ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р ИСО 17090-2— 2010**

# Информатизация здоровья

# ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

## Часть 2

## Профиль сертификата

**ISO 17090-2:2008**
**Health informatics — Public key infrastructure — Part 2: Certificate profile**
**(IDT)**

**Издание официальное**

Москва
Стандартинформ
2011

gost.e-ecolog.ru

## Предисловие

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

**Сведения о стандарте**

1 ПОДГОТОВЛЕН на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4, который выполнен Федеральным государственным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Росздрава» (ЦНИИОИЗ Росздрава) и обществом с ограниченной ответственностью «Корпоративные электронные системы»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Росздрава — постоянным представителем ISO TC 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 октября 2010 г. № 328-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 17090-2:2008 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 2. Профиль сертификата» (ISO 17090-2:2008 «Health informatics — Public key infrastructure — Part 2: Certificate profile»)

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (пункт 3.5).

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 ВПЕРВЫЕ

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

© Стандартинформ, 2011

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

## Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Условные обозначения и сокращения . . . 1
5 Политики сертификатов в здравоохранении . . . 2
5.1 Типы сертификатов, необходимых для здравоохранения . . . 2
5.2 Сертификаты центра сертификации . . . 2
5.3 Кросс-сертификаты (сертификаты посреднических центров сертификации) . . . 3
5.4 Сертификаты конечных объектов . . . 3
6 Общие требования к сертификатам . . . 5
6.1 Соответствие сертификата . . . 5
6.2 Общие поля всех типов сертификатов . . . 6
6.3 Спецификации общих полей . . . 6
6.4 Требования для каждого типа сертификатов в здравоохранении . . . 9
7 Использование расширений сертификата . . . 12
7.1 Общие сведения . . . 12
7.2 Общие расширения . . . 12
7.3 Специальные атрибуты каталога субъектов . . . 13
7.4 Расширение объявлений квалифицированного сертификата «qcStatements» . . . 15
7.5 Требования для каждого типа сертификатов в здравоохранении . . . 15
Приложение А (справочное). Примеры профилей сертификатов . . . 18
Приложение ДА (справочное). Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 25
Библиография . . . 25

## Введение

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

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

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

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

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

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

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

Технология цифровых сертификатов активно развивается в рамках определенных направлений, не специфичных для здравоохранения. Непрерывно проводится важнейшая работа по стандартизации и в некоторых случаях по правовому обеспечению такой технологии. В то же время поставщики медицинских услуг во многих странах уже используют или планируют использовать цифровые 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 для обеспечения использования цифровых сертификатов в целях обмена медицинской информацией в пределах одного домена, между доменами и за пределами границ одной юрисдикции. Его целью является создание основ глобальной интероперабельности. Настоящий стандарт изначально предназначен для поддержки трансграничного обмена данными на основе

цифровых сертификатов, однако он также может служить руководством по широкому использованию цифровых сертификатов в здравоохранении на национальном или региональном уровнях. Интернет все шире используется как средство передачи медицинских данных между организациями здравоохранения и является единственным реальным вариантом для трансграничного обмена данными в этой сфере.

Настоящий стандарт должен рассматриваться как единое целое, поскольку каждая из трех его частей вносит свой вклад в определение того, как цифровые сертификаты могут использоваться для обеспечения сервисов безопасности в системе здравоохранения, включая аутентификацию, конфиденциальность, целостность данных и технические возможности поддержки качества электронной подписи.

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

ИСО 17090-2 определяет специфичные для сферы здравоохранения профили электронных сертификатов, основанных на международном стандарте X.509 и его профиле, определенном в спецификации IETF/RFC 2459 [1] для разных типов сертификатов.

ИСО 17090-3 имеет отношение к проблемам управления, связанным с внедрением цифровых сертификатов в сферу здравоохранения и их эксплуатацией. В нем определены структура политик сертификатов и минимальные требования к ним, а также структура сопутствующих отчетов по практическому применению сертификации.

ИСО 17090-3 основан на информационных рекомендациях IETF/RFC 2527 [2] и определяет принципы политик безопасности медицинской информации при ее трансграничной передаче. В нем также определен минимально необходимый уровень безопасности применительно к аспектам, специфичным для сферы здравоохранения.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Информатизация здоровья**

# ИНФРАСТРУКТУРА С ОТКРЫТЫМ КЛЮЧОМ

**Часть 2**

**Профиль сертификата**

Health informatics. Public key infrastructure. Part 2. Certificate profile

**Дата введения — 2011—08—01**

## 1 Область применения

Настоящий стандарт определяет основные профили сертификатов, требуемые для обмена медицинской информацией внутри одной организации, между организациями и при трансграничном обмене. Он определяет детали применения цифровых сертификатов в области здравоохранения и фокусируется, в частности, на особенностях профилей сертификатов, специфичных для здравоохранения.

## 2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

ИСО 17090-1:2008 Информатика в области здравоохранения. Инфраструктура открытого ключа. Часть 1. Обзор услуг цифрового сертификата (ISO 17090-1, Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services)

ИСО 17090-3:2008 Информатика в области здравоохранения. Инфраструктура открытого ключа. Часть 3. Менеджмент политики органа по сертификации (ISO 17090-3, Health informatics — Public key infrastructure — Part 3: Policy management of certification authority)

IETF/RFC 3280 Интернет. Профиль сертификата X.509 инфраструктуры с открытым ключом и списка отозванных сертификатов (CRL) (IETF/RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

IETF/RFC 3281 Интернет. Профиль сертификата атрибута для авторизации (IETF/RFC 3281, An Internet Attribute Certificate Profile for Authorization)

IETF/RFC 3739 Интернет. Профиль аттестационных сертификатов инфраструктуры с открытым ключом (IETF/RFC 3739, Internet X.509 Public Key Infrastructure Qualified Certificates Profile)

## 3 Термины и определения

В настоящем стандарте применены термины с соответствующими определениями, установленные в ИСО 17090-1.

## 4 Условные обозначения и сокращения

ЦА центр присвоения атрибутов (AA — attribute authority)
СА сертификат атрибута (AC — attribute certificate)
ЦС центр сертификации (CA — certificate authority)

**Издание официальное**

ПС политика сертификата (CP — certificate policy)
ОПС отчет о практике сертификации (CPS — certification practice statement)
СОС список отозванных сертификатов (CRL — certificate revocation list)
СОК сертификат открытого ключа (PKC — public key certificate)
ИОК инфраструктура с открытым ключом (PKI — public key infrastructure)
ЦР центр регистрации (RA — registration authority)
ДТС доверенная третья сторона (TTP — trusted third party)

## 5 Политики сертификатов в здравоохранении

### 5.1 Типы сертификатов, необходимых для здравоохранения

Сертификаты идентичности должны выдаваться:

- лицам (квалифицированным медицинским работникам, вспомогательным медицинским работникам, субсидируемым поставщикам медицинских услуг, работникам поддерживающих организаций, а также пациентам/потребителям медицинской помощи);
- организациям (организациям здравоохранения и поддерживающим организациям);
- устройствам;
- приложениям.

Роли лиц и организаций должны быть записаны либо в самом сертификате идентичности (в расширении сертификата), либо в ассоциированном СА. Различные типы сертификата и их взаимоотношения показаны на рисунке 1.

### 5.2 Сертификаты центра сертификации

#### 5.2.1 Сертификаты корневых ЦС

Сертификаты корневых ЦС используются, если ЦС сам является субъектом сертификата. Они самоподписаны и применяются для выпуска сертификатов доверяющим им сторонам, включая подчиненные ЦС. Поле основных ограничений содержит признак, что субъектом сертификата является ЦС.

#### 5.2.2 Сертификаты подчиненных ЦС

Сертификаты подчиненных ЦС выпускаются для ЦС, который сертифицируется другим вышестоящим ЦС, наделенным правом выпускать сертификаты, или для других подчиненных ЦС, или для объектов.

