Международный союз электросвязи

МСЭ-Т X.1255

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2013)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Управление определением идентичности

Структура обнаружения информации по управлению определением идентичности

Рекомендация МСЭ-Т X.1255

ITU-T

International Telecommunication Union

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1255

Структура обнаружения информации по управлению определением идентичности

Резюме

Цель Рекомендации МСЭ-Т X.1255 заключается в обеспечении структуры открытой архитектуры, в которой возможно обнаружение информации по управлению определением идентичности. Эта информация IdM заведомо будет представляться различными способами и обеспечиваться различными структурами доверия или другими системами IdM, в которых используются различные схемы метаданных. Настоящая структура позволит, например, объектам, работающим в среде одной системы IdM, точно определять идентификаторы других систем IdM. В отсутствие способности обнаруживать такую информацию пользователи и организации (или программы, работающие от их имени) вынуждены определять оптимальный способ установления надежности и аутентичности соответствующей идентичности, будь то для пользователя, системного ресурса, информации или иных объектов. Решать вопрос, базируясь на этой информации, о том, стоит ли для этих целей полагаться на данную структуру доверия или другую систему IdM, предстоит пользователю или организации. К основным компонентам описываемой в настоящей Рекомендации структуры относятся: 1) модель данных цифрового объекта; 2) протокол интерфейса цифрового объекта; 3) одна или несколько систем идентификаторов/разрешения; и 4) один или несколько регистров метаданных. Эти компоненты составляют основу структуры открытой архитектуры.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1255	04.09.2013 г.	17-я

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1255

Структура обнаружения информации по управлению определением идентичности

1 Сфера применения

Обнаружение информации по управлению определением идентичности связано с необходимостью наличия возможности получать соответствующую информацию об идентификаторах, включая идентификаторы, в которых используется синтаксис адреса электронной почты, и идентификаторы, которые являются универсальными указателями ресурса (URL), а также постоянные идентификаторы. Такое обнаружение является ключевым элементом функциональной совместимости неоднородных информационных систем.

Сферу применения настоящей Рекомендации составляет структура, которая:

- позволяет обнаруживать относящуюся к идентичности информацию и определять ее происхождение, включая информацию, идентифицируемую как услуги, процессы и объекты;
- позволяет обнаруживать атрибуты относящейся к идентичности информации, включая, в том числе, визуальные логотипы и воспринимаемые человеком наименования сайтов;
- позволяет обнаруживать атрибуты и функциональные возможности приложений;
- описывает модель данных и протокол в целях обеспечения функциональной совместимости на мета-уровне для представления, доступа и обнаружения упомянутой выше информации в неоднородной среде IdM.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ISO 8601] ISO 8601 (2004), *Data elements and interchange formats – Information interchange – Representation of dates and times*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 объект (entity) [b-ITU-T Y.2720]: Все, что существует самостоятельно и является различимым и может быть идентифицировано уникальным образом. В контексте IdM примерами объектов являются абоненты, пользователи, сетевые элементы, сети, программные приложения, услуги и устройства. Любой объект может иметь несколько идентификаторов.

3.1.2 поставщик данных идентичности (identity provider) [b-ITU-T Y.2720]: Объект, который создает и поддерживает надежную информацию, подтверждающую идентичность других объектов (например, пользователей/абонентов, организаций и устройств), и управляет такой информацией, а также предоставляет базирующиеся на идентичности услуги на основе доверия, деловых отношений и других типов отношений.

3.1.3 полагающаяся сторона (relying party) [b-ITU-T Y.2720]: Объект, который полагается на представленную или заявленную идентичность запрашивающего/утверждающего объекта.

3.1.4 доверие (trust) [b-ITU-T Y.2720]: Мера того, насколько полагаются на характер, возможности, сильные стороны или истинность кого-либо или чего-либо.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.2.1 ассоциация (association): Отношение, если таковое существует, между двумя идентифицированными объектами.

3.2.2 цифровой объект (digital object): Машинно-независимая структура данных, состоящая из одного или нескольких элементов, разбор которых могут выполнить разные информационные системы; эта структура помогает обеспечивать функциональную совместимость разных информационных систем в интернете.

3.2.3 обнаружение (discovery): Действие или процесс поиска или определения местоположения информации о цели, то есть получение знаний, относящихся к цели.

3.2.4 элемент (element): Часть цифрового объекта, состоящая из пары тип-значение, в которой тип представляется различимым постоянным идентификатором, а значение является соответствующей цифровой информацией для данного типа.

3.2.5 федеративные регистры (federated registries): Набор функционально совместимых регистров, которые регистрируют метаданные и участвуют в общей совокупности методов совместного использования информации при обеспечении надежности и с использованием общепонятного формата.

3.2.6 идентификатор (identifier): Последовательность битов, используемая для получения информации о состоянии идентифицируемого объекта; как правило, это выполняется путем применения соответствующей системы разрешения.

3.2.7 управление определением идентичности (identity management): Средства, с помощью которых может быть проверена информация управления определением идентичности, будь то для пользователя, системного ресурса, информации или иных объектов.

3.2.8 информация управления определением идентичности (identity management information): Относящаяся к идентичности информация, включая все типы метаданных, связанных с идентичностью, происхождением, ассоциацией и доверием.

3.2.9 метаданные (metadata): Структурированная информация, которая относится к идентичности пользователей, систем, процессов, ресурсов, информации и других объектов.

3.2.10 постоянный идентификатор (persistent identifier): Уникальный идентификатор, который осуществляет разрешение в информацию о состоянии цифрового объекта и который является различимым в течение, по крайней мере, срока существования данного цифрового объекта.

3.2.11 происхождение (provenance): Информация, относящаяся к любому источнику информации, включая сторону или стороны, участвовавшие в создании, введении и/или гарантировании этой информации.

3.2.12 регистр (registry): Механизм, предназначенный для регистрации метаданных о цифровых объектах и хранения схем метаданных, который обеспечивает возможность поиска регистра для постоянных идентификаторов на основе использования схем метаданных.

3.2.13 репозиторий (repository): Интерфейс, который принимает депозиты цифровых объектов, обеспечивает возможность их сохранения и обеспечивает безопасный доступ к цифровым объектам через их идентификаторы.

3.2.14 система разрешения (resolution system): Система, которая принимает идентификаторы, известные системе как входные данные, и предоставляет соответствующую информацию о состоянии идентифицируемого объекта.

3.2.15 точка взаимодействия (touch point): Регистр в системе федеративных регистров, который выбран для интерфейса с назначенным регистром в другой федерации, как правило, для целей однорангового обмена.

3.2.16 структура доверия (trust framework): Система IdM, в которой каждая из различных сторон транзакции создает для своих контрагентов по этой транзакции набор поддающихся проверке обязательств; и эти обязательства непременно включают: a) средства управления, которые помогают обеспечить выполнение обязательств; и b) средства защиты при невозможности выполнения этих обязательств.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Program Interface		Интерфейс прикладного программирования
Bits	Binary Digits		Двоичные цифры
BNF	Backus Normal Form	БНФ	Бэкусова нормальная форма
DE	Digital Entity		Цифровой объект
DEIP	Digital Entity Interface Protocol		Протокол интерфейса цифрового объекта
DNA	Deoxyribonucleic acid	ДНК	Дезоксирибонуклеиновая кислота
HTTP	Hypertext Transfer Protocol		Протокол передачи гипертекста
ID	Identifier		Идентификатор
IdM	Identity Management		Управление определением идентичности
IdP	Identity Provider		Поставщик данных идентичности
MAC	Media Access Control		Управление доступом к среде
P2P	Peer-to-Peer		Одноранговый
PKI	Public Key Infrastructure		Инфраструктура открытых ключей
RP	Relying Party		Полагающаяся сторона
TCP	Transmission Control Protocol		Протокол управления передачей
TF	Trust Framework		Структура доверия
URL	Uniform Resource Locator		Универсальный указатель ресурса
XML	Extensible Markup Language		Расширяемый язык разметки

5 Условные обозначения

Отсутствуют.

6 Рекомендация

Назначением настоящей Рекомендации является структура открытой архитектуры для обеспечения обнаружения информации управления определением идентичности. В Рекомендации рассматриваются следующие вопросы:

a) концепция доверия, которая является важным аспектом управления определением идентичности;

b) информация о доверии, которая может использоваться для определения степени доверия к каждой информационной составляющей IdM;

c) федеративные регистры для обнаружения;

d) архитектура функциональной совместимости для федерации; и

e) рассмотрение иерархической и одноранговой федерации.

Обнаружение информации управления определением идентичности базируется на использовании метаданных, полученных их регистра или системы федеративных регистров. Структура включает наличие средств разрешения постоянных идентификаторов. В целом федеративные регистры будут управляться несколькими сторонами и поддерживать модель данных цифрового объекта для представления записей метаданных и протокол интерфейса цифрового объекта для обеспечения функциональной совместимости этих регистров. Предполагается использование нескольких схем, и каждый регистр должен представлять подробные данные о своих схемах метаданных, которые поддерживаются общедоступным и/или частным образом с помощью их соответствующих постоянных идентификаторов. Постоянные идентификаторы частным образом поддерживаемых схем при необходимости могут стать общедоступными или они могут оставаться частными вместе с

соответствующими схемами метаданных для ограниченного использования в пределах ограниченных сообществ.

В Дополнениях I и II, соответственно, представлен обзор сценариев использования и пример описания БНФ для записи типа (БНФ – это стандартная нотация для представления контекстно-свободной грамматики).

6.1 Понятия доверия

Слово "доверие" – профессиональный термин, который имеет ряд коннотаций. Доверие к частному лицу или процессу означает, как правило, некую степень уверенности в определенном результате события, даже в отсутствие точного описания такого события. Создание системы обнаружения, однако, потребует дополнительного описания. Для простоты понимания: утверждение, что A может доверять B, не означает, что A может доверять B в отношении всех возможных результатов события. Доверие к B в том, что за выполненный платеж будет предоставлена услуга, не то же самое, что доверие к B в том, что этот платеж будет сохранен в тайне или что не будут обнародованы имена плательщиков.

Наиболее важным вопросом в структуре доверия является управление определением идентичности, то есть, что стороны любой данной транзакции действительно являются теми, кем они себя объявили. Однако уверенность в результате данной транзакции с участием данной стороны зависит не только от идентичности этой стороны, но также и от других атрибутов заявлений и утверждений, сделанных этой стороной. Для унифицированной оценки этих атрибутов необходим словарь или набор метрик, которые могут быть применены к данным атрибутам. Такие меры и описания могут применяться третьими сторонами, которые являются рейтинговыми агентствами структур доверия, или они могут усредняться по группам рейтингов пользователей, как это делается в рекомендательных системах и других приложениях "краудсорсинга". Рекомендуемые категории этих мер и описаний представлены ниже.

Сила: Степень надежности. Какова вероятность того, что данная сторона выполнит то, что она обещала выполнить? Насколько вероятно, что утверждение идентичности (например, "я – автор этого программного обеспечения и роялти принадлежит мне) является верным? Это, скорее всего, должно обозначаться как цифровая или буквенная категория.

Классификация: Какой тип надежности представляется в утверждении? Могут ли быть установлены стандартные категории? Идентичность – это категория в самой себе. Другие категории могут включать кредитоспособность (например, какова вероятность того, что данная сторона будет действовать в ходе финансовой транзакции так, как обещала), конфиденциальность (какова вероятность того, что конфиденциальная информация, которую истребует данная сторона, не будет раскрыта) и авторитетность (например, какова вероятность того, что информация, полученная от данной стороны, является точной). Возможны другие классы высокого уровня и для каждого класса возможны более узкие уровни детализации.

Длина цепочки доверия: Некоторые доверенные транзакции базируются на цепочке доверия, которая часто представляется в категориях иерархии сертификатов или уровней программного обеспечения с цифровой подписью. Эта концепция применима в целом ко всем областям доверия: чем длиннее цепочка доверенных утверждений, которая отслеживается до какой-либо исходной точки доверия, тем ниже окончательный уровень доверия. Мера длины такой цепочки может быть ключевой мерой надежности любой идентичности или другого утверждения.

Все эти атрибуты (и многие другие) могли бы быть кандидатами на включение в записи метаданных, описывающие поставщиков данных идентичности, полагающиеся стороны и любые другие компоненты, участвующие в доверенных транзакциях.

6.2 Информация о доверии

Ниже рассматриваются три разных аспекта информации о доверии в связи с функциями и действиями, являющимися частью федеративного обнаружения, а также функциями и действиями участвующих объектов.

6.2.1 Информация о доверии в ответ на запрос обнаружения

Обеспечение возможности обнаружения информации управления определением идентичности является основной задачей открытой архитектуры, представленной в настоящей Рекомендации, однако, определение доверия возлагается на пользователя. Дополнительные функциональные

возможности или услуги могут обеспечиваться в рамках этой архитектуры в форме необязательных компонентов/модулей (программных и/или аппаратных). В этом смысле архитектура может включать структуру доверия как дополнительную возможность, а также улучшать/расширять ответ на запрос обнаружения, включая информацию о доверии или даже поддерживая определение доверия. Внешние объекты будут иметь возможность определять, хотят ли они получать эту информацию о доверии напрямую. Они могут выбрать деактивацию этой функции и осуществлять сбор информации о доверии собственными силами или даже из своих собственных источников, с тем чтобы выполнить определение доверия.

6.2.2 Доверие к системе обнаружения

Система обнаружения должна быть доверенной, так чтобы внешние стороны испытывали уверенность, используя ее возможности по регистрации информации управления определением идентичности или оценке этой информации. Такой тип доверия достигается разными способами, в том числе путем установления специальных методов, включая соответствующие стратегии и процедуры для целей обеспечения надежности. К ним могут относиться компоненты, реализуемые как часть структуры, действия (меры), предпринимаемые в отношении неверно функционирующих компонентов или внешних сторон, и адаптация жестких рамок безопасности и конфиденциальности. Вместе с тем определение точной методики достижения такого типа доверия не входит в сферу применения настоящего документа.

6.2.3 Доверяющие внешние стороны

Архитектура должна обеспечивать стратегии и процедуры, поощряющие надежные внешние стороны использовать ее для целей регистрации информации. По соображениям безопасности составляющие объекты, которые непосредственно участвуют в регистрации информации управления определением идентичности, должны иметь возможность контролировать данные, вводимые в систему, и определять и/или исключать случаи, когда злонамеренные стороны пытаются зарегистрировать ложную информацию.

Анонимные запросы следует принимать, но их большое количество может не привести к получению пригодных ответов, если только идентичность отдельных авторов запросов не известна заранее в результате применения каких-либо иных способов. В таких случаях следует обеспечивать возможность валидации идентичности с помощью возможности управления определением идентичности, которая применяется ко всем компонентам, включая пользователей/авторов запросов. В рамках этой структуры уполномоченные и признанные поставщики данных идентичности выделяют каждому компоненту уникальный постоянный идентификатор, который может быть разрешен в соответствующую информацию об этом компоненте. Как указано выше, не делается допущений о том, как какой-либо компонент конкретного экземпляра будет определять степень доверия к данной информации.

В случае большого числа запросов до представления ответа должна быть выполнена валидация идентичности автора запроса (внешняя сторона, направляющая запрос на обнаружение). В общем случае, все авторы запросов будут оцениваться до осуществления любых дальнейших действий. Архитектура не предполагает применения в ее рамках какой-либо возможности принятия решений; однако до составления окончательного ответа на запрос об обнаружении может быть задействован тот или иной внешний механизм поддержки решений, с тем чтобы получить заранее разрешение от автора идентичности.

6.3 Федеративные регистры для обнаружения

Система федеративных регистров для обнаружения описывается в настоящей Рекомендации в целях обеспечения возможности обнаружения и оценки метаданных и другой информации об идентификаторах, а также структурах доверия и других системах IdM. Федеративные регистры могут работать совместно, с тем чтобы использовать на коллективной основе свои объекты метаданных с учетом любых применимых ограничений. Фактическая информация, которая соответствует этим метаданным, может храниться в их соответствующих регистрах (если такое хранение разрешено), в одном или нескольких распределенных репозиториях, и в некоторых случаях информация, соответствующая этим метаданным, может быть полностью недоступной в интернете. В таком случае это ограничение будет, как правило, определяться разрешением идентификатора в соответствующую информацию состояния объекта, однако регистр может также выбрать вариант предоставления и этой информации.

В рамках системы федеративных регистров данный регистр может вносить запись метаданных данного объекта во второй регистр либо как полную копию оригинальной записи метаданных, либо как резюме такой оригинальной записи. Представление будет включать оригинальную запись или вариант оригинальной записи, описанный таким образом, который определяет, откуда эта запись была получена, и характеризует тип сообщества или домена, представленного этим регистром. Тот же исходный регистр может, следовательно, служить как междоменная точка сбора для большого числа других регистров и предоставлять услугу поиска, которая может направить осуществляющую поиск сторону к другим регистрам для сбора дополнительной информации. Такие точки сбора иногда называются точками взаимодействия.

Являющийся компонентом архитектуры регистр разработан на основе нескольких ключевых концепций. Наряду с тем, что для каждого зарегистрированного объекта требуется выделение идентификатора, записи метаданных в регистре сами структурированы как цифровые объекты, и каждая имеет связанный с ним идентификатор. Это позволяет осуществлять обращение к записям метаданных по отдельности, и их идентификаторы разрешаются в информацию о текущем состоянии объектов метаданных, даже если записи перемещаются из одного регистра в другой или доступны из нескольких регистров.

Архитектура никоим образом не ограничивает число объектов метаданных, которые могут быть зарегистрированы для одного цифрового объекта. Может быть желательным создание нескольких объектов метаданных для той же информации – для просмотра с разных точек зрения, для разной аудитории и т. д. Управление этими объектами метаданных существенно упрощено использованием уникальных и постоянных идентификаторов: например, легко можно определить, относятся или не относятся две записи метаданных к той же исходной информации. Кроме того, могут быть созданы дополнительные объекты для соотнесения между собой отдельных объектов метаданных таким образом, который в противном случае не был бы возможен с помощью поиска по отдельным объектам.

Архитектура позволяет устанавливать отношения "многие ко многим", в обоих направлениях, между репозиториями и регистрами. Данный репозиторий может вносить метаданные тех же объектов в несколько регистров, и данный регистр может принимать метаданные от нескольких репозиториев. Сбор метаданных из нескольких репозиториев в один регистр обеспечивает возможность федеративного объединения таких репозиториев. Возможность введения этими репозиториями метаданных о тех же объектах в несколько регистров позволяет одному репозиторию быть частью нескольких федераций, различающихся, вероятно, тем, что они обслуживают разные сообщества, используют разные схемы метаданных, разные способы индексации и поиска и другие возможности.

Наконец, экземпляр регистра может быть объединен в федерацию с другими регистрами. Несколько регистров могут передавать один другому свои объекты метаданных или объекты, которые являются функцией оригинальных записей метаданных. Данный регистр, назовем его Reg1, может внести запись метаданных для данного объекта во второй регистр, назовем его Reg2, либо как полную копию оригинальной записи метаданных, либо как резюме такой оригинальной записи. Представление будет включать оригинальную запись или вариант оригинальной записи, введенный в цифровой объект (DE) таким образом, который определяет его как поступивший из Reg1 и характеризует тип сообщества или домена, представленного Reg1. Если Reg1 уже объединен в федерацию с Reg2, тогда Reg2 может служить как междоменная точка сбора для большого числа других регистров, таких как Reg1, и предоставлять услугу поиска, которая может направить осуществляющую поиск сторону к другим регистрам или напрямую к самим DE, в зависимости от метода комбинирования и индексирования потенциально неоднородных записей метаданных.

Притом что настоящая Рекомендация посвящена управлению определением идентичности, такая система может также служить для обнаружения информации других типов в комплексных распределенных системах в интернете, таких как использующие "облачные вычисления" или "интернет вещей". Информация разрешения в системе федеративных регистров поступает из отдельных систем IdM. Использование предусмотренного в федерации механизма обнаружения сделает возможным функциональную совместимость систем IdM, в более общем смысле, и обеспечит информацию, пригодную для объекта, с тем чтобы получать сведения об остальных системах IdM и формировать доверие при использовании идентификаторов из этих систем.

Базовую технологию регистрации использует большое число групп, часть которых пользуются версиями на основе открытых исходных кодов, а другие – разрабатывают проприетарные адаптации на основе общепринятых спецификаций. Федерация образуется с помощью протоколов для совместного использования информации. Важной частью будущей работы на основе настоящей Рекомендации станет описание, а затем формализация этих спецификаций, определение пригодных протоколов и процедур вместе с надлежащими схемами метаданных и определение общепринятого подхода к обеспечению в надлежащих случаях конфиденциальности. Метод принятия решения о выборе или доверии к данной системе IdM не входит в сферу применения настоящей Рекомендации.

7 Архитектура функциональной совместимости для федеративных регистров

Система федеративных регистров в настоящей Рекомендации базируется на открытой архитектуре, которая обеспечивает возможность функциональной совместимости произвольно выбранных информационных систем. Архитектура предоставляет средства для аутентификации информации и для доступа к информации, которая структурирована в виде цифровых объектов и хранится в стандартных системах хранения данных большинства типов. Цифровой объект – это общая структура данных, которая делает возможной функциональную совместимость систем в интернете; элементы DE являются цифровым материалом, например типизированные данные, в том числе уникальный постоянный идентификатор для этого материала.

В управлении DE используются три компонента архитектуры. Каждый из этих компонентов может использоваться сам по себе, однако они дополняют друг друга и вместе обеспечивают для интернета возможность распределенного и масштабируемого управления информацией. Этими компонентами являются:

a) масштабируемая и распределенная система идентификаторов для идентификации DE и для разрешения идентификаторов;

b) репозитории для доступа к цифровым объектам и управления ими; и

c) регистры для федеративного поиска и обнаружения. Используя эти компоненты, результирующая распределенная система может управляться через спецификации интерфейсов и протоколов, а не через осуществляемое техническое обслуживание конкретных компонентов.

Цифровые объекты являются центральным элементом, вокруг которого организуются и управляются все другие компоненты и услуги. Цифровые объекты не заменяют существующие форматы и структуры данных, но обеспечивают общее средство для представления этих форматов и структур, делая возможной их унифицированную интерпретацию и, следовательно, их перемещение между различными неоднородными информационными системами и при изменениях в системах с течением времени. Эта модель, несмотря на свою простоту в основе, нетривиальна в своей детальной реализации и включает протокол для взаимодействия DE через репозитории. В настоящей Рекомендации все метаданные соответствуют модели данных DE для целей функциональной совместимости и удобства пользования.

Описанные ниже модель данных DE и протокол интерфейса цифрового объекта для доступа к DE, объединенные с системой идентификаторов и/или системой разрешения и подходом на основе регистра/репозитория для доступа к DE, формируют основу открытой архитектуры. Все вместе эти компоненты обеспечивают возможность долговременного управления информацией, структурированной в форме цифровых объектов, путем уникальной и постоянной их идентификации, создавая метод получения информации о текущем состоянии объекта, создавая услугу для получения или иного использования объектов, а также средство определения идентификаторов DE на основе информации в регистрах метаданных.

7.1 Модель данных цифрового объекта

Описанная в настоящем документе модель данных DE обеспечивает единообразный метод представления записи метаданных как DE и может также использоваться для представления в форме DE информации других типов. Это логическая модель, которая допускает несколько форм кодирования и хранения и позволяет использовать одну точку привязки (то есть идентификатор) для информации многих типов, которая может быть доступной в интернете. Каждый DE имеет свой

собственный набор атрибутов, определяемый пользователем набор атрибутов, которые входят в состав одного или нескольких элементов, и ни одного или несколько дополнительных элементов, содержащих такую информацию, как текст, видео или изображения, представленные в цифровой форме. Все эти элементы могут быть доступными через точно определенную спецификацию DEIP (см. раздел 7.2), которая включает возможность аутентификации с использованием системы безопасности на основе открытых ключей, и, возможно, другие средства аутентификации с использованием API более высоких уровней, что может быть реализовано с помощью репозиториев DE. Это обеспечивает доступ к DE при соблюдении конфиденциальности и безопасности.

Важнейшим фиксированным атрибутом DE является связанный с ним уникальный постоянный идентификатор, который может быть разрешен в информацию о текущем состоянии DE, включая его местоположение(я), доступ, средства контроля и валидацию, путем представления запроса на разрешение в систему разрешения. Примерами других собственных атрибутов элементов DE являются дата последнего изменения, дата создания и размер. Расширяемые пользовательские атрибуты могут устанавливаться пользователями, имеющими надлежащие допуски.

Атрибуты, которые специально не предусмотрены моделью данных DE, включают владение, условия и положения аутентификации и доступа. Эти атрибуты составят важную часть большинства реализаций DE; однако единое решение представляется маловероятным. Информация о владении и управлении доступом скорее всего будет содержаться в расширяемых пользователем атрибутах DE или в отдельных элементах данных. Это обеспечивает общий способ работы с различными схемами владения и управления информацией, а также схемами множественной аутентификации и авторизации, не делая допущения о том, что во всех доменах и сообществах пользователей будет использоваться единый подход.

Сочетание стандартной модели данных, обозначенного протокола для взаимодействия с этой моделью данных и системы идентификаторов/разрешения обеспечивает ключевой ингредиент согласованного долговременного управления информацией в интернете. Система разрешения должна быть распределенной, надежной, высокопроизводительной системой разрешения, спланированной для обеспечения возможности постоянной ссылки на цифровые объекты в течение длительных периодов времени и при изменении местоположения, методов доступа, владения и других изменяемых атрибутов.

Базовая способность обнаружения информации IdM является результатом использования компонента регистрирования, который включает репозиторий. Функцией отдельного регистра является объединение в федерацию наборов DE, что дает возможность пользователям и приложениям осуществлять поиск и навигацию по всей совокупности зарегистрированных объектов. Репозитории, содержащие наборы DE, могут вносить метаданные по DE, за которые они несут ответственность перед одним или несколькими регистрами. Один регистр может собирать метаданные от нескольких репозиториев, а один репозиторий может передавать метаданные нескольких регистрам. Регистры могут обеспечивать функции поиска и отчетности по представленным объектам и обеспечивать точку входа в структурированную совокупность DE и репозиториев.

Возможны ситуации, когда регистры, строго говоря, не требуются, например в случае если прямая ссылка на DE в форме его идентификатора заложена в другом DE или в сообщении или в другом документе. Во многих случаях, однако, конечный пользователь или автоматический процесс, действующий от имени пользователя, не будет знать идентификатора, с которым следует начинать работу, и для обнаружения необходимой ссылки ему потребуются различные виды поиска или процесс сортировки. Даже если пользователь знает идентификатор, этому пользователю может быть неизвестен порядок разрешения этого идентификатора или интерпретации результатов разрешения. Запись о существовании DE в регистрах может помочь решить эту задачу самым общим способом.

Путем определения операций, взаимодействующих с определенной моделью данных, могут быть построены цифровые объекты и использоваться для представления большинства типов структурированной информации. Этот вопрос рассматривается в следующем разделе. Стандартная модель данных цифрового объекта показана на рисунке 1. Представление объектов в форме, не зависящей от реализации конкретных элементов соответствующей системы хранения, является важным параметром функциональной совместимости, поскольку оно обеспечивает возможность нормирования нескольких форматов и способов хранения к единой логической модели.

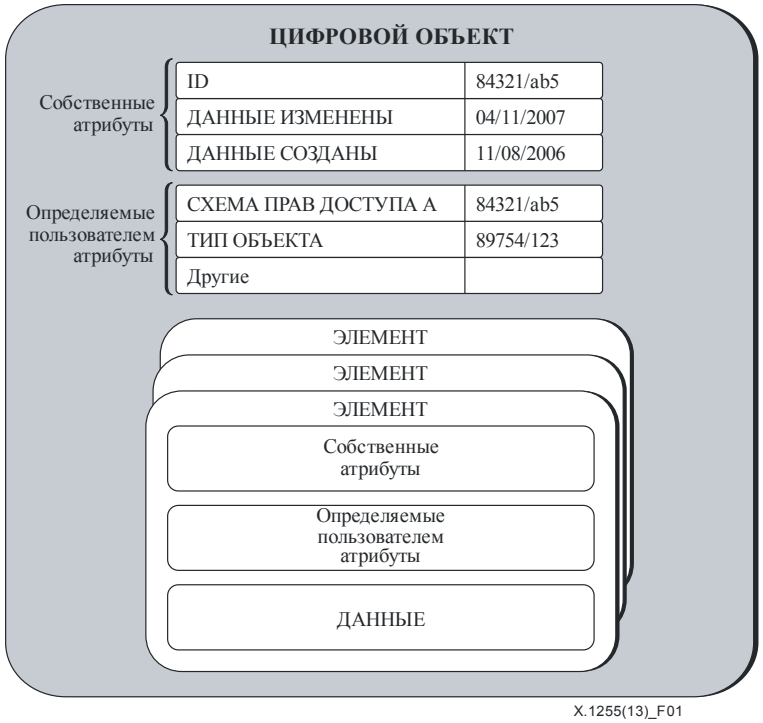

Рисунок 1 – Иллюстративный пример цифрового объекта

За исключением постоянного идентификатора в верхней части, все показанные на рисунке 1 данные являются схематичными. Каждый элемент цифрового объекта может принимать разные формы, то есть ссылки на цифровой объект по идентификатору, какой-либо фактический цифровой объект, подходящим образом введенные открытые локальные данные.

Регистры могут использовать или включать репозитории для хранения записей метаданных; а репозитории являются системами управления информацией, которые предоставляют доступ к совокупности DE через протокол интерфейса цифрового объекта. В общем случае можно представить, что репозитории включают в себя цифровые объекты, к которым они предоставляют доступ. При более детальном рассмотрении, однако, они представляются порталами в различные системы хранения и информационные системы, отображающие необработанные данные в цифровые объекты, которые могут храниться локально или удаленно. Это может быть аналогично файловой системе, в которой хранятся данные для данного DE в одном или более файлов, не известных или не видимых пользователю. Или же, специально для комплексных объектов, данные могут распределяться по нескольким местоположениям и системам и собираться вместе в форме DE только по запросу, при этом один компонент хранения содержит "карту" объекта, а весь объем данных находится в других системах. Этот метод взаимодействия с существующими системами является ключевым фактором создания федерации, поскольку информация в произвольно комплексной информационной системе может логически подразделяться на DE, и эти DE могут быть доступны стандартизованным образом с использованием DEIP в приложениях, ориентированных на пользователя.

DE-клиент может показать местоположение одного или нескольких репозиториев для данного DE путем разрешения его идентификатора. Запрос на разрешение возвращает местоположение одного или нескольких соответствующих репозиториев, с которым клиент может инициировать транзакцию на основе DE.

