Утвержден
Приказом Директора Фонда «Центр инноваций и информационных технологий»
№ 01-01.1/1 от 09 января 2019 г.

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ

Удостоверяющего центра нотариата России
по созданию и управлению неквалифицированными сертификатами
ключей проверки электронной подписи

Редакция №2

г. Москва
2019 г.

Оглавление

1. Сведения об Удостоверяющем центре

Фонд «Центр инноваций и информационных технологий» зарегистрирован на территории Российской Федерации в городе Москва (Свидетельство о регистрации некоммерческой организации № 7714012525 выдано 24.09.2010 г. Министерством Юстиции Российской Федерации, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1107799007425 от 27.02.2010 г.) и осуществляет выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Удостоверяющий центр нотариата России Фонда «Центр инноваций и информационных технологий» (далее - Удостоверяющий центр) осуществляет деятельность по созданию, выдаче и управлению неквалифицированными сертификатами ключей проверки электронных подписей на территории Российской Федерации на основании лицензии ЛЗС № 0015332 от 30 мая 2018 г. выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

Фонд «Центр инноваций и информационных технологий»
Юридический/фактический адрес:
127006, г. Москва, ул. Долгоруковская д. 15, стр. 4-5
Почтовый адрес:
127006, г. Москва, ул. Долгоруковская д. 15, стр. 4-5
Место нахождения Удостоверяющего центра: г. Москва, ул. Долгоруковская д. 15, стр. 4-5;
Тел./факс: (495) 730-57-05
e-mail: ca@fciit.ru
Адрес сайта в сети Интернет: www.fciit.ru

2. Термины и определения

В настоящем Регламенте используются следующие термины и их определения:

1) *Ключ неквалифицированной электронной подписи (далее - Ключ электронной подписи)* - уникальная последовательность символов, предназначенная для создания электронной подписи;

2) *Неквалифицированный ключ проверки электронной подписи (далее - Ключ проверки электронной подписи)* - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи;

3) *Ключ неквалифицированной электронной подписи Удостоверяющего центра (далее - Ключ электронной подписи Удостоверяющего центра)* - Ключ электронной подписи, использующийся Удостоверяющим центром для создания неквалифицированных сертификатов ключей проверки электронной подписи и списков отозванных сертификатов;

4) *Конфиденциальность ключа электронной подписи* - обязанность работника Удостоверяющего центра, создающего Ключ электронной подписи, Заявителя и Владельца сертификата обеспечить защиту Ключа электронной подписи от несанкционированного доступа и использования;

5) *Владелец неквалифицированного сертификата ключа проверки электронной подписи (далее – Владелец сертификата)* – лицо, которому Удостоверяющим центром в соответствии с законодательством Российской Федерации и настоящим Регламентом выдан неквалифицированный Сертификат ключа проверки электронной подписи;

6) *Неквалифицированный сертификат ключа проверки электронной подписи (далее - Сертификат ключа проверки электронной подписи)* - электронный документ, созданный Удостоверяющим центром и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу сертификата;

7) *Неквалифицированный сертификат ключа проверки электронной подписи Удостоверяющего центра* - Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи Удостоверяющего центра в созданных им Сертификатах ключей проверки электронной подписи и Списках отозванных сертификатов;

8) *Средство электронной подписи* - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание Ключа электронной подписи и Ключа проверки электронной подписи;

9) *Средство удостоверяющего центра* - программное и (или) аппаратное средство, используемое Удостоверяющим центром для выполнения своих функций;

10) *Электронный документ* – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

11) *Рабочий день Удостоверяющего центра (далее – рабочий день)* – промежуток времени с 9:00 до 18:00 (Московское время) каждого дня недели за исключением выходных и праздничных дней;

12) *Реестр сертификатов ключей проверки электронных подписей (далее – Реестр сертификатов)* - реестр выданных и аннулированных Удостоверяющим центром Сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром Сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования Сертификатов ключей проверки электронных подписей и об основаниях такого прекращения или аннулирования;

13) *Список отозванных сертификатов* – представленный для публичного доступа электронный документ с электронной подписью Удостоверяющего центра, формируемый на определенный момент времени и включающий в себя список серийных номеров Сертификатов ключей проверки электронных подписей, которые на данный момент времени аннулированы, действие которых прекращено и действие которых приостановлено;

14) *Единая информационная система нотариата России (далее – ЕИС)* – информационно-аналитическая система, предназначенная для предоставления нотариусам дополнительной информации при совершении нотариального действия, выполнения публичных полномочий Федеральной нотариальной палаты и нотариальных палат субъектов Российской Федерации и обеспечения надлежащего уровня защиты прав и законных интересов граждан и организаций в связи с их обращением к нотариусам за совершением нотариальных действий;

15) *Cryptographic Message Syntax (далее - CMS)* – стандарт определяющий формат и синтаксис криптографических сообщений (сообщений, подписанных электронной подписью);

3. Общие положения

1. Регламент деятельности Удостоверяющего центра нотариата России по созданию и управлению неквалифицированными сертификатами ключей проверки электронной подписи, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации.
2. Настоящий Регламент является документом, устанавливающим правила и порядок создания, выдачи и управления Сертификатами ключей проверки электронных подписей.
3. Удостоверяющий центр обеспечивает средствами электронной подписи и создает Ключи электронных подписей нотариусов, лиц, замещающих временно отсутствующих нотариусов, представителей нотариального сообщества для обеспечения функционирования ЕИС, а также иных категорий лиц по решению Правления Федеральной нотариальной палаты. Настоящий

Регламент утверждается единоличным исполнительным органом Фонда «Центр инноваций и информационных технологий» и вводится в действие его приказом.

4. Любое заинтересованное лицо может ознакомиться с Регламентом по запросу на адрес электронной почты ca@fciit.ru.

5. Внесение изменений в Регламент, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

7. Действие настоящего Регламента распространяется на Заявителей, Владельцев сертификатов, а также всех лиц, использующих предоставляемые Удостоверяющим центром информацию и сервисы.

4. Деятельность Удостоверяющего центра:

4.1. Виды деятельности Удостоверяющего центра

Удостоверяющий центр осуществляет следующую деятельность:

1. создание и выдача Сертификатов ключей проверки электронных подписей;
2. установление сроков действия Сертификатов ключей проверки электронных подписей;
3. изготовление Копий сертификатов ключей проверки электронных подписей;
4. аннулирование выданных Удостоверяющим центром Сертификатов ключей проверки электронных подписей;
5. прекращение действия выданных Удостоверяющим центром Сертификатов ключей проверки электронных подписей;
6. обеспечение доступа лиц к информации, содержащейся в Реестре сертификатов (к Списку отозванных сертификатов), в том числе с использованием информационно-телекоммуникационной сети "Интернет";
7. ведение Реестра сертификатов;
8. предоставление информации, содержащейся в Реестре сертификатов, в том числе информации об аннулировании Сертификата ключа проверки электронной подписи;
9. создание Ключей электронных подписей и Ключей проверки электронных подписей;
10. проверка уникальности Ключей проверки электронных подписей в Реестре сертификатов;
11. выдача по обращению Заявителя Средств электронной подписи;
12. осуществление иной деятельности, связанной с использованием электронной подписи.

4.2. Условия деятельности Удостоверяющего центра

Удостоверяющий центр осуществляет свою деятельность на безвозмездной основе для нотариусов, лиц, временно исполняющие обязанности нотариусов, а также иных категорий лиц по решению Правления Федеральной нотариальной палаты.

5. Права и обязанности

5.1. Права и обязанности Удостоверяющего центра

5.1.1. <u>Удостоверяющий центр имеет право:</u>

1. отказать Заявителю в создании Сертификата ключа проверки электронной подписи в случае ненадлежащего оформления им заявления на создание Сертификата ключа проверки электронной подписи;
2. запросить у Заявителя документы, указанные в п.6.1. и необходимые для выдачи Сертификата ключа проверки электронной подписи;

3. отказать Владельцу сертификата в прекращении, приостановлении или возобновлении действия Сертификата ключа проверки электронной подписи в случае ненадлежащего оформления им соответствующего заявления на прекращение, приостановление или возобновление действия Сертификата ключа проверки электронной подписи;

4. в одностороннем порядке приостановить действие Сертификата ключа проверки электронной подписи;

5. в одностороннем порядке вносить изменения в настоящий Регламент в части, не касающейся прав и обязанностей Заявителей и Владельцев сертификатов, если только изменения их прав и обязанностей не обусловлены изменением законодательства Российской Федерации.

5.1.2 Удостоверяющий центр обязан:

1. предоставить Заявителю, Владельцу сертификата по его требованию копию лицензии ЛЗС № 0015332 от 30 мая 2018 г., выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России;

2. предоставить Заявителю Сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме;

3. использовать для создания Ключа электронной подписи Удостоверяющего центра и создания электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации Средства электронной подписи;

4. использовать Ключ электронной подписи Удостоверяющего центра только для подписания создаваемых им Сертификатов ключей проверки электронной подписи и Списков отозванных сертификатов;

5. принять меры по защите Ключа электронной подписи Удостоверяющего центра от несанкционированного доступа и использования;

6. организовать свою работу по Московскому времени, синхронизировать по времени все свои программные и технические средства обеспечения деятельности;

7. создать Сертификат ключа проверки электронной подписи по заявлению на создание Сертификата ключа проверки электронной подписи в порядке, определенном настоящим Регламентом;

8. обеспечить уникальность серийных номеров создаваемых Сертификатов ключей проверки электронной подписи;

9. обеспечить уникальность значений Ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи;

10. обеспечить приём заявлений на прекращение, приостановление или возобновление действия Сертификатов ключей проверки электронной подписи;

11. прекратить действие Сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра, с использованием которого был создан данный сертификат;

12. аннулировать действие Сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;

13. официально уведомить об аннулировании, прекращении, приостановлении или возобновлении действия Сертификата ключа проверки электронной подписи посредством включения соответствующей информации в Список отозванных сертификатов;

14. публиковать 1 (один) раз в сутки актуальный Список отозванных сертификатов на сайте Удостоверяющего центра в сети Интернет по адресу: www.fciit.ru;

15. уведомить о нарушении конфиденциальности Ключа электронной подписи Удостоверяющего центра в течение не более чем одного рабочего дня со дня получения информации о таком нарушении посредством публикации соответствующего уведомления на сайте в сети Интернет по адресу: www.fciit.ru;

16. не использовать Ключ электронной подписи Удостоверяющего центра при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

17. информировать в письменной форме Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с

использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки (Приложение №7);

18. предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании Сертификата ключа проверки электронной подписи;

5.2. Права и обязанности Заявителя и Владельца сертификата

5.2.1. Заявитель, Владелец сертификата имеют право:

1. в одностороннем порядке прекратить взаимодействие с Удостоверяющим центром, направив в Удостоверяющий центр заявление на прекращение действия выданного ему Сертификата ключа проверки электронной подписи;
2. применять Сертификат ключа проверки электронной подписи Удостоверяющего центра для проверки электронной подписи Удостоверяющего центра в Сертификатах ключей проверки электронных подписей;
3. применять Список отозванных сертификатов для установления действительности Сертификатов ключей проверки электронной подписи;
4. обратиться в Удостоверяющий центр с заявлением на создание Сертификата ключа проверки электронной подписи;
5. обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия принадлежащего ему Сертификата ключа проверки электронной подписи в течение срока действия соответствующего Ключа электронной подписи;
6. обратиться в Удостоверяющий центр с заявлением на возобновление действия принадлежащего ему Сертификата ключа проверки электронной подписи в течение срока действия соответствующего Ключа электронной подписи и срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено;
7. обратиться в Удостоверяющий центр за получением справки о действительности Сертификатов ключей проверки электронной подписи на определенный момент времени;
8. при обращении за выдачей Сертификата ключа проверки электронной подписи получить информацию о рисках, связанных с использованием электронной подписи;

5.2.2. Заявитель, Владелец сертификата обязаны:

1. предоставить документы, необходимые для создания Сертификата ключа проверки электронной подписи;
2. обеспечить конфиденциальность принадлежащего ему Ключа электронной подписи;
3. не применять Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
4. для хранения Ключа электронной подписи применять защищенный носитель информации, совместимый одновременно со Средством электронной подписи, применяемым Владельцем сертификата, и Средствами удостоверяющего центра;
5. применять для создания электронной подписи только действующий Ключ электронной подписи;
6. применять Ключ электронной подписи с учетом ограничений, содержащихся в Сертификате ключа проверки электронной подписи, если такие ограничения были установлены;
7. прекратить использование Ключа электронной подписи и немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия соответствующего ему Сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности Ключа электронной подписи;
8. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента подачи заявления на прекращение действия сертификата в Удостоверяющий центр до официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;

9. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, с момента подачи заявления на приостановление действия сертификата в Удостоверяющий центр до официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия;

10. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

11. не использовать Ключ электронной подписи до приобретения статуса Владельца сертификата в соответствии с порядком, предусмотренным настоящим Регламентом;

12. использовать для создания и проверки квалифицированных электронных подписей, создания Ключа электронной подписи и Ключа проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации Средства электронной подписи, и применять эти средства в соответствии с правилами установленными нормативными правовыми актами Российской Федерации;

13. использовать при проверке электронной подписи в электронных документах актуальную информацию о Сертификатах ключей проверки электронных подписей, которые на данный момент времени аннулированы, действие которых прекращено и действие которых приостановлено, содержащуюся в Списке отозванных сертификатов, размещенном в сети Интернет по адресу: www.fciit.ru;

14. незамедлительно уведомить Удостоверяющий центр об изменении данных, указанных в заявлении на создание Сертификата ключа проверки электронной подписи, а так же иных данных предоставленных в Удостоверяющий центр;

15. соблюдать требования настоящего Регламента.

6. Порядок создания и выдачи Сертификатов ключей проверки электронной подписи и управления ими

Ключ электронной подписи считается действующим на определенный момент времени (действующий Ключ электронной подписи), если:

а) наступило время начала действия Ключа электронной подписи;

б) срок действия Ключа электронной подписи не истек;

в) Сертификат ключа проверки электронной подписи, соответствующий данному Ключу электронной подписи, действует на данный момент времени.

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

а) наступил момент начала действия Сертификата ключа проверки электронной подписи;

б) срок действия Сертификата ключа проверки электронной подписи не истек;

в) Сертификат ключа проверки электронной подписи не аннулирован, не прекратил действие и действие его не приостановлено.

6.1. Формирование Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи в Удостоверяющем центре в присутствии Заявителя

1. Удостоверяющий центр создает Сертификат ключа проверки электронной подписи в присутствии Заявителя на основании представленного им заявления на создание Сертификата ключа проверки электронной подписи. Формы заявлений на создание Сертификата ключа проверки электронной подписи приведены в Приложениях № 1, №1а, №1б, №1в настоящего Регламента.

2. Вместе с заявлением на создание Сертификата ключа проверки электронной подписи Заявителем предоставляются следующие документы:

а)Если Заявитель является юридическим лицом или работником юридического лица:

−выписка или нотариально заверенная копия выписки из Единого государственного реестра юридических лиц, полученная не ранее чем за один месяц до обращения в Удостоверяющий центр (если Заявителем является работник нотариальной палаты, то выписку из Единого государственного реестра юридических лиц получает работник Удостоверяющего центра с использованием ЕИС);

−нотариально заверенная копия свидетельства о постановке организации на учет в налоговом органе;

−нотариально заверенная копия Устава организации;

−заверенные юридическим лицом копии протоколов либо иных документов о назначении лиц, имеющих право действовать от имени юридического лица без доверенности;

−надлежащим образом оформленные доверенности на физических лиц, имеющих право действовать от имени юридического лица, которые указываются в Сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица;

−заверенные юридическим лицом копии приказов о назначении лиц, имеющих право действовать от имени юридического лица, которые указываются в Сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица (в том случае, если в Сертификате ключа проверки электронной подписи должна указывается должность данного лица);

−документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность - для тех лиц, которые указываются в Сертификатах ключей проверки электронной подписи наряду с указанием наименования юридического лица (либо нотариально заверенные копии этих документов);

−страховое свидетельство государственного пенсионного страхования для тех лиц, которые указываются в Сертификатах ключей проверки электронной подписи.

б) Если Заявитель является физическим лицом:

−документы, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность или их нотариально заверенные копии (для нотариусов и/или лиц, временно исполняющих обязанности нотариусов, возможно предоставление указанных документов, заверенных работником Нотариальной палаты, членом которой является Заявитель);

−страховое свидетельство государственного пенсионного страхования;

−свидетельство о постановке на учет в налоговом органе (либо нотариально заверенная копия, (для нотариусов и/или лиц, временно исполняющих обязанности нотариусов, возможно предоставление указанных документов, заверенных работником нотариальной палаты, членом которой является Заявитель).

В случае несогласованности документов, предоставляемых Заявителем – физическим лицом или работником юридического лица, дополнительно по требованию Удостоверяющего центра предоставляется документ, подтверждающий смену фамилии, имени, отчества: свидетельство о заключении брака, свидетельство о расторжении брака, свидетельство о перемене имени, фамилии, отчества.

3. Предоставление документов, указанных в пункте 2 настоящего раздела Регламента, для создания Сертификата ключа проверки электронной подписи в Удостоверяющем центре может быть осуществлено уполномоченным представителем Заявителя, действующим на основании соответствующей доверенности, которая для Заявителя - физического лица должна быть составлена по форме Приложения № 3а к настоящему Регламенту и удостоверена нотариально, а для Заявителя – представителя юридического лица по форме Приложения № 3б к настоящему

Регламенту за подписью руководителя или иного лица, уполномоченного на это его учредительными документами, с приложением печати этой организации.

4. Работник Удостоверяющего центра, на основе предоставленных документов, осуществляет создание ключей электронной подписи, запись Ключа электронной подписи на защищенный носитель информации, предоставленный Заявителем, создание Сертификата ключа проверки электронной подписи, запись Сертификата ключа проверки электронной подписи на защищенный носитель информации.

5. По окончании процедуры создания Сертификата ключа проверки электронной подписи Заявителю выдается защищенный носитель информации, содержащий Ключ электронной подписи и Сертификат ключа проверки электронной подписи.

6. При получении первого Сертификата ключа проверки электронной подписи Заявителю (либо его полномочному представителю) сообщается ключевая фраза, использующаяся для аутентификации Владельца сертификата при выполнении регламентных процедур, возникающих при нарушении конфиденциальности Ключа электронной подписи Владельца сертификата.

При получении второго и последующих сертификатов, ключевая фраза не изменяется.

Заявитель приобретает статус Владельца сертификата после получения защищенного носителя информации в соответствии с пунктом 5 настоящего раздела Регламента.

6.2. Формирование Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи в Удостоверяющем центре без присутствия Заявителя

6.2.1. Формирование посредством ЕИС Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи без присутствия в Удостоверяющем центре Заявителя, являющегося нотариусом либо лицом исполняющим обязанности нотариуса, либо работником нотариальной палаты субъекта Российской Федерации

1. Для формирования Ключа электронной подписи и получения Сертификата ключа проверки электронной подписи посредством ЕИС Заявитель должен быть зарегистрирован в ЕИС и иметь доступ к ЕИС.

2. Заявитель предоставляет в Удостоверяющий центр посредством ЕИС:

а)файл запроса на создание Сертификата ключа проверки электронной подписи;

б) заявление на создание Сертификата ключа проверки электронной подписи в электронной форме.

3. Если Заявитель имеет действующий Ключ электронной подписи и соответствующий ему действующий Сертификат ключа проверки электронной подписи, он подписывает своей электронной подписью заявление на создание Сертификата ключа проверки электронной подписи в электронной форме.

4. Работник Удостоверяющего центра в течение 3 (трех) рабочих дней осуществляет проверку корректности заполнения файла запроса и заявления на создание Сертификата ключа проверки электронной подписи в электронной форме, а также определяет и сообщает Заявителю перечень документов, необходимых для создания Сертификата ключа проверки электронной подписи, из числа документов, содержащихся в перечне, установленном пунктом 2 раздела 6.1 настоящего Регламента.

5. Если заявление на создание Сертификата ключа проверки электронной подписи не подписано электронной подписью Заявителя, он должен предоставить в Удостоверяющий центр заявление на бумажном носителе, подлинность подписи Заявителя на котором нотариально засвидетельствована, (для нотариусов и/или лиц, временно исполняющих обязанности нотариусов, возможно предоставление заявления, подлинность подписи Заявителя на котором засвидетельствована работником нотариальной палаты, членом которой является Заявитель).

6. В случае необходимости Заявитель направляет в Удостоверяющий центр требуемые документы с использованием почтовой либо курьерской службы или через нотариуса, имеющего действующий Сертификат ключа проверки электронной подписи. Нотариус,

засвидетельствовавший подлинность собственноручной подписи Заявителя, направляет через ЕИС сканированные копии требуемых документов, подписанные его (нотариуса) электронной подписью, (для нотариусов и/или лиц, временно исполняющих обязанности нотариусов, возможно направление через ЕИС сканированных копий требуемых документов, подписанных электронной подписью работника нотариальной палаты, членом которой является Заявитель, засвидетельствовавшего подлинность подписи Заявителя).

7. После получения Удостоверяющим центром заявительных документов работник Удостоверяющего центра в течение 3 (трех) рабочих дней по результатам проверки соответствия содержащихся в них сведений принимает решение о создании Сертификата ключа проверки электронной подписи.

8. В случае отказа в создании Сертификата ключа проверки электронной подписи работник Удостоверяющего центра уведомляет об этом Заявителя с указанием причины.

9. При принятии положительного решения работник Удостоверяющего центра создает Сертификат ключа проверки электронной подписи и предоставляет его Заявителю через ЕИС.

10. Заявитель подтверждает факт ознакомления с информацией, содержащейся в Сертификате ключа проверки электронной подписи, посредством подписания указанной информации своей электронной подписью.

11. При получении первого Сертификата ключа проверки электронной подписи работник Удостоверяющего центра сообщает Заявителю через ЕИС ключевую фразу, используемую для аутентификации Владельца сертификата при выполнении регламентных процедур, возникающих при нарушении конфиденциальности Ключа электронной подписи Владельца сертификата. При получении второго и последующих сертификатов, ключевая фраза не изменяется.

Заявитель приобретает статус Владельца сертификата после подтверждения факта ознакомления с информацией, содержащейся в Сертификате ключа проверки электронной подписи.

6.2.2. Формирование Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи без присутствия в Удостоверяющем центре Заявителя, не являющегося нотариусом либо лицом, исполняющим обязанности нотариуса, либо работником нотариальной палаты субъекта Российской Федерации

1. Формирование Ключа электронной подписи и файла запроса на создание Сертификата ключа проверки электронной подписи осуществляется Заявителем с использованием имеющегося у него рекомендованного Удостоверяющим центром специализированного программного обеспечения (далее – СПО), предназначенного для формирования с использованием Средства электронной подписи файла запроса на создание Сертификата ключа проверки электронной подписи в формате, позволяющем Удостоверяющему центру создать по данному запросу Сертификат ключа проверки электронной подписи.

2. Заявитель формирует на своем рабочем месте Ключ электронной подписи, файл запроса на создание Сертификата ключа проверки электронной подписи и заполняет заявление на создание Сертификата ключа проверки электронной подписи по форме Приложения №2 к настоящему Регламенту. Подлинность подписи Заявителя на заполненном заявлении должна быть засвидетельствована нотариусом.

3. Заявитель направляет в Удостоверяющий центр:

а) файл запроса на создание Сертификата ключа проверки электронной подписи;

б) заявление на создание Сертификата ключа проверки электронной подписи в электронной форме.

4. Файл запроса на создание Сертификата ключа проверки электронной подписи и заявление на создание Сертификата ключа проверки электронной подписи в электронной форме направляются в Удостоверяющий центр с использованием СПО. Заявление на создание Сертификата ключа проверки электронной подписи направляется также на почтовый адрес Удостоверяющего центра либо курьерской службой по адресу местонахождения Удостоверяющего центра.

5. Кроме выполнения указанных действий Заявитель должен направить посредством почтовой или курьерской связи в Удостоверяющий центр актуальные документы согласно перечню, установленному в части второй раздела 6.1 настоящего Регламента (если они ранее не

предоставлялись в Удостоверяющий центр). Конкретный перечень предоставляемых документов может быть предварительно согласован с Удостоверяющим центром.

6. После получения Удостоверяющим центром заявительных документов работник Удостоверяющего центра в течение 3 (трех) рабочих дней осуществляет проверку соответствия содержащихся в них сведений и по результатам проверки принимает решение о создании Сертификата ключа проверки электронной подписи.

7. В случае отказа в создании Сертификата ключа проверки электронной подписи работник Удостоверяющего центра уведомляет об этом Заявителя с указанием причины.

8. При принятии положительного решения о создании Сертификата ключа проверки электронной подписи работник Удостоверяющего центра создает Сертификат ключа проверки электронной подписи.

9. Заявитель подтверждает факт ознакомления с информацией, содержащейся в Сертификате ключа проверки электронной подписи, посредством подписания указанной информации своей электронной подписью.

10. При получении первого Сертификата ключа проверки электронной подписи работник Удостоверяющего центра сообщает Заявителю с использованием СПО ключевую фразу, используемую для аутентификации Владельца сертификата при выполнении регламентных процедур, возникающих при нарушении конфиденциальности Ключа электронной подписи Владельца сертификата. При получении Заявителем последующих сертификатов, ключевая фраза не изменяется.

Заявитель приобретает статус Владельца сертификата после подтверждения факта получения Сертификата ключа проверки электронной подписи.

6.3. Порядок управления Сертификатами ключа проверки электронной подписи

6.3.1. Приостановление действия Сертификата ключа проверки электронной подписи

1. Удостоверяющий центр приостанавливает действие Сертификата ключа проверки электронной подписи в следующих случаях:
   - по заявлению Владельца сертификата;
   - по инициативе Удостоверяющего центра.
2. Действие Сертификата ключа проверки электронной подписи приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия технологического Сертификата ключа проверки электронной подписи составляет 15 (Пятнадцать) дней.
3. Если в течение срока приостановления действия Сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то действие данного сертификата прекращается Удостоверяющем центром.
4. Официальным уведомлением о факте приостановления действия Сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) Списка отозванных сертификатов, содержащего сведения о Сертификате ключа проверки электронной подписи, действие которого было приостановлено, и изданного не ранее времени принятия Удостоверяющим центром решения о приостановлении действия.
5. Приостановление действия Сертификата ключа проверки электронной подписи может осуществляться по заявлению Владельца сертификата подаваемого в форме документа на бумажном носителе или в форме электронного документа, либо в устной форме.
6. Подача Владельцем сертификата заявления на приостановление действия Сертификата ключа проверки электронной подписи в форме документа на бумажном носителе осуществляется посредством почтовой или курьерской связи по форме Приложения № 4 к настоящему Регламенту.
7. Приостановление действия Сертификата ключа проверки электронной подписи по инициативе Удостоверяющего центра осуществляется в следующих случаях:
   - при наличии оснований, позволяющих предполагать, что нарушена конфиденциальность Ключа электронной подписи Владельца сертификата;

• неисполнения Владельцем сертификата обязанностей, предусмотренных настоящим Регламентом;

6.3.2. Возобновление действия Сертификата ключа проверки электронной подписи

1. Удостоверяющий центр возобновляет действие Сертификата ключа проверки электронной подписи только по заявлению Владельца сертификата, направленного в Удостоверяющий центр в форме документа на бумажном носителе по форме Приложения № 4 к настоящему Регламенту посредством почтовой или курьерской связи. Подача заявления на возобновление действия Сертификата ключа проверки электронной подписи возможна не позднее 5 (пяти) рабочих дней до окончания срока, на который было приостановлено действие Сертификата ключа проверки электронной подписи.

2. Удостоверяющий центр принимает решение о возобновлении Сертификата ключа проверки электронной подписи в течение 5 (пяти) рабочих дней, следующих за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр, и уведомляет об этом решении Владельца сертификата.

3. Официальным уведомлением о факте возобновления действия Сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) Списка отозванных сертификатов, содержащего сведения о Сертификате ключа проверки электронной подписи, действие которого было возобновлено.

4. Возобновление действия Сертификата ключа проверки электронной подписи возможно только в течение срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено с учетом подачи заявления на возобновление не позднее 5 (пяти) рабочих дней до окончания срока, на который было приостановлено действие Сертификата ключа проверки электронной подписи.

6.3.3. Прекращение действия Сертификата ключа проверки электронной подписи

Удостоверяющий центр прекращает действие Сертификата ключа проверки электронной подписи, в следующих случаях:

а) в связи с истечением установленного срока действия Сертификата ключа проверки электронной подписи;

б) на основании заявления Владельца сертификата;

в) в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;

г) при нарушении конфиденциальности Ключа электронной подписи Удостоверяющего центра;

6.4. Порядок предоставления информации Удостоверяющего центра

6.4.1. Порядок предоставления информации об изменении документов, ранее предоставленных в Удостоверяющий центр для получения Сертификата ключа проверки электронной подписи

В случае изменения, какого-либо документа, ранее предоставленного в Удостоверяющий центр Владелец сертификата предоставляет в Удостоверяющий центр сведения об измененном документе одним из следующих способов:

– лично доставляет оригинал измененного документа;

– направляет надлежащим образом заверенную копию нового документа посредством почтовой или курьерской связи;

– направляет через нотариуса электронный образ копии измененного документа, верность которого засвидетельствована этим нотариусом.

6.4.2. Предоставление Удостоверяющим центром справки о действительности Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром

1. Предоставление Удостоверяющим центром справки о действительности Сертификата ключа проверки электронной подписи, осуществляется в форме документа на бумажном носителе на основании заявления Владельца сертификата, которое оформляется в соответствии с Приложением № 5 к настоящему Регламенту и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

2. Заявление должно содержать следующую информацию:

а) время и дату подачи заявления;

б) время и дату (либо период времени), на момент наступления которых требуется установить статус Сертификата ключа проверки электронной подписи;

в) идентификационные данные Владельца сертификата, действительность Сертификата ключа проверки электронной подписи которого требуется установить;

г) серийный номер Сертификата ключа проверки электронной подписи, статус которого требуется установить.

3. Подготовленная Удостоверяющим центром по заявлению Владельца сертификата справка, содержащая информацию о действительности Сертификата ключа проверки электронной подписи, предоставляется Владельцу сертификата не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующего заявления.

6.4.3. Проверка подлинности электронной подписи (проверка электронной подписи) в электронном документе

1. По обращению Владельца сертификата либо иного лица Удостоверяющий центр осуществляет проверку подлинности электронной подписи в электронном документе.

2. В том случае, если формат электронного документа с электронной подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то Удостоверяющий центр обеспечивает проверку электронной подписи в электронном документе без заключения отдельного договора (соглашения) между Удостоверяющим центром и Владельцем сертификата либо иным обратившимся лицом. Решение о соответствии электронного документа с электронной подписью стандарту CMS принимает Удостоверяющий центр.

3. Для проверки подлинности электронной подписи в электронном документе Владелец сертификата подает в Удостоверяющий центр заявление в форме документа на бумажном носителе по форме, приведенной в Приложении № 6 к настоящему Регламенту.

4. Заявление должно содержать следующую информацию:

а) время и дату подачи заявления;

б) идентификационные данные Владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;

в) время и дату формирования электронной подписи в электронном документе;

г) время и дату, на момент наступления которых требуется проверить электронную подпись (в том случае если информация о времени подписания электронного документа отсутствует).

Обязательным приложением к заявлению на проверку электронной подписи в электронном документе является носитель информации, содержащий:

а) Сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить электронную подпись в электронном документе – в виде файла стандарта CMS;

б) Электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение электронной подписи этих данных, либо двух файлов: один из которых содержит данные, а другой значение электронной подписи этих данных (файл стандарта CMS).

5. Проверку электронной подписи в электронном документе осуществляет комиссия, сформированная из числа работников Удостоверяющего центра.

6. Результатом проверки электронной подписи в электронном документе является заключение комиссии Удостоверяющего центра, содержащее следующую информацию:

а) состав комиссии, осуществлявшей проверку;

б) основание для проведения проверки;

в) данные, представленные комиссии для проведения проверки;

г) отчет о выполненной проверке.

Отчет о выполненной проверке содержит:

а) время и место проведения проверки;

б) содержание и результаты проверки;

в) обоснование результатов проверки.

7. Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

8. Срок проведения работ по проверке электронной подписи в одном электронном документе и предоставлению заявителю заключения по выполненной проверке составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат электронного документа с электронной подписью не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), проведение экспертных работ по проверке электронной подписи осуществляется при условии заключения отдельного договора (соглашения) между Удостоверяющим центром и Владельцем сертификата либо иным лицом. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов, сроки проведения работ и иные существенные условия выполнения работ определяются указанным договором (соглашением).

7. Форма и сроки действия Сертификата ключа проверки электронной подписи и Ключа электронной подписи

7.4. Форма Сертификата ключа проверки электронной подписи

1. Форма Сертификата ключа проверки электронной подписи устанавливается удостоверяющим центром

2. Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть занесено:

- в поле Subject (идентифицирует Владельца сертификата):
  Поле E (Email) – адрес электронной почты;
  Поле T (Title) – должность полномочного представителя юридического лица (если Владелец сертификата – юридическое лицо, нотариус, или лицо, исполняющее обязанности нотариуса);
- расширение Private Key Validity Period – срок действия Ключа электронной подписи, соответствующего Сертификату ключа проверки электронной подписи:
  Действителен с (notBefore): дд.мм.гггг чч:мм:сс UTC;
  Действителен по(notAfter): дд.мм.гггг чч:мм:сс UTC;
- расширение Extended Key Usage (Улучшенный ключ, Расширенное использование ключа) – набор объектных идентификаторов, устанавливающих ограничения на применение квалифицированной электронной подписи совместно с Сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение CertificatePolicies (Политики сертификата) - набор объектных идентификаторов, устанавливающих ограничения на применение электронной подписи совместно с Сертификатом ключа проверки электронной подписи (если такие ограничения установлены);
- расширение CRL Distribution Point (Точка распространения Списка отозванных сертификатов) - набор адресов точек распространения Списков отозванных сертификатов;
- расширение Authority Information Access (Доступ к информации о центре) – Адрес обращения к Службе актуальных статусов сертификатов, Адрес размещения Сертификата ключа проверки электронной подписи Удостоверяющего центра;
- иные поля и расширения по усмотрению Удостоверяющего центра.

Информация о размещении списка отозванных сертификатов заносится в созданные Удостоверяющим центром Сертификаты ключей проверки электронной подписи в расширение CRL Distribution Point Сертификата ключа проверки электронной подписи.

3. Содержание полей Subject сертификатов ключей проверки электронной подписи для пользователей ЕИС:

- Поле T (Должность);
- Поле CN (Общее имя) – Фамилия Имя Отчество;
- Поле SN (Фамилия) – Фамилия;
- Поле G (Имя Отчество) – Имя Отчество;
- Поле L (Наименование населённого пункта) – Город (населенный пункт);
- Поле S (Наименование субъекта РФ) – код региона наименование региона;
- Поле C (Страна) – RU;
- Поле E (адрес электронной почты);
- Поле INN (ИНН) – личный ИНН заявителя;
- Поле SNILS (СНИЛС) - личный СНИЛС заявителя.
- Поле ОГРН (ОГРН)
- Поле ОГРНИП

4. Форма списка отозванных сертификатов (COC, CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель COC	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания COC	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен COC	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на прекращение действия сертификата (Time) 3. Код причины прекращения действия сертификаты сертификата (Reson Code) "0" Не указана "1" Нарушение конфиденциальности ключа "2" Нарушение конфиденциальности ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя COC	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор Ключа электронной подписи Удостоверяющего центра
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия Сертификата ключа проверки электронной подписи Удостоверяющего центра

7.5. Сроки действия Ключа электронной подписи и Сертификата ключа проверки электронной подписи

1. Сроки действия Ключа электронной подписи и Сертификата ключа проверки электронной подписи Удостоверяющего центра.

Срок действия Ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра и для Средства электронной подписи, с использованием которого данный Ключ электронной подписи был создан. Начало периода действия Ключа электронной подписи Удостоверяющего центра исчисляется с даты и времени его создания.

Срок действия Сертификата ключа проверки электронной подписи Удостоверяющего центра не превышает 15 (пятнадцать) лет. Время начала периода действия Сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в соответствующие поля Сертификата ключа проверки электронной подписи Удостоверяющего центра.

2. Сроки действия Ключа электронной подписи и Сертификата ключа проверки электронной подписи Владельца сертификата.

Срок действия Ключа электронной подписи Владельца сертификата составляет максимально допустимый срок действия Ключа электронной подписи, установленный для используемого Владельцем сертификата Средства электронной подписи. Начало периода действия Ключа электронной подписи Владельца сертификата исчисляется с даты и времени начала действия соответствующего Сертификата ключа проверки электронной подписи.

Срок действия Сертификата ключа проверки электронной подписи Владельца сертификата составляет 1 (один) год. В случае необходимости, данный срок может быть увеличен, но не более чем до 15 (пятнадцати) лет.

8. Меры по обеспечению информационной безопасности

8.1. Плановая смена ключей Удостоверяющего центра

Плановая смена Ключа электронной подписи и соответствующего ему Сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется в период действия Ключа электронной подписи Удостоверяющего центра.

Информирование Владельцев сертификатов о проведении смены ключей Удостоверяющего центра осуществляется посредством направления на адрес электронной почты Владельца сертификата или посредством размещения информации на сайте в сети Интернет по адресу www.fciit.ru: соответствующего уведомления о создании Удостоверяющим центром нового Ключа электронной подписи, соответствующего ему Ключа проверки электронной подписи, а также нового Сертификата ключа проверки электронной подписи Удостоверяющего центра.

Старый ключ электронной подписи Удостоверяющего центра используется Удостоверяющим центром в течение своего срока действия для формирования Списков отозванных сертификатов, создаваемых Удостоверяющим центром в период действия старого Ключа электронной подписи Удостоверяющего центра.

8.2. Внеплановая смена ключей Удостоверяющего центра

В случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра Сертификат ключа проверки электронной подписи Удостоверяющего центра прекращает действие. Удостоверяющий центр информирует о прекращении действия Сертификата ключа проверки электронной подписи Удостоверяющего центра путем рассылки соответствующего уведомления по адресам электронной почты Владельцев сертификатов или публикации информации о нарушении конфиденциальности Ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра в сети Интернет по адресу: www.fciit.ru. Все Сертификаты ключей проверки электронных подписей, подписанные с использованием Ключа электронной подписи Удостоверяющего центра, конфиденциальность которого нарушена, считаются прекратившими действие.

После информирования о прекращении действия Сертификата ключа проверки электронной подписи Удостоверяющего центра, Удостоверяющий центр создает новый Ключ электронной подписи, соответствующий ему Ключ проверки электронной подписи, а также новый Сертификат ключа проверки электронной подписи Удостоверяющего центра.

Информирование Владельцев сертификатов о проведении смены ключей Удостоверяющего центра осуществляется посредством направления на адрес электронной почты Владельца сертификата или посредством размещения информации на сайте в сети Интернет по адресу: www.fciit.ru соответствующего уведомления о создании Удостоверяющим центром нового Ключа электронной подписи, соответствующего ему Ключа проверки электронной подписи, а также нового Сертификата ключа проверки электронной подписи Удостоверяющего центра. Все действовавшие на момент нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра Сертификаты ключей проверки электронной подписи, а также Сертификаты ключей проверки электронной подписи, действие которых было приостановлено, подлежат внеплановой смене.

8.3. Обеспечение конфиденциальности информации

1. Ключ электронной подписи, соответствующий Сертификату ключа проверки электронной подписи является конфиденциальной информацией Владельца сертификата. Удостоверяющий центр не осуществляет хранение Ключей электронных подписей Владельцев сертификатов.
2. Удостоверяющий центр обеспечивает в соответствии с законодательством Российской Федерации, в том числе в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О

персональных данных», конфиденциальность информации, предоставляемой в Удостоверяющий центр в соответствии с настоящим Регламентом и не включенной в Сертификат ключа проверки электронной подписи.

3. Удостоверяющий центр не обеспечивает в соответствии с законодательством Российской Федерации, в том числе в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ «О персональных данных», конфиденциальность информации, включенной в состав Сертификата ключа проверки электронной подписи и Списка отозванных сертификатов, создаваемых Удостоверяющим центром.

4. Удостоверяющий центр имеет право раскрывать третьим лицам информацию, указанную в пункте 2 настоящего раздела Регламента только в случаях, установленных федеральным законом.

8.4. Хранение Сертификатов ключей проверки электронных подписей в Удостоверяющем центре

Хранение Сертификата ключа проверки электронной подписи в Удостоверяющем центре осуществляется в течение всего периода действия сертификата и 5 (Пяти) лет после его прекращения действия. По истечении указанного срока хранения Сертификаты ключей проверки электронной подписи переводятся в режим архивного хранения.

9. Список приложений

9.1 Приложение №1. Форма заявления для физического лица при личном обращении в Удостоверяющий центр

9.2 Приложение №1а. Форма заявления для индивидуального предпринимателя при личном обращении в Удостоверяющий центр

9.3 Приложение №1б.Форма заявления для представителя юридического лица при личном обращении в Удостоверяющий центр

9.4 Приложение №1в. Форма заявления для нотариуса и лица временно исполняющего обязанности нотариуса при личном обращении в Удостоверяющий центр

9.5 Приложение №2. Форма заявления на создание Сертификата ключа проверки электронной подписи Заявителя на основании запроса

9.7 Приложение №3а. Форма доверенности для физических лиц на получение ключей электронной подписи и Сертификата ключа проверки электронной подписи за Заявителя

9.8. Приложение №3б. Форма доверенности для юридических лиц на получение ключей электронной подписи и Сертификата ключа проверки электронной подписи за Заявителя

9.9. Приложение №4. Форма заявления на прекращение/приостановление/аннулирование/возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата

9.14. Приложение №5. Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром

9.15. Приложение №6. Форма заявления на проверку подлинности электронной подписи в электронном документе

9.19. Приложение №7. Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств электронной подписи

Приложение №1
к Регламенту Удостоверяющего центра
(Форма заявления для физического лица при личном обращении в Удостоверяющий центр)

Начальнику Удостоверяющего центра нотариата России

от_____
(И.О. Фамилия)

З А Я В Л Е Н И Е

Прошу изготовить мне (Заявителю), _____

_____

_____,
(фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, адрес места регистрации)

Ключ электронной подписи, а также создать Сертификат ключа проверки электронной подписи со следующими сведениями:

1. commonName Фамилия Имя Отчество Заявителя через пробел (не более 64 символов) –

2. surname Фамилия Заявителя (не более 128 символов) –

3. givenName Имя Отчество Заявителя (не более 128 символов) –

4. eMail Адрес электронной почты (не более 128 символов) –

5. localityName Наименование населенного пункта Заявителя (не более 128 символов) –

6. stateOrProvinceName Код региона с указанием названия региона через пробел (не более 128 символов) –

7. streetAddress Название улицы, номер дома, корпуса, строения, квартиры (30 символов) –

8. ИНН Заявителя (12 символов) –

9. СНИЛС Заявителя (11 символов) –

10. Страна/регион –

R	U

11. Сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение (в виде OID) –

Наименование объектного идентификатора	Цифровое обозначение

_____
(Фамилия Имя Отчество Заявителя полностью, собственноручно, подпись Заявителя)

«____» _____ 20___г.

Приложение №1а
к Регламенту Удостоверяющего центра
(Форма заявления для индивидуального предпринимателя при личном обращении в Удостоверяющий центр)

Начальнику Удостоверяющего центра нотариата России

от_____
(И.О. Фамилия)

З А Я В Л Е Н И Е

Прошу изготовить мне (Заявителю), _____

_____

_____,
(фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, адрес места регистрации)

Ключ электронной подписи, а также создать Сертификат ключа проверки электронной подписи со следующими сведениями:

1. commonName Фамилия Имя Отчество Заявителя через пробел (не более 64 символов) –

2. surname Фамилия Заявителя (не более 128 символов) –

3. givenName Имя Отчество Заявителя (не более 128 символов) –

4. eMail Адрес электронной почты (не более 128 символов) –

5. localityName Наименование населенного пункта Заявителя (не более 128 символов) –

6. stateOrProvinceName Код региона с указанием названия региона через пробел (не более 128 символов) –

7. streetAddress Название улицы, номер дома, корпуса, строения, квартиры (30 символов) –

8. ОГРНИП Заявителя (15 символов) –

9. ИНН Заявителя (12 символов) –

10. СНИЛС Заявителя (11 символов) –

11. Страна/регион –

R	U

12. Сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение (в виде OID) –

Наименование объектного идентификатора	Цифровое обозначение

_____
(Фамилия Имя Отчество Заявителя полностью, собственноручно, подпись Заявителя)

«____» _____ 20___г.

Приложение №1б
к Регламенту Удостоверяющего центра
(Форма заявления для представителя юридического лица при личном обращении в Удостоверяющий центр)

Начальнику Удостоверяющего центра нотариата России

от_____

_____

(полное наименование Заказчика – организации, ФИО руководителя организации, основание полномочий)

З А Я В Л Е Н И Е

Прошу изготовить Заявителю, _____

_____

_____,

(фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, адрес места регистрации)

Ключ электронной подписи, а также создать Сертификат ключа проверки электронной подписи со следующими сведениями:

1. commonName Наименование организации через пробел (не более 64 символов) –

2. surname Фамилия Работника (не более 128 символов) –

3. givenName Имя Отчество Работника (не более 128 символов) –

4. eMail Адрес электронной почты (не более 128 символов) –

5. localityName Наименование населенного пункта (по адресу местонахождения организации) (не более 128 символов) –

6. stateOrProvinceName Код региона с указанием названия через пробел (по местонахождению организации) (не более 128 символов) –

7. streetAddress Улица, номер дома, корпуса, строения местонахождения (по учредительным документам) (30 символов) –

8. organizationName Наименование организации через пробел (не более 64 символов) –

9. organizationUnitName Подразделение через пробел (не более 64 символов) –

10. title Должность Заявителя (не более 64 символов) –

11. ОГРН организации (13 символов) –

12. ИНН организации (12 символов) –

0 **0**

13. СНИЛС работника организации (11 символов) –

14. countryName Страна/регион –

R U

15. Сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение (в виде OID) –

Наименование объектного идентификатора	Цифровое обозначение

_____

(Фамилия Имя Отчество Заявителя полностью, собственноручно, подпись Заявителя)

«____» _____ 20___г.

Подпись руководителя организации (для юридических лиц), либо удостоверительная надпись нотариуса:

_____/_____

М.П.

«____» _____ 20___г

Приложение №1в
к Регламенту Удостоверяющего центра
(Форма заявления для нотариуса и лица временно исполняющего обязанности нотариуса при личном обращении в Удостоверяющий центр)

Начальнику Удостоверяющего центра нотариата России

от_____
(И.О. Фамилия)

З А Я В Л Е Н И Е

Прошу изготовить мне (Заявителю), _____

_____,
(фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, адрес места регистрации)

Ключ электронной подписи, а также создать Сертификат ключа проверки электронной подписи со следующими сведениями:

1. commonName Фамилия Имя Отчество Заявителя через пробел (не более 64 символов) –

2. surname Фамилия (не более 128 символов) –

3. givenName Имя Отчество (не более 128 символов) –

4. localityName Наименование населенного пункта, нотариального округа Заявителя (не более 128 символов) –

5. stateOrProvinceName Код региона с указанием названия региона через пробел (не более 128 символов) –

6. title Должность Заявителя (не более 64 символов) –

7. ИНН Заявителя (12 символов) –

8. СНИЛС Заявителя (11 символов) –

9. Страна/регион –

R	U

10. Поле «Адрес электронной почты Заявителя» - прошу заполнить в соответствии с требованиями «Федеральной службы государственной регистрации, кадастра и картографии»
11. Сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение (в виде OID) –

Наименование объектного идентификатора	Цифровое обозначение
Формирование документов для получения государственных услуг в сфере ведения государственного кадастра недвижимости со стороны заявителя	1.2.643.5.1.24.2.1.3
Проверка подлинности клиента	1.3.6.1.5.5.7.3.2
Защищенная электронная почта	1.3.6.1.5.5.7.3.4
Для ведения юридически значимого электронного документооборота	1.2.643.3.166.1.1
Пользователь ЕИС	1.2.643.3.166.2.1
Класс средства ЭП КС1	1.2.643.100.113.1
Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним	1.2.643.5.1.24.2.26
Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии	1.2.643.100.2.1

_____
(Фамилия Имя Отчество Заявителя полностью, собственноручно, подпись Заявителя)

«____» _____ 20___г.

приложение к заявлению _____ от «___»_____ 20___г.
(И.О. Фамилия)

Приложение №2
к Регламенту Удостоверяющего центра
(Форма заявления на создание Сертификата ключа проверки электронной подписи Заявителя на основании запроса)

В Удостоверяющий центр нотариата России (Фонд «Центр инноваций и информационных технологий»), юр. адрес: 127006, г. Москва, ул. Долгоруковская д. 15, стр. 4-5; тел.: (495) 730-57-05; адрес страницы в сети Интернет **www.fciit.ru**

Дата создания заявления: __.__.20___

З А Я В Л Е Н И Е

Я (Заявитель), ФИО: _____ _____ _____, паспорт серия номер: _____ _____, выдан: _____ дата выдачи: __.___.____, зарегистрированный по адресу: _____, прошу создать Сертификат ключа проверки электронной подписи в соответствии с указанными данными:

Сведения о запросе на сертификат:
Субъект:
T=тестировщик
CN=Наименование НП
SN=Фамилия
G=Имя Отчество
L=Москва
OU=подразделение НП
S=77 г. Москва
Street= ул. Радио, д.16
C=RU
E=test@test.ru
ИНН=000000000000
ОГРН=0000000000000
ОГРНИП=000000000000000
СНИЛС=00000000000
Алгоритм открытого ключа:
ObjectID алгоритма: 1.2.643.7.1.1.1.1 ГОСТ Р 34.10-2012 256 бит
Параметры алгоритма:
30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию
1.2.643.7.1.1.2.2 ГОСТ Р 34.11-2012 256 бит
Длина открытого ключа: 512 бит
Открытый ключ: UnusedBits = 0
05 50 3a 1f bd f4 86 e4 41 7d cf d3 ae 90 59 f9 f3 4b 8f 18 42 68 31 25 39 f5 22 64 6d 47 0f 32 0e 2a 0a 93 d5 2c 87 00 d4 35 b0 74 23 7d 02 7a 46 0b 1a 4c a1 c8 62 c4 df bc 8a 6a 2a dd 1d 14 7b 85
Запрос атрибутов: 3
Атрибуты 3:
Атрибут[0]: 1.3.6.1.4.1.311.13.2.3 (Версия ОС)
Значение[0][0]:
6.1.7600.2
Атрибут[1]: 1.3.6.1.4.1.311.2.1.14 (Расширения сертификатов)
Значение[1][0]:
Неизвестный тип атрибута
Расширения сертификатов: 3
2.5.29.15: Флаги = 1(Критический), Длина = 4
Использование ключа
Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
1.2.840.113549.1.9.15: Флаги = 0, Длина = c
Возможности SMIME
[1]Возможности SMIME
Идентификатор объекта=1.2.643.2.2.21
2.5.29.37: Флаги = 0, Длина = 46
Улучшенный ключ
Формирование документов для получения государственных услуг в сфере ведения государственного кадастра недвижимости со стороны заявителя (1.2.643.5.1.24.2.1.3)
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Для ведения юридически значимого электронного документооборота (1.2.643.3.166.1.1)
Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним (1.2.643.5.1.24.2.26)
Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии (1.2.643.100.2.1)
Пользователь ЕИС (1.2.643.3.166.2.1)
Класс средства ЭП КС1 (1.2.643.100.113.1)
Класс средства ЭП КС2 (1.2.643.100.113.2)
1.2.643.100.111: Флаги = 0, Длина = 2b
Средство электронной подписи владельца
Средство электронной подписи: КриптоПро CSP (версия 4.0)

1.3.6.1.4.1.311.20.2: Флаги = 0, Длина = e
Имя шаблона сертификата (Тип сертификата)
User.2
Атрибут[2]: 1.3.6.1.4.1.311.13.2.2 (CSP подачи заявок)
Значение[2][0]:
Неизвестный тип атрибута
Сведения о поставщике криптографии
KeySpec = 1
Поставщик = Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
Подпись: НеиспользБит=0
1e 7a 8f 4a 7e 50 10 9b 4f 1b 55 94 75 e2 0a 45 3d c5 75 e0 d7 a1 e3 4e f0 a2 97 fa 5d 40 08 73 8f 40 c5 2f 59 16 18 76 9c 93 26 09 cc 5c 26 79 a3 0c 3f ad 2c de 88 89 bd 7f 73 94 4d e5 0f 2c f0 a8 21 83 d1 f8 d1 81 7d 5a ab 25 55 8c 9f 14 74 60 43 00 04 b8 d0 6c d3 be 06 91 48 ad 3e 35 b5 ba 7d 68 7c 55 71 80 06 f2 af c3 a0 61 57 fe 68 d7 af e5 f6 27 9e 35 26 dd 88 98 ee 25 7e 46 00 00 34 00 21 00 56 00
Алгоритм подписи:
ObjectID алгоритма: 1.2.643.7.1.1.3.2 ГОСТ Р 34.11-2012/34.10-2012 256 бит
Параметры алгоритма: NULL
Подпись: НеиспользБит=0
de 15 12 43 9c 65 76 37 41 e4 9f 1d cd e5 b1 be dc 20 9a 77 74 61 be e8 43 17 fb 06 d4 6e 11 2d b9 e1 b1 d7 9d c3 fc b4 ad 17 bd 84 01 a6 aa bd e2 b0 5a 64 42 46 e2 ae aa c4 2c 60 ac bf 85 d7
Подпись соответствует открытому ключу
Хеш ИД ключа (rfc-sha1): 71 8c 95 76 d1 0e 60 f2 f4 cf 7a 26 c6 a7 f8 53 19 59 54 b0
Хеш ИД ключа (sha1): 23 a3 e3 65 53 63 0d 50 ea 2b ee cc f0 48 92 0f 2c 71 36 d3

_____

(Фамилия Имя Отчество Заявителя полностью, собственноручно)

Подпись владельца Ключа электронной подписи (Заявителя): _____

Подпись руководителя организации (для юридических лиц), либо удостоверительная надпись нотариуса:

_____/_____

М.П.

«____» _____ 20___г.

Приложение №3а
к Регламенту Удостоверяющего центра
(Форма доверенности для физических лиц на получение ключей электронной подписи и Сертификата ключа проверки электронной подписи за Заявителя)

Доверенность

г. _____ «_____» _____20___ г.

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта

_____
кем и когда выдан)

уполномочиваю _____
(фамилия, имя, отчество)

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

1. передать в Удостоверяющий центр нотариата России комплект документов для создания моих Ключа электронной подписи и Сертификата ключа проверки электронной подписи;
2. получить средства электронной подписи за Заявителя;
3. расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

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

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

Заявитель _____ _____
(фамилия, имя, отчество Заявителя) (подпись Заявителя)

«____» _____ 20____ г.

Приложение №3б
к Регламенту Удостоверяющего центра
(Форма доверенности для юридических лиц на получение ключей электронной подписи и Сертификата ключа проверки электронной подписи за Заявителя)

Доверенность

г. ________ «_____» _____20___ г.

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

в лице _____
(должность)

_____
(фамилия, имя, отчество)

действующего на основании _____
(фамилия, имя, отчество)

уполномочивает _____
(фамилия, имя, отчество)

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

1. передать в Удостоверяющий центр нотариата России комплект документов для создания Ключа электронной подписи и Сертификата ключа проверки электронной подписи Заявителя;
2. получить средства электронной подписи за Заявителя;
3. расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

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

Подпись уполномоченного представителя _____ _____
(Фамилия И.О.) (Подпись)

подтверждаю.

Заявитель _____ _____
(фамилия, имя, отчество Заявителя) (подпись Заявителя)

«____» _____ 20____ г.

