МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РОССИЙСКИЙ ФЕДЕРАЛЬНЫЙ ЦЕНТР СУДЕБНОЙ ЭКСПЕРТИЗЫ ПРИ МИНИСТЕРСТВЕ ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

Москва

«10» декабря 2019 г. № 259/1-1

Об утверждении Регламента Удостоверяющего центра федерального бюджетного учреждения Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации

В целях создания и обеспечения функционирования Удостоверяющего центра федерального бюджетного учреждения Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации, соблюдения положений Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»

п р и к а з ы в а ю:

1. Утвердить Регламент Удостоверяющего центра федерального бюджетного учреждения Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации согласно приложению к настоящему приказу.
2. Приказ вступает в силу с момента подписания.
3. Заведующему отделом информационной безопасности Шестихину А.А. организовать размещение приказа на официальном сайте ФБУ РФЦСЭ при Минюсте России в течение 10 дней после его подписания для общего доступа.
4. Признать утратившим силу приказ ФБУ РФЦСЭ при Минюсте России от 25 января 2019 г. № 21/1-1 «Об утверждении Регламента Удостоверяющего центра федерального бюджетного учреждения Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации».
5. Контроль за исполнением настоящего приказа возложить на заместителя директора по информатизации Хатунцева Н.А.

Директор С.А. Смирнова

Шестихин Аркадий Александрович
заведующий ОИБ
(495)181-57-57 доб. 3601

Приложение к приказу
ФБУ РФЦСЭ при Минюсте России
от 10.12.2019 № 259/1-1

Регламент
Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

1. Термины и определения

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности пользователя удостоверяющего центра.

Владелец сертификата ключа проверки электронной подписи (далее – владелец) - лицо, которому в установленном Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" порядке выдан сертификат ключа проверки электронной подписи.

Владельцами сертификатов ключей проверки электронных подписей, изданных Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России, являются федеральные бюджетные судебно-экспертные учреждения Министерства юстиции Российской Федерации и работники данных учреждений.

Доверенное лицо - лицо, которое удостоверяющий центр наделил полномочиями по выдаче сертификатов ключа проверки электронной подписи от имени удостоверяющего центра, подписываемых электронной подписью, основанной на сертификате ключа проверки электронной подписи, выданном доверенному лицу этим удостоверяющим центром.

Единая система идентификации и аутентификации - федеральная государственная информационная система «Единая система идентификации и аутентификации» в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Запрос на создание сертификата ключа проверки электронной подписи - файл, созданный с использованием сертифицированного средства электронной подписи, содержащий ключ проверки электронной подписи и иную информацию о владельце сертификата ключа проверки электронной подписи.

Заявитель - лицо, обратившееся за получением сертификата ключа проверки электронной подписи. С момента выдачи сертификата ключа проверки электронной подписи удостоверяющим центром заявитель становится владельцем сертификата ключа проверки электронной подписи (пользователем удостоверяющего центра).

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Квалифицированная электронная подпись - электронная подпись, которая соответствует всем признакам квалифицированной электронной подписи, определенным Федеральным законом «Об электронной подписи».

Квалифицированный сертификат ключа проверки электронной подписи (далее – квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Требования к полям квалифицированного сертификата ключа проверки электронной подписи определены в приказе ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

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

Ключ электронной подписи (далее - КЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

КЭП действует на определенный момент времени если:

- наступил момент времени начала действия КЭП;
- срок действия КЭП не истек;
- сертификат ключа проверки электронной подписи, соответствующий данному КЭП не аннулирован (не отозван).

Ключевой носитель - отчуждаемый физический носитель, содержащий один или несколько КЭП, а при необходимости и иную контрольную, служебную и технологическую информацию.

Компрометация ключа - утрата доверия к тому, что используемые ключи шифрования или электронной подписи обеспечивают безопасность информации (идентификация лица, контроль целостности информации, защита от изменений (подделки), отказ от авторства).

К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- потеря ключевых носителей, в том числе с их последующим обнаружением;
- увольнение работников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения КЭП;
- возникновение подозрений на утечку информации;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к

данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством РФ.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий работника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Пользователь удостоверяющего центра (далее – пользователь УЦ) - см. Владелец сертификата ключа проверки электронной подписи.

Пользователями удостоверяющего центра могут быть физические лица и юридические лица, присоединившиеся к настоящему Регламенту.

В случае, когда в качестве пользователя удостоверяющего центра выступает юридическое лицо, его интересы представляет физическое лицо, действующее на основании учредительных документов либо доверенности.

Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

Регистрационная информация пользователя удостоверяющего центра - информация, предоставляемая пользователем удостоверяющего центра в целях создания сертификата ключа проверки электронной подписи.

Под регистрацией пользователей удостоверяющего центра понимается внесение регистрационной информации о пользователях удостоверяющего центра в реестр удостоверяющего центра.

Реестр удостоверяющего центра - набор документов удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- реестр изготовленных сертификатов ключа проверки электронной подписи пользователей;
- реестр аннулированных/ отозванных сертификатов;
- реестр зарегистрированных пользователей удостоверяющего центра.

Сертификат ключа проверки электронной подписи (далее – сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи действует на определенный момент времени, т.е. является действующим сертификатом, если:

- наступил момент времени начала действия сертификата ключа проверки электронной подписи;
- срок действия сертификата ключа проверки электронной подписи не истек;
- сертификат ключа проверки электронной подписи не аннулирован либо не отозван.

Сертификат ключа проверки электронной подписи удостоверяющего центра – сертификат, с помощью которого проверяется достоверность сертификатов пользователей удостоверяющего центра и уполномоченного лица удостоверяющего центра, заверенных этим сертификатом.

Список аннулированных сертификатов (далее - САС) - электронный документ с электронной подписью удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронных подписей, которые на определенный момент времени были аннулированы.

Средства криптографической защиты информации (далее - СКЗИ) - аппаратные, программные и аппаратно-программные средства, системы и комплексы, осуществляющие криптографические преобразования информации для обеспечения ее защиты от несанкционированного доступа, от навязывания ложной информации и/или обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием ключа электронной подписи, подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи, создание ключей электронной подписи и ключей проверки электронной подписи.

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

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

Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России (далее – УЦ) - юридическое лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Уполномоченное лицо удостоверяющего центра – физическое лицо, являющееся работником ФБУ РФЦСЭ при Минюсте России и наделенное директором ФБУ РФЦСЭ при Минюсте России полномочиями по заверению издаваемых сертификатов ключей проверки электронных подписей и списков аннулированных сертификатов.

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

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

2. Общие положения

2.1. Предмет регулирования

Настоящий Регламент определяет порядок реализации функций Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России по созданию и выдаче сертификатов, осуществления прав и обязанностей УЦ, регулирования отношений,

возникающих в процессе предоставления услуг УЦ, а также основные организационно-технические меры по обеспечению информационной безопасности при использовании ключевой информации и средств электронной подписи.

Настоящий Регламент разработан в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - закон о персональных данных), приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», приказом Министерства связи и массовых коммуникаций Российской Федерации от 22 августа 2017 г. № 436 «Об утверждении Порядка формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров» (далее - Порядок ведения реестров сертификатов), приказом Минкомсвязи России от 13 августа 2018г. № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей».

В настоящем Регламенте используются понятия, термины, сокращения, которые применяются в указанных выше нормативных правовых актах.

Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.

Присоединение к настоящему Регламенту осуществляется путем подачи заявителем заявки на услуги УЦ. С момента подачи заявки заявитель считается присоединившимся к настоящему Регламенту и становится стороной настоящего Регламента – пользователем УЦ.

Факт присоединения заявителя к настоящему Регламенту является полным принятием им условий настоящего Регламента и всех его положений в редакции, действующей на момент подачи заявки на услуги УЦ. Сторона, присоединившаяся к настоящему Регламенту, принимает дальнейшие изменения (дополнения), вносимые в настоящий Регламент, в соответствии с условиями настоящего Регламента.

Уведомление пользователей УЦ о внесении изменений в настоящий Регламент осуществляется путем публикации актуальной версии Регламента Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России в электронном виде на сайте ФБУ РФЦСЭ при Минюсте России по адресу http://www.sudexpert.ru/uc/.

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России и пользователь УЦ.

При возникновении споров стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

Споры между сторонами, связанные с действием настоящего Регламента, не урегулированные в процессе совместных переговоров, разрешаются в судебном порядке в соответствии с законодательством Российской Федерации.

2.2. Сведения об Удостоверяющем центре ФБУ РФЦСЭ при Минюсте России

2.2.1. Информация о месте нахождения и графике работы Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Адрес места нахождения Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: 101000, г. Москва, Большой Спасоглинищевский переулок, дом 4.

Почтовый адрес Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: 109028, г. Москва, Хохловский переулок, дом 13, строение 2 (с пометкой «для Удостоверяющего центра»).

