

Международный союз электросвязи

**МСЭ-Т**

СЕКТОР СТАНДАРТИЗАЦИИ  
ЭЛЕКТРОСВЯЗИ МСЭ

**X.1250**

(09/2009)

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

Безопасность киберпространства – Управление  
определением идентичностью

---

**Базовые возможности для улучшенного  
доверия и функциональной совместимости  
при глобальном управлении определением  
идентичности**

Рекомендация МСЭ-Т X.1250

## 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
<b>Управление определением идентичности</b>	<b>X.1250–X.1279</b>
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.1250**

### **Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности**

#### **Резюме**

В настоящей Рекомендации описаны базовые возможности в отношении доверия и функциональной совместимости при глобальном управлении определением идентичности (IdM), т. е. для расширения обмена и доверия к идентичностям, используемым объектами в сетях и услугах электросвязи/ИКТ. Определения и потребность в доверии для управления определением идентичности весьма зависят от обстоятельств, и в разных странах их применение потенциально часто подчиняется совершенно разным правилам и практическим наработкам. Возможности включают защиту информации, позволяющей установить личность, и управление ею.

#### **Источник**

Рекомендация МСЭ-Т X.1250 утверждена 25 сентября 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

## 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 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/>.

© ITU 2010

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

## СОДЕРЖАНИЕ

	Стр.
1 Сфера применения .....	1
2 Справочные документы.....	1
3 Определения .....	1
3.1 Термины, определенные в других документах .....	1
3.2 Термины, определенные в настоящей Рекомендации.....	2
4 Сокращения .....	3
5 Условные обозначения .....	4
6 Общие положения .....	4
7 Возможности для функциональной совместимости при глобальном управлении определением идентичности .....	5
7.1 Примеры возможных моделей транзакций, относящихся к управлению определением идентичности .....	5
7.2 Набор совместимых возможностей управления определением идентичности (IdM).....	8
7.3 Четыре основных элемента идентичности .....	9
7.4 Обнаружение возможностей идентичности .....	11
7.5 Функциональная совместимость и установление мостовых схем .....	12
7.6 Безопасность IdM.....	13
7.7 Защита, управление и использование информации, позволяющей установить личность (PII) .....	14
7.8 Ревизия и соответствие требованиям.....	15
7.9 Качественные показатели, надежность и доступность .....	16
7.10 Использование на международном уровне .....	16
Библиография .....	17



### Базовые возможности для улучшенного доверия и функциональной совместимости при глобальном управлении определением идентичности

#### 1 Сфера применения

В настоящей Рекомендации описываются базовые возможности для улучшения доверия и функциональной совместимости при глобальном управлении определением идентичности с использованием сетей и услуг электросвязи общего пользования. Эти базовые возможности сгруппированы по функциональным областям:

- общие, структурированные модели управления определением идентичности;
- предоставление полномочий, идентификатора, атрибута, уровней достоверности и возможностей идентичности модели поведения;
- обнаружение авторитетных ресурсов поставщиков идентичности, возможностей и федераций поставщиков;
- функциональная совместимость между платформами привилегированного управления, санкционированием, поставщиками идентичности и федерациями поставщиков, включая поставщиков мостовых схем идентичности;
- безопасность и другие меры для смягчения угроз и рисков, включая защиту ресурсов идентичности и информации, позволяющей установить личность;
- ревизия и соответствие, включая выполнение правил и защиту персональной информации, позволяющей установить личность;
- качественные показатели, надежность и доступность возможностей по управлению определением идентичности.

Современные системы и службы электросвязи/ИКТ сильно отличаются друг от друга, распределены по большим территориям, в значительной степени взаимосвязаны, однако в значительной степени автономны в IdM. Так как эти сети и возможности постоянно развиваются, их размеры и сложность могут препятствовать обеспечению функциональной совместимости возможностей IdM. По этой причине возможности IdM, описанные в настоящей Рекомендации, в основном основываются на возможностях и общих моделях существующих сетей, включая и те, которые представляют собой образцы передового опыта. Однако, чтобы достичь доверия и функциональной совместимости при глобальном управлении определением идентичности, в настоящей Рекомендации описывается путь эволюции и то, как использовать для этого существующие возможности там, где это возможно. В частности, в ней определяется возможность мостовых схем идентичности, которая может применяться во многих IdM, и базовые архитектуры для объединения существующих возможностей IdM.

Специализированные потребности в IdM, такие как реализация или воспрепятствование возможности увязки идентичностей для удовлетворения требований к конфиденциальности или защите, касающихся национальных интересов, в настоящей Рекомендации не рассматриваются.

Реализация возможностей IdM в отдельных странах зависит от особых требований национальной юрисдикции.

ПРИМЕЧАНИЕ. – Термин "идентичность", используемый в настоящей Рекомендации в отношении IdM, употребляется не в своем основном значении. В частности, он не выражает никакого положительного подтверждения.

#### 2 Справочные документы

Нет.

#### 3 Определения

##### 3.1 Термины, определенные в других документах

В настоящей Рекомендации определены следующие термины:

**3.1.1 заявитель (claimant)** [b-ITU-T Y.2720] и [b-ITU-T X.811]: Объект, который является администратором доступа или представляет его для целей аутентификации. Заявитель обладает функциями, необходимыми для участия в аутентификационных обменах от имени администратора доступа.

<sup>1</sup> Данная Рекомендация может быть неприменима в некоторых странах из-за их национального законодательства.

**3.1.2 информация, позволяющая установить личность (personally identifiable information) (PII)** [b-ITU-T Y.2720]: Информация, относящаяся к любому живому человеку, которая позволяет идентифицировать этого человека (включая информацию, позволяющую идентифицировать человека, когда она объединена с другой информацией, даже если эта информация не позволяет четко идентифицировать этого человека).

**3.1.3 полагающаяся сторона (relying party)** [b-ITU-T Y.2720]: Объект, который опирается на представление идентичности или заявления запрашивающего/утверждающего объекта в рамках определенного запроса.

## **3.2 Термины, определенные в настоящей Рекомендации**

В настоящей Рекомендации определяются следующие термины:

**3.2.1 агент (agent)**: Объект, выступающий от имени другого объекта.

**3.2.2 анонимность (anonymity)**: Свойство, не позволяющее идентифицировать объект в рамках набора объектов.

**ПРИМЕЧАНИЕ.** – Анонимность препятствует отслеживанию объектов или их характеристик, например местоположение пользователя, частота пользования услугой и т. п.

**3.2.3 атрибут (attribute)**: Информация, относящаяся к объекту и определяющая характеристики объекта.

**3.2.4 аутентификация (authentication)**: См. аутентификация объекта.

**3.2.5 гарантия аутентификации (authentication assurance)**: Уверенность, полученная во время процесса аутентификации, что партнер по связи является тем объектом, который он заявляет или ожидается, что является.

**3.2.6 связь (binding)**: Однозначно установленная взаимосвязь, соединение или привязка.

**3.2.7 заявление (claim)**: Утверждение, сделанное заявителем о значении или значениях одного или более атрибутов идентичности цифрового субъекта, обычно это утверждение спорно или вызывает сомнения.

**3.2.8 объект (entity)**: Все, что существует самостоятельно и является различимым, что может быть идентифицировано в контексте.

**ПРИМЕЧАНИЕ.** – Объектом могут быть физические лица, животные, юридические лица, организации, активные или пассивные предметы, устройства, программные приложения, услуги и т. д. или группа этих лиц. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, программные приложения, услуги и устройства, интерфейсы и пр.

**3.2.9 аутентификация объекта (entity authentication)**: Процесс получения необходимой уверенности в связи между объектом и предоставленной идентичностью.

**3.2.10 федерация (federation)**: Взаимосвязь пользователей и поставщиков услуг и идентичности.

**3.2.11 идентификатор (identifier)**: Один или более атрибутов, применяемый для идентификации объекта в рамках контекста.

**3.2.12 идентичность**: Представление объекта в виде одного или более информативных элементов, которое позволяет объекту или объектам быть в достаточной мере отличимыми в пределах контекста. Для задач IdM термин "идентичность" понимается как контекстуальная идентичность (поднабор атрибутов), т. е. разнообразие атрибутов ограничено структурой с определенными граничными условиями (контекстом), в которой этот объект существует и взаимодействует.

**ПРИМЕЧАНИЕ.** – Каждый объект выражается одной целостной идентичностью, которая объединяет все возможные информативные элементы, характеризующие эту идентичность (атрибуты). Однако эта целостная идентичность является теоретическим объектом и не поддается никакому описанию и практическому применению, так как количество всех возможных атрибутов неопределимо.

**3.2.13 поставщик мостовых схем идентичности (identity service bridge provider)**: Поставщик услуг идентичности, выступающий в качестве посредника между другими поставщиками услуг.

**3.2.14 управление определением идентичности (identity management):** Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и связь, обеспечение реализации политики, аутентификация и утверждение), используемых для:

- гарантирования информации, подтверждающей идентичность (например, идентификаторов, полномочий, атрибутов);
- гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов); и
- поддержки коммерческих приложений и приложений безопасности.

**3.2.15 поставщик услуг идентичности (identity service provider):** Объект, осуществляющий проверку, техническое обслуживание, управление и могущий создавать и присваивать информацию об идентичности других объектов.

**3.2.16 модель идентичности (identity pattern):** Структурированное выражение атрибутов объекта, например характеристик объекта, которое можно использовать в некоторых процессах идентификации.

**3.2.17 реализация (manifestation):** Наблюдаемое или обнаруженное, т. е. не помещенное самим объектом, выражение объекта. (Сравните с утверждением.)

**3.2.18 псевдоним (pseudonym):** Идентификатор, чья связь с объектом неизвестна или известна только ограниченному кругу объектов, в рамках использующего его контекста.

**3.2.19 запрашивающий объект (requesting entity):** Объект, делающий выражение или заявление идентичности для проверяющей стороны в рамках контекста с определенными запросами.

**3.2.20 окончательный объект (terminal object):** Объект, например SIM-карта, который может иметь связь с сетевым окончательным устройством, например мобильным телефоном.

**3.2.21 доверие (trust):** Твердая уверенность в достоверности и истинности информации или в компетенции объекта для соответствующей деятельности в определенном контексте.

**3.2.22 пользователь (user):** Объект, использующий ресурсы, например систему, оборудование, окончательное устройство, процесс, приложение или корпоративную сеть.

**3.2.23 ориентация на пользователя (user-centric):** Система IdM, которая может предоставить пользователю (IdM) возможность управления и обеспечения разных политик конфиденциальности и безопасности, управляющих обменом между объектами информацией об идентичности, включая PII.

## 4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

DHCP	Dynamic Host Control Protocol		Протокол динамического управления хоста
ID	Identifier		Идентификатор
IdM	Identity Management		Управление определением идентичности
IdSP	Identity Service Provider		Поставщик услуг идентичности
IT	Information Technology		Информационная технология
NGN	Next Generation Network(s)	СПП	Сеть (сети) последующих поколений
PII	Personally Identifiable Information		Информация, позволяющая установить личность
RFID	Radio Frequency Identification		Радиочастотная идентификация
SIM	Subscriber Identity Module		Модуль идентичности абонента
URL	Uniform Resource Locator		Унифицированный указатель ресурсов

## 5 Условные обозначения

Нет.

## 6 Общие положения

Рост и развитие возможностей связи привели к возникновению многочисленных пользовательских, коммерческих и правительственных электронных услуг. Связь более не является просто ресурсом для поиска информации, протокол Интернет и связанные с ним технологии электросвязи, такие как СПП, становятся незаменимым средством для выполнения ежедневных электронных транзакций.

Описанные в настоящей Рекомендации возможности предназначены для того, чтобы способствовать развитию и размещению структурированных и совместимых возможностей управления определением идентичности в рамках общей структуры для всех сетей и услуг электросвязи/ИТ, зависящих от региональных и национальных правил в отношении информации, позволяющей установить личность, и конфиденциальности.

Возможности, описанные в настоящей Рекомендации, включают в себя:

- a) **Примеры общих, структурированных моделей управления определением идентичности**  
Управление определением идентичности обычно включает в себя обмен между объектами одной или несколькими идентичностями с использованием сети или услуги электросвязи/ИТ. Для того чтобы обеспечить требуемый уровень гарантии аутентификации, стороны могут решить, или от них потребуется сообщать дополнительную информацию им самим или третьей стороне. Первоначальный обмен сообщениями может содержать выражение предпочтительного процесса аутентификации или делегирования. Одна или обе стороны, участвующие в обмене, могут также остаться анонимными или использовать псевдонимы. Эти виды взаимодействий могут быть описаны общими моделями, возможности для которых приведены в Рекомендации далее. Эти модели позволяют обеспечить многим сторонам возможности определения идентичности, если это желательно или необходимо. Модели имеют также важное значение для внедрения описанных функционально совместимых возможностей IdM, поддерживаемых в сетях, например СПП.
- b) **Возможности предоставления и защиты полномочий, идентификатора, атрибута и идентичности модели поведения при помощи известных уровней гарантии**  
Эти категории информации об идентичности и их обеспечение, техническое обслуживание, использование, отмена и/или защита до желаемого уровня гарантии являются общими для деятельности по управлению определением идентичности.
- c) **Обнаружение ресурсов поставщика идентичности, возможностей и федераций**  
Важнейшей задачей IdM в очень динамичном и разнообразном мире сетевых услуг и приложений является обнаружение современных источников идентичности и услуг, которые они предоставляют. Часто одинаково важные возможности обнаружения должны соответствовать желаемым уровням гарантии.
- d) **Функциональная совместимость между платформами, поставщиками и федерациями идентичностей, включая поставщиков услуг мостовых схем идентичности**  
В условиях широко распространенных сетей общего пользования и инфраструктуры возможностей с большим количеством "кочующих" пользователей и поставщиков управление определением идентичности может включать в себя большое количество запросов и ответов между различными сторонами и федерациями, в рамках которых они могут работать. Глобальная функциональная совместимость между сторонами, предоставляющими возможности управления определением идентичности, является важной и включает в себя общие протоколы создания запросов, касающихся возможностей идентичностей.
- e) **Безопасность и другие меры по смягчению угроз и уменьшения рисков для идентификаторов, включая защиту ресурсов идентификации и информации, позволяющей установить личность**  
Поскольку информация и ресурсы идентичности являются очень ценными, уязвимыми и жизненно важными компонентами сетей, особенно тех, которые считаются участками важнейшей государственной инфраструктуры, и затрагивают неприкосновенность частной жизни, для защиты безопасности исходя из анализа опасностей в среде IdM необходимы информация об идентичности и ресурсы.

f) **Ревизия и соответствие требованиям, включая выполнение правил и защиту информации, позволяющей установить личность**

Обеспечение управления определением идентичности обычно подчиняется различным законодательным, регуляторным, государственным и деловым требованиям, что требует некоторого уровня ревизии и возможностей соответствия. Такие возможности находятся в широком диапазоне и включают в себя осуществление ревизии для обеспечения соответствия требованиям, меры по защите информации, позволяющей установить личность, уведомления потребителям, поддержание требуемой точности временных меток и прослеживаемости.

g) **Удобство использования и масштабируемость: качественные показатели, надежность, доступность, выход за рамки одного государства и восстановление после бедствия**

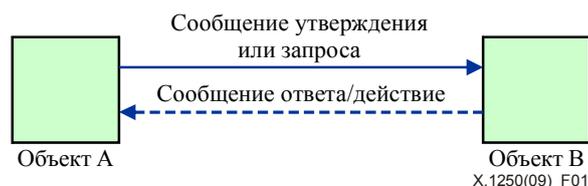
Возможности управления определением идентичности удобны в использовании и масштабируемы, для того чтобы соответствовать постоянному широкомасштабному развитию систем идентичности. Поскольку информация и ресурсы идентичности образуют основу, при помощи которой объекты аутентифицируют друг друга, т. е. считают друг друга партнерами связи, они часто являются компонентами важнейшей инфраструктуры, и может потребоваться поддерживать определенные уровни качественных показателей, надежности и доступности и возможностей.

## 7 **Возможности для функциональной совместимости при глобальном управлении определением идентичности**

В данном разделе приведены примеры возможных моделей транзакции, относящихся к управлению определением идентичности; создан функционально совместимый набор возможностей управления определением идентичности (IdM) и основные элементы идентичности. Также в данном разделе обсуждаются обнаружение возможностей идентичности, функциональная совместимость и мостовая схема, безопасность IdM, защита, управление и использование информации, позволяющей установить личность (PII), ревизия и соответствие. Также в работе рассматривается выход за рамки одного государства, качественные показатели, надежность и доступность.

### 7.1 **Примеры возможных моделей транзакций, относящихся к управлению определением идентичности**

Одной из основных транзакций в управлении определением идентичности является показанный на рисунке 1 базовый процесс запроса-ответа – общий для большей части обменов структурированной информацией. Наиболее простая форма аутентификации включает в себя две стороны, использующие согласованные протокол и информационную модель.

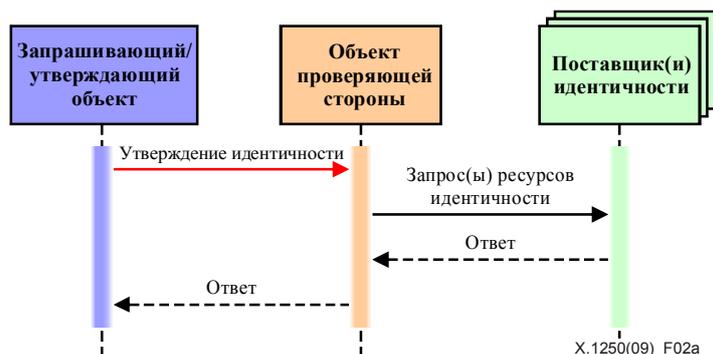


**Рисунок 1 – Базовый процесс обмена информацией с запросом/ответом**

Сторонами, которые участвуют в этом процессе, могут быть объекты любого вида. Объектом может быть физическое лицо, животное, юридическое лицо или организация, активные или пассивные предметы, устройства, программные приложения и пр. или группа этих лиц. В контексте электросвязи примеры объектов включают точки доступа, абоненты, пользователи, сетевые элементы, сети, программные приложения, услуги и устройства, интерфейсы и пр. Это может быть физический или виртуальный объект, например оборудование сети, программа, оконечные устройства, датчики, активно связанные физические объекты (например, с использованием устройств радиочастотной идентификации (RFID) или оптических кодов), пассивно связанные объекты. Сетевые устройства, например, можно рассматривать как объекты, выполняющие требования IdM от лица конечных пользователей, поставщиков и правительственных структур. В контексте управления цифровыми правами объект может быть интеллектуальной собственностью или материалом, с защищенными правами на копирование, например мультимедийным объектом или контентом IPTV. Отдельным типом объектов является группа. Идентичность этой группы представляет собой пересечение идентичностей (общих атрибутов) членов группы.

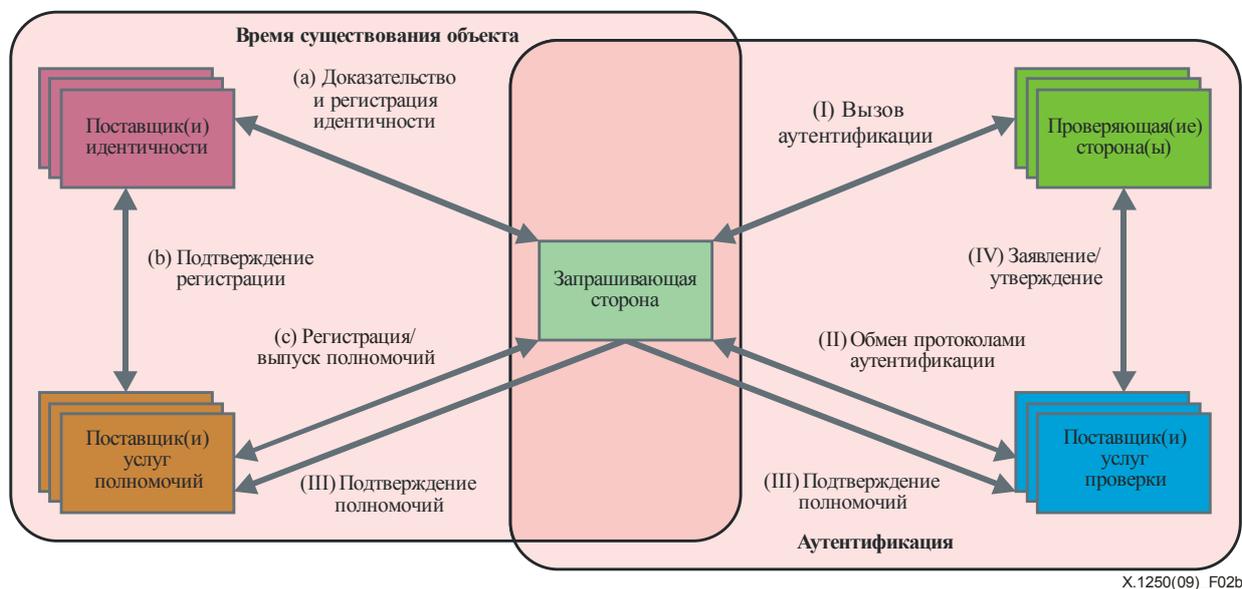
В большинстве случаев управление установлением идентичности использует случаи, включающие в себя применение комплексных моделей. Например, когда доверяющая сторона, которая изначально получает заявления, не является поставщиком услуг идентичности и, как показано на рисунках 2а или 2b, функция поставщика услуг идентичности отделена от доверяющей стороны; доверяющая сторона рассматривает ответы от поставщика услуг идентичности и решает, присутствует ли необходимый уровень гарантий аутентификации объекта. Основной функцией поставщика услуг идентичности является управление созданием, обновлением, подтверждением, приостановкой и удалением информации об идентичности.

Существует много возможных моделей обмена информацией об идентичности. Одной из наиболее широко используемых моделей является модель ответа на трехсторонний запрос, показанная на рисунке 2а. В этой модели заявлены некоторые недавно открытые протоколы IdM.



**Рисунок 2а – Пример трехсторонней модели управления определением идентичности**

На рисунке 2b показана другая модель управления определением идентичности, в которой запрашивающая сторона имеет более широкие возможности управления взаимоотношениями идентичности.



**Рисунок 2b – Пример пятисторонней модели управления определением идентичности, ориентированной на пользователя**

"Ориентированные на пользователя" модели, т. е. которые требуют обеспечения пользователей возможностью управления последующим использованием своих идентичностей, внимательно изучаются и тоже могут быть обязательными в национальных и региональных юрисдикциях. На рисунке 2b показан пример, когда определенные роли и возможности для управления определением идентичности поддерживаются разными поставщиками услуг. Все запросы/ответы направляются через запрашивающую сторону. В целях этих видов модели объекты определяются как:

- **Поставщик идентичности:** Объект, поддерживающий и управляющий, и который может создавать надежную информацию об идентичности других объектов, например окончательных пользователей, организаций и устройств, и предлагающий услуги на основе идентичности. Этот объект отвечает за присвоение и выдачу атрибутов, т. е. включающий идентичность, например, касающуюся абонента для поставщика полномочий, для определенного контекста, также описывается как регистрация, и за управление жизненным циклом идентичности, включающим в себя проверку, регистрацию и техническое обслуживание идентичности, включая отмену.
- **Поставщик услуг полномочий:** Объект, представляющий возможности, связанные с выдачей полномочий и меток, например полномочий, привязывающих метки к идентификаторам и атрибутам, которые можно проверить.
- **Поставщик услуг проверки:** Объект, предоставляющий возможности проверки информации об идентичности, например заявлений и полномочий, и классификации их действительности.
- **Полагающаяся сторона [b-ITU-T Y.2720]:** Объект, полагающийся на представление идентичности или заявление запрашивающего/утверждающего объекта в рамках определенного контекста запроса.

В целом действия по запросу-ответу могут быть разделены на две основные категории:

**а) Время существования идентичности**

- **Регистрация и утверждение идентичности (т. е. регистрация):** Данный информационный поток представляет собой введение объекта в определенный контекст, т. е. процессы регистрации и утверждения атрибутов, которые включают идентичность такого объекта в рамках данного контекста. Например, это может включать в себя подтверждающие и документирующие доказательства того, что с именем абонента или псевдонимом связан реальный человек.
- **Подтверждение регистрации:** Этот информационный поток представляет собой взаимодействие между поставщиком услуг идентичности и поставщиком услуги выдачи полномочий с целью утверждения зарегистрированных идентичностей.
- **Регистрация/выдача полномочий:** Этот информационный поток представляет собой обмен информацией между поставщиком услуги выдачи полномочий и запрашивающей стороной для регистрации идентичности и получения маркеров полномочий для связи с именем или псевдонимом и другими атрибутами, относящимися к объекту.

**б) Аутентификация и утверждение**

- **Утверждение:** Этот информационный поток представляет собой обмен информацией между полагающейся стороной и поставщиком услуги проверки с целью получения классификации заявителей.
- **Задача аутентификации:** Этот информационный поток представляет собой вызов или приглашение полагающейся стороной запрашивающей стороны для аутентификации. Например, полагающаяся сторона может перенаправить запрашивающую сторону к определенному поставщику услуги проверки, или запрашивающая сторона может выбрать определенного поставщика услуги проверки.
- **Обмен протоколом аутентификации:** Этот информационный поток представляет собой обмен протокольными сообщениями для аутентификации запрашивающей стороны поставщиком услуги проверки.
- **Утверждение полномочий:** Этот информационный поток представляет собой обмен информацией между поставщиком услуги проверки и поставщиком услуги выдачи полномочий для утверждения полномочий в случае необходимости.

Модели, представленные в настоящей Рекомендации, охватывают не все случаи. Они созданы таким образом, чтобы быть гибкими, и могут включать в себя как ситуации, когда существует много поставщиков идентичности, так и ситуации, когда полагающаяся сторона или запрашивающая сторона сами являются поставщиками идентичности.

### с) **Изменения утверждения**

- **Делегирование:** Утверждение может содержать также выражение предпочтительной проверки или "делегирование". Выражение предпочтительной проверки сообщает проверяющей стороне о том, какую службу поставщика идентичности запрашивать, при условии, что проверяющая сторона может установить доверенную цепочку соединений с предпочтительным поставщиком идентичности. Делегирование предоставляет средства для работы в ситуациях, когда один объект действует от лица другого объекта. Такое делегирование является вполне обычным, например, когда родитель может действовать вместо ребенка, один взрослый человек может действовать вместо другого недееспособного взрослого человека, служащий может действовать от лица компании, или юрист может действовать от лица клиента, или государство – от лица гражданина и наоборот.

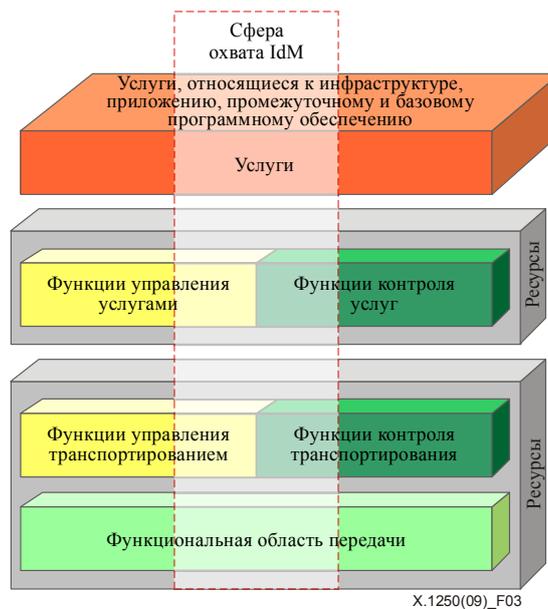
Делегирование может использоваться для предоставления делегируемому объекту некоторой части возможностей или санкционированных прав, которыми наделен объект, с которым связана идентичность. В таких условиях запрос проверяющей стороны поставщику идентичности может содержать дополнительные запросы для проверки того, что делегирующая сторона зарегистрировала своего делегата как санкционированного агента. Этот запрос передается в дополнение к аутентификации делегата. Взаимосвязи совместно используемых или делегированных прав могут существовать между многими объектами в этих моделях. Расширение цепочки делегирования, т. е. делегирование делегирования, зависит как от доступной технологии, так и от законов, регуляторных положений, деловых, федеративных и правовых правил.

- **Анонимность и псевдоним:** Объект может также представлять утверждение идентичности анонимного пользователя или псевдонима. В таких случаях уровень уверенности в идентичности зависит от внешних факторов, которые необходимо будет учесть проверяющей стороне, поскольку доверие может быть не достигнуто. Анонимность и псевдонимы могут использоваться, когда вид деятельности не требует фактической проверки, например, когда действия настолько тривиальны, что не требуется никакой надстройки для управления определением идентичности. Кроме того, некоторые законы, регуляторные положения или правила защиты данных могут требовать использования псевдонимов и анонимности.

## 7.2 **Набор совместимых возможностей управления определением идентичности (IdM)**

Управление определением идентичности возникло как общая возможность для всех уровней моделей базовой сети, например существующих в СПП [b-ITU-T Y.2012], [b-ITU-T Y.2720]. В прикладной области различные возможности IdM используются для управления сетевыми услугами как часть базовой функции транспортировки, а в возможностях управления они используются для администрирования этих уровней.

Часто между этими уровнями существует недостаточная координация, касающаяся управления определением идентичности. В надлежащих масштабах и в соответствии с региональными или национальными правилами функционально совместимые возможности IdM должны поддерживаться во всех слоях сети.



**Рисунок 3 – Сфера охвата функциональной совместимости слоев сети при управлении определением идентичности**

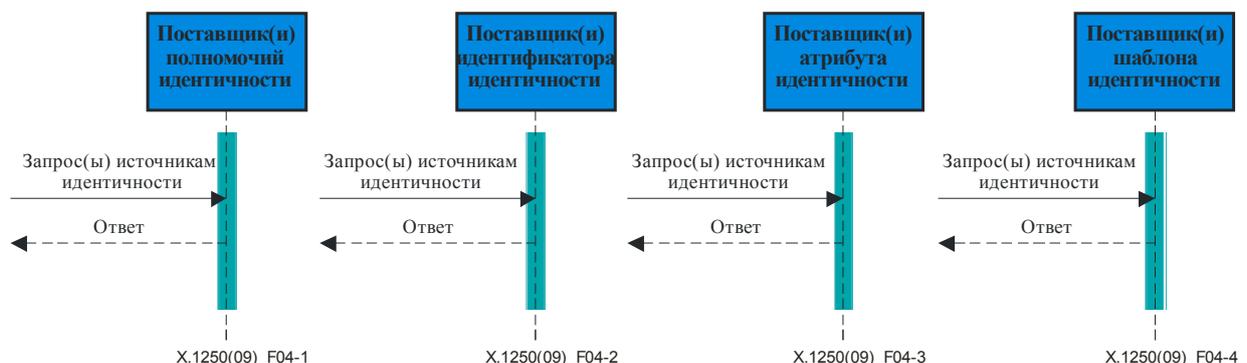
Рисунок 3 показывает, что относящиеся к IdM возможности могут существовать во всех вертикальных уровнях архитектуры сети, и что существует необходимость синхронизации и согласования.

### 7.3 Четыре основных элемента идентичности

С целью содействия функционально совместимым возможностям IdM в настоящей Рекомендации информация об идентичности подразделяется на следующие четыре основные категории:

- возможности идентификатора;
- возможности полномочий;
- возможности атрибутов;
- возможности модели.

Укрупнения каждой из четырех категорий информации об идентичности могут использоваться с целью обеспечения более детальных уровней гарантии идентичности и могут быть предоставлены в качестве возможностей идентичности либо отдельно, либо в некоторой комбинации различными объектами, как показано на рисунке 4. Этот рисунок можно рассматривать как дополнение к рисунку 2. Обычно используется модель запроса-ответа. Необязательно использование всех этих услуг определения идентичности в реализации IdM. Их применение и наличие в виде требования зависит от контекста IdM, особенно от требуемого или желаемого уровня достоверности идентичности.



**Рисунок 4 – Пример четырех основных возможностей идентичности при запросе-ответе**

Различия между этими возможностями идентичности могут быть функционально размыты. Например, полномочия имеют свои собственные идентификаторы, и поставщики поддерживают некоторую информацию об атрибутах соответствующей идентичности, которой принадлежат данные полномочия, а поставщик может поддерживать регистрационный файл, касающийся использования этих полномочий, который используется для анализа модели поведения с целью сведения к минимуму электронных краж или подделки идентичности.

Поставщики услуг IdM во многих вариантах реализации, таких как электросвязь/ИТ или поставщики финансовых услуг, или предприятие, или организация, имеющая особые отношения с конечным пользователем или потребителем, также могут обеспечивать реализацию всех этих возможностей в виде единого набора. Степень "открытости IdM" и взаимодействие с поставщиками IdM – это решение, основанное на доверии и схожих потребностях, коммерческих отношениях и регуляторных или законодательных требованиях.

### **7.3.1 Возможности идентификаторов**

Идентификаторы – это атрибуты, например имена, как правило, назначаемые объекту для управления информационными системами или адресации сообщений. По этой причине они обычно имеют специализированное применение. Например, номера телефонов, URL, адреса электронной почты используются как для доступа к услуге/устройству, так и для маршрутизации по сетям связи.

### **7.3.2 Возможности полномочий**

Полномочия используются для поддержки аутентификации объектов – одной или обеих сторон информационного обмена или транзакции. Одной из первых и все еще широко используемых форм сертификата полномочий является форма, основанная на разработанном стандарте цифрового сертификата МСЭ-Т X.509 [b-ITU-T X.509]. Среди других форм полномочий – полномочия, выпускаемые правительством, такие как удостоверения о трудоустройстве, подвижные беспроводные SIM-карты, и удостоверения финансовых организаций или карты АТМ.

Иногда полномочия также включают в себя биометрические данные. Некоторые приложения требуют возможность обеспечить быструю проверку достоверности полномочий и того, что они не отозваны. Однако следует отметить, что проверка полномочий может привести к множеству отслеживаемой информации с IdSP, что может являться угрозой конфиденциальности. Поэтому важное значение имеют надежные полномочия, не требующие проверки.

Сложность использования и управления цифровыми полномочиями в широком масштабе для населения может быть уменьшена с помощью ориентированных на пользователя подходов в области IdM в сочетании с возможностями управления полномочиями, как, например, цифровой кошелек [b-ITU-T X.1251]. В зависимости от ситуации поддержка полномочий может включать возможность использования множества полномочий для соответствия различным уровням требуемой гарантии.

### **7.3.3 Возможности атрибутов**

Как и характеристики объектов, атрибуты часто являются относительно статичными, полученными в процессе назначения полномочия или идентификатора, например имена, физический адрес, контактная информация и т. д. В других случаях, таких как текущее геопространственное местоположение, атрибуты могут быть весьма динамичными.

Обнаружение атрибутов и возможности направления запросов могут потребовать наличия специализированных функционально совместимых протоколов. Обычно такие протоколы поддерживают некоторый способ проверки для защиты и управления информацией, позволяющей установить личность, особенно при задействовании РП. Ориентированные на пользователя функционально совместимые протоколы и платформы могут также предоставить способы, позволяющие конечному пользователю называть причину, из-за которой информация об атрибуте должна быть рассмотрена.

### **7.3.4 Возможности модели**

Модели идентичности являются структурированным выражением атрибутов, которые можно использовать в определенных процессах идентификации.

Они могут состоять из наблюдаемой или обнаруженной, т. е. не заявленной или утверждаемой, идентичности, например из информации о репутации и транзакции, связанной с объектом. Часто особую важность имеет обнаружение кражи идентичности. Для обеспечения возможностей кибербезопасности используются также специализированные возможности определения идентичности модели поведения, например подпись модели поведения вируса или инфраструктурной атаки.

Как и возможности определения идентичности атрибута, когда модели поведения касаются физических лиц, предоставление также вызывает, возможно, существенно расширяющийся и иногда конфликтующий массив федеративных и возможных юридических и регуляторных требований, особенно для защиты информации, позволяющей установить личность. В некоторых юрисдикциях при использовании РИ хранение данных модели поведения и возможности анализа зависят от защиты важных данных и правил конфиденциальности, включая запрет на сбор данных и механизмы удаления данных.

### **7.3.5 Общие сведения о возможностях управления данными IdM**

Большое количество возможностей применяется в управлении системой IdM и управлении данными IdM для всех возможностей определения идентичности. Возможности включают в себя поддержку:

- способности запрашивающей стороны получать доступ/удалять/изменять/отслеживать/управлять информацией о своей идентичности, зависящей от законодательства, регуляторных положений и/или применяемых правил;
- способности санкционированных объектов, например системных администраторов, родителей, органов общественной безопасности, правоохранительных органов и других авторитетных третьих лиц получать доступ/изменять/отслеживать информацию о своей идентичности, зависящей от законодательства, регуляторных положений и/или применяемых правил;
- импорта/экспорта информации об идентичности, зависящего от законодательства, регуляторных положений и/или применяемых правил;
- механизма демонстрации определенного типа информации о качестве уровня информации, который они предоставляют проверяющим сторонам. Это требует соглашений между этими сторонами, касающихся информативного уровня;
- способности запрашивающей стороны делегировать управление своей информацией об идентичности другому объекту;
- управления сроком действия всех идентичностей, включая способы быстрого утверждения текущего статуса информации, зависящего от законодательства, регуляторных положений и/или применяемых правил;
- общего механизма идентификации и управления распространением всех идентичностей, зависящего от законодательства, регуляторных положений и/или применяемых правил.

### **7.3.6 Уровни гарантии объекта**

Ресурсы идентичности и ее предоставление обладают соответствующими уровнями гарантии, которые в значительной степени меняются в зависимости от большого количества технических и административных факторов, которые подчиняются правилам и стандартам в соответствии с ситуацией.

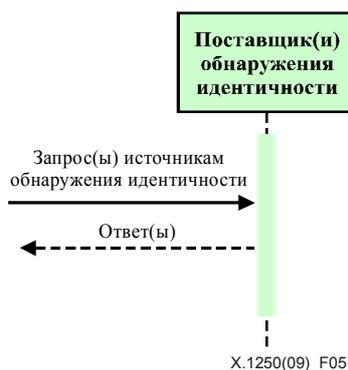
Функции включают в себя поддержку:

- индикации уровней достоверности информации идентификатора общего пользования, особенно для органов регистрации связи общего пользования, включая представителей идентификаторов подраспределения в иерархических именах и системах нумерации;
- взаимного протокола, показывающего уровни достоверности, связанные с предоставленной информацией. Рекомендуются общие глобальные, открытые механизмы;
- механизма для запрашивающей стороны, проверяющей стороны или, например, поставщика услуг идентичности для определения условий достоверности и утверждения для услуги идентичности и определения того, какие действия должны предприниматься, если условия не соблюдены.

## **7.4 Обнаружение возможностей идентичности**

Важнейшей задачей IdM в очень динамичном и разнообразном мире сетевых услуг и приложений является обнаружение источников для каждой из четырех основных услуг IdM. Существует множество доступных распределенных, автономных источников. Недостаточно, чтобы услуги IdM просто существовали. Проверяющим сторонам необходимы стандартные средства, для того чтобы узнать об их существовании и о том, как с ними связаться, как показано на рисунке 5, ниже. Процесс обнаружения может потребовать поддержки нового протокола обнаружения, который по своей природе похож на динамический протокол управления хостом, в котором клиент может раскрыть

сервер DHCP и получить его IP-адрес и информацию о шлюзах. Поэтому процесс обнаружения может быть так же прост, как и объект, содержащий идентичность, обеспечивающий проверяющей стороне действующий URI или OID доверенным образом.



**Рисунок 5 – Пример возможностей обнаружения идентичности при запросе-ответе от одного объекта**

Кроме того, обнаружение возможностей идентичности должно включать в себя обнаружение возможностей, доступных через федерации. Некоторые федерации и сообщества, использующие указанные протоколы, разработали частичные решения по удовлетворению потребностей обнаружения в пределах сообществ своих пользователей. Однако в настоящее время не существует средств для глобального обнаружения или обнаружения между федерациями. Необходима система, поддерживающая обнаружение. Желаемые возможности обнаружения включают в себя поддержку:

- правил делового соглашения в рамках федераций или других доверенных доменов;
- отдельного входа/отдельного выхода из системы и публикации этой возможности обычным способом, так чтобы она была обнаруживаемой.

## 7.5 Функциональная совместимость и установление мостовых схем

Глобальная функциональная совместимость между сторонами, обеспечивающими ресурсы управления определением идентичности, является важнейшим требованием к предоставлению услуг. В данном разделе описаны возможности создания запросов в рамках федерации или через поставщика мостовых схем.

Федерации основаны на принципах взаимного принятия результатов аутентификации в рамках участвующих доменов, а не на основе совместного использования информации об идентичности в этих доменах.

### 7.5.1 Возможности, относящиеся к федерациям

Возможности, относящиеся к федерации, включают в себя:

- способность проверяющей стороны устанавливать домен аутентификации (т. е. безопасность) при помощи альянсов и участия в федерациях;
- получение санкционирования от запрашивающей стороны для объединения в федерации идентичностей запрашивающей стороны в зависимости от законодательства, регуляторных положений и/или применяемых правил;
- способность запрашивающей стороны делегировать полномочия для объединения в федерации своей идентичности, в зависимости от законодательства, регуляторных положений и/или применяемых правил.

### 7.5.2 Возможности, относящиеся к идентичности мостовых схем

Возможности, относящиеся к идентичности мостовых схем, включают в себя:

- способность запрашивающей стороны устанавливать разрешения и запреты, относящиеся к возможностям мостовых схем идентичности;
- механизм обнаружения поставщика идентичности связанной запрашивающей стороны.

- механизм установления мостовых схем идентичности, позволяющий:
  - a) федерации запрашивающей стороны у поставщика идентичности и проверяющей стороны в разных доменах аутентификации иметь соответствующее разрешение для каждого от запрашивающей стороны и поставщика мостовых схем идентичности; и
  - b) перенаправлять адрес поставщика услуг идентичности в ответном сообщении проверяющей стороне;
- механизм завершения взаимодействия информации запрашивающей стороны, полученной от одного поставщика идентичности и позволяющей ей быть распознанной и использоваться связанным поставщиком идентичности и проверяющими сторонами в разных доменах аутентификации (например, двух сетях);
- там, где федерация была создана при помощи поставщика мостовых схем идентичности, способы оповещения проверяющих сторон или поставщиков идентичности в случае изменения правил поставщика мостовых схем идентичности. Этот механизм дает возможность проверяющей стороне или поставщику идентичности прекратить свое участие в федерации;
- там, где федерация была создана при помощи поставщика мостовых схем идентичности, способы оповещения запрашивающей стороны в случае изменения правил поставщика мостовых схем идентичности. Этот механизм дает возможность запрашивающей стороне прекратить свое участие в федерации.

## 7.6 Безопасность IdM

Поскольку информация об идентичности и сетевые ресурсы, которые предоставляют возможности определения идентичности, являются очень ценными, уязвимыми и жизненно важными компонентами сетей, особенно тех, которые считаются участками важнейшей государственной инфраструктуры, для них потребуется обеспечить безопасность. Защита инфраструктуры IdM охватывает административные правила, оперативную деятельность, технологии и методы для предотвращения раскрытия систем и данных IdM, вне зависимости от того, находятся ли они в стационарном состоянии или в состоянии перехода.

Дополняя передовой опыт обеспечения безопасности, описанный в [b-ITU-T X.1205], настоящий раздел предлагает несколько возможностей для повышения безопасности инфраструктур IdM, которые включают в себя:

- безопасные передачи, например, с защитой конфиденциальности, целостности и защитой от воспроизведения между всеми сторонами (поставщик утверждения, проверки, идентичности);
- предоставление механизма для безотказных транзакций IdM;
- безопасность обнаружения возможностей определения идентичности, например, для защиты от имитации поставщика идентичности;
- информации безопасности для ревизии транзакций IdM;
- введение функций обнаружения и ответа на деятельность нарушителя на основе анализа транзакций IdM и, возможно, для предупреждения владельцев о подозрении на атаку на их информацию об идентичности;
- предоставление способов, позволяющих проверяющим сторонам быстро оповещать поставщиков услуг идентичности об атаке на идентичность и обезопасить эту возможность оповещения от чрезмерного использования.

Правила и указания использования, также иногда называемые "Руководство определением идентичности", также являются важными мерами в условиях поставщика услуг множества идентичностей для уменьшения угроз и рисков, и для защиты информации, позволяющей установить личность. Если привлекаются федерации, альянсы или поставщики мостовых схем, то эти меры могут быть приняты всеми участвующими проверяющими сторонами и поставщиками услуг идентичности. Возрастающее использование приложений IdM, ориентированных на пользователя, может также предоставить возможность запросить конечного пользователя для определения правил, имеющих связь с их атрибутами идентичности, как это описывается и рекомендуется в разделе 7.7. Использование общих возможностей безопасности среди членов федерации имеет существенные преимущества, и федерации должны иметь хорошо разработанные требования безопасности.

Желаемые возможности правил и безопасности, касающихся IdM, включают:

- возможности гарантий идентичности в соответствии с применимыми руководящими указаниями;
- безотказный механизм для транзакций IdM;
- динамическое установление ограниченных по времени механизмов для кратковременных и изменяющихся отношений. Это может потребовать существования взаимодоверяемого поставщика мостовых схем, принадлежащего одной или нескольких федерациях;
- безопасность между федерациями, включая механизмы переговоров для безопасной связи между федерациями и обмена информацией между федерациями в ответ на угрозы кибербезопасности;
- предоставление возможности для приложений на оконечных объектах иметь способы для санкционированного доступа к информации об идентичности конечного пользователя оконечного объекта, в зависимости от законодательства, регуляторных положений и/или применяемых правил;
- механизм для отправки оповещения от поставщика услуг соответствующей идентичности ко всем заинтересованным сторонам, в случае если идентичность по сообщениям подверглась рискам или отозвана;
- безопасный метод изучения функций идентичности;
- регистрацию информации о безопасности для транзакций IdM с необходимой детализацией для создания подотчетности и возможности судебного анализа;
- функции обнаружения вторжения и ответа для транзакций IdM;
- механизмы, позволяющие проверяющим сторонам сообщать о компрометации идентичности.

#### **7.7 Защита, управление и использование информации, позволяющей установить личность (PII)**

Существует несколько аспектов, позволяющих предохранить информацию, позволяющую установить личность. Два наиболее важных аспекта включают в себя использование возможностей безопасности в инфраструктуре IdM и использование возможностей, которые поддерживает прозрачность и оповещение объектов об использовании их информации об идентичности вместе с функциями связи их предпочтений с этой информацией. В такой ситуации "связь" включает определенный постоянный механизм, который позволяет третьей стороне обладать информацией об идентичности для обнаружения возможностей правил PII соответствующего объекта. Все чаще и платформы, использующие продукты, ориентированные на пользователя, и возможности поставщика услуг мостовых схем идентичности позволяют использование этих видов предпочтения.

В некоторых национальных и региональных юрисдикциях PII должна собираться должным образом и в соответствии с точно определенной и законной конечной целью. Обмен соответствующей информацией между связывающимися сторонами должен быть ограничен для данных, которые нужны для того, чтобы позволить проверяющей стороне предоставить услугу или ресурс запрашивающей стороне.

С точки зрения конфиденциальности в некоторых национальных юрисдикциях существует некоторое количество принципов, которые нужно принять во внимание:

- связь с PII должна быть сосредоточена на конкретных, определенных и законных целях и в дальнейшем не должна подвергаться обработке способом, несовместимым с этими целями;
- информация PII должна быть достаточной, соответствующей и не излишней в отношении целей, с которыми ее собирают и/или в дальнейшем обрабатывают;
- информация PII должна быть точной и содержаться в обновленном виде; любые приемлемые меры должны быть приняты для обеспечения того, чтобы были стерты или исправлены неточные или неполные данные, имеющие отношение к целям, с которыми они были собраны или в дальнейшем обработаны;
- информация PII должна сохраняться в форме, которая позволяет идентифицировать субъекты данных не дольше, чем это необходимо для целей, с которыми эти данные были собраны или в дальнейшем обработаны;
- информация PII не должна совместно использоваться приложениями в разных целях;

- информация РП должна быть ограничена минимально необходимой информацией для конкретной цели;
- информация РП должна быть надежно защищена. Для защиты информации РП от случайного или незаконного разрушения или неожиданной потери, изменения, несанкционированного раскрытия или доступа и от всех других незаконных форм обработки должны быть приняты надлежащие технические и организационные меры, в частности там, где обработка предусматривает передачу данных по сети;
- физические лица имеют право доступа к касающейся их информации РП, ее исправления или стирания;
- информация РП не должна сохраняться дольше, чем это необходимо в целях, установленных в ее отношении.

Другие юрисдикции требуют применение механизмов защиты, включающих в себя использование оповещений каждый раз, как регистрируется доступ к учетной записи или изменение информации. Использование РП в сетях и службах электросвязи/ИКТ должно производиться в соответствии с определенными конечными задачами. Именно с учетом этой конкретной задачи можно рассматривать как соответствующую, достаточную и нечрезмерную природу записанных данных, категорий физических лиц или организаций, которые могут получать эти данные, и сроки, в течение которых могут храниться собранные данные.

Возможности включают в себя:

- сбор и обработку информации РП в соответствии с принципами и законодательством, относящимися к защите данных и конфиденциальности. Как минимум защита должна включать в себя действия, определенные ОЭСР в Руководящих указаниях по конфиденциальности. Применяемые региональные/национальные регуляторные положения могут предъявлять дополнительные обязательные требования обеспечения соответствия (например, Европейская директива о защите данных 95/46/ЕС);
- обеспечение безопасности и защиты признанных пределов в отношении признания минимального сбора информации, позволяющей установить личность. Информация РП должна собираться в определенных, четких и законных целях только с согласия субъекта данных;
- такие свойства, например, как если поставщик услуг идентичности отдельно включает в федерацию идентичность запрашивающей стороны вместе с двумя и более проверяющими сторонами, то он должен отвечать за то, как проверяющие стороны используют информацию, предоставленную им поставщиком услуг идентичности для определения того, что идентичности относятся к той же запрашивающей стороне;
- услугу оповещения, если изменяются атрибуты запрашивающей стороны;
- услугу оповещения, если изменяется объявление о согласии запрашивающей стороны;
- предоставление возможности предупреждения владельцев идентичности о деятельности по транзакции IdM, понятой поставщиком услуг идентичности как попытка компрометации их идентичности;
- предоставление возможности оповещения владельцев идентичности о компрометации систем и функций поставщика услуг идентичности;
- способность применять предельные сроки хранения информации РП, чтобы она не сохранялась дольше, чем это необходимо в целях, установленных в ее отношении;
- способность соответствующих объектов проверять, поправлять и удалять соответствующую РП, согласно законодательству, регуляторным положениям и/правилам.

## **7.8 Ревизия и соответствие требованиям**

IdM зависит от множества юридических, регламентарных и отраслевых предпринимательских требований, которые могут обуславливать определенный уровень ревизии и соответствия. Примеры мер по ревизии и соответствию включают в себя ведение записей безопасности, защиты и соответствующего использования личной информации и оповещения объектов, к которым применяется эта информация. Ревизия должна соответствовать возможностям защиты РП, описанным в разделе 7.7, выше, особенно в виду того что может быть включена еще одна новая сторона, что может привести к конфликту с законами, регуляторными положениями и правилами, касающимися конфиденциальности.

Возможности включают в себя:

- механизмы позволяющие провести судебный анализ;
- взаимные и безопасные механизмы обмена информацией о ревизии управления определением идентичности.

- установление метки времени;
- установление метки времени записи в зависимости от ситуации, в соответствии с важностью проверяемой информации и значения времени;
- следует обратить внимание на обеспечение того, чтобы реализации ревизии управления определением идентичности удовлетворяли применяемым требованиям в отношении конфиденциальности.

### **7.8.1 Возможности точности меток времени**

Точность меток времени очень важна для времени действия управления определением идентичности и для поддержки безопасности внутри систем IdM, так как вся информация об идентичности существует внутри этих временных рамок. В ревизии описываются события в рамках этих временных меток. Метки времени жизненно важны для проверки, а качество, если не простота использования, данных проверки определяется точностью временных отметок в местах соответствующих событий для правильной проверки чрезвычайно асинхронных и распределенных сетей и возможностей приложений. Желаемые возможности включают в себя функции точности временных отметок, достаточные для проверки в согласованных местах общего эталона, соответствующего взаимно согласованному уровню достоверности.

### **7.9 Качественные показатели, надежность и доступность**

IdM представляет собой важную сетевую возможность, которую требуется разработать и реализовать, для того чтобы получить желаемые качественные показатели, надежность и доступность. Рекомендуется, чтобы показатели надежности и доступности IdM были сравнимы с этими показателями других важнейших функций сети, потому что IdM образует основу аутентифицированного и санкционированного доступа и всех транзакций в сети. Сюда входит, например, обеспечение того, что задачи, касающиеся охвата IdM, внешней поддержки и возможности установления соединений, являются достаточными. Качественные показатели IdM, например время ответа на запрос, должны удовлетворять ожидаемым нагрузкам по запросам IdM.

Доступность системы IdM неоднородна для всех элементов (элементы выпуска, элементы поиска, элементы отмены) и в итоге должна быть привязана к уровню доверенности в полномочиях. Следующие требования доступности являются желательными, но будут различаться среди элементов стандартного блока (хранилище, система регистрации, возможность отмены):

- надежность и доступность на уровнях, сравнимых с другими важными функциями сети, системами и возможностями;
- использование возможностей IdM в планах поставщика по восстановлению после бедствия;
- функции IdM, поддерживающие достаточное время отклика для транзакций IdM.

### **7.10 Использование на международном уровне**

Для глобальной функциональной совместимости необходима поддержка применения различных наборов символов и языков, которые признаются как важный и необходимый элемент поддержки для всех приложений на основе сети общего пользования, включая возможности IdM.

## Библиография

- [b-ITU-T X.509] Рекомендация МСЭ-Т X.509 (2005 г.) | ISO/IEC 9594-8:2005, *Информационные технологии – Взаимосвязь открытых систем – Справочник: Структуры сертификатов открытых ключей и атрибутов.*
- [b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами.*
- [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.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности.*
- [b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity.*
- [b-ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture.*
- [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 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-IETF RFC 2560] IETF RFC 2650 (1999 г.), X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.





## СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	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
<b>Серия X</b>	<b>Сети передачи данных, взаимосвязь открытых систем и безопасность</b>
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи