УТВЕРЖДЕН
приказом Акционерного общества
«ИнфоТеКС Интернет Траст»
от 27.11.2024 № 145-11/24

РЕГЛАМЕНТ
оказания Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аккредитованный удостоверяющий центр - удостоверяющий центр, получивший аккредитацию в соответствии с требованиями, установленными статьей 16 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон «Об электронной подписи»).

Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата) - физическое лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Головной удостоверяющий центр - удостоверяющий центр, функции которого осуществляет уполномоченный федеральный орган.

Доверенное лицо - юридическое лицо или индивидуальный предприниматель, наделенные Удостоверяющим центром полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронных подписей, а также вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра при условии идентификации Заявителя при его личном присутствии.

Единая система идентификации и аутентификации - федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Единая биометрическая система - федеральная государственная информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации.

Единый портал госуслуг - федеральная государственной информационная система "Единый портал государственных и муниципальных услуг (функций)».

Запрос на сертификат ключа проверки электронной подписи (далее - запрос на сертификат) - электронное сообщение, соответствующее виду структуры CertificationRequest, определенной в пункте 7 Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи, утвержденного приказом Минцифры России от 14.09.2020 № 472 (далее - Формат электронной подписи), содержащее значение ключа проверки электронной подписи, а также иную информацию, необходимую для создания сертификата.

Заявитель - физическое лицо, обращающееся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в Удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Идентификация Заявителя - совокупность мероприятий по установлению сведений о Заявителе и их проверке, осуществляемых в соответствии с Федеральным законом «Об электронной подписи».

Информационная система Удостоверяющего центра - автоматизированная информационная система, обеспечивающая регистрацию Пользователей и выполнение сервисных операций в процессе создания и выдачи Пользователям квалифицированных сертификатов ключей проверки электронных подписей.

Инфраструктура - информационно-технологическая и коммуникационная инфраструктура, подключение Удостоверяющего центра к которой производится в порядке, установленном в

соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".

Квалифицированная электронная подпись - усиленная электронная подпись, которая соответствует всем признакам квалифицированной электронной подписи, определенным Федеральным законом «Об электронной подписи».

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом «Об электронной подписи», приказом ФСБ России от 27.12.2011 № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи», и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

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

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи**.**

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

Компрометация ключа электронной подписи - нарушение конфиденциальности ключа электронной подписи, связанное с утратой доверия к тому, что используемый ключ электронной подписи недоступен посторонним лицам, или подозрением, что ключ электронной подписи был временно доступен неуполномоченным лицам.

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Личный кабинет Пользователя - персональное информационное пространство Пользователя в информационной системе Удостоверяющего центра.

Метка доверенного времени - достоверная информация в электронной форме о дате и времени подписания электронного документа электронной подписью, создаваемая и проверяемая доверенной третьей стороной, удостоверяющим центром или оператором информационной системы и полученная в момент подписания электронного документа электронной подписью в установленном уполномоченным федеральным органом порядке с использованием программных и (или) аппаратных средств, прошедших процедуру подтверждения соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

Мобильное приложение - устанавливаемое на мобильное устройство Пользователя мобильное приложение, содержащее в своем составе средство криптографической защиты информации, выполняющее, в частности, функции средства электронной подписи, и входящее в состав специализированной защищенной автоматизированной системы Удостоверяющего центра.

Плановая смена ключа электронной подписи - смена ключа электронной подписи, производимая в период действия ключа электронной подписи в соответствии с установленной периодичностью, не вызванная компрометацией ключа электронной подписи.

Пользователь Удостоверяющего центра (далее - Пользователь) - физическое лицо, присоединившееся к настоящему Регламенту и зарегистрированное в информационной системе Удостоверяющего центра.

Пункт регистрации - место осуществления деятельности Удостоверяющего Центра либо Доверенного лица Удостоверяющего центра.

Регистрационные данные Пользователя - сведения, предоставляемые Пользователем в целях получения сертификата ключа проверки электронной подписи.

Реестр сертификатов - база данных Удостоверяющего центра, содержащая сведения о выданных и аннулированных Удостоверяющим центром квалифицированных сертификатах ключей проверки электронных подписей.

Сертификат ключа проверки электронной подписи (далее - сертификат) - электронный документ или документ на бумажном носителе, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных сертификатов - отдельный раздел реестра сертификатов, содержащий перечень уникальных номеров сертификатов ключей проверки электронных подписей, которые были аннулированы или действие которых на определенный момент времени было прекращено Удостоверяющим центром до истечения срока их действия, а также информацию о датах и об основаниях аннулирования или прекращения действия этих сертификатов.

Средства криптографической зашиты информации - аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографические преобразования информации для обеспечения ее защиты от несанкционированного доступа, от навязывания ложной информации и (или) обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций удостоверяющего центра.

Удостоверяющий центр - Акционерное общество «ИнфоТеКС Интернет Траст», осуществляющее функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».

Уполномоченный сотрудник Пункта регистрации - сотрудник Удостоверяющего центра или Доверенного лица Удостоверяющего центра, выполняющий непосредственные действия по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей при условии идентификации Заявителя при его личном присутствии.

Уполномоченный федеральный орган - федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи.

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.

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.

OCSP (Online Certificate Status Protocol) - протокол, используемый для получения в режиме реального времени информации о статусе сертификата от сервиса проверки статуса сертификата Удостоверяющего центра.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет регулирования Регламента

Настоящий Регламент устанавливает порядок реализации функций аккредитованного Удостоверяющего центра Акционерного общества «ИнфоТеКС Интернет Траст» и исполнения его обязанностей в соответствии с требованиями, установленными в соответствии с Федеральным законом «Об электронной подписи», определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра.

1.2. Идентификация Регламента

Наименование документа: «Регламент оказания Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей».

Версия: 8.2.

1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде на сайте Акционерного общества «ИнфоТеКС Интернет Траст» iitrust.ru.

1.4. Область применения Регламента

Настоящий Регламент предназначен служить средством официального уведомления и информирования всех заинтересованных сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра, а также соглашением, налагающим обязанности на все вовлеченные в эти взаимоотношения стороны.

1.5. Срок действия Регламента

1.5.1. Настоящий регламент вступает в силу со дня его публикации и действует до момента уведомления Удостоверяющим центром о прекращении действия Регламента.

1.5.2. Уведомление о прекращении действия Регламента осуществляется способом, определенным в разделе «Публикация Регламента».

1.6. Присоединение к Регламенту

1.6.1. Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса Российской Федерации.

1.6.2. Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявки на регистрацию в Удостоверяющем центре в порядке, определенном разделом 7.1 настоящего Регламента. С момента подачи заявки Заявитель считается присоединившимся к Регламенту и становится стороной Регламента – Пользователем Удостоверяющего центра.

1.6.3. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его положений в редакции, действующей на момент подачи заявки на регистрацию в Удостоверяющем центре. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

1.7. Порядок утверждения и внесения изменений в Регламент

1.7.1. Регламент утверждается приказом Акционерного общества «ИнфоТеКС Интернет Траст».

1.7.2. Сообщения об ошибках в положениях настоящего Регламента, а также предложения по уточнению его положений могут направляться в Удостоверяющий центр по электронной почте в соответствии с контактной информацией, указанной в разделе 1.10 настоящего Регламента.

1.7.3. Изменения и дополнения в Регламент вносятся Удостоверяющим центром в одностороннем порядке.

1.7.4. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра не оказывают либо оказывают незначительное влияние на условия предоставления услуг Удостоверяющего центра, вносятся без изменения номера версии данного документа.

1.7.5. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра могут иметь значительное влияние на условия предоставления услуг Удостоверяющего центра, вносятся с увеличением номера версии данного документа.

1.7.6. Уведомление пользователей о внесении изменений в Регламент осуществляется способом, определенным в разделе "Публикация Регламента".

1.8. Основания осуществления деятельности Удостоверяющего центра

1.8.1. Удостоверяющий центр осуществляет свою деятельность на основании разрешительных документов на осуществление видов деятельности, связанных с предоставлением услуг аккредитованного удостоверяющего центра:

- Лицензия на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
- Уведомление уполномоченного федерального органа об аккредитации Удостоверяющего центра.

1.8.2. Копии документов, указанных в пункте 1.8.1, публикуются на сайте Акционерного общества «ИнфоТеКС Интернет Траст» iitrust.ru.

1.9. Информация о месте нахождения и графике работы Удостоверяющего центра

1.9.1. Адрес места нахождения Удостоверяющего центра Акционерного общества «ИнфоТеКС Интернет Траст»: 127287, Москва, ул. Мишина, дом 56, стр. 2, этаж 3, пом. IX, комн. 11.

1.9.2. График работы Удостоверяющего центра: ежедневно, кроме выходных и праздничных дней, с 9:00 до 18:00 по московскому времени.

1.10. **Контактная информация Удостоверяющего центра**

Телефон: 8-800-250-8-265.

Адрес электронной почты: 77@iitrust.ru.

1.11. **Порядок информирования о предоставлении услуг Удостоверяющего центра**

Информация о предоставлении услуг Удостоверяющего центра размещена на сайте Удостоверяющего центра iitrust.ru. Указанную информацию можно также получить, обратившись в Удостоверяющий центр по телефону или электронной почте.

1.12. **Стоимость услуг Удостоверяющего центра**

1.12.1. Удостоверяющий центр осуществляет свою деятельность на платной основе.

1.12.2. Информация о стоимости услуг Удостоверяющего центра размещена на сайте Акционерного общества «ИнфоТеКС Интернет Траст» iitrust.ru, а также определяется договором, заключаемым Акционерным обществом «ИнфоТеКС Интернет Траст» с Пользователем или в интересах Пользователя.

1.12.3. Сроки и порядок расчетов за оказанные услуги Удостоверяющего центра определяются договором, заключаемым Акционерным обществом «ИнфоТеКС Интернет Траст» с Пользователем или в интересах Пользователя.

1.12.4. Оплата услуг Удостоверяющего центра осуществляется в российских рублях путем перечисления денежных средств на расчетный счет Акционерного общества «ИнфоТеКС Интернет Траст» или иным способом, предусмотренным договором, заключаемым Акционерным обществом «ИнфоТеКС Интернет Траст» с Пользователем или в интересах Пользователя.

1.12.5. На безвозмездной основе предоставляются следующие услуги Удостоверяющего центра:

- выдача копий сертификатов в форме документов на бумажном носителе;
- предоставление любому лицу в любое время доступа к реестру сертификатов Удостоверяющего центра с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;
- прекращение действия сертификатов по обращениям владельцев сертификатов;
- предоставление доступа к списку аннулированных Удостоверяющим центром сертификатов;
- осуществление по обращению лица, которому выдан квалифицированный сертификат, регистрации указанного лица в Единой системе идентификации и аутентификации.

1.13. **Пользователи Удостоверяющего центра**

Пользователями Удостоверяющего центра могут быть физические лица, присоединившиеся к настоящему Регламенту.

1.14. **Разрешение споров**

1.14.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту.

1.14.2. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

1.14.3. Сторона, получившая от другой стороны претензию, обязана в течение 10 (десяти) рабочих дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

1.14.4. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, и по которым не было достигнуто соглашение, разрешаются в судебном порядке в соответствии с законодательством Российской Федерации.

1.15. **Прекращение деятельности Удостоверяющего центра**

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

2. РЕАЛИЗУЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИИ И ОКАЗЫВАЕМЫЕ УСЛУГИ

В соответствии с Федеральным законом «Об электронной подписи» Удостоверяющий центр реализует следующие функции и оказывает услуги:

2.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям при условии идентификации Заявителя в порядке, установленном Федеральным законом «Об электронной подписи».

2.2. Осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи.

2.3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей.

2.4. Аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей.

2.5. Выдает по обращению Заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные Удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем.

2.6. Ведет реестр созданных и аннулированных Удостоверяющим центром сертификатов (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах, а также сведения о датах прекращения действия или аннулирования сертификатов и основаниях таких прекращения или аннулирования.

2.7. Создает по обращениям Заявителей ключи электронных подписей и ключи проверки электронных подписей.

2.8. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.

2.9. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.

2.10. Прекращает действие созданных и выданных Удостоверяющим центром квалифицированных сертификатов, по заявлениям владельцев сертификатов.

2.11. Выдает по обращениям владельцев квалифицированных сертификатов, выданных в форме электронных документов, копии квалифицированных сертификатов на бумажных носителях, заверенных Удостоверяющим центром.

2.12. Осуществляет по желанию владельцев квалифицированных сертификатов, выданных Удостоверяющим центром, их регистрацию в Единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

2.13. На безвозмездной основе обеспечивает физических лиц шифровальными (криптографическими) средствами, указанными в части 8 статьи 15 Федерального закона «Об электронной подписи», для проведения идентификации физических лиц в аккредитованном удостоверяющем центре на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети «Интернет».

2.14. Иные, связанные с использованием электронной подписи услуги.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. **Права Удостоверяющего центра**

Удостоверяющий центр имеет право:

3.1.1. Отказать Заявителю в принятии заявления на выдачу сертификата, с указанием причин отказа.

3.1.2. Прекратить действие выданного Удостоверяющим центром сертификата в следующих случаях:

- при наличии у Удостоверяющего центра существенных оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован;
- если установлено, что сертификат содержит сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя;
- если установлено, что в результате технической ошибки сертификат содержит недостоверные или неполные сведения;
- в случае невыполнения владельцем сертификата обязанностей, установленных Федеральным законом «Об электронной подписи», иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи», а также настоящим Регламентом.

3.1.3. Наделить Доверенных лиц полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронных подписей, идентификации Заявителей при их личном присутствии и вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра.

3.1.4. Осуществлять отправку сервисной информации в составе SMS-сообщений, направляемых на указанный Пользователем при регистрации абонентский номер мобильного телефона в целях получения Пользователем услуг Удостоверяющего центра.

3.2. **Обязанности Удостоверяющего центра**

3.2.1. Удостоверяющий центр обязан информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

3.2.2. Удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.2.3. Удостоверяющий центр обязан предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов

информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

3.2.4. Удостоверяющий центр обязан обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

3.2.5. Удостоверяющий центр обязан отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата ключа проверки электронной подписи.

3.2.6. Удостоверяющий центр обязан отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата ключа проверки электронной подписи.

3.2.7. Удостоверяющий центр обязан хранить информацию, внесенную в реестр сертификатов Удостоверяющего центра, в течение всего срока деятельности удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами.

3.2.8. Удостоверяющий центр обязан внести в реестр сертификатов информацию о сертификате ключа проверки электронной подписи не позднее указанной в нем даты начала действия такого сертификата.

3.2.9. Удостоверяющий центр обязан прекратить действие квалифицированного сертификата в следующих случаях:

- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или настоящим Регламентом.

3.2.10. Удостоверяющий центр обязан аннулировать квалифицированный сертификат в следующих случаях:

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

3.2.11. Удостоверяющий центр обязан внести информацию о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в пунктах 3.2.9 и 3.2.10 настоящего Регламента, или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

3.2.12. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи Удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

3.2.13. Удостоверяющий центр обязан хранить следующую информацию:

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

3.2.14. Удостоверяющий центр должен хранить информацию, указанную в пункте 3.2.13 настоящего Регламента, в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.2.15. Удостоверяющий центр для подписания от своего имени создаваемых квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему Головным удостоверяющим центром. Удостоверяющий центр не вправе использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему Головным удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными сертификатами.

3.2.16. Удостоверяющий центр обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к реестру квалифицированных сертификатов Удостоверяющего центра в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

3.2.17. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан:

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

3.2.18. Удостоверяющий центр обязан выполнять порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, установленный настоящим Регламентом в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с Федеральным законом «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи».

3.2.19. Удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени Удостоверяющего центра.

3.2.20. Удостоверяющий центр обязан не использовать ключ электронной подписи и немедленно обратиться в Головной удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

3.2.21. При выдаче квалифицированного сертификата Удостоверяющий центр обязан:

- в порядке, установленном Федеральным законом «Об электронной подписи», идентифицировать Заявителя – физическое лицо, обратившееся к нему за получением квалифицированного сертификата;
- предложить использовать шифровальные (криптографические) средства, указанные в части 8 статьи 15 Федерального закона «Об электронной подписи», физическим лицам, обратившимся в Удостоверяющий центр в целях проведения идентификации без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и информации из Единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в Удостоверяющем центре без его личного присутствия посредством сети «Интернет»), и указать страницу сайта в информационно-телекоммуникационной сети «Интернет», с которой безвозмездно предоставляются эти средства;
- отказать в проведении идентификации и выдаче квалифицированного сертификата физическому лицу, обратившемуся в Удостоверяющий центр в целях проведения идентификации без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и информации из Единой биометрической системы, в случае если такое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в Удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств;
- осуществить подтверждение достоверности сведений, устанавливаемых при идентификации Заявителя – физического лица, обратившегося к нему за получением квалифицированного сертификата, одним из следующих способов:
    1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;
    2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;
    3) с использованием Единой системы идентификации и аутентификации;
- с использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных Заявителем при обращении в Удостоверяющий центр за получением квалифицированного сертификата в соответствии с частями 2 и 2.1 статьи 18 Федерального закона «Об электронной подписи»;
- отказать Заявителю в выдаче квалифицированного сертификата в случаях если полученные с использованием инфраструктуры сведения не подтверждают достоверность информации, представленной Заявителем для включения в квалифицированный сертификат, или Заявитель не идентифицирован, а также в случаях, установленных пунктами 3.2.5 и 3.2.6 настоящего Регламента;

- ознакомить получателя квалифицированного сертификата с информацией, содержащейся в квалифицированном сертификате под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи Заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и информации из Единой биометрической системы.

3.2.22. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

3.2.23. Удостоверяющий центр одновременно с выдачей квалифицированного сертификата должен предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

3.2.24. В соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи», Удостоверяющий центр обязан направлять в Единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

3.2.25. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию владельца квалифицированного сертификата обязан безвозмездно осуществить его регистрацию в Единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.

4. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. **Права Пользователя Удостоверяющего центра**

Пользователь Удостоверяющего центра имеет право:

4.1.1. Получить и применять квалифицированный сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в квалифицированных сертификатах, созданных Удостоверяющим центром.

4.1.2. Обращаться в Удостоверяющий центр с целью получения квалифицированного сертификата.

4.1.3. Обращаться в Удостоверяющий центр с целью получения ключа электронной подписи.

4.1.4. Обращаться в Удостоверяющий центр с целью получения средств электронной подписи.

4.1.5. Получать доступ к списку аннулированных сертификатов и использовать его для установления статуса сертификатов, созданных Удостоверяющим центром.

4.1.6. Получить копию выданного ему квалифицированного сертификата на бумажном носителе, заверенную Удостоверяющим центром.

4.1.7. Обращаться в Удостоверяющий центр за подтверждением действительности электронных подписей, основанных на выданных Удостоверяющим центром

квалифицированных сертификатах, в соответствии с порядком, определенным настоящим Регламентом.

4.1.8. Обращаться в Удостоверяющий центр с заявлением на прекращение действия выданного ему квалифицированного сертификата, в течение срока действия сертификата.

4.2. **Обязанности Пользователя Удостоверяющего центра**

4.2.1. Обязанности лица, проходящего процедуру регистрации в Удостоверяющем центре:

4.2.1.1. Лицо, проходящее процедуру регистрации в Удостоверяющем центре, обязано предоставить регистрационные данные в объеме, необходимом для получения услуг Удостоверяющего центра.

4.2.1.2. Лицо, проходящее процедуру регистрации в Удостоверяющем центре, несет ответственность за достоверность предоставленных регистрационных данных.

4.2.2. Обязанности лица, пользующегося услугами Удостоверяющего центра (владельца квалифицированного сертификата):

4.2.2.1. Принимать все возможные меры для предотвращения компрометации ключа электронной подписи, принадлежащего владельцу сертификата, а также меры по обеспечению конфиденциальности аутентификационных данных, используемых для доступа к Информационной системе Удостоверяющего центра или к Мобильному приложению.

4.2.2.2. Не использовать принадлежащий владельцу сертификата ключ электронной подписи в случае его компрометации.

4.2.2.3. Немедленно обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата в случае компрометации ключа электронной подписи, принадлежащего владельцу сертификата.

4.2.2.4. Извещать Удостоверяющий центр обо всех изменениях своих регистрационных данных в течение 3 (трех) рабочих дней с даты регистрации изменений.

4.2.2.5. Обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата, содержащего сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя, не позднее 3 (трех) рабочих дней с даты регистрации таких изменений.

4.2.2.6. Использовать для создания ключей электронных подписей и запросов на квалифицированный сертификат только средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи".

4.2.2.7. Обеспечивать незамедлительное уничтожение ключа электронной подписи, принадлежащего владельцу квалифицированного сертификата, по истечении срока действия данного ключа. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

4.2.2.8. При создании ключей электронных подписей и запросов на квалифицированный сертификат выполнять требования о соблюдении конфиденциальности информации, установленные Федеральным законом от 27.07.2016 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

4.2.2.9. Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, который аннулирован, действие которого прекращено или заявление на прекращение действия которого подано в Удостоверяющий центр.

5. ОТВЕТСТВЕННОСТЬ

5.1. **Ответственность Удостоверяющего центра**

5.1.1. Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг Удостоверяющим центром;
- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом "Об электронной подписи".

5.1.2. Удостоверяющий центр (работник аккредитованного удостоверяющего центра, доверенные лица и их работники) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом "Об электронной подписи" и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом.

5.2. **Ответственность Пользователя**

5.2.1. Пользователь несет ответственность за достаточность принимаемых им мер по обеспечению безопасности использования электронной подписи и средств электронной подписи, включая защиту хранящегося у него ключа электронной подписи от компрометации, потери, уничтожения или изменения.

5.2.2. Пользователь несет ответственность за последствия, возникшие в результате неисполнения им положений настоящего Регламента.

6. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

6.1. **Виды конфиденциальной информации**

6.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего квалифицированного сертификата. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Пользователей Удостоверяющего центра.

6.1.2. Конфиденциальной является также следующая информация:

- аутентификационная информация, предоставляемая Пользователю в процессе прохождения процедуры регистрации и получения сертификата ключа поверки электронной подписи;
- персональные данные и корпоративная информация Пользователей, не подлежащая включению в состав квалифицированного сертификата.

6.2. **Виды информации, не относящейся к конфиденциальной**

6.2.1. Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

6.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации определяется решением Удостоверяющего центра.

6.2.3. Информация, включаемая в создаваемые Удостоверяющим центром квалифицированные сертификаты и реестр сертификатов, не считается конфиденциальной.

6.2.4. Также не считается конфиденциальной информация о настоящем Регламенте.

6.3. **Предоставление конфиденциальной информации**

Удостоверяющий центр не должен раскрывать информацию, относящуюся к конфиденциальной, каким бы то ни было третьим лицам за исключением случаев:

- определенных настоящим Регламентом;
- требующих раскрытия в соответствии с законодательством Российской Федерации или при наличии судебного постановления.

7. ПОРЯДОК И СРОКИ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

7.1. **Регистрация Пользователей Удостоверяющего центра**

7.1.1. Под регистрацией Пользователей Удостоверяющего центра понимается внесение регистрационных данных Пользователей в информационную систему Удостоверяющего центра.

7.1.2. Регистрация Пользователя Удостоверяющего центра осуществляется на основании заявки на регистрацию в Удостоверяющем центре, содержащей регистрационные данные Заявителя, включая информацию, подлежащую внесению в квалифицированный сертификат в соответствии с частью 2 статьи 17 Федерального закона "Об электронной подписи".

7.1.3. Заявка может быть подана Заявителем одним из следующих способов:

- путем подачи заявки в форме электронного документа через личный кабинет Пользователя в информационной системе Удостоверяющего центра;
- путем подачи заявки в форме электронного документа через Мобильное приложение;
- путем передачи в информационную систему Удостоверяющего центра заявки на регистрацию, сформированной по обращению Заявителя Уполномоченным сотрудником Пункта регистрации Доверенного лица Удостоверяющего центра на основании предоставленных Заявителем регистрационных данных.

7.2. **Порядок создания ключей электронных подписей и ключей проверки электронных подписей**

7.2.1. **Порядок создания ключей электронных подписей и ключей проверки электронных подписей Пользователей.**

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона "Об электронной подписи" создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется одним из двух способов:

7.2.1.1. **Создание ключа электронной подписи и ключа проверки электронной подписи самостоятельно Пользователем.**

7.2.1.1.1. Создание ключа электронной подписи и ключа проверки электронной подписи должно осуществляться Пользователем в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и

эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный № 6382) с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный № 17350).

7.2.1.1.2. Созданный Пользователем ключ проверки электронной подписи передается в Удостоверяющий центр в составе файла запроса на сертификат.

7.2.1.2. **Создание ключа электронной подписи и ключа проверки электронной подписи Удостоверяющим центром по обращению Пользователя.**

7.2.1.2.1. Создание ключа электронной подписи и ключа проверки электронной подписи для Пользователя осуществляется Удостоверяющим центром в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

7.2.1.2.2. Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Удостоверяющим центром на автоматизированном рабочем месте, в отношении которого выполнены требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049).

7.2.1.2.3. Создание ключа электронной подписи и ключа проверки электронной подписи Пользователя Доверенным лицом Удостоверяющего центра категорически запрещено.

7.2.2. **Порядок плановой смены ключа электронной подписи Удостоверяющего центра.**

7.2.2.1. Плановая смена ключа электронной подписи Удостоверяющего центра выполняется не позднее 15 месяцев с момента начала действия текущего ключа электронной подписи Удостоверяющего центра.

7.2.2.2. Выполнение плановой смены ключа электронной подписи Удостоверяющего центра не влечет за собой необходимости смены ключей электронных подписей и соответствующих квалифицированных сертификатов ключей проверки электронных подписей Пользователей.

7.2.2.3. Выполнение плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

- Удостоверяющий центр создает новые ключ электронной подписи и ключ проверки электронной подписи.
- Удостоверяющий центр направляет в Головной удостоверяющий центр запрос на новый квалифицированный сертификат ключа проверки электронной подписи Удостоверяющего центра.
- После получения из Головного удостоверяющего центра нового квалифицированного сертификата ключа проверки электронной подписи Удостоверяющий центр осуществляет информирование об этом Пользователей путем публикации нового квалифицированного сертификата Удостоверяющего центра на сайте Удостоверяющего центра.

7.2.2.4. Получение нового квалифицированного сертификата Удостоверяющего центра осуществляется Пользователями путем его загрузки с сайта Удостоверяющего центра. Указанный способ получения квалифицированного сертификата Удостоверяющего центра

является доверенным, поскольку квалифицированный сертификат Удостоверяющего центра подписан квалифицированной электронной подписью Головного удостоверяющего центра, выдавшего этот сертификат.

7.2.2.5. Ключ электронной подписи и соответствующий квалифицированный сертификат ключа проверки Удостоверяющего центра, действовавшие до ввода в действие нового ключа электронной подписи Удостоверяющего центра, используются Удостоверяющим центром в течение срока их действия для подписания списка аннулированных сертификатов, содержащего сведения о квалифицированных сертификатах, выданных Удостоверяющим центром до ввода в действие нового ключа электронной подписи Удостоверяющего центра.

7.2.3. **Порядок смены ключа электронной подписи Удостоверяющего центра в случаях нарушения его конфиденциальности.**

7.2.3.1. Внеплановая смена ключа электронной подписи Удостоверяющего центра производится при нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра в случаях наступления событий, связанных со следующими видами угроз нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра:

- физическая утрата ключевого носителя, содержащего ключ электронной подписи;
- нарушение правил хранения и использования ключа электронной подписи Удостоверяющего центра, установленных эксплуатационной документацией на средства удостоверяющего центра;
- несанкционированное копирование ключа электронной подписи Удостоверяющего центра;
- несанкционированный доступ постороннего лица в место размещения технических средств Удостоверяющего центра или подозрение на то, что такое событие имело место быть (нарушение слепков печатей, повреждение замков и т. п.);
- нарушение работоспособности или нештатное функционирование технических средств защиты информации, обрабатываемой на средствах удостоверяющего центра.

7.2.3.2. В случае компрометации ключа электронной подписи Удостоверяющий центр немедленно прекращает создание новых сертификатов ключей проверки электронных подписей Пользователей с использованием скомпрометированного ключа электронной подписи и не позднее двух часов с момента, когда Удостоверяющему центру стало известно о наступлении обстоятельств, вызвавших компрометацию или угрозу компрометации ключа электронной подписи, направляет в Головной удостоверяющий центр заявление на прекращение действия сертификата ключа проверки электронной подписи, соответствующего скомпрометированному ключу электронной подписи.

7.2.3.3. В случае выполнения внеплановой смены ключа электронной подписи Удостоверяющего центра прекращается действие всех сертификатов, подписанных электронной подписью Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи, с включением сведений о прекращении действия этих сертификатов в реестр сертификатов.

7.2.3.4. В случае выполнения внеплановой смены ключа электронной подписи Удостоверяющего центра должны быть проведены работы по внеплановой смене ключей электронных подписей Пользователей, сертификаты ключей проверки электронных подписей которых подписаны электронной подписью Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра. Создание и выдача новых сертификатов ключей проверки электронных подписей осуществляется Удостоверяющим центром безвозмездно в соответствии с порядком, указанным в разделе 7.3 настоящего Регламента.

7.2.3.5. Удостоверяющий центр информирует Пользователей, сертификаты ключей проверки электронных подписей которых подписаны электронной подписью Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра, о внеплановой смене ключа электронной подписи Удостоверяющего центра и, соответственно, о прекращении действия выданных им сертификатов путем размещения соответствующей информации на сайте Удостоверяющего центра.

7.2.3.6. Получение нового квалифицированного сертификата Удостоверяющего центра осуществляется Пользователями путем его загрузки с сайта Удостоверяющего центра. Указанный способ получения квалифицированного сертификата Удостоверяющего центра является доверенным, поскольку квалифицированный сертификат Удостоверяющего центра подписан квалифицированной электронной подписью Головного удостоверяющего центра, выдавшего этот сертификат.

7.2.4. **Порядок смены ключа электронной подписи Пользователя.**

7.2.4.1. **Плановая смена ключа электронной подписи Пользователя.**

7.2.4.1.1. Плановая смена ключа электронной подписи производится в связи с истечением срока действия ключа электронной подписи, соответствующего ключу проверки электронной подписи, указанному в выданном Удостоверяющим центром квалифицированном сертификате.

7.2.4.1.2. Плановая смена ключа электронной подписи производится не ранее чем за 30 (тридцать) календарных дней до даты окончания срока действия ключа электронной подписи и не позднее даты окончания срока действия ключа электронной подписи.

7.2.4.1.3. Создание нового ключа электронной подписи и соответствующего ему ключа проверки электронной подписи осуществляется Пользователем самостоятельно, в порядке, определенном пунктом 7.2.1.1.1 настоящего Регламента.

7.2.4.1.4. Созданный Пользователем ключ проверки электронной подписи передается в Удостоверяющий центр в составе файла запроса на сертификат вместе с заявлением на выдачу нового квалифицированного сертификата, сформированным в соответствии с требованиями пункта 7.3.2 настоящего Регламента. Запрос на сертификат и заявление на выдачу нового квалифицированного сертификата подаются Пользователем с использованием информационно-телекоммуникационных сетей в форме электронных документов, подписанных квалифицированной электронной подписью, ключ проверки которой содержится в выданном ранее Удостоверяющим центром квалифицированном сертификате ключа проверки электронной подписи, являющимся действительным на момент создания электронной подписи.

7.2.4.1.5. Выдача Пользователю квалифицированного сертификата осуществляется в порядке, определенном пунктом 7.3 настоящего Регламента, после идентификации Заявителя – физического лица без его личного присутствия с использованием квалифицированной электронной подписи, которой были подписаны электронные документы, указанные в пункте 7.2.4.1.4 настоящего Регламента.

7.2.4.1.6. В случае если Пользователь не произвел плановую смену ключа электронной подписи в указанные в пункте 7.2.4.1.2 сроки, создание новых ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата ключа проверки электронной подписи производится в порядке, определенном разделами 7.2.1 и 7.3 настоящего Регламента.

7.2.4.2. **Внеплановая смена ключей электронной подписи Пользователя.**

7.2.4.2.1. Внеплановая смена ключей электронной подписи производится:

- по инициативе владельца сертификата в случае прекращения действия квалифицированного сертификата до истечения срока его действия в связи с компрометацией соответствующего ключа электронной подписи;
- при компрометации ключа электронной подписи Удостоверяющего центра;
- в иных случаях, связанных с невозможностью использования имеющегося ключа электронной подписи.

7.2.4.2.2. Создание нового ключа электронной подписи, соответствующего ему ключа проверки электронной подписи и выдача квалифицированного сертификата ключа проверки электронной подписи при внеплановой смене ключа электронной подписи Пользователя производится в порядке, определенном разделами 7.2.1 и 7.3 настоящего Регламента. При этом, в случае если смена ключа электронной подписи владельца квалифицированного сертификата связана с его компрометацией или угрозой компрометации, соответствующее заявление на выдачу нового квалифицированного сертификата в форме электронного документа должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата.

7.3. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи Пользователя

7.3.1. Порядок подачи заявления на выдачу квалифицированного сертификата.

7.3.1.1. Создание и выдача квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявления на выдачу квалифицированного сертификата.

7.3.1.2. Заявление на выдачу квалифицированного сертификата может быть подано Пользователем как в форме документа на бумажном носителе, так и в форме электронного документа, подписанного квалифицированной электронной подписью Заявителя, либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (далее - Единая система идентификации и аутентификации) и информации из государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее - Единая биометрическая система).

7.3.1.3. Заявление на выдачу квалифицированного сертификата подается Пользователем в Пункт регистрации лично или с использованием информационно-телекоммуникационных сетей через личный кабинет Пользователя в информационной системе Удостоверяющего центра либо через Мобильное приложение.

7.3.2. **Требования к заявлению на выдачу квалифицированного сертификата.**

7.3.2.1. Требования к заявлению на выдачу квалифицированного сертификата, подаваемого в форме документа на бумажном носителе.

7.3.2.1.1. В случае если Заявитель создает ключ электронной подписи и ключ проверки электронной подписи самостоятельно, заявление на выдачу квалифицированного сертификата должно содержать значение ключа проверки электронной подписи. Форма заявления на выдачу квалифицированного сертификата в этом случае приведена в Приложении 1 к настоящему Регламенту.

7.3.2.1.2. В случае если Заявитель поручает создание ключа электронной подписи и ключа проверки электронной подписи Удостоверяющему центру, Заявителем подается заявление на выдачу ключа электронной подписи и квалифицированного сертификата ключа проверки электронной подписи. Форма заявления на выдачу ключа электронной подписи и квалифицированного сертификата приведена в Приложении 2 к настоящему Регламенту.

7.3.2.2. Требования к заявлению на выдачу квалифицированного сертификата, подаваемого в форме электронного документа.

7.3.2.2.1. Заявление на выдачу квалифицированного сертификата, подаваемое в форме электронного документа, должно соответствовать виду структуры, определенной в настоящем Регламенте для запроса на сертификат.

7.3.2.2.2. Заявление на выдачу квалифицированного сертификата, подаваемое в форме электронного документа, должно быть подписано квалифицированной электронной подписью Заявителя.

7.3.2.2.3. Для подписания заявления на выдачу квалифицированного сертификата, подаваемого в форме электронного документа, квалифицированной электронной подписью должен применяться принадлежащий Заявителю ключ электронной подписи, для которого соответствующий квалифицированный сертификат ключа проверки электронной подписи действует на момент подписания заявления.

7.3.2.2.4. Для подписания заявления на выдачу квалифицированного сертификата, подаваемого в форме электронного документа, должны использоваться средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

7.3.3. **Порядок идентификации Заявителя.**

7.3.3.1. Идентификация Заявителя, обратившегося за получением квалифицированного сертификата, осуществляется Удостоверяющим центром одним из следующих способов:

- идентификация Заявителя при его личном присутствии;
- идентификации Заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;
- идентификации Заявителя – гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные;
- идентификации Заявителя – гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и Единой биометрической системы, в порядке, установленном Федеральным законом от

27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7.3.3.2. Идентификация Заявителя – гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из Единой системы идентификации и аутентификации и Единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», осуществляется Удостоверяющим центром при наличии технической возможности проведения такой идентификации.

7.3.3.3. Идентификация Заявителя Доверенным лицом Удостоверяющего центра осуществляется только при личном присутствии Заявителя.

7.3.3.4. Идентификация Заявителя при его личном присутствии осуществляется по основному документу, удостоверяющему личность. При этом:

- идентификация гражданина Российской Федерации осуществляется по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации;
- идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства, с учетом требований пункта 7.3.4.2 настоящего Регламента;
- идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

7.3.3.5. В случае идентификации Заявителя при его личном присутствии, в целях выполнения требований пункта 1 части 1 и части 2 статьи 15 Федерального закона «Об электронной подписи», Удостоверяющий центр получает копии страниц основного документа, удостоверяющего личность владельца квалифицированного сертификата – физического лица, содержащих реквизиты этого документа.

7.3.4. Перечень документов и (или) сведений из них, запрашиваемых Удостоверяющим центром у Заявителя для создания и выдачи квалифицированного сертификата.

7.3.4.1. При обращении в Удостоверяющий центр Заявитель представляет документы либо их надлежащим образом заверенные копии и (или) сведения из них:

- основной документ, удостоверяющий личность Заявителя;
- страховой номер индивидуального лицевого счета Заявителя;
- идентификационный номер налогоплательщика Заявителя.

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

7.3.4.3. Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пункте 7.3.4.1 настоящего Регламента.

7.3.5. **Порядок проверки достоверности документов и сведений, представленных Заявителем.**

Удостоверяющий центр с использованием Инфраструктуры осуществляет проверку достоверности документов и сведений, представленных Заявителем в целях получения квалифицированного сертификата, используя при этом, в частности, документы и сведения, полученные Удостоверяющим центром из государственных информационных ресурсов:

- сведения об идентификационном номере налогоплательщика в отношении Заявителя;
- сведения о достоверности страхового номера индивидуального лицевого счета в отношении Заявителя;
- сведения о действительности паспорта гражданина РФ по его номеру.

7.3.6. **Порядок создания квалифицированного сертификата.**

В случае, если проверка, произведенная в соответствии с пунктом 7.3.5, настоящего Регламента, подтверждает достоверность информации, представленной Заявителем при обращении в Удостоверяющий центр за получением квалифицированного сертификата, и Удостоверяющим центром идентифицирован Заявитель, Удостоверяющий центр осуществляет процедуру создания и выдачи Заявителю квалифицированного сертификата. В противном случае, а также в случаях, установленных пунктами 3.2.5 и 3.2.6 настоящего Регламента, Удостоверяющий центр отказывает Заявителю в выдаче квалифицированного сертификата.

7.3.7. **Порядок выдачи квалифицированного сертификата.**

7.3.7.1. При получении квалифицированного сертификата Заявителем Удостоверяющий центр ознакомляет его с информацией, содержащейся в квалифицированном сертификате (форма бланка с информацией, содержащейся в выдаваемом сертификате ключа проверки электронной подписи приведена в Приложении 3 к настоящему Регламенту). Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и информации из Единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица.

7.3.7.2. Одновременно с квалифицированным сертификатом Пользователю выдаются:

- созданный Удостоверяющим центром ключ электронной подписи Пользователя, в случае наличия соответствующего обращения со стороны Пользователя;
- средство электронной подписи, имеющее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», в случае наличия соответствующего обращения со стороны Пользователя.

7.3.7.3. Одновременно с выдачей квалифицированного сертификата Пользователю предоставляется руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной

подписи в письменной форме, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

7.3.8. **Срок создания и выдачи квалифицированного сертификата.**

7.3.8.1. Создание и выдача квалифицированного сертификата осуществляется Удостоверяющим центром в течение не более двух рабочих дней со дня получения заявления на выдачу квалифицированного сертификата.

7.3.8.2. Для создания и выдачи квалифицированного сертификата в течение дня, в который в Удостоверяющий центр подано заявление на выдачу квалифицированного сертификата, Заявитель должен произвести дополнительную оплату срочного оказания услуги и представить в Удостоверяющий центр платежное поручение с отметкой банка о том, что платеж произведен.

7.3.9. **Сроки действия сертификата ключа проверки электронной подписи и ключа электронной подписи Пользователя**

7.3.9.1. Удостоверяющий центр создает и выдает квалифицированные сертификаты ключа проверки электронной подписи со сроком действия, равным сроку действия соответствующего ключа электронной подписи.

7.3.9.2. Срок действия ключа электронной подписи, соответствующего ключу проверки электронной подписи, содержащемуся в выданном Удостоверяющим центром квалифицированном сертификате, устанавливается равным одному году.

7.3.9.3. При использовании для создания и хранения ключа электронной подписи аппаратного криптографического токена срок действия ключа электронной подписи может быть установлен равным трем годам.

7.4. **Подтверждение действительности электронной подписи**

7.4.1. Подтверждение действительности электронной подписи в электронном документе осуществляется Удостоверяющим центром по обращению Пользователя на основании заявления в простой письменной форме на подтверждение действительности электронной подписи в электронном документе.

7.4.2. Заявление на подтверждение действительности электронной подписи в электронном документе должно содержать информацию о дате и времени формирования электронной подписи в электронном документе.

7.4.3. Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является внешний носитель информации, содержащий электронный документ с электронной подписью в формате, соответствующем требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

7.4.4. Срок проведения работ по подтверждению действительности электронной подписи в электронном документе составляет 5 (пять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

7.4.5. В ходе проведения работ по подтверждению действительности электронной подписи в электронном документе Удостоверяющим центром может быть запрошена дополнительная информация.

7.4.6. Квалифицированная электронная подпись признается действительной при одновременном соблюдении следующих условий:

- квалифицированный сертификат создан и выдан аккредитованным удостоверяющим центром, аккредитация которого действительна на день выдачи указанного сертификата.
- квалифицированный сертификат и все квалифицированные сертификаты, включенные в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему Головным удостоверяющим центром, действительны на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности проверяемого квалифицированного сертификата, если момент подписания электронного документа не определен.
- срок действия ключа электронной подписи, указанный в квалифицированном сертификате, не истек на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки квалифицированной электронной подписи, созданной с использованием данного ключа электронной подписи, если момент подписания электронного документа не определен;
- имеется положительный результат проверки принадлежности владельцу квалифицированного сертификата квалифицированной электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания (при этом проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», и с использованием квалифицированного сертификата лица, подписавшего электронный документ).

7.4.7. Результатом проведения работ по подтверждению действительности электронной подписи в электронном документе является ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника и печатью Удостоверяющего центра. Ответ должен содержать:

- результат проверки средством электронной подписи, имеющим подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», принадлежности электронной подписи в электронном документе владельцу квалифицированного сертификата и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- детальный отчет по выполненной проверке (экспертизе).

7.4.8. Детальный отчет по выполненной проверке должен включать следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или экспертной комиссии (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или экспертной комиссией;
- объекты исследований и материалы по заявлению, представленные для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения.

7.4.9. Материалы и документы, иллюстрирующие заключение эксперта или экспертной комиссии, прилагаются к детальному отчету и являются его составной частью.

7.4.10. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами экспертной комиссии.

7.5. Процедуры, выполняемые при прекращении действия или аннулировании квалифицированного сертификата

7.5.1. Основания прекращения действия или аннулирования квалифицированного сертификата

7.5.1.1. Квалифицированный сертификат прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, или настоящим Регламентом.

7.5.1.2. Удостоверяющий центр аннулирует квалифицированный сертификат в следующих случаях:

- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в таком квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- в связи с вступлением в силу решения суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию.

7.5.2. Порядок действий Удостоверяющего центра при прекращении действия или аннулировании квалифицированного сертификата

7.5.2.1. Порядок подачи и приема заявления на прекращение действия квалифицированного сертификата:

7.5.2.1.1. Заявление на прекращение действия квалифицированного сертификата может быть подано как в форме документа на бумажном носителе, так и в форме электронного документа, в том числе с использованием подсистемы «личный кабинет» Единого портала госуслуг.

7.5.2.1.2. При подаче заявления на прекращение действия квалифицированного сертификата без использования подсистемы «личный кабинет» федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» заявление на прекращение действия квалифицированного сертификата подается в Удостоверяющий центр по форме Приложения 4 к настоящему Регламенту.

7.5.2.1.3. Заявление на прекращение действия квалифицированного сертификата, подаваемое в форме документа на бумажном носителе, должно быть подписано собственноручной подписью лица, указанного в качестве владельца сертификата.

7.5.2.1.4. Заявление на прекращение действия квалифицированного сертификата, подаваемое в форме электронного документа, должно быть подписано квалифицированной

электронной подписью владельца квалифицированного сертификата, при этом, в случае если прекращение действия квалифицированного сертификата связано с компрометацией ключа электронной подписи, соответствующее заявление должно быть подписано квалифицированной электронной подписью владельца квалифицированного сертификата, основанной на ином квалифицированном сертификате ключа проверки электронной подписи.

7.5.2.1.5. В случае подачи заявления на прекращение действия квалифицированного сертификата с использованием Единого портала госуслуг принятое по такому заявлению решение Удостоверяющего центра в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Удостоверяющего центра, размещается в личном кабинете заявителя на Едином портале госуслуг после проведения проверки действительности усиленной квалифицированной электронной подписи Удостоверяющего центра, которой такое решение подписано, и подтверждения ее действительности. В случае принятия по такому заявлению решения о прекращении действия квалифицированного сертификата Удостоверяющий центр после внесения соответствующей информации в реестр квалифицированных сертификатов направляет на Единый портал госуслуг информацию о прекращении действия квалифицированного сертификата. Взаимодействие Удостоверяющего центра с Единым порталом госуслуг в рамках реализации норм, предусмотренных настоящим абзацем, осуществляется посредством единой системы межведомственного электронного взаимодействия.

7.5.2.2. Порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов:

7.5.2.2.1. Внесение информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов осуществляется путем внесения соответствующей информации в список аннулированных сертификатов.

7.5.2.2.2. Удостоверяющий центр вносит информацию о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов в срок, не превышающий двенадцать часов с момента наступления обстоятельств, указанных в разделе 7.5.1 настоящего Регламента или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.

7.5.2.2.3. До внесения в реестр сертификатов информации об аннулировании квалифицированного сертификата Удостоверяющий центр уведомляет владельца квалифицированного сертификата об аннулировании его сертификата путем направления уведомления в форме бумажного или электронного документа.

7.5.2.2.4. Удостоверяющий центр обязан официально уведомить о факте аннулирования или прекращения действия сертификата всех участников информационного взаимодействия.

7.5.2.2.5. Официальным уведомлением о факте аннулирования или прекращения действия сертификата является опубликование списка аннулированных сертификатов, содержащего сведения о сертификате, который был аннулирован или действие которого было досрочно прекращено.

7.5.2.2.6. Временем опубликования списка аннулированных сертификатов признается включенное в список аннулированных сертификатов время его создания.

7.5.2.2.7. Датой и временем аннулирования или прекращения действия квалифицированного сертификата признается дата и время внесения информации о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных сертификатов.

7.5.2.2.8. Удостоверяющий центр обязан осуществлять публикацию списка аннулированных сертификатов в точках распространения, указанных в полях CRLDistributionPoints и

AuthorityInfoAccess выдаваемых Удостоверяющим центром квалифицированных сертификатов.

7.6. Порядок ведения реестра квалифицированных сертификатов

7.6.1. Реестр квалифицированных сертификатов ведется Удостоверяющим центром в электронной форме в соответствии с требованиями, установленными Федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий согласно Закону "Об электронной подписи", и кроме информации, содержащейся в квалифицированных сертификатах, включает также информацию о датах прекращения действия или аннулирования квалифицированных сертификатов и об основаниях прекращения действия или аннулирования, а также иную информацию, подлежащую включению в реестр в соответствии с установленными требованиями.

7.6.2. Информация о созданном квалифицированном сертификате ключа проверки электронной подписи вносится Удостоверяющим центром в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

7.6.3. Удостоверяющий центр вносит информацию о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в реестр квалифицированных сертификатов в течение 12 часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия квалифицированного сертификата или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

7.7. Порядок технического обслуживания реестра квалифицированных сертификатов

7.7.1. Техническое обслуживание реестра сертификатов осуществляется, как правило, в нерабочее время и не может превышать 3 (трех) часов.

7.7.2. Удостоверяющий центр осуществляет заблаговременное оповещение о планируемом проведении технического обслуживания реестра сертификатов путем публикации соответствующей информации на сайте Удостоверяющего центра.

8. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

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

8.1.1. Удостоверяющий центр осуществляет информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, путем включения этой информации в предоставляемое каждому получателю квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (пункт 7.3.7.3 настоящего Регламента).

8.1.2. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, содержащее

указанную информацию, публикуется на сайте Удостоверяющего центра, а также размещается в Мобильном приложении.

8.2. Выдача по обращению Заявителя средств электронной подписи

8.2.1. Средства электронной подписи, выдаваемые Удостоверяющим центром Заявителю, должны иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

8.2.2. Выдача по обращению Заявителя средств электронной подписи осуществляется путем поставки средств криптографической защиты способом, определенным эксплуатационной документацией на эти средства.

8.3. Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

8.3.1. Актуальность информации, содержащейся в реестре квалифицированных сертификатов, обеспечивается путем выполнения Удостоверяющим центром порядка ведения реестра квалифицированных сертификатов, изложенного в разделе 7.6 настоящего Регламента, а также защиты указанной информации от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

8.3.2. Защита информации, содержащейся в реестре квалифицированных сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается комплексом организационно-технических мероприятий, осуществляемых Удостоверяющим центром в соответствии с требованиями, установленными эксплуатационной документацией на средства удостоверяющего центра, а также требованиями, установленными в области технической защиты информации.

8.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет»

Информация, содержащаяся в реестре квалифицированных сертификатов Удостоверяющего центра, доступна любому лицу в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, по адресу reestr.iitrust.ru.

8.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

8.5.1. Конфиденциальность созданных Удостоверяющим центром ключей электронных подписей обеспечивается комплексом организационно-технических мероприятий, осуществляемых Удостоверяющим центром в соответствии с требованиями, установленными:

- эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи;
- нормативными документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в отношении безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации;
- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих

государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 (далее – Инструкция).

8.5.2. Временное хранение ключей электронных подписей, созданных Удостоверяющим центром по обращению Заявителей, осуществляется в соответствии с требованиями, установленными Инструкцией.

8.5.3. Временное хранение ключей электронных подписей, созданных Удостоверяющим центром по обращению Заявителей, осуществляется в течение не более 30 (тридцати) дней с момента их создания. В случае неполучения Заявителями созданных по их обращениям ключей электронной подписи до истечения указанного срока ключи электронной подписи уничтожаются Удостоверяющим центром.

8.5.4. Удостоверяющий центр не осуществляет депонирование и (или) архивирование ключей электронных подписей Пользователей.

8.6. Регистрация квалифицированного сертификата в Единой системе идентификации и аутентификации

В соответствии с требованиями части 5 статьи 18 Федерального закона «Об электронной подписи» при выдаче квалифицированного сертификата Удостоверяющий центр направляет в Единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.

8.7. Регистрация владельца квалифицированного сертификата в Единой системе идентификации и аутентификации

8.7.1. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в Единой системе идентификации и аутентификации с проведением идентификации владельца сертификата при его личном присутствии.

8.7.2. Регистрация физического лица в Единой системе идентификации и аутентификации осуществляется Удостоверяющим центром на основании заявления, поданного в Удостоверяющий центр в форме документа на бумажном носителе с собственноручной подписью владельца сертификата (Приложение 5 к настоящему Регламенту).

8.8. Предоставление доступа к информации, содержащейся в реестре квалифицированных сертификатов

Доступ к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия или аннулировании квалифицированного сертификата, предоставляется безвозмездно любому лицу в соответствии с порядком, указанным в пункте 8.4 настоящего Регламента.

9. МЕХАНИЗМ ДОКАЗАТЕЛЬСТВА ВЛАДЕНИЯ КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1. В случае идентификации Заявителя - физического лица при его личном присутствии:

- если ключ электронной подписи и ключ проверки электронной подписи были созданы Удостоверяющим центром по обращению Заявителя, факт владения ключом электронной подписи подтверждается фактом передачи Заявителю ключевого носителя, содержащего ключ электронной подписи;

– если ключ электронной подписи был создан Заявителем самостоятельно, в Удостоверяющий центр наряду с заявлением на выдачу квалифицированного сертификата, содержащим значение ключа проверки электронной подписи, представляется запрос на сертификат. В целях получения доказательств того, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, содержащемуся в представленном запросе на сертификат, Удостоверяющий центр осуществляет проверку соответствия представленного запроса на сертификат требованиям, установленным в соответствии с пунктом 5 части 4 статьи 8 Федерального закона «Об электронной подписи».

9.2. В случае идентификации Заявителя - физического лица без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата Удостоверяющий центр дополнительно осуществляет проверку того, что квалифицированная электронная подпись создана с применением принадлежащего Заявителю ключа электронной подписи, для которого соответствующий сертификат ключа проверки электронной подписи действует на момент подписания запроса на сертификат.

9.3. В случае идентификации Заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, Удостоверяющий центр дополнительно осуществляет проверку электронной подписи, которой подписана информация, содержащаяся в запросе на сертификат.

9.4. В случае идентификации Заявителя - физического лица с применением информационных технологий без его личного присутствия путем предоставления сведений из Единой системы идентификации и аутентификации и Единой информационной системы персональных данных, Удостоверяющий центр дополнительно осуществляет проверку использования физическим лицом для предоставления своих биометрических персональных данных шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

9.5. Владение ключом электронной подписи не подтверждается в случае отрицательного результата любой из проверок, определенных пунктами 9.1 - 9.4 настоящего Регламента и (или) в случае если Заявитель не идентифицирован.

9.6. В случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата ключа проверки электронной подписи, Удостоверяющий центр отказывает Заявителю в создании и выдаче сертификата.

10. СОДЕРЖАНИЕ И ФОРМА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

Удостоверяющий центр создает и выдает квалифицированные сертификаты, содержание которых соответствует требованиям, установленным Федеральным законом «Об электронной подписи», а форма - требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, установленным федеральным органом исполнительной власти в области обеспечения безопасности в соответствии с требованиями Федерального закона «Об электронной подписи».

11. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

Удостоверяющий центр формирует списки аннулированных сертификатов в соответствии с рекомендациями IETF RFC 5280 (2008) «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile».

12. ДОПОЛНИТЕЛЬНЫЕ УСЛУГИ И СЕРВИСЫ, ПРЕДОСТАВЛЯЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

12.1. Создание меток доверенного времени.

Создание метки доверенного времени осуществляется службой меток доверенного времени Удостоверяющего центра по запросу участников электронного взаимодействия путем подписания квалифицированной электронной подписью Удостоверяющего центра текущего достоверного значения времени в соответствии с требованиями к структуре метки доверенного времени.

Адрес службы меток доверенного времени Удостоверяющего центра:
http://cades.iitrust.ru:8777/tsp.

12.2. Предоставление информации о статусах сертификатов ключей проверки электронных подписей в режиме реального времени.

Предоставление информации о статусах сертификатов ключей проверки электронных подписей осуществляется сервисом проверки статуса сертификатов Удостоверяющего центра по OCSP-запросам в режиме реального времени.

Информация о статусах сертификатов ключей проверки электронных подписей, предоставляемая сервисом проверки статуса сертификатов, подписывается квалифицированной электронной подписью лица, которому Удостоверяющим центром делегировано право подписывать указанную информацию. Явным признаком правомочия такого лица подписывать информацию о статусах сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра является наличие в расширении Extended key usage квалифицированного сертификата, выданного этому лицу Удостоверяющим центром, объектного идентификатора 1.3.6.1.5.5.7.3.9.

Адрес сервиса проверки статусов сертификатов, выданных Удостоверяющим центром:
http://cades.iitrust.ru:8777/ocsp.

13. УЧЕТНО-ОТЧЕТНОЕ ВРЕМЯ

В соответствии с Федеральным законом от 18.06.2003 № 126-ФЗ «О связи» при оказании услуг Удостоверяющего центра применяется единое учетно-отчетное время – московское.

14. ПРИЛОЖЕНИЯ:

1. Форма заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи физического лица.
2. Форма заявления на выдачу ключа электронной подписи и квалифицированного сертификата ключа проверки электронной подписи физического лица.
3. Форма бланка с информацией, содержащейся в выдаваемом квалифицированном сертификате ключа проверки электронной подписи.
4. Форма заявления на прекращение действия квалифицированного сертификата ключа проверки электронной подписи физического лица.
5. Форма заявления на регистрацию физического лица в Единой системе идентификации и аутентификации.

Приложение 1
к Регламенту оказания Удостоверяющим центром
Акционерного общества «ИнфоТеКС Интернет Траст»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных подписей

Форма заявления на выдачу квалифицированного
сертификата ключа проверки электронной подписи
физического лица

ЗАЯВЛЕНИЕ

на выдачу квалифицированного сертификата ключа проверки электронной подписи

Настоящим _____
(фамилия, имя, отчество физического лица)

обращается в Удостоверяющий центр Акционерного общества «ИнфоТеКС Интернет Траст» за получением квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие сведения:

1. Идентификационный номер налогоплательщика (ИНН) _____
2. Страховой номер индивидуального лицевого счета (СНИЛС) _____
3. Адрес электронной почты владельца сертификата _____
4. Наименование используемого средства электронной подписи _____
5. Класс средства электронной подписи _____
6. Ключ проверки электронной подписи _____

_____

_____ _____
(подпись) (фамилия и инициалы лица, обращающегося за получением сертификата)

_____
(дата подачи заявления)

Приложение 2
к Регламенту оказания Удостоверяющим центром
Акционерного общества «ИнфоТеКС Интернет Траст»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных подписей

Заявление

на выдачу ключа электронной подписи и квалифицированного сертификата ключа проверки электронной подписи физического лица

Настоящим _____
(фамилия, имя, отчество физического лица)

обращается в Удостоверяющий центр Акционерного общества «ИнфоТеКС Интернет Траст» за получением ключа электронной подписи и квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие сведения:

1. Идентификационный номер налогоплательщика (ИНН) _____
2. Страховой номер индивидуального лицевого счета (СНИЛС) _____
3. Адрес электронной почты владельца сертификата _____
4. Наименование используемого средства электронной подписи _____
5. Класс средства электронной подписи _____

_____ _____
(подпись) (фамилия и инициалы лица, обращающегося за получением сертификата)

_____
(дата подачи заявления)

Приложение 3
к Регламенту оказания Удостоверяющим центром
Акционерного общества «ИнфоТеКС Интернет Траст»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных подписей

ИНФОРМАЦИЯ,
содержащаяся в квалифицированном сертификате ключа проверки электронной подписи

<table>
<tr><td colspan="2">Номер квалифицированного сертификата:</td><td colspan="4">[серийный номер сертификата]</td></tr>
<tr><td>Срок действия:</td><td>с:</td><td>[дата и время начала действия сертификата]</td><td>по:</td><td colspan="2">[дата и время окончания действия сертификата]</td></tr>
<tr><td colspan="6">Сведения о владельце квалифицированного сертификата</td></tr>
<tr><td colspan="6">Фамилия, имя, отчество: [ФИО]
ИНН: [ИНН]
СНИЛС: [СНИЛС]
E-mail: [Адрес электронной почты]
Тип идентификации при выдаче сертификата: [Тип идентификации владельца сертификата]</td></tr>
<tr><td colspan="2">Ключ проверки ЭП:</td><td colspan="4">[Значение ключа проверки электронной подписи]</td></tr>
<tr><td colspan="2">Алгоритм ключа проверки ЭП:</td><td colspan="4">[Идентификатор криптографического алгоритма]</td></tr>
<tr><td colspan="2">Расширенное использование ключа проверки ЭП:</td><td colspan="4">[Extended Key Usage]</td></tr>
<tr><td colspan="2">Средство ЭП владельца сертификата:</td><td colspan="4">[Наименование средства электронной подписи владельца сертификата]</td></tr>
<tr><td colspan="2">Класс средства ЭП владельца сертификата:</td><td colspan="4">[КС1, КС2 или КС3]</td></tr>
<tr><td colspan="2">Срок действия ключа ЭП:</td><td>с:</td><td>[дата и время начала действия ключа ЭП]</td><td>по:</td><td>[дата и время окончания действия ключа ЭП]</td></tr>
<tr><td colspan="6">Сведения об издателе квалифицированного сертификата</td></tr>
<tr><td colspan="6">Наименование удостоверяющего центра: [commonName]
Место нахождения удостоверяющего центра: [Код страны], [Наименование субъекта РФ места нахождения УЦ], [Наименование населенного пункта, наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется) места нахождения УЦ]
ИНН: 7743020560, ОГРН: 1027739113049
Номер квалифицированного сертификата УЦ: [серийный номер сертификата УЦ]
Наименование средства электронной подписи: [issuerSignTool.signTool], Реквизиты заключения о подтверждении соответствия средства электронной подписи: [issuerSignTool.signToolCert], Наименование средства удостоверяющего центра: [issuerSignTool.cATool], Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра: [issuerSignTool.cAToolCert]</td></tr>
</table>

Подписывая настоящий документ, владелец квалифицированного сертификата:
1. выражает согласие с содержанием получаемого сертификата;
2. подтверждает присоединение заявителя к Регламенту оказания Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, опубликованному на сайте iitrust.ru, и полное принятие заявителем условий Регламента и всех его положений;
3. подтверждает получение руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
4. соглашается с обработкой своих персональных данных в соответствии с Политикой в отношении обработки персональных данных в Акционерном обществе «ИнфоТеКС Интернет Траст», опубликованной на сайте iitrust.ru.

✓_____
(Фамилия, имя, отчество)

✓_____ ✓___» _____ 20___ г.
подпись

Личность владельца сертификата установил*:

_____ _____ _____
(наименование Пункта регистрации) (подпись) (Фамилия и инициалы сотрудника Пункта регистрации)

_____
(дата вручения сертификата)

.

* Запись об установлении личности и полномочий получателя сертификат оформляется только на бланке с информацией, содержащейся в квалифицированном сертификате ключа проверки электронной подписи, в форме документа на бумажном носителе.

Приложение 4
к Регламенту оказания Удостоверяющим центром
Акционерного общества «ИнфоТеКС Интернет Траст»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных подписей

Заявление
на прекращение действия квалифицированного сертификата ключа проверки
электронной подписи физического лица

Прошу прекратить действие выданного Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» квалифицированного сертификата ключа проверки электронной подписи со следующими реквизитами:

Серийный номер сертификата: _____

Фамилия, имя, отчество владельца сертификата (полностью): _____

_____

Дата начала действия сертификата: _____

Дата окончания действия сертификата: _____

СНИЛС: _____ ИНН: _____

в связи с _____
(причина прекращения действия сертификата)

_____

_____

Подпись и расшифровка подписи физического лица, указанного в качестве владельца сертификата:

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20___ г.

Приложение 5
к Регламенту оказания Удостоверяющим центром
Акционерного общества «ИнфоТеКС Интернет Траст»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных подписей

В Удостоверяющий центр
Акционерного общества
«ИнфоТеКС Интернет Траст»

Заявление
на регистрацию в Единой системе идентификации и аутентификации

В соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» прошу зарегистрировать меня в Единой системе идентификации и аутентификации на основании следующих данных:

Фамилия заявителя: _____
(в именительном падеже)

Имя: _____ Отчество: _____
(в именительном падеже) (при наличии, в именительном падеже)

Пол: _____ Дата рождения: _____
(мужской / женский) (в формате ДД.ММ.ГГГГ)

Место рождения: _____

СНИЛС: _____ Гражданство: _____
(например, Россия)

Адрес электронной почты: _____

Номер мобильного телефона: _____
(в формате +7 (xxx) xxxxxxx)

Данные документа, удостоверяющего личность: _____
(наименование документа)

номер _____ выдан _____
(серия и номер документа) (кем выдан)

_____ дата выдачи: _____ код подразделения: _____
(когда выдан)

Настоящим даю согласие на обработку Акционерным обществом «ИнфоТеКС Интернет Траст» персональных данных, содержащихся в настоящем Заявлении, включая передачу этих данных в Единую систему идентификации и аутентификации.

_____ _____
(подпись) (фамилия, инициалы)

Дата подачи заявления: _____