УТВЕРЖДЕН
приказом Акционерного общества
«ИнфоТеКС Интернет Траст»
от 13.10.2023 № 27-07/22

РЕГЛАМЕНТ
оказания Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 4
1. ОБЩИЕ ПОЛОЖЕНИЯ 6
1.1. Предмет регулирования Регламента 6
1.2. Идентификация Регламента 6
1.3. Публикация Регламента 6
1.4. Срок действия Регламента 6
1.5. Присоединение к Регламенту 6
1.6. Порядок утверждения и внесения изменений в Регламент 6
1.7. Информация о месте нахождения и графике работы Удостоверяющего центра 7
1.8. Контактная информация Удостоверяющего центра 7
1.9. Разрешение споров 7
1.10. Прекращение деятельности Удостоверяющего центра 7
2. РЕАЛИЗУЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИИ И ОКАЗЫВАЕМЫЕ УСЛУГИ 7
3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 8
3.1. Права Удостоверяющего центра 8
3.2. Обязанности Удостоверяющего центра 8
4. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 10
4.1. Права Пользователя Удостоверяющего центра 10
4.2. Обязанности Пользователя Удостоверяющего центра 10
5. ОТВЕТСТВЕННОСТЬ 11
5.1. Ответственность Удостоверяющего центра 11
5.2. Ответственность Пользователя 11
6. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ 11
6.1. Виды конфиденциальной информации 11
6.2. Виды информации, не относящейся к конфиденциальной 11
6.3. Предоставление конфиденциальной информации 12
7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 12
8. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ 12
8.1. Регистрация Пользователя Удостоверяющего центра. 12
8.2. Порядок создания ключа электронной подписи и ключа проверки электронной подписи. 12
8.3. Порядок проверки достоверности сведений, содержащихся в запросе на сертификат… 13
8.4. Порядок создания и выдачи сертификата ключа проверки усиленной неквалифицированной электронной подписи. 13
8.5. Сроки действия ключа электронной подписи и сертификата ключа проверки усиленной неквалифицированной электронной подписи Пользователя. 13
8.6. Подтверждение действительности электронной подписи 13
8.7. Порядок прекращения действия или аннулирования сертификата ключа проверки электронной подписи 15
8.8. Порядок ведения и предоставления доступа к реестру сертификатов. 16

9. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА 17
9.1. 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 и их проверки 17
9.2. Выдача по обращению Заявителя средств электронной подписи 17
9.3. Обеспечение актуальности информации, содержащейся в реестре сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий 17
9.4. Предоставление доступа к информации, содержащейся в реестре сертификатов.....17
10. МЕХАНИЗМ ДОКАЗАТЕЛЬСТВА ВЛАДЕНИЯ КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ..17
11. СОДЕРЖАНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ УСИЛЕННОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ 17
12. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ.....18
13. УЧЕТНО-ОТЧЕТНОЕ ВРЕМЯ.....18
14. ПРИЛОЖЕНИЯ.....18

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Владелец сертификата ключа проверки электронной подписи (далее - владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 № 63-ФЗ "Об электронной подписи" (далее – Закон "Об электронной подписи") порядке выдан сертификат ключа проверки электронной подписи.

Единая система идентификации и аутентификации - федеральная государственная информационная система "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

Запрос на сертификат ключа проверки электронной подписи - электронное сообщение определенного формата и синтаксиса, созданное в соответствии со стандартом PKCS#10, содержащее значение ключа проверки электронной подписи, а также иную информацию, необходимую для создания сертификата.

Заявитель - физическое лицо, обращающееся с соответствующим заявлением на выдачу сертификата ключа проверки электронной подписи в Удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Заявление на выдачу сертификата ключа проверки электронной подписи - запрос на сертификат ключа проверки электронной подписи, созданный Пользователем и переданный в Удостоверяющий центр по протоколам, защищенным с использованием российских криптографических алгоритмов.

Инфраструктура - информационно-технологическая и коммуникационная инфраструктура, подключение Удостоверяющего центра к которой производится в порядке, установленном в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2010 года № 210-ФЗ "Об организации предоставления государственных и муниципальных услуг".

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи**.**

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

Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам.

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

Мобильное приложение - устанавливаемое на мобильное устройство программное обеспечение, реализующее, в том числе, функции средства криптографической защиты информации и функции средства электронной подписи, и входящее в состав специализированной защищенной автоматизированной системы Удостоверяющего центра.

Несанкционированный доступ к информации - доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Пользователь Удостоверяющего центра (далее - Пользователь) - физическое лицо, присоединившееся к настоящему Регламенту и зарегистрированное в реестре Пользователей Удостоверяющего центра.

Регистрационные данные Пользователя - сведения, предоставляемые Пользователем в целях регистрации в Удостоверяющем центре и создания сертификата ключа проверки электронной подписи.

Реестр Пользователей - база данных Удостоверяющего центра, содержащая регистрационные данные Пользователей.

Реестр сертификатов - база данных Удостоверяющего центра, содержащая сведения о выданных и аннулированных Удостоверяющим центром сертификатах 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.

Сертификат ключа проверки электронной подписи (далее - сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи**.**

Список аннулированных сертификатов - отдельный раздел Реестра сертификатов, содержащий список уникальных номеров сертификатов ключей проверки электронных подписей, которые были аннулированы или действие которых на определенный момент времени было прекращено Удостоверяющим центром до истечения срока их действия, а также информацию о датах и об основаниях аннулирования или прекращения действия этих сертификатов.

Средства 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.

Средства Удостоверяющего центра - программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра.

Удостоверяющий центр - Акционерное общество «ИнфоТеКС Интернет Траст», выполняющее функции удостоверяющего центра по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей, а также иные функции, предусмотренные Федеральным законом «Об электронной подписи».

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

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию**.**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Предмет регулирования Регламента

Настоящий Регламент устанавливает порядок реализации Акционерным обществом «ИнфоТеКС Интернет Траст» функций Удостоверяющего центра и исполнения его обязанностей в соответствии с требованиями, установленными Федеральным законом «Об электронной подписи».

1.2. Идентификация Регламента

Наименование документа: «Регламент предоставления Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей».
Версия: 3.0.

1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде на сайте Акционерного общества «ИнфоТеКС Интернет Траст» iitrust.ru.

1.4. Срок действия Регламента

1.4.1. Настоящий Регламент вступает в силу со дня его публикации и действует до момента уведомления Удостоверяющим центром о прекращении действия Регламента.

1.4.2. Уведомление о прекращении действия Регламента осуществляется способом, определенным в разделе «Публикация Регламента».

1.5. Присоединение к Регламенту

1.5.1. Настоящий Регламент со всеми приложениями к нему является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

1.5.2. Присоединение к настоящему Регламенту осуществляется путем подачи Заявителем заявления на выдачу сертификата ключа проверки электронной подписи. С момента подачи заявления Заявитель считается присоединившимся к Регламенту и становится стороной Регламента - Пользователем Удостоверяющего центра.

1.5.3. Факт присоединения Заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент подачи заявления на выдачу сертификата ключа проверки электронной подписи. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

1.6. Порядок утверждения и внесения изменений в Регламент

1.6.1. Регламент утверждается приказом Акционерного общества «ИнфоТеКС Интернет Траст».

1.6.2. Сообщения об ошибках в положениях настоящего Регламента, а также предложения по уточнению его положений могут направляться в Удостоверяющий центр по электронной почте в соответствии с контактной информацией, указанной в разделе 1.8 настоящего Регламента.

1.6.3. Изменения и дополнения в Регламент вносятся Удостоверяющим центром в одностороннем порядке.

1.6.4. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра не оказывают либо оказывают незначительное влияние на условия предоставления услуг Удостоверяющего центра, вносятся без изменения номера версии данного документа.

1.6.5. Изменения в разделы настоящего Регламента, которые по оценкам Удостоверяющего центра могут иметь значительное влияние на условия предоставления услуг Удостоверяющего центра, вносятся с увеличением номера версии данного документа.

1.6.6. Уведомление Пользователей о внесении изменений в Регламент осуществляется способом, определенным в разделе "Публикация Регламента".

1.7. **Информация о месте нахождения и графике работы Удостоверяющего центра**

1.7.1. Адрес места нахождения Удостоверяющего центра Акционерного общества «ИнфоТеКС Интернет Траст»: 127287, Москва, ул. Мишина, дом 56, стр. 2, этаж 3, пом. IX, комн. 11.

1.7.2. График работы Удостоверяющего центра: ежедневно, кроме выходных и праздничных дней, с 9:00 до 18:00 по московскому времени.

1.8. **Контактная информация Удостоверяющего центра**

Телефон: 8-800-250-8-265.

Адрес электронной почты: 77@iitrust.ru.

Почтовый адрес: 127083, г. Москва, ул. Мишина, дом 56, стр. 2, подъезд 1, этаж 2.

1.9. **Разрешение споров**

1.9.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и сторона, присоединившаяся к Регламенту.

1.9.2. Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

1.9.3. Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.

1.9.4. Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, и по которым не было достигнуто соглашение, разрешаются в судебном порядке в соответствии с законодательством Российской Федерации.

1.10. **Прекращение деятельности Удостоверяющего центра**

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

2. РЕАЛИЗУЕМЫЕ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ФУНКЦИИ И ОКАЗЫВАЕМЫЕ УСЛУГИ

В соответствии с Законом «Об электронной подписи» Удостоверяющий центр реализует следующие функции и оказывает услуги:

2.1. Создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты Заявителям, при условии идентификации Заявителя в порядке, установленном Федеральным законом «Об электронной подписи».

2.2. Осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения Заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи.

2.3. Устанавливает сроки действия сертификатов ключей проверки электронных подписей.

2.4. Аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей.

2.5. Выдает по обращению Заявителя средства электронной подписи, обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи Заявителем.

2.6. Ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов, в том числе включающий в себя информацию, содержащуюся в выданных Удостоверяющим центром сертификатах, а также сведения о датах прекращения действия или аннулирования сертификатов и основаниях таких прекращения или аннулирования.

2.7. Устанавливает порядок ведения реестра сертификатов и порядок доступа к нему, а также обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет".

2.8. Проверяет уникальность ключей проверки электронных подписей в реестре сертификатов.

2.9. Осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей.

2.10. Осуществляет иную связанную с использованием электронной подписи деятельность.

3. ПРАВА И ОБЯЗАННОСТИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. **Права Удостоверяющего центра**

Удостоверяющий центр имеет право:

3.1.1. Отказать в регистрации лицам, обратившимся в Удостоверяющий центр, с указанием причин отказа.

3.1.2. Отказать в выдаче сертификата Пользователям, обратившимся в Удостоверяющий центр за получением сертификата, с указанием причин отказа.

3.1.3. Прекратить действие выданного Удостоверяющим центром сертификата в следующих случаях:

- при наличии у Удостоверяющего центра существенных оснований полагать, что соответствующий ключ электронной подписи был скомпрометирован;
- если установлено, что сертификат содержит сведения, утратившие свою достоверность в связи с изменением регистрационных данных Пользователя;
- если установлено, что в результате технической ошибки сертификат содержит недостоверные или неполные сведения;
- в случае невыполнения владельцем сертификата обязанностей, установленных Федеральным законом «Об электронной подписи», иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи», а также настоящим Регламентом.

3.1.4. Осуществлять отправку сервисной информации в составе SMS-сообщений, направляемых на указанный Пользователем при регистрации абонентский номер подвижной радиотелефонной связи в целях получения Пользователем услуг Удостоверяющего центра.

3.2. **Обязанности Удостоверяющего центра**

3.2.1. Удостоверяющий центр обязан информировать 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.

3.2.2. Удостоверяющий центр обязан обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.2.3. Удостоверяющий центр обязан 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.

3.2.4. Удостоверяющий центр обязан отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае, если не было подтверждено то, что Заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному Заявителем для получения сертификата ключа проверки электронной подписи.

3.2.5. Удостоверяющий центр обязан отказать Заявителю в создании сертификата ключа проверки электронной подписи в случае отрицательного результата проверки в реестре сертификатов уникальности ключа проверки электронной подписи, указанного Заявителем для получения сертификата ключа проверки электронной подписи.

3.2.6. Удостоверяющий центр обязан хранить информацию, внесенную в реестр сертификатов Удостоверяющего центра, в течение всего срока деятельности удостоверяющего центра, если более короткий срок не установлен нормативными правовыми актами.

3.2.7. Удостоверяющий центр обязан внести в реестр сертификатов информацию о сертификате ключа проверки электронной подписи не позднее указанной в нем даты начала действия такого сертификата.

3.2.8. Удостоверяющий центр обязан прекратить действие сертификата в следующих случаях:

- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в иных случаях, установленных Федеральным законом "Об электронной подписи", другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или настоящим Регламентом.

