

Регламент
удостоверяющего центра ФСО России
(утвержден 7 февраля 2019 г.)

Москва 2019

1. Сведения об удостоверяющем центре ФСО России

1.1. Аккредитованный удостоверяющий центр ФСО России (далее – УЦ) осуществляет функции по созданию и выдаче квалифицированных сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

1.2. Деятельность УЦ осуществляется в целях обеспечения функционирования государственных информационных систем, находящихся в ведении ФСО России, служебной деятельности сотрудников органов государственной охраны, а также сотрудников органов государственной власти, государственных органов и органов местного самоуправления с использованием усиленной квалифицированной электронной подписи.

1.3. Реквизиты УЦ:

Полное наименование: Удостоверяющий центр Федеральной службы охраны Российской Федерации.

Местонахождение: город Москва, Кремль-9.

Фактическое местонахождение:

город Москва, улица Мясницкая 48, строение 1

Контактная информация:

тел. (495) 914-13-34, (495) 914-13-26

E-mail: ucgspi@msk.rsnet.ru

город Москва, Ипатьевский пер., д. 9/1, строение 1

Контактная информация:

тел. (495) 606-21-13

E-mail: dotsenko_a@gov.ru

2. Термины и определения настоящего Регламента

2.1. Администратор/Оператор УЦ – сотрудник ФСО России, наделенный полномочиями по осуществлению действий по управлению сертификатами ключей проверки электронных подписей, проверки электронных подписей, заверению собственноручной подписью сертификатов ключей проверки электронных подписей, изданных УЦ.

2.2. Заявитель – орган государственной власти, государственный орган, орган местного самоуправления, юридическое лицо, физическое лицо, обращающиеся с заявлением в УЦ об изготовлении квалифицированного сертификата ключа проверки электронной подписи. Заявитель вправе

обращаться в УЦ через уполномоченное лицо. Полномочия уполномоченного лица могут указываться в доверенности, выданной в установленном законом порядке и (или) в правовом акте.

2.3. Владелец сертификата ключа проверки электронной подписи (далее – владелец сертификата) – лицо, на чье имя в установленном порядке оформлен сертификат ключа проверки электронной подписи.

Владелец сертификата (будущий владелец сертификата) вправе поручить доверенному лицу получить сертификат ключа проверки электронной подписи владельца сертификата и иные документы, определенные Регламентом УЦ, сформированный ключевой носитель, а также осуществлять иные действия для выполнения данного поручения на основании нотариально выданной доверенности (приравненной к нотариально выданной доверенности) или доверенности, оформленной согласно Приложению № 1 к Регламенту УЦ.

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

2.5. Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ электронной подписи действует на определенный момент времени (действующий ключ электронной подписи), если:

наступил момент времени начала действия ключа электронной подписи;

срок действия ключа электронной подписи не истек;

сертификат ключа проверки электронной подписи, соответствующий данному ключу электронной подписи, не аннулирован (не отозван).

2.6. Ключевой носитель – отчуждаемый физический носитель информации, содержащий ключ электронной подписи. Допускается применять в качестве ключевых носителей устройства типа eToken, Rutoken.

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

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

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

увольнение (перевод) сотрудников, имевших доступ к ключу электронной подписи;

нарушение правил хранения и уничтожения ключа электронной подписи;

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

2.8. Конфликтная ситуация – ситуация, при которой у владельца сертификата возникает необходимость разрешения вопросов признания или не признания авторства или подлинности электронных документов, обработанных с помощью средств электронной подписи.

2.9. Реестр УЦ – набор документов УЦ в электронной и/или бумажной форме в следующем составе:

реестр заявлений на изготовление сертификатов ключей проверки электронных подписей;

реестр заявлений на аннулирование (отзыв) сертификатов ключей проверки электронных подписей;

реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

реестр выданных и аннулированных (отозванных) сертификатов ключей проверки электронных подписей.

2.10. Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата.

Сертификат ключа проверки электронной подписи действует на определенный момент времени (действующий сертификат), если:

наступил момент времени начала действия сертификата ключа проверки электронной подписи;

срок действия сертификата ключа проверки электронной подписи не истек;

сертификат ключа проверки электронной подписи не аннулирован (отозван).

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, выданный УЦ или доверенным лицом УЦ (далее - сертификат).

2.11. Страница УЦ – раздел «Официального интернет-портала правовой информации» в информационно-телекоммуникационной сети «Интернет» (www.pravo.gov.ru/uc), позволяющий получить информацию о деятельности УЦ, сертификатах УЦ и списках отозванных сертификатов.

