Приложение №1
УТВЕРЖДЕНО
приказом ТФОМС
Саратовской области
от 01.07.13 № 173

Регламент Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области

Оглавление

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ViPNet CUSTOM - линейка продуктов компании «ИнфоТеКС», включающая программные и программно-аппаратные комплексы (средства защиты информации ограниченного доступа, в том числе персональных данных), предназначенных для:

- создания защищенной, доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи (Интернет, телефонные и беспроводные линии связи) путем организации виртуальной частной сети (VPN) с одним или несколькими центрами управления;
- развертывания инфраструктуры открытых ключей (PKI) с организацией Удостоверяющего Центра с целью использования механизмов электронной подписи.

ViPNet Administrator (Администратор) - базовый программный комплекс для настройки и управления защищенной сетью, включающий в себя:

- ViPNet NCC (Центр Управления Сетью, ЦУС) — программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищенной сетью ViPNet;
- ViPNet KC & CA (Удостоверяющий и Ключевой Центр, УКЦ) — программное обеспечение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей - Ключевого Центра, а также функции Удостоверяющего Центра.

ViPNet Coordinator (Координатор) - программный сервер защищенной сети ViPNet, выполняющий следующие функции:

- сервера IP-адресов;
- прокси-сервера защищенных соединений;
- туннелирующего сервера (криптошлюза);
- межсетевого экрана для открытых, защищенных ресурсов и туннелируемых ресурсов;
- сервера защищенной почты;
- отказоустойчивого сервера защищенной сети ViPNet в конфигурации ViPNet Cluster.

ViPNet Client (Клиент) - выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях и состоит из следующих компонентов:

- низкоуровневый драйвер сетевой защиты ViPNet-драйвер;
- программа ViPNet Монитор;
- транспортный модуль ViPNet MFTP;
- программа ViPNet Контроль приложений;
- программа ViPNet Деловая почта.

ViPNet-драйвер - драйвер сетевой защиты выполняет функции фильтрации и шифрования/дешифрования входящих и исходящих IP-пакетов.

ViPNet Монитор - выполняет функции сетевого экрана, защищенного обмена сообщениями, файлового обмена, шифрации IP-трафика.

ViPNet MFTP - транспортный модуль обеспечивает обмен управляющими конвертами, конвертами программы «Деловая почта» и файлами с другими сетевыми узлами ViPNet.

ViPNet Деловая почта – «Деловая почта» предназначена для обмена электронной почтой между пользователями сети ViPNet. С помощью программы «Деловая почта» можно отправлять и получать сообщения и вложения, подписывать сообщения и вложения электронной подписью. В программе предусмотрена система автоматической обработки входящих сообщений и файлов в соответствии с заданными правилами (автопроцессинг).

Абонентский пункт (АП) - сетевой узел ViPNet, который является начальной или конечной точкой передачи данных.

Адресные справочники АП – справочники АП, определяющие возможности абонентского пункта по адресации корреспонденции (область видимости АП) в сети ViPNet.

Администратор сети ViPNet - лицо, назначенное руководителем организации, эксплуатирующей АРМ [Администратор], и предоставляющей услуги корпоративного удостоверяющего центра. Администратор безопасности обеспечивает эксплуатацию АРМ [Администратор] и является уполномоченным лицом, подписывающим своей электронной цифровой подписью сертификаты ключей подписей пользователей, зарегистрированных на

данном АРМ [Администратор].

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности). Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагает субъект.

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Доступ к информации - возможность получения информации и ее использования.

Дистрибутив ключей - файл с расширением .dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Запрос на сертификат ключа проверки электронной подписи - электронное сообщение определенного формата и синтаксиса, содержащее необходимую информацию для создания сертификата.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Корпоративная информационная система - информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Ключ электронной подписи (далее - ключ ЭП) - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (далее - ключ проверки ЭП) - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка ЭП).

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Ключевой документ - физический носитель определенной структуры, содержащий ключевую информацию (ключи электронной подписи).

Компрометация ключа электронной подписи - утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа

информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Область применения сертификатов - перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых Удостоверяющим Центром.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Обновление справочно-ключевой информации - при различных изменениях в сети ViPNet (добавление, удаление сетевого узла ViPNet, добавление пользователя, издание нового сертификата и т.д.), производимых администратором в ЦУС, УКЦ, может изменяться справочно-ключевая информация для сетевых узлов ViPNet. В этом случае администратор сети ViPNet централизованно высылает на сетевые узлы (СУ) сформированные обновления из ЦУС.

Организация межсетевого взаимодействия - между двумя различными сетями ViPNet может быть организовано межсетевое взаимодействие. В этих целях в программе ЦУС предусмотрены специальные меры по формированию экспортных данных для ЦУС других сетей и импорта данных от других ЦУС. Обмен информацией между пользователями двух различных сетей производится через один из серверов маршрутизаторов (СМ) каждой сети, называемых шлюзовыми.

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Плановая смена ключей электронной подписи - смена ключей электронной подписи, производимая в период действия ключей электронной подписи в соответствии с установленной в Удостоверяющем центре периодичностью, не вызванная компрометацией ключей электронной подписи.

Пользователь Удостоверяющего центра (пользователь) - лица, зарегистрированные в Удостоверяющем Центре и признающие настоящий Регламент.

Рабочий день Удостоверяющего Центра (далее - рабочий день) - промежуток времени с 9 часов до 18 часов каждого дня недели за исключением субботы, воскресенья и праздничных нерабочих дней.

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Регистрационная информация пользователя - информация, предоставляемая пользователем в целях создания сертификата ключа проверки электронной подписи.

Реестр Удостоверяющего центра - набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- регламент Удостоверяющего центра;
- реестр Соглашений о присоединении к Регламенту Удостоверяющего центра;
- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;
- реестр заявлений на изготовление сертификата ключа подписи;
- реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;
- реестр заявлений на приостановление/возобновление действия сертификата ключа подписи;
- реестр заявлений на подтверждение подлинности ЭП в электронном документе;
- реестр заявлений на подтверждение ЭП уполномоченного лица Удостоверяющего центра в изданных сертификатах;
- реестр сертификатов ключей подписи;
- реестр изготовленных списков отозванных сертификатов.

Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным

лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Список аннулированных (отозванных) сертификатов - списков уникальных номеров сертификатов ключей проверки ЭП, действие которых на определенный момент было прекращено Удостоверяющим центром до истечения их действия.

Средства электронной подписи (далее - средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

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

Сетевой узел ViPNet - узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet - логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet. Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Уровни адресации - каждому абонентскому пункту, с которым связан данный абонентский пункт, в адресной книге «Деловой почты» соответствует три уровня адресации:

- Абонентский пункт. Данный уровень адресации соответствует всем пользователям абонентского пункта. То есть зашифрованное письмо, адресованное абонентскому пункту, могут прочитать все его пользователи.

- Коллектив. Данный уровень адресации соответствует одному из коллективов пользователей, зарегистрированных на абонентском пункте (в сетях ViPNet CUSTOM на одном абонентском пункте может быть несколько коллективов). Зашифрованное письмо, адресованное коллективу, могут прочитать только члены этого коллектива.

- Пользователь. Данный уровень соответствует конкретному пользователю абонентского пункта. Письмо, адресованное пользователю, могут прочесть все члены коллектива этого пользователя. Таким образом, этот уровень адресации не может использоваться для разграничения доступа к зашифрованным письмам, а служит только для определения адресата.

Уполномоченное лицо Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов ключей подписей и списков отозванных сертификатов.

Уполномоченный представитель юридического лица - физическое лицо, которое действует от имени заявителя – юридического лица на основании учредительных документов, приказа о представителе юридического лица или доверенности и которое указывается в сертификате ключа проверки электронной подписи юридического лица в качестве владельца наряду с наименованием юридического лица.

Удостоверяющий центр корпоративного уровня ТФОМС Саратовской области (далее - УЦ) – Удостоверяющий Центр корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011г. № 63-ФЗ «Об электронной подписи».

Участники защищенного обмена электронными документами (ЗОЭД) – организации, осуществляющие обмен информацией в электронной форме в сфере ОМС.

Усиленная неквалифицированная электронная подпись (неквалифицированная электронная подпись) - является электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента

его подписания;

• создается с использованием средств электронной подписи.

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

Электронная подпись (далее - 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.

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

1.ОБЩИЕ ПОЛОЖЕНИЯ

Территориальный фонд обязательного медицинского страхования Саратовской области (далее - Фонд) является организатором и администратором (далее – Оператор) защищенной сети ViPNet №602 (далее – Защищенная сеть) и выполняет функции Удостоверяющего центра корпоративного уровня.

Регламент Удостоверяющего Центра корпоративного уровня Фонда (далее – Регламент), 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 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»:
- Гражданским кодексом Российской Федерации;
- Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Общими принципами построения и функционирования информационных систем и порядок информационного взаимодействия в сфере обязательного медицинского страхования, утв. приказом Федерального фонда обязательного медицинского страхования от 7 апреля 2011 г. № 79;
- Приказом Министерства здравоохранения и социального развития РФ от 25 января 2011 г. №29н «Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования»;
- Приказом Министерства здравоохранения и социального развития РФ от 28 февраля 2011 г. № 158н «Об утверждении Правил обязательного медицинского страхования»;
- Приказом ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ РФ 21 февраля 2008 г. № 149/6/6-622);
- Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утв. ФСБ РФ 21 февраля 2008 г. № 149/54-144);
- Приказом ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФАПСИ от 13 июня 2001 г. №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Целью настоящего Регламента является создание условий для организации защищенного обмена электронными документами и взаимодействия информационных систем, правовых условий использования электронной подписи в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе в соответствии с Федеральным законом РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Настоящий Регламент устанавливает общий порядок и условия предоставления УЦ участникам Защищённой сети возможность участвовать в обмене юридически значимыми электронными документами с применением электронной подписи.

