

УТВЕРЖДЕН

приказом ГКУ ТО «ЦИТТО»
от 23.04.2021 № 24/сог

**ПОРЯДОК РЕАЛИЗАЦИИ ФУНКЦИЙ
АККРЕДИТОВАННОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
ГКУ ТО «ЦИТТО» И ИСПОЛНЕНИЯ ЕГО
ОБЯЗАННОСТЕЙ**

город Тюмень, 2021г.

Содержание

1. Введение.....	5
2. Общие положения.....	9
2.1. Предмет регулирования Порядка.....	9
2.2. Сведения об Удостоверяющем центре.....	12
2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра.....	13
3. Перечень функций (оказываемых услуг), реализуемых Удостоверяющим центром.....	14
3.1. Пользователи услуг.....	14
4. Права и обязанности Удостоверяющего центра.....	15
4.1. Права Удостоверяющего центра.....	15
4.2. Обязанности Удостоверяющего центра:.....	17
5. Права и обязанности Стороны, присоединившейся к Порядку.....	20
5.1. Права Стороны, присоединившейся к Порядку, права Пользователя УЦ.....	20
5.2. Обязанности Стороны, присоединившейся к Порядку, обязанности Пользователя УЦ.....	22
6. Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром.....	24
6.1. Процедура создания ключей электронных подписей и ключей проверки электронных подписей.....	24
6.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра.....	28
6.3. Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности.....	30
6.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Пользователя УЦ.....	32
6.5. Процедура создания и выдачи квалифицированных сертификатов.....	35
6.6. Подтверждение действительности электронной подписи, использованной для подписания электронного документа.....	44
6.7. Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата.....	47
6.8. Порядок ведения реестра сертификатов Удостоверяющего центра.....	53
6.9. Порядок технического обслуживания реестра квалифицированных сертификатов.....	58
7. Порядок исполнения обязанностей Удостоверяющего центра.....	59
7.1. 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.....	59
7.2. Выдача по обращению заявителя средств электронной подписи.....	60
7.3. Обеспечение актуальности информации, содержащейся в реестре сертификатов, а также ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.....	61
7.4. Обеспечение доступности реестра квалифицированных сертификатов в информационно-телекоммуникационной сети «Интернет».....	62

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.....	63
7.6. Осуществление регистрации квалифицированного сертификата в единой системе идентификации и аутентификации.....	65
7.7. Осуществление по желанию лица, которому выдан квалифицированный сертификат, безвозмездной регистрации указанного лица в единой системе идентификации и аутентификации.....	66
7.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре сертификатов.....	67
7.9. Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени.....	67
8. Прочие положения.....	68
8.1. Прекращение деятельности Удостоверяющего центра.....	68
8.2. Политика конфиденциальности.....	69
9. Сроки действия ключевой информации.....	71
9.1 Срок действия ключевой информации Удостоверяющего центра.....	71
9.2 Сроки действия ключевой информации Пользователя УЦ.....	72
9.3 Программный комплекс обеспечения реализации целевых функций.....	72
10. Ролевое разграничение доступа.....	73
11. Перечень событий, регистрируемых программным обеспечением.....	74
12. Перечень данных, подлежащих резервному копированию.....	75
13. Инженерно-технические меры защиты информации.....	75
14. Программно-аппаратные меры защиты информации.....	76
15. Организационные меры защиты информации.....	78
16. Архивное хранение документированной информации.....	79
17. Восстановление после аварий.....	80
Приложение №1.....	81
Приложение №2.....	82
Приложение №3.....	83
Приложение №4.....	86
Приложение №5.....	89
Приложение №5а.....	90
Приложение №6.....	91
Приложение №6а.....	92
Приложение №7.....	93
Приложение №8.....	95
Приложение №9.....	97
Приложение №10.....	98
Приложение №11.....	99
Приложение №12.....	100
Приложение №13.....	101
Приложение №14.....	102
Приложение №15.....	103
Приложение №16.....	104
Приложение №17.....	105

Приложение №18.....	106
Приложение №19.....	107
Приложение №20.....	108

1. Введение

1.1. Порядок реализации функций аккредитованного удостоверяющего центра ГКУ ТО «Центр информационных технологий Тюменской области» и исполнения его обязанностей (далее соответственно также – Порядок, Удостоверяющий центр) определяет условия предоставления услуг Удостоверяющего центра, включая права, обязанности и ответственность Удостоверяющего центра, а также права, обязанности и ответственность лиц, присоединившихся к Порядку.

1.2. Настоящий Порядок разработан в соответствии с:

Федеральным законом «Об электронной подписи»;

Федеральным законом «Об информации, информационных технологиях и о защите информации»;

Федеральным законом «О персональных данных»;

Федеральным законом «О связи»;

Федеральным законом «Об организации предоставления государственных и муниципальных услуг»;

Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79;

Требованиями к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796;

Требованиями к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 795;

Требованиями к Порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, утвержденными приказом Минкомсвязи России от 13 августа 2018 г. № 397;

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 Минкомсвязи России от 14 августа 2017 г. № 416;

Порядком формирования и ведения реестров выданных аккредитованными удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22 августа 2017 г. № 436;

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 по правительству связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 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 февраля 2005 г. № 66;

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

1.3. Перечень сокращений.

АРМ	Автоматизированное рабочее место
ГКУ ТО «ЦИТТО»	Государственное казенное учреждение Тюменской области «Центр информационных технологий Тюменской области»
СКЗИ	Средство криптографической защиты информации
СОС	Список отзываемых сертификатов
УЦ	Удостоверяющий центр
ЦОД	Центр обработки данных (серверное помещение)
ЦС	Центр Сертификации
ЦР	Центр Регистрации
СКПЭП	Сертификат ключа проверки электронной подписи
ЭП	Электронная подпись
КЭП	Квалифицированная электронная подпись

1.4. Термины и определения.

Удостоверяющий центр – Государственное казенное учреждение Тюменской области «Центр информационных технологий Тюменской области», осуществляющее на основании распоряжения Правительства Тюменской области от 17.01.2011 № 21-рп «Об организации Удостоверяющего центра Тюменской области» выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон № 63-ФЗ).

Уполномоченное лицо удостоверяющего центра – физическое лицо, являющееся

сотрудником Удостоверяющего центра и наделенное полномочиями по заверению от имени Удостоверяющего центра сертификатов ключей проверки электронной подписи.

Оператор удостоверяющего центра, Оператор центра регистрации – сотрудник Удостоверяющего центра либо организации, заключившей договор с Удостоверяющим центром, осуществляющий прием заявлений и вручение сертификатов ключей проверки электронной подписи согласно настоящему Порядку.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись (ЭП) – 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.

Квалифицированная электронная подпись (КЭП) – электронная подпись, соответствующая следующим признакам:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи и средств (средства) электронной подписи, получивших (получившего) подтверждение соответствия требованиям, установленным Федеральным законом № 63-ФЗ;
- позволяет определить лицо, подпишавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
- ключ проверки электронной подписи указан в квалифицированном сертификате ключа проверки электронной подписи.

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.

Сертификат ключа проверки электронной подписи (СКПЭП) – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо уполномоченным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи. СКПЭП считается действующим на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия СКПЭП;
- срок действия СКПЭП не истек;
- СКПЭП не аннулирован (не отозван) и действие его не приостановлено.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный СКПЭП) – сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом № 63-ФЗ и иными принимаемыми в соответствии с ним нормативными правовыми актами, и

созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

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.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном настоящим Порядком порядке выдан сертификат ключа проверки электронной подписи.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 9.00 до 13.00 и с 14.00 до 17.00 (время Тюменское) каждого дня недели за исключением выходных и праздничных дней.

Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию, а при необходимости - контрольную, служебную и технологическую информацию.

Ключевая информация – ключи электронной подписи и ключи проверки электронной подписи, предназначенные для формирования/проверки электронной подписи и шифрования/расшифрования информации, действующие в течение определенного срока.

Список отозванных сертификатов (СОС) – электронный документ с электронной подписью Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей проверки электронных подписей, которые на определенный момент времени были аннулированы или действие которых было приостановлено.

Public Key Cryptography Standards (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений.

Подтверждение подлинности электронной подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанным данной электронной подписью электронном документе.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физические лица – представители органов власти Тюменской области или органов местного самоуправления Тюменской области, а также подведомственных им организаций и учреждений, зарегистрированные в УЦ ГКУ ТО «ЦИТТО», и являющиеся владельцами сертификата ключа проверки электронной подписи.

Центр регистрации (ЦР) – подразделение Удостоверяющего центра либо организации, заключившей договор с Удостоверяющим центром, осуществляющее прием заявлений и вручение сертификатов ключей проверки электронной подписи согласно настоящему Порядку.

Иные понятия и термины, используемые в настоящем Порядке, применяются в значениях, определенных федеральными законами «Об электронной подписи», «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О связи», «Об организации предоставления государственных и муниципальных услуг» и принимаемыми в соответствии с ними нормативными правовыми актами.

2. Общие положения.

2.1. Предмет регулирования Порядка.

2.1.1. Предметом регулирования Порядка являются отношения в области использования электронных подписей, возникающие между Удостоверяющим центром и участниками электронного взаимодействия при оказании услуг Удостоверяющего центра, реализации его функций и исполнении обязанностей.

2.1.2. Настоящий Порядок является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

2.1.3. Сторонами настоящего Порядка является Удостоверяющий центр и лица, присоединившиеся к Порядку.

2.1.4. Настоящий Порядок является средством официального уведомления и информирования всех Сторон во взаимоотношениях, возникающих в процессе предоставления и использования услуг Удостоверяющего центра.

2.1.5. Публикация и распространение настоящего Порядка.

Настоящий Порядок распространяется: в форме электронного документа

- на сайте Удостоверяющего центра по адресу <http://ca.72to.ru>
- через E-mail от отправителя citto-ca@72to.ru
- в бумажной форме предоставляется лицу, присоединившемуся к Порядку, по его требованию.

2.1.6. Присоединение к настоящему Порядку.

2.1.6.1. Присоединение к настоящему Порядку осуществляется путем предоставления в Удостоверяющий центр заявления о присоединении к Порядку по форме приложения № 1 или приложения № 2 к настоящему Порядку.

2.1.6.2. С момента регистрации заявления о присоединении к Порядку в Удостоверяющем центре заявитель считается Стороной, присоединившийся к Порядку.

2.1.6.3. Удостоверяющий центр вправе отказать любому лицу в приеме и регистрации заявления о присоединении к Порядку в случае ненадлежащего оформления заявителем документов, необходимых для оказания услуг, предоставления неактуальных документов или сведений, предоставления их не в полном объеме или предоставления заявителем не достоверных сведений.

2.1.6.4. Факт присоединения заявителя к Порядку является полным принятием им условий настоящего Порядка и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении Порядку в Удостоверяющем центре.

Сторона, присоединившаяся к Порядку, принимает дальнейшие изменения (дополнения), вносимые в Порядок, в соответствии с условиями настоящего Порядка.

2.1.6.5. После присоединения к Порядку Удостоверяющий центр и Сторона, присоединившаяся к Порядку, вступают в соответствующие договорные отношения.

2.1.6.6. Срок действия Порядка.

Настоящий Порядок вступает в силу со дня его публикации на сайте по адресу — <http://ca.72to.ru>.

Срок действия Порядка 9 лет.

Если Удостоверяющий центр официально не уведомит своих пользователей о прекращении действия Порядка, Порядок автоматически пролонгируется на следующие 3 года.

Прекращение действия Порядка не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Порядка, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

2.1.7. Порядок прекращения присоединения к настоящему Порядку.

2.1.7.1. Действие настоящего Порядка может быть прекращено по инициативе одной из Сторон в следующих случаях:

- волеизъявления одной из Сторон;
- нарушения одной из Сторон условий настоящего Порядка.

2.1.7.2. В случае, если договорные отношения, определенные настоящим Порядком, прекращаются по инициативе одной из Сторон, Сторона, принявшая решение о прекращении договорных отношений письменно уведомляет другую Сторону о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка. Договорные отношения в соответствии с настоящим Порядком считаются расторгнутым после выполнения Сторонами своих обязанностей.

2.1.7.3. Прекращение действия договорных отношений, определенных настоящим Порядком, не освобождает Стороны от исполнения обязательств, возникших до указанного дня их прекращения и не освобождает от ответственности за их неисполнение (ненадлежащее исполнение).

2.1.8. Внесение изменений и дополнений в Порядок.

2.1.8.1. Внесение изменений и дополнений в настоящий Порядок, включая внесение изменений и дополнений в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

2.1.8.2. Уведомление о внесении изменений, дополнений в Порядок осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений, дополнений на сайте по адресу — <http://ca.72to.ru> (далее также – сайт Удостоверяющего центра) новой версии Порядка, утвержденного приказом ГКУ ТО «Центр информационных технологий Тюменской области» включающего внесенные изменения и дополнения.

2.1.8.3. Все изменения и дополнения, вносимые Удостоверяющим центром в настоящий Порядок, не связанные с изменением действующего законодательства

Российской Федерации, вступают в силу и становятся обязательными по истечении одного месяца с даты размещения новой версии Порядка, опубликованного на сайте Удостоверяющего центра.

2.1.8.4. Все изменения, вносимые Удостоверяющим центром в Порядок в связи с изменениями, которые вносятся в нормативные правовые акты, регулирующие отношения в области использования электронных подписей, вступают в силу одновременно с вступлением в силу вышеуказанных изменений.

2.1.8.5. Любые изменения в Порядке с момента вступления в силу новой версии Порядка распространяются на всех лиц, присоединившихся к Порядку, в том числе присоединившихся к Порядку ранее даты вступления новой версии Порядка в силу. В случае несогласия с вышеуказанными изменениями Сторона, присоединившаяся к Порядку до вступления в силу таких изменений, имеет право прекратить договорные отношения и расторгнуть настоящий Порядок, письменно уведомив Удостоверяющий центр о своих намерениях за 1 (один) месяц до даты расторжения настоящего Порядка.

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

2.1.9. Применение Порядка.

2.1.9.1. Стороны понимают понятия и термины, применяемые в настоящем Порядке, строго в контексте общего смысла Порядка.

2.1.9.2. В случае противоречия и (или) расхождения названия какого-либо раздела Порядка со смыслом какого-либо пункта в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

2.1.9.3. В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Порядку с положениями собственно Порядка, Стороны считают доминирующим смысл и формулировки Порядка.

2.1.10. Ответственность Сторон.

2.1.10.1. Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Порядку, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях пользователя УЦ и предоставленных документах.

2.1.10.2. Удостоверяющий центр не несет ответственности за последствия и убытки при несоблюдении пользователем УЦ действующего законодательства и положений настоящего Порядка.

2.1.10.3. Удостоверяющий центр не несет ответственность за невозможность использования в информационной системе электронной подписи, основанной на квалифицированном сертификате, выданном Удостоверяющим центром, в случае предъявления оператором данной информационной системы требований к квалифицированному сертификату и его форме, требований аккредитованному удостоверяющему центру и иных требований, в том числе к условиям признания электронных документов, подписанных электронной подписью и условиям признания электронной подписи, если указанные требования, установленные оператором

информационной системы, не соответствуют требованиям, установленными Федеральным законом «Об электронной подписи» иными федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, в том числе Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 795.

2.1.10.4. Удостоверяющий центр несет ответственность перед Пользователями УЦ за причиненный ущерб связанный с использованием сертификатов ключей проверки электронной подписи Пользователей УЦ, в случае если данный ущерб нанесен Удостоверяющим центром вследствие нарушения действующего законодательства и (или) положений настоящего Порядка, выявленного в установленном законодательством порядке.

2.1.10.5. Стороны несут ответственность за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, соглашением Сторон, в том числе настоящим Порядком.

2.1.10.6. Ответственность Сторон, не урегулированная положениями настоящего Порядка, регулируется законодательством Российской Федерации.

2.1.11. Разрешение споров.

2.1.11.1. Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Сторона, присоединившаяся к настоящему Порядку.

2.1.11.2. При рассмотрении спорных вопросов, связанных с настоящим Порядком, Стороны будут руководствоваться действующим законодательством Российской Федерации.

2.1.11.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.

2.1.11.4. Сторона, получившая от другой Стороны претензию, обязана в течение 15 (пятнадцати) рабочих дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа.

2.1.11.5. Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, решаются в Арбитражном суде Тюменской области.

2.2. Сведения об Удостоверяющем центре.

2.2.1. Государственное казенное учреждение Тюменской области «Центр информационных технологий Тюменской области» (далее - ГКУ ТО «ЦИТТО») зарегистрировано на территории Российской Федерации в городе Тюмени. Свидетельство о государственной регистрации юридического лица за основным государственным регистрационным номером 1087232038794, выдано 24.09.2008 Межрайонной инспекцией Федеральной налоговой службы №14 по Тюменской области. УЦ ГКУ ТО «ЦИТТО» осуществляет свою деятельность по созданию и выдаче сертификатов ключей проверки электронной подписи на территории Российской Федерации на основании следующих документов:

- Свидетельство об аккредитации удостоверяющего центра, рег.№ 925 от 04 июля 2018 года;
- Лицензия РУ ФСБ РФ по Тюменской области ЛСЗ № 0010882 рег.№ 319 от 04 февраля 2016 года на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

2.2.2. Реквизиты Удостоверяющего центра.

Полное наименование юридического лица: Удостоверяющий центр государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области»

Юридический адрес: 625000, Российская Федерация, Тюменская область, город Тюмень, улица Советская, д.61

Почтовый адрес: 625000, Российская Федерация, Тюменская область, город Тюмень, улица Советская, д.61

Контактный телефон: (3452) 54-30-40, (3452) 54-30-47

Факс: (3452) 55-62-17

E-mail: citto-ca@72to.ru

2.2.3. Информация о месте нахождения и графике работы Удостоверяющего центра.

Место нахождение и почтовый адрес: 625000, Российская Федерация, Тюменская область, город Тюмень, улица Советская, д.61.

Адрес оказания услуг: Удостоверяющего центра: 625000, Российская Федерация, Тюменская область, город Тюмень, улица Советская, д.61.

График работы Удостоверяющего центра: ежедневно с 09:00 до 13:00 и с 14:00 до 17:00 (Тюменское время) за исключением выходных и праздничных дней.

2.3. Порядок информирования о предоставлении услуг Удостоверяющего центра.

2.3.1. Контактные телефоны Удостоверяющего центра: (83452) 54-30-40, 54-30-47.

2.3.2. Адреса электронной почты: citto-ca@72to.ru

2.3.3. Адрес сайта Удостоверяющего центра в информационно-телекоммуникационной сети «Интернет»: <http://ca.72to.ru>

2.3.4. Порядок получения информации заявителями по вопросам предоставления услуг Удостоверяющего центра.

Пользователи УЦ могут получить информацию по вопросам предоставления услуг Удостоверяющего центра с использованием следующих способов:

- ознакомиться с информацией, опубликованной на сайте Удостоверяющего центра;
- обратиться в Удостоверяющий центр за получением информации по справочным телефонам (83452) 54-30-40, 54-30-47.

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

Удостоверяющий центр предназначен для предоставления следующих услуг:

- внесение в реестр УЦ регистрационной информации о пользователях УЦ;
- создание сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме и выдача таких сертификатов лицам, обратившимся за их получением (заявителям);
- установление сроков действия сертификатов ключей проверки электронных подписей;
- выдача по обращению заявителя средств электронной подписи, содержащих ключ электронной подписи и ключ проверки электронной подписи;
- создание ключей электронной подписи и ключей проверки электронной подписи по обращениям пользователей УЦ с записью их на ключевой носитель (Перечень ключевых носителей, на которые производится запись ключей электронной подписи и ключей проверки электронной подписи определен в Приложении №23);
- ведение реестра выданных и аннулированных сертификатов ключей проверки электронной подписи пользователей УЦ, в том числе включающего в себя информацию, содержащуюся в выданных 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.

3.1. Пользователи услуг.

Проходить регистрацию в Удостоверяющем центре могут физические лица — представители органов власти Тюменской области или органов местного самоуправления Тюменской области, а также подведомственных им организаций и учреждений.

Владельцем сертификата ключа проверки электронной подписи может быть только физическое лицо, присоединившееся к Порядку и зарегистрированное в Удостоверяющем центре, в случае присоединения к Порядку УЦ органов власти Тюменской области или органов местного самоуправления Тюменской области, а также подведомственных им организаций и учреждений — физическое лицо, являющееся уполномоченным представителем указанных учреждений.

В случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата ключа проверки электронной подписи наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности. Допускается не указывать в качестве владельца сертификата ключа проверки электронной подписи физическое лицо, действующее от имени юридического лица, в сертификате ключа проверки электронной подписи (в том числе в квалифицированном сертификате), используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами. Владельцем такого сертификата ключа проверки электронной подписи признается юридическое лицо, информация о котором содержится в таком сертификате. При этом распорядительным актом юридического лица определяется физическое лицо, ответственное за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами. В случае отсутствия указанного распорядительного акта лицом, ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, является руководитель юридического лица. В случае возложения федеральным законом полномочий по исполнению государственных функций на конкретное должностное лицо ответственным за автоматическое создание и (или) автоматическую проверку электронной подписи в информационной системе при исполнении государственных функций является это должностное лицо.

4. Права и обязанности Удостоверяющего центра.

4.1. Права Удостоверяющего центра.

Удостоверяющий центр имеет право:

- Запрашивать у заявителя документы, необходимые для установления личности получателя квалифицированного сертификата (заявителя) либо документы, подтверждающие полномочия лица, выступающего от имени заявителя.
- Запрашивать у заявителя документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата.
- Отказать заявителю в выдаче квалифицированного сертификата в следующих случаях:
 - 1) не предоставлены документы либо их надлежащим образом заверенные копии

и сведения, необходимые для создания и выдачи квалифицированного сертификата;

2) документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания квалифицированного сертификата, представлены не в полном объеме или они ненадлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается;

3) не установлена личность заявителя – физического лица, обратившегося за получением квалифицированного сертификата;

4) не получено подтверждение правомочий лица, выступающего от имени заявителя – юридического лица, обращаться за получением квалифицированного сертификата.

- Не проводить регистрацию лиц, обратившихся по вопросу представления копий сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре Удостоверяющего центра.
- Устанавливать сроки действия выдаваемых квалифицированных сертификатов.
- Выдавать сертификаты ключей проверки электронных подписей как в форме электронных документов, так и в форме документов на бумажном носителе.
- Наделить третьих лиц (далее - доверенные лица) полномочиями по приему заявлений на выдачу сертификатов ключей проверки электронной подписи, а также вручению сертификатов ключей проверки электронных подписей от имени этого удостоверяющего центра. При совершении порученных удостоверяющим центром действий доверенное лицо обязано идентифицировать заявителя при его личном присутствии.
- Отказать в предоставлении услуг по регистрации пользователей УЦ лицам, подавшим заявление на регистрацию, без предоставления информации о причинах отказа.
- Отказать в создании ключей лицам, не зарегистрированным в Удостоверяющем центре, подавшим заявление на создание ключей, без предоставления информации о причинах отказа.
- Отказать в создании сертификата ключа проверки электронной подписи зарегистрированным пользователям УЦ, подавшим заявление на создание сертификата ключа проверки электронной подписи, с указанием причин отказа.
- Отказать заявителю в выдаче квалифицированного сертификата в случае, если полученные в соответствии с частью 2.2 статьи 18 Федерального закона №63-фз «Об электронной подписи» сведения не подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, а также в случаях, установленных пунктами 5 и 6 части 2 статьи 13 Федерального закона №63-фз «Об электронной подписи».
- Отказать в аннулировании (отзыва) сертификата ключа проверки электронной подписи пользователю УЦ, подавшему заявление на прекращение действия (аннулирование) сертификата, в случае если истек установленный срок действия

ключа электронной подписи, соответствующего данному сертификату ключа проверки электронной подписи.

- Отказать в приостановлении или возобновлении действия сертификата ключа проверки электронной подписи пользователю УЦ, подавшему заявление на приостановление или возобновление действия сертификата, в случае если истек установленный срок действия ключа электронной подписи, соответствующего данному сертификату ключа проверки электронной подписи.
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи пользователя УЦ в случае, если не подтверждено, что владелец сертификата ключа проверки электронной подписи владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате.
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи пользователя УЦ в случае, если установлено, что содержащийся в таком сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном сертификате ключа проверки электронной подписи.
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи пользователя УЦ в случае, если вступило в силу решение суда, которым, в частности, установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи пользователя УЦ в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием обоснованных причин.
- В одностороннем порядке прекратить действие квалифицированного сертификата, выданного Удостоверяющим центром, с направлением соответствующего уведомления его владельцу не позднее, чем за один рабочий день до прекращения действия квалифицированного сертификата, в случае невыполнения владельцем квалифицированного сертификата обязанностей, установленных Федеральным законом №63-фз «Об электронной подписи», иными принимаемыми в соответствии с ним нормативными правовыми актами, настоящим Порядком.
- Приостановить действие сертификата ключа проверки электронной подписи пользователя УЦ, с уведомлением владельца приостановленного сертификата ключа проверки электронной подписи и указанием обоснованных причин.
- В одностороннем порядке вносить изменения и дополнения в Порядок в соответствии с пунктом 2.1.8 настоящего Порядка.

4.2. Обязанности Удостоверяющего центра:

- Использовать в своей работе, в том числе для создания сертификатов ключей проверки электронной подписи Пользователей УЦ и формирования электронной

подписи только сертифицированные средства криптографической защиты информации.

- Использовать для подписания квалифицированных сертификатов от своего имени квалифицированную электронную подпись, основанную на квалифицированном сертификате, выданном ему головным удостоверяющим центром, функции которого осуществляют уполномоченный федеральный орган.
- Использовать ключ электронной подписи уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов.
- При выдаче квалифицированного сертификата идентифицировать заявителя - физическое лицо, обратившееся за получением квалифицированного сертификата.
- При выдаче квалифицированного сертификата получить от лица, выступающего от имени заявителя - юридического лица, подтверждение правомочия обращаться за получением квалифицированного сертификата.
- Осуществлять с использованием инфраструктуры проверку достоверности документов и сведений, представленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона №63-фз «Об электронной подписи».
- Для внесения в квалифицированный сертификат информации запрашивать и получать из государственных информационных ресурсов выписку из единого государственного реестра юридических лиц в отношении заявителя - юридического лица.
- Предоставить Пользователю УЦ, обратившемуся за его получением, сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра в электронной форме.
- Принять меры по защите ключа электронной подписи уполномоченного лица Удостоверяющего центра от несанкционированного доступа.
- Осуществлять регистрацию Пользователей УЦ в соответствии с порядком, определенным в настоящем Порядке.
- Обеспечить создание сертификата ключа проверки электронной подписи зарегистрированного в Удостоверяющем центре Пользователя УЦ по заявлению на создание сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Порядке.
- Обеспечить уникальность серийных номеров создаваемых сертификатов ключей проверки электронной подписи.
- Обеспечить уникальность значений ключей проверки электронной подписи в созданных сертификатах ключей проверки электронной подписи Пользователей УЦ.
- Обеспечить конфиденциальность созданных удостоверяющим центром ключей электронных подписей.
- 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.

- Одновременно с выдачей квалифицированного сертификата предоставляет владельцу квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.
- Ознакомить владельца квалифицированного сертификата под расписку с информацией, содержащейся в полученном квалифицированном сертификате.
- При выдаче квалифицированного сертификата направляет в единую систему идентификации и аутентификации сведения о выданном квалифицированном сертификате.
- 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.
- 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.
- Осуществлять проверку электронных подписей,ключи проверки которых указаны в выданных доверенными лицами сертификатах ключей проверки электронных подписей.
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Порядке.
- Приостановить действие сертификата ключа проверки электронной подписи Пользователя УЦ по заявлению на приостановление действия сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Порядке.
- Возобновить действие сертификата ключа проверки электронной подписи Пользователя УЦ по заявлению на возобновление действия сертификата ключа проверки электронной подписи (исключительно в случае поступления заявления в период течения срока, на который действие сертификата было приостановлено), в соответствии с порядком, определенным в настоящем Порядке.
- Уведомить владельца сертификата ключа проверки электронной подписи об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа до внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи.
- Уведомлять владельца сертификата ключа проверки электронной подписи о

фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут оказаться на возможности дальнейшего использования сертификата ключа проверки электронной подписи.

- Осуществлять плановую и внеплановую публикацию актуального списка отзываемых сертификатов ключей проверки электронной подписи Пользователей УЦ на сайте Удостоверяющего центра <http://ca.72to.ru>. Плановая публикация списка отзываемых сертификатов ключей проверки электронной подписи Пользователей УЦ производится не реже одного раза в сутки. Внеплановая публикация СОС производится по мере необходимости включения записей в течение двенадцати часов с момента наступления обстоятельств, указанных в частях 6 и 6.1 статьи 14 Федерального закона от 06.04.2011 № 63 «Об электронной подписи», или в течение двенадцати часов с момента, когда удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.
- Вести реестр всех созданных сертификатов ключей проверки электронной подписи Пользователей УЦ в течение установленного срока хранения. Сертификаты ключей проверки электронной подписи Пользователей УЦ представлены в реестре в форме электронных копий созданных сертификатов.
- Обеспечить актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- 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.
- Хранить следующую информацию в течение срока своей деятельности, если более короткий срок не предусмотрен нормативными правовыми актами Российской Федерации:
 - 1) реквизиты основного документа, удостоверяющего личность владельца квалифицированного сертификата - физического лица;
 - 2) сведения о наименовании, номере и дате выдачи документа, подтверждающего право лица, выступающего от имени заявителя - юридического лица, обращаться за получением квалифицированного сертификата;
 - 3) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат.

5. Права и обязанности Стороны, присоединившейся к Порядку.

5.1. Права Стороны, присоединившейся к Порядку, права Пользователя УЦ.

5.1.1. Сторона, присоединившаяся к Порядку, имеет право:

- Получить сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра.
- Получить список отозванных сертификатов ключей проверки электронной подписи, созданный Удостоверяющим центром.
- Получить копию сертификата ключа проверки электронной подписи, владельцем которого он является, на бумажном носителе, заверенную удостоверяющим центром.
- Формировать ключи электронной подписи и ключи проверки электронной подписи на своём рабочем месте посредством web-приложения, предоставляемого Удостоверяющим центром.
- Обратиться в Удостоверяющий центр для создания сертификата ключа проверки электронной подписи.
- Обратиться в Удостоверяющий центр для прекращения действия (аннулирования) сертификата ключа проверки электронной подписи владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.
- Обратиться в Удостоверяющий центр для приостановки действия сертификата ключа проверки электронной подписи владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.
- Обратиться в Удостоверяющий центр для возобновления действия сертификата ключа проверки электронной подписи владельцем которого он является, в течение срока действия соответствующего ключа электронной подписи.

5.1.2. Пользователь УЦ имеет все права Стороны, присоединившейся к Порядку, а также имеет право:

- Получить в соответствии с настоящим Порядком квалифицированный сертификат, созданный Удостоверяющим центром для данного Пользователя УЦ, при условии установления Удостоверяющим центром личности лица, обращающегося за получением данного сертификата и подтверждения его правомочий.

При получении квалифицированного сертификата:

- Получить копию сертификата на бумажном носителе, заверенную Удостоверяющим центром.
- Получить ключ электронной подписи и ключ проверки электронной подписи Пользователя УЦ, созданные Удостоверяющим центром.
- Пройти процедуру регистрации в единой системе идентификации и аутентификации.
- Получить ключевую фразу, которая в дальнейшем может использоваться для аутентификации Пользователя УЦ.
- Запрашивать и получать в Удостоверяющем центре в форме электронного документа квалифицированные сертификаты иных Пользователей УЦ,

информация о которых включена в реестр сертификатов Удостоверяющего центра.

- Обращаться в Удостоверяющий центр для прекращения действия (аннулирования), квалифицированного сертификата, владельцем которого он является, в течение срока действия данного квалифицированного сертификата.
- Обращаться в Удостоверяющий центр для получения технической поддержки по вопросам использования электронной подписи и средств электронной подписи.

5.2. Обязанности Стороны, присоединившейся к Порядку, обязанности Пользователя УЦ.

5.2.1. Сторона, присоединившаяся к Порядку, обязана:

- Исполнять требования, установленные Федеральным законом №63-фз «Об электронной подписи», принимаемыми в соответствии с ним нормативными правовыми актами и настоящим Порядком.
- Представить регистрационную и идентифицирующую информацию для регистрации в Удостоверяющем центре в объеме, определенном положениями настоящего Порядка.
- Предоставить актуальные и достоверные документы либо их надлежащим образом заверенные копии и сведения, в том числе необходимые для получения квалифицированного сертификата, регистрации квалифицированного сертификата в единой системе идентификации и аутентификации и (или) регистрации владельца сертификата в единой системе идентификации и аутентификации.
- Не реже одного раза в тридцать календарных дней обращаться на сайт Удостоверяющего центра по адресу <http://ca.72to.ru> за сведениями об изменениях, дополнениях в Порядке с целью обеспечения гарантированного ознакомления с полным текстом изменений, дополнений Порядка до вступления их в силу.
- Обеспечить конфиденциальность ключей электронных подписей, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.
- Использовать для формирования электронной подписи только действующий личный ключ электронной подписи.
- Использовать ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.
- Не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.
- 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 времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

- Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.
- Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован (отозван) или действие его приостановлено.
- Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

5.2.2. Пользователь УЦ должен соблюдать все обязанности Стороны, присоединившейся к Порядку, а также обязан:

При получении квалифицированного сертификата:

- Ознакомиться с информацией, содержащейся в квалифицированном сертификате.
- Ознакомиться с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, выдаваемым Удостоверяющим центром при выдаче квалифицированного сертификата.
- Не использовать ключ электронной подписи и незамедлительно обратиться в Удостоверяющий центр для прекращения действия квалифицированного сертификата, владельцем которого он является, при наличии оснований полагать, что конфиденциальность ключа электронной подписи нарушена.
- Использовать электронную подпись с учетом ограничений, содержащихся в квалифицированном сертификате, если такие ограничения установлены.
- Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, заявление на прекращение действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр до момента времени официального уведомления о прекращении действия квалифицированного сертификата, либо об отказе в прекращении действия.
- Не использовать ключ электронной подписи, связанный с квалифицированным сертификатом, который аннулирован или действие которого прекращено.
- При создании или проверке электронной подписи осуществлять проверку

действительности квалифицированного сертификата на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен.

- При проверке электронной подписи осуществлять проверку принадлежности владельцу сертификата электронной подписи, с помощью которой подписан электронный документ, а также осуществлять проверку отсутствия изменений, внесенных в этот документ после его подписания.
- Информировать Удостоверяющий центр об изменении регистрационных данных владельца сертификата, влияющих на актуальность сведений, содержащихся в квалифицированном сертификате, и обратиться в Удостоверяющий центр для прекращения действия такого сертификата в случае наличия оснований полагать, что несоответствие данных о владельце сертификата и сведений, содержащихся в квалифицированном сертификате, может повлиять на результат проверки электронной подписи при осуществлении обмена информацией с иными участниками информационного взаимодействия.

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.

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

6.1.1. Порядок создания ключей электронных подписей и ключей проверки электронных подписей заявителем.

6.1.1.1. Создание ключей электронных подписей и ключей проверки электронных подписей, предназначенных для создания и проверки усиленной квалифицированной 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.

6.1.1.2. 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)».

6.1.1.3. Сторона, присоединившаяся к Порядку, имеет право получить средства

электронной подписи при обращении в Удостоверяющий центр в соответствии с настоящим Порядком.

6.1.1.4. При создании ключа электронной подписи и ключа проверки электронной подписи заявитель формирует запрос на создание сертификата в электронной форме (файл в формате PKCS#10) и (или) в форме бумажного документа, подписанного заявителем собственноручно.

Сформированный запрос на создание сертификата прикладывается к заявительным документам при обращении заявителя в Удостоверяющий центр для получения квалифицированного сертификата.

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 усиленной квалифицированной электронной подписью заявителя.

6.1.1.5. 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.

6.1.1.6. При создании ключа электронной подписи и ключа проверки электронной подписи должен устанавливаться пароль доступа к ключевой информации, отвечающий требованиям к сложности паролей:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, \$, !, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (user, admin и т.д.).

6.1.1.7. Заявитель должен обеспечивать конфиденциальность ключей электронных подписей и паролей доступа к ключевой информации, принимать все возможные меры для предотвращения их потери, раскрытия, искажения и несанкционированного использования.

6.1.1.8. Хранение и использование ключей электронных подписей должно осуществляться заявителем в соответствии с Инструкцией ФАПСИ № 152, руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 20 к настоящему Порядку.

6.1.1.9. 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:

- установлена личность заявителя или получено подтверждение правомочий лица, выступающего от имени заявителя, обращающегося за получением

квалифицированного сертификата;

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

6.1.2. Порядок создания ключей электронных подписей и ключей проверки электронных подписей Удостоверяющим центром для заявителя.

6.1.2.1. Ключи электронных подписей и ключи проверки электронных подписей создаются Удостоверяющим центром с использованием средств электронной подписи и средств удостоверяющего центра, 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 и средства удостоверяющего центра.

6.1.2.2. Удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

6.1.2.3. Создание ключей электронных подписей и ключей проверки электронных подписей осуществляется Удостоверяющим центром в соответствии с требованиями постановления Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации», с использованием автоматизированных рабочих мест Удостоверяющего центра, а также средств защиты информации и средств криптографической защиты информации, прошедших процедуру оценки соответствия, аттестованных и (или) сертифицированных по требованиям безопасности информации.

6.1.2.4. Создание ключа электронной подписи и ключа проверки электронной подписи осуществляется Удостоверяющим центром для заявителя, присоединившегося к настоящему Порядку, при личном прибытии заявителя или его уполномоченного представителя в ЦР Удостоверяющего центра, при условии установления личности заявителя или получения подтверждения правомочий лица, выступающего от имени заявителя.

6.1.2.5. Ключ электронной подписи и ключ проверки электронной подписи создается Удостоверяющим центром одновременно с созданием квалифицированного сертификата в соответствии с пунктом 6.1 настоящего Порядка, при условии подтверждения достоверности документов и сведений, предоставленных заявителем.

6.1.2.6. Создание ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата осуществляется Оператором УЦ. Созданный ключ электронной подписи, ключ проверки электронной подписи и квалифицированный сертификат записываются на носитель ключевой информации (далее также – ключевой носитель) смарт-карту или принадлежащий заявителю (Рутокен, eToken). Удостоверяющий центр не осуществляет хранение ключа электронной подписи заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие заявителю.

6.1.2.7. Ключевой носитель, принадлежащий заявителю, перед осуществлением записи на него создаваемого Удостоверяющим центром ключа электронной подписи и ключа проверки электронной подписи, не должен содержать иной посторонней информации, в том числе иных ключей электронной подписи. Удостоверяющий центр не несёт ответственности в связи с компрометацией или удалением информации, находящейся на носителе, принадлежащем заявителю.

6.1.2.8. При создании ключа электронной подписи и ключа проверки электронной подписи Удостоверяющим центром формируется пароль доступа к ключевой информации, который устанавливается по согласованию с заявителем (Рутокен, eToken), на смарт-карту пароль генерируется автоматически в запечатанном пин-конверте. После получения ключа электронной подписи и ключа проверки электронной подписи заявитель должен произвести смену пароля доступа к ключевой информации (Рутокен, eToken), соблюдая требования к сложности паролей в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи.

6.1.2.9. В случае, если Удостоверяющий центр не имеет технической возможности использовать для создания ключа электронной подписи и ключа проверки электронной подписи средство электронной подписи, аналогичное средству электронной подписи заявителя, указанному им в заявительных документах, заявитель имеет право самостоятельно осуществить создание ключа электронной подписи и ключа проверки электронной подписи в соответствии с пунктом 6.1.1 настоящего Порядка.

6.1.2.10. В случае создания ключа электронной подписи и ключа проверки электронной подписи при личном прибытии заявителя или его уполномоченного представителя в ЦР Удостоверяющего центра основанием подтверждения владения заявителем ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения квалифицированного сертификата, является одновременное соблюдение следующих условий:

- установлена личность заявителя или получено подтверждение правомочий лица, выступающего от имени заявителя, обращающегося за получением квалифицированного сертификата;
- подтверждена достоверность документов и сведений, предоставляемых в

Удостоверяющий центр заявителем;

- заявитель или его уполномоченный представитель под расписку ознакомлен с информацией, включаемой в состав сертификата, которая содержится в заявлении на создание квалифицированного сертификата ключа проверки электронной подписи.

6.2. Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра.

6.2.1. В процессе организации деятельности Удостоверяющего центра осуществляется планирование мероприятий по осуществлению его деятельности, в том числе мероприятий по смене ключей электронной подписи Удостоверяющего центра и мероприятий по выводу ключей электронной подписи Удостоверяющего центра из эксплуатации.

6.2.2. Основаниями для выполнения процедуры плановой смены ключа электронной подписи Удостоверяющего центра и процедуры его вывода из эксплуатации являются запланированные мероприятия по осуществлению деятельности Удостоверяющего центра.

6.2.3. Выполнение процедуры плановой смены ключа электронной подписи Удостоверяющего центра осуществляется в период срока действия ключа электронной подписи Удостоверяющего центра, не ранее, чем через один год, и не позднее, чем через один год и три месяца после начала действия ключа электронной подписи Удостоверяющего центра. Процедура создания нового ключа электронной подписи Удостоверяющего центра осуществляется заранее, не позднее, чем за 10 дней до истечения одного года после начала срока действия ключа электронной подписи Удостоверяющего центра.

6.2.4. Выполнение процедуры вывода из эксплуатации ключа электронной подписи Удостоверяющего центра осуществляется не позднее, чем за один рабочий день до окончания срока действия ключа электронной подписи Удостоверяющего центра, установленного в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи, с использованием которого данный ключ электронной подписи был создан.

6.2.5. Срок действия ключа электронной подписи Удостоверяющего центра составляет максимально допустимый срок действия, установленный в соответствии с технической и эксплуатационной документацией на средства удостоверяющего центра и 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 создания ключа электронной подписи Удостоверяющего центра.

6.2.6. Порядок смены ключей электронной подписи Удостоверяющего центра.

