ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/ТС 17090-1 — 2009

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 1

Структура и общие сведения

ISO/TS 17090-1:2002
Health informatics — Public key infrastructure — Part 1: Framework and overview (IDT)

Издание официальное

БЗ 8—2009/436

Москва
Стандартинформ
2010

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 Росздрава» (ЦНИИОИЗ Росздрава) и Государственным научным учреждением «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики» на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 сентября 2009 г. № 403-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/ТС 17090-1:2002 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Структура и общие свойства» (ISO/TS 17090-1:2002 «Health informatics — Public key infrastructure — Part 1: Framework and overview»).

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, 2010

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
3.1 Термины сферы здравоохранения . . . 2
3.2 Термины сферы обеспечения безопасности . . . 3
3.3 Термины, относящиеся к инфраструктуре с открытым ключом . . . 4
4 Сфера здравоохранения . . . 6
4.1 Классы участников инфраструктуры с открытым ключом в сфере здравоохранения . . . 6
4.2 Примеры участников . . . 7
4.2.1 Квалифицированный медицинский работник . . . 7
4.2.2 Вспомогательный работник здравоохранения . . . 7
4.2.3 Пациент/потребитель услуг . . . 7
4.2.4 Субсидируемый поставщик медицинских услуг . . . 7
4.2.5 Работник поддерживающей организации . . . 7
4.2.6 Организация здравоохранения . . . 7
4.2.7 Поддерживающая организация . . . 7
4.2.8 Устройства . . . 8
4.2.9 Приложения . . . 8
4.3 Применимость инфраструктуры с открытым ключом к здравоохранению . . . 8
5 Требования к сервисам обеспечения безопасности в медицинских приложениях . . . 9
5.1 Медицинские характеристики . . . 9
5.2 Технические требования к инфраструктуре с открытым ключом в сфере здравоохранения . . . 9
5.2.1 Общие положения . . . 9
5.2.2 Аутентификация . . . 9
5.2.3 Целостность . . . 10
5.2.4 Конфиденциальность . . . 10
5.2.5 Электронная подпись . . . 10
5.2.6 Авторизация . . . 10
5.2.7 Контроль доступа . . . 10
5.3 Отличие аутентификации от шифрования . . . 10
5.4 Структура управления безопасностью ИОК в индустрии здравоохранения . . . 10
5.5 Требования к политикам для ИОК в сфере здравоохранения . . . 11
6 Криптография с открытым ключом . . . 11
6.1 Симметричная и асимметричная криптография . . . 11
6.2 Цифровые сертификаты . . . 11
6.3 Электронные подписи . . . 12
6.4 Защита секретного ключа . . . 12
7 Инфраструктура с открытым ключом . . . 13
7.1 Компоненты инфраструктуры с открытым ключом . . . 13
7.1.1 Общие положения . . . 13
7.1.2 Политика по сертификатам . . . 13
7.1.3 Свод правил по сертификации . . . 13
7.1.4 Уполномоченное лицо по сертификации . . . 13
7.1.5 Уполномоченное лицо по регистрации . . . 14
7.2 Установление личности посредством аттестационных сертификатов . . . 14
7.3 Установление специализации и ролей посредством идентифицирующих сертификатов . . . 14
7.4 Использование сертификатов атрибутов для авторизации и контроля доступа . . . 15
8 Требования к операционной совместимости . . . 16
8.1 Обзор . . . 16

8.2 Возможные варианты создания ИОК в сфере здравоохранения в международном масштабе 16
8.2.1 Введение . . . 16
8.2.2 Вариант 1 — Единая иерархия ИОК . . . 16
8.2.3 Вариант 2 — Управление доверием доверяющей стороной . . . 17
8.2.4 Вариант 3 — Перекрестное распознавание . . . 17
8.2.5 Вариант 4 — Перекрестная сертификация . . . 17
8.2.6 Вариант 5 — Мост между УС . . . 18
8.3 Практическое применение вариантов . . . 18
Приложение А (справочное) Сценарии использования инфраструктуры с открытым ключом в здравоохранении . . . 19
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 26
Библиография . . . 27

Введение

В индустрии здравоохранения возникла проблема сокращения расходов путем перехода от бумажной документации к автоматизированному электронному учету. Новые модели предоставления услуг в области здравоохранения особо подчеркивают необходимость обмена информацией о пациенте между все расширяющимся кругом медицинских специалистов, выходящего за рамки традиционных организационных барьеров.

Медицинская информация, касающаяся отдельных граждан, обычно передается посредством электронной почты, доступа к удаленной базе данных, обмена данными в электронном виде и других приложений. Интернет является высокоэффективным и доступным средством обмена информацией, однако это также небезопасная среда, требующая принятия дополнительных мер для соблюдения секретности и конфиденциальности информации. Возрастает угроза разглашения медицинской информации через несанкционированный доступ (случайный или преднамеренный). Системе здравоохранения необходимо иметь надежные средства защиты информации, минимизирующие риск несанкционированного доступа.

Как же в индустрии здравоохранения обеспечивается соответствующая надежная и эффективная защита при передаче данных через Интернет? Технологии инфраструктуры с открытым ключом (ИОК) позволяют найти подход к решению данной проблемы.

ИОК является сочетанием технологических, методических и административных процессов, обеспечивающих обмен конфиденциальными данными в незащищенной среде при использовании метода «шифрования с открытым ключом» для защиты информации при передаче и «сертификатов» для подтверждения личности человека или подлинности объекта. В сфере здравоохранения, в ИОК применяются аутентификация, шифрование и электронные подписи для облегчения конфиденциального доступа и передачи индивидуальных медицинских документов, что отвечает как клиническим, так и административным потребностям. Сервисы, предоставляемые ИОК (включая шифрование, целостность информации и электронные подписи), удовлетворяют многим требованиям к системам безопасности. Особо эффективно использование ИОК в сочетании с официальным стандартом защиты информации. Многие организации во всем мире приступили к использованию ИОК для этой цели.

Функциональная совместимость технологии ИОК и поддерживающих ее политик, процедур и практических приемов имеет принципиальное значение, если обмен информацией должен происходить между организациями и медицинскими учреждениями разной подведомственности (например, между больницей и районным терапевтом, работающими с одним и тем же пациентом).

Обеспечение функциональной совместимости между разными схемами ИОК требует создания системы доверия, при которой стороны, ответственные за защиту прав на неприкосновенность личной информации, могут опереться на методики и практические приемы и, как дополнение, на подлинность электронных сертификатов, выданных другими уполномоченными учреждениями.

Многие страны внедряют ИОК для поддержки безопасного обмена информацией в пределах своих национальных границ. Несовместимость методик и практических приемов между выдающими сертификаты учреждениями и регистрационными учреждениями разных стран проявляется, если деятельность по разработке стандартов ИОК ограничена пределами национальных границ.

Технология ИОК находится в стадии активного развития по определенным направлениям, которые не ограничиваются только здравоохранением. Непрерывно проводится важнейшая работа по стандартизации и, в некоторых случаях, по правовому обеспечению. С другой стороны, поставщики медицинских услуг во многих странах уже используют или планируют использовать ИОК. Настоящий стандарт призван удовлетворить потребность в управлении данным интенсивным международным процессом.

Настоящий стандарт содержит общие технические, эксплуатационные и методические требования, которые должны быть удовлетворены для обеспечения использования ИОК для защиты обмена медицинской информацией в пределах одной сети, между сетями и за пределами границ одной юрисдикции. Его основной целью является создание основы для глобального взаимодействия.

Он изначально предназначен для поддержки международного обмена данными на основе ИОК, однако может также служить руководством для создания национальных или региональных ИОК в области здравоохранения. Интернет все шире используется как средство передачи медицинских данных между организациями здравоохранения и является единственным реальным вариантом для международного обмена данными в этой области.

Настоящий стандарт должен рассматриваться как единое целое, поскольку каждая из трех его частей вносит свой вклад в определение того, как ИОК может быть использована для обеспечения сервисов безопасности в индустрии здравоохранения, включая аутентификацию, конфиденциальность, целостность данных и технические возможности поддержки качества электронной подписи.

ИСО/ТС 17090-1 определяет основные принципы ИОК в сфере здравоохранения и определяет структуру требований по функциональной совместимости, необходимых для создания системы защищенного обмена медицинской информацией на основе ИОК.

ИСО/ТС 17090-2 определяет специфичные для сферы здравоохранения профили электронных сертификатов на основе Международного стандарта X.509, профиль которого определен в IETF/RFC 2459 для разных типов сертификатов.

ИСО/ТС 17090-3 относится к проблемам управления, возникающим при внедрении и эксплуатации ИОК в сфере здравоохранения. В нем определены структура и минимальные требования к политикам по сертификатам, а также структура сопутствующих отчетов по практическому применению сертификации. Данная часть базируется на рекомендациях IETF/RFC 2527 «Интернет X.509: Политика сертификатов инфраструктуры с открытым ключом и основы практического применения сертификации» и определяет принципы защиты информации в сфере здравоохранения при международном взаимодействии. В ней также определен необходимый минимальный уровень безопасности применительно к аспектам, специфичным для здравоохранения.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

Часть 1

Структура и общие сведения

Health informatics. Public key infrastructure. Part 1. Framework and overview

Дата введения — 2010 — 07 — 01

1 Область применения

Настоящий стандарт определяет основные понятия инфраструктуры с открытым ключом (ИОК) в сфере здравоохранения и определяет структуру требований по функциональной совместимости, необходимых для создания системы защищенного обмена медицинской информацией на основе ИОК. В нем также установлены основные стороны, обменивающиеся медицинской информацией, а также основные сервисы обеспечения безопасности, необходимые при обмене медицинской информацией, где может быть востребована ИОК.

В настоящем стандарте представлены краткое введение в шифрование с открытым ключом и базовые компоненты ИОК в сфере здравоохранения. Кроме того, в нем определены сертификаты различных типов, сертификаты подлинности открытого ключа и связанные с ними сертификаты атрибутов для участвующих сторон, самоудостоверенные сертификаты уполномоченных лиц по сертификации (УС), иерархии и объединяющие структуры уполномоченных лиц по сертификации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

ИСО 7498-2:1989 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты (ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture)

ИСО/МКЭ 9594-8:2001 Информационные технологии. Взаимосвязь открытых систем. Директория. Часть 8. Структура сертификатов открытого ключа и атрибутов (ISO/IEC 9594-8:2001, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8)

ИСО/ТС 17090-2:2002 Информатизация здоровья. Инфраструктура с открытым ключом. Часть 2. Профиль сертификата (ISO/TS 17090-2:2002, Health informatics — Public key infrastructure — Part 2: Certificate profile)

ИСО/ТС 17090-3:2002 Информатизация здоровья. Инфраструктура с открытым ключом. Часть 3. Управление политиками уполномоченного лица по сертификации (ISO/TS 17090-3:2002, Health informatics — Public key infrastructure — Part 3: Policy management of certification authority)

ИСО/МКЭ 17799:2000 Информационные технологии. Свод правил по управлению защитой информации (ISO/IEC 17799:2000, Information technology — Code of practice for information security management)

Издание официальное

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Термины сферы здравоохранения

3.1.1 **приложение** (application): Идентифицируемый и выполняемый компьютером программный процесс, владеющий секретным ключом шифрования.

Примечания

1 Приложением в данном контексте может быть любой программный процесс, используемый в медицинских информационных системах, включая процессы, не имеющие прямого отношения к лечению или диагностике.

2 В некоторых случаях в программные процессы могут быть включены управляемые медицинские устройства.

3.1.2 **устройство** (device): Идентифицируемый управляемый компьютером аппарат или прибор, владеющий секретным ключом шифрования.

Примечания

1 Данный термин относится также к классу управляемых медицинских устройств, соответствующих приведенному выше определению.

2 Устройством в данном контексте является любое устройство, используемое в медицинских информационных системах, включая устройства, не имеющие прямого отношения к лечению или диагностике.

3.1.3 **участник системы здравоохранения** (healthcare actor): Квалифицированный медицинский работник, вспомогательный работник здравоохранения, субсидируемый поставщик медицинских услуг, работник поддерживающей организации, пациент или потребитель медицинских услуг, организация здравоохранения, устройство или приложение, используемые в сфере здравоохранения и требующие сертификата для системы безопасности на основе ИОК.

3.1.4 **организация здравоохранения** (healthcare organization): Официально зарегистрированная организация, основная деятельность которой связана с предоставлением медицинских услуг и профилактикой здоровья.

