УТВЕРЖДАЮ

Директор
ТФОМС Мурманской области

_____ В.А.Акульчев

_____ 2012 г.

РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ ЗАЩИЩЁННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET ТЕРРИТОРИАЛЬНОГО ФОНДА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ МУРМАНСКОЙ ОБЛАСТИ

1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ViPNet [Администратор]	-	программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet.
ViPNet [Клиент]	-	программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы.
ViPNet [Координатор]	-	программное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet.
VPN (Virtual Private Network)	-	обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
Абонент Защищённой сети	-	назначенный приказом руководителя, сотрудник Участника системы здравоохранения, использующий для выполнения своих служебных обязанностей сервисы и информационные системы Защищённой сети.
Абонентский пункт	-	персональный компьютер с установленным программным обеспечением ViPNet [Клиент].
Автопроцессинг	-	автоматическая обработка файлов и писем в программе «Деловая почта», в соответствии с различными правилами задаваемыми пользователем.
Владелец информационных систем	-	участник, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством.
Владелец сертификата ключа проверки электронной подписи	-	физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).
Главный администратор Защищённой сети	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области осуществляющий общую политику администрирования всей Защищённой сети.
Информационная система	-	совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Ключ проверки электронной подписи	-	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).
Ключ электронной подписи	-	уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.
Ключевой носитель	-	носитель, содержащий один или несколько ключей.
Компрометация ключа	-	утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.
Координатор Защищённой сети	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области, определяющий общую стратегию развития Защищённой сети.
Корпоративная информационная система МТФОМС	-	информационная система, участниками электронного взаимодействия в которой являются Участники системы здравоохранения.
Локальный администратор Защищённой сети	-	назначенный приказом сотрудник Участника системы здравоохранения, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному участнику.
Несанкционированный доступ	-	доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах путём изменения (повышения, фальсификации) своих прав доступа.
Пользователь Удостоверяющего центра	-	физическое лицо (уполномоченный представитель Участника присоединившегося к Регламенту Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области), зарегистрированное в Удостоверяющем центре.

Сертификат ключа проверки электронной подписи	-	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.
Список отозванных сертификатов	-	документ на бумажном носителе или электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.
Средство электронной подписи	-	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. В Защищённой сети, данные функции реализованы в модуле «Деловая почта».
Технология ViPNet	-	технология, предназначенная для построения виртуальных защищённых сетей, путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе средства криптографической защиты информации «Домен-К».
Удостоверяющий центр	-	Территориальный фонд обязательного медицинского страхования Мурманской области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством.
Уполномоченное лицо Удостоверяющего центра	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области, наделённый полномочиями по заверению сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.

Усиленная неквалифицированная электронная подпись (далее – неквалифицированная ЭП)	-	ЭП, полученная в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания.
Участник системы здравоохранения	-	обладатель информации, формирующейся в области здравоохранения, осуществляющий деятельность, направленную на реализацию прав граждан на охрану здоровья и медицинскую помощь.
Центр управления сетью	-	аппаратные или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети.
Электронная подпись (ЭП)	-	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.
Электронный документ	-	документ, в котором информация представлена в электронно-цифровой форме, и который может быть представлен в виде файла, хранящегося на носителе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Регламент Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Регламент УЦ) разработан в соответствии с:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской федерации»;
- Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Регламент устанавливает общий порядок и условия предоставления Удостоверяющим центром корпоративного уровня Защищённой сети VipNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Удостоверяющий центр) Участникам Защищённой сети возможности участвовать в обмене юридически значимыми электронными документами с применением электронной подписи.

2.3. Признание юридической значимости электронных документов в рамках Защищённой сети и присоединение к Регламенту УЦ, производится путём заключения

Участниками Защищённой сети Соглашения о защищённом обмене юридически значимыми электронными документами (далее – Соглашение) (Приложение №1).

2.4. Участник имеет право в одностороннем порядке расторгнуть Соглашение, письменно уведомив об этом Территориальный фонд обязательного медицинского страхования Мурманской области (далее ТФОМС Мурманской области) за 30 календарных дней, до дня расторжения.

2.5. Уведомление о расторжении Соглашения, полученное ТФОМС Мурманской области от Участника, является основанием для обязательного аннулирования сертификатов ключей проверки электронных подписей Пользователей Удостоверяющего центра (далее – Пользователей УЦ), уполномоченных данным Участником. Датой аннулирования, указанных сертификатов ключей проверки электронных подписей Пользователя УК будет дата расторжения Соглашения.

3. НАЗНАЧЕНИЕ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

3.1. Удостоверяющий центр предназначен для обеспечения:

-аутентификации Участников Защищённой сети в процессе взаимодействия;

-возможности использования электронной цифровой подписи;

-контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия Участников Защищённой сети;

-конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия Участников Защищённой сети;

3.2. В процессе своей деятельности Удостоверяющий центр:

-вносит в реестр Удостоверяющего центра регистрационную информацию о Пользователях УЦ;

-формирует и обновляет справочно-ключевую информацию для организации защищённого обмена информацией в рамках Защищённой сети;

- создает сертификаты ключей проверки электронных подписей;

- устанавливает сроки действия сертификатов ключей проверки электронных подписей;

- аннулирует выданные Удостоверяющим центром сертификаты ключей проверки электронных подписей;

- ведет реестр выданных и аннулированных Удостоверяющим центром сертификатов ключей проверки электронных подписей;

- создает ключи электронных подписей и ключи проверки электронных подписей;

- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

- осуществляет по обращениям Пользователей УЦ проверку электронных подписей;

- осуществляет иную связанную с использованием электронной подписи деятельность.

3.3. Все электронные подписи созданные в Удостоверяющем центре являются усиленными неквалифицированными электронными подписями.

3.4. Выполнение своих функций Удостоверяющий центр осуществляет на безвозмездной основе.

4. НАЗНАЧЕНИЕ ОТВЕТСТВЕННЫХ ЛИЦ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА КОРПОРАТИВНОГО УРОВНЯ

4.1. Назначение Уполномоченного лица.

4.1.1. Исполнение функций Уполномоченного лица возлагается на сотрудника ТФОМС Мурманской области.

4.1.2. Уполномоченное лицо назначается и отстраняется от исполнения возложенных функций, приказом директора ТФОМС Мурманской области.

4.1.3. Функции и полномочия Уполномоченного лица определены в разделе 10 Положения о Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области.

5. ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, ИЗГОТОВЛЕНИЯ И УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННЫХ ПОДПИСЕЙ

5.1. Пользователями УЦ называются лица зарегистрированные в Удостоверяющем центре и осуществляющие обмен электронными документами в рамках заключённого Соглашения.

5.2. Проходить процедуру регистрации в Удостоверяющем центре, либо быть зарегистрированным Пользователем УЦ, может только физическое лицо, представляющее юридическое лицо.

5.3. Порядок регистрации, изготовления и управления сертификатами ключей проверки электронной подписи Пользователей УЦ, являющихся сотрудниками ТФОМС Мурманской области.

5.3.1. Регистрация и изготовление сертификата ключа проверки электронной подписи Пользователя, являющегося сотрудником ТФОМС Мурманской области и участвующего в обмене юридически значимыми электронными документами с применением электронной подписи, осуществляется на основании заявки руководителя подразделения (Приложение №2).

5.3.2. После предоставления заявки на изготовление сертификата ключа проверки электронной подписи Уполномоченное лицо в течение 1 (одного) рабочего дня осуществляет её рассмотрение и обработку.

5.3.3. В случае отказа в регистрации и изготовлении сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет об этом руководителя подразделения, сотрудником которого является регистрирующееся лицо, с указанием причины отказа.

5.3.4. В случае принятия положительного решения Уполномоченное лицо осуществляет регистрацию, генерацию ключевой информации, изготовление сертификата ключа проверки электронной подписи и распечатывает сертификат ключа проверки электронной подписи в двух экземплярах.

5.3.5. Два экземпляра сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе визируются Уполномоченным лицом и заверяются печатью.

5.3.6. После изготовления сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет об этом руководителя подразделения, сотрудником которого является регистрирующееся лицо, после чего Пользователь УЦ должен лично получить сформированные ключевые документы у Уполномоченного лица.

5.3.7. Изготовленные ключи записываются на отчуждаемый машинный носитель, предоставляемый Пользователем УЦ.

5.3.8. Ключевой носитель должен удовлетворять следующим требованиям:

-быть отформатированным;

-не содержать никакой информации;

5.3.9. Ключевые носители, не удовлетворяющие требованиям п. 5.3.8, для записи ключевой информации не принимаются.

5.3.10. Факт выдачи ключей заносится в Журнал учёта изготовления и выдачи ключей под роспись владельца.

5.3.11. После получения всей необходимой ключевой информации и сертификата ключа проверки электронной подписи Главный администратор вводит полученные данные на Абонентском пункте Защищённой сети, на котором зарегистрирован Пользователь УЦ.

5.4. Аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователей УЦ, являющихся сотрудникам ТФОМС Мурманской области, осуществляется на основании заявки руководителя подразделения (Приложение №3).

5.4.1. Срок рассмотрения заявки на отзыв сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.5. Приостановление действия сертификата ключа проверки электронной подписи Пользователей УЦ, являющихся сотрудникам ТФОМС Мурманской области, осуществляется на основании заявки руководителя подразделения (Приложение №4).

5.5.1. Срок рассмотрения заявки на приостановление действия сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.6. Возобновление действия сертификата ключа проверки электронной подписи Пользователей УЦ, являющихся сотрудникам ТФОМС Мурманской области, осуществляется на основании заявки руководителя подразделения (Приложение №5)

5.6.1. Срок рассмотрения заявки на возобновление сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.7. Порядок регистрации, изготовления и управления сертификатами ключей проверки электронной подписи Пользователей УЦ, являющихся сотрудниками других Участников.

5.7.1. Регистрация Пользователей УЦ, являющихся сотрудниками других Участников, состоит из 3-х последовательных этапов:

- подключение Участника к Защищённой сети;
- присоединение к Регламенту УЦ;
- регистрация и изготовление сертификата ключа проверки электронной подписи Пользователя УЦ;

5.7.2. Подключение к Защищённой сети, осуществляется согласно разделу 3 Регламента Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области.

5.7.3. Присоединение к Регламенту УЦ производится путём заключения Участником Защищённой сети Соглашения о защищённом обмене юридически значимыми электронными документами.

5.7.4. Регистрация и изготовление сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется после предоставления в адрес ТФОМС Мурманской области:

-необходимых документов согласно п. 5.7.2 настоящего Регламента УЦ;

-подписанного директором ТФОМС Мурманской области и руководителем Участника Соглашения о присоединении к Регламенту УЦ;

-заявления на регистрацию Пользователя УЦ (Приложение №6);

-заявление на изготовление сертификата ключа проверки электронной подписи Пользователя УЦ (Приложение №7).

5.7.5. После предоставления заявлений на регистрацию и изготовление сертификата ключа проверки электронной подписи Уполномоченное лицо в течение 1 (одного) рабочего дня, осуществляет её рассмотрение и обработку.

5.7.6. В случае отказа в регистрации и изготовлении сертификата ключа проверки электронной подписи Уполномоченное лицо письменно уведомляет об этом руководителя Участника.

5.7.7. В случае принятия положительного решения Уполномоченное лицо осуществляет регистрацию Пользователя УЦ, генерацию ключевой информации, изготовление сертификата ключа проверки электронной подписи и распечатывает сертификат ключа проверки электронной подписи в двух экземплярах.

5.7.8. Два экземпляра сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе визируются Уполномоченным лицом и заверяются печатью.

5.7.9. После изготовления сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет об этом Пользователя УЦ, после чего Пользователь УЦ должен лично или через Локального администратора Участника, получить сформированные ключевые документы у Уполномоченного лица.

5.7.10. Локальный администратор Участника должен иметь доверенность на право подписи и получения сертификата ключа проверки электронной подписи за Пользователя УЦ, и получения сформированной ключевой информации (Приложение №8).

5.7.11. Изготовленные ключи записываются на отчуждаемый машинный носитель, предоставляемый Пользователем УЦ.

5.7.12. Ключевой носитель должен удовлетворять следующим требованиям:

-быть отформатированным;

-не содержать никакой информации;

5.7.13. Ключевые носители, не удовлетворяющие требованиям п. 5.7.12, для записи ключевой информации не принимаются.

5.7.14. Факт выдачи ключей заносится в Журнал учёта выдачи ключевых документов под роспись владельца или Локального администратора.

5.7.15. После получения всей необходимой ключевой информации и сертификата ключа проверки электронной подписи Локальный администратор вводит полученные данные на Абонентском пункте Защищённой сети, на котором зарегистрирован Пользователь УЦ.

5.8. Аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется по заявлению на отзыв сертификата ключа проверки электронной подписи руководителем Участника (Приложение №9).

5.8.1. Заявление на отзыв сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

5.8.2. Срок рассмотрения заявления на отзыв сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.8.3. Заявление на отзыв сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя УЦ.

5.8.4. Заявление включает в себя следующие обязательные реквизиты:

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

5.9. Приостановление действия сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется по заявлению на приостановление действия сертификата ключа проверки электронной подписи руководителем Участника (Приложение №10).

5.9.1. Заявление на приостановление действия сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

5.9.2. Срок рассмотрения заявления на приостановление сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.9.3. Заявление на приостановление сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе,

заверенный собственноручной подписью Пользователя УЦ. Заявление включает в себя следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого приостанавливается;
- причину приостановления действия сертификата;
- срок, на который приостанавливается действие сертификата;
- дату и подпись заявителя.

5.10. Возобновление действия сертификата ключа проверки электронной подписи Пользователя УЦ, осуществляется по заявлению на возобновление действия сертификата ключа проверки электронной подписи руководителем Участника (Приложение №11).

5.10.1. Заявление на возобновление действия сертификата ключа проверки электронной подписи в бумажной форме подаётся Пользователем УЦ лично.

5.10.2. Срок рассмотрения заявления на возобновление сертификата ключа проверки электронной подписи составляет 1 (один) рабочий день.

5.10.3. Заявление на возобновление сертификата ключа проверки электронной подписи в бумажной форме представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя УЦ. Заявление включает в себя следующие обязательные реквизиты:

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

5.11. Хранение сертификата ключа проверки электронной подписи Пользователей УЦ в реестре выданных и аннулированных сертификатов ключей проверки электронной подписи Удостоверяющего центра, осуществляется в течение установленного срока действия сертификата ключа проверки электронной подписи.

5.12. Срок архивного хранения сертификата ключа проверки электронной подписи устанавливается в соответствии со сроком, определённым разделом 10 Регламента УЦ.

5.13. Порядок ведения реестра сертификатов, осуществляется в соответствии с Руководством администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр].

6. ОРГАНИЗАЦИЯ ЗАЩИЩЁННОГО ОБМЕНА ЮРИДИЧЕСКИ ЗНАЧИМЫМИ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ МЕЖДУ СТОРОНАМИ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕДУР МЕЖСЕТЕВОГО ОБМЕНА СЕТЕЙ VIPNET

6.1. Организация межсетевого взаимодействия осуществляется согласно раздела 5 Регламента Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области.

6.2. В случае организации защищённого обмена юридически значимыми электронными документами с использованием процедур межсетевого обмена сетей ViPNet, между ТФОМС Мурманской области и доверенной сетью ViPNet заключается Соглашения о защищённом обмене юридически значимыми электронными документами.

6.3. Для проверки сертификатов ключей проверки электронной подписи доверенных сетей ViPNet, приславших подписанную информацию, используются сертификаты Администраторов доверенных сетей ViPNet

6.4. Обмен сертификатами Администраторов сетей ViPNet осуществляется согласно Руководству администратора ViPNet Administrator [Удостоверяющий и Ключевой Центр].

7. ПРОЦЕДУРА РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ, СВЯЗАННЫХ С ОСУЩЕСТВЕЛЕНИЕМ ОБМЕНА ЮРИДИЧЕСКИ ЗНАЧИМЫМИ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

7.1. Возникновение конфликтных ситуаций может быть связано сформированием, доставкой, получением, подтверждением получения электронных документов, а также использованием в данных документах электронной подписи. Данные ситуации могут возникать в случаях:

-не подтверждения подлинности защищённых электронных документов средствами проверки электронной подписи получателя;

-оспаривание факта идентификации владельца электронной подписи, подписавшего электронный документ;

-заявление отправителя или получателя электронного документа об его искажении;

-оспаривание факта отправления и/или получения защищённого электронного документа;

-оспаривание времени отправления и/или получения защищённого электронного документа;

-иные случаи возникновения конфликтных ситуаций.

7.2. В случае возникновения конфликтной ситуации Пользователь УЦ, предполагающий возникновение конфликтной ситуации, должен отправить Уполномоченному лицу:

-уведомление о конфликтной ситуации с изложением обстоятельств её возникновения;

-электронный документ, подлинность которого оспаривается. Электронный документ вместе с электронной подписью и сертификатом ключей проверки электронной подписи экспортируются из модуля «Деловая почта» программного обеспечения VipNet [Клиент].

7.3. Уполномоченное лицо проверяет обстоятельства, свидетельствующие о возникновении конфликтной ситуации, и направляет уведомителю информацию о результатах проверки, и в случае необходимости, о мерах принятых для разрешения возникшее конфликтной ситуации.

8. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ УПОЛНОМОЧЕННОГО ЛИЦА УЦ

8.1. Срок действия ключа электронной подписи и ключа проверки электронной подписи Уполномоченного лица составляет 2 года.

8.2. Начало периода действия ключа электронной подписи Уполномоченного лица исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки электронной подписи.

8.3. Максимальный срок, который может быть установлен в качестве срока действия сертификата ключа проверки электронной подписи Уполномоченного лица, составляет 5 лет.

9. СРОКИ ДЕЙСТВИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ И СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ ВЛАДЕЛЬЦЕВ СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1. Срок действия ключа электронной подписи Пользователя УЦ, соответствующего сертификату ключа проверки электронной подписи, владельцем которого он является, составляет 12 месяцев.

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

9.3. Срок действия ключа электронной подписи устанавливается равным сроку действия сертификата ключа проверки электронной подписи.

9.4. Максимальный срок, который может быть установлен в качестве срока действия сертификатов ключей проверки электронной подписи Пользователей УЦ, составляет 1 год.

9.5. Срок действия сертификата ключа проверки электронной подписи устанавливается УЦ в момент его изготовления.