2.12. Список отозванных сертификатов (СОС) – электронный документ с электронной подписью УЦ, включающий в себя список серийных номеров сертификатов ключей проверки электронной подписи, которые на определенный момент времени были аннулированы.

2.13. Средства электронной подписи – сертифицированное программное средство криптографической защиты информации (СКЗИ), которое обеспечивает реализацию следующих функций:

создание электронной подписи в электронном документе с использованием ключа электронной подписи;

проверка подлинности электронной подписи (подтверждение с использованием ключа проверки электронной подписи подлинности электронной подписи в электронном документе);

создание ключа электронной подписи и ключа проверки электронной подписи.

2.14. Информационное взаимодействие – деятельность органов государственной власти, государственных органов, органов местного самоуправления и юридических лиц, участвующих в процессе размещения в установленном порядке информации в информационных системах с использованием ключей электронной подписи.

3. Услуги, предоставляемые УЦ

3.1. Функционирование средств УЦ обеспечивает Федеральная служба охраны Российской Федерации.

3.2. Услуги, предоставляемые УЦ:

создание ключей электронной подписи (с гарантией сохранения в тайне ключа электронной подписи), сертификатов и выдача таких сертификатов по обращению заявителя;

выдача сертификатов в форме электронных документов и (или) в форме документов на бумажных носителях (по требованию заявителя);

предоставление в электронной форме копий сертификатов, внесенных в реестр сертификатов;

установление сроков действия сертификатов;

аннулирование (отзыв);

проверка уникальности ключей проверки электронных подписей в реестре сертификатов;

подтверждение подлинности электронных подписей, выданных УЦ сертификатов.

3.3. УЦ ведет реестр выданных и аннулированных (отозванных) и прекративших действие сертификатов, в том числе включающий в себя информацию о датах прекращения действия или аннулирования сертификатов и об основаниях такого прекращения или аннулирования, а также обеспечивает его актуальность. Хранение информации, содержащейся в реестре выданных и аннулированных (отозванных) сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Размещение списка отозванных сертификатов производится Администратором/Оператором УЦ на странице УЦ.

3.4. Услуги, указанные в пункте 3.2. настоящего Регламента, предоставляются заявителям по информационному взаимодействию безвозмездно.

4. Общие положения

4.1. Регламент УЦ (далее – Регламент) разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

4.2. Регламент является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.3. Регламент определяет условия и правила предоставления услуг УЦ, включая права, обязанности, ответственность заявителей, владельцев сертификатов (их доверенных лиц), основные организационно-технические мероприятия, направленные на обеспечение работы УЦ.

4.4. Регламент размещается на странице УЦ в формате pdf.

4.5. Присоединение к Регламенту осуществляется путем подписания и предоставления заявителем в УЦ заявления на изготовление сертификата ключа проверки электронной подписи.

Фактом присоединения к Регламенту является полное принятие заявителем условий Регламента и всех его приложений в редакции, действующей на момент регистрации в УЦ заявления на изготовление сертификата ключа проверки электронной подписи. Заявитель (владелец сертификата), присоединившийся к Регламенту, принимает дальнейшие изменения, которые будут вноситься в Регламент, в соответствии с условиями и порядком, установленными Регламентом.

4.6. Внесение изменений в Регламент, включая приложения к нему, производится путем размещения Регламента согласно пункту 4.4. Регламента.

4.7. Все изменения, вносимые в Регламент по собственной инициативе УЦ и не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными с момента их утверждения.

4.8. Все изменения, вносимые в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу новых положений законодательства Российской Федерации по указанным изменениям.

4.9. Любые изменения в Регламенте с момента их вступления в силу обязательны для исполнения заявителем, владельцем сертификата и их доверенными лицами.

5. Права и обязанности

5.1. УЦ имеет право:

5.1.1. Отказывать в регистрации заявления на изготовление сертификата ключа проверки электронной подписи в случае непредставления или ненадлежащего оформления необходимых документов.

5.1.2. Отказывать в аннулировании (отзыве) сертификата в случае ненадлежащего оформления соответствующего заявления.

5.1.3. Отказывать в аннулировании (отзыве), если истек установленный срок действия ключа электронной подписи, соответствующего сертификату.

5.1.4. Приостанавливать предоставление услуг УЦ в связи с проведением профилактических работ, обслуживания аппаратных, программных, технических или телекоммуникационных средств УЦ на срок не более 5 (пяти) рабочих дней.

