ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 17090-1— 2015

Информатизация здоровья

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

Часть 1

Общие свойства служб электронных сертификатов

ISO 17090-1:2013
Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services
(IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ISO ТС 215 (Росстандарт)

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2015 г. № 2217-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 17090-1:2013 «Информатизация здоровья. Инфраструктура открытых ключей. Часть 1. Общие свойства служб электронных сертификатов» (ISO 17090-1:2013 «Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services»).

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

5 ВВЕДЕН ВЗАМЕН ГОСТ Р ИСО/ТС 17090-1—2009

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (*gost.e-ecolog.ru

© Стандартинформ, 2016

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 . . . 1
3.1 Термины сферы здравоохранения . . . 1
3.2 Термины служб информационной безопасности . . . 3
3.3 Термины, относящиеся к инфраструктуре открытых ключей . . . 5
4 Сокращения . . . 6
5 Контекст сферы здравоохранения . . . 7
5.1 Владельцы сертификатов и доверяющие стороны в сфере здравоохранения . . . 7
5.2 Примеры участников . . . 7
5.3 Применимость электронных сертификатов в здравоохранении . . . 8
6 Требования к службам безопасности в медицинских приложениях . . . 9
6.1 Особенности сферы здравоохранения . . . 9
6.2 Технические требования к применению электронных сертификатов в сфере здравоохранения . . . 10
6.3 Потребности, специфичные для здравоохранения, и отделение аутентификации от шифрования . . . 11
6.4 Управление информационной безопасностью в сфере здравоохранения с помощью электронных сертификатов . . . 11
6.5 Требования к политикам издания электронных сертификатов и их применению в здравоохранении . . . 12
7 Криптография с открытым ключом . . . 12
7.1 Симметричная и асимметричная криптография . . . 12
7.2 Электронные сертификаты . . . 12
7.3 Электронные подписи . . . 13
7.4 Защита закрытого ключа . . . 13
8 Применение электронных сертификатов . . . 14
8.1 Необходимые компоненты . . . 14
8.2 Установление идентичности с помощью квалифицированных сертификатов . . . 15
8.3 Установление специальности и ролей с помощью сертификатов идентичности . . . 15
8.4 Использование сертификатов атрибутов для авторизации и контроля доступа . . . 16
9 Требования к взаимной приемлемости . . . 17
9.1 Общие положения . . . 17
9.2 Возможные варианты применения электронных сертификатов в международном и межрегиональном масштабе . . . 17
9.3 Практическое применение вариантов . . . 19
Приложение А (справочное) Сценарии использования электронных сертификатов в здравоохранении . . . 20
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 28
Библиография . . . 29

Введение

Перед сферой здравоохранения стоит задача сокращения расходов путем перехода от бумажной документации к автоматизированному электронному учету. Новые модели предоставления услуг в сфере здравоохранения особо подчеркивают необходимость обмена информацией о пациенте между все расширяющимся кругом медицинских специалистов, выходящим за рамки традиционных организационных барьеров.

Медицинская информация, касающаяся отдельных граждан, обычно передается с помощью 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. Угроза разглашения медицинской информации вследствие несанкционированного доступа (случайного или преднамеренного) возрастает. Системе здравоохранения необходимо иметь надежные средства защиты информации, минимизирующие риск такого доступа.

Как же в сфере здравоохранения обеспечивается соответствующая надежная и эффективная защита при передаче данных через Интернет? Технологии инфраструктуры открытых ключей (ИОК) и электронных сертификатов позволяют найти подход к решению данной проблемы.

Правильное внедрение электронных сертификатов требует сочетания 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 идентичности человека или подлинности объекта. В сфере здравоохранения в данной технологии применяются аутентификация, шифрование и электронные подписи для облегчения конфиденциального доступа и передачи индивидуальных медицинских документов, что отвечает как клиническим, так и административным потребностям. Службы, предоставляемые в случае внедрения электронных сертификатов (включая шифрование, целостность информации и электронные подписи), удовлетворяют многим требованиям к системам безопасности. Особенно эффективным является использование электронных сертификатов в сочетании с официальным стандартом защиты информации. Многие организации во всем мире приступили к использованию электронных сертификатов для этой цели.

Функциональная совместимость технологии электронных сертификатов и поддерживающих ее политик, процедур и практических приемов имеет принципиальное значение, если обмен информации 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 электронных сертификатов требует создания системы доверия, при которой стороны, ответственные за неприкосновенность личной жизни, могут опереться на методики и практические приемы и, как дополнение, на подлинность электронных сертификатов, выданных другими уполномоченными органами.

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

Технология электронных сертификатов 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 электронные сертификаты. Настоящий стандарт призван удовлетворить потребность в управлении данным интенсивным международным процессом.

Настоящий стандарт содержит общие технические, эксплуатационные и методические требования, которые должны быть удовлетворены при использовании электронных сертификатов 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 трансграничного обмена данными на основе электронных сертификатов, однако может также служить руководством для внедрения электронных сертификатов в сфере здравоохранения на национальном или региональном уровне. Интернет все шире используется как средство передачи медицинских данных между организациями здравоохранения и является единственным реальным вариантом для трансграничного обмена данными в этой области.

Все части настоящего стандарта следует рассматривать как единое целое, поскольку каждая из них вносит свой вклад в определение того, как электронные сертификаты могут быть использованы для обеспечения служб безопасности в сфере здравоохранения, включая аутентификацию, конфиденциальность, целостность данных и технические возможности поддержки качества электронной подписи.

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

ИСО 17090-2 определяет специфичные для сферы здравоохранения профили электронных сертификатов на основе X.509, профиль которого определен в IETF/RFC 3280 для разных типов сертификатов.

В ИСО 17090-3 освещены проблемы управления, возникающие при внедрении и эксплуатации электронных сертификатов в сфере здравоохранения. В нем определены структура и минимальные требования к политикам сертификатов, а также структура сопутствующих отчетов по практическому применению сертификации. ИСО 17090-3 основан на рекомендациях IETF/RFC 3647 и определяет принципы защиты информации в сфере здравоохранения при трансграничном взаимодействии. В нем также определен необходимый минимальный уровень безопасности применительно к аспектам, специфичным для здравоохранения.

Комментарии по содержанию настоящего стандарта, а также комментарии, предложения и информация по его применению могут направляться в секретариат ИСО/ТК 215.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

Часть 1

Общие свойства служб электронных сертификатов

Health informatics. Public key infrastructure. Part 1. Overview of digital certificate services

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт определяет основные понятия, связанные с использованием электронных сертификатов в сфере здравоохранения, и структуру требований по взаимной совместимости, необходимой для создания системы защищенного обмена медицинской информацией на основе электронных сертификатов. В нем также указаны основные стороны, обменивающиеся медицинской информацией, а также основные службы обеспечения безопасности, необходимые при обмене медицинской информацией, где могут потребоваться электронные сертификаты.

В настоящем стандарте представлены краткое введение в шифрование с открытым ключом и базовые компоненты, необходимые для внедрения электронных сертификатов в сфере здравоохранения. Кроме того, в нем определены разные типы электронных сертификатов: сертификаты идентичности участвующих сторон и связанные с ними сертификаты атрибутов, самоподписанные сертификаты удостоверяющего центра (УЦ), иерархии и связь структур удостоверяющих центров.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты (для датированных ссылок следует использовать указанное издание, для недатированных ссылок — последнее издание указанного документа, включая все поправки к нему):

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

ИСО 17090-3:2008 Информатизация здоровья. Инфраструктура открытых ключей. Часть 3. Управление политикой органов сертификации (ISO 17090-3:2008, Health informatics — Public key infrastructure — Part 3: Policy management of certification authority)

3 Термины и определения

В настоящем стандарте также применены следующие термины с соответствующими определениями:

3.1 Термины сферы здравоохранения

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

Издание официальное

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 юрисдикциях к приложениям могут быть отнесены регистрируемые медицинские устройства.

3.1.2 **устройство** (device): Идентифицируемое устройство или прибор, управляемый компьютером и владеющий закрытым ключом шифрования.

Примечания

1 Данный термин относится также к классу регистрируемых медицинских устройств, соответствующих данному 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): Сертифицированный медицинский работник, вспомогательный работник здравоохранения, субсидируемый поставщик медицинских услуг, работник обеспечивающей организации, пациент или потребитель медицинских услуг, организация здравоохранения, устройство или приложение, используемые в сфере здравоохранения и требующие сертификат для предъявления системе безопасности на основе электронных сертификатов.

3.1.4 **организация здравоохранения** (healthcare organization): Официально зарегистрированная организация, основная деятельность которой связана с предоставлением медицинской помощи и обеспечением профилактики.

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

Примечания

1 Организация, юридически ответственная за свои действия, но не обязательно получающая лицензию на специфическую деятельность в сфере здравоохранения.

2 В настоящем стандарте составная часть организации называется организационной единицей согласно X.501.

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

Пример — Медрегистратор, организующий прием, или младшая медицинская сестра, участвующая в оказании медицинской помощи пациенту.

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

3.1.6 **работник организации** (organization employee): Лицо, работающее в организации здравоохранения или в обеспечивающей организации.

Пример — Операторы по вводу медицинских документов, эксперты страховых медицинских организаций и операторы по вводу рецептов.

3.1.7 **пациент, потребитель** (patient, consumer): Лицо, получающее медицинскую помощь и участвующее в функционировании медицинской информационной системы.

3.1.8 **неприкосновенность личной жизни** (privacy): Защита от вмешательства в частную жизнь или деловые отношения отдельного лица, результатом которого являются неоправданный или незаконный сбор и использование персональных данных этого лица.

[ИСО/МЭК 2382-8:1998]

3.1.9 **сертифицированный медицинский работник** (regulated health professional): Лицо, имеющее сертификат уполномоченного национального органа на право ведения определенной медицинской деятельности.

Пример — Врачи, сертифицированные медсестры, провизоры.

Примечания

1 Типы органов, выдающих сертификаты, различаются в разных странах и для разных профессий. К уполномоченным национальным органам относятся в том числе местные или региональные правительственные агентства, независимые профессиональные ассоциации и другие организации, официально уполномоченные государством. Им может как принадлежать, так и не принадлежать исключительное право сертификации на данной территории.

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

3.1.10 **субсидируемый поставщик медицинских услуг** (sponsored healthcare provider): Поставщик услуг в области здравоохранения, не являющийся сертифицированным специалистом, но работающий в сфере здравоохранения и субсидируемый лицензированной организацией здравоохранения.

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

3.1.11 **обеспечивающая организация** (supporting organization): Официально зарегистрированная организация, действующая в сфере здравоохранения, но не оказывающая медицинскую помощь.

Пример — Органы, финансирующие систему здравоохранения, например страховые медицинские организации, поставщики лекарственных и других товаров.

3.2 Термины служб информационной безопасности

3.2.1 **контроль доступа** (access control): Средства, с помощью которых ресурсы системы обработки данных предоставляются только авторизованным субъектам в соответствии с установленными правилами.

