

Приложение № 1
к приказу от «29» июня 2021 № 63

УТВЕРЖДЕНО
приказом АО «НИИАС»
от « 29» июня 2021 № 63

**Порядок реализации функций
Аккредитованного Удостоверяющего центра АО «НИИАС»
и исполнения его обязанностей**

**г. Москва
2021 г.**

1. Термины и определения, используемые в настоящем Порядке

Электронная подпись (ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

Сертификат ключа проверки электронной подписи (СКПЭП) - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном настоящим Федеральным законом порядке выдан сертификат ключа проверки электронной подписи;

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

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

Ключевой носитель - отчуждаемый носитель информации, предназначенный для хранения ключей ЭП, ключей проверки ЭП, сертификатов ключей проверки электронных подписей;

Удостоверяющий центр (УЦ) - Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС»), осуществляющее выполнение целевых функций по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Аккредитация удостоверяющего центра - признание соответствия удостоверяющего центра требованиям Федерального закона «Об электронной подписи».

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

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

Участники электронного взаимодействия - осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

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

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

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра созданного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Подтверждение владения ключом электронной подписи - получение удостоверяющим центром, уполномоченным федеральным органом доказательств того, что лицо, обратившееся за получением сертификата ключа проверки электронной подписи, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Заявитель - коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица (далее - нотариусы), обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Реестр квалифицированных сертификатов ключей проверки электронной подписи (далее – Реестр сертификатов) - реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования.

Электронный документ – документ, информация в котором представлена в электронно-цифровой форме.

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений.

2. Общие положения

2.1. Предмет регулирования Порядка

- 2.1.1. Настоящий Порядок реализации функций аккредитованного удостоверяющего центра АО «НИИАС» и исполнения его обязанностей (далее – Порядок) является локальным нормативным актом, разработанным в соответствии с требованиями законодательства Российской Федерации об электронной подписи и Требованиями к порядку реализации функций аккредитованного и исполнения его обязанностей, установленными Приказом Минцифры России от 13.11.2020 N 584.
- 2.1.2. Предметом регулирования настоящего Порядка являются условия предоставления услуг Удостоверяющего центра АО «НИИАС», включая права, обязанности и ответственность Удостоверяющего центра, а также правила пользования услугами Удостоверяющего центра АО «НИИАС».
- 2.1.3. Настоящий Порядок размещен для свободного доступа и ознакомления на сайте Удостоверяющего центра в сети интернет <http://pkitrans.ru>. Порядок распространяет свое действие на всех лиц, которые в силу настоящего Порядка, договора или действующего законодательства обязаны соблюдать правила и выполнять все требования, предусмотренные настоящим Порядком: Заявитель, Уполномоченный представитель Заявителя, Участники электронного взаимодействия, Владелец сертификата, Удостоверяющий центр.
- 2.1.4. Любое лицо, подавшее в Удостоверяющий центр заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи (далее – Сертификат), считается присоединившимся к Порядку на основании статьи 428 Гражданского кодекса Российской Федерации. С момента присоединения Заявителя к настоящему Порядку, он полностью и безоговорочно соглашается со всеми условиями настоящего Порядка и приложений к нему. Владелец сертификата имеет право в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром в рамках настоящего Порядка, направив в Удостоверяющий центр заявление на прекращение действия выданного ему Сертификата.
- 2.1.5. В случае противоречия и/или расхождения названия какого-либо раздела настоящего Порядка со смыслом одного из его пунктов, считается доминирующим смысл и формулировка каждого конкретного пункта.
- 2.1.6. В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Порядку с положениями Порядка, считается доминирующим смысл и формулировка Порядка.
- 2.1.7. Внесение изменений (дополнений) в Порядок, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке. Уведомление заинтересованных лиц о внесении изменений (дополнений) в Порядок осуществляется Удостоверяющим центром путем публикации на сайте по адресу <http://pkitrans.ru/>. Изменения (дополнения), вносимые Удостоверяющим центром в Порядок, кроме изменений (дополнений), вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для сторон по истечению 10 (Десяти) календарных дней с даты их публикации на сайте по адресу <http://pkitrans.ru/>. Изменения (дополнения), вносимые Удостоверяющим центром в Порядок в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных актов.

2.2. Сведения об Удостоверяющем центре

2.2.1. Полное наименование Удостоверяющего центра: Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте».

2.2.2. Акционерное общество «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (АО «НИИАС») зарегистрировано на территории Российской Федерации в городе Москва, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1077758841555 от 08.08.2007 г.

2.2.3. Удостоверяющий центр в качестве профессионального участника рынка услуг по созданию и управлению квалифицированными сертификатами ключей проверки электронной подписи осуществляет свою деятельность на территории Российской Федерации на основании лицензии ФСБ России ЛСЗ № 0013867, Рег. № 15475 Н от 06.10.2016 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием 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), виды работ, выполняемые (оказываемые) в составе лицензируемого вида деятельности: работы, предусмотренные пунктами 2, 3, 7, 8, 9, 11, 12, 13, 14, 15, 17, 18, 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 апреля 2012 г. № 313.

2.2.4. Реквизиты АО «НИИАС»:

- ОГРН: 1077758841555;
- ИНН: 7709752846,
- КПП: 770901001
- Код по ОКВЭД: 74.20.3
- Код по ОКПО: 82462078

Банковские реквизиты:

- Банк ВТБ (ПАО).
- БИК 044525187.
- Р/с 40702810600420000008.
- К/с 30101810700000000187.

2.2.5. Адрес места нахождения Удостоверяющего центра: 109029 г. Москва, ул. Нижегородская, д. 27, стр. 1.

2.2.6. Адрес для корреспонденции: 109029 г. Москва, ул. Нижегородская, д. 27, стр. 1.

- 2.2.7. Адреса точек выдачи Удостоверяющего центра размещены на сайте Удостоверяющего центра в сети интернет по адресу <http://pkitrans.ru>. Под точкой выдачи Удостоверяющего центра понимается обособленное подразделение УЦ или действующее на основании договора с УЦ юридическое лицо или индивидуальный предприниматель, из числа сотрудников которого назначается Доверенное лицо УЦ.
- 2.2.8. График работы Удостоверяющего центра (далее – рабочий день) – промежуток времени 9:00 - 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра

2.3.1. Информирование о предоставлении услуг Удостоверяющего центра осуществляется следующими способами:

- по единому справочному телефону: (499) 262-55-29 (в том числе, это номер телефона-автоинформатора);
- путем направления уведомлений по адресу электронной почты: cainfo@vniias.ru;
- путем опубликования информации на сайте Удостоверяющего центра в сети интернет <http://pkitrans.ru>.

2.3.2. Заявители вправе получить информацию по вопросам предоставления услуг Удостоверяющего центра, обратившись в Удостоверяющий центр любым из указанных в п.2.3.1. настоящего Порядке способом, либо самостоятельным получением информации, размещенной на сайте Удостоверяющего центра.

2.4. Стоимость услуг Удостоверяющего центра

2.4.1. Удостоверяющий центр оказывает услуги на платной основе.

2.4.2. Стоимость услуг Удостоверяющего Центра устанавливается Прейскурантом АО «НИИАС», размещенным на сайте Удостоверяющего центра в сети интернет по адресу <http://pkitrans.ru>.

2.4.3. Сроки и порядок расчетов за оказание услуг Удостоверяющего центра устанавливается в соответствии с положениями гражданского законодательства Российской Федерации. Оплата услуг Удостоверяющего центра может осуществляться как путем внесения предоплаты (аванса), так и путем внесения частичной предоплаты. В случае проведения закупочных процедур оплата услуг Удостоверяющего центра производится в соответствии с требованиями процедур, предусмотренных Федеральным законом от 18.07.2011 N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" и Федеральным законом от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

2.4.4. Срок и порядок расчетов могут быть пересмотрены по согласованию с Заявителем, в том числе отдельно заключаемыми соглашениями между Заявителем и Удостоверяющим центром.

2.4.5. Размер платы, указанный в п.2.4.1 не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

3. Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)

3.1. Удостоверяющий центр осуществляет следующие функции (оказывает следующие услуги):

- 3.1.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя Сертификата (заявителя) либо правомочия лица, выступающего от имени заявителя, по обращению за получением данного Сертификата с учетом требований, установленных п.4 ч.4 ст.8 Федерального закона № 63-ФЗ.
- 3.1.2. Осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи.
- 3.1.3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей.
- 3.1.4. Аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей.
- 3.1.5. Выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем с гарантией обеспечения конфиденциальности ключей.
- 3.1.6. Ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее – реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования.
- 3.1.7. Устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет".
- 3.1.8. Создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей.
- 3.1.9. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.
- 3.1.10. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.
- 3.1.11. По желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации (ЕСИА).
- 3.1.12. Изготавливает и выдает по запросам владельцев Сертификатов заверенные копии Сертификатов на бумажных носителях.

- 3.1.13. Предоставляет безвозмездно любому лицу по его обращению, в соответствии с установленным Порядком, доступ к информации, содержащейся в реестре сертификатов, в том числе к информации об аннулировании Сертификата.
- 3.1.14. Осуществляет иные, связанные с использованием электронной подписи, функции, установленные законодательством Российской Федерации и иную, связанную с использованием электронной подписи, деятельность.
- 3.1.15. Предоставляет пользователям Удостоверяющего центра Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, а также иных инструкций по работе со средствами криптографической защиты информации и информационной безопасности.

4. Права и обязанности Удостоверяющего центра

4.1. Удостоверяющий центр имеет право:

- 4.1.1. Наделить третьих лиц полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени Удостоверяющего центра АО «НИИАС». При совершении порученных Удостоверяющим центром действий доверенное лицо обязано идентифицировать заявителя при его личном присутствии.
- 4.1.2. Запрашивать у заявителя документы для подтверждения любой содержащейся в Заявлении на создание и выдачу Сертификата информации.
- 4.1.3. Выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе. Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную удостоверяющим центром.
- 4.1.4. Осуществлять иные права, предусмотренные законодательством об электронной подписи и соглашением с Удостоверяющим центром.
- 4.1.5. Отказать Заявителю в выдаче Сертификата в случае, если полученные в соответствии с частью 2.2. статьи 18 Федерального закона № 63-ФЗ документы и сведения не подтверждают достоверность информации, представленной Заявителем для включения в Сертификат, и УЦ не может установить личность заявителя – физического лица или не получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, на обращение за получением Сертификата.
- 4.1.6. Отказать в выдаче Сертификата в случаях подачи заявления на выдачу Сертификата в неактуальной форме, оформленного ненадлежащим образом, имеющего исправления, ошибки и/или приписки, не подтвержденные собственноручной подписью Заявителя – физического лица или Уполномоченного представителя Заявителя, а также в случае непредставления в УЦ документов и сведений, предусмотренных пунктом 5.2.4 настоящего Порядка.
- 4.1.7. Отказать в выдаче Сертификата в случае, если Заявитель – физическое лицо или Уполномоченный представитель Заявителя не предоставил письменного согласия на обработку своих персональных данных.

- 4.1.8. Аннулировать Сертификат Пользователя УЦ, если УЦ стало известно, что Владелец Сертификата не владеет Ключом электронной подписи, соответствующим Ключу проверки электронной подписи, указанному в таком Сертификате.
- 4.1.9. Прекратить действие Сертификата Пользователя УЦ в случае получения УЦ подтвержденной информации о смерти Владельца Сертификата – физического лица, о внесении записи в Единый государственный реестр юридических лиц (далее – ЕГРЮЛ) о ликвидации Владельца Сертификата – юридического лица, об утрате силы государственной регистрации Владельца Сертификата – физического лица в качестве индивидуального предпринимателя, а также в случае вступления в силу судебного решения о дисквалификации Владельца Сертификата – физического лица, действующего от имени юридического лица.
- 4.1.10. Отказать в прекращении действия Сертификата Пользователя УЦ в случае ненадлежащего оформления соответствующего заявления на прекращение действия Сертификата.
- 4.1.11. УЦ не вправе наделять третьих лиц (Доверенных лиц УЦ) полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени УЦ.

4.2. Удостоверяющий центр обязан:

- 4.2.1. Информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.
- 4.2.2. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- 4.2.3. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.
- 4.2.4. Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.
- 4.2.5. Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи.
- 4.2.6. Отказать заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения сертификата ключа проверки электронной подписи;
- 4.2.7. Не указывать в создаваемом им сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном этому удостоверяющему центру любым другим удостоверяющим центром.

- 4.2.8. Уведомить в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам. Удостоверяющий центр должен направить уведомление не менее чем за один месяц до даты прекращения деятельности Удостоверяющего центра.
- 4.2.9. В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций.
- 4.2.10. Вносить информацию о прекращении действия сертификата ключа проверки электронной подписи в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.
- 4.2.11. Хранить в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации следующую, следующую информацию:
- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
 - сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
 - сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.
- Хранение указанной в настоящем пункте информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.
- 4.2.12. Для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном Удостоверяющему центру головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. Удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами.
- 4.2.13. Обязан обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к

реестру сертификатов этого аккредитованного удостоверяющего центра в любое время в течение срока деятельности этого удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

4.2.14. В случае принятия решения о прекращении своей деятельности:

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

4.2.15. Обязан выполнять настоящий Порядок реализации функций аккредитованного удостоверяющего центра АО «НИИАС» и исполнения его обязанностей в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения обязанностей, а также с требованиями Федерального закона «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с действующим законодательством Российской Федерации об электронной подписи.

4.2.16. Не наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени такого аккредитованного удостоверяющего центра.

4.2.17. На безвозмездной основе обеспечить физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", для проведения идентификации физических лиц в аккредитованном удостоверяющем центре на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети "Интернет".

4.2.18. Выдавать квалифицированный сертификат в форме, требования к которой устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности по согласованию с уполномоченным федеральным органом.

4.2.19. При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

1. в порядке, установленном Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя

без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя – гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Устанавливаются:

- в отношении физического лица - фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

- в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, - наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица;

- для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, - наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано.

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

4.2.21. В установленном порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата). Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы

в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

4.2.22. Предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", физическим лицам, обратившимся к нему в целях проведения идентификации без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы (для предоставления биометрических персональных данных физического лица в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством сети "Интернет"), и указать страницу сайта в информационно-телекоммуникационной сети "Интернет", с которой безвозмездно предоставляются эти средства.

4.2.23. С использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи». Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов:

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

4.2.24. При получении квалифицированного сертификата заявителем ознакомить Заявителя (владельца сертификата) с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования заявителем квалифицированной электронной подписи при наличии у него действующего квалифицированного сертификата либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемых Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы. Указанное согласие, подписанное электронной подписью, в том числе простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного физического лица. Удостоверяющий центр обязан хранить информацию, подтверждающую ознакомление заявителя с информацией, содержащейся в квалифицированном сертификате, в течение всего срока осуществления своей деятельности.

- 4.2.25. Одновременно с выдачей квалифицированного сертификата должен предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.
- 4.2.26. При выдаче квалифицированного сертификата направлять в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии.
- 4.2.27. Обеспечить актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- 4.2.28. Обеспечить доступность реестра сертификатов в информационно телекоммуникационной сети «Интернет» в любое время.

5. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в Удостоверяющий центр в рамках предоставления услуг

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

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

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется одним из следующих способов:

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

средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. N 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)".

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона "Об электронной подписи" создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также необходимость выполнения требований, установленных постановлением Правительства Российской Федерации от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (Собрание законодательства Российской Федерации, 2012, N 7, ст. 863; 2016, N 26, ст. 4049) в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя.

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

Смена ключей электронной подписи Удостоверяющего центра может быть плановой и внеплановой в связи с нарушением конфиденциальности ключей электронной подписи Удостоверяющего центра.

Плановая смена ключей электронной подписи Удостоверяющего Центра выполняется в период действия ключа электронной подписи удостоверяющего центра. Плановая смена ключей электронной подписи производится по следующим основаниям:

- истечение срока действия квалифицированного сертификата;
- переход на использование новых стандартов электронной подписи и функции хеширования в соответствии с требованиями, установленными органом исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр изготавливает новый сертификат ключа проверки электронной подписи Уполномоченного лица Удостоверяющего центра. При плановой замене ключа электронной подписи Удостоверяющего центра все владельцы электронных подписей должны установить на своих автоматизированных рабочих местах новый сертификат удостоверяющего центра.

Информирование Заявителей и Владельцев электронной подписи о проведении плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется посредством публикации информации на официальном сайте УЦ по адресу: <http://pkitrans.ru/>

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: <http://pkitrans.ru>, доступная для скачивания. Предыдущий ключ электронной подписи Удостоверяющего центра используется в течение своего срока действия для формирования списков аннулированных сертификатов, изданных Удостоверяющим центром в период действия старого ключа электронной подписи УЦ.

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

Смена ключа электронной подписи Удостоверяющим центром осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи. Одновременно со сменой такого ключа электронной подписи прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Процедура внеплановой смены ключей Удостоверяющего центра осуществляется в порядке, предусмотренным для процедуры плановой смены ключей Удостоверяющего центра.

Смена ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности осуществляется в срок, не превышающий 7 (семь) рабочих дней.

В случае компрометации ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра аннулируется, Владельцы электронных подписей уведомляются об указанном факте путем публикации информации о компрометации на сайте Удостоверяющего центра в сети Интернет по адресу: <http://pkitrans.ru>.

Все квалифицированные сертификаты ключа проверки электронной подписи, подписанные с использованием скомпрометированного ключа Удостоверяющего центра, считаются аннулированными с внесением соответствующих сведений об этих квалифицированных сертификатах ключа проверки электронной подписи в реестр квалифицированных сертификатов.

Доверенным способом получения нового квалифицированного сертификата Удостоверяющего центра является его публикация на официальном сайте УЦ по адресу: <http://pkitrans.ru>, доступная для скачивания.

Актуальными угрозами нарушения конфиденциальности (компрометации) ключа электронной подписи УЦ являются угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к рабочим местам автоматизированной системы УЦ.

К случаям нарушения конфиденциальности (компрометации) ключа электронной подписи Удостоверяющего центра относятся в том числе:

- физическая утрата носителя ключа электронной подписи Удостоверяющего центра, в том числе в случае хищения или иного злонамеренного действия злоумышленника;
- несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение пломб и устройств контроля входа в помещение, повреждение замков и т. п.);
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;
- иные случаи компрометации.

5.1.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи владельца квалифицированного сертификата.

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

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

Заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью владельца квалифицированного сертификата, при этом в случае, если смена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата. Процедура выдачи квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, в том числе в электронной форме, осуществляется в соответствии с требованиями, установленными статьей 18 Федерального закона "Об электронной подписи" и настоящим Порядком.

5.2. Процедура создания и выдачи квалифицированных сертификатов

5.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

Создание квалифицированного сертификата ключа проверки электронной подписи осуществляется на основании Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи.

Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи подается Заявителем в электронной или бумажной форме.

Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи в бумажной форме подается лично, подписанное собственноручной подписью заявителя.

Заявление на выдачу квалифицированного сертификата ключа проверки электронной подписи в электронной форме подписывается действующим квалифицированным сертификатом ключа проверки электронной подписи Заявителя.

5.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

Заявление на выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью. Заявление на выдачу квалифицированного сертификата в бумажной форме оформляется в соответствии с формами, утвержденными Приложением № 1 и Приложением № 2 настоящего Порядка. Заявление на создание и выдачу квалифицированного сертификата в электронной форме представляется заявителем в УЦ в виде структуры CertificationRequest, определенной в пункте 7 Формата электронной подписи, обязательного для реализации всеми средствами электронной подписи, утвержденного приказом Минцифры России от 14 сентября 2020 г. № 472.

5.2.3. Порядок идентификации заявителя

Идентификация гражданина Российской Федерации осуществляется:

1) при его личном присутствии по основному документу, удостоверяющему личность.

2) без его личного присутствия:

- с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата;

- путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. N 1427 "О проведении эксперимента по совершенствованию применения технологии электронной подписи" (Собрание законодательства Российской Федерации, 2019, N 46, ст. 6493);

- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3448; 2020, N 14, ст. 2035).

Идентификация гражданина иностранного государства осуществляется по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства.

Идентификация беженца, вынужденного переселенца и лица без гражданства осуществляется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

5.2.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя

Перечень документов и сведений, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата устанавливается действующим законодательством Российской Федерации об электронной подписи, в том числе частью 2 статьи 17 и частью 2 статьи 18 Федерального закона «Об электронной подписи».

Удостоверяющий центр выполняет свою обязанность по внесению в квалифицированный сертификат только достоверной информации путем подтверждения информации посредством предоставления документов и сведений в Удостоверяющем центре при получении квалифицированного сертификата, а также сбора и хранения копий документов, представленных заявителем, а также путем получения информации и сведений из соответствующих государственных реестров.

При обращении в удостоверяющий центр заявитель предоставляет следующие документы и сведения:

- основной документ, удостоверяющий личность;
- страховой номер индивидуального лицевого счета заявителя – физического лица;
- идентификационный номер налогоплательщика заявителя – физического лица;
- основной государственный регистрационный номер заявителя - юридического лица;
- основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя заявителя - индивидуального предпринимателя;
- номер свидетельства о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя - иностранной организации;

- документ, подтверждающий право заявителя действовать от имени юридического лица без доверенности либо подтверждающий право заявителя действовать от имени государственного органа или органа местного самоуправления.

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.

Заявитель представляет в Удостоверяющий центр документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности Уполномоченного представителя Заявителя, Заявителя-физического лица, а также документы, на основании которых Удостоверяющим центром вносятся сведения в Сертификат, такие как: полное или сокращенное наименование, основной государственный регистрационный номер, юридический адрес, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, наименование должности и иные данные.

5.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона "Об электронной подписи" Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона "Об электронной подписи":

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

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и Удостоверяющий центр идентифицировал заявителя - физическое лицо или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В ином случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата, в том числе, в случаях, установленных пунктами 5 и 6 части 2 статьи 13 Федерального закона «Об электронной подписи»:

- не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

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

5.2.6. Порядок создания квалифицированного сертификата

Создание квалифицированного сертификата ключа проверки электронной подписи осуществляется на основании Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи. Если владельцем сертификата является юридическое лицо, то наряду с указанием наименования такого юридического лица может вноситься информация о физическом лице, действующим от имени юридического лица на основании учредительных документов юридического лица или доверенности.

Удостоверяющий центр проверяет данные в Заявлении на выдачу квалифицированного сертификата на соответствие данным, содержащимся в представленных заявителем документах и данных и сведениях, полученных Удостоверяющим центром из соответствующих государственных информационных ресурсов и устанавливает:

- Факт принадлежности документов предоставившему их лицу и/или лицу, чьи интересы оно предоставляет;
- Факт соответствия сведений, указанных в Заявлении на создание квалифицированного сертификата ключа проверки электронной подписи предоставленным документам и сведениям, а также полученным сведениям из государственных информационных ресурсов;
- Факт отсутствия явных признаков подделки документов.

В случае внесения в квалифицированный сертификат ключа проверки электронной подписи персональных данных физического лица, заявитель – физическое лицо или уполномоченный представитель заявителя-юридического лица предоставляет свое письменное согласие на обработку персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

Удостоверяющий центр осуществляет подтверждение владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата ключа проверки электронной подписи.

Удостоверяющий центр на основаниях, предусмотренных действующем законодательством об электронной подписи или настоящем Порядком, вправе отказать заявителю в создании квалифицированного сертификата.

Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную Удостоверяющим центром.

5.2.7. Порядок выдачи и вручения квалифицированного сертификата

По окончании процедуры создания квалифицированного сертификата ключа проверки электронной подписи Удостоверяющий центр под расписку знакомит

заявителя с информацией, внесенной в квалифицированный сертификат и выдает заявителю:

- Ключ электронной подписи и квалифицированный сертификат (с ключом проверки электронной подписи);
- Копию Сертификата на бумажном носителе (по запросу).

Расписку на бумажном носителе, содержащую описание информации, включенной в квалифицированный сертификат, заявитель передает в Удостоверяющий центр.

Удостоверяющий центр одновременно с выдачей квалифицированного сертификата предоставляет Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При выдаче квалифицированного сертификата Заявитель получает:

- ключ электронной подписи и сертификат ключа проверки электронной подписи;
- лист ознакомления;
- руководство по обеспечению безопасности использования ключа электронной подписи и средств электронной подписи, об условиях и о порядке использования электронной подписи и средств электронной подписи о рисках, связанных с использованием электронной подписи, и о мерах, необходимых для обеспечения безопасности электронной подписи;
- правила использования электронной подписи и средств электронной подписи.

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

Создание и выдача квалифицированного сертификата производится в течение 12 (двенадцати) часов с момента подачи Заявления на выдачу квалифицированного сертификата ключа проверки электронной подписи и получения сведений из государственных информационных ресурсов, при условии подтверждения всех фактов соответствия сведений в заявлении и соблюдения порядка оплаты за услуги. Возможно создание сертификата в течение двадцати минут с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении, предоставлении полного пакета запрашиваемых документов, оплате путем полной предоплаты за услуги и личной явки будущего владельца ЭП за его получением. В случае невозможности автоматизированной проверки указанных данных, документы проверяются уполномоченным лицом Удостоверяющего центра в ручном (неавтоматическом) режиме.

5.3. Подтверждение действительности электронной подписи, использованной для подписания электронных документов

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

Подтверждение действительности электронной подписи, использованной для подписания электронных документов, осуществляется на основании Заявления на подтверждение действительности электронной подписи, использованной для подписания электронных документов, составленного в соответствии с формой, утвержденной Приложением № 3 и Приложением № 4 настоящего Порядка, и подписанного заявителем.

Заявление может быть подано как в форме бумажного документа, подписанного собственноручной подписью заявителя – физического лица или уполномоченного представителя заявителя – юридического лица либо в форме электронного документа, подписанного квалифицированной электронной подписью заявителя.

Обязательным приложением к Заявлению на подтверждение подлинности электронной подписи в электронном документе является предоставление информации, содержащей:

- сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе – в виде файла стандарта CMS;
- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

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

Срок проведения экспертизы по подтверждению действительности электронной подписи в электронном документе составляет 30 (тридцать) рабочих дней с даты получения Удостоверяющим центром Заявления на подтверждение действительности электронной подписи, использованной для подписания электронных документов.

5.3.3. Порядок оказания услуги

Процедура подтверждения действительности электронной подписи в электронном документе осуществляется с использованием специализированного программного обеспечения, входящего в состав сертифицированного средства удостоверяющего центра.

Оказание услуги по подтверждению подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

В ходе процедуры подтверждения действительности ЭП комиссией осуществляется проверка всех квалифицированных сертификатов ключей проверки электронной подписи, на основании которых были сформированы электронные подписи на документах, определение даты формирования каждой электронной подписи в документах, проверку каждого квалифицированного сертификата ключа проверки электронной подписи в цепочке до квалифицированного сертификата ключа проверки электронной подписи Головного удостоверяющего центра, проверку действительности всех квалифицированных сертификатов на момент проверки и отсутствие их в CRL.

Результатом оказания услуги по подтверждению действительности электронной подписи в электронном документе является заключение Удостоверяющего центра.

Заключение содержит:

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

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

При проведении работ Удостоверяющим центром может быть запрошена дополнительная информация.

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

5.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата

Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;

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

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

Заявление на прекращение действия сертификата ключа проверки электронной подписи подается заявителем в Удостоверяющий центр по форме, установленной Приложением № 5 и Приложением № 6 к настоящему Порядку.

Заявление на прекращение действия сертификата ключа проверки электронной подписи может быть подано как в форме бумажного документа, подписанного собственноручной подписью заявителя – физического лица или уполномоченного представителя заявителя – юридического лица либо в форме электронного документа, подписанного квалифицированной электронной подписью заявителя.

При приеме Заявления на Подтверждения прекращения действия сертификата ключа проверки электронной подписи Удостоверяющий центр должен подтвердить полномочия владельца электронной подписи.

Полномочия владельца электронной подписи подтверждаются на основании предоставляемых Заявителем документов, а также с использованием инфраструктуры.

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

Информация о прекращении действия или аннулировании сертификата ключа проверки электронной подписи должна быть внесена удостоверяющим центром в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

Официальным уведомлением о факте прекращения действия и/или аннулировании сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем прекращения действия сертификата ключа проверки электронной подписи признается время издания указанного списка отозванных сертификатов, хранящегося в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей проверки электронных подписей в расширение CRL Distribution Point сертификата ключа подписи.

В случае прекращения действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра по истечении срока его действия в момент прекращения действия сертификата ключа подписи Пользователя Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity

сертификата ключа проверки электронной подписи. В данном случае информация об этом сертификате ключа проверки электронной подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

В случае компрометации ключа электронной подписи Уполномоченного лица Удостоверяющего центра временем прекращения действия сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра признается время компрометации ключа электронной подписи Удостоверяющего центра, фиксирующееся в реестре Удостоверяющего центра. В случае компрометации ключа электронной подписи Удостоверяющего центра информация о сертификате ключа проверки электронной подписи Пользователя Удостоверяющего центра в список отозванных сертификатов не заносится.

5.5. Порядок ведения реестра квалифицированных сертификатов

5.5.1. Формы ведения реестра квалифицированных сертификатов

Реестр квалифицированных сертификатов ведется в электронной форме. Формирование реестра квалифицированных сертификатов включает в себя внесение сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов. Ведение реестра квалифицированных сертификатов включает в себя:

- внесение изменений в реестр квалифицированных сертификатов в случае изменения содержащихся в нем сведений;
- внесение в реестр квалифицированных сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

Доступ к Реестру сертификатов предоставляется путем представления Сертификата в форме электронного документа, либо в форме копии Сертификата на бумажном носителе.

Информация, внесенная в реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в реестре квалифицированных сертификатов, должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

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

Формирование и ведение реестра квалифицированных сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре квалифицированных сертификатов, должна формироваться его резервная копия.

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

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

Сведения о прекращении действия квалифицированного сертификата вносятся аккредитованным удостоверяющим центром в реестр квалифицированных сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в части 6 статьи 14 Федерального закона N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи в реестр квалифицированных сертификатов.

Сведения об аннулировании квалифицированного сертификата вносятся аккредитованным удостоверяющим центром в течение одного рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании аккредитованным удостоверяющим центром сертификатов ключей проверки электронной подписи по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона N 63-ФЗ «Об электронной подписи». Квалифицированный сертификат считается аннулированным с момента внесения указанной записи в реестр квалифицированных сертификатов.

До внесения в реестр квалифицированных сертификатов сведений об аннулировании квалифицированного сертификата аккредитованный удостоверяющий центр обязан уведомить владельца квалифицированного сертификата об аннулировании его квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа.

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

5.6. Порядок технического обслуживания реестра квалифицированных сертификатов

5.6.1. Максимальные сроки проведения технического обслуживания

Плановое и внеплановое техническое обслуживание реестра квалифицированных сертификатов осуществляется преимущественно во внерабочее время Удостоверяющего центра и не может превышать 12 (двенадцати) часов.

5.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

Удостоверяющий центр уведомляет лиц, использующих реестр квалифицированных сертификатов, о проведении планового или внепланового технического обслуживания реестра квалифицированных сертификатов путем размещения информации на официальном сайте Удостоверяющего центра в сети Интернет по адресу: <http://pkitrans.ru/>.

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

Удостоверяющий центр одновременно с выдачей квалифицированного сертификата предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи владельцем сертификата ключа проверки электронной подписи.

6.2. Выдача по обращению заявителя средств электронной подписи

Удостоверяющий центр по обращению заявителя выдает средства электронной подписи, отвечающие требованиям, установленным Федеральным органом исполнительной власти в области обеспечения безопасности.

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона "Об электронной подписи" должны обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями

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

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов, защиту информации от неправомерного доступа, уничтожения, модификации, блокирования и иных неправомерных действий. Актуальность обеспечивается путем своевременного внесения записи о выпуске и аннулировании сертификата ключа проверки электронной подписи в реестр квалифицированных сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения специальных шифровальных средств, способствующих защите информации от несанкционированного проникновения.

Защита информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем:

- предотвращения несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

- своевременным обнаружением фактов несанкционированного доступа к информации;
- предупреждения возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянного контроля за обеспечением уровня защищенности информации;
- размещения баз данных информации в контролируемой зоне, исключающей свободное пребывание посторонних лиц;
- использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре квалифицированных сертификатов, должна формироваться его резервная копия.

Персонал Удостоверяющего центра до получения допуска к работам, связанным с выполнением целевых функций удостоверяющего центра, в обязательном порядке проходит специализированное обучение и инструктаж по соблюдению требований информационной безопасности при реализации целевых функций Удостоверяющего центра. Сотрудники Удостоверяющего центра выполняют требования обеспечения информационной безопасности, содержащиеся в соответствующих должностных инструкциях сотрудников Удостоверяющего центра и в организационно-распорядительных документах Удостоверяющего центра.

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

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

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.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет по адресу <http://cert.pkitrans.ru/> к реестру квалифицированных сертификатов Удостоверяющего центра в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами.

6.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Ключ электронной подписи является конфиденциальной информацией владельца квалифицированного сертификата. Владелец квалифицированного сертификата должен обеспечивать конфиденциальность ключа электронной подписи, в частности не допускать использование ключа электронной подписи без его согласия.

В Удостоверяющем центре ключ электронной подписи создается заявителем на автоматизированном рабочем месте, аттестованном на соответствие требованиям по безопасности информации, размещенным в помещении центра выдачи Удостоверяющего центра, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается на ключевой носитель. После окончания процедуры создания ключа электронной подписи заявитель забирает ключевой носитель с записанным на нем ключом электронной подписи.

Для создания ключа электронной подписи в Удостоверяющем центре используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63-ФЗ «Об электронной подписи».

В случае нарушения конфиденциальности ключа электронной подписи, а также в случае наличия оснований полагать, что конфиденциальность ключа электронной подписи была нарушена, владелец сертификата ключа проверки электронной подписи, соответствующего такому ключу электронной подписи, должен прекратить использование этого ключа и подать в Удостоверяющий центр Заявление на прекращение действия квалифицированного сертификата.

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

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для

регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

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

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии. Регистрация осуществляется на основании Заявления на регистрацию в Единой системе идентификации и аутентификации, составленному по форме Приложения № 7 к настоящему Порядку.

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

Информация, содержащаяся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, предоставляется безвозмездно. Обращение подается при личном прибытии владельца электронной подписи в Удостоверяющий центр в рабочее время Удостоверяющего центра, либо почтовой или курьерской службой, или круглосуточно через форму на сайте Удостоверяющего центра <http://cert.pkitrans.ru/> (по выбору лица, обратившегося за получением информации из реестра квалифицированных сертификатов). Обработка запроса осуществляется в режиме реального времени «онлайн». Информация предоставляется заинтересованному лицу в форме электронного сообщения.

7. Сроки действия ключей и сертификатов

7.1. Сроки действия Ключей электронной подписи Удостоверяющего центра

- 7.1.1. Срок действия Ключей электронной подписи Удостоверяющего центра составляет 1 год и 3 месяца.
- 7.1.2. Начало действия Ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего Сертификата.
- 7.1.3. В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия Ключа проверки электронной подписи не должен превышать срок действия соответствующего Ключа электронной подписи более чем

на 15 лет, максимально допустимый срок действия Сертификата Удостоверяющего центра составляет 16 лет.

7.2. Сроки действия Ключей электронной подписи и Сертификатов Ключей проверки электронной подписи

7.2.1. Срок действия Ключей электронной подписи составляет 1 год и 3 месяца.

7.2.2. В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия Ключа проверки электронной подписи не должен превышать срок действия соответствующего Ключа электронной подписи более чем на 15 лет, максимально допустимый срок действия Сертификата Пользователя УЦ – 15 лет.

7.2.3. Начало действия Ключа электронной подписи Пользователя УЦ исчисляется с даты и времени начала действия соответствующего Сертификата Пользователя УЦ.

7.2.4. Срок действия Сертификата Пользователя УЦ устанавливается УЦ в момент его изготовления.

Приложение № 1
к Порядку реализации функций
Аккредитованного удостоверяющего центра АО
«НИИАС» и исполнения его обязанностей

**Форма заявления на выдачу квалифицированного сертификата ключа
проверки электронной подписи для юридических лиц**

Для юридических лиц

Заявление

на выдачу квалифицированного сертификата ключа проверки электронной подписи

Наименование юридического лица, включая организационно-правовую форму

должность руководителя юридического лица или уполномоченного сотрудника

фамилия, имя, отчество

действующий на основании _____

основание полномочий

заявляет об акцепте действующего на дату регистрации Заявления «Порядка реализации функций Аккредитованного Удостоверяющего центра АО «НИИАС» и исполнения его обязанностей», в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации и просит создать квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) с указанием физического лица - Пользователя Аккредитованного удостоверяющего центра АО «НИИАС» - в соответствии со следующими идентификационными данными:

Сведения о физическом лице – Пользователе Аккредитованного удостоверяющего центра	
Фамилия	
Имя	
Отчество	
Пол	
Дата рождения	
СНИЛС	
Гражданство	
Документ, удостоверяющий личность	Тип документа: _____ серия _____ номер _____ дата выдачи _____ выдан _____ код подразделения (при наличии) _____ - _____
Должность	
<p>Настоящим выражаю согласие с обработкой своих персональных данных АО «НИИАС», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение). Персональные данные, на обработку которых дается согласие в целях исполнения договора, предусматривающего оказание услуг удостоверяющего центра в соответствии с федеральным законом от 06.04.2008 №63-ФЗ «Об электронной подписи» (далее ФЗ «Об электронной подписи») для изготовления квалифицированных сертификатов: фамилия, имя, отчество, ИНН, СНИЛС, место работы (организация), подразделение, должность, адрес места жительства, адрес электронной почты, пол, телефон, паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации). Соглашаюсь с указанием своих персональных данных согласно приказу Минкомсвязи РФ от 05.10.2011 № 250 в реестре выданных АО «НИИАС» квалифицированных сертификатов, при этом признаю, что в соответствии с п. 3 ст. 15 ФЗ «Об электронной подписи» АО «НИИАС» обязан обеспечить любому лицу безвозмездный доступ к реестру квалифицированных сертификатов АО «НИИАС». Соглашаюсь с передачей своих персональных данных в Единую систему идентификации и аутентификации в целях обеспечения требования ч. 5 ст. 18 ФЗ «Об электронной подписи».</p> <p style="text-align: right;">Подпись субъекта персональных данных (лица, указываемого в квалифицированном сертификате)</p>	

Сведения об организации

ОГРН	
ИНН	
Контактный телефон	
Адрес электронной почты	

просит указать при заполнении квалифицированного сертификата адрес места нахождения и наименование юридического лица согласно данных выписки из государственных информационных ресурсов на дату создания квалифицированного сертификата.

Должность руководителя (или уполномоченного
сотрудника)

подпись

Ф.И.О.

М.П.

«__»_____20__г.

**Форма заявления на подтверждение действительности электронной подписи,
использованной для подписания электронных документов для юридических лиц**

Для юридических лиц

**Заявление
на подтверждение действительности электронной подписи
в электронном документе**

Полное наименование юридического лица, включая организационно-правовую форму

должность руководителя юридического лица или уполномоченного сотрудника

фамилия, имя, отчество

действующий на основании _____,

основание полномочий

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

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе - рег. № XXX;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе - рег. № XXX;
3. Время на момент наступления которого требуется подтвердить подлинность электронной подписи¹

« _____ : _____ » « _____ / _____ / _____ »;
Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

« _____ : _____ » « _____ / _____ / _____ »;
Час минута день месяц год

подпись

Ф.И.О.

**Форма заявления на подтверждение действительности электронной подписи,
использованной для подписания электронных документов для физических лиц и ИП**

Для физических лиц

**Заявление
на подтверждение действительности электронной подписи, использованной для
подписания электронных документов**

Я, _____

(фамилия, имя, отчество)

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

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе - рег. № XXX;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе - рег. № XXX;
3. Время на момент наступления которого требуется подтвердить подлинность электронной подписи²

«_____ : _____» «_____ / _____ / _____»;
Час минута день месяц год

Если момент подписания электронного документа не определен, то указать время, на момент наступления которого необходимо проверить подлинность электронной подписи:

«_____ : _____» «_____ / _____ / _____»;
Час минута день месяц год

«_____» _____ 20 _____ года _____

подпись

Ф.И.О.

**Форма заявления на прекращение действия сертификата ключа проверки
электронной подписи для юридических лиц**

Для юридических лиц

Заявление
на прекращение действия сертификата ключа проверки электронной подписи

Полное наименование организации, включая организационно-правовую форму

должность руководителя юридического лица или уполномоченного сотрудника

фамилия, имя, отчество

действующий на основании _____

основание полномочий

просит прекратить действие сертификата ключа проверки электронной подписи,
содержащего следующие данные:

Серийный номер сертификата	
Наименование юридического лица	
ИНН	
ОГРН	
Фамилия	
Имя Отчество	

Должность руководителя (или уполномоченного
сотрудника)

подпись

Ф.И.О.

М.П.

«__» _____ 20__ г.

Приложение № 6
к Порядку реализации
функций Аккредитованного
удостоверяющего центра АО «НИИАС» и
исполнения его обязанностей

**Форма заявления на прекращение действия сертификата ключа
проверки электронной подписи для физических лиц и ИП**

Для физических лиц

Заявление

на прекращение действия сертификата ключа проверки электронной подписи

Я, _____

фамилия, имя, отчество

паспорт серии _____ № _____ выдан « _____ » _____ года

наименование органа, выдавшего документ

прошу прекратить действие сертификата ключа проверки электронной
подписи, содержащего следующие данные:

Серийный номер сертификата	
Фамилия, имя, отчество	
СНИЛС	

подпись

Ф.И.О. Заявителя

« _____ » _____ 20 _____ года

Приложение № 7
к Порядку реализации
функций Аккредитованного
удостоверяющего центра АО «НИИАС» и
исполнения его обязанностей

**Форма Заявления на регистрацию в Единой системе
идентификации и аутентификации**

Заявление

на регистрацию в Единой системе идентификации и аутентификации

Я, _____

фамилия, имя, отчество

в соответствии с пунктом 5 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ "Об электронной подписи" прошу Удостоверяющий центр АО «НИИАС» зарегистрировать меня в единой системе идентификации и аутентификации в соответствии со следующими сведениями:

Фамилия	
Имя	
Отчество	
Пол	
Дата рождения	
СНИЛС	
Гражданство	
Документ, удостоверяющий личность	Тип документа: _____ серия_номер_дата выдачи _____ выдан _____ код подразделения (при наличии) _____ - _____
Номер мобильного телефона	+7 (_____) _____
Адрес электронной почты	
Способ доставки пароля для первого входа в систему	[] – отправка на email [] – отправка на номер мобильного телефона

Настоящим выражаю согласие с обработкой своих персональных данных АО «НИИАС», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение). Персональные данные, на обработку которых дается согласие в целях регистрации в единой системе идентификации и аутентификации в соответствии с ч.5 ст. 18 федерального закона от 06.04.2008 №63-ФЗ «Об электронной подписи» (далее ФЗ «Об электронной подписи»): фамилия, имя, отчество, СНИЛС, адрес электронной почты, пол, абонентский номер(мобильный телефон), паспортные данные (серия и номер, код подразделения, место и дата рождения, дата выдачи паспорта, адрес регистрации).

_____/_____/_____ «___» _____ 20__ г.

ПОДПИСЬ