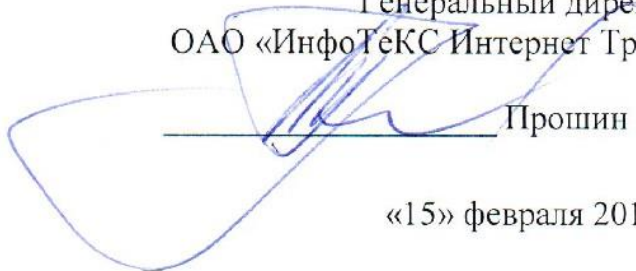


"УТВЕРЖДАЮ"
Генеральный директор
ОАО «ИнфоТеКС Интернет Траст»



Прошин А.Е.

«15» февраля 2017 г.

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

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	4
1. ВВЕДЕНИЕ	7
1.1. Обзорная информация.....	7
1.2. Идентификация Регламента.....	7
1.3. Публикация Регламента	7
1.4. Область применения Регламента	7
1.5. Заключение договора присоединения	7
1.6. Контактная информация Удостоверяющего центра ОАО «ИнфоТеКС Интернет Траст»	7
2. ОБЩИЕ ПОЛОЖЕНИЯ	8
2.1. Услуги, предоставляемые Удостоверяющим центром	8
2.2. Функции, выполняемые Удостоверяющим центром	8
2.3. Пользователи.....	10
2.4. Разрешение споров	10
2.5. Возмездность услуг	10
2.6. Прекращение деятельности Удостоверяющего центра	10
3. ПРАВА	10
3.1. Права Удостоверяющего центра	10
3.2. Права Пользователей Удостоверяющего центра.....	11
4. ОБЯЗАННОСТИ	11
4.1. Обязанности Удостоверяющего центра	11
4.2. Обязанности Пользователя	13
5. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ	14
5.1. Виды конфиденциальной информации	14
5.2. Виды информации, не относящейся к конфиденциальной	15
5.3. Предоставление конфиденциальной информации	15
6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	15
7. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ	16
7.1. Регистрация Пользователей Удостоверяющего центра.....	16
7.2. Создание ключей электронной подписи	17
7.3. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи.....	17
7.4. Сроки действия ключей электронной подписи Пользователя	18
7.5. Смена ключей электронной подписи Пользователя	18
7.6. Смена ключей электронной подписи Удостоверяющего центра.....	20
7.7. Подтверждение подлинности электронной подписи Удостоверяющего центра в выданных квалифицированных сертификатах.....	21
7.8. Подтверждение подлинности электронной подписи Пользователя в электронном документе.....	21
7.9. Порядок предоставления доступа к реестру квалифицированных сертификатов Удостоверяющего центра.....	22

7.10. Порядок регистрации Пользователей в Единой системе идентификации и аутентификации.....	23
8. СОДЕРЖАНИЕ И ФОРМА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА	23
9. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ (ОТОЗВАННЫХ) СЕРТИФИКАТОВ	23
10. РАЗРЕШЕНИЕ СПОРОВ.....	23
11. ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА	24
12. ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ	24
13. ПРИЛОЖЕНИЯ	24

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аккредитованный Удостоверяющий центр - удостоверяющий центр, прошедший процедуру признания уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон "Об электронной подписи").

Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата) - лицо, которому в установленном Законом порядке выдан сертификат ключа проверки электронной подписи.

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".

Запрос на сертификат ключа проверки электронной подписи - электронное сообщение определенного формата и синтаксиса, содержащее необходимую информацию для создания сертификата.

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

Информационная система общего пользования - информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Квалифицированная электронная подпись - 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" и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

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

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

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

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

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 действующим законодательством РФ.

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Личный кабинет Заявителя – персональное информационное пространство Заявителя в информационной системе Удостоверяющего центра.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

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

Пользователь Удостоверяющего центра (далее - Пользователь) – лицо, присоединившееся к настоящему Регламенту.

Пункт регистрации - территориальное подразделение Удостоверяющего Центра либо юридическое лицо или индивидуальный предприниматель, осуществляющие от имени Удостоверяющего Центра функции по проверке регистрационных данных Пользователей, вручению квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом "Об электронной подписи".

Регистрационная информация Пользователя - информация, предоставляемая Пользователем в целях создания сертификата ключа проверки электронной подписи.

Реестр Пользователей – база данных Удостоверяющего центра, содержащая регистрационную информацию Пользователей.

Реестр сертификатов – база данных Удостоверяющего центра, содержащая сведения о созданных Удостоверяющим центром сертификатах.

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 защиты информации - (далее - СКЗИ) - 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 с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи и ключей 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 - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об 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.

1. ВВЕДЕНИЕ

ОАО «ИнфоТеКС Интернет Траст» выполняет функции аккредитованного Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» и является ответчиком по всем юридическим вопросам деятельности Удостоверяющего центра.

1.1. Обзорная информация

Настоящий Регламент определяет механизмы предоставления услуг Удостоверяющего центра по созданию и выдаче квалифицированных сертификатов, включая обязанности Удостоверяющего центра и пользователей Удостоверяющего центра (далее - стороны), процедуры взаимодействия сторон, форматы документов и данных, а также основные организационно-технические меры по обеспечению информационной безопасности при использовании ключевой информации и средств электронной подписи.

1.2. Идентификация Регламента

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

Версия: 2.0.

Дата вступления в силу: 15.02.2017 г.

1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде в репозитории ОАО «ИнфоТеКС Интернет Траст» по адресу iitrust.ru.

1.4. Область применения Регламента

1.4.1. Настоящий Регламент предназначен для определения порядка реализации функций Удостоверяющего центра ОАО «ИнфоТеКС Интернет Траст», осуществления его прав и исполнения обязанностей, а также для регулирования отношений, возникающих в процессе предоставления услуг Удостоверяющего центра.

1.5. Заключение договора присоединения

1.5.1. Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.

1.5.2. Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявки на услуги Удостоверяющего центра. С момента подачи заявки Заявитель считается присоединившимся к Регламенту и становится стороной Регламента – Пользователем Удостоверяющего центра.

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

1.6. Контактная информация Удостоверяющего центра ОАО «ИнфоТеКС Интернет Траст»

Юридический адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1.

Почтовый адрес: 127287, Москва, Старый Петровско-Разумовский проезд, дом. 1/23, стр.1.

Телефон: (495) 737-93-72, факс: (495) 737-93-73.

Телефон технической поддержки: (495) 737-33-69.

Телефон для справок, по России звонок бесплатный: 8-800-250-0-260 (кроме звонков из Москвы)

E-mail: 77@iitrust.ru

Web: <http://iitrust.ru/>

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Услуги, предоставляемые Удостоверяющим центром

2.1.1. Создание и выдача квалифицированных сертификатов лицам, обратившимся за их получением.

2.1.2. Предоставление по обращениям Пользователей средств электронной подписи.

2.1.3. Создание по обращениям Пользователей ключей электронной подписи, с гарантией обеспечения их конфиденциальности.

2.1.4. Прекращение действия созданных и выданных Удостоверяющим центром квалифицированных сертификатов, по заявлению владельца сертификата.

2.1.5. Предоставление информации из реестра квалифицированных сертификатов Удостоверяющего центра.

2.1.6. Проверку уникальности ключей проверки электронных подписей в создаваемых квалифицированных сертификатах.

2.1.7. Осуществление по обращениям Пользователей подтверждения подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов.

2.1.8. Осуществление по обращениям Пользователей подтверждения подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах.

2.1.9. Регистрация владельцев квалифицированных сертификатов, выданных Удостоверяющим центром, в Единой системе идентификации и аутентификации.

2.1.10. Другие, связанные с использованием электронной подписи, услуги.

2.2. Функции, выполняемые Удостоверяющим центром

Функционирование Удостоверяющего центра обеспечивается выполнением следующих функций:

2.2.1. Административные функции:

2.2.1.1 Управление деятельностью Удостоверяющего центра.

2.2.1.2 Координация деятельности Удостоверяющего центра и Пунктов регистрации.

2.2.1.3 Взаимодействие с Пользователями в части разрешения вопросов, связанных с применением предоставленных средств электронной подписи, ключей электронных подписей и квалифицированных сертификатов.

2.2.1.4 Взаимодействие с Пользователями в части разрешения вопросов подтверждения подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов.

2.2.1.5 Взаимодействие с Пользователями в части разрешения вопросов, связанных с подтверждением электронной подписи Удостоверяющего центра в квалифицированных сертификатах, выданных Удостоверяющим центром в форме электронного документа.

2.2.2. **Функции регистрации**

Функции регистрации включают:

- установление личности заявителя - физического лица, обратившегося за получением квалифицированного сертификата, по документу, удостоверяющему личность;
- проверка правомочий лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
- проверка достоверности регистрационной информации Пользователей на основании информации, содержащейся в представленных Пользователем документах, а также полученной из государственных информационных ресурсов;
- передача в Единую систему идентификации и аутентификации сведений о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате;
- иное взаимодействие с Пользователями в соответствии с настоящим Регламентом.

2.2.3. **Функции создания ключей и сертификации ключей проверки электронных подписей**

- создание и выдача Пользователям квалифицированных сертификатов в форме электронного документа, а также, по обращению Пользователей, в форме бумажного документа;
- создание и выдача по обращениям Пользователей ключей электронных подписей и ключей проверки электронных подписей.

2.2.4. **Функции безопасности**

- выполнение комплекса организационно-технических мероприятий по защите ключей электронной подписи Удостоверяющего центра и Пользователей, а также информационных ресурсов Удостоверяющего центра, включающих, в частности, информацию, содержащуюся в реестре сертификатов, от несанкционированного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечение выполнения процедур создания, использования, хранения и уничтожения ключевой информации в соответствии с требованиями эксплуатационной документации на средства электронной подписи;
- недопущение копирования ключей электронных подписей на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без ее предварительного шифрования, осуществляемого при помощи средства криптографической защиты информации;
- реализация средствами Удостоверяющего центра протоколов аннулирования или прекращения действия сертификатов, формирования, обновления и публикации списков аннулированных сертификатов;
- установление сроков действия ключей электронных подписей и квалифицированных сертификатов;
- аннулирование квалифицированных сертификатов в случаях, установленных Федеральным законом "Об электронной подписи";
- прекращение действия квалифицированных сертификатов в случаях, установленных Федеральным законом "Об электронной подписи", другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, а также настоящим Регламентом;
- приостановление действия квалифицированных сертификатов в случаях, установленных настоящим Регламентом;

- предоставление в любое время любому лицу доступа к актуальным спискам аннулированных (отозванных) сертификатов;
- техническое обеспечение процедуры подтверждения подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов;
- техническое обеспечение процедуры подтверждения подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах.

