УТВЕРЖДЕН

Приказом ООО «Модум»

от «11» июля 2019 г.

№ 11

Порядок реализации функций

Аккредитованного Удостоверяющего центра

и исполнения его обязанностей

ООО «Модум»

Москва, 2019 г.

Содержание

1. Введение.

1.1. Порядок реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум» и исполнения его обязанностей (далее – Порядок, Удостоверяющий центр) определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, а также права, обязанности и ответственность лиц, присоединившихся к Порядку.

1.2. Настоящий Порядок разработан в соответствии с:

Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ;

Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года № 149-ФЗ;

Федеральным законом «О персональных данных» от 27.07.2006 года № 152-ФЗ;

Федеральным законом «О связи» от 07.07.2003 года № 126-ФЗ;

Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 года № 210-ФЗ;

Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012 года № 79;

Требованиями к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27.12.2011 года № 796;

Требованиями к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27.12. 2011 года № 795;

Требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Минкомсвязи России от 13.08.2018 года № 397;

Порядком 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, утвержденным приказом Минкомсвязи России от 14.08.2017 года № 416;

Порядком формирования и ведения реестров, выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22.08.2017 года № 436;

Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты

информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.07. 2001 года № 152 (далее – Инструкция ФАПСИ № 152);

Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ - 2005), утвержденным приказом ФСБ России 09.02.2005 года № 66;

Нормативными правовыми актами, регулирующими отношения в области информационных технологий, защиты информации и использования электронных подписей, в том числе методическим и руководящим документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) в области защиты информации.

1.3. В настоящем Порядке используются следующие термины и понятия:

Администратор Удостоверяющего центра (далее – Администратор УЦ) – уполномоченное лицо Удостоверяющего центра, являющееся сотрудником общества с ограниченной ответственностью «Модум», наделенное полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, квалифицированных сертификатов ключей проверки электронной подписи (далее – квалифицированный сертификат), управлению и обслуживанию квалифицированных сертификатов, выданных Удостоверяющим центром, полномочиями по заверению копий сертификатов ключей проверки электронной подписи на бумажном носителе, администрированию и обслуживанию средств Удостоверяющего центра, а также иными полномочиями согласно настоящему Порядку;

заявитель – лицо, обратившееся в Удостоверяющий центр для получения квалифицированного сертификата или для получения иных услуг Удостоверяющего центра;

квалифицированный сертификат ключа проверки электронной подписи Удостоверяющего центра (далее – квалифицированный сертификат УЦ) – квалифицированный сертификат, выданный Удостоверяющему центру головным удостоверяющим центром федерального органа исполнительной власти, уполномоченным в сфере использования электронной подписи (далее соответственно – головной удостоверяющий центр, уполномоченный федеральный орган), и использующийся для проверки подлинности усиленной квалифицированной электронной подписи (далее – электронная подпись) Удостоверяющего центра в созданных им квалифицированных сертификатах и списках отозванных сертификатов;

ключ электронной подписи Удостоверяющего центра – ключ электронной подписи, использующийся Удостоверяющим центром для создания квалифицированных сертификатов и списков отозванных сертификатов;

копия сертификата ключа проверки электронной подписи (далее – копия сертификата) – документ на бумажном носителе, подписанный собственноручной подписью уполномоченным на это действие сотрудником Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Содержательная часть копии сертификата ключа проверки электронной подписи на бумажном носителе соответствует содержательной части квалифицированного сертификата, выданного в форме электронного документа;

Оператор Удостоверяющего центра (далее – Оператор УЦ) – уполномоченное лицо Удостоверяющего центра, являющееся работником общества с ограниченной ответственностью «Модум», наделенное полномочиями по созданию ключей электронной подписи, ключей проверки электронной подписи, квалифицированных сертификатов, обслуживанию квалифицированных сертификатов, выданных Удостоверяющим центром, а также полномочиями по заверению копий сертификатов на бумажном носителе, выданных Удостоверяющим центром;

Пользователь Удостоверяющего центра (далее – Пользователь УЦ) – лицо, прошедшее процедуру регистрации в Удостоверяющем центре, сведения о котором включены в реестр пользователей Удостоверяющего центра, в том числе владелец квалифицированного сертификата (далее – владелец сертификата);

список отозванных сертификатов – электронный документ с электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров квалифицированных сертификатов, которые на этот определенный момент времени аннулированы или действие которых было прекращено;

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.

Иные понятия и термины, используемые в настоящем Порядке, применяются в значениях, определенных федеральными законами «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О связи», «Об организации предоставления государственных и муниципальных услуг» и принимаемыми в соответствии с ними нормативными правовыми актами.

2. Общие положения.

2.1. Предмет регулирования Порядка.

2.1.1. Предметом регулирования Порядка являются отношения в области использования электронных подписей, возникающие между Удостоверяющим центром и участниками электронного взаимодействия при оказании услуг Удостоверяющего центра, реализации его функций и исполнении обязанностей.

2.1.2. Настоящий Порядок является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

2.1.3. Сторонами настоящего Порядка является Удостоверяющий центр и лица, присоединившиеся к Порядку.

2.1.4. Настоящий Порядок является средством официального уведомления и информирования всех Сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра.

2.1.5. Публикация и распространение настоящего Порядка.

Настоящий Порядок распространяется:

в форме электронного документа путем размещения на сайте Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет) по адресу http://modum.pro;

в форме документа на бумажном носителе по адресу: 105082, г. Москва, ул. Большая Почтовая, 36 стр. 1, этаж 2, комната 6,6Б.

2.1.6. Присоединение к настоящему Порядку.

2.1.6.1 Присоединение к настоящему Порядку осуществляется путем предоставления в Удостоверяющий центр заявления о присоединении к Порядку по форме приложения № 1 или приложения № 2 к настоящему Порядку.

2.1.6.2. С момента регистрации заявления о присоединении к Порядку в Удостоверяющем центре заявитель считается Стороной, присоединившийся к Порядку.

2.1.6.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации заявления о присоединении к Порядку в случае ненадлежащего оформления заявителем документов, необходимых для оказания услуг, предоставления неактуальных документов или сведений, предоставления их не в полном объеме или предоставления заявителем не достоверных сведений.

2.1.6.4. Факт присоединения заявителя к Порядку является полным принятием им условий настоящего Порядка и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении Порядку в Удостоверяющем центре. Сторона, присоединившаяся к Порядку, принимает дальнейшие изменения (дополнения), вносимые в Порядок, в соответствии с условиями настоящего Порядка.

2.1.6.5. После присоединения к Порядку Удостоверяющий центр и Сторона, присоединившаяся к Порядку, вступают в соответствующие договорные отношения.

2.1.7. Порядок прекращения присоединения к настоящему Порядку.

2.1.7.1. Действие настоящего Порядка может быть прекращено по инициативе одной из Сторон в следующих случаях:

волеизъявления одной из Сторон;

нарушения одной из Сторон условий настоящего Порядка.

2.1.7.2. В случае, если договорные отношения, определенные настоящим Порядком, прекращаются по инициативе одной из Сторон, Сторона, принявшая решение
о прекращении договорных отношений письменно уведомляет другую Сторону о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка. Договорные отношения в соответствии с настоящим Порядком считаются расторгнутым после выполнения Сторонами своих обязанностей.

2.1.7.3. Прекращение действия договорных отношений, определенных настоящим Порядком, не освобождает Стороны от исполнения обязанностей, возникших до указанного дня их прекращения и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

2.1.8. Внесение изменений и дополнений в Порядок.

2.1.8.1. Внесение изменений и дополнений в настоящий Порядок, включая внесение изменений и дополнений в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

2.1.8.2. Уведомление о внесении изменений и дополнений в Порядок осуществляется Удостоверяющим центром путем обязательного размещения на сайте Удостоверяющего центра в сети Интернет по адресу http://modum.pro (далее – сайт Удостоверяющего центра) новой версии Порядка, утвержденного приказом общества с ограниченной ответственностью «Модум», включающего внесенные изменения и дополнения.

2.1.8.3. Все изменения и дополнения, вносимые Удостоверяющим центром в настоящий Порядок, не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца с даты размещения новой версии Порядка, опубликованного на сайте Удостоверяющего центра.

2.1.8.4. Все изменения, вносимые Удостоверяющим центром в Порядок в связи с изменениями, которые вносятся в нормативные правовые акты, регулирующие отношения в области использования электронных подписей, вступают в силу одновременно с вступлением в силу вышеуказанных изменений.

2.1.8.5. Любые изменения в Порядке с момента вступления в силу новой версии Порядка распространяются на всех лиц, присоединившихся к Порядку, в том числе присоединившихся к Порядку ранее даты вступления новой версии Порядка в силу. В случае несогласия с вышеуказанными изменениями Сторона, присоединившаяся к Порядку до вступления в силу таких изменений, имеет право прекратить договорные отношения и расторгнуть настоящий Порядок, письменно уведомив Удостоверяющий центр о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка.

2.1.8.6. Все приложения, изменения и дополнения к настоящему Порядку являются его составной и неотъемлемой частью.

2.1.9. Применение Порядка.

2.1.9.1. Стороны понимают понятия и термины, применяемые в настоящем Порядке, строго в контексте общего смысла Порядка.

2.1.9.2. В случае противоречия и (или) расхождения названия какого-либо раздела Порядка со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

2.1.9.3. В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Порядку с положениями собственно Порядка, Стороны считают доминирующим смысл и формулировки Порядка.

2.1.10. Ответственность Сторон.

2.1.10.1. За невыполнение или ненадлежащее выполнение обязанностей, определенных настоящим Порядком, Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязанностей другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

2.1.10.2. Стороны не несут ответственность за неисполнение, либо ненадлежащее исполнение своих обязанностей, определенных настоящим Порядком, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной своих обязанностей.

2.1.10.3. Удостоверяющий центр не несет ответственность за невозможность использования в информационной системе электронной подписи, основанной на квалифицированном сертификате, выданном Удостоверяющим центром, в случае предъявления оператором данной информационной системы требований к квалифицированному сертификату и его форме, требований аккредитованному удостоверяющему центру и иных требований, в том числе к условиям признания электронных документов, подписанных электронной подписью и условиям признания электронной подписи, если указанные требования, установленные оператором информационной системы, не соответствуют требованиям, установленными Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, иными федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, в том числе требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27.12.2011 года № 795.

2.1.10.4. Стороны несут ответственность за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, соглашением Сторон, в том числе настоящим Порядком.

2.1.10.5. Ответственность Сторон, не урегулированная положениями настоящего Порядка, регулируется законодательством Российской Федерации.

2.1.11. Разрешение споров.

2.1.11.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к настоящему Порядку.

2.1.11.2. При рассмотрении спорных вопросов, связанных с настоящим Порядком, Стороны будут руководствоваться действующим законодательством Российской Федерации.

2.1.11.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

2.1.11.4. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

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

2.2. Сведения об Удостоверяющем центре.

2.2.1. Общество с ограниченной ответственностью «Модум» осуществляет оказание услуг, реализацию функций и исполнение обязанностей Удостоверяющего центра на основании:

- Устава общества с ограниченной ответственностью «Модум»;

- лицензии на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России от 10.07.2018 года № 16719Н (ЛСЗ № 0015684). Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности: работы, предусмотренные пунктами 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ,17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность,

в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16.04.2012 года № 313;

2.2.2. Реквизиты Удостоверяющего центра.

Полное наименование юридического лица: Общество с ограниченной ответственностью «Модум».

Сокращенное наименование юридического лица: ООО «Модум».

ОГРН: 1177746857045, ИНН: 7716866347, КПП:770101001

Банковские реквизиты:

Отделение – ПАО «Сбербанк» г. Москва р/с 40702810638000149194

кор/сч 30101810400000000225

БИК 044525225

2.2.3. Информация о месте нахождения и графике работы Удостоверяющего центра.

Место нахождения и почтовый адрес: 105082, г. Москва, ул. Большая Почтовая, 36 стр. 1, этаж 2, комната 6,6Б.

Адрес оказания услуг Удостоверяющего центра г. Москва, ул. Большая Почтовая, 36 стр. 1, этаж 2, комната 6,6Б.

График работы Удостоверяющего центра: ежедневно с 10:00 до 18:00 (московское время) с понедельника по пятницу за исключением выходных и праздничных дней.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра.

2.3.1. Справочные телефоны Удостоверяющего центра: 8 (495) 505 45 48.

2.3.2. Адрес электронной почты: ucinfo@modum.pro

2.3.3. Адрес сайта Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет»: http://modum.pro.

2.3.4. Порядок получения информации заявителями по вопросам предоставления услуг Удостоверяющего центра.

Любые заинтересованные лица могут получить информацию по вопросам предоставления услуг Удостоверяющего центра с использованием следующих способов:

- ознакомиться с информацией, опубликованной на сайте Удостоверяющего центра; обратиться в Удостоверяющий центр за получением информации по справочным телефонам 8 (495) 505 45 48;

- направить запрос по электронной почте на адрес uc@modum.pro. Срок ответа по запросу, направленному по электронной почте, составляет не более 3 (трех) рабочих дней со дня получения Удостоверяющим центром данному запроса;

- непосредственно обратиться по месту нахождения Удостоверяющего центра;

- направить письменное обращение в адрес Удостоверяющего центра. Данное обращение рассматривается в течение 30 (тридцати) дней со дня его поступления

в Удостоверяющий центр.

2.4. Стоимость услуг Удостоверяющего центра.

2.4.1. Любое лицо может обратиться в Удостоверяющий центр с запросом о оказании услуг. Запрос и рассмотрение такого запроса осуществляются в соответствии с пунктом 2.3.4 настоящего Порядка.

2.4.2. Услуги, оказываемые Удостоверяющим центром, предоставляются на платной основе.

2.4.3. Стоимость услуг, оказываемых Удостоверяющим центром на платной основе, определяется прейскурантом, утвержденным приказом. Прейскурант публикуется на сайте Удостоверяющего центра.

2.4.4. Сроки и порядок расчетов за оказываемые на платной основе услуги Удостоверяющего центра регулируются отдельными договорами (соглашениями), заключаемыми между обществом с ограниченной ответственностью «Модум» и заявителем.

Оплата осуществляется в российских рублях по безналичному расчету путем перечисления денежных средств на лицевой счет общества с ограниченной ответственностью «Модум». Датой оплаты считается дата поступления денежных средств на лицевой счет ООО «Модум».

2.4.5. По обращениям участников электронного взаимодействия Удостоверяющий центр на безвозмездной основе оказывает следующие услуги:

- предоставление участникам электронного взаимодействия информации, содержащейся в реестре выданных, аннулированных и прекративших свое действие сертификатов ключей проверки электронных подписей (далее – реестр сертификатов);
- аннулирование выданных Удостоверяющим центром квалифицированных сертификатов в соответствии с правилами, определенными настоящим Порядком;
- регистрация лица, которому выдан квалифицированный сертификат, в единой системе идентификации и аутентификации;
- создание и выдача квалифицированных сертификатов, выданных Удостоверяющим центром, в случае выполнения процедуры внеплановой смены ключа электронной подписи Удостоверяющего центра.

3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром.

В процессе реализации своей деятельности Удостоверяющий центр:

- создает квалифицированные сертификаты и выдает такие сертификаты лицам, обратившимся за их получением, при условии установления личности заявителя либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата;
- осуществляет проверку достоверности документов и сведений, представленных заявителем;
- 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 квалифицированного сертификата;
- устанавливает сроки действия квалифицированных сертификатов;
- выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;
- ведет реестр сертификатов, обеспечивает безвозмездный доступ к нему с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- 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;
- осуществляет по желанию лица, которому выдан квалифицированный сертификат, регистрацию указанного лица в единой системе идентификации и аутентификации;
- обеспечивает конфиденциальность созданных удостоверяющим центром ключей электронных подписей, за исключением ключей электронных подписей, полученных заявителями;
- обеспечивает целостность, достоверность и конфиденциальность информации,

подлежащей хранению в удостоверяющем центре;

- осуществляет сопровождение квалифицированных сертификатов, выдаваемых Удостоверяющим центром, в том числе обеспечивает внесение реестр сертификатов информации об аннулированных или прекративших свое действие сертификатах ключей проверки электронной подписи;

- обеспечивает актуализацию и публикацию списка отозванных сертификатов в электронном виде, предоставляет к нему безвозмездный доступ с использованием сети Интернет;

- осуществляет информирование лиц, обращающихся в Удостоверяющий центр для получения квалифицированных сертификатов, 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

- оказывает техническую поддержку Пользователей УЦ и осуществляет предоставление консультаций по вопросам использования электронной подписи и средств электронной подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи;

- осуществляет мероприятия по техническому сопровождению и обеспечению бесперебойного функционирования средств Удостоверяющего центра, обновлению программных и технических средств Удостоверяющего центра;

- обеспечивает информационную безопасность Удостоверяющего центра и осуществляет мероприятия по технической защите информации, обрабатываемой с использованием средств Удостоверяющего центра;

- осуществляет иную связанную с использованием электронной подписи деятельность.

4. Права и обязанности Удостоверяющего центра.

4.1. Права Удостоверяющего центра. Удостоверяющий центр имеет право:

- запрашивать у заявителя документы, необходимые для установления личности получателя квалифицированного сертификата (заявителя) либо документы, подтверждающие полномочия лица, выступающего от имени заявителя;

- запрашивать у заявителя документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата;

- отказать заявителю в выдаче квалифицированного сертификата в следующих случаях:

не предоставлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата;

документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания квалифицированного сертификата, представлены не в полном объеме или они не надлежаще оформлены, а также в случае, когда достоверность

и актуальность представленных заявителем сведений не подтверждается;

не установлена личность заявителя – физического лица, обратившегося за получением квалифицированного сертификата;

не получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;

- отказать заявителю в прекращении действия квалифицированного сертификата, выданного Удостоверяющим центром, в следующих случаях:

соответствующие заявительные документы не оформлены, оформлены ненадлежащим образом или не получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица;

квалифицированный сертификат был аннулирован или прекратил свое действие в соответствии с частями 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ.

- В одностороннем порядке прекратить действие квалифицированного сертификата, выданного Удостоверяющим центром, с одновременным направлением соответствующего уведомления его владельцу, в следующих случаях:

при наличии у Удостоверяющего центра достоверных сведений о нарушении конфиденциальности ключа проверки электронной подписи, принадлежащего владельцу соответствующего квалифицированного сертификата;

удостоверяющему центру стало известно и получены официальные сведения о том, что документы или сведения, представленные заявителем для получения квалифицированного сертификата, не являются подлинными или не подтверждают достоверность информации, включенной в квалифицированный сертификат;

в одностороннем порядке прекратить действие квалифицированного сертификата, выданного Удостоверяющим центром, с направлением соответствующего уведомления его владельцу не позднее, чем за один рабочий день до прекращения действия квалифицированного сертификата, в случае невыполнения владельцем квалифицированного сертификата обязанностей, установленных Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, иными принимаемыми в соответствии с ним нормативными правовыми актами, настоящим Порядком или договором оказания услуг Удостоверяющего центра;

- устанавливать сроки действия квалифицированных сертификатов;

- выдавать квалифицированные сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе;

- в одностороннем порядке вносить изменения и дополнения в Порядок в соответствии с пунктом 2.1.8 настоящего Порядка.

4.2. Обязанности Удостоверяющего центра.

4.2.1. Удостоверяющий центр обязан:

4.2.1.1. осуществлять деятельность в соответствии с требованиями федеральных законов «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года № 149-ФЗ, «О персональных данных» от 27.07.2006 года № 152-ФЗ, требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Минкомсвязи России от 13.08.2018 года № 397, иными нормативными правовыми актами в области использования электронной

подписи и защиты информации, настоящим Порядком;

4.2.1.2. обеспечить размещение настоящего Порядка на сайте Удостоверяющего центра;

4.2.1.3. 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;

4.2.1.4. обеспечить любому лицу безвозмездный доступ с использованием информационно- телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности Удостоверяющего центра;

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

4.2.1.6. обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей, за исключением ключей электронных подписей, полученных заявителями;

4.2.1.7. обеспечивать бесперебойное функционирование средств УЦ, осуществлять мероприятия по технической защите информации, обрабатываемой с использованием средств УЦ, принимать меры по обеспечению безопасности персональных данных при их обработке в Удостоверяющем центре;

4.2.1.8. организовать свою работу с учетом часового пояса по местонахождению Удостоверяющего центра и обеспечить синхронизацию по времени средств Удостоверяющего центра;

4.2.1.9. использовать для подписания квалифицированных сертификатов, выдаваемых Удостоверяющим центром, квалифицированную электронную подпись, основанную на квалифицированном сертификате УЦ, выданном Головным Удостоверяющим центром;

4.2.1.10. не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате УЦ, выданном Головным Удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными сертификатами;

4.2.1.11. использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате УЦ, только для подписания квалифицированных сертификатов, выдаваемых Удостоверяющим центром, и списка отозванных сертификатов;

4.2.1.12. осуществлять процедуру плановой смены ключей электронной подписи Удостоверяющего центра, используемого для подписания квалифицированных сертификатов, выдаваемых Удостоверяющим центром;

4.2.1.13. использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей

их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленными в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ;

4.2.1.14. использовать для реализации функций Удостоверяющего центра средства удостоверяющего центра, соответствующие требованиям к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27.12.2011 года № 796;

4.2.1.15. создавать квалифицированный сертификат в соответствии с требованиями к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27.12.2011 года № 795;

4.2.1.16. осуществлять проверку достоверности документов и сведений, представленных заявителем, в том числе 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 (далее – инфраструктура);

4.2.1.17. для внесения в квалифицированный сертификат информации 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.

