ОФЕРТА
о присоединении к Договору об оказании услуг Удостоверяющего центра Фонда «Центр инноваций и информационных технологий»

1. ОБЩИЕ ПОЛОЖЕНИЯ

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

1.2. Предложение адресовано физическим лицам, имеет силу исключительно на территории Российской Федерации.

1.3. Неотъемлемой частью Договора является Порядок реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей Удостоверяющим центром (далее – Порядок), утвержденный Приказом Директора Фонда «Центр инноваций и информационных технологий» № 01-01.4/24 от 21.10.2024, размещенный в сети Интернет по адресу www.fciit.ru.

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

1.5. Заключение Договора производится путем совершения письменного акцепта условий, определенных настоящей офертой, и положений Порядка. Акцепт настоящей оферты производится путем направления заявителем в адрес Удостоверяющего центра заявления.

1.6. Акцепт будет считаться полным, безоговорочным и совершенным после ознакомления заявителя с настоящей офертой, Порядком в момент подачи заявления.

1.7. В соответствии с пунктом 3 статьи 438 ГК РФ в случае принятия изложенных в настоящей оферте условий Договора заявитель, 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 обязуется оказать Заявителю услуги, связанные с созданием квалифицированных ключей электронной подписи и квалифицированных сертификатов ключей проверки электронной подписи и сопровождение их использования, а Заявитель обязуется принять надлежаще оказанные УЦ услуги в соответствии с условиями Договора.

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

2.3. Права и обязанности Сторон настоящего Договора установлены Порядком, являющимся неотъемлемой частью настоящего Договора.

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 заявителем положений настоящего Договора и Порядка.

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, природных пожаров, катастроф, военных действий, революций, забастовок, транспортных или производственных аварий, аварийных отключений электроэнергии, 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 палатой), 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 (ДОПОЛНЕНИЯ) ДОГОВОРА И ПОРЯДКА

6.1. Внесение изменений в настоящий Договор и Порядок 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.fciit.ru, а также размещения текста Договора с внесенными изменениями в разделе «Запрос на создание сертификата» клиентского модуля ЕИС.

6.3. Уведомление о внесении изменений в Порядке осуществляется Удостоверяющим центром путем обязательного размещения информации о внесении изменений в Порядок с указанием перечня измененных пунктов Порядка и/или Приложений к Порядку на сайте в сети Интернет по адресу: www.fciit.ru.

6.4. Все изменения, вносимые Удостоверяющим центром в Договор и/или Порядок 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 по вышеуказанным адресам текста настоящего Договора или Порядка с учетом внесенных изменений.

6.5. Все изменения, вносимые Удостоверяющим центром в Договор и/или Порядок 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/или Порядку являются их составной и неотъемлемой частью.

7. СРОК ДЕЙСТВИЯ ДОГОВОРА

7.1. Договор заключается на срок действия квалифицированного 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 Порядком. 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 Договора заявитель (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» (далее – 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» (далее – Закон о персональных данных).

8.3. Персональные данные, содержащиеся в заявлении на создание Удостоверяющим центром квалифицированного сертификата ключа проверки электронной подписи, используются Удостоверяющим центром для сопровождения использования квалифицированного сертификата ключа проверки электронной подписи субъекта персональных данных.

8.4. Обработка персональных данных Удостоверяющим центром включает сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение; использование; обезличивание; блокирование, удаление, уничтожение персональных данных 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 Законом о персональных данных, конфиденциальность персональных данных, предоставляемых в Удостоверяющий центр в соответствии с настоящим Договором и не включенных в состав квалифицированного сертификата ключа проверки электронной подписи.

8.6. Удостоверяющий центр не обеспечивает в соответствии с законодательством Российской Федерации, в том числе в соответствии с Законом о персональных данных, конфиденциальность персональных данных, включенных в состав квалифицированного 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, передаются на архивное хранение в соответствии с требованиями законодательства 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: 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 ПАО Сбербанк
- БИК 044525225

- Р/с 40703810338090000364
- К/с 30101810400000000225
ИНН/КПП: 7708237747 /770701001
ОГРН: 1107799007425
Код по ОКВЭД: 62.01
Код по ОКПО: 65313922
Тел.: (495) 730-57-05
e-mail: ca@fciit.ru
Адрес сайта в сети Интернет: www.fciit.ru

Утвержден
Приказом Директора Фонда «Центр инноваций и информационных технологий»
№01-01.4/11 от «27» марта 2025 г.

Порядок реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

г. Москва
2025

Содержание

1. Термины и сокращения 4
2. Общие положения 6
2.1. Предмет регулирования 6
2.2. Сведения об Удостоверяющем центре 7
2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра 7
2.4. Стоимость услуг Удостоверяющего центра 7
3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром 8
4. Права и обязанности Удостоверяющего центра 9
4.1. Права Удостоверяющего центра 9
4.2. Обязанности Удостоверяющего центра 9
5. Права и обязанности Заявителя и Владельца Сертификата 11
5.1. Права Заявителя, Владельца сертификата 11
5.2. Обязанности Заявителя, Владельца сертификата 11
6. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром 13
6.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей 13
6.2. Порядок осуществления плановой смены ключей электронной подписи Удостоверяющего центра 13
6.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности 13
6.4. Форма и сроки действия ключа электронной подписи и Сертификата ключа проверки электронной подписи, форма списка отозванных сертификатов 14
6.4.1 Сроки действия ключа электронной подписи и Сертификата ключа проверки электронной подписи 14
6.4.2 Форма ключа электронной подписи и Сертификата ключа проверки электронной подписи 15
6.4.3 Форма списка отозванных сертификатов. 15
6.5. Обеспечение конфиденциальности информации 16
6.6. Порядок создания ключей электронной подписи и Сертификатов ключей проверки электронной подписи и управления ими 16
7. Процедура создания и выдачи квалифицированных сертификатов ключей проверки электронной подписи 18
7.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов 18
7.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов 18
7.3. Порядок установления личности заявителя 18
7.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи квалифицированного сертификата 18
7.5. Порядок проверки достоверности документов и сведений, представленных Заявителем 19
7.6. Порядок создания и выдачи квалифицированного сертификата в Удостоверяющем центре в присутствии Заявителя 19
7.7. Порядок создания и выдачи квалифицированного сертификата в Удостоверяющем центре без присутствия Заявителя 19
7.8. Подтверждение действительности электронной подписи, использованной для подписания электронных документов 20
7.9. Процедуры, осуществляемые при приостановлении действия, прекращении действия и аннулировании квалифицированного сертификата 21
7.9.1. Возобновление действия Сертификата ключа проверки электронной подписи 22
7.9.2 Прекращение действия Сертификата ключа проверки электронной подписи 22
7.9.3. Аннулирование Сертификата ключа проверки электронной подписи 24
7.10. Порядок ведения реестра квалифицированных сертификатов 24
7.11. Порядок технического обслуживания реестра квалифицированных сертификатов 24
8. Порядок исполнения обязанностей Удостоверяющего центра 25
8.1. Информирование 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 25
8.2. Требования к средствам электронной подписи используемым заявителем 25

