International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1256

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Guidelines and framework for sharing network authentication results with service applications

Recommendation ITU-T X.1256

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1256

Guidelines and framework for sharing network authentication results with service applications

Summary

With the surge of mobile devices and applications accessing the Internet, the network and the service environment are becoming increasingly complicated. As a result, there is a pressing need to simplify the user authentication mechanism to improve user experience and service quality.

Many standardization organizations including ITU-T have conducted a lot of research work on the unified authentication mechanism (i.e., single sign-on). However, all the current work is basically focused on unified authentication among the service applications, without considering the relationship with the network authentication.

From the network operator's perspective, users undergo some forms of network authentication when they access the network. However, when they log in again to request access to a service their initial network authentication is not reused. When adopting an authentication results sharing mechanism between the service and the network, the service applications can identify a user by using the authentication results from the network. Such mechanism allows a user to be authenticated only once by the network and directly gain access to the service.

Recommendation ITU-T X.1256 develops guidelines for network operators and service providers to share network authentication results, and provides a framework for sharing minimum attributes across multiple services within an established trust relationship.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1256	2016-03-23	17	11.1002/1000/12605

Keywords

Authentication, identity attributes, network level authentication.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1256

Guidelines and framework for sharing network authentication results with service applications

1 Scope

This Recommendation develops guidelines for network operators and service providers to share network authentication results, and provides a framework for sharing minimum attributes across multiple services within an established trust relationship.

The methods for network operators to perform, integrate or implement network level authentication is out of the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G/3G Second/Third Generation

AC Access Controller

AKA Authentication and Key Agreement

AN Access Network

AP Access Point

API Application Programming Interface

AUG Authentication Gateway

BRAS Broadband Remote Access Server

EAP-SIM Extensible Authentication Protocol Method for (GSM) Subscriber Identity Modules

GGSN Gateway GPRS Support Node

GPRS General Packet Radio Service

HTTP Hyper Text Transfer Protocol

IMPI IP Multimedia Private Identity

IMPU IP Multimedia Public User identity

IMS IP Multimedia Subsystem

IMSI International Mobile Subscriber Identity

IP Internet Protocol

ISDN Integrated Services Digital Network

LoA Level of Assurance

MSISDN Mobile Subscriber International ISDN/PSTN Number

PSTN Public Switched Telephone Network

RADIUS Remote Authentication Dial-In User Service

SGSN Serving GPRS Support Node

SIM Subscriber Identity Module

SIP Session Initiation Protocol

SNS Social Network Service

UE User Equipment

USIM Universal Subscriber Identity Module

URI Uniform Resource Identifier

WAP Wireless Application Protocol

WLAN Wireless Local Area Network

5 Conventions

None.

6 Authentication attributes sharing mechanisms

6.1 Framework

When users access an operator's network, it is required that they should be strongly authenticated by the access network. However, this authentication capability does not usually facilitate the services. In most cases, the end users are authenticated respectively on the network and in the service system. For example, end users are authenticated by the third generation (3G) network based on the universal subscriber identity module (USIM) card inside their cell phones (what they have), but when they visit a certain social network service (SNS) they need to be authenticated by the web server again based on the (username, password) pair registered beforehand (what they know).

The basic concept of authentication attributes sharing is to enable the services to utilize the authentication attributes of the network. The authentication attributes sharing framework is shown in Figure 6-1.

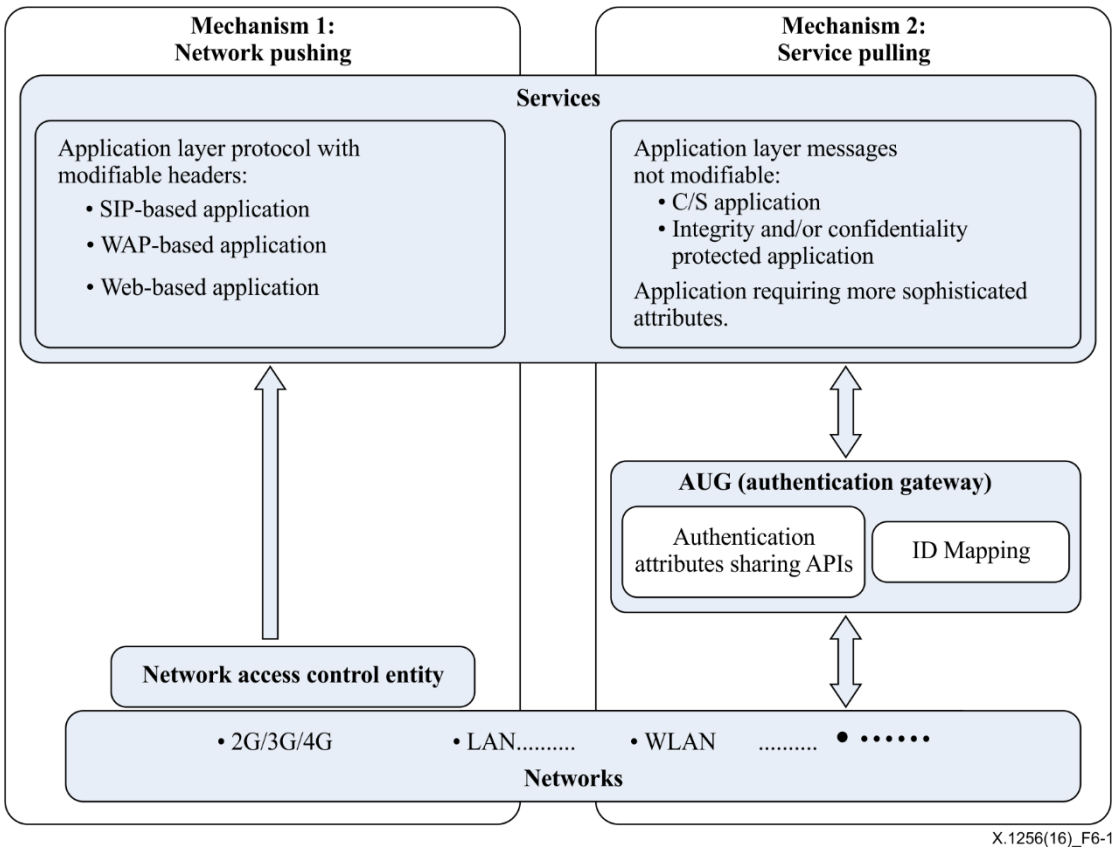

Figure 6-1 – Framework of sharing network authentication attributes with service applications

In this framework there are two types of authentication attributes sharing mechanisms:

- Mechanism 1 – Network pushing mechanism: transfer the network authentication attributes to service applications directly

  When the network access control entity understands the service's application layer protocol (e.g., SIP, WAP, HTTP, etc.), it is feasible for it to insert the network authentication attributes into the application layer messages and transfer them directly to the service platform. In this case, no application programming interface (API) needs to be defined for the service applications to actively obtain the authentication attributes because they only passively receive these parameters contained in the headers of the messages.

  The service applications may decide to parse and use the headers inserted by the network, or simply ignore them. If the service applications need more attributes than what is pushed, they should use the service pulling mechanism.

  See Appendix I.1 for a concrete use case.

- Mechanism 2 – Service pulling mechanism: share the network authentication attributes through the authentication gateway (AUG)

  If the network access control entity cannot parse or modify the service's application layer messages (e.g., when the application layer protocol is a proprietary one, or the application layer messages are integrity and/or confidentiality protected), a standalone AUG needs to be introduced to the network for authentication attributes sharing. The AUG implements well-defined network APIs which the service applications can call to obtain the authentication attributes from the network.

In addition, if the service applications as mentioned in network pushing mechanism require more attributes than what is pushed, they should also use this service pulling mechanism to obtain additional authentication attributes from the network.

See Appendix I.2 for a concrete use case.

6.2 Network pushing mechanism

6.2.1 Implementation guidance

When the user visits the network, the network access control entity at the border of the network authenticates the user's identity. Typical examples of the network access control entity include the access controller (AC) device in a wireless local area network (WLAN), serving GPRS support node (SGSN) or gateway GPRS support node (GGSN) in a general packet radio service (GPRS) network, and the broadband remote access server (BRAS) device in a fixed network. The network access control entity knows the user identity as a result of the network authentication.

If the network access control entity understands the service's application layer protocol (e.g., SIP, WAP, HTTP, etc.) it is feasible for it to encapsulate the user's identity and some accompanying information in the service request messages and transfer them to the service platform.

If the service platform trusts the network access control entity, it can directly extract the user identity from the service requests and regard the user to be authenticated already.

In this architecture, the service platform needs to determine whether or not to trust the authentication attributes inserted by the network access control entity. To support this, the network operator should make an agreement with the service provider, and provide a list of trustable access control devices or a mechanism (e.g., pre-shared keys, or digital certificates) to identify the trustable access control devices. The user information transferred between the access control device and the service platform should be protected. The access control devices of the network should also maintain a white list of the contracted service platforms. The network authentication attributes should only be transferred to the service platforms on the white list. Guidelines on how to achieve this trust relationship is out of the scope of this Recommendation.

6.2.2 Interface description

The network authentication attributes are loaded in the application protocol (e.g., SIP or HTTP) header of the service request messages, and transferred from the network access control entity to the service platform.

The following attributes should be included:

1) User identity:

   The content of this field is the user's network identity (e.g., SIP URI, MSISDN, Username, etc.). The service platform can use it to identify the user.

2) Authentication method with known level of assurance (LoA) [ITU-T X.1254]:

   The content of this field is the identifier of the authentication method (e.g., 2G/3G/4G AKA, IMS AKA, HTTP/SIP Digest, EAP-SIM, etc.).

   The network operator and the service providers should agree on a list of recognizable authentication method identifiers and their corresponding LoA.

   A given service platform should decide whether or not to accept the authentication attributes pushed from the network based on the LoA of the authentication method and its own security policy.

3) Other attributes required in the contract between the operator and the service provider.

6.3 Service pulling mechanism

6.3.1 Implementation guidance

It is not feasible to implement network pushing mechanism if the network access control entity cannot parse or modify the service's application layer messages, for example, when the application layer protocol is a proprietary one, or when the service messages are encrypted or integrity-protected. In this case, an AUG can be placed between the network and the service platform, acting as a proxy for the service platform to obtain the network authentication attributes.

Another justification for the service pulling model is that the attributes included in the messages pushed by the network may not be adequate for a specific service request. In this case, the service platform may need to actively contact the network to obtain additional information about the network authentication attributes.

To enable the service pulling model, the AUG needs to expose a set of network APIs which the service applications can call to obtain various information about the authentication results from the network. The network and service platforms may use different IDs (identifiers) to identify the users. Therefore the AUG should contain an ID mapping function which maps a user's service ID to his/her network ID, and vice versa.

In this architecture, the service platform and the AUG need to trust each other. To support this, the network operator should make an agreement with the service provider, and provide a list of trustable AUG devices or a mechanism (e.g., pre-shared keys, or digital certificates) to identify the trustable AUG devices. The user information transferred between the AUG device and the service platform should be protected. The AUG devices should execute an authorization mechanism (e.g., white list) on the exposed APIs so that the network authentication attributes can only be shared with contracted service platforms. Guidelines on how to achieve this trust relationship is out of the scope of this Recommendation.

6.3.2 Interface description

The AUG implements well-defined network APIs which the service applications can call to obtain the authentication attributes from the network.

The network operators may implement the APIs in some forms of their own preferences. The definition of these APIs is out of the scope of this Recommendation.

The authentication attributes which can be shared in this way may include any information related to an authenticated network user, such as user location, user subscription information, user network usage statistics, and so on.

7 Security considerations

When technical solutions pertaining to the framework in clause 6 are deployed, some security considerations need to be noted:

- It is vital to protect the authentication elements on the network, and to ensure the trustworthiness and security of network authentication capability.
- The service systems should establish a trust relationship with the network, so that the authentication attributes transferred from the network can be trusted by the relying service systems. The service platform should only trust the user identity information from known authentication server to avoid authentication server impersonating.
- It is vital to ensure that the authentication attributes are securely transferred to the service platform. Confidentiality and integrity of user identity information should be guaranteed and its transmission should be protected against replaying and forging attacks.

- When providing authentication results and other user information to the service platform, the network should strictly abide by the applicable privacy protection law and regulations for the jurisdiction where the service is provided.
- The service platform should properly handle users' authentication information obtained from the network, e.g., to securely store it for use, and to promptly destroy it after use. Abuse and leakage of user information should be prevented.

Appendix I

Use Cases

(This appendix does not form an integral part of this Recommendation.)

I.1 Network pushing use case

I.1.1 2G/3G/4G network to WAP service

Wireless application protocol (WAP) is a popular mobile data service which users can access via 2G/3G/4G networks. After network attachment and authentication, the WAP GW (gateway) can insert the user's mobile subscriber international ISDN/PSTN number (MSISDN) into the upcoming WAP requests. The WAP server can extract the MSISDN from the requests and identify the user directly by his MSISDN, or map the MSISDN to a registered user ID.

A typical example of such WAP-based applications is the one that people use to book a taxi. An anonymous user can visit such a WAP site on his/her cell phone without exposing their real name. The WAP server can use the MSISDN to identify the user and manage his/her order(s). If the taxi driver needs to contact the user a call can be placed back to the corresponding MSISDN.

The WAP server can also require the users to register beforehand and specify a user ID and bind it with one or several MSISDNs. In this case, the WAP server needs to map the MSISDN pushed from the network to a registered user ID before processing the request.

The detailed technical procedure is defined below (see Figure I.1):

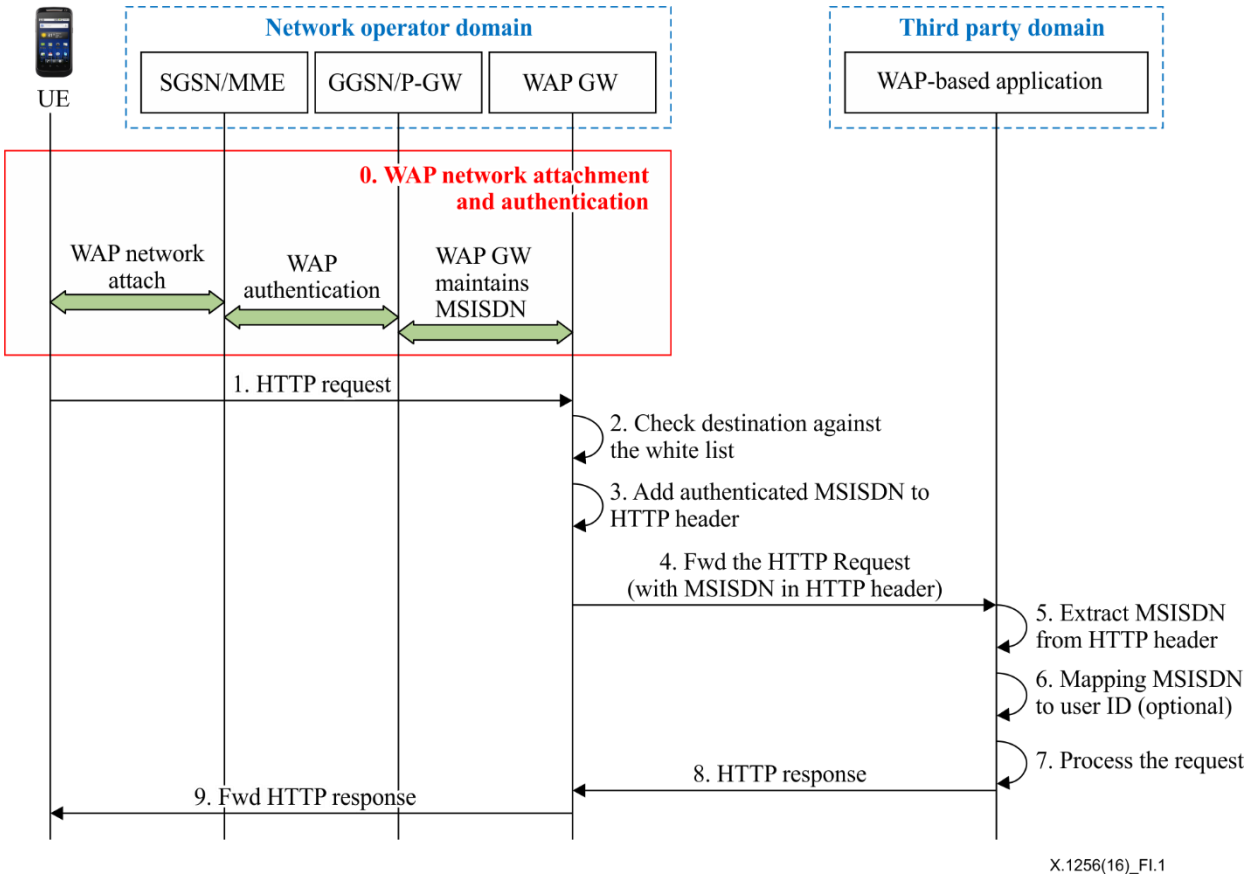

Figure I.1 – Authentication sharing for WAP service via 2G/3G/4G network

0. User equipment (UE) attaches to the 2G/3G/4G network. WAP GW maintains the MSISDN of each authenticated user.

1. UE starts a hypertext transfer protocol (HTTP) request to access a WAP service.
2. WAP GW receives the request and checks whether the service destination is on the white list.
3. If the destination address is on the white list, WAP GW inserts a new HTTP header field (e.g., "x-up-calling-line-id") into the request, containing the user's MSISDN.
4. WAP GW forwards the modified HTTP request to the WAP server.
5. The WAP server extracts user's MSISDN from the HTTP header.
6. Optionally, the WAP server maps the MSISDN to a registered user ID.
7. The WAP server processes the request according to the MSISDN or the user ID mapped from the MSISDN.
8. The WAP server sends the HTTP response to WAP GW.
9. WAP GW forwards the HTTP response to UE.

I.2 Service pulling use case

I.2.1 Internet service using 2G/3G/4G network location attributes

There are many location-based services available on the Internet and mobile Internet. For example, a user can visit a WAP service from his/her cell phone and search for a nearby bank, hotel, restaurant or shopping mall. If the phone is equipped with a GPS, it can send the user's location parameters to the WAP server as part of the search request. However, if there is no GPS or the GPS does not work at the moment (e.g., indoor environment), the WAP server may need the support of the 2G/3G/4G core network to locate the user.

The detailed technical procedure of Internet service using 2G/3G/4G network location results is defined below (see Figure I.2):

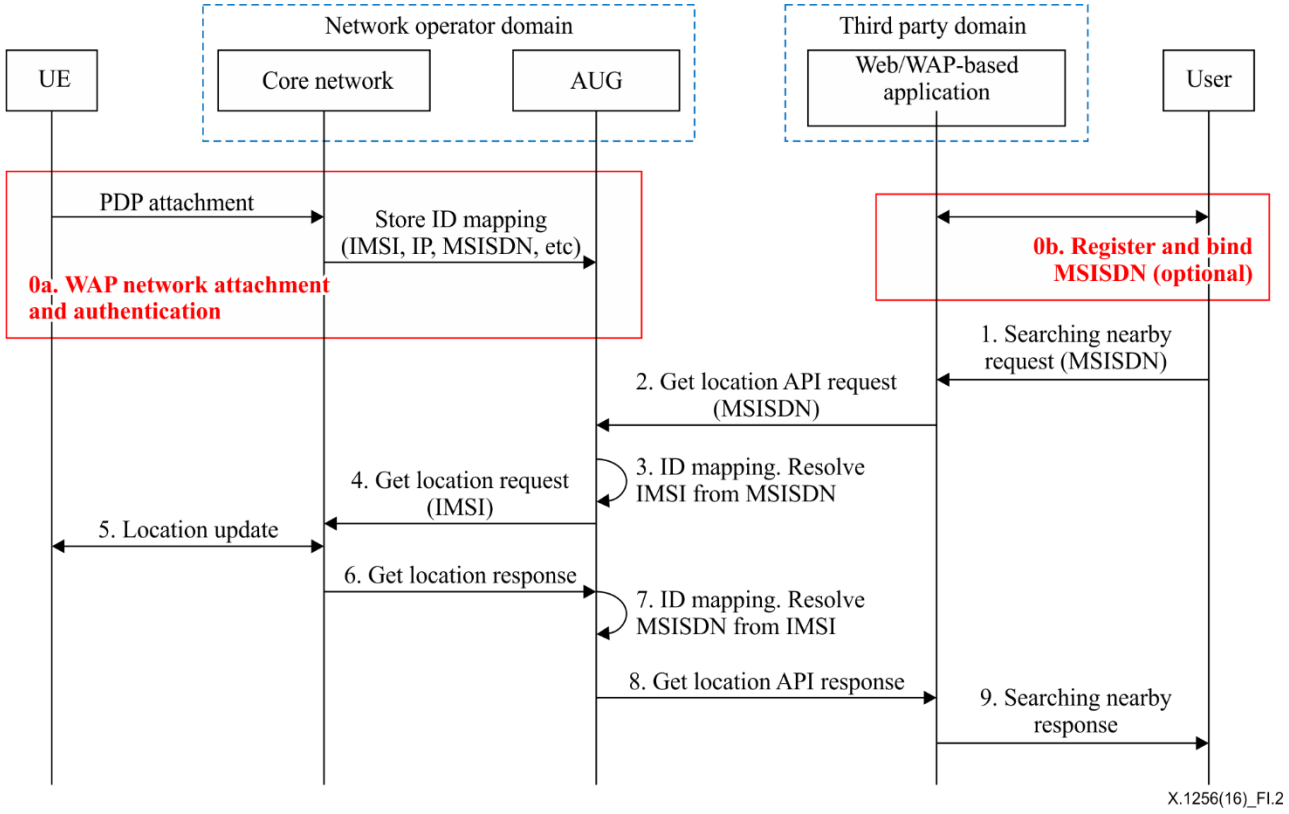

Figure I.2 – Internet service using 2G/3G/4G network location attributes

0a. UE attaches to the 2G/3G/4G network. GGSN/P-GW sends the mapping relationship between user international mobile subscriber identity (IMSI), MSISDN and IP address to AUG using remote authentication dial-in user service (RADIUS) protocol.

0b. Optionally, user registers on the Web/WAP based application server and binds his/her user ID with one or more MSISDNs.

1. The user initiates a searching nearby request, including his/her MSISDN as one of the parameters. The MSISDN may be inserted by the WAP GW as described in Appendix I.1.1, or input by the user himself/herself and verified by the server in some way out of scope of this Recommendation.

2. The WAP/Web server parses the MSISDN from the request and calls the get location API to send the AUG a request with the specified MSISDN.

3. The AUG maps the MSISDN (service ID) to IMSI (network ID).

4. The AUG queries the core network about the current location corresponding to the IMSI.

5. The core network contacts the UE corresponding to the IMSI and finishes the location update.

6. The core network responds to the AUG's get location request.

7. The AUG resolves MSISDN from IMSI.

8. The AUG responds to the WAP/Web server's get location API call.

9. The WAP/Web server responds to the user's searching nearby request by using the location information returned from the network and shows the searching results to the user.

Bibliography

[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)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016