4.2.1.18. установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

4.2.1.19. получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата;

4.2.1.20. осуществить подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата;

4.2.1.21. создать и выдать квалифицированный сертификат заявителю в соответствии с настоящим Порядком при условии подтверждения достоверности информации, представленной заявителем для включения в квалифицированный сертификат, установления личности заявителя - физического лица и получения подтверждения правомочий лица, выступающего от имени заявителя - юридического лица;

4.2.1.22. создать по обращению заявителя ключ электронной подписи и ключ проверки электронной подписи;

4.2.1.23. выдать 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;

4.2.1.24. осуществлять по обращениям участников электронного взаимодействия проверку электронных подписей;

4.2.1.25. обеспечивать уникальность ключей проверки электронных подписей и номеров квалифицированных сертификатов, выдаваемых Удостоверяющим центром;

4.2.1.26. при выдаче квалифицированного сертификата:

- ознакомить под расписку владельца квалифицированного сертификата с информацией, содержащейся в квалифицированном сертификате;

- направить 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;

- по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию указанного лица в единой системе идентификации и аутентификации;

- внести в реестр сертификатов информацию о выданном квалифицированном сертификате не позднее указанной в нем даты начала действия такого сертификата;

- выдать владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

4.2.1.27. 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 квалифицированного сертификата;

4.2.1.28. отказать заявителю в создании квалифицированного сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения квалифицированного сертификата;

4.2.1.30. отказать заявителю в выдаче квалифицированного сертификата в случае, если не подтверждена достоверность информации, представленной заявителем для включения в квалифицированный сертификат, или не установлена личность заявителя - физического лица или не получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата;

4.2.1.31. аннулировать квалифицированный сертификат, выданный Удостоверяющим центром, в следующих случаях:

- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной

подписи, указанному в таком сертификате;

- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

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

4.2.1.32. прекратить действие квалифицированного сертификата на основании надлежаще оформленного заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа, подписанного квалифицированной электронной подписью владельца сертификата;

4.2.1.33. внести в реестр сертификатов информацию о прекращении действия квалифицированного сертификата в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, или в течение 12 (двенадцати) часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств;

4.2.1.34. уведомить владельца сертификата о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования квалифицированного сертификата, выданного Удостоверяющим центром владельцу сертификата, в том числе об аннулировании или прекращении действия квалифицированного сертификата;

4.2.1.35. официально уведомить участников электронного взаимодействия об аннулировании или прекращении действия квалифицированного сертификата посредством внесения соответствующей информации в список отозванных сертификатов;

4.2.1.36. публиковать список отозванных сертификатов на сайте Удостоверяющего центра, обеспечить его актуальность и круглосуточную доступность. Информация о адресах публикации списка отозванных сертификатов указывается в квалифицированных сертификатах, выдаваемых Удостоверяющим центром;

4.2.1.37. хранить информацию, внесенную в реестр сертификатов, в течение всего срока деятельности Удостоверяющего центра;

4.2.1.38. обеспечить целостность и достоверность информации, хранящейся в Удостоверяющем центре;

4.2.1.39. обеспечить хранение следующей информации:

- 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.

4.2.1.40. в случае принятия решения о прекращении деятельности Удостоверяющего центра:

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

- передать в уполномоченный федеральный орган реестр сертификатов Удостоверяющего центра и информацию, подлежащую хранению в Удостоверяющем центра, в соответствии с Порядком 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, утвержденным приказом Минкомсвязи России от 14.08.2017 года № 416;

4.2.1.41. уведомить не менее чем за один месяц до даты прекращения деятельности Удостоверяющего центра владельцев сертификатов, имеющих квалифицированные сертификаты, срок действия которых не истек.

4.3. Права и обязанности Стороны, присоединившейся к Порядку.

4.3.1. Права Стороны, присоединившаяся к Порядку, права Пользователя УЦ.

Сторона, присоединившаяся к Порядку, имеет право:

- обратиться в Удостоверяющий центр для получения услуг, оказываемых Удостоверяющим центром в соответствии с настоящим Порядком, в том числе для регистрации в Удостоверяющем центре в качестве Пользователя УЦ и получения квалифицированного сертификата;

- получить квалифицированный сертификат Удостоверяющего центра в форме электронного документа и его копию на бумажном носителе, заверенную Удостоверяющим центром;

- получать в электронной форме списки отозванных сертификатов, созданные Удостоверяющим центром;

- применять квалифицированный сертификат Удостоверяющего центра и список отозванных сертификатов для проверки квалифицированных сертификатов, выданных Удостоверяющим центром;

- применять квалифицированные сертификаты, выданные Удостоверяющим центром, для проверки электронных подписей в электронных документах в соответствии со сведениями, указанными в квалифицированных сертификатах;

- получать средства электронной подписи, обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи;

- создавать с использованием средства электронной подписи ключ электронной подписи и ключ проверки электронной подписи;

- обращаться в Удостоверяющий центр для проведения проверки подлинности электронной подписи, основанной на квалифицированном сертификате, выданном Удостоверяющим центром;

- обращаться в Удостоверяющий центр для получения консультаций по вопросам использования электронной подписи, средств электронной подписи, вопросам обеспечения безопасности использования электронной подписи и средств электронной

подписи.

4.3.2. Пользователь УЦ имеет все права Стороны, присоединившейся к Порядку, а также имеет право:

4.3.2.1. получить в соответствии с настоящим Порядком квалифицированный сертификат, созданный Удостоверяющим центром для данного Пользователя УЦ, при условии установления Удостоверяющим центром личности лица, обращающегося за получением данного сертификата и подтверждения его правомочий;

4.3.2.2. при получении квалифицированного сертификата:

- получить копию сертификата на бумажном носителе, заверенную Удостоверяющим центром;
- получить ключ электронной подписи и ключ проверки электронной подписи Пользователя УЦ, созданные Удостоверяющим центром;
- пройти процедуру регистрации в единой системе идентификации и аутентификации; получить ключевую фразу, которая в дальнейшем может использоваться для аутентификации Пользователя УЦ;

4.3.2.3. запрашивать и получать в Удостоверяющем центр в форме электронного документа квалифицированные сертификаты иных Пользователей УЦ, информация о которых включена в реестр сертификатов Удостоверяющего центра;

4.3.2.4. обращаться в Удостоверяющий центр для прекращения действия (отзыва), квалифицированного сертификата, владельцем которого он является, в течение срока действия данного квалифицированного сертификата;

4.3.2.5. обращаться в Удостоверяющий центр для получения технической поддержки по вопросам использования электронной подписи и средств электронной подписи.

4.4. Обязанности Стороны, присоединившаяся к Порядку, обязанности Пользователя УЦ.

4.4.1. Сторона, присоединившаяся к Порядку, обязана:

- исполнять требования, установленные Федеральным законом «Об электронной подписи», от 06.04.2011 года № 63-ФЗ, принимаемыми в соответствии с ним нормативными правовыми актами и Порядком;
- предоставлять в соответствии с настоящим Порядком в Удостоверяющий центр актуальные и достоверные документы либо их надлежащим образом заверенные копии и сведения, в том числе необходимые для получения квалифицированного сертификата, регистрации квалифицированного сертификата в единой системе идентификации и аутентификации и (или) регистрации владельца сертификата в единой системе идентификации и аутентификации;
- использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ;
- обеспечивать конфиденциальность используемых ключей электронных подписей, в частности не допускать использование ключей электронных подписей иными лицами без своего согласия;
- предоставлять подтверждение, что лицо, обратившееся за получением квалифицированного сертификата, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом

/для получения квалифицированного сертификата;

- уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

- не использовать ключ электронной подписи, срок действия которого истек;

- оплатить услуги Удостоверяющего центра, если это предусмотрено договором оказания услуг Удостоверяющего центра;

4.4.2. Пользователь УЦ должен соблюдать все обязанности Стороны, присоединившаяся к Порядку, а также обязан:

4.4.2.1. при получении квалифицированного сертификата:

- ознакомится с информацией, содержащейся в квалифицированном сертификате; ознакомится с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, выдаваемым Удостоверяющим центром при выдаче квалифицированного сертификата;

- не использовать ключ электронной подписи и незамедлительно обратиться в Удостоверяющий центр для прекращения действия квалифицированного сертификата, владельцем которого он является, при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена;

- не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление на прекращение, действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр до момента времени официального уведомления о прекращении действия квалифицированного сертификата, либо об отказе в прекращении действия;

- не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, который аннулирован или действие которого прекращено;

- при создании или проверке электронной подписи осуществлять проверку действительности квалифицированного сертификата на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

- при проверке электронной подписи осуществлять проверку принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, а также осуществлять проверку отсутствия изменений, внесенных в этот документ после его подписания;

- информировать Удостоверяющий центр об изменении регистрационных данных владельца сертификата, влияющих на актуальность сведений, содержащихся в квалифицированном сертификате, и обратиться в Удостоверяющий центр для прекращения действия такого сертификата в случае наличия оснований полагать, что несоответствие данных о владельце сертификата и сведений, содержащихся в квалифицированном сертификате, может повлиять на результат проверки электронной подписи при осуществлении обмена информацией с иными участниками информационного взаимодействия.

5. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром.

5.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей.

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется Удостоверяющим центром или самостоятельно заявителем.

5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей заявителем.

5.1.1.1. Создание ключей электронных подписей и ключей проверки электронных подписей, предназначенных для создания и проверки усиленной квалифицированной электронной подписи, осуществляется заявителем с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с эксплуатационной и технической документацией на используемые средства электронной подписи.

5.1.1.2. Создание ключей электронных подписей и ключей проверки электронных подписей должно осуществляться заявителем в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» от 09.02.2005 года № 66.

5.1.1.3. Сторона, присоединившаяся к Порядку, имеет право получить средства электронной подписи при обращении в Удостоверяющий центр в соответствии с настоящим Порядком.

5.1.1.4. При создании ключа электронной подписи и ключа проверки электронной подписи заявитель формирует запрос на создание сертификата в электронной форме (файл в формате PKCS#10) и в форме бумажного документа, подписанного заявителем собственноручно.

Сформированный запрос на создание сертификата прикладывается к заявительным документам при обращении заявителя в Удостоверяющий центр для получения квалифицированного сертификата.

В случае, если используемые заявителем средства электронной подписи не позволяют сформировать запрос на создание сертификата в форме бумажного документа, допускается предоставление данного запроса в электронной форме, подписанного усиленной квалифицированной электронной подписью заявителя.

5.1.1.5. Заявитель при обращении в Удостоверяющий центр за получением квалифицированного сертификата обязан информировать Удостоверяющий центр о средстве электронной подписи (наименование и реквизиты заключения ФСБ России о подтверждении соответствия средства электронной подписи), которое было

использовано для создания ключа электронной подписи и ключа проверки электронной подписи.

5.1.1.6. При создании ключа электронной подписи и ключа проверки электронной подписи должен устанавливаться пароль доступа к ключевой информации, отвечающий требованиям к сложности паролей в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 12 к настоящему Порядку.

5.1.1.7. Заявитель должен обеспечивать конфиденциальность ключей электронных подписей и паролей доступа к ключевой информации, принимать все возможные меры для предотвращения их потери, раскрытия, искажения и несанкционированного использования.

5.1.1.8. Хранение и использование ключей электронных подписей должно осуществляться заявителем в соответствии с Инструкцией ФАПСИ № 152, руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 12 к настоящему Порядку.

5.1.1.9. При создании ключа электронной подписи и ключа проверки электронной подписи заявителем основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, является одновременное соблюдение следующих условий:

- подтверждена достоверность документов и сведений, предоставляемых в Удостоверяющий центр заявителем;

- установлена личность заявителя и получено подтверждение правомочий лица, выступающего от имени юридического лица, обращающегося за получением квалифицированного сертификата;

- информация, указанная в запросе на создание сертификата, в том числе информация о полномочиях лица, подписавшего запрос, соответствуют сведениям, указанными заявителем в документах, предоставляемых в Удостоверяющий центр;

- сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя;

- имеется положительный результат проверки электронной подписи, с помощью которой подписан запрос на создание сертификата, в случае если он предоставлен в электронной форме.

5.1.2. Порядок создания ключей электронных подписей и ключей проверки электронных подписей Удостоверяющим центром для заявителя.

5.1.2.1. Ключи электронных подписей и ключи проверки электронных подписей создаются Удостоверяющим центром с использованием средств электронной подписи и средств УЦ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности,

в соответствии с эксплуатационной и технической документацией на используемые средства электронной подписи и средства удостоверяющего центра.

5.1.2.2. Удостоверяющий центр 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 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» от 09.02.2005 года № 66.

5.1.2.3. Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется Удостоверяющим центром в соответствии с требованиями постановления Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» от 3.02.2012 года № 79, с использованием автоматизированных рабочих мест Удостоверяющего центра, а также средств защиты информации и средств криптографической защиты информации, прошедших процедуру оценки соответствия, аттестованных и (или) сертифицированных по требованиям безопасности информации.

5.1.2.4. Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Удостоверяющим центром для заявителя, присоединившегося к настоящему Порядку, при личном прибытии заявителя или его уполномоченного представителя в Удостоверяющий центр, при условии установления личности заявителя и получения подтверждения правомочий лица, выступающего от имени заявителя юридического лица.

5.1.2.5. Ключ электронной подписи и ключ проверки электронной подписи создается Удостоверяющим центром одновременно с созданием квалифицированного сертификата в соответствии с пунктом 5.1 настоящего Порядка, при условии подтверждения достоверности документов и сведений, предоставленных заявителем.

5.1.2.6. Создание ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата осуществляется Оператором УЦ в присутствии заявителя или его уполномоченного представителя.

Созданный ключ электронной подписи, ключ проверки электронной подписи и квалифицированный сертификат записываются Оператором УЦ на носитель ключевой информации (далее – ключевой носитель), принадлежащий заявителю, который непосредственно передается заявителю или е уполномоченному представителю юридического лица под расписку и записью в соответствующих журналах поэкземплярного учета Удостоверяющего центра. Удостоверяющий центр не осуществляет хранение ключа электронной подписи заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие заявителю.

5.1.2.7. Ключевой носитель, принадлежащий заявителю, перед осуществлением записи на него создаваемого Удостоверяющим центром ключа электронной подписи и ключа проверки электронной подписи, не должен содержать иной посторонней

информации, в том числе иных ключей электронной подписи. Удостоверяющий центр не несёт ответственности в связи с компрометацией или удалением информации, находящейся на носителе, принадлежащем заявителю.

5.1.2.8. При создании ключа электронной подписи и ключа проверки электронной подписи Удостоверяющим центром формируется пароль доступа к ключевой информации, который устанавливается по согласованию с заявителем. После получения ключа электронной подписи и ключа проверки электронной подписи заявитель должен произвести смену пароля доступа к ключевой информации, соблюдая требования к сложности паролей в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 12 к настоящему Порядку.

5.1.2.9. В случае, если Удостоверяющий центр не имеет технической возможности использовать для создания ключа электронной подписи и ключа проверки электронной подписи средство электронной подписи, аналогичное средству электронной подписи заявителя, указанному им в заявительных документах, заявитель имеет право самостоятельно осуществить создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 5.1.1 настоящего Порядка.

5.1.2.10. В случае создания ключа электронной подписи и ключа проверки электронной подписи при личном прибытии заявителя или лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, является одновременное соблюдение следующих условий:

- подтверждена достоверность документов и сведений, предоставляемых в Удостоверяющий центр заявителем;

- установлена личность заявителя и получено подтверждение правомочий лица, выступающего от имени заявителя- юридического лица, обращающегося за получением квалифицированного сертификата;

- заявитель или уполномоченный представитель юридического лица под расписку ознакомился с информацией, содержащейся в запросе на создание сертификата, сформированном Удостоверяющим центром.

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

5.2.1. В процессе организации деятельности Удостоверяющего центра осуществляется планирование мероприятий по осуществлению его деятельности, в том числе мероприятий по смене ключей электронной подписи Удостоверяющего центра и мероприятий по выводу ключей электронной подписи Удостоверяющего центра из эксплуатации.

5.2.2. Основаниями для выполнения процедуры плановой смены ключа электронной подписи Удостоверяющего центра и процедуры его вывода из

эксплуатации являются запланированные мероприятия по осуществлению деятельности Удостоверяющего центра.

5.2.3. Выполнение процедуры плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в период срока действия ключа электронной подписи Удостоверяющего центра, не ранее, чем через шесть месяцев, и не позднее, чем через один год после начала действия ключа электронной подписи Удостоверяющего центра. Процедура создания нового ключа электронной подписи Удостоверяющего центра осуществляется заранее, не позднее, чем за 15 дней до истечения одного года после начала срока действия ключа электронной подписи Удостоверяющего центра.

5.2.4. Выполнение процедуры вывода из эксплуатации ключа электронной подписи Удостоверяющего центра осуществляется не позднее, чем за один рабочий день до окончания срока действия ключа электронной подписи Удостоверяющего центра, установленного в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

5.2.5. Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени создания ключа электронной подписи Удостоверяющего центра.

5.2.6. Порядок смены ключей электронной подписи Удостоверяющего центра.

5.2.6.1. Плановая смены ключей электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

5.2.6.1.1. Администратор УЦ с использованием сертифицированных по требованиям безопасности средств удостоверяющего центра и средств электронной подписи создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, записывает их на сертифицированный учтенный ключевой носитель и обеспечивает его хранение в соответствии с требованиями, предъявляемыми к обеспечению целостности и конфиденциальности ключа электронной подписи Удостоверяющего центра;

Одновременно с созданием вышеуказанных ключей производится формирование запроса на создание квалифицированного сертификата Удостоверяющего центра.

5.2.6.1.2. сформированный запрос на создание квалифицированного сертификата Удостоверяющего центра, а также иная информация, необходимая для получения квалифицированного сертификата Удостоверяющего центра, направляется в уполномоченный федеральный орган, являющийся Головным Удостоверяющим центром в отношении Удостоверяющего центра;

5.2.6.1.3. после получения квалифицированного сертификата, созданного головным удостоверяющим центром уполномоченного федерального органа, Администратор УЦ, по истечении шести месяцев после начала срока действия предыдущего ключа электронной подписи Удостоверяющего центра:

- осуществляет ввод в эксплуатацию и установку нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Удостоверяющего центра;

- производит в соответствии с технической и эксплуатационной документацией настройку средств удостоверяющего центра для использования нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Удостоверяющего центра;

- обеспечивает хранение и использование ключей электронной подписи и ключей проверки электронной подписи Удостоверяющего центра в соответствии с требованиями безопасности, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

5.2.6.2. Направление сформированного запроса на создание квалифицированного сертификата Удостоверяющего центра и получение квалифицированного сертификата, созданного головным удостоверяющим центром уполномоченного федерального органа, осуществляется с использованием доверенного способа взаимодействия.

Доверенным способом взаимодействия является использование информационной системы головного удостоверяющего центра, входящей в состав инфраструктуры.

5.2.6.3. Информирование участников электронного взаимодействия о проведении плановой смены ключа электронной подписи Удостоверяющего центра осуществляется посредством размещения на сайте Удостоверяющего центра информации о новом квалифицированном сертификате Удостоверяющего центра, соответствующему новому ключу проверки электронной подписи и ключу электронной подписи Удостоверяющего центра.

