ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 17090-3— 2010

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 3

Управление политиками центра сертификации

ISO 17090-3:2008
Health informatics — Public key infrastructure — Part 3: Policy management of certification authority
(IDT)

Издание официальное

Москва
Стандартинформ
2011

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения» Минздравсоцразвития (ЦНИИОИЗ Минздравсоцразвития) и Государственным научным учреждением «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздравсоцразвития — постоянным представителем ИСО ТК 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 октября 2010 г. № 329-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 17090-3:2008 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 3. Управление политиками центра сертификации» (ISO 17090-3:2008 «Health informatics — Public key infrastructure — Part 3: Policy management of certification authority»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2011

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 ОБЛАСТЬ ПРИМЕНЕНИЯ . . . 1
2 НОРМАТИВНЫЕ ССЫЛКИ . . . 1
3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ . . . 2
4 СОКРАЩЕНИЯ . . . 2
5 ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ПОЛИТИКАМИ ПО ЦИФРОВЫМ СЕРТИФИКАТАМ В СФЕРЕ ЗДРАВООХРАНЕНИЯ . . . 2
5.1 Общие сведения . . . 2
5.2 Необходимость высокой степени гарантии правильного функционирования . . . 2
5.3 Необходимость высокой степени доступности инфраструктуры . . . 2
5.4 Необходимость высокой степени доверия . . . 3
5.5 Необходимость совместимости со стандартами Интернет . . . 3
5.6 Необходимость упрощения оценки и сравнения политик по сертификатам . . . 3
6 СТРУКТУРА ПОЛИТИК ПО СЕРТИФИКАТАМ И РЕГЛАМЕНТОВ ЦЕНТРОВ СЕРТИФИКАЦИИ В СФЕРЕ ЗДРАВООХРАНЕНИЯ . . . 3
6.1 Общие требования к ПС . . . 3
6.2 Общие требования к РЦС . . . 4
6.3 Взаимосвязь между ПС и РЦС . . . 4
6.4 Область применения . . . 4
7 МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К ПОЛИТИКЕ ПО СЕРТИФИКАТАМ В СФЕРЕ ЗДРАВООХРАНЕНИЯ . . . 5
7.1 Общие требования . . . 5
7.2 Ответственность за публикацию и хранение . . . 5
7.2.1 Хранилища . . . 5
7.2.2 Публикация информации о сертификации . . . 5
7.2.3 Частота публикаций . . . 5
7.2.4 Контроль доступа к хранилищам . . . 5
7.3 Идентификация и аутентификация . . . 5
7.3.1 Начальная регистрация . . . 5
7.3.2 Начальная проверка идентичности . . . 6
7.3.3 Идентификация и аутентификация запросов на замену ключей . . . 7
7.3.4 Идентификация и аутентификация при запросе на отзыв сертификата . . . 7
7.4 Эксплуатационные требования к жизненному циклу сертификата . . . 8
7.4.1 Получение сертификата . . . 8
7.4.2 Обработка заявки на получение сертификата . . . 8
7.4.3 Выпуск сертификата . . . 9
7.4.4 Принятие сертификата . . . 9
7.4.5 Пара ключей и использование сертификата . . . 9
7.4.6 Продление действия сертификата . . . 9
7.4.7 Замена ключа в сертификате . . . 10
7.4.8 Изменение сертификата . . . 10
7.4.9 Отзыв и приостановка сертификата . . . 11
7.4.10 Службы статуса сертификатов . . . 13
7.4.11 Завершение подписки . . . 13
7.4.12 Временное депонирование секретного ключа у третьего лица . . . 13
7.5 Физические средства контроля . . . 13
7.5.1 Общие сведения . . . 14
7.5.2 Физические средства контроля . . . 14
7.5.3 Процедурные средства контроля . . . 14

7.5.4 Средства контроля персонала . . . 14
7.5.5 Процедуры ведения журнала аудита безопасности . . . 14
7.5.6 Архив записей . . . 14
7.5.7 Замена ключей . . . 14
7.5.8 Устранение последствий компрометации и аварий . . . 14
7.5.9 Завершение деятельности ЦС . . . 14
7.6 Технические средства контроля безопасности . . . 15
7.6.1 Генерация и установка пары ключей . . . 15
7.6.2 Защита секретного ключа . . . 15
7.6.3 Другие аспекты управления ключами . . . 17
7.6.4 Данные активации . . . 17
7.6.5 Средства контроля защиты компьютера . . . 17
7.6.6 Технические средства контроля жизненного цикла . . . 18
7.6.7 Средства контроля защиты сети . . . 18
7.6.8 Метки времени . . . 18
7.7 Профили сертификата, СОСи ОПСС . . . 18
7.8 Аудит соответствия . . . 18
7.8.1 Общие сведения . . . 18
7.8.2 Периодичность аудита соответствия ЦС . . . 18
7.8.3 Идентичность/квалификация аудитора . . . 18
7.8.4 Взаимосвязь аудитора с проверяемой стороной . . . 18
7.8.5 Вопросы, затрагиваемые аудитом . . . 18
7.8.6 Действия, предпринимаемые в результате выявления недостатков . . . 18
7.8.7 Рассылка результатов аудита . . . 19
7.9 Юридические и другие аспекты деятельности . . . 19
7.9.1 Оплата . . . 19
7.9.2 Финансовая ответственность . . . 19
7.9.3 Конфиденциальность деловой информации . . . 19
7.9.4 Защита персональной информации . . . 20
7.9.5 Права интеллектуальной собственности . . . 20
7.9.6 Претензии и гарантии . . . 20
7.9.7 Отказ от гарантийных обязательств . . . 22
7.9.8 Ограничение ответственности . . . 22
7.9.9 Возмещение убытков . . . 22
7.9.10 Сроки и прекращение полномочий . . . 22
7.9.11 Индивидуальные уведомления и обмен информацией с участниками . . . 23
7.9.12 Поправки . . . 23
7.9.13 Процедуры разрешения споров . . . 23
7.9.14 Правовые нормы . . . 23
7.9.15 Соответствие применяемым правовым нормам . . . 23
7.9.16 Прочие положения . . . 23
8 МОДЕЛЬ ОФИЦИАЛЬНОГО ОТЧЕТА ОБ ИОК . . . 23
8.1 Введение . . . 23
8.2 Структура официального отчета об ИОК . . . 24
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 26
Библиография . . . 27

Введение

Перед отраслью здравоохранения стоит проблема сокращения расходов с помощью перехода от бумажного документирования процессов к электронному документообороту. В новых моделях оказания медицинской помощи особо подчеркивается необходимость совместного использования сведений о пациенте расширяющимся кругом медицинских специалистов, выходящего за рамки традиционных организационных барьеров.

Персональная медицинская информация обычно передается с помощью электронной почты, удаленного доступа к базе данных, электронного обмена данными и других приложений. Среда Интернет предоставляет высокоэффективные и доступные средства обмена информацией, однако она не безопасна, и при ее использовании необходимо принимать дополнительные меры обеспечения конфиденциальности и неприкосновенности личной информации. Усиливаются такие угрозы безопасности, как случайный или преднамеренный несанкционированный доступ к медицинской информации. Поэтому системе здравоохранения необходимо иметь надежные средства защиты, минимизирующие риск несанкционированного доступа.

Каким же образом отрасль здравоохранения может обеспечить соответствующую эффективную и в то же время экономичную защиту передачи данных через сеть Интернет? Решение этой проблемы может быть обеспечено с помощью технологии цифровых сертификатов и инфраструктуры с открытым ключом (ИОК).

Для правильного применения цифровых сертификатов требуется сочетание технологических, методических и административных процессов, обеспечивающих защиту передачи конфиденциальных данных в незащищенной среде с помощью «шифрования с открытым ключом» и подтверждение идентичности лица или объекта с помощью сертификатов. В сфере здравоохранения в это сочетание входят средства аутентификации, шифрования и электронной цифровой подписи, предназначенные для выполнения административных и клинических требований конфиденциальности доступа и защиты передачи медицинских документов индивидуального учета. Многие из этих требований могут быть удовлетворены с помощью служб, использующих цифровые сертификаты (включая шифрование, целостность информации и электронные подписи). Особо эффективно использование цифровых сертификатов в рамках официального стандарта защиты информации. Многие организации во всем мире начали использовать цифровые сертификаты подобным образом.

Если обмен информацией должен осуществляться между медицинским прикладным программным обеспечением разных организаций, в том числе относящихся к разным ведомствам (например, между информационными системами больницы и поликлиники, оказывающих медицинскую помощь одному и тому же пациенту), то интероперабельность технологий цифровых сертификатов и сопутствующих политик, регламентов и практических приемов приобретает принципиальное значение.

Для обеспечения интероперабельности различных систем, использующих цифровые сертификаты, необходимо создать систему доверительных отношений, с помощью которой стороны, ответственные за обеспечение прав личности на защиту персональной информации, могут полагаться на политики и практические приемы и, в дополнение, на действительность цифровых сертификатов, выданных другими уполномоченными организациями.

Во многих странах система цифровых сертификатов используется для обеспечения безопасного обмена информацией в пределах национальных границ. Если разработка стандартов также ограничена этими пределами, то это приводит к несовместимости политик и регламентов центров сертификации (ЦС) и центров регистрации (ЦР) разных стран.

Технология цифровых сертификатов продолжает развиваться в определенных направлениях, не специфичных для здравоохранения. Непрерывно проводится важная работа по стандартизации и в некоторых случаях по правовому обеспечению их применения. Поставщики медицинских услуг во многих странах уже используют или планируют использовать цифровые сертификаты. Серия стандартов ИСО 17090 призвана удовлетворить потребность в управлении данным интенсивным международным процессом.

Серия стандартов ИСО 17090 содержит общие технические, эксплуатационные и методические требования, которые должны быть удовлетворены для обеспечения использования цифровых сертификатов в целях защиты обмена медицинской информацией в пределах одного домена, между доменами и за пределами границ одной юрисдикции. Основной целью серии является создание основы для глобальной интероперабельности. Стандарты данной серии изначально предназначены для поддержки трансграничного обмена данными на основе цифровых сертификатов, однако они также могут служить руководством по использованию цифровых сертификатов в здравоохранении на национальном или региональном уровнях. Интернет все шире используется как средство передачи медицинских данных

между организациями здравоохранения и является единственным реальным вариантом для трансграничного обмена данными в этой сфере.

Серия стандартов ИСО 17090 должна рассматриваться как единое целое, поскольку каждая из трех его частей вносит свой вклад в определение того, как цифровые сертификаты могут использоваться для обеспечения сервисов безопасности в отрасли здравоохранения, включая аутентификацию, конфиденциальность, целостность данных и технические возможности поддержки качества электронной цифровой подписи.

ИСО 17090-1 определяет основные принципы применения цифровых сертификатов в сфере здравоохранения и структуру требований к интероперабельности, необходимой для создания системы защищенного обмена медицинской информацией на основе применения цифровых сертификатов.

ИСО 17090-2 определяет специфические для сферы здравоохранения профили цифровых сертификатов, основанных на международном стандарте X.509 и его профиле, определенном в спецификации IETF/RFC 3280 для разных типов сертификатов.

В настоящем стандарте — ИСО 17090-3 рассматриваются проблемы управления, связанные с внедрением и эксплуатацией цифровых сертификатов в сфере здравоохранения. В нем определены структура политик по сертификатам (ПС) и минимальные требования к ним, а также структура сопутствующих отчетов по практическому применению сертификации. Настоящий стандарт базируется на информационных рекомендациях спецификации IETF/RFC 3647 и определяет принципы политик безопасности медицинской информации при ее трансграничной передаче. В нем также определен минимально необходимый уровень безопасности применительно к аспектам, специфичным для здравоохранения.

Комментарии по содержанию настоящего стандарта, а также комментарии, предложения и информация по применению настоящего стандарта могут направляться в секретариат ИСО/ТК 215 по адресу gost.e-ecolog.ru, либо в секретариат РГ4, или руководителю РГ4 Россу Фрейзеру по адресу gost.e-ecolog.ru.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 3

Управление политиками центра сертификации

Health informatics. Public key infrastructure.
Part 3. Policy management of certificate authority

Дата введения — 2011—08—01

1 Область применения

В настоящем стандарте приведены методические указания по вопросам управления сертификатами, возникающим при использовании цифровых сертификатов в сфере здравоохранения. В нем определены структура и минимальные требования к политикам по сертификатам, а также структура регламента центра сертификации.

Кроме того, настоящий стандарт устанавливает правила, необходимые для защиты информации в сфере здравоохранения при международном взаимодействии, и определяет необходимый минимальный уровень безопасности применительно к аспектам, специфичным для здравоохранения.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие международные стандарты. Если в ссылке указана дата издания, то должно использоваться только цитируемое издание. Если дата в ссылке не указана, то должно использоваться последнее издание документа (включая все поправки).

ИСО 17090-1:2008 Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Общие вопросы применения цифровых сертификатов (ISO 17090-1:2008, Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services)

ИСО 17090-2:2008 Информатизация здоровья. Инфраструктура с открытым ключом. Часть 2. Профиль сертификатов (ISO 17090-2:2008, Health informatics — Public key infrastructure — Part 2: Certificate profile)

ИСО/МЭК 27002 Информационная технология. Методы обеспечения безопасности. Свод правил по управлению защитой информации (ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management)

IETF/RFC 3647 Политика по сертификатам X.509 инфраструктуры с открытым ключом и основы практического применения сертификации в Интернет (IETF/RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework)

IETF/RFC 4211 Формат сообщения с запросом сертификата X.509 инфраструктуры с открытым ключом в Интернет (IETF/RFC 4211, Internet X.509 Public Key Infrastructure Certificate Request Message Format)

Издание официальное

3 Термины и определения

В настоящем стандарте использованы термины и определения, установленные в ИСО 17090-1.

4 Сокращения

В настоящем стандарте использованы следующие сокращения:
ЦА — центр присвоения атрибутов (attribute authority — AA);
ЦС — центр сертификации (certificate authority — CA);
ПС — политика по сертификатам (certificate policy — CP);
РЦС — регламент центра сертификации (certification practice statement — CPS);
СОС — список отозванных сертификатов (certificate revocation list — CRL);
ОИД — объектный идентификатор (object identifier — OID);
ОПСС — оперативный протокол статуса сертификата (online certificate status protocol — OCSP);
СОК — сертификат открытого ключа (public key certificate — PKC);
ИОК — инфраструктура с открытым ключом (public key infrastructure — PKI);
ЦР — центр регистрации (registration authority — RA);
ДТС — доверенная третья сторона (trusted third party — TTP).

5 Требования к управлению политиками по цифровым сертификатам в сфере здравоохранения

5.1 Общие сведения

Чтобы применение цифровых сертификатов в сфере здравоохранения способствовало эффективной защите передачи персональной медицинской информации, оно должно обеспечивать решение следующих задач:

- надежная и безопасная привязка уникальных и отличительных имен к лицам, организациям, приложениям и устройствам, участвующим в электронном обмене персональной медицинской информацией;
- надежная и безопасная привязка профессиональных ролей в здравоохранении к лицам, организациям и приложениям, участвующим в электронном обмене персональной медицинской информацией, в той мере, в которой данные роли могут быть использованы в качестве основы ролевого управления доступом к медицинской информации;
- (факультативно) надежная и безопасная привязка атрибутов к лицам, организациям, приложениям и устройствам, участвующим в электронном обмене персональной медицинской информацией, в той мере, в которой данные атрибуты могут содействовать безопасному обмену медицинской информацией.

Вышеуказанные задачи должны решаться способами, обеспечивающими доверительные отношения всех участников, полагающихся на целостность и конфиденциальность передаваемой персональной медицинской информации, защищенной с помощью цифровых сертификатов.

С этой целью каждый центр сертификации, выпускающий цифровые сертификаты для сферы здравоохранения, должен действовать в соответствии с четким набором публично установленных политик, способствующих решению вышеуказанных задач.

5.2 Необходимость высокой степени гарантии правильного функционирования

Сервисы безопасности, требуемые для медицинских приложений, определены в ИСО 17090-1:2008, раздел 6. Для каждого из этих сервисов безопасности (аутентификация, целостность, конфиденциальность, электронная цифровая подпись, авторизация, контроль доступа) необходима высокая степень гарантии правильного функционирования.

5.3 Необходимость высокой степени доступности инфраструктуры

Медицинские услуги оказываются круглосуточно, и возможность получать и отзывать сертификаты, проверять их действительность ни в коем случае не должна быть ограничена обычными рабочими часами, что принято в большинстве отраслей. В отличие от электронной торговли здравоохранение предъявляет высокие требования доступности к применению цифровых сертификатов, обеспечивающих безопасный обмен персональной медицинской информацией.

5.4 Необходимость высокой степени доверия

В отличие от электронной торговли (где поставщик и покупатель часто являются единственными участниками электронного обмена информацией и сами отвечают за ее безопасность и целостность) медицинским приложениям, хранящим и передающим персональную медицинскую информацию, может косвенным образом требоваться доверие пациентов, чью информацию они обрабатывают, а также доверие широкой общественности. Вряд ли поставщики медицинских услуг или пациенты согласятся использовать электронный обмен персональной медицинской информацией, если такой обмен представляется им небезопасным.

5.5 Необходимость совместимости со стандартами Интернет

Поскольку целью настоящего стандарта является определение основных элементов применения цифровых сертификатов в сфере здравоохранения для обеспечения безопасной трансграничной передачи медицинской информации, то настоящий стандарт, насколько возможно, основан на стандартах Интернет, обеспечивающих эффективный выход за границы стран и территорий.

5.6 Необходимость упрощения оценки и сравнения политик по сертификатам

Способы применения цифровых сертификатов, способствующие безопасному трансграничному обмену персональной медицинской информацией, рассмотрены в ИСО 17090-1:2008, подраздел 9.2. Их реализация (например, перекрестное признание и кросс-сертификация) существенно упрощается, если политики по сертификатам, применяемые в здравоохранении, описаны в едином формате, позволяющем без труда переходить с одной политики на другую.

Кроме того, политики по сертификатам в сфере здравоохранения создают основу для аккредитации центров сертификации. (ЦС аккредитуется на соответствие одной или нескольким политикам по сертификатам, которые он предполагает реализовать.) Определение критериев аккредитации выходит за рамки настоящего стандарта, однако в целом процесс аккредитации центров сертификации для сферы здравоохранения ускоряется за счет согласованности его формы и соответствия минимальной совокупности стандартов, упомянутых в настоящем стандарте.

6 Структура политик по сертификатам и регламентов центров сертификации в сфере здравоохранения

6.1 Общие требования к ПС

Выдав сертификат, ЦС гарантирует доверяющей стороне, что конкретный открытый ключ связан с конкретным держателем сертификата. Разные сертификаты выдаются в соответствии с разными правилами и процедурами и могут предназначаться для разных приложений или целей.

ЦС отвечает за все аспекты выдачи сертификата и управления сертификатом, включая контроль процесса регистрации, проверку информации, содержащейся в сертификате, изготовление, выпуск, отзыв, приостановку действия и обновление сертификата. ЦС несет ответственность за то, что все аспекты его услуг и действий осуществляются в соответствии с требованиями, представлениями и гарантиями данной ПС и РЦС данного ЦС.

ЦС, выдающий цифровые сертификаты для применения в сфере здравоохранения, должен иметь политики и процедуры, соответствующие предоставляемым услугам. Эти политики и процедуры должны обеспечивать:

- регистрацию потенциальных держателей сертификатов до выдачи сертификатов, включая, когда это возможно, указание роли держателя сертификата в соответствии с ИСО 17090-2:2008, раздел 6;
- аутентификацию идентичности потенциальных держателей сертификата до выдачи сертификата;
- обеспечение конфиденциальности любой персональной информации о лицах, которым выдаются сертификаты;
- передачу сертификатов держателям сертификатов и регистрацию сертификатов в реестрах;
- прием информации о возможной компрометации секретного ключа;
- распространение списков отозванных сертификатов (периодичность, способ и место их опубликования);
- другие проблемы управления ключами, включая размер ключа, процесс генерации ключа, срок службы ключа, замену ключа и т. д.;

- кросс-сертификацию с другими ЦС;
- контроль и аудит безопасности.

Чтобы выполнять вышеперечисленные функции, каждый ЦС, входящий в состав инфраструктуры, должен предоставить некоторые основные сервисы своим держателям сертификатов и доверяющим сторонам. Данные сервисы ЦС перечисляются в ПС.

Цифровые сертификаты содержат один или несколько зарегистрированных объектных идентификаторов, идентифицирующих ПС, в соответствии с которой выпущен данный сертификат. Объектные идентификаторы могут использоваться для принятия решения, предназначен ли сертификат для конкретной цели. Процесс регистрации ОИД соответствует процедурам, установленным стандартами ИСО/МЭК и МСЭ. Сторона, регистрирующая ОИД, также публикует ПС для ознакомления держателей сертификатов и доверяющих сторон.

Вследствие важности ПС в установлении доверия к СОК крайне необходимо, чтобы ПС была понята и принята во внимание не только держателями сертификатов, но и всеми доверяющими сторонами. Поэтому держатели сертификатов и доверяющие стороны должны иметь быстрый и надежный доступ к ПС, в соответствии с которой был выпущен данный сертификат.

К любой ПС, определенной в соответствии с настоящим стандартом, предъявляются следующие требования:

a) каждый цифровой сертификат, выпущенный в соответствии с настоящим стандартом, должен содержать по крайней мере один зарегистрированный ОИД, идентифицирующий ПС, в соответствии с которой выпущен данный сертификат;

b) структура ПС должна соответствовать спецификации IETF/RFC 3647;

c) ПС должна быть доступна держателям сертификатов и доверяющим сторонам.

Хотя документы ПС и РЦС являются основными для описания и управления политиками и правилами сертификации, многие держатели цифровых сертификатов, особенно потребители, находят эти подробные документы трудными для понимания. Таким держателям сертификатов и другим доверяющим сторонам может помочь возможность доступа к сжатому описанию элементов ПС, требующих внимания и объяснения, и для этой цели в разделе 8 представлена модель официального отчета об ИОК.

6.2 Общие требования к РЦС

РЦС представляет собой подробное описание таких деталей, как точная реализация предложений сервисов и детальные процедуры управления жизненным циклом сертификатов, и обычно является более детальным документом, чем ПС.

К любому РЦС, определенному в соответствии с настоящим стандартом, предъявляются следующие требования:

a) РЦС должен соответствовать спецификации IETF/RFC 3647;

b) ЦС с одним РЦС может поддерживать несколько политик по сертификатам (используемых для разных прикладных целей и/или разными группами доверяющих сторон);

c) несколько центров сертификации с неидентичными РЦС могут поддерживать одну и ту же ПС;

d) ЦС может не делать свой РЦС доступным держателям сертификатов или доверяющим сторонам или может обеспечить им доступ только к отдельным частям своего РЦС.