[ИСО/МЭК 2382-8:1998]

3.2.2 **учетность** (accountability): Свойство, обеспечивающее однозначное отслеживание действий логического объекта.

[ИСО 7498-2:1989]

3.2.3 **асимметричный алгоритм шифрования** (asymmetric cryptographic algorithm): Алгоритм, используемый для зашифрования и расшифрования информации, в котором ключи зашифрования и расшифрования различаются.

[ИСО 10181-1:1996]

3.2.4 **аутентификация** (authentication): Процесс надежной идентификации субъекта информационной безопасности путем защищенной ассоциации, установленной между идентификатором и субъектом.

[ИСО 7498-2:1989]

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

3.2.5 **авторизация** (authorization): Процесс предоставления субъекту полномочий, в том числе предоставление доступа на основе полномочий доступа.

[ИСО 7498-2:1989]

3.2.6 **доступность** (availability): Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

[ИСО 7498-2:1989]

3.2.7 **шифротекст** (ciphertext): Данные, получаемые в результате использования шифрования, смысловое содержание которых недоступно.

Примечание — Заимствовано из ИСО 7498-2:1989.

3.2.8 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного лица, логического объекта или процесса.

[ИСО 7498-2:1989]

3.2.9 **криптография** (cryptography): Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержания с целью предотвращения их необнаруживаемой модификации и/или несанкционированного использования.

[ИСО 7498-2:1989]

3.2.10 **криптографический алгоритм, шифр** (cryptographic algorithm, cipher): Метод преобразования данных для сокрытия их информационного содержания либо предотвращения их необнаруживаемой модификации или несанкционированного использования.

[ИСО 7498-2:1989]

3.2.11 **целостность данных** (data integrity): Свойство данных не подвергаться несанкционированному изменению или уничтожению.

[ИСО 7498-2:1989]

3.2.12 **аутентификация источника данных** (data origin authentication): Подтверждение того, что источник полученных данных соответствует заявленному.

[ИСО 7498-2:1989]

3.2.13 **расшифрование, декодирование** (decipherment, decryption): Процесс получения исходных данных из шифротекста.

[ИСО/МЭК 2382-8:1998]

Примечание — Шифротекст мог быть повторно зашифрован, и однократное расшифрование может не привести к получению исходных незашифрованных данных.

3.2.14 **электронная подпись** (digital signature): Данные, добавленные к блоку данных, или криптографическое преобразование этого блока, позволяющие получателю блока данных убедиться в подлинности источника и целостности блока и защитить его от искажения, например, получателем.

[ИСО 7498-2:1989]

Примечание — См. криптография.

3.2.15 **зашифрование, кодирование** (encipherment, encryption): Криптографическое преобразование данных для получения шифротекста.

[ИСО 7498-2:1989]

Примечание — См. криптография.

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

[ИСО/МЭК 2382-8:1998]

3.2.17 **идентификатор** (identifier): Информационный объект, используемый для объявления идентичности перед тем, как получить подтверждение соответствия от определенного аутентификатора.

[ENV 13608-1]

3.2.18 **целостность** (integrity): Доказательство, что содержание сообщения не было каким-либо способом случайно или преднамеренно изменено при передаче сообщения.

Примечание — Заимствовано из ИСО 7498-2:1989.

3.2.19 **ключ** (key): Последовательность символов, управляющая операциями зашифрования и расшифрования.

[ИСО 7498-2:1989]

3.2.20 **управление ключами** (key management): Генерация, сохранение, распределение, удаление, архивирование и применение ключей в соответствии с политикой безопасности.

[ИСО 7498-2:1989]

3.2.21 **неоспоримость** (non-repudiation): Услуга, обеспечивающая каждой из участвующих сторон доказательство целостности и происхождения данных (неразрывно друг от друга).

Примечание — Заимствовано из [19].

3.2.22 **закрытый ключ** (private key): Ключ, используемый в асимметричном криптографическом алгоритме, обладание которым ограничено (обычно принадлежит только одному субъекту).

[ИСО/МЭК 10181-1:1996]

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

[ИСО/МЭК 10181-1:1996]

3.2.24 **роль** (role): Комплекс способностей и/или действий, связанный с выполнением работы.

3.2.25 **безопасность** (security): Состояние защищенности, при котором обеспечиваются доступность, конфиденциальность, целостность и учетность.

[ENV 13608-1]

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

[ИСО/МЭК 2382-8:1998]

3.2.27 **служба безопасности** (security service): Служба, предоставляемая уровнем взаимодействия открытых систем и обеспечивающая адекватную защиту систем или передачи данных.

[ИСО 7498-2:1989]

3.3 Термины, относящиеся к инфраструктуре открытых ключей

3.3.1 **орган по присвоению атрибутов, ОА** (attribute authority; AA): Уполномоченный орган, назначающий полномочия путем выдачи сертификатов атрибутов.

[X.509]

3.3.2 **сертификат атрибута** (attribute certificate): Информационный объект, содержание которого заверено электронной подписью ОА, привязывающий некоторые значения атрибута к идентификации его владельца.

[X.509]

3.3.3 **сертификат уполномоченного органа** (authority certificate): Сертификат, выпущенный для удостоверяющего центра или органа по присвоению атрибутов.

Примечание — Заимствовано из X.509.

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

3.3.5 **распространение сертификатов** (certificate distribution): Акт издания сертификатов и их передачи принципалам безопасности.

3.3.6 **расширение сертификата** (certificate extension): Поля расширений (называемые просто расширениями) в сертификатах 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 критичными (т. е. система, использующая сертификат, должна отклонить сертификат, если он содержит не распознаваемое системой критичное расширение) или некритичными (т. е. не распознаваемое системой расширение может быть проигнорировано).

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

3.3.8 **управление сертификатами** (certificate management): Процедуры, имеющие отношение к сертификатам: генерация сертификатов, распространение сертификатов, архивирование и отзыв сертификатов.

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

3.3.10 **отзыв сертификата** (certificate revocation): Акт аннулирования достоверной связи между сертификатом и его владельцем (или владельцем принципала безопасности) вследствие того, что сертификату больше нельзя доверять, хотя срок его действия и не истек.

3.3.11 **владелец сертификата** (certificate holder): Организация или лицо, указанное субъектом в действительном сертификате.

3.3.12 **проверка сертификата** (certificate verification): Проверка аутентичности сертификата.

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

[ИСО/МЭК 2382-8:1998]

3.3.14 **удостоверяющий центр;** УЦ, **издатель сертификата** (certification authority; CA, certificate issuer): Уполномоченный орган, которому одна или несколько участвующих сторон доверили создание и присвоение сертификатов и который дополнительно может создавать ключи для доверяющих сторон.

Примечания

1 Заимствовано из ИСО/МЭК 9594-8.

2 Слово «центр» в термине «удостоверяющий центр» означает всего лишь доверенную сторону, а не какое-либо государственное лицензирование.

3 Более удачным термином может быть «издатель сертификата», но термин «удостоверяющий центр» очень широко употребляется.

3.3.15 **политика сертификата;** ПС (certificate policy; CP): Именованный свод правил, описывающих применимость сертификата в конкретном кругу субъектов и/или в классе приложений с общими требованиями к информационной безопасности.

[IETF/RFC 3647]

3.3.16 **свод правил по сертификации;** СПС (certification practices statement; CPS): Формулировка правил, которые УЦ использует при издании сертификатов.

[IETF/RFC 3647]

3.3.17 **сертификат открытого ключа;** СОК (public key certificate; PKC): Сертификат открытого ключа (СОК), соответствующий X.509, обеспечивающий связь идентичности с открытым ключом.

Примечания

1 Идентичность может быть использована для обеспечения принятия решений системой контроля доступа, основанной на использовании идентификации, с помощью которой клиент предоставляет доказательство обладания закрытым ключом, соответствующим открытому ключу, содержащемуся в сертификате открытого ключа.

2 Заимствовано из IETF/RFC 3280.

3.3.18 **инфраструктура открытых ключей;** ИОК (public key infrastructure; PKI): Инфраструктура, используемая в отношениях между владельцем ключа и доверяющей стороной и позволяющая доверяющей стороне использовать сертификат, связанный с владельцем ключа, по меньшей мере для одного приложения, использующего службу безопасности, зависящую от открытого ключа. К ИОК относятся УЦ, структура данных сертификата, средства, позволяющие доверяющей стороне получить текущую информацию о состоянии отзыва сертификата, политика сертификации и методы проверки практики сертификации.

3.3.19 **квалифицированный сертификат** (qualified certificate): Сертификат, основное назначение которого состоит в идентификации личности с высокой степенью достоверности в публичных службах неоспоримости участия.

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

3.3.20 **центр регистрации;** ЦР (registration authority, RA): Орган, ответственный за идентификацию и аутентификацию субъектов сертификатов, но не подписывающий и не издающий сертификаты (то есть ЦР делегировано выполнение определенной работы от имени УЦ).

[IETF/RFC 3647]

3.3.21 **доверяющая сторона** (relying party): Получатель сертификата, доверяющий этому сертификату или электронной подписи, проверенной с помощью этого сертификата.

[IETF/RFC 3647]

3.3.22 **третья сторона** (third party): Сторона, выполняющая определенную функцию безопасности как часть протокола обмена данными, но не являющаяся ни создателем, ни получателем данных.

3.3.23 **доверенная третья сторона;** ДТС (trusted third party; TTP): Третья сторона, считающаяся доверенной в рамках протокола информационной безопасности.

[IETF/RFC 3647]

Примечание — Этот термин использован во многих стандартах ИСО/МЭК и в других документах, которые в основном описывают службы УЦ. Однако это понятие шире и включает в себя такие службы, как штампы времени и, возможно, депонирование ключей.

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

ОА — орган по присвоению атрибутов (attribute authority);

УЦ — удостоверяющий центр (certification authority);

ПС — политика сертификата (certificate policy);

СПС — свод правил по сертификации (certification practice statement);

СОС — список отозванных сертификатов (certificate revocation list);

ЭКГ — электрокардиограмма (electrocardiogram);

ЭМК — электронная медицинская карта (electronic health record);

СОК — сертификат открытого ключа (public key certificate);

ИОК — инфраструктура открытых ключей (public key infrastructure);

ЦР — центр регистрации (registration authority);

ДТС — доверенная третья сторона (trusted third party).

5 Контекст сферы здравоохранения

5.1 Владельцы сертификатов и доверяющие стороны в сфере здравоохранения

В целях упрощения процесса обсуждения требований к электронным сертификатам 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 предъявления службе безопасности на базе ИОК. Определения перечисленным ниже участникам даны в подразделе 3.1.

Физические лица:

- сертифицированный медицинский работник;
- вспомогательный работник здравоохранения;
- пациент/потребитель услуг;
- субсидируемый поставщик медицинских услуг;
- работник обеспечивающей организации.

Организации:

- организация здравоохранения;
- обеспечивающая организация.

Другие объекты:

- устройства;
- регистрируемые медицинские устройства;
- приложения.

Кроме перечисленных участников для широкого внедрения электронных сертификатов необходимы УЦ и органы регистрации, которые сами являются важными владельцами сертификатов.

Некоторые работники здравоохранения связаны с несколькими организациями здравоохранения. Поэтому в здравоохранении крайне важно избегать дублирующей или избыточной регистрации, влекущей за собой лишние расходы и множественность сертификатов.

В рамках сферы здравоохранения назначением ЦР является либо идентификация участника в качестве действующего медицинского работника, выполняющего данную роль, либо идентификация потребителя медицинской помощи в качестве лица, обладающего правами на персональную информацию. Кроме того, необходимо регистрировать персонал, обслуживающий врачей частной практики (медрегистраторы, бухгалтеры, секретари и т. д.). Данные лица не связаны с такими организациями, как больницы, которые находятся в подчинении национальных, государственных или региональных органов здравоохранения.

5.2 Примеры участников

5.2.1 Сертифицированный медицинский работник

Примерами сертифицированных медицинских работников служат врачи, стоматологи, сертифицированные медсестры и провизоры. Существует много разных классификаций официально сертифицируемых/аккредитуемых профессий в сфере здравоохранения разных стран. Важной задачей будущей работы по стандартизации в ИСО является создание глобальной системы соответствий между этими классификациями, но в настоящем стандарте предполагается, что только самые общие классы могут признаваться в мировом масштабе. В ИСО 17090-2 определена структура данных, допускающая параллельное использование общей международной классификации и более детализированной классификации, которая может быть национальной или соответствовать иной юрисдикции, например в некоторых странах сертификацию медицинских работников осуществляют в провинциях или штатах.

5.2.2 Вспомогательный работник здравоохранения

Вспомогательными работниками здравоохранения являются лица, работающие в организациях здравоохранения, но не являющиеся сертифицированными медицинскими работниками. К ним относятся медрегистраторы, секретари, операторы по вводу данных (например, надиктованных), бухгалтеры и младший медицинский персонал. Для настоящего стандарта важно обозначить в сертификате, предъявляемом службе безопасности, связь между нанимающей медицинской организацией и работником. Для медицинских специалистов необходимо включить в структуру электронных сертификатов связь с уполномоченным сертифицирующим органом, но важно также предусмотреть в ней и информацию о возможном работодателе или членстве в профессиональной ассоциации, например врачебной.

Существует множество различных типов ролей или должностей работников сферы здравоохранения, но в настоящем стандарте не определена 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 своем деле.

5.2.3 Пациент/потребитель медицинской помощи

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 медицинской помощи, более уместно называть данное лицо потребителем медицинской помощи. В данном контексте под пациентом/потребителем понимается только непосредственный пользователь медицинской информационной системы.

5.2.4 Субсидируемый поставщик медицинской помощи

Существует несколько типов лиц, являющихся поставщиками медицинской помощи, 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 помогающие при родах сестры (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).

5.2.5 Работник обеспечивающей организации

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

5.2.6 Организация здравоохранения

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

5.2.7 Обеспечивающая организация

Обеспечивающие организации предоставляют услуги организациям здравоохранения, но непосредственно не оказывают медицинской помощи.

5.2.8 Устройства

К устройствам относится оборудование, например: электрокардиографы, автоматизированное лабораторное оборудование, разное переносное диагностическое оборудование, измеряющее различные физиологические параметры пациента. Кроме того, к устройствам относятся компьютерное оборудование, например серверы электронной почты, веб-серверы и серверы приложений.

5.2.9 Приложения

Приложения — это компьютерные программы, исполняемые на автономных компьютерах и/или в сетях. В сфере здравоохранения к приложениям, работа которых строится на доверии к электронным сертификатам, могут относиться интегрированные медицинские информационные системы, системы ведения электронных медицинских карт, информационные системы отделений скорой помощи, системы обработки изображений, а также системы выписки рецептов, системы ведения формуляров лекарственных средств и аптечные информационные системы.

5.3 Применимость электронных сертификатов в здравоохранении

Настоящий стандарт применим в сфере здравоохранения как в национальном, так и в международном масштабе. Его действие распространяется на органы (государственные) управления здравоохранением, частных поставщиков медицинской помощи всего спектра, включая больницы, амбулаторно-поликлинические учреждения, и врачей общей практики. Настоящий стандарт также распространяется на страховые медицинские организации, медицинские образовательные учреждения и другую деятельность по охране здоровья (например, уход на дому).

Хотя основной целью настоящего стандарта является создание общего подхода, в рамках которого медицинские работники, организации здравоохранения и страховые медицинские организации могут безопасно обмениваться медицинской информацией, он также предназначен для обеспечения возможности потребителям иметь безопасный доступ к информации о их собственном здоровье. Транзакции могут происходить при участии УЦ и ЦР, действующих как доверенные третьи стороны, обеспечивающие поставщикам медицинской помощи, страховым медицинским организациям и потребителям возможность обмена информацией с гарантией ее безопасности и защищенности, а также оперативного оповещения в случае их нарушения.

Подходящими приложениями электронных сертификатов в сфере здравоохранения являются:

a) защищенная электронная почта;

b) запросы на доступ к больничным информационным системам от приложений, используемых медицинскими специалистами амбулаторно-поликлинических учреждений;

c) запросы на доступ от приложений, используемых внутри больничных информационных систем. К таким системам могут относиться системы управления движением пациентов и коечным фондом, клинические информационные системы, а также информационные системы отделений лучевой диагностики, патологоанатомических отделений, службы питания и т. д.;

d) финансовые приложения, в которых требуется неоспоримость, целостность сообщений, конфиденциальность информации, аутентификация пациентов, поставщиков медицинской помощи и страховщиков, а также (в некоторых юрисдикциях) защита от мошенничества;

e) приложения дистанционной обработки изображений, которые требуют аутентификации медицинского работника и надежной привязки изображений к идентификации пациента;

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

g) приложения электронных рецептов, которым требуется весь спектр служб безопасности, использующих электронные сертификаты для гарантии, что данный рецепт выписан конкретным медицинским работником (аутентификация источника) и отпущенное по нему лекарство направлено нужному пациенту. Чтобы гарантировать отсутствие ошибок при передаче информации, необходимо использовать службу проверки целостности данных, основанную на применении электронных сертификатов, и обеспечить учетность с помощью службы неоспоримости;

h) электронные документы об информированном согласии пациента, заверенные электронной подписью;

i) службы трансграничного или межтерриториального операторского ввода данных;

j) другие системы в соответствии с местными политиками безопасности.

Местные политики могут исключать необходимость использования электронных сертификатов в одном или нескольких из вышеперечисленных приложений.

Некоторые сценарии, в которых могут применять электронные сертификаты, представлены в приложении А.

6 Требования к службам безопасности в медицинских приложениях

6.1 Особенности сферы здравоохранения

Сфера здравоохранения предъявляет специфичные требования к информационной безопасности, нуждающиеся в отдельной интерпретации, что и послужило причиной создания настоящего стандарта. В этих требованиях отражены следующие конкретные особенности сферы здравоохранения:

a) медицинская информация многократно используется и может существовать в течение всей жизни лица, к которому она относится, и даже дольше. Это обстоятельство, в свою очередь, приводит к необходимости длительного хранения электронных подписей, в котором значительную роль играет технология меток времени, обеспечивающая такую возможность;

b) существуют важные потребители и поставщики медицинской помощи, озабоченные тем, чтобы собранная медицинская информация использовалась в медицинских целях и никак иначе, за исключением тех случаев, когда пациент дал явное согласие на использование данной информации (например, анонимные сведения о пациенте могут быть использованы в образовательных и исследовательских целях);

c) существует необходимость укрепить уверенность потребителей медицинской помощи в способности системы здравоохранения управлять предоставленной информацией;

d) существует необходимость в том, чтобы медицинские работники и организации соблюдали обязательства по защите информации при оказании медицинской помощи;

e) существует необходимость получать подтверждение, что медицинские работники, торговые партнеры и стороны, использующие электронные сертификаты в сфере здравоохранения, доверяют мерам, обеспечивающим защиту неприкосновенности личной жизни и безопасность персональной информации пациента.

Вопросы информационной безопасности в сфере здравоохранения становятся все более актуальными по мере того, как для хранения медицинской информации все чаще применяются электронные информационные системы вместо бумажной документации. Первоочередной задачей сферы здраво-

охранения является защита безопасности пациента и неприкосновенности его личной жизни. В частности, необходимо обеспечить выполнение требований законодательства о защите персональных данных, в том числе касающихся их трансграничной передачи. Если информационная система предназначается для использования как медицинскими работниками, так и пациентами/потребителями, то она должна вызывать доверие. Поэтому выполнение требований к информационной безопасности и неприкосновенности личной жизни имеет особую важность для информационных систем в сфере здравоохранения.

6.2 Технические требования к применению электронных сертификатов в сфере здравоохранения

6.2.1 Общие положения

Основными угрозами безопасности, которым должны противодействовать медицинские информационные и коммуникационные системы, связаны с несанкционированным доступом путем кражи закрытого ключа у законного владельца сертификата и последующей незаконной деятельности от его имени. Подобный несанкционированный доступ может привести к изменению, утере или копированию медицинской информации. Применение электронных сертификатов в соответствии со стандартом информационной безопасности, например ИСО/МЭК 27002, может значительно снизить риск несанкционированного доступа.

Применение электронных сертификатов способствует созданию уникального комплекса политик, методов и технологии, предлагающего все службы аутентификации, целостности, конфиденциальности и электронной подписи. В сфере здравоохранения оно дает возможность поставщикам и потребителям медицинской помощи, которые могут быть не знакомы, уверенно осуществлять безопасный обмен информацией в электронной среде, основанной на цепочке доверия.

Используя электронные сертификаты, можно предложить использовать службы безопасности, особо востребованные сферой здравоохранения. Эти службы и их применение в сфере здравоохранения описаны ниже более детально.

6.2.2 Аутентификация

В здравоохранении развита специализация медицинских работников, поэтому при анализе медицинских карт, заключений консультантов и других документов о состоянии здоровья пациентов медицинским работникам приходится полагаться на суждения других поставщиков медицинской помощи. Если эти документы и записи представлены и обновляются в электронном виде, то необходима уверенность, что содержащаяся в них информация действительно предоставлена их авторами.

Крайне важно, чтобы медицинские работники могли получать доступ к конфиденциальной медицинской информации пациентов из разных медицинских учреждений, но в то же время, чтобы эта информация была защищена от несанкционированного доступа и изменения. Аутентификация рассматривается в 7.4.

6.2.3 Целостность

Обеспечение целостности персональной медицинской информации может в буквальном смысле быть вопросом жизни и смерти, когда такая информация необходима при оказании экстренной медицинской помощи. Более того, существуют веские мотивы для нарушения целостности некоторых форм персональной медицинской информации (например, при назначении наркотических средств).

