МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/TS 22600-3— 2013

Информатизация здоровья

УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 3

Реализация

(ISO/TS 22600-3:2009, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Корпоративные электронные системы», ФБУ «Консультационно-внедренческая фирма в области международной стандартизации и сертификации — «Фирма «ИНТЕРСТАНДАРТ» и Федеральным государственным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Росздрава» (ЦНИИОИЗ Росздрава) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 5

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

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 5 ноября 2013 г № 61-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Молдова	MD	Молдова-Стандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 3 июня 2014 г. № 493-ст межгосударственный стандарт ГОСТ ISO/TS 22600-3—2013 введен в действие в качестве национального стандарта Российской Федерации с 1 июля 2015 г.

5 Настоящий стандарт идентичен международному документу ISO/TS 22600-3:2009 «Информатизация здоровья. Управление привилегиями и контроль доступа. Часть 3. Реализация» («Health informatics — Privilege management and access control — Part 3: Implementations», IDT).

Международный документ разработан Техническим комитетом Межгосударственной электротехнической комиссии ISO/TS 215 «Health informatics» (Информатизация здоровья).

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

6 ВВЕДЕН ВПЕРВЫЕ

7 ПЕРЕИЗДАНИЕ. Январь 2019 г.

*Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном 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 (*gost.e-ecolog.ru

© ISO, 2009 — Все права сохраняются
© Стандартинформ, оформление, 2015, 2019

В Российской Федерации 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 2
3 Термины и определения 2
4 Список сокращений 10
5 Структуры и сервисы управления привилегиями и контроля доступа 11
6 Интерпретация формальных моделей, определенных в ISO/TS 22600-2, для сферы здравоохранения 14
7 Представление понятий в информационных системах здравоохранения 15
8 Согласие 19
9 Экстренный доступ 19
10 Детализация модели контроля доступа 19
11 Детализация модели делегирования 20
Приложение А (справочное) Инфраструктура управления привилегиями 21
Приложение В (справочное) Расширения структуры сертификата атрибута 50
Приложение С (справочное) Сравнение терминологии 51
Приложение D (справочное) Примеры управления политикой и представления политики 52
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов межгосударственным стандартам 55
Библиография 56

Введение

В лечебно-профилактических учреждениях нередко внедряются информационные системы разных поставщиков, каждая из которых требует от пользователя отдельной аутентификации и авторизации доступа, поскольку они реализуют эти функции по-разному. Интеграция этих функций требует значительных затрат на взаимные отображения сведений о пользователях и организациях. В такой ситуации ресурсы, необходимые для разработки и эксплуатации функций обеспечения безопасности, растут в геометрической прогрессии с увеличением числа информационных систем.

С другой стороны, если посмотреть на авторизацию с позиции учреждения здравоохранения, то будет очевидна потребность в гибкой модели ее реализации, поскольку в учреждениях постоянно происходят изменения. Одни подразделения закрываются, другие создаются, третьи объединяются.

Ситуация становится еще более сложной, когда для взаимодействия требуется пересечение периметров зон с разными политиками безопасности. Для преодоления различий между этими политиками необходимы взаимные соглашения о политиках между сторонами, обеспечивающими безопасность.

Другая сложность заключается в назначении пользователям функциональных и структурных ролей. В то время как пользователь может иметь две или более структурные роли одновременно, в конкретном запросе информации он может выступать в единственной функциональной роли. Политика определяет отношения между несколькими функциональными ролями, назначенными пользователю, включая отношения группировки, иерархии, комплексных структурных ролей, упорядоченности функциональных ролей и недопустимости определенных сочетаний ролей. Например, если врач общей практики является также и психиатром, то в политике может быть указано, что роль психиатра может сочетаться с другими структурными ролями со схожими привилегиями, что роль психиатра наследует привилегии, назначенные роли врача общей практики, что создается новая комплексная структурная роль или что эти две структурных роли не могут сочетаться. Примером ограничения последовательного выполнения функциональных ролей может служить конфликт обязанностей, который может быть запрещен действующим законодательством (например, лицо, получающее возмещение оплаты оказанной ему медицинской помощи, не имеет право подписывать платеж этого же возмещения). Кроме того, в организации здравоохранения могут быть определены различные должностные обязанности, учитывающие роли и деятельность пользователей. В разных странах или в разных условиях оказания медицинской помощи аналогичным категориям пользователей могут назначаться разные типы или уровни авторизации выполнения конкретных функций или доступа к информации.

Другой не менее важный и актуальный вопрос — как повысить качество обслуживания, используя информационные технологии (ИТ), не нарушая при этом права личности пациента. Чтобы врачи могли получать наиболее адекватную информацию о пациенте, необходимо иметь что-то вроде «виртуальной электронной медицинской карты», которая позволяет регистрировать всю медицинскую помощь, оказанную пациенту, независимо от того, где и кем она документировалась. При таком подходе необходима общая модель авторизации доступа или специальное соглашение об авторизации между сторонами, обеспечивающими безопасность.

Кроме необходимости учета многообразия ролей и обязанностей, типичного для любой крупной организации, решающее значение могут иметь и другие критичные аспекты медицинской помощи, например, этические или юридические, обусловленные особенностями используемой информации.

Необходимость в строго ограниченной авторизации актуальна и сейчас, но будет существенно возрастать в ближайшие пару лет в связи с ростом числа актов обмена информацией между прикладными программами, необходимых для удовлетворения потребностей врачей в получении все большего и большего объема информации о пациенте в целях обеспечения высокого качества и эффективности лечения.

За последнее десятилетие произошли заметные изменения в части сервисов информационной безопасности прикладных программ и передачи данных. Далее указаны некоторые факторы, способствующие этим изменениям:

- переход от централизованных систем на базе больших компьютеров к распределенным системам на базе местных вычислительных ресурсов;
- все больше данных хранится в информационных системах, и тем ценнее они для пользователей;
- пациенты становятся все более мобильными, и их медицинские данные требуются в разных местах пребывания.

Вследствие необходимости защиты персональных данных, требуемой для исключения нежелательных личных и социальных последствий, эти изменения влекут за собой повышение требований к средствам защиты передачи и обработки медицинских данных. Эта защита должна распространяться как на обмен информацией, так и на ее обработку. Что касается таких механизмов защиты передачи данных как аутентификация, целостность, конфиденциальность, доступность, отчетность (включая ведение аудита и неоспоримость), а также службы удостоверения, то первый упомянутый механизм, а именно, аутентификация, критичен для большей части остальных механизмов. Это справедливо и по отношению к безопасности обработки данных, где необходимы управление доступом, целостность, конфиденциальность, доступность, мониторинг действий, аудит и службы удостоверения.

Применение данного стандарта будет вызывать особую сложность в связи с тем, что участвующие стороны уже располагают действующими системами и не проявят особого желания немедленно обновить их или полностью заменить. Поэтому очень важно, чтобы стороны подписали соглашение о политике, в котором они подтверждают намерение к движению в сторону применения настоящего стандарта по мере возникновения потребности в модификации этих систем.

Соглашение о политике должно также содержать описание выявленных различий в системах обеспечения информационной безопасности и согласованных мер по их преодолению. Например, при аутентификации права и обязанности одной стороны, запрашивающей доступ к информации другой стороны, должны обеспечиваться в соответствии с согласованной политикой, записанной в соглашении между сторонами. Для решения этой задачи необходимо обеспечить соответствующую группировку и классификацию как пользователей и поставщиков информации и информационных услуг, так и самой информации и предоставляемых услуг. Такая классификация может служить основой для применения механизмов обработки требований доступа, категорирования информации и информационных услуг, а также механизмов описания политик контроля доступа и управления ими. Если все взаимодействующие стороны не видят каких-либо угроз, взаимодействие существующих систем и обмен информацией можно начинать сразу же после подписания соглашения о политике контроля доступа. Если угрозы настолько существенны, что их надо исключить до начала обмена информацией, то эти угрозы надо описать в соглашении о политике контроля доступа и добавить к нему перечень мероприятий по устранению угроз. Соглашение должно содержать график выполнения этих мероприятий и определить способ их финансирования.

Процесс документирования очень важен и служит основой для выработки соглашения о политике контроля доступа. Настоящий стандарт состоит из трех частей.

- Часть 1: Обзор и управление общей политикой, содержащая описание сценариев и критичных характеристик трансграничного обмена информацией. В ней также приводятся примеры необходимых методов документирования, которые должны послужить основой соглашения о политике контроля доступа.

- Часть 2: Формальные модели, содержащая более детальные описания архитектуры и моделей привилегий и управления привилегиями, реализуемых для обеспечения защиты совместного доступа к информации. Эти описания дополнены примерами шаблонов соглашений о политике контроля доступа.

- Часть 3: Применение, содержащая более детальные описания реализуемых спецификаций механизмов безопасности обработки данных и инфраструктурных служб, использующие разные языки спецификации.

Настоящий стандарт представляет принципы и описывает сервисы, необходимые для управления привилегиями и контроля доступа. Криптографические протоколы не входят в область его применения.

Данная часть стандарта ISO/TS 22600 тесно связана с другими международными стандартами в этой предметной области, например, ISO/TS 17090, ISO/TS 21091 и ISO/TC 21298.

Данную часть стандарта ISO/TS 22600 следует рассматривать в сочетании с полным комплектом связанных стандартов.

Распределенная архитектура совместно используемых медицинских информационных систем, которая постепенно становится сервис-ориентированной и обеспечивающей ведение персональных медицинских записей, все в большей степени основана на применении вычислительных сетей. Благодаря ощутимым выгодам для пользователей применение стандартизованных интерфейсов пользователя, инструментальных средств и протоколов, обеспечивающее платформенную независимость предлагаемых решений, становится все более популярным, что за пару последних лет привело к ощутимому росту числа действительно открытых информационных систем, предназначенных для функционирования в корпоративных вычислительных сетях и в частных виртуальных сетях.

Настоящий стандарт предназначен для обеспечения потребности совместной обработки медицинской информации самостоятельными медицинскими работниками, организациями здравоохранения, медицинскими страховыми организациями, их пациентами, персоналом и контрагентами.

В настоящем документе учтена возможность запросов как со стороны физических лиц, так и со стороны информационных систем.

Стандарт ISO/TS 22600 описывает методы управления авторизацией и контролем доступа к данным или к функциям. В нем предусмотрена интеграция политик. В его основу положена концептуальная модель, в соответствии с которой местные серверы управления авторизацией и трансграничный сервер каталога участвуют в контроле доступа к различным приложениям (программным компонентам). Сервер каталога предоставляет информацию о правилах доступа к различным прикладным функциям в зависимости от ролей и других атрибутов, назначенных отдельному пользователю. Разрешение доступа зависит от следующих аспектов:

- аутентифицированная идентификация пользователя;
- правила доступа, связанные со специфичным информационным объектом;
- правила, использующие атрибуты авторизации, назначенные пользователю и предоставляемые сервером управления авторизацией;
- функции специфичного приложения.

Настоящий стандарт может использоваться в широких масштабах от местного до регионального или национального применения. Одним из ключевых моментов такого применения должны быть организационные критерии в сочетании с профилями авторизации, согласованными между запрашивающей и предоставляющей стороной в письменном соглашении о политике.

В настоящем стандарте предусмотрена возможность взаимодействия нескольких авторизующих сторон, которые могут функционировать более чем в одной организации или в сфере действия политики.

Такое взаимодействие регламентируется соглашением о политике, подписанным всеми участвующими сторонами и создающим базовую платформу для их деятельности.

В качестве платформы соглашения о политике предлагается определенный формат ее документирования, позволяющий получить сопоставимую документацию от всех сторон, участвующих в обмене информацией.

Для определения необходимых моделей ограничений сконструирована трехмерная архитектурная модель, основанная на уже упомянутом процессе унификации. Размерностями этой Общей компонентной модели служат ось предметной области, ось композиции/декомпозиции и ось, описывающая общее представление о системе и ее компонентах. Чтобы такая модель была развиваемой, устойчивой, гибкой, переносимой и масштабируемой, представлены только процесс ограничений и полученные в его результате метамодели, относящиеся к информационной безопасности. Конкретизация и реализация модели, например, описание механизмов контроля доступа и определения необходимых справочников и классификаторов, представляют собой длительный процесс, который должен найти свое отражение в других стандартах и проектах, инициируемых производителями и поставщиками.

После краткого обзора основ, изложенных в стандарте ISO/TS 22600-2, будут обсуждены различные способы представления разных уровней зрелости с разными уровнями интероперабельности, не достигающими идеала семантической интероперабельности.

Для таких разных условий и уровней настоящий стандарт описывает примеры конкретизации и применения формальных высокоуровневых моделей архитектурных компонентов, основанных на стандарте ISO/IEC 10746 и определенных в стандарте ISO/TS 22600-2. Эти примеры и описания соответствующих сервисов сгруппированы в отдельных приложениях.

Определения даются на языках SAML (Security Assertion Markup Language — язык разметки объявлений безопасности) и XACML (eXtensible Access Control Markup Language — расширяемый язык разметки контроля доступа), сконструированных организацией OASIS на базе расширяемого языка разметки XML (eXtensible Markup Language). Дополнительные определения представлены с использованием традиционного синтаксиса Абстрактной синтаксической нотации ASN.1.

Настоящий стандарт в существенной мере гармонизирован со стандартом ASTM E2595-07.

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

Информатизация здоровья

УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ И КОНТРОЛЬ ДОСТУПА

Часть 3

Реализация

Health informatics. Privilege management and access control.
Part 3. Implementations

Дата введения — 2015—07—01

1 Область применения

Настоящий стандарт конкретизирует требования к хранилищам политик контроля доступа и требования к инфраструктуре управления привилегиями в сфере информационных систем здравоохранения. В нем предложены примеры применения формальных моделей, описанных в стандарте ISO/TS 22600-2.

Настоящий документ тесно связан с другими документами, разрабатываемыми Техническим комитетом 215 ISO, например, ISO 17090, ISO 22857 и ISO/TS 21091. Он также связан со стандартом ISO/TS 21298.

Настоящий стандарт не содержит платформенно-зависимых деталей и других деталей применения. В нем не специфицированы технические сервисы безопасности передачи данных, методы аутентификации и протоколы, описанные в других стандартах, например, ISO 7498-2, ISO/IEC 10745 (ITU-T X.803), ISO/IEC TR 13594 (ITU-T X.802), ISO/IEC 10181-1 (ITU-T X.810), ISO/IEC 9594-8 «Основы аутентификации» (эквивалентен стандарту ITU-T X.509), ISO/IEC 9796, ISO/IEC 9797 и ISO/IEC 9798.

Стандарт ISO/TS 22600 определяет службы управления привилегиями и контроля доступа, требуемые для передачи и использования распределенной медицинской информации между организациями здравоохранения и периметрами безопасности. В стандарте ISO/TS 22600 описаны принципы построения и спецификации служб, необходимых для управления привилегиями и контроля доступа. Он описывает необходимые понятия, связанные с использованием компонентов, и предназначен для обеспечения их технической реализации. Стандарт не содержит указаний по применению этих понятий в конкретных лечебно-диагностических процессах и не касается вопросов безопасности пациентов, связанных с их применением.

В то время как стандарт ISO/TS 22600-1 содержит общее описание проблемы согласования политик в контексте обмена данными между организациями и совместного использования этих данных, стандарт ISO/TS 22600-2 определяет общий процесс анализа, конструирования, реализации и семантической гармонизации информационных систем здравоохранения. Сервисы информационной безопасности, необходимые для выполнения юридических, социальных, организационных, пользовательских, функциональных и технических требований, должны быть встроены в развитую и устойчивую архитектуру систем, отвечающую парадигме информационной безопасности.

Издание официальное

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения к нему):

ISO 8601:2004, Data elements and interchange formats — Information interchange — Representation of dates and times (Элементы данных и форматы обмена. Информационный обмен. Представление дат и времени)

ISO/IEC 9594-8:2001, Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks (Информационная технология. Взаимодействие открытых систем. Каталог: платформы открытых ключей и атрибутов сертификата)

ISO/IEC 10181-3:1996, Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework (Информационная технология. Взаимодействие открытых систем. Платформы безопасности для открытых систем. Платформа управления доступом)

ISO/TS 21298:2008, Health informatics — Functional and structural roles (Информатизация здоровья. Функциональные и структурные роли)

ASTM E2595-07, Standard Guide for Privilege Management Infrastructure (Стандартное руководство по инфраструктуре управления привилегиями)

ASTM E1762-07, Standard Guide for Electronic Authentication of Health Care Information (Стандартное руководство по электронной аутентификации информации в здравоохранении)

ASTM E1986-98, Standard Guide for Information Access Privileges to Health Information (Стандартное руководство по привилегиям информационного доступа к медицинской информации)

ASTM E2212-02a, Standard Practice for Healthcare Certificate Policy (Общепринятая практика для политики сертификатов в здравоохранении)

OASIS, eXtensible Access Control Markup Language (XACML) v2.0, February 2005 (Расширяемый язык разметки по управлению доступом)

OASIS, XACML Profile for Role Based Access Control (RBAC): Committee Draft 01 (normative; 13 February 2004) (Профиль управления ролевым доступом в языке XACML)

OASIS, Security Assertion Markup Language (SAML), Version 2.0, March 2005 OASIS 200306, Service Provisioning Markup Language (SPML), V1.0, October 2003 (Язык разметки для объявлений безопасности)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **контроль доступа** (access control): Средства, с помощью которых ресурсы системы обработки данных предоставляются только авторизованному субъекту в соответствии с установленными правами на доступ.

[ISO/IEC 2382-8:1998]

3.2 **функция принятия решения о доступе** (access control decision function, ADF): Специализированная функция, применяющая правила политики контроля доступа к требуемому действию для принятия решения о доступе.

3.3 **функция применения решения о доступе** (access control enforcement function, AEF): Специализированная функция, обеспечивающая запрашивающей стороне доступ к требуемому ресурсу в соответствии с решением, принятым функцией принятия решения о доступе.

3.4 **информация, используемая для управления доступом** (access control information): Любая информация, используемая для целей контроля доступа, в том числе контекст.

3.5 **учетность** (accountability): Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

[ISO 7498-2:1989]

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

[ISO/IEC 10181-1:1996]

3.7 **орган по присвоению атрибутов, ОА** (attribute authority, AA): Уполномоченное лицо, назначающие привилегии путем выдачи сертификатов атрибута.

[ISO/IEC 9594-8:2001]

3.8 **список отозванных сертификатов органов по присвоению атрибутов** (attribute authority revocation list, AARL): Список отозванных сертификатов, содержащий ссылки на сертификаты, выпущенных для ОА, которые признаны недействительными центром сертификации.

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

[ISO/IEC 9594-8:2001]

3.10 **список отозванных сертификатов атрибута** (attribute authority revocation list, AARL): Список отозванных сертификатов, содержащий ссылки на сертификаты атрибута, которые признаны недействительными органом сертификации.

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

Примечание — См. также аутентификацию источника данных (3.50).

[ISO 7498-2:1989]

3.12 **токен аутентификации** (authentication token): Информация, передаваемая процедуре усиленной аутентификации и предназначенная для аутентификации ее отправителя.

3.13 **уполномоченный орган** (authority): Субъект, ответственный за выпуск сертификатов.

Примечание — В настоящем стандарте даны определения двум категориям органов сертификации: органу, выпускающему сертификаты открытых ключей, и органу, выпускающему сертификаты атрибута.

3.14 **сертификат уполномоченного органа** (authority certificate): Сертификат, выпущенный для органа сертификации или органа по присвоению атрибутов.

Примечание — Адаптация определения, приведенного в ISO/IEC 9594-8:2001.

3.15 **список отозванных сертификатов уполномоченных органов** (authority revocation list, ARL): Список отозванных сертификатов открытого ключа, выпущенных для уполномоченных органов, которые признаны недействительными органом сертификации.

3.16 **авторизация** (authorization): Процесс предоставления субъекту привилегий, в том числе предоставление доступа на основе привилегий доступа или путем передачи привилегий от субъекта, обладающего более высокими привилегиями, субъекту с меньшими привилегиями.

Примечание — Адаптация определения, приведенного в ISO 7498-2:1989.

3.17 **удостоверение авторизации** (authorization credential): Подписанное объявление атрибутов разрешений, выданных пользователю.

3.18 **доступность** (availability): Свойство доступности и возможности беспрепятственного использования авторизованным субъектом.

[ISO 7498-2:1989]

3.19 **базовый список отозванных сертификатов** (base CRL): Список отозванных сертификатов, который служит основой для выпуска разностных списков отозванных сертификатов.

3.20 **соглашение деловых партнеров** (business partner agreement): Документ, используемый для разграничения юридической, этической и практической ответственности между подписчиками защищаемой медицинской информации (ЗМИ) и между взаимодействующими реализациями ЗМИ.

3.21 **сертификат центра сертификации** (CA certificate): Сертификат центра сертификации, выпущенный другим центром сертификации.

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

3.23 **распространение сертификатов** (certificate distribution): Акт публикации сертификатов и их передачи принципалам безопасности.

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

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

3.26 **политика сертификатов** (certificate policy): Именованный свод правил, описывающих применимость сертификата в конкретном кругу субъектов и/или класс приложений с общими требованиями к информационной безопасности.

Пример — В конкретной политике сертификатов может быть указана применимость некоторого типа сертификатов для аутентификации транзакций электронного обмена данными в целях торговли товарами определенного ценового диапазона.

3.27 **отзыв сертификата** (certificate revocation): Акт аннулирования достоверной связи между сертификатом и его владельцем, поскольку сертификату больше нельзя доверять, хотя его срок и не истек.

3.28 **список отозванных сертификатов;** СОС (certificate revocation list, CRL): Заверенный список сертификатов, которые издатель сертификатов считает недействительными.

Примечание — Наряду с СОС общего назначения могут быть определены специфичные типы СОС для конкретных сфер применения. Существует опубликованный список приостановленных и отозванных сертификатов (заверенный электронной подписью центра сертификации).

3.29 **порядковый номер сертификата** (certificate serial number): Целочисленное значение, уникальное для данного центра сертификации, который может быть однозначно связан с выпущенным им сертификатом.

3.30 **список приостановленных сертификатов;** СПС (certificate suspension list, CSL): Опубликованный список приостановленных сертификатов (заверенный электронной подписью центра сертификации).

3.31 **пользователь сертификата** (certificate user): Организация или лицо, которому необходимы точные данные публичного ключа другой организации или лица.

3.32 **система применения сертификатов** (certificate using system): Реализация тех функций, определенных в спецификации каталога, которые применяются пользователем сертификата.

3.33 **подтверждение действительности сертификата** (certificate validation): Процесс установления того, что на заданный момент сертификат является действительным, включая возможность создания и проверки пути сертификации и подтверждение того, что на этот момент времени все сертификаты данного пути действительны (т. е. не просрочены и не отозваны).

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

3.35

3.35.1 **орган сертификации** (certification authority, CA): Уполномоченный орган, которому одна или несколько участвующих сторон доверили выпуск и присвоение сертификатов. Орган сертификации может факультативно генерировать ключи для доверяющих ему участников.

Примечание — Адаптация определения, приведенного в ISO/IEC 9594-8:2001.

3.35.2 **орган сертификации** (certification authority): Орган, выпускающий сертификаты, подписывая их своим секретным ключом.

Примечание — Слово «орган» в термине «орган сертификации» означает всего лишь доверенную сторону, а не какое-либо государственное лицензирование. Более удачным термином может быть «издатель сертификата», но термин «орган сертификации» очень широко употребляется.

3.36 **список отозванных центров сертификации;** СОЦС (certification authority revocation list, CARL): Список сертификатов открытого ключа, выпущенных для центров сертификации, которые издатель сертификатов считает недействительными.

3.37 **путь сертификации** (certification path): Упорядоченная последовательность сертификатов объектов в дереве информации каталога, которая может быть обработана с использованием открытого ключа первого объекта пути для получения последнего объекта пути.

3.38 **шифротекст** (ciphertext): Данные, получаемые в результате использования шифрования.

Примечание — Семантическое содержимое полученных в результате шифрования данных недоступно

[ISO 7498-2:1989].

3.39 **заявитель** (claimant): Организация или лицо, запрашивающее у контролера выполнение или предоставление чувствительного сервиса в соответствии с привилегиями, указанными в его сертификате атрибута или в расширении атрибутов каталога субъекта его сертификата открытого ключа.

3.40 **конфиденциальность** (confidentiality): Свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неуполномоченным лицам, логическим объектам или процессам.

[ISO 7498-2:1989]

3.41 **информированное согласие** (consent): Специальная политика, определяющая соглашение между организацией или лицом, выступающим в роли субъекта действия, и организацией или лицом, выполняющим это действие.

3.42 **удостоверение** (credential): Информация, описывающая атрибуты безопасности (идентичность или привилегию, либо и то, и другое), являющаяся необходимым условием/предпосылкой для назначения на роль или соответствия требованиям к назначению на роль.

Примечание — Удостоверения предъявляются при аутентификации либо делегировании и используются системой контроля доступа.

3.43 **точка распространения; СОС** (CRL distribution point): Элемент каталога либо иной источник распространения СОС.

Примечание — СОС, распространяющийся такой точкой, может содержать только подмножество сертификатов, отозванных одним центром сертификации, а также отозванные сертификаты, выпущенные несколькими центрами сертификации.

3.44 **криптография** (cryptography): Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого либо предотвращения их не обнаруживаемой модификации или несанкционированного использования.

[ISO 7498-2:1989]

3.45 **криптографический алгоритм, шифр** (cryptographic algorithm, cipher): Метод преобразования данных для сокрытия их информационного содержимого либо предотвращения их не обнаруживаемой модификации или несанкционированного использования.

[ISO 7498-2:1989]

3.46 **криптографическая система, криптосистема** (cryptographic system, cryptosystem): Совокупность преобразований из обычного текста в шифротекст и обратно, конкретные преобразования, применяемые в зависимости от ключей.

Примечание — Преобразования обычно задаются математическим алгоритмом.

3.47 **служба конфиденциальности данных** (data confidentiality): Служба, которая может использоваться для защиты данных от несанкционированного раскрытия.

Примечание — Служба конфиденциальности опирается на систему аутентификации. Она может использоваться для защиты данных от перехвата.

3.48 **целостность данных** (data integrity): Способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа.

[ISO 7498-2:1989]

3.49 **аутентификация источника данных** (data origin authentication): Подтверждение, что источник полученных данных именно тот, который объявлен.

[ISO 7498-2:1989]

3.50 **дешифрование, дешифрация** (decipherment, decryption): Процесс получения исходных данных из шифротекста.

Примечания

1 Шифротекст мог быть повторно зашифрован, и однократная расшифровка может не привести к получению исходных незашифрованных данных.

2 Адаптация определения из ISO/IEC 2382-8:1998.

3.51 **делегирование** (delegation): Передача привилегии от ее обладателя другому субъекту.

3.52 **путь делегирования** (delegation path): Упорядоченная последовательность сертификатов, которая может быть обработана наряду с аутентификацией идентичности заявителя привилегий для проверки аутентичности его привилегий.

3.53 **разностный СОС (рСОС)** (delta CRL, dCRL): Частичный список отозванных сертификатов, в котором перечислены только те сертификаты, чье состояние отзыва изменилось с момента выпуска базового СОС.

3.54 **электронная подпись** (digital signature): Электронная подпись — дополнительные данные или криптографическое преобразование (см. криптография) какого-либо блока данных, позволяющие получателю блока данных убедиться в подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, получателем.

[ISO 7498-2:1989]

3.55 **шифрование, шифрация** (encipherment, encryption): Криптографическое преобразование данных (см. криптография) для получения шифротекста.

[ISO 7498-2:1989]

3.56 **конечный субъект** (end entity): Субъект сертификата, использующий свой секретный ключ для иных целей, нежели подпись сертификата, или доверяющий субъект.

3.57 **список отзыва сертификатов атрибута конечных субъектов;** САКС (end-entity attribute certificate revocation list, EARL): Список отозванных сертификатов атрибута, признанных недействительными издателем сертификатов и выпущенных для владельцев сертификатов, не являющихся органами по присвоению атрибутов.

3.58 **список отзыва сертификатов открытого ключа конечных субъектов;** СОКС (end-entity public key certificate revocation list, EPRL): Список отозванных сертификатов открытого ключа, выпущенных для владельцев сертификатов, не являющихся центрами сертификации, и признанных недействительными издателем сертификатов.

3.59 **переменные среды** (environmental variables): Положения политики, требуемые для принятия решений об авторизации, которые не входят в статические структуры, но могут быть предоставлены контролеру привилегий с помощью местных средств (например, время суток или текущий баланс счета).

3.60 **полный СОС** (full CRL): Полный список отозванных сертификатов, в котором перечислены все сертификаты, отозванные в определенной сфере действия.

3.61 **функциональная роль** (functional role): Роль, связанная с действием, которая может быть назначена для выполнения в процессе этого действия.

Примечания

1 Функциональные роли соответствуют понятию участия, определенного в справочной информационной модели RIM (Reference Information Model).

2 Адаптация определения из стандарта ISO/TS 21298:2008.

3 См. также структурную роль (3.105).

3.62 **функция хэширования** (hash function): Функция (математическая), которая отображает значения из большого домена (возможно, очень большого) на меньший диапазон значений.

Примечание — Функция хэширования считается «хорошей», если результат ее применения к значениям из (большого) подмножества домена равномерно (и практически случайным образом) распределяется по меньшему диапазону значений.

3.63 **владелец** (holder): Организация или лицо, которому делегированы некоторые привилегии либо непосредственно источником авторизации, либо косвенным образом другим органом по присвоению атрибутов.

3.64 **идентификация** (identification): Выполнение тестов, позволяющих системе обработки данных опознать субъект.

[ISO/IEC 2382-8:1998]

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

[ENV 13608-1:2007]

3.66 **косвенный СОС;** кСОС (indirect CRL, iCRL): Список отозванных сертификатов, содержащий информацию об отзыве сертификатов, выпущенных органами, отличающимися от того, который выпустил этот список.

3.67 **целостность** (integrity): Свойство информации, согласно которому она случайно или преднамеренно не изменена.

[ISO 7498-2:1989]

3.68 **ключ** (key): Последовательность символов, управляющая операциями шифрования и дешифрования.

[ISO 7498-2:1989]

3.69 **соглашение о ключе** (key agreement): Метод соглашения о значении ключа без передачи значения ключа, даже в зашифрованной форме, например, алогоритм Диффи-Хеллмана.

Примечание — Дополнительную информацию о механизмах соглашения о ключе см. в ISO/IEC 11770-1.

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

[ISO 7498-2:1989]

3.71 **протокол LDAP** (Lightweight Directory Access Protocol, LDAP — облегченный протокол доступа к каталогам): Стандартный протокол доступа к каталогам, обеспечивающий публичный или контролируемый доступ к сертификатам и к другой информации, необходимой для инфраструктуры открытых ключей.

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

3.73 **объектный идентификатор;** ОИД (object identifier, OID): Уникальный алфавитно-цифровой/цифровой идентификатор, зарегистрированный в соответствии со стандартом регистрации идентификаторов ISO и присвоенный конкретному объекту или классу объектов.

Примечание — Объектный идентификатор служит именем политики сертификации, которое записано в поле каждого сертификата, выпущенного в соответствии с этой политикой.

3.74 **метод объекта** (object method): Действие, которое может быть осуществлено с ресурсом.

Пример — Файловая система может читать и записывать данные объекта, а также выполнять его методы.

3.75 **односторонняя функция** (one-way function): Легко вычисляемая (математическая) функция, для которой по значению y в диапазоне возможных значений вычислительно сложно найти такое входное значение x, для которого $f(x) = y$.

Примечание — Может существовать небольшое число значений y, для которых поиск x не будет вычислительно сложным.

3.76 **разрешение** (permission): Разрешение выполнения операции над одним или несколькими объектами, защищенными в соответствии с ролевым управлением доступом.

3.77 **политика** (policy): Комплекс юридических, методических, организационных, функциональных и технических обязательств или запретов по обмену информацией и совместной деятельности.

3.78 **соглашение о политиках** (policy agreement): Письменное соглашение, в котором все участвующие стороны обязуются придерживаться определенного комплекса политик.

3.79 **точка принятия решения о политике;** ТРП (policy decision point, PDP): Системный объект, выбирающий применяемую политику и предоставляющий решение об авторизации.

Примечания

1 Этот термин имеет иное определение в документе RFC 3198 [45].

2 Этот термин соответствует термину «Access Decision Function» (ADF, функция принятия решения о доступе), определенному в ISO 10181-3:1996.

3.80 **точка применения политики;** ТПП (policy enforcement point, PEP): Системный объект, выполняющий контроль доступа путем запросов на принятие решения о доступе и применения решений об авторизации.

Примечания

1 Это определение термина дано совместно рабочей группой Policy Framework Working Group организации IETF и рабочей группой DMTF/CIM (Distributed Management Task Force/Common Information Model) в документе RFC 3198.

2 Этот термин соответствует термину «Access Enforcement Function» (AEF, функция применения решения о доступе), определенному в ISO 10181-3:1996.

3.81 **отображение политик** (policy mapping): При условии, что центр сертификации (ЦС), действующий в одном домене, сертифицирует ЦС, действующий в другом домене, конкретная политика, определенная во втором домене, может считаться уполномоченным органом первого домена эквивалентной (но не обязательно идентичной во всех отношениях) некоторой политике, определенной в первом домене.

3.82 **принципал** (principal): Действующее лицо, способное реализовать определенные сценарии (пользователь, организация, система, устройство, прикладная программа, компонент, объект).

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

[ISO/IEC 10181-1:1996]

3.84 **привилегия** (privilege): Право, предоставленное субъекту уполномоченным органом в соответствии с атрибутом этого субъекта.

3.85 **заявитель привилегии** (privilege asserter): Обладатель привилегии, использующий свой сертификат атрибута или сертификат открытого ключа для заявления о наличии привилегии.

3.86 **инфраструктура управления привилегиями; ИУП** (privilege management infrastructure, PMI): Инфраструктура, способная поддерживать функцию управления привилегиями для обеспечения развитой службы авторизации во взаимодействии с инфраструктурой открытых ключей.

3.87 **политика привилегий** (privilege policy): Политика, описывающая условия, при которых контролер привилегий может предоставить/выполнить защищенный сервис в интересах заявителя привилегии.

Примечание — Политика привилегий определяется в терминах атрибутов, ассоциированных с сервисом, и атрибутов, ассоциированных с заявителем привилегии.

3.88 **контролер привилегий** (privilege verifier): Субъект, подтверждающий соответствие сертификатов политике привилегий.

3.89 **открытый ключ** (public key): Ключ, используемый в асимметричном криптографическом алгоритме и допускающий его общедоступную реализацию.

[ISO/IEC 10181-1:1996]

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

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

3.91 **инфраструктура открытых ключей; ИОК** (public key infrastructure, PKI): Инфраструктура, используемая в отношениях между владельцем ключа и доверяющей стороной и позволяющая доверяющей стороне использовать сертификат, связанный с владельцем ключа по меньшем мере для одного приложения, использующего сервис безопасности, зависящий от открытого ключа.

Примечание — В ИОК входят центр сертификации, структура данных сертификата, средства, позволяющие доверяющей стороне получить текущую информацию о состоянии отзыва сертификата, политика сертификации и методы проверки практики сертификации.

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

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

Примечание — Для управления ролью могут быть определены связи между субъектами, структурными и функциональными ролями [ISO/TS 21298:2008].

3.94 **сертификат назначения роли** (role assignment certificate): Сертификат, содержащий атрибут роли, назначающий одну или более ролей владельцу сертификата.

3.95 **сертификат роли** (role certificate): Сертификат, назначающий привилегии роли, а не напрямую какому-либо лицу.

Примечание — Лица, которым назначена данная роль с помощью сертификата атрибута или сертификата открытого ключа, в котором это назначение указано в дополнении Subject Directory Attributes, косвенно обладают привилегиями, назначенные сертификатом роли.

3.96 **сертификат спецификации роли** (role specification certificate): Сертификат, содержащий назначение привилегий роли.

3.97 **чувствительность** (sensitivity): Характеристика ресурса с позиции его ценности или важности.

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

3.99

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

[ISO/IEC 2382-8:1998]

3.99.2 **политика безопасности** (security policy): Свод правил, составленный уполномоченным органом по безопасности, регулирующий использование и предоставление сервисов и средств безопасности.

3.100 **сервис безопасности** (security service): Сервис, предоставляемый каким-либо уровнем взаимодействия открытых систем, который обеспечивает адекватную защиту систем или процедур передачи данных.

[ISO 7498-2:1989]

3.101 **простая аутентификация** (simple authentication): Аутентификация, основанная на применении паролей.

3.102 **источник полномочий** (source of authority, SoA): Орган по присвоению атрибутов, которому контролер привилегий доступа к определенному ресурсу доверяет как единственному лицу, уполномоченному назначать набор привилегий, либо специальный вид такого органа, которому контролер неограниченно доверяет.

Примечание — Контролер доверяет источнику привилегий делегировать свою привилегию владельцам сертификатов, часть из которых, в свою очередь, могут делегировать ее другим владельцам сертификатов.

3.103 **усиленная аутентификация** (strong authentication): Аутентификация с помощью удостоверений, созданных с помощью криптографических методов.

3.104 **структурная роль** (structural role): Структурные роли описывают отношения между субъектами в части компетенции (роли, определенные в модели RIM). Они нередко отражают организационные или структурные отношения (иерархии).

[ISO/TS 21298:2008]

Примечание — См. определение функциональной роли (3.61).

3.105 **цель** (target): Ресурс, к которому субъект запрашивает доступ.

Примечание — Чувствительность цели моделируется в данном документе как набор атрибутов, описанный либо нотацией ASN.1, либо в форме элементов на языке XML.

3.106 **доверие** (trust): Качество, при наличии которого о субъекте говорят, что он «оказывает доверие» другому субъекту, т. е. он (первый субъект) предполагает, что второй субъект будет действовать в полном соответствии с ожиданиями первого субъекта.

Примечание — Понятие доверия может относиться только к некоторой специфичной функции. Ключевая роль доверия в данном контексте состоит в описании отношений между аутентифицирующимся субъектом и уполномоченным органом; субъект должен быть уверен, что он может доверять тому, что уполномоченный орган создает только валидные и надежные сертификаты.

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

3.108 **доверенная третья сторона; ДТС** (trusted third party, TTP): Третья сторона, которая при реализации протокола безопасности считается доверенной.

Примечание — Этот термин используется во многих стандартах ISO/IEC и в других документах, которые, в основном, описывают сервисы ЦС. Однако это понятие шире и включает в себя такие сервисы как штампы времени и, возможно, депонирование ключей. Третьи доверенные стороны обеспечивают базовые сервисы, инфраструктурные сервисы и дополнительные сервисы.

3.109 **контролер** (verifier): Субъект, ответственный за выполнение или предоставление чувствительного сервиса квалифицированным заявителям или за получение сервиса от таких заявителей.

Примечание — Контролер применяет политику привилегий. При проверке пути сертификации контролер является доверенной стороной определенного типа.

4 Список сокращений

В настоящем стандарте применены следующие сокращения:

AA — орган по присвоению атрибутов (Attribute Authority);

AARL — список отзыва органов по присвоению атрибутов (Attribute Authority Revocation List);

ACI — информация контроля доступа (Access Control Information);

ACRL — список отзыва сертификатов атрибута (Attribute Certificate Revocation List);

ADF — функция принятия решения о доступе (Access Decision Function);

ADI — информация о решении контроля доступа (Access Control Decision Information);

AEF — функция применения решения о доступе (Access Enforcement Function);

ANSI — Американский национальный институт стандартов (American National Standards Institute);

ARL — список отзыва уполномоченных органов (Authority Revocation List);

CA — центр сертификации (Certification Authority);

CARL — список отзыва центров сертификации (Certification Authority Revocation List);

CIM — общая информационная модель (Common Information Model);

CORBA — общая архитектура брокера объектных запросов (Common Object Request Broker Architecture);

CRL — список отзыва сертификатов (Certificate Revocation List);

dCRL — разностный список отзыва сертификатов (Delta Certificate Revocation List);

DAP — протокол доступа к каталогам (Directory Access Protocol);

DEA — управление по борьбе с наркотиками (Drug Enforcement Administration);

DIB — информационная база каталога (Directory Information Base);

DIT — информационное дерево каталога (Directory Information Tree);

DMTF — Рабочая группа по распределенному управлению (Distributed Management Task Force);

DSA — агент системы каталога (Directory System Agent);

DTD — определение типов данных (Data Type Definition);

DUA — агент пользователя каталога (Directory User Agent);

EARL — список отзыва сертификатов атрибута конечных субъектов (End-entity Attribute Certificate Revocation List);

EHR — электронная медицинская карта (Electronic Health Record);

EPRL — список отзыва сертификатов открытого ключа конечных субъектов (End-entity Public Key Certificate Revocation List);

HL7 — организация Health Level Seven;

iCRL — косвенный список отзыва сертификатов (Indirect Certificate Revocation List);

IETF — организация Internet Engineering Task Force;

IT — информационная технология (Information Technology);

LDAP — облегченный протокол доступа к каталогам (Lightweight Directory Access Protocol);

OASIS — организация Organization for the Advancement of Structured Information Standards;

OCSP — Онлайновый протокол статуса сертификата (Online Certificate Status Protocol);

OMG — организация Object Management Group;

PA — орган по присвоению привилегий (Privilege Allocator);

PDP — точка принятия решения о политике (Policy Decision Point);

PEP — точка применения политики (Policy Enforcement Point);

PKC — сертификат открытого ключа (Public Key Certificate);

PKCS — криптосистема открытых ключей (Public Key Cryptosystem);

PKI — инфраструктура открытых ключей (Public Key Infrastructure);

PMI — инфраструктура управления привилегиями (Privilege Management Infrastructure);

PPS — комплекс политик разрешения доступа (Permission Policy Set);

RA — центр регистрации (Registration Authority);

RBAC — ролевой контроль доступа (Role-Based Access Control);

RPS — комплекс политик роли (Role Policy Set);

S/MIME — защищенные многоцелевые расширения почты Интернет (Secure Multipurpose Internet Mail Extensions);

SAML — язык разметки подтверждения безопасности (Security Assertion Markup Language);

SOA — сервис-ориентированная архитектура (Service-Oriented Architecture);

SoA — источник полномочий (Source of Authority);

SPML — язык разметки предоставления сервисов (Service Provisioning Markup Language);

TTP — доверенная третья сторона (Trusted Third Party);

UDDI — Универсальное описание, поиск и взаимодействие (Universal Description, Discovery and Integration);

UHID — универсальный идентификатор пациента (Universal Healthcare Identifier);

UML — Унифицированный язык моделирования (Unified Modeling Language);

URI — универсальный идентификатор ресурса (Uniform Resource Identifier);

XACML — расширяемый язык разметки контроля доступа (eXtensible Access Control Markup Language);

XML — расширяемый язык разметки (eXtensible Markup Language).

5 Структуры и сервисы управления привилегиями и контроля доступа

Управление привилегиями и контроль доступа регулируются политиками. Для обеспечения интероперабельности эти политики должны быть формализованы. В соответствие с Общей компонентной моделью базовый класс структуры политик был определен в стандарте ISO/TS 22600-2 (рисунок 1). Как упоминалось в этом стандарте, политики могут иметь разные представления. Например, определение политик веб-сервисов, использованное организацией OASIS, предусматривает общую модель и синтаксис для описания и передачи политики веб-сервиса. Оно задает описание политики в форме общих сообщений, в которых передаются заявления о политике, а также механизмы вложений, позволяющие использовать представление политики в существующих технологиях сервисов XML. В настоящем документе конкретное представление политик не используется.

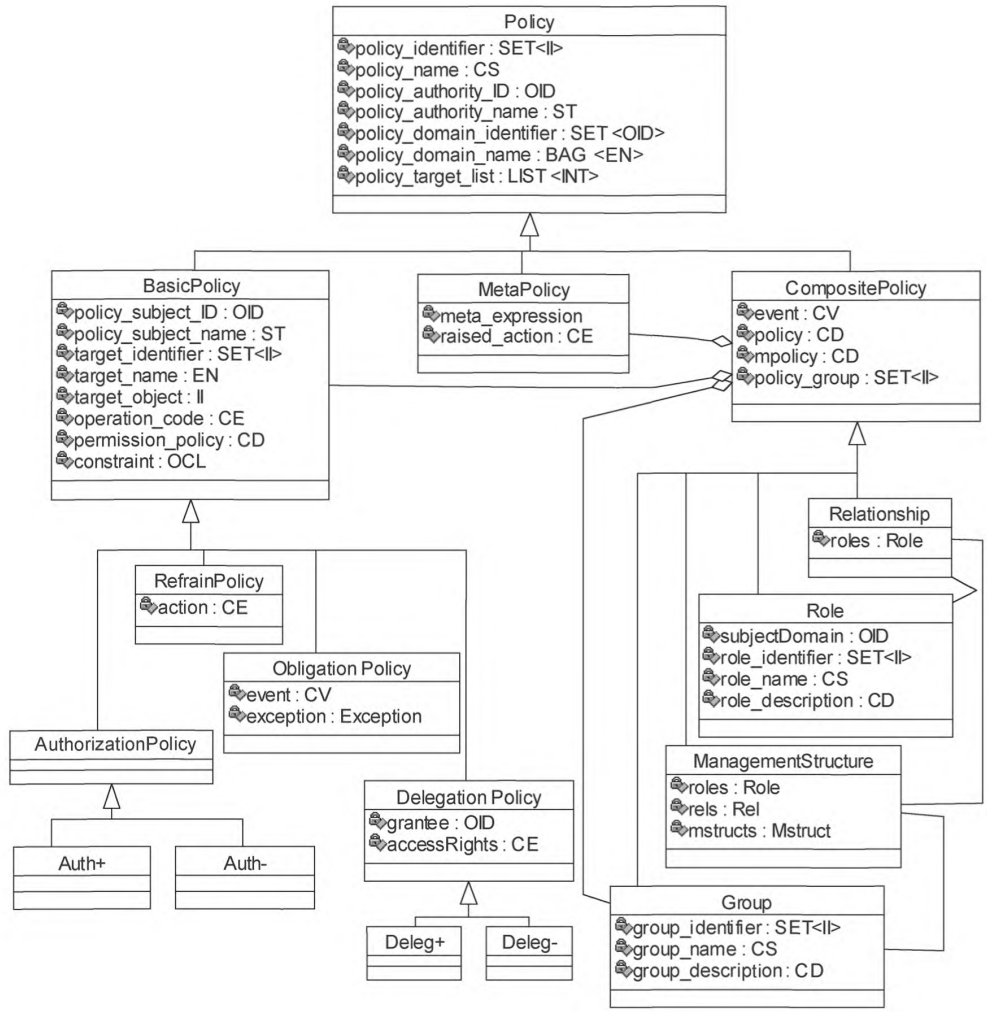


Рисунок 1 — Диаграмма базовых классов политик

Управление привилегиями и контроль доступа основаны на некотором комплексе инфраструктурных сервисов, которые прямо или косвенно связаны с сервисами информационной безопасности и конфиденциальности. В этом аспекте необходимо упомянуть ряд сервисов ИОК и доверенных третьих сторон, например, управление идентификацией, управление ролями и привилегиями, управление политиками, управление объектами и т.д. Кроме того, требуется обсудить такие сервисы как аудит, LDAP, обнаружение вторжений и т.д. Их реализации, в том числе механизмы сервисов и состав нормативно-справочной информации, быстро меняются и обсуждение этих вопросов вынесено в справочные приложения. Содержание настоящего документа в максимально возможной степени согласовано со стандартом ASTM E2585-07.

В описанной далее модели информационной безопасности в связи со специфичными требованиями и условиями здравоохранения необходимо рассмотреть весь спектр сервисов и механизмов безопасности, которые могут выполняться в микро-областях.

а) Взаимодействие между зонами безопасности

По соглашению участвующих сторон отдельные зоны безопасности в доменной модели могут передавать информацию о привилегиях. Такое взаимодействие между зонами должно координироваться как на техническом, так и на документальном уровне. При создании и передаче информации о комплексах привилегий должна приниматься во внимание организационная структура.

b) Техническая основа

Необходим контроль обменов информацией о привилегиях, гарантирующий, что смысл привилегий согласован между зонами безопасности. Для обеспечения возможности такого контроля можно создать стандартный комплекс привилегий. Он может включать в себя отображение эквивалентных привилегий, совместно определенное зонами безопасности. Эквивалентность передаваемых привилегий может быть проверена на технической основе, чтобы гарантировать необходимые следствия их применения.

c) Административная основа

1) Информация о привилегиях, передаваемая между зонами безопасности, может относиться к разным административным субъектам (например, разным деловым партнерам или организациям). В этом случае соглашение об обмене привилегиями и их применении должно документироваться, обычно в форме «соглашения деловых партнеров». Наличие такого соглашения необходимо для разделения юридической, этической и практической ответственности между деловыми партнерами. Оно может быть распространено на других участников реализованной инфраструктуры управления привилегиями. Эквивалентная процедура выполняется в инфраструктуре открытых ключей с помощью заявления о практике сертификации и политик сертификации. В политиках веб-сервисов используется альтернативная процедура «заявлений о политике».

2) В одном учреждении или организации может существовать несколько зон безопасности. Документ, регламентирующий разделение ответственности между такими зонами, должен быть оформлен в виде соглашения деловых партнеров или протокола о намерениях (MOU — memorandum of understanding). Этот документ должен периодически пересматриваться, чтобы обмен привилегиями между зонами безопасности осуществлялся, пока у организации есть в этом необходимость.

d) Организационные требования.

Информация о привилегиях, передаваемая между зонами безопасности, должна быть структурирована. Ее структура должна соответствовать организационным требованиям. Образование зоны безопасности, охватывающей определенную организационную цель (например, бухгалтерский или кадровый учет), является существенным элементом согласованного подхода. С учетом других внешних факторов (например, угроз) результирующий стандартный набор привилегий, пригодный для обмена между зонами безопасности, должен быть, как следствие, весьма ограниченным. При этом набор привилегий, предназначенный для одной части организации (например, для бухгалтерии), не должен включать в себя привилегии, необходимые другой, не связанной части организации (например, кадровой службе). Кроме того, результирующий набор общих привилегий должен содержать ровно те привилегии, которые необходимы для достижения определенной цели.

В настоящем документе рассматриваются только те аспекты, которые представлены затененными прямоугольниками на рисунке 2.

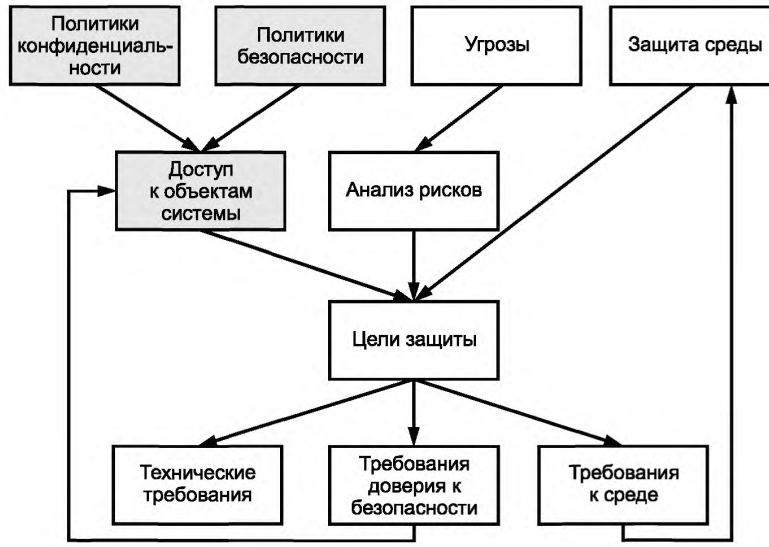


Рисунок 2 — Аспекты безопасности, рассматриваемые в настоящем документе

Все сервисы управления включают в себя создание, именование, определение, группировку или классификацию, присваивание, эксплуатацию, исправление, синхронизацию и деактивацию, и т. д.

Будучи основаны на данной модели политик, управление привилегиями и контроль доступа должны управляться политиками в соответствии со стандартами ISO/TS 22600-1 и ISO/TS 22600-2, как показано на рисунке 3 (см. [2, 3]).

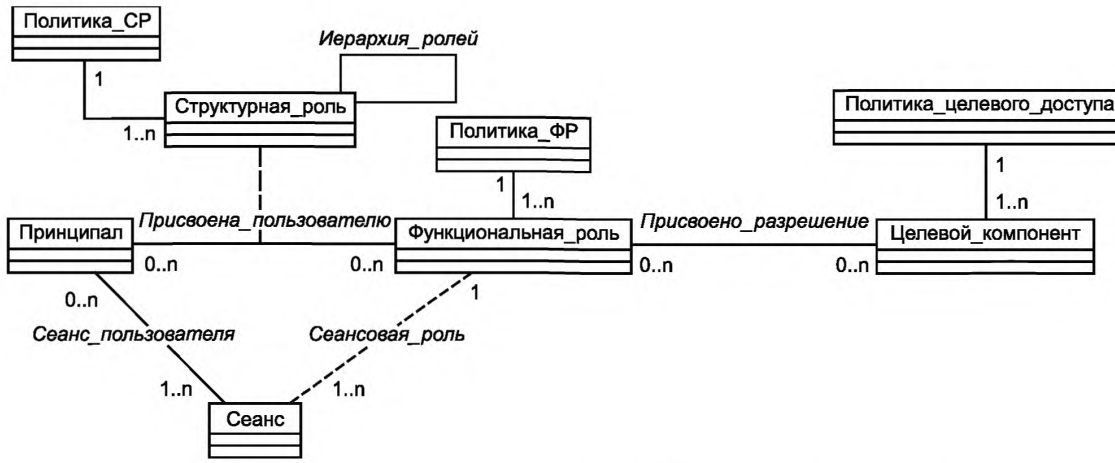


Рисунок 3 — Схема ролевого контроля доступа, управляемого политиками

6 Интерпретация формальных моделей, определенных в ISO/TS 22600-2, для сферы здравоохранения

Формальные модели, определенные в ISO/TS 22600-2, основаны на Общей компонентной модели (см. [3, 4]). В этой модели применен архитектурный подход, состоящий в формальном представлении понятий и связей между ними. Эти понятия и связи представляют знания и являются производными от источников, полученными с помощью моделирования ограничений. Чтобы облегчить понимание моделей, представленных в настоящем документе, далее приведено краткое описание основных принципов, сопровождаемое некоторыми уточнениями или профилями моделей, определенных в стандарте ISO/TS 22600-2.

Чтобы понять, передать и изменить реальность в соответствии с нашими социальными, экологическими, организационными или техническими деловыми целями, ее надо наблюдать, описывать и правильно интерпретировать в замкнутом цикле с помощью моделей (см. [5, 6, 7, 8]). Модель является мысленным представлением чего-то полезного в реальном мире, в которой не обязательно учитывать каждую деталь реальности. С помощью моделей создаются знания. Разработка математических моделей помогает их разработчикам и лицам, принимающим решения, понимать связи между важными характеристиками деловых процессов. С другой стороны, описание и особенно интерпретация реальных систем основаны на знании. Знание суть сочетание инстинктов, идей, правил и процедур, которые управляют действиями и решениями. Оно используется для преобразования данных в информацию, полезную в конкретной ситуации. Знание помогает пользователям интерпретировать информацию и действовать на ее основе. Построение терминов подразумевает знание. Следовательно, классификация наборов терминов представляет собой упорядочение знания. Модель классификации терминов состоит из элементов и их представлений (семантических понятий, терминов), связей между элементами терминологии классификации, явного представления этих связей (см. [9]).

7 Представление понятий в информационных системах здравоохранения

7.1 Введение

Понятие можно рассматривать как формальную модель. Оно должно быть уникально идентифицируемым, независимым и признанным экспертами и пользователями. Понятие как компонент знания может, как и любой компонент, иметь специализации и обобщения. Оно обеспечивает согласованное описание объектов предметной области, которые идентифицируются и пользователями предметной области используются независимо для записи информации (см. [8]). Совокупность понятий называется «онтологией». Онтология обеспечивает формализацию знаний предметной области. Для представления знаний наиболее часто используются два из ряда возможных подходов: продукционный подход (продукционные правила, правила «если-то») и фреймовый подход. Продукционный подход основан на различных стратегиях рассуждений. В основе фреймов лежит объектно-ориентированный подход, описывающий необходимые характеристики объекта. Фреймы состоят из слотов, описывающих атрибуты объекта конкретного типа. Данные во фрейме могут использоваться для описания соответствующей ситуации, для организации данных и для идентификации исключений. Любой слот фрейма должен иметь значение, заданное по умолчанию, или ссылку на другой фрейм. Таким образом, понятие представляет собой согласованное описание предметных сущностей (компонентов), которые определяются отдельно и используются для записи информации. Знание состоит из понятий, которые могут объединяться или декомпозироваться с помощью обобщения или специализации, которые определяют отношения между этими понятиями. Для достижения целей организации от внедрения информационных систем необходимо организовать выполнение: анализа, концептуализации, проектирования, реализации и эксплуатации информационных систем, учитывая методы работы, имеющуюся информацию, уровень персонала и применяемые информационные технологии.

Подобно представлению знаний о мире объектов или компонентов, понятия также структурированы (организованы) в виде слотов (см. определение фрейма выше). Такое структурирование может быть выполнено с помощью всех известных представлений понятий в сфере здравоохранения, например, архетипов (archetypes), модулей представления медицинских знаний, записанных с помощью синтаксиса Ардена (Arden Syntax MLM), языков ограничений объектов (OCL — Object Constraint Language), а также с помощью формальных представлений политик безопасности, например, с помощью логики первого порядка или логики предикатов, либо с помощью таких формальных языков как SAML, XACML и т. д.

7.2 Языки описания предметных областей

Для обеспечения представления и передачи знаний необходимо адекватно представлять соответствующие понятия, что реализуется с помощью общих языков, языков для конкретных предметных областей, формальных языков и формальных моделей. Термины и применяемые знания могут объединяться в терминологии и онтологии. Метатезаурусы определяют представление знаний о предметной области (см. таблицу 1). Понятия, специфичные для предметной области, формируются из требований к бизнес-процессам. Поэтому любой процесс разработки современной информационной системы должен начинаться с выбора процессов и методов разработки требований и анализа архитектуры, т. е. с создания модели бизнес-процессов. На этом этапе эксперты в данной предметной области определяют структуру бизнес-процессов или выбирают их шаблоны, отражающие реальные бизнес-процессы, без учета их дальнейшей реализации в информационно-коммуникационной среде. На следующем этапе должна быть выбрана методология разработки, установки, тестирования, эксплуатации и интеграции приложений. Обеспечивая полный цикл разработки информационной системы, Общая компонентная модель описывает любую модель бизнес-процессов предприятия. Трехмерная архитектура модели позволяет представлять знания с помощью понятий и связей между ними, включая обобщение и специализацию. С другой стороны, для моделирования понятий, используемых в здравоохранении, могут использоваться архетипы.

Таблица 1 — Представление знаний с помощью метатезаурусов

Понятия
Термины с одинаковым значением объединяются в понятие.
Понятиям назначаются свойства, например:
- уникальный идентификатор,
- определение.
Связи
Понятия связаны с другими понятиями.
Связям назначаются свойства, например:
- тип связи,
- источник связи.

Представления понятий и правил на разных уровнях представления знаний обеспечивают разные степени интероперабельности. На самом верхнем уровне стабильной архитектуры, построенной в соответствии с Общей компонентной моделью и формальными моделями, предложенными в ISO/TS 22600-2 для управления привилегиями и контроля доступа, обеспечивается автономная семантическая интероперабельность. В зависимости от средств выражения понятий, с помощью которых структурная и функциональная информация может интерпретироваться человеком или компьютером, интероперабельность переносится на нижележащие уровни. В то время как структурная информация позволяет договариваться о политиках, функциональная основана на присваивании атрибутов, осуществляемом администраторами или другими системными пользователями (например, пациентами). В этом контексте требуется управлять взаимосвязями представлений понятий разных предметных областей, используя разные языки предметных областей. Далее кратко обсуждаются различные способы представления политик, а также средства назначения и реализации.

7.3 Моделирование ограничений на языке OCL

Язык ограничений объектов OCL является стандартным расширением языка UML, позволяющим формулировать запросы к элементам модели, ограничивать элементы (во время моделирования) и определять операции запросов [5, 11]. Он обеспечивает возможность интеграции в архитектурном процессе. В парадигме Общей компонентной модели определение бизнес-правил вызывает большие затруднения. Язык OCL обеспечивает ограничения моделей со специальным поведением. Выражения языка OCL состоят из трех частей: контекст пакета (необязательный), контекст выражения (обязательный) и одно или несколько выражений. Ограничения на языке OCL организованы в форме выражений (таблица 2).

Таблица 2 — Моделирование ограничений на языке OCL

package < путьКПакету>	контекст пакета
context <имяЭкземпляраКонтекста>:<элементМодели>	контекст выражения
<типВыражения><имяВыражения>:	выражение
<телоВыражения>	
<типВыражения><имяВыражения>:	выражение
<телоВыражения>	
endpackage	

7.4 Другие представления ограничений

7.4.1 Общие сведения

В соответствии с Общей компонентной моделью, здравоохранение и используемые в нем информационные системы имеют дело не только с медициной и биологией, но и с другими предметными областями. Среди них необходимо упомянуть финансирование, технологию, правовые аспекты и безопасность. Рассматривая безопасность, необходимо моделировать юридические понятия и понятия, в которых формулируются политики безопасности. Политика охватывает все аспекты системы здравоохранения и информационных систем здравоохранения, например, юридические, социальные, психологические, функциональные и технические.

Управление политикой безопасности может включать в себя все или часть следующих этапов: составление, пересмотр, тестирование, утверждение, публикация, комбинирование, анализ, модификация, прекращение действия, поиск и применение политики. Полная политика, применимая к запросу, требующему решения, может состоять из ряда отдельных правил или политик. Например, для приложения, обеспечивающего конфиденциальность персональных данных, субъект персональной информации может определить одни аспекты политики раскрытия этой информации, в то время как организация, являющаяся владельцем этой информации, может определить другие аспекты. Чтобы принять решение об авторизации запроса, необходимо объединить эти две отдельные политики и сформировать из них одну, применимую к запросу на доступ к информации.

Язык разметки объявлений безопасности SAML (Security Assertion Markup Language), предложенный организацией OASIS, описывает средствами языка XML сервисы безопасности, сопоставленные элементам структуры заголовок-тело-ссылка. Для формального моделирования политик и описания правил контроля доступа эта организация предложила язык XACML, который также является метаязыком по отношению к языку XML.

7.4.2 Язык XACML

Язык XACML определяет три элемента политики верхнего уровня: <Rule> (правило), <Policy> (политика) и <PolicySet> (комплекс политик) [12]. Элемент <Rule> содержит булево выражение, которое может быть вычислено отдельно. Однако решение об авторизации (например, принимаемое точкой принятия решения о политике), не должно приниматься без ссылки на соответствующую политику. В языке XACML предложены алгоритмы комбинирования правил, позволяющие, к примеру, не разрешать переопределение (упорядоченное и неупорядоченное), разрешать переопределение (упорядоченное и неупорядоченное), выбор первого или только одного применимого правила.

Элемент политики <Policy> содержит совокупность элементов правил <Rule> и заданную процедуру сочетания результатов применения этих правил. Результат выполнения этой процедуры служит основой для решения об авторизации, принимаемом точкой принятия решения о политике.

Элемент комплекса политик <PolicySet> содержит совокупность элементов политик <Policy> или другие комплексы политик <PolicySet>, а также заданную процедуру сочетания результатов применения этих политик и комплексов политик. Это стандартный способ образования одной комбинированной политики путем сочетания отдельных политик.

Основными компонентами правил являются: цель, эффект и условие. Цель определяет комплекс ресурсов, субъектов и среду.

Следовательно, политика включает в себя цель основных компонентов, идентификатор алгоритма сочетания правил, комплекс правил и обязательства.

Представленная структура и функция частично отражают компонентную архитектуру политик, описанную в стандарте ISO/TS 22600-2. При этом, однако, упрощены определенные субкомпоненты политики. Детальные сведения см. в определении языка XACML [12].

7.4.3 Язык WSDL

Язык описания веб-сервисов WSDL (Web Services Description Language) представляет собой грамматику на языке XML, предназначенную для описания веб-сервисов. На нем описывается информация об интерфейсах общедоступных функций, типах данных для всех сообщений, привязках к используемому транспортному протоколу, а также к адресам заданных сервисов. Такое описание представляет собой контракт между запрашивающим приложением и приложением, реализующим сервис. Этот контракт не зависит от платформы реализации и языка.

7.4.4 Язык BPEL

Язык выполнения бизнес-процессов BPEL (Web Services Description Language) построен на основе языка XML и предназначен для описания бизнес-процесса в распределенной взаимодействующей

среде. Он формализует управляемые компоненты и исключения. Модель процессов BPEL4WS является надстройкой над моделью сервисов, определенной в языке WSPL (Web Services Policy Language).

7.4.5 Спецификация WS-policy

Спецификация политик веб-сервисов WS-policy является гибкой и расширяемой грамматикой на языке XML и предназначена для описания возможностей, требований и общих характеристик объектов систем, основанных на применении веб-сервисов, в форме информации о политике веб-сервиса, специфичной для конкретной предметной области. Она определяет комплекс альтернативных политик, каждая из которых является комплексом объявлений политики, например, схема аутентификации, выбор транспортного протокола, политика конфиденциальности, характеристики качества сервиса QoS (Quality of Service) и т.д. Для совместимости политик необходимы договоренности о словаре данных и семантике. Спецификация WS-PolicyAttachment (Web Services Policy Attachment) описывает, как связать политики с субъектами, к которыми они применяются, используя описания WSDL.

7.4.6 Язык WSPL

Язык политик веб-сервисов WSPL (Web Services Policy Language) является ограниченным подмножеством стандарта XACML организации OASIS, обеспечивающим отображение политик. Объединенные политики могут быть выражены с помощью детальных атрибутов, например, время дня, цена или сетевые характеристики. В языке WSPL можно использовать булевские операторы «Исключительное ИЛИ» (eXclusive-OR) и «И» (AND). Комплекс <PolicySet> описывает политики конкретного сервиса, при этом каждая политика состоит из последовательности правил, представляющих отдельный аспект сервиса. Правила задают допустимое множество атрибутов, описанное с помощью предикатов. В языке предусмотрена возможность принятия решений в зависимости от допустимости нескольких множеств атрибутов.

7.4.7 Язык DIPAL

Не зависящий от предметной области язык объявлений политики веб-сервисов DIPAL (Domain-Independent Web Services Policy Assertion Language) оперирует выбором развертывания (политиками), а не бизнес-логикой и интерфейсами сервиса, использующими информацию, зависящую от предметной области.

7.4.8 Язык SAML

Язык разметки объявлений безопасности SAML описывает грамматику конвертов, содержащих идентифицирующую информацию и информацию безопасности и предназначенных для передачи из одной зоны безопасности в другую. На этом языке организации могут составлять объявления (утверждения) об идентичности, атрибутах и полномочиях субъекта (нередко пользователя — физического лица) и передавать их другим организациям.

Протоколы SAML определяют структуру пар запрос-ответ, обмен которыми позволяет получить объявления и управлять необходимой идентичностью, задавая протоколы запроса-ответа объявлений, протоколы запроса аутентификации, протоколы управления именами-идентификаторами, протоколы единого входа и единого выхода.

Привязки SAML определяют способы использования протоколов SAML в стандартных протоколах сообщений и обменов данными. Примером могут служить привязки SAML SOAP, привязки SAML PAOS (обратный SOAP), привязки перенаправления HTTP или привязки HTTP POST.

Профили SAML обеспечивают комбинирование выбранных объявлений, протоколов и привязок и определяют поведение в определенных ситуациях. Здесь стоит упомянуть профили единого входа SSO (Single Sign-On), расширенные профили клиентов и агентов ECP (Enhanced Client and Proxy), профили единого выхода, профили запросов объявлений и ответов на них, а также профили атрибутов.

Контекст аутентификации SAML описывает типы и силу существующих методов аутентификации (например, протокола Internet Protocol Password, протокола Kerberos, протокола распространения открытых ключей X.509, управление интеллектуальными картами на основе инфраструктуры открытых ключей, аутентификацию клиентов на основе протоколов SSL-TLS).

Метаданные SAML позволяют действующим лицам, использующим SAML, описывать свои предпочтения и конфигурации.

8 Согласие

8.1 Общие сведения

Политика представляет собой объявление о юридических, организационных, социальных, функциональных и прочих требованиях, которые должны быть выполнены, и тем самым формулирует правила ограничения соответствующих понятий другой зоны безопасности. Согласие представляет собой специальную политику отношений между субъектами, включающую в себя выражение одобрения или приемлемости указанных в ней заявлений. Законодательство многих стран требует, чтобы взаимодействующие субъекты были детально информированы о своих обязательствах и возможных последствиях. Тем самым обеспечивается юридически и этически приемлемая основа такого одобрения (информированное согласие). Согласие должно формулироваться в соответствии с заданной моделью политик и выражаться на формальном языке представления политик.

8.2 Информированное согласие пациента

Чтобы обеспечить уже упомянутые требования, информированное согласие пациента должно формулироваться высокотехнологичным образом и отражать тонкие и детальные понятия и связи применительно к данным, функциональности и сервисам. Таким образом, информированное согласие пациента может покрывать отношения со всеми аспектами оказания медицинской помощи, включая данные и информацию, документы, функции, системы, лица, организации, приложения и т. д., то есть включая принципалов и их действия/результаты действий.

8.3 Управление информированным согласием пациентов

Управление информированным согласием пациентов должно удовлетворять всем принципам политики, включая определение, достижение договоренности, гармонизацию, присваивание, отзыв и т.д.

9 Экстренный доступ

Экстренный доступ должен предоставляться в соответствии с возникшей потребностью и отвечать всем базовым принципам, в том числе юридическим ограничениям, принципу необходимости получения информации и т.д., изложенным в политике экстренного доступа. Важным требованием, которое должно включаться в политику экстренного доступа, является полная регистрация всех выполненных действий.

10 Детализация модели контроля доступа

10.1 Сфера применения модели

В силу общности модели контроля доступа имена ее компонентов довольно абстрактны, однако при соответствующей интерпретации эта модель может быть применима ко всем ситуациям, описанными и обсуждающимся в настоящем документе.

10.2 Использование прямого или обратного вызова

Модель контроля доступа предполагает наличие контролера, обрабатывающего управляющую информацию для принятия решения о разрешении доступа. Заявитель может представить эту информацию (например, токен) при вызове верификатора (прямой вызов) либо контролер может получить требуемую информацию от доверенного источника (обратный вызов). Принимая решение о выборе механизма прямого или обратного вызова, следует учесть ряд факторов, описанных в подпунктах 10.2.1 и 10.2.2.

10.2.1 Прямой вызов

Токены должны иметь короткое время жизни.

Токены должны проверяться сервисом аутентификации.

При передаче токены должны быть зашифрованы.

В зашифрованный токен должен быть включен разовый или уникальный ключ.

10.2.2 Обратный вызов

Сервисы аутентификации должны быть доступны.

Хранилище элементов контроля доступа (ACI — access control item) должно быть доступно сервисам аутентификации.

Доступ к этому хранилищу должен осуществляться с помощью доверенного канала передачи данных.

Токены, содержащие информацию об аутентификации, должны быть достаточно безопасными для защищаемой среды во избежание атак повторения токенов.

11 Детализация модели делегирования

Ограничения делегирования могут задаваться источником аутентификации, заявителем или целью доступа и включать в себя следующую информацию:

a) Уровень делегирования — например, заявителю с ролью делегата может быть запрещено дальнейшее делегирование привилегий.

b) Контекст делегирования — например, делегирование имеющейся привилегии «лучевой диагност» только по отношению к пациенту с данным идентификатором, только для данной серии рентгеновских снимков и только на указанный период времени.

c) Группа делегатов — например, уровень делегирования может не ограничиваться, но все делегаты должны принадлежать определенной группе заявителей.

d) Ограничение использования ссылок — привилегии использования объекта при определенных условиях передаются получателю в виде ссылки на объект. Например, при делегировании привилегии информация контроля доступа, принадлежащая делегирующему принципалу (то есть его атрибуты безопасности) может быть делегирована другому объекту цепочки, чтобы разрешить ему действовать от имени делегирующего принципала при определенных условиях.

e) Неподходящее делегирование — ограничения, препятствующие передаче имеющихся привилегий неподходящему делегату, например, передаче права врача на выписку рецептов представителю административного персонала.

Приложение А
(справочное)

Инфраструктура управления привилегиями

А.1 Гармонизация настоящего приложения со стандартом ASTM E2595-07

В существующих стандартах, включая ANSI X9.45 [46], ISO/IEC 9594-8, IETF RFC 3280 X.509 [47], OASIS SPML, SAML, WS-* и XACML определен ряд механизмов, которые можно использовать для конструирования инфраструктуры управления привилегиями, специфичной для здравоохранения. К ним относятся описанные далее возможности.

Привилегии, необходимые для доступа к целевому объекту, обозначены в удостоверении авторизации заявителя. Таким удостоверением может быть сертификат авторизации, соответствующий стандарту ISO/IEC 9594-8 (частная форма сертификата атрибута), или описание набора политик, совместимое со стандартом XACML либо с другими справочными стандартами авторизации.

Категория чувствительности или иные свойства целевого объекта, к которому требуется доступ, могут храниться в местной базе данных или в подписанной структуре данных. Настоящее приложение не определяет стандартный способ представления этой информации, поскольку он оставлен на местное усмотрение. Он содержит указания, как такая информация может быть представлена и обработана с помощью общих способов описания, например, синтаксиса ASN.1 и языка XML. Если над данным целевым объектом может быть выполнено несколько разных операций, то каждая такая операция может иметь свой набор атрибутов чувствительности.

Политика привилегий может храниться централизовано или локально либо передаваться в виде подписанной структуры данных. Различные операции над целевым объектом могут быть предметом разных политик привилегий. В настоящем приложении описано несколько стандартных политик, и конкретные службы могут использовать дополнительные политики.

В парадигме авторизации документа требования равнозначных подписей могут быть ассоциированы с пользователем или документом, например, подписанный документ может считаться авторизованным (юридически значимым) только в том случае, когда к нему приложены все необходимые подписи.

Пользователи могут делегировать привилегии другим пользователям.

Пользователям могут быть назначены роли, позволяющие передавать привилегии.

Некоторые авторизации могут быть настолько динамичными, что их включение в корпоративную структуру авторизации будет нецелесообразным (вследствие того что стоимость их эксплуатации будет слишком велика, а срок их жизни будет кратким либо они будут часто меняться). Такие авторизации могут храниться в базе данных авторизации местного сервера и назначаться в форме переменных среды.

В оставшейся части настоящего приложения обсуждаются механизмы передачи привилегий, а также информации о чувствительности и политике в распределенной инфраструктуре управления привилегиями.

А.2 Базовая инфраструктура управления привилегиями

А.2.1 Сервисы инфраструктуры управления привилегиями

Базовая инфраструктура управления привилегиями описывает отношения между компонентами абстрактной системы ролей и компонентами нижележащей инфраструктуры безопасности.

Модель контроля доступа, описанная в стандарте ISO/TS 22600-1, расширяется до распределенной архитектуры безопасности или сервис-ориентированной архитектуры в соответствии с рисунком А.1. Контролер показан со своими компонентами PDP/PEP (точкой принятия решения о политиках и точкой применения политик). В защищенной сервис-ориентированной архитектуре безопасная аутентификация и авторизация предоставляются приложениям как сервисы. На рисунке А.1 показано абстрактное представление моделей контроля доступа, предложенных в стандарте ISO/IEC 10181-3 (PDP/PEP в терминологии организации OASIS).

Если удалить внешнего (по отношению к целевому объекту) контролера, то получится традиционная модель контроля доступа. Различные варианты реализации могут быть получены с помощью функциональных размещений сервиса между уровнем приложения и уровнем сервис-ориентированной архитектуры. Информация контроля доступа используется для информирования точки принятия решения о политиках PDP о дополнительных условиях, влияющих на принятие решения.

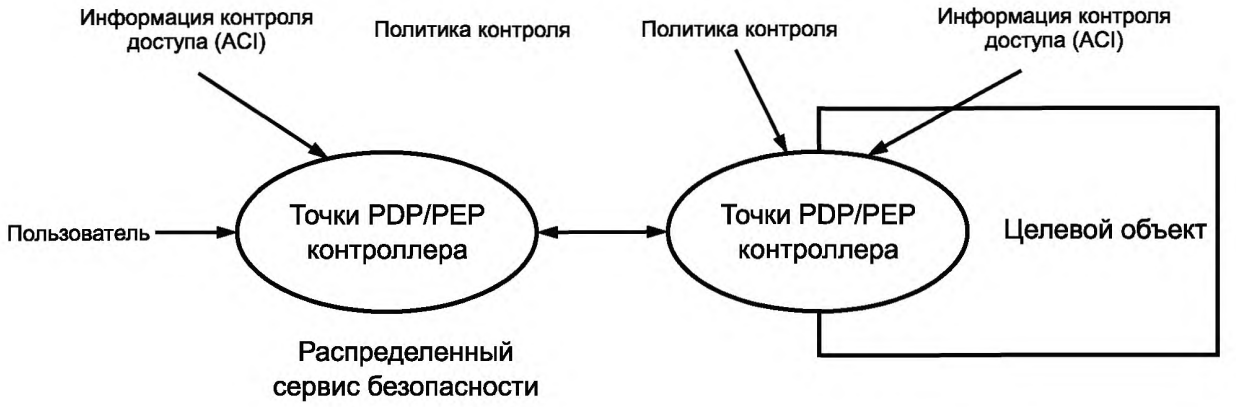


Рисунок А.1 — Расширенная модель контроля доступа

А.2.2 Информация контроля доступа

Информация контроля доступа (ACI), определенная в стандарте ISO, включает в себя следующие данные.

a) Информация контроля доступа инициатора или пользователя:

- индивидуальная идентификация контроля доступа;
- идентификатор иерархической группы, в которой заявлено участие, например, должность в организации;
- идентификатор функциональной группы, в которой заявлено участие, например, идентификатор проекта или рабочей группы;
- роль, которая может быть принята;
- категории чувствительности, к которым разрешен доступ;
- категории целостности, к которым разрешен доступ;
- идентификация контроля управления целевым объектом и допустимые действия над объектом, т. е. целевая возможность;
- атрибуты безопасности делегатов;
- местонахождение, например, рабочая станция, в операционную систему которой вошел пользователь.

b) Информация контроля целевого объекта:

- идентификация контроля доступа целевого объекта;
- идентификация контроля доступа индивидуального инициатора и разрешенные или запрещенные ему действия над целевым объектом;
- идентификация членства в иерархических группах контроля доступа и разрешенные или запрещенные им действия над целевым объектом;
- идентификация членства в функциональных группах контроля доступа и разрешенные или запрещенные им действия над целевым объектом;
- идентификация роли контроля доступа и разрешенные или запрещенные ей действия над целевым объектом;
- уполномоченные органы и авторизованные им действия;
- категории чувствительности;
- категории целостности.

c) Информация контроля доступа к действию:

1) Информация контроля доступа, ассоциированная с действием по зонированию (информация контроля доступа к данным), например:

- категории чувствительности,
- категории целостности,
- идентификация автора,
- идентификация субъекта медицинской помощи[1)].

2) Информация контроля доступа, ассоциированная с действием в целом, например:

- идентификация инициатора.

3) Разрешенные пары инициаторов и целевых объектов:

- разрешенные целевые объекты,
- разрешенные инициаторы (заявители),
- допустимый класс операций (например, чтение, запись),
- требуемый уровень целостности.

[1)] В стандарте ASTM E2595-07 используется термин «идентификация владельца».

d) Информация контекста контроля доступа:

- периоды времени,
- маршрут (доступ может быть разрешен только в том случае, если маршрут обладает специфичными характеристиками),
- местонахождение (доступ может быть разрешен только в том случае, если заданы два инициатора: как специфичные системы — рабочие станции или терминалы — или специфичные местонахождения),
- статус системы (при данной информации контроля доступа требуемый доступ может быть разрешен только в том случае, если система находится в определенном состоянии, например, восстанавливается после аварии),
- сила аутентификации (доступ может быть разрешен только в том случае, если использован механизм аутентификации, сила которого не менее заданной),
- наличие другого текущего доступа у данного инициатора или других инициаторов.

Существуют два типа высокоуровневых ролей в здравоохранении, поддерживаемые инфраструктурой: структурные роли и функциональные роли. Структурные роли описывают предварительные условия, требуемую компетенцию или способности к действиям. Функциональные роли отражают функциональные аспекты связей между объектами. Функциональные роли связаны с реализацией (выполнением) действий.

Возможными примерами структурных ролей медицинских работников служат:

- директор медицинской организации,
- директор клиники,
- заведующий отделением,
- старший врач,
- ординатор,
- врач,
- ассистент,
- интерн,
- главная медсестра,
- медсестра,
- студент.

Возможными примерами функциональных ролей медицинских работников служат:

- лечащий врач (отвечающий за лечение пациента),
- сотрудник диагностического отделения,
- сотрудник терапевтического отделения,
- консультант,
- врач приемного отделения,
- семейный врач,
- функциональная (например, операционная) медсестра.

Детальное описание структурных и функциональных ролей представлено в следующих подразделах.

А.2.3 Управление безопасностью, риск и соответствие

Эффективная схема управления безопасностью включает в себя такое распределение ответственности, полномочий, организацию взаимодействия, которое обеспечивает персоналу требуемую степень управления системой. Управление службами безопасности крайне необходимо, равно как управление политиками безопасности и их применением жизненно необходимо для системной среды.

В сценарии создания сервиса управление включает в себя мониторинг соответствия служб безопасности политикам безопасности, мониторинг соответствия развернутых структур управления, а также мониторинг общей эффективности безопасности системной среды.

При управлении соответствием требованиям безопасности измеряется степень соответствия реализованных сервисов безопасности мерам, определенным в политике безопасности. Реализация таких измерений может быть основана на отчетах о поведении системы, построенных на основе сведений, полученных из регистрационных журналов. Эти отчеты должны позволять сравнение наблюдаемого поведения с тем, которое ожидается на основе сконфигурированных политик. Когда результаты сравнения просматриваются в контексте деловых политик, можно получить всеобъемлющее представление о том, в какой мере предприятие реализовало и применило требуемые политики.

А.2.4 Управление доверием

С деловом отношении управление доверием включает в себя распределение ответственности и юридические аспекты применения сервисов безопасности. Оно также включает в себя сообщения о защите, которые сервис-провайдер может реализовать для чувствительных данных.

На технологическом уровне управление доверием может включать в себя:

- протоколы, с помощью которых потребитель сервиса взаимодействует с его поставщиком. Например, может требоваться передача сообщений SOAP (simple object access protocol) по протоколу HTTPS;
- уникальную идентификацию всех интересующих лиц; к ним относятся лица, имеющие роли потребителей, контрагентов или служащих;
- обеспечение совместного доступа к информации, необходимого внутренним структурам предприятия и внешним партнерам.

К примеру, может быть определена политика регистрации, автоматически создающая учетные записи пользователей (каталог LDAP или база данных с идентификатором учетной записи joe для Joe Smith) в хранилище предприятия (идентификатор учетной записи joesmith для Joe Smith) и в системе сервиса идентификации объектов (учетная запись прикладного уровня с идентификатором joe1234 все для того же пользователя Joe Smith).

Эта политика может быть расширена за границы предприятия, например, учетная запись пользователя создается еще и в регистре внешних потребителей сервиса (с идентификатором homejoe для Joe Smith). Эта политика регистрации может включать в себя несколько рабочих процессов, например, получение разрешений на управление пользователями.

Составной частью таких политик регистрации являются политики идентификации и паролей. Политики идентификации описывают, каким образом создаются различные атрибуты различных учетных записей на основе идентифицирующей информации пользователя и корпоративных правил безопасности.

В данном примере политика идентификации может состоять в создании имени учетной записи, которое состоит из первой буквы имени и букв фамилии пользователя (например, jsmith для Joey Smith). Политика идентификации может распространяться и на другие атрибуты, например, на адреса электронной почты.

Политики паролей могут применяться для контролирования способов создания и управления паролями. Например, в политике может быть указана минимально допустимая длина пароля, обязательно использование букв и специальных символов, а также срок действия, вынуждающий пользователей менять свои пароли каждые три месяца. Выполнение этих требований усиливает безопасность системы, поскольку слабость паролей создает известные риски.

Федеративные политики образуют другой базовый уровень сценария. Они позволяют осуществлять проверку, отображение и передачу различных используемых токенов безопасности между зонами безопасности или системами.

Предприятия должны обеспечивать возможность предоставления доступа к защищаемой медицинской информации на основе наименьшей необходимой привилегии и необходимости знания, определяемой ролями пользователя в организации и порученными ему заданиями.

Поэтому предприятиям необходим интегрированный подход к безопасности, предполагающий создание инфраструктуры, удовлетворяющей следующим требованиям:

- согласованным образом аутентифицировать пользователей при пересечении периметра безопасности предприятия и периметра федерации или внешней сети;
- согласованным образом авторизовать пользователей или предоставлять им разрешения доступа к защищаемым информационным активам;
- регистрировать доступ к чувствительной информации и к чувствительным функциям, а также их использование;
- удовлетворять релевантным методическим указаниям и требованиям информационной безопасности.

Для аутентификации на своем портале пользователям могут требоваться ввод имени своей учетной записи (например, homejoe, jsmith или joe) или средства усиленной аутентификации.

Если пользователь запрашивает сервис как внешний потребитель, то для его аутентификации может потребоваться объявление на языке SAML, в то время как для доступа к приложению во внутренней сети от него будет достаточно токена с именем учетной записи. Представляемый им токен с именем учетной записи может отличаться от того, который необходим для аутентификации на местном портале (например, joesmith). Наконец, приложение может проверить действительность удостоверения пользователя и отобразить его на местную учетную запись.

В сценарии с прямым воздействием потребители внутреннего сервиса должны использовать доверенный сервис, чтобы передать идентифицирующую информацию, свидетельствующую, что пользователь имеет действительное удостоверение. Например, местные имена учетных записей jsmith или joe передаются с удостоверением, сгенерированным для учетной записи joe1234. Затем вызванное приложение проверяет это удостоверение. Службу доверенных токенов безопасности STS (security token service) надо сконфигурировать таким образом, чтобы токены безопасности правильно отображались на те, что воспринимаются получающими их субъектами в данном сценарии.

А.3 Описание сервисов инфраструктуры управления привилегиями на языке ASN.1

А.3.1 Спецификации сертификатов, основанных на стандарте X.509

А.3.1.1 Общие сведения

Ролевая модель инфраструктуры управления привилегиями, основанная на стандарте X.509, использует сертификаты атрибута, описанные в стандарте ISO/IEC 9594-8. Примером использования такой инфраструктуры может служить проект Permis [13]. Сертификаты атрибута выпускаются органами по присвоению атрибутов. Сертификат атрибута привязан к идентификации субъекта с помощью поля владельца (holder) в сертификате идентификации X.509. Такое объединение обеспечивает возможность раздельного управления инфраструктурой управления привилегиями и инфраструктурой открытых ключей [13]. Это позволяет обеспечить конфиденциальность чувствительной информации контроля доступа, если сертификаты идентичности могут управляться третьей стороной. Спецификации ролей в инфраструктуре управления привилегиями, основанной на стандарте X.509, используют, по крайней мере, три типа сертификатов атрибута: сертификаты атрибута спецификации роли, сертифи-

каты атрибута назначения роли и сертификаты атрибута политик. Все они заверены электронной подписью органа по присвоению атрибутов и тем самым защищены от подделки.

Сертификаты атрибута спецификации роли содержат разрешения, назначенные этой роли. Сертификаты атрибута назначения роли содержат список ролей, назначенных субъекту сертификата. Сертификаты атрибута политик указывают корневой узел доверия для инфраструктуры управления привилегиями и в качестве значения атрибута содержат ссылку на файл политики. Сертификаты атрибута обычно хранятся в каталоге, управляемом сервисом LDAP. Контролер находит в каталоге все сертификаты атрибута назначения роли, выпущенные для данного пользователя, проверяет электронную подпись каждого сертификата и проверяет, что сертификаты не отозваны. Затем контролер находит сертификаты атрибута спецификации роли для каждой роли, назначенной пользователю. Существует несколько способов оптимизации этого процесса, сохраняющих общий подход.

Ролевая модель инфраструктуры управления привилегиями, основанная на стандарте X.509, может использовать такие языки описания политик как Ponder, Keynote или XACML. Использование контролером политики авторизации, распространяющейся на всю зону безопасности, обеспечивает безопасный, централизованно управляемый подход.

Местный источник полномочий в зоне безопасности создает политику авторизации, распространяющуюся на всю зону. Сервисы размещения привилегий (PA — Privilege allocator) используют политики, подписанные источником полномочий, возможно, даже из другой зоны безопасности, чтобы сгенерировать сертификаты атрибутов политик и аутентифицировать их с помощью электронной подписи. Источник полномочий или орган по присвоению атрибутов использует результат работы этих сервисов для подписи и публикации сертификатов атрибута назначения роли в каталоге LDAP. Эти сертификаты используются контролером для принятия решения о контроле доступа.

Приведенные далее реализуемые спецификации взяты из существующих официальных стандартов или из стандартов де-факто и включены в настоящий документ для удобства чтения, что является общим подходом в аналогичных спецификациях. Поэтому они представлены с использованием абстрактной синтаксической нотации ASN.1.

В настоящем документе представлены спецификации, разработанные независимо от формальных моделей, описанных в стандарте ISO/TS 22600-2.

A.3.1.2 Сертификаты аутентичности

Сертификат аутентичности соответствует спецификации X.509V3:

```
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
```

Поле version указывает версию закодированного сертификата. Версия сертификата ДОЛЖНА быть v3.

Существует несколько способов привязки сертификатов идентификации, использующих ключи, с сертификатами атрибута, не содержащими ключей: монолитный, автономный и цепочка связанных подписей.

При монолитном способе сертификат атрибута является часть сертификата идентификации.

При автономном способе для привязки сертификата атрибута к сертификату идентификации в сертификат атрибута включается некоторая релевантная информация из сертификата идентификации.

При применении цепочки связанных подписей для привязки сертификата атрибута к сертификату идентификации используется подпись центра сертификации, издавшего сертификат идентификации. В стандарте ISO 17090 зафиксирован первый способ.

A.3.1.3 Сертификаты атрибута

A.3.1.3.1 Общие сведения

Привилегии заявителя передаются как атрибуты либо в сертификате открытого ключа (в расширении поля subjectDirectoryAttributes), либо (что чаще) в сертификате атрибута.

Синтаксис сертификата атрибута описан в стандарте X.509:

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo} AttributeCertificateInfo ::= SEQUENCE
{
Version                    AttCertVersion DEFAULT v1,
holder                     Holder,
issuer                     AttCertIssuer,
```

```
signature                   AlgorithmIdentifier,
serialNumber                CertificateSerialNumber,
attrCertValidityPeriod      AttCertValidityPeriod,
attributes                  SEQUENCE OF Attribute,
issuerUniqueID              UniqueIdentifier OPTIONAL,
extensions                  Extensions OPTIONAL
}
AttCertVersion::=           INTEGER {v1(0), v2(1) }
Holder ::=                  SEQUENCE
{
    baseCertificateID       [0] IssuerSerial OPTIONAL,
    -- Издатель и серийный номер сертификата открытого ключа владельца
    entityName              [1] GeneralNames OPTIONAL,
    -- Имя объекта или роли
    objectDigestInfo        [2] ObjectDigestInfo OPTIONAL
    -- Если версия указана, то она должна иметь значение v2
    -- Как минимум, одно из полей baseCertificateID, entityName или objectDigestInfo, должно быть указано--}
    ObjectDigestInfo ::= SEQUENCE
{
digestedObjectType          ENUMERATED {
                                publicKey           (0),
                                publicKeyCert       (1),
                                otherObjectTypes    (2)},
otherObjectTypeID           OBJECT IDENTIFIER OPTIONAL,
digestAlgorithm             AlgorithmIdentifier,
objectDigest                BIT STRING }
AttCertIssuer ::= CHOICE
{
    v1Form GeneralNames,            -- В версии v1 или v2
    v2Form [0] V2Form               -- Только в версии v2
}
V2Form ::= SEQUENCE
{
    issuerName GeneralNames OPTIONAL,
    baseCertificateID       [0]     IssuerSerial OPTIONAL,
    objectDigestInfo        [1]     ObjectDigestInfo OPTIONAL
}
-- Как минимум один из компонентов должен присутствовать
( WITH COMPONENTS { ..., issuerName PRESENT } |
WITH COMPONENTS { ..., baseCertificateID PRESENT } |
WITH COMPONENTS { ..., objectDigestInfo PRESENT } )
IssuerSerial ::= SEQUENCE {
    Issuer              GeneralNames,
    serial              CertificateSerialNumber,
    issuerUID           UniqueIdentifier OPTIONAL }
CertificateSerialNumber ::= INTEGER
UniqueIdentifier ::= BIT STRING
Attribute ::= CLASS
{
    &id                 OBJECT IDENTIFIER UNIQUE,
    &singleValued       BOOLEAN DEFAULT FALSE,
    &Syntax }
Attribute ::= SEQUENCE
{
    attrTypeATTRIBUTE.&id ({SupportedAttrs}),
    attrValues          ATTRIBUTE.&Syntax ({SupportedAttrs} {@attrType}) }
AttCertValidityPeriod ::= SEQUENCE
{
    notBefore GeneralizedTime,
    notAfter GeneralizedTime }
```

Компоненты сертификата атрибута используются следующим образом.

Номер версии позволяет различить разные версии сертификата атрибута. Если поле objectDigestInfo присутствует или издатель идентифицирован с помощью поля baseCertificateID, то версия должна быть v2.

В поле владельца (holder) передается идентификация владельца сертификата атрибута. Настоящий стандарт требует, чтобы использование имени издателя и серийный номер специфичного сертификата открытого ключа были обязательными, использование общих имен — необязательным, а использование дайджеста объекта запрещено. Использование поля GeneralNames самого по себе для идентификации владельца сертификата несет тот риск, что привязки имени к открытому ключу может быть недостаточно для обеспечения выполнения процесса аутентификации идентичности владельца сертификата, связанного с использованием сертификата атрибута. Кроме того, некоторые из необязательных полей элемента GeneralNames (например, сетевой адрес IPAddress) непригодны для использования в наименовании владельца сертификата атрибута, которым чаще является роль, а не конкретный объект. Варианты форм общего имени должны быть ограничены отличительным именем, адресом электронной почты, соответствующим документу RFC 822 (email, см. [48]) и объектными иденификаторами (для имен ролей).

В поле издателя (issuer) передается идентификация органа по присвоению атрибутов, выпустившего данный сертификат. Использование имени издателя и серийного номера специфичного сертификата открытого ключа обязательно, а использование общего имени (имен) необязательно.

В поле signature указывается криптографический алгоритм, использованный дя электронной подписи сертификата атрибута.

В поле serialNumber передается серийный номер, уникально идентифицирующий сертификат атрибута среди тех, за которых несет ответственность его издатель.

В поле attrCertValidityPeriod, имеющем формат GeneralizedTime, передается период времени, в течение которого атрибут сертификата считается действительным.

Поле атрибутов attributes содержит атрибуты, ассоциированные с владельцем сертификата и подлежащие сертификации (например, привилегии).

Поле issuerUniqueID может быть использовано для идентификации издателя атрибута сертификата в случаях, когда имени издателя недостаточно.

Поле расширений extensions field позволяет включать в сертификат атрибута новые поля. Стандартные расширения, описанные в стандарте ISO/IEC 9594-8, рассмотрены в приложении Б

А.3.1.3.2 Конфиденциальность сертификатов атрибута

В некоторых применениях может оказаться желательным защищать содержание сертификатов атрибута от субъектов, отличающихся от владельца сертификата и доверяющей стороны (которая использует сертификат). Это может быть сделано с помощью одного или нескольких сертификатов открытого ключа владельца сертификата атрибута и установления аутентифицированного зашифрованного пути к доверяющей стороне (например, с помощью протокола SSL). Этот путь может затем использоваться для конфиденциальной передачи сертификатов атрибута.

А.3.1.3.3 Пути сертификата атрибута

Как и в случае сертификатов открытого ключа, может предъявляться требование передачи пути сертификата атрибута (например, для объявления привилегий в прикладном протоколе). Следующие типы данных, описанные на языке ASN.1, могут использоваться для представления пути сертификата атрибута:

```
AttributeCertificationPath ::= SEQUENCE
{
    attributeCertificate    AttributeCertificate,
    acPath                  SEQUENCE OF ACPathData OPTIONAL }
ACPathData ::= SEQUENCE
{
certificate                 [0]     Certificate OPTIONAL,
attributeCertificate        [1]     AttributeCertificate OPTIONAL }
```

А.3.1.4 Сертификаты роли

Сертификат атрибута пользователя может содержать ссылку не другой сертификат атрибута, содержащий дополнительные привилегии. Тем самым обеспечивается эффективный механизм реализации привилегированных ролей.

Возможны следующие спецификации:

- любое число ролей может быть определено любым органом по присвоению атрибутов;
- собственно роль и члены роли могут быть определены и управляться отдельно, разными органами по присвоению атрибутов;
- привилегии, назначенные данной роли, могут быть помещены в один или несколько сертификатов атрибута;
- при желании члену роли может быть назначено только подмножество привилегий, ассоциированных с ролью;

- членство в роли может быть делегировано;
- ролям и членству может быть назначено любое требуемое время жизни.

Субъекту присваивается атрибут сертификата, содержащий атрибут, представляющий собой объявление, что субъекту назначена определенная роль. Этот сертификат может иметь расширение, указывающее на другой сертификат атрибута, который определяет эту роль (т. е. этот сертификат роли указывает в качестве владельца роль и содержит список привилегий, присвоенных этой роли). Издатель сертификата субъекта может быть независимым от издателя сертификата роли, и каждый из этих сертификатов может управляться совершенно независимо (например, могут истекать их сроки действия, сертификаты могут отзываться и т.д.).

Не все формы общего имени GeneralName пригодны для использования в качестве имен ролей. Наиболее полезными способами представления имени роли являются объектные идентификаторы и отличительные имена.

A.3.1.5 Удостоверения

Удостоверение является предварительным условием назначения роли или представления на роль. Удостоверения связаны с их средой (локализованы).

Удостоверения обычно ищут по типу (например, врач) или по типу и издателю (например, «врач, имеющий лицензию Вирджинии»).

```
Credential ::= SEQUENCE
{
    credType            OBJECT IDENTIFIER,
    issuer              GeneralName OPTIONAL,
    identifier          UTF8String }
    credentials   ATTRIBUTE ::=
{
    &id           id-credentials,
    &SEQUENCE OF Credential }
```

Если имя издателя удостоверения отсутствует, то используется имя издателя из атрибута, в который вложено удостоверение, или из сертификата открытого ключа. Если отсутствует имя издателя сертификата, то имя издателя удостоверения должно быть указано. (Учтите, что в целях минимизации в системе числа органов по присвоению атрибутов в сертификате может быть явным образом указано более одного удостоверения от более чем одного издателя).

A.3.2 Допуск

Атрибут допуска сопоставляется с меткой безопасности целевого объекта. С его помощью обеспечиваются тонкие механизмы авторизации и контроля доступа.

```
Clearance ::= SEQUENCE
{
    policyId            OBJECT IDENTIFIER,
    classList           ClassList DEFAULT {unclassified},
    securityCategories SET OF SecurityCategory OPTIONAL }
ClassList ::= BIT STRING
{
    unmarked            (0),
    unclassified        (1),
    restricted          (2),
    confidential        (3),
    secret              (4),
    topSecret           (5)}
SECURITY-CATEGORY ::= TYPE-IDENTIFIER
SecurityCategory ::= SEQUENCE
{
    type                [0]     SECURITY-CATEGORY.&id({Categories}),
    value               [1]     SECURITY-CATEGORY.&Syntax({Categories}{@type}) }
```

Идентификатор политики безопасности идентифицирует семантику метки (допустимые грифы секретности и категории безопасности). Идентификатор политики должен быть одним и тем же как у допуска, так и у метки безопасности целевого объекта, чтобы их можно было сравнивать. Поле classList идентифицирует список иерархических грифов секретности. Грифы секретности в допуске сравниваются с грифом секретности целевого объекта; как минимум, один гриф допуска должен быть не ниже грифа секретности целевого объекта. Категории безопасности содержат другую, не иерархическую информацию. Значение категории в допуске должно «доминировать» над соответствующей категорией метки безопасности целевого объекта; значение понятия «доминировать» задается при определении категории. К примеру, в военных применениях метка безопасности может содержать набор кодовых

слов или разделов. Чтобы доминировать над меткой, допуск должен содержать все кодовые слова (разделы) метки (и возможно, дополнительные к ним). Другие сведения о метках безопасности можно найти в разделах А.3.4.3 и А.9.17.

А.3.3 Механизмы заявителя

Текущие подходы к управлению привилегиями пользователя включают в себя следующие варианты:

a) централизованное хранилище привилегий (например, каталог LDAP), из которого они могут быть легко извлечены;

b) хранение привилегий в расширении subjectDirectoryAttributes сертификата открытого ключа пользователя;

c) хранение привилегий в сертификатах атрибута.

Последние два подхода представляют собой механизм хранения привилегии пользователя в удостоверениях, заверенных электронной подписью.

Вариант a) легко реализовать, но при этом сервер привилегий должен быть постоянно доступен. Другие два варианта позволяют передавать информацию об авторизации в сертификатах, что исключает необходимость в оперативном доступе к серверу. Существует несколько причин, почему отдельному органу присвоения атрибутов более предпочтительно помещать привилегии в сертификаты атрибута, а не в сертификаты открытого ключа. К ним относятся:

d) различие в сроках жизни привилегий и открытых ключей;

e) разделение обязанностей (центр сертификации не является субъектом, отвечающим за управление привилегиями);

f) принцип минимально необходимых знаний (не всегда желательно, чтобы каждый субъект знал все привилегии заявителя);

g) принцип наименьших привилегий (для выполнения определенной операции пользователь должен получать или предоставлять минимально необходимые привилегии).

А.3.4 Механизмы чувствительности целевого объекта

А.3.4.1 Общие сведения

Управление атрибутами целевого объекта (например, списками контроля доступа и метками безопасности) традиционно осуществляется в рамках конкретной системы, и представление этой информации мало стандартизовано. Хотя настоящий документ не диктует правила ее представления, в нем приведены рекомендации, основанные на нескольких формах представления (ASN.1 или XML).

А.3.4.2 Инкапсуляция подписанных данных

Атрибуты и другая чувствительная информация могут быть привязаны к дайджесту целевого объекта с помощью конструкции SignedData. В частности, уместно использовать отделенные подписи (передаваемые отдельно от объекта). Чувствительная информация может переноситься в виде подписанных атрибутов, у которых автором будет подписавший субъект.

К целевому объекту могут быть добавлены следующие типы авторизующей информации:

- информация контроля доступа, описанная в стандарте ISO/IEC 10181-3;
- требования равнозначной подписи (см. раздел А.9.19);
- описательные сведения о документе (например, тип документа), приведенные в разделе А.11.3.

А.3.4.3 Метки безопасности

Приведенный далее синтаксис метки безопасности позаимствован из спецификации RFC 2634 [49].

```
ESSSecurityLabel ::= SET
{
    security-policy-identifier SecurityPolicyIdentifier,
    security-classification    SecurityClassification OPTIONAL,
    privacy-mark               ESSPrivacyMark OPTIONAL,
    security-categories        SecurityCategories OPTIONAL }
    id-aa-securityLabel OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-
9(9) smime(16) id-aa(2)}
SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
SecurityClassification ::= INTEGER {
    unmarked                   (0),
    unclassified               (1),
    restricted                 (2),
    confidential               (3),
    secret                     (4),
    top-secret                 (5) } (0..ub-integer-options)
    ub-integer-options INTEGER ::= 256
ESSPrivacyMark ::= CHOICE
{
    pString                    PrintableString SIZE (1..ub-privacy-mark-length),
    utf8String                 UTF8String SIZE (1 ..MAX) }
```

ub-privacy-mark-length INTEGER ::= 128
SecurityCategories ::= SET SIZE (1..ub-security-categories) OF SecurityCategory ub-security-categories INTEGER ::= 64
-- определение класса SecurityCategory см. в разделе А.3.2

Политика безопасности представляет собой комплекс критериев, предъявляемых к предоставлению сервисов безопасности. Поле security-policy-identifier используется для идентификации применяемой политики безопасности, с которой связана данная метка безопасности. Идентификатор политики указывает семантику других компонентов метки безопасности.

Настоящая спецификация описывает использование поля классификации уровней конфиденциальности (грифов секретности) security-classification в точном соответствии со спецификацией RFC 2634 [49] и стандартом ITU-T X.411 [50].

Если это поле присутствует, то классификация уровней конфиденциальности может содержать один из иерархических списков значений. В настоящем документе описана базовая иерархия уровней, но их использование зависит от применяемой политики безопасности. Дополнительные уровни конфиденциальности и их позиции в иерархии могут быть определены в политике безопасности на основе местных правил или двустороннего соглашения. Базовая классификация уровней конфиденциальности содержит в порядке возрастания следующие значения: unmarked (без грифа), unclassified (открытая), restricted (для служебного пользования), confidential (конфиденциальная), secret (секретная), top-secret (совершенно секретная).

Это означает, что в применяемой политике безопасности (идентифицированной в поле security-policy-identifier) определяются целые значения перечислимого типа данных SecurityClassification и их интерпретация. Организация может разработать собственную политику безопасности, определяющую целые значения типа SecurityClassification и их интерпретацию. Однако общее правило состоит в том, что значения с 0 по 5 резервируются для значений «базовой иерархии», а именно unmarked, unclassified, restricted, confidential secret и top-secret.

Правила применения этой «базовой иерархии» уровней конфиденциальности не имеют универсального определения. Каждая организация (или группа организаций) определяет политику безопасности, которая документирует требования к использованию этой «базовой иерархии» (если они должны использоваться) и к проведению контроля доступа в своей зоне безопасности (если таковой проводится). Следовательно, значению уровня конфиденциальности ДОЛЖНО соответствовать значение идентификатора политики security-policy-identifier, определяющей правила использования этого уровня. Например, трактовка уровня «секретная» в организации может отличаться от принятой правительством США. Как правило, политика безопасности НЕ ДОЛЖНА использовать уровни 0—5 со значением уровня конфиденциальности, отличающимся от указанного в стандарте X.411, и вместо этого ДОЛЖНА использовать иные значения, выстроенные в собственную иерархию.

Обратите внимание, что совокупность действительных значений уровней конфиденциальности ДОЛЖНА быть иерархической, но при этом они не обязаны быть упорядочены по возрастанию. Более того, эта совокупность не обязана быть непрерывной. Например, в политике безопасности системы передачи сообщений число 11 может соответствовать уровню конфиденциальности «чувствительная информация без грифа» (sensitive-but-unclassified), а число 5 — уровню «совершенно секретная» (top-secret). Но при этом в иерархии уровней значение top-secret означает более чувствительную информацию, нежели значение sensitive-but-unclassified, хотя целое число, соответствующее значению top-secret, меньше числа, соответствующего значению sensitive-but-unclassified. (Конечно, если значения уровней конфиденциальности security-classification не только образуют иерархию, но при этом обозначены числами, упорядоченными по возрастанию, обычному читателю политики будет легче ее понять.)

Можно привести следующий пример совокупности уровней конфиденциальности в политике безопасности, не использующей никаких значений из стандарта X.411:

10 — общедоступная информация;

15 — общая информация о корпорации Morgan Corporation и ее контрагентах;

20 — информация о служащих корпорации Morgan Corporation;

25 — информация о членах Совета директоров корпорации Morgan Corporation.

Совокупность уровней конфиденциальности в политике безопасности, использующей часть значений из стандарта X.411, может выглядеть следующим образом:

0 — unmarked (без грифа);

1 — unclassified (общедоступная), может читаться всеми;

2 — restricted (предназначена для сотрудников фирмы Timberwolf Productions);

6 — предназначена для руководителей фирмы Timberwolf Productions.

Примером иерархии уровней конфиденциальности могут быть: административная (unclassified), клиническая, чувствительная (информация о ВИЧ или о психическом здоровье). Эти уровни могут быть анонимизированы.

Поле метки конфиденциальности privacy-mark может присутствовать, но оно не используется для контроля доступа. Его содержание может быть определено в применяемой политике доступа (идентифицированной в поле security-policy-identifier), которая может содержать список допустимых значений. В качестве альтернативы это значение может быть задано автором метки безопасности.

В поле категорий безопасности security-categories, если оно присутствует, может передаваться информация, предусматривающая более тонкое описание чувствительности сообщения. В применяемой политике доступа

(идентифицированной в поле security-policy-identifier) может быть указан разрешенный синтаксис представления категорий безопасности. В качестве альтернативы это значение может быть определено в двустороннем соглашении.

У одного и того же объекта может быть несколько меток безопасности с разными схемами проверки, например, требующими наличия всех или только некоторых разрешений (или даже одного разрешения), совпадающих с разрешениями доступа.

А.3.5 Базовая схема контроля доступа

В настоящем подразделе опеределен атрибут информации контроля доступа, который можно использовать для указания получателю (или доверенной третьей стороне), какие субъекты могут читать содержание целевого объекта.

```
ACCESS-CONTROL-SCHEME ::= TYPE-IDENTIFIER
AccessControlScheme ::= INSTANCE OF ACCESS-CONTROL-SCHEME
astmScheme ACCESS-CONTROL-SCHEME ::= {ASTMScheme IDENTIFIED BY id-astmScheme}
ASTMScheme ::= SEQUENCE OF ASTMEntry
ASTMEntry ::= SEQUENCE
{
    who                 Requester,
    constraints         Constraints OPTIONAL }
Requester ::= CHOICE
{
    role                [0]     OBJECT IDENTIFIER,
    individual          [1]     GeneralName,    -- from X9.55
    group               [2]     GeneralName,
    organizationalUnit  [3]     GeneralName}
Constraints ::= SEQUENCE OF Constraint
CONSTRAINT ::= TYPE-IDENTIFIER
Constraint ::= INSTANCE OF CONSTRAINT
caseID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-caseID }
encounterID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-encounterID }
claimEventID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-claimEventID }
planRegistration CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-planRegistration }
encounterRegistration       CONSTRAINT ::=
{OCTET STRING IDENTIFIED BY id-encounterRegistration}
admission CONSTRAINT ::= {OCTET STRING IDENTIFIED BY id-admission}
diagnosis CONSTRAINT ::= { Code IDENTIFIED BY id-code }
disease CONSTRAINT ::= { Code IDENTIFIED BY id-disease }
disorder CONSTRAINT ::= { Code IDENTIFIED BY id-disorder }
department CONSTRAINT ::= { GeneralName IDENTIFIED BY id-department }
testID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-testID }
resultID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-resultID }
procedureID CONSTRAINT ::= { OCTET STRING IDENTIFIED BY id-procedureID }
specimenType CONSTRAINT ::= { Code IDENTIFIED BY id-specimenType }
shift CONSTRAINT ::= { INTEGER IDENTIFIED BY id-shift }
workgroup CONSTRAINT ::= { GeneralName IDENTIFIED BY id-workgroup }
training CONSTRAINT ::= { BOOLEAN IDENTIFIED BY id-disorder }
therapeuticAgent CONSTRAINT ::= { Code IDENTIFIED BY id-therapeuticAgent }
diagnosticAgent CONSTRAINT ::= { Code IDENTIFIED BY id-diagnosticAgent }
disidentified CONSTRAINT ::= { BOOLEAN IDENTIFIED BY id-disidentified }
Code ::= SEQUENCE
{
    codeSet             PrintableString,
    codeValue           IA5String }
```

Доступ к целевому объекту разрешен, если для запрашивающей стороны найдена запись в списке субъектов Who (по имени, роли, группе или структурной единице организации) и если атрибут сертификата запрашивающей стороны удовлетворяет всем ограничениям, указанным в атрибуте информации контроля доступа целевого объекта. Эти ограничения должны содержаться в атрибуте ограничений сертификата запрашивающей стороны. У этого атрибута есть синтаксические ограничения.

А.4 Описание сервисов инфраструктуры управления привилегиями на языке XML

А.4.1 Описание назначения ролей на языке XACML

Консорциум по разработке стандартов OASIS разработал язык XACML для описания сущностей, связанных с принятием решений о контроле доступа. Техническая спецификация на языке XACML содержит профиль ролевого контроля доступа, соответствующий стандарту ANSI RBAC.

Для удобства чтения в таблице А.1 сопоставлены термины, используемые в базовой спецификации RBAC Национального института стандартов США NIST [14], с терминами, используемыми в профиле XACML, и с терминами, используемыми в настоящем документе.

Таблица А.1 — Отображение терминов, используемых в базовой спецификации RBAC

Базовая спецификация RBAC	Профиль XACML	Инфраструктура управления привилегиями ASTM PMI
Пользователи (Users)	Субъекты (XACML Subjects)	Заявители (Claimants)
Роли (Roles)	Атрибуты субъектов (XACML Subject Attributes)	Роли (Roles)
Объекты (Objects)	Ресурсы (XACML Resources)	Объекты (Objects)
Операции (Operations)	Действия (XACML Actions)	Операции (Operations)
Разрешения (Permissions)	Роли <PolicySet> и разрешения <PolicySet> (XACML Role <PolicySet> and Permission <PolicySet>	Разрешения (Permissions)

Профиль XACML RBAC поддерживает также иерархический ролевой контроль доступа, позволяя описывать наследование свойств ролей. Для поддержки системных функций и функций пересмотра, описанных в стандарте ANSI RBAC, в этом профиле описаны дополнительные политики, и именно, роль RPS (Role PolicySet) ассоциирует владельца данного атрибута роли с набором разрешений PPS (Permission PolicySet), который описывает разрешения, назначенные данной роли. Объекты RPS и PPS эквивалентны сертификатам атрибута назначения роли и сертификатам атрибута спецификации роли в ролевой модели, основанной на стандарте X.509.

Интегрированное описание свойств ролевой инфраструктуры управления привилегиями на языке XACML предоставляет богатые и расширяемые средства описания политик. Понятия структурных и функциональных ролей обеспечиваются с помощью двухслойной системы, охватывающей атрибуты ролей, и именно, пользователи могут иметь роли, назначенные им в контексте запроса. Компонент, отделенный от точки принятия решений, может использовать политику назначения ролей XACML или PolicySet, чтобы активировать атрибуты в сеансе пользователя.

А.4.2 Другие сервисы инфраструктуры управления привилегиями

В А.5 приведены примеры других сервисов инфраструктуры управления привилегиями, описанных на языке XML.

А.5 Примеры управления привилегиями, сценариев контроля доступа и сервисов

А.5.1 Назначение привилегий на основе структуры организации

Когда привилегии назначаются на основе структуры организации, то структурные роли, определенные в соответствии со стандартом ISO/TS 21298, отражают отношения между физическим лицом и структурной единицей, включающие в себя назначение привилегий. В этом случае привилегия основана на принадлежности к организации. Этот подход распространяется не только на лица, но и на такие типы субъектов как системы, компоненты, устройства. Назначенные привилегии могут использоваться как внутри данной организации, так и во внешних организациях (например, принадлежность к уполномоченным органам).

А.5.2 Назначение привилегий на основе рабочих процессов

Чтобы обеспечить реализацию процесса, привилегии могут назначаться на его выполнение. Привилегии могут быть назначены на выполнение всего процесса, определенных действий или даже определенных транзакций. Этот подход состоит в назначении привилегий в соответствии с функциональной ролью субъекта, следуя стандарту ISO/TS 21298. Он отражает связь между отдельным субъектом и действием.

А.5.3 Управление привилегиями на основе политик

Привилегии могут назначаться в соответствии с ограничениями на время, условия среды, функции, операции, установленные законодательством, нормативными актами, спецификациями и т.д.

А.5.4 Назначение роли и разрешений

Ограничения, задающие привилегии и обязанности, обычно указаны в политиках. В случае простых политик и взаимосвязей привилегии и обязанности могут быть преобразованы в роли, как это делается в простых реализациях ролевого контроля доступа, например, в стандарте HL7 RBAC [15]. Недостаток такого упрощенного подхода состоит в том, что число создаваемых ролей растет при появлении новых политик. Кроме того, такие существенные аспекты как контекст доступа и другие переменные (см. стандарт ISO/TS 22600-2) не могут быть подходящим образом рассмотрены. Дополнительные сведения см. в стандарте ISO/TS 21298.

А.5.5 Спецификация авторизации

Орган по присвоению атрибутов (ОА) и центр сертификации (ЦС) логически (и во многих случаях физически) совершенно независимы. Создание и эксплуатация «идентичности» могут (и часто должны) быть отдельными от инфраструктуры управления привилегиями. Таким образом, вся инфраструктура открытых ключей, включая ЦС, могут существовать и действовать до создания инфраструктуры управления привилегиями. Хотя ЦС и является уполномоченным органом идентификации в своей зоне безопасности, он автоматически не становится уполномоченным органов по присвоению привилегий. Следовательно, ЦС не обязательно выполняет функции ОА. Отсюда можно сделать вывод, что ЦС не обязан нести ответственность за решение, что другие субъекты могут функционировать в качестве ОА (например, не обязан включать такое назначение в их сертификаты идентификации).

Источником полномочий является субъект, которому контролер привилегий доверяет как органу, всецело отвечающему за назначение комплекса привилегий. Ресурс может ограничить сферу ответственности источника полномочий, доверяя определенным источникам разные функции (например, один источник отвечает за назначение привилегий чтения, а другой — привилегий записи). Любой источник полномочий в то же время является ОА, поскольку он выпускает для других субъектов сертификаты, идентифицирующие привилегии, назначенные этим субъектам. Источник полномочий аналогичен «корневому» ЦС или «доверенной привязке» в инфраструктуре открытых ключей в том отношении, что контролер привилегий доверяет сертификатам, выпущенным источником полномочий. В некоторых реализациях необходимы ЦС, тщательно контролирующие субъектов, действующих как источники полномочий. В настоящем приложении предусмотрен механизм обеспечения такого требования. В других реализациях такой контроль не является необходимым, и механизмы удостоверения того, что субъект может выступать в качестве источника полномочий, могут оказаться вне рамок данной части настоящего стандарта.

Предложения, сформулированные в настоящем приложении, являются гибкими и могут удовлетворить требования, предъявляемые во многих реализациях.

Если сертификаты атрибута содержат ссылки на сертификаты открытого ключа, выпущенные для их издателей и владельцев, то для аутентификации владельцев (заявителей привилегий) и проверки электронных подписей издателей может использоваться инфраструктура открытого ключа.

А.5.6 Описание стратегий управления привилегиями с помощью сертификатов

А.5.6.1 Указание привилегий в сертификатах атрибута

Субъекты могут получить привилегии двумя способами:

- орган по присвоению атрибутов может назначить субъекту привилегии с помощью выпуска сертификата (может быть полностью по своей инициативе или с помощью запроса к некоторой третьей стороне). Сертификат может храниться в общедоступном хранилище и может затем обрабатываться одним или несколькими контролерами привилегий для принятия решения об авторизации. При этом субъект, получающий полномочия, может оставаться в неведении о назначении полномочий либо получать уведомление об этом факте;
- субъект может направить в ОА запрос на получение привилегий. Будучи созданным, сертификат может быть возвращен (только) запросившей стороне, которая явным образом включает его в запрос доступа к некоторому защищенному ресурсу.

Обратите внимание, что в обоих вариантах для выполнения своей обязанности ОА должен удостовериться, что субъекту действительно должна быть назначена данная привилегия. Этот процесс может включать в себя некоторые сторонние механизмы, аналогичные сертификации пары идентификация/ключ, создаваемой ЦС.

Управление привилегиями с помощью сертификатов атрибута применимо в тех случаях, когда выполняется одно из следующих условий:

- за выпуск сертификата открытого ключа для определенного владельца привилегии отвечает один субъект, а за назначение конкретной привилегии — другой;
- владельцу назначается несколько атрибутов привилегий более чем одним органом;
- срок жизни привилегии отличается от срока действия сертификата открытого ключа владельца привилегии (обычно срок жизни привилегии гораздо короче);
- привилегия действительна только в течение определенных периодов времени, асинхронных по отношению к сроку действия открытого ключа пользователя или к сроку жизни других его привилегий.

А.5.6.2 Указание привилегий в сертификатах открытого ключа

В некоторых реализациях назначение субъекту привилегий осуществляет ЦС. Такие привилегии могут быть указаны непосредственно в сертификатах открытого ключа (подобный подход обеспечивает повторное использование уже развернутой инфраструктуры) вместо выпуска сертификатов атрибута. В этих случаях привилегии должны быть указаны в поле расширения сертификата открытого ключа subjectDirectoryAttributes.

Этот способ применим в тех случаях, когда выполняется одно из следующих условий:

- один и тот же физический субъект действует и как ЦС, и как ОА;
- срок жизни привилегии и срок действия открытого ключа, содержащегося в сертификате, одинаковы;
- делегирование привилегий не разрешено;
- делегирование привилегий разрешено, но при каждом делегировании все привилегии, указанные в сертификате (в поле расширения subjectDirectoryAttributes), имеют одинаковые параметры делегирования и все расширения, релевантные делегированию, применяются к этим привилегиям одинаковым образом.

А.5.7 Инфраструктура управления привилегиями

Объект может быть защищаемым ресурсом, например, для приложения, контролирующего доступ. Защищаемый ресурс можно рассматривать как объект. У объектов этого типа есть методы, которые могут быть вызваны (например, объект представляет собой межсетевой экран, имеющий метод «разрешить вход», или файл в файловой системе, имеющий методы «читать», «записать» или «выполнить»). Другим примером моделируемого объекта может служить объект, подписанный приложением, отвечающим за неоспоримость.

Заявителем привилегии является субъект, который обладает конкретной привилегией и заявляет свои привилегии в конкретном контексте использования.

Контролером привилегии является субъект, определяющий, достаточны ли заявленные привилегии для данного контекста использования.

Вследствие обязанности определения достаточности привилегий контролер зависит от следующих четырех объектов:

- привилегия заявителя;
- применяемая политика привилегий;
- текущие значения переменных среды, относящихся к запросу;
- чувствительность релевантных методов объекта.

Привилегия, имеющаяся у ее владельца, отражает степень доверия, оказанного этому владельцу издателем сертификата в том, что владелец будет следовать тем требованиям политики, которые не могут быть проверены техническими средствами. Эта привилегия инкапсулируется в сертификат(ы) атрибута, выпущенные для владельца, либо в поле расширения subjectDirectoryAttributes его сертификата открытого ключа, которые могут быть предоставлены контролеру привилегий при вызове метода объекта, или могут распространяться другими средствами, например, с помощью каталога. Кодирование привилегии осуществляется с помощью конструкции Attribute, содержащейся в объекте AttributeType или во множестве SET OF AttributeValue. Некоторые типы атрибутов, используемых для указания привилегии, могут иметь очень простой синтаксис, например, могут быть представлены отдельным целым числом типа INTEGER или строкой байтов типа OCTET STRING. Синтаксис других типов привилегий может быть более сложным. Пример приведен в приложении Г.

Политика привилегий описывает уровень привилегии, который считается достаточным для вызова метода объекта, имеющего данную чувствительность, или для данного контекста использования. Целостность и аутентичность политики привилегий должны быть защищены. Существуют разные возможности передачи политики. Одна крайность состоит в том, что на самом деле политика не передается, а хранится в среде контролера привилегий. Другая крайность состоит в том, что некоторые политики «универсальны» и должны передаваться или быть известными всем субъектам системы. Между этими крайностями существует много вариантов. Схема компонентов, предназначенных для хранения информации политики привилегий, описана в настоящем приложении.

Политика привилегий описывает порог приемлемости данного комплекса привилегий. В ней точно указано, в каких случаях контролер привилегий должен принимать решение, что комплекс привилегий, представленный ему в запросе, «достаточен» для представления заявителю права доступа (к требуемому объекту, ресурсу, приложению и т. д.).

Синтаксис описания политик привилегий в настоящем приложении не специфицирован. Приложение Г содержит пару примеров синтаксиса, который может использоваться для этой цели. Однако это только примеры. Для описания политик может использоваться любой синтаксис, в том числе обычный текст. Независимо от синтаксиса, используемого для описания политики привилегий, каждый экземпляр политики должен иметь уникальный идентификатор. Для этого используются объектные идентификаторы:

PrivilegePolicy ::= OBJECT IDENTIFIER

В релевантных переменных среды хранятся те параметры политики, которые с помощью некоторых местных средств доступны контролеру привилегий и которые необходимы для принятия им решения о разрешении вызова (например, время дня или текущий баланс счета). Способ представления переменных среды оставляется на местное усмотрение.

Чувствительность метода объекта, если таковая используется, может отражать атрибуты документа или запроса на обработку, например, сумма платежного поручения, которое требуется авторизовать, или уровень конфиденциальности содержания документа. Чувствительность метода объекта может быть явно закодирована в метке безопасности этого объекта или инкапсулирована в структуре и содержании этого объекта данных. Кодирование чувствительности может быть выполнено разными способами. Например, код чувствительности может передаваться вне информации управления привилегиями, скажем, в метке, привязанной к документу и соответствующей стандарту X.411, в полях сообщения по стандарту EDIFACT или даже содержаться в программном коде контролера привилегий. Код чувствительности может передаваться и в составе информации управления привилегиями, в сертификате атрибута, связанном с данным методом объекта. В других вариантах используемого контекста чувствительность метода объекта может вообще не использоваться.

В существовании связи между контролером привилегий и конкретным ОА нет никакой необходимости. Подобно тому как владелец привилегий может иметь сертификаты атрибута, выпущенные многими разными ОА, контролеры привилегий могут для принятия решения о предоставлении доступа к конкретному ресурсу принимать сертификаты, выпущенные различными ОА, между которыми не обязательно будут иерархические связи.

Управление привилегиями с помощью сертификатов может использоваться для управления различными типами привилегий и для различных целей. Термины, используемые в настоящем документе, например, заявитель привилегий, контролер привилегий и т.д., не зависят от конкретного приложения или применения.

А.5.8 Ограничения разрешений

Ограничения разрешений формулируются в процесс конструирования ролей. Примером ограничения разрешений служит правило, по которому только одной роли разрешается выполнять определенное действие в каждый момент времени. Другим примером может служить ограничение кратности. В этом случае оно формулируется в форме указания кратности.

Примерами ограничений разрешений служат:

- роль главной медицинской сестры больницы (кратность 1 для больницы);
- роль заведующего отделением (кратность 1 для отделения);
- роль исполнителя лабораторных анализов и дежурного врача-лаборанта (запрет на совмещение обязанностей);
- дистанционный доступ врача к информационной системе больницы, которая не является его местом основной работы (ограничение местонахождения);
- доступ в зависимости от смены (ограничение на время доступа).

Приведенное обсуждение опирается на предположение, что имя функциональной роли является случайным и служит только идентификатором совокупности разрешений, соответствующих стандарту ANSI INCITS. Далее, описания ролей обязательно специфичны для организации, в которой они созданы, и, следовательно, сами по себе не предполагают какой-либо иной интероперабельности с деловыми партнерами, нежели та, что описана в деловых соглашениях с ними. Для достижения полной интероперабельности организациям требуются стандартизация разрешений доступа в здравоохранении и средства назначения и объявления стандартных привилегий.

А.5.9 Отделение функций безопасности от логики бизнес-процессов

При конструировании базовой инфраструктуры управления привилегиями необходимо проводить различия между применением политики безопасности и логики бизнес-процессов. Насаждение этой логики инфраструктуре управления привилегиями может привести к ослаблению безопасности системы и к ухудшению архитектуры и не обеспечивает выделения точно описанных ролей безопасности. Поэтому по возможности необходимо отделять и изолировать программный код приложений безопасности и приложений логики бизнес-процессов. Такое отделение существенно помогает разработчикам системы безопасности определять периметры безопасности, гарантировать, что изменения в логике бизнес-процессов не воздействуют на программный код приложений безопасности, и сертифицировать безопасность системы.

Отделение функций безопасности от логики бизнес-процессов может оказаться затруднительным. В общем случае доступ к ресурсу в рамках логики бизнес-процесса организован в виде взаимодействия с совокупностью ресурсов, к которым пользователю разрешен доступ. Логика функций безопасности может быть идентифицирована с помощью описанных далее критериев.

Целесообразно рассмотреть следующие факторы:

- изменение категории конфиденциальности (например, преобразование конфиденциальной информации в неконфиденциальную),
- необходимые уровни конфиденциальности, целостности и доступности данных;
- применение принципов минимально необходимых привилегий, необходимости знания информации для выполнения служебных обязанностей, запретов совмещения обязанностей;
- нормативные акты и организационно-распорядительные документы, регулирующие вопросы безопасности.

А.5.10 Руководство по использованию точки применения политик

Архитектура инфраструктуры управления привилегиями может повлиять на место размещения точки применения политик. В распределенной инфраструктуре управления привилегиями точка применения политик может быть размещена на уровне приложений или на корпоративном уровне. При принятии решения о размещении важно учесть следующие факторы:

- доступность точки применения политик;
- сокращение числа точек применения политик;
- возможность централизованного управления;
- сопровождение точки применения политик в течение ее жизненного цикла;
- физическая безопасность точки применения политик;
- необходимость сетевого доступ к точке применения политик;
- максимально возможная близость точки применения политик к приложению.

Совмещение места размещения точки применения политик с приложениями снижает время реакции. В этом случае должно быть использовано местное хранилище политик, позволяющее использовать политики в отсутствие доступа к внешним сетям.

А.6 Сравнение сервисов на базе каталога LDAP и сервисов обработки политик

А.6.1 Общие сведения

Выбор механизмов обработки заявлений может влиять на производительность и сложность базовой инфраструктуры управления привилегиями. Механизмы на базе каталога LDAP обычно обеспечивают хорошее время

реакции, но при этом оперируют простыми данными, позволяя, к примеру, определить, является ли заявитель членом определенной роли. В отличие от них сервисы обработки политик позволяют включить в процесс принятия решения об авторизации несколько независимых элементов. Обсуждение этих вариантов приведено в А.6.2 — А.6.4.

А.6.2 Сервисы на базе каталога LDAP

Использование сервиса на базе каталога LDAP целесообразно в том случае, если требуется быстрая реакция и решение об авторизации может быть основано на факте обладания определенной роли, в первую очередь структурной.

При принятии решения об использовании такого сервиса необходимо учитывать следующее:

- извлекаемые из каталога данные состоят из простых строк;
- требуемая дополнительная обработка обладает определенной чувствительностью;
- необходимо документировать интерфейс;
- обработка политик не требуется.

А.6.3 Сервисы обработки политик

Применение сервисов обработки политик обеспечивает гибкие возможности, но при их реализации с помощью аппаратно-программных средств общего назначения скорость обработки запросов оказывается ниже, нежели в случае применения сервисов на базе каталога LDAP. При реализации с помощью специальных аппаратно-программных средств сервисы обработки политик более эффективны по сравнению с LDAP при обработке сложных правил и ограничений, а также при комбинировании правил, предоставляемых несколькими точками информации о политиках. Учтите, что кэширование решений (на время срока их действия), принимаемых сервисом обработки политик, с использованием для поиска в кэше свертки атрибутов запроса может значительно повысить производительность в ситуации, когда в течение данного периода делается много актов доступа и значительная их часть использует одинаковые атрибуты запроса на доступ.

При принятии решения об использовании такого сервиса необходимо учитывать следующее:

- извлекаемые данные состоят из комплексных или кратных элементов;
- требуется обработка кратных элементов;
- необходима поддержка сложных языков описания политик (например, языка XACML);
- пониженная скорость реакции сервиса допустима.

Если необходима быстрая реакция и решение об авторизации может быть принято на основе обладания определенной ролью, в первую очередь структурной, то следует рассмотреть возможность использования сервиса на базе каталога LDAP.

Сервисы обработки политик пригодны для ситуаций, когда принятие решения основано на участии в рабочем процессе, особенно на обладании функциональными ролями (см. А.11.1). В базовой инфраструктуре управления привилегиями может использоваться сочетание сервиса на базе каталога LDAP и сервисов обработки политик [16].

А.6.4 Точки принятия решений о политике

Точки принятия решений о политике могут быть реализованы многими способами в зависимости от использованной модели инфраструктуры (см. профиль SAML 2.0 для утверждений на языке XACML). Они отвечают за принятие решения, может ли запрос контроля доступа быть удовлетворен или должен быть отвергнут. Решение должно быть основано на политиках, которые точка принятия решений о политике может получить от одного или нескольких хранилищ политик. При принятия решения может использоваться также дополнительная информация контроля доступа. Принятое решение возвращается заявителю непосредственно через точку применения политик или через промежуточное программное обеспечение, например, обработчик контекста.

При реализации точки принятия решений о политике необходимо учитывать следующее:

- точка должна размещаться таким образом, чтобы ею можно было централизованно управлять;
- для описания передаваемых запросов контроля доступа и решений о доступе используйте язык XACML;
- обеспечьте безопасность точки принятия решений о политике и коммуникаций между процессами;
- рассмотрите варианты размещения точки в приложении (местное принятие решений), в сети (централизованное принятие решений) или смешанный вариант;
- рассмотрите способы гарантирования выполнения решений, переданных точке применения политик;
- для улучшения производительности точки принятия решений о политике используйте аппаратные ускорители.

Существует большое число архитектурных решений, повышающих безопасность и гибкость инфраструктуры, основанной на применении точек принятия решений о политиках [17].

А.7 Системы управления идентификацией

Для некоторых функциональных областей инфраструктуры управления привилегиями необходима защищенная подсистема управления идентификацией IdM (identity management subsystem), отвечающая за безопасное предоставление идентифицирующей информации и функций управления идентификацией. К этим функциям относятся:

- административные функции (регистрация пользователей, управление паролями);
- функции контроля идентифицирующих данных (метаданные, содержание данных);
- функции доступа (запросы аутентификации, конфиденциальность);

- управление жизненным циклом (настройка, применение обновлений, аварийное восстановление);
- функции резервного копирования, аудита, ведения журналов, выдачи отчетов.

В подсистеме управления идентификацией должны быть обеспечены защищенные механизмы запросов и передачи идентифицирующей информации, обычно с использованием взаимной аутентификации. Доступ к этой подсистеме надо рассматривать как сервис, доступный во всей организации. Такая подсистема может быть развернута в организации различными способами:

- как авторитарный источник, интегрированный в базовую инфраструктуру управления привилегиями;
- как административная функция, доступная этой инфраструктуре по мере необходимости;
- как отдельное специализированное решение.

Реализация подсистемы управления идентификацией в виде сервиса имеет определенные преимущества по сравнению с реализацией в виде местного специализированного приложения. По своей природе сервисы предлагают сетевые интерфейсы, использующие стандартные протоколы, что обеспечивает больше гибкости при изменениях архитектуры организации. Сервис управления идентификацией может управляться централизованно, что позволяет обеспечить согласованное применение политик безопасности и политик деловых процессов.

А.8 Аудит

Основным назначением подсистемы аудита является обеспечение учета действий, совершаемых агентами вычислительной сети. Аудит не является инструментом использования привилегий для разрешения доступа или отказа в доступе к защищаемому ресурсу. Однако подсистема аудита должна взаимодействовать с инфраструктурой управления привилегиями, с тем чтобы можно было проверить правильность ее функционирования. Обсуждение использования аудита в информационных системах здравоохранения см. в документе RFC 3881 [51].

Аудит обеспечивает поддержку сервис-ориентированной архитектуры и сервисов аутентификации и авторизации.

Понятие учетности (accountability) означает, что отдельные лица или субъекты могут быть ответственными за выполнение определенных действий, например за получение информированного согласия или за нарушение конфиденциальности [18]. Учетность обеспечивается с помощью реализации всеобъемлющего технического сервиса аудита. Аудит обеспечивает регистрацию таких записей о потенциальных нарушениях безопасности, которые позволяют неопровержимо отследить инициатора действия. Аудит безопасности не только обеспечивает учетность, но также и позволяет оценить ущерб, нанесенный системе умышленным действием или инцидентом. Аудит безопасности, генерируемый действиями других служб безопасности, позволяет проверить правильность их работы. В распределенной системе централизованный сбор информации аудита и ее централизованная обработка являются способом обнаружения неправильного использования системы и выдачи тревожных сигналов почти в режиме реального времени. Чтобы быть эффективным, аудит должен быть всегда включен.

В журнале аудита регистрируются события, имеющие отношение к безопасности и собираемые в целях потенциального обнаружения вторжения, или для аудита безопасности, или для того и для другого. Аудит является всеобъемлющей функцией информационной системы здравоохранения, обеспечивающей существенные возможности учетности. Кроме того, аудит обеспечивает проверку правильности системных функций безопасности с помощью мониторинга доступа пользователей и системы к данным и ресурсам. Журнал аудита генерируется как побочный продукт деятельности сервисов безопасности, например, в нем регистрируются действия аутентификации, доступа и авторизации (предоставления привилегий), а также информация о других событиях, имеющих отношение к безопасности (например, изменение файла). Аудит используется как средство предохранения от (неавторизованных) действий пользователей, которые должны знать, что их действия регистрируются (обычно такая информация выводится на экранную форму входа в систему). С помощью анализа журнала аудита можно оценить степень ущерба, нанесенного действия злоумышленника.

В системе с распределенной архитектурой, содержащей различные коммерческие готовые компоненты (commercial off-the-shelf products — COTS), каждый из этих компонентов ведет отдельный журнал аудита в собственном формате. Даже типы регистрируемых событий могут отличаться от одного компонента к другому (например, событие «предоставить права доступа» (grant) может иметь смысл в системе управления базами данных, но не в операционной системе). Системные журналы аудита могут содержать строчные или двоичные записи. Для просмотра и обработки журналов аудита, которые ведутся коммерческими готовыми компонентами, нередко требуются специальные программные утилиты. Журналы аудита могут храниться в файловой системе, в таблицах базы данных и т. д. В системах анализа журналов аудита эти различия должны учитываться и нивелироваться.

В распределенных системах аудит ведется в разных местах и разными компонентами, что затрудняет просмотр и анализ журналов аудита. В таких системах, конечно, крайне желательно консолидировать данные, регистрируемые в журналах аудита, и переправлять их в центральный сервер аудита, где они могут быть приведены к общему формату и автоматически обработаны с помощью соответствующей утилиты. Доступны несколько таких коммерческих готовых программ, рассчитанных на сбор, передачу, обработку и выдачу отчетов о событиях аудита, которые регистрируются в распределенной системе и исходят из разных источников. Поскольку размеры журналов аудита могут быть значительными, единый центральный сервер аудита является практичным решением управления сбором данных аудита, не ухудшающим время реакции операционных систем. Обработка данных аудита может осуществляться как в пакетном режиме, так и в режиме реального времени.

Автоматизированные инструменты аудита предоставляют возможности идентификации событий разных уровней безопасности, выполнения автоматического профилирования, выдачи отчетов и тревожных сигналов, а также хранения, сортировки и поиска потенциальных нарушений безопасности. С помощью автоматизированных средств можно управлять сбором журналов аудита в централизованных и распределенных системах. Должно выбираться такое размещение инструментов аудита, агентов и компонентов (включая средства мониторинга сети в режиме реального времени и обнаружения вторжений), которое обеспечит максимальную эффективность системы аудита.

Окончательные правила применения стандартов безопасности и электронной подписи, утвержденные Министерством здравоохранения и социального обеспечения США (Department of Health and Human Services — DHHS), содержат требования к аудиту, включая выдачу тревожных сигналов и отчетов о событиях (раздел 45 CFR, части 160, 162 и 164).

Программные средства, разработанные или предназначенные для использования Управлением по вопросам здравоохранения ветеранов (Veterans' Health Administration), должны либо включать в себя средства аудита, либо интегрироваться с существующими системами аудита.

Предварительно настроенные отчеты готовятся на основе выбранных критериев документирования критичных событий безопасности и предоставления сводной информации, графиков и статистики активности системной безопасности. Записи журналов аудита могут храниться в файле или в базе данных. Чтобы регистрировать записи о событиях, инициируемых всеми пользователями, в настройках системы аудита должна иметься возможность указать признак «все пользователи».

Для получения аудиторской информации анализируются записи журналов аудита. Консолидация журналов аудита, когда на центральном «сервере аудита» собираются записи из разных журналов, облегчает анализ, осуществляемый с помощью автоматизированных средств обработки (как правило) больших объемов информации о регистрируемых событиях. Непрерывный мониторинг записей журналов должен быть неотъемлемой частью эксплуатационной фазы жизненного цикла разработки системы [19].

Архитектура безопасности должна обеспечивать поддержку развертывания средств аудита на уровне приложения, учреждения или на уровне страны. Для выполнения требования длительного хранения аудиторской информации необходимо использовать долговременные системы хранения и архивирования данных. Это требование устанавливает минимальный срок хранения (пять лет). Организации должны определять политики и процедуры для управления ведением журналов, совместимым с принятыми стандартами [20].

Согласие пациента может считаться одним из событий, требующих аудита. Поскольку необходимо регистрировать раскрытие информации о пациенте, то в настройках системы аудита это событие должно быть указано как «обязательное». Архитектура безопасности обеспечивает централизованный сбор и обработку сведений о раскрытии этой информации и выдачу необходимых отчетов. В соответствии с законодательством о персональных данных для хранения сведений о подобном раскрытии информации может быть установлен более длительный срок, нежели для хранения сведений о простых событиях безопасности.

Системы обнаружения вторжений должны быть неотъемлемой частью распределенной архитектуры. Коммерчески доступные системы обнаружения вторжений предоставляют возможности быстрой подачи тревожных сигналов, уведомляющих об определенных вторжениях. Вторжения можно подразделить на два основных класса: несанкционированные и аномальные. К несанкционированным вторжениям относятся организованные атаки на известные слабые места системы. Они могут быть обнаружены путем наблюдения за определенными действиями, выполняемыми над определенными объектами. Аномальные вторжения вызывают отклонения от нормального режима работы системы. Их можно обнаружить с помощью построения профиля работы мониторируемой системы и регистрации значительных отклонений от этого профиля.

Применение промышленных стандартов позволяет создавать качественные подсистемы аудита. Промышленные группы по разработке профилей стандартов, например Integrating the Healthcare Enterprise (IHE), публикуют профили, которые описывают применение уже разработанных стандартов для улучшения совместного использования медицинской информации при лечении пациентов. Организация IHE опубликовала несколько интеграционных профилей, предназначенных для обеспечения безопасности и конфиденциальности, в том числе ATNA (Audit Trail and Node Authentication — Журнал аудита и аутентификация узла), BPPC (Basic Patient Privacy Consents — базовое информированное согласие пациента), ВЫП (Document Digital Signature — электронная подпись документа), EUA (Enterprise User Authentication — корпоративная аутентификация пользователей) и XUA (Cross-enterprise User Assertion — передача объявлений идентичности пользователей между зонами безопасности). Эти интеграционные профили описывают меры безопасности, которые в сочетании с политиками и процедурами безопасности позволяют обеспечить конфиденциальность информации о пациентах, целостность данных и учетность [21]. В профиле IHE ATNA описано ведение журнала аудита безопасности, совместимого с дополнением 95 к стандарту DICOM «Сообщения журнала аудита» (DICOM Supplement 95: Audit Trail Messages, [22]).

А.9 Дополнительные сервисы инфраструктуры управления привилегиями

А.9.1 Размещение сервисов аудита

Сервисы аудита размещаются на конечных системах: рабочих станциях, информационных серверах, шлюзовых и транслирующих системах, включая серверы безопасности (контроллеры доменов, прокси-серверы и т. д.). Сервис аудита, размещенный на сервере, обеспечивает регистрацию активности по обработке данных. Сетевой

сервис аудита, размещенный, к примеру, в шлюзе, регистрирует информацию о получаемых сетевых пакетах. Вместе с сервисом аудита могут размещаться средства управления безопасностью, обеспечивающие настройку и обработку журналов аудита и выдачу необходимых отчетов. Эти средства могут также предоставлять базовые данные, предназначенные для обработки системой обнаружения вторжений.

А.9.2 Обнаружение вторжений

Вторжения можно подразделить на два основных класса: несанкционированные и аномальные. К несанкционированным вторжениям относятся организованные атаки на известные слабые места системы, которые могут быть обнаружены путем наблюдения за определенными действиями, выполняемыми над определенными объектами. Аномальные вторжения вызывают отклонения от нормального режима работы системы. Их можно обнаружить с помощью построения профиля работы мониторируемой системы и регистрации значительных отклонений от этого профиля.

Система обнаружения вторжений (Intrusion Detection System — IDS) может также выполнять собственный мониторинг и сохранять агрегированную статистику, характеризующую профиль использования системы. Данные этой статистики могут быть собраны из разных характеристик работы системы, например, использование процессора, интенсивность обменов с диском, использование памяти, активность пользователей, число попыток входа в систему и т.д. Эта статистика должна постоянно обновляться и отражать текущее состояние работы системы. С помощью сопоставления указанной статистики с внутренней моделью система обнаружения вторжений способна определять, можно ли рассматривать ряд действий как попытку вторжения в систему. Модель может описывать ряд сценариев вторжения и может также кодировать профиль невозмущенной системы.

Серверная система обнаружения вторжений представляет собой программное обеспечение, которое выполняет мониторинг системных или прикладных журналов. При обнаружении попыток пользователя получить неавторизованный доступ к данным, файлам или сервисам оно подает тревожный сигнал или принимает контрмеры.

Сетевая система обнаружения вторжений выполняет мониторинг сетевого трафика и подает тревожный сигнал при обнаружении последовательности пакетов, которая может свидетельствовать о попытке сканирования, атаке отказа в обслуживании или иной атаки.

Сетевые системы обнаружения вторжений должны размещаться в сетевых узлах, выполняющих функции безопасности, например в шлюзах. Серверные системы обнаружения вторжений устанавливаются на защищаемых серверах. В архитектурном отношении различают транзитные и конечные системы.

А.9.3 Средства заявителя

Возможные подходы к управлению привилегиями пользователей в сервис-ориентированной архитектуре инфраструктуры управления привилегиями включают в себя:

- хранение привилегий в удостоверениях, заверенных электронной подписью;
- централизованное хранение привилегий (например, с помощью сервиса, использующего каталог LDAP);
- объявления в форме сертификатов атрибута.

Хранение привилегий в удостоверениях, заверенных электронной подписью, может осуществляться в форме сертификата открытого ключа, сертификата атрибута или удостоверения, записанного на языке XACML. Преимущества каждого из этих подходов описаны в стандарте ISO/IEC 9594-8. В сертификатах открытого ключа привилегии могут храниться как некритичные расширения в соответствии со стандартом ASTM E2212. При подобном использовании сертификатов идентификации возникает тесная связь между аутентификацией и авторизацией, что, как утверждается, повышает устойчивость к сетевым отказам. Однако у этого подхода есть несколько недостатков.

Отмена или изменение любой привилегии владельца сертификата потребует отзыва и перевыпуска сертификата. При отзыве сертификата его номер обычно помещается в список отозванных сертификатов (СОС). В результате владелец идентичности не сможет использовать свою смарт-карту (или другой токен), пока на нее не будет записан обновленный сертификат. Поскольку сертификаты идентификации обычно находятся у их владельца, процесс обновления оказывается затруднительным. Учтите, что хранение привилегий в сертификатах идентичности не обеспечивает устойчивости к сетевым сбоям, поскольку при проверке сертификата надо иметь доступ к СОС. В связи с этим сертификаты идентичности более пригодны для медленно меняющихся «структурных» ролей, нежели динамичных «функциональных» ролей.

Одна из альтернатив состоит в использовании отдельного подписанного сертификата, а именно, сертификата атрибута, рассчитанного на хранение привилегий пользователя. Для выпуска таких типов сертификатов и управления ими необходима дополнительная инфраструктура.

Однако у этого подхода есть несколько преимуществ. Сертификат атрибута выпускается и подписывается ОА, отдельным от ЦС, управляющего сертификатами идентичности. Однако при этом сохраняется тесная связь между авторизацией и аутентификацией за счет помещения серийного номера сертификата идентификации пользователя в поле владельца сертификата атрибута. Отзыв атрибута может осуществляться с помощью списка отзыва сертификатов атрибута. Однако пользователь вовсе не обязан физически обладать сертификатом атрибута. Сертификаты атрибутов могут храниться с помощью сервиса, использующего каталог LDAP. В этом случае при отзыве и перевыпуске сертификата атрибута прежний сертификат заменяется в каталоге на текущий. Это устраняет сложности частой замены привилегий, которые присущи хранению привилегий в сертификатах идентичности.

В использовании дополнительной инфраструктуры, обеспечивающей применение сертификатов атрибута, есть определенное преимущество [23]. ЦС, выпускающие сертификаты идентичности, обычно управляются до-

веренной стороной, не являющейся структурной единицей предприятия. Дополнительная инфраструктура, созданная внутри предприятия для выпуска сертификатов атрибута, позволяет скрыть чувствительную информацию о привилегиях от чужих глаз. Сертификаты атрибута обычно нужны только контролеру привилегий, поэтому владельцу привилегий нет необходимости предъявлять их за пределами предприятия.

А.9.4 Выборка роли из каталога LDAP

Выборка роли может обеспечиваться с помощью хранения информации о роли в структуре LDAP. При таком хранении обеспечивается быстрая функциональность поиска и чтения, необходимая для сбора информации о привилегиях, назначенных пользователю. Применение каталога LDAP для выборки роли обычно обеспечивается с помощью серверов веб-приложений. К каталогу LDAP можно также обращаться из приложений, которые выполняются независимо от серверов веб-приложений. Предпочтительный подход состоит в использование точки принятия решений о политике, которая выполняет выборку роли в ответ на запрос контроля доступа. В каждом случае использование выборки роли из каталога LDAP имеет то преимущество, что информация о роли отделена от кода приложения, запрашивающего информацию.

Информация о роли может быть предоставлена в форме удостоверения (например, в формате SAML), что снижает потребность в выборке роли из каталога LDAP.

А.9.5 Сертификаты

А.9.5.1 Общие сведения

Как уже обсуждалось, связь между идентичностью и сертификатом гарантируется с помощью использования криптографического ключа. Сертификаты могут использоваться сервисами для установления доверительных отношений в инфраструктуре управления привилегиями. С помощью заверенных сертификатов можно гарантировать подлинность объявлений идентичности или привилегий, передаваемых доверенными сервисами доверяющей стороне. Информация о роли может передаваться в сертификатах идентификации. Однако такая информация должна быть по своей природе достаточно статичной (например, информация о структурной роли), поскольку при изменении роли, хранящейся в сертификате идентификации, его надо перевыпустить. Для передачи более динамичной информации о привилегиях и ролях (например, функциональных ролях) более пригодны сертификаты атрибутов. Применение сертификатов обеспечивает конфиденциальность и неоспоримость.

А.9.5.2 Сертификаты атрибута

Сертификат атрибута пользователя может иметь ссылку на другой сертификат атрибута, содержащий дополнительные привилегии. Тем самым обеспечивается эффективный механизм реализации привилегированных ролей.

Для выполнения некоторых операций во многих системах, где необходима авторизация, требуется использовать ролевые привилегии (обычно в сочетании с привилегиями, основанными на идентичности). В этом случае заявитель может представить контролеру нечто, свидетельствующее только о наличии у заявителя определенной роли (например, «лицензированный медицинский работник» или «конторский служащий»). Контролер может априори знать, какие привилегии имеет объявленная роль или каким-то образом получить информацию об этих привилегиях, и на основании этой информации принять решение об авторизации доступа или об отказе в доступе.

Необходимо принять во внимание следующие факторы:

- отсутствие надежной коммуникационной системы;
- намерение не подтверждать информацию у издателя сертификатов;
- стабильность привилегий или относительная статичность ролей;
- применимость подхода к функциональным ролям.

Возможны следующие варианты реализации:

- каждый орган по присвоению атрибутов может присвоить любое число ролей;
- как роль, так и участники роли могут определяться и управляться отдельно разными органами по присвоению атрибутов;
- привилегии, назначенные роли, могут быть помещены в один или несколько сертификатов атрибута;
- при необходимости участнику роли может быть присвоено только подмножество привилегий, назначенных роли;
- участие в роли может быть делегировано;
- ролям и участию в ролях могут быть заданы любые требуемые сроки жизни.

Для субъекта выпускается сертификат атрибута, в котором объявлено, что этот субъект выполняет определенную роль. Этот сертификат может иметь расширение, содержащее ссылку на другой сертификат, описывающий роль (т. е. в этом сертификате роли в качестве владельца указаны имя роли и список привилегий, назначенных этой роли). Издатель сертификата атрибута может быть независимым от издателя сертификата роли, и эти типы сертификатов могут управляться совершенно раздельно (например, иметь разные сроки действия, отзываться и т. д.).

Не все формы общего имени GeneralName пригодны для использования в качестве имен ролей. Наиболее полезными вариантами являются объектные идентификаторы и отличительные имена.

А.9.6 Медицинские удостоверения

Одним из общих типов носителей привилегий является удостоверение пользователя. Такие удостоверения выпускаются доверенными органами и содержат идентифицирующую строку. Примерами могут служить лицензии на право медицинской деятельности, выдаваемые уполномоченными органами, и номера, присваиваемые Управ-

лением по борьбе с наркотиками (Drug Enforcement Agency — DEA). Удостоверение содержит тип, имя издателя и идентификатор. В структуру имени издателя могут включаться географические указания, например, штат и другое местонахождение. Удостоверения обычно различаются по типу (например, «врач») или по типу и издателю (например, «врач, лицензированный в Вирджинии»).

Если имя издателя удостоверения отсутствует, то вместо него берется имя издателя сертификата атрибута или сертификата открытого ключа, в котором передано удостоверение. Если имя издателя сертификата отсутствует, то имя издателя удостоверения должно присутствовать. (Учтите, что для минимизации числа органов по присвоению атрибутов, используемых в системе, один сертификат может содержать несколько удостоверений, выданных более чем одним издателем.)

Необходимо принять во внимание:

- возможность использования некритичных полей сертификата идентификации, соответствующего стандарту X.509, для описания медицинских удостоверений в соответствии со стандартом ASTM E2212;
- возможность использования медицинских удостоверений (текущих, не текущих, область действия) в качестве дополнительных ограничений при авторизации доступа медицинских работников к медицинской информации;
- альтернативную возможность использования медицинских удостоверений врачей при защищенном предъявлении атрибутов пользователя в инфраструктуре управления привилегиями.

А.9.7 Объявления на языке SAML

Объявления на языке SAML могут использоваться для передачи заявителем информации безопасности доверяющей стороне. Объявление может быть сделано от имени субъекта при его аутентификации либо в ответ на запрос другого субъекта, также составленный на языке SAML. Объявления могут быть составлены из информации о привилегии или роли, хранящейся на центральном сервере, либо из информации, содержащейся в подписанном сертификате.

Необходимо принять во внимание:

- гибкость применения федеративной среды;
- необходимость получения дополнительной информации от заявителя;
- уровень надежности и доступности вычислительной сети;
- наличие службы обработки запросов на языке SAML;
- наличие поддержки обращения удостоверений внутри предприятия;
- совместимость с безопасностью веб-сервисов и запросов по протоколу SOAP;
- необходимость одновременного применения различных механизмов аутентификации (например, удостоверения в инфраструктуре открытых ключей, протокол Kerberos, токены, биометрическая аутентификация и т.д.).

А.9.8 Механизмы чувствительности целевого объекта

Управление атрибутами целевого объекта (например, списками контроля доступа и метками чувствительности) традиционно выполняется в рамках конкретной системы, поэтому представление этой информации слабо стандартизовано. Настоящее приложение не предъявляет требований к ее представлению, но содержит некоторые предложения, основанные на применении некоторых синтаксисов описания данных (ASN.1 или XML).

А.9.9 Инкапсуляция подписанных данных

Атрибуты и другая чувствительная информация могут быть привязаны к дайджесту целевого объекта с помощью конструкции SignedData. В частности, уместно использовать отделенные подписи (передаваемые отдельно от объекта). Чувствительная информация может переноситься в виде подписанных атрибутов, у которых автором будет подписавший субъект.

К целевому объекту могут быть добавлены следующие типы авторизующей информации:

- информация контроля доступа, описанная в стандарте ISO/IEC 10181-3;
- требования равнозначной подписи (см. А.9.19);
- описательные сведения о документе (например, тип документа), приведенные в А.11.3.

А.9.10 Использование языка XML

Применение расширяемого языка разметки XML позволяет передавать информацию независимо от программной и аппаратной платформы. Поэтому можно ожидать, что содержание многих передаваемых документов будет представлено на языке XML. Структура содержания такого документа будет указана в определении типа документа DTD (document-type definition) или в XML-схеме.

Привилегии могут быть переданы в элементах XML, у которых в качестве имени используется идентификатор привилегии. В качестве альтернативы можно передавать идентификаторы привилегий в виде имен атрибутов элемента.

Язык XML позволяет группировать привилегии в форме полезных комплексов. Например, комплексу привилегий, описанному на языке XML, может быть присвоен следующий универсальный идентификатор ресурса URI (uniform resource identifier):

“urn:application_name:attribute:privilege_set_name”

В качестве альтернативного представления можно ассоциировать комплекс привилегий с уникальным пространством имен, указанным в XML-схеме, например:

xmlns: privilege_set_name=”gost.e-ecolog.ru privilege_set_name/”

Комплексы привилегий, представленные на языке XML, могут быть использованы контролером, чтобы ассоциировать заявителя с его сферой полномочий. Заявители могут быть заранее (до контроля) ассоциированы

со стандартной группой или ролью. В другом варианте контролер может ассоциировать заявителя с одним или несколькими комплексами привилегий с помощью запроса к базе данных или к сервису, использующему каталог LDAP. Контролер может также извлечь информацию о группе или роли заявителя из внешнего XML-документа с помощью указания пути на языке XPath.

При использовании политики привилегий контролер может иметь дело непосредственно с XML-элементами (например, сравнивая значения атрибутов, хранящиеся в сертификате авторизации, с элементами документа). В качестве формата описания политики на языке XML, которое может использоваться при контроле привилегий, можно предложить расширяемый язык разметки контроля доступа XACML (eXtensible Access Control Markup Language). Правила сравнения детально обсуждаются в А.9.11 — А.9.19. В общем случае однократные атрибуты будут сравниваться с единственным (полным) элементом, а многократные атрибуты — с коллекцией элементов моделируемой группы.

А.9.11 Базовый контроль доступа

Далее определяется атрибут информации контроля доступа, который может использоваться для указания получателю (или доверенной третьей стороне), какие субъекты могут читать содержание целевого объекта.

Доступ к целевому объекту разрешается, если идентификатор запрашивающей стороны совпадает с одним из элементов списка, указанного в поле who (по имени, роли, группе или организационной единице) и если значения, переданные в сертификате атрибута запрашивающей стороны, совпадают со всеми ограничениями, указанными в атрибуте информации контроля доступа целевого объекта. Эти значения должны содержаться в атрибуте constraints сертификата запрашивающей стороны.

А.9.12 Способы указания политик

Хотя настоящее приложение и не предъявляет требований к представлению политик в конечной системе, тем не менее можно рекомендовать применение языка XACML в качестве стандартного средства описания политик. Очевидны следующие несколько сценариев.

Два субъекта могут нуждаться в определении, являются ли их политики авторизации совместимыми, что нередко требуется в среде, использующей веб-сервисы. Если их политики совместимы, то может потребоваться задание специфичных переменных, описывающих эти политики и приемлемых для обоих субъектов. Для этого можно создать объявление XACMLAuthzAssertion, структура которого описана в документе «XACML Profile for Web Services (WS-XACML)». Такое объявление может быть включено в экземпляр веб-политики или предоставлено в форме независимых метаданных.

Объявление XACMLAuthzAssertion может также использоваться поставщиком веб-сервисов для публикации политики авторизации потенциальным клиентам. Публикация политик авторизации приемлема не для всех реализаций, но публикация некоторых аспектов политики авторизации может быть полезной даже в том случае, если публикация всей политики признана нецелесообразной по причинам безопасности.

Управление политикой безопасности может включать в себя следующие шаги или некоторую их часть: составление, пересмотр, тестирование, утверждение, публикация, комбинирование, анализ, модификация, прекращение действия, поиск и применение политики.

Полная политика, применимая к конкретному запросу решения, может состоять из ряда отдельных правил или политик. Например, в приложении, обеспечивающем конфиденциальность, субъект персональных данных, получающий медицинскую помощь, может задать одни аспекты политики раскрытия его данных, в то время как организация, обладающая этими данными, может задать некоторые другие аспекты. Чтобы принять решение об авторизации, должна быть возможность образования одной политики из этих двух, применимых к запросу.

В языке XACML определены три верхнеуровневых элемента политики: <Rule> (правило), <Policy> (политика) и <PolicySet> (комплекс политик). Элемент <Rule> содержит булевское выражение, которое может быть вычислено изолированно, но его результат не предназначен для изолированного использования точкой принятия решения о политике. Это выражение существует отдельно только для точки доступа к политике, которая может рассматривать его как базовую единицу управления и повторно использовать в нескольких политиках.

Элемент политики <Policy> содержит совокупность элементов правил <Rule> и заданную процедуру сочетания результатов применения этих правил. Он представляет собой базовую единицу политики, используемую точкой принятия решения о политике, и, следовательно, предназначен служить основой для решения об авторизации.

Элемент комплекса политик <PolicySet> содержит совокупность элементов политик <Policy> или другие комплексы политик <PolicySet>, а также заданную процедуру сочетания результатов применения этих политик и комплексов политик. Это стандартный способ образования одной комбинированной политики путем сочетания отдельных политик.

В языке XACML определено несколько алгоритмов сочетания политик, которые могут быть указаны в атрибутах RuleCombiningAlgId или PolicyCombiningAlgId элементов <Policy> или <PolicySet> соответственно. Алгоритм сочетания политик определяет процедуру вычисления решения об авторизации по отдельным результатам вычисления комбинации правил.

Определены следующие стандартные алгоритмы сочетания:

- перекрытие отказом (упорядоченное и неупорядоченное) (deny-overrides);
- перекрытие разрешением (упорядоченное и неупорядоченное) (permit-overrides);
- выбор первого применимого правила (first-applicable);
- выбор только одного применимого правила (only-one-applicable).

Правило rule может вычисляться на основе его содержания. Основными компонентами правила rule являются:

- цель (target);
- эффект (effect);
- условие (condition).

Цель target включает в себя совокупность следующих элементов:

- ресурсы (resource),
- субъекты (subjects),
- действия (action),
- среда (environment).

Элемент условия <Condition> может накладывать дополнительное условие на применимость политики, заданную целью target. Если правило rule должно быть применимо ко всем объектам определенного типа данных, то соответствующий объект удаляется из цели target. Точка принятия решения о политике проверяет, что элементы, описанные в цели target, соответствуют субъектам subjects, ресурсу resource, действию action и атрибутам среды environment, содержащимся в контексте запроса context. Определения цели target являются дискретными, чтобы применяемые правила rule могли быть эффективно идентифицированы точкой принятия решения о политике. Элемент цели <Target> может быть не указан в правиле <Rule>. В этом случае цель правила <Rule> считается той же, что указана в родительском элементе политики <Policy>.

Возникают следующие вопросы: как точка принятия решения о политике должна интерпретировать имя, идентифицирующее комплекс субъектов или ресурсов, когда оно появляется в политике или в контексте запроса? Предназначено ли это имя для идентификации только узла дерева объектов или оно предназначено для идентификации всего поддерева этого узла?

Эффект effect правила rule описывает, какие последствия предполагает составитель правила в случае, когда результат его вычисления имеет значение «Истина» (True). Эффект может иметь два значения: «Разрешить» (Permit) и «Отказать» (Deny).

Условие condition представляет собой булевское выражение, которое дополнительно ограничивает применимость правила сверх той проверки, которая проводится по содержанию цели target. Поэтому оно может отсутствовать.

А.9.13 Передача политик, представленных на языке XACML

В инфраструктуре управления привилегиями может потребоваться передача политики от одного субъекта к другому. Далее приведено несколько примеров подобных ситуаций:

- точка принятия решения о политике обрабатывает политику, содержащую ссылку на имя другой политики. Эта политика при необходимости может быть получена с помощью запроса к точке управления политиками;
- точке принятия решения о политике может понадобиться получение «корневой» политики от точки управления политиками предприятия, чтобы учесть некоторые настройки системы;
- может потребоваться передача ресурса из одной зоны безопасности в другую, и источник ресурса может вместе с ним передать политику его защиты, которая должна применяться в зоне безопасности получателя;
- в целях повышения производительности распределенной системы, в которой точки принятия решения о политике размещены локально, может потребоваться применение общего комплекса политик. В этом случае центральной точке управления политиками необходимо передавать из каждой точки принятия решения о политике.

Язык XACML, в основном предназначен для описания политик, но его конструкции рассчитаны на применение в компонентах всей системы авторизации. Для этого необходимы другие компоненты, предоставляющие средства проверки, удостоверяющие что экземпляры политик предоставлены доверенной точкой управления политиками, защищающие целостность и конфиденциальность экземпляров политик и реализующие протоколы запросов экземпляров политик и получения ответов на запросы. Для обеспечения выполнения этих функций конструкции на языке XACML можно интегрировать в сообщения языка разметки объявлений безопасности SAML версии 2.0, разработанные организацией OASIS. Это позволяет защищать не только атрибуты информации контроля доступа, но и политики. Интеграция сообщений на языке SAML и конструкций на языке XACML иллюстрируется рисунком А.2.

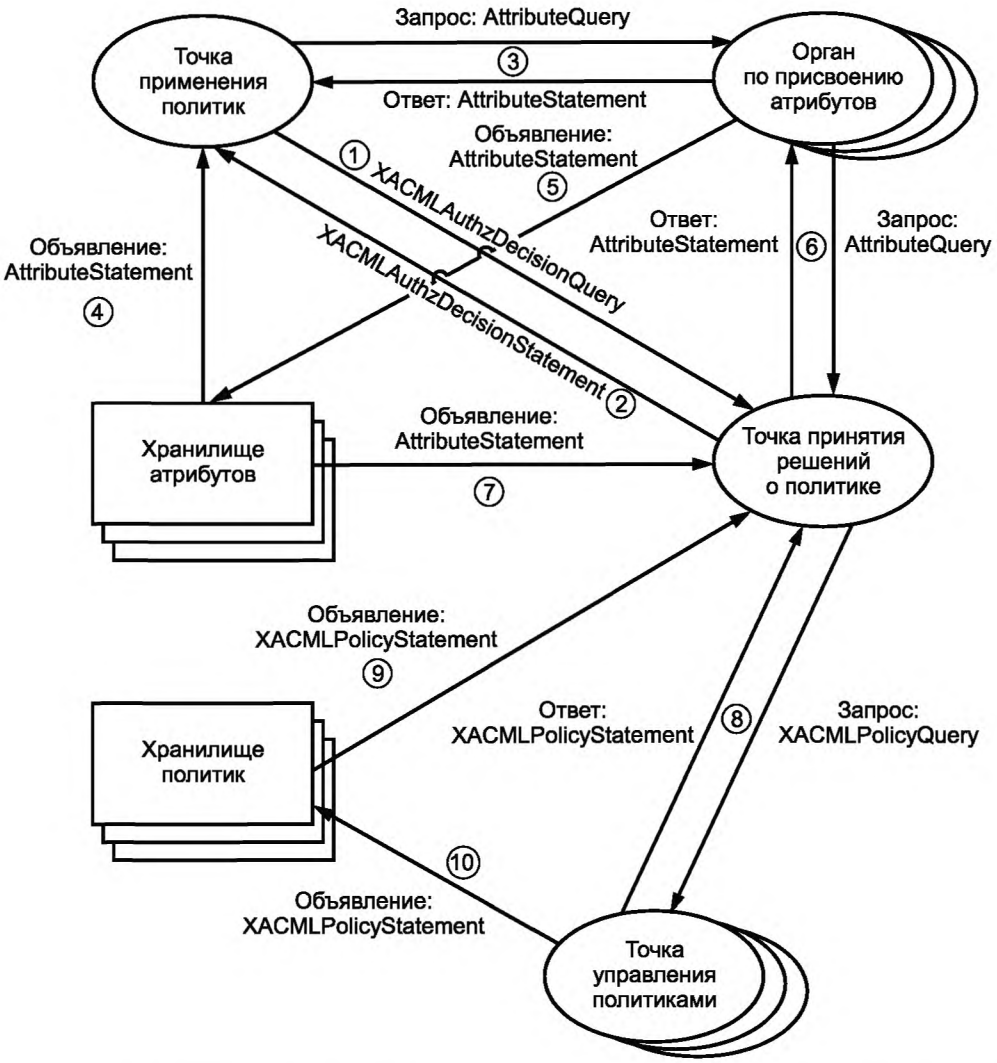


Рисунок А.2 — Использование спецификации SAML 2.0 для транспорта данных в формате XACML [12]

Как показано на этом рисунке, когда точке применения политик требуется получить решение об авторизации, она посылает запрос (1) точке принятия решения о политике, которая по этому запросу обрабатывает доступные ей политики и атрибуты, принимает решение об авторизации (2) и возвращает его точке применения политик. Эта точка применения политик может либо получить необходимые атрибуты непосредственно от онлайнового ОА (3), либо извлечь их из хранилища атрибутов (4), в которое ОА заранее переслали атрибуты (5). Точка принятия решения о политике также может получить необходимые атрибуты от онлайнового ОА (6) либо извлечь их из хранилища атрибутов (7).

Решение об авторизации, принятое точкой принятия решения о политике, основано на информации о политиках, полученной от точки управления политиками (8) либо извлеченной из онлайнового хранилища политик (9). Это хранилище служит кэшем политик, ранее сохраненных точкой управления политиками (10).

Запрос XACMLPolicyQuery сформирован на языке SAML, определен в этом профиле и может использоваться для запроса политик у точки управления политиками, осуществляемого по имени политики или по применимости политики к определенному запросу авторизации. Требуемая информация в формате XACMLPolicyStatement возвращается в ответе на языке SAML. Эта информация может быть заверена электронной подписью и может быть привязана к издателю информации, сроку ее действия и другим атрибутам.

Можно определить несколько политик. Они могут применяться отдельно друг от друга или совместно.

А.9.14 Отображение типов данных ANS.1 на элементы XML

Можно рекомендовать следующее отображение типов данных ANS.1 на элементы XML (по возможности в этом отображении используется текущая работа над XML-схемами):

а) булевский тип данных ASN.1 (BOOLEAN) отображается на содержание элемента или атрибут элемента со следующими возможными значениями (не чувствительными к регистру): значение TRUE преобразуется в true, yes или 1, значение FALSE преобразуется в false, no или 0. Сравнение разрешается только на точное совпадение;

b) целочисленный тип данных ASN.1 (INTEGER) отображается на содержание элемента или атрибут элемента в виде строки, состоящей из цифровых символов, в начале которой может стоять знак (+ или -);

c) вещественный тип данных ASN.1 (REAL) отображается на содержание элемента или атрибут элемента, используя ту же нотацию вещественного числа, что и в ASN.1;

d) типы данных ASN.1 BIT STRING и OCTET STRING отображаются на произвольное содержание элемента (#PCDATA). По мере развития аппарата XML-схем значения этих типов данных будут отображаться на двоичный объект. При передаче данных его значение будет записано в кодировке base64, которая может быть указана в схеме или как значение атрибута элемента;

e) перечислимый тип данных ASN.1 (ENUMERATED) отображается на атрибут типа NMTOKENS (список строк), где каждая строка является идентификатором одного из перечисляемых значений.

Примечание — XML-схемы позволят передавать такие данные как в элементах, так и в атрибутах.

f) строковые типы данных ASN.1 отображаются на содержание элемента (#PCDATA);

g) объектные идентификаторы, используемые в ASN.1, не имеют прямого аналога в XML.

Примечание — В языке XML-для похожих целей используются универсальные идентификаторы объектов URI. Для передачи объектных идентификаторов в XML можно использовать имя пространства имен в URI или имя протокола «oid».

h) типы данных, описывающие в ASN.1 время (UTCTime и GeneralizedTime), отображаются на элементы, используя синтаксис, предложенный в стандарте ISO 8601;

i) тип последовательности значений ASN.1 (SEQUENCE) преобразуется с использованием модели группировки содержания с запятой в качестве разделителя, например, <!ELEMENT x (foo,bar)>;

j) тип выбора значений ASN.1 (CHOICE) преобразуется с использованием модели группировки содержания с вертикальной чертой в качестве разделителя, например, <!ELEMENT x (foo|bar)>;

k) множество значений ASN.1 (SET) не имеет прямого эквивалента в XML, хотя в SGML его можно отобразить на группировку содержания со знаком & в качестве разделителя;

l) конструкция ASN.1 «SEQUENCE OF» отображается на повторяющийся компонент, используя синтаксис регулярных выражений XML (* для нуля, одного или нескольких повторений, + для одного или нескольких повторений), например, <ELEMENT y (foo*)>;

m) конструкция ASN.1 «SET OF» не имеет эквивалента в XML;

n) необязательные поля в ASN.1 (OPTIONAL) отображаются на необязательные компоненты XML, например, <!ELEMENT z (foo?)>.

ОА должны гарантировать, что описания политик внутренне непротиворечивы, например, один и тот же тип атрибута не должен появляться в двух логически противоречивых конструкциях политики. Политики должны быть подписаны ОА; они могут передаваться в сертификате авторизации заявителя или как отдельные объекты.

А.9.15 Согласие пациента

Согласие пациента представляет собой специальную политику, которая должна быть описана на определенном языке (например, XACML) в соответствии с принятой моделью политик.

А.9.16 Совпадение удостоверения

Атрибуты удостоверений описаны в стандарте ISO/TS 22600-2:2006 (в 11, а также в 5.6 и 5.8). Удостоверения выпускаются доверенными органами и содержат идентифицирующую строку. Примерами могут служить лицензии на право медицинской деятельности, выдаваемые уполномоченными органами, и номера, присваиваемые Управлением по борьбе с наркотиками (Drug Enforcement Agency — DEA). Удостоверение содержит тип, имя издателя и идентификатор.

Для совпадения с политикой удостоверений сертификаты заявителя, вместе взятые, должны содержать совпадающее удостоверение для каждого элемента списка credentias. Для совпадения с элементом удостоверение должно иметь тот же тип, а если в элементе указано имя издателя, то удостоверение (или содержащий его сертификат) должно иметь то же имя издателя.

А.9.17 Совпадение метки безопасности

Чтобы установить совпадение метки безопасности, необходимо сравнить допуск инициатора запроса с меткой безопасности целевого объекта. Чтобы доступ был разрешен, должны выполняться все следующие условия:

- идентификаторы политики безопасности должны быть идентичны;
- гриф допуска инициатора должен быть не ниже, чем гриф секретности целевого объекта (т. е. в списке грифов допуска хотя бы одно значение должно быть не ниже грифа секретности целевого объекта);
- для каждой категории безопасности, указанной в метке целевого объекта, должна существовать доминирующая категория безопасности того же типа в допуске инициатора.

А.9.18 Совпадение общего объявления

Политика привилегий включает в себя один из следующих параметров:

- предикат ppPredicate: объявление специфичного атрибута;
- связь «И» (and): список политик; чтобы данная политика была истинна, все политики из этого списка должны быть истинны;

- связь «ИЛИ» (or): список более простых политик; чтобы данная политика была истинна, хотя бы одна политика из этого списка должна быть истинна;

- функция «НЕ» (not): отдельная политика; чтобы данная политика была истинна, эта политика должна быть ложной;

- упорядоченный список orderedPPE: список более простых политик, проверяемых в заданном порядке.

В качестве предикатов могут использоваться:

- объявление простого значения: значение одного атрибута целевого документа (или переменной контекста) сравнивается с объявленным значением атрибута;

- объявление множества значений: все множество значений атрибута целевого документа (или переменной контекста) сравнивается с объявленным множеством значений;

- объявление наличия: атрибут должен присутствовать в документе;

- возможное совпадение (approximateMatch): объявленные значения атрибута сравниваются со значениями атрибута в документе с помощью некоторого местного алгоритма совпадения (например, фонетическое совпадение или приближенное арифметическое сравнение);

- расширяемое совпадение (extensibleMatch): объявленные значения атрибута сравниваются со значениями атрибута документа, используя макросы модуля MATCHING-RULE, описанные в стандарте X.500.

Объявления простого значения позволяют выполнять авторизацию на основе сравнения с одним значением. Например, значение атрибута lessOrEqual может задавать предельную сумму платежного поручения. Семантика каждого варианта такова:

- равенство (equality): значение атрибута документа должно быть равно значению атрибута в объявлении. Равенство может применяться к атрибутам любого типа; для сравнения атрибутов с комплексными типами данных их значения должны быть записаны в кодировке DER;

- подстроки (substrings): значение атрибута документа должно содержать объявленные подстроки в заданном порядке; начальная подстрока значения должна совпадать с начальным компонентом объявления (если таковой есть), любые компоненты (если они есть) должны появляться в значении в заданном порядке; последняя подстрока значения должна совпадать с последним компонентом объявления (если таковой есть). Подстроки не должны пересекаться в атрибуте документа. В таком объявлении могут использоваться строки любого типа, определенного в синтаксисе ASN.1 (например, IA5, UTF8 и т. д.);

- больше или равно (greaterOrEqual): значение атрибута документа должно быть больше объявленного значения атрибута или равно ему. Такое объявление может содержать числа, перечислимые данные и двоичные строки;

- меньше или равно (lessOrEqual): значение атрибута документа должно быть меньше объявленного значения атрибута или равно ему. Такое объявление может содержать числа, перечислимые данные и двоичные строки;

- подчинено (subordinate): объявленное значение совпадает с ведущими компонентами значения атрибута документа. Такое объявление может содержать только объектные идентификаторы и имена (последовательность относительных отличительных имен).

Совокупность проверенных объявлений включает в себя все значения атрибута, которые найдены в целевом объекте. Например, в стандартной военной процедуре ограничения доступа к документам может быть предписано, что совокупность кодовых слов, приписанных документу, должна быть подмножеством (subsetOf) кодовых слов, указанных в сертификате заявителя. Аналогичным образом механизм предоставления доступа, если есть необходимость знания, может использовать объявление с непустым пересечением (nonNullIntersection). Атрибуты таких объявлений должны иметь тип данных SEQUENCE OF или SET OF. Используется следующая семантика:

- подмножество (subsetOf): все значения атрибута документа должны присутствовать в объявленном атрибуте;

- надмножество (supersetOf): все значения объявленного атрибута должны присутствовать в атрибуте документа;

- непустое пересечение (nonNullIntersection): хотя бы одно значение атрибута документа должно присутствовать в объявленном атрибуте.

В предикате могут быть указаны специфичные значения, сравниваемые со значениями атрибута документа. Предикат может также содержать ссылку на атрибут, передаваемый в сертификате атрибута заявителя и содержащий значения, которые должны сравниваться со значениями атрибута документа. В этом случае объявление должно иметь элемент с типом данных PrivilegeIDPair, содержащий два типа атрибутов: первый относится к целевому объекту, второй — к заявителю.

Поддерживаются смешанные синтаксисы описания атрибутов. В настоящее время они включают в себя синтаксис ASN.1 и язык XML. Поскольку привилегии заявителя передаются в атрибутах, описанных с помощью синтаксиса ASN.1, в идентификаторе привилегии должен быть указан тип атрибута; связь с XML-данными (указывающая на соответствующий элемент содержания целевого XML-документа) необязательна. Связь структурируется в соответствии с правилами конструирования XLink, XPointer и XPath при дополнительном ограничении, что она указывает на один элемент XML или связную группу элементов (атрибутов).

А.9.19 Требования к электронной подписи

Для лиц, подписывающих данные, выпускаются сертификаты атрибута, в которых указаны разрешаемые им цели подписи. При подписании документа цель подписи включается в него как подписанный атрибут (см. PS 100).

Политика представляется, используя, к примеру, синтаксис SignatureRequirements в соответствии с рекомендациями ASTM E1762.

Контролер может выполнить следующие действия:

а) проверить сертификат атрибута каждого лица, подписавшего данные, чтобы убедиться, что им разрешена цель подписи;

б) проверить, что в соответствии с политикой привилегий документ содержит все необходимые подписи.

Несколько подписей можно передать в форме повторяющихся структур SignerInfo, включенных в экземпляр класса SignedData. Подписи, заверяющие другие подписи, могут быть присоединены, используя (неподписанный) атрибут заверяющей подписи. Требования к подписанию передаются в форме политики привилегий, ассоциированной с конкретным целевым объектом и конкретной операцией.

Каждая подпись документа содержит или идентификацию подписавшего лица (имя роли или лица либо идентификатор сертификата), или список требуемых целей подписи, или и то, и другое. Если указана роль, то у документа должна быть подпись с этой ролью (указанной в атрибуте подписи), и подписывающее лицо должно иметь право участвовать в этой роли (это должно быть указано в атрибуте роли сертификата авторизации, выданного этому лицу). Если указано имя лица, то у документа должна быть подпись, которую можно проверить с помощью одного из сертификатов пользователя. Если идентифицирован конкретный сертификат (по имени и идентификатору ключа либо по имени издателя и серийному номеру), то у документа должна быть подпись, которую можно проверить с помощью указанного сертификата. Если указан список целей подписи, то у документа должна быть подпись, в которой указана какая-либо из этих целей (в атрибуте signaturePurpose подписи). Если указаны и идентификатор лица, и цели подписи, то в подписи этого лица должна быть указана одна из этих целей.

Каждой подписи документа может быть присвоен необязательный вес на тот случай, если число подписывающих лиц может быть переменным. Кворум задает суммарный вес, вычисляемый по списку подписавших лиц, при котором документ считается утвержденным. В общем случае, когда все веса равны единице, кворум указывает число лиц, которые должны подписать документ. Присваивая веса, можно, к примеру, задать схему, согласно которой для утверждения документа нужна подпись президента, любых двух вице-президентов или любых четырех директоров. Нулевое значение кворума означает, что все лица, перечисленные в списке, должны подписать документ. Может потребоваться указывать подпись в определенном порядке (совместная подпись документа или заверение других подписей [24]).

А.10 Интеграция с инфраструктурой открытых ключей

Для идентификации сертификатов инфраструктура управления привилегиями должна полагаться на инфраструктуру открытых ключей или, по крайней мере, должна быть сконструирована в расчете на нее. С помощью этой инфраструктуры контролер аутентифицирует владельца сертификата атрибута (используя электронные подписи). Каждый сертификат атрибута либо содержит имя владельца, либо (что чаще) ссылку на сертификат идентификации владельца. Такое сращивание двух инфраструктур обеспечивает несколько уже описанных преимуществ.

Сертификаты атрибута выпускаются ОА. Эти органы могут иметь иерархическую организацию, подобную иерархии центров сертификации. Когда подписчик запрашивает сертификат идентичности, то это не обязательно влечет за собой выпуск сертификатов атрибута. Так бывает в том случае, когда подписчики не распоряжаются своими привилегиями.

Отзыв сертификатов атрибута осуществляется аналогично отзыву сертификатов идентификации (т. е. с использованием списков отзыва). В другом варианте используется онлайновый протокол статуса сертификата OCSP (online certificate status protocol). Однако обычно пользователь не обязан физически обладать своим сертификатом атрибута. Такие сертификаты могут храниться сервисом каталога и просто обновляться, если содержание сертификата атрибута устарело. В этой модели отзыв сертификата не нужен, поскольку с помощью доступа к хранилищу сертификатов атрибута можно получить все текущие сертификаты атрибута.

В инфраструктуре управления привилегиями могут быть использованы два типа делегирования:

- ОА может делегировать свои полномочия подчиненным ОА или конечным пользователям. В этом случае полномочия возрастают по мере продвижения к корню иерархии. Контроль делегирования осуществляется с помощью сертификатов, выпущенных для ОА;

- пользователи обращаются с запросом делегирования своей авторизации, и ОА выпускает соответствующий сертификат после проверки, что сертификат делегирующего пользователя разрешает делегирование. Иерархия подобного делегирования может быть выстроена с помощью использования в сертификатах атрибута расширения delegatorAttributeIdentifier.

Дальнейшее обсуждение интеграция инфраструктуры управления полномочиями с инфраструктурой открытых ключей см. в ISO/IEC 9594-8.

А.11 Примеры приложений управления привилегиями и контроля доступа

А.11.1 Общие сведения

Здесь представлены несколько примеров приложений, использующих механизмы, определенные в А.2 — А.10. Они описаны не с высокой степенью детализации. Конкретные приложения могут быть описаны в будущих стандартах или в спецификациях разработчиков. Приведенные примеры служат иллюстрацией применения механизмов управления привилегиями для поддержки типов приложений, описанных в рекомендациях ASTM E1762 и ASTM E1986. Они также служат иллюстрацией текущей работы в области политик сертификации и расширений.

А.11.2 Применение удостоверений

В этом примере врач выписывает контролируемую субстанцию. Рецепт заверяется электронной подписью и отправляется в аптеку с помощью защищенных многоцелевых расширений электронной почты S/MIME (secure/ multipurpose internet mail extensions). Поскольку в рецепте указана контролируемая субстанция, фармацевт должен проверить, присвоен ли врачу действующий идентификатор Управления по борьбе с наркотиками (DEA). Эту проверку можно выполнить по удостоверению врача в форме сертификата идентификации (ID) или сертификата атрибута. Удостоверение должно иметь тип «номер DEA», а его издателем должно быть Управление по борьбе с наркотиками.

Аналогичные средства могут использоваться, чтобы определить, является ли лицо врачом (тип удостоверения «лицензия на право медицинской деятельности»). Чтобы узнать штат, в котором действительна лицензия врача, можно проверить издателя удостоверения. Учтите, что при использовании отличительных имен правила именования издателей могут быть регламентированы на уровне штата, на федеральном уровне (на уровне агентства) или с использованием стандартов обработки федеральной информации FIPS PUB 66 (Federal Information Processing Standards Publications).

А.11.3 Контроль доступа

Приложение контроля доступа позволяет контролеру управлять доступом к целевому объекту (в данном случае — к некоторой части медицинской карты пациента) на основе значений атрибутов целевого объекта. При этом учитываются ограничения, использующие следующую информацию:

- наличие регистрации планируемой медицинской помощи;
- отделение.

Сертификат атрибута заявителя содержит одну или несколько ролей, а также список зарегистрированных планов медицинской помощи и отделений, в которых работает заявитель. Отдельные сертификаты роли (с атрибутами, специфичными для каждой роли) в данном примере не используются.

Информация контроля доступа целевого объекта содержится в соответствующем атрибуте (см. А.2.2). Доступ заявителя к целевому объекту будет разрешен при выполнении следующих условий:

- хотя бы одна из ролей заявителя должна совпасть с какой-либо ролью из списка, указанного в информации контроля доступа целевого объекта;
- хотя бы один из планов медицинской помощи должен присутствовать в списке ограничений целевого объекта.

А.11.4 Требования подписи

В этом примере используется механизм цели подписи, определенный в стандарте ASTM E1762. Чтобы документ можно было включить в состав медицинской карты, он должен быть скреплен одной или несколькими подписями в соответствии с политикой привилегий. Например, в политике может быть указано, что документ должен быть подписан автором либо оператором и контролером документа.

Каждая подписывающая сторона имеет сертификат атрибута, в котором указаны цели подписи, разрешенные этой стороне. При подписи документа цель подписи добавляется к его метаданным как подписанный атрибут. Политика представляется, используя, к примеру, синтаксис SignatureRequirements в соответствии с рекомендациями ASTM E1762.

Контролер выполняет следующие действия:

- проверяет сертификат атрибута каждой подписавшей стороны, разрешена ли в нем цель подписи;
- устанавливает, присутствуют ли все подписи, требуемые политикой привилегий.

А.11.5 Авторизация документа

В этом примере используются механизмы и атрибуты, определенные в стандарте ANSI X9.45 [46].

Привилегии заявителей передаются в сертификатах авторизации. Заявитель может иметь несколько ролей, указанных в сертификатах роли (но в каждый момент времени может выполнять только одну из них). Сертификат авторизации заявителя содержит атрибут allowableRoles, указывающий, какие роли может выполнять заявитель.

Целевые атрибуты могут быть извлечены из документа (например, элементы XML), сохранены в местной базе данных или вложены в структуру SignedData (отделенная подпись). Для связи этой структуры с целевым объектом используется дайджест объекта.

Политика привилегий включает в себя требования подписи и общую политику объявлений, как описано в разделе контроля доступа.

Контролер использует сертификат авторизации заявителя вместе с ассоциированными сертификатами роли, а также атрибуты целевого объекта в качестве входных данных общей политики объявлений, описанной в разделе контроля доступа. Если требования этой политики выполнены, то проверяются требования к подписи. Текущая структура данных подписей (содержащая одну или несколько подписей документа, а также, возможно, подписи, которые их заверяют) проверяется на соответствие политике требований к подписи. Если и эта проверка выполнена успешно, то документ считается авторизованным.

К специфичным атрибутам, включаемым в сертификат авторизации, относятся:

a) ограничения документов, указывающие. что он может быть подписан;

b) разрешенные роли;

c) разрешенные цели подписи;

d) атрибуты, ассоциированные с документом, включая:
- тип документа;
- местонахождение;
- идентификатор пациента;
- идентификатор события;
- информацию о замене (указатель на заменяемый документ);
- организацию, создавшую документ;
- дату и время события;
- даты и время создания и модификации документа, доступа к документу;
- денежную сумму;
- список категорий;
- информацию о создателе и авторе (которых можно установить также по подписям документа);

e) подписанные атрибуты, которые могут быть приложены к документу, включая:
- дату и время подписи;
- цель подписи;
- выполняемые роли;
- идентификаторы подписывающего сертификата и политики;
- причину подписи (текстовое описание);
- аннотацию;
- идентификатор устройства использованного криптографического модуля.

Подпись, заверяющая другую подпись, передается как неподписанный атрибут, который подписывает значение подписи, содержащейся в структуре SignerInfo.

А.11.6 Модель ролевого доступа ANSI RBAC

В стандарте ANSI RBAC разрешения определены как действия над защищенным объектом; однако этот стандарт не описывает ни специфические действия, ни специфические объекты. Объекты могут существовать на разных логических уровнях. Например, конкретные объекты могут быть определены как отдельные элементы данных, таблицы либо агрегаты элементов данных и таблиц. К более абстрактным объектам относятся профили работ, задачи, сценарии или шаги.

В стандарте ISO/TS 22600-2:2006 на рисунке 9 представлена схема ролевого контроля доступа, адаптирующая стандарт ANSI RBAC. На этом рисунке показано, что связь функциональных ролей с сеансом представляет собой сеансовую роль, активированную в этом сеансе пользователя, а связь пользователя с сеансом описывает сеанс пользователя. Разрешения, которые доступны пользователю, суть разрешения, присвоенные ролям, которые в настоящий момент активны во всех сеансах пользователя.

Каждый компонент модели состоит из субкомпонентов:
- совокупность базовых множеств элементов;
- совокупность отношений ролевого контроля доступа, ассоциированных с этими множествами элементов (содержащие подмножества декартова произведения, обозначающие допустимые присваивания);
- совокупность отображающих функций, которые связывают члены одного множества элементов с данным членом другого множества.

А.12 Эквивалентность политик

Обмен информацией о привилегии между зонами безопасности возможен по соглашению сторон. Такое взаимодействие между зонами подлежит координации как на техническом, так и на документальном уровне.

При передаче информации о привилегии необходимо обеспечить одинаковую интерпретацию привилегии в каждой зоне безопасности. Этого можно достичь, создав стандартный комплекс привилегий. Такой комплекс может включать в себя взаимно однозначное отображение эквивалентных процедур между зонами. Чтобы достичь требуемой степени безопасности, необходимо выполнять техническую проверку эквивалентности передаваемых привилегий.

Информация о привилегии, передаваемая между зонами безопасности, может содержать сведения о различных административных субъектах, например деловых партнерах или организациях. Соглашение о передаче привилегий и их интерпретации должно документироваться, обычно — в «соглашении деловых партнеров». Это необходимо для разграничения юридической, этической и практической ответственности сторон в инфраструктуре управления привилегиями. Кроме того, такое соглашение может быть расширено на другие стороны, взаимодействующие с инфраструктурой управления привилегиями. Эквивалентная процедура выполняется в инфраструктуре открытых ключей с помощью объявления о практике сертификации и политик сертификации. Альтернативным вариантом является использование «объявлений политики» в спецификации политик веб-сервисов WS-policy.

Приложение В
(справочное)

Расширения структуры сертификата атрибута

Для структуры сертификата атрибута определен ряд расширений. Полную информацию можно найти в ISO/IEC 9594-8.

В.1 Базовые расширения для управления привилегиями

С помощью расширения timeSpecification (спецификация времени) задаются конкретные периоды времени, в течение которых сертификат атрибута может быть использован.

В расширении targetingInformation (целевая информация) перечисляются конкретные серверы или сервисы, которые могут использовать сертификат атрибута.

Расширение userNotice (уведомление пользователя) содержит текст, который может быть прочитан владельцем сертификата или доверяющей стороной.

Расширение acceptablePrivilegePolicies (приемлемые политики привилегий) накладывает ограничение на политики привилегий, с которыми может использоваться сертификат атрибута.

В.2 Расширения для отзыва привилегии

В расширении cRLDistributionPoints (точка распределения списков отозванных сертификатов) можно указать, какие точки распределения списков отозванных сертификатов будут содержать информацию об отзыве сертификата атрибута.

В расширении noRevAvail (отсутствие информации об отзыве) может быть указано, что информация о статусе сертификата атрибута не предоставляется. Обычно такое расширение используется в сертификатах с очень коротким сроком действия.

В.3 Расширения для источников полномочий

Расширение sOAIdentifier (идентификатор источника полномочий) указывает, является ли владелец сертификата источником полномочий. Эта информация может также предоставляться другими средствами.

С помощью расширения attributeDescriptor (описатель атрибута) источник полномочий может публиковать определения атрибутов привилегий и правила доминирования domination rules.

В.4 Расширения для ролей

Расширение roleSpecCertIdentifier (сертификат спецификации роли) содержит ссылку на сертификат, который описывает привилегии, назначенные роли. Сама роль может быть идентифицирована с помощью атрибута роли role, указанного в сертификате атрибута пользователя.

В.5 Расширения для делегирования

С помощью расширения basicAttConstraints (базовые ограничения атрибута) можно указать, могут ли быть делегированы привилегии, указанные в сертификате атрибута.

Если делегирование разрешено, то может быть также указано расширение pathLenConstraint (ограничение длины пути).

С помощью расширения delegatedNameConstraints (ограничение имен делегатов) можно указать пространство имен, которому должны соответствовать все имена владельцев сертификатов атрибута в пути делегирования.

В расширении acceptableCertPolicies (приемлемые политики сертифицирования) можно указать приемлемые политики сертификатов открытых ключей, ассоциированные с сертификатами атрибута в пути делегирования.

Расширение authorityAttributeIdentifier содержит ссылку на орган по присваиванию атрибутов, выпустивший данный сертификат атрибута. Его можно использовать для проверки, что полномочия органа по присваиванию атрибутов достаточны для выпуска сертификата атрибута с таким расширением.

В.6 Расширения, предложенные организацией IETF

Расширение auditIdentity (идентификатор аудита) содержит идентификатор, который может использоваться при аудите транзакции, выполненной с предъявлением данного сертификата. Оно может использоваться, когда в соответствии с требованиями законодательства о персональных данных фактическая идентификация владельца сертификата не должна разглашаться.

С помощью расширения authorityInfoAccess (доступ к информации уполномоченного лица) может быть указано, где можно найти информацию об отзыве сертификата атрибута. В настоящее время единственным механизмом отзыва сертификатов, использующим это расширение, является онлайновый протокол статуса сертификата OCSP.

С помощью расширения aaControls (контроль органа по присваиванию атрибутов) можно указать, какие атрибуты разрешены, а какие запрещены в атрибуте сертификата, выпускаемом органом по присваиванию атрибутов. Это расширение может быть включено в сертификат открытого ключа органа по присваиванию атрибутов. Это расширение может также содержать ограничение длины пути.

Приложение С
(справочное)

Сравнение терминологии

Таблица С.1 — Сравнение терминологии

Терминология стандартов ISO	Терминология других стандартов	Перевод
Пример: ISO/IEC 10181-3	Пример: OASIS XACML	
Access Control Enforcement Function (AEF)	Policy Enforcement Point (PEP)	Точка применения политик
Access Control Decision Function (ADF)	Policy Decision Point (PDP)	Точка принятия решения о политике
Access Control Decision Information (ADI)	Request Context	Контекст запроса
Initiators	Access Requester	Инициатор
Target	Resource	Ресурс
ADI Element (формат не задан)	Attribute (в формате XML)	Атрибут
Initiator ADI (формат не задан)	Subject (в формате XML)	Субъект
Attribute Certificate	(не используется)	Сертификат атрибута
Rule Element (формат не задан)	Condition	Элемент правила
Claimant (не в стандарте ISO/IEC 10181-3)	Access Requester	Заявитель
Context ACI	Environment	Контекст информации контроля доступа
Access Control Policy (формат не задан)	Policy (XML Format)	Политика контроля доступа
Target	Target	Целевой объект
(Не в стандарте ISO/IEC 10181-3)	Role Policy Set	Комплекс политик роли
(Не в стандарте ISO/IEC 10181-3)	Permission Policy Set	Комплекс политик разрешений
Role Specification (не в стандарте ISO/IEC 10181-3)		Спецификация роли
Role Assignment (не в стандарте ISO/IEC 10181-3)		Назначение роли

Приложение D
(справочное)

Примеры управления политикой и представления политики

D.1 Пример объявления на языке SAML

Настоящее приложение не предъявляет требований к представлению политик привилегий в конечной системе. Далее дан пример управления политикой и представления политики с помощью объявлений на языке SAML:

```
<S12:Envelope>
  <S12:Header>
    <wsse:Security>
      <saml:Assertion
        AssertionID="_adf55-01d7-40cc-929f-dbd8372ebdfc"
        IssueInstant="2003-04-17T00:46:02Z"
        Issuer="gost.e-ecolog.ru
        MajorVersion="1"
        MinorVersion="1"
        ...
      </saml:Assertion>
    <wsse:SecurityTokenReference wsu:Id="STR1">
    <wsse:KeyIdentifier wsu:Id="..."
      ValueType= gost.e-ecolog.ru                                    >
      -a75adf55-01d7-40cc-929f-dbd8372ebdfc
    </wsse:SecurityTokenReference>
    </wsse:Security>
  </S12:Header>
  <S12:Body>
  ...
  </S12:Body>
</S12:Envelope>
```

D.2 Представление политики не на языке XML

Далее приведен пример представления политики авторизации на языке логики предикатов:

canActivate(cli, Clinician(org, area))
ra.is-certified-NHS-clinician-cert(cli, org, area, start, end),
is-registration-authority(ra, org),
no-main-role-active(cli),
Current-time() 2 [start, end]

Далее приведен пример представления политики на языке логики первого порядка:

$\forall u$:user, r_i r_j:roles, $i \neq j$
$u \in$ role_memberships(r_i) $\wedge$ $u \in$ role_memberships(r_j)
$\rightarrow r_j \notin$ mutually_exclusive_authorization(r_j)

D.3 Пример представления политики на языке XACML

В следующем примере, показывающем представление политики на языке XACML, элемент <Apply> выполняет математическую функцию «urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration», вычисляющую дату шестидесятилетия пациента. Он также иллюстрирует использование предикатов в форме функции с идентификатором functioned, равным «urn:oasis:names:tc:xacml:1.0:function:and». В этом примере одна функция вложена в элемент <Condition>, а на другую есть ссылка в элементе <VariableDefinition>.

```
<?xml version="1.0" encoding"UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os" xmlns:xacml-
context="urn:oasis:names:tc:xacml:2.0:context:schema:os"
xmlns:xsi="gost.e-ecolog.ru                                    "
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:osgost.e-ecolog.ru
open.org/xacml/access_control-xacml-2.0-policy-schema-os.xsd"
xmlns:xf="gost.e-ecolog.ru                                    "
xmlns:md="http:www.med.example.com/schemas/record.xsd"
```

```
PolicyId="urn:oasis:names:tc:xacml:2.0:example:policyid:2"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
        <PolicyDefaults>
          <XPathVersion>gost.e-ecolog.ru                                                    >
        </PolicyDefaults>
        <Target/>
        <VariableDefinition VariableId="17590035">
          <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:date-less-or-equal">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
              <EnvironmentAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-date"
        DataType="gost.e-ecolog.ru                                    >
          </Apply>
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-add-yearMonthDuration">
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:date-one-and-only">
              <AttributeSelector
RequestContextPath="//md:record/md:patient/md:patientDoB/text()"
DataType="gost.e-ecolog.ru                                    >
          </Apply>
          <AttributeValue DataType="gost.e-ecolog.ru                                                0 02
0816#yearMonthDuration">
            <xf:dt-yearMonthDuration> P16Y</xf:dt-yearMonthDuration>
          </AttributeValue>
        </Apply>
      </Apply>
    </VariableDefinition>
    <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:ruleid:2" Effect="Permit">
        <Description>
Лицо может читать любую медицинскую карту в пространстве имён gost.e-ecolog.ru                                , кото-
рую оно создало или которую ведёт, при условии, что пациенту меньше 16 лет</Description>
          <Target>
            <Resources>
              <Resource>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                  <AttributeValue
DataType="gost.e-ecolog.ru
Value>
                  <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:resource:target-namespace"
DataType="gost.e-ecolog.ru                                    >
                </ResourceMatch>
                <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:xpath-node-match">
                  <AttributeValue DataType="gost.e-ecolog.ru                                                "> /md:record
</AttributeValue>
                <ResourceAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
DataType="gost.e-ecolog.ru                                    >
              </ResourceMatch>
            </Resource>
          </Resources>
          <Actions>
            <Action>
              <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="gost.e-ecolog.ru
001/XMLSchema#string">read</AttributeValue>
                <ActionAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
DataType="gost.e-ecolog.ru                                    >
              </ActionMatch>
            </Action>
          </Actions>
      </Target>
```

```
    <Condition>
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
            <SubjectAttributeDesignator
AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:parent-guardian-id"
DataType="gost.e-ecolog.ru                                    >
          </Apply>
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
            <AttributeSelector RequestContextPath="//xacml-context:Resource/xacml-
context:ResourceContent/md:record/md:parentGuardian/md:parentGuardianId/text()"
DataType="gost.e-ecolog.ru                                    >
          </Apply>
        </Apply>
        <VariableReference VariableId="17590035"/>
      </Apply>
    </Condition>
  </Rule>
</Policy>
```

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO 8601:2004	—	*
ISO/IEC 9594-8:2001	—	*
ISO/IEC 10181-3:1996	—	*
ISO/TS 21298:2008	—	*
ASTM E2595-07	—	*
ASTM E1762-07	—	*
ASTM E1986-98	—	*
ASTM E2212-02a	—	*
OASIS, eXtensible Access Control Markup Language (XACML) v2.0, February 2005	—	*
OASIS, XACML Profile for Role Based Access Control (RBAC): Committee Draft 01 (normative; 13 February 2004)	—	*
OASIS, Security Assertion Markup Language (SAML), Version 2.0, March 2005 OASIS 200306, Service Provisioning Markup Language (SPML), V1.0, October 2003	—	*
* Соответствующий межгосударственный стандарт отсутствует.		

Библиография

[1] HITSP Access Control Transaction Package V. 1.1.1 (September 27, 2007)

[2] BLOBEL B., NORDBERG R., DAVIS J.M., PHAROW P. Modelling privilege management and access control.// International Journal of Medical Informatics? 75, 8 (2006). pp. 597—623

[3] ISO/TS 13606:2009, Health informatics — Electronic health record communication — Part 4: Security

[4] BLOBEL B. Assessment of Middleware Concepts Using a Generic Component Model.// Proceedings of the Conference «Toward an Electronic Health Record Europe '97», pp. 221—228. October 20-23, 1997, London

[5] ARLOW J., NEUSTADT I. UML2 and the Unified Process, 2nd Edition. Upper Saddle River: Addison-Wesley; 2005

[6] BLOBEL B., ROGER-FRANCE F. A Systematic Approach for Analysis and Design of Secure Health Information Systems.// International Journal of Medical Informatics, 62 (3) (2001), pp. 51—78

[7] BLOBEL B. Analysis, Design and Implementation of Secure and Interoperable Distributed Health Information Systems./ Series «Studies in Health Technology and Informatics» Vol. 89. IOS Press, Amsterdam 2002

[8] BLOBEL B. Concept representation in health informatics for enabling intelligent architectures. In: HASMAN, A., HAUX, R., VAN DER LEI, J., DE CLERCQ, E., ROGER-FRANCE, F. (Edrs.): Ubiquity: Technologies for better health in aging societies, pp. 285—291. Series «Studies in Health Technology and Informatics», Vol. 124. IOS Press, Amsterdam 2006

[9] BEALE T. Health Information Standards Manifesto, Rev. 2.0. Mooloolah: Deep Thought Informatics Pty Ltd.; 2001.

[10] BODENREIDER O. The Unified Medical Language System. Tutorial Handouts. Geneva: MIE 2005 [11] Object Management Group: gost.e-ecolog.ru [12] OASIS: gost.e-ecolog.ru

[13] CHADWICK D.W. et al. Role-Based Access Control with X.509 Attribute Certificates. IEEE Internet Computing, 2003, pp. 62-69

[14] FERRAIOLO D.F., SANDHU R., GAVRILA S., KUHN D.R., CHANDRAMOULI R. Proposed NIST Standard for Role-Based Access Control./ ACM Transactions on Information and System Security, Vol. 4 No. 3, August 2001, pp. 224—274 France

[15] Health Level 7, Inc.: Role-Based Access Control (RBAC), 2007. gost.e-ecolog.ru

[16] KIRSCHNER B.A., HACKER T.J., ADAMSON W.A., ATHEY B.D. Walden: A Scalable Solution for Grid Account Management./ 5th IEEE/ACM International Workshop on Grid Computing (GRID '04), 2004, pp. 102—109

[17] STOWE G. A Secure Network Node Approach to the Policy Decision Point in Distributed Access Control. Thesis, Tech Report TR2004-502, Dartmouth College Department of Computer Science, 2004

[18] National Research Council. Computers at Risk: Safe Computing in the Information Age. National Academy Press, 1991, Washington, DC

[19] BOWEN P., HASH J., WILSON M. Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100, NIST Computer Security Division, Gaithersburg, October 2006

[20] KENT K., SOUPPAYA M. Guide to Computer Security Log Management. NIST Special Publication 800-92, NIST Computer Security Division, Gaithersburg, September 2006

[21] Integrating the Healthcare Enterprise, Inc.: IHE IT Infrastructure Technical Framework, Vol. 1 (ITI TF-1) Integration Profiles, Rev. 3.0. ACC/HIMSS/RSNA, 2006, p. 55

[22] DICOM: Digital Imaging and Communications in Medicine (DICOM) Supplement 95: Audit Trail Messages, Trial Standard, 2004

[23] WELCH V. et al. X.509 Proxy Certificates for Dynamic Delegation. 3rd Annual PKI R&D Workshop, 2004

[24] FISCHER A. Electronic Document Authorization. Proceedings of the 13th National Computer Security Conference, 1990

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

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

[27] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[28] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[29] ISO/IEC 9798 (all parts), Information technology — Security techniques — Entity authentication

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

[31] ISO/IEC 10745, Information technology — Open Systems Interconnection — Upper layers security model

[32] ISO/IEC 10746 (all parts), Information technology — Open Distributed Processing — Reference Model [33] ISO/IEC TR 13594, Information technology — Lower layers security

[34] ISO/IEC 11770-1:1996, Information technology — Security techniques — Key management — Part 1: Framework

[35] ISO 17090 (all parts), Health informatics — Public key infrastructure

[36] ISO/TS 21091, Health informatics — Directory services for security, communications and identification of professionals and patients

[37] ISO 22857, Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information

[38] EN 13608-1:2007, Health informatics — Electronic health record communication — Part 1: Reference model

[39] ASTM E1986, Standard Guide for Information Access Privileges to Health Information list of "Healthcare Personnel that Warrant Differing Levels of Access Control"

[40] ASTM E1714-07, Standard Guide for Properties of a Universal Healthcare Identifier (UHID)

[41] ASTM E1985-98, Standard Guide for User Authentication and Authorization

[42] ASTM E2085-00a, Standard Guide on Security Framework for Healthcare Information

[43] ANSI INCITS 359-2004 19, Role Based Access Control, February 2004

[44] OASIS, Universal Description, Discovery and Integration, v3.0.2 (UDDI), February 2005

[45] RFC 3198, Terminology for policy-based management. Available (2009-09-16) at: gost.e-ecolog.ru html

[46] ANSI X9.45-1999. Enhanced management controls using digital signatures and attribute certificates

[47] IETF RFC 3280, Internet X.509 public key infrastructure certificate and certificate revocation list (RL) profile

[48] RFC 822, Standard for the format of ARPA internet text messages. Available (2009-09-16) at: gost.e-ecolog.ru html/rfc822

[49] RFC 2634, Enhanced security services for S/MIME. Available (2009-09-16) at: gost.e-ecolog.ru

[50] ITU-T X.411, Information technology — Message Handling Systems (MHS)— Message Transfer System: Abstract Service Definition and Procedures SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS Message Handling Systems

[51] RFC 3881, Security audit and access accountability message XML data definitions for healthcare applications. Available (2009-09-16) at: gost.e-ecolog.ru

УДК 004:61:006.354 МКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, передача электронной медицинской карты, информационная безопасность

Редактор *Е.В. Яковлева*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.01.2019. Подписано в печать 31.01.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 6,73.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru