Приложение

УТВЕРЖДЕН
приказом АО «НИИАС»
от 27 января 2025 г. № 05

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

г. Москва
2025 г.

Термины и определения, используемые в настоящем Порядке

Единая биометрическая система (ЕБС) — государственная цифровая платформа, которая позволяет установить и подтвердить личность человека по его физиологическим и биологическим характеристикам.

Единая система идентификации и аутентификации (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах.

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, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий 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 Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» 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 Федеральным законом № 63-ФЗ 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 - физический носитель определенной структуры, предназначенный для хранения ключевой информации 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».

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.

Инфраструктура - информационно-технологическая и коммуникационная инфраструктура, установленная частью 4 статьи 19 Федерального закона от 27 июля 2010 года N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Заявитель - физическое лицо, 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.

Список сокращений

Сокращение	Значение
ЕПГУ	Единый портал государственных и муниципальных услуг
ПО	Программное обеспечение
СМЭВ	Единая система межведомственного электронного взаимодействия
СКЗИ	Средство криптографической защиты информации
СКПЭП, Сертификат	Сертификат ключа проверки электронной подписи
УЦ	Удостоверяющий центр
ЭП	Электронная подпись
КЭП	Квалифицированная электронная подпись
Владелец сертификата	Владелец квалифицированного сертификата ключа проверки электронной подписи
Порядок	Порядок реализации функций и исполнения обязанностей Удостоверяющего центра АО «НИИАС»
Вручение сертификата ключа проверки электронной подписи	Передача Удостоверяющим центром или его Доверенным лицом, 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 в соответствии с Приказом ФСБ России от 20.04.2021 №154 «Об утверждении Правил подтверждения владения ключом электронной подписи» (далее – Приказ ФСБ №154)

1. Общие положения

1.1. Предмет регулирования Порядка

1.1.1. Настоящий Порядок реализации функций аккредитованного удостоверяющего центра АО «НИИАС» и исполнения его обязанностей (далее – Порядок) разработан в соответствии с действующим законодательством Российской Федерации, в том числе с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», и устанавливает порядок реализации функций УЦ, условия предоставления и правила пользования услугами УЦ, включая права, обязанности и ответственность УЦ, Заявителя, организационные мероприятия, направленные на обеспечения работы УЦ.

1.1.2. 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.

1.1.3. Любое физическое лицо, подавшее в Удостоверяющий центр заявление (Приложение № 1) на создание 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.

1.1.4. 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.

1.1.5. Любые изменения, вносимые в Порядок, с момента вступления в силу распространяются на всех лиц, присоединившихся к Порядку, независимо от даты присоединения.

1.1.6. В случае несогласия с изменениями Владелец сертификата имеет право на расторжение договора присоединения в соответствии с подп. 2.1.3. Порядка.

1.1.7. Заявитель, присоединившийся к настоящему Порядку, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Порядок в виде его новой редакции путем самостоятельного ознакомления с текстом Порядка на сайте УЦ по адресу – http://pkitrans.ru.

1.1.8. Присоединяясь к настоящему Порядку и принимая его нормы и правила, Заявитель выражает согласие с обработкой своих персональных данных УЦ АО «НИИАС», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение. Персональные данные, на обработку которых дается согласие в целях получения Заявителем рассылок информационного характера:

фамилия, имя, отчество, номер телефона, адрес электронной почты. Настоящее согласие действует со дня его подписания до дня его отзыва, но не более 50 лет.

1.1.9. Заявитель вправе отозвать согласие путем личного обращения или направления им письменного обращения (в том числе в форме электронного документа, подписанного простой электронной подписью или усиленной квалифицированной электронной подписью), на имя руководителя УЦ АО «НИИАС» в письменном виде на почтовый адрес: 109029, Россия, г. Москва, ул. Нижегородская 27, строение 1, а также на адрес электронной почты – cainfo@vniias.ru.

1.2. Сведения об Удостоверяющем центре

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

1.2.2. 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 Единый государственный реестр юридических лиц (далее – ЕГРЮЛ) за основным государственным регистрационным номером 1077758841555 от 08.08.2007 г.

1.2.3. 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 следующих документов:

- лицензия 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 (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;

- Приказ Минкомсвязи России № 179 от 17.07.2013 «Об аккредитации удостоверяющих центров»;

- УЦ НИИАС аккредитован в соответствии с решением Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров (протокол от 01.10.2021 № 9пр).

1.2.4. 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.

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

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

1.2.7. График работы Удостоверяющего центра (далее – рабочий день) – промежуток времени 9:00 - 18:00 с понедельника по четверг и 9:00 до 16:45 в пятницу (время Московское) за исключением выходных и праздничных дней.

1.3. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.3.1. Контактные данные:
Телефон: (499) 262-55-29;
E-mail: cainfo@vniias.ru;
Электронный адрес в сети Интернет (сайт Удостоверяющего центра): http://pkitrans.ru.

1.3.2. Заявители вправе получить информацию по вопросам предоставления услуг Удостоверяющего центра, обратившись в Удостоверяющий центр любым из указанных в п.1.3.1. настоящего Порядка способом, либо самостоятельным получением информации, размещенной на сайте Удостоверяющего центра.

1.4. Стоимость услуг Удостоверяющего центра

1.4.1. Удостоверяющий центр оказывает услуги на платной основе.

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

1.4.3. 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».

1.4.4. При оплате услуг путем полной или частичной предоплаты, срок изготовления сертификата может составлять до 5-ти (пяти) рабочих дней с момента осуществления следующих действий в совокупности:

а. представления всех документов и/ или сведений, необходимых для выпуска сертификата;

б. зачисления перечисленных Заявителем денежных средств на расчетный счет УЦ.

1.4.5. Срок действия сертификата начинается с момента его изготовления согласно дате начала действия, указанной в нем.

1.4.6. В случае отказа заказчика от получения уже изготовленного на основании заявления сертификата, уплаченные денежные средства не возвращаются.

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

1.4.8. Размер платы, указанный в п.1.4.2 не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации.

1.5. Присоединение к Порядку

1.5.1. Настоящий Порядок является договором присоединения на основании статьи 428 Гражданского кодекса РФ. Настоящий Порядок предназначен служить соглашением, налагающим обязанности на все вовлечённые стороны, а также средством официального уведомления и информирования всех сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

1.5.2. Фактом присоединения Заявителя к настоящему Порядку является подача в Удостоверяющий центр заявления на создание квалифицированного СКПЭП (Приложение № 1).

1.5.3. С момента присоединения Заявителя к настоящему Порядку, Заявитель полностью и безоговорочно соглашается со всеми условиями настоящего Порядка и приложений к нему.

1.5.4. Заявитель, присоединившийся к настоящему Порядку, самостоятельно отслеживает изменения (дополнения), вносимые в настоящий Порядок в виде его новой редакции путем самостоятельного ознакомления с текстом Порядка на сайте УЦ по адресу – http://pkitrans.ru.

1.6. Изменение Порядка

1.6.1. Внесение изменений в Порядок, включая приложения к нему, производится УЦ в одностороннем порядке.

1.6.2. Уведомление Владельцев сертификатов о внесении изменений в Порядок осуществляется УЦ путем размещения новой редакции настоящего Порядка, включающей указанные изменения, на сайте УЦ по адресу – http://pkitrans.ru.

1.6.3. Изменения, вносимые УЦ в Порядок, кроме изменений, вносимых в связи с изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон с даты их публикации на сайте по адресу: http://pkitrans.ru.

1.6.4. Изменения, вносимые УЦ в Порядок в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих нормативных правовых актов, повлекших изменения законодательства Российской Федерации.

1.6.5. Любые изменения, вносимые в Порядок, с момента вступления в силу распространяются на всех лиц, присоединившихся к Порядку, независимо от даты присоединения.

1.7. Разрешение споров

1.7.1. Сторонами в споре, в случае его возникновения, считаются УЦ и Заявитель или Владелец сертификата.

1.7.2. Стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Порядка, путём переговоров.

1.7.3. Споры между сторонами, связанные с действием настоящего Порядка, не урегулированные в процессе переговоров, рассматриваются в судебном порядке в соответствии с действующим законодательством Российской Федерации, по месту нахождения УЦ.

2. Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)

В перечень реализуемых УЦ функций (оказываемых услуг) в соответствии с настоящим Порядком, входят:

2.1. Создание сертификатов ключей проверки электронных подписей и выдача таких сертификатов лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) при его личном присутствии либо посредством идентификации заявителя с применением информационных технологий 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, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы.

2.2. Осуществление в соответствии с правилами подтверждения владения ключом ЭП подтверждения владения Заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному им для получения СКПЭП.

2.3. Установление сроков действия СКПЭП.

2.4. Аннулирование выданных УЦ СКПЭП.

2.5. Выдача по обращению заявителя средства ЭП, содержащие ключ ЭП и ключ проверки ЭП (в том числе созданные УЦ) или обеспечивающие возможность создания ключа ЭП и ключа проверки ЭП Заявителем.

2.6. Ведение Реестра сертификатов, в том числе включающего в себя информацию, содержащуюся в выданных УЦ СКПЭП, и информацию о датах прекращения действия или аннулирования СКПЭП и об основаниях таких прекращения или аннулирования.

2.7. Создание по обращениям Заявителей ключей ЭП и ключей проверки ЭП (Приложение № 1).

2.8. Проверка уникальности ключей проверки электронных подписей в Реестре сертификатов.

2.9. Осуществление по обращениям участников электронного взаимодействия подтверждения действительности ЭП, используемой для подписания электронных документов (Приложение № 2).

2.10. По желанию лица, которому выдан квалифицированный сертификат, безвозмездное осуществление регистрации указанного лица в ЕСИА (при подаче заявления на регистрацию в ЕСИА по форме Приложения № 4).

2.11. Изготовление и выдача по запросам владельцев Сертификатов заверенных копий Сертификатов на бумажных носителях.

2.12. Предоставление безвозмездно любому лицу по его обращению, в соответствии с установленным Порядком, доступа к информации, содержащейся в Реестре сертификатов, в том числе к информации об аннулировании Сертификата.

2.13. Осуществление иных, связанных с использованием ЭП, функций, установленных законодательством Российской Федерации и иную, связанную с использованием ЭП, деятельность.

2.14. Предоставление пользователям УЦ Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи – Правил использования СКЗИ и ЭП (Приложение № 5), а также иных инструкций по работе со СКЗИ и информационной безопасности.

3. Права и обязанности Удостоверяющего центра

3.1. Удостоверяющий центр имеет право:

3.1.1. Наделить третьих лиц полномочиями по приему заявлений на выдачу СКПЭП, а также вручению СКПЭП от имени УЦ. При совершении порученных УЦ действий доверенное лицо обязано идентифицировать Заявителя при его личном присутствии.

3.1.2. Выдавать СКПЭП как в форме электронных документов, так и в форме документов на бумажном носителе. Владелец СКПЭП, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную удостоверяющим центром.

3.1.3. Отказать Заявителю в изготовлении 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.

3.1.4. Отказать Заявителю в принятии Заявления на выдачу СКПЭП в случае, если использованное Заявителем для формирования запроса на сертификат СКЗИ технически не поддерживается УЦ.

3.1.5. Аннулировать Сертификат Пользователя УЦ, если УЦ стало известно, что Владелец Сертификата не владеет Ключом ЭП, соответствующим Ключу проверки ЭП, указанному в таком Сертификате в соответствии с Приказом ФСБ России от 20.04.2021 №154.

3.1.6. Прекратить действие Сертификата Пользователя УЦ в случае получения УЦ подтвержденной информации о смерти Владельца Сертификата – физического лица.

3.1.7. Отказать в принятии Заявления на выдачу СКПЭП в случаях подачи заявления на выдачу Сертификата в неактуальной форме, оформленного ненадлежащим образом, имеющего исправления, ошибки и/или приписки, не подтвержденные собственноручной подписью Заявителя, а также в случае непредставления в УЦ документов и сведений, предусмотренных настоящим Порядком.

3.1.8. Отказать в изготовлении сертификата ключа подписи Заявителю в случае невыполнения Заявителем обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Порядком.

3.1.9. Подтверждать достоверность сведений, перечисленных в пунктах 1 и 2 части 1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» одним из следующих способов:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;
2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;
3) с использованием единой системы идентификации и аутентификации.

3.1.10. Взимать плату, размер которой не должен превышать предельный размер, порядок определения которого вправе установить Правительство Российской Федерации, за выдачу квалифицированного сертификата.

3.2. Удостоверяющий центр обязан:

3.2.1. Информировать заявителей об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки.

3.2.2. Обеспечивать актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.2.3. 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 СКПЭП.

3.2.4. Обеспечивать конфиденциальность созданных УЦ ключей ЭП.

3.2.5. Отказать Заявителю в создании СКПЭП в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения СКПЭП.

3.2.6. Отказать заявителю в создании СКПЭП в случае отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки электронной подписи, указанного заявителем для получения СКПЭП.

3.2.7. Незамедлительно информировать Владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа ЭП, не предусмотренных соглашением сторон, или возникновения у аккредитованного УЦ обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа ЭП.

3.2.8. Не указывать в создаваемом им СКПЭП ключ проверки ЭП, который содержится в СКПЭП, выданном УЦ любым другим УЦ.

3.2.9. Вносить информацию о прекращении действия СКПЭП 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 УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие СКПЭП прекращается с момента внесения записи об этом в реестр сертификатов.

3.2.10. Хранить информацию, указанную в ч. 1 ст. 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» в течение всего срока деятельности УЦ, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации.

3.2.11. Хранить следующую информацию:

- реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
- СНИЛС - номер страхового номера индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;
- ИНН - идентификационный номер налогоплательщика.

3.2.12. Хранение указанной в пункте 3.2.11 информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

3.2.13. Для подписания от своего имени квалифицированных сертификатов использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном УЦ головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. УЦ 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.

3.2.14. Обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к

Реестру сертификатов УЦ 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.

3.2.15. 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;
- уведомить в письменной форме владельцев СКПЭП, которые выданы УЦ и срок действия которых не истек. УЦ должен направить такое уведомление не менее чем за один месяц до даты прекращения деятельности УЦ.

3.2.16. 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 от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с действующем законодательством Российской Федерации об электронной подписи.

3.2.17. При выдаче квалифицированного сертификата:

1) В порядке, установленном Федеральным законом от 06.04.2011 № 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, или 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, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические данные, или путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы.

2) Предложить использовать шифровальные (криптографические) средства, указанные в статье 19 Федерального закона от 29 декабря 2022 г. № 572-ФЗ

«Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», 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»), безвозмездно предоставляемые по адресу – http://pkitrans.ru. При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения его идентификации в аккредитованном удостоверяющем центре без его личного присутствия посредством информационно-телекоммуникационной сети «Интернет» при выдаче сертификата ключа проверки электронной подписи отказывается от использования шифровальных (криптографических) средств, аккредитованный удостоверяющий центр обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

3) 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.

3.2.18. С использованием инфраструктуры осуществить проверку достоверности документов и сведений, представленных заявителем – физическим лицом в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

3.2.19. При получении квалифицированного сертификата Заявителем, ознакомить Заявителя (владельца сертификата) с информацией, содержащейся в квалифицированном сертификате (Приложение № 6). 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.

3.2.20. Одновременно с выдачей квалифицированного сертификата предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования КЭП и средств КЭП - Правила использования СКЗИ и ЭП (Приложение № 5).

3.2.21. При выдаче квалифицированного сертификата направлять в ЕСИА 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 УЦ по желанию владельца квалифицированного сертификата безвозмездно осуществлять его регистрацию в ЕСИА с проведением идентификации владельца при его личном присутствии.

3.2.22. Незамедлительно информировать владельца сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа ЭП, не предусмотренных соглашением сторон, или возникновения у УЦ обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа ЭП.

3.2.23. Изготавливать ключ ЭП с пометкой «неэкспортируемый». Под неэкспортируемостью понимается невозможность копирования/извлечения контейнера ключа электронной подписи с защищённого ключевого носителя.

3.2.24. Отказать в прекращении действия сертификата в случае ненадлежащего оформления соответствующего Заявления на прекращение действия сертификата ключа проверки электронной подписи (Приложение № 3).

4. Права и обязанности Владельцев СКПЭП

4.1. Владелец сертификата обязан:

4.1.1. Обеспечить конфиденциальность ключа ЭП. Не использовать ключ ЭП и немедленно обратиться в УЦ, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа ЭП нарушена.

4.1.2. Извещать УЦ обо всех изменениях данных, внесенных в сертификат.

4.1.3. При подаче заявления на СКПЭП указать действующий электронный почтовый адрес Владельца сертификата для получения извещений, уведомлений от УЦ, связанных с применением СКПЭП или его аннулированием.

4.1.4. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

4.1.5. Применять для формирования электронной подписи только действующий личный закрытый ключ.

4.1.6. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

4.1.7. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи.

4.1.8. Немедленно обратиться в УЦ с заявлением на прекращение действия СКПЭП (Приложение № 3) в случае утери, кражи, а также в случае, если Владельцу сертификата стало известно, что ключ используется или использовался ранее другими лицами.

4.1.9. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление, на аннулирование которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата по момент времени официального уведомления об аннулировании сертификата.

4.1.10. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который аннулирован.

4.1.11. Предоставлять в УЦ только достоверную информацию.

4.1.12. С целью обеспечения гарантированного ознакомления с изменениями и дополнениями Порядка до вступления их в силу не реже одного раза в 10 (десять) календарных дней обращаться на сайт УЦ за сведениями об изменениях и дополнениях в Порядке.

4.1.13. Использовать для хранения ключа ЭП ключевой носитель, поддерживаемый используемым средством ЭП и соответствующей требованиями законодательства и нормативных правовых актов Российской Федерации.

4.1.14. Не использовать ключ ЭП, связанный с СКПЭП, заявление на прекращение действия которого (Приложение № 3) подано в УЦ в течение времени, исчисляемого с момента времени подачи такого заявления в УЦ по момент времени официального уведомления о прекращении действия данного СКПЭП.

4.1.15. Известить УЦ об изменениях в ранее представленных данных, указанных в заявлении на создание квалифицированного СКПЭП (Приложение № 1), и по требованию УЦ в течение 5 (пяти) рабочих дней представить документы, подтверждающие изменения, а при необходимости по согласованию с УЦ провести внеплановую замену СКПЭП.

4.1.16. Обеспечивать незамедлительное уничтожение принадлежащих ему ключей ЭП по истечении сроков их действия, применяя для этого прошедшие в установленном порядке процедуру оценки соответствия средства ЭП, в составе которых реализована функция уничтожения информации.

4.2. Владелец СКПЭП имеет право:

4.2.1. Получать сведения об УЦ и (или) Доверенном лице УЦ.

4.2.2. Получать информацию о перечне, стоимости, сроках и порядке оказания услуг УЦ.

4.2.3. Ознакамливаться с актуальной редакцией Порядка.

4.2.4. Владелец СКПЭП, выданного в форме электронного документа, вправе получить также копию СКПЭП на бумажном носителе, заверенную УЦ.

4.2.5. Обратиться в УЦ с заявлением на создание квалифицированного СКПЭП (Приложение № 1).

4.2.6. Обратиться в УЦ с заявлением на прекращение действия СКПЭП (Приложение № 3), владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.

4.2.7. Обратиться в УЦ за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени.

4.2.8. Обратиться в УЦ за подтверждением действительности ЭП, используемой для подписания электронного документа (Приложение № 2), сформированной с использованием сертификата ключа подписи, изданного УЦ.

4.2.9. Осуществлять иные права, предусмотренные для Заявителей, действующим законодательством и Порядком.

4.2.10. Владелец-юридическое лицо в связи с использованием им СКПЭП, выданного ему до 31.08.2023 г., имеет права, предусмотренные подпунктами 4.2.1 – 4.2.10 пункта 4.2 настоящего Порядка и обязанности, установленные подпунктами 4.1.1 – 4.1.16 пункта 4.1 настоящего Порядка.

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 ЭП и ключей проверки ЭП

Ключ ЭП и ключ проверки ЭП, предназначенные для создания и проверки усиленной КЭП, в соответствии с частью 4 статьи 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» создаются с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Создание ключей ЭП и ключей проверки ЭП осуществляется одним из следующих способов:

1) Заявитель создает ключи ЭП самостоятельно на своем рабочем месте с использованием предоставленных УЦ либо собственных средств ЭП 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).

2) УЦ создает ключ ЭП и ключ проверки ЭП для заявителя в соответствии с правилами пользования СКЗИ, 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 ЭП и ключ проверки ЭП, 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 УЦ, используемого для создания ключа ЭП и ключа проверки ЭП для Заявителя.

Ключ ЭП и ключ проверки ЭП, независимо от способа создания, записывается на ключевой носитель в соответствии с эксплуатационной документацией на используемое СКЗИ.

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

Плановая смена ключей ЭП УЦ выполняется в период действия ключа ЭП УЦ по следующим основаниям:

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

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

1. УЦ создает новый ключ ЭП и соответствующий ему ключ проверки ЭП;
2. УЦ направляет во ФГИС ГУЦ запрос на выдачу подчиненного сертификата аккредитованного удостоверяющего центра;
3. ФГИС ГУЦ изготавливает новый СКПЭП Уполномоченного лица УЦ и передает УЦ;
4. УЦ устанавливает выданный ФГИС ГУЦ новый СКПЭП Уполномоченного лица УЦ.

При плановой замене ключа ЭП УЦ все владельцы ЭП должны установить на своих автоматизированных рабочих местах новый сертификат УЦ.

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

Доверенным способом получения нового квалифицированного СКПЭП 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 УЦ в период действия старого ключа УЦ.

5.1.3. Порядок осуществления смены ключей ЭП УЦ в случаях нарушения их конфиденциальности

Внеплановая смена ключей выполняется в следующих случаях:

1) ключ ЭП УЦ закончил свой срок действия, а плановая смена произведена не была;

2) произошла компрометация ключа ЭП УЦ;

3) есть подозрение, что ключ ЭП УЦ мог быть скомпрометирован;

4) ключ ЭП УЦ не доступен (ключевой носитель поврежден, уничтожен и т.д.);

5) в связи с необходимостью внести изменение в содержимое СКПЭП УЦ (введение новых Требований к форме или формату сертификата и т.д.);

6) по решению суда, вступившему в законную силу, по решению учредителя (учредителей) УЦ и т.д.

Смена ключа ЭП УЦ осуществляется в случае нарушения конфиденциальности ключа ЭП или угрозы нарушения конфиденциальности такого ключа ЭП.

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

К случаям нарушения конфиденциальности (компрометации) ключа ЭП УЦ относятся в том числе:

а) физическая утеря/кража носителя ключа ЭП УЦ.

б) 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 устройств контроля несанкционированного доступа (слепков печатей), повреждение замков и т. п.);

в) увольнение сотрудников, имевших доступ к ключевой информации;

г) нарушение правил хранения и уничтожения (после окончания срока действия) ключа ЭП;

д) иные случаи компрометации.

Процедура внеплановой смены ключей УЦ выполняется в порядке, определённом процедурой плановой смены ключей УЦ согласно п. 5.1.2.

Смена ключей ЭП УЦ в случаях нарушения их конфиденциальности осуществляется в срок, не превышающий 7 (семь) рабочих дней.

В случае компрометации ключа ЭП УЦ СКПЭП УЦ прекращает свое действие, Владельцы сертификатов уведомляются об указанном факте путем публикации информации о компрометации на сайте УЦ по адресу: http://pkitrans.ru.

Все сертификаты, созданные с использованием скомпрометированного ключа ЭП УЦ, считаются прекратившими свое действие с занесением соответствующих сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: http://pkitrans.ru, доступная для скачивания и исключающая уничтожение, модифицирование, блокирование при передаче и иные неправомерные действия с квалифицированным сертификатом.

5.1.4. Порядок осуществления УЦ смены ключа ЭП владельца квалифицированного сертификата

5.1.4.1. Смена ключа электронной подписи владельца квалифицированного сертификата осуществляется в случаях, указанных в пунктах 1, 2, 4 части 6 и части 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», в том числе:

1) в связи с истечением установленного срока его действия;

2) на основании заявления владельца СКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

3) если не подтверждено, что владелец СКПЭП владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

4) если установлено, что содержащийся в таком сертификате ключ проверки ЭП уже содержится в ином ранее созданном СКПЭП;

5) если вступило в силу решение суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию;

6) иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и Владельцем сертификата.

5.1.4.2. При смене сертификата Владелец сертификата подает заявление на изготовление квалифицированного СКПЭП в соответствии с требованиями к заявлению, указанными в п. 5.2.2. настоящего Порядка.

5.1.4.3. Заявление на смену ключа электронной подписи владельца квалифицированного сертификата может быть создано в форме электронного документа, подписанного усиленной квалифицированной ЭП владельца валидного квалифицированного сертификата (квалифицированного сертификата срок действия которого не истек, который не аннулирован, действие которого не прекращено, конфиденциальность ключа ЭП не нарушена), 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 ЭП владельца квалифицированного сертификата.

5.1.4.4. Процедура выдачи квалифицированного сертификата и ключа ЭП (при необходимости) Владельцу сертификата

При выдаче квалифицированного сертификата УЦ:

1) в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», идентифицирует заявителя - физическое лицо, обратившееся за получением квалифицированного сертификата;

2) с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных Заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

3) отказывает в создании СКПЭП, в случае:

- если не было подтверждено то, что Заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному Заявителем для получения СКПЭП;
- отрицательного результата проверки в Реестре сертификатов уникальности ключа проверки ЭП, указанного Заявителем для получения СКПЭП;
- отрицательного результата проверки с использованием инфраструктуры достоверности документов и сведений, предоставленных Заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

4) создает СКПЭП, в случае положительного результата проверки с использованием инфраструктуры достоверности документов и сведений, предоставленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и идентификации Заявителя;

5) ознакамливает с информацией, содержащейся в СКПЭП. Подтверждение ознакомления (Приложение № 6) с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку посредством использования Заявителем КЭП 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;

6) предоставляет Владельцу сертификата руководство по обеспечению безопасности использования КЭП и средств КЭП, об условиях и о порядке использования ЭП и средств ЭП (СКЗИ), о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП - Правила использования СКЗИ и ЭП (Приложение № 5);

7) направляет в ЕСИА сведения о выданном квалифицированном сертификате;

8) по желанию лица, которому выдан квалифицированный сертификат безвозмездно осуществляет регистрацию в ЕСИА (при подаче заявления по форме Приложения № 4) с проведением идентификации Владельца при его личном присутствии.

5.2. Процедура создания и выдачи квалифицированных сертификатов

5.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

5.2.1.1. Заявитель обращается с заявлением на создание квалифицированного СКПЭП в УЦ (Приложение № 1). В УЦ принимаются представленные Заявителем документы, вручаются готовые СКПЭП от имени УЦ. Заявитель может заранее предоставить в УЦ электронные копии документов при условии последующего их сличения с оригиналами.

5.2.1.2. УЦ в СКПЭП вносится информация на основании заявления на создание квалифицированного СКПЭП (Приложение № 1).

5.2.1.3. УЦ проверяет данные в заявлении на изготовление СКПЭП на соответствие данным, содержащимся в иных представленных Заявителем документах, и устанавливает:

1) факт принадлежности документов предоставившему их лицу;

2) факт соответствия сведений, указанных в заявлении, представленным

документам и, в необходимых случаях в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», информации, полученной с использованием инфраструктуры;

3) факт отсутствия явных признаков подделки документов.

5.2.1.4. При внесении в Сертификат персональных данных физического лица, Заявитель - физическое лицо предоставляет свое согласие на обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Текст согласия включен в заявление на создание квалифицированного СКПЭП (Приложение № 1). Согласие должно быть подписано лицом, данные о котором вносятся в Сертификат (субъектом персональных данных).

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 ЭП, либо посредством простой электронной подписи заявителя - физического лица, ключ которой получен им при личном обращении в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, устанавливаемыми Правительством Российской Федерации, при условии идентификации гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из федеральной государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) и информации из государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (ЕБС);

Форма заявления на создание квалифицированного СКПЭП (Приложение № 1) предоставляется Заявителю в электронном виде. Актуальную форму заявления УЦ определяет самостоятельно и по своей инициативе вправе вносить в нее любые изменения без уведомления участников электронного взаимодействия.

Заявление на создание квалифицированного сертификата в бумажной форме оформляется в соответствии с формой, утвержденной Приложением № 1 настоящего Порядка. Заявление на создание 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.

Форма заявления на создание квалифицированного СКПЭП включает следующие сведения для Владельца сертификата - физического лица:

1) ФИО;

2) паспортные данные - серия, номер паспорта, дата выдачи, код подразделения, дата и место рождения;

3) СНИЛС;

4) ИНН;

5) адрес электронной почты;

6) область, город/населенный пункт;

7) телефон для информирования.

5.2.3. Порядок идентификации заявителя

5.2.3.1. 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;
- путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (Собрание законодательства Российской Федерации, 2023, N 1, ст. 19). При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия отказывается от использования шифровальных (криптографических) средств, указанных в статье 19 Федерального закона от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации», удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

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

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

5.2.3.4. При идентификации заявителя 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.

5.2.3.5. Подтверждение достоверности сведений, перечисленных в п. 1 и 2 ч. 1 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» осуществляется одним из следующих способов:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Фонда пенсионного и социального страхования Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием ЕСИА.

5.2.3.6. Заявитель при обращении в УЦ (Центр регистрации) предоставляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) основной документ, удостоверяющий личность;

2) страховой номер индивидуального лицевого счета заявителя - физического лица;

3) идентификационный номер налогоплательщика заявителя - физического лица.

5.2.3.7. Личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность - паспорту гражданина Российской Федерации.

5.2.3.8. Личность гражданина иностранного государства и лица без гражданства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства и лица без гражданства.

Документы, удостоверяющие личность иностранных граждан на территории РФ:

а. паспорт иностранного гражданина или иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина – для иностранных граждан, если они постоянно проживают на территории РФ;

б. документ, выданный иностранным государством и признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность лица без гражданства;

в. временное удостоверение личности лица без гражданства в РФ;

г. иной документ, установленный федеральным законом или признаваемый в соответствии с международным договором РФ в качестве документа, удостоверяющего личность иностранного гражданина или лица без гражданства;

д. разрешение на временное проживание является документом, удостоверяющим личность иностранного гражданина или лица без гражданства (оформленное в виде документа установленной формы, выдаваемого в РФ лицу без гражданства, не имеющему документа, удостоверяющего личность). Данный документ подтверждает право иностранного гражданина или лица без гражданства временно проживать в Российской Федерации до получения вида на жительство;

е. вид на жительство в РФ является документом, удостоверяющим личность лица без гражданства, подтверждающим его право на постоянное проживание в РФ;

ж. удостоверение беженца или свидетельство о рассмотрении ходатайства о признании беженцем на территории РФ является документом, удостоверяющим личность лица (иностранного гражданина или лица без гражданства), ходатайствующего о признании беженцем (статьи 4, 7 Федерального закона от 19.02.1993 № 4528-1 «О беженцах»).

Все документы на иностранном языке должны быть апостилированы в консульстве (посольстве) РФ за границей (на территории того государства, где эти документы выданы), либо в консульстве (посольстве) иностранного государства (выдавшего документы, удостоверяющие личность) на территории РФ и иметь заверенный перевод на русский язык.

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

5.2.3.10.При получении ЭП Заявитель должен предоставить оригинал документа, удостоверяющего личность.

5.2.3.11.Требования к документу, удостоверяющему личность:

1) документ не должен быть просрочен;
2) документ не должен быть поврежден или испорчен;
3) документ не может содержать неточности и орфографические ошибки.

При выдаче СКПЭП Заявителю – физическому лицу УЦ берет согласие с Заявителя на обработку его персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

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

Перечень документов и сведений, запрашиваемых УЦ 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».

УЦ выполняет свою обязанность по внесению в квалифицированный сертификат только достоверной информации путем подтверждения информации посредством предоставления документов и сведений в УЦ 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 для получения квалифицированного сертификата заявитель предоставляет следующие документы либо их надлежащим образом заверенные копии и (или) сведения из них:

1) заявление на создание квалифицированного СКПЭП, содержащее в том числе фамилию, имя отчество (если имеется) владельца сертификата (Приложение № 1);

2) основной документ, удостоверяющий личность;

3) страховой номер индивидуального лицевого счета заявителя – физического лица;

4) идентификационный номер налогоплательщика заявителя – физического лица.

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

Заявитель представляет в УЦ документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности Уполномоченного представителя Заявителя, Заявителя-физического лица, а также документы, на основании которых УЦ вносятся сведения в Сертификат, такие как: идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета, наименование должности и иные данные.

5.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

5.2.5.1. Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УЦ осуществляет с использованием инфраструктуры проверку достоверности документов и сведений, представленных Заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

5.2.5.2. В случае, если УЦ идентифицировал Заявителя - физическое лицо, УЦ осуществляет процедуру создания и выдачи Заявителю квалифицированного сертификата.

В ином случае УЦ отказывает заявителю в выдаче квалифицированного сертификата, в том числе, в случаях, установленных пунктами 5 и 6 части 2 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

- не было подтверждено то, что заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному заявителем для получения СКПЭП;

- 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

5.2.6.1. Регистрация Заявителя и изготовление сертификата

Под регистрацией Заявителей понимается внесение регистрационной информации о Заявителях в Реестр УЦ.

Процедура регистрации Заявителя применяется в отношении физических лиц, обращающихся к услугам УЦ в части изготовления СКПЭП Заявителей и/или формирования ключей ЭП и ключей проверки ЭП Заявителей с записью их на ключевой носитель.

5.2.6.2. Процедура создания ключей ЭП и выпуска СКПЭП:

1) Процедура создания ключей ЭП и выпуска СКПЭП в УЦ:

а. получение от Заявителя сертификата заявления на создание квалифицированного СКПЭП (Приложение № 1);

б. проверка сведений, указанных в заявлении на создание квалифицированного СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений проводится проверка будущего носителя ключа, допустимого эксплуатационной документацией к СКЗИ, на вирусы, при необходимости производится инициализация и создание ключа ЭП;

г. формирование запроса на СКПЭП;

д. предоставление запроса на сертификат в УЦ для выпуска СКПЭП;

е. проверка сведений в запросе;

ж. выпуск СКПЭП в УЦ;

з. размещение сертификата на носителе ключа;

и. внесение данных о выпущенных СКПЭП и ключевых носителях в журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

к. осуществление конвертования носителя с ключевой парой;

л. передача Владельцу сертификата носителя ключа с ключевой парой под подпись в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

м. ознакомление Владельца сертификата со сведениями, содержащимися в сертификате.

2) Процедура создания ключей ЭП Заявителем самостоятельно:

а. получение от Заявителя сертификата заявления на создание квалифицированного СКПЭП (Приложение № 1);

б. проверка сведений, указанных в заявлении на создание квалифицированного СКПЭП и представленных документов;

в. в случае подтверждения достоверности сведений Владельцу сертификата рекомендуется приступить к созданию ключа ЭП и запроса на сертификат на его персональном компьютере с использованием сертифицированных ФСБ России СКЗИ;

г. предоставление запроса на сертификат в УЦ для выпуска СКПЭП;

д. проверка сведений в запросе;

е. выпуск СКПЭП в УЦ;

ж. ознакомление Владельца сертификата со сведениями, содержащимися в СКПЭП;

з. передача Владельцу сертификата;

и. размещение сертификата Владельцем сертификата на носитель.

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

5.2.7. Порядок выдачи и вручения квалифицированного сертификата

5.2.7.1. При личной идентификации Владельца квалифицированного сертификата:

1) Работник УЦ приглашает Владельца сертификата для вручения СКПЭП в офис УЦ.

2) Работник УЦ выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по основному документу, удостоверяющему личность, и проверку подлинности представленных документов.

3) Документы на электронных и бумажных носителях выдаются Заявителю с соблюдением требований по обеспечению конфиденциальности.

4) При получении квалифицированного сертификата Заявитель знакомится 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. Заявителю выдается лист ознакомления с данными СКПЭП (Приложение № 6) в 2 экземплярах, на котором он ставит свою подпись, а работник УЦ собственноручной подписью подтверждает факт ознакомления Заявителя с информацией, содержащейся в сертификате. Один экземпляр листа ознакомления

передается Заявителю, второй экземпляр передается в УЦ.

5) По запросу Владельца сертификата УЦ может выдать бланк сертификата на бумажном носителе, подписанный Уполномоченным лицом УЦ.

6) УЦ одновременно с выдачей СКПЭП предоставляет руководство по обеспечению безопасности использования КЭП и средств КЭП, об условиях и о порядке использования ЭП и средств ЭП (СКЗИ), о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП - Правила использования СКЗИ и ЭП (Приложение № 5).

7) При выдаче квалифицированного сертификата Заявитель получает:

- ключ ЭП и СКПЭП;
- лист ознакомления (Приложение № 6), подписанный собственноручной подписью Владельца сертификата и собственноручной подписью работника УЦ.

5.2.7.2. При идентификации Владельца квалифицированного сертификата без его личного присутствия с использованием квалифицированной ЭП Владельца сертификата при наличии действующего квалифицированного сертификата, ранее выданного УЦ:

1) Формирование ключа ЭП и СКПЭП Владельца сертификата осуществляется на основании Заявления на изготовление квалифицированного СКПЭП, запроса на сертификат, подписанных усиленной КЭП с использованием ключа ЭП и СКПЭП владельца сертификата, либо подписанных ПЭП ЕСИА. Для подписания заявления на изготовление СКПЭП и запроса на сертификат должен использоваться СКПЭП ранее выданный УЦ, срок действия которого не истек на момент подписания.

2) УЦ с использованием инфраструктуры осуществляет проверку достоверности сведений, представленных Заявителем в соответствии с частями 2 и 2.1 ст. 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3) При получении положительных результатов проверки данных в запросе на сертификат УЦ выпускает новый СКПЭП, направляет лист ознакомления по защищенным каналам связи.

4) Заявитель проверяет данные в выпущенном сертификате, если все данные внесены верно, то подписывает лист ознакомления (Приложение № 6) с информацией, содержащейся в квалифицированном СКПЭП действующей на момент подписания усиленной квалифицированной ЭП, ранее выданной УЦ, с использованием ключа ЭП и СКПЭП, владельцем которых является Заявитель, и направляет подписанный документ в УЦ, тем самым подтверждая свое согласие с данными, внесенными в сертификат, и обеспечивая неотрекаемость от сертификата.

5) УЦ направляет Заявителю СКПЭП.

6) По запросу Владельца сертификата УЦ может выдать бланк сертификата на бумажном носителе, подписанный Уполномоченным лицом УЦ.

7) При выдаче квалифицированного сертификата Заявитель получает:

- ключ ЭП и СКПЭП.

5.2.8. Срок создания и выдачи квалифицированного сертификата с момента получения УЦ 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 с момента подачи Заявления на выдачу квалифицированного СКПЭП 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 УЦ 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 Приложения № 2 настоящего Порядка, и подписанного заявителем.

Заявление может быть подано как в форме бумажного документа, подписанного собственноручной подписью заявителя – физического 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:

- СКПЭП, 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 ЭП в электронном документе составляет 30 (тридцать) рабочих дней с даты получения УЦ Заявления на подтверждение действительности электронной подписи, использованной для подписания электронных документов.

5.3.3. Порядок оказания услуги

Процедура подтверждения действительности ЭП в электронном документе осуществляется с использованием специализированного программного обеспечения, входящего в состав сертифицированного средства УЦ.

Оказание услуги по подтверждению подлинности электронной подписи в электронном документе осуществляет комиссия, сформированная из числа сотрудников УЦ. По согласованию сторон в комиссию могут входить представители Заявителя или Уполномоченные сотрудники правоохранительных органов.

В ходе процедуры подтверждения действительности ЭП комиссией осуществляется проверка всех квалифицированных СКПЭП, на основании которых были сформированы ЭП на документах, определение даты формирования каждой ЭП в документах, проверку каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП 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 УЦ.

Заключение содержит:

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

Отчет по выполненной проверке содержит:

- время и место проведения проверки;
- содержание проверки;
- результат проверки квалифицированного СКПЭП или нескольких квалифицированных СКПЭП, необходимых для проверки ЭП;
- результат проверки ЭП электронного документа с использованием одного или нескольких квалифицированных СКПЭП;
- результат проверки действительности каждого квалифицированного СКПЭП в цепочке до квалифицированного СКПЭП Головного УЦ.

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

При проведении работ УЦ может быть запрошена дополнительная информация.

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

5.4.1. Основания прекращения действия квалифицированного сертификата

СКПЭП прекращает свое действие в случаях, установленных статьей 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

1) в связи с истечением установленного срока его действия;

2) на основании заявления о прекращении действия СКПЭП владельца СКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа (Приложение № 3) при:

- смене реквизитов Владельца сертификата;
- поломке ключевого носителя;
- утере, краже и иной компрометации ключа;
- ошибке в реквизитах;
- иных случаях.

3) в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;

4) 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 УЦ и владельцем СКПЭП.

5.4.2. УЦ аннулирует СКПЭП в следующих случаях:

1) не подтверждено, что владелец СКПЭП владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в таком сертификате;

2) установлено, что содержащийся в таком СКПЭП ключ проверки ЭП уже содержится в ином ранее созданном СКПЭП;

3) вступило в силу решение суда, которым, в частности, установлено, что СКПЭП содержит недостоверную информацию.

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

Заявление на прекращение действия СКПЭП (Приложение № 3) может подаваться в УЦ в бумажной форме при личном прибытии Владельца сертификата в УЦ либо почтовой или курьерской службой, форме электронного документа, подписанного усиленной КЭП Владельца сертификата, в том числе с использованием сервиса приёма заявлений о прекращении действия квалифицированного СКПЭП, поданного Владельцем посредством Единого портала государственных и муниципальных услуг (далее – ЕПГУ).

В случае направления Владельцем сертификата заявления о прекращении действия квалифицированного СКПЭП с использованием ЕПГУ, принятое по такому заявлению решение УЦ в форме электронного документа, подписанного КЭП УЦ, размещается в личном кабинете Заявителя на ЕПГУ после проведения проверки действительности КЭП УЦ, которой такое решение подписано, и подтверждения ее действительности. В случае принятия по такому заявлению решения о прекращении действия квалифицированного СКПЭП УЦ, после внесения соответствующей информации в Реестр квалифицированных СКПЭП, направляет на ЕПГУ информацию о прекращении действия квалифицированного СКПЭП. Взаимодействие УЦ с ЕПГУ в рамках реализации указанных норм, осуществляется посредством СМЭВ. В случае направления заявления о

прекращении действия квалифицированного СКПЭП с использованием ЕПГУ оно должно содержать: серийный номер квалифицированного СКПЭП, даты начала и окончания действия квалифицированного СКПЭП, наименование УЦ, причины прекращения действия квалифицированного СКПЭП, а также фамилию, имя, отчество (при наличии), страхового номера индивидуального лицевого счета, идентификационного номера налогоплательщика Владельца сертификата.

Подтверждение полномочий Владельца сертификата осуществляется на основании предоставляемых Заявителем документов, а также с использованием инфраструктуры.

Заявление на прекращение квалифицированного СКПЭП должно содержать:

- серийный номер квалифицированного СКПЭП,
- фамилию, имя, отчество (если имеется) владельца квалифицированного сертификата - для физического лица,
- страховой номер индивидуального лицевого счета;
- идентификационный номер налогоплательщика владельца квалифицированного сертификата - для физического лица.

По волеизъявлению обратившегося лица, в заявлении могут быть указаны иные сведения, относящиеся к СКПЭП.

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

Информация о прекращении действия или аннулировании СКПЭП должна быть внесена УЦ 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 УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие СКПЭП прекращается с момента внесения записи об этом в Реестр сертификатов.

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

Информация о размещении списка отозванных сертификатов заносится в изданные УЦ СКПЭП в расширение CRL Distribution Point сертификата ключа подписи.

В случае прекращения действия СКПЭП Пользователя УЦ по истечении срока его действия временем прекращения действия сертификата ключа подписи Пользователя УЦ признается время, хранящееся в поле notAfter поля Validity СКПЭП. В данном случае информация об этом СКПЭП Пользователя УЦ в список отозванных сертификатов не заносится.

В случае компрометации ключа электронной подписи Уполномоченного лица УЦ временем прекращения действия СКПЭП Пользователя УЦ признается время компрометации ключа ЭП УЦ, фиксирующееся в реестре УЦ. В случае компрометации ключа ЭП УЦ информация о СКПЭП Пользователя УЦ в список отозванных сертификатов не заносится.

5.5. Порядок ведения реестра квалифицированных сертификатов

5.5.1. Формы ведения реестра квалифицированных сертификатов

5.5.1.1. Реестр квалифицированных сертификатов ведется в электронной форме. Формирование Реестра квалифицированных сертификатов включает в себя внесение СКПЭП 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.

5.5.1.2. Информация, внесенная в Реестр квалифицированных сертификатов, подлежит хранению в течение всего срока деятельности аккредитованного УЦ, если более короткий срок не установлен законодательством Российской Федерации.

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

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

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

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

5.5.1.7. 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 или аннулировании квалифицированного сертификата вносятся аккредитованным УЦ 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 УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи в Реестр квалифицированных сертификатов.

До внесения в Реестр квалифицированных сертификатов сведений об аннулировании квалифицированного сертификата аккредитованный УЦ 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. Сроки проведения технического обслуживания

Плановое техническое обслуживание Реестра сертификатов осуществляется не чаще одного раза в месяц и не может превышать 12 (двенадцати) часов.

Внеплановое техническое обслуживание Реестра сертификатов осуществляется в случае необходимости и невозможности дождаться срока наступления планового обслуживания, не может превышать 12 (двенадцати) часов.

5.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

УЦ уведомляет лиц, использующих реестр квалифицированных сертификатов, о проведении планового или внепланового технического обслуживания реестра квалифицированных сертификатов путем размещения информации на официальном сайте УЦ 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

УЦ одновременно с выдачей квалифицированного сертификата предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности использования КЭП и средств КЭП - Правила использования СКЗИ и ЭП (Приложение № 5).

6.2. Выдача по обращению заявителя средств электронной подписи

6.2.1. УЦ по обращению Заявителя выдает средства ЭП, отвечающие требованиям:

1) средства ЭП позволяют установить факт изменения подписанного электронного документа после момента его подписания;

2) средства ЭП обеспечивают практическую невозможность вычисления ключа ЭП из ЭП или из ключа ее проверки;

3) средства ЭП позволяют создать ЭП в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами ЭП.

6.2.2. При создании ЭП средства ЭП должны (не относится к средствам ЭП, используемым для автоматического создания ЭП):

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

2) создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;

3) однозначно показывать, что ЭП создана.

6.2.3. При проверке ЭП средства ЭП должны (не относится к средствам ЭП, используемым для автоматической проверки ЭП):

1) показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного ЭП, включая визуализацию данной ЭП, содержащую информацию о том, что такой документ подписан ЭП, а также о номере, Владельце сертификата и периоде действия СКПЭП;

2) показывать информацию о внесении изменений в подписанный ЭП электронный документ;

3) указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

6.2.4. Средства ЭП, предназначенные для создания ЭП в электронных документах, содержащих информацию ограниченного доступа (в том числе персональные данные), не должны нарушать конфиденциальность такой информации.

6.2.5. Средство ЭП должно противостоять угрозам, представляющим собой целенаправленные действия с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемой средством ЭП информации или с целью создания условий для этого.

6.2.6. Средство ЭП должно проводить аутентификацию субъектов доступа (лиц, процессов) к этому средству, при этом:

1) при осуществлении доступа к средству ЭП аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства ЭП;

2) механизмы аутентификации должны блокировать доступ этих субъектов

к функциям средства ЭП при отрицательном результате аутентификации.

6.2.7. Средство ЭП должно проводить аутентификацию лиц, осуществляющих локальный доступ к средству ЭП.

6.2.8. Средства ЭП должны обеспечивать возможность проверки всех усиленных КЭП в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной КЭП, или в случае, если электронный документ подписан несколькими усиленными КЭП.

6.2.9. Средства ЭП аккредитованного УЦ и средства ЭП Заявителя/Владельца ЭП должны соответствовать требованиям Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и требованиям Приказа ФСБ РФ от 27.12.2011 г. № 796.

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

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

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

Аккредитованный УЦ 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 УЦ 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

6.5.1. Требования к обеспечению конфиденциальности.

Ключ ЭП является конфиденциальной информацией владельца квалифицированного сертификата. Владелец квалифицированного сертификата должен обеспечивать конфиденциальность ключа ЭП, в частности не допускать использование ключа ЭП без его согласия. Необходимо немедленно обратиться в УЦ с заявлением на прекращение действия квалифицированного СКПЭП (Приложение № 3) в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа ЭП.

Запрещается:

1) оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, средства усиленной КЭП, после ввода ключевой информации;
2) вносить какие-либо изменения в ПО СКЗИ;
3) осуществлять несанкционированное копирование ключевых носителей;
4) разглашать содержимое носителей ключевой информации или

передавать сами носители лицам, к ним не допущенным;

5) использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

6) записывать на ключевые носители постороннюю информацию;

7) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ;

8) защищать ключи ЭП на ключевом носителе паролем (PIN-кодом);

9) оставлять без присмотра ключи ЭП на ключевом носителе (на столе, подключенным к ПЭВМ и пр.);

10) применять ключ КЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

6.5.2. Условия временного хранения ключей ЭП.

1) при хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец сертификата несет персональную ответственность за хранение личных ключевых носителей;

2) запрещается оставлять без контроля вычислительные средства с установленным СКЗИ после ввода ключевой информации;

3) в случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности (если он имеется) несет персональную ответственность за хранение личных ключевых носителей пользователей.

6.5.3. Сроки уничтожения ключей ЭП.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты и т.п.), в том числе срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения Владелец сертификата устанавливает самостоятельно.

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

При выдаче квалифицированного сертификата аккредитованный УЦ направляет в ЕСИА сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного УЦ).

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 УЦ по желанию владельца квалифицированного сертификата безвозмездно осуществляет

его регистрацию в ЕСИА с проведением идентификации владельца при его личном присутствии. Регистрация осуществляется на основании Заявления на регистрацию в ЕСИА, составленному по форме Приложения № 4 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 УЦ в рабочее время УЦ, либо почтовой или курьерской службой, или круглосуточно через форму на сайте УЦ http://cert.pkitrans.ru/ (по выбору лица, обратившегося за получением информации из Реестра квалифицированных сертификатов), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов Информация предоставляется в форме выписки из реестра квалифицированных сертификатов и направляется обратившемуся лицу, как почтовым отправлением, так и с использованием информационно-телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из Реестра квалифицированных сертификатов).

Выписка из Реестра позволяет определить действительность СКПЭП Владельцев сертификатов. Доступ к информации организован в соответствии с защитой персональных данных согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и предоставляется при условии владения необходимыми данными из сертификата.

Для получения информации необходимо предоставить (по форме Приложения № 7):

- серийный номер сертификата;
- ИНН Заявителя;
- СНИЛС Владельца сертификата;
- даты начала и окончания действия квалифицированного сертификата.

Также УЦ публикует перечень прекративших свое действие (аннулированных) квалифицированных сертификатов, позволяющий определить действительность СКПЭП Владельцев сертификатов на официальном сайте http://pkitrans.ru.

Срок предоставления информации не превышает семи дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно- телекоммуникационных сетей.

7. Персональные данные

7.1. Обработка персональных данных Заявителей/Владельцев сертификатов:

7.1.1. Цель обработки персональных данных в УЦ – исполнение требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»; изготовление и хранение СКПЭП, изготовление списков аннулированных сертификатов, ведение Реестра выданных и аннулированных сертификатов, подтверждение неотрекаемости от подачи заявления и запроса на сертификат, от получения СКПЭП, установление личности Заявителя - физического лица, обратившегося за получением СКПЭП и подтверждения правомочия обращаться за получением СКПЭП.

7.1.2. Обработка персональных данных в УЦ осуществляется на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.3. Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, реквизиты основного документа, удостоверяющего личность (серия, номер, код подразделения, дата выдачи), СНИЛС, которому выдан СКПЭП, номер телефона, адрес электронной почты и иные сведения, необходимые для исполнения целей Порядка.

7.1.4. УЦ осуществляет действия по сбору, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, использованию, блокированию, уничтожению, передаче персональных данных Заявителя в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

7.1.5. УЦ не раскрывает третьим лицам и не распространяет персональные данные Заявителя без наличия его письменного согласия на раскрытие данной информации, за исключением случаев, прямо установленных действующим законодательством Российской Федерации.

7.1.6. Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации, установленного ч. 2 ст.15 Федерального закона от 04.06.2011 № 63-ФЗ «Об электронной подписи».

7.2. Архивное хранение информации и сведений УЦ

На основании Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ч. 1 ст. 15) Аккредитованный УЦ хранит следующую информацию: реквизиты основного документа, удостоверяющего личность Владельца сертификата - физического лица, СНИЛС, ИНН.

Хранение информации осуществляется в соответствии с ч.1 ст. 15, ч. 7 статьи 13 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

7.2.1. Документы УЦ, подлежащие архивному хранению, являются документами временного хранения, архив ведется в электронном виде.

7.2.2. Архивному хранению подлежат следующие документы и (или) сведения:

1) заявление на создание квалифицированного СКПЭП (Приложение № 1);

2) реквизиты основного документа, удостоверяющего личность Владельца сертификата – физического лица;

3) реквизиты СНИЛС;

4) ИНН;
5) СКПЭП;
6) лист ознакомления с данными СКПЭП (Приложение № 6).

8. Сроки действия ключей и сертификатов

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

8.1.1. Срок действия Ключей ЭП составляет 1 год и 3 месяца.

8.1.2. В соответствии с требованиями Приказа ФСБ России № 796 от 27 декабря 2011 года о том, что срок действия Ключа проверки ЭП не должен превышать срок действия соответствующего Ключа ЭП более чем на 15 лет, срок действия Сертификата Пользователя УЦ – не менее 12 лет, максимально допустимый срок действия Сертификата Пользователя УЦ – 15 лет.

8.1.3. Начало действия Ключа электронной подписи Пользователя УЦ исчисляется с даты и времени генерации запроса на Сертификат Пользователя УЦ.

8.1.4. Срок действия Сертификата Пользователя УЦ устанавливается УЦ в момент его изготовления и составляет не менее 12 лет и не более 15 лет

9. Ответственность

9.1. Стороны несут ответственность за соблюдение положений настоящего Порядка в соответствии с действующим законодательством РФ.

9.2. Владелец сертификата несет ответственность за достоверность документов и сведений, предоставляемых в УЦ, неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», настоящим Порядком.

9.3. УЦ в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

1) неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг УЦ;

2) неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом № 63-ФЗ «Об электронной подписи».

9.4. УЦ (работник УЦ) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Порядком.

10. Список приложений

10.1. Приложение 1. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи

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

Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

Я,

_____

фамилия, имя, отчество

заявляю об акцепте действующего на дату регистрации Заявления «Порядка реализации функций Аккредитованного Удостоверяющего Центра АО «НИИАС» и исполнения его обязанностей», в порядке, предусмотренном ст. 428 ГражданскогоКодекса Российской Федерации и прошу создать квалифицированный сертификат ключа проверки электронной подписи (далее квалифицированный сертификат) в соответствии со следующими данными:

Сведения о физическом лице – Пользователе Аккредитованного удостоверяющего центра	
Фамилия	
Имя	
Отчество	
Пол	
Дата рождения	
СНИЛС	
ИНН	
Гражданство	
Документ, удостоверяющий личность	*Тип документа:*_____ *серия__номер__дата выдачи*_____ *выдан*_____ _____ *код подразделения (при наличии)* -
Город	
Субъект РФ	
Страна	*RU*
Контактный телефон	
Адрес электронной почты	

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, абонентский номер, 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».

« » 20 г.

_____

подпись М.П.

Приложение № 2
к Порядку реализации
функцийАккредитованного
удостоверяющего центра
АО «НИИАС» и исполнения
его обязанностей

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

Заявление
на подтверждение действительности электронной подписи, использованной дляподписания электронных документов

Я,_____

(фамилия,имя,отчество)

прошу подтвердить подлинность электронной подписи в электронном документе наосновании 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 подписи

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

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

«_____:_____» «_____/_____/_____»;

Час минута день месяц год

«_____» _____ 20 года _____
_____

подпись Ф.И.О.

Приложение № 3
к Порядку реализации
функций Аккредитованного
удостоверяющего центра
АО «НИИАС» и исполнения
его обязанностей

Форма заявления на прекращение действия сертификата ключа проверки электронной подписи

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	
ИНН	

_____ _____

подпись Ф.И.О. Заявителя

«_____»_____ 20 года

Приложение № 4
к Порядку реализации
функцийАккредитованного
удостоверяющего центра
АО «НИИАС» и исполнения
его обязанностей

Форма Заявления на регистрацию в Единой системе идентификации иаутентификации

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 всоответствии 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

Приложение № 5
к Порядку реализации
функций Аккредитованного
удостоверяющего центра
АО «НИИАС» и исполнения
его обязанностей

Правила использования средств криптографической защиты информации и электронной подписи

1. Средства электронной подписи - шифровальные (криптографические) средства (СКЗИ), используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» СКЗИ и средства ЭП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Ключ электронной подписи (ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

3. Пользователи СКЗИ несут персональную ответственность за:

а. сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

б. сохранение в тайне содержания ключей ЭП и СКЗИ;

в. сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

4. Юридическим лицом, ИП, владельцем сертификата должны быть обеспечены условия хранения ключевых носителей ключей ЭП, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

5. Владелец сертификата несет ответственность за то, чтобы на компьютере, на котором установлены СКЗИ, не были установлены и не эксплуатировались программы (в том числе, - вирусы), которые могут нарушить функционирование программных СКЗИ. При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

6. Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 г.

№ 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Неиспользованные или выведенные из действия ключевые документы подлежат уничтожению обладателем конфиденциальной информацией на месте, путем переформатирования ключевых носителей средствами ПО СКЗИ. Ключи квалифицированных электронных подписей по истечении сроков действия данных ключей подлежат незамедлительному уничтожению. Для уничтожения ключей электронных подписей должны применяться прошедшие в установленном порядке процедуру оценки соответствия средства электронной подписи, в составе которых реализована функция уничтожения информации.

7. Не допускается:

а. разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б. вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;

в. записывать на ключевом носителе постороннюю информацию;

г. вносить какие-либо изменения в СКЗИ и ключ ЭП;

д. использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей);

е. оставлять без контроля аппаратные средства, на которых эксплуатируются средства электронной подписи;

ж. оставлять без контроля носители ключевой информации;

з. сообщать PIN – код к ключевому носителю кому бы то ни было.

8. Действия в случае компрометации ключей:

а. Под компрометацией ключей ЭП понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых ключи ЭП могут стать доступными несанкционированным лицам и (или) процессам;

б. Владелец сертификата (уполномоченное лицо) самостоятельно должен определить факт компрометации ключа ЭП и оценить значение этого события для Владельца сертификата. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Владелец сертификата;

в. При компрометации ключа ЭП, Владелец сертификата должен немедленно поставить в известность представителей Удостоверяющего центра о факте компрометации. Заявление на аннулирование сертификата может подаваться в УЦ в бумажной форме при личном прибытии Заявителя в офис удостоверяющего центра, либо почтовой или курьерской доставкой, а также в электронной форме через личный кабинет, с подписью лица, имеющего право действовать от имени организации без доверенности. Не позднее 1 часа после поступления заявления на аннулирование ключа ЭП, сертификат проверки ключа ЭП будет аннулирован. Последующая разблокировка аннулированного сертификата ключа проверки ЭП невозможна.

Для получения новых ключей уполномоченный представитель Заявителя, у которого были скомпрометированы ключи, должен обратиться в УЦ, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.

9. PIN-код Владельца сертификата на носителе

Владелец сертификата обязан изменить PIN-код при первом использовании ключевого носителя. Надежный PIN-код должен состоять из смешанного набора цифровых и буквенных символов.

10. Рекомендации по использованию ключа:

1) Владелец ключевого носителя несет личную ответственность за сохранность ключа подписи находящегося на его носителе. В случае утери ключевого носителя, необходимо незамедлительно сообщить в техническую поддержку УЦ АО «НИИАС» для блокировки сертификата и предотвращение компрометации ключа подписи.

2) Держать ключевой носитель вставленным в USB-разъем компьютера только во время работы с информационными системами АО «НИИАС» (ИС НИИАС) (от момента регистрации, ввод логина/пароля до момента выхода из системы).

3) НЕ отсоединять ключевой носитель от USB-порта, когда к нему идет обращение (мигает световой диод) - может привести к физическому выходу из строя ключевого носителя JaCarta.

4) В окне «Криптопро CSP: введите pin-код для контейнера» **НЕ РЕКОМЕНДУЕТСЯ** отмечать поле «Запомнить pin-код».

5) **ЗАПРЕЩАЕТСЯ** оказывать какое-либо воздействие (механическое, химическое, температурное) на ключевой носитель, в результате которого может произойти выход ключевого носителя из строя.

6) **ВНИМАНИЕ:** Использование ключевого носителя рекомендуется **только во время работы в информационных системах**. После окончания работы в указанных системах следует **прекратить** использование ключевого носителя и **извлечь** устройство из USB-разъема компьютера. Оставление устройства в USB-разъеме может вызвать блокировку ключевого носителя. **Не форматируйте** (не инициализируйте) ключевой носитель и **не удаляйте** контейнеры с ключевого

носителя без прямого указания сотрудников технической поддержки УЦ АО «НИИАС».

7) Количество попыток ввода неправильного pin-кода ограничено – не более 10 раз для ключевого носителя JaCarta.

8) По вопросам, связанным с настройкой ПО и использованием ключевого носителя, обращаться по телефону: 8(499)262-55-29.

11. Порядок установки и эксплуатации СКЗИ допускается в четком соответствии с документацией на используемое СКЗИ: https://www.cryptopro.ru/.

12. В случае отсутствия у пользователя СКЗИ установочного модуля СКЗИ «КриптоПро CSP», последний может быть получен одним из ниже перечисленных способов:

1) Дистрибутив на носителе (за дополнительную плату).

2) Посредством загрузки через Интернет.

На странице загрузки вместе с дистрибутивом и документацией размещается отделенная электронная подпись, для проверки которой необходимо использовать утилиту «cpverify», полученную доверенным образом и содержащую ключ проверки данной электронной подписи. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru.

13. Пользователи допускаются к работе с СКЗИ после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники органа криптографической защиты – Лицензиата ФСБ (в соответствии с тарифами) или обладателя конфиденциальной информации.

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

Форма ознакомления с содержимым сертификата ключа проверки электронной подписи

Удостоверяющий Центр АО «НИИАС»

Сертификат ключа проверки электронной подписи

Сведения о сертификате:

Версия: 3

Серийный номер:

Издатель сертификата:

Владелец сертификата:

Срок действия:

Действителен с:

Действителен по:

Ключ проверки электронной подписи:

Алгоритм:

Параметры:

Значение:

Расширения сертификата X.509

Расширение: Использование ключа (критичное)

Идентификатор:

Значение:

Расширение: Улучшенный ключ

Идентификатор:

Значение:

Расширение:

Идентификатор:

Значение:

Расширение: Идентификатор ключа центра сертификатов

Идентификатор:

Значение:

Расширение: Идентификатор ключа субъекта

Идентификатор:

Значение:

Расширение: Политики применения

Идентификатор:

Значение:

Расширение: Политики сертификата

Идентификатор:

Значение:

Расширение: Сведения о шаблоне сертификата

Идентификатор:

Значение:

Расширение: Средства электронной подписи и УЦ издателя

Идентификатор:

Значение:

Расширение: Средство электронной подписи владельца

Идентификатор:

Значение:

Расширение: Точки распространения списков отзыва (CRL)

Идентификатор:

Значение:

Расширение: Доступ к информации о центрах сертификации

Идентификатор:

Значение:

Расширение: Период использования ключа электронной подписи

Идентификатор:

Значение:

Подпись Удостоверяющего центра:

Алгоритм подписи:

Параметры:

Значение:

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

М. П.

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

Форма Выписки из Реестра СКПЭП Владельцев сертификатов

Выписка из Реестра СКПЭП Владельцев сертификатов

Я, _____
фамилия, имя, отчество

паспорт серии _____ № _____ выдан «____» _____ года
_____
наименование органа, выдавшего документ

код подразделения _____,
прошу предоставить выписку из Реестра СКПЭП Владельцев сертификатов, содержащего следующие данные сертификата:

Серийный номер сертификата	
Фамилия, имя, отчество	
СНИЛС Владельца сертификата	
ИНН Владельца сертификата	
Даты начала и окончания действия квалифицированного сертификата	

_____ _____
подпись Ф.И.О. Владельца

«_____» _____ 20__г.