Пример — Больницы, провайдеры веб-сайтов на тему здравоохранения в Интернете, медицинские исследовательские институты.

Примечания

1 Организация, которая признана несущей юридическую ответственность за свои действия, не обязана получать регистрацию на специфическую деятельность в области здравоохранения.

2 Составная часть организации называется отделением организации согласно X.501.

3.1.5 **вспомогательный работник здравоохранения** (non-regulated health professional): Лицо, работающее в организации здравоохранения, но не являющееся медицинским работником.

Пример — Регистратор или секретарь в приемной, который назначает прием, или управляющий делами, который несет ответственность за подтверждение медицинской страховки пациента.

Примечание — Тот факт, что профессиональная компетенция работника не подтверждена официально независимым от работодателя органом, конечно, не подразумевает, что работник не является специалистом в сфере выполняемых им обязанностей.

3.1.6 **пациент, потребитель** (patient, consumer): Лицо, получающее медицинские услуги и являющееся участником медицинской информационной системы.

3.1.7 **защита от несанкционированного доступа** (privacy): Защита от вмешательства в частную жизнь или дела отдельной личности в случае неуместного или незаконного сбора и использования данных об этой личности [1].

3.1.8 **квалифицированный медицинский работник** (regulated health professional): Лицо с подтвержденной уполномоченным государственным органом квалификацией для предоставления определенных медицинских услуг.

Пример — Врачи, квалифицированные медсестры, фармацевты.

Примечания

1 Типы регистрирующих или выдающих аккредитацию органов различны в разных странах и для разных профессий. К уполномоченным государственным органам относятся местные или региональные правительствен-

ные агентства, независимые профессиональные ассоциации и другие официально и в государственном масштабе уполномоченные организации. Они могут быть как местными, так и межтерриториальными.

2 Термин «уполномоченный государственный орган» в данном определении не подразумевает существование единой подконтрольной государству системы профессиональной регистрации, но для содействия международному взаимодействию предпочтительным является наличие единого общенационального справочника органов, регистрирующих медицинских работников.

3.1.9 **субсидируемый поставщик медицинских услуг** (sponsored healthcare provider): Поставщик услуг в области здравоохранения, не являющийся официально признанным специалистом по роду своей деятельности, но работающий в сфере здравоохранения и субсидируемый официальной организацией здравоохранения.

Пример — Инспектор службы наркологического просвещения, работающий с определенной этнической группой, или медико-санитарный работник в развивающейся стране.

3.1.10 **поддерживающая организация** (supporting organization): Официально зарегистрированная организация, предоставляющая услуги организации здравоохранения, но не предоставляющая сама медицинских услуг.

Пример — Органы, финансирующие систему здравоохранения, например страховые компании, поставщики фармацевтических и других товаров.

3.1.11 **работник поддерживающей организации** (supporting organization employee): Лицо, работающее в поддерживающей организации.

Пример — Работники, перезаписывающие данные медицинских карт, инспекторы страховых медицинских компаний, работники, оформляющие заказ на медикаменты.

3.2 Термины сферы обеспечения безопасности

3.2.1 **контроль доступа** (access control): Средства, обеспечивающие доступ к ресурсам системы обработки данных только авторизованным субъектам авторизованными способами [1].

3.2.2 **отслеживаемость** (accountability): Свойство, гарантирующее однозначное отслеживание действий объекта (ИСО 7498-2).

3.2.3 **асимметричный алгоритм шифрования** (asymmetric cryptographic algorithm): Алгоритм шифрования и соответствующего дешифрования, в котором для шифрования и дешифрования используются разные ключи [3].

3.2.4 **аутентификация** (authentication): Процесс достоверной идентификации субъектов информационной безопасности посредством надежной связи между идентифицируемым субъектом и его удостоверением (ИСО 7498-2).

Примечание — См. также аутентификацию происхождения данных и аутентификацию равноправных объектов.

3.2.5 **авторизация** (authorization): Предоставление прав, включая предоставление доступа на основе прав доступа (ИСО 7498-2).

3.2.6 **доступность** (availability): Свойство быть доступным и годным к использованию по запросу авторизованного субъекта (ИСО 7498-2).

3.2.7 **шифрограмма** (ciphertext): Данные, созданные путем применения шифрования, смысловое содержание которых недоступно.

Примечание — Заимствовано из ИСО 7498-2.

3.2.8 **конфиденциальность** (confidentiality): Свойство, заключающееся в том, что информация не может быть доступной или раскрытой для неавторизованных лиц, объектов или процессов (ИСО 7498-2).

3.2.9 **криптография** (cryptography): Область знаний, охватывающая принципы, средства и методы преобразования данных для сокрытия их информативного содержания с целью предотвращения их случайной модификации и/или несанкционированного использования (ИСО 7498-2).

3.2.10 **криптографический алгоритм, шифр** (cryptographic algorithm, cipher): Способ преобразования данных для сокрытия их информативного содержания с целью предотвращения их случайной модификации и/или несанкционированного использования (ИСО 7498-2).

3.2.11 **целостность данных** (data integrity): Свойство, удостоверяющее, что данные не были изменены или уничтожены неправомочным образом (ИСО 7498-2).

3.2.12 **аутентификация происхождения данных** (data origin authentication): Подтверждение того, что источник полученных данных соответствует заявленному (ИСО 7498-2).

3.2.13 **дешифрование, декодирование** (decipherment, decryption): Процесс получения из шифрограммы исходных данных [1].

Примечание — Шифрограмма может быть зашифрована вторично, и в этом случае однократное дешифрование не позволит получить исходный открытый текст.

3.2.14 **электронная подпись** (digital signature): Присоединенные данные или криптографически преобразованный блок данных, позволяющие получателю блока данных подтвердить источник и целостность блока данных и защитить их от подделки, например получателем (ИСО 7498-2).

Примечание — См. криптография.

3.2.15 **шифрование, кодирование** (encipherment, encryption): Криптографическое преобразование данных для получения шифрограммы (ИСО 7498-2).

Примечание — См. криптография.

3.2.16 **идентификация** (identification): Выполнение проверок, позволяющих системе обработки данных распознавать объекты [1].

3.2.17 **идентификатор** (identifier): Информационный объект, используемый для объявления идентичности до потенциального подтверждения соответствующим аутентификатором [7].

3.2.18 **целостность** (integrity): Гарантия того, что содержание сообщения не было случайно или преднамеренно изменено каким-либо образом в ходе передачи.

Примечание — Заимствовано из ИСО 7498-2.

3.2.19 **ключ** (key): Последовательность символов, управляющая операциями шифрования и дешифрования (ИСО 7498-2).

3.2.20 **управление ключами** (key management): Создание, хранение, распространение, удаление, архивирование и применение ключей в соответствии с политикой обеспечения безопасности (ИСО 7498-2).

3.2.21 **неоспоримость** (non-repudiation): Сервис, обеспечивающий подтверждение целостности и происхождения данных (неразрывно друг от друга) любой из участвующих сторон.

Примечание — Заимствовано из [13].

3.2.22 **секретный ключ** (private key): Ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно только одним субъектом) [3].

3.2.23 **открытый ключ** (public key): Ключ, используемый в асимметричном криптографическом алгоритме, который может быть сделан общедоступным [3].

3.2.24 **роль** (role): Поведенческий комплекс, связанный с некоторым заданием.

3.2.25 **безопасность** (security): Сочетание доступности, конфиденциальности, целостности и отслеживаемости [7].

3.2.26 **политика безопасности** (security policy): Утвержденный план или способ действий по обеспечению информационной безопасности [1].

3.2.27 **сервис безопасности** (security service): Сервис, предоставляемый уровнем взаимодействия открытых систем, обеспечивающий надлежащую степень безопасности систем или передачи данных (ИСО 7498-2).

3.3 Термины, относящиеся к инфраструктуре с открытым ключом

3.3.1 **уполномоченное лицо по атрибутам;** УА (attribute authority; AA): Уполномоченное лицо, назначающее полномочия путем выдачи сертификатов атрибутов [9].

3.3.2 **сертификат атрибута** (attribute certificate): Структура данных, заверенная электронной подписью уполномоченного лица по атрибутам, которая связывает некоторые значения атрибута с идентификацией его владельца [9].

3.3.3 **сертификат уполномоченного лица** (authority certificate): Сертификат, выданный уполномоченному лицу по сертификации или уполномоченному лицу по атрибутам.

Примечание — Заимствовано из [9].

3.3.4 **сертификат** (certificate): Сертификат открытого ключа.

3.3.5 **выдача сертификатов** (certificate distribution): Действие по выпуску и передаче сертификатов субъектам системы обеспечения безопасности.

3.3.6 **расширение сертификатов** (certificate extension): Поля расширений (называемые просто расширениями) в сертификатах по X.509, предназначенные для обеспечения способов связывания дополнительных атрибутов с пользователями или открытыми ключами и управления иерархической структурой сертификации.

Примечание — Расширения сертификата могут быть либо критическими (т.е. система, использующая сертификат, должна отклонить сертификат, если он содержит не распознаваемое системой критическое расширение), либо некритическими (т.е. не распознаваемое системой расширение может быть проигнорировано).

3.3.7 **формирование сертификатов** (certificate generation): Деятельность по созданию сертификатов.

3.3.8 **управление сертификатами** (certificate management): Процедуры, связанные с сертификатами, то есть формирование сертификатов, выдача сертификатов, архивирование и аннулирование сертификатов.

3.3.9 **профиль сертификата** (certificate profile): Спецификация структуры и допустимого содержания сертификатного типа.

3.3.10 **аннулирование сертификата** (certificate revocation): Действие по удалению всех действующих связей между сертификатом и его владельцем (или владельцем субъекта системы безопасности) по причине утери доверия к сертификату, даже при неистекшем сроке его действия.

3.3.11 **держатель сертификата** (certificate holder): Объект, признанный субъектом действующего сертификата.

3.3.12 **проверка сертификата** (certificate verification): Подтверждение того, что сертификат является подлинным.

3.3.13 **сертификация** (certification): Процедура, в соответствии с которой третья сторона предоставляет гарантию, что вся система обработки данных или ее часть соответствует требованиям обеспечения безопасности [1].

3.3.14 **уполномоченное лицо по сертификации;** УС, **эмитент сертификата** (certification authority; CA, certificate issuer): Уполномоченное лицо, которому одна или несколько участвующих сторон доверили создание и присвоение сертификатов и которое может дополнительно создавать ключи для доверяющих сторон.

Примечания

1 Заимствовано из ИСО 9594-8.

2 Под уполномоченным лицом в данном определении не подразумевается какой-либо официальный правительственный орган; ему просто выказывают доверие участвующие стороны.

3 Термин «эмитент сертификата» может быть более удачным, однако термин «уполномоченное лицо по сертификации» используется очень широко.

3.3.15 **политика по сертификатам;** ПС (certificate policy; CP): Свод правил, которому присвоено наименование, определяющий применимость сертификата к определенному сообществу и/или классу приложения с общими требованиями к обеспечению безопасности [9].

3.3.16 **свод правил по сертификации;** СПС (certification practices statement; CPS): Формулировка правил, которые уполномоченное лицо по сертификации использует при выдаче сертификатов [9].

3.3.17 **сертификат открытого ключа;** СОК (public key certificate; PKC): Сертификаты открытого ключа по X.509, связывающие удостоверение подлинности с открытым ключом; удостоверение подлинности может использоваться для поддержки принятия решений по контролю доступа, основанному на подлинности, после подтверждения клиентом наличия у него доступа к секретному ключу, соответствующему открытому ключу, содержащемуся в СОК.

Примечание — Заимствовано из [8].

3.3.18 **инфраструктура с открытым ключом;** ИОК (public key infrastructure; PKI): Инфраструктура, используемая в отношениях между держателем ключа и доверяющей стороной, которая позволяет доверяющей стороне использовать сертификат, относящийся к держателю ключа, по крайней мере, для одного применения, используя сервис системы обеспечения безопасности на основе открытого ключа. ИОК включает в себя уполномоченное лицо по сертификатам, структуру данных сертификатов, средства получения доверяющей стороной текущей информации о статусе сертификата, политику сертификации и способы проверки подлинности сертификатов при использовании.

3.3.19 **аттестационный сертификат** (qualified certificate): Сертификат, основное назначение которого состоит в идентификации личности с высокой степенью достоверности в публичных сервисах с идентификацией авторства.

Примечание — Реальные механизмы принятия решения о том, должен или нет сертификат рассматриваться как «аттестационный сертификат» в отношении какого-либо законодательства, находятся вне области применения настоящего стандарта.

3.3.20 **уполномоченное лицо по регистрации;** УР (registration authority, RA): Объект, ответственный за идентификацию и аутентификацию субъектов сертификатов, но не подписывающий и не выдающий сертификаты (то есть УР поручено выполнение определенной работы от имени УС) [9].

3.3.21 **доверяющая сторона** (relying party): Получатель сертификата, который действует, опираясь на данный сертификат и/или электронную подпись, подтвержденную посредством данного сертификата [9].

3.3.22 **третья сторона** (third party): Сторона, не являющаяся создателем или получателем данных, но необходимая для выполнения функции обеспечения безопасности как части протокола обмена информацией.

3.3.23 **доверенная третья сторона;** ДТС (trusted third party; TTP): Третья сторона, которая наделена полномочиями для реализации протокола обеспечения безопасности [7].

Примечание — Данный термин используется во многих Международных стандартах ИСО/МЭК и других документах, главным образом описывающих услуги УС. Однако это понятие шире и включает в себя такие услуги, как отсчет времени и, возможно, передачу на временное хранение.

4 Сфера здравоохранения

4.1 Классы участников инфраструктуры с открытым ключом в сфере здравоохранения

Для упрощения процесса рассмотрения требований к ИОК введены следующие классы участников. Это не означает, что другие классы и определения не являются более подходящими в ином контексте.

В данном случае внимание сосредоточено на участниках, непосредственно вовлеченных в обмен медицинской информацией, которым может потребоваться сертификат для системы обеспечения безопасности на базе ИОК. Определения участников, перечисленных ниже, приведены в 3.1.

Персонал:
- квалифицированный медицинский работник;
- вспомогательный работник здравоохранения;
- пациент/потребитель услуг;
- субсидируемый поставщик медицинских услуг;
- работник поддерживающей организации.

Организации:
- организация здравоохранения;
- поддерживающая организация.

Другие объекты:
- устройства;
- управляемые медицинские устройства;
- приложения.

Помимо перечисленных участников, для инфраструктуры с открытым ключом неотъемлемыми частями всей системы должны быть уполномоченные лица по сертификации и регистрации, являющиеся важными держателями сертификатов в данной инфраструктуре.

Некоторые работники в области здравоохранения связаны со многими организациями здравоохранения. В здравоохранении существует первостепенная необходимость избежать дублирующей или избыточной регистрации, влекущей за собой неизбежные расходы и множественность сертификатов.

В рамках сферы здравоохранения назначением УР является идентификация участника либо как удостоверенного медицинского работника, выполняющего заданную роль, либо как потребителя, обладающего правами на свою персональную информацию. Кроме того, необходимо регистрировать персонал, обслуживающий врачей частной практики (секретари в приемной, лица, выписывающие счета, регистраторы и т.д.). Данные лица не связаны с такими институтами, как больницы, которые находятся в подчинении общенациональных, государственных или региональных органов здравоохранения.

4.2 Примеры участников

4.2.1 Квалифицированный медицинский работник

Примерами квалифицированных медицинских работников являются: врачи, стоматологи, сертифицированные медсестры и фармацевты. Существует много различных классификаций официально регламентированных/аккредитованных профессий в области здравоохранения в разных странах. Важной задачей в будущей работе по стандартизации в ИСО является создание глобальной системы соответствий между этими классификациями, но в настоящем стандарте предполагается, что только самые общие классы могут быть признаны в мировом масштабе. В ИСО/ТС 17090-2 определена структура данных, допускающая параллельное использование общей международной классификации и более детализированной классификации, которая может быть национальной или соответствовать иной юрисдикции, например квалифицированные медицинские работники в некоторых странах аккредитуются в провинциях или штатах.

4.2.2 Вспомогательный работник здравоохранения

Вспомогательными работниками здравоохранения являются лица, работающие в организациях здравоохранения, но не имеющие медицинской квалификации. К ним относятся медицинские секретари, регистраторы, машинистки, перепечатывающие надиктованный текст, записанный на носителе, лица, выписывающие счет, и младшие медицинские сестры. Для настоящего стандарта важно включить взаимосвязь между нанимающей медицинской организацией и работником в сертификат для служб обеспечения безопасности. Для медицинских специалистов важно включить их взаимосвязь с профессиональным регистрирующим органом в структуре ИОК, но важным также может быть возможная должность или принадлежность к некоторой категории, например к врачам.

Существует множество различных типов ролей или должностей для работников в сфере здравоохранения, но в настоящем стандарте не определяется какая-либо классификационная схема.

Примечание — Тот факт, что профессиональная компетенция работника не подтверждена официально независимым от работодателя органом, конечно, не подразумевает, что работник не является специалистом в сфере выполняемых им обязанностей.

4.2.3 Пациент/потребитель услуг

Лицо, получающее услуги в сфере здравоохранения, преимущественно называется пациентом, но в отдельных случаях, в частности, когда речь идет о здоровом человеке или о контрактных отношениях с поставщиком медицинских услуг, более уместно называть данное лицо потребителем услуг здравоохранения. В данном контексте под пациентом/потребителем услуг понимается только непосредственный пользователь медицинской информационной системы.

4.2.4 Субсидируемый поставщик медицинских услуг

Существует несколько типов лиц, являющихся поставщиками медицинских услуг, но не регламентированных в данной юрисдикции, которые активно участвуют в сфере здравоохранения, где их профессиональная роль может быть сертифицирована и субсидирована официальной организацией здравоохранения. Примерами в некоторых странах могут быть сестры, помогающие при родах (которые могут субсидироваться акушерами или другими врачами), физиотерапевты всех видов, лица, осуществляющие уход за инвалидами и престарелыми людьми (которые могут субсидироваться врачами общей практики или больницами).

4.2.5 Работник поддерживающей организации

Работником поддерживающей организации является лицо, работающее в поддерживающей организации и не являющееся квалифицированным медицинским работником или вспомогательным работником здравоохранения.

4.2.6 Организация здравоохранения

Примерами официально зарегистрированных организаций, основная деятельность которых связана с предоставлением услуг в сфере здравоохранения или профилактикой здоровья, являются поставщики медицинских услуг, органы финансирования здравоохранения (страховые компании или органы государственной системы финансирования здравоохранения) и медицинские научно-исследовательские институты.

4.2.7 Поддерживающая организация

Поддерживающие организации предоставляют услуги организациям здравоохранения, но непосредственно не оказывают медицинских услуг.

4.2.8 Устройства

К устройствам относится оборудование, такое как аппараты ЭКГ, автоматизированное лабораторное оборудование, различное переносное диагностическое оборудование, измеряющее различные физиологические параметры пациента. Кроме того, к устройствам относится компьютерное оборудование, например серверы электронной почты, веб-серверы и серверы приложений.

4.2.9 Приложения

Приложения — это компьютерные программы, выполняемые на персональных компьютерах и/или в сетях. В сфере здравоохранения приложения могут быть частью ИОК и включать в себя интегрированные системы управления клиникой, программы электронного медицинского учета, информационную систему отделения скорой помощи, систему обработки изображений, систему управления предписанием и назначением лекарственных средств.

4.3 Применимость инфраструктуры с открытым ключом к здравоохранению

Настоящий стандарт относится к индустрии здравоохранения, как в национальном, так и в международном масштабе. Его действие распространяется на государственные (правительственные) медицинские учреждения, частных поставщиков медицинских услуг во всем диапазоне, включая больницы, санитарно-просветительскую работу и общую практику. Он также распространяется на медицинские страховые организации, медицинские образовательные учреждения и другую деятельность, связанную со здравоохранением (например, уход на дому).

Хотя основной целью настоящего стандарта является создание базовой структуры, в рамках которой медицинские работники, организации здравоохранения и страховые компании могут безопасно обмениваться медицинской информацией, он также предназначен для обеспечения возможности потребителям иметь безопасный доступ к информации об их собственном здоровье. Транзакции могут происходить при участии УС и УР, действующих как доверенные третьи стороны, чтобы обеспечить возможность обмена информацией поставщикам медицинских услуг, страховым компаниям и потребителям с гарантией безопасности, защищенности информации и немедленного оповещения в случае нарушения ее целостности.

Приложениями, подходящими для использования в рамках ИОК сферы здравоохранения, являются следующие:

a) безопасная электронная почта;

b) запросы на доступ от приложений, используемых местными медицинскими специалистами для получения информации о пациентах в информационных системах лечебных учреждений;

c) запросы на доступ от приложений, используемых в информационных системах лечебных учреждений. К таким системам могут относиться информационные системы ведения медицинских карт пациентов, управления лечением, ведения данных о патологиях, рентгенологических исследованиях, режимах питания и т.д.;

d) финансовые приложения, которые требуют идентификации авторства, целостности сообщений, конфиденциальности и аутентификации пациентов, поставщиков медицинских услуг и медицинских страховых компаний, а также (в некоторых юрисдикциях) защиты от мошенничества;

e) приложения дистанционной обработки изображений, которые требуют надежной связи между изображением и личностью пациента наряду с аутентификацией медицинского специалиста;

f) приложения контроля удаленного доступа, которые особо нуждаются в проверке аутентичности, конфиденциальности и целостности;

g) приложения электронных предписаний, которые требуют всевозможных сервисов обеспечения безопасности аутентичности ИОК, чтобы гарантировать, что данное предписание сделано конкретным медицинским работником и направлено нужному пациенту. Гарантия отсутствия ошибок при передаче требует наличия сервиса проверки целостности данных, а контролируемость процесса лечения требует сервиса идентификации авторства;

h) подписанные в электронной форме документы об информированном согласии пациента;

i) сервисы передачи информации за пределы государственных границ;

j) другие системы, соответствующие местному законодательству.

Местное законодательство может исключить одно или несколько из вышеперечисленных приложений из использования в рамках ИОК.

Некоторые сценарии применения инфраструктуры с открытым ключом детализированы в приложении А.

5 Требования к сервисам обеспечения безопасности в медицинских приложениях

5.1 Медицинские характеристики

Индустрия здравоохранения предъявляет определенные требования безопасности, которые требуют отдельного рассмотрения, что и послужило причиной создания данной технической спецификации. Далее перечислены конкретные медицинские характеристики.

a) Медицинская информация допускает многократное использование и может существовать в течение всей жизни лица, к которому относится, и даже дольше.

b) Существуют важные потребители и поставщики медицинских услуг, заинтересованные в том, чтобы полученная медицинская информация использовалась в медицинских целях и никак иначе, за исключением случаев, когда пациент дал добровольное согласие на использование данной информации (например, анонимные сведения о пациенте могут быть использованы в образовательных и исследовательских целях).

c) Существует необходимость укрепить уверенность потребителей медицинских услуг в способности системы здравоохранения оперировать их информацией.

d) Существует необходимость в том, чтобы медицинские работники и организации соблюдали обязательства по защите информации при осуществлении медицинского обслуживания.

e) Существует необходимость получить подтверждение, что медицинские работники, торговые партнеры и стороны, участвующие в инфраструктуре с открытым ключом в сфере здравоохранения, уверены в мерах обеспечения защиты личной и секретной информации о пациенте.

Необходимость защиты безопасности в сфере здравоохранения становится все более явной, по мере того как для хранения медицинской информации все чаще применяются электронные информационные системы вместо бумажной документации. Первоочередной задачей индустрии здравоохранения является защита личной неприкосновенности и безопасности пациента. В частности, данная задача подразумевает необходимость согласованности с соответствующим законом об охране частной жизни в условиях передвижения медицинской информации в международном пространстве. Если информационная система предназначается для использования и медицинскими специалистами, и пациентами/потребителями, она должна вызывать доверие. По этой причине удовлетворение требований по защите личной неприкосновенности и безопасности имеет особую важность для информационных систем в сфере здравоохранения.

5.2 Технические требования к инфраструктуре с открытым ключом в сфере здравоохранения

5.2.1 Общие положения

Основными угрозами безопасности, которые могут возникнуть для медицинских информационных и коммуникационных систем, являются несанкционированный доступ путем кражи секретного ключа у законного держателя сертификата и последующая незаконная деятельность от имени держателя сертификата. Подобный несанкционированный доступ может привести к изменению, утере или копированию медицинской информации. Инфраструктура с открытым ключом, используемая в сочетании со стандартом обеспечения безопасности, например ИСО/МЭК 17799, может значительно снизить риск несанкционированного доступа.

ИОК является единственным комплексом политики, методов и технологии, предлагающим сервисы аутентификации, целостности, конфиденциальности и электронной подписи. В рамках сферы здравоохранения ИОК дает возможность поставщикам и потребителям медицинских услуг, которые могут не знать друг друга, уверенно осуществлять безопасный обмен информацией в электронной среде, основанной на доверии.

