国 际 电 信 联 盟

ITU-T X.1256

(03/2016)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

网络空间安全 – 身份管理

与业务应用共用网络认证结果的导则和框架

ITU-T X.1256 建议书

国际电信联盟

ITU-T X 系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
远程生物特征测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	**X.1250–X.1279**
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
策略交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1256 建议书

与业务应用共用网络认证结果的导则和框架

摘要

互联网移动设备和应用的爆发增长，使网络和业务环境变得愈发复杂。因此，有迫切必要通过简化用户认证机制改善用户的体验和服务质量。

包括ITU-T在内的许多标准化组织就统一认证机制（即单一登录）开展了大量研究工作。但是，当前所有工作基本均聚焦于业务应用间的统一认证，而并未考虑与网络认证的关系。

从网络运营商的角度看，用户在接入网络时会使用某种形式的网络认证，但当其再次登录获取业务时，并未重复使用初次网络认证。如果采用业务与网络之间共享认证结果的机制，则业务应用可利用网络认证结果确定用户（身份）。此机制允许网络仅对用户进行一次认证，便可直接使用相关业务。

ITU-T X.1256建议书为网络运营商和服务提供商制定了共享网络认证结果的导则，为在业已建立的信任关系内跨业务分享最低数量的属性提供了框架。

沿革

版本	建议书	批准日期	研究组	识别码*
1.0	ITU-T X.1256	2016-03-23	17	11.1002/1000/12605

关键词

认证，身份属性，网络认证。

* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/ ，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1256 建议书

与业务应用共用网络认证结果的导则和框架

1 范围

本建议书为网络运营商和服务提供商制定了共享网络认证结果的导则，为在业已建立的信任关系内跨业务分享最低数量的属性提供了框架。

有关网络运营商在网络层面进行、综合或实施认证的方法不属于本建议书的范围。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1254] ITU-T X.1254建议书（2012） – 实体认证保证框架。

3 定义

3.1 在其他地方定义的术语

无。

3.2 本建议书中定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

2G/3G 第二/第三代

AC 接入控制器

AKA 认证和秘钥协议

AN 接入网

AP 接入点

API 应用程序接口

AUG 认证关口

BRAS 宽带远程接入服务器

EAP-SIM （GSM）用户身份模块的可扩展认证协议方法

GGSN 网关GPRS支持节点

GPRS 通用分组无线业务

HTTP 超文本传送协议

IMPI IP多媒体个人身份

IMPU IP多媒体公共用户身份

IMS IP多媒体子系统

IMSI 国际移动用户身份

IP 网际协议

ISDN 综合业务数字网

LoA 保障水平

MSISDN 移动用户国际ISDN/PSTN号码

PSTN 公用交换电话网

RADIUS 远程认证拨入用户业务

SGSN GPRS服务支持节点

SIM 用户身份模块

SIP 会话起始协议

SNS 社交网络服务

UE 用户设备

USIM 通用签约用户身份模块

URI 统一资源识别符

WAP 无线应用协议

WLAN 无线局域网

5 惯例

无。

6 认证属性共用机制

6.1 框架

当用户接入运营商网络时，需要由接入网对该用户进行强力认证。然而，这一认证能力通常不能为业务提供便利。多数情况下，最终用户分别在网络和业务系统中得到认证。例如，最终用户由3G网络基于其蜂窝电话内的USIM卡（用户所拥有的）得到认证，但当他们访问某一SNS业务时，需要由网络服务器按照事先登记的（用户名、密码）对（用户所知道的）再次对其进行认证。

认证属性共用的基本理念是方便各业务使用网络的认证属性。图6-1所示为认证属性共用框架。

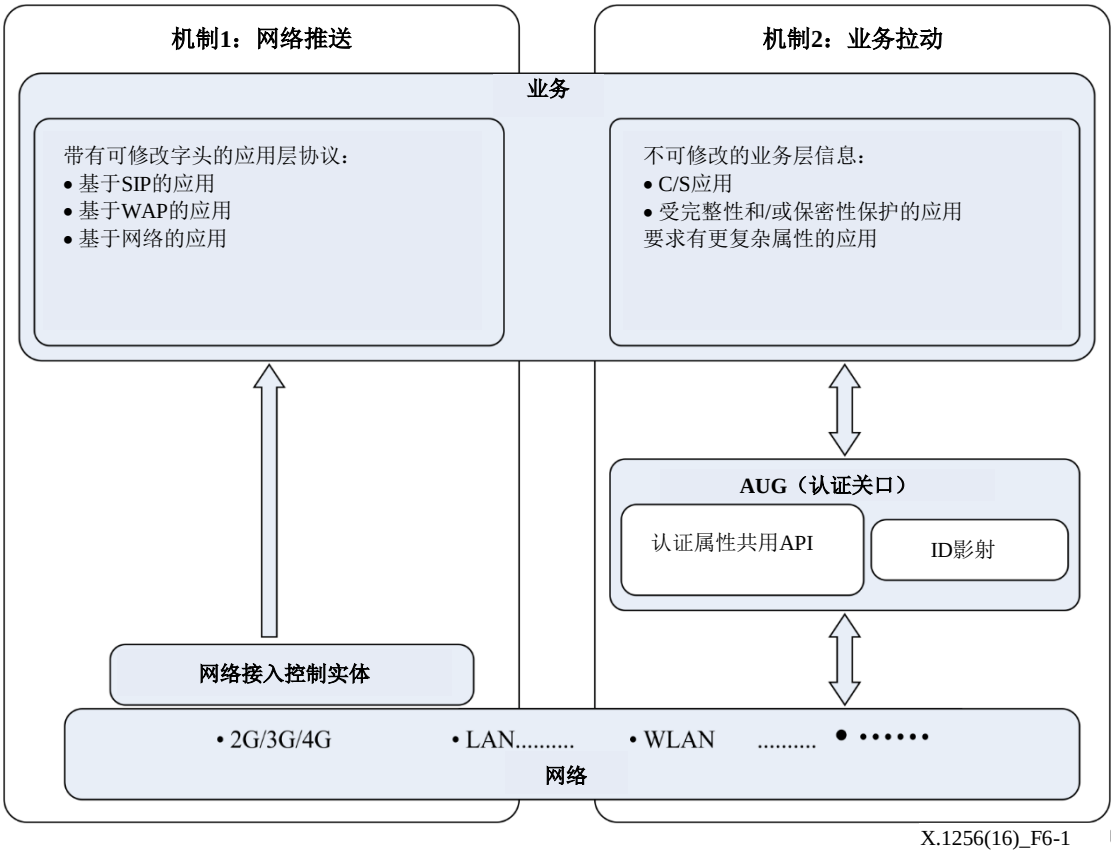


图6-1 – 与业务应用共用网络认证属性的框架

在该框架中，存在两类认证属性共用机制：

- 机制1 – 网络推送机制：直接将网络认证属性传送至业务应用

  当网络接入控制实体理解业务应用层协议（如SIP、WAP、HTTP等）时，可将网络认证属性插入应用层信息中并将其直接传送至业务平台。在此情况下，不需要为业务应用确定应用编程接口（API）即可使前者主动获得认证属性，因为这些应用仅是被动地接收包含在信息字头中的相关参数。

  业务应用可决定对网络插入的字头进行解析和使用，亦或完全对其视而不见。如果业务应用需要更多的超出推送的属性，则应使用业务拉动机制。

  有关具体使用案例请见附录I.1。

- 机制2 – 业务拉动机制：通过认证网关（AUG）共用网络认证属性

  如果网络接入控制实体无法解析或修改业务应用层信息（如，当应用层协议为专用协议，或应用层信息到受到完整性和/或保密性保护时），则需要在网络上引入一个自成一体的AUG来进行认证属性共用。该AUG实施得到明确定义的网络API，而网络应用则可以通过调用这些接口来从网络那里获得认证属性。

此外，如前所述，如果网络推送机制中的业务应用需要超过推送的更多的属性，则它们应当使用该业务拉动机制来从网络那里获得更多的认证属性。

有关具体使用案例请见附录I.2。

6.2 网络推送机制

6.2.1 实施指南

当用户访问网络时，处于网络边界的网络接入控制实体对用户身份进行认证。网络接入控制实体的典型示例包括无线局域网（WLAN）中的接入控制（AC）设备、通用分组无线业务（GPRS）网络中的服务GPRS支持节点（SGSN）/网关GPRS支持节点（GGSN）和固定网络中的宽带远程接入服务器（BRAS）设备。网络接入控制实体通过进行网络认证了解用户身份。

如果网络接入控制实体理解业务应用层协议（如，SIP、WAP、HTTP 等），则可对用户身份和业务请求信息中的一些伴随信息进行封装，并将其传至业务平台。

如果业务平台信任网络接入控制实体，则可直接从业务请求处提取用户身份并将该用户视为已得到认证的用户。

在该架构中，业务平台需要确定是否信任由网络接入控制实体插入的认证属性。为支持这一工作，网络运行商应与服务提供商达成协议，并提供可信任接入控制设备清单或一种机制（如，预先共用秘钥，或数字证书），以确定可信任的接入控制设备。在接入控制设备与业务平台之间传送的用户信息应得到保护。网络接入控制设备还应保留一份已与之签订合同的业务平台白色清单。应只向白色清单所含业务平台传送网络认证属性。如何建立这种信任关系的导则不属于本建议书的范围。

6.2.2 接口描述

网络认证属性载于业务请求信息的应用协议（如SIP或HTTP）字头中，并从网络接入控制实体传至业务平台。

应包括下列属性：

1) 用户身份：

该字段的内容是用户网络身份（如SIP URI、MSISDN、用户名等）。业务平台可利用该内容识别用户。

2) 利用已知保障水平（LoA）[ITU-T X.1254]:的认证方法：

该字段的内容是认证方法识别符（如2G/3G/4G AKA、IMS AKA、HTTP/SIP Digest、EAP-SIM等）。

网络运营商和服务提供商应就可被认识的认证方法识别符及其相应LoA清单达成一致。

特定业务平台应按照认证方法的LoA和其自身安全政策，决定是否接受网络推送的认证属性。

3) 运营商与服务提供商之间所签合同要求的其他属性。

6.3 业务拉动机制

6.3.1 实施指南

如果网络接入控制实体不能解析或修改业务应用层信息（如应用层协议为专用协议，或业务信息被加密或受到完整性保护），则无法实施网络推送机制。在此情况下，可在网络与业务平台之间放置一个AUG，作为业务平台的代理来获得网络认证属性。

业务拉动模式的另一个合理理由是，包含在网络推送信息中的属性对于某一具体业务请求可能是不充分的。在此情况下，业务平台可能需要主动与网络进行联系，以获得有关网络认证属性的更多信息。

为了实现业务拉动模式，AUG需要对一套网络API进行曝光（业务应用可调用这些接口来从网络那里获得有关认证结果的多种不同信息）。网络和业务平台可采用不同ID（识别符）来识别用户，因此，AUG应包含一个ID影射功能，以便将用户的业务ID影射到他/她的网络ID，反之亦然。

在该架构中，业务平台和AUG之间需要相互信任。为了支持这一工作，网络运营商应与服务提供商达成协议并提供可信任AUG设备清单或一种机制（如预先共享秘钥或数字证书），以确定可信任AUG设备。在AUG设备与业务平台之间传送的用户信息应得到保护。AUG设备应在得到暴露的API上实施授权机制（如白色清单），以便只能与已与之签订合同的业务平台共用网络认证属性。如何建立这一信任关系的导则不属于本建议书的范围。

6.3.2 接口描述

AUG实施得到明确定义的网络API，业务应用可对这些接口进行调用，以便从网络那里获得认证属性。

网络运营商可按照其自身喜好以某种形式实施API。API的定义不属于本建议书的范围。

可以此种方法共用的认证属性可包括与得到认证的网络用户有关的任何信息，如用户地点、用户订购服务情况、用户网络使用统计数据等。

7 安全考虑

在部署与第6部分所述框架相关的技术解决方案时，需注意到一些安全考虑：

- 保护网络的认证元素并确保网络认证能力的可信任性和安全性至关重要。
- 业务系统应与网络建立一种信任关系，以便使网络传送的认证属性得到依赖网络的业务系统的信任。业务平台应只信任来自已知认证服务器的用户身份信息，以避开伪装的认证服务器。
- 确保将认证属性安全地传送至业务平台至关重要。用户身份信息的保密性和完性应得到保障，且在传送过程中应保护其免受重试和伪造攻击。

- 网络在向业务平台提供认证结果和其他认证信息时，应严格遵守服务提供辖区内适用的隐私保护法律法规。
- 业务平台应适当处理从网络那里获得的用户认证信息，如，安全存储（以便时机合适时使用）并在使用后及时销毁。应避免滥用或泄露用户信息。

附录I

使用案例

（本附录不构成本建议书不可分割的部分）

I.1 网络推送使用案例

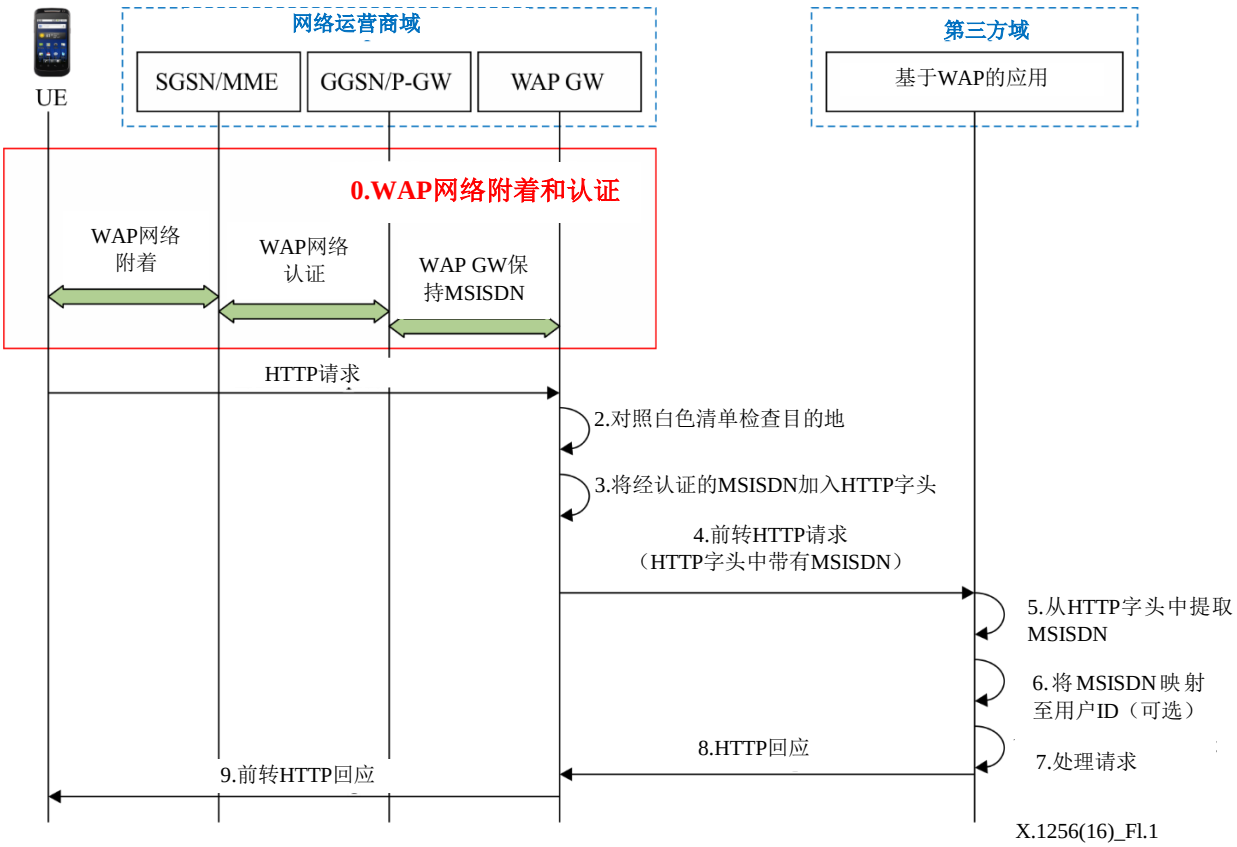
I.1.1 2G/3G/4G网络到WAP业务

无线应用协议（WAP）是一种用户可通过2G/3G/4G网络获得的、受人欢迎的移动数据业务。在进行网络附着和认证后，WAP GW（关口）可将用户的移动签约用户国际ISDN/TSTN号码（MSISDN）插入到WAP请求中。WAP服务器可从请求中提取MSISDN并通过用户的MSISDN直接对其予以身份确定，或将MSISDN映射至已登记的用户ID。

这种基于WAP的应用的一个典型示例是用户用此来预定出租车。某匿名用户可在不暴露其真实姓名的情况下通过其移动电话访问这种WAP。WAP服务器可利用MSISDN确认用户的身份并对其订单进行管理。如果出租车司机需要与用户联系，则可回呼相应MSISDN。

WAP服务器还可要求用户事先登记并指明其用户身份，同时将该身份与一个或若干MSISDN绑定。在此情况下，WAP服务器需将网络推送的MSISDN映射至已登记的用户ID，然后再处理相关请求。

以下所述为详细技术流程（参见图I.1）：



图I.1 – 通过2G/3G/4G网络的WAP业务认证共用

0 用户设备（UE）附着于2G/3G/4G网络。WAP GW保留每一个经认证的用户的MSISDN。

1 UE启动获得超文本传送协议（HTTP）业务的WAP请求。

2 WAP GW收到请求，查验业务目的地是否在白色清单上。

3 如果目的地地址在白色清单上，则WAP GW在请求中插入新的、包含用户MSISDN的HTTP字头字段（如“x-up-calling-line-id”）。

4 WAP GW将修改的HTTP请求前转至WAP服务器。

5 WAP服务器从HTTP字头中提取用户的MSISDN。

6 作为一种可选功能，WAP服务器将MSISDN映射至已登记的用户身份。

7 WAP服务器按照MSISDN或由MSISDN映射过来的用户ID处理请求。

8 WAP服务器向WAP GW发送HTTP回应。

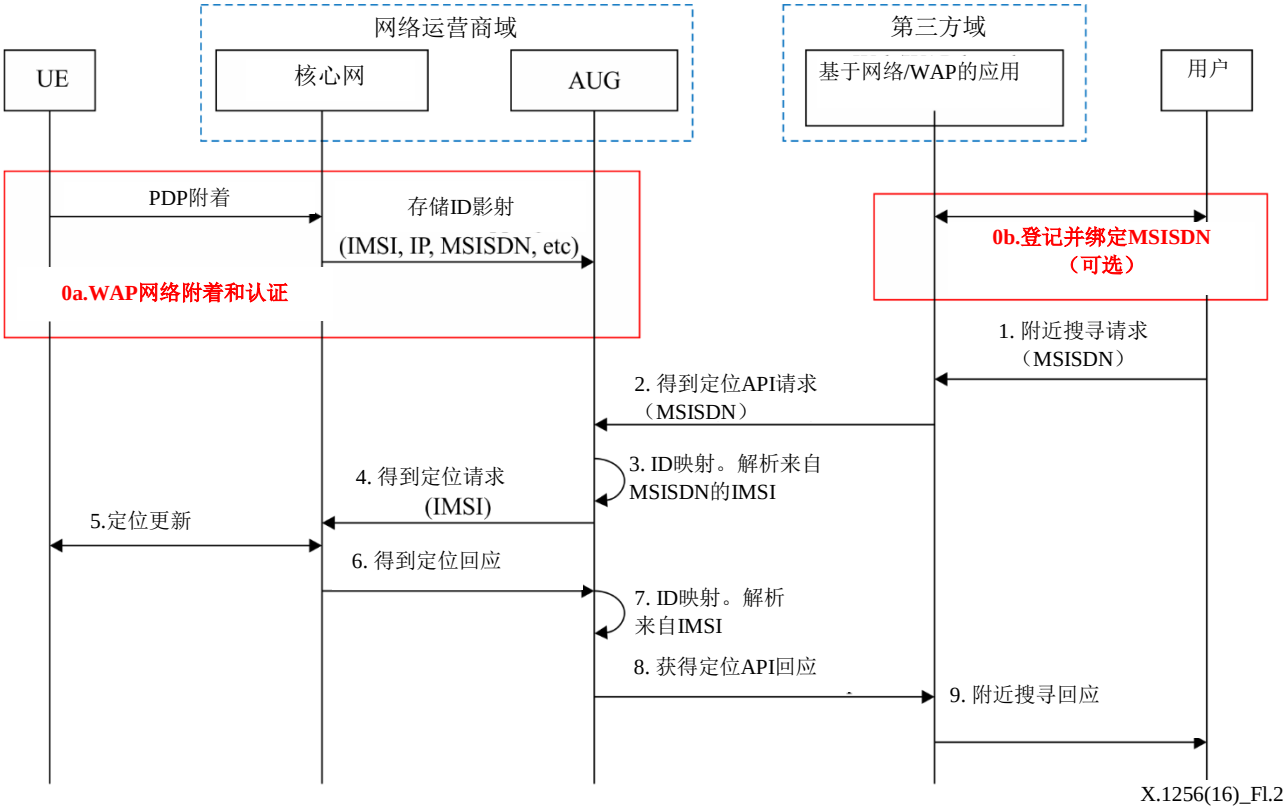
9 WAP GW向UE前转HTTP回应。

I.2 业务拉动使用案例

I.2.1 使用2G/3G/4G网络定位属性的互联网服务

互联网和移动互联网上存在很多基于地点的服务，例如，用户可通过其移动电话访问某种WAP服务，如搜寻附近银行、酒店、餐馆或购物中心。如果电话配有GPS，则可将用户地点参数作为搜寻请求的一部分发至WAP服务器。然而，如果电话未配备GPS或当前GPS不工作（如在室内环境中），则WAP服务器可能需要借助2G/3G/4G核心网来对用户进行定位。

以下详述使用2G/3G/4G网络定位结果的互联网服务技术流程（见图I.2）：



图I.2 – 使用2G/3G/4G网络定位属性的互联网服务

0a UE附着于2G/3G/4G网络。GGSN/P-GW将用户国际移动用户身份（IMSI）、MSISDN与IP地址之间的映射关系发送至使用远程认证拨入用户业务（RADIUS）协议的AUG。

0b 作为可选功能，用户在基于网络/WAP的应用服务器上进行登记，并将其用户ID与一个或更多MSISDN绑定。

1 用户启动附近搜寻请求，包括作为参数之一的该用户的MSISDN。MSISDN可如附录I.1.1所述，由WAP GW插入，或由用户自己输入，并由服务器以某种形式进行验证（不属于本建议书的范围）。

2 WAP/Web网络服务器对来自请求的MSISDN进行解析，并调用获得定位API，以便向AUG发送带有特定MSISDN的请求。

3 AUG将MSISDN（业务ID）映射至IMSI（网络ID）。

4 AUG就对应IMSI的当前定位向核心网进行查询。

5 核心网与对应IMSI的UE进行联系并完成定位更新。

6 核心网对AUG的获得定位请求做出回应。

7 AUG解析源自MSISDN的IMSI。

8 AUG对WAP/Web服务器的获得定位API呼叫做出回应。

9 WAP/Web服务器利用从网络返回的定位信息响应用户的附近搜寻请求并向用户显示搜寻结果。

参考资料

[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).

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般资费原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2017年，日内瓦