5.2. Владелец сертификата имеет право:

5.2.1. Применять сертификат УЦ для проверки электронной подписи в сертификатах, изготовленных УЦ.

5.2.2. Применять для хранения ключа электронной подписи ключевой носитель, поддерживаемый средствами электронной подписи УЦ и владельца сертификата.

5.2.3. Обращаться в установленном порядке в УЦ с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи, владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.

5.2.4. Обращаться в установленном порядке к Администратору/Оператору УЦ с целью получения списка отозванных сертификатов.

5.3. УЦ обязан:

5.3.1. Предоставить заявителю (доверенному лицу) сертификат УЦ в электронной форме.

5.3.2. Принимать меры по защите ключей электронной подписи от несанкционированного доступа при их генерации в УЦ.

5.3.3. Обеспечивать регистрацию заявителей и занесение регистрационной информации владельцев сертификатов в реестр УЦ.

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

5.3.5. Обеспечивать конфиденциальность созданных УЦ ключей электронных подписей до их передачи владельцам сертификатов (доверенным лицам).

5.3.6. Обеспечивать изготовление и выдачу сертификата заявителю по его заявлению, с записью ключа электронной подписи на ключевой носитель заявителя или УЦ.

5.3.7. Приостанавливать действие сертификата по заявлению владельца сертификата.

5.3.8. Аннулировать (отзывать) сертификат в случаях, указанных в Регламенте.

5.3.10. Производить внеплановую замену сертификатов в случаях, определенных Регламентом.

5.3.11. Уведомлять владельцев сертификатов о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификатов и ключей электронной подписи, изготовленных УЦ.

5.3.12. Уведомлять владельца сертификата о факте изготовления или аннулирования сертификата.

5.3.13. Уведомлять владельцев сертификатов о приостановке деятельности УЦ за две недели до приостановки деятельности УЦ.

5.3.14. Уведомлять владельцев сертификатов о начале процедуры внеплановой замены сертификатов за две недели до начала процедуры замены.

5.4. Владелец сертификата обязан:

5.4.1. Извещать УЦ об изменениях в ранее предоставленных данных, указанных в заявлении на изготовление сертификата ключа проверки электронной подписи. При необходимости, по согласованию с УЦ, провести внеплановую смену ключа электронной подписи и сертификата согласно п. 7.2. Регламента.

5.4.2. С целью обеспечения гарантированного ознакомления с полным текстом изменений, не реже одного раза в 30 (тридцать) календарных дней обращаться на страницу УЦ за сведениями об изменениях в Регламенте.

5.4.3. Хранить в тайне (обеспечивать конфиденциальность) ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и (или) несанкционированного использования.

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

5.4.5. Использовать для создания и проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.4.6. Уведомлять УЦ о нарушении конфиденциальности ключа электронной подписи в течение рабочего дня со дня получения информации о таком нарушении.

5.4.7. Применять ключ электронной подписи только в соответствии с областями использования, указанными в заявлении на изготовление сертификата ключа проверки электронной подписи, и соответствующими полномочиями, возложенными заявителем.

5.4.8. Самостоятельно принимать решение о факте или возможной компрометации ключа электронной подписи и направлять в УЦ соответствующее заявление, а также не применять ключ электронной подписи, если стало известно, что этот ключ скомпрометирован.

5.4.9. Не использовать ключ электронной подписи, связанный с сертификатом, заявление на аннулирование (отзыв) которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на отзыв сертификата в УЦ по момент времени официального уведомления об отзыве сертификата, либо об отказе в его отзыве.

5.4.11. Не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено.

5.4.12. Использовать средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в

соответствии с положениями документации на применяемое средство электронной подписи.

6. Изготовление ключа электронной подписи и сертификата

6.1. Изготовление ключа электронной подписи и сертификата осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи.

6.2. Заявление на изготовление сертификата ключа проверки электронной подписи оформляется по форме, согласно Приложению № 2 к Регламенту, в случае, если заявитель зарегистрирован в Едином государственном реестре юридических лиц.

Заявление на изготовление сертификата ключа проверки электронной подписи оформляется по форме, согласно Приложению № 3 к Регламенту, в случае, если заявитель не зарегистрирован в Едином государственном реестре юридических лиц.

Заявление на изготовление сертификата ключа проверки электронной подписи представляется по одному из адресов УЦ, указанных в п. 1.3. Регламента. Требования к заполнению полей и их состав приведены в Приложении № 4 к Регламенту.

Совместно с заявлением на изготовление сертификата ключа проверки электронной подписи в УЦ заявителем предоставляются документы, либо их надлежащим образом заверенные копии для подтверждения данных, указанных в заявлении, а именно:

основной документ, удостоверяющий личность будущего владельца сертификата (паспорт гражданина Российской Федерации);

копия страхового свидетельства государственного пенсионного страхования будущего владельца сертификата (СНИЛС);

копия документа, подтверждающего факт внесения записи о юридическом лице в Единый государственный реестр юридических лиц (при наличии регистрации заявителя в Едином государственном реестре юридических лиц) (ОГРН);

копия свидетельства о постановке на учет в налоговом органе – заявителя (при наличии регистрации заявителя в Едином государственном реестре юридических лиц) (ИНН), либо будущего владельца сертификата (при отсутствии регистрации заявителя в Едином государственном реестре юридических лиц);

документ о наделении полномочиями будущего владельца сертификата на использование ключа электронной подписи.

6.3. Предоставленное заявление с копиями подтверждающих документов регистрируется в УЦ в установленном порядке как входящий документ.

6.4. Вместе с заявлением на изготовление сертификата ключа проверки электронной подписи заявителем в УЦ предоставляется ключевой носитель.

6.5. После получения заявления на изготовление сертификата ключа проверки электронной подписи Администратор/Оператор УЦ осуществляет рассмотрение правильности заполнения полей, сверку данных и наличия собственноручных подписей лиц, указанных в заявлении, а также печатей (при необходимости).

6.6. В случае отказа в регистрации и (или) изготовлении сертификата Администратор/Оператор УЦ уведомляет об этом заявителя с указанием причины отклонения заявления.

6.7. При принятии положительного решения Администратор/Оператор УЦ в срок до 5 (пяти) рабочих дней с момента получения заявления на изготовление сертификата ключа проверки электронной подписи осуществляет:

создание и запись ключа электронной подписи и сертификата на ключевой носитель в соответствии с правилами пользования СКЗИ, согласованными с федеральным органом исполнительной власти в области обеспечения безопасности;

изготовление копий сертификата на бумажном носителе в двух экземплярах.

6.8. Ключ электронной подписи и сертификат, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также соблюдением требований, устанавливаемых Правительством Российской Федерации в отношении автоматизированного рабочего места УЦ, используемого для создания ключа электронной подписи и сертификата для заявителя.

6.8. Два экземпляра сертификата на бумажном носителе заверяются Администратором/Оператором УЦ.

6.9. После изготовления сертификата Администратор/Оператор УЦ уведомляет об этом владельца сертификата, после чего владельцу сертификата (его доверенному лицу) необходимо явиться в УЦ за получением ключа электронной подписи и сертификатом.

6.10. По прибытии в УЦ владелец сертификата (его доверенное лицо) предоставляет Администратору/Оператору УЦ на сверку основной документ, удостоверяющий его личность (и доверенность – в случае получения сертификата доверенным лицом).

Администратор/Оператор УЦ осуществляет проверку полномочий прибывшего лица на получение сертификата.

После успешной проверки Администратор/Оператор УЦ ознакомляет под роспись владельца сертификата (его доверенное лицо) с информацией, содержащейся в сертификате на бумажном носителе.

Владельцу сертификата (его доверенному лицу) передаются:

ключевой носитель, содержащий ключ электронной подписи и сертификат, соответствующий ключу электронной подписи;

экземпляр сертификата на бумажном носителе;

руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств электронной подписи, содержащее информацию об обязанностях владельца сертификата, порядок применения средств электронной подписи, ответственность и риски применения средств электронной подписи.

6.11. При выдаче сертификата УЦ направляет в единую систему идентификации и аутентификации (ЕСИА) сведения о лице, получившем сертификат, в объеме, необходимом для регистрации в ЕСИА, и о полученном им сертификате (уникальный номер сертификата, даты начала и окончания его действия, наименование УЦ).

При выдаче сертификата по желанию владельца сертификата УЦ безвозмездно осуществляется регистрация владельца сертификата в ЕСИА.

6.12. В устной форме владелец сертификата может сообщить Администратору/Оператору УЦ ключевую фразу, которая будет использоваться для аутентификации владельца сертификата при выполнении регламентных процедур, возникающих при компрометации ключа электронной подписи.