Регламент предназначен для определения сертификационной политики при организации

защищенного обмена электронными документами и взаимодействия информационных систем всеми Участниками Защищенной сети.

Сертификационная политика УЦ определяет создание, управление и использование усиленных неквалифицированных сертификатов формата X.509 для обеспечения идентификации владельца сертификата и целостности электронной информации.

Организация защищенного обмена электронными документами и взаимодействия информационных систем, признание юридической значимости электронных документов в рамках Защищённой сети между Фондом и юридическим лицом производится путем заключения Соглашения о присоединении к Регламенту (далее - Соглашение) (Приложение №3 к Регламенту) в порядке, предусмотренном положениями статьи 428 Гражданского Кодекса РФ.

С момента заключения Соглашения о присоединении к Регламенту, юридическое лицо, считается присоединившемся к Регламенту и является Стороной Регламента (далее – Сторона).

Факт присоединения Стороны к Регламенту подтверждается полным принятием ею условий настоящего Регламента и всех его приложений в редакции, действующей на момент присоединения, и Сторона принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

Сторона имеет право в одностороннем порядке расторгнуть Соглашение, письменно уведомив об этом УЦ за один месяц до дня расторжения. Уведомление о расторжении Соглашения, полученное УЦ от Стороны, является основанием для обязательного аннулирования сертификатов ключей проверки электронных подписей Пользователей УЦ, уполномоченных данной Стороной. Датой аннулирования указанных сертификатов ключей подписей Пользователей УЦ будет дата расторжения Соглашения.

Расторжение Соглашения не освобождает Стороны от исполнения обязательств, возникших до указанного прекращения, и не освобождает от ответственности за его неисполнение (ненадлежащее исполнение).

1.1. Порядок утверждения и внесения изменений в Регламент

Настоящий Регламент утверждается приказом директора Фонда.

Все изменения и дополнения к настоящему Регламенту составляются в письменной форме и являются его составной и неотъемлемой частью.

Публикация изменений и дополнений осуществляется в порядке, утвержденным Регламентом.

Все изменения и дополнения, вносимые в Регламент и не связанные с изменением законодательства РФ вступают в силу и становятся обязательными для Сторон по истечении 10 (Десять) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте www.sartfoms.ru ТФОМС Саратовской области в разделе «Удостоверяющий Центр корпоративного уровня»,.

Все изменения и дополнения, вносимые в Регламент в связи с изменением законодательной и нормативной базы, вступают в силу одновременно с вступлением в силу изменений и дополнений в указанных актах.

1.2. Идентификация Регламента

Наименование документа: «Регламент Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области».

Версия: 2.0.

Дата: 01.07.2013г.

Объектный идентификатор УЦ: **1.2.643.3.164**

1.3. Публикация Регламента

Настоящий Регламент публикуется в электронном виде на корпоративном сайте www.sartfoms.ru ТФОМС Саратовской области в разделе «Удостоверяющий Центр корпоративного уровня».

Регламент публикуется в виде файла формата PDF.

Любое заинтересованное лицо может ознакомиться с Регламентом на сайте www.sartfoms.ru.

2.УЦ, ПОЛЬЗОВАТЕЛИ УЦ

2.1. Сведения об УЦ

Полное наименование юридического лица УЦ: Территориальный фонд обязательного медицинского страхования Саратовской области (ТФОМС Саратовской области).

Юридический адрес: 410012, г. Саратов, пр. Кирова, 10,12

Фактическое местонахождение: 410012, Саратов, пр. Кирова, 10,12

Для почты: 410000, г. Саратов, Главпочтамт, а/я 1534

Адрес электронной почты: ucku@sartfoms.ru

Контактный телефон УЦКУ: (8452) 23-87-98

Факс: (8452) 23-88-02 (125)

Банковские реквизиты:

Территориальный фонд обязательного медицинского страхования Саратовской области (ТФОМС Саратовской области)

410012,г.Саратов, проспект Кирова, дом 10,12

ИНН 6455005067

ОГРН 1026403672591

КПП 645501001

р/с 40404810300000020008 в ГРКЦ ГУ Банка России по Саратовской области, БИК 046311001.

Руководитель: директор – Саухин Андрей Николаевич

УЦ имеет разрешение (лицензии) по всем видам деятельности, связанным с осуществлением функций УЦ:

- Лицензия ФСБ на право осуществлять деятельность по техническому обслуживанию шифровальных (криптографических) средств ЛЗ № 0009030 №1161Х от 24 декабря 2009г.;
- Лицензия ФСБ на право осуществлять деятельность по распространению шифровальных (криптографических) средств ЛЗ №0009013 №1163Р от 24 декабря 2009г.;
- Лицензия ФСБ на право осуществлять предоставление услуг в области шифрования информации ЛЗ №0009011 №1162У от 24 декабря 2009.

Система безопасности и защиты информации УЦ создана и поддерживается на договорной основе с юридическими лицами, осуществляющими свою деятельность на основании лицензий, полученных в соответствии с действующим законодательством РФ.

Документы, регламентирующие обеспечение мер по защите информации УЦ введены в действие соответствующими приказами.

Для обеспечения деятельности УЦ использует средства УЦ, включая средства ЭП, сертифицированные в соответствии с действующим законодательством РФ (ПО ViPNet Custom, разработчик ОАО «Инфотекс» г.Москва, http://infotecs.ru/products/cert/).

Директор Фонда своим приказом:

- Возлагает исполнение обязанностей Уполномоченного лица УЦ на сотрудника управления информационных технологий;
- Наделяет Уполномоченное лицо УЦ правом подписывать своей электронной подписью сертификаты ключей подписей пользователей УЦ и заверять собственноручной подписью копии сертификатов ключей проверки электронной подписи на бумажном носителе;
- Возлагает функции обеспечения информационной безопасности и технической эксплуатации УЦ на отдел системного администрирования и защиты информации управления информационных технологий.

2.2. Назначение УЦ

УЦ предназначен для обеспечения участников Защищенной сети средствами и спецификациями для использования сертификатов ключей проверки электронной подписи в целях обеспечения:

- аутентификации участников информационных систем в процессе взаимодействия;
- применения электронной подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

В процессе своей деятельности УЦ:

- создает сертификаты ключей проверки электронных подписей;
- устанавливает сроки действия сертификатов ключей проверки электронных подписей;
- аннулирует выданные УЦ сертификаты ключей проверки электронных подписей;
- создает ключи электронных подписей и ключи проверки электронных подписей;
- ведет реестр выданных и аннулированных этим удостоверяющим центром сертификатов ключей проверки электронных подписей;
- проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

Выполнение своих функций УЦ осуществляет на безвозмездной основе.

2.3. Функции, выполняемые УЦ

2.3.1 Административные функции:

- управление деятельностью УЦ;
- взаимодействие с пользователями в части разрешения вопросов, связанных с применением средств ЭП, ключей ЭП и сертификатов;
- взаимодействие с пользователями в части разрешения вопросов подтверждения подлинности ЭП в ЭД в отношении созданных УЦ сертификатов;
- взаимодействие с пользователями в части разрешения вопросов, связанных с подтверждением ЭП УЦ в сертификатах, созданных УЦ в электронной форме.

2.3.2 Функции регистрации:

- заключение Соглашения о присоединении к Регламенту УЦ;
- ведение реестра пользователей;
- создание сертификатов ключей проверки электронных подписей и выдачи таких сертификатов лицам, обратившимся за их получением (заявителям);
- установление сроков действия сертификатов ключей проверки электронных подписей;
- выдача по обращению заявителя средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи;
- ведение реестра выданных и аннулированных сертификатов ключей проверки электронных подписей (далее - реестр сертификатов), в том числе включающий в себя информацию, содержащуюся в выданных сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;
- создание по обращениям заявителей ключей электронных подписей и ключей проверки электронных подписей;
- проверка на уникальность ключей проверки электронных подписей в реестре сертификатов;
- осуществление по обращениям участников электронного взаимодействия проверки

электронных подписей;
- предоставление копий сертификатов в электронной форме, находящихся в реестре сертификатов, по запросам пользователей;
- осуществляет иную связанную с использованием электронной подписи деятельность.

2.3.3 Функции безопасности:

- организация и выполнение мероприятий по защите информационных ресурсов УЦ от несанкционированного доступа, уничтожения, модификации, блокирования, иных неправомерных действий; обеспечение выполнения процедур создания, использования, хранения и уничтожения ключевой информации в соответствии с требованиями эксплуатационной документации на средства УЦ;
- недопущение копирования ключевой информации (криптографических ключей, в том числе ключей ЭП) на носители, не являющиеся ключевыми носителями;
- обеспечение взаимодействия с внешними УЦ, участниками различных корпоративных информационных систем на основе установления доверительных отношений между УЦ путем организации межсетевого взаимодействия;
- аннулирование (отзыв) сертификатов ключей проверки электронных подписей;
- приостановление и возобновление действия сертификатов;
- предоставление в любое время любому лицу доступа к актуальному списку аннулированных (отозванных) сертификатов;
- техническое обеспечение процедуры подтверждения подлинности ЭП в ЭД в отношении созданных УЦ сертификатах, по обращениям пользователей; техническое обеспечение процедуры подтверждения подлинности ЭП УЦ в созданных УЦ сертификатах, по обращениям пользователей;
- техническое обслуживание средств ЭП.

2.4. Пользователи УЦ

Пользователями УЦ называются юридические лица, зарегистрированные в УЦ.

Интересы юридического лица может представлять физическое лицо, действующее на основании учредительных документов, либо приказа о наделении соответствующими полномочиями, либо доверенности.

ТФОМС Саратовской области является зарегистрированным пользователем УЦ.

3.ПРАВА и ОБЯЗАННОСТИ, ОТВЕТСТВЕННОСТЬ

3.1. Права УЦ

УЦ имеет право:

- Отказать в регистрации к УЦ лицам, подавшим заявку на подключение, с указанием причин отказа.
- Отказать в создании сертификата зарегистрированным пользователям, подавшим заявление на его создание, с указанием причин отказа.
- Отказать в аннулировании (отзыве) сертификата в случае, если истек установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате.
- Отказать в приостановлении или возобновлении действия сертификата в случае, если истек установленный срок действия ключа ЭП, соответствующего ключу проверки ЭП в сертификате.
- Аннулировать (отозвать) сертификат в случае установленного факта компрометации соответствующего ключа ЭП, с уведомлением владельца аннулированного (отозванного) сертификата и указанием обоснованных причин.
- Приостановить действие сертификата с обязательным уведомлением владельца

сертификата, действие которого приостановлено, и указанием обоснованных причин.

3.2. Обязанности УЦ

УЦ обязан:

- Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.
- Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.
- Обеспечивать конфиденциальность созданных удостоверяющим центром ключей электронных подписей.

3.3. Права Пользователей

Пользователи имеют право:

- Обращаться в УЦ для регистрации в качестве пользователя.
- Обращаться в УЦ с целью получения средств ЭП.
- Получить доступ к актуальному списку аннулированных (отозванных) сертификатов.
- Получить копии сертификатов, находящихся в реестре УЦ, как в форме электронных документов, так и в форме документов на бумажном носителе.
- Обращаться в УЦ за подтверждением подлинности ЭП пользователя в ЭД в соответствии с порядком, определенным настоящим Регламентом.
- Обращаться в УЦ за подтверждением подлинности ЭП в созданных УЦ сертификатах в соответствии с порядком, определенным настоящим Регламентом.
- Обращаться в УЦ с заявлениями на:
  - создание сертификата;
  - аннулирование (отзыв) сертификата (в течение срока действия соответствующего ключа ЭП);
  - приостановление действия сертификата (в течение срока действия соответствующего ключа ЭП);
  - возобновление действия сертификата (в течение срока действия соответствующего ключа ЭП).

3.4. Обязанности Пользователя

3.4.1. Обязанности лиц, проходящих процедуру регистрации

- Лица, проходящие процедуру регистрации в УЦ, обязаны представить регистрационную информацию в требуемом для создания сертификата объеме.
- Лица, проходящие процедуру регистрации в УЦ, несут ответственность за достоверность предоставленной регистрационной информации.

3.4.2. Обязанности владельца сертификата

- Использовать для создания и проверки усиленных неквалифицированных электронных подписей, создания ключей усиленных неквалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с Федеральными законами, совместимых со средствами УЦ.
- Обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их

согласия.

- Применять ключ ЭП только в соответствии с областями применения, определенными в полях сертификата: KeyUsage, ExtendedKeyUsage и CertificatePolicies.
- Уведомлять УЦ, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.
- Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.
- Не использовать ключ ЭП и связанный с ним сертификат, заявление на аннулирование (отзыв) которого подано в УЦ.

3.5. Ответственность

- Ответственность Сторон регулируется законодательством РФ.
- УЦ не несет ответственности в случае нарушения Пользователем положений настоящего Регламента.
- Пользователь несет ответственность за достаточность применяемых им мер по обеспечению безопасности использования электронной подписи и средств ЭП, включая защиту ключа ЭП от компрометации, потери, уничтожения, изменения или иного неавторизованного использования.
- Пользователь обязан известить УЦ обо всех изменениях своей регистрационной информации в течение 3-х рабочих дней с момента регистрации изменений. УЦ вправе затребовать у пользователя необходимые документы, подтверждающие изменения регистрационной информации.

4.ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ УЦ, ИЗГОТОВЛЕНИЯ И УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПРОВЕРКИ ЭП

4.1. Регистрация Пользователей УЦ

Руководитель организации направляет на имя директора Фонда письмо на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем (Приложение №1) с указанием необходимого числа абонентских пунктов и Заявки на подключение к системе (Приложение №2);

На основании письма с положительной резолюцией директора и заявки, Фонд подготавливает и передает в организацию Соглашение о присоединении к Регламенту (Приложение №3) в системе защищенного обмена электронными документами и взаимодействия информационных систем - 2 экземпляра;

С момента заключения Соглашения о присоединении к Регламенту, юридическое лицо, считается присоединившимся к Регламенту и является Стороной Регламента – зарегистрированным Пользователем УЦ.

4.1.1. Регистрация АП, Коллектива и Пользователей АП

Пользователь УЦ направляет Заявление на регистрацию Пользователя АП в коллективе на абонентском пункте (Приложение №5).

4.1.2. Адресные справочники АП

Пользователь УЦ направляет Заявление на формирование Адресного справочника Пользователя АП (Приложение №6), определяющие возможности абонентского пункта по адресации корреспонденции (область видимости АП);

Администратор сети ViPNet регистрирует абонентские пункты, коллективы и Пользователя АП, задает необходимые связи с абонентскими пунктами, с которыми требуется установить взаимодействие.

4.2. Изготовление сертификата ключа проверки ЭП

Изготовление сертификата ключа проверки электронной подписи Пользователя АП для участия в обмене юридически значимыми электронными документами с применением электронной подписи, осуществляется на основании Заявления Пользователя УЦ (Приложение №8) и заверенной копии приказа (форма приказа - Приложение №7) о полномочиях Пользователя АП – уполномоченного представителя юридического лица, определяющих области применения сертификатов ключей проверки ЭП (перечень объектных идентификаторов (OID) – Приложение № 14).

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

В случае отказа в регистрации и изготовлении сертификата ключа проверки электронной подписи Уполномоченное лицо уведомляет Пользователя УЦ, с указанием причины отказа.

В случае принятия положительного решения Уполномоченное лицо в течение 3 (три) рабочих дней осуществляет регистрацию, генерацию ключевой информации, изготовление сертификата ключа проверки электронной подписи и распечатывает сертификат ключа проверки электронной подписи в двух экземплярах.

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

Два экземпляра сертификата ключа проверки электронной подписи Пользователя УЦ на бумажном носителе визируются Уполномоченным лицом и заверяются печатью, а также собственноручной подписью пользователя или его доверенного лица .

Доверенное лицо Пользователя АП должно иметь доверенность на право подписи и получения сертификата ключа проверки электронной подписи за Пользователя АП и получения сформированной ключевой информации - Дистрибутива ключей (Приложение №4).

Изготовленный Дистрибутив ключей записывается на отчуждаемый машинный носитель (ключевой носитель), предоставляемый Пользователем УЦ.

Ключевой носитель должен удовлетворять следующим требованиям:

- быть отформатированным;
- не содержать никакой информации.

Ключевые носители, не удовлетворяющие вышеуказанным требованиям, для записи ключевой информации не принимаются.

Факт выдачи ключей заносится в Журнал учёта выдачи ключевых документов под роспись владельца или Доверенного лица (Приложение №15).

4.3. Подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем

После получения всех необходимых ключевых носителей и сертификата Пользователя АП:

- Производится установка и настройка ПО ViPNet Клиент;
- Требования к конфигурации ПО ViPNet Клиент в п.8. Регламента;
- Вводится полученный Дистрибутив ключей (первичная инициализация) на абонентском пункте в действие;
- Производится тестовый обмен защищенными сообщениями и зашифрованными и подписанными ЭП файлами с Администратором сети ViPNet.

После успешного тестового обмена зашифрованной информацией и проверки ЭП Пользователь АП приступает к выполнению задач по защищенному обмену электронными документами и взаимодействию информационных систем с разрешенными абонентскими пунктами и становится Участником Защищенной сети.

4.4. Смена ключей ЭП Пользователя

4.4.1. Сроки действия ключей ЭП Пользователя

Срок действия ключа ЭП, ключа проверки ЭП и соответствующего сертификата пользователя составляет 12 месяцев.

4.4.2. Плановая смена ключей ЭП

Плановая смена ключей ЭП производится не ранее, чем за 20 (двадцать), и не позднее, чем за 5 (пять) суток до окончания срока действия текущего сертификата (ключей ЭП и ключей проверки ЭП) пользователя.

4.4.3. Внеплановая смена ключей ЭП

Внеплановая смена ключей ЭП производится по инициативе пользователя в период срока действия ключей ЭП и сертификата пользователя, в следующих случаях:

- при изменении регистрационной информации пользователя;
- при компрометации ключа ЭП пользователя;
- при компрометации ключа ЭП УЛ УЦ.

4.4.4. Аннулирование (отзыв) сертификата

Аннулирование (отзыв) сертификатов осуществляется УЦ в следующих случаях:

- по заявлению пользователя на аннулирование (отзыв) сертификата;
- по инициативе УЦ в случаях невыполнения пользователем обязательств, предусмотренных Регламентом или установления факта компрометации ключа ЭП пользователя.

Заявление на аннулирование (отзыв) сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя (Приложение №9).

При выполнении УЦ процедуры аннулирования (отзыва) сертификата, информация об аннулированном сертификате заносится в список аннулированных (отозванных) сертификатов.

Аннулирование (отзыв) сертификата по инициативе УЦ осуществляется с уведомлением Пользователя (владельца отозванного сертификата) с указанием обоснованных причин отзыва.

4.4.5. Приостановление действия сертификата

Приостановление действия сертификата осуществляется УЦ в следующих случаях:

- по заявлению Пользователя на приостановление действия сертификата;
- по заявлению Пользователя в форме телефонограммы в случае компрометации или угрозы компрометации ключа ЭП пользователя;
- по инициативе УЦ в случае невыполнения Пользователем обязательств, предусмотренным Регламентом.

