

ОФЕРТА о присоединении к Договору об оказании услуг Удостоверяющего центра нотариата России

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ, в соответствии со статьей 435 Гражданского кодекса Российской Федерации (ГК РФ), является официальным предложением (офертой) Фонда «Центр инноваций и информационных технологий», именуемого в дальнейшем Удостоверяющий центр, и содержит все существенные условия Договора об оказании услуг Удостоверяющего центра нотариата России (далее – Договор).

1.2. Предложение адресовано нотариусам/исполняющим обязанности нотариуса/работникам нотариальной палаты субъекта Российской Федерации, имеет силу исключительно на территории Российской Федерации.

1.3. Неотъемлемой частью Договора является Регламент Удостоверяющего центра нотариата России (далее – Регламент УЦ), утвержденный Приказом Директора Фонда «Центр инноваций и информационных технологий» № 01-01.1/4 от 19 августа 2014 г., размещенный в сети Интернет по адресу www.fciit.ru.

1.4. Термины и определения, применяемые в настоящей оферте, используются в значениях, установленных Регламентом УЦ.

1.5. Заключение Договора производится путем совершения письменного акцепта условий, определенных настоящей офертой, и положений Регламента УЦ. Акцепт настоящего Договора производится путем направления нотариусом/исполняющим обязанности нотариуса/работником нотариальной палаты субъекта Российской Федерации в адрес Удостоверяющего центра заявления, указанного в п. 1.6. настоящей оферты.

1.6. Акцепт будет считаться полным, безоговорочным и совершенным с момента проставления нотариусом/исполняющим обязанности нотариуса/работником нотариальной палаты субъекта Российской Федерации в разделе «Запрос на создание сертификата» клиентского модуля «eNot» Единой информационной системы (ЕИС) отметки в виде «галочки» в графе «Я принимаю условия настоящей оферты» и последующим нажатием кнопки «далее».

1.7. В соответствии с пунктом 3 статьи 438 ГК РФ в случае принятия изложенных в настоящей оферте условий Договора нотариус/исполняющий обязанности нотариуса/работник нотариальной палаты субъекта Российской Федерации, акцептовавший настоящую оферту, и Удостоверяющий центр становятся в дальнейшем Сторонами настоящего Договора (далее также - Стороны).

1.8. Настоящая оферта размещена в сети Интернет по адресу: www.fciit.ru.

2. ПРЕДМЕТ ДОГОВОРА

2.1. Удостоверяющий центр на безвозмездной основе предоставляет нотариусу/исполняющему обязанности нотариуса/работнику нотариальной палаты субъекта Российской Федерации/иным категориям лиц по решению Правления Федеральной нотариальной палаты услуги, связанные с созданием ключей электронной подписи и сертификата ключа проверки электронной подписи и сопровождением использования сертификата ключа проверки электронной подписи.

2.2. Порядок и условия предоставления услуг, предусмотренных в п. 2.1. настоящего Договора, определяются Регламентом УЦ.

2.3. Права и обязанности Сторон настоящего Договора установлены Регламентом УЦ.

3. ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. В случае неисполнения либо ненадлежащего исполнения обязательств по настоящему Договору Стороны несут ответственность, установленную законодательством Российской Федерации.

3.2. Удостоверяющий центр не несет ответственности за последствия, возникшие в результате нарушения положений Регламента УЦ нотариусом/исполняющим обязанности нотариуса/работником нотариальной палаты субъекта Российской Федерации.

4. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

4.1. Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору, если надлежащее исполнение оказалось невозможным вследствие непреодолимой силы, например, вследствие массовых беспорядков, стихийных бедствий, пожаров, катастроф, военных действий, революций, забастовок, транспортных или производственных аварий, аварийных отключений электроэнергетики, аварийных нарушений и сбоев в электроснабжении, глобальных перебоев в работе российских и международных сегментов сети Интернет, сбоев систем маршрутизации сети Интернет, сбоев в распределенной системе доменных имен, запретительных или ограничительных действий органов власти.

4.2. Документ, выданный соответствующим компетентным органом торгово-промышленной палаты, либо информация, официально объявленная в средствах массовой информации, являются достаточным подтверждением наличия и продолжительности действия непреодолимой силы.

4.3. Сторона, подвергшаяся действию обстоятельств непреодолимой силы, обязана немедленно в письменном виде уведомить другую Сторону о возникновении, виде и возможной продолжительности действия соответствующих обстоятельств с приложением подтверждающих документов. Если эта Сторона не сообщит о наступлении обстоятельств непреодолимой силы, она лишается права ссылаться на них, разве что само такое обстоятельство препятствовало отправлению такого сообщения.

4.4. Если обстоятельства непреодолимой силы продолжают непрерывно действовать более 30 (тридцати) календарных дней, то каждая Сторона имеет право расторгнуть настоящий Договор с предварительным уведомлением другой Стороны в одностороннем порядке.

5. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ И РАЗНОГЛАСИЙ

5.1. При рассмотрении спорных вопросов, связанных с настоящим Договором, Стороны будут руководствоваться законодательством Российской Федерации.

5.2. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, путем переговоров.

5.3. В случае невозможности разрешения споров путем переговоров споры разрешаются в судебном порядке по месту нахождения Удостоверяющего центра.

6. ИЗМЕНЕНИЕ (ДОПОЛНЕНИЕ) ДОГОВОРА И РЕГЛАМЕНТА

6.1. Внесение изменений в настоящий Договор и Регламент УЦ производится Удостоверяющим центром в одностороннем порядке в части, не касающейся изменений прав и обязанностей Сторон, если только изменения прав и обязанностей Сторон не обусловлены изменением законодательства Российской Федерации.

6.2. Уведомление о внесении изменений в Договор осуществляется Удостоверяющим центром путем обязательного размещения информации о внесении изменений в Договор с указанием перечня измененных пунктов Договора в разделе «Новости» ЕИС на сайте в сети Интернет по адресу: www.fcii.ru, а также размещения текста Договора с внесенными изменениями в разделе «Запрос на создание сертификата» клиентского модуля «eNot» ЕИС.

6.3. Уведомление о внесении изменений в Регламент УЦ осуществляется Удостоверяющим центром путем обязательного размещения информации о внесении изменений в Регламент УЦ с указанием перечня измененных пунктов Регламента УЦ и/или Приложений к Регламенту УЦ в разделе «Новости» ЕИС, а также размещения текста Регламента с внесенными изменениями на сайте Удостоверяющего центра в сети Интернет по адресу: www.fcii.ru.