10. АРХИВНОЕ ХРАНЕНИЕ ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИИ

10.1. Архивированию подлежит следующая информация:

-реестр выданных и аннулированных сертификатов ключей проверки электронных подписей Пользователей УЦ;

-сертификаты ключей проверки электронных подписей Уполномоченного лица УЦ;

-журналы аудита программно-аппаратных средств обеспечения деятельности УЦ;

-реестр зарегистрированных Пользователей УЦ;

-заявления на изготовление ключей Пользователей УЦ;

-заявление на аннулирование (отзыв) сертификатов ключей проверки электронных подписей Пользователей УЦ;

-заявление на приостановление действия сертификатов ключей проверки электронных подписей Пользователей УЦ;

-заявление на возобновление действия сертификатов ключей проверки электронных подписей Пользователей УЦ;

-служебные документы УЦ.

10.2. Информация, внесенная в реестр выданных и аннулированных сертификатов ключей проверки электронных подписей, подлежит хранению в течение всего срока деятельности Удостоверяющего центра.

10.3. Выделение архивных документов к уничтожению и уничтожение осуществляется в соответствии с инструкцией по общему делопроизводству.

11. УПРАВЛЕНИЕ КЛЮЧАМИ

11.1. Плановая смена ключей Уполномоченного лица.

11.1.1. Плановая смена ключей Уполномоченного лица выполняется в соответствии со сроком действия сертификата ключа проверки электронной подписи Уполномоченного лица Удостоверяющего Центра.

11.1.2. Процедура плановой смены ключей Уполномоченного лица осуществляется в следующем порядке:

-Уполномоченное лицо формирует новый ключ электронной подписи;

-Уполномоченное лицо изготавливает сертификат нового ключа проверки электронной подписи и подписывает его электронной подписью с использованием нового ключа электронной подписи.

11.2. Внеплановая смена ключей Уполномоченного лица.

11.2.1. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа электронной подписи Уполномоченного лица.

11.2.2. При компрометации ключей шифрования Уполномоченного лица прекращается работа по их использованию.

11.2.3. Процедура внеплановой смены ключей электронной подписи Уполномоченного лица выполняется после получения уведомления о компрометации ключа электронной подписи. В течение одного рабочего дня:

- аннулируется сертификат ключа проверки электронной подписи Уполномоченного лица ключа электронной подписи;

- ключи Уполномоченного лица объявляются скомпрометированными;

-производится рассылка сформированных обновлений ключей на узлы Защищённой сети.

11.2.4. После выполнения процедуры внеплановой смены ключей Уполномоченного лица, сертификат ключа проверки электронной подписи Уполномоченного лица аннулируется (отзывается) путём занесения в список отозванных сертификатов.

11.3. Плановая смена ключей Пользователей.

11.3.1. Плановая смена ключей электронной подписи Пользователя УЦ выполняется в соответствии со сроком действия сертификата ключа проверки электронной подписи Пользователя УЦ.

110.3.2. Процедура плановой смены ключей Пользователей УЦ осуществляется в следующем порядке:

-Уполномоченное лицо формирует новый ключ электронной подписи;

-Уполномоченное лицо изготавливает сертификат нового ключа проверки электронной подписи и подписывает его электронной подписью.

11.4. Внеплановая смена ключей Пользователей УЦ

11.4.1. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации ключа Пользователя УЦ.

11.4.2. В случае компрометации только ключей электронной подписи Пользователь УЦ обязан немедленно сообщить об этом своему Локальному администратору и не использовать эти ключи для подписи документов. При компрометации ключей шифрования Пользователь УЦ обязан прекратить работу на своём Абонентском пункте.

11.4.3. Ключи пользователя могут считаться скомпрометированными в следующих случаях:

-посторонним лицам мог стать доступным файл ключевого дистрибутива;

-посторонним лицам мог стать доступным съёмный носитель с ключевой информацией;

-посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере;

11.4.4. Процедура внеплановой смены ключей Пользователей УЦ выполняется Уполномоченным лицом.

11.4.5. Уполномоченное лицо после получения уведомления о компрометации ключа электронной подписи в течение одного рабочего дня:

-аннулирует сертификат ключа проверки электронной подписи;

-объявляет ключи данного Пользователя УЦ скомпрометированными;

Производит рассылку сформированных обновлений ключей на Абонентские пункты сети.

11.4.6. После выполнения процедуры внеплановой смены ключей Пользователя УЦ, сертификат ключа проверки электронной подписи Пользователя УЦ аннулируется (отзывается) путём занесения в список отозванных сертификатов.

12. СТРУКТУРЫ СЕРТИФИКАТОВ И СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ

12.1. Удостоверяющий центр издаёт сертификаты ключей проверки электронной подписи Пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее – Сертификаты открытых ключей) формата X.509 версии 3.

12.2. Удостоверяющий центр издаёт списки отозванных сертификатов ключей проверки электронной подписи Пользователей УЦ и Уполномоченного лица УЦ в электронной форме (далее – Сертификаты открытых ключей) формата X.509.

Приложение №1
к Регламенту Удостоверяющего центра
корпоративного уровня Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

Соглашение
об организации защищённого обмена юридически значимыми электронными документами

г.Мурманск **«_____»_____20___г.**

Территориальный фонд обязательного медицинского страхования Мурманской области, в лице директора Акульчева Вячеслава Александровича, действующего на основании _____, именуемый в дальнейшем ТФОМС Мурманской области, и _____
_____, именуемый в дальнейшем Организация, в лице _____, действующего на основании _____, вместе именуемые «Стороны» на основании «Федерального закона «Об электронной цифровой подписи» от 10.01.2002 №1-ФЗ, в целях организации защищённого обмена юридически значимыми электронными документами в рамках Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области, заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В силу настоящего Соглашения Организация присоединяется к Регламенту удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Регламент УЦ).

1.2.Организация, присоединившаяся к Регламенту УЦ, осуществляет обмен документами в электронном виде с использованием программных продуктов, объединённых под торговой маркой ViPNet, обеспечивающих создание защищённой виртуальной сети с возможностью использования электронной подписи на базе общедоступной сети Интернет.

2. ПРАВА И ОЯЗАННОСТИ СТОРОН

2.1. Стороны признают, что любые электронные документы, в Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее Защищённая сеть), заверенные электронной подписью должностных лиц, имеющие сертификаты ключей проверки электронной подписи, полученные в соответствии с Регламентом УЦ, юридически эквивалентны

полученным документам на бумажных носителях, заверенных соответствующими подписями и оттиском печатей сторон.

2.2. Стороны признают, что используемые при электронном обмене средства защиты, обеспечивающие защиту от несанкционированного доступа через каналы связи, шифрование и электронную подпись, достаточны для обеспечения конфиденциальности информационного взаимодействия сторон, а также подтверждения того, что:

- электронный документ исходит от Участника Защищенной сети, его передавшего (подтверждение авторства документа);

- электронный документ не претерпел изменений при информационном взаимодействии Участников Защищенной сети (подтверждение целостности и подлинности документа);

- электронный документ доставлен получателю в срок, указанный в формируемом и подписанным получателем извещении о доставке документа;

- электронный документ юридически эквивалентен документу на бумажном носителе.

2.3. Стороны обязуются:

2.3.1. Принимать на себя в полном объёме все обязательства, связанные с электронным документом, удостоверенным корректной электронной подписью.

2.3.2. При проведении защищённого обмена юридически значимыми электронными документами руководствоваться законодательством Российской Федерации, Регламентом УЦ, Положением о виртуальной Защищённой сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области, Регламентом виртуальной Защищённой сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области, настоящим Соглашением и документацией на программные средства ViPNet.

2.3.3. Обеспечивать целостность прикладного и системного программного обеспечения на рабочем месте Стороны и отсутствие в программной среде злонамеренного программного кода.

2.3.4. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам средства электронной цифровой подписи, программное обеспечение и соответствующую техническую документацию.

2.3.5. Содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные и технические меры для предотвращения несанкционированного доступа к данным компьютерам, установленному на них программному обеспечению и средствам защиты информации, а также в помещения, в которых они установлены, не допускать появления на взаимодействующих компьютерах компьютерных вирусов.

2.3.6. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна о наступлении и прекращении обстоятельств препятствующих исполнению обязательств, немедленно извещать другую сторону.

2.4. Сторона имеет право:

2.4.1. Отказывать Участнику Защищенной сети в приёме/передаче электронных документов с указанием причины отказа.

2.4.2. Приостанавливать обмен электронными документами при:

-несоблюдении Участником Защищенной сети требований к приёму/передаче электронных документов и обеспечению информационной безопасности, предусмотренных законодательством Российской Федерации и условиями настоящего Соглашения;

-разрешении спорных ситуаций, а также для выполнения неотложных, аварийных и ремонтно-восстановительных работ на АРМ Стороны с уведомлением других Участников Защищенной сети о сроках проведения этих работ.

2.4.3. Требовать от других Участников Защищенной сети приостановления обработки всех электронных документов в случаях компрометации ключей электронной подписи.

2.4.4. В случае невозможности защищённого обмена юридически значимыми электронными документами Сторона принимает/передаёт документы на бумажных носителях или в виде файлов на машинных носителях по согласованию с соответствующими Участниками Защищенной сети.

3. ТЕХНИЧЕСКИЕ УСЛОВИЯ

3.1. Стороны за свой счёт приобретают, устанавливают и обеспечивают работоспособность средств защиты информации и электронной подписи, обеспечивающих подключение и функционирование в Защищённой сети.

3.2. Стороны оплачивают средства связи и каналы связи, необходимые для работы в Защищённой сети.

