УТВЕРЖДАЮ
Первый заместитель директора ХКФОМС

А.Л. Марычев

« 06 » 04 2017 г.

Р Е Г Л А М Е Н Т
удостоверяющего центра Хабаровского краевого фонда
обязательного медицинского страхования

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данный Регламент удостоверяющего центра Хабаровского краевого фонда обязательного медицинского страхования (далее – Регламент) определяет основные принципы использования электронной цифровой подписи при различных вариантах организации управления системой сертификации ключей подписи на базе средства криптографической защиты информации «Домен-К», входящего в состав программного комплекса ViPNet Custom, реализующего функции электронной подписи и шифрования информации.

1.2. Целью настоящего Регламента является создание необходимых условий для реализации в Хабаровском краевом фонде обязательного медицинского страхования (далее – ХКФОМС, Фонд), подчинённых ему органах и участниках обязательного медицинского страхования (далее – ОМС) Хабаровского края действующего законодательства Российской Федерации, по использованию электронной подписи, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

1.3. Регламент разработан в соответствии с требованиями действующих Федеральных законов от 6 апреля 2011 года № 63 «Об электронной подписи»; от 7 июля 2003 года № 126-ФЗ «О связи» и от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и является основным руководящим документом для Фонда, выполняющего функции удостоверяющего центра, для абонентов защищенной сети ViPNet №620.

1.4. Любой заинтересованный участник ОМС может ознакомиться с Регламентом на сайте Фонда по адресу http://www.khfoms.ru либо по запросу получить его копию в офисе Фонда.

1.5. Внесение изменений (дополнений) в Регламент, в том числе Приложений к нему, производится удостоверяющим центром Фонда в одностороннем порядке. Уведомление пользователей удостоверяющего центра Фонда о внесении изменений (дополнений) в Регламент осуществляется удостоверяющим центром Фонда путем размещения актуальной версии Регламента, включающей изменения (дополнения) на сайте Фонда и/или веерной рассылкой по Деловой почте сети ViPNet.

1.6. Изменения (дополнения), вносимые удостоверяющим центром Фонда, кроме изменений (дополнений), вызванных изменениями законодательства РФ и нормативными документами государственных органов, вступают в силу и становятся обязательными по истечении 5 (пяти) календарных дней с даты размещения указанных изменений и дополнений в Регламенте на сайте Фонда.

1.7. Изменения (дополнения), вносимые удостоверяющим центром Фонда в Регламент в связи с изменением законодательства РФ и нормативными документами государственных органов, регулирующих деятельность удостоверяющих центров, вступают в силу одновременно с вступлением в силу соответствующих законодательных и нормативных актов.

1.8. Действие изменений и дополнений в Регламенте с момента их вступления в силу распространяется на всех пользователей удостоверяющего центра Фонда, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

1.9. Услуги удостоверяющего центра Фонда, в рамках защищенной сети ViPNet № 620, предоставляется на безвозмездной основе.

1.10.Удостоверяющий центр Фонда не несет никакой ответственности в случае нарушения пользователями удостоверяющего центра Фонда положений настоящего Регламента. Претензии к удостоверяющему центру Фонда ограничиваются указанием на несоответствие его действий настоящему Регламенту.

1.11.Деятельность удостоверяющего центра Фонда может быть прекращена в порядке, установленном законодательством Российской Федерации. В случае прекращения деятельности удостоверяющего центра Фонда реестр удостоверяющего центра Фонда, включающий реестр зарегистрированных пользователей удостоверяющего центра Фонда, реестр изготовленных сертификатов открытых ключей, могут передаваться другому удостоверяющему центру по согласованию с владельцами сертификатов.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ [1]

ViPNet [Клиент] – ПО, обеспечивающее установление криптографически защищенных соединений, а также возможность гарантированной доставки подписанных *ЭП* сообщений (файлов) по назначению с автоматическим подтверждением доставки и прочтения документов, а также надежную защиту компьютера от несанкционированного доступа к различным информационным и аппаратным ресурсам на нем при работе компьютера в локальных или глобальных сетях, например, Интернет, в том числе от сетевых атак.

ViPNet [Координатор] – ПО, обеспечивающее маршрутизацию почтовых конвертов и управляющих сообщений при взаимодействии *ЦУС* и объектов сети между собой, регистрацию и предоставление информации о текущих IP-адресах и способах подключения объектов *Защищенной сети*, выполняющее функции ViPNet-Firewall и ViPNet-сервер открытого Интернета.

ViPNet [Удостоверяющий и ключевой центр], УКЦ – ПО, состоящее из *Удостоверяющего Центра*, практически реализующего выполнение функций *УЦ*, связанных с изданием, заверением, отзывом и хранением *Сертификатов ключей подписи*, а также других функций, предусмотренных действующими Федеральным законом от 6 апреля 2011 года № 63 «Об электронной подписи», и ключевого центра, обеспечивающего формирование и обновление ключевой информации для взаимодействия между *Узлами Защищенной Сети* и *Абонентами* в соответствии с заданными связями.

ViPNet [Центр управления сетью], *ЦУС – ПО*, предназначенное для создания и управления конфигурацией виртуальной сети на базе распределенной системы персональных и межсетевых экранов *Технологии ViPNet*, обеспечивающей защиту функционирования компьютеров и передаваемой информации в *ЗСПД Фонда*, и решает следующие основные задачи:

- построение инфраструктуры виртуальной сети (*Узлы Защищенной Сети* и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка защищенных адресных справочников, защищенных таблиц маршрутизации;
- формирование информации о ключевых связях *Абонентов* для ключевого центра;
- определение прав доступа к ресурсам каждого *Абонента*.

Абонент ЗСПД Фонда, *Абонент – Владелец Сертификата ключа подписи*, включённый в список *Абонентских пунктов* и *Абонентов ЗСПД Фонда* и зарегистрированный хотя бы на одном из *Абонентских пунктов*.

[1] - далее в тексте документа, для лучшего понимания, термины и определения написаны с Прописной буквы и выделены *курсивом* (например – *Внеплановая смена ключей*)

Абонентский пункт ЗСПД Фонда, *Абонентский пункт*, *АП* – компьютер, включённый в список *Абонентских пунктов* и *Абонентов ЗСПД Фонда*, на котором зарегистрирован хотя бы один *Абонент*, с установленными *СКЗИ – ПО ViPNet [Клиент]*, реализующими функции шифрования и *ЭП*, в том числе:

- создание *ЭП* в *Электронном документе* с использованием *Закрытого ключа ЭП*;
- *Подтверждение подлинности ЭП* в *ЭД* с использованием *Открытого ключа ЭП*;
- контроль целостности и достоверности ключей и *Сертификатов*;
- предупреждение о приближающемся истечении срока действия *Сертификата*;
- создание *Закрытых* и *Открытых ключей ЭП* и электронных запросов в *УЦ* на получение новых *Сертификатов*.

Автоматизированное рабочее место ViPNet [Администратор], *АРМ [Администратор]* – аппаратно-программный комплекс представляющий собой компьютер с установленным *ПО ViPNet [Центр управления сетью]* и *ViPNet [Удостоверяющий и ключевой центр]*, установленный в Фонде и эксплуатируемый *Администратором.*

Администратор – должностное лицо Фонда, назначенное для эксплуатации *АРМ [Администратор]*. *Администратор* одновременно является *Уполномоченным лицом УЦ* (*Главным абонентом ViPNet*), удостоверяющим своей *ЭП Сертификаты ключей подписей* всех остальных *Абонентов* сети ViPNet.

Владелец Сертификата ключа подписи, *Владелец* – физическое лицо, на имя которого *УЦ* издан *Сертификат ключа подписи*, и которое владеет соответствующим *Закрытым ключом ЭП*, позволяющим с помощью *Средств ЭП АП* подписывать своей *ЭП Электронные документы*.

Владельцем Сертификата ключа подписи может быть только физическое лицо, уполномоченное организацией участником ОМС Хабаровского края.

Владельцем Сертификата ключа подписи, изданного *УЦ Фонда*, может быть только сотрудник структурного подразделения организации, входящей в ОМС, наделённый полномочиями ведения переписки в *ЗСПД Фонда*, согласно уставным документам организации или приказа организации на право подписания *Электронных документов*.

Внеплановая смена ключей – смена ключей вне установленной периодичности, вызванная *Компрометацией ключей*.

Главный абонент сети ViPNet, *Уполномоченное лицо УЦ* – лицо, назначенное в *УЦ* удостоверять *Сертификаты ключей подписи*, выдаваемых *УЦ*, от имени *УЦ*, на своем *Закрытом ключе ЭП.*

Доверенный способ передачи информации – способ передачи информации, принятый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности (соглашения) и обеспечивающий требуемую степень её защищенности.

Закрытый ключ Электронной цифровой подписи, *Закрытый ключ* – уникальная последовательность символов, доступная только *Владельцу Сертификата ключа подписи* и предназначенная для формирования в *Электронных документах Электронной цифровой подписи* с использованием *Средств ЭП Абонентского пункта.*

Защищенная сеть – информационная система, в которой для защиты информации, передаваемой по каналам открытой сети, используется её шифрование.

Защищенная сеть передачи данных Фонда, *ЗСПД Фонда* – корпоративная *Защищенная сеть*, использующая *Технологию ViPNet*, владельцем которой является Фонд.

Копия Сертификата ключа подписи – документ на бумажном носителе, содержащий информацию из *Сертификата ключа подписи* и заверенный собственноручными подписями *Владельца Сертификата ключа подписи* и *Уполномоченного лица Удостоверяющего Центра*, а также печатью *Удостоверяющего Центра*.

Ключевой дистрибутив – файл с расширением .dst, создаваемый *ПО УКЦ* для каждого *Абонента* сетевого *Узла*, в котором в зашифрованном на парольном ключе виде помещена необходимая адресная и ключевая информация для обеспечения первичного запуска на компьютере *ПО ViPNet [Клиент]* или *ViPNet [Координатор]*.

Компрометация ключа – утрата доверия к тому, что используемые ключи шифрования и/или *ЭП* обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Конфликтная ситуация – ситуация, при которой у *Владельца Сертификата ключа подписи* возникает необходимость разрешения вопросов признания или не признания авторства и/или подлинности *Электронных документов*, обработанных с помощью *Средств ЭП.*

Координатор – компьютер (сервер) с установленным *ПО ViPNet [Координатор]*, который обеспечивает:

- включение в *Защищенную сеть* открытых и защищенных компьютеров, находящихся в этой ЛВС, независимо от типа адреса, выделяемого им;
- разделение и защиту сетей от сетевых атак;
- оповещение *АП* о состоянии других сетевых *Узлов*, связанных с ним.

Открытый ключ Электронной подписи, Открытый ключ – уникальная последовательность символов, соответствующая *Закрытому ключу ЭП*, доступная любому *Абоненту* и предназначенная для *Подтверждения подлинности ЭП* в *ЭД* с использованием *Средств ЭП*.

Пользователь УЦ, *Пользователь* – физическое лицо, признающее данный регламент и получающее услуги *Удостоверяющего Центра*.

Плановая смена ключей – смена ключей с установленной периодичностью, не вызванная *Компрометацией ключей.*

ПО – программное обеспечение.

Подтверждение подлинности электронной подписи в электронном документе – положительный результат проверки средствами *Абонентского пункта* с использованием *Сертификата ключа подписи* принадлежности *ЭП* в *Электронном документе Владельцу Сертификата ключа подписи* и отсутствия искажений в подписанном данной *ЭП Электронном документе*.

Сертификат ключа подписи, *СКП, Сертификат ключа, Сертификат* – *Электронный документ* с *ЭП Уполномоченного лица УЦ* (*Администратора*) или документ на бумажном носителе, которые включают в себя *Открытый ключ ЭП*, выдаваемые *Абоненту* для *Подтверждения подлинности ЭП* и идентификации *Владельца Сертификата ключа подписи*.

Список отозванных сертификатов, *СОС* – созданный *УЦ* список *Сертификатов ключей подписи*, отозванных (аннулированных) до окончания срока их действия или действие которых было приостановлено.

Средства криптографической защиты информации, *СКЗИ* –программно-аппаратные средства, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Средства электронной подписи – СКЗИ, обеспечивающие реализацию следующих функций: создание *Электронной подписи* в *Электронном документе* с использованием *Закрытого ключа Электронной подписи*, *Подтверждение подлинности Электронной подписи в Электронном документе* с использованием *Открытого ключа Электронной подписи*, создание *Закрытых* и *Открытых ключей Электронных подписей*.

Технология ViPNet – технология, предназначенная для построения *Защищенной сети* путем использования системы персональных и межсетевых экранов на защищаемых элементах распределенной сети (рабочие станции, сервера, локальные сети), и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе *СКЗИ* «Домен-К».

Удостоверяющий Центр, *УЦ* – комплекс организационных и технических мероприятий, обеспечивающий изготовление, выдачу и управление *Сертификатами ключей подписи Пользователей*.

Удостоверяющий Центр Фонда, *УЦ Фонда* – комплекс организационных, штатных, технических мероприятий, обеспечивающих реализацию функций *Удостоверяющего Центра* в соответствии с нормами действующего Федерального закона от 6 апреля 2011 года № 63 «Об электронной подписи» в Фонде.

Узел Защищенной сети, *Узел* – это функционирующий *Абонентский пункт* или *Координатор*.

Уполномоченное лицо УЦ – см. Главный абонент сети ViPNet.

Электронная подпись, *ЭП* – реквизит *ЭД*, предназначенный для защиты данного *ЭД* от подделки, полученный в результате криптографического преобразования информации с использованием *Закрытого ключа ЭП* и позволяющий идентифицировать *Владельца Сертификата ключа подписи*, а также установить отсутствие искажения информации в *ЭД*.

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

3. СТАТУС И ОБЛАСТЬ ДЕЙСТВИЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1. Функции *Удостоверяющего Центра Фонда* выполняет Хабаровский краевой фонд обязательного медицинского страхования.

3.2. Фонд является корпоративным *Удостоверяющим Центром ЗСПД Фонда*, т.е. *Владельцами Сертификатов ключей подписи*, изданных УЦ *Фонда*, могут являться только уполномоченные сотрудники Фонда и уполномоченные сотрудники организаций участников ОМС Хабаровского края.

3.3. При необходимости устанавливается защищенный юридически значимый электронный документооборот с внешними организациями в соответствии с Регламентом регистрации и подключения к *Удостоверяющему Центру Фонда* пользователей сторонних организаций (Приложение №1 к настоящему Регламенту) с заключением Соглашения об обмене *Электронными документами* или Соглашения о совместных действиях по организации информационного обмена по телекоммуникационным каналам связи между Фондом и внешней организацией (примерный текст Соглашения приведен в Приложение №2 к настоящему Регламенту).

3.4. Если внешняя организация не использует сервисы *ЭП*, Фонд заблаговременно сообщает данной организации реквизиты внешних доверенных *УЦ*, с которыми Фонд заключил Соглашения о сотрудничестве по организации юридически значимого электронного документооборота между Фондом и внешними организациями и взаимном признании *ЭП*, и где для назначенных лиц внешней организации могут быть организованы выдача *Сертификатов ключей ЭП* и их подключение к системе электронного документооборота Фонда в соответствии с регламентом внешнего *УЦ*.

4. ПРАВА И ОБЯЗАННОСТИ

4.1. *Удостоверяющий Центр* вправе запросить у *Пользователя УЦ*, а *Пользователь УЦ* обязан предоставить *Удостоверяющему Центру* документы, подтверждающие следующую информацию: сведения, необходимые для идентификации *Пользователя УЦ* (фамилия, имя, отчество, должность, серия и номер документа удостоверяющего личность, СНИЛС, ИНН).

4.2. *Пользователь УЦ* имеет право:

4.2.1. Обратиться в *Удостоверяющий Центр* для аннулирования (отзыва) *Сертификата Открытого ключа* в течении срока действия соответствующего *Закрытого ключа*;

4.2.2. Обратиться в *Удостоверяющий Центр* для приостановления действия *Сертификата Открытого ключа* в течении срока действия соответствующего *Закрытого ключа*;

4.2.3. Обратиться в *Удостоверяющий Центр* для возобновления действия *Сертификата Открытого ключа* в течении срока действия соответствующего *Закрытого ключа*;

4.2.4. Обратиться в *Удостоверяющий Центр* за *Подтверждением подлинности Электронных подписей в Электронных документах*;

4.2.5. Обратиться в *Удостоверяющий Центр* за *Подтверждением подлинности Электронных подписей Уполномоченного лица Удостоверяющего Центра* в изготовленных им *Сертификатах Открытых ключей*

4.3. Организация участник ОМС, присоединившаяся к регламенту, имеет право:

4.3.1. Обратиться в *Удостоверяющий Центр* для регистрации своих должностных лиц (работников) в качестве *Пользователей УЦ*.

4.3.2. Обратиться в *Удостоверяющий Центр* для аннулирования (отзыва) *Сертификата Открытого ключа* своего работника в течении срока действия соответствующего *Закрытого ключа*;

4.4. *Удостоверяющий Центр* имеет право:

4.4.1. Отказать в изготовлении *Сертификата ключа подписи Пользователя УЦ* в случае ненадлежащего оформления заявления на изготовление *Сертификата ключа подписи*.

4.4.2. Отказать в изготовлении *Сертификата ключа подписи Пользователя УЦ* в случае, если использованное *Пользователем УЦ* для формирования запроса на *Сертификат ключа подписи Средство криптографической защиты информации* не поддерживается *Удостоверяющим Центром*.

4.4.3. Отказать в аннулировании (отзыве) *Сертификата ключа подписи Пользователя УЦ* в случае ненадлежащего оформления заявления на аннулирование (отзыв) *Сертификата ключа подписи*.

4.4.4. Отказать в приостановлении/возобновлении действия *Сертификата ключа подписи Пользователя УЦ* в случае ненадлежащего оформления заявления на приостановление/возобновление действия *Сертификата ключа подписи*.

4.4.5. Отказать в аннулировании (отзыве) *Сертификата ключа подписи Пользователя УЦ* в случае, если истек установленный срок действия *Закрытого ключа*, соответствующего этому *Сертификату*.

4.4.6. Отказать в приостановлении/возобновлении действия *Сертификата ключа подписи Пользователя УЦ* в случае, если истек установленный срок действия *Закрытого ключа*, соответствующего этому *Сертификату*.

4.4.7. Аннулировать (отозвать) *Сертификат ключа подписи Пользователя УЦ* в случае установленного факта *Компрометации* соответствующего *Закрытого ключа*, с уведомлением *Владельца* аннулированного (отозванного) *Сертификата ключа подписи* и указанием обоснованных причин.

4.4.8. Приостановить действие *Сертификата ключа подписи Пользователя УЦ* с уведомлением *Владельца Сертификата ключа подписи*, действие которого приостановлено, и указанием обоснованных причин.

4.5. *Пользователь* обязан:

4.5.1. Сформировать (инициализировать) *Открытые* и *Закрытые ключи* на своем рабочем месте с использованием средства *ЭП*.

4.5.2. Хранить в тайне личный пароль, отвечающий за *Закрытый ключ ЭП*, принимать все возможные меры для предотвращения его раскрытия, искажения и несанкционированного использования.

4.5.3. Использовать *Сертификат Открытого ключа* только для целей, разрешенных соответствующими областями использования, определенными в *Сертификате*.

4.5.4. Немедленно обратиться в *Удостоверяющий Центр* с заявлением на аннулирование (отзыв) *Сертификата ключа подписи* в случае раскрытия, искажения личного пароля, отвечающего за *Закрытый ключ ЭП*, а также в случае, если *Пользователю* стало известно, что этот ключ используется или использовался ранее другими лицами.

4.5.5. Применять для формирования *Электронной подписи* только действующий личный *Закрытый ключ*.

4.5.6. Применять личный *Закрытый ключ* только в соответствии с областями действия, указанными в соответствующем данному ключу *Сертификате ключа подписи*.

4.5.7. Не использовать личный *Закрытый ключ*, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

4.5.8. Не использовать личный *Закрытый ключ,* связанный с *Сертификатом ключа подписи*, заявление на аннулирование (отзыв) которого подано в *Удостоверяющий Центр*, в течение времени, исчисляемого с момента подачи заявления на аннулирование (отзыв) *Сертификата* в *Удостоверяющий Центр* по момент времени официального уведомления *Пользователя* об аннулировании (отзыве) *Сертификата*.

4.5.9. Не использовать личный *Закрытый ключ*, связанный с *Сертификатом ключа подписи*, заявление на приостановление действия которого подано в *Удостоверяющий Центр*, в течение времени, исчисляемого с момента подачи заявления на приостановление действия *Сертификата* в *Удостоверяющий Центр* по момент времени официального уведомления *Пользователя* о приостановлении действия *Сертификата*.

4.5.10. Не использовать личный *Закрытый ключ*, связанный с *Сертификатом ключа подписи*, который аннулирован (отозван) или действие которого приостановлено.

4.5.11. Сформировать новый запрос на *Сертификат* (соответствующий новым *Закрытым* и *Открытым ключам*), с новыми регистрационными данными, если изменились регистрационные данные, указанные в текущем (действующем) *Сертификате Пользователя*.

4.5.12. Перед тем как использовать *Сертификат Открытого* ключа другого *Пользователя*, изготовленный *Удостоверяющим Центром*, должен удостовериться, что назначение *Сертификата*, определенное соответствующими областями использования, определенными в *Сертификате*, соответствует предполагаемому использованию.

4.6. Организация участник ОМС, присоединившаяся к регламенту, обязана:

4.6.1. Представить регистрационную и идентифицирующую информацию на лиц, проходящих процедуру регистрации в *Удостоверяющем Центре*, в объеме, определенном положениями настоящего Регламента.

4.6.2. Извещать *Удостоверяющий Центр* об изменениях в регистрационной информации *Пользователя*, приведенных в *Сертификате Пользователя* и предоставлять их по требованию *Удостоверяющего Центра* в течение 5 (Пяти) рабочих дней с момента регистрации изменений.

4.7. *Удостоверяющий Центр* обязан:

4.7.1. Использовать *Закрытый ключ Уполномоченного лица Удостоверяющего Центра* только для подписи издаваемых им *Сертификатов ключей подписи Пользователей УЦ* и *Списков отозванных Сертификатов*.

4.7.2. Принять меры по защите *Закрытого ключа Уполномоченного лица Удостоверяющего Центра* от несанкционированного доступа.

4.7.3. Обеспечить уникальность регистрационной информации *Пользователей УЦ*, заносимой в реестр *Удостоверяющего Центра* и используемой для идентификации *Владельцев Сертификатов Открытых ключей*.

4.7.4. Уведомлять *Владельца Сертификата Открытого ключа* о фактах, которые стали известны *Удостоверяющему Центру* и которые существенным образом могут сказаться на возможности дальнейшего использования *Сертификата Открытого ключа*.

4.7.5. Организовать свою работу по GMT (Greenwich Mean Time, Среднее Время по Гринвичскому Меридиану) с учетом часового пояса и синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

4.7.6. Предоставить *Пользователю УЦ* по его требованию:

- Копию лицензии на право предоставления услуг в области шифрования информации.
- Копию лицензии на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств.

5. УСЛОВИЯ ПРИЗНАНИЯ РАВНОЗНАЧНОСТИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И СОБСТВЕННОРУЧНОЙ ПОДПИСИ

5.1. *Электронный документ*, полученный *Абонентом ЗСПД Фонда* с использованием средств *Абонентского пункта*, на основании действующего Федерального закона от 6 апреля 2011 года № 63 «Об электронной подписи» и настоящего Регламента признаётся эквивалентным такому же документу на бумажном носителе, заверенному собственноручной подписью должностного лица, от имени которого получен документ, и печатью соответствующего юридического лица (если документ подразумевает простановку печати), при условии соблюдения следующих условий:

- *Сертификат ключа подписи*, соответствующий *Электронной подписи* полученного *Электронного документа*, не утратил силу (действует) на момент получения документа средствами *Абонентского пункта*, указанный в соответствующем журнале регистрации *Абонентского пункта*, или на момент подписания данного документа, указанный при проверке его свойств, средствами *Абонентского пункта* в соответствующем реквизите;
- подлинность *Электронной подписи* в *Электронном документе* подтверждена средствами *Абонентского пункта*;
- *Электронная подпись* в *Электронном документе* используется в соответствии со сведениями, указанными в *Сертификате ключа подписи*;
- *Сертификат ключа подписи*, относящийся к *ЭП* полученного документа, издан в *УЦ Фонда* или во внешнем *УЦ*, если с указанным сторонним *УЦ* соответствующим договором (соглашением) установлены доверительные отношения.

5.2. При одновременном наличии *Электронного документа*, подлинность *ЭП* которого подтверждается с помощью средств *Абонентского пункта*, и эквивалентного ему документа на бумажном носителе, заверенного собственноручной подписью и печатью, подлинником документа считается *Электронный документ*, а документ на бумажном носителе – его бумажной копией.

6. ФУНЦИИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

6.1. Функции *УЦ Фонда*:

6.1.1. внесение в реестр *Удостоверяющего Центра* регистрационной информации о *Пользователях УЦ*.

6.1.2. создание *Ключевых дистрибутивов* при регистрации новых *Абонентских пунктов ЗСПД Фонда*, а также при регистрации на *Абонентских пунктах ЗСПД Фонда* новых *Абонентов* с гарантией конфиденциальности *Закрытого ключа Электронной подписи*.

6.1.3. издание *Сертификатов ключей подписи* в электронной форме.

6.1.4. изготовление *Копий Сертификатов ключей подписи Пользователей УЦ* на бумажном носителе.

6.1.5. ведение реестра изданных *Сертификатов ключей подписи Пользователей УЦ*, обеспечение его актуальности и возможности доступа к нему *Абонентов ЗСПД Фонда* и взаимодействующих информационных систем.

6.1.6. приостановление и возобновление действия *Сертификатов ключей подписи*, а также их отзыв (аннулирование).

6.1.7. предоставление сведений об аннулированных и приостановленных *Сертификатах ключей подписи Пользователей УЦ*.

6.1.8. *Подтверждение подлинности Электронных подписей Пользователей УЦ* в *Электронных документах*.

7. ПРИСОЕДИНЕНИЕ К РЕГЛАМЕНТУ УЦ ФОНДА ОРГАНИЗАЦИЙ УЧАСТНИКОВ ОМС ХАБАРОВСКОГО КРАЯ

7.1. Фонд считается присоединившимся к регламенту априори.

7.2. Любая организация участник ОМС Хабаровского края, желающая присоединиться к регламенту *УЦ Фонда*, должна выполнить определенный набор действий:

7.2.1 приобрести, если не имеет в наличии в нужном количестве, необходимое ПО, поддерживаемое *УЦ Фонда* (*ViPNet [Клиент]* и/или *ViPNet [Координатор]*).

7.2.2 обеспечить возможность синхронизации смены *ПО* на своих рабочих местах со сменой *ПО* в *УЦ*, для этого необходимо иметь договор технической поддержки на обновление используемого *ПО*.

7.2.3 обеспечить эксплуатацию используемого *ПО* в соответствии с эксплуатационно-технической документацией и законодательными и руководящими документами на *СКЗИ* и *ЭП*, действующими в Российской Федерации.

7.2.4 подать заявление на присоединение к Регламенту *Удостоверяющего Центра Фонда*. Форма заявления на присоединение к Регламенту *Удостоверяющего Центра Фонда*, направляемого организацией, приведена в Приложении №3 к Регламенту.

8. РЕГИСТРАЦИЯ ДОЛЖНОСТНЫХ ЛИЦ ЗСПД ФОНДА В КАЧЕСТВЕ АБОНЕНТОВ УЦ

8.1. Регистрация *Абонентских пунктов* и *Абонентов ЗСПД Фонда* в качестве *Узлов* и *Абонентов* сети ViPNet осуществляется *Администратором* в *АРМ [Администратор]* в соответствии с функциональными обязанностями *Абонентов* (для должностных лиц Фонда) или бланка запроса на регистрацию *Пользователя*, переданного в Фонд с сопроводительным письмом (для должностных лиц организаций, присоединившихся к Регламенту, Форма бланка запроса приведена в приложении №4 к Регламенту.) и эксплуатационно-технической документацией организации-разработчика ПО ViPNet.

8.2. В запросе на регистрацию, при необходимости, дополнительно могут быть уточнены реквизиты *Абонента*, указываемые в электронном запросе на *Сертификат*, и иные сведения, включаемые в *Сертификат*:

8.2.1. реквизит «Имя» (CN) - состоит из фамилии, имени и отчества (если есть) *Владельца Сертификата подписи* в именительном падеже;

8.2.2. реквизит «ИНН» (INN) – состоит из уникального регистрационного номера *Владельца СКП*. Для формирования уникального регистрационного номера представителя организации (*Владельца СКП*), входящей в систему ОМС, применяется последовательность, состоящая из 10-символьного индивидуального номера налогоплательщика (ИНН) без пробелов или иных разделителей;

8.2.3. реквизит «СНИЛС» (SNILS) – состоит из уникального регистрационного номера *Владельца СКП*. Для формирования уникального регистрационного номера представителя организации (*Владельца СКП*), входящей в систему ОМС, применяется последовательность, состоящая из 11-символьного страховой номер индивидуального лицевого счета (СНИЛС) без пробелов или иных разделителей

8.2.4. реквизит «Должность» (T) - состоит из полного наименования должности *Владельца СКП* (в именительном падеже);

8.2.5. реквизит «Подразделение» (OU) - состоит из наименования структурного подразделения организации, входящей в систему ОМС. В связи с ограничением длины данного реквизита допускается указывать общепринятое сокращённое наименование, например: «Удостоверяющий и Ключевой центр»;

8.2.6. реквизит «Организация» (O) – состоит из официального полного наименования и общепринятого сокращённого наименования организации, входящей в систему ОМС, например: «Хабаровский краевой фонд обязательного медицинского страхования (ХКФОМС)»;

8.2.7. реквизит «Город» (L) – состоит из наименования города (в именительном падеже), в котором расположена организация (подразделение организации), входящей в систему ОМС, в котором открыта должность *Владельца Сертификата подписи*;

8.2.8. реквизит «Область» (S) – состоит из наименования области, без слов «область» или «обл.»;

8.2.9. реквизит «Страна» (C) – состоит из международного идентификатора Российской Федерации – «RU»;

8.2.10. реквизит «E-mail» (EMail) – состоит из одного адреса электронной почты организации, входящей в систему ОМС (указывается только официальный почтовый ящик и заполняется только строчными буквами);

8.2.11. реквизит «Почтовый адрес» (STREET) – состоит из юридического адреса организации (подразделения организации), входящей в систему ОМС, в котором открыта должность *Владельца Сертификата ключа подписи*, с обязательным указанием почтового индекса, например: 680000 г.Хабаровск ул.Фрунзе д.69.

Запрос подписывается собственноручной подписью *Абонента (Владельца СКП)*, заверяется подписью руководителя и печатью организации, входящей в систему ОМС. Содержащиеся в запросе сведения подтверждаются, при необходимости, предъявлением соответствующих документов.

8.3. Запрос на регистрацию *Пользователя УЦ* рассматривается в течение 3 (трёх) рабочих дней. В случае отказа, запрос на регистрацию, возвращается заявителю. В случае положительного решения о регистрации, на основании введенных данных об *Абонентских пунктах*, *Абонентах* и разрешенных связях между *Узлами*, формируется *Ключевой дистрибутив* для каждого конкретного *Абонента*. Одновременно для каждого конкретного *Абонента* формируется резервный набор персональных ключей, необходимый для дистанционного обновления ключей *Абонента* при их *Компрометации*, который передается *Абоненту или Администратору* организации входящей в систему ОМС, если тот территориально удален от месторасположения *УЦ Фонда*.

8.4. *Ключевой дистрибутив* вместе с паролем доступа к нему передается лично *Абоненту* одним из установленных *Доверенных способов передачи*, либо используется *Администратором*, при установке ПО *ViPNet [Клиент]*, о чем делается отметка в Журнале учета выдачи *Ключевых дистрибутивов* (Приложение №5 к настоящему Регламенту). Журнал ведётся *Уполномоченным лицом УЦ*.

8.5. Повторно *Ключевой дистрибутив* для конкретного *Абонента* может быть выдан при исправлении технических сбоев аппаратуры, решении организационно-технических вопросов, *Компрометации*, с подачей заявления руководителя организации участника ОМС на бумажном носителе. В случае отсутствия *Компрометации*, переиздание *Ключевого дистрибутива* допускается не чаще одного раза в четыре месяца.

8.6. Установка ПО *ViPNet [Клиент]* на *Абонентские пункты* производится с использованием выданных *Ключевых дистрибутивов Абонентов*, одновременно организуется допуск *Абонентов* к работе с *АП*. Съёмный носитель (флэш-носитель, CD и др.) с выданным резервным набором персональных ключей *Абонента*, необходимым для дистанционного обновления ключей *Абонента* при их *Компрометации*, если он выдан, должен храниться в надежном месте (в сейфе, запираемом ящике или шкафе).

8.7. *Закрытый ключ Электронной подписи* из состава *Ключевого дистрибутива*, сформированного *УЦ*, применяется только для подписи электронного запроса на *Сертификат* с новым *Открытым ключом*, формируемым *Абонентом* в ходе сеанса работы на своем *АП* и отправляемым в *УКЦ* для получения *Сертификата ключа подписи*.

Допускается использование ключей *ЭП Абонента* из состава его *Ключевого дистрибутива* в процессе обучения и допуска *Абонента* к работе с *АП*.

9. ИЗДАНИЕ СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСИ АБОНЕНТОВ

9.1. Издание *Сертификата ключа подписи Абонента* осуществляется *Администратором* в *АРМ [Администратор]* на основании бумажного и/или электронного запроса *Абонента* на *Сертификат*.

Электронный запрос формируется ПО *АП*, при этом автоматически вырабатываются новые ключи подписи *Абонента*.

9.2. Все изданные *Сертификаты ключей подписи* учитываются в Реестре *Сертификатов ключей подписи*, который ведётся *Уполномоченным лицом УЦ Фонда* в электронном виде в *УКЦ*.

9.3. Электронные запросы на *Сертификат* и изданные *Сертификаты ключей подписи Абонентов* хранятся в *АРМ [Администратор]* и на *АП Абонентов* в электронном виде. *Уполномоченное лицо УЦ Фонда* распечатывает на бумажном носителе (на листах белой бумаги формата А4, не содержащих средств защиты от копирования и подделки) один экземпляр *Копии Сертификата ключа подписи* (Приложение №6 к настоящему Регламенту), которые заверяются собственноручной подписью *Уполномоченного лица* и печатью *УЦ Фонда*. *Копия Сертификата* на бумажном носителе также заверяется собственноручной подписью его *Владельца*. Экземпляр оформленных документов выдается *Владельцу СКП* или направляется в адрес организации.

9.4. После ввода в действие на своем *АП,* полученного *Сертификата ключа подписи,* его *Владелец* может приступать к юридически значимому информационному обмену *Электронными документами*.

10.ПОРЯДОК ПЛАНОВОЙ СМЕНЫ КЛЮЧЕЙ ПОДПИСИ

10.1. Срок действия *Сертификата ключа подписи Пользователя* в *ЗСПД Фонда* устанавливается в один год + 1 (один) месяц переходного периода. *Владельцы Сертификатов ключей подписи* обязаны производить периодическую (*Плановую*) замену используемых ключей подписи не реже указанного срока. Программное обеспечение *АП* заблаговременно[2] информирует *Абонента* о необходимости проведения данной процедуры.

10.2. Замена ключей подписи также может осуществляться *Абонентом* по собственной инициативе в любое время, но не чаще одного раза в квартал.

10.3. Замена ключей подписи осуществляется в обязательном порядке, если изменился любой из реквизитов, указанных в *Сертификате ключа подписи*. При этом *Владелец Сертификата* обязан заблаговременно известить *Администратора* о характере изменения реквизитов и согласовать с ним дату и порядок смены ключей подписи.

10.4. Смена ключей подписи, до истечения срока их действия, осуществляется *Абонентом* автоматизировано непосредственно на *АП* путем формирования новых ключей подписи и отправки электронного запроса на *Сертификат*, без необходимости прибытия в *УЦ Фонда*.

10.5. *Администратор* должен осуществлять сертификацию ключа подписи *Абонента* по возможности в день получения электронного запроса, но не позднее дня истечения срока действия действующего *СКП*. После ввода *Сертификата ключа подписи* в действие *Абонент* осуществляет информационный обмен с *ЭП* на новых ключах. *Копии Сертификата* на бумажном носителе оформляются аналогично указанному в п.9.3, но пересылка, для подписания *Пользователем Копий Сертификатов*, осуществляется обычной почтой.

10.6. Если *Абонент* не выполнил смену ключей подписи до истечения срока действия *Сертификата*, то изготовление нового *Сертификата* ключа подписи и, при необходимости, *Ключевого дистрибутива* осуществляется согласно п. 11.9.

[2] – по умолчанию за 15 дней, максимальное значение может быть установлено вручную до 30 дней.

11.СМЕНА КЛЮЧЕЙ В СЛУЧАЕ ИХ КОМПРОМЕТАЦИИ (ВНЕПЛАНОВАЯ СМЕНА КЛЮЧЕЙ)

11.1. Если возникает сомнение в неизвестности посторонним лицам пароля доступа *Абонента* при старте модулей ViPNet (этот пароль отвечает за доступ к ключам *ЭП* и шифрования *Абонента*), но доступ к компьютеру этих посторонних лиц был невозможен, *Абоненту* следует сменить пароль и продолжить работу. Если доступ к компьютеру посторонних лиц был возможен, то ключи *Абонента* считаются скомпрометированными.

11.2. К событиям *Компрометации*, когда ключи *Абонента* считаются скомпрометированными, также относятся следующие случаи:

11.2.1. посторонним лицам мог стать доступным файл *Ключевого дистрибутива Абонента*;

11.2.2. посторонним лицам мог стать доступным съемный носитель с ключевой информацией *Абонента*;

11.2.3. посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере *Абонента*;

11.2.4. на *Абонентском пункте Абонента* сформирована конфигурация, допускающая использование данного АП в качестве прокси сервера, через который осуществляется web-доступ к серверам Фонда (сервер РС ЕРЗ, сервер портал АП и др.) пользователей локальной сети организации, не имеющих *ViPNet*;

11.2.5. на *Абонентском пункте Абонента* отсутствовал (был отключен) модуль *ViPNet [Клиент]* [Монитор], или он устанавливался в открытые режимы работы, и в локальной сети считается возможным присутствие посторонних лиц;

11.2.6. на *Абонентском пункте Абонента* отсутствовал (был отключен) модуль *ViPNet [Клиент]* [Монитор], или он устанавливался в открытые режимы работы, и на границе локальной сети отсутствовал (был отключен) сертифицированный межсетевой экран;

11.2.7. уволился *Абонент* (в т.ч. дублёр основного *Абонента* или его непосредственный начальник) или сотрудник подразделения автоматизации (информационных технологий, защиты информации), имевший доступ к паролям и ключам;

11.2.8. на сейфе с ключевыми документами (резервным набором персональных ключей) нарушена печать и/или замок имеет следы несанкционированного вскрытия;

11.2.9. случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в т.ч. когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошёл в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения на предмет происшествия *Компрометации* ключевой информации, относится возникновение подозрений в утечке информации при её передаче посредством *Защищенной сети*.

В случае увольнения *Абонента*, зарегистрированного на одном или нескольких *АП*, считаются скомпрометированными ключи всех *Абонентов*, зарегистрированных на этом (этих) *АП*.

В случае увольнения сотрудника подразделения автоматизации (информационных технологий, защиты информации) организации (подразделения организации), входящей в систему ОМС, имевший доступ к паролям и ключам, считаются скомпрометированными ключи всех *Абонентов* данной организации (подразделения организации).

В случае увольнения *Администратора УЦ Фонда* или его дублёра, считается скомпрометированной вся ключевая информация в корпоративной информационной системе ОМС Хабаровского края, т.е. ключи всех *Абонентов ЗСПД Фонда*.

11.3. В случае наступления любого из событий, связанных с *Компрометацией* ключевой информации, *Абонент* немедленно прекращает связь с другими *Абонентами* и сообщает о факте *Компрометации* (или предполагаемом факте *Компрометации*) *Администратору* или ответственному сотруднику организации участнику системы ОМС.

11.4. *Администратор*, при получении сообщения о *Компрометации* ключевой информации, определяет объём скомпрометированной ключевой информации, в том числе факт *Компрометации* резервного набора персональных ключей, исходя из следующих правил:

11.4.1. в случае признания факта *Компрометации* любого из *Закрытых* (секретных) *ключей*, записанных на ключевой дискете (или ином съёмном носителе ключевой информации) *Абонента*, признаются непосредственно скомпрометированными все ключи на данной дискете (носителе). Данный *Абонент* признается непосредственно скомпрометированным;

11.4.2. в случае признания факта непосредственной *Компрометации* любого из ключей у любого *Абонента* коллектива, однозначно признаются скомпрометированными все ключи, общие для *Абонентов* данного коллектива. *Абоненты* коллектива, не подвергшиеся непосредственной *Компрометации*, признаются косвенно скомпрометированными. У *Абонентов* коллектива, не подвергшихся непосредственной *Компрометации*, не скомпрометированными могут быть признаны только индивидуальные ключи (например, *Закрытый* (секретный) *ключ ЭП*);

11.4.3. в случае признания факта *Компрометации* любого из *Закрытых* (секретных) *ключей*, записанных на жестком диске, признаются скомпрометированными все ключи данного *АП*.

11.5. *Администратор* при получении сообщения о *Компрометации* ключевой информации в течение не более двух рабочих дней:

11.5.1. в ПО *ViPNet [Центр управления сетью]* объявляет ключи скомпрометированного *Абонента* (*Абонентского пункта*) скомпрометированными и создает средствами ПО *ЦУС* справочники связей при *Компрометациях* с необходимой информацией для *УКЦ*: файлы связей для полной замены индивидуальной ключевой информации скомпрометированных *Абонентов* и замены ключей *Абонентских пунктов*, где зарегистрированы скомпрометированные *Абоненты*; файлы связей для частичного обновления ключевой информации для всех *АП*, с которыми связаны *АП*, где зарегистрированы скомпрометированные *Абоненты*;

11.5.2. формирует средствами *УКЦ* для генерации ключей при *Компрометации* новую ключевую информацию. Все сформированные файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный *АП* и скомпрометированному *Абоненту* по любым каналам связи, в том числе и открытым;

11.5.3. производит рассылку сформированных обновлений ключей на *Узлы* сети ViPNet, в том числе и скомпрометированному *Абоненту*;

11.5.4. в случае признания факта *Компрометации Закрытого* (секретного) *ключа* подписи *Абонента*, средствами *УКЦ* отзывает (аннулирует) *Сертификат* этого *Абонента*. Производит рассылку *Списка отозванных Сертификатов* всем *Абонентам* сети ViPNet, а также во все взаимодействующие *УЦ*.

11.6. Отозванные *Сертификаты Открытых ключей Пользователя* не удаляются из базы *УКЦ* и хранятся согласно разделу 16 настоящего Регламента для проведения (в случае необходимости) разбора *Конфликтных ситуаций*, связанных с применением *ЭЦП*.

11.7. Информация, содержащаяся на скомпрометированных съемных ключевых носителях, после проведения служебного расследования должна быть уничтожена либо одним из гарантированных способов, например с помощью механизма затирания данных СЗИ Secret Net или альтернативного, либо путем физического уничтожения носителя, с отметкой в Журнале учета выдачи *Ключевых дистрибутивов*.

11.8. В случае признания факта *Компрометации* резервного набора персональных ключей скомпрометированного *Абонента*, для него средствами *УКЦ* создается ключевая дискета с новыми ключами.

11.9. Изготовление нового *Сертификата* и, при необходимости, *Ключевого дистрибутива* происходит согласно процедурам, указанным в разделе 8.

11.10. В случае *Компрометации* ключей *Администратора УЦ Фонда* или его дублёра, считается скомпрометированной вся ключевая информация в корпоративной информационной системе ОМС Хабаровского края, т.е. ключи всех *Абонентов ЗСПД Фонда*. В этом случае должна быть немедленно остановлена работа на симметричных ключах шифрования и оповещены *Администраторы* (*Уполномоченные лица*) взаимодействующих *УЦ*. Для восстановления работы системы электронного документооборота необходимо:

11.10.1. удалить с жесткого диска *УКЦ* все ключи с использованием штатных средств ПО *УКЦ*;

11.10.2. начать формирование ключевой системы с нулевой отметки согласно эксплуатационной документации на ПО *УКЦ*;

11.10.3. до полного развертывания ключевой системы ключевая информация передается *Абонентам* посредством доверенного способа с документальным подтверждением отправки и приема.

12.ОТЗЫВ (АННУЛИРОВАНИЕ) СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

12.1. Отзыв *СКП* производится либо в случае *Компрометации*, либо по заявке *Пользователя – Владельца СКП* или организации, сотрудником которой является (являлся) *Пользователь*.

12.2. Заявление на аннулирование (отзыв) *Сертификата ключа подписи Пользователя* (например при увольнении *Пользователя* – один из видов *Компрометации СКП*) может подать организация, сотрудником которой является (являлся) *Пользователь*. Форма заявления на аннулирование (отзыв) *Сертификата ключа подписи Пользователя УЦ*, направляемого организацией, приведена в Приложении №8 к Регламенту.

12.3. Для осуществления аннулирования (отзыва) своего *Сертификата ключа подписи Пользователь УЦ* лично подает письменное заявление на аннулирование (отзыв) принадлежащего ему *Сертификата ключа подписи* в *УЦ*. Заявление на аннулирование (отзыв) *Сертификата ключа подписи* заверяется собственноручной подписью *Владельца Сертификата* (*Пользователя УЦ*). Форма заявления на аннулирование (отзыв) *Сертификата ключа подписи Пользователя УЦ* приведена в Приложении №9 к Регламенту. *Уполномоченное лицо УЦ* выполняет процедуру идентификации *Пользователя УЦ* путем установления личности по документам, удостоверяющим личность.

12.4. Заявление на аннулирование (отзыв) *Сертификата ключа подписи Пользователя УЦ* рассматривается в течение 1 (одного) рабочего дня с момента поступления. При принятии положительного решения, *Уполномоченное лицо УЦ* выполняет действия по аннулированию (отзыву) *Сертификата ключа подписи Пользователя УЦ* с серийным номером, указанным в заявлении, о чём делается соответствующая отметка в электронном реестре *Копий СКП*.

12.5. Оповещение *Пользователя УЦ* об аннулировании (отзыве) его *Сертификата ключа подписи* производится в течение пяти рабочих дней с момента выполнения *Уполномоченным лицом УЦ* действий по аннулированию (отзыву) *Сертификата ключа подписи Пользователя УЦ* путем отправки электронного письма либо по «Деловой почте», если у *Пользователя* есть другой действующий *Сертификат*, либо на электронный адрес (e-mail), указанный в отозванном *Сертификате.*

12.6. Отозванные *Сертификаты Открытых ключей Пользователя* не удаляются из базы *УКЦ* и хранятся согласно разделу 16 настоящего Регламента для проведения (в случае необходимости) разбора *Конфликтных ситуаций*, связанных с применением *ЭЦП*.

13.ПРИОСТАНОВЛЕНИЕ/ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

13.1. Приостановление действия сертификата ключа подписи:

13.1.1. Для приостановления действия *Сертификата ключа подписи Пользователь УЦ* лично подает заявление на приостановление действия принадлежащего ему *Сертификата ключа подписи*.

13.1.2. Заявление на приостановление действия *Сертификата ключа подписи* заверяется собственноручной подписью *Владельца Сертификата* (*Пользователя УЦ*). Форма заявления на приостановление действия *Сертификата ключа подписи Пользователя УЦ* приведена в Приложении №10 к Регламенту.

13.1.3. *Уполномоченное лицо УЦ* выполняет процедуру идентификации *Пользователя УЦ* путем установления личности *Пользователя УЦ* по документам, удостоверяющим личность.

13.1.4. После положительной идентификации *Пользователя УЦ Уполномоченное лицо УЦ* принимает заявление на приостановление действия *Сертификата ключа подписи Пользователя УЦ*.

13.1.5. Заявление на приостановление действия *Сертификата ключа подписи Пользователя УЦ* рассматривается в течение 1 (одного) рабочего дня с момента поступления. При принятии положительного решения, *Уполномоченное лицо Удостоверяющего Центра* приостанавливает действие *Сертификата ключа подписи Пользователя УЦ* с серийным номером, указанным в заявлении.

13.1.6. Оповещение *Пользователя УЦ* о приостановлении действия его *Сертификата ключа подписи* производится в течение пяти рабочих дней с момента выполнения *Уполномоченным лицом УЦ* действий по приостановлении действия *Сертификата ключа подписи Пользователя УЦ* путем отправки электронного письма либо по «Деловой почте», если у *Пользователя* есть другой действующий *Сертификат*, либо на электронный адрес (e-mail), указанный в отозванном *Сертификате*.

13.1.7. В случае если в течение срока приостановления действия *Сертификата ключа подписи Пользователя УЦ* в *Удостоверяющий Центр* **не поступает заявление** от *Пользователя УЦ* **о возобновлении** действия этого *Сертификата*, ***Сертификат* аннулируется (отзывается)** *Удостоверяющим Центром*.

13.2. Возобновление действия *Сертификата ключа подписи*:

13.2.1. Возобновление действия *Сертификата ключа подписи Пользователя УЦ* возможно только в течение срока, на который было приостановлено действие этого *Сертификата*.

13.2.2. Для осуществления возобновления действия *Сертификата ключа подписи Пользователь УЦ* лично подает заявление на возобновление действия принадлежащего ему *Сертификата ключа*.

13.2.3. Заявление на возобновление действия *Сертификата ключа подписи* заверяется собственноручной подписью *Владельца Сертификата*. Форма заявления на возобновление действия *Сертификата ключа подписи Пользователя УЦ* приведена в Приложении №11 к Регламенту.

13.2.4. *Уполномоченное лицо УЦ* выполняет процедуру идентификации *Пользователя УЦ* путем установления личности *Пользователя УЦ*.

13.2.5. После положительной идентификации *Пользователя УЦ Уполномоченное лицо УЦ* принимает заявление на возобновление действия *Сертификата ключа подписи Пользователя УЦ*.

13.2.6. Заявление на возобновление действия *Сертификата ключа подписи Пользователя УЦ* рассматривается в течение не более 3 (трёх) рабочих дней с момента поступления. При принятии положительного решения, Оператор *Удостоверяющего Центра* выполняет действия по возобновлению действия *Сертификата ключа подписи Пользователя УЦ* с серийным номером, указанным в заявлении.

13.2.7. Оповещение *Пользователя УЦ* о возобновлении действия его *Сертификата ключа подписи* производится в течение пяти рабочих дней с момента выполнения *Уполномоченным лицом Удостоверяющего Центра* действий по возобновлению действия *Сертификата ключа подписи Пользователя УЦ* путем отправки электронного письма либо по «Деловой почте», либо на электронный адрес (e-mail), указанный в *Сертификате*.

14.ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

14.1. Возникновение *Конфликтных ситуаций* может быть связано с формированием, доставкой, получением, подтверждением получения и исполнением *Владельцами СКП Электронных документов*, а также использованием в данных документах *ЭП*.

14.2. Разбор *Конфликтных ситуаций* осуществляется в два этапа. Сначала, путем взаимодействия *Владельца СКП*, у которого возникли претензии, с *Владельцем СКП*, к которому возникли претензии, и *Администратором* или уполномоченным представителем *Удостоверяющего Центра*. В случае если *Владелец СКП* не удовлетворен полученной информацией, для разрешения *Конфликтной ситуации* проводится техническая экспертиза в соответствии с Порядком разрешения *Конфликтных ситуаций* (Приложение №12 к настоящему Регламенту).

15.КОНФИДЕНЦИАЛЬНОСТЬ

15.1. Типы конфиденциальной информации:

Закрытый ключ, соответствующий *Сертификату ключа подписи Пользователя УЦ* является конфиденциальной информацией данного *Пользователя УЦ.*

Персональная и корпоративная информация *Пользователей УЦ*, содержащаяся в *Удостоверяющем Центре*, не подлежащая непосредственной рассылке в качестве части *Сертификата Открытого ключа*, *Списка отозванных Сертификатов*, считается конфиденциальной и не публикуется.

15.2. Типы информации, не являющейся конфиденциальной:

Информация, не являющаяся конфиденциальной, считается открытой.

Информация, содержащаяся в Регламенте, не является конфиденциальной.

Информация, включаемая в *Сертификаты ключей подписи Пользователей УЦ* и *Списки отозванных сертификатов*, издаваемых *Удостоверяющим Центром*, не является конфиденциальной.

Тем не менее, информационный массив, представляющий собой совокупность персональных сведений *Абонентов* (базы данных, Реестр изготовленных *Сертификатов*), подлежит защите в соответствии с режимом, принятым для конфиденциальной информации.

Открытая информация может публиковаться по решению *Удостоверяющего Центра*. Место, способ и время публикации открытой информации определяется *Удостоверяющим Центром*.

15.3. Исключительные полномочия *Удостоверяющего Центра*

Удостоверяющий Центр имеет право предоставлять конфиденциальную информацию третьим лицам только в случаях, определенных в настоящем Регламенте, либо требующих предоставления в соответствии с действующим законодательством или при наличии судебного постановления.

16.ХРАНЕНИЕ ДОКУМЕНТАЦИИ И СЕРТИФИКАТОВ КЛЮЧЕЙ ПОДПИСИ В УДОСТОВЕРЯЮЩЕМ ЦЕНТРЕ

Хранение в *Удостоверяющем Центре Сертификатов ключей подписи Пользователей УЦ* осуществляется в соответствии с порядком ведения (хранения) делопроизводства Фонда.

Архивное хранение

Документы *Удостоверяющего Центра* на бумажных носителях хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Перечень документов *Удостоверяющего Центра*, подлежащих архивному хранению:

- Договоры, соглашения об информационном обмене;
- Заявления о присоединении к Регламенту *Удостоверяющего Центра*;
- Бланк запроса на регистрацию *Пользователя*;
- *Сертификаты ключей подписи*;
- Бумажные *Копии Сертификатов ключей подписи*;
- Заявления на аннулирование (отзыв) *Сертификатов ключей подписи Пользователей УЦ*;
- Заявления на приостановление действия *Сертификатов ключей подписи Пользователей УЦ*;
- Заявления на возобновление действия *Сертификатов ключей подписи Пользователей УЦ*;
- Служебные документы *Удостоверяющего Центра*.

Документы *Удостоверяющего Центра*, подлежащие архивному хранению, являются документами постоянного хранения. Срок хранения архивных документов – 5 (пять) лет после истечения срока действия договора, соглашения.

Выделение архивных документов к уничтожению и их уничтожение осуществляется комиссией, формируемой из числа сотрудников подразделения, в чьём ведении находится *Удостоверяющий Центр*.

Приложение №1 к Регламенту
Удостоверяющего Центра ХКФОМС

Р Е Г Л А М Е Н Т
регистрации и подключения к Удостоверяющему Центру Хабаровского краевого фонда обязательного медицинского страхования пользователей сторонних организаций

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данный Регламент регистрации и подключения к *УЦ Фонда* пользователей сторонних организаций (далее — Регламент) направлен на создание единого пространства доверия *Сертификатов ключей подписей*, изданных доверенными *УЦ*, в целях обеспечения требуемого уровня качества и надежности предоставляемых организациям услуг.

Регламент разработан в соответствии с требованиями действующего Федерального закона от 6 апреля 2011 года № 63 «Об электронной подписи» и является основным руководящим документом для Фонда, выполняющего функции *УЦ*, при подключении *Абонентов* сторонних *УЦ*.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Внешняя организация – юридическое лицо, не входящее в структуру ОМС Хабаровского края, но осуществляющее с ней обмен *Электронными документами* (далее – *ЭД*) в рамках заключенного соглашения об электронном документообороте (далее – ЭДО).

Доверенный способ передачи информации – способ передачи информации, принятый двумя или несколькими юридическими или физическими лицами на основе взаимной договоренности и обеспечивающий требуемую степень её защищенности.

Доверенный Удостоверяющий Центр — УЦ внешней организации, с которой у *УЦ Фонда* установлены *Доверенные отношения* на основании Соглашения об обмене *Электронными документами*.

Доверительные отношения, Установление Доверительных отношений — организационно-техническая процедура, проводимая между двумя *УЦ*, в результате которой *Владельцы СКП*, получившие *Сертификаты* в первом *УЦ*, получают возможность проверить подлинность *ЭП* в *Электронном документе Владельцев СКП*, получивших *Сертификаты* во втором *УЦ*, а также *Владельцев СКП*, получивших *Сертификаты* в некотором третьем *УЦ*, если вторым *УЦ* выпущен *Кросс-сертификат Уполномоченного лица* третьего *УЦ*.

Кросс-сертификат ключа подписи Уполномоченного лица УЦ некоторой третьей организации, не имеющей Соглашения с Учреждением, — это *Сертификат ключа подписи* с *Открытым ключом* этого *Уполномоченного лица*, удостоверенный *ЭП Уполномоченного лица* доверенного УЦ, имеющего

Соглашение с этой третьей организацией, передаваемый в *УЦ Фонда* для обеспечения признания *ЭП*, *Сертификат ключа* которой выдан в *УЦ* этой третьей организации.

Межсетевое взаимодействие между *АРМами [Администратор]*, *Организация Межсетевого взаимодействия* — организационно-техническая процедура, проводимая между двумя организациями, *Защищенные сети* которых построены на основе *Технологии ViPNet*, с целью установления доверительных отношений и объединения взаимодействующих *Узлов* в корпоративную информационную систему. Первоначальная процедура *Организации Межсетевого взаимодействия* между *АРМами [Администратор]* выполняется путем обмена *Доверенным способом* файлами экспорта и межсетевым ключом связи в соответствии с документацией на *ЦУС* и *УКЦ*. С этой целью:

- в *АРМ [Администратор]* одной из сетей формируется межсетевой ключ, а также файлы экспорта для *АРМ [Администратор]* другой сети со списком *Узлов*, которым требуется взаимодействие с *Узлами* другой сети;
- файлы экспорта вместе с паролями доступа к межсетевому ключу связи *Доверенным способом* передаются *Администратору* другой сети, который производит ввод (импорт) данных из полученных файлов экспорта в свой *АРМ [Администратор]* и задание необходимых связей своих *Узлов* с импортированными *Узлами* другой сети. Формируются ответные файлы экспорта;
- ответные файлы экспорта *Доверенным способом* передаются *Администратору* первой сети, где они вводятся в *АРМ [Администратор]*.

В дальнейшем при модификации структуры обеих *Защищенных сетей*, регистрации (удалении) *Абонентских пунктов* и *Абонентов*, изменении связей, выпуске новых *Сертификатов Администраторов*, *Списков отозванных сертификатов* производится автоматическое формирование файлов экспорта с соответствующей информацией и их отправка в другие *АРМ [Администратор]* через установленные с ними защищенные соединения.

На основании полученной информации в *АРМ [Администратор]* каждой из сетей формируется необходимая ключевая и справочная информация для У*злов* своей сети, после рассылки которой между соответствующими Узлами обеих *Защищенных сетей* возможен электронный документооборот.

Удостоверяющий Центр внешней организации — юридическое лицо, обеспечивающее организацию работ *Владельцев СКП* различных организаций с *ЭП* в соответствии с действующим Федеральным законом от 6 апреля 2011 года № 63 «Об электронной подписи».

Файлы экспорта – набор файлов, автоматически формируемых в *АРМ [Администратор]* для каждого другого *АРМ [Администратор]* при организации защищенного *Межсетевого взаимодействия* между *Узлами Защищенных сетей* и при изменениях, происходящих в процессе взаимодействия. В состав файлов экспорта включается:

- информация об *Узлах* сети, которые должны взаимодействовать с другой сетью, и установленных связях этих *Узлов* с *Узлами* другой сети, информация о пользователях, другая информация, необходимая для организации защищенного взаимодействия между *Узлами* сетей;
- *Сертификаты Администраторов* (*Главных абонентов сетей ViPNet*), *Списки отозванных сертификатов*, другая информация, необходимая для организации юридически значимого электронного документооборота.

Электронный документооборот Хабаровского краевого фонда обязательного медицинского страхования (далее – ЭДО Фонда) – принятая в Фонде технология по обмену и работе с *Электронными документами*.

3. УСТАНОВЛЕНИЕ ДОВЕРИТЕЛЬНЫХ ОТНОШЕНИЙ МЕЖДУ УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ХАБАРОВСКОГО КРАЕВОГО ФОНДА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ И УДОСТОВЕРЯЮЩИМ ЦЕНТРОМ ВНЕШНЕЙ ОРГАНИЗАЦИИ

3.1. Установление доверительных отношений между *УЦ Фонда* и *УЦ* внешней организации осуществляется либо напрямую, путем заключения Соглашения об обмене *Электронными документами* или Соглашения о совместных действиях по организации информационного обмена по телекоммуникационным каналам связи между Фондом и внешней организацией (примерный текст Соглашения приведен в Приложении № 2 к Регламенту *Удостоверяющего Центра Хабаровского краевого фонда обязательного медицинского страхования*), либо косвенным образом, путем получения *Кросс-сертификатов* от Доверенных *УЦ*.

3.2. Доверительные отношения могут быть установлены с *Удостоверяющими Центрами*, которые имеют следующий статус:

3.2.1. обладают необходимыми материальными и финансовыми возможностями, позволяющими нести гражданскую ответственность перед *Владельцами Сертификатов ключей подписи* за убытки, которые могут быть понесены ими вследствие недостоверности сведений, содержащихся в *Сертификатах ключей подписи*, а также в результате других виновных действий *УЦ*. Мера ответственности за упомянутые выше убытки должны быть отражены в договорах, заключенных между *УЦ* и *Владельцами СКП*;

3.2.2. имеют необходимые лицензии в соответствии с требованиями действующего законодательства Российской Федерации о лицензировании отдельных видов деятельности;

3.2.3. имеют материально-техническую базу и квалифицированный персонал, позволяющий выполнять следующие функции:

- ♦ обеспечивать эффективную поддержку сервисов информационной безопасности для информационных и телекоммуникационных систем;

- ♦ обеспечивать отсутствие коллизий между своими технологиями и технологиями, применяемыми в Системе юридически значимого ЭДО Фонда (программно-аппаратные средства, протоколы и т.д.);
- ♦ обеспечивать доступность актуальных реестров *Сертификатов ключей подписи Уполномоченных лиц УЦ*, *Списков отозванных Сертификатов ключей подписи*.

3.3. Установлению доверительных отношений на основании Соглашения предшествует процедура с многоступенчатым процессом, направленным на достижение взаимных доверительных отношений и включает следующие стадии:

- заявительная стадия;
- стадия рассмотрения заявления;
- оформление договорных отношений.

Инициатором доверительных отношений может выступать как Фонд, так и внешняя организация, с которой устанавливаются доверительные взаимоотношения.

3.4. **Заявительная стадия:** одна из организаций — Владелец *УЦ* (Инициатор), претендующая на установление доверительных отношений с другой организацией – владельцем второго *УЦ* (Реципие́нтом), направляет в адрес Реципиента комплект заявительных документов, подтверждающих выполнение Инициатором условий для Доверенных *УЦ*.

3.5. **Стадия рассмотрения заявления.** Реципиент проводит анализ документов, представленных Претендентом, оценку материально-технической базы Инициатора, а также, при необходимости, запрашивает дополнительные документы. При необходимости проводятся тестовые испытания по согласованной с организацией-разработчиком ПО ViPNet (ОАО «ИнфоТеКС») методике, которые должны подтвердить возможность функционирования технологического оборудования и программного обеспечения Инициатора и Реципиента в системе ЭДО обоих Учреждений. Реципиент и Инициатор совместно принимают решение о возможности или невозможности установления *Межсетевого взаимодействия* или *Кросс-сертификации*.

3.6. **Оформление договорных отношений**. После принятия положительного заключения о возможности установления *Межсетевого взаимодействия* или *Кросс-сертификации*, Реципиент заключает с Инициатором Соглашение об обмене *Электронными документами* или Соглашение о совместных действиях по организации информационного обмена.

3.7. После оформления договорных отношений происходит техническая процедура установления *Межсетевого взаимодействия*.

Если внешняя организация использует *УЦ* ViPNet, то между *АРМами [Администратор]* устанавливается стандартное *Межсетевое взаимодействие* сетей ViPNet.

Если внешняя организация использует сервисы *ЭП* на базе технологии, отличной от ViPNet, и при этом *УЦ*, в котором изданы *СКП* сотрудников внешней организации, не имеет доверительных отношений с *УЦ Фонда*, то выполняется процедура установления доверительных отношений напрямую или путем получения *Кросс-сертификата* от доверенного *УЦ*. При установлении прямых отношений на основании Соглашения вся цепочка *Сертификатов ключей* подписи участника ЭДО от внешних организаций, участвующих в заверении *ЭП*, и *Список отозванных сертификатов УЦ* внешней организации должны быть импортированы в *УЦ Фонда*, а *Сертификаты Администраторов* и *Список отозванных сертификатов УЦ Фонда* должны быть переданы во внешний *УЦ*, обслуживающий эту внешнюю организацию.

4. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С УДОСТОВЕРЯЮЩИМИ ЦЕНТРАМИ ПРИ ИЗМЕНЕНИИ СТРУКТУРЫ СЕТИ ОБМЕНА ЭД, ФОРМИРОВАНИИ НОВЫХ СПИСКОВ ОТОЗВАННЫХ СЕРТИФИКАТОВ, ПРИ СМЕНЕ КЛЮЧЕЙ ПОДПИСИ АДМИНИСТРАТОРОВ

4.1. Если внешняя организация использует *УЦ* ViPNet: при организации взаимодействия с новыми *АП* той или другой Стороны (изменение структуры сети), при изменении *Списка отозванных сертификатов*, ключей подписи *Уполномоченных лиц*, обмен файлами экспорта, содержащими всю необходимую информацию, производится через установленный защищенный канал между *АРМами [Администратор]*.

На основании полученной информации в *АРМ [Администратор]* обеих Сторон формируется необходимая ключевая и адресная информация для *Узлов* своей сети, после рассылки которой между соответствующими *Узлами* обеих *Защищенных сетей* возможен ЭДО.

4.2. Если внешняя организация использует сервисы *ЭП* на базе технологии, отличной от ViPNet: каждый раз при организации взаимодействия с новыми *АП* той или другой Стороны (изменение структуры сети), при изменении *Списка отозванных сертификатов*, ключей подписи *Уполномоченных лиц*, вся цепочка *Сертификатов ключей подписи* участника ЭДО от внешних организаций, участвующих в заверении *ЭП*, и *Список отозванных сертификатов УЦ* внешней организации должны быть импортированы в *УЦ Фонда*, а *Сертификаты Администраторов* и *Список отозванных сертификатов УЦ Фонда* должны быть переданы во внешний *УЦ*, обслуживающий эту внешнюю организацию.

4.3. *Уполномоченные лица УЦ* обязаны производить периодическую (*Плановую*) замену своих ключей подписи не реже срока действия ключа подписи, задаваемого в ПО *УКЦ*. ПО *УКЦ* заблаговременно информирует о необходимости проведения данной процедуры. При появлении такого предупреждения *Уполномоченное лицо УЦ* в соответствии с эксплуатационной документацией ПО *УКЦ* формирует новые ключи подписи и *Сертификат ключа подписи* и рассылает их на взаимодействующие *УЦ*.

4.4. В случае *Компрометации* своих ключей подписи *Уполномоченное лицо* немедленно сообщает об этом во взаимодействующие *УЦ*, аннулирует свой *Сертификат ключа подписи* и отправляет файлы экспорта с новым *Список отозванных сертификатов* во все взаимодействующие сети, формирует новые ключи подписи и *Сертификат ключа подписи*.

Приложение №2 к Регламенту
Удостоверяющего Центра ХК ФОМС

С О Г Л А Ш Е Н И Е
об обмене электронными документами

г. Хабаровск «___»_____201__г.

_____ _____
г. Хабаровска в лице _____ действующего на основании _____*(распоряжения, постановления, приказа или другое)* с одной стороны, и Хабаровский краевой фонд обязательного медицинского страхования, в лице директора Пузаковой Елены Викторовны, действующего на основании распоряжения Губернатора Хабаровского края от 14.09.2012 г. №142-рк, с другой стороны, совместно именуемые Стороны, заключили настоящее Соглашение о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. Стороны договорились о совместных действиях по организации и функционированию системы защищенного электронного документооборота по телекоммуникационным каналам связи (далее – Системы) между пользователями Сторон (далее – Абонентами), подключенными к соответствующим *Удостоверяющим Центрам*.

1.2. Отношения между участниками информационного обмена регулируются действующими: Гражданским кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральным законом «Об обязательном медицинском страховании в Российской Федерации» от 29 ноября 2017 г. № 326-ФЗ, Приказом Министерства здравоохранения и социального развития Российской Федерации «Об утверждении порядка ведения персонифицированного учета в сфере обязательного медицинского страхования» от 25 января 2011 г. №29н, Федеральным законом от 6 апреля 2011 года № 63 «Об электронной подписи», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» и иными Федеральными законами, нормативными правовыми актами.

1.3. Абоненты, подключенные к Системе, осуществляют обмен документов, содержащих конфиденциальную информацию (персональные данные), в электронном виде по защищенным телекоммуникационным каналам связи.

1.4. Стороны обеспечивают возможность обмениваться документами в электронном виде Абонентам, подключенным к Системе, и предоставляют следующие услуги:

- услуги *Удостоверяющего Центра*, определенные действующим Федеральным законом от 6 апреля 2011 года № 63 «Об электронной подписи»;
- обеспечение ключевой информацией, для защищенного электронного документооборота;

- обеспечение *Сертификатами ключа Электронной подписи* (далее – *ЭП*);
- предоставление транспортного сервиса при информационном обмене в Системе.

Права Сторон на оказание услуг подтверждаются копиями соответствующих лицензий области шифрования и криптографии.

2. ОПЛАТА СОГЛАШЕНИЯ

2.1. Соглашение является безвозмездным.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. При организации информационного обмена в рамках Системы Стороны принимают на себя следующие права и обязанности:

- соблюдение требований Российского законодательства в области обеспечения безопасности информации;
- обеспечение поддержания в работоспособном состоянии аппаратных и программных средств Сторон, необходимых для передачи и приема документов в электронном виде по телекоммуникационным каналам связи;
- обеспечение поддержания работоспособности телекоммуникационных средств Системы в границах своей зоны ответственности;
- обеспечение установки и сопровождения *средств криптографической защиты (далее – СКЗИ)* у Абонентов соответствующих Сторон;
- соблюдение требований порядка ведения персонифицированного учета в сфере обязательного медицинского страхования, утвержденного приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 N 29н "Об утверждении Порядка ведения персонифицированного учета в сфере обязательного медицинского страхования" (зарегистрирован Министерством юстиции Российской Федерации 08.02.2011, регистрационный N 19742), в том числе наличие приказа, определяющего работников страховой медицинской организации, допущенных к работе с региональным сегментом единого регистра застрахованных лиц, соблюдение сроков передачи данных о застрахованных лицах и сведений об изменениях в этих данных в территориальный фонд, достоверность сведений, внесенных страховой медицинской организацией в региональный сегмент единого регистра застрахованных лиц;
- определение работников, допущенных к работе с данными персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, и обеспечивающих их конфиденциальность в соответствии с установленными законодательством Российской Федерации требованиями по защите персональных данных;

- обеспечение безопасности хранения, обработки, проверки достоверности данных и их передачи по каналам связи с использованием СКЗИ в рамках Системы.

3.2. При организации информационного обмена в рамках Системы, стороны обмениваются необходимыми информационно-техническими материалами, в том числе сертификатами закрытого и открытого ключей. Передача дистрибутивного набора ключевой информации может производиться лично сотруднику – инициатору обмена или по каналам общего пользования «Интернет». Получателем дистрибутивного набора ключевой информации должен являться сотрудник организации-инициатора информационного обмена, имеющий право на получение. Передача дистрибутивного набора ключевой информации по сети «Интернет» возможна только с использованием средств криптографической защиты информации. При этом, после получения указанного дистрибутива сторона – инициатор информационного обмена направляет в адрес Хабаровского краевого фонда обязательного медицинского страхования уведомление о получении дистрибутива. Уведомление составляется в произвольной форме, с указанием даты получения дистрибутива, наименования файла-ключа (*.dst) и места его установки (адрес). Уведомление подписывается лицом, ответственным за организацию работ по СКЗИ и утверждается руководителем организации.

3.3. В соответствии с Федеральным законом от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании», для выполнения требований приказа от 25.01.2011 г. № 29н «Об утверждении порядка ведения персонифицированного учета в сфере обязательного медицинского страхования», в части обеспечения безопасности персональных данных застрахованных лиц, Хабаровский краевой фонд обязательного медицинского страхования оставляет за собой право внепланового проведения контроля автоматизированных рабочих мест, обрабатывающих сведения персонифицированного учета застрахованных лиц, в целях проверки соблюдения требований по безопасности информации при обработке персональных данных и их передачи по каналам связи с использованием средств криптографической защиты.

4. ГРАНИЦЫ ЗОНЫ ОТВЕТСТВЕННОСТИ СТОРОН

4.1. Стороны несут ответственность за работоспособность телекоммуникационного оборудования и выполнение требований законодательства РФ, а также условий настоящего Соглашения, в своей зоне ответственности, в т.ч.:

- работоспособность транспортных серверов Сторон;
- регистрацию Абонентов на серверах Сторон и обеспечение *Сертификатами ключей ЭП*;
- техническую поддержку Абонентов;
- администрирование внутренних сетевых ресурсов.

5. ПРОВЕДЕНИЕ ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ

5.1. Проведение профилактических мероприятий по поддержанию

работоспособности телекоммуникационных средств в границах своей зоны ответственности стороны обязаны осуществлять не чаще 1 раза в месяц при соблюдении следующих условий:

- срок проведения профилактических мероприятий не должен превышать 1 (одни) сутки;
- профилактические мероприятия, как правило, должны проводиться в пределах первых 10 (десяти) календарных дней месяца;

5.2. Стороны обязаны заблаговременно, не позднее чем за 7 (семь) дней до дня проведения профилактических мероприятий какой-либо из сторон, оповестить о сроках проведения профилактических мероприятий Абонентов.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Стороны несут ответственность за использование информации в соответствии с законодательством Российской Федерации.

6.2. В случае выявления нарушений требований по обеспечению безопасности персональных данных, нарушений порядка ведения персонифицированного учета в сфере обязательного медицинского страхования, а также при передаче конфиденциальной информации по каналам связи с использованием средств криптографической защиты информации принимается решение об аннулировании сертификата ключа подписи и ограничении доступа к информационным ресурсам ХКФОМС посредством канала связи сети VipNet до устранения нарушений.

6.2. Стороны самостоятельно несут ответственность в соответствии с законодательством Российской Федерации перед Абонентами с которыми имеют договорные отношения.

7. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ И СПОРОВ

7.1. Возникновение *Конфликтных ситуаций* в процессе электронного документооборота:

7.1.1. Возникновение *Конфликтных ситуаций* может быть связано с формированием, доставкой, получением, подтверждением получения *Электронного документа* (далее – *ЭД*), а также использованием в данных документах *ЭП*. *Конфликтные ситуации* могут возникать в следующих случаях:

не подтверждение подлинности защищенных *Электронных документов* средствами проверки *ЭП* получателя;

- оспаривание факта идентификации *Владельца ЭП*, подписавшего *ЭД*;
- заявление отправителя или получателя *ЭД* об его искажении;
- оспаривание факта отправления и (или) получения защищенного *ЭД*;
- оспаривания времени отправления и (или) получения защищенного *ЭД*;
- иные случаи возникновения *Конфликтных ситуаций*.

7.1.2. Разбор *Конфликтных ситуаций* осуществляется в два этапа. На первом этапе Абонент Стороны, у которой возникли претензии, взаимодействует с *Администратором безопасности* своего *Удостоверяющего Центра*. На втором этапе, в случае если Абонент не удовлетворен полученной информацией, для разрешения *Конфликтной ситуации* Стороны

взаимодействуют между собой.

7.1.3. *Конфликтные ситуации* разрешаются (урегулируются) Сторонами в рабочем порядке и/или по итогам работы Экспертной комиссии.

7.1.4. В случае невозможности разрешения *Конфликтной ситуации* в рабочем порядке и по итогам работы Экспертной комиссии, стороны разрешают *Конфликтную ситуацию* в судебном порядке, в соответствии с законодательством Российской Федерации.

7.2. Уведомление о *Конфликтной ситуации*:

7.2.1. В случае возникновения обстоятельств, свидетельствующих, по мнению одной из Сторон, о возникновении и/или наличии *Конфликтной ситуации*, данная Сторона (далее – Сторона-инициатор) незамедлительно извещает другую заинтересованную Сторону о возможном возникновении и/или наличии *Конфликтной ситуации*, обстоятельствах, свидетельствующих о ее возникновении или наличии, а также ее предполагаемых причинах.

7.2.2. Сторона, которой было направлено извещение о *Конфликтной ситуации* и участвующая в ее разрешении (далее – Сторона-ответчик), обязана в течении двух рабочих дней, следующих за днем поступления извещения, проверить наличие указанных в извещении обстоятельств, и по необходимости, принять меры по разрешению *Конфликтной ситуации* со своей стороны.

7.2.3. В тот же срок Сторона-ответчик извещает доступными способами сторону-инициатора о результатах проверки и, при необходимости, о мерах, принятых для разрешения *Конфликтной ситуации*.

7.3. Разрешение *Конфликтной ситуации* в рабочем порядке:

7.3.1. *Конфликтная ситуация* признается разрешенной в рабочем порядке в случае, если Сторона-инициатор удовлетворена информацией, полученной в извещениях Стороны-ответчика, и не имеет к ней претензий в связи с *Конфликтной ситуацией*.

7.3.2. В случае если Сторона-инициатор не удовлетворена информацией, полученной от Стороны-ответчика, для рассмотрения *Конфликтной ситуации* формируется Экспертная комиссия.

7.4. Предложение по формированию экспертной комиссии по разрешению *Конфликтной ситуации*:

7.4.1. В случае, если *Конфликтная ситуация* не была разрешена в рабочем порядке, Сторона-инициатор, должна не позднее чем в течение трех рабочих дней после возникновения *Конфликтной ситуации*, направить уведомление о *Конфликтной ситуации* (далее – Уведомление) и предложение о создании Экспертной комиссии по разрешению *Конфликтной ситуации* (далее – Предложение) Стороне-ответчику.

7.4.2. Уведомление должно содержать информацию о предмете и существе *Конфликтной ситуации*, обстоятельствах, по мнению Стороны-инициатора, свидетельствующих о наличии *Конфликтной ситуации*, возможных причинах и последствиях ее возникновения.

7.4.3. Уведомление должно содержать информацию, с указанием фамилий, имен, отчеств, должностей и контактной информации, должностных лиц Стороны-инициатора, уполномоченных в разрешении *Конфликтной ситуации*.

7.4.4. Предложение должно содержать информацию о предлагаемом месте, дате и времени сбора Экспертной комиссии, список предлагаемых для

участия в работе Экспертной комиссии представителей Стороны-инициатора с указанием фамилий, имен, отчеств, должностей, при необходимости исполняемых при обмене *Электронными документами* функциональных ролей (администратор, администратор безопасности и т.п.), их контактной информации (телефон, факс, электронная почта).

7.4.5. Уведомление и Предложение составляются на бумажном носителе, подписываются должностными лицами Стороны-инициатора, уполномоченными в разрешении *Конфликтной ситуации* и передаются Стороне-ответчику в установленном порядке, обеспечивающим подтверждение вручения корреспонденции.

7.4.6. Уведомление и Предложение могут быть составлены и направлены в форме *Электронного документа*. При этом факт их доставки должен быть подтвержден.

7.5. Формирование экспертной комиссии по разрешению *Конфликтной ситуации,* ее состав:

7.5.1. Не позднее, чем на третий рабочий день после получения Предложения, Сторонами, участвующими в разрешении *Конфликтной ситуации*, должна быть сформирована Экспертная комиссия.

7.5.2. Экспертная комиссия формируется на основании писем Сторон и оформляется совместным приказом. В приказе определяется состав Экспертной комиссии, время и место ее работы.

7.5.3. Устанавливается тридцатидневный срок работы Экспертной комиссии. В исключительных случаях срок работы Экспертной комиссии по согласованию Сторон может быть дополнительно продлен не более чем на тридцать дней.

7.5.4. Если Стороны не договорятся об ином, в состав Экспертной комиссии входит равное количество уполномоченных лиц каждой из Сторон, участвующих в разрешении *Конфликтной ситуации*.

7.5.5. В состав Экспертной комиссии назначаются представители служб информационно-технического обеспечения, служб обеспечения информационной безопасности, уполномоченный представитель *Удостоверяющего Центра* (далее – *УЦ*), а также представители подразделений – исполнителей *Электронного документа*.

7.5.6. По инициативе любой из сторон к работе Экспертной комиссии, для проведения технической экспертизы, могут привлекаться независимые эксперты, в том числе представители поставщиков средств защиты информации. При этом Сторона, привлекающая независимых экспертов, самостоятельно решает вопрос об оплате экспертных услуг.

7.5.7. Лица, входящие в состав Экспертной комиссии, должны обладать необходимыми знаниями и опытом работы в области подготовки и исполнения *Электронных документов*, построения и функционирования Системы, организации и обеспечения информационной безопасности при обмене *Электронными документами*, должны иметь соответствующий допуск к необходимым для проведения работы Экспертной комиссии документальным материалам и программно-техническим средствам.

7.5.8. При участии в Экспертной комиссии представителей сторонних органов и организаций, их право представлять соответствующие органы и организации должно подтверждаться официальным документом

(доверенностью, предписанием, копией приказа или распоряжения).

7.6. Права и полномочия экспертной комиссии по разрешению *Конфликтной ситуации*:

Экспертная комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам Сторон, на бумажных и электронных носителях;
- проводить ознакомление с условиями и порядком подготовки, формирования, обработки, доставки, исполнения, хранения и учета *Электронных документов*;
- проводить ознакомление с условиями и порядком эксплуатации Сторонами программно-технических средств обмена *Электронными документами*;
- проводить ознакомление с условиями и порядком изготовления, использования и хранения Сторонами ключевой информации, а также иной конфиденциальной информации и ее носителей, необходимых для работы Экспертной комиссии;
- получать объяснения от должностных лиц Сторон, обеспечивающих обмен *Электронными документами*;
- получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой *Конфликтной ситуации*.

7.7. Работа экспертной комиссии по разрешению *Конфликтной ситуации*:

7.7.1. В случае если представители одной из Сторон по оспариваемому *Электронному документу* не явились для участия в экспертной комиссии, экспертиза проводится без их участия, а об отсутствии представителей по оспариваемому *Электронному документу* составляется акт, подписываемый всеми присутствующими участниками экспертной комиссии.

7.7.2. Экспертиза оспариваемого *Электронного документа* проводится на программно-аппаратной базе *УЦ*, обеспечивающего проверку *Электронного документа*, авторство или содержание которого оспаривается.

7.7.3. *Сертификат ключа подписи* признается изданным *УЦ*, если *Подтверждена подлинность Электронной подписи* издателя *Сертификата ключа подписи* с использованием *Сертификата ключа подписи Уполномоченного лица УЦ*.

7.7.4. *Электронная подпись* в *Электронном документе* равнозначна собственноручной подписи *Владельца Сертификата ключа подписи* при одновременном соблюдении следующих условий:

- *Сертификат ключа подписи*, соответствующий *Электронной подписи*, издан соответствующим *Удостоверяющим Центром*;
- серийный номер *Сертификата ключа подписи*, относящийся к этой *Электронной подписи*, не содержится в актуальном *Списке отозванных сертификатов* на момент подписания *Электронного документа*;
- срок действия *Сертификата ключа подписи*, относящегося к этой *Электронной подписи*, наступил и не окончен на момент подписания *Электронного документа*;

- положительный результат проверки с использованием средства *Электронной подписи* на предмет отсутствия искажений в подписанном данной *Электронной подписью Электронном документе*;
- *Электронная подпись* используется в соответствии со сведениями, указанными в *Сертификате ключа подписи*.

7.7.5. Все мероприятия Экспертной комиссии по проверке с применением аппаратно-программных средств должны протоколироваться. Протоколы прилагаются к акту работы комиссии.

7.8. Оформление результатов работы экспертной комиссии по разрешению *Конфликтной ситуации*:

7.8.1. По итогам работы Экспертной комиссии составляется акт, при этом акт должен содержать следующую информацию:

- состав Экспертной комиссии;
- дату и место составления акта;
- даты и время начала и окончания работы Комиссией;
- фактические обстоятельства, установленные Комиссией;
- краткий перечень мероприятий, проведенных Комиссией;
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
- подписи членов Экспертной комиссии;

7.8.2. К Акту может прилагаться особое мнение члена или членов Экспертной комиссии, не согласных с выводами Экспертной комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Экспертной комиссии, чье мнение оно отражает.

7.8.3. Акт составляется в форме документа на бумажном носителе, по одному экземпляру каждой Стороне. По обращению любого из членов Экспертной комиссии, Стороной, к которой было направлено обращение, ему должна быть выдана заверенная копия Акта.

7.8.4. Акт Экспертной комиссии является основанием для принятия Сторонами решения по урегулированию *Конфликтной ситуации*.

8. СРОКИ ДЕЙСТВИЯ СОГЛАШЕНИЯ

8.1. Настоящее Соглашение вступает в силу с момента его подписания и действует в течение одного года с момента подписания.

8.2. Действие настоящего Соглашения автоматически продлевается на следующий календарный год, если ни одна из сторон не заявит о его прекращении не позднее, чем за месяц до истечения строка действия настоящего Соглашения.

8.3. Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию сторон либо в одностороннем порядке с предупреждением другой стороны не позднее, чем за два месяца до расторжения Соглашения.

9. ФОРС МАЖОР

9.1. При возникновении обстоятельств, которые делают полностью или

частично невозможным выполнение настоящего Соглашения одной из сторон, таких как: стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

9.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую сторону в течение трех рабочих дней.

9.3. Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

10. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

10.1. В случае возникновения споров и разногласий Стороны приложат все усилия, чтобы устранить их путём переговоров.

10.2. Стороны признают, что факт доставки *Электронного документа* между участниками документооборота подтверждается квитанциями о доставке.

10.3. Переговорный порядок урегулирования споров и разногласий не исключает права каждой из Сторон на обращение в Арбитражный суд.

10.4. Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

10.5. Соглашение составлено в 2-х (двух) экземплярах, имеющих одинаковую юридическую силу – по одному для каждой из Сторон.

11. АДРЕСА И РЕКВИЗИТЫ СТОРОН

Краевое государственное бюджетное учреждение здравоохранения
«Городская поликлиника»
680000 г. Хабаровск,
ул. Ленина, д.00
Телефон: (4212) 00-00-00
Тел./Факс: (4212) 00-00-00

Главный врач _____
_____/_____
м.п.

Хабаровский краевой фонд
обязательного медицинского
страхования
680000, г. Хабаровск,
ул. Фрунзе, д.69
Телефон: (4212) 97-03-00
Тел./Факс: (4212) 32-92-45
Директор ХК ФОМС
_____ / Е.В. Пузакова
м.п.

Приложение №3 к Регламенту
Удостоверяющего Центра ХКФОМС

Директору ХКФОМС

_____

_____ _____

О присоединении к Регламенту
Удостоверяющего Центра
ХКФОМС

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

1. Присоединяется к Регламенту Удостоверяющего Центра Хабаровского краевого фонда обязательного медицинского страхования (далее – Регламент) и становится Стороной Регламента с момента получения Хабаровским краевым фондом ОМС настоящего заявления.

2. Соглашается с тем, что изменения в Регламент вносятся в одностороннем порядке Хабаровским краевым фондом ОМС.

_____ _____ / _____ /
должность, наименование организации подпись Ф.И.О.

«____» _____ 20___ г.

М.П.

Приложение №4 к Регламенту
Удостоверяющего Центра ХКФОМС

Удостоверяющий Центр
Хабаровского краевого ФОМС

Запрос на регистрацию пользователя

_____, в лице _____
действующего на основании _____, просит зарегистрировать своего сотрудника Пользователем УЦ ХКФОМС в соответствии с указанными в настоящем запросе данными:

Фамилия Имя Отчество		
ИНН		
СНИЛС		
Должность		
Подразделение		
Полное наименование организации		
Почтовый адрес организации (подразделения)		
Адрес электронной почты		
Область:	Хабаровский край	
Страна:	**RU**	
Версия	**V3**	
Алгоритм подписи	**ГОСТ Р 34.10/34.11-2001**	
Программа применения ЭП	**ViPNet Custom версии 4.3 (или новее)**	
Использование	**Проверка подлинности клиента** **Защищенная электронная почта** **Подписывание документа**	**(1.3.6.1.5.5.7.3.2)** **(1.3.6.1.5.5.7.3.4)** **(1.3.6.1.4.1.311.10.3.12)**

В соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяюсь к Регламенту Удостоверяющего Центра Хабаровского краевого ФОМС в качестве Пользователя. С Регламентом Удостоверяющего Центра Хабаровского краевого ФОМС и приложениями к нему ознакомлен(а) и обязуюсь соблюдать все положения указанного документа. Соглашаюсь с обработкой своих персональных данных Удостоверяющим Центром и признаю, что персональные данные, заносимые в Сертификаты ключей подписи, относятся к общедоступным персональным данным.

Подтверждаю, что пароль, соответствующий Закрытому ключу ЭП, будет известен только мне и не будет передаваться в какой-либо форме другим лицам.

Признаю, что ЭП Электронного документа, корректность которого подтверждается при проверке с помощью соответствующего Открытого ключа, равнозначна моей собственноручной подписи, а Электронные документы, подписанные такой ЭП, порождают с моей стороны обязательства равные обязательствам по документам аналогичного содержания на бумажном носителе, заверенным моей собственноручной подписью.

Пользователь УЦ ХКФОМС: _____ / / «___» _____ 20__г.	Заверяю подпись Пользователя УЦ ХКФОМС Руководитель _____ / / «___» _____ 20__г. *М.П.*

Настоящим подтверждаю, что Запрос на регистрацию получен.

Уполномоченное лицо УЦ ХКФОМС:
_____ / /
«___» _____ 20__г.

Приложение №5 к Регламенту
Удостоверяющего Центра ХКФОМС

ЖУРНАЛ
учета выдачи ключевых дистрибутивов

(левая сторона, четная страница)

Дата	Подразделение, организация	Должность, ФИО Абонента	Тип носителя	Отметка о выдаче резервного набора персональных ключей
1	2	3	4	5

(правая сторона, нечетная страница)

Способ передачи (установка администратором, лично в руки, нарочным в адрес…)	Подпись администратора, выдавшего дистрибутив	Подпись Абонента (отметка о доставке или установке)	Отметка о возврате и уничтожении дистрибутива	Подпись администратора об уничтожении
6	7	8	9	10

Приложение №6 к Регламенту
Удостоверяющего Центра ХКФОМС

Удостоверяющий Центр Хабаровского краевого фонда ОМС

Сертификат ключа проверки электронной подписи

Кому выдан: Петров Петр Петрович
Кем выдан: Абдрахманов Алексей Зуфарович
Действителен с 1 августа 2017 г. по 1 сентября 2018 г.

Версия:	V3
Серийный номер:	01 D2 AD C1 BA DD B0 F0 00 00 3A F5 02 6C 01 0E
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Почтовый адрес: 680000, г.Хабаровск, ул.Фрунзе, д.69 Имя: Абдрахманов Алексей Зуфарович Должность: Администратор Подразделение: Удостоверяющий и Ключевой центр Организация: ТФОМС, Хабаровский край Электронная почта: dis@khfoms.ru Город: Хабаровск Страна: RU Адрес, улица: 680000, г.Хабаровск, ул.Фрунзе, д.69
Действителен с:	1 августа 2017 г. 14:04:00 (GMT+10:00)
Действителен по:	1 сентября 2018 г. 14:04:00 (GMT+10:00)
Субъект:	Отчество: Петрович Фамилия: Петров Петр Адрес, улица: 680000, г.Хабаровск, ул.Ленина, д.120 Страна: RU Город: Хабаровск ИНН: 272829303132 Подразделение: отдел программного обеспечения Должность: ведущий специалист Имя: Петров Петр Петрович Организация: КГБУЗ РБ СНИЛС: 01234546789
Открытый ключ:	ГОСТ Р 34.10-2012/512 (512 бит) 04 40 D6 43 57 85 C2 FD 8D E2 9E 21 77 39 DA C7 F8 2A 06 5D 88 FA ED 12 EA 31 23 40 F7 BE 1F 98 84 B8 D6 FB EB 5F 31 28 67 55 68 86 5B 96 E4 FC F4 5B 29 FC 2E DA AD 0A F0 06 7A 7C 12 FF 1D CA C7 DD
Расширения сертификата X.509 Использование ключа:	Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Подписывание документа (1.3.6.1.4.1.311.10.3.12)
Доступ к информации о центрах сертификации:	[1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=ftp://192.168.1.81/Issuers
Точки распространения списков отзыва (CRL):	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=ftp://192.168.1.81/CDP
Идентификатор ключа центра сертификатов:	Идентификатор ключа=A8 C5 C7 D0 45 C9 33 10 0E F2 9B D9 AC E0 2B C4 00 82 51 09
Срок действия закрытого ключа:	С 1 августа 2017 г. 14:04:00 (GMT+10:00) по 1 августа 2018 г. 14:04:00 (GMT+10:00)
Идентификатор ключа :	95 93 02 0D 46 7B 08 4D F6 9B 78 68 83 C6 7E 09 F1 C5 28 9A
Основные ограничения:	Тип субъекта=Пользователь
Результат проверки сертификата	Сертификат действителен. Проверен 1 августа 2017 г. 15:04:35 (GMT+10:00).

Владелец ЭЦП (Пользователь) _____/_____
подпись ФИО

Администратор УЦ _____ /_____/
подпись ФИО

М.П.

Приложение №7 к Регламенту
Удостоверяющего Центра ХКФОМС

Р Е Е С Т Р
копий сертификатов ключей подписи на бумажных носителях, изданных Удостоверяющим Центром Хабаровского краевого ФОМС

(левая сторона, чётная страница)

№ п/п	Дата издания	Основание для издания	Владелец сертификата ключа пользователя		Срок действия сертификата ключа подписи	
			фамилия, имя, отчество	должность, структурное подразделение	действи-телен с	действи-телен по
1	2	3	4	5	6	7

(правая сторона, нечетная страница)

Серийный номер сертификата ключа подписи	Издатель	Отметка об отзыве (аннулировании), дата отзыва	Основание для отзыва	Примечание
8	9	10	11	12

Приложение №8 к Регламенту
Удостоверяющего Центра ХКФОМС

Директору ХКФОМС

_____

_____ _____

Об отзыве Сертификата ключа подписи

В соответствии с Регламентом Удостоверяющего Центра Хабаровского краевого ФОМС,

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____
(должность)

_____,
(фамилия, имя, отчество)

действующего на основании _____,

в связи с _____,
(причина отзыва сертификата)

просит аннулировать (отозвать) Сертификат ключа подписи своего сотрудника – Пользователя Удостоверяющего Центра Хабаровского краевого ФОМС

_____
(фамилия, имя, отчество)

содержащий следующие данные:

Фамилия Имя Отчество	
ИНН	
СНИЛС	
Должность	
Подразделение	
Полное наименование организации	
Почтовый адрес организации (подразделения)	
Адрес электронной почты (e-mail)	
Область	
Страна	**RU**

_____ _____ / _____ /
должность, наименование организации подпись Ф.И.О.

«____» _____ 20___ г.

М.П.

Приложение №9 к Регламенту
Удостоверяющего Центра ХКФОМС

ЗАЯВЛЕНИЕ НА АННУЛИРОВАНИЕ (ОТЗЫВ)
СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

Прошу аннулировать (отозвать) Сертификат ключа подписи,
серийный номер: _____,
выданный на имя _____
(ФИО владельца сертификата)

в связи с _____
(причина аннулирования (отзыва) сертификата ключа подписи: компрометация закрытого ключа, прекращение работы и т.д.).

_____
_____

Владелец Сертификата ключа подписи:

_____ / /

«___» _____ 20__г.

Настоящим подтверждаю, что Заявление на аннулирование (отзыв) Сертификата ключа подписи получено, сведения указанные в Заявлении, проверены.

Уполномоченное лицо УЦ Хабарвоского краевого ФОМС:

_____ / /

«___» _____ 20__г.

Приложение №10 к Регламенту
Удостоверяющего Центра ХКФОМС

ЗАЯВЛЕНИЕ НА ПРИОСТАНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

Прошу приостановить действие Сертификата ключа подписи,
серийный номер: _____,
выданный на имя _____
(ФИО владельца сертификата)
в связи с _____
(причина приостановления действия сертификата ключа подписи)
_____
_____

Срок приостановления действия Сертификата ключа подписи:
с «___» _____ 20__г. по «___» _____ 20__г. включительно.

Владелец Сертификата ключа подписи:

_____ / /

«___» _____ 20__г.

Настоящим подтверждаю, что Заявление на приостановление действия Сертификата ключа подписи получено, сведения указанные в Заявлении, проверены.

Уполномоченное лицо УЦ Хабаровского краевого ФОМС:

_____ / /

«___» _____ 20__г.

Приложение №11 к Регламенту
Удостоверяющего Центра ХКФОМС

ЗАЯВЛЕНИЕ НА ВОЗОБНОВЛЕНИЕ ДЕЙСТВИЯ СЕРТИФИКАТА КЛЮЧА ПОДПИСИ

Прошу возобновить действие Сертификата ключа подписи,
серийный номер: _____,
выданный на имя _____
(ФИО владельца сертификата)

Владелец Сертификата ключа подписи:

_____ / /

«___» _____ 20__г.

Настоящим подтверждаю, что Заявление на возобновление действия Сертификата ключа подписи получено, сведения указанные в Заявлении, проверены.

Уполномоченное лицо УЦ Хабаровского краевого ФОМС:

_____ / /

«___» _____ 20__г.

Приложение №12 к Регламенту
Удостоверяющего Центра ХКФОМС

П О Р Я Д О К
разрешения конфликтных ситуаций

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Возникновение *Конфликтных ситуаций* может быть связано с формированием, доставкой, получением, подтверждением получения и исполнением *Владельцами СКП УЦ ХКФОМС Электронных документов*, а также использованием в данных документах *ЭП*.

1.2. Разбор *Конфликтных ситуаций* осуществляется в два этапа. Сначала, путем взаимодействия *Владельца СКП*, у которого возникли претензии, с *Владельцем СКП*, к которому возникли претензии, и *Администратором* или уполномоченным представителем *Удостоверяющего Центра*. В случае если *Владелец СКП* не удовлетворен полученной информацией, для разрешения *Конфликтной ситуации* проводится техническая экспертиза путем созыва экспертной комиссии.

2. ПОРЯДОК ПРОВЕДЕНИЯ ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

2.1. Экспертная комиссия созывается *Удостоверяющим Центром ХКФОМС* на основании письменного заявления (претензии) *Владельца СКП*, оспаривающего *ЭД*. В указанном заявлении, в обязательном порядке, должны быть указаны реквизиты оспариваемого *Электронного документа*.

2.2. Состав экспертной комиссии формируется из представителей *Удостоверяющего Центра ХКФОМС*, руководства ХКФОМС, непосредственных руководителей *Владельцев СКП*, задействованных в конфликте. В состав комиссии могут также включаться эксперты – представители организаций-разработчиков и поставщиков *СКЗИ*. Состав комиссии утверждается приказом руководства ХКФОМС.

2.3. Не позднее 10 рабочих дней с момента подачи претензии назначается место, дата и время начала работы комиссии, о чем уведомляются все заинтересованные Стороны, включая *Владельцев СКП*, задействованных в конфликте.

2.4. Права и полномочия экспертной комиссии по разрешению *Конфликтной ситуации*:

Экспертная комиссия имеет право:

- получать доступ к необходимым для проведения ее работы документальным материалам на бумажных и электронных носителях;
- получать объяснения от должностных лиц, работающих с *ЭД*, и обеспечивающих обмен *ЭД*;
- получать от Сторон любую иную информацию, относящуюся, по ее мнению, к рассматриваемой *Конфликтной ситуации*.

2.5. Экспертиза оспариваемого *ЭД* осуществляется согласно Руководству администратора «Порядок разбора *Конфликтных ситуаций*, возникающих при использовании электронной подписи» ФРКЕ.00006-05 90 05, определенному организацией-разработчиком используемого *СКЗИ* (ОАО «ИнфоТеКС» г.

Москва) на предоставленном *Удостоверяющим Центром АП* (персональном компьютере с установленным ПО *ViPNet [Клиент]*), обеспечивающем проверку подписи и подпись *ЭД*.

2.6. По итогам работы Экспертной комиссии составляется акт, который должен содержать следующую информацию:

- дату и место составления акта;
- состав Экспертной комиссии;
- даты и время начала и окончания работы Комиссией;
- краткий перечень мероприятий, проведенных Комиссией;
- фактические обстоятельства, установленные Комиссией;
- выводы, к которым пришла Экспертная комиссия в результате проведенных мероприятий;
- подписи членов Экспертной комиссии;

К Акту может прилагаться особое мнение члена или членов Экспертной комиссии, не согласных с выводами Экспертной комиссии, указанными в Акте. Особое мнение составляется в произвольной форме, подписывается членом или членами Экспертной комиссии, чье мнение оно отражает.

По обращению любого из членов Экспертной комиссии ему должна быть выдана заверенная копия Акта.

2.7. Акт, составленный экспертной комиссией, с приложенными распечатками материалов, предоставленных на экспертизу, предоставляются руководству ХКФОМС для принятия решения по разрешению *Конфликтной ситуации*.