Заявление на приостановление действия сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя АП (Приложение №10).

При устном заявлении на приостановление действия сертификата Пользователь должен сообщить идентификационные данные, содержащиеся в сертификате.

При выполнении УЦ процедуры приостановления действия сертификата ключа подписи, информация о сертификате, действие которого приостановлено, заносятся в список аннулированных (отозванных) сертификатов.

Приостановление действия сертификата по инициативе УЦ осуществляется с уведомлением Пользователя (владельца отозванного сертификата) с указанием обоснованных причин приостановления.

Информация о прекращении действия сертификата ключа проверки электронной подписи должна быть внесена УЦ в реестр сертификатов в течение одного рабочего дня со дня наступления обстоятельств, повлекших за собой прекращение действия сертификата ключа проверки электронной подписи. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в реестр сертификатов.

4.4.6. Возобновление действия сертификата

Возобновление действия сертификата осуществляется УЦ в следующих случаях:

- по заявлению Пользователя на возобновление действия сертификата;
- при неполучении УЦ по истечении 3 (три) рабочих дней с момента получения телефонограммы заявления Пользователя на приостановления действия сертификата, его документального подтверждения.

Заявление на возобновление действия сертификата представляет собой документ на бумажном носителе, заверенный собственноручной подписью Пользователя АП (Приложение №11).

При выполнении УЦ процедуры возобновления действия сертификата, информация о сертификате, действие которого возобновлено, удаляется из списка аннулированных (отозванных) сертификатов.

4.5. Смена ключей ЭП Уполномоченного лица УЦ

4.5.1. Сроки действия ключей ЭП УЛ УЦ

- Срок действия ключа ЭП Уполномоченного лица (УЛ) УЦ составляет 12 месяцев.
- Срок действия ключа проверки ЭП и соответствующего сертификата УЛ УЦ составляет 24 месяца.
- Начало действия ключей ЭП УЛ УЦ исчисляется с даты и времени начала действия соответствующего сертификата.

4.5.2. Плановая смена ключей ЭП УЛ УЦ

- Плановая смена ключей ЭП УЛ УЦ выполняется в соответствии со сроком действия и не позднее окончания срока действия текущего ключа ЭП УЛ УЦ.
- Процедура плановой смены ключей ЭП УЛ УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.

4.5.3. Внеплановая смена ключей ЭП УЛ УЦ

- Внеплановая смена ключей ЭП УЦ производится в случае компрометации или угрозы компрометации ключа ЭП УЛ УЦ.
- Процедура по внеплановой смене ключей ЭП УЛ УЦ выполняется в порядке, определенном эксплуатационной документацией на средства УЦ.
- При выполнении процедуры по внеплановой смене ключей ЭП УЛ УЦ сертификат ключа проверки ЭП, соответствующий скомпрометированному ключу ЭП УЦ должен быть аннулирован (отозван) и занесен в список аннулированных (отозванных) сертификатов. Также должны быть проведены работы по внеплановой смене ключей ЭП пользователей, сертификаты которых созданы с использованием скомпрометированного ключа ЭП УЛ УЦ.

4.6. Подтверждение подлинности ЭП УЛ УЦ в созданных сертификатах

- УЦ осуществляет подтверждение подлинности ЭП УЛ УЦ в созданных УЦ сертификатах по заявлению Пользователя на подтверждение подлинности ЭП УЛ УЦ в сертификате Пользователя (Приложение №12).
- Обязательным приложением к заявлению на подтверждение подлинности ЭП УЛ УЦ в сертификате пользователя является внешний носитель информации, содержащий файл сертификата, подвергающегося процедуре проверки, в формате PKCS#7 в кодировке Base64 (CER).
- Срок проведения работ по подтверждению подлинности ЭП УЛ УЦ в созданном УЦ сертификате и предоставлению заключения о произведенной проверке составляет 10 (десять) рабочих дней с момента поступления в УЦ заявления Пользователя на подтверждение подлинности ЭП УЛ УЦ в сертификате Пользователя.
- Результатом проведения работ по подтверждению подлинности ЭП УЛ УЦ в сертификате пользователя является заключение УЦ, заверенное собственноручной подписью ответственного сотрудника и печатью УЦ.

4.7. Подтверждение подлинности ЭП пользователя в ЭД

- Подтверждение подлинности ЭП в ЭД осуществляется УЦ по обращению владельца сертификата (далее - заявителя) на основании заявления на подтверждение подлинности ЭП в ЭД (Приложение №13).
- Заявление на подтверждение подлинности ЭП в ЭД должно содержать информацию о дате и времени формирования ЭП в ЭД.
- Бремя доказывания достоверности даты и времени формирования ЭП в ЭД возлагается на заявителя.
- Обязательным приложением к заявлению на подтверждение ЭП в ЭД является внешний носитель информации, содержащий ЭД с ЭП в формате PKCS#7.
- Срок проведения работ по подтверждению подлинности ЭП в ЭД составляет 10 (десять) рабочих дней с момента поступления заявления в УЦ.
- В ходе проведения работ по подтверждению подлинности ЭП в ЭД Удостоверяющим центром может быть запрошена дополнительная информация.
- Результатом проведения работ по подтверждению подлинности ЭП в ЭД является ответ в письменной форме, заверенный собственноручной подписью ответственного сотрудника и печатью УЦ.

5.РАЗРЕШЕНИЕ СПОРОВ

- При рассмотрении спорных вопросов, связанных с настоящим Регламентом, стороны должны руководствоваться действующим законодательством РФ.
- Стороны должны принять все необходимые меры для того, чтобы в случае возникновения спорных вопросов решить их, прежде всего, в претензионном порядке.
- Сторона, получившая от другой стороны претензию, обязана в течение 20 (двадцать) дней удовлетворить заявленные в претензии требования или направить другой стороне мотивированный отказ с указанием оснований отказа.
- Все споры и разногласия между сторонами, возникающие из Регламента или в связи с ним, в том числе касающиеся его заключения, действия, исполнения, изменения, прекращения или действительности, и по которым не было достигнуто соглашение, разрешаются в соответствии с действующим законодательством РФ.

6.СТРУКТУРА СЕРТИФИКАТА

УЦ создает усиленные неквалифицированные сертификаты, соответствующие

международным рекомендациям ITU-T X.509 (далее - рекомендации X.509 версии 3)

6.1. Базовые поля сертификата

Наименование поля	Описание	Содержание/ «Значение»
Version:	Версия формата X.509 сертификата	«V3»
SerialNumber:	Серийный номер сертификата	Уникальный номер сертификата
Signature:	Алгоритм подписи	«ГОСТ Р 34.10/34.11-2001»
Issuer:	Идентифицирующие данные издателя сертификата	Согласно п. 6.3 настоящего Регламента
Validity:	Даты начала и окончания действия сертификата	«Действителен с: ДД.ММ.ГГГГ ЧЧ:ММ:СС» «Действителен по: ДД.ММ.ГГГГ ЧЧ:ММ:СС»
Subject:	Идентифицирующие данные владельца сертификата	Согласно п.6.4 настоящего Регламента
SubjectPublicKeyInfo:	Ключ проверки ЭП владельца сертификата	Значение ключа проверки ЭП

6.2. Дополнения сертификата

Наименование поля	Описание	Содержание/ «Значение»
Key Usage	Использование ключа	**В сертификатах УЛ УЦКУ:** Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписывание списка отзыва (CRL) (f6) **В сертификатах пользователей:** Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование
ExtendedKeyUsage	Расширенное использование ключа	Набор объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, описывающие юридическую сферу применения
CertificatePolicies	Политики сертификата	Класс средства электронной подписи

SubjectKeyIdentifier	Идентификатор ключа субъекта	Идентификатор ключа ЭП владельца сертификата
AuthorityKey Identifier	Идентификатор ключа издателя сертификата	Номер сертификата УЦ

Перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых Удостоверяющим Центром, содержится в Приложении №14 настоящего Регламента.

6.3. Структура данных поля Issuer (идентификационных данных УЛ УЦ)

Наименование поля	Описание	Содержание/ «Значение»
Common Name, CN	Общее имя	Уполномоченное лицо УЦКУ Вахлаев В.М.
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Саратов
StateOrProvinceName,	Наименование области	Саратовская
StreetAdress, Street	Адрес	пр. Кирова, д. 10,12
OrganizationName, O	Наименование организации	ТФОМС Саратовской области
OrganizationUnit, OU	Подразделение	Управление информационных технологий
Title, T	Должность	Заместитель начальника управления
Email, E	Адрес электронной почты	vakhlaev@sartfoms.ru
OGRN	Основной государственный регистрационный номер (ОГРН)	1026403672591
INN	Идентификационный номер налогоплательщика (ИНН)	6455005067

6.4. Структура данных поля Subject (идентификационных данных владельцев сертификатов юридических лиц)

Наименование поля	Описание	Содержание/ «Значение»
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
StateOrProvinceName, S	Наименование области	Субъект РФ места нахождения юридического лица
StreetAddress, Street	Адрес	Часть адреса места нахождения юридического лица, включающая наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationName, O	Наименование организации	Наименование юридического лица
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
Title, T	Должность	Наименование должности уполномоченного представителя юридического лица (владельца сертификата)
OGRN	Основной государственный регистрационный номер (ОГРН)	ОГРН юридического лица
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

7.СТРУКТУРА СПИСКА АННУЛИРОВАННЫХ (ОТОЗВАННЫХ) СЕРТИФИКАТОВ

Издаваемые УЦ списки аннулированных (отозванных) сертификатов должны соответствовать рекомендациям X.509. Все поля и дополнения, включаемые в список аннулированных (отозванных) сертификатов должны быть заполнены в соответствии с рекомендациями X.509 версии 2.

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	Атрибуты имени Удостоверяющего центра
Effective date	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
Next update	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
Revoked Certificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (Serial Number) 2. Время аннулирования или время обработки заявления на прекращение действия сертификата (Revokation Date) 3. Код причины отзыва сертификата (CRL Reason Code): "0" Не указана " 1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия
Signature algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи Удостоверяющего центра, которым подписан СОС
CA Version	Версия сертификата издателя	Версия сертификата Удостоверяющего центра
CRL Number	Номер СОС	Порядковый номер СОС
CRL Next Publish	Следующая публикация СОС	дд.мм.гггг чч:мм:сс GMT

8.ТРЕБОВАНИЯ К КОНФИГУРАЦИИ ПО VIPNET [КЛИЕНТ]

На рабочем месте Участника Защищенной сети с полномочиями, предоставляемыми настройками ПО ViPNet [Клиент] реализуется следующая общая политика безопасности:

- информационный обмен с Участниками только шифрованным трафиком, т.е. блокировка всего открытого IP-трафика;

- правила фильтрации открытой сети, только для работы внутри корпоративной сети. Если рабочей станции требуется работать с внутренними корпоративными сетевыми ресурсами, то в настройках программы ViPNet [Клиент] [Монитор] должен быть установлен «2» или «3» режим безопасности работы (функции персонального сетевого экрана по отношении к открытой сети) и произведены дополнительные настройки фильтров IP-пакетов;

- правила доступа для пропуска трафика от адресатов защищенной сети должны разрешать работу только по разрешенным протоколам и портам;

- Пользователь не может самостоятельно отказаться от работы с ПО ViPNet;

- Пользователь не может самостоятельно изменять режим безопасности работы ПО ViPNet [Клиент];

- правами по модификации конфигурации абонентского пункта обладает Администратор безопасности.

Основной функциональный состав абонентского пункта ПО ViPNet[Клиент] представлен в Таблице 1.

Таблица 1

Наименование	Значение	Примечание
Программное обеспечение ViPNet [Клиент]		
Драйвер сетевой защиты	+	
Монитор	+	
MFTP	+	
Деловая почта	+	
Полномочия и настройки		
Полномочия	1 (Средние)	
Подпись (сертификат)	+	Рабочие ключи ЭП и сертификат изготавливаются в соответствии с порядком, определенным в Регламенте УЦКУ
Разрешенные связи	с Участниками Защищенной сети	
Режим безопасности	«2» «3»	Определяется в зависимости от варианта подключения к сети Интернет

9.ПОРЯДОК ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В ЗАЩИЩЕННОЙ СЕТИ

9.1. Передача сведений

Передача сведений обеспечивается средствами ПО ViPNet MFTP, входящими в состав ПАК защиты информации "ViPNet", в соответствии с "Руководством пользователя. ViPNet [MFTP] Транспортный модуль".

9.2. Подтверждение приема/передачи передаваемых сведений

Подтверждение приема/передачи передаваемых сведений обеспечивается средствами ПО ViPNet [Клиент] [Деловая почта], входящей в состав ПАК защиты информации "ViPNet", в соответствии с "Руководством пользователя. ViPNet [Клиент] [Деловая почта]".

9.3. Подтверждение достоверности и подлинности передаваемых сообщений

Подтверждение достоверности, подлинности и авторства передаваемых сведений обеспечивается средствами электронной подписи, предоставляемой ПО ViPNet [Клиент] [Деловая почта], входящей в состав ПАК защиты информации "ViPNet", в соответствии с "Руководством пользователя. ViPNet [Клиент] [Деловая почта]".

9.4. Хранение сведений

Отправленные и полученные сведения сохраняются и могут быть перенесены на любые носители.

Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах регистрации электронных документов.

9.5. Хранение подписанных ЭП сведений

Все подписанные ЭП сведения должны храниться с ЭП в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров - до их разрешения.

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

Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

9.6. Задание правил автопроцессинга в ПО ViPNet[Деловая почта] для обработки электронных документов, принимаемых и передаваемых в процессе защищенного обмена

Правила автопроцессинга определяют каталоги приема и передачи для соответствующего адресата защищенной сети ViPNet, используя которые участники документооборота обмениваются электронными документами:

- электронные документы, помещаются уполномоченным лицом отправителя в соответствующий получателю каталог передачи ПО ViPNet[Деловая почта];
- электронные документы, помещенные уполномоченным лицом отправителя в каталог передачи в соответствии с правилом автопроцессинга ПО ViPNet [Деловая почта] и адресованные определенному получателю, автоматически отправляются получателю, при этом шифруются и подписываются ЭП отправителя;
- для контроля доставки исходящих электронных документов и результатах проверки ЭП в адрес отправителя направляется электронная квитанция о доставке, которая формируется в ПО ViPNet [Деловая почта] получателя на каждое входящее письмо и автоматически отправляется отправителю;
- входящие электронные документы, принятые ПО ViPNet [Деловая почта] автоматически расшифровываются и согласно правилам автопроцессинга сохраняются в каталог приема, соответствующий получателю. Проверка ЭП отправителя под принятым электронным документом производится автоматически в соответствии с заданным правилом автопроцессинга для данного получателя.

10.ПОРЯДОК ОРГАНИЗАЦИИ ЗАЩИЩЕННОГО МЕЖСЕТЕВОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

10.1. Порядок организации защищенного межсетевого информационного взаимодействия между сторонами

Защищенное информационное взаимодействие в рамках защищенного сегмента единого информационного пространства системы обязательного медицинского страхования организуется на базе технологии межсетевого взаимодействия ViPNet-сетей.

Защищенное информационное взаимодействие организуется с помощью Индивидуального Симметричного Межсетевого Мастер-ключа (ИСММК).

ИСММК формирует Администратор безопасности в АРМ [Администратор] для каждой из сетей, с которой должно осуществляться взаимодействие.

Администраторы сетей ViPNet Организаций выделяют сетевые узлы своих сетей, которые будут участвовать в межведомственном взаимодействии. Выделенные узлы сетей будут связаны в ЦУСах взаимодействующих сетей, а также будут иметь ключи для шифрования и подтверждения достоверности и подлинности передаваемых данных.

Администраторы безопасности выбирают Координаторы, которые будут выполнять функции серверов-шлюзов при межведомственном взаимодействии сетей.

10.2. Порядок организации межведомственного защищенного информационного взаимодействия между ViPNet - сетями организаций

Порядок организации защищенного информационного взаимодействия между ViPNet-сетями Организаций предполагает выполнение следующих технологических и организационных мероприятий:

- В каждом Центре управления сетью (ЦУС) и Удостоверяющем Ключевом центре (УКЦ), в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]», производится формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая свои корневые сертификаты для каждой из сетей, с которой должно осуществляться взаимодействие.
- Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие ЦУСы сторонних организаций, с которыми должно осуществляться защищенное взаимодействие.
- Во всех ЦУСах и УКЦ других организаций в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]» производится ввод и обработка (импорт) полученных из других ЦУСов данных (начального экспорта), установление связей своих узлов с узлами ЦУСов, предоставившими информацию. Далее в ЦУСах и УКЦ создается ответная информация (ответный экспорт) для ЦУСов, приславших первичную информацию, включая свои корневые сертификаты.
- Ответная информация (ответный экспорт) доверенным способом передается в ЦУС Фонда, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межведомственного защищенного взаимодействия между ЦУСами, и дальнейший обмен данными между ними производится в автоматическом режиме.
- После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межведомственном взаимодействии, между данными узлами сетей Фондов и организаций можно производить защищенный электронный документооборот.
- После завершения процедуры организации защищенного информационного взаимодействия между ViPNet-сетью Фонда и сетями организаций подписывается Протокол установления межсетевого взаимодействия (Приложение №16).

10.3. Порядок модификации защищенного информационного взаимодействия между ViPNet - сетями организаций при изменении состава узлов

Порядок модификации межведомственного защищенного информационного взаимодействия между ViPNet - сетями Организаций предполагает выполнение следующих технологических и организационных мероприятий:

- В процессе функционирования защищенного информационного взаимодействия между сетями ViPNet Организаций в одной или нескольких сетях может потребоваться модификация межведомственного защищенного информационного взаимодействия, т.е. изменение состава узлов, участвующих в межведомственном защищенном взаимодействии, - добавление или удаление сетевого узла.
- При модификации защищенного информационного взаимодействия в какой-либо сети, администратор данной сети в своем ЦУСе производит соответствующие изменения в структуре связей своей сети, формирует экспортные данные и передает их в соответствующие ЦУСы в автоматическом режиме в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]».
- В ЦУСах сетей, которых касается данная модификация, в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» производится обработка (импорт) полученных данных. Далее в ЦУСах создается ответная информация (ответный экспорт) для ЦУСов, приславших первичную информацию ЦУСов.
- Ответная информация передается в ЦУСы сетей, от которых поступила первичная информация, в автоматическом режиме по защищенному каналу связи, где она обрабатывается и вводится в действие. На этом завершается процесс модификации межведомственного защищенного взаимодействия между ЦУСами Организаций.
- После рассылки каждым ЦУСом сформированных обновлений ключевой и справочной информации на свои узлы, которых касается модификация, данные узлы продолжают или прекращают производить защищенный электронный документооборот при межведомственном взаимодействии.

10.4. Журнал изменений межведомственного защищенного информационного взаимодействия

При каждой модификации межведомственного защищенного информационного взаимодействия Администраторы безопасности заносят соответствующие записи в Журнал изменений (Приложение №17).

10.5. Порядок организации защищенного информационного взаимодействия между ViPNet-сетями организаций в случае плановой смены межсетевого мастер-ключа

Порядок модификации межведомственного защищенного информационного взаимодействия между ViPNet - сетями Организаций в случае плановой смены межсетевого мастер-ключа предполагает выполнение следующих технологических и организационных мероприятий:

- Предварительные организационные мероприятия.

Перед тем, как осуществлять плановую смену межсетевого мастер-ключа, Администраторы ViPNet-сетей Организаций, для связи которых будет использоваться новый межсетевой мастер-ключ, должны договориться по следующим вопросам:

- Выбрать тип межсетевого мастер – ключа, который будет использоваться для связи между сетями.
- Если предполагается использовать симметричный мастер-ключ, то выбрать Администратора, который будет создавать новый межсетевой мастер – ключ.
- Выбрать время проведения смены межсетевого мастер-ключа и последующего

обновления ключей шифрования для узлов своих сетей.

- Формирование нового межсетевого мастер-ключа

Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]».

- Процедура создания экспорта и приема импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приема импортных данных в соответствии с «Руководством администратора. ViPNet [Центр управления сетью]» и «Руководством администратора. ViPNet [Удостоверяющий и ключевой центр]».

- Межведомственное Взаимодействие после Смены Межсетевого Мастер-Ключа.

После смены межсетевого мастер-ключа связь между сетевыми узлами взаимодействующих сетей Организаций возможна только после прохождения обновлений ключевой информации на всех соответствующих сетевых узлах данных сетей.

- Записи в журнале изменений межведомственного защищенного информационного взаимодействия:

После смены межсетевого мастер-ключа Администраторы сетей ViPNet и сторонних организаций заносят соответствующие записи в Журнал изменений (Приложение №17).

11.ПРИЛОЖЕНИЯ

1 Образец письма о подключении к системе защищенного обмена электронными документами и взаимодействия информационных систем в защищенной сети ОМС Саратовской области.
2 Заявка на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем сети ViPNet №602 по телекоммуникационным каналам связи.
3 Соглашение о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области для организации защищенного обмена электронными документами и взаимодействия информационных систем.
4 Доверенность на предоставление заявительных документов и получения ключей ЭП и сертификата ключа проверки ЭП Пользователя АП.
5 Заявление на регистрацию Пользователя АП.
6 Заявление на формирование адресного справочника АП (область видимости АП).
7 Форма приказа «О допуске к работе в защищенной сети и предоставлении права владения сертификатами ключей проверки электронной подписи».
8 Заявление на изготовление сертификата ключа проверки электронной подписи Пользователя АП при генерации ключей подписей в УЦ.
9 Заявление на аннулирование (отзыв) сертификата ключа проверки электронной подписи Пользователя АП.
10 Заявление на приостановление действия сертификата ключа проверки электронной подписи Пользователя АП.
11 Заявление на возобновление действия сертификата ключа проверки электронной подписи Пользователя АП.
12 Заявление на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки электронной подписи.
13 Заявление на подтверждение подлинности электронной подписи в электронном документе.
14 Перечень объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых УЦ.
15 Журнал учета изготовления и выдачи ключей под роспись.
16 Протокол установления межсетевого взаимодействия.
17 Журнал изменений.

Приложение №1
к Регламенту

Образец письма

Директору
Территориального фонда ОМС
Саратовской области
Саухину А.Н.
г. Саратов, ул. Кирова 10,12

О подключении к системе
защищенного обмена электронными документами
и взаимодействия информационных систем
в защищенной сети ОМС
Саратовской области

Прошу подключить (наименование организации) к системе защищенного обмена электронными документами и взаимодействия информационных систем в защищенной сети ОМС Саратовской области.
Необходимое число абонентских пунктов - ___

_____ _____ _____
Должность руководителя подпись И.О.Фамилия

Приложение №2
к Регламенту

Заявка
на подключение к системе защищенного обмена электронными документами и взаимодействия информационных систем сети ViPNet №602 по телекоммуникационным каналам связи

Директору
ТФОМС Саратовской области
Саухину Андрею Николаевичу от

1. Полное наименование организации без сокращений (на основании учредительных документов)
2. Код МО(СМО) в системе ОМС:
3. Сокращенное наименование организации
4. Юридический адрес организации с индексом
5. Фактический (почтовый) адрес организации с индексом
6. ИНН
7. ОГРН
8. КПП
9. Расчетный счет
10. БИК
11. Банк
12. ФИО руководителя
13. Должность руководителя
14. Действует на основании (указать документ: устав, положение, доверенность или другое)
15. Контактные телефоны
16. Контактный E-mail

Дата		Подпись руководителя	М.П.

Приложение №3
к Регламенту

Соглашение №_____
о присоединении к Регламенту Удостоверяющего Центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области для организации защищенного обмена электронными документами и взаимодействия информационных систем

г. Саратов «___»_____201__ г.

Территориальный фонд обязательного медицинского страхования Саратовской области, именуемый в дальнейшем «Фонд», в лице директора Саухина Андрея Николаевича, действующего на основании Положения, с одной стороны, и _____, именуемый в дальнейшем «Пользователь УЦ», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», на основании Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи», положений статьи 11 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» и положений статей 428, 160 Гражданского Кодекса РФ в целях организации и осуществления защищенного обмена электронными документами и взаимодействия информационных систем с использованием средств защиты информации, заключили настоящее соглашение (далее - Соглашение) о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В силу настоящего Соглашения Пользователь УЦ присоединяется к Регламенту Удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области (далее - Регламент).
1.2. Стороны, присоединившиеся к Регламенту, осуществляют обмен документами в электронном виде и взаимодействие информационных систем с использованием сетевых продуктов, объединенных под торговой маркой ViPNet (далее «VipNet Custom»), использующих СКЗИ «Домен-КС2», соответствующий Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 года №796, для реализации функций электронной подписи (далее – ЭП) (создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) и обеспечивающих создание защищенной виртуальной сети на базе общедоступной сети Интернет.
1.3. Соглашение регулирует отношения между Сторонами при организации и осуществлении защищенного обмена электронными документами и взаимодействия информационных систем в соответствии с Регламентом и с использованием программы «ViPNet Custom».
1.4. Соглашение определяет права и обязанности Сторон, возникающие при осуществлении взаимодействия в системе защищенного обмена электронными документами (далее - ЗОЭД) с учетом обеспечения информационной безопасности.
1.5. Соглашение определяет условия и порядок обмена электронными документами (далее - ЭД) с использованием средств электронной подписи при осуществлении ЗОЭД между Сторонами.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Фонд является Администратором защищенной сети ViPNet № 602 и осуществляет все права, вытекающие из Регламента.
2.2. Фонд обязуется исполнять Регламент, в том числе своевременно и в полном объеме

выполнять следующие обязанности:

- своевременно извещать Пользователя УЦ об изменениях и дополнениях, вносимых в Регламент или прекращении их действия;
- организовывать работу с криптографическими ключами Пользователя УЦ в объеме и в соответствии с порядком, определяемым Регламентом и Приложениями к нему;
- соблюдать режим конфиденциальности информации (паролей, идентификаторов, криптографических ключей), которая становится доступной Удостоверяющему центру в связи с выполнением им своих функций в соответствии с Регламентом;
- выполнять иные обязанности перед Пользователем УЦ, возникающие в соответствии с Регламентом.

2.3. Стороны признают, что:

2.3.1. Применяемые в системе ЗОЭД сертифицированные средства криптографической защиты информации (далее - СКЗИ) обеспечивают аутентификацию, конфиденциальность, целостность и подлинность ЭД и достаточны для осуществления Сторонами обмена ЭД с использованием общедоступных каналов связи при условии использования не скомпрометированных ключей ЭП.

2.3.2. ЭП в ЭД признается равнозначной собственноручной подписи уполномоченных представителей Сторон, наделенных правом подписи соответствующих документов, и для этой ЭП соблюдены следующие условия:

- сертификат создан и выдан УЦ Фонда, сертификат УЛ которого действителен на день выдачи указанного сертификата;
- сертификат действителен на момент подписания ЭД (при наличии достоверной информации о моменте подписания ЭД) или на день проверки действительности указанного сертификата, если момент подписания ЭД не определен;
- имеется положительный результат проверки принадлежности владельцу сертификата ЭП, с помощью которой подписан ЭД, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания. Проверка осуществляется в соответствии с положениями Регламента и с использованием сертификата лица, подписавшего ЭД;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате (Приложение №14) с учетом ограничений, содержащихся в сертификате лица, подписывающего ЭД (если такие ограничения установлены).

2.3.3. Удостоверенные корректными ЭП ЭД, подтверждают Сторонам при ЗОЭД:

- аутентификацию участников информационных систем в процессе взаимодействия;
- контроль целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- конфиденциальность информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

2.4. Стороны обязуются:

2.4.1. Принимать на себя в полном объеме все обязательства, связанные с ЭД, удостоверенные корректной ЭП.

2.4.2. При проведении обмена ЭД с использованием ЗОЭД руководствоваться законодательством Российской Федерации, Регламентом, настоящим Соглашением и документацией на программные средства системы ЗОЭД, включая средства криптографической защиты информации.

2.4.3. При компрометации ключей ЭП участников системы ЗОЭД руководствоваться положениями, установленные Регламентом.

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

2.4.5. Оперативно обрабатывать оформленные должным образом ЭД участника системы ЗОЭД в соответствии с настоящим Соглашением.

2.4.6. Осуществить подключение АРМ Стороны к системе ЗОЭД при выполнении Стороной необходимых условий, изложенных в Регламенте, а также корректировать настройки в случае изменения параметров подключения в соответствии с настоящим Соглашением.

2.4.7. Использовать АРМ Стороны исключительно в целях, предусмотренных настоящим

Соглашением.
2.4.8. Не вносить исправления, изменения или дополнения, а также не передавать третьим лицам средства ЭП, программное обеспечение и соответствующую техническую документацию.
2.4.9. Содержать в исправном состоянии компьютеры, участвующие в электронном взаимодействии, принимать организационные меры для предотвращения несанкционированного доступа к 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.
2.4.10. Сторона, для которой создалась невозможность исполнения обязательств по настоящему Соглашению, должна о наступлении и прекращении обстоятельств, препятствующих исполнению обязательств, немедленно извещать другую сторону. Обмен ЭД, передаваемыми по каналам связи с использованием программного продукта «VipNet Custom», на время действия этих обстоятельств приостанавливается.
2.5. Сторона имеет право:
2.5.1. Отказывать другой Стороне в приеме/передаче ЭД с указанием мотивированной причины отказа.
2.5.2. Приостанавливать обмен ЭД при:
- несоблюдении Стороной требований к приему/передаче ЭД 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 другой Стороны о сроках проведения этих работ.
При возникновении споров, связанных с принятием или непринятием и (или) с исполнением или неисполнением электронного документа, стороны обязаны соблюдать порядок согласования разногласий, предусмотренный Регламентом.
2.5.3. Требовать от другой стороны приостановления обработки всех ЭД в случаях компрометации закрытых ключей ЭП.
2.5.4. В случае невозможности обмена ЭД в системе ЗОЭД Сторона принимает/передает документы на бумажных носителях или в виде файлов на машинном носителе по согласованию с другой Стороной.

3. ТЕХНИЧЕСКИЕ УСЛОВИЯ

3.1. Стороны за свой счет приобретают, устанавливают и обеспечивают работоспособность средств защиты информации, необходимых для электронного взаимодействия на основе программы «ViPNet Custom».
3.2. Стороны самостоятельно оплачивают средства связи и каналы связи, необходимые для работы в системе электронного документооборота.

4. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

4.1. Защищенный обмен электронными документами Сторон осуществляется по открытым каналам связи с использованием средств криптографической защиты информации и ЭП, в соответствии с Регламентом.
В исключительных случаях, при отсутствии каналов связи или их отказах, обмен не конфиденциальной информацией по настоящему Соглашению осуществляется на машинных носителях (далее - «электронных носителях») в заархивированном виде с контрольной суммой CRC. К электронному носителю с информацией прилагается Акт приема-передачи информации и сопроводительное письмо, в котором указываются все прилагаемые документы. Обмен конфиденциальной информацией (персональными данными) осуществляется на предназначенных для этого учтенных машинных носителях информации, защищенных согласно требованиям законодательства РФ.
4.2. Обмен информацией в электронном виде между Сторонами осуществляется в соответствии

с составом и форматами файлов обмена данными, заранее согласованными Сторонами.
4.3. Обмен электронными документами, их подпись, подтверждение целостности и подлинности документа осуществляется в соответствии с руководствами пользователей на технические средства и средства защиты, обеспечивающие такой обмен.
4.4. Отправленные и полученные электронные документы сохраняются и могут быть перенесены на машинные носители.
4.5 Стороны должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных журналах регистрации электронных документов.
4.6. Осуществлять хранение подписанных электронных документов. Все электронные документы в подписанном виде должны храниться в течение сроков, предусмотренных законодательством Российской Федерации, нормативными документами сторон, а в случае возникновения споров - до их разрешения.
4.7. Обязанности по организации сохранности архивов электронных документов возлагаются на каждую из Сторон, в части их касающейся.
4.8. Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.
4.9. ЭД, подписанные некорректными ЭП, 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 несет ответственность за содержание всех ЭД принятых/переданных в системе ЗОЭД, подписанных владельцем Сертификата ключа подписи Стороны.
5.3. Стороны не несут ответственность за возможные временные задержки исполнения и/или искажения ЭД, возникающие по вине третьих лиц, предоставляющих услуги связи для использования в ЗОЭД.
5.4. Сторона не несет ответственность за убытки другой Стороны, возникшие вследствие несвоевременного другой Стороной сообщения о компрометации закрытых ключей ЭП ее представителей.
5.5. Сторона не несет ответственность за убытки, возникшие вследствие несвоевременного контроля другой Стороной электронных сообщений, подтверждающих получение и обработку ЭД, неисполнения другой Стороной ЭД, а также за несоблюдение мер обеспечения защиты от несанкционированного доступа к АРМ другой Стороны.
5.6. Сторона не несет ответственности за ущерб, возникший вследствие разглашения пользователем другой Стороной собственного ключа ЭП, его утраты или его передачи, вне зависимости от причин, неуполномоченным лицам.
5.7. Сторона не несет ответственности за последствия изменения электронного документа, защищенного корректной ЭП другой Стороны, в том числе в случае использования ключей ЭП и программно-аппаратных средств клиентской части другой Стороны неуполномоченным лицом.
5.8. Сторона не несет ответственности за неработоспособность оборудования и программных средств другой Стороны, повлекшую за собой невозможность доступа к защищенной сети «VipNet» и возникшие в результате задержки в осуществлении передачи информации, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах другой Стороны, подключенных к сети Интернет.
5.9. Сторона полностью несет всю ответственность за риски, связанные с подключением его вычислительных средств к сети Интернет. Сторона самостоятельно обеспечивает защиту собственных вычислительных средств и криптографических ключей от несанкционированного доступа и вирусных атак из сети Интернет.

6. КОНФИДЕНЦИАЛЬНОСТЬ

6.1. Стороны обязуются не разглашать сведения конфиденциального характера, полученные в процессе

осуществления обмена электронными документами и взаимодействия информационных систем.
6.2. Стороны относят информацию к сведениям конфиденциального характера в порядке, установленным законодательством Российской Федерации
6.3. Порядок защиты и доступа к сведениям конфиденциального характера регламентируется соответствующими нормативными правовыми актами Российской Федерации.

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.
8.3 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 заключается на неопределенный срок и вступает в силу со дня его подписания.
8.2. Изменения и дополнения к настоящему Соглашению оформляются в письменной форме и действительны с момента подписания Сторонами.
8.3. Настоящее Соглашение может быть расторгнуто по инициативе любой из Сторон, о чем необходимо письменно уведомить другую Сторону не позднее, чем за один месяц до дня его расторжения.

9. РЕКВИЗИТЫ СТОРОН

Фонд

Территориальный фонд обязательного медицинского страхования Саратовской области
Юридический адрес: 410012, г. Саратов, пр. Кирова, д.10,12
Почтовый адрес: 410012, г. Саратов, пр. Кирова, д.10,12
тел.: (8452) 23-88-02, 23-88-05
факс: (8452) 23-88-02 *125
e-mail: general@sartfoms.ru

Пользователь УЦ

10. ПОДПИСИ СТОРОН

Директор

_____ **А.Н. Саухин**
мп

_____ _____
мп

Приложение №4
к Регламенту

Доверенность

на предоставление заявительных документов и получения ключей ЭП
и сертификата ключа проверки ЭП Пользователя АП

г. _____ «_____» _____20___ г.

_____
(наименование организации)

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 для регистрации, генерации ключей и изготовления сертификата ключа подписи своего полномочного представителя - Пользователя АП _____
(Ф.И.О. Пользователя АП)

2. Получить сертификат ключа ЭП Пользователя АП и иные документы.

3. Получить сформированный ключевой носитель, содержащий дистрибутив ключей Пользователя АП _____.
(Ф.И.О. Пользователя АП)

4. Расписываться в копии сертификата ключа проверки ЭП на бумажном носителе и в соответствующих документах Удостоверяющего центра для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность действительна по «_____» _____ 20_____ г.

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

Пользователь АП _____ _____
подпись И.О.Фамилия

«_____» _____ 20_____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«_____» _____ 20_____ г.
дата подписания заявления

Приложение №5
к Регламенту

Заявление

на регистрацию Пользователя АП

_____
(наименование Организации)

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 АП на абонентском пункте _____, в коллективе _____ .

Настоящим _____
(фамилия, имя, отчество)

соглашается с обработкой своих персональных данных Удостоверяющим центром и признает, что персональные данные, заносимые в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Пользователь АП _____ _____
подпись И.О.Фамилия

«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №6
к Регламенту

Заявление

на формирование адресного справочника АП (область видимости АП)

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит сформировать адресный справочник АП Пользователя АП:

(добавить, удалить) _____

_____

Пользователь АП _____ _____
подпись И.О.Фамилия

«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №7
к Регламенту

Форма приказа

О допуске к работе в защищенной сети и предоставлении права владения сертификатами ключей проверки электронной подписи

В целях обеспечения юридической значимости электронных документов при осуществлении обмена документами в электронном виде и взаимодействие информационных систем в защищенной сети ViPNet №602 ТФОМС Саратовской области п р и к а з ы в а ю:

1. Создать группу по изучению правил работы со средством криптографической защиты информации (далее – СКЗИ) ViPNet Custom и допустить после прохождения обучения к работе с СКЗИ ViPNet Custom __ членов группы в составе:

руководителя организации Иванова И.И;

главного бухгалтера главной бухгалтерии Петрова П.П.;

специалиста-эксперта отдела ОМС Сидорова С.С.;

- -

2. Предоставить права владения сертификатами ключей проверки электронной подписи с полномочиями по подписанию электронных документов при осуществлении обмена документами в электронном виде и взаимодействие информационных систем в защищенной сети ViPNet №602 ТФОМС Саратовской области следующим сотрудникам < наименование организации >:

№ п/п	Фамилия, инициалы	Должность	Структурное подразделение	Полномочия
1	2	3	4	5
1.	Иванов И.И	руководитель		Пользователь Руководитель
2.	Петрова П.П.	главный бухгалтер	главная бухгалтерия	Пользователь Главный бухгалтер
3.	Сидорова С.С.	специалист-эксперт	отдел ОМС	Пользователь
4.	....			

3. Контроль за исполнением приказа оставляю за собой.

Должность руководителя	подпись	И.О.Фамилия

ПРИМЕЧАНИЕ:

1. Для «Полномочия» возможно указание следующих полномочий:

Руководитель - уполномоченное лицо юридического лица с правом первой подписи на основании учредительных документов или доверенности;

Главный бухгалтер - уполномоченное лицо юридического лица с правом второй подписи на основании учредительных документов или доверенности;

Пользователь – пользователь защищенной сети, аутентификация участников защищенной сети

2. Для каждого уполномоченного лица в таблице делается отдельная строка, в которой указываются все полномочия данного лица.

Приложение №8
к Регламенту

Заявление

на изготовление сертификата ключа проверки электронной подписи Пользователя АП
при генерации ключей подписей в УЦ

_____
(наименование организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

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

_____
(фамилия, имя, отчество)

в соответствии с указанными в настоящем заявлении идентификационными данными и областями использования ключа:

Наименование поля	**Описание**	**Значение**
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
CountryName, C	Страна	RU
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
StateOrProvinceName, S	Наименование области	Субъект РФ места нахождения юридического лица
StreetAddress, Street	Адрес	Часть адреса места нахождения юридического лица, включающую наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationName, O	Наименование организации	Наименование юридического лица
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
Title, T	Должность	Наименование должности уполномоченного представителя юридического лица (владельца сертификата)

OGRN	Основной государственный регистрационный номер (ОГРН)	ОГРН юридического лица
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица
Extended Key Usage	Расширенное использование ключа	Набор объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, описывающие юридическую сферу применения соответствующего сертификата

Пользователь АП

_____ _____
подпись И.О.Фамилия

«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №9
к Регламенту

Заявление

на аннулирование (отзыв) сертификата ключа проверки электронной подписи
Пользователя АП

_____
(наименование организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит аннулировать (отозвать) сертификат ключа проверки электронной подписи своего уполномоченного представителя – Пользователя АП: _____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Наименование поля	**Описание**	**Значение**
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица
CRL Reason Code	Код отзыва	Код причины отзыва сертификата "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановление действия

Пользователь АП _____ _____
подпись И.О.Фамилия
«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия
МП
«____» _____ 20____ г.
дата подписания заявления

Приложение №10
к Регламенту

Заявление

на приостановление действия Сертификат ключа проверки электронной подписи Пользователя АП

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит приостановить действие сертификата ключа подписи своего полномочного представителя - Пользователя АП: _____ ,
(фамилия, имя, отчество)

содержащего следующие идентификационные данные:

Наименование поля	Описание	Значение
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

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

Пользователь АП

_____ _____
подпись И.О.Фамилия

«____» _____ 20____ г.

_____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

ПРИМЕЧАНИЕ:
Приостановление действия сертификата может осуществляться по инициативе Владельца сертификата на период возможного длительного неисполнения обязанностей, связанных с подписанием ЭД.

Приложение №11
к Регламенту

Заявление

на возобновление действия сертификата ключа проверки электронной подписи
Пользователя АП

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит возобновить действие сертификата ключа проверки электронной подписи своего полномочного представителя – Пользователя АП: _____
(фамилия, имя, отчество)

содержащий следующие идентификационные данные:

Наименование поля	**Описание**	**Значение**
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата)
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

_____ _____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №12
к Регламенту

Заявление

на подтверждение подлинности электронной подписи Уполномоченного лица УЦ в сертификате ключа проверки электронной подписи

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность электронной подписи Уполномоченного лица УЦ в изданном УЦ сертификате ключа проверки электронной подписи Пользователя АП и установить его статус (действует / не действует) на основании предоставленных исходных данных:

1. Файл сертификата ключа проверки подписи на прилагаемом к заявлению внешнем носителе данных;
2. Время[1] (период времени) на момент наступления которого требуется установить статус сертификата: «_____» по «_____».

_____ подпись _____
Должность руководителя И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

---

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

Приложение №13
к Регламенту

Заявление

на подтверждение подлинности электронной подписи в электронном документе

_____
(наименование Организации)

в лице _____,
(должность руководителя)

_____,
(фамилия, имя, отчество руководителя)

действующего на основании _____

Просит подтвердить подлинность ЭП в электронном документе и предоставить информацию о статусе сертификата ключа проверки электронной подписи Пользователя АП (действовал / не действовал):

1. Файл электронного документа на прилагаемом к заявлению внешнем носителе данных;
2. Дата подписания документа ЭП: «____» _____ 20___г.»;
3. Значения полей сертификата:

Наименование поля	Описание	Значение
SerialNumber, SN	Серийный номер	Серийный номер сертификата ключа подписи
Common Name, CN	Общее имя	Сокращенное наименование юридического лица
SureName	Фамилия	Фамилия уполномоченного представителя юридического лица (владельца сертификата
GivenName	Приобретенное имя	Имя и отчество (если имеется) уполномоченного представителя юридического лица (владельца сертификата)
LocalityName, L	Наименование населенного пункта	Город или населенный пункт места нахождения юридического лица
Email, E	Адрес электронной почты	Адрес электронной почты владельца сертификата
OrganizationUnitName, OU	Подразделение организации	Наименование подразделения, сотрудником которого является уполномоченный представитель юридического лица (владелец сертификата)
INN	Идентификационный номер налогоплательщика (ИНН)	ИНН юридического лица
UnstructuredName	Неструктурированное имя	Наименование абонентского пункта юридического лица

_____ _____ _____
Должность руководителя подпись И.О.Фамилия

МП

«____» _____ 20____ г.
дата подписания заявления

Приложение №14
к Регламенту

Перечень

объектных идентификаторов (OID), определяющих области применения сертификатов ключей проверки ЭП, создаваемых УЦ

Объектный идентификатор	Описание	Область правоотношений
	Базовые OID	
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента	
1.3.6.1.5.5.7.3.4	Защищенная электронная почта	
	Дополнительные OID из ветки OID УЦ	
1.2.643.3.164	Идентификация удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области	Идентификация удостоверяющего центра корпоративного уровня Территориального фонда обязательного медицинского страхования Саратовской области для организации юридической значимости защищенного обмена электронными документами и взаимодействия информационных систем путем формирования и утверждения перечня объектных идентификаторов областей применения сертификатов ключей проверки ЭП и включения перечня объектных идентификаторов в форму соглашения с пользователями
1.2.643.3.164.1	Уполномоченное лицо УЦКУ	Уполномоченное лицо, наделенное Удостоверяющим центром правом по заверению сертификатов ключей подписей и списков отозванных сертификатов
1.2.643.3.164.2	Пользователь абонентского пункта защищенной сети ViPNet №602	Уполномоченное лицо юридического лица с правом Аутентификации участников защищенной сети, проверки ЭП в ЭД (кроме сертификатов и списков отозванных сертификатов); невозможности отказа от ЭП в ЭД (кроме сертификатов и списков отозванных сертификатов); зашифрования закрытых и секретных ключей; зашифрования данных; согласования ключей
1.2.643.3.164.2.1	Руководитель	Уполномоченное лицо юридического лица с правом первой подписи на основании учредительных документов или доверенности
1.2.643.3.164.2.2	Главный бухгалтер	Уполномоченное лицо юридического лица с правом второй подписи на основании учредительных документов или доверенности

Приложение №15
к Регламенту

ЖУРНАЛ УЧЕТА ИЗГОТОВЛЕНИЯ И ВЫДАЧИ КЛЮЧЕЙ ПОД РОСПИСЬ

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)			Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ,ключевых документов		Примечание
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении	дата и номер сопроводительного письма	дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Приложение №16
к Регламенту

ПРОТОКОЛ
установления межсетевого взаимодействия
«__» _____ 20___г. г. _____

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
№ ____	_____
№ ____	_____

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet-сетей _____ и _____.
3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№ ___	_____	_____
№ ___	_____	_____

4. Передача начального и ответного экспорта между сетями № ___ и № ___ осуществлялась через специалиста _____.
5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети №___.
6. Для установления межсетевого взаимодействия были назначены серверы-маршрутизаторы для организации шлюза:
в сети № ___ – «_____»,
в сети № _____ – «_____».
7. При установлении межсетевого взаимодействия в части электронной цифровой подписи, были произведены импорты справочников главных абонентов сети № _____ и сети № ___.
8. Смена межсетевых ключей, изменение состава АП, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Деловая почта] с указанием производимых изменений.
9. Стороны обязуются без предварительного согласования не производить изменений в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия.

Руководитель (должность)
ФИО _____

Специалист (должность)
ФИО _____

«____»_____20___ г.

Руководитель (должность)
ФИО _____

Специалист (должность)
ФИО _____

«____»_____20___ г.

Приложение №17
к Регламенту

Журнал изменений
ТФОМС Саратовской области (либо название сторонней организации)
по организации защищенного информационного взаимодействия
с _название сторонней организации_ (либо ФОМС (ТФОМС))

№ п/п	Наименование произведенного изменения в межсетевом взаимодействии с ФОМС (ТФОМС) (либо _название сторонней организации_)	Дата изменения	Подпись специалиста, проводившего изменения
1			
2			
3			

Пояснение по ведению журнала изменений

1. В журнал заносятся все события, которые относятся к организации защищенного информационного взаимодействия с название сторонней организации_ (либо ФОМС (ТФОМС)):

0 установление межсетевого взаимодействия,

1 выбор Координатора, выполняющего функции сервера-шлюза,

2 формирование межсетевого мастер-ключа,

3 плановая смена межсетевого мастер-ключа,

4 смена ключей при компрометации,

5 модификация межсетевого взаимодействии (добавление или удаление сетевого узла и т.д.

2. Каждая запись журнала должна заверяться специалистом, производившим изменение.

Приложение №2
к приказу ТФОМС
Саратовской области
от 01.07.2013 № 173

ОБРАЗЕЦ
печати для деятельности УЦ