График работы Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: ежедневно, кроме выходных и праздничных дней, с 9:00 до 18:00 по местному времени, в соответствии с часовым поясом места нахождения Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

2.3.1. Справочные телефоны Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Контактный телефон Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России для получения справочной информации и технической поддержки: (495) 181-57-57 доб. 3600, 3601, 3602, 3603, 3604.

2.3.2. Адреса сайтов Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России в информационно-телекоммуникационной сети «Интернет», адреса электронной почты

Адрес сайта Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России http://www.sudexpert.ru/uc/.

Адрес электронной почты Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: uc@sudexpert.ru .

2.3.3. Порядок получения информации заявителями по вопросам предоставления услуг Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Информация о предоставлении услуг Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России опубликована на сайте ФБУ РФЦСЭ при Минюсте России по адресу http://www.sudexpert.ru/uc/.

Настоящий Регламент публикуется в форме электронного документа на сайте ФБУ РФЦСЭ при Минюсте России по адресу http://www.sudexpert.ru/uc/ .

С целью обеспечения гарантированного ознакомления с полным текстом изменений и дополнений, не реже одного раза в 30 (тридцать) календарных дней пользователю УЦ обращаться на сайт Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России в сети Интернет по адресу http://www.sudexpert.ru/uc/ за сведениями об изменениях и дополнениях в Регламенте Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России.

2.4. Стоимость услуг Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России является государственным учреждением и выдает квалифицированные сертификаты

заявителям на безвозмездной основе. Заявителями являются федеральные бюджетные судебно-экспертные учреждения Министерства юстиции Российской Федерации и работники данных учреждений.

3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России

3.1. Функции Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

УЦ выполняет следующие функции, предусмотренные статьей 13 Федерального закона «Об электронной подписи»:

– 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;

– 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 изготовленные Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России 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 ФБУ РФЦСЭ при Минюсте России) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

– ведет реестр изготовленных и аннулированных (отозванных) Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в изготовленных Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России 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.

УЦ, являющийся головным УЦ, выполняет следующие функции:

1) осуществляет проверку электронных подписей, ключи проверки которых указаны в выданных доверенными лицами сертификатах ключей проверки электронных подписей;

2) обеспечивает электронное взаимодействие доверенных лиц между собой, а также доверенных лиц с УЦ.

3.2. Услуги, предоставляемые Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России

В процессе своей деятельности УЦ предоставляет пользователям УЦ следующие виды услуг:

– внесение в реестр УЦ регистрационной информации о владельцах сертификатов ключа проверки электронной подписи;

– изготовление сертификатов ключа проверки электронной подписи в электронной форме;

– изготовление сертификатов ключа проверки электронной подписи на бумажном носителе;

– формирование КЭП и КПЭП по обращениям заявителей с записью их на ключевой носитель;

– ведение реестра сертификатов;

– предоставление в электронной форме сертификатов ключа проверки электронной подписи, находящихся в реестре изготовленных сертификатов ключа проверки электронной подписи, по запросам любого лица;

– отзыв (аннулирование) сертификатов ключа проверки электронной подписи по обращениям владельцев сертификатов ключа проверки электронной подписи;

– ведение списков аннулированных сертификатов и предоставление информации об аннулировании сертификата ключа проверки электронной подписи любому лицу по его обращению;

– подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей УЦ;

– выдача средств ЭП по обращениям пользователей УЦ.

4. Права и обязанности Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

4.1. Права Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

УЦ имеет право:

- наделить третьих лиц (далее - доверенные лица) полномочиями по вручению сертификатов ключей проверки электронных подписей от имени УЦ. При вручении сертификата ключа проверки электронной подписи доверенное лицо

обязано установить личность получателя сертификата (заявителя) либо полномочия лица, выступающего от имени заявителя, по обращению за получением данного сертификата в соответствии с настоящим Регламентом;

- выдавать сертификаты как в форме электронных документов, так и в форме документов на бумажном носителе;
- отказать в изготовлении сертификата заявителю в случае непредставления документов, предоставления документов не в полном объеме или предоставления документов, подлинность которых вызывает сомнение;
- отказать в изготовлении сертификата заявителю в случае, если использованное заявителем для формирования запроса на сертификат СКЗИ не поддерживается УЦ;
- отказать в изготовлении сертификата заявителю в случае невыполнения заявителем обязанностей, установленных Федеральным законом от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами, а также Регламентом УЦ;
- отказать в изготовлении сертификата, если предоставленные заявителем сведения не прошли проверку в соответствии с п.2.2, 2.3 ст.18 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- отказать в изготовлении сертификата заявителя подписи при расхождении данных, предоставленных заявителем с данными, указанными в ЕГРЮЛ;
- аннулировать сертификат, в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного сертификата по электронной почте, указанной при заполнении заявления на сертификат;
- проверять достоверность документов и сведений, предоставленных заявителем, с использованием инфраструктуры, запрашивать и получать из государственных информационных ресурсов:

а) выписку из Единого государственного реестра юридических лиц в отношении заявителя - юридического лица;

б) выписку из Единого государственного реестра налогоплательщиков в отношении заявителя - иностранной организации.

В случае, если полученные в соответствии с частью 2.2 статьи 18 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и аккредитованным удостоверяющим центром установлена личность заявителя - физического лица или получено подтверждение правомочий лица, выступающего от имени заявителя - юридического лица, на обращение за получением квалифицированного сертификата, аккредитованный удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае аккредитованный удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

4.2. Обязанности Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

УЦ обязан:

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

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

– 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;

– обеспечивать конфиденциальность созданных УЦ ключей электронных подписей;

– отказать заявителю в создании сертификата 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;

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

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

Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности УЦ, если более короткий срок не установлен нормативными правовыми актами. В случае прекращения деятельности УЦ без перехода его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты прекращения деятельности этого удостоверяющего центра. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть уничтожена. В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

Аккредитованный удостоверяющий центр обязан хранить в течение срока его деятельности, если более короткий срок не предусмотрен нормативными правовыми

актами Российской Федерации, следующую информацию:

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

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

3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

Аккредитованный удостоверяющий центр для подписания от своего имени квалифицированных сертификатов обязан использовать квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

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

В случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

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

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

3) передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре.

Аккредитованный удостоверяющий центр не вправе наделять третьих лиц полномочиями по созданию ключей квалифицированных электронных подписей и квалифицированных сертификатов от имени такого аккредитованного удостоверяющего центра.

При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр обязан:

1) установить личность заявителя - физического лица, обратившегося к нему за получением квалифицированного сертификата;

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

Аккредитованный УЦ обязан выполнять порядок реализации функций аккредитованного УЦ и исполнения его обязанностей, установленный таким аккредитованным УЦ в соответствии с утвержденными уполномоченным федеральным органом требованиями к порядку реализации функций аккредитованного УЦ и исполнения обязанностей, а также с Федеральным законом «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи».

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

При выдаче квалифицированного сертификата аккредитованный УЦ направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра). При выдаче квалифицированного сертификата аккредитованный удостоверяющий центр по желанию лица, которому выдан квалифицированный сертификат, безвозмездно осуществляет регистрацию указанного лица в единой системе идентификации и аутентификации.

5. Права и обязанности пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

5.1. Пользователь УЦ обязан:

– обеспечить конфиденциальность КЭП. Не использовать КЭП и немедленно обратиться в аккредитованный УЦ, выдавший сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность КЭП нарушена;

– извещать УЦ обо всех изменениях данных, внесенных в сертификат;

– при подаче заявления на создание сертификата указать действующий электронный почтовый адрес владельца ЭП для получения извещений, уведомлений от УЦ, связанных с применением сертификата, его аннулированием;

– хранить в тайне личный КЭП, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования;

– применять для формирования электронной цифровой подписи только действующий личный КЭП;

– не применять личный КЭП, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

– немедленно обратиться в УЦ с заявлением на отзыв/аннулирование сертификата в случае утери, кражи, а также в случае если владельцу ЭП стало известно, что ключ используется или использовался ранее другими лицами;

– не использовать личный КЭП, связанный с сертификатом, заявление на отзыв/аннулирование которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на отзыв/аннулирование сертификата по момент времени официального уведомления об прекращении/аннулировании сертификата;

– не использовать КЭП, связанный с сертификатом, который аннулирован.

5.2. Пользователь УЦ имеет право:

– владелец сертификата, выданного в форме электронного документа, вправе получить также копию сертификата на бумажном носителе, заверенную УЦ;

– обратиться в УЦ с заявлением на создание квалифицированного сертификата;

– обратиться в УЦ с заявлением на отзыв сертификата, владельцем которого он является, в течение срока действия соответствующего КЭП;

– обратиться в УЦ за получением информации о статусе сертификатов и их действительности на определенный момент времени;

– обратиться в УЦ за подтверждением действительности электронной подписи в электронном документе, сформированной с использованием сертификата, изданного УЦ.

6. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России

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

6.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей (далее – пара ключей ЭП) с учетом следующих способов создания

Создание пары ключей ЭП и сертификата заявителю в УЦ возможно в следующих случаях:

1) Заявитель самостоятельно формирует при помощи средства ЭП, имеющего подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», пару ключей ЭП и файл запрос на создание сертификата ключа проверки электронной подписи, приносит данный файл запрос на создание сертификата с заявлением на создание квалифицированного сертификата ключа проверки электронной подписи в офис УЦ.

Заявитель создает КЭП и КПЭП при помощи средств ЭП, предоставленных УЦ либо собственных. Средства ЭП, являющиеся СКЗИ, должны эксплуатироваться в соответствии с правилами пользования ими, 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 проверяет и обрабатывает запрос, регистрирует пользователя УЦ, издает квалифицированный сертификат. УЦ передает созданный сертификат заявителю в электронном виде, также по обращению владельца сертификата выдается ему копия сертификата на бумажном носителе, заверенная УЦ. Заявитель проверяет правильность данных и заверяет сертификат своей личной подписью.

2) Заявитель лично обращается с заявлением на создание квалифицированного сертификата на создание КЭП, КПЭП и сертификата в офис УЦ. На автоматизированном рабочем месте УЦ, используемом для создания КЭП и КПЭП для заявителя, формируется при помощи сертифицированного СКЗИ пара ключей ЭП и файл запрос на создание сертификата. КЭП создается непосредственно на ключевом носителе, предоставленным заявителем. УЦ проверяет и обрабатывает запрос, регистрирует пользователя УЦ, издает сертификат, сохраняя его в контейнер на ключевой носитель с уже имеющимся там КЭП, и передает данный носитель заявителю. Также по обращению владельца сертификата выдается ему копия сертификата на бумажном носителе, заверенная УЦ. Заявитель проверяет правильность данных и заверяет сертификат своей личной подписью.

УЦ создает КЭП и КПЭП для заявителя при помощи средств ЭП. Средства ЭП, являющиеся СКЗИ, эксплуатируются в соответствии с правилами пользования ими, согласованными с Федеральной службой безопасности Российской Федерации, в соответствии с приказом ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

КЭП и КПЭП, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона «Об электронной подписи» создаются с использованием средства ЭП, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

В отношении автоматизированного рабочего места УЦ, используемого для создания КЭП и КПЭП для заявителя, выполнены требования, установленные постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049).

Изготовление пары ключей ЭП осуществляется в УЦ по обращению заявителя. Обращение заявителя оформляется в форме заявления на создание квалифицированного сертификата ключа проверки электронной подписи

Прием заявлений, изготовление и выдача пары ключей ЭП осуществляется УЦ при личном присутствии заявителя.

Заявление на создание квалифицированного сертификата подается заявителем в письменной форме на бумажном носителе и заверяется собственноручной подписью заявителя.

Заявление на создание квалифицированного сертификата рассматривается УЦ

в течение трех рабочих дней с момента поступления.

Изготовленная пара ключей ЭП записывается на ключевой носитель, предоставляемый заявителем, независимо от способа создания. Ключевой носитель должен соответствовать требованиям, указанным в документации на сертифицированное средство ЭП по требованиям ФСБ России.

Ключевой носитель, содержащий изготовленную пару ключей ЭП, передается владельцу сертификата (заявителю). Факт выдачи ключевого носителя, содержащего изготовленную пару ключей ЭП, фиксируется актом передачи ключевого носителя под роспись владельца. Форма акта передачи ключевого носителя приведена в приложении № 7 к настоящему Регламенту.

УЦ осуществляет по обращению заявителя выдачу средства ЭП, имеющего подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», и эксплуатационной документации к нему. Выдача средств ЭП осуществляется во временное пользование по письменному обращению владельца сертификата (заявителя). Форма заявления на выдачу средств ЭП приведена в приложении № 8 к настоящему Регламенту.

Выдача средства ЭП и эксплуатационной документации к нему осуществляется не позднее шести рабочих дней с даты приема заявления на выдачу средств ЭП владельца сертификата (заявителя) и оптического носителя.

При выдаче средства ЭП осуществляется идентификация лица, указанного в заявлении на выдачу средств ЭП, по документу, удостоверяющему личность.

Установка, настройка и эксплуатация средства ЭП осуществляется владельцем сертификата самостоятельно в соответствии с требованиями эксплуатационной документации к нему и законодательства Российской Федерации.

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

Плановая смена КЭП и соответствующего ему сертификата УЦ выполняется в период действия КЭП УЦ и не позднее срока действия сертификата УЦ.

Плановая смена КЭП УЦ производится по следующим основаниям:

– истечение срока действия сертификата УЦ;

– переход на использование новых стандартов ЭП и функции хэширования в соответствии с руководящими документами органа исполнительной власти, уполномоченного в сфере использования электронной подписи.

Срок действия сертификата УЦ не может превышать 192 месяца (16 лет). Заданный срок действия сертификата определяет срок действия КЭП.

Процедура плановой смены КЭП УЦ осуществляется в следующем порядке:

1) УЦ создает новый КЭП и соответствующий ему КПЭП;

2) УЦ создает новый сертификат.

Уведомление пользователей УЦ о проведении смены КЭП УЦ осуществляется посредством электронной почты с указанием доверенного способа получения

нового сертификата УЦ.

6.1.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России в случаях нарушения их конфиденциальности, содержащей основание, процедуры и сроки осуществления такой смены ключей электронной подписи Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, а также порядок информирования владельцев квалифицированных сертификатов об осуществлении такой смены с указанием доверенного способа получения нового квалифицированного сертификата Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

К случаям нарушения конфиденциальности (компрометации) КЭП УЦ относятся, включая, но не ограничиваясь, следующие:

– потеря ключевых носителей, в том числе с их последующим обнаружением;

– увольнение работников, имевших доступ к ключевой информации;

– нарушение правил хранения и уничтожения КЭП;

– возникновение подозрений на утечку информации;

– несанкционированный доступ постороннего лица в место физического хранения ключевого носителя, к устройству хранения КЭП или подозрение, что данные факты имели место (срабатывание сигнализации с подтверждением несанкционированного вскрытия помещения, повреждение замков, повреждение устройств контроля несанкционированного доступа (слепков печатей) и т.п.);

– случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

Актуальными угрозами нарушения конфиденциальности (компрометации) КЭП УЦ являются:

– угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к рабочим местам автоматизированной системы УЦ.

В случае нарушения конфиденциальности КЭП УЦ сертификат УЦ прекращает действие.

Пользователи УЦ уведомляются о случае нарушения конфиденциальности КЭП УЦ путем рассылки соответствующего уведомления по электронной почте и публикации информации о нарушении.

Все сертификаты, подписанные с использованием КЭП УЦ, конфиденциальность которого была нарушена, считаются прекратившими действие.

После прекращения действия сертификата УЦ выполняется внеплановая смена ключей УЦ. Процедура внеплановой смены КЭП УЦ выполняется в порядке, аналогичном процедуре плановой смены КЭП УЦ раздела 6.1.2 настоящего Регламента.

Все действовавшие на момент нарушения конфиденциальности КЭП УЦ сертификаты подлежат смене.

6.1.4. Порядок осуществления Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России смены ключа электронной подписи владельца квалифицированного сертификата ключа проверки электронной подписи

Смена КЭП владельца сертификата осуществляется в следующих случаях:

1) в связи с истечением установленного срока действия сертификата;

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

3) если не подтверждено, что владелец сертификата владеет КЭП, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;

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

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

6) в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и владельцем сертификата.

В случае истечения установленного срока действия сертификата, порядок смены КЭП владельца сертификата в этом случае аналогичен порядку, установленному разделом 6.2 настоящего Регламента. Смена КЭП владельца сертификата осуществляется на основании заявления на создание квалифицированного сертификата ключа проверки электронной подписи. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи для юридических и физических лиц приведена в приложении № 2 к настоящему Регламенту.

В случае изменения сведений о пользователе УЦ или юридическом лице, от лица которого пользователь УЦ выступает, содержащихся в сертификате, пользователь УЦ вправе обратиться в офис УЦ с заявлением на отзыв квалифицированного сертификата ключа проверки электронной подписи, форма которого приведена в приложении № 9 к настоящему Регламенту, с последующей сменой (создания) сертификата. Процедура смены (создания) сертификата описана разделом 6.2 настоящего Регламента. Заявления формируются и представляются на бумажном носителе.

В случае внеплановой смены КЭП УЦ, создание новых сертификатов пользователей УЦ осуществляется в соответствии с разделом 6.1.3 настоящего Регламента.

В случае компрометации или угрозы компрометации КЭП пользователя УЦ. Если пользователю УЦ стало известно, что КЭП используется или использовался ранее другими лицами, а также при утрате, раскрытии, искажении КЭП пользователь УЦ немедленно должен обратиться в УЦ с заявлением на отзыв квалифицированного сертификата ключа проверки электронной подписи, а УЦ обязан аннулировать такой сертификат в порядке и сроки, установленные разделом 6.4 настоящего Регламента. Создание нового сертификата осуществляется на

основании заявления на создание квалифицированного сертификата ключа проверки электронной подписи в порядке, установленном разделом 6.2 настоящего Регламента.

Требования к указанным в настоящем разделе заявлениям установлены соответствующими разделами настоящего Регламента, ссылки на которые содержатся в данном разделе.

Заявления могут быть поданы в форме документов, оформленных надлежащим образом на бумажных носителях, по месту нахождения офиса УЦ.

Процедура выдачи сертификата и (при необходимости) КЭП владельцу сертификата, в том числе в электронной форме, производится с соблюдением положений статьи 18 Федерального закона «Об электронной подписи».

6.2. Процедура создания и выдачи квалифицированных сертификатов ключей проверки электронных подписей

6.2.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

Создание сертификата осуществляется на основании заявления на создание квалифицированного сертификата ключа проверки электронной подписи. Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи для юридических и физических лиц приведена в приложении № 2 к настоящему Регламенту.

Заявитель обращается с заявлением на изготовление сертификата и другими необходимыми документами, содержащими сведения, вносимые в сертификат, указанными в разделе 6.2.4 настоящего Регламента, в офис УЦ.

УЦ в сертификат вносится информация на основании заявления.

6.2.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи может быть оформлено как на бумажном носителе, заверенном собственноручной подписью владельца ЭП, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью. 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.

Использование факсимиле (клише подписи) на заявлении не допускается.

6.2.3. Порядок установления личности заявителя

Порядок установления личности следующий:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность, – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, УЦ может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации;

- личность гражданина иностранного государства устанавливается по

паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами;

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

6.2.4. Перечень документов, запрашиваемых Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России у заявителя для изготовления и выдачи квалифицированного сертификата КПЭП, в том числе для удостоверения личности заявителя

Уполномоченный работник УЦ выполняет процедуру идентификации пользователя УЦ путем установления личности пользователя УЦ по документам, удостоверяющим личность.

УЦ обязан:

- установить личность заявителя - физического лица, обратившегося к нему за получением сертификата КПЭП, на основании документа, удостоверяющего личность;

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

Обратиться для получения (создание и выдача) сертификата КПЭП вправе:

1. Для юридических лиц:

- физическое лицо, которое указывается в сертификате наряду с наименованием юридического лица;

- физическое лицо на основании доверенности на получение КЭП и сертификата, оформленной по форме приложения № 4 к настоящему Регламенту;

2. Для физических лиц:

- непосредственно этим физическим лицом;

- физическим лицом на основании нотариально заверенной доверенности на получение КЭП и сертификата, оформленной по форме приложения № 5 к настоящему Регламенту.

Пользователь УЦ представляет в УЦ документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности владельца ЭП (его доверенного лица), а также документы, подтверждающие сведения, на основании которых УЦ вносятся сведения в сертификат. К таким сведениям относятся:

- для заявителя – юридического лица – полное или сокращенное наименование юридического лица, основной государственный регистрационный номер, адрес местонахождения, идентификационный номер налогоплательщика, код причины постановки на учет;

- для заявителя – физического лица – страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика.

Пользователь УЦ обязан предоставлять в УЦ только достоверную информацию. В случае если после создания сертификата выяснится факт

предоставления недостоверных данных, УЦ вправе в одностороннем порядке прекратить действие такого сертификата.

Для подтверждения сведений, вносимых в сертификат, пользователь УЦ предоставляет в офис УЦ документы по форме, определенной действующим законодательством Российской Федерации, а именно:

1. Для юридических лиц:

- основной документ, удостоверяющий личность лица, являющегося владельцем ЭП, - предоставляется копия, заверенная печатью организации и подписью руководителя организации;

- основной государственный регистрационный номер заявителя (заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

- номер свидетельства о постановке на учет в налоговом органе заявителя-иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) или идентификационный номер налогоплательщика заявителя-иностранной организации (заявитель вправе по собственной инициативе представить копии документов, содержащих данные сведения);

- СНИЛС (страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования) владельца ЭП - предоставляется копия, заверенная печатью организации и подписью руководителя организации;

- доверенность, подтверждающая полномочия владельца ЭП, заверенная печатью организации и подписью руководителя организации, уполномочивающая выступать пользователем УЦ, по форме, установленной приложением № 3 к настоящему Регламенту (если сертификат изготавливается на уполномоченного представителя организации, не имеющего права действовать без доверенности от имени юридического лица).

Пользователь УЦ по собственной инициативе вправе предоставить:

- свидетельство о государственной регистрации юридического лица - предоставляется копия, заверенная печатью организации и подписью руководителя организации;

- свидетельство о постановке на учет в налоговом органе заявителя - иностранной организации (в том числе филиалов, представительств и иных обособленных подразделений иностранной организации) - предоставляется копия, заверенная печатью организации и подписью руководителя организации.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

2. Для физических лиц:

- основной документ, удостоверяющий личность лица, являющегося владельцем ЭП, - предоставляется оригинал данного документа и копия, заверенная нотариально;

- СНИЛС (страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования) владельца ЭП - предоставляется оригинал данного документа и копия, заверенная нотариально;

- свидетельство о постановке на учет в налоговом органе – предоставляется оригинал документа либо копия, заверенная нотариально.

К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

6.2.5. Порядок проверки достоверности документов и сведений, представленных заявителем

УЦ с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, представленных заявителем. УЦ самостоятельно запрашивает и получает из государственных информационных ресурсов выписку из Единого государственного реестра юридических лиц, а в отношении заявителя – иностранной организации – выписку из Единого государственного реестра налогоплательщиков.

В случае, если полученные УЦ сведения подтверждают достоверность информации, представленной пользователем УЦ для включения в сертификат, и УЦ установлена личность лица, обращающегося за получением сертификата, а также получено подтверждение правомочий лица, выступающего от имени владельца ЭП, на обращение за получением сертификата, УЦ осуществляет процедуру создания и выдачи квалифицированного сертификата. В противном случае УЦ отказывает заявителю в выдаче сертификата.

После положительной идентификации пользователя УЦ уполномоченный работник УЦ принимает указанные выше документы и файл с запросом на создание сертификата ключа проверки электронной подписи пользователя УЦ. Заявление на создание квалифицированного сертификата ключа проверки электронной подписи, предоставленные пользователем УЦ в соответствии с настоящим разделом документы, файл с запросом на создание сертификата ключа проверки электронной подписи подлежат рассмотрению УЦ. Данные о пользователе УЦ, содержащиеся в файле запросе на создание сертификата ключа проверки электронной подписи пользователя УЦ, должны совпадать с данными, указанными в заявлении на создание квалифицированного сертификата ключа проверки электронной подписи пользователя УЦ. Невыполнение этого условия служит безусловной причиной для отказа в создании сертификата пользователя УЦ.

В случае отказа в создании сертификата пользователя УЦ, заявление на создание квалифицированного сертификата ключа проверки электронной подписи вместе с предоставленными документами возвращается пользователю УЦ или его уполномоченному на основании доверенности лицу с отметкой работника УЦ.

При принятии положительного решения работник УЦ создает сертификат пользователя УЦ.

6.2.6. Порядок создания квалифицированного сертификата

Создание сертификата осуществляется на основании запроса, полученного в порядке, установленном разделом 6.1.1 настоящего Регламента.

При создании сертификатов УЦ проверяет уникальность ключей проверки электронных подписей. В случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного пользователем УЦ для получения сертификата, УЦ обязан отказать пользователю

УЦ в создании сертификата.

Структура и форма квалифицированного сертификата, выдаваемого УЦ, соответствует требованиям приказа ФСБ России от 27.12.2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи». В случае создания сертификата юридическому лицу наряду с указанием в сертификате наименования юридического лица должно указываться физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности.

6.2.7. Порядок выдачи квалифицированного сертификата

Работник УЦ приглашает владельца ЭП для вручения сертификата в УЦ.

Работник УЦ выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту и проверке подлинности документов, получает от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.

При получении квалифицированного сертификата владелец ЭП или иным надлежащим образом уполномоченное лицо знакомится под расписку с информацией, содержащейся в сертификате. Для ознакомления с данными сертификата владельцу ЭП/уполномоченному лицу выдаются две копии сертификата на бумажном носителе. На одной копии сертификата, которая остается в УЦ, владелец ЭП/уполномоченное лицо ставит свою подпись и пишет, что ознакомлен с информацией, содержащейся в квалифицированном сертификате, а уполномоченное лицо УЦ собственноручной подписью подтверждает факт ознакомления владельца ЭП/уполномоченного лица с информацией, содержащейся в сертификате. Вторая копия сертификата, которая остается у владельца ЭП, заверяется собственноручной подписью со стороны владельца ЭП/уполномоченного лица, а также собственноручной подписью уполномоченного лица УЦ.

6.2.8. Срок создания и выдачи квалифицированного сертификата с момента получения Удостоверяющим центром ФБУРФЦСЭ при Минюсте России соответствующего заявления, а также условия для срочного создания и выдачи квалифицированного сертификата заявителю

Срок создания и выдачи сертификата не должен превышать 5 (пяти) рабочих дней с момента получения УЦ соответствующего заявления на создание квалифицированного сертификата ключа проверки электронной подписи.

Срок действия сертификата пользователя УЦ исчисляется с даты его создания и составляет не менее 1 (одного) года. Заданный срок действия сертификата определяет срок действия КЭП.

Возможно создание сертификата в течение тридцати минут с момента подачи заявления, при условии подтверждения всех фактов соответствия сведений в заявлении, предоставлении полного пакета запрашиваемых документов и личной явки будущего владельца сертификата за его получением.

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

6.3.1. Требования к заявлению на подтверждение действительности

электронной подписи, в том числе перечень прилагаемых к такому заявлению документов

Лицо, присоединившееся к Регламенту Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, вправе обратиться в УЦ за подтверждением действительности электронной подписи, использованной для подписания электронных документов. Для подтверждения действительности ЭП такое лицо подает в УЦ заявление на подтверждение действительности по форме, установленной приложением № 6 к настоящему Регламенту. Заявление подается в форме документа, оформленного надлежащим образом на бумажном носителе и заверенного собственноручной подписью обращающегося лица, при личном прибытии по месту нахождения офиса УЦ.

Обязательным приложением к заявлению на подтверждение действительности электронной подписи, использованной для подписания электронного документа, является носитель, содержащий сертификат, с использованием которого необходимо проверить действительность ЭП в электронном документе и электронный документ, содержащий данные и значение ЭП.

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

Срок предоставления услуги составляет 30 (тридцать) рабочих дней с момента поступления заявления в УЦ на безвозмездной основе.

6.3.3. Порядок оказания услуги

Оказание услуги по проверке действительности ЭП осуществляет комиссия, сформированная из числа работников УЦ. При оказании данного вида услуги УЦ проверяет действительность всех сертификатов, включенных в цепочку проверки для данного сертификата до сертификата УЦ, выданного ему головным УЦ.

По результатам оказания услуги оформляется справка, содержащая информацию о действительности ЭП, которая предоставляется заявителю, в частности:

- ЭП действительна/недействительна;
- на момент времени подписания электронного документа и времени, указанного в заявлении, сертификат пользователя УЦ действовал/не действовал;
- время и место проведения проверки;
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- содержание и результаты проверки с указанием примененных методов;
- обоснование результатов проверки;
- данные, представленные для проведения проверки.

6.4. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата ключа проверки электронной подписи

6.4.1. Основания прекращения действия или аннулирования квалифицированного сертификата

Сертификат прекращает свое действие:

1) по истечении срока его действия;

2) на основании заявления владельца на отзыв квалифицированного сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе в УЦ. Заявление в форме документа, на бумажном носителе и заверенного собственноручной подписью владельца ЭП, предоставляется по месту нахождения офиса УЦ.

Заявление на отзыв квалифицированного сертификата ключа проверки электронной подписи по инициативе владельца сертификата представляется в следующих случаях:

- в случае прекращения деятельности;
- в случае лишения владельца сертификата полномочий;
- в случае увольнения владельца сертификата;
- в случае изменения сведений, включенных в сертификат (при этом в течение пяти рабочих дней пользователем УЦ представляется соответствующее заявление на отзыв квалифицированного сертификата ключа проверки электронной подписи с последующим осуществлением смены сертификата);
- в случае компрометации КЭП владельца сертификата;
- выхода из строя ключевого носителя, содержащего КЭП владельца сертификата, при отсутствии учтенных резервных ключевых носителей КЭП;
- в иных случаях по решению владельца сертификата.

Форма заявления на отзыв квалифицированного сертификата ключа проверки электронной подписи приведена в приложении № 9 к настоящему Регламенту, заявление формируется и представляется на бумажном носителе.

3) в случае прекращения деятельности УЦ без передачи его функций другим лицам;

4) в иных случаях, установленных настоящим Регламентом и законодательством Российской Федерации в области электронной подписи.

УЦ аннулирует квалифицированный сертификат ключа проверки электронной подписи в следующих случаях:

1) не подтверждено, что владелец сертификата владеет КЭП, соответствующим КПЭП, указанному в таком сертификате;

2) установлено, что содержащийся в таком сертификате КПЭП уже содержится в ином ранее созданном сертификате;

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

6.4.2. Порядок действий Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России при прекращении действия (аннулировании) квалифицированного сертификата

Заявление на отзыв сертификата может подаваться в УЦ в бумажной форме при личном прибытии владельца ЭП в УЦ, а также в электронной форме, подписанное усиленной квалифицированной ЭП руководителя или лица, имеющего право действовать от имени организации по доверенности.

При обращении пользователя УЦ с заявлением на отзыв квалифицированного сертификата ключа проверки электронной подписи уполномоченный работник УЦ выполняет процедуру идентификации пользователя УЦ путем установления

личности по документам, удостоверяющим личность, а также подтверждаются полномочия владельца сертификата или его доверенного лица. Удостоверение личности и проверка полномочий осуществляются в порядке, предусмотренном для создания и выдачи квалифицированного сертификата ключа проверки электронной подписи в разделе 6.2 настоящего Регламента.

После положительной идентификации пользователя УЦ УЦ принимает заявление на отзыв квалифицированного сертификата ключа проверки электронной пользователя УЦ. Данное заявление подлежит проверке УЦ. При принятии положительного решения УЦ выполняет действия по отзыву сертификата ключа проверки электронной подписи пользователя УЦ с серийным номером, указанным в заявлении.

Информация об отзыве (прекращении действия) и аннулировании сертификата должна быть внесена УЦ в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в настоящем разделе, или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

Использование аннулированного сертификата не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием. До внесения в реестр сертификатов информации об аннулировании сертификата пользователя УЦ Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России обязан уведомить владельца сертификата КПЭП об аннулировании его сертификата КПЭП путем направления документа на бумажном носителе или электронного документа по электронному адресу пользователя УЦ, указанному в заявлении на создание квалифицированного сертификата ключа проверки ЭП.

Оповещение пользователей УЦ о прекращении действия (аннулировании) сертификатов производится путем публикации актуального списка отозванных и аннулированных сертификатов по адресу: http://www.sudexpert.ru/crl/ . САС актуализируется не реже двух раз в неделю.

6.5. Порядок ведения реестра квалифицированных сертификатов ключей проверки электронных подписей

6.5.1. Формы ведения реестра квалифицированных сертификатов

УЦ обязан вести реестр изготовленных и аннулированных им сертификатов. Реестр сертификатов 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.

Реестр сертификатов включает в себя информацию, содержащуюся в изготовленных УЦ сертификатах, информацию о датах прекращения (отзыве) действия или аннулирования сертификатов, а также об основаниях прекращения (отзыве) или аннулирования, а именно реестр сертификатов состоит из следующих разделов:

1) изготовленные (выданные) сертификаты;

2) аннулированные или отозванные (прекратившие свое действие) сертификаты.

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

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

Аккредитованный удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре квалифицированных сертификатов.

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

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

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

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

При прекращении действия и аннулировании сертификатов информация об этом должна быть внесена УЦ в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона «Об электронной подписи», или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств.

Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.

6.6. Порядок технического обслуживания реестра квалифицированных сертификатов ключей проверки электронных подписей

6.6.1. Максимальные сроки проведения технического обслуживания

Плановые технические работы по обслуживанию реестра сертификатов проводятся УЦ в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации) с целью минимизации и возможности исключения перерывов в работе при использовании сертификатов пользователями УЦ и в доступе к реестру сертификатов УЦ.

Внеплановые технические работы проводятся при появлении такой необходимости в оперативном режиме.

Максимальные сроки проведения технического обслуживания реестра сертификатов составляют не более 24 часов. Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин.

6.6.2. Порядок уведомления участников информационного взаимодействия о проведении технического обслуживания

УЦ информирует пользователей УЦ о проведении технического обслуживания путем публикации сообщения на официальном сайте УЦ http://www.sudexpert.ru/uc/.

7. Порядок исполнения обязанностей Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

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

УЦ осуществляет информирование пользователей УЦ об условиях и о порядке использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП, и о мерах, необходимых для обеспечения безопасности ЭП и их проверки в следующем порядке:

- в консультационном режиме при выдаче пользователю УЦ сертификата;
- одновременно с выдачей сертификата осуществляется выдача владельцу сертификата руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи, приведенного в приложении № 1 к настоящему Регламенту;
- одновременно с выдачей сертификата осуществляется выдача рекомендаций производителя средства электронной подписи по выбору ключевых носителей электронной подписи, приведенных в приложении № 10 к настоящему Регламенту.

7.2. Выдача по обращению заявителя средств электронной подписи

УЦ по обращению заявителя выдает средства электронной подписи, отвечающие требованиям:

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

– средства ЭП обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки;

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

Выдача средств ЭП осуществляется во временное пользование по письменному обращению владельца сертификата (заявителя). Форма заявления на выдачу средств ЭП приведена в приложении № 8 к настоящему Регламенту.

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

– показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписываемой с использованием указанных средств, лицу,

осуществляющему создание электронной подписи, содержание информации, подписание которой производится;

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

– однозначно показывать, что электронная подпись создана.

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

– показывать самостоятельно или с использованием программных, программно-аппаратных и технических средств, необходимых для отображения информации, подписанной с использованием указанных средств, содержание электронного документа, подписанного электронной подписью;

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

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

Средства ЭП должны в соответствии с частью 4 статьи 6 Федерального закона «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.

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

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

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

– при осуществлении доступа к средству электронной подписи аутентификация субъекта доступа должна проводиться до начала выполнения первого функционального модуля средства электронной подписи;

– механизмы аутентификации должны блокировать доступ этих субъектов к функциям средства ЭП при отрицательном результате аутентификации.

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

Средства электронной подписи аккредитованного УЦ и средства электронной подписи заявителя/владельца ЭП удовлетворяют требованиям Федерального закона

от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и требованиям приказа ФСБ РФ от 27 декабря 2011 г. №796.

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

Актуальность обеспечивается путем своевременного внесения записи о выпуске и аннулировании сертификата в реестр квалифицированных сертификатов. Режим защиты является общим требованием в отношении всей сферы применения электронной подписи, он обеспечивается посредством применения СКЗИ, способствующих защите информации от несанкционированного проникновения.

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

УЦ обеспечивает круглосуточную доступность реестра сертификатов в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания реестра сертификатов, при этом УЦ обязан обеспечить безвозмездный доступ в любое время в течение срока деятельности УЦ, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами. Информация, содержащаяся в реестре сертификатов, в том числе информация об аннулировании сертификата, предоставляется безвозмездно любому лицу.

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ФБУ РФЦСЭ при Минюсте России ключей электронных подписей

Требования к обеспечению конфиденциальности.

Необходимо немедленно обратиться в УЦ с заявлением на отзыв квалифицированного сертификата в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

Запрещается:

– оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, средства усиленной квалифицированной электронной подписи, 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 (на столе, подключенным к ПЭВМ и пр.);

– допускать использование ключей электронных подписей другими лицами без согласия владельца ЭП;

– применять ключ квалифицированной электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

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 установленным СКЗИ после ввода ключевой информации;

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

Сроки уничтожения ключей электронной подписи.

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

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

УЦ осуществляет регистрацию сертификата в единой системе идентификации и аутентификации в соответствии с ФЗ «Об электронной подписи». При выдаче каждого сертификата УЦ направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате, в частности:

- уникальный номер квалифицированного сертификата;

- дата начала и окончания действия квалифицированного сертификата;

- наименование выдавшего квалифицированный сертификат удостоверяющего центра.

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

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

7.8. 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

УЦ обязан предоставлять безвозмездно любому лицу по его обращению информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов (выражением выписки из реестра является список отозванных (аннулированных) сертификатов) и направляется обратившемуся лицу как почтовым отправлением, так и с использованием информационно-телекоммуникационных сетей (по выбору лица, обратившегося за получением информации из реестра сертификатов). Срок предоставления указанной информации не может превышать 7 (семи) рабочих дней для направления информации почтовым отправлением и 24 часов для направления выписки посредством информационно-телекоммуникационных сетей.

Выписка из реестра сертификатов позволяет определить действительность сертификатов владельцев. Доступ к информации организован в соответствии с защитой персональных данных согласно требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и предоставляется при условии владения необходимыми данными из сертификата.

Для получения информации необходимо предоставить:

- серийный номер сертификата;
  или
- ИНН заявителя;
- СНИЛС владельца;
- даты начала и окончания действия квалифицированного сертификата.

Также УЦ публикует перечень прекративших свое действие (аннулированных) квалифицированных сертификатов, позволяющий определить действительность сертификатов владельцев, на официальном сайте http://www.sudexpert.ru/crl/.

8. Персональные данные

8.1. Обработка персональных данных заявителей/владельцев

8.1.1. Цель обработки персональных данных в УЦ – исполнение требований Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»; изготовление и хранение сертификатов, изготовление списков аннулированных сертификатов, ведение реестра выданных и аннулированных сертификатов, подтверждение неотрекаемости от подачи заявления и запроса на сертификат, от получения сертификата, установление личности заявителя – физического лица, обратившегося за получением сертификата и подтверждения правомочия обращаться за получением сертификата.

8.1.2 Обработка персональных данных в УЦ осуществляется на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.1.3. Персональные данные, обрабатываемые УЦ: фамилия, имя, отчество, реквизиты основного документа, удостоверяющего личность (серия, номер, код подразделения, дата выдачи), место работы, адрес регистрации, должность, контактный телефон, СНИЛС, ИНН, адрес электронной почты и иные сведения, необходимые для исполнения целей настоящего Регламента УЦ.

8.1.4. Персональные данные, вносимые в сертификат, относятся к категории общедоступных.

8.1.5. УЦ осуществляет действия по сбору, систематизации, накоплению, использованию, хранению, уточнению, обновлению, изменению, использованию, блокированию, уничтожению персональных данных заявителя в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

8.1.7. Согласие на обработку персональных данных заявителя может быть отозвано по письменному заявлению в бумажном виде в произвольной форме при личном прибытии заявителя при удовлетворении которого, впоследствии УЦ аннулируются все выпущенные сертификаты данного заявителя, при этом УЦ вправе не прекращать их обработку до окончания срока действия согласия.

8.1.8. Согласие вступает в силу с момента его подписания, действует до истечения срока хранения информации, установленного п. 2 ст.15 Федерального закона от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Приложение № 1 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

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

1. Общие положения

Настоящее руководство составлено в соответствии с требованиями Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

При применении квалифицированной электронной подписи в информационных системах владельцу сертификата необходимо выполнять требования:

– Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, в части обращения со средствами криптографической защиты информации;

– Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 г. № 66, в части эксплуатации средств криптографической защиты информации;

– эксплуатационной документации к средствам электронной подписи;

– приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств вычислительной техники с установленными на них средствами квалифицированной электронной подписи:

– должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены средства квалифицированной электронной подписи, посторонним лицам, не имеющим допуск к работе в этих

помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями во избежание негативных воздействий с их стороны на средства электронной подписи, средства криптографической защиты и передаваемую информацию;

– внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

3. Требования по установке средств электронной подписи, общесистемного и специального программного обеспечения

3.1. При использовании средств электронной подписи должны выполняться следующие меры по защите информации от несанкционированного доступа:

3.1.1. Необходимо формировать пароли в соответствии со следующими правилами:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и т.д.), а также сокращения (USER, ADMIN, root, и т.д.);

– при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях;

– личный пароль пользователь не имеет права никому сообщать;

– периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

3.1.2. При использовании ключей электронных подписей средства вычислительной техники должны быть сконфигурированы с учетом следующих требований:

– не использовать нестандартные, измененные или отладочные версии операционных систем;

– исключить возможность загрузки и использования операционной системы, отличной от предусмотренной штатной работой;

– исключить возможность удаленного управления, администрирования и модификации операционной системы и ее настроек;

– на средствах вычислительной техники с установленными средствами квалифицированной электронной подписи должна быть установлена только одна операционная система;

– все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.);

– режимы безопасности, реализованные в операционной системе должны быть настроены на максимальный уровень;

– всем пользователям и группам, зарегистрированным в операционной системе, необходимо назначить минимально возможные для нормальной работы права;

– необходимо предусмотреть меры, максимально ограничивающие доступ к:

– системному реестру;

– файлам и каталогам;

– временным файлам;

– журналам системы;

– файлам подкачки;

– кэшируемой информации (пароли и т.п.);

– отладочной информации.

3.1.3. На средствах вычислительной техники необходимо:

– организовать удаление (по окончании сеанса работы средств квалифицированной электронной подписи) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе их работы. Если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;

– исключить попадание в систему программ, позволяющих использовать ошибки операционной системы, для повышения предоставленных привилегий;

– регулярно устанавливать пакеты обновлений безопасности операционной системы (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

3.1.4. В случае подключения технических средств с установленными средствами электронной подписи к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

3.1.5. Необходимо организовать и использовать:

– систему аудита, организовать регулярный анализ результатов аудита;

– комплекс мероприятий по антивирусной защите.

3.2. Запрещается:

– осуществлять несанкционированное копирование ключевых носителей;

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

– использовать ключевые носители в режимах, не предусмотренных штатным режимом использования ключевого носителя;

– вносить какие-либо изменения в программное обеспечение средств электронной подписи;

– записывать на ключевые носители постороннюю информацию;

– оставлять средства вычислительной техники с установленными средствами электронной подписи без контроля после ввода ключевой информации;

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован;

– удалять ключевую информацию с ключевого носителя до истечения срока действия, аннулирования или прекращения действия сертификата ключа проверки электронной подписи.

4. Требования по обеспечению информационной безопасности при обращении с носителями ключевой информации, содержащими ключи квалифицированной электронной подписи

4.1. Меры защиты ключей квалифицированной электронной подписи.

Ключи квалифицированной электронной подписи при их создании должны записываться на предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным владельцем сертификата.

Ключи квалифицированной электронной подписи на ключевом носителе могут быть защищены паролем (ПИН-кодом). При этом пароль (ПИН-код) формирует лицо, выполняющее процедуру генерации ключей, в соответствии с требованиями на используемое средство электронной подписи.

Ответственность за конфиденциальность сохранения пароля (ПИН-кода) возлагается на владельца ключа квалифицированной электронной подписи.

4.2. Обращение с ключевой информацией и ключевыми носителями.

Недопустимо пересылать файлы с ключевой информацией для работы в информационных системах по электронной почте сети Интернет или по внутренней электронной почте (кроме открытых ключей).

Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действии злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем и храниться в месте не доступном третьим лицам (сейф, опечатываемый бокс, закрывающийся металлический ящик и т.д.).

Носитель ключевой информации должен быть вставлен в считывающее устройство только на время выполнения средствами электронной подписи операций формирования и проверки квалифицированной электронной подписи, шифрования и дешифрования. Размещение носителя ключевой информации в считывателе на продолжительное время существенно повышает риск несанкционированного доступа к ключевой информации третьими лицами.

На носителе ключевой информации недопустимо хранить иную информацию (в том числе рабочие или личные файлы).

4.3. Обеспечение безопасности автоматизированного рабочего места с установленными средствами электронной подписи.

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования.

На технических средствах, используемых для работы в информационных системах:

– на учетные записи пользователей операционной системы должны быть установлены пароли, удовлетворяющие требованиям, приведенным в разделе 3 настоящего Руководства;

– должно быть установлено только лицензионное программное обеспечение;

– должно быть установлено лицензионное антивирусное программное обеспечение с регулярно обновляемыми антивирусными базами данных;

– должны быть отключены все неиспользуемые службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети, системные диски и т.д.);

– должны регулярно устанавливаться обновления операционной системы;

– должен быть исключен доступ (физический и/или удаленный) к техническим средствам с установленными средствами электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в соответствующей информационной системе;

– должна быть активирована регистрация событий информационной безопасности;

– должна быть включена автоматическая блокировка экрана после ухода ответственного работника с рабочего места.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства электронной подписи, необходимо гарантированно удалить всю информацию (при условии исправности технических средств), использование которой третьими лицами может потенциально нанести вред организации, в том числе средства электронной подписи, журналы работы систем обмена электронными документами и так далее.

Приложение № 2 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи
(для юридических лиц)

Удостоверяющему центру
ФБУ РФЦСЭ при Минюсте России

Заявление
на создание квалифицированного сертификата ключа проверки электронной подписи

Наименование организации: _____,
лицо, выступающее от имени организации:
_____
(фамилия, имя, отчество руководителя организации),
действует на основании: _____,
просит создать ключ электронной подписи и сертификат ключа проверки электронной подписи *(нужное подчеркнуть)* уполномоченного представителя:
_____
_____ *(фамилия, имя, отчество)*
в соответствии с указанными в настоящем заявлении данными:

Наименование организации, которую представляет владелец сертификата	Common Name	
СНИЛС владельца сертификата (представителя организации)	SNILS	
Фамилия владельца сертификата	Surname	
Имя и отчество владельца сертификата	Given Name	
Наименование организации, которую представляет владелец сертификата	Organization	
Наименование структурного подразделения организации, работником которого является владелец сертификата	Organization Unit	

Должность владельца сертификата	Title	
ИНН (индивидуальный номер налогоплательщика) организации — юридического лица	INN	
ОГРН (основной государственный регистрационный номер) организации — юридического лица	OGRN	
Страна (RU)	Country	
Субъект Российской Федерации, в котором зарегистрирована организация, индекс	State	
Наименование населенного пункта	LocalityName	
Адрес, улица	StreetAddress	
Адрес электронной почты	E-mail	
Контактный телефон	Phone number	

Настоящим

_____

(фамилия, имя, отчество)

_____

_____

(серия и номер паспорта, кем и кода выдан)

в соответствии с частью 4 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях получения квалифицированного сертификата ключа проверки электронной подписи даю согласие ФБУ РФЦСЭ при Минюсте России (адрес Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: 101000, г. Москва, Большой Спасоглинищевский переулок, дом 4) на обработку моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение, и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцем которых я являюсь, не считаются конфиденциальными.

Настоящее согласие действует со дня его подписания до дня предоставления соответствующего отзыва по письменному заявлению в бумажном виде в произвольной форме.

Информацию, указанную в заявлении, и подлинность предоставленных копий документов подтверждаю.

Подпись уполномоченного представителя _____ _____
(подпись) *(фамилия, инициалы)*

Руководитель организации _____ _____
(подпись) *(фамилия, инициалы)*

м.п.

«_____» _____ 20____ г.

Данное заявление зарегистрировано в реестре Удостоверяющего центра.
Рег.№_____ от «____»_____20__г.
Оператор _____/_____
(подпись) *(фамилия, инициалы)*

Форма заявления на создание квалифицированного сертификата ключа проверки электронной подписи

(для физических лиц)

Удостоверяющему центру
ФБУ РФЦСЭ при Минюсте России

Заявление на создание квалифицированного сертификата ключа проверки электронной подписи

_____

_____

_____

_____

(фамилия, имя, отчество, должность, структурное подразделение, наименование организации)

просит создать ключ электронной подписи и сертификат ключа проверки электронной подписи *(нужное подчеркнуть)* в соответствии с указанными в настоящем заявлении данными:

Фамилия, имя, отчество владельца сертификата	Common Name	
ИНН (индивидуальный номер налогоплательщика) владельца сертификата	INN	
СНИЛС (страховой номер индивидуального лицевого счета) владельца сертификата	SNILS	
Фамилия владельца сертификата	Surname	
Имя и отчество владельца сертификата	Given Name	
Страна (RU)	Country	
Субъект Российской Федерации, в котором зарегистрирован владелец сертификата, индекс	State	
Наименование населенного пункта	LocalityName	

Адрес, улица	StreetAddress	
Адрес электронной почты	E-mail	
Контактный телефон	Phone number	

Настоящим

_____

(фамилия, имя, отчество)

_____

_____

(серия и номер паспорта, кем и кода выдан)

в соответствии с частью 4 статьи 9 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», в целях получения квалифицированного сертификата ключа проверки электронной подписи даю согласие ФБУ РФЦСЭ при Минюсте России (адрес Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России: 101000, г. Москва, Большой Спасоглинищевский переулок, дом 4) на обработку моих персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, удаление, уничтожение, и признаю, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцем которых я являюсь, не считаются конфиденциальными.

Настоящее согласие действует со дня его подписания до дня предоставления соответствующего отзыва по письменному заявлению в бумажном виде в произвольной форме.

Информацию, указанную в заявлении, и подлинность предоставленных копий документов подтверждаю.

Подпись _____ _____

(подпись) (фамилия, инициалы)

«_____» _____ 20____ г.

Данное заявление зарегистрировано в реестре Удостоверяющего центра.

Рег.№_____ от «____»_____20__г.

Оператор _____/_____

(подпись) (фамилия, инициалы)

Приложение № 3 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма доверенности полномочного представителя юридического лица, наделенного правом выступать в роли пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Доверенность

_____ «_____» _____ 20___ г.

Наименование организации: _____, лицо, выступающее от имени организации: _____, действует на основании: _____, уполномочивает: _____ _____ *(фамилия, имя, отчество)* _____ _____ *(серия и номер паспорта, кем и когда выдан)* выступать в роли пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России с правом использования электронной подписи и получить на свое имя сертификат ключа проверки электронной подписи, а также осуществлять действия, предусмотренные Регламентом Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России.

Настоящая доверенность действительна по «____»_____ 20____г.*

Подпись уполномоченного представителя _____ _____
(подпись) *(фамилия, инициалы)*

подтверждаю.

_____ _____ _____
Должность руководителя организации *(подпись)* *(фамилия, инициалы)*

м.п.

Примечание: *- срок действия доверенности должен быть не менее срока действия сертификата ключа проверки электронной подписи

Приложение № 4 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма доверенности, выдаваемая полномочному представителю, на получение за владельца сертификата ключа проверки электронной подписи
(для юридического лица)

Доверенность

_____ «_____» _____ 20___ г.

Наименование организации: _____, лицо, выступающее от имени организации: _____, действует на основании: _____, уполномочивает:
_____
_____ *(фамилия, имя, отчество)*
_____
_____ *(серия и номер паспорта, кем и когда выдан)*

1. Предоставить в Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России документы, необходимые для создания сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России _____ *(фамилия, имя, отчество).*

2. Получить сертификат ключа проверки электронной подписи Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, сформированные ключ проверки и сертификат ключа проверки электронной подписи пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России _____ *(фамилия, имя, отчество).*

Доверенность выдана сроком на _____ без права передоверия.

Подпись уполномоченного
представителя _____ _____
(подпись) *(фамилия, инициалы)*

подтверждаю.

_____ _____ _____
Должность руководителя организации *(подпись)* *(фамилия, инициалы)*

м.п.

Приложение № 5 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма доверенности, выдаваемая полномочному представителю, на получение за владельца сертификата ключа проверки электронной подписи
(для физического лица)

Доверенность

_____ «_____» _____ 20___ г.

Я,_____
_____ *(фамилия, имя, отчество)*
_____
_____ *(серия и номер паспорта, кем и когда выдан)*
уполномочиваю
_____
_____ *(фамилия, имя, отчество)*
_____
_____ *(серия и номер паспорта, кем и когда выдан)*

1. Предоставить в Удостоверяющий центр ФБУ РФЦСЭ при Минюсте России документы, необходимые для создания сертификата ключа проверки электронной подписи на моѐ имя.

2. Получить сертификат ключа проверки электронной подписи Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, сформированные ключ проверки и сертификат ключа проверки электронной подписи на моѐ имя.

Доверенность выдана сроком на _____ без права передоверия.

Подпись уполномоченного
представителя _____ _____
(подпись) *(фамилия, инициалы)*

подтверждаю.

_____ _____
(подпись) *(фамилия, инициалы)*

«____» _____ 20____ г.

Приложение № 6 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма заявления на проверку действительности электронной подписи в электронном документе

Удостоверяющему центру
ФБУ РФЦСЭ при Минюсте России

Заявление на проверку действительности электронной подписи в электронном документе

_____
_____ *(Ф.И.О. для физического лица, полное наименование организации с указанием организационно-правовой формы)* в лице:
_____
_____ *(должность, Ф.И.О. (для юридических лиц))*, действующего на основании:_____

Просит проверить действительность электронной подписи в электронном документе на основании следующих данных:

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе на прилагаемом к заявлению носителе _____;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата, на носителе _____.

Серийный номер сертификата ключа проверки электронной подписи:
_____

Время* подписания электронной подписью электронного документа:
«_____ : _____ » «___ / _____ / _____»;
Час минута день месяц год

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

«_____ : _____ » «___ / _____ / _____»;

Час минута день месяц год

_____ _____

(подпись) *(фамилия, инициалы)*

М.П.

(для юридического лица)

«____» _____ 20____ г.

Примечание: * - Время и дата должны быть указаны с учетом часового пояса г. Москва.

Приложение № 7 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма акта передачи ключевого носителя

Акт передачи ключевого носителя № ____

г. Москва «____» _____ 20____ г.

Настоящий акт составлен о том, что в соответствии с разделом 5.1.1 Регламента Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, уполномоченный работник Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России в лице оператора Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

_____

ФИО полностью

изготовил, записал и передал, а

_____

Наименование организации-заявителя или ФИО физического лица

ИНН _____, ОГРН _____

организации-заявителя *организации-заявителя*

в лице _____

ФИО и должность владельца ключа электронной подписи

принял ключевой носитель, заводской номер № _____, содержащий ключ электронной подписи.

Согласен с фактом отсутствия нарушения конфиденциальности ключа электронной проверки

_____.

ФИО и подпись владельца ключа электронной подписи

Настоящий акт составлен в двух экземплярах, имеющих одинаковую юридическую силу: один экземпляр акта передается владельцу ключа электронной проверки, один экземпляр – Удостоверяющему центру ФБУ РФЦСЭ при Минюсте России.

Ключевой носитель передал:	Ключевой носитель принял:
_____	_____
_____	_____
ФИО полностью, подпись владельца ключа электронной подписи	*ФИО полностью, подпись оператора УЦ*
м.п.(для юридического лица)	м.п.

Приложение № 8 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма заявления на выдачу средств электронной подписи

Заявление на выдачу средств электронной подписи

_____ *(наименование организации-заявителя или ФИО физического лица)* в связи с присоединением к Регламенту Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России, утвержденному приказом ФБУ РФЦСЭ при Минюсте России от _____ № _____, просит предоставить:

1.Средство электронной подписи _____ *(наименование средства электронной подписи)* в количестве 1 шт. и лицензий на его использование в количестве __ шт.*

Количество получателей квалифицированных сертификатов ключей проверки электронной подписи __ работника (ов).

Лицо, уполномоченное на получение указанных средств и эксплуатационной документации к ним,

_____

_____

_____

(*ФИО, должность, наименование структурного подразделения).*

Должность руководителя
(уполномоченного лица) _____ _____

(подпись) *(фамилия, инициалы)*

«_____» _____ 20____ г.

Примечание: * - количество лицензий должно соответствовать количеству получателей квалифицированных сертификатов (владельцев сертификатов ключей проверки электронной подписи)

Приложение № 9 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Форма заявления на отзыв квалифицированного сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

Заявление
на отзыв квалифицированного сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра ФБУ РФЦСЭ при Минюсте России

_____

(наименование организации-заявителя или ФИО физического лица)

Прошу отозвать сертификат ключа проверки электронной подписи:

№ п/п	Серийный номер сертификата	Ф.И.О.	Код причины отзыва	Подпись владельца сертификата
1				
2				
3				

Код причины отзыва сертификата:
«1» Компрометация КЭП владельца сертификата,
«2» Лишения владельца сертификата полномочий,
«3» Изменения сведений, включенных в сертификат,
«4» Прекращения деятельности,
«5» Увольнение владельца сертификата,
«6» Выход из строя ключевого носителя, содержащего КЭП владельца сертификата, при отсутствии учтенных резервных ключевых носителей КЭП,
«7» в иных случаях по решению владельца сертификата

_____ _____/ _____/

руководитель организации (для юридического лица), должность (для физического лица) *подпись* *Ф.И.О.*

«_____» _____ 20____ г.

Приложение № 10 к Регламенту
УЦ ФБУ РФЦСЭ при Минюсте России

Рекомендации производителя средства электронной подписи по выбору ключевых носителей электронной подписи

Название семейства устройств в программе ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
UEC	Универсальная электронная карта (УЭК)	Необходимое ПО входит в поставку ViPNet CSP. В настройках ViPNet CSP должно быть запрещено использование устройств всех типов, кроме UEC. В качестве ПИН-кода используется код ПИН2 вашей карты. В качестве считывателя контактных смарт-карт рекомендуется использовать модель GemPC Twin от компании Gemalto или ACR38 от компании Advanced Card Systems Ltd.
ESMART Token	Смарт-карты и токены семейств ESMART Token, ESMART Token ГОСТ	На компьютере должно быть установлено ПО ESMART PKI Client (рекомендуемая версия — 4.0).
Infotecs Software Token	Infotecs Software Token — программная реализация стандарта PKCS#11	Необходимое ПО входит в поставку ViPNet CSP. С помощью программы token_manager.exe на компьютере должен быть создан виртуальный токен.
A-Key	Смарт-карты aKey S1000, aKey S1003, aKey S1004 производства компании Ak Kamal Security	На компьютере должна быть установлена библиотека akpkcs11.dll, предоставленная компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — 12345678. Перенос ключей подписи на данный тип устройств невозможен.
ViPNet HSM	Виртуальный токен ViPNet HSM производства ОАО «ИнфоТеКС»	Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен.
JaCarta	Персональные электронные ключи и смарт-карты JaCarta PKI производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО JC-Client компании «Аладдин Р.Д.» (рекомендуемая версия — 6.30.06).
JCDS	Смарт-карты Gemalto Optelio Contactless D72, KONA 131 72K и JaCarta	На карту должен быть загружен апплет Datastore, позволяющий

	LT с апплетом от компании «Аладдин Р.Д.»	модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой. Для администрирования смарт-карт JaCarta LT на компьютере должно быть установлено ПО JC-PROClient версии 1.5.0.199, рекомендуется использовать модуль сопряжения jcpkcs11ds.dll версии 1.1.3.20.
Siemens CardOS	Смарт-карты CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4 производства компании Atos (Siemens)	На компьютере должно быть установлено ПО Siemens CardOS API V5.0. Смарт-карты должны быть особым образом размечены. Обратитесь к производителю устройств.
eToken GOST/ JaCarta GOST	Персональные электронные ключи eToken ГОСТ и JaCarta ГОСТ производства компании «Аладдин Р.Д.»	Для работы с указанными устройствами на компьютере должно быть установлено ПО JC-GOST Client (рекомендуемая версия —1.5.3.446). Перенос ключей подписи на данный тип устройств невозможен.
Rutoken ECP/ Rutoken Lite	Электронные идентификаторы Рутокен ЭЦП и Рутокен Lite производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 2.100.00.0542). Перенос ключей подписи на идентификаторы Рутокен ЭЦП невозможен.
Rutoken/ Rutoken S	Электронные идентификаторы Рутокен и Рутокен S производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 2.100.00.0542).
eToken Aladdin	Персональные электронные ключи eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO, JaCarta PRO производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено ПО PKI Client версии 5.1 SP1. Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. Для работы смарт-карты JaCarta PRO на компьютере должно быть установлено ПО JC-PROClient версии 1.0.6 и должен быть включен режим совместимости с eToken.