3.2.9. Удостоверяющий центр обязан аннулировать сертификат в следующих случаях:

- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

3.2.10. Удостоверяющий центр обязан внести информацию о прекращении действия сертификата ключа проверки электронной подписи в реестр сертификатов в течение двенадцати часов с момента наступления обстоятельств, указанных в пунктах 3.2.8 и 3.2.9 настоящего Регламента, или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

3.2.11. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи Удостоверяющий центр обязан уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления электронного документа на мобильное устройство, на котором установлен зарегистрированный за владельцем сертификата экземпляр Мобильного приложения.

3.2.12. Удостоверяющий центр обязан выполнять порядок реализации функций Удостоверяющего центра и исполнения его обязанностей, установленный настоящим Регламентом в соответствии с Федеральным законом «Об электронной подписи» и иными нормативными правовыми актами, принимаемыми в соответствии с Федеральным законом «Об электронной подписи».

3.2.13. Удостоверяющий центр обязан обеспечить взаимодействие Удостоверяющего центра с единой системой идентификации и аутентификации, гражданами (физическими лицами) с применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

3.2.14. При выдаче сертификата Удостоверяющий центр обязан:

- определить лицо, подающее заявление в электронной форме без личного присутствия, с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации;
- с использованием Инфраструктуры осуществить проверку достоверности сведений, представленных Заявителем в составе заявления на выдачу сертификата;
- отказать Заявителю в выдаче сертификата в случаях если достоверность сведений, представленных Заявителем в составе заявления на выдачу сертификата, не подтверждена.

4. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. **Права Пользователя Удостоверяющего центра**

Пользователь Удостоверяющего центра имеет право:

4.1.1. Обращаться в Удостоверяющий центр с целью получения сертификата ключа проверки электронной подписи.

4.1.2. Обращаться в Удостоверяющий центр с целью получения средств электронной подписи.

4.1.3. Получать доступ к списку аннулированных сертификатов и использовать его для установления статуса сертификатов, созданных Удостоверяющим центром.

4.1.4. Получить копию сертификата на бумажном носителе, заверенную Удостоверяющим центром.

4.1.5. Обращаться в Удостоверяющий центр с заявлением на выполнение Удостоверяющим центром действий, предусмотренных настоящим Регламентом.

4.1.6. Обращаться в Удостоверяющий центр за подтверждением действительности электронных подписей, основанных на выданных Удостоверяющим центром сертификатах, в соответствии с порядком, определенным настоящим Регламентом.

4.1.7. Обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата, в течение срока действия сертификата.

4.2. **Обязанности Пользователя Удостоверяющего центра**

4.2.1. Принимать все возможные меры для предотвращения компрометации ключа электронной подписи, принадлежащего владельцу сертификата, а также меры по обеспечению конфиденциальности аутентификационных данных, используемых для доступа к Мобильному приложению.

4.2.2. Не использовать принадлежащий владельцу сертификата ключ электронной подписи в случае его компрометации.

4.2.3. Немедленно обращаться в Удостоверяющий центр с заявлением на прекращение действия сертификата в случаях компрометации ключа электронной подписи, принадлежащего владельцу сертификата или при компрометации аутентификационной информации Пользователя, используемой для доступа к Мобильному приложению.

4.2.4. Использовать для создания ключей электронных подписей и запросов на сертификат только входящие в состав Мобильного приложения средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом "Об электронной подписи".

4.2.5. Не использовать ключ электронной подписи, соответствующий ключу проверки электронной подписи, указанному в сертификате, который аннулирован, действие которого прекращено или заявление на прекращение действия которого подано в Удостоверяющий центр.

5. ОТВЕТСТВЕННОСТЬ

5.1. **Ответственность Удостоверяющего центра**

5.1.1. Удостоверяющий центр несет ответственность за неисполнение либо ненадлежащее исполнение своих обязанностей, установленных Федеральным законом «Об электронной подписи», а также настоящим Регламентом, за исключением случаев, предусмотренных пунктом 5.1.2 настоящего Регламента.

5.1.2. Удостоверяющий центр не несет ответственности за последствия, возникшие в результате нарушения Пользователем обязанностей, установленных настоящим Регламентом.

5.2. **Ответственность Пользователя**

5.2.1. Пользователь несет ответственность за достаточность принимаемых им мер по обеспечению безопасности использования электронной подписи и средств электронной подписи, включая защиту принадлежащего ему ключа электронной подписи и аутентификационных данных, используемых для доступа к Мобильному приложению, от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.

5.2.2. Пользователь несет ответственность за последствия, возникшие в результате использования им скомпрометированного ключа электронной подписи и соответствующего сертификата ключа поверки электронной подписи в целях создания электронной подписи.

6. ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

6.1. **Виды конфиденциальной информации**

6.1.1. Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего сертификата ключа проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключей электронных подписей Пользователей Удостоверяющего центра.

6.1.2. Конфиденциальной являются также следующая информация:

- аутентификационные данные, используемые для доступа к Мобильному приложению;
- персональные данные Пользователей, не подлежащие включению в состав сертификата.

6.2. **Виды информации, не относящейся к конфиденциальной**

6.2.1. Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

6.2.2. Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации определяется решением Удостоверяющего центра.

6.2.3. Информация, включаемая в создаваемые УЦ сертификаты и списки аннулированных сертификатов, не считается конфиденциальной.

6.2.4. Также не считается конфиденциальной информация о настоящем Регламенте.

6.3. Предоставление конфиденциальной информации

УЦ не должен раскрывать информацию, относящуюся к конфиденциальной информации, каким бы то ни было третьим лицам за исключением случаев:

- определенных в настоящем Регламенте;
- требующих раскрытия в соответствии с действующим законодательством РФ или при наличии судебного постановления.

7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

Обработка персональных данных Пользователей Удостоверяющего центра осуществляется в соответствии с Политикой в отношении обработки персональных данных в Акционерном обществе «ИнфоТеКС Интернет Траст», опубликованной на сайте iitrust.ru

8. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ

8.1. Регистрация Пользователя Удостоверяющего центра.

8.1.1. Под регистрацией Пользователя Удостоверяющего центра понимается внесение регистрационных данных Пользователя в информационную систему Удостоверяющего центра.

8.1.2. Регистрация Пользователя Удостоверяющего центра осуществляется на основании заявки на регистрацию в Удостоверяющем центре, содержащей регистрационные данные Пользователя, включая информацию, подлежащую внесению в сертификат, а именно:

- абонентский номер подвижной радиотелефонной связи;
- адрес электронной почты;
- реквизиты основного документа, удостоверяющего личность;
- страховой номер индивидуального лицевого счета;
- идентификационный номер налогоплательщика.

8.1.3. Заявка подается Пользователем в форме электронного документа с использованием информационно-телекоммуникационных технологий и может быть направлена, в том числе, через информационную систему, между которой и информационной системой Удостоверяющего центра организовано информационно-технологическое взаимодействие.

8.1.4. Обязательным условием регистрации Пользователя является наличие у него подтвержденной учетной записи в Единой системе идентификации и аутентификации.

8.2. Порядок создания ключа электронной подписи и ключа проверки электронной подписи.

8.2.1. Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Пользователем самостоятельно при помощи средства электронной подписи, входящего в состав Мобильного приложения, ссылку на скачивание которого с ресурсов производителей мобильных операционных систем iOS, Android или Huawei Пользователь получает в составе SMS-сообщения, направляемого на указанный Пользователем при регистрации абонентский номер подвижной радиотелефонной связи.

8.2.2. Созданный Пользователем ключ электронной подписи сохраняется в Мобильном приложении, а ключ проверки электронной подписи передается по каналу связи, защищенному с использованием шифровальных (криптографических) средств, в Удостоверяющий центр в составе запроса на сертификат, содержащего также следующие

данные для включения в состав сертификата: фамилия, имя, отчество (при наличии), страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика.

8.3. **Порядок проверки достоверности сведений, содержащихся в запросе на сертификат.**

Удостоверяющий центр с использованием Инфраструктуры осуществляет проверку достоверности сведений, содержащихся в запросе на сертификат:

- сведения о действительности паспорта гражданина РФ;
- сведения о достоверности идентификационного номера налогоплательщика;
- сведения о достоверности страхового номера индивидуального лицевого счета.

8.4. **Порядок создания и выдачи сертификата ключа проверки усиленной неквалифицированной электронной подписи.**

8.4.1. В случае положительного результата проверки достоверности сведений, содержащихся в запросе на сертификат, Удостоверяющий центр осуществляет передачу сведений о полученном заявлении на выдачу сертификата ключа проверки электронной подписи (запросе на сертификат) в информационную систему Единого портала государственных и муниципальных услуг (функций) с целью определения лица, подающего заявление в электронной форме без личного присутствия с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации.

8.4.2. Пользователь с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации, проходит процедуру авторизации в подсистеме личных кабинетов Единого портала государственных и муниципальных услуг (функций) и подтверждает подачу заявления на выдачу сертификата усиленной неквалифицированной электронной подписи.

8.4.3. В случае подтверждения Пользователем подачи им заявления на выдачу сертификата усиленной неквалифицированной электронной подписи Удостоверяющий центр создает сертификат ключа проверки электронной подписи Пользователя и передает его в Мобильное приложение, установленное на мобильном устройстве Пользователя.

8.4.4. Мобильное приложение отображает информацию, содержащуюся в созданном Удостоверяющим центром сертификате, и Пользователь подтверждает в Мобильном приложении ознакомление с этой информацией.

8.4.5. После подтверждения Пользователем ознакомления с информацией, содержащейся в сертификате, Пользователь получает возможность использования ключа электронной подписи и сертификата ключа проверки электронной подписи для подписания электронных документов своей усиленной неквалифицированной электронной подписью при помощи Мобильного приложения.

8.5. **Сроки действия ключа электронной подписи и сертификата ключа проверки усиленной неквалифицированной электронной подписи Пользователя.**

Сроки действия ключа электронной подписи и сертификата ключа проверки электронной подписи, выдаваемого Удостоверяющим центром, составляют 12 месяцев.

8.6. **Подтверждение действительности электронной подписи**

8.6.1. Подтверждение действительности электронной подписи в электронном документе осуществляется Удостоверяющим центром по обращению Пользователя на основании

заявления в простой письменной форме на подтверждение действительности электронной подписи в электронном документе.

8.6.2. Заявление на подтверждение действительности электронной подписи в электронном документе должно содержать информацию о дате и времени формирования электронной подписи в электронном документе.

8.6.3. Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является внешний носитель информации, содержащий электронный документ с электронной подписью в формате, утвержденном приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 14.09.2020 № 472.

8.6.4. Срок проведения работ по подтверждению действительности электронной подписи в электронном документе составляет 5 (пять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

8.6.5. В ходе проведения работ по подтверждению действительности электронной подписи в электронном документе Удостоверяющим центром может быть запрошена дополнительная информация.

8.6.6. Электронная подпись признается действительной при одновременном соблюдении следующих условий:

- Сертификат ключа проверки электронной подписи создан и выдан Удостоверяющим центром.
- Сертификат ключа проверки электронной подписи является действительным на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности проверяемого сертификата, если момент подписания электронного документа не определен.
- Имеется положительный результат проверки принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. При этом, проверка осуществляется с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», и с использованием сертификата ключа проверки электронной подписи лица, подписавшего электронный документ.

8.6.7. Результатом проведения работ по подтверждению действительности электронной подписи в электронном документе является ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника и печатью Удостоверяющего центра. Ответ должен содержать:

- результат проверки средством электронной подписи, имеющим подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», принадлежности электронной подписи в электронном документе владельцу сертификата и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- детальный отчет по выполненной проверке (экспертизе).

8.6.8. Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или экспертной комиссии, которым поручено проведение проверки (экспертизы);
- вопросы, поставленные перед экспертом или экспертной комиссией;

- объекты исследований и материалы по заявлению, представленные для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения.

8.6.9. Материалы и документы, иллюстрирующие заключение эксперта или экспертной комиссии, прилагаются к детальному отчету и являются его составной частью.

8.6.10. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами экспертной комиссии.

8.7. **Порядок прекращения действия или аннулирования сертификата ключа проверки электронной подписи**

8.7.1. Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, или настоящим Регламентом.

8.7.2. Удостоверяющий центр аннулирует сертификат ключа проверки электронной подписи в следующих случаях:

- не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи;
- в связи с вступлением в силу решения суда, которым, в частности, установлено, что сертификат содержит недостоверную информацию.

8.7.3. Порядок подачи заявления на прекращение действия сертификата.

8.7.3.1 Заявление на прекращение действия сертификата может быть подано как в форме документа на бумажном носителе, так и в форме электронного документа.

8.7.3.2 Заявление на прекращение действия сертификата, подаваемое в форме документа на бумажном носителе, должно быть подписано собственноручной подписью лица, указанного в качестве владельца сертификата.

8.7.3.3 Заявление на прекращение действия сертификата ключа проверки усиленной неквалифицированной электронной подписи, подаваемое в форме электронного документа, должно быть подписано усиленной неквалифицированной или квалифицированной электронной подписью владельца сертификата.

8.7.4. Порядок внесения информации о прекращении действия или аннулировании сертификата в реестр сертификатов:

8.7.4.1 Внесение информации о прекращении действия или аннулировании сертификата в реестр сертификатов осуществляется путем внесения соответствующей информации в список аннулированных сертификатов.

8.7.4.2 Удостоверяющий центр вносит информацию о прекращении действия или аннулировании сертификата в реестр сертификатов в срок, не превышающий двенадцать часов с момента наступления обстоятельств, указанных в пунктах 3.2.8 и 3.2.9 настоящего Регламента или в течение двенадцати часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

8.7.4.3 До внесения в реестр сертификатов информации об аннулировании сертификата Удостоверяющий центр уведомляет владельца сертификата об аннулировании его сертификата путем направления уведомления в форме бумажного или электронного документа.

8.7.4.4 Удостоверяющий центр обязан официально уведомить о факте аннулирования или прекращения действия сертификата всех участников информационного взаимодействия.

8.7.4.5 Официальным уведомлением о факте аннулирования или прекращения действия сертификата является опубликование списка аннулированных сертификатов, содержащего сведения о сертификате, который был аннулирован или действие которого было досрочно прекращено.

8.7.4.6 Временем опубликования списка аннулированных сертификатов признается включенное в список аннулированных сертификатов время его создания.

8.7.4.7 Датой и временем аннулирования или прекращения действия сертификата признается дата и время внесения информации о сертификате, который был аннулирован или действие которого было досрочно прекращено, в список аннулированных сертификатов.

8.8. **Порядок ведения и предоставления доступа к реестру сертификатов.**

8.8.1. Реестр сертификатов ведется Удостоверяющим центром в электронной форме и кроме информации, содержащейся в сертификатах, включает также информацию о датах прекращения действия или аннулирования сертификатов и об основаниях прекращения действия или аннулирования.

8.8.2. Информация о созданном сертификате ключа проверки электронной подписи вносится Удостоверяющим центром в реестр сертификатов не позднее указанной в нем даты начала действия такого сертификата.

8.8.3. Удостоверяющий центр вносит информацию о сертификате, который был аннулирован или действие которого было досрочно прекращено, в реестр сертификатов в течение двенадцати часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия сертификата или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

8.8.4. Информация, содержащаяся в реестре сертификатов Удостоверяющего центра, предоставляется любому лицу по его запросу, направляемому в Удостоверяющий центр по электронной почте либо через сайт Удостоверяющего центра. Запрос должен содержать реквизиты сертификата, информация о котором запрашивается, в объеме, необходимом и достаточном для осуществления поиска в реестре сертификатов:

- фамилия, имя, отчество;
- страховой номер индивидуального лицевого счета.

8.8.5. Удостоверяющий центр предоставляет информацию, содержащуюся в реестре сертификатов, в течении 8 (восьми) рабочих часов с момента получения соответствующего запроса.

9. ПОРЯДОК ИСПОЛНЕНИЯ ОБЯЗАННОСТЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

9.1. **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 и их проверки**

Удостоверяющий центр осуществляет 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 и их проверки, путем размещения соответствующей информации в Приложении 2 к настоящему Регламенту.

9.2. **Выдача по обращению Заявителя средств электронной подписи**

Выдача Заявителям средств электронной подписи осуществляется путем распространения Мобильного приложения, реализующего функции средств электронной подписи, через ресурсы производителей мобильных операционных систем iOS, Android или Huawei.

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

9.3.1. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем выполнения Удостоверяющим центром порядка ведения реестра сертификатов, изложенного в разделе 8.8 настоящего Регламента, а также защиты указанной информации от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

9.3.2. Защита информации, содержащейся в реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается комплексом организационно-технических мероприятий, осуществляемых Удостоверяющим центром в соответствии с требованиями, установленными эксплуатационной документацией на средства удостоверяющего центра, а также требованиями, установленными в области технической защиты информации.