ИОК может предложить сервисы, особо востребованные индустрией здравоохранения. Данные сервисы и их применение в здравоохранении подробно описаны ниже.

5.2.2 Аутентификация

Здравоохранение является многогранной областью интересов, и медицинские работники постоянно полагаются на компетентность других поставщиков медицинских услуг при анализе медицинских карт пациентов, результатов консилиумов и других документов, содержащих личную медицинскую информацию. Если эти документы изучаются и обновляются в электронном виде, то необходима уверенность, что содержащаяся в них информация действительно предоставлена указанными лицами.

Крайне важно, чтобы медицинские работники могли получать доступ к конфиденциальной личной медицинской информации из разных медицинских учреждений и в то же время обеспечить защиту данной

информации от доступа и изменения со стороны неавторизованных лиц. Аутентификация рассмотрена в 6.4.

5.2.3 Целостность

Поддержание целостности личной медицинской информации может буквально стать вопросом жизни и смерти, когда такая информация необходима при оказании неотложной медицинской помощи. Более того, существуют веские стимулы для нарушения целостности некоторых форм личной медицинской информации (например, при назначении наркотических средств).

5.2.4 Конфиденциальность

Личная медицинская информация часто рассматривается как наиболее конфиденциальная информация в повседневной жизни. В отличие от электронного обмена информацией в электронной торговле, конфиденциальность личной медицинской информации не может быть выражена в денежном эквиваленте, и однажды нарушенное право пациента на неприкосновенность частной жизни не может быть легко восстановлено.

5.2.5 Электронная подпись

Электронные подписи, используемые в здравоохранении, а также политики и практические приемы по подтверждению их целостности, в конечном счете могут быть объектами особого интереса в ходе слушаний на следствии, рассмотрения дел о врачебной ошибке, заседаний профессиональных дисциплинарных комитетов и других правомерных или квазиправомерных мероприятий, когда документы с электронной подписью представляются в качестве вещественных доказательств.

ИОК также поддерживает сервисы авторизации и основанного на ролях контроля доступа. Данные сервисы жизненно необходимы в сфере здравоохранения, поскольку в ней существует множество специализаций и ситуаций, требующих разных уровней доступа к фрагментам личной медицинской информации в зависимости от ситуации и роли привлеченного медицинского работника.

5.2.6 Авторизация

В сфере здравоохранения важно, чтобы права на доступ к личной медицинской информации предоставлялись только лицам, которым она необходима для лечения пациента/потребителя услуг, или другим лицам, которым дано информированное согласие пациента.

5.2.7 Контроль доступа

В сфере здравоохранения важно, чтобы имелись средства, обеспечивающие доступ к ресурсам системы обработки данных только авторизованным лицам, авторизованными способами и для авторизованных целей или функций, поскольку последствия неавторизованного доступа могут быть необратимыми.

При использовании в сочетании с соответствующим стандартом обеспечения безопасности ИОК может значительно снизить риск неавторизованного доступа к медицинской информации пациента.

Целью настоящего стандарта является определение общих элементов ИОК, которые обеспечат цепочку доверия при обмене медицинской информацией в международном масштабе.

5.3 Отличие аутентификации от шифрования

В индустрии здравоохранения существует четкая потребность отделения подписания от функции шифрования. Причина заключается в том, что авторизованным медицинским специалистам может потребоваться доступ к медицинской карте пациента в срочных или особых ситуациях, когда медицинский специалист, для которого сообщение предназначалось, отсутствует на месте или недоступен. В системе безопасности в здравоохранении обычной практикой является наличие индивидуального идентификационного сертификата, используемого для аутентификации, и сертификата организационной структуры, используемого для шифрования.

Настоящий стандарт поддерживает различение сертификатов и связанных с ними ключей, используемых для аутентификации и шифрования (обеспечивающих конфиденциальность). В нем также подтверждается необходимость иметь отдельные сертификаты для установления личности и для управления контролем доступа, привязанные к ключу аутентификации субъекта.

5.4 Структура управления безопасностью ИОК в индустрии здравоохранения

Инфраструктура с открытым ключом, необходимая для поддержки безопасного обмена медицинской информацией и доступа к данным в национальном и международном масштабе, должна поддерживаться структурой общих политик по управлению безопасностью. Чтобы обеспечить уверенность в том, что данная инфраструктура функционирует безопасно, необходимо установить нормы и правила по управлению безопасностью.

Стандарты, определяющие нормы и правила по управлению информационной безопасностью, уже существуют и являются общепринятыми. ИСО/МЭК 17799, ИСО/ТО 13335-1 [4] и спецификация COBIT [16]

устанавливают правила для идентификации рисков безопасности, а также для применения соответствующих средств управления этими рисками.

Подобные нормы и правила накладывают небольшие ограничения или не накладывают вообще никаких ограничений на сервисы, которые могут быть предоставлены инфраструктурой с открытым ключом в сфере здравоохранения, и дают подписывающему или проверяющему лицу уверенность в том, что электронная подпись не утратит актуальности из-за плохого управления безопасностью.

Поэтому настоящий стандарт ссылается на ИСО/МЭК 17799 при решении вопросов обеспечения безопасности, изложенных в [9].

5.5 Требования к политикам для ИОК в сфере здравоохранения

Требования к политикам и связанные с ними правила для ИОК в сфере здравоохранения определены в ИСО/ТС 17090-3.

6 Криптография с открытым ключом

6.1 Симметричная и асимметричная криптография

В симметричной криптографии секретный ключ используется для шифрования открытого текста в нечитаемую криптограмму. Такая зашифрованная информация может быть дешифрована с помощью того же секретного ключа посредством обратного шифрованию порядка действий. Данный тип криптографической системы широко используется для обеспечения конфиденциальности и называется симметричной системой или системой с секретным ключом.

Криптография с открытым ключом была впервые описана Уитфилдом Диффи и Мартином Хеллманом в 1976 г. В данном подходе используются два разных ключа — открытый и секретный. Любой обладатель открытого ключа может зашифровать сообщение, но не может его расшифровать. Расшифровать сообщение может только владелец секретного ключа. Невозможно вычислить секретный ключ, зная только открытый ключ, поэтому открытый ключ может быть известен всем без угрозы нарушения конфиденциальности.

Такая криптографическая система называется асимметричной. Широко используется асимметричный алгоритм RSA, названный в честь трех его изобретателей (Rivest, Shamir и Adelman), как самостоятельно, так и в сочетании с симметричными криптографическими системами. В таких гибридных системах асимметричный алгоритм используется для защиты секретного ключа симметричной криптографической системы.

Асимметричные криптографические системы могут повысить эффективность симметричных криптографических систем или виртуальных частных сетей, обеспечивая аутентификацию участвующих сторон посредством гарантированной целостности данных при обмене, а также авторизацию и контроль доступа.

Некоторые алгоритмы открытого ключа, например RSA, могут быть использованы для восстановления исходного сообщения и поэтому пригодны для защиты конфиденциальности при вышеописанном шифровании. Данный алгоритм может быть также использован в обратном направлении, когда текст, зашифрованный с помощью секретного ключа, может быть расшифрован с помощью открытого ключа. Данный принцип не подходит для защиты конфиденциальности, но может быть использован для аутентификации. Только держатель секретного ключа может создать криптограмму, которая может быть расшифрована с помощью соответствующего секретного ключа. Данное свойство может быть использовано для аутентификации источника сообщений владельцем секретного ключа.

6.2 Цифровые сертификаты

Цифровой сертификат — это структура данных, связывающая открытый ключ субъекта и один или несколько атрибутов, определяющих личность субъекта, открытые ключи субъекта и другую информацию, воспроизводимую без искажений после шифрования с использованием секретного ключа УС, выданного в соответствии с ИСО/МЭК 9594-8. Одним из атрибутов, относящихся к личности, является назначенное ей имя, по которому данный субъект может быть идентифицирован.

Субъектом может быть физическое лицо, подразделение организации, приложение, сервер или техническое устройство. Назначением цифрового сертификата является обеспечение определенной степени уверенности в том, что открытый ключ принадлежит идентифицированному субъекту и что данный субъект владеет соответствующим секретным ключом.

Степень уверенности обеспечивается уполномоченным лицом по сертификации, подписавшим цифровой сертификат своим собственным секретным ключом. Подписывая цифровой сертификат, УС берет на себя ответственность за информацию, содержащуюся в цифровом сертификате, и за обеспечение держателя сертификата определенным уровнем аутентификации.

УС выпускает сертификаты, ведет каталог сертификатов (вместе с их открытыми ключами), аннулирует сертификаты, которые могут стать недействительными, и обеспечивает своевременное информирование всех участвующих сторон об аннулировании сертификатов. Процесс управления сертификатами определен в ИСО/ТС 17090-3, в котором также определены роль УР и ограничения на тех, кто может исполнять роль УР.

6.3 Электронные подписи

Электронная подпись представляет собой присоединенные данные или криптографическое преобразование блока данных, позволяющее получателю этого блока данных подтвердить происхождение и целостность данных и защитить их от подделки, например, получателем по ИСО 7498-2.

Электронную подпись создают посредством использования секретного ключа отправителя для выполнения некоторой математической операции над посылаемым сообщением. Метод заключается в использовании секретного ключа и односторонней математической функции, известной как алгоритм хеширования, для создания хеш-кода (некоего числа) из исходного сообщения. Хеш-функция имеет свойство необратимости, заключающееся в невозможности получения исходного сообщения или секретного ключа из хеш-кода. Хеш-код присоединяют к сообщению и посылают вместе с ним. Получатель использует отрытый ключ отправителя для выполнения такой же операции над сообщением и сравнивает получавшийся в результате хеш-код с тем, который был прислан с сообщением. Если эти хеш-коды совпадают, то получатель имеет определенную степень уверенности, что сообщение было отправлено именно тем источником, который заявил об его отправке.

Поскольку секретный ключ является частью пары ключей, в которой открытый ключ связан с личностью, указанной в цифровом сертификате, то личность отправителя может быть установлена с ранее недостижимой степенью уверенности. Степень уверенности гарантируется УС, подписавшим цифровой сертификат своим собственным секретным ключом. Подписывая цифровой сертификат, УС берет на себя ответственность за информацию, содержащуюся в цифровом сертификате, и за обеспечение держателя сертификата определенным уровнем аутентификации.

Степень уверенности зависит от политик и правил УС и управления ключами участвующими сторонами.

Помимо обеспечения определенной степени уверенности при аутентификации отправителей, использование электронной подписи может гарантировать определенную степень уверенности в целостности данных при обмене, поскольку совпадение хеш-кодов может иметь место, только если сообщения, использованные для их получения, идентичны на передающей и принимающей сторонах.

6.4 Защита секретного ключа

Сертификат не связывает ключи с личностями; он связывает ключи только с именем личности. Необходимо выполнить специальные действия для полной привязки секретного ключа к личности, чтобы обеспечить возможность использования данного секретного ключа только названной личностью. Поэтому для успешного функционирования любой ИОК в сфере здравоохранения решающее значение имеет надлежащее управление секретными ключами. Если секретный ключ рассекречен, то ИОК не является больше эффективной защитой информации, передаваемой и хранимой с использованием данной пары открытого и секретного ключей. Более того, если секретный ключ УС рассекречен, то система безопасности зоны данного УС может рухнуть.

Защита секретного ключа требует сочетания управленческих процессов и технических методов. Какие бы технические средства ни использовались, защита ключа должна поддерживаться в рамках всеобщей структуры управления информационной безопасностью в соответствии с ИСО 17799.

Секретный ключ может быть защищен посредством электронного устройства, в котором он хранится и которое может осуществлять криптографические вычисления. Доступ к такому устройству держатель сертификата может получить с использованием пароля, кодовой фразы или биометрических данных. Это более надежный метод защиты секретного ключа, поскольку он не требует электрического соединения с компьютером, к нему невозможно получить доступ через сеть и в нем могут использоваться сложные алгоритмы аутентификации. Определенные типы смарт-карт могут выполнять роль подобных электронных устройств. Также возможно использование USB-устройства или подобных электронных устройств, в которых хранится только секретный ключ, а криптографический алгоритм хранится на компьютере.

Секретный ключ может также храниться на дискете. Это менее безопасно. Секретный ключ может также храниться на жестком диске рабочей станции. Это наименее безопасный способ, поскольку доступ к секретному ключу может быть осуществлен через сеть, к которой подключена рабочая станция.

Для получения доступа к секретному ключу, хранящемуся на одном из вышеперечисленных устройств, держателю сертификата либо другому устройству или приложению необходимо пройти аутентификацию, чаще всего посредством ввода пароля, кодовой фразы или биометрических данных. Существуют разные способы аутентификации, главным образом основанные на таких характеристиках аутентифицируемого, как его местонахождение, нечто ему известное, его специальность или нечто ему принадлежащее. Например, требуется ввод пароля (нечто ему известное) с использованием электронного устройства (нечто ему принадлежащее). Рекомендуется использование более одного способа аутентификации, называемое двухступенчатой аутентификацией, значительно повышающее защищенность секретного ключа.

Настоящий стандарт определяет необходимость многоуровневой защиты и устанавливает, что для более высоких уровней безопасности защита секретного ключа должна осуществляться с помощью электронных устройств. Управление секретным ключом определено подробно в ИСО/ТС 17090-3.

Перемещение личной медицинской информации между ведомствами, за пределы государственных границ с использованием незащищенной среды, например Интернет, в которой отправитель и получатель раньше не вступали в контакт и не знали друг друга лично, требует наличия способов аутентификации участвующих сторон для обеспечения того, чтобы передаваемая и хранимая информация оставалась конфиденциальной, не была изменена при передаче и чтобы ни одна из сторон не смогла позже отрицать факт отправления или получения информации. Это является основным требованием индустрии здравоохранения к сервисам обеспечения безопасности, используемым в ИОК.

7 Инфраструктура с открытым ключом

7.1 Компоненты инфраструктуры с открытым ключом

7.1.1 Общие положения

ИОК является инфраструктурой, содержащей перечисленные ниже компоненты и используемой в процессе взаимодействия между держателем ключа и участвующей стороной, включая УС, которая позволяет участвующей стороне использовать сертификат, связанный с держателем ключа, по крайней мере, для одной операции с использованием сервиса обеспечения безопасности на основе открытого ключа.

7.1.2 Политика по сертификатам

Политика по сертификатам (ПС) представляет собой поименованный свод правил, определяющий применимость сертификата в определенной отрасли здравоохранения и/или классе приложений с общими требованиями к обеспечению безопасности. Сертификаты, основанные на ПС, которая специально разработана для удовлетворения потребностей медицинской информации, поддерживают такие сервисы, как авторизация, контроль доступа и целостность информации. Специфические потребности системы здравоохранения, описанные в разделе 5, требуют, чтобы цифровые сертификаты были определены особым образом именно для нужд здравоохранения.

7.1.3 Свод правил по сертификации

Свод правил по сертификации (СПС) представляет собой формулировку правил, которые уполномоченное лицо по сертификации использует при выдаче сертификатов, реализуя ПС. Например, в СПС указаны действия, которые необходимо предпринять, когда из медицинского учреждения поступает запрос на выдачу сертификата медицинскому работнику.

7.1.4 Уполномоченное лицо по сертификации

Уполномоченное лицо по сертификации (УС) является доверенным субъектом, который подтверждает личность держателя сертификата и присваивает «персональное имя» данному держателю сертификата. УС также подтверждает правильность информации, относящейся к личности держателя сертификата, подписывая данные и таким образом подтверждая связь между именами или личностями и открытыми ключами, которые устанавливают электронную подпись для данного держателя сертификата. Некоторые из этих функций могут быть делегированы УР (см. 7.1.5), например функции подтверждения личности и присвоения персонального имени, поскольку данные функции наилучшим образом могут быть выполнены на местном уровне.

Секретный ключ может храниться на компьютере субъекта, дискете или другом носителе, например смарт-карте. Обычно доступ к ключу осуществляется держателем сертификата посредством ввода кодовой фразы.

Настоящий стандарт допускает, что медицинские учреждения могут получать услуги по сертификации разными способами. Некоторые могут осуществлять эту деятельность самостоятельно, другие могут передать полномочия на нее уполномоченным частным организациям. Кроме того, могут существовать

различные системы сертификации в зависимости от назначения выпускаемых сертификатов. Держатели сертификатов также могут иметь разные сертификаты.

В зависимости от способа организации ИОК в сфере здравоохранения в конкретной стране может существовать несколько уровней УС, выпускающих сертификаты для держателей сертификатов в медицинском учреждении, для системы здравоохранения в целом или для любого жителя этой страны.

УС должно быть общепризнанной организацией, обладающей собственной системой контроля и правил, необходимой для обеспечения требуемой степени доверия. По меньшей мере, система контроля и правил должна соответствовать ИСО 17799 (или его аналогу) и, где это возможно, принятой схеме безопасности ИОК в пределах сферы полномочий выполняемого действия.

7.1.5 Уполномоченное лицо по регистрации

Уполномоченное лицо по регистрации (УР) является субъектом, устанавливающим личности держателей сертификатов и регистрирующим их требования по сертификации, направленные УС. УР может также проверять роль, служебное положение или статус занятости держателя сертификата на соответствие информации, записанной в сертификате атрибутов. В данном случае УР может проверить, что таким атрибутом, как статус занятости (например, администрация государственной больницы), может быть другое УР, относящееся к организации, которая подтверждает профессиональную квалификацию медицинских работников (например, комитет по регистрации медицинских работников).

Идентификация роли медицинских работников может осуществляться следующими органами:

- национальными, региональными или местными органами здравоохранения (включая относящиеся к ним больницы и медицинские учреждения);
- органами по регистрации медицинских специалистов и работников здравоохранения;
- профессиональными медицинскими объединениями, например, коллегиями хирургов, психиаторов, медсестер;
- частными или государственными организациями медицинского страхования.

ИОК в сфере здравоохранения может опираться на один или несколько таких органов для подтверждения полномочий медицинских работников. Процедуры регистрации определены в ИСО/ТС 17090-3.

7.2 Установление личности посредством аттестационных сертификатов

Аттестационные сертификаты относятся к типу сертификатов, основным назначением которых является идентификация личности с высокой степенью уверенности в сервисах, использующих электронные подписи. Аттестационные сертификаты имеют особое значение для официального распознавания электронных подписей. Настоящий стандарт обеспечивает использование аттестационных сертификатов в связи с постоянно возрастающим числом стран, законодательно устанавливающих требования к поставщикам медицинских и других услуг, использующих электронные подписи, а также к лицам, ставящим и подтверждающим электронную подпись, с тем чтобы электронная подпись могла быть юридически признана.

Необходимость аттестационных сертификатов была признана Рабочей группой по разработке стандартов для сети Интернет (Internet Engineering Task Force; IETF), выпустившей соответствующий документ [10]. В данном документе установлен профиль для аттестационных сертификатов, а его целью является определение базового синтаксиса независимого от требований местного законодательства. Профиль аттестационных сертификатов используется IETF для описания формата сертификата, основным назначением которого является надежная идентификация физических лиц. Профиль аттестационных сертификатов IETF используется в настоящем стандарте как основа для поддержки аттестационных сертификатов. Профиль аттестационных сертификатов определен в ИСО/ТС 17090-2.

В сфере здравоохранения аттестационные сертификаты могут использоваться для надежной идентификации отдельных поставщиков или потребителей медицинских услуг с той степенью уверенности, которая позволит подтвердить электронную подпись данного лица. Настоящий стандарт рекомендует использовать аттестационные сертификаты для квалифицированных медицинских работников и вспомогательных работников здравоохранения.

7.3 Установление специализации и ролей посредством идентифицирующих сертификатов

Настоящий стандарт учитывает, что не все врачи одинаковы с точки зрения пациента/потребителя услуг. Пациенты/потребители услуг, имеющие разные проблемы со здоровьем, могут обращаться к разным врачам. ВИЧ/СПИД, инфекционные болезни, психические заболевания являются только некоторыми из проблем со здоровьем, когда люди вступают в отдельные отношения. В результате решение о разрешении доступа медицинского работника к конкретным данным медицинской карты пациента/потребителя услуг обычно зависит от специализации данного медицинского работника, например хирург, и его роли, например дежурный хирург отделения скорой помощи центральной городской больницы.

Важно отметить, что информация авторизации не имеет того же срока действия, что и привязка удостоверения личности к открытому ключу, и намного меньше срока первичной медицинской квалификации. Например, человек может быть профессиональным врачом со стажем 40 лет, но быть принятым на работу на должность консультирующего психиатора в конкретную больницу всего на несколько месяцев. Если информация авторизации кодируется в расширении СОК, то обычным результатом является сокращение срока действия СОК. Кроме того эмитент СОК обычно не отвечает за информацию авторизации. В данном случае эмитент СОК может иметь возможность проверить, что указанное лицо является конкретным медицинским работником, однако менее вероятно, что он имеет возможность проверить, что данное лицо занимает должность консультирующего психиатора в конкретной больнице. Это приводит к необходимости дополнительных действий со стороны эмитента СОК, чтобы получить информацию из авторитетного источника. Это может также привести к сокращению срока действия СОК, поскольку некоторая информация, содержащаяся в нем, больше не достоверна, что вызывает увеличение объема административной работы по аннулированию данного СОК и выпуску нового. По этим причинам зачастую удобнее отделить информацию авторизации от СОК. Работа по детальной спецификации сертификатов атрибутов все еще продолжается, и существует необходимость более широкого внедрения данной спецификации в индустрию программного обеспечения (см. [25]).

Хотя спецификация сертификатов атрибутов IETF описывает использование открытого ключа для подтверждения электронных подписей или операций по управлению криптографическими ключами, она устанавливает, что не все запросы и решения о предоставлении информации основаны на идентификации личности. Подобные решения, касающиеся контроля доступа, могут быть также основаны на правилах, ролях и категориях, и поэтому требовать дополнительной информации. Например, информация о медицинском работнике как о специалисте в конкретной области может быть более важной при принятии решения о доступе, чем информация о его личности. В подобных случаях информация авторизации, необходимая для поддержки принятия таких решений, может быть закодирована в расширении СОК или в отдельном сертификате атрибута согласно [25] и ИСО/ТС 17090-2.

Настоящий стандарт рекомендует, чтобы основным назначением СОК являлось подтверждение личности. Информация о личности держателя сертификата, содержащаяся в сертификатах X.509, может быть использована в качестве основания для принятия решений о предоставлении информации в ответ на запрос, посланный на сервер с определенной целью. СОК по X.509 связывает личность клиента с открытым ключом. Информация о личности может быть использована для поддержки принятия решений на основе идентификации личности, управляющих запросами и предоставлением информации, после того как держатель сертификата подтвердит, что его секретный ключ соответствует открытому ключу, содержащемуся в СОК (см. [25]).

После того как личность подтверждена, сертификаты атрибутов могут быть использованы для более подходящего управления с информацией в ситуациях, когда некоторая информация, связанная с СОК, более изменчива или недолговечна, чем остальная информация. По этой причине настоящий стандарт содержит положение о сертификатах атрибутов.

Вместе с тем данный подход сталкивается с рядом трудностей. Подробная спецификация сертификатов атрибутов все еще находится в стадии разработки, и существует необходимость более широкого внедрения данной спецификации в индустрию программного обеспечения. Более того, информация о специализации медицинского работника, например психиатрия, педиатрия и урология, имеет определенный срок действия. Кроме того, должна существовать возможность регистрации информации о роли пациента/потребителя услуг. По этим причинам в ИСО/ТС 17090-2 определено расширение идентифицирующих типов сертификатов СОК под названием HCRole.

7.4 Использование сертификатов атрибутов для авторизации и контроля доступа

Спецификация сертификатов атрибутов IETF определяет, что размещение информации авторизации в СОК нежелательно. Настоящий стандарт признает желательность многократного использования и необходимость минимизации информации, содержащейся в идентифицирующих сертификатах. Рекомендуется, чтобы информация о дополнительных ролях, групповой принадлежности, категории допуска размещалась в сопутствующих сертификатах атрибутов.

Следует отметить, что информация авторизации отличается от информации о медицинских ролях и лицензиях, которая может быть соответствующим образом включена в СОК. Роль или лицензия подразумевает некий уровень авторизации, однако сами по себе они не являются необходимой информацией авторизации. Настоящий стандарт обеспечивает использование сертификатов атрибутов для поддержки передачи информации на основе ролей относительно поставщиков медицинских услуг.

Хотя идентифицирующий сертификат, выпущенный СОК, может предписывать некоторую роль, во многих ситуациях он не содержит достаточной информации для принятия решения о разрешении доступа. Например, хотя СОК, выданный врачу от имени УР, например Хирургической Коллегии, подтверждает, что врач является хирургом, в нем обычно не содержится достаточной информации для авторизации данного врача, несмотря на то, что он является штатным сотрудником отделения скорой помощи конкретной больницы, чтобы принимать пациента в больнице.

Подобная детальная информация идентификации более успешно предоставляется посредством использования сертификата атрибута, связанного с открытым ключом медицинского работника. Медицинский работник может иметь много сертификатов атрибутов, отражающих его многочисленные роли. Такие сертификаты атрибутов обычно имеют более короткий срок действия, чем идентифицирующий сертификат.

IETF также констатирует, что информация авторизации должна быть защищена аналогично СОК и сертификат атрибута обеспечивает такую защиту. Он представляет собой просто набор атрибутов, подписанный или сертифицированный в электронной форме. Сертификат атрибута по структуре подобен СОК; основное отличие состоит в том, что он не содержит открытый ключ. Он может содержать атрибуты, определяющие групповую принадлежность, роль, категорию допуска и другую информацию по контролю допуска, относящуюся к владельцу сертификата атрибута.

Спецификация элементов данных в сертификате атрибута, соответствующая [25], определена в ИСО/ТС 17090-2. Поскольку спецификация сертификатов атрибутов все еще находится в стадии разработки, типы медицинских сертификатов атрибутов более подробно должны быть определены в последующих изданиях настоящего стандарта.

8 Требования к операционной совместимости

8.1 Обзор

Настоящий стандарт обеспечивает поддержку безопасной электронной передаче медицинской информации в международном масштабе на основе доработки документов IETF и других существующих стандартов по безопасности. Все чаще в качестве среды для международного обмена информацией используется Интернет.

Целью настоящего стандарта является определение элементов ИОК в сфере здравоохранения, необходимых для поддержки безопасного обмена медицинской информацией в международном масштабе. Для реализации международного обмена информацией он должен базироваться на Интернет-технологиях. Поэтому в качестве основы настоящего стандарта взят документ, указанный в [9], и по мере необходимости использованы другие документы IETF.

Безопасная передача медицинской информации в международном масштабе может быть обеспечена участвующими странами путем взаимного признания способов, используемых в каждой стране для реализации политик, практических приемов и процедур аккредитации УС.

Управление ИОК в сфере здравоохранения требует дальнейшей проработки и находится вне области применения настоящего стандарта. Настоящий стандарт предлагает, чтобы функциональная совместимость в международном масштабе была достигнута путем подписания серии двусторонних и многосторонних соглашений между странами, основанных на минимальных требованиях, определенных в ИСО/ТС 17090-3. В конечном счете доверяющей стороне нужны УС, чтобы установить необходимые процедуры для обеспечения использования имеющейся инфраструктуры с требуемым уровнем гарантии безопасности.

8.2 Возможные варианты создания ИОК в сфере здравоохранения в международном масштабе

8.2.1 Введение

Основной проблемой для любой ИОК, стремящейся охватить разные юрисдикции, включая государственные границы, является доверие. Доверие — это линия поведения многих сторон, основанная на политиках и практических приемах и, как продолжение, на достоверности электронных сертификатов, выданных держателю сертификата уполномоченным органом. Ниже приведен обзор возможных вариантов построения архитектуры ИОК в сфере здравоохранения.

8.2.2 Вариант 1 — Единая иерархия ИОК

С технической точки зрения это самый простой вариант. Однако нереально создать ИОК в сфере здравоохранения, охватывающую весь мир, с единым централизованным регистрирующим и выдающим сертификаты органом. Полномочия по регистрации в данном варианте могут быть переданы другому органу. Однако в этом случае структура управления может оказаться неработоспособной.

8.2.3 Вариант 2 — Управление доверием доверяющей стороной

В данном варианте на доверяющей стороне лежит ответственность за принятие решения о доверии данному УС. Этот вариант имеет свои недостатки, так как требует, чтобы принятие решения о доверии лежало на доверяющей стороне и, в некоторых случаях, это может привести к слишком высокой степени ответственности для доверяющей стороны, у которой может быть недостаточно информации для принятия обоснованного решения.

8.2.4 Вариант 3 — Перекрестное распознавание

Перекрестное распознавание представляет собой вариант урегулирования функциональной совместимости, при котором доверяющая сторона из зоны одной ИОК может использовать информацию об уполномоченном органе из зоны другой ИОК для аутентификации субъекта из зоны другой ИОК и наоборот. Обычно подобная информация об уполномоченном органе является результатом либо официального процесса лицензирования или аккредитации в рамках юрисдикции зоны другой ИОК, либо процесса официального аудита, выполняемого представительным УС (самим или по его поручению) зоны ИОК доверяющей стороны. С технической точки зрения данная информация может храниться в виде значения поля сертификата, доступного доверяющей стороне.

В отличие от перекрестной сертификации, ответственность за принятие решения о доверии зоне другой ИОК лежит на доверяющей стороне или на владельце приложения или сервиса, а не на УС, которому непосредственно доверяет доверяющая сторона. При этом не обязательно иметь подписанный договор или соглашение между зонами двух ИОК.

При перекрестном распознавании подробное отображение ПС и СПС не является необходимым. Вместо этого доверяющая сторона (посредством имеющегося приложения) принимает решение о принятии внешнего сертификата для заявленных целей в зависимости от того, был ли сертификат выдан заслуживающим доверие внешним УС.

УС считается заслуживающим доверие, если оно получило лицензию/аккредитацию от официального органа по лицензированию/аккредитации или прошло официальную проверку независимой доверенной стороной. Кроме того, доверяющая сторона должна иметь возможность в одностороннем порядке принимать обоснованное решение, опираясь на политики, установленные в ПС и СПС в зоне внешней ИОК. Следовательно, данный процесс сравнительно менее сложен, чем перекрестная сертификация, особенно в отношении политики и согласования правового обеспечения. Данный процесс по своей сути является также масштабируемым.

Однако перекрестное распознавание методологически является менее строгим, чем перекрестная сертификация, и возлагает потенциальную ответственность на доверяющую сторону, которая может быть не осведомлена обо всех возможных последствиях принятия сертификата (см. [12]).

При перекрестном распознавании принятие решения о доверии внешнему сертификату лежит на доверяющей стороне, а не на УС.

8.2.5 Вариант 4 — Перекрестная сертификация

При перекрестной сертификации принятие решений о доверии переходит к протоколам, функционирующим в рамках инфраструктуры ИОК. Данная модель является более сложной для реализации, чем варианты 1, 2 или 3, но она является более прозрачной для пользователя и, следовательно, более легкой для поддержки с позиции конечного пользователя. Это также означает, что конечный пользователь не обязан принимать на себя ответственность за принятие решения о доверии, поскольку данная функция может быть передана УС зоны данного конечного пользователя.

Перекрестная сертификация приводит к двустороннему сближению, когда зоны двух ИОК (целиком или частично) объединяются в одну более крупную зону посредством детально разработанного процесса, осуществляемого двумя представительными УС. Для иерархических ИОК представительным УС обычно является корневой УС. Однако перекрестная сертификация может также быть реализована между любыми двумя УС. В последнем случае зона каждой ИОК создает только одно УС и его абонентов. Для того чтобы перекрестная сертификация была возможна, должна иметь место совместимость на прикладном, методическом и техническом уровнях. Если это условие достигнуто, то для доверяющей стороны в зонах УС, охватываемых перекрестной сертификацией, перемещение информации является прозрачным, а за принятие решения о доверии отвечают УС.

Процесс перекрестной сертификации требует детального отображения соответствующих политик каждого УС, а необходимые для этого усилия будут возрастать в геометрической прогрессии с включением в зону ИОК каждой последующей зоны УС. Это вызывает проблемы масштабируемости. Существует также риск, что третье УС может иметь перекрестную сертификацию со вторым УС, но при этом считать политику

первого УС неподходящей. В подобной ситуации УС-3 не может исключить УС-1. В результате перекрестная сертификация больше подходит для относительно закрытых моделей здравоохранения и наилучшим образом — для открытых, но ограниченных систем. Предпочтительней всего, если зоны двух ИОК принадлежат к двум рабочим структурам, между которыми налажено тесное оперативное взаимодействие. Например, обе рабочие зоны могут совместно использовать один набор приложений и сервисов, например электронную почту и бухгалтерские прикладные программы (см. [12]).

При перекрестной сертификации принятие решения о доверии внешнему сертификату возложено на УС.

8.2.6 Вариант 5 — Мост между УС

Модель моста между УС базируется на принятии всеми УС в рамках потенциального объединения зон УС общего минимального набора стандартов. Данный минимум стандартов затем включается в их собственные ПС и СПС. Отличие данной модели от перекрестной сертификации состоит в том, что отдельные УС могут иметь свои собственные локальные требования, помимо общего минимума стандартов. Данные локальные требования не являются необходимыми для сертификатов моста от доверяющих сторон, не относящихся к зоне данного локального УС. Данная модель лучше всего работает там, где все УС имеют значительный общий интерес и готовы допустить некоторые локальные отклонения, например, в случае перекрестной сертификации между государственными и региональными уполномоченными медицинскими органами страны.

В данной модели организации могут создавать свои собственные УС, а потом решать, присоединяться к мосту между УС или нет.

В модели моста между УС принятие решения о доверии внешнему сертификату возложено на УС, а не на доверяющую сторону.

8.3 Практическое применение вариантов

Настоящий стандарт признает, что между юрисдикциями существуют административные и политические различия. Поэтому может быть принят любой из представленных выше вариантов. Какой бы вариант ни был выбран, использование настоящего стандарта при его реализации будет полезным.

Для достижения максимальной гибкости в ИСО/ТС 17090-2 определены профили для сертификатов моста и поля сертификатов УС для статуса аудита УС и аккредитации аудиторов, поддерживающие перекрестное распознавание.

Приложение А
(справочное)

Сценарии использования инфраструктуры с открытым ключом в здравоохранении

А.1 Введение

Приведенные в настоящем приложении высокоуровневые варианты реализации или сценарии представляют основные административные и технические требования к решениям по ИОК, поддерживающие широкий профиль сферы здравоохранения.

Сначала изложены общие требования, относящиеся к основным принципам обеспечения конфиденциальности и безопасности, а также к основным потребностям сферы здравоохранения. Каждый сценарий содержит:

- описание сценария или ситуации в здравоохранении, в которых требуется безопасный конфиденциальный обмен информацией;
- административные и технические требования, которым должно соответствовать решение по ИОК.

А.2 Комментарии к сценариям

Медицинские сценарии, изложенные в А.3, показывают, как ИОК может быть использована в здравоохранении. Каждый из сценариев должен:

- управляться политикой: сценарии предназначены для демонстрации того, как ИОК может обеспечивать выполнение требований сферы здравоохранения с учетом международных, национальных и местных требований с целью обеспечения использования по назначению информации, необходимой для предоставления медицинской помощи отдельным лицам и сообществам людей;
- соответствовать сфере здравоохранения: в связи с распределенным характером оказания медицинских услуг во всем мире, а также широким диапазоном лиц и организаций, которые должны активно сотрудничать для обеспечения непрерывного оказания медицинских услуг, необходимо, чтобы любая ИОК могла функционировать в разных условиях организации здравоохранения, включая лечение в больницах и на дому, государственный и частный секторы;
- быть технологически нейтральным: одной из главных целей разработки технической спецификации ИОК для сферы здравоохранения является обеспечение того, что информация может безопасно передаваться между поставщиками услуг, потребителями, страховщиками и другими участвующими сторонами независимо от поставщика, аппаратного обеспечения, операционной системы или выполняемых приложений;
- удовлетворять существующим и возникающим требованиям к конфиденциальности: если электронные медицинские приложения должны стать широко используемыми, то им должны доверять поставщики услуг и пациенты. Забота о конфиденциальности и безопасности призвана обеспечить кредит доверия;
- быть удобными в использовании: сервисы обеспечения безопасности, предоставляемые ИОК, не должны мешать выполнению авторизованной функции медицинского специалиста или организации. Если повседневная работа системы обеспечения безопасности станет слишком обременительной, то врачи попытаются игнорировать ее или не будут достаточно точно выполнять необходимые процедуры. Если это произойдет, то возникнет значительный риск нарушения безопасности.

А.3 Сервисы, иллюстрируемые медицинскими сценариями

Медицинские сервисы и сценарии представлены в таблице А.1.

