СОГЛАСОВАНО **УТВЕРЖДАЮ**

УДОСТОВЕРЯЮЩИЙ ЦЕНТР

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

УЦ

Регламент деятельности Удостоверяющего центра

17404049.4255009.259.И9

Листов: 23

Согласовано

Аннотация

Настоящий документ представляет собой проект локального нормативного акта Министерства здравоохранения Российской Федерации, описывающего порядок предоставления услуг Удостоверяющим Центром (далее – УЦ), связанных с изготовлением и управлением сертификатами открытых ключей пользователей информационных систем Министерства здравоохранения Российской Федерации.

Настоящий документ содержит обязанности, права, ответственность удостоверяющего центра и его пользователей, формализует порядок предоставления услуг удостоверяющего центра, устанавливает форматы объектов инфраструктуры открытых ключей, форматы заявительных документов.

Содержание

1 Общие положения

1.1 Регламент деятельности Удостоверяющего центра Министерства здравоохранения Российской Федерации, именуемый в дальнейшем «Регламент», разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

1.2 Настоящий Регламент определяет порядок регистрации, изготовления и управления сертификатами открытых ключей пользователей Удостоверяющего центра Министерства здравоохранения Российской Федерации, права и обязанности Удостоверяющего центра Министерства здравоохранения Российской Федерации и владельцев сертификатов открытых ключей – пользователей Удостоверяющего центра Министерства здравоохранения Российской Федерации.

1.3 Регламент распространяется на всех должностных лиц и все подразделения Министерства здравоохранения Российской Федерации.

2 Термины и определения

Администратор Удостоверяющего центра – ответственный сотрудник Удостоверяющего центра, наделенный Удостоверяющим центром полномочиями по осуществлению действий по управлению сертификатами ключей подписей Пользователей Удостоверяющего центра и уполномоченный Удостоверяющим центром расписываться собственноручной подписью в сертификатах ключей подписей на бумажном носителе, изданных Удостоверяющим центром.

Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).

Закрытый ключ электронной подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной подписи.

Закрытый ключ электронной подписи действует на определенный момент времени (действующий закрытый ключ) если:

- наступил момент времени начала действия закрытого ключа;
- срок действия закрытого ключа не истек;
- сертификат ключа подписи, соответствующий данному закрытому ключу, действует на указанный момент времени.

Оператор Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по регистрации пользователей и формированию первых ключей и сертификатов пользователей.

Открытый ключ электронной подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Пользователь Удостоверяющего центра (Пользователь УЦ) – пользователь информационных систем Министерства здравоохранения Российской Федерации, зарегистрированный в Удостоверяющем центре.

Псевдоним владельца сертификата ключа подписи – вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Рабочий день Удостоверяющего центра (далее – рабочий день) – промежуток времени с 9:00 до 18:00 (время Московское) каждого дня недели за исключением выходных и праздничных дней.

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

- реестр заявлений о присоединении к Регламенту Удостоверяющего центра;
- реестр заявлений на регистрацию в Удостоверяющем центре;
- реестр зарегистрированных пользователей Удостоверяющего центра;

- реестр заявлений на изготовление сертификатов ключей подписей;
- реестр заявлений на аннулирование (отзыв) сертификатов ключей подписей;
- реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;
- реестр сертификатов ключей подписей;
- реестр изготовленных списков отозванных сертификатов.

Руководитель Удостоверяющего центра - ответственный сотрудник Удостоверяющего центра, наделенный полномочиями по управлению Удостоверяющим центром, и является владельцем сертификата электронной подписи, которым подписываются сертификаты пользователей Удостоверяющего центра.

Сертификат ключа подписи - электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра или документ на бумажном носителе, подписанный собственноручной подписью уполномоченного на то лица Удостоверяющего центра и заверенный печатью Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи.

Сертификат ключа подписи действует на определенный момент времени (действующий сертификат) если:

- наступил момент времени начала действия сертификата ключа подписи;
- срок действия сертификата ключа подписи не истек;
- сертификат ключа подписи не аннулирован (отозван).

Список аннулированных сертификатов (CAC) – электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей подписей, которые на определенный момент времени были аннулированы.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографические преобразования информации для обеспечения ее безопасности.

Средство электронной подписи – средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивающее реализацию следующих функций - создание электронной подписи в электронном документе с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи в электронном документе, создание закрытых и открытых ключей электронных подписей.

Удостоверяющий центр – Министерства здравоохранения Российской Федерации, осуществляющее выполнение целевых функций удостоверяющего центра в соответствии с ФЗ №1 «Об электронной цифровой подписи» от 10.01.2002 года и ФЗ №63 «Об электронной подписи» от 06.04.2011 года и выполняющее следующие основные функции по управлению сертификатами ключей подписей:

- изготавливает сертификаты ключей подписей;
- создает закрытые ключи электронных подписей с гарантией сохранения в тайне закрытого ключа электронной подписи;
- аннулирует действие сертификатов;

- ведет реестр Удостоверяющего центра, обеспечивает его актуальность;
- проверяет уникальность открытых ключей;
- выдает сертификаты ключей подписей с информацией об их действии;
- осуществляет подтверждение подлинности электронной подписи в электронном документе.

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

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

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

Cryptographic Message Syntax (CMS) – стандарт, определяющий формат и синтаксис криптографических сообщений.

3 Права и обязанности Сторон

3.1 Удостоверяющий центр обязан:

3.1.1 Предоставить Пользователю Удостоверяющего центра сертификат ключа подписи уполномоченного лица Удостоверяющего центра в электронной форме.

3.1.2 Использовать для изготовления закрытого ключа уполномоченного лица Удостоверяющего центра и формирования электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи.

3.1.3 Использовать закрытый ключ уполномоченного лица Удостоверяющего центра только для подписи издаваемых им сертификатов ключей подписей и списков отозванных сертификатов.

3.1.4 Принять меры по защите закрытого ключа уполномоченного лица Удостоверяющего центра от несанкционированного доступа.

3.1.5 Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы. Удостоверяющий центр обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

3.1.6 Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре, в соответствии с порядком, определенным в настоящем Регламенте.

3.1.7 Обеспечить занесение регистрационной информации Пользователя Удостоверяющего центра в Реестр Удостоверяющего центра и обеспечить уникальность регистрационной информации всех зарегистрированных в Удостоверяющем центре лиц, используемой для идентификации владельцев сертификатов ключей подписей.

3.1.8 Изготовить сертификат ключа подписи Пользователя Удостоверяющего центра по заявлению на изготовление сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

3.1.9 Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей подписей.

3.1.10 Обеспечить уникальность значений открытых ключей в изготовленных сертификатах ключей подписей пользователей Удостоверяющего центра.

3.1.11 Обеспечить сохранение в тайне изготовленного закрытого ключа Пользователя Удостоверяющего центра.

3.1.12 Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра по соответствующему заявлению на аннулирование (отзыв) сертификата ключа подписи, в соответствии с порядком, определенным в настоящем Регламенте.

3.1.13 Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра в случае компрометации закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого был издан сертификат ключа подписи.

3.1.14 Уведомить об аннулировании (отзыве) сертификата ключа подписи всех лиц, зарегистрированных в Удостоверяющем центре.

3.1.15 Проверять публикацию списка отозванных сертификатов в точке распространения.

3.1.16 Полный адрес точки распространения списка отозванных сертификатов должен быть указан в соответствующем поле сертификата пользователя.

3.1.17 Осуществлять обновление списка отозванных сертификатов проводится УЦ по факту аннулирования (отзыва) любого сертификата.

3.1.18 Период времени с момента аннулирования (отзыва) действия сертификата до момента публикации в точке распространения не должен превышать 4 часа.

3.1.19 Публиковать актуальный список аннулированных сертификатов в ресурсе: http://crl1.rosminzdrav.ru/crl/cbb2fd0569a1c99f223e53c884f68bbcd4fdabfa.crl, Период публикации списка аннулированных сертификатов в рабочее время Удостоверяющего центра – 3 (Три) дня.

3.2 Пользователь Удостоверяющего центра обязан:

3.2.1 Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

3.2.2 Применять для формирования электронной подписи только действующий личный закрытый ключ.

3.2.3 Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

3.2.4 Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи (расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи).

3.2.5 Немедленно обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

3.2.6 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 времени подачи заявления на аннулирование (отзыв) сертификата в Удостоверяющий центр по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве).

3.2.7 Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, который был аннулирован (отозван).

3.2.8 Не использовать личный закрытый ключ до предоставления Удостоверяющему центру подписанной копии сертификата ключа подписи на бумажном носителе, соответствующего данному закрытому ключу.

3.3 Удостоверяющий центр имеет право:

3.3.1 Отказать пользователю в регистрации в Удостоверяющем центре в случае ненадлежащего оформления необходимых регистрационных документов.

3.3.2 Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи.

3.3.3 Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления соответствующего заявления на аннулирование (отзыв) сертификата ключа подписи.

3.3.4 Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего сертификату.

3.4 Пользователь удостоверяющего центра имеет право

3.4.1 Применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки электронной подписи уполномоченного лица Удостоверяющего центра в сертификатах ключей подписей, изготовленных Удостоверяющим центром.

3.4.2 Применять список аннулированных сертификатов ключей подписей, изготовленный Удостоверяющим центром, для установления статуса сертификатов ключей подписей, изготовленных Удостоверяющим центром.

3.4.3 Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

3.4.4 Для хранения личного закрытого ключа применять носитель, поддерживаемый средством электронной подписи и Удостоверяющим центром

3.4.5 Обратиться в Удостоверяющий центр с заявлением на изготовление сертификата ключа подписи.

3.4.6 Обратиться в Удостоверяющий центр с заявлением на аннулирование (отзыв) сертификата ключа подписи, владельцем которого он является, в течение срока действия соответствующего закрытого ключа.

3.4.7 Обратиться в Удостоверяющий центр за получением информации о статусе сертификатов ключей подписей и их действительности на определенный момент времени.

3.4.8 Обратиться в Удостоверяющий центр за подтверждением подлинности электронной подписи в электронном документе, сформированной с использованием сертификата ключа подписи, изданного Удостоверяющим центром.

4 Порядок предоставления и пользования услугами Удостоверяющего центра

4.1 Изготовление первого сертификата ключа подписи

Изготовление первого сертификата ключа подписи осуществляется удаленно пользователем с использованием ПО АРМ регистрации. Пользователь формирует запрос на регистрацию в электронной форме и по защищенному каналу ставит в очередь на обработку в Центр Регистрации.

Центр Регистрации формирует маркер временного доступа пользователя и также по защищенному каналу передает регистрируемому пользователю. Центр Регистрации автоматически обрабатывает (принимает) запрос на регистрацию пользователя.

Зарегистрированный пользователь с использованием АРМ зарегистрированного пользователя с маркерным доступом производит со своего рабочего места аутентификацию с Центром Регистрации по временному маркеру доступа, формирует ключи и запрос на рабочий сертификат и ставит его (запрос) в очередь на обработку в Центр Регистрации.

Оператор Удостоверяющего центра с использованием ПО АРМ администратора Центра Регистрации обрабатывает (принимает) стоящий в очереди запрос на рабочий сертификат (и тут же он смотрит заявительные бумаги для основания действия).

Пользователь с помощью АРМ зарегистрированного пользователя с маркерным доступом получает сертификат на ключи, изготовленные им на своем рабочем месте, и устанавливает его.

Пользователь использует новые рабочие ключи и сертификат в информационной системе.

Обработка запроса на служебный сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «оператор», а обработка запроса на рабочий сертификат осуществляется привилегированным пользователем (сотрудником УЦ) с ролью «администратор».

4.2 Изготовление и получение ключей подписей и сертификата ключа подписи при плановой и внеплановой смене ключей Пользователя Удостоверяющего центра

Формирование ключей подписей и сертификата ключа подписи Пользователя Удостоверяющего центра осуществляется при плановой и внеплановой смене ключей осуществляется в соответствии с п.4.1. настоящего Регламента.

4.3 Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра

Удостоверяющий центр аннулирует сертификат ключа подписи Пользователя Удостоверяющего центра в следующих случаях:

- по истечении срока его действия;
- по заявке на отзыв сертификата;
- при компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра.

В случае отзыва сертификата пользователя по заявке, Удостоверяющий центр должен уведомить пользователя и всех лиц, зарегистрированных в Удостоверяющем центре, об аннулировании (отзыве) сертификата не позднее одного рабочего дня с момента наступления описанного события.

Уведомлением о факте отзыва сертификата ключа подписи является опубликование первого (наиболее раннего) списка аннулированных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая. Временем отзыва сертификата ключа подписи признается время издания указанного списка отозванных сертификатов, хранящееся в поле thisUpdate списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключей подписей в расширение CRL Distribution Point сертификата ключа подписи.

В случае аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра по истечении срока его действия временем аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра признается время, хранящееся в поле notAfter поля Validity сертификата ключа подписи. В данном случае информация об аннулированном сертификате ключа подписи Пользователя Удостоверяющего центра в список аннулированных сертификатов не заносится.

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра временем аннулирования сертификата ключа подписи Пользователя Удостоверяющего центра признается время компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра, фиксирующееся в реестре Удостоверяющего центра. В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра информация о сертификате ключа подписи Пользователя Удостоверяющего центра в список аннулированных сертификатов не заносится.

4.3.1 Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра по заявке

Заявка на отзыв сертификата ключа подписи оформляется по форме Приложения №2 настоящего Регламента и предоставляется Администратору Удостоверяющего центра.

После предоставления заявки на отзыв сертификата ключа подписи Администратор Удостоверяющего центра осуществляет ее рассмотрение и обработку.

В случае отказа в отзыве сертификата ключа подписи Администратор Удостоверяющего центра уведомляет об этом руководителя подразделения, сотрудником которого является Пользователь Удостоверяющего центра.

При принятии положительного решения Администратор Удостоверяющего центра отзывает сертификат ключа подписи.

4.4 Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром

Получение информации о статусе сертификата ключа подписи, изданного Удостоверяющим центром осуществляется на основании заявки Пользователя Удостоверяющего

центра. Данная заявка оформляется по форме Приложения № 5 настоящего Регламента и предоставляется Администратору Удостоверяющего центра.

Заявка должна содержать следующую информацию:

- время и дата подачи заявки;
- время и дата (либо период времени), на момент наступления которых требуется установить статус сертификата ключа подписи;
- идентификационные данные пользователя Удостоверяющего центра, статус сертификата ключа подписи которого требуется установить;
- серийный номер сертификата ключа подписи, статус которого требуется установить.

По результатам проведения работ по заявке оформляется справка, содержащая информацию о статусе сертификата ключа подписи, которая предоставляется Пользователю Удостоверяющего центра.

Предоставление Пользователю Удостоверяющего центра справки о статусе сертификата ключа подписи должно быть осуществлено не позднее 10 (Десяти) рабочих дней с момента получения Удостоверяющим центром соответствующей заявки от пользователя.

4.5 Подтверждение подлинности электронной подписи в электронном документе

Удостоверяющий центр осуществляет проведение экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

В том случае, если формат электронного документа с ЭП соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то Удостоверяющий центр обеспечивает подтверждение подлинности ЭП в электронном документе. Решение о соответствии электронного документа с ЭП стандарту CMS принимает Удостоверяющий центр.

Подтверждение подлинности электронной подписи в электронном документе осуществляется на основании заявки Пользователя Удостоверяющего центра. Данная заявка оформляется по форме Приложения № 4 настоящего Регламента и предоставляется Администратору Удостоверяющего центра.

Заявление должно содержать следующую информацию:

- дата и время подачи заявления;
- идентификационные данные пользователя, подлинность ЭП которого необходимо подтвердить в электронном документе;
- время и дата формирования ЭП электронного документа;
- время и дата, на момент наступления которых требуется установить подлинность ЭП.

Обязательным приложением к заявлению на подтверждение подлинности ЭП в электронном документе является носитель, содержащий:

- сертификат ключа подписи, с использованием которого необходимо осуществить подтверждение подлинности ЭП в электронном документе – в виде файла стандарта CMS;

- электронный документ – в виде одного файла (стандарта CMS), содержащего данные и значение ЭП этих данных, либо двух файлов: один из которых содержит данные, а другой значение ЭП этих данных (файл стандарта CMS).

Проведение работ по подтверждению подлинности ЭП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭП в электронном документе является заключение Удостоверяющего центра.

Заключение Удостоверяющего центра по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью Удостоверяющего центра. Один экземпляр заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению подлинности ЭП в одном электронном документе и предоставлению пользователю заключения по выполненной проверке составляет 10 (десять) рабочих дней с момента поступления заявления в Удостоверяющий центр.

В том случае, если формат электронного документа с ЭП не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по подтверждению подлинности ЭП осуществляется Удостоверяющим центром после определения перечня исходных данных для проведения экспертизы, состава и содержания отчетных документов, сроков проведения данных работ.

5 Структура сертификатов ключей подписей и сроки действия ключевых документов

5.1 Структура сертификата ключа подписи уполномоченного лица Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ Министерства здравоохранения РФ – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = Министерство здравоохранения Российской Федерации Organization Unit (OU) = Департамент информационных технологий и связи – наименование структурного подразделения Locality (Город) = Москва Country (Страна) = RU STREET (Адрес) = Рахмановский пер. 3 Email (Электронная почта) = ca@rosminzdrav.ru 1.2.643.3.131.1.1 (ИНН) = 7707778246 1.2.643.100.1 (ОГРН) = 127746460896
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = УЦ Министерства здравоохранения РФ – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = Министерство здравоохранения Российской Федерации Organization Unit (OU) = Департамент информационных технологий и связи – наименование структурного подразделения Locality (Город) = Москва Country (Страна) = RU STREET (Адрес) = Рахмановский пер. 3 Email (Электронная почта) = ca@rosminzdrav.ru 1.2.643.3.131.1.1 (ИНН) = 7707778246 1.2.643.100.1 (ОГРН) = 127746460896
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2001)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Дополнения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Subject Key	Идентификатор	Идентификатор закрытого ключа Уполномоченного лица

Idendifier	ключа владельца сертификата	Удостоверяющего Центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SybjectType (Тип владельца сертификата) =ЦС Path Length Constraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор версии сертификата	Версия сертификата Уполномоченного лица Удостоверяющего центра

5.2 Структура сертификата ключа подписи Пользователя Удостоверяющего центра

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer	Издатель сертификата	CommonName = УЦ Министерства здравоохранения РФ – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = Министерство здравоохранения Российской Федерации Organization Unit (OU) = Департамент информационных технологий и связи – наименование структурного подразделения Locality (Город) = Москва Country (Страна) = RU STREET (Адрес) = Рахмановский пер. 3 Email (Электронная почта) = ca@rosminzdrav.ru 1.2.643.3.131.1.1 (ИНН) = 7707778246 1.2.643.100.1 (ОГРН) = 127746460896
Validity Period	Срок действия сертификата	Действителен с (notBefore): дд.мм.гггг чч:мм:сс GMT Действителен по(notAfter): дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CommonName = Фамилия, Имя, Отчество или псевдоним OrganizationUnit = Подразделение Organization = Организация Locality = Город State = Субъект Федерации Country = Страна = RU Email = Электронная почта Компоненты имени CommonName, Locality, State, Country, Email обязательна для заполнения, необходимость заполнения остальных значений определяется владельцем сертификата и Удостоверяющим центром. В поле Subject сертификата могут быть добавлены дополнительные компоненты имени согласно RFC 3280
Public Key	Открытый ключ	Открытый ключ (алгоритм подписи)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2001
Issuer Sign	ЭЦП издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения сертификата		
Key Usage (critical)	Использование ключа	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ	Набор областей использования ключей и сертификатов
Application Policy	Политика применения	Набор областей использования ключей и сертификатов
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан

	сертификата	данный сертификат
CRL Distribution Point	Точка распространения списка отозванных сертификатов	Набор адресов точек распространения списков отозванных сертификатов следующего вида: URL=http://ResourceServer/Path/hex.crl, где ResourceServer – имя сервера, Path – путь к файлу списка отозванных сертификатов, hex – шестнадцатеричное значение идентификатора закрытого ключа уполномоченного лица Удостоверяющего центра, с использованием которого издан сертификат и список аннулированных сертификатов
		В сертификат ключа подписи могут быть добавлены дополнительные поля и расширения согласно RFC 3280

5.3 Структура списка отозванных сертификатов (CRL) Удостоверяющего центра

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CommonName = УЦ Министерства здравоохранения РФ – псевдоним Уполномоченного лица Удостоверяющего Центра Organization (Организация) = Министерство здравоохранения Российской Федерации Organization Unit (OU) = Департамент информационных технологий и связи – наименование структурного подразделения Locality (Город) = Москва Country (Страна) = RU STREET (Адрес) = Рахмановский пер. 3 Email (Электронная почта) = ca@rosminzdrav.ru 1.2.643.3.131.1.1 (ИНН) = 7707778246 1.2.643.100.1 (ОГРН) = 127746460896
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список аннулированных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) сертификата (Time) 3. Код причины отзыва сертификата (Reson Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2001
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2001
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа Уполномоченного лица Удостоверяющего Центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра

5.4 Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи содержат объектные идентификаторы (OID), определяющие отношения, при осуществлении которых электронный документ, подписанный ЭП, будет иметь юридическое значение.

5.5 Сертификат ключа подписи в расширении Extended Key Usage должен содержать, включая, но не ограничиваясь, следующие области использования:

- Проверка подлинности клиента (1.3.6.1.5.5.7.3.2);
- Защищенная электронная почта (1.3.6.1.5.5.7.3.4);
- Пользователь центра регистрации (1.2.643.2.2.34.6).

5.6 Расширения Key Usage, Extended Key Usage, Application Policy сертификата защиты виртуальных частных сетей содержат объектные идентификаторы (OID), определяющие область использования сертификата.

5.7 Сроки действия ключевых документов

5.7.1 Сроки действия ключевых документов Уполномоченного лица Удостоверяющего центра

Срок действия закрытого ключа Уполномоченного лица Удостоверяющего центра составляет 5 (Пять) лет. Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа уполномоченного лица Удостоверяющего центра.

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

5.7.2 Сроки действия ключевых документов Пользователей Удостоверяющего центра

Срок действия закрытого ключа Пользователя Удостоверяющего составляет 1 (Один) год 3 (Три) месяца. Начало периода действия закрытого ключа Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра (клиентский сертификат ключа подписи) составляет 1 (Один) год 3 (Три) месяца. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра и его окончания заносится в поля «notBefore» и «not After» поля «Validity Period» соответственно.

6 Дополнительные положения

6.1 Плановая смена ключей уполномоченного лица Удостоверяющего центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) Уполномоченного лица Удостоверяющего центра выполняется не ранее 3 (Трех) и не позднее 3 (Трех) лет 1 (Одного) месяца с даты изготовления сертификата Уполномоченного лица Удостоверяющего центра, смену которого необходимо произвести.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

- Уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;
- Уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

Уведомление пользователей о проведении смены ключей уполномоченного лица Удостоверяющего центра осуществляется посредством электронной почты.

Старый закрытый ключ Уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа Уполномоченного лица Удостоверяющего центра.

6.2 Компрометация ключевых документов Уполномоченного лица Удостоверяющего центра, внеплановая смена ключей Уполномоченного лица Удостоверяющего центра

В случае компрометации закрытого ключа Уполномоченного лица Удостоверяющего центра сертификат Уполномоченного лица Удостоверяющего центра аннулируется (отзывается), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и обновлении и публикации списка отозванных сертификатов. Все сертификаты, подписанные с использованием скомпрометированного ключа Уполномоченного лица Удостоверяющего центра, считаются аннулированными.

После аннулирования сертификата Уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей Уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра.

6.3 Компрометация ключевых документов Пользователя Удостоверяющего центра

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь связывается с Удостоверяющим центром по телефону и аннулирует сертификат, соответствующий скомпрометированному ключу, посредством подачи заявки на отзыв сертификата в устной форме.

6.4 Конфиденциальность информации

6.4.1 Закрытый ключ, соответствующий сертификату ключа подписи является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Удостоверяющий центр не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

6.4.2 Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре, содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной.

6.4.3 Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях установленных законодательством Российской Федерации.

6.4.4 Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

6.4.5 Открытая информация может публиковаться по решению Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

6.4.6 Информация, включаемая в сертификаты ключей подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

6.4.7 Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

6.5 Хранение сертификатов ключей подписей в Удостоверяющем центре

Срок хранения сертификата ключа подписи в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 (Пяти) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты ключа подписи переводятся в режим архивного хранения.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изменённых	заменённых	новых	аннулированных					