Международный союз электросвязи

МСЭ-Т X.1252

(04/2010)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность киберпространства – Управление определением идентичности

Базовые термины и определения в области управления определением идентичности

Рекомендация МСЭ-Т X.1252

ITU-T

Международный союз электросвязи

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.379
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	
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.1252

Базовые термины и определения в области управления определением идентичности

Резюме

В Рекомендации МСЭ-Т X.1252 предлагаются определения основных терминов, используемых в области управления определением идентичности (IdM). Эти термины взяты из многих источников, однако считается, что все эти источники являются общеупотребительными в работе в области IdM. Данная Рекомендация не рассчитана на то, чтобы стать большим сборником терминов, относящихся к IdM. Напротив, определенные в Рекомендации термины ограничены теми терминами, которые, как предполагается, составляют базовый перечень наиболее важных и общеупотребительных терминов, касающихся IdM. В настоящую Рекомендацию включено Приложение A, в котором приводятся соображения, лежащие в основе некоторых из этих основных терминов.

Одной из главных задач настоящей Рекомендации является содействие общему пониманию этих терминов группами, которые в настоящее время разрабатывают (или планируют разрабатывать) стандарты в области IdM. Эти определения сформулированы таким образом, чтобы по возможности не зависеть от реализаций или конкретного контекста, и, следовательно, должны подходить в качестве базовых определений для любой деятельности в области IdM. Следует признать, что в некоторых случаях и контекстах может потребоваться более подробная информация по тому или иному конкретному термину, и при этом может быть рассмотрен вопрос о разработке базового определения.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1252	16.04.2010 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

Введение

Составление настоящего перечня терминов и определений в области IdM началось в 2007 году. Оно проводилось в несколько этапов, были получены вклады и замечания от многих людей, и перечень многократно пересматривался. Термины и определения взяты из многих источников. Некоторые из них, но отнюдь не все, перечислены в библиографии. В ряде случаев первоначальное определение было признано соответствующим и включено в перечень, но во многих случаях оно было изменено или объединено с другими, чтобы выработать наилучшее определение для каждого конкретного термина.

Прилагались значительные усилия, с тем чтобы обеспечить, что определения передают то же значение, что и определения в других Рекомендациях | международных стандартах по IdM. Это означает, что в некоторых случаях слова могут не совпадать полностью, но значение должно быть тем же.

Поскольку термин может применяться в ряде различных контекстов, определения ограничиваются базовым или простым описанием термина без возможных альтернатив и вариантов, которые могут иметь место. Если потребуются дополнительные подробности или пояснения, их можно добавить по мере необходимости.

Основные источники, из которых получены определения, обсуждаются ниже, в Приложении A.

Рекомендация МСЭ-Т X.1252

Базовые термины и определения в области управления определением идентичности

1 Сфера применения

В настоящей Рекомендации содержится базовый набор определений терминов, обычно применяемых в отношении управления определением идентичности (IdM). Определения представляют собой базовое определение термина, т. е. их целью является передать основное значение, хотя в порядке исключения включается примечание, если это способствует прояснению ситуации. Соображения, лежащие в основе некоторых из этих основных терминов/определений, включены в Приложение A.

ПРИМЕЧАНИЕ. – Использование термина "идентичность" в настоящей Рекомендации в отношении IdM не указывает на его абсолютное значение. В частности, этот термин не обозначает какого-либо положительного результата установления личности.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T X.501] Рекомендация МСЭ-Т X.501 (2005 г.) | ISO/IEC 9594-2:2005, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Модели.*

[ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

[ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Overview.*

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Authentication framework.*

[ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности для сетей последующих поколений версии 1.*

[ITU-T Y.2702] Рекомендация МСЭ-Т Y.2702 (2008 г.), *Требования к аутентификации и авторизации для СПП варианта 1.*

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

3 Определения

Этот раздел намеренно не заполнен.

4 Аббревиатуры и акронимы

В настоящей Рекомендации используются следующие аббревиатуры:

IdM	Identity management	Управление определением идентичности
IdP	Identity Provider	Поставщик данных идентичности
IdSP	Identity Service Provider	Поставщик услуг определения идентичности
NGN	Next Generation Network	Сеть последующего поколения
PII	Personally Identifiable information	Информация, позволяющая установить личность
RP	Relying Party	Полагающаяся сторона

5 Условные обозначения

Этот раздел намеренно не заполнен.

6 Термины и определения

6.1 контроль доступа (access control): Процедура, применяемая для определения того, следует ли предоставлять тому или иному объекту доступ к ресурсам, устройствам, услугам или информации, на основе заранее установленных правил и конкретных прав или полномочий, связанных с запрашивающей стороной.

6.2 адрес (address): Идентификатор конкретного пункта завершения связи, который используется для маршрутизации.

6.3 агент (agent): Объект, действующий от имени другого объекта.

6.4 объединение (alliance): Соглашение между двумя или более независимыми объектами, которое определяет, как они соотносятся друг с другом и как они совместно ведут деятельность.

6.5 анонимность (anonymity): Ситуация, при которой объект невозможно определить в комплексе объектов.

ПРИМЕЧАНИЕ. – Анонимность препятствует отслеживанию объектов или их поведения, например местоположение пользователя, частота использования услуги и т. д.

6.6 утверждение (assertion): высказывание, сделанное объектом и не сопровождаемое доказательствами его истинности[1].

6.7 гарантия (assurance): См. обеспечение аутентификации и обеспечение идентичности.

6.8 уровень гарантии (assurance level): Уровень доверия в связи между объектом и представленной информацией идентичности.