6.13. Срочное создание и выдача сертификата заявителю осуществляется в течение одного рабочего дня с момента поступления его мотивированного заявления в УЦ.

7. Плановая и внеплановая смена ключей электронных подписей и сертификатов

7.1. Администратор/Оператор УЦ выполняет плановую смену ключа электронной подписи и изготовление нового сертификата на основании

заявления на изготовление сертификата ключа проверки электронной подписи, поданного не ранее 90 и не позднее 15 календарных дней до окончания срока действия ключа электронной подписи.

7.2. Внеплановая смена ключа электронной подписи и сертификата осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи в следующих случаях:

изменения регистрационных данных заявителя или владельца сертификата, заносимых в сертификат;

компрометации ключа электронной подписи владельца сертификата;

компрометации ключа электронной подписи УЦ.

7.3. Порядок проведения плановой и внеплановой смены ключей электронных подписей и сертификатов аналогичен порядку, приведенному в разделе 6 Регламента.

7.4. В случае установления факта компрометации ключа электронной подписи УЦ одновременно с проведением процедуры внеплановой смены ключа электронной подписи осуществляется прекращение действия всех сертификатов, созданных с использованием этого ключа, с занесением сведений об этих сертификатах в реестр сертификатов.

7.5. Информацию о способах получения сертификатов УЦ, исключающих уничтожение, модификацию, блокирование при передаче и иных неправомерных действиях, владельцы сертификатов могут получить обратившись в УЦ, согласно контактной информации.

8. Аннулирование (отзыв) или прекращение действия сертификата

8.1. Аннулирование (отзыв) или прекращение действия сертификата сертификат осуществляется в следующих случаях:

в связи с истечением установленного срока его действия;

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

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

в иных случаях, установленных Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между УЦ и владельцем сертификата.

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

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

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

8.3. Официальным уведомлением о факте аннулирования (отзыва) или прекращения действия сертификата является размещение первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате и изданного не ранее времени наступления произошедшего случая. Датой и временем аннулирования (отзыва) сертификата признаются дата и время издания указанного списка отозванных сертификатов, хранящиеся в поле «Действителен с» списка аннулированных (отозванных) сертификатов.

8.4. Информация о размещении списка аннулированных (отозванных) или прекращения действия сертификатов заносится в изданные УЦ сертификаты в расширение «Точка распределения списка отзыва (CRL)» сертификата.

8.5. В случае аннулирования (отзыва) или прекращения его действия сертификата по истечении срока его действия датой и временем аннулирования (отзыва) сертификата признаются дата и время, хранящиеся в поле «Действителен по» сертификата. В данном случае информация об аннулированном (отозванном) сертификате в список аннулированных (отозванных) сертификатов не заносится.

8.6. В случае компрометации ключа электронной подписи УЦ временем аннулирования (отзыва) сертификата признаются дата и время издания списка отозванных сертификатов удостоверяющим центром федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

8.7. Заявление на аннулирование (отзыв) или прекращение действия сертификата оформляется по форме, согласно Приложению № 5 к Регламенту. Заявление может быть подано как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью.

8.8. После получения заявления на аннулирование (отзыв) или прекращение действия сертификата Администратор/Оператор УЦ осуществляет его рассмотрение и обработку и в случае принятия

положительного решения отзывает сертификат в течение 1 (одного) рабочего дня с момента получения указанного заявления.

8.9. В случае отказа в аннулировании (отзыве) сертификата Администратор/Оператор УЦ уведомляет об этом владельца сертификата.

8.10. Срок внесения информации о прекращении действия или аннулировании (отзыве) сертификата в реестр сертификатов не может превышать двенадцать часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

9. Получение информации о статусе сертификата

9.1. Получение информации о статусе сертификата, изданного УЦ, осуществляется на основании заявления в УЦ о получении соответствующей информации по форме, согласно Приложению № 6 к Регламенту. Предоставление указанного заявления может быть осуществлено при личном прибытии в УЦ, по электронной почте, почтовой и иной связью.

9.2. Заявление должно содержать следующую информацию:

время и дата подачи заявления;

время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата;

идентификационные данные заявителя и владельца сертификата, статус сертификата которого требуется установить;

серийный номер сертификата, статус которого требуется установить.

9.3. По результатам проведения работ по заявлению оформляется справка, содержащая информацию о статусе сертификата, которая предоставляется обратившемуся лицу.

9.4. Предоставление обратившемуся лицу справки о статусе сертификата должно быть осуществлено не позднее 10 (десяти) рабочих дней с момента получения УЦ соответствующего заявления.

10. Сроки действия ключей электронных подписей

10.1. Начало периода действия ключа электронной подписи УЦ исчисляется с даты и времени начала действия соответствующего сертификата, изготовленного удостоверяющим центром федерального органа исполнительной власти, осуществляющего функции по выработке и

реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

10.2. Срок действия сертификата УЦ устанавливается удостоверяющим центром федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий.

10.3. Дата и время начала периода действия сертификата УЦ и его окончания заносится в поля «Действителен с» и «Действителен по» соответственно.

10.4. Срок действия ключа электронной подписи владельца сертификата устанавливается в зависимости от средства электронной подписи, используемого владельцем сертификата и средств электронной подписи УЦ.

10.5. Начало периода действия ключа электронной подписи владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата.

10.6. Дата и время начала периода действия сертификата владельца сертификата и его окончания заносится в поля «Действителен с» и «Действителен по» соответственно.

11. Порядок технического обслуживания реестра сертификатов

11.1. УЦ уведомляет владельцев сертификатов о проведении технического обслуживания реестра выданных, аннулированных (отозванных) и прекративших действие сертификатов посредством размещения информации на странице УЦ.

11.2. Максимальный срок проведения технического обслуживания реестра выданных, аннулированных (отозванных) и прекративших действие сертификатов должен составлять не более 5 (пяти) рабочих дней.

Приложение № 1
к Регламенту

Доверенность

_____ (наименование заявителя)

в лице _____
(наименование должности руководителя или уполномоченного сотрудника заявителя)

_____ (фамилия, имя, отчество руководителя или уполномоченного сотрудника заявителя)

уполномочивает _____
(фамилия, имя, отчество доверенного лица)

_____ (серия и номер паспорта, кем и когда выдан)

1. Получить сертификат ключа проверки электронной подписи владельца сертификата и иные документы, определенные Регламентом УЦ.
2. Получить сформированный ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи

_____ (фамилия, имя, отчество будущего владельца сертификата)

_____ (серия и номер паспорта, кем и когда выдан)

Доверенное лицо наделяется правом расписываться в копии сертификата ключа проверки электронной подписи владельца сертификата и в соответствующих документах УЦ для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по « ____ » _____ 20 ____ г.

Доверитель _____ / _____ /
(подпись) (ФИО будущего владельца сертификата)

Подпись _____ подтверждаю.
(фамилия, имя, отчество будущего владельца сертификата)

_____ / _____ /
(наименование должности руководителя или уполномоченного сотрудника заявителя) (подпись) (Инициалы, Фамилия)

« ____ » _____ 20 ____ г.

М.П.

Приложение № 2
к Регламенту

В удостоверяющий
центр ФСО России

Заявление
на изготовление сертификата ключа проверки электронной подписи
(форма № 1)

_____ (наименование заявителя)

_____ (должность руководителя или уполномоченного сотрудника заявителя)

_____ (фамилия, имя, отчество руководителя или уполномоченного сотрудника заявителя)

действующий на основании _____

(основание полномочий)

просит создать усиленный квалифицированный сертификат ключа проверки электронной подписи, в соответствии со следующими идентификационными данными

Фамилия, Имя, Отчество	<i>фамилия, имя, отчество будущего владельца сертификата</i>
Организация	<i>наименование заявителя</i>
Должность	<i>должность будущего владельца сертификата</i>
Субъект РФ	<i>код региона, наименование субъекта РФ</i>
Населенный пункт	<i>наименование населенного пункта</i>
Адрес	<i>Адрес местонахождения заявителя</i>
СНИЛС	<i>СНИЛС будущего владельца сертификата</i>
ОГРН	<i>ОГРН заявителя</i>
ИНН	<i>ИНН заявителя</i>
E-mail	<i>электронный адрес будущего владельца сертификата</i>

Паспортные данные будущего владельца сертификата:

серия _____ № _____ дата выдачи _____
кем выдан _____

Средство электронной подписи: СКЗИ «КриптоПро CSP версии _____»
(указать версию СКЗИ)

С обработкой, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение указанных персональных данных Удостоверяющим центром ФСО России в целях изготовления и обслуживания сертификата ключа проверки электронной подписи согласен. Признаю, что персональные данные, заносимые в мой сертификат ключа проверки электронной подписи, относятся к общедоступным персональным данным. Полностью и безусловно присоединяюсь к Регламенту УЦ. С Регламентом УЦ ознакомлен и обязуюсь соблюдать все положения данного документа.

_____ /
(подпись будущего владельца сертификата)

_____ /
(Инициалы, Фамилия)

Настоящим подтверждаю, что _____
(ФИО будущего владельца сертификата)

уполномочен использовать ключ электронной подписи, полученный в удостоверяющем центре ФСО России, для осуществления функций по _____
(указать область применения)

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

_____/_____/_____
(наименование должности руководителя или уполномоченного сотрудника заявителя) (подпись) (Инициалы, Фамилия)

« _____ » _____ 20 ____ г.

М.П.

Приложение № 3
к Регламенту

В удостоверяющий
центр ФСО России

Заявление
на изготовление сертификата ключа проверки электронной подписи
(форма № 2)

_____ (наименование заявителя)

_____ (должность руководителя или уполномоченного сотрудника заявителя)

_____ (фамилия, имя, отчество руководителя или уполномоченного сотрудника заявителя)

действующий на основании _____

(основание полномочий)

просит создать усиленный квалифицированный сертификат ключа проверки электронной подписи, в соответствии со следующими идентификационными данными

Фамилия, Имя, Отчество	<i>фамилия, имя, отчество будущего владельца сертификата</i>
Организация	<i>наименование заявителя (заполняется по желанию)</i>
Должность	<i>должность будущего владельца сертификата (заполняется по желанию)</i>
Субъект РФ	<i>код региона, наименование субъекта РФ</i>
Населенный пункт	<i>наименование населенного пункта</i>
СНИЛС	<i>СНИЛС будущего владельца сертификата</i>
ИНН	<i>ИНН будущего владельца сертификата</i>
E-mail	<i>электронный адрес будущего владельца сертификата</i>

Паспортные данные будущего владельца сертификата:

серия _____ № _____ дата выдачи _____
кем выдан _____

Средство электронной подписи: СКЗИ «КриптоПро CSP версии _____»
(указать версию СКЗИ)

С обработкой, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение) извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение указанных персональных данных Удостоверяющим центром ФСО России в целях изготовления и обслуживания сертификата ключа проверки электронной подписи согласен. Признаю, что персональные данные, заносимые в мой сертификат ключа проверки электронной подписи, относятся к общедоступным персональным данным. Полностью и безусловно присоединяюсь к Регламенту УЦ. С Регламентом УЦ ознакомлен и обязуюсь соблюдать все положения данного документа.

(подпись будущего владельца сертификата)

(Инициалы, Фамилия)

Настоящим подтверждаю, что _____
(ФИО будущего владельца сертификата)

уполномочен использовать ключ электронной подписи, полученный в удостоверяющем центре ФСО России, для осуществления функций по _____ .
(указать область применения)

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

_____/ _____ / _____ /
(наименование должности руководителя или уполномоченного сотрудника заявителя) (подпись) (Инициалы, Фамилия)

« _____ » _____ 20____ г.

М.П.

Правила заполнения полей заявления на изготовление сертификата ключа проверки электронной подписи

1. Введение

1.1. Использование настоящего приложения рекомендуется при заполнении заявления на изготовление сертификата ключа проверки электронной подписи.

1.2. Использование настоящего приложения необходимо Администратору/Оператору УЦ при заполнении полей в процессе изготовления сертификата.

1.3. Данный документ разработан на основании:

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

приказа ФСБ России от 27 декабря 2011 г. № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

1.4. Используемые сокращения:

ИНН – индивидуальный номер налогоплательщика;

ОГРН – основной государственный регистрационный номер;

СНИЛС – страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

КЛАДР – классификатор адресов Российской Федерации.

2. Состав полей заявления

Наименование поля	Заполнение	Условное обозначение в сертификате
Фамилия, Имя, Отчество	Раздел 4	CN
Организация	Раздел 5	O
Субъект РФ	Раздел 6	S
Населенный пункт	Раздел 7	L
Должность	Раздел 8	T
СНИЛС	Раздел 9	СНИЛС
ОГРН	Раздел 10	ОГРН
ИНН	Раздел 11	ИНН

3. Общие требования к заполнению полей

3.1. Не разрешается использовать пробел в начале и в конце текста.

3.2. Каждое слово в тексте должно быть отделено 1 пробелом.

3.3. Перечень допустимых символов приведен в разделе 12.

