МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т Y.2720

(01/2009)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ Y: ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

Сети последующих поколений – Безопасность

Структура управления определением идентичности в СПП

Рекомендация МСЭ-Т Y.2720

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Y

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА, АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ И СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ

ГЛОБАЛЬНАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА	
Общие положения	Y.100–Y.199
Услуги, приложения и промежуточные программные средства	Y.200–Y.299
Сетевые аспекты	Y.300–Y.399
Интерфейсы и протоколы	Y.400–Y.499
Нумерация, адресация и присваивание имен	Y.500–Y.599
Эксплуатация, управление и техническое обслуживание	Y.600–Y.699
Безопасность	Y.700–Y.799
Рабочие характеристики	Y.800–Y.899
АСПЕКТЫ ПРОТОКОЛА ИНТЕРНЕТ	
Общие положения	Y.1000–Y.1099
Услуги и приложения	Y.1100–Y.1199
Архитектура, доступ, возможности сетей и административное управление ресурсами	Y.1200–Y.1299
Транспортирование	Y.1300–Y.1399
Взаимодействие	Y.1400–Y.1499
Качество обслуживания и сетевые показатели качества	Y.1500–Y.1599
Сигнализация	Y.1600–Y.1699
Эксплуатация, управление и техническое обслуживание	Y.1700–Y.1799
Начисление платы	Y.1800–Y.1899
СЕТИ ПОСЛЕДУЮЩИХ ПОКОЛЕНИЙ	
Структура и функциональные модели архитектуры	Y.2000–Y.2099
Качество обслуживания и рабочие характеристики	Y.2100–Y.2199
Аспекты обслуживания: возможности услуг и архитектура услуг	Y.2200–Y.2249
Аспекты обслуживания: взаимодействие услуг и СПП	Y.2250–Y.2299
Нумерация, присваивание имен и адресация	Y.2300–Y.2399
Управление сетью	Y.2400–Y.2499
Архитектура и протоколы сетевого управления	Y.2500–Y.2599
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899

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

Рекомендация МСЭ-Т Y.2720

Структура управления определением идентичности в СПП

Резюме

В Рекомендации МСЭ-Т Y.2720 представлена структура управления определением идентичности (IdM) в сетях последующих поколений (СПП). Основной целью этой структуры является описание структурного подхода к разработке, определению и реализации решений IdM и содействие функциональной совместимости в неоднородной среде.

Управление информацией, подтверждающей идентичность объекта (например, идентификаторами, регистрационными данными и атрибутами), не является новым понятием. Однако по мере того, как мы продвигаемся в направлении среды конвергентных сетей, в которых услуги базируются на контекстах и ролях и могут быть доступны в любом месте и в любое время, гарантирование и безопасность информации, подтверждающей идентичность, а также управление ею становятся все более сложными. Кроме того, к необходимости функциональной совместимости могут приводить разные и независимые решения. Следовательно, новые, усовершенствованные, автоматизированные и взаимодействующие средства необходимы по следующим причинам:

- конечные пользователи все шире используют многочисленные идентичности;
- эти идентичности могут быть связаны с разными контекстами и привилегиями в отношении услуг;
- идентичности могут лишь частично идентифицировать конечного пользователя;
- идентичности могут использоваться повсеместно и в любое время; и
- идентичности могут быть несовместимыми между поставщиками.

IdM разрешает эту ситуацию и представляет собой набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации политики, аутентификация и утверждение), используемых для:

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

Данная структура предназначена для использования в качестве основы при разработке и определении конкретных аспектов IdM, таких как детальные требования, механизмы и процедуры, в соответствии с потребностями. Она также обеспечивает четкий и взаимосвязанный обзор всей совокупности IdM в СПП.

Представленная в настоящей Рекомендации структура предназначена для СПП (т. е. управляемых сетей с коммутацией пакетов), которые определены в Рекомендации Y.2001 МСЭ – Общий обзор СПП. Однако в соответствующих случаях она могла бы применяться для других типов сетей (например, корпоративные сети и сети предприятий).

ПРИМЕЧАНИЕ. – Использование термина "идентичность" в настоящей Рекомендации в связи с IdM не указывает на его абсолютное значение. В частности, этот термин не предполагает какую-либо положительную оценку того или иного лица.

Источник

Рекомендация МСЭ-Т Y.2720 утверждена 23 января 2009 года 13-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/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т Y.2720

Структура управления определением идентичности в СПП

1 Сфера применения

В настоящей Рекомендации представлена структура IdM для СПП. Основной целью этой Рекомендации является описание основных концепций, функциональных компонентов и возможностей IdM, которые могут использоваться для организации и определения структурированных решений для СПП. Сфера применения настоящей Рекомендации включает:

- описание мотивации бизнеса, выгод и преимуществ услуг IdM, а также общие возможности, используемые для обеспечения гарантии идентичности и определения концепций IdM, применимых к СПП и основанных на функциональных требованиях и архитектуре (FRA), касающихся СПП, как это определено в [b-ITU-T Y.2012], *Функциональные требования и архитектура СПП выпуска 1*;
- определение и описание функциональных объектов, ролей, отношений, инструментов реализации и связи, поддерживающих услуги и возможности IdM для СПП;
- определение и описание внутрисетевых отношений для поддержки услуг и возможностей IdM внутри СПП; и
- определение и описание отношений для поддержки услуг и возможностей IdM между поставщиками доступа к СПП (например, внутри федерации), а также между поставщиками доступа к СПП и другими поставщиками (например, между федерациями).

Представленная в настоящей Рекомендации структура предназначена для СПП (т. е. управляемых сетей с коммутацией пакетов), которые определены в Рекомендации [b-ITU-T Y.2001], *Общий обзор СПП*. Однако в соответствующих случаях она могла бы применяться для других типов сетей (например, частные корпоративные сети и сети предприятий).

Настоящая структура предназначена для использования в качестве основы для разработки и определения конкретных аспектов IdM для СПП, таких как подробные требования, механизмы и процедуры, по мере необходимости. Она также обеспечивает четкий и согласованный обзор всей совокупности связанных с IdM вопросов в СПП.

ПРИМЕЧАНИЕ. – Использование термина "идентичность" в настоящей Рекомендации в связи с IdM не указывает на его абсолютное значение. В частности, этот термин не предполагает какую-либо положительную оценку того или иного лица.

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 всем 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 в настоящей Рекомендации на какой-либо документ не придает ему как отдельному документу статус рекомендации.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks.*

3 Определения

3.1 Термины, определенные в других местах

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

3.1.1 анонимность (anonymity) [b-ITU-T X.1121]: Способность обеспечивать анонимный доступ к услугам, при котором не допускается отслеживание персональной информации о пользователе и его поведении, например местоположение пользователя, частота пользования услугой и т. д.

3.1.2 аутентификация (authentication) [b-ITU-T X.811]: Обеспечение гарантии заявленной идентичности объекта.

3.1.3 авторизация (authorization) [b-ITU-T X.800]: Предоставление прав, которое включает предоставление доступа на основании прав доступа.

3.1.4 заявитель (claimant) [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.

3.1.5 делегирование (delegation) [b-ITU-T X.911]: Действие, которым другому объекту передаются полномочия, ответственность или какая-либо функция.

3.1.6 идентификатор (identifier) [b-ITU-T Y.2091]: Идентификатор представляет собой серию цифр, букв и символов или данных в любой другой форме, используемых для определения абонента(ов), пользователя(ей), элемента(ов) сети, функции(й), объекта(ов) сети, предоставляющего(их) услуги/приложения, или других объектов (например, физические или логические объекты).

3.1.7 сеть последующего поколения (СПП) (Next Generation Network (NGN)) [b-ITU-T Y.2001]: Сеть с коммутацией пакетов, которая может предоставлять услуги электросвязи и использовать многочисленные широкополосные технологии транспортировки с включенной функцией QoS и в которой связанные с услугами функции не зависят от лежащих в основе технологий, связанных с транспортировкой. Она обеспечивает беспрепятственный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым ими услугам. Она поддерживает универсальную подвижность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.1.8 администратор доступа (principal) [b-ITU-T X.811]: Объект, идентичность которого может быть аутентифицирована.

3.1.9 домен безопасности (security domain) [b-ITU-T X.810]: Совокупность элементов, политика безопасности, орган обеспечения безопасности и набор связанных с безопасностью действий, в рамках которых к набору элементов применяется политика безопасности для указанных действий, а политикой безопасности управляет орган обеспечения безопасности для данного домена безопасности.

3.1.10 верификатор (verifier) [b-ITU-T X.811]: Объект, который является объектом, требующим аутентифицированной идентичности, или представляет такой объект. Верификатор включает в себя функции, необходимые для участия в аутентификационных обменах.

3.2 Термины, определенные в других документах, не являющихся стандартами МСЭ

3.2.1 атрибут (attribute) [b-ETSI TS102 042]: Описательная информация, предназначенная для объекта, в которой указываются такие характеристики объекта, как состояние, качество или другая информация, касающаяся этого объекта.

3.3 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины:

3.3.1 гарантия (assurance): Мера доверия к тому, что элементы безопасности и архитектура возможностей по управлению определением идентичности в точности содействуют политике безопасности, как она понимается полагающейся стороной и поставщиком данных идентичности, и обеспечивают реализацию такой политики.

3.3.2 гарантия аутентификации (authentication assurance): См. Гарантия.

3.3.3 уровень гарантии (assurance level): Количественное выражение гарантии, согласованной между полагающейся стороной и поставщиком данных идентичности.

3.3.4 регистрационные данные (credential): Объект, который можно идентифицировать и который можно использовать для аутентификации того, что заявитель является именно тем, за кого он себя выдает, и для того, чтобы дать заявителю разрешение на право доступа.

3.3.5 обнаружение (discovery): Действие по установлению местоположения машиночитаемого описания связанного с сетью ресурса, который мог быть ранее неизвестен и который отвечает некоторым функциональным критериям. Обнаружение включает сопоставление набора функциональных и иных критериев с набором описаний ресурсов. Цель состоит в нахождении надлежащего относящегося к услуге ресурса.

3.3.6 объект (entity): Все, что существует самостоятельно и является различимым, что может быть идентифицировано уникальным образом. В контексте IdM примерами объектов являются абоненты, пользователи, сетевые элементы, сети, программные приложения, услуги и устройства. Какой-либо один объект может иметь множество идентификаторов.

3.3.7 федерация (federation): Установление отношений между двумя или более объектами или создание ассоциации, включающей любое количество поставщиков услуг и поставщиков данных идентичности.

3.3.8 федеративная идентичность (federated identity): Идентичность, которая может использоваться для доступа к группе услуг или приложений, для которых обязательными являются политика и условия федерации.

3.3.9 идентичность (identity): Информация об объекте, которой достаточно для идентификации этого объекта в том или ином конкретном контексте.

3.3.10 поставщик данных идентичности (identity provider): Объект, который создает и поддерживает надежную информацию, подтверждающую идентичность других объектов (например, пользователей/абонентов, организаций и устройств), и управляет такой информацией, а также предоставляет основанные на идентичности услуги на основе доверия, деловых отношений и других типов отношений.

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

- гарантирования информации, подтверждающей идентичность (например, идентификаторов, регистрационных данных, 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
- обеспечения коммерческих приложений и приложений безопасности.

3.3.12 модель поведения (pattern): Структурированное выражение, полученное на основе поведения, которое связано с объектом и описывает объект, давая возможность его распознать или отличить; это может включать прошлый опыт объекта. Модель поведения может быть однозначным образом связана с каким-либо объектом или классом, к которому относится этот объект.

3.3.13 информация, позволяющая установить личность (personally identifiable information): Информация, относящаяся к любому [живому] лицу, которая дает возможность идентифицировать такое лицо (включая информацию, которая может идентифицировать лицо в сочетании с другой информацией, даже если такая информация не точно идентифицирует данное лицо).

3.3.14 присутствие (presence): Набор атрибутов, характеризующий объект по отношению к его текущему статусу.

3.3.15 конфиденциальность (privacy): Защита информации, позволяющей установить личность.

3.3.16 полагающаяся сторона (relying party): Объект, который полагается на представленную или заявленную идентичность запрашивающего/утверждающего объекта.

3.3.17 доверие (trust): Мера того, насколько полагаются на характер, возможности, сильные стороны или истинность кого-либо или чего-либо.

4 Сокращения

В настоящей Рекомендации используются следующие сокращения:

API	Application Programming Interface		Интерфейс прикладного программирования
BSS	Business Support System		Система поддержки деятельности предприятия
CSCF	Call Session Control Function		Функция управления сеансами связи
FRA	Functional Requirements and Architecture		Функциональные требования и архитектура
GBA	Generic Bootstrapping Architecture		Общая архитектура начальной загрузки
IdM	Identity Management		Управление определением идентичности
IdP	Identity Provider		Поставщик данных идентичности
NGN	Next Generation Networks	СПП	Сети последующих поколений
OAM&P	Operation, Administration, Maintenance and Provisioning		Эксплуатация, администрирование, техническое обслуживание и обеспечение
OSS	Operations Support System		Система эксплуатационной поддержки
PII	Personally Identifiable information		Информация, позволяющая установить личность
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
QoE	Quality of Experience		Оценка пользователем качества услуги
QoS	Quality of Service		Качество обслуживания
RP	Relying Party		Полагающаяся сторона
SAML	Security Assertion Markup Language		Язык разметки утверждений безопасности
BC	Session Border Controller		Пограничный контроллер сеансов связи
SIP	Session Initiation Protocol		Протокол инициирования сеанса
ПУ	Service Provider		Поставщик услуг
SS7	Signaling System No. 7		Система сигнализации № 7
URI	Uniform Resource Identifier		Универсальный идентификатор ресурса
VoIP	Voice over Internet Protocol		Передача голоса по протоколу Интернет

5 Введение

5.1 Обзор управления определением идентичности (IdM)

Управление информацией, подтверждающей идентичность объекта (например, идентификаторами, регистрационными данными и атрибутами), не является новым понятием. Однако по мере того, как мы продвигаемся в направлении среды конвергентных сетей, в которых услуги базируются на контексте и ролях и к которым имеется повсеместный и постоянный доступ, гарантирование и безопасность информации, подтверждающей идентичность, а также управление ею становятся все более сложными. Кроме того, к необходимости функциональной совместимости могут приводить разные и независимые решения. Следовательно, необходимы новые, усовершенствованные, автоматизированные и взаимодействующие средства. Основной целью этой структуры является описание структурного подхода к разработке, определению и реализации решений, которые будут содействовать функциональной совместимости в неоднородной среде.

IdM разрешает эту ситуацию и представляет собой набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации политики, аутентификация и утверждение), используемых для:

- гарантирования информации, подтверждающей идентичность;
- гарантирования идентичности объекта; и
- обеспечения коммерческих приложений и приложений безопасности.

На рисунке 1 представлен общий обзор IdM.

Рисунок 1 – Обзор IdM

Информацию, подтверждающую идентичность, которая касается того или иного объекта, можно сгруппироваться следующим образом:

- идентификаторы (например, ID пользователя, адреса электронной почты, номера телефонов, URI и адреса IP);
- регистрационные данные (например, цифровые сертификаты, маркеры и биометрические данные); и
- атрибуты (например, роли, заявляемая информация, привилегии, модели поведения и местоположение).

Функции и возможности IdM используются для гарантирования информации, подтверждающей идентичность, гарантирования идентичности объекта, а также для поддержки коммерческих приложений и приложений безопасности, включая услуги на основе идентичности.

Кроме того, услуги и возможности IdM позволяют также объектам, которые являются пользователями/абонентами, контролировать, каким образом используется и распространяется информация, подтверждающая их идентичность. IdM также дает возможность членам федерации (например, деловым партнерам) обмениваться информацией, подтверждающей федеративную идентичность, и использовать такую информацию для поддержки федеративных услуг.

IdM дает возможность разработки различных приложений. Примерами приложений являются, среди прочего:

- *коммерческие приложения*
  - однократный вход в систему и выход из системы (например, доступ к многим приложениям и услугам без необходимости индивидуальной аутентификации каждого приложения или платформы услуг);
  - федеративные услуги (например, доступ к услугам различных поставщиков услуг или поставщиков доступа к СПП);

- *услуги на основе идентичности*
  - услуги в области идентификаторов, регистрационных данных и атрибутов;
  - услуги сопряжения (преобразование и взаимодействие информации, подтверждающей идентичность, в неоднородной среде);
  - услуги по предоставлению информации о модели поведения;
- *приложения безопасности*
  - управление доступом для сетевых и прикладных услуг (например, VoIP, IPTV и передача данных);
  - управление доступом к информации, ресурсам и средствам по ролевому признаку;
  - управление авторизацией и привилегиями;
  - услуги по обеспечению защиты (например, средства безопасности для защиты ресурсов сетевой инфраструктуры, а также информации, подтверждающей идентичность пользователей/абонентов, и их средств);
  - защиты информации, позволяющей установить личность (PII).

В среде с участием многих поставщиков услуг и федеративной среде услуги и возможности IdM используются для обнаружения и сообщения информации для создания доверия к идентичности(ям) какого-либо объекта среди различных объектов сети, таких как абоненты/заявители, полагающиеся стороны (например, пользователи, поставщики услуг и поставщики доступа к сети) и поставщики услуг в области идентичности (например, поставщики регистрационных данных и поставщики верификаторов), во всей сети и доменах безопасности. Например, выбранный поставщик данных идентичности (например, поставщик услуг аутентификации/верификации) может проверить идентификаторы, регистрационные данные и атрибуты, связанные с идентичностью, и сообщить их полагающейся стороне (например, поставщику услуг) через утверждающие стороны для содействия управлению доступом, принятию решений в области бизнеса и обеспечения реализации применимой политики (например, конфиденциальность и защита информации, позволяющей установить личность).

5.2 Стимулы и мотивация бизнеса

Помимо того, что IdM обеспечивает безопасность СПП, она дает возможность внедрять в СПП новые и появляющиеся коммерческие приложения и услуги (например, конвергированные приложения фиксированной и подвижной связи и приложения на базе веб) и способствует их использованию. В частности, услуги, возможности и функции IdM поддерживают широкий диапазон приложений и услуг конечных пользователей/абонентов, коммерческих предприятий (например, поставщиков доступа к сетям, поставщиков услуг, корпораций) и государственных предприятий, как это показано на рисунке 2.

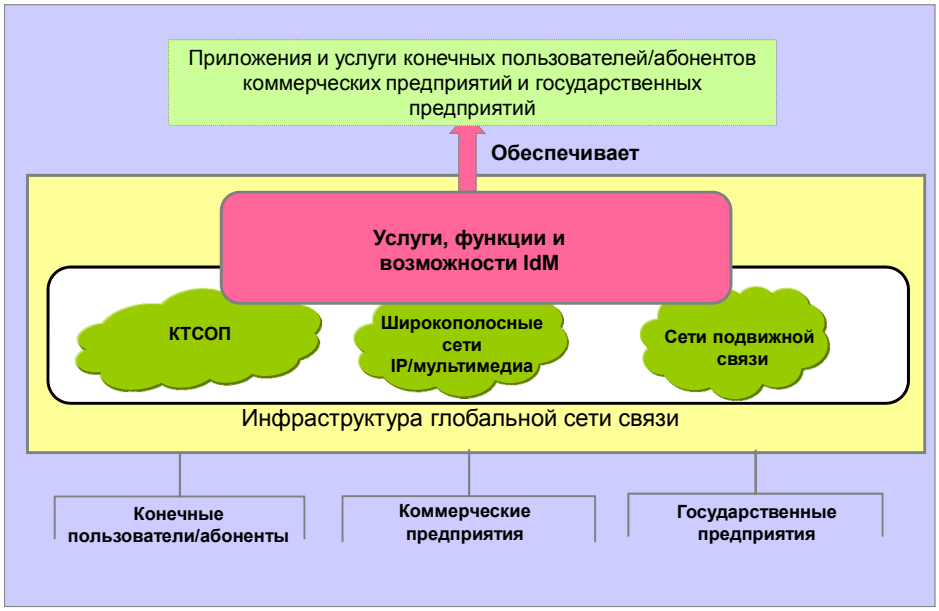

Рисунок 2 – Использование услуг IdM

IdM – это важнейший компонент управления безопасностью СПП и обеспечения возможности кочевого доступа по запросу к услугам и приложениям СПП, характеризующим ожидания конечных пользователей в эпоху информации. Наряду с другими защитными механизмами (например, брандмауэры, системы обнаружения вторжения и защита от вирусов), IdM играет важную роль в защите инфраструктуры, а также услуг и приложений СПП от киберпреступности, такой как мошенничество и хищение данных идентичности. Кроме того, поскольку пользователи будут доверять тому, что транзакции в СПП будут защищенными и надежными, IdM будет содействовать предложениям новых услуг на основе идентичности. Таким образом, использование IdM существенно улучшит существующие услуги и возможности сети. Стимулы и мотивация IdM в кратком виде приводятся в таблице 1.

Таблица 1 – Стимулы и мотивация IdM

Точка зрения	Стимулы и мотивация IdM
Конечные пользователи/ абоненты	• Контроль пользователем личной информации и защита информации, позволяющей установить личность [PPII] – позволяет контролировать, кому разрешен доступ (т. е. дает согласие) к личной информации и как она используется. • Однократный вход в систему/выход из системы – обеспечивает одинаковый доступ к многим приложениям/услугам и среди многих поставщиков услуг/федераций. • Гибкое управление доступом для сетевых и прикладных услуг (например, VoIP, IPTV и передача данных). • Создание общественных сетей – обеспечивает динамичные и гибкие возможности в области идентичности для уверенного доступа к услугам общественных сетей. • Безопасность – обеспечивает уверенность в транзакциях и должна включать защиту от хищений данных идентичности (ID).

Таблица 1 – Стимулы и мотивация IdM

Точка зрения	Стимулы и мотивация IdM
Коммерческие предприятия (например, поставщики доступа к СПП)	• Дает возможность доступа к подписным услугам из любого места, в любое время и с любого устройства. • Обеспечивает функции и возможности в области гарантирования идентичности для поддержки многих приложений и услуг. • Дает возможность динамичного/автоматического установления соединений между многими партнерами (например, конечными пользователями, посещаемыми и домашними сетями) в сравнении с двусторонними договоренностями по заключению соглашений об обслуживании, обмену информацией, подтверждающей идентичность, и обеспечению реализации политики. • Дает возможность внедрения новых приложений и услуг (например, конвергенция фиксированной и подвижной связи), включая услуги на основе идентичности, такие как услуги в области идентичности, регистрационных данных и атрибутов для абонентов и поставщиков других услуг. • Дает возможность использовать стандартную схему API и данных для проектирования приложений для всего диапазона платформ многих поставщиков и платформ предоставления услуг. • Дает возможность федеративной идентичности и федеративных услуг. • Обеспечивает защиту прикладных услуг, сетевой инфраструктуры и ресурсов. • Позволяет легче соответствовать регламентарным требованиям.
Государственные предприятия	• Дает возможность внедрения услуг и приложений по гарантированию идентичности и повышает уровень доверия к поддерживаемым данным идентичности и уровень их безопасности: – услуги электронного правительства (eGovernment) (например, транзакции на базе веб); – службы общественной безопасности (например, службы неотложной помощи 911); – службы по охране правопорядка (например, правомерный перехват); – служба электросвязи в чрезвычайных ситуациях; – службы раннего предупреждения; – службы национальной безопасности. • Дает возможность предоставления федеративных государственных услуг. • Обеспечивает защиту инфраструктуры связи (например, против угроз кибербезопасности).

5.3 Поставщик данных идентичности (IdP)

В настоящей Рекомендации не налагаются какие-либо ограничения на то, кто предоставляет услуги поставщика данных идентичности (IdP).

IdP – это объект, который создает и поддерживает надежную информацию, подтверждающую идентичность других объектов (например, пользователей/абонентов, организаций и устройств), и управляет такой информацией, а также предоставляет основанные на идентичности услуги на основе доверия, деловых отношений и других типов отношений.

В среде с участием многих поставщиков услуг может оказаться, что поставщиком данных идентичности будет поставщик доступа к СПП. Также возможно, что поставщик доступа к СПП будет предоставлять услуги IdP (например, услуги на основе идентичности) другим поставщикам. Кроме того, возможно использовать услуги IdP третьей стороны.

5.4 Функциональная архитектура СПП и использование идентификаторов

Как описывается в Рекомендации [b-ITU-T Y.2012], *Функциональные требования и архитектура СПП выпуска 1*, СПП состоит из многих функциональных элементов, которые используют идентификаторы объектов для осуществления своих функций с целью поддержки услуг и приложений и содействия им. На рисунке 3 показаны примеры идентичностей, отображенных на функциональной диаграмме СПП, т. е. архитектура, приведенная в Рекомендации [b-ITU-T Y.2012].

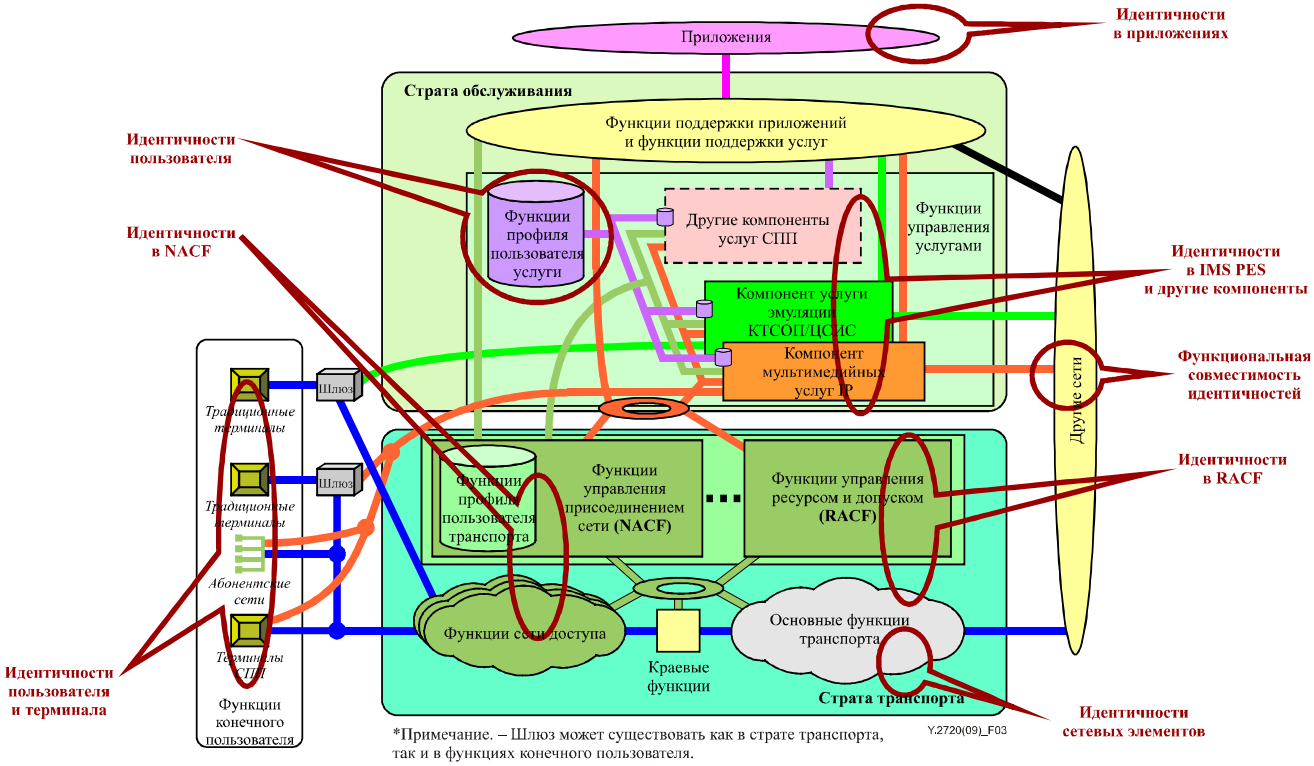

Рисунок 3 – Пример данных идентичности СПП

Поскольку эти различные идентичности используются во всех операциях СПП, важно поддерживать их целостность. IdM обеспечивает услуги, возможности и функции поддержания их целостности и использования идентичностей СПП.

В сетевой среде СПП один объект может иметь множество атрибутов идентичности. Различные элементы сети могут использовать эти атрибуты идентичности (например, в различных доменах поставщиков услуг доступа к СПП или в разных стратах СПП (например, страта услуг или страта транспорта)). Различные объекты в разных местоположениях также могут использовать эти атрибуты идентичности. Поэтому необходимо, чтобы IdM обеспечивало возможности, которые позволяют гарантировать безопасный обмен информацией между объектами (и/или местоположениями), такими как полагающиеся стороны (например, приложения, услуги или их поставщики) и поставщики данных идентичности (IdP). Следует учесть, что поставщик доступа к СПП также может быть IdP. Обмен информацией при IdM основан на разработанной политике и доверии, установленном между этими объектами в среде с участием многих поставщиков услуг. Такое доверие основано на утверждении и проверке достоверности идентичностей объектов во всех системах распределенных СПП. IdM также предоставляет возможности для защиты конфиденциальности информации объектов (например, особые атрибуты идентичности) и обеспечивает, чтобы по СПП распространялась только авторизованная информация.

6 Обзор структуры IdM

Структура IdM организована таким образом, как это показано на рисунке 4.

Рисунок 4 – Обзор структуры IdM

Структура состоит из следующих функций и возможностей IdM:

1) Управление жизненным циклом идентичности:

   Включает процессы управления жизненным циклом и функции для данных идентичности и информации, подтверждающей идентичность (например, идентификаторы, регистрационные данные и атрибуты). Управление жизненным циклом идентичности охватывает процессы и процедуры, связанные с регистрацией и выдачей данных идентичности, или данные и информацию, связанные с идентичностью объекта.

2) Функции эксплуатации, администрирования, технического обслуживания и обеспечения (OAM&P) при управлении определением идентичности (IdM):

   Включают функции и возможности по управлению эксплуатацией, администрированием, техническим обслуживанием и обеспечением (OAM&P), особенно относящиеся к поддержке IdM. OAM&P – это группа функций по управлению, которые обеспечивают поиск неисправностей в системе или сети, мониторинг качества работы, управление безопасностью, функции диагностики, конфигурацию и обеспечение пользователей. В частности, сюда входят функции и возможности, поддерживаемые системами управления сетью, обычно называемыми OSS (система эксплуатационной поддержки) и BSS (система поддержки деятельности предприятия).

3) Функции сигнализации и контроля при управлении определением идентичности (IdM):

   Включают функции и возможности по сигнализации и контролю, используемые для поддержки услуг, возможностей и функций IdM. Включают сигнализацию и контроль при связи в реальном времени и близком к реальному времени.

4) Функции федеративной идентичности при управлении определением идентичности (IdM):

   Включают функции и возможности для федерации идентичности и поддержки федеративных услуг.

5) Функции пользователей и абонентов при управлении определением идентичности (IdM):

Включают функции и процессы, связанные с контролем со стороны конечных пользователей и абонентов за информацией, касающейся их идентичности (например, PII, личные предпочтения и местоположение). Включают функции контроля, делегирования и разрешения использования и распространения информации, связанной с идентичностью.

6) Качество работы, надежность и масштабируемость при управлении определением идентичности (IdM):

Включают функции и процедуры, касающиеся качества работы, надежности и масштабируемости систем и решений IdM.

7) Безопасность при управлении определением идентичности (IdM):

Включает функции и процедуры, касающиеся обеспечения защиты систем, услуг и возможностей IdM.

8) Правовые и регламентарные нормы при управлении определением идентичности (IdM):

Правовые и регламентарные нормы не входят в сферу охвата настоящей Рекомендации.

ПРИМЕЧАНИЕ. – Этот пункт приводится для полноты информации.

Подробное описание каждого пункта приводится в разделе 8.

7 IdM в контексте архитектуры и эталонных моделей СПП

7.1 Общая связь с архитектурой и услугами СПП

Рисунок 5 иллюстрирует связь структуры IdM в более широком контексте сетей СПП.

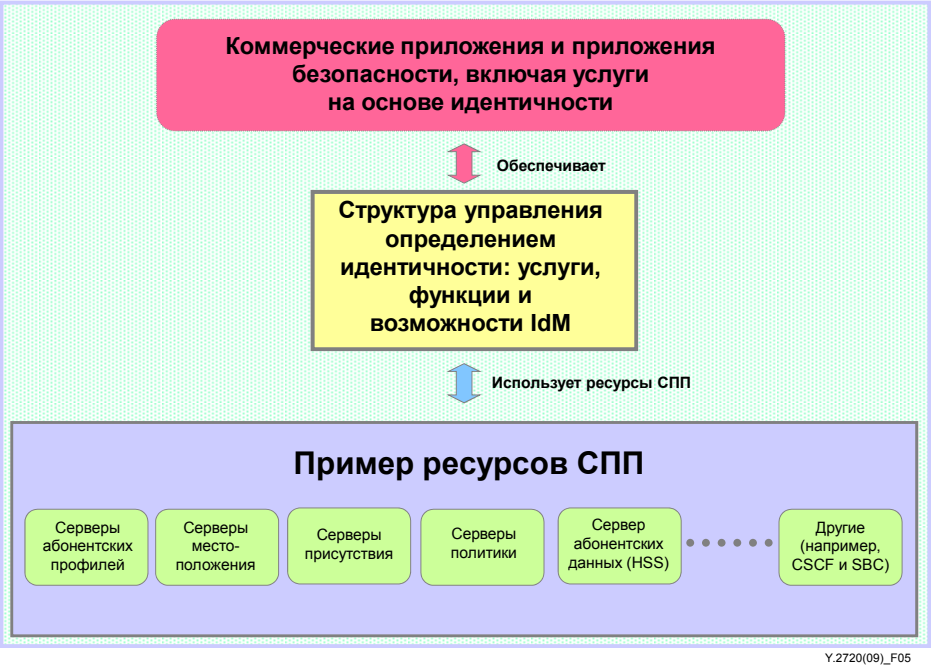

Рисунок 5 – Связь с архитектурой и услугами СПП

Как показано на диаграмме, в структуре используются ресурсы сети СПП (например, информация в серверах абонентов, местоположений, политики, присутствия и серверах абонентских данных, а также других элементах сети, таких как функция управления сеансами связи (CSCF) и пограничный контроллер сеансов связи (SBC)). Услуги, функции и возможности IdM, обеспечиваемые этой структурой, используются для поддержки и усиления коммерческих приложений и приложений безопасности, включая услуги на основе идентичности.

7.2 Эталонные модели, указанные в Рекомендации МСЭ-Т Y.2011 (Общие принципы и общая эталонная модель для СПП)

В данном разделе описываются услуги, функции и возможности IdM в контексте архитектурных моделей СПП и справочных документов, указанных в Рекомендации [ITU-T Y.2011], *Общие принципы и общая эталонная модель для СПП.*

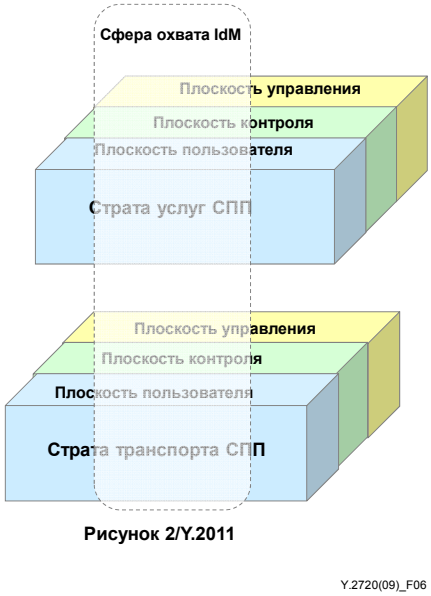

Рисунок 6 – Сфера охвата IdM в контексте рисунка 2 [ITU-T Y.2011]

На рисунке 6 показана сфера охвата IdM в контексте эталонной архитектурной модели СПП, определенной на рисунке 2 Рекомендации [ITU-T Y.2011]. На нем показано, что связанные с IdM функции могут находиться в плоскостях пользователей, контроля и управления.

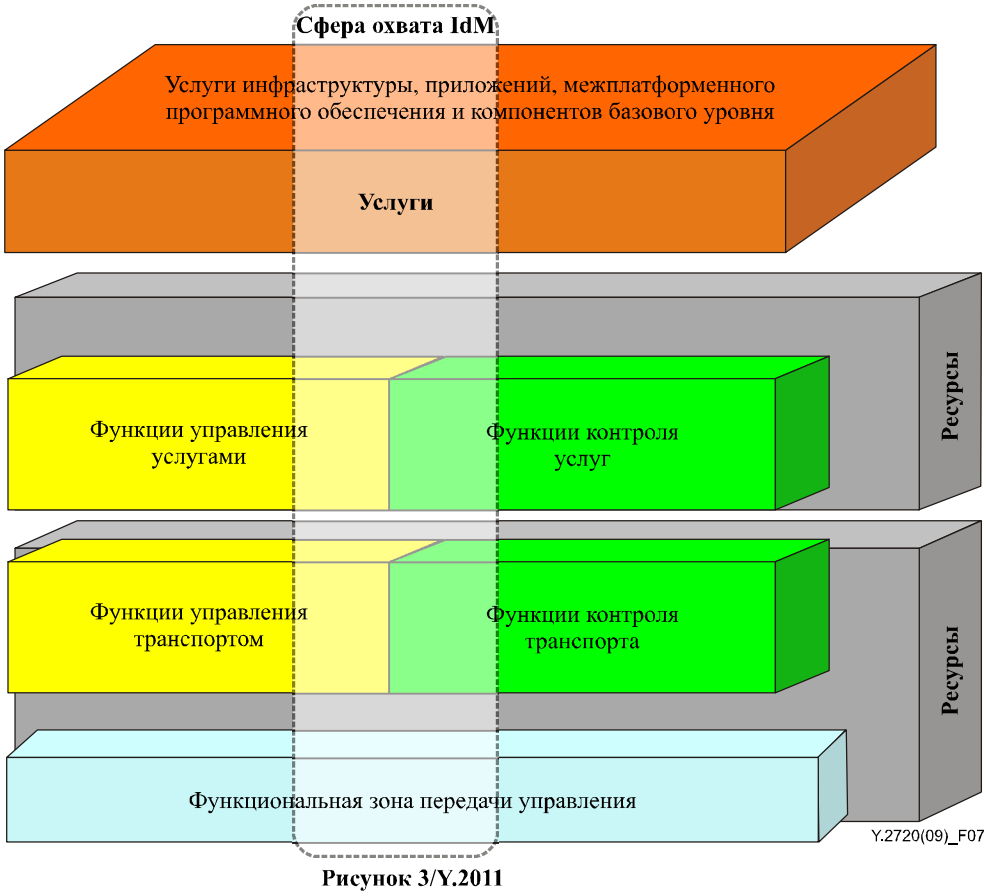

Рисунок 7 – IdM в контексте рисунка 3 [ITU-T Y.2011]

На рисунке 7 показана сфера охвата IdM в контексте эталонной архитектурной модели СПП, определенной на рисунке 3 Рекомендации [ITU-T Y.2011]. На нем показано, что связанные с IdM функции могут быть включены во все вертикальные слои архитектуры СПП.

8 Структура управления определением идентичности

В данном разделе дается подробное описание функциональных групп, упомянутых в разделе 6.

8.1 Управление жизненным циклом идентичности

8.1.1 Проверка подлинности и запись

Первый этап создания идентичности для какого-либо объекта (например, абонента, устройства, организации, поставщика доступа к СПП или элемента) начинается с процесса проверки подлинности и записи идентичности или регистрационных данных. Это процесс описания идентичности или регистрационных данных, связанных с тем или иным конкретным объектом, который может быть основан на конкретном контексте (например, ролях).

В случае абонентов из числа конечных пользователей – это процесс, при котором сторона подает заявку на то, чтобы стать абонентом IdP или поставщика доступа к СПП.

Для абонентов из числа конечных пользователей имя абонента может быть проверенным именем. Проверенное имя связано с идентичностью объекта. Прежде чем заявитель может получить регистрационные данные или запись маркера, связанного с проверенным именем, он должен доказать, что его идентичность является подлинной и что он является именно тем объектом, который имеет право использовать эту идентичность. Такой процесс называется проверкой подлинности идентичности. Как только имя проверено, оно может быть ассоциировано с псевдонимом для обеспечения анонимности.

Проверка подлинности включает проверку атрибутов и заявляемой информации, связанных с идентичностью. Она охватывает процессы и процедуры проверки и проверки достоверности информации при записи объекта в системе идентичности.

Эффективность IdM в целом зависит первоначально от процесса проверки подлинности и записи. Для обеспечения того, чтобы процесс записи в целом был правильно разработан и внедрен, нужны четко определенные требования гарантии, а также необходимо наличие надлежащей политики и процедур управления.

Руководящие указания, которые необходимо рассмотреть, включают:

- профессиональную подготовку персонала, участвующего в процессе записи;
- надлежащее качество документов и других подтверждающих материалов, обеспечивающих запись объекта;
- процессы, позволяющие избегать подлога при записи;
- процессы, позволяющие избегать множественной или двойной записи одного и того же объекта.

8.1.2 Выдача и аннулирование

Успешное завершение процесса записи приводит к выдаче средств (например, регистрационных данных), с помощью которых объект может быть в будущем аутентифицирован. Например, к выдаче IdP (или поставщиком доступа к СПП) регистрационных данных, увязанных с идентичностью или с соответствующим атрибутом (например, привилегией или заявляемой информацией) идентичности, относящейся к объекту.

Аннулирование идентичности – это процесс объявления недействительными идентичности и связанных с ней регистрационных данных. За поддержание и защиту информации, касающейся идентичности, отвечают сторона или система (например, IdP или поставщик доступа к СПП), которые выдают идентичность или регистрационные данные. Аннулирование требуется для того, чтобы предотвратить продолжающееся использование идентичности или регистрационных данных, которые более не действительны или у которых есть пробел в защите.

Руководящие указания, которые необходимо рассмотреть, включают:

- разработку критерия выдачи и аннулирования;
- разработку критерия обновлений и изменений;
- синхронизацию информации, подтверждающей идентичность;
- разработку процессов и процедур выдачи и аннулирования;
- аудит и рассмотрение процессов выдачи и аннулирования;
- процедуры и процессы заявления о выдаче, обновления и аннулирования идентичности или регистрационных данных (например, во всех системах и процессах, с помощью которых была создана идентичность, необходимо предусмотреть возможность определения того, что идентичность или регистрационные данные выданы, обновлены и аннулированы);
- четко определенные процедуры и процессы выдачи и аннулирования идентичности или регистрационных данных, а также соответствующая политика. Кроме того, для обеспечения того, чтобы процесс в целом был должным образом разработан и внедрен, необходимы процедуры управления; и
- механизмы защиты процессов и процедур аннулирования от угроз безопасности.

8.2 Функции OAM&P при управлении определением идентичности

8.2.1 Модель и схема данных

Каждый поставщик доступа к СПП, каждая федерация или предприятие могут иметь собственные форматы, схемы, определения или семантику для представления данных и информации, касающихся идентичности, и обмена ими. Например, такая информация, как дата рождения, может быть представлена в двух разных системах различным образом (например, месяц/день/год иди день/месяц/год). Кроме того, семантика, схемы и протоколы, которые используются для запроса информации, связанной с идентичностью, и обмена такой информацией, могут различаться, что приведет к проблемам в функциональной совместимости. Например, в коммутируемой телефонной сети общего пользования (КТСОП) информация, подтверждающая идентичность, такая как номер вызывающей стороны и идентичность вызывающего абонента, представляется с использованием

конкретной семантики и извлекается с использованием конкретных протоколов (например, SS7), и они отличаются от системы SIP на базе VoIP.

Большое значение имеют решения, которые дают возможность функциональной совместимости между неоднородными системами IdM, в которых используются различные модели, структуры и схемы данных.

Руководящие указания, которые необходимо рассмотреть, включают:

- модели и схемы данных для содействия функциональной совместимости между неоднородными системами IdM (например, источники данных идентичности) в рамках домена поставщика доступа к СПП (например, продукция различных поставщиков);
- модели и схемы данных для содействия функциональной совместимости между различными поставщиками доступа к СПП (между сетями); и
- модели и схемы данных для содействия функциональной совместимости между различными федерациями (например, поставщик доступа к СПП и поставщики веб-услуг).

8.2.2 Управление использованием идентификаторов

Идентичность объекта (например, пользователя/абонента, организации, федерации, предприятия, поставщика услуг, устройства и элементов) может включать один или несколько идентификаторов, связанных с идентичностью, определением которой необходимо управлять и которую необходимо поддерживать.

Идентификатор – это любое обозначение, которое используется для представления идентичность объекта, такое как ID пользователя, ID сети, адрес электронной почты, псевдоним, групповое имя и т. д. Например, к идентичности пользователя/абонента могут относиться следующие идентификаторы:

- ID пользователя;
- адрес электронной почты;
- номер телефона;
- URI;
- адрес IP.

Эффективность IdM в целом зависит от гарантии индивидуальных идентификаторов, которые могут сопоставляться и увязываться для гарантирования идентичности объекта. В связи с этим для управления использованием идентификаторов необходимы четко определенные требования и процедуры.

Руководящие указания, которые необходимо рассмотреть при разработке и внедрении IdM, включают:

- Есть разные типы идентификаторов с различными характеристиками, использованием которых необходимо управлять. К примеру, некоторые идентификаторы могут быть глобальными (например, едиными в различных федерациях), псевдонимы могут быть значимыми в рамках какой-либо системы или однократный идентификатор может быть действительным в течение определенного периода времени.
- Идентификаторы могут иметь различные характеристики, которые влияют на конфиденциальность в том, что касается защиты от неверного сопоставления действий пользователей.

8.2.3 Управление использованием атрибутов

Атрибуты идентичности – это дескрипторы объекта, такие как тип объекта, предпочитаемый адрес IP, домен, информация об адресе, номер телефона. Атрибуты также могут содержать заявляемую информацию, права, привилегии, списки, касающиеся передачи полномочий, и специальные ограничения. Другие типы атрибутов включают информацию, которую отслеживают для обнаружения вторжения, такую как неудавшиеся попытки утверждения идентичности, подсчет вводов нового ключа и т. д.

Эффективность IdM будет зависеть от гарантии атрибутов, которые могут сопоставляться и увязываться для гарантирования идентичности объекта. Такие действия включают хранение и предоставление атрибутов. В связи с этим для управления использованием атрибутов необходимо ввести в действие четко определенные требования и процедуры.

Модель поведения является особым типом атрибута, который представляет собой любую характеристику, связанную с поведением объекта. Информация о модели поведения может

присваиваться системами IdM на основе прошлого опыта и прошлого взаимодействия, а не устанавливаться самим объектом. Примерами информации о модели поведения, которая может использоваться для оценки гарантии идентичности, являются адрес IP, пункт доступа, информация о местоположении, время пользования и системы, к которым осуществляется доступ.

Руководящие указания, которые необходимо рассмотреть при управлении использованием атрибутов, включают:

- информация о модели поведения может считаться PII;
- строгие требования и процедуры для управления использованием информации о модели поведения;
- использование информации о модели поведения для уменьшения возможности хищения данных идентичности;
- соответствие политике в области PII.

8.2.4 Управление использованием регистрационных данных

Регистрационные данные используются для аутентификации заявляемой идентичности. Регистрационные данные включают:

- имя пользователя/пароли;
- цифровые сертификаты;
- маркеры и смарт-карты;
- защитные подсказки;
- информацию, связанную с PKI, такую как ключи, сертификаты, орган, подписывающий сертификаты, криптографическая информация и т. д.; и
- биометрические данные.

Управление использованием регистрационных данных объекта охватывает операционную деятельность по созданию и выдаче информации, используемой для аутентификации заявлений идентичности, и управлению использованием такой информации. Эффективность IdM зависит от процессов, процедур и возможностей управления использованием регистрационных данных. В связи с этим для управления использованием регистрационных данных необходимы четко разработанные требования и процедуры.

Руководящие указания по управлению использованием регистрационных данных включают:

- разработку и поддержание политики в области регистрационных данных;
- процессы и процедуры управления жизненным циклом регистрационных данных (подгруппа управления жизненным циклом идентичности, рассмотренная в разделе 8.1);
- политику и соглашения о предоставлении услуг в среде с участием многих поставщиков услуг/доступа к сети (обсуждение политики в области регистрационных данных, обеспечение соответствия требованиям федерации, публикация информации о регистрационных данных, такой как открытые ключи).

8.2.5 Ведение журнала и аудит информации

Функции и возможности в области ведения журнала и аудита информации имеют большое значение для эффективности решений IdM. Примерами мер в области ведения журнала и аудита информации являются ведение журналов безопасности для выполнения требований к отчетности, защита и надлежащее использование личной информации, а также представление уведомлений соответствующим системам или объектам (например, владельцам идентичности).

Руководящие указания по ведению журнала и аудиту информации включают:

- ведение журнала и аудит информации о связанных с IdM событиях (например, доступ к информации, подтверждающей идентичность, попытки несанкционированного доступа, обновление меток времени и т. д.) для криминалистического анализа;
- механизмы и процедуры, дающие возможность обратного прослеживания;
- обнаружение случаев несоблюдения применяемой политики;
- гарантирование соблюдения требований национальных регуляторных органов.

8.3 Функции сигнализации и контроля при управлении определением идентичности

8.3.1 Введение

Функции сигнализации и контроля используются для обнаружения и сообщения надежной информации, подтверждающей идентичность (например, идентификаторов, атрибутов, заявляемой информации) и связанной с тем или иным объектом (например, пользователем/абонентом, группой, организацией, элементом сети, поставщиком услуг), для поддержки услуг, функций и возможностей IdM.

В данном разделе описываются связанные с IdM функции сигнализации и контроля.

8.3.2 Обнаружение информации, подтверждающей идентичность

В распределенной среде, такой как СПП, информация, подтверждающая идентичность, может находиться в различных элементах сети (например, абонентский сервер, сервер местоположения, сервер присутствия, сервер абонентских данных и т. д.). Неотъемлемой частью IdM являются структурированные средства обнаружения источников информации, подтверждающей идентичность. Чтобы приложение могло использовать информацию, подтверждающую идентичность, оно должно знать, что такая информация существует. Ожидается, что в динамично развивающейся и появляющейся среде СПП информация, подтверждающая идентичность, и источники такой информации также будут динамичными. В связи с этим полагающимся сторонам и объектам (например, приложениям) будут необходимы структурированные средства, чтобы узнавать о наличии информации, подтверждающей идентичность, и обнаруживать такую информацию. Это включает также обнаружение услуг и возможностей функций IdM.

Руководящие указания, которые необходимо рассмотреть при определении и внедрении возможностей по обнаружению, включают:

- обнаружение в рамках домена поставщика доступа к СПП (внутри сети);
- обнаружение между различными доменами поставщиков доступа к СПП (между сетями); и
- обнаружение среди членов федерации. См. раздел 8.4.2 (Обнаружение федерации).

Обнаружение включает также возможности найти или установить местонахождения IdP. В структуре IdM СПП обнаружение необходимо, поскольку в ней может иметься много IdP. В тех ситуациях, когда есть только один IdP (например, предприятие), необходимость в операции обнаружения отсутствует, поскольку будет известно, где получать атрибуты идентичности. Кроме того, в рамках отдельно взятой сети поставщика доступа к СПП может быть много систем, обеспечивающих различные функции, связанные с управлением определением идентичности, и соответствующие функции по обнаружению.

Обнаружение аналогично поиску идентичности в веб. В поисковую систему водятся такие данные, как элементы идентичности, а на выходе получают список идентификаторов и IdP, которые удовлетворяют требованиям. Для такого сценария запроса и ответа обычно требуется, чтобы IdP зарегистрировались как поставщики конкретной услуги в области идентичности для данного пользователя/устройства.

Имеющиеся методы, которые используются для поддержки соответствующих потребностей в обнаружении и доступе, в общих чертах относятся к двум категориям: 1) перекрываемые методы "корня корней" и/или 2) дедуктивное обнаружение. Первый метод основан на том, что некоторый объект берет на себя роль главного регистратора областей имен с поддерживающим сервером, тогда как второй подход основан на хорошо известных правилах, с помощью которых можно рекурсивно получить адрес для поддерживающего сервера. Также могут использоваться комбинации этих методов.

8.3.3 Связь при IdM

Включает возможности и функции по обнаружению информации, подтверждающей идентичность, и обмену такой информацией (например, идентификаторами, регистрационными данными и атрибутами), связанной с данными идентичности объекта, который находится в различных системах сети (например, в абонентском сервере, сервере местоположения, сервере присутствия т. д.) в рамках сети поставщика доступа к СПП и которые можно сопоставить и проверить (т. е. с помощью сервера приложения IdM, обеспечивающего функции аутентификации и сопоставления) для обеспечения возможностей гарантии идентичности. Об утверждении идентичности и соответствующих атрибутов (например, заявляемой информации и привилегий) можно сообщить для утверждений полагающихся

систем (например, прикладных услуг), с тем чтобы принять решения по управлению доступом. Это даст возможность использовать в различных прикладных услугах (т. е. платформах различных поставщиков) общую инфраструктуру для IdM, в отличие от независимых и автономных решений. Отношения в области связи, которые необходимо рассмотреть, включают:

- внутрисетевые: связь с доменом поставщика доступа в СПП (например, между элементами сети);
- межсетевые: связь между двумя различными поставщиками доступа в СПП; и
- федерация: связь между членами федерации.

8.3.3.1 Связь в реальном времени и близком к реальному времени

В этом решении, используемом для обнаружения информации, подтверждающей идентичность, и обмена такой информацией, необходимо учитывать, требуется ли связь в реальном времени или близком к реальному времени. Это будет зависеть от конкретных поддерживаемых приложений.

8.3.3.2 Протоколы и интерфейсы сигнализации и контроля

На рисунке 8 показаны внешние интерфейсы, которые применяются для поддержки связи при IdM. Например, интерфейсы используются для обмена информацией, подтверждающей идентичность, или контролирования услуг, функций и возможностей IdM.

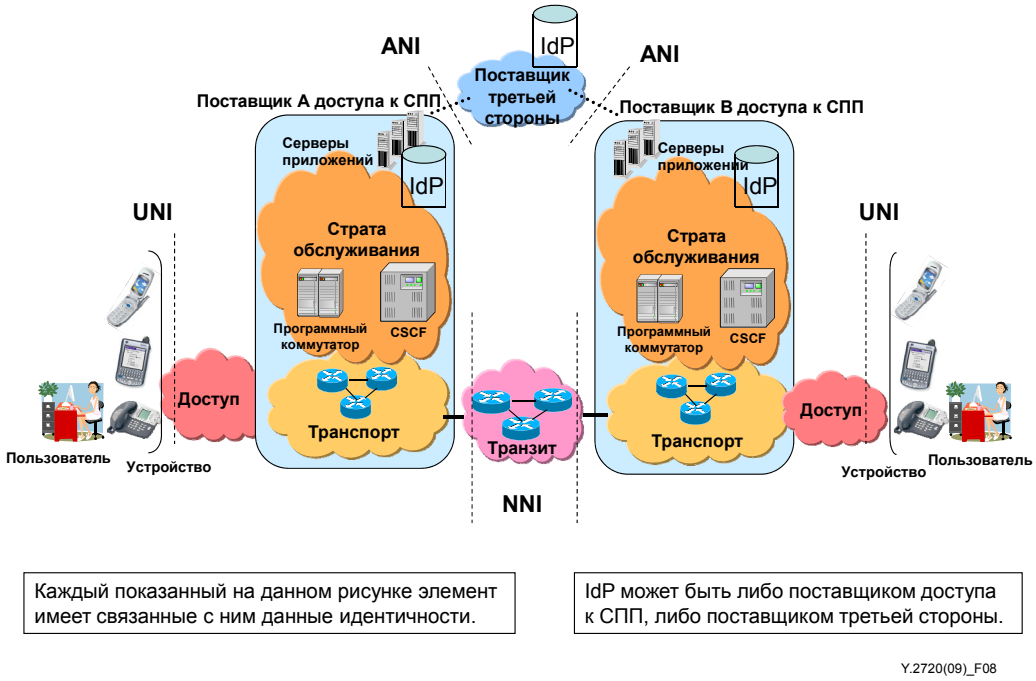

Рисунок 8 – Внешние интерфейсы

Внешние интерфейсы включают:

- интерфейс "пользователь-сеть" (UNI);
- интерфейс "приложение-сеть" (ANI); и
- интерфейс "сеть-сеть" (NNI).

Конкретные требования и протоколы, которые должны использоваться, зависят от конкретного интерфейса, информации, которую необходимо передать, или функций контроля, который необходимо осуществлять. Для содействия функциональной совместимости следует определить и указать конкретные требования, а также варианты и профили протоколов, которые должны использоваться. Решения в области интерфейсов зависят от таких факторов, как потребности в конкретных приложениях и услугах (например, в реальном времени или близком к реальному времени), решения в области протокола (например, SAML, Diameter, RADIUS), а также механизмы и подходы (например, [b-ITU-T X.509], общая архитектура начальной загрузки (GBA)).

Помимо внешних интерфейсов, для общих решений также важны внутренние интерфейсы. В рамках сети СПП информация, подтверждающая идентичность, может также быть расположена в различных элементах сети и прикладных услугах (например, абонентский сервер, сервер местоположения и сервер присутствия и другие элементы сети, такие как CSCF и SBC). Внутренние интерфейсы и протоколы, которые должны использоваться для обнаружения информации, подтверждающей идентичность, и обмена такой информацией, являются важными факторами для функциональной совместимости при наличии многих поставщиков.

8.3.3.3 Механизмы и процедуры

Следует определить и указать механизмы и процедуры, используемые для внедрения конкретных функций или возможностей IdM. Например, следует определить и указать конкретные механизмы или протоколы, а также где и как они используются. Примеры механизмов и протоколов включают:

- SAML;
- X.509;
- GBA; и
- E.115.

8.3.4 Сопоставление и увязка

Информация, подтверждающая идентичность (например, идентификаторы, регистрационные данные и атрибуты), может сопоставляться для создания увязки с целью гарантирования идентичности объекта. Например, информация, подтверждающая идентичность, которая относится к абоненту (например, ID пользователя), абонентскому устройству (например, ID устройства) и информация о местоположении может быть сопоставлена для создания увязки с целью обеспечения более надежной гарантии абонента.

Руководящие указания, которые необходимо рассмотреть при определении и внедрении сопоставления и увязки, включают:

- обеспечение реализации применяемой политики (например, политика анонимности или конфиденциальности).

8.3.5 Аутентификация

Аутентификация – это процесс создания доверия к идентичности объекта. Одним из средств гарантирования аутентификации является описание задач и руководящих указаний, необходимых для оценки рисков, связанных с тем, что объект является именно таким объектом, за который он себя выдает. Это включает определение того, какие идентификаторы объекта имеют более важное значение по сравнению с другими в процессе аутентификации и почему некоторые идентификаторы, используемые при аутентификации, не должны иметь для нее такое же значение.

Обычно доверие достигается с помощью выдачи для отдельных систем пар ID пользователя и пароль. Однако, в СПП такой подход нежелателен, неэффективен с эксплуатационной точки зрения и может привести в небезопасной практике. Руководящие указания, которые необходимо рассмотреть при определении и внедрении аутентификации, включают:

- конфиденциальность и целостность механизмов аутентификации;
- достаточно надежные регистрационные данные, которым можно доверять в различных системах.

8.3.6 Гарантия аутентификации

Гарантирование аутентификации – это процесс создания доверия к идентификаторам и заявляемой информации, которые представлены в информационной системе. Не вся информация, используемая для аутентификации, должна рассматриваться равным образом или обязательно иметь одно и то же значение для гарантии. Например, доверие при аутентификации, при которой используются биометрические данные, существенно отличается по сравнению с аутентификаций, при которой используется ID пользователя/пароль. Для оценки доверия к тому, что аутентифицируемый объект является действительным объектом, каждому идентификатору необходимо присвоить относительное значение на основе базисных принципов.

Задача гарантии аутентификации состоит в оценке рисков, связанных с тем, что объект является именно таким объектом, за который он себя выдает. Не все идентификаторы, используемые в процессе принятия решений в области аутентификации, рассматриваются равным образом или

обязательно имеют одно и то же значение для аутентификации. Кроме того, по мере того как последствия аутентификационной ошибки становятся более серьезными, требуемый уровень гарантии аутентификации должен повышаться в зависимости от возможных последствий (например, критический характер воздействия) аутентификационной ошибки.

Механизм оценки и сообщения гарантии аутентификации позволяет полагающимся сторонам принимать решения, касающиеся доверия в процессе аутентификации, используемой для проверки достоверности идентичности или заявляемой информации об объекте.

Основным преимуществом гарантии аутентификации является возможность определить уровень доверия к тому, что объект является именно тем объектом, который заявляется на протяжении жизненного цикла идентичности. Важнейшее значение для поддержки федеративных услуг и обеспечения кибербезопасности имеют стандартный критерий присвоения и сообщения относительного значения гарантии процесса, механизмов и данных аутентификации (например, пароля, регистрационных данных, биометрических данных) в различных федерациях.

В процессе гарантирования аутентификации следует учитывать следующее:

- Механизм аутентификации: неизменяемые пароли менее надежны, чем однократные пароли, и, как правило, маркеры аппаратных средств с PIN более надежны, чем маркеры программного обеспечения.
- Протокол аутентификации: протокол, про который известно, что он защищен от атак типа "злоумышленник в середине" или который основан на криптографических операциях, считающихся в целом надежными.
- Характеристики устройства, используемого для аутентификации: доверие к аутентификации частично основано на характеристиках устройства, используемого пользователем, т. е. серийно выпускаемый промышленностью компьютер, принадлежащий соответствующей организации и контролируемый ею, или специальное защищенное от несанкционированного доступа устройство более надежны, чем общедоступное серийно выпускаемое промышленностью устройство.
- Местоположение аутентифицируемого объекта: следует принимать во внимание местоположение пользователя, т. е. помещения организации или информационный киоск общего пользования, интернет-кафе и т. д. Доверие к аутентификации может быть выше, если терминалу общего пользования в информационном киоске сложно убедить аутентификационный сервер в том, что он расположен в физических границах какой-либо организации.
- Канал связи: при аутентификации, как правило, задействуется канал связи (беспроводные сети, коммерческие арендованные линии и т. д.) между аутентифицируемым объектом и сервером, обеспечивающим аутентификацию и/или связанные с доступом решения. Используемую для аутентификации информацию необходимо надежным образом сообщить серверу аутентификации и обеспечить, чтобы она не была восприимчива к обманным действиям какого-либо злоумышленника.
- Относительная легкость манипуляции с аутентификаций при злонамеренном поведении: важно оценить риск, связанный с компрометаций криптографических ключей.

8.3.7 Делегирование

Делегирование включает действия и процессы передачи привилегий на осуществление некоторых действий от имени администратора доступа от объекта, имеющего такие привилегии, перед другим объектом, у которого нет таких привилегий.

Например, делегирование полномочий начинается с того, что можно определить, какие счета дают возможность осуществлять некоторые управленческие действия (такие, как создание новых счетов) или управлять конкретными функциями (такими, как изменение пароля счета). Таким образом, с учетом возможности делегирования действий или работы администрации, цель состоит в обеспечении среды, в которой эта задача выполняется безопасным и ответственным образом.

8.3.8 Обеспечение реализации политики

При разработке и внедрении решений в области IdM следует учитывать, что применимая политика должна реализовываться. Например, обеспечение реализации политики обычно связывается с:

- анонимностью и конфиденциальностью;
- созданием и сбором информации, подтверждающей идентичность;
- использованием и распространением информации, подтверждающей идентичность.

8.3.9 Поддержка услуг, требующих приоритетного режима

При разработке и внедрении решений в области IdM следует принимать во внимание поддержку прикладных услуг и сеансов связи, которые требуют приоритетного режима, например в службе электросвязи в чрезвычайных ситуациях (ETS). Например, приоритетный режим должен предоставляться любому взаимодействию с системами IdM для установления и поддержания сеансов связи ETS. Информация об услугах и возможностях, требующих приоритетного режима, приводится в Рекомендациях [b-ITU-T E.107] и [b-ITU-T Y.2205].

8.4 Функции федеративной идентичности при управлении определением идентичности

8.4.1 Федеративная идентичность

Общая концепция федерации состоит в том, чтобы предоставить возможность каждому члену федерации оставаться независимым и при этом содействовать обмену конкретной информацией, подтверждающей идентичность, для обеспечения возможности федеративных услуг. Например, в федерации могла бы быть объединена (т. е. предоставляться членам федерации) некоторая информация, подтверждающая идентичность пользователя/абонента (например, подгруппа профиля абонента).

8.4.2 Обнаружение федерации

Обнаружение федерации состоит из функций и механизмов обнаружения информации о федеративной идентичности и обмена такой информацией. Например, в федерации может быть объединена некоторая информация, подтверждающая идентичность, о пользователе/абоненте, такая как подгруппа информации о профиле абонента.

Основной аспект обнаружения федерации заключается в определении или обнаружении подходящего IdP или IdP, который является авторитетным источником какой-либо конкретной информации, подтверждающей идентичность и связанной с объектом (например, местоположение информации).

Обнаружение необходимо в любой архитектуре, в которой участвуют многие IdP или для которой местоположение IdP потенциально является динамичным. В ситуациях, когда имеется лишь один поставщик данных идентичности (т. е. предприятие), необходимость в операции по обнаружению отсутствует, поскольку любой RP/SP потенциально будет знать, где получать информацию, подтверждающую идентичность объекта.

8.4.3 Сопряжение и взаимодействие сетей

В целом, каждый поставщик доступа к СПП, каждое предприятие или каждый член федерации могут иметь собственные форматы, схемы, определения или семантику для представления данных и информации, касающихся идентичности, и обмена ими. Например, такая информация, как дата рождения, может быть представлена в двух разных системах различным образом. Кроме того, семантика, схемы и механизмы, которые используются для запроса информации, связанной с идентичностью, и обмена такой информацией, могут различаться, что приведет к проблемам в функциональной совместимости. В связи с этим будут необходимы соответствующие возможности, обеспечивающие сопряжение и взаимодействие сетей между различными федерациями.

8.5 Функции пользователей и абонентов при управлении определением идентичности

Для эффективных решений в области IdM требуются функции, которые дают конечному пользователю/абоненту возможность предоставлять информацию, касающуюся контроля информации, подтверждающей их идентичность. Сюда входят функции и возможности, позволяющие объекту, такому как конечный пользователь/абонент, предоставлять поставщику услуг и IdP информацию об условиях, ограничениях, согласии, авторизации, касающихся создания, сбора, использования и распространения информации, подтверждающей их идентичность.

Эти функции связаны с обеспечением реализации применимой политики, такой как политика в области защиты PII, анонимной или псевдонимной информации, подтверждающей идентичность.

Руководящие указания, которые необходимо рассмотреть, включают:

- средства, позволяющие конечным пользователям/абонентам сообщать поставщику доступа в СПП сведения о контроле информации, подтверждающей их идентичность;
- соответствие применяемой политике в области защиты PII; и
- удобство пользования для конечного пользователя/абонента.

8.6 Качество работы и надежность

8.6.1 Качество работы

Возможности и функции IdM будут использоваться для того, чтобы поддерживать и увеличивать широкий диапазон коммерческих приложений и приложений безопасности. Например, функции IdM могут использоваться для гарантии идентичности объектов связи до того, как будет разрешен сеанс связи (например, сеанс VoIP, IPTV или передачи данных). В связи с этим воздействие качества работы IdM на поддерживаемые прикладные услуги более высокого уровня (например, VoIP, IPTV, передача данных) имеет большое значение для общей эффективности решения. Например, IdM не должен оказывать негативного воздействия на поддерживаемые прикладные услуги более высокого уровня таким образом, чтобы затрагивались общее качество обслуживания (QoS) и оценка пользователем качества услуги (QoE) конечных пользователей/абонентов.

При разработке решений в области IdM большое значение имеют соображения, связанные с управлением качеством работы. Управление качеством работы включает сбор и анализ статистических данных для целей мониторинга качества работы. Мониторинг качества работы – это систематическая оценка способности сетевой системы осуществлять присвоенные ей функции с помощью постоянного сбора и анализа соответствующих рабочих данных. Процедуры мониторинга качества работы предназначены для сбора данных об условиях нерегулярных ошибок и нарушений работы в результате постепенного изнашивания сетевого оборудования. Методы упреждающего обслуживания, такие как мониторинг качества работы, позволяют заблаговременно обнаруживать нарушения, до того как они станут более серьезными.

8.6.2 Точность меток времени

Точность меток времени является одним из факторов при IdM. С помощью аудита описывается появление событий в пределах этих временных рамок. Метки времени имеют важнейшее значение для целей аудита, а точность меток времени предопределяет качество, если не пригодность к использованию, данных аудита.

Точность меток времени определяется тремя факторами: точность, с которой считывается местный тактовый импульс меток времени, возможность отслеживать местный тактовый импульс по отношению к опорному тактовому импульсу, а также степень математической неопределенности местного тактового импульса, измеренного по отношению к опорному тактовому импульсу.

8.6.3 Надежность и готовность

Надежность и отказоустойчивость сетевых элементов и систем, обеспечивающих функции и возможности IdM, являются важным аспектом разработки и внедрения решений, поскольку IdM будет использоваться для поддержки и увеличения широкого диапазона коммерческих приложений и приложений безопасности, у которых могут иметься конкретные требования в области готовности. В связи с этим необходимо рассмотреть следующие требования и руководящие указания в отношении факторов готовности:

- разработки систем (например, дублирование) для целей устойчивости и отказоустойчивости; и
- разнообразие (например, географическое разнообразие) для целей готовности.

Помимо разработки и внедрения решений в области IdM, следует также рассмотреть меры обеспечения безаварийной работы. Например, полагающееся приложение может позволять некоторые ограниченные привилегии, если вся система IdM отказала в работе или стала не готовой к работе.

8.7 Безопасность при IdM

8.7.1 Безопасность сетевых элементов, обеспечивающих IdM

В связи с тем, что информация и ресурсы, подтверждающие идентичность, являются ценными и чувствительными и используются для поддержки коммерческих приложений и услуг, сетевые элементы, обеспечивающие услуги, функции и возможности IdM, будут подвергаться атакам на безопасность и поэтому будут требовать обеспечения безопасности.

Необходимы надлежащие требования и меры в области безопасности и защиты сетевых элементов и систем, которые обеспечивают функции, услуги и возможности IdM. Примерами мер в области безопасности являются:

- обеспечение безопасности услуг, функций и возможностей IdM;

- обеспечение безопасности интерфейсов сигнализации и связи; и
- обеспечение безопасности интерфейсов управления системами IdM (т. е. интерфейсов, используемых для конфигурации и управления информацией, подтверждающей идентичность).

8.7.2 Защита информации, позволяющей установить личность (PII)

Защита PII является очень важным аспектом IdM. Следует определить и внедрить конкретные возможности по защите PII. Это связано с обеспечением реализации применяемой политики в области защиты PII, при условии соблюдения нормативных положений национального и регионального уровней. Функции и возможности, которые необходимо рассмотреть, включают:

- возможности пользователей/абонентов сообщать предпочтения, касающиеся PII;
- возможности обеспечивать прозрачность (т. е. возможности гарантировать, чтобы доступ к PII имели только санкционированные объекты и чтобы только они могли просматривать PII); и
- возможности предоставлять заявки, касающиеся распространения и использования информации, подтверждающей идентичность.

Библиография

[b-ITU-T E.107] Рекомендация МСЭ-Т E.107 (2007 г.), *Служба электросвязи в чрезвычайных ситуациях (ETS) и основа для взаимодействия реализованных на национальном уровне ETS*.

[b-ITU-T E.115] Рекомендация МСЭ-Т E.115 (2008 г.), *Компьютеризированное справочное обслуживание*.

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

[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 1081-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

[b-ITU-T X.911] Рекомендация МСЭ-Т X.911 (2005 г.) | ISO/IEC 15414:2006, *Информационные технологии – Открытая распределенная обработка – Эталонная модель – Корпоративный язык*.

[b-ITU-T X.1121] Рекомендация МСЭ-Т X.1121 (2004 г.), *Структура технологий безопасности для подвижной передачи данных от конца до конца*.

[b-ITU-T X.1141] Рекомендация МСЭ-Т X.1121 X.1141 (2006 г.), *Язык разметки, предусматривающий защиту данных (SAML 2.0)*.

[b-ITU-T Y.2001] Рекомендация МСЭ-Т Y.2001 (2004 г.), *Общий обзор СПП*.

[b-ITU-T Y.2012] Рекомендация МСЭ-Т Y.2012 (2006 г.), *Функциональные требования и архитектура СПП выпуска 1*.

[b-ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2008 г.), *Термины и определения для сетей последующих поколений*.

[b-ITU-T Y.2205] Рекомендация МСЭ-Т (2008 г.), *Сети последующих поколений – Электросвязь в чрезвычайных ситуациях – Технические соображения*.

[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*.

[b-ETSI EG 202 072] ETSI EG 202 072, V1.1.1 (2002), *Universal Communications identifier (UCI); Placing UCI in context; Review and analysis of existing identification schemes*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=14108>

[b-ETSI EG 202 236] ETSI EG 202 236, V1.1.1 (2003), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)*; *Design guide; Use of non-numeric names*. <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17732>

[b-ETSI EG 284 004] ETSI EG 284 004, V1.1.2 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21139>

[b-ETSI TS 102 042] ETSI TS 102 042, V1.3.4 (2007), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27736>

[b-RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*.
<http://www.ietf.org/rfc/rfc3650.txt?number=3650>

[b-NIST] NIST SP800-63, v6.3.3, *Electronic Authentication Guidelines*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OGIM] The Open Group, *Identity Management White Paper* (03/2004).
<http://www.opengroup.org/bookstore/catalog/w041.htm>

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

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

Отпечатано в Швейцарии
Женева, 2010 г.