Регламент
удостоверяющего центра
ФСО России

(утвержден 30 июня 2020 г.)

Москва 2020

I. Общие положения

1. В настоящем Регламенте удостоверяющего центра ФСО России (далее – Регламент и УЦ соответственно) применяются следующие термины и определения:

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

3. 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.

4. 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, 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.

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

6. 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).

7. Ключевой носитель – отчуждаемый физический носитель информации, содержащий ключ электронной подписи. Допускается применять в качестве ключевых носителей устройства типа e Token, Rutoken, JaCarta.

8. 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).

9. 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.

10. 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 (далее – реестр сертификатов).

11. 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).

12. 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 реестре выданных и аннулированных (отозванных) сертификатов.

13. 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.

14. 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.

Средства электронной подписи должны иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом.

15. 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.

Предмет регулирования

16. Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

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

18. 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.

19. Регламент размещается на Странице УЦ в формате pdf.

20. 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.

21. Внесение изменений в Регламент, включая приложения к нему, производится путем размещения Регламента согласно п. 19 Регламента.

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.

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.

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

Сведения об УЦ

22. 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».

23. 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.

24. Реквизиты УЦ:

Полное наименование: удостоверяющий центр Федеральной службы охраны Российской Федерации.

Место нахождение юридического лица: город Москва, Кремль-9.

Фактическое место нахождение:

город Москва, улица Мясницкая 48, строение 1;

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

Порядок информирования о предоставлении услуг УЦ

25. УЦ осуществляет информирование о предоставлении услуг по телефонам, по электронной почте, через Страницу УЦ.

26. Справочные телефоны адреса электронной почты УЦ

Контактная информация: тел. (495) 914-13-34, (495) 914-13-26

E-mail: ucgspi@msk.rsnet.ru, uc@gov.ru

Контактная информация: тел. (495) 606-21-13, (495) 606-49-72
E-mail: dotsenko_a@gov.ru

II. Перечень реализуемых УЦ функций, оказываемых услуг (далее – услуги)

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

28. 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.

29. Услуги, указанные в п. 28 Регламента, предоставляются заявителям по информационному взаимодействию безвозмездно.

III. Права и обязанности УЦ и владельцев сертификатов

30. УЦ имеет право:

отказывать в регистрации заявления на изготовление сертификата ключа проверки электронной подписи в случае непредставления или ненадлежащего оформления необходимых документов;

отказывать в аннулировании (отзыве) сертификата в случае ненадлежащего оформления соответствующего заявления;

отказывать в аннулировании (отзыве), если истек установленный срок действия ключа электронной подписи, соответствующего сертификату;

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, планового или внепланового технического обслуживания реестра сертификатов.

31. Владелец сертификата имеет право:

применять сертификат УЦ для проверки электронной подписи в сертификатах, изготовленных УЦ;

применять для хранения ключа электронной подписи ключевой носитель, поддерживаемый средствами электронной подписи УЦ и владельца

сертификата;

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;

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

32. УЦ обязан:

предоставить заявителю (доверенному лицу) сертификат УЦ в электронной форме;

принимать меры по защите ключей электронной подписи от несанкционированного доступа при их генерации в УЦ;

обеспечивать регистрацию заявителей и занесение регистрационной информации владельцев сертификатов в реестр УЦ;

обеспечивать конфиденциальность созданных УЦ ключей электронных подписей до их передачи владельцам сертификатов (доверенным лицам);

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

приостанавливать действие сертификата по заявлению владельца сертификата;

аннулировать (отзывать) сертификат в случаях, указанных в Регламенте;

производить внеплановую замену сертификатов в случаях, определенных Регламентом;

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;

уведомлять владельца сертификата о факте изготовления или аннулирования сертификата;

уведомлять владельцев сертификатов о приостановке деятельности УЦ за две недели до приостановки деятельности УЦ;

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

33. Владелец сертификата обязан:

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;

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;

хранить в тайне (обеспечивать конфиденциальность) ключ электронной подписи, принимать все возможные меры для предотвращения его утраты,

раскрытия, искажения и (или) несанкционированного использования;

применять для формирования электронной подписи только действующий ключ электронной подписи;

использовать для создания и проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи;

уведомлять УЦ о нарушении конфиденциальности ключа электронной подписи в течение рабочего дня со дня получения информации о таком нарушении;

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;

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;

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;

не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован или действие которого прекращено;

использовать средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с положениями документации на применяемое средство электронной подписи.