6.9 атрибут (attribute): Информация, связанная с объектом, которая означает какую-либо его характеристику.

6.10 тип атрибута (attribute type) [ITU-T X.501]: Компонент атрибута, который указывает класс информации, передаваемой атрибутом.

6.11 значение атрибута (attribute value) [ITU-T X.501]: Конкретный экземпляр класса информации, указанного типом атрибута.

6.12 аутентификация (объекта) ((entity) authentication): Процесс, используемый для достижения достаточной меры доверия в связи между объектом и представленной идентичностью.

ПРИМЕЧАНИЕ. – Использование термина "аутентификация" в контексте управления определением идентичности (IdM) означает аутентификацию объекта.

---

[1] Термины "утверждение" и "заявление" считаются очень схожими.

6.13 гарантия обеспечения аутентификации (authentication assurance): Степень доверия, достигаемого в процессе аутентификации, в отношении того, что партнер по связи является тем объектом, которым он утверждает, что является, или которым ожидается, что он является.

ПРИМЕЧАНИЕ. – Доверие основано на степени доверия в связи между взаимодействующим объектом и представленной информацией идентичности.

6.14 авторизация (authorization) [ITU-T Y.2720] и [ITU-T X.800]: Предоставление прав и, на основе этих прав, предоставление доступа.

6.15 связь (binding): Явно установленная взаимосвязь, соединение или привязка.

6.16 биометрическое распознавание (biometric recognition) [b-ISO/IEC CD 2382-37]: Автоматическое распознавание лиц на основе измерения поведенческих и биологических характеристик.

6.17 сертификат (certificate) [ITU-T X.810]: Набор данных, относящихся к безопасности, который выдается руководящим органом по безопасности или доверенной третьей стороной и который используется вместе с информацией безопасности в данных для обеспечения услуг целостности и аутентификации источника данных.

6.18 заявление (claim) [b-OED]: Высказывание, что дело обстоит таким образом, без возможности представить доказательства[1].

6.19 лицо, предъявляющее требование (claimant) [ITU-T Y.2720] и [ITU-T X.811]: Объект, который является или представляет администратора доступа для целей аутентификации.

ПРИМЕЧАНИЕ. – Лицо, предъявляющее требование, выполняет функции, необходимые для участия в аутентификационном обмене от имени администратора доступа.

6.20 контекст (context): Среда с определенными граничными условиями, в которой существуют и взаимодействуют объекты.

6.21 полномочия (credential): Набор данных, представляемых как доказательство утверждаемой идентичности и/или прав.

6.22 делегирование (delegation): Действие по передаче полномочий, ответственности или функций другому объекту.

6.23 цифровая идентичность (digital identity): Цифровое представление информации, известной о конкретном лице, группе или организации.

6.24 запись (enrolment): Процесс включения объекта в контекст.

ПРИМЕЧАНИЕ 1. – Запись может включать верификацию идентичности объекта и создание контекстуальной идентичности.

ПРИМЕЧАНИЕ 2. – Наряду с этим запись может служить предпосылкой для процесса регистрации. Во многих случаях последний термин используется для описания обоих процессов.

6.25 объект (entity): Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п., или группа таких объектов. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

6.26 аутентификация объекта (entity authentication): Процесс достижения достаточного доверия к связи между объектом и представленной идентичностью.

ПРИМЕЧАНИЕ. – Использование термина "аутентификация" в контексте управления определением идентичности (IdM) означает аутентификацию объекта.

6.27 федерация (federation): Ассоциация пользователей, поставщиков услуг и поставщиков услуг данных идентичности.

6.28 идентификация (identification): Процесс опознания объекта по контекстуальным характеристикам.

6.29 идентификатор (identifier): Один или несколько атрибутов, используемых для идентификации объекта в том или ином контексте.

6.30 идентичность (identity): Представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют однозначно распознать объект или объекты в каком-либо контексте в той мере, в какой это необходимо. В целях управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

ПРИМЕЧАНИЕ. – Каждый объект представлен одной целостной идентичностью, которая включает все возможные элементы информации, характеризующие такой объект (атрибуты). Вместе с тем такая целостная идентичность является теоретическим понятием и не может быть описана и практически использована, поскольку число всех возможных атрибутов бесконечно.

6.31 гарантия определения идентичности (identity assurance): Степень доверия в процессе валидации и верификации, используемом для установления идентичности объекта, которому были предоставлены полномочия, и степень доверия в отношении того, что объект, который использует полномочия, является данным объектом или объектом, которому полномочия были предоставлены или переданы.

6.32 политика безопасности на базе идентичности (identity based security policy) [ITU-T X.800]: Политика безопасности, базирующаяся на идентичностях и/или атрибутах пользователей, группы пользователей или объектов, действующих от имени пользователей, и оцениваемых ресурсах/объектах.

6.33 поставщик мостовых услуг определения идентичности (identity service bridge provider): Поставщик услуг определения идентичности, выступающий в качестве доверенного посредника между другими поставщиками услуг определения идентичности.

6.34 управление определением идентичности (identity management) [ITU-T Y.2720]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и связывание, обеспечение реализации политики, аутентификация и утверждения), используемых для: гарантирования информации, подтверждающей идентичность (например, идентификаторов, полномочий, атрибутов); гарантирования идентичности объекта и обеспечения коммерческих приложений и приложений безопасности.

6.35 схема идентичности (identity pattern): Структурированное выражение атрибутов объекта (например, поведение объекта), которое может применяться в некоторых процессах идентификации.

6.36 проверка подлинности идентичности (identity proofing): Процесс, в ходе которого выполняется валидация и верификация достаточного объема информации, чтобы подтвердить заявленную идентичность объекта.

6.37 поставщик данных идентичности (identity provider) (IdP): См. поставщик услуг определения идентичности (IdSP).

6.38 поставщик услуг данных идентичности (identity service provider) (IdSP): Объект, который выполняет верификацию, поддерживает информацию об идентичности других объектов, управляет ею и может ее создавать и назначать.

6.39 верификация идентичности (identity verification): Процесс подтверждения того, что заявленная идентичность подлинна, путем сравнения предложенных заявлений идентичности с ранее проверенной информацией.

6.40 проявление (manifestation): Наблюдаемое или обнаруженное (т. е. не самозаявленное) представление объекта. (Сравнить с утверждением.)

6.41 взаимная аутентификация (mutual authentication): Процесс, в ходе которого два объекта (например, клиент и сервер) аутентифицируют друг друга таким образом, что каждый убеждается а идентичности другого.

6.42 наименование (name): Выражение, под которым известен объект, и с помощью которого осуществляется его адресация и обращение к нему.

ПРИМЕЧАНИЕ. – Наименование используется в том или ином контексте, и не предполагается, что оно является уникальным или однозначных. Для целей маршрутизации оно может быть преобразовано или транслировано в адрес.

6.43 предотвращение от отказа (non-repudiation): Способность защиты от отказа со стороны одного из объектов, задействованных в действии, принимать участие во всем действии или в его части.

6.44 схема (pattern): См. схема идентичности.

6.45 устойчивый (persistent): Существующий и способный к использованию в службах вне прямого контроля наделяющего полномочиями объекта без заявленных ограничений по времени.

6.46 информация, позволяющая установить личность (personally identifiable information, PII): Любая информация, a) которая идентифицирует или может использоваться для идентификации, обращения или установления местоположения лица, к которому такая информация относится; b) на основе которой может быть осуществлена идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

6.47 администратор доступа (principal) [ITU-T Y.2720], [ITU-T X.811] и [ITU-T Y.2702]: Объект, идентичность которого может быть аутентифицирована.

6.48 неприкосновенность частной жизни (privacy): Право частных лиц осуществлять контроль или влияние в отношении того, какую информацию личного характера, относящуюся к ним, можно собирать, управлять, сохранять, делать доступной, использовать или распространять.

6.49 политика в отношении неприкосновенности частной жизни (privacy policy): Политика, которая определяет требования к защите доступа к информации, позволяющей установить личность (PII), и ее распространения, а также права частных лиц в отношении использования их информации личного характера.

6.50 привилегия (privilege): Право, которое при его предоставлении какому-либо объекту разрешает этому объекту выполнять то или иное действие.

6.51 проверка подлинности (proofing): Верификация и валидация информации при записи новых объектов в системах идентичности.

6.52 псевдоним (pseudonym): Идентификатор, связь которого с объектом неизвестна или известна лишь в ограниченной степени, в контексте, в котором он используется.

ПРИМЕЧАНИЕ. – Псевдоним может использоваться для предотвращения или снижения рисков, связанных с использованием связей идентификатора, которые могут раскрыть идентичность объекта.

6.53 регистрация (registration): Процесс, в ходе которого объект запрашивает и получает привилегии использования услуги или ресурса.

ПРИМЕЧАНИЕ. – Запись является предпосылкой регистрации. Эти функции могут быть объединенными или отдельными.

6.54 полагающаяся сторона (relying party (RP)) [ITU-T Y.2720]: Объект, который полагается на представленную или заявленную идентичность запрашивающего/утверждающего объекта в каком-либо контексте запроса.

6.55 непризнание участия (repudiation): Отрицание одним из задействованных объектов своего участия во всем действии или в его части.

6.56 запрашивающий объект (requesting entity): Объект, обращающийся к полагающейся стороне с представлением или заявлением идентичности в каком-либо контексте запроса.

6.57 аннулирование (revocation): признание имеющим полномочия недействительным чего-либо, что сделано ранее.

6.58 роль (role): Комплекс свойств или атрибутов, которые описывают способности или функции, выполняемые объектом; каждый объект может играть много ролей.

ПРИМЕЧАНИЕ. – Каждый объект может иметь/играть много ролей. Способности могут быть изначальными или полученными.

6.59 проверка безопасности (security audit) [ITU-T X.800]: Независимый анализ и рассмотрение записей и действий системы для обеспечения соблюдения установленных политических и эксплуатационных процедур, для обнаружения брешей в системе безопасности и для рекомендаций каких-либо указанных изменений в контроле, политике и процедурах.

6.60 домен безопасности (security domain) [ITU-T Y.2720], [ITU-T Y.2701] и [ITU-T X.810]: Совокупность элементов, политика безопасности, орган безопасности и совокупность действий по обеспечению безопасности, в которых управление элементами осуществляется в соответствии с политикой безопасности.

6.61 зона безопасности (security zone) [ITU-T Y.2701]: Защищенная зона, определяемая оперативным управлением, местоположением и возможностью соединения с другими устройствами/элементами сети.

6.62 полномочия в отношении домена безопасности (security domain authority) [ITU-T X.810]: Полномочия в отношении обеспечения безопасности, касающиеся реализации политики безопасности в домене безопасности.

6.63 самозаявленная идентичность (self-asserted identity): Идентичность, которая по заявлению объекта является его собственной идентичностью.

6.64 доверие (trust): Твердая уверенность в надежности и истинности информации или в возможности или расположенность объекта действовать надлежащим образом в конкретном контексте.

6.65 уровень доверия (trust level): Постоянная, поддающаяся измерению мера уверенности в репутации, способностях, силе или истинности кого-то или чего-то.

6.66 доверенная третья сторона (trusted third party) [ITU-T Y.2702], [ITU-T X.800] и [ITU T X.810]: В контексте политики обеспечения безопасности – орган обеспечения безопасности или его агент, который является доверенным в отношении некоторых связанных с безопасностью действий.

6.67 пользователь (user): Любой объект, использующий ресурс, например систему, оконечное оборудование, процесс, приложение или корпоративную сеть.

6.68 ориентированная на пользователя (user-centric): Система управления определением идентичности (IdM), при которой пользователю предоставляется право контролирования и обеспечения соблюдения различных видов политики конфиденциальности и безопасности, определяющих обмен между объектами информацией об идентичности, в том числе информацией, позволяющей установить личность (PII) пользователей.

6.69 верификация (verification): Процесс или экземпляр установления аутентичности чего-либо.

ПРИМЕЧАНИЕ. – Верификация информации (идентичности) может охватывать рассмотрение на предмет действительности, правильности источника, подлинности (отсутствия изменений), правильности, связи с объектом и т. д.

6.70 верификатор (verifier): Объект, который выполняет верификацию и валидацию информации идентичности.

Приложение A

Основные пункты и обоснование базовой терминологии IdM

(Настоящее Приложение является неотъемлемой частью настоящей Рекомендации)

Базовая информация

Дискуссии по поводу управления определением идентичности (IdM) выявили различия в представлениях людей о назначении IdM, о применяемых базовых процедурах, а также в терминологии и определениях терминов. Эти различия приводили к недопониманию и к длительным обсуждениям в процессе стандартизации IdM.

Чтобы помочь избегать этого недопонимания в будущем, в настоящем приложении отражены некоторые соглашения, достигнутые в ходе дискуссий в МСЭ-Т по этим базовым концепциям и терминологии, а также разъясняется ход мыслей, приведших к разработке (а в некоторых случаях – к принятию) терминов, включенных в настоящую Рекомендацию. Следует отметить, что в настоящем Приложении не излагается и не разъясняется общая концепция управления определением идентичности.

Введение

Идентичность – это термин, который лежит в основе всех остальных терминов IdM. Например, в реальном мире, в отличие от цифрового мира, идентичность физического лица является общепринятым понятием и основывается на обширном круге характеристик или атрибутов. Некоторые из них являются физическими характеристиками, такими как рост, цвет волос, наружность в целом, привычки, поведение и т. п. Могут использоваться и другие, такие как дата и место рождения, домашний адрес, номер телефона. В процессе коммуникации обеим сторонам обычно необходимо быть в достаточной мере уверенными, что они общаются с нужным им партнером. В этом процессе обеспечения уверенности зачастую участвуют два или более лиц или "объектов": объект, идентичность которого подлежит подтверждению – *запрашивающий объект,* и объект, который будет полагаться на подтвержденную идентичность – *полагающаяся сторона*. Может участвовать и третья сторона, которая управляет определением идентичности – *поставщик услуг определения идентичности.*

В "цифровом" или "онлайновом" мире "идентичность" также складывается из атрибутов, как и в реальном мире. Вместе с тем в этом случае "идентичность" может ограничиваться одной характеристикой или состоять из многих; это зависит от контекста, в котором она находится. Это относится к неодушевленным предметам, а также к физическим лицам, поэтому пользователей часто называют объектами.

Как правило, идентификаторы и/или атрибуты однозначно характеризуют объект в конкретном контексте. Ввиду этого тот или иной объект может иметь ряд различных идентичностей, и некоторые из них будут подмножеством других идентичностей.

A.1 Аутентификация и уверенность

Процесс аутентификации является существенной частью IdM. Ниже дается объяснение процесса аутентификации и его значения для уверенности.

Следует отметить, что при применении этой модели к реальным процедурам и приложениям нужно очень четко представлять себе соответствующих партнеров по общению и применимые цепочки доверия.

Процесс аутентификации можно описать следующим образом:

Для большинства процессов коммуникации необходимо, чтобы партнеры по коммуникации обладали достаточными уверенностью или доверием в отношении того, что они действительно общаются с тем партнером, с которым и собирались. Ввиду этого в начале процесса коммуникации партнеры стремятся достичь надлежащего уровня уверенности на основании имеющей информации идентичности о партнере, т. е. уверенности в связи между объектом и представленным объектом.

Процесс установления уверенности особенно важен, когда партнеры по коммуникации удалены друг от друга и соединены только линией электросвязи. Процесс аутентификации проводится, чтобы убедиться с достаточной степенью уверенности, что идентичность, представленная партнером по коммуникации, действительно ему принадлежит.

В процессе коммуникации всегда участвуют два или более отдельных партнеров, которые обмениваются информацией. В связи с широким разнообразием возможных партнеров (людей и вещей) необходимо дать определение общему термину. Был выбран термин *объект*, который определяется как: что-либо, что существует отдельно и самостоятельно и что можно идентифицировать в контексте.

ПРИМЕЧАНИЕ:

- Объект может быть физическим лицом, животным, юридическим лицом, организацией, активной или пассивной вещью, устройством, приложением программного обеспечения, услугой, или группой этих объектов.
- В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

Информация, которая может использоваться для идентификации объекта, основывается на атрибутах объекта. *Атрибут* определяется как информация, связанная с объектом, которая означает какую-либо его характеристику. В практическом отношении идентификация объекта обычно основывается на подмножестве его атрибутов, поскольку идентификация ограничивается тем, что называется контекстом, в котором объект существует и взаимодействует. Чем уже контекст и четче граничные условия, тем меньше число атрибутов, необходимых для идентификации. *Контекст* определяется как среда с определенными граничными условиями, в которой существуют и взаимодействуют объекты.

Поскольку определение объекта зависит от способности быть идентифицированным, необходимо иметь надлежащее определение *идентификации*: процесс опознания объекта по тому, как он характеризуется в контексте.

Для того чтобы различать объекты, достаточно использовать подмножество атрибутов, адекватное контексту. Это называется *идентичность*, которая определяется как представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют однозначно распознать объект или объекты в каком-либо контексте в той мере, в какой это необходимо. В целях IdM термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

Идентичность может быть подмножеством другой идентичности. Также могут существовать области пересечения идентичностей. Вместе с тем по различным причинам (например, по соображениям неприкосновенности частной жизни) использование областей пересечения идентичностей в различных целях и в различных контекстах может быть явно нежелательным или даже исключаться.

На рисунке А.1 показаны взаимосвязи между объектом, идентичностями и атрибутами.

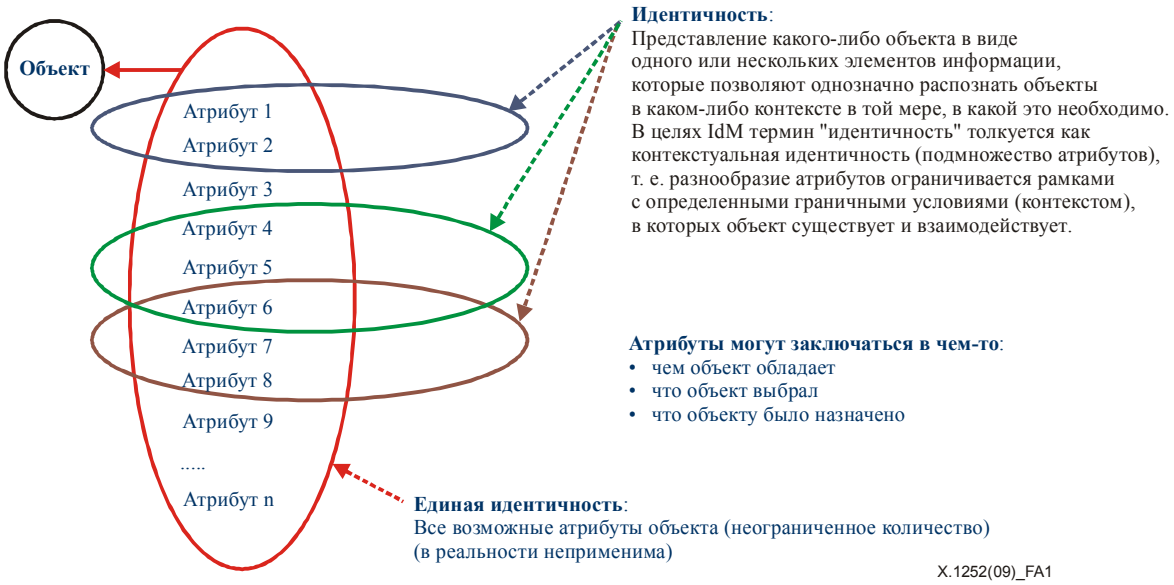


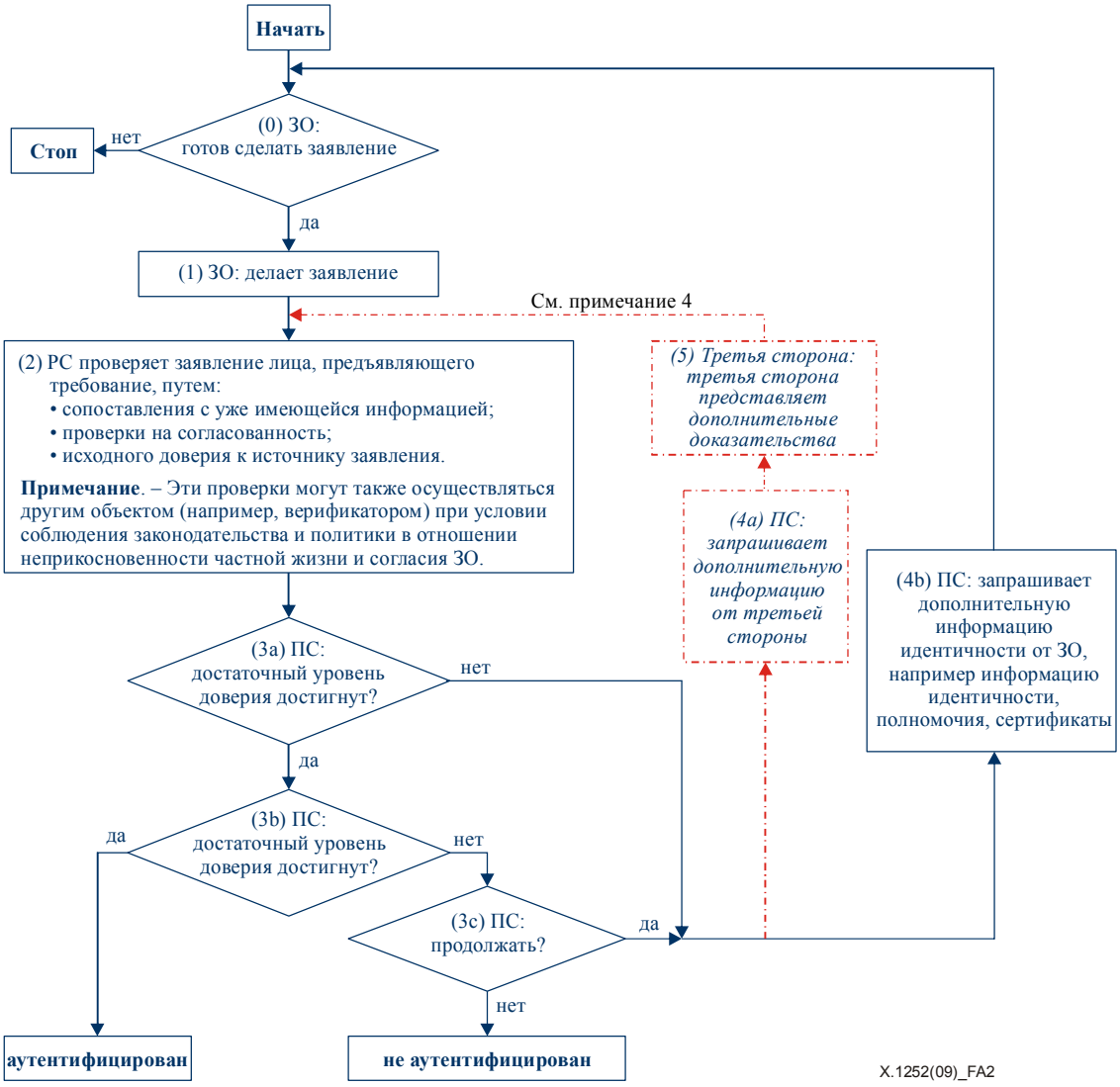
Рисунок А.1 – Взаимосвязи между объектом, идентичностями и атрибутами

Как уже отмечалось, аутентификация имеет значение для управления определением идентичности. Это процесс, необходимый для обеспечения достаточной уверенности в отношении того, что коммуникация происходит с нужным партнером. Фактический уровень требуемой уверенности будет зависеть от степени конфиденциальности приложения и/или от риска причинения ущерба вследствие общения с не тем партнером.

Права или привилегии могут назначаться для различных целей, в том числе, например:

- для совместного использования или доставки информации, которая не предназначается для всеобщего ознакомления;
- для предоставления доступа к:
  - информации;
  - помещениям/зонам/доменам;
  - услугам;
  - использованию ресурсов;
- для заключения контрактов.

Для обретения такого доверия необходимо, чтобы партнера по коммуникации можно было легко отличить от других возможных партнеров по коммуникации и чтобы при необходимости это отличие можно было периодически переоценивать.



Примечание 1. – На данном рисунке показан однонаправленный процесс аутентификации. Обычно этот процесс осуществляется во взаимном и/или перемежающемся порядке.
Примечание 2. – Если уровень уверенности не требуется, этап 2 можно опустить.
Примечание 3. – Этот поток можно выполнять несколько раз, и эти повторения также могут быть разнесены во времени и/или пространстве.
Примечание 4. – Участие третьей стороны возможно при условии соблюдения законодательства и политики в отношении неприкосновенности частной жизни и согласия ЗО. (-·-·-·-·-)

Рисунок А.2 – Однонаправленный процесс аутентификации

Как правило, этот процесс обеспечения уверенности, т. е. процесс аутентификации, происходит на взаимной основе. Это означает, что процесс аутентификации, показанный на рисунке А.2, проходит дважды, при этом каждый из объектов играет каждую из ролей, т. е.:

Аутентификация Y: Объект Y выступает в роли запрашивающего объекта (ЗО), а объект X – в роли полагающейся стороны (ПС).

Аутентификация X: Объект X выступает в роли запрашивающего объекта, Y – в роли полагающейся стороны.

Для упрощения и лучшего понимания показанный на рисунке А.2 процесс описан только в одном направлении. В то же время потоки этих двух процессов перемежаются.

Перемежающееся исполнение дает сторонам возможность проверить предпосылки до представления потенциально конфиденциальных атрибутов. Такими условиями могут быть:

- знание того, как обращаться к полагающейся стороне;
- достаточное доверие в отношении того, что полагающаяся сторона является той самой (например: пользователи должны быть в определенной мере уверены, что они находятся на нужной веб-странице, прежде чем заносить информацию идентичности, такую как имя пользователя и пароль).

В некоторых случаях (но не в ориентированных на пользователя системах) может быть непосредственно задействована третья сторона для предоставления дополнительной информации в качестве доказательств полагающейся стороне для повышения доверия к атрибутам запрашивающего объекта.

Идентичности состоят из атрибутов. Они могут быть чем-то:

- что объект имеет (например, кодовой картой);
- что объект знает (например, пароль);
- каким объект является (например, цвет, размер);
- что объект способен делать (например, особое кодирование);
- местонахождением объекта;
- сочетанием этих факторов.

Идентичность можно проверить:

- по последовательности самой информации;
- по соответствию другой поддерживающей информации;
- в сравнении с уже известной информацией.

Атрибуты могут также указываться в виде *схемы идентичности*, которая представляет собой структурированное выражение атрибутов объекта (например, поведение объекта), которое может применяться в некоторых процессах идентификации.

Следует особо отметить, что, как показано в примере блок-схемы на рисунке А.2, решение относительно того, принимать ли запрашивающий объект, всегда принимает полагающаяся сторона на основе процесса аутентификации. Больше никто этого решения принять не может.

Как правило, каждый партнер по коммуникации должен быть в состоянии установить уровень уверенности, необходимый для осуществления привилегий. Вместе с тем это право может быть ограниченным, а в ряде случаев – ограничиваться в законодательном порядке.

Когда налицо значительная асимметрия между партнерами по коммуникации, существует также опасность того, что более сильный партнер злоупотребит этой ситуацией и затребует недостаточно высокий уровень доверия или же откажет в собственной аутентификации. Ввиду этого необходимо, чтобы техническая реализация механизмов аутентификации основывалась на симметричных механизмах в целях избежания асимметрии. Наряду с этим может возникнуть необходимость в регулировании для предотвращения доминирования одной из сторон с целью предупреждения использования положения доминирования в асимметричных ситуациях.

В целом при применении управления определением идентичности необходимо очень четко представлять себе задействованные объекты и их цель, с тем чтобы ограничить контекст и идентичности (комплекс атрибутов) для этой конкретной цели.

Для уровня уверенности исключительно в целях электросвязи обычно достаточно, чтобы клиент обладал достаточной уверенностью для подключения к соответствующему поставщику транспорта или услуг, а поставщики были уверены в том, что использование услуг разрешено, за них можно выставлять счета и они должны быть оплачены. Последнего можно добиться аутентификацией, например, точки доступа или счета абонента, который не обязательно должен быть идентичным фактическому пользователю услуги или указывать на него. В некоторых случаях, таких как телефонные карты с предоплатой или SIM-карты с предоплатой, аутентификации не требуется.

В процессе аутентификации могут быть представлены полномочия как доказательство некоторых или всех атрибутов представленной контекстуальной идентичности. *Полномочия* определяются как набор данных, представляемых как доказательство утверждаемой идентичности и/или прав. В то же время необходимо четко различать два вида полномочий:

1) набор данных, представленных как доказательство заявленной идентичности, что важно для целей аутентификации (например, паспорт). Полномочия такого рода используются для повышения доверия к атрибутам путем подтверждения через сторону, которая выдает полномочия; и

2) набор данных, представленных как доказательство прав, что важно только для целей аутентификации (например, билет на концерт или футбольный матч). Он дает возможность воспользоваться привилегией (быть допущенным на мероприятие на основе обладания билетом), при этом не обязательно раскрывая идентичность объекта, предъявляющего полномочия.

Некоторые полномочия могут выполнять обе функции, и оба типа полномочий могут подвергаться отдельному процессу аутентификации.

A.2 Заявление/утверждение

Обычно признается, что значения терминов "заявление" и "утверждение" несколько схожи, но немного различаются. В некоторых случаях утверждение считается более "сильным" высказыванием, чем заявление. Так, в Оксфордском словаре английского языка "заявление" определяется как:

a) утверждение, что дело обстоит таким образом, без возможности представить доказательства;

b) утверждение, что что-то имеет место,

а "утверждение" – как уверенное и убедительное заявление. Вместе с тем в цифровом контексте определения "уверенный" и "убедительный" практически лишены смысла.

В открытых сетях существуют более сложные и многозначные отношения между делающей заявление стороной (т. е. представляющей информацию идентичности) и стороной, которая на него полагается. Ввиду этого любое заявление подвергается сомнению, и вследствие этого подвергается верификации, или же запрашиваются дополнительные доказательства. Нельзя заранее принимать, что заявления или утверждения делаются с какими-либо полномочиями. Решение относительно того, принимать ли заявление или утверждение на основании верификации полагающейся стороной (или верификатором, действующим по поручению полагающейся стороны), всегда принимает полагающаяся сторона.

A.3 Запись и регистрация

Запись и регистрация – это два процесса, которые тесно взаимосвязаны и которые частично совпадают. Иногда эти термины взаимозаменяемы и, хотя они могут сочетаться в одном этапе, по сути своей это два отдельных процесса.

Запись – это процесс включения объекта в контекст (или его создания в контексте). Запись может включать верификацию идентичности объекта и создание контекстуальной идентичности. Регистрация – это процесс, в ходе которого объект запрашивает и получает привилегии использования услуги или ресурса. Запись является предпосылкой регистрации.

В реальном мире пользователь может, например, в какой-то момент, записаться для получения общих банковских услуг, а затем, позже, зарегистрироваться для получения онлайновых банковских услуг. Или же пользователь может, открывая новый счет, осуществить идентификацию (и связанные с ней формальности) (т. е. записаться) и в то же время зарегистрироваться для получения онлайновых банковских услуг.

A.4 Поставщик данных идентичности и поставщик услуг данных идентичности

Изучение текущей практики показывает, что широко применяется как термин *поставщик данных идентичности*, так и термин *поставщик услуг определения идентичности*. Хотя термин *поставщик данных идентичности* используется в некоторых действующих Рекомендациях МСЭ-Т, можно понять его так, будто им обозначается объект, который *поставляет* данные идентичности, а не объект, который *управляет* определением идентичности. Кроме того, этот термин неточен, поскольку идентичности нельзя предоставлять, они существуют или развиваются, когда придаются атрибуты.

Наряду с этим термин *поставщик услуг* широко употребляется в таких обозначениях, как поставщик услуг верификации, поставщик услуг полномочий, поставщик финансовых услуг и т. п.

Ввиду этого термин *поставщик услуг определения идентичности* считается несколько более точным, чем *поставщик данных идентичности*, и ему следует отдавать предпочтение. Такое переход возможно осуществить при минимальном воздействии на существующие документы, используя действующее в настоящее время определение *поставщика данных идентичности* для *поставщика услуг определения идентичности* и сохраняя термин *поставщик данных идентичности*, но, вместо того чтобы давать ему определение, просто отсылая к термину *поставщик услуг определения идентичности.* Следует применять акроним IdSP.

A.5 Схема идентичности

Как правило, схемы рассматриваются в качестве информации, которая наблюдается или распознается, и у которой может быть обнаружена структура, либо которая соответствует уже известной структуре. Таким образом, схему идентичности можно рассматривать в качестве характеризующей объект информации, которая наблюдается или опознается, и для которой может быть обнаружена структура, либо которая соответствует уже известной структуре.

Например, двумя соответствующими словарными определениями термина *схема* являются: "регулярная или повторяющаяся форма, порядок или расположение"; и "надежный образец признаков, событий, тенденций или других наблюдаемых характеристик лица, группы или учреждения".

В общем плане и с учетом указанных выше определений схема подразумевает, что существует несколько элементов схемы, однако повтор одного атрибута с течением времени также представляет собой схему. Одно появление одного атрибута не будет представлять собой схему, однако способ появления одного или нескольких атрибутов может образовывать схему. Кроме того, схема идентичности может основываться не только на деятельности или поведении, и она не ограничивается информацией, которая наблюдается или опознается. Иногда она может базироваться на любом(ых) атрибуте(ах). Например, профиль шины имеет четкую и поддающуюся обнаружению структуру. Таким образом, в данном случае сам атрибут может рассматриваться как схема идентичности. Также не всегда имеет место обязательное наблюдение схемы несколько раз, приводящее к практическим результатам. Например, когда два человека говорят о каком-либо автомобиле в автосалоне компании-продавца, то они могут указать на него как на "тот, что стоит в дальнем левом углу".

Схемы могут допускать повторное применение, но можно также представить себе ситуации, когда схема используется только один раз, например однократные коды.

Можно возразить, что все атрибуты имеют какую-либо структуру, но, несмотря на это, четкое различие между атрибутами и схемами идентичности заключается в том, что структура обнаруживается и устанавливается наблюдателем, однако не всегда структура известна другим объектам, даже наблюдаемым.

Схемы идентичности могут использоваться не только для целей идентификации, но также в ряде случаев для аутентификации, либо просто для определения категории или классификации объектов. Одним из примеров классификации является изучение поведения потребителей для определения того, какие виды продуктов они покупают и как часто они это делают. В данном "маркетинговом" контексте схемы используются для классификации объектов в зависимости от определенных групп объектов, однако соединение ряда таких схем друг с другом могло бы привести к идентификации одиночных объектов.

Элементы, используемые для идентификации объекта, должны позволять однозначно распознавать объект в каком-либо контексте в той мере, в какой это необходимо. Если схему идентичности предполагается использовать для индивидуальной (в отличие от групповой) идентификации или аутентификации, то схема идентичности должна быть уникальной и однозначной. Однако в ряде случаев, когда схема идентификации используется для авторизации, то может не потребоваться, чтобы она была уникальной или однозначной. В качестве примера можно привести ситуацию, когда необходимо ограничить число пользователей конкретной услуги, например при участии в спортивных соревнованиях. В этом случае, возможно, потребуется применять ограничения, например, на основе режима потребления определенных лекарств.

Библиография

При разработке данного перечня терминов и определений IdM использовались многочисленные публикации по IdM, уже существующие работы и глоссарии. Перечень отнюдь не является исчерпывающим, но включает:

[b-ISO/IEC CD 2382-37] ISO/IEC CD 2382-37, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary*.

[b-ANSI] Американский национальный институт стандартов: http://www.ansi.org/.

[b-AusCert] Конференция AusCert-2005.

[b-Carnegie] Вычислительные услуги университета Карнеги-Меллона®: www.cmu.edu/acs/documents/idm/.

[b-NSS] Рабочая группа по Глоссарию Комитета по системам национальной безопасности.

[b-Edentity] Компания Edentity: http://www.edentity.co.uk/.

[b-ETSI] Интерактивная база данных терминов и определений ETSI: http://webapp.etsi.org/Teddi/.

[b-EU] Подразделение по вопросам электронного правительства Комиссии ЕС, Генеральный директорат по вопросам информационного общества и СМИ.

[b-ICANN] Корпорация Интернет по присваиванию наименований и номеров (ICANN): http://www.icann.org/en/general/glossary.htm.

[b-Identity] Портал Identity Commons http://wiki.idcommons.net/Main_Page.

[b-IETF] Сетевая рабочая группа Целевого фонда IETF Trust (2007 г.).

[b-ISO/IEC] ISO/IEC JTC 1/SC 27/WG5.

[b-ITU-T Id Mgmt] Оперативная группа МСЭ-Т по вопросам управления определением идентичности.

[b-ITU-T Terms] База терминов и определений МСЭ-Т: http://www.itu.int/ITU-T/dbase.

[b-Cameron] Kim Cameron's Laws of Identity: http://www.identityblog.com/?p=354.

[b-Liberty] Технический глоссарий организации Liberty Alliance.

[b-Modinis] Веб-портал Modinis: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome.

[b-NetMesh] Компания NetMesh® Inc.: http://www.netmesh.us/.

[b-NIST] Национальный институт стандартов и технологии: http://www.nist.gov/index.html.

[b-OASIS] Организация по развитию стандартов структурированной информации (ОРССИ): http://www.oasis-open.org/committees/security/ipr.php.

[b-OED] Оксфордский словарь английского языка.

[b-OECD] Рекомендация ОЭСР по электронной аутентификации.

[b-Mobile] Альянс Open Mobile Alliance™: http://www.openmobilealliance.org/UseAgreement.html.

[b-STORK] Консорциум STORK-eID: http://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1.

[b-Trusted] Организация Trusted Computing Group: http://www.trustedcomputinggroup.org/.

[b-IAAC] Консультативный совет по вопросам информации Соединенного Королевства: http://www.iaac.org.uk/Default.aspx?tabid=1.

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, 2010 г.