доверенность отзывается, а также даты, с которой доверенность считается отозванной, за подписью представителя Стороны, имеющего право действовать от ее имени с приложением печати (если применимо). УЦ прекращает действие сертификата не позднее 12 (двенадцати) часов с момента либо получения указанного официального письма, либо, при наличии даты прекращения доверенности в письме, с момента наступления указанных обстоятельств.

6.4.9. В случае прекращения действия сертификата по указанным в настоящем разделе основаниям, УЦ официально уведомляет всех заинтересованных лиц о прекращении действия сертификата не позднее 12 (двенадцати) часов с момента наступления указанных обстоятельств. Действие сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов УЦ.

6.4.10. Официальным уведомлением о факте прекращения действия сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об аннулированном сертификате, и изданного не ранее времени наступления произошедшего случая.

6.4.11. Временем прекращения действия сертификата признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов, соответствующее моменту внесения записи о прекращении действия сертификата в реестр сертификатов УЦ.

6.4.12. Информация о размещении списка отозванных сертификатов заносится в созданные УЦ сертификаты в расширение CRL Distribution Point сертификата ключа проверки ЭП.

6.4.13. УЦ осуществляет размещение реестра квалифицированных сертификатов и списков отозванных сертификатов в сети Интернет на сайте УЦ.

6.5. Порядок ведения реестра квалифицированных сертификатов

6.5.1. Формирование реестра квалифицированных сертификатов включает в себя внесение сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов.

6.5.2. Ведение реестра сертификатов включает в себя:

- внесение изменений в реестр квалифицированных сертификатов в случае изменения сведений;

- внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

6.5.3. Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности УЦ, если более короткий срок не установлен нормативными правовыми актами Российской Федерации.

6.5.4. Хранение информации, содержащейся в реестре сертификатов, осуществляется в защищенных базах данных УЦ и в электронных архивах в форме, позволяющей проверить ее целостность и достоверность. Формирование и ведение единого реестра осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

6.5.5. Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре, формируется его резервная копия.

6.5.6. Информация о прекращении действия сертификата вносится УЦ в соответствующий раздел реестра квалифицированных сертификатов в течение одного

рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение действия сертификата. Действие сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

6.5.7. Запись об аннулировании сертификата в соответствующий раздел реестра квалифицированных сертификатов вносится УЦ в реестр квалифицированных сертификатов в течение не более чем одного рабочего дня с момента вступления решения суда, явившемся основанием для аннулирования, в законную силу. Сертификат считается аннулированным с момента внесения указанной записи в реестр квалифицированных сертификатов.

6.6. Порядок технического обслуживания реестра квалифицированных сертификатов

6.6.1. УЦ обеспечивает круглосуточный доступ для владельцев сертификатов к реестру сертификатов в режиме реального времени на сайте УЦ, за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

6.6.2. Максимальные сроки проведения технического обслуживания реестра квалифицированных сертификатов не могут превышать 3 (трех) дней.

6.6.3. УЦ заблаговременно оповещает владельцев сертификатов и иных лиц, использующих реестр сертификатов, о планируемом проведении планового или внепланового технического обслуживания реестра сертификатов путем размещения соответствующего уведомления на сайте УЦ.

7. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ

7.1. УЦ информирует заявителей, что при использовании электронной подписи возникают следующие основные риски:

- Риски, связанные с аутентификацией (подтверждением подлинности) пользователя электронной подписи. Лицо, на которое указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.
- Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.
- Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.
- Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.
- Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя электронной подписи, ключ которого был скомпрометирован.

7.2. Информация о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, содержится в Руководстве по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи (Приложение №6 к настоящему Регламенту), размещенному в электронной форме на сайте, а также выдаваемому владельцу сертификата под роспись при получении квалифицированного сертификата.

7.3. Ключ ЭП, соответствующий сертификату ключа проверки ЭП, является конфиденциальной информацией лица, зарегистрированного в реестре УЦ. УЦ ООО «ЭТП ГПБ Консалтинг» не осуществляет хранение ключей ЭП владельцев сертификатов.

7.4. Получение информации о статусе сертификата ключа проверки ЭП, созданного УЦ, осуществляется на основании заявления Стороны, присоединившейся к Регламенту.

Данное заявление оформляется по форме Приложения №5 Регламента и предоставляется в УЦ посредством почтовой либо курьерской связи.

7.4.1. Заявление должно содержать следующую информацию: время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа проверки ЭП, статус сертификата ключа проверки ЭП которого требуется установить; серийный номер сертификата ключа проверки ЭП, статус которого требуется установить.

7.4.2. По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата ключа проверки ЭП, которая предоставляется заявителю.

7.4.3. Предоставление заявителю справки о статусе сертификата ключа проверки ЭП должно быть осуществлено не позднее 7 (семи) рабочих дней с момента получения УЦ соответствующего заявления.

8. СПИСОК ПРИЛОЖЕНИЙ

Приложение №1. Форма заявления на создание и выдачу сертификата ключа проверки электронной подписи.

Приложение №2. Форма доверенности на представителя индивидуального предпринимателя или юридического лица, данные которого указываются в сертификате.

Приложение №3. Форма заявления на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи.

Приложение №4. Форма заявления на подтверждение подлинности электронной подписи в электронном документе.

Приложение №5. Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи.

Приложение №6. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи.

Приложение №7. Соглашение об использовании Личного кабинета Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг».

8.1. Приложение №1 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Форма Заявления на создание и выдачу сертификата ключа проверки электронной подписи (для юридических лиц)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» *

Настоящим _____

(наименование организации, включая организационно-правовую форму, ОГРН, ИНН

в лице

_____

(должность, фамилия, имя, отчество руководителя организации)

действующего на основании

_____

(наименование документа, подтверждающего право действовать от имени юридического лица)

Просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	Наименование организации
E-Mail (E)	Адрес электронной почты представителя владельца сертификата
Organization	Наименование организации
Title	Должность представителя владельца
Organization Unit	Наименование подразделения, сотрудником которого является представитель владельца сертификата
Surname	Фамилия представителя владельца сертификата
GivenName	Имя и отчество представителя владельца сертификата
StreetAddress	Адрес местонахождения юридического лица
Locality (L)	Наименование населенного пункта по адресу местонахождения организации
State (S)	Субъект Федерации по адресу местонахождения организации
Country (C)	Страна (RU)
OGRN	ОГРН организации
INN	ИНН организации
SNILS	СНИЛС представителя владельца сертификата

Полностью и безусловно присоединяюсь к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Регламентом УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования квалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Регламенте перечнем рисков, возникающих при проведении операций с использованием квалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков, указанный в Регламенте, не может раскрыть все возможные риски и другие аспекты использования квалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием квалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я, _____,

(фамилия, имя, отчество субъекта персональных данных)

зарегистрированн(ый/ая) по адресу: _____,

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется заявителю.