IV. Порядок и сроки выполнения процедур, необходимых для предоставления услуг УЦ

Процедура создания ключей электронных подписей и ключей проверки электронных подписей

34. Порядок создания ключей электронных подписей и ключей проверки электронных подписей реализуется с учетом следующих способов создания:

заявитель создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования СКЗИ, согласованными с Федеральной службой безопасности Российской Федерации;

удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами

пользования СКЗИ, согласованными с Федеральной службой безопасности Российской Федерации.

35. 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.

36. Срок действия ключа электронной подписи УЦ составляет максимально допустимый срок действия, установленный для применяемых средств УЦ и ЭП, с использованием которых данный ключ электронной подписи был создан.

37. Начало периода действия ключа электронной подписи УЦ исчисляется с даты и времени создания сертификата УЦ.

38. Плановая смена ключа электронной подписи УЦ выполняется в период действия ключа электронной подписи УЦ.

39. УЦ уведомляет владельцев сертификатов о сроках плановой смены ключа электронной подписи УЦ и действиях владельцев сертификатов в связи со сменой ключа электронной подписи УЦ посредством размещения информации на Странице УЦ.

40. Процедура плановой смены ключа электронной подписи УЦ включает:

создание за 1 (один) месяц до даты смены ключа электронной подписи УЦ нового ключа электронной подписи и соответствующего ему нового сертификата;

размещение нового сертификата УЦ на Странице УЦ.

41. Владелец сертификата получает новый сертификат УЦ на Странице УЦ.

42. Для замены ключа электронной подписи владельца сертификата выполняется процедура создания и выдачи сертификатов, описанная в Регламенте.

43. Внеплановая замена ключа электронной подписи УЦ осуществляется в случае нарушения конфиденциальности или угрозы нарушения конфиденциальности такого ключа. В этом случае ключ электронной подписи УЦ и соответствующий ему сертификат прекращают действовать.

К событиям, на основании которых принимается решение о нарушения конфиденциальности ключа электронной подписи, относятся, включая, но не ограничиваясь, следующие:

утрата носителей ключа электронной подписи;

утрата носителей ключа электронной подписи с последующим обнаружением;

возникновение подозрений на нарушение конфиденциальности ключа электронной подписи;

нарушение целостности печатей на сейфах с носителями ключа электронной подписи, если используется процедура опечатывания сейфов;

временный доступ посторонних лиц к носителям ключа электронной подписи, а также другие события, при которых достоверно не известно, что произошло с носителями ключа электронной подписи.

44. Все сертификаты, подписанные с использованием скомпрометированного ключа электронной подписи УЦ, прекращают действовать с момента времени создания Списка отозванных сертификатов, содержащего сведения о сертификате УЦ, прекратившем действовать, с занесением сведений об этих сертификатах в реестр сертификатов.

45. УЦ незамедлительно уведомляет о компрометации ключа электронной подписи УЦ и действиях владельцев сертификатов в связи с заменой ключа электронной подписи УЦ посредством размещения данной информации на Странице УЦ.

46. Для замены скомпрометированного ключа электронной подписи и соответствующего ему сертификата УЦ выполняет процедуру создания нового ключа электронной подписи УЦ и соответствующего ему нового сертификата по аналогии с п. 40 Регламента.

47. Для замены ключа электронной подписи владельца сертификата выполняется процедура создания и выдачи сертификатов, описанная в Регламенте.

48. 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.

49. Администратор/Оператор УЦ выполняет плановую смену ключа электронной подписи и изготовление нового сертификата владельца сертификата на основании заявления на изготовление сертификата ключа проверки электронной подписи (приложение № 2 и приложение № 3), поданного не ранее 90 и не позднее 15 календарных дней до окончания срока действия ключа электронной подписи.

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

51. Внеплановая смена ключа электронной подписи и сертификата владельца 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.

Процедура создания и выдачи сертификатов

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

53. 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. 24 Регламента. Требования к заполнению полей и их состав приведены в приложении № 4 к Регламенту.

Заявление на изготовление сертификата ключа проверки электронной подписи может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью;

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) либо документ, в том числе электронный, подтверждающий регистрацию в системе обязательного пенсионного страхования в случае отсутствия 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.

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

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

56. 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). Для заполнения сертификата Удостоверяющий центр запрашивает и получает сведения из государственных информационных ресурсов.

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

58. 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.

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

60. 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.

61. 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.

62. 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.

63. Срок создания и выдачи сертификата с момента получения УЦ соответствующего заявления не превышает 5 (пяти) рабочих дней.

