[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/30 (2006.01)
H04Q 7/34 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200680036350.7

[43] 公开日 2008 年 10 月 1 日

[11] 公开号 CN 101278576A

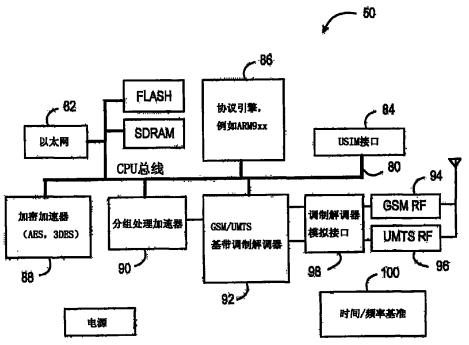
[22] 申请日 2006.7.28
[21] 申请号 200680036350.7
[30] 优先权
[32] 2005. 8. 1 [33] GB [31] 0515888.6
[32] 2006. 5.30 [33] GB [31] 0610650.4
[86] 国际申请 PCT/GB2006/002838 2006.7.28
[87] 国际公布 WO2007/015075 英 2007.2.8
[85] 进入国家阶段日期 2008.3.31
[71] 申请人 UBIQUISYS 有限公司
地址 英国威尔特郡
[72] 发明人 彼得·凯威尔 安德里亚·吉斯蒂娜
理查德·伯恩
克瑞斯特沃·达西尔瓦
[74] 专利代理机构 广州新诺专利商标事务所有限公司
代理人 罗毅萍
权利要求书 2 页 说明书 30 页 附图 12 页

[54] 发明名称

包含 SIM 卡的专用访问点

[57] 摘要

可以由用户安装用于诸如蜂窝通信网络等移动通信网络的访问点或基站，以在他们自己的家庭或办公室内或附近使用。 此基站具有 SIM 卡，可以在用户的现有宽带互联网连接上建立与移动通信网络的核心网络的安全通信。 此基站还能够获取必需的加密密钥，从而允许移动设备与基站进而与核心网络安全地通信。



1．一种用于蜂窝通信系统的基站，包括用于 SIM 卡的接口。

2. 如权利要求 1 要求保护的基站，包括 SIP 客户机软件，以便可以将根据 GSM/UMTS 协议的通信映射到相应 SIP 服务上。

3．如权利要求 1 或 2 要求保护的基站，包括 UMA 客户机软件，以便基站可以在宽带 IP 网络上与在蜂窝通信系统的核心网络内的 UMA UNC 通信。

4．如权利要求 3 要求保护的基站，其中在基站内的软件适合于将根据 GSM/UMTS 协议的通信映射成 UMA 协议。

5．如前面任一权利要求要求保护的基站，包括 IPSec 软件，由此基站能够提供在蜂窝通信系统的基站和核心网络之间的加密和安全传输介质。

6．如权利要求 5 要求保护的基站，其中基站适合于从蜂窝通信系统的核心网络接收加密密钥。

7．如权利要求 6 要求保护的基站，其中基站适合于适用于从蜂窝通信系统的核心网络接收的至少一个加密密钥，加密和解密在基站和移动站之间传输的消息。

8．如前面任一权利要求要求保护的基站，其中基站适合于使用在 SIM 卡内存储的数据向蜂窝通信系统的核心网络标识自身，以便将其识别为移动设备，并支持其发起和结束消息和呼叫。

9．如权利要求 8 要求保护的基站，其中基站适合于使用在 SIM 卡上存储的标识数据建立与蜂窝通信系统的核心网络的 IPSec 通道。

10．如前面任一权利要求要求保护的基站，其中基站适合于用作用于在无线通信协议上与其连接的任一通信设备的代理，以便支持该通信设备与蜂窝通信系统的核心网络通信。

11．如权利要求 1 要求保护的基站，其中基站适合于接收来自预先登记用户的 SMS 消息和按照其动作，指示基站执行特定功能。

12．如权利要求 11 要求保护的基站，其中特定功能包括维护数据库。

13．如权利要求 12 要求保护的基站，其中基站还适合于使用对所述数据库的任意改变更新相关管理系统。

14．如权利要求 11 要求保护的基站，其中特定功能包括控制连接到用户局域网的设

备。

15．如权利要求 1 要求保护的基站，其中基站适合于响应于预定义条件，将 SMS 或 MMS 消息发送给用户。

16．如权利要求 15 要求保护的基站，其中预定义条件涉及基站的操作。

17．如权利要求 15 要求保护的基站，其中预定义条件涉及连接到用户局域网的设备。

18．如权利要求 15 至 17 中任一权利要求要求保护的基站，其中，如果用户的移动通信设备驻留到基站上，将所述 SMS 或 MMS 消息直接发送给所述用户，而不通过蜂窝通信系统的核心网络。

19．如权利要求 1 要求保护的基站，其中基站适合于接收由广域网内的用户始发的呼叫或数据和按照其动作，以便用户可以访问在用户局域网上的信息。

20．如权利要求 1 要求保护的基站，其中基站适合于响应于预定义条件，始发到用户的呼叫或数据对话。

21．如权利要求 20 要求保护的基站，其中预定义条件涉及连接到用户局域网的设备。

22．如权利要求 20 至 21 中任一权利要求要求保护的基站，其中，如果用户的移动通信设备驻留在基站上，则由所述用户直接始发所述呼叫或数据对话，而不通过蜂窝通信系统的核心网络。

包含 SIM 卡的专用访问点

技术领域

本发明涉及一种访问点，尤其涉及一种用于移动通信网络的访问点。

背景技术

为了允许诸如蜂窝通信网络的移动通信网络的运营商提高网络的覆盖区域，建议用户应当能够安装访问点或者基站，以在他们自己的家或办公室内或者附近使用。此类基站可以在用户的现有的宽带互联网连接上建立与移动通信网络的核心网络的通信。

为了实现这一目的，基站必需能够安全地与移动通信网络的核心网络通信，并允许与基站通信的移动设备与核心网络安全地通信。

发明内容

根据本发明的一方面，提供一种用于蜂窝通信系统的基站，包括用于 SIM 卡的接口。

附图说明

图 1 是根据本发明的包含基站的系统的方框示意图。

图 2 是图示根据本发明的基站硬件结构的方框示意图。

图 3 是图示根据本发明的基站软件结构的方框示意图。

图 4 是根据本发明的包含基站的另一个系统的方框示意图。

图 5 图示常规网络结构。

图 6 图示根据本发明一个方面的网络结构。

图 7 图示根据本发明一个方面的信令程序。

图 8 是所使用的图 4 的另一系统的一部分的方框示意图。

图 9 图示根据本发明一个方面的另一信令程序。

图 10 图示根据本发明一个方面的另一网络结构。

图 11 图示根据本发明一个方面的另一网络结构。

图 12 图示所使用的权利要求 10 的另一网络结构。

图 13 图示根据本发明一个方面的另一信令程序。

具体实施方式

图 1 是图示系统结构的方框示意图。移动网络运营商（MNO）拥有和操作无线通信网络，包括无线电网络 10，其包括蜂窝基站网络（未图示），和核心网络 20，其具有到固定电话网络的连接。这些通常是常规的，除了如下面所描述的。

当在由无线通信网络覆盖的地区内漫游时，移动电话 30 能够建立与蜂窝基站之一的无线连接，从而与固定电话网络内的其它电话通信，或者与已经建立它们自身的与蜂窝基站的无线连接的其它移动电话通信，因而与固定电话网络通信。

根据本发明，例如在家庭或办公室 40 或者在需要附加无线覆盖的另一位置内，提供其它基站或访问点 50。此访问点 50 提供用于由其所处的居所业主使用，但是集成到无线通信网络内。也就是说，通过固定或临时地向其分配一组信道中的一些信道，该访问点共享分配给该无线通信网络的部分射频频谱。因而，与其它基站共享该组信道，所述基站可以服务于宏小区、微小区、微微小区，甚至在公共广域网内的“毫微微小区”。因此，当离开访问点 50 的相邻位置时，移动电话 30 可以从访问点 50 漫游到另一个基站，或者当返回访问点 50 的相邻位置时，可以从另一基站漫游进入访问点 50。

因此，访问点 50 用作相关无线通信网络内的基站。例如，它可以允许整个常规和未修改移动电话 30 或者其它用户设备使用 GSM/GPRS 和/或 UMTS 空中接口建立用于语音和/或数据服务的连接。当然，可以支持该访问点 50 使用任意适当蜂窝无线通信系统的标准空中接口建立与移动电话 30 的连接。

访问点 50 具有在家庭或办公室 40 内用于以太网局域网（LAN）42 的连接。如图 1 所示，访问点 50 可以在以太网 LAN 42 上连接到一个或多个本地 PC 或服务器 44。

访问点 50 可以在以太网 LAN 42 上连接到 IP 网关设备 60。通过数字用户线路（DSL）或者通过诸如数字多媒体有线网络等其它 IP 传输方法，IP 网关设备 60 提供在诸如互联网等 IP 网络 70 上到 MNO 网络的 IP 连接。因而，可以使用自家庭或办公室的现有 IP 连接提供自访问点 50 的回程。使用通过 UMA 网关 22 的 UMA 标准，通过到 MNO 核心网络或者无线电访问网络的连接可以提供到运营商网络 20 的灵活接口。此方法支持使用基于网际协议的语音（VoIP）技术的数据和语音的低成本传输。

由 UMA 未许可网络控制器（UNC）12 提供在 IP 网络 70 上从 IP 网关 60 到 MNO 无

线电访问网络 10 的连接，所述控制器已经由 3GPP 标准化为普通访问网络控制器（GANC）。也可以使用到无线电访问网络 10 的接口的其它非标准化解决方案作为替代方法。通过使用在访问点和诸如 SIP 网关或 IP 多媒体子系统等适当网关之间的 SIP 接口，可以实现到运营商核心网络的直接连接。

在该图示的实施例中，DSL 或电缆 IP 网关设备 60 包括规定用于 POTS 电话或传真设备 62 的连接，和用于提供 IPTV 服务给 TV 64 的音频/视频连接。访问点 50 包括允许将这些设备集成到 MNO 网络内，支持用户的复杂新服务的服务环境。

在本发明的替代实施方式内，可以将访问点 50 集成为在 IP 网关设备 60 内的组件；随后，内部 IP 连接将嵌入的访问点组件链接到 IP 网关设备内的路由器功能。此配置可以潜在地提供较低的整体成本，并便于运营商寻求提供统一数据、固定语音、多媒体和移动服务的网关单元。

因此，当移动电话 30 处于家庭或办公室 40 内，或者在访问点 50 的覆盖区域内时，它可以以与通过蜂窝无线通信网络内的任何其它基站相同的方式连接到 MNO 网络内。

图 1 还图示连接到 IP 网络 70 的网络服务器 72。如将理解的，在 IP 网络 70 是互联网的情况下，将大量服务器和其它设备连接到网络。如下文将更详细描述的，移动电话 30 的用户可以通过访问点 50 访问这些设备。

图 1 还图示连接到 IP 网络 70 的管理系统 74。由移动网络运营商提供管理系统 74，用于管理访问点 50 的操作，包括控制可用服务。

例如，如上所述，和如下文更详细描述的，移动电话 30 的用户可以在以太网 LAN 42 上通过访问点 50 建立到一个或多个本地 PC 或服务器 44 的连接，或者通过 IP 网关设备 60 到其连接到的另一设备的连接，或者通过 IP 网关设备 60 到连接到 IP 网络 70 的网络服务器 72 的连接。可以在此无线通信网络的核心网络 20 上不传送业务的情况下，建立这些连接。管理系统 74 能够定义设备或者 IP 地址，使用其可以建立此类连接。因此，如果移动网络运营商期望，可以仅使用有限数量的设备或 IP 地址建立这些连接。

而且，管理系统 74 能够规定分配给访问点 50 的信道（其可以由频率、时隙和/或扩频码定义，取决于特定蜂窝无线通信系统）。根据整体网络要求，可以半固定地或者可以定期改变这些信道。

图 2 是图示访问点 50 的硬件结构的示意方框图。该结构包括通过诸如 ARM AMBA 总线等处理器总线 80 互连的多个功能模块。

访问点 50 包括各种外部有线接口，包括 RJ45 以太网 10/100 接口 82，其提供到本地

LAN 的连接，用于连接到 IP 网关设备 60，从而连接到 MNO 网络和互联网，还提供到连接到以太网网络的其它设备的访问，例如一个或多个 PC 44，或者例如用于先进服务规定的 IPTV 64。因此，访问点 50 可以具有通过标准 UMA UNC 的修改版本到无线电访问网络 10 或者通过与普通 Iub（UMTS）或 Abis（GSM）接口相对的 SIP 到核心网络的基于 IP 的接口。

访问点 50 还包括用户标识模块（SIM）卡接口 84 以允许使用标准 SIM 卡提供用于访问点 50 的唯一标识符，从而识别到管理系统 74 和运营商无线电网络 10 和核心网络 20 的单元，进而支持将要提供的各种服务。

访问点 50 还包括协议引擎 216，将其实施为由用于加密的专用协处理器 88 和用于分组处理的专用协处理器 90 支持的诸如 ARM926（具有适当的外围设备）的小型内嵌 CPU，其将为主 CPU 分担特定密集任务。例如，由加密加速器 88 处理 IPSec 分组负载的加密，其支持 AES 和 3DES 加密协议。访问点 50 至 UNC 12 和管理系统 74 的 VPN 连接将使用内部加密处理；可以在访问点 50 外部处理用户 VPN 加密处理。

主 CPU 还负责通过主 CPU 总线 80 配置和控制该系统内的所有功能块，包括基带调制解调器 92 和以太网端口 82。将包括用于所有系统功能块的配置数据的系统软件映象存储在访问点 50 内的 FLASH 存储器 94 内；存储两个完整系统映象，以便可以从管理系统 74 将更新后的系统映象下载到访问点 50，同时将先前映象保存为中断下载情况下的后退选项。

主 CPU 外围设备包括：用于软件稳健检查的看门狗（Watchdog）定时器，用于系统内调试的 JTAG 和序列端口；和用于包括 LED 状态指示的系统控制、系统功率管理和系统告警收集的 GPIO。

访问点 50 包括用于在 900MHz 或 1800MHz 上的 GSM 的第一射频接口 94 和用于在 2100MHz 上的 UMTS 的第二射频接口 96。因此，支持 GSM 和 UMTS 的同时操作。对于 GSM 和 UMTS 接收路径，上行链路（基站接收）和下行链路（终端接收）频率都是可访问的；对于发射路径，仅下行链路（基站发射）频率是可获得的。在安装时，访问点 50 从由管理系统 74 提供的 GSM 和 UMTS 载波频率的许可列表中选择出对于 GSM 和 UMTS 都具有最低噪声/干扰的下行链路射频载波频率；将由将其接收路径配置为 UE 模式和禁用其发射路径的访问点 50 扫描许可的下行链路频率。

设计访问点 50 以在建筑物内在距离固定或步行（例如不超过 10km/h）用户不超过 50 米的距离上提供蜂窝服务，从而与常规宏小区基站相比，动态地降低所需要的发射功率。

然而，可以在任一功率电平上操作和处理任意类型的移动用户的任意基站上提供在此描述的功能。

射频接口 94，96 通过调制解调器模拟接口 98 连接到基带调制解调器 92，其支持用于 GSM 和 UMTS 基站调制解调器的抽样速率处理、码片速率处理（仅 UMTS）和用于 GSM 和 UMTS 的符号速率处理。

访问点 50 将具有有限的 GSM 移动站（MS）和 UMTS 用户装置（UE）调制解调器功能，从而允许访问点 50 恢复来自本地 GSM/UMTS 基站和其它相邻访问点的广播信道（BCH）。将在初始安装过程中进入 UE 调制解调器模式以观察本地射频环境，和在初始安装之后在定期间隔上监视射频环境，如果需要，修改访问点配置。

使用基于软件的结构实施基带调制解调器 92 以保证在最长 5 年的现场寿命上的高适应性，例如可升级以允许进一步增强将要在现场内发送的 HSDPA 或 EDGE 服务，而不需要替换该单元。

访问点 50 包括在 5 年使用寿命上为 GSM 和 UMTS 基站操作提供足够精确性的定时和频率基准 100。

因此，该访问点 50 的实施例提供各种操作特征。例如，它是用户可安装、自配置和适应周围射频环境的。可以将访问限制于使用标准 GSM/UMTS 协议的指定用户。此外，在连接到公共以太网 LAN 的大型室内区域内安装多个访问点可以管理在它们自身之间的越区切换，而不需要无线电网络 10 内的其它系统或者运营商蜂窝网络的核心网络 20 的干预。

图 3 提供在访问点 50 的协议引擎 86 以及加密加速器 88 和分组处理加速器 90 上运行的软件的结构概念图，重点是服务环境及其到较低栈层内的控制路径。

访问点 50 包括服务平台，其可以是四个数据网络的潜在联合，即外部 MNO 核心网络 20、外部互联网 70、诸如移动电话 30 的移动设备（通过 GSM/UMTS）和家庭网络（通过以太网）。

访问点堆栈结构包括功能强大的服务环境 120。服务环境是基于 Java 的，并包括 Java 虚拟机 122 和形式为 API 接口的访问点库 124，所述接口允许应用 126 与堆栈低层交互以控制呼叫/数据对话、业务路由选择和诸多其它功能。服务环境 120 还包括 Web 服务器 128，其提供到用户的便利接口，用于配置和监视，还用于选择和购买期望应用，带有用于通过本地 PC 的调试和维护的安全保护选项。服务环境 120 还包括管理系统（MS）客户机 130，其配置访问点 50 和监视其操作的各个方面。MS 客户机 130 控制规定系统，以便可

以替换和重新启动在如图 3 所示的系统内的任意软件组件。

如上所述，服务环境 120 还包括各种应用 126，例如由移动网络运营商或 IP 网关 60 供应商建立的，可以将其预先安装在访问点 50 内，或者可以通过在运营商安装或者在用户请求时从运营商网络下载而发送，例如作为可计费服务的一部分。

软件网络（ZN）层 132 提供对话控制功能以管理和执行确定如何配置访问点 50 的服务流和策略，和操作用于任意特定移动网络运营商（MNO）配置和终端用户设置。通过管理系统（MS）客户机 130、Java 应用或者通过 Web 服务器 128，将配置参数装载到 ZN 数据库 134。这些参数提供在访问点内用于对话控制操作的“规则”。对话控制功能包括：用于在 MNO 核心网络上的访问点 50 的登记、呼叫控制和业务流/路由选择的策略的实施；用于登记、呼叫控制和业务流的 UMA 客户机（下文将进一步描述）的控制；和在发送 GSM/UMTS 服务和通过 IP 网关 60 与其它服务接口的访问点资源的有效管理。

在软件的网络（ZN）层 132 之下，存在非访问层（NAS）功能 136，需要它以便当 MNO GSM/UMTS 核心网络 20 未连接到访问点 50 时将服务提供给 UE。此功能支持访问点 50 提供普通 GSM/UMTS 服务，例如移动用户定制的 SMS 和 MMS，同时未以常规方式连接到 GSM/UMTS 核心网络。为了提供此类服务，访问点 50 包含通常在移动交换中心（MSC）、服务 GPRS 服务节点（SGSN）、GSM 基站子系统（BSS）和 UMTS 无线电网络子系统（RNS）内包含的核心网络功能的压缩子集。

因此，如在访问点 50 内实施的非访问层 136 提供在常规 GSM/UMTS 网络内通常包含在 MSC 和 SGSN 节点内的各种功能。一种这样的特征是呼叫控制（CC）。这支持在两个对等实体之间的呼叫建立，主要用于电路交换连接。

NAS 层 136 还提供：对话管理（SM），用于控制分组数据对话；短消息服务（SMS）功能，用于在访问点 50 和网络 SMS 服务中心之间的 SMS 消息传输；辅助服务（SS），例如呼叫等待、呼叫保持和多方呼叫；移动性管理/GPRS 移动性管理（MM/GMM），用于管理 UE 移动性单元，例如位置登记、鉴权和加密；和与可以安装在访问点 50 内的 USIM 卡相关的控制功能。访问点 50 还提供分组路由选择性能，其本质上是在常规网络内的 GGSN 功能。

在 NAS 功能之下，存在访问层功能，具体而言 UMTS 访问层功能 138 和 GERAN 访问层功能 140。

UMTS 访问层功能 138 包括一些 SGSN 功能、无线电网络控制器（RNC）功能和在基带调制解调器 92 上实施的到 UMTS 物理层的接口。对于支持 UMTS 的所有访问点服

务都需要 RNC 和物理层接口功能，而与所使用的核心网络接口无关。

更详细地，访问层功能包括下述单元：

分组数据收敛协议（PDCP）

IP 数据流的首部压缩和解压缩（可选）、用户数据传输、PDCP 序列号的维护（通常是 SGSN 功能的一部分）。

无线电资源控制（RRC）

NAS 和 AS 相关信息的广播；RRC 连接的建立、维护和释放；无线电载体和无线电资源的建立、重新配置和释放；RRC 连接移动性功能；所请求 QoS 的控制；UE 测量报告和控制；外环功率控制；加密控制。

无线电链路控制（RLC）

信令和数据分组的发送和接收，包括分组的缓冲、分段和级联。包括三个实体类型，用于确认模式、未确认模式和透明模式。

介质访问控制（MAC）

在逻辑信道和传输信道之间的映射、选择用于每个传输信道的适当传输格式、UE 之间的优先权处理、在公共和专用传输信道上到/自传输块（组）的上层 PDU 的复用/解复用。

UMTS 层 1

在基带调制解调器上实施的到 UMTS 调制解调器功能的接口。

GERAN 访问层功能 140 包括 BSS 和一些有限 SGSN 功能。需要 BSS 功能以支持全部的 GSM/GPRS/EDGE 服务，而与在访问点 50 和 MNO 核心网络 20 之间使用的接口无关。

GERAN 访问层 140 的 SGSN 功能包括下述单元：

子网络依赖收敛协议（SNDCP）

若干分组数据协议的复用；数据压缩/解压缩（可选的）；首部压缩/解压缩（可选的）；分段和重新装配。

逻辑链路控制（LLC）

LLC 提供对等未确认和确认数据传输和 GPRS 加密功能。

GERAN 访问层功能 140 的 BSS 功能包括下述单元：

无线电链路控制/媒体访问控制（RLC/MAC）

RLC/MAC 支持确认和未确认模式；LLC PDU 的分段和重新装配；复用到若干物理

信道；广播系统信息。

无线电资源管理（RR）

RR 连接建立；维护和释放；系统信息广播；分组数据资源管理。

GSM/GPRS 层 1

到在基带调制解调器内实施的 GSM/GPRS/EDGE 调制解调器功能的接口。

因而，如上所述，访问点 50 包括通常位于用于 UMTS 和 GSM 标准的无线电访问网络的更高层内的一些功能。这是部分因为，为了能够将数据业务路由选择到 MNO 核心网络，或者到互联网或者到在局域网上的设备，访问点 50 必需访问流向和流出远程设备的数据分组。然而，非常希望通过与在其余蜂窝网络内使用的相同加密机制确保到蜂窝设备的空中接口。因此，如果希望予以维持，因而，为了支持上面描述的服务和路由选择性能，访问点 50 应当包含用于空中接口加密的端接功能（即在 UMTS 内的 RLC/MAC 层）。

在访问点 50 内运行的软件还包括 UMA 客户机 142，允许访问点 50 在非标准配置内使用 UMA 协议。具体而言，设计标准 UMA 协议以支持 GSM MS 或者 UMTS UE，其包括 UMA 客户机和诸如 IEEE 802.11b/g 或蓝牙等未许可频谱空中接口，以使用未许可频谱与 GSM/UMTS 核心网络通信。然而，在访问点 50 内的实施方式使用 UMA 客户机作为 GSM/UMTS 基站的网络接口的一部分，以便可以修改开发以通过未许可网络控制器（UNC）与 GSM/UMTS 核心网络通信的 UMA 协议以管理由该基站处理的呼叫，包括到/自宏网络的越区切换。如先前指出的，可以使用 SIP 接口作为替代方法。

访问点 50 还包括一个或多个 IP 设备客户机 144，以支持在“移动域”（驻留到访问点 50 上的移动电话和到 MNO 核心网络 20 内的业务路径）和其它 IP 设备之间的呼叫、控制信息或数据的传输，所述其它 IP 设备例如是用于固定线路电话/传真服务的在 IP 网关 60 内的 VoIP/POTS 端口、在用于 IPTV 和/或视频服务的 IP 网关 60 内的 AV 端口、在本地以太网 LAN 上的 PC 或服务器 44 或者通过 IP 网关 60 在互联网 70 上可访问的远程网页和/或服务器 72。

每个 IP 设备客户机 144 访问在访问点 50 内的业务路径，并可以由在 ZN 层 132 内的对话控制器控制，所述控制器可以开始和结束与可访问 IP 设备的呼叫/数据对话。在访问点 50 内包括专用于特定设备或服务的 IP 设备客户机的软件结构支持将在访问点 50 内路由选择来自该特定设备或服务的业务，以便可以将其连接到通过 GSM 或 UMTS 访问层访问的 GSM/UMTS 移动设备或者通过 UMA 客户机访问的 MNO 核心网络。

此外，每个 IP 设备客户机 144 访问在 LAN 上的其它设备，并还访问在互联网 70 上

可访问的其它设备。例如，通过使用适当的IP设备客户机144，可以在互联网70上将连接到访问点50的POTS电话连接到另一个POTS电话，从而进行语音呼叫。

而且，每个IP设备客户机144访问MNO的移动网络。具体而言，连接到LAN 42的任意设备或者连接到IP网关60的任意设备可以具有IP设备客户机144，该客户机可以关联自身与连接到SIM接口84的SIM卡。从MNO网络的观点来看，任一此类设备因此看起来将是移动的，并将允许其访问MNO网络。因此，通过提供具有适当期望功能的设备，随后使用USIM卡以允许在MNO核心网络上将该设备连接到一个或多个其它设备，可以将各种服务提供给用户。

进一步使用连接到USIM接口84的SIM卡以允许驻留到访问点上的移动电话以类似于多扩展无绳电话系统的方式工作。在该特定服务配置内，在访问点50内的USIM卡承载IMSI标识符，其实际上定义安装访问点50的家庭或办公室的电话线路，尽管它在移动网络运营商的系统看起来是移动号码。当呼叫在访问点50内SIM卡的IMSI时，振铃驻留到访问点50的全部移动电话，直到它们中的一个应答。以这种方式，将把到个人的来话呼叫引导到该个人的移动电话的IMSI编号，因此可能不同于通过呼叫IMSI标识符呼叫在家庭或办公室内任一用户的呼叫。当呼叫访问点自身的IMISI标识符时，则改变访问点50的呼叫处理功能。

因而，概括地说，访问点50包括由访问点使用其频谱的运营商，即相关移动网络的运营商发出的UMTS SIM卡。USIM卡承载用于移动终端的标准标识信息，最显著地，作为与SIM卡关联的电话号码的IMSI标识符和MSISDN编号。使用IMSI标识符标识访问点，予以鉴权，和使用与用于经IP接口访问MNO网络的包含SIM卡的移动终端完全相同的机制，建立经IP互联与MNO网络的安全通信。为终端设备到MNO网络的IP连接，最普通地为无线LAN或WiFi，UMA和WLAN/IMS标准接口占主流的设备，定义多个标准接口。(还可以接口支持包括SIM卡的IP设备的所谓的“Pre-IMS”系统以使用此原理)。在下文中更详细地描述这些接口的程序，但是此原理扩展到设计以支持到MNO网络内包含SIM的远程设备的任意接口。

通过在访问点50内包含SIM支持的另一性能是访问点可以与移动终端一样与MNO网络通信。具体而言，访问点能够发出到其它移动终端或固定线路设备的呼叫和接收自其的呼叫，以初始化和结束与其它设备的数据对话和发送和接收SMS和MMS消息。这允许由访问点支持大量有用的功能，包括：

• 接收来自在访问点上预先登记的用户之一的关键字SMS消息，其指示访问点执行

特定功能，例如将新用户添加给在访问点内存储的“许可用户”列表（可选地，访问点可以使用该对许可用户的改变更新管理系统 74 以维持在数据库之间的同步）。此性能可以与访问点内的应用功能和适当的 IP 设备客户机组合，从而可以在用户的家庭网络上初始化这些动作，例如编程基于 PC 的视频记录器或者启动窃贼告警或加热控制。

• 将 SMS 或 MMS 消息发送给用户以向它们警告重要信息，例如新许可用户成功地添加到访问点，或者特定用户变得驻留到访问点上（即已经到家），或者错误状态，例如由于高电平干扰导致在安装处不能提供服务。可以组合此设备与访问点应用和适当的 IP 设备客户机 144，以便当在家庭外部时，可以将用户家庭网络内的活动中继给用户；例如，作为 MMS 消息，可以将由安全网络摄像机采集的在用户家门口的呼叫者的照片转发给用户。

• 接收在广域网内由用户启动的呼叫/数据对话，以便用户能够访问用户家庭网络的相关信息，例如来自安全网络摄像机的现场视频或者浏览在用户家庭 PC 服务器内存储的信息。

• 启动呼叫/数据对话，以便当由事件触发或者在预定时间上，访问点可以将信息“推送”给用户。例如，使用在访问点 50 内的适当 IP 设备客户机 144 和在访问点和家庭 PC 服务器内的适当应用软件，可以将下载到用户家庭 PC 上的多媒体新闻剪辑转发给用户电话，或者由股票跟踪软件或互联网拍卖站点生成的告警可以启动到用户的呼叫以邀请对触发事件的响应。

将由访问点 50 启动的消息、呼叫和数据对话引导到 MNO 网络，以便由在广域宏小区网络内的用户能够予以接收；可选地，可以将逻辑电路包括在访问点内以识别出消息/呼叫/数据对话的接收者是否已经驻留到小区上，以便可以在访问点 50 的空中接口上直接启动事务处理，而不浪费不必要的核心网络资源。以类似的方式，将从核心网络直接接收由访问点 50 端接的消息、呼叫和数据对话；可选地，访问点可以筛选输出事务处理以识别出其自身的 MSISDN 是否是事务处理的预期接收者，从而确定是否截取该呼叫以避免不必要地使用核心网络资源。

图 4 是移动通信网络的方框示意图，其中使用修改版本的现有标准 UMA 接口将访问点（AP）50 连接到核心网络以支持回程。在此将其称作 3G 许可 UMA（L-UMA）或 3G L-UMA。在图 4 中，访问点（AP）50 还包括图 1 所示的 IP 网关 60 的功能。

UMA 或 3GPP GAM 标准定义在 GANC 控制器和 UE 之间的接口，Up 接口。访问点 50 使用标准化消息将其自身登记和鉴权为移动设备，和建立到核心网络的安全 IPSec 通

道。

图 4 图示单个 UE 30，尽管多个 UE 可以驻留到单个访问点 50 上。UE 是没有附加客户的 3GPP 标准 UMTS UE。它们可以是手机、PDA、PC 卡或任何其它形式因素。

使用 POTS 或 SIP 电话 62 通过访问点 50 发出家庭号码呼叫。

PC 客户机 44 控制本地服务优先级、关系和动态呼叫/对话行为。可以将软电话功能包括在 PC 客户机内。

访问点 50 提供下述功能：

它提供在 3GPP 标准上的本地 UMTS 覆盖。

它包括 USIM160，其专用于访问点 50 规定、配置和与核心网络鉴权，并支持用于家庭号码服务的 UMTS 服务。

它在 3GPP 标准 Uu 接口上与多个 UE 30 对接，结束本地 AS 和 NAS 层。

它在 POTS 接口或者到独立 VoIP（SIP）电话的家庭网络/以太网接口上与本地 POTS 或 SIP 电话 62 对接。

它经以太网接口 82 在 IP 上与本地 PC 客户机 44 和软电话对接。

它经 Itf-Zz 接口与其它本地或远程访问点 162 对接。

它在不涉及 CN 网络信令的情况下发送本地服务，包括本地呼叫处理和本地互联网下载。

它在 Up'接口上通过普通 IP 访问网络 70 与 L-GANC 164 对接，用于 RRC 等同信令和键控资料交换。

它在 3GPP 标准 Uu（NAS）接口上通过 Up'接口与 CN 合法 NE（MSC 166，SGSN 168）接口，用于 NAS 层信令（MM，CC/SS/SMS，GMM，SM）。

它在 Itf-Zz 接口上通过普通 IP 访问网络 70 和 L-GANC 安全网络 170 与管理系统（ZMS）74 对接，用于网络管理、服务管理、软件升级、故障报告、活动监视和故障诊断。Itf-Zz 通过 L-GANC 安全网关 170 连接。

它在 Gi-L（本地 Gi）接口上与公共数据网络和互联网 172 接口，以在没有核心网络的参与下提供到本地数据的直接访问和本地互联网下载服务。

普通 IP 访问网络 70 提供在访问点 50，162 和 L-GANC 164 之间和在访问点 50，162 和互联网 172 之间的 IP 连接性。普通 IP 访问网络可以应用 NAT/PAT，通常是常规的。

3G L-GANC 164 是 UMTS 许可普通访问网络控制器。该 L-GANC 164 提供下述功能：

它提供与 UMTS 结构内的 RNC 的功能等同的功能。

它提供在普通 IP 访问网络 70 上到核心网络的安全访问。

它包括用于鉴权和 IPSec 通道的标准安全网关 170。

它在 3GPP 标准 Wm 接口上与核心网络 AAA 174 接口，用于支持鉴权、授权和记帐程序。

它在 Up'接口上通过普通 IP 访问网络 70 与多个访问点 50，162 接口，用于 RRC 等同信令和键控资料交换。

它提供用于在访问点 50 和 ZMS 74 之间的 Itf-Z 的安全传输。

它在 3GPP 标准 Iu-CS 接口上与核心网络 MSC 166 接口，用于支持电路交换服务。

它在 3GPP 标准 Iu-PS 接口上与核心网络 SGSN 168 接口，用于支持分组交换服务。

它提供用于在访问点 50 和核心网络 MSC 166 和 SGSN 168 之间的 3GPP 标准 Uu（NAS）接口的安全传输。

它在 3GPP 标准 Lb 接口上与核心网络 SMLC 176 接口，用于支持在访问点网络内漫游的 UE 的位置信息。

它在 3GPP 标准 CBC-RNC 接口上与核心网络 CBC 178 接口，用于支持小区广播服务。

管理系统（ZMS）74 提供用于访问点 50 的 OAM&P 功能。

更具体地：

它使用在 DSL 论坛 TR-069 规范内描述的程序和方法管理访问点 50。

它负责在安装处理过程中提供访问点 50。

它监视由所管理访问点报告的故障。

它提供用于运营商管理每个访问点 50 的配置的装置。

它提供具有安全性以限制用户已经访问的功能的用户接口。

它使用安全 IP 连接在 Itf-Z 上与访问点 50 对接。

它提供管理用于访问点的软件升级的装置。

它收集由访问点报告的性能量度。

它与客户服务和网络操作中心对接。

UMTS 核心网络单元 MSC 166，SGSN 168，AAA 174 和 HLR/HSS 180 是 3GPP 标准单元，将不作进一步描述。

访问点 50 使用标准 UE 机制鉴权自身。使用 IMS/SIP 情况作为例子予以图示。3GPP

IMS 标准包括用于支持包含 SIM 卡的无线 LAN UE 的接口的定义，在此称作 WLAN/IMS 接口。因为访问点 50 包括 SIM 卡 160，它可能看起来是包含 SIM 卡的无线 LAN UE，以便可以重复使用此机制以鉴权 MNO 核心网络内的访问点 50。在非标准的所谓“Pre-IMS”解决方案中包括非常类似的机制，明确地设计许多这种解决方案以支持在常规 3GPP 网络内包含无线 LAN 设备。

因此，图 5 图示标准 WLAN/IMS 接口，由此 WLAN UE 190 在 3GPP 网络 194 内与分组数据网关（PDG）192 鉴权自身。

图 6 图示在此使用的鉴权机制的修改版本。实际上，访问点 50 使用如在 3GPP 标准内规定的相同鉴权机制与 AAA 服务器鉴权自身，和建立在分组数据网关（PDG）200 上结束的安全 IPSec 通道。

访问点建立到家庭网络的专用于自身的 IPsec 通道。因此，在启动访问点 50 之后，它从与 DSL 访问关联的 ISP 获取本地 IP 地址。随后，访问点 50 需要用于若干目的的到家庭网络的安全专用 IP 连接，例如远程配置，为 POTS 电话提供 VoIP 支持，和当代表连接到访问点的每个 UE 建立 UE 专用 IPsec 通道时，UE 专用键控资料的安全发送。通过建立到家庭网络内的 PDG 200 的 VPN 类 IPsec ESP 通道予以实现。

该访问点的优势在于它包含家庭 MNO 网络规定 USIM，以与根据 R6 TS 23.234 的 WLAN UE 完全相同的方式，使用 IKEv2 和 EAP/AKA 鉴权建立此通道。

在通道建立上执行下述步骤：

1．访问点获取在家庭 MNO 网络内 PDG 200 的 IP 地址。

2. 访问点使用 IKEv2 和 EAP-AKA 鉴权以建立到在该处理中获取远程 IP 地址的 PDG 200 的 IPsec 通道。

以类似于在 WLAN 3GPP 互通框架内 W-APN 的方式，使用指向 PDG 200 的完全资格域名(FQDN)本地地配置该访问点。访问点 50 通过在 FQDN 上的 DNS 程序解析 PDG 200 的 IP 地址。如在 WLAN 3GPP 互通的情况下，假设 PDG 200 的 FQDN 存在于公共 DNS 内。

访问点使用基于 IMSI 的网络访问标识符，ANI，以向家庭 MNO 网络标识自身，例如：

0.<IMSI_ZAP>@.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org 或

IMSI_ZAP@.zap.home_network_domain.

其中：

IMSI_ZAP 是位于访问点内的 USIM 的 IMSI。

MNC 是家庭 MNO 网络移动网络代码和 MCC 是移动国家代码。

可以使用前缀 0 表示请求 AKA 而非 SIM 鉴权。

对于基于 IKE 的通道建立程序，访问点将调整 IKEv2 的本地 NAT 横向支持，即 IETF RFC 3948“IPsec ESP 分组的 UDP 封装”，以处理访问点位于 NAT 设备之后的（可能）事实。

图 7 图示在家庭 MNO 网络内在访问点 50 和 PDG 200 之间设置 IPsec 中涉及的信令。这假设家庭 MNO 网络结构类似于 3GPP-WLAN 互通所考虑的结构。然而，该解决方案并不严格的取决于网络结构的相关假定，该结构支持至如下所述的 PDG 信令的访问点是足够的。尽管在访问点/USIM 和家庭 MNO 网络之间的通道建立程序完全按照 R6 TS 23.234，在此在某些细节上予以描述，从而可以描述当访问点代表每个 UE 建立 UE 专用通道时需要的改变（用于将 UE 专用键控资料发送给访问点）。

在访问点已经将 PDG 的 FQDN 解析成 IP 地址之后，它启动通道建立程序。

在步骤 701，访问点 50 将 IKE_SA_INT 消息从其 UDP 端口 500 发送到 PDG 200 内的 UDP 端口 500。此消息启动在访问点和 PDG 之间的 IKE SA 的建立，它包含：

承载所支持的加密组，例如在 TS 33.234 内的组#2 的 SAI 负载：

加密：在 CBC 模式内具有固定密钥长度的 AES；

完整性：AES-XCBC-MAC-96；

伪随机功能：AES-XCBC-PRF-128；

Diffie-Hellman 组 2

访问点的 Diffie-Hellman（DH）公共密钥，Kei 和当前 Ni；承载源 IP 地址（访问点的本地 IP 地址）和源端口的散列信息的 NAT_DETECTION_DESTINATION_IP 负载。

在步骤 702，PDG 200 接收 IKE_SA_INIT 消息和前进以计算承载其的分组的源 IP 地址和源端口编号的散列信息。如果它不同于在 NAT_DETECTION_DESTINATION_IP 负载内的值，则 PDG 获知访问点在 NAT 之后。PDG 还计算在 NAT_DETECTION_DESTINATION_IP 负载内的其 IP 地址和带有该地址的端口的散列信息。如果这不同，则 PDG 获知它自身在 NAT 之后，在这种情况下，它应当开始发送保持活动分组以保持该 NAT 绑定不改变。以与访问点相同的方式，PDG 生成其自身的 NAT_DETECTION_SOURCE_IP 和 NAT_DETECTION_DESTINATION_IP 负载，从而允许访问点确定它和/或 PDG 是否在 NAT 之后。

PDG 使用所接收的 Kei 和 Ni 以及其专用 DH 密钥和其自己生成的当前 Nr 以生成七个秘密共享密钥：

SK_ai/SK_ar，将由完整性保护算法（AES-XCBC-MAC-96）用于保护 IKE 信令。

SK_ai/SK_er，将由加密算法（在 CBC 模式内 AES）用于保护 IKE 信令。

SK_d，SK_pi/SK_pr。

通过发 IKE_SA_INIT 响应，PDG 完成 IKE SA 的协商。在承载 IKE_SA_INIT 的 IP 分组内将其（从端口 500 到端口 500）发送给源 IP 地址，从而确保其返回访问点，而与 NAT 的存在无关。这包含：

承载访问点建议加密组从而确认其接收的 SAi 负载；

PDG 的 Diffie-Hellman（DH）公共密钥，Ker 和当前 Nr；

承载源 IP 地址（PDG 的本地 IP 地址）和源端口（500）的散列信息的 NAT_DETECTION_SOURCE_IP 负载；

承载目标 IP 地址（访问点的 IP 地址）和目标端口（500）的散列信息的 NAT_DETECTION_DESTINATION_IP 负载。

在步骤 703，当访问点接收 IKE_SA_INT 响应时，它以与 PDG 相同的方式检查 NAT_DETECTION_SOURCE_IP 和 NAT_DETECTION_DESTINATION_IP 负载，以检测它和/或 PDG 是否在 NAT 之后。如果检测到 NAT，则访问点将切换以将所有未来 IKE 信令从端口 4500 发送给端口 4500。

PDG 使用所接收的 KEr 和 Nr 以及其专用 DH 密钥和其自身生成的当前 Ni 以生成相同的七个秘密共享密钥：如同 PDG 向前所做的，并开始使用 SK_ai/SK_ar 和 SK_ei/SK_er 保护全部未来 IKE 信令。

此时，已经建立 IKE SA，访问点和 PDG 可以安全地通信但是不存在鉴权。通过发送第一 IKE_AUTH 请求消息，由访问点启动此操作。访问点通过 Idi 负载维护它的 IMSI 推导标识。它还宣称通过不包括通过这两种方法之一生成的 AUTH 负载，将 EAP 用于其鉴权而非缺省 IKEv2 鉴权方法（基于预共享的秘密密钥或者基于证书）的它的意图。

IKE_AUTH 请求消息还启动将保护将在通道上承载的全部业务的 IPsec ESP SA（CHILD_SA）的建立。该消息包含：

带有访问点标识的 IDi 负载；

IMSI_ZAP@.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org

带有 PDG FQDN 的 IDr 负载

需要在 PDG 上的远程 IP 地址（以结束 IPsec 通道）和潜在地位于家庭 MNO 网络内的 DNS 服务器的 IP 地址（例如用于 P-CSCF 发现）的 CP 负载；

SAi，包含支持用于保护在通道内承载的业务（即通过 IPsec ESP SA）的一个或多个加密组的启动者的（即访问点的）安全关联负载，例如在 TS 33.234 内的组#2：

加密：在 CBC 模式内带有 128 比特密钥的 AES；

完整性：AES-XCBC-MAC-96；

通道模式；

TSi，TSr 包含标识将在通道上承载的 IP 流（源范围－目标范围）的建议业务选择器。

在步骤 704，通过发送包含宣称标识 IMSI_ZAP@.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org 的 EAP 鉴权请求消息，PDG 请求 AAA 服务器鉴权访问点。

在步骤 705，如果 AAA 并不具有正确的 AKA 鉴权矢量（RAND，AUTN，RES，CK，IK），它与 HSS 通信以获得一个。HSS 将运行用于 IMSI_ZAP 的 AKA 算法以鉴权矢量生成。

在步骤 706，AAA 服务器使用 CK 和 IK 以生成用于 IMSI，（MSK_ZAP）的主对话密钥和用于保护 EAP-AKA 分组的附加密钥（TEK）。

在步骤 707，AAA 服务器使用矢量内的 AUTN 和 RAND 以鉴权自身，和通过 PDG 将承载（RAND，AUTN）的 EAP-请求/AKA 质询消息发送给访问点，质询访问点 AKA 鉴权自身。它还承载 MAC 以允许访问点确定不在途中篡改该 EAP 分组。

在步骤 708，PDG 在 IKE_AUTH 响应消息内将 EAP-请求/AKA-质询（RAND，AUTN，MAC）转发给访问点，并包括证书以向访问点鉴权自身（除了在步骤 718 内执行基于 EAP-AKA 的鉴权）。

在步骤 709，访问点使用它的 USIM 以运行 AKA 算法，即它：

计算 MAC 以检查该 EAP 消息未被篡改；

检查 AUTN 正确性；

生成（RES，CK，IK）。

此外，访问点根据 CK、IK 和 IMSI_ZAP 计算 MSK_ZAP 点。

在步骤 710，通过在新 IKE_AUTH 请求消息内封装的 EAP-请求/AKA-质询内发送 RES 值，访问点鉴权自身。它还可以检查 PDG 证书的正确性。

在步骤 711，PDG 将 EAP-请求/AKA-质询（RES）转发给 AAA 服务器，其比较它与

从 HSS 接收到的 RES 值以鉴权该访问点。

在步骤 712，如果鉴权成功，则 AAA 服务器在成功鉴权应答内封装的 EAP 成功负载内将 MSK_ZAP 转发给 PDG。

在步骤 713，PDG 请求 AAA 服务器授权访问点使用与其 FQDN 相关的服务（如 W-APN）。

在步骤 714，AAA 服务器检查与 IMSI_ZAP 关联的概况以确定是否能够建立通道。

在步骤 715，AAA 服务器确认通道建立的授权。

在步骤 716，通过在 IKE_AUTH 响应内发送 EAP 成功负载，PDG 向访问点通知与 AAA 服务器的鉴权成功。

在步骤 717，通过使用 MAK_ZAP 签名步骤 701 的 IKE_SA_INIT 消息和在新 IKE_AUTH 请求消息的 AUTH 负载内包括结果，访问点向 PDG 鉴权自身。

在步骤 718，PDG 使用其 MSK_ZAP 的确认以检查 AUTH 负载，从而鉴权访问点。随后，通过签名步骤 702 的 IKE_SA_INIT 响应，PDG 使用 MSK_ZAP 生成其自身的 AUTH 负载，从而向访问点鉴权其标识。PDG 在 IKE_AUTH 响应消息内予以发送。此外，PDG 发送在配置负载（CFG_REPLY）内通道的签名远程 IP 地址，和协商的加密组（与所推荐的相同），SAr2 和业务选择器 TSi，TSr，从而完成将保护在通道内所有业务的 IPsec ESP SA 的协商。最后，访问点使用其 MSK_ZAP 的确认以检查 AUTH 负载，从而鉴权 PDG。

访问点 50 包括用于 UMA 和 WLAN/IMS 接口的客户机软件功能（专用于特定非标准 Pre-IMS 解决方案的客户机软件也可以包括在访问点内）。客户机功能允许访问点对于 MNO 网络看起来是如上所述的终端设备，但是它们还包括互通功能以允许驻留到访问点 50 上的标准 GSM/UMTS 终端对于 UMA 或 IMS 接口看起来分别是 UMA 设备或 WLAN UE。（再次，可以将相同原理扩展到基于专用 Pre-IMS 解决方案的围绕 SIP，其具有与 SIP/IMS 方法的高度通用性）。可以使用为移动设备开发的 SIP 和 UMA 客户机作为这些客户机功能的基础－对于移动运营商的巨大优点在于在访问点 50 内而不是在电话内支持能够在 IP 网络上访问的客户机，以便可以继续使用合法电话与基于 IP 的访问网络，降低运营商的投资和改善对客户的服务。

应当使用标准 GSM/UMTS 程序加密从访问点 50 到移动终端的空中接口。为了支持加密，访问点 50 需要访问从 MNO 核心网络直接分配给 UE 的加密密钥信息。为了便于访问加密密钥信息，已经对标准机制进行小型修改以允许访问点使用 UE 标识访问通常仅提供给 UE 的密钥。仅在已经由核心网络鉴权访问点 50 之后，以便它是“可信单元”，启

动此处理。此外，所包含的密钥是必需为每次呼叫刷新的临时密钥－不与访问点交换主密钥。

下面更详细地描述此用于 UMA 和 SIP/IMS 接口的此互通原理的实施。

互通功能的一个用途是支持使用 UMA 的 UE 访问和加密密钥交换。如上所述，访问点 50 在普通 IP 访问网络上连接到核心网络。存在此连接的两个选项，移动网络运营商必需能够在部署时选择：

安全 IP 访问，其中将安全 IPsec 通道应用于所有访问点至核心网络通信，包括访问点专用 IPsec 通道和 UE 专用 IPsec 通道；和

专用 IP 地址，其中 MNO 拥有或直接控制 IP 访问网络，其不通过任意专用 PDN 进入，在这种情况下，MNO 可能不希望具有 IPsec 管理和开销，并可以依赖于专用 IP 访问的内在安全。

如果 MNO 要求普通 IP 访问网络的安全 IP 访问，则下文应用。在启动时，使用基于 USIM 的鉴权，访问点建立与 SeGW 的 IPsec 通道。使用访问点 IPsec 通道：

支持访问点信令和网络管理功能；

支持家庭号码服务，用于非 UE 呼叫（类似 POTS）和固定线路替换。

对于漫游到访问点覆盖区内的每个 UE，使用基于 USIM 的鉴权（使用访问点作为代理），访问点建立与 SeGW 的一个或多个 UE 专用 IPsec 通道。图 8 图示一个例子，图示图 4 系统的相关部分，其中存在第一 UE（UE1）210 和第二 UE（UE2）220。在这种情况下，UE1 是提供关联高 QoS PDP 上下文 230 和 MNO 数据服务（例如 MMS）和通过 GGSN 关联最佳努力 PDP 上下文 232 和互联网的 CS 服务的 UE，而 UE2 是仅 CS 的 UE，例如终端用户未为其启动数据连接性的 UE。

在该例子中，访问点 50 建立用于两个 UE 中每个 UE 的相应通道，即用于第一 UE 210 的第一通道 222，和用于第二 UE 220 的第二通道 224。这些通道承载 CS 业务和可选地第一 PDP 上下文。在该例子中，访问点 50 还建立与 SeGW 的附加 IPsec 通道 226，228，例如用于多个/次要 PDP 上下文的 QoS 区分。

访问点 50 还用具体例子说明对于合法 UE 透明的用于 CN 信令的 UE NAS 和 L-UMA 客户机。可选地，访问点支持本地互联网下载。

在其它例子中，可以存在每访问点一个通道和每 UE 一个通道，或者修饰所有业务的每访问点的一个通道（在外部 IP 首部上的 QoS 区别），或者 IPsec 通道，但是 PPP 或者从访问点到核心网络的等同物。

在下文中规定高层安全结构。

IP 互通安全

在家庭外部存在防火墙。而且，在安全 IP 访问选项而非专用 IP 地址选项的情况下，通过在访问点和 CN 安全 GW 之间的 IPsec 通道保护所有通信的安全，存在每个访问点的一个 IPsec 通道和每个 UE 至少一个，全部使用基于 USIM 的鉴权。

访问点层安全

访问点与管理系统 74 鉴权服务；访问点向 W-GANC 登记；使用基于 USIM 的 MM 层鉴权，访问点与 CN MSC/SGSN 鉴权呼叫/数据服务。而且，在安全 IP 访问选项而非专用 IP 访问选项的情况下，访问点与 CN 安全 GW 鉴权和建立基于 USIM 的 IPsec 通道。

UE 层安全

筛选每个 UE 以由访问点（由 IMSI）本地地访问，UE 向 L-GANC 登记，UE 与用于呼叫/数据服务的 CN MSC/SGSN 和与访问点鉴权，所述访问点用作代理，使用与 MSC/SGSN 的基于 USIM 的 MM 层鉴权，使用在 MM 鉴权程序中捕获的 IK，CK，存在对 UE 和访问点之间无线电接口的加密。在 RANAP 安全模式命令，MSC 将这些发送给 L-GANC，L-GANC 在当前 GA-CSR(URR)消息的扩展上或者在新的专用消息上，L-GANC 将它们转发给访问点。而且，在安全 IP 访问选项而非专用 IP 访问选项的情况下，可以在访问点专用 IPsec 通道上承载与核心网络的初始 UE 信令，UE 与核心网络安全 GW，与访问点（基于 USIM）鉴权，所述访问点用作代理和建立 UE 专用 IPsec 通道和可选地建立附加 IPsec 通道，用于次要/多个 PDP 上下文建立，用于 QoS 区别，除非仅使用每个访问点的一个 IPsec 通道。

在访问点 IPsec 通道建立的情况下，当使用安全 IP 访问选项时，用于访问点的 IPsec 使用基于 USIM 的鉴权。不需要改变标准 IKEv2 和 EAP-AKA 程序。

根据标准程序，访问点 IPsec 通道建立继之以向 L-GANC 的访问点登记，再次根据标准程序，访问点 MM 鉴权。

在安全 IP 访问选项的情况下，假设不仅仅存在每个访问点单个 IPsec 通道，建立 UE IPsec 通道。在这一阶段不开启无线电加密，该程序必需是基于 UE USIM。

在已经建立 IPsec 通道之后，访问点 L-UMA 客户机在标准程序之后向 L-GANC 登记 UE。

使用 MM LAU 程序同步无线电加密与 MSC。使用 MSC 在 IuCS RANAP 安全模式命令内已经发送给 L-GANC 的加密材料，在这一阶段在访问点内存储加密密钥（IK，CK）。

L-GANC 在当前 GA-CSR（URR）消息的扩展上或者在新的专用消息上将它们转发给访问点。

图 9 详细图示在电路交换登记的情况下，其中在 MSC 内支持鉴权和加密，用于执行 MM 位置区域更新和加密的程序。

在步骤 901，通过将位置更新请求消息发送给访问点 50，UE 30 可以在空闲模式内执行 PLMN 和/或小区选择/重新选择。该消息可以包含 UE 的 IMSI 或 TMSI。

在步骤 902，可以由访问点启动识别程序，从而从 UE 获得 IMSI，如果在位置更新请求消息内仅接收到 TMSI。

步骤 903 仅可以应用于安全 IP 地址选项（而不可应用于每个访问点选项的单个 IPsec），否则该程序直接继之以步骤 904。执行 IKEv2 和 EAP-AKA，从而建立在访问点和 UNC 之间的安全 IPsec 通道。在 EAP-AKA 过程中，将执行鉴权和安全程序。在这种情况下，在 EAP-AKA 程序中将安全模式消息发送给 UE。

在步骤 904，一旦成功建立 IPsec 通道，访问点生成 URR 登记请求消息和将其发送给 UNC，从而将 UE 登记到 UNC 上。我们假设服务 UNC 已经由访问点发现，在步骤 905，从 UNC 接收 URR 登记接受消息，表示已经将 UE 登记到 UNC 上。

在步骤 906，将从 UE 接收到的原始位置更新请求消息传送给在 URR UL 直接传输包装器内的 UNC，在步骤 907，UNC 将位置更新请求传送给在 MSC 内的 MM 子层。

假设在 3G MSC 内支持鉴权和加密，则在步骤 908，MM 子层生成包含 3G RAND 和 AUTN 参数的鉴权请求消息，和在步骤 909，UNC 生成包含鉴权请求的 URR DL 直接传输消息并将其发送给访问点。

在步骤 910，访问点接收 URR DL 直接传输和将鉴权请求消息发送给 UE。

在步骤 911，UE 执行 3G 鉴权程序，和生成 RES，将其在鉴权响应消息内发送给访问点。在步骤 912，访问点在 URR UL 直接传输内将鉴权响应消息发送给 UNC，和在步骤 913，UNC 接收 URR UL 直接传输和将鉴权响应消息发送给 MSC。

在步骤 914，在 MSC 内验证在鉴权响应内包含的 RES。通过将安全模式命令发送给 UNC，其应当包含 CK 和 IK 加密和完整性密钥，支持加密。在步骤 915，UNC 将在修改 URR 加密模式命令(或新消息 URR 安全模式命令)内的加密和完整性信息发送给访问点。

作为响应，在步骤 916，访问点生成包含 UEA(加密算法)、UIA(完整性算法)、FRESH 和 MAC-I 信息的安全模式命令消息。应当指出 UEA、UIA、FRESH 和 MAC-I 可以来自访问点。

在步骤 917，将安全模式完成消息从 UE 发送给访问点，和在步骤 918，访问点生成修改的 URR 加密模式完成消息（或新的 URR 安全模式完成消息）。在步骤 919，UNC 将加密模式完成消息发送给 MSC。

在步骤 920，MSC 将位置更新接受消息发送给 UNC，和在步骤 921，UNC 将包含位置更新接受的 URR DL 直接传输消息发送给访问点，和在步骤 922，访问点将位置更新接受发送给 UE 以完成登记程序。

因此，L-GANC 164 将加密密钥转发给访问点 50，用于无线电加密。IuCS 消息是标准消息，L-UMA 消息是标准 UMA 消息的演变。

作为上述的替代，或者附加的，可以在访问点内提供互通功能以支持使用 3GPP WLAN/IMS 接口的 UE 访问和加密密钥交换。访问点 SIP 框架重复使用 3GPP-WLAN 互通框架的这些方面，它们对于到 3GPP 服务的普通 IP 访问是正确，而非 WLAN 访问专用的。

重复使用的基本概念是：

使用 IKEv2 生成 IPsec ESP 通道作为到家庭 MNO 网络内的访问/安全网关的 IP 连接性载体，（以与当访问 NW 是 GPRS 时 PDP 上下文相同的方式）；和

使用 IPsec 通道的基于 EAP-AKA/SIM 的相互鉴权。

为了简化，重复使用术语 PDG 表示结束通道的在家庭 MNO 网络内的访问/安全网关，但是网关功能当然并不必需与 3GPP-WLAN PDG 相同。

访问点将建立到 PDG 的两种 IPsec 通道：一个访问点专用通道（以处理所有访问点相关信令）和用于连接到访问点的 GSM/UMTS 的每个 UE 的一个或多个 UE 专用通道。因而，所图示的访问点 SIP 解决方案依赖于访问点代表 UE 建立 UE 专用 IPsec 通道，通过此通道与家庭 MNO 网络交换全部 UE 相关业务，以便当 UE 是连接到访问点的 GSM/UMTS 时，它具有到普通基于 3GPP CS 和 PS 服务的无缝访问。

在建立这些 EAP AKA/SIM 鉴权 UE 专用通道中将要处理的关键问题是，当访问点结束 EAP 信令时，它并不具有到在 UE 内驻留的（U）SIM 的直接访问。虽然访问点可以通过启动 UMTS/GSM 鉴权程序来触发 UE/(U)SIM 以运行 AKA/SIM 算法（从而耦合 UE 访问点 GSM/UMTS 鉴权程序与访问点 PDG 通道鉴权程序），当 AKA/SIM 运行时，它将不具有到在 UE/(U)SIM 内生成的关键资料的直接访问。同样地，访问点可以直接从家庭 MNO 网络获得该关键资料。描述了实现这一目的的两种替代方法，每种方法要求在访问点和家庭 MNO 网络之间略微不同的接口结构。

图 10 图示第一结构，其应用于使用在通道建立上获取 UE 专用键控资料的“带内”方法的情况。

因而，在图 10 所示的结构中，存在在 UE 30 和访问点 50 之间的 Uu 接口 240、在访问点 50 和 PDG 200 之间的 Wu’接口 242 和在 PDG 200 和 AAA 服务器 174 之间的 Wm 接口。

Uu 接口 240 是在 UE 和访问点之间的普通 GSM/UMTS 空中接口。

Wu’接口 242 是在 R6 TS 23.234 内定义的 Wu 接口的增强版本。当由访问点使用以代表自身建立 EAP-AKA 鉴权 IPsec 通道（使用本地访问点 USIM）时，不能区别其与标准 Uu 接口。然而，也可以由访问点使用其以代表 UE 建立 EAP-AKA/SIM 鉴权 IPsec 通道，在这种情况下，支持附加功能以允许访问点请求家庭 MNO 网络以发送 UE 专用 AKA/SIM 生成键控资料。

这转换成定义用于 IKEv2 CFG_REQUEST 负载类型的三个新专用属性类型，两个在 AKA 鉴权的情况下承载加密密钥（CK）和完整性保护密钥（IK），第三个在 SIM 鉴权的情况下承载独立加密密钥（Kc）。

Wm’接口是在 R6 TS 23.234 内定义的 Wm 接口的增强版本。当在访问点专用通道的鉴权和授权过程中使用时，不能区分其与标准 Wm 接口。然而，当在 UE 专用通道的鉴权和授权过程中使用时，支持附加功能以允许 AAA 服务器在 AKA 鉴权情况下将加密密钥（CK）和完整性保护密钥（IK）转发（给 PDG），或者在 SIM 鉴权的情况下，独立加密密钥（Kc）。

图 11 图示第二结构，其应用于使用在通道建立时获取 UE 专用键控资料的“带外”方法。在这种情况下，访问点 50 需要在家庭 MNO 网络内到 AAA 服务器 174 的直接接口，从而在 UE 专用通道建立时提取 UE 专用键控资料。因而，在图 11 所示的结构内，存在在 UE 30 和访问点 50 之间的 Uu 接口、在访问点 50 和 PDG 200 之间的 Wu 接口 252、在 PDG 200 和 AAA 服务器之间的 Wm 接口 254 和在访问点 50 和 AAA 服务器 174 之间的 Wax 接口 256。

Uu 接口 250 是在 UE 和访问点之间的普通 GSM/UMTS 空中接口。

Wu 接口 252 与 R6 TS 23.234 内定义的 Wu 接口基本上相同，唯一区别与所使用的标识格式相关。用作访问点标识的 NAI 包含专用前缀，从而区分它与 WLAN UE。使用访问点标识（IMSI）修饰用作 UE 标识的 NAI，从而使家庭 MNO 网络清楚该 UE 连接到该专用访问点。

Wm 接口 254 与在 R6 TS 23.234 内定义的 Wm 基本上相同，唯一区别与用于标识访问点和连接到访问点的 UE 的标识格式相关，如在先前段落内讨论的。

由访问点使用 Wax 接口 256 以（从 AAA 服务器）提取当 AKA/SIM 算法在 UE 专用通道的鉴权过程中运行时生成的 Ue 专用键控资料。根据 AAA 服务器支持，所使用的协议是 RADIUS 或 DIAMETER。Wax 接口是在用于 3GPP WLAN 互通的 R6 TS 23.234 内定义的 Wa 和 Wx 接口的组合。其类似于 Wa 接口在于它通过 AAA 协议将访问网络（访问点）连接到家庭 MNO 网络内的 AAA 服务器。然而，其目的（以提取鉴权矢量材料 CK 和 IK 或 Kc）类似于在 AAA 服务器和 HSS 之间的 Wx 接口。

访问点 SIP 解决方案的最终目的是提供用于相同服务的无缝支持，当 UE 是连接到访问点 SIP 的 GSM/UMTS 时，如同当通过宏蜂窝 GSM/UMTS 访问网络连接到家庭 MNO 网络的 GSM/UMTS 时享受的服务。

因为 UE 能够访问在普通 IP 访问网络上的家庭 MNO 网络的 3GPP 服务，访问点代表 UE 执行此任务。

为此目的，访问点需要代表 UE 在自身和家庭 MNO 网络之间建立用于承载 UE 相关业务的 IP 载体。实现这一目的的最佳方式是代表 UE 以与在 3GPP R6 TS 23.234 内在用于 WLAN-3GPP IP 访问（情况 3）的 WLAN-3GPP 互通框架内为 WLAN UE 所定义的完全相同的方式建立 VPN 类似 IPsec ESP 通道。这是因为，以这种方式，访问点使每个 UE 对于家庭 MNO 网络看起来像 WLAN UE，因此，可以为了访问点 SIP 访问解决方案重复使用用于 WLAN-3GPP 互通的家庭 MNO 网络的基础设施。

可以如下所述描述通道管理框架：

1．访问点将包含在 1-1 基础上将 GPRS APN 映射到 PDG FQDN 的数据库，即：

如果将 GPRS APN x 映射到 FQDN x，FQDN x 提供访问同一组的基于 3GPP PS 的服务，如将通过 GPRS APN x 可用于 UE 的，如果其位于在宏蜂窝 GSM/UMTS 访问网络。

2．在 UE 启动 GSM/UMTS 连接到访问点的过程中，这代表 UE 建立到 PDG 的缺省 IPsec 通道。通过访问点将在 UE 访问点和访问点 PDG 接口内的鉴权和密钥生成程序耦合在一起。建立这个到缺省（本地配置）完整资格域名 FQDN_0 的通道，FQDN_0 同时标识 PDG 和将要提供的一组服务。该组由 FQDN_0 支持的服务包括当驻留到宏蜂窝 GSM/UMTS 访问网络上时通常可用于 UE 的全部基于 3GPP CS 的服务，即 CS 语音呼叫、SMS 等。FQDN_0 还可以支持与特定 GPRS APN 关联的基于 3GPP PS 的服务。

3．随后，如果 UE 请求启动朝向 GPRS APN 的 PDP 上下文：

如果不存在用于该 GPRS APN 的已经活动的 PDP 上下文（主 PDP 上下文启动程序），则访问点检查在 GPRS APN 和 PDG FQDN 之间关联的内部数据库以查看 APN 是否与 FQDN_0 关联。如果是此情况，则重复使用现有的 IPsec 通道。访问点将与现有通道关联的远程 IP 地址和内部 DNS 服务器地址分配给 PDP 上下文（即它在活动 PDP 上下文接受内予以发送）。如果不是这种情况，则访问点建立朝向与 GPRS APN 关联的 FQDN 的新通道，和将与该新通道关联的远程 IP 地址和内部 DNS 服务器地址分配给 PDP 上下文（即它在活动 PDP 上下文接受内予以发送）。

如果存在用于该 GPRS APN 的已经活动的 PDP 上下文（第二 PDP 上下文启动程序），则重复使用现有的通道。

当 UE GSM/UMTS 连接到访问点时，访问点自动地建立朝向 FQDN_0 的缺省 UE 专用 IPsec 通道。FQDN_0 提供到用于基于 3GPP CS 的服务的 CS-SIP 互通的最小访问，还可以提供到为专用 GPRS APN 支持的基于 3GPP PS 的服务。

在建立访问点专用通道时，访问点重复使用从 PDG 的 FQDN 分析中获得的 IP 地址。以这种方式，使用同一 PDG 结束从访问点开始的全部通道，即访问点专用通道和全部 UE 专用通道。

当访问点代表 UE 请求建立通道时，通过使用访问点的 IMSI 修饰 UE 的基于 IMSI 的 NAI，组成所使用的宣称标识。以这种方式，代表其请求该通道的 UE 的标识和发出请求的访问点的标识对于家庭网络是清楚的。以类似于在 WLAN 3GPP IP 访问内使用的方式【参见 3GPP R6 TS 23.003，“用于 3GPP 系统到 WLAN 互通的编号、寻址和标识”】，也可以使用标记修饰所宣称的标识，所述标记表示是否应当使用 EAP AKA 或 EAP SIM 鉴权，例如用于 EAP-AKA 的 0<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org 或者用于 EAP-SIM 的 1<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

对于基于 IKE 的通道建立程序，访问点将调控 IKEv2 的本地 NAT 横向支持以处理访问点位于 NAT 设备之后的（类似）事实。一旦建立 IPsec ESP 通道，则访问点使用 IETF RFC 3948“IPsec ESP 分组的 UDP 封装”以处理访问点位于 NAT 设备之后的事实。

用于代表 UE 建立到家庭 MNO 网络的 IPsec 通道的访问点 SIP 解决方案依赖于用于在访问网络层上提供端到端安全的两个互锁安全程序。

首先，在 UE 执行 UMTS 连接到访问点的情况下，访问点代表家庭 MNO 网络（HSS/HLR）根据 R99 TS 33.102“3G 安全：安全结构”执行与 UE/USIM 的相互 UMTS

访问鉴权；访问点代表 UE/USIM（使用 EAP-AKA 根据 IKEv2）执行与家庭 MNO 网络（与 AAA 服务器/HSS 和 PDG）的相互通道鉴权。

其次，在 UE 执行 GSM 连接到访问点的情况下，访问点代表家庭 MNO 网络（HSS/HLR）根据 ETSI GSM 03.20:“数字蜂窝电信系统（阶段 2+）；安全相关网络功能”执行 UE/SIM 的 GSM 访问鉴权，和访问点代表 UE/SIM（使用 EAP-SIM 根据 IKEv2）执行与家庭 MNO 网络（与 AAA 服务器/HSS 和 PDG）的相互通道鉴权。

在两种情况下，可以耦合这两个程序，因为它们都依赖于运行鉴权和生成用于访问层加密和完整性保护的键控资料的 SIM/AKA 算法。然而，访问点并不必需直接访问 SIM/AKA 算法运行的任一实体，即 UE 或 HSS/HLR 的（U）SIM。

虽然通过将 EAP 请求/响应交换映射给 MM：鉴权请求/响应交换，访问点能够代表 UE/(U)SIM 执行与在家庭 MNO 网络内 AAA 服务器的相互鉴权，它依然需要获得当 AKA/SIM 算法运行时生成的键控资料，从而代表 UE 根据 IKEv2/EAP 执行向 PDG 的鉴权，从而保护 GSM/UMTS 空中接口。

考虑到执行到 PDG 的鉴权，通常是这种情况，当将 EAP-AKA（封装在 IKEv2 内）用于在（IPsec 通道建立）上在两个 IKEv2 对等体之间的鉴权，此相互鉴权基于对等体检查一获得作为 EAP AKA 交换结果的相同共享秘密。此共享秘密是根据当在 EAP AKA 交换过程中在两个终端上运行 AKA 算法时生成的公共 CK 和 IK 密钥获得的主对话密钥 MSK。

在当前情况下，PDG 从 AAA 服务器接收主对话密钥。然而，因为访问点自身不能运行 AKA 算法，自身不能根据 UE/USIM 获得 CK 和 IK，必需存在一种外部方式，访问点通过其获取代表 UE 向 PDG 鉴权自身必需的 CK 和 IK。

在 EAP SIM 鉴权的情况下，这同样适用，使用 Kc 替代 CK 和 IK。

考虑保护 GSM/UMTS 空中接口，当 UE 执行到访问点的 UMTS 登记时，访问点必需获得与在 UE/USIM 上生成的一组密钥相同的用于（在 UE 和 RNC 之间）UMTS 加密和完整性保护算法的一组密钥（CK，IK）。在加密密钥 Kc 相关的 GSM 登记的情况下，出现类似的问题。

因而，每次在 UE/USIM 和 HSS/HLR 之间运行 AKA 算法时，访问点需要访问 CK 和 IK，每次在 UE/SIM 和 HSS/HLR 之间运行“SIM”算法时，访问 Kc。

如在此描述的，访问点从家庭 MNO 网络获得这些密钥。访问点可以代表 UE 在 IPsec 通道建立的过程中从家庭 MNO 网络获得密钥，或者“带外”，通过根据位于访问点自身

内的 USIM 在访问点和家庭 MNO 网络之间的先前存在连接，或者“带内”，通过代表 UE 在用于建立通道的 EAP 信令上借道。

在任一解决方案中，必需安全地传输这些密钥。通过依赖于存在在访问点和家庭 MNO 网络之间的预共享秘密的事实，即当访问点根据其自身的 USIM 先前建立与家庭 MNO 网络的 IPsec 通道时在两个终端上生成的 MSK_ZAP。

图 12 图示“带内”解决方案，其中在自身建立 UE 相关 IPsec 通道的信令的过程中，从家庭 MNO 网络内的 AAA 服务器向访问点（通过网关）发送密钥。这要求对来自为 TS 23.234 内 Wu 和 Wm 接口定义的 IKEv2/EAP 交换的负载的某些修改，从而承载密钥。

可以在 PDG 和访问点之间安全地发送密钥，因为在它们之间存在预先共享的秘密，MSK_ZAP，其在访问点/USIM 和家庭 MNO 网络之间建立预先存在 IPsec 通道时生成。

当访问点代表 UE 请求建立 IPsec 通道时，它将其标识宣称为：

在 UMTS 连接的情况下，0<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org；或者

在 GSM 连接的情况下，1<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

在 GSM 连接的情况下，通过在初始 IKE_AUTH Req 消息的 CFG_REQUEST 负载内包括附加（专用）属性 Kc_AT，访问点请求 PDG 发送 UE 专用加密密钥 Kc。

在 UMTS 连接的情况下，通过在初始 IKE_AUTH Req 消息的 CFG_REQUEST 负载内包括两个附加（专用）属性 CK_AT 和 IK_AT，访问点请求 PDG 发送 UE 专用加密和完整性密钥（CK，IK）。

随后，PDG 将鉴权请求发送给 AAA 服务器，引用在 IDi 负载内接收的标识（和标识用于 CS-SIP 互通的访问点的 FQDN_0）。

根据 IDi 负载包含用另一个 IMSI（访问点）修饰的 IMSI（UE）的事实，AAA 服务器变得获知这是请求 UE 专用通道而非访问点专用通道。同样地，它获知除了“普通”UE 专用 MSK 之外它还必需将 UE 专用键控密钥发送给 PDG。假设在 PDG 和 AAA 服务器之间使用的 AAA 协议是 DIAMETER（如由 3GPP WLAN 互通要求的），则在 AKA 鉴权的情况下，AAA 服务器可以使用：“机密性密钥 AKA”AVP 和“完整性密钥 AKA”AVP。

在 SIM 鉴权的情况下，AAA 服务器可以使用“机密性密钥 AKA”AVP。

根据 IDi 负载关联 UE 的 IMSI 和访问点的 IMSI 的事实，PDG 获知提取 MSK_ZAP

密钥以加密从 AAA 服务器接收的 UE 专用键控资料，PDG 自建立访问点专用通道时与访问点共享此密钥。

PDG 在承载 EAP 成功负载的 IKE_AUTH 响应的 CFG_REPLY 负载内包括此资料。

因为访问点还已知 MSK_ZAP，它可以解密一个或多个负载，并访问 UE 专用键控资料。

图 13 图示所需要的 IPsec 通道建立信令以允许在 EAP-AKA 鉴权的情况下将 UE/USIM 相关密钥（CK，IK）传送给访问点。这基于标准的 IPsec 通道建立信令（TS 23.234）。类似机制适用于 EAP-SIM 鉴权。

具体地，图 13 图示在由访问点（代表 UE）建立 UE 相关 IPsec 通道时可以如何将 CK 和 IK 从家庭 MNO 网络传送给访问点。在步骤 1301，如上所述，每次开启访问点时，它建立在家庭 MNO 网络内到 PDG 的 IPsec 通道。此程序完全根据在 R6 TS 23.234 6.1.5 节“用于建立 UE 启动通道（WLAN 3GPP IP 访问）的机制”定义的程序。作为此程序的结果，访问点、PDG 和 AAA 服务器全部共享秘密密钥，MSK_ZAP。

在步骤 1302 和 1303，访问点和 PDG 建立新的 IKE_SA 和同意用于保护 IKE 信令的 IPsec 协议/算法，所述 IKE 信令用于建立 UE 相关 IPsec 通道。

IKEv2 协议提供用于 IKE 对等体之一向另一对等体请求配置信息的普通机制。这在于在列表所请求属性的 IKE 请求内包括 CFG_REQUEST 负载。IKEv2 定义若干缺省属性，包括 INTERNAL_IP4_ADDRESS，其已经用于获取建立 IPsec 通道必需的 PDG 内的远程 IP 地址。然而，IKEv2 允许扩展新专用属性类型。在这种情况下，我们定义将由访问点在步骤 1304 内请求 PDG 提供与 UE 关联的必需 CK 和 IK 中使用的两个附加属性 CK_AT 和 IK_AT。此外，为了允许家庭 MNO 网络理解该通道建立程序与此专用访问点关联，访问点使用其自身的 IMSI 修饰 UE 的 NAI，即，

0<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

因而，如果在访问点内 USIM 的 IMSI 是 234150999999999 和 UE 的 USIM 的 IMSI 是 234150888888888，则访问点代表 UE 宣称下述标识：

IDi=0234150888888888@234150999999999.zap.mnc234.mcc15.3gppnetwork.org。

根据 3GPP-WLAN 协议（R6 TS 23.003），0 前缀通知将要使用 EAP_AKA。前缀 1 将通知 EAP-SIM。

因为 IDi 包含访问点的 IMSI，所以 PDG 能够提取在访问点和 GW 之间的预先共享秘密，即 MSK_ZAP，因而使用它以当随后在信令内从 AAA 服务器接收到 CK 和 IK 时加

密 UE 相关 CK 和 IK。

在步骤 1306，AAA 服务器检查它是否具有与 UE 的 IMSI 关联的存储 AKA 鉴权矢量（RAND，AUTN，XRES，CK，IK）。如果不是，则它向 HSS 查询一个新的。

当 AAA 服务器读取此特定形式的 IDi 时，它获知对于这种情况，它必需将与 UE 的 IMSI 关联的 CK 和 IK 发送给 PDG，以便它最终发送给访问点。除了由 AAA 通常根据 CK 和 IK 生成的 MSK_UE 之外。

在步骤 1308，访问点将 EAP 请求/AKA 质询（RAND，MAC，AUTN）映射到 MM：鉴权请求（RAND，MAC，AUTN）和将其发送给 UE 以触发运行 AKA 算法。

在步骤 1309，访问点从 UE 接收 MM：鉴权请求（RES，MAC），将其映射成 EAP 响应/AKA 质询（RES，MAC），其将鉴权 UE 与 AAA 服务器。

在标准信令（TS 23.234 6.1.5 节）内，AAA 服务器将仅发送与 UE 的 IMSI 关联的主对话密钥。然而，在这种情况下，在步骤 1311，AAA 服务器将两个额外 AVP，即机密性密钥 AKA 和完整性密钥 AKA 添加给鉴权应答，从而使得 CK 和 IK 在 PDG 内可用。

如果在步骤 1312 至 1314 内授权该通道，则在步骤 1315 内，PDG 通过 CFG_REPLY 负载将 CK 和 IK 发送给访问点，除了远程 IP 地址之外，该负载现在将承载 CK 和 IK 属性。

为了保证仅访问点能够访问 CK 和 IK，PDG 使用预先共享秘密 MSK_ZAP 加密这些密钥。这可以通过多种方式实现，但是需要与家庭 MNO 网络供应商协商具体方式。

在步骤 1316，访问点使用共享秘密 MSK_ZAP 解密 CK 和 IK 负载。随后，访问点可以生成 MSK_UE（如在[EAP-AKA]第 6.4 节“密钥生成”内定义的），使用其生成正确的 AUTH 负载（如在[IKEv2]第 2.16 节“可扩展鉴权协议方法”内定义的）。

另一方面，访问点将 CK 和 IK 用于在空中接口上的加密和完整性保护。

在步骤 1317，PDG 检查 AUTH 如此鉴权通道和生成其自身的 AUTH 负载。访问点使用 MSK_UE 检查 AUTH 的有效性，从而鉴权 PDG。

如图 11 所示，并参考其描述，不同结构应用于“带外”解决方案的情况。在此解决方案中，在 UE 专用通道建立过程中，通过向家庭 MNO 网络内的 AAA 服务器直接查询必需的 UE 专用键控资料，即在 UMTS 连接的情况下 CK 和 IK 和在 GSM 连接的情况下 Kc，访问点获取 UE 专用键控资料。此查询通过 RADIUS 或 DIAMETER 经上述 Wax 接口执行，并介绍以支持访问点 SIP 解决方案。

在这种解决方案中，UE 专用通道建立按照与如图 13 所示的相同的程序，直到访问点

接收到承载 EAP 成功消息的 IKE_AUTH 响应的点，此响应向访问点通知 AAA 服务器已经成功地为 UE 执行 EAP 鉴权。在这一点上，访问点需要从 AAA 服务器提取 UE 专用键控资料，从而向 PDG 鉴权自身，并使用在空中接口上的加密和完整性保护启动。此资料是在刚刚发生的在访问点（通过使用 GSM/UMTS 鉴权程序查询 UE）和 AAA 服务器之间的成功的基于 EAP 的相互鉴权过程中使用的鉴权矢量的一部分。

在使用 DIAMETER 时，则可以重新使用在 TS 29.234 内定义的用于 3GPP WLAN 互通框架的 Wx 接口，用于 AAA 服务器从 HSS 中提取鉴权矢量的应用。

访问点 50 将鉴权请求发送给 AAA 服务器，具有格式：

信息单元名称	映射到 DIAMETER AVP	数值
永久用户标识	用户名称	IMSI_UE
访问网络标识符	访问网络标识符	IMSI_ZAP
编号鉴权项目	SIP 编号鉴权项目	1
鉴权数据	SIP 鉴权数据项目	参见下表

在该请求内的加权数据内容具有格式：

信息单元名称	映射到 DIAMETER AVP	描述
鉴权方法	鉴权方法	EAP/SIM 或 EAP/AKA

AAA 服务器将鉴权应答发送给访问点 50，具有格式：

信息单元名称	映射到 DIAMETER AVP	数值
永久用户标识	用户名称	IMSI_UE
访问网络标识符	访问网络标识符	IMSI_ZAP
结果	结果编码/实验结果	成功
鉴权数据	SIP 鉴权数据项目	参加下表

在应答中的鉴权数据内容，在 EAP-AKA 情况下，具有格式：

信息单元名称	映射到 DIAMETER AVP	描述
鉴权方法	鉴权方法	EAP/AKA
机密性密钥 AKA	机密性密钥	CK
完整性密钥 AKA	完整性密钥	IK

在应答中的鉴权数据内容，在 EAP-SIM 情况下，具有格式：

信息单元名称	映射到 DIAMETER AVP	描述
鉴权方法	鉴权方法	EAP/AKA
鉴权信息 SIM	鉴权信息 SIM	鉴权质询 RAND 和加密密钥 Kc 的级联

因此，已经描述了方法，由此安装有 SIM 卡的基站可以向网络鉴权自身。

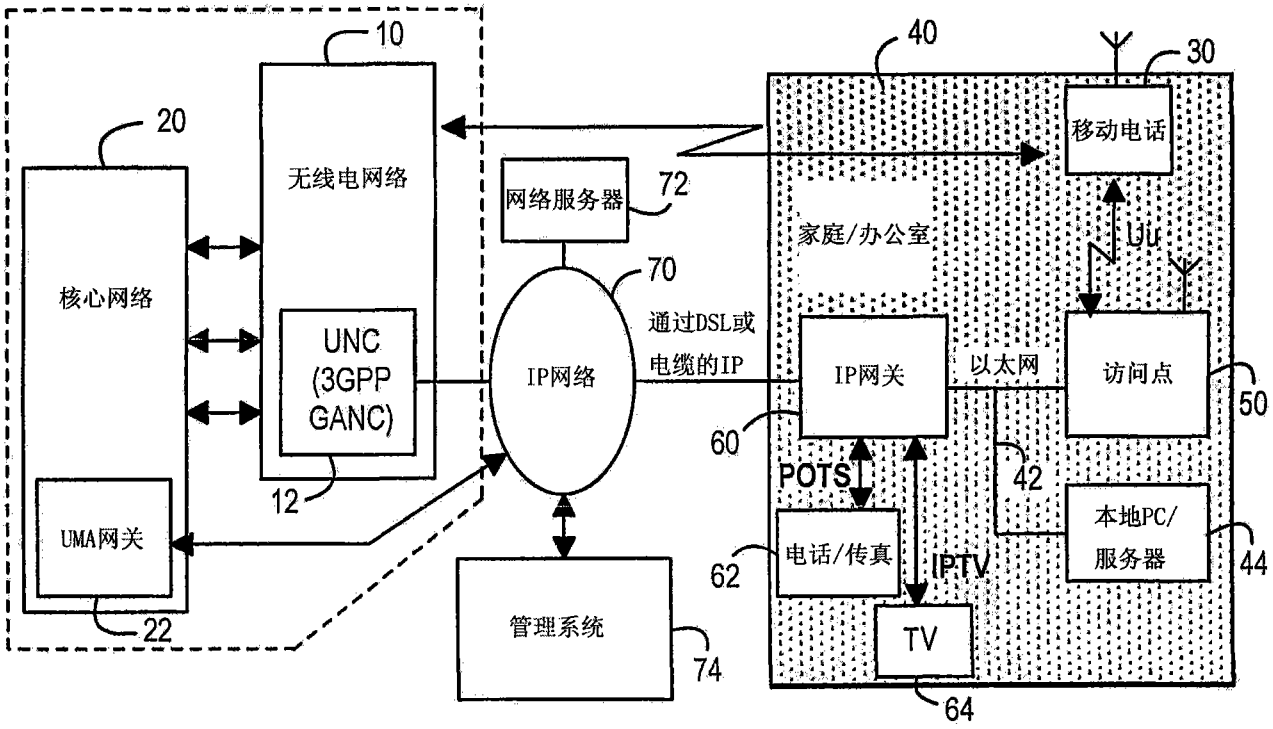

10
20
无线电网络
核心网络
UNC
(3GPP
GANC)
UMA网关
12
22
网络服务器
72
70
IP网络
通过DSL或
电缆的IP
管理系统
74
40
30
移动电话
家庭/办公室
Uu
IP网关
以太网
访问点
50
60
POTS
42
本地PC/
服务器
44
62
电话/传真
IPTV
TV
64

图 1

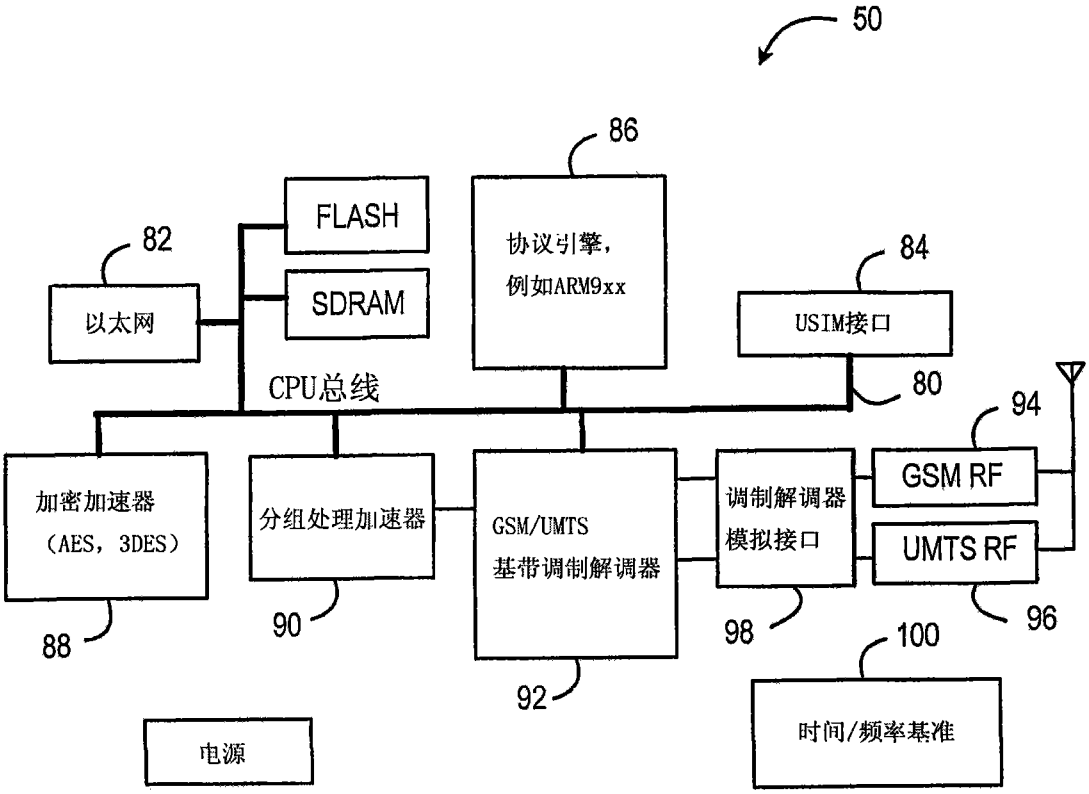

50
86
FLASH
协议引擎，
例如ARM9xx
82
84
SDRAM
以太网
USIM接口
CPU总线
80
94
加密加速器
（AES，3DES）
分组处理加速器
GSM/UMTS
基带调制解调器
调制解调器
模拟接口
GSM RF
UMTS RF
88
90
98
96
100
92
电源
时间/频率基准

图 2

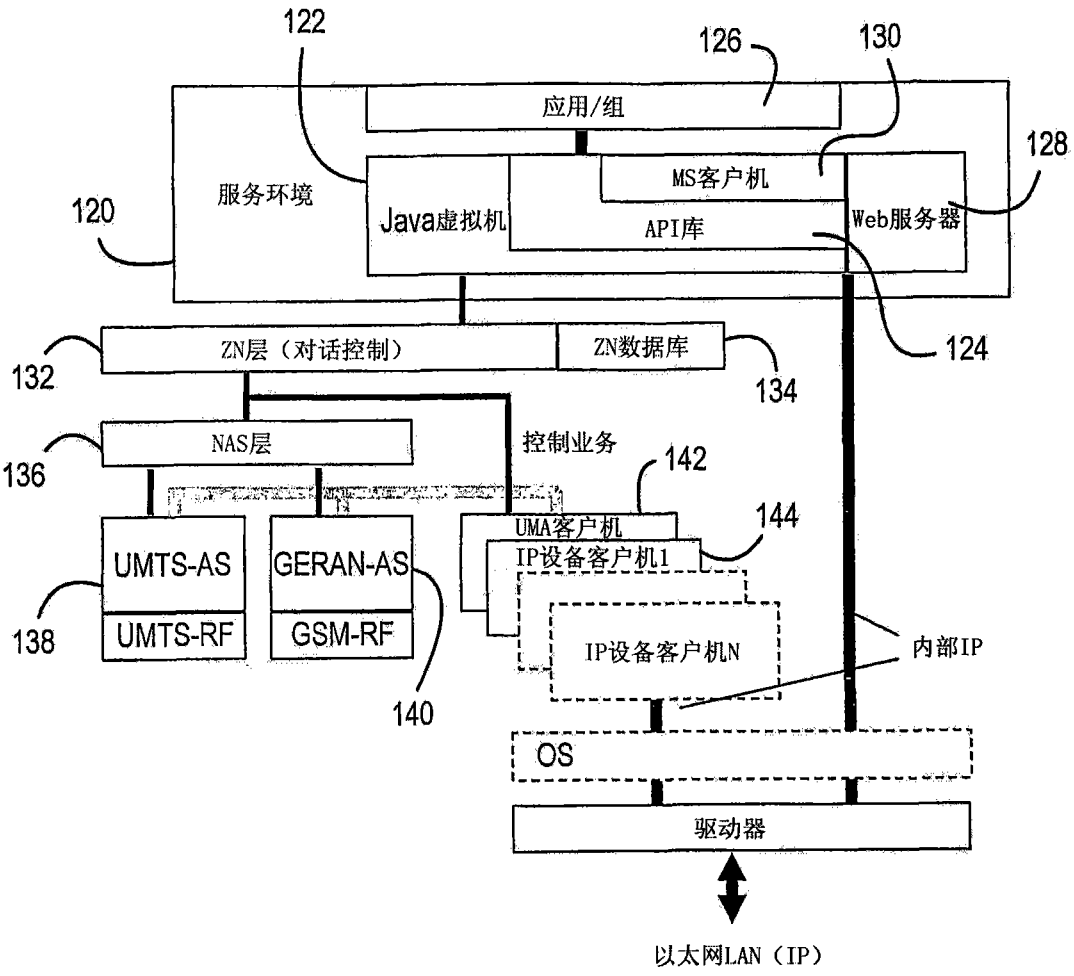

122
126
130
128
应用/组
服务环境
MS客户机
Java虚拟机
API库
Web服务器
120
124
ZN层（对话控制）
ZN数据库
132
134
NAS层
控制业务
136
142
144
UMA客户机
IP设备客户机1
UMTS-AS
GERAN-AS
IP设备客户机N
内部IP
138
UMTS-RF
GSM-RF
140
OS
驱动器
以太网LAN（IP）

图 3

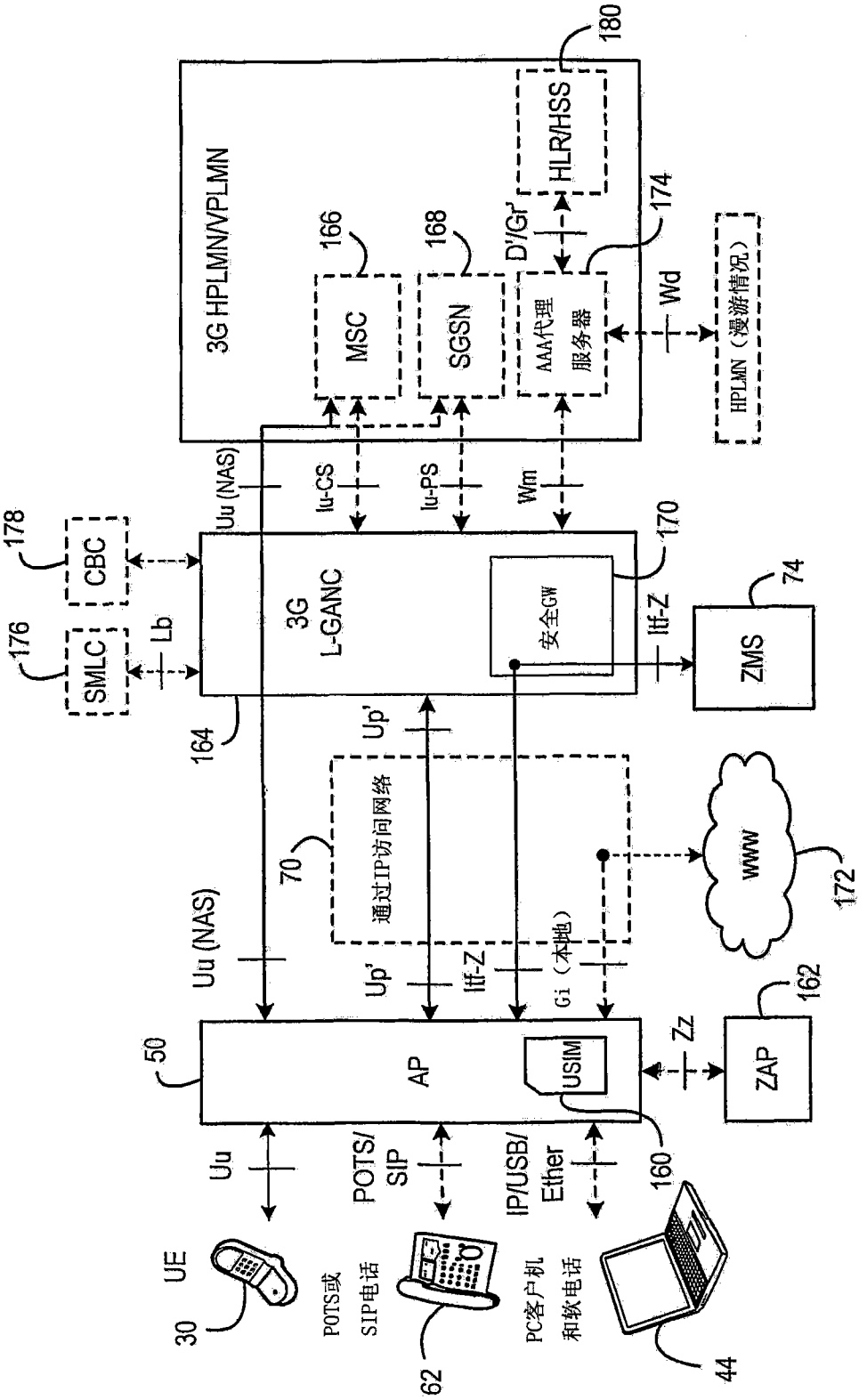

3G HPLMN/VPLMN
180
HLR/HSS
D'/Gr'
174
166
MSC
168
SGSN
AAA代理
服务器
Wd
HPLMN（漫游情况）
Uu (NAS)
Iu-CS
Iu-PS
Wm
178
CBC
176
SMLC
Lb
3G
L-GANC
安全GW
170
Iff-Z
74
ZMS
164
Up'
70
通过IP访问网络
Uu (NAS)
Up'
Iff-Z
Gi（本地）
WWW
172
50
AP
USIM
Zz
162
ZAP
Uu
POTS/
SIP
IP/USB/
Ether
160
UE
30
POTS或
SIP电话
62
PC客户机
和软电话
44

图 4

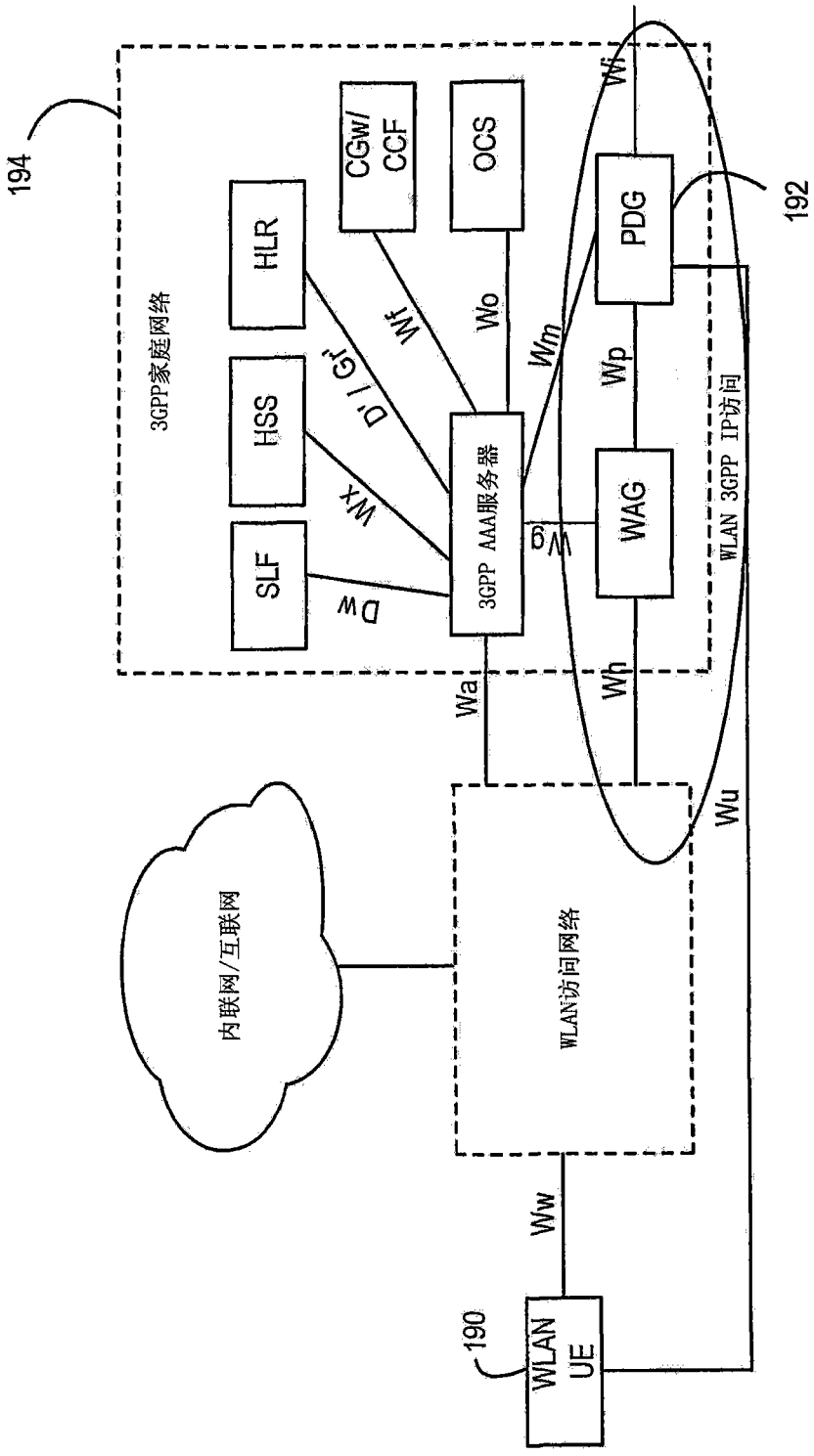

194
3GPP家庭网络
HLR
HSS
SLF
CGw/
CCF
OCS
3GPP AAA服务器
PDG
WAG
192
WLAN 3GPP IP访问
Wf
Wm
Wp
Wo
Wi
Wx
Dw
D/Gr
Wg
Wa
Wh
Wu
内联网/互联网
WLAN访问网络
Ww
190
WLAN
UE

图 5

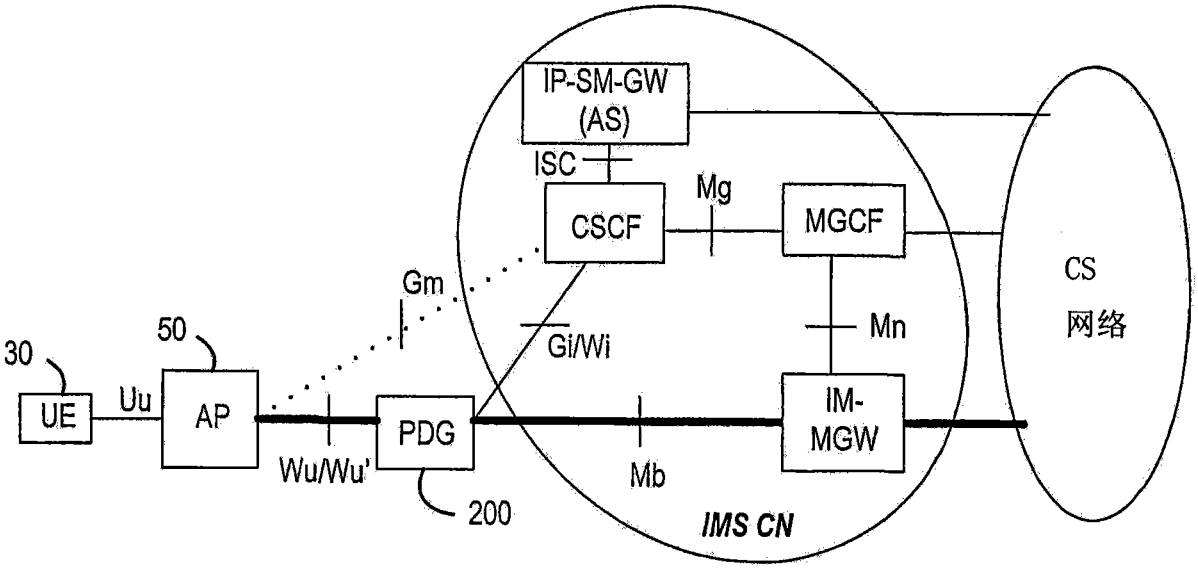

IP-SM-GW
(AS)
ISC
CSCF
Mg
MGCF
CS
网络
Gm
Gi/Wi
Mn
30
50
UE
Uu
AP
PDG
IM-
MGW
Wu/Wu'
Mb
200
IMS CN

图 6

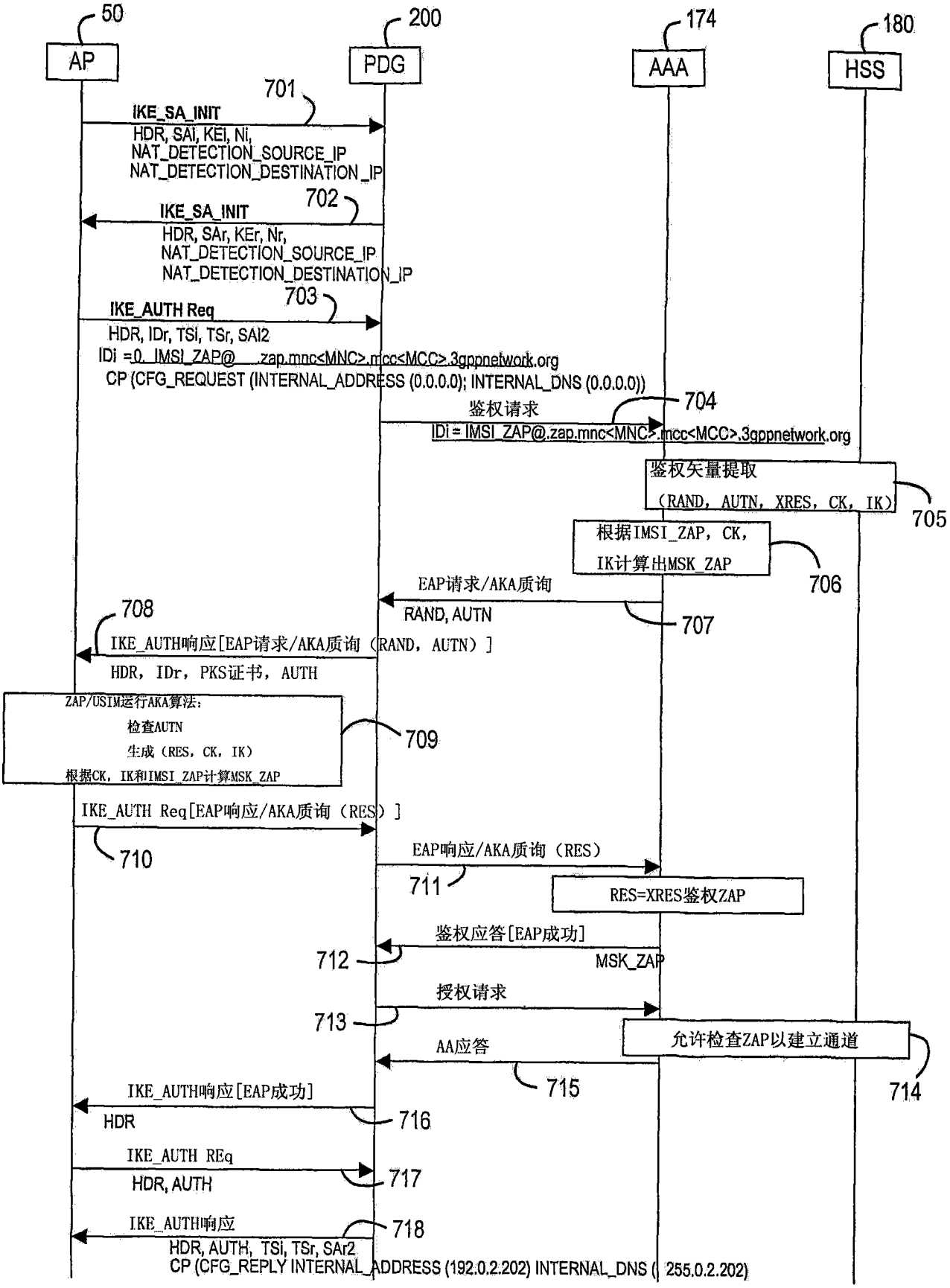

50
AP
200
PDG
174
AAA
180
HSS
701
IKE_SA_INIT
HDR, SAi, KEi, Ni,
NAT_DETECTION_SOURCE_IP
NAT_DETECTION_DESTINATION_IP
702
IKE_SA_INIT
HDR, SAr, KEr, Nr,
NAT_DETECTION_SOURCE_IP
NAT_DETECTION_DESTINATION_IP
703
IKE_AUTH Req
HDR, IDr, TSi, TSr, SAI2
IDi =0_IMSI_ZAP@ .zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org
CP (CFG_REQUEST (INTERNAL_ADDRESS (0.0.0.0); INTERNAL_DNS (0.0.0.0))
鉴权请求
704
IDi = IMSI_ZAP@.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org
鉴权矢量提取
(RAND, AUTN, XRES, CK, IK)
705
根据IMSI_ZAP, CK,
IK计算出MSK_ZAP
706
EAP请求/AKA质询
RAND, AUTN
707
708
IKE_AUTH响应[EAP请求/AKA质询 (RAND, AUTN)]
HDR, IDr, PKS证书, AUTH
ZAP/USIM运行AKA算法:
检查AUTN
生成 (RES, CK, IK)
根据CK, IK和IMSI_ZAP计算MSK_ZAP
709
IKE_AUTH Req[EAP响应/AKA质询 (RES)]
710
EAP响应/AKA质询 (RES)
711
RES=XRES鉴权ZAP
鉴权应答[EAP成功]
712
MSK_ZAP
授权请求
713
允许检查ZAP以建立通道
714
AA应答
715
IKE_AUTH响应[EAP成功]
HDR
716
IKE_AUTH REq
HDR, AUTH
717
IKE_AUTH响应
718
HDR, AUTH, TSi, TSr, SAr2
CP (CFG_REPLY INTERNAL_ADDRESS (192.0.2.202) INTERNAL_DNS (255.0.2.202)

图 7

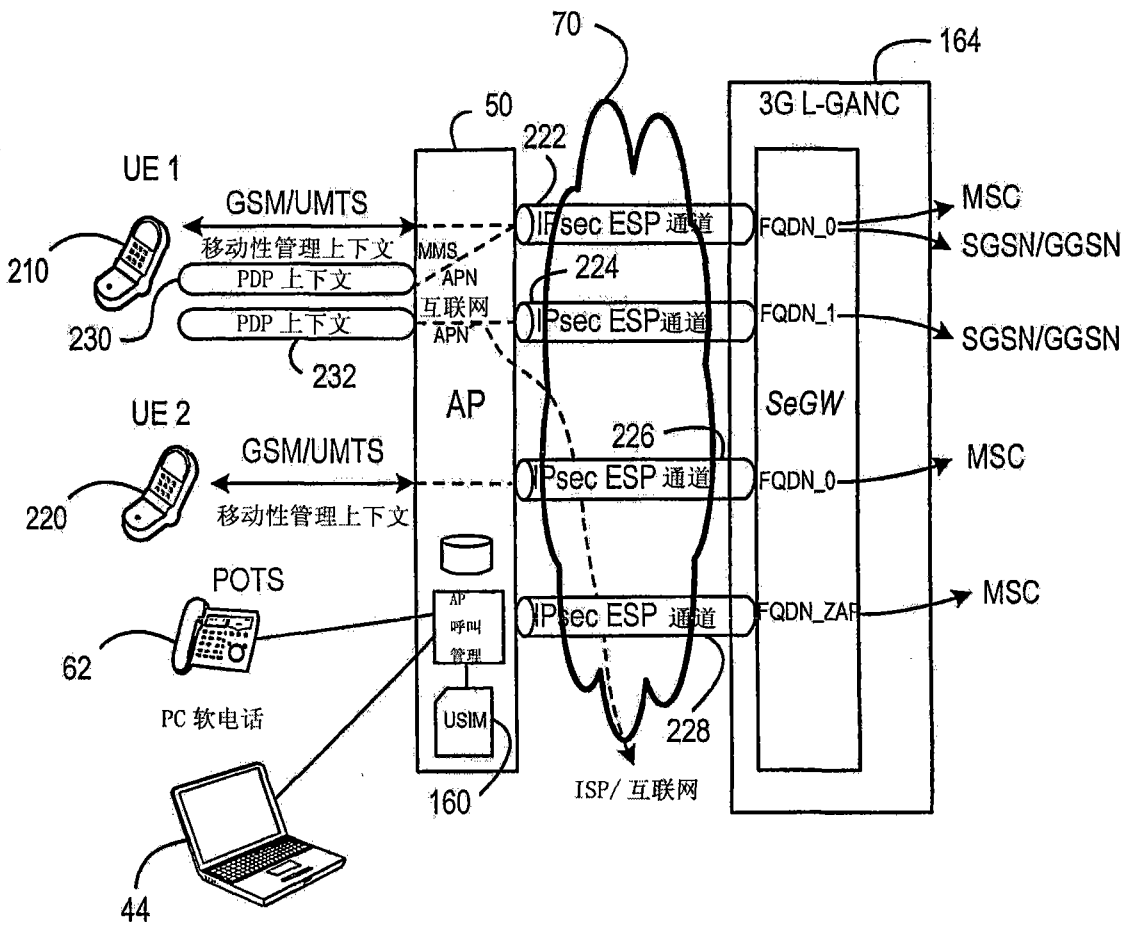

70
164
3G L-GANC
50
222
UE 1
GSM/UMTS
移动性管理上下文
MMS
APN
PDP 上下文
互联网
APN
PDP 上下文
IPsec ESP 通道
FQDN_0
MSC
SGSN/GGSN
224
IPsec ESP通道
FQDN_1
SGSN/GGSN
210
230
232
AP
SeGW
UE 2
GSM/UMTS
移动性管理上下文
226
IPsec ESP 通道
FQDN_0
MSC
220
POTS
AP
呼叫
管理
IPsec ESP 通道
FQDN_ZAP
MSC
62
PC 软电话
USIM
228
160
ISP/ 互联网
44

图 8

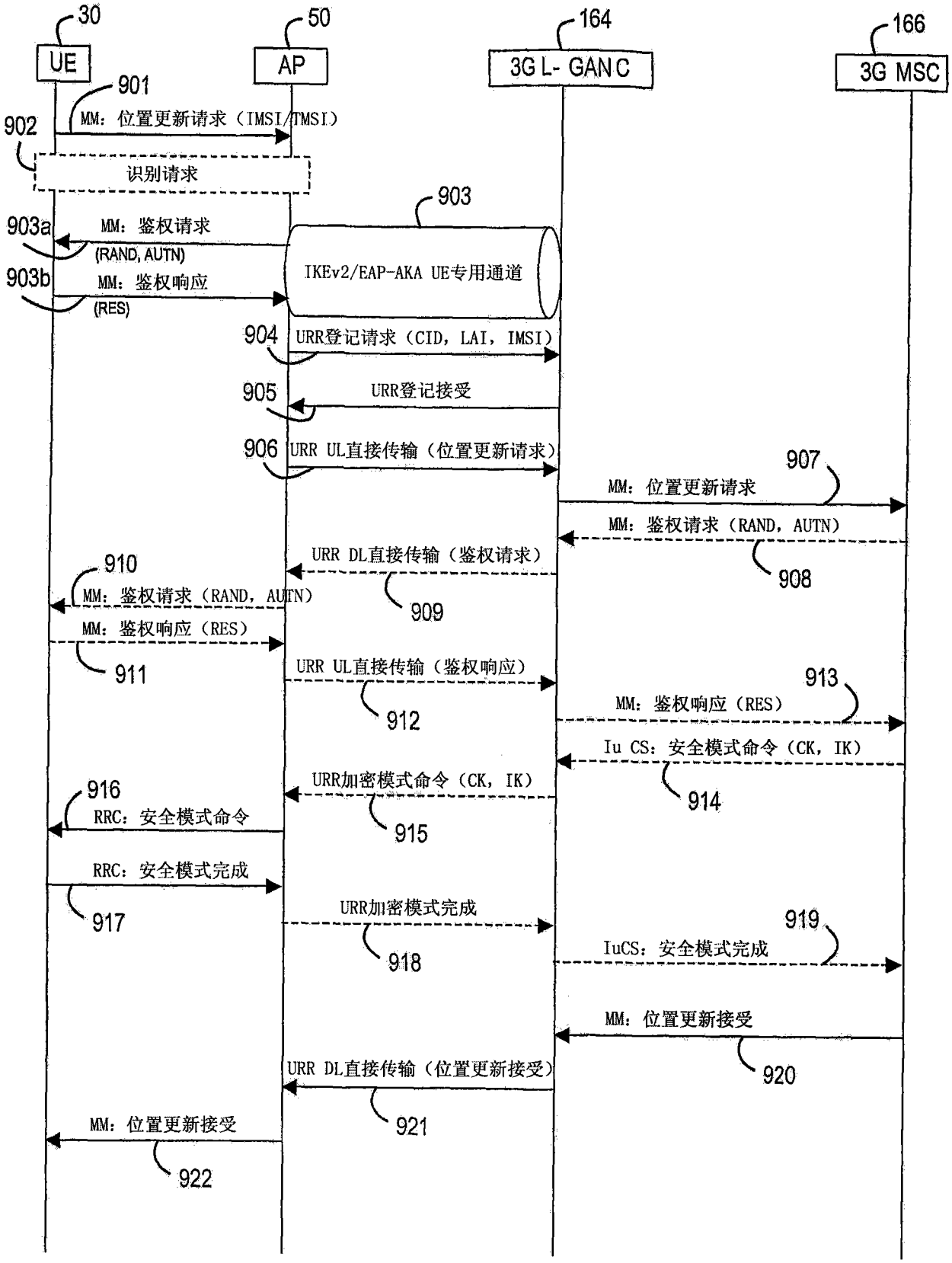

30
UE
50
AP
164
3G L- GANC
166
3G MSC
901
MM：位置更新请求（IMSI/TMSI）
902
识别请求
903
903a
MM：鉴权请求
(RAND, AUTN)
IKEv2/EAP-AKA UE专用通道
903b
MM：鉴权响应
(RES)
904
URR登记请求（CID，LAI，IMSI）
905
URR登记接受
906
URR UL直接传输（位置更新请求）
907
MM：位置更新请求
MM：鉴权请求（RAND，AUTN）
908
URR DL直接传输（鉴权请求）
909
910
MM：鉴权请求（RAND，AUTN）
MM：鉴权响应（RES）
911
URR UL直接传输（鉴权响应）
912
913
MM：鉴权响应（RES）
Iu CS：安全模式命令（CK，IK）
914
URR加密模式命令（CK，IK）
915
916
RRC：安全模式命令
RRC：安全模式完成
917
URR加密模式完成
918
919
IuCS：安全模式完成
MM：位置更新接受
920
URR DL直接传输（位置更新接受）
921
MM：位置更新接受
922

图 9

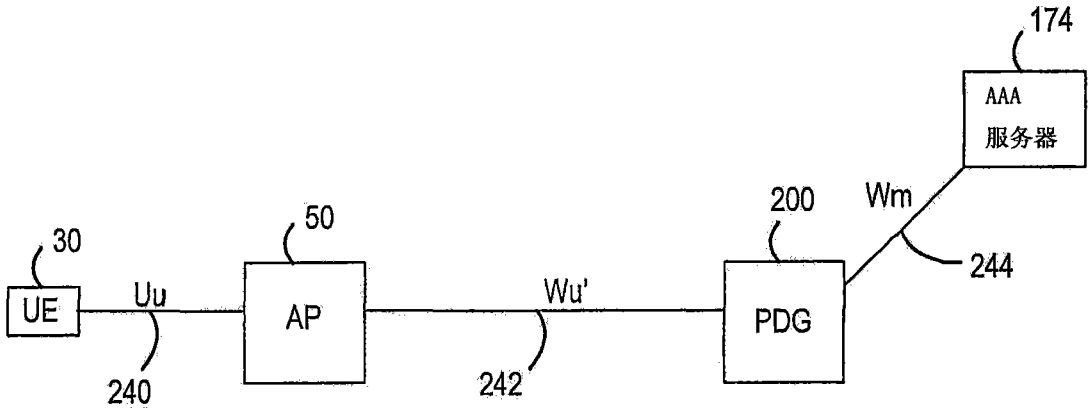

174
AAA
服务器
200
Wm
244
30
50
UE
Uu
AP
Wu'
PDG
240
242

图 10

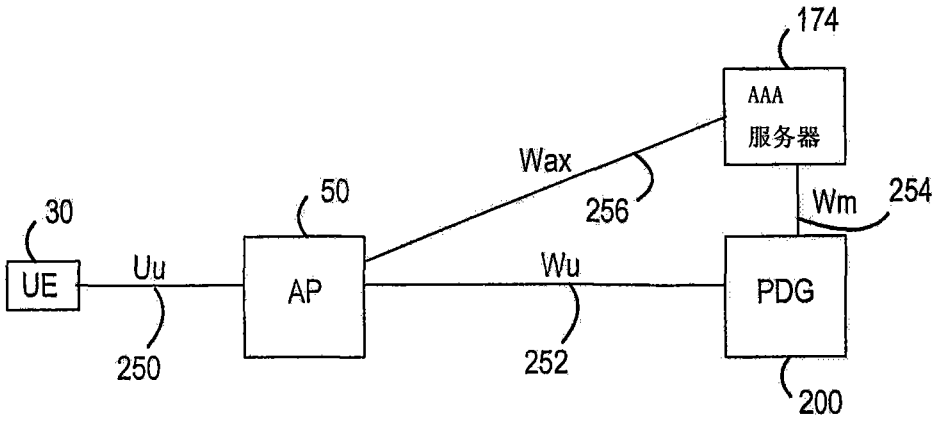

174
AAA
服务器
Wax
256
Wm
254
30
50
UE
Uu
AP
Wu
PDG
250
252
200

图 11

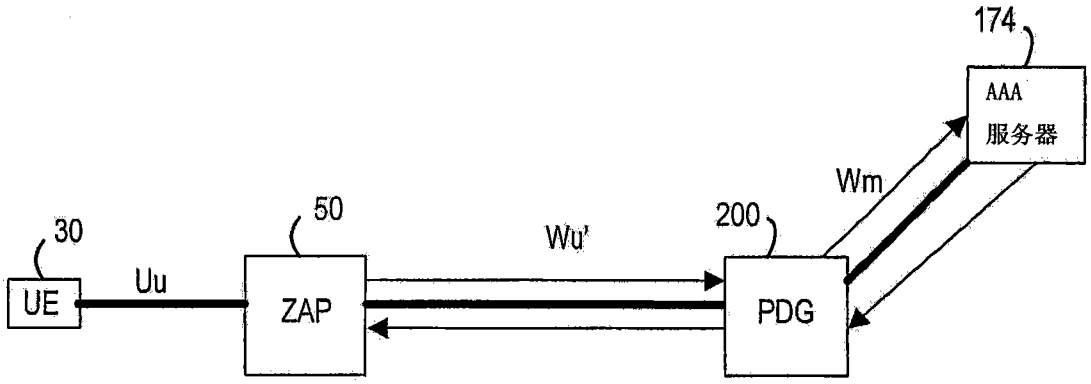


图 12

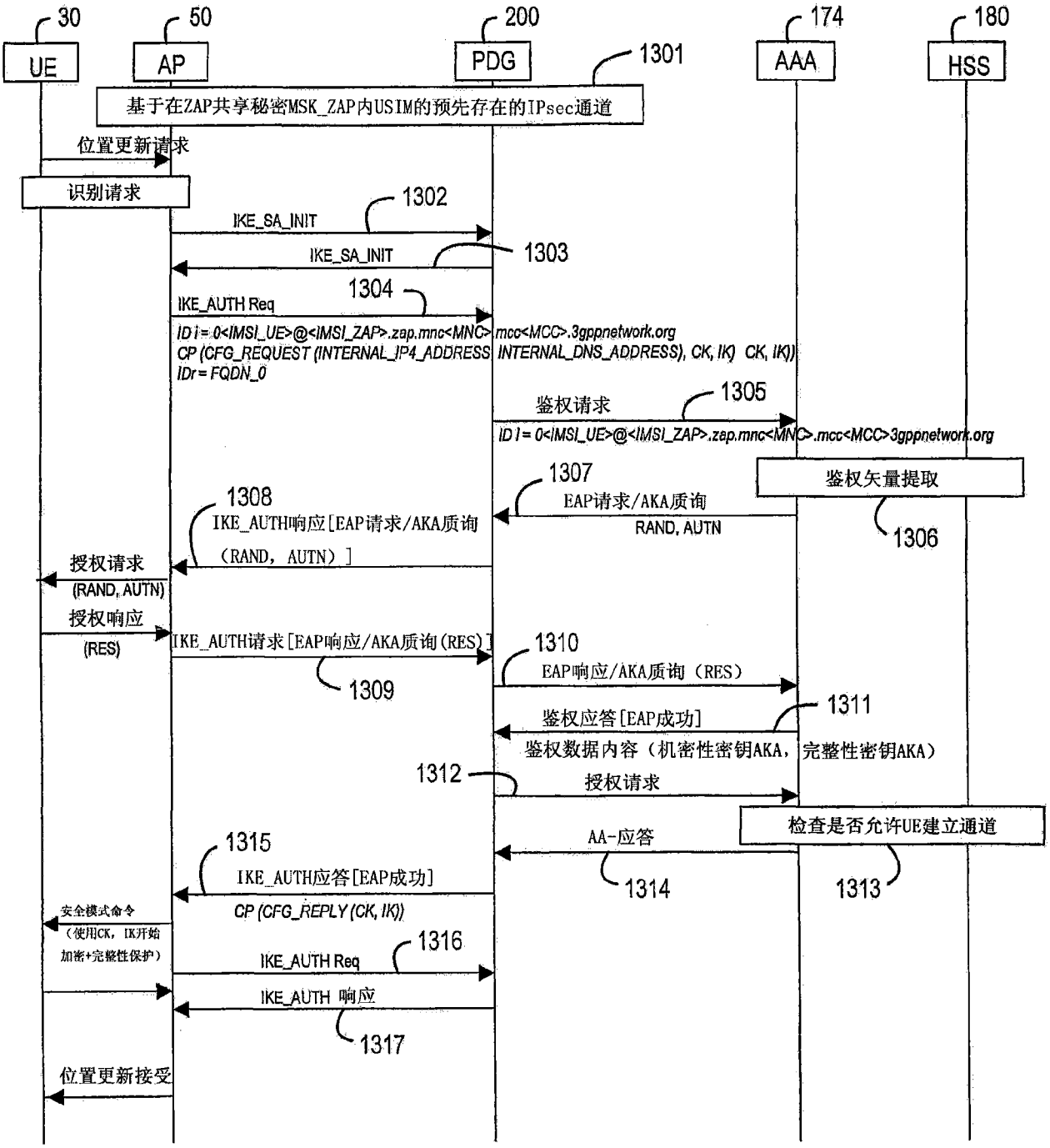

30
50
200
174
180
UE
AP
PDG
AAA
HSS
1301
基于在ZAP共享秘密MSK_ZAP内USIM的预先存在的IPsec通道
位置更新请求
识别请求
1302
IKE_SA_INIT
IKE_SA_INIT
1303
1304
IKE_AUTH Req
IDi = 0<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>.3gppnetwork.org
CP (CFG_REQUEST (INTERNAL_IP4_ADDRESS, INTERNAL_DNS_ADDRESS), CK, IK) CK, IK))
IDr = FQDN_0
鉴权请求
1305
IDi = 0<IMSI_UE>@<IMSI_ZAP>.zap.mnc<MNC>.mcc<MCC>3gppnetwork.org
鉴权矢量提取
1307
EAP请求/AKA质询
RAND, AUTN
1306
1308
IKE_AUTH响应[EAP请求/AKA质询
（RAND，AUTN）]
授权请求
(RAND, AUTN)
授权响应
(RES)
IKE_AUTH请求[EAP响应/AKA质询(RES)]
1309
1310
EAP响应/AKA质询（RES）
1311
鉴权应答[EAP成功]
鉴权数据内容（机密性密钥AKA，完整性密钥AKA）
1312
授权请求
检查是否允许UE建立通道
1315
AA-应答
1314
1313
IKE_AUTH应答[EAP成功]
CP (CFG_REPLY (CK, IK))
安全模式命令
（使用CK，IK开始
加密+完整性保护）
1316
IKE_AUTH Req
IKE_AUTH 响应
1317
位置更新接受

图 13