МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ КАЗНАЧЕЙСТВО
(КАЗНАЧЕЙСТВО РОССИИ)

ПРИКАЗ

25 июля 2016 г. № 280

Москва

О внесении изменений в приложение к приказу Федерального казначейства от 31 июля 2015 г. № 197 «Об утверждении Регламента Удостоверяющего центра Федерального казначейства»

В целях реализации положений Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2016, № 1, ст. 65) и в соответствии с пунктом 5.18(2) Положения о Федеральном казначействе, утвержденного постановлением Правительства Российской Федерации от 1 декабря 2004 г. № 703 «О Федеральном казначействе» (Собрание законодательства Российской Федерации, 2004, № 49, ст. 4908; Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 7 июля 2016 г.), п р и к а з ы в а ю:

1. Приложение к приказу Федерального казначейства от 31 июля 2015 г. № 197 «Об утверждении Регламента Удостоверяющего центра Федерального казначейства» изложить в новой редакции согласно приложению к настоящему приказу.

2. Территориальным органам Федерального казначейства обеспечить уведомление юридических лиц, с которыми заключены Договоры присоединения (Соглашения) к Регламенту Удостоверяющего

центра Федерального казначейства, о соответствующих изменениях до вступления в силу настоящего приказа.

3. Настоящий приказ вступает в силу с 1 сентября 2016 года.

4. Контроль за исполнением настоящего приказа возложить на заместителя руководителя Федерального казначейства С.Б. Гуральникова.

Руководитель  Р.Е. Артюхин

Приложение к приказу
Федерального казначейства
от «25» июля 2016 г. №280

УТВЕРЖДЕН

Приказом
Федерального казначейства
от 31.07.2015 № 197

РЕГЛАМЕНТ
Удостоверяющего центра Федерального казначейства

1. Сокращения

№ п/п	Сокращение	Значение
1	УЦ	Удостоверяющий центр
2	Средство создания запроса	Средство создания КЭП, Запроса на сертификат, Заявления на сертификат
3	Сертификат	Квалифицированный сертификат ключа проверки электронной подписи
4	ИНН	Идентификационный номер налогоплательщика
5	ОГРН	Основной государственный регистрационный номер
6	КПП	Код причины постановки на учет в налоговых органах
7	ТОФК	Территориальный орган Федерального казначейства
8	ЭП	Электронная подпись
9	ФК	Федеральное казначейство
10	КЭП	Ключ электронной подписи
11	КПЭП	Ключ проверки электронной подписи
12	СНИЛС	Страховой номер индивидуального лицевого счета
13	САС	Список аннулированных сертификатов
14	АРМ	Автоматизированное рабочее место
15	Заявление на сертификат	Заявление на получение сертификата в УЦ ФК
16	Заявление на изменение статуса сертификата	Заявление на приостановление/возобновление/прекращение действия сертификата
17	Заявление о статусе сертификата	Заявление на получение информации о статусе сертификата
18	Реестр сертификатов	Реестр выданных и аннулированных УЦ ФК сертификатов
19	ЕГРЮЛ	Единый государственный реестр юридических лиц
20	ЕСИА	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»

2. Термины и определения

Запрос на сертификат – файл, созданный с использованием средств ЭП, содержащий КПЭП и иную информацию об Организации-заявителе и (или) Заявителе.

Заявитель – сотрудник Организации-заявителя, обратившийся за получением сертификата, фамилия, имя, отчество (если имеется) которого указаны в Запросе на сертификат.

Компрометация КЭП – ознакомление неуполномоченного лица (лиц) с КЭП; потеря ключевого носителя; нарушение правил хранения и уничтожения КЭП (после окончания срока действия); нарушение печати на сейфе с ключевыми носителями; случаи, когда невозможно 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).

Конфликтная ситуация – возникновение разногласий между владельцем сертификата и УЦ ФК.

Организация-заявитель – юридическое лицо, обратившееся за получением сертификата(ов).

Печать – печать с воспроизведением Государственного герба Российской Федерации или иная печать Организации-заявителя, содержащая ее наименование и используемая для заверения подлинности подписи лица, имеющего право действовать от имени Организации-заявителя в соответствии с гражданским законодательством Российской Федерации.

Список аннулированных сертификатов (САС) – электронный документ, подписанный ЭП УЦ ФК, представляющий собой список серийных номеров сертификатов, которые были аннулированы или действие которых было прекращено/приостановлено.

Уполномоченное лицо – сотрудник Организации-заявителя, наделенный правом обращаться в УЦ ФК на основании доверенности, оформленной в соответствии с требованиями законодательства Российской Федерации, или иного документа.

Лицо, действующее от имени Организации-заявителя – лицо, уполномоченное действовать от имени Организации-заявителя на основании документа, подтверждающего данные полномочия, либо в случае наличия сведений о таком лице и его полномочиях в ЕГРЮЛ, либо информации об источнике опубликования и (или) общедоступных изданиях и информационных системах, в которых размещены сведения о таком лице и его полномочиях.

Копия документа, удостоверяющего личность – копия паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность, в соответствии с законодательством Российской Федерации,

содержащая фамилию, имя, отчество (если имеется) и реквизиты данного документа.

3. Общие положения

3.1. Регламент Удостоверяющего центра Федерального казначейства (далее – Регламент) определяет:

– порядок выдачи средства ЭП и Средства создания запроса;

– порядок создания, выдачи, смены, прекращения действия, аннулирования, приостановления и возобновления действия сертификатов;

– порядок предоставления информации о статусе сертификатов.