6.4. Все изменения, вносимые Удостоверяющим центром в Договор или Регламент УЦ по собственной инициативе и не связанные с изменением законодательства Российской Федерации, вступают в силу и становятся обязательными по истечении 30 (тридцати) дней со дня размещения на сайте Удостоверяющего центра по вышеуказанным адресам текста настоящего Договора или Регламента УЦ с учетом внесенных изменений.

6.5. Все изменения, вносимые Удостоверяющим центром в Договор или Регламент УЦ в связи с изменением законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений в соответствующих законодательных актах.

6.6. Все приложения, изменения и дополнения к настоящему Договору и Регламенту УЦ являются его составной и неотъемлемой частью.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Настоящий Договор заключается на срок действия сертификата ключа проверки электронной подписи.

7.2. Любая из Сторон вправе в одностороннем порядке расторгнуть настоящий Договор в случае неисполнения или ненадлежащего исполнения другой Стороной обязанностей, предусмотренных настоящим Договором.

7.3. В случае расторжения договорных отношений инициативная Сторона направляет другой Стороне уведомление о своих намерениях в порядке, предусмотренном Регламентом УЦ. Договорные отношения считаются расторгнутым после выполнения Сторонами своих обязательств согласно условиям Договора.

7.4. Прекращение действия Договора не освобождает Стороны от исполнения обязательств, возникших до указанной даты прекращения действия Договора, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

8. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

8.1. Для исполнения настоящего Договора нотариус/исполняющий обязанности нотариуса/работник нотариальной палаты субъекта Российской Федерации (далее - субъект персональных данных) представляет свои персональные данные, состав которых определен в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

8.2. Удостоверяющий центр осуществляет обработку персональных данных в качестве оператора персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

8.3. Персональные данные, содержащиеся в Заявлении на создание Удостоверяющим центром Сертификата ключа проверки электронной подписи, используются Удостоверяющим центром для сопровождения использования Сертификата ключа проверки электронной подписи субъекта персональных данных, а также при взаимодействии единой информационной системы нотариата России с государственными и муниципальными информационными системами, в том числе с Федеральной службой государственной регистрации, кадастра и картографии (Росреестр).

8.4. Обработка персональных данных Удостоверяющим центром включает передачу их третьим лицам в соответствии с законодательством Российской Федерации и настоящим Договором.

8.5. Удостоверяющий центр обеспечивает в соответствии с законодательством Российской Федерации, в том числе в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», конфиденциальность персональных данных, предоставляемых в Удостоверяющий центр в соответствии с настоящим Договором и не включенных в Сертификат ключа проверки электронной подписи.

8.6. Удостоверяющий центр не обеспечивает в соответствии с законодательством Российской Федерации, в том числе в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», конфиденциальность персональных данных, включенных в состав Сертификата ключа проверки электронной подписи и Списка отозванных сертификатов, создаваемых Удостоверяющим центром.

8.7. Подписание субъектом персональных данных Заявления на создание Удостоверяющим центром Сертификата ключа проверки электронной подписи рассматривается как согласие на обработку персональных данных, которое действительно в течение действия настоящего Договора.

8.8. Согласие на обработку персональных данных не может быть отозвано без одновременного расторжения договорных отношений в порядке, предусмотренном настоящим Договором.

8.9. После прекращения Договора документы, содержащие персональные данные, будут находиться на архивном хранении в соответствии с законодательством Российской Федерации.

9. АДРЕСА И РЕКВИЗИТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Удостоверяющий центр: Полное наименование: Фонд «Центр инноваций и информационных технологий», зарегистрирован на территории Российской Федерации в городе Москве (Свидетельство о регистрации № 7714012525 выдано Главным управлением Министерства юстиции Российской Федерации по Москве, Свидетельство о внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1107799007425 от 27 февраля 2010 года).

Сокращенное наименование: Фонд «Центр инноваций»

Юридический адрес: 127006, г. Москва, ул. Долгоруковская д. 15, стр. 4-5

Адрес местонахождения Удостоверяющего центра: 119071, г. Москва, ул. Малая Калужская, д. 15, стр. 1, г. Москва, ул. Долгоруковская д. 15, стр. 4-5

Почтовый адрес: 127006, г. Москва, ул. Долгоруковская д. 15, стр. 4-5

Банковские реквизиты (наименование банка, р/с, к/с, БИК):

- Московский банк Сбербанка России ОАО г. Москва

- БИК 044525225

- Р/с 40703810338090000364

- К/с 30101810400000000225

ИНН/КПП: 7708237747 /770701001

ОГРН: 1107799007425

Код по ОКВЭД: 65.2

Код по ОКПО: 65313922

Контактный телефон, адрес электронной почты:

тел.: 8 (495) 730 57 05; e-mail: ca@fciit.ru

Адрес в сети Интернет: www.fciit.ru

Директор Фонда «Центр инноваций и информационных технологий»

В.В. Голобоков

РЕГЛАМЕНТ ДЕЯТЕЛЬНОСТИ

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

Редакция № 3

г. Москва
2014 г.

СОДЕРЖАНИЕ

1. Сведения об Удостоверяющем центре	7
2. Термины и определения	7
3. Общие положения	9
4. Деятельность Удостоверяющего центра:	10
4.1. Виды деятельности Удостоверяющего центра	10
4.2. Условия деятельности Удостоверяющего центра	10
5. Права и обязанности	11
5.1. Права и обязанности Удостоверяющего центра	11
5.2. Права и обязанности Заявителя и Владельца сертификата	13
6. Порядок создания и выдачи Сертификатов ключей проверки электронной подписи и управления ими	15
6.1. Формирование Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи в Удостоверяющем центре в присутствии Заявителя	15
6.2. Формирование Ключа электронной подписи и создание Сертификата ключа проверки электронной подписи в Удостоверяющем центре без присутствия Заявителя	17
6.3. Порядок управления Сертификатами ключа проверки электронной подписи	19
6.4. Порядок предоставления информации и дополнительных сервисов Удостоверяющего центра	23
7. Форма и сроки действия Сертификата ключа проверки электронной подписи и Ключа электронной подписи	25
7.1. Форма Сертификата ключа проверки электронной подписи	25
7.2. Сроки действия Ключа электронной подписи и Сертификата ключа проверки электронной подписи	27
8. Меры по обеспечению информационной безопасности	28
8.1. Плановая смена ключей Удостоверяющего центра	28
8.2. Внеплановая смена ключей Удостоверяющего центра	28
8.3. Обеспечение конфиденциальности информации	28
8.4. Хранение Сертификатов ключей проверки электронных подписей в Удостоверяющем центре	29
9. Список приложений	30

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. N 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 квалифицированными сертификатами ключей проверки электронных подписей на территории Российской Федерации на основании Свидетельства об аккредитации удостоверяющего центра № 46 от 06 августа 2012 г., выданного Минкомсвязи России (федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи), и на основании лицензии ЛЗС № 0010225 от 15 апреля 2014 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;

г. Москва, ул. Малая Калужская, д.15 стр.1, офис 7

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

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

3) *Ключ квалифицированной электронной подписи Удостоверяющего центра* – Ключ электронной подписи, используемый Удостоверяющим центром для создания квалифицированных 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 сертификата ключа проверки электронной подписи (далее – Владелец сертификата)* – лицо, которому Удостоверяющим центром в соответствии с законодательством Российской Федерации и настоящим Регламентом выдан квалифицированный Сертификат ключа проверки электронной подписи;

6) *Квалифицированный 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) *Сертификат ключа проверки электронной подписи Удостоверяющего центра* – квалифицированный 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) *Копия сертификата ключа проверки электронной подписи* - документ на бумажном носителе, подписанный собственноручной подписью уполномоченного на это действие работника Удостоверяющего центра и заверенный печатью Удостоверяющего центра. Форма копии Сертификата ключа проверки электронной подписи определяется настоящим Регламентом;

9) *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;

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

11) *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;

12) *Заявитель* - физическое или юридическое лицо, обратившееся в Удостоверяющий центр за получением квалифицированного Сертификата ключа проверки электронной подписи;

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

14) *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 таких прекращения или аннулирования;

15) *Служба актуальных статусов сертификатов* – сервис Удостоверяющего центра (построенный на базе протокола OCSP), с использованием которого предоставляется информация о действительности Сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром в виде электронного документа, подписанного квалифицированной электронной подписью службы актуальных статусов сертификатов;

16) *Служба штампов времени* – сервис Удостоверяющего центра (построенный на базе протокола TSP), с использованием которого предоставляется штамп времени в виде электронного документа подписанного квалифицированной электронной подписью службы штампов времени;

17) *Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра* – квалифицированный Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в электронных ответах Службы актуальных статусов сертификатов, содержащих информацию о статусе Сертификатов ключей проверки электронных подписей;

18) *Сертификат ключа проверки электронной подписи Службы штампов времени Удостоверяющего центра* – квалифицированный Сертификат ключа проверки электронной подписи, использующийся для проверки подлинности электронной подписи в штампах времени, сформированных Службой штампов времени Удостоверяющего центра;

19) *Сканирование документа на бумажном носителе* - создание электронного образа бумажного документа с помощью специальных средств, обеспечивающих преобразование изображения на бумажном носителе в электронную форму;

20) *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;

21) *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;

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

23) *Online Certificate Status Protocol (далее - OCSP)* – протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 «X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP»;

24) *Time-Stamp Protocol (далее - TSP)* – протокол получения штампа времени, реализующий RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)».

3. Общие положения

3.1. Регламент деятельности Удостоверяющего центра нотариата России, именуемый в дальнейшем «Регламент», разработан в соответствии с законодательством Российской Федерации.

3.2. Настоящий Регламент является документом, устанавливающим правила и порядок создания, выдачи и управления Сертификатами ключей проверки электронных подписей, а также предоставления Удостоверяющим центром информации и дополнительных сервисов.

3.3. Удостоверяющий центр обеспечивает средствами электронной подписи и создает Ключи электронных подписей нотариусов, лиц, замещающих временно отсутствующих нотариусов (далее - временно исполняющих обязанности нотариусов), а также иных категорий лиц по решению Правления Федеральной нотариальной палаты.

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

3.5. Любое заинтересованное лицо может ознакомиться с Регламентом на сайте в сети Интернет по адресу: www.fciit.ru.

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

1) Уведомление о внесении изменений в Регламент осуществляется Удостоверяющим центром путем публикации новой редакции Регламента на сайте в сети Интернет по адресу: www.fciit.ru.

2) Изменения, вносимые Удостоверяющим центром в Регламент, кроме изменений, вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для субъектов, на которых распространяет свое действие настоящий Регламент, по истечению 30 (Тридцати) календарных дней со дня их публикации на сайте в сети Интернет по адресу: www.fciit.ru.

3) Изменения (дополнения), вносимые Удостоверяющим центром в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих законодательных актов.

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

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

3.9. Информирование субъектов Удостоверяющим центром производится посредством направления электронного письма на адрес, указанный при обращении в Удостоверяющий центр или посредством размещения информации на сайте в сети Интернет по адресу: www.fciit.ru.

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) ведение Реестра сертификатов;
- 7) обеспечение доступа лиц к информации, содержащейся в Реестре сертификатов (к Списку отозванных сертификатов), в том числе с использованием информационно-телекоммуникационной сети "Интернет";
- 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 как на возмездной, так и на безвозмездной основе.

Правом на безвозмездное получение услуг Удостоверяющего центра обладают нотариусы, лица, временно исполняющие обязанности нотариусов, а также иные категории лиц по решению Правления Федеральной нотариальной палаты.

5. Права и обязанности

5.1. Права и обязанности Удостоверяющего центра

5.1.1. Удостоверяющий центр имеет право:

- 1) запросить у Заявителя документы, указанные в п.6.1. и необходимые для выдачи Сертификата ключа проверки электронной подписи;
- 2) отказать Заявителю в создании Сертификата ключа проверки электронной подписи в случае ненадлежащего оформления им заявления на создание Сертификата ключа проверки электронной подписи и/или не предоставления им всех документов, необходимых для создания 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 с обязательным уведомлением Владельца сертификата и указанием обоснованных причин;
- 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.
- 6) Наделять нотариальные палаты субъектов Российской Федерации следующими полномочиями:
 - а) Устанавливать личность Заявителя, обращающегося в Удостоверяющий центр за получением Сертификата ключа проверки электронной подписи на основании паспорта или других документов, исключающих любые сомнения относительно личности гражданина, выступающего в качестве заявителя;
 - б) Свидетельствовать подлинность подписи Заявителя на предоставленном заявлении на создание сертификата ключа проверки электронной подписи;
 - в) Осуществлять предварительную проверку сведений, передаваемых в Удостоверяющий центр, включая проверку полноты комплекта документов, предусмотренных настоящим Регламентом, проверку соответствия сведений, указанных в заявлении и запросе на создание Сертификата ключа проверки электронной подписи – предоставленным документом, но не ограничиваясь перечисленным;
 - г) Присоединять к запросам на создание Сертификатов ключей проверки электронных подписей, сформированным заявителями в единой информационной системе, электронные образы предоставленных документов, подписанные усиленной квалифицированной подписью работника Нотариальной палаты субъекта Российской Федерации, уполномоченного Нотариальной палатой субъекта Российской Федерации на совершение таких действий.

