УТВЕРЖДАЮ
Руководитель
Удостоверяющего центра АО «Тандер»
_____ Шевцова Е.Б.
«01» июля 2026 г.

ПОРЯДОК (РЕГЛАМЕНТ) РЕАЛИЗАЦИИ ФУНКЦИЙ АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА АО «ТАНДЕР» И ИСПОЛНЕНИЯ ЕГО ОБЯЗАННОСТЕЙ

Краснодар 2026

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Электронная подпись (далее – 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.

Квалифицированный сертификат ключа проверки электронной подписи (далее – КСКПЭП, квалифицированный сертификат) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи» (далее - Федеральным законом «Об электронной подписи») и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным Удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее -уполномоченный федеральный орган), и являющийся в связи с этим официальным документом.

Заявитель – физическое лицо, обратившееся в Удостоверяющий центр для получения КСКПЭП и присоединившееся к порядку реализации функций аккредитованного Удостоверяющего центра АО «Тандер».

Владелец КСКПЭП – физическое лицо, которому в установленном настоящим Регламентом порядке выдан КСКПЭП, в соответствии с Федеральным законом № 63-ФЗ.

Оператор Удостоверяющего центра – физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по осуществлению действий по регистрации Заявителей, управлению и выпуску КСКПЭП, включая заверение копий документов, принятых от Заявителей, собственноручной подписью.

Удостоверяющий центр (далее - УЦ) – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции 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».

Ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП.

Сертификат ключа проверки ЭП – электронный документ или документ на бумажном носителе, выданный УЦ и подтверждающий принадлежность ключа проверки ЭП Владельцу КСКПЭП.

Средства ЭП – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка ЭП, создание ключа ЭП и ключа проверки ЭП.

Автоматизированная информационная система личный кабинет клиента УЦ (далее ИС ЛК УЦ) – система, позволяющая производить загрузку документов для регистрации Заявителей, осуществлять выпуск и управление КСКПЭП.

Аккредитация УЦ – признание соответствия Удостоверяющего центра требованиям Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Сокращения:

Обозначение	Описание
AIA	Authority Information Access (Доступ к сведениям о центрах сертификации)
OCSP	Online Certificate Status Protocol (Протокол получения статуса сертификата в реальном времени)
TSP	Time Stamp Protocol (Протокол штампов времени)
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи
СНИЛС	Страховой номер индивидуального лицевого счета
СОС	Список отозванных сертификатов

Обозначение	Описание
AIA	Authority Information Access (Доступ к сведениям о центрах сертификации)
ЭП	Электронная подпись
СКЗИ	Средство криптографической защиты информации
ИС ЛК УЦ	Автоматизированная информационная система личный кабинет клиента УЦ
ПО	Программное обеспечение

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет регулирования Порядка

1.1.1. Настоящий Порядок реализации функций аккредитованного Удостоверяющего центра АО «Тандер» (далее – Регламент или Порядок) устанавливает правила пользования услугами УЦ, включая права, обязанности Заявителя, Владельца КСКПЭП, УЦ, определяет ответственность УЦ, а также содержит описание основных процедур и организационно-технических мероприятий, используемых УЦ при выпуске КСКПЭП, управлении их жизненным циклом, форматы данных и протоколы работы.

1.1.2. Регламент разработан в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»), Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативно-правовыми актами Российской Федерации.

1.1.3. Регламент распространяется в форме электронного документа в сети интернет по адресу https://ca-magnit.ru в разделе Документация.

1.1.4. Субъектами, на которых распространяется действие настоящего Регламента, являются все лица, которые в силу настоящего Регламента, договора или действующего законодательства должны соблюдать все правила и требования, предусмотренные настоящим Регламентом: Заявитель, Владелец КСКПЭП, УЦ (далее - Субъекты).

1.2. Присоединение к Регламенту

1.2.1. Лицо, обратившееся в УЦ за получением услуг, присоединяется к Регламенту путем заключения с УЦ договора об оказании услуг, в том числе на условиях публичной оферты, либо путем подписания заявления на изготовление КСКПЭП по форме Приложения №1 настоящего Регламента.

1.2.2. Владелец КСКПЭП имеет право в одностороннем порядке прекратить взаимодействие с УЦ в рамках Регламента, направив в УЦ заявление на прекращение действия (аннулирование) выданного ему КСКПЭП.

1.3. Сведения об Удостоверяющем центре

1.3.1. Акционерное общество «Тандер», именуемое в дальнейшем «Удостоверяющий Центр», «УЦ», зарегистрировано на территории Российской Федерации в городе Краснодаре – Свидетельство о постановке на учет Российской организации в налоговом органе по месту ее нахождения серия 23 №009538203, выдано 28 июня 1996 г. Инспекцией Федеральной налоговой службы №1 по г. Краснодару.

Удостоверяющий Центр в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов открытых ключей осуществляет свою деятельность на территории Российской Федерации в соответствии с положениями Федерального закона № 63-ФЗ от 06.04.2011 г. «Об электронной подписи» и на основании следующих документов:

- решение Правительственной комиссии, уполномоченной на принятие решения об аккредитации удостоверяющих центров на основании протокола от 01.12.2023 № 9пр;
- лицензии ФСБ России ЛСЗ 0011486 рег. №1731Н от 22 марта 2017 г. на осуществление разработки, производства, распространения шифровальных (криптографических)

средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению 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).

2.3.2. Полное наименование: Акционерное общество «Тандер».

2.3.3. Юридический адрес: г. Краснодар, ул. Им. Леваневского, д. 185.

2.3.4. Фактический адрес: г. Краснодар, ул. Солнечная 15/5.

2.3.5. ИНН 2310031475

2.3.6. КПП 997350001

2.3.7. ОГРН 1022301598549

2.3.8. Контактный телефон: 8 (861) 210-48-60

2.3.9. Адрес электронной почты: ca@magnit.ru

2.3.10. Сайт УЦ АО «Тандер»: https://ca-magnit.ru

2.3.11. График работы:

1) информация о времени работы УЦ размещена на официальном сайте УЦ https://ca-magnit.ru;

2) техническая поддержка осуществляется в круглосуточном режиме.

1.4. Порядок информирования о предоставлении услуг Удостоверяющего центра

1.4.1. Информирование по вопросам получения услуг УЦ осуществляется следующими способами:

1) по адресу электронной почты: ca@magnit.ru;

2) по контактному телефону: 8 (861) 210-48-60;

3) путем опубликования информации на официальном сайте: https://ca-magnit.ru.

1.4.2. Информирование Субъектов осуществляется УЦ посредством:

1) направления электронного письма на адрес, указанный при обращении в УЦ;

2) направления SMS-уведомлений на телефонный номер, представленный Заявителем в УЦ;

3) размещения информации на сайте УЦ: https://ca-magnit.ru.

1.4.3 Порядок получения информации Заявителями по вопросам предоставления услуг Удостоверяющего центра.

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

- ознакомиться с информацией, опубликованной на сайте https://ca-magnit.ru;
- обратиться в Удостоверяющий центр за получением информации по справочным телефонам +7 (861) 210-48-60;
- направить запрос по электронной почте на адрес ca@magnit.ru. Срок ответа по запросу, направленному по электронной почте, составляет не более 3 (трех) рабочих дней со дня получения Удостоверяющим центром данному запроса;
- непосредственно обратиться по месту нахождения Удостоверяющего центра;
- направить письменное обращение в адрес Удостоверяющего центра. Данное обращение рассматривается в течение 30 (тридцати) дней со дня его поступления в Удостоверяющий центр.

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

1.5. Стоимость услуг Удостоверяющего центра

1.5.1. Актуальная информация о стоимости и составе услуг УЦ размещена в Прайс-листе на официальном сайте УЦ: https://ca-magnit.ru.

1.5.2. Сроки и порядок расчетов за услуги УЦ определяются договором об оказании услуг, в том числе заключенному на условиях публичной оферты.

1.5.3. Договор об оказании услуг УЦ на условиях публичной оферты размещен в сети Интернет по адресу: https://ca-magnit.ru в разделе Документация.

1.5.4. Сроки и порядок расчетов за услуги УЦ могут быть изменены по согласованию с Заявителем.

1.5.5. УЦ на безвозмездной основе предоставляет любому лицу доступ 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.

1.6. Внесение изменений и дополнений в Регламент

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

1.6.2. Уведомление о внесении изменений и дополнений в Регламент осуществляется Удостоверяющим центром путем обязательного размещения на сайте Удостоверяющего центра в сети Интернет по адресу https://ca-magnit.ru новой версии Регламента, включающей внесенные изменения и дополнения.

1.6.3. Все изменения и дополнения, вносимые Удостоверяющим центром в настоящий Регламент, не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными с даты размещения новой версии Регламента, опубликованного на сайте Удостоверяющего центра.

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

1.6.5. Любые изменения в Регламенте с момента вступления в силу новой версии Регламента распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления новой версии Регламента в силу. В случае несогласия с вышеуказанными изменениями Субъект, присоединившийся к Регламенту до вступления в силу таких изменений, имеет право прекратить договорные отношения и расторгнуть заключенный договор, письменно уведомив Удостоверяющий центр о своих намерениях не позднее, чем 14 (четырнадцать) календарных дней до даты планируемого расторжения договора.

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

2 ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИЙ (ОКАЗЫВАЕМЫХ УСЛУГ)

В процессе реализации своей деятельности Удостоверяющий центр:

- создает квалифицированные сертификаты и выдает такие сертификаты лицам, обратившимся за их получением, при условии установления личности Заявителя;
- осуществляет проверку достоверности документов и сведений, представленных Заявителем;
- осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей;
- выдает по обращению Заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем;
- ведет реестр выданных и аннулированных сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных 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;

- обеспечивает безвозмездный доступ к реестру сертификатов с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, обеспечивает актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- создает по обращениям Заявителей ключи электронных подписей и ключи проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате;
- осуществляет по желанию лица, которому выдан квалифицированный сертификат, регистрацию указанного лица в единой системе идентификации и аутентификации;
- обеспечивает конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;
- обеспечивает целостность, достоверность и конфиденциальность информации, подлежащей хранению в Удостоверяющем центре;
- осуществляет сопровождение квалифицированных сертификатов, выдаваемых Удостоверяющим центром, в том числе обеспечивает внесение в реестр сертификатов информации об аннулированных или прекративших свое действие сертификатах ключей проверки электронной подписи;
- обеспечивает актуализацию и публикацию списка отозванных сертификатов в электронном виде, предоставляет к нему безвозмездный доступ с использованием сети Интернет;
- осуществляет информирование лиц, обращающихся в Удостоверяющий центр для получения квалифицированных сертификатов, об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;
- оказывает техническую поддержку, консультации по вопросам использования электронной подписи и средств электронной подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи;
- осуществляет мероприятия по техническому сопровождению и обеспечению бесперебойного функционирования средств Удостоверяющего центра, обновлению программных и технических средств Удостоверяющего центра;
- обеспечивает информационную безопасность Удостоверяющего центра и осуществляет мероприятия по технической защите информации, обрабатываемой с использованием средств Удостоверяющего центра;
- осуществляет иную связанную с использованием электронной подписи деятельность.

3 ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. Обязанности Удостоверяющего центра

1) осуществлять деятельность в соответствии с требованиями федеральных законов №63 «Об электронной подписи», №149 «Об информации, информационных технологиях и о защите информации», №152 «О персональных данных», требованиями к порядку реализации функций аккредитованного Удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Минцифры России от 13 ноября 2020 г. № 584, иными нормативными правовыми актами в области использования электронной подписи и защиты информации, настоящим Порядком;

2) обеспечить размещение настоящего Порядка на сайте Удостоверяющего центра https://ca-magnit.ru;

3) информировать в письменной форме Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

4) обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в любое время в течение срока деятельности Удостоверяющего центра, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

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

6) обеспечивать конфиденциальность созданных Удостоверяющим центром ключей электронных подписей;

7) обеспечивать бесперебойное функционирование средств Удостоверяющего центра, осуществлять мероприятия по технической защите информации, обрабатываемой с использованием средств Удостоверяющего центра, принимать меры по обеспечению безопасности персональных данных при их обработке в Удостоверяющем центре;

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

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

10) не использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате УЦ, выданном головным Удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными сертификатами;

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

12) использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленными в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

13) использовать для реализации функций Удостоверяющего центра средства Удостоверяющего центра, соответствующие требованиям к средствам Удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796;

14) выдать квалифицированный сертификат в соответствии с требованиями к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 795;

15) осуществлять проверку достоверности документов и сведений, представленных Заявителем, в том числе с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме (далее также – инфраструктура);

16) для внесения в квалифицированный сертификат информации запрашивать и получать из государственных информационных ресурсов сведения об ИНН, паспорте и СНИЛС Заявителя;

17) в установленном порядке идентифицировать Заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация Заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления

сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

В отношении физического лица устанавливаются: 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;

18) осуществить подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата;

19) создать и выдать квалифицированный сертификат Заявителю в соответствии с настоящим Порядком при условии подтверждения достоверности информации, представленной Заявителем для включения в квалифицированный сертификат, установления личности Заявителя - физического лица;

20) создать по обращению Заявителя ключ электронной подписи и ключ проверки электронной подписи;

21) выдать по обращению Заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные Удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем;

22) осуществлять по обращениям участников электронного взаимодействия проверку электронных подписей;

23) обеспечивать уникальность ключей проверки электронных подписей и номеров квалифицированных сертификатов, выдаваемых Удостоверяющим центром;

24) при выдаче квалифицированного сертификата:

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

- подтверждение ознакомления с информацией, содержащейся в квалифицированном сертификате, осуществляется под расписку или 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;

- направить в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате;

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

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

- одновременно с выдачей квалифицированного сертификата предоставить владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

25) отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения квалифицированного сертификата;

26) отказать Заявителю в создании квалифицированного сертификата в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения квалифицированного сертификата;

27) отказать Заявителю в выдаче квалифицированного сертификата в случае, если не подтверждена достоверность информации, представленной Заявителем для включения в квалифицированный сертификат, или не установлена личность Заявителя;

28) аннулировать квалифицированный сертификат, выданный Удостоверяющим центром, в следующих случаях:

- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;
- вступило в силу решение суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию.

29) прекратить действие квалифицированного сертификата на основании надлежаще оформленного заявления Владельца КСКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа, подписанного квалифицированной электронной подписью Владельца КСКПЭП;

30) внести в реестр сертификатов информацию о прекращении действия и (или) об аннулировании квалифицированного сертификата не позднее 12 (двенадцати) часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», или в течение 12 (двенадцати) часов с момента, с момента получения Удостоверяющим центром соответствующих сведений;

31) уведомить Владельца КСКПЭП о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования квалифицированного сертификата, выданного Удостоверяющим центром Владельцу КСКПЭП, в том числе об аннулировании или прекращении действия квалифицированного сертификата;

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

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

34) хранить информацию, внесенную в реестр сертификатов, в течение всего срока деятельности Удостоверяющего центра;

35) обеспечить целостность и достоверность информации, хранящейся в Удостоверяющем центре;

36) незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением сторон, или возникновения у аккредитованного Удостоверяющего центра обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи;

37) не указывать в создаваемом сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном Удостоверяющему центру любым другим Удостоверяющим центром;

38) в случае принятия решения о прекращении деятельности Удостоверяющего центра:

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

- передать в уполномоченный федеральный орган реестр выданных Удостоверяющим центром квалифицированных сертификатов в соответствии с Порядком, утвержденным Приказом Минцифры России от 02.11.2021 №1134;

- передать на хранение в уполномоченный федеральный орган информацию, подлежащую хранению в аккредитованном Удостоверяющем центре.

39) аккредитованный Удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным Удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган. Аккредитованному Удостоверяющему центру запрещается использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным Удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, для подписания сертификатов, не являющихся квалифицированными сертификатами;

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

41) обязан выполнять порядок реализации функций аккредитованного Удостоверяющего центра и исполнения его обязанностей, установленный таким аккредитованным Удостоверяющим центром в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного Удостоверяющего центра и исполнения обязанностей, а также с Федеральным законом «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи»;

42) в течение срока деятельности Удостоверяющего центра, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации, хранить информацию о реквизитах основного документа, удостоверяющего личность Владельца КСКПЭП. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность.

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

3.2. Права Удостоверяющего центра

Удостоверяющий центр имеет право:

1) запрашивать у Заявителя документы, необходимые для установления личности получателя квалифицированного сертификата (Заявителя);

2) запрашивать у Заявителя документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата;

3) отказать Заявителю в приеме заявления на создание и выдачу квалифицированного сертификата в следующих случаях:

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

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

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

- в случае подачи заявления на создание и выдачу квалифицированного сертификата с ошибками, исправлениями, подчистками и/или приписками, не подтвержденными собственноручной подписью Заявителя;

4) отказать Заявителю в прекращении действия квалифицированного сертификата, выданного Удостоверяющим центром, в следующих случаях:

- соответствующие заявительные документы не оформлены либо оформлены ненадлежащим образом;

- квалифицированный сертификат был аннулирован или прекратил свое действие в соответствии с частями 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

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

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

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

6) отказать в выдаче КСКПЭП Заявителю в случаях:

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

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

7) устанавливать сроки действия квалифицированных сертификатов;

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

9) использовать представленные Заявителем номера мобильной связи и адреса электронной почты для рассылки уведомлений об окончании срока действия КСКПЭП, и иной информации;

10) отказать в прекращении действия КСКПЭП в случае ненадлежащего оформления заявления на прекращение действия КСКПЭП, а также в случае, если КСКПЭП аннулирован или прекратил своё действие по другим основаниям.

3.3. Ответственность Удостоверяющего центра

1) УЦ (работник аккредитованного Удостоверяющего центра) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного Удостоверяющего центра и исполнения его обязанностей.

2) Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате:

- неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора об оказании услуг УЦ;
- неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом «Об электронной подписи».

3) УЦ не несет ответственность за невозможность использования КСКПЭП в случае, если такая возможность возникла после создания КСКПЭП и вызвана изменением требований информационных систем или действующих нормативно-правовых актов.

4 ПРАВА И ОБЯЗАННОСТИ ЗАЯВИТЕЛЯ И ВЛАДЕЛЬЦА КСКПЭП

4.1. Права Заявителя

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

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

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

4.2. Права Владельца КСКПЭП

Владелец КСКПЭП имеет все права Заявителя, присоединившегося к Регламенту, а также имеет право:

1) получить в соответствии с настоящим Порядком квалифицированный сертификат в Удостоверяющем центре, при условии установления Удостоверяющим центром личности лица, обращающегося за получением данного сертификата;

2) при получении квалифицированного сертификата:

- получить ключ электронной подписи и ключ проверки электронной подписи, созданные Удостоверяющим центром;
- пройти процедуру регистрации в единой системе идентификации и аутентификации;

3) запрашивать и получать в Удостоверяющем центре информацию из реестра сертификатов Удостоверяющего центра;

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

5) создавать с использованием средства электронной подписи ключ электронной подписи

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

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

4.3. Обязанности Заявителя

1) исполнять требования, установленные Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»», принимаемыми в соответствии с ним нормативными правовыми актами и Порядком;

2) представлять в соответствии с настоящим Порядком в Удостоверяющий центр актуальные и достоверные документы, надлежащим образом заверенные копии и сведения, в том числе необходимые для получения квалифицированного сертификата, регистрации квалифицированного сертификата в единой системе идентификации и аутентификации и (или) регистрации Владельца КСКПЭП в единой системе идентификации и аутентификации.

4.4. Обязанности Владельца КСКПЭП

Владелец КСКПЭП должен соблюдать все обязанности Заявителя, присоединившегося к Порядку, а также обязан:

1) при получении квалифицированного сертификата:

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

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

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

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

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

6) при проверке электронной подписи осуществлять проверку принадлежности Владельцу КСКПЭП электронной подписи, с помощью которой подписан электронный документ, а также осуществлять проверку отсутствия изменений, внесенных в этот документ после его подписания;

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

8) использовать для создания и проверки электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

9) обеспечивать конфиденциальность используемых ключей электронных подписей, в частности не допускать использование ключей электронных подписей иными лицами без своего согласия;

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

11) не использовать ключ электронной подписи, срок действия которого истек.

5 ПОРЯДОК И СРОКИ ВЫПОЛНЕНИЯ ПРОЦЕДУР (ДЕЙСТВИЙ), НЕОБХОДИМЫХ ДЛЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

5.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей

Порядок создания ключей электронных подписей и ключей проверки электронных подписей осуществляется самостоятельно Заявителем или Удостоверяющим центром.

5.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей самостоятельно Заявителем:

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

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

информации (Положение ПКЗ-2005)" (зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 г., регистрационный N 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. N 173 "О внесении изменений в некоторые нормативные правовые акты ФСБ России" (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный N 17350).

3) Заявитель, присоединившийся к Регламенту, имеет право получить средства электронной подписи при обращении в Удостоверяющий центр в соответствии с настоящим Порядком.

4) При создании ключа электронной подписи и ключа проверки электронной подписи Заявитель формирует запрос на создание сертификата в электронной форме (файл в формате PKCS#10) в ИС ЛК УЦ. Сформированный запрос на создание сертификата прикладывается к заявке на создание и изготовление квалифицированного сертификата ключа проверки электронной подписи в ИС ЛК УЦ.

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

6) Хранение и использование ключей электронных подписей должно осуществляться Заявителем в соответствии с Инструкцией ФАПСИ № 152, руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в Приложении №2 к настоящему Порядку.

5.1.2. Порядок создание ключей электронных подписей и ключей проверки электронных подписей Удостоверяющим центром для Заявителя:

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

2) Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона от 06.04.2011 N 63-ФЗ «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" в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для Заявителя.

3) Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Удостоверяющим центром для Заявителя, присоединившегося к настоящему Порядку, при условии установления личности Заявителя.

4) Ключ электронной подписи и ключ проверки электронной подписи создается Удостоверяющим центром одновременно с созданием квалифицированного сертификата в соответствии с настоящим Порядком, при условии подтверждения достоверности документов и сведений, представленных Заявителем.

5) Создание ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата осуществляется Оператором УЦ в присутствии Заявителя.

Созданный ключ электронной подписи, ключ проверки электронной подписи и квалифицированный сертификат записываются Оператором УЦ на носитель ключевой информации (далее также – ключевой носитель), предоставленный Заявителем. Передача ключевого носителя с записанной на него ключевой информацией осуществляется под расписку и сопровождается записью в соответствующих журналах поэкземплярного учета СКЗИ. Удостоверяющий центр не осуществляет хранение ключа электронной подписи Заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие Заявителю.

6) Ключевой носитель, предоставленный Заявителем, перед осуществлением записи на него создаваемого Удостоверяющим центром ключа электронной подписи и ключа проверки электронной подписи, не должен содержать иной посторонней информации, в том числе ключей электронной подписи. Удостоверяющий центр не несёт ответственности в связи с компрометацией или удалением информации, находящейся на ключевом носителе, предоставленном Заявителем.

7) При создании ключа электронной подписи и ключа проверки электронной подписи Удостоверяющим центром формируется пароль доступа к ключевой информации, который устанавливается по согласованию с Заявителем. После получения ключа электронной подписи и ключа проверки электронной подписи Заявитель должен произвести смену пароля доступа к ключевой информации.

8) В случае, если Удостоверяющий центр не имеет технической возможности использовать для создания ключа электронной подписи и ключа проверки электронной подписи средство электронной подписи, аналогичное средству электронной подписи Заявителя, указанному им в Заявительных документах, Заявитель имеет право самостоятельно осуществить создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с настоящим Порядком.

9) В случае создания ключа электронной подписи и ключа проверки электронной подписи при личном прибытии Заявителя в Удостоверяющий центр основанием подтверждения владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, является одновременное соблюдение следующих условий:

- подтверждена достоверность документов и сведений, представленных Заявителем в Удостоверяющий центр Заявителем;
- установлена личность Заявителя;
- Заявитель ознакомился с информацией, содержащейся в запросе на создание сертификата, сформированном Удостоверяющим центром.

5.1.3. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены:

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

2) Основаниями для выполнения процедуры плановой смены ключа электронной подписи Удостоверяющего центра и процедуры его вывода из эксплуатации являются запланированные мероприятия по осуществлению деятельности Удостоверяющего центра.

3) Выполнение процедуры плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в период срока действия ключа электронной подписи Удостоверяющего центра, не ранее, чем через один год, и не позднее, чем через один год и три месяца после начала действия ключа электронной подписи Удостоверяющего центра. Процедура создания нового ключа электронной подписи Удостоверяющего центра осуществляется заранее, не позднее, чем за 45 дней до истечения одного года и трех месяцев после начала срока действия ключа электронной подписи Удостоверяющего центра.

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

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

6) Начало периода действия ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени выпуска сертификата Головным Удостоверяющим центром Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

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

1) В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра или реализации угрозы нарушения его конфиденциальности осуществляется внеплановая

смена ключа электронной подписи и ключа проверки электронной подписи Удостоверяющего центра.

2) К случаям нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра относятся:

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

3) Виды угроз нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра:

- угрозы, непосредственно связанные с нарушением конфиденциальности ключа электронной подписи Удостоверяющего центра;
- угрозы, связанные с несанкционированным доступом в помещения, где размещаются технические средства Удостоверяющего центра, или доступам к хранилищам ключевой информации;
- угрозы, связанные с несанкционированным доступом к средствам Удостоверяющего центра;
- угрозы, связанные с лицами, имеющими доступ в контролируемую зону, к средствам Удостоверяющего центра, ключам электронной подписи Удостоверяющего центра;
- угрозы, связанные с проведением нарушителем атак на технические средства Удостоверяющего центра, в том числе на носители защищаемой информации, средства вычислительной техники, среду функционирования средств криптографической защиты информации, каналы (линии) связи.

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

5) Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра осуществляется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра в соответствии с пунктом 5.1.5 настоящего Порядка.

6) Одновременно со сменой ключа электронной подписи Удостоверяющего центра прекращается действие всех ранее выданных квалифицированных сертификатов, созданных с

использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

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

8) Прекращение действия квалифицированного сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия квалифицированного сертификата Удостоверяющего центра включается в список отозванных сертификатов, который публикуется головным Удостоверяющим центром.

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

10) Доверенными способами получения нового квалифицированного сертификата Удостоверяющего центра являются:

- получение Заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении квалифицированного сертификата, созданного Удостоверяющим центром для Заявителя;
- загрузка нового квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

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

1) Смена ключа электронной подписи Владельца КСКПЭП осуществляется в следующих случаях:

а) в связи с истечением установленного срока действия ключа электронной подписи;

б) на основании заявления Владельца КСКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

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

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

д) вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию;

е) 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, настоящим Порядком или договором оказания услуг Удостоверяющего центра.

2) В случае наступления обстоятельств, указанных в подпунктах «в», «г», «д» пункта 5.1.5 настоящего Порядка, Удостоверяющий центр аннулирует квалифицированный сертификат Владельца КСКПЭП и уведомляет об этом Владельца КСКПЭП. Информация о прекращении действия и (или) об аннулировании сертификата вносится Удостоверяющим центром в реестр сертификатов не позднее 12 (двенадцати) часов с момента наступления указанных обстоятельств, или в течение 12 (двенадцати) часов с момента получения Удостоверяющим центром соответствующих сведений. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

3) Процедура выдачи квалифицированного сертификата и ключа электронной подписи (при необходимости) владельцу, в том числе в электронной форме осуществляется в соответствии со статьей 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и настоящего Порядка.

4) Требования к заявлению на смену ключа электронной подписи владельца квалифицированного сертификата и выдачу квалифицированного сертификата:

- создание Удостоверяющим центром нового ключа электронного подписи осуществляется одновременно с созданием и выдачей Заявителю ключа проверки электронной подписи и

квалифицированного сертификата на основании соответствующего заявления Стороны, присоединившейся к Порядку, и документов, представленных в Удостоверяющий центр.

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

- заявление на смену ключа электронной подписи оформляется по форме, приведенной в Приложении №1 к настоящему Порядку и должно содержать:

- фамилию, имя и отчество;
- ИНН физического лица;
- страну;
- регион;
- город;
- страховой номер индивидуального лицевого счета (СНИЛС);
- реквизиты основного документа, удостоверяющего личность;
- адрес электронной почты;
- контактный телефон;
- дату подписания;
- собственноручную подпись Заявителя - при подаче заявления на бумажном носителе или усиленную квалифицированную электронную подпись Заявителя - при подаче заявления в форме электронного документа.

5.1.6. Плановая смена ключей электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

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

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

2) Сформированный запрос на создание квалифицированного сертификата Удостоверяющего центра, а также иная информация, необходимая для получения квалифицированного сертификата Удостоверяющего центра, направляется в уполномоченный федеральный орган, являющийся головным Удостоверяющим центром в отношении Удостоверяющего центра.

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

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

3) После получения квалифицированного сертификата, созданного Головным Удостоверяющим центром уполномоченного федерального органа, Администратор Удостоверяющего центра:

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

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

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

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

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

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

Доверенными способами получения квалифицированного сертификата Удостоверяющего центра являются:

- получение Заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении квалифицированного сертификата, созданного Удостоверяющим центром для Заявителя;
- загрузка квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи».

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

5.2.1.2. Присоединение к Порядку осуществляется в соответствии с настоящим Порядком. Для присоединения к настоящему Порядку и возможности получения услуг Удостоверяющего центра Заявитель направляет заявление о присоединении к Порядку по форме Приложения №1 к настоящему Порядку.

5.2.1.3. Удостоверяющий центр осуществляет создание квалифицированных сертификатов при условии выполнения Субъектом, присоединившимся к Порядку, своих обязанностей.

5.2.1.4. Создание квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявления на создание и выдачу квалифицированного сертификата, а также документов и сведений, представленных Заявителем в Удостоверяющий центр, при условии установления личности Заявителя.

5.2.1.5. Для регистрации в Удостоверяющем центре Заявитель направляет в Удостоверяющий центр заявление на создание и выдачу квалифицированного сертификата на бумажном носителе, подписанное собственноручно, или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Заявителя.

5.2.1.6. Заявитель имеет право представить в Удостоверяющий центр заявление на создание и выдачу квалифицированного сертификата, а также документы и сведения, необходимые для регистрации и создания квалифицированного сертификата, одним пакетом документов при личном прибытии Заявителя в Удостоверяющий центр, либо представить указанные документы в форме электронных документов, подписанных усиленной квалифицированной электронной подписью Заявителя, направив их в Удостоверяющий центр с использованием ИС ЛК УЦ.

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

5.2.1.8. После получения Удостоверяющим центром от Заявителя заявления на создание и выдачу квалифицированного сертификата, в случае, если Заявителем не представлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не в полном объеме или их

достоверность и актуальность не подтверждается, Удостоверяющий центр имеет право запросить, а Субъект, присоединившийся к Порядку, обязан представить документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата.

5.2.1.9. Удостоверяющий центр имеет право отказать Заявителю в приеме заявления на создание и выдачу квалифицированного сертификата , в случае, если тот не представил документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не в полном объеме или они не надлежаще оформлены, а также в случае, когда достоверность и актуальность представленных Заявителем сведений не подтверждается.

5.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов.

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

Заявление оформляется по форме, приведенной в Приложении №1 к настоящему Порядку и должно содержать:

- фамилию, имя и отчество;
- ИНН физического лица;
- страну;
- регион;
- город;
- страховой номер индивидуального лицевого счета (СНИЛС);
- реквизиты основного документа, удостоверяющего личность;
- адрес электронной почты;
- контактный телефон;
- собственноручную подпись Заявителя - при подаче заявления на бумажном носителе или усиленную квалифицированную электронную подпись Заявителя - при подаче заявления в форме электронного документа.

5.2.3. Порядок идентификации Заявителя.

Идентификации Заявителя осуществляется в соответствии со статьей 18 Федерального закона "Об электронной подписи.

Идентификация гражданина Российской Федерации осуществляется:

- при его личном присутствии по основному документу, удостоверяющему личность;
- 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 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

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

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

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

При обращении в аккредитованный УЦ Заявитель представляет следующие документы либо их надлежащим образом заверенные копии и сведения:

а) основной документ, удостоверяющий личность.

б) страховой номер индивидуального лицевого счета Заявителя - физического лица;

в) идентификационный номер налогоплательщика Заявителя - физического лица;

УЦ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных Заявителем в соответствии с ФЗ 63 ст. 18 частями 2 и 2.1.

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

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

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

5.2.5. Порядок проверки достоверности документов и сведений, представленных Заявителем.

Для заполнения КСКПЭП в соответствии с частью 2 статьи 17 Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов сведения, предусмотренные частью 2.2 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной Заявителем для включения в КСКПЭП, и Удостоверяющим центром идентифицирован Заявитель, Удостоверяющий центр осуществляет процедуру создания и выдачи Заявителю КСКПЭП. В противном случае Удостоверяющий центр отказывает Заявителю в выдаче КСКПЭП.

5.2.6. Порядок создания квалифицированного сертификата

5.2.6.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13 – 15, 17 и 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и настоящим Порядком. Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

5.2.6.2. Удостоверяющий центр не позднее одного рабочего дня со дня получения из государственных информационных ресурсов положительного результата проверки документов и сведений, представленных Заявителем, уведомляет Заявителя о необходимости прохождения процедуры установления личности и согласовывает с Заявителем дату и время прибытия Заявителя в Удостоверяющий центр.

Создание квалифицированного сертификата осуществляется Удостоверяющим центром только при успешной идентификации Заявителя. В противном случае создание и выдача квалифицированного сертификата Удостоверяющим центром не осуществляется, а Заявителю возвращаются представленные им документы с пояснением причин отказа.

5.2.6.3. Если Заявителем не представлены надлежащим образом заверенные копии документов, такие копии заверяются в Удостоверяющем центре при представлении оригиналов документов.

5.2.6.4. Для создания квалифицированного сертификата Оператор УЦ осуществляет:

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

- с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, осуществляет создание ключа электронной подписи и ключа проверки электронной подписи. При создании ключа электронной подписи и ключа проверки электронной подписи производится их запись непосредственно на ключевой носитель, предоставленный Заявителем;

- одновременно с созданием ключа электронной подписи и ключа проверки электронной подписи Оператор УЦ осуществляет формирование запроса на создание сертификата в форме

электронного документа, проверяет уникальность созданного ключа проверки электронной подписи;

- на основании сформированного запроса на создание сертификата, осуществляет создание квалифицированного сертификата с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

5.2.6.5. Допускается осуществлять процедуру создания квалифицированного сертификата без прибытия Заявителя в Удостоверяющий центр при одновременном соблюдении следующих условий:

1) информационное взаимодействие, осуществляется способами, позволяющими обеспечить целостность информации и ее конфиденциальность, в случае передачи конфиденциальной информации;

2) личность лица, обращающегося за получением сертификата, была установлена Удостоверяющим центром дистанционно согласно требованиям Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

3) получен положительный результат проведения проверки документов и сведений, представленных Заявителем.

5.2.7 Порядок выдачи квалифицированного сертификата

5.2.7.1. Выдача квалифицированного сертификата, осуществляется Удостоверяющим центром в соответствии с положениями статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и настоящим Порядком. При получении квалифицированного сертификата Заявитель ознакамливается с информацией, содержащейся в квалифицированном сертификате.

5.2.7.2. Выдача квалифицированного сертификата, созданного Удостоверяющим центром, осуществляется при условии идентификации личности Заявителя в Удостоверяющем центре.

5.2.7.3. УЦ предоставляет Заявителю руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении №2 настоящего Порядка.

5.2.7.4. Процедура выдачи квалифицированного сертификата, созданного Удостоверяющим центром.

После создания квалифицированного сертификата в соответствии с пунктом 5.2.6 настоящего Порядка Оператор УЦ:

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

- передает Владельцу КСКПЭП ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи. Указанный ключевой носитель передается Владельцу КСКПЭП под расписку и записью в соответствующих журналах поэкземплярного учета СКЗИ, в том числе журнале учета сертификатов ключей проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключа электронной подписи Заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие Заявителю;

- выдает Владельцу КСКПЭП квалифицированный сертификат, созданный Удостоверяющим центром в форме электронного документа, квалифицированный сертификат Удостоверяющего центра и квалифицированный сертификат головного Удостоверяющего центра;

- выдает руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в Приложении №2 настоящего Порядка.

Указанное руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в Приложении №2 настоящего Порядка, может быть направлено Владельцу КСКПЭП по электронной почте в форме электронного документа.

По согласованию с Владельцем КСКПЭП направляет Владельцу КСКПЭП или записывает на носитель информации, представленный Заявителем, документацию в форме электронных документов, в том числе содержащую руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в Приложении №2 настоящего Порядка, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

- направляет в единую систему идентификации и аутентификации сведения о Владельце КСКПЭП, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного Удостоверяющего центра);

- вносит в реестр сертификатов Удостоверяющего центра информацию о выданном квалифицированном сертификате и сведения о Владельце КСКПЭП;

- по желанию Владельца КСКПЭП безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации.

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

5.2.8.1. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата Заявителя исчисляется с момента получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, а также надлежаще оформленных документов и сведений от Заявителя и зависит от сроков и результатов проверки сведений, выполняемой Удостоверяющим центром с использованием инфраструктуры в соответствии частью 2.2 и частью 2.3 статьи 18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» из государственных информационных ресурсов. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата Заявителя не может превышать 3 (трех) рабочих дней со дня получения Удостоверяющим центром положительных ответов на запросы Удостоверяющего центра по проверке сведений и документов, представленных Заявителем, с помощью государственных информационных ресурсов.

5.2.8.2. Удостоверяющий центр оказывает услуги по срочному выпуску квалифицированного сертификата при:

- представлении полного пакета необходимых документов;

- получении положительных результатов проверок данных, представленных Заявителем с использованием инфраструктуры согласно п. 2.2 ст.18 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

- установлении личности Заявителя;

- поступлении средств на счет Удостоверяющего центра за выбранные товары и услуги.

Создание и выдача квалифицированного сертификата осуществляется в соответствии с требованиями Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи» и условиями, определенными настоящим Порядком.

5.3 Подтверждение действительности электронной подписи, использованной для подписания электронных документов

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

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

5.3.1.1. Для подтверждения действительности электронной подписи участник электронного взаимодействия представляет в Удостоверяющий центр заявление на подтверждение действительности электронной подписи в электронном документе. Заявление представляется в Удостоверяющий центр в форме документа на бумажном носителе, подписанного Заявителем собственноручно, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью по форме, приведенной в Приложении №5 к настоящему Порядку.

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

5.3.1.3. Заявление должно содержать:

- дата письма;

- собственноручную подпись физического лица;

- серийный номер квалифицированного сертификата, выданного Удостоверяющим центром, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе;

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

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

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

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

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

- электронный документ, подписанный электронной подписью, основанной на квалифицированном сертификате, выданный Удостоверяющим центром (в виде одного файла стандарта CMS), либо электронный документ (в виде файла) и отдельно электронную подпись данного документа (в виде файла стандарта CMS).

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

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

- заявление не соответствует требованиям, приведенным в пункте 5.3.1 настоящего Порядка, в том числе в случае, если заявление не оформлено надлежащим образом, не содержит необходимой информации или содержит трудноразличимый текст;

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

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

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

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

5.3.3. Порядок оказания услуги.

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

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

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

3) При проведении экспертизы по проверке действительности электронной подписи в электронном документе выполняется проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного

сертификата до квалифицированного сертификата Удостоверяющего центра, выданного ему головным Удостоверяющим центром.

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

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

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

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

5.4 Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата

5.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата.

5.4.1.1 КСКПЭП прекращает свое действие в случаях, установленных Федеральным законом № 63-ФЗ:

- в связи с истечением установленного срока действия квалифицированного сертификата;
- на основании заявления Владельца КСКПЭП, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или соглашением (договором оказания услуг Удостоверяющего центра) с Владельцем КСКПЭП.

5.4.1.2. Удостоверяющий центр аннулирует КСКПЭП в следующих случаях:

- не подтверждено, что владелец квалифицированного сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;
- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;
- вступило в силу решение суда, которым установлено, что квалифицированный сертификат содержит недостоверную информацию.

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

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

1) Порядок подачи в Удостоверяющий центр заявления о прекращении действия квалифицированного сертификата:

а) Владелец КСКПЭП передает в Удостоверяющий центр заявление о прекращении действия квалифицированного сертификата либо на бумажном носителе, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Владельца КСКПЭП, в том числе с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (далее – Единый портал).

В случае направления Владельцем КСКПЭП заявления о прекращении действия квалифицированного сертификата с использованием Единого портала, принятое по заявлению о прекращении действия квалифицированного сертификата решение Удостоверяющего центра в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Удостоверяющего центра, направляется в Единый портал для размещения решения после проведения проверки действительности усиленной квалифицированной электронной подписи Удостоверяющего центра, которой решение подписано, и подтверждения ее действительности в личном кабинете Заявителя. В случае принятия положительного решения по заявлению о прекращении действия квалифицированного сертификата Удостоверяющий центр направляет информацию в Единый портал о прекращении действия квалифицированного сертификата после внесения соответствующей информации в реестр квалифицированных сертификатов. Направление указанных в настоящем абзаце решений и информации осуществляется посредством единой системы межведомственного электронного взаимодействия.

б) Владелец КСКПЭП передает заявление о прекращении действия квалифицированного сертификата в Удостоверяющий центр в следующих случаях:

- принятие Владельцем КСКПЭП решения о прекращении действия квалифицированного сертификата;
- изменились сведения о Владельце КСКПЭП, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными;
- нарушена конфиденциальность ключа электронной подписи Владельца КСКПЭП.

в) Заявление о прекращении действия квалифицированного сертификата оформляется по форме, приведенной в Приложении №4 к настоящему Порядку, и должно содержать:

- серийный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
-наименование аккредитованного удостоверяющего центра, выдавшего квалифицированный сертификат;
- фамилия, имя, отчество (при наличии);
- страховой номер индивидуального лицевого счета;
- индивидуальный номер налогоплательщика;
- дату подписания заявления;
- причину прекращения действия квалифицированного сертификата;
- собственноручную подпись Владельца КСКПЭП при подаче заявления на бумажном носителе или усиленную квалифицированную электронную подпись Владельца КСКПЭП при подаче заявления в форме электронного документа, в том числе с использованием Единого портала.

2) Порядок приема Удостоверяющим центром заявления о прекращении действия квалифицированного сертификата.

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

а) Проверка заявления на соответствие требованиям, указанным в пункте 5.4.2.1 настоящего Порядка.

б) Проверка соответствия сведений, указанных в заявлении, и сведений, которые имеются в Удостоверяющем центре о Владельце КСКПЭП и выданном ему квалифицированном сертификата.

5.4.3. Установление личности Владельца КСКПЭП осуществляется в порядке, предусмотренном для процедуры создания и выдачи квалифицированного сертификата, приведенном в настоящем Порядке. Владелец КСКПЭП должен обратиться в Удостоверяющий центр с заявлением о прекращении действия квалифицированного сертификата лично.

В случае, если заявление не соответствует условиям и требованиям в соответствии с настоящим Порядком, в том числе в случае, если квалифицированный сертификат, сведения о котором указаны в заявлении о прекращении действия квалифицированного сертификата, не выдавался Удостоверяющим центром, либо сведения, указанные в заявлении, не соответствуют сведениям о Владельце КСКПЭП, Удостоверяющий центр отказывает в прекращении действия квалифицированного сертификата.

В случае, если причиной прекращения действия квалифицированного сертификата в заявлении о прекращении действия квалифицированного сертификата указано нарушение конфиденциальности ключа электронной подписи Владельца КСКПЭП, Заявитель должен подписать заявление о прекращении действия такого квалифицированного сертификата собственноручно, либо другим КСКПЭП.

Удостоверяющий центр имеет право отказать Заявителю в приеме заявления о прекращении действия квалифицированного сертификата в форме электронного документа, если оно подписано усиленной квалифицированной электронной подписью, конфиденциальность ключа которой была нарушена.

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

5.4.4.1. После проверки заявления и полномочий Владельца КСКПЭП Удостоверяющий центр:

- выполняет процедуру прекращения действия квалифицированного сертификата;
- вносит информацию о прекращении действия квалифицированного сертификата в список отозванных сертификатов Удостоверяющего центра;
- вносит информацию о прекращении действия квалифицированного сертификата в реестр сертификатов Удостоверяющего центра.

5.4.4.2. Информация о прекращении действия или аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр квалицированных сертификатов Удостоверяющего центра. Срок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов не может превышать 12 (двенадцать) часов с момента приема заявления на прекращение действия (аннулирование) КСКПЭП или наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения Удостоверяющим центром соответствующих сведений.

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

5.4.4.4. Информация о прекращении действия или аннулировании квалифицированных сертификатов включается Удостоверяющим центром в список отозванных сертификатов, который подписывается электронной подписью, основанной на квалифицированном сертификате Удостоверяющего центра, и публикуется на сайте Удостоверяющего центра.

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

5.4.4.6. Оповещение участников электронного взаимодействия о факте прекращения действия квалифицированного сертификата осуществляется Удостоверяющим центром путем опубликования первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о квалифицированном сертификате, который аннулирован или действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем оповещения о прекращении действия квалифицированного сертификата является время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» («thisUpdate») списка отозванных сертификатов.

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

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

5.5 Порядок ведения реестра квалифицированных сертификатов

5.5.1. Формы ведения реестра квалифицированных сертификатов.

5.5.1.1 Формирование и ведение реестра сертификатов Удостоверяющего центра.

1) Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»,

Порядком формирования и ведения реестров выданных аккредитованными Удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минцифры России от 08 ноября 2021 г. № 1138, иными принимаемыми в соответствии с Федеральным законом «Об электронной подписи» и Федеральным законом «Об информации, информационных технологиях и о защите информации» нормативными правовыми актами и настоящим Порядком.

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

3) Ведение реестра сертификатов включает в себя:

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

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

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

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

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

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

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

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

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

7) Срок предоставления Удостоверяющим центром запрошенной Заявителем информации, содержащейся в реестре сертификатов, не превышает:

- 5 (пяти) рабочих дней со дня получения запроса от Заявителя в случае, если Удостоверяющий центр направляет запрошенную информацию в форме документа на бумажном носителе с использованием почтового отправления;

- 1 (один) рабочий день для направления выписки посредством информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

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

В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан передать в уполномоченный федеральный орган реестр сертификатов в соответствии с Порядком передачи реестров выданных аккредитованными Удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного Удостоверяющего центра, утвержденным приказом Минцифры России от 08 ноября 2021 г. № 1138.

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

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

Информация о прекращении действия или аннулирования квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра не позднее 12 (двенадцати) часов с момента приема заявления на прекращение действия (аннулирование) КСКПЭП или наступления обстоятельств, указанных в подпунктах 5.4.1 настоящего Порядка.

5.6 Порядок технического обслуживания реестра квалифицированных сертификатов

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

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

5.6.1. Максимальные сроки проведения технического обслуживания.

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

Техническое обслуживание реестра сертификатов при проведении внеплановых технических работ осуществляется не более 24 (двадцати четырех) часов с момента их начала.

Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин, но не более чем на 5 (пять) дней со дня их начала, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия.

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

Перед проведением работ по техническому обслуживанию реестра сертификатов, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия, Удостоверяющий центр оповещает о проведении вышеуказанных работ посредством публикации соответствующей информации на сайте Удостоверяющего центра.

6 ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

6.1 Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки.

6.1.1. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, содержащее информацию об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, приведено в Приложении №2 к настоящему Порядку. Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи передается Заявителю одновременно с выдачей КСКПЭП.

6.1.2. Удостоверяющий центр осуществляет информирование Заявителя об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки путем размещения настоящего Порядка, а также руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, которое приведено в Приложении №2 к настоящему Порядку, отдельным документом в электронной форме на сайте Удостоверяющего центра по адресу https://ca-magnit.ru/.

Заявитель при оформлении заявления на регистрацию и изготовление КСКПЭП предоставляет свое письменное 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 и выдачу КСКПЭП, форма которого приведена в Приложении №1 к настоящему Порядку. Заявление на создание и выдачу КСКПЭП подписывает лицо, указанное в заявлении на создание и выдачу КСКПЭП. Персональные данные, внесенные в КСКПЭП, в силу публичности КСКПЭП в соответствии с Федеральным законом N 63-ФЗ становятся общедоступными.

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

6.2 Выдача по обращению Заявителя средств электронной подписи

6.2.1. Средства электронной подписи, используемые Заявителем, должны соответствовать требованиям частью 4 статьи 6 и статьи 12 Федерального закона «Об электронной подписи», Требованиями к средствам электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, а также обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

6.2.2. Выдача и распространение сертифицированных средств электронной подписи и эксплуатационной документации к ним осуществляется Удостоверяющим центром на основании положений, приведенных в настоящем Порядке, в соответствии с требованиями Инструкция ФАПСИ № 152. Факт выдачи Заявителям сертифицированных средств электронной подписи и эксплуатационной документации к ним учитывается в соответствующих журналах поэкземплярного учета СКЗИ.

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

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

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

6.3.2. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем соблюдения порядка формирования и ведения реестра сертификатов в соответствии с настоящим Порядком.

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

6.3.4. Мероприятия по обеспечению защиты информации, при её обработке с использованием средств Удостоверяющего центра, осуществляются в том числе в соответствии с требованиями федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, Составом и содержанием организационных и технических

мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10 июля 2014 года № 378, Требованиями к средствам электронной подписи и Требованиями к средствам Удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, Инструкцией ФАПСИ № 152.

6.3.5. Обработка информации осуществляется с использованием средств Удостоверяющего центра, соответствующих Требованиям к средствам электронной подписи и Требованиями к средствам Удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, прошедших оценку соответствия по требованиям безопасности информации.

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

- обеспечивается контроль доступа в помещения, где размещены технические средства Удостоверяющего центра;
- реализована ролевая модель доступа к компонентам средств Удостоверяющего центра, обеспечивается идентификация, аутентификация и разграничение доступа уполномоченных лиц к программным и техническим средствам Удостоверяющего центра и защищаемой информации;
- обеспечивается контроль действий уполномоченных лиц Удостоверяющего центра и обслуживающего персонала, приняты меры по предотвращению несанкционированного доступа к средствам Удостоверяющего центра и защищаемой информации;
- формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему;
- осуществляется регулярное резервное копирование информации, содержащейся в реестре сертификатов с соблюдением требований к защите от несанкционированного доступа к средствам резервного копирования и резервируемой информации;
- для хранения информации используются опечатываемые хранилища информации (металлические шкафы, сейфы, пеналы).

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

6.4.1. Удостоверяющий центр в соответствии с пунктом 3 части 2 статьи 13 и частью 3 статьи 15 Федерального закона «Об электронной подписи» обеспечивает безвозмездный круглосуточный доступ к реестру сертификатов, опубликованному на сайте Удостоверяющего центра, при обращении к нему любого лица с использованием сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов, проводимых Удостоверяющим центром в соответствии с настоящим Порядком.

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

6.4.3. В соответствии с Порядком формирования и ведения реестров выданных аккредитованными Удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минцифры России от 08 ноября 2021 г. № 1138, доступ заинтересованных лиц к реестру квалифицированных сертификатов осуществляется с использованием информационно-телекоммуникационных сетей.

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

6.5 Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

6.5.1. Конфиденциальность созданных Удостоверяющим центром ключей электронных подписей, а также ключей электронных подписей Удостоверяющего центра, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной

безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра.

6.5.2. Хранение и использование ключей электронных подписей Удостоверяющего центра осуществляется в соответствии с требованиями Инструкции ФАПСИ № 152.

6.5.3. Средства Удостоверяющего центра, с использованием которых осуществляется использование и хранение ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра, имеют документ, подтверждающий оценку соответствия по требованиям безопасности информации и соответствуют Требованиям к средствам электронной подписи и Требованиями к средствам Удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796.

6.5.4. Ключи электронной подписи Удостоверяющего центра выводятся из эксплуатации при окончании срока их действия.

6.5.5. Порядок обеспечения конфиденциальности ключей электронных подписей Заявителей:

1) Конфиденциальность ключей электронных подписей Заявителей обеспечивается Удостоверяющим центром в период времени получения носителя ключевой информации от Заявителя и записи на него ключей электронной подписи, созданных Удостоверяющим центром, до момента передачи ключевого носителя Заявителю, при этом создание и запись ключа электронной подписи на ключевой носитель, представленный Заявителем осуществляется Удостоверяющим центром только в случае личного прибытия Заявителя в Удостоверяющий центр и в его присутствии.

2) Выдача ключей электронной подписи Заявителю осуществляется Удостоверяющим центром в порядке, определенном настоящим Регламентом.

3) После создания Удостоверяющим центром ключа электронных подписи Заявителя и его записи на носитель ключевой информации, предоставленный непосредственно перед созданием ключа электронных подписи Заявителем, данный носитель ключевой информации, в том числе содержащий ключ электронной подписи, указанный ключевой носитель выдается Заявителю под расписку, при этом в соответствующий журнал учета СКЗИ вносится запись о выдаче ключа электронной подписи и соответствующего ему квалифицированного сертификата, с которой Заявитель должен быть ознакомлен под расписку.

4) Создание ключей электронной подписи Заявителя осуществляется с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

5) Удостоверяющий центр не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи Заявителя (Владельца КСКПЭП).

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

7) Владелец сертификата, получивший квалифицированный сертификат в Удостоверяющем центре обеспечивает конфиденциальность ключей электронных подписей и обязан:

- хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;
- не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;
- уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

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

6.6 Регистрация квалифицированного сертификата в единой системе идентификации и аутентификации

Удостоверяющий центр непосредственно после выдачи квалифицированного сертификата Владельцу КСКПЭП осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи».

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

6.7.1. При выдаче квалифицированного сертификата Удостоверяющий центр по желанию Владельца КСКПЭП безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации и (или) осуществляет подтверждение учетной записи физического лица в единой системе идентификации и аутентификации.

6.7.2. Основанием для регистрации или подтверждения учетной записи служит заявление Владельца КСКПЭП, содержащее сведения, необходимые для регистрации или подтверждения учетной записи в единой системе идентификации и аутентификации, а также согласие на обработку персональных данных, представляемое Владельцем КСКПЭП. Форма предоставляется путем представления заявления согласно Приложения №3 при выполнении процедуры регистрации Владельца КСКПЭП в единой системе идентификации и аутентификации или подтверждения его учетной записи, которая осуществляется Удостоверяющим центром при личном прибытии Владельца КСКПЭП в Удостоверяющий центр.

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

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

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

6.8.2. Актуальность и доступность реестра квалифицированных сертификатов, опубликованного на сайте Удостоверяющего центра в сети Интернет обеспечивается Удостоверяющим центром в соответствии с настоящим Порядком соответственно.

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

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

6.8.5. В целях обеспечения гарантированного доступа участников электронного взаимодействия к списку отозванных сертификатов Удостоверяющим центр обеспечивается

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

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

6.8.7. Внесение информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов осуществляется Удостоверяющим центром в соответствии с настоящим Порядком.

Приложение №1
Форма заявления на регистрацию и изготовление КСКПЭП для физических лиц

В Удостоверяющий центр АО «Тандер»

Заявление на регистрацию и изготовление квалифицированного сертификата ключа проверки электронной подписи физического лица

«____» _____ 20___.

Присоединяюсь к Регламенту Удостоверяющего центра (https://ca-magnit.ru/documentation/) в силу ст. 428 ГК РФ и прошу выдать квалифицированный сертификат ключа проверки электронной подписи (далее — КСКПЭП) в соответствии с указанными в настоящем заявлении данными:

Фамилия Имя Отчество (CommonName – CN)	
ИНН (INN)	
Страна (Country – C)	
Регион (State – S)	
Город (Locality – L)	
Фамилия (Surname – SN)	
Имя и отчество (GivenName – G)	
СНИЛС (SNILS)	
Адрес электронной почты (E-Mail – E)	

Настоящим _____паспорт _____выдан_____

фамилия, имя, отчество | серия, номер | дата выдачи

код подразделения / орган, выдавший документ

место рождения / дата рождения

- соглашается с обработкой своих персональных данных (в том числе с использованием технических средств) Удостоверяющим центром (далее — УЦ) и признает, что указанные в настоящем заявлении данные будут сохранены в реестре сертификатов. Обеспечение доступа любого лица к реестру сертификатов — обязанность УЦ в силу ч. 3 ст. 15 ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее — Закон).
- признает, что сведения о нем после получения КСКПЭП будут переданы в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч. 5 ст. 18 Закона.
- для своей идентификации указывает абонентский номер подвижной (мобильной) связи _____
- гарантирует своевременное письменное уведомление о смене указанного номера.

УЦ не несет ответственность за действия операторов информационных систем, которые привели к невозможности использования сертификатов в этих информационных системах.
Все поля обязательны для заполнения.

Субъект персональных данных
владелец сертификата _____ подпись, не факсимиле _____ расшифровка подписи

Приложение № 2
Руководство по обеспечению безопасности

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

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах Владельцу КСКПЭП необходимо выполнять требования:

- 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, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. N 152, в части обращения со средствами криптографической защиты информации;
- Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. N 66, в части эксплуатации средств криптографической защиты информации;
- эксплуатационной документации к средствам электронной подписи;
- приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Работа со средствами электронной подписи (ЭП)

2. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

2.1. Обеспечить конфиденциальность ключей электронных подписей.

2.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

2.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

2.4. Немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия (аннулирование) КСКПЭП владельца КСКПЭП в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

2.5. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на прекращение действия, которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

2.6. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

2.7 Сохранность носителей ключевой информации и других документов, выдаваемых с ключевыми носителями;

2.8 Сохранение в тайне пин – кодов для доступа к электронным ключам и средствам ЭП;

2.9 Обеспечение соответствующих условий хранения электронных ключей, исключающих возможность доступа к ним посторонних лиц, несанкционированного использования или копирования средств ЭП;

3. Порядок применения средств квалифицированной электронной подписи

3.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи, размещенной на сайте http://ca-magnit.ru/documentation/, либо на сайте производителя.

3.2 Для предотвращения заражения вредоносным программным обеспечением компьютера с установленными средствами квалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского, программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

3.3 В помещениях владельцев средств квалифицированной электронной подписи для хранения выданных им носителей ключей электронной подписи, эксплуатационной и технической документации,

инсталлирующих средства квалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих владельцев средств квалифицированной электронной подписи.

3.4 Заявителем Удостоверяющего центра соответствующими приказами должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации этих средств; средства квалифицированной ЭП и ключевые носители в соответствии с их серийными номерами должны быть взяты на поэкземплярный учет в выделенных для этих целей журналах.

4. Риски использования электронной подписи

При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

1) Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.

2) Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.

3) Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.

4) Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.

5) Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для снижения данных рисков или их избегания помимо определения порядка использования электронной подписи при электронном взаимодействии предусмотрен комплекс правовых и организационно-технических мер обеспечения информационной безопасности.

5. Компрометация ключа

Компрометация ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

1. Потеря ключевых носителей.
2. Потеря ключевых носителей с их последующим обнаружением.
3. Увольнение сотрудников, имевших доступ к ключевой информации.
4. Нарушение правил хранения и уничтожения (после окончания срока действия).
5. Возникновение подозрений на утечку информации или ее искажение.
6. Нарушение печати на сейфе с ключевыми носителями.
7. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника.

Различают два вида компрометации ключа ЭП: явную и неявную. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

6. Меры, необходимые для обеспечения безопасности электронных подписей и их проверки

1) Для хранения электронных ключей и средств ЭП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей (один у исполнителя, другой в службе безопасности).

2) Использовать автоматизированное рабочее место (АРМ) с установленными средствами ЭП необходимо в однопользовательском режиме. В отдельных случаях, при необходимости использования АРМ несколькими лицами, эти лица должны обладать равными правами доступа к информации.

3) При загрузке операционной системы и при возвращении после временного отсутствия пользователя на рабочем месте должен запрашиваться пароль, состоящий не менее чем из 6 символов. В отдельных случаях, при невозможности использования парольной защиты, допускается загрузка операционной системы (ОС) без запроса пароля. При этом должны быть реализованы дополнительные организационно – режимные меры, исключающие несанкционированный доступ к этим АРМ.

4) Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ с установленными средствами ЭП.

5) Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными средствами ЭП.

6) Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

7) Администрирование должно осуществляться доверенными лицами Владельца КСКПЭП.

8) Вхождение пользователей в режим конфигурирования BIOS штатными средствами BIOS должно осуществляться только с использованием парольной защиты при длине пароля не менее 6 символов.

9) После получения электронного ключа в точке выдачи АО «Тандер» рекомендуется произвести смену стандартного пин – кода электронного ключа на свой собственный. Длина пароля должна быть не менее 6 символов.

Приложение №3
Форма заявления на регистрацию Учетной записи в единой системе идентификации и аутентификации

В Удостоверяющий центр АО «Тандер»

Заявление
на выдачу ключа простой электронной подписи для получения государственных и муниципальных услуг в электронной форме

В соответствии с постановлением Правительства Российской Федерации от 25.01.2013 № 33 "Об использовании простой электронной подписи при оказании государственных и муниципальных услуг" прошу выдать мне ключ простой электронной подписи на основании следующих данных:

1. Фамилия Заявителя: _____
(в именительном падеже)
2. Имя: _____
(в именительном падеже)
3. Отчество: _____
(при наличии, в именительном падеже)
4. Пол: _____
(мужской / женский)
5. Дата рождения: _____
(в формате ДД.ММ.ГГГГ)
6. СНИЛС: _____

7. Гражданство: _____
(например, Россия)
8. Адрес электронной почты: _____
(при наличии)
9. Номер мобильного телефона: _____
(в формате +7(xxx)xxxxxxx)
10. Данные документа, удостоверяющего личность: _____
(наименование документа)
номер _____ выдан _____ _____
(серия и номер документа) (когда выдан) (код подразделения)

Пароль ключа простой электронной подписи прошу выдать мне следующим способом (отметить):
□ путем отправки электронного сообщения на указанный адрес электронной почты;
□ путем отправки SMS-сообщения на указанный номер мобильного телефона.

С Правилами использования простой электронной подписи при оказании государственных и муниципальных услуг, утвержденными постановлением Правительства Российской Федерации от 25.01.2013 № 33 ознакомлен.
Даю согласие на обработку содержащихся в настоящем заявлении персональных данных в заявленных целях, включая их сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение, а также передачу Оператору Федеральной государственной информационной системы "Единой системы идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".
Настоящее согласие дается до истечения сроков хранения соответствующей информации или документов, содержащих вышеуказанную информацию, определяемых в соответствии с законодательством Российской Федерации, после чего может быть отозвано путем направления соответствующего письменного уведомления не менее чем за три месяца до даты отзыва согласия.

Дата: _____ Подпись Заявителя: _____

Приложение №4
Форма заявления на прекращение действия (аннулирование) КСКПЭП

В Удостоверяющий центр АО «Тандер»

Заявление на прекращение действия (аннулирование) квалифицированного сертификата ключа проверки электронной подписи

«____» _____20___ г.

Я, _____
(Ф.И.О.)

прошу прекратить действие квалифицированного сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром АО «Тандер» (ИНН 2310031475), содержащего следующие данные:

Фамилия, имя и отчество	
ИНН	
СНИЛС	
Серийный номер	
Дата начала действия сертификата	
Дата окончания действия сертификата	

Основание прекращения действия квалифицированного сертификата:

_____
(причина аннулирования сертификата)

Владелец КСКПЭП _____ / _____/
(подпись) (расшифровка подписи)

Отметки Удостоверяющего центра АО «Тандер»_____

Аннулирование сертификата произведено. Информация об аннулированном сертификате внесена в список аннулированных сертификатов.

Сотрудник Удостоверяющего центра _____/ _____/
(подпись) (расшифровка подписи)

«____» _____20___ г.

Приложение №5
Форма заявления на проверку подлинности электронной подписи электронного документа

В Удостоверяющий центр АО «Тандер»

Заявление
на проверку подлинности электронной подписи в электронном документе

«___» _____20___ г.

Я, _____
(Ф.И.О.)

Прошу проверить подлинность электронной подписи электронного документа в соответствии со следующими идентификационными данными:

1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению носителе;
2. Файл, содержащий подписанные электронной подписью данные, на прилагаемом к заявлению носителе;
3. Серийный номер сертификата ключа проверки электронной подписи
_____
4. Время подписания электронной подписью электронного документа.
_____часов _____мин МСК «____» _____20___г.
5. Время, на момент наступления которых требуется проверить действительность электронной подписи в электронном документе (в том случае, если информация о дате и времени подписания электронного документа отсутствует).
_____часов _____мин МСК «____» _____20___г.

_____ / _____/
(подпись) (расшифровка подписи)