Международный союз электросвязи

МСЭ-Т X.1252

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(04/2021)

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

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 (1)	
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 (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
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
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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 определены основные термины, используемые 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. Рекомендация МСЭ-Т X.1252 не рассчитана на то, чтобы стать масштабным сборником терминов, относящихся к IdM. Напротив, определенные в Рекомендации термины ограничены теми, которые, как предполагается, составляют базовый перечень наиболее важных и общеупотребительных терминов, касающихся IdM. В Рекомендацию МСЭ-Т X.1252 включено приложение, в котором приведены соображения, лежащие в основе некоторых из этих основных терминов.

Одной из главных задач Рекомендации МСЭ-Т X.1252 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 исключить зависимость 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 тогда возможно рассматривать вопрос о разработке базового определения.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1252	16.04.2010 г.	17-я	11.1002/1000/10440
2.0	МСЭ-Т X.1252	30.04.2021 г.	17-я	11.1002/1000/14642

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

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 в целях 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 извещения 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.1252

Базовые термины и определения в области управления определением идентичности

1 Сфера применения

В настоящей Рекомендации определен базовый набор терминов, обычно используемых в области управления определением идентичности (IdM). Определения терминов являются базовыми, то есть они предназначены для передачи основного значения, хотя в порядке исключения добавляется примечание, если оно способствует разъяснению определения. Соображения, лежащие в основе некоторых из этих основных терминов и 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.

Отсутствуют.

3 Определения

Собранные термины и определения IdM перечислены в разделе 6.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

CID	Cryptographic Identifier	Криптографический идентификатор
DDO	DID Object Descriptor	Дескриптор объекта DID
DID	Decentralized Identifier	Децентрализованный идентификатор
DLT	Distributed Ledger Technology	Технология распределенного реестра
ID	Identifier	Идентификатор
IdM	Identity management	Управление определением идентичности
IdP	Identity Provider	Поставщик данных идентичности
IdSP	Identity Service Provider	Поставщик услуг определения идентичности
IH	Identity Hub	Концентратор данных идентичности
PII	Personally Identifiable information	Информация, позволяющая установить личность
PKI	Public Key Infrastructure	Инфраструктура открытых ключей
RA	Registration Authority	Регистрационный орган
RE	Requesting Entity	Запрашивающий объект

RP	Relying Party	Полагающаяся сторона
SIM	Subscriber Identity Module	Модуль идентификации абонента
SSI	Self-Sovereign Identity	Суверенная идентичность
URL	Uniform Resource Locator	Унифицированный указатель ресурса
ZKP	Zero-Knowledge Proof	Доказательство с нулевым разглашением

5 Соглашения

Отсутствуют.

6 Термины и определения

6.1 контроль доступа (access control): Процедура, с помощью которой администратор может ограничивать 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): Определяет конкретный пункт завершения в сети и может быть использован для маршрутизации к этому физическому или логическому пункту по сети общего пользования или частной сети.

ПРИМЕЧАНИЕ. – На основании [b-ITU-T E.101].

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

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

6.5 аноним (anonym): Идентификатор, используемый только один раз.

6.6 анонимность (anonymity): Ситуация, при которой объект невозможно определить в совокупности объектов.

ПРИМЕЧАНИЕ. – Анонимность может препятствовать слежению, отслеживанию, обнаружению и созданию цифрового отпечатка объектов или их характеристик, таких как местоположение пользователя и частота использования услуги.

6.7 утверждение (assertion): Высказывание, сделанное объектом и не сопровождаемое доказательствами его истинности.

ПРИМЕЧАНИЕ. – Термины "утверждение" и "заявление" считаются очень схожими.

6.8 гарантия (assurance).

ПРИМЕЧАНИЕ. – См. "Гарантия обеспечения аутентификации" и "Гарантия определения идентичности ".

6.9 уровень гарантии (assurance level): Уровень уверенности в привязывании к объекту представленной информации об идентичности.

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

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

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

6.13 аутентификация (authentication) [b-ISO/IEC 24760-1]: Формализованный процесс проверки, при успешном прохождении которого идентичность объекта считается установленной.

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

6.14 гарантия обеспечения аутентификации (authentication assurance): Подтверждение в процессе аутентификации, направленное на обеспечение уверенности в том, что партнер по связи является тем объектом, которым, как он утверждает, он является или которым, как ожидается, он является.

ПРИМЕЧАНИЕ. – Гарантия основана на степени уверенности в привязывании к взаимодействующему объекту представленной информации об идентичности.

6.15 авторизация (authorization): Предоставление прав и, на основе этих прав, предоставление доступа.

ПРИМЕЧАНИЕ. – Основано на [b-ITU-T X.800].

6.16 привязывание (binding): Явно установленная взаимосвязь, соединение или увязка.

6.17 биометрическое распознавание; биометрия (biometric recognition; biometrics) [b-ISO/IEC 2382-37]: Автоматическое распознавание лиц на основе их биологических и поведенческих характеристик.

6.18 сертификат (certificate): Набор данных, относящихся к безопасности, который выдается руководящим органом по безопасности или доверенной третьей стороной и который используется вместе с информацией о безопасности в данных для обеспечения услуг целостности и аутентификации источника данных.

ПРИМЕЧАНИЕ. – Основано на определении "сертификат безопасности" в [b-ITU-T X.810].

6.19 заявление (claim): Утверждение объекта в цифровой форме об атрибутах идентичности (своих или другого объекта). **Заявлять** – утверждать, что дело обстоит таким образом, без возможности представить доказательства.

ПРИМЕЧАНИЕ. – Термины "утверждение" и "заявление" считаются очень схожими.

6.20 лицо, предъявляющее требование (claimant): Объект, который является администратором доступа или представляет его для целей аутентификации.

ПРИМЕЧАНИЕ 1. – Лицо, предъявляющее требование, выполняет функции, необходимые для участия в аутентификационном обмене от имени администратора доступа.

ПРИМЕЧАНИЕ 2. – Основано на [b-ITU-T X.811].

6.21 определение заявления (claim definition): Машиночитаемое определение семантической структуры заявления.

ПРИМЕЧАНИЕ. – Определения заявлений облегчают обеспечение функциональной совместимости заявлений и доказательств для множества различных эмитентов, держателей и полагающихся сторон.

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

6.23 увязка (correlation): Сочетание различных элементов информации, которые связаны с некоторым объектом или приобретают такую связь, будучи объединены друг с другом.

ПРИМЕЧАНИЕ. – Увязка тесно связана с идентификацией. Увязка облегчает идентификацию и логический вывод недостающей информации об объекте, которая отсутствует непосредственно в имеющихся данных.

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

ПРИМЕЧАНИЕ. – Стандарт [b-ISO/IEC 29115] сходен по содержанию с [b-ITU-T X.1254] и содержит то же определение полномочий, которое было разработано группами, участвовавшими в создании обоих документов.

6.25 минимизация данных (data minimization): Ограничение сбора, хранения и использования идентификаторов, атрибутов и прочих связанных с объектом данных только тем объемом, который необходим для аутентификации, а также ограничение обмена и раскрытия связанных с объектом данных (включая информацию о контексте запроса) только тем объемом, который необходим для ответа на запрос, и исключительно полагающейся стороной по данному запросу.

6.26 децентрализованный идентификатор (DID): Глобальный уникальный идентификатор, для регистрации которого не требуется централизованного регистрационного органа, поскольку он зарегистрирован с помощью технологии распределенного реестра или другой децентрализованной системы. DID связан ровно с одним дескриптором объекта DID.

ПРИМЕЧАНИЕ. – См. [b-W3C-DIDs].

6.27 дескриптор объекта DID (DID object descriptor (DDO)): Набор данных, описывающий субъект децентрализованного идентификатора (DID), включая механизмы, такие как открытые криптографические ключи, которые субъект DID или делегат DID могут использовать для аутентификации и подтверждения своей связи с DID.

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

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

6.30 распределенный реестр (distributed Ledger) [b-ITU-T X.1400]: Тип реестра, который используется совместно, копируется и синхронизируется распределенным и децентрализованным образом.

6.31 децентрализованная система управления ключами (decentralized key management system): Стандарт функционально совместимой системы управления криптографическими ключами на основе децентрализованных идентификаторов.

6.32 домен (domain): Среда, в которой объект может использовать набор атрибутов для идентификации и других целей.

ПРИМЕЧАНИЕ. – Домен обеспечивает контекст.

6.33 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.

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

ПРИМЕЧАНИЕ 1. – Объект может иметь физическое или логическое воплощение.

ПРИМЕЧАНИЕ 2. – 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, устройства и интерфейсы.

6.35 аутентификация объекта (entity authentication): Процесс подтверждения и достижения достаточного уровня уверенности в привязывании к объекту представленной идентичности.

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

6.36 федерация (federation) [b-ITU-T Y.2720]: Установление отношений между двумя или более объектами или создание ассоциации, включающей любое количество поставщиков услуг и поставщиков данных идентичности.

6.37 держатель (holder): Объект, которому эмитент выдал заявление. Если заявление поддерживает доказательство с нулевым разглашением, держатель является также проверяющим.

6.38 идентификация (identification) [b-ISO/IEC 24760-1]: Процесс опознания объекта в конкретном домене как отличного от других объектов.

6.39 идентификатор (identifier (ID)) [b-ITU-T E.101]: Последовательность цифр, знаков и символов, используемая для однозначной идентификации абонента, пользователя, элемента сети, функции, объекта сети, услуги или приложения. Идентификаторы могут использоваться для регистрации или авторизации. Они могут быть открытыми, то есть доступными для всех сетей, или закрытыми, то есть доступными для конкретной сети (закрытые идентификаторы, как правило, не разглашаются третьим сторонам).

ПРИМЕЧАНИЕ. – Идентификатор может быть специально созданным атрибутом, которому присвоено уникальное значение в пределах домена.

6.40 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 термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), то есть 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.

6.41 гарантия определения идентичности (identity assurance): Доверие 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.

6.42 политика безопасности на базе идентичности (identity based security policy) [b-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.

6.43 управление определением идентичности (identity management (IdM)): Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и привязывание, 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.

ПРИМЕЧАНИЕ. – Основано на [b-ITU-T Y.2720].

6.44 владелец идентичности (identity owner): Объект, на который может быть возложена ответственность. Владелец идентичности должен быть частным лицом или организацией. Имеет взаимоисключающий смысл с понятием "вещь".

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

6.46 проверка подлинности идентичности (identity proofing) [b-ISO/IEC 29115]: Процесс, в рамках которого орган регистрации (RA) осуществляет сбор и верификацию информации, достаточной для идентификации объекта с определенным или предполагаемым уровнем гарантии.

6.47 поставщик данных идентичности (identity provider (IdP)).

ПРИМЕЧАНИЕ. – См. поставщик услуг определения идентичности (IdSP).

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

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

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

6.51 независимое лицо (independent): Частное лицо, которое непосредственно контролирует личные ключи и мастер-секрет (мастер-секреты), необходимые для администрирования децентрализованной идентичности.

6.52 частное лицо (individual): Владелец идентичности, являющийся физическим лицом. Имеет взаимоисключающий смысл с понятием "организация".

6.53 эмитент (issuer): Объект, который выдает заявление.

6.54 ключ эмитента (issuer key): Особый тип криптографического ключа, необходимый эмитенту для того, чтобы выдать заявление с поддержкой доказательств с нулевым разглашением.

6.55 цепочка ключей (key-chain): Задача обеспечения безопасности хранения личных ключей или данных в доверенном аппаратном блоке устройства.

6.56 юридическая идентичность (legal identity): Набор информации, достаточный, чтобы определить идентичность владельца идентичности для целей юридической ответственности по крайней мере в одной юрисдикции. Для целей временной сети юридическая идентичность может быть установлена путем ссылки на один или множество общедоступных веб-ресурсов, таких как веб-сайты, блоги, профили в социальных сетях или другие веб-страницы, содержащие достаточное количество информации для того, чтобы соответствовать этому критерию.

6.57 ассоциируемость (linkability): Возможность определить, связаны ли между собой два или более атрибута, идентификатора или идентичности в некотором наборе информации с достаточно высокой степенью вероятности, чтобы из этого можно было извлечь какую-то пользу.

6.58 проявление (manifestation): Наблюдаемое или обнаруженное (то есть не самозаявленное) представление объекта.

ПРИМЕЧАНИЕ. – Ср. с термином "утверждение".

6.59 взаимная аутентификация (mutual authentication) [b-ISO/IEC 29115]: Аутентификация идентичности объектов, в результате которой каждый объект убеждается в идентичности другого объекта.

6.60 наименование (name): Сочетание знаков, которое используется для идентификации объектов (например, абонента, сетевого элемента) и может быть разрешено или транслировано в адрес. Знаки – это цифры, буквы или специальные символы.

ПРИМЕЧАНИЕ 1. – 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.

ПРИМЕЧАНИЕ 2. – Основано на [b-ITU-T E.101].

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

6.62 схема (pattern).

ПРИМЕЧАНИЕ. – См. схема идентичности.

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

6.64 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 могут быть осуществлены идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

6.65 администратор доступа (principal): Объект, идентичность которого может быть аутентифицирована.