документ, удостоверяющий личность: _____,
(наименование документа, N, сведения о дате выдачи документа и выдавшем его органе)

в целях создания и выдачи квалифицированного сертификата ключа проверки электронной подписи, в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", даю согласие ООО «ЭТП ГПБ Консалтинг», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, д.40, эт.1, пом.IV, ком.20; ООО «ЭТП ГПБ», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, дом 40, подвал, помещение I, ком 25

(либо: _____,
(указать наименование или Ф.И.О. лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена такому лицу)

находящемуся по адресу: _____,)

на обработку (совокупность действий (операций), совершаемых с использованием средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных, а именно: фамилии, имени, отчества, номера СНИЛС, ИНН, паспортных данных, данных о местонахождении, адреса электронной почты, на срок, установленный для хранения информации аккредитованным удостоверяющим центром Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативно-правовыми актами Российской Федерации.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Представитель заявителя _____/_____
«___»_____20__ г.

Руководитель организации _____/_____/
«___»_____20__ г.
М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ. Регистрационный №_____ от «___»_____ 20_ г.

_____ _____/
(должность/полномочия) _____/
«____» _____20_г.

(для физических лиц)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» *

От_____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

Прошу сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	ФИО владельца сертификата
E-Mail (E)	Адрес электронной почты владельца сертификата
Surname	Фамилия владельца сертификата
GivenName	Имя и отчество владельца сертификата
StreetAddress	Адрес регистрации владельца сертификата
Locality (L)	Наименование населенного пункта по адресу регистрации владельца сертификата
State (S)	Субъект Федерации по адресу регистрации пользователя владельца сертификата
Country (C)	Страна (RU)
INN	ИНН владельца сертификата
SNILS	СНИЛС владельца сертификата

Полностью и безусловно присоединяюсь к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Регламентом УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования квалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Регламенте перечнем рисков, возникающих при проведении операций с использованием квалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков, указанный в Регламенте, не может раскрыть все возможные риски и другие аспекты использования квалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием квалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)

зарегистрированн(ый/ая) по адресу: ___,
документ, удостоверяющий личность: _____,
(наименование документа, N, сведения о дате выдачи документа и выдавшем его органе)

в целях создания и выдачи квалифицированного сертификата ключа проверки электронной подписи, в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", даю согласие ООО «ЭТП ГПБ Консалтинг», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, д.40, эт.1, пом.IV, ком.20; ООО «ЭТП ГПБ», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, дом 40, подвал, помещение I, ком 25
(либо: _____,
(указать наименование или Ф.И.О. лица, осуществляющего обработку персональных данных по поручению оператора,

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в УЦ ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется заявителю.

если обработка поручена такому лицу)

находящемуся по адресу: _____,)

на обработку (совокупность действий (операций), совершаемых с использованием средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных, а именно: фамилии, имени, отчества, номера СНИЛС, ИНН, паспортных данных, данных о местонахождении, адреса электронной почты, на срок, установленный для хранения информации аккредитованным удостоверяющим центром Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативно-правовыми актами Российской Федерации.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Заявитель _____/_____

"___" _____ 20__ г.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ. Регистрационный №_____ от «___»_____ 20_ г.

_____ _____/
(должность/полномочия) _____/

«____» _____20_г.

(для индивидуальных предпринимателей)

Заявление на создание и выдачу сертификата ключа проверки электронной подписи в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» *

Настоящим _____
(наименование организации, включая организационно-правовую форму, ОГРНИП, ИНН)

_____

Просит сформировать ключи электронной подписи и создать сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	ФИО владельца сертификата
E-Mail (E)	Адрес электронной почты владельца сертификата
Surname	Фамилия владельца сертификата
GivenName	Имя и отчество владельца сертификата
StreetAddress	Адрес регистрации владельца сертификата
Locality (L)	Наименование населенного пункта по адресу регистрации владельца сертификата
State (S)	Субъект Федерации по адресу регистрации пользователя владельца сертификата
Country (C)	Страна (RU)
OGRNIP	ОГРНИП владельца сертификата
INN	ИНН владельца сертификата
SNILS	СНИЛС владельца сертификата

Полностью и безусловно присоединяюсь к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг», условия которого определены ООО «ЭТП ГПБ Консалтинг».

С Регламентом УЦ ООО «ЭТП ГПБ Консалтинг», приложениями к нему и с Руководством по обеспечению безопасности использования квалифицированной электронной подписи ознакомлен и обязуюсь соблюдать все положения указанных документов.

Настоящим подтверждаю факт ознакомления с указанным в Регламенте перечнем рисков, возникающих при проведении операций с использованием квалифицированной электронной подписи и средств электронной подписи. Я понимаю, что перечень рисков, указанный в Регламенте, не может раскрыть все возможные риски и другие аспекты использования квалифицированной электронной подписи и средств электронной подписи. Риски, связанные с использованием квалифицированной электронной подписи и средств электронной подписи, мне понятны и принимаются полностью.

Я, _____,
(фамилия, имя, отчество субъекта персональных данных)

зарегистрированн(ый/ая) по адресу: _____,
документ, удостоверяющий личность: _____,
(наименование документа, N, сведения о дате выдачи документа и выдавшем его органе)

в целях создания и выдачи квалифицированного сертификата ключа проверки электронной подписи, в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", даю согласие ООО «ЭТП ГПБ Консалтинг», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, д.40, эт.1, пом.IV, ком.20; ООО

* Заявление на создание и выдачу сертификата ключа проверки электронной подписи в УЦ ООО «ЭТП ГПБ Консалтинг» подается в УЦ или Доверенному лицу УЦ в двух экземплярах. После регистрации заявления один экземпляр предоставляется заявителю.

«ЭТП ГПБ», находящемуся по адресу: г. Москва, ул. Миклухо-Маклая, дом 40, подвал, помещение I, ком 25

(либо:

_____,

(указать наименование или Ф.И.О. лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена такому лицу)

находящемуся по адресу: _____,)
на обработку (совокупность действий (операций), совершаемых с использованием средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) моих персональных данных, а именно: фамилии, имени, отчества, номера СНИЛС, ИНН, паспортных данных, данных о местонахождении, адреса электронной почты, на срок, установленный для хранения информации аккредитованным удостоверяющим центром Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Федеральным законом от 22.10.2004 №125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативно-правовыми актами Российской Федерации.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Заявитель _____/_____

"___" __ ____ 20__ г.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на создание и выдачу сертификата зарегистрировано в реестре УЦ. Регистрационный №_____ от «___»_____ 20_ г.

_____ _____/ _____/
(должность/полномочия)

«____» _____20_г.

8.2. Приложение №2 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Форма доверенности на представителя индивидуального предпринимателя или юридического лица, данные которого указываются в сертификате

ДОВЕРЕННОСТЬ

г. Москва «__»_____20___ г.

_____
(наименование организации, включая организационно-правовую форму, ИНН, ОГРН, ОГРНИП (только для индивидуальных предпринимателей))

в лице _____,
(должность, фамилия, имя, отчество индивидуального предпринимателя/руководителя организации)

действующего на основании _____
(наименование документа, подтверждающего право действовать от имени юридического лица)

уполномочивает _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта, кем и когда выдан)

выступать в роли заявителя Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг», получить в Удостоверяющем центре ООО «ЭТП ГПБ Консалтинг» сертификат ключа проверки электронной подписи на свое имя, и осуществлять действия в рамках Регламента Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг», установленные для заявителя Удостоверяющего центра «ЭТП ГПБ Консалтинг».

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г.

Подпись представителя _____ _____ подтверждаю.
(Фамилия И.О.) (Подпись)

Руководитель организации _____/_____/

«___»_____20__ г.
М.П.

8.3. Приложение №3 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи

Заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг»

Прошу прекратить действие (аннулировать) сертификат ключа проверки электронной подписи, содержащий следующие поля:

Серийный номер сертификата	
Дата начала действия и дата окончания действия сертификата	
Ф.И.О.	
Организация (не заполняется физическим лицом - владельцем сертификата)	

Владелец (представитель владельца) сертификата _____ / _____/
(ФИО)

«___»_____20__ г.

Руководитель организации _____ / _____/
«___»_____20__ г.
М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «___»_____ 20_ г.

_____ _____/ _____/
(должность/полномочия)

«____» _____20_г.

8.4. Приложение №4 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на подтверждение подлинности электронной подписи в электронном документе

Заявление на подтверждение подлинности электронной подписи в электронном документе

Прошу подтвердить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № _____;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи, на прилагаемом к заявлению носителе – рег. № _____
3. Время, на момент наступления которого требуется подтвердить подлинность электронной подписи: _____

Владелец (представитель владельца) сертификата _____/_____/

«___»_____20__ г.

Руководитель организации _____ / _____/

«___»_____20__ г.

М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на подтверждение подлинности электронной подписи в электронном документе, созданной с сертификатом ключа проверки ЭП, изготовленным Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «___»_____ 20_ г.

_____ _____/ _____/

(должность/полномочия)

«____» _____20_г.

8.5. Приложение №5 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Форма заявления на получение информации о статусе сертификата ключа проверки электронной подписи

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг»

_____
(полное наименование организации, включая организационно-правовую форму/фамилия, имя, отчество)

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____,
(наименование документа, подтверждающего право действовать от имени юридического лица)

просит предоставить информацию о статусе квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг» и содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	ФИО пользователя

Время[1] (период времени) на момент наступления которого требуется установить статус сертификата:
с «_____» по «_____».

Подпись руководителя организации/физического лица: _____
Дата подписания заявления: «____» _____ 20____ г.
М.П.

Отметка Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг»

Данное заявление на получение информации о статусе сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром ООО «ЭТП ГПБ Консалтинг», зарегистрировано в реестре УЦ. Регистрационный №_____ от «___» _____ 20_ г.

_____ _____/ _____/
(должность/полномочия)

«____» _____20_г.

[1] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром.

8.6. Приложение №6 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи

Использование электронных подписей сопровождается рисками финансовых потерь при несанкционированном получении злоумышленниками ключей электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.

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

1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.5. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

1.6. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

1.8. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

1.9. Обратиться в Удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, с заявлением о подтверждении подлинности электронной подписи в электронном документе в случае возникновения конфликтной ситуации, заключающейся в оспаривании авторства и/или содержимого документа, подписанного электронной подписью.

2**. Порядок применения средств квалифицированной электронной подписи**

2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.

2.2. При эксплуатации средств квалифицированной электронной подписи должны использоваться только квалифицированные сертификаты ключей проверки электронной подписи, выпущенные аккредитованным Удостоверяющим центром.

2.3. Средства квалифицированной электронной подписи должны использоваться с сертифицированными средствами антивирусной защиты.

2.4. Инсталляция средств квалифицированной электронной подписи на рабочих

местах должна производиться только с дистрибутива, полученного по доверенному каналу.

2.5. При установке и использовании средств квалифицированной электронной подписи должна быть обеспечена защита аппаратного и программного обеспечения от несанкционированного доступа в соответствии с Руководством администратора безопасности из состава эксплуатационной документации на средство квалифицированной электронной подписи.

2.6. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства вычислительной техники с установленным средствами квалифицированной электронной подписи, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями и обеспечена невозможность негативных действий с их стороны на средства квалифицированной электронной подписи, средства вычислительной техники, на которых эксплуатируются средства квалифицированной электронной подписи, и защищаемую информацию.

2.7. На средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, должно использоваться только лицензионное программное обеспечение фирм-изготовителей и не должны устанавливаться средства разработки программного обеспечения и отладчики.

2.8. Программное обеспечение, устанавливаемое на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

2.9. Для идентификации пользователя при входе в операционную систему и BIOS на технических средствах, предназначенных для работы со средствами квалифицированной электронной подписи, необходимо использовать пароли в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п .);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля не должна превышать 6 месяцев.

2.10. Средствами BIOS должна быть исключена возможность работы на средствах вычислительной техники, предназначенных для работы со средствами квалифицированной электронной подписи, если во время начальной загрузки не проходят встроенные тесты.

2.11. ЗАПРЕЩАЕТСЯ:

– оставлять без контроля средства вычислительной техники, на которых эксплуатируется средства квалифицированной электронной подписи, после ввода ключевой информации либо иной конфиденциальной информации;

– вносить какие-либо изменения в программное обеспечение средств электронной подписи;

– осуществлять копирование ключевых носителей;

– разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

– использовать ключевые носители в режимах, не предусмотренных функционированием средств квалифицированной электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– изменять настройки, установленные программой установки средства электронной подписи или администратором.

– использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами квалифицированной электронной подписи.

3.Правила использования ключевых носителей

3.1. Хранить ключ квалифицированной электронной подписи необходимо исключительно на защищенном ключевом носителе.