3.3. Выдача сертификатов ключей проверки электронной подписи осуществляется ТФОМС Мурманской области.

4. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

4.1. Обмен электронными документами осуществляется по открытым каналам связи с использованием средств криптографической защиты информации и электронной подписи.

4.2. Обмен документами, их подпись и подтверждение целостности и подлинности осуществляется в соответствии с руководствами пользователей на технические средства и средства защиты, обеспечивающие такой обмен.

4.3. Отправленные и полученные электронные документы сохраняются и могут быть перенесены на любые носители.

4.4. Все подписанные электронные документы должны хранится в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров – до их разрешения.

4.5. Обязанности по организации архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.

4.6. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения.

4.7. Электронные документы, подписанные некорректными электронными подписями, в обработку не принимаются.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

5.2. Каждая из Сторон несёт ответственность за содержание всех принятых/переданных электронных документов, подписанных владельцем Сертификата ключа проверки электронной подписи Стороны.

5.3. Стороны не несут ответственность за возможные временные задержки исполнения и/или искажения электронного документа, возникающие по вине третьих лиц, предоставляющих услуги связи для работы Защищённой сети.

5.4. Сторона не несёт ответственность за убытки других Участников Защищенной сети, возникшие вследствие несвоевременного сообщения соответствующего Участника Защищенной сети о компрометации ключей электронной подписи.

5.5. Сторона не несёт ответственность за ущерб, возникший вследствие несвоевременного контроля другим Участниками Защищенной сети электронных сообщений, подтверждающих получение и обработку электронного документа, неисполнения другой стороной электронного документа, а также за несоблюдение мер обеспечения защиты от несанкционированного доступа к АРМ Участника Защищенной сети.

5.6. Сторона не несёт ответственность за ущерб, возникший вследствие разглашения пользователем другого Участника Защищенной сети собственного ключа электронной подписи, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.

5.7. Сторона не несёт ответственность за неработоспособность оборудования и программных средств других Участников Защищенной сети, повлекшую за собой невозможность доступа к Защищённой сети и возникшие в результате задержки в осуществлении передачи информации, а также за возможное уничтожение (в полном или частичном объёме) информации, содержащейся на вычислительных средствах других Участников Защищенной сети.

5.8. Сторона полностью несёт ответственность за риски, связанные с подключением ее вычислительных средств к сети Интернет. Стороны самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет.

6. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

6.1. При возникновении конфликтных ситуаций, возникающих в ходе защищённого обмена юридически значимыми электронными документами, Стороны разрешают их путём переговоров.

6.2. При недостижении согласия, споры разрешаются в соответствии с действующим законодательством.

7. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

7.1. По взаимному согласию Сторон в текст Соглашения могут вноситься изменения и дополнения.

7.2. Все изменения и дополнения к настоящему Соглашению имеют юридическую силу и являются действительными, если они составлены в письменном виде и подписаны Сторонами.

7.3. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

8. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение заключено на неопределённый срок.

8.2. Настоящее Соглашение вступает в силу и становится обязательным для Сторон с момента его заключения.

8.3. Изменения и дополнения к настоящему Соглашению оформляются в письменной форме и действительны с момента подписания Сторонами.

8.4. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чём необходимо письменно уведомить другую Сторону не позднее, чем за 30 календарных дней до дня его расторжения.

9. ЮРИДИЧЕСКИЕ АДРЕСА И ПОДПИСИ СТОРОН:

Организация:	**ТФОМС Мурманской области:**
Наименование: **Адрес:** **Тел./факс:**	**Наименование:** **Адрес:** **Тел./факс:**
_____	**Директор ТФОМС Мурманской области**
_____/_____/	_____/ _____/

Приложение №2
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на изготовление сертификатов ключей проверки электронных подписей сотрудников

_____
(Наименование подразделения)

Прошу сформировать ключи и изготовить сертификаты ключей проверки электронных подписей следующих сотрудников:

№ п/п	Фамилия Имя Отчество	Должность	Дополнительная идентификационная информация, заносимая в сертификат	Подпись сотрудника
1	**2**	**3**	**4**	**5**

Руководитель подразделения _____ /Фамилия И.О./

Приложение №3
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на отзыв сертификатов ключей проверки электронных подписей сотрудников

_____
(Наименование подразделения)

Прошу отозвать сертификаты ключей проверки электронных подписей следующих сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Причина отзыва сертификата	Подпись владельца сертификата
1	**2**	**3**	**4**	**5**	**6**

Руководитель подразделения _____ /Фамилия И.О./

Приложение №4
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на приостановление сертификатов ключей проверки электронных подписей сотрудников

_____
(Наименование подразделения)

Прошу приостановить действие сертификатов ключей проверки электронных подписей следующих сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Срок приостановления действия (в днях)	Подпись владельца сертификата
1	**2**	**3**	**4**	**5**	**6**

Руководитель подразделения _____ /Фамилия И.О./

Приложение №5
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВКА
на возобновление действия сертификатов ключей проверки электронных подписей сотрудников

_____
(Наименование подразделения)

Прошу возобновить действие сертификатов ключей проверки электронных подписей следующих сотрудников:

№ п/п	Серийный номер сертификата	Фамилия Имя Отчество	Должность	Подпись владельца сертификата
1	**2**	**3**	**4**	**5**

Руководитель подразделения _____ /Фамилия И.О./

Приложение №6
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВЛЕНИЕ
на регистрацию Пользователя Удостоверяющего центра

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____

Просит зарегистрировать уполномоченного представителя
_____
(Фамилия, имя, отчество)
в Реестре Удостоверяющего центра и наделить полномочиями Пользователя Удостоверяющего центра, установленными Соглашением от «____»_____20___г. №____ «Об организации защищённого обмена юридически значимыми электронными документами».

Настоящим _____
(Фамилия, имя, отчество)
соглашается с обработкой своих персональных данных Удостоверяющим центром и признаёт, что персональные данные, заносимые в сертификаты ключей проверки электронных подписей, владельцами которых он является, относятся к общедоступным персональным данным.

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №7
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВЛЕНИЕ
на изготовление сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____

Просит сформировать ключи электронной подписи, записать сформированный ключ электронной подписи на предоставленный ключевой носитель и изготовить сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____
(Фамилия, имя, отчество)
в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

CommonName (CN)	Фамилия, Имя, Отчество	
E-Mail (E)	Адрес электронной почты	
Organization (O)	Наименование организации	
Organization Unit (OU)	Наименование подразделения	
Locality (L)	Город	
State (S)	Субъект Федерации	
Contry (C)	RU	
Extended Key Usage	Проверка подлинности клиента Защищённая электронная почта	(1.3.6.1.5.5.7.3.2) (1.3.6.1.5.5.7.3.4)

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №8
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ДОВЕРЕННОСТЬ
на предоставление заявительных документов и получение подписей и сертификата Пользователя Удостоверяющего центра

г._____ «____»_____20___г.

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____
уполномочивает_____
(Фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

1. Предоставить в Удостоверяющий центр необходимые документы, определённые Соглашением от «____»_____20___г. №____ «Об организации защищённого обмена юридически значимыми электронными документами» - Пользователя Удостоверяющего центра _____
(Ф.И.О. Пользователя Удостоверяющего центра)

2. Получить сформированный ключевой носитель, содержащий ключ электронной подписи и сертификат ключа проверки электронной подписи Пользователя Удостоверяющего центра _____
(Ф.И.О. Пользователя Удостоверяющего центра)

3. Представитель наделяется правом расписываться в сертификате ключа проверки электронной подписи на бумажном носителе и в соответствующих документах Удостоверяющего центра для исполнения поручений, определённых настоящей доверенностью.

Настоящая доверенность действительна по «____»_____20___г.

Подпись _____ _____ подтверждаю.
(Фамилия И.О. уполномоченного лица) (подпись)

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №9
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВЛЕНИЕ
на аннулирование (отзыв) сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____
(Фамилия, имя, отчество)

Содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата
CommonName (CN)	Фамилия, Имя, Отчество
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №10
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВЛЕНИЕ
на приостановление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____

Просит приостановить действие сертификата ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____
(Фамилия, имя, отчество)

Содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата
CommonName (CN)	Фамилия, Имя, Отчество
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Срок приостановления действия сертификата _____ дней.

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.

Приложение №11
к Регламенту Удостоверяющего центра корпоративного уровня
Защищённой виртуальной сети ViPNet
Территориального фонда обязательного медицинского
страхования Мурманской области

ЗАЯВЛЕНИЕ
на возобновление действия сертификата ключа проверки электронной подписи
Пользователя Удостоверяющего центра

_____
(Наименование Участника)
в лице _____
(Должность руководителя)
_____
(Фамилия, имя, отчество руководителя)
действующего на основании_____

Просит возобновить действие сертификата ключа проверки электронной подписи своего уполномоченного представителя – Пользователя Удостоверяющего центра

_____
(Фамилия, имя, отчество)

Содержащего следующие идентификационные данные:

SerialNumber (SN)	Серийный номер сертификата
CommonName (CN)	Фамилия, Имя, Отчество
E-Mail (E)	Адрес электронной почты
Organization (O)	Наименование организации
Organization Unit (OU)	Наименование подразделения
Locality (L)	Город
State (S)	Область
Contry (C)	Страна

Пользователь Удостоверяющего центра _____/Фамилия И.О./

«___»_____20___г.

Должность и Ф.И.О. руководителя Участника
Подпись руководителя Участника, дата подписания заявления
М.П.