9.4. **Предоставление доступа к информации, содержащейся в реестре сертификатов**

Доступ к информации, содержащейся в реестре сертификатов, включая информацию о прекращении действия или аннулировании сертификата, предоставляется безвозмездно любому лицу в соответствии с порядком, указанным в пункте 8.8 настоящего Регламента.

10. МЕХАНИЗМ ДОКАЗАТЕЛЬСТВА ВЛАДЕНИЯ КЛЮЧОМ ЭЛЕКТРОННОЙ ПОДПИСИ

Подтверждение владения ключом электронной подписи осуществляется путем определения лица, подающего заявление на выдачу сертификата без личного присутствия с использованием простой электронной подписи, ключ которой получен при личной явке в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации.

11. СОДЕРЖАНИЕ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ УСИЛЕННОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

Удостоверяющий центр создает и выдает сертификаты ключей проверки усиленных неквалифицированных электронных подписей, содержащих серийный номер сертификата, даты начала и окончания срока действия, идентификатор алгоритма и значение ключа проверки электронной подписи, а также следующую информацию в поле «Субъект»

сертификата: фамилия, имя, отчество (если имеется), страховой номер индивидуального лицевого счета, идентификационный номер налогоплательщика.

12. СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ СЕРТИФИКАТОВ

УЦ формирует списки аннулированных сертификатов в соответствии с рекомендациями IETF RFC 5280 (2008) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

13. УЧЕТНО-ОТЧЕТНОЕ ВРЕМЯ

В соответствии с Федеральным законом от 18.06.2003 № 126-ФЗ «О связи» при оказании услуг Удостоверяющего центра применяется единое учетно-отчетное время – московское.

14. ПРИЛОЖЕНИЯ

Приложение 1. Форма Заявления на прекращение действия сертификата ключа проверки электронной подписи, выданного физическому лицу.

Приложение 2. Информация об условиях и 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 1
к Регламенту предоставления Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей

В Удостоверяющий Центр
Акционерного общества «ИнфоТеКС Интернет Траст»

Заявление
на прекращение действия сертификата ключа проверки электронной подписи, выданного физическому лицу

Прошу прекратить действие выданного Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» сертификата ключа проверки электронной подписи со следующими реквизитами:

Серийный номер сертификата: _____

Фамилия, имя, отчество владельца сертификата (полностью): _____

_____

СНИЛС: _____

в связи с _____
(причина прекращения действия сертификата)

_____

_____

Подпись и расшифровка подписи физического лица, указанного в качестве владельца сертификата:

_____ _____
(подпись) (фамилия, инициалы)

«___» _____ 20___ г.

Приложение 2
к Регламенту предоставления Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей

Информация
об условиях и 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

1. Риски, связанные с использованием электронной подписи.

К основным рискам, связанным с использованием электронной подписи, относятся:

1.1. Несанкционированное подписание электронного документа электронной подписью, которое может быть произведено в результате:

- компрометации ключа электронной подписи;
- подмены подписываемого документа в результате работы вредоносного программного обеспечения.

1.2. Негативные последствия, вызванные невозможностью подписания электронного документа электронной подписью, обусловленной следующими событиями:

- уничтожение ключа и (или) сертификата ключа проверки электронной подписи;
- неисправность мобильного устройства, на котором установлено Мобильное приложение;
- блокировка мобильного устройства или блокировка доступа к Мобильному приложению»;
- физическая утрата мобильного устройства, на котором установлено Мобильное приложение.

2. Порядок получения средств электронной подписи.

Получение средств электронной подписи осуществляется путем скачивания Мобильного приложения, реализующего функции средств электронной подписи, с ресурсов производителей мобильных операционных систем iOS, Android или Huawei.

3. Действия при компрометации ключей электронной подписи.

3.1. Владелец сертификата ключа проверки электронной подписи самостоятельно должен определить факт компрометации ключа электронной подписи, оценить значение этого события и выполнить мероприятия по локализации последствий компрометации ключа электронной подписи.

3.2. При компрометации ключа электронной подписи владелец сертификата должен немедленно обратиться в Удостоверяющий центр с заявлением на прекращение действия сертификата ключа проверки электронной подписи одним из способов, определенных Регламентом предоставления Удостоверяющим центром Акционерного общества «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки усиленных неквалифицированных электронных подписей.