3.4.Символы, дополнительно приведенные в разделе 12, разрешается использовать только в том случае, если они встречаются внутри официальных названий, указанных в документах.

4. Поле «Фамилия, Имя, Отчество»

4.1.Поле является обязательным для заполнения.

4.2.Поле «Фамилия, Имя, Отчество» должно быть заполнено полностью так, как оно указано в основном документе, удостоверяющем личность будущего владельца сертификата.

4.3.Максимальная длина поля составляет 64 символа.

4.4.Если в фамилии, имени или отчестве в написании присутствует «дефис», то в сертификат так и вносится с дефисом без пробелов (например: Салтыков-Щедрин).

4.5.Если фамилия, имя или отчество состоит из нескольких слов разделенных пробелом, то в сертификат вносится одним словом, части которого соединены «подчеркиванием» без пробелов (например: фамилия «Ван Чо» будет записана Ван_Чо).

4.6.Разрешается использование символов из раздела 12, за исключением символов:

Символ	Название	Символ	Название
"	универсальная кавычка	+	знак плюс
%	процент	«	двойная левая угловая кавычка
&	амперсанд	№	знак номер
'	апостроф	»	двойная правая угловая кавычка

5. Поле «Организация»

5.1.Поле является обязательным для заполнения при оформлении заявления по форме № 1.

5.2.Поле «Организация» должно быть заполнено в виде полного или сокращенного наименования заявителя согласно записи в Едином государственном реестре юридических лиц.

5.3.Рекомендуемая длина поля составляет не более 128 символов.

6. Поле «Субъект РФ»

6.1.Поле является обязательным для заполнения.

6.2.Поле «Субъект РФ» заполняется, как наименование субъекта РФ в соответствии с адресом местонахождения заявителя (при оформлении заявления по форме № 1), либо в соответствии с адресом регистрации будущего владельца сертификата (при оформлении заявления по форме № 2).

6.3.Максимальная длина поля составляет 128 символов.

6.4.Первое слово – номер (код) региона, текст длиной 2 цифры, лидирующий ноль указывать обязательно. Код должен соответствовать КЛАДР.

6.5.1 пробел.

6.6.Остальной текст – название региона с заглавной буквы. Название региона должно соответствовать КЛАДР.

7. Поле «Населенный пункт»

7.1. Обозначает наименование населенного пункта, без указания типа населенного пункта (город, село, поселок, г., с., п., и т.д.), в соответствии с адресом местонахождения заявителя (при оформлении заявления по форме № 1), либо в соответствии с адресом регистрации будущего владельца сертификата (при оформлении заявления по форме № 2).

7.2. Максимальная длина поля составляет 128 символов.

8. Поле «Должность»

8.1.Поле является обязательным для заполнения при оформлении заявления по форме № 1.

8.2.Поле «Должность» заполняется, как наименование должности будущего владельца сертификата, действующего от имени заявителя.

8.3.Рекомендуемая длина поля составляет 64 символа.

9. Поле «СНИЛС»

9.1.Поле является обязательным для заполнения.

9.2.В поле «СНИЛС» заносится страховой номер будущего владельца сертификата.

9.3.Длина поля составляет 11 цифр.

10. Поле «ОГРН»

10.1. Поле является обязательным для заполнения при оформлении заявления по форме № 1.

10.2. В поле «ОГРН» заносятся данные заявителя, указанные в записи Единого государственного реестра юридических лиц, действующие на момент подачи заявления.

10.3. Длина поля составляет 13 цифр.

11. Поле «ИНН»

11.1. Поле является обязательным для заполнения.

11.2. В поле «ИНН» заносятся данные заявителя (при оформлении заявления по форме № 1), либо будущего владельца сертификата (при оформлении заявления по форме № 2).

11.3. Длина поля составляет 10 цифр (при оформлении заявления по форме № 1), либо 12 цифр (при оформлении заявления по форме № 2).

12. Перечень допустимых символов

Кроме цифр, символов латинского и кириллического алфавита допустимо использовать следующие символы:

Символ	Название	Символ	Название
	пробел	-	Дефис
"	универсальная кавычка	.	Точка
%	процент	:	Двоеточие
&	амперсанд	;	точка с запятой
'	апостроф	@	коммерческое АТ, «собака»
(левая скобка	<u> </u>	Подчеркивание
)	правая скобка	«	двойная левая угловая кавычка
+	знак плюс	№	знак номер
,	запятая	»	двойная правая угловая кавычка