6.2.4 Конфиденциальность

Персональную медицинскую информацию часто рассматривают как наиболее конфиденциальную информацию в повседневной жизни. В отличие от информации, которая передается в электронной форме для целей электронной торговли, конфиденциальность персональной медицинской информации не может быть выражена в денежном эквиваленте, и однажды нарушенное право пациента на неприкосновенность личной жизни не может быть легко восстановлено.

6.2.5 Электронная подпись

Электронные подписи, используемые в здравоохранении, а также политики и практика подтверждения их целостности, в конечном счете, могут быть объектами особого интереса в процессе судебных слушаний, рассмотрения дел о врачебных ошибках, заседаний профессиональных дисциплинарных комитетов и других юридических или менее официальных мероприятий, по ходу которых документы с электронной подписью представляют в качестве доказательств.

Должна быть обеспечена возможность проверки электронных подписей документов даже в том случае, если срок действия сертификата истек или сертификат был отозван. Это можно сделать с помощью использования меток времени (см. IETF/RFC 3161). В качестве формата подписи, рассчитанной на длительное хранение, рекомендуется использовать тот, что описан в IETF/RFC 3162.

Электронные сертификаты используются также службами авторизации и контроля ролевого доступа. Данные службы жизненно необходимы в сфере здравоохранения, поскольку в ней существует множество специальностей и множество ситуаций, требующих разных уровней доступа к компонентам персональной медицинской информации в зависимости от ситуации и роли участвующего медицинского работника.

6.2.6 Авторизация

В сфере здравоохранения важно, чтобы права на доступ к персональной медицинской информации предоставлялись только тем лицам, которым она необходима для оказания медицинской помощи пациенту/потребителю, либо другим лицам, которым дано явное согласие пациента.

6.2.7 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.

Использование электронных сертификатов в соответствии со стандартом информационной безопасности может значительно снизить риск неавторизованного доступа к медицинской информации пациента.

Целью настоящего стандарта является определение общих элементов процессов издания и использования электронных сертификатов, которые обеспечат цепочку доверия при обмене медицинской информацией в межрегиональном или международном масштабе.

6.3 Потребности, специфичные для здравоохранения, и отделение аутентификации от шифрования

В сфере здравоохранения существует выраженная потребность отделения функции подписи 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, которому предназначалось сообщение, отсутствует на месте или недоступен. В системах информационной безопасности, рассчитанных на сферу здравоохранения, обычной практикой является наличие личного идентификационного сертификата, используемого для аутентификации, и сертификата организационной единицы, используемого для шифрования.

Настоящий стандарт рекомендует использовать отдельные сертификаты и связанные с ними ключи для аутентификации и шифрования (обеспечивающих конфиденциальность). В нем также подтверждена необходимость иметь отдельные сертификаты для установления идентичности и для управления контролем доступа, привязанные к ключу аутентификации субъекта.

Если ключи используют для шифрования данных, то для предотвращения потери данных в случае отсутствия доступа к ключам расшифрования необходимы определенные средства управления ключами.

6.4 Управление информационной безопасностью в сфере здравоохранения с помощью электронных сертификатов

Инфраструктура применения электронных сертификатов, необходимая для безопасного обмена медицинской информацией и доступа к данным в национальном и международном масштабе, должна обеспечиваться согласованными общими политиками управления информационной безопасностью. Чтобы обеспечить уверенность в том, что данная инфраструктура функционирует безопасно, следует установить нормы и правила по управлению информационной безопасностью.

Стандарты, определяющие нормы и правила по управлению информационной безопасностью, уже существуют и являются общепринятыми. ИСО/МЭК 27002 и спецификация COBIT [16] устанавливают правила идентификации рисков безопасности, а также правила применения соответствующих средств управления этими рисками.

Подобные нормы и правила накладывают небольшие ограничения или не накладывают вообще никаких ограничений на службы, которые могут быть предоставлены при внедрении электронных сертификатов и дают подписывающему или проверяющему лицу уверенность в том, что электронная подпись не будет подвержена риску компрометации из-за плохого управления безопасностью.

Исходя из этого, настоящий стандарт ссылается на ИСО/МЭК 27002 при решении вопросов обеспечения информационной безопасности, представленных в IETF/RFC 3647 [11].

6.5 Требования к политикам издания электронных сертификатов и их применению в здравоохранении

Требования к политикам и связанные с ними правила издания и использования электронных сертификатов в сфере здравоохранения определены в ИСО 17090-3.

7 Криптография с открытым ключом

7.1 Симметричная и асимметричная криптография

При симметричной криптографии для преобразования открытого текста в нечитаемую криптограмму используют закрытый ключ. Такая зашифрованная информация может быть расшифрована посредством того же закрытого ключа с помощью обращения алгоритма шифрования. Данный тип криптографической системы широко используется для обеспечения конфиденциальности и называется симметричной системой, или системой с закрытым ключом.

Криптография с открытым ключом была впервые описана Уитфилдом Диффи и Мартином Хеллманом в 1976 г. В данном подходе использованы два разных ключа — открытый и закрытый. Любой обладатель открытого ключа может зашифровать сообщение, но не может его расшифровать. Только владелец закрытого ключа может расшифровать такое сообщение. Невозможно вычислить закрытый 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 использован для защиты закрытого ключа симметричной криптографической системы.

Асимметричные криптографические системы могут повысить эффективность симметричных криптографических систем или виртуальных частных сетей, обеспечивая аутентификацию участвующих сторон посредством гарантированной целостности передачи данных, 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 закрытого ключа, может быть расшифрован с помощью открытого ключа. Такой принцип не подходит для защиты конфиденциальности, но может быть использован для аутентификации. Только владелец закрытого ключа способен создать криптограмму, которая может быть расшифрована при помощи соответствующего открытого ключа. Данное свойство может быть использовано для аутентификации владельца закрытого ключа в качестве источника сообщений.

7.2 Электронные сертификаты

Электронный сертификат — это структура данных, связывающая открытый ключ субъекта и один или несколько атрибутов, относящихся к идентичности субъекта, его открытым ключам и другой информации, которая воспроизводится без искажения после шифрования с использованием закрытого ключа УЦ в соответствии с ИСО/МЭК 9594-8. Одним из атрибутов, относящихся к идентичности субъекта, является отличительное имя, по которому данный субъект может быть идентифицирован.

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

Степень уверенности обеспечивается УЦ, подписавшим электронный сертификат собственным закрытым ключом. Подписывая электронный сертификат, УЦ берет на себя ответственность за информацию, содержащуюся в электронном сертификате, и за обеспечение владельца сертификата определенным уровнем аутентификации.

УЦ издает сертификаты, ведет каталог сертификатов (вместе с их открытыми ключами), отзывает сертификаты, которые могли стать недействительными, и обеспечивает своевременное информирование всех участвующих сторон об отзыве сертификатов. Процесс управления сертификатами определен в ИСО 17090-3, в котором также описаны роль ЦР и ограничения, накладываемые на те субъекты, которые могут исполнять роль ЦР.

7.3 Электронные подписи

Согласно ИСО 7498-2, [2] электронная подпись представляет собой данные, добавленные к блоку данных, или криптографическое преобразование этого блока, позволяющие получателю блока данных убедиться в подлинности источника и целостности блока и защитить его от искажения, например, получателем.

Электронная подпись создается посредством использования закрытого ключа отправителя для выполнения некоторой математической операции над посылаемым сообщением. Эта операция заключается в использовании закрытого ключа и математической функции, известной как алгоритм хеширования, для создания хеш-кода (некоторого очень большого числа) из исходного сообщения. Хеш-функция имеет свойство необратимости, заключающееся в вычислительной невозможности восстановления исходного сообщения или закрытого ключа из хеш-кода. Этот хеш-код передается вместе с сообщением. Получатель использует отрытый ключ отправителя для выполнения такой же операции над сообщением и сравнивает полученный 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 о его отправке. Поскольку закрытый ключ является частью пары ключей, в которой открытый ключ связан с идентичностью, указанной в электронном сертификате, то идентичность отправителя может быть установлена с ранее не достижимой степенью уверенности. Степень уверенности гарантируется УЦ, подписавшим электронный сертификат собственным закрытым ключом. Подписывая электронный сертификат, УЦ берет на себя ответственность за информацию, содержащуюся в этом сертификате, и за обеспечение владельца сертификата определенным уровнем аутентификации.

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

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

7.4 Защита закрытого ключа

Сертификат не связывает ключи с идентичностями; он связывает ключи только с отличительным именем субъекта. Для завершения привязки закрытого ключа к субъекту, обеспечивающей возможность использования данного закрытого ключа только поименованным субъектом, необходимо выполнить специальные действия. Поэтому для успешного применения электронных сертификатов в сфере здравоохранения решающее значение имеет надлежащее управление закрытыми ключами. Если закрытый ключ скомпрометирован, то соответствующий электронный сертификат не является больше эффективной защитой информации, передаваемой и хранящейся с использованием данной пары открытого и закрытого ключей. Более того, если скомпрометирован закрытый ключ УЦ, то вся система безопасности в зоне ответственности данного УЦ может обрушиться.

Защита закрытого ключа требует сочетания процессов управления и технических методов. Какие бы технические средства ни использовались, защита ключа должна обеспечиваться всей структурой управления информационной безопасностью в соответствии с ИСО/МЭК 27002.

Закрытый ключ может быть защищен с помощью аппаратного устройства, в котором он хранится, и которое может осуществлять криптографические вычисления. Доступ к такому устройству владелец сертификата может получать с использованием пароля, кодовой фразы или биометрических данных. Это более надежный метод защиты закрытого ключа, поскольку он не требует электрического соединения с компьютером, к нему невозможно получить доступ через сеть и в нем могут использоваться сложные алгоритмы аутентификации. Роль подобных электронных устройств могут выполнять определенные типы смарт-карт. Также возможно использование USB-ключа или аналогичных токенов, в которых хранится только закрытый ключ, а криптографический алгоритм хранится на основном компьютере.

Для получения доступа к закрытому ключу владельцу сертификата либо другому устройству или приложению необходимо пройти аутентификацию, чаще всего с помощью ввода пароля, кодовой фразы или предъявления биометрических данных. Существуют разные способы аутентификации, главным образом основанные на таких характеристиках аутентифицируемого, как его местонахождение, нечто ему известное, кем он является или что ему принадлежит. Например, требуется ввод пароля (нечто ему известное) с использованием физического устройства, например токена (нечто ему принадлежащее). Рекомендуется использовать более одного способа аутентификации (так называемую двухфакторную аутентификацию), что значительно повышает защищенность закрытого ключа.

Настоящий стандарт определяет необходимость многоуровневой защиты и устанавливает, что для более высоких уровней безопасности защиту закрытого ключа следует осуществлять с помощью аппаратных устройств. Управление закрытым ключом подробно описано в пунктах 7.6.2,7.6.3 ИСО 17090-3.