6.3 Взаимосвязь между ПС и РЦС

ПС устанавливает, какие гарантии могут быть даны для сертификата (включая ограничения на использование сертификата и ограничения ответственности). РЦС утверждает, каким образом ЦС обеспечивает эти гарантии. ПС может применяться не только в рамках одной организации, но и шире, в то время как РЦС относится только к одному ЦС. ПС служит в качестве фундамента, на котором основываются общие стандарты интероперабельности и общие критерии гарантии в масштабах отрасли (или, возможно, в более глобальном масштабе). Подробный РЦС сам по себе не создает подходящей основы для интероперабельности центров сертификации, обслуживающих разные организации.

6.4 Область применения

Настоящий стандарт применим к политикам по сертификатам и регламентам центров сертификации, используемым для целей выпуска сертификатов в сфере здравоохранения в соответствии с ИСО 17090-2:2008, раздел 5.

7 Минимальные требования к политике по сертификатам в сфере здравоохранения

7.1 Общие требования

Чтобы соответствовать настоящему стандарту, ПС должна удовлетворять указанным ниже требованиям.

В данном разделе числа в круглых скобках под заголовками обозначают номер соответствующего раздела спецификации IETF/RFC 3647.

7.2 Ответственность за публикацию и хранение

7.2.1 Хранилища

(2.1)

Информация о держателях сертификатов, помещаемая в хранилища ЦР или ЦС, должна:

- поддерживаться актуальной и своевременной (изменения должны вноситься ежедневно или чаще, в зависимости от обстоятельств);
- управляться в соответствии с ИСО/МЭК 27002 (или его эквивалентом) или с утвержденными критериями аккредитации или лицензирования.

7.2.2 Публикация информации о сертификации

(2.2)

Любой ЦС, выпускающий цифровые сертификаты для использования в сфере здравоохранения, должен сделать доступными для своих держателей сертификатов и доверяющих сторон сведения:

- об адресе URL доступного веб-сайта, контролируемого непосредственно ЦС или по его поручению и содержащего описания его политик по сертификатам;
- о каждом сертификате, выпущенном или обновленном в соответствии с данной политикой;
- о текущем статусе каждого сертификата, выпущенного в соответствии с данной политикой;
- о критериях аккредитации или лицензирования, в соответствии с которыми функционирует ЦС, а также сведения о том, на какую часть ведомства, в котором функционирует ЦС, распространяется данная аккредитация или лицензирование.

Электронная копия документа ПС, заверенная электронной цифровой подписью уполномоченного представителя ЦС, должна быть доступна:

- на веб-сайте, доступном всем доверяющим сторонам, или
- через запрос по электронной почте.

Поскольку РЦС подробно описывает реализацию сервисов, предоставляемых ЦС, а также процедуры управления жизненным циклом ключей и является более подробным документом, чем ПС, то в целях обеспечения безопасности ЦС эта информация может быть признана конфиденциальной.

7.2.3 Частота публикаций

(2.3)

ЦС должен публиковать информацию при каждом ее изменении.

7.2.4 Контроль доступа к хранилищам

(2.4)

Публикуемые сведения, например, политики, правила, сертификаты и текущий статус сертификатов, должны быть доступны только для чтения.

7.3 Идентификация и аутентификация

7.3.1 Начальная регистрация

7.3.1.1 Типы идентификаторов

(3.1.1)

Идентификаторы субъектов, используемые в сертификатах, выпущенных в соответствии с данной политикой, должны соответствовать ИСО 17090-2.

7.3.1.2 Необходимость смысловых идентификаторов

(3.1.2)

Для эффективного использования сертификатов требуется, чтобы отличительные идентификаторы, присутствующие в сертификате, могли быть поняты и использованы доверяющей стороной. Идентификаторы, используемые в сертификатах, должны однозначно устанавливать личность держателя сертификата, которому они присвоены. См. также 7.3.1.3.

Идентификаторы держателей сертификатов, являющихся квалифицированными медицинскими работниками, вспомогательными медицинскими работниками, субсидируемыми поставщиками меди-

цинских услуг, работниками поддерживающих организаций, а также пациентами/потребителями медицинской помощи, должны соответствовать положениям пункта 7.3.2.

7.3.1.3 Анонимность или использование псевдонимов

(3.1.3)

Требование смысловой значимости идентификаторов (см. 7.3.1.2) не препятствует использованию псевдонимов в сертификатах, выпущенных для пациентов/потребителей.

7.3.1.4 Правила интерпретации различных форм идентификаторов

(3.1.4)

ПС должна содержать процедуру, применяемую при разрешении споров по поводу присвоения идентификаторов, и соглашение, используемое для интерпретации их форм в тех случаях, когда возникают споры по поводу присвоения идентификаторов.

7.3.1.5 Уникальность идентификаторов

(3.1.5)

Чтобы различать держателей сертификатов данного ЦС, отличительный идентификатор субъекта, указанный в сертификате, должен быть недвусмысленным и уникальным.

В случае необходимости для обеспечения уникальности обозначения субъекта в состав его отличительного идентификатора может быть включен атрибут типа «порядковый номер» (в соответствии с IETF/RFC 3280). По возможности рекомендуется, чтобы такой порядковый номер имел определенный смысл (например, номер лицензии квалифицированного медицинского работника). См. 7.3.1.2.

7.3.1.6 Распознавание, аутентификация и роль товарных знаков

(3.1.6)

ЦС не должен сознательно выпускать сертификаты, содержащие товарные знаки, не принадлежащие субъекту сертификата.

7.3.2 Начальная проверка идентичности

7.3.2.1 Способ доказательства обладания секретным ключом

(3.2.1)

В тех случаях, когда ЦС не генерирует пару ключей, держателям ключей необходимо подтвердить, что они являются обладателями своих секретных ключей (например, подачей запроса на подпись сертификата — ЗПС). От держателей сертификатов может также потребоваться периодически подписывать запросы подлинности, направляемые ЦС.

7.3.2.2 Аутентификация идентичности организаций

(3.2.2)

Организации здравоохранения, поддерживающие организации, лица, действующие от имени организаций или применяющие сертификаты для идентификации устройств, должны представить в ЦР документы, свидетельствующие об их существовании и роли в системе здравоохранения, а также соответствующие требованиям, установленным в их стране, регионе или иной административной единице. ЦС, ЦР и, где это необходимо, ЦА должны проверить представленную информацию, а также аутентичность запрашивающего представителя и его полномочия на право действовать от имени организации.

7.3.2.3 Аутентификация идентичности физических лиц

(3.2.3)

Перед выпуском сертификата физические лица, включая квалифицированных медицинских работников, вспомогательных медицинских работников, субсидируемых поставщиков медицинских услуг, работников поддерживающих организаций, а также пациентов/потребителей медицинской помощи, должны подтвердить свою идентичность в ЦР. Настоящий стандарт рекомендует использовать для подтверждения идентичности ту же процедуру, которая необходима для получения паспорта, либо иную аналогичную процедуру.

Для аутентификации своей лицензии на право медицинской деятельности, роли и медицинской специальности (если таковая имеется) квалифицированные медицинские работники должны представить в ЦР доказательство своих профессиональных прав, выданное органом управления здравоохранением или органом аккредитации в рамках своих полномочий.

Для подтверждения своей занятости и роли в системе здравоохранения вспомогательные медицинские работники должны представить в ЦР доказательство субсидирования или занятости от своих субсидирующих медицинских учреждений или субсидирующих (контролирующих) медицинских работников.

Для подтверждения своей деятельности и роли в системе здравоохранения субсидируемые поставщики медицинских услуг должны представить в ЦР доказательство субсидирования от своих субсидирующих медицинских учреждений или субсидирующих (контролирующих) медицинских работников.

Для подтверждения своей занятости и роли в системе здравоохранения работники поддерживающих организаций должны представить в ЦР доказательство занятости от своих поддерживающих организаций здравоохранения.

7.3.2.4 Непроверенная информация о подписчике

(3.2.4)

Непроверенная информация о подписчике должна быть определена в соответствии со спецификацией IETF/RFC 3647, пункт 3.2.4.

7.3.2.5 Проверка полномочий

(3.2.5)

Проверка полномочий должна быть определена в соответствии со спецификацией IETF/RFC 3647, пункт 3.2.5.

7.3.2.6 Критерии взаимодействия

(3.2.6)

Критерии взаимодействия должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 3.2.6 и ИСО 17090-2.

7.3.3 Идентификация и аутентификация запросов на замену ключей

7.3.3.1 Идентификация и аутентификация при обычной замене ключей

(3.3.1)

7.3.3.1.1 Обычная замена ключей ЦС

Обычная замена ключей или повторный выпуск сертификатов ЦС должны осуществляться на основе исходной документации, использованной при создании исходной записи.

7.3.3.1.2 Обычная замена ключей ЦР

Обычная замена ключей или повторный выпуск сертификатов ЦР должны осуществляться на основе исходной документации, использованной при создании исходной записи.

7.3.3.1.3 Обычная замена ключей держателя сертификата

Обычная замена ключей держателя сертификата должна осуществляться посредством обращения к исходной документации или записям, использованным при создании исходной записи, включая текущий действующий ключ с неистекшим сроком.

Если исходная документация утрачена или уничтожена, то может быть использована заменяющая документация.

7.3.3.2 Замена ключей после отзыва

(3.3.2)

7.3.3.2.1 Замена ключей ЦС после отзыва

Замена ключей после отзыва сертификата требует повторного представления исходной информации, которая использовалась при первоначальной аккредитации ЦС.

7.3.3.2.2 Замена ключей ЦР после отзыва

Замена ключей после отзыва сертификата требует повторного представления исходной информации, которая использовалась при первоначальной аккредитации ЦР.

7.3.3.2.3 Замена ключей держателя сертификата после отзыва

Замена ключей держателя сертификата требует либо представления исходной документации, использованной при создании исходной записи, либо обращения к использованным исходным записям. Если исходная документация утрачена или уничтожена, то может быть использована заменяющая ее документация.

7.3.4 Идентификация и аутентификация при запросе на отзыв сертификата

(3.4)

7.3.4.1 ЦС

Когда данный ЦС в соответствии с политикой по сертификатам в сфере здравоохранения отправляет другому ЦС запрос на отзыв сертификата, он должен:

- идентифицировать сертификат;
- указать причины отзыва сертификата;
- подписать запрос своим секретным ключом, зашифровать сообщение и послать его в ЦС соответствующего домена.

7.3.4.2 ЦР

Когда ЦР отправляет в ЦС запрос на отзыв сертификата, выпущенного в соответствии с политикой по цифровым сертификатам в сфере здравоохранения, он должен:

- идентифицировать сертификат, подлежащий отзыву;
- указать причины отзыва сертификата;

- подписать запрос своим секретным ключом, зашифровать сообщение и послать его в ЦС соответствующего домена.

7.3.4.3 Держатель сертификата

Когда держатель цифрового сертификата, выпущенного в соответствии с политикой по цифровым сертификатам в сфере здравоохранения, отправляет в ЦС запрос на отзыв этого сертификата, он должен:

- идентифицировать принадлежащий ему сертификат, подлежащий отзыву;
- указать причины, по которым сертификат должен быть отозван;
- защищенным способом передать запрос на отзыв в ЦС соответствующего домена.

Если носитель секретного ключа утерян или украден (и поэтому держатель сертификата не может инициировать подачу запроса, скрепленного электронной цифровой подписью), то запрос на отзыв должен сопровождаться свидетельством идентичности, эквивалентным тому, которое было первоначально представлено для получения сертификата.

7.4 Эксплуатационные требования к жизненному циклу сертификата

7.4.1 Получение сертификата

7.4.1.1 Кто может обращаться за получением сертификата

(4.1.1)

Критерии, определяющие, кто может обращаться за получением сертификата, должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 4.1.1.

7.4.1.2 Процесс признания права на получение сертификата и ответственность

(4.1.2)

ЦС может делегировать функции идентификации и аутентификации, за которые он несет ответственность, ЦР. Основной функцией, выполняемой ЦР организации здравоохранения, является проверка идентичности и роли в системе здравоохранения держателя сертификата при его первичной регистрации. ЦР должен придерживаться той же совокупности правил и способов аутентификации, которую использует данный ЦС. ЦР может быть аккредитован самостоятельно, вне зависимости от конкретного ЦС.

Чтобы подлинность и целостность сертификата и содержащихся в нем открытых ключей были гарантированы, держатели сертификатов должны получать сертификаты от надежного источника. Поскольку ЦР выполняет функции аутентификации для ЦС, он должен обладать доверием в части осуществления политики ЦС по аутентификации держателя сертификата и направления правильной информации о держателе сертификата в ЦС. Аналогично ЦР должен обладать доверием в части точной и своевременной подачи запроса на отзыв сертификата в ЦС.

Рекомендуется, чтобы центры регистрации индивидуально отчитывались за действия, выполняемые от имени ЦС. ЦР должен:

- гарантировать, что его секретный ключ используется только для подписи запросов на выдачу и отзыв сертификатов и для других аутентифицированных обменов информацией с держателями сертификатов, если ЦР выполняет свои обязанности в интерактивном режиме;
- подтвердить в ЦС, что ЦР аутентифицировал идентичность держателя сертификата;
- безопасно передавать и хранить информацию о заявке на получение сертификата и регистрационные записи;
- инициировать запрос на отзыв сертификата (при необходимости) в соответствии с 7.3.4.2.

В случае применения цифровых сертификатов в сфере здравоохранения держатель сертификата должен при подаче заявки на получение сертификата гарантировать точность представленной им информации, а при получении сертификата подтвердить, что вся информация, содержащаяся в сертификате, является истинной.

7.4.2 Обработка заявки на получение сертификата

7.4.2.1 Выполнение функций идентификации и аутентификации

(4.2.1)

Критерии выполнения функций идентификации и аутентификации должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.2.1.

7.4.2.2 Утверждение или отклонение заявок на получение сертификатов

(4.2.2)

Критерии утверждения или отклонения заявок на получение сертификатов должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.2.2.

7.4.2.3 Срок обработки заявок на получение сертификатов

(4.2.3)

Рекомендуется, чтобы ЦС объявлял максимальный срок, в течение которого держатель сертификата должен завершить процесс активации ключа после инициирования процесса выпуска сертификата.

7.4.3 Выпуск сертификата

7.4.3.1 Действия ЦС в процессе выпуска сертификата

(4.3.1)

Процедуры замены ключа в сертификате должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 4.7.

7.4.3.2 Уведомление о выпуске сертификата, направляемое ЦС держателям сертификата

(4.3.2)

ЦС, выпускающий сертификат, должен уведомить каждого держателя сертификата о выпуске сертификата, содержащего уникальный идентификатор данного держателя сертификата.

7.4.4 Принятие сертификата

7.4.4.1 Действия, подтверждающие принятие сертификата

(4.4.1)

Держатель сертификата, предназначенного для применения в сфере здравоохранения, должен:

- ознакомиться с ПС или с документом по ИОК, в котором простым языком четко устанавливаются обязанности держателя сертификата;
- формально признать эти обязанности, подписав соглашение держателя сертификата.

7.4.4.2 Публикация сертификата в ЦС

(4.4.2)

См. 7.2.2.

7.4.4.3 Уведомление о выпуске сертификата, направляемое ЦС другим субъектам

(4.4.3)

Критерии уведомления о выпуске сертификата, направляемого ЦС другим субъектам, должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.4.3.

7.4.5 Пара ключей и использование сертификата

7.4.5.1 Секретный ключ держателя сертификата и использование сертификата

(4.5.1)

Держатель сертификата, предназначенного для применения в сфере здравоохранения, должен:

- защищать свои секретные ключи и ключевые носители (если таковые имеются) и принимать все меры для предотвращения их утери, раскрытия, изменения или несанкционированного использования;
- прилагать все усилия для предотвращения утери, раскрытия или несанкционированного использования своего секретного ключа;
- немедленно уведомлять ЦС и/или ЦР о любой реальной или подозреваемой утере, раскрытии или другой компрометации своего секретного ключа;
- уведомлять ЦР и/или ЦС о любом изменении информации, содержащейся в сертификате, а также об изменении роли или статуса в организации здравоохранения;
- использовать пары ключей в соответствии с ПС.

Рекомендуется, чтобы держатель сертификата, предназначенного для применения в сфере здравоохранения, также подтвердил прохождение обучения по информационной безопасности, соответствующего функциям обработки медицинской информации, для которых будет использоваться данный сертификат.

7.4.5.2 Открытый ключ доверяющей стороны и использование сертификата

(4.5.2)

Доверяющая сторона имеет право доверять сертификату, предназначенному для применения в сфере здравоохранения, только при следующих условиях:

- цель применения сертификата соответствует данной политике;
- доверие является обоснованным и добросовестным в свете всех обстоятельств, известных доверяющей стороне на данный момент;
- доверяющая сторона удостоверилась в текущей действительности сертификата, проверив, что данный сертификат не был отозван или приостановлен;
- доверяющая сторона удостоверилась в текущей действительности электронных цифровых подписей, если таковые применялись;
- признаны имеющиеся ограничения на ответственность и гарантийные обязательства.

7.4.6 Продление действия сертификата

(4.6)

Выпускающий ЦС должен гарантировать, что все процедуры продления действия сертификата соответствуют релевантным положениям данной ПС.

7.4.6.1 Причины продления действия сертификата

(4.6.1)

Причины продления действия сертификата должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.6.1.

7.4.6.2 Кто может подать запрос на продление действия сертификата

(4.6.2)

Критерии, определяющие, кто может подать запрос на продление действия сертификата, должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 4.6.2.

7.4.6.3 Обработка запросов на продление действия сертификата

(4.6.3)

Критерии обработки запросов на продление действия сертификата должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 4.6.3.

7.4.6.4 Уведомление держателя сертификата о продлении действия сертификата

(4.6.4)

ЦС, выпускающий сертификат, должен уведомить каждого держателя сертификата о продлении действия сертификата, содержащего уникальный идентификатор данного держателя сертификата.

7.4.6.5 Действия, подтверждающие принятие продленного сертификата

(4.6.5)

Действия, подтверждающие принятие продленного сертификата, должны соответствовать 7.4.4.1.

7.4.6.6 Публикация продленного сертификата в ЦС

(4.6.6)

См. 7.2.2.

7.4.6.7 Уведомление о продлении действия сертификата, направляемое ЦС другим субъектам

(4.6.7)

См. 7.4.4.3.

7.4.7 Замена ключа в сертификате

(4.7)

Процедуры замены ключа в сертификате должны соответствовать 7.3.3.

7.4.8 Изменение сертификата

7.4.8.1 Причины изменения сертификата

(4.8.1)

Выпускающий ЦС должен изменять сертификат в следующих случаях:

- если какая-либо информация, содержащаяся в сертификате, более не соответствует действительности;
- если изменилось место работы держателя сертификата, например, квалифицированный медицинский работник уволился из конкретной организации;
- независимо от причины, если получена заявка держателя сертификата или спонсора субсидируемого поставщика медицинских услуг.

Держатели сертификата, центры регистрации и спонсоры обязаны информировать ЦС о том, что им стало известно о неточности информации, содержащейся в сертификате.

7.4.8.2 Кто может подать запрос на изменение сертификата

(4.8.2)

Изменение сертификата может быть запрошено одним или несколькими из следующих субъектов:

- держателем сертификата, на чье имя был выпущен данный сертификат;
- физическим или юридическим лицом, которое подало заявку на выпуск данного сертификата, идентифицирующего устройство или приложение;
- регистрирующим или лицензирующим органом здравоохранения, которому подведомствен держатель сертификата, являющийся квалифицированным медицинским работником;
- спонсором субсидируемого поставщика медицинских услуг;
- персоналом ЦС, выпустившего сертификат;
- персоналом ЦР, ассоциированного с ЦС, выпустившим сертификат.

7.4.8.3 Обработка запросов на изменение сертификата

(4.8.3)

Критерии обработки запросов на изменение сертификата должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.8.3.

7.4.8.4 Уведомление держателя сертификата о выпуске измененного сертификата

(4.8.4)

Уведомление держателя сертификата о выпуске измененного сертификата должно осуществляться в соответствии с 7.4.3.2.

7.4.8.5 Действия, подтверждающие принятие измененного сертификата

(4.8.5)

Действия, подтверждающие принятие измененного сертификата, должны осуществляться в соответствии с 7.4.4.1.

7.4.8.6 Публикация измененного сертификата в ЦС

(4.8.6)

Критерии публикации измененного сертификата в ЦС должны соответствовать 7.4.4.2.

7.4.8.7 Уведомление о выпуске измененного сертификата, направляемое ЦС другим субъектам

(4.8.7)

Уведомление о выпуске измененного сертификата, направляемое ЦС другим субъектам, должно производиться в соответствии с 7.4.4.3.

7.4.9 Отзыв и приостановка сертификата

(4.9)

Центры регистрации могут быть полезны при обработке запросов на отзыв сертификатов. В некоторых реализациях цифровых сертификатов, предназначенных для применения в сфере здравоохранения, центры регистрации могут инициировать или аутентифицировать запросы на отзыв сертификатов. По возможности они должны переправлять аутентифицированные запросы соответствующему ЦС. ЦР может сам инициировать запрос на отзыв (например, если квалифицированный медицинский работник временно отстранен от работы за неправильные действия, а ЦР является регистрирующим или лицензирующим органом здравоохранения). В любом случае обязанностью ЦР является аутентификация сообщения. Если ЦР, применяя те же критерии, которые использовал бы ЦС, убедится, что сообщение подлинное, то ЦР должен защищенным способом послать в ЦС сообщение, содержащее информацию, идентифицирующую сертификат, и, возможно, причину отзыва данного сертификата.

Рекомендуется, чтобы в сертификате были определены адреса мест рассылки СОС в соответствии с ИСО 17090-2:2008, пункт 7.2.8.

7.4.9.1 Причины отзыва

(4.9.1)

ЦС, выпустивший сертификат, должен отозвать его в следующих случаях:

- при неспособности держателя сертификата, нанимателя (в случае вспомогательного медицинского работника или работника поддерживающей организации) или спонсора (в случае субсидируемого поставщика медицинских услуг) выполнять обязательства, соответствующие данной политике, любому применяемому РЦС или любому иному соглашению, правилу или закону, применяемому к сертификату и действующему на данный момент;
- при знании или обоснованном предположении факта компрометации секретного ключа;
- если информация, содержащаяся в сертификате, перестала быть истинной;
- если изменилась ведомственная принадлежность держателя сертификата, например, квалифицированный медицинский работник уволился из конкретной организации;
- если ЦС установил, что процедура выпуска сертификата не соответствовала текущей политике и/или любому применимому РЦС;
- по любой причине, изложенной в запросе держателя сертификата или спонсора субсидируемого поставщика медицинских услуг.

Держатели сертификата, центры регистрации и спонсоры обязаны информировать ЦС, если им стало известно о неточности информации, содержащейся в сертификате.

7.4.9.2 Кто может подать запрос на отзыв сертификата

(4.9.2)

Отзыв сертификата может быть запрошен одним или несколькими следующими субъектами:

- держателем сертификата, для которого был выпущен данный сертификат;
- физическим или юридическим лицом, которое подавало заявку на выпуск данного сертификата, идентифицирующего устройство или приложение;
- спонсором субсидируемого поставщика медицинских услуг;
- персоналом ЦС, выпустившего сертификат;
- персоналом ЦР, ассоциированного с ЦС, выпустившим сертификат.

7.4.9.3 Процедура обработки запроса на отзыв сертификата

(4.9.3)

Получив запрос на отзыв сертификата в соответствии с 7.3.4, ЦС должен:

- удостовериться, что субъект, запрашивающий отзыв, является держателем сертификата, указанным в отзываемом сертификате;
- если субъект, запрашивающий отзыв, действует в качестве агента держателя сертификата, то убедиться, что данный субъект имеет достаточные полномочия на запрос отзыва;
- проверить причины отзыва и отозвать сертификат, если подтвердится их истинность.

7.4.9.4 Льготный срок отзыва сертификата

(4.9.4)

Любое действие, предпринимаемое в результате запроса на отзыв сертификата, должно быть начато сразу после его получения.

7.4.9.5 Срок обработки в ЦС запроса на отзыв

(4.9.5)

Отзыв сертификата должен быть инициирован ЦС сразу после получения запроса.

7.4.9.6 Требования проверки отзыва доверяющими сторонами

(4.9.6)

Доверяющие стороны должны проверять СОС перед началом использования открытого ключа другого субъекта. Обновление СОС должно проверяться по меньшей мере один раз в день.

7.4.9.7 Частота публикации СОС

(4.9.7)

Извещение об отзыве сертификатов должно публиковаться своевременно (в день отзыва) и корректироваться при любых изменениях в СОС.

7.4.9.8 Максимальная задержка СОС

(4.9.8)

Критерии максимальной задержки СОС должны быть указаны в соответствии со спецификацией IETF/RFC 3647, пункт 4.9.8.

7.4.9.9 Доступность оперативной проверки отзыва/статуса сертификата

(4.9.9)

ЦС должен обеспечить доверяющим сторонам доступ к своей службе проверки отзыва/статуса сертификата (например, с использованием СОС или ОПСС) в рабочие часы этих сторон.

7.4.9.10 Требования к оперативной проверке отзыва сертификата

(4.9.10)

Оперативная проверка отзыва (например, с помощью ОПСС) требует, чтобы держатели сертификата установили безопасное соединение с сервером оперативной проверки статуса сертификата, способным отвечать на запросы. Если этим сервером является ЦС, то тогда будет проверяться аутентичность ЦС. Вместо ЦС могут также использоваться иные контролирующие организации или внешние каталоги.

7.4.9.11 Другие доступные формы извещений об отзыве сертификатов

(4.9.11)

ЦС, выпускающий сертификаты, должен уведомлять всех держателей сертификатов об отзыве сертификата, содержащего уникальный идентификатор данного держателя сертификата (в случае сертификатов устройства или приложения уведомление должно быть направлено физическому или юридическому лицу, ответственному за их применение).

7.4.9.12 Специальные требования в связи с компрометацией ключа

(4.9.12)

В случае компрометации своего ключа ЦС должен немедленно уведомить об этом центры сертификации, которым он выпустил кросс-сертификаты или сертификаты подчиненных центров сертификации.

7.4.9.13 Причины приостановки действия сертификата

(4.9.13)

В соответствии с ПС, предназначенной для сферы здравоохранения, ЦС может приостановить действие сертификата по следующим причинам:

- проведение расследования в связи с подозрением о компрометации секретных ключей;
- незавершенное уточнение информации, содержащейся в сертификате;
- запрос держателя сертификата на приостановку действия сертификата;
- другие причины, определенные в местном домене цифровых сертификатов, применяемых в сфере здравоохранения.

7.4.9.14 Кто может подать запрос на приостановку действия сертификата

(4.9.14)

Если ЦС поддерживает приостановку действия сертификата, то она может быть запрошена одним или несколькими следующими субъектами:

- держателем сертификата, на чье имя был выпущен данный сертификат;
- физическим или юридическим лицом, которое подавало заявку на выпуск данного сертификата, идентифицирующего устройство или приложение;
- спонсором субсидируемого поставщика медицинских услуг;
- персоналом ЦС, выпустившего сертификат;
- персоналом ЦР, ассоциированного с ЦС, выпустившим сертификат;
- доверяющей стороной.

7.4.9.15 Процедуры приостановки действия сертификата

(4.9.15)

ЦС, получивший запрос на приостановку действия сертификата в соответствии с 7.4.9.13 и 7.4.9.14, должен:

- удостоверить идентичность субъекта, запрашивающего приостановку, если он является держателем сертификата или спонсором субсидируемого поставщика медицинских услуг;
- удостоверить идентичность субъекта, запрашивающего приостановку, если он является физическим или юридическим лицом, которое подавало заявку на выпуск данного сертификата, идентифицирующего устройство или приложение;
- в том случае, когда субъект, запрашивающий приостановку, выступает в качестве спонсора держателя сертификата, проверить его полномочия на подачу такого запроса;
- проверить причины приостановки и приостановить действие сертификата, если подтвердится их истинность.

7.4.9.16 Ограничение срока приостановки

(4.9.16)

Срок приостановки действия сертификата должен быть ограничен временем требуемого расследования (например, для проверки информации). Рекомендуется, чтобы срок приостановки действия сертификата не превышал десяти рабочих дней.

7.4.9.17 Уведомление о приостановке действия сертификата

(4.9.17)

ЦС, выпускающий сертификаты, должен уведомить всех держателей сертификата о приостановке действия сертификата, содержащего отличительное имя данного держателя сертификата (в случае сертификатов устройства или приложения уведомление должно быть направлено физическому или юридическому лицу, ответственному за их применение).

7.4.10 Службы статуса сертификатов

7.4.10.1 Эксплуатационные характеристики

(4.10.1)

Критерии эксплуатационных характеристик должны быть установлены в соответствии со спецификацией IETF/RFC 3647, пункт 4.10.1.

7.4.10.2 Доступность службы

ЦС должен обеспечить доверяющим сторонам доступ к своей службе проверки статуса сертификата в рабочие часы этих сторон.

7.4.10.3 Эксплуатационные свойства

(4.10.3)

Критерии эксплуатационных свойств должны быть установлены в соответствии со спецификацией IETF/RFC 3647, подраздел 4.10.3.

7.4.11 Завершение подписки

(4.11)

Критерии для завершения подписки должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 4.11.

7.4.12 Временное депонирование секретного ключа у третьего лица

(4.12)

Секретные ключи, используемые для аутентификации или электронной цифровой подписи, не должны депонироваться у третьих лиц, за исключением случаев, когда это требуется по закону.

7.5 Физические средства контроля

(5)

7.5.1 Общие сведения

Физические и процедурные средства контроля безопасности, а также средства контроля персонала должны соответствовать ИСО/МЭК 27002 (или его эквиваленту) либо утвержденным критериям аккредитации или лицензирования.

7.5.2 Физические средства контроля

(5.1)

Физические средства контроля должны соответствовать ИСО/МЭК 27002 (или его эквиваленту).

7.5.3 Процедурные средства контроля

(5.2)

Процедурные средства контроля должны соответствовать ИСО/МЭК 27002 (или его эквиваленту).

7.5.4 Средства контроля персонала

(5.3)

Средства контроля персонала должны соответствовать ИСО/МЭК 27002 (или его эквиваленту).

7.5.5 Процедуры ведения журнала аудита безопасности

(5.4)

Процедуры ведения журнала аудита безопасности должны соответствовать ИСО/МЭК 27002.

7.5.6 Архив записей

7.5.6.1 Общие сведения

(5.5)

Записи должны архивироваться в соответствии с ИСО/МЭК 27002 и с национальными законами, нормами и правилами по сохранности архивов. Медицинская информация является повторно используемой и может существовать столько же (и даже дольше), сколько и человек, к которому она относится. Это создает особую потребность в долговременном хранении записей, заверенных электронной цифровой подписью, при этом важную роль играют технологии, обеспечивающие хранение меток времени и невозможность отказа от авторства в течение длительного срока.

7.5.6.2 Типы архивированных записей

(5.5.1)

В будущем важно знать, как или почему сертификат был создан. Центры регистрации в сфере здравоохранения или их центры сертификации должны архивировать такие события, как запросы на создание или отзыв сертификатов.

7.5.6.3 Срок хранения архива

(5.5.2)

Критерии для срока хранения архива должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 5.5.2. Как отмечено выше, медицинская информация является повторно используемой и может существовать столько же (и даже дольше), сколько и человек, к которому она относится. Это создает особую потребность в долговременном хранении электронных цифровых подписей.

7.5.7 Замена ключей

(5.6)

Чтобы держатели сертификата могли безболезненно переходить от одного открытого ключа к другому, уполномоченное лицо по сертификации должно выпустить новый сертификат за 30 дней до даты замены и четко проинформировать держателей сертификата о дате, начиная с которой они должны будут использовать новый сертификат.

7.5.8 Устранение последствий компрометации и аварий

(5.7)

Процедуры аудита безопасности должны соответствовать ИСО/МЭК 27002.

7.5.9 Завершение деятельности ЦС

(5.8)

Если ЦС прекращает работу, то он должен уведомить об этом своих держателей сертификатов сразу после завершения деятельности, подготовить заключительную публикацию СОС и обеспечить продолжение хранения ключей и информации ЦС. Он также должен уведомить все центры сертификации, с которыми имеются кросс-сертификаты.

При передаче деятельности одного ЦС другому ЦС, работающему на более низком уровне гарантий, сертификаты, выпущенные ЦС, чья деятельность передается, должны быть отозваны через СОС, подписанный данным ЦС до передачи дел.

При ликвидации ЦС должны быть приняты меры по обеспечению безопасного архивирования или уничтожения записей данного ЦС.

7.6 Технические средства контроля безопасности

(6)

7.6.1 Генерация и установка пары ключей

7.6.1.1 Генерация пары ключей

(6.1.1)

Открытый и секретный ключи держателя сертификата должны быть сгенерированы одним из следующих субъектов:

- ЦС;
- доверенной третьей стороной, назначенной ЦС;
- держателем сертификата с помощью функции управления ключами или приложения, согласованного с ЦС.

Если пара ключей создана третьей стороной, то для нее должно быть обязательным применение мер по обеспечению безопасности (например, аппаратных жетонов), предотвращающих подделку пар ключей и компрометацию сгенерированных секретных ключей.

Генерация ключей должна осуществляться безопасным способом.

7.6.1.2 Доставка секретного ключа держателю сертификата

(6.1.2)

Если секретный дешифрующий ключ создан не будущим держателем сертификата, то он должен быть доставлен держателю сертификата с помощью он-лайновой транзакции в соответствии со спецификацией IETF/RFC 4211 либо иным способом с равноценной степенью защиты. ЦС либо субъект доверенной третьей стороны, генерирующий ключи, должен обладать возможностью доказательства того, что у него не осталось копий секретного ключа после передачи оригинала секретного ключа, за исключением случаев, когда такие копии хранятся в целях аварийного восстановления ключа в соответствии с 7.6.2.5.