5.1.2. Удостоверяющий центр обязан:

- 1) предоставить Заявителю, Владельцу сертификата по его требованию:
 - а) копию лицензии ЛЗС № 0010225 от 15 апреля 2014 г. выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России
 - б) копию свидетельства об аккредитации удостоверяющего центра № 46 от 06 августа 2012 г., выданного Минкомсвязи 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 конфиденциальность Ключа электронной подписи, созданного Удостоверяющим центром до передачи его Заявителю;
- 11) обеспечить приём заявлений на прекращение, приостановление или возобновление действия Сертификатов ключей проверки электронной подписи;
- 12) прекратить, приостановить или возобновить действие Сертификата ключа проверки электронной подписи по соответствующему заявлению на прекращение, приостановление или возобновление действия Сертификата ключа проверки электронной подписи, в соответствии с порядком, определенным в настоящем Регламенте;
- 13) прекратить действие Сертификата ключа проверки электронной подписи Владельца сертификата, если истек установленный срок, на который действие данного сертификата было приостановлено;
- 14) прекратить действие Сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра, с использованием которого был создан данный сертификат;
- 15) аннулировать действие Сертификата ключа проверки электронной подписи по решению суда, вступившему в законную силу;
- 16) официально уведомить об аннулировании, прекращении, приостановлении или возобновлении действия Сертификата ключа проверки электронной подписи посредством включения соответствующей информации в Список отозванных сертификатов;
- 17) публиковать 1 раз в сутки актуальный Список отозванных сертификатов на сайте Удостоверяющего центра в сети Интернет по адресу: www.fciit.ru;
- 18) 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;
- 19) не использовать Ключ электронной подписи Удостоверяющего центра при наличии оснований полагать, что конфиденциальность данного ключа нарушена;
- 20) 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 №12);

21) обеспечивать актуальность информации, содержащейся в Реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

22) 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;

23) осуществлять обработку персональных данных в качестве оператора персональных данных в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

24) размещать на сайте Удостоверяющего центра в сети Интернет по адресу: www.fcit.ru утвержденную новую редакцию Регламента, включающую внесенные в него изменения, за тридцать календарных дней до вступления их в силу. Соблюдать требования настоящего Регламента.

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) получить Копию сертификата ключа проверки электронной подписи;

5) обратиться в Удостоверяющий центр с заявлением на создание Сертификата ключа проверки электронной подписи;

6) 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;

7) 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;

8) обратиться в Удостоверяющий центр за получением справки о действительности Сертификатов ключей проверки электронной подписи на определенный момент времени;

9) обратиться в Удостоверяющий центр за проверкой электронной подписи, сформированной с использованием Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром;

10) при обращении за выдачей Сертификата ключа проверки электронной подписи получить информацию о рисках, связанных с использованием электронной подписи;

11) обратиться в Удостоверяющий центр для получения информации, касающейся обработки его персональных данных (Приложение №13);

12) требовать от Удостоверяющего центра уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для

заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.2.2. Заявитель, Владелец сертификата обязаны:

1) с целью ознакомления с полным текстом изменений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра в сети Интернет по адресу: www.fciit.ru за сведениями об изменениях Регламента;

2) предоставить документы, необходимые для создания Сертификата ключа проверки электронной подписи;

3) обеспечить конфиденциальность принадлежащего ему Ключа электронной подписи;

4) не применять Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

5) для хранения Ключа электронной подписи применять защищенный носитель информации, совместимый одновременно со Средством электронной подписи, применяемым Владелец сертификата, и Средствами удостоверяющего центра;

6) применять для создания электронной подписи только действующий Ключ электронной подписи;

7) применять Ключ электронной подписи с учетом ограничений, содержащихся в Сертификате ключа проверки электронной подписи, если такие ограничения были установлены;

8) 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;

9) 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;

10) 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;

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

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

13) 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;

14) 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;

15) 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;

16) 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 указываться 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 заявительных 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 заявительных 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, а также Копия сертификата ключа проверки электронной подписи по форме Приложения №10 к настоящему Регламенту, которую он подписывает собственноручно.

6. При получении первого Сертификата ключа проверки электронной подписи Заявителю (либо его полномочному представителю) сообщается ключевая фраза, используемая 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. Формирование Ключа электронной подписи и файла запроса на создание Сертификата ключа проверки электронной подписи осуществляется Заявителем в разделе ЕИС «Запрос на создание сертификата».

3. 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.

4. 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.

5. 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.

6. 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).

7. 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).

8. 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.

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

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

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

12. 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. Сертификат ключа проверки электронной подписи и файл копии сертификата ключа проверки электронной подписи, созданный Удостоверяющим центром по форме Приложения № 10 к настоящему Регламенту, подписанный электронной подписью работника Удостоверяющего центра, направляются Заявителю с использованием СПО.

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 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 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 Удостоверяющим 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 № 5 к настоящему Регламенту.

7. Подача Владельцем сертификата заявления на приостановление действия Сертификата ключа проверки электронной подписи в форме электронного документа осуществляется путем направления в Удостоверяющий центр электронного документа по форме Приложения № 5 к настоящему Регламенту подписанного электронной подписью Владельца сертификата.

8. Приостановление действия Сертификата ключа проверки электронной подписи по заявлению Владельца сертификата в устной форме осуществляется исключительно при нарушении конфиденциальности Ключа электронной подписи или подозрении в нарушении конфиденциальности Ключа электронной подписи Владельца сертификата. Владелец сертификата самостоятельно определяет факт нарушения конфиденциальности своего Ключа электронной подписи или угрозу такого нарушения.

Владелец сертификата сообщает в Удостоверяющий центр по телефону следующую информацию:

- идентификационные данные, содержащиеся в Сертификате ключа проверки электронной подписи, действие которого необходимо приостановить;
- серийный номер Сертификата ключа проверки электронной подписи, действие которого требуется приостановить;
- срок, на который приостанавливается действие Сертификата ключа проверки электронной подписи;
- ключевую фразу Владельца сертификата.

Решение о приостановлении действия Сертификата ключа проверки электронной подписи по заявлению Владельца сертификата в устной форме принимается работником Удостоверяющего центра круглосуточно, но только в случае соответствия информации представленной Владельцем сертификата и информации хранящейся в Удостоверяющем центре.

9. После получения Удостоверяющим центром заявления на приостановление действия Сертификата ключа проверки электронной подписи работник Удостоверяющего центра осуществляет его рассмотрение не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было получено Удостоверяющим центром. В случае принятия работником Удостоверяющего центра решения о приостановлении действия Сертификата ключа проверки электронной подписи соответствующая информация вносится в Реестр сертификатов.

10. 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;
- при получении заявления о приостановлении действия Сертификата ключа проверки электронной подписи в связи со смертью Владельца сертификата.

11. Заявление о приостановлении Сертификата ключа проверки электронной подписи в связи со смертью Владельца сертификата подается по форме Приложения № 5а настоящего Регламента в отношении нотариуса, лица, временно исполняющего обязанности нотариуса, или работника нотариальной палаты - нотариальной палатой субъекта Российской Федерации, в связи со смертью Владельца сертификата, являющегося работником юридического лица, - работодателем.

12. После приостановления действия Сертификата ключа проверки электронной подписи работник Удостоверяющего центра уведомляет Владельца сертификата о факте и причинах, повлекших приостановление действия Сертификата ключа проверки электронной подписи. Информация о приостановлении действия Сертификата ключа проверки электронной подписи вносится в Реестр сертификатов.

Если в течение срока приостановления действия Сертификата ключа проверки электронной подписи Владелец сертификата не направит в Удостоверяющий центр заявление на возобновление действия Сертификата ключа проверки электронной подписи, то Удостоверяющий центр автоматически прекращает действие данного сертификата.

Создание нового Ключа электронной подписи и нового Сертификата ключа проверки электронной подписи осуществляются в порядке, предусмотренном разделами 6.1. или 6.2. настоящего Регламента.

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 № 6 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.

6.3.3. Прекращение действия Сертификата ключа проверки электронной подписи

1. 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 отзыве доверенности, выданной лицу, указанному в Сертификате ключа проверки электронной подписи;
- д) в случае документального подтверждения факта истечения или прекращения срока действия полномочий Владельца сертификата;
- е) по истечении срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено;
- ж) при нарушении конфиденциальности Ключа электронной подписи Удостоверяющего центра;
- з) при получении от юридического лица заявления о прекращении действия Сертификата ключа проверки электронной подписи Владельца сертификата с приложением копии документа, подтверждающего факт смерти Владельца сертификата.

2. В случае прекращения действия Сертификата ключа проверки электронной подписи по истечении срока его действия, датой и временем прекращения действия Сертификата ключа проверки электронной подписи признаются дата и время, указанные в соответствующем поле Сертификата ключа проверки электронной подписи. Информация о Сертификате ключа проверки электронной подписи, действие которого прекращено по указанному обстоятельству, не вносится Удостоверяющим центром в Список отозванных сертификатов.

3. Прекращение действия Сертификата ключа проверки электронной подписи может осуществляться по заявлению его владельца, подаваемого в форме документа на бумажном носителе или в форме электронного документа.

Подача Владельцем сертификата заявления на прекращение действия Сертификата ключа проверки электронной подписи осуществляется в форме документа на бумажном носителе по форме Приложения № 4 к настоящему Регламенту посредством почтовой или курьерской связи.

Подача Владельцем сертификата заявления на прекращение действия Сертификата ключа проверки электронной подписи в форме электронного документа осуществляется путем

направления в Удостоверяющий центр электронного документа по форме Приложения № 4 к настоящему Регламенту, подписанного электронной подписью Владельца сертификата.

После получения Удостоверяющим центром заявления на прекращение действия Сертификата ключа проверки электронной подписи работник Удостоверяющего центра осуществляет его рассмотрение не позднее рабочего дня, следующего за рабочим днем, в течение которого указанное заявление было получено Удостоверяющим центром. В случае принятия работником Удостоверяющего центра решения о прекращении действия Сертификата ключа проверки электронной подписи соответствующая информация вносится в Реестр сертификатов.

4. Прекращение действия Сертификата ключа проверки электронной подписи в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам осуществляется не менее чем за один месяц до дня прекращения деятельности Удостоверяющего центра, при условии уведомления об этом в письменной форме Владельцев сертификатов, срок действия Сертификатов ключей проверки электронной подписи, которых не истек.

5. В случае поступления в Удостоверяющий центр документов, подтверждающих факт отзыва доверенности либо факт, истечения или прекращения срока действия полномочий Владельца сертификата, Удостоверяющий центр уведомляет Владельца сертификата о прекращении действия Сертификата ключа проверки электронной подписи не позднее одного рабочего дня с момента наступления описанного события. Информация о прекращении действия Сертификата ключа проверки электронной подписи вносится в Реестр сертификатов.

6. В случае, когда действие Сертификата ключа проверки электронной подписи приостановлено и в течение срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено, Владельцем сертификата не было направлено в Удостоверяющий центр заявление на возобновление Сертификата ключа проверки электронной подписи, информация о прекращении действия Сертификата ключа проверки электронной подписи вносится в Реестр сертификатов.

7. Прекращение действия Сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра осуществляется посредством уведомления об этом Владельцев сертификатов в письменной форме. Временем прекращения действия Сертификата ключа проверки электронной подписи признается время получения указанного уведомления Владельцем сертификата. В этом случае информация о прекращении действия Сертификата ключа проверки электронной подписи в Реестр сертификатов не заносится.

8. Прекращение действия Сертификата ключа проверки электронной подписи осуществляется на основании заявления по форме Приложения № 5а настоящего Регламента от юридического лица (нотариальной палаты субъекта Российской Федерации либо юридического лица-работодателя Владельца сертификата) о прекращении действия сертификата с приложениями копии документа, подтверждающего факт смерти Владельца сертификата. При получении Удостоверяющим центром указанного заявления, работник Удостоверяющего центра осуществляет его рассмотрение не позднее рабочего дня, следующего за рабочим днем, в течение которого указанный документ был получен Удостоверяющим центром. В случае принятия работником Удостоверяющего центра решения о прекращении действия Сертификата ключа проверки электронной подписи, информация о прекращении действия Сертификата ключа проверки электронной подписи вносится в Реестр сертификатов.

6.3.4. Аннулирование Сертификата ключа проверки электронной подписи

1. Основанием для аннулирования Сертификата ключа проверки электронной подписи является решение суда, вступившее в законную силу. Удостоверяющий центр в течение не более чем одного рабочего дня аннулирует Сертификат ключа проверки электронной подписи путем внесения записи о его аннулировании в Реестр сертификатов.

2. До внесения в Реестр сертификатов информации об аннулировании Сертификата ключа проверки электронной подписи Удостоверяющий центр уведомляет Владельца сертификата об аннулировании его Сертификата ключа проверки электронной подписи путем направления электронного документа на адрес электронной почты Владельца сертификата.

6.4. Порядок предоставления информации и дополнительных сервисов 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 № 7 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 № 8 к настоящему Регламенту.

4. Заявление должно содержать следующую информацию:

- а) время и дату и 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 десять рабочих дней с момента поступления заявления в Удостоверяющий центр.

9. 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 Владелец 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).

6.4.4. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени

1. Удостоверяющий центр предоставляет актуальную информацию о статусе Сертификата ключа проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов.

2. Служба актуальных статусов сертификатов по запросам любых лиц формирует и предоставляет им OCSP-ответы, которые содержат информацию о статусе запрашиваемого Сертификата ключа проверки электронной подписи.

3. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием Сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается

действительным при соблюдении условий признания квалифицированной электронной подписи, а также при условии, что Сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра включает ограничение - в расширении Extended Key Usage содержится объектный идентификатор 1.3.6.1.5.5.7.3.9 (Подпись службы OCSP). Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – <http://ocsp2.fcii.ru/ocsp2-qual/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых Удостоверяющим центром Сертификатов ключей проверки электронной подписи.

4. Удостоверяющий центр выдает штампы времени посредством сервиса Службы штампов времени. Штмп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при соблюдении условий признания квалифицированной электронной подписи, а также при условии, что Сертификат ключа проверки электронной подписи Службы штампов времени включает ограничение - в расширении Extended Key Usage содержится объектный идентификатор 1.3.6.1.5.5.7.3.8 (Установка штампа времени). Адрес обращения к Службе штампов времени Удостоверяющего центра – <http://tsp2.fcii.ru/tsp2-qual/tsp.srf>.

6.4.5. Блокировка защищенного носителя информации содержащего Ключ электронной подписи Владельца сертификата

1. В случае блокировки защищенного носителя информации содержащего Ключ электронной подписи Владельца сертификата по причине многократного ввода неверного пароля Владелец сертификата самостоятельно осуществляет его форматирование (инициализацию) или обращается в Удостоверяющий центр с заявлением, по форме Приложения № 9 настоящего Регламента.

Форматирование защищенного носителя информации приводит к уничтожению всех Ключей электронной подписи, содержащихся на этом носителе.

2. Создание нового ключа электронной подписи и нового сертификата ключа проверки электронной подписи осуществляются в соответствии с разделами 6.1. или 6.2. настоящего Регламента.

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

7.1. Форма Сертификата ключа проверки электронной подписи

1. Форма Сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, соответствует требованиям Приказа ФСБ РФ от 27 декабря 2011 года №795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи».

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 квалифицированной 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 нотариусов и лиц, исполняющих обязанности нотариуса:

Поле T (Должность) – нотариус, врио нотариуса Фамилия И. О. (ИНН нотариуса обязанности которого исполняет врио нотариуса);

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), нотариальный округ (в соответствии с печатью нотариуса);

Поле S (Наименование субъекта РФ) – код региона наименование региона;

Поле Street (Адрес) – 0;

Поле C (Страна) – RU;

Поле E (адрес электронной почты) – федеральный номер@fciit.ru.rosreestr.ru;

Поле INN (ИНН) – личный ИНН заявителя;

Поле SNILS (СНИЛС) - личный СНИЛС заявителя.

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

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Идентификационные данные Удостоверяющего центра
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	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 (Reason 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 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
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

7.2. 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 Службы актуальных статусов сертификатов и Сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов

Срок действия Ключа электронной подписи Службы актуальных статусов сертификатов составляет максимально допустимый срок действия, установленный для применяемого Средства электронной подписи, с использованием которого данный Ключ электронной подписи был сформирован. Начало периода действия Ключа электронной подписи Службы актуальных статусов сертификатов исчисляется с даты и времени создания Сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов.

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

3. Сроки действия Ключа электронной подписи Службы штампов времени и Сертификата ключа проверки электронной подписи Службы штампов времени

Срок действия Ключа электронной подписи Службы штампов времени составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный Ключ электронной подписи был создан. Начало периода действия Ключа электронной подписи Службы штампов времени исчисляется с даты и времени создания Сертификата ключа проверки электронной подписи Службы штампов времени.

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

4. 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. Время начала периода действия Сертификата ключа проверки электронной подписи Владельца сертификата и его окончания заносится в соответствующие поля Сертификата ключа проверки электронной подписи Владельца сертификата.

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 действия Сертификата ключа проверки электронной подписи Владельца сертификата**
- 9.10. Приложение №4а. Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи с приложением копии документа, подтверждающего факт смерти Владельца сертификата**
- 9.11. Приложение №5. Форма заявления на приостановление действия Сертификата ключа проверки электронной подписи Владельца сертификата**
- 9.12. Приложение №5а. Форма заявления на приостановление действия Сертификата ключа проверки электронной подписи в связи со смертью Владельца сертификата**
- 9.13. Приложение №6. Форма заявления на возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата**
- 9.14. Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи созданного Удостоверяющим центром**
- 9.15. Приложение №8. Форма заявления на проверку подлинности электронной подписи в электронном документе**
- 9.16. Приложение №9. Форма заявления на форматирование защищенного носителя информации**
- 9.17. Приложение №10. Форма Сертификата ключа проверки электронной подписи**
- 9.18. Приложение №11. Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре**
- 9.19. Приложение №12. Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи**
- 9.20. Приложение №13. Форма запроса субъекта персональных данных об обрабатываемых персональных данных**

З А Я В Л Е Н И Е

о присоединении к Договору об оказании услуг Удостоверяющего центра нотариата России

Я, _____

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

принимаю в полном объеме условия оферты о присоединении к Договору об оказании услуг Удостоверяющего центра нотариата России, являющегося неотъемлемой частью Регламента Удостоверяющего центра нотариата России, утвержденного Приказом Директора Фонда «Центр инноваций и информационных технологий» № 01-01.1/3 от 4 октября 2013 г., также являющегося в соответствии со статьей 428 Гражданского кодекса Российской Федерации договором присоединения; оферта размещена в сети Интернет по адресу: www.fciit.ru.

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

« ____ » _____ 20__ г.

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

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.fcit.ru

Дата создания заявления: __.__.20__

ЗАЯВЛЕНИЕ

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=тестирующий
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=000000000000
ОГРНИП=000000000000000
СНИЛС=000000000000

Алгоритм открытого ключа:

ObjectID алгоритма: 1.2.643.2.2.19 ГОСТ Р 34.10-2001

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
1.2.643.2.2.30.1 ГОСТ Р 34.11-94, параметры по умолчанию

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 34.10-2001 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: 1.2.643.2.2.3 ГОСТ Р 34.11/34.10-2001

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.

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.

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

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

З А Я В Л Е Н И Е
на прекращение действия Сертификата ключа проверки электронной подписи Владельца
сертификата

Я, _____
(Фамилия Имя Отчество Владельца сертификата)

(паспортные данные Владельца сертификата)

настоящим прошу прекратить действие моего Сертификата ключа проверки электронной подписи,
содержащего следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	
CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС

в связи с _____.

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

« ____ » _____ 20 ____ г.

Приложение №4а
к Регламенту Удостоверяющего центра

(Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи с приложением копии документа, подтверждающего факт смерти Владельца сертификата)

Начальнику Удостоверяющего центра
нотариата России

от _____
(наименование организации)

З А Я В Л Е Н И Е

на прекращение действия Сертификата ключа проверки электронной подписи с приложением
копии документа, подтверждающего факт смерти Владельца сертификата

Я, _____
(Фамилия Имя Отчество, должность уполномоченного лица)

настоящим прошу прекратить действие Сертификата ключа проверки электронной подписи,

(Фамилия Имя Отчество умершего)

содержащего следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	
CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС

в связи со смертью указанного лица.

Приложение на _____ л.

_____/_____
(И.О. Фамилия уполномоченного лица) (Подпись уполномоченного лица)

« ____ » _____ 20__ г.

М.П.

Приложение №5
к Регламенту Удостоверяющего центра

(Форма заявления на приостановление 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 приостановление действия Сертификата ключа проверки электронной подписи Владельца
сертификата

Я, _____
(Фамилия Имя Отчество Владельца сертификата)

(паспортные данные)

настоящим прошу приостановить действие моего Сертификата ключа проверки электронной
подписи, содержащего следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	
CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС

Срок приостановления действия сертификата ключа подписи _____ дней.

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

« ____ » _____ 20 ____ г.

Приложение №5а
к Регламенту Удостоверяющего центра
(Форма заявления на приостановление действия Сертификата ключа проверки
электронной подписи в связи со смертью Владельца сертификата)

Начальнику Удостоверяющего центра
нотариата России

от _____
(наименование организации)

З А Я В Л Е Н И Е
на приостановление действия Сертификата ключа проверки электронной подписи в связи со
смертью Владельца сертификата

Я, _____
(Фамилия Имя Отчество, должность уполномоченного лица)

настоящим прошу приостановить действие Сертификата ключа проверки электронной подписи,

(Фамилия Имя Отчество умершего)

содержащего следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	
CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС

в связи со смертью указанного лица.

_____/_____
(И.О. Фамилия уполномоченного лица) (Подпись уполномоченного лица)

« ____ » _____ 20__ г.

М.П.

Приложение №6
к Регламенту Удостоверяющего центра
(Форма заявления на возобновление 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 возобновление действия Сертификата ключа проверки электронной подписи Владельца
сертификата

Я, _____
(Фамилия Имя Отчество Владельца сертификата)

_____ (паспортные данные)

настоящим прошу возобновить действие моего сертификата ключа подписи, содержащего
следующие данные:

Серийный номер сертификата ключа подписи (SerialNumber)	
CommonName (CN)	Фамилия Имя Отчество
SNILS	СНИЛС

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

« ____ » _____ 20__ г.

Приложение №7
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

Время¹ (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

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

ЗАЯВЛЕНИЕ
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–XXX;
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–XXX
3. Время¹ 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).

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

З А Я В Л Е Н И Е
на форматирование защищенного носителя информации

Я, _____
(Фамилия Имя Отчество Владельца сертификата)

в связи с отсутствием информации, обеспечивающей доступ к имеющемуся у меня защищенному носителю информации, не возражаю против уничтожения всей информации находящейся на данном носителе. В связи с вышеизложенным, прошу произвести процедуру форматирования предоставленного мной защищенного носителя информации с идентификационным номером _____.

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

« ____ » _____ 20 ____ г.

Удостоверяющий центр нотариата России
Бланк сертификата ключа подписи

Сведения о сертификате:

Кому выдан:

Фамилия Имя Отчество

Кем выдан:

Notariat Russia

Действителен с 29 мая 2013 г. 11:12:00 UTC по 29 мая 2014 г. 11:22:00 UTC

Версия: 3 (0x2)

Серийный номер: 3294 C60A 0000 0000 7058

Издатель сертификата: CN = Notariat Russia, OU = Удостоверяющий центр, O = Фонд "Центр инноваций и информационных технологий", L = Москва, C = RU, S = 77 г. Москва, E = ca@fciit.ru, ИНН = 007708237747, ОГРН = 1107799007425

Срок действия:

Действителен с: 29 мая 2013 г. 11:12:00 UTC

Действителен по: 29 мая 2014 г. 11:22:00 UTC

Владелец сертификата: CN = Фамилия Имя Отчество

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.19

Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01

Значение: 0440 57F7 F082 0C60 C6D6 FCC8 57D1 6C3F 8A65 B3D2 1AED 37D1 40BE 35C5 65EA 4848 6FB6 09B4 73E2 8D84 D078 56AF 53F5 FD7F 73DA CE6F BDCB EF13 CA84 66EB 8132 6D59 29A0

Расширения сертификата X.509

1. Расширение 2.5.29.15 (критическое)

Название: Использование ключа

Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2. Расширение 2.5.29.37

Название: Улучшенный ключ

Значение: Пользователь Центра Регистрации, НТТР, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

3. Расширение 2.5.29.14

Название: Идентификатор ключа субъекта

Значение: Идентификатор ключа: 88 26 a8 c2 79 91 38 18 f5 f7 7f be 3c b5 04 26 df 45 bc 95

4. Расширение 2.5.29.35

Название: Идентификатор ключа центра сертификатов

Значение: Идентификатор ключа=c1 b4 e0 72 92 a2 c3 09 fe c8 b7 94 31 61 0a d1 80 2e 16 4f Поставщик сертификата: Адрес каталога: CN=Notariat Russia OU=Удостоверяющий центр O="Фонд ""Центр инноваций и информационных технологий"" L=Москва C=RU S=77 г. Москва E=ca@fciit.ru ИНН=007708237747 ОГРН=1107799007425 Серийный номер сертификата=50 e3 83 a4 b3 3f c8 ac 4e e7 f5 5b f8 d6 de ce

5. Расширение 2.5.29.31

Название: Точки распространения списков отзыва (CRL)

Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:

URL=http://cdp1.fciit.ru/cdp/C1B4E07292A2C309FEC8B79431610AD1802E164F.crl [2]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://cdp2.fciit.ru/cdp/C1B4E07292A2C309FEC8B79431610AD1802E164F.crl

6. Расширение 1.3.6.1.5.5.7.1.1

Название: Доступ к информации о центрах сертификации

Значение: [1]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния сертификата через сеть

(1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.fciit.ru/ocsp-qual/ocsp.srf [2]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://cdp1.fciit.ru/cdp/ca-qual.cer

7. Расширение 2.5.29.16

Название: Период использования закрытого ключа

Значение: Начало действия: 29 Май 2013 г. 15:12:00 Окончание действия: 29 Май 2014 г. 15:12:00

8. Расширение 2.5.29.32

Название: Политики сертификата

Значение: [1]Политика сертификата: Идентификатор политики=Для ведения юридически значимого электронного документооборота

[2]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1

9. Расширение 1.2.643.100.111

Название: Средство электронной подписи владельца

Значение: Средство электронной подписи: КриптоПро CSP (версия 3.6)

10. Расширение 1.2.643.100.112

Название: Средства электронной подписи и УЦ издателя

Значение: Средство электронной подписи: "КриптоПро CSP" (версия 3.6) Заключение на средство ЭП: Сертификат соответствия № СФ/121-1859 от 17.06.2012 Средство УЦ: "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 Заключение на средство УЦ: Сертификат соответствия № СФ/128-1822 от 01.06.2012

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ЭЦП ГОСТ Р 34.10-2001

Идентификатор: 1.2.643.2.2.3

Значение: F08A ADAE 7FB1 2ACA 1290 3D53 1A6B 9085 63D7 0D64 9391 EB36 59D0 1A78 FB9A C70B 3335 DFA7 176F 0F17 EBB6 A886 A937 9A2C 6705 B7F8 26BE 4889 CFAD 75DF 2447 F1C0

Подпись Владельца сертификата: _____/_____

"__" _____ 20__ г.

Подпись Уполномоченного лица УЦ: _____/_____

«__» _____ 20__ г.

М.П.

Приложение №11
к Регламенту Удостоверяющего центра

(Список объектных идентификаторов, зарегистрированных в Удостоверяющем центре)

Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре и определяющих отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение

№ п/п	OID	Область применения
1.	1.3.6.1.5.5.7.3.9	Подпись ответа службы OCSP – формирование электронной подписи ответов Службы актуальных статусов сертификатов
2.	1.3.6.1.5.5.7.3.8	Установка штампа времени – формирование электронной подписи штампов времени, предоставляемых Службой штампов времени
3.	1.2.643.3.166.1.1	Для ведения юридически значимого электронного документооборота
4.	1.2.643.5.1.24.2.26	Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним
5.	1.2.643.5.1.24.2.1.3	Формирование документов для получения государственных услуг в сфере ведения государственного кадастра недвижимости со стороны заявителя
6.	1.2.643.5.1.24.2.2.6	Обеспечение шифрования и аутентификации на транспортном уровне веб сервисов Удостоверяющих центров
7.	1.2.643.3.166.9.5	Обеспечение шифрования, аутентификации и подписи на транспортном уровне ЕИС
8.	1.2.643.100.2.1	Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии
9.	1.2.643.2.2.34.6	Пользователь Центра Регистрации, HTTP, TLS клиент
10.	1.3.6.1.5.5.7.3.2	Проверка подлинности клиента
11.	1.3.6.1.5.5.7.3.1	Проверка подлинности сервера
12.	1.3.6.1.5.5.7.3.4	Защищенная электронная почта
13.	1.2.643.100.2.2	Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии (ФНП)
14.	1.2.643.3.166.9.1	Оператор сервера
15.	1.2.643.3.166.9.2	Технологический оператор ЕИС
16.	1.2.643.3.166.9.5	Обеспечение шифрования, аутентификации и подписи на транспортном уровне ЕИС
17.	1.2.643.3.166.9.6	Подписание конфигурационных файлов ЕИС
18.	1.2.643.3.166.9.7	Тестирование ЕИС
19.	1.2.643.3.166.9.8	Централизованный электронный реестр ЕИС
20.	1.2.643.3.166.9.9	Реестре уведомлений о залоге движимого имущества ЕИС
21.	1.3.6.1.5.5.7.3.3	Подписывание кода
22.	1.2.643.3.166.9.4	Администратор ЕИС
23.	1.2.643.100.113.1	Класс средства ЭП КС1
24.	1.2.643.100.113.2	Класс средства ЭП КС2
25.	1.2.643.3.166.2.1	Пользователь ЕИС

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

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

1.1. Средства усиленной квалифицированной электронной подписи должны применяться Владелцем квалифицированного сертификата в соответствии с положениями эксплуатационной документации на применяемое средство усиленной квалифицированной электронной подписи.

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

1.3. Для предотвращения заражения компьютера с установленными средствами усиленной квалифицированной 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. Владелцем квалифицированного сертификата должны предприниматься меры организационного характера, направленные на обеспечение безопасности информации и эксплуатации средств усиленной квалифицированной электронной подписи (в том числе, в организации Владельца квалифицированного сертификата могут быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации средств усиленной квалифицированной электронной подписи, назначены лица, ответственные за обеспечение безопасности).

1.5. Помещения, в которых установлены Средства усиленной квалифицированной 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 квалифицированной электронной подписи для хранения носителей Ключей электронной подписи, эксплуатационной и технической документации, дистрибутивов программного обеспечения средств усиленной квалифицированной электронной подписи, необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, в целях предотвращения несанкционированного доступа к средствам усиленной квалифицированной электронной подписи.

1.7. Используемые или хранимые Средства усиленной квалифицированной 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 квалифицированной 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 квалифицированных 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 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;

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.fcii.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.

Начальнику Удостоверяющего центра
нотариата России

от _____
(И.О. Фамилия)

ЗАПРОС

субъекта персональных данных об обрабатываемых персональных данных

Я, _____
(Фамилия Имя Отчество)

(паспортные данные: номер и серия, кем и когда выдан)

(сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором)

в соответствии с частью 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» прошу Удостоверяющий центр нотариата России - Оператора моих персональных данных предоставить мне в течение 30 рабочих дней со дня получения данного запроса, информацию, касающуюся обработки моих персональных данных, в том числе содержащую:

- 1) подтверждение факта обработки персональных данных Оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

Ответ прошу направить по
адресу:

Заявитель _____ / _____
(И.О. Фамилия) (Подпись)
« ____ » _____ 20 ____ г.