Для трансграничной и межрегиональной передачи персональной медицинской информации с использованием незащищенной среды, например Интернет, при которой отправитель и получатель раньше не вступали в контакт и не знали друг друга лично, необходимы такие способы аутентификации участвующих сторон, которые гарантируют, что передаваемая и хранящаяся информация остается конфиденциальной, что она не изменена при передаче и что ни одна из сторон не сможет позже отрицать факт отправки или получения информации. Это является основным требованием, предъявляемым сферой здравоохранения к службам информационной безопасности, основанным на использовании электронных сертификатов.

8 Применение электронных сертификатов

8.1 Необходимые компоненты

8.1.1 Общие положения

ИОК является инфраструктурой, содержащей перечисленные ниже компоненты.

8.1.2 Политика сертификата

ПС представляет собой поименованные правила, определяющие применимость сертификата в определенных группах учреждений здравоохранения и/или в классе приложений с общими требованиями к обеспечению информационной безопасности. Сертификаты, основанные на ПС, которая специально разработана для удовлетворения потребностей в медицинской информации, предназначены для использования службами, обеспечивающими авторизацию, контроль доступа и целостность информации. Специфические потребности системы здравоохранения, описанные в разделе 6, требуют, чтобы электронные сертификаты были определены особым образом именно для нужд сферы здравоохранения.

8.1.3 Свод правил по сертификации

Свод правил по сертификации (СПС) представляет собой формулировку правил, которые УЦ использует при выпуске сертификатов в соответствии с ПС. Например, в СПС указаны действия, которые необходимо предпринять, когда от органа управления здравоохранением поступает запрос на выдачу сертификата медицинскому работнику.

8.1.4 Удостоверяющий центр

УЦ является доверенным органом, который подтверждает идентичность владельца сертификата и присваивает ему «отличительное имя». УЦ также подтверждает правильность информации, относящейся к идентифицированному владельцу сертификата, подписывая эту информацию и, таким образом, подтверждая связь между именами или идентичностью и открытыми ключами, которые вводят в действие электронную подпись данного владельца сертификата. Некоторые из этих функций могут быть делегированы ЦР (см. 8.1.5), например функции подтверждения идентичности и присвоения отличительного имени, поскольку данные функции могут быть выполнены наилучшим образом на местном уровне.

Закрытый ключ может храниться на компьютере субъекта или на внешнем носителе, например на смарт-карте. Обычно доступ к ключу осуществляется владельцем сертификата посредством ввода кодовой фразы.

Настоящий стандарт допускает, что органы управления здравоохранением могут получать услуги обращения сертификатов разными способами. Некоторые могут осуществлять эту деятельность сами, другие могут передать полномочия на нее уполномоченным частным организациям. Кроме того, могут существовать различные системы обращения сертификатов в зависимости от их назначения. Владельцы сертификатов также могут иметь несколько сертификатов.

В зависимости от способа организации обращения электронных сертификатов в сфере здравоохранения конкретной страны, может существовать несколько уровней УЦ, выпускающих сертификаты для владельцев сертификатов в пределах медицинской организации, для всей системы здравоохранения или для любого жителя данной страны.

УЦ должен быть зарегистрированной организацией, обладающей собственной системой контроля и процедурами, обеспечивающими требуемую степень доверия. Они должны, как минимум, соответствовать ИСО/МЭК 27002 (или его аналогу) и по возможности должны соответствовать схеме безопасности электронного сертификата, принятой на территории действия УЦ.

8.1.5 Центр регистрации

ЦР является органом, устанавливающим идентичность владельцев сертификатов и регистрирующим их требования по сертификации, направленные УЦ. Центр регистрации может также проверять информацию о роли, служебном положении или статусе занятости владельца сертификата, которая может быть записана в сертификате атрибутов. В принципе ЦР может проверить, что атрибут статуса занятости (например, руководителя государственной больницы) может быть получен от другого ЦР, принадлежащего организации, подтверждающей профессиональную квалификацию медицинских работников (например, органу сертификации медицинских работников).

Идентификация роли медицинских работников может осуществляться следующими органами:

- национальными, региональными или местными органами здравоохранения (для работников подведомственных больниц и других медицинских организаций);
- органами по сертификации медицинских специалистов и работников здравоохранения;
- профессиональными медицинскими ассоциациями, например ассоциациями хирургов, психиатров, медсестер;
- частными или государственными страховыми медицинскими организациями.

Для проверки полномочий медицинских работников пользователи электронных сертификатов могут обращаться к одному или нескольким таким органам. Процедуры регистрации определены в 6.1 и 7.2.1.2, 7.3.1.2, 7.3.2.2, 7.3.3.2 и 7.3.4.2 технической спецификации ИСО/ТС 17090-3.

8.2 Установление идентичности с помощью квалифицированных сертификатов

Квалифицированные сертификаты относятся к типу сертификатов, основным назначением которых является надежная идентификация личности с помощью служб электронной подписи. Квалифицированные сертификаты имеют особое значение для юридического признания электронных подписей. Настоящий стандарт создает основу для использования квалифицированных сертификатов в связи с ростом числа стран, законодательно устанавливающих требования к поставщикам медицинских и других услуг, использующим электронные подписи, а также к лицам, ставящим и проверяющим электронную подпись, с тем чтобы электронная подпись могла быть юридически признана.

Необходимость использования квалифицированных сертификатов была признана Рабочей группой по разработке стандартов для сети Интернет (Internet Engineering Task Force; IETF), выпустившей [12]. В этом документе описан профиль квалифицированных сертификатов, а его целью является определение базового синтаксиса, независимого от требований местного законодательства. Профиль квалифицированных сертификатов используется IETF для описания формата сертификата, основным назначением которого является надежная идентификация физических лиц. Профиль квалифицированных сертификатов IETF использован в настоящем стандарте как основа для применения квалифицированных сертификатов. Профиль квалифицированных сертификатов определен в ИСО 17090-2.

В сфере здравоохранения квалифицированные сертификаты могут использоваться для надежной идентификации отдельных поставщиков и потребителей медицинской помощи с той степенью доверия, которая возникает при проверке электронной подписи данного лица. Настоящий стандарт рекомендует использовать квалифицированные сертификаты как для сертифицированных медицинских работников, так и для вспомогательных работников здравоохранения.

8.3 Установление специальности и ролей с помощью сертификатов идентичности

Настоящий стандарт учитывает, что не все врачи одинаковы с точки зрения пациента/потребителя медицинской помощи. Пациенты/потребители могут обращаться к разным врачам с разными проблемами со здоровьем. ВИЧ/СПИД, инфекционные болезни, психические заболевания являются только некоторыми из проблем со здоровьем, при которых люди вступают в отдельные отношения с разными медицинскими работниками. Поэтому решение о предоставлении доступа медицинского работника к конкретным данным медицинской карты пациента/потребителя медицинской помощи обычно зависит от специальности данного медицинского работника, например хирургии, и от его роли, к примеру дежурный хирург отделения скорой помощи центральной городской больницы.

Важно отметить, что срок действия авторизующей информации отличается от срока действия привязки идентичности субъекта к открытому ключу и намного меньше срока действия основной медицинской квалификации. Например, некто является квалифицированным врачом со стажем 40 лет, но его приняли на должность консультирующего психиатра в конкретную больницу всего на несколько месяцев. Если авторизующая информация кодируется в расширении СОК, то в результате срок полезного действия СОК сокращается. Кроме того, издатель СОК обычно не несет ответственность за авторизующую информацию. В принципе издатель СОК может иметь возможность проверить, что лицо, которому он выдает электронный сертификат, является конкретным медицинским работником, однако менее вероятно, что он имеет возможность проверить, что это лицо выполняет роль консультирующего

психиатра в конкретной больнице. Для получения этой информации из авторитетного источника издатель СОК должен выполнить дополнительные действия. При этом срок действия СОК может сократиться, поскольку некоторая информация, содержащаяся в нем, может довольно быстро стать недостоверной, что влечет за собой увеличение объема административной работы по отзыву данного СОК и выпуску нового. По этим причинам зачастую удобнее отделить авторизующую информацию от СОК. Работа по детальной спецификации сертификатов атрибутов все еще нуждается в более широком внедрении в индустрию программного обеспечения (см. [16]).

Хотя спецификация сертификата атрибута, разработанная организацией IETF, описывает использование открытого ключа для проверки электронных подписей или для выполнения операций по управлению криптографическими ключами, в ней утверждается, что не все запросы и решения о раскрытии информации основаны на идентичности. Подобные решения по контролю доступа могут быть также основаны на правилах, ролях и рангах, поэтому для них может требоваться дополнительная информация. Например, информация о том, что медицинский работник принадлежит к определенной группе специалистов, может быть более важной при принятии решения о доступе, нежели его идентичность. В подобных случаях авторизующая информация, необходимая при принятии таких решений, может быть закодирована в расширении СОК или в отдельном сертификате атрибута в соответствии с положениями [16], а также в соответствии с подпунктом 5 пункта 6.3.3 и 7.3.1 ИСО 17090-2.

Настоящий стандарт рекомендует, чтобы основным назначением СОК являлось подтверждение идентичности. Информация об идентичности владельца 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, соответствующий X.509, связывает идентичность клиента с открытым ключом. Идентичность может быть использована при принятии решений по управлению запросами и предоставлению информации, основанных на идентичности, после того, как владелец сертификата подтвердит, что он имеет закрытый ключ, соответствующий открытому ключу, содержащемуся в СОК (см. [16]).

В качестве альтернативы включению различных атрибутов, указывающих профессиональные роли, в основной изданный сертификат идентичности, другие организации, ответственные за присвоение этих ролей, могут с ведома основного УЦ выдать второй сертификат ключа, использующий тот же ключ, что и основной сертификат идентичности, но содержит один или несколько дополнительных атрибутов.

После подтверждения идентичности сертификаты атрибутов могут быть использованы для более подходящего управления информацией в тех ситуациях, когда часть информации, связанная с СОК, более изменчива или недолговечна, чем остальная информация. Поэтому в настоящем стандарте рассмотрено применение сертификатов атрибутов. Однако этот подход сталкивается с рядом трудностей. Применение сертификатов атрибутов все еще находится в стадии развития и должно более широко внедряться в индустрию программного обеспечения. Далее, информация о специальности медицинского работника, например психиатрии, педиатрии и урологии, имеет определенную длительность. Кроме того, необходимо иметь возможность регистрации информации о роли пациента/потребителя медицинской помощи. Для этих целей в подразделе 5.1 ИСО 17090-2 определено расширение типов сертификатов идентичности с именем HCRole.

В заключение необходимо отметить, что электронные сертификаты можно также использовать для подписи объявлений безопасности посредством такого стандарта, как SAML (Security Assertion Markup Language — язык разметки объявлений безопасности). Подобные объявления безопасности могут содержать сведения о специальности медицинского работника и его роли.

8.4 Использование сертификатов атрибутов для авторизации и контроля доступа

В спецификации сертификатов атрибутов, принятой организацией IETF, указано, что размещение авторизующей информации в СОК нежелательно. В настоящем стандарте признается желательность многократного использования сертификатов идентичности и минимизации содержащейся в них информации. В нем рекомендуется, чтобы информация о дополнительных ролях, членстве в группах и категории допуска размещалась в сопутствующих сертификатах атрибутов.