5.2.6.4. Предыдущий ключ электронной подписи Удостоверяющего центра действует в течение своего срока действия до вывода его из эксплуатации и используется для создания и подписания списка отозванных сертификатов, созданных Удостоверяющим центром в период действия предыдущего ключа электронной подписи Удостоверяющего центра.

5.2.6.5. Введенный в эксплуатацию новый ключ электронной подписи Удостоверяющего центра используется только для подписания создаваемых Удостоверяющим центром квалифицированных сертификатов и списков отозванных сертификатов.

5.2.6.6. Доверенными способами получения квалифицированного сертификата Удостоверяющего центра являются:

- получение заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении

квалифицированного сертификата, созданного Удостоверяющим центром для заявителя;

- загрузка квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ.

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

5.3.1. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра или реализации угрозы нарушения его конфиденциальности осуществляется внеплановая смена ключа электронной подписи и ключа проверки электронной подписи Удостоверяющего центра.

5.3.2 К случаям нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра, относятся:

- получение доступа неуполномоченного лица к ключу электронной подписи Удостоверяющего центра или к ключевому носителю, содержащего ключ электронной подписи Удостоверяющего центра;
- утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра;
- утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра, с его последующим обнаружением;
- получение доступа неуполномоченного лица к техническим средствам Удостоверяющего центра или средствам электронной подписи, содержащих ключ электронной подписи Удостоверяющего центра;
- несанкционированное копирование ключа электронной подписи Удостоверяющего центра;
- нарушение правил хранения и использования ключа электронной подписи Удостоверяющего центра, которое привело или могло привести к его компрометации;
- нарушение целостности печатей на сейфах (шкафах, хранилищах) и пеналах (конвертах), предназначенных для хранения ключевых носителей, содержащих ключи электронной подписи Удостоверяющего центра;
- утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них ключевых носителей, содержащих ключи электронной подписи Удостоверяющего центра;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем, в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий нарушителя.

5.3.3. Виды угроз нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра:

- угрозы, непосредственно связанные с нарушением конфиденциальности ключа электронной подписи Удостоверяющего центра;

- угрозы, связанные с несанкционированным доступом в помещения, где размещаются технические средства удостоверяющего центра, или доступам к хранилищам ключевой информации;

- угрозы, связанные с несанкционированным доступом к средствам удостоверяющего центра;

- угрозы, связанные с лицами, имеющими доступ в контролируемую зону, к средствам Удостоверяющего центра, ключам электронной подписи Удостоверяющего центра;

- угрозы, связанные с проведением нарушителем атак на технические средства удостоверяющего центра, в том числе на носители защищаемой информации, средства вычислительной техники, среду функционирования средств криптографической защиты информации, каналы (линии) связи.

5.3.4. Удостоверяющего центр начинает процедуру внеплановой смены ключа электронной подписи Удостоверяющего центра после устранения причин, повлекших нарушение конфиденциальности электронной подписи Удостоверяющего центра, и не позднее 12 (двенадцати) часов с момента выявления факта компрометации или факта реализации угрозы нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра уведомляет уполномоченный федеральный орган о факте компрометации ключа электронной подписи Удостоверяющего центра и необходимости внеплановой смены ключа электронной подписи Удостоверяющего центра, для чего направляет в уполномоченный федеральный орган соответствующие заявление на прекращение действия квалифицированного сертификата Удостоверяющего центра и заявление на создание и выдачу нового квалифицированного сертификата Удостоверяющего центра.

5.3.5. Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра осуществляется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра в соответствии с пунктом 6.2 настоящего Порядка.

5.3.6. Одновременно со сменой ключа электронной подписи Удостоверяющего центра прекращается действие всех ранее выданных квалифицированных сертификатов, подписанных ключом электронной подписи Удостоверяющего центра, который скомпрометирован.

5.3.7. Удостоверяющий центр уведомляет о факте компрометации ключа электронной подписи Удостоверяющего центра всех владельцев сертификатов путем направления соответствующего уведомления по электронной почте и публикации информации на сайте Удостоверяющего центра.

5.3.8. Прекращение действия квалифицированного сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия квалифицированного сертификата

Удостоверяющего центра включается в список отозванных сертификатов, который публикуется головным удостоверяющим центром.

5.3.9. После смены ключа электронной подписи Удостоверяющего центра и получения нового квалифицированного сертификата Удостоверяющего центра, выданного головным уполномоченным органом, Удостоверяющий центр уведомляет всех владельцев сертификатов о возможности получения ими новых квалифицированных сертификатов на безвозмездной основе.

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

- получение заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении квалифицированного сертификата, созданного Удостоверяющим центром для заявителя;

- загрузка нового квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ.

5.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Пользователя УЦ.

5.4.1. Сроки действия ключей электронной подписи и квалифицированных сертификатов, выдаваемых Удостоверяющим центром Пользователям УЦ.

5.4.1.1 Срок действия ключа электронной подписи и квалифицированного сертификата, выдаваемого Удостоверяющим центром Пользователю УЦ, включается в состав квалифицированного сертификата и составляет 1 (один) год.

5.4.1.2. Начало периода действия ключа электронной подписи исчисляется с даты и времени начала действия соответствующего квалифицированного сертификата.

5.4.1.3 Время начала действия квалифицированного сертификата включается в поле «Действителен с» («NotBefore») квалифицированного сертификата. Время окончания действия квалифицированного сертификата включается в поле «Действителен по» («NotAfter») квалифицированного сертификата.

5.4.1.4. Период действия ключа электронной подписи включается в поле «Период использования закрытого ключа» («PrivateKeyUsagePeriod») квалифицированного сертификата, содержащего время начала и окончания действия ключа электронной подписи, которые включаются соответственно в поле «Действителен с» («NotBefore») и в поле «Действителен по» («NotAfter») квалифицированного сертификата.

5.4.2. Смена ключа электронной подписи Пользователя УЦ осуществляется Удостоверяющим центром в следующих случаях:

5.4.2.1. в связи с истечением установленного срока действия ключа электронной подписи;

5.4.2.2. на основании заявления, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

5.4.2.3. не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

5.4.2.4. установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

5.4.2.5 вступило в силу решение суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию;

5.4.2.6. изменение сведений о владельце сертификата, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными;

5.4.2.7. нарушение конфиденциальности ключа электронной подписи владельца сертификата;

5.4.2.8. осуществлена процедура внеплановой смена ключа электронной подписи Удостоверяющего центра. В таком случае создание новых ключей электронной подписи для Пользователя УЦ и соответствующих им квалифицированных сертификатов осуществляется в соответствии с пунктом 5.3 настоящего Порядка;

5.4.2.9. в иных случаях, установленных Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или договором оказания услуг удостоверяющего центра.

5.4.3. В случае наступления обстоятельств, указанных в пунктах 5.4.2.3-5.4.2.5 настоящего Порядка, Удостоверяющий центр, в соответствии с пунктом 6.1, статьи 14 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, аннулирует квалифицированный сертификат владельца сертификата и уведомляет об этом владельца сертификата. Информация о прекращении действия сертификата вносится Удостоверяющим центром в реестр сертификатов в течение 12 (двенадцати) часов с момента наступления указанных обстоятельств, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

5.4.4. В случае наступления обстоятельств, указанных в пунктах 5.4.2.6 и 5.4.2.7 настоящего Порядка, Сторона, присоединившаяся к Порядку, обязана обратиться в Удостоверяющий центр с заявлением на прекращение действия квалифицированного сертификата.

5.4.5. Смена ключа электронной подписи Пользователя УЦ осуществляется по его инициативе Стороны, присоединившейся к Порядку, в соответствии процедурой создания ключей электронных подписей и ключей проверки электронных подписей, приведенной в пункте 5.1 настоящего Порядка.

5.4.6. Создание Удостоверяющим центром нового ключа электронного подписи

осуществляется одновременно с созданием и выдачей Пользователю УЦ ключа проверки электронной подписи и квалифицированного сертификата на основании соответствующего заявления Стороны, присоединившейся к Порядку, и документов, представленных в Удостоверяющий центр.

5.4.7. Требования к заявлению на смену ключа электронной подписи Пользователя УЦ.

Заявление на смену ключа электронной подписи Пользователя УЦ оформляется по форме заявления на создание и выдачу квалифицированного сертификата, приведенной в приложении № 3 или приложения № 4 к настоящему Порядку, и должно соответствовать требованиям к заявлению на создание и выдачу квалифицированного сертификата, указанным в пункте 5.5.2 и следующим требованиям:

5.4.7.1. в случае, если заявителем является юридическое лицо, заявление должно быть оформлено на бланке организации (при наличии) и заверено печатью юридического лица, а также содержать:

- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;
- реквизиты (дата и номер письма);
- собственноручную подпись физического лица, действующее от имени юридического лица на основании учредительных документов юридического лица ;
- собственноручную подпись физического лица в предоставляемом согласии на обработку персональных данных, в случае, если сведения о нем указаны в заявлении на создание квалифицированного сертификата;

5.4.7.2. в случае, если заявителем является физическое лицо, заявление должно содержать:

- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;
- собственноручную подпись физического лица и дату подписания;
- собственноручную подпись физического лица и дату подписания в предоставляемом согласии на обработку персональных данных;

5.4.7.3. в случае, если заявитель самостоятельно осуществил создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 5.1.1 настоящего Порядка, к вышеуказанному заявлению прикладывается сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

5.4.8. Заявитель имеет право создать заявление на смену ключа электронной подписи Пользователя УЦ в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя, при этом заявление должно соответствовать требованиями, указанным в пунктах 5.4.7 и 5.5.2 настоящего Порядка.

Процедура смены ключа электронной подписи Пользователя УЦ осуществляется

заявителем в соответствии с пунктами 5.1 и 5.4 настоящего Порядка в том же порядке, как и создание ключа электронной подписи, при этом осуществляется также создание квалифицированного сертификата в соответствии с пунктом 5.5 настоящего Порядка.

В случае, если смена ключа электронной подписи Пользователя УЦ связана с нарушением его конфиденциальности или реализацией угрозы нарушения конфиденциальности, соответствующее заявление должно быть подписано усиленной квалифицированной электронной подписью заявителя, основанной на действующем квалифицированном сертификате, не связанном с ключом электронной подписи, конфиденциальность которого нарушена.

5.4.9. Процедура создания и выдачи квалифицированного сертификата и (при необходимости) ключа электронной подписи его владельцу, в том числе в электронной форме, производится с соблюдением положений статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и настоящим Порядком.

5.5. Процедура создания и выдачи квалифицированных сертификатов.

5.5.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов.

5.5.1.1. Заявитель обязан ознакомиться с положениями настоящего Порядка, опубликованного на сайте Удостоверяющего центра, в том числе с приложениями к настоящему Порядку.

5.5.1.2. В случае, если заявитель не направлял запрос на получение услуг Удостоверяющего центра на безвозмездной основе или такой запрос не был удовлетворён, услуги Удостоверяющего центра оказываются на платной основе в соответствии с действующим прейскурантом, размещенном на сайте Удостоверяющего центра, и договором на оказание услуг удостоверяющего центра.

5.5.1.3. Присоединение к Порядку осуществляется в соответствии с пунктом 2.1.6 настоящего Порядка. Для присоединения к настоящему Порядку и возможности получения услуг Удостоверяющего центра заявитель направляет заявление о присоединении к Порядку по форме приложения № 1 или приложения № 2 к настоящему Порядку.

5.5.1.4. Удостоверяющий центр осуществляет создание квалифицированных сертификатов при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

5.5.1.5. Создание квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявления на создание и выдачу квалифицированного сертификата, а также документов и сведений, представленных заявителем в Удостоверяющий центр, при условии установления личности заявителя и получения подтверждения правомочий лица, выступающего от имени заявителя – юридического лица, обращаться за получением квалифицированного сертификата.

5.5.1.6. Для регистрации в Удостоверяющем центре лица, на имя которого будет создан квалифицированный сертификат, в качестве Пользователя УЦ, заявитель направляет в Удостоверяющий центр заявление на создание и выдачу

квалифицированного сертификата на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной подписью заявителя.

5.5.1.7. Заявитель имеет право предоставить в Удостоверяющий центр заявление о присоединении к Порядку, заявление на создание и выдачу квалифицированного сертификата, а также документы и сведения, необходимые для регистрации Пользователя УЦ и создания квалифицированного сертификата, одним пакетом документов при личном прибытии заявителя или лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр, либо посредством почтовой или курьерской связи, либо предоставить указанные документы в форме электронных документов, подписанных усиленной квалифицированной подписью заявителя, на электронном носителе информации или направив их в Удостоверяющий центр по информационно - телекоммуникационной сети, в том числе сети Интернет.

5.5.1.8. В случае, если представляемые заявителем документы содержат персональные данные, не являющиеся общедоступными, или иную конфиденциальную информацию, заявитель обязан обеспечить конфиденциальность такой информации при ее направлении в Удостоверяющий центр, в том числе с использованием сертифицированных средств криптографической информации, либо представить такие документы при личном прибытии в Удостоверяющий центр.

5.5.1.9. В случае, если Сторона, присоединившаяся к Порядку, обращается в Удостоверяющий центр для проведения плановой смены ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Пользователя УЦ и сведения, содержащиеся в ранее представленных документах, потеряли свою актуальность и достоверность, Сторона, присоединившаяся к Порядку, предоставляет в Удостоверяющий центр заявление на создание и выдачу квалифицированного сертификата, а также актуальные документы и сведения, необходимые для создания квалифицированного сертификата.

5.5.1.10. После получения Удостоверяющим центром от заявителя заявления о присоединении к Порядку и (или) заявления на создание и выдачу квалифицированного сертификата, в случае, если заявителем не представлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или их достоверность и актуальность не подтверждается, Удостоверяющий центр имеет право запросить, а Сторона, присоединившаяся к Порядку, обязана предоставить документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата.

5.5.1.11. Удостоверяющий центр имеет право отказать заявителю в регистрации Пользователя УЦ и создании квалифицированного сертификата, в случае, если Сторона, присоединившаяся к Порядку, не предоставила документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или они не

надлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается.

5.5.2. Требования к заявлению на создание и выдачу квалифицированного сертификата.

5.5.2.1. Требования к оформлению заявления на создание и выдачу квалифицированного сертификата.

5.5.2.1.1. В случае, если заявителем является юридическое лицо, заявление оформляется по форме, приведенной в приложении № 3 к настоящему Порядку, на бланке организации (при наличии) и заверено печатью юридического лица, а также должно содержать:

- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;

- реквизиты (дата и номер письма);

- собственноручную подпись физического лица, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности;

- собственноручную подпись физического лица в предоставляемом согласии на обработку персональных данных, в случае, если сведения о нем указаны в заявлении на создание квалифицированного сертификата.

5.5.2.1.2. В случае, если заявителем является физическое лицо, заявление оформляется по форме, приведенной в приложении № 4 к настоящему Порядку, и должно содержать:

- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;

- собственноручную подпись физического лица и дату подписания;

- собственноручную подпись физического лица и дату подписания в предоставляемом согласии на обработку персональных данных.

5.5.2.2. В случае, если заявитель самостоятельно осуществил создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 5.1.1 настоящего Порядка, к заявлению прикладывается сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

5.5.2.3. Требования к сведениям, включаемым в заявление на создание и выдачу квалифицированного сертификата, если заявителем является юридическое лицо:

5.5.2.3.1 в случае, если заявителем является юридическое лицо, в заявлении в обязательном порядке указывается следующая информация:

- наименование юридического лица;

- место нахождения юридического лица;

- основной государственный регистрационный номер (далее – ОГРН);

- идентификационный номер налогоплательщика (далее – ИНН) юридического

лица.

5.5.2.3.2. В случае, если заявителем является иностранная организация (в том числе филиал, представительство или иное обособленное подразделение иностранной организации), в заявлении в обязательном порядке указывается следующая информация:

- наименование владельца сертификата;
- место нахождения владельца сертификата;
- ИНН организации (при наличии).

5.5.2.3.3. В случае выдачи квалифицированного сертификата юридическому лицу в качестве владельца сертификата наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности (далее также – уполномоченный представитель юридического лица), в связи с чем в заявлении на создание и выдачу квалифицированного сертификата дополнительно указываются следующая информация:

- фамилия, имя и отчество (если имеется) уполномоченного представителя юридического лица;
- страховой номер индивидуального лицевого счета (далее – СНИЛС) уполномоченного представителя юридического лица;
- подразделение организации (при наличии);
- должность уполномоченного представителя юридического лица (при наличии).

5.5.2.4. Требования к сведениям, включаемым в заявление на создание и выдачу квалифицированного сертификата, если заявителем является физическое лицо:

5.5.2.4.1. В случае, если заявителем является физическое лицо, не являющееся индивидуальным предпринимателем, в заявлении в обязательном порядке указывается следующая информация:

- фамилия, имя и отчество (если имеется) физического лица;
- СНИЛС;
- ИНН физического лица.

5.5.2.4.2. В случае, если заявителем является физическое лицо, являющееся индивидуальным предпринимателем, в заявлении в обязательном порядке указывается следующая информация:

- фамилия, имя и отчество (если имеется) физического лица;
- СНИЛС;
- ИНН физического лица;
- ОГРН индивидуального предпринимателя.

5.5.2.5. Заявление на создание и выдачу квалифицированного сертификата должно содержать информацию о наименовании и классе средства электронной подписи, используемом заявителем.

5.5.2.6. В случае, если заявителем представлены в 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.

5.5.2.7. Заявитель имеет право оформить заявление на создание и выдачу квалифицированного сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

5.5.3. Порядок установления личности заявителя.

В соответствии со статьей 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ при выдаче квалифицированного сертификата Удостоверяющий центр устанавливает личность физического лица, обратившегося к нему за получением квалифицированного сертификата, руководствуясь следующими положениями:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность;

- 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.

5.5.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи квалифицированного сертификата.

При обращении в Удостоверяющий центр заявитель представляет документы либо их надлежащим образом заверенные копии и сведения.

5.5.4.1. Заявители, являющиеся юридическими лицами, предоставляют:

5.5.4.1.1. основной документ, удостоверяющий личность физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица, либо основной документ, удостоверяющий личность уполномоченного представителя юридического лица, действующего по доверенности, если сведения об этом лице включаются в квалифицированный сертификат наряду с указанием наименования юридического лица. Допускается вместо основного документа, удостоверяющего личность физического лица, предоставлять его надлежащим образом заверенную копию;

5.5.4.1.2. учредительные документы юридического лица либо их надлежащим образом заверенные копии, подтверждающие полномочия физического лица, действовать от имени юридического лица на основании учредительных документов юридического лица;

5.5.4.1.3. доверенность, подтверждающая право физического лица (уполномоченного представителя юридического лица), действовать от имени юридического лица по доверенности, если сведения об этом лице включаются в квалифицированный сертификат наряду с указанием наименования юридического

лица. Указанная доверенность оформляется в соответствии с формой, приведенной в приложении № 5 к настоящему Порядку;

5.5.4.1.4 страховой номер индивидуального лицевого счета (либо его надлежащим образом заверенную копию) уполномоченного представителя юридического лица (физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности), если такое физическое лицо указано в качестве владельца сертификата наряду с указанием наименования юридического лица и сведения о СНИЛС включены в заявление на создание и выдачу квалифицированного сертификата;

5.5.4.1.5. свидетельство о постановке на учет российской организации в налоговом органе по месту ее нахождения либо его надлежащим образом заверенную копию – для российского юридического лица, либо свидетельство о постановке на учет в налоговом органе заявителя – для иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации);

5.5.4.1.6. свидетельство о государственной регистрации юридического лица, либо его надлежащим образом заверенную копию;

5.5.4.1.7. выписку из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента обращения в Удостоверяющий центр, либо ее надлежащим образом заверенную копию.

Заявитель имеет право по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 5.5.4.1.5-5.5.4.1.7 настоящего пункта, в том числе в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

5.5.4.2. Заявители, являющиеся физическими лицами, предоставляют:

- основной документ, удостоверяющий личность, либо его надлежащим образом заверенную копию;

- страховой номер индивидуального лицевого счета либо его надлежащим образом заверенную копию;

- свидетельство о постановке на учет физического лица в налоговом органе либо его надлежащим образом заверенную копию;

5.5.4.3. Заявители, являющиеся индивидуальными предпринимателями, предоставляют:

5.5.4.3.1. основной документ, удостоверяющий личность, либо его надлежащим образом заверенную копию;

5.5.4.3.2. страховой номер индивидуального лицевого счета, либо его надлежащим образом заверенную копию;

5.5.4.3.3. свидетельство о постановке на учет физического лица в налоговом органе либо его нотариально заверенную копию;

5.5.4.3.4. свидетельство о государственной регистрации физического лица в качестве индивидуального предпринимателя, либо его надлежащим образом заверенную копию;

5.5.4.3.5. выписку из Единого государственного реестра индивидуальных предпринимателей, полученную не ранее чем за один месяц до момента обращения в Удостоверяющий центр, либо ее надлежащим образом заверенную копию;

Заявитель имеет право по собственной инициативе представить копии документов, содержащих сведения, указанные в пунктах 5.5.4.3.4- 5.5.4.3.5 настоящего пункта, в том числе в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

5.5.4.4. В случае, если документы и сведения, предоставляемые заявителем, оформлены не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

5.5.4.5. В случае, если лицо, которое указано в заявлении на создание и выдачу квалифицированного сертификата, при получении квалифицированного сертификата изъявило желание воспользоваться услугой Удостоверяющего центра по регистрации указанного лица в единой системе идентификации и аутентификации, данное лицо предоставляет в Удостоверяющий центр сведения в объеме, необходимом для регистрации в единой системе идентификации и аутентификации.

5.5.4.6. В случае, если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

5.5.5. Порядок проверки достоверности документов и сведений, представленных заявителем.

5.5.5.1. При получении от заявителя документов и сведений, необходимых для создания и выдачи квалифицированного сертификата, Оператор УЦ, в целях определения возможности регистрации Пользователя УЦ, в течение одного рабочего дня со дня их получения осуществляет предварительную проверку представленных заявителем документов и сведений на предмет их надлежащего оформления и полноты представления.

5.5.5.2. Полученные Удостоверяющим центром заявления и иные документы регистрируются в соответствии с правилами ведения делопроизводства.

5.5.5.3. В случае, если Сторона, присоединившаяся к Порядку, обращается в Удостоверяющий центр для проведения плановой смены ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата зарегистрированного Пользователя УЦ, и документы, представленные заявителем ранее, имеются в Удостоверяющем центре, Оператор УЦ осуществляет проверку их актуальности и достоверности, а также соответствия сведений, содержащихся в заявлении на создание квалифицированного сертификата, с регистрационными данными Пользователя УЦ.

5.5.5.4. В случае, если документы представлены заявителем в форме электронных документов, подписанных усиленной квалифицированной электронной

подписью, Оператор УЦ осуществляет ее проверку в соответствии со статьей 11 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ.

5.5.5.5. В случае положительной предварительной проверки 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» от 06.04.2011 года № 63-ФЗ и в течение одного рабочего дня со дня получения документов и сведений, представленных заявителем, запрашивает 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.

5.5.5.6. Процедура регистрации Пользователя УЦ или изменение регистрационных данных Пользователя УЦ.

5.5.5.6.1. В течение одного рабочего дня со дня получения из государственных информационных ресурсов сведений, запрошенных Удостоверяющим центром, в случае, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем, Оператор УЦ:

- осуществляет регистрацию лица, сведения о котором указаны в заявлении на создание и выдачу квалифицированного сертификата, в реестре Удостоверяющего центра в качестве Пользователя УЦ и направляет ему соответствующее уведомление о регистрации Пользователя УЦ;

- осуществляет изменение регистрационных данных Пользователя УЦ и направляет ему соответствующее уведомление, в случае, если лицо, сведения о котором указаны в заявлении на создание и выдачу квалифицированного сертификата, зарегистрировано в реестре Удостоверяющего центра в качестве Пользователя УЦ и сведения о нем изменились.

5.5.5.6.2. Удостоверяющий имеет право отказать в регистрации Пользователя УЦ в реестре Удостоверяющего центра или изменения регистрационных данных Пользователя УЦ в случае отрицательного результата проверки документов и сведений, предоставленных заявителем, в том числе в следующих случаях:

- не предоставлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата;

- документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания квалифицированного сертификата, представлены не в полном объеме или они не надлежаще оформлены, а также в случае, если актуальность представленных заявителем сведений не подтверждается;

- не получено подтверждение правомочий лица, выступающего от имени

заявителя – юридического лица, обращаться за получением квалифицированного сертификата;

- сведения, полученные из государственных информационных ресурсов, не подтверждают достоверность информации, представленной заявителем.

5.5.5.7. В случае отрицательного результата проверки документов и сведений Удостоверяющий центр уведомляет об этом заявителя в течение одного дня после проведения их проверки. В случае, если заявитель, после получения от Удостоверяющего центра соответствующего уведомления, не представил в течение пяти рабочих дней актуальные и соответствующие требованиям документы, Удостоверяющий центр возвращает документы заявителю.

5.5.6. Порядок создания квалифицированного сертификата.

5.5.6.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13 – 15, 17 и 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и настоящим Порядком.

Заявителям, которым услуги Удостоверяющего центра оказываются в соответствии с заключенным договором на оказание услуг удостоверяющего центра, квалифицированные сертификаты создаются при выполнении Стороной, присоединившейся к Порядку, обязанностей, предусмотренных настоящим Порядком и вышеуказанным договором.

5.5.6.2. Удостоверяющий центр в течение не более чем одного рабочего дня со дня получения сведений из государственных информационных ресурсов и положительного результата проведения проверки документов и сведений, предоставленных заявителем, уведомляет об этом заявителя и, в целях установления личности физического лица, обращающего за получением квалифицированного сертификата, а также для предоставления заявителем (при необходимости) оригиналов документов или их надлежаще заверенных копий, согласовывает с заявителем дату и время прибытия заявителя либо лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр.

5.5.6.3. При прибытии заявителя, либо лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр, Оператор УЦ осуществляет установление его личности и проверку оригиналов документов или их надлежаще заверенных копий, проверку соответствия сведений, полученных из государственных информационных ресурсов, со сведениями, содержащимися в представленных заявителем документах и регистрационных данных Пользователя УЦ, а также правомочий лица, выступающего от имени заявителя - юридического лица.

5.5.6.4. Если заявителем не представлены надлежащим образом заверенные копии документов, такие копии заверяется в Удостоверяющем центре при предоставлении оригиналов документов.

5.5.6.5. В случае установления личности лица, обращающегося за получением квалифицированного сертификата, и положительного результата проверки документов

и сведений, Оператор УЦ осуществляет создание квалифицированного сертификата для соответствующего ранее зарегистрированного Пользователя УЦ с использованием одного из следующих способов:

- на основании запроса на создание сертификата, сформированного и представленного заявителем в форме электронного документа (файла запроса на создание сертификата), подписанного усиленной квалифицированной электронной подписью заявителя;

- на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра.

5.5.6.6. Процедура создания квалифицированного сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного и представленного заявителем.

5.5.6.6.1. При получении от заявителя запроса на создание сертификата Оператор УЦ осуществляет проверку:

- сформированного заявителем запроса на создание сертификата на бумажном носителе, подписанного собственноручной подписью заявителя, либо запроса в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя;

- владение заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, в соответствии с пунктом 5.1.1, настоящего Порядка и в соответствии с пунктом 5.4 настоящего Порядка, если выполняется смена ключа электронной подписи владельца сертификата;

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

5.5.6.6.2. Ознакомление под расписку лицом, обратившимся за получением квалифицированного сертификата, со сведениями, содержащимися в запросе на создание сертификата, и их соответствие со сведениями, содержащимися в заявлении на создание и выдачу квалифицированного сертификата и иных представленных заявителем документах, является одним из условий подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата.

5.5.6.6.3. При положительных результатах проверки документов и сведений, представленных заявителем, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем, установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, а также если подтверждено владение заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, и уникальность ключа проверки электронной

подписи, указанного заявителем для получения сертификата, подтверждена, Оператор УЦ на основании запроса на создание сертификата, представленного заявителем в виде электронного документа, осуществляет создание квалифицированного сертификата Пользователя УЦ с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации. В противном случае создание и выдача квалифицированного сертификата Пользователя УЦ не осуществляется и заявителю возвращаются представленные им документы с пояснением причин отказа. Удостоверяющий центр имеет право сохранить у себя копии документов, на основании которых было отказано заявителю в создании и выдаче квалифицированного сертификата.

5.5.6.7. Процедура создания квалифицированного сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра.

5.5.6.7.1. Создание квалифицированного сертификата Пользователя УЦ на основании запроса на создание сертификата, сформированного с использованием средств Удостоверяющего центра, осуществляется Удостоверяющим центром только при личном прибытии заявителя либо лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр в случае получения Удостоверяющим центром положительных результатов проверки документов и сведений, представленных заявителем, если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем, установлена личность заявителя – физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата. В противном случае создание и выдача квалифицированного сертификата Пользователя УЦ не осуществляется и заявителю возвращаются представленные им документы с пояснением причин отказа. Удостоверяющий центр имеет право сохранить у себя копии документов, на основании которых было отказано заявителю в создании и выдаче квалифицированного сертификата.

5.5.6.7.2. Для создания квалифицированного сертификата Пользователя УЦ Оператор УЦ осуществляет:

- проверку работоспособности ключевого носителя, представленного заявителем, в том числе его проверку на наличие вредоносного программного обеспечения или посторонней информации и, при необходимости, выполняет его инициализацию (форматирование), если он не был ранее проинициализирован;

- с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, осуществляет создание ключа электронной подписи и ключа проверки электронной подписи Пользователя УЦ в соответствии с пунктом 5.1.2 настоящего Порядка и в соответствии пунктом 5.4 настоящего Порядка, если выполняется смена ключа электронной подписи владельца сертификата. При создании ключа электронной подписи и ключа проверки

электронной подписи производится их запись непосредственно на ключевой носитель, представленный заявителем;

- одновременно с созданием ключа электронной подписи и ключа проверки электронной подписи Оператор УЦ осуществляет формирование запроса на создание сертификата в форме электронного документа, проверяет уникальность созданного ключа проверки электронной подписи, распечатывает на бумажном носителе сформированный запрос на создание сертификата на соответствующем бланке в двух экземплярах и предоставляет его для ознакомления и подписания лицу, обратившемуся за получением квалифицированного сертификата. Один экземпляр бланка запроса на создание сертификата, подписанного заявителем или лицом, выступающем от имени заявителя - юридического лица, остается в Удостоверяющем центра, другой его экземпляр передается заявителю или лицу, выступающему от имени заявителя - юридического лица;

- на основании сформированного в виде электронного документа запроса на создание сертификата, осуществляет создание квалифицированного сертификата Пользователя УЦ с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

5.5.6.7.3. Ознакомление под расписку лицом, обратившимся за получением квалифицированного сертификата, со сведениями, содержащимися в запросе на создание сертификата, и их соответствие со сведениями, содержащимися в заявлении на создание и выдачу квалифицированного сертификата и иных представленных заявителем документах, является одним из условий подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата.

5.5.7. Порядок выдачи квалифицированного сертификата.

5.5.7.1 Выдача квалифицированного сертификата, созданного в соответствии с пунктом 5.5.6, осуществляется Удостоверяющим центром в соответствии с положениями статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и настоящим Порядком. Заявителям, которым услуги Удостоверяющего центра оказываются в соответствии с заключенным договором, квалифицированные сертификаты выдаются при выполнении Стороной, присоединившейся к Порядку, обязанностей, предусмотренных настоящим Порядком и вышеуказанным договором.

5.5.7.2. Выдача квалифицированного сертификата, созданного Удостоверяющим центром, осуществляется при личном прибытии заявителя либо лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр.

5.5.7.3. Процедура выдачи квалифицированного сертификата, созданного Удостоверяющим центром.

После создания квалифицированного сертификата в соответствии с пунктом 5.5.6 настоящего Порядка, установления личности заявителя или лица, выступающего от имени заявителя - юридического лица, а также получения подтверждения их полномочий, с использованием средств Удостоверяющего центра, прошедших оценку

соответствия по требованиям безопасности информации, Оператор УЦ:

5.5.7.3.1 обеспечивает ознакомление заявителя под расписку с информацией, содержащейся в квалифицированном сертификате, в следующем порядке:

- распечатывает в двух экземплярах на бумажном носителе копию сертификата ключа проверки электронной подписи владельца сертификата, соответствующего электронной форме квалифицированного сертификата Пользователя УЦ (далее – бланк сертификата);

- предоставляет на ознакомление и подпись заявителю или лицу, выступающего от имени заявителя - юридического лица;

- заявитель или лицо, выступающее от имени заявителя - юридического лица, проверяет соответствие сведений, содержащихся в распечатанном бланке сертификата Пользователя УЦ и при успешной проверке сведений, заверяет его собственноручной подписью;

- один экземпляр заверенного бланка сертификата передается владельцу сертификата или лицу, выступающему от имени заявителя - юридического лица, другой экземпляр остается в Удостоверяющем центре;

5.5.7.3.2. в случае, если ключ электронной подписи создан с использованием средств Удостоверяющего центра:

- предоставляет владельцу сертификата парольную информацию, необходимую для получения доступа к ключу электронной подписи, содержащемся на ключевом носителе, а также информирует его о необходимости обязательной смены пароля доступа к ключевой информации. По согласованию с владельцем сертификата осуществляет тестирование работоспособности контейнера ключа электронной подписи, содержащейся на ключевом носителе, смену пароля доступа к нему, либо предоставляет эту возможность владельцу сертификата;

- передает владельцу сертификата или лицу, выступающему от имени заявителя - юридического лица ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи. Указанный ключевой носитель передается владельцу сертификата или его уполномоченному представителю под расписку и записью в соответствующих журналах поэкземплярного учета Удостоверяющего центра, в том числе журнале учета сертификатов ключей проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключа электронной подписи заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие заявителю;

5.5.7.3.3. по согласованию с владельцем сертификата осуществляет формирование ключевой фразы, которая в дальнейшем использоваться для аутентификации Пользователя УЦ при его обращении в Удостоверяющий центр;

5.5.7.3.4. выдает владельцу сертификата или лицу, выступающему от имени заявителя - юридического лица квалифицированный сертификат, созданный Удостоверяющим центром в форме электронного документа, квалифицированный сертификат Удостоверяющего центра и квалифицированный сертификат головного

удостоверяющего центра;

5.5.7.3.5. информирует под расписку владельца сертификата или лицо, выступающее от имени заявителя - юридического лица в письменной форме 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 руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 12 настоящего Порядка;

5.5.7.3.6. распечатывает на бумажном носителе краткое руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи и под расписку выдает его владельцу сертификата или лицу, выступающему от имени заявителя - юридического лица.

Указанное руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 12 настоящего Порядка, может быть направлено владельцу сертификата по электронной почте в форме электронного документа, при этом владелец сертификата подтверждает факт его получения, подписывая указанный электронный документ своей электронной подписью и направляя его в Удостоверяющий центр, либо направляя по электронной почте уведомление о прочтении, подписанное электронной подписью владельца сертификата. Получение Удостоверяющим центром указанного уведомления о прочтении является фактом, подтверждающим получение указанного электронного документа владельцем сертификата;

5.5.7.3.7. по согласованию с владельцем сертификата или лицу, выступающему от имени заявителя - юридического лица направляет владельцу сертификата или записывает на носитель информации, предоставленный заявителем, документацию в форме электронных документов, в том числе содержащую:

- руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 12 настоящего Порядка, содержащее информацию о 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;

- инструкцию по использованию средства электронной подписи, входящую в состав эксплуатационной документации на средство электронной подписи (по желанию владельца сертификата и при наличии в Удостоверяющем центре документации
на средство электронной подписи, которое использует владелец сертификата);

5.5.7.3.8. направляет в единую систему идентификации и аутентификации сведения о владельце сертификата, 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);

5.5.7.3.9. вносит в реестр сертификатов Удостоверяющего центра информацию о выданном квалифицированном сертификате и сведения о владельце сертификата;

5.5.7.3.10. по желанию владельца сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации.

5.5.8. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата заявителя.

5.5.8.1. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата заявителя с момента получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, а также надлежаще оформленных документов и сведений, представленных заявителем в Удостоверяющий центр для получения квалифицированного сертификата, зависит от сроков и результатов получения сведений, запрашиваемых Удостоверяющим центром с использованием инфраструктуры в соответствии частью 2.2 и частью 2.3 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ из государственных информационных ресурсов, но не может превышать 30 (тридцати) дней со дня получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, если иное не определено договором оказания услуг или дополнительным соглашением, заключаемым с заявителем.

5.5.8.2. Сроки проведения проверки достоверности документов и сведений, представленных заявителем, в том числе сроки уведомления заявителя со дня получения сведений из государственных информационных ресурсов приведены в пунктах 5.5.5 и 5.5.6 настоящего Порядка.

5.5.8.3. В случае, если Удостоверяющим центром был направлен запрос с использованием инфраструктуры в соответствии частью 2.2 и частью 2.3 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и сведения, подтверждающие достоверность информации, представленной заявителем для включения в квалифицированный сертификат, не получены Удостоверяющим центром в течение 30 (тридцати) дней со дня получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, Удостоверяющий центр отказывает заявителю в создании и выдаче квалифицированного сертификата.

5.5.8.4. В случае, если заявитель, после получения от Удостоверяющего центра уведомления о необходимости предоставления документов либо их надлежащим образом заверенные копий и сведений, необходимых для создания и выдачи квалифицированного сертификата, не представил их, Удостоверяющий центр по истечении 30 (тридцати) дней со дня получения Удостоверяющим центром соответствующего заявления на создание и выдачу квалифицированного сертификата отказывает в создании и выдаче

квалифицированного сертификата и направляет соответствующее уведомление заявителю.

5.5.8.5. Выдача квалифицированных сертификатов, созданных Удостоверяющим центром, осуществляется при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

5.5.8.6. Удостоверяющий центр не оказывает услуг по срочному выпуску квалифицированного сертификата, создание и выдача квалифицированного сертификата осуществляется в соответствии с требованиями Федерального закона «Об электронной подписи» от 06.04.2011 года №63-ФЗ и условиями, определенными настоящим Порядком.

5.6. Подтверждение действительности электронной подписи, использованной для подписания электронного документа.

По обращению участника электронного взаимодействия Удостоверяющий центр осуществляет проведение экспертных работ по проверке действительности усиленной квалифицированной электронной подписи, использованной для подписания электронных документов, созданного с использованием ключа электронной подписи, соответствующего квалифицированному сертификату, выданного Удостоверяющим центром.

5.6.1. Требования к заявлению на подтверждение действительности электронной подписи и перечень прилагаемых к такому заявлению документов.

5.6.1.1 Для подтверждения действительности электронной подписи участник электронного взаимодействия предоставляет в Удостоверяющий центр заявление на подтверждение действительности электронной подписи в электронном документе. Заявление предоставляется в Удостоверяющий центр в форме документа на бумажном носителе, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

5.6.1.2. Удостоверяющий центр обеспечивает проверку действительности электронной подписи в электронном документе в случае, если формат представления электронной подписи (формат представления электронного документа с электронной подписью) соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS) или стандарту PKCS #7. Решение о соответствии формата представления электронной подписи (формата представления электронного документа с электронной подписью) стандарту CMS или стандарту PKCS #7 принимает Удостоверяющий центр.

5.6.1.3. В случае, если заявителем является юридическое лицо, заявление оформляется по форме, приведенной в приложении № 6 к настоящему Порядку, на бланке организации (при наличии) и заверено печатью юридического лица, а также должно содержать:

5.6.1.3.1. реквизиты (дата и номер письма);

5.6.1.3.2. собственноручную подпись физического лица, действующее от имени юридического лица на основании учредительных документов юридического лица

или доверенности;

5.6.1.3.2. данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе, позволяющие однозначно определить квалифицированный сертификат, выданный Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе, либо серийный номер квалифицированного сертификата, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе;

5.6.1.3.4. дату и время подписания электронного документа электронной подписью, основанной на квалифицированном сертификате, выданный Удостоверяющим центром;

5.6.1.3.5. дату и время, на момент наступления которых требуется проверить действительность электронной подписи в электронном документе (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

5.6.1.4. В случае, если заявителем является физическое лицо, заявление оформляется по форме, приведенной в приложении № 7 к настоящему Порядку, и должно содержать:

5.6.1.4.1. собственноручную подпись физического лица и дату подписания;

5.6.1.4.2. данные владельца сертификата, электронную подпись которого необходимо проверить в электронном документе, позволяющие однозначно определить квалифицированный сертификат, выданный Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе, либо серийный номер квалифицированного сертификата, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе;

5.6.1.4.3. дату и время подписания электронного документа электронной подписью, основанной на квалифицированном сертификате, выданный Удостоверяющим центром;

5.6.1.4.4. дату и время, на момент наступления которых требуется проверить действительность электронной подписи в электронном документе (в том случае, если информация о дате и времени подписания электронного документа отсутствует).

5.6.1.5. Перечень документов, прилагаемых к заявлению на подтверждение действительности электронной подписи.

К заявлению на подтверждение действительности электронной подписи заявитель прилагает следующие документы в электронной форме:

- квалифицированный сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить действительность электронной подписи в электронном документе (в виде файла стандарта CMS или PKCS #7);

- электронный документ, подписанный электронной подписью, основанной

на квалифицированном сертификате, выданный Удостоверяющим центром (в виде одного файла стандарта CMS), либо электронный документ (в виде файла) и отдельно электронную подпись данного документа (в виде файла стандарта CMS или PKCS #7).

5.6.1.6. Удостоверяющий центр имеет право отказать заявителю в проведении проверки действительности электронной подписи в электронном документе в следующих случаях:

- заявитель не предоставил для проведения проверки действительности электронной подписи необходимые документы (файлы) или их формат не соответствует требованиям;

- заявление не соответствует требованиям, приведенным в пункте 5.6.1 настоящего Порядка, в том числе в случае, если заявление не оформлено надлежащим образом, не содержит необходимой информации или содержит трудноразличимый текст;

- квалифицированный сертификат, с использованием которого необходимо проверить действительность электронной подписи в электронном документе, выдан не Удостоверяющим центром.

В случае отказа в проведении проверки действительности электронной подписи в электронном документе Удостоверяющий центр в течение 1 (одного) рабочего дня после принятия решения об отказе направляет заявителю уведомление в форме документа на бумажном носителе, подписанного собственноручной подписью уполномоченного лица Удостоверяющего центра, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра, с информацией, содержащей причины отказа
в проведении проверки действительности электронной подписи в электронном документе.

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

Срок предоставления услуги по проверке действительности электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр, если иное не определено договором оказания услуг или дополнительным соглашением, заключаемым с заявителем.

5.6.3. Порядок оказания услуги по подтверждению действительности электронной подписи в электронном документе.

5.6.3.1. После поступления от заявителя заявления на подтверждение действительности электронной подписи в электронном документе и его регистрации в Удостоверяющем центре осуществляется проверка заявления и приложенных к нему документов.

5.6.3.2. Удостоверяющий центр, в случае отсутствия замечаний к представленным заявителем документам, в течение 2 (двух) рабочих дней со дня

получения от заявителя заявления на подтверждение действительности электронной подписи в электронном документе направляет заявителю предложение о заключении договора на оказание услуг по проведению экспертизы по проверке действительности электронной подписи в электронном документе.

5.6.3.3. В целях проведения экспертизы по проверке действительности электронной подписи в электронном документе создается комиссия, сформированная из числа сотрудников Удостоверяющего центра.

5.6.3.4. При проведении экспертизы по проверке действительности электронной подписи в электронном документе выполняется проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата Удостоверяющего центра, выданного ему головным удостоверяющим центром.

5.6.3.5. По результатам проведения экспертизы по проверке действительности электронной подписи в электронном документе комиссией составляется заключение, которое содержит:

- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку; основание для проведения проверки;
- данные, предоставленные комиссии для проведения проверки; вопросы, поставленные перед экспертом или комиссией;
- средства, используемые Удостоверяющим центром для проверки электронной подписи электронного документа;
- результат проверки электронной подписи электронного документа;
- выводы по поставленным вопросам, в том числе содержащий вывод о действительности (недействительности) электронной подписи в электронном документе и их обоснование.

5.6.3.6. Материалы и документы, сформированные в ходе работы комиссии, прилагаются к детальному отчёту и хранятся в Удостоверяющем центре.

5.6.3.7. Заключение комиссии по выполненной проверке составляется в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью. Один экземпляр заключения комиссии по выполненной проверке предоставляется заявителю. По согласованию с заявителем ему может быть направлена копия заключения комиссии в форме электронного документа, подписанного усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра.

5.6.4. Получение информации о статусе квалифицированного сертификата.

5.6.4.1. Владелец сертификата, заинтересованный в получении информации о статусе квалифицированного сертификата, выданного Удостоверяющим центром, имеют право направить в Удостоверяющий центр запрос в форме документа

на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

5.6.4.2. Получение информации о статусе сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром, осуществляется на основании заявления, которое оформляется по форме, приведенной в приложения № 8 или приложения № 9 к настоящему Порядку и предоставляется в Удостоверяющий центр в форме документа на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

5.6.4.3. Заявление должно содержать следующую информацию:

5.6.4.3.1. дата подачи заявления;

5.6.4.3.2. время и дата (либо период времени), на момент наступления которых требуется установить статус квалифицированного сертификата, выданного Удостоверяющим центром;

5.6.4.3.3. идентификационные данные владельца, статус квалифицированного сертификата которого требуется установить;

5.6.4.3.4. серийный номер квалифицированного сертификата, статус которого требуется установить.

5.6.4.4. По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе квалифицированного сертификата, которая предоставляется заявителю в форме в форме документа на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра.

5.6.4.5. Предоставление заявителю справки о статусе квалифицированного сертификата осуществляется Удостоверяющим центром не позднее 10 (десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

5.7. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата.

5.7.1. Основания прекращения действия или аннулирования квалифицированного сертификата.

5.7.1.1. Квалифицированный сертификат прекращения свое действие:

- в связи с истечением установленного срока действия квалифицированного сертификата; на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или соглашением (договором оказания услуг Удостоверяющего центра) с владельцем сертификата.

5.7.1.2. Удостоверяющий центр признает квалифицированный сертификат аннулированным, если в следующих случаях:

- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

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

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

5.7.2.1. Порядок подачи и приема заявления о прекращении действия квалифицированного сертификата

5.7.2.1.1. Порядок подачи в Удостоверяющий центр заявления о прекращении действия квалифицированного сертификата.

5.7.2.1.1.1. Заявитель имеет право предоставить в Удостоверяющий центр заявление о прекращении действия квалифицированного сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца сертификата.

5.7.2.1.1.2. Заявление о прекращении действия квалифицированного сертификата направляется заявителем в Удостоверяющий центр в случае:

- принятия Стороной, присоединившейся к Порядку, решения о прекращении действия квалифицированного сертификата владельца сертификата;

- договорные отношения, определенные настоящим Порядком, прекращаются по инициативе Стороны, присоединившейся к Порядку, в соответствии с пунктом 2.1.7 настоящего Порядка;

- изменились сведения о владельце сертификата, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными;

- прекращения полномочий владельца сертификата;

- нарушена конфиденциальность ключа электронной подписи владельца сертификата.

5.7.2.1.1.3. Требования к заявлению о прекращении действия квалифицированного сертификата.

Заявление о прекращении действия квалифицированного сертификата оформляется по форме, приведенной в приложении № 10 или приложения № 11 к настоящему Порядку, и должно соответствовать следующим требованиям:

5.7.2.1.1.3.1. В случае, если заявителем является юридическое лицо, заявление должно быть оформлено на бланке организации (при наличии) и заверено печатью юридического лица, а также содержать:

- сведения о квалифицированном сертификате, действие которого прекращается;

реквизиты (дата и номер письма);

- собственноручную подпись владельца сертификата.

5.7.2.1.1.3.2. В случае, если заявителем является физическое лицо, заявление должно содержать: сведения о квалифицированном сертификате, действие которого прекращается; собственноручную подпись физического лица, являющегося владельцем сертификата, и дату подписания заявления.

5.7.2.1.2. Порядок приема Удостоверяющим центром заявления о прекращении действия квалифицированного сертификата.

5.7.2.1.2.1. После поступления заявления о прекращении действия квалифицированного сертификата и его регистрации в Удостоверяющем центре осуществляется:

- проверка заявления на соответствие требованиям, указанным в пункте 5.7.2.1.1.3 настоящего Порядка;

- проверка соответствия сведений, указанных в заявлении, и сведений, которые имеются в Удостоверяющем центре о владельце сертификата и выданном ему квалифицированном сертификате;

- проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата.

5.7.2.1.2.2. Проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата, и удостоверение его личности и осуществляются в порядке, предусмотренном для процедуры создания и выдачи сертификата, приведенной в пункте 5.5 настоящего Порядка, с соблюдением следующих условий:

5.7.2.1.2.2.1. с заявлением о прекращении действия квалифицированного сертификата, владельцем которого является физическое лицо, имеет право обращаться указанное физическое лицо;

5.7.2.1.2.2.2. с заявлением о прекращении действия квалифицированного сертификата, владельцем которого является юридическое лицо или уполномоченный представитель юридического лица, имеет право обращаться физическое лицо, имеющее право действовать от имени этого юридического лица без доверенности.

Полномочия физического лица, имеющего право действовать от имени этого юридического лица без доверенности, подтверждаются Удостоверяющим центром с использованием инфраструктуры и актуальных сведений, полученных Удостоверяющим центром из государственных информационных ресурсов.

5.7.2.1.2.3. В случае, если заявление не соответствует условиям и требованиям в соответствии с пунктом 5.7.2.1 настоящего Порядка, в том числе в случае, если квалифицированный сертификат, сведения о котором указаны в заявлении о прекращении действия квалифицированного сертификата, не выдавался Удостоверяющим центром, либо сведения, указанные в заявлении, не соответствуют сведениям о владельце сертификата, либо не подтверждены полномочия владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия

квалифицированного сертификата, Удостоверяющий центр отказывает в проведении процедуры прекращения действия квалифицированного сертификата и направляет соответствующее уведомление заявителю в течение 1 (одного) рабочего дня с момента получения сведений из государственных информационных ресурсов, в случае, если полномочия лица, обращающегося для прекращения действия квалифицированного сертификата, не подтверждены, но не позднее 3 (трех) рабочих дней со дня получения заявления о прекращении действия квалифицированного сертификата.

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

5.7.2.2.1. После проверки заявления и полномочий владельца сертификата и (или) лица, обратившегося для прекращения действия квалифицированного сертификата, Удостоверяющий центр:

- выполняет процедуру прекращения действия квалифицированного сертификата; направляет в форме электронного документа соответствующее уведомление владельцу квалифицированного сертификата;

- вносит информацию о прекращении действия квалифицированного сертификата в реестр сертификатов Удостоверяющего центра.

5.7.2.2.2. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 5.7.1 настоящего Порядка, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно о наступлении таких обстоятельств.

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

5.7.2.2.4. Информация о прекращении действия и аннулировании квалифицированных сертификатов в течение 1 (одного) рабочего дня включается Удостоверяющим центром в список отозванных сертификатов, который подписывается электронной подписью, основанной на квалифицированном сертификате Удостоверяющего центра, и публикуется на сайте Удостоверяющего центра. Период публикации списка отозванных сертификатов составляет 24 (двадцать четыре) часа.

5.7.2.2.5. Информация о адресах публикации списка отозванных сертификатов указывается в квалифицированных сертификатах, созданных Удостоверяющим центром, и включается в расширение «Точка распределения списка отзыва» («CRL Distribution Point») квалифицированного сертификата.

5.7.2.2.6. Оповещение участников электронного взаимодействия о факте прекращения действия квалифицированного сертификата осуществляется Удостоверяющим центром путем опубликования первого (наиболее раннего) списка

отозванных сертификатов, содержащего сведения о квалифицированном сертификате, который аннулирован или действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем оповещения о прекращении действия квалифицированного сертификата является время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» («thisUpdate») списка отозванных сертификатов.

5.7.2.2.7. В случае прекращения действия квалифицированного сертификата по истечению срока его действия временем прекращения действия квалифицированного сертификата является время, хранящееся в поле «Действителен по» («NotAfter») квалифицированного сертификата. В этом случае информация о квалифицированном сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

5.7.2.2.8. В случае внеплановой смены ключа электронной подписи Удостоверяющего центра в связи с нарушением его конфиденциальности временем прекращения действия квалифицированного сертификата Удостоверяющего центра является время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, при этом прекращение действия квалифицированного сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия квалифицированного сертификата Удостоверяющего центра включается в список отозванных сертификатов, который публикуется головным удостоверяющим центром.

5.7.2.3. В случае аннулирования в соответствии с пунктом 5.7.1.2 настоящего Порядка квалифицированного сертификата, выданного Удостоверяющим центром, Удостоверяющий центр уведомляет владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра.

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

5.8. Порядок ведения реестра сертификатов Удостоверяющего центра.

5.8.1. Формирование и ведение реестра сертификатов Удостоверяющего центра.

5.8.1.1. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Федеральным законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22.08.2017 года № 436, иными принимаемыми в соответствии с Федеральными законами нормативными правовыми актами и настоящим Порядком.

5.8.1.2. Формирование реестра сертификатов включает в себя внесение квалифицированных сертификатов, выданных Удостоверяющим центром, в реестр сертификатов.

5.8.1.3. Ведение реестра сертификатов включает в себя:

- внесение изменений в реестр сертификатов в случае изменения содержащихся в нем сведений;

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

5.8.1.4. Хранение информации, содержащейся в реестре сертификатов, осуществляется Удостоверяющим центром в форме, позволяющей проверить ее целостность и достоверность.

5.8.1.5. Удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

5.8.1.6. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром с соблюдением требований к мерам и способам защиты информации, обеспечивающих предотвращение несанкционированного доступа к нему.

5.8.1.7. В целях обеспечения целостности информации, в том числе предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре сертификатов, Удостоверяющий центр осуществляет резервной копирование баз данных, обрабатываемых с использованием сертифицированных средств Удостоверяющего центра, а также реестра сертификатов.

5.8.1.8. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

5.8.1.9. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности Удостоверяющего центра. Актуальный реестр сертификатов в электронной форме ежедневно публикуется на сайте Удостоверяющего центра.

5.8.1.10. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как в форме документа на бумажном носителе с использованием почтового отправления, так и с в форме электронного документа использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты (по выбору лица, обратившегося за получением информации из реестра сертификатов).

Срок предоставления Удостоверяющим центром запрошенной заявителем информации, содержащейся в реестре сертификатов, не превышает 7 (семи) дней со дня

получения запроса от заявителя, в случае, если Удостоверяющий центр направляет запрошенную информацию в форме документа на бумажном носителе с использованием почтового отправления, и 24 (двадцати четырех) часов для направления выписки посредством информационно- телекоммуникационных сетей, в том числе с использованием электронной почты.

5.8.1.11. В процессе реализации функций Удостоверяющего центра и исполнения обязанностей Удостоверяющий центр осуществляет также формирование и ведение:

5.8.1.11.1. реестра Пользователей УЦ, который в том числе содержит:

- информацию о Пользователях УЦ, владельцах сертификатов, выданных им квалифицированных сертификатах, в том числе прекративших действие и аннулированных сертификатах;
- реестр запросов на создание Пользователей УЦ, квалифицированных сертификатов, а также запросов на прекращение их действия (аннулирование);
- реестр списка отозванных сертификатов в электронном виде за все время деятельности Удостоверяющего центра.

Реестр Пользователей УЦ ведется в электронном виде с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации;

5.8.1.11.2. журнала учета сертификатов ключей проверки электронной подписи, соответствующего форме журнала поэкземплярного учета, приведенной в приложении № 1 Инструкции ФАПСИ № 152, в том числе содержащего информацию о серийном номере сертификата, выдаче сертификата, прекращении его действия, основания выдачи или прекращении его действия, о лице, получившем и выдавшем сертификат. Журнал учета сертификатов ключей проверки электронной подписи ведется в электронном и бумажном виде.

5.8.1.11.3. реестра лицевых счетов владельцев сертификатов в бумажном и электронном виде, содержащий документы и сведения, предоставляемые заявителями, а также документы и сведения, направленные в их адрес Удостоверяющим центром.

5.8.1.12. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

5.8.1.13. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан передать в уполномоченный федеральный орган реестр сертификатов в соответствии с Порядком 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, утвержденным приказом Минкомсвязи России от 14.08.2017 года № 416.

5.8.2. Формы ведения реестра сертификатов.

Реестр сертификатов Удостоверяющего центра включает реестр сертификатов

юридических лиц и реестр сертификатов физических лиц.

5.8.2.1. Реестр сертификатов юридических лиц состоит из следующих разделов:

- квалифицированные сертификаты, выданные юридическим лицам;
- квалифицированные сертификаты, выданные юридическим лицам, прекратившие свое действие;
- аннулированные квалифицированные сертификаты, выданные юридическим лицам.

5.8.2.1.1. Раздел «квалифицированные сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- реквизиты документа, подтверждающего факт внесения записи в Единый государственный реестр юридических лиц (для юридических лиц, зарегистрированных на территории Российской Федерации);
- основные реквизиты (наименование, номер и дата выдачи) доверенности или иного документа, подтверждающего право заявителя действовать от имени других лиц;
- 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;
- ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

5.8.2.1.2. Раздел «квалифицированные сертификаты, выданные юридическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- дата прекращения действия квалифицированного сертификата;
- основание прекращения действия квалифицированного сертификата.

5.8.2.1.3. Раздел «аннулированные квалифицированные сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;

- дата аннулирования квалифицированного сертификата;

- основание аннулирования квалифицированного сертификата.

5.8.2.2. Реестр сертификатов физических лиц состоит из следующих разделов:

- квалифицированные сертификаты, выданные физическим лицам;

- квалифицированные сертификаты, выданные физическим лицам, прекратившие свое действие;

- аннулированные квалифицированные сертификаты, выданные физическим лицам.

5.8.2.2.1. Раздел «квалифицированные сертификаты, выданные физическим лицам» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;

- даты начала и окончания действия квалифицированного сертификата;

- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;

- страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца 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;

- ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

5.8.2.2.2. Раздел «квалифицированные сертификаты, выданные физическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;

- даты начала и окончания действия квалифицированного сертификата;

- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;

- дата прекращения действия квалифицированного сертификата;

- основание прекращения действия квалифицированного сертификата.

5.8.2.2.3. Раздел «аннулированные квалифицированные, выданные физическим лицам» содержит следующие обязательные поля:

- уникальный номер квалифицированного сертификата;

- даты начала и окончания действия квалифицированного сертификата;

- фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;

- дата аннулирования квалифицированного сертификата;

- основание аннулирования квалифицированного сертификата.

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

5.8.3.1. Информация о выданных Удостоверяющим центром

квалифицированных сертификатах вносится в реестр сертификатов одновременно с их выдачей, но не позднее даты начала действия квалифицированного сертификата, указанной
в квалифицированном сертификате.

5.8.3.2. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 5.7.1 настоящего Порядка, или в течение
12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

5.8.3.3. Информация об аннулировании квалифицированного сертификата вносится Удостоверяющим центров в реестр сертификатов не позднее 1 (одного) рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании Удостоверяющим центром квалифицированных сертификатов по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ:

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

- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате.

5.8.3.4. В случае аннулирования в соответствии с пунктом 5.7.1.2 настоящего Порядка квалифицированного сертификата, выданного Удостоверяющим центром, Удостоверяющий центр уведомляет владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра

5.9. Порядок технического обслуживания реестра квалифицированных сертификатов.

Плановые технические работы по обслуживанию реестра сертификатов, в том числе процедуры резервного копирования, проводятся Удостоверяющим центром в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации) с целью минимизации и возможности исключения перерывов в работе
при использовании квалифицированных сертификатов и в возможности получения доступа к реестру сертификатов Удостоверяющего центра, опубликованному на сайте Удостоверяющего центра.

Внеплановые технические работы по обслуживанию реестра сертификатов проводятся в оперативном режиме, при появлении такой необходимости.

5.9.1. Максимальные сроки проведения технического обслуживания.

Техническое обслуживание реестра сертификатов при проведении плановых технических работ осуществляется не более 8 (восьми) часов с момента их начала.

Техническое обслуживание реестра сертификатов при проведении внеплановых технических работ осуществляется не более 24 (двадцати четырех) часов с момента их начала. Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин, но не более чем на 5 (пять) дней со дня их начала, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия.

5.9.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания.

Перед проведением работ по техническому обслуживанию реестра сертификатов, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия, Удостоверяющий центр оповещает о проведении вышеуказанных работ посредством публикации соответствующей информации на сайте Удостоверяющего центра и (или) направлением уведомления в электронной форме с использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

6. Порядок исполнения обязанностей Удостоверяющего центра

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.

6.1.1 Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, приведено в приложении № 12 к настоящему Порядку.

6.1.2. Удостоверяющий центр осуществляет информирование Стороны, присоединившейся к Порядку, в том числе Пользователей УЦ и владельцев сертификатов, 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 следующими способами:

6.1.2.1. Удостоверяющий центр информирует всех участников электронного взаимодействия об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путем размещения настоящего Порядка, а также руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, которое приведено в приложении № 12 к настоящему Порядку, отдельным документом в электронной форме на сайте Удостоверяющего центра;

6.1.2.2. Сторона, присоединившаяся к Порядку, обязана ознакомится с настоящим Порядком и всеми приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи,о чем подтверждает путем подписания заявления о присоединении к Порядку, по форме, приведенной в приложении № 1 или приложении № 2 к настоящему Порядку;

6.1.2.3. заявитель, при оформлении заявления на создание и выдачу квалифицированного сертификата по форме, приведенной в приложении № 3 или приложении № 4 к настоящему Порядку предоставляет также согласие на обработку персональных данных, которое собственноручно подписывает лицо, указанное в заявлении на создание и выдачу квалифицированного сертификата, в том числе подтверждает, что с настоящим Порядком и всеми приложениями к нему, в том числе с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен;

6.1.2.4. При выдаче квалифицированного сертификата в соответствии с пунктом

5.5.7.3, Удостоверяющий центр одновременно с выдачей квалифицированного сертификата информирует лицо, обратившееся за получением квалифицированного сертификата, 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, и под расписку выдает краткое руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, а также, по согласованию с владельцем сертификата или его уполномоченным представителем, направляет владельцу сертификата или записывает на носитель информации, предоставленный заявителем, документацию в форме электронных документов, в том числе содержащую:

- руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 12 к настоящему Порядку, содержащее информацию о 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;

- инструкцию по использованию средства электронной подписи, входящую в состав эксплуатационной документации на средство электронной подписи (по желанию владельца сертификата и при наличии в Удостоверяющем центре документации
на средство электронной подписи, которое использует владелец сертификата);

6.1.2.5. Удостоверяющий центр оказывает техническую поддержку Пользователей УЦ и осуществляет предоставление консультаций по вопросам использования электронной подписи и средств электронной подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи.

6.2. Выдача по обращению заявителя средств электронной подписи.

6.2.1. Средства электронной подписи, используемые заявителем, должны соответствовать требованиям частью 4 статьи 6 и статьи 12 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, Требованиями к средствам электронной подписи, утвержденными приказом ФСБ России от 27.12.2011 года № 796, а также 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.

6.2.2. Выдача Удостоверяющим центром сертифицированных по требованиям безопасности средств электронной подписи заключается в:

- консультировании Пользователей УЦ по вопросам получения по доверенным

каналам распространения от производителей данных средств, обеспечивающих возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

- выдаче средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи;

- выдаче лицензий на право использования средств электронной подписи на возмездной основе.

6.2.3. Выдача и распространение сертифицированных средств электронной подписи и эксплуатационной документации к ним осуществляется Удостоверяющим центром на основании положений, приведенных в пункте 2.2.1 настоящего Порядка, в соответствии с требованиями Инструкция ФАПСИ № 152. Факт выдачи заявителям сертифицированных средств электронной подписи и эксплуатационной документации к ним учитывается в соответствующих журналах поэкземплярного учета Удостоверяющего центра.

6.2.4. Если лицензионным соглашением, условия которой определил правообладатель (производитель) средства электронной подписи, правообладателем предоставлена возможность бесплатного использования средства электронной подписи без необходимости приобретения права использования продукта на условиях простой (неисключительной) лицензии, либо использования без установки ключа (лицензионного номера), либо предоставлена возможность его использования в рамках ограниченного периода времени в целях демонстрации программного продукта и ознакомления пользователя с его возможностями, Удостоверяющий центр имеет право, в рамках лицензионного соглашения, безвозмездно передать заявителю средство электронной подписи, которое есть в наличии в Удостоверяющем центре, и которое соответствует требованиям, указанным в пункте 6.2.1 настоящего Порядка, либо предоставить заявителю информацию о сайте правообладателя (производителя) в сети Интернет,в том числе информацию, содержащую условия лицензионного соглашения и информацию (при её наличии) о возможности ознакомления с программным продуктом, соответствующим требованиям к сертифицированным средствам электронной подписи.

6.2.5. Порядок использования средств электронной подписи определяются эксплуатационной документацией на средство электронной подписи и лицензионным соглашением, условия которой определяет правообладатель.

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

6.3.1. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

6.3.2. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем соблюдения порядка формирования и ведения реестра сертификатов в соответствии с пунктом 5.8 настоящего Порядка.

6.3.3. Защита информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой
с использованием средств Удостоверяющего центра, которые в том числе включают меры по защите информации, содержащейся в реестре сертификатов.

6.3.4. Мероприятия по обеспечению защиты информации, при её обработке с использованием средств Удостоверяющего центра, осуществляются в том числе в соответствии с требованиями Федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 года № 17, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 года № 21, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных
для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 года № 378, Требованиями к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, Инструкцией ФАПСИ № 152.

6.3.5. Обработка информации осуществляется с использованием средств Удостоверяющего центра, соответствующих Требованиям к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27.12.2011 года № 796, прошедших оценку соответствия по требованиям безопасности информации.

6.3.6. Защита информации, содержащейся в реестре сертификатов Удостоверяющего центра, осуществляется, в частности, путем реализации следующих мероприятий:

- обеспечивается контроль доступа в помещения, где размещены технические средства Удостоверяющего центра;

- реализована ролевая модель доступа к компонентам средств Удостоверяющего

центра, обеспечивается идентификация, аутентификация и разграничение доступа уполномоченных лиц к программным и техническим средствам Удостоверяющего центра и защищаемой информации;

- обеспечивается контроль действий уполномоченных лиц Удостоверяющего центра и обслуживающего персонала, приняты меры по предотвращению несанкционированного доступа к средствам Удостоверяющего центра и защищаемой информации;

- формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему;

- осуществляется регулярное резервное копирование информации, содержащейся в реестре сертификатов с соблюдением требований к защите от несанкционированного доступа к средствам резервного копирования и резервируемой информации;

- для хранения информации используются опечатываемые хранилища информации (металлические шкафы, сейфы, пеналы).

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

6.4.1. Удостоверяющий центр в соответствии с пунктом 3 части 2 статьи 13 и частью 3 статьи 15 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ обеспечивает безвозмездный круглосуточный доступ к реестру сертификатов, опубликованному на сайте Удостоверяющего центра, при обращении к нему любого лица с использованием сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов, проводимых Удостоверяющим центром в соответствии с пунктом 5.9 настоящего Порядка.

6.4.2. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов в соответствии с пунктом 5.8.1.10 настоящего Порядка.

6.4.3. В соответствии с «Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи», а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22.08.2017 года № 436, доступ заинтересованных лиц к реестру квалифицированных сертификатов с использованием информационно-телекоммуникационных сетей осуществляется путем размещения, формирования и ведения реестра квалифицированных сертификатов в информационной системе Головного Удостоверяющего центра, являющейся составной частью инфраструктуры, обеспечивающей информационно - технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Доступ заинтересованных лиц к информационной системе Головного

Удостоверяющего центра с целью получения сведений из реестра квалифицированных сертификатов осуществляется с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» на безвозмездной основе.

6.4.4 Удостоверяющий центр обеспечивает доступность и целостность информации, опубликованной на сайте Удостоверяющего центра, в том числе реестра сертификатов, квалифицированных сертификатов Удостоверяющего центра, списка отозванных сертификатов.

6.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

6.5.1. Порядок обеспечения конфиденциальности ключей электронных подписей уполномоченных лиц Удостоверяющего центра и ключа электронной подписи Удостоверяющего центра.

6.5.1.1. Конфиденциальность ключей электронных подписей уполномоченных лиц Удостоверяющего центра, а также ключа электронной подписи Удостоверяющего центра, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра.

6.5.1.2. Хранение и использование ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра осуществляется в соответствии с требованиями с Инструкции ФАПСИ № 152, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 02.03.2001 года № 28, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

6.5.1.3. Средства Удостоверяющего центра, с использованием которых осуществляется использование и хранение ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра, имеют документ, подтверждающий оценку соответствия по требованиям безопасности информации и соответствуют «Требованиям к средствам электронной подписи» и «Требованиями к средствам удостоверяющего центра», утвержденными приказом ФСБ России от 27.12.2011 года № 796.

6.5.1.4. Ключи электронной подписи Удостоверяющего центра и уполномоченных лиц Удостоверяющего центра выводятся из эксплуатации при окончании срока их действия. Временное их хранение не осуществляется.

6.5.2. Порядок обеспечения конфиденциальности ключей электронных подписей заявителей.

6.5.2.1. Конфиденциальность ключей электронных подписей заявителей обеспечивается Удостоверяющим центром в период времени получения носителя ключевой информации от заявителя или лица, выступающего от имени заявителя -

юридического лица и записи на него ключей электронной подписи, созданных Удостоверяющим центром, до момента передачи ключевого носителя заявителю или лицу, выступающему от имени заявителя - юридического лица, при этом создание и запись ключа электронной подписи на ключевой носитель, представленный заявителем или его уполномоченным представителем осуществляется Удостоверяющим центром только в случае личного прибытия заявителя или лица, выступающего от имени заявителя - юридического лица в Удостоверяющий центр и в его присутствии.

6.5.2.2. Выдача ключей электронной подписи заявителю или лицу, выступающему от имени заявителя - юридического лица осуществляется Удостоверяющим центром в порядке, определенном в пункте 5.1.2 и 5.5.7.3 настоящего Порядка.

6.5.2.3. После создания Удостоверяющим центром ключа электронных подписи заявителя и его записи на носитель ключевой информации, представленный непосредственно перед созданием ключа электронных подписи заявителем или его уполномоченным представителем, данный носитель ключевой информации, в том числе содержащий ключ электронной подписи, выдается заявителю или лицу, выступающему от имени заявителя - юридического лица под расписку, при этом вносится запись в соответствующий журнал учета Удостоверяющего центра о выдаче ключа электронной подписи и соответствующего ему квалифицированного сертификата, с которой заявитель или лицо, выступающее от имени заявителя - юридического лица должен быть ознакомлен под расписку.

6.5.2.4. Создание ключей электронной подписи заявителя осуществляется с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

6.5.2.5. Удостоверяющий центр не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи заявителя (владельца сертификата).

6.5.2.6. В случае, если заявитель направил в Удостоверяющий в электронном виде ключ электронной подписи по информационно - телекоммуникационной сети или иными способами, не гарантирующими обеспечение конфиденциальности ключа электронной подписи, такой ключ считается скомпрометированным в связи нарушением конфиденциальность ключа электронной подписи, при этом заявитель обязан провести процедуру его внеплановой смены. В случае наличия действующего квалифицированного сертификата, соответствующего указанному ключу электронной подписи, такой квалифицированный сертификат прекращает действие, при этом владелец сертификата обязан обратится в Удостоверяющий центр с заявлением о прекращении его действия в соответствии с пунктом 5.4.3 и 5.7.1 настоящего Порядка.

6.5.2.7. Владелец сертификата, получивший квалифицированный сертификат в Удостоверяющем центре обеспечивает конфиденциальность ключей электронных

подписей и обязан:

- хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;

- не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;

- уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

- не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

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

6.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации.

6.6.1. Удостоверяющий центр непосредственно после выдачи квалифицированного сертификата владельцу сертификата или лицу, выступающему от имени заявителя - юридического лица осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ.

6.6.2. При выдаче квалифицированного сертификата Удостоверяющий центр с использованием специализированного программного обеспечения и инфраструктуры осуществляет регистрацию выданного квалифицированного сертификата в единой системе идентификации и аутентификации, для чего направляет в единую систему идентификации и аутентификации сведения о владельце сертификата, в объеме, необходимом для регистрации квалифицированного сертификата в единой системе идентификации и аутентификации сведений о владельце сертификата, и о полученном им квалифицированном сертификате, в том числе:

- уникальный серийный номер квалифицированного сертификата;

- тип владельца квалифицированного сертификата (физическое лицо, индивидуальный предприниматель, должностное (уполномоченное) лицо, информационная система);

- даты начала и окончания действия квалифицированного сертификата;

- наименование Удостоверяющего центра, выдавшего квалифицированный сертификат;

- Фамилия, Имя и Отчество владельца квалифицированного сертификата – для физических лиц, индивидуальных предпринимателей и должностных

(уполномоченных) лиц;

- номер страхового свидетельства государственного пенсионного страхования заявителя физического лица, являющегося владельца квалифицированного сертификата (для физических лиц, индивидуальных предпринимателей, должностных (уполномоченных) лиц);

- идентификационный номер налогоплательщика – юридического лица;

- реквизиты документа, удостоверяющего личность владельца квалифицированного сертификата, в том числе серия и номер документа, удостоверяющего личность, код подразделения, выдавшего документ, дата выдачи – для физических лиц, индивидуальных предпринимателей и должностных (уполномоченных) лиц;

- адрес регистрации (места жительства) – для физических лиц;

- пол владельца квалифицированного сертификата – для физических лиц, индивидуальных предпринимателей и должностных (уполномоченных) лиц;

- дата рождения владельца квалифицированного сертификата – для физических лиц, индивидуальных предпринимателей и должностных (уполномоченных) лиц;

- место рождения владельца квалифицированного сертификата – для физических лиц, индивидуальных предпринимателей и должностных (уполномоченных) лиц;

- гражданство владельца квалифицированного сертификата – для физических лиц, индивидуальных предпринимателей и должностных (уполномоченных) лиц;

- основной государственный регистрационный номер юридического лица;

- основной государственный регистрационный номер индивидуального предпринимателя;

- идентификационный номер налогоплательщика (физического лица);

- адрес электронной почты;

- номер мобильного телефона (только при регистрации или подтверждении его учетной записи владельца сертификата – физического лица при его желании в единой системе идентификации и аутентификации).

6.6.3. В соответствии с требованиями статьи 6 и статьи 9 Федерального закона «О персональных данных» от 27.07.2006 года № 152-ФЗ Удостоверяющий центр осуществляет регистрацию в единой системе идентификации и аутентификации лица, которое указанное в предоставляемом заявителем заявлении на создание и выдачу квалифицированного сертификата (владелец сертификата), в соответствии с предоставляемым этим лицом согласием на обработку персональных данных, приведенным в приложении № 3 и приложении № 4 к настоящему Порядку.

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

6.7.1. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию владельца сертификата (физического лица) безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации

и (или) осуществляет подтверждение учетной записи физического лица в единой системе идентификации и аутентификации.

6.7.2. Основанием для регистрации или подтверждения учетной записи служит заявление владельца сертификата, содержащее сведения необходимые для регистрации или подтверждения учетной записи в единой системе идентификации и аутентификации, а также согласие на обработку персональных данных, предоставляемое владельцем сертификата. Форма соответствующих заявлений предоставляется Удостоверяющим центром при выполнении процедуры регистрации владельца сертификата в единой системе идентификации и аутентификации или подтверждения его учетной записи, которая осуществляется Удостоверяющим центром при личном прибытии владельца сертификата в Удостоверяющий центр.

6.7.3. Результатом регистрации лица в единой системе идентификации и аутентификации или подтверждения его учетной записи является соответственно выдача этому лицу пароля для первого входа в единую систему идентификации и аутентификации или подтверждение его учетной записи в единой системе идентификации и аутентификации.

6.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре сертификатов.

6.8.1. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации, содержащейся в реестре сертификатов Удостоверяющего центра, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата путем публикации реестра сертификатов на сайте Удостоверяющего центра в форме электронного документа, который доступен для загрузки с использованием сети Интернет.

6.8.2. Актуальность и доступность реестра квалифицированных сертификатов, опубликованного на сайте Удостоверяющего центра в сети Интернет обеспечивается Удостоверяющим центром в соответствии с пунктом 6.3 и 6.4 настоящего Порядка соответственно.

6.8.3. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов в соответствии с пунктом 5.8.1.10 настоящего Порядка.

6.8.4. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, путем публикации актуального перечня прекративших свое действие (аннулированных) квалифицированных сертификатов в виде электронного документа (списка отозванных сертификатов), включающий в себя список серийных номеров квалифицированных сертификатов, которые аннулированы или действие которых было прекращено.

6.8.5. В целях обеспечения гарантированного доступа участников электронного

взаимодействия к списку отозванных сертификатов Удостоверяющим центр обеспечивается публикация списка отозванных сертификатов на не менее чем двух независимых друг от друга ресурсах, размещаемых в сети Интернет, доступ к которым неограничен.

6.8.6. Адреса публикации списка отозванных сертификатов Удостоверяющего центра указывается в квалифицированных сертификатах, созданных Удостоверяющим центром.

6.8.7. Внесение информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов осуществляется Удостоверяющим центром в соответствии с пунктом 5.7.2.2 настоящего Порядка.

7. Прочие положения

7.1. Прекращение деятельности Удостоверяющего центра.

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

В случае прекращения своей деятельности Удостоверяющий центр обязан:

- сообщить об этом в уполномоченный федеральный орган не позднее чем за 1 (один) месяц до даты прекращения своей деятельности;
- уведомить владельцев сертификатов ключей проверки электронной подписи, срок действия которых не истек, не позднее чем за 1 (один) месяц до даты прекращения своей деятельности;
- передать в уполномоченный федеральный орган в установленном порядке реестр сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в Удостоверяющем центре.

Передача реестра сертификатов и информации, подлежащей хранению в Удостоверяющем центре, осуществляется в соответствии с Порядком 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, утвержденным приказом Минкомсвязи России от 14.08.2017 года № 416.

7.2. Политика конфиденциальности.

7.2.1. Типы конфиденциальной информации.

К конфиденциальной информации, обрабатываемой в Удостоверяющем центре, относится:

7.2.1.1. информация, обрабатываемая с использованием средств Удостоверяющего центра:

- ключи электронной подписи Удостоверяющего центра и ключи электронной

подписи уполномоченных лиц Удостоверяющего центра;

- сведения о мерах и способах защиты инфраструктуры Удостоверяющего центра, включая идентифицирующую и аутентифицирующую информацию, информацию

о среде функционирования технических и программных средств Удостоверяющего центра, средств защиты информации и шифровальных (криптографических) средств;

- техническая и эксплуатационная документация Удостоверяющего центра, в том числе содержащая информация о настройках средств Удостоверяющего центра, средств защиты информации, средств межсетевого экранирования, средств криптографической защиты информации;

7.2.1.2. информация, содержащая персональные данные, за исключением:

- сведений, включаемых в квалифицированный сертификат, выданный Удостоверяющим центром;

- информации, содержащейся в реестре сертификатов;

- общедоступной информации и информации, включенной в общедоступные источники персональных данных.

7.2.1.3. ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего квалифицированного сертификата, выданного ему Удостоверяющим центром. Удостоверяющий центр не осуществляет хранение ключей электронных подписей владельцев сертификатов, в том числе их временное хранение. Ключи электронной подписи, создаваемые Удостоверяющим центром при личном присутствии заявителя или лицу, выступающему от имени заявителя - юридического лица, непосредственно сразу после их изготовления передаются лично заявителю или лицу, выступающему от имени заявителя - юридического лица под расписку.

7.2.2. Типы информации, не являющейся конфиденциальной.

Удостоверяющий центр осуществляет обработку следующей информации, которая не является конфиденциальной:

7.2.2.1. информация, подлежащая в соответствии с законодательством Российской Федерации размещению в сети Интернет, доступ к которой не ограничен, в том числе информация, являющаяся общедоступной информацией в соответствии со статьей 7 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года № 149-ФЗ или информация, включенная в общедоступные источники персональных данных в соответствии со статьей 8 Федерального закона «О персональных данных» от 27.07.2006 года № 152-ФЗ, а также информация с письменного согласия субъекта персональных данных включенная в общедоступные источники персональных данных;

7.2.2.2. информация, включаемая в квалифицированные сертификаты, выдаваемые Удостоверяющим центром, информация, содержащейся в реестре сертификатов, а также информация, включаемая в списки отозванных сертификатов Удостоверяющего центра;

7.2.2.3. информация, содержащаяся в настоящем Порядке.

7.2.3. Типы информации, не подлежащей публикации.

Не подлежит публикации следующая информация о заявителях и владельцах сертификатов:

7.2.3.1. сведения, направляемые Удостоверяющим центром в единую систему идентификации и аутентификации, в объеме, необходимом для регистрации сведений о владельце сертификата в единой системе идентификации и аутентификации, а также для регистрации или подтверждения учетной записи владельца сертификата (по желанию физического лица) в единой системе идентификации и аутентификации, содержащие серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, номер мобильного телефона. Вышеуказанные сведения являются персональными данными владельца сертификата (физического лица), обрабатываемыми Удостоверяющим центром в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и согласием на обработку персональных данных, предоставляемым указанным физическим лицом;

7.2.3.2. сведения, содержащиеся в договорах на оказание услуг, заключаемых заявителем с Удостоверяющим центром, заявлениях, доверенностях, согласии на обработку персональных данных и иных документах, предоставляемых заявителем в Удостоверяющий центр, за исключением информации не являющейся конфиденциальной, указанной в пункте 7.2.2 настоящего Порядка.

7.2.4. Обеспечение конфиденциальности.

Сведения, относящиеся к конфиденциальной информации в соответствии с действующим законодательством Российской Федерации и настоящим Порядком, полученные Удостоверяющим центром или Стороной, присоединившейся к Порядку, в целях оказания или получения услуг в соответствии с настоящим Порядком, не подлежат разглашению, распространению и передаче третьим лицам, если иное не оговорено особо, а также в случаях, предусмотренных законодательством Российской Федерации, настоящим Порядком, договором оказания услуг Удостоверяющего центра или соглашением Сторон.

Приложение № 1
к Порядку реализации функций аккредитованного
Удостоверяющего центра
общества с ограниченной ответственностью «Модум»
(Форма заявления о присоединении к Порядку
для юридических лиц)[1]

Заявление о присоединении к Порядку
Удостоверяющего центра ООО «Модум»

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

_____
(полное наименование юридического лица, включая организационно-правовую форму)

ИНН _____ ОГРН _____

в лице _____
(должность, фамилия, имя, отчество)

действующего на основании _____
в соответствии со статьей 428 Гражданского кодекса Российской Федерации присоединяется к Порядку реализации функций аккредитованного удостоверяющего центра Общество с ограниченной ответственностью «Модум» и исполнения его обязанностей (далее – Порядок), опубликованному на сайте Удостоверяющего центра общества с ограниченной ответственностью «Модум» в информационно-телекоммуникационной сети «Интернет» по адресу http://modum.pro.

Уполномоченные лица _____
(сокращенное наименование организации)

регистрирующиеся в удостоверяющем центре общество с ограниченной ответственностью «Модум», с Порядком и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлены и обязуются соблюдать все его положения.

_____/_____/_____
(должность) (подпись) (расшифровка подписи)

М.П.

(заполняется уполномоченным лицом Удостоверяющего центра)

1 Заявление подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления

в Удостоверяющем центре один экземпляр предоставляется заявителю

Данное заявление зарегистрировано в реестре Удостоверяющего центра в качестве договора присоединении к Порядку реализации функций аккредитованного удостоверяющего центра Общество с ограниченной ответственностью «Модум» и исполнения его обязанностей.

Регистрационный № _____ от «____»_____ 20____г.

Уполномоченное лицо Удостоверяющего центра общества с ограниченной ответственностью «Модум» _____/_____/
(подпись) (расшифровка подписи)

М.П

Приложение № 2
к Порядку реализации функций аккредитованного
Удостоверяющего центра
общества с ограниченной ответственностью «Модум»
(Форма заявления о присоединении к Порядку
для физических лиц и индивидуальных предпринимателей)[1]

Заявление о присоединении к Порядку
Удостоверяющего центра ООО «Модум»

г. Москва

Удостоверяющий центр
ООО «Модум»

Я, _____
(фамилия, имя, отчество)

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

_____
(адрес места регистрации и проживания)

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Порядку реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум» (далее – Порядок), опубликованному на сайте Удостоверяющего центра общества с ограниченной ответственностью «Модум» в информационно- телекоммуникационной сети «Интернет» по адресу http://modum.pro, с Порядком и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен и обязуюсь соблюдать все его положения.

_____/_____ «____»_____20____г.
подпись Ф.И.О.

М.П.

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное заявление зарегистрировано в реестре Удостоверяющего центра в качестве договора присоединении к Порядку реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум» и исполнения его обязанностей.

Регистрационный № _____ от «____»_____20____г.

Уполномоченное лицо Удостоверяющего центра общества с ограниченной ответственностью «Модум» _____/_____/
(подпись) (расшифровка подписи)

М.П

1 Заявление подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Приложение № 3
к Порядку реализации функций аккредитованного
Удостоверяющего центра
общества с ограниченной ответственностью «Модум»
(Форма заявления на создание и выдачу
квалифицированного сертификата ключа проверки электронной подписи
для юридических лиц)

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи

_____

(полное наименование организации, включая организационно-правовую форму согласно ЕГРЮЛ)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

(устава, положения, иное)

Просит изготовить квалифицированный сертификат ключа проверки электронной подписи уполномоченного представителя, в соответствии с указанными в настоящем заявлении данными, передать в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат подписи уполномоченного представителя:

_____

Ф.И.О.

пол: «____» дата рождения: «___» _____ _____г., место рождения: _____

_____

документ, удостоверяющий личность: серия «_____» номер «_____» кем выдан:

_____

дата выдачи «_____»_____ _____г., код подразделения «_____-_____»

Наименование юридического лица[1]	
Наименование населенного пункта	
Название улицы, номер дома	
Область	
Страна	
ИНН организации	
ОГРН организации	
Фамилия	
Имя Отчество	
Должность	
Подразделение организации	
СНИЛС	
Адрес электронной почты	

[1] Рекомендуется указывать сокращенное наименование юридического лица (если имеется).

Области использования (расширения сертификата)	*При необходимости указать области использования ключа[1], либо указать (отметить) шаблон сертификата:* □ *Сертификат ЭП-ОВ;* □ *Сертификат для работы в ИС дополнительного лекарственного обеспечения;* □ *Сертификат для работы оформления электронных листов нетрудоспособности;* □ *Сертификат для подписания электронных медицинских документов.*
Ключ электронной подписи и ключ проверки электронной подписи	□ *Создать с использованием средств Удостоверяющего центра* □ *Создан с использованием средств электронной подписи заявителя*
Наименование средства электронной подписи заявителя	□ *СКЗИ «КриптоПро CSP» версии 4.0* □ *иное:* _____
Класс средств электронной подписи заявителя	□ *КС1* □ *КС2* □ *КС3*

Приложение: Согласие лица, на имя которого создается квалифицированный сертификат, на обработку персональных данных[2];
Запрос на создание сертификата в электронном и (или) бумажном виде[3]

_____ _____ _____
(должность) (подпись) (Ф.И.О)

М.П.

« ____ » _____ 20 ____ г.

Уполномоченный представитель

_____ _____ _____
(должность) (подпись) (Ф.И.О)

« ____ » _____ 20 ____ г.

(заполняется уполномоченным лицом УЦ ООО «Модум»)

Данное Заявление зарегистрированы в реестре Удостоверяющего центра.
Регистрационный № _____ от «____»_____ 20____ г.

Уполномоченное лицо Удостоверяющего центра _____/_____/
общества с ограниченной ответственностью «Модум» (подпись) (расшифровка подписи)

М.П.

---

[1] Области использования ключа опубликованы на сайте Удостоверяющего центра.

[2] Не предоставляется в случае, если данное согласие ранее предоставлялось, либо если создается квалифицированный сертификат, используемый для автоматического подписания электронной подписью в информационной системе.

[3] Предоставляется в случае самостоятельного создания заявителем ключа электронной подписи и ключа проверки электронной подписи с использованием средств электронной подписи заявителя.

Приложение № 3.1
к Порядку реализации функций аккредитованного
Удостоверяющего центра
общества с ограниченной ответственностью «Модум»
(Форма заявления на создание и выдачу
квалифицированного сертификата ключа проверки электронной подписи
для физических лиц и индивидуальных предпринимателей)

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Заявление на изготовление квалифицированного сертификата ключа проверки электронной подписи для физических лиц и индивидуальных предпринимателей

Я, _____
(фамилия, имя, отчество)

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

прошу УЦ ООО «Модум» сформировать ключи электронной подписи и создать квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении данными, передать в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат подписи.

С Регламентом Удостоверяющего центра ознакомлен. В случае выявления факта компрометации ключа электронной подписи, соответствующего выпускаемому на мое имя сертификату, обязуюсь немедленно проинформировать УЦ ООО «Модум».

Общие сведения	
Фамилия	
Имя	
Отчество	
Дата рождения (дд.мм.гггг)	
СНИЛС	
ИНН	
ОГРНИП *(при наличии)*	
Адрес электронной почты	
Ключевая фраза	
Адрес	
Страна	RU
Область	
Регион	
Город (населенный пункт)	
Улица	
Дом, корпус, офис(кв.)	

Паспортные данные	
Серия	
Номер	
Дата выдачи	
Кем выдан	
Подразделение	
Место рождения	
Гражданство	
Дополнительно	
Области использования (расширения сертификата)	
Ключ электронной подписи и ключ проверки электронной подписи	□ *Создать с использованием средств Удостоверяющего центра* □ *Создан с использованием средств электронной подписи заявителя*
Наименование средства электронной подписи заявителя	СКЗИ «КриптоПро CSP» версии 4.0 иное:
Класс средств электронной подписи заявителя	□ КС1 □ КС2 □ КС3
Контактный телефон	

«____» _____20____г. _____ / _____ /
(подпись) (ФИО)

Приложение № 4
к заявлению на создание и выдачу квалифицированного сертификата
ключа проверки электронной подписи **для юридических лиц**
(Форма согласия на обработку персональных данных)

_____
(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат, серия и номер паспорта, кем и когда выдан)

_____
(адрес места регистрации и проживания)

в соответствии со статьей 9 Федерального закона «О персональных данных» даю согласие оператору персональных данных – обществу с ограниченной ответственностью «Модум», расположенному по адресу: г. Москва, ул. Большая Почтовая, 36 стр. 1, к. 6,6Б, на автоматизированную, а также без использования средств автоматизации, обработку своих персональных данных, включающих: фамилию, имя, отчество, адрес регистрации (места жительства), серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, страховой номер индивидуального лицевого счета (СНИЛС), адрес электронной почты, номер мобильного телефона, сведения о месте работы, должность.

Настоящее согласие предоставляется мной в целях получения услуг в соответствии с Порядком реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум» (далее – Порядок), включения сведений в квалифицированный сертификат, а также для регистрации меня и выданного мне квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ. Настоящим соглашаюсь на включение моих сведений, содержащихся в выданном мне квалифицированном сертификате ключа проверки электронной подписи, в том числе включающих фамилию, имя, отчество, сведений о месте работы и занимаемой должности, СНИЛС, адрес электронной почты, в общедоступные источники персональных данных, которыми являются квалифицированный сертификат ключа проверки электронной подписи и реестр сертификатов удостоверяющего центра общества с ограниченной ответственностью «Модум».

Настоящим предоставляю обществу с ограниченной ответственностью «Модум» право осуществлять все действия (операции) со своими персональными данными, предусмотренные Порядком, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, распространение, предоставление, блокирование и уничтожение персональных данных.

Настоящее согласие на обработку персональных данных действует в течение всего срока осуществления обществом с ограниченной ответственностью «Модум» функций удостоверяющего центра в соответствии с требованиями статей 13, 14, 15 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и может быть отозвано в порядке, установленном Федеральным законом
«О персональных данных» от 27.07.2006 года № 152-ФЗ.

В случае отзыва согласия на обработку персональных данных общества с ограниченной ответственностью «Модум» имеет право не прекращать их обработку до окончания установленных нормативными правовыми актами Российской Федерации сроков хранения соответствующей информации или документов, при обработке которых использовалась электронная подпись данного субъекта персональных данных, а также в случаях, предусмотренных статьей 6 Федерального закона «О персональных данных».

Подтверждаю, что с Порядком, опубликованным на сайте Удостоверяющего центра общества с ограниченной ответственностью «Модум» в информационно-телекоммуникационной сети «Интернет» по адресу http://modum.pro, и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен
и обязуюсь соблюдать все его положения.

Уполномоченное лицо, на имя которого / / _____

изготавливается сертификат (подпись) (ФИО) дата

Приложение 4.1.
к заявлению на создание и выдачу квалифицированного сертификата
ключа проверки электронной подписи **для физических лиц**
(Форма согласия на обработку персональных данных)

(Фамилия, Имя, Отчество лица, на имя которого изготавливается сертификат, серия и номер паспорта, кем и когда выдан)

(адрес места регистрации и проживания)

в соответствии со статьей 9 Федерального закона «О персональных данных» от 27.07.2006 года № 152-ФЗ даю согласие оператору персональных данных – обществу с ограниченной ответственностью «Модум», расположенному по адресу г. Москва, ул. Большая Почтовая, 36 стр. 1, к. 6,6Б, на автоматизированную, а также без использования средств автоматизации, обработку своих персональных данных, включающих: фамилию, имя, отчество, адрес регистрации (места жительства), серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, страховой номер индивидуального лицевого счета (СНИЛС), идентификационный номер налогоплательщика (ИНН), адрес электронной почты, номер мобильного телефона, основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП).

Настоящее согласие предоставляется мной в целях получения услуг в соответствии с Порядком реализации функций аккредитованного Удостоверяющего центра общества с ограниченной ответственностью «Модум» (далее – Порядок), а также для регистрации меня и выданного мне квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ. Настоящим соглашаюсь на включение моих сведений, содержащихся в выданном мне квалифицированном сертификате ключа проверки электронной подписи, в том числе включающих фамилию, имя, отчество, ИНН, СНИЛС, ОГРНИП, адрес регистрации (места жительства), адрес электронной почты, в общедоступные источники персональных данных, которыми являются квалифицированный сертификат ключа проверки электронной подписи и реестр сертификатов удостоверяющего центра общества с ограниченной ответственностью «Модум».

Настоящим предоставляю обществу с ограниченной ответственностью «Модум» право осуществлять все действия (операции) со своими персональными данными, предусмотренные Порядком, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, использование, распространение, предоставление, блокирование и уничтожение персональных данных.

Настоящее согласие на обработку персональных данных действует в течение всего срока осуществления обществом с ограниченной ответственностью «Модум» функций удостоверяющего центра в соответствии с требованиями статей 13, 14, 15 Федерального закона «Об электронной подписи» от 06.04.2011 года № 63-ФЗ и может быть отозвано в порядке, установленном Федеральным законом
«О персональных данных» от 27.07.2006 года № 152-ФЗ.

В случае отзыва согласия на обработку персональных данных общество с ограниченной ответственностью «Модум» имеет право не прекращать их обработку до окончания установленных нормативными правовыми актами Российской Федерации сроков хранения соответствующей информации или документов, при обработке которых использовалась электронная подпись данного субъекта персональных данных, а также в случаях, предусмотренных статьей 6 Федерального закона «О персональных данных» от 27.07.2006 года № 152-ФЗ.

Подтверждаю, что с Порядком, опубликованным на сайте общества с ограниченной ответственностью «Модум» в информационно- телекоммуникационной сети «Интернет» по адресу http://modum.pro, и приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен и обязуюсь соблюдать все его положения.

Заявитель, на имя которого изготавливается сертификат	_____ (подпись)	/ _____ (ФИО)	/ _____ дата

Приложение № 5
к Порядку реализации функций аккредитованного
удостоверяющего центра общества с ограниченной
ответственностью «Модум»
(Форма доверенности на право действия от имени
юридического лица)

Доверенность

г._____ «____» _____20____г.

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

в лице _____
(должность,)

_____
(фамилия, имя, отчество)

действующего на основании _____
(устава, положения, иное)

уполномочивает _____
(фамилия, имя, отчество доверенного лица)

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

_____
(адрес места регистрации и проживания)

действовать от имени _____
(сокращенное наименование организации)

в качестве владельца квалифицированного сертификата ключа проверки электронной подписи при использовании квалифицированной электронной подписи, а также выступать в роли Пользователя Удостоверяющего центра общества с ограниченной ответственностью «Модум» и осуществлять, в рамках Порядка реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум», действия установленные для владельца квалифицированного сертификата ключа проверки электронной подписи и пользователя Удостоверяющего центра общества с ограниченной ответственностью «Модум».

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

Настоящая доверенность действительна «____» _____20____г. по

Подпись доверенного лица _____ / _____ / подтверждаю
(Фамилия И.О.) (подпись)

_____ _____ / _____ / _____
(должность) (подпись) (ФИО) дата

М.П.

Приложение № 6
к Порядку реализации функций аккредитованного
удостоверяющего центра общества с ограниченной ответственностью «Модум»
(Форма заявления на подтверждение действительности электронной
подписи в электронном документе
для юридических лиц

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Заявление на подтверждение действительности электронной подписи в электронном документе

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

в лице _____
(должность,)

_____
(фамилия, имя, отчество)

действующего на основании _____
(устава, положения, иное)

просит проверить действительность усиленной квалифицированной электронной подписи, использованной для подписания электронного документа на основании следующих данных:

1. Серийный номер квалифицированного сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе:

_____

2. Время[1] подписания электронного документа электронной подписью:

«_____:_____» «_____/_____/_____»
час минута день месяц год

3. Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):

«_____:_____» «_____/_____/_____»
час минута день месяц год

Приложение: 1. Квалифицированный сертификат ключа проверки электронной подписи, выданный удостоверяющим центром общество с ограниченной ответственностью «Модум», с использованием которого необходимо проверить действительность электронной подписи в электронном документе (файл формата CMS / PKCS #7), на носителе информации

– рег. №_____;

2. Электронный документ, подписанный электронной подписью, основанной на квалифицированном сертификате, выданным удостоверяющим центром Общество с ограниченной ответственностью «Модум», действительность которой необходимо проверить (в виде файла стандарта CMS / PKCS #7), на носителе информации – рег. №_____.

_____	_____ / _____ /
(должность)	(подпись) (ФИО)

Приложение № 7
к Порядку реализации функций аккредитованного удостоверяющего центра общества с ограниченной ответственностью «Модум
(Форма заявления на проверку подлинности усиленной квалифицированной электронной подписи в электронном документе)
для физических лиц и индивидуальных предпринимателей

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Я, _____
(фамилия, имя, отчество,)
прошу проверить действительность усиленной квалифицированной электронной подписи, использованной для подписания электронного документа на основании следующих данных:

1. Серийный номер квалифицированного сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе:

_____

2. Время[1] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»
час минута день месяц год

3. Время, на момент наступления которого необходимо проверить подлинность электронной подписи (если момент подписания электронного документа не определен):

«_____:_____» «_____/_____/_____»
час минута день месяц год

Приложение: 1. Квалифицированный сертификат ключа проверки электронной подписи, выданный удостоверяющим центром Общество с ограниченной ответственностью «Модум», с использованием которого необходимо проверить действительность электронной подписи в электронном документе (файл формата CMS / PKCS #7), на носителе информации – рег. №_____;
2. Электронный документ, подписанный электронной подписью, основанной на квалифицированном сертификате, выданным удостоверяющим центром общество с ограниченной ответственностью «Модум», действительность которой необходимо проверить (в виде файла стандарта CMS / PKCS #7), на носителе информации – рег. №_____.

_____ _____/_____/
(Ф.И.О. заявителя) (подпись) (расшифровка подписи)

[1] Время и дата указываются с учетом часового пояса (по Московскому времени).

Приложение № 8
к Порядку реализации функций аккредитованного удостоверяющего
центра общества с ограниченной
ответственностью «Модум»
(Форма заявления на получение информации о статусе
квалифицированного сертификата)
Для юридических лиц

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

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

в лице _____
(должность,)

_____
(фамилия, имя, отчество)

действующего на основании _____
(устава, положения, иное)

просит предоставить информацию о статусе квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Наименование организации	
ОГРН организации	
Фамилия	
Имя Отчество	
СНИЛС	

Период времени[1] на момент наступления которого требуется установить статус квалифицированного сертификата ключа проверки электронной подписи:
с «_____» по «_____».

_____ _____/_____/
(должность) (подпись) (ФИО)

[1] Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 9
к Порядку реализации функций аккредитованного удостоверяющего
центра общества с ограниченной
ответственностью «Модум»
(Форма заявления на получение информации
о квалифицированного статусе сертификата)
Для физических лиц и индивидуальных предпринимателей

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Я, _____
(фамилия, имя, отчество,)
прошу предоставить информацию о статусе квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
СНИЛС	

Период времени[1] на момент наступления которого требуется установить статус квалифицированного сертификата ключа проверки электронной подписи: с «_____» по «_____».

_____ _____/_____/
(Ф.И.О. заявителя) (подпись) (расшифровка подписи)

[1] Если время и дата не указаны, то статус сертификата устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение № 10
к Порядку реализации функций аккредитованного удостоверяющего центра Общество с ограниченной ответственностью «Модум»
(Форма заявления о прекращении действия квалифицированного сертификата ключа проверки электронной подписи)
Для юридических лиц

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Заявление о прекращении действия квалифицированного сертификата ключа проверки электронной подписи

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

в лице _____
(должность,)

_____
(фамилия, имя, отчество)

действующего на основании _____
(устава, положения, иное)

в связи с _____
(причина прекращения действия сертификата)

просит прекратить действие квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие данные[1]:

Серийный номер сертификата	
Наименование юридического лица	
ИНН	
ОГРН	
Фамилия	
Имя Отчество	
СНИЛС	

_____ _____/_____/
(должность) (подпись) (ФИО)

[1] Указываются сведения, содержащиеся в квалифицированном сертификате владельца сертификата

Приложение № 11
к Порядку реализации функций аккредитованного удостоверяющего центра
общества с ограниченной ответственностью «Модум»
(Форма заявления о прекращении действия квалифицированного
сертификата ключа проверки электронной подписи)
Для физических лиц и индивидуальных предпринимателей

г. Москва

Удостоверяющий центр
ООО «Модум»

«____» _____20____г. №_____

Заявление о прекращении действия квалифицированного сертификата ключа проверки электронной подписи

Я, _____
(фамилия, имя, отчество,)

в связи с _____
(причина прекращения действия сертификата)

прошу прекратить действие квалифицированного сертификата ключа проверки электронной подписи, владельцем которого я являюсь, содержащего следующие данные:

Серийный номер сертификата	
Фамилия	
Имя Отчество	
ИНН	
СНИЛС	

_____ _____/_____/
(Ф.И.О. заявителя) (подпись) (расшифровка подписи)

Приложение № 12
к Порядку реализации функций
аккредитованного удостоверяющего центра
общества с ограниченной ответственностью «Модум»

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Общие принципы обеспечения информационной безопасности при организации электронного взаимодействия с использованием электронной подписи.

Организация электронного взаимодействия с использованием электронной подписи должна осуществляться с учетом требований федеральных законов «Об электронной подписи» от 06.04.2011 года № 63-ФЗ, «Об информации, информационных технологиях и о защите информации» от 27.07.2006 года № 149-ФЗ, Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.07.2001 года № 152 (далее - Инструкцией ФАПСИ №152), других федеральных законов и нормативных правовых актов, осуществляющих правовое регулирование отношений в области обеспечения защиты информации и использования электронной подписи, руководящих документов ФСТЭК России и ФСБ России, эксплуатационной и технической документации на используемые средства электронной подписи, средства криптографической защиты информации (далее – СКЗИ).

Если иное не установлено федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или решением о создании корпоративной информационной системы, порядок использования электронной подписи в корпоративной информационной системе может устанавливаться оператором этой системы или соглашением между участниками электронного взаимодействия в ней.

2. Риски, связанные с использованием электронных подписей и средств электронной подписи.

2.1. Виды рисков, связанных с использованием электронных подписей и средств электронной подписи.

В случае, если электронное взаимодействие с использованием электронной подписи осуществляется без учета требований нормативных правовых актов, регулирующих отношения в области использования электронных подписей, используется неквалифицированная электронная подпись или средства электронной подписи не сертифицированы на соответствие требованиям безопасности информации, могут возникнуть или существенно возрасти риски, связанные с использованием электронной подписи, основными из которых могут являться:

- риски, связанные с нарушением целостности электронного документа и возможностью отказа от него. Данные риски могут быть связаны с внесенными в электронный документ изменениями, произведенными после его подписания. Лицо, подписавшее электронный документ неквалифицированной электронной подписью, или лицо, осуществляющее проверку такой электронной подписи, может заявить о том, что содержание

электронного документа было изменено после его подписания и электронный документ не соответствует тому документу, который был подписан неквалифицированной электронной подписью;

- риски, связанные с проверкой принадлежности ключа электронной подписи, с помощью которой подписан электронный документ, владельцу сертификата ключа проверки электронной подписи (далее – владелец сертификата). Лицо, владеющее сертификатом ключа проверки электронной подписи и соответствующим ключом электронной подписи, которым был подписан электронный документ, может заявить о том, что неквалифицированная электронная подпись, содержащаяся в электронном документе, не принадлежит данному владельцу сертификата;

- риски, связанные с признанием юридической силы электронного документа, подписанного неквалифицированной электронной подписью. Одна из сторон может заявить о том, что подписанный неквалифицированной электронной подписью документ не может порождать юридически значимых последствий или считаться достаточным доказательством в суде;

- риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае, если порядок использования неквалифицированной электронной подписи и средств электронной подписи не соответствует требованиям нормативных правовых актов Российской Федерации, осуществляющих правовое регулирование отношений в использовании электронной подписи или не соответствует порядку использования неквалифицированной электронной подписи, определяемому соглашениями сторон, юридическая значимость подписанных такой электронной подписью документов может быть не признана одной из сторон участника электронного взаимодействия;

- риски, связанные с нарушением конфиденциальности ключей электронной подписи (использование ключей электронной подписи без согласия владельца). В случае нарушения конфиденциальности ключей электронной подписи, в том числе компрометации ключей, несанкционированного доступа к ключевым носителям или средствам электронной подписи, участником электронного взаимодействия может быть принят в исполнение подписаны неквалифицированной электронной подписью документ, порождающий юридически значимые последствия;

- риски, связанные с несовместимостью средств электронной подписи, используемых сторонами для организации электронного взаимодействия. Несовместимость средств электронной подписи, протоколов и форматов данных, используемых сторонами для организации электронного взаимодействия, может привести к невозможности проверки неквалифицированной электронной подписи документа или к её некорректной проверке;

- риски, связанные с определением полномочий лица, подписавшего электронной подписью документ. В случае, если участниками электронного взаимодействия не определены лица, участвующие в электронном взаимодействии, полномочия данных лиц по подписанию электронных документов от имени участника электронного взаимодействия, а также в случае, если полномочия лица по подписанию электронных документов прекращены, одна из сторон может заявить, что полученный электронный документ содержит неквалифицированную электронную подпись лица, не уполномоченного на подписание данного документа и не может быть принят в исполнение;

- риски, связанные с использованием сертификатов ключей проверки электронной подписи и ключей электронной подписи, прекративших своё действие. В случае использования

для подписания электронных документов ключа электронной подписи, прекратившего своё действие на момент подписания, либо, если момент подписания электронного документа не определен, а также в случае использования сертификата ключа проверки электронной подписи, который стал недействующим на день проверки электронной подписи, сторона, получившая подписанный неквалифицированной электронной подписью документ, может заявить о непризнании такого электронного документа.

2.2. Меры по снижения вероятности возникновения рисков, связанных с использованием электронных подписей.

В целях снижения вероятности возникновения и реализации указанных рисков участникам электронного взаимодействия необходимо предусмотреть обеспечение комплекса правовых и организационно-технических мероприятий по обеспечению информационной безопасности при осуществлении электронного взаимодействия с использованием усиленной квалифицированной электронной подписи (далее – электронная подпись) и сертифицированных по требованиям безопасности информации средств электронной подписи, получивших подтверждение соответствия требованиям к средствам электронной подписи, установленным
в соответствии с Федеральными законом «Об электронной подписи» от 06.04.2011 года № 63-ФЗ (далее – сертифицированные средства электронной подписи).

Электронное взаимодействие с использованием усиленной квалифицированной электронной подписи и сертифицированных средств электронной подписи, осуществляемое с учетом требований Федерального закона «Об электронной подписи», других федеральных законов, принимаемых в соответствии с ними нормативных правовых актов, регулирующих отношения в области использования электронных подписей, позволяет обеспечить:

- неотказуемость от электронного документа, содержащего электронную подпись. Квалифицированная электронная подпись позволяет определить лицо, подписавшее электронный документ;

- целостность электронного документа. Квалифицированная электронная подпись позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания.

В случае необходимости обеспечения конфиденциальности передаваемой информации ключи электронной подписи и СКЗИ могут использоваться для обеспечения защиты информации, в том числе при её передаче по информационно-телекоммуникационным сетям, а также для организации защищенных каналов связи с использованием шифровальных (криптографических) средств.

Использование квалифицированной электронной подписи и сертифицированных средств электронной подписи позволяет:

- установить факт изменения подписанного электронного документа после момента его подписания;

- обеспечить практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;

- создать электронную подпись в формате, обеспечивающем возможность ее проверки всеми средствами электронной подписи.

При создании электронной подписи сертифицированные средства электронной подписи должны:

- показывать лицу, подписывающему электронный документ, содержание информации,

которую он подписывает;

- показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу, осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

- создавать электронную подпись только после подтверждения лицом, подписывающим электронный документ, операции по созданию электронной подписи

- однозначно показывают, что квалифицированная электронная подпись создана.

При проверке электронной подписи сертифицированные средства электронной подписи должны:

- показывать содержание электронного документа, подписанного электронной подписью;

- показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;

- указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Одной из составных частей инфраструктуры открытых ключей и системы криптографической защиты информации является аккредитованный удостоверяющий центр, выполняющий функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей (далее – квалифицированный сертификат).

Удостоверяющий центр осуществляет свою деятельность в строгом соответствии с нормативными правовыми актами Российской Федерации, руководящими документами, эксплуатационной документацией на используемые средства, Порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее – Порядок) и другими документами, регулирующими вопросы использования электронной подписи.

Квалифицированные сертификаты, изготавливаемые Удостоверяющим центром, заверяются электронной подписью уполномоченного лица удостоверяющего центра, что подтверждает факт принадлежности ключа электронной подписи конкретному лицу участника электронного взаимодействия. Использование квалифицированных сертификатов позволяет участника электронного взаимодействия идентифицировать лицо, подписавшее электронной подписью документ, а также позволяет подтвердить целостность (неизменность) содержания подписанного электронного документа при проверке электронной подписи. Таким образом, при соблюдении требований информационной безопасности и соблюдения порядка использования квалифицированной электронных подписей, практически исключаются риски, связанные использованием электронных подписей, в том числе риски, связанные с подтверждением юридической значимости электронных документов, подписанных усиленной квалифицированной электронной подписью

3. Меры, необходимые для обеспечения безопасности при использовании электронных подписей.

3.1. Требования и рекомендации по обеспечению информационной безопасности при использовании средств электронной подписи.

В организации, эксплуатирующей средства электронной подписи (СКЗИ), должны быть предусмотрены организационные и организационно - технические мероприятия, направленные на обеспечение информационной безопасности при использовании средств электронной подписи и определяющие требования к ответственным лицам,

автоматизированным рабочим местам пользователей СКЗИ (далее - АРМ), системному и прикладному программному обеспечению, условиям хранения и использования средств электронной подписи, ключей электронной подписи и ключевых носителей.

3.1.1. Требования и рекомендации по назначению ответственных лиц.

В организации должны быть определены лица, ответственные за осуществление электронного взаимодействии с использованием электронной подписи и имеющие доступ к ключевым носителям, а также лица, ответственные за организацию работ по защите информации и соблюдению условий хранения и использования ключей электронной подписи и средств электронной подписи.

К работе со средствами электронной подписи должны допускаться лица, прошедшие соответствующее обучение и ознакомленные с Инструкцией ФАПСИ №152, другими нормативными правовыми актами и руководящими документами, в том числе внутренними организационными документами и инструкциями по защите информации при использовании электронной подписи, а также эксплуатационной документацией на используемые средства электронной подписи.

В организации, эксплуатирующей СКЗИ, должно быть назначено лицо, выполняющее функции администратора информационной безопасности, на которого возлагаются задачи организации работ по защите информации, подготовки соответствующих инструкций, обучения и инструктажа пользователей СКЗИ, ведению журналов учета СКЗИ, настройке системного, прикладного программного обеспечения, СКЗИ и средств защиты от несанкционированного доступа, устанавливаемого на АРМ пользователей СКЗИ, контролю за соблюдением требований по безопасности, а также взаимодействия с удостоверяющим центром по вопросам использования электронной подписи.

3.1.2. Требования и рекомендации к помещениям и размещению технических средств АРМ.

Помещения, в которых расположены АРМ, предназначенные для работы со средствами электронной подписи (далее – спецпомещения), должны соответствовать требованиям Инструкции ФАПСИ №152. Должен быть исключен бесконтрольный допуск лиц, не допущенных к работе в указанных спецпомещениях. В случае необходимости присутствия посторонних лиц в спецпомещениях должен быть обеспечен контроль за их действиями.

Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Размещение АРМ должно производиться с учетом схемы контролируемой зоны и исключать возможность просмотра посторонними лицами работ, осуществляемых на АРМ.

Спецпомещения рекомендуется оснащать охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

3.1.3. Требования и рекомендации к АРМ пользователей СКЗИ.

Не допускается оставлять без контроля АРМ при включенном питании и подключенными ключевыми носителями. Перед уходом пользователь СЗКИ должен выключить АРМ либо заблокировать рабочую станцию с использованием средств защиты

информации от несанкционированного доступа или с использованием средств операционной системы. Рекомендуется настроить автоматическое включение экранной заставки, защищенной паролем.

На АРМ пользователей рекомендуется установить сертифицированные средства защиты информации от несанкционированного доступа, а также средства антивирусной защиты.

В целях исключения возможности несанкционированного изменения аппаратной части системного блока администратору рекомендуется предусмотреть опечатывание системного блока АРМ.

Необходимо предусмотреть организацию парольной защиты при включении АРМ и загрузке операционной системы с использованием средств защиты информации (средств доверенной загрузки), либо средств BIOS и средств операционной системы, также рекомендуется определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске, отключить возможность загрузки
с внешних съемных дисков, исключить возможность нестандартных видов загрузки операционной системы.

3.1.4. Требования и рекомендации по настройке системного и прикладного программного обеспечения.

На технических средствах АРМ с установленными средствами электронной подписи необходимо использовать только лицензионное программное обеспечение, полученное из доверенных источников. Не допускается использовать нестандартные, измененные или отладочные версии операционной системы.

Не допускается установка на АРМ средств разработки и отладки программного обеспечения. Необходимо исключить возможность установки средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также вредоносного программного обеспечения, позволяющего получать привилегии администратора.

Рекомендуется ограничить права пользователя АРМ по самостоятельной установке программного обеспечения и настроить возможность выполнения пользователем АРМ только тех приложений, которые разрешены администратором информационной безопасности.

Необходимо регулярно отслеживать и устанавливать обновления безопасности для операционной системы, программного обеспечения АРМ, регулярно осуществлять обновление антивирусных баз.

3.1.5. Требования к настройкам операционной системы, установленной на АРМ пользователя.

До начала использования средств электронной подписи администратор информационной безопасности должен произвести настройку операционной системы, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль настроек в соответствии со следующими рекомендациями:

- правом установки и настройки операционной системы и средств электронной подписи должен обладать только администратор безопасности;

- в целях возможности разграничения прав доступа рекомендуется использовать средства, входящие в состав средств защиты информации;

- всем пользователям и группам, зарегистрированным в операционной системе,

необходимо назначить минимально возможные для работы права;

- все привилегии группы Everyone должны быть удалены;

- необходимо исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке без ввода пароля;

- рекомендуется переименовать стандартную учетную запись администратора; рекомендуется отключить учетная запись для гостевого входа;

- исключить возможность удаленного управления, администрирования и модификации операционной системы и её настроек, системного реестра, для всех, включая группу администраторов;

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

- должно быть исключено или ограничено использование пользователями сервиса планировщика задач. При использовании данного сервиса состав запускаемого программного обеспечения на АРМ согласовывается с администратором информационной безопасности;

- рекомендуется организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы средств электронной подписи. Если это невыполнимо, то операционная система должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

- должны быть отключены средства удаленного администрирования, в случае если такое подключение осуществляется без использования защищенных каналов связи;

- должны быть установлены ограничения на доступ пользователей к системному реестру путем настройки прав доступа к системному реестру;

- на все директории (папки), содержащие системные файлы и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме пользователя, имеющего права администратора, создателя (владельца) и права системы;

- необходимо обеспечить ведение журналов аудита в операционной системе;

- настройка параметров системного реестра производится в соответствии с эксплуатационной документацией на средства электронной подписи.

3.1.6. Требования и рекомендации при организации парольной защиты.

Рекомендуется разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, доступа к ключам электронной подписи), использовать правила формирования и хранения паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8 символов;

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

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

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

- пользователь АРМ должен обеспечивать конфиденциальность паролей, не допускается хранить записанные пароли в легкодоступных местах;

- периодичность смены пароля определяется принятой политикой безопасности (инструкцией по организации парольной защиты), но не должна превышать двух месяцев.

Указанная политика должна применяться для всех учетных записей пользователей,

зарегистрированных в операционной системе.

3.1.7. Требования к установке, настройке и использованию средств электронной подписи.

Установка и настройка средств электронной подписи (СКЗИ) должна выполняться администратором информационной безопасности либо лицом, ответственным за работоспособность АРМ и прошедшим соответствующее обучение.

Установка средств электронной подписи должна производиться только с дистрибутива, полученного по доверенному каналу, в соответствии с эксплуатационной документацией на средства электронной подписи.

При установке средств электронной подписи должен быть обеспечен контроль целостности устанавливаемого программного обеспечения.

Перед установкой средств электронной подписи необходимо произвести проверку операционной системы на отсутствие вредоносных программ с помощью антивирусных средств.

После завершения установки осуществляются настройка и контроль работоспособности средств электронной подписи.

Использование средств электронной подписи должно осуществляться в соответствии с эксплуатационной документацией и инструкциями на средства электронной подписи.

3.1.8. Требования обеспечения информационной безопасности при подключении АРМ к сетям связи общего пользования, в том числе к информационно - телекоммуникационной сети «Интернет».

Не рекомендуется подключать к сетям связи общего пользования АРМ пользователя при работе со средствами электронной подписи и носителями ключей электронной подписи. В случае необходимости подключения АРМ к сетям связи общего пользования такое подключение рекомендуется производить с использованием сертифицированного межсетевого экрана, настроенного в соответствии с требованиями эксплуатационной документации на средства межсетевого экранирования.

В случае подключения АРМ с установленными средствами электронной подписи к сетям связи общего пользования необходимо ограничить возможность запуска и исполнения файлов
и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования. Не допускается открывать такие файлы без проведения соответствующих проверок антивирусными средствами на предмет содержания в них программных закладок и вредоносных программ.

3.2. Порядок обращения с носителями ключевой информации.

При использовании и хранении ключей электронной подписи должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации (ключевых носителей), содержащих ключи электронной подписи, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

В качестве ключевых носителей рекомендуется использовать учтенные в установленном порядке сертифицированные ключевые носители USB-ключи и смарт-карты.

При хранении и использовании ключей электронной подписи пользователю СКЗИ запрещается:

- выполнять копирование ключа электронной подписи на иные ключевые носители без разрешения администратора информационной безопасности;

- знакомить с содержанием ключевых носителей или передавать ключевые носители иным лицам;

- устанавливать ключевой носитель в другие АРМ, не предназначенные для работы с ключевой информацией;

- записывать на ключевой носитель постороннюю информацию;

- использовать ранее использовавшиеся ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации с использованием сертифицированных средств электронной подписи либо средств, гарантирующих практическую невозможность восстановления информации с ключевых носителей.

Владелец ключа электронной подписи (владелец сертификата) обязан:

- хранить в тайне ключ электронной подписи;

- немедленно обратиться в удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи или его отзыва в случае компрометации ключа электронной подписи или при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

- не использовать ключ проверки электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который отозван или действие которого приостановлено.

3.3. Учет и контроль выполнения требований информационной безопасности и порядка использования средств электронной подписи.

Действия, связанные с хранением и эксплуатацией средств электронной подписи и ключей электронной подписи, должны фиксироваться в журналах поэкземплярного учета, ведение которого осуществляется администратором информационной безопасности в соответствии с Инструкцией ФАПСИ № 152.

Администратор информационной безопасности должен периодически, не реже одного раза в два месяца, проводить проверку установленного программного обеспечения, журналов аудита операционной системы и средств защиты информации на всех АРМ пользователей СКЗИ, осуществлять контроль за условиями использования и хранения ключевых носителей, а также проводить периодическое тестирование технических и программных средств защиты информации.

В случае обнаружения постороннего программного обеспечения, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной руководителем организации, а также организованы работы по анализу и устранению выявленных нарушений.