Должность и Ф.И.О. руководителя организации
Подпись руководителя организации, дата подписания заявления
Печать организации

Приложение №4
к Регламенту Удостоверяющего центра
(Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи Владельца сертификата)

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

З А Я В Л Е Н И Е

на прекращение/приостановление/аннулирование/возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата

Я,_____
(Фамилия Имя Отчество Владельца сертификата)

_____
(паспортные данные Владельца сертификата)

настоящим прошу прекратить/приостановить/аннулировать/возобновить действие моего Сертификата ключа проверки электронной подписи, содержащего следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	

в связи с _____.

Владелец сертификта _____/_____
(И.О. Фамилия Владельца сертификата) (Подпись Владельца сертификата)

«____» _____ 20____ г.

Приложение №5
к Регламенту Удостоверяющего центра
(Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи созданного Удостоверяющим центром)

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

З А Я В Л Е Н И Е

на получение информации о статусе Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром нотариата России

Я,_____
(Фамилия Имя Отчество)

_____
(паспортные данные)

настоящим прошу предоставить информацию о статусе Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром и содержащего следующие данные:

SerialNumber (SN)	Серийный номер сертификата ключа проверки электронной подписи
CommonName (CN)	Наименование организации, если владелец сертификата – юридическое лицо; Фамилия, Имя, Отчество, если владелец сертификата – физическое лицо

Время[1] (период времени) на момент наступления которого требуется установить статус сертификата: с «_____» по «_____».

Заявитель _____/_____
(И.О. Фамилия) (Подпись)

«____» _____ 20____ г.

[1] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по московскому времени). Если время и дата не указаны, то статус Сертификата ключа проверки электронной подписи устанавливается на момент времени принятия заявления Удостоверяющим центром

Приложение №6
к Регламенту Удостоверяющего центра
(Форма заявления на проверку подлинности электронной подписи в электронном документе)

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

З А Я В Л Е Н И Е
на проверку подлинности электронной подписи в электронном документе

Я,_____
(Фамилия Имя Отчество)

_____
(паспортные данные)

настоящим прошу проверить подлинность электронной подписи в электронном документе на основании следующих данных:

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–ХХХ;

2. Файл, содержащий подписанные электронной подписью данные и значение электронной подписи формата CMS, либо файл, содержащий исходные данные и файл, содержащий значение электронной подписи формата CMS, на прилагаемом к заявлению носителе – рег. № Н–ХХХ

3. Время[1] подписания электронной подписью электронного документа:

«_____:_____» «_____/_____/_____»;
Час минута день месяц год

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

«_____:_____» «_____/_____/_____»;
Час минута день месяц год

Заявитель _____/_____
(И.О. Фамилия) (Подпись)

«____» _____ 20____ г.

[1] Время и дата должны быть указаны с учетом часового пояса г. Москвы (по московскому времени).

Приложение №7
к Регламенту Удостоверяющего центра
(Руководство по обеспечению безопасности использования неквалифицированной электронной подписи и средств неквалифицированной электронной подписи)

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

1. Условия и порядок использования электронных подписей и средств электронной подписи

1.1. Средства усиленной неквалифицированной электронной подписи должны применяться Владельцем неквалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство усиленной неквалифицированной электронной подписи.

1.2. На компьютерах с установленными средствами усиленной неквалифицированной электронной подписи должно использоваться только лицензионное программное обеспечение фирм-производителей.

1.3. Для предотвращения заражения компьютера с установленными средствами усиленной неквалифицированной электронной подписи необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак, спама, шпионского программного обеспечения и других вредоносных программ антивирусным программным обеспечением с рекомендуемым разработчиком периодом обновления антивирусных баз.

1.4. Владельцем неквалифицированного сертификата должны предприниматься меры организационного характера, направленные на обеспечение безопасности информации и эксплуатации средств усиленной неквалифицированной электронной подписи (в том числе, в организации Владельца неквалифицированного сертификата могут быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств усиленной неквалифицированной электронной подписи, назначены лица, ответственные за обеспечение безопасности).

1.5. Помещения, в которых установлены Средства усиленной неквалифицированной электронной подписи или хранятся носители Ключей электронной подписи, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

1.6. В помещениях, где установлены и применяются Средства усиленной неквалифицированной электронной подписи для хранения носителей Ключей электронной подписи, эксплуатационной и технической документации, дистрибутивов программного обеспечения средств усиленной неквалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, в целях предотвращения несанкционированного доступа к средствам усиленной неквалифицированной электронной подписи.

1.7. Используемые или хранимые Средства усиленной неквалифицированной электронной подписи, эксплуатационная и техническая документация к ним, носители Ключей электронной подписи подлежат поэкземплярному учету в соответствии с требованиями Приказа ФАПСИ от 13 июня 2001 г. № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну".

2. Риски, связанные с использованием электронных подписей

2.1 Утрата конфиденциальности Ключа проверки электронной подписи (в том числе нарушение правил хранения Ключа проверки электронной подписи, несоблюдение требований Регламента в случаях приостановления, прекращения либо аннулирования действия Сертификата ключа подписи) или нарушение правил эксплуатации Средств неквалифицированной электронной

подписи может привести к нарушению прав и законных интересов Владельца сертификата и/или третьих лиц.

2.2 Использование для хранения Ключа проверки электронной подписи защищенного носителя информации, несовместимого со Средством электронной подписи, применяемым Владельцем сертификата, может привести к невозможности подписания документа электронной подписью.

2.3 Использование для хранения Ключа проверки электронной подписи защищенного носителя информации, несовместимого со Средствами удостоверяющего центра, может привести к невозможности использования электронной подписи.

2.4 Применение Ключа электронной подписи без учета ограничений, содержащихся в Сертификате ключа проверки электронной подписи, если такие ограничения были установлены, может привести к тому, что будет принят документ, подписанный электронной подписью неуполномоченного лица.

2.5 Использование для создания и проверки неквалифицированных электронных подписей, создания Ключа электронной подписи и Ключа проверки электронной подписи несертифицированных в соответствии с правилами сертификации Российской Федерации Средств электронной подписи, и применение этих средств в нарушение правил, установленных нормативными правовыми актами Российской Федерации, может повлечь административную ответственность.

2.6 Несвоевременное предоставление данных, указанных в заявлении на создание Сертификата ключа проверки электронной подписи, а так же иных данных предоставленных в Удостоверяющий центр может привести к нарушению прав и законных интересов Владельца сертификата и/или третьих лиц.

3. Меры, необходимые для обеспечения безопасности электронных подписей и их проверки

Владелец сертификата должен принять следующие меры:

1. обеспечить конфиденциальность Ключа электронной подписи, принадлежащего Владельцу сертификата;
2. не применять Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
3. для хранения Ключа электронной подписи применять защищенный носитель информации, совместимый одновременно со Средством электронной подписи, применяемым Владельцем сертификата, и Средствами удостоверяющего центра;
4. применять для создания электронной подписи только действующий Ключ электронной подписи;
5. применять Ключ электронной подписи с учетом ограничений, содержащихся в Сертификате ключа проверки электронной подписи, если такие ограничения были установлены;
6. прекратить использование Ключа электронной подписи и немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия соответствующего ему Сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности Ключа электронной подписи;
7. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия;
8. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, с момента подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия;

9. не использовать Ключ электронной подписи, связанный с Сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено;

10. не использовать Ключ электронной подписи до приобретения статуса Владельца сертификата в соответствии с порядком, предусмотренным Регламентом;

11. использовать для создания и проверки неквалифицированных электронных подписей, создания Ключа электронной подписи и Ключа проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации Средства электронной подписи, и применять эти средства в соответствии с правилами. установленными нормативными правовыми актами Российской Федерации;

12. использовать при проверке электронной подписи в электронных документах актуальную информацию о Сертификатах ключей проверки электронных подписей, которые на данный момент времени аннулированы, действие которых прекращено и действие которых приостановлено, содержащуюся в Списке отозванных сертификатов, размещенном в сети Интернет по адресу: www.fciit.ru;

13. незамедлительно уведомить Удостоверяющий центр об изменении данных, указанных в заявлении на создание Сертификата ключа проверки электронной подписи, а так же иных данных предоставленных в Удостоверяющий центр.