Таблица А.1 — Медицинские сервисы и сценарии

Сервис	Номер сценария														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Аутентификация	X	—	X	X	X	X	X	X	X	X	X	X	X	X	X
Конфиденциальность	X	—	X	—	—	X	X	X	X	X	X	—	X	—	—
Целостность	—	X	—	X	X	—	X	X	—	—	—	—	—	X	—
Электронная подпись	—	X	—	X	X	—	—	X	—	—	X	X	X	X	X

Сценарии:
1 Доступ к медицинским картам для отделения скорой помощи
2 Временное обслуживание (скорая помощь)
3 Регистрация нового клиента
4 Передача изображений
5 Автоматическая передача результатов обследования врачу

Окончание таблицы А.1

6 Обсуждение результатов анализа с врачом 7 Обсуждение хода лечения между врачом и пациентом 8 Составление выписки по результатам лечения пациента 9 Вопрос пациента фармацевту 10 Переписка пациента с врачом 11 Дистанционный доступ к медицинской информационной системе 12 Доступ в экстренной ситуации 13 Дистанционное медицинское заключение 14 Электронный рецепт 15 Аутентификация назначения врача

А.4 Описание сценариев

А.4.1 Доступ к медицинским картам для отделения скорой помощи

Описание сценария: Пациент, прибывший из другой страны, доставлен в отделение скорой помощи. Пациент не может связно отвечать на вопросы, и историю болезни достоверно получить невозможно. Полис медицинского страхования находится в его бумажнике, а его личность установлена по паспорту.

Ситуация без ИОК:

Используя информацию из полиса медицинского страхования, дежурный врач отделения скорой помощи делает международный звонок в указанную медицинскую страховую компанию. Поскольку временные зоны различаются, врача просят перезвонить, когда откроется административный офис. Врач осматривает пациента. Причина бессвязности речи пациента неясна.

Ситуация с ИОК:

Используя информацию из полиса медицинского страхования, дежурный врач отделения скорой помощи выходит через Интернет на сайт медицинской страховой компании пациента и вводит свой электронный сертификат, идентифицируя себя в своей текущей роли как врача отделения скорой помощи. Веб-сервис медицинской страховой компании проверяет достоверность электронного удостоверения личности путем проверки подлинности электронной подписи и того, что сертификат не аннулирован и срок его действия не истек. Поскольку удостоверение личности подтверждено и соответствует существующим стандартам, оно принимается веб-сервисом медицинской страховой компании и разрешается доступ к медицинской карте пациента. Создается документирующая доступ учетная запись с датой, временем, полным именем и номером медицинской лицензии дежурного врача и идентификацией отделения скорой помощи. Врач узнает из истории болезни об аллергических реакциях, текущих назначениях лекарственных препаратов и недавних изменениях в назначениях, которые могли вызвать побочную реакцию. После осмотра пациента врач отделения скорой помощи отправляет зашифрованное сообщение с электронной подписью о посещении отделения скорой помощи в медицинскую страховую компанию, которая помещает его в электронную медицинскую карту пациента, указывая все симптомы, поставленный диагноз, оказанное лечение и предписание.

А.4.2 Временное обслуживание (скорая помощь)

Описание сценария:

Сильнов землетрясение приводит к массовым разрушениям на обширной территории города. Местные больницы и клиники также разрушены, зафиксировано огромное число раненых и погибших. Национальные службы здравоохранения не справляются с ситуацией, и приняты международные предложения по оказанию помощи.

Ситуация без ИОК:

Невозможно сразу же проверить квалификацию и лицензии медицинских работников, предлагающих помощь. Также невозможно гарантировать то, что в ранее предложенной помощи не будет отказано.

Ситуация с ИОК:

Предложения помощи от медицинских работников немедленно проверяются на достоверность посредством считывания их электронных сертификатов. Сообщения с предложением помощи не могут быть отвергнуты, поскольку они завизированы электронной подписью с использованием секретного ключа лиц, предложивших помощь.

А.4.3 Регистрация нового клиента

Описание сценария:

Собираясь уехать на срок от 6 до 12 мес в другую страну, глава семьи согласовывает условия страховки.

Будущий клиент, мистер Чарльз, собирается зарегистрировать план медицинского страхования. Он обращается к домашней странице медицинской страховой компании, на которой выложены образцы форм регистрации. Он заполняет форму и посылает ее на электронный почтовый ящик регистрационного отдела. Форма проверяется и направляется в отдел медицинского осмотра. Отдел медицинского осмотра назначает прием будущему клиенту для прохождения медосмотра, о чем информирует его письмом. Будущий клиент приходит на прием, и врач определяет, что он может стать клиентом страховой компании. Врач уведомляет об этом отдел медицинско-

го осмотра, и данная информация передается обратно в отдел регистрации клиентов. Отдел регистрации клиентов посылает мистеру Чарльзу контракт, по которому он обязуется оплачивать ежемесячный взнос, который удерживается с его текущего счета. Отдел регистрации клиентов принимает нового клиента и отправляет распоряжение о выдаче его страхового полиса с фотографией. В процессе регистрации в качестве нового клиента будущий клиент должен предъявить водительские права или другое удостоверение личности с фотографией. Когда мистер Чарльз получает новый страховой полис с фотографией, он также получает инструкции по загрузке электронного сертификата из плана медицинского страхования.

Ситуация без ИОК:

Ни новый клиент не имеет возможности надежно удостоверить свою личность для врача, ни врач не может идентифицировать себя пациенту. Хотя существуют другие средства шифрования сообщений, которыми они обмениваются, но сочетание аутентичности и конфиденциальности невозможно.

Ситуация с ИОК:

Используя выданный новый электронный сертификат, мистер Чарльз может получить доступ к службе поддержки клиентов через Интернет, включая его персональные медицинские данные, и обмениваться защищенными электронными письмами с врачом.

А.4.4 Передача изображений

Описание сценария:

Врач-специалист расшифровывает серию рентгенограмм, выведенных на экран персонального компьютера, и печатает текст заключения. У врача высокая рабочая нагрузка (10—15 пациентов в день), и он предпочитает взять часть работы на дом. Дома врач выходит через Интернет на сервер с рентгенограммами, используя свой электронный сертификат для идентификации, и загружает изображения. Во время просмотра изображений на своем компьютере врач также получает через Интернет доступ к базе медицинских данных учреждения, чтобы получить остальную медицинскую информацию о пациенте. Врач уверен в правильности изображений, поскольку применяемая программа включает в себя функцию проверки целостности с использованием алгоритма хеширования, который подтверждает целостность сообщения. Врач заносит результаты анализа изображения в заключение и применяет схему дистанционной электронной подписи заключения.

Ситуация без ИОК:

Врач не в состоянии осуществить свою аутентификацию в лечебном учреждении на том же уровне конфиденциальности, как в случае использования электронного сертификата, что означает наличие элемента риска для лечебного учреждения, так как изображение может быть передано пользователю, выдающему себя за другое лицо. Отправленные в электронном виде выводы и заключение врача подвергаются тому же риску. Врач также не может быть уверен, что загруженные изображения не пострадали от сбоев при передаче или из-за преднамеренного изменения.

Ситуация с ИОК:

Врач может аутентифицировать себя в лечебном учреждении с уровнем конфиденциальности, соответствующим действующему законодательству. Врач может быть уверен, что загруженные изображения не искажены и что он не даст заключение по искаженным изображениям. Лечебное учреждение также может доверять электронной подписи врача, подтверждающей переданное им заключение.

А.4.5 Автоматическая передача результатов обследования врачу

Описание сценария:

Во вторник пациент приходит в лабораторию, где у него берут кровь на анализ. Когда результат готов, система автоматически отправляет сообщение врачу, информируя его о готовности результатов. В четверг врач регистрируется на веб-сайте лечебного учреждения, используя свой идентификатор медицинского работника (ID) и ПИН-код (PIN), и видит, что его ожидает сообщение. Он открывает свой электронный почтовый ящик и находит в нем сообщение, в теме которого указано: «Тест на холестерин». Врач узнает из сообщения, что уровень холестерина его пациента составляет 220, что переводит пациента в категорию умеренного риска. Врач обсуждает результаты анализа с пациентом и предлагает пациенту обратиться в группу по контролю массы тела, чтобы узнать, как можно снизить уровень холестерина с помощью диет и упражнений. Врач также рекомендует пациенту проводить анализ на уровень холестерина и приходить на прием раз в полгода. Пациент просит врача внести результаты в систему электронного учета его здоровья, доступную через Интернет. Веб-сайт пациента содержит несколько ссылок на дополнительную информацию. Одна из ссылок связана с информацией по самому анализу крови на уровень холестерина, другая — с режимом, назначенным специалистами по контролю над липидами, а третья ссылка связана с рекомендациями по персональной диете на основе текущих клинических данных, которые включают в себя различные данные о пациенте (например, возраст). Рекомендации по диете содержат дальнейшие ссылки на программу по планированию изменения режима, которая поможет ему разработать собственную диету и придерживаться ее в течение 6 мес.

Ситуация без ИОК:

Лаборатория не может быть уверена, что врач получил сообщение. Нет гарантий, что сообщение не было прочитано или изменено.

Ситуация с ИОК:

Электронная подпись подтвердит врачу, что сообщение было действительно отправлено из лаборатории, и ссылки, указывающие на рекомендованные пациенту действия для контроля состояния его уровня холестерина, являются действительными. Уведомление о доставке сообщения с электронной подписью подтвердит, что врач действительно получил сообщение.

А.4.6 Обсуждение результатов анализа с врачом

Описание сценария:

Во время планового приема врач назначает пациенту клеточный анализ крови. Обсудив с пациентом удобную дату и время, врач вводит в компьютер запись о назначении, помечая, что результаты следует отправить пациенту через Интернет после того, как врач ознакомится с ними и сможет прокомментировать.

Полученные результаты в целом оказываются в пределах нормы, только один показатель слегка повышен. Врачу известно, что для данного пациента нет поводов для беспокойства, поэтому он формирует краткое примечание по этому факту и присоединяет его к заключению по результатам анализа.

Позже в тот же день пациент получает автоматическое уведомление по электронной почте, что на защищенном веб-сайте его ожидает сообщение от лаборатории или врача. Он переходит по указанному адресу веб-сайта, вводит номер своей медицинской карты и пароль, после чего получает возможность прочитать результаты анализа из лаборатории и сообщение от своего врача. Веб-сайт автоматически определяет, что это результат клеточного анализа крови, и выводит на экран ссылку на раздел медицинской энциклопедии, содержащий общее описание клеточного анализа крови и его результатов.

Ситуация без ИОК:

Не имея возможности убедиться с достаточной степенью уверенности, что электронное сообщение действительно отправлено из лаборатории или от врача, а также что оно было передано защищенным способом, пациент получает результаты по почте, замечает слегка повышенный показатель и звонит врачу для получения разъяснений. Врач принимает другого пациента и не может ответить, а у звонящего пациента назначена важная встреча. В результате они связываются, но после нескольких дней беспокойства со стороны пациента и значительного числа неудачных попыток дозвониться со стороны врача.

Ситуация с ИОК:

Результаты быстро направляются пациенту надежным и защищенным способом. Пациент имеет возможность прочитать заключение врача в его электронном сообщении и получить доступ к веб-сайтам для получения необходимой информации, поэтому его беспокойство быстро исчезает и без телефонного разговора с врачом.

А.4.7 Обсуждение хода лечения между врачом и пациентом

Описание сценария:

У клиента с определенным планом медицинского страхования возникает вопрос о ходе его лечения. Он регистрируется на веб-сайте своего врача, используя удостоверенный электронный сертификат для аутентификации, заполняет форму запроса, и нажимает «Отправить» для начала переписки:

Здравствуйте, д-р С.

Вчера Вы сказали мне, что надо менять повязку на ране. Но я не помню, как часто мне необходимо ее менять. Вы сказали что-то вроде того, что ее не нужно менять слишком часто, но я не помню, раз в неделю или как-то иначе. Также я забыл спросить Вас, как Вы думаете, останется ли большой шрам после нее?

Через два часа консультирующая медсестра из информационного центра читает сообщение пациента и решает, что оно не срочное и на него должен ответить сотрудник бригады первой медико-санитарной помощи. Вскоре после этого сообщение появляется на экране компьютера сотрудника бригады первой помощи, который вводит ответ и визирует сообщение электронной подписью. На следующее утро пациент снова регистрируется на веб-сайте своего врача и читает сообщение:

Здравствуйте, [имя пациента].

В течение следующих двух недель меняйте повязку раз в 4 — 5 дней, если она не мокнет, в противном случае меняйте по мере намокания. После этого Вы можете связаться со мной снова, и мы обсудим дальнейшие действия. Что касается шрама, я думаю, у Вас навсегда останется шрам, но небольшой — всего лишь небольшая линия.

Ситуация без ИОК:

Отсутствие надежной методики аутентификации означает, что лечебное учреждение, в котором работает врач, не имеет возможности проверить, что именно данный пациент отправил электронное сообщение, а не кто-нибудь еще пытается получить бесплатный совет. Пациент также не может быть уверен, что ответ действительно был отправлен врачом, что он не был перехвачен и прочитан кем-либо еще.

Ситуация с ИОК:

Медицинская страховая компания и врач могут быть уверены в защищенности переписки, которую они ведут с идентифицированным и действительным клиентом одного из их планов медицинского страхования. Пациент может быть уверен, что именно его врач направил ему назначение и ведет с ним переписку.

А.4.8 Составление выписки по результатам лечения пациента

Описание сценария:

Регистратура больных диабетом собирает клинические данные из различных медицинских информационных систем о пациентах, страдающих диабетом. Установленные правила, которыми руководствуется регистрату-

ра, позволяют создать индивидуальное заключение, суммирующее общее состояние пациента, историю его болезни, факторы риска и дальнейшие шаги. Данное заключение после его просмотра врачом передается пациенту через веб-сайт медицинского учреждения. Пациент регистрируется на этом веб-сайте, используя электронный сертификат, выданный УС данного медицинского учреждения. Когда пациент просматривает заключение, включенные в него гипертекстовые ссылки позволяют пациенту легко получить соответствующую информацию (например, расписание консультаций, описание анализов, разъяснения пациенту), записаться на прием или отправить сообщение врачу. Система гарантирует, что пациент получил заключение.

Ситуация без ИОК:

Нельзя обеспечить достаточную степень уверенности пациента в том, что веб-сайт действительно принадлежит регистратуре больных диабетом и что взаимодействие с данным сайтом происходит конфиденциально. Регистратура не может быть уверена, что именно данный пациент осуществил доступ к сайту и получил информацию.

Ситуация с ИОК:

ИОК позволяет пациенту и регистратуре идентифицировать друг друга, вести конфиденциальное общение. Регистратура может быть уверена, что именно данный пациент осуществил доступ к сайту и получил информацию.

А.4.9 Вопрос пациента фармацевту

Описание сценария:

У семилетней дочери клиента страховой медицинской компании астма. Педиатр недавно прописал ей интал, но клиент не может определить, когда ингалятор пуст, а когда наполнен. Он заходит на веб-сайт своего медицинского учреждения в поисках информации об этом, но ему еще не все понятно, и он направляет вопрос дежурному фармацевту, как определить, когда ингалятор пуст.

Дежурный фармацевт использует электронную почту с доступом к каталогу медицинской ИОК, в котором хранятся электронный сертификат и открытый ключ клиента, и посылает зашифрованное сообщение, используя шаблон, предусмотренный для данного вопроса, а также добавляет несколько строчек от себя и телефонный номер для связи, если все еще останутся вопросы.

Ситуация без ИОК:

Фармацевт не может аутентифицировать клиента медицинской страховой компании с достаточной степенью достоверности. Имеется возможность отправить защищенное сообщение, но оно не может быть аутентифицировано.

Ситуация с ИОК:

Имеется возможность аутентифицировать клиента и отправить ему зашифрованное сообщение. Клиент может быть уверен, что оно пришло именно от фармацевта.

А.4.10 Переписка пациента с врачом

Описание сценария:

У пациента появляется сыпь, и он посещает дерматолога, который прописывает мазь. Дерматолог говорит пациенту, что если сыпь не пройдет в течение трех недель, ему необходимо сообщить об этом врачу, чтобы тот выписал другое лекарство.

Три недели спустя сыпь выглядит практически так же, поэтому пациент регистрируется на веб-сайте врачебной практики, воспользовавшись своим медицинским электронным сертификатом для аутентификации. Пациент отправляет врачу защищенное неструктурированное сообщение:

Я применял эту мазь уже в течение трех недель, и улучшений не последовало. Что мне теперь делать?

Врач выписывает новое назначение и сообщает пациенту, что он может купить мазь в аптеке или заказать через Интернет.

Когда пациент читает сообщение от дерматолога на защищенном веб-сайте, он просто переходит в раздел заказов данного сайта и заказывает мазь с доставкой на дом.

Ситуация без ИОК:

Врач не может с достаточной степенью уверенности аутентифицировать пациента, чтобы дать рекомендации по электронной почте о действиях в данной ситуации.

Ситуация с ИОК:

Врач и пациент могут аутентифицировать себя друг другу, а также фармацевту. Конфиденциально могут быть осуществлены обмен сообщениями и заказ новой мази в аптеке. Все стороны уверены, что отправили свои сообщения по нужным адресам.

А.4.11 Дистанционный доступ к медицинской информационной системе

Описание сценария:

Врач настраивает функции обработки результатов обследований в медицинской информационной системе своей организации. Он использует возможности системы для:

- просмотра результатов анализов;
- уведомления пациентов о результатах их анализов с помощью автоматических писем или электронных сообщений, содержащих и персональные комментарии врача;
- направления на новые анализы;

- назначения новых лекарств;
- изменения дозировки лекарств.

Пациенты получают уведомления по телефону, в письме или по электронной почте о новом входящем сообщении для них на защищенном веб-сайте организации.

Система помечает просмотренные результаты анализов как:
- подписанные (просмотренные),
- с отправкой уведомления пациенту,
- зарегистрированные,
- обработанные.

Ситуация без ИОК:

Невозможность аутентифицировать личность врача с достаточной степенью уверенности делает вышеприведенный обмен данными невозможным.

Ситуация с ИОК:

Безотказное подтверждение источника отправления и факта получения сообщения, целостность и конфиденциальность этих действий и сообщений обеспечиваются медицинской информационной системой и веб-сайтом, использующими ИОК медицинского учреждения.

А.4.12 Доступ в экстренной ситуации

Описание сценария:

Врач скорой помощи осматривает пациента, доставленного в отделение скорой помощи в полубессознательном состоянии. У пациента бессвязная речь, и он не может объяснить, что случилось. Между тем возможных причин данного состояния много, оно могло быть вызвано физической травмой или осложнением после нее, или лекарственными препаратами для лечения психических заболеваний. Жизни пациента угрожает опасность, и важно ознакомиться с его историей болезни (включая возможное применение каких-либо наркотических средств), а также со всеми выписанными ему лекарственными препаратами. В США, например, назначение метадона, возможно, будет скрыто от общего доступа, поскольку это предусмотрено Государственной законодательной программой борьбы с алкоголизмом и наркоманией. Врач начинает процесс получения доступа к информации о назначениях медикаментов пациенту, включая закрытую информацию. Система использует аутентификацию ИОК, а также данные электронного сертификата врача для создания учетной записи об экстренном доступе к закрытой информации.

Врач скорой помощи видит, что у пациента были случаи применения кокаина и амфетаминов и что ему прописан литий. Он действует согласно предписаниям, убедившись, что диагноз и лечение установлены в самые сжатые сроки. Полный отчет о регистрации экстренного доступа будет сформирован отделом информационной безопасности и/или комитетом по безопасности.

Ситуация без ИОК:

В зависимости от степени защиты файла с данными пациента врач, не являющийся лечащим врачом пациента, может не получить доступа к данным. Данная ситуация может быть опасна для жизни пациента. Если врач смог получить доступ к данным без электронного сертификата, нет возможности установить связь степени конфиденциальности сеанса доступа к данным и личности врача, осуществляющего доступ.

Ситуация с ИОК:

Врач может аутентифицировать себя в системе, используя свой электронный сертификат, и получить необходимую информацию о пациенте. Однако сохраняется контрольная запись, которая впоследствии может быть проанализирована в случае какого-либо несанкционированного доступа.

А.4.13 Дистанционное медицинское заключение

Описание сценария:

Врач диктует заключение по результатам осмотра одного из своих пациентов по телефону в компанию ABC Transcription Service в штате Вирджиния, США, которая связана условиями контракта с больницей Toronto Memorial Hospital в Канаде, куда пациент госпитализирован в настоящее время. Диктуемый текст принимается и записывается медицинским стенографистом в Индии, работающим на условиях субконтракта, который отправляет его на защищенный веб-сайт компании ABC Transcription Service. После того как данный документ был проверен и одобрен рецензентом компании, его снова отправляют на защищенный веб-сайт компании и соответствующее должностное лицо в Toronto Memorial Hospital получает уведомление по электронной почте, что документ доступен. Он отправляет документ на защищенный веб-сайт больницы и, в свою очередь, сообщает врачу, что документ доступен для просмотра. После получения доступа, просмотра и аутентификации со стороны врача документ добавляется к электронной медицинской карте пациента.

Ситуация без ИОК:

Ни один из участников информационного обмена не может аутентифицировать себя с достаточной степенью достоверности для реализации взаимодействия.

Ситуация с ИОК:

Аутентификация всех авторизованных сторон и конфиденциальность медицинской информации гарантированы. Кроме того, никто впоследствии не сможет отрицать факт участия в обмене информацией.

А.4.14 Электронный рецепт

Описание сценария:

По окончании приема врач оформляет в электронном виде рецепт для пациента. Система электронных рецептов проверяет, что выписанные лекарства имеются в фармакологическом справочнике, что у пациента нет установленных аллергических реакций на данные лекарства, проверяет взаимодействие с другими лекарствами, которые пациент может принимать, и соответствие назначенных дозировок рекомендуемым. Врач ставит электронную подпись на рецепте и передает его в аптеку, выбранную пациентом. Аптека получает рецепт, проверяет медицинские полномочия и электронную подпись врача, оформляет и архивирует рецепт. Когда пациент приходит в аптеку, назначенные лекарства для него уже приготовлены.

Ситуация без ИОК:

Невозможно аутентифицировать врача. Кроме того, впоследствии врач может отрицать, что он посылал электронный рецепт.

Ситуация с ИОК:

Аптека может проверить личность и полномочия врача и тот факт, что именно данный врач отправил данный рецепт. Впоследствии врач не сможет отрицать факт отправки данного электронного рецепта.

А.4.15 Аутентификация назначения врача

Описание сценария:

Пациент приходит в кабинет врача с жалобой на боли в области желудка в течение уже нескольких месяцев. Пациент сообщает, что боль уменьшается после еды и после приема антацидов, но постоянна и регулярно повторяется. После первичного осмотра врач подозревает пептическую язву и решает направить пациента на гастроэнтероскопию. С компьютера в своем офисе врач может получить доступ к расписанию процедур амбулаторной клиники и выяснить, что утром свободно подходящее время для данного обследования. Затем врач может заполнить и заверить электронной подписью входящее направление пациента на гастроэнтероскопию.

Ситуация без ИОК:

Клиника не может с достаточной степенью достоверности аутентифицировать врача, и, как результат, врач вынужден позвонить в клинику по телефону, чтобы записать пациента на процедуру, что потребует намного больше времени.

Ситуация с ИОК:

Врач может аутентифицировать себя в клинике и сделать заявку, а клиника может быть уверена, что именно данный врач сделал заявку и что впоследствии он не сможет заявить, что не делал этой заявки.

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 7498-2:1989	IDT	ГОСТ Р ИСО 7498-2—99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
ИСО/МЭК 9594-8:2001	IDT	ГОСТ Р ИСО/МЭК 9594-8—98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации
ИСО/ТС 17090-2:2002	—	*
ИСО/ТС 17090-3:2002	—	*
ИСО/МЭК 17799:2000	IDT	ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью

* 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/IEC 8824-1:1998, Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1

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

[4] ISO/IEC TR 13335-1, Information technology — Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security

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

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

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

[8] IETF/RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[9] IETF/RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[10] IETF/RFC 3039, Internet X.509 Public Key Infrastructure Qualified Certificates Profile

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

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

[13] ASTM Draft Standard, Standard Guide for Model Certification Practice Statement for Healthcare. January 2000

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

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

[16] COBIT (Control Objectives for Information and Related Technologies) specification produced by the Information Systems Audit and Control Foundation

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

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

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

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

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

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

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

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

[25] INTERNET-DRAFT October 1999 4.1, X.509 Attribute Certificate

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, инфраструктура с открытым ключом, защита данных, безопасные информационные системы

Редактор *О. А. Стояновская*
Технический редактор *Н. С. Гришанова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 08.10.2010. Подписано в печать 22.10.2010. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 4,18. Уч.-изд. л. 3,50. Тираж 79 экз. Зак. 1410

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.