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

Подтверждение действительности электронной подписи

65. УЦ по заявлению заявителя/владельца сертификата предоставляет услугу по подтверждению действительности электронной подписи. Заявление на подтверждение действительности электронной подписи электронного документа (приложение № 5) должно содержать следующую информацию:

дата и время подачи заявления на подтверждение действительности электронной подписи электронного документа;

идентификационные данные владельца сертификата, действительность электронной подписи которого необходимо подтвердить в электронном документе;

время и дата, на момент наступления которых требуется установить действительность электронной подписи.

66. Заявление на подтверждение действительности электронной подписи электронного документа составляется на бумажном носителе, подписывается заявителем/владельцем сертификата.

67. К заявлению на подтверждение действительности электронной подписи электронного документа должны быть приложены на информационном носителе:

сертификат заявителя/владельца сертификата, с использованием которого необходимо осуществить подтверждение действительности электронной подписи электронного документа;

электронный документ с электронной подписью.

68. УЦ в результате проведения работ по подтверждению действительности электронной подписи электронного документа составляет заключение, которое должно содержать:

основание для проведения проверки действительности электронной

подписи в электронном документе;

результат проверки действительности электронной подписи электронного документа;

сведения, представленные УЦ для проведения проверки действительности электронной подписи электронного документа;

отчет по выполненной проверке действительности электронной подписи электронного документа, содержащий время и место проведения проверки, содержание и результаты проверки.

69. Заключение УЦ по выполненной проверке действительности электронной подписи электронного документа составляется в произвольной форме в 2 (двух) экземплярах на бумажном носителе.

70. Один экземпляр заключения по выполненной проверке действительности электронной подписи электронного документа передается заявителю/владельцу сертификата.

71. Срок предоставления услуги по подтверждению действительности электронной подписи электронного документа не может превышать 5 (пяти) рабочих дней с момента поступления Заявления на подтверждение действительности электронной подписи электронного документа в УЦ.

Процедуры, осуществляемые при прекращении действия и аннулировании (отзыва) сертификата

72. Аннулирование (отзыв) или прекращение действия сертификата 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 УЦ без перехода его функций другим лицам;

в иных случаях, установленных Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», другими федеральными законами и 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.

73. 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.

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

75. 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.

76. 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.

77. Заявление на аннулирование (отзыв) или прекращение действия сертификата оформляется по форме, согласно приложению № 6 к Регламенту.

78. 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.

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

80. 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 от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», или в течение двенадцати часов с момента получения УЦ соответствующих сведений.

81. Получение информации о статусе сертификата, изданного УЦ, осуществляется на основании заявления в УЦ о получении соответствующей информации по форме, согласно приложению № 7 к Регламенту. Предоставление указанного заявления может быть осуществлено при личном прибытии в УЦ, по электронной почте, почтовой и иной связью.

82. 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.

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

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

Порядок ведения реестра сертификатов

85. УЦ ведет реестр 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 сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Размещение списка отозванных сертификатов производится Администратором/Оператором УЦ на Странице УЦ.

86. Срок внесения информации о прекращении действия или аннулировании (отзыве) сертификата в реестр сертификатов указан в п. 78 настоящего Регламента.

Порядок технического обслуживания реестра сертификатов

87. Плановое и внеплановое техническое обслуживание реестра сертификатов не может превышать 1 (одного) рабочего дня.

УЦ заблаговременно оповещает владельцев сертификатов о проведении планового или внепланового технического обслуживания реестра сертификатов и иных работ, указанных в п. 30 Регламента, на Странице УЦ.

V. Порядок исполнения обязанностей УЦ

Информирование заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи

88. УЦ информирует владельцев сертификатов о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, предоставлением владельцам сертификатов Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи.

Выдача по обращению заявителя средств электронной подписи

89. Средства электронной подписи должны в соответствии с ч. 4 статьи 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями;

Обеспечение актуальности информации, содержащейся в реестре сертификатов

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

Обеспечение доступности реестра сертификатов

91. УЦ обеспечивает доступность реестра сертификатов в информационно-телекоммуникационной сети «Интернет» на Странице УЦ в любое время, за исключением периодов технического обслуживания реестра сертификатов.

Порядок обеспечения конфиденциальности созданных УЦ ключей электронных подписей

92. Ключ электронной подписи является конфиденциальной информацией. УЦ обеспечивает конфиденциальность созданных УЦ ключей электронных подписей, информации, содержащейся в паролях, идентификаторах, а также в документах владельца сертификата и персональных данных владельца сертификата, которая становится доступной УЦ в связи с выполнением им своих функций в соответствии с Регламентом.

93. При создании ключа электронной подписи и ключа проверки электронной подписи используется автоматизированное рабочее место УЦ, аттестованное на соответствие требованиям законодательства Российской Федерации по технической защите информации, размещенное в помещении, доступ в которое ограничен. Ключ электронной подписи, созданный таким образом, записывается УЦ н ключевой носитель, который выдается Владельцу сертификата по окончании процедуры его выдачи.

94. Хранение в УЦ всех выданных сертификатов осуществляется

постоянно в форме электронных документов.

95. Документы на бумажных носителях, в том числе копии сертификатов на бумажном носителе, хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

96. Документы, подлежащие архивному хранению, являются документами временного хранения.

97. Документы, срок архивного хранения которых закончился, подлежат уничтожению в порядке, уставленным законодательством Российской Федерации об архивном деле.

Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации (далее – ЕСИА)

98. При выдаче сертификата УЦ направляет в 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).

Осуществление по желанию лица, которому выдан сертификат, его регистрации в ЕСИА

99. При выдаче сертификата по желанию владельца сертификата УЦ безвозмездно осуществляет его регистрацию в ЕСИА.

Безвозмездное предоставление любому лицу доступа к информации, содержащейся в реестре сертификатов

100. УЦ предоставляет любому лицу посредством Страницы УЦ доступ к информации, содержащейся в реестре сертификатов, включая информацию о прекращении действия сертификата или об аннулировании сертификата, в том числе путем публикации перечня прекративших свое действие (аннулированных) сертификатов.

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	*фамилия, имя, отчество будущего владельца сертификата*
Организация	*наименование заявителя*
Должность	*должность будущего владельца сертификата*
Субъект РФ	*код региона, наименование субъекта РФ*
Населенный пункт	*наименование населенного пункта*
Адрес	*Адрес местонахождения заявителя*
СНИЛС	*СНИЛС будущего владельца сертификата*
ОГРН	*ОГРН заявителя*
ИНН	*ИНН заявителя*
E-mail	*электронный адрес будущего владельца сертификата*

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

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 № 4
к Регламенту

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 года № 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 Российской Федерации 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	_	Подчеркивание
)	правая скобка	«	двойная левая угловая кавычка
+	знак плюс	№	знак номер
,	запятая	»	двойная правая угловая кавычка

Приложение № 5
к Регламенту

В удостоверяющий
центр ФСО России

Заявление на подтверждение действительности электронной подписи электронного документа

_____
(фамилия, имя, отчество для физического лица, полное наименование организации с указанием организационно-правовой формы)

в лице _____,
(наименование должности руководителя или уполномоченного сотрудника заявителя (для юридических лиц))

действующего на основании_____

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

1. Файл, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку действительности электронной подписи в электронном документе на прилагаемом к заявлению носителе _____;
2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата, на носителе _____;

Время* подписания электронной подписью электронного документа:
"____:____" "____/_____/_____";
Час минута день месяц год

Если момент подписания электронного документа не определен, то указать момент наступления которого необходимо проверить действительность электронной подписи:
"____:____" "____/_____/_____";
Час минута день месяц год

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

« _____ » _____ 20____ г.

М.П.

Приложение № 6
к Регламенту

В удостоверяющий
центр ФСО России

Заявление
на аннулирование (отзыв) или прекращение действия сертификата ключа проверки электронной подписи

_____
(наименование заявителя)

Прошу аннулировать (отозвать или прекратить действие – выделить нужное) сертификат ключа проверки электронной подписи:

Серийный номер сертификата	ФИО владельца сертификата	Код причины отзыва	Подпись владельца сертификата

Код причины отзыва сертификата:
"1" Компрометация ключа
"3" Изменение принадлежности
"4" Сертификат заменен
"5" Прекращение работы

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

« ____ » _____ 20____ г.

М.П.

Приложение № 7
к Регламенту

В удостоверяющий
центр ФСО России

Заявление
на получение информации о статусе сертификата
ключа проверки электронной подписи

Прошу предоставить информацию о статусе сертификата ключа проверки электронной подписи:

Серийный номер сертификата	
Общее имя (CN) сертификата	

Время и дата на момент наступления которых требуется установить статус сертификата*:

с «_____:_____» «_____/_____/_____»
час минута день месяц год

по «_____:_____» «_____/_____/_____»
час минута день месяц год

_____ / _____ /
(подпись) (ФИО)

«____» _____20___ г.

* Время и дата должны быть указаны с учетом часового пояса г. Москвы (по Московскому времени)
Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи заявления в УЦ