6.2.6.1. Плановая смены ключей электронной подписи Удостоверяющего центра осуществляется в следующем порядке:

- 1) Администратор Удостоверяющего центра с использованием

сертифицированных по требованиям безопасности средств удостоверяющего центра и средств электронной подписи создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи, записывает их на сертифицированный учтенный ключевой носитель и обеспечивает его хранение в соответствии с требованиями, предъявляемыми к обеспечению целостности и конфиденциальности ключа электронной подписи Удостоверяющего центра. Одновременно с созданием вышеуказанных ключей производится формирование запроса на создание квалифицированного сертификата Удостоверяющего центра.

2) Сформированный запрос на создание квалифицированного сертификата Удостоверяющего центра, а также иная информация, необходимая для получения квалифицированного сертификата Удостоверяющего центра, направляется в уполномоченный федеральный орган, являющийся головным удостоверяющим центром в отношении Удостоверяющего центра.

3) После получения квалифицированного сертификата, созданного головным удостоверяющим центром уполномоченного федерального органа, Администратор Удостоверяющего центра, по истечении одного года после начала срока действия предыдущего ключа электронной подписи Удостоверяющего центра:

осуществляет ввод в эксплуатацию и установку нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Удостоверяющего центра;

производит в соответствии с технической и эксплуатационной документацией настройку средств удостоверяющего центра для использования нового ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Удостоверяющего центра;

обеспечивает хранение и использование ключей электронной подписи и ключей проверки электронной подписи Удостоверяющего центра в соответствии с требованиями безопасности, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

Доверенным способом взаимодействия является использование информационной системы головного удостоверяющего центра, входящей в состав инфраструктуры.

6.2.6.2. Информирование участников электронного взаимодействия о проведении плановой смены ключа электронной подписи Удостоверяющего центра осуществляется посредством размещения на сайте Удостоверяющего центра <http://ca.72to.ru/> , информации о новом квалифицированном сертификате Удостоверяющего центра, соответствующему новому ключу проверки электронной подписи и ключу электронной подписи Удостоверяющего центра.

6.2.6.3. Предыдущий ключ электронной подписи Удостоверяющего центра действует в течение своего срока действия до вывода его из эксплуатации и используется для создания и подписания списка отзываемых сертификатов, созданных Удостоверяющим центром в период действия предыдущего ключа электронной подписи Удостоверяющего центра.

6.2.6.4. Введенный в эксплуатацию новый ключ электронной подписи Удостоверяющего центра используется только для подписания создаваемых

Удостоверяющим центром квалифицированных сертификатов и списков отзываемых сертификатов.

6.2.6.5. Доверенными способами получения квалифицированного сертификата Удостоверяющего центра являются:

- получение заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении квалифицированного сертификата, созданного Удостоверяющим центром для заявителя;
- загрузка квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона «Об электронной подписи».

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

6.3.1. В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра или реализации угрозы нарушения его конфиденциальности осуществляется внеплановая смена ключа электронной подписи и ключа проверки электронной подписи Удостоверяющего центра.

6.3.2. К случаям нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра, относятся:

- получение доступа неуполномоченного лица к ключу электронной подписи Удостоверяющего центра или к ключевому носителю, содержащего ключ электронной подписи Удостоверяющего центра;
- утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра;
- утрата или хищение ключевого носителя, содержащего ключ электронной подписи Удостоверяющего центра, с его последующим обнаружением;
- получение доступа неуполномоченного лица к техническим средствам Удостоверяющего центра или средствам электронной подписи, содержащих ключ электронной подписи Удостоверяющего центра;
- несанкционированное копирование ключа электронной подписи Удостоверяющего центра;
- нарушение правил хранения и использования ключа электронной подписи Удостоверяющего центра, которое привело или могло привести к его компрометации;
- нарушение целостности печатей на сейфах (шкафах, хранилищах) и пеналах (конвертах), предназначенных для хранения ключевых носителей, содержащих ключи электронной подписи Удостоверяющего центра;
- утрата ключей от сейфов (шкафов, хранилищ) в случае нахождения в них

ключевых носителей, содержащих ключи электронной подписи Удостоверяющего центра;

- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем, в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий нарушителя.

6.3.3. Виды угроз нарушения конфиденциальности ключей электронной подписи Удостоверяющего центра:

- угрозы, непосредственно связанные с нарушением конфиденциальности ключа электронной подписи Удостоверяющего центра;
- угрозы, связанные с несанкционированным доступом в помещения, где размещаются технические средства удостоверяющего центра, или доступом к хранилищам ключевой информации;
- угрозы, связанные с несанкционированным доступом к средствам удостоверяющего центра;
- угрозы, связанные с лицами, имеющими доступ в контролируемую зону, к средствам Удостоверяющего центра, ключам электронной подписи Удостоверяющего центра;
- угрозы, связанные с проведением нарушителем атак на технические средства удостоверяющего центра, в том числе на носители защищаемой информации, средства вычислительной техники, среду функционирования средств криптографической защиты информации, каналы (линии) связи.

6.3.4. Удостоверяющий центр начинает процедуру внеплановой смены ключа электронной подписи Удостоверяющего центра после устранения причин, повлекших нарушение конфиденциальности электронной подписи Удостоверяющего центра, и не позднее 12 (двенадцати) часов с момента выявления факта компрометации или факта реализации угрозы нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра уведомляет уполномоченный федеральный орган о факте компрометации ключа электронной подписи Удостоверяющего центра и необходимости внеплановой смены ключа электронной подписи Удостоверяющего центра, для чего направляет в уполномоченный федеральный орган соответствующие заявление на прекращение действия квалифицированного сертификата Удостоверяющего центра и заявление на создание и выдачу нового квалифицированного сертификата Удостоверяющего центра.

6.3.5. Процедура внеплановой смены ключей электронной подписи Удостоверяющего центра осуществляется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра в соответствии с пунктом 6.2 настоящего Порядка.

6.3.6. Одновременно со сменой ключа электронной подписи Удостоверяющего центра прекращается действие всех ранее выданных квалифицированных сертификатов, подписанных ключом электронной подписи Удостоверяющего центра, который скомпрометирован.

6.3.7. Удостоверяющий центр уведомляет о факте компрометации ключа электронной подписи Удостоверяющего центра всех владельцев сертификатов путем направления соответствующего уведомления по электронной почте и публикации информации на сайте Удостоверяющего центра.

6.3.8. Прекращение действия квалифицированного сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия квалифицированного сертификата Удостоверяющего центра включается в список отзываемых сертификатов, который публикуется головным удостоверяющим центром.

6.3.9. После смены ключа электронной подписи Удостоверяющего центра и получения нового квалифицированного сертификата Удостоверяющего центра, выданного головным уполномоченным органом, Удостоверяющий центр уведомляет всех владельцев сертификатов о возможности получения ими новых квалифицированных сертификатов на безвозмездной основе.

6.3.10. Доверенными способами получения нового квалифицированного сертификата Удостоверяющего центра являются:

- получение заявителем квалифицированного сертификата Удостоверяющего центра непосредственно в Удостоверяющем центре, в том числе при получении квалифицированного сертификата, созданного Удостоверяющим центром для заявителя;
- загрузка нового квалифицированного сертификата Удостоверяющего центра с сайта Удостоверяющего центра или Портала уполномоченного федерального органа в области использования электронной подписи, с последующей проверкой электронной подписи квалифицированного сертификата в соответствии со статьей 11 Федерального закона «Об электронной подписи».

6.4. Порядок осуществления Удостоверяющим центром смены ключа электронной подписи Пользователя УЦ.

6.4.1. Сроки действия ключей электронной подписи и квалифицированных сертификатов, выдаваемых Удостоверяющим центром Пользователям УЦ.

6.4.1.1. Срок действия ключа электронной подписи и квалифицированного сертификата, выдаваемого Удостоверяющим центром Пользователю УЦ, включается в состав квалифицированного сертификата и не превышает 15 (пятнадцать) месяцев.

6.4.1.2. Начало периода действия ключа электронной подписи исчисляется с даты и времени начала действия соответствующего квалифицированного сертификата.

6.4.1.3. Время начала действия квалифицированного сертификата включается в поле «Действителен с» («NotBefore») квалифицированного сертификата. Время окончания действия квалифицированного сертификата включается в поле «Действителен по» («NotAfter») квалифицированного сертификата.

6.4.1.4. Период действия ключа электронной подписи включается в поле «Период использования закрытого ключа» («PrivateKeyUsagePeriod») квалифицированного сертификата, содержащего время начала и окончания действия ключа электронной

подписи, которые включаются соответственно в поле «Действителен с» («NotBefore») и в поле «Действителен по» («NotAfter») квалифицированного сертификата.

6.4.2. Смена ключа электронной подписи Пользователя УЦ осуществляется владельцем сертификата в следующих случаях:

1. В связи с истечением установленного срока действия ключа электронной подписи.
2. На основании заявления, подаваемого в форме документа на бумажном носителе или в форме электронного документа.
3. Не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате.
4. Установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате.
5. Вступило в силу решение суда, которым, в частности, установлено, что квалифицированный сертификат содержит недостоверную информацию.
6. Изменение сведений о владельце сертификата, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными.
7. Нарушение конфиденциальности ключа электронной подписи владельца сертификата.
8. Осуществлена процедура внеплановой смены ключа электронной подписи Удостоверяющего центра. В таком случае создание новых ключей электронной подписи для Пользователя УЦ и соответствующих им квалифицированных сертификатов осуществляется в соответствии с пунктом 6.3 настоящего Порядка.
9. В иных случаях, установленных Федеральным законом «Об электронной подписи», другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами, настоящим Порядком или договором оказания услуг удостоверяющего центра.

6.4.3. В случае наступления обстоятельств, указанных в подпунктах 3 – 5 пункта 6.4.2 настоящего Порядка, Удостоверяющий центр аннулирует квалифицированный сертификат владельца сертификата и уведомляет об этом владельца сертификата. Информация о прекращении действия сертификата вносится Удостоверяющим центром в реестр сертификатов в течение 12 (двенадцати) часов с момента наступления указанных обстоятельств, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств. Действие квалифицированного сертификата прекращается с момента внесения записи об этом в реестр сертификатов.

6.4.4. В случае наступления обстоятельств, указанных в подпунктах 6 и 7 пункта 6.4.2 настоящего Порядка, Сторона, присоединившаяся к Порядку, обязана обратиться в Удостоверяющий центр с заявлением на прекращение действия квалифицированного сертификата.

6.4.5. Смена ключа электронной подписи Пользователя УЦ осуществляется по его

инициативе в соответствии процедурой создания ключей электронных подписей и ключей проверки электронных подписей, приведенной в пункте 6.1 настоящего Порядка.

6.4.6. Создание Удостоверяющим центром нового ключа электронного подписи осуществляется одновременно с созданием ключа проверки электронной подписи и квалифицированного сертификата на основании соответствующего заявления Стороны, присоединившейся к Порядку, и документов, представленных в Удостоверяющий центр.

6.4.7. Требования к заявлению на смену ключа электронной подписи Пользователя УЦ.

Получение ключей электронной подписи и сертификата ключа проверки электронной подписи пользователя УЦ осуществляется на основании заявления на создание сертификата ключа проверки электронной подписи при плановой смене. Заявление подается в ЦР в бумажной форме при личном прибытии пользователя. Форма заявления на создание ключей электронной подписи и сертификата ключа проверки электронной подписи при плановой смене приведена в Приложениях №№ 3,4,5а,6а,7,8 к настоящему Порядку. Документы по форме приложений №№ 5а,6а могут быть предоставлены уполномоченным представителем пользователя УЦ, действующим на основании доверенности на получение ключей электронной подписи и сертификата в Удостоверяющем центре. Доверенность должна быть составлена по форме Приложения № 10 Порядка УЦ.

После положительной идентификации пользователя УЦ или доверенного лица оператор ЦР принимает документы, осуществляет их рассмотрение и записывает ключи электронной подписи и сертификат ключа проверки электронной подписи на ключевой носитель. Типы ключевых носителей приведены в Приложении № 11 Порядка УЦ. Смарт-карта предоставляется Удостоверяющим центром, защищенные носители Рутокен, eToken должны быть предоставлены пользователем УЦ или его представителем.

6.4.8. Заявитель имеет право самостоятельно произвести плановую смену, создав ключ электронной подписи в соответствии с разделом 6.1.1 настоящего Порядка.

В случае, если смена ключа электронной подписи Пользователя УЦ связана с нарушением его конфиденциальности или реализацией угрозы нарушения конфиденциальности, Пользователь УЦ обязан обратиться в Удостоверяющий центр с заявлением на прекращение действия квалифицированного сертификата. В этом случае, новый ключ электронной подписи создаются Удостоверяющим центром в соответствии с разделом 6.1.2 настоящего Порядка.

6.4.9. Процедура смены ключа электронной подписи Пользователя УЦ осуществляется в соответствии с пунктами 6.1 и 6.4 настоящего Порядка в том же порядке, как и создание ключа электронной подписи, при этом осуществляется также создание квалифицированного сертификата в соответствии с пунктом 6.5 настоящего Порядка.

6.4.10. Процедура создания и выдачи квалифицированного сертификата и (при необходимости) ключа электронной подписи его владельцу, в том числе в электронной форме, производится с соблюдением положений статьи 18 Федерального закона «Об электронной подписи» и настоящим Порядком.

6.5. Процедура создания и выдачи квалифицированных сертификатов.

6.5.1. Порядок подачи заявления на создание и выдачу квалифицированных сертификатов.

6.5.1.1. Заявитель обязан ознакомиться с положениями настоящего Порядка, опубликованного на сайте Удостоверяющего центра, в том числе с приложениями к настоящему Порядку.

6.5.1.2. Присоединение к Порядку осуществляется в соответствии с пунктом 2.1.6 настоящего Порядка. Для присоединения к настоящему Порядку и возможности получения услуг Удостоверяющего центра заявитель направляет заявление о присоединении к Порядку по форме приложения № 1 или приложения № 2 к настоящему Порядку.

6.5.1.3. Удостоверяющий центр осуществляет создание квалифицированных сертификатов при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

6.5.1.4. Создание и выдача квалифицированного сертификата ключа проверки электронной подписи осуществляется на основании Заявления на создание квалифицированного сертификата ключа проверки электронной подписи.

6.5.1.5. Заявление на создание и выдачу квалифицированного сертификата ключа проверки электронной подписи подается Заявителем в электронной или бумажной форме:

- Заявление на создание квалифицированного сертификата ключа проверки электронной подписи в бумажной форме подается лично, подписанное собственноручной подписью заявителя. Форма заявления приведена в Приложениях №№ 3-8 к настоящему Порядку УЦ.
- Заявление на создание квалифицированного сертификата ключа проверки электронной подписи в электронной форме подписывается действующим квалифицированным сертификатом ключа проверки электронной подписи Заявителя.

6.5.1.6. Создание квалифицированного сертификата осуществляется Удостоверяющим центром на основании заявления на создание и выдачу квалифицированного сертификата, а также документов и сведений, представленных заявителем в Удостоверяющий центр, при условии установления личности заявителя или доверенного лица, путем установления личности по документу, удостоверяющему личность, устанавливает соответствие данных, указанных в заявлении, предоставленным документам либо их надлежащим образом заверенным копиям, проверяет прочие подтверждающие документы, необходимые для регистрации.

6.5.1.7. В случае, если Сторона, присоединившаяся к Порядку, обращается в Удостоверяющий центр для проведения плановой смены ключа электронной подписи, ключа проверки электронной подписи и квалифицированного сертификата Пользователя УЦ и сведения, содержащиеся в ранее представленных документах, потеряли свою актуальность и достоверность, Сторона, присоединившаяся к Порядку, предоставляет в Удостоверяющий центр заявление на создание и выдачу квалифицированного

сертификата, а также актуальные документы и сведения, необходимые для создания квалифицированного сертификата.

6.5.1.8. После получения Удостоверяющим центром от заявителя заявления о присоединении к Порядку и (или) заявления на создание и выдачу квалифицированного сертификата, в случае, если заявителем не представлены документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или их достоверность и актуальность не подтверждается, Удостоверяющий центр имеет право запросить, а Сторона, присоединившаяся к Порядку, обязана предоставить документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата.

6.5.1.9. Удостоверяющий центр имеет право отказать заявителю в создании и выдаче квалифицированного сертификата, в случае, если Сторона, присоединившаяся к Порядку, не предоставила документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания и выдачи квалифицированного сертификата, либо они представлены не полном объеме или они ненадлежаще оформлены, а также в случае, когда достоверность и актуальность представленных заявителем сведений не подтверждается.

6.5.2. Требования к заявлению на создание и выдачу квалифицированного сертификата.

6.5.2.1. Требования к оформлению заявления на создание и выдачу квалифицированного сертификата.

6.5.2.1.1. В случае, если заявителю необходим сертификат юридического лица, заявление оформляется по форме, приведенной в приложениях №№ 3, 7 к Порядку УЦ и должно содержать:

- реквизиты (дата и номер) договора присоединения к Порядку УЦ;
- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;
- собственноручную подпись физического лица, действующего от имени юридического лица на основании учредительных документов или доверенности;
- собственноручную подпись заявителя и дату подписания.

6.5.2.1.2. В случае, если заявителю необходим сертификат физического лица, заявление оформляется по форме, приведенной в приложениях №№ 4, 8 к Порядку УЦ, и должно содержать:

- сведения, необходимые для создания квалифицированного сертификата, а также сведения о средстве электронной подписи, используемом заявителем;
- собственноручную подпись физического лица, действующего от имени юридического лица на основании учредительных документов или доверенности;
- собственноручную подпись заявителя и дату подписания.

6.5.2.2. В случае, если заявитель самостоятельно осуществил создание ключа электронной подписи и ключа проверки электронной подписи к заявлению

прикладывается 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.

6.5.2.3. Требования к сведениям, включаемым в заявление на создание и выдачу квалифицированного сертификата:

6.5.2.3.1. В случае, получения сертификата юридического лица, в заявлении в обязательном порядке указывается следующая информация:

- 1) фамилия, имя и отчество (если имеется), СНИЛС и ИНН физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности, если такое физическое лицо указано в качестве владельца сертификата наряду с указанием наименования юридического лица и сведения о нем включены в заявление на создание и выдачу квалифицированного сертификата.;
- 2) наименование организации в соответствии с выпиской из ЕГРЮЛ;
- 3) местонахождение организации в соответствии с выпиской из ЕГРЮЛ;
- 4) ОГРН организации;
- 5) ИНН организации.

6.5.2.3.2. Допускается не указывать в качестве владельца сертификата физическое лицо, действующее от имени юридического лица, в квалифицированном сертификате, используемом для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами (далее также – квалифицированный сертификат информационной системы). В этом случае в заявлении допускается указывать только информацию, предусмотренную пунктом 6.5.2.3.1 настоящего Порядка.

6.5.2.3.3. В случае, получения сертификата физического лица, в заявлении в обязательном порядке указывается следующая информация:

- 1) фамилия, имя и отчество (если имеется) физического лица;
- 2) СНИЛС физического лица;
- 3) ИНН физического лица.

6.5.2.3.4. Заявление на создание и выдачу квалифицированного сертификата должно содержать информацию о наименовании и классе средства электронной подписи, используемом заявителем.

6.5.2.4. Заявитель имеет право оформить заявление на создание и выдачу квалифицированного сертификата как на бумажном носителе, так и в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

6.5.3. Порядок идентификации заявителя.

В соответствии со статьей 18 Федерального закона «Об электронной подписи» при выдаче квалифицированного сертификата Удостоверяющий центр идентифицирует личность заявителя — физического лица, обратившегося к нему за получением квалифицированного сертификата, руководствуясь следующими положениями:

1) при его личном присутствии:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность;
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства;
- личность беженца, вынужденного переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

2) без его личного присутствия с использованием усиленной квалифицированной электронной подписи при наличии действующего квалифицированного сертификата.

6.5.4. Перечень документов, запрашиваемых Удостоверяющим центром у заявителя для создания и выдачи квалифицированного сертификата.

6.5.4.1. Заявители, являющиеся юридическими лицами, предоставляют:

- 1) Основной документ, удостоверяющий личность физического лица.
- 2) Учредительные документы юридического лица (либо их копии).
- 3) Доверенность, подтверждающая право физического лица, действовать от имени юридического лица или копия документа, подтверждающего полномочия лица на осуществление действий от имени юридического лица (для руководителя юридического лица - копия решения о назначении или об избрании либо копия приказа о назначении физического лица на должность, в соответствии с которыми такое физическое лицо обладает правом действовать от имени юридического лица без доверенности).

Указанная доверенность оформляется в соответствии с формой, приведенной в приложении № 9 к настоящему Порядку.

- 4) Страховое свидетельство государственного пенсионного страхования (либо его копию).
- 5) Свидетельство о постановке на учет в налоговом органе физического лица (либо его копию).
- 6) Свидетельство о государственной регистрации юридического лица (либо его копию).
- 7) Свидетельство о постановке на учет в налоговом органе юридического лица (либо его копию).
- 8) Выписку из Единого государственного реестра юридических лиц, полученную не ранее чем за один месяц до момента обращения в Удостоверяющий центр (либо ее копию).

6.5.4.2. Заявители, являющиеся физическими лицами, предоставляют:

- 1) основной документ, удостоверяющий личность;
- 2) страховое свидетельство государственного пенсионного страхования (либо его копию);
- 3) свидетельство о постановке на учет в налоговом органе физического лица (либо его копию).

6.5.4.3. В случае, если документы и сведения, предоставляемые заявителем, оформлены не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

6.5.4.4. В случае, если для подтверждения сведений, вносимых в квалифицированный сертификат, законодательством Российской Федерации установлена определенная форма документа, заявитель представляет в Удостоверяющий центр документ соответствующей формы.

6.5.5. Порядок проверки достоверности документов и сведений, представленных заявителем.

6.5.5.1. При получении от заявителя документов и сведений, необходимых для создания и выдачи квалифицированного сертификата, Оператор УЦ, в целях определения возможности регистрации Пользователя УЦ, в течение не более чем одного рабочего дня со дня их получения осуществляет предварительную проверку предоставленных заявителем документов и сведений на предмет их надлежащего оформления и полноты представления, соответствия положениям части 3 статьи 14, части 2 статьи 17 и части 2 статьи 18 Федерального закона «Об электронной подписи», а также требованиям, указанным в пунктах 6.5.2 и 6.5.4 настоящего Порядка.

6.5.5.2. Полученные Удостоверяющим центром заявления и иные документы регистрируются в соответствии с правилами ведения делопроизводства.

6.5.5.3. В случае, если документы представлены заявителем в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, Оператор УЦ осуществляет ее проверку в соответствии со статьей 11 Федерального закона «Об электронной подписи».

6.5.5.4. В случае положительной предварительной проверки документов и сведений, предоставленных заявителем, Удостоверяющий центр с использованием инфраструктуры осуществляет проверку достоверности документов и сведений, предоставленных заявителем в соответствии с частями 2 и 2.1 статьи 18 Федерального закона «Об электронной подписи» и в течение не более чем одного рабочего дня со дня получения документов и сведений, предоставленных заявителем, запрашивает из государственных информационных ресурсов выписку из единого государственного реестра юридических лиц в отношении заявителя – юридического лица.

6.5.5.5. Удостоверяющий имеет право отказать в регистрации Пользователя УЦ в реестре Удостоверяющего центра или изменения регистрационных данных Пользователя УЦ в случае отрицательного результата проверки документов и сведений, предоставленных заявителем, в том числе в следующих случаях:

- не предоставлены документы либо их надлежащим образом заверенные копии и

сведения, необходимые для создания и выдачи квалифицированного сертификата;

- документы либо их надлежащим образом заверенные копии и сведения, необходимые для создания квалифицированного сертификата, представлены не в полном объеме или они ненадлежаще оформлены, а также в случае, если актуальность представленных заявителем сведений не подтверждается;
- сведения, полученные из государственных информационных ресурсов, не подтверждают достоверность информации, представленной заявителем.

6.5.5.6. В случае отрицательного результата проверки документов и сведений Удостоверяющий центр уведомляет об этом заявителя в течение трех дней после проведения их проверки.

6.5.6. Порядок создания квалифицированного сертификата.

6.5.6.1. Создание квалифицированного сертификата осуществляется Удостоверяющим центром в соответствии с положениями статей 13 – 15, 17 и 18 Федерального закона «Об электронной подписи» и настоящим Порядком.

Заявителям квалифицированные сертификаты создаются при выполнении Стороной, присоединившейся к Порядку, обязанностей, предусмотренных настоящим Порядком.

6.5.6.2. Удостоверяющий центр в течение пяти рабочих дней со дня получения сведений из государственных информационных ресурсов и положительного результата проведения проверки документов и сведений, предоставленных заявителем, осуществляет процедуру создания квалифицированного сертификата.

6.5.6.3. При прибытии заявителя либо его уполномоченного представителя в ЦР Удостоверяющего центра, Оператор ЦР осуществляет установление его личности и проверку оригиналов документов или их надлежаще заверенных копий, проверку соответствия сведений, полученных из государственных информационных ресурсов, со сведениями, содержащимися в представленных заявителем документах и регистрационных данных Пользователя УЦ, а также проверку доверенностей (в случае, если за получением сертификата обращается лицо, не указанное в заявлении на создание и выдачу квалифицированного сертификата).

6.5.6.4. После установления личности пользователя УЦ или доверенного лица и положительного результата проверки документов и сведений, Оператор УЦ осуществляет создание квалифицированного сертификата.

6.5.6.5. Для создания квалифицированного сертификата Оператор УЦ осуществляет:

- проверку работоспособности ключевого носителя, представленного заявителем, в том числе его проверку на наличие вредоносного программного обеспечения или посторонней информации и, при необходимости, выполняет его инициализацию (форматирование), если он не был ранее проинициализирован;
- с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, осуществляет создание ключа электронной подписи и ключа проверки электронной подписи Пользователя УЦ в соответствии с пунктом 6.1.2 настоящего Порядка и в соответствии с

пунктом 6.4 настоящего Порядка, если выполняется смена ключа электронной подписи владельца сертификата. При создании ключа электронной подписи и ключа проверки электронной подписи производится их запись непосредственно на ключевой носитель, представленный Удостоверяющим центром или заявителем.

6.5.6.6. Допускается осуществлять процедуру создания квалифицированного сертификата без прибытия заявителя или его уполномоченного представителя в Удостоверяющий центр при одновременном соблюдении следующих условий:

- личность лица, обращающегося за получением сертификата, была установлена Удостоверяющим центром ранее;
- лицо, обращающееся за получением сертификата, ранее было зарегистрировано в реестре Удостоверяющего центра в качестве Пользователя УЦ и указанное лицо является владельцем сертификата, который был выдан Удостоверяющим центром;
- сведения о лице, обращающемся за получением сертификата, который является владельцем сертификата, выданным Удостоверяющим центром, не изменились;
- документы, которые должны составляться исключительно на бумажном носителе, предоставляются посредством курьерской или почтовой связи;
- подтверждена актуальность и достоверность документов и сведений о владельце сертификата, которые получены Удостоверяющим центром ранее, в том числе оригиналов документов или их надлежаще заверенных копий;
- получен положительный результат проведения проверки документов и сведений, предоставленных заявителем, в том числе подтверждены полномочия заявителя и лица, обращающегося за получением квалифицированного сертификата;
- создание ключа электронной подписи осуществлено заявителем самостоятельно и заявителем представлен в Удостоверяющий центр запрос на создание сертификата в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя;
- имеется положительный результат проверки запроса на создание сертификата в форме электронного документа, представленного заявителем, а также подтверждено владение лицом, обращающимся за получением сертификата, ключом электронной подписи и ключом проверки электронной подписи, соответствующему запросу на создание сертификата;
- имеется положительный результат проверки усиленной квалифицированной электронной подписи документов, предоставленных заявителем в электронной форме, в том числе запроса на создание сертификата, представленного заявителем в форме электронного документа, подписанного усиленной квалифицированной электронной подписью заявителя.

6.5.7. Порядок выдачи квалифицированного сертификата.

6.5.7.1. Выдача квалифицированного сертификата, созданных в соответствии с пунктом 6.5.6. осуществляется Удостоверяющим центром в соответствии с положениями статьи 18 Федерального закона «Об электронной подписи» и настоящим Порядком.

Заявителям, квалифицированные сертификаты создаются при выполнении Стороной, присоединившейся к Порядку, обязанностей, предусмотренных настоящим

Порядком.

6.5.7.2. Выдача квалифицированного сертификата, созданного Удостоверяющим центром, осуществляется при личном прибытии заявителя либо его уполномоченного представителя в Удостоверяющий центр.

6.5.7.3. Допускается выдача квалифицированного сертификата без личного прибытия заявителя либо его уполномоченного представителя в Удостоверяющий центр, при одновременном соблюдении всех условий, указанных в пункте 6.5.6.6 настоящего Порядка, при этом создание и (или) смена ключа электронной подписи и ключа проверки электронной подписи осуществляется заявителем в соответствии с пунктами 6.1.1 и 6.4 настоящего Порядка.

Выдача квалифицированного сертификата без личного прибытия заявителя либо его уполномоченного представителя в Удостоверяющий центр осуществляется в порядке, определенном пунктом 6.5.7.4 настоящего Порядка, при этом:

- информационное взаимодействие между Удостоверяющим центром и заявителем должно осуществляться способами, позволяющими обеспечить целостность информации и ее конфиденциальность, в случае передачи конфиденциальной информации;
- ключ электронной подписи создается заявителем с использованием сертифицированных средств электронной подписи и не передается в Удостоверяющий центр;
- документы и их копии в электронной форме, должны подписываться действующей усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра или заявителя соответственно;
- документы, которые должны составляться исключительно на бумажном носителе, предоставляются посредством курьерской или почтовой связи.

6.5.7.4. Процедура выдачи квалифицированного сертификата, созданного Удостоверяющим центром.

После создания квалифицированного сертификата в соответствии с пунктом 6.5.6 настоящего Порядка, установления личности заявителя или его уполномоченного представителя, а также получения подтверждения их полномочий, с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации, Оператор УЦ:

1) Обеспечивает ознакомление заявителя под расписку с информацией, содержащейся в квалифицированном сертификате, в следующем порядке:

- распечатывает в двух экземплярах на бумажном носителе копию сертификата ключа проверки электронной подписи владельца сертификата, соответствующего электронной форме квалифицированного сертификата Пользователя УЦ (далее также – бланк сертификата), и заверяет его собственноручной подписью;
- предоставляет на ознакомление и подпись заявителю или его уполномоченному представителю;
- заявитель или его уполномоченный представитель проверяет соответствие сведений, содержащихся в распечатанном бланке сертификата Пользователя УЦ и,

при успешной проверке сведений, заверяет его собственоручной подписью;

- один экземпляр заверенного бланка сертификата передается владельцу сертификата или его уполномоченному представителю, другой экземпляр остается в Удостоверяющем центре.

2) Передает владельцу сертификата или его уполномоченному представителю ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи. Указанный ключевой носитель передается владельцу сертификата или его уполномоченному представителю под расписку и записью в соответствующих журналах поэкземплярного учета Удостоверяющего центра, в том числе журнале учета сертификатов ключей проверки электронной подписи. Удостоверяющий центр не осуществляет хранение ключа электронной подписи заявителя в Удостоверяющем центре или его копирование на иные ключевые носители, не принадлежащие заявителю.

3) Информирует владельца сертификата или его уполномоченного представителя 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, в соответствии с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенном в приложении № 20 настоящего Порядка.

4) Вносит в реестр сертификатов Удостоверяющего центра информацию о выданном квалифицированном сертификате и сведения о владельце сертификата.

5) Направляет в единую систему идентификации и аутентификации сведения о владельце сертификата, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

6.5.8. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата заявителя.

6.5.8.1. Срок создания и выдачи Удостоверяющим центром квалифицированного сертификата заявителя с момента получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, а также надлежаще оформленных документов и сведений, представленных заявителем в Удостоверяющий центр для получения квалифицированного сертификата, зависит от сроков и результатов получения сведений, запрашиваемых Удостоверяющим центром с использованием инфраструктуры в соответствии частью 2.2 и частью 2.3 статьи 18 Федерального закона «Об электронной подписи» из государственных информационных ресурсов, но не может превышать 30 (тридцати) дней со дня получения Удостоверяющим центром заявления на создание и выдачу квалифицированного сертификата, если иное не определено договором оказания услуг или дополнительным соглашением, заключаемым с заявителем.

6.5.8.2. Выдача квалифицированных сертификатов, созданных Удостоверяющим центром, осуществляется при условии выполнения Стороной, присоединившейся к Порядку, своих обязанностей.

6.6. Подтверждение действительности электронной подписи, использованной для подписания электронного документа.

По обращению участника электронного взаимодействия Удостоверяющий центр осуществляет проведение экспертных работ по проверке действительности усиленной квалифицированной электронной подписи, использованной для подписания электронных документов, созданного с использованием ключа электронной подписи, соответствующего квалифицированному сертификату, выданного Удостоверяющим центром.

6.6.1. Требования к заявлению на подтверждение действительности электронной подписи и перечень прилагаемых к такому заявлению документов.

Подтверждение электронной подписи в электронном документе осуществляется

Удостоверяющим центром по обращению граждан (далее по тексту раздела – заявитель), на основании заявления на подтверждение электронной подписи в электронном документе в простой письменной форме.

Заявление на подтверждение электронной подписи в электронном документе подается заявителем в ЦР Удостоверяющего центра лично.

6.6.1.1. Перечень документов, прилагаемых к заявлению на подтверждение действительности электронной подписи.

Обязательным приложением к заявлению на подтверждение электронной подписи в электронном документе является машинный (оптический) носитель информации, содержащий следующие файлы:

- файл, содержащий электронный документ, к которому применена электронная подпись;
- файл, содержащий электронную подпись формата PKCS#7 электронного документа, к которому применена электронная подпись;
- сертификат ключа проверки электронной подписи лица, подписавшего электронный документ, либо ключ проверки электронной подписи, соответствующий сертификату ключа проверки электронной подписи лица, подписавшего электронный документ;
- сертификат ключа проверки электронной подписи уполномоченного лица УЦ, являющегося издателем сертификата ключа проверки электронной подписи электронной подписи электронного документа.

6.6.1.2. Удостоверяющий центр имеет право отказать заявителю в проведении проверки действительности электронной подписи в электронном документе в следующих случаях:

- заявитель не предоставил для проведения проверки действительности электронной подписи необходимые документы (файлы) или их формат не соответствует требованиям;
- заявление не содержит необходимой информации или содержит трудноразличимый текст;

- квалифицированный сертификат, с использованием которого необходимо проверить действительность электронной подписи в электронном документе, выдан не Удостоверяющим центром.

В случае отказа в проведении проверки действительности электронной подписи в электронном документе Удостоверяющий центр в течение 1 (одного) рабочего дня после принятия решения об отказе направляет заявителю уведомление в форме документа на бумажном носителе, подписанного собственноручной подписью уполномоченного лица Удостоверяющего центра, либо в форме электронного документа, подписанного усиленной квалифицированной электронной подписью уполномоченного лица Удостоверяющего центра, с информацией, содержащей причины отказа в проведении проверки действительности электронной подписи в электронном документе.

6.6.2. Срок предоставления услуги по подтверждению действительности электронной подписи в электронном документе.

Срок рассмотрения заявления и процедура подтверждения электронной подписи в электронном документе определяется в соответствии с документом «Положение о порядке разбора конфликтных ситуаций, связанных с использованием электронной подписи».

6.6.3. Порядок оказания услуги по подтверждению действительности электронной подписи в электронном документе.

6.6.3.1. После поступления от заявителя заявления на подтверждение действительности электронной подписи в электронном документе и его регистрации в Удостоверяющем центре осуществляется проверка заявления и приложенных к нему документов.

6.6.3.2. В целях проведения экспертизы по проверке действительности электронной подписи в электронном документе создается комиссия, сформированная из числа сотрудников Удостоверяющего центра.

6.6.3.3. При проведении экспертизы по проверке действительности электронной подписи в электронном документе выполняется проверка действительности всех квалифицированных сертификатов, включенных в последовательность проверки от проверяемого квалифицированного сертификата до квалифицированного сертификата Удостоверяющего центра, выданного ему головным удостоверяющим центром.

6.6.3.4. По результатам проведения экспертизы по проверке действительности электронной подписи в электронном документе комиссией составляется заключение, которое содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа проверки электронной подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе;
- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основание для проведения проверки (экспертизы);
- состав комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, которые должны были быть разрешены при проведении проверки (экспертизы);
- результаты проверки (экспертизы) с указанием примененных методов.

6.6.3.5. Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов и печатью Удостоверяющего центра.

6.6.4. Процедура подтверждения электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи.

6.6.4.1. Владелец сертификата, заинтересованный в получении информации о статусе квалифицированного сертификата, выданного Удостоверяющим центром, имеет право направить в Удостоверяющий центр запрос в форме документа на бумажном носителе.

6.6.4.2. Подтверждение электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи осуществляется Удостоверяющим центром по обращению граждан (далее по тексту раздела – заявитель) на основании заявления по форме Приложений №№ 18, 19 настоящего Порядка.

6.6.4.3. Заявление должно содержать следующую информацию:

- 1) дата подачи заявления;
- 2) время и дата (либо период времени), на момент наступления которых требуется установить статус квалифицированного сертификата.

Заявление на подтверждение электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи подается заявителем в ЦР Удостоверяющего центра лично.

Обязательным приложением к заявлению на подтверждение электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи является машинный (оптический) носитель информации, содержащий следующие файлы:

- сертификат ключа проверки электронной подписи зарегистрированного пользователя УЦ, подвергающийся процедуре проверки;
- сертификат ключа проверки электронной подписи уполномоченного лица УЦ, являющегося издателем сертификата ключа проверки электронной подписи пользователя УЦ, подвергающегося процедуре проверки.

6.6.4.4. Срок рассмотрения заявления на подтверждение электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи составляет 5 рабочих дней с момента его поступления в ЦР Удостоверяющего центра.

6.6.4.5. В случае отказа от подтверждения электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи заявителю возвращается заявление на подтверждение электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи с резолюцией ответственного сотрудника ГКУ ТО «ЦИТТО» и предоставленные заявителем материалы.

6.6.4.6. Результатом проведения работ по подтверждению электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи является заключение, которое содержит:

- результат проверки соответствующим сертифицированным средством электронной подписи уполномоченного лица УЦ на сертификате ключа проверки электронной подписи и отсутствия искажений в подписанным данной электронной подписью сертификате ключа проверки электронной подписи;
- детальный отчет по выполненной проверке.

Детальный отчет по выполненной проверке включает следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основание для проведения проверки (экспертизы);
- состав комиссии экспертов (фамилия, имя, отчество, образование, специальность, стаж работы, ученая степень и/или ученое звание, занимаемая должность), которым поручено проведение проверки (экспертизы);
- вопросы, которые должны были быть разрешены при проведении проверки (экспертизы);
- результаты проверки (экспертизы) с указанием примененных методов.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью. Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов и печатью Удостоверяющего центра.

6.6.5. Механизм доказательства обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи.

6.6.5.1. Заявления на создание сертификатов ключей проверки электронной подписи, поступающие в Удостоверяющий центр от владельцев ключей подписи должны содержать собственноручную подпись заявителя и, в качестве реквизита, запрос на сертификат, подготовленный в соответствии с форматом криптографических сообщений PKCS#10 в формате Base64. Подтверждение электронной подписи запроса на сертификат и наличие собственноручной подписи заявителя в заявлении на создание сертификата ключа проверки электронной подписи подтверждает, что заявитель является владельцем ключа электронной подписи, соответствующего ключу проверки электронной подписи из запроса на сертификат.

6.7. Процедуры, осуществляемые при прекращении действия и аннулировании

квалифицированного сертификата.

6.7.1. Основания прекращения действия или аннулирования квалифицированного сертификата.

6.7.1.1. Квалифицированный сертификат прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности 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, настоящим Порядком или соглашением между Удостоверяющим центром и владельцем сертификата.

6.7.1.2. Удостоверяющий центр признает квалифицированный сертификат аннулированным, в следующих случаях:

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

6.7.2. Порядок действий Удостоверяющего центра при прекращении действия (аннулировании) квалифицированного сертификата.

6.7.2.1. Порядок подачи и приема заявления о прекращении действия квалифицированного сертификата

6.7.2.1.1. Порядок подачи в Удостоверяющий центр заявления о прекращении действия квалифицированного сертификата.

6.7.2.1.1.1. Аннулирование (отзыв) сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению на прекращение действия сертификата ключа проверки электронной подписи его владельца (далее по тексту раздела – заявитель).

Заявление на прекращение действия сертификата ключа проверки электронной подписи подается заявителем в бумажной форме в ЦР Удостоверяющего центра лично.

6.7.2.1.1.2. Заявление о прекращении действия квалифицированного сертификата направляется заявителем в Удостоверяющий центр в случае:

- принятия Стороной, присоединившейся к Порядку, решения о прекращении действия квалифицированного сертификата владельца сертификата;
- договорные отношения, определенные настоящим Порядком, прекращаются по

инициативе Стороны, присоединившейся к Порядку, в соответствии с пунктом 2.1.7 настоящего Порядка;

- изменились сведения о владельце сертификата, в результате которых сведения, внесенные в квалифицированный сертификат, перестали быть достоверными;
- прекращения полномочий владельца сертификата;
- нарушена конфиденциальность ключа электронной подписи владельца сертификата.

6.7.2.1.1.3. Требования к заявлению о прекращении действия квалифицированного сертификата.

Заявление на прекращение действия сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе по форме Приложений №№ 12, 13 настоящего Порядка, заверенный собственноручной подписью заявителя. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер отзываемого сертификата;
- причину отзыва сертификата;
- дата и подпись заявителя.

6.7.2.1.2. Порядок приема Удостоверяющим центром заявления о прекращении действия квалифицированного сертификата.

6.7.2.1.2.1. После поступления заявления о прекращении действия квалифицированного сертификата и его регистрации в Удостоверяющем центре осуществляется:

- проверка заявления на соответствие требованиям, указанным в пункте 6.7.2.1.1.3 настоящего Порядка;
- проверка соответствия сведений, указанных в заявлении, и сведений, которые имеются в Удостоверяющем центре о владельце сертификата и выданном ему квалифицированном сертификате;
- проверка полномочий владельца сертификата и (или) лица, обратившегося с заявлением о прекращении действия квалифицированного сертификата.