8.3. Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий 25
8.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет» 26
8.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей 26
8.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации 27
8.7. Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации 27
8.8. Предоставление доступа к информации, содержащейся в реестре квалифицированных сертификатов 28
9. Порядок предоставления информации в Удостоверяющий центр 28
10. Дополнительные сервисы Удостоверяющего центра 28
10.1. Проверка подлинности электронной подписи (проверка электронной подписи) в электронном документе 28
10.2. Блокировка защищенного носителя информации, содержащего Ключ электронной подписи Владельца сертификата 29
11. Список приложений: 30
Форма заявления для физического лица при личном обращении в Удостоверяющий центр 31
Форма заявления на создание Сертификата ключа проверки электронной подписи Заявителя на основании запроса 33
Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи 35
Владельца сертификата 35
Форма заявления на приостановление действия Сертификата ключа проверки электронной подписи Владельца сертификата 36
Форма заявления на возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата 37
Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи созданного Удостоверяющим центром 38
Форма заявления на проверку подлинности электронной подписи в электронном документе 39
Форма заявления на форматирование защищенного носителя информации 40
Форма Сертификата ключа проверки электронной подписи 41
Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи 42
Форма запроса субъекта персональных данных об обрабатываемых персональных данных 45

1. Термины и сокращения

В настоящем Порядке реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей Удостоверяющим центром Фонда «Центр инноваций и информационных технологий» (далее – Порядок):

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, использующийся Удостоверяющим центром для создания квалифицированных сертификатов ключей проверки электронной подписи и Списков отозванных сертификатов;

4. *Конфиденциальность квалифицированного ключа электронной подписи* - обеспечение работником Удостоверяющего центра, создающего Ключ электронной подписи, Заявителя и Владельца сертификата защиты Ключа электронной подписи от несанкционированного доступа и использования;

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

6. *Квалифицированный сертификат ключа проверки электронной подписи* (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом;

7. *Квалифицированный 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 Порядком;

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* – 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 лицо, обратившееся в Удостоверяющий центр за получением квалифицированного Сертификата ключа проверки электронной подписи;

13. *Рабочий день Удостоверяющего центра (далее – рабочий день)* – ПН-ЧТ с 9:00 до 18:00, ПТ до 16:45 (по московскому времени) за исключением выходных и нерабочих праздничных дней в соответствии с утвержденным производственным календарем на соответствующий календарный год;

14. *Реестр квалифицированных 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. *Сканирование документа на бумажном носителе* - создание электронного образа бумажного документа с помощью специальных средств, обеспечивающих преобразование изображения на бумажном носителе в электронную форму;

16. *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;

17. *Единая система идентификации и аутентификации (далее ЕСИА)* - информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах;

18. *Удостоверяющий центр* - Удостоверяющий центр Фонда «Центр инноваций и информационных технологий»;

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

2. Общие положения

2.1. Предмет регулирования

2.1.1. Настоящий Порядок разработан в соответствии с законодательством Российской Федерации:

− Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ;

− Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ;

− Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ;

− Федеральным законом «О связи» от 07.07.2003 № 126-ФЗ;

− Федеральным законом «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ;

− Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79;

− Требованиями к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27.12.2011 № 796;

− Требованиями к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27.12.2011 № 795;

− Требованиями к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Минцифры России от 13.11.2020 № 584 (в редакции приказов Минцифры России от 14.07.2023 № 634, от 02.11.2023 № 948);

− Порядком передачи реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи и иной информации в федеральный орган исполнительной власти, уполномоченный в сфере использования электронной подписи, в случае прекращения деятельности аккредитованного удостоверяющего центра, утвержденным приказом Минцифры России от 02.11.2021 № 1134;

− Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минцифры России от 08.11.2021 № 1138;

− Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 (далее также – Инструкция ФАПСИ № 152);

− Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России 09.02.2005 № 66;

− иными нормативными правовыми актами, регулирующими отношения в области информационных технологий, защиты информации и использования электронных подписей, в том числе методическим и руководящим документов Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) и Федеральной службы безопасности Российской Федерации (далее – ФСБ России) в области защиты информации.

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

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

2.1.4. Любое заинтересованное лицо может ознакомиться с Порядком на официальном сайте Фонда «Центр инноваций и информационных технологий» в сети Интернет по адресу: www.fciit.ru.

2.1.5. Внесение изменений в Порядок, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке:

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

2) Изменения, вносимые Удостоверяющим центром в Порядок, кроме изменений, вызванных изменениями законодательства Российской Федерации, вступают в силу и становятся обязательными для субъектов, на которых распространяет свое действие настоящий Порядок, 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 Порядок в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу соответствующих законодательных актов.

2.1.6. Все приложения, изменения и дополнения к настоящему Порядку являются его составной и неотъемлемой частью.

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

2.1.8. 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.

2.2. Сведения об Удостоверяющем центре

2.2.1. Фонд «Центр инноваций и информационных технологий» зарегистрирован на территории Российской Федерации в городе Москва (Свидетельство о регистрации некоммерческой организации № 7714012525 выдано 24.09.2010 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 ФЗ «Об электронной подписи».

2.2.2. Удостоверяющий центр осуществляет деятельность по созданию, выдаче и управлению квалифицированными сертификатами ключей проверки электронных подписей на территории Российской Федерации на основании лицензии ЛЗС № 0015332 от 30 мая 2018 г. выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России.

2.2.3. Место нахождения и почтовый адрес:

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

3. Контактные данные Удостоверяющего центра:

Телефон: +7(495)730-57-05

e-mail: ca@fciit.ru

Адрес официального сайта в сети Интернет: www.fciit.ru

2.2.4. Рабочие часы Удостоверяющего центра: ПН-ЧТ с 9:00 до 18:00 (по МСК), ПТ с 09:00 до 16:45 (по МСК) за исключением выходных и нерабочих праздничных дней в соответствии с производственным календарем на соответствующий календарный год.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра

2.3.1.Информирование Удостоверяющим центром о предоставляемых услугах осуществляется:

- по месту оказания услуг Удостоверяющего центра: г. Москва, ул. Долгоруковская д. 15, стр. 4-5;
- по телефону: +7 (495) 730-57-05 (ПН-ЧТ с 9:00 до 18:00 (по МСК), ПТ с 09:00 до 16:45 (по МСК) за исключением выходных и праздничных дней);
- по адресу электронной почты: ca@fciit.ru, (приём обращений осуществляется ежедневно круглосуточно, обработка и ответ на обращение предоставляется в рамках режима работы Удостоверяющего центра);
- размещение информации на сайте в сети Интернет по адресу: www.fciit.ru

2.4. Стоимость услуг Удостоверяющего центра

2.4.1. Перечень оказываемых услуг, тарифы и порядок оплаты услуг утверждаются приказом Директора Фонда «Центр инноваций и информационных технологий».

2.4.2. Тарифы и порядок оплаты услуг размещаются в сети Интернет по адресу: www.fciit.ru

3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром

3.1. 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) приостановление действия выданных Удостоверяющим центром Сертификатов ключей проверки электронных подписей;

7) возобновление действия выданных Удостоверяющим центром Сертификатов ключей проверки электронных подписей;

8) ведение Реестра сертификатов;

9) обеспечение доступа лиц к информации, содержащейся в Реестре сертификатов (к Списку отозванных сертификатов), в том числе с использованием сети Интернет;

10) предоставление информации, содержащейся в Реестре сертификатов, в том числе информации об аннулировании Сертификата ключа проверки электронной подписи;

11) создание Ключей электронных подписей и Ключей проверки электронных подписей;

12) проверка уникальности Ключей проверки электронных подписей в Реестре сертификатов;

13) выдача по обращению Заявителя Средств электронной подписи;

14) осуществление иной деятельности, связанной с использованием электронной подписи.

4. Права и обязанности Удостоверяющего центра

4.1. Права Удостоверяющего центра

В рамках исполнения функций, предусмотренных ФЗ «Об электронной подписи», Удостоверяющий центр имеет право:

1) запросить у Заявителя документы, указанные в п.7.4. Порядка 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 Порядок в части, не касающейся прав и обязанностей Заявителей и Владельцев сертификатов, если только изменения их прав и обязанностей не обусловлены изменением законодательства Российской Федерации.

4.2. Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

1. предоставить Заявителю, Владельцу сертификата по его требованию:

- копию лицензии № 16654/Н от 30 мая 2018 г., выданной Центром по лицензированию, сертификации и защите государственной тайны ФСБ России;

2. предоставить Заявителю Сертификат ключа проверки электронной подписи Удостоверяющего центра в электронной форме;
3. использовать для создания Ключа электронной подписи Удостоверяющего центра и создания электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации Средства электронной подписи;
4. использовать Ключ электронной подписи Удостоверяющего центра только для подписания создаваемых им Сертификатов ключей проверки электронной подписи и Списков отозванных сертификатов;
5. принять меры по защите Ключа электронной подписи Удостоверяющего центра от несанкционированного доступа и использования;
6. организовать свою работу по Московскому времени, синхронизировать по времени все свои программные и технические средства обеспечения деятельности;
7. создать Сертификат ключа проверки электронной подписи по заявлению на создание Сертификата ключа проверки электронной подписи, в порядке, определенном настоящим Порядком;
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 Порядке;

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 2 раз в сутки (каждые 12 часов) 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 квалифицированной 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 № 10);

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 27.07.2006 №152-ФЗ «О персональных данных»;

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

5. Права и обязанности Заявителя и Владельца Сертификата

5.1. Права Заявителя, Владельца сертификата

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 №11);

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. Обязанности Заявителя, Владельца сертификата

Заявитель, Владелец сертификата обязаны:

1) с целью ознакомления с полным текстом изменений Порядка 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 Порядка;

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

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 Владельцем 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 Порядком;

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 также иных данных предоставленных в Удостоверяющий центр;

16) соблюдать требования настоящего Порядка.

6. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром

6.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей

Заявитель создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с ФСБ России в порядке, предусмотренном Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ РФ от 09.02.2005 № 66 (в ред. приказа ФСБ РФ от 12.04.2010 № 173).

Удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с ФСБ России в порядке предусмотренном Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ РФ от 09.02.2005 № 66 (в ред. приказа ФСБ РФ от 12.04.2010 № 173).

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 ФЗ «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, а также необходимость выполнения требований, установленных постановлением Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» от 03.02.2012 № 79, в отношении автоматизированного рабочего места Удостоверяющего центра, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя.

6.2. Порядок осуществления плановой смены ключей электронной подписи 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.

Ранее сформированный 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.

6.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности

В случае нарушения конфиденциальности Ключа электронной подписи Удостоверяющего центра Сертификат ключа проверки электронной подписи Удостоверяющего центра признается недействующим 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, признаются 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.

6.4. Форма и сроки действия ключа электронной подписи и Сертификата ключа проверки электронной подписи, форма списка отозванных сертификатов

6.4.1 Сроки действия ключа электронной подписи и Сертификата ключа проверки электронной подписи

6.4.1.1. 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 вносится в соответствующие поля Сертификата ключа проверки электронной подписи Удостоверяющего центра.

6.4.1.4. 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 вносится в соответствующие поля Сертификата ключа проверки электронной подписи Владельца сертификата.

6.4.2 Форма ключа электронной подписи и Сертификата ключа проверки электронной подписи

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».

Дополнительно в выдаваемые сертификаты ключей проверки электронной подписи может быть внесены:

в поле Subject (идентифицирует Владельца сертификата):

Поле E (Email) – адрес электронной почты (опционально);

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;

Тип идентификации Заявителя при выдаче сертификата ключа проверки электронной подписи (при личном присутствии, при удаленной идентификации;

иные поля и расширения по усмотрению Удостоверяющего центра.

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

Содержание полей Subject Сертификатов ключей проверки электронной подписи:

Поле CN (Общее имя) – Фамилия Имя Отчество;

Поле SN (Фамилия) – Фамилия;

Поле G (Имя Отчество) – Имя Отчество;

Поле L (Наименование населённого пункта) – Город населенный пункт;

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

Поле C (Страна) – RU;

Поле E (адрес электронной почты) – опционально

Поле INN (ИНН) – личный ИНН заявителя;

Поле SNILS (СНИЛС) - личный СНИЛС заявителя.

6.4.3 Форма списка отозванных сертификатов.

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 Серийный номер сертификата (CertificateSerialNumber) Время обработки заявления на прекращение действия сертификата (Time) Код причины прекращения действия сертификаты сертификата (Reson Code) "0" Не указана "1" Нарушение конфиденциальности ключа "2" Нарушение конфиденциальности ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор Ключа электронной подписи Удостоверяющего центра
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия Сертификата ключа проверки электронной подписи Удостоверяющего центра

6.5. Обеспечение конфиденциальности информации

Ключ электронной подписи, соответствующий Сертификату ключа проверки электронной подписи, является конфиденциальной информацией Владельца сертификата. Удостоверяющий центр не осуществляет хранение Ключей электронных подписей Владельцев сертификатов.

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 информации, предоставляемой в Удостоверяющий центр в соответствии с настоящим Порядком и не включенной в Сертификат ключа проверки электронной подписи.

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 информации, включенной в состав Сертификата ключа проверки электронной подписи и Списка отозванных сертификатов, создаваемых Удостоверяющим центром.

Удостоверяющий центр имеет право раскрывать третьим лицам информацию, только в случаях, установленных и предусмотренных действующим законодательством Российской Федерации.

6.6. Порядок создания ключей электронной подписи и Сертификатов ключей проверки электронной подписи и управления ими

Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется Удостоверяющим центром или самостоятельно заявителем.

Создание ключей электронных подписей и ключей проверки электронных подписей, предназначенных для создания и проверки ключей электронной подписи, осуществляется заявителем с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с эксплуатационной и технической документацией на используемые средства электронной подписи.

Создание ключей электронных подписей и ключей проверки электронных подписей должно осуществляться заявителем в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Перед созданием запроса на сертификат Заявитель формирует ключ электронной подписи и ключ проверки электронной подписи в распределенном режиме работы Удостоверяющего центра. В централизованном режиме работы Удостоверяющего центра оператор удостоверяющего центра формирует (в присутствии Заявителя) ключ электронной подписи и ключ проверки электронной подписи. Далее формируется запрос на создание сертификата в электронной форме (файл в формате PKCS#10) и (или) в форме бумажного документа, подписанного заявителем собственноручно.

В случае, если используемые заявителем средства электронной подписи не позволяют сформировать запрос на создание сертификата в форме бумажного документа, допускается предоставление данного запроса в электронной форме, подписанного Ключом электронной подписью заявителя.

Заявитель, при обращении в Удостоверяющий центр за получением квалифицированного сертификата, обязан информировать Удостоверяющий центр о средстве электронной подписи (наименование и реквизиты заключения ФСБ России о подтверждении соответствия средства электронной подписи), которое было использовано для создания ключа электронной подписи и ключа проверки электронной подписи.

При создании ключа электронной подписи и ключа проверки электронной подписи должен устанавливаться пароль доступа к ключевой информации, отвечающий требованиям к сложности паролей в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 10 к настоящему Порядку.

При создании ключа электронной подписи и ключа проверки электронной подписи заявителем основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, является одновременное соблюдение следующих условий:

− подтверждена достоверность документов и сведений, предоставляемых в Удостоверяющий центр заявителем;

− установлена личность заявителя при его личном присутствии или удаленно в соответствии с пунктом 1 статьи 18 ФЗ № 63 «Об электронной подписи»;

− информация, указанная в запросе создание сертификата, в том числе информация о полномочиях лица, подписавшего запрос, соответствуют сведениям, указанными заявителем в документах, предоставляемых в Удостоверяющий центр;

− сформированный заявителем запрос на создание сертификата на бумажном носителе, подписанный собственноручной подписью заявителя, либо запрос в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя;

− имеется положительный результат проверки электронной подписи, с помощью которой подписан запрос на создание сертификата, в случае если он предоставлен в электронной форме.

Сертификат ключа проверки электронной подписи выпускается работником УЦ в присутствии заявителя или без (с вручением и ознакомлением с сертификатом ключа проверки электронной подписи на бумажном носителе или его электронной формы).

7. Процедура создания и выдачи квалифицированных сертификатов ключей проверки электронной подписи

7.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов

Удостоверяющий центр создает Сертификат ключа проверки электронной подписи в присутствии Заявителя, так и в отсутствии Заявителя на основании представленного им заявления и запроса в формате pkcs#10 на создание Сертификата ключа проверки электронной подписи. Формы заявлений на создание Сертификата ключа проверки электронной подписи приведены в Приложениях № 1, №1а, настоящего Порядка.

7.2. Требования к заявлению на создание и выдачу квалифицированных сертификатов

Заявление на создание и выдачу квалифицированного сертификата может быть оформлено как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью Заявителя.

7.3. Порядок установления личности заявителя

Личность гражданина Заявителя идентифицируется при обращении в Удостоверяющий центр за получением квалифицированного сертификата ключа проверки электронной подписи. Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием ключа квалифицированной электронной подписи при наличии действующего квалифицированного сертификата ключа проверки электронной подписи либо посредством идентификации заявителя - гражданина Российской Федерации с применением информационных технологий без его личного присутствия путем предоставления информации, указанной в документе, удостоверяющем личность гражданина Российской Федерации за пределами территории Российской Федерации, содержащем электронный носитель информации с записанными на нем персональными данными владельца паспорта, включая биометрические персональные данные, или путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы в порядке, установленном Федеральным законом от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации". При этом в случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации и единой биометрической системы отказывается от использования шифровальных (криптографических) средств, указанных в части 19 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", удостоверяющий центр обязан отказать такому лицу в проведении указанной идентификации.

7.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для изготовления и выдачи квалифицированного сертификата

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

1. В отношении физического лица:

- Реквизиты документов, признаваемые в соответствии с законодательством Российской Федерации документами, удостоверяющими личность или их нотариально заверенные копии;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговом органе;
- Фамилия, имя, отчество (при наличии), дата и место рождения.

7.5. Порядок проверки достоверности документов и сведений, представленных Заявителем

Сведения, содержащиеся в заявление на выпуск квалифицированного сертификата ключа проверки электронной подписи (часть 2 статьи 17 ФЗ «Об электронной подписи»), Удостоверяющий центр запрашивает и получает из государственных информационных ресурсов в соответствии с частью 1.1 статьи 18 ФЗ «Об электронной подписи».

В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат ключа проверки электронной подписи, и Удостоверяющим центром установлена личность заявителя - физического лица Удостоверяющий центр осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата ключа проверки электронной подписи. В противном случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата ключа проверки электронной подписи.

7.6. Порядок создания и выдачи квалифицированного сертификата в Удостоверяющем центре в присутствии Заявителя

Работник Удостоверяющего центра на основе предоставленных заявительных документов осуществляет создание ключей электронной подписи и запись Ключа электронной подписи на защищенный носитель информации, предоставленный Заявителем.

Также работник Удостоверяющего центра производит создание Сертификата ключа проверки электронной подписи, запись Сертификата ключа проверки электронной подписи на предоставленный защищенный носитель информации, указанный в абзаце первом настоящего раздела.

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 №9 к настоящему Порядку, которую он подписывает собственноручно.

При получении первого Сертификата ключа проверки электронной подписи Заявителю сообщается ключевая фраза, использующаяся для аутентификации Владельца сертификата при выполнении процедур, установленных настоящим Порядком, 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 и после расписки в бумажной форме Сертификата ключа проверки электронной подписи в соответствии с пунктом 5 настоящего раздела Порядка.

7.7. Порядок создания и выдачи квалифицированного сертификата в Удостоверяющем центре без присутствия Заявителя

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

1) Для формирования Ключа электронной подписи и получения Сертификата ключа проверки электронной подписи Заявитель производит формирование Ключа электронной подписи и файла запроса на создание Сертификата ключа проверки электронной подписи с помощью Средств электронной подписи.

2) Заявитель предоставляет в Удостоверяющий центр:

- файл запроса на создание Сертификата ключа проверки электронной подписи;
- заявление на создание Сертификата ключа проверки электронной подписи в электронной форме (Приложениях № 2).

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

4) Работник Удостоверяющего центра в течение 3 (трех) рабочих дней осуществляет проверку корректности заполнения файла запроса и заявления на создание Сертификата ключа проверки электронной подписи в электронной форме, а также определяет и сообщает Заявителю перечень документов, необходимых для создания Сертификата ключа проверки электронной подписи, из числа документов, содержащихся в перечне, раздела 7.4 настоящего Порядка.

5) 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.

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

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

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

9) При получении первого Сертификата ключа проверки электронной подписи работник Удостоверяющего центра сообщает Заявителю ключевую фразу, используемую для аутентификации Владельца сертификата при выполнении процедур, установленных настоящим Порядком, 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.

7.8. Подтверждение действительности электронной подписи, использованной для подписания электронных документов

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 № 6 к настоящему Порядку и предоставляется в Удостоверяющий центр посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

- время и дату подачи заявления;
- время и дату (либо период времени), на момент наступления которых требуется установить статус Сертификата ключа проверки электронной подписи;
- идентификационные данные Владельца сертификата, действительность Сертификата ключа проверки электронной подписи которого требуется установить;
- серийный номер Сертификата ключа проверки электронной подписи, статус которого требуется установить.

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.

7.9. Процедуры, осуществляемые при приостановлении действия, прекращении действия и аннулировании квалифицированного сертификата

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

- по заявлению Владельца сертификата;
- по инициативе Удостоверяющего центра.

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.

Если в течение срока приостановления действия Сертификата ключа проверки электронной подписи действие этого сертификата не будет возобновлено, то действие данного сертификата прекращается Удостоверяющим центром.

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.

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.

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

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 № 4 к настоящему Порядку подписанного электронной подписью Владельца сертификата.

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.

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 днем, в течение которого указанное заявление было получено Удостоверяющим центром. В случае принятия работником Удостоверяющего центра решения о приостановление действия Сертификата ключа проверки электронной подписи соответствующая информация вносится в Реестр сертификатов.

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 Порядком;
- при получении заявления о приостановлении действия Сертификата ключа проверки электронной подписи в связи со смертью Владельца сертификата с приложением к заявлению копии свидетельства о смерти.

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. Официальным уведомлением о факте приостановления действия Сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) Списка отозванных 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 7.1

7.9.1. Возобновление действия Сертификата ключа проверки электронной подписи

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 № 5 к настоящему **Порядку** 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.

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.

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.

Возобновление действия Сертификата ключа проверки электронной подписи возможно только в течение срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено.

7.9.2 Прекращение действия Сертификата ключа проверки электронной подписи

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

- в связи с истечением установленного срока действия Сертификата ключа проверки электронной подписи;
- на основании заявления Владельца сертификата;
- в случае прекращения деятельности Удостоверяющего центра без перехода его функций другим лицам;
- по истечении срока, на который действие Сертификата ключа проверки электронной подписи было приостановлено;
- при нарушении конфиденциальности Ключа электронной подписи Удостоверяющего центра;

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.

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 № 3 к настоящему Порядку 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 № 3 к настоящему Порядку, подписанного квалифицированной электронной подписью Владельца сертификата.

Подача Владельцем сертификата заявления на прекращение действия Сертификата ключа проверки электронной подписи в форме электронного документа помощью Единого портала государственных и муниципальных услуг.

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 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.

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.

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. Официальным уведомлением о прекращении действия Сертификата ключа проверки электронной подписи является опубликование первого (наиболее раннего) Списка отозванных сертификатов. 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.

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 вносится.

7.9.3. Аннулирование Сертификата ключа проверки электронной подписи

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 с момента получения решения в адрес Фонда аннулирует Сертификат ключа проверки электронной подписи путем внесения записи о его аннулировании в Реестр сертификатов.

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.

7.10. Порядок ведения реестра квалифицированных сертификатов

Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с ФЗ «Об электронной подписи», Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минцифры России от 08 ноября 2022 г. № 1138, иными принимаемыми в соответствии с ФЗ «Об электронной подписи» и Федеральным законом «Об информации, информационных технологиях и о защите информации» нормативными правовыми актами и настоящим Порядком

Удостоверяющий центр обеспечивает защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к Реестру сертификатов ежедневно и круглосуточно. Актуальную информацию из реестра сертификатов в электронной форме ежедневно можно получить, отправив заявку по адресу: ca@fciit.ru

7.11. Порядок технического обслуживания реестра квалифицированных сертификатов

Плановые технические работы по обслуживанию реестра сертификатов, в том числе процедуры резервного копирования, проводятся Удостоверяющим центром в выходные дни либо в ночное время (с учетом часовых поясов на территории Российской Федерации, Москва UTC+3) с целью минимизации и возможности исключения перерывов в работе при использовании квалифицированных сертификатов и в возможности получения доступа к реестру сертификатов Удостоверяющего центра, опубликованному на сайте: www.fciit.ru

Внеплановые технические работы по обслуживанию реестра сертификатов проводятся в оперативном режиме при выявлении такой необходимости.

Перед проведением плановых (внеплановых) работ по техническому обслуживанию реестра сертификатов, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия, Удостоверяющий центр оповещает о проведении вышеуказанных работ посредством публикации соответствующей информации на сайте Удостоверяющего центра.

8. Порядок исполнения обязанностей Удостоверяющего центра

8.1. Информирование 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

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, содержащее информацию 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, приведено в приложении № 10 к настоящему Порядку.

8.2. Требования к средствам электронной подписи используемым заявителем

Средства электронной подписи, используемые заявителем, должны соответствовать требованиям части 4 статьи 12 ФЗ «Об электронной подписи», Требованиями к средствам электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, а также обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные ключом квалифицированной электронной подписи, или в случае, если электронный документ подписан несколькими ключами квалифицированной электронной подписи.

8.3. Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов, а также защиту информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности.

Защита информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра, которые в том числе включают меры по защите информации, содержащейся в реестре сертификатов, путем реализации следующих мероприятий:

- обеспечивается контроль доступа в помещения, где размещены технические средства Удостоверяющего центра;
- реализована ролевая модель доступа к компонентам средств Удостоверяющего центра, обеспечивается идентификация, аутентификация и разграничение доступа уполномоченных лиц к программным и техническим средствам Удостоверяющего центра и защищаемой информации;
- обеспечивается контроль действий уполномоченных лиц Удостоверяющего центра и обслуживающего персонала, приняты меры по предотвращению несанкционированного доступа к средствам Удостоверяющего центра и защищаемой информации;
- формирование и ведение реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему;
- осуществляется регулярное резервное копирование информации, содержащейся в реестре сертификатов с соблюдением требований к защите от несанкционированного доступа к средствам резервного копирования и резервируемой информации;

• для хранения информации используются опечатываемые хранилища информации (металлические шкафы, сейфы, пеналы).

8.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет»

Удостоверяющий центр в соответствии с пунктом 5 части 1 статьи 13 и частью 3 статьи 15 ФЗ «Об электронной подписи» обеспечивает безвозмездный круглосуточный доступ к реестру сертификатов, путем обращения на электронный почтовый адрес заявки в сервис технической поддержки ca@fciit.ru Удостоверяющего центра, за исключением периодов технического обслуживания реестра сертификатов, проводимых Удостоверяющим центром в соответствии с пунктом 7.11 настоящего Порядка.

Удостоверяющий центр также обеспечивает круглосуточный доступ к списку отозванных сертификатов в информационно телекоммуникационной сети Интернет (по двум точкам распространения списка отозванных http://cdp1.fciit.ru/cdp и http://cdp2.fciit.ru/cdp не реже двух раз в сутки).

8.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Конфиденциальность ключей электронных подписей уполномоченных лиц Удостоверяющего центра, а также ключа электронной подписи Удостоверяющего центра, обеспечивается путем реализации комплекса организационных и технических мер по обеспечению информационной безопасности инфраструктуры Удостоверяющего центра, обеспечению защиты информации, обрабатываемой с использованием средств Удостоверяющего центра.

Хранение и использование ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра осуществляется в соответствии с требованиями Инструкции ФАПСИ № 152, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

Средства Удостоверяющего центра, с использованием которых осуществляется использование и хранение ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра, имеют документ, подтверждающий оценку соответствия по требованиям безопасности информации и соответствуют Требованиям к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796.

Хранение и использование ключей электронной подписи пользователей Удостоверяющего центра осуществляется в соответствии с требованиями с Инструкции ФАПСИ № 152, ответственность за целостность и конфиденциальность ключей при этом возложена на Владельца сертификата проверки ключа электронной подписи. Владелец, получивший квалифицированный сертификат в Удостоверяющем центре, обеспечивает конфиденциальность ключей электронных подписей и обязан:

• хранить в тайне ключ электронной подписи, принимать все возможные меры для предотвращения его утраты, раскрытия, искажения и несанкционированного использования;

• не допускать использование принадлежащих ему ключей электронных подписей без своего согласия;

• уведомлять Удостоверяющий центр и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

• не использовать ключ электронной подписи, если ему стало известно, что этот ключ используется или использовался ранее другими лицами;

• не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр, выдавший квалифицированный сертификат, для прекращения действия этого сертификата при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.

8.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации

Удостоверяющий центр непосредственно после выдачи квалифицированного сертификата владельцу сертификата или его уполномоченному представителю осуществляет регистрацию квалифицированного сертификата в единой системе идентификации и аутентификации в соответствии с частью 5 статьи 18 ФЗ «Об электронной подписи».

При выдаче квалифицированного сертификата Удостоверяющий центр с использованием специализированного программного обеспечения и инфраструктуры осуществляет регистрацию выданного квалифицированного сертификата в единой системе идентификации и аутентификации, для чего направляет в единую систему идентификации и аутентификации сведения о владельце сертификата в объеме, необходимом для регистрации квалифицированного сертификата в единой системе идентификации и аутентификации сведений о владельце сертификата, и о полученном им квалифицированном сертификате, в том числе:

- уникальный серийный номер квалифицированного сертификата;
- тип владельца квалифицированного сертификата физическое лицо;
- даты начала и окончания действия квалифицированного сертификата;
- наименование Удостоверяющего центра, выдавшего квалифицированный сертификат;
- Фамилия, Имя и Отчество владельца квалифицированного сертификата;

номер страхового свидетельства государственного пенсионного страхования заявителя физического лица, являющегося владельца квалифицированного сертификата;

- реквизиты документа, удостоверяющего личность владельца квалифицированного сертификата, в том числе серия и номер документа, удостоверяющего личность, код подразделения, выдавшего документ, дата выдачи;
- адрес регистрации (места жительства);
- пол владельца квалифицированного сертификата;
- дата рождения владельца квалифицированного сертификата;
- место рождения владельца квалифицированного сертификата;
- гражданство владельца квалифицированного сертификата;
- идентификационный номер налогоплательщика (физического лица);
- адрес электронной почты;
- номер мобильного телефона (только при регистрации или подтверждении его учетной записи владельца сертификата при его желании в единой системе идентификации и аутентификации).

8.7. Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации

При выдаче квалифицированного сертификата Удостоверяющий центр по желанию владельца сертификата (физического лица) безвозмездно осуществляет его регистрацию в единой системе идентификации и аутентификации и (или) осуществляет подтверждение учетной записи физического лица в единой системе идентификации и аутентификации.

Результатом регистрации лица в единой системе идентификации и аутентификации или подтверждения его учетной записи является соответственно выдача этому лицу пароля для первого входа в единую систему идентификации и аутентификации или подтверждение его учетной записи в единой системе идентификации и аутентификации.

При централизованной выдачи сертификата ключа проверки электронной подписи, заявитель указывает свое согласие на регистрацию и подтверждение учетной записи в ЕСИА в поле «галочкой» «Прошу меня зарегистрировать в ЕСИА», согласно Приложению № 1.

При распределенной выдаче сертификата ключа проверки электронной подписи, заявитель указывает свое согласие на регистрацию и подтверждение учетной записи в ЕСИА в поле «галочкой» «Прошу меня зарегистрировать в ЕСИА» в Приложению № 2.

8.8. Предоставление доступа к информации, содержащейся в реестре квалифицированных сертификатов

Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации, содержащейся в реестре сертификатов Удостоверяющего центра, по соответствующему запросу, направленному на адрес технической поддержки: ca@fciit.ru, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата путем публикации реестра сертификатов на www.fciit.ru в форме электронного документа, который доступен для загрузки с использованием сети Интернет.

9. Порядок предоставления информации в Удостоверяющий центр

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;

10. Дополнительные сервисы Удостоверяющего центра

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

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

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.

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 № 7 к настоящему Порядку.

Заявление должно содержать следующую информацию:

- время и дату подачи заявления;
- идентификационные данные Владельца сертификата, электронную подпись которого необходимо проверить в электронном документе;
- время и дату формирования электронной подписи в электронном документе;
- 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:
- Сертификат ключа проверки электронной подписи, с использованием которого необходимо проверить электронную подпись в электронном документе – в виде файла стандарта CMS;

- 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).
- Проверку электронной подписи в электронном документе осуществляет комиссия, сформированная из числа работников Удостоверяющего центра.
- Результатом проверки электронной подписи в электронном документе является заключение комиссии Удостоверяющего центра, содержащее следующую информацию:
- состав комиссии, осуществлявшей проверку;
- основание для проведения проверки;
- данные, представленные комиссии для проведения проверки;
- отчет о выполненной проверке.
- Отчет о выполненной проверке содержит:
- время и место проведения проверки;
- содержание и результаты проверки;
- обоснование результатов проверки.

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.

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.

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

10.2. Блокировка защищенного носителя информации, содержащего Ключ электронной подписи Владельца сертификата

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, заполненным по форме Приложения № 8 настоящего Порядка.

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

Создание нового ключа электронной подписи и нового сертификата ключа проверки электронной подписи осуществляются в соответствии с разделами 7.1. и 7.4. настоящего Порядка.

11. Список приложений:

1	Форма заявления для физического лица при личном обращении в Удостоверяющий центр
1а	Форма заявления о присоединении к Договору об оказании услуг Удостоверяющего центра Фонда «Центр инноваций»
2	Форма заявления на создание Сертификата ключа проверки электронной подписи Заявителя на основании запроса
3	Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи
4	Форма заявления на приостановление действия Сертификата ключа проверки электронной подписи Владельца сертификата
5	Форма заявления на возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата
6	Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром
7	Форма заявления на проверку подлинности электронной подписи в электронном документе
8	Форма Сертификата ключа проверки электронной подписи
9	Форма Сертификата ключа проверки электронной подписи
10	Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи
11	Форма запроса субъекта персональных данных об обрабатываемых персональных данных

Приложение №1

к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

Форма заявления для физического лица при личном обращении в Удостоверяющий центр

Руководителю службы информационной безопасности Фонда «Центр инновации»

от_____

(И.О. Фамилия)

З А Я В Л Е Н И Е

Прошу изготовить мне (Заявителю), _____

_____

_____,

(фамилия, имя, отчество, серия и номер паспорта, кем и когда выдан, адрес места регистрации, код подразделения, пол, дата рождения, место рождения, гражданство)

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

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

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

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

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

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

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

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

8. ИНН Заявителя (12 символов) –

9. СНИЛС Заявителя (11 символов) –

10. Страна/регион –

R	U

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

Наименование объектного идентификатора	Цифровое обозначение

12. Согласие на регистрацию учетной записи Заявителя в ЕСИА (поставить☑ при согласии)

	Прошу зарегистрировать мою учетную запись в ЕСИА

_____

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

«____» _____ 20___г.

Приложение №1а

к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

Форма заявления о присоединении к Договору об оказании услуг Удостоверяющего центра Фонда «Центр инноваций»

З А Я В Л Е Н И Е

о присоединении к Договору об оказании услуг Удостоверяющего центра Фонда «Центр инноваций»

Я, _____

_____

_____

_____

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

принимаю в полном объёме условия оферты о присоединении к Договору об оказании услуг Удостоверяющего центра, являющегося неотъемлемой частью Порядка, утвержденного Приказом Директора Фонда «Центр инноваций и информационных технологий» № 01-01.4/24 от 21.10.2024, 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 (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 Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

Форма заявления на создание Сертификата ключа проверки электронной подписи Заявителя на основании запроса

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

Дата создания заявления: __.__.20___

З А Я В Л Е Н И Е

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

Сведения о запросе на сертификат:
Субъект:
CN=ФИО
SN=Фамилия
G=Имя Отчество
L=Москва
S=77 г. Москва
Street= ул. Радио, д.16 (опционально)
C=RU
E=test@test.ru (опционально)
ИНН ФЛ=000000000000

СНИЛС=00000000000
Алгоритм открытого ключа:
ObjectID алгоритма: 1.2.643.7.1.1.1.1 ГОСТ Р 34.10-2012 256 бит
Параметры алгоритма:
30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
1.2.643.2.2.36.0 ГОСТ Р 34.10-2001, параметры обмена по умолчанию
1.2.643.7.1.1.2.2 ГОСТ Р 34.11-2012 256 бит
Длина открытого ключа: 512 бит
Открытый ключ: UnusedBits = 0
05 50 3a 1f bd f4 86 e4 41 7d cf d3 ae 90 59 f9 f3 4b 8f 18 42 68 31 25 39 f5 22 64 6d 47 0f 32 0e 2a 0a 93 d5 2c 87 00 d4 35 b0 74 23 7d 02 7a 46 0b 1a 4c a1 c8 62 c4 df bc 8a 6a 2a dd 1d 14 7b 85
Запрос атрибутов: 3
Атрибуты 3:
Атрибут[0]: 1.3.6.1.4.1.311.13.2.3 (Версия ОС)
Значение[0][0]:
6.1.7600.2
Атрибут[1]: 1.3.6.1.4.1.311.2.1.14 (Расширения сертификатов)
Значение[1][0]:
Неизвестный тип атрибута
Расширения сертификатов: 3
2.5.29.15: Флаги = 1(Критический), Длина = 4
Использование ключа
Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
1.2.840.113549.1.9.15: Флаги = 0, Длина = c
Возможности SMIME
[1]Возможности SMIME
Идентификатор объекта=1.2.643.2.2.21
2.5.29.37: Флаги = 0, Длина = 46
Улучшенный ключ
Формирование документов для получения государственных услуг в сфере ведения государственного кадастра недвижимости со стороны заявителя (1.2.643.5.1.24.2.1.3)
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Для ведения юридически значимого электронного документооборота (1.2.643.3.166.1.1)
Формирование запроса о предоставлении сведений из Единого государственного реестра прав на недвижимое имущество и сделок с ним (1.2.643.5.1.24.2.26)
Уполномоченное лицо для подписания электронных документов при межведомственном взаимодействии (1.2.643.100.2.1)
Пользователь ЕИС (1.2.643.3.166.2.1)
Класс средства ЭП КС1 (1.2.643.100.113.1)

Класс средства ЭП КС2 (1.2.643.100.113.2)
1.2.643.100.111: Флаги = 0, Длина = 2b
Средство электронной подписи владельца
Средство электронной подписи: КриптоПро CSP (версия 4.0)
1.3.6.1.4.1.311.20.2: Флаги = 0, Длина = e
Имя шаблона сертификата (Тип сертификата)
User.2
Атрибут[2]: 1.3.6.1.4.1.311.13.2.2 (CSP подачи заявок)
Значение[2][0]:
Неизвестный тип атрибута
Сведения о поставщике криптографии
KeySpec = 1
Поставщик = Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider
Подпись: НеиспользБит=0
1e 7a 8f 4a 7e 50 10 9b 4f 1b 55 94 75 e2 0a 45 3d c5 75 e0 d7 a1 e3 4e f0 a2 97 fa 5d 40 08 73 8f 40 c5 2f 59 16 18 76 9c 93 26 09 cc 5c 26 79 a3 0c 3f ad 2c de 88 89 bd 7f 73 94 4d e5 0f 2c f0 a8 21 83 d1 f8 d1 81 7d 5a ab 25 55 8c 9f 14 74 60 43 00 04 b8 d0 6c d3 be 06 91 48 ad 3e 35 b5 ba 7d 68 7c 55 71 80 06 f2 af c3 a0 61 57 fe 68 d7 af e5 f6 27 9e 35 26 dd 88 98 ee 25 7e 46 00 00 34 00 21 00 56 00
Алгоритм подписи:
ObjectID алгоритма: 1.2.643.7.1.1.3.2 ГОСТ Р 34.11-2012/34.10-2012 256 бит
Параметры алгоритма: NULL
Подпись: НеиспользБит=0
de 15 12 43 9c 65 76 37 41 e4 9f 1d cd e5 b1 be dc 20 9a 77 74 61 be e8 43 17 fb 06 d4 6e 11 2d b9 e1 b1 d7 9d c3 fc b4 ad 17 bd 84 01 a6 aa bd e2 b0 5a 64 42 46 e2 ae aa c4 2c 60 ac bf 85 d7
Подпись соответствует открытому ключу
Хеш ИД ключа (rfc-sha1): 71 8c 95 76 d1 0e 60 f2 f4 cf 7a 26 c6 a7 f8 53 19 59 54 b0
Хеш ИД ключа (sha1): 23 a3 e3 65 53 63 0d 50 ea 2b ee cc f0 48 92 0f 2c 71 36 d3

Согласие на регистрацию учетной записи Заявителя в ЕСИА (поставить☑ при согласии)

	Прошу зарегистрировать мою учетную запись в ЕСИА

_____
(Фамилия Имя Отчество Заявителя полностью, собственноручно)

Подпись владельца Ключа электронной подписи (Заявителя): _____

«____» _____ 20___г.

