«Утверждаю»
Генеральный директор
ООО «Системы управления
идентификацией»

С.В. Белова
« 15 » января 2019 г

РЕГЛАМЕНТ

оказания Удостоверяющим центром ООО «Системы управления идентификацией» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей

2019 г.

Содержание

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 Федеральным законом "Об электронной подписи" 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.

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 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 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

ООО «Системы управления идентификацией» выполняет функции аккредитованного Удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «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.

Порядок реализации функций аккредитованного Удостоверяющего центра, исполнения его обязанностей и осуществления его прав, устанавливается Удостоверяющим центром и определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, если иное не установлено Федеральным законом «Об электронной подписи» и иными федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия.

1.2 Идентификация Регламента

Наименование документа: «Регламент оказания Удостоверяющим центром ООО «Системы управления идентификацией» услуг по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей».

Версия: 3.0.

Дата: 15.01.2019 г.

1.3 Публикация Регламента

Настоящий Регламент публикуется в электронном виде на сайте ООО «Системы управления идентификацией» по адресу http://signature.iidx.ru.

1.4 Пользователи Удостоверяющего центра

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

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

1.5 Присоединение к регламенту Удостоверяющему центру

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.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Предмет регулирования Порядка

Настоящий Регламент предназначен для определения порядка реализации функций Удостоверяющего центра ООО «Системы управления идентификацией» (далее – Удостоверяющий центр), осуществления его прав и исполнения обязанностей, а также для регулирования отношений, возникающих в процессе предоставления услуг Удостоверяющего центра, в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи" и принимаемыми в соответствии с ним нормативными правовыми актами, в том числе, в соответствии с Приказом Минкомсвязи России от 13.08.2018 N 397 "Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей".

Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Удостоверяющего центра и Пользователя УЦ, форматы данных, организационные мероприятия, направленные на обеспечение работы Удостоверяющего центра.

Настоящий Регламент предназначен для определения порядка реализации функций Удостоверяющего центра ООО «Системы управления идентификацией**» (далее – Удостоверяющий центр),** осуществления его прав и исполнения обязанностей, а также для регулирования отношений, возникающих в процессе предоставления услуг Удостоверяющего центра.

2.2 Сведения об Удостоверяющем центре

2.2.1. Адрес места нахождения Удостоверяющего центра ООО «Системы управления идентификацией**»:** 101000, г. Москва, ул. Мясницкая, дом 22 стр.1, подъезд 1А, комната 6.

2.2.2. График работы Удостоверяющего центра: ежедневно, кроме выходных и праздничных дней, с 10:00 до 19:00 по местному времени, в соответствии с часовым поясом места нахождения ООО «Системы управления идентификацией**»** или его обособленных подразделений (филиалов).

2.3 Порядок информирования о предоставлении услуг Удостоверяющего центра

Информирование заявителей по вопросам предоставления услуг Удостоверяющего центра осуществляется следующими способами:

- по месту нахождения офиса Удостоверяющего центра, адрес которого указан в разделе 2.2.1 Регламента, в рамках графика работы Удостоверяющего центра;
- по телефону +7 (495) 651-8424 (справочная, консультационная и техническая поддержка), согласно режиму работы, указанному в разделе 2.2.2 Регламента;
- по адресу электронной почты verification@iidx.ru; прием обращений осуществляется круглосуточно без обеда и выходных, обработка обращений и ответ на обращение осуществляются в рамках режима работы, указанного в разделе 2.2.2 Регламента;
- на официальном сайте Удостоверяющего центра http://signature.iidx.ru/.

Форма информирования Удостоверяющим центром лица, обратившегося в Удостоверяющий центр, соответствует форме обращения такого лица, либо возможна иная форма информирования с учетом пожеланий обратившегося лица и (или) характера обращений.

2.4 Стоимость услуг Удостоверяющего центра

2.4.1. Удостоверяющий центр осуществляет свою деятельность на платной основе;

2.4.2. Информацию о стоимости услуг Удостоверяющего центра любое лицо может получить способами, указанными в разделе 2.3 Регламента.

2.4.3. Стоимость услуг Удостоверяющего центра составляет:

- 3900 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на ключевом носителе Рутокен ЭЦП 2.0 для юридического лица
- 2400 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на носителе, предоставленном пользователем, для юридического лица
- 2900 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на ключевом носителе Рутокен ЭЦП 2.0 для индивидуальных предпринимателей
- 1400 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на носителе, предоставленном пользователем, для индивидуальных предпринимателей
- 2400 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на ключевом носителе Рутокен ЭЦП 2.0 для физических лиц
- 900 рублей 00 копеек - услуга изготовления ключа электронной подписи, ключа проверки электронной подписи и сертификата ключа проверки электронной подписи на носителе, предоставленном пользователем, для физических лиц.

2.4.4. Расчет между Пользователем и Удостоверяющим центром производится по тарифам, указанным на официальном сайте Удостоверяющего центра на день выставления счета, либо на договорной основе.

2.4.5. Оплата услуг Удостоверяющего центра осуществляется в российских рублях путем перечисления денежных средств на расчетный счет ООО «Системы управления идентификацией» или иным способом, предусмотренным договором, заключаемым между ООО «Системы управления идентификацией» и Пользователем. Датой оплаты считается дата поступления денежных средств на счет Удостоверяющего центра.

2.4.6. Удостоверяющий центр на безвозмездной основе оказывает следующие услуги:

- создание сертификатов ключей проверки электронной подписи пользователей УЦ в случае выполнения внеплановой смены ключей электронных подписей Удостоверяющего центра (в соответствии с процедурой, определенной Регламентом);
- предоставление участникам информационных систем в форме электронных документов сертификатов ключей проверки электронной подписи пользователей УЦ, находящихся в реестре сертификатов, а также информации об их действии в виде списков отозванных сертификатов;
- аннулирование (отзыв) действия сертификата ключей проверки электронной подписи пользователей УЦ в порядке и случае, указанных в настоящем Регламенте;

- регистрацию лица, которому выдан квалифицированный сертификат ключа проверки электронной подписи, в единой системе идентификации и аутентификации по его желанию.

3. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

В соответствии со ст. 13 Федерального закона от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" Удостоверяющий центр:

- создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона от 06.04.2011 N 63-ФЗ;
- 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;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей;
- 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;
- ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

Информируем в письменной форме 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;

обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

предоставляет 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;

обеспечивает конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

отказывает 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

отказывает 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 (п. 6 введен Федеральным законом от 30.12.2015 N 445-ФЗ);

Удостоверяющему центру запрещается указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром

Удостоверяющий центр по отношению к доверенным лицам является головным удостоверяющим центром и выполняет следующие функции:

- осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных доверенными лицами сертификатах ключей проверки электронных подписей;

- обеспечивает электронное взаимодействие доверенных лиц между собой, а также доверенных лиц с удостоверяющим центром.

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами. В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена. В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

1) сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

2) передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

Порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей, устанавливается удостоверяющим центром самостоятельно, если иное не установлено настоящим Федеральным законом и иными федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия

Договор об оказании услуг удостоверяющим центром, осуществляющим свою деятельность в отношении неограниченного круга лиц с использованием информационной системы общего пользования, является публичным договором.

4. ПРАВА И ОБЯЗАННОСТИ

4.1 Права и обязанности Удостоверяющего центра

Изложенные в настоящем Регламенте права и обязанностей Удостоверяющего центра, включают в себя права и обязанности, предусмотренные статьями 13 - 15, 17 и 18 Федерального закона "Об электронной подписи".

4.1.1. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

4.1.1.1. Запрашивать у заявителя документы для подтверждения сведений, представленных им при обращении в Удостоверяющий центр.

4.1.1.2. С использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных заявителем.

4.1.1.3. Запрашивать и получать из государственных информационных ресурсов:

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

4.1.1.4. Запросить у заявителя дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными заявителем, и сведениями, полученными Удостоверяющим центром в соответствии с частью 2.2 статьи 18 Федерального закона «Об электронной подписи».

4.1.1.5. Не принимать от заявителя документы, не соответствующие требованиям нормативных правовых актов Российской Федерации.

4.1.1.6. Отказать заявителю в создании / выдаче сертификата ключа проверки электронной подписи в случае:

- невыполнения заявителем обязанностей, установленных частью 2 статьи 18 Федерального закона «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами;
- 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;

- отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи.

4.1.1.7. Отказать владельцу сертификата в прекращении действия сертификата в случае, если сертификат уже аннулирован или прекратил свое действие по другим основаниям;

4.1.1.8. Без заявления владельца сертификата прекратить действие сертификата в случае наличия у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа электронной подписи владельца сертификата, а также невыполнения владельцем сертификата обязанностей, установленных законодательством Российской Федерации в области электронной подписи, а также в случае появления у Удостоверяющего центра достоверных сведений о том, что документы, представленные заявителем в целях создания и получения им сертификата, не являются действительными и/или не подтверждают достоверность всей информации, включенной в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

4.1.1.9. Приостановить действие квалифицированного сертификата в случае наличия у Удостоверяющего центра оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован, с уведомлением владельца квалифицированного сертификата и указанием обоснованных причин.

4.1.1.10. 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.

4.1.1.11. Удостоверяющий центр вправе наделить третьих лиц (далее - доверенные лица) полномочиями по вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра. При вручении сертификата ключа проверки электронной подписи доверенное лицо обязано установить личность получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата в соответствии с порядком реализации функций удостоверяющего центра и исполнения его обязанностей, установленным наделившим указанное доверенное лицо полномочиями по вручению сертификатов ключей проверки электронной подписи удостоверяющим центром с учетом предусмотренных пунктом 4 части 4 статьи 8 требований Федерального закона «Об электронной подписи».

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

4.1.1.13. Самостоятельно устанавливать порядок реализации функций Удостоверяющего центра, осуществления его прав и исполнения обязанностей, если иное не установлено Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» и иными федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия;

4.1.1.14. Выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе;

4.1.1.15. Осуществлять иную связанную с использованием электронной подписи деятельность, регламентированную Федеральным законом «Об электронной подписи» и иными законодательными документами Российской Федерации.

4.1.2. Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

4.1.2.1. информировать в письменной форме 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;

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

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

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

4.1.2.5. обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

4.1.2.6. 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;

4.1.2.7. 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;

4.1.2.8. не указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром;

4.1.2.9. использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном Удостоверяющему центру головным удостоверяющим центром, функции которого осуществляет

уполномоченный федеральный орган, для подписания от своего имени квалифицированных сертификатов;

4.1.2.10. не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном Удостоверяющему центру головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами;

4.1.2.11. хранить информацию, внесенную в реестр сертификатов в течение всего срока деятельности удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами;

4.1.2.12. хранить следующую информацию в течение срока своей деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, в форме, позволяющей проверить ее целостность и достоверность:

- 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 по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

4.1.2.13. В случае принятия решения о прекращении своей деятельности аккредитованный 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 этим аккредитованным удостоверяющим центром квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре;

В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена.

В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В

указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

4.1.2.14. Удостоверяющий центр обязан выполнять порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», и иными нормативными правовыми актами;

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

4.1.2.16. вносить информацию о сертификате ключа проверки электронной подписи в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата;

4.1.2.17. аннулировать сертификат ключа проверки электронной подписи в следующих случаях, предусмотренных частями 6 и 6.1 ст.14 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи»

4.1.2.18. вносить информацию о прекращении действия сертификата ключа проверки электронной подписи в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 ст.14 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств;

4.1.2.19. уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа до внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи;

4.2 Права и обязанности Пользователей Удостоверяющего центра

4.2.1. Права пользователей Удостоверяющего центра

Пользователи Удостоверяющего центра имеют право:

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

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

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

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

4.2.1.5. Получить доступ к актуальным спискам аннулированных сертификатов.

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

4.2.1.7. Обращаться в Удостоверяющий центр с заявлением на выпуск сертификата ключа проверки электронной подписи.

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

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

4.2.1.10. Обращаться в Удостоверяющий центр с заявлениями на прекращение действия квалифицированного сертификата, в течение срока действия сертификата.

4.2.2. Обязанности Пользователей Удостоверяющего центра

4.2.2.1. Обязанности лица, проходящего процедуру регистрации в Удостоверяющем центре

- Лицо, проходящее процедуру регистрации в Удостоверяющем центре, обязано представить регистрационную информацию в объеме, необходимом для получения услуг Удостоверяющего центра.
- Лицо, проходящее процедуру регистрации в Удостоверяющем центре, несет ответственность за достоверность предоставленной регистрационной информации.

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

- 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.
- 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.
- 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.
- 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.

- 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".
- При создании ключей электронных подписей и запросов на квалифицированный сертификат выполнять требования о соблюдении конфиденциальности информации, установленные Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
- Не использовать принадлежащий владельцу сертификата ключ электронной подписи в случае его компрометации.
- Не использовать квалифицированный сертификат, заявление, на прекращение действия которого подано в Удостоверяющий центр.

4.2.2.3. Ответственность Пользователя

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

5. ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ, В ТОМ ЧИСЛЕ ТРЕБОВАНИЯ К ДОКУМЕНТАМ, ПРЕДОСТАВЛЯЕМЫМ В УДОСТОВЕРЯЮЩИЙ ЦЕНТР В РАМКАХ ПРЕДОСТАВЛЕНИЯ УСЛУГ

Удостоверяющий центр исполняет обязанности в соответствии с порядком, установленным Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи" и принимаемыми в соответствии с ним нормативными правовыми актами.

5.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей

5.1.1. 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.

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

5.1.3. Удостоверяющий центр обязан обеспечить конфиденциальность созданных Удостоверяющим центром ключей электронных подписей.

5.1.4. 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.

5.2 Порядок создания ключей электронных подписей и ключей проверки электронных подписей

5.2.1. 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 ViPNet УЦ, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также выполняющего требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя;

5.2.2. Создание ключей электронной подписи осуществляется:

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

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

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

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

5.3 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра

Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра:

5.3.1. Плановая смена ключей электронной подписи Удостоверяющего центра и соответствующего сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется не позднее 15 месяцев с момента начала действия текущего ключа электронной подписи Удостоверяющего центра.

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

5.3.3. Информирование владельцев квалифицированных сертификатов об осуществлении плановой смены ключей электронной подписи Удостоверяющего центра осуществляется в соответствии с п.2.3. Регламента

5.3.4. Доверенными способами получения нового квалифицированного сертификата Удостоверяющего центра являются:

- на сайте уполномоченного федерального органа в области использования электронной подписи https://e-trust.gosuslugi.ru/ в реестре сертификатов
- на сайте Удостоверяющего центра http://signature.iidx.ru
- личное обращение в Удостоверяющий центр по адресу и в соответствии с графиком работы, в соответствии с п.2.2 Регламента

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

При использовании Ключа электронной подписи Удостоверяющего центра существуют различные угрозы нарушения конфиденциальности. Угроза, реализованная с использованием уязвимостей информационно-программной системы, называется атакой. Существует три основные вида угроз нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра:

- Отказ в обслуживании.
- Раскрытие информации.
- Нарушение целостности.

Для предотвращения атак на Ключ электронной подписи Удостоверяющего центра реализован изолированным режим работы программно-аппаратного комплекса Удостоверяющего центра − комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с Удостоверяющим центром. Реализованные меры защиты нацелены на предотвращение компрометации или угрозы компрометации Ключа электронной подписи Удостоверяющего центра. Компрометация или угроза компрометации Ключа электронной подписи Удостоверяющего центра является основанием полагать, что конфиденциальность Ключа электронной подписи нарушена.

Под компрометацией Ключа электронной подписи понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых Ключ электронной подписи может стать доступными несанкционированным лицам и (или) процессам.

К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь, следующие случаи нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра:

- Потеря ключевых носителей.
- Потеря ключевых носителей с их последующим обнаружением.
- Увольнение сотрудников, имевших доступ к ключевой информации.
- Нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа.
- Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.
- Нарушение печати на сейфе с ключевыми носителями.

- Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности, содержащий основание, процедуры и сроки осуществления такой смены ключей электронной подписи Удостоверяющего центра, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра:

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

5.4.2. Смена ключа электронной подписи Удостоверяющим центром осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи.

5.4.3. Одновременно со сменой ключа электронной подписи Удостоверяющего центра прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

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

5.4.5. В случае выполнения внеплановой смены ключей 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.

5.4.6. В случае выполнения внеплановой смены ключей электронной подписи Удостоверяющий центр должны быть проведены работы по внеплановой смене ключей электронных подписей Пользователей, сертификаты ключей проверки 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.

5.4.7. Информирование владельцев квалифицированных сертификатов об осуществлении внеплановой смены ключей электронной подписи Удостоверяющего центра с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра осуществляется посредством уведомления на электронную почту, указанную в сертификате пользователя, и размещения информации на официальном сайте Удостоверяющего центра: http://signature.iidx.ru После получения уведомления о факте внеплановой смены Ключей Удостоверяющего центра Владельцам сертификатов необходимо выполнить процедуру создания и выдачи новых

Сертификатов в соответствии с порядком, установленным подразделом 5.6 настоящего Регламента.

5.4.8. Доверенными способами получения нового квалифицированного сертификата Удостоверяющего центра являются:

- на сайте уполномоченного федерального органа в области использования электронной подписи https://e-trust.gosuslugi.ru/ в реестре сертификатов
- на сайте Удостоверяющего центра http://signature.iidx.ru
- личное обращение в Удостоверяющий центр по адресу и в соответствии с графиком работы, в соответствии с п.2.2 Регламента

5.5 Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата

5.5.1. смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона "Об электронной подписи":

- 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 иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи 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.

5.5.2. требования к заявлению на смену ключа электронной подписи владельца квалифицированного сертификата, в том числе состав реквизитов такого заявления, указаны в Приложениях 1, 2, 5, 6 настоящего Регламента;

5.5.3. заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца квалифицированного сертификата, при этом в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата;

5.5.4. процедура выдачи квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, в том числе в электронной форме в соответствии со статьей 18 Федерального закона "Об электронной подписи";

5.5.5. Создание новых 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".

5.5.6. Запрос на сертификат, сформированный с использованием средства электронной подписи, установленного 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.

5.5.7. 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.

5.5.8. 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.

5.5.9. Создание квалифицированного сертификата для вновь сформированного ключа проверки электронной подписи Пользователя осуществляется Удостоверяющим центром не позднее 3 (трёх) рабочих дней, следующих за рабочим днем, в течение которого Удостоверяющим центром был получен запрос на квалифицированный сертификат.

5.6 Процедура создания и выдачи квалифицированных сертификатов

5.6.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

Заявление на создание и выдачу квалифицированных сертификатов может быть подано путем подачи в Удостоверяющий центр **заявления** в форме документа, 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.

Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью;

5.6.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

Создание квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявления на услуги удостоверяющего центра, содержащего регистрационные данные Заявителя, включая информацию, подлежащую внесению в квалифицированный сертификат в соответствии с Федеральным законом "Об электронной подписи".

Заявление на создание и выдачу квалифицированного сертификата оформляется в соответствии с приложениями №5 и №6.

Заявление на услуги Удостоверяющего центра может быть подано в форме документа, 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. Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью;

5.6.3. Порядок установления личности заявителя с указанием следующих положений в соответствии со статьей 18 Федерального закона "Об электронной подписи"

В соответствии со статьей 18 Федерального закона "Об электронной подписи", при выдаче квалифицированного сертификата аккредитованный Удостоверяющий центр устанавливает личность заявителя - физического лица, обратившегося за получением квалифицированного сертификата, по основному документу, удостоверяющему личность. При этом:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, Удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
- личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

5.6.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя, в соответствии с частью 2 статьи 17 и частью 2 статьи 18 Федерального закона N 63-ФЗ

Для получения квалифицированного сертификата Пользователь, в соответствии с требованиями п.2 Статьи 17 и п.2 Статьи 18 Федерального закона от 06.04.2011 №63-ФЗ "Об электронной подписи", представляет в Пункт регистрации Удостоверяющего центра следующие документы либо их надлежащим образом заверенные копии и сведения:

1) основной документ, удостоверяющий личность;

2) номер страхового свидетельства государственного пенсионного страхования заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица;

4) основной государственный регистрационный номер заявителя - юридического лица;

5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;

6) номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

7) доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц.

5.6.5. Порядок проверки достоверности документов и сведений, представленных заявителем

Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона "Об электронной подписи".

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона "Об электронной подписи" Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов:

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

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и Удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата;

5.6.6. Порядок создания квалифицированного сертификата

Квалифицированный сертификат подлежит созданию с использованием средств аккредитованного удостоверяющего центра.

Квалифицированный сертификат должен содержать следующую информацию:

1) уникальный номер квалифицированного сертификата, даты начала и окончания его действия;

2) фамилия, имя, отчество (если имеется) владельца квалифицированного сертификата - для физического лица, не являющегося индивидуальным предпринимателем, либо фамилия, имя, отчество (если имеется) и основной государственный регистрационный номер индивидуального предпринимателя - владельца квалифицированного сертификата - для физического лица, являющегося индивидуальным предпринимателем, либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для российского юридического лица, либо наименование, место нахождения владельца квалифицированного сертификата, а также идентификационный номер налогоплательщика (при наличии) - для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);

3) страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;

4) уникальный ключ проверки электронной подписи;

5) наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;

6) наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;

7) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);

Если заявителем представлены в аккредитованный удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат может быть включена информация о таких правомочиях заявителя и сроке их действия.

5.6.7. Порядок выдачи квалифицированного сертификата

Процедура выдачи квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, в том числе в электронной форме, производится в соответствии со статьей 18 Федерального закона "Об электронной подписи".

Полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона «Об электронной подписи».

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр:

- устанавливает личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;
- получает от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

При обращении в аккредитованный удостоверяющий центр заявитель указывает на ограничения использования квалифицированного сертификата (если такие ограничения им устанавливаются) и представляет следующие документы либо их надлежащим образом заверенные копии и сведения:

1) основной документ, удостоверяющий личность;

2) номер страхового свидетельства государственного пенсионного страхования заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица;

4) основной государственный регистрационный номер заявителя - юридического лица;

5) основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;

6) номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

7) доверенность или иной документ, подтверждающий право заявителя действовать от имени других лиц.

Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 4 - 6 части 2 статьи 18 Федерального закона «Об электронной подписи».

Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем, а также запрашивает и получает информацию из государственных информационных ресурсов в соответствии с частями 2 и 2.1 статьи 18 и частью 2 статьи 17 Федерального закона «Об электронной подписи» и п.5.2.5 Регламента.

В случае, если полученные сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и Удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица,

на обращение за получением квалифицированного сертификата, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае аккредитованный удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

При получении квалифицированного сертификата заявителем он под расписку ознакамливается Удостоверяющим центром с информацией, содержащейся в квалифицированном сертификате.

Удостоверяющий центр одновременно с выдачей квалифицированного сертификата выдает владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 8 к настоящему Регламенту).

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра). При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

5.6.8. Срок создания и выдачи квалифицированного сертификата

Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром соответствующего заявления, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю:

5.6.8.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром не позднее 3 (трех) рабочих дней с момента получения Удостоверяющим центром соответствующей заявки, в том числе и в форме запроса на сертификат.

5.6.8.2. Условием для срочного создания и выдачи квалифицированного сертификата заявителю является информирование удостоверяющего центра заявителем о необходимости срочного создания и выдачи квалифицированного сертификата в любой форме (письменно или устно). В случае срочного создания и выдачи квалифицированного сертификата заявителю создание и выдача осуществляется в день обращения (рабочий день).

5.7 Подтверждение действительности электронной подписи, использованной для подписания электронных документов

5.7.1. Требования к заявлению на подтверждение действительности электронной подписи, в том числе перечень прилагаемых к такому заявлению документов

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.

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

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

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.

5.7.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе

Срок проведения работ по подтверждению действительности электронной подписи в электронном документе составляет 3 (три) рабочих дня с момента поступления заявления в Удостоверяющий центр.

5.7.3. Порядок оказания услуги

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

Подтверждение действительности электронной подписи в электронном документе включает в себя проверку действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата аккредитованного удостоверяющего центра, выданного ему головным удостоверяющим центром

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, 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).

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.

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

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

5.8 Подтверждение действительности электронной подписи Удостоверяющего центра в выданных квалифицированных сертификатах

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

Обязательным приложением к заявлению на подтверждение действительности 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).

Срок проведения работ по подтверждению действительности электронной подписи Удостоверяющего центра в выданном Удостоверяющим центром квалифицированном сертификате и предоставлению заключения о произведенной проверке составляет 3 (три) рабочих дня с момента поступления в Удостоверяющий центр заявления пользователя на подтверждение действительности электронной подписи Удостоверяющего центра в выданном им квалифицированном сертификате.

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

5.9 Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата

5.9.1. Основания прекращения действия или аннулирования квалифицированного сертификата

Квалифицированный сертификат прекращает свое действие в случаях, установленных статьей 14 Федерального закона "Об электронной подписи", а именно:

- 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 настоящим Федеральным законом, другими федеральными законами, принимаемыми в соответствии с ними нормативными

правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи 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.

5.9.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалифицированного сертификата

5.9.2.1. 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.

5.9.2.2. 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.

5.9.2.3. Информация 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 частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов

5.9.2.4. Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием. 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.

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

5.10 Порядок ведения реестра квалифицированных сертификатов

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

Удостоверяющий центр ведет реестр выданных и аннулированных Удостоверяющим центром квалифицированных сертификатов ключей проверки электронных подписей, в том числе включающего в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей, а также об основаниях прекращения действия или аннулирования сертификатов.

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

Удостоверяющий центр обеспечивает любому лицу к информации, содержащейся в реестре сертификатов в любое время, за исключением периодов планового или внепланового технического обслуживания, доступ с использованием информационно-телекоммуникационных сетей общего пользования.

5.10.1. Формы ведения реестра квалифицированных сертификатов

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, а также иную информацию, подлежащую включению в реестр в соответствии с требованиями нормативных правовых документов.

5.10.2. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов

Информация 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 части 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

5.11 Порядок технического обслуживания реестра квалифицированных сертификатов

Удостоверяющий центр обеспечивает любому лицу в любое время, за исключением периодов планового или внепланового технического обслуживания, доступ с использованием информационно-телекоммуникационных сетей общего пользования к реестру сертификатов.

5.11.1. Максимальные сроки проведения технического обслуживания

Максимальные сроки проведения технического обслуживания составляет 3 (три) рабочих дня.

5.11.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

Уведомление участников информационного взаимодействия о проведении технического обслуживания осуществляется посредством размещения информации на сайте Удостоверяющего центра по адресу http://signature.iidx.ru.

6. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Порядок исполнения обязанностей Удостоверяющего центра, установлен Федеральным законом от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи" и принимаемыми в соответствии с ним нормативными правовыми актами.

6.1 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

В соответствии с частью 4 Статьи 18 Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» Удостоверяющий центр одновременно с выдачей квалифицированного сертификата выдает владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи. Данное руководство является средством официального информирования об условиях, рисках и порядке использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи и их проверки.

Также с данным руководством заявитель может ознакомиться в порядке, описанном в п.2.3 настоящего Регламента и в Приложении 8 к настоящему Регламенту.

6.2 Выдача по обращению заявителя средств электронной подписи

Удостоверяющий центр выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи.

Также Удостоверяющий центр выдает заявителю инструкцию, позволяющую установить на своем рабочем месте средство электронной подписи ViPNet CSP (распространяется разработчиком с помощью информационно-телекоммуникационной сети интернет). Данное средство электронной подписи в соответствии с частью 4 статьи 6 Федерального закона "Об электронной подписи" обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями;

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

В соответствии с требованиями п.2 части 2 Статьи 13 Федерального закона от 06.04.2011 №63-ФЗ "Об электронной подписи" Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также выполняет комплекс организационно-технических мероприятий по защите ключей электронных подписей Удостоверяющего центра и Пользователей, а также информационных ресурсов Удостоверяющего центра, включающих, в частности, информацию, содержащуюся в реестре сертификатов, от неправомерного доступа, уничтожения, уничтожения, модификации, блокирования, иных неправомерных действий;

6.4 Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети "Интернет" в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов

Согласно части 3 статьи 15 Федерального закона «Об электронной подписи», Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к реестру квалифицированных сертификатов Удостоверяющего центра в любое время, в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

Для получения доступа к реестру квалифицированных сертификатов лицо, желающее получить такой доступ, может обратиться в порядке, описанном в п. 2.3 Регламента.

Также реестр квалифицированных сертификатов опубликован на сайте Удостоверяющий центра http://signature.iidx.ru.

6.5 Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Конфиденциальность Ключей ЭП обеспечивается за счёт генерации Ключей ЭП на автоматизированном рабочем месте, аттестованном на соответствие требованиям по технической защите конфиденциальной информации, размещенном в помещении Удостоверяющего центра, доступ в которое ограничен, на отчуждаемый сертифицированный защищённый ключевой носитель.

Хранение ключей электронных подписей осуществляется в сейфе, расположенном в аттестованном помещении. Доступ к сейфу и помещению ограничен.

Ключи на ключевых носителях, срок действия которых истёк, уничтожаются путём переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

6.6 Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи"

В соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи" Удостоверяющий центр при выдаче квалифицированного сертификата направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

6.7 Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации

В соответствии с частью 5 статьи 18 Федерального закона "Об электронной подписи" Удостоверяющий центр при выдаче квалифицированного сертификата по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

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).

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.

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.

6.8 Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов

В соответствии с требованием пункта 3 Части 2 Статьи 13 Федерального закона «Об электронной подписи» Удостоверяющий центр безвозмездно предоставляет по обращению любому лицу информацию, содержащуюся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата.

Для получения доступа к реестру квалифицированных сертификатов лицо, желающее получить такой доступ, может обратиться в порядке, описанном в п. 2.3 Регламента.

Также Удостоверяющий центр публикует перечень прекративших свое действие (аннулированных) квалифицированных сертификатов на сайте http://signature.iidx.ru.

.

7. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

7.1 Виды конфиденциальной информации

7.1.1. Ключ электронной подписи владельца квалифицированного сертификата.

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

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

7.2 Виды информации, не относящейся к конфиденциальной

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

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

7.1.6. Информация, включаемая в создаваемые Удостоверяющим центром квалифицированные сертификаты и списки аннулированных сертификатов, не считается конфиденциальной.

7.1.7. Также не считается конфиденциальной информация о настоящем Регламенте.

7.3 Предоставление конфиденциальной информации

7.1.8. 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 законодательством РФ или при наличии судебного постановления.

8. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

8.1. 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 и дата выдачи основного документа, удостоверяющего личность.
- Пол.
- Дата и место рождения.

8.2. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица на обработку Удостоверяющим центром его персональных данных, перечисленных в пункте 8.1 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.

8.3. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица на поручение Удостоверяющим центром обработки его персональных данных, перечисленных в пункте 8.1 настоящего Регламента, другому лицу в целях проверки регистрационных данных Пользователя и вручения квалифицированного сертификата ключа проверки электронной подписи его владельцу.

8.4. Присоединение Заявителя - физического лица к настоящему Регламенту означает согласие этого физического лица, с тем, что его персональные данные, включаемые Удостоверяющим центром в реестр квалифицированных сертификатов ключей проверки электронных подписей, а также в создаваемый на его имя квалифицированный сертификат

ключа проверки электронной подписи, относятся к общедоступным персональным данным. К таким персональным данным, в соответствии с требованиями, установленными в соответствии с Федеральным законом "Об 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.

8.5. 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.

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

- персональные данные, перечисленные в пункте 8.1. 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 8.2 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 8.4 настоящего Регламента, относятся к общедоступным персональным данным.

9. 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 части 2 статьи 17 Федерального закона "Об электронной подписи", кквалифицированный сертификат должен содержать следующую информацию:

- уникальный номер квалифицированного сертификата, даты начала и окончания его действия;
- фамилия, имя, отчество (если имеется) владельца квалифицированного сертификата - для физического лица, не являющегося индивидуальным предпринимателем, либо фамилия, имя, отчество (если имеется) и основной государственный регистрационный номер индивидуального предпринимателя - владельца квалифицированного сертификата - для физического лица, являющегося индивидуальным предпринимателем, либо наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата - для российского юридического лица, либо наименование, место нахождения владельца квалифицированного сертификата, а также идентификационный номер налогоплательщика (при наличии) - для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);
- страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица либо идентификационный номер налогоплательщика владельца квалифицированного сертификата - для юридического лица;
- уникальный ключ проверки электронной подписи;
- наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с настоящим Федеральным законом;
- наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат, номер квалифицированного сертификата удостоверяющего центра;
- ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются);
- Операторы государственных и муниципальных информационных систем, а также информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования не вправе требовать наличие в квалифицированном сертификате информации, ограничивающей его применение в иных информационных системах;
- Если заявителем представлены в аккредитованный удостоверяющий центр документы, подтверждающие его право действовать от имени третьих лиц, в квалифицированный сертификат может быть включена информация о таких правомочиях заявителя и сроке их действия;

- Квалифицированный сертификат выдается в форме, требования к которой устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности по согласованию с уполномоченным федеральным органом.

10.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".

11.РАЗРЕШЕНИЕ СПОРОВ

11.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту, в том числе, Пользователь.

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

11.3. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов, которые могут возникнуть в рамках действия настоящего Регламента, решить их, прежде всего, путем совместных переговоров и в претензионном порядке.

11.4. 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.

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, не урегулированные в процессе совместных переговоров и в претензионном порядке, разрешаются в Арбитражном суде в соответствии с законодательством РФ по месту нахождения ООО «Системы управления идентификацией».

12.ОСНОВЫ ДЕЯТЕЛЬНОСТИ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

12.1. Удостоверяющий центр осуществляет свою деятельность на основании разрешительных документов на осуществление всех видов деятельности, связанных с предоставлением услуг Удостоверяющего центра.

12.2. Удостоверяющий центр обеспечивает выполнение мер по защите информации, в соответствии с требованиями о соблюдении конфиденциальности информации, установленными Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

12.3. 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".

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

13.ПОРЯДОК УТВЕРЖДЕНИЯ И ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РЕГЛАМЕНТ

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

13.2. 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 2.3. настоящего Регламента.

13.3. 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.

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

13.5. Уведомление пользователей о внесении изменений в Регламент осуществляется путем публикации актуальной версии Регламента в электронном виде на сайте ООО «Системы управления идентификацией» по адресу https://signature.iidx.ru/.

14.ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

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

В случае принятия решения о прекращении своей деятельности Удостоверяющий центр, в соответствии с частью 4 статьи 15 Федерального закона «Об электронной подписи» 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 (Приказ Минкомсвязи России от 14.08.2017 N 416 "Об утверждении Порядка передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра" (Зарегистрировано в Минюсте России 11.09.2017 N 48141) реестр выданных Удостоверяющим центром квалифицированных сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.
- В случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам он обязан уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена.

В случае прекращения деятельности Удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы Удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности Удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции Удостоверяющего центра, прекратившего свою деятельность.

15.ПРИЛОЖЕНИЯ

Приложение 1. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи (для юридических лиц).

Приложение 2. Форма заявления на прекращение действия сертификата ключа проверки электронной подписи (для физических лиц).

Приложение 3. Форма заявления на подтверждение действительности электронной подписи Удостоверяющего центра в сертификате пользователя (для юридических лиц).

Приложение 4. Форма заявления на подтверждение действительности электронной подписи Удостоверяющего центра в сертификате пользователя (для физических лиц).

Приложение 5. Форма заявления на присоединении к Регламенту Удостоверяющего центра ООО «СУИ» и на выпуск сертификат ключа проверки электронной подписи (для юридических лиц).

Приложение 6. Форма заявления на присоединении к Регламенту Удостоверяющего центра ООО «СУИ» и на выпуск сертификат ключа проверки электронной подписи (для физических лиц).

Приложение 7. Акт приема-передачи сертификата ключа проверки электронной подписи.

Приложение 8. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Приложение 1
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией» ООО

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

Прошу прекратить действие выданного Удостоверяющим центром ООО «Системы управления идентификацией» 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
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

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

Прошу прекратить действие выданного Удостоверяющим центром ООО «Системы управления идентификацией» 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 3
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией» услуг
по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

Заявление
на подтверждение подлинности электронной подписи Удостоверяющего центра ООО «Системы управления идентификацией» в сертификате ключа проверки электронной подписи
(для юридических лиц)

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(наименование занимаемой должности)

_____
(фамилия, имя, отчество)

действующего на основании _____

просит подтвердить подлинность электронной подписи Удостоверяющего центра ООО «Системы управления идентификацией» в выданном Удостоверяющим центром сертификате ключа проверки электронной подписи и установить его статус (действует / не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе информации.
2. Время и дата, на момент наступления которых требуется установить статус сертификата*:
   « _____ : _____ » « _____ / _____ / _____ »
   час минута день месяц год

_____	_____	_____
(наименование должности руководителя организации)	(подпись)	(фамилия, инициалы руководителя организации)

"____" _____ 20__г. М.П.

* Время и дата должны быть указаны с учетом часового пояса г. Москва (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи заявления в Удостоверяющий центр.

Приложение 4
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией» услуг
по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

Заявление
на подтверждение подлинности электронной подписи Удостоверяющего центра ОАО
ООО «Системы управления идентификацией» в сертификате ключа проверки
электронной подписи
(для физических лиц)

_____
(фамилия, имя, отчество)

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

просит подтвердить подлинность электронной подписи Удостоверяющего центра ООО «Системы управления идентификацией» в выданном Удостоверяющим центром сертификате ключа проверки электронной подписи и установить его статус (действует / не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе информации.
2. Время и дата, на момент наступления которых требуется установить статус сертификата*:
   « _____ : _____ » « _____ / _____ / _____ »
   час минута день месяц год

_____ _____
(подпись) (фамилия, инициалы)

"____" _____ 20__г.

* Время и дата должны быть указаны с учетом часового пояса г. Москва (по Московскому времени). Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи заявления в Удостоверяющий центр.

Приложение 5
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

Заявление
на присоединении к Регламенту Удостоверяющего центра ООО «СУИ»
и на выпуск сертификата ключа проверки электронной подписи
(для юридических лиц)

_____
(наименование организации)
В лице_____

действующего на основании _____
Просит зарегистрировать уполномоченного представителя
_____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

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

Общее имя (ФИО)	
Должность	
СНИЛС*	
ИНН**	
Организация	
Наименование подразделения***	
E-Mail	
Страна (C)	
Регион (S)	
Населенный пункт (L)	
Адрес местонахождения (STREET)	
ОГРН****	
ОГРН(ИП)*****	
Область применения сертификата	

* указывается СНИЛС пользователя Удостоверяющего центра.
** Указывается ИНН организации (12 цифр: для юр. лиц дополняется двумя лидирующими нулями.
*** указывается подразделение в котором работает должностное лицо на которое выдается ключ (при наличии).
**** указывается ОГРН юр. лица.
***** указывается ОГРН индивидуального предпренимателя.

Подпись уполномоченного представителя организации _____/_____/

«____» _____ 20____ г.

Должность и ФИО руководителя организации

Подпись руководителя организации, дата подписания заявления

Печать организации

В соответствии со ст. 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре ООО «СУИ», в т.ч. его регистрационных отделениях, своих персональных данных, указанных в настоящем заявлении, а также в других документах, в целях идентификации и аутентификации меня в качестве Пользователя УЦ и информационных систем с применением электронной подписи, в т.ч. для направления в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Я согласен с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом Удостоверяющего центра ООО «СУИ».

Я согласен(на), что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

С Регламентом Удостоверяющего центра ООО «СУИ», расположенным на сайте http://iidx.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате. 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, опубликованных на сайте аккредитованного Удостоверяющего центра ООО «СУИ» по адресу http://iidx.ru infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

«____» _____ 20____ г. _____ _____

(Подпись) (ФИО)

Приложение 6
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

Заявление
на присоединении к Регламенту Удостоверяющего центра ООО «СУИ»
и на выпуск сертификата ключа проверки электронной подписи (для физических лиц)

Я, _____
(Фамилия, имя, отчество полностью)
Паспорт серии_____№_____выдан_____года_____
_____
(наименование органа, выдавшего документ)

Прошу изготовить сертификат ключа проверки электронной подписи в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 №63-ФЗ "Об электронной подписи" в Единой системе идентификации и аутентификации на основании следующих данных:

Общее имя (ФИО)	
СНИЛС*	
ИНН**	
E-Mail	
Страна (C)	
Регион (S)	
Населенный пункт (L)	
Адрес местонахождения (STREET)	
Область применения сертификата	

* указывается адрес по прописке (наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения)

«____» _____ 20____ г. _____ _____
(Подпись) (ФИО)

В соответствии со ст. 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре ООО «СУИ», в т.ч. его регистрационных отделениях, своих персональных данных, указанных в настоящем заявлении, а также в других документах, в целях идентификации и аутентификации меня в качестве

Пользователя УЦ и информационных систем с применением электронной подписи, в т.ч. для направления в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Я согласен с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом Удостоверяющего центра ООО «СУИ».

Я согласен(на), что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

С Регламентом Удостоверяющего центра ООО «СУИ», расположенным на сайте http://iidx.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате. 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, опубликованных на сайте аккредитованного Удостоверяющего центра ООО «СУИ» по адресу http://iidx.ru infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

«____» _____ 20____ г. _____ _____

(Подпись) (ФИО)

Приложение 7
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

В Удостоверяющий Центр
ООО «Системы управления идентификацией»

А К Т
приема-передачи сертификата ключа проверки электронной подписи

Удостоверяющий центр ООО «СУИ» изготовил сертификат ключа проверки электронной подписи_____
___
(серийный номер сертификата)
И передал _____
(Фамилия, имя, отчество полностью)
_____
___

в рамках оказания услуги удостоверяющего центра, определенные Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Я ознакомился(ась) с информацией, содержащейся в квалифицированном сертификате.

«____» _____ 20____ г. _____ _____
(Подпись) (ФИО)

Приложение 8
к Регламенту оказания Удостоверяющим центром
ООО «Системы управления идентификацией»
услуг по созданию и выдаче квалифицированных
сертификатов ключей проверки электронных
подписей

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

1. Общие положения

1.1. Настоящее руководство разработано в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» и предназначено для лиц, заинтересованных в получении или владеющих квалифицированным сертификатом ключа проверки электронной подписи, создаваемым ООО «Системы управления идентификацией» (далее – Удостоверяющий центр),

1.2. Руководство является средством официального информирования об условиях, рисках и порядке использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (далее – средства ЭП), а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

1.3. Применение квалифицированной электронной подписи в государственных и иных информационных системах, а также в системах юридически значимого электронного документооборота, сопровождаются, в том числе следующими рисками:

1) финансовые убытки (в том числе штрафы и т.п.);

2) репутационные риски;

3) нарушение сроков оказания государственных и муниципальных услуг;

4) нарушение правильного функционирования информационных систем.

1.4. Риски, связанные с применение квалифицированной электронной подписи, возникают вследствие возможности признания недействительности сделок, совершенных с использованием квалифицированной электронной подписи, недействительности документов, подписанных квалифицированной электронной подписью при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка квалифицированной электронной подписи.

1.5. В целях снижения рисков необходимо выполнение приведенных в настоящем руководстве организационно-технических и административных мер по обеспечению безопасного функционирования средств обработки и передачи информации.

1.6. В соответствии с правилами функционирования информационных системах и систем обмена электронными документами, а также требованиями по эксплуатации средств ЭП могут быть установлены дополнительные требования по обеспечению их безопасной эксплуатации.

2. Требования к организация режима обеспечения безопасности помещений, в которых эксплуатируются средства квалифицированной электронной подписи

2.1. При эксплуатации средств ЭП должны быть реализованы меры, препятствующие возможности неконтролируемого проникновения или пребывания в помещениях, где размещены (или хранятся) используемые средства ЭП и (или) носители ключевой, аутентифицирующей и парольной информации средств ЭП (далее - Помещения), лиц, не имеющих права доступа в Помещения. Указанные меры могут быть реализованы, в том числе, путем:

а) оснащения Помещений входными дверьми с замками, обеспечения закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений;

б) утверждения правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждения перечня лиц, имеющих право доступа в Помещения.

2.2. В случае необходимости присутствия посторонних лиц в Помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства обработки информации и передаваемую информацию.

2.3. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им документов и сведений, включая ключи электронной подписи.

3. Требования по защите информации от несанкционированного доступа средств квалифицированной электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств ЭП должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в операционную систему, BIOS и т.д.) в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- личный пароль пользователь не должен никому сообщать;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

- не использовать нестандартные, измененные или отладочные версии операционных систем;

- исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

- на средствах вычислительной техники с установленными средствами ЭП должна быть установлена только одна операционная система;

- все неиспользуемые сетевые компоненты системы необходимо отключить (протоколы, сервисы и т.п.);

- режимы безопасности, реализованные в операционной системе, должны быть настроены на максимальный уровень;

- всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

- системному реестру;
- файлам и каталогам;
- временным файлам;
- журналам системы;
- файлам подкачки;
- кэшируемой информации (пароли и т.п.);
- отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

- организовать стирание (по окончании сеанса работы средств электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их

работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

- исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

- регулярно устанавливать пакеты обновлений безопасности операционной системы, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

3.1.4. В случае подключения технических средств с установленными средствами ЭП к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных с ресурсов или с использованием общедоступных сетей передачи данных (в т.ч. Интернет), без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства ЭП и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

3.1.5. Необходимо организовать и использовать:

- систему аудита, организовать регулярный анализ результатов аудита.

- комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

- осуществлять несанкционированное копирование ключевых носителей;

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

- использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

- вносить какие-либо изменения в программное обеспечение средств ЭП;

- записывать на ключевые носители постороннюю информацию;

- оставлять средства вычислительной техники с установленными средствами ЭП без контроля после ввода ключевой информации;

- использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи

Ключи квалифицированной электронной подписи при их создании должны записываться на типы ключевых носителей, которые поддерживаются используемым средством ЭП согласно технической и эксплуатационной документации к ним. Ключи квалифицированной электронной подписи на ключевом носителе должны быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру создания ключей, в соответствии с требованиями на используемое средство ЭП. Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями

Недопустимо пересылать файлы с ключевой информацией для работы в системах обмена электронными документами, по электронной почте сети Интернет или по внутренней электронной почте (кроме файлов квалифицированных сертификатов ключей проверки электронной подписи). Ключевая информация должна размещаться на сменном носителе информации (USBflash накопитель, Рутокен и др.). Размещение ключевой информации в реестре Windows, на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами ЭП, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками. Носители ключевой информации должны использоваться только их владельцем либо уполномоченным лицом на использование данного носителя, и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.). Носитель ключевой информации должен подключаться в считывающее устройство только на время выполнения средствами электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами. На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности средств вычислительной техники с установленными средствами ЭП С целью контроля исходящего и входящего подозрительного трафика, средства вычислительной техники с установленными средствами ЭП должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку во внешние сети информации, инициированную программами, не имеющими соответствующих полномочий. На технических средствах, используемых для работы в системах обмена электронными документами:

- на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям безопасности;

- должно быть установлено только лицензионное программное обеспечение;

- должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

- должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

- должны регулярно устанавливаться обновления операционной системы;

- должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами ЭП третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

- должна быть активирована подсистема регистрации событий информационной безопасности;

- должна быть включена автоматическая блокировка экрана после ухода ответственного сотрудника с рабочего места.

Если в качестве автоматизированного рабочего места для работы в системах обмена электронными документами выбран переносной компьютер, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации. В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства ЭП, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства ЭП, журналы работы систем обмена электронными документами и т.д.).

5. Действия при компрометации ключей квалифицированной электронной подписи

5.1. К событиям, относящимся к компрометации ключей квалифицированной электронной подписи, относятся следующие ситуации:

1) ознакомление неуполномоченного лица (лиц) с ключами квалифицированной электронной подписи;

2) утрата ключевого носителя с ключами квалифицированной электронной подписи;

3) увольнение пользователя ключа квалифицированной электронной подписи;

4) нарушение целостности печатей на сейфах (шкафах, хранилищах), предназначенных для хранения ключевых носителей;

5) утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей;

6) случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника, утрата ключевого носителя с последующим обнаружением).

5.2. В случае компрометации ключей квалифицированной электронной подписи владелец квалифицированного сертификата ключа проверки электронной подписи должен:

1) прекратить использование ключа квалифицированной электронной подписи и соответствующего квалифицированного сертификата ключа проверки электронной подписи;

2) незамедлительно обратиться в Удостоверяющий центр для аннулирования (прекращения действия) соответствующего квалифицированного сертификата ключа проверки электронной подписи и получения (при необходимости) нового квалифицированного сертификата ключа проверки электронной подписи в соответствии с Регламентом оказания услуг Удостоверяющего центра