2.3. Пользователи

2.3.1. Пользователями Удостоверяющего центра могут быть физические лица, в том числе зарегистрированные в качестве индивидуальных предпринимателей, и юридические лица, присоединившиеся к настоящему Регламенту.

2.3.2. В случае, когда в качестве Пользователя выступает юридическое лицо, его интересы представляет физическое лицо, действующее на основании учредительных документов, либо доверенности.

2.4. Разрешение споров

2.4.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Пользователь.

2.4.2. При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках действия настоящего Регламента, путем совместных переговоров.

2.4.3. Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе совместных переговоров, разрешаются в судебном порядке в соответствии с законодательством РФ.

2.5. Возмездность услуг

Услуги Удостоверяющего центра оказываются на возмездной основе.

2.6. Прекращение деятельности Удостоверяющего центра

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

3. ПРАВА

3.1. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

3.1.1. Отказать в регистрации и предоставлении услуг Удостоверяющего центра лицам, подавшим заявку на услуги, с указанием причин отказа.

3.1.2. Отказать в аннулировании (отзыве) сертификата в случае, если истек установленный срок действия ключа электронной подписи, соответствующего ключу проверки электронной подписи, содержащемуся в квалифицированном сертификате.

3.1.3. Приостановить действие квалифицированного сертификата при наличии у Удостоверяющего центра оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован, с уведомлением владельца квалифицированного сертификата и указанием обоснованных причин.

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. Права Пользователей Удостоверяющего центра

Пользователи Удостоверяющего центра имеют право:

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

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

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

3.2.4. Использовать имеющиеся или предоставленные Удостоверяющим центром средства электронной подписи для формирования ключей электронной подписи и запросов на квалифицированный сертификат.

3.2.5. Получить доступ к актуальным спискам аннулированных (отозванных) сертификатов.

3.2.6. Получить квалифицированные сертификаты как в форме электронных документов, так и в форме бумажных документов.

3.2.7. Обращаться в Удостоверяющий центр с заявлением на регистрацию в Единой системе идентификации и аутентификации.

3.2.8. Обращаться в Удостоверяющий центр за подтверждением подлинности электронных подписей, созданных с использованием выданных Удостоверяющим центром квалифицированных сертификатов, в соответствии с порядком, определенным настоящим Регламентом.

3.2.9. Обращаться в Удостоверяющий центр за подтверждением подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах в соответствии с порядком, определенным настоящим Регламентом.

3.2.10. Обращаться в Удостоверяющий центр с заявлениями на аннулирование (отзыв) квалифицированного сертификата, в течение срока действия сертификата.

4. ОБЯЗАННОСТИ

4.1. Обязанности Удостоверяющего центра

4.1.1. По работе с ключами электронной подписи Удостоверяющего центра

4.1.1.1 Удостоверяющий центр обязан использовать ключ электронной подписи Удостоверяющего центра только для подписи создаваемых им квалифицированных сертификатов и списков аннулированных (отозванных).

4.1.1.2 Удостоверяющий центр обязан принимать меры по защите ключа электронной подписи Удостоверяющего центра в соответствии с положениями настоящего Регламента и действующими нормативными правовыми актами РФ.

4.1.2. По регистрации Пользователей

4.1.2.1 Удостоверяющий центр обеспечивает регистрацию Пользователей в реестре пользователей по их заявкам на услуги удостоверяющего центра в соответствии с порядком, изложенном в настоящем Регламенте.

4.1.2.2 Удостоверяющий центр обязан не разглашать (не публиковать) регистрационную информацию пользователей, за исключением информации, включаемой в состав квалифицированных сертификатов.

4.1.3. По созданию ключей электронных подписей Пользователей

4.1.3.1 Удостоверяющий центр создает ключи электронных подписей и ключи проверки электронных подписей на основании соответствующих обращений Пользователей. Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется при помощи средств электронной подписи, входящих в состав программно-технических средств Удостоверяющего центра.

4.1.3.2 Удостоверяющий центр обязан обеспечить уникальность создаваемых ключей проверки электронных подписей в реестре квалифицированных сертификатов Удостоверяющего центра.

4.1.3.3 Удостоверяющий центр обязан обеспечить безопасное хранение ключей электронных подписей (ключевых документов) после их создания до момента передачи Пользователю.

4.1.3.4 Удостоверяющий центр обязан информировать в письменной форме Пользователей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, а также о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

4.1.4. По созданию квалифицированных сертификатов

4.1.4.1 Удостоверяющий центр обеспечивает создание квалифицированных сертификатов по обращениям Пользователей, в соответствии с порядком, определенным настоящим Регламентом.

4.1.4.2 Удостоверяющий центр обязан обеспечить уникальность номеров создаваемых квалифицированных сертификатов в реестре квалифицированных сертификатов Удостоверяющего центра.

4.1.5. По аннулированию квалифицированных сертификатов

Удостоверяющий центр аннулирует квалифицированный сертификат в случаях, установленных Федеральным законом "Об электронной подписи", а именно:

- 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.

4.1.6. По прекращению действия квалифицированных сертификатов

4.1.6.1 Удостоверяющий центр обязан прекратить действие квалифицированного сертификата по заявлению на аннулирование (отзыв) сертификата, в соответствии с порядком и на основаниях, указанным в разделе 7.4.4 настоящего Регламента.

4.1.7. По поддержанию актуальности списков аннулированных квалифицированных сертификатов

4.1.7.1 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 (отозванных) сертификатов.

4.1.7.2 Удостоверяющий центр обязан внести информацию о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных сертификатов в течение 12 часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия квалифицированного сертификата.

4.1.7.3 Удостоверяющий центр обязан осуществлять публикацию списков аннулированных сертификатов в точках распространения, указанных в полях CRLDistributionPoints и AuthorityInfoAccess выдаваемых Удостоверяющим центром квалифицированных сертификатов.

4.1.8. По ведению реестра сертификатов

4.1.8.1 Удостоверяющий центр обязан обеспечивать формирование и ведение реестра квалифицированных сертификатов в течение всего срока деятельности Удостоверяющего центра.

4.1.8.2 Реестр квалифицированных сертификатов ведется Удостоверяющим центром в электронном виде 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.

4.1.8.3 Удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов.

4.1.8.4 Удостоверяющий центр обязан обеспечить любому лицу в любое время доступ с использованием информационно-телекоммуникационных сетей общего пользования к реестру сертификатов.

4.1.9. Ответственность Удостоверяющего центра

4.1.9.1. Удостоверяющий центр несет ответственность за неисполнение либо ненадлежащее исполнение обязательств по настоящему Регламенту, за исключением случаев, предусмотренных пунктом 4.1.9.2 настоящего Регламента, в соответствии с законодательством Российской Федерации.

4.1.9.2. Удостоверяющий центр не несет ответственности за неисполнение либо ненадлежащее исполнение обязательств по настоящему Регламенту и за причиненные в результате этого убытки, в случаях нарушения Пользователем настоящего Регламента, а также в случаях подделки, подлога либо иного искажения Пользователем или третьими лицами документов, удостоверяющих личность Заявителя - физического лица, подтверждающих правомочия лица, выступающего от имени Заявителя - юридического лица или содержащих регистрационную информацию Пользователя.

4.2. Обязанности Пользователя

4.2.1. Обязанности лица, проходящего процедуру регистрации в Удостоверяющем центре

4.2.1.1 Лицо, проходящее процедуру регистрации в Удостоверяющем центре, обязано представить регистрационную информацию в объеме, необходимом для получения услуг Удостоверяющего центра.

4.2.1.2 Лицо, проходящее процедуру регистрации в Удостоверяющем центре, несет ответственность за достоверность предоставленной регистрационной информации.

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, в том числе меры по обеспечению конфиденциальности аутентификационных данных, используемых для доступа к электронным сервисам, предоставляемым Удостоверяющим центром.

4.2.2.2 Немедленно обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата в следующих случаях:

- при компрометации ключа электронной подписи, принадлежащего владельцу сертификата;
- при компрометации аутентификационной информации Пользователя, используемой для получения доступа к электронным сервисам, предоставляемым Удостоверяющим центром.

4.2.2.3 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.

4.2.2.4 Извещать Удостоверяющий центр обо всех изменениях своей регистрационной информации в течение 3 (трех) рабочих дней с даты регистрации изменений. При этом Удостоверяющий центр вправе затребовать у пользователя документы, подтверждающие изменение регистрационной информации.

4.2.2.5 Использовать для формирования 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".

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

4.2.2.7 Не использовать квалифицированный сертификат, заявление на прекращение действия которого подано в Удостоверяющий центр.

4.2.3. Ответственность Пользователя

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

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

5. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

5.1. Виды конфиденциальной информации

5.1.1. Ключ электронной подписи владельца квалифицированного сертификата.

5.1.2. Идентификационная и аутентификационная информация, предоставляемая Пользователю в процессе прохождения процедуры регистрации и получения сертификата ключа поверки электронной подписи.

5.1.3. Персональные данные и корпоративная информация Пользователей, не подлежащие распространению в составе квалифицированного сертификата.

5.2. Виды информации, не относящейся к конфиденциальной

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

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

5.2.3. Информация, включаемая в создаваемые Удостоверяющим центром квалифицированные сертификаты и списки аннулированных (отозванных) сертификатов, не считается конфиденциальной.

5.2.4. Также не считается конфиденциальной информация о настоящем Регламенте.

5.3. Предоставление конфиденциальной информации

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

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

6.1. При оказании услуг по выдаче квалифицированного сертификата ключа проверки электронной подписи Удостоверяющий центр, в соответствии с требованиями, установленными в соответствии с Законом "Об электронной подписи", обрабатывает следующие персональные данные физических лиц, обращающихся за получением квалифицированного сертификата:

- Фамилия, имя, отчество.
- Наименование занимаемой должности, в случае физического лица, обращающегося за получением квалифицированного сертификата от имени заявителя - юридического лица.
- Абонентский номер мобильного телефона.
- Адрес электронной почты.
- Страховой номер индивидуального лицевого счета в системе персонифицированного учета ПФР.
- Идентификационный номер налогоплательщика, в случае заявителя - физического лица.
- Основной государственный номер индивидуального предпринимателя, в случае заявителя - физического лица, зарегистрированного в качестве индивидуального предпринимателя.
- Номер основного документа, удостоверяющего личность.
- Пол.
- Дата и место рождения.

6.2. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица на обработку Удостоверяющим центром его персональных данных, перечисленных в пункте 6.1 настоящего Регламента, в целях создания квалифицированного сертификата ключа проверки электронной подписи. При этом Удостоверяющему центру предоставляется право на:

- обработку персональных данных любыми способами, в том числе путем включения в электронные базы, осуществление всех действий (операций) с персональными данными,

включая сбор, запись, систематизацию, накопление, хранение, уточнение, обновление, изменение, извлечение, использование, обезличивание, блокирование, удаление, уничтожение;

- передачу персональных данных в Единую систему идентификации и аутентификации.

6.3. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица на поручение Удостоверяющим центром обработки его персональных данных, перечисленных в пункте 6.1 настоящего Регламента, другому лицу в целях проверки регистрационных данных Пользователя и вручения квалифицированного сертификата ключа проверки электронной подписи его владельцу.

6.4. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица, с тем, что его персональные данные, включаемые Удостоверяющим центром в создаваемый на его имя квалифицированный сертификат ключа проверки электронной подписи, относятся к общедоступным персональным данным. К персональным данным, включаемым в состав квалифицированного сертификата ключа проверки электронной подписи, относятся:

- Фамилия, имя, отчество.
- Адрес электронной почты.
- Страховой номер индивидуального лицевого счета в системе персонифицированного учета ПФР.
- Идентификационный номер налогоплательщика.
- Основной государственный номер индивидуального предпринимателя, в случае Заявителя - физического лица, зарегистрированного в качестве индивидуального предпринимателя.

6.5. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица на получение сервисной информации в составе SMS-сообщений, направляемых на указанный Заявителем при регистрации абонентский номер мобильного телефона.

6.6. Присоединение Заявителя - юридического лица к настоящему Регламенту является подтверждением того, что:

- персональные данные, перечисленные в пункте 6.1. настоящего Регламента, физического лица, указанного в качестве владельца сертификата наряду с указанием наименования юридического лица, передаются Удостоверяющему центру в целях создания квалифицированного сертификата ключа проверки электронной подписи с согласия этого физического лица с предоставлением Удостоверяющему центру права осуществлять с персональными данными все действия, указанные в пункте 6.2 настоящего Регламента;
- физическое лицо, указанное в качестве владельца сертификата наряду с указанием наименования юридического лица, уведомлено юридическим лицом о том, что персональные данные этого физического лица, включаемые Удостоверяющим центром в создаваемый сертификат ключа проверки электронной подписи и перечисленные в пункте 6.3 настоящего Регламента, относятся к общедоступным персональным данным.

7. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ

7.1. Регистрация Пользователей Удостоверяющего центра

7.1.1. Регистрация Пользователя Удостоверяющего центра осуществляется на основании заявки на услуги удостоверяющего центра, содержащей регистрационные данные Заявителя,

включая информацию, подлежащую внесению в квалифицированный сертификат в соответствии с Федеральным законом "Об электронной подписи".

7.1.2. Заявка на услуги удостоверяющего центра может быть подана Заявителем одним из следующих способов:

7.1.2.1 Путем подачи в Удостоверяющий центр заявки в форме документа на бумажном носителе, подписанного собственноручной подписью заявителя – физического лица или лица, обращающегося за получением квалифицированного сертификата от имени заявителя – юридического лица на основании учредительных документов юридического лица или доверенности.

7.1.2.2 Путем подачи заявки в форме электронного документа, сформированного Заявителем при помощи программного обеспечения, распространяемого с сайта Удостоверяющего центра и переданного в адрес Удостоверяющего центра по доверенным каналам связи.

7.1.2.3 Путем подачи заявки в форме электронного документа через личный кабинет Заявителя в информационной системе Удостоверяющего центра.

7.2. Создание ключей электронной подписи

Создание ключей электронной подписи осуществляется:

7.2.1. Самостоятельно Пользователем Удостоверяющего центра при помощи установленного на рабочем месте Пользователя средства электронной подписи или при помощи отчуждаемого устройства, являющегося самостоятельным СКЗИ (например, eToken ГОСТ или JaCarta ГОСТ), имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи".

7.2.2. Удостоверяющим центром, при наличии соответствующего обращения со стороны Пользователя.

7.3. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи

7.3.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявки, содержащей регистрационные данные Пользователя.

7.3.2. В случае самостоятельного создания Пользователем ключа электронной подписи в соответствии с пунктом 7.2.1 настоящего Регламента, в Удостоверяющий центр должен быть передан файл запроса на сертификат ключа проверки электронной подписи в формате PKCS#10. Передача файла запроса на сертификат ключа проверки электронной подписи осуществляется Пользователем на отчуждаемом носителе информации или через личный кабинет Заявителя в информационной системе Удостоверяющего центра.

7.3.3. Для получения квалифицированного сертификата Пользователь представляет в Пункт регистрации Удостоверяющего центра документы, определенные Федеральным законом "Об электронной подписи", а также дополнительные документы, определенные требованиями отдельных информационных систем, для обеспечения информационного взаимодействия с участниками которых предназначен запрашиваемый сертификат. Перечень и формы необходимых документов публикуются на сайте Удостоверяющего центра.

7.3.4. Перед выдачей квалифицированного сертификата Удостоверяющий центр:

- устанавливает личность заявителя - физического лица, обратившегося за получением квалифицированного сертификата, по основному документу, удостоверяющему личность;
- осуществляет проверку правомочия лица, выступающего от имени заявителя – юридического лица, обращаться за получением квалифицированного сертификата;

- осуществляет проверку достоверности документов и сведений, представленных Пользователем в целях получения квалифицированного сертификата, используя при этом, в частности, документы, полученные из государственных информационных ресурсов:
 - выписка из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
 - выписка из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
 - выписка из единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

7.3.5. При выдаче квалифицированного сертификата Удостоверяющий центр под расписку ознакомляет Пользователя с информацией, содержащейся в выдаваемом квалифицированном сертификате.

7.3.6. Одновременно с квалифицированным сертификатом Пользователю выдаются:

- созданный Удостоверяющим центром ключ электронной подписи Пользователя, в случае наличия соответствующего обращения со стороны Пользователя;
- средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи", в случае наличия соответствующего обращения со стороны Пользователя;
- 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.

7.4. Сроки действия ключей электронной подписи Пользователя

Срок действия ключа электронной подписи, ключа проверки электронной подписи и, соответственно, квалифицированного сертификата ключа проверки электронной подписи Пользователя устанавливаются равными 12 месяцам.

7.5. Смена ключей электронной подписи Пользователя

7.5.1. Плановая смена ключей электронной подписи Пользователя

7.5.1.1 Плановая смена ключей электронной подписи производится не ранее, чем за 40 (сорок), и не позднее, чем за 10 (десять) суток до окончания срока действия текущего квалифицированного сертификата (ключа электронной подписи и ключа проверки электронной подписи) Пользователя.

7.5.1.2 Создание нового ключа электронной подписи, ключа проверки электронной подписи и запроса на квалифицированный сертификат осуществляется Пользователем самостоятельно, с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи".

7.5.1.3 Запрос на сертификат, сформированный с использованием средств электронной подписи, установленных на автоматизированном рабочем месте Пользователя, должен быть подписан квалифицированной электронной подписью Пользователя, основанной на действующем квалифицированном сертификате ключа проверки электронной подписи Пользователя, и передан в Удостоверяющий центр.

7.5.1.4 Если владельцем квалифицированного сертификата является юридическое лицо или индивидуальный предприниматель, то перед выдачей нового сертификата Удостоверяющий центр осуществляет проверку актуальности содержащейся в сертификате информации, используя документы, полученные из государственных информационных ресурсов:

- выписка из единого государственного реестра юридических лиц в отношении заявителя - юридического лица;
- выписка из единого государственного реестра индивидуальных предпринимателей в отношении заявителя - индивидуального предпринимателя;
- выписка из единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

7.5.1.5 Если владельцем квалифицированного сертификата является юридическое лицо, то перед выдачей нового сертификата Удостоверяющий центр осуществляет проверку правомочия лица, выступающего от имени юридического лица, обращаться за получением квалифицированного сертификата.

7.5.1.6 Создание квалифицированного сертификата для вновь сформированного ключа проверки электронной подписи Пользователя осуществляется Удостоверяющим центром не позднее 7 (семи) рабочих дней, следующих за рабочим днем, в течение которого Удостоверяющим центром был получен запрос на квалифицированный сертификат.

7.5.1.7 В случае если Пользователь не произвел плановую смену ключа электронной подписи в указанные в п. 7.5.1.1 сроки, то создание нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата ключа проверки электронной подписи производится в порядке, определенном пунктом 7.3 настоящего Регламента.

7.5.2. Внеплановая смена ключей электронной подписи Пользователя

7.5.2.1 Внеплановая смена ключей электронной подписи производится:

- По инициативе Пользователя в случае прекращения действия квалифицированного сертификата до истечения срока его действия по основаниям, указанным в пунктах 4.2.2.2 и 4.2.2.3 настоящего Регламента.
- При компрометации ключа электронной подписи Удостоверяющего центра.
- В иных случаях, связанных с невозможностью использования имеющегося ключа электронной подписи.

7.5.2.2 Создание и выдача квалифицированного сертификата ключа проверки электронной подписи при внеплановой смене ключа электронной подписи Пользователя производится в порядке, определенном в п. 7.3 настоящего Регламента.

7.5.3. Аннулирование квалифицированного сертификата

7.5.3.1 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.

7.5.3.2 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.

7.5.4. Прекращение действия квалифицированного сертификата

Удостоверяющий центр прекращает действие квалифицированного сертификата в следующих случаях:

- на основании заявления владельца квалифицированного сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа с квалифицированной электронной подписью владельца квалифицированного сертификата, поданного в Удостоверяющий центр по форме Приложений 1 или 2 к настоящему Регламенту;
- установлено, что в результате технической ошибки квалифицированный сертификат содержит недостоверные или неполные сведения;
- установлено, что квалифицированный сертификат содержит сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя.

7.5.5. Приостановление действия квалифицированного сертификата

7.5.5.1 Приостановление действия квалифицированного сертификата может быть осуществлено Удостоверяющим центром в следующих случаях:

- при наличии у Удостоверяющего центра оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован;
- при нарушении Пользователем обязанностей, изложенных в пункте 4.2.2 настоящего Регламента.

7.5.5.2 В случае устранения причин, послуживших основанием для приостановления, действие квалифицированного сертификата может быть возобновлено.

7.6. Смена ключей электронной подписи Удостоверяющего центра

7.6.1. Сроки действия ключей электронной подписи Удостоверяющего центра

Сроки действия ключей электронной подписи и сертификатов ключей проверки электронной подписи Удостоверяющего центра устанавливаются федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

7.6.2. Плановая смена ключей электронной подписи Удостоверяющего центра

Плановая смена ключей электронной подписи Удостоверяющего центра и соответствующего сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется не позднее окончания срока действия текущего ключа электронной подписи Удостоверяющего центра в соответствии с порядком, определяемым федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

7.6.3. Внеплановая смена ключей электронной подписи Удостоверяющего центра

7.6.3.1 Внеплановая смена ключей электронной подписи Удостоверяющего центра производится в случае компрометации или угрозы компрометации ключа электронной подписи Удостоверяющего центра.

7.6.3.2 Внеплановая смена ключей электронной подписи Удостоверяющего центра выполняется в порядке, определенном эксплуатационной документацией на средства удостоверяющего центра.

7.6.3.3 При выполнении внеплановой смены ключей электронной подписи Удостоверяющего центра также должны быть проведены работы по внеплановой смене ключей электронных подписей пользователей, сертификаты которых подписаны электронной подписью

Удостоверяющего центра, созданной с использованием скомпрометированного ключа электронной подписи Удостоверяющего центра.

7.7. Подтверждение подлинности электронной подписи Удостоверяющего центра в выданных квалифицированных сертификатах

7.7.1. Удостоверяющий центр осуществляет подтверждение подлинности электронной подписи Удостоверяющего центра в выданных Удостоверяющим центром квалифицированных сертификатах по заявлению Пользователя на подтверждение подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя, поданного в Удостоверяющий центр по формам Приложений 2 и 3 к настоящему Регламенту.

7.7.2. Обязательным приложением к заявлению на подтверждение подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя является внешний носитель информации, содержащий файл сертификата, подвергающегося процедуре проверки, в формате PKCS#7 в кодировке Base64 (CER).

7.7.3. Срок проведения работ по подтверждению подлинности электронной подписи Удостоверяющего центра в выданном Удостоверяющим центром квалифицированном сертификате и предоставлению заключения о произведенной проверке составляет 10 (десять) рабочих дней с момента поступления в Удостоверяющий центр заявления пользователя на подтверждение подлинности электронной подписи Удостоверяющего центра в выданном им квалифицированном сертификате.

7.7.4. Результатом проведения работ по подтверждению подлинности электронной подписи Удостоверяющего центра в квалифицированном сертификате пользователя является заключение Удостоверяющего центра, заверенное собственноручной подписью ответственного сотрудника и печатью Удостоверяющего центра.

7.8. Подтверждение подлинности электронной подписи Пользователя в электронном документе

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

7.8.2. Заявление на подтверждение подлинности электронной подписи в электронном документе подается Пользователем в Удостоверяющий центр или Пункт регистрации лично.

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

7.8.4. Бремя доказывания достоверности даты и времени формирования электронной подписи в электронном документе возлагается на заявителя.

7.8.5. Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является внешний носитель информации, содержащий электронный документ с электронной подписью в формате PKCS#7.

7.8.6. Срок проведения работ по подтверждению подлинности электронной подписи в электронном документе составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

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

7.8.8. Результатом проведения работ по подтверждению подлинности 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, имеющем 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).

7.8.9. 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.

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

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

7.9. Порядок предоставления доступа к реестру квалифицированных сертификатов Удостоверяющего центра

7.9.1. Информация, содержащаяся в реестре квалифицированных сертификатов Удостоверяющего центра, предоставляется любому лицу по его запросу, направляемому в Удостоверяющий центр по электронной почте либо через сайт Удостоверяющего центра.

7.9.2. Запрос должен содержать идентификационные данные лица, информация о квалифицированном сертификате которого запрашивается, в объеме, необходимом и достаточном для осуществления поиска в реестре сертификатов:

- полное наименование и идентификационный номер налогоплательщика – для юридического лица;
- фамилия, имя, отчество и страховой номер индивидуального лицевого счета в системе персонифицированного учета ПФР – для физического лица.

7.9.3. Удостоверяющий центр предоставляет информацию, содержащуюся в реестре квалифицированных сертификатов, в течении 8 (восьми) рабочих часов с момента получения соответствующего запроса.

7.10. Порядок регистрации Пользователей в Единой системе идентификации и аутентификации

7.10.1. Удостоверяющий центр осуществляет регистрацию физических лиц в Единой системе идентификации и аутентификации на основании заявления, поданного в Удостоверяющий центр в форме документа на бумажном носителе с собственноручной подписью владельца сертификата (Приложение 5 к настоящему Регламенту).

7.10.2. Удостоверяющий центр осуществляет регистрацию в Единой системе идентификации и аутентификации как физических лиц, являющихся владельцами выданных Удостоверяющим центром квалифицированных сертификатов, так и физических лиц, имеющих право действовать от имени юридического лица без доверенности и указанных в качестве владельца квалифицированного сертификата наряду с наименованием юридического лица, которому был выдан сертификат.

7.10.3. Регистрация в Единой системе идентификации и аутентификации юридических лиц осуществляется самостоятельно физическими лицами, имеющими право действовать от имени юридического лица без доверенности, после прохождения ими процедуры регистрации в Единой системе идентификации и аутентификации в качестве физических лиц.

8. СОДЕРЖАНИЕ И ФОРМА КВАЛИФИЦИРОВАННОГО СЕРТИФИКАТА

Удостоверяющий центр создает по обращениям Заявителей 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".

9. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ (ОТОЗВАННЫХ) СЕРТИФИКАТОВ

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

10. РАЗРЕШЕНИЕ СПОРОВ

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

10.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, стороны должны руководствоваться законодательством РФ.

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

10.4. Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

10.5. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в Арбитражном суде в соответствии с законодательством РФ.

11. ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

11.1. Удостоверяющий центр осуществляет свою деятельность на основании разрешительных документов на осуществление всех видов деятельности, связанных с предоставлением услуг Удостоверяющего центра (см. раздел 2.1 настоящего Регламента).

11.2. Удостоверяющий центр обеспечивает выполнение мер по защите информации, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом "Об информации, информационных технологиях и о защите информации".

11.3. Для обеспечения своей деятельности Удостоверяющий центр использует средства удостоверяющего центра, включая средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи".

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

12. ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

12.1. Оригинал настоящего Регламента формируется в форме документа на бумажном носителе и заверяется собственноручной подписью руководителя и печатью Удостоверяющего центра.

12.2. Сообщения об ошибках в положениях настоящего Регламента, а также предложения по уточнению его положений могут направляться в Удостоверяющий центр в соответствии с контактной информацией, указанной в разделе 1.6 настоящего Регламента.

12.3. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра не оказывают, либо оказывают незначительное влияние на работу пользователей, вносятся без изменения номера версии данного документа.

12.4. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра могут иметь значительное влияние на работу пользователей, вносятся с увеличением номера версии данного документа.

12.5. Уведомление пользователей о внесении изменений в Регламент осуществляется путем публикации актуальной версии Регламента в электронном виде в репозитории ОАО "ИнфоТеКС Интернет Траст" по адресу <https://itrust.ru/>.

13. ПРИЛОЖЕНИЯ:

1. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи (для юридических лиц).
2. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи (для физических лиц).
3. Форма заявления на подтверждение подлинности электронной подписи Удостоверяющего центра в сертификате пользователя (для юридических лиц).
4. Форма заявления на подтверждение подлинности электронной подписи Удостоверяющего центра в сертификате пользователя (для физических лиц).
5. Форма заявления на регистрацию в Единой системе идентификации и аутентификации.

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

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на прекращение действия сертификата ключа проверки электронной подписи, выданного
юридическому лицу

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

Серийный номер сертификата: _____

Полное наименование юридического лица: _____

Фамилия, имя, отчество физического лица, указанного в качестве владельца сертификата
наряду с наименованием юридического лица: _____

ИНН: _____ КПП: _____

в связи с _____
(причина прекращения действия сертификата)

Подпись и расшифровка подписи физического лица, указанного в качестве владельца сертификата наряду с
наименованием юридического лица, или физического лица, имеющего право действовать от имени юридического
лица без доверенности (руководителя юридического лица):

(подпись)

(фамилия, инициалы)

" ____ " _____ 20__ г.

М.П.

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

В Удостоверяющий Центр
ОАО «ИнфоТеКС Интернет Траст»

Заявление
на прекращение действия сертификата ключа проверки электронной подписи, выданного
физическому лицу

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

Серийный номер сертификата: _____

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

СНИЛС: _____ ИНН: _____

ОГРНИП (для индивидуальных предпринимателей): _____

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
ОАО «ИнфоТеКС Интернет Траст» услуг по созданию
и выдаче квалифицированных сертификатов ключей
проверки электронных подписей

В Удостоверяющий Центр
ОАО «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 ОАО «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: _____