6.7.2.2. Порядок внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов.

6.7.2.2.1. После проверки заявления и полномочий владельца сертификата и (или) лица, обратившегося для прекращения действия квалифицированного сертификата, Удостоверяющий центр:

- выполняет процедуру прекращения действия квалифицированного сертификата;
- вносит информацию о прекращении действия квалифицированного сертификата в реестр сертификатов Удостоверяющего центра.

6.7.2.2.2. Структура списка отзываемых сертификатов, создаваемого УЦ в электронной форме.

Удостоверяющий центр издает списки отзываемых сертификатов ключей проверки электронной подписи пользователей УЦ и уполномоченного лица Удостоверяющего центра в электронной форме (далее по тексту раздела – СОС).

СОС (CRL) представляет собой структуру электронных данных файла формата X.509 v2 (версии 2), включающих в свой состав список серийных номеров аннулированных (отозванных) или приостановленных сертификатов с указанием для каждого номера сертификата времени его отзыва.

В СОС обязательно указываются время его издания и время, когда будет выпущен СОС с более свежей информацией. В сертификаты пользователей УЦ включено дополнение - CDP (CRL Distribution Point - точка распространения СОС).

СОС подписывается ключом подписи уполномоченного лица Удостоверяющего центра.

СОС не отражает информацию о статусах сертификатов в реальном времени.

Формат списка отзываемых сертификатов включает себя следующие поля:

Базовые поля списка отзываемых сертификатов	
Version	Версия
Issuer	Издатель СОС
thisUpdate	Дата выпуска текущего СОС
nextUpdate	Дата выпуска следующего СОС
revokedCertificates	Список отзываемых сертификатов
signatureAlgorithm	Алгоритм подписи
Issuer Sign	Подпись издателя СОС
Расширения списка отзываемых сертификатов	
Authority Key Identifier	Идентификатор ключа Удостоверяющего центра
cRLNumber	Номер списка отзываемых сертификатов
certificateSerialNumber	Серийный номер сертификата
revocationDate	Дата отзыва сертификата
Reason Code	Код причины отзыва сертификата "0" Не указана "1" Компрометация ключа (нарушение конфиденциальности ключа) "2" Компрометация ЦС (нарушение конфиденциальности ключа Удостоверяющего центра) "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия

6.7.2.2.3. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр

сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 6.7.1 настоящего Порядка, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.7.2.2.4. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов Удостоверяющего центра.

6.7.2.2.5. Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате.

6.7.2.2.6. Информация о адресах публикации списка отозванных сертификатов указывается в квалифицированных сертификатах, созданных Удостоверяющим центром, и включается в расширение «Точка распределения списка отзыва» («CRL Distribution Point») квалифицированного сертификата.

6.7.2.2.7. Оповещение участников электронного взаимодействия о факте прекращения действия квалифицированного сертификата осуществляется Удостоверяющим центром путем опубликования первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения о квалифицированном сертификате, который аннулирован или действие которого прекращено, и изданного не ранее времени наступления произошедшего случая. Временем оповещения о прекращении действия квалифицированного сертификата является время издания указанного списка отозванных сертификатов, хранящееся в поле «Действителен с» («thisUpdate») списка отозванных сертификатов.

6.7.2.2.8. В случае прекращения действия квалифицированного сертификата по истечению срока его действия временем прекращения действия квалифицированного сертификата является время, хранящееся в поле «Действителен по» («NotAfter») квалифицированного сертификата. В этом случае информация о квалифицированном сертификате, действие которого прекращено, в список отозванных сертификатов не заносится.

6.7.2.2.9. В случае внеплановой смены ключа электронной подписи Удостоверяющего центра в связи с нарушением его конфиденциальности временем прекращения действия квалифицированного сертификата Удостоверяющего центра является время нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра, при этом прекращение действия квалифицированного сертификата Удостоверяющего центра осуществляется уполномоченным федеральным органом. Информация о прекращении действия квалифицированного сертификата Удостоверяющего центра включается в список отозванных сертификатов, который публикуется головным удостоверяющим центром.

6.7.2.3. В случае аннулирования в соответствии с пунктом 6.7.1.2 настоящего Порядка квалифицированного сертификата, выданного Удостоверяющим центром,

Удостоверяющий центр уведомляет владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра.

Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием.

6.7.3. Приостановление действия сертификата ключа проверки электронной подписи.

Приостановление действия сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению на приостановление действия сертификата ключа проверки электронной подписи его владельца (далее по тексту раздела – заявитель). Заявление на приостановление действия сертификата ключа проверки электронной подписи подается заявителем в бумажной или устной форме в ЦР Удостоверяющего центра.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в бумажной форме подается заявителем в ЦР Удостоверяющего центра лично. Заявление на приостановление действия сертификата ключа проверки электронной подписи в устной форме подается заявителем в Удостоверяющий центр посредством телефонной связи с аутентификацией владельца сертификата по кодовой фразе.

6.7.3.1. Приостановление действия сертификата ключа проверки электронной подписи и официальное уведомление пользователя УЦ о приостановлении действия сертификата должны быть осуществлены в течение двенадцати часов с момента подачи в Удостоверяющий центр заявления на приостановление действия.

6.7.3.2. Официальным уведомлением о приостановлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено.

Заявление на приостановление действия сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе по форме Приложений №№ 14, 15 настоящего Порядка, заверенный собственноручной подписью заявителя. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого приостанавливается;
- срок, на который приостанавливается действие сертификата;
- причина приостановки действия сертификата;
- дата и подпись заявителя.

6.7.4. Порядок возобновления действия сертификата ключа проверки электронной подписи.

Возобновление действия сертификата ключа проверки электронной подписи, созданного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению на возобновление действия сертификата ключа проверки электронной подписи его владельца. Заявление на возобновление действия сертификата ключа проверки электронной подписи подается заявителем бумажной форме. Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме подается заявителем в ЦР Удостоверяющего центра лично.

6.7.4.1. Возобновление действия сертификата ключа проверки электронной подписи и официальное уведомление пользователя УЦ о возобновлении действия сертификата должны быть осуществлены не позднее 3 рабочих дней, следующих за рабочим днем, в течение которого было принято заявление Удостоверяющим центром.

6.7.4.2. Официальным уведомлением о возобновлении действия сертификата ключа проверки электронной подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа проверки электронной подписи признается время издания списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено.

Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе по форме Приложений №№ 16, 17 настоящего Порядка, заверенный собственноручной подписью заявителя. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого возобновляется;
- причина возобновления действия сертификата;
- дата и подпись заявителя.

6.8. Порядок ведения реестра сертификатов Удостоверяющего центра.

6.8.1. Формирование и ведение реестра сертификатов Удостоверяющего центра.

6.8.1.1. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром в соответствии с Федеральным законом «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 Минкомсвязи России от 22 августа 2017 г. № 436, иными принимаемыми в соответствии с Федеральным законом «Об электронной подписи» и Федеральным законом «Об информации, информационных технологиях и о защите информации» нормативными правовыми актами и настоящим Порядком.

6.8.1.2. Формирование реестра сертификатов включает в себя внесение квалифицированных сертификатов, выданных Удостоверяющим центром, в реестр сертификатов.

6.8.1.3. Ведение реестра сертификатов включает в себя:

- внесение изменений в реестр сертификатов в случае изменения содержащихся в нем сведений;
- внесение в реестр сертификатов сведений о прекращении действия или об аннулировании квалифицированных сертификатов.

6.8.1.4. Хранение информации, содержащейся в реестре сертификатов, осуществляется Удостоверяющим центром в форме, позволяющей проверить ее целостность и достоверность.

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

6.8.1.6. Формирование и ведение реестра сертификатов осуществляется Удостоверяющим центром с соблюдением требований к мерам и способам защиты информации, обеспечивающих предотвращение несанкционированного доступа к нему.

6.8.1.7. В целях обеспечения целостности информации, в том числе предотвращения утраты сведений о квалифицированных сертификатах, содержащихся в реестре сертификатов, Удостоверяющий центр осуществляет резервное копирование баз данных, обрабатываемых с использованием сертифицированных средств Удостоверяющего центра, а также реестра сертификатов.

6.8.1.8. Удостоверяющий центр обеспечивает актуальность информации, содержащейся в реестре сертификатов.

6.8.1.9. Удостоверяющий центр обеспечивает любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет, к реестру сертификатов в любое время в течение срока деятельности Удостоверяющего центра.

6.8.1.10. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов и направляется обратившемуся лицу как в форме документа на бумажном носителе с использованием почтового отправления, так и в форме электронного документа с использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты (по выбору лица, обратившегося за получением информации из реестра сертификатов).

Срок предоставления Удостоверяющим центром запрошенной заявителем информации, содержащейся в реестре сертификатов, не превышает 7 (семи) дней со дня получения запроса от заявителя, в случае, если Удостоверяющий центр направляет запрошенную информацию в форме документа на бумажном носителе с использованием почтового отправления, и 24 (двадцати четырех) часов для направления выписки посредством информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

6.8.1.11. В процессе реализации функций Удостоверяющего центра и исполнения обязанностей Удостоверяющий центр осуществляет также формирование и ведение

реестра Пользователей УЦ, который в том числе содержит:

- информацию о Пользователях УЦ, владельцах сертификатов, выданных им квалифицированных сертификатах, в том числе прекративших действие и аннулированных сертификатах;
- реестр запросов на создание Пользователей УЦ, квалифицированных сертификатов, а также запросов на прекращение их действия (аннулирование);
- реестр списка отзываемых сертификатов в электронном виде за все время деятельности Удостоверяющего центра;
- Реестр Пользователей УЦ ведется в электронном виде с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

6.8.1.12. Информация, внесенная в реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

6.8.1.13. В случае принятия решения о прекращении своей деятельности Удостоверяющий центр обязан передать в уполномоченный федеральный орган реестр сертификатов в соответствии с 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 Минкомсвязи России от 14 августа 2017 г. № 416.

6.8.2. Формы ведения реестра сертификатов.

6.8.2.1. Реестр сертификатов Удостоверяющего центра включает реестр сертификатов юридических лиц и реестр сертификатов физических лиц.

6.8.2.2. Реестр сертификатов юридических лиц состоит из следующих разделов:

квалифицированные сертификаты, выданные юридическим лицам;

квалифицированные сертификаты, выданные юридическим лицам, прекратившие свое действие;

аннулированные квалифицированные сертификаты, выданные юридическим лицам.

6.8.2.2.1. Раздел «квалифицированные сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- 5) реквизиты документа, подтверждающего факт внесения записи в Единый государственный реестр юридических лиц (для юридических лиц,

зарегистрированных на территории Российской Федерации);

6) основные реквизиты (наименование, номер и дата выдачи) доверенности или иного документа, подтверждающего право заявителя действовать от имени других лиц;

7) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;

8) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

6.8.2.2. Раздел «квалифицированные сертификаты, выданные юридическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) дата прекращения действия квалифицированного сертификата;
- 5) основание прекращения действия квалифицированного сертификата.

6.8.2.2.3. Раздел «аннулированные квалифицированные сертификаты, выданные юридическим лицам» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) наименование, место нахождения и основной государственный регистрационный номер владельца квалифицированного сертификата;
- 4) дата аннулирования квалифицированного сертификата;
- 5) основание аннулирования квалифицированного сертификата.

6.8.2.3. Реестр сертификатов физических лиц состоит из следующих разделов:

- квалифицированные сертификаты, выданные физическим лицам;
- квалифицированные сертификаты, выданные физическим лицам, прекратившие свое действие;
- аннулированные квалифицированные сертификаты, выданные физическим лицам.

6.8.2.3.1. Раздел «квалифицированные сертификаты, выданные физическим лицам» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;

- 4) страховой номер индивидуального лицевого счета и идентификационный номер налогоплательщика владельца квалифицированного сертификата;
- 5) сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать по поручению третьих лиц, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;
- 6) ограничения использования квалифицированного сертификата (если такие ограничения устанавливаются).

6.8.2.3.2. Раздел «квалифицированные сертификаты, выданные физическим лицам, прекратившие свое действие» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- 4) дата прекращения действия квалифицированного сертификата;
- 5) основание прекращения действия квалифицированного сертификата.

6.8.2.3.3. Раздел «аннулированные квалифицированные, выданные физическим лицам» содержит следующие обязательные поля:

- 1) уникальный номер квалифицированного сертификата;
- 2) даты начала и окончания действия квалифицированного сертификата;
- 3) фамилия, имя и отчество (если имеется) владельца квалифицированного сертификата;
- 4) дата аннулирования квалифицированного сертификата;
- 5) основание аннулирования квалифицированного сертификата.

6.8.3. Сроки внесения информации о прекращении действия или аннулировании квалифицированного сертификата в реестр сертификатов.

6.8.3.1. Информация о выданных Удостоверяющим центром квалифицированных сертификатах вносится в реестр сертификатов одновременно с их выдачей, но не позднее даты начала действия квалифицированного сертификата, указанной в квалифицированном сертификате.

6.8.3.2. Информация о прекращении действия и аннулировании квалифицированного сертификата вносится Удостоверяющим центром в реестр сертификатов Удостоверяющего центра в течение 12 (двенадцати) часов с момента наступления обстоятельств, указанных в пункте 6.7.1 настоящего Порядка, или в течение 12 (двенадцати) часов с момента, когда Удостоверяющему центру стало известно или должно было стать известно о наступлении таких обстоятельств.

6.8.3.3. Информация об аннулировании квалифицированного сертификата вносится Удостоверяющим центрами в реестр сертификатов не позднее 1 (одного) рабочего дня со дня вступления в законную силу решения суда, явившегося основанием

для аннулирования, а также при аннулировании Удостоверяющим центром квалифицированных сертификатов по основаниям, указанным в пунктах 1 и 2 части 6.1 статьи 14 Федерального закона «Об электронной подписи»:

- не подтверждено, что владелец сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;
- установлено, что содержащийся в квалифицированном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате.

6.8.3.4. В случае аннулирования в соответствии с пунктом 6.7.1.2 настоящего Порядка квалифицированного сертификата, выданного Удостоверяющим центром, Удостоверяющий центр уведомляет владельца сертификата не менее чем за 1 (один) рабочий день до внесения в реестр сертификатов Удостоверяющего центра информации об аннулировании квалифицированного сертификата путем направления документа на бумажном носителе или электронного документа, подписанного усиленной квалифицированной подписью уполномоченного лица Удостоверяющего центра.

6.9. 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) 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 Удостоверяющего центра.

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

6.9.1. Максимальные сроки проведения технического обслуживания.

Техническое обслуживание реестра сертификатов при проведении плановых технических работ осуществляется не более 8 (восьми) часов с момента их начала.

Техническое обслуживание реестра сертификатов при проведении внеплановых технических работ осуществляется не более 24 (двадцати четырех) часов с момента их начала.

Время проведения технического обслуживания может быть увеличено при наличии объективных оснований и причин, но не более чем на 5 (пять) дней со дня их начала, если такие работы могут повлиять на возможность создания или проверки электронной подписи участниками электронного взаимодействия.

Перед проведением 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 и (или) направлением уведомления в электронной форме с использованием информационно-телекоммуникационных сетей, в том числе с использованием электронной почты.

7. Порядок исполнения обязанностей Удостоверяющего центра.

7.1. 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.

7.1.1. 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 № 20 к настоящему Порядку.

7.1.2. Удостоверяющий центр осуществляет информирование Стороны, присоединившейся к Порядку УЦ, в том числе Пользователей УЦ и владельцев сертификатов, 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 следующими способами:

1) Удостоверяющий центр информирует всех участников электронного взаимодействия 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 настоящего Порядка, а также руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи, которое приведено в приложении № 20 к настоящему Порядку УЦ, отдельным документом в электронной форме на сайте Удостоверяющего центра;

2) Сторона, присоединившаяся к Порядку, обязана ознакомится с настоящим Порядком и всеми приложениями к нему, в том числе с руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, о чем подтверждает путем подписания заявления о присоединении к Порядку УЦ, по форме, приведенной в приложении № 1 или приложении № 2 к Порядку УЦ;

3) заявитель, при оформлении заявления на создание и выдачу квалифицированного сертификата по форме, приведенной в приложении № 3 или приложении № 4 к настоящему Порядку предоставляет также согласие на обработку персональных данных, которое собственноручно подписывает лицо, указанное в заявлении на создается создание и выдачу квалифицированного сертификата, и, в том числе, подтверждает, что с настоящим Порядком и всеми приложениями к нему, в том числе с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи, ознакомлен;

4) При выдаче квалифицированного сертификата в соответствии с пунктом 6.5.7.4,

Удостоверяющий центр одновременно с выдачей квалифицированного сертификата информирует лицо, обратившееся за получением квалифицированного сертификата, 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, и под расписку выдает краткое руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, а также, по согласованию с владельцем сертификата или его уполномоченным представителем, направляет владельцу сертификата или записывает на носитель информации, предоставленный заявителем, документацию в форме электронных документов, в том числе содержащую:

руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, приведенное в приложении № 20 к Порядку УЦ, содержащее информацию о 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;

инструкцию по использованию средства электронной подписи, входящую в состав эксплуатационной документации на средство электронной подписи (по желанию владельца сертификата и при наличии в Удостоверяющем центре документации на средство электронной подписи, которое использует владелец сертификата);

5) Удостоверяющий центр оказывает техническую поддержку Пользователей УЦ и осуществляет предоставление консультаций по вопросам использования электронной подписи и средств электронной подписи, в том числе по вопросам обеспечения безопасности при использовании электронной подписи и средств электронной подписи.

7.2. Выдача по обращению заявителя средств электронной подписи.

7.2.1. Средства электронной подписи, используемые заявителем, должны соответствовать требованиям частью 4 статьи 6 и статьи 12 Федерального закона «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 усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

7.2.2. Выдача Удостоверяющим центром сертифицированных по требованиям безопасности средств электронной подписи, которые выдаются на безвозмездной основе и приобретаются за счет бюджета Тюменской области, органам власти Тюменской области и органам местного самоуправления Тюменской области, а также подведомственным им организациям и учреждениям, в пределах их потребности и при наличии данных средств электронной подписи в Удостоверяющем центре.

7.2.3. Порядок использования средств электронной подписи определяются

эксплуатационной документацией на средство электронной подписи и лицензионным соглашением, условия которой определяет правообладатель.

7.3. Обеспечение актуальности информации, содержащейся в реестре сертификатов, а также ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

7.3.1. 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.

7.3.2. Актуальность информации, содержащейся в реестре сертификатов, обеспечивается путем соблюдения порядка формирования и ведения реестра сертификатов в соответствии с пунктом 6.8 настоящего Порядка.

7.3.3. 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.

7.3.4. Мероприятия по обеспечению защиты информации, при её обработке с использованием средств Удостоверяющего центра, осуществляются в том числе в соответствии с требованиями федеральных законов «Об информации, информационных технологиях и о защите информации», «О персональных данных», Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 года № 21, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10 июля 2014 года № 378, Требованиями к средствам электронной подписи и Требованиями к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, Инструкцией ФАПСИ № 152.

7.3.5. Обработка информации осуществляется с использованием средств Удостоверяющего центра, соответствующих Требованиям к средствам электронной подписи и Требованиям к средствам удостоверяющего центра, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 796, прошедших оценку соответствия по требованиям безопасности информации.

7.3.6. Защита информации, содержащейся в реестре сертификатов Удостоверяющего центра, осуществляется, в частности, 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).

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

7.4.1. Удостоверяющий центр в соответствии с пунктом 3 части 2 статьи 13 и частью 3 статьи 15 Федерального закона «Об электронной подписи» обеспечивает безвозмездный круглосуточный доступ к реестру сертификатов, опубликованному на сайте Удостоверяющего центра, при обращении к нему любого лица с использованием сети «Интернет» в любое время, за исключением периодов технического обслуживания реестра сертификатов, проводимых Удостоверяющим центром в соответствии с пунктом 6.9 настоящего Порядка.

7.4.2. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов в соответствии с пунктом 6.8.1.10 настоящего Порядка.

7.4.3. В соответствии с Порядком формирования и ведения реестров выданных аккредитованными Удостоверяющими центрами квалифицированных сертификатов ключей проверки электронной подписи, а также предоставления информации из таких реестров, утвержденным приказом Минкомсвязи России от 22 августа 2017 г. № 436, доступ заинтересованных лиц к реестру квалифицированных сертификатов с использованием информационно-телекоммуникационных сетей осуществляется путем

размещения, формирования и ведения реестра квалифицированных сертификатов в информационной системе головного Удостоверяющего центра, являющейся составной частью инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Доступ заинтересованных лиц к информационной системе головного Удостоверяющего центра с целью получения сведений из реестра квалифицированных сертификатов осуществляется с использованием федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» на безвозмездной основе.

7.4.4. Удостоверяющий центр обеспечивает доступность и целостность информации, опубликованной на сайте Удостоверяющего центра, в том числе реестра сертификатов, квалифицированных сертификатов Удостоверяющего центра, списка отзывающихся сертификатов.

7.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей.

7.5.1. Порядок обеспечения конфиденциальности ключей электронных подписей уполномоченных лиц Удостоверяющего центра и ключа электронной подписи Удостоверяющего центра.

7.5.1.1. 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.

7.5.1.2. Хранение и использование ключей электронной подписи Удостоверяющего центра и ключей электронной подписи уполномоченных лиц Удостоверяющего центра осуществляется в соответствии с требованиями с Инструкции ФАПСИ № 152, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 02 марта 2001 г. № 28, в форме, позволяющей обеспечить целостность и конфиденциальность ключей электронной подписи Удостоверяющего центра.

7.5.1.3. 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.

7.5.1.4. Ключи электронной подписи Удостоверяющего центра и уполномоченных лиц Удостоверяющего центра выводятся из эксплуатации при окончании срока их действия. Временное их хранение не осуществляется.

7.5.2. Порядок обеспечения конфиденциальности ключей электронных подписей заявителей.

7.5.2.1. Конфиденциальность ключей электронных подписей заявителей обеспечивается Удостоверяющим центром в период времени получения носителя ключевой информации от заявителя или его уполномоченного представителя и записи на него ключей электронной подписи, созданных Удостоверяющим центром, до момента передачи ключевого носителя заявителю или его уполномоченному представителю, при этом создание и запись ключа электронной подписи на ключевой носитель, представленный заявителем или его уполномоченным представителем осуществляется Удостоверяющим центром только в случае личного прибытия заявителя или его уполномоченного представителя в Удостоверяющий центр и в его присутствии.

7.5.2.2. Выдача ключей электронной подписи заявителю или его уполномоченному представителю осуществляется Удостоверяющим центром в порядке, определенном в пункте 6.1.2 и 6.5.7.4 настоящего Порядка.

7.5.2.3. После создания Удостоверяющим центром ключа электронных подписи заявителя и записи на носитель ключевой информации, представленный непосредственно перед созданием ключа электронных подписи заявителем или его уполномоченным представителем, данный носитель ключевой информации, в том числе содержащий ключ электронной подписи, указанный ключевой носитель выдается заявителю или его уполномоченному представителю под расписку, при этом вносится запись в соответствующий журнал учета Удостоверяющего центра о выдаче ключа электронной подписи и соответствующего ему квалифицированного сертификата, с которой заявитель или его уполномоченный представитель должен быть ознакомлен под расписку.

7.5.2.4. Создание ключей электронной подписи заявителя осуществляется с использованием средств Удостоверяющего центра, прошедших оценку соответствия по требованиям безопасности информации.

7.5.2.5. Удостоверяющий центр не осуществляет хранение (в том числе временное хранение) ключей электронной подписи, а также носителей ключевой информации, содержащих ключи электронной подписи заявителя (владельца сертификата).

7.5.2.6. В случае, если заявитель направил в Удостоверяющий в электронном виде ключ электронной подписи по информационно-телекоммуникационной сети или иными способами, не гарантирующими обеспечение конфиденциальности ключа электронной подписи, такой ключ считается скомпрометированным в связи с нарушением конфиденциальность ключа электронной подписи, при этом заявитель обязан провести процедуру его внеплановой смены. В случае наличия действующего квалифицированного сертификата, соответствующего указанному ключу электронной подписи, такой квалифицированный сертификат прекращает действие, при этом владелец сертификата обязан обратиться в Удостоверяющий центр с заявлением о прекращении его действия в соответствии с пунктом 6.4.3 и 6.7.1 настоящего Порядка.

7.5.2.7. Владелец сертификата, 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.

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

7.6.1. 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 Федерального закона «Об электронной подписи».

7.6.2. 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;
- 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 владельцем квалифицированного сертификата;
- реквизиты документа, удостоверяющего личность владельца квалифицированного сертификата, в том числе серия и номер документа,

удостоверяющего личность, код подразделения, выдавшего документ, дата выдачи;

- идентификационный номер налогоплательщика;
- адрес регистрации (места жительства);
- дата рождения владельца квалифицированного сертификата;
- место рождения владельца квалифицированного сертификата;
- пол владельца квалифицированного сертификата;
- гражданство владельца квалифицированного сертификата;
- основной государственный регистрационный номер юридического лица;
- идентификационный номер налогоплательщика юридического лица;
- адрес электронной почты (по желанию);
- номер мобильного телефона (только при регистрации или подтверждении его учетной записи владельца сертификата – физического лица при его желании в единой системе идентификации и аутентификации).

7.6.3. В соответствии с требованиями статьи 6 и статьи 9 Федерального закона «О персональных данных» Удостоверяющий центр осуществляет регистрацию в единой системе идентификации и аутентификации лица, которое указанное в предоставляемом заявителем заявлении на создание и выдачу квалифицированного сертификата (владелец сертификата), в соответствии с предоставляемым этим лицом согласием на обработку персональных данных, приведенным в приложении № 3 и приложении № 4 к настоящему Порядку.

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

7.7.1. 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.

7.7.2. Основанием для регистрации или подтверждения учетной записи служит заявление владельца сертификата, содержащее сведения необходимые для регистрации или подтверждения учетной записи в единой системе идентификации и аутентификации, а также согласие на обработку персональных данных, предоставляемое владельцем сертификата. Форма соответствующих заявлений предоставляется Удостоверяющим центром при выполнении процедуры регистрации владельца сертификата в единой системе идентификации и аутентификации или подтверждения его учетной записи, которая осуществляется Удостоверяющим центром при личном прибытии владельца сертификата в Удостоверяющий центр.

7.7.3. 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.

7.8. Предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре сертификатов.

7.8.1. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации, содержащейся в реестре сертификатов Удостоверяющего центра, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата путем публикации реестра сертификатов на сайте Удостоверяющего центра в форме электронного документа, который доступен для загрузки с использованием сети Интернет.

7.8.2. Актуальность и доступность реестра квалифицированных сертификатов, опубликованного на сайте Удостоверяющего центра в сети Интернет обеспечивается Удостоверяющим центром в соответствии с пунктом 7.3 и 7.4 настоящего Порядка соответственно.

7.8.3. Удостоверяющий центр предоставляет безвозмездно любому лицу по его обращению сведения, содержащиеся в реестре сертификатов, в том числе информацию об аннулировании квалифицированного сертификата. Указанная информация предоставляется в форме выписки из реестра сертификатов в соответствии с пунктом 6.8.1.10 настоящего Порядка.

7.8.4. Удостоверяющий центр предоставляет безвозмездно любому лицу доступ к информации о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, путем публикации актуального перечня прекративших свое действие (аннулированных) квалифицированных сертификатов в виде электронного документа (списка отозванных сертификатов), включающий в себя список серийных номеров квалифицированных сертификатов, которые аннулированы или действие которых было прекращено.

7.8.5. В целях обеспечения гарантированного доступа участников электронного взаимодействия к списку отозванных сертификатов Удостоверяющим центром обеспечивается публикация списка отозванных сертификатов на не менее чем двух независимых друг от друга ресурсах, размещаемых в сети Интернет, доступ к которым неограничен.

7.8.6. Адреса публикации списка отозванных сертификатов Удостоверяющего центра указывается в квалифицированных сертификатах, созданных Удостоверяющим центром.

7.8.7. Внесение информации о прекращении действия или аннулировании квалифицированного сертификата в реестр квалифицированных сертификатов осуществляется Удостоверяющим центром в соответствии с пунктом 6.7.2.2 настоящего Порядка.

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

7.9.1. Удостоверяющий центр оказывает услуги по предоставлению актуальной информации о статусе сертификатов ключей проверки электронной подписи посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам Пользователей Удостоверяющего центра формирует и предоставляет OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата ключа проверки электронной подписи. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов Удостоверяющего центра. OCSP-ответ признается действительным при одновременном выполнении следующих условий:

- Выполнены условия признания квалифицированной электронной подписи в OCSP-ответе;
- Квалифицированная электронная подпись в OCSP-ответе сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы актуальных статусов сертификатов, а именно: сертификат ключа проверки электронной подписи Службы актуальных статусов сертификатов в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.9 – «Подпись ответа службы OCSP».

Адрес обращения к Службе актуальных статусов сертификатов Удостоверяющего центра – <http://ocsp.72to.ru/ocsp2/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центров сертификатов ключей проверки электронной подписи.

7.9.2. Удостоверяющий центр оказывает услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Штамп времени, относящийся к подписанному электронной подписью электронному документу, признается действительным при одновременном выполнении следующих условий:

1. Выполнены условия признания квалифицированной электронной подписи в штампе времени;
2. Квалифицированная электронная подпись в штампе времени сформирована с учетом ограничения, содержащегося в сертификате ключа проверки электронной подписи Службы штампов времени, а именно: сертификат ключа проверки электронной подписи Службы штампов времени в расширении Extended Key Usage содержит информацию о данном ограничении в виде объектного идентификатора 1.3.6.1.5.5.7.3.8 – «Установка штампа времени».
3. Допустимые алгоритмы хэширования:
4. ГОСТ Р 34.11-94 идентификатор 1.2.643.2.2.9
5. ГОСТ Р 34.11-2012/256 идентификатор 1.2.643.7.1.1.2.2

Адрес обращения к Службе штампов времени – <http://tsp.72to.ru/tsp/tsp.srf>.

8. Прочие положения.

8.1. Прекращение деятельности Удостоверяющего центра.

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

В случае прекращения своей деятельности Удостоверяющий центр обязан:

- сообщить об этом в уполномоченный федеральный орган не позднее чем за 1 (один) месяц до даты прекращения своей деятельности;
- уведомить владельцев сертификатов ключей проверки электронной подписи, срок действия которых, не истек не позднее чем за 1 (один) месяц до даты прекращения своей деятельности;
- передать в уполномоченный федеральный орган в установленном порядке реестр сертификатов;
- передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в Удостоверяющем центре.

Передача реестра сертификатов и информации, подлежащей хранению в Удостоверяющем центре, осуществляется в соответствии с 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 Минкомсвязи России от 14 августа 2017 г. № 416.

8.2. Политика конфиденциальности.

8.2.1. Типы конфиденциальной информации.

К конфиденциальной информации, обрабатываемой в Удостоверяющем центре, относится:

- информация, обрабатываемая с использованием средств Удостоверяющего центра;
- ключи электронной подписи Удостоверяющего центра и ключи электронной подписи уполномоченных лиц Удостоверяющего центра;
- сведения о мерах и способах защиты инфраструктуры Удостоверяющего центра, включая идентифицирующую и аутентифицирующую информацию, информацию о среде функционирования технических и программных средств Удостоверяющего центра, средств защиты информации и шифровальных (криптографических) средств;
- техническая и эксплуатационная документация Удостоверяющего центра, в том числе содержащая информация о настройках средств Удостоверяющего центра, средств защиты информации, средств межсетевого экранирования, средств криптографической защиты информации;
- информация, содержащая персональные данные, за исключением:
- сведений, включаемых в квалифицированный сертификат, выданный Удостоверяющим центром;

- информации, содержащейся в реестре сертификатов;
- общедоступной информации и информации, включенной в общедоступные источники персональных данных.

Ключ электронной подписи является конфиденциальной информацией лица, являющегося владельцем соответствующего квалифицированного сертификата, выданного ему Удостоверяющим центром. Удостоверяющий центр не осуществляет хранение ключей электронных подписей владельцев сертификатов, в том числе их временное хранение. Ключи электронной подписи, создаваемые Удостоверяющим центром при личном присутствии заявителя или его уполномоченного представителя, непосредственно сразу после их изготовления передаются лично заявители или его уполномоченному представителю под расписку.

8.2.2. Типы информации, не являющейся конфиденциальной.

Удостоверяющий центр осуществляет обработку следующей информации, которая не является конфиденциальной:

- информация, подлежащая в соответствии с законодательством Российской Федерации размещению в сети Интернет, доступ к которой не ограничен, в том числе информация, являющаяся общедоступной информацией в соответствии со статьей 7 Федерального закона «Об информации, информационных технологиях и о защите информации» или информация, включенная в общедоступные источники персональных данных в соответствии со статьей 8 Федерального закона «О персональных данных», а также информация с письменного согласия субъекта персональных данных включенная в общедоступные источники персональных данных;
- информация, включаемая в квалифицированные сертификаты, выдаваемые Удостоверяющим центром, информация, содержащаяся в реестре сертификатов, а также информация, включаемая в списки отзываемых сертификатов Удостоверяющего центра;
- информация, содержащаяся в настоящем Порядке.

8.2.3. Типы информации, не подлежащей публикации.

Не подлежит публикации следующая информация о заявителях и владельцах сертификатов:

- сведения, направляемые Удостоверяющим центром в единую систему идентификации и аутентификации, в объеме, необходимом для регистрации сведений о владельце сертификата в единой системе идентификации и аутентификации, а также для регистрации или подтверждения учетной записи владельца сертификата (по желанию физического лица) в единой системе идентификации и аутентификации, содержащие серию, номер, дату и место выдачи основного документа, удостоверяющего личность, пол, дату и место рождения, гражданство, номер мобильного телефона. Вышеуказанные сведения являются персональными данными владельца сертификата (физического лица), обрабатываемыми Удостоверяющим центром в соответствии с частью 5 статьи 18 Федерального закона «Об электронной подписи» и согласием на обработку

персональных данных, предоставляемым указанным физическим лицом;

- сведения, содержащиеся в заявлениях, доверенностях, согласии на обработку персональных данных и иных документах, предоставляемых заявителем в Удостоверяющий центр, за исключением информации не являющейся конфиденциальной, указанной в пункте 8.2.2 настоящего Порядка.

8.2.4. Обеспечение конфиденциальности.

Сведения, относящиеся к конфиденциальной информации в соответствии с действующим законодательством Российской Федерации и настоящим Порядком, полученные Удостоверяющим центром или Стороной, присоединившейся к Порядку, в целях оказания или получения услуг в соответствии с настоящим Порядком, не подлежат разглашению, распространению и передаче третьим лицам, если иное не оговорено особо, а также в случаях, предусмотренных законодательством Российской Федерации, настоящим Порядком, договором оказания услуг Удостоверяющего центра или соглашением Сторон.

9. Сроки действия ключевой информации.

9.1 Срок действия ключевой информации Удостоверяющего центра.

9.1.1. Срок действия ключа электронной подписи уполномоченного лица УЦ 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 сформирован.

Начало периода действия ключа электронной подписи уполномоченного лица УЦ исчисляется с даты и времени генерации соответствующего ключа электронной подписи.

9.1.2. Срок действия сертификата ключа проверки электронной подписи уполномоченного лица УЦ составляет 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

9.1.3. Срок действия ключа электронной подписи Службы актуальных статусов сертификатов составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы актуальных статусов сертификатов исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов.

9.1.4. Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

9.1.5. Срок действия ключа электронной подписи Службы штампов времени

составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи Службы штампов времени исчисляется с даты и времени создания сертификата ключа проверки электронной подписи Службы штампов времени.

9.1.6. Срок действия сертификата ключа проверки электронной подписи Службы штампов времени не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы штампов времени и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

9.2 Сроки действия ключевой информации Пользователя УЦ.

9.2.1. Срок действия ключа электронной подписи Пользователя УЦ устанавливается Удостоверяющим центром, но не может превышать 1 год 3 месяца.

Начало периода действия ключа электронной подписи Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

9.2.2. Срок действия сертификата ключа проверки электронной подписи Пользователя УЦ не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity» соответственно.

9.3 Программный комплекс обеспечения реализации целевых функций.

9.3.1. Для выполнения своих целевых функций Удостоверяющий центр использует следующее программное обеспечение от компании КриптоПро:

- Центр Сертификации;
- Центр Регистрации;
- АРМ администратора Центра регистрации;
- АРМ разбора конфликтных ситуаций.

9.3.2. В функции Центра Сертификации входят:

- формирование сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме с использованием ключа электронной подписи и сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра;
- формирование списков аннулированных (отозванных) и приостановленных сертификатов ключей проверки электронной подписи пользователей УЦ (СОС) в электронной форме с использованием ключа электронной подписи и сертификата ключа проверки электронной подписи уполномоченного лица Удостоверяющего

центра на основе эталонной копии списка аннулированных (отозванных) и приостановленных сертификатов ключей проверки электронной подписи пользователей УЦ;

- ведение эталонной копии Реестра сертификатов ключей проверки электронной подписи Удостоверяющего центра;
- ведение эталонной копии списка аннулированных (отозванных) и приостановленных сертификатов ключей проверки электронной подписи пользователей УЦ;
- обеспечение уникальности ключей проверки электронной подписи в изданных сертификатах ключей проверки электронной подписи пользователей УЦ.

9.3.3.Ответственность за эксплуатацию Центра Сертификации возлагается на Уполномоченное лицо Удостоверяющего центра.

Основной функционал Центра Регистрации:

- ведение Реестра зарегистрированных пользователей УЦ;
- ведение Реестра сертификатов ключей проверки электронной подписи пользователей УЦ;
- ведение Реестра запросов на регистрацию пользователей УЦ в электронной форме;
- ведение Реестра запросов на создание сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- ведение Реестра запросов на прекращение действия (аннулирование) сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- ведение Реестра запросов на приостановление действия сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- ведение Реестра запросов на возобновление действия сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме.

9.3.4.АРМ администратора Центра Регистрации является приложением программного комплекса Удостоверяющего центра и предназначен для обеспечения реализации своих функциональных обязанностей сотрудниками Удостоверяющего центра в части регистрации пользователей и управления процессом создания сертификатов.

9.3.5.АРМ разбора конфликтных ситуаций является приложением программного комплекса Удостоверяющего центра и предназначен для обеспечения реализации своих функциональных обязанностей сотрудниками Удостоверяющего центра в части взаимодействия с пользователями УЦ при разрешении вопросов, связанных с подтверждением электронной подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей проверки электронной подписи, созданных Удостоверяющим центром в электронной форме.

10.Ролевое разграничение доступа.

10.1. В Удостоверяющем центре применяется ролевая модель доступа и каждый привилегированный пользователь ассоциирован с соответствующей ролью.

Принадлежность пользователя к той или иной роли, определяет список действий, которые он может выполнять.

Доступ к функциям Удостоверяющего центра определяется исходя из следующих ролей:

1. администратор Удостоверяющего центра.

2. оператор Удостоверяющего центра.

3. 10.2. Основные действия, осуществляемые привилегированными пользователями УЦ:

4. регистрация пользователя, включающая создание регистрационной записи в базе данных Центра Регистрации Удостоверяющего центра;

5. создание сертификата ключа проверки электронной подписи пользователя;

6. управление сертификатами ключей проверки электронной подписи пользователя;

7. действия, связанные с получением данных, хранящихся в Удостоверяющем центре (информация о сертификатах зарегистрированных пользователей, информация о запросах, список отозванных сертификатов и т.д.).

Администратор Удостоверяющего центра обладает неограниченным доступом к функционалу Удостоверяющего центра.

Оператор Удостоверяющего центра обладает следующими правами:

<i>Право</i>	<i>Краткое описание</i>
Выполнение	Для отправки запроса на регистрацию заявки, получения шаблона сертификата.
Делегирование	Для одобрения заявки на выпуск сертификата

11. Перечень событий, регистрируемых программным обеспечением.

События регистрируются программными компонентами Центр Сертификации и Центр Регистрации, предусмотрена регистрация следующих событий:

Центр Сертификации:

1. установлено сетевое соединение с программной компонентой Центра Регистрации;

2. издан СОС;

3. принят запрос на сертификат;

4. издание сертификата;

5. невыполнение внутренней операции программной компоненты;

6. системные события общесистемного программного обеспечения.

7. Центром Регистрации:

8. помещен запрос на регистрацию;
9. принят запрос на регистрацию;
10. отклонен запрос на регистрацию;
11. помещен запрос на сертификат;
12. принят запрос на сертификат;
13. отклонен запрос на сертификат;
14. установка сертификата подтверждена пользователем;
15. помещен запрос на отзыв сертификата;
16. принят запрос на отзыв сертификата;
17. отклонен запрос на отзыв сертификата;
18. помещен запрос на первый сертификат;
19. запрошен список отзываемых сертификатов;
20. опубликован список отзываемых сертификатов;
21. невыполнение внутренней операции программной компоненты;
22. установлено сетевое соединение с внешней программной компонентой;
23. системные события общесистемного программного обеспечения.

12. Перечень данных, подлежащих резервному копированию.

Для обеспечения функциональности Удостоверяющего центра необходимо ежесуточно проводить резервное копирование данных Удостоверяющего центра.

Перечень данных Удостоверяющего центра, подлежащих резервному копированию, включает в себя:

- сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра в электронном виде;
- базу данных службы сертификации Центра Сертификации программного комплекса Удостоверяющего центра, включая журнал выданных сертификатов и очередь запросов;
- базу данных Центра Регистрации (базу данных SQL сервера Центра Регистрации);
- журналы аудита компонент Удостоверяющего центра в составе, определенном эксплуатационной документацией Удостоверяющего центра.

13. Инженерно-технические меры защиты информации.

13.1. Размещение технических средств.

Технические средства Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование размещены в выделенном помещении (далее по тексту – серверное помещение или ЦОД). Сервера Центра Сертификации, Центра Регистрации и телекоммуникационное оборудование размещаются в шкафу-стойке.

Остальные технические средства размещаются в рабочих помещениях Удостоверяющего центра по схеме организации рабочих мест персонала.

13.2.Физический доступ в помещения.