Программное обеспечение DE-репозитория обеспечивает, как правило, несколько сетевых интерфейсов для выполнения операций с цифровыми объектами, то есть протокол интерфейса цифрового объекта для взаимодействия с самим DE, а также требуемые на локальном уровне интерфейсы в соответствии с используемыми технологическими вариантами. Каждый из различных интерфейсов обладает своими преимуществами в отношении безопасности, совместимости с прокси-серверами и использования повсеместного клиентского программного обеспечения. Резервирование встроено в протокол интерфейса цифрового объекта вместе с жесткой индивидуальной и групповой аутентификацией. Резервирование поддерживается системой зеркального отображения, в которой каждый DE-репозиторий поддерживает связь с другими для обеспечения синхронизации

дублирующих объектов. Аутентификация основана на использовании либо секретной информации, либо открытого/секретного ключа или других механизмах аутентификации.

К другим важным возможностям относятся репликация, позволяющая выполнять зеркальное отображение по репозиториям, и расширяемость на основе механизма подключаемых модулей. Подключаемые модули могут быть встроенными для управления как деятельностью объекта, зависящей от типа, например разбор формата видеоизображения и выдача требуемого раздела или деятельность, ориентированная на сетевые услуги, например внесение метаданных в регистр DE.

7.2 Протокол интерфейса цифрового объекта

Каждое взаимодействие с DE включает идентифицированный объект, который вызывает или применяет операцию цифрового объекта. Информация управления определением идентичности об этом объекте, каждая операция и цель операции являются уникальными и постоянно идентифицированными. Кроме того, ресурсы разных видов являются идентифицированными объектами, и соответствующая информация о состоянии данного ресурса может включать, наряду с прочими записями, его открытый ключ.

Операции применяются к объектам репозиториями, которые сами являются цифровыми объектами и которые предоставляют доступ к содержащимся в них объектам. Протокол интерфейса цифрового объекта определяет метод, с помощью которого объект поддерживает связь с репозиторием для целей вызова операций над цифровыми объектами, к которым этот репозиторий предоставляет доступ. Эти операции могут использоваться, в частности, для доступа к конкретным записям метаданных по их идентификаторам; однако эти записи могут быть также доступны семантически с помощью иных средств, таких как выделенный регистр "apps" и веб-браузеры.

Операции над цифровым объектом включают следующие элементы:

- EntityID: идентификатор объекта, запрашивающего вызов операции;
- TargetObjectID: идентификатор объекта, над которым будет осуществляться операция;
- OperationID: идентификатор, определяющий операцию, которая должна быть выполнена;
- Input: последовательность битов, содержащая входные данные для операции, в том числе любые параметры, контент и другую информацию; и
- Output: последовательность битов, содержащая выходные данные операции, в том числе любой контент или иную информацию.

Информация управления определением идентичности может сопровождаться частью сертификата или передаваться как часть сертификата, который делает явное или неявное утверждение доверия в отношении этой информации. Вместе с тем получатель может принять или не принять этот сертификат, если он не был создан приемлемым органом, определяющим доверие. Для получения аналогичного результата о доверии вместо сертификатов могут использоваться жетоны. Эти сертификаты или жетоны повышают вероятность того, что будет передана точная информация идентичности, однако внутренние механизмы безопасности, которые могут быть реализованы как часть этой открытой архитектуры, могут независимым образом проверить, что объект, использующий информацию управления определением идентичности, владеет соответствующим секретным ключом, который может использоваться для валидации идентифицированного объекта. Любая из сторон запроса транзакции с участием идентифицированных объектов может запросить другую сторону зашифровать строку, содержащую ее секретный ключ, и вернуть ее запрашивающей стороне для валидации. Стороны любой транзакции в рамках системы могут вызывать другие средства аутентификации, но не существует априорной необходимости согласовывать эти другие средства. Показанный ниже механизм по умолчанию должен использовать пару открытый/секретный ключ, что является неотъемлемой возможностью DEIP. Вместе с тем при желании и по согласованию сторон могут использоваться другие механизмы аутентификации. Вызов DEIP должен повлечь за собой, как минимум, следующие не факультативные шаги:

a) создание ассоциации между стороной A и стороной B, то есть двумя сторонами транзакции, если уже не существует ассоциации, которой они могут воспользоваться для этой цели;

b) факультативно, сторона A может запросить сторону B провести собственную валидацию для стороны A такую, которая использует метод PKI;

c) далее, в надлежащем случае, сторона A выдает специальный запрос стороне B;

d) факультативно, сторона B может запросить сторону A провести собственную валидацию для стороны B такую, которая использует метод PKI;

e) сторона B выполняет или отклоняет этот запрос, в зависимости от случая; и

f) транзакция заканчивается и либо генерируется новый запрос, либо прекращает существовать ассоциация, в зависимости от случая.

Возможный пример спецификации DEIP приведен в библиографии [b-DOIP] (см. также [b-DO Repo]), но он не составляет официальной части настоящей Рекомендации.

7.3 Взаимодействие с регистром

Любое взаимодействие с регистром включает идентифицированный объект, который может быть отдельным лицом или ресурсом системы; и каждый из них имеет постоянный идентификатор, который может использоваться для аутентификации объекта. В процессе настройки может быть выполнена предварительная конфигурация регистра, предполагающая доверие к каждому клиенту или к клиентам, идентифицированным каким-либо определенным образом с помощью их идентификаторов. Клиенты также могут выбирать аутентификацию регистров, используя ту же процедуру. Далее, может быть выполнена конфигурация определенных клиентов, с тем чтобы они функционировали в соответствии с конкретными требованиями федеративного процесса. Это позволит выполнять определенную операцию с регистром в дополнение к операциям, обычно доступным всем доверенным клиентам. Если клиенты взаимодействуют с регистром, он выдает запрос-ответ для проверки наличия у клиента совпадающего секретного ключа. После такой проверки регистр проверяет принадлежность идентификатора объекту.

Интерфейс регистра обеспечивает следующие операции:

- **Регистрация цифрового объекта**: регистрационная информация может содержать только метаданные, но это также могут быть метаданные в сочетании с DE, к которому применяются эти метаданные. Регистр управляет зарегистрированным цифровым объектом, используя свой внутренний репозиторий. Далее, регистр индексирует информацию, структурированную как цифровой объект, используя правила предварительной конфигурации, которые определяют, как разбирать, снабжать метками и индексировать содержащуюся информацию. Если требуется, регистр создает идентификатор для цифрового объекта и вызывает его включение в систему разрешения.
- **Снятие с регистрации ранее зарегистрированного цифрового объекта**: регистр удаляет цифровой объект из своего внутреннего репозитория, снимает его с регистрации и обновляет систему разрешения, включая запись об удалении данного объекта.
- **Извлечение ранее зарегистрированного цифрового объекта по его идентификатору**: регистр организует в последовательную форму цифровой объект, управляемый в его внутреннем репозитории и перенаправляет его клиенту.
- **Поиск**: регистр разбирает выражение поиска на ключевые слова, точные совпадения или запросы диапазона для сравнения с индексированными цифровыми объектами и возвращает идентификаторы совпадающих цифровых объектов. Более прогрессивные методы поиска, такие как запросы на естественном языке, могут интегрироваться проще, если это позволяют результаты поиска.
- **Получение номера последней транзакции**: регистр, который последовательным образом присваивает номера каждой выполненной им операции регистрации и снятия с регистрации, возвращает последний такой номер клиенту, который согласно своей конфигурации участвует в федеративном процессе с этим регистром. Это позволяет потенциальным клиентам (другим регистрам, участвующим в этом федеративном процессе) определять состояние регистра в целях проталкивания зарегистрированных объектов в зависимости от определенной в конфигурации топологии федерации и выбранного уровня агрегирования.

Притом что аутентификация может быть отключена, рекомендуется, чтобы регистр аутентифицировал клиента и наоборот. Кодирование участвующих в обмене сообщений может меняться и определяется на уровне реализации. Кодирование сообщений может выполняться как операции репозитория цифровых объектов, и в этой точке транзакция регистрации будет представлять собой серию операций репозитория, например создание объекта, добавление элемента. Альтернативно, кодирование сообщений может осуществляться с использованием библиотеки кодирования данных третьих сторон при условии, что и источник, и получатель согласились (возможно, заранее) с использованием такой библиотеки.

7.4 Системы разрешения

Одним из компонентов структуры является система разрешения (которых может быть несколько), которая может выполнить отображение идентификаторов в полезную информацию о состоянии идентифицируемого цифрового объекта, такую как местонахождение в интернете или информация аутентификации данного цифрового объекта или открытый ключ, связанный с данным идентификатором. Открытый характер архитектуры структуры обеспечивает возможность функциональной совместимости систем разрешения, что является желательной задачей настоящей Рекомендации. Информация о состоянии может меняться в соответствии с потребностью отображения текущего состояния идентифицированного цифрового объекта без изменения его идентификатора, что позволяет сохранять идентификатор элемента в ходе изменения местоположения и других соответствующих изменений состояния.

Если идентификатор необходимого ресурса известен, система разрешения и совокупность репозиториев обеспечивают то, что необходимо для авторизованного конечного пользователя или процесса для выполнения просмотра или иного доступа к цифровому объекту. Однако если известна идентичность необходимого ресурса, потребуется ее раскрытие. В терминах библиотечных и информационных систем первый случай называется поиск "известного предмета" (то есть вы знаете, чего вы хотите, и вам необходимо узнать, как это получить). Второй случай обычно требует предметного поиска, и задачей инструментов, используемых в предметном поиске, является сведение его к поиску известного предмета. Регистр цифровых объектов обеспечивает возможность выполнения этой функции.

Притом что экземпляр регистра может функционировать самостоятельно, он может выполнять только запросы обнаружения, связанные с известным ему предметом. При федеративном объединении нескольких регистров, регистр может знать о цифровых объектах, зарегистрированных в ином месте, и, следовательно, возможен широкий поиск по всей совокупности цифровых объектов. Способность определить, какие регистры могут содержать соответствующую связанную с идентичностью информацию, является важным аспектом обнаружения информации управления определением идентичности. Раскрытие информации, имеющейся в одной системе, может потребоваться для другой системы, возможно, с отличающейся схемой. Предположим, что какой-либо объект определил способ ассоциации таких различных систем и содержащейся в них информации, тогда структура обнаружения должна обеспечивать возможность раскрытия таких ассоциаций. Однако в настоящей Рекомендации не рассматривается вопрос о том, кто или что несет ответственность за создание таких ассоциаций, какой вид информации может включаться в ассоциацию, а также как ассоциация создается и каким образом она становится доступной. Эти вопросы будут, как правило, меняться и определяться контекстом, и поэтому в настоящей Рекомендации не предлагается какого-либо вида применения ассоциаций. Для пояснения данного вопроса термин "ассоциация" включен в определения и это понятие включено в определение информации управления определением идентичности.

Во многих случаях определяющее значение имеет конфиденциальность; и это регулируется путем использования методов IdM на основе идентификаторов для отдельных лиц, групп, ролей и ресурсов, а также условий и положений, получаемых из хранящихся метаданных.

7.5 Распределенные запросы и агрегированные метаданные в федеративных регистрах

Система федеративных регистров, определенная в настоящей Рекомендации, должна быть широко доступна и создавать основу системы обнаружения с открытой архитектурой. Система обеспечивает унифицированный способ обнаружения информации управления определением идентичности. Система федеративных регистров позволяет нескольким поставщикам IdM участвовать в обеспечении функционально совместимых регистров и определять, какую информацию они готовы использовать совместно с другими регистрами.

Технология построения регистров обеспечивает средство, с помощью которого стороны, ответственные за создание цифровых объектов в интернете, включая услуги и другие объекты, могут регистрировать существование данного множества таких объектов, сопровождать эту регистрацию дескриптивными и структурными метаданными об объектах, включая информацию о происхождении, и, таким образом, усиливать возможность обнаружения объектов как для широкой публики, так и для определенного сообщества. Одним из ключевых элементом метаданных, которые должны быть зарегистрированы вместе с объектом, является их постоянный идентификатор, и каждый такой идентификатор должен поддаваться разрешению в интернете. Для объектов, которые еще не идентифицированы, конфигурация регистра может предусматривать создание идентификаторов как часть процесса регистрации и обеспечение инструментов, необходимых администратору объекта для сопровождения информации разрешения.

Система федеративных регистров обеспечивает реализацию четырех основных задач обнаружения. Во-первых, она делает возможным применение унифицированных стратегий выбора в рамках участвующих структур доверия и других систем IdM. Во-вторых, она обеспечит пользователю возможность доступа к содержащейся в регистрах информации, к которой у этого пользователя есть допуск, без необходимости общения напрямую с несколькими регистрами. В-третьих, она обеспечивает инфраструктурную поддержку конфиденциальности и других ограничений доступа, установленных отдельными системами IdM. И, в-четвертых, она сделает возможным семантический доступ к регистрам для поддержки многоязычия.

Концепция федеративных регистров базируется на определенной в настоящем документе открытой архитектуре, которая обеспечивает следующие преимущества:

- Унифицированные стратегии выбора: регистры и ассоциированные с ними структуры доверия или, в более широком смысле, другие системы IdM могут быть отобраны для запроса на основе свойств информации, для хранения которой они предназначены. Как правило, отобрана будет система IdM, имеющая определенный уровень фонового исследования для обоснования своей информации. Альтернативно, может быть отобрана минимальная структура доверия или другая система IdM, которая может только проверить информацию кредитной карты или водительские права. Другим предельным случаем является выбор системы IdM, которая проводит проверку ДНК отдельных лиц. Может быть отобрана организация, поддерживающая стратегии обеспечения целостности систем. Благодаря таким средствам возможно применение унифицированного метода в генеральной совокупности регистров и ассоциированных с ними систем IdM.
- Совместное использование метаданных: информация, имеющаяся в системе федеративных регистров, указывается как совместно используемые метаданные. С совместно используемыми метаданными ассоциирован общий шаблон, который определяет, как представлены метаданные и, следовательно, каким образом они могут быть доступны для последующей обработки. Шаблон не содержит каких-либо определенных записей.
- Федеративный доступ: если один регистр не имеет желательной информации, она может быть доступной из одного или нескольких других регистров. В нормальном режиме система будет функционировать так, чтобы сделать такую информацию легкодоступной пользователю, независимо от того, в каком регистре она может содержаться. Такое доступ может обеспечиваться разнообразными средствами, включая иерархическую федерацию и одноранговые системы.
- Частный доступ: доступ к некоторым регистрам будет ограничен определенными группами пользователей, типами приложений или ролями, связанными с использованием системы; а некоторые регистры могут быть открыты для всех. Средства ограничения доступа к информации обнаружения на основе критерия такого ограничения являются неотъемлемой частью системы. Для поддержания конфиденциальности в рамках системы будет использоваться один или несколько механизмов, согласованных участвующими регистрами.
- Семантический доступ: для интерпретации вставленных "типов" используется система типов. Поставщики данных идентичности могут назначать типы по собственному выбору в соответствии с установленными в спецификации руководящими принципами. Это позволит обеспечить семантический доступ к соответствующей информации независимо от возможного места ее хранения в системе, и это сможет содействовать выполнению требований многоязычия.

Метаданные в такой системе доступны как структурированные данные с соответствующими уникальными постоянными идентификаторами, которые существуют столько же, сколько существует этот цифровой объект. Метаданные из разных регистров могут различаться в предметной области и/или схемой метаданных, что затрудняет простой, но согласованный поиск по агрегации всех записей. Если метаданные из разных схем или предметных областей сокращаются до схемы наименьшего общего знаменателя, которая является одним из решений агрегирования такого типа данных, то оптимальной стратегией поиска может быть выявление тех регистров, которые были бы наилучшими кандидатами для более детального поиска. Преобразование в схему наименьшего общего знаменателя может быть выполнено регистрами источника или регистром коллектора. Или же сам поиск может быть определенным образом отображен в запрос различных схем метаданных, результатом чего является совокупность запросов, которая ответвляется от оригинала.

Агрегирование объектов метаданных для обнаружения информации из многих доменов является одной из возможностей, другая возможность заключается в формировании распределенных запросов по многим регистрам, каждый из которых управляет объектами метаданных своего домена. Ландшафт федерации между регистрами включает различные другие возможности, что показано в трехмерном пространстве на рисунке 2.

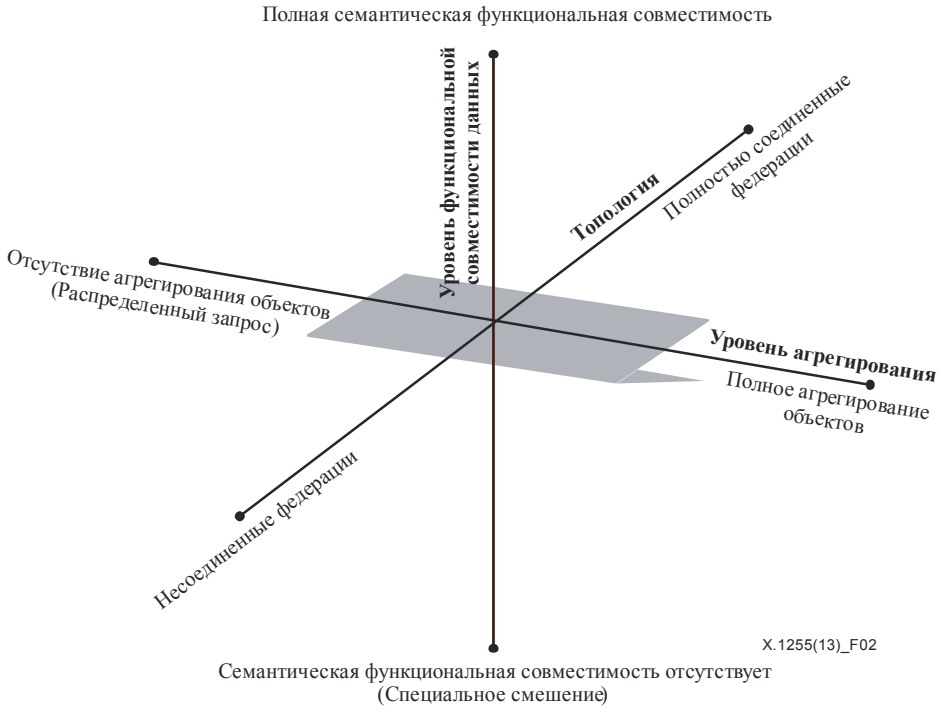

Рисунок 2 – Распределенные запросы по многим регистрам

На рисунке 2 показаны три оси. По одной оси показан уровень агрегирования метаданных регистров – от отсутствия агрегирования до полного агрегирования. По второй оси показана степень топологической соединяемости регистров. Третья ось связана с функциональной совместимостью информации из разных регистров. Ниже приводится описание каждой из этих осей.

По оси уровня агрегирования показывается степень выполнения предварительно определенного порядка в пределах регистров для включения в агрегирование объектов метаданных. Крайняя левая точка оси показывает объекты, по которым не выполняется агрегирование по регистрам до любого запроса, а крайняя правая точка оси показывает, что выполняется агрегирование всех объектов по регистрам до любого запроса. Точка на оси показывают другие возможности, включая агрегирование информации метаданных наименьшего общего знаменателя, агрегирование индексов поиска и т. д. При движении слева направо действительность агрегированной информации также уменьшается; распределенные запросы дают более актуальные результаты, в то время как действительность агрегированных объектов метаданных зависит от времени их последнего агрегирования.

По оси топологии показывается степень соединенности регистров. На одном из концов оси регистры не имеют сетевого соединения между собой, результатом чего является отсутствие совместного использования информации; другой конец оси показывает, что регистры полностью соединены между собой. Следует отметить, что "как" они соединены, по-прежнему определяется уровнем агрегирования, а топология определяет только возможные связи.

Ось уровня функциональной совместимости данных показывает степень, в которой объекты метаданных из регистра, который обслуживает определенный информационный домен, функционально совместимы с объектами метаданных из другого регистра, обслуживающего другой информационный домен. Другими словами, схемы метаданных, принятые одним регистром, могут быть совместимы или несовместимы со схемами, принятыми другим регистром. Иногда для достижения определенного уровня, если не полной, функциональной совместимости необходимо преобразование объектов метаданных. В других случаях, когда схемы весьма различаются семантически, добиться приемлемого уровня функциональной совместимости с помощью преобразования не удастся.

Следует заметить, что все точки в трехмерном пространстве, показанные на рисунке 2, являются действительными. Например, распределенный запрос по несоединенным узлам не предполагает какого-либо распределения запросов. Аналогично полное агрегирование функционально несовместимых объектов предполагает систему некогерентных объектов. В той степени, в которой действительны точки в иллюстративном трехмерном пространстве, базовая схема регистра должна

допускать такие возможности конфигурации. Кроме того, выполняется ли отображение в преобразовании записей метаданных или в поиске, а также преобразуются ли записи метаданных вносящими регистрами или собирающим регистром, все эти вопросы решаются на уровне реализации. Могут существовать значительные последствия для характеристик, но базовая схема должна допускать вариации реализации.

Подход, принятый в настоящей Рекомендации, не ведет к решению и не решает проблему поиска и извлечения в рамках гетерогенных информационных систем, но он обеспечивает общую структуру, в которой могут использоваться разные подходы. Вероятно, что не существует единого решения этой проблемы и что оптимизированные подходы могут различаться в зависимости от сообщества заинтересованных сторон и предметной области.

7.6 Схемы метаданных

Основной задачей настоящей Рекомендации является обеспечение основы для определения совокупности схем метаданных "высокого уровня" для обеспечения обнаружения информации о: a) идентификаторах, используемых в различных системах IdM; b) поставщиках данных идентичности; c) полагающихся сторонах; и d) структурах доверия и других системах IdM на всех уровнях, включая стратегии, процедуры и основополагающую техническую инфраструктуру. Необходимые элементы этих схем метаданных будут получены в соответствии с определенными сценариями использования, но они должны быть расширяемыми и на уровне элементов, и на уровне схемы, с тем чтобы обеспечивать рост и изменение в динамической области.

Различные объекты, участвующие в управлении определением идентичности, каждый, может определять собственные конкретные схемы и в зависимости от потребностей преобразовывать их в стандартизованные схемы метаданных высокого уровня для описания их услуг, стратегий и процедур, а также регистрации этих описаний в одной или нескольких совокупностях федеративных регистров. Эти регистры будут обеспечивать услуги обнаружения по зарегистрированным объектам.

Если существует возможность создания одной схемы метаданных, учитывающей все аспекты технологий IdM, соответствующих организаций и связанных с ними стратегий и процедур, предлагается начинать с одной схемы для каждого типа участвующего объекта. Процесс получения согласованной совокупности схем метаданных станет коллективным процессом, в котором заинтересованные стороны будут вносить свои знания атрибутов, подлежащих охвату этими схемами; возникающие схемы далее могут быть протестированы в условиях различных сценариев использования, с тем чтобы убедиться в том, что они действительно предоставляют информацию, необходимую для обеспечения процессов обнаружения, и далее, в случае необходимости, они могут наращиваться.

7.7 Функциональная совместимость метаданных

Идентификаторы являются одной из важных составляющих достижения функциональной совместимости метаданных. Вместе с тем ряд других аспектов функциональной совместимости метаданных, том числе выполняемое человеком определение и контекст описаний, не входят в сферу действия настоящей Рекомендации. Другие атрибуты, определенные в метаданных, такие как описание или возможность конкретной конфигурации, например конкретный режим соединения и метод агрегирования, относятся к сфере функционирования регистров. Для целей управления объектами метаданных в разных регистрах функциональная совместимость метаданных будет упрощаться, если сотрудничающие стороны примут решение об общих схемах метаданных. В таком случае управление метаданными будет осуществляться как управление гомогенными объектами, а регистры будут интерпретировать и обрабатывать метаданные согласованным образом. В разделе 9 ниже показаны два конкретных случая федерации в контексте уровня агрегирования и топологии – двух параметров, которые, как правило, применяются к данной структуре.

8 Типы и атрибуты типов

Регистры предоставляют записи метаданных в форме цифровых объектов, которые предполагаются к обмену с другими федеративными регистрами. Каждый такой регистр состоит из совокупности элементов, каждый из которых содержит поле "тип" и поле "значение". Понимание значения каждого типа является решающим для объявления ассоциированных значений в форме, отличной от скрытой последовательности битов или совокупности последовательности битов.

Для того чтобы понять значение типа, типы представляются постоянными идентификаторами, которые могут быть разрешены в полезную информацию о типе. Притом что выполнение описания типов предполагается отдельными лицами, необходимы стандартные средства описания и представления типов.

Конкретные аспекты и атрибуты того, что в конечном счете составит описание типа, как предполагается, с течением времени будут меняться, но следующие четыре аспекта рассматриваются как важнейшие:

- Первая категория атрибутов является простейшей и включает воспринимаемые человеком описания назначения данного типа. Эти описания предназначены для определения назначения типа, ресурсов и понятий, которые он описывает, и его использование. Эти атрибуты обеспечат описания на многих языках.
- Вторая категория атрибутов описания типа включает информацию о его происхождении. Каждое описание типа должно включать дату его создания, дату последнего обновления, участников, его статус и любой идентификатор псевдонима, который он может иметь.
- Третья категория атрибутов относится к описанию разделения типов на категории, а также возможности типов использовать другие типы.
- Четвертая категория атрибутов обеспечивает для различных систем возможность динамично воздействовать на ресурс определенного типа.

Ниже более подробно описаны три последние категории.

Тип используется, как правило, для описания конкретной категории ресурсов и/или понятий в соответствии с определенным набором характеристик. Эта категория представляет домен применимости типа и называется видом типа. Например, тип кодирования символов, используемый для определения того, как символ должен быть представлен в двоичном формате, будет иметь вид "кодирование". Тип форматирования данных, используемый для определения того, как должна быть представлена структура в форме совокупности битов, будет иметь вид "форматирование".

Описание каждого типа включает атрибут, который определяет его вид. Атрибут описания вида типа обеспечивает простую схему классификации, которая нормализует разработку новых типов и поможет пользователям типов обнаружить существующие типы. Вид типа сам является типом и при необходимости могут быть добавлены новые виды типа для расширения классификации видов.

Для максимального повторного использования типов и сведения к минимуму создания дубликатов, каждый тип сможет описывать себя в терминах существующих типов. Если, например, новому виду необходимо описать, что его ресурсы упорядочены в XML, он должен сделать это путем включения ссылки на существующий тип упорядочения XML. Типы могут использовать другие типы путем расширения или конкретизации.

Каждый тип должен включать любой и все типы, которые он использует, и порядок использования. Способность типов определять самих себя в терминах других типов не только снижает уровень дублирования типов, но и допускает определение пользователями типа своего понимания конкретного типа с большей глубиной детализации.

Наконец, описание типа должно позволять разным системам динамически приобретать способность воздействовать на любой классифицированный ресурс. Описание типа должно содержать атрибуты, определяющие местоположение привязок сетевых услуг и/или конкретных модульных реализаций, их платформ и связанных с ними интерфейсов. Это позволит библиотеке общей обработки типов динамически и безопасно осуществлять привязку к таким услугам или собирать, загружать и запускать соответствующие модули реализации типов и обрабатывать ресурс.

Типы, рассмотренные выше, имеют уникальную идентификацию. Разрешение идентификаторов этих типов в какой-либо заранее определенной системе разрешения будет возвращать запись типа. В Дополнении II, в котором концептуально определена группа объектов, образующих такую запись типа, приведен пример представления БНФ для записи типа.

Для однозначного и согласованного определения типа требуются четыре раздела, а именно: описание, происхождение, вид и обработка.

Раздел описания представляет собой последовательность одного или нескольких воспринимаемых человеком описания, которые наряду с прочим определяют назначение и использование этого типа. Язык, который может соответствовать [b-IETF RFC 1766] и на котором выполнены эти описания, должен быть уникальным образом представлен своим типом и предшествовать описаниям.

Раздел происхождения фиксирует данные о создании, дате изменения, участниках, псевдонимах (или идентификаторах) и статусе. Даты должны соответствовать стандарту [ISO 8601]. Участники – это имена сотрудников или организаций, которые участвовали в создании или регистрации типа в регистре назначенного типа. Псевдонимы собираются для ссылки на их предыдущую регистрацию в других регистрах местного типа, которые объявлены здесь для целей создания контекста определенного типа. Статус определяет, используется ли, исключен или устарел этот тип.

Раздел вида фиксирует существо типа. Определение новых типов на основе существующих – это мощное понятие, которое является ключом к определению сложных типов. Окончательное понятие относительно видов должно определять, является ли информация вида составным блоком для определения других типов, или определяет конкретное представление типа. Например, тип двоичного кодирования сам является составным блоком, позволяющим определять другие типы.

Информация может проходить к услуге, которая знает, как разобрать и обработать информацию типа. Клиенты вызывают услугу для синхронизации данной информации. Определение услуги должно указывать, где найти услугу, как вызвать услугу и чего ожидать в качестве результатов этой услуги. Для определения такой услуги конкретная нотация в рекомендацию не входит.

9 Иерархическая федерация и одноранговая федерация

При иерархическом подходе главный регистр используется для отслеживания информации, для удобства хранящейся во многих регистрах, поэтому необходимо выполнить адресацию только одного регистра. Может существовать несколько главных регистров, но все они должны быть известны и к ним следует обращаться для выполнения полного поиска.

В рамках одноранговой подхода определенные регистры выбирают одноранговое взаимодействие с отобранными другими регистрами. Причины выбора одноранговых схем могут быть разными. Организационные стратегии, окружающие управление регистрами, стратегии доверия, которые запрещают или поддерживают точки взаимодействия федерации между регистрами, доступность/надежность регистров, участвующих в одноранговой сети – вот лишь некоторые причины, которые могут определить, какие регистры отбираются данным регистром для одноранговой обмена.

И иерархическое, и одноранговое построения, однако, дают понятие только о топологии федерации и не определяют уровень агрегирования, выбранный для одного из этих сценариев. Могут применяться различные уровни агрегирования, но ниже в иллюстративных целях представлены два конкретных примера. В таблице 1 приведены преимущества (обозначенные знаком "+") и недостатки (обозначенные знаком "–") двух федеративных систем, когда либо полностью заранее агрегируются объекты метаданных, либо в ответ на запрос системы IdM в реальном времени по регистрам распространяются запросы.

Таблица 1

	Иерархическая федерация	**Одноранговая федерация**
Полное агрегирование объектов метаданных в регистре-сборщике	+ Достигается полное обнаружение по доменам путем процесса полного агрегирования. + Достигается гарантированная актуальность междоменной информации путем нормализации объектов метаданных в процессе агрегирования. + Эффективное функционирование благодаря локализованному поиску и выборкам. – Жесткое построение. Требует процессов тщательной настройки, которые могут препятствовать организационным стратегиям. – Единые точки отказа либо в главном сборщике, либо в промежуточных сборщиках. – Вероятность ввода устаревшей информации в результате низкой частоты обновления агрегирования. – Вероятны проблемы масштабируемости на высшем уровне в иерархии.	+ Обеспечивает возможность гибких, нежестких группировок, которые обслуживают конкретные области интересов. + Отсутствуют единые точки отказа, поскольку для федерации могут быть разрешены несколько маршрутов. + Достигается гарантированная актуальность междоменной информации путем нормализации объектов метаданных в процессе агрегирования. + Эффективное функционирование благодаря локализованному поиску и выборкам. – Не гарантируется полнота междоменного обнаружения, если только построение не является полностью соединенным. – Требуются дорогостоящие мероприятия для устранения дублирования, если регистры могут объединяться в федерацию по нескольким маршрутам. – Проблемы безопасности, если не все точки взаимодействия являются доверенными.
Распространение запросов по регистрам	+ Действительность объектов и информации в этих объектах. + Масштабируемая система. – Не гарантируется полнота междоменного обнаружения вследствие вероятной неготовности узлов регистров в момент распространения запроса. – Нарушается оценка актуальности результатов вследствие слияния результатов на этапе исполнения. – Жесткое построение. Требует процессов тщательной настройки, которые могут препятствовать организационным стратегиям. – Единые точки отказа, либо в главном сборщике, либо в промежуточных сборщиках, которые осуществляют распространение запросов в нисходящем направлении и проталкивают результаты в восходящем направлении. – Проблемы эффективности функционирования вследствие неустойчивости аппаратного оборудования для развертывания регистров.	+ Действительность объектов и информации в этих объектах. + Масштабируемая система. – Не гарантируется полнота междоменного обнаружения вследствие вероятной неготовности узлов регистров в момент распространения запроса, даже при наличии резервных маршрутов федерации. – Нарушается оценка актуальности результатов вследствие слияния результатов на этапе исполнения. – Требуются дорогостоящие мероприятия для устранения дублирования, если регистры могут объединяться в федерацию по нескольким маршрутам. – Проблемы эффективности функционирования вследствие неустойчивости аппаратного оборудования для развертывания регистров.

Программное обеспечение регистров поддерживает и допускает различные комбинации матрицы, приведенной в таблице 1. Некоторые комбинации обусловливают большее число проблем реализации по сравнению с другими. Вопросы масштабируемости решаются путем использования технологии репозитория, которая рассматривает реальные системы хранения абстрактно и делает возможным одновременное использование нескольких систем хранения. Также обеспечивается репликация и распределение загрузки регистров, что устраняет проблему масштабируемости. Обнаружение дублирования, которое в противном случае могло бы создать проблему в отношениях регистров "многие ко многим", может быть эффективно устранено путем использования постоянных идентификаторов.

Агрегирование данных, в противоположность распределенному запросу, предполагает, что регистр инициирует перемещение записей метаданных, проталкивает их в противоположность выдаче ответов на принятые запросы. Кроме того, обеспечивающие записи обозначаются как источник, а получатель обозначается как получатель. В федерации получателем будет точка взаимодействия для системы федеративных регистров. Регистр-источник ретранслирует успешно выполненные изменения в метаданных, например создание или редактирование записей метаданных, получателю. Эти транзакции охватывают изменения в состоянии объекта, то есть взаимоотношения создания, изменения, псевдонимов, удаления, а также добавления/исключения/замены. Каждая запись регистрации, представленная в регистр, транслируется в действия регистрации и снятия с регистрации в ядре регистра. Каждое такое действие является транзакцией, которая имеет идентификатор транзакции – номер, который, как правило, увеличивается начиная с нуля. Такой подход в равной степени применим к сценариям, в которых регистры сгруппированы одноранговым образом, а также иерархическим образом.

Определение конфигурации отдельных регистров для ориентирования и распространения запросов к выбранным регистрам, как при иерархическом, так и одноранговом построении, обеспечивает возможность распространения запросов. Регистры цифровых объектов, в дополнение к поддержке определяемых сообществом интерфейсов, поддерживают также протокол интерфейса цифрового объекта как протокол по умолчанию. Запросы могут распространяться к другим регистрам в зависимости от использования данного протокола.

Дополнение I

Сценарии использования

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Для иллюстрации использования системы федеративных регистров полезно привести несколько сценариев. Эти сценарии описаны ниже с указанием возможных атрибутов, которые необходимо регистрировать для обеспечения приемлемого функционирования процесса(ов) обнаружения.

- Клиент – человек или машина – хочет получить услугу от поставщика услуг в интернете. Поставщик услуг требует доказательство идентичности и принимает регистрационные данные идентичности от любой из совокупностей поставщиков информации идентичности. Клиент (как правило, программное обеспечение) должен иметь возможность определять, какие поставщики IdP являются приемлемыми, обладает ли уже клиент соответствующими регистрационными данными, полученными от одного или нескольких приемлемых IdP, и если нет, то как их получить.

  Поставщик услуг должен объявлять, какие IdP являются приемлемыми для соответствующей услуги или услуг. Это может быть выполнено либо непосредственно поставщиком услуг стандартизованным образом, либо путем ссылки на регистр также стандартизованным образом. В любом случае IdP должны уникально и точно идентифицироваться. Далее клиент может соответствовать текущему участию в какой-либо организации IdP или иным образом получить знания о том, как соответствовать требованиям IdP, и представить соответствующие регистрационные данные поставщику услуг. В случае прямого объявления поставщиком услуг, при наличии уникальной и точной идентификации соответствующего или соответствующих IdP и при условии, что клиент может предоставить определяемые IdP регистрационные данные, регистр не потребуется. Во всех других случаях должна существовать возможность обнаружения определенного уровня информации о приемлемых IdP. При наличии уникального и постоянного идентификатора это может быть прямой поиск в регистре данных IdP. Для удовлетворения требований настоящего сценария использования метаданные, описывающие данного IdP, должны предоставить клиентам информацию, необходимую для определения, является ли данный IdP разумным выбором для предусмотренного ими использования данной услуги. Соответствующие атрибуты будут включать уникальный постоянный идентификатор самого IdP для вероятных перекрестных ссылок, например просмотра сайтов, структур доверия, в которых участвует этот IdP, стратегий и процедур, юридических требований, требуемого программного обеспечения, любых прейскурантов ставок и т. д. Часть этой информации будет представлена в форме второго уровня косвенности, например многие технические и стратегические сведения о любом данном IdP будут определяться участием IdP в одной или нескольких определенных структурах доверия.
- Те же данные, которые позволят клиенту обнаружить соответствие данного IdP, позволят также поставщику услуг обнаружить одного или нескольких IdP, регистрационные данные которого будут приняты, и таким образом добавить его к своему списку приемлемых IdP. Метаданные IdP будут охватывать оба эти случая использования.
- В противоположность первому сценарию, клиент осуществляет доступ к услуге и представляет регистрационные данные идентичности, которые эта услуга ранее никогда не получала. Основываясь на предположении о том, что представление этих регистрационных данных состоит из или, по крайней мере, начинается с идентификатора для IdP, услуга должна принять решение, принимать или не принимать эти регистрационные данные, далее исследовать возможность приема этих регистрационных данных или просто отклонить их без дальнейшего исследования. Регистр в этом сценарии должен обнаружить общую информацию о типе идентификатора и IdP, который его представляет. Это, в свою очередь, может привести к дальнейшему поиску по регистру конкретных технологий, используемых этим IdP, в том числе соответствующих структур доверия.
- Различные объекты, участвующие в управлении определением идентичности, явно или косвенно, являются, как правило, членами одной или нескольких структур доверия или другой системы IdM. Для создания схемы метаданных, описывающих эту структуру доверия, потребуется спецификация атрибутов каждой системы IdM. При этом возникает ряд важных вопросов. Описывается система IdM организацией, которая ее обеспечивает, набором

стандартов, в соответствии с которыми она реализована, каков способ измерения соответствия стандартам и т. д.? Независимо от ответов на эти вопросы, очевидно, что некоторые IdP и даже некоторые RP будут подсоединены к описаниям высокого уровня, таким как описания организаций InCommon, Kantara, Safe-BioPharma и OIX, которые возможно обнаружить в регистре или федерации регистров.

На рисунке I.1 мы показали возможный порядок использования системы федеративных регистров ("система") с конкретным сценарием использования.

Шаг 1: В этом примере конечный пользователь запрашивает услугу у полагающейся стороны.

Шаг 2: Полагающаяся сторона отвечает, предоставляя идентичность одной или нескольких структур доверия, которым RP доверяет, в данном случае – одной структуры (TF1).

Шаг 3: Конечный пользователь обращается к системе с идентификатором TF1.

Шаг 4: Система отвечает, предоставляя соответствующую запись TF1. Информация для TF1 включает минимальные атрибуты, которые потребуются для доверия в пределах структуры.

Шаг 5: Конечный пользователь оценивает эти минимальные требования для того, чтобы определить, возможно ли получить доверие RP. Здесь мы предполагаем, что результат оценки конечного пользователя положительный и показывает, что конечный пользователь может соответствовать минимальным атрибутам, например водительским правам.

Шаг 6: Далее конечный пользователь может вернуться в систему, запрашивая IdP, попадающих в рамки TF1 и способных соответствовать протоколу(ам), который поддерживает конечный пользователь, например HTTP и электронная почта, показанные нами в примере как протокол "X".

Шаг 7: Система находит поставщиков данных идентичности (IdP), соответствующих протоколу "X" и находящихся в рамках TF1.

Шаг 8: Система отвечает конечному пользователю предоставляя совокупность IdP, отвечающих требованиям полагающейся стороны и конечного пользователя.

Шаг 9: Конечный пользователь оценивает совокупность IdP, которую вернула система, и осуществляет выбор (IdP1).

Шаг 10: Конечный пользователь, имеющий атрибуты, требуемые IdP1, и пользуясь протоколом, понятным для IdP1, участвует во взаимодействии запрос/ответ с IdP1.

Шаг 11: В результате успешного взаимодействия запрос/ответ IdP1 предоставляет RP регистрационные данные.

Шаг 12: Полагающаяся сторона, которая теперь доверяет конечному пользователю, предоставляет требуемую услугу.

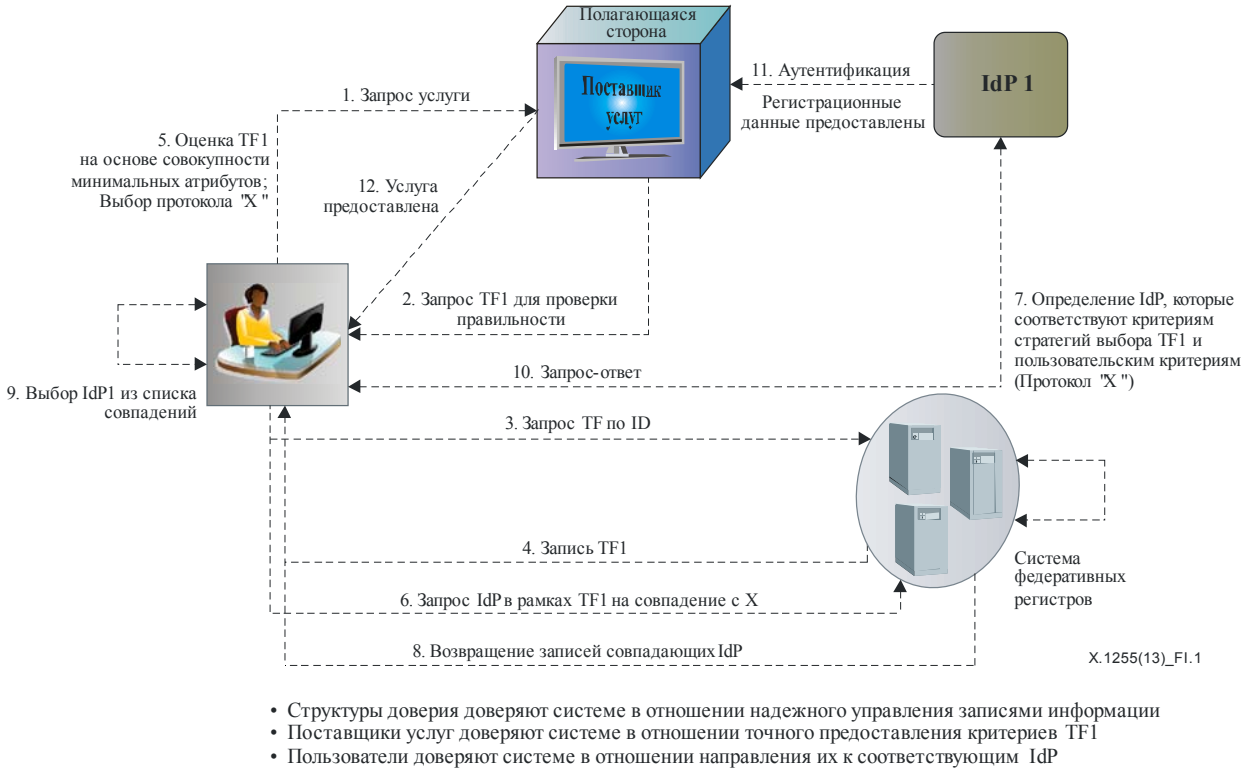

Рисунок I.1 – Аутентификация с участием структур доверия

На рисунке I.2 показаны схемы высокого уровня записей, которые хранятся в системе федеративных регистров, что делает возможным транзакцию, описанную на рисунке I.1, а также другие сценарии использования, описанные выше. Эти записи будут сохраняться системой как цифровые объекты, каждый из которых имеет постоянный идентификатор. Далее каждая должна будет перестраиваться в конкретные схемы, для того чтобы было возможным создание прототипа.

Каждая структура доверия будет иметь идентификатор, общее описание структуры, набор атрибутов, используемых для аутентификации, и указатели на одну или несколько стратегий выбора IdP, которые сами являются отдельными цифровыми объектами, хранящимися в системе. Это служит еще одним уровнем косвенности, для того чтобы все IdP, попадающие в одну TF, могли быть сгруппированы по критерию взамен нумерации. Каждый объект стратегии выбора IdP имеет идентификатор, общее описание, перечень приемлемых технологий (например, поддерживаемые протоколы), перечень организационных органов аккредитации (например, правительственная организация) и любые конкретные эксплуатационные ограничения. Взаимоотношения TF и стратегии выбора IdP будут в обоих направлениях отношениями типа "многие ко многим", то есть данная TF может принять несколько стратегий выбора IdP и данная стратегия выбора IdP может использоваться несколькими TF.

Оставшимися двумя предлагаемыми типами объектов, хранящимися системой, являются IdP и полагающиеся стороны. Каждый IdP имеет постоянный идентификатор, общее описание, требуемые пользовательские атрибуты, стратегию оценки для этих атрибутов, конкретные протоколы и принятые аккредитации, а также конкретные конечные точки, например местоположение IdP в форме приемлемых протоколов. Каждая полагающаяся сторона имеет постоянный идентификатор, общее описание, совокупность TF, на которые она полагается, и любые эксплуатационные ограничения.

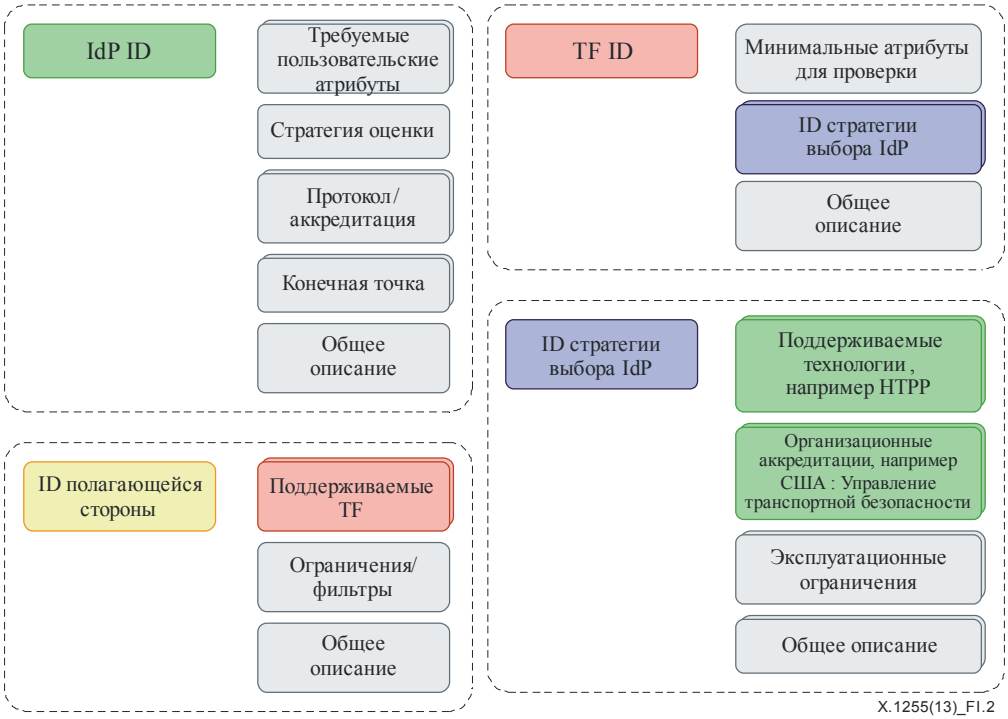

Рисунок I.2 – Схемы высокого уровня

Дополнение II

Представление БНФ для записи типа

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

БНФ для записи типа:

```
<type identifier> := <unicode string>
<type> := <description section> <section delimiter>
    <provenance section> <section delimiter>
    <genre section> <section delimiter>
    <processing section>
```

```
<description section> := <language> '=' <human readable description>
    [<repetition delimiter> <description section>]
<language> := Any item from RFC 1766
<human readable description> := <unicode string>
```

```
<provenance section> := <creation date> <list delimiter>
    <last modified date> <list delimiter>
    <contributors> <list delimiter>
    <aliases> <list delimiter>
    <status>
<creation date> := Conforms to ISO 8601
<last modified date> := Conforms to ISO 8601
<contributors> := <unicode string>
    [<repetition delimiter> <contributors>]
<aliases> := <unicode string>
    [<repetition delimiter> <aliases>]
<status> := 'in use' | 'deprecated' | 'obsolete'
```

```
<genre section> := <genre> '=' <genre details>
    [<repetition delimiter> <genre section>]
<genre> := 'data structure' | 'encoding' | 'format'
<genre details> := <human readable description>
    [<list delimiter> <genre subsection>]
<genre subsection> := 'form='<form> <list delimiter>
    'relationship=' <relationship> <list delimiter>
    'related to=' <type identifier>
    [<repetition delimiter> <genre subsection>]
<form> := 'expression' | 'manifestation'
<relationship> := 'is equivalent to' | 'is derived from' |
    'is informed from'
```

```
<processing section> := <processor type> '=' <processor>
    [<repetition delimiter> <processing section>]
<processor type> := 'network service' | 'downloadable program' |
    'parsing function'
<processor> := <network service type> '=' <network service binding> |
   <compatible platform> <list delimiter>
   <program network location> <list delimiter>
   <program arguments> |
   <pseudo code>
<compatible platform> := 'Linux' | 'Windows' | 'Mac OS'
<program arguments> := <type>
     {<list delimiter> <unicode string>}
<pseudo code> := <unicode string>
```

```
<unicode string> := <visible character> [<unicode string>] |
    <whitespace character> <[unicode string>]
<visible character> = Any visible character in Unicode presumably encoded in UTF-8
<whitespace character> := Any whitespace character in Unicode presumably encoded in UTF-8
```

Примечания:

1 Идентификатор <type identifier>, выданный глобальной системе разрешения, разрешается в запись <type>.

2 Все разделители, то есть <section delimiter>, <repetition delimiter> и <list delimiter>, определяются на уровне реализации и намеренно не определены в настоящем документе.

3 Тип <network service type> также не определен в настоящем документе, но должен охватывать массовые сетевые услуги по усмотрению реализующей организации.

4 Привязка <network service binding> также не определена в настоящем документе, но должна базироваться на типе сетевой услуги. Здесь должны быть указаны реальные определения, соответствующие каждому типу услуги.

5 Местоположение <program network location> также не определено в настоящем документе, но оно должно определять сетевой протокол, который клиент должен использовать для загрузки программы из сети.

6 Платформа <compatible platform> может быть расширена или определена более детально, чем это сделано в настоящем документе.

Библиография

[b-ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП*.

[b-IETF RFC 1766] IETF RFC 1766 (1995), *Tags for the Identification of Languages*. <http://www.ietf.org/rfc/rfc1766.txt>

[b-DO Repo] Reilly, S. and Tupelo-Schneck, R. (2010), *Digital Object Repository Server: A Component of the Digital Object Architecture*, D-Lib Magazine, Vol. 16, No. 1/2. <http://dx.doi.org/10.1045/january2010-reilly>

[b-DOIP] Reilly, S. (2009), *Digital Object Protocol Specification, Version 1.0, Corporation for National Research Initiatives*. <http://hdl.handle.net/4263537/5045>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2013 г.