Международный союз электросвязи

МСЭ-Т X.1256

(03/2016)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасность киберпространства –
Управление определением идентичности

Руководящие указания и основа для обмена результатами сетевой аутентификации с сервисными приложениями

Рекомендация МСЭ-Т X.1256

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	**X.1250–X.1279**
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
Рекомендации, связанные с PKI	X.1340–X.1349
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

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

Рекомендация МСЭ-Т X.1256

Руководящие указания и основа для обмена результатами сетевой аутентификации с сервисными приложениями

Резюме

В условиях быстрого развития мобильных устройств и приложений, обеспечивающих доступ в интернет, сетевая среда и среда услуг становятся все более сложными. В результате ощущается настоятельная необходимость в упрощении механизмов аутентификации пользователей для совершенствования опыта пользователей и повышения качества обслуживания.

Многие организации по стандартизации, включая МСЭ-Т, провели обширную исследовательскую работу по созданию единого механизма аутентификации (то есть механизма однократной регистрации входа). Несмотря на это, вся текущая работа в основном направлена на единую аутентификацию сервисных приложений без учета ее связи с сетевой аутентификацией.

С точки зрения сетевых операторов, когда пользователи получают доступ к сети, они проходят сетевую аутентификацию в той или иной форме, но когда они снова входят в систему, чтобы запросить доступ к услуге, их первоначальная сетевая аутентификация более повторно не используется. При принятии механизма обмена результатами аутентификации между услугой и сетью сервисные приложения могут идентифицировать пользователя с применением результатов аутентификации в сети. Такой механизм позволяет пользователю аутентифицироваться сетью только один раз и непосредственно получить доступ к услуге.

В Рекомендации МСЭ-Т X.1256 разработаны руководящие указания для сетевых операторов и поставщиков услуг по обмену результатами сетевой аутентификации и представлена основа для обмена минимальным набором атрибутов между многочисленными услугами в рамках установленных доверительных отношений.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1256	23.03.2016 г.	17-я	11.1002/1000/12605

Ключевые слова

Аутентификация, атрибуты идентификации, аутентификация сетевого уровня.

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

ПРЕДИСЛОВИЕ

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

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

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

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

ПРИМЕЧАНИЕ

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

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

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

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

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

СОДЕРЖАНИЕ

		Стр.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
3.1	Термины, определенные в других документах	1
3.2	Термины, определенные в настоящей Рекомендации	1
4	Сокращения и акронимы	1
5	Соглашения по терминологии	2
6	Механизмы обмена атрибутами аутентификации	2
6.1	Основа	2
6.2	Механизм принудительной доставки сетью	4
6.3	Механизм доставки по запросу услуги	5
7	Аспекты безопасности	6
Дополнение I – Сценарии использования		7
I.1	Сценарии использования принудительной доставки сетью	7
I.2	Сценарий использования доставки по запросу услуги	8
Библиография		10

Рекомендация МСЭ-Т X.1256

Руководящие указания и основа для обмена результатами сетевой аутентификации с сервисными приложениями

1 Сфера применения

В настоящей Рекомендации разработаны руководящие указания для сетевых операторов и поставщиков услуг по обмену результатами сетевой аутентификации и представлена основа для обмена минимальным набором атрибутов между многочисленными услугами в рамках установленных доверительных отношений.

Методы выполнения, интегрирования или реализации аутентификации сетевого уровня сетевыми операторами не входят в сферу применения настоящей Рекомендации.

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 X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта*

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

Отсутствуют.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

2G/3G	Second/Third Generation	Второе/третье поколение
AC	Access Controller	Контроллер доступа
AKA	Authentication and Key Agreement	Соглашение об аутентификации и ключе
AN	Access Network	Сеть доступа
AP	Access Point	Пункт доступа
API	Application Programming Interface	Интерфейс прикладного программирования
AUG	Authentication Gateway	Шлюз аутентификации
BRAS	Broadband Remote Access Server	Сервер широкополосного удаленного доступа
EAP-SIM	Extensible Authentication Protocol Method for (GSM) Subscriber Identity Modules	Метод расширяемого протокола аутентификации для (GSM) модулей идентификации абонента

GGSN	Gateway GPRS Support Node	Узел поддержки шлюза GPRS
GPRS	General Packet Radio Service	Служба пакетной радиосвязи общего пользования
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
IMPI	IP Multimedia Private Identity	Закрытый идентификатор пользователя мультимедийной IP-подсистемы
IMPU	IP Multimedia Public User identity	Открытый идентификатор пользователя мультимедийной IP-подсистемы
IMS	IP Multimedia Subsystem	Мультимедийная IP-подсистема
IMSI	International Mobile Subscriber Identity	Международный идентификатор абонента подвижной связи
IP	Internet Protocol	Протокол Интернет
ISDN	Integrated Services Digital Network	Цифровая сеть с интеграцией служб (ЦСИС)
LoA	Level of Assurance	Уровень гарантии
MSISDN	Mobile Subscriber International ISDN/PSTN Number	Международный номер мобильного абонента в сети ЦСИС/КТСОП
PSTN	Public Switched Telephone Network	Коммутируемая телефонная сеть общего пользования (КТСОП)
RADIUS	Remote Authentication Dial-In User Service	Услуга удаленной аутентификации пользователей по телефонным линиям
SGSN	Serving GPRS Support Node	Обслуживающий узел поддержки GPRS
SIM	Subscriber Identity Module	Модуль идентификации абонента
SIP	Session Initiation Protocol	Протокол инициирования сеанса
SNS	Social Network Service	Услуги социальных сетей
UE	User Equipment	Оборудование пользователя
USIM	Universal Subscriber Identity Module	Универсальный модуль идентификации абонента
URI	Uniform Resource Identifier	Универсальный идентификатор ресурса
WAP	Wireless Application Protocol	Протокол беспроводных приложений
WLAN	Wireless Local Area Network	Беспроводная локальная сеть

5 Соглашения по терминологии

Отсутствуют.

6 Механизмы обмена атрибутами аутентификации

6.1 Основа

При получении доступа к сети оператора пользователям требуется пройти строгую аутентификацию, осуществляемую сетью доступа. Вместе с тем, как правило, возможность данной аутентификации не обеспечивает доступ к услугам. В большинстве случаев конечные пользователи проходят аутентификацию соответственно в сети и в системе предоставления услуг. Например, конечные пользователи аутентифицируются сетью третьего поколения (3G) на основе карты универсального модуля идентификации абонента (USIM), находящейся в их сотовых телефонах (то, что у них есть), однако если они обращаются к какой-то конкретной услуге социальной сети (SNS), необходимо, чтобы веб-сервер вновь аутентифицировал их на основе пары "имя пользователя, пароль", зарегистрированной ранее (то, что им известно).

Основной принцип обмена атрибутами аутентификации заключается в том, чтобы позволить услугам пользоваться атрибутами сетевой аутентификации. Основа для обмена атрибутами аутентификации изображена на рисунке 6.1.

Рисунок 6.1 – Основа для обмена атрибутами сетевой аутентификации с сервисными приложениями

В этой основе есть два типа механизмов обмена атрибутами аутентификации.

- Механизм 1 (механизм принудительной доставки сетью) – передача атрибутов сетевой аутентификации непосредственно сервисным приложениям.

  Если объект управления доступом к сети понимает протокол прикладного уровня, используемый услугой (например, SIP, WAP, HTTP и т. д.), он может вставлять атрибуты сетевой аутентификации в сообщения прикладного уровня и передавать их непосредственно платформе предоставления услуг. В этом случае необходимо определить интерфейс прикладного программирования (API), который будет получать в активном режиме атрибуты аутентификации для сервисных приложений, потому что они лишь пассивно принимают параметры, содержащиеся в заголовках сообщений.

  Сервисные приложения могут принимать решение об анализе и использовании заголовков, вставленных сетью, или о том, чтобы просто их игнорировать. Если сервисным приложениям нужны и другие атрибуты, помимо принудительно доставленных, им следует использовать механизм доставки по запросу услуги.

  Конкретный сценарий использования представлен в Дополнении I.1.

- Механизм 2 (механизм доставки по запросу услуги) – обмен атрибутами сетевой аутентификации через шлюз аутентификации (AUG).

  Если объект управления доступом к сети не может анализировать или изменять сообщения прикладного уровня услуги (например, если протокол прикладного уровня является проприетарным или если обеспечивается защита целостности и/или конфиденциальности

сообщения прикладного уровня), необходимо установить в сети отдельный шлюз AUG для обмена атрибутами аутентификации. AUG реализует строго определенные сетевые интерфейсы API, которые могут быть вызваны сервисными приложениями для получения атрибутов аутентификации от сети.

Кроме того, если сервисным приложениям, указанным в механизме принудительной доставки сетью, требуются и другие атрибуты, помимо принудительно доставленных, им следует использовать данный механизм доставки по запросу услуги для получения дополнительных атрибутов аутентификации от сети.

Конкретный сценарий использования представлен в Дополнении I.2.

6.2 Механизм принудительной доставки сетью

6.2.1 Руководящие указания по реализации

Когда пользователь посещает сеть, объект управления доступом к сети, расположенный на ее границе, аутентифицирует идентичность этого пользователя. К типичным примерам объектов управления доступом к сети относятся устройство, являющееся контроллером доступа (AC) в беспроводной локальной сети (WLAN), обслуживающий узел поддержки GPRS (SGSN) или узел шлюзовой поддержки GPRS (GGSN) в сети службы пакетной радиосвязи общего пользования (GPRS) и сервер широкополосного удаленного доступа (BRAS) в сети фиксированной связи. Объекту управления доступом к сети идентичность пользователя становится известна по результатам сетевой аутентификации.

Если объект управления доступом к сети понимает протокол прикладного уровня, используемый услугой (например, SIP, WAP, HTTP и т. д.), он может инкапсулировать идентичность пользователя и некоторую сопроводительную информацию в сообщения запроса услуги и передавать их платформе предоставления услуг.

Если платформа предоставления услуг доверяет объекту управления доступом к сети, она может непосредственно извлекать идентичность пользователя из запросов услуги и считать, что пользователь уже аутентифицирован.

В этой архитектуре платформе предоставления услуг необходимо определить, доверять или не доверять атрибутам аутентификации, вставленным объектом управления доступом к сети. Для этого сетевому оператору следует заключить договор с поставщиком услуг и предоставить список заслуживающих доверия устройств управления доступом или механизм (например, предварительно опубликованные ключи или цифровые сертификаты) для определения заслуживающих доверия устройств управления доступом. Следует защищать информацию пользователя, передаваемую устройством управления доступом платформе предоставления услуг. Сетевым устройствам управления доступом следует также вести "белый" список платформ предоставления услуг, предусмотренных в договоре. Атрибуты сетевой аутентификации следует передавать только платформам предоставления услуг из "белого" списка. Руководящие указания по установлению этих доверительных отношений не входят в сферу применения настоящей Рекомендации.

6.2.2 Описание интерфейса

Атрибуты сетевой аутентификации вводятся в заголовок сообщений запроса услуги, используемых протоколом приложения (например, SIP или HTTP), и передаются объектом управления доступом к сети платформе предоставления услуг.

Следует включать приведенные ниже атрибуты.

1) Идентичность пользователя.

   Содержимым этого поля является сетевая идентичность пользователя (например, SIP URI, MSISDN, имя пользователя и т. д.). Платформа предоставления услуг может использовать ее для идентификации пользователя.

2) Метод аутентификации с известным уровнем гарантии (LoA) [ITU-T X.1254].

Содержимым этого поля является идентификатор метода аутентификации (например, 2G/3G/4G AKA, IMS AKA, HTTP/SIP Digest, EAP-SIM и т. д.).

Сетевому оператору и поставщикам услуг следует согласовать список распознаваемых идентификаторов методов аутентификации и соответствующих им уровней гарантии.

Любой заданной платформе предоставления услуг следует решать, принимать или не принимать атрибуты аутентификации, принудительно доставленные от сети, с учетом уровня гарантии метода аутентификации и собственной политики в области безопасности.

3) Другие атрибуты, требуемые по договору между оператором и поставщиком услуг.

6.3 Механизм доставки по запросу услуги

6.3.1 Руководящие указания по реализации

Невозможно реализовать механизм принудительной доставки сетью, если объект управления доступом к сети не может анализировать или изменять сообщения прикладного уровня услуги, например если протокол прикладного уровня является проприетарным или если обеспечивается шифрование и защита целостности сообщений услуг. В этом случае, чтобы получить атрибуты сетевой аутентификации, между сетью и платформой предоставления услуг можно разместить AUG, выполняющий для платформы предоставления услуг роль посредника.

Еще одним обстоятельством, оправдывающим использование модели доставки по запросу услуги, является то, что включенные в сообщения атрибуты, которые принудительно доставляются сетью, могут не соответствовать запросу какой-либо конкретной услуги. В этом случае может потребоваться, чтобы платформа предоставления услуг активно взаимодействовала с сетью для получения дополнительной информации об атрибутах сетевой аутентификации.

Для обеспечения возможности использования модели доставки по запросу услуги необходимо, чтобы AUG предоставил набор сетевых API, которые могут быть вызваны прикладными приложениями для получения от сети различной информации о результатах аутентификации. Сеть и платформы предоставления услуг могут использовать различные идентификаторы (ID) для идентификации пользователей. Поэтому в AUG должна содержаться функция преобразования идентификаторов, которая преобразует идентификатор услуги, вызываемой пользователем, в идентификатор сети пользователя, и наоборот.

В этой архитектуре необходимо, чтобы платформа предоставления услуг и AUG доверяли друг другу. Для этого сетевому оператору следует заключить договор с поставщиком услуг и предоставить список заслуживающих доверия устройств AUG или механизм (например, предварительно опубликованные ключи или цифровые сертификаты) для определения заслуживающих доверия устройств AUG. Следует защищать информацию пользователя, передаваемую устройством AUG платформе предоставления услуг. Устройствам AUG следует также использовать механизм авторизации (например, "белый" список) на предоставляемых API, с тем чтобы обмен атрибутами сетевой аутентификации мог осуществляться только с платформами предоставления услуг, предусмотренными в договоре. Руководящие указания по установлению этих доверительных отношений не входят в сферу применения настоящей Рекомендации.

6.3.2 Описание интерфейса

AUG реализует строго определенные сетевые интерфейсы API, которые могут быть вызваны сервисными приложениями для получения атрибутов аутентификации от сети.

Сетевые операторы могут реализовывать API в произвольной форме по своему усмотрению. Определение этих API не входит в сферу применения настоящей Рекомендации.

Атрибуты аутентификации, которыми можно обмениваться таким образом, могут включать любую информацию, касающуюся аутентифицированного пользователя сети, например информацию о местоположении и абонентских данных пользователя, статистические данные об использовании сети пользователем и т. д.

7 Аспекты безопасности

При внедрении технических решений, относящихся к основе, приведенной в пункте 6, необходимо учитывать некоторые аспекты безопасности.

- Крайне важно защищать элементы аутентификации в сети, а также обеспечивать возможность благонадежной и безопасной сетевой аутентификации.
- Системам предоставления услуг следует устанавливать доверительные отношения с сетью, с тем чтобы полагающиеся системы предоставления услуг могли доверять атрибутам аутентификации, передаваемым от сети. Платформе предоставления услуг следует доверять информации об идентичности пользователя, поступающей только от известного сервера аутентификации, с тем чтобы не допускать того, чтобы другой сервер выдавал себя за сервер аутентификации.
- Крайне важно обеспечивать защищенную передачу атрибутов аутентификации платформе предоставления услуг. Следует гарантировать конфиденциальность и целостность информации об идентичности пользователя и следует защищать ее передачу от атак методом воспроизведения и подделки.
- При передаче платформе предоставления услуг результатов аутентификации и другой пользовательской информации следует обеспечивать строгое соблюдение сетью законов и нормативных актов по защите конфиденциальности, действующих в юрисдикциях, в которых предоставляется услуга.
- Платформе предоставления услуг следует надлежащим образом обрабатывать информацию об аутентификации пользователей, полученную от сети, например, обеспечивать безопасное хранение при использовании и немедленное уничтожение после использования. Следует предотвращать злоупотребление пользовательской информацией и ее утечку.

Дополнение I

Сценарии использования

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

I.1 Сценарии использования принудительной доставки сетью

I.1.1 Сеть 2G/3G/4G для услуги WAP

Протокол беспроводных приложений (WAP) является популярной услугой мобильной передачи данных, доступ к которой пользователи могут получить по сетям 2G/3G/4G. После присоединения к сети и аутентификации шлюз WAP может вставлять международный номер мобильного абонента в сети ЦСИС/КТСОП (MSISDN) пользователя в ближайшие запросы WAP. Сервер WAP может извлекать MSISDN из запросов и определять пользователя непосредственно по его MSISDN или преобразовывать MSISDN в идентификатор зарегистрированного пользователя.

Типичным примером таких приложений на базе WAP является приложение, которым люди пользуются для заказа такси. Анонимный пользователь может посетить WAP-сайт со своего сотового телефона, не раскрывая своего настоящего имени. Сервер WAP может использовать MSISDN для идентификации пользователя и управления его/ее заказом(ами). Если водителю такси необходимо связаться с пользователем, то он/она может перезвонить на соответствующий MSISDN.

Сервер WAP может также потребовать, чтобы пользователь зарегистрировался заранее и указал идентификатор пользователя, привязав его к одному или нескольким MSISDN. В этом случае, прежде чем обрабатывать запрос, серверу WAP необходимо преобразовать MSISDN, принудительно доставленный от сети, в идентификатор зарегистрированного пользователя.

Ниже представлена подробная техническая процедура (см. рисунок I.1).

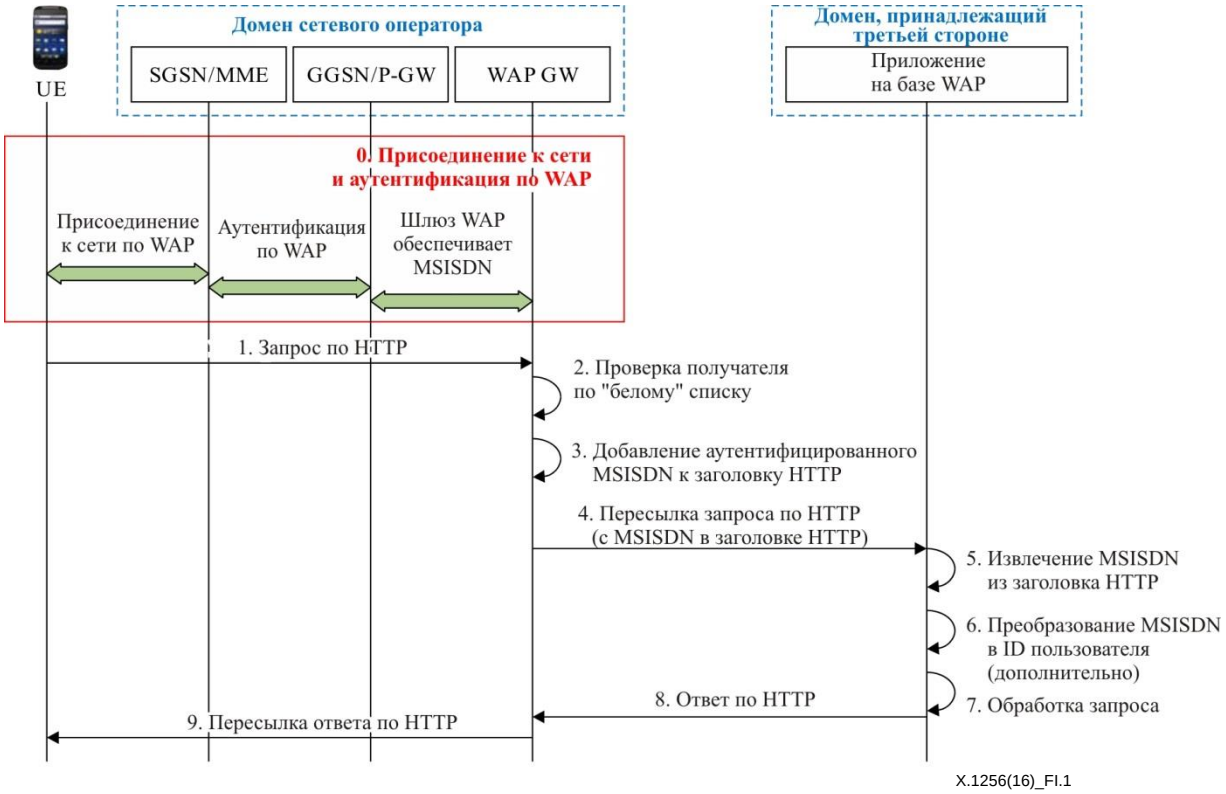

Рисунок I.1 – Обмен данными аутентификации по сети 2G/3G/4G для услуги WAP

0 Оборудование пользователя (UE) осуществляет присоединение к сети 2G/3G/4G. Шлюз WAP обеспечивает MSISDN каждого аутентифицированного пользователя.

1 UE начинает осуществлять запрос по протоколу передачи гипертекста (HTTP), чтобы получить доступ к услуге WAP.

2 Шлюз WAP получает этот запрос и проверяет, включен ли получатель услуги в "белый" список.

3 Если адрес получателя есть в "белом" списке, шлюз WAP вставляет в запрос новое поле заголовка HTTP (например, "идентификатор-вызывающего-абонента-x"), содержащее MSISDN пользователя.

4 Шлюз WAP пересылает измененный запрос по HTTP серверу WAP.

5 Сервер WAP извлекает MSISDN пользователя из заголовка HTTP.

6 В качестве дополнительной возможности сервер WAP преобразует MSISDN в идентификатор зарегистрированного пользователя.

7 Сервер WAP обрабатывает запрос в соответствии с MSISDN или идентификатором пользователя, преобразованным из MSISDN.

8 Сервер WAP направляет ответ по HTTP шлюзу WAP.

9 Шлюз WAP пересылает ответ по HTTP оборудованию пользователя (UE).

I.2 Сценарий использования доставки по запросу услуги

I.2.1 Услуга интернета, использующая атрибуты местоположения в сети 2G/3G/4G

Существует множество услуг на основе данных о местоположении, доступных в интернете, в том числе мобильном. Например, пользователь может обращаться к услуге WAP со своего сотового телефона, чтобы найти ближайший банк, гостиницу, ресторан или торговый комплекс. Если телефон оснащен функцией GPS, он может направлять параметры местоположения пользователя серверу WAP в рамках поискового запроса. В случае если функция GPS отсутствует или не работает в данный момент (например, в условиях помещения), серверу WAP может потребоваться поддержка базовой сети 2G/3G/4G для определения местоположения пользователя.

Ниже представлена подробная техническая процедура услуги интернета с использованием результатов определения местоположения в сети 2G/3G/4G (см. рисунок I.2).

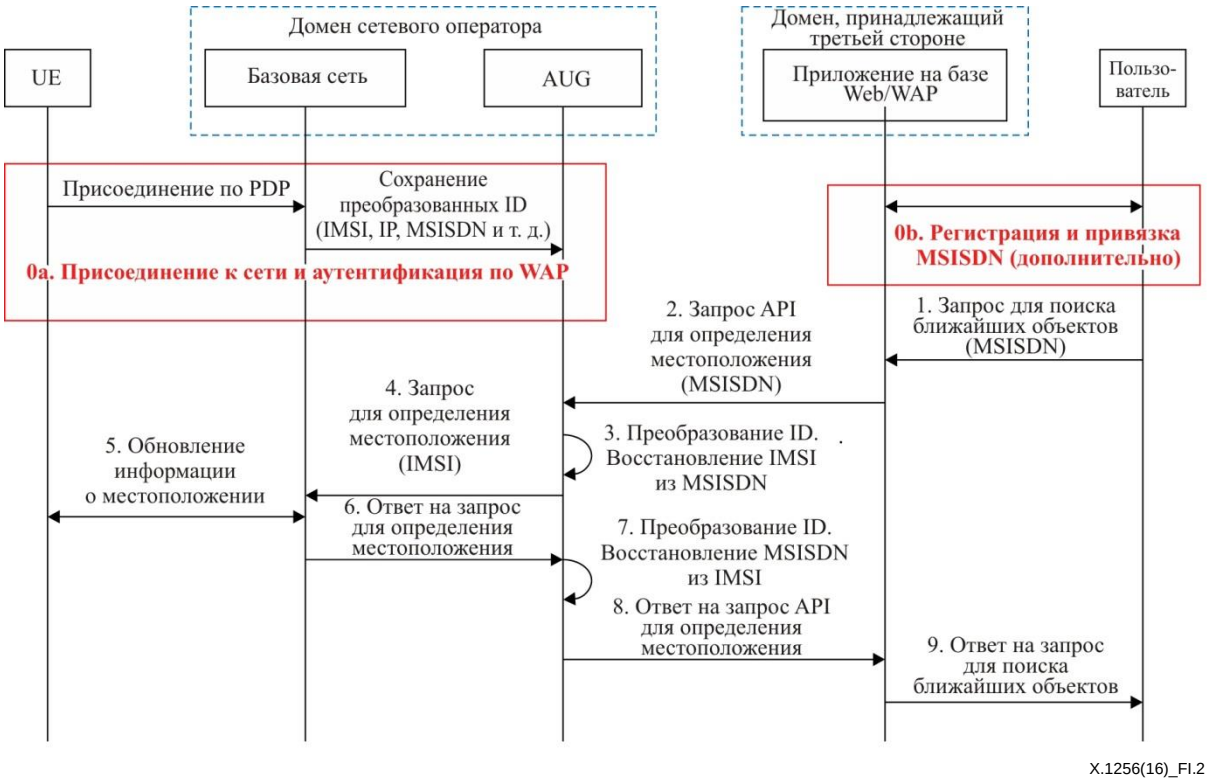

Рисунок I.2 – Услуга интернета с использованием атрибутов местоположения в сети 2G/3G/4G

0a UE осуществляет присоединение к сети 2G/3G/4G. Шлюз GGSN/P направляет AUG функцию преобразования международного идентификатора абонента подвижной связи (IMSI), MSISDN и IP-адреса пользователя, используя протокол услуг удаленной аутентификации пользователей по телефонным линиям (RADIUS);

0b В качестве дополнительной возможности пользователь регистрируется на сервере приложений на базе Web/WAP и привязывает свой идентификатор к одному или нескольким MSISDN.

1 Пользователь инициирует запрос для поиска ближайших объектов, включающий его/ее MSISDN как один из параметров. MSISDN может быть вставлен шлюзом WAP, как описано в Дополнении I.1.1, или введен самим пользователем и проверен сервером некоторым способом, который не входит в сферу применения настоящей Рекомендации.

2 Сервер Web/WAP анализирует MSISDN на основе запроса и вызывает API для определения местоположения, чтобы направить AUG запрос с указанным MSISDN.

3 AUG преобразует MSISDN (идентификатор услуги) в IMSI (идентификатор сети).

4 AUG направляет базовой сети запрос относительно текущего местоположения, соответствующего IMSI.

5 Базовая сеть связывается с UE соответствующим IMSI и завершает обновление информации о местоположении.

6 Базовая сеть отвечает на запрос AUG для определения местоположения.

7 AUG восстанавливает MSISDN из IMSI.

8 AUG отвечает на вызов API для определения местоположения, осуществленный сервером Web/WAP.

9 Сервер Web/WAP обрабатывает запрос пользователя для поиска ближайших объектов, используя информацию о местоположении, полученную от сети, и показывает результаты поиска пользователю.

Библиография

[IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[IETF RFC 4186] IETF RFC 4186 (2006), *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).*

[3GPP TS 33.328] 3GPP TS 33.328 V12.6.0 (2014), *IP Multimedia Subsystem (IMS) media plane security (Release12).*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2017 г.