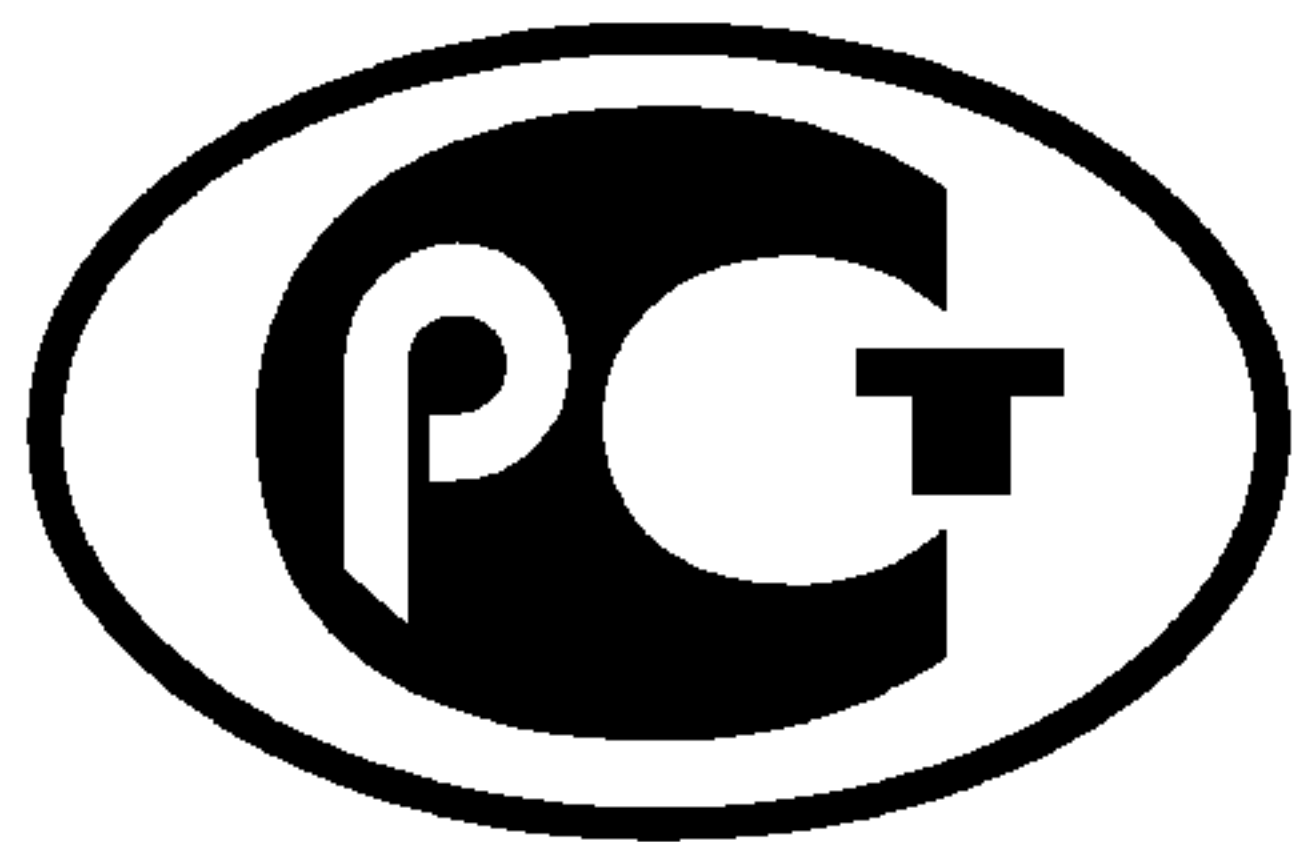

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



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

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

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)

- 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.

Инфраструктура с открытым ключом



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 60x84¹/₈. Гарнитура Ариал. Усл. печ. л. 3,72.
Уч.-изд. л. 3,16. Тираж 99 экз. Зак. 1023.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник»,
105062 Москва, Лялин пер., 6.