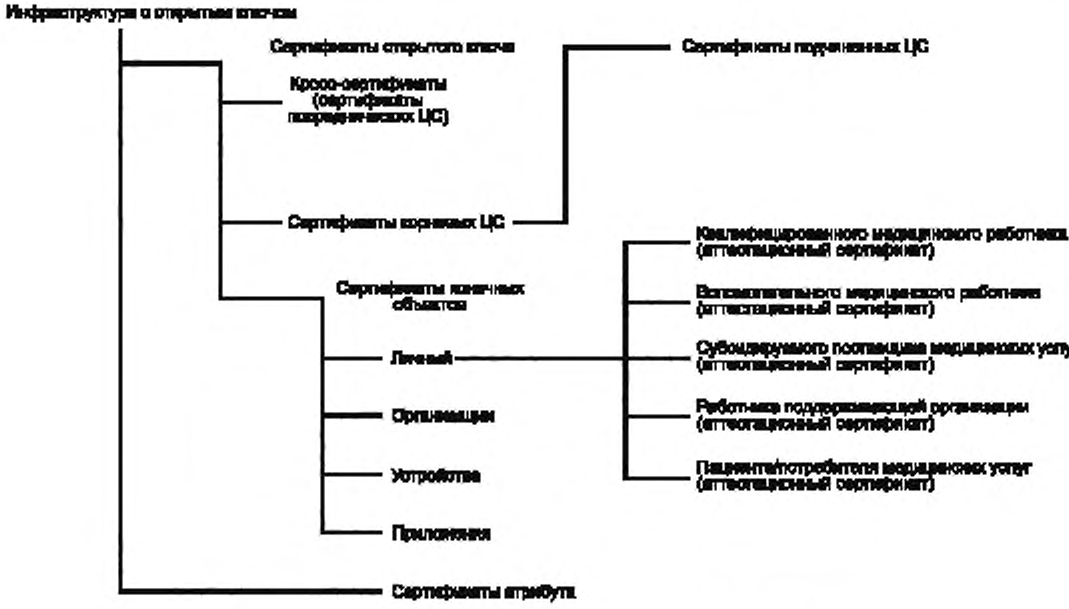



Рисунок 1 — Типы сертификатов, используемых в здравоохранении

### 5.3 Кросс-сертификаты (сертификаты посреднических центров сертификации)

В среде Интернет не приходится рассчитывать на наличие ЦС верхнего уровня, которому будут доверять организации здравоохранения, если они подчинены разным ведомствам или должны участвовать в трансграничном обмене информацией. Вместо этого в системе здравоохранения должны создаваться отдельные «островки доверия», каждый со своим корневым ЦС, обслуживающим группу учреждений здравоохранения, образованную по признаку специализации, ведомственной подчиненности или географического положения. Каждый корневой ЦС каждого «островка доверия» должен выдать кросс-сертификат другому корневому ЦС.

В такой ситуации группа ЦС может согласовать минимальный набор стандартов, включаемый в их политики и соответствующие отчеты о практике сертификации. Как только это сделано, доверяющая сторона может принять сертификат от ЦС, находящегося за пределами ее домена. Этот подход может быть особенно полезен региональным органам управления здравоохранением для организации межтерриториального обмена информацией.

Для взаимной сертификации различных доменов ЦС используется особый тип сертификатов — кросс-сертификаты (сертификаты посреднических ЦС). С их помощью обеспечивается масштабное развертывание приложений открытых ключей, например, защищенная электронная почта и другие приложения, требуемые для системы здравоохранения.

### 5.4 Сертификаты конечных объектов

#### 5.4.1 Общие сведения

Сертификаты конечных объектов выдаются таким объектам, как лица, организации, приложения или устройства.

Они называются сертификатами конечных объектов, поскольку не используются для выдачи сертификатов другим объектам.

#### 5.4.2 Сертификаты идентичности лиц

Сертификаты идентичности лиц относятся к подтипу сертификатов конечных объектов и предназначены для выдачи отдельным лицам в целях аутентификации.

Следующие пять типов действующих лиц в здравоохранении рассматриваются как отдельные лица:

a) квалифицированные медицинские работники:

- каждый владелец такого сертификата является медицинским работником, которому для выполнения профессиональных обязанностей необходимы сертификат или лицензия от органа государственного управления (см. ИСО 17090-1, подраздел 5.1). Эти сертификаты могут иметь тип аттестационного сертификата (см. ИСО 17090-1, подразделы 8.2 и 7.3 настоящего стандарта);

b) вспомогательные медицинские работники:

- каждый владелец такого сертификата является медицинским работником, которому для выполнения профессиональных обязанностей не требуется сертификат или лицензия от органа государственного управления (см. ИСО 17090-1, подраздел 5.1). Эти сертификаты могут иметь тип аттестационного сертификата;

c) субсидируемый поставщик медицинских услуг:

- каждый владелец такого сертификата является лицом, выполняющим определенные обязанности в системе здравоохранения по субсидии официальной организации здравоохранения или частнопрактикующего врача. Эти сертификаты могут иметь тип аттестационного сертификата;

d) работник поддерживающей организации:

- каждый владелец такого сертификата является работником организации здравоохранения или поддерживающей организации. Эти сертификаты могут иметь тип аттестационного сертификата;

e) пациент/потребитель медицинской помощи:

- каждый владелец такого сертификата является лицом, которое на определенном этапе либо получало, либо получает услуги квалифицированного или вспомогательного медицинского работника. Эти сертификаты могут иметь тип аттестационного сертификата.

#### 5.4.3 Сертификат идентичности организации

Организация, связанная с системой здравоохранения, может владеть сертификатом в целях идентификации или для шифрования данных. В настоящем стандарте предусмотрено указание ее названия в поле сертификата в соответствии с IETF/RFC 3647 [3].

#### 5.4.4 Сертификат идентичности устройства

Индивидуальная идентификация и аутентификация могут потребоваться таким устройствам, как сервер или медицинский прибор, например, устройство лучевой диагностики, монитор жизненно важных показателей или протезирующее устройство.

**5.4.5 Сертификат приложения**

Индивидуальная идентификация и аутентификация могут потребоваться такому приложению, как автоматизированная информационная система, например, система учета коечного фонда и движения пациентов.

Хотя настоящий стандарт посвящен в основном применению сертификатов поставщиков медицинской помощи, необходимо отметить, что пациентам/потребителям медицинских услуг для контроля своего здоровья все чаще необходимы данные, для защиты которых могут применяться цифровые сертификаты.

**5.4.6 CA**

CA представляет собой сертифицированную или заверенную цифровой подписью совокупность атрибутов. Структура CA похожа на структуру СОК. Основное отличие состоит в том, что CA не содержит открытый ключ. CA может содержать атрибуты, специфицирующие членство в группе, категорию допуска к информации и другие сведения о владельце сертификата, которые могут быть использованы для контроля доступа. Структура CA должна соответствовать IETF/RFC 3281.

В системе здравоохранения CA может выполнять существенную роль носителя сведений об авторизации.

Сведения об авторизации отличаются от информации о роли работника в системе здравоохранения или от лицензий, которые могут быть переданы в СОК. Наличие информации о роли или лицензии влияет на авторизацию, но само по себе не обязательно идентично авторизации. Важно отметить, что детальная спецификация CA еще не устоялась и будет уточняться по мере более широкого применения разработчиками информационных систем.

Синтаксис CA описан в IETF/RFC 3281.

Компоненты CA используются следующим образом.

Разные версии CA отличаются по номеру версии **«version»**. Если в CA присутствует поле свертки **«objectDigestInfo»** или если поле **«baseCertificateID»** идентифицирует издателя сертификата, то номер версии **«version»** должен быть **«v2»**.

Поле **«owner»** задает идентичность владельца CA. Обязательно должны быть указаны наименование издателя и серийный номер конкретного СОК. Могут быть указаны одно или несколько общих наименований, а указание свертки объекта запрещено.

Использование общих наименований **«GeneralName»** в качестве идентификации владельца заключает в себе тот риск, что они не могут обеспечить достаточно точной привязки наименования к открытому ключу, что затруднит применение CA для аутентификации идентичности владельца. Кроме того, некоторые формы общих наименований **«GeneralName»** (например, **«IPAddress»**) не годятся для наименования владельца CA, которого скорее можно отнести к роли, нежели к конкретному объекту. Необходимо ограничиться применением таких форм общего наименования, как отличительные имена, адреса, соответствующие спецификации ETF/RFC 822 [4] (электронная почта), и объектные идентификаторы (для имен ролей).

Поле **«issuer»** содержит идентификацию ЦС, выпустившего сертификат. Наименование издателя и серийный номер СОК должны быть указаны обязательно. Общие наименования указывать необязательно.

Поле **«signature»** идентифицирует криптографический алгоритм, используемый для цифровой подписи CA.

Поле **«serialNumber»** содержит серийный номер, уникально идентифицирующий CA среди всех сертификатов, выпущенных его издателем.

Поле **«attrCertValidityPeriod»** задает срок действия CA, представленный в формате генерализированного времени **«GeneralizedTime»**.

Поле **«attributes»** содержит атрибуты владельца сертификата, которые заверяются этим сертификатом (например, привилегии доступа).

Поле **«issuerUniqueID»** может быть использовано для идентификации издателя CA в инстанциях, которым одного имени издателя недостаточно.

Поле **«extensions»** позволяет добавлять новые поля к CA.

Детали использования CA в здравоохранении приведены в ИСО 17090-1:2008, подраздел 8.4.

**5.4.7 Сертификаты роли**

CA пользователя может содержать ссылку на другой CA, содержащий сведения о дополнительных привилегиях. Это является эффективным механизмом реализации привилегированных ролей.

В ряде организаций для выполнения определенных работ требуется авторизация на основе привилегий, назначенных ролям (обычно в сочетании с индивидуально назначенными привилегиями).

Претендент на привилегии может представить контролеру нечто, демонстрирующее наличие у него определенной роли (например, роли «продавца» или роли «покупателя»). Контролер может знать априори или узнать с помощью каких-либо средств, какие привилегии связаны с этой ролью, и принять положительное или отрицательное решение об авторизации.

Возможны следующие ситуации:

- любой ЦА может определять любое число ролей;
- сама роль и ее обладатели могут определяться и управляться раздельно с помощью отдельных ЦА;
- привилегии, назначенные данной роли, могут быть записаны в одном или нескольких СА;
- при необходимости обладателю роли может присваиваться только подмножество привилегий, назначенных роли;
- право владения ролью может делегироваться;
- ролям и правам владения ими могут назначаться определенные сроки действия.

Объекту может быть присвоен СА, содержащий атрибут, уведомляющий, что этому объекту назначена определенная роль. Этот сертификат имеет расширение, содержащее указатель на другой СА, определяющий эту роль (такой сертификат роли указывает роль в качестве владельца и содержит список привилегий, назначенных этой роли). Издатели сертификата объекта и сертификата роли могут быть независимыми, и эти сертификаты могут управляться (прекращать действие, отзываться и т. д.) отдельно друг от друга.

Не все формы общего наименования **«GeneralName»** пригодны для использования в качестве имени роли. Полезнее всего использовать объектные идентификаторы и отличительные имена.

## 6 Общие требования к сертификатам

### 6.1 Соответствие сертификата

Ко всем сертификатам, определенным в настоящем стандарте, предъявляются следующие требования:

- они должны являться сертификатами формата X.509 версии 3 [5];
- они должны соответствовать IETF/RFC 3280. Отклонения от нее допускаются только в том случае, если они соответствуют предложенным решениям выявленных проблем этой спецификации;
- сертификаты, подтверждающие индивидуальную идентичность, должны соответствовать IETF/RFC 3739. Отклонения от нее допускаются только в том случае, если они соответствуют предложенным решениям выявленных проблем этой спецификации;
- поле **«signature»** должно идентифицировать используемый алгоритм цифровой подписи;
- минимальная длина сертифицированного открытого ключа должна зависеть от используемого алгоритма. Длины ключей должны соответствовать ИСО 17090-3, подпункт 7.6.1.5;
- назначение ключа для шифрования не должно сочетаться ни с неоспоримостью, ни с цифровой подписью (см. 7.2.3).

Ниже описаны общие элементы всех цифровых сертификатов, предназначенных для здравоохранения и показанных на рисунке 1. Эти элементы одинаковы у различных типов сертификатов.

**Certificate ::= SIGNED { SEQUENCE {**
**version [0] Version DEFAULT v1,**
**serialNumber CertificateSerialNumber,**
**signature AlgorithmIdentifier,**
**issuer Name,**
**validity Validity,**
**subject Name,**
**subjectPublicKeyInfo SubjectPublicKeyInfo,**
**issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,**
**subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,**
**extensions [3] Extensions MANDATORY,**

**version** версия кодированного сертификата. Должна иметь значение v3.

.....

### 6.2 Общие поля всех типов сертификатов

1) Поле **«serialNumber»** имеет целое значение, присваиваемое ЦС каждому сертификату. Оно предназначено для уникальной идентификации сертификатов. Значение **«serialNumber»** должно быть уникальным для каждого сертификата, выпущенного данным ЦС (то есть наименование издателя сертификата в сочетании с серийным номером является глобально уникальным идентификатором).

2) Поле **«signature»** содержит идентификатор алгоритма, использованного ЦС для подписи сертификата.

3) Поле **«issuer»** идентифицирует наименование организации, подписавшей и выпустившей сертификат. Значение этого поля представляет собой соответствующую ISO [6] структуру имени, состав которой соответствует определению класса объектов роли в организации **«organizationalRole»**, находящегося под классом объектов организации **«organization»** или подразделения **«organizationUnit»**.

4) Поле **«validity»** содержит интервал времени, в течение которого ЦС гарантирует действительность информации, содержащейся в сертификате. При выдаче сертификата квалифицированному медицинскому работнику ЦС должен принять меры, чтобы срок действия цифрового сертификата не превысил срок действия сертификата специалиста или профессиональной лицензии. Чтобы выполнить это условие, ЦС должен либо установить срок действия цифрового сертификата, не превышающий срока действия сертификата специалиста (профессиональной лицензии), либо надежным образом получить подтверждение, что сертификат специалиста (лицензия) продлен до истечения его срока действия, а если срок истек, а подтверждение не получено, — отозвать цифровой сертификат или приостановить его действие.

Примечание — Отличительные правила кодирования (Distinguished Encoding Rules — DER) разрешают использовать несколько способов форматирования значений даты и времени типа «UTCTime» и «GeneralizedTime». Чтобы минимизировать проблемы с верификацией цифровой подписи, в реализациях стандарта важно использовать один и тот же формат. Если год больше или равен 2050, то время должно кодироваться, используя формат «GeneralizedTime». Чтобы кодирование значений типа «UTCTime» было совместимым, необходимо кодировать их, используя формат «Z», и не опускать поле секунд, даже если оно имеет значение 00 (т. е. формат должен быть YYMMDDHHMMSSZ). При таком кодировании поле года YY должно интерпретироваться как 19YY, если YY больше или равно 50, и как 20YY, если YY меньше 50. Когда используется тип «GeneralizedTime», то значение этого типа должно кодироваться, используя формат «Z», и поле секунд должно быть включено (то есть формат должен быть YYYYMMDDHHMMSSZ).

5) Поле **«subject»** идентифицирует наименование субъекта, ассоциированного с открытым ключом, содержащимся в поле **«subjectPublicKeyInfo»**.

6) В поле **«subjectPublicKeyInfo»** хранятся открытый ключ и идентификатор алгоритма применения этого ключа.

7) Необязательное поле **«issuerUniqueIdentifier»** представляет собой битовую строку, используемую для уникальной идентификации издателя (в соответствии с IETF/RFC 3280 настоящий стандарт не рекомендует использовать это поле).

8) Необязательное поле **«subjectUniqueIdentifier»** представляет собой битовую строку, используемую для уникальной идентификации субъекта (в соответствии с IETF/RFC 3280 настоящий стандарт не рекомендует использовать это поле).

9) Поле **«extensions»** должно содержать последовательность из одного или нескольких расширений сертификата.

Подпись сертификата добавляется к типу данных сертификата с помощью стандартного типа данных **«SignedData»**.

### 6.3 Спецификации общих полей

#### 6.3.1 Общие сведения

Ниже приведены специфические требования к информации, содержащейся в базовых полях сертификата, которые еще не были включены в IETF/RFC 3280 или IETF/RFC 3279 [7].

#### 6.3.2 Поле «signature»

Рекомендуется присваивать полю **«signature»** одно из следующих значений:

1. md5WithRSAEncryption (1.2.840.113549.1.1.4)
2. sha1WithRSAEncryption (1.2.840.113549.1.1.5)
3. dsa-with-sha1 (1.2.840.10040.4.3)
4. md2WithRSAEncryption (1.2.840.113549.1.1.2)

5. ecdsa-with-SHA1 (1.2.840.10045.4.1)
6. ecdsa-with-SHA224 (1.2.840.10045.4.3.1)
7. ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
8. ecdsa-with-SHA384 (1.2.840.10045.4.3.3)
9. ecdsa-with-SHA512 (1.2.840.10045.4.3.4)
10. id-RSASSA-PSS (1.2.840.113549.1.1.10)
11. sha256WthRSAEncryption 1.2.840.113549.1.1.11
12. sha384WithRSAEncryption 1.2.840.113549.1.1.12
13. sha512WithRSAEncryption 1.2.840.113549.1.1.13

**6.3.3 Поле «validity»**

Значения дат срока действия, передаваемые в поле **«validity»**, должны соответствовать IETF/RFC 3280. В настоящем стандарте приняты ограничения сроков действия сертификатов, выдаваемых в системе здравоохранения, представленные в ИСО 17090-3, подпункт 7.6.3.2.

Момент времени **«notBefore»**, указанный в сертификате, отражает точный момент, начиная с которого ЦС будет управлять актуальной информацией о статусе сертификата и публиковать ее.

**6.3.4 Поле «subjectPublicKeyInfo»**

В этом поле должен быть задан идентификатор алгоритма, например:

1. Алгоритм *RSA*

pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) 1 }
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}

2. Алгоритм *Diffie-Hellman*

Объектный идентификатор алгоритма *Diffie-Hellman*, поддерживаемый в настоящем профиле, определен в ANSI X9.42:2003 [8].

dhpublicnumber OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-x942(10046) number-type(2) 1 }

3. Алгоритм *DSA*

Объектный идентификатор алгоритма *DSA*, поддерживаемый в настоящем профиле, имеет значение

id-dsa ID ::= { iso(1) member-body(2) us(840) x9-57(10040)
x9cm(4) 1 }

4. Эллиптические кривые

Ecdsa {[1, 2, 840, 10045, 2, 1]}

Требования к размерам ключа см. в ИСО 17090-3:2008, подпункт 7.6.1.5.

**6.3.5 Поле наименования издателя «issuer»**

Наименование издателя, хранящееся в поле **«issuer»**, должно иметь формат, совместимый с соответствующей ISO [6] структурой имени, состав которой соответствует определению класса объектов роли в организации **«organizationalRole»**, находящегося под классом объектов организации **«organization»** или подразделения **«organizationUnit»**, с приведенными ниже дополнениями и ограничениями.

Содержание поля наименования издателя **«issuer»** для каждого типа сертификата описано в 6.4.

1. Поле наименования страны **«countryName»** должно содержать двухбуквенный код ISO страны.

***Пример — countryName = "US".***

Это поле обязательное, поскольку в сфере здравоохранения важно знать страну происхождения сертификата, предъявленного для запроса доступа к персональной медицинской информации. В разных странах существуют свои законы по защите персональных данных и своя практика их применения, поэтому знание страны происхождения запроса на доступ поможет принять решение, удовлетворить его или нет.

2. Поле наименования местонахождения **«localityName»** может использоваться для хранения по меньшей мере одного наименования местонахождения. Спецификация его формата требует использовать два уровня наименования местонахождения. Верхний уровень указывает страну, после которой указано географическое наименование местонахождения. В поле наименования издателя сертификата поле **«localityName»** страны можно опустить и ограничиться только полем **«localityName»** географического местонахождения.

***Пример — localityName = "California".***

3. Поле наименования организации **«organizationName»** используется для хранения наименования субсидирующей организации здравоохранения в сертификате конечного объекта и наименования ЦС в сертификате ЦС. Это поле должно содержать полное зарегистрированное наименование организации.

***Пример — organizationName = "California Hospital Authority".***

4. Поле наименования подразделения **«organizationalUnitName»**. Если это поле присутствует, то оно используется для хранения наименования подразделения данной организации. Можно формировать несколько уровней подчиненности подразделений, задавая более одного значения этого поля. Если это поле указано, то его значение должно выбираться таким образом, чтобы исключить неоднозначность в домене данного ЦС.

***Пример — organizationalUnitName = "Midtown Hospital Radiology".***

5. Поле общего наименования **«commonName»**. Назначение этого поля — описать общеупотребительное наименование издателя. Это поле в сочетании с общим наименованием субъекта **«commonName»** нередко используется стандартными компонентами программного обеспечения при выдаче сертификата пользователю. Поэтому наименование должно быть информативным, чтобы дать полное представление о назначении сертификата и его издателе. Кроме того, рекомендуется включать в значение поля **«commonName»** наименование управляющей ПС. Оно служит дополнением к идентификации политики с помощью объектного идентификатора.

***Пример — commonName = "Patient Health Information Policy".***

### 6.3.6 Поле наименования субъекта «subject»

Наименование субъекта, хранящееся в поле **«subject»**, должно иметь формат, совместимый с соответствующей ISO [6] структурой имени, состав которой соответствует определению класса объектов роли в организации **«organizationalRole»**, находящегося под классом объектов организации **«organization»** или подразделения **«organizationUnit»**, с приведенными ниже дополнениями и ограничениями.

Квалификация и должности участников системы здравоохранения отражаются в поле **«hcRole»** расширения сертификата.

Содержание поля наименования субъекта **«subject»** для каждого типа сертификата описано в 6.4. Дополнительные советы и указания можно найти в ISO/TS 21091 [9].

1. Поле наименования страны **«countryName»** должно содержать двухбуквенный код ISO страны.

***Пример — countryName = "US".***

Практика заполнения этого поля зависит от конкретной страны.

Это поле, обязательное для ЦС, квалифицированных и вспомогательных медицинских работников, субсидируемых поставщиков медицинских услуг, организаций и работников поддерживающих организаций, поскольку в сфере здравоохранения важно знать страну происхождения субъекта, предъявляющего сертификат для запроса доступа к персональной медицинской информации. В разных странах существуют свои законы по защите персональных данных и своя практика их применения, поэтому знание страны происхождения запроса на доступ поможет принять решение, удовлетворить его или нет.

2. Поле наименования местонахождения **«localityName»** может использоваться для хранения по меньшей мере одного наименования местонахождения. Спецификация его формата требует использовать два уровня наименования местонахождения. Верхний уровень указывает страну, после которой указано географическое наименование местонахождения. В поле наименования субъекта сертификата поле **«localityName»** страны можно опустить и ограничиться только полем **«localityName»** географического местонахождения.

***Пример — localityName = "California".***

3. Поле наименования организации **«organizationName»** используется для хранения наименования субсидирующей организации здравоохранения в сертификате конечного объекта и наименования центра сертификации в сертификате ЦС. Это поле должно содержать полное зарегистрированное наименование организации.

***Пример – organizationName = "Midtown General Hospital".***

4. Поле наименования подразделения **«organizationalUnitName»**. Если это поле присутствует, то оно используется для хранения наименования подразделения данной организации. Можно формировать несколько уровней подчиненности подразделений, задавая более одного значения этого поля. Если это поле указано, то его значение должно выбираться таким образом, чтобы исключить неоднозначность в домене данного ЦС.

В некоторых местных системах здравоохранения, например в Японии, поле наименования подразделения используется для хранения роли участника здравоохранения. Это поле может быть полезным при реализации частных виртуальных сетей (VPN), поскольку маршрутизаторы или межсетевые экраны некоторых провайдеров VPN могут распознавать элемент наименования подразделения OU и использовать его при применении правил разрешения доступа или отказа в доступе. С его помощью доверяющая сторона легко может считать информацию о роли непосредственно из сертификата. Таким образом, если поле **«organizationalUnitName»** указано, то оно может использоваться для хранения роли участника системы здравоохранения.

***Примеры***

***1. organizationalUnitName = "Midtown Hospital Radiology".***

***2. organizationalUnitName = "Licensed Physician".***

5. Поле общего наименования **«commonName»**. Назначение этого поля — описать общеупотребительное наименование субъекта. Оно должно присутствовать и содержать точное наименование субъекта, известное системе здравоохранения.

***Пример — commonName = "Bruce Wayne".***

Это поле должно быть обязательным для лиц и организаций, являющихся субъектами сертификатов. Если надо принять решение о доступе к персональной медицинской информации или об отказе в доступе, то возможность идентифицировать название лица, известное системе здравоохранения, может иметь существенное значение.

6. Поле фамилии «surname». Это поле используется для указания фамилии субъекта сертификата. Если оно присутствует, то должно содержать точную фамилию субъекта, известную системе здравоохранения.

***Пример — surName = "Wayne".***

7. Поле имени **«givenName»**. Это поле используется для указания имени и отчества субъекта сертификата. Если оно присутствует, то должно содержать точные имя и отчество субъекта, известные системе здравоохранения.

***Пример — givenName = "Bruce".***

8. Поле адреса электронной почты **«e-mail»**. Основное рекомендованное назначение этого поля — хранение адреса электронной почты субъекта.

***Пример — e-mail = "***gost.e-ecolog.ru***".***

Разрешается параллельное включение атрибута **«EmailAddress»** в наименование субъекта для поддержки нестандартизованных реализаций, но в IETF/RFC 3280 объявлено устаревшим.

Настоящий стандарт рекомендует использовать элемент e-mail в поле альтернативного наименования субъекта **«subjectAltName»**, а не в поле наименования субъекта.

9. Поле серийного номера **«serialNumber»** может использоваться в целях обеспечения уникальности наименования субъекта **«subjectDN»**. Например, его можно использовать для хранения номера сертификата медицинского специалиста. Это поле является необязательным.

### 6.4 Требования для каждого типа сертификатов в здравоохранении

#### 6.4.1 Элементы поля издателя «issuer»

Требования к элементам поля издателя **«issuer»** для каждого типа сертификатов в здравоохранении приведены в таблице 1.

#### 6.4.2 Элементы поля субъекта «subject»

Требования к элементам поля субъекта **«subject»** для каждого типа сертификатов в здравоохранении приведены в таблице 2.

Таблица 1 — Требования к элементам поля издателя («**issuer**») для каждого типа сертификатов в здравоохранении

| Элементы сертификата | Сертификаты ЦС | | Сертификаты идентичности | | | | | | Сертификат атрибута |
|---|---|---|---|---|---|---|---|---|---|
| | Сертификат центра сертификации[1)] | Кросс-сертификат | Сертификат квалифицированного медицинского работника | Сертификат вспомогательного медицинского работника[2)] | Сертификат потребителя | Сертификат организации | Сертификат устройства | Сертификат приложения | |
| Элементы поля издателя «**issuer**»[3)] | | | | | | | | | |
| **CountryName** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **LocalityName** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **Organization_Name** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **Organizational_Unit Name** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **CommonName** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Не применимо |

[1)] Под центрами сертификации понимаются все, кто выпускает сертификаты конечным объектам.

[2)] Требования, предъявляемые к сертификатам вспомогательных медицинских работников, относятся также к сертификатам субсидируемых поставщиков медицинских услуг и работников поддерживающих организаций здравоохранения.