3.2. 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), постановлением Правительства Российской Федерации от 1 декабря 2004 г. № 703 «О Федеральном казначействе» (в редакции постановления Правительства Российской Федерации от 13 апреля 2016 г. № 300), приказом Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», приказом Федерального казначейства от 11 сентября 2013 г. № 182 «Об организации работы Удостоверяющего центра Федерального казначейства» (в редакции приказа Федерального казначейства от 27 ноября 2015 г. № 323).

В настоящем Регламенте используются понятия, термины, сокращения, которые применяются в Федеральном законе от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

При возникновении вопросов, не урегулированных положениями Регламента, следует руководствоваться законодательством Российской Федерации.

3.3. Взаимодействие ТОФК и Организации-заявителя осуществляется на основании заключенного Договора присоединения (Соглашения) к Регламенту Удостоверяющего центра Федерального казначейства[1] (далее – Соглашение).

3.4. Создание и выдача сертификата осуществляется при условии наличия у Организации-заявителя:

– средства ЭП и Средства создания запроса;

– ключевого носителя, удовлетворяющего следующим требованиям:

– тип ключевого носителя включен в Перечень ключевых носителей, поддерживаемых УЦ ФК, определяемый УЦ ФК и

[1] Примерный образец представлен в приложении № 1 к настоящему Регламенту.

публикуемый на официальных сайтах ТОФК в разделе «Удостоверяющий центр»;

– ключевой носитель проинициализирован (отформатирован);

– на ключевом носителе имеется маркировка с учетным номером, присвоенным Организацией-заявителем.

3.5. Срок действия КЭП составляет максимально допустимый срок действия КЭП, установленный эксплуатационной документацией для используемого средства ЭП. Начало периода действия КЭП владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата.

3.6. Срок изготовления сертификата не должен превышать пяти рабочих дней с даты приема документов, оформленных в соответствии с настоящим Регламентом.

3.7. УЦ ФК предоставляет доступ к информации об аннулированных и прекративших действие сертификатах путем размещения актуального САС на официальном сайте Федерального казначейства в информационно-телекоммуникационной сети «Интернет» по адресу URL=http://crl.roskazna.ru/crl/.

Информация о размещении САС заносится в поле CRL Distribution Point сертификатов, изданных УЦ ФК.

Публикация обновленного САС УЦ ФК осуществляется регулярно, не реже двух раз в сутки.

3.8. Уведомление Организации-заявителя, Заявителя, владельцев сертификатов производится в случаях, предусмотренных настоящим Регламентом, любым способом, удостоверяющим его получение, в том числе посредством доставки сообщения по электронной почте на адрес, указанный в Заявлении на сертификат и в сертификате.

В случае превышения срока изготовления сертификата, Заявитель (Уполномоченное лицо), Организация-заявитель уведомляется в письменной форме за подписью руководителя ТОФК или его заместителя.

3.9. За неисполнение либо ненадлежащее исполнение правил настоящего Регламента Организация-заявитель, Заявитель (Уполномоченное лицо), владелец сертификата, УЦ ФК несут ответственность в соответствии с законодательством Российской Федерации.

4. Средство ЭП и Средство создания запроса

4.1. Требования к средству ЭП.

4.1.1. Средство ЭП должно обеспечивать работу с сертификатами формата X.509 версии 3, определенного рекомендациями «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» (RFC 5280), и соответствовать требованиям к средствам ЭП, устанавливаемым законодательством Российской Федерации.

4.2. Прием документов для выдачи средства ЭП и Средства создания запроса.

4.2.1. Выдача средства ЭП, Средства создания запроса и эксплуатационной документации к ним производится во временное пользование по письменному обращению Организации-заявителя, оформленному на бланке Организации-заявителя, в количестве, не превышающем число планируемых Заявителей, с приложением оптического носителя информации с возможностью однократной записи. В письменном обращении указывается фамилия, имя, отчество (при наличии) лица, уполномоченного на получение средства ЭП и Средства создания запроса.

4.2.2. Срок подготовки для выдачи средства ЭП, Средства создания запроса и эксплуатационной документации к ним не должен превышать трех рабочих дней с даты приема письменного обращения Организации-заявителя и оптического носителя.

4.3. Выдача средства ЭП и Средства создания запроса.

4.3.1. При выдаче средства ЭП и Средства создания запроса Оператор УЦ осуществляет:

– идентификацию лица, указанного в письменном обращении Организации-заявителя, по основному документу, удостоверяющему личность;

– выдачу оптического носителя информации (с записанной копией дистрибутива средства ЭП, Средства создания запроса) и учетной карточки лицензий на право использования средства ЭП и Средства создания запроса под подпись в соответствующем журнале.

4.4. Эксплуатация средства ЭП.

4.4.1. Установка, настройка и дальнейшее сопровождение средства ЭП проводится Организацией-заявителем самостоятельно в соответствии с требованиями эксплуатационной документации к нему и законодательства Российской Федерации. Установка средства ЭП оформляется Актом установки средства электронной подписи[2], второй экземпляр которого направляется в УЦ ФК (по месту получения средства ЭП) не позднее десяти рабочих дней с даты установки средства ЭП.

4.4.2. Средство ЭП деинсталлируется с рабочих станций, а оптические носители информации с копиями дистрибутивов и Формуляры уничтожаются комиссией Организации-заявителя с оформлением Акта уничтожения средства ЭП[3] в случае прекращения полномочий, ликвидации или реорганизации Организации-заявителя, расторжения Соглашения или при необходимости замены на другое средство ЭП. Один экземпляр акта передается в ТОФК (по месту получения средства ЭП) не позднее десяти рабочих дней с даты уничтожения.

---

[2] Примерный образец представлен в приложении № 5 к настоящему Регламенту.

[3] Примерный образец представлен в приложении № 6 к настоящему Регламенту.

5. Порядок создания и выдачи сертификата

5.1. УЦ ФК осуществляет создание и выдачу сертификатов Заявителю и Организации-заявителю.

5.2. Создание и выдача сертификата производится в следующем порядке:

5.2.1. Заключение Соглашения в соответствии с пунктом 3.3 настоящего Регламента.

5.2.2. Выдача средства ЭП и Средства создания запроса в соответствии с пунктами 4.2–4.3 настоящего Регламента (при необходимости).

5.2.3. Создание КЭП и Запроса на сертификат.

Создание КЭП и Запроса на сертификат производится одним из следующих способов:

– Заявителем (Уполномоченным лицом) на АРМ Организации-заявителя;

– Заявителем в присутствии Оператора УЦ на АРМ ТОФК.

Создание КЭП и Запроса на сертификат производится в условиях, исключающих нарушение конфиденциальности КЭП.

5.2.4. Формирование Заявления на сертификат.

Заявление на сертификат формируется Средством создания запроса на сертификат в автоматизированном режиме.

Заявление на сертификат на бумажном носителе подписывается Заявителем и лицом, действующим от имени Организации-заявителя, а также заверяется печатью. Подписание Заявителем Заявления на сертификат на бумажном носителе подтверждает, в том числе, факт того, что он владеет КЭП, соответствующим КПЭП, указанному в таком заявлении.

5.2.5. Комплект документов и сведений, необходимых для получения сертификата (далее – Документы на получение сертификата).

Для получения сертификата Заявителя, Организации-заявителя представляются:

– Заявление на сертификат[4], оформленное в соответствии с пунктом 5.2.4 настоящего Регламента;

– копия документа, удостоверяющего личность Заявителя, с представлением его оригинала либо копии, заверенной в установленном порядке, для визуального контроля с целью сличения;

– согласие Заявителя на обработку персональных данных, содержащихся в копии документа, удостоверяющего личность, оформленное в соответствии с требованиями Закона о персональных данных;

– номер страхового свидетельства государственного пенсионного страхования Заявителя с представлением страхового свидетельства

[4] Примерный образец представлен в приложении № 2 к настоящему Регламенту.

государственного пенсионного страхования либо его копии, заверенной в установленном порядке, для визуального контроля с целью сличения;

– файл Запроса на сертификат на съемном носителе информации, не содержащем КЭП;

– доверенность или иной документ Организации-заявителя, подтверждающие полномочия Заявителя и Уполномоченного лица на:

– владение сертификатом(ами);

– представление в УЦ ФК комплекта(ов) документов и сведений, необходимых для получения сертификата, изменения статуса сертификата (ов), предусмотренного(ых) настоящим Регламентом;

– ознакомление с информацией, содержащейся в получаемом(ых) сертификате(ах);

– получение руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи.

В случае обращения за сертификатом Заявителя дополнительно представляется идентификационный номер налогоплательщика – Заявителя с представлением свидетельства о постановке на учет физического лица в налоговом органе либо его копии, заверенной в установленном порядке, для визуального контроля с целью сличения.

В случае получения сертификата Организации-заявителя, который будет использоваться для автоматического создания и (или) автоматической проверки электронных подписей в информационных системах, без указания фамилии, имени, отчества (если имеется) владельца сертификата, представление копии документа, удостоверяющего личность Заявителя, и номера страхового свидетельства государственного пенсионного страхования Заявителя не требуется.

Документы на получение сертификата представляются Заявителем либо Уполномоченным лицом. В случае подачи документов Уполномоченным лицом дополнительно необходимо представление следующих документов:

– копия документа, удостоверяющего личность Уполномоченного лица, с представлением его оригинала либо копии, заверенной в установленном порядке, для визуального контроля с целью сличения;

– согласие Уполномоченного лица на обработку персональных данных, содержащихся в копии документа, удостоверяющего личность, оформленное в соответствии с требованиями Закона о персональных данных.

В случае отказа Заявителя (Уполномоченного лица) представить вышеуказанные документы и сведения, изготовление сертификата не производится.

Организация-заявитель вправе по собственной инициативе представить копии документов, содержащих сведения, указанные в пункте 4 части 2

статьи 18 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

В случае подписания документов, предусматривающих подпись руководителя, лицом, действующим от имени Организации-заявителя, дополнительно необходимо представление соответствующего документа или сведений (информации об официальном источнике опубликования и (или) общедоступных изданиях и информационных системах), подтверждающих полномочия данного лица.

Доверенности или иные документы, подтверждающие полномочия, копии документов, удостоверяющих личность, согласия на обработку персональных данных, Заявления на получение сертификата, файлы Запросов на сертификат, сведения, представленные Заявителем, Уполномоченным лицом, хранятся в УЦ ФК с учетом требований Закона о персональных данных.

5.2.6. Прием и проверка Документов на получение сертификата.

При приеме Документов на получение сертификата Оператор УЦ осуществляет идентификацию Заявителя (Уполномоченного лица) по основному документу, удостоверяющему личность, а также проверяет правильность формирования и представления сведений и подтверждающих документов в части:

– полноты комплекта Документов на получение сертификата;

– соответствия сведений, указанных в Заявлении на сертификат, сведениям в документах, указанных в пункте 5.2.5 настоящего Регламента, ЕГРЮЛ;

– отсутствия в представленных Документах на получение сертификата исправлений, не заверенных в установленном порядке;

– заверения копий документов в установленном порядке;

– соответствия значений полей электронной формы Запроса на сертификат значениям полей Заявления на получение сертификата;

– соответствия полномочий лица действовать от имени Организации-заявителя без доверенности сведениям из ЕГРЮЛ либо источников официального опубликования правовых актов.

Копия документа, удостоверяющего личность Заявителя (Уполномоченного лица), по результатам сличения заверяется подписями Заявителя (Уполномоченного лица) и Оператора УЦ.

В случае отрицательного результата проверки Документов на получение сертификата, Оператор УЦ отказывает в приеме документов и возвращает с мотивированным отказом в письменной форме, заверенным подписью Оператора УЦ и печатью УЦ.

В случае положительного результата проверки Документов на получение сертификата Оператор УЦ выполняет необходимые действия по созданию сертификата.

Ошибки в Документах на получение сертификата на бумажном носителе исправляются путем зачеркивания тонкой чертой неправильного текста так, чтобы можно было прочитать зачеркнутое, и написания над зачеркнутым исправленного текста. Исправление ошибки в документе на бумажном носителе должно быть оговорено надписью «исправлено», подтверждено подписью тех же лиц, которые подписали документ, с проставлением даты исправления.

5.2.7. Выдача сертификата Заявителю, Организации-заявителю, Уполномоченному лицу.

Оператор выдает владельцу сертификата (Уполномоченному лицу) файл сертификата и два экземпляра на бумажном носителе[5], каждый из которых подписывается Оператором УЦ и владельцем сертификата (Уполномоченным лицом), тем самым последний знакомится с информацией, содержащейся в сертификате. Один экземпляр сертификата остается в УЦ ФК.

Одновременно с выдачей сертификата Оператор УЦ под расписку в соответствующем журнале УЦ ФК выдает Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи[6].

При выдаче сертификата в ЕСИА направляются сведения о владельце сертификата в объеме, необходимом для регистрации в данной системе, и о полученном им сертификате (уникальный номер сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра)[7]. По желанию Заявителя, безвозмездно осуществляется его регистрация в ЕСИА.

6. Смена сертификата

6.1. Смена сертификата осуществляется не ранее двадцати календарных дней до окончания срока его действия на основании обращения владельца сертификата (Уполномоченного лица) по месту получения сертификата.

6.2. Процедура смены сертификата производится в порядке, предусмотренном пунктами 5.2.3–5.2.7 настоящего Регламента, при этом

---

[5] Образец представлен в приложении № 8 к настоящему Регламенту.

[6] Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи представлено в приложении № 3 к настоящему Регламенту.

[7] При наличии технической возможности.

повторная выдача Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи не производится.

В срок, не превышающий пяти рабочих дней с даты поступления документов, УЦ ФК уведомляет владельца сертификата о готовности сертификата либо об отказе в выдаче сертификата.

Повторное представление Документов на получение сертификата не требуется в случае отсутствия изменений в ранее представленных в УЦ ФК Документах на получение сертификата.

7. Прекращение действия, аннулирование, приостановление и возобновление действия сертификата

7.1. Сертификат прекращает свое действие:

– в автоматическом режиме в связи с истечением установленного срока его действия;

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

– на основании Заявления на изменение статуса сертификата[8]:

– в случае изменения сведений, включенных в сертификат (при этом владелец сертификата в течение пяти рабочих дней представляет соответствующее Заявление на изменение статуса сертификата с последующим осуществлением смены сертификата);

– в случае компрометации КЭП владельца сертификата, Оператора УЦ;

– выхода из строя ключевого носителя, содержащего КЭП владельца сертификата, при отсутствии учтенных резервных ключевых носителей КЭП;

– в случае ликвидации, реорганизации владельца сертификата;

– в случае увольнения владельца сертификата;

– в иных случаях по решению владельца сертификата или Организации-заявителя.

Заявление на изменение статуса сертификата Заявителя подписывается владельцем сертификата, лицом, действующим от имени Организации-заявителя.

Заявление на изменение статуса сертификата представляется владельцем сертификата (Уполномоченным лицом) в форме документа на

---

[8] Образец представлен в приложении № 4 к настоящему Регламенту.

бумажном носителе или в форме электронного документа[9] и хранится в УЦ ФК с учетом требований Закона о персональных данных.

В случае представления Заявления на изменение статуса сертификата Уполномоченным лицом повторное представление доверенности или иного документа, подтверждающего право действовать от имени владельца сертификата, не требуется при наличии в УЦ ФК актуальной версии данного документа.

Заявление на изменение статуса сертификата проверяется Оператором УЦ на предмет соответствия реквизитов, указанных в Заявлении, данным Реестра сертификатов. В случае выявления несоответствия реквизитов, Заявление на изменение статуса сертификата отклоняется посредством уведомления владельца сертификата (Уполномоченного лица) с указанием причины отказа.

7.2. Аннулирование сертификата осуществляется в следующих случаях:

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

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

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

7.3. Информация о прекращении действия сертификата вносится в Реестр сертификатов, САС в течение двенадцати часов с момента наступления обстоятельств, указанных в пунктах 7.1 и 7.2 настоящего Регламента, или в течение двенадцати часов с момента, когда УЦ ФК стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

Официальным уведомлением о факте аннулирования сертификата является опубликование САС, содержащего сведения об аннулированном сертификате.

7.4. Приостановление действия сертификата может осуществляться по инициативе его владельца на период возможного длительного неисполнения обязанностей, связанных с использованием сертификата, непредставления Организацией-заявителем, владельцем сертификата Акта установки средства ЭП в срок, определенный пунктом 4.4.1 настоящего Регламента, а также до урегулирования конфликтной ситуации в случае письменного обращения Организации-заявителя.

---

[9] При наличии технической возможности.

Приостановление действия сертификата может осуществляться на основании устного обращения его владельца, в том числе по телефону[10], или посредством подачи Заявления на изменение статуса сертификата[11], представленного владельцем сертификата (Уполномоченным лицом), на бумажном носителе.

7.4.1. Приостановление действия сертификата по устному обращению владельца сертификата возможно исключительно при возникновении обстоятельств, требующих оперативного приостановления действия сертификата на период урегулирования конфликтной ситуации.

При устном обращении владелец сертификата должен сообщить Оператору УЦ следующую информацию о сертификате, действие которого необходимо приостановить:

– фамилию, имя, отчество (если имеется) / наименование юридического лица владельца сертификата;

– уникальный номер сертификата;

– причину, по которой действие сертификата приостанавливается;

– ключевую фразу (кодовое слово).

Обращение в устной форме принимается к исполнению Оператором УЦ только в случае совпадения информации, переданной в обращении, с информацией из Реестра сертификатов.

В случае несовпадения информации, переданной владельцем сертификата, с информацией из Реестра сертификатов владелец сертификата уведомляется об этом с указанием причины.

В случае совпадения информации, переданной владельцем сертификата, с информацией, содержащейся в Реестре сертификатов, Оператор УЦ приостанавливает действие сертификата на срок, определенный в обращении.

Приостановление действия сертификата на основании устного обращения осуществляется в день обращения и не должно превышать 10 рабочих дней со дня обращения.

Владелец сертификата в срок, не превышающий 10 календарных дней с даты устного обращения, обязан представить в УЦ ФК Заявление на изменение статуса сертификата в зависимости от результата отработки причин, повлекших приостановление действия сертификата.

В случае непредставления Заявления на изменение статуса сертификата, в установленный срок, сертификат возобновляет действие, с уведомлением об этом владельца сертификата.

---

[10]Телефонные обращения владельцев сертификатов принимаются Операторами УЦ в соответствии с порядком, установленным ТОФК.

[11]Образец представлен в приложении № 4 к настоящему Регламенту.

7.4.2. Приостановление действия сертификата на основании Заявления на изменение статуса сертификата владельца сертификата (Уполномоченного лица), направленного на бумажном носителе, осуществляется на срок не более 56 календарных дней. Минимальный срок приостановления действия сертификата на основании Заявления на изменение статуса сертификата составляет 10 календарных дней.

Заявление на изменение статуса сертификата представляется владельцем сертификата (Уполномоченным лицом) в форме документа на бумажном носителе и хранится в УЦ ФК с учетом требований Закона о персональных данных.

В случае представления Заявления на изменение статуса сертификата Уполномоченным лицом повторное представление доверенности или иного документа, подтверждающего право действовать от имени владельца сертификата, не требуется при наличии в УЦ ФК актуальной версии данного документа.

Оператор УЦ при приеме Заявления на изменение статуса сертификата осуществляет:

– идентификацию Заявителя (Уполномоченного лица) по основному документу, удостоверяющему личность;

– проверку соблюдения требований порядка оформления и подписания Заявления на изменение статуса сертификата.

Заявление на изменение статуса сертификата проверяется Оператором УЦ на предмет соответствия реквизитов, указанных в Заявлении, данным Реестра сертификатов. В случае выявления несоответствия реквизитов Заявление на изменение статуса сертификата отклоняется. Владелец сертификата уведомляется с указанием причины отказа.

В случае положительного результата проверки действие сертификата приостанавливается, а его владелец уведомляется.

Уведомлением о приостановлении действия сертификата является опубликование САС, содержащего сведения о приостановленном сертификате.

7.5. Возобновление действия сертификата возможно исключительно в период приостановления его действия.

Возобновление действия приостановленного сертификата осуществляется при условии, что срок, на который действие сертификата было приостановлено, не истек.

Возобновление действия сертификата осуществляется на основании Заявления на изменение статуса сертификата на бумажном носителе.

Заявление на изменение статуса сертификата представляется владельцем сертификата (Уполномоченным лицом) в форме документа на

бумажном носителе и хранится в УЦ ФК с учетом требований Закона о персональных данных.

В случае представления Заявления на изменение статуса сертификата Уполномоченным лицом повторное представление доверенности или иного документа, подтверждающего право действовать от имени владельца сертификата, не требуется при наличии в УЦ ФК актуальной версии данного документа.

Оператор УЦ при приеме Заявления на изменение статуса сертификата осуществляет:

– идентификацию владельца сертификата (Уполномоченного лица) по основному документу, удостоверяющему личность;

– проверку соблюдения требований порядка оформления и подписания Заявления на изменение статуса сертификата.

Заявление на изменение статуса сертификата проверяется Оператором УЦ на предмет соответствия реквизитов, указанных в Заявлении, данным Реестра сертификатов.

В случае выявления несоответствия реквизитов Заявление на изменение статуса сертификата отклоняется с уведомлением владельца сертификата.

В случае положительного результата проверки действие приостановленного сертификата возобновляется с уведомлением владельца сертификата.

Возобновление действия сертификата либо отказ в возобновлении действия сертификата, включая уведомление владельца сертификата, осуществляется в течение одного рабочего дня, следующего за днем принятия заявления.

Уведомлением о возобновлении действия сертификата является опубликование САС, не содержащего сведений о возобновленном сертификате.

8. Предоставление информации о статусе сертификата

8.1. Предоставление информации о статусе сертификата, изданного УЦ ФК, осуществляется на основании Заявления о статусе сертификата[12].

Заявление о статусе сертификата представляется на бумажном носителе владельцем сертификата (Уполномоченным лицом) в УЦ ФК.

Заявление о статусе сертификата проверяется Оператором УЦ на предмет соответствия реквизитов, указанных в Заявлении о статусе сертификата, данным Реестра сертификатов.

Заявление о статусе сертификата принимается к исполнению в случае совпадения информации о сертификате, его владельце, указанной в Заявлении о статусе сертификата, с информацией из Реестра сертификатов.

---

[12]Образец представлен в приложении № 7 к настоящему Регламенту.

Информация о статусе сертификата направляется в виде Справки о статусе сертификата. Справка оформляется в соответствии с требованиями Инструкции по делопроизводству в ТОФК.

Справка о статусе сертификата должна содержать следующие обязательные сведения: уникальный номер, сведения о владельце, статус сертификата на запрошенный момент времени.

Справка о статусе сертификата направляется в форме документа на бумажном носителе посредством почтовой связи.

Представление Справки о статусе сертификата должно быть осуществлено не позднее 7 рабочих дней с даты официальной регистрации Заявления о статусе сертификата.

Приложение № 1
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

ДОГОВОР ПРИСОЕДИНЕНИЯ (СОГЛАШЕНИЕ) № _____
К РЕГЛАМЕНТУ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА

г. _____ «__» _____ 20__г.

_____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Орган ФК», с одной стороны, и _____, в лице _____, действующего на основании _____, именуем____ в дальнейшем «Организация-заявитель», с другой стороны, вместе именуемые «Сторонами», заключили настоящий договор (далее – Соглашение) о нижеследующем.

I. Предмет Соглашения

1.1. Предметом настоящего Соглашения является присоединение Организации-заявителя в порядке статьи 428 Гражданского кодекса Российской Федерации к Регламенту Удостоверяющего центра Федерального казначейства (далее – Регламент).

II. Права, обязанности и ответственность Сторон

2.1. Права, обязанности и ответственность Сторон определяются Регламентом и настоящим Соглашением.

III. Заключительные положения

3.1. Настоящее Соглашение вступает в силу с даты его подписания Сторонами и действует до его расторжения по основаниям, предусмотренным законодательством Российской Федерации, или по решению любой из Сторон, подписавших Соглашение, в одностороннем внесудебном порядке.

IV. Адреса и реквизиты Сторон

Орган Федерального казначейства:	Организация-заявитель:
Руководитель (уполномоченное лицо)	Руководитель (уполномоченное лицо)

Приложение № 2
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Заявление на получение квалифицированного сертификата ключа проверки электронной подписи в Удостоверяющем центре Федерального казначейства

На основании договора присоединения (соглашения) от_____№_____к регламенту Удостоверяющего центра Федерального казначейства и доверенности* от_____№_____, прошу выдать квалифицированный сертификат ключа проверки электронной подписи (ЭП), в состав которого включена следующая информация:

Фамилия, имя, отчество
организация
должность
подразделение
полномочия
ИНН ОГРН

СНИЛС

Учетная запись пользователя АСФК | Формализованная должность

Адрес электронной почты владельца СКП

предъявлен серия номер

(наименование документа, серия и номер основного документа, удостоверяющего личность)

выдан

(дата выдачи) (кем выдан)

Алгоритм открытого ключа: , *Parameters:*
Распечатка значения ключа проверки ЭП пользователя:
Алгоритм подписи запроса: , *Parameters:*
Распечатка значения подписи запроса:

Область использования ключа проверки ЭП:
Назначение сертификата:

Я, владелец ключей ЭП, прошу дополнительно включить в состав квалифицированного сертификата следующие сведения:
– адрес электронной почты;
– должность;
– наименование структурного подразделения;
– ограничения на использование квалифицированного сертификата (если имеются): _____
_____
_____

Информация для приостановления СКП «_____»
Ключевая фраза (кодовое слово)

Владелец ключей ЭП**

_____ / _____ /
(должность) *(подпись)* *(И.О. Фамилия)*

«__»_____ 20__г.
(дата)

/ /

(должность руководителя Организации-заявителя, уполномоченного им лица) *(подпись)* *(И.О. Фамилия)*

М.П. «__»_____ 20__г.

(дата)

Заполняется в УЦ ФК

Данные, указанные в заявлении, идентичны данным, указанным в представленных и предоставленных документах

/ /

(должность Оператора УЦ) *(подпись)* *(Фамилия И.О.)*

«__»_____ 20__г.

(дата)

Номер транзакции «__» _____ 20__г.

(дата загрузки запроса)

Серийный номер сертификата «__»_____ 20__г.

(дата издания сертификата)

* Не заполняется в случае получения сертификата руководителем Организации-заявителя.
** В случае получения сертификата Организации-заявителя без указания ФИО физического лица, подписывается Уполномоченным лицом.

Приложение № 3
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

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 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, заинтересованных в получении или владеющих квалифицированной электронной подписью, об условиях, рисках и порядке использования квалифицированной электронной подписи и средств электронной подписи, а так же о мерах, необходимых для обеспечения безопасности при использовании квалифицированной электронной подписи.

Применение квалифицированной электронной подписи в системах юридически значимого электронного документооборота и иных системах, сопровождаются рисками финансовых убытков и иного рода потерь, связанных с признанием недействительности сделок, совершенных с использованием квалифицированной электронной подписи при несанкционированном получении злоумышленником ключа электронной подписи или несанкционированного использования рабочего места пользователя, на котором осуществляется выработка квалифицированной электронной подписи. В связи с этим необходимо выполнение приведенных ниже организационно-технических и административных мер по обеспечению правильного функционирования средств обработки и передачи информации.

2. Требования по размещению

При размещении средств 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 квалифицированной электронной подписи, общесистемного и специального программного обеспечения

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

3.1.1. Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

– длина пароля должна быть не менее 6 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:

– ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

– 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 стирание (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, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий.

3.1.4. В случае подключения технических средств с установленными средствами квалифицированной 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. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем к программному обеспечению, в окружении которого функционируют средства квалифицированной электронной подписи и к компонентам средств квалифицированной электронной подписи со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). Все средства защиты, должны иметь сертификат уполномоченного органа по сертификации средств защиты.

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 квалифицированной электронной подписи;

– работать со средствами квалифицированной электронной подписи при включенных в техническое средство штатных средствах выхода в радиоканал;

– записывать на ключевые носители постороннюю информацию;

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

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, Заявление на изменение статуса которого подано в Удостоверяющий центр Федерального казначейства (далее – УЦ ФК), в течение времени, исчисляемого с момента времени подачи Заявления на изменение статуса сертификата в УЦ ФК по момент времени официального уведомления об изменении статуса сертификата, либо об отказе в изменении статуса;

– использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

– 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 типы ключевых носителей, которые поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

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 квалифицированной 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 системах обмена электронными документами по электронной почте сети Интернет или по внутренней электронной почте (кроме запросов на сертификат и открытых ключей).

Ключевая информация должна размещаться на сменном носителе информации (floppy-диск, USB-flash накопитель, e-Token, ru-Token и др.). Размещение ключевой информации на локальном или сетевом диске, а также во встроенной памяти технического средства с установленными средствами квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий злоумышленниками.

Носители ключевой информации должны использоваться только их владельцем либо Уполномоченным лицом на использование данного носителя, 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 квалифицированной 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 АРМ с установленными средствами квалифицированной электронной подписи

С целью контроля исходящего и входящего подозрительного трафика, технические средства с установленными средствами квалифицированной электронной подписи должны быть защищены от внешнего доступа программными или аппаратными средствами межсетевого экранирования. Эти средства должны пресекать отправку в Интернет информации, инициированную программами, не имеющими соответствующих полномочий.

На технических средствах, используемых для работы в системах обмена электронными документами:

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

– 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 квалифицированной электронной подписи и средствами криптографической защиты третьих лиц, не имеющих полномочий для работы в системе обмена электронными документами;

– должна быть активирована подсистема регистрации событий информационной безопасности;

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

В качестве автоматизированного рабочего места для работы в системах обмена электронными документами крайне не рекомендуется выбирать переносной компьютер (ноутбук). Если выбран ноутбук, недопустимо его подключение к сетям общего доступа в местах свободного доступа в Интернет (Интернет-кафе, гостиницы, офисные центры и т.д.), при этом для хранения ключевой информации должен использоваться сменный носитель информации.

В случае передачи (списания, сдачи в ремонт) сторонним лицам технических средств, на которых были установлены средства квалифицированной 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 квалифицированной электронной подписи, журналы работы систем обмена электронными документами и т.д.).

5. Дополнительные требования

Дополнительные требования по обеспечению информационной безопасности при работе в системах обмена электронными документами могут дополнительно устанавливаться правилами систем ЭДО, требованиями по эксплуатации и безопасности средств квалифицированной электронной подписи.

Приложение № 4
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Заявление
на изменение статуса
сертификата ключа проверки электронной подписи

_____ «__»_____ 20__г.
(наименование населенного пункта) *(дата)*

Я, _____

_____
(должность, ФИО)

паспорт серия _____ № _____ выдан _____

_____
(кем и когда выдан)

в связи с _____
(указать причину)

прошу приостановить/возобновить/прекратить (*нужное подчеркнуть*) действие квалифицированного сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата _____
Фамилия, имя, отчество _____
Наименование организации _____
ОГРН, ИНН _____
СНИЛС* _____
E-mail _____
с _____ по _____**

_____ « » 20 г.
*(подпись)**** *(Ф.И.О. полностью)*

Заполняется Оператором УЦ

№ транзакции _____ *Дата регистрации* _____

_____ / _____
(должность Оператора УЦ) *(подпись Оператора УЦ)* *(ФИО)*

№	*Действие*	*Дата, время*	*Код причины*	*Примечание*
1	*Сертификат прекратил действие*			
2	*Сертификат приостановлен*			
3	*Сертификат возобновлен*			
4	*В прекращении действия отказано*			

* Заполняется в случае прекращения действия сертификата Заявителя.
** Заполняется в случае приостановления действия сертификата.
*** Для сертификата Заявителя подписывается владельцем сертификата или руководителем Организации-заявителя. Для сертификата Организации-заявителя, без указания ФИО, подписывается руководителем Организации-заявителя.

Приложение № 5
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Акт
установки средства электронной подписи

_____ _____
(наименование населенного пункта) *(дата)*

Настоящий акт составлен о том, что _____ сотрудником
(дата)

_____

_____

_____

_____
(наименование организации, должность, фамилия, имя, отчество, иные сведения (например, дата номер лицензии, в случаях установки средства ЭП с привлечением специализированной организации))

(далее – Уполномоченное лицо) была произведена установка и настройка средства ЭП

_____
(наименование)

Серийный № (Инв. №) АРМ _____

Место установки _____

_____
(адрес местонахождения, номер помещения)

ФИО ответственного лица пользователя АРМ Заявителя _____

(далее – пользователь средства ЭП)

_____
(должность, фамилия, имя, отчество)

Рег. № дистрибутива средства ЭП (номер экземпляра) _____

Номер и дата карточки учета лицензии _____

Размещение АРМ Заявителя, хранение ключевых носителей, охрана помещений организованы установленным порядком.

Обучение правилам работы со средством ЭП и проверка знаний нормативных правовых актов и эксплуатационной и технической документации к нему проведены.

Условия для использования средства ЭП, установленные эксплуатационной и технической документацией к средству ЭП созданы.

Установленное и настроенное средство ЭП находится в работоспособном состоянии.

Формуляр_____(указать номер формуляра) выведен на бумажный носитель, раздел, содержащий сведения о движении (закреплении) изделия Формуляра заполнен установленным порядком, Формуляр передан на ответственное хранение

пользователю АРМ Заявителя.

Пользователь АРМ Заявителя обязуется:

- не разглашать конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;
- соблюдать требования к обеспечению безопасности средства ЭП и ключевых документов к нему;
- сдать установочный комплект средства ЭП, эксплуатационную и техническую документацию к нему, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием средства ЭП;
- сообщать исполнителю о попытках посторонних лиц получить сведения об используемом средстве ЭП или ключевых документах к нему;
- немедленно уведомлять исполнителя о фактах утраты или недостачи средства ЭП, ключевых документов к нему.

Акт составлен в двух экземплярах.

	/	/
(должность Уполномоченного лица)	*(подпись)*	*(Фамилия И.О.)*
	/	/
(должность ответственного лица пользователя АРМ заявителя)	*(подпись)*	*(Фамилия И.О.)*

Приложение № 6
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Акт уничтожения средства электронной подписи

«____» _____ 201_ года <Наименование населенного пункта>

Комиссия _____ в составе:
(указывается наименование организации)

_____

_____

_____

Ф.И.О., должность членов комиссии

составила настоящий акт о том, что на системном блоке с серийным (инвентарным) номером №_____ произведено уничтожение *«Указывается наименование средства ЭП»* серийный номер дистрибутива (номер экземпляра)_____, путем удаления программ через «Панель управления» - «Установка и удаление программ» и утилиту очистки компьютера от не удаленных элементов продуктов *«указать наименование утилиты»*. Произведено уничтожение дистрибутива программ и документации к средству ЭП *«указать наименование средства ЭП»* путем физического уничтожения *отчужденного* или *оптического* носителя информации.

Карточка учета лицензии средства ЭП *«указать наименование средства ЭП»* версии *«указать версию средства ЭП»* от _____ № ____ подготовлена к возврату в «*указать орган Федерального казначейства*».

Настоящий акт составлен в 2-х экземплярах на 1 листе каждый.

Подписи членов комиссии:

_____ _____

_____ _____

_____ _____

Ф.И.О. и подпись, членов комиссии

Приложение № 7
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Заявление на получение информации о статусе сертификата ключа проверки электронной подписи

_____ «__»_____ 20__г.
(наименование населенного пункта) (дата)

_____

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

в лице _____
(руководителя, ФИО)

действующего на основании _____

_____
(учредительный документ)

в связи с _____
(причина проверки статуса сертификата)

просит предоставить сведения о статусе сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром Федерального казначейства, содержащего следующие сведения:

Серийный номер сертификата _____
Фамилия, имя, отчество _____
Наименование организации _____
ОГРН, ИНН организации _____
СНИЛС* _____

в период с __ часов __минут __.__.20__г. по __часов __ минут __.__.20__г.

Справку просим предоставить по адресу: _____

_____
(почтовый адрес получателя (включая индекс) либо e-mail)

_____ / _____ / _____
(руководитель Организации-заявителя, уполномоченное им лицо) *(подпись)* *(Фамилия И.О.)*

М.П. «__»_____ 20__г.

Приложение № 8
к Регламенту
Удостоверяющего центра
Федерального казначейства,
утвержденному приказом
Федерального казначейства
от «31» июля 2015 г. № 197

Региональный центр регистрации органа Федерального казначейства

_____

(индекс, город, улица, дом)[14]

Квалифицированный сертификат ключа проверки электронной подписи

Номер квалифицированного сертификата:

Действие квалифицированного сертификата: **с** _____ **по** _____

Сведения о владельце квалифицированного сертификата

Фамилия, имя, отчество:

Основной государственный регистрационный номер:

Идентификационный номер налогоплательщика:

СНИЛС:

Место нахождения юридического лица:

Сведения об издателе квалифицированного сертификата

Наименование удостоверяющего центра:

Место нахождения удостоверяющего центра:

Номер квалифицированного сертификата удостоверяющего центра:

Наименование средства электронной подписи:

Реквизиты заключения о подтверждении соответствия средства электронной подписи:

Наименование средства удостоверяющего центра:

Реквизиты заключения о подтверждении соответствия средства удостоверяющего центра:

Класс средств удостоверяющего центра: КС2

Сведения о ключе проверки электронной подписи

Используемый алгоритм:

---

[14] Указывается адрес выдачи квалифицированного сертификата ключа проверки электронной подписи.

Используемое средство электронной подписи:

Класс средства электронной подписи:
- КС1,
- КС2

Область использования ключа:

Значение ключа:

Электронная подпись под квалифицированным сертификатом

Используемый алгоритм:

Значение электронной подписи:

Оператор УЦ ФК / /

Подпись Фамилия И.О.

Дата

Доверенность[15] от «___»_____20___г. № _____

М.П.

Владелец квалифицированного сертификата ключа проверки электронной подписи (Уполномоченное лицо)

Подпись

Дата

[15] Заполняется в случае получения Уполномоченным лицом.