7.6.1.3 Доставка открытого ключа издателю сертификата

(6.1.3)

Если открытый шифрующий ключ не генерируется ЦС, то он должен быть доставлен ему с помощью он-лайновой транзакции в соответствии со спецификацией IETF/RFC 4211 либо иным способом с равноценной степенью защиты.

7.6.1.4 Доставка открытого ключа ЦС доверяющим сторонам

(6.1.4)

Поскольку данный открытый ключ связан с сертификатом электронной цифровой подписи ЦС, доверяющие стороны должны иметь возможность получить его с помощью доступа к хранилищу сертификатов.

7.6.1.5 Размеры ключей

(6.1.5)

Минимальный размер ключа зависит от используемого алгоритма. При использовании алгоритма RSA минимальный размер ключа для сертификатов ЦС должен равняться 2048 битам. При использовании других алгоритмов минимальный размер ключа для сертификатов ЦС должен обеспечивать равноценную защиту. При использовании алгоритма RSA или его технологического эквивалента минимальный размер ключа для сертификатов, не принадлежащих ЦС, должен равняться 1024 битам. При использовании других алгоритмов минимальный размер ключа для сертификатов, не принадлежащих ЦС, должен обеспечивать равноценную защиту.

7.6.1.6 Генерация параметров открытого ключа и контроль качества

(6.1.6)

Параметры открытого ключа должны генерироваться ЦС либо доверенной третьей стороной.

Контроль качества параметров операционной системы возлагается на аудиторскую организацию.

7.6.1.7 Цели использования ключа в соответствии с полем использования ключа, определенным в X.509 v3

(6.1.7)

Ключи аутентификации и электронной цифровой подписи должны использоваться только для целей идентификации и/или обеспечения невозможности отказа. Для шифрования должна использоваться отдельная пара ключей.

7.6.2 Защита секретного ключа

(6.2)

7.6.2.1 Общие сведения

Настоящий стандарт рекомендует, чтобы существовали две пары ключей: одна пара — для шифрования, при этом ЦС может создавать резервную копию секретного ключа, а вторая пара ключей — для

аутентификации или электронной цифровой подписи, при этом секретный ключ ни при каких обстоятельствах не может быть депонирован.

7.6.2.2 Стандарты и средства контроля криптографического модуля

(6.2.1)

Ключи электронной цифровой подписи ЦС должны соответствовать уровню 2, определенному в [12] (либо его эквиваленту). Если ЦС медицинского учреждения (например, небольшой больницы) не выпускает перекрестные сертификаты, то соответствие уровню 2 является достаточным, пока это допускается ПС. Для обеспечения доверительных отношений между организациями ЦС должен соответствовать уровню 3 или выше.

Другие сертификаты должны соответствовать уровню 1, определенному в [12], или выше (либо его эквиваленту).

Технические средства контроля криптографического модуля должны соответствовать ИСО/МЭК 27002 (либо его эквиваленту) или утвержденным критериям аккредитации или лицензирования.

7.6.2.3 Контроль секретного ключа несколькими лицами (*n* из *m*)

(6.2.2)

Если держателем сертификата является медицинское учреждение или поддерживающая организация, то секретный ключ может быть разделен на несколько частей, контролируемых разными людьми.

7.6.2.4 Депонирование секретного ключа

(6.2.3)

Секретные ключи, используемые для аутентификации или электронной цифровой подписи, не должны депонироваться, за исключением случаев, когда это требуется по закону.

7.6.2.5 Резервное копирование секретного ключа

(6.2.4)

Рекомендуется, чтобы держатель сертификата при возможности создавал резервные копии секретных ключей, например, когда секретный ключ записан в программном жетоне.

Резервные копии секретных ключей для аутентификации и электронной цифровой подписи должны создаваться исключительно под контролем держателя сертификата. Резервные копии ключей должны храниться по местонахождению держателя сертификата (на рабочем месте, в отделе или организации).

Держатель сертификата может разрешить ЦС создавать и хранить резервную копию его секретного дешифрующего ключа. Такое резервное копирование должно осуществляться с помощью сертифицированного процесса. Резервные копии секретных ключей должны создаваться с уровнем защиты не ниже того, что требуется для основной копии.

ЦС не должен раскрывать секретные дешифрующие ключи какой-либо третьей стороне без предварительного согласия держателя сертификата, если только это не требуется по закону. Тем не менее ЦС может предлагать услуги по резервному копированию секретных ключей для целей восстановления зашифрованных данных. Поскольку квалифицированный медицинский работник или работник вспомогательной организации получает сертификат для выполнения своих обязанностей, порученных нанимателем, ЦС может в целях восстановления данных раскрыть секретные дешифрующие ключи нанимателю данного работника, если подобные действия были согласованы до выпуска сертификата.

7.6.2.6 Архив секретных ключей

(6.2.5)

Если с согласия держателя сертификата ЦС создал резервную копию секретного ключа, то данный ключ должен храниться в течение срока не меньшего, чем срок, установленный для хранения медицинских карт пациентов ведомством, обслуживаемым данным ЦС.

7.6.2.7 Передача секретного ключа в криптографический модуль и обратно

(6.2.6)

Если секретный дешифрующий ключ генерируется не в криптографическом модуле субъекта, то он должен быть передан в данный модуль в соответствии со спецификацией IETF/RFC 4211 либо иным способом с равноценной степенью защиты.

7.6.2.8 Хранение секретного ключа в криптографическом модуле

(6.2.7)

Если секретный дешифрующий ключ генерируется не в криптографическом модуле субъекта, то он должен быть передан в данный модуль в соответствии со спецификацией IETF/RFC 4211 либо иным способом с равноценной степенью защиты.

7.6.2.9 Способ активации секретного ключа

(6.2.8)

Для цифровых сертификатов, выпущенных в соответствии с ПС для сферы здравоохранения, только держатель сертификата может активировать секретный ключ.

Перед активацией секретного ключа держатель сертификата должен быть аутентифицирован криптографическим модулем или приложением, защищающим секретный ключ. Такая аутентификация может осуществляться в форме ввода пароля, идентификационной фразы, ПИН-кода или биометрических данных. Деактивированные секретные ключи должны храниться только в зашифрованном виде.

7.6.2.10 Способ деактивации секретного ключа

(6.2.9)

При деактивации ключей они должны быть удалены из памяти до ее перераспределения. Дисковое пространство, в котором хранились ключи, должно быть перезаписано прежде, чем оно будет возвращено операционной системе. Криптографический модуль должен автоматически деактивировать секретный ключ после заранее заданного периода неактивности.

7.6.2.11 Способ уничтожения секретного ключа

(6.2.10)

По окончании использования секретного ключа все копии секретного ключа в памяти компьютера и совместно используемом дисковом пространстве должны быть надежно уничтожены путем многократной перезаписи. Процедуры уничтожения секретного ключа должны быть приведены в РЦС или в публично доступном документе.

7.6.2.12 Ранжирование криптографического модуля

(6.2.11)

Ключи электронной цифровой подписи ЦС должны соответствовать уровню 2, определенному в [12] (или его эквиваленту).

Другие сертификаты должны соответствовать уровню 1, определенному в [12] (или его эквиваленту).

7.6.3 Другие аспекты управления ключами

(6.3)

7.6.3.1 Архив открытых ключей

(6.3.1)

Сертификаты открытых ключей и списки отозванных сертификатов должны архивироваться ДТС, чтобы обеспечить проверку подписи в будущем. ЦС должен гарантировать, что СОК и СОС архивируются.

7.6.3.2 Сроки действия сертификата и использования пары ключей

(6.3.2)

При выдаче сертификатов квалифицированным медицинским работникам ЦС должен проследить, чтобы срок действия сертификата не превышал срока действия профессиональной лицензии. Для выполнения этого требования ЦС должен установить срок действия сертификата, не превышающий срока действия профессиональной лицензии, либо должным образом подтвердить продление срока действия профессиональной лицензии, либо отозвать сертификат или приостановить его действие, если профессиональная лицензия не была продлена.

Срок действия открытых и секретных ключей, не принадлежащих ЦС, не должен превышать трех лет, после чего необходимо выпустить новую пару ключей. Сертификаты атрибутов могут иметь более короткий срок действия, зависящий от потребности.

Использование открытых и секретных ключей ЦС не должно длиться более десяти лет, после чего должна быть выпущена новая пара ключей.

7.6.3.3 Ограничения на использование секретного ключа ЦС

ЦС должен гарантировать, что его секретный ключ, предназначенный для подписи сертификатов, используется только для подписи сертификатов и СОС. ЦС должен гарантировать, что секретные ключи, выпущенные для его сотрудников для доступа и работы с приложениями ЦС, используются только для этих целей.

7.6.4 Данные активации

(6.4)

Данные активации должны быть уникальными, непредсказуемыми и должны передаваться держателю сертификата безопасным способом.

7.6.5 Средства контроля защиты компьютера

(6.5)

Средства контроля защиты компьютера должны соответствовать ИСО/МЭК 27002 (или его эквиваленту) либо утвержденным критериям аккредитации или лицензирования, а также следующим документам:

- IETF/RFC 3647, пункт 6.5.1 — Особые технические требования защиты компьютеров;
- IETF/RFC 3647, пункт 6.5.2 — Ранжирование защиты компьютера.

7.6.6 Технические средства контроля жизненного цикла

(6.6)

Технические средства контроля жизненного цикла должны соответствовать ИСО/МЭК 27002 (или его эквиваленту) либо утвержденным критериям аккредитации или лицензирования, а также следующим документам:

- IETF/RFC 3647, пункт 6.6.1 — Средства контроля разработки системы;
- IETF/RFC 3647, пункт 6.6.2 — Средства контроля управления безопасностью;
- IETF/RFC 3647, пункт 6.6.3 — Средства контроля безопасности жизненного цикла.

7.6.7 Средства контроля защиты сети

(6.7)

Средства контроля защиты сети должны соответствовать ИСО/МЭК 27002 (или его эквиваленту) либо утвержденным критериям аккредитации или лицензирования.

7.6.8 Метки времени

(6.8)

Критерии применения меток времени должны быть указаны в соответствии со спецификацией IETF/RFC 3647, подраздел 6.8.

7.7 Профили сертификата, СОС и ОПСС

Профили сертификата, СОС и ОПСС (при их наличии) должны соответствовать ИСО 17090-2.

7.8 Аудит соответствия

7.8.1 Общие сведения

(8)

Аудит соответствия является существенной составляющей многих моделей интероперабельности цифровых сертификатов (см., например, ИСО 17090-1:2008, пункт 9.2.4).

7.8.2 Периодичность аудита соответствия ЦС

(8.1)

ЦС, выпускающий сертификаты в соответствии с ПС для сферы здравоохранения, должен убедить любую доверяющую сторону, что они полностью соответствуют требованиям данной политики. Аудит соответствия ЦС должен осуществляться квалифицированной независимой третьей стороной с периодичностью не реже одного раза в год.

7.8.3 Идентичность/квалификация аудитора

(8.2)

Аудитор должен иметь квалификацию аудитора по информационным системам, подтвержденную соответствующим профессиональным органом (например, аккредитация по ИСО 9000). Аудитор должен обладать большим опытом в области цифровых сертификатов. Если существует формальный орган аккредитации, то аудитор должен соответствовать его требованиям.

7.8.4 Взаимосвязь аудитора с проверяемой стороной

(8.3)

Аудитор должен быть полностью независим от проверяемой стороны и принадлежать к организации, независимой от ЦС. Аудитор не должен иметь финансовый интерес в проверяемой стороне.

7.8.5 Вопросы, затрагиваемые аудитом

(8.4)

Аудиту должны подлежать такие события, как регистрация держателей сертификатов, регистрация сертификатов, публикация отчетов о скомпрометированных ключах и отзыв сертификатов. Аудит обычно охватывает их соответствие ПС и РЦС.

Чтобы гарантировать доверие к ЦР и предоставить информацию лицам, осуществляющим внутренний аудит, действия каждого ЦР должны регистрироваться. Аудиторские записи и журналы аудита должны создаваться для событий в соответствии с релевантной политикой.

7.8.6 Действия, предпринимаемые в результате выявления недостатков

(8.5)

7.8.6.1 Общие сведения

Если в процессе аудита выявлены нарушения, то ЦС должен предпринять действия по их устранению. Если ЦС не удается принять необходимые меры по устранению нарушения, то орган управления ЦС может предпринять следующие действия:

- отметить недостатки, но разрешить ЦС продолжить работу до следующего аудита, или
- разрешить ЦС продолжить работу в течение не более 30 дней для решения любых проблем до отзыва сертификата, или
- отозвать сертификат ЦС.

Любое решение относительно того, какое из указанных действий следует предпринять, должно основываться на серьезности выявленных недостатков. Однако работа ЦС не может быть остановлена, поскольку это может нарушить работу существующих служб.

7.8.6.2 Категория критического нарушения

Неспособность ЦС соответствовать основным разделам РЦС, установленная органом аккредитации ЦС (если данная аккредитация существует в ведомстве, которое обслуживается ЦС), должна классифицироваться как критическое нарушение. Например, выявление факта, что ЦС экономит на дорогостоящих процедурах и это приводит к компрометации выпускаемых сертификатов, должно классифицироваться как критическое нарушение.

Если ЦС был аккредитован ведомством, то рекомендуется немедленно отозвать данную аккредитацию.

7.8.6.3 Категория существенного нарушения

Неспособность ЦС соответствовать важным элементам РЦС, считающимся частью процесса обеспечения гарантий, должна классифицироваться как существенное нарушение. Например, установление факта, что ЦС не обеспечивает достаточной непрерывности работы, должно классифицироваться как серьезное нарушение.

Если у ЦС выявлены дополнительные нарушения этой же категории или ЦС не удается решить проблему несоответствия в течение нескольких дней, то нарушение может быть признано критическим.

7.8.6.4 Категория частного нарушения

Любое несоответствие положениям РЦС, считающимся частью процесса обеспечения гарантий, которое вряд ли перерастет в категорию существенного нарушения, но может повлиять на целостность действий ЦС, должно классифицироваться как частное нарушение. Например, устаревшие политики и процедуры обеспечения безопасности должны классифицироваться как частное нарушение.

Если у ЦС выявлены дополнительные нарушения этой же категории или ЦС не удается решить проблему несоответствия в течение 30 дней, то нарушение может быть признано существенным.

7.8.6.5 Категория незначительного нарушения

Нарушения соответствия, которые вряд ли перерастут в категорию частного нарушения, но могут снизить общее представление о целостности действий ЦС, должны классифицироваться как незначительные нарушения. Например, административные нарушения (наподобие несвоевременного выставления счетов) должны классифицироваться как незначительные нарушения.

Если у ЦС выявлены дополнительные нарушения этой же категории или ЦС не удается решить проблему несоответствия до следующей аудиторской проверки, то нарушение может быть признано частным.

7.8.7 Рассылка результатов аудита

(8.6)

Если аудитором были выявлены нарушения у какого-либо ЦС или ЦР, то об этом немедленно должны быть уведомлены держатели сертификатов и доверяющие стороны.

7.9 Юридические и другие аспекты деятельности

(9)

7.9.1 Оплата

(9.1)

Оплата должна быть определена в соответствии со спецификацией IETF/RFC 3647, подраздел 9.1.

7.9.2 Финансовая ответственность

(9.2)

Финансовая ответственность должна быть определена в соответствии со спецификацией IETF/RFC 3647, подраздел 9.2.

7.9.3 Конфиденциальность деловой информации

(9.3)

Конфиденциальность деловой информации должна быть определена в соответствии со спецификацией IETF/RFC 3647, подраздел 9.3.

7.9.4 Защита персональной информации

(9.4)

7.9.4.1 План защиты персональной информации

(9.4.1)

Критерии для плана защиты персональной информации должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 9.4.1.

7.9.4.2 Информация, считающаяся персональной

(9.4.2)

Следующая информация должна рассматриваться как персональная и защищаться как конфиденциальная:

- личные данные держателей сертификатов и регистраторов, собранные для целей идентификации, но не включенные в сертификат (например, идентификация физического лица, факты биографии, домашний адрес, контактная информация); с согласия держателя сертификата часть его персональной информации может быть опубликована в каталоге держателей сертификатов;
- секретные ключи.

ЦС должен сохранять конфиденциальность информации о причинах, вызвавших отзыв или приостановку действия сертификата любого держателя сертификата.

7.9.4.3 Информация, не считающаяся персональной

(9.4.3)

Следующая информация не должна рассматриваться как персональная или конфиденциальная:

- открытый ключ;
- роль квалифицированного медицинского работника или работника поддерживающего учреждения;
- медицинская специальность.

7.9.4.4 Обязанность защищать конфиденциальную информацию

(9.4.4)

Конфиденциальная информация должна раскрываться только в случае явного согласия держателя сертификата либо в соответствии с законодательством страны, в которой работает ЦС или ЦР.

7.9.4.5 Уведомление и согласие на использование персональной информации

(9.4.5)

Уведомление и согласие на использование персональной информации должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 9.4.5.

7.9.4.6 Раскрытие конфиденциальной информации в соответствии с судебным или административным решением

(9.4.6)

Конфиденциальная информация должна раскрываться только при предъявлении ордера инстанции, наделенной этим правом по законодательству страны, в которой работает ЦС или ЦР.

7.9.4.7 Другие обстоятельства разглашения информации — раскрытие по запросу держателя сертификата

(9.4.7)

Конфиденциальная информация должна быть раскрыта сторонам, указанным держателем сертификата в запросе, переданном по аутентифицируемой электронной почте (содержащем электронную цифровую подпись держателя сертификата) либо представленном в письменной форме с подписью держателя сертификата.

Конфиденциальная информация должна раскрываться без письменного заявления держателя сертификата только при предъявлении ордера инстанции, наделенной этим правом по законодательству страны, в которой работает ЦС или ЦР.

7.9.5 Права интеллектуальной собственности

(9.5)

Права интеллектуальной собственности должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 9.5.

7.9.6 Претензии и гарантии

(9.6)

7.9.6.1 Общие сведения

Рамки ответственности в ситуациях, перечисленных в 7.9.6.2, являются частью общей политики, в соответствии с которой центры сертификации действуют в доменах сферы здравоохранения своих стран. Эти домены, в свою очередь, являются предметом государственного регулирования и международных соглашений. Предъявляемые требования вытекают из рамок ответственности ЦС и ЦР. При

наличии ЦА его рамки ответственности могут быть отнесены к вышеуказанным либо определены в явной форме.

7.9.6.2 Претензии и гарантии ЦС

(9.6.1)

Когда ЦС, выпускающий сертификаты, публикует сертификат, то тем самым он удостоверяет, что сертификат выпущен для некоторого держателя сертификата и информация, указанная в сертификате, проверена в соответствии с ПС данного ЦС. Публикация сертификата в хранилище, к которому имеет доступ держатель сертификата, должна являться уведомлением о такой проверке.

ЦС должен предоставить каждому держателю сертификата уведомление о его правах и обязанностях в соответствии с ПС. Данное уведомление может принимать форму договора с держателем сертификата и должно содержать описание разрешенного использования сертификатов, выпущенных в соответствии с ПС, обязанности держателя сертификата в части защиты ключей, а также процедуры обмена информацией между держателем сертификата и ЦС или ЦР, включая обмен информацией об изменениях в предоставлении услуг или о существующей политике. ЦС должен уведомить держателей сертификатов о действиях, предпринимаемых при подозрении компрометации ключа, при продлении действия сертификата или замене ключа, при отмене услуги и при разрешении споров.

Ответственность ЦС, выпускающего цифровые сертификаты для применения в сфере здравоохранения, не должна ограничиваться только одними перечисленными ниже факторами:

a) ЦС должен нести ответственность за компрометацию секретного ключа в процессе распространения ключей;

b) ЦС должен отвечать за неправомерное установление связи отдельной личности с электронной цифровой подписью и другой сертификационной информацией, если только не может быть доказано, что соблюдались все документированные правила и процедуры идентификации и аутентификации. Данная ответственность распространяется на случаи, когда ЦС знал или подозревал либо должен был знать или подозревать, что данная связь может быть неправомерной;

c) ЦС должен нести ответственность за то, что сертификаты не были отозваны, хотя это требовалось правилами отзыва;

d) ЦС должен нести ответственность за то, что сертификат был отозван по причине, которая не указана в правилах отзыва.

7.9.6.3 Претензии и гарантии ЦР

(9.6.2)

Ответственность ЦР, регистрирующего потенциальных держателей сертификатов в сфере здравоохранения, не должна ограничиваться только одними перечисленными ниже факторами:

a) ЦР должен отвечать за неправомерное установление связи отдельной личности с электронной цифровой подписью и другой сертификационной информацией, если только не может быть доказано, что соблюдались все документированные правила и процедуры идентификации и аутентификации. Данная ответственность распространяется на случаи, когда ЦР знал или подозревал либо должен был знать или подозревать, что данная связь может быть неправомерной;

b) ЦР должен нести ответственность за то, что сертификаты не были отозваны, хотя это требовалось правилами отзыва.

c) ЦР должен нести ответственность за то, что сертификат был отозван по причине, которая не указана в правилах отзыва.

7.9.6.4 Претензии и гарантии держателя сертификата

(9.6.3)

Держатель сертификата в ИОК сферы здравоохранения должен:

- при подаче заявки на получение сертификата гарантировать точность представленной им информации, а при получении сертификата подтвердить, что вся информация, содержащаяся в сертификате, является истинной;

- защищать свои секретные ключи и ключевые носители (если таковые имеются) и принимать все возможные меры для предотвращения их утери, раскрытия, изменения или несанкционированного использования;

- прилагать все усилия для предотвращения утери, раскрытия или несанкционированного использования своего секретного ключа;

- немедленно уведомить ЦС и/или ЦР о любой реальной или подозреваемой утере, раскрытии или другой компрометации своего секретного ключа;

- уведомлять ЦР и/или ЦС о любом изменении информации, содержащейся в сертификате, роли или статуса в организации здравоохранения;

- ознакомиться с ПС или с документом по ИОК, в котором простым языком четко устанавливаются обязанности держателя сертификата;
- использовать пары ключей в соответствии с ПС;
- формально признать свои обязанности путем подписи соглашения держателя сертификата.

Рекомендуется, чтобы держатель сертификата, относящегося к сфере здравоохранения, также подтвердил прохождение обучения по информационной безопасности, соответствующего функциям медицинской информации, для которых будет использоваться данный сертификат.

7.9.6.5 Претензии и гарантии доверяющей стороны

(9.6.4)

Доверяющая сторона в ИОК сферы здравоохранения имеет право доверять сертификату, выданному для применения в здравоохранении, только при следующих условиях:

- цель применения сертификата соответствует ПС;
- доверие является обоснованным и добросовестным в свете всех обстоятельств, известных доверяющей стороне на данный момент;
- доверяющая сторона удостоверилась в текущей действительности сертификата, проверив, что данный сертификат не был отозван или приостановлен;
- доверяющая сторона удостоверилась в текущей действительности электронных цифровых подписей, если таковые применялись;
- признаны имеющиеся ограничения на ответственность и гарантийные обязательства.

7.9.7 Отказ от гарантийных обязательств

(9.7)

Отказ от гарантийных обязательств должен быть определен в соответствии со спецификацией IETF/RFC 3647, подраздел 9.7.

7.9.8 Ограничение ответственности

(9.8)

7.9.8.1 Ограничение ответственности ЦС

Ответственность за халатность ЦС, выпускающего цифровые сертификаты для применения в сфере здравоохранения, может быть ограничена следующим образом:

a) ЦС может не принимать на себя ответственность за потерю секретных ключей держателем сертификата;

b) ЦС может не принимать на себя ответственность за ключи, генерируемые держателем сертификата, если только они не были созданы в полном соответствии с положениями ПС в сфере здравоохранения;

c) ЦС может не принимать на себя ответственность за компрометацию секретных ключей, которые он выпускает, если только не будет доказано, что ключи были скомпрометированы в ЦС либо при генерации ключей не соблюдались документированные политики и процедуры, вследствие чего секретный ключ оказался более восприимчивым к компрометации или был действительно раскрыт;

d) ЦС может не принимать на себя ответственность за подделанные цифровые подписи, если только подделка не произошла из-за несоблюдения установленных политик и правил ПС в сфере здравоохранения или сам ЦС не допустил подделку;

e) ЦС может ограничить свою ответственность прямыми убытками, понесенными доверяющей стороной и вызванными неспособностью ЦС соответствовать положениям данной политики.

7.9.8.2 Ограничения ответственности ЦР

Ответственность ЦР, регистрирующего потенциальных держателей сертификатов для сферы здравоохранения, может быть ограничена установлением ненадлежащего исполнения обязанностей от имени ЦР.

7.9.8.3 Ограничения ответственности держателей сертификатов

Ответственность держателей сертификатов в сфере здравоохранения должна быть ограничена установлением ненадлежащего исполнения обязанностей от имени держателя сертификата.

7.9.9 Возмещение убытков

(9.9)

Возмещение убытков (если таковое предусмотрено) должно быть определено в соответствии со спецификацией IETF/RFC 3647, подраздел 9.9.

7.9.10 Сроки и прекращение полномочий

(9.10)

Сроки и прекращение полномочий должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 9.10.

7.9.11 Индивидуальные уведомления и обмен информацией с участниками

(9.11)

Индивидуальные уведомления и обмен информацией с участниками должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 9.11.

7.9.12 Поправки

(9.12)

7.9.12.1 Процедура внесения поправок

(9.12.1)

ПС и РЦС, а также любые их изменения должны быть утверждены руководящим органом ЦС.

7.9.12.2 Механизм и срок уведомления

(9.12.2)

До внесения любых изменений в конкретную ПС руководящий орган ЦС должен уведомить все центры сертификации, имеющие прямые кросс-сертификаты с данным ЦС, и запросить у них замечания.

7.9.12.3 Обстоятельства, при которых должен быть изменен ОИД

(9.12.3)

Обстоятельства, при которых должен быть изменен ОИД, должны быть определены в соответствии со спецификацией IETF/RFC 3647, пункт 9.12.3.

7.9.13 Процедуры разрешения споров

(9.13)

Процедуры разрешения споров должны быть определены в соответствии со спецификацией IETF/RFC 3647, подраздел 9.13.

7.9.14 Правовые нормы

(9.14)

Применение цифровых сертификатов в здравоохранении должно соответствовать национальным и международным юридическим требованиям согласно ИСО/МЭК 27002 (или его эквиваленту) или утвержденным критериям аккредитации или лицензирования.

7.9.15 Соответствие применяемым правовым нормам

(9.15)

Соответствие применяемым правовым нормам должно быть определено согласно спецификации IETF/RFC 3647, подраздел 9.15.

7.9.16 Прочие положения

(9.16)

7.9.16.1 Полный объем соглашения

(9.16.1)

Полный объем соглашения должен быть определен в соответствии со спецификацией IETF/RFC 3647, пункт 9.16.1.

7.9.16.2 Переуступка прав

(9.16.2)

Если происходит слияние ЦС или ЦР с другой организацией, то новая организация становится ответственной за выполнение исходного соглашения.

7.9.16.3 Частичное нарушение

(9.16.3)

ПС в сфере здравоохранения должна оговаривать, что при обнаружении факта ошибочности или необоснованности одного из разделов политики ее другие разделы должны оставаться действующими до тех пор, пока данная политика не будет изменена.

7.9.16.4 Правоприменение

(9.16.4)

Правоприменение должно быть определено в соответствии со спецификацией IETF/RFC 3647, пункт 9.16.4.

8 Модель официального отчета об ИОК

8.1 Введение

Модель официального отчета об ИОК разработана для использования ЦС в качестве вспомогательного документа, определяющего элементы ПС и/или РЦС, которые требуют особого внимания и раскрытия их сущности. Официальный отчет об ИОК может помочь ЦС реагировать на обязательные требования и вопросы доверяющих сторон. Хотя документы ПС и РЦС существенны для описания и

руководства политиками и правилами сертификации, многие держатели цифровых сертификатов, особенно потребители, находят данные документы трудными для понимания.

Поэтому рекомендуется использовать официальный отчет об ИОК.

Пример структуры официального отчета об ИОК, перечисляющий информацию, которая должна быть раскрыта, представлен в таблице 1.

8.2 Структура официального отчета об ИОК

Структура официального отчета об ИОК должна содержать разделы для каждого определенного типа документов. Каждый раздел отчета содержит описательную часть, которая может содержать гиперссылки на соответствующие разделы ПС или РЦС.

Таблица 1 — Модель официального отчета об ИОК

Тип документа	Описание документа	Требования ПС
Контактная информация ЦС	Имя, месторасположение и необходимая контактная информация	Отсутствуют
Информация и регистрация ПС	Зарегистрированный ОИД ПС	Зарегистрированный ОИД ПС Публикация ПС и РЦС (см. 7.2)
Уровень гарантий сертификата, процедуры проверки и использование	Описание уровня гарантий сертификата, выпущенного ЦС, соответствующие процедуры проверки и любые ограничения на использование сертификата	Любые ограничения на использование сертификата
Пределы доверия	Пределы доверия, если они существуют	Любые ограничения на использование сертификата (например, сертификат может использоваться только для электронной цифровой подписи, ограничения использования сертификата для поддержки невозможности отказа от авторства)
Обязанности держателя сертификата	Описание обязанностей держателя сертификата	Обязанности держателя сертификата, определенные в соответствии с 7.9.6.2
Обязанности доверяющей стороны	В какой мере доверяющая сторона обязана проверять статус сертификата и «разумно доверять» сертификату	Обязанности доверяющей стороны
Ограниченная гарантия и ограничение ответственности	Аннотации гарантии, отказов от ответственности, ограничений ответственности и любых применимых программ гарантий и страхования	Ограничения ответственности (см. 7.9.8)
Применяемые соглашения, РЦС, сертификат	Идентификация и ссылки на применяемые соглашения, РЦС, ПС и другие сопутствующие документы	Применение уточненной ПС
Политика защиты конфиденциальной информации	Описание и ссылки на применяемые законы и политику защиты конфиденциальной информации	Требуется, чтобы при данной политике ЦС соответствовали требованиям законодательства данной страны по защите конфиденциальной информации
Политика компенсации убытков	Описание и ссылка на применяемую политику компенсации убытков	Отсутствуют
Применяемые правовые нормы, претензии и разрешение споров	Положение о выборе правовых норм, процедуры урегулирования претензий и механизмов разрешения споров	Процедуры урегулирования претензий и споров

Окончание таблицы 1

Тип документа	Описание документа	Требования ПС
Аудит ЦС	Описание процесса аудита и аудиторской фирмы	Был ли сертифицирован ЦС на соответствие своей ПС
Кросс-сертификация	Описание кросс-сертификации и идентификации других ЦС, имеющих кросс-сертификацию с данным ЦС	Политика управления кросс-сертификацией
Лицензии ЦС и хранилища данных, характеристики доверия	Перечень любых государственных лицензий, средств защиты информации	Отсутствуют

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 17090-1:2008	IDT	ГОСТ Р ИСО/ТС 17090-1—2009 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Структура и общие сведения»
ИСО 17090-2:2008	—	*
ИСО/МЭК 27002	—	*
IETF/RFC 3647	—	*
IETF/RFC 4211	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] ISO/IEC 2382-8:1998, Information technology — Vocabulary — Part 8: Security

[2] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

[3] ISO/IEC 8824-1:2002, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation

[4] ISO/IEC 9594-8:2001, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks

[5] ISO/IEC 10181-1:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview

[6] ISO/IEC 13335-1, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[7] ISO/IEC 14516, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services

[8] ISO/IEC 15945, Information technology — Security techniques — Specification of TTP services to support the application digital signatures

[9] IETF/RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols

[10] IETF/RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[11] IETF/RFC 3739, Internet X.509 Public Key Infrastructure Qualified Certificates Profile

[12] U.S. government standard FIPS-140-2, level 1 and level 2

[13] ENV 13608-1, Health informatics — Security for healthcare communication — Concepts and terminology

[14] Ankey, R., CertCo. Privilege Management Infrastructure, v0.4, August 24, 1999

[15] APEC Telecommunications Working Group, Business Facilitation Steering Group, Electronic Authentication Task Group, PKI Interoperability Expert Group, Achieving PKI Interoperability, September, 1999

[16] Bernd B., Roger-France F. A Systemic Approach for Secure Health Information Systems, International Journal of Medical Informatics, 2001, p. 51—78

[17] Canadian Institute for Health Information. Model Digital Signature and Confidentiality Certificate Policies, June 30, 2001. gost.e-ecolog.ru = infostand_pki_e

[18] Drummond Group. The Healthkey Program, PKI in Healthcare: Recommendations and Guidelines for Community-Based Testing, May 2000

[19] EESSI (European Electronic Signature Standardization Iniiative), Final Report of the EESSI Expert Team 20th July 1999

[20] Feghhi, J. and Williams, P. Digital Certificates — Applied Internet Security, Addison-Wesley, 1998

[21] Government of Canada. Criteria for Cross Certification, 2000

[22] Klein, G., Lindstrom, V., Norr, A., Ribbegard, G. and Torlof, P. Technical Aspects of PKI, January 2000

[23] Klein, G., Lindstrom, V., Norr, A., Ribbegard, G., Sonnergren, E. and Torlof, P. Infrastructure for Trust in Health Informatics, January 2000

[24] SAA MP75 (Standards Australia), Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia, 1996

[25] Wilson, S. Audit Based Public Key Infrastructure, Price Waterhouse Coopers White Paper, November 2000

УДК 61:004:006:354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, инфраструктура с открытым ключом, политики по сертификатам, управление политиками, защита информации, безопасные информационные системы

Редактор *М.В. Григорьева*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 31.10.2011. Подписано в печать 21.11.2011. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 4,10. Тираж 79 экз. Зак. 1110.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru