Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Y.2721

(09/2010)

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

Сети последующих поколений – Безопасность

Требования к управлению определением идентичности СПП и случаи применения

Рекомендация МСЭ-Т Y.2721

ITU-T

Международный союз электросвязи

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
IPTV по СПП	Y.1900–Y.1999
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
Будущие сети	Y.2600–Y.2699
Безопасность	**Y.2700–Y.2799**
Обобщенная мобильность	Y.2800–Y.2899
Открытая среда операторского класса	Y.2900–Y.2999
Будущие сети	Y.3000–Y.3099

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

Рекомендация МСЭ-Т Y.2721

Требования к управлению определением идентичности СПП и случаи применения

Резюме

В Рекомендации МСЭ-Т Y.2721 представлены примеры случаев использования управления определением идентичности (IdM), а также требования к IdM для сетей последующих поколений (СПП) и их интерфейсов. Функции и возможности IdM используются для повышения уровня доверия к информации идентичности, а также поддержки и совершенствования коммерческих приложений и приложений безопасности, включающих услуги на основе идентичности.

Требования, представленные в настоящей Рекомендации, предназначены для СПП (т. е. управляемой сети с коммутацией пакетов), определение которых содержится в Рекомендации МСЭ-Т Y.2001.

Задачи и требования в настоящей Рекомендации основаны на структуре IdM, представленной в Рекомендации МСЭ-Т Y.2720, и на анализе примеров случаев применения, относящихся к СПП. Эти примеры случаев применения являются информативными и описаны в Дополнениях к настоящей Рекомендации.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т Y.2721	16.09.2010 г.	13-я

Ключевые слова

Федеративная идентичность, управление определением идентичности, сеть последующих поколений, безопасность.

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

© ITU 2012

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		2
3	Определения		2
	3.1	Термины, определенные в других Рекомендациях МСЭ	2
	3.2	Термины, определенные в настоящей Рекомендации	5
4	Сокращения и акронимы		5
5	Условные обозначения		7
6	Обзор IdM		7
	6.1	Общие сведения	7
	6.2	Взаимосвязи IdM	8
	6.3	Факторы развития и мотивации	11
	6.4	Несколько поставщиков услуг и федеративная среда	11
	6.5	Поставщик услуг определения идентичности (IdSP)	11
	6.6	IdM в контексте архитектуры и эталонных моделей СПП	12
7	Задачи IdM		13
8	Требования к IdM		14
	8.1	Общие требования	14
	8.2	Требования к управлению жизненным циклом идентичности	15
	8.3	Функции OAM&P по управлению определением идентичности	17
	8.4	Функции сигнализации и управления	18
	8.5	Управления определением идентичности – функции федеративной идентичности	21
	8.6	Функции пользователя/абонента и защита PII	22
	8.7	Безопасность	23
Дополнение I − Общие случаи использования IdM			25
	I.1	Введение	25
	I.2	Государственные органы	25
	I.3	Коммерческие предприятия	25
	I.4	Конечные пользователи/абоненты	26
Дополнение II − Сценарии использования IdM для приложений СПП			27
	II.1	Введение	27
	II.2	Пример базового случая использования	27
	II.3	Использование общей системы IdM для поддержки нескольких прикладных услуг (например передачи голоса, данных, IPTV) в пределах сетей поставщика услуг	28
	II.4	Единая регистрация в системе/единый выход из системы для нескольких прикладных услуг (например, передача голоса, данных, IPTV) в пределах сети поставщика услуг	32

Стр.

II.5 Корреляция распределенной информации идентичности для гарантии обеспечения многофакторной аутентификации 36

II.6 Обеспечение контроля пользователем информации, позволяющей установить личность (например, предпочтения), в доменах одноранговой сети/поставщика услуг 38

II.7 Сопряжение/преобразование между неоднородными системами IdM 40

II.8 Поддержка конвергированных услуг (например, фиксированный и подвижный доступа) в пределах сети поставщика услуг 41

II.9 Пример случая использования – Аутентификация и авторизация пользователем поставщика СПП (взаимная аутентификация и авторизация).. 42

II.10 Пример случая использования – Утверждение однорангового пользователя (безналичные транзакции) 43

II.11 Случай использования IdM – Обеспечение идентичности и целостности устройства конечного пользователя 44

Дополнение III − Случаи использования IdM, относящиеся к службе электросвязи в чрезвычайных ситуациях (ETS) 48

III.1 Введение 48

III.2 Гарантия обеспечения аутентификации с использованием сочетания устройства и пользователя 48

III.3 Улучшенная аутентификация пользователей ETS для приоритетных услуг последующих поколений (приоритетных мультимедийных услуг) 50

III.4 Аутентификация вызываемой стороны и источников передачи данных 53

III.5 Доверенная идентификация и аутентификация поставщиков услуг в условиях с несколькими поставщиками 56

III.6 Однократная регистрация и однократный выход 59

Дополнение IV − Случаи использования, относящиеся к подвижной службе..... 63

IV.1 Введение 63

IV.2 Примеры случаев использования 63

Дополнение V − Пример моделей транзакций IdM 66

V.1 Введение 66

V.2 Примеры возможных моделей транзакций управления определением идентичности..... 66

Дополнение VI − Иллюстративный пример сценария развертывания для IdM в СПП..... 69

VI.1 Введение 69

VI.2 Развертывание архитектуры IdM 69

Библиография 71

Рекомендация МСЭ-T Y.2721

Требования к управлению определением идентичности СПП и случаи применения

1 Сфера применения

В настоящей Рекомендации представлены задачи, требования, руководящие указания и примеры случаев применения управления определением идентичности (IdM) для сетей последующих поколений (СПП) и их интерфейсов. Функции и возможности IdM используются для повышения уровня доверия к информации идентичности, а также поддержки и совершенствования коммерческих приложений и приложений безопасности, включающих услуги на основе идентичности.

В сферу применения настоящей Рекомендации входят задачи, требования, руководящие указания и примеры случаев применения, касающиеся:

- повышения уровня доверия к информации идентичности объекта СПП (например, пользователя, группы, устройства пользователя, поставщика услуг, предприятия, федерации, элемента сети и объекта);
- управления безопасностью рабочего цикла информации идентичности (например, регистрация, валидация, аннулирование) при условии конкретного и информированного согласия пользователя;
- IdM как инструмента коммерческих приложений (например, однократная регистрация в системе и однократный выход из системы для услуг нескольких приложений) и приложений безопасности (например, управление доступом), включая услуги на основе идентичности (например, аутентификация, подтверждение и федеративная идентификация);
- обнаружения и передачи информации о безопасности, касающейся идентичности или идентичностей объекта СПП при условии конкретного и информированного согласия пользователя. Это включает информацию, которая может находиться в пределах СПП и в разных административных доменах и федерациях;
- межсетевого взаимодействия/функциональной совместимости систем и функций IdM в пределах домена поставщика СПП (т. е. в интрасети);
- межсетевого взаимодействия/функциональной совместимости систем и функций IdM в разных доменах поставщика или их федераций при условии конкретного и информированного согласия пользователя, если пользователь является заинтересованной стороной (например, домены поставщиков СПП, поставщиков веб-услуг и поставщиков контента);
- обеспечения выполнения применяемой политики (например, защиты информации, позволяющей установить личность), относящейся к идентичности объекта или информации идентичности;
- безопасности систем, функций, возможностей, данных и каналов связи IdM.

Задачи и требования, представленные в настоящей Рекомендации, предназначены для СПП, т. е. для управляемой сети с коммутацией пакетов, описанной в [ITU-T Y.2001] "Общий обзор СПП".

Задачи и требования настоящей Рекомендации основаны на структуре IdM, представленной в [ITU-T Y.2720], и на анализе примеров случаев применения, описанных в Дополнениях.

ПРИМЕЧАНИЕ 1. – В настоящей Рекомендации использование термина "идентичность" в отношении IdM не отражает его полного значения. В частности, оно не означает получения положительных результатов проверки личности.

ПРИМЕЧАНИЕ 2. – В настоящей Рекомендации "пользователь" может быть физическим лицом, группой, компанией, юридическим лицом или любым иным объектом, который пользуется услугами СПП.

ПРИМЕЧАНИЕ 3. – В настоящей Рекомендации термин "СПП/поставщик услуг определения идентичности (СПП/IdSP)" используется для указания на то, что может это может быть поставщик СПП или третья сторона, которая предоставляют услуги IdM.

2 Справочные документы

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

[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*.

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

[ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности*.

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

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[ITU-T Y.2201] Рекомендация МСЭ-Т Y.2201 (2009 г.), *Требования к СПП МСЭ-Т и возможности этих сетей*.

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

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

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

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 анонимность (anonymity) [ITU-T X.1252]: Ситуация, при которой объект невозможно определить в комплексе объектов.

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

3.1.2 утверждение (assertion) [ITU-T X.1252]: Утверждение, сделанное объектом и не сопровождаемое доказательствами его истинности.

3.1.3 атрибут (attribute) [ITU-T X.1252]: Информация, связанная с объектом, которая определяет какую-либо его характеристику.

3.1.4 аутентификация (authentication) [ITU-T X.1252]: Процесс, используемый для достижения достаточной меры доверия к связи между объектом и представленной идентичностью.

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

3.1.5 гарантия обеспечения аутентификации (authentication assurance) [ITU-T X.1252]: Степень доверия, достигаемого в процессе аутентификации, в отношении того, что партнер по связи является тем объектом, которым, как он утверждает, является, или которым, как ожидается, он является.

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

3.1.6 авторизация (authorization) [ITU-T X.1252]: Предоставление прав и, на основе этих прав, предоставление доступа.

3.1.7 связь (binding) [ITU-T X.1252]: Явно установленная взаимосвязь, соединение или привязка.

3.1.8 заявление (claim) [ITU-T X.1252]: Высказывание, что дело обстоит таким образом, без возможности представить доказательства.

3.1.9 лицо, предъявляющее требование (claimant) [ITU-T X.1252]: Объект, который является администратором доступа или представляет его для целей аутентификации.

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

3.1.10 контекст (context) [ITU-T X.1252]: Среда с определенными граничными условиями, в которой существуют и взаимодействуют объекты.

3.1.11 полномочия (credential) [ITU-T X.1252]: Набор данных, представленных в качестве доказательств заявленной идентичности и/или прав.

3.1.12 делегирование (delegation) [ITU-T X.1252]: Действие по передаче полномочий, ответственности или функций другому объекту.

3.1.13 обнаружение (discovery) [ITU-T Y.2720]: Действие по установлению местоположения машиночитаемого описания относящегося к сети ресурса, который мог быть ранее неизвестен и который отвечает определенным функциональным критериям. Обнаружение включает сопоставление набора функциональных и иных критериев с набором описаний ресурса. Цель обнаружения состоит в отыскании надлежащего ресурса, относящегося к данной услуге.

3.1.14 объект (entity) [ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в контексте.

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

3.1.15 электросвязь в чрезвычайных ситуациях (emergency telecommunications) (ET) [ITU-T Y.2205]: ET означает любую службу, связанную с чрезвычайными ситуациями, для которой требуется специальный режим со стороны СПП по сравнению с другими службами. К таким службам относятся уполномоченные правительством службы экстренной помощи и службы общественной безопасности.

3.1.16 служба электросвязи в чрезвычайных ситуациях (emergency telecommunications service) (ETS) [ITU-T E.107]: Национальная служба, предоставляющая приоритетную электросвязь уполномоченным пользователям ETS в период бедствий и чрезвычайных ситуаций.

3.1.17 федерация (federation) [ITU-T X.1252]: Ассоциация пользователей, поставщиков услуг и поставщиков услуг определения идентичности.

3.1.18 федеративная идентичность (federated identity) [ITU-T Y.2720]: Идентичность, которая может использоваться для доступа к группе услуг или приложений, для которых обязательными являются политика и условия федерации.

3.1.19 идентификатор (identifier) [ITU-T X.1252]: Один или несколько атрибутов, используемых для идентификации объекта в каком-либо контексте.

ПРИМЕЧАНИЕ. – В контексте СПП, согласно определению в [b-ITU-T Y.2091], идентификатор представляет собой серию цифр, букв и символов или данных в любой другой форме, используемую 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).

3.1.20 идентичность (identity) [ITU-T X.1252]: Представление какого-либо объекта в виде одного или нескольких атрибутов, которые позволяют распознать объект или объекты в каком-либо контексте в той мере, в какой это необходимо. Для целей управления определением идентичности (IdM) термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

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

3.1.21 гарантия идентичности (identity assurance) [ITU-T X.1252]: Степень доверия к процессу валидации и верификации идентичности, используемому для установления идентичности объекта, которому были предоставлены полномочия, и степень доверия в отношении того, что объект, который использует полномочия, является данным объектом или объектом, которому полномочия были предоставлены или переданы.

3.1.22 управление определением идентичности (identity management) [ITU-T Y.2720]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, корреляция и связь, обеспечение реализации политики, аутентификация и утверждения), используемых для:

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

3.1.23 схема идентичности (identity pattern) [ITU-T X.1252]: Структурированное выражение атрибутов объекта (например, поведение объекта), которое может применяться в некоторых процессах идентификации.

3.1.24 поставщик данных идентичности (identity provider): См. "поставщик услуг определения идентичности (IdSP)".

ПРИМЕЧАНИЕ. – Термин "поставщик данных идентичности (IdP)" используется в [ITU-T Y.2720] и спецификациях других организаций. Однако во избежание неверного толкования этого термина, как обозначающего объект, предоставляющий данные идентичности, а не объект, управляющий данными идентичности, в настоящей Рекомендации используется термин "поставщик услуг определения идентичности (IdSP)".

3.1.25 поставщик услуг определения идентичности (identity service provider) [ITU-T X.1252]: Объект, который выполняет верификацию, поддерживает информацию идентичности других объектов, управляет ею и может ее создавать и назначать.

3.1.26 сеть последующих поколений (next generation network) [ITU-T Y.2001]: Сеть с коммутацией пакетов, пригодная для предоставления услуг электросвязи и для использования нескольких широкополосных технологий транспортирования с включенной функцией QoS, в которой связанные с обслуживанием функции не зависят от лежащих в основе технологий, обеспечивающих транспортирование. Сеть обеспечивает беспрепятственный доступ пользователей к сетям и конкурирующим поставщикам услуг и/или выбираемым пользователями услугам. Сеть поддерживает универсальную мобильность, которая обеспечивает постоянное и повсеместное предоставление услуг пользователям.

3.1.27 информация, позволяющая установить личность (personally identifiable information) (PII) [ITU-T X.1252]: Любая информация, a) которая идентифицирует или может использоваться для идентификации, установления контакта с лицом или местоположения лица, к которому такая информация относится; b) на основе которой может быть осуществлена идентификация или получение контактной информации частного лица; или c) которая прямо или косвенно связана либо может быть связана с физическим лицом.

3.1.28 присутствие (presence) [ITU-T Y.2720]: Набор атрибутов, характеризующий объект по отношению к его текущему статусу.

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

3.1.30 неприкосновенность частной жизни (privacy) [ITU-T X.1252]: Право частных лиц осуществлять контроль или воздействие в отношении того, какая относящаяся к ним информация личного характера подлежит сбору, управлению, хранению, доступу, использованию или распространению.

3.1.31 полагающаяся сторона (relying party) (RP) [ITU-T X.1252]: Объект, который полагается на представленную или заявленную идентичность запрашивающего/заявляющего объекта в каком-либо контексте запроса.

3.1.32 домен безопасности (security domain) [ITU-T X.1252]: Совокупность элементов, политика безопасности, орган безопасности и совокупность действий по обеспечению безопасности, в которых управление элементами осуществляется в соответствии с политикой безопасности.

3.1.33 доверие (trust) [ITU-T X.1252]: Твердая уверенность в надежности и истинности информации или в возможности или расположенность объекта действовать надлежащим образом в конкретном контексте.

3.1.34 пользователь (user) [ITU-T X.1252]: Любой объект, использующий ресурс, например система, оборудование, терминал, процесс, приложение или корпоративная сеть.

ПРИМЕЧАНИЕ. – В контексте СПП в соответствии с [b-ITU-T Y.2091] сюда относится конечный пользователь, физическое лицо, абонент, система, оборудование, терминал (например, факс, ПК), (функциональный) объект, процесс, приложение, поставщик и корпоративная сеть.

3.1.35 верификатор (verifier) [ITU-T X.1252]: Объект, который выполняет верификацию и валидацию информации идентичности.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения:

3G	3rd Generation	3-е поколение
AKA	Authentication and Key Agreement	Аутентификация и соглашение о ключе
ANI	Application-to-Network Interface	Интерфейс приложение-сеть
API	Application Programming Interface	Интерфейс прикладного программирования
BSS	Business Support System	Система поддержки деятельности предприятия
CSP	Communications Service Provider	Поставщик услуг связи
DDoS	Distributed Denial of Service	Распределенная атака типа отказ в обслуживании
DeviceID	Device Identity	Идентификатор устройства
DoS	Denial of Service	Отказ в обслуживании
EAG	External Application Gateway	Шлюз внешнего приложения
EDS	Enterprise Directory Service	Служба телефонного справочника предприятия
ET	Emergency Telecommunications	Электросвязь в чрезвычайных ситуациях
ETS	Emergency Telecommunications Service	Служба электросвязи в чрезвычайных ситуациях
EV-DO	Evolution Data Optimized	Эволюция с оптимизацией данных
FE	Functional Entity	Функциональный объект
FTTX	Fiber-To-The-X	Волоконная линия до *x*
GBA	Generic Bootstrapping Architecture	Общая архитектура начальной загрузки
HSS	Home Subscriber Server	Сервер абонентов
IBGC-FE	Interconnection Border Gateway Control Functional Entity	Функциональный объект управления пограничным шлюзом присоединения
IdM	Identity Management	Управление определением идентичности

IdMCC-FE	IdM Coordination and Control Functional Entity		Функциональный объект управления и координации IdM
IdSP	Identity Service Provider		Поставщик услуг определения идентичности
IDPS	Intrusion Detection and Prevention Systems		Системы определения и предотвращения вторжения
ID-WSF	Identity Web Services Framework		Структура веб-услуг идентичности
IMS	IP Multimedia Subsystem		Мультимедийная IP-подсистема
IP	Internet Protocol		Протокол Интернет
IPTV	IP Television		IP телевидение
ISC	IMS Service Control		Управление службой IMS
IT	Information Technology		Информационная технология
KDC	Key Distribution Center		Центр распределения ключей
LS	Location Server		Сервер местоположения
LTE	Long Term Evolution		Долгосрочное развитие
MNO	Mobile Network Operator		Оператор подвижной сети
MSISDN	Mobile Subscriber Integrated Service Director Number		Международный номер абонента подвижной связи в сети ISDN
NACF	Network Attachment Control Functions		Функция управления присоединением сети
NGN	Next Generation Network	СПП	Сеть последующих поколений
NNI	Network-to-Network Interface		Интерфейс сеть-сеть
OAM&P	Operation, Administration, Maintenance and Provisioning		Эксплуатация, управление, техническое обслуживание и обеспечение
OSS	Operations Support System		Система эксплуатационной поддержки
PC	Personal Computer	ПК	Персональный компьютер
P-CSC-FE	Proxy Call Session Control Functional Entity		Функциональный объект управления вызовом сеанса с прокси-элементом
PDA	Personal Digital Assistant	КПК	Карманный персональный компьютер
PII	Personally Identifiable Information		Информация, позволяющая установить личность
POTS	Plain Old Telephone System		Традиционная аналоговая телефонная служба
PS	Presence Server		Сервер присутствия
PSTN	Public Switched Telephone Network	КТСОП	Коммутируемая телефонная сеть общего пользования
QoS	Quality of Service		Качество обслуживания
RACF	Resource and Admission Control Functions		Функция управления ресурсами и допуском
RFID	Radio-Frequency Identification		Радиочастотная идентификация
RP	Relying Party		Полагающаяся сторона
SAA-FE	Service Authentication and Authorization Functional Entity		Функциональный объект аутентификации и авторизации услуги
SAML	Security Assertion Markup Language		Язык разметки, предусматривающий защиту данных
S-CSC-FE	Serving Call Session Control Functional Entity		Функциональный объект управления сеансом обслуживающего вызова
SIM	Subscriber Identity Module		Модуль идентификации абонента
SIP	Session Initiation Protocol		Протокол инициирования сеанса связи
SLA	Service Level Agreement		Соглашение об уровне обслуживания
SN	Service Node		Узел предоставления услуг
SNI	Server-to-Network Interface		Интерфейс сервер-сеть

SP	Service Provider	Поставщик услуг
SUP-FE	Service User Profile Functional Entity	Функциональный объект профиля пользователя услуги
TGS	Ticket Granting Server	Сервер предоставления мандата
UE	User Equipment	Оборудование пользователя
UICC	Universal Integrated Circuit Card	Универсальная смарт-карта
UNI	User-to-Network Interface	Интерфейс пользователь-сеть
URI	Uniform Resource Identifier	Универсальный идентификатор ресурса
UserID	User Identity	Идентичность пользователя
VoD	Video on Demand	Видео по запросу
VoIP	Voice over Internet Protocol	Передача голоса по протоколу IP
WiFi	Wireless Fidelity	Беспроводная точность
WiMAX	Worldwide Interoperability for Microwave Access	Всемирная функциональная совместимость для микроволнового доступа
WLAN	Wireless Local Area Network	Беспроводная локальная сеть
WS	Web Server	Веб-сервер
WSG	Web Services Gateway	Шлюз веб-служб
xDSL	x Digital Subscriber Loop	Цифровая абонентская линия типа *x*

5 Условные обозначения

В настоящей Рекомендации:

Ключевые слова "**требуется, чтобы**" обозначают требование, которое должно строго соблюдаться, и от которого не допускается отклонений, если должно быть заявлено соответствие настоящей Рекомендации.

Ключевые слова "**рекомендуется**" обозначают требование, которое рекомендовано, но не обязательно требуется. Поэтому, для заявления о соответствии это требование не обязательно.

Ключевые слова "**запрещено, чтобы**" обозначают требование, которое должно строго соблюдаться, и от которого не допускается отклонений, если должно быть заявлено соответствие настоящей Рекомендации.

Ключевые слова "**дополнительно можно**" обозначают дополнительное требование, которое допускается, не предполагая никакого оттенка рекомендации. Этот термин не предназначен для утверждения, что реализация поставщика должна обеспечивать возможность, и данная функция может дополнительно предоставляться оператором сети/поставщиком услуг. Наоборот, это значит, что поставщик может дополнительно обеспечивать эту функцию и тем не менее заявлять о соответствии техническим условиям.

В тексте настоящей Рекомендации и его приложениях иногда встречаются слова *должен*, *не должен*, *следует* и *может*, в этом случае их следует понимать как *требуется*, *чтобы*, *запрещено*, *чтобы*, *рекомендуется* и *дополнительно можно*, соответственно. Появление таких фраз или ключевых слов в дополнении или материалах, однозначно помеченных, как *информативные*, должно пониматься, как не несущее нормативного смысла.

6 Обзор IdM

6.1 Общие сведения

В [ITU-T Y.2720] представлена структура IdM. Функции и возможности используются для повышения уровня доверия к информации идентичности объекта и поддержки коммерческих приложений и приложений безопасности (например, управление доступом и авторизация), включая услуги на основе идентичности. Объектом считается что-либо, что является отдельной и выраженной сущностью и может идентифицировано в каком-либо контексте. В контексте IdM примерами объектов являются абоненты, пользователи, элементы сети, сети, программные приложения, услуги и устройства.

СПП будет поддерживать широкий спектр прикладных услуг для конечных абонентов, правительственных органов и коммерческих предприятий. Для обеспечения защиты целостности и безопасности прикладных услуг рекомендуется, чтобы СПП поддерживала необходимые функции и возможности для гарантирования идентичности и данных идентичности, связанных с объектом на основе определенного контекста. Определение IdM см. в [ITU-T X.1252].

Примеры случаев использования, описанные в нижеследующих Дополнениях, принимались во внимание при определении требований к IdM:

- Дополнение I – Общие случаи использования IdM.
- Дополнение II – Случаи использования IdM для приложений СПП.
- Дополнение III – Случаи использования IdM, относящиеся к службе электросвязи в чрезвычайных ситуациях (ETS).
- Дополнение IV – Случаи использования, относящиеся к службе подвижной связи.

Кроме того, при определении требований к IdM во внимание принимались следующие факторы, связанные с идентичностью конечного пользователя в среде СПП:

- конечные пользователи все чаще используют несколько идентичностей;
- идентичность может быть связана с разными контекстами и привилегиями в обслуживании;
- идентичность может идентифицировать конечного пользователя только частично;
- в качестве идентичности могут использоваться псевдонимы;
- идентичности можно использовать в любом месте, в любое время и с любого устройства;
- может не обеспечиваться функциональная совместимость идентичности между разными поставщиками СПП.

6.2 Взаимосвязи IdM

На рисунке 1 представлен общий обзор взаимосвязей IdM на основе структуры из [ITU-T Y.2720].

Рисунок 1 – Взаимосвязи IdM

Объектами могут быть как отдельные физические лица – пользователи, так и организации в широком смысле, например коммерческие предприятия и виртуальные объекты, такие как электронные приложения. Информация идентичности, относящаяся к каждому из них, может отличаться по критичности – от данных, находящихся в относительно свободном доступе, например телефонных номеров, включенных в общедоступный справочник, до конфиденциальных данных идентичности, например паролей, цифровых сертификатов и других данных аутентификации личности.

Объект может иметь одну или более идентичностей. Идентичности могут использоваться для представления различных ролей (например, гражданин, супруг, родитель, потребитель и пациент), а также конкретных транзакций от коммерческой до общественной деятельности. Физическое лицо или индивидуум в разных ситуациях может ассоциироваться с несколькими цифровыми идентичностями, как показано на рисунке 1. Кроме того, физическое лицо, действующее посредством цифровых идентичностей, может быть известно другим лицам как одно или более лицо, предполагаемое или показывающееся публично или в обществе, или посредством ролей (например, отвечающая сторона в чрезвычайных ситуациях), которые присвоены или даны определенным органом.

На рисунке 1 показано следующее:

а) Объекты

В среде СПП, где услуги основаны на контексте и ролях, и доступ к ним осуществляется в любом месте, в любое время и с любого устройства, с объектом может быть связана информация различного типа, относящаяся к идентичности. Кроме того, объект может иметь одну или более идентичностей, в зависимости от контекста. К примерам объектов относятся:

- пользователи и абоненты;
- устройства пользователя, элементы и объекты сети;
- организации, группы, коммерческие предприятия и государственные предприятия;

- поставщики сети и услуг;
- виртуальные объекты.

b) Информация идентичности

Информация идентичности, связанная с объектом, может быть классифицирована следующим образом:

- идентификаторы (например, счет абонента, адреса элементов сети, идентификатор поставщика услуг);
- атрибуты (например, адреса электронной почты, номера телефонов, URI и IP-адреса, роли, заявления, привилегии, метод аутентификации, модели поведения и местоположение);
- полномочия (например, цифровые сертификаты и жетоны).

c) Функции и возможности IdM

Функции и возможности IdM используются для повышения уровня доверия к информации идентичности, а также поддержки и совершенствования коммерческих приложений и приложений безопасности, например управление доступом и авторизацией, включая услуги на основе идентичности. К примерам функций и возможностей IdM относятся:

- управление жизненным циклом идентичности;
- организация, корреляция и связь информации идентичности;
- аутентификация, гарантия обеспечения и утверждение аутентификации;
- обнаружение информации идентичности и обмен ею;
- функции и возможности для сопряжения разных систем IdM в целях обеспечения функциональной совместимости.

d) Коммерческие приложения и приложения безопасности

Функции и возможности IdM поддерживают и расширяют коммерческие приложения и приложения безопасности, включая услуги на основе идентичности.

К примерам коммерческих приложений относятся:

- федеративные услуги (например, доступ к услугам в среде разных федераций или поставщиков СПП);
- единая регистрация в системе и однократный выход из системы, например доступ к нескольким приложениям и услугам без необходимости повторного предоставления каждому приложению или платформе услуг полномочий для аутентификации.

К примерам приложений безопасности относятся:

- управление доступом;
- управление авторизацией привилегий;
- защита информации, позволяющей установить личность (PII).

К примерам услуг на основе идентичности относятся:

- услуги, связанные с идентификатором, полномочиями и атрибутами;
- услуги связывания (отображение и совместное использование информации идентичности в разнотипных средах);
- услуги, связанные с информацией о модели поведения.

IdM включает процессы управления жизненным циклом, плюс функции и возможности для обнаружения и получения источников идентичности, которые можно использовать для верификации и валидации идентичности. Услуги и возможности IdM позволяют объектам управлять использованием и распространением информации своей идентичности. IdM обеспечивает объекты (например, полагающиеся стороны) необходимой информацией для принятия решений об аутентификации и уверенности в соответствующих передачах и сеансах связи. IdM также позволяет членам федерации (например, разным поставщикам СПП, коммерческим предприятиям или государственным предприятиям) совместно использовать федеративную информацию идентичности для обеспечения федеративных услуг. Например, услуги федеративной идентичности позволят прошедшим авторизацию объектам из числа членов федерации получать доступ к ресурсам на основе ролей и привилегий в соответствии с правилами и политикой федерации без необходимости регистрации и аутентификации каждого члена федерации.

6.3 Факторы развития и мотивации

Так как многие услуги и возможности СПП включают услуги на основе идентичности абонента, его предпочтений и доступа с любого устройства, в любом месте и в любое время, решения IdM должны обладать возможностью соответствовать растущему числу комплексных взаимодействий в режиме реального времени, так как пользователи перемещаются между устройствами, технологиями доступа, методами оплаты и даже идентичностями. Кроме того, конечным пользователям также требуются простые или удобные в обращении возможности. Еще более важно то, что конечным пользователям требуются возможности для управления защитой частной жизни и информации, позволяющей установить личность (PII).

Факторы развития и мотивации для IdM определяются конечными пользователями (например, абонентами приложений и услуг, поставщиками СПП), коммерческими и государственными предприятиями, и все они хотели бы, чтобы в реализациях IdM учитывались их интересы и потребности. При определении требований к IdM для СПП во внимание принимались следующие факторы:

- конечным пользователям/абонентам требуется управлять своей информацией идентичности и защищать ее, они хотят иметь гибкие и универсальные методы доступа к ресурсам, и им нужно соблюдать баланс между преимуществами работы в социальных сетях и раскрытием личной информации;
- поставщикам СПП (поставщикам сети и услуг) требуется защищать свои ресурсы инфраструктуры сети, услуги и приложения, обеспечивать возможность федеративных услуг, содействовать распространению широко доступных услуг на основе контрактов и отвечать потребностям конечных пользователей в отношении неприкосновенности частной жизни и защиты информации, позволяющей установить личность (PII);
- коммерческим предприятиям необходимо защищать свои коммерческие интересы, быть уверенными в возможностях аутентификации для коммерческих транзакций и защищать данные идентичности партнеров;
- защита инфраструктуры сети от кибератак и защита частных данных;
- государственные организации поддерживают услуги электронного правительства, службы общественной безопасности, службы раннего предупреждения, службы электросвязи в чрезвычайных ситуациях (ETS) и другие национальные службы.

6.4 Несколько поставщиков услуг и федеративная среда

В условиях наличия нескольких поставщиков услуг и федеративной среды услуги и возможности IdM используются для обнаружения и передачи информации, необходимой для формирования доверия к идентичности(ям) объекта. Например, идентификаторы, полномочия и атрибуты, связанные с идентичностью, могут быть верифицированы поставщиком услуг определения идентичности, который рассматривается как доверенный полагающейся стороной, и переданы, при помощи утверждений, этой полагающейся стороне (например, пользователю, поставщику услуг) для обеспечения аутентификации, которая может служить основой управления доступом, принятия коммерческих решений и обязательного применения соответствующей политики (например, защита частной жизни и защита информации, позволяющей установить личность.

Дополнительно могут существовать различные и независимые решения IdM, приводящие к необходимости функциональной совместимости между поставщиками услуг.

6.5 Поставщик услуг определения идентичности (IdSP)

В настоящей Рекомендации не налагается никаких ограничений в отношении того, кто представляет услуги поставщика услуг определения идентичности (IdSP).

IdSP является объектом, который поддерживает информацию идентичности других объектов (пользователей/абонентов, организаций и устройств), управляет этой информацией и может создавать такую информацию, а также предлагает услуги на основе идентичности, базируясь на отношениях доверия, коммерческих отношениях и отношениях иного типа.

В условиях наличия нескольких поставщиков услуг, возможно, что поставщик СПП будет также и IdSP и будет предлагать услуги управления определением идентичности (например, услуги на основе идентичности) другим поставщикам.

В настоящей Рекомендации термин "СПП/IdSP" используется для указания на то, что услуги IdM может предоставлять поставщик СПП или третья сторона.

6.6 IdM в контексте архитектуры и эталонных моделей СПП

6.6.1 Взаимосвязь с функциональной архитектурой СПП

В контексте эталонной модели архитектуры СПП, определенной в [ITU-T Y.2012], возможно, что с вязанные с IdM функции будут располагаться в разных плоскостях (например, пользователя, управления и контроля) и разных стратах распределенной архитектуры (например, в страте обслуживания и страте транспортирования). В аспекте реализации или внедрения, поддержка услуг и возможностей IdM может включать использование существующих сетевых элементов, или она может включать использование дополнительных сетевых элементов в СПП (например, специализированные серверы приложений).

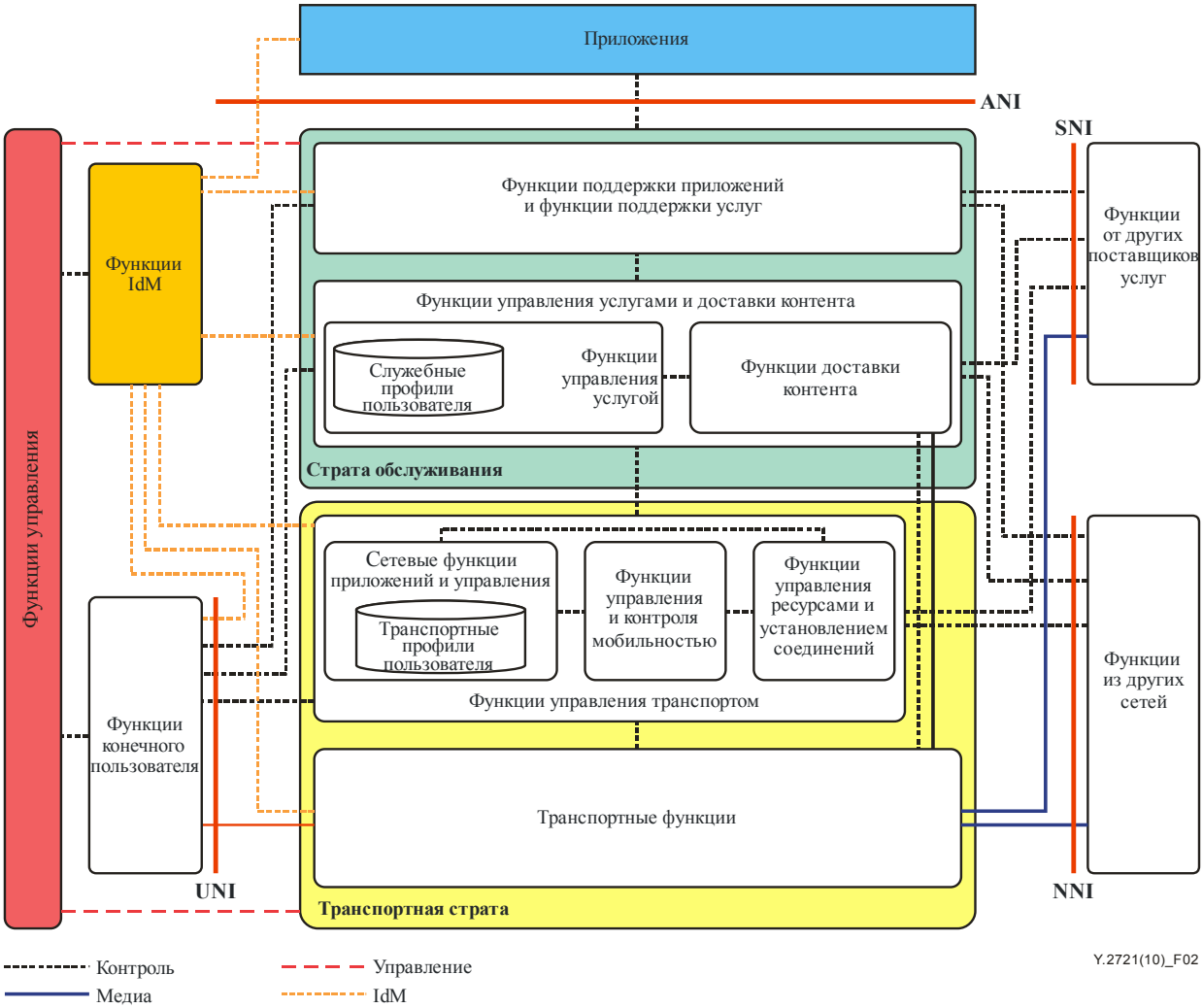


Рисунок 2 – Общее представление архитектуры СПП

Основу рисунка 2 составляет рисунок 7-1 в [ITU-T Y.2012], который включает функциональный блок, представляющий функцию IdM в функциональной архитектуре СПП. На рисунке 7-1 из [ITU-T Y.2012] отражены общие концепции того, что поддержка услуг и возможностей IdM может включать взаимодействие с определенными функциональными объектами (FE), с тем чтобы обеспечить и поддержать использование услуг, включая услуги идентичности. В зависимости от определенных поддерживаемых услуг или возможностей IdM и проектного решения, это может включать взаимодействие с FE в следующих функциональных блоках:

– приложений;

– страте обслуживания: функции поддержки приложений и функции поддержки услуг, функции управления услугами и функции доставки контента;

– страте транспортирования: функции управления транспортированием и функции транспортирования;

– функций конечного пользователя;

– функций управления.

В функциональной архитектуре СПП функции IdM могут находиться в разных плоскостях (например, пользователя, контроля и управления) и разных стратах распределенной архитектуры (например, страте обслуживания и страте транспортирования). Хотя функции IdM показаны как автономная группа функций, это не означает применения в отношении IdM каких-либо проектных решений или ограничений. Реализация функций IdM определяется соответствием применяемой политике, например национальным и региональным регламентам и законодательствам по защите данных идентичности (например, PII). В частности, реализация и использование функций IdM должны соответствовать применяемой политике в отношении базовых принципов защиты информации:

- связь данных с определенной целью;
- невозможность совместного использования данных приложениями, предназначенными для разных целей;
- ограничение состава данных минимальным набором, необходимым для конкретной цели;
- право частных лиц на контроль в отношении своей PII.

ПРИМЕЧАНИЕ. – В ряде конкретных национальных регламентах это может означать реализацию отдельных функций IdM в разных стратах СПП.

6.6.2 Внешние интерфейсы и линии связи IdM

Для обмена данными идентичности между разными административными доменами и федерациями используются стандартные интерфейсы, определенные в [ITU-T Y.2012]. Они могут соответствующим образом включать следующие интерфейсы:

- интерфейс пользователь-сеть (UNI);
- интерфейс сеть-сеть (NNI);
- интерфейс приложение-сеть (ANI);
- интерфейс сервер-сеть (SNI).

Решения интерфейсов будут зависеть от таких факторов, как потребности определенного приложения и услуг (например, режим реального времени и режим, близкий к реальному времени), решений протокола (например, SAML, Radius, SIP), а также механизмов и подходов.

Пример сценария реализации IdM, показывающего как могут применяться внешние интерфейсы СПП, приведен в Дополнении VI.

6.6.3 Модели транзакций

В [b-ITU-T X.1250] представлено описание примера моделей транзакций с участием многих сторон, (например, пользователей, IdSP и полагающихся сторон). Краткая информация о моделях транзакций, описанных в [b-ITU-T X.1250], содержится в Дополнении V.

7 Задачи IdM

Далее приведены общие задачи IdM:

1) Способствует принятию решений о доверии между объектами.

2) Поддерживает решение(я) IdM, снижая воздействие на пользователей/абонентов.

3) Решение(я), использующее(и)е новые возможности, должно(ы) обеспечить соответствующее решение для перехода.

4) Поддержка функционально совместимых решений IdM в пределах домена поставщика СПП. Например, функциональная совместимость между продуктами разных поставщиков, поддерживающих несколько прикладных услуг (например, VoIP, IPTV, видео и данные).

5) Поддержка функционально совместимых решений IdM в пределах доменов и федераций разных поставщиков СПП и поставщиков услуг на основе коммерческих соглашений и взаимоотношений, а также при применении нормативов и политики защиты PII.

6) Поддержка сопряжения разнородных систем и федераций IdM. Например, возможность обеспечивать сопряжение между системами IdM поставщика СПП и другими типами систем IdM (например, веб-услугами, контентом и системами IdM поставщика третьей стороны) на основе коммерческих соглашений и взаимоотношений, а также при применении нормативов и политики защиты PII.

7) Конечные пользователи/абоненты должны иметь возможность взаимодействовать и использовать прикладные услуги простым и интуитивным образом, сохраняя при этом контроль над своими личными данными в течение всего их жизненного цикла. Это касается и того, как, когда и кем используется эта информация.

8) Конечные пользователи/абоненты должны иметь возможность раскрыть только минимально необходимую информацию для установления взаимного доверия и проведения транзакций на основе применимой политики.

9) Конечные пользователи/абоненты должны иметь возможность проверить аутентичность объекта, запрашивающего данные идентичности и PII. Важно, чтобы конечный пользователь/абонент мог использовать разные идентификаторы в зависимости от контекста.

10) Конечные пользователи/абоненты должны иметь возможность действовать анонимно, под псевдонимом или под известным в международном масштабе именем на основе контекста приложения и применяемой политики.

8 Требования к IdM

В данном разделе описываются требования IdM, применимые к СПП, в соответствии с высокоуровневыми требованиями СПП, описанными в [ITU-T Y.2201].

8.1 Общие требования

Далее приведены общие требования для управления определением идентичности:

R-1 Требуется, чтобы СПП/IdSP поддерживали функции и возможности для управления определением идентичности разных типов объектов, поддерживаемых СПП, включая:

a) пользователей/группы;

b) организации/федерации/предприятия/поставщиков услуг;

c) устройства/элементы сети/системы;

d) объекты (например, прикладной процесс, контент, данные).

R-2 Требуется, чтобы СПП/IdSP поддерживали:

a) управление безопасностью жизненного цикла идентичности (например, от выдачи до аннулирования);

b) безопасное обнаружение и обмен информацией идентичности. Это включает обнаружение и обмен информацией идентичности, которая может находиться в СПП и в разных административных доменах.

R-3 Требуется, чтобы СПП/IdSP обязательно поддерживали выполнение применимой политики, связанной с идентичностью объекта или информацией идентичности.

R-4 Требуется, чтобы СПП/IdSP поддерживали функции и возможности IdM как для приложений в реальном времени (например, VoIP и IPTV), так и для приложений в режиме, близком к реальному времени (например, передача данных на основе веб-технологий).

R-5 Требуется, чтобы СПП/IdSP поддерживали функции и возможности IdM, позволяющие анонимное утверждение в отношении информации идентичности (например, идентичность и атрибуты), относящиеся к применимой политике.

R-6 Требуется, чтобы СПП/IdSP поддерживали безопасное взаимодействие IdM с элементами сети в пределах домена поставщика СПП (т. е. интрасети) и с доменами разных поставщиков (например, другого поставщика СПП, поставщика веб-услуг).

R-7 Требуется, чтобы СПП/IdSP поддерживали простые в использовании услуги и функции конечных пользователей, например:

a) единая регистрация в системе/единый выход из системы для нескольких прикладных услуг;

b) конвергентные услуги (например, конвергенцию фиксированной и подвижной связи);

c) управление информацией, позволяющей установить личность (PII), и защита этой информации.

R-8 Требуется, чтобы СПП/IdSP поддерживали однократную регистрацию в системе/единый выход из системы при использовании полномочий, связанных с устройством абонента (например, полномочия UICC), или полномочий, связанных с пользователем/абонентом (например, дайджест полномочия SIP), в зависимости от случая, на основе требований к безопасности данного приложения. В частности:

- Должна быть обеспечена возможность использования полномочий абонента (например, дайджест-полномочий SIP) для поддержки однократной регистрации в системе для приложений, доступ к которым осуществляется через мобильные устройства.
- Должна быть обеспечена возможность использования полномочий абонента (например, дайджест-полномочий SIP) для поддержки однократной регистрации в системе для приложений, доступ к которым осуществляется через фиксированные устройства.

8.2 Требования к управлению жизненным циклом идентичности

Управление жизненным циклом идентичности включает процессы и процедуры, связанные с регистрацией и выдачей информации идентичности (например, идентификаторов, полномочий и атрибутов).

R-9 Требуется, чтобы СПП/IdSP устанавливали и обеспечивали выполнение политики управления жизненным циклом идентичности. Это включает процессы, процедуры и правила проверки, регистрации, выдачи и аннулирования идентичности.

8.2.1 Регистрация и выдача

Регистрация объекта (например, абонента, устройства, организации, поставщика или объекта СПП) в каком-либо контексте начинается с процесса проверки и регистрации идентичности или полномочий. Регистрация является процессом введения объекта в какой-либо контекст и включает запись идентичности объекта и, возможно, присвоение конкретных атрибутов (например, идентификаторов) или же полномочий либо ролей. В случае, когда абоненты – конечные пользователи, это процесс, где заявитель пытается стать абонентом IdSP или поставщика СПП.

Проверка включает верификацию и валидацию атрибутов и, возможно, связанных полномочий.

R-10 Требуется, чтобы СПП/IdSP осуществляли верификацию и валидацию идентичности в процессе регистрации в соответствии с требованиями данного контекста. Запись идентичности объекта и присвоение идентификаторов, полномочий и атрибутов для конкретного контекста обусловливаются успешным подтверждением применимых критериев и политики проверки.

Процесс правила проверки должны основываться на значениях ресурсов (например, услуг, передач, информации и привилегий), разрешенных данной идентичностью, и рисков, связанных с получением и использованием этой идентичности несанкционированным объектом. В частности, для обеспечения этого необходимы следующие меры:

- Объект (например, физическое лицо, организация или юридическое лицо) с заявленными атрибутами существует, и эти атрибуты позволяют распознать объект в данном контексте в той мере, в какой это необходимо.
- Заявитель, чья идентичность записывается, на самом деле является объектом, с которым связана эта идентичность.
- Для объекта, который использовал записанную идентичность и полномочия, сложно позднее отказаться от регистрации/записи и поставить под сомнение аутентификацию.

Успешное завершение процесса записи и проверки приводит к записи идентичности, которая может включать присвоенные атрибуты и/или полномочия, с помощью которых данный объект может быть аутентифицирован в будущем.

R-11 Требуется, чтобы информация идентичности (например, идентификаторы, полномочия и атрибуты), связанные с идентичностью, выдавались только после успешной проверки идентичности объекта.

В некоторых сценариях это может включать запись и выдачу электронных полномочий, например цифровых сертификатов и жетонов, привязанных к идентичности или составляющих заявление (т. е. атрибут) об идентичности. В зависимости от типа используемого жетона СПП/IdSP либо создаст новый жетон для абонента и предоставит его абоненту, либо потребует, чтобы заявитель зарегистрировал жетон, которым он уже обладает, или заново его создал.

R-12 В любом случае требуется, чтобы механизм транспортирования жетона из точки его создания в другую часть был безопасен, с тем чтобы гарантировать конфиденциальность и целостность вновь созданного жетона.

8.2.2 Поддержание и обновление

После регистрации и выдачи идентичности(ей), включая любую информацию идентичности (идентификатор, регистрационные данные и атрибуты), и СПП/IdSP и абонент обязаны обеспечить безопасное хранение идентичности в течение этапа эксплуатации и использования.

R-13 Требуется, чтобы СПП/IdSP надежно осуществляли безопасное управление связанными с этой идентичностью данными и статусом данных (например, идентификаторами, полномочиями, атрибутами) и их поддержание.

R-14 Требуется, чтобы СПП/IdSP надежно управляли любыми обновлениями или изменениями в идентичности и вели журнал их регистрации.

R-15 Требуется, чтобы СПП/IdSP осуществляли периодическую валидацию статуса идентичности.

R-16 Требуется, чтобы СПП/IdSP поддерживали процедуры оповещения об обновлениях или изменениях в идентичности или любых данных, относящихся к идентичности, систем или элементов сети, которые должны быть осведомлены об этом.

R-17 Требуется, чтобы СПП/IdSP обеспечивали функции информирования пользователя о данных его идентичности, их изменении или удалении.

Абонент также несет ответственность за безопасность присвоенных полномочий, базирующихся на коммерческих соглашениях и соглашениях о политике с СПП/IdSP. Например, абонент несет ответственность за управление его/ее электронными полномочиями (например, жетонами) и их безопасное хранение.

R-18 Требуется, чтобы СПП/IdSP принимали меры на основе коммерческих и контрактных соглашений, обеспечивающие, что объект (например, абонент или иной СПП/IdSP) безопасно управляет и использует выданные полномочия (например, цифровые сертификаты или жетоны), связанные с идентичностью, при условии соблюдения применимых регламентов и политики.

8.2.3 Аннулирование

Аннулирование идентичности является процессом отмены идентичности и связанных с ней полномочий. Сторона или система (например, СПП/IdSP), которая управляет идентичностью или полномочиями, отвечает за их прекращение или вывод из эксплуатации. Аннулирование необходимо для предотвращения продолжения использования идентичности или полномочий, которые более недействительны или имеют нарушения безопасности.

R-19 Требуется, чтобы СПП/IdSP создавали политику аннулирования идентичности(ей) и контролировали осуществление этой политики. В частности, будут поддерживаться возможности прекращения или уничтожения полномочий (например, цифровых сертификатов или жетонов), связанных с идентичностью(ями), которая(ые) уже недействительна(ы) или имеет(ют) нарушения безопасности.

R-20 Требуется, чтобы СПП/IdSP поддерживали процедуры оповещения объекта и систем или элементов сети, которые должны быть предупреждены, об аннулировании или прекращении идентичности(ей) или любых данных, связанных с идентичностью(ями) (т. е. должны быть предупреждены все системы и процессы, для доступа к которым могла использоваться идентичность, что эта идентичность уже недействительна).

8.3 Функции OAM&P по управлению определением идентичности

8.3.1 Модель и схема данных

Каждый поставщик СПП, федерация или предприятие могут иметь собственные форматы, схемы, определения или семантику для представления и совместного использования данных и информации, относящихся к идентичности. В п. 8.2.1 [ITU-T Y.2720] описывается необходимость взаимодействия между разнородными системами IdM, использующими разные модели, структуры и схемы данных.

R-21 Требуется, чтобы СПП/IdSP поддерживали функции и возможности, разрешающие при необходимости функциональную совместимость разнородных систем IdM, использующих разные модели, структуры и схемы данных.

8.3.2 Управление данными идентичности

В п. 8.2 [ITU-T Y.2720] описывается необходимость управления данными идентичности (например, управление идентификаторами, полномочиями и атрибутами). Подробные требования в отношении управления данными идентичности не входят в сферу применения настоящей Рекомендации.

В СПП разные данные идентичности (например, такие идентификаторы, как адреса электронной почты, номера телефонов, URI и IP адреса) могут управляться разными системами управления и эксплуатационными процессами (например, системой эксплуатационной поддержки (OSS)/системой поддержки бизнеса (BSS)). Следующие общие требования представлены в контексте обеспечения структурированного и скоординированного подхода к взаимодействиям между разными системами управления и системами сервисной службы для поддержки услуг и возможностей IdM.

R-22 Требуется, чтобы СПП/IdSP поддерживали стандартный интерфейс (например, портал потребителя), позволяя конечным пользователям/абонентам взаимодействовать с применимыми системами и процессами управления СПП для поддержки передачи управления данными идентичности конечных пользователей/абонентов (например, изменений и обновлений) при условии соблюдения применимых регламентов и политики защиты данных.

R-23 Требуется, чтобы СПП/IdSP поддерживали необходимые интерфейсы, функции и возможности для облегчения согласованных передач и потоков рабочих данных между разными системами и процессами управления, связанными с управлением данными идентичности (например, изменения и обновления, которые должны передаваться в разных OSS/BSS, системы сервисной поддержки и платформы прикладных услуг), в зависимости от случая, при условии соблюдения применимых регламентов и политики защиты данных.

R-24 Требуется, чтобы СПП/IdSP поддерживали функции и возможности ведения журнала регистрации и хранения записей о транзакциях, связанных с управлением данными идентичности (например, данных резервного копирования) при условии соблюдения применимых регламентов и политики защиты данных.

R-25 Требуется, чтобы СПП/IdSP поддерживали функции и возможности синхронизации изменения и обновления данных идентичности между разными системами и процессами, в зависимости от случая, управления при условии соблюдения применимых регламентов и политики защиты данных.

R-26 Требуется, чтобы СПП/IdSP поддерживали функции и возможности верификации связей между данными идентичности, относящимися к объекту (например, абоненту), и услугами по контракту (например, доступ, передача голоса, данных, видео) при условии соблюдения применимых регламентов и политики защиты данных.

8.4 Функции сигнализации и управления

8.4.1 Обнаружение информации идентичности

В среде распределенных СПП информация идентичности может существовать в разных элементах сети (например, сервере контрактов, сервере местонахождения, сервере присутствия, сервере домашних контрактов и т. п). Приложениям, использующим информацию идентичности, необходимо знать, что она существует, и где ее найти.

R-27 Требуется, чтобы СПП/IdSP поддерживали функции и возможности обнаружения источников информации идентичности в домене СПП/IdSP. Например, функции и возможности сервера управления определением идентичности в целях обнаружения существования информации идентичности в других элементах сети, таких как серверы местонахождения, присутствия или контрактов, или для приложения/услуги в целях обнаружения данных управления определением идентичности или других серверов, на которых содержатся данные идентичности.

R-28 Требуется, чтобы СПП/IdSP поддерживали функции и возможности при помощи стандартных интерфейсов и протоколов для обнаружения источников информации идентичности в разных доменах СПП/IdSP. Например, использование стандартных интерфейсов и протоколов для обнаружения источников информации идентичности в другом домене СПП/IdSP основывается на применимых соглашениях о межсетевом взаимодействии.

R-29 Требуется, чтобы СПП/IdSP поддерживали возможности защиты и механизмов и возможностей обнаружения.

8.4.2 Управление доступом к информации идентичности

К данным идентичности должны иметь доступ только объекты, имеющие авторизацию для доступа к информации.

R-30 Требуется, чтобы информация идентичности была доступна только авторизованным объектам, при условии соблюдения применимых регламентов и политики. В частности,

- Требуется, чтобы СПП/IdSP осуществляли аутентификацию объекта (например, полагающейся стороны), запрашивающего данные идентичности, или взаимную аутентификацию.
- Требуется, чтобы СПП/IdSP осуществляли аутентификацию объекта (например, полагающейся или запрашивающей стороны), запрашивающего данные идентичности, а также верификацию и валидацию его авторизации, прежде чем предоставить доступ к информации или выполнить обмен запрашиваемыми данными идентичности.

8.4.3 Линии связи IdM

Необходимо, чтобы системы и элементы сети создавали сеансы связи для обмена информацией идентичности (например, идентификаторами, полномочиями и атрибутами), расположенной в разных системах сети (например, сервере управления определением идентичности, сервере контрактов, сервере местоположения, сервере присутствия и т. д.), которые могут быть взаимосвязаны и верифицированы (т. е. сервером приложений IdM, обеспечивающим функции аутентификации и корреляции) для предоставления возможностей гарантии обеспечения идентичности,.

СПП/IdSP может передавать полагающимся сторонам утверждения идентичности и соответствующие атрибуты (например, заявления и привилегии) для принятия решений по управлению доступом. Это позволит разным прикладным услугам (т. е. платформам разных поставщиков) использовать общую доступную услугу IdM в отличие от независимых и автономных решений. К рассматриваемым взаимосвязям связи относятся:

- внутрисетевые: линии связи с доменом поставщика СПП (например, между сетевыми элементами);
- межсетевые: линии связи между двумя разными поставщиками СПП;
- федерация: линии связи между членами федерации.

8.4.3.1 Линии связи в режиме реального времени и режиме, близком к реальному времени

Решение, используемое для обнаружения и обмена информацией идентичности, должно учитывать, требуется ли связь в реальном времени или в режиме, близком к реальному времени. Это будет определяться конкретным поддерживаемым приложением. Для некоторых приложений (например, VoIP и IPTV) может требоваться валидация идентичности запрашивающего пользователя/абонента и авторизация для прикладной услуги. Для других приложений (например, услуги передачи данных и сообщений) могут требоваться только сеансы связи в режиме, близком к реальному времени, для валидации идентичности запрашивающего пользователя/абонента и авторизации для прикладных услуг.

R-31 Требуется, чтобы СПП/IdSP поддерживали возможности создания сеансов связи в соответствии с требованиями определенной прикладной услуги для обмена информацией в режиме реального или близком к реальному времени. Это включает сеансы связи для обмена информацией идентичности в домене поставщика СПП, между двумя разными поставщиками СПП и между членами федерации.

Информация об атрибутах может ограничиваться, но это не требуется, статусом членства, присоединенными функциями (выставление счетов, эксплуатация), атрибутами, используемыми другими услугами (например, справочная служба или служба сертификатов). Это позволяет полагающейся стороне предоставлять пользователям индивидуализированную информацию и контент в соответствии с их атрибутами.

R-32 Для СПП/IdSP и полагающейся стороны должна существовать возможность обмена утверждениями, связанными с идентичностью. Это включает утверждение атрибута.

8.4.4 Корреляция и связь

Информация идентичности (например, идентификаторы, полномочия и атрибуты) может быть коррелированы для установления связи, с тем чтобы гарантировать идентичность объекта. Например, информация идентичности, связанная с абонентом (например, идентификатор пользователя (UserID)), устройством абонента (например, идентификатор устройства (DeviceID)) и другая соответствующая информация (например, данные о местоположении и модели поведения), могут быть коррелированы для установления связи, с тем чтобы обеспечить более высокую степень гарантирования идентичности абонента (т. е. уверенности в действительности идентичности).

R-33 Требуется, чтобы СПП/IdSP поддерживали возможности корреляции нескольких частей данных, связанных с идентичностью (например, местоположение и модель поведения), и создание соответствующей связи с идентичностью объекта, при условии соблюдения применимых регламентов и политики. Использование этих возможностей требует конкретного и информированного согласия пользователя.

ПРИМЕЧАНИЕ. – В некоторых национальных регламентах и политике защиты данных возможно ограничение обеспечения этого требования.

8.4.5 Требования к аутентификации

Аутентификация – это процесс достижения доверия к связи между идентичностью и объектом. Одним из способов получения гарантии аутентификации является описание задач и руководящих указаний, необходимых для количественно измерения рисков того, что объект является тем, кто или что соответствует его заявлению. Это включает определение того, какие идентификаторы объекта более важны в процессе идентификации, и почему определенные идентификаторы, используемые в аутентификации, должны иметь то же значение аутентификации.

Требования к аутентификации СПП см. в [ITU-T Y.2702].

Ниже приведены требования безопасности для аспектов аутентификации IdM:

R-34 Должна быть возможной взаимная аутентификация между объектами (например, пользователем, СПП/IdSP, полагающейся стороной).

R-35 Полагающаяся сторона должна иметь возможность направлять СПП/IdSP запросы на аутентификацию объекта (например, пользователя/абонента).

R-36 СПП/IdSP должны иметь возможность поддержки аутентификации объекта (например, пользователя/абонента) и предоставления утверждений полагающейся стороне.

R-37 Полагающаяся сторона должна иметь возможность запрашивать повторную аутентификацию объекта, определяя требуемый существующий или альтернативный метод повторной аутентификации.

8.4.6 Гарантия обеспечения аутентификации

Гарантия обеспечения аутентификации – это степень доверия, достигаемого в процессе аутентификации, в отношении того, что партнер по связи является тем объектом, которым, как он утверждает, является, или которым, как ожидается, он является. Доверие основано на степени доверия к связи между взаимодействующим объектом и представленной информацией идентичности. Объекты (например, пользователи, прикладные услуги и т. д.) могут иметь разные потребности в гарантии обеспечения аутентификации, что обусловливается контекстом. Существуют случаи, которые требуют разной жесткости аутентификации для доступа к разным ресурсам в зависимости от предполагаемой чувствительности и значимости информации и транзакций. В таких случаях полагающимся сторонам (например, пользователям, СПП/IdSP) потребуется больше деталей (например, данных о методе аутентификации, числе факторов аутентификации, контекстах аутентификации и т. д.), чем обычно, с тем чтобы предоставить ожидаемые гарантии обеспечения аутентификации. Это включает оценку возможных рисков, связанных с последствиями ошибок аутентификации или определение соответствующего уровня обеспечения идентичности объекта. Ошибки аутентификации с возможно наихудшими последствиями потребуют более высоких уровней проверки.

R-38 Требуется, чтобы СПП/IdSP поддерживали соответствующие методы аутентификации в зависимости от необходимого уровня гарантии.

R-39 Полагающаяся сторона должна иметь возможность указывать СПП/IdSP необходимый уровень гарантии для аутентификации объекта.

R-40 Следует иметь возможность согласования уровня гарантии между СПП/IdSP, полагающейся стороной и объектом, проходящим аутентификацию.

8.4.6.1 Гарантии идентичности и целостности устройства пользователя

СПП будут поддерживать разнообразные устройства пользователя (например, фиксированные телефоны, беспроводные устройства, персональные компьютеры, карманные персональные компьютеры (КПК), телевизионные приставки IPTV). Компоненты оборудования и программного обеспечения устройств, связанных с СПП, могут быть и очень простыми, и очень сложными, и если они будут похищены и вскрыты, их могут использовать для проведения разных атак. Признается, что СПП также необходимо поддерживать устройств (таких, как "немой" терминал или устройства POTS), которые не смогут обеспечить необходимый уровень защиты.

R-41 СПП/IdSP должны иметь возможность поддерживать устройства конечного пользователя, в которых – в устойчивых к взлому компонентах аппаратного оборудования – включены функции безопасности и зашифрованные данные управления определением идентичности (например, пароли, цифровые ключи и сертификаты).

R-42 СПП/IdSP должны иметь возможность установления связи с функциями безопасности в устойчивых к взлому компонентах аппаратного оборудования устройств конечного пользователя при помощи стандартизованных интерфейсов для поддержки прикладных услуг безопасности, полагающихся на специализированный устойчивый к взлому компонент аппаратного оборудования, выступающего как "точка доверия" для осуществления уникальной идентификации и гарантии идентичности устройства конечного пользователя.

Приложения, используемые устройствами абонента, для того чтобы абонент мог взаимодействовать с услугами и функциями локального устройства, могут потенциально подвергать риску целостность устройств. Популярные интернет-приложения (например, веб-браузеры и электронная почта) могут вносить уязвимости, изменяющие целостность устройств пользователя. Загрузка программных средств и файлов, особенно из ненадежного источника, делает абонента уязвимым для вредоносных кодов, червей, вирусов и троянских программ. Для верификации целостности устройства, вероятно, возможно разработать и внедрить специализированные компоненты аппаратного оборудования, устойчивые к взлому. Например, специализированный компонент аппаратного оборудования, устойчивый к взлому, может содержать определенные алгоритмы и функции производителя для проверки нарушения идентичности. Такой специализированый компонент аппаратного оборудования может включать эталонную модель с набором заведомо правильных метрик целостности, определенным образом идентифицирующих правильный код и дающих эталонные значения для устройств. Заведомо правильные метрики целостности могут использоваться для сравнения фактических представленных значений с конфигурацией и определения соответствия аппаратного устройства.

R-43 СПП/IdSP должны иметь возможность поддержки устройств конечных пользователей со специализированными компонентами аппаратного оборудования, устойчивыми к взлому, с тем чтобы проводить проверку целостности и подтверждать соответствие целостности устройства приложениям и услугам.

R-44 СПП/IdSP должны иметь возможность установления связи с функциями безопасности в устойчивом к взлому компоненте оборудования устройств конечного пользователя при помощи стандартизованных интерфейсов для поддержки прикладных услуг безопасности, полагающихся на проверки целостности и подтверждение соответствия целостности устройства.

Потеря или кража устройства с PII и другими конфиденциальными данными может привести к серьезным последствиям для частных лиц, коммерческих и государственных предприятий. Специализированные компоненты оборудования, предназначенные для уникальной идентификации и подтверждения целостности доверенных устройств, могут потенциально поддерживать возможности шифрования и защиты PII и других чувствительных данных на устройствах конечного пользователя.

R-45 СПП/IdSP должны иметь возможность поддерживать устройства конечного пользователя со специализированными компонентами аппаратного оборудования, устойчивыми к взлому, для шифрования и защиты PII и других чувствительных данных в устройствах конечного пользователя.

8.4.7 Поддержка услуг, требующих реализации приоритета

Системы и возможности IdM СПП должны поддерживать прикладные услуги и сеансы связи, требующие реализации приоритета относительно других услуг. В [ITU-T Y.2205] описывается электросвязь в чрезвычайных ситуациях (ET) как требующая особого режима со стороны СПП. Конкретным примером является служба электросвязи в чрезвычайных ситуациях (ETS), определенная в [ITU-T E.107]. ETS использует возможности IdM, применяемые для обычных услуг (например, обеспечение определения идентичности и обнаружение доверенных идентичностей). Поэтому система IdM должна поддерживать необходимые функции и возможности для определения и предоставления приоритета при установлении и поддержании вызова/сеанса ETS на основе применимых национальных правил и политики. Информацию об услугах и возможностях, требующих реализации приоритета, см. в [ITU-T E.107] и [ITU-T Y.2205].

R-46 Требуется, чтобы системы СПП/IdSP IdM поддерживали функции и возможности определения и предоставления приоритета при установлении и поддержании вызова/сеанса ETS на основе применимых национальных правил и политики.

R-47 Требуется, чтобы элементы и базы данных сети IdM, используемые для поддержки вызовов/сеансов ETS обеспечивали предоставление приоритета на основе применимых национальных правил и политики. Это включает в том числе:

- внутрисетевые линии связи IdM (например, взаимодействие в системе IdM поставщика СПП);
- межсетевые линии связи IdM (например, взаимодействие между системами двух поставщиков СПП на основе двусторонних соглашений и политики);
- федеративные линии связи IdM (например, взаимодействие между членами федерации на основе применимых правил и политик федеративной идентификации).

Примеры случаев использования ETS приводятся в Дополнении III.

8.5 Управления определением идентичности – функции федеративной идентичности

Федерация включает установление взаимосвязи между двумя или более объектами или установление ассоциации, объединяющей любое число поставщиков услуг и поставщиков услуг определения идентичности. Общей концепцией федерации является предоставление каждому члену федерации возможности оставаться независимым, вместе с тем упрощая совместное использование определенной информации идентичности, с тем чтобы сделать возможными федеративные услуги. Например, определенная информация идентичности пользователя/абонента (например, поднабор профиля абонента) может быть федеративной (т. е. доступной для членов федерации), т. е. для нее обязательными являются политика и условия федерации и регламенты и политика защиты данных. Федеративная идентификация позволяет обеспечивать переносимость и передачу информации идентичности через домены безопасности, которые в ином случае были бы автономными и для которых обязательными являются политика и условия федерации, при условии соблюдения применимых правил, регламентов и политики. Федеративная идентификация позволяет пользователям одного домена иметь безопасный доступ к данным или системам другого домена без необходимости полного резервирования процесса административного управления пользователями.

R-48 Необходимо иметь возможность обнаруживать и обмениваться федеративной информацией идентичности между членами федерации при условии соблюдения применимых правил, регламентов и политики.

R-49 Требуется, чтобы СПП/IdSP поддерживали возможности, позволяющие абоненту обеспечить необходимую авторизацию для федеративного объединения своих идентичностей.

R-50 Требуется, чтобы СПП/IdSP поддерживали возможности, позволяющие абоненту прервать участие во всех или определенных услугах и приложениях федеративной идентичности и завершить действие федерации своих идентичностей.

R-51 Требуется, чтобы СПП/IdSP поддерживали возможности, позволяющие абоненту устанавливать разрешения и запреты в отношении информации своей федеративной идентичности. Абонент должен обладать возможностью контролировать то, какие личные данные выдаются, кому они выдаются и для каких целей.

ПРИМЕЧАНИЕ. – Требования относительно защиты PII, изложенные в п. 8.6, также применимы к федеративным идентичностям.

Как правило, каждый поставщик СПП, предприятие или член федерации может иметь свои собственные форматы, схемы, определения или семантику для представления и совместного использования данных и информации, относящихся к идентичности. Например, та же информация, такая как дата рождения, может по-разному представляться двумя разными системами. Кроме того, семантика, схемы, технологии и механизмы, используемые для представления относящейся к идентичности информации, ее запроса и обмена ею, могут по-разному обусловить проблемы функциональной совместимости. Поэтому необходимы будут соответствующие возможности, позволяющие сопряжение и функциональную совместимость доверенных федераций.

R-52 Должна иметься возможность сопряжения и функциональной совместимости доверенных федераций, использующими разные системы IdM, семантику, схемы, механизмы и технологии. Например, полагающиеся стороны в разных доменах (например, домене СПП и веб-услуг/интернета) должны иметь возможность взаимодействия функциональной совместимости, используя разные возможности и технологии IdM. В частности, должна гарантироваться безопасная передача информации федеративной идентичности.

8.6 Функции пользователя/абонента и защита PII

Конечных пользователей/абонентов необходимо обеспечивать применимыми установленными интерфейсами и возможностями для контроля своей PII и принятия информированного решения и согласия относительно своих личных данных. Конечные пользователи/абоненты должны иметь возможность выражать свою политику и предпочтения, связанные с неприкосновенностью частной жизни, и согласовывать с СПП/IdSP условия раскрытия данных.

Личные данные должны раскрываться только авторизованным объектам на основе применимой политики (например, согласия пользователя/абонента, государственных регуляторных правил). Кроме того, должен быть минимизирован объем собираемой, хранимой и используемой PII и осуществляться применимая политика.

R-53 Требуется, чтобы СПП/IdSP обеспечивали защиту услуг IdM и конфиденциальности PII в соответствии с применимыми регламентами, политикой и правилами.

R-54 Конечные пользователи/абоненты должны иметь возможность передавать СПП/IdSP свои предпочтения, касающиеся личных данных (например, устанавливать предпочтения в отношении защиты частной жизни) в соответствии с применимыми регламентами и политикой (например, выраженное согласие физических лиц, политика поставщиков или регуляторные правила).

R-55 Требуется, чтобы конечные пользователи/абоненты имели возможность верифицировать аутентичность запрашивающего PII объекта до предоставления запрошенной информации.

R-56 Требуется, чтобы СПП/IdSP удаляли PII после достижения конкретных задач сбора и хранения данных на основе применимых регламентов, политики и правил.

R-57 Конечные пользователи/абоненты должны иметь возможность действовать анонимно или под псевдонимом на основе контекста приложения и применимых регламентов, политики и правил.

8.7 Безопасность

Данные и информация идентичности являются конфиденциальными данными и за ними охотятся взломщики. Кроме того, поскольку услуги и возможности IdM будут использоваться для управления доступом к коммерческим, государственным сетевым приложениям и приложениям социальных сетей, элементы и системы сети (например, элементы и базы данных сети, поддерживающие функции и возможности IdM) будут целью атак и вторжений, нарушающих безопасность. Поэтому для обеспечения безопасности и защиты элементов и систем сети, предоставляющих функции, услуги и возможности IdM, должны быть реализованы соответствующие меры безопасности.

8.7.1 Управление доступом к системам и данным

Управление доступом к системам включает меры безопасности по предотвращению несанкционированного доступа к элементам и системам сети и точкам доступа к ним. Существуют угрозы, связанные с несанкционированным доступом к элементам и системам сети, поддерживающим функции, возможности и данные IdM. Поэтому должны быть установлены надлежащие меры управления доступом для предотвращения несанкционированного доступа, и обеспечено их неукоснительное выполнение.

R-58 Требуется, чтобы СПП/IdSP поддерживали и обеспечивали обязательное выполнение мер управления доступом к системе для предотвращения несанкционированного доступа к элементам и системам сети, поддерживающим функции и возможности IdM. СПП/IdSP не должны позволять объекту получать доступ к элементам и базам данных сети, поддерживающим функции и возможности IdM, если объект не прошел идентификацию, аутентификацию и авторизацию. Это относится ко всем объектам (т. е. лицам, процессам и удаленным системам).

Управление доступом к данным включает меры безопасности для предотвращения несанкционированного доступа к хранящимся или предоставленным данным и данным в процессе передачи. Существуют угрозы, связанные с несанкционированным доступом к предоставленным или хранящимся данным, связанным с IdM. Поэтому должны быть установлены надлежащие меры управления доступом для предотвращения несанкционированного доступа, и обеспечено их неукоснительное выполнение.

R-59 Требуется, чтобы СПП/IdSP поддерживали и обеспечивали обязательное выполнение мер управления доступом для предотвращения несанкционированного доступа к данным IdM. К ним относятся любые данные идентичности, хранящиеся или представленные в базах данных IdM, на серверах приложений, серверах абонентов (HSS) или в любых других элементах сети. СПП/IdSP не должны позволять объекту получать доступ к к данным IdM, если объект не прошел идентификацию, аутентификацию и авторизацию. Это применимо ко всем объектам (т. е. лицам, процессам и удаленным системам).

8.7.2 Целостность данных и систем

Должна обеспечиваться защита целостности элементов, систем и функций сети, поддерживающих услуги и возможности IdM. Это относится к базам данных IdM и серверам приложений.

R-60 Требуется, чтобы СПП/IdSP обеспечивали защиту целостности всех элементов, систем и функций сети, поддерживающих услуги и возможности IdM.

Для предотвращения любого повреждения или манипуляций с данными, влияющих на их целостность, должна обеспечиваться защита целостности хранимых данных и информации идентичности.

R-61 Требуется, чтобы СПП/IdSP обеспечивали защиту целостности предоставленных данных IdSM.

R-62 Требуется, чтобы СПП/IdSP обеспечивали защиту целостности всех данных при их распространении, передаче, обновлении или изменении, а также любых офлайновых данных, связанных с IdM.

8.7.3 Конфиденциальность данных

R-63 Требуется, чтобы СПП/IdSP поддерживали и обеспечивали обязательное выполнение мер защиты предоставленных данных IdM от доступа не прошедших авторизацию объектов (например, не прошедших авторизацию сотрудников).

R-64 Требуется, чтобы СПП/IdSP поддерживали и обеспечивали обязательное выполнение мер защиты данных IdM при их распространении, передаче, обновлении или изменении, а также любых офлайновых данных, связанных с IdM, от доступа не прошедших авторизацию объектов (например, не прошедших авторизацию сотрудников).

8.7.4 Защита безопасности линий связи IdM

Линии связи IdM (линии сигнализации и среда передачи) должны быть защищены от несанкционированного доступа, повреждения, манипуляций и перехвата (например, подслушивания).

R-65 Требуется, чтобы СПП/IdSP обеспечивали защиту целостности и конфиденциальности линий связи IdM внутри сетей и между сетями. Весь трафик сигнализации и информационный трафик, связанный с IdM и проходящий через интерфейс сеть-сеть (NNI), интерфейс приложение-сеть (ANI) или интерфейс сервер-сеть (SNI) между доменами сети, должен быть обеспечен защитой целостности.

8.7.5 Безопасность управления

Управление доступом к элементами и конфигурируемым данным СПП должно быть безопасным и защищенным от несанкционированного доступа и управления.

R-66 Требуется, чтобы СПП/IdSP предотвращали несанкционированный доступ к интерфейсам управления и управлению элементами и функциональным объектам сети, поддерживающим IdM.

Трафик управления должен быть безопасным и защищенным от повреждения, манипуляций и несанкционированного наблюдения.

R-67 Требуется, чтобы СПП/IdSP обеспечивали защиту целостности и конфиденциальности трафика управления, связанного с обеспечением IdM.

8.7.6 Журнал безопасности и проверки

Необходимо иметь журнал безопасности и проверки, куда должны заноситься события в целях содействия расследованию после совершения определенных действий.

R-68 Требуется, чтобы в СПП/IdSP велись журналы безопасности для целей регистрации событий, служащие для обеспечения расследований после совершения определенных действий, связанных с поддержкой IdM (например, регистрация в системе, изменения критически важных системных ресурсов и данных, управление доступом к конфигурируемым параметрам и ресурсам СПП).

8.7.7 Защита от атак типа отказ в обслуживании (DoS) и распределенных DoS (DDoS) атак

Услуги и возможности IdM должны характеризоваться высокой готовностью и потому должны быть защищены от угроз атак типа DoS и DDoS, потенциально затрагивающих готовность.

R-69 Требуется, чтобы СПП/IdSP обеспечивали защиту от DoS, DDoS и других типов атак, влияющих на готовность услуг и возможностей IdM. Это включает поддержку и использование возможностей и инструментов, в зависимости от случая, для обнаружения, изолирования и смягчения последствий атак DoS, DDoS и других типов атак.

8.7.8 Наблюдение и обнаружение вторжения

R-70 Требуется, чтобы СПП/IdSP поддерживали и использовали инструменты контроля безопасности и определения вторжений, в зависимости от случая, для обнаружения мошенничества, злонамеренного использования и вторжения в элементах и системах сети IdM.

Дополнение I

Общие случаи использования IdM

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Введение

В настоящем Дополнении представлены общие случаи использования IdM, организованные по группам государственных органов, коммерческих предприятий, конечных пользователей/абонентов.

I.2 Государственные органы

Возможности IdM могут использоваться государственными органы для расширения возможностей и поддержки приложений и транзакций между государственными учреждениями и гражданами, между различными государственными организациями (федеративные государственные услуги) и учреждениями, а также между различными государственными органами (например, межучрежденческие федеративные услуги). К примерам случаев использования государственными органами относятся:

- Гарантия идентификации гражданина: IdM может использоваться государственными органами для валидации идентичности граждан при получении электронных услуг государственных органов, улучшая при этом защиту PII. В качестве примера можно привести сферу здравоохранения, где конфиденциальность информации о состоянии здоровья обусловливает важность минимизации объема данных и, в более широком смысле, необходимость безопасности и защиты частной жизни в аспекте информации идентичности.
- Гарантия идентификации государственных служащих при предоставлении федеративных государственных услуг: возможности IdM могут использоваться государственными предприятиями для разработки общих вариантов безопасных и надежных форм идентификации государственных служащих, обеспечивая при этом более высокий уровень безопасности, эффективности, снижение мошенничества с использованием идентичности и защиту персональных данных.
- Расширение и поддержка федеративных услуг между различными государственными органами: IdM могут использоваться для расширения и поддержки федеративных услуг между различными государственными органами. Например, государственные органы могут сотрудничать с целью разработки улучшенных решений IdM для граждан, путешествующих по разным странам, решая вопросы безопасности, защиты частной жизни и способов работы пользователей.

I.3 Коммерческие предприятия

IdM может использоваться в помощь коммерческим организациям при расширении и обеспечении новой и существующей коммерческой деятельности, повышая при этом уровень безопасности, защиты частной жизни и PII. К примерам случаев использования коммерческими предприятиями относятся:

- Услуги федеративной идентичности: IdM может использоваться для однократной регистрации в системе и однократного выхода из системы нескольких деловых партнеров (включая поставщиков СПП, веб-услуг, контента и услуг третьей стороны).
- Услуги связи: IdM может использоваться поставщиками СПП для предоставления конечным пользователям/абонентам возможности получать прикладные услуги через различные платформы (например, управляемые IP-сети, интернет и мобильные платформы), а также для предоставления пользователям доступа к выбранным ими приложениям через несколько платформ такими способами, которые отвечают их собственным предпочтениям.
- Электронные финансовые транзакции и приложения: IdM может использоваться для расширения и поддержки приложений, позволяющих осуществлять электронные платежи в транзакциях электронной коммерции.

I.4 Конечные пользователи/абоненты

Для конечных пользователей/абонентов IdM может использоваться для упрощения методов работы и управления PII. К примерам случаев использования конечными пользователями/абонентами относятся:

- Контроль пользователями своей PII: IdM может использоваться для упрощения методов работы пользователя и обеспечения возможности контроля своей PII. Физические лица могут использовать несколько псевдонимов для участия в различных видах деятельности, таких как чтение новостных лент, публикация сообщений в блогах, управление социальными сервисами и обмен фотографиями или музыкой. IdM может способствовать предоставлению физическим лицам более широкого выбора способов участия в различных сообществах и определения желаемой степени увязки аспектов их различных идентичностей (т. е. контроль своей PII).
- Социальные сети: IdM может использоваться для расширения и поддержки приложений социальных сетевых сервисов, предоставляя необходимые инструменты для эффективного контроля пользователями своей PII и подотчетности.

Дополнение II

Сценарии использования IdM для приложений СПП

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

II.1 Введение

В настоящем Дополнении представлены примеры случаев использования управления определением идентичности (IdM) для СПП. Эти примеры использования будут служить в качестве основы для разработки требований к IdM для СПП.

II.2 Пример базового случая использования

На рисунке II.1 представлен пример базового случая использования, включающий три основных элемента. Кроме этого базового примера существуют другие возможные сценарии. В Дополнении V приведены другие возможные сценарии (например, ориентированные на пользователя сценарии).

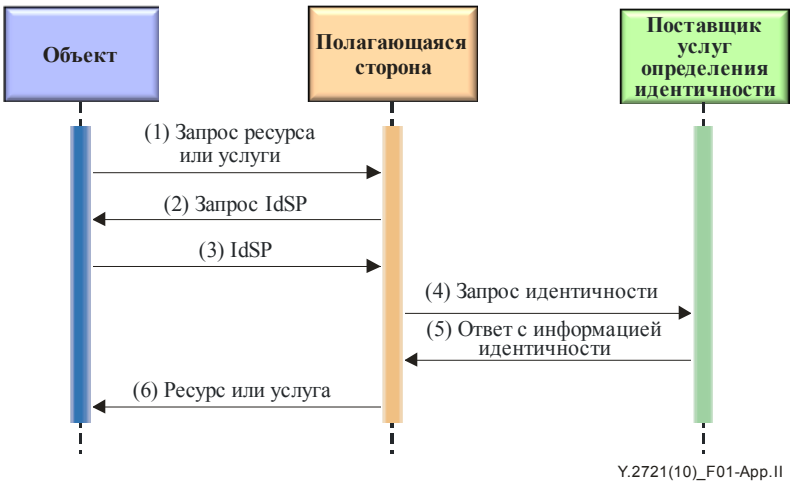


Рисунок II.1 – Пример основного сценария использования

К этим трем элементам относится объект (заявляющая сторона или администратор доступа), которому требуются услуги полагающейся стороны (RP, каковая может быть сетью или приложением), и который получает связанное утверждение идентичности, включая утверждения, сделанные анонимно или под псевдонимом, от поставщика услуг определения идентичности (IdSP) на основе политики доверия и безопасности.

На рисунке II.1 показан следующий информационный поток IdM высокого уровня.

1) Объект предоставляет заявляемую идентичность полагающейся стороне (поставщику ресурса или услуги) и запрашивает ресурс или услугу у полагающейся стороны.

2) Для полагающейся стороны (сеть или приложение) необходимо, чтобы объект был аутентифицирован до предоставления запрашиваемого ресурса или услуги. Для аутентификации полагающейся стороне необходима информация от соответствующего IdSP, который должен быть определен и с ним осуществлено соединение. Полагающаяся сторона возвращает объекту "Запрос информации IdSP", запрашивая объект, предоставить соответствующее имя IdSP.

3) Объект отвечает на этот "Запрос информации для IdSP", указывая полагающейся стороне соответствующего IdSP. Объект может определить несколько IdSP.

4) Полагающаяся сторона в свою очередь запрашивает соответствующего(их) IdSP для валидации заявляемой объектом идентичности с достаточным уровнем доверия (уровень гарантии).

5) IdSP подтверждает заявляемую объектом идентичность. Функции IdSP могут включать делегирование (подразумевается, что этот IdSP могут делегировать некоторые аспекты процесса аутентификации другим IdSP с помощью передачи им утверждения идентичности). В случае необходимости в более высоком уровне гарантии аутентификации или для

обеспечения других, определяемых реализацией, возможностей к поставщику(ам) IdSP могут поступать последующие запросы от полагающейся стороны.

6) Полагающаяся сторона после получения от поставщика(ов) IdSP подтверждения истинности заявляемой объектом идентичности предоставляет требуемый ресурс или услугу.

Возможны комбинации этих трех элементов (объект, полагающаяся сторона и IdSP). Лежащая в основе среда передачи значения не имеет. Единственным требованием является то, чтобы эти механизмы связи были "хорошо структурированы" с синтаксисом и профилями, которые известны или потенциально доступны участвующим сторонам, если они обладают необходимыми разрешениями на использования этих механизмов. Там, где это возможно, следует использовать стандартные механизмы для доверительной, глобальной функциональной совместимости.

Кроме того, возможны другие информационные потоки IdM высокого уровня. Например:

1) RP может запросить полномочия аутентификации непосредственно у объекта.

2) Объект может предоставить свои полномочия аутентификации доверенному IdSP.

3) IdSP может осуществить валидации полномочий, которые поступили от объекта, а затем создать новые полномочия для этого объекта, для того чтобы выполнить запрос аутентификации от RP.

4) Объект (или его представитель) может получить созданные полномочия от IdSP и выдать их RP.

5) Созданные полномочия, отправленные объектом к RP, могут содержать или 1) копию заявляемых данных идентичности, созданных IdSP; или 2) ссылку на них.

Кроме того, объект может принять решение не передавать RP полномочия аутентификации, созданные поставщиком IdSP.

Также возможно существование иерархии поставщиков данных идентичности или иерархии полагающихся сторон. Кроме того, возможно, что объект может иметь несколько представителей.

II.3 Использование общей системы IdM для поддержки нескольких прикладных услуг (например, передачи голоса, данных, IPTV) в пределах сетей поставщика услуг

II.3.1 Обзор

Поставщики сети/услуги (например, поставщики СПП) будут поддерживать и размещать несколько приложений и услуг. Распределенная природа среды СПП позволяет размещать различные прикладные услуги на различных элементах сети и определяемых поставщиком платформах (например, VoIP, передача данных и IPTV). Каждая услуга может иметь свои собственные определяемые поставщиком или технологией средства управления доступом, которые могут не быть совместимыми, и поэтому их конфигурация, управление и использование должны осуществляться раздельно.

Подход, использующий общую инфраструктуру IdM и позволяющий функционировать нескольким приложениям/услугам, может обеспечить эффективность затрат и коммерческую эффективность. Он может также обеспечить стандартный подход, позволяющий разработчикам приложений использовать для IdM общие инструменты, а не создавать для каждого приложения/услуги отдельную функцию IdM (например, определяемые поставщиком возможности и механизмы управления доступом), а также эффективный процесс разработки, реализации и предоставления других прикладных услуг. Кроме того, общий подход может упрощать управление рисками безопасности для каждой прикладной услуги и всей инфраструктуры сети в целом.

Подход IdM для СПП будет включать как внутрисетевые решения (т. е. решения в пределах домена поставщика СПП), так и межсетевые решения (т. е. решения между различными поставщиками СПП, включая поставщиков услуг 3-й стороны). Для внутрисетевого сценария это может включать подходы, позволяющие взаимодействие различных элементов или компонентов сети в пределах домена поставщика СПП (например, лицо, предъявляющее требование, полагающиеся системы и системы идентичности). Для межсетевого сценария это может включать спецификацию подходов, позволяющих взаимодействие объектов элементов сети между доменами разных СПП (например, лицо, предъявляющее требование, полагающиеся стороны и IdSP).

ПРИМЕЧАНИЕ. – Поставщик услуг доступа к СПП также может быть IdSP.

II.3.2 Описание случая использования

Данный пример случая использования показывает, каким образом разные прикладные услуги (например, VoIP, передача данных и IPTV) используют общую инфраструктуру управления определением идентичности для управления доступом и защиты безопасности прикладной услуги. Случай использования включает взаимодействие между следующими объектами:

- конечные пользователи (т. е. конечный пользователь и/или устройство конечного пользователя);
- полагающаяся система (т. е. прикладная услуга или система);
- система IdM (т. е. сетевая система, предоставляющая услуги IdM, такие как регистрация, аутентификация и авторизация, информацию профиля абонента).

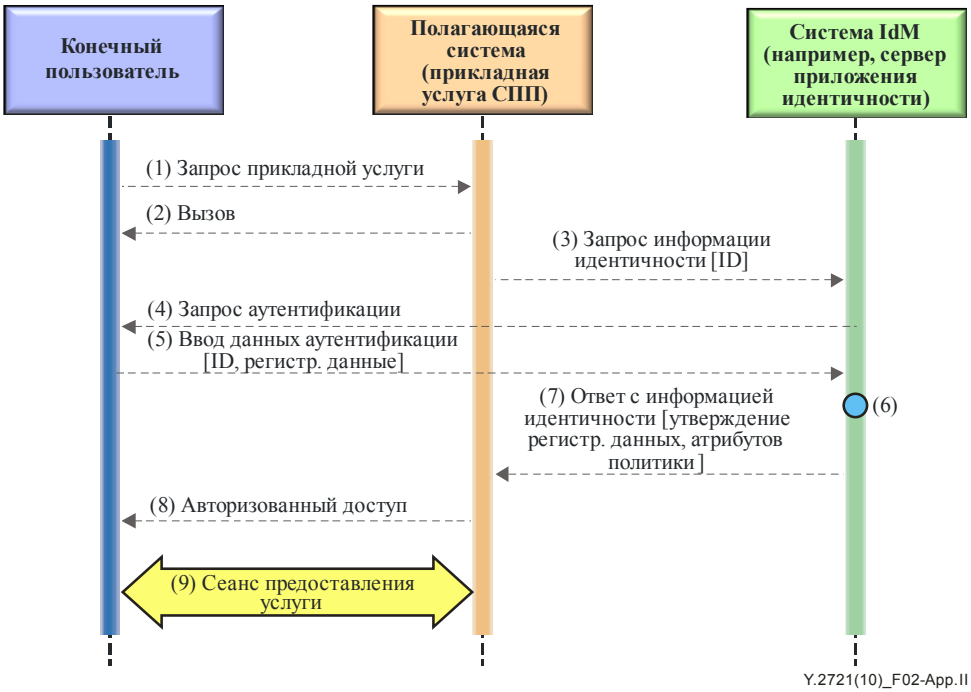


Рисунок II.2 – Пример базового случая использования

На рисунке II.2 представлен базовый пример, где прикладная услуга использует услуги системы IdM, которая является внешней или не зависящей от прикладной услуги в отношении управления доступом и управления привилегиями. Например, существуют следующие потоки вызова:

1) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя на использование прикладной услуги.

2) Требование. Прикладная услуга направляет отклик, требуя доступа для пользователя.

3) Запрос информации идентичности [ID пользователя]. Прикладная услуга направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Это может включать такую информацию как профиль услуги, привилегии, предпочтения и информацию о политике, например, это может быть любая политика или ограничения, связанные с идентичностью.

4) Запрос аутентификации. Система IdM направляет пользователю запрос на получение аутентификации.

5) Ввод данных аутентификации [Полномочия]. Пользователь предоставляет информацию для аутентификации (например, ID пользователя и пароль или личный идентификационный номер).

6) Аутентификация. Система IdM выполняет аутентификацию и получает другую необходимую информацию. Это может включать информацию, получаемую от других сетевых систем (например, HSS).

7) Ответ с информацией идентичности [Утверждение полномочий, атрибуты, политика]: система IdM предоставляет информацию, утверждающую полномочия. Другой

информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение, касающееся использования, воспроизведения и распространения).

8) Авторизация доступа. Прикладная услуга предоставляет пользователю указание о том, что доступ к услуге разрешен.

9) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой.

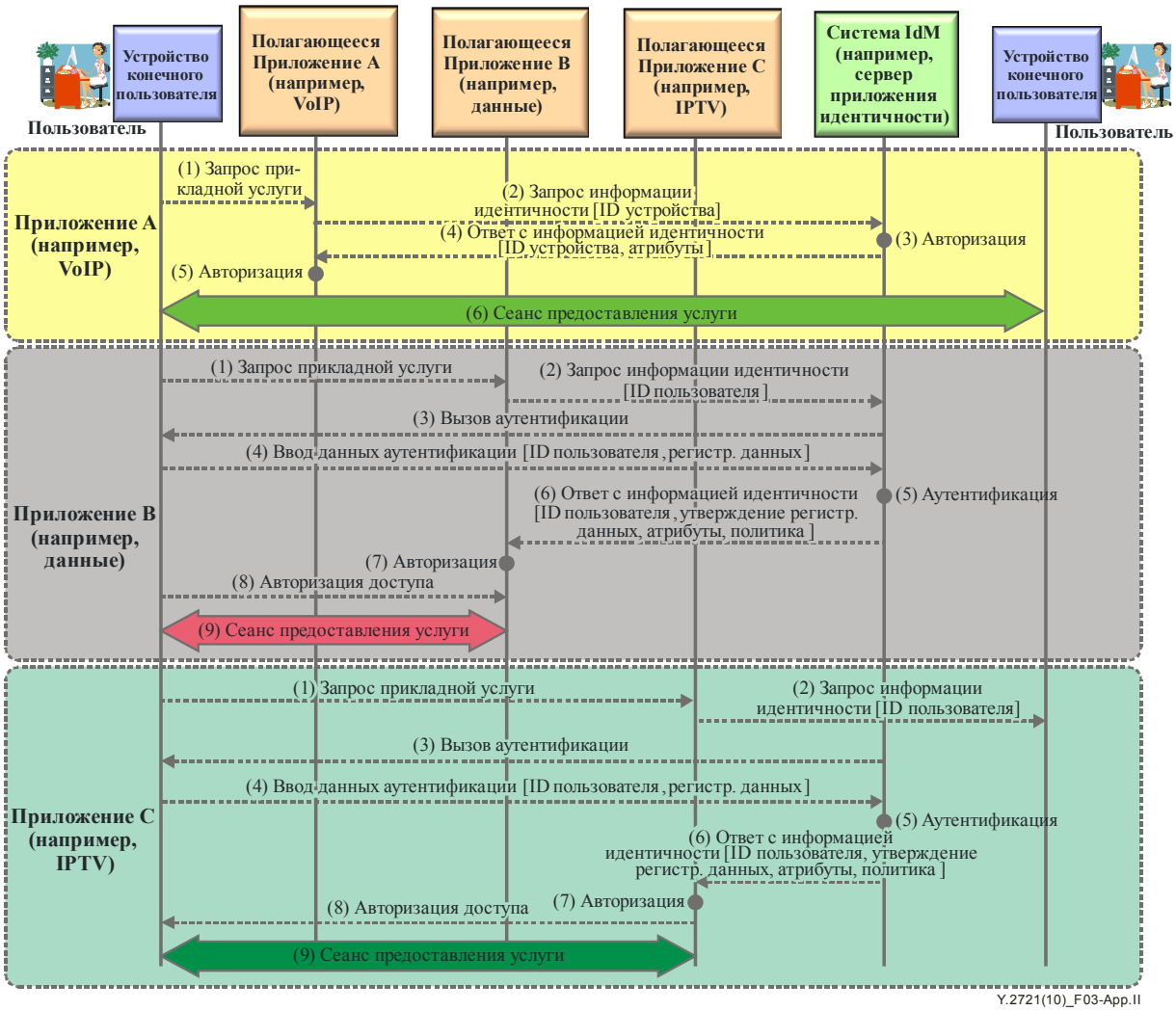


Рисунок II.3 – Использование несколькими прикладными услугами общей инфраструктуры IdM

Рисунок II.3 иллюстрирует пример случая использования несколькими прикладными услугами (например, VoIP, передача данных и IPTV) общей системы IdM, которая является внешней и не зависящей от этих прикладных услуг. В данном примере предполагается, что устройство конечного пользователя зарегистрировано и прикреплено к поставщику услуг с использованием обычных процедур.

Примером потоков для Приложения A (VoIP) является следующий:

1) Запрос прикладной услуги. Данный информационный поток представляет конечного пользователя, инициирующего вызов.

2) Запрос информации идентичности [ID устройства]. Прикладная услуга направляет запрос системе IdM для проверки того, является ли устройство конечного пользователя авторизованным для услуги VoIP. В данном примере предполагается, что услуга VoIP основана на абонентском профиле устройства или линии пользователя (например, подписка на xDSL).

3) Авторизация. Система IdM определяет, является ли конечный пользователь авторизованным для услуги VoIP.

ПРИМЕЧАНИЕ 1. – Предполагается, что это включает выборку информации профиля абонента для устройства или линии конечного пользователя (например, xDSL). Также предполагается, что для VoIP аутентификация конечного пользователя не требуется.

4) Ответ с информацией идентичности [ID устройства, атрибуты]. Система IdM предоставляет атрибуты, связанные с ID устройства, т. е. является ли устройство авторизованным для услуги VoIP. Они будут включать соответствующую информацию, полученную от абонентского профиля (например, привилегии и предпочтения).

5) Авторизация доступа. Прикладная услуга предоставляет пользователю указание о том, что доступ к услуге разрешен.

6) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой.

Например, потоки вызовов для Приложения B (передача данных) следующие:

1) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя, активизирующего прикладную услугу.

2) Запрос информации идентичности [ID пользователя]. Прикладная услуга направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Они могут включать информацию, такую как профиль услуги, привилегии, предпочтения и информацию о политике, например любую политику или ограничения, связанные с идентичностью.

3) Вызов аутентификации. Системы IdM направляют пользователю запрос для проведения аутентификации.

4) Ввод данных аутентификации [Полномочия]. Пользователь предоставляет информацию для аутентификации (например, ID пользователя и пароль или личный идентификационный номер).

5) Аутентификация. Система IdM выполняет аутентификацию и получает другую необходимую информацию. Она может содержать информацию, получаемую от других систем сети (например, HSS или другой абонентской базы данных).

6) Ответ с информацией идентичности [Утверждения полномочий, атрибуты, политика]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

7) Авторизация. Прикладная услуга обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

8) Авторизация доступа. Прикладная услуга предоставляет пользователю указание о том, что доступ к услуге разрешен.

9) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой.

Например, потоки вызовов для Приложения C (IPTV) следующие:

1) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя, активизирующего прикладную услугу.

2) Запрос информации идентичности [ID пользователя]. Прикладная услуга направляет запрос системе IdM на подтверждение идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Они могут включать информацию, такую как профиль услуги, привилегии, предпочтения и информацию о политике. Например, любую политику или ограничения, связанные с идентичностью.

3) Вызов аутентификации. Системы IdM направляют пользователю запрос для проведения аутентификации.

4) Ввод данных аутентификации [Полномочия]. Пользователь предоставляет информацию для аутентификации (например, ID пользователя и пароль или личный идентификационный номер).

5) Аутентификация. Система IdM выполняет аутентификацию и получает другую необходимую информацию. Она может содержать информацию, получаемую от других систем сети (например, HSS или другой абонентской базы данных).

6) Ответ с информацией идентичности [Утверждение полномочий, атрибутов, политики]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

7) Авторизация. Прикладная услуга обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

8) Авторизация доступа. Прикладная услуга предоставляет пользователю указание о том, что доступ к услуге разрешен.

9) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой.

ПРИМЕЧАНИЕ 2. – Для обеспечения взаимной аутентификации (т. е. для аутентификации поставщика приложения или услуги) потребуются дополнительные функциональные возможности и потоки. Однако они не показаны на рисунке II.3.

II.3.3 Предполагаемые требования

В примере данного использования предполагаются следующие требования:

- СПП должны поддерживать общую инфраструктуру IdM, которая будет использоваться многими приложениями и услугами, не зависящими от платформы приложения или решения поставщика.
- Общие функции IdM не должны использоваться, если они противоречат принципам ограничения сбора данных, минимизации объема данных, разделения данных, спецификации назначения и ограничения использования.
- СПП должны поддерживать стандартный и структурированный подход, для того чтобы позволить прикладным услугам обнаружить систему(ы) IdM и безопасно обмениваться данными идентичности.

II.4 Единая регистрация в системе/единый выход из системы для нескольких прикладных услуг (например, передача голоса, данных, IPTV) в пределах сети поставщика услуг

II.4.1 Обзор

Обычно пользователи должны регистрироваться в нескольких системах, в которых размещены прикладные услуги (например, VoIP, передача данных и IPTV), что требует такого же числа диалогов входа, каждый из которых может содержать различные имена пользователей и информацию аутентификации. Администраторы системы должны осуществлять управление учетными записями пользователя в пределах каждой из этих нескольких систем скоординированным образом, для того чтобы поддерживать целостность политики безопасности.

Абоненты, являющиеся конечными пользователями, требуют обеспечивающие простоту использования функции, такие как "Однократная регистрация в системе/единый выход из системы". Преимуществом "Однократной регистрации в системе" является то, что конечный пользователь, устройство или сочетание конечного пользователя и устройства могут войти в систему только однажды (т. е. осуществив ввод полномочий для установления аутентификации и авторизации), для того чтобы получить услугу в сети последующих поколений (СПП) и в результате получить аутентификацию для использования одной или более дополнительных услуг в той же СПП, т. е. конечный пользователь не обременен аутентификацией для каждой услуги. Термин "Регистрация в системе", используемый здесь, означает то же, что и термин "Регистрация в", "Вход в систему" или "Ввод имени/пароля", когда конечный пользователь/устройство "Регистрируется в", "Входит в систему" или "Вводит имя/пароль" для получения услуги. Подобно этому, "Однократный выход из системы" предоставляет возможность избежать необходимости "Выхода из" каждой прикладной услуги в данном сеансе.

Преимущества, предоставляемые услугами однократной регистрации в системе/однократного выхода из системы:

- Сокращение времени, затрачиваемого пользователями при операции входа в каждый отдельный домен, включая снижение вероятности ошибочных операций при входе.
- Усиление безопасности благодаря сокращению потребности для пользователя использовать и запоминать несколько наборов информации аутентификации.
- Сокращение затраченного времени и времени отклика администратора системы при добавлении и удалении пользователей системы или изменение их прав доступа.
- Усиление безопасности благодаря расширению возможности администраторов системы поддерживать целостность конфигурации счета пользователя, включая возможность запретить или удалить доступ отдельного пользователя ко всем ресурсам системы скоординированным и последовательным способом.

II.4.2 Описание случая использования

Данный пример случая использования показывает использование системы IdM для поддержки "Однократной регистрации в системе/однократного выхода из системы" для нескольких прикладных услуг (например, VoIP, передача данных и IPTV) в пределах домена поставщика СПП. Случай использования включает взаимодействие между следующими объектами:

- конечные пользователи (т. е. конечный пользователь и/или устройство конечного пользователя);
- полагающаяся система (т. е. прикладная услуга или система);
- система IdM (т. е. сетевая система, предоставляющая услуги IdM, такие как регистрация, аутентификация и авторизация, информацию профиля абонента).

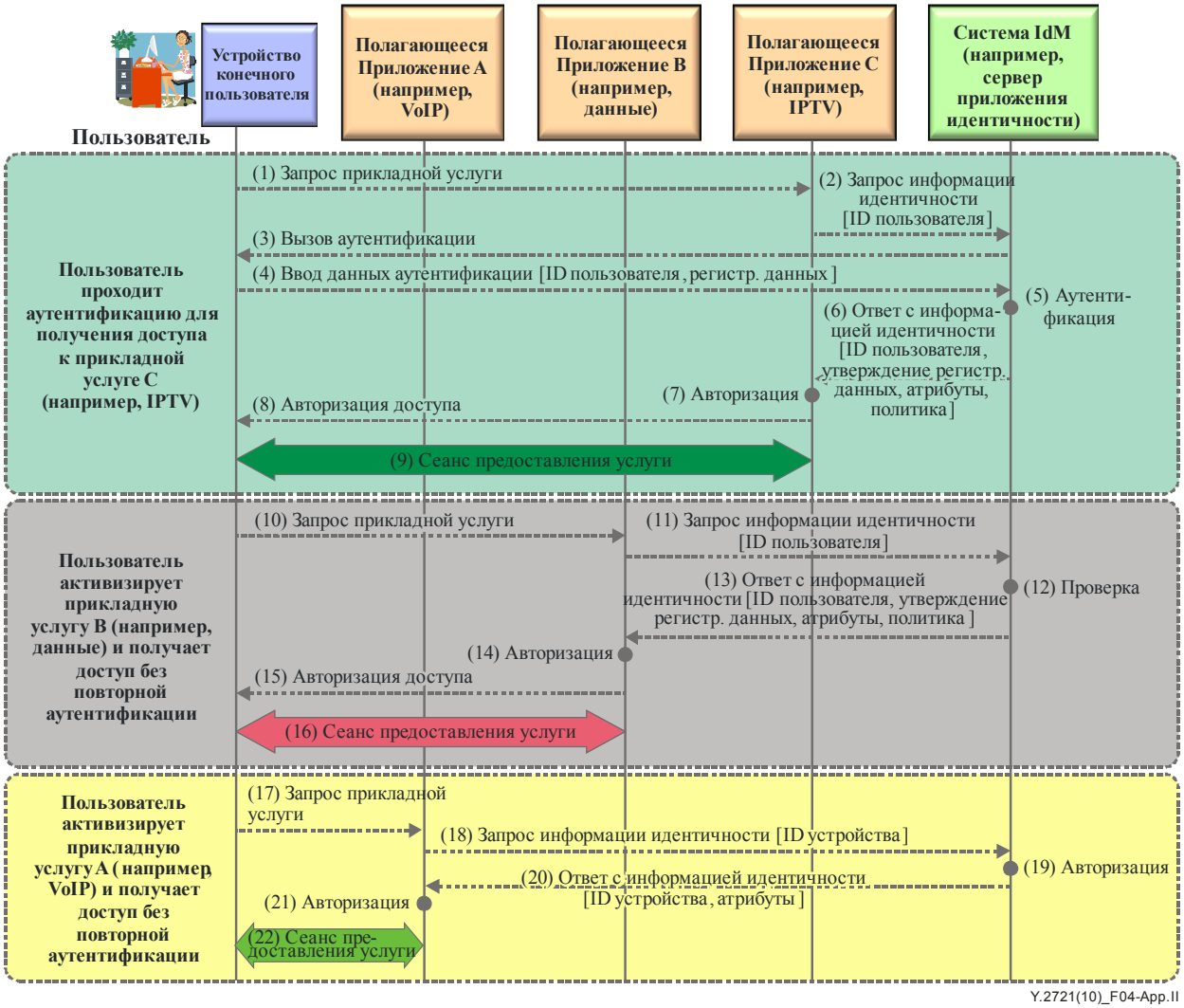


Рисунок II.4 – Однократная регистрация в системе

На рисунке II.4 показан абонент, являющийся конечным пользователем, использующий однократная регистрация в системе для получения доступа к нескольким прикладным услугам (например, VoIP, передаче данных и IPTV). Данный пример предполагает, что устройство конечного пользователя зарегистрировано и прикреплено к СПП с использованием обычных процедур.

Примерами потоков вызовов являются следующие:

1) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя, активизирующего прикладную услугу C (IPTV).

2) Запрос информации идентичности [ID пользователя]. Прикладная услуга C (IPTV) направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Они могут включать информацию, такую как профиль услуги, привилегии, предпочтения и информацию о политике. Например, любую политику или ограничения, связанные с идентичностью.

3) Вызов аутентификации. Система IdM направляет пользователю запрос для проведения аутентификации.

4) Ввод данных аутентификации [Полномочия]. Пользователь предоставляет информацию для аутентификации (например, ID пользователя и пароль или личный идентификационный номер).

5) Аутентификация. Система IdM выполняет аутентификацию и получает другую необходимую информацию. Она может содержать информацию, получаемую от других систем сети (например, HSS или другой абонентской базы данных).

6) Ответ с информацией идентичности [Утверждение полномочий, атрибутов, политики]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

7) Авторизация. Прикладная услуга C (IPTV) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

8) Авторизация доступа. Прикладная услуга C (IPTV) Прикладная услуга предоставляет пользователю указание о том, что доступ к услуге разрешен.

9) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой C (IPTV).

10) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя, активизирующего прикладную услугу B (передача данных).

11) Запрос информации идентичности [ID пользователя]. Прикладная услуга B (передача данных) направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Они могут включать информацию, такую как профиль услуги, привилегии, предпочтения и информацию о политике. Например, любую политику или ограничения, связанные с идентичностью.

12) Верификация. Система IdM обрабатывает запрос и определяет, что применима однократная регистрация в системе, и проверенная аутентификация пользователя еще действительна.

13) Ответ с информацией идентичности [Утверждение полномочий, атрибутов, политики]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

14) Авторизация. Прикладная услуга B (передача данных) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

15) Авторизация доступа. Прикладная услуга B (передача данных) предоставляет пользователю указание о том, что доступ к услуге разрешен.

16) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой B (передача данных).

17) Запрос прикладной услуги. Данный информационный поток представляет запрос конечного пользователя, активизирующего прикладную услугу A (VoIP).

18) Запрос информации идентичности [ID устройства]. Прикладная услуга A (VoIP) направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID устройства.

19) Верификация. Система IdM обрабатывает запрос и определяет, что применима однократная регистрация в системе, и проверенная аутентификация пользователя еще действительна.

20) Ответ с информацией идентичности [Утверждение полномочий, атрибутов, политики]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID устройства (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

21) Авторизация. Прикладная услуга A (VoIP) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

22) Сеанс прикладной услуги. Данный информационный поток отображает успешный сеанс связи пользователя с прикладной услугой A (VoIP).

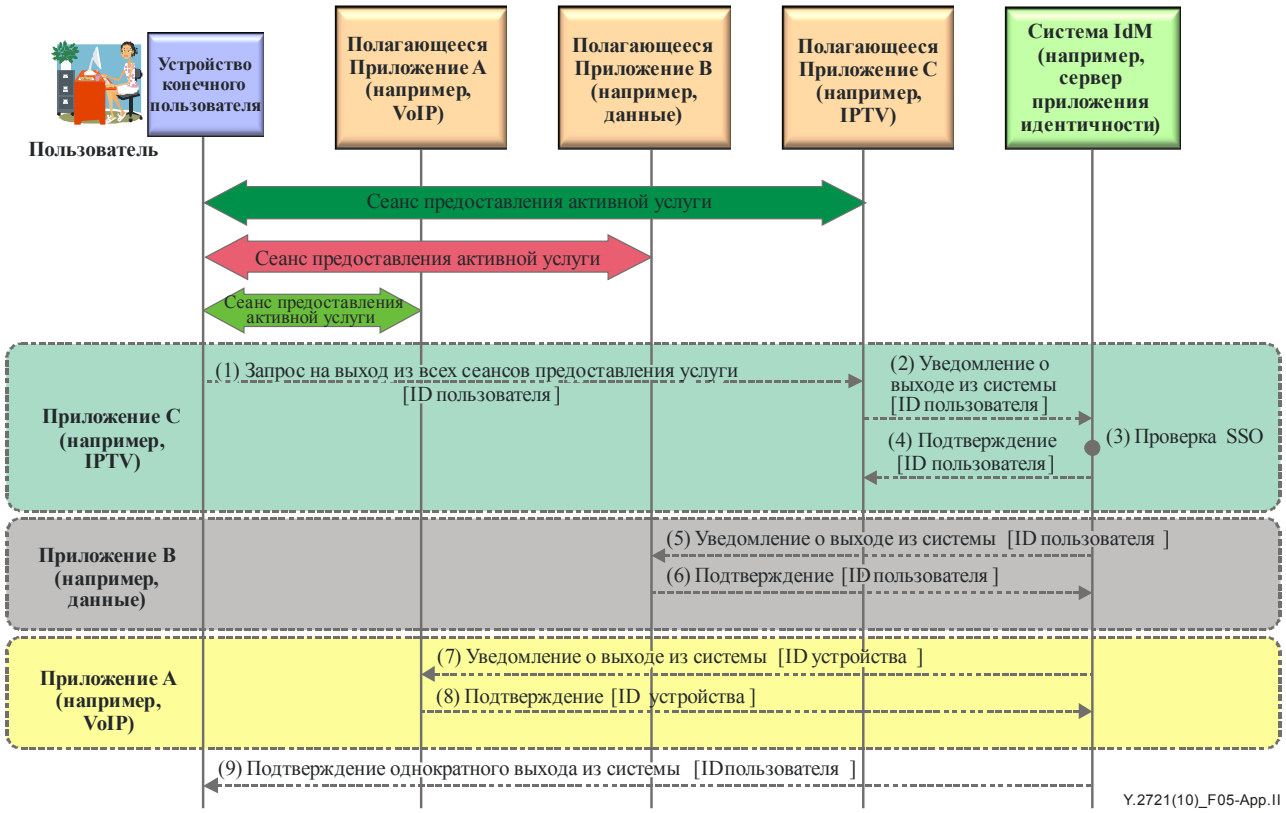


Рисунок II.5 – Услуга однократного выхода из системы

Рисунок II.5 иллюстрирует услугу "Однократный выход из системы", обеспечивающую пользователю возможность автоматического выхода из нескольких прикладных услуг (VoIP, передача данных и видео) без необходимости выхода из каждой услуги в сеансе. В данном случае подразумевается, что пользователь находится в активном сеансе связи с прикладными услугами A (VoIP), B (передача данных) и C (передача видео).

Потоки вызовов следующие:

1) Выход из обслуживания [ID пользователя]. Данный поток вызова представляет запрос пользователя на окончание всех сеансов услуг.

2) Уведомление о выходе [ID пользователя]. Прикладная услуга C (IPTV) уведомляет систему IdM о запросе пользователя на выход из системы.

3) Верификация SSO. Система IdM определяет, что применим однократный выход из системы, и проверяет активные прикладные услуги.

4) Подтверждение [ID пользователя]. Система IdM направляет подтверждение прикладной услуге C (IPTV) об окончании сеанса обслуживания.

5) Уведомление о выходе из системы [ID пользователя]. Система IdM уведомляет прикладную услугу B (передача данных) о выходе из системы.

6) Подтверждение [ID пользователя]. Прикладная услуга B (передача данных) подтверждает выход из системы.

7) Уведомление о выходе из системы [ID устройства]. Система IdM уведомляет прикладную услугу A (VoIP) о выходе из системы.

8) Подтверждение [ID устройства]. Прикладная услуга A (VoIP) подтверждает выход из системы.

9) Подтверждение однократного выхода из системы [ID пользователя]. Система IdM направляет подтверждение пользователю о выходе из всех активных прикладных услуг в сеансе.

II.5 Корреляция распределенной информации идентичности для гарантии обеспечения многофакторной аутентификации

II.5.1 Обзор

Данный случай использования показывает применение IdM для корреляции и увязки многих частей информации идентичности (например, идентификаторов, полномочий и атрибутов), для того чтобы гарантировать обеспечение идентичности конечного пользователя/абонента. Например, информация идентичности, связанная с абонентом (например, ID пользователя), абонентским устройством абонента (например, ID устройства), и информация о местоположении могут коррелироваться для обеспечения более высокой гарантии идентичности абонента.

II.5.2 Пример случая использования

На рисунке II.6 показан в качестве примера случай использования связи идентичности пользователя с идентичностью устройства и корреляция с информацией о присутствии и местоположении, для того чтобы обеспечить более высокий уровень гарантии идентичности и заявлений, связанных с идентичностью.

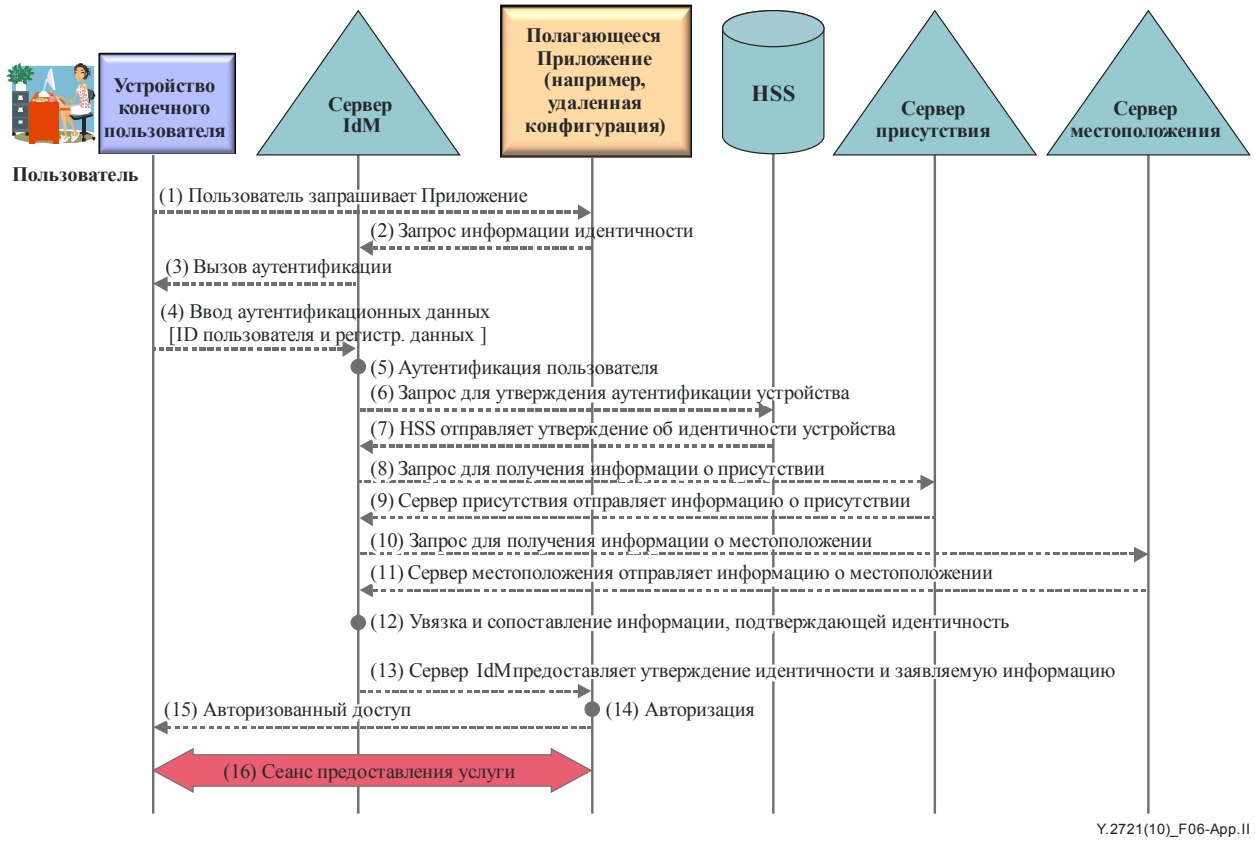


Рисунок II.6 – Корреляция информации идентичности

В данном примере конечный пользователь/абонент пытается получить доступ к приложению, которое требует высокого уровня гарантии обеспечения идентичности пользователя и привилегий, связанных с идентичностью, потому что риски безопасности, связанные с разрешением неавторизованного доступа к приложению или ресурсу, могут быть дорогостоящими.

Примером потоков вызова является следующий:

1) Пользователь запрашивает доступ к приложению.

2) Приложение направляет запрос серверу IdM для утверждения идентичности пользователя и заявлений, связанных с идентичностью.

3) Сервер IdM направляет вызов аутентификации пользователю.

4) Пользователь обеспечивает ввод данных аутентификации для сервера IdM (например, ID пользователя и полномочия).

5) Сервер IdM производит аутентификацию пользователя.

6) Сервер IdM направляет запрос на HSS для утверждения идентичности устройства пользователя. (Отметим, что предполагается, что устройство пользователя зарегистрировано и аутентифицировано в сети с использованием обычных процедур.)

7) HSS направляет утверждение идентичности устройства пользователя.

8) Сервер IdM направляет запрос на сервер присутствия для получения информации о присутствии.

9) Сервер присутствия предоставляет информацию о присутствии на сервер IdM.

10) Сервер IdM направляет запрос на сервер местоположения для получения информации о местоположении.

11) Сервер местоположения предоставляет информацию о местоположении на сервер IdM.

12) Сервер IdM связывает информацию идентичности пользователя и идентичности устройства пользователя. Сочетание идентичностей сопоставляется с информацией о присутствии и местоположении для верификации заявлений, связанных с идентичностью (например, привилегий).

13) Сервер IdM предоставляет приложению утверждения идентичности пользователя и заявления, связанные с идентичностью.

14) Приложение определяет, авторизован ли пользователь для получения доступа.

15) Пользователю разрешается доступ к приложению.

16) Сеанс услуги установлен.

II.6 Обеспечение контроля пользователем информации, позволяющей установить личность (например, предпочтения), в доменах одноранговой сети/поставщика услуг

II.6.1 Краткий обзор

Защита PII очень важна для конечных пользователей/абонентов. Важная особенность IdM заключается в том, что она дает возможность конечным пользователям/абонентам предоставить поставщикам услуг и IdSP информацию об условиях, ограничениях, согласии, авторизации, касающихся создания, сбора, использования и распространения информации о своей идентичности.

II.6.2 Описание случая использования

Данный случай использования связан с обеспечением реализации применяемой политики, такой как политика относительно анонимной или псевдонимной информации идентичности.

На рисунке II.7 показан пример случая использования, в котором пользователь запрашивает анонимность.

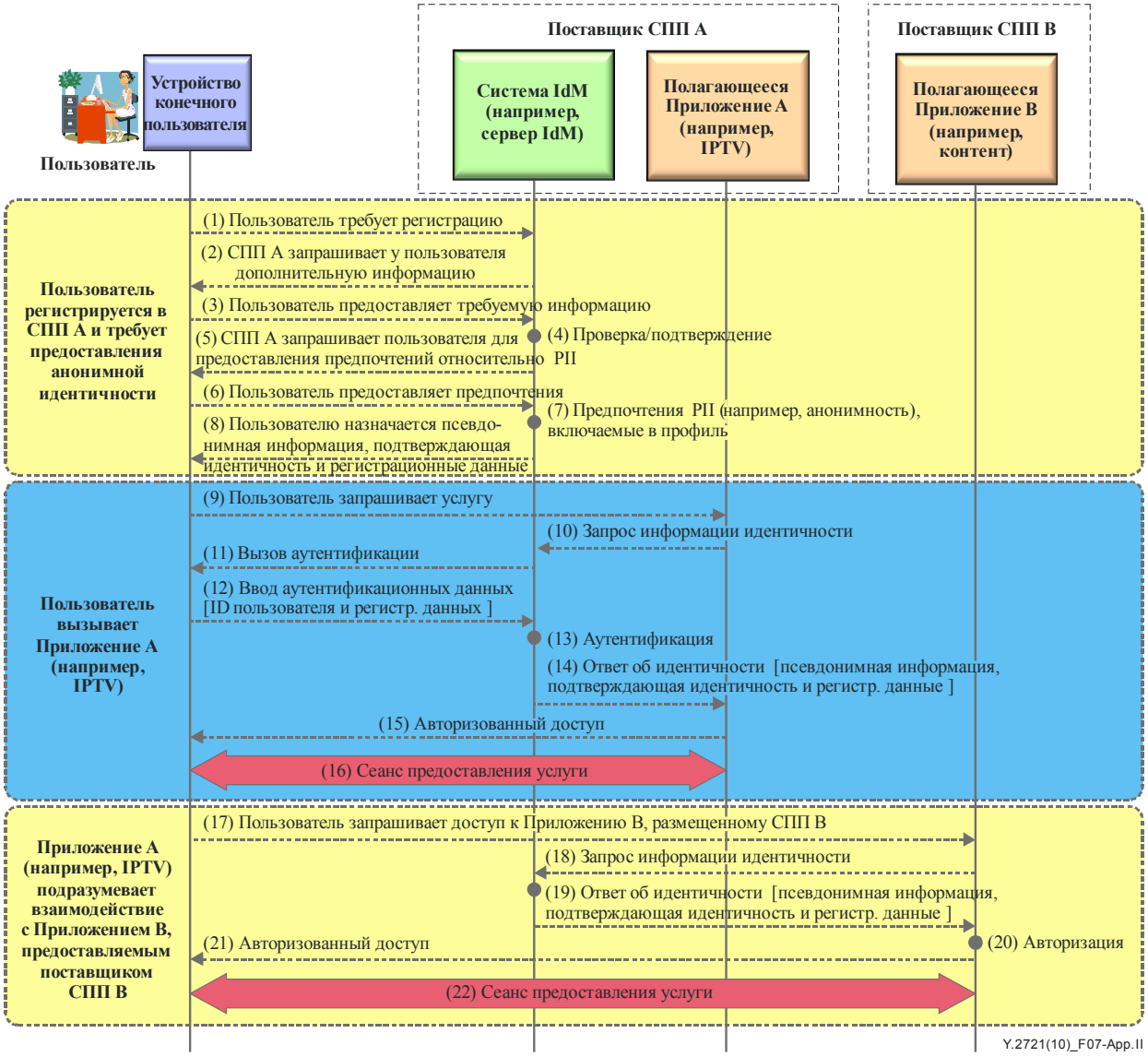


Рисунок II.7 – Идентичность анонимного пользователя

ПРИМЕЧАНИЕ. – Термин "система IdM" используется в качестве общего термина, для того чтобы представить любой элемент сети, который мог бы обеспечить функции IdM и разные возможности реализации/выполнения.

Этот пример использования показывает поставщика СПП (поставщик А СПП), который выполняет присвоение идентичности, используя при этом псевдонимы согласно запросу анонимности от конечного пользователя/абонента. Псевдонимная информация идентичности, используется для взаимодействия с поставщиком В СПП в целях защиты позволяющей установить личность информации абонента, являющего конечным пользователем.

Примером потоков вызова является следующий:

1) Пользователь требует осуществить регистрацию с поставщиком А СПП.

2) Поставщик А СПП запрашивает у пользователя дополнительную информацию.

3) Пользователь предоставляет поставщику А СПП запрашиваемую информацию.

4) Поставщик А СПП проверяет и подтверждает информацию.

5) Поставщик А СПП запрашивает у пользователя информацию о предпочтениях относительно информации, позволяющей установить личность (PII).

6) Пользователь указывает предпочтение анонимности.

7) Поставщик А СПП включает предпочтение анонимности в информацию о профиле пользователя.

8) Пользователю назначается псевдонимная идентичность и полномочия, связанные с идентичностью.

9) Пользователь активизирует Приложение А, например IPTV, размещенное у поставщика СПП А.

10) Полагающееся Приложение А запрашивает информацию идентичности пользователя у системы IdM (например, сервера IdM).

11) Система IdM направляет вызов аутентификации пользователю.

12) Пользователь предоставляет данные аутентификации для сервера IdM, например вводит ID пользователя и полномочия.

13) Система IdM осуществляет аутентификацию пользователя.

14) Система IdM направляет полагающемуся Приложению А утверждение идентичности пользователя и полномочия.

ПРИМЕЧАНИЕ. – Для соблюдения анонимности предоставляется только псевдонимная информация идентичности.

15) Пользователь авторизуется для доступа к Приложению А.

16) Сеанс услуги.

17) Пользователь запрашивает доступ к Приложению В, размещенному у поставщика СПП В.

18) Приложение В направляет в систему IdM запрос информации, утверждающей идентичность пользователя, и связанных с ней заявлений.

19) Система IdM предоставляет утверждение идентичности пользователя и связанных с ней заявлений. Для соблюдения политики анонимности направляется только псевдонимная информация идентичности.

20) Приложение В верифицирует информацию для авторизации.

21) Пользователю предоставляется авторизация для доступа.

22) Устанавливается сеанс услуги.

II.7 Сопряжение/преобразование между неоднородными системами IdM

II.7.1 Краткий обзор

Для того чтобы позволить пользователю получать несколько услуг, предлагаемых различными СПП, в СПП должны быть предусмотрены механизмы для сопряжения различных систем IdM. В качестве иллюстрации этой необходимости служит случай использования, описанный в следующем разделе.

II.7.2 Описание случая использования

В данном сценарии описывается доступ, осуществляемый абонентом СПП к ресурсу (например, серверу телефонного справочника), расположенному в сети предприятия, с использованием телефонной трубки абонента. Поскольку СПП и сети предприятия используют различные механизмы IdM, то существует необходимость в сопряжении систем IdM этих сетей.

В примере, иллюстрирующем данный сценарий, участвуют следующие объекты:

- Система IdM СПП. Даная система модифицирована таким способом, что она может, в дополнение к поддержке взаимной аутентификации, основанной на АКА телефонной трубки пользователя, обеспечить для этой телефонной трубки полномочия для аутентификации в системе IdM сети предприятия.
- Система IdM сети предприятия (например, центр распределения ключей.
- Сервер телефонного справочника предприятия (EDS), расположенный в сети предприятия.
- Телефонная трубка пользователя.

- Эти объекты выполняют следующее взаимодействие:
  - Телефонная трубка пользователя и сеть подвижной связи осуществляют аутентификацию друг друга, используя метод AKA.
  - Пользователь, использующий телефонную трубку, направляет запрос на сервер телефонного справочника предприятия (EDS), расположенный в сети предприятия.
  - EDS направляет в отклике запрос об аутентификации.
  - Пользователь получает от системы IdM СПП полномочия для аутентификации (например, мандат Kerberos), которые основана на результатах аутентификации AKA и действуют для аутентификации в системе IdM предприятия.

Например, телефонная трубка пользователя получает мандат из центра распределения ключей (KDC) сети предприятия. В частности, мандат позволяет пользователю получить аутентификацию с помощью сервера предоставления мандата (TGS), который является частью KDC.

- Пользователь запрашивает у TGS мандат для аутентификации с EDS.
- TGS проверяет достоверность представленных полномочий и в отклике направляет пользователю мандат для EDS.
- Конечный пользователь отвечает на запрос об аутентификации EDS с помощью мандата, полученного от TGS.
- EDS осуществляет аутентификацию пользователя и направляет отклик пользователю с его собственными полномочиями для аутентификации и подтверждением для получения запрашиваемой услуги. После валидации полномочий EDS пользователь может получить доступ к EDS.

II.7.3 Предполагаемые требования

- Система IdM СПП должна поддерживать механизм аутентификации AKA и механизм аутентификации (например, Kerberos), используемый сетью предприятия).
- Система IdM СПП должна уметь выдавать полномочия для аутентификации (например, мандат Kerberos) устройству конечного пользователя, для того чтобы осуществить аутентификацию пользователя в системе IdM предприятия.
- Система IdM СПП должна управлять идентичностью и полномочиями пользователя.
- Система IdM предприятия должна управлять идентичностью и полномочиями сервера.

ПРИМЕЧАНИЕ. – a) Не требуются новых возможностей для сетей 3G (которые, таким образом, могут выступать в качестве примера); b) Требования, изложенные здесь, применяются конкретно для поддержки вышеприведенного случая.

II.8 Поддержка конвергированных услуг (например, фиксированный и подвижный доступа) в пределах сети поставщика услуг

II.8.1 Обзор

Преимуществом сетей последующих поколений является поддержка огромного числа конвергированных услуг, предоставляемых сетями фиксированного и подвижного доступа. Таким образом, пользователь в каждый конкретный момент должен иметь гибкость для активизации услуги с использованием удобного для него устройства и сети доступа. (В свою очередь, поставщик услуг увеличит свою абонентскую базу и прибыль.) Поскольку основные механизмы безопасности, пригодные для среды фиксированной и подвижной связи, как правило, различаются, важным посредником будет конвергированная система IdM, которая может справиться с данными различиями. Конвергированная IdM управляет идентичностью и полномочиями конечных пользователей и серверов сети независимо от технологии доступа.

II.8.2 Описание случая использования

В данном сценарии описывается доступ, осуществляемый абонентом сети 3G к ресурсу (например, к серверу, предоставляющему видео по запросу), который расположен в сети фиксированной связи, с использованием своей телефонной трубки. В данном сценарии сеть 3G и ресурс в сети фиксированной связи поддерживают различные механизмы, связанные с IdM. В примере, иллюстрирующем данный сценарий, участвуют следующие объекты:

- Система IdM сети 3G. Даная система модифицирована таким способом, что она может, в дополнение к поддержке взаимной аутентификации, основанной на AKA телефонной трубки пользователя, обеспечить для этой телефонной трубки полномочия для аутентификации на сервере, предоставляющем видео по запросу (VoD).
- Сервер VoD, расположенный в сети фиксированной связи.
- Телефонная трубка 3G пользователя.
- Эти объекты выполняют следующее взаимодействие:
  - Телефонная трубка пользователя и сеть подвижной связи осуществляют аутентификацию друг друга, используя метод AKA.
  - Пользователь, использующий телефонную трубку, направляет запрос на сервер VoD.
  - Сервер VoD направляет в ответ запрос об аутентификации пользователя.
  - Пользователь получает полномочия для аутентификации (например, мандат Kerberos) от системы IdM сети 3G, которая создает такие полномочия на основе результатов аутентификации AKA.
  - Пользователь направляет отклик серверу VoD с полномочиями для аутентификации (мандатом).
  - Сервер VoD осуществляет аутентификацию пользователя и направляет отклик с подтверждением для запрашиваемой услуги.

II.8.3 Предполагаемые требования

- Система IdM сети 3G должна поддерживать механизм аутентификации AKA и механизм аутентификации (например, Kerberos), используемый сервером VoD.
- Система IdM СПП должна уметь выдавать полномочия для аутентификации (например, мандат) устройству пользователя, для того чтобы осуществить аутентификацию пользователя на сервере VoD.
- Система IdM сети 3G должна управлять идентичностью и полномочиями пользователя.
- Система IdM сети 3G должна управлять идентичностью и полномочиями сервера VoD.

ПРИМЕЧАНИЕ. – Требования, изложенные здесь, применяются конкретно для поддержки вышеприведенного случая.

II.9 Пример случая использования – Аутентификация и авторизация пользователем поставщика СПП (взаимная аутентификация и авторизация)

На рисунке II.8 показан в качестве примера сценарий использования, включающий аутентификацию пользователем поставщика СПП. В данном примере принимается открытая среда услуг, где поставщики СПП имеют возможность предоставления пользователю рекламных услуг. В данном примере случая использования показаны разрывы или отсутствие возможностей для пользователя аутентифицировать и авторизовать поставщиков СПП (или выполнять взаимную аутентификацию) в открытой среде услуг, в которой имеется несколько поставщиков.

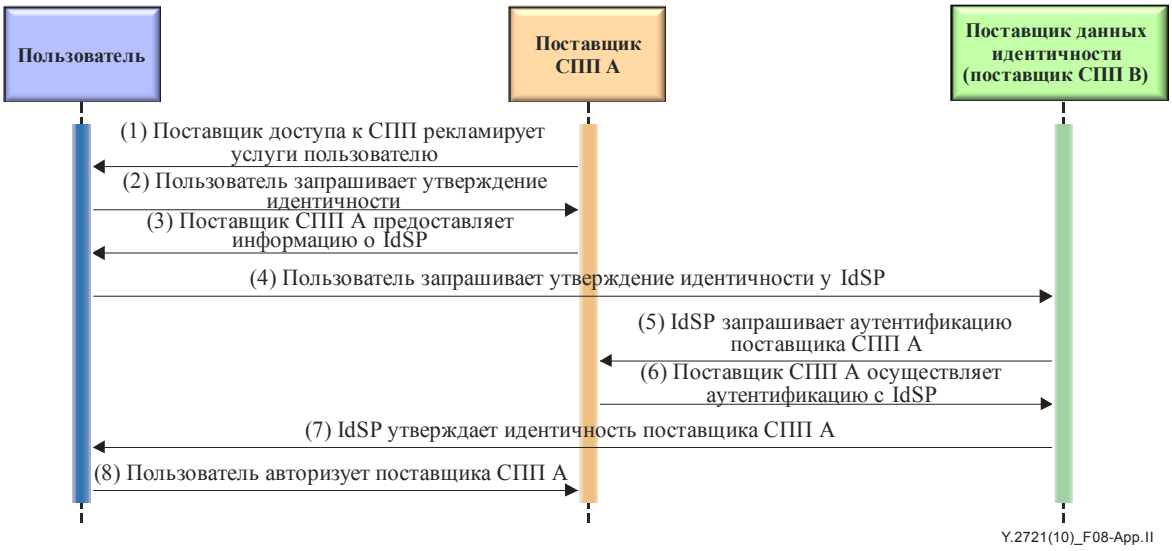


Рисунок II.8 – Пример сценария использования: аутентификация и авторизация пользователя поставщика СПП

Пример потоков в кратком виде выглядит следующим образом:

1) Поставщик А СПП рекламирует услуги пользователю.

2) Пользователь запрашивает утверждение идентичности поставщика А СПП.

3) Поставщик А СПП предоставляет пользователю адрес IdSP.

4) Пользователь направляет запрос IdSP на утверждение идентичности поставщика А СПП.

5) IdSP направляет запрос поставщику А СПП для аутентификации.

6) Поставщик А СПП предоставляет информацию аутентификации.

7) IdSP направляет пользователю информацию, утверждающую идентичность поставщика А СПП.

8) Пользователь авторизует поставщика А СПП для предоставления услуг.

ПРИМЕЧАНИЕ. – В данном примере не показаны потоки, связанные с аутентификацией и авторизацией поставщиком СПП пользователя.

II.10 Пример случая использования – Утверждение однорангового пользователя (безналичные транзакции)

В настоящее время отсутствуют возможности IdM СПП, позволяющие пользователям осуществлять аутентификацию при установлении соединения или доступа к источникам данных. В основном, подходы IdM, которые определены, главным образом относятся к IdM для транзакций с наличностью и электронной коммерции. СПП должна будет поддерживать возможности IdM для осуществления более широкого диапазона транзакций и соединений. Это особенно важно для определенных услуг в чрезвычайных ситуациях, которые должны поддерживаться СПП. На рисунке II.9 показан в качестве примера случай использования, иллюстрирующий необходимость в наличии возможностей IdM СПП, для того чтобы обеспечить пользователям возможность утверждать идентичность друг друга для одноранговых соединений и безналичных транзакций. Например, пользователю может потребоваться аутентификация источника принимаемого сообщения (например, сообщения электронной почты или мгновенного сообщения), запроса на установление связи (например, голосовой связи, или видео, или передачи данных) или принимаемых данных. В настоящее время отсутствует спецификация СПП для обеспечения таких возможностей IdM.

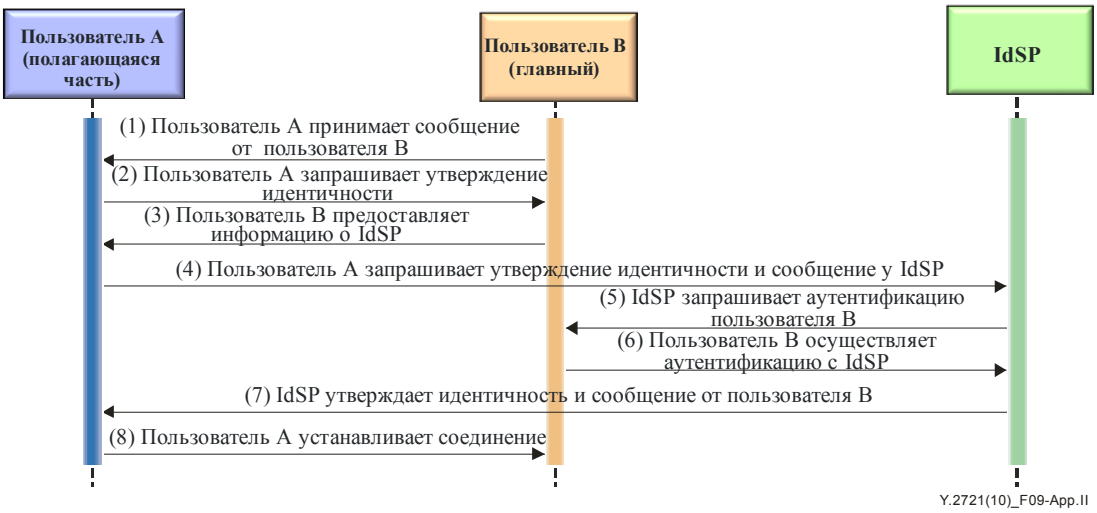


Рисунок II.9 – Пример случая использования: Утверждение одноранговоого пользователя (безналичные транзакции)

В качестве примера на рисунке II.9 показан случай использования, предполагающий, что пользователь A получает сообщение или запрос для установления соединения от пользователя B и хотел бы утвердить идентичность пользователя B и полученных данных. Пример потоков вызовов кратко выглядит следующим образом:

1) Пользователь A получает сообщение или запрос для установления соединения с пользователем B.

2) Пользователь A запрашивает утверждение идентичности пользователя B и аутентификацию полученной от пользователя B информации.

3) Пользователь B предоставляет пользователю A адрес поставщика услуг определения идентичности (IdSP).

4) Пользователь A направляет запрос IdSP для утверждения идентичности пользователя B и осуществления аутентификации принятой информации.

5) IdSP направляет запрос пользователю B для осуществления аутентификации.

6) Пользователь B направляет отклик и аутентифицируется IdSP.

7) IdSP направляет отклик пользователю A, подтверждающий идентичность пользователя B и принятой информации.

8) Пользователь A подтверждает соединение с пользователем B.

II.11 Случай использования IdM – Обеспечение идентичности и целостности устройства конечного пользователя

СПП будут поддерживать большое число типов устройств пользователя (например, фиксированные телефоны, беспроводные телефонные трубки, персональные компьютеры, КПК, телевизионные приставки IPTV). Компоненты оборудования и программного обеспечения устройств, связанных с СПП, могут быть и очень простыми, и очень сложными, и если они будут похищены и вскрыты, их могут использовать для проведения разных атак.

Специальные возможности безопасности могут быть разработаны и реализованы как часть устойчивого к взлому компонента аппаратного оборудования в устройствах конечного пользователя для хранения данных управления определением идентичности в зашифрованной форме и поддерживать специализированные возможности безопасности для валидации идентичности и целостности устройств конечного пользователя. В данном разделе в качестве примера описываются случаи использования, в которых специализированный компонент безопасности аппаратного оборудования может быть разработан и реализован как часть устройства конечного пользователя и использоваться для поддержки услуги управления определением идентичности, с тем чтобы:

1) гарантировать идентичность устройства конечного пользователя;

2) гарантировать целостность устройства конечного пользователя (например, верифицировать, что не нарушена конфигурация программного и аппаратного оборудования);

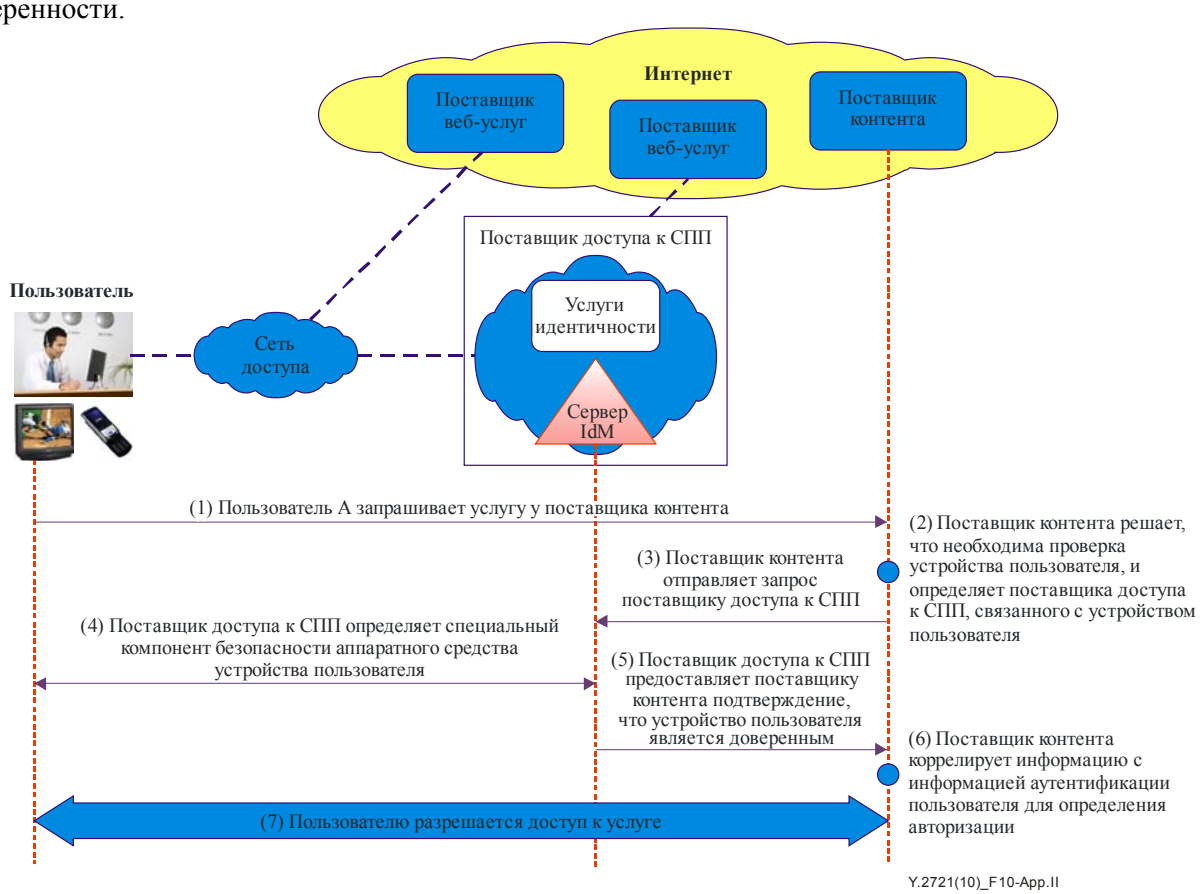
3) разрешать пользователям зашифровывать защищать PII и другие уязвимые данные на устройствах конечного пользователя.

II.11.1 Пример случая использования – Гарантия обеспечения аутентификации пользователя и устройства

Данный случай использования включает поддержку специализированного устойчивого к взлому компонента аппаратного оборудования в устройствах конечного пользователя для обеспечения уникальной идентификации устройства. Например, для обеспечения уникальной идентификации устройства пароли, цифровые ключи и сертификаты могут храниться в специализированном устойчивом к взлому компоненте устройства аппаратного оборудования. Специализированный компонент аппаратного оборудования может поддерживать стандартизированные интерфейсы прикладного программирования (API), для поддержки прикладных услуг безопасности, полагающихся на специализированный устойчивый к взлому компонент аппаратного оборудования, выступающего как "точка доверия" для устройства конечного пользователя.

Уникальная идентификация и аутентификация устойчивого к взлому компонента аппаратного оборудования может коррелироваться с идентификацией и аутентификацией пользователя, для того чтобы обеспечить более высокую степень гарантии для контроля доступа в среде поставщиков нескольких услуг.

На рисунке II.10 в качестве примера показан случай использования, где устойчивый к взлому компонент аппаратного оборудования разработан и реализован в устройствах конечного пользователя для обеспечения уникальной идентификации устройства. В данном примере предполагается, что специализированный устойчивый к взлому компонент аппаратного оборудования контролируется поставщиком СПП через договорное соглашение с абонентом. При условии информированного согласия пользователя поставщик IdSP/СПП может предоставлять услуги идентичности другим поставщикам (например, поставщикам контента, поставщикам веб-услуг и поставщикам услуг 3-й стороны) и партнерам, гарантирующим идентичность и аутентификацию устройства конечного пользователя. Это позволило бы поставщикам услуг быть уверенными в идентичности и аутентификации устройства конечного пользователя. Информация идентичности и аутентификации устройства пользователя может быть коррелирована с аутентификацией пользователя для обеспечения более высокой степени гарантирования и уверенности.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок II.10 – Корреляция аутентификации пользователя и устройства для гарантирования

Пример потоков в кратком виде выглядит следующим образом:

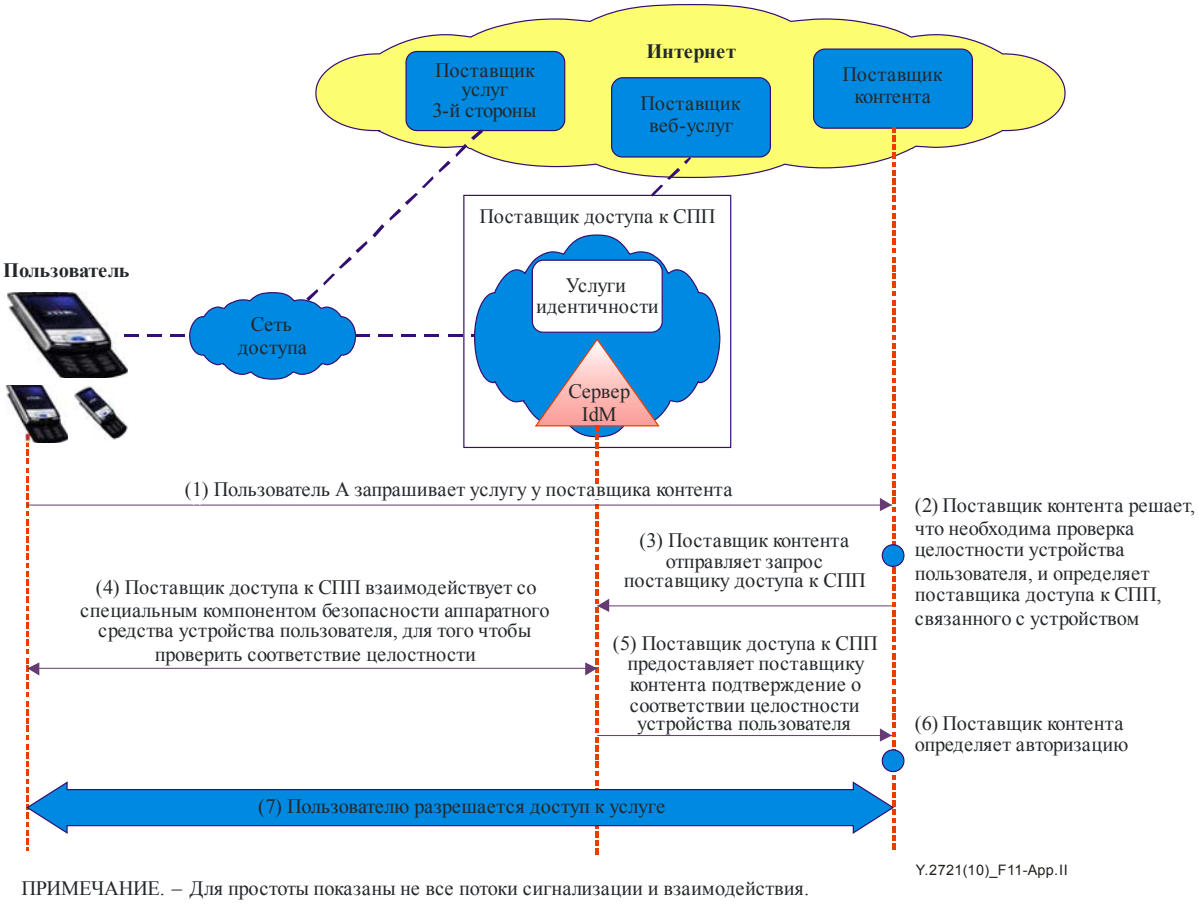
1) Пользователь запрашивает услугу у поставщика контента.
2) Поставщик контента решает, что необходима проверка устройства пользователя для предоставления доступа к услуге и определяет, что поставщик СПП связан с устройством пользователя.
3) Поставщик контента направляет запрос поставщику СПП, для того чтобы утвердить идентичность и аутентификацию устройства пользователя.
4) Поставщик СПП производит идентификацию и аутентификацию специального компонента безопасности аппаратного оборудования устройства пользователя (например, верифицируя сертификаты, хранящиеся в устойчивом к взлому компоненте аппаратного оборудования.
5) Поставщик СПП направляет отклик поставщику контента с результатом валидации идентичности и аутентификации устройства пользователя.
6) Поставщик контента коррелирует информацию, полученную от поставщика СПП, с информацией аутентификации пользователя и определяет авторизацию на получение услуги.
7) Пользователю разрешается доступ к услуге (например, контенту).

II.11.2 Пример случая использования – Гарантирование целостности устройства пользователя

В сегодняшней среде безопасности для присоединения к сети абоненты используют различные устройства (например, фиксированные телефоны, беспроводные телефонные трубки, персональные компьютеры, КПК, телевизионные приставки IPTV). Целостность устройств конечного пользователя (например, конфигурация программного и аппаратного оборудования) может быть легко нарушена втайне от пользователя/абонента. Популярные приложения интернета, такие как веб-браузеры и электронная почта, и другие приложения, которые предоставляются на устройствах абонента, для того чтобы абонент мог взаимодействовать с услугами и функциями локального устройства, могут потенциально подвергать риску целостность устройств, вводя у них фактор уязвимости. Например, эти приложения могут иметь внутренние недостатки безопасности или возможности поддержки, такие как загрузка файлов, приложения программного обеспечения, программные расширения браузера и вложенные ссылки, которые могут использоваться. Программное обеспечение и загрузка файлов, особенно из ненадежного источника, делают устройства абонента уязвимыми для вредоносного кода, червей, вирусов и троянских программ. Клавиатурные шпионы (которые записывают всю вводимую с клавиатуры информацию, включая имена пользователя и пароли, а затем передают информацию злоумышленнику, который может использовать ее для получения несанкционированного доступа) являются распространенным типом вредоносного кода. Другие типы вредоносного кода включают программы-шпионы (программы, которые отслеживают действия абонента), и рекламное программное обеспечения (программы, которые выводят нежелательные рекламные объявления, часто основанные на информации, собранной при наблюдении за абонентом). Некоторые из этих программ буквально захватывают устройства абонента и маскируют их присутствие, путем глубоко внедрения в операционную систему.

Представляемый случай использования включает поддержку специализированного устойчивого к взлому компонента аппаратного оборудования в устройствах конечного пользователя для обеспечения проверки целостности и предоставления приложениям и услугам подтверждения целостности устройства. Например, специализированный компонент аппаратного оборудования, устойчивый к взлому, может содержать определенные алгоритмы и функции производителя для проверки нарушения идентичности. Такой специализированый компонент аппаратного оборудования может включать эталонную модель с набором заведомо правильных метрик целостности, определенным образом идентифицирующих правильный код и дающих эталонные значения для устройств. Заведомо правильные метрики целостности могут использоваться для сравнения фактических представленных значений с конфигурацией и определения соответствия аппаратного устройства.

На рисунке II.11 в качестве примера представлен случай использования, в котором устойчивый к взлому компонент аппаратного оборудования разработан и реализован в устройстве конечного пользователя для обеспечения проверки целостности устройства. В данном примере предполагается, что специализированный устойчивый к взлому компонент аппаратного оборудования контролируется поставщиком СПП через договорное соглашение с абонентом. При условии информированного согласия пользователя поставщик IdSP/СПП может предоставлять услуги идентичности другим поставщикам (например, поставщикам контента, поставщикам веб-услуг и поставщикам услуг 3-й стороны) и партнерам, осуществляющим валидацию целостности и соответствия устройства конечного пользователя.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок II.11 – Гарантирование целостности устройства

Пример потоков в кратком виде выглядит следующим образом:

1) Пользователь запрашивает услугу у поставщика контента.

2) Поставщик контента определяет, что необходима проверка целостности устройства и определяет поставщика СПП, связанного с устройством пользователя.

3) Поставщик контента направляет запрос поставщику СПП на подтверждение целостности устройства пользователя.

4) Поставщик СПП взаимодействует со специальным компонентом безопасности аппаратного оборудования устройства конечного пользователя для верификации соответствия целостности.

5) Поставщик СПП предоставляет поставщику контента подтверждение целостности устройства пользователя.

6) Поставщик контента определяет авторизацию.

7) Пользователю разрешается доступ к услуге (например, контенту).

II.11.3 Пример сценария использования – Шифрование PII и конфиденциальных файлов/данных

Потеря или кража устройства с PII и другими конфиденциальными данными может привести к серьезным последствиям для частных лиц, коммерческих и государственных предприятий. Специализированные компоненты оборудования, предназначенные для уникальной идентификации и подтверждения целостности доверенных устройств, могут потенциально поддерживать возможности шифрования и защиты PII и других чувствительных данных на устройствах конечного пользователя. С зашифрованными конфиденциальными данными неавторизованные стороны не могут получить доступ к данным на компьютере, сотовом телефоне или запоминающем устройстве, что устраняет необходимость принятия дорогостоящих корректирующих мер.

Дополнение III

Случаи использования IdM, относящиеся к службе электросвязи в чрезвычайных ситуациях (ETS)

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

III.1 Введение

В данном Дополнении представлены примеры случаев использования IdM, относящиеся к ETS. См. п. 8.4.7.

III.2 Гарантия обеспечения аутентификации с использованием сочетания устройства и пользователя

Аутентификация авторизованных пользователей ETS необходима для защиты доступности и целостности ETS и связанных сетей. В настоящее время для традиционных приложений ETS применяются два метода аутентификации:

1) метод на основе PIN; и

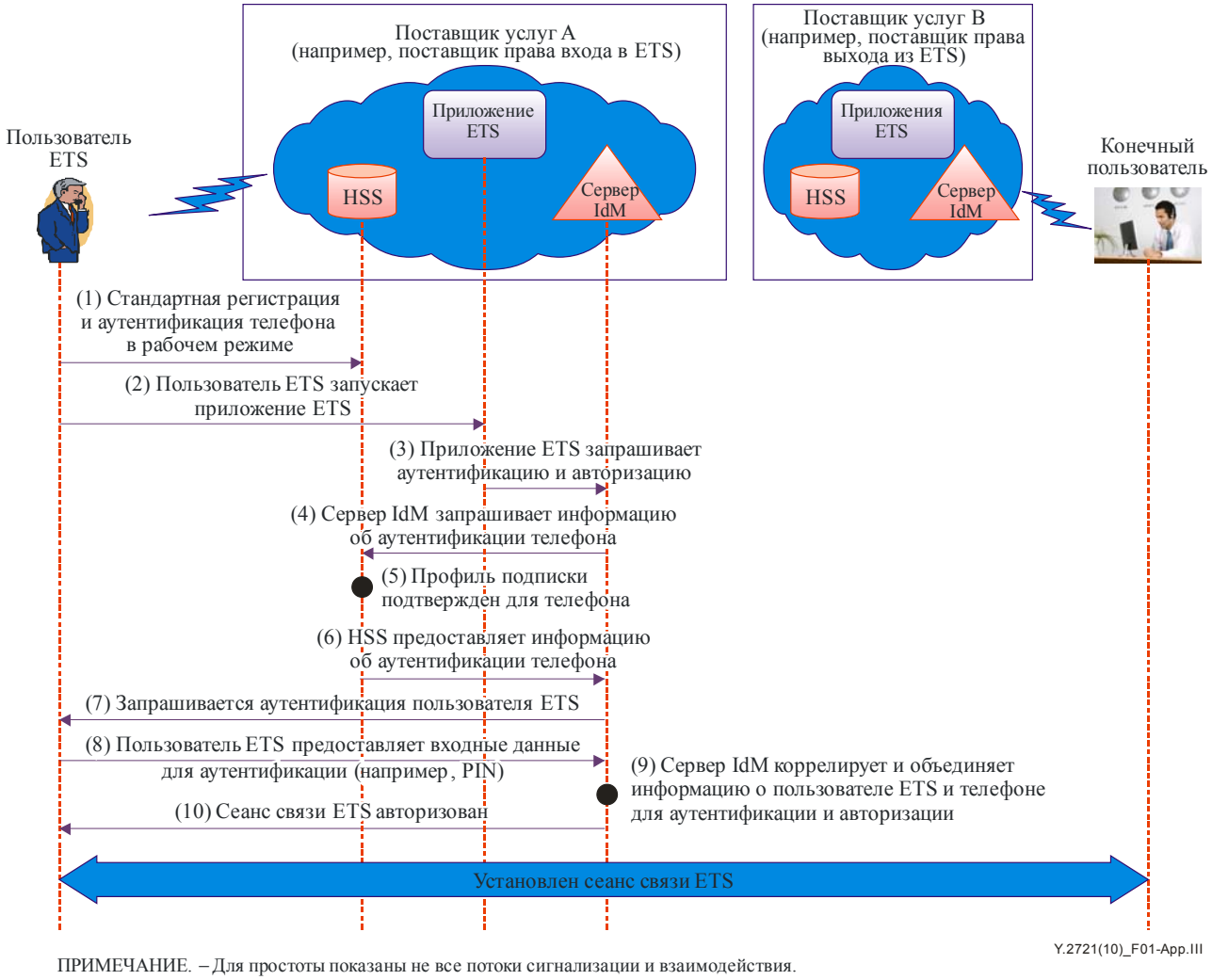
2) метод на основе подписки.

Первый метод включает применение персональных идентификационных номеров (PIN) для аутентификации и авторизации. Проверка PIN аутентифицирует пользователя, тем самым авторизуя его для ETS. Этот подход идентифицирует пользователя, а не устройства пользователя. Поэтому он обычно применяется в случаях, когда пользователю разрешено активировать ETS с любого устройства.

Второй метод использует аутентификацию и авторизацию на основе информации профиля подписки, связанной с определенным терминалом или устройством конечного пользователя. Идентичность устройства пользователя или терминала аутентифицируется как часть стандартной регистрации и аутентификации поставщика СПП (т. е. поставщика ETS), а отдельные вызовы/сеансы ETS авторизуются посредством проверки профиля подписки на услуги (т. е. проверки того, позволяет ли подписка на услугу вызов/сеанс ETS с этого устройства). Этот подход аутентифицирует устройство пользователя (т. е. беспроводной телефон, а не пользователя).

Применение простых методов аутентификации на основе PIN или подписки подходит для традиционных приложений ETS. Однако простые методы на основе PIN или подписки не подходят для всех типов приложений ETS в условиях СПП. В частности, такие приложения как приоритетные мультимедийные приложения (например, службы передачи данных и видео), потребуют более высокого уровня гарантии или уверенности в отношении идентичности пользователя ETS и уровня авторизации для доступа к приложению ETS и связанных с ним ресурсам. Поэтому кроме поддержки существующих методов аутентификации на основе PIN и подписки, в СПП потребуется также поддержка расширенных механизмов аутентификации и авторизации пользователей и устройств ETS.

Подходом к рассмотрению перехода приложения ETS, т. е. приоритетных голосовых услуг, в среду СПП является использование IdM для корреляции и связи аутентификации пользователя и аутентификации устройства пользователя. Это даст расширенные гарантии (т. е. уверенность) в идентичности и авторизации пользователя для доступа к ETS. Эта концепция описана далее в общих примерах случаев использования.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.1 – Комбинированная аутентификация пользователя и устройства

На рисунке III.1 показан пример, в котором функции IdM используются для объединения аутентификации пользователя и устройства для более высокого уровня гарантии авторизации пользователей ETS.

Пример потоков в кратком виде выглядит следующим образом:

1) Телефон пользователя регистрируется и получает аутентификацию посредством стандартных процедур после включения питания.

2) Пользователь ETS инициирует приложение ETS.

3) Приложение ETS запрашивает аутентификацию и авторизацию у сервера IdM.

4) Сервер IdM запрашивает у HSS информацию об аутентификации телефона.

5) HSS верифицирует профиль подписки телефона.

6) HSS представляет серверу IdM информацию об аутентификации телефона.

7) Запрашивается аутентификация пользователя ETS.

8) Пользователь ETS предоставляет данные для аутентификации (например, PIN).

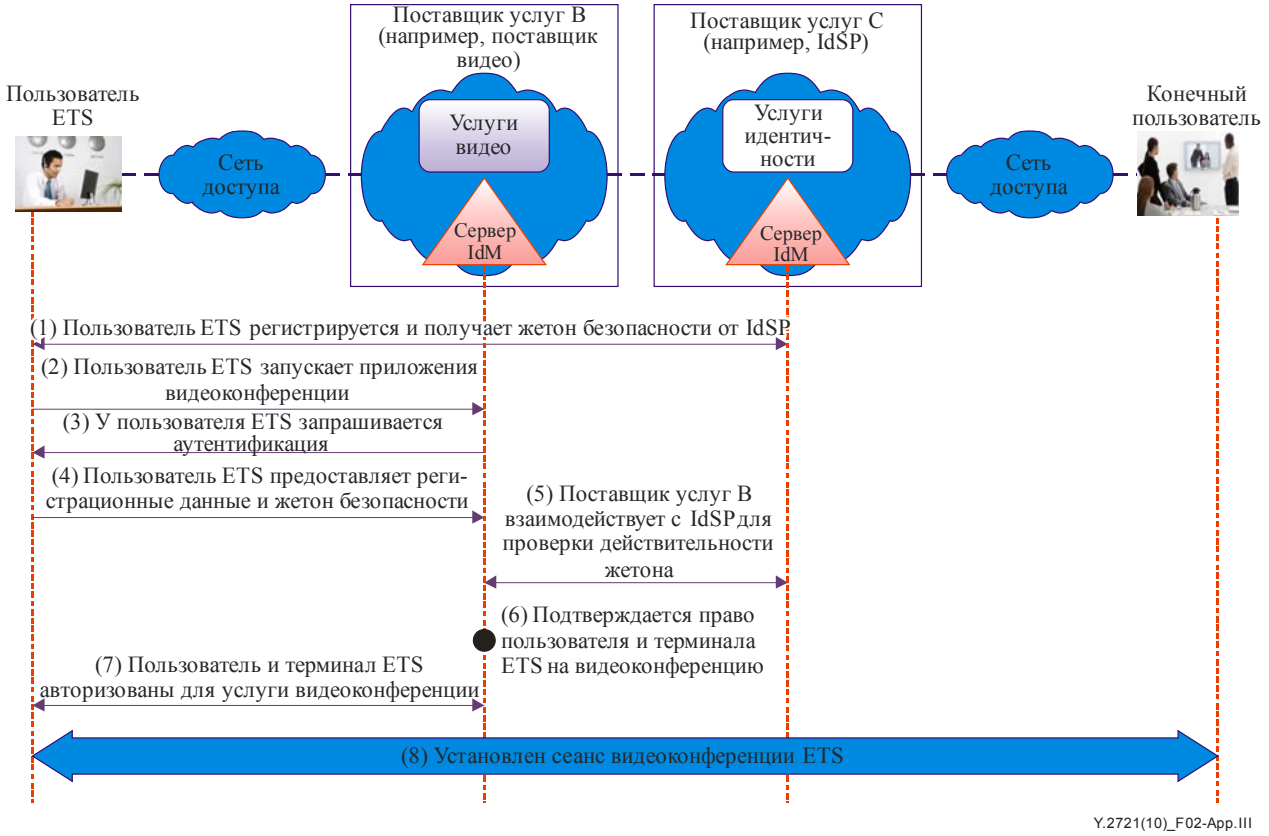
9) Сервер IdM коррелирует и связывает информацию пользователя и устройства ETS для расширенной аутентификации и авторизации.

10) Сеанс связи ETS авторизован.

В результате этого примера потоков дается расширенная гарантия идентичности пользователя ETS и авторизация на использование услуги. Комбинирование аутентификации устройства с пользователем потребует дополнительного взаимодействия с пользователем ETS для аутентификации и может считаться обременительной. Однако это может не потребоваться для всех сеансов ETS. Это может рассматриваться для сеансов ETS, требующих более высокой степени гарантии.

III.3 Улучшенная аутентификация пользователей ETS для приоритетных услуг последующих поколений (приоритетных мультимедийных услуг)

Так как среда передачи переходит в среду СПП/IMS, пользователям ETS потребуется следить за техническим развитием и новыми тенденциями в области связи. Например, пользователи ETS при выполнении своих задач все больше становятся зависимыми от услуг связи помимо голосовой связи (например, мгновенных сообщений, текстовых сообщений и электронной почты). В целом существуют инициативы на этапах планирования и развития, чтобы позволить пользователям ETS получать приоритетный доступ к мультимедийным услугам (например, услуги передачи голоса, данных и видео). Однако механизмы на основе PIN и подписки, используемые для ETS в условиях КТСОП, будут недостаточными для мультимедийных услуг в условиях СПП/IMS. В частности, такие приложения, как приоритетные мультимедийные сообщения (например, услуги передачи данных и видео), потребуют большее высокой степени гарантии или уверенности в идентичности пользователя ETS и более высокого уровня авторизации для доступа к приложениям ETS и их соответствующим ресурсам из-за более высокого уровня рисков и угроз безопасности в среде СПП в целом. Кроме того, в отличие от существующих ETS, которые поддерживаются КТСОП, ожидается, что авторизация для использования приоритетных мультимедийных услуг последующих поколений может предоставляться только определенной группе пользователей ETS. Далее, учитывая общие задачи предоставления пользователям ETS простого и удобного доступа из любой точки, в любое время и с любого устройства, важно разрабатывать и использовать более современные механизмы IdM. Высокая степень гарантии в идентичности пользователя ETS будет крайне важна для защиты целостности и доступности мультимедийных услуг и ресурсов ETS и всей инфраструктуры СПП/IMS в целом во время стихийных бедствий и чрезвычайных ситуаций. Мультимедийные приложения передачи данных и видео (например, загрузка информации из сети или видеоклипов) требуют более широкую полосу пропускания и больше ресурсов, чем голосовые приложения. Без необходимого контроля несанкционированный доступ к приложениям ETS по передаче данных и видео может оказать негативное влияние на сами приложения ETS и всю инфраструктуру связи в целом. Например, несанкционированный доступ к приложениям ETS с интенсивным использованием ресурсов может привести к перегрузке сети или к атакам "отказ в обслуживании". Поэтому для аутентификации и авторизации пользователей и/или терминалов ETS необходимо рассматривать более сложные подходы, использующие особые жетоны безопасности, цифровые сертификаты, возможности голосового или биометрического распознавания.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.2 – Расширенная аутентификация для приоритетных услуг последующих поколений

На рисунке III.2 показан пример случая использования, включающий расширенную аутентификацию авторизованных пользователей для приоритетных услуг последующих поколений (например, видеоконференции). Этот случай предполагает, что полномочия идентичности (т. е. жетоны безопасности или цифровые сертификаты) представлены IdSP, который не является поставщиком мультимедийных услуг (хотя возможно, что поставщик услуг и IdSP являются одним лицом). Если IdSP и поставщик услуг – разные лица, то потребуется заранее установить необходимые коммерческие и доверенные отношения. Также потребуется взаимная аутентификация между IdSP и поставщиком услуг.

Далее кратко представлен поток вызовов:

1) Пользователь ETS регистрируется и получает полномочия (т. е. жетоны безопасности или цифровые сертификаты), идентифицирующие пользователя ETS и привилегии для мультимедийных услуг.

2) Пользователь ETS инициирует приложение видеоконференции.

3) У пользователя ETS запрашивается аутентификация.

4) Пользователь ETS предоставляет полномочия (например, жетоны безопасности или цифровые сертификаты) для аутентификации.

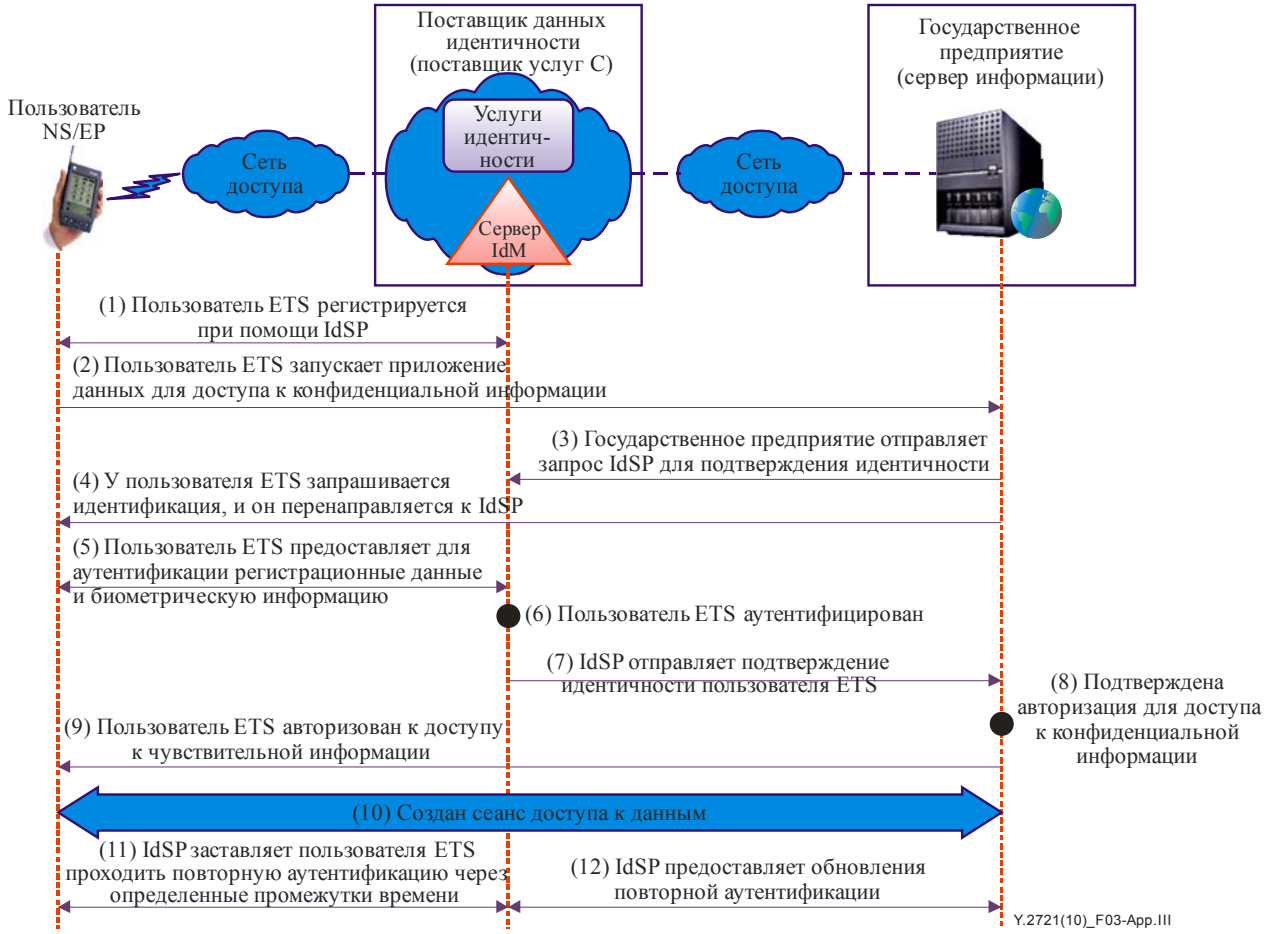
5) Поставщик услуг B взаимодействует с поставщиком услуг определения идентичности (IdSP), запрашивая подтверждение полномочий (например, жетонов безопасности или цифровых сертификатов).

6) Поставщик услуг B обрабатывает и подтверждает информацию для определения того, имеют ли право пользователь и терминал ETS использовать приоритетные мультимедийные услуги.

7) После успешной аутентификации пользователь ETS получает авторизацию для запуска приоритетной мультимедийной услуги (например, видеоконференции).

8) Мультимедийный сеанс настроен и установлен.

Определенные мультимедийные средства связи последующих поколений могут потребовать применения биометрической информации для аутентификации авторизованного пользователя ETS. Например, конфиденциальный характер информации определенного типа может потребовать, чтобы она находилась в совместном пользовании только подгруппы авторизованных пользователей ETS. В таком сценарии крайне важна высокая степень уверенности в утверждении идентичности пользователя ETS. В таких случаях в качестве технологий утверждения могут рассматриваться биометрические механизмы.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.3 – Пример случая использования биометрических данных

На рисунке III.3 показан пример случая использования, включающий биометрические данные. В этом примере подразумевается, что телефон пользователя имеет необходимые функции для считывания биометрической информации. Также подразумевается, что пользователь ETS уже зарегистрирован у IdSP, и необходимая биометрическая информация получена и сохранена. Следует заметить, что также возможно, что государственное предприятие будет хранить и предоставлять услуги идентичности (например, регистрировать и хранить биометрическую информацию и информацию идентичности пользователя ETS), а не использовать услуги поставщика третьей стороны. Далее кратко представлен поток вызовов:

1) ETS регистрируется у IdSP для активации услуги биометрической аутентификации. Подразумевается, что необходимый процесс сбора и подтверждения биометрической и другой информации идентичности уже закончен (например, личная регистрация).

2) Пользователь ETS инициирует соединение для удаленного доступа к базе данных государственного предприятия, содержащей конфиденциальную информацию.

3) Правила безопасности государственного предприятия указывают, что необходима высокая степень гарантии, чтобы позволить доступ, и инициируют процедуру перенаправления к IdSP.

4) Пользователю ETS направляется запрос на аутентификацию и перенаправляется у IdSP.

5) Пользователь ETS предоставляет данные для аутентификации. Например, отпечаток большого пальца на специальном биометрическом сканере, встроенном в беспроводный телефон.

6) IdSP использует входные данные для аутентификации пользователя ETS.

7) IdSP направляет государственному предприятию информацию, подтверждающую идентичность пользователя ETS.

8) Государственное предприятие проверяет, авторизована ли идентичность ETS для доступа к серверу информации, содержащему конфиденциальные данные.

9) ETS авторизована для доступа.

10) Установлен сеанс доступа к данным.

11) IdSP отвечает пользователю ETS запросом на повторную идентификацию после определенных промежутков времени как результат применения политики безопасности для доступа к серверу информации государственного предприятия.

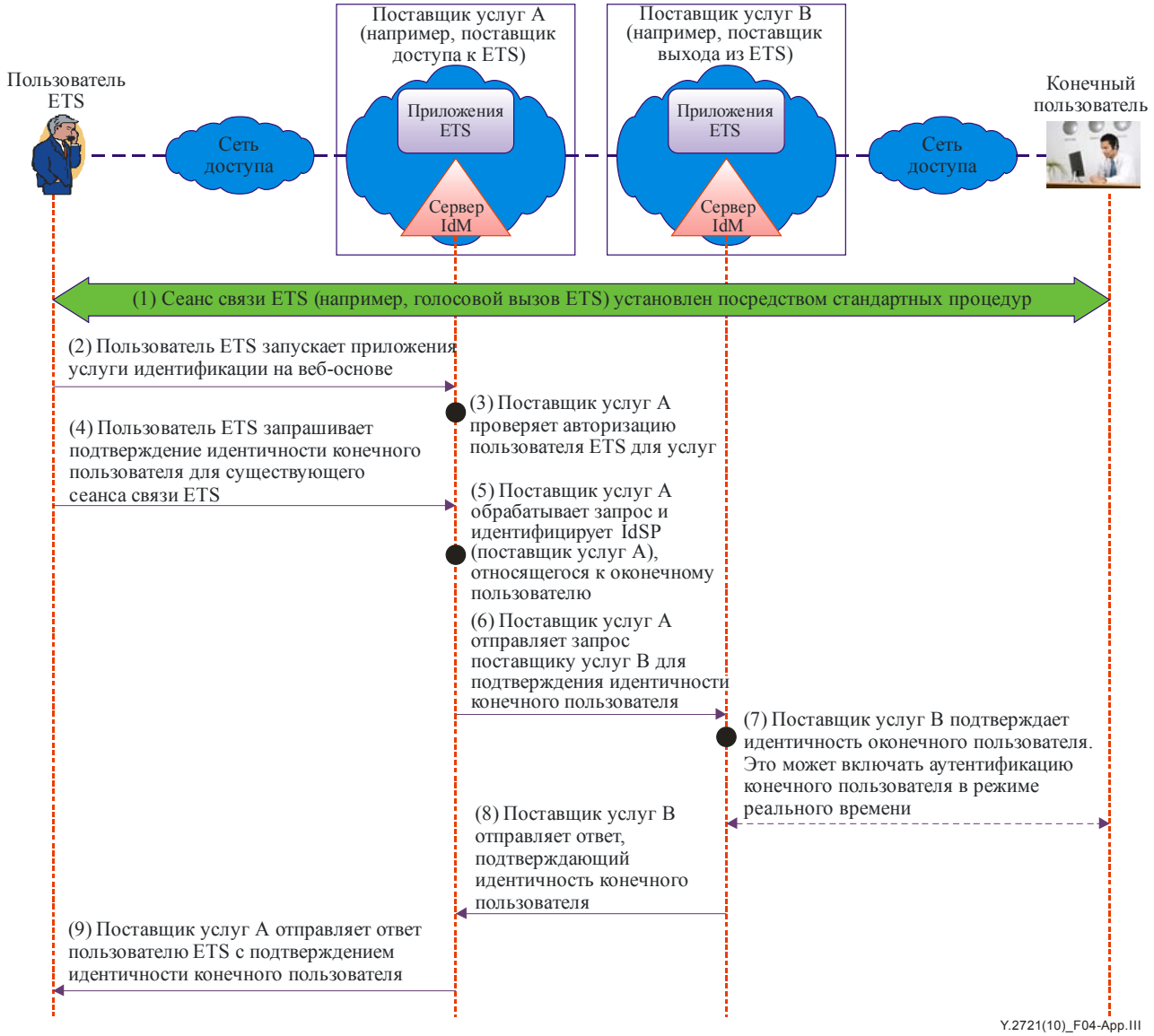
12) IdSP предоставляет государственному предприятию информацию о повторной аутентификации пользователя ETS.

III.4 Аутентификация вызываемой стороны и источников передачи данных

В настоящее время не существует определенных механизмов, являющихся частью самих приложений ETS, для аутентификации вызываемой стороны в сеансе связи (т. е. стороны, завершающей вызов ETS). В закрытой среде КТСОП это не было большой проблемой. Однако переход к среде СПП/IMS с IP транспортом дает возможность подделать номер вызываемой стороны и направить информацию, создав замаскированные угрозы.

В будущем можно будет использовать услуги управления определением идентичности, предлагаемые поставщиками услуг связи (CSP) и поставщиками услуг третьей стороны, для аутентификации вызываемой стороны или стороны, завершающей сеанс связи ETS. В частности, поставщик услуг ETS может поддерживать возможности IdM для предоставления услуг идентификации для аутентификации пользователей и утверждения идентичности пользователей. Примером информации идентичности может быть простая проверка линии и имени вызывающей стороны или использование более мощных механизмов аутентификации (например, жетонов безопасности, смарт-карт или цифровых сертификатов) для обеспечения идентичности пользователей.

На рисунке III.4 приведен пример использования, включающий подтверждение конечного пользователя сеанса связи ETS (например, голосового вызова ETS). В частности, этот случай использования подразумевает, что пользователь ETS заранее зарегистрировался у поставщика услуг ETS для услуг идентичности на веб-основе. После установления связи ETS (например, голосового вызова ETS) с пользователем из сети общего пользования, пользователь ETS инициирует услугу идентификации при помощи веб-портала для верификации идентичности завершающего вызов пользователя на другой стороне сеанса связи ETS. В этом случае создание сеанса связи ETS не зависит от услуг идентичности, которые применяются для обеспечения идентичности конечного пользователя.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.4 – Утверждение идентичности конечного пользователя

Далее кратко представлен поток вызовов и взаимодействия:

1) Пользователь ETS начинает сеанс связи ETS (например, голосовой вызов ETS). Сеанс связи ETS установлен посредством стандартных процедур.

2) Пользователь ETS инициирует услугу идентичности на веб-основе (например, через веб-портал поставщика услуг A, поставщика доступа к ETS) для проверки пользователя на оконечной стороне установленного сеанса связи ETS.

3) Поставщик услуг A проверяет авторизацию ETS для услуги.

4) Пользователь ETS запрашивает проверку идентичности пользователя на оконечной стороне установленного сеанса связи.

5) Поставщик услуг A обрабатывает запрос и определяет IdSP, связанного с конечным пользователем (т. е. поставщика выхода из ETS).

6) Поставщик услуг A направляет запрос поставщику услуг B для утверждения идентичности конечного пользователя.

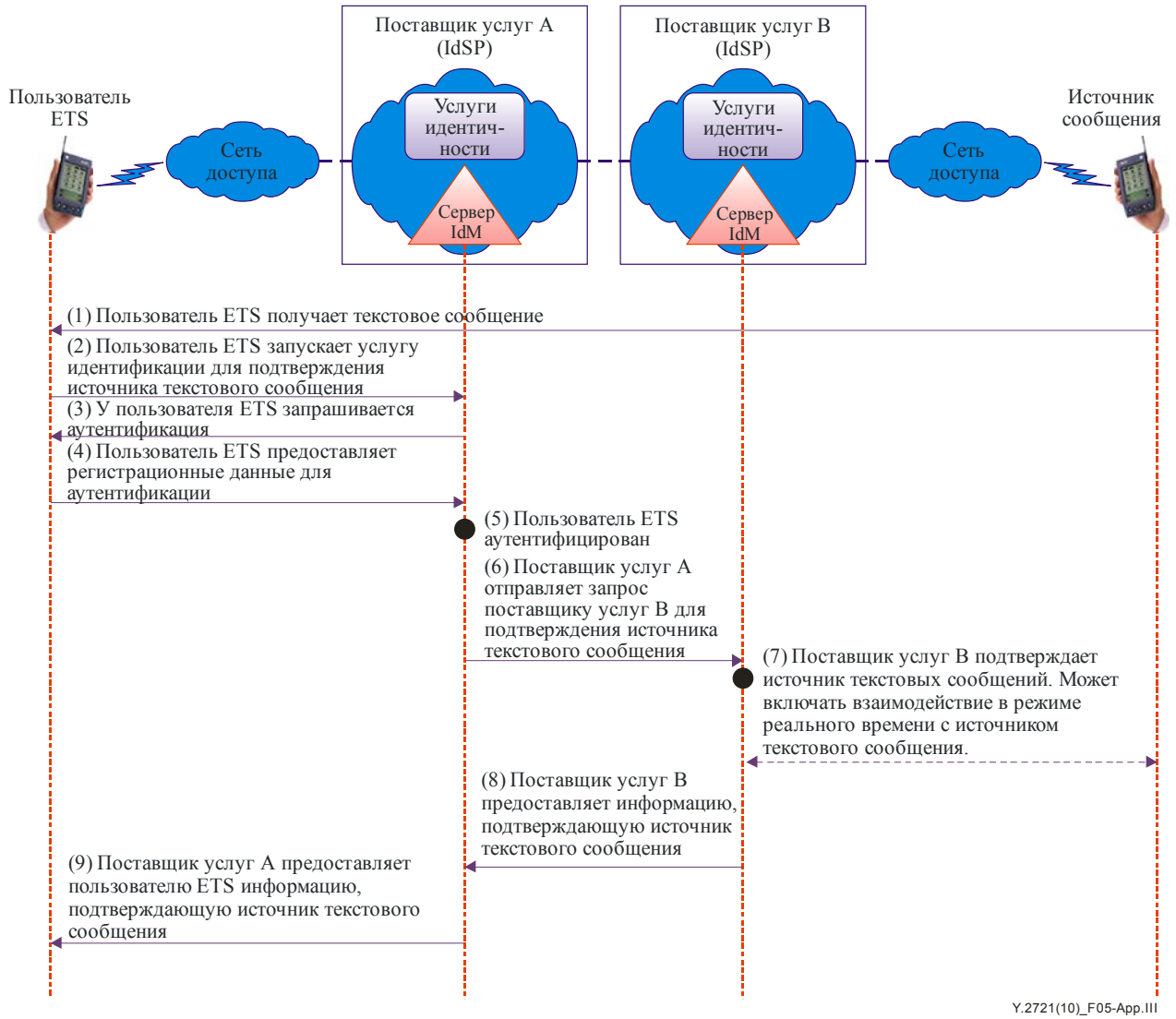
7) Поставщик услуг B верифицирует идентичность конечного пользователя. Это может включать аутентификацию конечного пользователя в режиме реального времени.

8) Поставщик услуг B направляет отклик с утверждением идентичности конечного пользователя.

9) Поставщик услуг A направляет отклик пользователю ETS (например, визуальному веб-дисплею) с утверждением идентичности конечного пользователя сеанса связи ETS.

Пользователи ETS также все шире используют услуги передачи данных (например, электронной почты, служб мгновенного сообщения и текстовых сообщений). В определенных ситуациях может потребоваться аутентифицировать или подтвердить источники таких услуг передачи данных. Учитывая большой объем почтовых отправок, содержащих спам, в период определенных событий в условиях бедствий для пользователей ETS очень важна способность различения и валидации аутентичных сообщений.

На рисунке III.5 приведен пример случая использования, подтверждающий источник текстового сообщения. В этом примере подразумевается, что пользователь ETS получает текстовое сообщение, от источника, которым может быть или не быть другой пользователь ETS. Для того чтобы иметь уверенность в источнике текстового сообщения, используются услуги определения идентичности, предоставляемые поставщиком услуг. Услуги определения идентичности для утверждения источника текстового сообщения могут быть или не быть частью самой службы текстовых сообщений.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.5 – Подтверждение источника текстовых сообщений

Далее приведен краткий порядок взаимодействия:

1) Пользователь ETS получает текстовое сообщение.

2) Пользователь ETS желает проверить аутентичность источника текстового сообщения и инициирует услугу определения идентичности, предоставляемую поставщиком услуг A.

3) У поставщика услуг ETS запрашивается аутентификация.

4) Пользователь ETS предоставляет полномочия для аутентификации.

5) Поставщик услуг A аутентифицирует пользователя ETS и проверяет аутентификацию для услуг определения идентичности.

6) Поставщик услуг A направляет запросы поставщику услуг B для подтверждения источника текстовых сообщений.

7) Поставщик услуг B обрабатывает запросы и подтверждает источник текстовых сообщений. Это может включать взаимодействие с источником текстового сообщения.

8) Поставщик услуг B направляет отклик поставщику услуг A с подтверждением источника текстового сообщения.

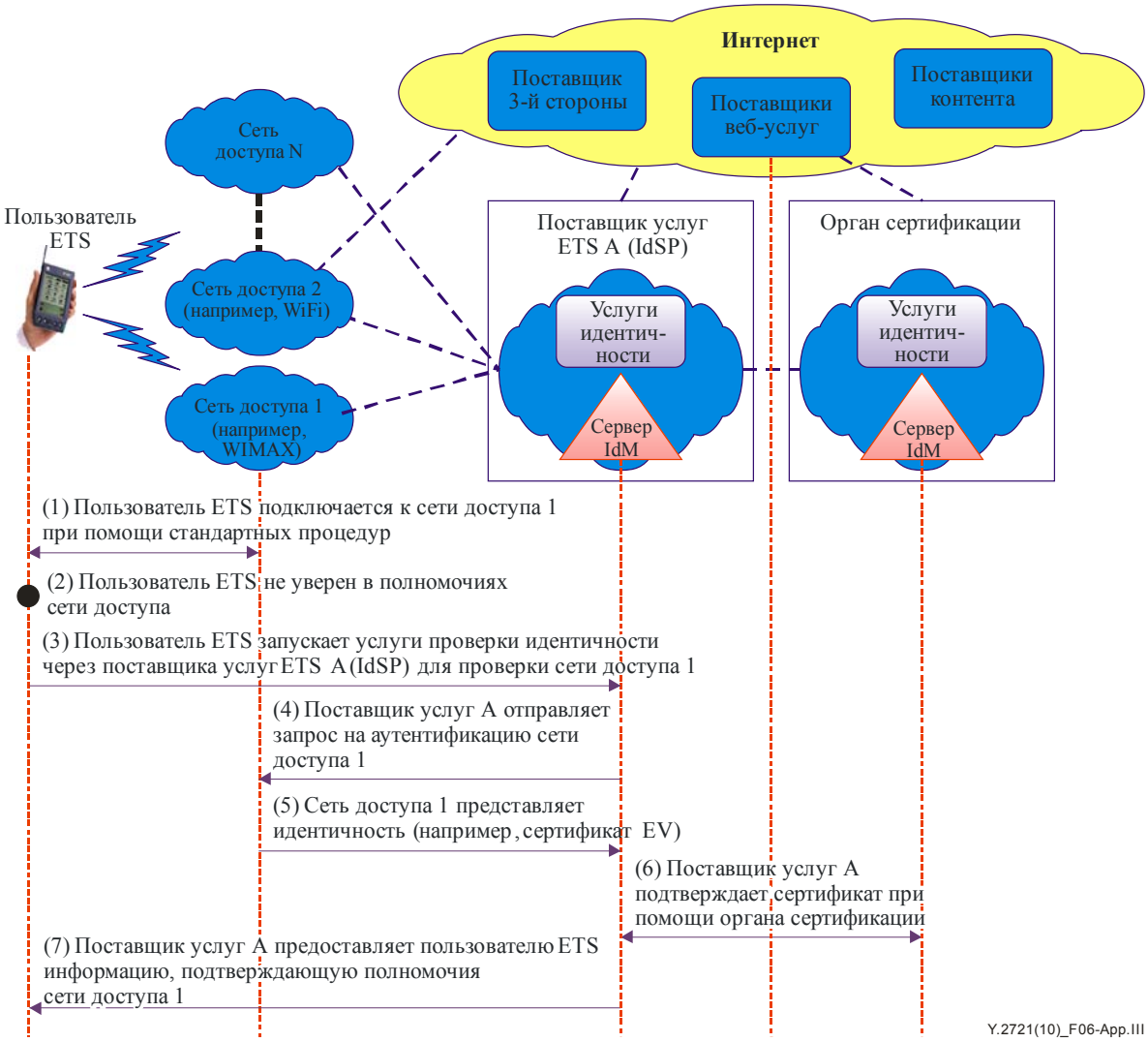
9) Поставщик услуг A направляет пользователю ETS информацию, подтверждающую источник текстового сообщения.

III.5 Доверенная идентификация и аутентификация поставщиков услуг в условиях с несколькими поставщиками

Современная инфраструктура связи позволяет наличие нескольких поставщиков, которые включают нескольких поставщиков доступа к фиксированным и подвижным службам, использующих разные технологии (например, xDSL, кабель, FTTX, WiFi, WiMAX, EV-DO, LTE), поставщиков услуг связи, использующих "управляемые центральные IP сети", поставщиков веб-услуг, поставщиков контента и поставщиков 3-й стороны. В этой среде с множеством поставщиков более недопустимо безоговорочно доверять идентичности поставщика услуг, как это было в условиях КТСОП.

В открытой среде с несколькими поставщиками услуг отсутствуют возможности для обеспечения надежной идентификации, аутентификации и авторизации поставщиков услуг, что может привести к вероятности действий незаконных объектов, которые маскируют, фальсифицируют или искажают услуг законных поставщиков услуг. Поэтому возможности IdM по идентификации и подтверждению поставщиков услуг важны для защиты инфраструктуры. Если поставщики услуг поддерживают услуги ETS, эти возможности важны для национальной безопасности.

На рисунке III.6 представлен пример случая использования ETS, в котором пользователь ETS пытается получить доступ к сети в среде с несколькими поставщиками. В частности, пользователь ETS находится в роуминге, и мобильный телефон потенциально может быть прикреплен к одному из наборов поставщиков сети доступа, предлагающих услуги в этой области (не все поставщики услуг могут быть авторизованными поставщиками услуг ETS). В данном примере случая использования подразумевается, что пользователь ETS по умолчанию прикреплен к сети доступа 1. После прикрепления к сети доступа 1, пользователь ETS пожелает проверить сеть, прежде чем создавать любые конфиденциальные сеансы связи ETS. Существует множество способов и вариаций для рассмотрения проверки поставщика сети, включая прямую аутентификацию пользователем ETS. В этом примере подразумевается, что пользователь ETS использует услуги определения идентичности, предоставляемые поставщиком A услуг ETS, для валидации сети доступа. В данном примере пользователь ETS доверяет поставщику услуг A и примет информацию валидации, которую направит поставщик услуг A относительно сети доступа 1.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.6 – Валидация поставщика услуг доступа

Далее приведен краткий порядок взаимодействия:

1) Пользователь ETS находится в роуминге с мобильным телефоном, который может подключаться к нескольким типов сетей доступа (например, WiFi, WIMAX, LTE или EV-DO). Мобильный телефон пользователя ETS подключается к сети 1 (т. е. выбор по умолчанию на основе таких факторов, как известные поставщики ETS и мощность сигнала).

2) Пользователь ETS желает проверить полномочия сети 1 прежде, чем авторизовать услуги.

3) Пользователь ETS инициирует услуги определения идентичности через поставщика A услуг ETS для проверки сети доступа 1.

4) Поставщик услуг A направляет запрос на аутентификацию сети доступа 1.

5) Сеть доступа 1 предоставляет для аутентификации информацию идентичности (например, сертификат расширенного подтверждения (EV) X.509).

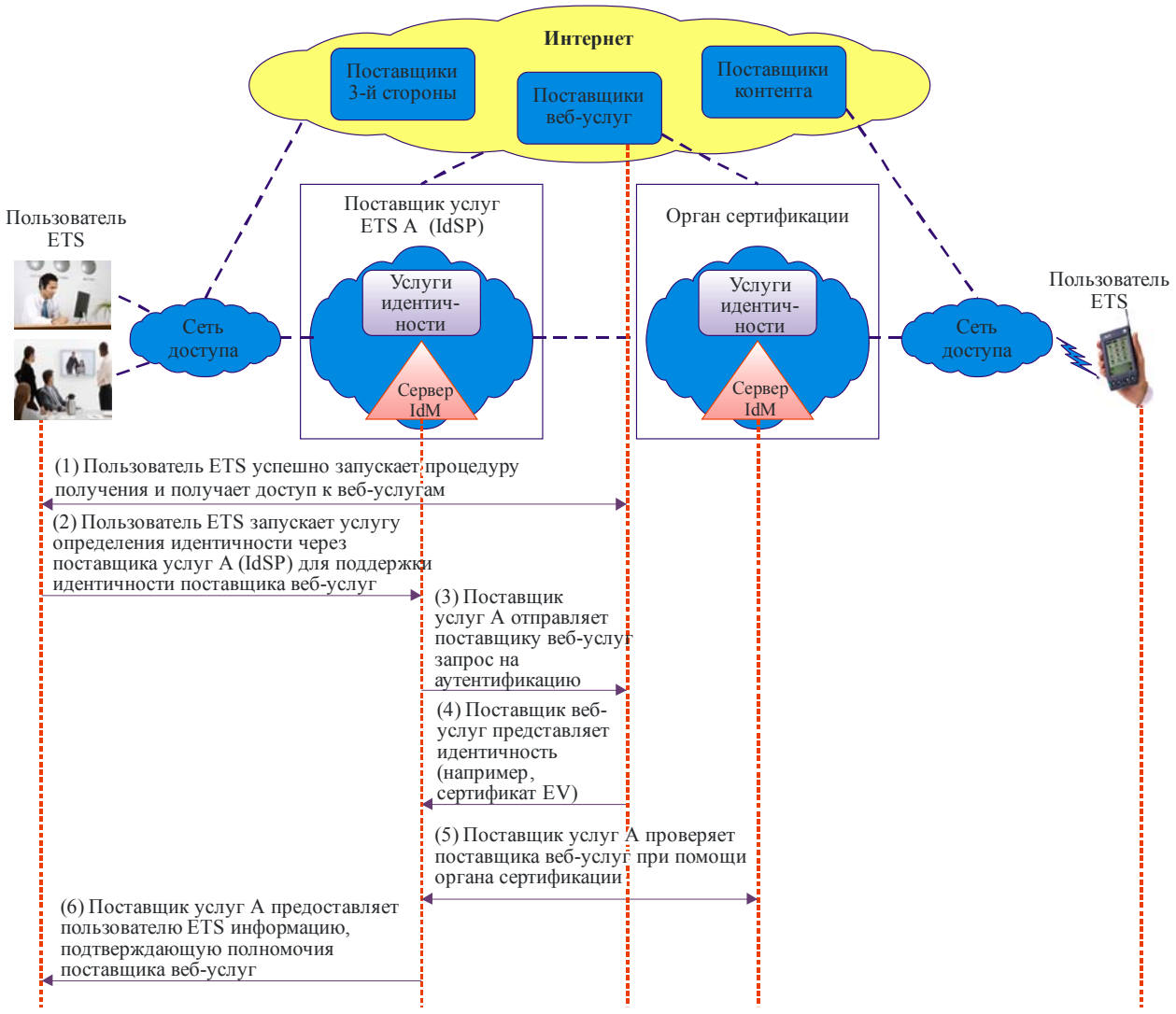
6) Поставщик A услуг ETS верифицирует сертификат сети 1 при помощи органа сертификации.

7) Поставщик A услуг ETS предоставляет пользователю ETS информацию, подтверждающую полномочия сети 1.

Это позволяет пользователю ETS продолжать работу с уверенностью, что его мобильный телефон подключен к авторизованной сети доступа.

После получения доступа к сети пользователь ETS имеет возможность пользоваться услугами нескольких поставщиков услуг в инфраструктуре с множеством поставщиков. Например, возможно, что пользователю ETS потребуется использовать услуги поставщиков веб-услуг (например, поставщиков карт Земли или других карт/данных) или поставщиков контента (например, поставщиков услуг, предлагающих передачу данных в режиме реального времени с камер наблюдения, сводки погоды или видео). Возможно, что пользователь ETS может получить доступ к услугам поставщиков веб-услуг и контента напрямую через доступ в интернет или опосредованно через услуги поставщиков СПП. В любом из этих случаев пользователю ETS может потребоваться проверка поставщика определенной услуги.

На рисунке III.7 показан пример случая использования, когда пользователю ETS требуется проверить идентичность поставщика веб-услуг. Как и в случае использования, приведенном выше, существует множество возможностей и вариантов способов проверки поставщика веб-услуг, включая прямую аутентификацию пользователем ETS. В данном примере предполагается, что для проверки поставщика веб-услуг пользователь ETS использует услуги определения идентичности, предоставляемые поставщиком услуг A. Как и в предыдущем примере, пользователь A ETS доверяет поставщику услуг A и примет направленную им информацию валидации поставщика веб-услуг.



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.7 – Валидация поставщика веб-услуг или контента

Далее приведен краткий порядок взаимодействия:

1) Пользователь ETS успешно инициирует и получает доступ к веб-услугам. Однако пользователь ETS желает осуществить валидацию поставщика веб-услуг, с тем чтобы быть уверенным в данных.

2) Пользователь ETS инициирует услугу определения идентичности поставщика услуг A для валидации поставщика веб-услуг.

3) Поставщик A услуг ETS направляет поставщику веб-услуг запрос на аутентификацию.

4) Поставщик веб-услуг предоставляет информацию для аутентификации (например, сертификат EV[1]).

5) Поставщик A услуг ETS проверяет информацию при помощи Органа сертификации.

6) Поставщик A услуг ETS предоставляет пользователю ETS информацию, подтверждающую идентичность поставщика веб-услуг.

Валидация поставщика веб-услуг позволяет пользователю ETS доверять идентичности веб-услуг, что может повысить доверие к информации, полученной от веб-услуг.

III.6 Однократная регистрация и однократный выход

Обычно пользователи должны регистрироваться в нескольких системах, в которых размещены прикладные услуги (например, VoIP, передача данных и видео), что требует такого же числа диалогов входа, каждый из которых может содержать различные имена пользователей и информацию аутентификации. Администраторы системы должны осуществлять управление учетными записями пользователя в пределах каждой из этих нескольких систем скоординированным образом, для того чтобы поддерживать целостность политики безопасности.

Пользователям ETS может потребоваться использовать возможности IdM (например, "Однократная регистрация/однократный выход"). Преимуществом "Однократной регистрации в системе" является то, что конечный пользователь, устройство или сочетание конечного пользователя и устройства могут войти в систему только однажды (т. е. осуществив ввод полномочий для установления аутентификации и авторизации), и тем самым получить аутентификацию для одной или нескольких дополнительных услуг в одном домене СПП или, в случае федеративных услуг, в нескольких доменах СПП. Ценность однократной регистрации состоит в том, что конечный пользователь не обременен авторизацией для каждой услуги. Термин "Регистрация в системе", используемый здесь, означает то же, что и термин "Регистрация в", "Вход в систему" или "Ввод имени/пароля", когда конечный пользователь/устройство "Регистрируется в", "Входит в систему" или "Вводит имя/пароль" для получения услуги. Подобно этому "Однократный выход из системы" предоставляет возможность избежать необходимости "Выхода из" каждой прикладной услуги в данном сеансе.

Потенциальные преимущества, предоставляемые услугами однократной регистрации в системе/однократного выхода из системы, для пользователей ETS могут включать:

- Сокращение времени, затрачиваемого пользователями при операции входа в каждый отдельный домен, включая снижение количества ошибок при регистрации. Усиление безопасности благодаря сокращению потребности для пользователя использовать и запоминать несколько наборов информации аутентификации.
- Уменьшение затрат времени системных администраторов на добавление и удаление в системе пользователей или изменение их прав доступа.
- Усиление безопасности благодаря расширению возможности администраторов системы поддерживать целостность конфигурации счета пользователя, включая возможность запретить или удалить доступ отдельного пользователя ко всем ресурсам системы скоординированным и последовательным способом.

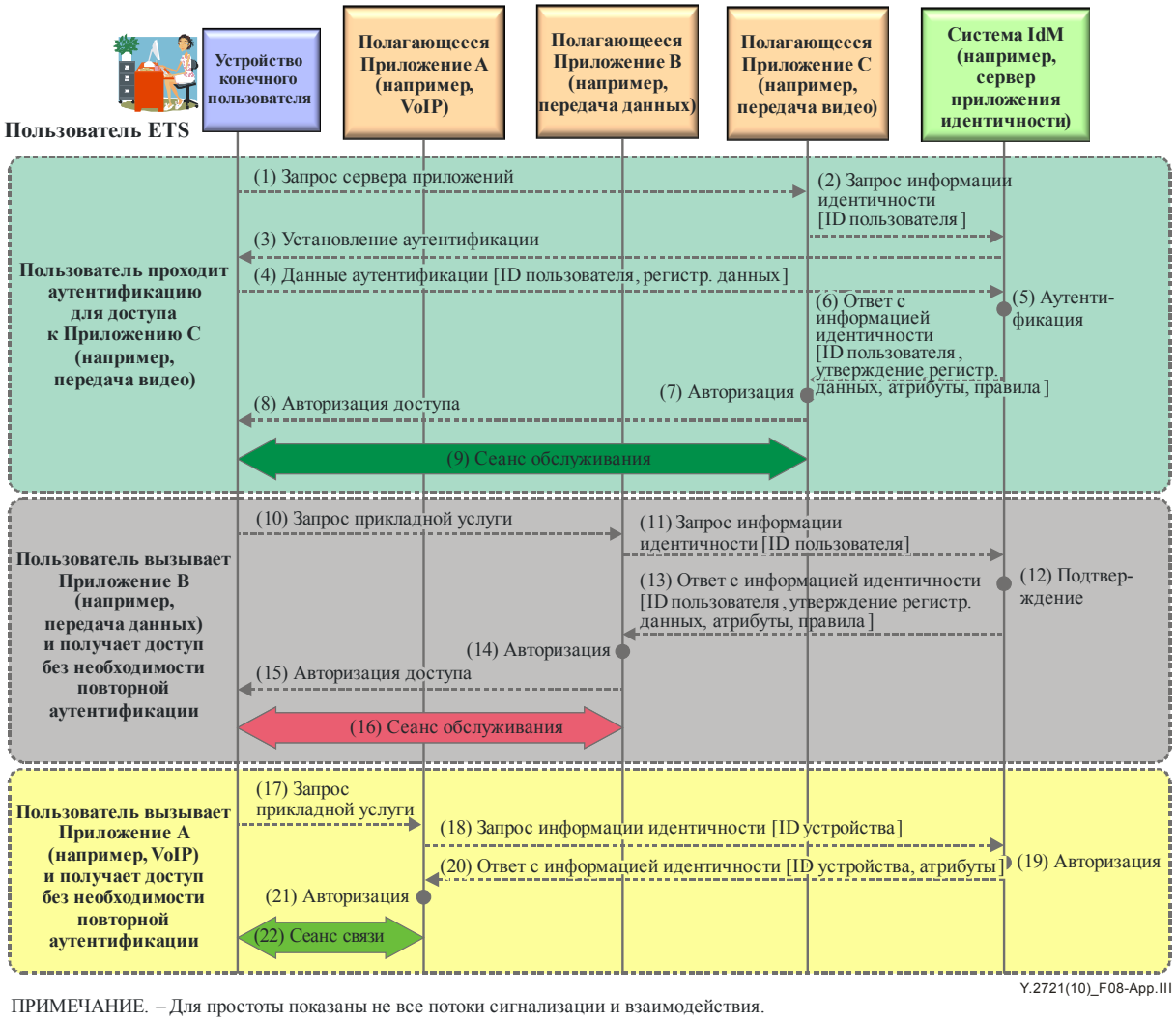
На рисунке III.8 приведен пример случая использования, включающий использование системы IdM для поддержки "Однократной регистрации/однократного выхода" с несколькими прикладными услугами (например, VoIP, передача данных и видео) в пределах домена поставщика СПП. Случай использования включает взаимодействие между следующими объектами:

- Конечные пользователи (т. е. конечный пользователь и/или устройство конечного пользователя).

---

[1] Сертификаты расширенной валидации являются особым типом сертификата X.509, который до выдачи требует всестороннего исследования запрашиваемого объекта органом сертификации.

- Доверяющая система (т. е. прикладная услуга или сетевая система).
- Система IdM (т. е. сетевая система, предоставляющая услуги IdM, такие как регистрация, аутентификация и авторизация, информация профиля подписки).



ПРИМЕЧАНИЕ. – Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.8 – Однократная регистрация в системе

В данном примере подразумевается, что устройство конечного пользователя регистрируется и подключается к СПП при помощи стандартных процедур.

Последовательность операций при обработке вызова выглядит следующим образом:

1) Запрос сервера приложений. Запрос конечного пользователя ETS для вызова прикладной услуги C (передача видео).

2) Запрос информации идентичности [ID пользователя]. Прикладная услуга C (передача видео) направляет системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Это может включать такую информацию как профиль услуги, привилегии, предпочтения и информацию о политике, например, это может быть любая политика или ограничения, связанные с идентичностью.

3) Запрос аутентификации. Система IdM направляет пользователю запрос на получение аутентификации.

4) Ввод данных аутентификации [Полномочия]. Пользователь предоставляет информацию для аутентификации (например, ID пользователя и пароль или личный идентификационный номер).

5) Аутентификация. Система IdM выполняет аутентификацию и получает другую необходимую информацию. Она может содержать информацию, получаемую от других систем сети (например, HSS или другой абонентской базы данных).

6) Ответ с информацией идентичности [Утверждения полномочий, атрибуты, политика]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

7) Авторизация. Прикладная услуга C (передача видео) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

8) Авторизация доступа. Прикладная услуга C (передача видео) предоставляет пользователю указание о том, что доступ к услуге разрешен.

9) Сеанс прикладной услуги. Установлен успешный сеанс пользователя с прикладной услугой C (передача видео).

10) Запрос прикладной услуги. Пользователь активизирует прикладную услугу B (передача данных).

11) Запрос информации идентичности [ID пользователя]. Прикладная услуга B (передача данных) направляет запрос системе IdM на подтверждение идентичности пользователя и предоставления атрибутов, связанных с ID пользователя. Они могут включать информацию, такую как профиль услуги, привилегии, предпочтения и информацию о политике. Например, любую политику или ограничения, связанные с идентичностью.

12) Верификация. Система IdM обрабатывает запрос, определяет, что применима однократная регистрация и подтверждает, что аутентификация пользователя еще действительна.

13) Ответ с информацией идентичности [Утверждение полномочий, атрибуты, политика]: система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID пользователя (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение, касающееся использования, воспроизведения и распространения).

14) Авторизация. Прикладная услуга B (передача данных) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

15) Авторизация доступа. Прикладная услуга B (передача данных) предоставляет пользователю указание о том, что доступ к услуге разрешен.

16) Сеанс прикладной услуги. Создан успешный сеанс пользователя с прикладной услугой B (передача данных).

17) Запрос прикладной услуги. Пользователь запрашивает активизацию прикладной услуги A (VoIP).

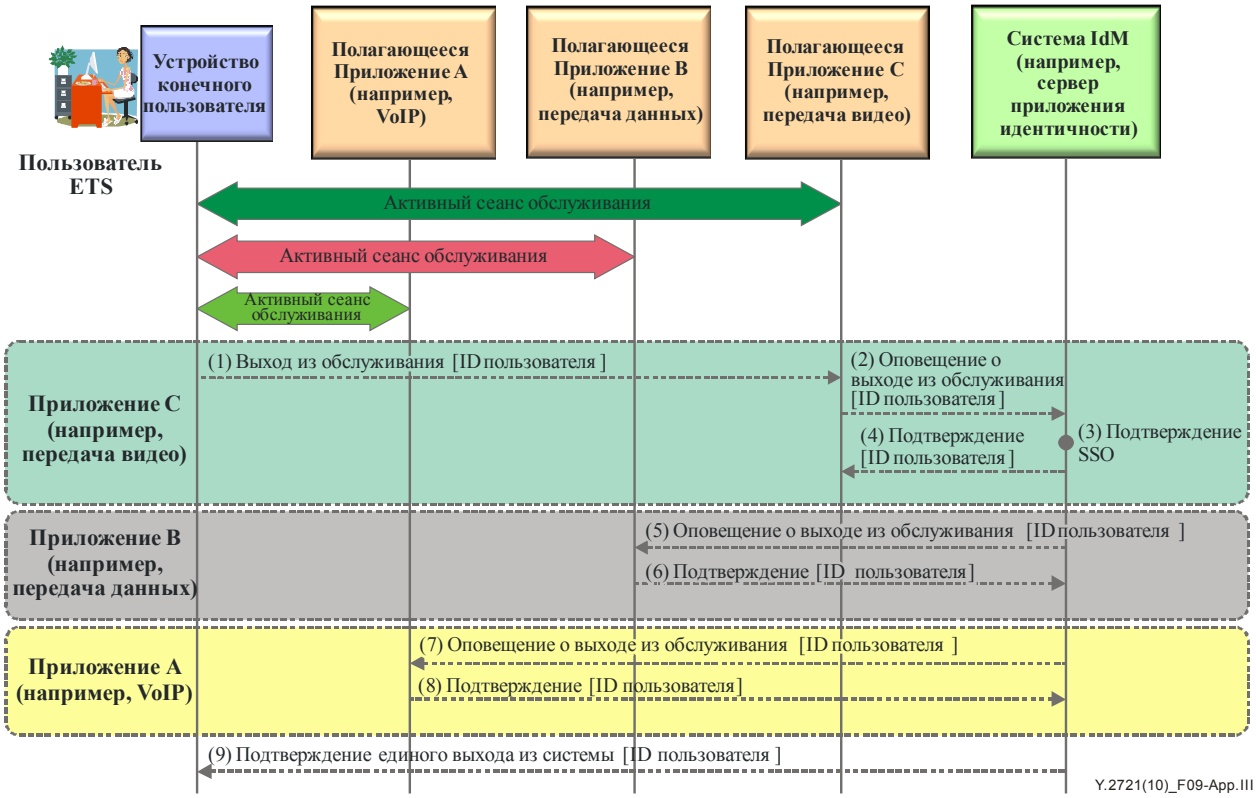
18) Запрос информации идентичности [ID устройства]. Прикладная услуга A (VoIP) направляет запрос системе IdM для утверждения идентичности пользователя и предоставления атрибутов, связанных с ID устройства.

19) Верификация. Система IdM обрабатывает запрос и определяет, что применима однократная регистрация в системе, и проверенная аутентификация пользователя еще действительна.

20) Ответ с информацией идентичности [Утверждение полномочий, атрибутов, политики]. Система IdM предоставляет информацию, утверждающую полномочия. Другой информацией, которая может быть включена, являются атрибуты, связанные с ID устройства (например, привилегии и предпочтения), и политика, связанная с информацией идентичности (например, любое ограничение использования, воспроизведения и распространения).

21) Авторизация. Прикладная услуга A (VoIP) обрабатывает информацию и определяет, что пользователь авторизован для получения услуги.

22) Сеанс прикладной услуги. Пользователь устанавливает сеанс с прикладной услугой A (VoIP).



ПРИМЕЧАНИЕ.– Для простоты показаны не все потоки сигнализации и взаимодействия.

Рисунок III.9 – Однократный выход из системы

Рисунок III.9 иллюстрирует услугу "Однократный выход из системы", обеспечивающую пользователю возможность автоматического выхода из нескольких прикладных услуг (VoIP, передача данных и видео) без необходимости выхода из каждой услуги в сеансе. В данном случае подразумевается, что пользователь находится в активном сеансе связи с прикладными услугами A (VoIP), B (передача данных) и C (передача видео).

Потоки вызовов следующие:

1) Выход из обслуживания [ID пользователя]. Пользователь ETS направляет запрос на окончание сеанса обслуживания.

2) Уведомление о выходе [ID пользователя]. Прикладная услуга C (передача видео) уведомляет систему IdM о запросе пользователя на выход из системы.

3) Верификация SSO. Система IdM определяет, что применим однократный выход из системы, и проверяет активные прикладные услуги.

4) Подтверждение [ID пользователя]. Система IdM направляет подтверждение прикладной услуге C (передача видео) об окончании сеанса обслуживания.

5) Уведомление о выходе из системы [ID пользователя]. Система IdM уведомляет прикладную услугу B (передача данных) о выходе из системы.

6) Подтверждение [ID пользователя]. Прикладная услуга B (передача данных) подтверждает выход из системы.

7) Уведомление о выходе из системы [ID устройства]. Система IdM уведомляет прикладную услугу A (VoIP) о выходе из системы.

8) Подтверждение [ID устройства]. Прикладная услуга A (VoIP) подтверждает выход из системы.

9) Подтверждение однократного выхода из системы [ID пользователя]. Система IdM направляет подтверждение пользователю о выходе из всех активных прикладных услуг в сеансе.

Дополнение IV

Случаи использования, относящиеся к подвижной службе

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

IV.1 Введение

В данном разделе представлены примеры случаев использования IdM, относящиеся к подвижной службе. Примеры случаев использования, приведенные в данном разделе, основаны на случаях использования, описанных в Белой книге 3G для Северной и Южной Америки, *Управление идентичностью: Обзор стандартов и технологий для подвижного и фиксированного интернета* [b-3G Americas White Paper].

IV.2 Примеры случаев использования

IV.2.1 Подвижный пользователь с 3G устройством с активной UICC осуществляет доступ к порталу MNO (интернет-магазину) для покупки рингтона.

Участники:

- подвижный пользователь;
- MNO (оператор подвижной связи);
- SP (поставщик услуг), которым является MNO.

Преимущества для пользователя:

- возможность однократной регистрации в системе с доступом к разным услугам MNO.

Основные ограничения:

- SP и MNO находятся в одном круге доверенных лиц (согласно проекту Liberty Alliance).

IV.2.2 Подвижный пользователь с 3G устройством с активной UICC для доступа к интернет-магазину портала MNO; пользователь перемещается по цифровому каталогу товаров, смотрит специальные рекламные акции (например, видеоигры, благодаря которым MNO обладает эксклюзивным правом распространения контента) и совершает покупки, затем он соглашается на перечисление счета за покупки на счет его мобильного телефона; пользователь может загружать видеоигры по защищенной линии связи, перенаправленной с MNO к поставщику контента.

Участники:

- подвижный пользователь;
- MNO (оператор сети подвижной связи);
- SP-a (поставщик услуг), которым является MNO; SP-b, которым является внешний поставщик контента (например, видеоигр).

Преимущества для пользователя:

- возможность однократной регистрации в системе с доступом к MNO и порталу внешнего продавца.

Основные ограничения:

- SP-a – MNO и SP-b – поставщик контента видеоигр находятся в одном круге доверенных лиц.

IV.2.3 Подвижный пользователь использует свой 3G смартфон с активной UICC и находится в роуминге в другой стране; просматривая интернет, пользователь регистрируется в зарубежном автожурнале с платной подпиской и переводит ее на свою кредитную карту (атрибуты из профиля пользователя, хранящиеся у его MNO, избирательно раскрыты для завершения процесса подачи заявки на подписку); платеж авторизован компанией, выдавшей кредитную карту, от лица подвижного пользователя в адрес портала автожурнала.

Участники:

- подвижный пользователь;
- MNO (оператор сети подвижной связи);
- SP-a, который является поставщиком контента (автожурнал); SP-b, который является компанией, выдавшей кредитную карту.

Преимущества для пользователя:

- возможность однократной регистрации в системе с доступом к MNO пользователя и компании, выдавшей кредитную карту;
- возможность использовать свои полномочия, хранящиеся у MNO пользователя, для авторизации платежей у компании, выдавшей кредитную карту, для завершения транзакции с внешним поставщиком контента;
- возможность повторного использования личных атрибутов, хранящихся в профиле абонента MNO пользователя, для завершения подписки на внешние услуги, что сокращает время на повторный ввод этих реквизитов.

Основные ограничения:

- MNO и компания SP-b, выдавшая кредитную карту, находятся в одном круге доверенных лиц;
- SP-a – зарубежный поставщик автожурнала не находится в круге доверенных лиц.

IV.2.4 Подвижный пользователь использует свой 3G ноутбук с активной UICC, находясь в роуминге в другой стране и в зале ожидания в аэропорту, регистрируется на несколько часов в сети WiFi аэропорта; оператор WLAN имеет соглашение с MNO подвижного пользователя и потому может включать счет за пользование WiFi в счет за мобильный телефон; далее подвижный пользователь в среде WiFi посещает несколько веб-порталов, с которыми он часто взаимодействует, включая порталы: банка, агентства путешествий и инвестиционной компании; пользователь хочет использовать услуги, предоставляемые этими веб-коммерсантами, без повторной регистрации, а также иметь возможность безопасно обмениваться конфиденциальной частной информацией.

Участники:

- подвижный пользователь;
- оператор WLAN;
- MNO;
- SP-a, который является MNO; SP-b, который является банком, SP-c, который является агентством путешествий, а SP-d, который является инвестиционной компанией.

Преимущества для пользователя:

- возможность однократной регистрации в системе с доступом к MNO и оператору WiFi;
- возможность использовать свои полномочия, хранящиеся у MNO, для авторизации оплаты услуг WiFi;
- возможность иметь доступ к нескольким поставщикам услуг на веб-основе, не связанных с MNO, используя упрощенную процедуру регистрации и осуществляя безопасную передачу частной информации.

Основные ограничения:

- MNO и оператор WLAN находятся в одном круге доверенных лиц.
- SP-b – банк, SP-c – агентство путешествий и SP-d – инвестиционная компания не находятся в одном круге доверенных лиц.

IV.2.5 Подвижный пользователь использует свой 3G ноутбук с активной UICC, находясь дома и просматривая сеть в рамках своей домашней широкополосной услуги DSL, при помощи которой пользователь получает доступ к порталу своего MNO; пользователь оплачивает счет за услуги подвижной связи (используя свою кредитную карту, заранее авторизованную на сервере) и добавляет новые функции к своему контракту на подвижную связь; затем пользователь переходит на сайт проката кинофильмов и загружает кинофильм, счет за который выставляется на его кредитную карту (заранее не авторизованную).

Участники:

- подвижный пользователь;
- оператор фиксированной сети DSL;
- MNO;
- SP-a, который является MNO; SP-b, который является порталом проката кинофильмов; SP-c, который является компанией, выдавшей кредитную карту.

Преимущества для пользователя:

- возможность однократной регистрации в системе с доступом к своему оператору фиксированной сети и MNO;
- возможность использовать свои полномочия, хранящиеся у своего оператора фиксированной сети, для аутентификации своей учетной записи подвижной службы и заказа дополнительных услуг MNO;
- возможность авторизации оплаты приобретения контента у внешнего поставщика услуг (например, прокат кинофильмов) со своей кредитной карты.

Основные ограничения:

- MNO, оператор фиксированной сети и SP-c – компания, выдавшая кредитную карту, находятся в одном круге доверенных лиц.
- SP-b – поставщик проката кинофильмов не находится в том же круге доверенных лиц.

IV.2.6 Подвижный пользователь с 3G устройством с активной UICC желает получить доступ к ресурсам (например, справочной службе предприятия), находящимся в сети предприятия.

Участники:

- подвижный пользователь;
- MNO;
- система IdM предприятия;
- сервер услуг телефонного справочника предприятия (сервер EDS).

Ниже описаны высокоуровневые взаимодействия между этими участниками. Подвижный пользователь запрашивает услугу у сервера EDS.

- Сервер EDS запрашивает у пользователя аутентификацию.
- Пользователь, получивший аутентификацию от системы MNO, получает полномочия для аутентификации от MNO для аутентификации в системе IdM предприятия.
- Пользователь предоставляет полномочия системе IdM предприятия и после успешной аутентификации получает от нее полномочия для сервера EDS.
- Пользователь отвечает на запрос сервера EDS, представляя полномочия, полученные от системы IdM предприятия.
- Прошедший аутентификацию пользователь получает запрошенную услугу от сервера EDS.

Преимущества для пользователя:

- Подвижный пользователь может получить доступ к ресурсам, доступным в его корпоративной сети (например, справочнику предприятия), экономичным способом, выполняя строгие требования безопасности, обычно применяемые корпоративными службами IT (информативных технологий).

Основные ограничения:

- Система IdM предприятия может потребовать двухфакторную аутентификацию (например, ID пользователя/пароль/PIN) дополнительно к предоставленным MNO полномочиям пользователя.
- Системы IdM MNO и предприятия находятся в одном круге доверенных лиц.

Дополнение V

Пример моделей транзакций IdM

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

V.1 Введение

В настоящем Дополнении представлены примеры моделей транзакций IdM. Модели, представленные в данном Дополнении, описываются в [b-ITU-T X.1250]. Также возможны другие модели, выходящие за рамки данного Дополнения.

V.2 Примеры возможных моделей транзакций управления определением идентичности

Одной из главных транзакций в управлении определением идентичности является базовый процесс запроса-ответа, стандартный для большинства процессов структурированного обмена информацией и показанный на рисунке V.1. Самый обычный вид обмена сообщениями включает две стороны, использующие согласованный протокол и информационную модель.

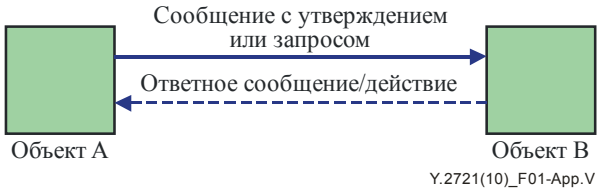


Рисунок V.1 – Стандартный процесс обмена информацией запрос/отклик

Стороны, принимающие участие в данном процессе, могут быть объектами любого вида. Объект может быть физическим лицом, животным, юридическим лицом, организацией, активным или пассивным объектом, устройством, программным приложением, службой и т. д. или их группой. В контексте электросвязи примеры объектов включают точки доступа, абонентов, пользователей, сетевые элементы, сети, программные приложения, службы и устройства, интерфейсы и т. д. Они могут быть физическими или виртуальными объектами (например, сетевое оборудование, программное обеспечение, оконечные устройства, датчики, активно помеченные физические объекты (например, использующие RFID или оптические коды), пассивно помеченные объекты. Сетевые устройства, например, могут рассматриваться как объекты, подчиняющиеся особым возможностям IdM от лица конечных пользователей, поставщиков и государственных учреждений. В контексте управления цифровыми правами объект может быть интеллектуальной собственностью или материалом, защищаемым авторскими правами (например, мультимедийный или IPTV контент). Особым типом объекта является группа. Идентичность группы является местом пересечения идентичностей (общих атрибутов) членов группы.

Большинство случаев управления определением идентичности включают комплексные модели. Например, когда доверяющая сторона, которая сначала получает заявление, не является поставщиком услуг идентичности и, как показано на рисунке V.2 или V.3, функция поставщика услуг идентичности разделена и отделена от доверяющей стороны; доверяющая сторона оценивает запросы от поставщиков услуг идентичности и решает, достаточен ли уровень гарантирования аутентификации объекта. Основной функцией поставщика услуг идентичности является управление созданием, обновлением, проверкой, приостановкой и удалением информации идентичности.

Существует множество возможных моделей обмена информацией идентичности. Одной из часто применяемых моделей является трехсторонняя модель запроса-отклика, показанная на рисунке V.2. В этой модели были спрогнозированы некоторые новые открытые протоколы IdM.

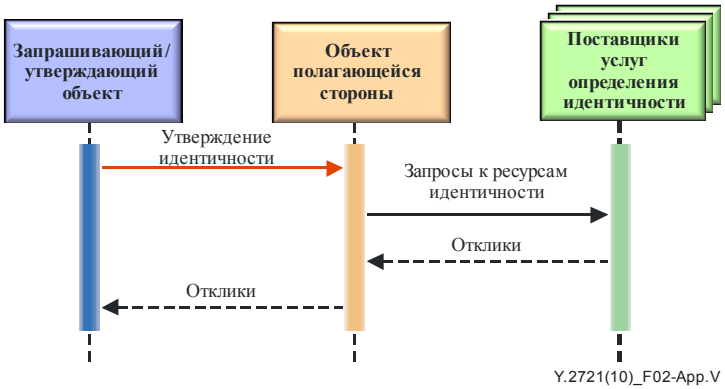


Рисунок V.2 – Пример трехсторонней модели управления идентичностью

Другая модель управления идентичностью, дающая запрашивающей стороне больший контроль над взаимоотношениями идентичности, показана на рисунке V.3.

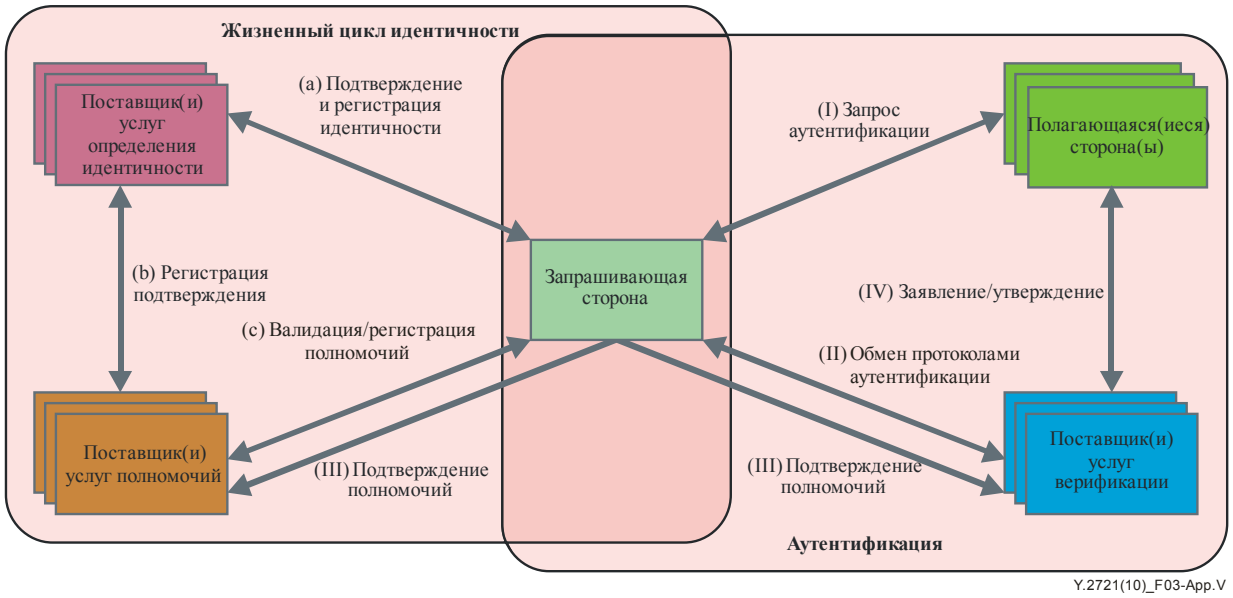


Рисунок V.3 – Пример пятисторонней модели управления, ориентированной на пользователя

Моделям, "ориентированным на пользователя" (т. е. требующим обеспечения полного контроля запрашивающей стороны над использованием своей идентичности) уделяют значительное внимание, и они также могут быть переданы под национальное и региональное управление. На рисунке V.3 приведен пример, когда особые роли и возможности управления идентичностью предоставлены разными поставщиками услуг. Все запросы/отклики направляются через запрашивающую сторону. Для целей такого рода модели, объекты определяются следующим образом.

- Поставщик услуг определения идентичности: объект, поддерживающий, управляющий и имеющий право создавать надежную информацию идентичности других объектов (например, конечных пользователей, организаций и устройств) и предлагать услуги на основе идентичности. Этот объект отвечает за присвоение и выдачу атрибутов (т. е. с участием идентичности (например, для абонента в направлении поставщика полномочий) в определенном контексте), также называемую регистрацией, и за управление жизненным циклом идентичности, который включает подтверждение, регистрацию и поддержку идентичности, включая отзыв.
- Поставщик услуг полномочий: объект, обеспечивающий возможности, связанные с выдачей полномочий и жетонов (например, полномочий, связывающих жетоны с подлежащим верификации идентификаторами и атрибутами).

- Поставщик услуг верификации: объект, обеспечивающий возможности оценки информации идентичности (например, заявлений и полномочий) и классифицирующий ее действительность.
- Полагающаяся сторона [ITU-T Y.2720]: объект, который полагается на представленную или заявленную идентичность запрашивающего/заявляющего объекта в каком-либо контексте запроса.

Дополнение VI

Иллюстративный пример сценария развертывания для IdM в СПП

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

VI.1 Введение

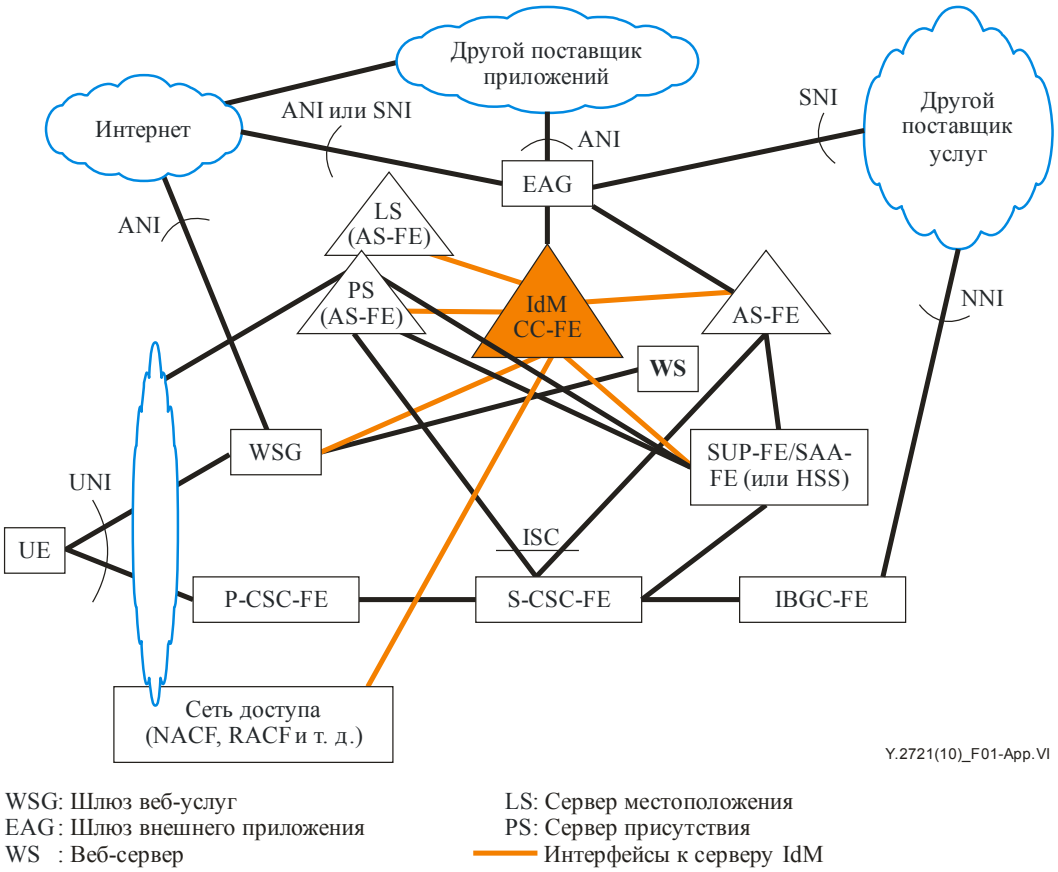
В настоящем Дополнении представлен пример сценария развертывания для IdM в СПП.

VI.2 Развертывание архитектуры IdM

СПП может развертывать инфраструктуру IdM с возможностями, поддерживающими для своих пользователей услуги на основе идентичности, используя возможности и технические условия веб-услуг, определенные в рамках проекта Liberty Alliance и OpenID. Например, возможности IdM, позволяющие пользователям получать услуги в условиях разных поставщиков услуг и приложений, включая федеративные прикладные услуги. Кроме того, СПП может поддерживать возможности IdM для предложения услуг IdSP другим приложениям и поставщикам услуг (например, утверждение идентичности устройства пользователя и аутентификация, местонахождение и другая информация, относящаяся к идентичности).

Поддержка возможностей IdM для предложения услуг IdSP или партнерства с другими поставщиками услуг и приложений, которые используют разные типы систем IdM на основе разных семантик, схем, механизмов и технологий, потребует соответствующих функций сопряжения и взаимодействия для облегчения функциональной совместимости. Так например, для поддержки услуги и возможностей IdM с другими поставщиками приложений и услуг (например, поставщиками веб-услуг и контента), СПП могла бы поддерживать возможности для:

- взаимодействия 3GPP GBA со структурой Liberty Alliance;
- взаимодействия 3GPP GBA с OpenID;
- других механизмов взаимодействия с OpenID и структурой Liberty Alliance.



WSG: Шлюз веб-услуг
EAG: Шлюз внешнего приложения
WS : Веб-сервер
LS: Сервер местоположения
PS: Сервер присутствия
Интерфейсы к серверу IdM

Рисунок VI.1 – Пример развертывания IdM в СПП

Рисунок VI.1 иллюстрирует пример развертывания IdM для СПП. В этом примере показано использование сервера IdM, который может быть автономным устройством или набором функций, которые распределены и/или размещены в HSS. Сервер IdM осуществляет сопряжение и взаимодействие с элементами сети, поддерживающими функциональные объекты, определенные для СПП. Например, сервер IdM может осуществлять взаимодействие с:

- обеспечивающими услугу серверами приложений, например сервером местонахождения (LS) или сервером присутствия (PS) или другими приложениями с целью обеспечения более высокой степени гарантирования аутентификации и поддержки прикладных услуг на основе идентичности;
- серверами присоединения и контроля политики и сети для гарантирования аутентификации и управления политикой.

ПРИМЕЧАНИЕ. – В ряде конкретных национальных регламентах это может означать реализацию отдельных функций IdM в разных стратах СПП.

Для поддержки определенных услуг IdM для пользователей/абонентов и в целях предложения услуг IdSP или установления партнерских отношений с другими поставщиками услуг и приложений, СПП потребуется поддерживать специальные возможности для управления доступом и обмена IdM с другими поставщиками приложений и услуг (например, поставщиками веб-услуг и контента). Этот иллюстративный пример показывает использование шлюза веб-услуг (WSG) и шлюза внешнего приложения (EAG) для поддержки определенных услуг IdM, использующих возможности других поставщиков приложений и услуг или взаимодействующих с ними. В частности, на рисунке VI.1 показан сервер IdM, взаимодействующий с пользователем через шлюз веб-служб (WSG), который аутентифицирует пользователя и предоставляет ему интерфейс для управления своим профилем идентичности. При необходимости также поддерживается взаимная аутентификация пользователя и поставщика услуг. Сервер IdM также взаимодействует со шлюзом внешнего приложения (EAG), который разрешает пользователю доступ к услугам на веб-основе в СПП или от других поставщиков приложений или услуг.

Библиография

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2009), *A framework for user control of digital identity*.

[b-ITU-T Y.2091] Recommendation ITU-T Y.2091 (2008), *Terms and definitions for Next Generation Networks*.

[b-NIST SP 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.

[b-NIST SP 800-94] NIST Special Publication 800-94 (2007), *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-CA/Browser Forum] CA/Browser Forum, *Guidelines For The Issuance And Management Of Extended Validation Certificates*.

[b-3G Americas White Paper] 3G Americas White Paper (2009), *Identity Management, Overview of Standards and Technologies for Mobile and Fixed Internet*.

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	Оконечное оборудование, субъективные и объективные методы оценки
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, 2012 г.