3.2. При создании и записи на ключевой носитель ключ квалифицированной электронной подписи должен быть отмечен как неэкспортируемый.

3.3. На ключевой носитель должен быть установлен индивидуальный PIN-код доступа (отличный от установленного по умолчанию).

3.4. Владелец ключа квалифицированной электронной подписи обязан обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц (хранить и использовать носитель таким образом, чтобы исключался несанкционированный доступ к нему других лиц) и сохранять в конфиденциальности PIN-код доступа. Владелец ключа несет персональную ответственность за хранение личных ключевых носителей.

3.5. В случае утери ключевого носителя или наличия оснований подозревать о получении к нему несанкционированного доступа сторонних лиц владелец ключа электронной подписи обязан обратиться в Удостоверяющий центр с заявлением о прекращении или приостановлении действия сертификатов ключей проверки электронной подписи, ключи электронной подписи которых хранятся на носителе.

3.6. Максимальный срок действия ключа квалифицированной электронной подписи составляет 1 (один) год 3 (три) месяца. Ключи квалифицированной электронной подписи, срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами квалифицированной электронной подписи, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

8.7. Приложение №7 к Регламенту УЦ ООО «ЭТП ГПБ Консалтинг». Соглашение об использовании Личного кабинета УЦ ООО «ЭТП ГПБ Консалтинг»

СОГЛАШЕНИЕ
об использовании Личного кабинета
Удостоверяющего центра
Общества с ограниченной ответственностью (ООО) «ЭТП ГПБ Консалтинг»

Настоящее Соглашение об использовании Личного кабинета ООО «ЭТП ГПБ Консалтинг» (далее – Соглашение), устанавливает порядок и общие принципы Дистанционного обслуживания Клиентов с использованием Личного Кабинета. Текст настоящего Соглашения публикуется на Сайте Общества (https://ca.etpgpb.ru).

Настоящее Соглашение является договором присоединения в соответствии с положениями действующего законодательства РФ и заключается путем присоединения потенциального Клиента к установленным настоящим Соглашением условиям в целом, в порядке, определяемом настоящим Соглашением.

Заключение настоящего Соглашения осуществляется путем акцепта потенциальным Клиентом размещенного на Сайте Общества (https://ca.etpgpb.ru) настоящего Соглашения при прохождении процедуры Регистрации в Личном кабинете. Акцепт считается полученным, а Соглашение заключенным с момента успешного прохождения потенциальным Клиентом (по его собственному волеизъявлению) процедуры Регистрации в Личном кабинете, в порядке, изложенном в Разделе 3 настоящего Соглашения и присоединения Клиента к Регламенту Удостоверяющего центра ООО «ЭТП ГПБ Консалтинг» (далее – Регламент), в порядке, предусмотренном Регламентом. После присоединения к Регламенту, настоящее Соглашение является неотъемлемой частью Регламента (Приложением №7 к Регламенту).

Общество вправе по своему усмотрению и без объяснения причин отказаться от заключения настоящего Соглашения с лицом, имеющим намерение стать Клиентом Общества. Изменения и дополнения к настоящему Соглашению, а также решения Общества о сроках и порядке вступления их в силу, доводятся до сведения Клиентов путем их размещения на Сайте Общества, не позднее, чем за 5 (пять) рабочих дней до вступления их в силу. Любые изменения и дополнения в Соглашении с момента вступления в силу равно распространяются на всех Клиентов, присоединившихся к Соглашению, в том числе присоединившихся к Соглашению ранее даты вступления изменений (дополнений) в силу.

Прекращение действия Регламента в отношении Стороны Регламента, в порядке и на основаниях, указанных в Регламенте, автоматически влечет расторжение настоящего Соглашения, которое будет считаться прекращенным (расторгнутым) в дату, когда Регламент будет считаться прекращенным. Обмен сторонами либо направление друг другу отдельного уведомления о прекращении (расторжении) Соглашения в указанном случае не требуется.

Прекращение действия настоящего Соглашения не влияет на юридическую силу и действительность Электронных документов, которыми Общество и Клиент обменивались до прекращения действия Соглашения.

Все споры и разногласия, возникающие между Клиентом и Обществом в процессе исполнения своих прав и обязанностей по настоящему Соглашению или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, Клиент и Общество стараются разрешить путем переговоров. В случае невозможности урегулирования разногласий путем переговоров, предмет спора передается на рассмотрение в Арбитражный суд города Москвы в порядке, определенном действующим законодательством.

1. Термины и определения

1.1. Авторизация – подтверждение полномочий (предоставление прав доступа) Клиента, успешно прошедшего Аутентификацию входа, на получение услуг Общества, предусмотренных Регламентом, с использованием Личного Кабинета на протяжении одного Сеанса соединения.

1.2. Аутентификационные данные – Логин и Пароль, используемые для целей установления личности Клиента при оказании услуг Дистанционного обслуживания Обществом и являющиеся простой электронной подписью Клиента.

1.3. Аутентификация входа – процедура проверки соответствия предъявленных Аутентификационных данных и Учетной записи Клиента на вход, выполняемая перед установлением Сеанса соединения. Без успешной Аутентификации входа Сеанс соединения не устанавливается.

1.4. Аутентификация операции – процедура подписания Клиентом Электронного документа простой электронной подписью и проверки принадлежности Клиенту полученного Обществом посредством Личного кабинета Электронного документа с использованием простой электронной подписи в соответствии с настоящим Соглашением.

1.5. Дистанционное обслуживание – предоставление услуг (далее - **Услуги**) в соответствии с Регламентом на основании запросов, передаваемых Клиентом удаленным образом с использованием Личного кабинета. Дистанционное обслуживание предоставляет возможность Клиентам осуществлять Операции и получать информацию в соответствии с Регламентом. Функциональные возможности Личного Кабинета определяются Обществом самостоятельно.

1.6. Защита информации – комплекс мероприятий по предотвращению утечки информации или воздействия на нее по техническим каналам за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности технических средств. Мероприятия по Защите информации при использовании Личного Кабинета реализуются в обязательном порядке как Обществом, так и Клиентом.

1.7. Клиент – индивидуальный предприниматель, юридическое или физическое лицо, присоединившиеся к Регламенту, которому Общество предоставляет Услуги. Все положения и обязанности, установленные в отношении Клиента согласно настоящего Соглашения, в равной мере относятся к представителю Клиента, если Клиент – юридическое лицо или физическое лицо, уполномоченное иным физическим лицом получить квалифицированный сертификат ключа проверки электронной подписи от его имени на основании доверенности.

1.8. Компрометация Аутентификационных данных – утрата, подозрение в утрате или возникновение подозрения о доступе третьих лиц к Аутентификационным данным.

1.9. Личный кабинет (ЛК) – раздел сайта «Финансовый супермаркет» (https://etpfs.ru), размещенный в закрытой части указанного сайта и доступный только зарегистрированным пользователям – Клиентам (представителям Клиента) и используемый Обществом для Дистанционного обслуживания Клиентов в рамках Регламента. Личный кабинет позволяет Обществу и Клиенту (представителю Клиента) осуществлять обмен определенными Электронными документами и информацией. Для использования Личного кабинета отсутствует необходимость установки клиентской части программного обеспечения на компьютер (иное устройство) Клиента. Правообладателем сайта «Финансовый супермаркет» (https://etpfs.ru) является Общество с ограниченной ответственностью «Электронная торговая площадка ГПБ» (ИНН 7724514910). Доступ к Личному кабинету Клиентам Общества через сайт «Финансовый супермаркет» (https://etpfs.ru) предоставляется на основании соглашения, заключенного между Правообладателем и Обществом. Правообладателем программного обеспечения Личного кабинета является Общество. Через Личный кабинет осуществляется формирование Клиентом Аутентификационных данных, передача Клиентом Обществу для предварительной проверки сканированных копий документов (если применимо), формирование Клиентом запроса сертификата ключа проверки электронной подписи, а также подписание Клиентом простой электронной подписью документов, предлагаемых к подписанию Обществом. Доступ Клиента (представителя Клиента) в Личный кабинет осуществляется после Авторизации, на основе введенных Клиентом (представителем Клиента) Логина и Пароля для входа в Личный кабинет.

1.10. Логин (Имя Пользователя) – комбинация символов (букв и цифр) установленная программным обеспечением Личного кабинета при создании учетной записи, используемая для Аутентификации входа в Личный кабинет. Логин используется многократно.

1.11. Общество – Общество с ограниченной ответственностью «ЭТП ГПБ Консалтинг», ОГРН 5167746487651, ИНН 7728356929.

1.12. Операция – любая операция Клиента (действие, связанное с оказанием Обществом Клиенту Услуг) осуществляемая в соответствии с Регламентом с использованием Личного кабинета.

1.13. Пароль – часть Аутентификационных данных, комбинация символов (букв и цифр), служащая для Аутентификации входа. Пароль Клиента в сочетании с Логином обеспечивают однозначную Аутентификацию входа. Пароль используется многократно, и может быть изменен Клиентом самостоятельно неограниченное количество раз. По требованию Общества Клиент обязан изменить Пароль в течение не более чем 24 (двадцать четыре) часа.

1.14. Правообладатель - Общество с ограниченной ответственностью «Электронная торговая площадка ГПБ» (ИНН 7724514910), владеющее интеллектуальным правом на сайты «ЭТП» (https://etpgpb.ru) и «Финансовый супермаркет» (https://etpfs.ru).

1.15. Простая электронная подпись (ПЭП) - электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом. Для создания ПЭП используется сочетание идентификатора (логина) и пароля (кода). Случаи и порядок использования ПЭП определяются настоящим Соглашением.

1.16. Регистрация – процедура успешного ввода персональных данных Клиента (представителя Клиента) на Сайте, и последующее создание Аутентификационных данных для получения доступа к функционалу Личного кабинета.

1.17. Сайт – официальная интернет-страница Общества в сети «Интернет»: https://ca.etpgpb.ru.

1.18. Сайт «Финансовый супермаркет» - интернет-страница Правообладателя в сети «Интернет»: https://etpfs.ru, в закрытой части которой размещен Личный кабинет.

1.19. Сеанс соединения – промежуток времени, в течение которого Клиент авторизован для работы в Личном кабинете. Для начала Сеанса соединения необходимо пройти Аутентификацию входа. Длительность Сеанса соединения при отсутствии активности Клиента в Личном кабинете определяется Обществом самостоятельно.

1.20. Учетная запись Клиента – уникальная взаимно-однозначно связанная с Аутентификационными данными последовательность символов, присваиваемая Обществом каждому Клиенту.

1.21. Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

2. Общие положения

2.1. Дистанционное обслуживание с использованием ЛК позволяет Клиенту получать определенную информацию, проводить определенные Операции и получать доступ к определенным Услугам Общества через Интернет. Перечень Операций, которые могут осуществляться посредством ЛК определяется Обществом самостоятельно.

2.2. Настоящее Соглашение определяет:

• порядок подключения Клиента к ЛК, при котором Клиент принимает полностью условия настоящего Соглашения;

• порядок использования Клиентом ЛК;

• порядок Защиты информации при использовании Клиентом ЛК;

• порядок осуществления Обществом Дистанционного обслуживания Клиента с использованием ЛК;

• порядок прекращения Обществом Дистанционного обслуживания с

использованием ЛК.

2.3. Общество предоставляет Клиенту право использовать ЛК на следующих условиях:

• территория использования – все страны мира;

• срок использования - в течение срока действия настоящего Соглашения;

• стоимость использования – безвозмездно;

• Клиент не вправе заключать сублицензионные договоры или соглашения с третьими лицами.

2.4. Дистанционное обслуживание Клиентов при помощи ЛК осуществляется Обществом на основании присоединения Клиента к Регламенту и настоящему Соглашению.

2.5. С использованием ЛК могут осуществляться только те Операции, перечень которых определен Обществом. Общество имеет право в одностороннем порядке ограничить все или часть Операций, или функциональных возможностей ЛК без объяснения причин такого ограничения.

2.6. Все Операции в ЛК осуществляются только после формирования Клиентом и успешной проверки Обществом Аутентификационных данных. Клиент и Общество признают, что сформированные Клиентом и успешно проверенные Обществом Аутентификационные данные являются Простой электронной подписью клиента, равнозначной собственноручной подписи Клиента на документах, составленных на бумажном носителе.

2.7. Информирование Клиента об изменении Условий Соглашения происходит путем размещения указанной информации, в том числе в виде Соглашения в новой редакции, на Сайте Общества.

2.8. Клиент может пользоваться ЛК с помощью персонального компьютера (иного устройства), подключенного к сети Интернет. Требования, предъявляемые к оборудованию и программному обеспечению, необходимому для доступа в ЛК, содержатся на Сайте Общества. Требования, предъявляемые к защите информации на используемом для получения доступа к ЛК на персональном компьютере (ином устройстве), приведены в Приложении 1 к настоящему Соглашению.

3. Регистрация и авторизация Клиента

3.1. Регистрация Клиента и активация доступа к ЛК осуществляется на сайте «Финансовый супермаркет» (https://etpfs.ru) в соответствии с процедурой, указанной в п.3.2 настоящего Соглашения.

В отношении Клиента – юридического лица процедура Регистрации и Авторизации Клиента осуществляется в отношении каждого представителя Клиента.

3.2. В целях Регистрации каждый потенциальный Клиент - физическое лицо/представитель Клиента - юридического лица/индивидуальный предприниматель, имеющий намерение присоединиться к Регламенту, вводит запрашиваемые на Сайте персональные данные, а также подтверждает (путем проставления символов в специальных полях) ознакомление с условиями обработки персональных данных и ознакомление с условиями настоящего Соглашения, являющегося Приложением №7 к Регламенту, тем самым подтверждая готовность акцептовать их.

3.2.1. На адрес электронной почты потенциального Клиента, указанный при введении персональных данных на Сайте, поступает уведомление о создании учетной записи зарегистрированного пользователя, содержащее функционал подтверждения регистрации, ссылку для входа в Личный кабинет.

3.2.2. При входе потенциального Клиента в ЛК запускается процедура Аутентификации входа. При успешной Аутентификации входа осуществляется Авторизация и устанавливается Сеанс соединения, а процедура Регистрации считается завершенной.

3.2.3. Потенциальный Клиент - физическое лицо/представитель Клиента - юридического лица/индивидуальный предприниматель в течение не более 5 (пяти) рабочих дней с момента завершения процедуры Регистрации предоставляет Обществу подписанный бланк заявления на создание и выдачу сертификата ключа проверки электронной подписи и полный комплект документов, указанных в Регламенте,

необходимых для оказания Услуг, в порядке, определенном Регламентом.

3.3. Соглашение считается заключенным в порядке ст.428 ГК РФ с момента завершения в отношении потенциального Клиента процедуры Регистрации, получения Обществом полного комплекта документов и присоединения к Регламенту в порядке, предусмотренном Регламентом.

3.4. С момента завершения процедуры Регистрации и до момента присоединения потенциального Клиента к Регламенту, ЛК функционирует с ограниченным функционалом.

3.5. Клиент-физическое лицо/представитель Клиента-юридического лица/индивидуальный предприниматель получает полный доступ в ЛК и вправе использовать его для осуществления Операций, только с момента присоединения Клиента к Регламенту и настоящему Соглашению.

3.6. Требования, указанные в настоящем Соглашении в отношении Клиента, также применимы и обязательны для соблюдения представителями Клиента.

3.7. Созданные Аутентификационные данные используются Клиентом при каждой Аутентификации входа и Авторизации в ЛК.

3.7.1. Пароль, созданный Клиентом, должен быть изменен им по требованию Общества, которое может быть передано Клиенту с использованием ЛК или иным способом, определяемым по усмотрению Общества.

3.7.2. Клиент не должен сообщать Аутентификационные данные третьим лицам, в том числе работникам Общества по телефону, электронной почте или иным способом. Использование Аутентификационных данных допускается только при работе через сеть Интернет без участия работников Общества.

3.7.3. Доступ в ЛК в случае утраты/Компрометации Аутентификационных данных Клиентом может быть восстановлен путем повторного прохождения Клиентом процедуры Регистрации (восстановления Логина или Пароля) в ЛК в порядке, указанном в инструкции по восстановлению Логина или Пароля, размещенной на Сайте.

3.8. При каждой попытке получения доступа в ЛК, Клиенту необходимо ввести запрашиваемые Аутентификационные данные. После ввода указанных данных и прохождения процедуры Аутентификации входа, ЛК осуществит Авторизацию и автоматически запустит Сеанс соединения.

4. Особенности использования простой электронной подписи

4.1. В случае присоединения Клиента к Регламенту и для целей исполнения настоящего Соглашения в целях обеспечения безопасности при осуществлении Операций и формировании Электронных документов с использованием ЛК применяется механизм подтверждения Операций и подписания Электронных документов с использованием Простой электронной подписи.

4.2. Формирование, использование и подтверждение Сторонами Простой электронной подписи осуществляется в соответствии с настоящим Соглашением.

4.3. Для создания Простой электронной подписи при Аутентификации операции применяется Логин и Пароль Клиента. Для проверки Простой электронной подписи при Аутентификации операции применяется проверка Аутентификационных данных.

4.4. Общество вправе самостоятельно определять Операции, осуществление которых и подписание Простой электронной подписью возможно без или с использованием простой электронной подписи.

4.5. Формирование Простой электронной подписи Клиентом осуществляется путем выполнения последовательных действий в ЛК в соответствии с инструкциями в экранных формах при совершении Операции, при этом:

• Клиент производит Аутентификацию входа;

• Клиент инициирует Операцию и инициирует Аутентификацию операции, вводя Аутентификационные данные;

• при получении запроса на Аутентификацию операции Общество проверяет соответствие Аутентификационных данных учетной записи Клиента, имеющейся в Обществе;

• соответствие Аутентификационных данных учетной записи Клиента расценивается Обществом как одобрение на Операцию;

• формируется Электронный документ и соответствующая ему Простая электронная

подпись в соответствии с настоящим Соглашением.

4.6. Общество вправе потребовать от Клиента, а Клиент обязан подписать Электронный документ, подписанный ранее Простой электронной подписью, собственноручно и передать его Обществу почтовым отправлением по адресу Общества: 117342, г. Москва, ул. Миклухо-Маклая, д. 40, этаж 1, помещение IV, комната 20. Требования о подписании собственноручной подписью документов передается Обществом Клиенту через ЛК или по адресу электронной почты, указанной Клиентом при Регистрации.

5. Порядок Дистанционного обслуживания

5.1. Перечень Операций, которые может совершать Клиент с использованием ЛК, обусловлен функциональными возможностями программного обеспечения ЛК и может быть изменен Обществом в одностороннем порядке без объяснения причин.

Общество оставляет за собой право в любое время улучшать или модифицировать ЛК, расширять или сужать его функционал.

5.2. Все Операции в ЛК осуществляются в соответствии с законодательством Российской Федерации и Регламентом.

5.4. Экранные формы Электронных документов, подаваемых Клиентом в Общество с использованием ЛК, могут отличаться от форм документов, установленных Регламентом, и могут содержат лишь необходимую (существенную) информацию направляемого Электронного документа.

В случае необходимости данная информация преобразовывается в автоматическом режиме и переносится на бумажные формы соответствующих Электронных документов, предусмотренных Регламентом, при этом вместо собственноручной подписи Клиента в бумажной форме указывается Электронная подпись, которой подписан такой Электронный документ в соответствии с настоящим Соглашением.

5.5. Все Операции в ЛК осуществляются на основании Электронных документов, оформленных Клиентом и подписанных Электронной подписью (за исключением случаев, указанных в настоящем Соглашении) в соответствии с настоящим Соглашением. Электронные документы формируются в ЛК в электронном виде с использованием средств, подтверждающих, что подпись создана Клиентом (данным средством является совокупность мер по Аутентификации входа и Аутентификации операции).

5.6. Стороны признают, что Электронные документы, сформированные, подписанные Простой электронной подписью в соответствии с настоящим Соглашением и переданные в порядке, предусмотренном настоящим Соглашением, имеют равную юридическую силу и влекут такие же правовые последствия, что и документы, оформленные на бумажном носителе в соответствии с требованиями законодательства Российской Федерации, Регламента и подписанные собственноручной подписью Клиента.

5.7. Для осуществления некоторых Операций Клиенту может потребоваться установить дополнительное программное обеспечение на свой персональный компьютер. Сведения о необходимости установки дополнительного программного обеспечения содержаться в ЛК.

6. Права и обязанности Сторон

6.1. Общество обязано:

6.1.1. предоставить Клиенту возможность получить доступ к ЛК в случае заключения Клиентом с Обществом настоящего Соглашения в порядке, предусмотренном Соглашением;

6.1.2. производить за свой счет и в разумно короткие сроки проведение работ по восстановлению работоспособности ЛК в случае сбоев оборудования и коммуникаций Общества;

6.1.3. принять все возможные меры к недопущению приема от Клиента Электронного документа без предварительной успешной Аутентификации входа и Аутентификации операции;

6.1.4. незамедлительно с момента получения обращения Клиента об утрате Аутентификационных данных, Компрометации Аутентификационных данных

приостановить предоставление Клиенту доступа к ЛК. При обращении Клиента по телефону установление личности Клиента производится в порядке, предусмотренном Регламентом;

6.1.5. осуществлять консультирование Клиента по вопросам эксплуатации ЛК;

6.1.6. обеспечить Защиту информации;

6.1.7. хранить Электронные документы в течение срока, установленного законодательством Российской Федерации и Регламентом для хранения соответствующих документов;

6.1.8. предоставлять по письменному требованию Клиенту документы, связанные с использованием Клиентом ЛК, в срок не позднее 30 (тридцати) дней со дня получения соответствующего запроса.

6.2. Общество имеет право:

6.2.1. не принимать Электронный документ Клиента в случае, если Аутентификация операции произошла неуспешно;

6.2.2. приостановить доступ в ЛК в случае неисполнения или ненадлежащего исполнения Клиентом условий настоящего Соглашения или Регламента как полностью, так и частично;

6.2.3. в одностороннем порядке изменять условия настоящего Соглашения, с уведомлением Клиента о таких изменениях в порядке и сроки, предусмотренные Регламентом и настоящим Соглашением;

6.2.4. определять, дополнять и изменять перечень Операций и Электронных документов, которые можно осуществлять/направлять в Общество с использованием ЛК;

6.2.5. определять и изменять порядок и время передачи Клиентом Электронных документов, порядок и время приема и обработки Обществом Электронных документов;

6.2.6. приостановить использование ЛК в случае возникновения у Общества технических неисправностей или других обстоятельств, препятствующих использованию ЛК до устранения возникших обстоятельств;

6.2.7. о возникшем сбое (неисправности) и предполагаемых сроках его устранения Общество оповещает Клиента публикацией информации на Сайте Общества;

6.2.8. без предварительного уведомления Клиента временно приостановить или ограничить доступ Клиента в ЛК, а также обязать Клиента выполнить требования (устранить нарушения требований) Приложения №1 к настоящему Соглашению, сменить Логин и/или Пароль, используемые Клиентом для Аутентификации входа в ЛК, при наличии у Общества достаточных оснований считать, что по используемому Клиентом каналу доступа возможна попытка несанкционированного доступа от имени Клиента или в иных случаях по усмотрению Общества;

6.2.9. проводить комплекс технических мероприятий по поддержанию ЛК в режиме нормальной эксплуатации;

6.2.10. в целях обеспечения безопасности устанавливать средствами ЛК ограничения по времени на периоды бездействия в пределах одного Сеанса соединения (тайм- аут);

6.2.14. в любой момент потребовать от Клиента подписания документов на бумажном носителе, эквивалентных по смыслу и содержанию, переданных Клиентом Электронных документов;

6.2.15. приостановить Дистанционное обслуживание Клиента в случае нарушения последним порядка использования ЛК, предусмотренного Соглашением.

6.3. Клиент обязан:

6.3.1. соблюдать положения настоящего Соглашения;

6.3.2. обеспечить конфиденциальность, а также хранение информации об Аутентификационных данных способом, исключающим доступ к ним третьих лиц, а также немедленно уведомлять Общество о подозрении, что Аутентификационные данные могут быть использованы посторонними лицами;

6.3.3. в случае утраты Аутентификационных данных или наличия подозрений, что они стали известны третьим лицам, Клиент должен незамедлительно, после обнаружения указанных фактов, сообщить об этом Обществу по телефонной связи по номеру, указанному на Сайте Общества;

6.3.4. контролировать правильность реквизитов, указываемых в Электронных документах;

6.3.5. немедленно сообщать Обществу любыми доступными способами обо всех случаях, свидетельствующих о попытках посторонних лиц получить доступ к ЛК;

6.3.6. исполнять требования Приложения №1 к настоящему Соглашению;

6.3.7. регулярно обращаться к Сайту Общества в целях ознакомления с возможными уведомлениями, сообщениями Общества, а также изменениям, дополнениям Соглашения и приложений к нему.

6.4. Клиент имеет право:

6.4.1. обращаться в Общество для получения консультаций по работе с ЛК;

6.4.2. в случае возникновения сбоев в работе ЛК представлять в Общество и получать от Общества документы в ином порядке, предусмотренном Регламентом;

6.4.3. в случае несогласия с изменениями Соглашения или в иных случаях в любое время отказаться от исполнения настоящего Соглашения в порядке, предусмотренном настоящим Соглашением;

6.4.4. обращаться в Общество с заявлениями, в том числе при возникновении споров, связанных с использованием ЛК, а также получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме, в срок не более 30 (тридцати) календарных дней со дня получения Обществом таких заявлений.

7. Ответственность Сторон

7.1. Стороны не несут ответственность за убытки, понесенные одной Стороной не по вине другой Стороны в результате использования ЛК, в том числе при исполнении ошибочных Электронных документов, если переданные Электронные документы были оформлены надлежащем образом и подписаны действительной Электронной подписью, используемой в соответствии с настоящим Соглашением.

7.2. Стороны взаимно освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению, если оно вызвано факторами непреодолимой силы и/или чрезвычайными обстоятельствами, к которым относятся, в частности:

• пожары, наводнения, иные стихийные бедствия или техногенные катастрофы;

• разрушения или значительные повреждения занимаемых Обществом помещений;

• нестабильность или отключение электроэнергии;

• неработоспособность средств связи, включая средства телекоммуникаций;

• массовые беспорядки, вооруженные столкновения, демонстрации;

• террористические акты или диверсии;

• любые другие подобные события или обстоятельства, которые могут существенным образом затруднить или сделать невозможным выполнение обязательств по

настоящему Соглашению;

• принятие или любые изменения законодательных, или иных актов государственных органов Российской Федерации, или распоряжения данных органов, инструкции, указания, заявления, письма, телеграммы или иные действия (далее – акты), которые прямо или косвенно, или при определенном их толковании или определенном стечении обстоятельств, начиная с момента утверждения данных актов, или с иного срока, временно или на неопределенный срок сделали, делают или могут сделать невозможным, или значительно затруднить дальнейшее выполнение обязательств по настоящему Соглашению.

7.3. Общество не несет ответственность за ущерб, возникший:

• вследствие Компрометации Аутентификационных данных, их утраты или несанкционированного доступа к ним и их использования третьими лицами;

• в случае нарушения Клиентом условий настоящего Соглашения;

• вследствие принятия высшими органами законодательной и исполнительной власти Российской Федерации решений, которые делают невозможным для Общества выполнение своих обязательств по настоящему Соглашению;

• вследствие сбоев в работе линий связи, обрыва линий связи, выхода из строя оборудования у Оператора сотовой связи и/или оператора доступа к сети Интернет;

• в случае несанкционированного подключения к ЛК и получения доступа третьих лиц, если такой доступ имел место не по вине Общества.

7.4. Общество не несет ответственность:

• за качество линий связи;

• за убытки или упущенную выгоду, понесенные Клиентом, вследствие исполнения Обществом Электронного документа, составленного Клиентом с ошибками (некорректно).

7.5. Клиент несет ответственность за все действия, произведенные через ЛК после прохождения Аутентификации входа и (при совершении Операции) Аутентификации операции.

7.6. Клиент принимает программное обеспечение ЛК в пользование в состоянии «как есть». Клиенту известны важнейшие функциональные свойства ЛК, а также лицензионные условия использования, предусмотренные в Соглашении. Общество не несет ответственности за какой-либо ущерб (включая все, без исключения, случаи понесенных либо предполагаемых расходов, потери прибылей, прерывания деловой активности, потери деловой информации, либо других денежных потерь), связанный с использованием или невозможностью использования ЛК.

7.7. Общество не несет ответственности за совместимость ЛК с программными продуктами, установленным на компьютере (ином устройстве) Клиента.

7.8. Общество не несет ответственности за последствия и ущерб, которые могут быть причинены в случае использования ЛК не в соответствии с Соглашением.

7.9. Общество не несет ответственность за возникновение сбоев и ошибок в работе ЛК, за потери и повреждение данных, связанные с использованием ЛК.

7.10. Клиент, осуществляя подписание Электронных документов и их направление через информационно-телекоммуникационную сеть Интернет с использованием ЛК, принимает на себя все риски, связанные с несанкционированным доступом третьих лиц к ЛК и конфиденциальным данным Клиента.

8. Соглашение и гарантии Сторон

8.1. Клиент и Общество признают используемые ими в рамках настоящего Соглашения системы обработки, хранения, Защиты информации и передачи информации достаточными для обеспечения надежной, эффективной и безопасной работы и защиты от несанкционированного доступа, а также для подтверждения авторства и подлинности Электронных документов.

8.2. Клиент подтверждает свое согласие с тем, что Электронные документы, сформированные в ЛК в электронном виде и подтвержденные (подписанные) Электронной подписью в соответствии с настоящим Соглашением имеют юридическую силу и влекут предусмотренные для данного документа правовые последствия в соответствии с законодательством Российской Федерации и настоящим Соглашением.

8.3. Клиент признает, что получение Обществом документов, сформированных в ЛК в электронном виде с использованием Электронной подписи, эквивалентно получению Обществом документов на бумажном носителе, заверенных собственноручной подписью Клиента.

8.4. Клиент подтверждает и гарантирует соблюдение режима Защиты информации и отсутствие доступа третьих лиц к ЛК.

8.5. Клиент подтверждает, что уведомлен о рисках, связанных с использованием Электронной подписи при подписании Электронных документов и передаче таких документов по защищенным и/или открытым каналам связи, согласен с рисками и принимает их на себя в полном объеме.

9. Конфиденциальность

9.1. Общество обязуется принять меры для предотвращения несанкционированного доступа третьих лиц к конфиденциальной информации, связанной с использованием Клиентом ЛК. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Российской Федерации и Договором.

9.2. В случаях, когда использование паролей предполагает передачу Клиенту либо хранение Обществом какой-либо конфиденциальной информации, Общество обязуется

принять все необходимые меры организационного и технического характера для предотвращения доступа третьих лиц к такой информации до передачи ее Клиенту, а также во время ее хранения.

9.3. Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации по сети Интернет влечет риск несанкционированного доступа к такой информации сторонних лиц.

10. Приложение

Приложение 1. Требования реализации мер по защите информации Клиентом при работе с Личным кабинетом.

Приложение 1 к Соглашению об использовании Личного кабинета ООО «ЭТП ГПБ Консалтинг»

ТРЕБОВАНИЯ
к реализации мер по защите информации Клиентом
при работе с Личным кабинетом

1. Требования технической защиты устройства доступа Клиента к Личному кабинету, реализуемые Клиентом.

Перед подключением к Личному кабинету (далее – ЛК) Клиент должен обеспечить работу устройства в следующем режиме:

• на устройстве, с которого планируется осуществлять подключение к ЛК, должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение и web-браузер;

• устройство должно использовать процедуру Аутентификации доступа к устройству прежде, чем предоставить ресурсы пользователю (требуется ввод Логина и Пароля).

2. Организационные меры по защите информации, реализуемые Клиентом:

• Клиент никогда и никому не сообщает Логин и Пароль;

• Клиент перед Аутентификацией входа должен убедиться, что в адресной строке браузера указан правильный адрес ЛК;

• Клиент внимательно проверяет информацию об Операции, которую собирается совершить;

• Клиент, используя устройство, с которого получает доступ в ЛК, осуществляет избирательную навигацию в сети Интернет и старается не посещать неизвестные ему сайты.