Приложение №3
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

Форма заявления на прекращение действия Сертификата ключа проверки электронной подписи Владельца сертификата

Руководителю службы информационной безопасности
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 сертификта _____/_____
(И.О. Фамилия Владельца сертификата) (Подпись Владельца сертификата)

«____» _____ 20____ г.

Приложение №4
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»
Форма заявления на приостановление действия Сертификата ключа проверки электронной подписи Владельца сертификата

Руководителю службы информационной безопасности
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 №5
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»

Форма заявления на возобновление действия Сертификата ключа проверки электронной подписи Владельца сертификата

Руководителю службы информационной безопасности

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 №6
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»
Форма заявления на получение информации о статусе Сертификата ключа проверки электронной подписи созданного Удостоверяющим центром

Руководителю службы информационной безопасности

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

Я,_____
(Фамилия Имя Отчество)

_____
(паспортные данные)

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

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

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

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

«____» _____ 20____ г.

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

Приложение №7
к Порядку Удостоверяющего центра нотариата России
Форма заявления на проверку подлинности электронной подписи в электронном документе

Руководителю службы информационной безопасности

от _____
(И.О. Фамилия)

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

Я,_____
(Фамилия Имя Отчество)

_____
(паспортные данные)

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

1. Файл формата CMS, содержащий сертификат ключа проверки электронной подписи, с использованием которого необходимо осуществить проверку подлинности электронной подписи в электронном документе на прилагаемом к заявлению носителе – рег. № Н–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. Время[2] 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.

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

Приложение №8
к Порядку Удостоверяющего центра нотариата России
Форма заявления на форматирование защищенного носителя информации

Руководителю службы информационной безопасности

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.

Приложение №9
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»
Форма Сертификата ключа проверки электронной подписи

Удостоверяющий центр
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: 3BD1F0C1D3A0BD80E911D90163A9169C
Издатель сертификата: CN=Фонд "Центр инноваций", O=Фонд "Центр инноваций и информационных технологий", STREET=улица Долгоруковская, д. 15, стр. 4-5, L=г. Москва, S=77 г. Москва, C=RU, ИНН=007708237747, ОГРН=1107799007425, E=ca@fciit.ru
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
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1)
Параметры: 30 13 06 07 2A 85 03 02 02 24 00 06 08 2A 85 03 07 01 01 02 02
Значение: 0440 9F78 BBD0 F3FA 5E5D 5E4E C967 0E32 742E 84B4 9D73 B20D 1BB7 25BD 0BAB 4482 6AFD 5706 8056 340E 0382 B90A F6E4 36F3 3174 47C2 3639 A352 420E 5E31 B15D 4466 D2A0
Расширения сертификата X.509
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (f8)
Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.14
Значение: 6a 2a a2 c6 14 59 86 02 5e 82 6d 6a 11 ea a8 00 51 fa aa 02
Расширение: Идентификатор ключа субъекта
Идентификатор: 1.3.6.1.4.1.311.21.7
Значение: Шаблон=1.2.643.2.2.50.1.9.13323757.11834142.10634780.1840493.53542.59589, Основная версия=1, Вспомогательная версия=0
Расширение: Сведения о шаблоне сертификата
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=7f 48 21 2c be 54 f5 7a 31 18 25 6a ba 64 71 e0 93 4a 3c 9c, Поставщик сертификата: Адрес каталога:CN=Минцифры России, ИНН=007710474375, ОГРН=1047702026701, O=Минцифры России, STREET="улица Тверская, дом 7", L=г. Москва, S=77 Москва, C=RU, E=dit@minsvyaz.ru, Серийный номер сертификата=00 b9 ed c1 ee 00 00 00 00 00 fa
Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.37
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4),
Расширение: Улучшенный ключ
Идентификатор: 2.5.29.32
Значение: [1]Политика сертификата: Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата: Идентификатор политики=1.2.643.3.166.1.1, [3]Политика сертификата: Идентификатор политики=1.2.643.3.166.2.1
Расширение: Политики сертификата
Идентификатор: 1.2.643.100.112
Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" версий 4.0 (заключение: Сертификат соотвествия № СФ/124-3380 от 11.05.2018), средство удостоверяющего центра: ПАК "КриптоПро УЦ" версий 2.0 (заключение: Сертификат соотвествия № СФ/128-2983 от 18.11.2016)
Расширение: Средства электронной подписи и УЦ издателя
Идентификатор: 1.2.643.100.111
Значение: Средство электронной подписи: СКЗИ "КриптоПро CSP" версий 4.0
Расширение: Средство электронной подписи владельца
Идентификатор: 2.5.29.31
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:
Полное имя:URL=http://cdp1.fciit.ru/cdp/7f48212cbe54f57a3118256aba6471e0934a3c9c.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения: Полное имя:URL=http://cdp2.fciit.ru/cdp/7f48212cbe54f57a3118256aba6471e0934a3c9c.crl
Расширение: Точки распространения списков отзыва (CRL)
Идентификатор: 1.3.6.1.5.5.7.1.1
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-qual2012.cer, [3]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://cdp2.fciit.ru/cdp/ca-qual2012.cer
Расширение: Доступ к информации о центрах сертификации
Идентификатор: 2.5.29.16
Значение: Действителен с 17 декабря 2018 г. 11:46:16 по 17 декабря 2019 г. 11:46:16
Расширение: Период использования ключа электронной подписи
Подпись Удостоверяющего центра:
Алгоритм подписи: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)
Параметры:
Значение: 64F7 3019 A1BE 4FED D2DE 1CD9 2EFA 3E18 05D9 C2F9 5BF5 7BA9 A8ED CB1E 6452 F50E CD3B 7CD7 F900 49E3 30C9 1659 3069 A9D5 58C4 26C3 C77D 2850 40BA BF9A 80B9 3F3A

Подпись Владельца сертификата: _____/_____

"___" _____ 20__ г.

Подпись Уполномоченного лица УЦ: _____/_____

«____» _____ 20__ г.
М.П.

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

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

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

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

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.

Владельцем 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).

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.

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.

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

Утрата конфиденциальности Ключа проверки электронной подписи (в том числе нарушение правил хранения Ключа проверки электронной подписи, несоблюдение требований Порядка 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.

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.

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

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.

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.

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 Порядком;

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.fciit.ru;

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

Приложение №11
к Порядку реализации функций аккредитованного удостоверяющего центра и исполнение его обязанностей удостоверяющим центром Фонда «Центр инноваций и информационных технологий»
Форма запроса субъекта персональных данных об обрабатываемых персональных данных

Руководителю службы информационной безопасности

от _____
(И.О. Фамилия)

З А П Р О С

субъекта персональных данных об обрабатываемых персональных данныхЯ,_____

(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 - 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.