

УТВЕРЖДАЮ:

Директор ГКУ ТО «ЦИТТО»



А.Р. Усманов

«15» января 2015 г.

РЕГЛАМЕНТ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

государственного казенного учреждения Тюменской области
«Центр информационных технологий Тюменской области»

Версия 5.2015

Тюмень

2015г.

СОДЕРЖАНИЕ

1	Перечень сокращений	6
2	Термины и определения	7
3	Сведения об Удостоверяющем центре	9
3.1	Назначение.....	9
3.2	Пользователи услуг.....	9
3.3	Контактная информация.....	10
4	Общие положения	11
4.1	Область применения	11
4.2	Присоединение к Регламенту	11
4.3	Публикация Регламента	11
4.4	Изменение и дополнение Регламента	11
4.5	Срок действия Регламента	12
4.6	Расторжение договора присоединения	12
4.7	Разрешение споров.....	12
4.8	Ответственность сторон	12
4.9	Прекращение деятельности.....	13
5	Права и обязанности Сторон.....	14
5.1	Обязанности Удостоверяющего центра.....	14
5.2	Обязанности лица, присоединившегося к Регламенту.....	15
5.3	Обязанности пользователя Удостоверяющего центра	15
5.4	Права Удостоверяющего центра	16
5.5	Права пользователя Удостоверяющего центра.....	16
6	Структура сертификата ключа проверки электронной подписи, изготавливаемого УЦ в электронной форме	17
6.1	Базовые поля сертификата ключа проверки электронной подписи.....	17
6.2	Дополнения сертификата	17
6.3	Объектные идентификаторы алгоритма	17
6.4	Форма сертификата.....	18

6.5	Структура поля идентификационных данных сертификата	18
7	Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме ...	20
8	Процедуры и механизмы	21
8.1	Регистрация пользователей	21
8.2	Изготовление сертификата ключа проверки электронной подписи	21
8.2.1.	Изготовление первого сертификата ключа проверки электронной подписи при личном прибытии пользователя, проходящего процедуру регистрации в Центре регистрации.....	21
8.2.2.	Изготовление первого сертификата ключа проверки электронной подписи самостоятельно посредством web-приложения Удостоверяющего центра	22
8.2.3.	Изготовление сертификата ключа проверки электронной подписи пользователя УЦ при плановой смене ключей при личном прибытии пользователя в Центр регистрации	22
8.2.4.	Изготовление сертификата ключа проверки электронной подписи пользователя УЦ при плановой смене ключей самостоятельно посредством web-приложения, предоставляемого Удостоверяющим центром.....	23
8.2.5.	Изготовление сертификата ключа проверки электронной подписи при внеплановой смене ключей пользователя УЦ.....	23
8.3	Аннулирование сертификата ключа проверки электронной подписи.....	23
8.4	Приостановление действия сертификата ключа проверки электронной подписи.	24
8.5	Порядок возобновления действия сертификата ключа проверки электронной подписи ..	24
8.6	Процедура подтверждения электронной подписи в электронном документе с использованием сертификата ключа проверки электронной подписи	25
8.7	Процедура подтверждения электронной подписи уполномоченного лица УЦ в сертификате ключа проверки электронной подписи.	26
8.8	Механизм доказательства обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи	27
8.9	Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени	27
9	Сроки действия ключевой информации	28
9.1	Срок действия ключевой информации Удостоверяющего центра	28
9.2	Сроки действия ключевой информации Пользователя УЦ	28
9.3	Плановая смена ключей Удостоверяющего центра	29
9.4	Внеплановая смена ключей Удостоверяющего центра.....	29
10	Программный комплекс обеспечения реализации целевых функций	30
11	Ролевое разграничение доступа.....	31
12	Перечень событий, регистрируемых программным обеспечением	32
13	Перечень данных, подлежащих резервному копированию	33
14	Инженерно-технические меры защиты информации	34

14.1	Размещение технических средств	34
14.2	Физический доступ в помещения	34
14.3	Электроснабжение и кондиционирование воздуха	34
14.4	Предупреждение и защита от возгорания	34
14.5	Хранение документированной информации	34
14.6	Уничтожение документированной информации	34
15	Программно-аппаратные меры защиты информации	35
15.1	Организация доступа к техническим средствам	35
15.2	Организация доступа к программным средствам	35
15.3	Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами Удостоверяющего центра	35
15.4	Контроль целостности программного обеспечения	36
15.5	Контроль целостности технических средств	36
15.6	Защита внешних сетевых соединений	36
15.7	Перечень информации, подлежащей защите	36
16	Организационные меры защиты информации	38
16.1	Предъявляемые требования к персоналу	38
16.2	Профессиональная переподготовка и повышение квалификации персонала	38
16.3	Организация работы	38
16.4	Организация доступа персонала к документам и документации	38
16.5	Охрана здания и помещений	38
17	Архивное хранение документированной информации	39
17.1	Состав архивируемых документов	39
17.2	Архивирование ключа электронной подписи	39
17.3	Источник комплектования архивного фонда	39
17.4	Архивохранилище	39
17.5	Срок архивного хранения	39
17.6	Уничтожение архивных документов	39
18	Восстановление после аварий	40
18.1	Восстановление после компрометации	40
18.2	Восстановление после прочих бедствий	40
	Приложение №1	41
	Приложение №2	42
	Приложение №3	43
	Приложение №4	45
	Приложение №5	47
	Приложение №6	48
	Приложение №7	49
	Приложение №8	51

Приложение №9.....	52
Приложение №10.....	53
Приложение №11.....	54
Приложение №12.....	55
Приложение №13.....	56
Приложение №14.....	57
Приложение №15.....	58
Приложение №16.....	59
Приложение №17.....	60
Приложение №18.....	61
Приложение №19.....	62
Приложение №20.....	63
Приложение №21.....	65
Приложение №22.....	67

1 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 отозванных 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

2 Термины и определения

Удостоверяющий центр – государственное казенное учреждение Тюменской области «Центр информационных технологий Тюменской области», осуществляющее на основании распоряжения Правительства Тюменской области №21-рп от 17.01.2011 «Об организации Удостоверяющего центра Тюменской области» выполнение целевых функций удостоверяющего центра в соответствии с Федеральным законом №63-ФЗ от 06.04.2011 «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 – сотрудник Удостоверяющего центра либо организация, заключившая договор с Удостоверяющим центром, осуществляющие выдачу сертификатов ключей проверки электронной подписи согласно настоящему Регламенту.

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

Электронная подпись (ЭП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа проверки электронной подписи, а также установить отсутствие искажения информации в электронном документе.

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, подписавшее 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 доверенным 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, выданный аккредитованным Удостоверяющим центром либо Доверенным лицом аккредитованного Удостоверяющего центра в форме, требования к которой утверждены Приказом ФСБ России от 27

декабря 2011 года № 795 «Об утверждении требований к форме квалифицированного сертификата ключа проверки 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 Регламентом 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 Standarts (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 подписанном данной электронной подписью электронном документе.

Пользователь Удостоверяющего центра (Пользователь УЦ) – физические лица и юридические лица, зарегистрированные в УЦ ГКУ ТО «ЦИТТО», и являющиеся владельцами сертификата ключа проверки электронной подписи.

3 Сведения об Удостоверяющем центре

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 изготовлению и выдаче сертификатов ключей проверки электронной подписи на территории Российской Федерации на основании следующих документов:

1. Лицензия ФСБ России ЛЗ № 0020530 рег.№ 195Р от 15 февраля 2011 г. на осуществление деятельности по распространению шифровальных (криптографических) средств;
2. Лицензия ФСБ России ЛЗ № 0020531 рег.№ 196Х от 15 февраля 2011 г. на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств;
3. Лицензия ФСБ России ЛЗ № 0020532 рег.№ 197У от 15 февраля 2011 г. на предоставление услуг в области шифрования информации;
4. Приказ Министерства связи и массовых коммуникаций Российской Федерации №150 от 28 июня 2013 г. «Об аккредитации удостоверяющих центров».

3.1 Назначение

Удостоверяющий центр предназначен для предоставления следующих услуг:

- внесение в реестр УЦ регистрационной информации о пользователях УЦ;
- изготовление сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- формирование ключей электронной подписи и ключей проверки электронной подписи по обращениям пользователей УЦ с записью их на ключевой носитель;
- ведение реестра изготовленных сертификатов ключей проверки электронной подписи пользователей УЦ;
- аннулирование (отзыв) сертификатов ключей проверки электронной подписи пользователей УЦ по обращениям владельцев сертификатов ключей проверки электронной подписи;
- приостановление и возобновление действия сертификатов ключей проверки электронной подписи пользователей УЦ по обращениям владельцев сертификатов ключей проверки электронной подписи;
- предоставление пользователям УЦ сведений об аннулированных (отозванных) и приостановленных сертификатах ключей проверки электронной подписи;
- подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям пользователей УЦ;
- подтверждение подлинности электронной подписи уполномоченного лица УЦ в изготовленных им сертификатах ключей проверки электронной подписи по обращениям пользователей УЦ.

3.2 Пользователи услуг

Проходить регистрацию в Удостоверяющем центре могут как физические лица, так и юридические лица.

Владельцем сертификата ключа проверки электронной подписи может быть только физическое лицо, присоединившееся к Регламенту и зарегистрированное в Удостоверяющем центре (в случае присоединения к Регламенту юридического лица – физическое лицо, являющееся уполномоченным представителем юридического лица).

Физическое лицо может представлять юридическое лицо на основании доверенности, дающей право данному физическому лицу пользоваться услугами Удостоверяющего центра, и представлять интересы юридического лица.

В случае если физическое лицо действует от имени юридического лица на основании учредительных документов в Удостоверяющий центр представляется нотариально заверенная копия учредительных документов, подтверждающих полномочия физического лица.

В случае если сертификат ключа проверки электронной подписи Пользователя УЦ выдаётся для обеспечения работоспособности устройств, назначается ответственное лицо, на имя которого выпускается сертификат.

3.3 Контактная информация

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

Факс: (3452) 54-30-46

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

4 Общие положения

4.1 Область применения

Настоящий Регламент определяет условия предоставления и правила пользования услугами Удостоверяющего центра, включая права, обязанности, ответственность Сторон, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего центра.

4.2 Присоединение к Регламенту

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

Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр Заявления о присоединении к Регламенту по форме Приложений №№ 1, 2 настоящего Регламента

Присоединение лица к Регламенту подтверждает полное принятие им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении в реестре Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента

После присоединения к настоящему Регламенту Удостоверяющий центр и лицо, присоединившееся к Регламенту, вступают в соответствующие договорные отношения на неопределённый срок.

4.3 Публикация Регламента

Настоящий Регламент 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 Регламенту, по его требованию.

4.4 Изменение и дополнение Регламента

4.4.1. Изменения, дополнения в Регламент, а также в приложения к нему вносятся Удостоверяющим центром в одностороннем порядке.

4.4.2. Уведомление о внесении изменений, дополнений в Регламент осуществляется Удостоверяющим центром путем обязательного размещения указанных изменений, дополнений на сайте по адресу – **<http://ca.72to.ru>**

4.4.3. Все изменения, дополнения, вносимые Удостоверяющим центром в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении одного месяца с даты размещения указанных изменений, дополнений на сайте по адресу - **<http://ca.72to.ru>**

4.4.4. Все изменения, дополнения, вносимые Удостоверяющим центром в Регламент в связи с изменением законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений, дополнений в нормативных правовых актах.

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

4.5 Срок действия Регламента

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

Срок действия Регламента 9 лет.

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

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

4.6 Расторжение договора присоединения

4.6.1. Действие договора присоединения может быть прекращено по инициативе одной из Сторон. В этом случае Сторона письменно уведомляет другую Сторону о своих намерениях за 30 (тридцать) календарных дней до даты расторжения договора.

4.6.2. Уведомление о расторжении договора, полученное Удостоверяющим центром от Пользователя УЦ является основанием для обязательного аннулирования (отзыва) сертификатов ключей проверки электронной подписи пользователя УЦ.

4.6.3. Датой аннулирования (отзыва) данных сертификатов ключей проверки электронной подписи Пользователя УЦ будет дата расторжения договора о присоединении к Регламенту.

4.7 Разрешение споров

При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны руководствуются действующим законодательством Российской Федерации.

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

Сторона, получившая от другой Стороны претензию, обязана в течение 15 (пятнадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ. К ответу должны быть приложены все необходимые документы.

Порядок разрешения конфликтных ситуаций, связанных с использованием электронной подписи при обеспечении электронного документооборота осуществляется в соответствии с документом «Положение о порядке разбора конфликтных ситуаций связанных с использованием электронной подписи».

Спорные вопросы между Сторонами, не урегулированные в претензионном порядке, решаются в Арбитражном суде Тюменской области.

4.8 Ответственность сторон

Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, 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.

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

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 Регламента, выявленного в установленном законодательством порядке. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется в соответствии с законодательством Российской Федерации.

4.9 Прекращение деятельности

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

В случае прекращения деятельности Удостоверяющего центра все сертификаты ключей проверки электронной подписи Пользователей УЦ, выданные этим Удостоверяющим центром, могут быть переданы другому Удостоверяющему центру по согласованию с владельцами сертификатов. Сертификаты ключей проверки электронной подписи Пользователей УЦ, не переданные в другой Удостоверяющий центр, аннулируются.

Архивы Удостоверяющего центра сохраняются в порядке и на сроки, согласно разделу 17 настоящего Регламента.

5 Права и обязанности Сторон

5.1 Обязанности Удостоверяющего центра

Удостоверяющий центр обязан:

- Использовать в своей работе, в том числе для издания сертификатов ключей проверки электронной подписи Пользователей УЦ и формирования электронной подписи только сертифицированные средства криптографической защиты информации;
- Использовать ключ электронной подписи уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей проверки электронной подписи и списков отозванных сертификатов;
- Предоставить Пользователю УЦ 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 Регламенте;
- Обеспечить изготовление сертификата ключа проверки электронной подписи зарегистрированного в Удостоверяющем центре Пользователя УЦ по заявлению на изготовление сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте;
- 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 сохранение в тайне созданного ключа электронной подписи Пользователя УЦ;
- Аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя УЦ по заявлению об аннулировании (отзыве) сертификата ключа проверки электронной подписи в соответствии с порядком, определенным в настоящем Регламенте;
- 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 Регламенте;
- 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 Регламенте;
- Официально уведомить об аннулировании (отзыве), приостановлении и возобновлении действия сертификата ключа проверки электронной подписи Пользователей УЦ посредством публикации списка отозванных сертификатов;
- Осуществлять плановую и внеплановую публикацию актуального списка отозванных сертификатов ключей проверки электронной подписи Пользователей УЦ на сайте Удостоверяющего центра <http://ca.72to.ru>. Плановая публикация списка отозванных сертификатов ключей проверки электронной подписи Пользователей УЦ производится не реже одного раза в месяц. Внеплановая публикация СОС производится по мере необходимости включения записей;
- Уведомлять владельца сертификата ключа проверки электронной подписи о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа проверки электронной подписи;

- Вести реестр всех изготовленных 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 изготовленных сертификатов.

5.2 Обязанности лица, присоединившегося к Регламенту

- Лицо, присоединившееся к Регламенту, обязано 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 Регламенте с целью обеспечения гарантированного ознакомления с полным текстом изменений, дополнений Регламента до вступления их в силу.

5.3 Обязанности пользователя Удостоверяющего центра

Пользователь УЦ обязан:

- Представить регистрационную и идентифицирующую информацию для регистрации в Удостоверяющем центре в объеме, определенном положениями настоящего Регламента;
- 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.

5.4 Права Удостоверяющего центра

Удостоверяющий центр имеет право:

- Не проводить регистрацию лиц, обратившихся по вопросу представления копий сертификатов ключей проверки электронной подписи в электронной форме, находящихся в реестре Удостоверяющего центра;
- Отказать в предоставлении услуг по регистрации пользователей УЦ лицам, подавшим заявление на регистрацию, без предоставления информации о причинах отказа;
- Отказать в изготовлении ключей лицам, не зарегистрированным в Удостоверяющем центре, подавшим заявление на изготовление ключей, без предоставления информации о причинах отказа;
- Отказать в изготовлении сертификата ключа проверки электронной подписи зарегистрированным пользователям УЦ, подавшим заявление на изготовление сертификата ключа проверки электронной подписи, с указанием причин отказа;
- Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи пользователю УЦ, подавшему заявление на аннулирование (отзыв) 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 установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием обоснованных причин;
- Приостановить действие сертификата ключа проверки электронной подписи пользователя УЦ, с уведомлением владельца приостановленного сертификата ключа проверки электронной подписи и указанием обоснованных причин.

5.5 Права пользователя Удостоверяющего центра

Пользователь УЦ имеет право:

- Получить сертификат ключа проверки электронной подписи уполномоченного лица Удостоверяющего центра;
- Получить список отозванных сертификатов ключей проверки электронной подписи, изготовленный 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 изготовления сертификата ключа проверки электронной подписи;
- Обратиться в Удостоверяющий центр для аннулирования (отзыва) 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.

6 Структура сертификата ключа проверки электронной подписи, изготавливаемого УЦ в электронной форме

Удостоверяющий центр издает сертификаты ключей проверки электронной подписи пользователей УЦ и уполномоченного лица Удостоверяющего центра в электронной форме (далее по тексту раздела – СКПЭП) формата X.509 версии 3.

6.1 Базовые поля сертификата ключа проверки электронной подписи

Квалифицированные СКПЭП содержат следующие базовые поля X.509:

Version	Версия сертификата формата X.509 - версия 3
SerialNumber	Уникальный серийный (регистрационный) номер сертификата в Реестре СКПЭП Удостоверяющего центра
Signature	Электронная подпись уполномоченного лица УЦ
Issuer	Идентифицирующие данные уполномоченного лица УЦ
Validity	Даты начала и окончания срока действия СКПЭП
Subject	Идентифицирующие данные владельца СКПЭП
SubjectPublicKeyInfo	Идентификатор алгоритма средства электронной подписи, с которыми используется данный ключ проверки электронной подписи, значение ключа проверки электронной подписи
Extensions	Дополнительная информация, касающаяся использования СКПЭП

6.2 Дополнения сертификата

Квалифицированные СКПЭП содержат следующие дополнения (Extensions):

AuthorityKeyIdentifier	Идентификатор ключа уполномоченного лица УЦ
SubjectKeyIdentifier	Идентификатор ключа владельца СКПЭП
KeyUsage	Область (области) использования ключа
ExtendedKeyUsage	Расширенное использование ключа
CertificatePolicies	Политики сертификата
SubjectSignTool	Средство ЭП владельца сертификата
IssuerSignTool	Средство ЭП Удостоверяющего центра
CRLDistributionPoint	Точка распространения списка аннулированных (отозванных) сертификатов ключей проверки электронной подписи, изданных Удостоверяющим центром

6.3 Объектные идентификаторы алгоритма

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства электронной подписи, имеющего наименование «СКЗИ КриптоПро CSP»:

ГОСТ Р 34.10-94	1.2.643.2.2.20	Алгоритм открытых ключей
ГОСТ Р 34.10-2001	1.2.643.2.2.19	Алгоритм открытых ключей
Диффи-Хеллмана	1.2.643.2.2.99	Алгоритм на базе экспоненциальной функции
Диффи-Хеллмана	1.2.643.2.2.98	Алгоритм на базе эллиптической кривой
ГОСТ Р 34.11-94	1.2.643.2.2.9	Алгоритм хеширования
ГОСТ 28147-89	1.2.643.2.2.21	Алгоритм шифрования

6.4 Форма сертификата

В сертификате ключа проверки электронной подписи поля идентификационных данных уполномоченного лица Удостоверяющего центра и владельца сертификата содержат атрибуты имени формата X.509.

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

6.5 Структура поля идентификационных данных сертификата

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего центра являются:

CommonName	Псевдоним Удостоверяющего центра
Organization	Наименование организации
OrganizationUnit	Наименование подразделения организации, в случае выпуска сертификата на должностное лицо
Country	RU
State	Субъект РФ местонахождения ПАК УЦ
Locality	Населенный пункт местонахождения ПАК УЦ
OGRN	ОГРН организации
INN	ИНН организации

Обязательными атрибутами поля идентификационных данных владельца квалифицированного сертификата, являющегося физическим лицом, являются:

CommonName	Фамилия, имя, отчество
SNILS	СНИЛС

Обязательными атрибутами поля идентификационных данных владельца квалифицированного сертификата, являющегося юридическим лицом, являются:

CommonName	Наименование организации
Country	RU
State	Субъект РФ, где зарегистрирована организация
Locality	Населенный пункт, где зарегистрирована организация
OGRN	ОГРН организации
INN	ИНН организации

Обязательными атрибутами поля идентификационных данных владельца квалифицированного сертификата, являющегося физическим лицом и представляющего юридическое лицо, являются:

CommonName	Фамилия, имя, отчество
Organization	Наименование организации, которую представляет владелец сертификата
OrganizationUnit	Наименование подразделения организации, сотрудником которого является владелец сертификата
Country	RU
State	Субъект РФ, где зарегистрирована организация, которую представляет

	владелец сертификата
Locality	Населенный пункт, где зарегистрирована организация, которую представляет владелец сертификата
OGRN	ОГРН организации
INN	ИНН организации

7 Структура списка отозванных сертификатов, изготавливаемого УЦ в электронной форме

Удостоверяющий центр издает списки отозванных 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 отозванных сертификатов включает себя следующие поля:

Базовые поля списка отозванных сертификатов	
Version	Версия
Issuer	Издатель СОС
thisUpdate	Дата выпуска текущего СОС
nextUpdate	Дата выпуска следующего СОС
revokedCertificates	Список отозванных сертификатов
signatureAlgorithm	Алгоритм подписи
Issuer Sign	Подпись издателя СОС
Расширения списка отозванных сертификатов	
Authority Key Identifier	Идентификатор ключа уполномоченного лица Удостоверяющего центра
cRLNumber	Номер списка отозванных сертификатов
IssuingDistributionPoint	Атрибуты выпускающего пункта распространения СОС
deltaCRLIndicator	Индикатор СОС как разностного списка отозванных сертификатов (дельта-списка)
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
szOID_CERTSRV_CA_VERSION	Объектный идентификатор MS Certificate Server, определяющий версию службы сертификации MS CA
holdInstructionCode	Код временного приостановления сертификата (OID)
invalidateDate	Дата утраты валидности сертификата
certificateIssuer	Имя издателя сертификата, ассоциированного с косвенным СОС

8 Процедуры и механизмы

8.1 Регистрация пользователей

Регистрация Пользователя УЦ осуществляется при личном прибытии регистрирующегося лица (либо его уполномоченного представителя) в Центр регистрации Удостоверяющего центра (далее – ЦР).

Под регистрацией пользователя понимается занесение идентификационной информации регистрирующегося лица в реестр Пользователей УЦ. Реестр ведется в электронной базе данных и в бумажном архиве.

Регистрация пользователя в Удостоверяющем центре и изготовление первого сертификата ключа проверки электронной подписи осуществляется на основании заявления на регистрацию при личном прибытии пользователя в ЦР Удостоверяющего центра. Форма заявления на регистрацию приведена в Приложениях №№ 3-6 к настоящему Регламенту.

К заявлению физического лица, представляющего юридическое лицо, прилагается доверенность, подтверждающая правомочность действий от имени юридического лица.

Заявитель заверяет заявление на регистрацию собственноручной подписью и передает заявление вместе с необходимыми приложениями сотруднику ЦР Удостоверяющего центра.

Регистрация пользователя в Удостоверяющем центре может быть осуществлена уполномоченным представителем пользователя УЦ, действующим на основании доверенности на осуществление регистрации в Удостоверяющем центре. Доверенность на осуществление регистрации в Удостоверяющем центре должна быть составлена по форме Приложений №№ 10-11 настоящего Регламента. Доверенность, выданная физическим лицом, должна быть заверена нотариально.

Сотрудник ЦР Удостоверяющего центра выполняет процедуру идентификации лица, проходящего процедуру регистрации или доверенного лица, путем установления личности по паспорту и выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего центра.

8.2 Изготовление сертификата ключа проверки электронной подписи

Пользователь УЦ на свое усмотрение определяет порядок изготовления первого сертификата ключа проверки электронной подписи:

- изготовление сертификата ключа проверки электронной подписи осуществляет сотрудник ЦР Удостоверяющего центра при личном прибытии пользователя (либо его уполномоченного представителя);
- изготовление сертификата ключа проверки электронной подписи осуществляет пользователь самостоятельно посредством web-приложения Удостоверяющего центра.

8.2.1. Изготовление первого сертификата ключа проверки электронной подписи при личном прибытии пользователя, проходящего процедуру регистрации в Центре регистрации.

По окончании процедуры регистрации пользователя в реестре УЦ Удостоверяющего центра ответственный сотрудник ЦР Удостоверяющего центра изготавливает ключ подписи, сертификат ключа проверки электронной подписи и записывает их на ключевой носитель.

Формирование ключей подписи и сертификата ключа проверки электронной подписи пользователя УЦ осуществляется на основании заявления на изготовление сертификата ключа проверки электронной подписи. Заявление на изготовление сертификата ключа проверки электронной подписи подается в ЦР Удостоверяющего центра в бумажной форме при личном прибытии пользователя. Форма заявления приведена в Приложениях №№ 3-6 к настоящему Регламенту.

Данные документы могут быть предоставлены уполномоченным представителем пользователя УЦ, действующим на основании доверенности на получение ключей подписи и сертификата в Удостоверяющем центре. Доверенность должна быть составлена по форме Приложений №№ 10, 11 настоящего Регламента. Доверенность, выданная физическим лицом, должна быть заверена нотариально.

По окончании процедуры изготовления сертификата ключа проверки электронной подписи пользователю УЦ выдаются:

- ключевой носитель, содержащий ключ электронной подписи;
- сертификат ключа проверки электронной подписи пользователя УЦ, соответствующий ключу электронной подписи (записывается на ключевой носитель).

8.2.2. Изготовление первого сертификата ключа проверки электронной подписи самостоятельно посредством web-приложения Удостоверяющего центра

По окончании процедуры регистрации пользователя в реестре Удостоверяющего центра посредством web-приложения, предоставляемого Удостоверяющим центром пользователь самостоятельно формирует ключевую пару и записывает ее на ключевой носитель. Сформированный файл запроса на сертификат ключа проверки электронной подписи пользователь передает в Удостоверяющий центр.

Изготовление сертификата ключа проверки электронной подписи пользователя УЦ осуществляется на основании файла запроса на сертификат и заявления на изготовление сертификата ключа проверки электронной подписи. Заявление на изготовление сертификата ключа проверки электронной подписи подается в ЦР Удостоверяющего центра в бумажной форме при личном прибытии пользователя. Форма заявления приведена в Приложениях №№ 3-6 к настоящему Регламенту.

Данные документы могут быть предоставлены уполномоченным представителем пользователя УЦ, действующим на основании доверенности на получение ключей подписи и сертификата в Удостоверяющем центре. Доверенность должна быть составлена по форме Приложений №№ 10, 11 настоящего Регламента. Доверенность, выданная физическим лицом, должна быть заверена нотариально.

После поступления заявления в ЦР Удостоверяющего центра сотрудник УЦ Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата с информацией, указанной в запросе на сертификат, поданном в электронной форме, и принимает решение об изготовлении сертификата ключа проверки электронной подписи.

В случае отказа в изготовлении сертификата ключа проверки электронной подписи пользователь УЦ уведомляется об этом с указанием причины отклонения заявления.

При принятии положительного решения, ответственный сотрудник УЦ Удостоверяющего центра изготавливает сертификат ключа проверки электронной подписи и передает его пользователю.

Пользователь УЦ получает сертификат ключа проверки электронной подписи и записывает его на ключевой носитель посредством web-приложения.

8.2.3. Изготовление сертификата ключа проверки электронной подписи пользователя УЦ при плановой смене ключей при личном прибытии пользователя в Центр регистрации

Формирование ключей подписи и сертификата ключа проверки электронной подписи пользователя УЦ осуществляется в ЦР Удостоверяющего центра на основании заявления на изготовление сертификата ключа проверки электронной подписи. Заявление на изготовление сертификата ключа проверки электронной подписи подается в ЦР в бумажной форме при личном прибытии пользователя.

Форма заявления на изготовление ключей подписи и сертификата ключа проверки электронной подписи приведена в Приложениях №№ 8, 9 к настоящему Регламенту.

Данные документы могут быть предоставлены уполномоченным представителем пользователя УЦ, действующим на основании доверенности на получение ключей подписи и сертификата в

Удостоверяющем центре. Доверенность должна быть составлена по форме Приложений №№ 10, 11 настоящего Регламента. Доверенность, выданная физическим лицом, должна быть заверена нотариально.

После положительной идентификации пользователя УЦ или доверенного лица сотрудник ЦР принимает документы, осуществляет их рассмотрение и изготавливает ключи подписи и сертификат ключа проверки электронной подписи на предоставляемый пользователем УЦ или его представителем ключевой носитель.

8.2.4. Изготовление сертификата ключа проверки электронной подписи пользователя УЦ при плановой смене ключей самостоятельно посредством web-приложения, предоставляемого Удостоверяющим центром

Посредством web-приложения, предоставляемого Удостоверяющим центром пользователь самостоятельно формирует ключевую пару и записывает ее на ключевой носитель. Сформированный файл запроса на сертификат ключа проверки электронной подписи пользователь передает в Удостоверяющий центр. В качестве подписываемых данных используются данные файла запроса на сертификат ключа проверки электронной подписи пользователя УЦ, а электронная подпись осуществляется на действующем ключе электронной подписи пользователя УЦ.

Удостоверяющий центр осуществляет изготовление и предоставление пользователю сертификата ключа проверки электронной подписи для записи на ключевой носитель посредством web-приложения.

8.2.5. Изготовление сертификата ключа проверки электронной подписи при внеплановой смене ключей пользователя УЦ

Внеплановая смена ключей осуществляется пользователем в следующих случаях:

- при компрометации ключа электронной подписи пользователя УЦ;
- при компрометации ключа электронной подписи уполномоченного лица УЦ;
- в случае, если пользователь по каким-либо причинам не смог осуществить плановую смену ключей в установленные для этой процедуры сроки;
- в иных случаях, вызванных форс-мажорными обстоятельствами.

Изготовление сертификата ключа проверки электронной подписи при внеплановой смене ключей осуществляется аналогично процедуре изготовления первого сертификата пользователя УЦ (8.2.1-8.2.2).

8.3 Аннулирование сертификата ключа проверки электронной подписи

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

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

Аннулирование (отзыв) сертификата ключа проверки электронной подписи и официальное уведомление пользователя УЦ об аннулировании (отзыве) сертификата ключа проверки электронной подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было принято заявление на отзыв Удостоверяющим центром.

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.

Заявление на отзыв сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе по форме Приложений №№ 12, 13 настоящего

Регламента, заверенный собственноручной подписью заявителя. Заявление включает в себя следующие обязательные реквизиты:

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

8.4 Приостановление действия сертификата ключа проверки электронной подписи.

Приостановление действия сертификата ключа проверки электронной подписи, изготовленного Удостоверяющим центром, осуществляется Удостоверяющим центром по заявлению на отзыв 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.

Приостановление действия сертификата ключа проверки электронной подписи и официальное уведомление пользователя УЦ о приостановлении действия сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было принято заявление Удостоверяющим центром.

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 Регламента, 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.

8.5 Порядок возобновления действия сертификата ключа проверки электронной подписи

Возобновление действия сертификата ключа проверки электронной подписи, изготовленного 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.

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.

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 Регламента, 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.

8.6 Процедура подтверждения электронной подписи в электронном документе с использованием сертификата ключа проверки электронной подписи

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. 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 электронного документа.

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».

Результатом проведения работ по подтверждению подлинности электронной подписи в электронном документе является заключение Удостоверяющего центра, 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.

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.

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

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

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.

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.

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.

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 подписанном 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.

8.8 Механизм доказательства обладания ключом электронной подписи, соответствующим ключу проверки электронной подписи

Заявления на изготовление 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 изготовление сертификата ключа проверки электронной подписи подтверждает, что заявитель является владельцем ключа электронной подписи, соответствующего ключу проверки электронной подписи из запроса на сертификат.

8.9 Предоставление Удостоверяющим центром сервисов Службы актуальных статусов сертификатов и Службы штампов времени

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/ocsp/ocsp.srf>. Указанный адрес заносится в расширение Authority Information Access (AIA) создаваемых Удостоверяющим центром сертификатов ключей проверки электронной подписи.

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:

- Выполнены условия признания квалифицированной электронной подписи в штампе времени;
- 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».

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

9 Сроки действия ключевой информации

9.1 Срок действия ключевой информации Удостоверяющего центра

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.

Срок действия сертификата ключа проверки электронной подписи уполномоченного лица УЦ составляет 9 (девять) лет. Время начала периода действия сертификата ключа проверки электронной подписи Удостоверяющего центра и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

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

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

Срок действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата ключа проверки электронной подписи Службы актуальных статусов сертификатов и его окончания заносится в поля «notBefore» и «notAfter» поля «Validity Period» соответственно.

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.

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 «notAfter» поля «Validity Period» соответственно.

9.2 Сроки действия ключевой информации Пользователя УЦ

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.

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 «notAfter» поля «Validity» соответственно.

9.3 Плановая смена ключей Удостоверяющего центра

Плановая смена ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи уполномоченного лица УЦ выполняется в период действия ключа электронной подписи.

Процедура плановой смены ключей уполномоченного лица УЦ определяется эксплуатационной документацией на средства Удостоверяющего центра и осуществляется в следующем порядке:

- Удостоверяющий центр создает новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;
- Удостоверяющий центр создает новый сертификат ключа проверки электронной подписи.

Уведомление пользователей о проведении смены ключей уполномоченного лица УЦ осуществляется посредством размещения сведений на сайте Удостоверяющего центра <http://ca.72to.ru/>.

Старый ключ электронной подписи уполномоченного лица УЦ используется в течение своего срока действия для формирования списков отозванных сертификатов, созданных Удостоверяющим центром в период действия старого ключа электронной подписи уполномоченного лица Удостоверяющего центра.

9.4 Внеплановая смена ключей Удостоверяющего центра

В случае нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификат ключа проверки электронной подписи Удостоверяющего центра прекращает действие, Пользователи Удостоверяющего центра уведомляются об указанном факте путем публикации информации о нарушении конфиденциальности ключа электронной подписи Удостоверяющего центра на сайте Удостоверяющего центра <http://ca.72to.ru/>. Все сертификаты, подписанные с использованием ключа Удостоверяющего центра, конфиденциальность которого нарушена, считаются прекратившими действие.

После прекращения действия сертификата ключа проверки электронной подписи Удостоверяющего центра выполняется процедура внеплановой смены ключей Удостоверяющего центра. Процедура внеплановой смены ключей Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего центра.

Все действовавшие на момент нарушения конфиденциальности ключа электронной подписи Удостоверяющего центра сертификаты ключей проверки электронной подписи, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

10 Программный комплекс обеспечения реализации целевых функций

Для выполнения своих целевых функций Удостоверяющий центр использует следующее программное обеспечение от компании КристоПро:

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

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.

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 изготовление сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- ведение Реестра запросов на аннулирование (отзыв) 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.

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 изготовления сертификатов.

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, изготовленных Удостоверяющим центром в электронной форме.

11 Ролевое разграничение доступа

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:

- администратор Удостоверяющего центра.
- оператор Удостоверяющего центра.

Основные действия, осуществляемые привилегированными пользователями УЦ:

- регистрация пользователя, включающая создание регистрационной записи в базе данных Центра Регистрации Удостоверяющего центра;
- изготовление сертификата ключа проверки электронной подписи пользователя;
- управление сертификатами ключей проверки электронной подписи пользователя;
- 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

12 Перечень событий, регистрируемых программным обеспечением

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

Центром Сертификации:

- установлено сетевое соединение с программной компонентой Центра Регистрации;
- издан СОС;
- принят запрос на сертификат;
- издание сертификата;
- невыполнение внутренней операции программной компоненты;
- системные события общесистемного программного обеспечения.

Центром Регистрации:

- помещен запрос на регистрацию;
- принят запрос на регистрацию;
- отклонен запрос на регистрацию;
- помещен запрос на сертификат;
- принят запрос на сертификат;
- отклонен запрос на сертификат;
- установка сертификата подтверждена пользователем;
- помещен запрос на отзыв сертификата;
- принят запрос на отзыв сертификата;
- отклонен запрос на отзыв сертификата;
- помещен запрос на первый сертификат;
- запрошен список отозванных сертификатов;
- опубликован список отозванных сертификатов;
- невыполнение внутренней операции программной компоненты;
- установлено сетевое соединение с внешней программной компонентой;
- системные события общесистемного программного обеспечения.

13 Перечень данных, подлежащих резервному копированию

Для обеспечения функциональности Удостоверяющего центра необходимо ежедневно 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.

14 Инженерно-технические меры защиты информации

14.1 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.

14.2 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.

14.3 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.

14.4 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.

14.5 Хранение документированной информации

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

14.6 Уничтожение документированной информации

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

15 Программно-аппаратные меры защиты информации

15.1 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, утвержденном директором ГКУ ТО «ЦИТТО».

15.2 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 утвержден приказом директора ГКУ ТО «ЦИТТО».

15.3 Перечень объектов доступа, предоставляемых аутентифицированным пользователям УЦ при осуществлении сетевого взаимодействия с программными средствами Удостоверяющего центра

Аутентифицированным Пользователям УЦ предоставляются следующие объекты доступа:

- копия сертификата ключа проверки электронной подписи уполномоченного лица УЦ в электронной форме;
- копия списка аннулированных (отозванных) сертификатов ключей проверки электронной подписи в электронной форме;
- копии сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме;
- программное обеспечение предоставления учетной информации о сертификатах ключей проверки электронной подписи аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение предоставления учетной информации о запросах (заявлениях) в электронной форме, поступивших на Удостоверяющий центр от аутентифицированного пользователя УЦ и статусе их обработки;
- программное обеспечение формирования ключей и заявления на сертификат ключа проверки электронной подписи в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение получения и установки на рабочем месте изданного сертификата ключа проверки электронной подписи аутентифицированного пользователя УЦ;
- программное обеспечение формирования электронного бланка копии сертификата ключа проверки электронной подписи аутентифицированного пользователя УЦ в бумажной форме;
- программное обеспечение формирования заявления на аннулирование (отзыв) сертификата ключа проверки электронной подписи в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение формирования заявления на приостановление действия сертификата ключа проверки электронной подписи в электронной форме аутентифицированного пользователя УЦ;

- программное обеспечение формирования заявления на возобновление действия сертификата ключа проверки электронной подписи в электронной форме аутентифицированного пользователя УЦ;
- программное обеспечение предоставления учетной информации о сертификатах ключей проверки электронной подписи пользователей УЦ и копий сертификатов ключей проверки электронной подписи пользователей УЦ в электронной форме.

15.4 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.

Состав программных модулей, подлежащих контролю целостности, определяется внутренним документом, утверждаемым руководителем Удостоверяющего центра. Контроль целостности программных модулей средств электронной подписи и криптографической защиты информации осуществляется средствами электронной подписи и криптографической защиты информации. Периодичность выполнения мероприятий по контролю целостности – ежеквартально. Ответственность за выполнение мероприятий по контролю целостности программных средств возложена на Удостоверяющий центр.

15.5 Контроль целостности технических средств.

Контроль целостности технических средств Удостоверяющего центра обеспечивается ограничением физического доступа в Серверное помещение. Ответственность за выполнение мероприятий по контролю целостности технических средств возложена на ГКУ ТО «ЦИТТО».

15.6 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.

15.7 Перечень информации, подлежащей защите

Поступающая в Удостоверяющий центр информация:

- заявление на регистрацию в электронной форме;
- заявление на изготовление сертификата ключа проверки электронной подписи в электронной форме;
- заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи в электронной форме;
- заявление на приостановление действия сертификата ключа проверки электронной подписи в электронной форме;

- заявление на возобновление действия сертификата ключа проверки электронной подписи в электронной форме;
- пароль, передаваемый пользователем УЦ при аутентификации по паролю;
- ключевая фраза пользователя УЦ.

Передаваемая из Удостоверяющего центра информация:

- пароль, передаваемый пользователю УЦ для аутентификации по паролю;
- список сертификатов ключа проверки электронной подписи пользователя УЦ и их статус;
- список запросов на сертификаты ключей проверки электронной подписи пользователя УЦ и их статус;
- список запросов на аннулирование (отзыв), приостановление и возобновление действия сертификатов ключей проверки электронной подписи пользователя УЦ и их статус.

16 Организационные меры защиты информации

16.1 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.

16.2 Профессиональная переподготовка и повышение квалификации персонала

Сотрудники Удостоверяющего центра осуществляют повышение квалификации в областях знаний согласно занимаемым должностям не реже одного раза в 2 года.

16.3 Организация работы

Деятельность по работе с пользователями УЦ в части приема заявлений в бумажной форме и изготовления 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.

16.4 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.

16.5 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.

17 Архивное хранение документированной информации

17.1 Состав архивируемых документов

Архивированию подлежит следующая документированная информация:

- заявления о присоединении к настоящему Регламенту;
- заявления на регистрацию пользователей УЦ;
- заявления на изготовление сертификатов ключей проверки электронной подписи;
- сертификаты 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.

17.2 Архивирование ключа электронной подписи

Удостоверяющий центр ни при каких обстоятельствах не хранит и не архивирует ключи электронной подписи пользователей УЦ - владельцев сертификатов ключей проверки электронной подписи.

17.3 Источник комплектования архивного фонда

Источником комплектования архивного фонда Удостоверяющего центра являются подразделения (службы) ГКУ ТО «ЦИТТО», обеспечивающие документирование.

17.4 Архивохранилище

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

17.5 Срок архивного хранения

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

17.6 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».

18 Восстановление после аварий

18.1 Восстановление после компрометации

В случае компрометации ключа ЦС, используемого для подписи сертификатов и СОС, Удостоверяющий центр должен быть остановлен.

Для восстановления работы Удостоверяющего центра необходимо:

- повторно произвести формирование ключа и сертификата ЦС;
- произвести выпуск новых сертификатов всех пользователей УЦ;
- обеспечить получение новых личных сертификатов пользователями УЦ.

18.2 Восстановление после прочих бедствий

В случае повреждения оборудования ЦС 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 18.1.

Для юридических лиц

Заявление о присоединении
к Регламенту Удостоверяющего центра*

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

действующего на основании

1. В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту 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 Регламентом 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 Регламенту 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 Регламенту подается в Удостоверяющий центр в двух экземплярах. После регистрации Заявления в Удостоверяющем центре один экземпляр предоставляется заявителю

Для физических лиц

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

**Заявление на регистрацию пользователя и изготовление
квалифицированного сертификата ключа проверки электронной подписи**

(полное наименование организации, включая организационно-правовую форму)
в лице
(должность, фамилия, имя, отчество)
действующего на основании

1. Просит зарегистрировать

(общее имя)
(серия и номер паспорта должностного лица, кем и когда выдан)

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

Общее имя (CommonName)	ФИО должностного лица
Организация (Organization)	Полное или сокращенное наименование организации
Подразделение (OrganizationUnit)	Подразделение/отдел организации (если имеется)
Должность (Title)	Должность
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ
Город (Locality)	Наименование населенного пункта
Улица (Street)	Улица, номер дома, корпуса, строения, помещения
ОГРН (OGRN)	ОГРН организации
ИНН (INN)	ИНН организации
СНИЛС (SNILS)	Рекомендуется к включению для упрощения идентификации должностных лиц
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

3. 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

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

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

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

действующего на основании

1. Просит зарегистрировать

(общее имя)

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

Общее имя (CommonName)	Наименование информационной системы
Организация (Organization)	Полное или сокращенное наименование организации
Подразделение (OrganizationUnit)	Подразделение/отдел организации (если имеется)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ
Город (Locality)	Наименование населенного пункта
Улица (Street)	Улица, номер дома, корпуса, строения, помещения
ОГРН (OGRN)	ОГРН организации
ИНН (INN)	ИНН организации
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

3. 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

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

(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.

Для физических лиц

**Заявление на регистрацию пользователя и изготовление
квалифицированного сертификата ключа проверки электронной подписи**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. Прошу зарегистрировать меня в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и изготовить ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

3. 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

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

Для физических лиц

**Заявление на регистрацию пользователя и изготовление КСКП
электронной подписи на Универсальной электронной карте (УЭК)**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1. Прошу зарегистрировать меня в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и изготовить ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Улица (Street)	Улица, номер дома, корпуса, строения, квартиры
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP 3.6.1 (исполнение 8)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

3. 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

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

Для юридических лиц

**Заявление на изготовление
квалифицированного сертификата ключа проверки электронной подписи
при плановой/неплановой смене**

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

действующего на основании

в связи с

(причина изготовления сертификата)

1. Просит изготовить ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра:

(общее имя)

в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	ФИО должностного лица, наименование информационной системы или организации (в зависимости от типа владельца сертификата)
Организация (Organization)	Полное или сокращенное наименование организации
Подразделение (OrganizationUnit)	Подразделение/отдел организации (если имеется)
Должность (Title)	В случае выпуска сертификата на должностное лицо – его должность
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ
Город (Locality)	Наименование населенного пункта
Улица (Street)	Улица, номер дома, корпуса, строения, помещения
ОГРН (OGRN)	ОГРН организации
ИНН (INN)	ИНН организации
СНИЛС (SNILS)	Не обязательно, но в случае выпуска сертификата на должностное лицо – данное поле рекомендуется включать для упрощения идентификации должностных лиц
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

3. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

Для физических лиц

**Заявление на изготовление
квалифицированного сертификата ключа проверки электронной подписи
при плановой/неплановой смене**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

в связи с

(причина изготовления сертификата)

1. Прошу сформировать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

3. 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

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

Для физических лиц

**Заявление на изготовление КСКП
электронной подписи на Универсальной электронной карте (УЭК)
при плановой/неплановой смене**

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

в связи с

(причина изготовления сертификата)

1. Прошу изготовить и записать на Универсальную электронную карту (УЭК) ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Улица (Street)	Улица, номер дома, корпуса, строения, квартиры
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP 3.6.1 (исполнение 8)
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)

2. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

3. 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	
---------------	--

4. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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.

Для юридических лиц

Доверенность

Г. _____

«_____» _____ 20__ г.

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

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 Регламентом УЦ для регистрации Пользователя УЦ.

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

(общее имя пользователя УЦ)

3. Получить в УЦ иные документы, определенные Регламентом 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 руководителя организации)

_____/_____
(подпись) (Ф.И.О.)

«_____» _____ 20__ г.

М.П.

Приложение №11
к Регламенту Удостоверяющего центра
(Форма доверенности на получение ключей
в Удостоверяющем центре)

Для физических лиц

Доверенность*

г. _____

«_____» _____ 20__ г.

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

уполномочиваю

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

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

2. Получить в Удостоверяющем центре Государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ) изготовленные для меня ключи электронной подписи и сертификат ключа проверки электронной подписи и иные документы, определенные Регламентом 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)

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

* Настоящая Доверенность должна быть заверена нотариусом

Для юридических лиц

Заявление на аннулирование (отзыв)
сертификата ключа проверки электронной подписи

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

действующего на основании

в связи с

(причина отзыва сертификата)

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи (СКПЭП) Пользователя Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области»:

(общее имя пользователя УЦ)

содержащий следующие данные:

Общее имя (CommonName)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

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

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

Для физических лиц

Заявление на аннулирование (отзыв)
сертификата ключа проверки электронной подписи

Я,

(фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

В СВЯЗИ С

(причина отзыва сертификата)

прошу аннулировать (отозвать) сертификат ключа проверки электронной подписи (СКПЭП),
содержащий следующие данные:

Общее имя (CommonName)	
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»

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

Для юридических лиц

Заявление на приостановление действия
сертификата ключа проверки электронной подписи

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

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»:

(общее имя пользователя УЦ)

содержащего следующие данные:

Общее имя (CommonName)	
Серийный номер сертификата ключа проверки электронной подписи (SerialNumber)	

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

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, содержащий сведения о сертификате, действие которого было приостановлено.

Уполномоченное лицо ЦР
УЦ ГКУ ТО «ЦИТТО»

_____/_____
«_____» _____ 20____ г.

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, содержащего следующие данные:

Общее имя (CommonName)	
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 юридических лиц

Заявление на возобновление действия
сертификата ключа проверки электронной подписи

(полное наименование организации, включая организационно-правовую форму)

в лице

(должность, фамилия, имя, отчество)

действующего на основании

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

(общее имя пользователя УЦ)

содержащего следующие данные:

Общее имя (CommonName)	
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.

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, содержащего следующие данные:

Общее имя (CommonName)	
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.

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

Для физических лиц

Заявление на присоединение и изготовление первого КСКП
электронной подписи на Универсальной электронной карте (УЭК)

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 Регламенту Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ), условия которого определены ГКУ ТО «ЦИТТО» и опубликованы на сайте Удостоверяющего центра по адресу <http://ca.72to.ru>. С Регламентом Удостоверяющего центра и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

2. Прошу зарегистрировать меня в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и сформировать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Улица (Street)	Улица, номер дома, корпуса, строения, квартиры
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP версии 3.6.1 (исполнение 8)
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)

3. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

4. 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

5. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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 Пользователь зарегистрирован в реестре Удостоверяющего центра ГКУ ТО «Центр информационных технологий Тюменской области».

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

Уполномоченное лицо _____ / _____ /
УЦ ГКУ ТО «ЦИТТО» (подпись) (Ф.И.О.)
М.П.

Для физических лиц

Заявление на присоединение и изготовление первого
квалифицированного сертификата ключа проверки электронной подписи

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 Регламенту Удостоверяющего центра государственного казенного учреждения Тюменской области «Центр информационных технологий Тюменской области» (далее – УЦ), условия которого определены ГКУ ТО «ЦИТТО» и опубликованы на сайте Удостоверяющего центра по адресу <http://ca.72to.ru>. С Регламентом Удостоверяющего центра и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

2. Прошу зарегистрировать меня в Реестре Удостоверяющего центра, наделить полномочиями Пользователя УЦ и сформировать ключи электронной подписи и квалифицированный сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

Общее имя (CommonName)	Фамилия Имя Отчество
СНИЛС (SNILS)	Страховой номер индивидуального лицевого счета
ИНН (INN)	Индивидуальный номер налогоплательщика (не обязательно, но рекомендуется к включению для целей взаимодействия с ФНС)
Электронная почта (Email)	Адрес электронной почты (если имеется)
Страна (Country)	RU
Область (State)	Наименование субъекта РФ, по адресу регистрации
Город (Locality)	Наименование населенного пункта, по адресу регистрации
Средство электронной подписи (SubjectSignTool)	КриптоПро CSP (версия 3.6)
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)

3. Даю согласие на обработку своих персональных данных Удостоверяющим центром ГКУ ТО «ЦИТТО» и признаю, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

4. 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	
---------------	--

5. С Руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (Приложение 22 Регламента) ознакомлен.

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 Пользователь зарегистрирован в реестре Удостоверяющего центра ГКУ ТО «Центр информационных технологий Тюменской области».

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

Уполномоченное лицо _____ / _____ /
УЦ ГКУ ТО «ЦИТТО» (подпись) (Ф.И.О.)
М.П.

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

[illegible]