ПРИМЕЧАНИЕ. – Эта запись включена в [ITU-T X.811], [ITU-T Y.2720] и [ITU-T Y.2702].

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

6.67 личный ключ (private key) [b-ITU-T X.509]: (В криптосистеме с открытыми ключами) тот ключ пары ключей объекта, который известен только данному объекту.

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

6.69 доказательство (proof): Криптографическое подтверждение заявления. Цифровая подпись представляет собой простую форму доказательства. Еще одна разновидность доказательства – криптографический хеш. Доказательства могут быть двух типов: прозрачное доказательство или доказательство с нулевым разглашением. Прозрачные доказательства предполагают раскрытие всей информации в заявлении. Доказательства с нулевым разглашением допускают частичное раскрытие информации в заявлении.

6.70 проверяющий (prover): Объект, который выдает доказательство заявления. Проверяющий является также держателем заявления.

6.71 псевдоним (pseudonym) [b-ISO/IEC 24760-1]: Идентификатор, содержащий минимальную информацию об идентичности, достаточную для того, чтобы верификатор мог привязать ее к известной идентичности.

ПРИМЕЧАНИЕ 1. – Псевдоним может быть идентификатором, значение которого выбирается самим лицом или присваивается случайным образом.

ПРИМЕЧАНИЕ 2. – Псевдоним может использоваться для предотвращения или снижения рисков конфиденциальности и безопасности, связанных с использованием привязываний идентификатора, которые могут раскрыть идентичность объекта.

6.72 открытые данные (public data) [b- ITU-T L.1410]: Данные, которые доступны для общественности без ограничения требованием членства, соглашениями о неразглашении или аналогичными ограничениями.

6.73 открытый ключ (public key) [b-ITU-T X.509]: Тот ключ из пары ключей объекта, который общеизвестен.

6.74 открытый профиль (public profile): Информация, описывающая поставщика услуги, в том числе его юридическая идентичность, логотипы или другие товарные знаки, места ведения деятельности, маркетинговая информация, веб-ссылки и любая другая информация, требуемая структуре доверия для обеспечения полной прозрачности в отношении юридической идентичности и характеристик поставщика услуг.

6.75 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.

6.76 полагающаяся сторона (relying party (RP)): Объект, который полагается на представленную или заявленную идентичность запрашивающего или утверждающего объекта в каком-либо контексте запроса.

ПРИМЕЧАНИЕ. – Основано на [b-ITU-T Y.2720].

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

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

6.79 аннулирование (revocation): Признание недействительным чего-либо, что сделано ранее, кем-то, имеющим полномочия.

6.80 роль (role): Комплекс свойств или атрибутов, которые описывают способности или функции, выполняемые объектом.

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

6.81 проверка безопасности (security audit) [b-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 вынесения рекомендаций относительно каких-либо указанных изменений в контроле, политике и процедурах.

6.82 домен безопасности (security domain): Совокупность элементов, политика безопасности, орган безопасности и совокупность действий по обеспечению безопасности, в которых управление элементами осуществляется в соответствии с политикой безопасности.

ПРИМЕЧАНИЕ. – Основано на [b-ITU-T X.810]. Аналогичные определения содержатся в [b-ITU-T Y.2701] и [b-ITU-T Y.2720].

6.83 зона безопасности (security zone): Защищенная зона, характеризующаяся оперативным управлением, местоположением и возможностью соединения с другими устройствами или элементами сети.

ПРИМЕЧАНИЕ. – Основано на [b-ITU-T Y.2701].

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

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

6.86 вещь (thing): Объект, на который не может быть возложена юридическая ответственность. Вещь может быть животным (домашнее животное, скот), физическим объектом (дом, автомобиль, телефон) или цифровым объектом (компьютерная программа, сетевая услуга, структура данных). Имеет взаимоисключающий смысл с понятием "владелец идентичности".

6.87 доверие (trust): Уверенность одной стороны или объекта в том, что другая сторона или объект будет вести себя четко определенным образом, не нарушающим принятые сторонами правила, политику или юридические положения системы управления определением идентичности.

6.88 точка доверия (trust anchor): Владелец идентичности, способный служить опорной точкой в децентрализованной сети доверия. Точка доверия имеет две особых привилегии:

- добавлять в сеть новых владельцев идентичности;
- выдавать приглашения на роль точки доверия.

Она должна отвечать требованиям к точке доверия и согласиться соблюдать обязанности точки доверия, установленные в структуре доверия. Все доверенные лица и управляющие автоматически получают статус точек доверия.

6.89 структура доверия (trust framework): Имеющий юридическую силу набор спецификаций, правил и соглашений, регулирующих систему определения идентичности.

ПРИМЕЧАНИЕ. – Основано на [b-OIX-TFIS].

6.90 доверенная третья сторона (trusted third party): В контексте политики обеспечения безопасности – орган обеспечения безопасности или его агент, который является доверенным в отношении некоторых связанных с безопасностью действий.

ПРИМЕЧАНИЕ 1. – Основано на [b-ITU T X.810] и [b-ITU-T Y.2702].

ПРИМЕЧАНИЕ 2. – См. [b-ITU-T X.800].

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

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

6.93 ориентированная на пользователя (user-centric): Система управления определением идентичности, при которой пользователю предоставляется право контролирования и обеспечения соблюдения различных видов политики, определяющих управление данными пользователей, в том числе информацией, позволяющей установить личность.

6.94 валидирущий узел (validator node): Узел, валидирующий новые транзакции, относящиеся к записям об идентичности, и активно записывающий действительные транзакции в реестр по протоколу согласования реестра.

6.95 верифицируемое заявление (verifiable claim): Заявление, снабженное доказательством от эмитента. Как правило, это доказательство имеет вид цифровой подписи. Верифицируемое заявление может быть верифицировано при помощи открытого ключа, связанного с децентрализованным идентификатором эмитента.

ПРИМЕЧАНИЕ 1. – Основано на [b-W3C-VC].

6.96 верификация (verification) [b-ISO/IEC 24760-1]: Процесс установления правильности информации об идентичности, связанной с конкретным объектом.

ПРИМЕЧАНИЕ 1. – В ходе идентификации производится верификация заявленных или наблюдаемых атрибутов.

ПРИМЕЧАНИЕ 2. – Верификация информации (об идентичности) может включать рассмотрение на предмет действительности, правильности источника, подлинности (отсутствия изменений), правильности, привязывания к объекту и т. д.

ПРИМЕЧАНИЕ 3. – Правильность информации устанавливается на момент верификации.

6.97 верификатор (verifier) [b-ISO/IEC 24760-1]: Объект, который выполняет верификацию.

6.98 кошелек (кошелек идентичности) (wallet, identity wallet): Приложение, которое в первую очередь позволяет пользователю хранить идентификаторы и регистрационные данные, сохраняя соответствующие личные ключи на своем устройстве.

6.99 доказательство с нулевым разглашением (zero knowledge proof (ZKP)): Доказательство с использованием специальной криптографической системы и мастер-секрета, допускающее выборочное раскрытие информации в наборе заявлений. Доказательство с нулевым разглашением доказывает, что некоторые или все данные в наборе заявлений верны, без раскрытия какой бы то ни было дополнительной информации, включая идентичность проверяющего.

ПРИМЕЧАНИЕ 1. – Понятие выборочного раскрытия предполагает широкий выбор информации, которая может быть раскрыта. Например, ZKP можно использовать для подтверждения многочисленных заявлений о конфиденциальных данных, например: 1) о совершеннолетии без раскрытия даты рождения; 2) о финансовой состоятельности (ненахождении в состоянии банкротства) без раскрытия состава портфеля; 3) о владении активом без раскрытия предшествующих сделок или привязки к ним.

ПРИМЕЧАНИЕ 2. – Основано на [b-ITU-T X.1403].

Приложение A

Основные пункты и обоснование базовой терминологии управления определением идентичности

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Базовая информация

Дискуссии по поводу IdM иллюстрируют различия в представлениях людей о назначении IdM, о применяемых базовых процедурах, а также в определениях терминов. Эти различия приводили к недопониманию и к длительным обсуждениям в процессе стандартизации IdM.

Для того чтобы помочь избегать этого недопонимания в будущем, в настоящем приложении приведены 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 IdM.

Введение

Идентичность – это термин, который лежит в основе всех остальных терминов IdM. Например, в реальном мире, в отличие от цифрового, 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 и поведение. Могут использоваться и другие, такие как дата и место рождения, домашний адрес и номер телефона. В процессе коммуникации обеим сторонам обычно требуется достаточная мера уверенности в том, что они взаимодействуют с нужным им партнером. В этом процессе обеспечения уверенности зачастую участвуют два или более лиц или "объектов": объект, идентичность которого подлежит подтверждению, – RE, и объект, который будет полагаться на подтвержденную идентичность, – RP. Может участвовать и третья сторона, которая управляет определением идентичности, – IdSP.

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 (ID) 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. В этом разделе представлено объяснение процесса аутентификации и его значения для обеспечения уверенности.

Следует отметить, что при применении этой модели к реальным процедурам и приложениям необходимо четкое представление о соответствующих партнерах по общению и применимых цепочек 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 имеющейся информации об идентичности в отношении партнера, то есть уверенности в привязывании к объекту представленной идентичности.

Процесс обеспечения 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 отдельных партнера или более, 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 1. – Объект может иметь физическое или логическое воплощение.

ПРИМЕЧАНИЕ 2. – 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, устройства и интерфейсы.

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 в конкретном домене как отличного от других объектов.

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), то есть 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 A.1 показаны взаимосвязи между объектом, идентичностями и атрибутами.

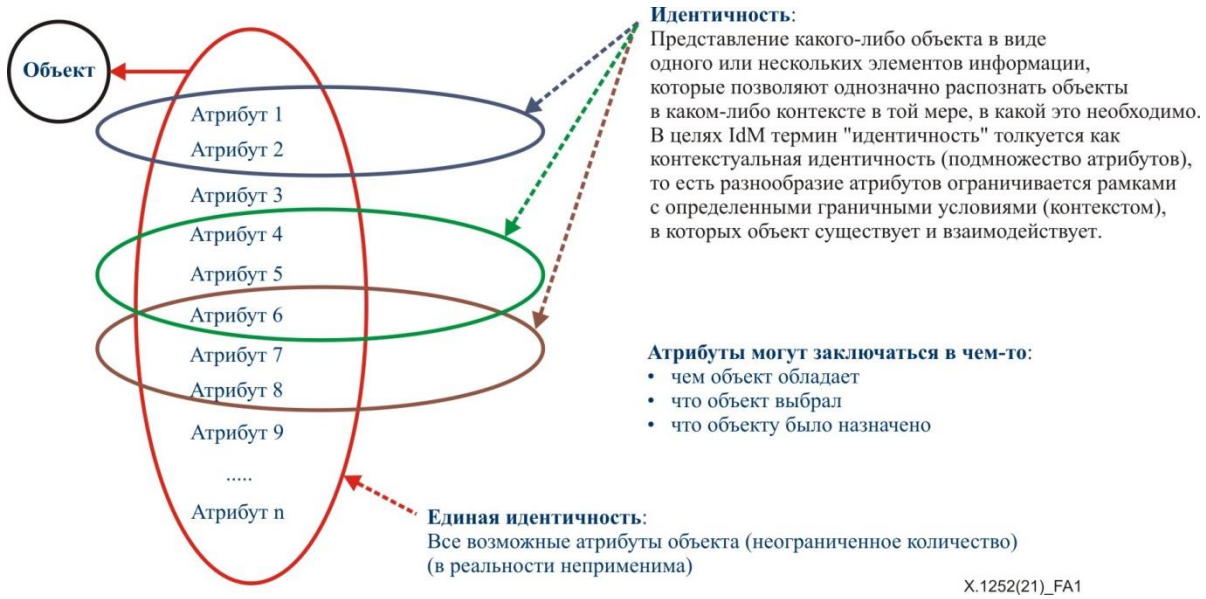


Рисунок A.1 – Взаимосвязи между объектом, идентичностями и атрибутами

Как уже отмечалось, аутентификация имеет значение для IdM. 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 или от риска причинения ущерба вследствие общения с не тем партнером.

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

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

Для обретения такой уверенности 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.

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

Аутентификация Y: объект Y выступает в роли RE, а объект X – в роли RP.

Аутентификация X: объект X выступает в роли RE, Y – в роли RP.

Для упрощения и лучшего понимания показанный на рисунке A.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 RP;
- достаточное доверие в отношении того, что RP является той самой стороной (например: пользователи должны быть в определенной мере уверены, что они находятся на нужной веб-странице, прежде чем заносить информацию об идентичности, такую как имя пользователя и пароль).

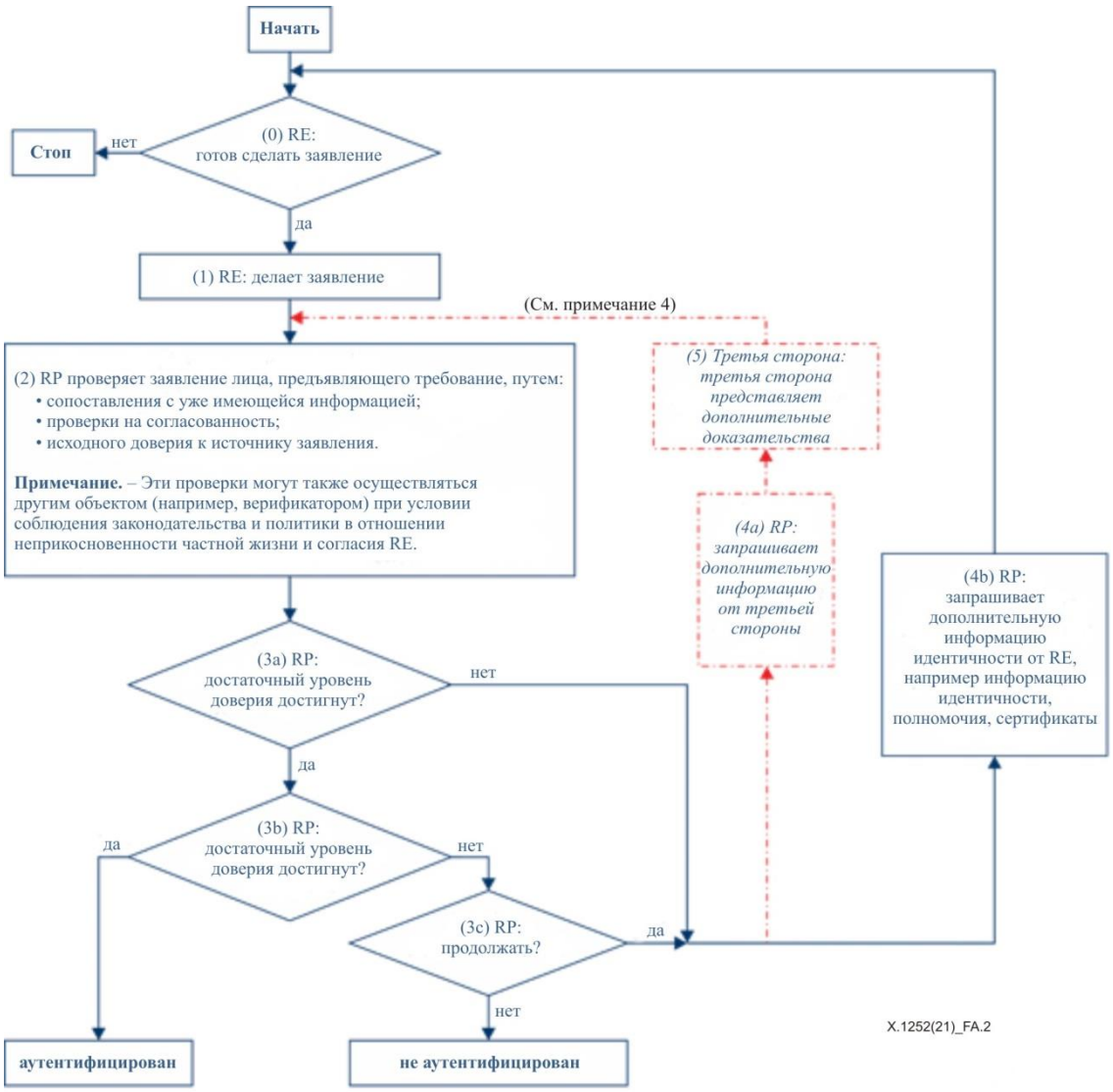
В некоторых случаях (но не в ориентированных на пользователя системах) может быть непосредственно задействована третья сторона для предоставления дополнительной информации в качестве доказательств RP для повышения доверия к атрибутам RE.

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

- что объект имеет (например, кодовая карта);
- что объект знает (например, пароль);
- чем 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.



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 RE.

Рисунок A.2 – Однонаправленный процесс аутентификации

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 A.2, решение относительно того, принимать ли RE, всегда принимает полагающаяся сторона на основе процесса аутентификации. Никто другой 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 IdM 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 модули идентификации абонента (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;

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 или утверждение

Обычно признается, что значения терминов "заявление" и "утверждение" несколько схожи, но немного различаются по значимости. В некоторых случаях утверждение считается более "сильным" высказыванием, чем заявление. Например, "заявление" можно определить 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 прилагательные "уверенный" и "убедительный" практически лишены смысла.

В открытых сетях существуют более сложные и многозначные отношения между делающей заявление стороной (то есть представляющей информацию об 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 RP (или верификатором, действующим по поручению RP), всегда принимает RP.

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) (то есть записаться) и в то же время зарегистрироваться для получения онлайновых банковских услуг.

A.4 Поставщик данных идентичности и поставщик услуг определения идентичности

Изучение текущей практики показывает, что широко применяется как термин "поставщик данных идентичности" (IdP), так и термин IdSP. Хотя термин IdP используется в некоторых действующих Рекомендациях МСЭ-Т, можно понять его так, будто им обозначается объект, который поставляет данные идентичности, а не объект, который управляет ими. 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 и поставщик финансовых услуг.

Ввиду этого термин IdSP считается несколько более точным, чем IdP, и ему следует отдавать предпочтение. Такой переход возможно осуществить при минимальном воздействии на существующие документы, используя действующее в настоящее время определение IdP для IdSP и сохраняя термин IdP, но, вместо того чтобы давать ему определение, просто отсылая к термину 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 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 ее образовывать. 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 атрибуте (любых атрибутах). 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 приема определенных лекарств.

Приложение B

Основные пункты и обоснование базовой терминологии децентрализованного управления определением идентичности

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

B.1 Децентрализованное определение идентичности

Модели определения идентичности, представленные в Приложении A, ориентированы на IdP. В такого рода моделях предполагается, что установлением, поддержанием и предоставлением идентичностей пользователям для использования в сетевых взаимодействиях ведают IdP. Этот подход требует, чтобы пользователи доверяли свои идентичности IdP. В рамках подхода, ориентированного на IdP, для многократного использования идентичностей IdP предлагают службы федерации. Возможность многократного использования идентичности пользователя предоставляется только членам федерации. При федеративном определении идентичности главным оплотом доверия становятся поставщики соответствующих услуг, которые сосредоточены на защите своей бизнес-модели, а не на создании условий для развития по-настоящему децентрализованной экосистемы определения идентичности, которая бы позволяла пользователям управлять своей идентичностью и своими взаимоотношениями. Модель определения идентичности, ориентированная на IdP, требует полного доверия к централизованным IdP. Как таковая, она не является гибкой или динамичной.

В децентрализованной же модели определения идентичности пользователи имеют возможность самостоятельно управлять своей идентичностью. При децентрализованном подходе поставщики услуг сосредоточиваются на выдвижении утверждений о конкретных идентичностях. В основе децентрализованных моделей определения идентичности лежат разработанные в последнее время технологии распределенного реестра (DLT).

Для того чтобы обеспечить предоставление услуг на множестве участвующих доменов, в централизованной модели определения идентичности услуги аутентификации сосредоточиваются в каком-то одном домене, а доступ в другие предоставляется через федеративные мостовые схемы идентичности. При сетевом взаимодействии от систем на основе идентичности требуется подтверждать заявленную идентичность объектов, а не обеспечивать контроль доступа. Соответственно, одна из важнейших функций децентрализованных систем определения идентичности – предоставлять механизм для доставки утверждений об идентичности пользователя, который могли бы легко использовать различные поставщики услуг.

Модель определения идентичности, ориентированная на пользователей, предусматривает индивидуальный или административный контроль на множестве доменов идентичности без необходимости в федерации, задающей круг доверия. Такая модель призвана наделить объект постоянной сетевой идентичностью, чтобы повысить удобство сетевого взаимодействия и одновременно предоставить пользователям больший контроль над своей идентичностью, используя для этого децентрализованные модели доверия. Ввиду своей сложности и отсутствия необходимых технологий, таких как DLT, ориентированная на пользователей модель поначалу не имела успеха.

Однако с появлением DLT модель определения идентичности, ориентированная на пользователей, стала завоевывать популярность. В настоящее время разрабатывается стек протоколов на основе DLT, позволяющий создать по-настоящему децентрализованную инфраструктуру определения идентичности. Управление цифровыми идентичностями в таких системах может осуществляться с применением открытой, закрытой, общедоступной или контролируемой DLT. Цель состоит в том, чтобы вернуть пользователям контроль над утверждениями об идентичности, не жертвуя безопасностью системы, целостностью данных в ней и неприкосновенностью частной жизни ее пользователей.

B.2 Децентрализованная модель определения идентичности

Децентрализованная модель определения идентичности способствует индивидуальному контролю (с возможностью его делегировать) в рамках сколь угодно широкого круга органов идентификации, включая IdP. Одна из децентрализованных моделей определения идентичности называется моделью суверенной идентичности (SSI). В основе ее лежат предположения, перечисленные в таблице B.1.

Таблица B.1 – Предположения модели суверенной идентичности

Существование	Пользователи должны существовать независимо
Контроль	У пользователей должен быть контроль над своими идентичностями
Доступ	У пользователей должен быть доступ к собственным данным
Прозрачность	Системы и алгоритмы должны быть прозрачными
Постоянство	Идентичности должны быть долгосрочными
Переносимость	Информация об идентичности и услуги, связанные с идентичностью, должны быть переносимыми
Функциональная совместимость	Идентичности должны допускать максимально широкое использование
Согласие	Пользователи должны выразить согласие на использование их идентичности
Минимизация	Раскрытие заявлений должно быть сведено к минимуму
Защита	Права пользователей должны быть защищены

Эти требования находятся вполне в русле того, что способна обеспечить DLT. Реализация децентрализованных систем определения идентичности основывается, как правило, на заявлениях и заверениях, причем соответствующие участники могут зачастую выступать в различных ролях.

Децентрализованные системы определения идентичности могут использоваться для облегчения заключения доверенных транзакций по сети. Такие системы позволяют пользователям представлять доказательства тех или иных своих атрибутов поставщикам услуг (и наоборот) посредством верифицируемых заявлений (заверений). Весь этот процесс может реализовываться на началах функциональной совместимости и доверия с использованием комплекса технологий, позволяющего распространять доверенные заявления без необходимости непосредственных взаимоотношений между участниками транзакций.

В децентрализованной системе определения идентичности поставщик услуг выступает в роли RP, а заявления делаются заверителем, который представляет недостающие заверения. Заверение – это набор высказываний о соответствии действительности другого набора высказываний. Исходный набор высказываний может также называться заявлением. Получатель заверения должен иметь возможность проверить приверженность заверителя сделанным заявлениям. Подтверждение приверженности должно, таким образом, иметь форму цифровой подписи или указателя на данные в распределенном реестре.

Идентификация узлов в сети происходит посредством децентрализованных идентификаторов (DID). DID имеет основополагающее значение для участия в сети и осуществления транзакций. Это номер, имя или строка, по которым идентифицируется тот или иной участник. Криптографический идентификатор (CID) – это DID, имеющий криптографическую привязку к определенному личному ключу.

Сегодня большинство решений для определения идентичности имеют ограниченную поддержку контроля над идентичностью, прозрачностью и переносимостью, поскольку эти решения предоставляются сторонними поставщиками услуг определения идентичности. В ближайшем будущем может не появиться полностью соответствующая требованиям система управления определением идентичности, но это не исключает необходимости установления основополагающих принципов суверенности.

Для того чтобы обеспечить возможность реализации модели суверенной идентичности (SSI), в настоящее время идет стандартизация новой серии протоколов децентрализованного управления определением идентичности, которая описывается в разделах B.2.1–B.2.5.

B.2.1 Децентрализованные идентификаторы

DID – это идентификаторы для верифицируемых децентрализованных систем определения идентичности, включая системы на основе модели "суверенной" цифровой идентичности. В общем случае пользователи сами создают DID и владеют ими. DID обладают уникальными характеристиками, дающими более надежную гарантию неизменности и устойчивости к несанкционированным манипуляциям. DID находятся под единоличным контролем субъекта DID и не зависят от какого-либо

централизованного реестра, IdP или органа сертификации. DID – это унифицированные указатели ресурсов (URL), связывающие субъект DID со средствами заслуживающего доверия взаимодействия с этим субъектом.

Вообще говоря, DID подразделяются на два класса: открытые и парные (полузакрытые).

1) Открытые DID – это идентификаторы, используемые теми пользователями, которые по собственному выбору связали себя с данными, предназначенными для публичного распространения. Примерами могут служить открытый профиль в социальной сети или свидетельство о профессиональной квалификации (например, медицинского работника). Открытые DID позволяют пользователям участвовать в деятельности, информацией о которой они согласны делиться с другими и которая может быть проверена другими. Например: я могу проверить, что мой лечащий врач действительно владеет соответствующим DID. Открытые DID характеризуются прослеживаемостью и возможностью ссылаться на них через интернет.

2) Парные DID формируются в рамках взаимоотношений или набора взаимодействий, посредством которых пользователи желают осуществить двустороннюю транзакцию. Парные DID изолируют пользователей и предотвращают увязку с ними. Для большинства пользователей парные DID будут основным механизмом осуществления транзакций на основе идентичности.

DID разрешается в документ DID, который представляет собой простой документ с описанием способа применения данного конкретного DID. Каждый документ DID содержит как минимум три элемента: криптографический материал, аутентификационные комплексы и оконечные точки обслуживания. Криптографический материал в сочетании с аутентификационными комплексами предоставляет набор механизмов аутентификации субъекта DID (например, открытые ключи и псевдонимные биометрические протоколы). Оконечные точки обслуживания обеспечивают надежную связь с субъектом DID.

Для того чтобы использовать DID с конкретным распределенным реестром или сетью, необходимо определить метод DID посредством отдельной спецификации метода DID. Метод DID задает набор правил регистрации, разрешения, обновления и аннулирования DID в данном конкретном реестре или сети.

Такая схема устраняет зависимость идентификаторов от централизованных реестров, а также зависимость управления ключами от централизованных органов сертификации, характерную для иерархической инфраструктуры открытых ключей (PKI). Поскольку DID хранятся в распределенном реестре, каждый объект может выступать сам для себя в роли соответствующего органа.

Обратите внимание, что методы DID могут разрабатываться также для ID, зарегистрированных в федеративных или централизованных системах IdM. Со своей стороны, во всех системах ID может реализовываться поддержка DID. Это обеспечивает мост функциональной совместимости между системами централизованных, федеративных и децентрализованных идентификаторов.

B.2.2 Концентраторы данных идентичности

Концентраторы данных идентичности (IH) – это компоненты, ответственные за хранение заверений об идентичности субъектов. В основе IH лежит децентрализованная модель, предусматривающая хранение семантического представления любого объекта и предоставления доступа к нему по конкретному URL. В архитектуре IH могут сводиться воедино идентичности, данные о которых хранятся у различных поставщиков услуг – от облачных каталогов до устройств.

B.2.3 Универсальный распознаватель децентрализованного идентификатора

Универсальный распознаватель DID действует как распределенная система, обеспечивающая распознавание DID во множестве DLT или блокчейнов. По своему назначению универсальный распознаватель DID сходен с механизмом привязывания в системе доменных имен. Вместо работы с доменными именами универсальные распознаватели DID нацелены на реализацию SSI-системы, которая может быть создана и зарегистрирована непосредственно объектами, на которые они ссылаются. Понятие универсального распознавателя DID иллюстрирует рисунок B.1.

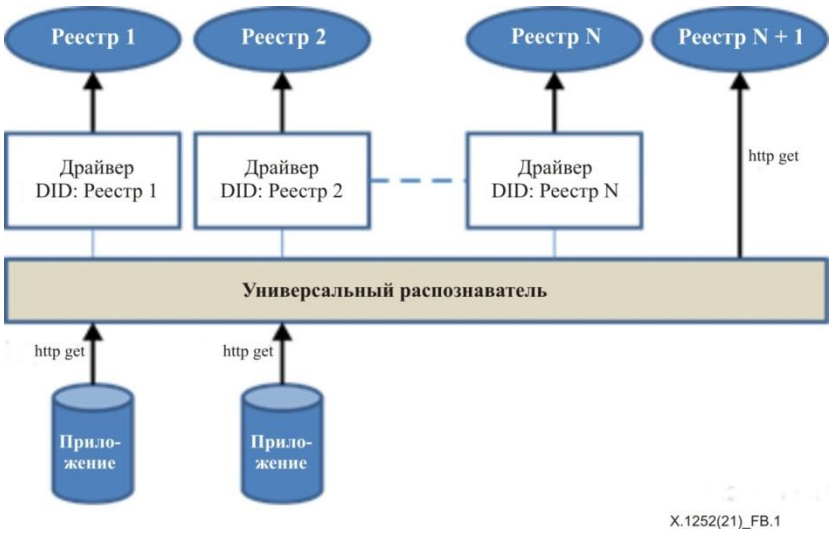


Рисунок B.1 – Универсальный распознаватель DID

B.2.4 Верифицируемые регистрационные данные

Верифицируемые заявления полезны, когда объекту требуется доказать, что он:

- старше определенного возраста;
- имеет право управлять конкретным транспортным средством;
- нуждается в определенном лекарстве;
- имеет образование и диплом электрика;
- имеет лицензию на осуществление медицинской деятельности; и
- имеет разрешение на поездки за границу.

Экосистема верифицируемых заявлений состоит из четырех основных позиций:

1) эмитента, выдающего верифицируемые регистрационные данные, относящиеся к конкретному субъекту;
2) держателя, хранящего регистрационные данные по поручению субъекта. Как правило, держатели также являются субъектами регистрационных данных;
3) верификатора, запрашивающего профиль субъекта. Профиль содержит определенный набор регистрационных данных. Верификатор подтверждает, что представленные в профиле регистрационные данные соответствуют своему назначению;
4) реестра идентификаторов – механизма, используемого для выдачи идентификаторов субъектам.

Схема этой экосистемы показана на рисунке B.2.

Рисунок B.2 – Экосистема

B.2.5 Децентрализованный кошелек

В этой модели пользователь может получить доступ к услугам, представив поставщику услуг (RP) свой ID в форме маркера. Поставщик услуг проверяет идентичность, сравнивая хеш-значения идентификаторов с соответствующими хеш-записями, хранящимися в DLT-реестре. Полагающаяся сторона предоставляет доступ или отказывает в доступе по результатам верификации. В более сложных сценариях пользователь может производить отдельные пары ключей на основе главного личного ключа для генерирования отдельных ID, предназначенных к использованию в контексте разных взаимоотношений, что обеспечивает возможность взаимодействия с сохранением неприкосновенности частной жизни.

На рисунке B.3 показана общая схема взаимодействий при определении идентичности для поддержки услуг на основе идентичности. На рисунке представлены следующие этапы осуществления транзакций в децентрализованной системе определения идентичности:

- Пользователь решает взаимодействовать, применяя услуги децентрализованной идентичности надежной структуры определения идентичности. Как показано на рисунке B.3 (см. блок "Децентрализованный реестр"), DLT предоставляет услуги, позволяющие конечному пользователю создать DID и установить связь с реестром. Задача создания DID для пользователя завершается сохранением адреса реестра этого пользователя и созданием пары из открытого и личного ключей для взаимодействия с пользователем. Реестр также поддерживает документ DID и устанавливает необходимые ссылки на связанные данные на основе нотации объектов JavaScript, указанные пользователем. Реестр предоставляет основные услуги определения идентичности, которые позволяют определять, каким образом следует взаимодействовать с электронным кошельком пользователя, чтобы подавать доступные заявления под управлением пользователя.
- Создание DID в реестре приводит к созданию электронного кошелька, посредством которого пользователь будет подавать в RP верифицированные заявления. В электронном кошельке хранятся личные ключи пользователя, открытые ключи и другие профили идентичности, необходимые DID. Применение методов доказательства с нулевым разглашением гарантирует, что заявления можно верифицировать таким способом, чтобы сохранить конфиденциальность, и в соответствии с существующим порядком использования традиционных бумажных регистрационных данных и документов. Например, находясь в ресторане, пользователь может подтвердить свой возраст при помощи водительских прав без необходимости участия эмитента в транзакции. Необходимые шаги описаны в следующих пунктах. Кошелек может быть виртуальным, так что одна его часть находится в мобильном устройстве пользователя, а другая – в облаке. Эта конфигурация позволяет создавать агенты, действующие от имени пользователя и реализующие услуги без необходимости непосредственного участия пользователя.

  1) Регистрация DID. Пользователь загружает электронный кошелек, связанный с базовым поставщиком услуг DLT, и регистрирует его DID в реестре. DLT генерирует пары из личного и открытого ключей для кошелька идентичности. Кроме того, в рамках процесса регистрации создается местоположение или адрес и сохраняется в DLT-реестре.
  2) Создание идентичности. Для использования DLT в децентрализованных системах определения идентичности предполагается, что существует структура доверия, определяющая перечень доступных участникам услуг определения идентичности. В этом случае пользователь может рассчитывать на наличие эмитента (доверенной стороны), способного подтверждать идентичность услуг. Пользователи могут применить первоначальные заявления для сбора заявлений от нескольких поставщиков, чтобы внести их в свой электронный кошелек и тем самым укрепить достоверность своих идентификационных данных в системе. Из рисунка B.3 видно, что каждая связь защищена взаимным DID между эмитентом, держателем (пользователем) и верификатором.
  3) Верификация. Если держатель (пользователь) желает получить доступ к услуге RP, то RP (верификатор) запрашивает у пользователя доступные заявления. Затем верификатор обращается к реестру, чтобы проверить подписанные заявления, используя открытые ключи, соответствующие DID и связанные с транзакцией. Этот шаг включает другие уровни аутентификации. В частности, в плане того, как работает система: она считает электронный кошелек источником достоверных данных в отношении личных ключей

владельца. Система предполагает, что имела место надлежащая аутентификация, гарантирующая, что объект, выполняющий транзакцию, является законным владельцем электронного кошелька.

4) Валидация заявления. RP использует предоставленные заявления из кошелька для верификации идентичности пользователя и ее атрибутов с применением методов электронной подписи и хеш-валидации на основе PKI.

5) Авторизация. По результатам проверок идентичности RP определяет, к каким услугам может быть предоставлен доступ.

- Для схемы с DID необходим универсальный распознаватель любого DID. Сообщество разработчиков DLT еще трудится над его созданием. В децентрализованных моделях определения идентичности существует необходимость в создании уровня аутентификации DID, на котором обеспечивалась бы функциональная совместимость. Работа над этим еще идет.
- Аутентификация DID позволяет владельцу идентичности доказать наличие контроля над DID во время своего взаимодействия с RP. Для этого RP должна выполнить следующие шаги:

  1) RP преобразует DID владельца идентичности в документ DID;

  2) RP пытается аутентифицировать владельца идентичности, используя объект (объекты) аутентификации, найденный (найденные) в документе DID;

  3) когда подтверждение владельца идентичности распознано как криптографическая подпись, объект аутентификации может включать в себя объект открытого ключа или ссылаться на него.

- Аутентификацию DID необходимо понимать как расширяемую в смысле способов, которыми владелец идентичности может доказывать наличие контроля над DID.

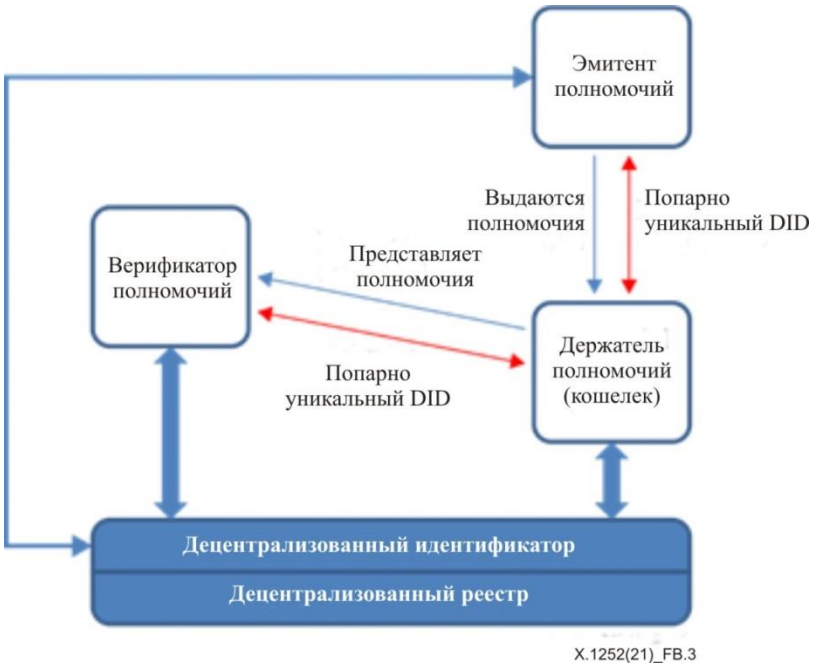


Рисунок B.3 – Децентрализованный кошелек идентичности с верифицируемыми заявлениями

Библиография

[b-ITU-T E.101] Рекомендация МСЭ-Т E.101 (2009 г.), *Определения терминов, используемых в Рекомендациях серии E для идентификаторов (наименований, номеров, адресов и других идентификаторов) служб и сетей электросвязи общего пользования.*

[b-ITU-T L.1410] Recommendation ITU-T L.1410 (2014), *Methodology for environmental life cycle assessments of information and communication technology goods, networks and services.*

[b-ITU-T X.501] Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models.*

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ.*

[b-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.*

[b-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.*

[b-ITU-T X.1254] ITU-T X.1254 (2020), *Entity authentication assurance framework.*

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology.*

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management.*

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

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

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

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology – Vocabulary – Part 37: Biometrics.*

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT Security and Privacy – A frame work for identity management – Part 1: Terminology and concepts.*

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information Technology – Security techniques – Entity authentication assurance framework.*

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). *Trust frameworks for identity systems*, White paper, Trust framework series. London: Open Identity Exchange. 18 pp. Available [viewed 2021-05-17] at: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [Untitled], Decentralized identifiers (DIDs) … Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-15] at: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases*. Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-17] at: http://www.w3.org/TR/vc-use-cases/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; 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, а также соответствующие измерения и испытания
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, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.