[3)] В настоящей таблице указаны те элементы поля издателя «**issuer**», требования к которым могут отличаться для разных типов сертификатов.

Таблица 2 — Требования к элементам поля субъекта («subject») для каждого типа сертификатов в здравоохранении

| Элементы сертификата | Сертификаты ЦС | | Сертификаты идентичности | | | | | | Сертификат атрибута |
|---|---|---|---|---|---|---|---|---|---|
| | Сертификат центра сертификации[1)] | Кросс-сертификат | Сертификат квалифицированного медицинского работника | Сертификат вспомогательного медицинского работника[2)] | Сертификат потребителя | Сертификат организации | Сертификат устройства | Сертификат приложения | |
| Элементы поля субъекта «subject»[3)] | | | | | | | | | |
| **CountryName** | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное | Обязательное | Необязательное | Необязательное | Необязательное |
| **LocalityName** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **Organization_Name** | Обязательное | Обязательное | Необязательное | Необязательное | Необязательное | Обязательное | Необязательное | Необязательное | Необязательное |
| **Organizational_Unit Name** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **CommonName** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное | Необязательное | Необязательное |
| **GivenName** | Не применимо | Не применимо | Необязательное | Необязательное | Необязательное | Не применимо | Не применимо | Не применимо | Необязательное |
| **SurName** | Не применимо | Не применимо | Необязательное | Необязательное | Необязательное | Не применимо | Не применимо | Не применимо | Необязательное |
| **Electronic mail** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |

[1)] Под центрами сертификации понимаются все, кто выпускает сертификаты конечным объектам.

[2)] Требования, предъявляемые к сертификатам вспомогательных медицинских работников, относятся также к сертификатам субсидируемых поставщиков медицинских услуг и работников поддерживающих организаций здравоохранения.

[3)] В настоящей таблице указаны те элементы поля субъекта **«subject»**, требования к которым могут отличаться для разных типов сертификатов.

## 7 Использование расширений сертификата

### 7.1 Общие сведения

Ниже приведены требования к использованию элементов полей расширения (**«extensions»**) сертификатов формата X.509 версии 3 [5], предъявляемые при решении задач здравоохранения. Более детальная информация об этих полях приведена в IETF/RFC 3280 и IETF/RFC 3739.

### 7.2 Общие расширения

#### 7.2.1 Поле идентификатора ключа ЦС «authorityKeyIdentifier»

Это расширение должно идентифицировать открытый ключ, используемый для проверки подписи сертификата. С его помощью можно отличать разные ключи, используемые одним ЦС (например, при обновлении ключа).

Должен использоваться только элемент **«keyIdentifier»** поля расширения **«authorityKeyIdentifier»**.

Это расширение является некритическим. Если оно используется, рекомендуется объявлять его обязательным.

#### 7.2.2 Поле идентификатора ключа субъекта «subjectKeyIdentifier»

Это расширение используется для идентификации открытого ключа, содержащегося в поле сертификата **«subjectPublicKeyInfo»**.

В IETF/RFC 3280 приведены указания, каким образом элемент идентификатора может быть извлечен из открытого ключа. Разрешен любой алгоритм извлечения при условии, что идентификатор будет обладать свойством уникального представления ключа.

Это расширение является обязательным и некритическим для всех сертификатов конечных объектов и всех сертификатов ЦС в цепочке доверия, построенной для системы здравоохранения.

#### 7.2.3 Поле основного назначения ключа «keyUsage»

Это расширение должно идентифицировать основное назначение, ассоциированное с открытым ключом сертификата. Использование единственной пары ключей и для шифрования, и для цифровой подписи воспрещается. Использование ключа для шифрования не должно сочетаться ни с неоспоримостью, ни с цифровой подписью (см. 6.1).

Это расширение должно быть обязательным. Рекомендуется специфицировать его как критическое (как это указано в IETF/RFC 3280).

#### 7.2.4 Поле срока использования секретного ключа «privateKeyUsagePeriod»

Использование этого расширения не рекомендуется.

По умолчанию в отсутствие этого расширения период действия секретного ключа совпадает со сроком действия сертификата.

#### 7.2.5 Поле политик сертификата «certificatePolicies»

Расширение **«certificatePolicies»** должно содержать объектный идентификатор стандартизованной политики сертификатов ЦС в соответствии с ИСО 17090-3.

Это расширение является обязательным и может быть критическим или некритическим в зависимости от ПС.

#### 7.2.6 Поле альтернативного наименования субъекта «subjectAltName»

Рекомендуется, чтобы это расширение присутствовало в сертификате и содержало адрес электронной почты получателя сертификата, соответствующий спецификации ETF/RFC 822 [4]. Если в него включен элемент наименования каталога **«directoryName»**, то в целях обеспечения поддержки международного набора символов для отличительного наименования субъекта он должен иметь тип данных UTF8String.

Это расширение является необязательным и некритическим.

#### 7.2.7 Поле базовых ограничений «basicConstraints»

Расширение **«basicConstraints»** содержит булевское значение, применяемое для указания, может ли субъект действовать как ЦС, используя сертифицированный ключ для подписи сертификатов. Если это значение равно TRUE, то может быть также указано ограничение длины пути сертификации.

Сертификаты ЦС должны включать в себя расширение **«basicConstraints»** со значением TRUE.

Чтобы удостовериться, является ли данное расширение критическим либо некритическим и обязательным либо необязательным, см. таблицу 3.

Сертификаты конечных объектов (выдаваемых квалифицированному медицинскому работнику, вспомогательному медицинскому работнику, субсидируемому поставщику медицинских услуг, работнику поддерживающей организации здравоохранения, потребителю, организации, приложению или устройству) не должны иметь расширение со значением TRUE.

**7.2.8 Поле точек распространения списков отозванных сертификатов «CRLDistributionPoints»**

IETF/RFC 3280 рекомендует поддержку этого расширения для ЦС и приложений. Для реализаций стандарта в здравоохранении, использующих точки распространения списков отозванных сертификатов, это расширение должно идентифицировать местонахождение соответствующего СОС (или списка отозванных центров сертификации для сертификатов ЦС) в каталоге цифровых сертификатов. В этом случае оно должно быть обязательным и некритическим.

**7.2.9 Поле расширенного назначения ключа «extKeyUsage»**

Это поле указывает одно или несколько назначений сертифицированного открытого ключа, для которых он может использоваться в дополнение к основному назначению, описанному в поле основного назначения ключа **«keyUsage»**, содержащемся в расширении, или вместо этого назначения.

Это расширение является необязательным и некритическим.

**7.2.10 Поле информации о доступе к сертификатам центров сертификации «authorityInfoAccess»**

Расширение **«authorityInfoAccess»** указывает, как получить доступ к сертификатам ЦС и серверам услуг определения статуса сертификата в реальном времени (OCSP Responders).

Это расширение не задает местонахождение СОС. Его значение состоит из последовательности описаний методов доступа и адресов объектов доступа.

Каждый элемент этой последовательности описывает формат и местонахождение дополнительной информации о ЦС. Тип и формат информации указываются в методе доступа, а местонахождение информации — в адресе доступа.

Это расширение является необязательным и некритическим.

**7.2.11 Поле доступа к информации о субъекте «subjectInfoAccess»**

Это поле указывает, как получить доступ к сертификатам ЦС субъекта и таким службам, как метки времени.

Это расширение является необязательным и некритическим.

**7.3 Специальные атрибуты каталога субъектов**

**7.3.1 Атрибут профессиональной роли «hcRole»**

Атрибут **«hcRole»** позволяет кодировать сведения о роли квалифицированного или вспомогательного медицинского работника. Этот атрибут рекомендуется использовать при реализациях стандарта, поскольку его применение будет способствовать международной интероперабельности сертификации ролей в здравоохранении. С этим атрибутом можно выпустить несколько сертификатов для одного и того же лица. С полем **«hcRole»** можно ассоциировать целый ряд таблиц классификации. Предлагаемое поле имеет механизм расширения, позволяющий использовать национальные или региональные системы кодирования ролей в здравоохранении.

Это поле требуется для сертификатов идентичности, поскольку роль владельца сертификата в здравоохранении составляет неотъемлемую часть его/ее идентичности.

Когда этот атрибут проверен, дополнительную информацию удобнее помещать в СА, как это обсуждается в ИСО 17090-1, подраздел 7.4.

Настоящий стандарт позволяет предъявлять в сертификате такие региональные сведения, как регистрационные номера, номера счетов и идентификаторы пациентов. Ниже представлена спецификация класса объектов REGIONAL-DATA.

```
hcRole ATTRIBUTE     ::= {
WITH SYNTAX                        HCActorData
EQUALITY MATCHING RULE             hcActorMatch
SUBSTRINGS MATCHING RULE           hcActorSubstringsMatch
ID                                 id-hcpki-at-healthcareactor}
```

**Назначение объектных идентификаторов**

В настоящем стандарте назначены следующие объектные идентификаторы:

```
{iso (1) standard (0) hcpki (17090)}
  id-hcpki OBJECT IDENTIFIER    ::= 1.0.17090
```

```
id-hcpki-at OBJECT IDENTIFIER   ::= {id-hcpki 0 }
   id-hcpki-at OBJECT IDENTIFIER          ::= 1.0.17090.0
id-hcpki-at-healthcareactor OBJECT IDENTIFIER ::= {id-hcpki-at 1}
   id-hcpki-at-healthcareactor OBJECT IDENTIFIER ::= 1.0.17090.0.1
id-hcpki-cd OBJECT IDENTIFIER   ::= {id-hcpki 1}
   id-hcpki-cd OBJECT IDENTIFIER          ::= 1.0.17090.1
id-hcpki-is OBJECT IDENTIFIER   ::= {id-hcpki 2}
   id-hcpki-is OBJECT IDENTIFIER::= 1.0.17090.2
```

**Определения типов данных:**

```
HCActorData       ::= SET OF HCActor
HCActor           ::= SEQUENCE {
codedData                 [0] CodedData OPTIONAL,
RegionalHCActorData       [1] SEQUENCE OF RegionalData OPTIONAL }
CodedData ::= SET {
   codingSchemeReference     [0] OBJECT IDENTIFIER,
   - - - - Содержит ссылку на систему кодирования ISO или ссылку
   - - - - на местную систему кодирования, зарегистрированную в ISO
   - - - - либо у национального регистратора объектных идентификаторов.
   - - - - Объектный идентификатор системы кодирования ISO
   - - - - определен выше (id-hcpki-is).
   - - - - По меньшей мере один из следующих элементов
   - - - - должен присутствовать:
   codeDataValue             [1] UTF8String OPTIONAL,
   codeDataFreeText          [2] DirectoryString OPTIONAL }
RegionalData      ::= SEQUENCE {
   type REGIONALDATA.&id({SupportedRegionalData}),
   value REGIONALDATA.&Type({SupportedRegionalData}{@type})}
```

**Определение класса объектов «REGIONALDATA»:**

```
REGIONALDATA  ::= CLASS {
    &Type,
        &id OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
    WITH SYNTAX &Type
        ID &id }
```

**Определение множества классов объектов «SupportedRegionalData»:**

```
SupportedRegionalData REGIONALDATA ::=
    {coded,
        ... - - здесь могут быть определены дополнительные
            - - региональные/национальные объекты}
```

**Определение информационного объекта кодированных данных «coded»:**

```
coded     ::= REGIONAL-DATA {
    WITH SYNTAX CodedRegionalData
        ID id-hcpki-cd}
CodedRegionalData  ::= SEQUENCE {
    country                   [0] PrintableString (SIZE (2)),
        - - Код страны издателя сертификата в соответствии с ISO 3166-1 [10].
    issuingAuthority          [1] DirectoryString,
        - - Идентификатор издателя сертификата как регионального объекта.
        - - Может быть указан как настоящий идентификатор или
        - - как строка поиска в каталоге (требует дополнительного
        - - определения).
    hcMajorClassCode [2] CodedData,
    hcMinorClassCode [3] CodedData OPTIONAL
```

Для этого поля должны использоваться коды, например, взятые из системы кодирования имен ролей пользователей данных ASTM E1986-98 [11].

Значения элементов класса объектов **«HcActor»** рекомендуется брать из соответствующей национальной системы кодирования.

В сертификатах квалифицированных и вспомогательных медицинских работников это расширение является обязательным и некритическим. В остальных случаях оно необязательное и некритическое.

### 7.3.2 Поле атрибутов каталога субъектов «subjectDirectoryAttributes»

Рекомендуется, чтобы это расширение присутствовало в индивидуальных сертификатах идентичности. В этих сертификатах оно может содержать атрибут **«hcRole»** (см. 7.3.1). Кроме того, поле **«subjectDirectoryAttributes»** может содержать другие атрибуты, не специфицированные в настоящем стандарте.

Это расширение должно быть помечено как некритическое. Поскольку сертификат может использоваться как в целях аутентификации, так и в целях присвоения роли, то в сертификатах квалифицированных и вспомогательных медицинских работников он должен быть обязательным. В сертификатах других типов он должен быть необязательным.

## 7.4 Расширение объявлений квалифицированного сертификата «qcStatements»

Рекомендуется включать поле **«qcStatements»** в сертификаты квалифицированных и вспомогательных медицинских работников. Сертификаты пациентов/потребителей, субсидируемых поставщиков медицинских услуг и работников поддерживающих организаций также могут содержать это поле. Сертификаты устройств и приложений не должны его содержать. Детальные сведения об этом поле приведены в IETF/RFC 3739.

Рекомендуется, чтобы приложения, соответствующие настоящему стандарту, были способны поддерживать использование расширения **«qcStatements»**.

Это расширение является необязательным и некритическим.

## 7.5 Требования для каждого типа сертификатов в здравоохранении

Требования к элементам поля расширения **«extensions»** для каждого типа сертификатов в здравоохранении приведены в таблице 3.

Таблица 3 — Требования к элементам поля расширения **«extensions»** для каждого типа сертификатов в здравоохранении

| Элементы сертификата | Сертификаты ЦС | | Сертификаты идентичности | | | | | | Сертификат атрибута |
|---|---|---|---|---|---|---|---|---|---|
| | Сертификат центра сертификации | Кросс-сертификат | Сертификат квалифицированного медицинского работника | Сертификат вспомогательного медицинского работника[1)] | Сертификат потребителя | Сертификат организации | Сертификат устройства | Сертификат приложения | |
| Общие расширения | | | | | | | | | |
| **authorityKeyIdentifier**[2)] | Обязательное[2)] | Обязательное[2)] | Обязательное[2)] | Обязательное[2)] | Обязательное[2)] | Обязательное[2)] | Обязательное | Обязательное[2)] | Необязательное |
| **subjectKeyIdentifier** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **keyUsage** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **privateKeyUsagePeriod** | Отсутствует | Отсутствует | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **certificatePolicies** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **subjectAltName** | Отсутствует | Отсутствует | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **subjectDirectoryAttributes**[3)] | Отсутствует | Отсутствует | Обязательное[3)] | Обязательное[3)] | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **basicConstraints** | Обязательное и критическое | Обязательное и критическое | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **CRLDistributionPoints** | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Обязательное | Необязательное |
| **extKeyUsage** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Отсутствует | Необязательное |

*Окончание таблицы 3*

| Элементы сертификата | Сертификаты ЦС | | Сертификаты идентичности | | | | | | Сертификат атрибута |
|---|---|---|---|---|---|---|---|---|---|
| | Сертификат центра сертификации | Кросс-сертификат | Сертификат квалифицированного медицинского работника | Сертификат вспомогательного медицинского работника[1)] | Сертификат потребителя | Сертификат организации | Сертификат устройства | Сертификат приложения | |
| Другие расширения | | | | | | | | | |
| **authorityInfoAccess** | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное | Необязательное |
| **qcStatements** | Отсутствует | Отсутствует | Обязательное[4)] | Обязательное[4)] | Обязательное[4)] | Отсутствует | Отсутствует | Отсутствует | Необязательное |
| **hcRole**[3)] | Отсутствует | Отсутствует | Обязательное[3)] | Обязательное[3)] | Необязательное | Необязательное | Необязательное | Отсутствует | Отсутствует |

[1)] Требования, предъявляемые к сертификатам вспомогательных медицинских работников, относятся также к сертификатам субсидируемых поставщиков медицинских услуг и работников поддерживающих организаций здравоохранения.

[2)] Рекомендуется, чтобы это поле было обязательным.

[3)] Использование поля **«hcRole»** в сертификатах квалифицированного медицинского работника и вспомогательного медицинского работника требует, чтобы поле **«subjectDirectoryAttributes»** в этих сертификатах было обязательным.

[4)] Требование обязательности распространяется на области действия, где по национальному законодательству требуется использование квалифицированных сертификатов.

**Приложение А**
**(справочное)**

## Примеры профилей сертификатов

### А.1 Введение

Ниже в целях иллюстрации приведено несколько простых примеров каждого типа сертификатов. Эти примеры не являются нормативными. Код на языке ASN.1 и нормативные положения содержатся в основном тексте настоящего стандарта.

### А.2 Профиль сертификата потребителя

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов Национальной службы здравоохранения Великобритании (NHS).

Пациент Bill Smith, его номер NHS 368964278. Дата выпуска сертификата — 1 августа 2001 года. Дата завершения действия сертификата — 1 августа 2006 года.

| | |
|---|---|
| **version** | (2 — десятичный код сертификатов версии 3) |
| **serialNumber** | (уникальный номер, генерируемый ЦС) |
| **signature** | (sha-1WithRSAEncryption {1,2,840,113549,1,1,5}) |
| **issuer** | |
| **countryName** | (UK) |
| **localityName** | (London) |
| **organizationName** | (Dept. of Health) |
| **organizationalUnit** | (National Health Service) |
| **commonName** | (Сертификат пациента версии 1) |
| **serialNumber** | ({серийный номер издателя}) |
| **validity** | (срок действия в формате UTCTime:<br>notBefore 010801000000z<br>notAfter 060801000000z) |
| **subject** | |
| **countryName** | (UK) |
| **localityName** | (London) |
| **organizationName** | (NHS) |
| **organizationalUnit** | (Регистратура) |
| **commonName** | (Smith Bill) |
| **surName** | (Smith) |
| **givenName** | (William) |
| **e-mail** | (gost.e-ecolog.ru |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись) |
| **certificatePolicies** | |
| **policyIdentifier** OBJECT IDENTIFIER ::= Policy-OID-for-Patient-Certificate-v1 | |
| **cRLDistributionPoints** | gost.e-ecolog.ru ) |
| **authorityInformationAccess** | (http:ocspserver.nhs.uk/OCSP_SERVER:5555) |
| **subjectDirectoryAttributes** | |
| **hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor | |
| **hcActorData** SET OF { | |
| **codedData** CodedData ::= { | |
| **codingSchemeReference** OBJECT IDENTIFIER ::= id-hcpki, | |
| **codeDataValue** UTF8String ::= the-code-for-patient, | |
| **codeDataFreeText** DirectoryString ::= optional-data } | |

**regionalHCData Sequence of RegionalData** ::= {
**type** OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
**country** PrintableString (SIZE (2) ::= ISO-country-code-for-UK,
**issuingAuthority** DirectoryString ::= (c=UK, National Health Service,
ou=patients),
**hcMajorClassCode CodedData** ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::=
Coding-Scheme-for-Type-OID,
**codeDataValue** UTF8String ::= Type-OID-for-patient,
**codeDataFreeText** UTF8String ::= "patient ID 368964278"} } }

### A.3 Профиль сертификата вспомогательного медицинского работника

Пример — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

Betty Smith — сотрудница "сертифицированного медицинского регистратора (CMP)". Сертификаты CMP выпускаются Американской ассоциацией медицинских регистраторов.

**version** (2 — десятичный код сертификатов версии 3)
**serialNumber** (уникальный номер, генерируемый ЦС)
**signature** (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
**issuer**
**countryName** (US)
**localityName** (California)
**organizationName** (наименование ЦС службы здравоохранения Калифорнии)
**commonName** (наименование ЦС службы здравоохранения Калифорнии)
**validity** (срок действия в формате UTCTime)
**subject**
**countryName** (US)
**localityName** (California)
**organizationName** (организация владельца сертификата)
**commonName** (Smith Betty)
**surname** (Smith)
**givenName** (Betty)
**subjectPublicKeyInfo**
**algorithm** (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1})
**subjectPublicKey** (открытый ключ субъекта)
**extensions**
**authorityKeyIdentifier** (уникальный идентификатор открытого ключа ЦС)
**subjectKeyIdentifier** (уникальный идентификатор открытого ключа субъекта)
**keyUsage** (цифровая подпись, или неоспоримость, или шифрование)
**certificatePolicies** (объектный идентификатор соответствующей политики)
**cRLDistributionPoints** (место входа в СОС X.500)
**subjectDirectoryAttributes**
**(hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor
**hcActorData** SET OF {
**codedData** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::= id-hcpki,
**codeDataValue** UTF8String ::= the-code-for-transcriptionist-role,
**codeDataFreeText** DirectoryString ::= optional-data}
**regionalHCData** Sequence of RegionalData ::= {
**type** OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
**country** PrintableString (SIZE (2) ::= ISO-country-code-for-USA,
**issuingAuthority** DirectoryString ::= (C=US,
OU= American Association of Medical Transcriptionists),
**nameAsIssued** DirectoryString ::= (CN= Elizabeth Smith),
**hcMajorClassCode** CodedData ::= {
codingSchemeReference OBJECT IDENTIFIER ::= ASTM-Coding-Scheme-for-Type,
**codeDataValue** UTF8String ::= ASTM-Type-OID-for-transcriptionist}
**codeDataFreeText** UTF8String ::= "лицензия № 1234567") } )

### А.4 Профиль сертификата квалифицированного медицинского работника

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

Медицинский специалист John Stuart Woolley, он же Tink Woolley. Ему выдана лицензия Медицинской лицензионной комиссией штата Калифорния. Номер лицензии 20А4073. Код статуса лицензии 17 ("01" — "действительная и активная". Дата выдачи — 22 марта 2000 года. Дата завершения действия лицензии — 21 марта 2002 года.

**version** (2 — десятичный код сертификатов версии 3)
**serialNumber** (уникальный номер, генерируемый ЦС)
**signature** (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
**issuer**
- **countryName** (US)
- **localityName** (California)
- **organizationName** (наименование ЦС службы здравоохранения Калифорнии)
- **commonName** (наименование ЦС службы здравоохранения Калифорнии)

**validity** (срок действия в формате UTCTime)
**subject**
- **countryName** (US = Соединенные Штаты Америки)
- **localityName** (California)
- **organizationName** (организация владельца сертификата)
- **commonName** (Woolley Tink)
- **surname** (Woolley)
- **givenName** (John Stuart)

**subjectPublicKeyInfo**
- **algorithm** (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1})
- **subjectPublicKey** (открытый ключ субъекта)

**extensions**
**authorityKeyIdentifier** (уникальный идентификатор открытого ключа ЦС)
**subjectKeyIdentifier** (уникальный идентификатор открытого ключа субъекта)
**keyUsage** (цифровая подпись, или неоспоримость, или шифрование)
**certificatePolicies** (объектный идентификатор соответствующей политики)
**cRLDistributionPoints** (место входа в СОС X.500)
**subjectDirectoryAttributes**

(**hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor
**hcActorData** SET OF {
**codedData** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::= id-hcpki,
**codeDataValue** UTF8String ::= the-code-for-physician-role,
**codeDataFreeText** DirectoryString ::= optional-data}
**regionalHCData** Sequence of RegionalData ::= {
**type** OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
**country** PrintableString (SIZE (2) ::= ISO-country-code-for-USA,
**issuingAuthority** DirectoryString ::= (C=US, L=CA, OU=California Medical License Board),
**nameAsIssued** DirectoryString ::= (CN= John Stuart Woolley)
**hcMajorClassCode** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::=
ASTM-Coding-Scheme-for-Type-OID,
**codeDataValue UTF8String** ::= ASTM-Type-OID-for-physician}
**codeDataFreeText** UTF8String ::= "лицензия № 20А4073"}
**hcMinorClassCode** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::=
ASTM-Coding-Scheme-for-License-Status-OID,
**codeDataValue** UTF8String ::= "unrestricted",
**codeDataFreeText** UTF8String ::= "неограниченная"} } )

Обратите внимание, что в данном примере номер и статус лицензии закодированы как региональные данные. Такие региональные данные являются необязательными, и решение, включать их в сертификат или нет, остается на усмотрение ЦС, выпускающего сертификат.

### А.5 Профиль субсидируемого поставщика медицинских услуг

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения провинции Онтарио (Канада).

Julie LeClerk, акушерка из провинции Онтарио.

**version** (2 — десятичный код сертификатов версии 3)
**serialNumber** (уникальный номер, генерируемый ЦС)
**signature** (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
**issuer**
- **countryName** (CA=Канада)
- **localityName** (Ontario)
- **organizationName** (наименование ЦС службы здравоохранения Онтарио)
- **commonName** (наименование ЦС службы здравоохранения Онтарио)

**validity** (срок действия в формате UTCTime)
**subject**
- **countryName** (CA=Канада)
- **localityName** (Ontario)
- **organizationName** (организация владельца сертификата)
- **commonName** (LeClerk Julie)
- **surname** (LeClerk)
- **givenName** (Julie)

**subjectPublicKeyInfo**
- **algorithm** (открытый ключ RSA, 1024 бита {1,2,840,113549,1,1,1})
- **subjectPublicKey** (открытый ключ субъекта)

**extensions**
**authorityKeyIdentifier** (уникальный идентификатор открытого ключа ЦС)
**subjectKeyIdentifier** (уникальный идентификатор открытого ключа субъекта)
**keyUsage** (цифровая подпись, или неоспоримость, или шифрование)
**certificatePolicies** (объектный идентификатор соответствующей политики)
**cRLDistributionPoints** (место входа в COC X.500)
**subjectDirectoryAttributes**

(**hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor
**hcActorData** SET OF {
**codedData** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::= id-hcpki,
**codeDataValue** UTF8String ::= the-code-for-midwife-role,
**codeDataFreeText** DirectoryString ::= optional-data}
**regionalHCData** Sequence of RegionalData ::= {
**type** OBJECT IDENTIFIER ..= OID-for-this-regional-encoding,
**country** PrintableString (SIZE (2) ::= ISO-country-code-for-Canada,
**issuingAuthority** DirectoryString ::= (C=US, L=CA, OU= Name-of-CA-for-Ontario-Health-Care),
**hcMajorClassCode** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::= ISO-Role-Coding-Scheme,
**codeDataValue UTF8String** ::= the-code-for-midwife-role }
**codeDataFreeText** UTF8String ::= "необязательные печатаемые данные"} } )

### А.6 Профиль сертификата работника поддерживающей организации

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

Sally R. Jones, оператор бухгалтерии в организации American Health Systems.

**version** (2 — десятичный код сертификатов версии 3)
**serialNumber** (уникальный номер, генерируемый ЦС)
**signature** (sha-1WithRSAEncryption {1,2,840,113549,1,1,5})
**issuer**
- **countryName** (US)
- **localityName** (California)
- **organizationName** (наименование ЦС службы здравоохранения Калифорнии)

| | |
|---|---|
| **commonName** | (наименование ЦС службы здравоохранения Калифорнии) |
| **validity** | (срок действия в формате UTCTime) |
| **subject** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (California) |
| **organizationName** | (American Health Systems) |
| **commonName** | (Jones Sally R.) |
| **surname** | (Jones) |
| **givenName** | (Sally R.) |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бита {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись, или неоспоримость, или шифрование) |
| **certificatePolicies** | (объектный идентификатор соответствующей политики) |
| **cRLDistributionPoints** | (место входа в СОС X.500) |
| **subjectDirectoryAttributes** | |

**(hcRole** OBJECT IDENTIFIER ::= id-hcpki-at-healthcareactor
**hcActorData** SET OF {
**codedData** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::= id-hcpki,
**codeDataValue** UTF8String ::= the-code-for-file-clerk-role,
**codeDataFreeText** DirectoryString ::= CN=Sally R. Jones }
**regionalHCData** Sequence of RegionalData ::= {
**type** OBJECT IDENTIFIER ::= OID-for-this-regional-encoding,
**country** PrintableString (SIZE (2) ::= ISO-country-code-for-USA,
**issuingAuthority** DirectoryString ::= (C=US, L=CA, OU= American Health Systems),
**hcMajorClassCode** CodedData ::= {
**codingSchemeReference** OBJECT IDENTIFIER ::=
ASTM-Coding-Scheme-for-Type,
**codeDataValue UTF8String** ::= ASTM-Type-OID-for-file-clerk }

Обратите внимание, что в отличие от примера, представленного в А.4 (сертификат квалифицированного медицинского работника), здесь нет ни номера лицензии, ни кода статуса лицензии. Такое допускается, поскольку эти региональные поля являются необязательными и решение, включать их в сертификат или нет, остается на усмотрение ЦС, выпускающего сертификат.

### А.7 Профиль сертификата организации

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

| | |
|---|---|
| **version** | (2 — десятичный код сертификатов версии 3) |
| **serialNumber** | (уникальный номер, генерируемый ЦС) |
| **signature** | (sha-1WithRSAEncryption {1,2,840,113549,1,1,5}) |
| **issuer** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (California) |
| **organizationName** | (California Hospital Authority) |
| **commonName** | (Health Digital Certificate policy v01) |
| **validity** | (срок действия в формате UTCTime) |
| **subject** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион = California) |
| **organizationName** | (Midtown Hospital) |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |

| | |
|---|---|
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись, или неоспоримость, или шифрование) |
| **certificatePolicies** | (объектный идентификатор соответствующей политики) |
| **cRLDistributionPoints** | (место входа в COC X.500) |

**А.8 Профиль CA**

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

| | |
|---|---|
| **version** | (2 — десятичный код сертификатов версии 3) |
| **serialNumber** | (уникальный номер, генерируемый ЦС) |
| **signature** | (sha-1WithRSAEncryption {1,2,840,113549,1,1,5}) |
| **baseCertificateID** | (339393322281) |
| **entityName** | (д-р Benjamin Casey) |
| **Optional** | |
| **AttCertValidity** | (срок) |
| **Attributes** | (доступ к дневникам операций) |
| **issuer** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (California) |
| **organizationName** | (California Hospital Authority) |
| **commonName** | (CA - / policy V.01) |
| **validity** | (срок действия в формате UTCTime) |
| **subject** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион = California) |
| **organizationName** | (Midtown Hospital) |
| **commonName** | (Midtown Secure Server 01) |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись, или неоспоримость, или шифрование) |
| **certificatePolicies** | (объектный идентификатор соответствующей политики) |
| **cRLDistributionPoints** | (место входа в COC X.500) |

**А.9 Профиль сертификата ЦС**

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

| | |
|---|---|
| **version** | (2 — десятичный код сертификатов версии 3) |
| **serialNumber** | (уникальный номер) |
| **signature** | (sha-1WithRSAEncryption {1,2,840,113549,1,1,5}) |
| **issuer** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион California) |
| **organizationName** | (California Hospital Authority) |
| **commonName** | (CA – Health PKI US-CT/ policy V.01) |
| **validity** | (срок действия в формате UTCTime) |
| **subject** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион California) |
| **organizationName** | (El Cerrito Health Authority) |
| **commonName** | (CalifHA PKI US CT/ policy V.03) |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бит {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |

| | |
|---|---|
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись СОС и сертификатов) |
| **certificatePolicies** | (объектный идентификатор соответствующей политики) |
| **basicConstraints** | (ЦС = true) |
| **cRLDistributionPoints** | (место входа в СОС X.500) |

### А.10 Профиль кросс-сертификата

Примечание — Этот пример служит только для целей иллюстрации и не является прототипом будущего формата сертификатов службы здравоохранения штата Калифорния.

| | |
|---|---|
| **version** | (2 — десятичный код сертификатов версии 3) |
| **serialNumber** | (уникальный номер) |
| **signature** | (sha-1WithRSAEncryption {1,2,840,113549,1,1,5}) |
| **issuer** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион California) |
| **organizationName** | (California Hospital Authority) |
| **commonName** | (CA — Health PKI US-CT/ policy V.01) |
| **validity** | (срок действия в формате UTCTime) |
| **subject** | |
| **countryName** | (US = Соединенные Штаты Америки) |
| **localityName** | (регион Washington) |
| **organizationName** | (Washington Health Authority) |
| **commonName** | (CalifHA PKI US CT/ policy V.03) |
| **subjectPublicKeyInfo** | |
| **algorithm** | (открытый ключ RSA, 1024 бита {1,2,840,113549,1,1,1}) |
| **subjectPublicKey** | (открытый ключ субъекта) |
| **extensions** | |
| **authorityKeyIdentifier** | (уникальный идентификатор открытого ключа ЦС) |
| **subjectKeyIdentifier** | (уникальный идентификатор открытого ключа субъекта) |
| **keyUsage** | (цифровая подпись СОС и сертификатов) |
| **certificatePolicies** | (объектный идентификатор соответствующей политики) |
| **basicConstraints** | (ЦС = true) |
| **cRLDistributionPoints** | (место входа в СОС X.500) |

**Приложение ДА**
**(справочное)**

## Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

| Обозначение ссылочного международного стандарта | Степень соответствия | Обозначение и наименование соответствующего национального стандарта |
|---|---|---|
| ИСО 17090-1:2008 | IDT | ГОСТ Р ИСО 17090-1—2009 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 1. Структура и общие сведения» |
| ИСО 17090-3:2008 | IDT | ГОСТ Р ИСО 17090-3—2010 «Информатизация здоровья. Инфраструктура с открытым ключом. Часть 3. Управление политиками центра сертификации» |
| IETF/RFC 3280 | — | * |
| IETF/RFC 3281 | — | * |
| IETF/RFC 3739 | — | * |

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

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия:
- IDT — идентичные стандарты.

## Библиография


[1] IETF/RFC 2459 Internet X.509. Public Key Infrastructure Certificate and CRL Profile
[2] IETF/RFC 2527 Internet X.509. Public Key Infrastructure Certificate Policy and Certification Practices Framework
[3] IETF/RFC 3647 Internet X.509. Public Key Infrastructure Certificate Policy and Certification Practices Framework
[4] ETF/RFC 822 Standard for the Format of ARPA Internet Text Messages
[5] ISO/IEC 9594-8:2005 Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks
[6] ISO/IEC 8825-1:2002 Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[7] IETF/RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[8] ANSI X9.42:2003 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
[9] ISO/TS 21091 Health Informatics — Directory services for security, communications and identification of professionals and patients
[10] ISO 3166-1:2006 Codes for the representation of names of countries and their subdivisions — Part 1: Country codes
[11] ASTM E 1986—98 Standard Guide for Information Access Privileges to Health Information

УДК 004:61 ОКС 35.240.80 П85 ОКСТУ 4002

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

Редактор *М.В. Григорьева*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 14.10.2011. Подписано в печать 01.11.2011. Формат 60x84 1/8. Гарнитура Ариал. Усл. печ. л. 3,72. Уч.-изд. л. 3,16. Тираж 99 экз. Зак. 1023.

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

gost.e-ecolog.ru