УТВЕРЖДЕН

Приказом
Федерального казначейства
от «14» сентября 2018 г. №261

РЕГЛАМЕНТ
Удостоверяющего центра Федерального казначейства

1. Термины и определения

Запрос на квалифицированный сертификат ключа проверки электронной подписи (далее – сертификат) – файл, созданный с использованием сертифицированного средства электронной подписи (далее – ЭП), содержащий ключ проверки электронной подписи (далее – КПЭП) и иную информацию о Заявителе и/или о получателе сертификата.

Заявитель – юридическое лицо, индивидуальный предприниматель, крестьянское фермерское хозяйство, с которыми заключен Договор присоединения (Соглашение) к Регламенту Удостоверяющего центра Федерального казначейства.

Получатель сертификата – руководитель юридического лица, индивидуальный предприниматель, глава крестьянского фермерского хозяйства или лицо, уполномоченное ими на подписание документов с использованием сертификата Заявителя.

Уполномоченное лицо – лицо, уполномоченное Заявителем на представление документов и сведений, предусмотренных настоящим Регламентом; при получении сертификата за его владельца – на ознакомление под расписку с информацией, содержащейся в сертификате, получение сертификата и Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

Компрометация ключа электронной подписи (далее – 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).

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

Копия документа, удостоверяющего личность – копия страниц паспорта гражданина Российской Федерации или иного документа, удостоверяющего личность, в соответствии с законодательством Российской Федерации, содержащая фамилию, имя, отчество (если имеется), дату выдачи документа и сведения о выдавшем его органе.

2. Общие положения

2.1. 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», 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).

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

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

2.2. Взаимодействие территориального органа Федерального казначейства (далее – ТОФК) и Заявителя в рамках настоящего Регламента осуществляется на основании заключенного Договора присоединения (Соглашения) к Регламенту Удостоверяющего центра Федерального казначейства[1] (далее – Соглашение).

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

2.3. 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 создания КЭП.

2.4. Создание сертификата осуществляется в течение шести рабочих дней с даты приема документов и сведений, предусмотренных пунктом 4.1 настоящего Регламента.

Срок создания сертификата увеличивается в случае несвоевременного получения сведений, находящихся в распоряжении государственных органов, иных органов, необходимых для создания сертификата, о чем Заявитель, получатель сертификата, владелец сертификата информируются.

2.5. В случае аннулирования сертификата Заявитель, владелец сертификата уведомляются об этом до внесения соответствующей информации в Реестр выданных и аннулированных сертификатов (далее – Реестр сертификатов).

2.6. Информирование получателя сертификата, владельца сертификата в случаях, предусмотренных настоящим Регламентом, производится посредством направления сообщения на адрес электронной почты или номер телефона[2], указанные в Заявлении на создание сертификата (далее – Заявление на сертификат) или предоставленные посредством информационной системы «Удостоверяющий центр Федерального казначейства» (далее – ИС УЦ).

2.7. САС публикуется по адресу URL=http://crl.roskazna.ru/crl/ и актуализируется не реже двух раз в сутки.

2.8. Выписка из Реестра сертификатов предоставляется в соответствии с Порядком ведения реестров сертификатов на основании письменного обращения Заявителя или с использованием ИС УЦ.

2.9. По инициативе владельца сертификата осуществляется его регистрация в Федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» посредством направления сведений 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).

---

[2] При наличии технической возможности.

3. Выдача средства ЭП

3.1. Выдача средства ЭП и эксплуатационной документации к нему производится во временное пользование по письменному обращению Заявителя с указанием фамилии, имени, отчества (при наличии) получающего лица в количестве, соответствующем количеству получателей сертификатов, с приложением оптического носителя информации с возможностью однократной записи.

В случае расторжения Соглашения Заявитель возвращает ТОФК средство ЭП и эксплуатационную документацию к нему.

3.2. Выдача средства ЭП и эксплуатационной документации к нему осуществляется не позднее трех рабочих дней с даты приема письменного обращения Заявителя и оптического носителя.

3.3. При выдаче средства ЭП осуществляется идентификация лица, указанного в письменном обращении Заявителя, по документу, удостоверяющему личность.

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

4. Формирование и представление документов и сведений, необходимых для создания сертификата

4.1. Документы и сведения, необходимые для создания сертификата (далее – Документы на создание сертификата):

– Заявление на сертификат;

– заверенная копия документа, удостоверяющего личность получателя сертификата[3];

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

– Страховой номер индивидуального лицевого счета (СНИЛС) получателя сертификата[4];

---

[3] В случае представления Документов на создание сертификата непосредственно получателем сертификата заверенная копия документа, удостоверяющего личность, не представляется.

[4] Не представляется в случае получения сертификата, предназначенного для автоматического создания и (или) автоматической проверки электронных подписей в информационных системах, без указания фамилии, имени, отчества владельца сертификата.

– Идентификационный номер налогоплательщика (ИНН) получателя сертификата;

– Основной государственный регистрационный номер (ОГРН) юридического лица[5];

– Основной государственный регистрационный номер (ОГРН) индивидуального предпринимателя[6];

– Запрос на сертификат[7];

– документ или сведения, подтверждающие полномочия получателя сертификата, уполномоченного лица;

– документ или сведения (информация об официальном источнике опубликования и (или) общедоступных изданиях и информационных системах), подтверждающие полномочия лица, действующего от имени Заявителя.

4.2. Формирование Заявления на сертификат, создание КЭП, Запроса на сертификат осуществляется получателем сертификата, владельцем сертификата одним из следующих способов:

4.2.1. на автоматизированном рабочем месте (далее – АРМ) Заявителя с использованием ИС УЦ;

4.2.2. на АРМ Заявителя с использованием Средства создания запроса[8] в случае отсутствия технической возможности использования ИС УЦ;

4.2.3. на АРМ ТОФК в присутствии сотрудника ТОФК в случае отсутствия технической возможности использования ИС УЦ.

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

4.3. Представление Документов на создание сертификата осуществляется одним из следующих способов:

4.3.1. в ТОФК по месту нахождения Заявителя, обособленного подразделения юридического лица.

При этом в случае отсутствия изменений в ранее представленных в ТОФК Документах на создание сертификата их повторное представление не требуется.

---

[5] Представляется также в случае создания сертификата крестьянскому фермерскому хозяйству.

[6] Представляется также в случае создания сертификата главе крестьянского фермерского хозяйства.

[7] Запрос на сертификат, сформированный с использованием Средства создания запроса на АРМ Заявителя, представляется на съемном носителе информации, не содержащем КЭП.

[8] Средство создания КЭП, Запроса на сертификат, Заявления на сертификат. Дистрибутив Средства создания запроса размещен на официальном сайте Федерального казначейства в информационно-телекоммуникационной сети «Интернет».

Лицо, непосредственно представившее Документы на создание сертификата, в целях идентификации представляет оригинал документа, удостоверяющего его личность, с которого снимается копия, удостоверяемая подписями лица и сотрудника ТОФК;

4.3.2. посредством ИС УЦ при наличии ЭП и соответствующего ей действующего сертификата, выданного удостоверяющим центром Федерального казначейства.

5. Создание и выдача сертификата

5.1. Создание сертификата осуществляется в случае положительного результата проверки Документов на создание сертификата на:

– полноту комплекта Документов на создание сертификата;

– соответствие сведений, указанных в Заявлении на сертификат, сведениям в документах, указанных в пункте 4.1 настоящего Регламента;

– отсутствие в представленных Документах на создание сертификата исправлений, не заверенных в установленном порядке[9];

– заверение копий документов;

– соответствие сведений и электронных образов документов, направленных с использованием ИС УЦ, документам и сведениям, представленным на бумажных носителях;

– соответствие значений полей электронной формы Запроса на сертификат представленного на съемном носителе информации значениям полей Заявления на сертификат;

– соответствие сведений, указанных в Документах на создание сертификата, информации, полученной с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие действующих и создаваемых информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

В случае отрицательного результата проверки Документы на создание сертификата возвращаются с мотивированным отказом в письменной форме

---

[9] Исправления в Документах на создание сертификата на бумажном носителе оформляются путем зачеркивания тонкой чертой неправильного текста так, чтобы можно было прочитать зачеркнутое, и написания над зачеркнутым исправленного текста. Исправления в документе на бумажном носителе должны быть оговорены надписью «исправлено», подтверждены подписью тех же лиц, которые подписали документ, проставлением даты исправления. Не допускается внесение изменений в Заявление на сертификат в части сведений, включенных в Запрос на сертификат.

либо в форме электронного документа в случае их представления посредством ИС УЦ.

5.2. Выдача сертификата осуществляется:

5.2.1. Получателю сертификата, владельцу сертификата[10] либо их уполномоченным лицам в ТОФК по месту нахождения Заявителя, обособленного подразделения юридического лица.

Одновременно выдаются файл сертификата, сертификат на бумажном носителе и Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи[11].

При получении сертификата владелец сертификата (уполномоченное лицо) под расписку ознакамливается с информацией, содержащейся в сертификате.

Ознакомление уполномоченного лица с информацией, содержащейся в сертификате, возможно при наличии согласия владельца сертификата на предоставление персональных данных, содержащихся в сертификате, уполномоченному лицу, оформленного в соответствии с требованиями Закона о персональных данных.

5.2.2. Владельцу сертификата с использованием ИС УЦ при наличии ЭП и соответствующего ей действующего сертификата, выданного удостоверяющим центром Федерального казначейства.

При получении сертификата владелец сертификата ознакамливается с информацией, содержащейся в сертификате, и скачивает файл сертификата.

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

6.1. Сертификат прекращает свое действие:

– по истечении срока действия;

– в случае прекращения осуществления Федеральным казначейством функций удостоверяющего центра без перехода его функций другим лицам;

– по инициативе ТОФК, в случае если стало известно об увольнении (отстранении от исполнения обязанностей) владельца сертификата, прекращении деятельности Заявителя или изменении его реквизитов, компрометации КЭП сотрудника ТОФК;

---

[10] При отсутствии технической возможности использования ИС УЦ.

[11] Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи представлено в приложении № 2 к настоящему Регламенту и выдаётся единовременно под подпись в соответствующем журнале.

– по инициативе Заявителя на основании Заявления на изменение статуса сертификата[12]:

– 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 представляется соответствующее Заявление на изменение статуса сертификата 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 Заявителя.

6.2 Заявление на изменение статуса сертификата формируется и представляется с использованием ИС УЦ.

В случае отсутствия технической возможности использования ИС УЦ Заявление на изменение статуса сертификата представляется в ТОФК по месту нахождения Заявителя, обособленного подразделения юридического лица на бумажном носителе.

В случае представления Заявления на изменение статуса сертификата на бумажном носителе[13] осуществляется идентификация лица, его представившего, по документу, удостоверяющему личность.

Заявление на изменение статуса сертификата проверяется на предмет соответствия данным Реестра сертификатов.

В случае выявления несоответствия Заявление на изменение статуса сертификата возвращается с указанием причин отказа в форме электронного документа посредством ИС УЦ или на бумажном носителе.

6.3. Аннулирование сертификата осуществляется в следующих случаях:

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

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

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

---

[12] Образец представлен в приложении № 3 к настоящему Регламенту.

[13] В случае представления Заявления на изменение статуса сертификата уполномоченным лицом, представление документа, подтверждающего его полномочия, не требуется при наличии в ТОФК актуальной версии данного документа.

6.4. В течение двенадцати часов с момента наступления обстоятельств, указанных в пунктах 6.1 и 6.3 настоящего Регламента, или в течение двенадцати часов с момента, когда ТОФК стало известно или должно было стать известно о наступлении таких обстоятельств, соответствующая информация вносится в Реестр сертификатов, САС.

Действие сертификата прекращается с момента внесения записи об этом в Реестр сертификатов.

6.5. Приостановление действия сертификата осуществляется по инициативе Заявителя.

Приостановление действия сертификата производится на основании устного обращения владельца сертификата, в том числе по телефону[14], или Заявления на изменение статуса сертификата[15].

6.5.1. Приостановление действия сертификата по устному обращению владельца сертификата возможно исключительно при возникновении обстоятельств, требующих оперативного приостановления действия сертификата.

При устном обращении владелец сертификата сообщает следующую информацию:

– 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 в случае совпадения информации, переданной в обращении, с информацией из Реестра сертификатов, и действие сертификата приостанавливается на срок, определенный в обращении, но не более чем на 10 рабочих дней.

Приостановление действия сертификата на основании устного обращения осуществляется в день обращения.

В срок, не превышающий 10 календарных дней с даты устного обращения, в ТОФК представляется Заявление на изменение статуса сертификата.

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

---

[14] Телефонные обращения принимаются сотрудниками ТОФК в соответствии с порядком, установленным ТОФК.

[15] Образец представлен в приложении № 3 к настоящему Регламенту.

6.5.2. Приостановление действия сертификата на основании Заявления на изменение статуса сертификата осуществляется на срок не более 56 календарных дней и не менее 10 календарных дней.

Формирование, представление и рассмотрение Заявления на изменение статуса сертификата осуществляются в соответствии с пунктом 6.2 настоящего Регламента.

В случае положительного результата проверки действие сертификата приостанавливается, о чем информируются Заявитель и владелец сертификата.

6.6. Возобновление действия сертификата осуществляется в отношении приостановленных сертификатов.

Возобновление действия приостановленного сертификата осуществляется на основании Заявления на изменение статуса сертификата[16] и при условии, что срок, на который действие сертификата было приостановлено, не истек.

Формирование, представление и рассмотрение Заявления на изменение статуса сертификата осуществляются в соответствии с пунктом 6.2 настоящего Регламента.

В случае положительного результата проверки действие приостановленного сертификата возобновляется с информированием Заявителя и владельца сертификата.

Возобновление действия сертификата либо отказ в возобновлении действия сертификата, включая информирование, осуществляется в течение одного рабочего дня, следующего за днем принятия Заявления на изменение статуса сертификата.

[16] Образец представлен в приложении № 3 к настоящему Регламенту.

Приложение № 1
к Регламенту
Удостоверяющего центра
Федерального казначейства

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

г. _____ «__» _____ 20__г.

Федеральное казначейство* в лице _____, действующего на основании _____, с одной стороны, и

_____
(наименование юридического лица (крестьянского фермерского хозяйства), ФИО индивидуального предпринимателя (главы крестьянского фермерского хозяйства)

_____,
ФИО лица, действующего от имени юридического лица (крестьянского фермерского хозяйства), индивидуального предпринимателя (главы крестьянского фермерского хозяйства), документ,

_____,
подтверждающий его полномочия)

именуем____ в дальнейшем «Заявитель», с другой стороны, вместе именуемые «Сторонами», заключили настоящий договор (далее – Соглашение) о нижеследующем.

I. Предмет Соглашения

1.1. Предметом настоящего Соглашения является присоединение 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

Федеральное казначейство: Заявитель:

---

* Федеральное казначейство, включая его территориальные органы

Приложение № 2
к Регламенту
Удостоверяющего центра
Федерального казначейства

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 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:

– 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 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.

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;

– 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 и соответствующий сертификат ключа проверки электронной подписи, Заявление на изменение статуса которого подано в территориальный орган Федерального казначейства, в течение времени, исчисляемого с момента подачи Заявления на изменение статуса сертификата по момент официального информирования 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 предварительно проинициализированные (отформатированные) ключевые носители, типы которых поддерживаются используемым средством квалифицированной электронной подписи согласно технической и эксплуатационной документации к ним.

Ключевые носители должны иметь маркировку с учетным номером, присвоенным Заявителем.

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 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 квалифицированной электронной подписи, способствует реализации многочисленных сценариев совершения мошеннических действий 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 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. 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;

– 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 соответствующей информационной системе;

– должна быть активирована регистрация событий информационной безопасности;

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

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 так далее.

Приложение № 3
к Регламенту
Удостоверяющего центра
Федерального казначейства

Заявление
на изменение статуса
сертификата ключа проверки электронной подписи

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

_____

_____
(полное наименование Заявителя)

в лице* _____
(ФИО лица, действующего от имени Заявителя)

действующего на основании* _____

_____

в связи с _____
(указать причину)

просит 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, ОГРНИП _____
СНИЛС _____
E-mail _____

с _____ по _____**

_____ « » 20 г. ***
(подпись) *(фамилия, инициалы владельца сертификата)*

_____ « » 20 г.
(подпись) *(фамилия, инициалы лица, действующего от имени Заявителя)*

Заполняется сотрудником ТОФК

№ транзакции _____ *Дата регистрации* _____

_____ /_____/
(должность сотрудника ТОФК) *(подпись сотрудника ТОФК)* *(ФИО)*

№	*Действие*	*Дата, время*	*Код причины*	*Примечание*
1	*Сертификат прекратил действие*			
2	*Сертификат приостановлен*			
3	*Сертификат возобновлен*			

4	*В прекращении действия отказано*			

* Не заполняется при обращении индивидуального предпринимателя или главы крестьянского фермерского хозяйства.
** Заполняется в случае приостановления действия сертификата.
*** В случае увольнения владельца сертификата может не заполняться.