Серверное помещение, а также рабочие и служебные помещения Удостоверяющего центра оборудованы системой контроля доступа. Регламенты доступа в выделенные помещения утверждены приказами директора ГКУ ТО «ЦИТТО».

Рабочие и служебные помещения Удостоверяющего центра, кроме системы контроля доступа, оборудованы механическими замками. Ключи механических замков рабочих помещений Удостоверяющего центра хранятся на круглосуточном посту охраны здания и выдаются сотрудникам под роспись в журнале.

13.3.Электроснабжение и кондиционирование воздуха

Технические средства Удостоверяющего центра подключены к общегородской сети электроснабжения через устройства бесперебойного электропитания, обеспечивающие их работу в течение 1,5 часов после прекращения основного электропитания. Электрические сети и электрооборудование, используемые в Удостоверяющем центре, отвечают требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей». Технические средства, эксплуатируемые на рабочих местах сотрудников Удостоверяющего центра, также оборудуются источниками бесперебойного питания. Серверное помещение оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение необходимых для бесперебойной работы оборудования параметров температурно-влажностного режима, вентиляции и очистки воздуха.

Рабочие и прочие служебные помещения Удостоверяющего центра оборудованы средствами вентиляции и кондиционирования воздуха.

13.4.Предупреждение и защита от возгорания.

Серверное помещение Удостоверяющего центра оборудовано системой пожарной сигнализации и газового пожаротушения. Необходимые для эксплуатации серверного помещения документы по пожарной безопасности утверждены приказами директора ГКУ ТО «ЦИТТО» и согласованы с арендодателем.

13.5.Хранение документированной информации.

Документальный фонд Удостоверяющего центра, как фондообразователя, подлежит хранению в соответствии с действующим законодательством Российской Федерации по делопроизводству и архивному делу.

13.6.Уничтожение документированной информации.

Выделение к уничтожению и уничтожение документов, не подлежащих архивному хранению, осуществляется сотрудниками Удостоверяющего центра, обеспечивающими документирование.

14.Программно-аппаратные меры защиты информации.

14.1. Организация доступа к техническим средствам.

Доступ к техническим средствам Удостоверяющего центра, размещенным в серверном помещении, осуществляется с использованием системы контроля доступа. Организация доступа к техническим средствам Удостоверяющего центра, размещенных на рабочих местах сотрудников Удостоверяющего центра, возлагается на сотрудников, ответственных за эксплуатацию данных технических средств и перечисленных в списке, утверждённом директором ГКУ ТО «ЦИТТО».

14.2. Организация доступа к программным средствам.

Рабочие места сотрудников Удостоверяющего центра, на которых эксплуатируются программные приложения «АРМ администратора ЦР» и «АРМ разбора конфликтных ситуаций» оснащены программно-аппаратными комплексами защиты от несанкционированного доступа. Доступ системных администраторов общесистемного программного обеспечения серверов Центра Сертификации и Центра Регистрации для выполнения регламентных работ осуществляется в присутствии сотрудников Удостоверяющего центра, отвечающих за эксплуатацию соответствующего прикладного программного обеспечения (Центра Сертификации и/или Центра Регистрации). Перечень сотрудников, имеющих доступ к программно-аппаратным комплексам УЦ утверждён приказом директора ГКУ ТО «ЦИТТО».

14.3. Контроль целостности программного обеспечения.

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого Удостоверяющим центром:

- программные модули средств электронной подписи и криптографической защиты информации;
- программные модули Центра Сертификации;
- программные модули Центра Регистрации.

Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами электронной подписи и криптографической защиты информации.

14.4. Контроль целостности технических средств.

Контроль целостности технических средств технических средств Удостоверяющего центра обеспечивается ограничением физического доступа в Серверное помещение.

14.5. Защита внешних сетевых соединений.

Защита конфиденциальной информации, передаваемой между программно-техническими средствами обеспечения деятельности Удостоверяющего центра и программными средствами, предоставляемыми Удостоверяющим центром пользователям, в процессе обмена документами в электронной форме, осуществляется путем шифрования информации с использованием шифровальных (криптографических) средств, сертифицированных в соответствии с действующим законодательством Российской Федерации. В качестве шифровальных (криптографических) средств пользователей УЦ, используемых для защиты конфиденциальной информации, используется средство электронной подписи Удостоверяющего центра. Защита

программно-технических средств обеспечения деятельности Удостоверяющего центра от несанкционированного доступа по внешним сетевым соединениям осуществляется путем использования межсетевого экрана.

14.6. Перечень информации, подлежащей защите.

Поступающая в Удостоверяющий центр информация:

1. заявление на регистрацию в электронной форме;
2. заявление на создание сертификата ключа проверки электронной подписи в электронной форме;
3. заявление на прекращение действия (аннулирование) сертификата ключа проверки электронной подписи в электронной форме;
4. заявление на приостановление действия сертификата ключа проверки электронной подписи в электронной форме;
5. заявление на возобновление действия сертификата ключа проверки электронной подписи в электронной форме;
6. пароль, передаваемый пользователем УЦ при аутентификации по паролю;
7. ключевая фраза пользователя УЦ.
8. Передаваемая из Удостоверяющего центра информация:
9. пароль, передаваемый пользователю УЦ для аутентификации по паролю;
10. список сертификатов ключа проверки электронной подписи пользователя УЦ и их статус;
11. список запросов на сертификаты ключей проверки электронной подписи пользователя УЦ и их статус;
12. список запросов на прекращение действия (аннулирование), приостановление и возобновление действия сертификатов ключей проверки электронной подписи пользователя УЦ и их статус.

15. Организационные меры защиты информации.

15.1. Предъявляемые требования к персоналу.

Уполномоченное лицо Удостоверяющего центра имеет высшее профессиональное образование и профессиональную подготовку в области информационной безопасности, а также стаж работы в этой области более 2 лет. Сотрудники Удостоверяющего центра имеют высшее профессиональное образование и прошли курсы повышения квалификации в области информационной безопасности.

15.2. Профессиональная переподготовка и повышение квалификации персонала.

Сотрудники Удостоверяющего центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 5 лет.

15.3. Организация работы.

Деятельность по работе с пользователями УЦ в части приема заявлений в бумажной форме и создания сертификатов ключей проверки электронной подписи

организована ГКУ ТО «ЦИТТО» в одну рабочую смену с 9.00 до 13.00 и с 14:00 до 17:00 в будние дни. Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

15.4. Организация доступа персонала к документам и документации.

Доступ сотрудников Удостоверяющего центра к документам и документации, составляющей документальный фонд организации, организован в соответствии с должностными инструкциями и функциональными обязанностями.

15.5. Охрана здания и помещений.

Здание, в котором расположено ГКУ ТО «ЦИТТО», имеет централизованную службу охраны, обеспечивающую:

- обнаружение и задержание злоумышленников, пытающихся проникнуть в здание (помещения) ГКУ ТО «ЦИТТО»;
- круглосуточное централизованное видеонаблюдение за местами возможного проникновения злоумышленников с обеспечением долгосрочного хранения видеозаписи;
- сохранность материальных ценностей и документов;
- предупреждение происшествий и ликвидацию их последствий.

16. Архивное хранение документированной информации.

16.1. Состав архивируемых документов.

Архивированию подлежит следующая документированная информация:

- заявления о присоединении к настоящему Порядку;
- заявления на регистрацию пользователей УЦ;
- заявления на создание сертификатов ключей проверки электронной подписи;
- копии сертификатов ключей проверки электронной подписи пользователей и уполномоченного лица УЦ на бумажном носителе;
- заявления на аннулирование (отзыв) сертификатов ключей проверки электронной подписи;
- заявления на приостановление действия сертификатов ключей проверки электронной подписи;
- заявления на возобновление действия сертификатов ключей проверки электронной подписи;
- служебные документы Удостоверяющего центра.

16.2. Архивирование ключа электронной подписи.

Удостоверяющий центр ни при каких обстоятельствах не хранит и не архивирует ключи электронной подписи пользователей УЦ.

16.3. Источник комплектования архивного фонда.

Источником комплектования архивного фонда Удостоверяющего центра являются

подразделения (службы) ГКУ ТО «ЦИТТО», обеспечивающие документирование.

16.4.Архивохранилище.

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

16.5.Срок архивного хранения.

Документы, подлежащие архивному хранению, являются документами временного хранения. Срок хранения архивных документов устанавливается 9 лет.

16.6.Уничтожение архивных документов.

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Удостоверяющего центра и назначаемой приказом руководителя ГКУ ТО «ЦИТТО».

17.Восстановление после аварий.

17.1.Восстановление после компрометации.

В случае компрометации ключа УЦ, используемого для подписи сертификатов и СОС, осуществляется внеплановая смена ключа электронной подписи и ключа проверки электронной подписи Удостоверяющего центра в соответствии с разделом 6.3.

17.2.Восстановление после прочих бедствий.

В случае повреждения оборудования УЦ вследствие каких-либо бедствий Удостоверяющий центр должен принять все возможные меры для скорейшего восстановления своей работоспособности. Приоритет должен быть отдан возможности отзыва сертификатов и выпуска СОС. В случае невозможности восстановления функции отзыва сертификатов до окончания срока действия СОС, Удостоверяющий центр должен объявить свои ключи скомпрометированными и действовать в соответствии с разделом 6.3.

Приложение №1
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для органов власти

Заявление о присоединении
к Порядку Удостоверяющего центра[□]

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

1. В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Порядку Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области», условия которого определены государственным казенным учреждением Тюменской области «Центр информационных технологий Тюменской области» и опубликованы на сайте Удостоверяющего центра по адресу <http://ca.72to.ru>.

2. С Порядком Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

(должность руководителя организации)

(подпись) / (Ф.И.О.)

«_____» _____ 20____ г.
М.П.

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Порядку Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от «____» _____ 20____ г.

Уполномоченное лицо
УЦ ГКУ ТО «ЦИТТО»

(подпись) / (Ф.И.О.)

М.П.

Заявление о присоединении к Порядку подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Приложение №2
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для физических лиц

Заявление о присоединении
к Порядку Удостоверяющего центра[□]

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Порядку Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области», условия которого определены государственным казенным учреждением Тюменской области «Центр информационных технологий Тюменской области» и опубликованы на сайте Удостоверяющего центра по адресу <http://ca.72to.ru>.
2. С Порядком Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

_____/_____
(подпись) (Ф.И.О.)
«_____» 20____ г

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Порядку Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от «_____» 20____ г.

Уполномоченное лицо
УЦ ГКУ ТО «ЦИТТО»

_____/_____
(подпись) (Ф.И.О.)

М.П.

Заявление о присоединении к Порядку подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Заявление
на изготовление карты с электронной подписью
(сертификат юридического лица)

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица)

действующего на основании

просит изготовить карту на имя

(фамилия, имя, отчество должностного лица)

в связи с

(первичный выпуск/истечение срока действия/неисправность/блокировка/утеря карты/иное - указать)

просит зарегистрировать в Реестре пользователей Удостоверяющего центра (далее – УЦ), создать и записать на карту ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи юридического лица в соответствии с указанными идентификационными данными:

Сведения о должностном лице:

Фамилия Имя Отчество	Фамилия имя отчество (если имеется) должностного лица
Электронная почта	Адрес электронной почты (если имеется)
Место жительства (Страна, субъект РФ, населенный пункт)	RU, 72 Тюменская область,
ИНН/СНИЛС физ.лица	ИНН и СНИЛС должностного лица

Сведения о юридическом лице:

Организация	Наименование организации
Подразделение	Подразделение/отдел организации (если имеется)
Должность	Должность
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP

Расширенное использование ключа (ExtendedKeyUsage)

Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Дополнительные области использования (множественный выбор):

СМЭВ ТО СЭД Directum/Дело/Бюрократ АЦК-Финансы АЦК-Госзаказ ГАС «Управление»

ГИСЗ ТО ЕИС СЗН ТО РГУ АИС «ЕЦУ»

ФИАС* ЕСИА. Регистрация юридического лица* ЕСИА. Центр обслуживания (1.2.643.100.2.1) *

ИС Министерства финансов РФ * ИС ФСРАР * Федресурс (1.3.6.1.4.1.40870.1.1.1) *;** МИК *

Доступ к сервисам Росреестра на Портале поставщиков услуг (выбрать один из типов субъекта)**:

РОИВ (1.2.643.5.1.24.2.6) ОМСУ (1.2.643.5.1.24.2.19) ФОИВ (1.2.643.5.1.24.2.43)

Внебюджетный фонд (1.2.643.5.1.24.2.52) Подвед. РОИВ (1.2.643.5.1.24.2.53)

Я,

(ФИО, дата и место рождения, гражданство, пол (М/Ж) должностного лица – пользователя УЦ)

(серия и номер паспорта должностного лица, кем и когда выдан, код подразделения)

1. С Порядком УЦ ГКУ ТО «ЦИТТО» и приложениями к нему, включая Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, ознакомлен и обязуюсь соблюдать все положения указанного документа.
2. Даю согласие на обработку своих персональных данных, указанных в заявлении, ГКУ ТО «ЦИТТО» по адресу: г.Тюмень, ул.Советская, д.61, путем неавтоматизированной и автоматизированной обработки, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных с целью выпуска, выдачи и обслуживания карты с электронной подписью.
3. Даю согласие на проверку предоставленных мною сведений на предмет их полноты и достоверности, в том числе с использованием государственных и муниципальных информационных систем и ресурсов, а также путем направления запросов в иные ведомства.
4. Даю согласие на передачу своих персональных данных в объеме, необходимом для регистрации сертификата в Единой системе идентификации и аутентификации (ЕСИА), в Министерство цифрового развития, связи и массовых коммуникаций (оператор ЕСИА).
5. Признаю, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным.
6. Прошу аннулировать сертификат на ранее выданной карте (заполняется в случае перевыпуска):

Серийный номер сертификата	
----------------------------	--

7. Контактная информация:

номер мобильного телефона	
---------------------------	--

адрес электронной почты	
-------------------------	--

Пользователь Удостоверяющего центра

_____ / _____ / _____
(подпись) _____ (Ф.И.О.)

(должность лица, уполномоченного действовать от имени юридического лица)

_____ / _____ / _____
(подпись) _____ (Ф.И.О.)

«_____» _____ 20____ г.
М.П.

На настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Оператор ППВ _____ / _____ /
(адрес пункта) «_____» _____ 20____ г.

Данные внесены в информационную систему: _____
(номер комплекта дела)

На основании данного Заявления СКПЭП аннулирован (отозван). Опубликован список
отозванных сертификатов, содержащий сведения об аннулированном (отозванном) сертификате.

Уполномоченное лицо ЦР
Удостоверяющего центра

_____ / _____ /
« _____ » 20 ____ г.

* необходимо предоставить документ, подтверждающий полномочия лица на осуществление действий от имени юридического лица (для руководителя юридического лица - копия решения о назначении или об избрании либо копия приказа о назначении физического лица на должность, в соответствии с которыми такое физическое лицо обладает правом действовать от имени юридического лица без доверенности, для иных лиц – доверенность)

** необходимо предоставить документы, подтверждающие полномочия пользователя выступать от имени юридического лица при использовании электронной подписи в указанной системе (приказ или доверенность)

Заявление
на изготовление карты с электронной подписью
(сертификат физического лица)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица)

действующего на основании

просит изготовить карту на имя

(фамилия, имя, отчество должностного лица)

в связи

(первичный выпуск/истечение срока действия/неисправность/блокировка/утеря карты/иное указать)

просит зарегистрировать в Реестре пользователей Удостоверяющего центра (далее – УЦ), создать и записать на карту ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи физического лица в соответствии с указанными идентификационными данными:

Сведения о должностном лице:

Фамилия Имя Отчество	Фамилия имя отчество (если имеется) должностного лица
Электронная почта	Адрес электронной почты (если имеется)
Место жительства (Страна, субъект РФ, населенный пункт)	RU, 72 Тюменская область,
ИНН/СНИЛС физ.лица	ИНН и СНИЛС должностного лица

Сведения о месте работы (не включаются в сертификат):

Организация	Наименование организации
Подразделение	Подразделение/отдел организации (если имеется)
Должность	Должность
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP

Расширенное использование ключа (ExtendedKeyUsage)

Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Дополнительные области использования (множественный выбор):

- СМЭВ ТО СЭД Directum/Дело/Бюрократ АЦК-Финансы АЦК-Госзаказ ГАС «Управление»
 ГИСЗ ТО ЕИС СЗН ТО РГУ АИС «ЕЦУ»

Доступ к сервисам Росреестра на Портале поставщиков услуг (выбрать один из типов субъекта)**:

- РОИВ (1.2.643.5.1.24.2.6) ОМСУ (1.2.643.5.1.24.2.19) ФОИВ (1.2.643.5.1.24.2.43)
 Внебюджетный фонд (1.2.643.5.1.24.2.52) Подвед. РОИВ (1.2.643.5.1.24.2.53)

Я,

(ФИО, дата и место рождения, гражданство, пол (М/Ж) должностного лица – пользователя УЦ)

(серия и номер паспорта должностного лица, кем и когда выдан, код подразделения)

1. В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Порядку УЦ государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области», условия которого определены ГКУ ТО «ЦИТТО» и опубликованы на сайте по адресу <http://ca.72to.ru>. С Порядком УЦ и приложениями к нему, включая Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, ознакомлен и обязуюсь соблюдать все положения указанного документа.
2. Даю согласие на обработку своих персональных данных, указанных в заявлении, ГКУ ТО «ЦИТТО» по адресу: г.Тюмень, ул.Советская, д.61, путем неавтоматизированной и автоматизированной обработки, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных с целью выпуска, выдачи и обслуживания карты с электронной подписью.
3. Даю согласие на проверку предоставленных мною сведений на предмет их полноты и достоверности, в том числе с использованием государственных и муниципальных информационных систем и ресурсов, а также путем направления запросов в иные ведомства.
4. Даю согласие на передачу своих персональных данных в объеме, необходимом для регистрации сертификата в Единой системе идентификации и аутентификации (ЕСИА), в Министерство цифрового развития, связи и массовых коммуникаций (оператор ЕСИА).
5. Признаю, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным.
6. Прошу аннулировать сертификат на ранее выданной карте (заполняется в случае перевыпуска):

Серийный номер сертификата	
----------------------------	--

7. Контактная информация:

номер мобильного телефона	
---------------------------	--

адрес электронной почты	
-------------------------	--

Пользователь Удостоверяющего центра

_____ / _____ /
(подпись) (Ф.И.О.)

(должность лица, уполномоченного действовать
от имени юридического лица)

_____ / _____ /
(подпись) (Ф.И.О.)

«_____» _____ 20____ г.

М.П.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Оператор ППВ _____ /
(адрес пункта приема заявления) «_____» _____ 20____ г.

Данные внесены в информационную систему ППВ: _____
(номер комплекта дела)

На основании данного Заявления СКПЭП аннулирован (отозван). Опубликован список
отозванных сертификатов, содержащий сведения об аннулированном (отозванном) сертификате.

Уполномоченное лицо ЦР
Удостоверяющего центра

_____ / _____ /
«_____» _____ 20____ г.

Заявление зарегистрировано в УЦ: №

(регистрационный номер заполняется сотрудником удостоверяющего центра)

*** необходимо предоставить документы, подтверждающие полномочия пользователя на использование
электронной подписи в указанной системе (приказ или доверенность)*

Приложение №5

к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(создание сертификата на информационную систему)
Для органов власти

Заявление на регистрацию пользователя и создание
квалифицированного сертификата ключа проверки электронной подписи

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

1. Просит зарегистрировать

(наименование информационной системы)

в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и создать ключи
электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в
соответствии с указанными в настоящем заявлении идентификационными данными:

Организация	Наименование организации
Подразделение	Наименование информационной системы (необязательно)
Электронная почта	Адрес электронной почты (необязательно)
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP
Расширенное использование ключа	Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

2. Прошу предоставить услугу удаленной аутентификации по кодовой фразе. С рисками,
возникающими при пользовании данной услугой ознакомлен и согласен нести за них
ответственность.

Кодовая фраза

(должность лица, уполномоченного действовать от
имени юридического лица)

/ / /
(подпись) (Ф.И.О.)

«_____» 20____г.
М.П.

(заполняется сотрудником Удостоверяющего центра)

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов,
удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении,
предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо

Центра Регистрации

/ /
«_____» 20____г.

Приложение №5а

к Порядку реализации функций аккредитованного

Удостоверяющего центра ГКУ ТО «ЦИТТО»

(обновление сертификата на информационную систему)

Для органов власти

Заявление на создание

квалифицированного сертификата ключа проверки электронной подписи
при плановой/внеплановой смене

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

в связи с

(причина создания сертификата)

1. просит создать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра:

(наименование информационной системы)

в соответствии с указанными в настоящем заявлении идентификационными данными:

Организация	Наименование организации
Подразделение	Наименование информационной системы
Электронная почта	Адрес электронной почты (необязательно)
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организаций
Средство электронной подписи	КриптоПро CSP
Расширенное использование ключа	Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

2. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 20 Порядка) ознакомлен.

(должность лица, уполномоченного действовать от имени юридического лица)

(подпись)

(Ф.И.О.)

«_____» / _____ 20____ г.
М.П.

(заполняется сотрудником Удостоверяющего центра)

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо

Центра Регистрации

_____ / _____
«_____» / _____ 20____ г.

Приложение №6
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(создание серверного сертификата)
Для органов власти

Заявление на регистрацию пользователя и создание
квалифицированного сертификата ключа проверки электронной подписи

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

1. Просит зарегистрировать

(наименование веб-узла)

в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и создать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Список полных имён DNS	DNS имя/имена
Организация	Наименование организации
Подразделение	Наименование веб-узла <i>(необязательно)</i>
Электронная почта	Адрес электронной почты <i>(необязательно)</i>
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP
Расширенное использование ключа	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

2. Прошу предоставить услугу удаленной аутентификации Пользователя УЦ по кодовой фразе. С рисками, возникающими при пользовании данной услугой ознакомлен и согласен нести за них ответственность.

Кодовая фраза

(должность лица, уполномоченного действовать от
имени юридического лица)

(подпись)

(Ф.И.О.)

«_____» _____ 20____ г.
М.П.

(заполняется сотрудником Удостоверяющего центра)

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____ / _____
«_____» _____ 20____ г.

Приложение №6а
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(обновление серверного сертификата)
Для органов власти

Заявление на создание
квалифицированного сертификата ключа проверки электронной подписи
при плановой/внеплановой смене

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

в связи с

(причина создания сертификата)

1. просит создать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра:

(наименование веб-узла)

в соответствии с указанными в настоящем заявлении идентификационными данными

Список полных имён DNS	DNS имя/имена
Организация	Наименование организации
Подразделение	Наименование веб-узла (необязательно)
Электронная почта	Адрес электронной почты (необязательно)
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP
Расширенное использование ключа	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)

2. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 20 Порядка) ознакомлен.

_____ / _____ /
(должность лица, уполномоченного действовать от
имени юридического лица)

_____ / _____ /
(подпись) (Ф.И.О.)

«_____» _____ 20____ г.
М.П.

(заполняется сотрудником Удостоверяющего центра)

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____ / _____ /
(подпись) (Ф.И.О.)
«_____» _____ 20____ г.

Приложение №7

к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(создание ключа ЭП на защищенном носителе пользователя)
Для органов власти

**Заявление на создание
квалифицированного сертификата ключа проверки электронной подписи
(сертификат юридического лица)**

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

в связи с

(первичный выпуск/плановая смена сертификата)

просит зарегистрировать в Реестре пользователей Удостоверяющего центра (далее – УЦ), создать и записать на предоставленный защищенный носитель ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи юридического лица в соответствии с указанными идентификационными данными:

Сведения о должностном лице:	
Фамилия Имя Отчество	Фамилия имя отчество (если имеется) должностного лица
Электронная почта	Адрес электронной почты (необязательно)
Место жительства (Страна, субъект РФ, населенный пункт)	RU, 72 Тюменская область,
ИНН/СНИЛС физ.лица	ИНН и СНИЛС должностного лица
Сведения о юридическом лице:	
Организация	Наименование организации
Подразделение	Подразделение/отдел организации (если имеется)
Должность	Должность
Место нахождения юр.лица (страна, субъект РФ, населенный пункт, улица, дом/корпус)	RU, 72 Тюменская область,
ИНН/ОГРН юр.лица	ИНН и ОГРН организации
Средство электронной подписи	КриптоПро CSP
Расширенное использование ключа (ExtendedKeyUsage)	
Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)	
Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)	
Защищенная электронная почта (1.3.6.1.5.5.7.3.4)	
Дополнительные области использования (множественный выбор):	
<input type="checkbox"/> СМЭВ ТО <input type="checkbox"/> СЭД Directum/Дело/Бюрократ <input type="checkbox"/> АЦК-Финансы <input type="checkbox"/> АЦК-Госзаказ <input type="checkbox"/> ГАС «Управление» <input type="checkbox"/> ГИСЗ ТО <input type="checkbox"/> ЕИС СЗН ТО <input type="checkbox"/> РГУ <input type="checkbox"/> АИС «ЕЦУ» <input type="checkbox"/> ФИАС* <input type="checkbox"/> ЕСИА. Регистрация юридического лица* <input type="checkbox"/> ЕСИА. Центр обслуживания (1.2.643.100.2.1)*,** <input type="checkbox"/> ИС Министерства финансов РФ* <input type="checkbox"/> ИС ФСРАР* <input type="checkbox"/> Федресурс (1.3.6.1.4.1.40870.1.1.1)*,** <input type="checkbox"/> МИК *	
Доступ к сервисам Росреестра на Портале поставщиков услуг (выбрать один из типов субъекта)**:	
<input type="checkbox"/> РОИВ (1.2.643.5.1.24.2.6) <input type="checkbox"/> ОМСУ (1.2.643.5.1.24.2.19) <input type="checkbox"/> ФОИВ (1.2.643.5.1.24.2.43) <input type="checkbox"/> Внебюджетный фонд (1.2.643.5.1.24.2.52) <input type="checkbox"/> Подвед. РОИВ (1.2.643.5.1.24.2.53)	

Я,

(ФИО, дата и место рождения, гражданство, пол (М/Ж) должностного лица – пользователя УЦ)

(серия и номер паспорта должностного лица, кем и когда выдан, код подразделения)

1. С Порядком УЦ ГКУ ТО «ЦИТТО» и приложениями к нему, включая Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, ознакомлен и обязуюсь соблюдать все положения указанного документа.
2. Даю согласие на обработку своих персональных данных, указанных в заявлении, ГКУ ТО «ЦИТТО» по адресу: г.Тюмень, ул.Советская, д.61, путем неавтоматизированной и автоматизированной обработки, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных с целью выпуска, выдачи и обслуживания карты с электронной подписью.
3. Даю согласие на проверку предоставленных мною сведений на предмет их полноты и достоверности, в том числе с использованием государственных и муниципальных информационных систем и ресурсов, а также путем направления запросов в иные ведомства.
4. Даю согласие на передачу своих персональных данных в объеме, необходимом для регистрации сертификата в Единой системе идентификации и аутентификации (ЕСИА), в Министерство цифрового развития, связи и массовых коммуникаций (оператор ЕСИА).
5. Признаю, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра

_____/_____/_____
(подпись) (Ф.И.О.)(должность лица, уполномоченного
действовать от имени юридического лица)_____/_____/_____
(подпись) (Ф.И.О.)
«_____» _____ 20____ г.
М.П.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Оператор ЦР

_____/_____/_____
«_____» _____ 20____ г.

* необходимо предоставить документ, подтверждающий полномочия лица на осуществление действий от имени юридического лица (для руководителя юридического лица - копия решения о назначении или об избрании либо копия приказа о назначении физического лица на должность, в соответствии с которыми такое физическое лицо обладает правом действовать от имени юридического лица без доверенности, для иных лиц – доверенность)

** необходимо предоставить документы, подтверждающие полномочия пользователя выступать от имени юридического лица при использовании электронной подписи в указанной системе (приказ или доверенность)

Приложение №8

к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(создание ключа ЭП на защищенном носителе пользователя)
Для физических лиц

**Заявление на создание
квалифицированного сертификата ключа проверки электронной подписи
(сертификат физического лица)**

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

в связи

(первичный выпуск/плановая смена сертификата)

просит зарегистрировать в Реестре пользователей Удостоверяющего центра (далее – УЦ), создать и записать на предоставленный защищенный носитель ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными идентификационными данными:

Сведения о должностном лице:

Фамилия Имя Отчество	Фамилия имя отчество (если имеется) должностного лица
Электронная почта	Адрес электронной почты (необязательно)
Место жительства (Страна, субъект РФ, населенный пункт)	RU, 72 Тюменская область,
ИНН/СНИЛС физ.лица	ИНН и СНИЛС должностного лица
Средство электронной подписи	КриптоПро CSP

Расширенное использование ключа (ExtendedKeyUsage)

Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6)

Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

Защищенная электронная почта (1.3.6.1.5.5.7.3.4)

Дополнительные области использования (множественный выбор):

- СМЭВ ТО СЭД «DIRECTUM» СЭД «Дело» СЭД «Бюрократ» АЦК-Финансы
 ГИСЗ ТО ГАС «Управление» Реестр государственных услуг (РГУ 4.0) АЦК-Госзаказ
 ЕИС СЗН ТО Единый центр услуг (АИС «ЕЦУ»)

Доступ к сервисам Росреестра на Портале поставщиков услуг (выбрать один из типов субъекта)**:

- Руководитель органа государственной власти субъекта РФ или иное уполномоченное лицо данного органа в соответствии с федеральным законом (РОИВ) (1.2.643.5.1.24.2.6)
- Руководитель органа местного самоуправления или иное уполномоченное лицо данного органа в соответствии с федеральным законом (ОМСУ) (1.2.643.5.1.24.2.19)
- Руководитель территориального органа федерального органа исполнительной власти или иное уполномоченное лицо данного органа в соответствии с федеральным законом (ФОИВ) (1.2.643.5.1.24.2.43)
- Руководитель (заместитель руководителя) территориального органа государственного внебюджетного фонда или иное уполномоченное лицо данного фонда в соответствии с федеральным законом (Внебюджетный фонд) (1.2.643.5.1.24.2.52)
- Руководитель подведомственной организации органа государственной власти субъекта РФ, участвующей в предоставлении государственных или муниципальных услуг, или иное уполномоченное лицо данной организации в соответствии с федеральным законом (1.2.643.5.1.24.2.53)

Я,

(ФИО, дата и место рождения, гражданство, пол (М/Ж) должностного лица – пользователя УЦ)

(серия и номер паспорта должностного лица, кем и когда выдан, код подразделения)

1. В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Порядку УЦ государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области», условия которого определены ГКУ ТО «ЦИТТО» и опубликованы на сайте по адресу <http://ca.72to.ru>. С Порядком УЦ и приложениями к нему, включая Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, ознакомлен и обязуюсь соблюдать все положения указанного документа.
2. Даю согласие на обработку своих персональных данных, указанных в заявлении, ГКУ ТО «ЦИТТО» по адресу: г.Тюмень, ул.Советская, д.61, путем неавтоматизированной и автоматизированной обработки, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, обезличивание, блокирование, удаление, уничтожение персональных данных с целью выпуска, выдачи и обслуживания карты с электронной подписью.
3. Даю согласие на проверку предоставленных мною сведений на предмет их полноты и достоверности, в том числе с использованием государственных и муниципальных информационных систем и ресурсов, а также путем направления запросов в иные ведомства.
4. Даю согласие на передачу своих персональных данных в объеме, необходимом для регистрации сертификата в Единой системе идентификации и аутентификации (ЕСИА), в Министерство цифрового развития, связи и массовых коммуникаций (оператор ЕСИА).
5. Признаю, что персональные данные, занесимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра

_____ / _____ /
(подпись) (Ф.И.О.)

_____ / _____ /
(должность лица, уполномоченного
действовать от имени юридического лица)

«_____» _____ 20____ г.
М.П.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Оператор
Центра регистрации

_____ / _____ /
<_____> _____ 20____ г.

Заявление зарегистрировано в УЦ: №

(регистрационный номер заполняется сотрудником удостоверяющего центра)

** необходимо предоставить документы, подтверждающие полномочия пользователя выступать от имени юридического лица при использовании электронной подписи в указанной системе (приказ или доверенность)

Приложение №9

к Порядку реализации функций аккредитованного

Удостоверяющего центра ГКУ ТО «ЦИТТО»

(Форма доверенности на право действовать от имени юр.лица)

Для органов власти

Доверенность

Г. _____

«_____» _____ 20 ____ г.

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

уполномочивает

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

действовать от имени

(полное наименование организации)

при использовании квалифицированной электронной подписи, владельцем которой он является.

Настоящая доверенность действительна по «_____» 20____ г.

Подпись пользователя УЦ ГКУ ТО «ЦИТТО» (_____) _____ подтверждаю.
(Ф.И.О.) (подпись)

(должность лица, уполномоченного действовать от имени юридического лица)

_____ / _____ /
(подпись) (Ф.И.О.)

«_____» _____ 20____ г.

M.P.

к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»
(Форма доверенности на получение ключей
в Удостоверяющем центре)

Для органов власти

Доверенность

г. _____

«_____» 20 ____ г.

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

уполномочивает

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Удостоверяющий центр государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ) необходимые документы, определенные Порядком УЦ для регистрации Пользователя УЦ.

2. Получить в УЦ сформированные ключи электронной подписи и сертификат ключа проверки электронной подписи Пользователя УЦ:

(имя пользователя УЦ)

3. Получить в УЦ иные документы, определенные Порядком УЦ.

Представитель наделяется правом расписываться на копии сертификата ключа проверки электронной подписи на бумажном носителе и в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «____» 20 ____ г.

Подпись уполномоченного представителя (_____) _____
подтверждаю.

(Ф.И.О.) (подпись)

Пользователь Удостоверяющего центра

/_____/

(подпись)

(Ф.И.О.)

(должность лица, уполномоченного
действовать от имени юридического лица)

(подпись) /____/ (Ф.И.О.)

«____» 20 ____ г.

М.П.

Приложение №11
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Используемые типы носителей

1. Смарт-карта;
2. Рутокен;
3. eToken.

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

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)

действующего на основании

в связи с

(причина аннулирования сертификата)

Просит прекратить действие сертификата ключа проверки электронной подписи (СКПЭП) Пользователя Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области»:

(ФИО владельца сертификата)

содержащий следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

____ / ____ / ____
(должность лица, уполномоченного
действовать от имени юридического лица)

____ / ____ / ____
(подпись) (Ф.И.О.)

«_____» _____ 20____ г.

М.П.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

____ / ____ / ____
«_____» _____ 20____ г.

На основании данного Заявления СКПЭП аннулирован (отозван). Опубликован список
отозванных сертификатов, содержащий сведения об аннулированном (отозванном) сертификате.

Уполномоченное лицо ЦР
УЦ ГКУ ТО «ЦИТТО»

____ / ____ / ____
«_____» _____ 20____ г.

Приложение №13
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для физических лиц

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

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

в связи с

(причина аннулирования сертификата)

прошу прекратить действие сертификата ключа проверки электронной подписи (СКПЭП),
владельцем которого я являюсь, содержащий следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

Пользователь Удостоверяющего центра

_____/_____
(подпись) (Ф.И.О.)
«_____» 20____ г.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов,
удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении,
предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____/_____
«_____» 20____ г.

На основании данного Заявления СКПЭП аннулирован (отозван). Опубликован список
отозванных сертификатов, содержащий сведения об аннулированном (отозванном) сертификате.

Уполномоченное лицо ЦР
УЦ ГКУ ТО «ЦИТТО»

_____/_____
(подпись) (Ф.И.О.)
«_____» 20____ г.

**Заявление на приостановление действия
сертификата ключа проверки электронной подписи**

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

Просит приостановить действие сертификата ключа проверки электронной подписи (СКПЭП) Пользователя Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области»:

(ФИО владельца сертификата)
содержащего следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Пользователь Удостоверяющего центра _____ / _____ /
(подпись) (Ф.И.О.)

_____ / _____ /
(подпись) (Ф.И.О.)

«_____» _____ 20____ г.

М.П.

На настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо _____ / _____ /
Центра Регистрации «_____» _____ 20____ г.

На основании данного Заявления действие СКПЭП приостановлено. Опубликован список отозванных сертификатов, содержащий сведения о сертификате, действие которого было приостановлено.

Уполномоченное лицо ЦР _____ / _____ /
УЦ ГКУ ТО «ЦИТТО» «_____» _____ 20____ г.

Приложение №15
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для физических лиц

**Заявление на приостановление действия
сертификата ключа проверки электронной подписи**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

прошу приостановить действие сертификата ключа проверки электронной подписи, владельцем которого я являюсь, содержащего следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

Срок приостановления действия сертификата _____ дней.
(количество дней прописью)

Пользователь Удостоверяющего центра _____

/ _____ /

(подпись)

(Ф.И.О.)

«_____» _____ 20____ г.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____ / _____ /
«_____» _____ 20____ г.

На основании данного Заявления действие СКПЭП приостановлено. Опубликован список отозванных сертификатов, содержащий сведения о сертификате, действие которого было приостановлено.

Уполномоченное лицо ЦР
УЦ ГКУ ТО «ЦИТТО»

_____ / _____ /
«_____» _____ 20____ г.

Для органов власти

Заявление на возобновление действия
сертификата ключа проверки электронной подписи

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

Просит возобновить действие сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области»:

(ФИО владельца сертификата)

содержащего следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

Пользователь Удостоверяющего центра

_____ / _____ /
(подпись) (Ф.И.О.)

(должность руководителя организации)

_____ / _____ /
(подпись) (Ф.И.О.)
« _____ » 20 ____ г.

М.П.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____ / _____ /
« _____ » 20 ____ г.

На основании данного Заявления действие СКПЭП приостановлено. Опубликован список отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено.

Уполномоченное лицо
Центра Регистрации

_____ / _____ /
« _____ » 20 ____ г.

Приложение №17
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для физических лиц

**Заявление на возобновление действия
сертификата ключа проверки электронной подписи**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

прошу возобновить действие сертификата ключа проверки электронной подписи, владельцем которого я являюсь, содержащего следующие данные:

СНИЛС (SNILS)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

Пользователь Удостоверяющего центра

_____/_____
(подпись) (Ф.И.О.)
«_____» 20____ г.

Настоящим подтверждаю, что Заявитель идентифицирован на основании документов, удостоверяющих личность. Установлено соответствие данных, указанных в Заявлении, предоставленным документам либо их надлежащим образом заверенным копиям.

Уполномоченное лицо
Центра Регистрации

_____/_____
«_____» 20____ г.

На основании данного Заявления действие СКПЭП приостановлено. Опубликован список отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено.

Уполномоченное лицо
Центра Регистрации

_____/_____
«_____» 20____ г.

Приложение №18
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для органов власти

Заявление на подтверждение подлинности
электронной подписи уполномоченного лица Удостоверяющего центра

На основании договора присоединения к Порядку УЦ №

(регистрационный номер и дата регистрации заявления о присоединении)

(наименование организации, включая ИНН/ОГРН)

в лице

(должность, фамилия, имя, отчество лица, уполномоченного действовать от имени юридического лица)
действующего на основании

Просит подтвердить подлинность электронной подписи уполномоченного лица Удостоверяющего центра Государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ) в изданном УЦ сертификате ключа подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи, содержащий электронную подпись уполномоченного лица УЦ, на прилагаемом к заявлению машинном (оптическом) носителе – сер.№ XXXXX;
2. Время и дата[□], на момент наступления которых требуется установить статус сертификата:

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

Время и дата подачи заявления в УЦ:

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

(должность лица, уполномоченного
действовать от имени юридического лица)

_____ / _____ / _____

(подпись) (Ф.И.О.)

«_____» 20____ г.

М.П.

Время и дата должны быть указаны с учетом часового пояса г. Тюмени (по Тюменскому времени)

Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи заявления в Удостоверяющий центр

Приложение №19
к Порядку реализации функций аккредитованного
Удостоверяющего центра ГКУ ТО «ЦИТТО»

Для физических лиц

Заявление на подтверждение подлинности
электронной подписи уполномоченного лица Удостоверяющего центра

Я,

(фамилия, имя, отчество)

прошу подтвердить подлинность электронной подписи уполномоченного лица Удостоверяющего центра Государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ) в изданном УЦ сертификате ключа подписи и установить его статус (действует/не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки электронной подписи, содержащий электронную подпись уполномоченного лица УЦ, на прилагаемом к заявлению машинном (оптическом) носителе – сер.№ XXXXX;
2. Время и дата[□], на момент наступления которых требуется установить статус сертификата:

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

Время и дата подачи заявления в УЦ:

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

Пользователь Удостоверяющего центра

_____/_____/_____
(подпись) (Ф.И.О.)
«_____» 20____ г.

Время и дата должны быть указаны с учетом часового пояса г. Тюмени (по Тюменскому времени)
Если время и дата не указаны, то статус сертификата устанавливается на момент времени подачи
заявления в Удостоверяющий центр

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

1. Обязанности владельца квалифицированного сертификата ключа проверки электронной подписи

1.1. Обеспечить конфиденциальность ключей электронных подписей.

1.2. Применять для формирования электронной подписи только действующий ключ электронной подписи.

1.3. Не применять ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

1.4. Применять ключ электронной подписи с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи (в расширениях Extended Key Usage, Application Policy сертификата ключа проверки электронной подписи), если такие ограничения были установлены.

1.5. Не использовать ключ электронной подписи и немедленно обратиться в Удостоверяющий центр с заявлением на прекращение или приостановление действия сертификата ключа проверки электронной подписи в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности ключа электронной подписи.

1.6. 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 времени подачи заявления на прекращение действия сертификата в Удостоверяющий центр по момент времени официального уведомления о прекращении действия сертификата, либо об отказе в прекращении действия.

1.7. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия сертификата, либо об отказе в приостановлении действия.

1.8. Не использовать ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован, действие которого прекращено или приостановлено.

1.9. Использовать для создания и проверки квалифицированных электронных подписей, создания ключей электронной подписи и ключей проверки электронной подписи сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

2. Порядок применения средств квалифицированной электронной подписи

2.1. Средства квалифицированной электронной подписи должны применяться владельцем квалифицированного сертификата ключа проверки электронной подписи в соответствии с положениями эксплуатационной документации на применяемое средство квалифицированной электронной подписи.