Следует отметить, что авторизующая информация отличается от информации о медицинских ролях и лицензиях, которая в принципе может быть включена в СОК. Роль или лицензия подразумевает некоторый уровень авторизации, однако сами по себе они недостаточны для авторизации. Настоящий стандарт предусматривает использование сертификатов атрибутов для обеспечения передачи информации о ролях поставщиков медицинских услуг.

Хотя в сертификате идентичности, изданном УЦ, может подразумеваться некоторая роль, во многих ситуациях он не содержит информации, достаточной для принятия решения о предоставлении

доступа. Например, СОК, выданный врачу от имени такого ЦР, как Коллегия хирургов, может подтвердить, что этот врач является хирургом, однако содержания этого СОК обычно недостаточно для предоставления данному врачу, временно работающему в отделении скорой помощи, права выполнения обязанностей врача приемного отделения.

Подобная детальная авторизующая информация более успешно предоставляется с помощью сертификата атрибутов, связанного с открытым ключом медицинского работника. Такой работник может иметь много сертификатов атрибутов, отражающих его различные роли. Подобные сертификаты атрибутов обычно имеют более короткий срок действия, нежели сертификат идентичности.

Упомянутый выше документ IETF также констатирует, что авторизующая информация должна быть защищена аналогично СОК и что такая защита обеспечивается сертификатом атрибутов, который представляет собой просто набор атрибутов, заверенный (или сертифицированный) электронной подписью. Сертификат атрибутов по структуре подобен СОК; основное отличие состоит в том, что он не содержит открытый ключ. Он может содержать атрибуты, определяющие членство в группе, роль, категорию допуска и другую информацию по контролю доступа, относящуюся ко владельцу сертификата атрибутов.

Спецификация элементов данных в сертификате атрибутов описана в ИСО/ТС 17090-2 в соответствии с [16]. Поскольку спецификация сертификатов атрибутов все еще находится в стадии разработки, типы сертификатов атрибутов, используемых в здравоохранении, должны быть описаны более подробно в следующих изданиях настоящего стандарта.

9 Требования к взаимной приемлемости

9.1 Общие положения

В настоящем стандарте предлагается принять за основу и дополнить документы организации IETF и другие существующие стандарты информационной безопасности в целях обеспечения безопасной трансграничной и межрегиональной электронной передачи медицинской информации. Все чаще в качестве среды для такого обмена информацией используют Интернет.

Поскольку одной из целей настоящего стандарта является обеспечение безопасной трансграничной, межрегиональной и межучрежденческой передачи медицинской информации, то для повышения ее общей эффективности следует использовать Интернет-технологии. Поэтому в качестве организационной основы настоящего стандарта используется [11] и по мере необходимости даются ссылки на другие документы IETF/RFC.

Безопасная трансграничная передача медицинской информации может быть обеспечена участвующими странами путем взаимного признания механизмов, используемых в каждой стране для реализации политик, правил и процедур регистрации УЦ.

Управление изданием и применением электронных сертификатов в сфере здравоохранения требует дальнейшей проработки и не входит в область применения настоящего стандарта. В нем предлагается обеспечить взаимную приемлемость средств информационной безопасности в международном масштабе путем подписания серии двусторонних и многосторонних соглашений между странами, основанных на минимальных требованиях, определенных в ИСО 17090-3. В конечном счете доверяющей стороне нужны УЦ, обеспечивающие выполнение процедур, необходимых для достижения требуемого уровня доверия в создаваемой инфраструктуре.

9.2 Возможные варианты применения электронных сертификатов в международном и межрегиональном масштабе

9.2.1 Общие положения

Основной проблемой внедрения электронных сертификатов в международном и межрегиональном масштабе является доверие, то есть практика многих сторон, полагающихся на политики и своды правил и, как продолжение, на проверку электронных сертификатов, выданных владельцу уполномоченным органом. Ниже приведен обзор возможных вариантов архитектуры применения электронных сертификатов в сфере здравоохранения.

9.2.2 Вариант 1. Единая иерархия УЦ

С технической точки зрения — это самый простой вариант. Однако нереально внедрить электронные сертификаты в сфере здравоохранения по всему миру с единым централизованным УЦ. Хотя полномочия по регистрации в данном варианте могут быть делегированы, общая структура управления может оказаться неработоспособной.

9.2.3 Вариант 2. Управление доверием

В данном варианте на доверяющей стороне лежит ответственность за принятие решения о доверии данному УЦ. Этот вариант имеет свои недостатки, так как требует, чтобы принятие такого решения возлагалось на доверяющую сторону, и в некоторых случаях степень ответственности доверяющей стороны, не всегда способной получить информацию, требуемую для обоснования решения, может оказаться слишком высокой.

9.2.4 Вариант 3. Взаимное признание

Взаимное признание представляет собой вариант обеспечения взаимной совместимости, при котором доверяющая сторона из одного домена электронных сертификатов может использовать информацию об уполномоченном органе, управляющем другим доменом, для аутентификации субъекта из другого домена и наоборот. Обычно подобная информация об уполномоченном органе является результатом либо официального процесса лицензирования или аккредитации на территории действия другого домена, либо официального процесса аудита, выполняемого УЦ (или от его имени) того домена, в который входит доверяющая сторона. С технической точки зрения данная информация может храниться в виде значения поля сертификата, доступного доверяющей стороне.

В отличие от кросс-сертификации, при взаимном признании ответственность за принятие решения о доверии другому домену электронных сертификатов лежит на доверяющей стороне или на владельце приложения или службы, а не на УЦ, которому непосредственно доверяет доверяющая сторона. При этом не обязательно иметь подписанный договор или соглашение между двумя доменами.

При взаимном признании детальное отображение соответствующих ПС и СПС не является необходимым. Вместо этого доверяющая сторона (с помощью имеющегося приложения) принимает решение о принятии внешнего сертификата для заявленных целей в зависимости от того, был ли этот сертификат издан внешним УЦ, заслуживающим доверие.

УЦ считается заслуживающим доверие, если он получил лицензию/аккредитацию от соответствующего уполномоченного органа или прошел официальную проверку независимой доверенной стороной. Кроме того, доверяющая сторона должна иметь возможность в одностороннем порядке принимать обоснованное решение, опираясь на политики, описанные в ПС и СПС внешнего домена. Следовательно, данный процесс относительно менее сложен, чем кросс-сертификация, особенно в отношении согласования политик и правовой гармонизации. Данный процесс по своей сути является масштабируемым.

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

Кратко говоря, при взаимном признании принятие решения о доверии внешнему сертификату лежит на доверяющей стороне, а не на УЦ.

9.2.5 Вариант 4. Кросс-сертификация

При кросс-сертификации принятие решения о доверии смещается на уровень соглашений между удостоверяющими центрами. Затем эти соглашения воплощаются в технических протоколах, обеспечивающих взаимную приемлемость. Данная модель является более сложной для реализации, чем варианты 1, 2 или 3, но и более прозрачной для пользователя и, следовательно, более легкой для поддержки с позиции конечного пользователя. Это также означает, что конечный пользователь не обязан брать на себя ответственность за принятие решения о доверии, поскольку оно остается за УЦ домена этого пользователя.

Кросс-сертификация приводит к двустороннему сближению, когда два домена (целиком или частично) объединяются в один более крупный домен посредством детально разработанного процесса, осуществляемого двумя представительными УЦ. Для иерархий УЦ представительным обычно является корневой УЦ. Однако кросс-сертификация может также быть реализована между любыми двумя УЦ. В последнем случае каждый домен образован только одним УЦ и его абонентами. Чтобы кросс-сертификация была возможна, необходима совместимость на прикладном уровне, уровне политик и техническом уровне. Если она обеспечена, то для доверяющей стороны в доменах УЦ, охваченных кросс-сертификацией, перемещение информации является прозрачным, а за принятие решения о доверии отвечают УЦ.

Процесс кросс-сертификации требует детального отображения соответствующих политик каждого УЦ друг на друга, а необходимые для этого усилия будут возрастать в геометрической прогрессии по мере включения домена нового УЦ в объединенный домен. Таким образом, возникают проблемы масштабируемости. Существует также риск, что третий УЦ может достичь кросс-сертификации со вторым УЦ, но при этом признает политику первого УЦ неподходящей. В подобной ситуации УЦ-3 не может исключить УЦ-1 из объединенного домена. Поэтому кросс-сертификация больше подходит для относительно закрытых моделей здравоохранения и наиболее пригодна для открытых, но ограниченных

систем. Она является предпочтительной в ситуации, когда два домена принадлежат двум рабочим структурам, между которыми налажено тесное взаимодействие. Например, оба рабочих домена могут совместно использовать один набор приложений и служб, скажем, электронную почту и финансовые прикладные программы (см. [12]).

Кратко говоря, при кросс-сертификации ответственность за принятие решения о доверии внешнему сертификату возложена на УЦ.

9.2.6 Вариант 5. Мосты доверия

Модель моста доверия УЦ основана на принятии всеми УЦ в рамках потенциального объединения доменов УЦ общего минимального набора стандартов. Эти минимальные стандарты затем включаются в ПС и СПС всех этих УЦ. Отличие данной модели от кросс-сертификации состоит в том, что отдельные УЦ могут иметь собственные местные требования помимо общего минимального набора стандартов. Эти местные требования не являются необходимыми для мостовых сертификатов доверяющих сторон, не входящих в домен местного УЦ. Данная модель наиболее пригодна там, где все УЦ имеют значительный общий интерес и готовы допустить некоторые местные вариации, что может иметь место, например, в случае кросс-сертификации между центральными и региональными органами управления здравоохранения.

В данной модели отдельные организации могут создавать собственные УЦ, а позже принять решение, присоединиться к мосту доверия между УЦ или нет.

Кратко говоря, в модели моста доверия между УЦ ответственность за принятие решения о доверии внешнему сертификату возложена на УЦ, а не на доверяющую сторону.

9.3 Практическое применение вариантов

Настоящий стандарт исходит из того, что между территориями существуют административные и политические различия. Поэтому может оказаться приемлемым любой из представленных выше вариантов. Какой бы вариант не был выбран, настоящий стандарт будет полезен при его реализации.

Для достижения максимальной гибкости в ИСО 17090-2 определены профили мостовых сертификатов и поля сертификатов УЦ, предназначенные для передачи статуса аудита УЦ и аккредитации аудиторов, поддерживающих взаимное признание.

Приложение А
(справочное)

Сценарии использования электронных сертификатов в здравоохранении

А.1 Введение

Приведенные в настоящем приложении высокоуровневые варианты реализации, или сценарии, представляют основные административные и технические требования к решениям по применению электронных сертификатов, обеспечивающих широкое перекрестное взаимодействие в сфере здравоохранения.

Вначале описаны общие требования, относящиеся к базовым принципам обеспечения неприкосновенности личной жизни и информационной 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 к решению по применению электронных сертификатов.

А.2 Комментарии к сценариям

Сценарии оказания медицинской помощи, изложенные в разделе А.3, показывают, как электронные сертификаты можно использовать в здравоохранении. Каждый из сценариев должен:

- управляться политикой: сценарии предназначены для демонстрации того, как с помощью электронных сертификатов можно обеспечить выполнение требований сферы здравоохранения, ориентированных на реализацию международных, национальных и местных требований, в целях использования информации, необходимой для предоставления медицинской помощи отдельным лицам и популяциям, по ее прямому назначению;
- соответствовать сфере здравоохранения: в связи с распределенным характером оказания медицинской помощи во всем мире, а также широким спектром лиц и организаций, которые должны активно сотрудничать для обеспечения преемственности оказания медицинской помощи, необходимо, чтобы любой процесс применения электронных сертификатов мог функционировать в разных условиях оказания медицинской помощи, включая лечение в больницах и на дому, в государственном и частном секторе;
- быть технологически нейтральным: одной из главных целей разработки стандарта электронных сертификатов для сферы здравоохранения является обеспечение безопасной передачи информации между поставщиками медицинской помощи, ее потребителями, страховщиками и другими участвующими сторонами независимо от производителя, аппаратного обеспечения, операционной системы или выполняемых приложений;
- удовлетворять существующим и возникающим требованиям к неприкосновенности личной жизни: если электронные медицинские приложения должны широко использоваться, то им должны доверять поставщики медицинской помощи и пациенты. Забота о неприкосновенности личной жизни и информационной безопасности призвана обеспечить кредит доверия;
- быть удобным в использовании: службы обеспечения безопасности, использующие электронные сертификаты, не должны мешать выполнению авторизованной функции медицинского специалиста или организации. Если повседневная работа системы обеспечения безопасности становится слишком обременительной, то врачи будут стараться обойти ее или не будут достаточно точно выполнять необходимые процедуры. Если это происходит, то возникает значительный риск нарушения безопасности.

А.3 Службы, иллюстрируемые медицинскими сценариями

Медицинские службы и сценарии представлены в таблице А.1.

Таблица А.1 — Медицинские службы и сценарии

Сервис	Номер сценария															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
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	X

Окончание таблицы А.1

Сервис	Номер сценария															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Сценарии:
1 Доступ отделения скорой помощи к медицинским картам.
2 Временное обслуживание (скорая помощь).
3 Регистрация нового клиента.
4 Дистанционный доступ к медицинским изображениям.
5 Автоматическая передача результатов.
6 Передача результатов исследований и уведомлений от врача.
7 Обсуждение хода лечения между врачом и пациентом.
8 Передача эпикриза.
9 Вопрос пациента провизору.
10 Переписка пациента с врачом.
11 Дистанционный доступ к медицинской информационной системе.
12 Доступ в экстренной ситуации.
13 Дистанционный ввод медицинской информации.
14 Электронный рецепт.
15 Аутентификация назначения врача.
16 Потенциальные приложения электронной подписи в сфере здравоохранения.

А.4 Описание сценариев

А.4.1 Доступ отделения скорой помощи к медицинским картам

Описание сценария: Пациент, прибывший из другой страны, доставлен в отделение скорой помощи. Пациент не может связно отвечать на вопросы, поэтому достоверный анамнез невозможен. Полис медицинского страхования находится в его бумажнике, а его личность установлена по паспорту.

Без электронных сертификатов: Используя информацию из полиса медицинского страхования, дежурный врач отделения скорой помощи делает международный звонок в указанную страховую медицинскую организацию. Поскольку часовые пояса различаются, врача просят перезвонить, когда откроется административный офис. Врач осматривает пациента. Причина бессвязности речи пациента неясна.

С электронными сертификатами: Используя информацию из полиса медицинского страхования, дежурный врач отделения скорой помощи выходит через Интернет на сайт страховой медицинской организации пациента и вводит свой электронный сертификат, идентифицируя себя в своей текущей роли врача отделения скорой помощи. Веб-сервис медицинской страховой компании определяет достоверность электронного удостоверения личности путем проверки электронной подписи сертификата и того, что он не отозван и срок его действия не истек. Поскольку удостоверение личности подтверждено и соответствует текущим стандартам, оно принимается веб-сервисом страховой медицинской организации, и разрешается доступ к медицинской карте пациента. В регистрационном журнале веб-сервиса создается запись о предоставлении доступа, содержащая дату и время, фамилию, имя, отчество дежурного врача, номер его сертификата на право оказания медицинской помощи, идентификацию организации, которой принадлежит отделение скорой помощи. Врач получает из медицинской карты пациента сведения об анамнезе, об аллергических реакциях, о текущих медикаментозных назначениях и недавних изменениях в медикаментозной терапии, которые могли вызвать побочную реакцию. После оказания пациенту медицинской помощи врач отправляет зашифрованное сообщение с электронной подписью о посещении отделения скорой помощи в страховую медицинскую организацию, которая помещает его в электронную медицинскую карту пациента, указывая симптомы, диагноз, оказанное лечение и его результат.

А.4.2 Временное обслуживание (скорая помощь)

Описание сценария: Сильное 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.

Без электронных сертификатов: Невозможно сразу же проверить квалификацию и сертификаты медицинских работников, предлагающих помощь. Также невозможно обеспечить, что ранее поданные предложения о помощи не будут отклонены.

С электронными сертификатами: Предложения помощи от медицинских работников немедленно проверяют на достоверность с помощью чтения их электронных сертификатов. Сообщения с предложением помощи не могут быть отклонены, поскольку они заверены электронной подписью с использованием закрытых ключей 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 приобрести программу медицинского страхования. Он обращается к домашней странице страховой медицинской организации, на которой выложены образцы регистрационных форм. Он заполняет соответствующую форму и посылает ее на электронный почтовый ящик договорного отдела. Форма проверяется и направляется в отдел медицинского осмотра. Последний 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 медицинского осмотра, и данная информация передается обратно в договорной отдел, который посылает мистеру Чарльзу контракт, по которому он обязуется оплачивать ежемесячный взнос со своего текущего счета. Договорной отдел регистрирует нового клиента и отправляет распоряжение о выдаче его страхового полиса с фотографией. В процессе регистрации 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 выгрузке электронного сертификата из оформленной ему программы медицинского страхования.

Без электронных сертификатов: Ни новый клиент не имеет возможности надежно удостоверить свою личность врачу, ни врач не может идентифицировать себя пациенту. Хотя существуют другие средства шифрования сообщений, которыми они обмениваются, но эти средства не могут обеспечить сочетание аутентичности и конфиденциальности.

С электронными сертификатами: Используя выданный новый электронный сертификат, мистер Чарльз может получить доступ к службе поддержки клиентов через Интернет, включая доступ к части его персональных медицинских данных. Он может также обмениваться защищенными электронными письмами со своим лечащим врачом. Сертификат электронной подписи позволяет мистеру Чарльзу предоставить доступ к своей медицинской карте другим поставщикам медицинской помощи (например, поставщику медицинской помощи, к которому он обратится за пределами своей территории проживания).

А.4.4 Дистанционный доступ к медицинским изображениям

Описание сценария: Врач-специалист по дистанционной обработке медицинских изображений интерпретирует серию ангиограмм, выведенных на экран персонального компьютера, и вводит текст заключения. У врача высокая рабочая нагрузка (10—15 серий ангиограмм в день) и он предпочитает взять часть работы на дом. Дома врач выходит через Интернет на сервер медицинских изображений, используя свой электронный сертификат для аутентификации, и загружает изображения. При просмотре изображений на своем домашнем компьютере врач также получает через Интернет доступ к медицинской информационной системе своего учреждения, чтобы получить другую медицинскую информацию о пациенте. Врач уверен в правильности изображений, поскольку применяемая им программа обеспечивает проверку целостности с использованием алгоритма хеширования, подтверждающую целостность сообщения. Врач вводит результаты анализа изображения в заключение и может дистанционно заверить это заключение своей электронной подписью.

Без электронных сертификатов: Врач не в состоянии осуществить свою аутентификацию в лечебном учреждении с тем же уровнем доверия, что обеспечивается при использования электронного сертификата. Для медицинского учреждения это означает наличие элемента риска того, что изображение может быть выгружено подставным лицом. Протоколы исследований и заключения врача, отправленные в электронном виде, подвергаются аналогичному риску. Врач также не может быть уверен, что загруженные изображения не искажены вследствие ошибок передачи или преднамеренного изменения.

С электронными сертификатами: Врач может аутентифицировать себя медицинскому учреждению с уровнем доверия, соответствующим действующему законодательству. Врач может быть уверен, что загруженные изображения не искажены и что он даст заключение по аутентичным изображениям. Медицинское учреждение также может доверять электронной подписи врача, подтверждающей, что он является автором переданного протокола.

А.4.5 Автоматическая передача результатов

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 входит на веб-сайт медицинского учреждения, используя свой идентификатор медицинского работника (ID) и пароль (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 к специалистам по контролю массы тела, чтобы узнать, как можно снизить уровень холестерина с помощью диеты и упражнений. Врач также рекомендует проводить анализ уровня холестерина и приходить на прием раз в полгода. Пациент просит врача внести результаты в систему ведения его персональной медицинский карты, доступную через Интернет. Веб-сайт пациента содержит несколько ссылок на дополнительную информацию. Одна из ссылок связана с информацией по анализу уровня холестерина в крови, другая — с режимом, назначенным специалистами по контролю уровня липидов, а третья отсылает к персональным рекомендациям по диете, предложенным на основе текущих клинических протоколов, учитывающих различные данные о пациенте (например, возраст). Рекомендации по диете содержат дальнейшие ссылки на программу по планированию изменения режима, которая помогает пациенту разработать собственную диету и придерживаться ее в течение шести месяцев.

Без электронных сертификатов: Лаборатория не может быть уверена, что врач получил сообщение. Нет гарантии, что сообщение не было прочитано или изменено.

С электронными сертификатами: Электронная подпись подтвердит врачу, что сообщение действительно пришло от лаборатории, и ссылки, указывающие на рекомендации пациенту по контролю уровня холестерина, являются действительными. Подтверждение сообщения, заверенное электронной подписью врача, уведомит лабораторию, что врач действительно получил сообщение.

А.4.6 Передача результатов исследований и уведомлений от врача

Описание сценария: Во время планового приема хирург назначает пациенту общий анализ крови. Обсудив с пациентом удобную дату и время, хирург отмечает на экранной форме ввода направления на анализ, что результаты следует отправить пациенту через Интернет после того, как хирург ознакомится с ними и сможет прокомментировать. Полученные результаты в целом оказываются в пределах нормы, только один показатель слегка повышен. Хирургу известно, что для данного пациента нет поводов для беспокойства, поэтому он формирует краткое примечание по этому факту и присоединяет его к результатам анализа.
Позже в тот же день пациент получает автоматическое уведомление по электронной почте, что на защищенном веб-сайте его ожидает сообщение от хирурга. Он переходит по адресу веб-сайта, указанному в уведомлении, вводит номер своей медицинской карты и пароль, после чего получает возможность прочитать результаты лабораторного анализа и сообщение хирурга. Веб-сайт автоматически определяет, что это результат общего анализа крови, и предоставляет на экране ссылку на раздел медицинской энциклопедии, содержащий описание общего анализа крови и его результатов, доступное непрофессионалу.

Без электронных сертификатов: Не имея возможности убедиться с достаточной степенью уверенности, что электронное сообщение действительно отправлено лабораторией или хирургом, а также, что оно было передано защищенным способом, пациент получает результаты по почте, замечает слегка повышенный показатель и звонит хирургу для получения разъяснений. Хирург принимает другого пациента и не может ответить, а у пациента назначена важная встреча. В результате они связываются, но после нескольких дней беспокойства со стороны пациента и значительного числа неудачных попыток дозвониться со стороны хирурга.

С электронными сертификатами: Результаты быстро направляются пациенту надежным и защищенным способом. Пациент может прочитать примечание хирурга в его электронном сообщении и получить доступ к веб-сайтам для получения необходимой информации, поэтому причин для беспокойства не возникнет и без телефонного разговора с хирургом.

А.4.7 Обсуждение хода лечения между врачом и пациентом

Описание сценария: У пациента с определенной программой медицинского страхования возник вопрос о ходе его лечения. Он входит на веб-сайт своего врача, используя для аутентификации доверенный электронный сертификат, заполняет форму запроса и нажимает кнопку «Отправить» для начала переписки:
«Здравствуйте, д-р С.
Вчера вы сказали мне, что надо менять повязку на ране. Но я не помню, как часто это надо делать. Вы сказали что-то вроде того, что не надо менять повязку слишком часто, но я не помню, раз в неделю или иначе. Забыл еще спросить, останется ли большой шрам?»

Через пару часов медсестра контакт-центра читает сообщение пациента, находит, что оно не срочное и что на него должен ответить участковый терапевт. Вскоре после этого сообщение пациента появляется на экране компьютера участкового терапевта, координирующего медицинскую помощь, оказываемую этому пациенту. Участковый терапевт вводит ответ и заверяет сообщение своей электронной подписью. На следующее утро пациент снова входит на веб-сайт своего врача и читает сообщение:
«Здравствуйте, (имя и отчество пациента).
В течение следующих двух недель меняйте перевязку один раз в четыре—пять дней, если она не мокнет, в противном случае меняйте по мере намокания. После этого придите ко мне на прием, и мы обсудим дальнейшие действия. Что касается шрама, он останется у вас навсегда, но не очень заметный — всего лишь небольшая линия».

Без электронных сертификатов: Отсутствие надежного способа аутентификации означает, что медицинское учреждение, в котором работает врач, не имеет возможности проверить, что электронное сообщение пришло именно от пациента (имя и отчество пациента), а не от иного лица, желающего получить бесплатный совет. Пациент также не может быть уверен, что ответ действительно был отправлен данным врачом, что этот ответ не был перехвачен и прочитан кем-либо еще.

С электронными сертификатами: Страховая медицинская организация и врач могут быть уверены в защищенности переписки, которую они ведут с идентифицированным и действительным участником одной из их программ медицинского страхования. Пациент может быть уверен, что именно его врач получил его запрос и отправил ему ответ.

А.4.8 Передача эпикриза

Описание сценария: Регистр пациентов с факторами риска диабета собирает от различных медицинских информационных систем клинические данные о пациентах с диабетом. Программное обеспечение регистра, разработанное на основе клинических руководств, позволяет автоматически сгенерировать эпикриз, в котором суммируется состояние пациента, анамнез и факторы риска, а также предлагаются дальнейшие шаги. После проверки врачом этот эпикриз передается пациенту через веб-сайт медицинского учреждения. Пациент входит на этот веб-сайт, используя электронный сертификат, выданный УЦ данного медицинского учреждения. Когда пациент просматривает эпикриз, включенные в него гипертекстовые ссылки позволяют пациенту легко получить необходимую дополнительную информацию (например, расписание консультаций, описание анализов, санитарное просвещение), сделать предварительную запись на прием или отправить сообщение врачу. В системе предусмотрена проверка того, что пациент получил доступ к эпикризу.

Без электронных сертификатов: Пациент не может быть в достаточной мере уверен, что веб-сайт действительно принадлежит регистру пациентов с факторами риска диабета и что обеспечена конфиденциальность взаимодействия с этим сайтом. Регистр не может гарантировать, что данный пациент осуществил доступ к сайту и получил информацию.

С электронными сертификатами: Использование электронных сертификатов обеспечивает пациенту и регистру взаимную аутентификацию, позволяет вести конфиденциальный обмен данными. Регистр может быть уверен, что данный пациент осуществил доступ к сайту и получил информацию.

А.4.9 Вопрос пациента провизору

Описание сценария: У семилетней дочери клиента страховой медицинской организации астма. Педиатр недавно прописал ей кромолин, но данный клиент не может определить, когда ингалятор пуст, а когда полон. Он входит на веб-сайт своего медицинского учреждения в поисках нужной информации, но ему еще не все понятно, и он направляет вопрос дежурному провизору, как определить, что ингалятор пуст. Дежурный провизор использует электронную почту с доступом к каталогу электронных сертификатов, в котором хранятся электронный сертификат и открытый ключ клиента, и посылает зашифрованное сообщение, используя шаблон, предусмотренный для ответа на данный вопрос, а также добавляет несколько строчек от себя и телефонный номер для связи, если вопросы еще останутся.

Без электронных сертификатов: Провизор не может аутентифицировать клиента медицинской страховой компании с достаточной степенью достоверности. Он может отправить защищенное сообщение, которое не может быть аутентифицировано.

С электронными сертификатами: Имеется возможность аутентифицировать клиента и отправить ему зашифрованное сообщение. Клиент может быть уверен, что оно пришло именно от провизора.

А.4.10 Переписка пациента с врачом

Описание сценария: У пациента появилась сыпь, и он обратился к дерматологу, который прописал ему мазь и сказал, что если сыпь не пройдет в течение трех недель, надо сообщить об этом, чтобы врач выписал другое лекарство.

Три недели спустя сыпь практически не изменилась, поэтому пациент входит на веб-сайт поликлиники, воспользовавшись для аутентификации своим электронным сертификатом. Пациент отправляет врачу защищенное неструктурированное сообщение:
«Я применял эту мазь уже в течение трех недель, а улучшения нет. Что делать?»
Врач выписывает новый рецепт и сообщает пациенту, что он может купить мазь в аптеке или заказать ее через Интернет. Когда пациент читает сообщение дерматолога на защищенном веб-сайте, он может перейти в раздел аптечных заказов данного сайта и заказать мазь с доставкой на дом.

Без электронных сертификатов: Врач не может аутентифицировать пациента с достаточной степенью уверенности, чтобы отправить по электронной почте рекомендации о дальнейшем лечении.

С электронными сертификатами: Врач и пациент могут аутентифицировать друг друга, а также провизора. Обмен сообщениями может быть осуществлен конфиденциально, и новая мазь может быть заказана в аптеке. Все стороны уверены, что отправили свои сообщения соответствующему адресату.

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);
- уведомления с отправкой пациенту;
- зарегистрированные;
- обработанные.

Без электронных сертификатов: Невозможность аутентифицировать личность врача с достаточной степенью уверенности делает вышеприведенный обмен данными невозможным.

С электронными сертификатами: Безотказное подтверждение источника отправления и факта получения сообщения, целостность и конфиденциальность этих действий и сообщений обеспечиваются медицинской информационной системой и веб-сайтом, использующими электронные сертификаты 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 Северной Америке, 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 электронного сертификата, 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 в том, 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.

Без электронных сертификатов: 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.

С электронными сертификатами: 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 Дистанционный ввод медицинской информации

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 принимает и записывает медицинский стенографист в Индии, работающий 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, он снова отправляется 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.

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

С электронными сертификатами: 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 приготовлены и ожидают его.

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

С электронными сертификатами: 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 успокаивается после еды и антацида, 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.

Без электронных сертификатов: 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.

С электронными сертификатами: 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.

А.4.16 Потенциальные приложения электронной подписи в сфере здравоохранения

Описание сценария: Ниже представлен список категорий документов, которые требуют подпись квалифицированного медицинского работника. Законодательные и административные процедуры устанавливают это требование в отношении подписи:

1) медицинских справок:
- об оказанных медицинских услугах (платежи врачу или больнице, справка об уплате налогов),
- нетрудоспособности,
- пропуске школы по болезни,
- отпуске социального характера (отпуск по уходу за ребенком, отпуск по уходу за больным членом семьи),

- болезни для страхования от аннулирования,
- неспособности дать осознанное согласие (невменяемость, например слабоумие),
- срочной медицинской помощи,
- смерти,
- рождении;

2) рецептов:
- на лекарства,
- физиотерапию;

3) при возмещении средств:
- за лекарства,
- ортопедические изделия и т. д.;

4) медицинского освидетельствования в случае:
- несчастного случая,
- страхования,
- заявления о приеме на работу,
- помощи третьим сторонам, льготы, получение пособия,
- разрешения на получение парковочного места для инвалидов,
- выделения социальных пособий,
- предоставления путевки в дом для престарелых и инвалидов;

5) направлений к специалистам или для получения медицинской помощи и сдачи анализов:
- в лаборатории радиологии,
- клинической лаборатории,
- патологоанатомической лаборатории,
- а также при направлении к врачу,
- при госпитализации: прием, продление срока пребывания, выписка.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 17090-2:2008	—	*
ИСО 17090-3:2008	—	*
* 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.		

Библиография

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

[2] ISO/IEC 8824-1:2008, 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 — Part 1

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

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

[6] ISO/IEC 9594-8:2008, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8

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

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

[9] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

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

[11] IETF/RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

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

[13] IETF/RFC 3126, Electronic Signature Formats for long term electronic signatures

[14] IETF/RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

[15] IETF/RFC 3280, Internet X.509 Public Key Infrastructure CRL Profile

[16] IETF/RFC 3281, An Internet Attribute Certificate Profile for Authorization

[17] Ankney, R., CertCo. Privilege Management Infrastructure, v0.4, August 24, 1999

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

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

[20] Bernd B., & Roger-France F. A Systemic Approach for Secure Health Information Systems. Int. J. Med. Inform. 2001, pp. 51—78

[21] Canadian Institute for Health Information. Model Digital Signature and Confidentiality Certificate Policies, June 30, 2001

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

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

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

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

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

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

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

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

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

УДК 004:61 ОКС 35.240.80

Ключевые слова: здравоохранение, информатизация здоровья, структуры данных, персональные медицинские приборы передачи данных, информационное взаимодействие, номенклатура

Редактор *А.Ф. Колчин*
Технический редактор *В.Ю. Фотиева*
Корректор *М.В. Бучная*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 20.04.2016. Подписано в печать 26.04.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,70. Тираж 30 экз. Зак. 1148.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru