ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПРИКАЗ

от 13.09.2021 № 78-п

Об утверждении Порядка реализации функций аккредитованного регионального удостоверяющего центра Самарской области и исполнения его обязанностей и признании утратившими силу отдельных приказов департамента информационных технологий и связи Самарской области

В целях приведения нормативных правовых актов департамента информационных технологий и связи Самарской области в соответствие с действующим законодательством ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Порядок реализации функций аккредитованного регионального удостоверяющего центра Самарской области и исполнения его обязанностей.

2. Признать утратившими силу следующие приказы департамента информационных технологий и связи Самарской области:

от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей»;

от 20.06.2012 № 41-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и органов исполнительной власти Самарской области»;

от 30.12.2013 № 97-п «О внесении изменений в Приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и органов исполнительной власти Самарской области»;

от 12.05.2014 № 26-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и органов исполнительной власти Самарской области»;

от 10.03.2015 № 14-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей»;

от 18.12.2015 № 91-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей»;

пункт 1 приказа департамента информационных технологий и связи Самарской области от 16.03.2016 № 34-п «О внесении изменений в отдельные приказы департамента информационных технологий и связи Самарской области»;

от 21.06.2017 № 36-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п "Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей»;

от 28.10.2020 № 105-п «О внесении изменения в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей»;

от 10.11.2020 № 107-п «О внесении изменений в приказ департамента информационных технологий и связи Самарской области от 29.06.2011 № 54-п «Об утверждении Регламента взаимодействия регионального удостоверяющего центра Самарской области и его пользователей».

3. Опубликовать настоящий приказ в средствах массовой информации.

4. Настоящий приказ вступает в силу со дня его официального опубликования.

Заместитель председателя
Правительства Самарской области –
руководитель департамента
информационных технологий и связи
Самарской области К.Г.Пресняков

Батяшин 2215405

Ткаченко 2000125 (доб.230)

ПРИЛОЖЕНИЕ
к приказу департамента
информационных технологий и связи
Самарской области
от 13.09.2021 № 78-н

Порядок реализации функций аккредитованного регионального удостоверяющего центра Самарской области и исполнения его обязанностей

Термины и определения, используемые в настоящем Порядке

аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;

владелец сертификата ключа проверки электронной подписи (далее – владелец СКПЭП) – лицо, которому региональным удостоверяющим центром Самарской области в установленном порядке выдан сертификат ключа проверки электронной подписи;

валидность сертификата ключа проверки электронной подписи – положительный результат прохождения сертификатом ключа проверки электронной подписи всех операций проверки;

Головной УЦ (ГУЦ) – Федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи;

доверенное лицо – физическое лицо, уполномоченное на выполнение определенных действий в порядке, установленном гражданским законодательством Российской Федерации;

доступ – получение возможности ознакомления с информацией, результатами ее обработки и (или) воздействия на информацию на основе ресурсов автоматизированной информационной системы с использованием программных и (или) технических средств. Доступ осуществляется субъектами доступа, к которым относятся физические лица, а также логические и физические объекты;

заявитель – лицо, направляющее пакет документов в УЦ для получения услуг, определенных Порядком;

информация конфиденциального характера (конфиденциальная информация) – любая информация, доступ к которой ограничен, не содержащая сведений, относящихся к государственной тайне;

квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) – сертификат ключа проверки электронной подписи, выданный аккредитованным УЦ или доверенным лицом аккредитованного УЦ либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи;

ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания ЭП;

ключ проверки электронной подписи (ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП;

ключевой носитель (носитель ключа ЭП, носитель ключевой информации) – носитель информации, содержащий один или несколько ключей ЭП;

ключи (ключи ЭП) – совокупность ключа ЭП и соответствующего ему ключа проверки ЭП;

ключевая информация – специальным образом организованная совокупность ключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

компрометация ключа – утрата доверия к тому, что используемые ключи подписи не доступны посторонним лицам;

конфиденциальность информации (ресурсов автоматизированной информационной системы) – состояние информации (ресурсов автоматизированной информационной системы), при котором доступ к ней (к ним) осуществляют только субъекты, имеющие на него право;

ключевая фраза для удаленной аутентификации – секретное слово (последовательность символов), известное только пользователю УЦ и сотрудникам УЦ, исполняющим роль оператора (администратора), предназначенное для аутентификации пользователя;

плановая смена ключей – смена ключей с установленной в системе периодичностью, не вызванная компрометацией ключей;

пользователь УЦ – юридическое лицо или индивидуальный предприниматель, указанные в п. 1.4.1. настоящего Порядка, сотрудник органа, организации или индивидуального предпринимателя, указанных в п. 1.4.1. настоящего Порядка (далее – сотрудник органа, организации или ИП), физическое лицо, юридическое лицо или индивидуальный предприниматель, указанные в п.1.5.1. настоящего Порядка;

пользователь средства криптографической защиты информации – сотрудник, на рабочем месте которого установлено средство криптографической защиты информации;

проверка подлинности ЭП в электронном документе – положительный результат проверки средством ЭП с использованием сертификата ключа проверки электронной подписи принадлежности ЭП в электронном документе владельцу СКПЭП и отсутствия искажений в подписанном данной ЭП электронном документе;

проверка валидности сертификата ключа проверки электронной подписи – действия, производимые над проверяемым сертификатом ключа проверки электронной подписи для того, чтобы убедиться в возможности его использования. Проверка валидности включает в себя:

проверку целостности сертификата ключа проверки электронной

подписи;

проверку срока действия сертификата ключа проверки электронной подписи;

проверку отсутствия сертификата ключа проверки электронной подписи в актуальном списке отозванных сертификатов ключей подписей;

проверку области действия сертификата ключа проверки электронной подписи;

реестр пользователей УЦ – созданный УЦ список зарегистрированных пользователей, содержащий информацию о них;

реестр сертификатов ключей проверки электронных подписей УЦ – созданный УЦ список выданных сертификатов ключей проверки электронной подписи;

сертификат ключа проверки электронной подписи (сертификат ключа проверки ЭП) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

список отозванных сертификатов (COC, CRL) – электронный документ с ЭП уполномоченного лица УЦ, включающий в себя список серийных номеров сертификатов ключей проверки ЭП, которые на момент времени формирования списка отозванных сертификатов были отозваны или действие которых было приостановлено;

средства криптографической защиты информации (далее – СКЗИ) – средства шифрования, средства имитозащиты, средства ЭП, средства кодирования, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации);

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключей подписи и ключей проверки подписи;

участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы Самарской области, органы местного самоуправления Самарской области, иные учреждения и организации, а также граждане Самарской области;

УЦ – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключа проверки электронной подписи, а также иные функции;

уполномоченное лицо УЦ – администратор, оператор, а также иные сотрудники, назначенные правовым актом руководителя УЦ;

ЭП – информация в электронной форме, которая присоединена или иным образом связана с другой информацией в электронной форме (подписываемой информацией) и которая используется для определения лица, подписывающего информацию;

ЭП УЦ – квалифицированная ЭП аккредитованного УЦ;

сертификат ключа проверки ЭП УЦ – квалифицированный сертификат ключа проверки ЭП аккредитованного УЦ;

электронный документ – документ, в котором информация представлена в электронной форме.

CMS – стандарт криптографических защищенных сообщений.

1. Общие положения

1.1. Предмет регулирования Порядка.

Настоящий Порядок реализации функций аккредитованного регионального УЦ Самарской области и исполнения его обязанностей (далее – Порядок) разработан в соответствии с требованиями законодательства Российской Федерации, регулирующего отношения в области использования электронной подписи и требованиями к порядку реализации функций аккредитованного УЦ и исполнения его обязанностей, установленными приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 13.11.2020 № 584

1.1.1. Предметом регулирования настоящего Порядка являются условия предоставления услуг регионального УЦ Самарской области и порядок взаимодействия регионального УЦ Самарской области и пользователей регионального УЦ Самарской области.

1.1.2. Настоящий Порядок размещен для свободного доступа и ознакомления на сайте УЦ в сети интернет https://ruc.samregion.ru/.

1.2. Сведения об Удостоверяющем центре

Место нахождения УЦ: 443068, г. Самара, ул. Н.Панова, д. 16.

График работы УЦ:

понедельник-четверг с 9:00 до 18:00, пятница с 9:00 до 17:00

перерыв на обед с 13:00 до 13:48

выходные дни: суббота, воскресенье, а также дни государственных праздников России.

Тел. (846) 2000-933

Сайт https://ruc.samregion.ru/.

1.3. Порядок информирования о предоставлении услуг УЦ.

Информирование о предоставлении услуг УЦ осуществляется следующими способами:

- по единому справочному телефону: (846) 2000-933;
- путем направления уведомлений по адресу электронной почты: ruc@samregion.ru;
- путем опубликования информации на сайте УЦ в сети интернет: https://ruc.samregion.ru/.

1.4. Стоимость услуг УЦ.

1.4.1. Услуги УЦ предоставляются на безвозмездной основе следующим органам, организациям и индивидуальным предпринимателям, включая их сотрудников до 31.12.2021:

органам государственной власти Самарской области и подведомственным им учреждениям;

государственным органам Самарской области;

органам местного самоуправления Самарской области и подведомственным им учреждениям, использующим информационные системы и ресурсы, операторами которых являются органы государственной власти Самарской области и подведомственные им учреждения (далее – муниципальные органы);

федеральным органам исполнительной власти и их территориальным подразделениям, использующим информационные системы и ресурсы, операторами которых являются органы государственной власти Самарской области и подведомственные им учреждения (далее - федеральные органы);

иным учреждениям и организациям, индивидуальным предпринимателям, использующим информационные системы, операторами которых являются органы государственной власти Самарской области или подведомственные им учреждения, в целях обеспечения выполнения государственных функций органов государственной власти Самарской области (далее – иные учреждения, организации и ИП).

1.4.2. Услуги УЦ предоставляются на платной основе физическим лицам, юридическим лицам, независимо от организационно-правовой формы, и индивидуальным предпринимателям.

Стоимость услуг, вид и состав УЦ определены прайс-листом, который предоставлен на официальном сайте УЦ в сети Интернет (https://ruc.samregion.ru/).

Сроки и порядок расчетов за оказание платных услуг установлены положениями гражданского законодательства Российской Федерации и договором на оказание платных услуг, который предоставлен на официальном сайте УЦ в сети Интернет (https://ruc.samregion.ru/).

Не является публичной офертой.

1.4.3. Для оптимизации процесса работы УЦ перед визитом пользователь УЦ проходит процедуру предварительной записи. Предварительная запись на прием осуществляется по телефону (846) 2000-933.

В случае визита в УЦ без прохождения процедуры предварительной записи пользователь УЦ имеет право подать документы в порядке очередности либо записаться на свободное время.

2. Перечень функций (оказываемых услуг), реализуемых УЦ

2.1. УЦ осуществляет следующие функции (оказывает следующие услуги):

2.1.1. создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований,

установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

2.1.1.1. 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;

2.1.2. устанавливает сроки действия сертификатов ключей проверки электронных подписей;

2.1.3. аннулирует выданные этим УЦ сертификаты ключей проверки электронных подписей;

2.1.4. выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные УЦ) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

2.1.5. ведет реестр выданных и аннулированных этим УЦ сертификатов ключей проверки электронных, в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

2.1.6. 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»;

2.1.7. создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

2.1.8. проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

2.1.9. осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

2.1.10. предоставляет безвозмездно любому лицу по его обращению, в соответствии с установленным Порядком, доступ к информации, содержащейся в Реестре Сертификатов, в том числе информации об аннулировании Сертификата.

2.1.11. предоставляет пользователям УЦ Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, а также иных инструкций по работе со средствами криптографической защиты информации и информационной безопасности.

2.1.12. осуществляет иные, связанные с использованием электронной подписи функции, установленные законодательством Российской Федерации. Осуществляет иную связанную с использованием электронной подписи деятельность.

3. Права и обязанности УЦ

3.1. УЦ:

создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты лицам, обратившимся за их получением (заявителям), при условии установления личности получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата с учетом требований, установленных в соответствии с пунктом 4 части 4 статьи 8 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

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 этим удостоверяющим центром сертификаты ключей проверки электронных подписей;

выдает по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных этим удостоверяющим центром сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

устанавливает порядок ведения реестра сертификатов, не являющихся квалифицированными, и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

осуществляет иную связанную с использованием электронной подписи деятельность.

3.2. УЦ имеет право:

отказать пользователю УЦ в регистрации, получении ключей ЭП, изготовлении сертификата ключа проверки ЭП пользователя УЦ, аннулировании (отзыве) сертификата ключа проверки ЭП пользователя УЦ в случае ненадлежащего оформления документов, необходимых для совершения соответствующей процедуры (наличие ошибок, исправлений, подчисток и приписок);

аннулировать (отозвать) сертификат ключа проверки ЭП пользователя УЦ (сотрудника органа, организации или ИП) в случае его увольнения. Орган государственной власти Самарской области, подведомственное ему учреждение, муниципальный орган, федеральный орган, а также иное учреждение, организация или ИП, от имени которых был получен сертификат ключа проверки ЭП, обязаны уведомить УЦ об увольнении пользователя УЦ (сотрудника органа, организации или ИП) в течение 3 (трех) рабочих дней со дня его увольнения. Уведомление оформляется либо в виде письма на бумажном носителе или в электронном виде посредством автоматизированной информационной системы делопроизводства и документооборота Правительства Самарской области, либо в виде заявления на аннулирование поданного через портал https://lk-ruc.samregion.ru;

заключать соглашения с органами, организациями и ИП, указанными в 1.4.1 настоящего Порядка, а также физическими, юридическими лицами и индивидуальным предпринимателям, указанными в п. 1.4.2. настоящего Порядка, в части оказания услуг УЦ;

отказать пользователю УЦ в выдаче сертификата ключа проверки ЭП в случае, предусмотренном частью 2.3. статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3.3. УЦ обязан:

3.3.1. информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

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

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

3.3.4. обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей;

3.3.5. отказать заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения сертификата ключа проверки электронной подписи;

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

3.3.7. незамедлительно информировать владельца квалифицированного сертификата о выявленных случаях приостановления (прекращения) технической возможности использования ключа электронной подписи, не предусмотренных соглашением сторон, или возникновения у аккредитованного УЦ обоснованных сомнений в получении поручения от уполномоченного соглашением сторон лица об использовании ключа электронной подписи (при осуществлении аккредитованным удостоверяющим центром деятельности, предусмотренной частью 2.2 статьи 15 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»);

3.3.8. при выдаче квалифицированного сертификата аккредитованный УЦ направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате. Требования к порядку предоставления владельцам квалифицированных сертификатов сведений о выданных им квалифицированных сертификатах с использованием единого портала государственных и муниципальных услуг устанавливаются Правительством Российской Федерации. При выдаче квалифицированного сертификата аккредитованный УЦ по желанию владельца квалифицированного сертификата безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации с проведением идентификации владельца при его личном присутствии; 3.3.9. обеспечивать физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», для проведения идентификации физических лиц в УЦ на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети «Интернет»;

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

3.3.11. хранить следующую информацию в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации. Хранение информации должно осуществляться в форме, позволяющей проверить ее целостность и достоверность:

реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;

сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного

сертификата;

сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;

3.3.12. 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;

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

3.3.14. случае принятия решения о прекращении своей деятельности аккредитованный УЦ обязан:

в письменной форме уведомить пользователей УЦ не позднее чем за один месяц до даты прекращения своей деятельности;

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

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

передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре. Ключи электронной подписи, хранимые аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи, подлежат уничтожению в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности;

3.3.15. выполнять порядок реализации функций аккредитованного УЦ и исполнения его обязанностей, установленный таким аккредитованным удостоверяющим центром в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного УЦ и исполнения обязанностей, а также с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и

иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

3.3.16. при выдаче квалифицированного сертификата аккредитованный УЦ обязан:

в порядке, установленном Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата 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 № 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 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», УЦ обязан отказать такому лицу в проведении указанной идентификации.

Устанавливаются:

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

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

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

территории государства, в котором оно зарегистрировано;

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

3.3.18. в установленном порядке идентифицировать заявителя - физическое лицо, обратившееся к нему за получением квалифицированного сертификата (в целях получения от заявителя, выступающего от имени юридического лица, подтверждения правомочия обращаться за получением квалифицированного сертификата). Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата, информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и информации из единой биометрической системы в порядке, установленном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3.3.19. предложить использовать шифровальные (криптографические) средства, указанные в части 19 статьи 14.1 Федерального закона от 27.06.2006 № 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 УЦ обязан отказать такому лицу в проведении идентификации и выдаче сертификата ключа проверки электронной подписи.

При получении квалифицированного сертификата заявителем ознакомить с информацией, содержащейся в квалифицированном сертификате. Подтверждение ознакомления с информацией, содержащейся в

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

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

4. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг УЦ, в том числе требования к документам, предоставляемых в УЦ в рамках предоставления услуг

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

4.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей.

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

Пользователь УЦ 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. № 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 № 6382), с изменениями, внесенными приказом ФСБ России 12 апреля 2010 г. № 173 «О внесении изменений в некоторые нормативные правовые акты ФСБ России» (зарегистрирован Министерством юстиции Российской Федерации 25 мая 2010 г., регистрационный № 17350);

УЦ 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. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона от 06.04.2011 № 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 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) в отношении автоматизированного рабочего места УЦ, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя.

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

Плановая смена ключей ЭП и сертификата ключа проверки ЭП производиться в период действия ключа ЭП УЦ. Плановая смена ключей ЭП производится по следующим основаниям:

истечение срока действия квалифицированного сертификата;

переход на использование новых стандартов электронной подписи и функции хеширования в соответствии с требованиями, установленными органом исполнительной власти, уполномоченного в сфере использования электронной подписи.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

УЦ создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;

УЦ изготавливает новый сертификат ключа проверки электронной подписи Уполномоченного лица УЦ. При плановой замене ключа электронной подписи УЦ все владельцы электронных подписей должны установить на своих автоматизированных рабочих местах новый сертификат УЦ.

Старый ключ ЭП не изымается из обращения до тех пор, пока не истекут сроки действия всех сертификатов ключей проверки ЭП, выданных с его использованием, и применяется для формирования списков отозванных

сертификатов в электронной форме, изданных УЦ в период действия старого ключа проверки ЭП УЦ.

Информирование пользователей УЦ о проведении плановой смены ключей уполномоченного лица УЦ осуществляется посредством публикации информации на официальном сайте УЦ по адресу: https://ruc.samregion.ru/.

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: https://ruc.samregion.ru/reestr, доступная для скачивания.

4.1.3. Порядок осуществления смены ключей электронной подписи УЦ в случаях нарушения их конфиденциальности.

Смена ключа электронной подписи УЦ осуществляется в случае нарушения конфиденциальности ключа электронной подписи или угрозы нарушения конфиденциальности такого ключа электронной подписи, а также указание на то, что одновременно со сменой такого ключа электронной подписи прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов.

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

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

В случае компрометации ключа электронной подписи УЦ сертификат ключа проверки электронной подписи УЦ аннулируется, пользователи УЦ уведомляются об указанном факте путем публикации информации о компрометации на сайте УЦ в сети Интернет по адресу: https://ruc.samregion.ru/.

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

Доверенным способом получения нового квалифицированного сертификата УЦ является его публикация на официальном сайте УЦ по адресу: https://ruc.samregion.ru/reestr, доступная для скачивания.

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

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

угрозы, реализуемые по локальной сети: осуществление доступа к файлам базы данных путем использования неправомерно полученных аутентификационных данных для подключения с помощью средств удаленного

доступа, функционирующих на сервере баз данных;

угрозы, связанные с непосредственным доступом: хищение сетевого оборудования, линий связи;

непреднамеренно реализуемые угрозы: нарушение функционирования локальной сети, влекущее недоступность сервера баз данных, вызванное сбоем в функционировании сетевого оборудования, повреждение линии связи или отказом (сбоем) сетевых служб;

физическая утрата носителя ключа электронной подписи УЦ, в том числе в случае хищения или иного злонамеренного действия злоумышленника;

несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение пломб и устройств контроля входа в помещение, повреждение замков и т. п.;

иные случаи компрометации.

4.1.4. Порядок осуществления УЦ смены ключей ЭП и сертификата ключа проверки ЭП владельца квалифицированного сертификата.

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

в связи с истечением установленного срока его действия;

на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

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

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

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

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

Процедура выдачи квалифицированного сертификата и ключа

электронной подписи (при необходимости) владельцу, в том числе в электронной форме осуществляется в соответствии с требованиями, установленными статьей 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и настоящим Порядком.

4.2. Процедура создания и выдачи квалифицированных сертификатов.

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

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

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

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

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

4.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов и перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата, в том числе для удостоверения личности заявителя

4.2.2.1. Заявление на изготовление ключа электронной подписи и сертификата ключа проверки электронной подписи сотрудника в УЦ (приложение № 1), заявление на изготовление ключа электронной подписи и сертификата ключа проверки электронной подписи юридического лица в УЦ (приложение № 6), заявление на изготовление ключа проверки электронной подписи и сертификата ключа проверки электронной подписи физического лица (приложение № 12) заполняются:

на бумажном носителе при помощи средств электронно-вычислительной техники или от руки разборчиво (печатными буквами) чернилами черного или синего цвета;

в электронной форме с использованием портала https://lk-ruc.samregion.ru и подписываются ЭП.

Заявление на изготовление ключа электронной подписи и сертификата ключа проверки электронной подписи сотрудника в УЦ (приложение № 1) и заявление на изготовление ключа проверки электронной подписи и сертификата ключа проверки электронной подписи физического лица (приложение № 12) подаются на бумажном носителе при личном прибытии сотрудника или физического лица в УЦ или в электронной форме с использованием портала https://lk-ruc.samregion.ru.

Заявление на изготовление ключа электронной подписи и сертификата

ключа проверки электронной подписи юридического лица в УЦ (приложение № 6) подается на бумажном носителе при личном прибытии руководителя учреждения или доверенного лица при наличии доверенности, оформленной согласно приложению № 2 к настоящему Порядку, в УЦ или в электронной форме с использованием портала https://lk-ruc.samregion.ru.

Все документы, предоставляемые в УЦ на бумажном носителе, должны быть подписаны подписью руководителя организации либо лиц, наделенными полномочиями, достаточными для подписания такого рода документов, а также печатью организации (при наличии).

Все документы, предоставляемые в УЦ в электронной форме, должны быть подписаны ЭП владельца ЭП и ЭП руководителя организации либо лиц, наделенных полномочиями, достаточными для подписания такого рода документов. В случае если у владельца ЭП или руководителя учреждения нет действующей ЭП, то с использованием портала https://lk-ruc.samregion.ru документы могут быть направлены на проверку без ЭП. После подтверждения корректности документов пользователь обязан предоставить в УЦ данные документы на бумажном носителе с подписью руководителя и печатью организации (при наличии).

Все документы, предоставляемые в УЦ, физическим лицом подписываются им лично.

4.2.2.2. Регистрация сотрудника органа, организации или ИП и изготовление ключей ЭП и сертификата ключа проверки ЭП для него осуществляются при наличии подписанного соглашения о присоединении к порядку взаимодействия регионального УЦ Самарской области и его пользователей (Приложение № 10) на основании следующих документов:

заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре (приложение № 1);

согласия на обработку персональных данных (приложение № 11);

При подаче заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре пользователь УЦ представляет следующие документы либо их заверенные копии и сведения:

основной документ, удостоверяющий личность сотрудника органа, организации или ИП;

номер страхового свидетельства государственного пенсионного страхования сотрудника органа, организации или ИП;

основной государственный регистрационный номер юридического лица, сотрудником которого является лицо, подлежащее регистрации, или основной государственный регистрационный номер записи о государственной регистрации физического лица в качестве индивидуального предпринимателя, сотрудником которого является лицо, подлежащее регистрации.

Пользователь УЦ вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в абзаце 2 настоящего пункта.

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

В случае подачи заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре сотрудниками иных учреждений, организаций или ИП необходимо также наличие согласования оператора информационной системы, в которой будут применяться изготовленные ключи ЭП и сертификат ключа проверки ЭП. Указанное согласование оформляется путем заполнения раздела «Согласование выдачи ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем центре» заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре (приложение № 1) с подписью представителя оператора информационной системы, заверенной печатью оператора информационной системы.

4.2.2.3. Регистрация юридического лица (индивидуального предпринимателя) и изготовление ключей ЭП и сертификата ключа проверки ЭП для него осуществляются при наличии подписанного соглашения о присоединении порядку взаимодействия регионального УЦ Самарской области и его пользователей (приложение № 10) на основании следующих документов:

заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица (индивидуального предпринимателя) в Удостоверяющем Центре (приложение № 6);

доверенности (приложение № 2). В случае подачи заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющем Центре заявителем, действующим от имени юридического лица на основании учредительных документов юридического лица, указанное лицо вправе предоставлять вместо доверенности заверенные копии учредительных документов юридического лица.

При подаче заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющий Центр заявитель представляет следующие документы либо их заверенные копии и сведения:

основной документ, удостоверяющий личность доверенного лица;

основной государственный регистрационный номер юридического лица.

Заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в абзаце 3 настоящей пункта.

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

В случае подачи заявления на изготовление ключей электронной подписи

и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющем Центре иными учреждениями и организациями необходимо также наличие согласования оператора информационной системы, в которой будут применяться изготовленные ключи ЭП и сертификат ключа проверки ЭП. Указанное согласование оформляется путем заполнения раздела «Согласование выдачи ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющем Центре» заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющем центре (приложение № 6) с подписью представителя оператора информационной системы, заверенной печатью оператора информационной системы.

4.2.2.4. Регистрация физического лица и изготовление ключей ЭП и сертификата ключа проверки ЭП для него осуществляются при наличии подписанного соглашения о присоединении порядку взаимодействия регионального УЦ Самарской области и его пользователей (приложение № 10) на основании следующих документов:

заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи физического лица в Удостоверяющем Центре (приложение № 12);

согласия на обработку персональных данных (приложение № 11).

При подаче заявления на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре пользователь УЦ представляет следующие документы либо их заверенные копии и сведения:

основной документ, удостоверяющий личность физического лица;

номер страхового свидетельства государственного пенсионного страхования физического лица;

идентификационный номер налогоплательщика физического лица.

Пользователь УЦ вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в абзаце 2 настоящего пункта.

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

4.2.3. Порядок идентификации пользователя УЦ

4.2.3.1. Идентификация гражданина Российской Федерации осуществляется:

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

2) без его личного присутствия:

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

путем предоставления информации, указанной в документе,

удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные. Реализация данного способа осуществляется с учетом требований постановления Правительства Российской Федерации от 8 ноября 2019 г. № 1427 «О проведении эксперимента по совершенствованию применения технологии электронной подписи» (Собрание законодательства Российской Федерации, 2019, № 46, ст. 6493);

путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2020, № 14, ст. 2035).

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

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

4.2.3.2. Удаленная аутентификация пользователя УЦ предназначена для идентификации пользователя УЦ посредством телефонной связи для оказания технической поддержки. Удаленная аутентификация пользователя УЦ выполняется по ключевой фразе для удаленной аутентификации.

4.2.4. Порядок проверки достоверности документов и сведений, предоставленных пользователем УЦ.

Для заполнения квалифицированного сертификата в соответствии с частью 2 статьи 17 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» УЦ 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 квалифицированный сертификат, и УЦ идентифицировал заявителя - физическое лицо или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, УЦ осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В ином случае УЦ отказывает заявителю в выдаче квалифицированного сертификата.

В случае отказа в регистрации пользователь УЦ имеет право забрать заявление вместе с приложениями.

4.2.5. Порядок создания квалифицированного сертификата.

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

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

факт принадлежности документов предоставившему их лицу и/или лицу, чти интересы оно предоставляет;

факт соответствия сведений, указанных в Заявлении на создание квалифицированного сертификата ключа проверки электронной подписи предоставленным документам и сведениям, а также полученным сведениям из государственных информационных ресурсов;

факт отсутствия явных признаков подделки документов.

В случае внесения в квалифицированный сертификат ключа проверки электронной подписи персональных данных физического лица, заявитель – физическое лицо или уполномоченный представитель заявителя-юридического лица предоставляет свое письменное согласие на обработку персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

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

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

4.2.5.2. Подача документов при личном посещении УЦ.

Порядок создания квалифицированного сертификата в случае подачи комплекта документов на бумажном носителе включает в себя следующие этапы:

- Получение от пользователя УЦ документов, указанных в пунктах 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4 настоящего Порядка.
- Проверка предоставленных документов.

- Проверка достоверности сведений, указанных в заявлении, с использованием системы межведомственного взаимодействия в соответствии с требованиями пункта 2.2 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

- Проверка носителя ЭП, допустимого эксплуатационной документацией к СКЗИ, при необходимости инициализация носителя.

- Формирование запроса на создание ключа ЭП и сертификата ключа проверки ЭП в случае подтверждения сведений и корректности документов. Оформление уведомления об отказе в изготовлении сертификата ключа проверки ЭП в случае выявления ошибок в оформлении документов, предоставления ошибочных данных, получения отрицательного результата проверки с использованием системы межведомственного взаимодействия предоставленных данных.

- Выпуск сертификата ключа проверки ЭП.

- Направление сведения о сертификате ключа проверки ЭП и лице, его получившем, в единую систему идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

- Внесение информации о выпущенном сертификате ключа ЭП и сертификата ключа проверки ЭП и ключевых носителях в журнал поэкземплярного учета ключевых документов.

- Ознакомление пользователя УЦ со сведениями, содержащимися в сертификате.

- Передача пользователю УЦ носителя ЭП под роспись в журнале поэкземплярного учета ключевых документов.

- Выдача руководства по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи (приложение № 7) под роспись в соответствующем журнале.

Срок действия ключа ЭП пользователя УЦ составляет 1 год.

4.2.5.3. Подача документов через портал https://lk-ruc.samregion.ru.

Порядок создания квалифицированного сертификата в случае подачи комплекта документов через портал https://lk-ruc.samregion.ru включает в себя следующие этапы:

- Получение от пользователя УЦ документы, подписанные ЭП, указанные в пунктах 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4 настоящего Порядка.

- Проверка предоставленных документов и запроса на сертификат.

- Проверка достоверности сведений, указанных в заявлении, с использованием системы межведомственного взаимодействия в соответствии с требованиями пункта 2.2. статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

- Формирование запроса на создание ключа ЭП и сертификата ключа проверки ЭП в случае подтверждения сведений и корректности документов. Оформление уведомления об отказе в изготовлении сертификата ключа проверки ЭП в случае выявления ошибок в оформлении документов,

предоставления ошибочных данных, получения отрицательного результата проверки с использованием системы межведомственного взаимодействия предоставленных данных.

- Направление сведения о сертификате ключа проверки ЭП и лице, его получившем, в единую систему идентификации и аутентификации в соответствии с частью 5 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

- Внесение информации о выпущенном сертификате ключа ЭП и сертификата ключа проверки ЭП в электронный журнал поэкземплярного учета ключевых документов.

- Направление сертификата ключа проверки ЭП и руководства по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи (приложение № 7) пользователю в его личный кабинет.

- Ознакомление пользователя УЦ со сведениями, содержащимися в сертификате.

Срок действия ключа ЭП пользователя УЦ составляет 1 год.

4.2.6. Порядок выдачи квалифицированного сертификата

4.2.6.1. По окончании процедуры изготовления ключей ЭП и сертификата ключа проверки ЭП УЦ под расписку знакомит заявителя с информацией, внесенной в квалифицированный сертификат, и выдает пользователю УЦ в случае подачи документов на бумажном носителе:

ключи ЭП, записанные на ключевой носитель;

сертификат ключа проверки ЭП в электронной форме, соответствующий ключу проверки ЭП;

сертификат ключа проверки ЭП на бумажном носителе; памятка пользователя УЦ (приложение № 3) с ключевой фразой для удаленной аутентификации;

руководство по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи (приложение № 7). Факт выдачи руководства по обеспечению информационной безопасности использования ЭП и средств ЭП фиксируется в соответствующем журнале под роспись пользователя УЦ.

4.2.6.2. По окончании процедуры изготовления ключей ЭП и сертификатов ключей проверки ЭП в случае подачи через портал https://lk-ruc.samregion.ru УЦ под расписку знакомит заявителя с информацией, внесенной в квалифицированный сертификат, и выдает пользователю УЦ:

сертификат ключа проверки ЭП в электронной форме, соответствующий ключу проверки ЭП;

руководство по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи (приложение № 7). Факт выдачи руководства по обеспечению информационной безопасности использования ЭП и средств ЭП фиксируется в соответствующем журнале в электронном виде.

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

4.2.7. Срок создания и выдачи квалифицированного сертификата с момента получения УЦ соответствующего заявления.

Срок создания квалифицированного сертификата осуществляется в течение шести рабочих дней с даты приема документов и сведений. Срок создания квалифицированного сертификата увеличивается в случае несвоевременного получения сведений, находящихся в распоряжении государственных органов, иных органов, необходимых для создания сертификата, о чем пользователь информируется.

Срочное создание квалифицированного сертификата не предусмотрено.

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

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

Подтверждение действительности электронной подписи, использованной для подписания электронных документов осуществляется на основании Заявления на подтверждение действительности электронной подписи, использованной для подписания электронных документов, составленного в соответствии с подписанным заявлением, утвержденным приложением № 4.

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

Обязательным приложением к заявлению на подтверждение подлинности

электронной подписи в электронном документе является предоставление информации, содержащей:

сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить подтверждение подлинности электронной подписи в электронном документе – в виде файла стандарта CMS;

электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

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

Срок проведения экспертизы по подтверждению действительности электронной подписи в электронном документе составляет 10 (десять) рабочих дней с даты получения Удостоверяющим центром Заявления на подтверждение действительности электронной подписи, использованной для подписания электронных документов.

4.3.3. Порядок оказания услуги.

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

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

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

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

Заключение содержит:

состав комиссии, осуществлявшей проверку;

основание для проведения проверки;

результат проверки электронной подписи электронного документа;

данные, представленные комиссии для проведения проверки.

отчет по выполненной проверке.

отчет по выполненной проверке содержит:

время и место проведения проверки;

содержание и результаты проверки;

обоснование результатов проверки.

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

При проведении работ УЦ может быть запрошена дополнительная информация.

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

4.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата.

Сертификат ключа проверки электронной подписи прекращает свое действие:

в связи с истечением установленного срока его действия;

на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;

в случае прекращения деятельности УЦ без перехода его функций другим лицам;

в иных случаях, установленных Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

УЦ аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

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

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

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

4.4.2. Порядок действий УЦ при прекращении действия (аннулировании) квалифицированного сертификата

Заявление на аннулирование сертификата ключа проверки электронной подписи подается пользователем УЦ в УЦ по форме, установленной приложениями № 5, 8 и 13 к настоящему Порядку.

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

электронного документа, подписанного квалифицированной электронной подписью заявителя.

При приеме Заявления аннулирование сертификата ключа проверки электронной подписи УЦ должен подтвердить полномочия владельца электронной подписи.

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

4.4.3. УЦ обязан аннулировать (отозвать) действие сертификата ключа проверки ЭП сотрудника органа, организации или ИП, юридического лица, по заявлению его владельца (приложение № 5) за исключением случаев, предусмотренных пунктом 3.2. Порядка, аннулировать (отозвать) действие сертификата ключа проверки ЭП юридического лица на основании заявления (Приложение № 8),поданного руководителем организации или доверенным лицом с надлежащим образом оформленной доверенностью (приложение № 2), аннулировать (отозвать) действие сертификата ключа проверки ЭП физического лица по заявлению его владельца (Приложение № 13)

Заявление подается в УЦ либо письменном виде, либо через портал https://lk-ruc.samregion.ru.

4.4.4. Заявление подается в электронном виде через портал https://lk-ruc.samregion.ru либо заполняется при помощи средств электронно-вычислительной техники или от руки разборчиво (печатными буквами) чернилами черного или синего цвета и подается руководителем организации в УЦ лично либо доверенным лицом при наличии надлежащим образом оформленной доверенности и представляет собой документ на бумажном носителе, заверенный собственноручной подписью руководителя организации и печатью (при наличии), а также носитель, содержащий сертификат ключа проверки ЭП, соответствующий заявлению.

4.4.5. Срок рассмотрения заявления составляет 1 рабочий день с момента его поступления в УЦ.

4.4.6. Срок внесения информации об аннулировании сертификата в реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

4.5. Порядок ведения реестра квалифицированных сертификатов.

4.5.1. Формы ведения реестра квалифицированных сертификатов.

Реестр квалифицированных сертификатов ключей проверки ЭП ведется в электронной форме.

Ведение реестра квалифицированных сертификатов включает в себя:

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

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

сертификатов.

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

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

УЦ обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

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

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

Для предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре, формируется его резервная копия.

4.5.2. Сроки внесения информации о прекращении действия или аннулирования квалифицированного сертификата в реестр квалифицированных сертификатов.

Сведения о прекращении действия квалифицированного сертификата вносятся аккредитованным удостоверяющим центром в реестр квалифицированных сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в части 6 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи в реестр квалифицированных сертификатов.

Сведения об аннулировании квалифицированного сертификата вносятся аккредитованным удостоверяющим центром в течение одного рабочего дня со дня вступления в законную силу решения суда, явившегося основанием для аннулирования, а также при аннулировании аккредитованным удостоверяющим центром сертификатов ключей проверки электронной подписи по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Квалифицированный сертификат считается аннулированным с момента внесения указанной записи в реестр квалифицированных сертификатов.

До внесения в реестр квалифицированных сертификатов сведений об аннулировании квалифицированного сертификата аккредитованный УЦ обязан уведомить владельца квалифицированного сертификата об аннулировании его квалифицированного сертификата путем направления документа на бумажном

носителе или электронного документа.

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

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

4.6. Порядок технического обслуживания реестра квалифицированных сертификатов.

4.6.1. Максимальные сроки проведения технического обслуживанию

Плановое и внеплановое техническое обслуживание Реестра квалифицированных сертификатов осуществляется во внерабочее время УЦ и не может превышать двенадцати часов.

4.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

УЦ оповещает лиц, использующих Реестр квалифицированных сертификатов, о проведении планового или внепланового технического обслуживания Реестра квалифицированных сертификатов на официальном сайте УЦ в сети Интернет: https://ruc.samregion.ru/.

5. Порядок исполнения обязанностей УЦ

5.1. Информирование пользователей УЦ 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.

Данная обязанность реализуется посредством предоставления пользователю УЦ, одновременно с выдачей ЭП, Руководства по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи (приложение № 7).

5.2. Выдача по обращению пользователя УЦ средств электронной подписи.

УЦ обязан обеспечивать физических лиц шифровальными (криптографическими) средствами, указанными в части 19 статьи 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», для проведения идентификации физических лиц в УЦ на основе предоставления биометрических персональных данных без личного присутствия посредством информационно-телекоммуникационной сети «Интернет».

Выдаваемые средства электронной подписи должны в соответствии с частью 4 статьи 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об

электронной подписи» обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

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

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

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

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

своевременным обнаружением фактов несанкционированного доступа к информации;

предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможностью незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянным контролем за обеспечением уровня защищенности информации;

нахождением баз данных информации в контролируемой зоне, исключающей свободное пребывание посторонних лиц;

использованием средств защиты информации, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

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

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

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

Доступ заинтересованных лиц к реестру квалифицированных сертификатов с использованием информационно-телекоммуникационных сетей осуществляется путем размещения, формирования и ведения реестра квалифицированных сертификатов в информационной системе головного УЦ, являющейся составной частью инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Доступ заинтересованных лиц к информационной системе головного УЦ с целью получения сведений из реестра квалифицированных сертификатов осуществляется с использованием федеральной государственной информационной системы "Единый портал государственных и муниципальных услуг (функций)" на безвозмездной основе.

УЦ обеспечивает доступность реестра квалифицированных сертификатов круглосуточно, с использованием информационно-телекоммуникационных сетей к выданным УЦ квалифицированным с сертификатами (https://ruc.samregion.ru/node/124), за исключением периодов планового или внепланового технического обслуживания реестра сертификатов.

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

5.5.1. Требования к обеспечению конфиденциальности.

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

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

Для создания ключа электронной подписи в УЦ используются средства электронной подписи, имеющие подтверждение соответствия требованиям,

установленным в соответствии с Федеральным законом №63-ФЗ «Об электронной подписи».

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

Запрещается:

оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, средства квалифицированной ЭП, после ввода ключевой информации;

вносить какие-либо изменения в программное обеспечение СКЗИ;

осуществлять несанкционированное копирование ключевых носителей;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;

использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;

записывать на ключевые носители постороннюю информацию;

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

оставлять без присмотра ключи ЭП на ключевом носителе;

применять ключ ЭП при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

5.5.2. Условия временного хранения ключей электронной подписи.

При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям не допущенных к ним лиц. Владелец несет персональную ответственность за хранение личных ключевых носителей.

Запрещается оставлять без контроля вычислительные средства с установленными СКЗИ после ввода ключевой информации.

В случае централизованного хранения ключевых носителей в организации, эксплуатирующей СКЗИ, администратор безопасности несет персональную ответственность за хранение личных ключевых носителей.

5.5.3. Сроки уничтожения ключей электронной подписи.

Ключи на ключевых носителях, в том числе срок действия которых истек, уничтожается путем переформатирования ключевых носителей средствами СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации. Срок уничтожения составляет один день с момента предоставления ключевого носителя в УЦ.

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

При выдачи квалифицированного сертификата аккредитованный УЦ направляет в единую систему идентификации и аутентификации сведения о

лице, получившем квалифицированный сертификата, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного УЦ).

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

При выдаче квалифицированного сертификата аккредитованный УЦ по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

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

Информация, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата предоставляется безвозмездно. Доступ к реестру квалифицированных сертификатов предоставляется круглосуточно через форму на сайте УЦ https://ruc.samregion.ru/node/124 или через личный кабинет на портале https://lk-ruc.samregion.ru, за исключением периодов планового или внепланового технического обслуживания реестра. Доступ к информации организован в соответствии с защитой персональных данных согласно требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данным» и предоставляется при условии владения необходимыми данными из сертификата.

Для получения информации о выданном или аннулированном сертификате юридического лица необходимо предоставить один из параметров:

Номер сертификата;
Название организации;
ИНН организации;
ОГРН организации;
Дата выпуска сертификата;
Дата окончания срока действия сертификата.

Для получения информации о выданном или аннулированном сертификате физического лица необходимо предоставить один из параметров:

Номер сертификата;
ФИО;
СНИЛС;
ИНН;

Дата выпуска сертификата;
Дата окончания срока действия сертификата.

Приложение № 1
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____
(фамилия, имя, отчество)
действующего на основании _____
доверяет выступать в качестве владельца сертификата ключа проверки электронной подписи
_____ и просит:
(фамилия, имя, отчество сотрудника юридического лица или ИП)

☐ зарегистрировать уполномоченного представителя в Реестре Удостоверяющего Центра, наделить полномочиями Пользователя Удостоверяющего Центра, установленными Порядком Удостоверяющего Центра;

☐ сформировать ключи электронной подписи (далее - ЭП) и изготовить сертификат ключа проверки ЭП сотрудника органа, организации или ИП в Удостоверяющем Центре;

в соответствии с указанными в настоящем заявлении идентификационными данными и областями применения сертификата ключа

Фамилия, имя, отчество	
Должность	
СНИЛС пользователя УЦ	
Адрес электронной почты пользователя УЦ	
Организация*	
ИНН организации	
ОГРН/ОГРНИП	
Наименование подразделения	
Адрес местонахождения организации согласно выписки из ЕГРЮЛ/ЕГРИП	
Страна	RU
Регион	
Область применения сертификата, дополнительные объектные идентификаторы (при необходимости)**	

* - полное или сокращенное наименование согласно положению (уставу), не более 64 знаков

** - может требоваться подтверждение полномочия на получения данного объектного идентификатора

зарегистрировать квалифицированный сертификат ключа проверки ЭП в ЕСИА во исполнение требований ч. 5 ст. 18 Федерального закона № 63-ФЗ "Об электронной подписи" в соответствии со следующими дополнительными данными:

Основной документ, удостоверяющий личность	Серия		Номер		Дата выдачи	
Дата рождения						
Пол	☐ Мужской				☐ Женский	
Гражданство						

Криптопровайдер (отметьте используемый): ☐ КриптоПро ☐ ViPNet

Носитель ЭП (не более одного):

☐ Рутокен ☐ iPad ☐ JaCarta ☐ СЭП КриптоПро DSS ☐ _____

Настоящим Пользователь Удостоверяющего Центра подтверждает, что ознакомлен с руководством по обеспечению безопасности использования ЭП и средств ЭП (Приложение № 7 к Порядку Удостоверяющего Центра)

Пользователь Удостоверяющего Центра _____ _____
(подпись) (Фамилия И.О.)
"__" _____ 20___ года

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)
"__" _____ 20___ года
М.П. (при наличии)

Согласование выдачи ключей электронной подписи и сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем центре (страница печатается и заполняется на обратной стороне заявления в случае получения ключей электронной подписи и сертификата ключа проверки электронной подписи в Удостоверяющем центре иными учреждениями, организациями и индивидуальными предпринимателями, использующими информационные системы, операторами которых являются органы государственной власти Самарской области или подведомственные им учреждения, в целях обеспечения выполнения государственных функций органов государственной власти Самарской области)

Оператор информационной системы:

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

_____
(фамилия, имя, отчество)

действующий на основании _____

Согласовал выдачу ключей ЭП для работы в следующих информационных системах:	

_____

(должность представителя Оператора информационной системы) (подпись) (Фамилия И.О.)

"___" _____ 20____ года

М.П.

Приложение № 2
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Доверенность

Город _____ _____
(дата прописью)
_____
(полное наименование организации, включая организационно-правовую форму/индивидуального предпринимателя)
в лице _____
(должность)
_____,
(фамилия, имя, отчество)
действующего на основании_____,
уполномочивает _____
(фамилия, имя, отчество)
паспорт серии _____ № _____ выдан "___" _____ 20____ года
_____
(наименование органа, выдавшего документ)

1. Представить в Удостоверяющий Центр необходимые документы, содержащие достоверные данные, определенные Порядком Удостоверяющего Центра, для изготовления ключей электронной подписи (далее - ЭП) и сертификата ключа проверки ЭП юридического лица/аннулирования (отзыва)юридического лица (пользователя)
_____
(фамилия, имя, отчество сотрудника органа, организации или ИП/
2. Получить ключевую информацию/идентификационные данные для доступа к ключевой информации, сертификат ключа проверки ЭП юридического лица, а также иные документы, определенные Порядком Удостоверяющего Центра.
3. Представить в УЦ ключевую информацию, сертификат ключа проверки ЭП Пользователя УЦ, а также иные документы, определенные Порядком Удостоверяющего Центра для аннулирования (отзыва)/сертификата ключа проверки ЭП.
4. Доверенное лицо наделяется правом расписываться на копии сертификата ключа проверки ЭП на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по "___"_____ 20__ года и дана без права передоверия

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

Руководитель _____ _____ _____
(должность) (подпись) (Фамилия И.О.)

"___" _____ 20___ года
М.П.

_____
(заполняет физическое лицо - доверенное лицо организации)

Настоящим я, _____,
(фамилия, имя, отчество полностью)
_____,
(адрес регистрации)

соглашаюсь с обработкой (сбор, систематизация, накопление, хранение, изменение, использование, обезличивание, блокирование, уничтожение) моих персональных данных (ПДн) ГБУ СО "Цифровой регион" (адрес: 443068, г. Самара, ул. Николая Панова, д. 16) согласно Порядку Удостоверяющего Центра и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцем которых я являюсь, относятся к общедоступному источнику персональных данных. Удостоверяю, что ПДн были предоставлены мною лично, даю свое согласие на архивное хранение (в течение срока деятельности УЦ) с целью исполнения требований ФЗ № 63-ФЗ от 6 апреля 2011 г. «Об электронной подписи».

Подпись _____ Дата _____

Приложение № 3
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Памятка

пользователя Удостоверяющего центра

Владелец сертификата ключа проверки электронной подписи:
Фамилия Имя Отчество
Наименование организации
Подразделение
Должность
Серийный номер сертификата ключа проверки электронной подписи:
Серийный номер
Наименование криптопровайдера:
Наименование криптопровайдера
Пароль носителя:
Пароль
Ключевая фраза для удаленной аутентификации <*>:
Фраза
Оператор УЦ _____ Фамилия И.О. Дата
Телефон службы технической поддержки: (846) 2000-933

<*> Удаленная аутентификация зарегистрированного пользователя УЦ предназначена для установления личности зарегистрированного пользователя УЦ по телефону. Лицо, проходящее данную процедуру, должно сообщить свои идентификационные данные и по запросу сотрудника УЦ, назвать ключевую фразу для удаленной аутентификации.

При компрометации ключа ЭП (потеря носителей ключевой информации, потеря носителей ключевой информации с их последующим обнаружением; носители ключевой информации стали на время доступными постороннему лицу без контроля со стороны владельца или ответственного за хранение ключевой информации; увольнение работников, имевших доступ к ключевой информации, или их перевод на другой участок работы) пользователь немедленно прекращает использование соответствующего ключа ЭП и уведомляет об этом сотрудника УЦ и иных участников электронного взаимодействия в течение одного рабочего дня со дня получения информации о таком нарушении.

Приложение № 4
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление

О проверке подлинности электронной подписи удостоверяющего центра в сертификате ключа проверки электронной подписи

_____
(полное наименование организации, включая
организационно-правовую форму)
в лице _____
(должность)
_____
(фамилия, имя. отчество)
действующего на основании_____,

просит проверить подлинность электронной подписи Удостоверяющего Центра в изданном Удостоверяющим Центром сертификате ключа проверки электронной подписи и установить его статус (действует/не действует) на основании представленных исходных данных:
1. Файл сертификата ключа проверки электронной подписи на прилагаемом к заявлению магнитном (магнито-оптическом, оптическом, флэш) носителе, регистрационный № МД-XXX;
2. Время и дата, на момент наступления которых требуется установить статус сертификата:
"_____:_____" "_____/_____/_____/"
(час) (минута) (день) (месяц) (года)
Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи заявления в Удостоверяющий Центр.
Время и дата подачи заявления в Удостоверяющий Центр:
"_____:_____" "_____/_____/_____/"

Пользователь Удостоверяющего Центра _____ _____
(подпись) (Фамилия И.О.)
"_____" _____ 20 ____ года
Руководитель (должность)_____ _____ _____
(подпись) (Фамилия И.О.)

"_____" _____ 20 ____ года
МП

Приложение № 5
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление

на аннулирование (отзыв) сертификата ключа проверки электронной подписи сотрудника в Удостоверяющем Центре

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____
(фамилия, имя, отчество)
действующего на основании _____
в связи с _____
(причина аннулирования (отзыва) сертификата ключа проверки электронной подписи)

Просит аннулировать
сертификат ключа проверки электронной подписи сотрудника
_____
(фамилия, имя, отчество)
содержащего следующие данные:

Серийный номер сертификата	
Фамилия, имя, отчество	
ОГРН/ОГРНИП	
СНИЛС пользователя УЦ	
Организация	

Пользователь Удостоверяющего Центра _____ _____
(подпись) (Фамилия И.О.)
"___"_____ 20___ года

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)

"___" _____ 20___ года
М.П.

Приложение № 6
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица (индивидуального предпринимателя) в Удостоверяющем Центре

_____
(наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____
(фамилия, имя, отчество)
действующего на основании _____

Просит:

☐ зарегистрировать юридическое лицо в Реестре Удостоверяющего Центра;

☐ сформировать ключи электронной подписи (далее - ЭП) и изготовить сертификат ключа проверки ЭП юридического лица в Удостоверяющем Центре

в соответствии со следующими данными и областью применения сертификата ключа проверки ЭП:

Организация *	
ИНН организации	
ОГРН/ОГРНИП	
Страна	RU
Регион	
Адрес местонахождения организации согласно выписки из ЕГРЮЛ/ЕГРИП	
Адрес электронной почты организации	
Область применения сертификата	

* указывается полное или сокращенное наименование согласно положению (уставу), не более 64 знаков

зарегистрировать квалифицированный сертификат ключа проверки электронный подписи в ЕСИА во исполнение требований ч. 5 ст. 18 Федерального закона № 63-ФЗ «Об электронной подписи».

Криптопровайдер (отметьте используемый): ☐ КриптоПро ☐ ViPNet

Носитель ЭП: ☐ СЭП Крип ☐ Рутокен ☐ JaCarta ☐

_____

(должность руководителя) (подпись) (Фамилия И.О.)

"___" _____ 20___ года

М.П. (при наличии)

Согласование выдачи ключей электронной подписи и сертификата ключа проверки электронной подписи юридического лица в Удостоверяющем Центре (страница печатается и заполняется на обратной стороне заявления в случае получения ключей электронной подписи и сертификата ключа проверки электронной подписи в Удостоверяющем центре иными учреждениями и организациями, использующими информационные системы, операторами которых являются органы государственной власти Самарской области или подведомственные им учреждения, в целях обеспечения выполнения государственных функций органов государственной власти Самарской области)

Оператор информационной системы:

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность)

действующий на основании _____

Согласовал выдачу ЭП для работы в следующих информационных системах:	

(должность представителя Оператора информационной системы) (подпись) (Фамилия И.О.)

"___" _____ 20____ года

М.П.

Приложение № 7
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Руководство

по обеспечению безопасности использования электронной подписи и средств квалифицированной электронной подписи

1. Пользователь УЦ обязан:

не передавать индивидуальные электронные носители ЭП другим лицам:

не разглашать конфиденциальную информацию, к которой он допущен, рубежи ее защиты, в том числе сведения о ключах ЭП:

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ

сообщать ответственному сотруднику за эксплуатацию ЭП о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним:

немедленно уведомлять ответственного сотрудника за эксплуатацию ЭП о фактах утраты криптографических ключей ЭП, ключей от помещений и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений:

при эксплуатации руководствоваться технической документацией (формулярами) на используемое СКЗИ:

вести поэкземплярный учет используемых или хранимых СКЗИ, эксплуатационной и технической документации к ним. ключевых документов по установленным формам в соответствии с требованиями Приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование;

2. Пользователю УЦ категорически запрещается:

оставлять ключевой носитель ЭП в устройстве считывания при оставлении рабочего места без присмотра, т.к. постороннее лицо может получить доступ к использованию ЭП в информационных системах;

осуществлять несанкционированное копирование криптографических ключей ЭП;

использовать ключевые носители ЭП для работы на других рабочих местах или для шифрования и подписи электронных документов, не относящейся к работе согласно области применения, для которой была получена ЭП;

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

вставлять носители ключевой информации в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ. а также в устройства считывания других

ПЭВМ;

записывать на носители ключевой информации постороннюю информацию;

подключать к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации;

работать на ПЭВМ, если во время ее начальной загрузки не проходят встроенные тесты, предусмотренные в ПЭВМ;

вносить какие-либо изменения в программное обеспечение СКЗИ.

3. Пользователь УЦ имеет право:

обращаться в Региональный удостоверяющий центр Самарской области по тел. (846) 2000-933 за консультациями по вопросам использования носителей ключевой информации, а также по вопросам обеспечения информационной безопасности технологического процесса.

Пользователь ЭП несет персональную ответственность за сохранность и правильное использование вверенной ему персональной ключевой информации и содержание документов, подписанных его персональным носителем ЭП.

г. Самара, ул. Николая Панова, д. 16.

Телефон: (846) 2000 933.

Факс: (846) 2000 131.

E-mail: ruc@samregion.ru.

http://ruc.samregion.ru.

Приложение № 8
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление

на аннулирование (отзыв) сертификата ключа проверки электронной подписи юридического лица (индивидуального предпринимателя) в Удостоверяющем центре

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____
(должность)
_____,
(фамилия, имя, отчество)
действующего на основании _____,
в связи с _____
(причина аннулирования (отзыва сертификата ключа проверки электронной подписи)

Просит аннулировать

сертификат ключа проверки электронной подписи юридического лица
_____
(наименование юридического лица)
содержащего следующие данные:

Серийный номер сертификата	
Организация *	
ОГРН/ОГРНИП	

* указывается полное или сокращенное наименование согласно положению (уставу), не более 64 знаков.

_____ _____ _____
(должность руководителя) (подпись) (Фамилия И.О.)
"___"_____ 20___ года
М.П.

Приложение № 9
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Памятка

пользователя Удостоверяющего центра (юридического лица)

Владелец сертификата ключа проверки электронной подписи:
Наименование организации
Серийный номер сертификата ключа проверки электронной подписи:
Серийный номер
Логин для аутентификации на сервере электронной подписи Криптопро DSS:
Логин
Пароль для аутентификации на сервере электронной подписи Криптопро DSS:
Пароль
Наименование криптопровайдера:
Наименование криптопровайдера
Пароль носителя:
Пароль
Ключевая фраза для удаленной аутентификации*:
Фраза
Оператор Удостоверяющего центра _____Ф.И.О. Дата
Телефон службы технической поддержки (846) 2000-933

* - Удаленная аутентификация пользователя удостоверяющего центра (далее - УЦ) предназначена для установления наименования юридического лица, зарегистрированного в качестве пользователя УЦ, по телефону. Уполномоченное лицо, проходящее данную процедуру, должно сообщить идентификационные данные юридического лица и, по запросу сотрудника УЦ, назвать ключевую фразу для удаленной аутентификации.

При компрометации ключа ЭП (потеря носителей ключевой информации, потеря носителей ключевой информации с их последующим обнаружением, носители ключевой информации стали на время доступными постороннему лицу без контроля со стороны владельца или ответственного за хранение ключевой информации, увольнение работников, имевших доступ к ключевой информации, или их перевод на другой участок работы) пользователь УЦ немедленно прекращает использование соответствующего ключа ЭП и уведомляет об этом сотрудника УЦ и иных участников электронного взаимодействия в течение одного рабочего дня со дня получения информации о таком нарушении.

Приложение № 10
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

ЗАЯВКА
на присоединение к Порядку реализации функций аккредитованного регионального удостоверяющего центра Самарской области и исполнения его обязанностей

_____ (указывается полное наименование Заявителя, включая организационно-правовую форму,) в лице _____ (указывается должность, фамилия, имя и отчество лица, уполномоченного действовать от имени Заявителя), действующего на основании _____ (указывается наименование и реквизиты документа, на основании которого действует уполномоченное лицо), в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Порядку реализации функций аккредитованного регионального удостоверяющего центра Самарской области и исполнения его обязанностей (далее - Порядок) в целях получения услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иных услуг регионального удостоверяющего центра Самарской области в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». Условия Порядка определены и опубликованы в информационно-телекоммуникационной сети «Интернет» на сайте Регионального удостоверяющего центра Самарской области по адресу https://ruc.samregion.ru.

С Порядком и приложениями к нему ознакомлены и обязуемся соблюдать все его условия.

Основные учетные данные указаны в Приложении к настоящей Заявке.

(Полное наименование должности) _____ФИО
(подпись)

М.П.

Далее заполняется уполномоченным лицом регионального удостоверяющего центра Самарской области

Данная Заявка зарегистрирована в реестре заявок участников Системы, регистрационный № _____ от «___» _____ 20___г.

Заявку зарегистрировал:

_____
_____
(должность, ФИО)

«___» _____ 20___г. _____
(подпись)

М.П.

ПРИЛОЖЕНИЕ
к заявке на присоединение к
Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Учетные данные Заявителя

Основные данные		
1.	Полное наименование заявителя, включая организационно-правовую форму	
2.	Сокращенное наименование организации	
3.	Юридический адрес	
4.	Почтовый адрес	
5.	ИНН	
6.	ОГРН	
7.	ОКТМО	
8.	ФИО руководителя	
9.	Телефон	
10.	Факс	
11.	Адрес электронной почты (E-mail)	

Приложение № 11
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество (при наличии) субъекта персональных данных)
проживающ__ по адресу: _____
_____,
документ, удостоверяющий личность: _____
_____,
(наименование документа, удостоверяющего личность, серия и №, сведения о дате выдачи документа и выдавшем его органе)

соглашаюсь с обработкой (сбор, систематизация, накопление, хранение, изменение, использование, обезличивание, блокирование, уничтожение, передачу в ЕСИА) моих персональных данных (ПД) ГБУ СО "Цифровой регион" (адрес: 443068, г. Самара, ул. Николая Панова, д. 16) согласно Порядку Удостоверяющего Центра и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцем которых я являюсь, являются достоверными и относятся к общедоступному источнику персональных данных. Удостоверяю, что ПД были предоставлены мною лично, даю свое согласие на архивное хранение (в течение срока деятельности УЦ) с целью исполнения требований ФЗ № 63-ФЗ от 06 апреля 2011 г. «Об электронной подписи».

Подпись _____ Дата _____

Приложение № 12
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление на изготовление ключей электронной подписи и сертификата ключа проверки электронной подписи физического лица в Удостоверяющем Центре

_____ прошу
(фамилия, имя, отчество)

☐ зарегистрировать в Реестре Удостоверяющего Центра, наделить полномочиями Пользователя Удостоверяющего Центра, установленными Порядком Удостоверяющего Центра;

☐ сформировать ключи электронной подписи (далее - ЭП) и изготовить сертификат ключа проверки ЭП физического лица в Удостоверяющем Центре;

в соответствии с указанными в настоящем заявлении идентификационными данными и областями применения сертификата ключа

Фамилия, имя, отчество	
СНИЛС пользователя УЦ	
Адрес электронной почты пользователя УЦ	
ИНН	
Страна	RU
Регион	
Город	

Область применения сертификата, дополнительные объектные идентификаторы (при необходимости)*	

* - может требоваться подтверждение полномочия на получения данного объектного идентификатора

зарегистрировать квалифицированный сертификат ключа проверки ЭП в ЕСИА во исполнение требований ч. 5 ст. 18 Федерального закона № 63-ФЗ «Об электронной подписи» в соответствии со следующими дополнительными данными:

Основной документ, удостоверяющий личность	Серия		Номер		Дата выдачи	
Дата рождения						
Пол	☐ Мужской				☐ Женский	

Гражданство _____

Криптопровайдер (отметьте используемый): ☐ КриптоПро ☐ ViPNet

Носитель ЭП (не более одного):

☐ Рутокен ☐ iPad ☐ JaCarta ☐ СЭП КриптоПро DSS ☐ _____

Настоящим Пользователь Удостоверяющего Центра подтверждает, что ознакомлен с руководством по обеспечению безопасности использования ЭП и средств ЭП (Приложение № 7 к Порядку Удостоверяющего Центра)

Пользователь Удостоверяющего Центра _____ _____
(подпись) (Фамилия И.О.)
"__" _____ 20___ года

Приложение № 13
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Заявление

на аннулирование (отзыв) сертификата ключа проверки электронной подписи физического лица в Удостоверяющем центре

_____
(фамилия, имя, отчество)
в связи с _____
(причина аннулирования (отзыва сертификата ключа проверки
электронной подписи)

Просит аннулировать сертификат ключа проверки электронной подписи физического лица

содержащего следующие данные:

Серийный номер сертификата	
ИНН	
СНИЛС	

Пользователь Удостоверяющего Центра _____ _____
(подпись) (Фамилия И.О.)
"__" _____ 20___ года

Приложение № 14
к Порядку реализации функций
аккредитованного регионального
удостоверяющего центра
Самарской области
и исполнения его обязанностей

Памятка

Пользователя (физического лица) Удостоверяющего центра

Владелец сертификата ключа проверки электронной подписи:
Фамилия Имя Отчество
Серийный номер сертификата ключа проверки электронной подписи:
Серийный номер
Наименование криптопровайдера:
Наименование криптопровайдера
Пароль носителя:
Пароль
Ключевая фраза для удаленной аутентификации <*>:
Фраза
Оператор УЦ _____ Фамилия И.О. Дата
Телефон службы технической поддержки: (846) 2000-933

<*> Удаленная аутентификация зарегистрированного пользователя УЦ предназначена для установления личности зарегистрированного пользователя УЦ по телефону. Лицо, проходящее данную процедуру, должно сообщить свои идентификационные данные и по запросу сотрудника УЦ, назвать ключевую фразу для удаленной аутентификации.

При компрометации ключа ЭП (потеря носителей ключевой информации, потеря носителей ключевой информации с их последующим обнаружением; носители ключевой информации стали на время доступными постороннему лицу без контроля со стороны владельца или ответственного за хранение ключевой информации; увольнение работников, имевших доступ к ключевой информации, или их перевод на другой участок работы) пользователь немедленно прекращает использование соответствующего ключа ЭП и уведомляет об этом сотрудника УЦ и иных участников электронного взаимодействия в течение одного рабочего дня со дня получения информации о таком нарушении.