[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公开说明书

[21] 申请号 200510077476.6

[43] 公开日 2006 年 7 月 12 日

[11] 公开号 CN 1802016A

[22] 申请日 2005.6.21
[21] 申请号 200510077476.6
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 黄迎新 朱奋勤

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 王 琦 程殿军

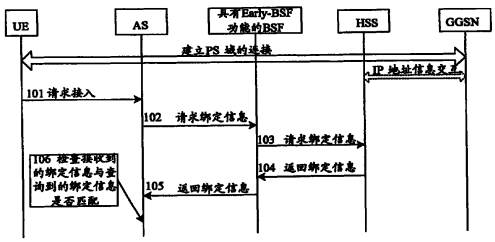
权利要求书 3 页 说明书 10 页 附图 1 页

[54] 发明名称

对用户终端进行鉴权的方法

[57] 摘要

本发明公开了一种对用户终端进行鉴权的方法，关键是，应用业务实体接收到来自 2G 用户终端的包含用户身份标识的接入请求后，根据接入请求中的用户身份标识，从 HSS 获取由该 2G 用户终端的 IP 地址及其身份标识构成的绑定信息；之后，应用业务实体判断自身保存的该 2G 用户终端的 IP 地址及其身份标识的绑定信息与发起接入请求的 2G 用户终端的 IP 地址及其身份标识的绑定信息是否相匹配，如果匹配，则该 2G 用户终端通过鉴权，否则该 2G 用户终端不能通过鉴权。 应用本发明，实现了对直接接入应用业务实体的 2G 用户终端进行鉴权，既保证了合法的用户能够接入，又保证了网络的安全。 特别对于早期应用的基于 IMS 的业务，能够正常部署和运行。



1、一种对用户终端进行鉴权的方法，适用于直接接入应用业务实体的 2G 用户终端，其特征在于，接入 3GPP 的 2G 用户终端已获得 IP 地址，且在用户归属网络服务器 HSS 中已保存由该 2G 用户终端的 IP 地址及其身份标识构成的绑定信息，该方法还包括以下步骤:

a、2G 用户终端向应用业务实体发起接入请求，该请求中包含自身的标识；应用业务实体根据接收到的接入请求，从 HSS 获取由该 2G 用户终端的 IP 地址及其身份标识构成的绑定信息；

b、应用业务实体判断自身保存的该 2G 用户终端的 IP 地址及其身份标识的绑定信息，与发起接入请求的 2G 用户终端的 IP 地址及其身份标识的绑定信息是否相匹配，如果匹配，则该 2G 用户终端通过鉴权，否则该 2G 用户终端不能通过鉴权。

2、根据权利要求 1 所述的方法，其特征在于，所述 2G 用户终端发起的接入请求中还包括鉴权方式标识，

所述鉴权方式标识为早期的通用鉴权框架鉴权方式时，所述应用业务实体通过执行用户身份初始检查验证的实体 BSF 从 HSS 获取该 2G 用户终端的 IP 地址及其身份标识的绑定信息。

3、根据权利要求 2 所述的方法，其特征在于，所述应用业务实体通过 BSF 从 HSS 获取该 2G 用户终端的 IP 地址及其身份标识的绑定信息的过程包括以下步骤:

应用业务实体向 BSF 发送请求鉴权信息的消息，该请求消息中包含用户终端的身份标识，BSF 接收到该请求后，根据请求中的用户终端的身份标识向 HSS 请求该 2G 用户终端的 IP 地址及其身份标识的绑定信息，并将得到的绑定信息直接返回给应用业务实体，应用业务实体保存接收到的绑定信息；

所述 BSF 向 HSS 请求绑定信息的消息中包含鉴权方案字段，该鉴权方案字段指示为 early IMS。

4、根据权利要求 3 所述的方法，其特征在于，所述 BSF 为早期的仅具备查询功能的 Early-BSF，或支持完全 3G 功能且具备 Early-BSF 功能的 BSF。

5、根据权利要求 3 所述的方法，其特征在于，所述应用业务实体与已保存绑定信息的 HSS 属于相同或不同的归属网络。

6、根据权利要求 1 所述的方法，其特征在于，所述 2G 用户终端发起的接入请求中还包括鉴权方式标识，

所述鉴权方式标识为直接鉴权方式时，所述应用业务实体直接向 HSS 发送绑定信息请求消息，接收并保存 HSS 返回的该 2G 用户终端的 IP 地址及其身份标识的绑定信息。

7、根据权利要求 6 所述的方法，其特征在于，所述应用业务实体向 HSS 发送的请求消息由用户数据请求 UDR 消息承载，且该消息中的属性信息指明请求绑定信息；HSS 给应用业务实体返回的响应消息由用户数据应答 UDA 消息承载，且该消息中的属性信息指明请求绑定信息。

8、根据权利要求 6 所述的方法，其特征在于，所述应用业务实体与已保存绑定信息的 HSS 属于相同的归属网络。

9、根据权利要求 2 或 6 所述的方法，其特征在于，

所述 2G 用户终端向应用业务实体发起的接入请求由基于 HTTP 协议的请求消息 HTTP GET 承载；

所述请求消息中的鉴权方式标识由 HTTP GET 中的用户代理 user agent 字段承载。

10、根据权利要求 1 所述的方法，其特征在于，所述接入请求中的身份标识为用户公共身份标识 IMPU；

所述应用业务实体从 HSS 获取的该 2G 用户终端的 IP 地址及其身份标识的绑定信息为：接入请求中所包含的 IMPU 和该 2G 用户终端的 IP 地址的对应关系；或发起接入请求的 2G 用户终端所拥有的所有 IMPU 和该 2G 用户终端的 IP 地址的对应关系。

11、根据权利要求 1 所述的方法，其特征在于，该方法进一步包括：2G 用

户终端与应用业务实体之间建立传输层安全 TLS 隧道，然后再执行步骤 a。

12、根据权利要求 1 所述的方法，其特征在于，所述应用业务实体为应用服务器 AS 或应用服务器代理 AP。

5

对用户终端进行鉴权的方法

技术领域

本发明涉及移动通信技术领域，特别是指对直接接入应用业务实体的2G用户终端进行鉴权的方法。

背景技术

随着宽带网络的发展，移动通信不仅仅局限于传统的话音通信，通过与呈现业务（presence）、短消息、网页（WEB）浏览、定位信息、推送业务（PUSH）以及文件共享等数据业务的结合，移动通信能够实现音频、视频、图片和文本等多种媒体类型的业务，以满足用户的多种需求。

第三代移动通信标准化伙伴项目（3GPP）以及第三代移动通信标准化伙伴项目2（3GPP2）等组织都先后推出了基于IP的多媒体子系统（IMS）架构，其目的是在移动网络中使用一种标准化的开放结构来实现多种多样的多媒体应用，以给用户提供更多的选择和更丰富的感受。

IMS 架构叠加在分组域网络（PS-Domain）之上，其与鉴权相关的实体包括呼叫状态控制功能（CSCF）实体和归属签约用户服务器（HSS）功能实体。CSCF 又可以分成服务 CSCF（S-CSCF）、代理 CSCF（P-CSCF）和查询 CSCF（I-CSCF）三个逻辑实体，该三个逻辑实体可能是不同的物理设备，也可能是同一个物理设备中不同的功能模块。其中，S-CSCF 是 IMS 的业务控制中心，用于执行会话控制，维持会话状态，管理用户信息，产生计费信息等；P-CSCF 是终端用户接入 IMS 的接入点，用于完成用户注册，服务质量（QoS）控制和安全管理等；I-CSCF 负责 IMS 域之间的互通，管理 S-CSCF 的分配，对外隐藏网络拓扑结构和配置信息，并产生计费数据等。HSS 是非常重要的用户数据库，用于支持各个网络实体对呼叫和会话的处理。

IMS 在初始推出（R5 版本协议）时只考虑在第三代移动通信网络使用。由于 IMS 上的业务非常丰富，所以出现了运营商在 2G 的网络上使用 IMS 的需求。但在 2G 的网络上是无法支持基于 3G 网络的 IMS 的安全相关功能的，例如五元组鉴权/网络认证等，为解决 2G 用户使用 IMS 网络面临的用户鉴权问题，3GPP 提出了一种过渡鉴权方案，该方案为 2G 上的 IMS 业务提供一定的安全功能。当用户支持 3G 鉴权方案时，再采用完整的基于 3G 的鉴权方案对接入用户进行鉴权。这样，无论是 2G 用户还是 3G 用户，都可以在鉴权通过后应用 IMS 中的业务。通常，将过渡鉴权方案称为 Early IMS 的鉴权方式，将完整的基于 3G 的鉴权方案称为 Full 3GPP IMS 鉴权方式。

对于任何一个 2G 或 3G 的 UE，其既可以使用基于 IMS 的应用服务器（AS）所提供的业务，如使用 presence 业务，也可以对基于 IMS 的 AS 或 AS 的代理（AP）进行一些简单的管理操作，如管理 AS 或 AP 上的一些组列表（group list）信息等。

当一个 UE 需要使用基于 IMS 的 AS 所提供的业务时，其需要首先接入 3GPP 分组域，然后经过 IMS 的鉴权后才能使用 AS 所提供的业务，此时，对于 2G 的 UE，IMS 将使用 Early IMS 的鉴权方式进行鉴权，对于 3G 的 UE，IMS 将使用 Full 3GPP IMS 的鉴权方式进行鉴权。

当一个 UE 需要对基于 IMS 的 AS 或通过 AP 对 AS 进行管理操作时，其仍然要首先接入 3GPP 分组域，然后该 UE 可通过 Ut 接口直接接入 AS 或 AP，因而 IMS 不再对该 UE 进行鉴权。同时在现有的协议中规定，该直接接入 AS 或 AP 的 UE 采用通用鉴权框架（GAA）的方式鉴权后，才能接入 AS 或 AP。

但是，现有的基于通用鉴权框架（GAA）的鉴权方式是针对 3G 用户终端的，其不支持对 2G 用户终端的鉴权，这样，必然会存在这样的情况：2G 用户终端不能接入或 2G 用户终端不需鉴权就可直接接入。

如果不让 2G 用户终端接入，不但使运营商损失很多业务，还会导致用户对运营商的满意度下降。

如果 2G 用户终端不需鉴权就可直接接入，显然无法保证 AS 和整个网络的安全。

发明内容

有鉴于此，本发明的目的在于提供一种对用户终端进行鉴权的方法，以对直接接入应用业务实体的 2G 用户终端实现鉴权。

为达到上述目的，本发明的技术方案是这样实现：

一种对用户终端进行鉴权的方法，适用于直接接入应用业务实体的 2G 用户终端，接入 3GPP 的 2G 用户终端已获得 IP 地址，且在用户归属网络服务器 HSS 中已保存由该 2G 用户终端的 IP 地址及其身份标识构成的绑定信息，该方法还包括以下步骤：

a、2G 用户终端向应用业务实体发起接入请求，该请求中包含自身的标识；应用业务实体根据接收到的接入请求，从 HSS 获取由该 2G 用户终端的 IP 地址及其身份标识构成的绑定信息；

b、应用业务实体判断自身保存的该 2G 用户终端的 IP 地址及其身份标识的绑定信息与发起接入请求的 2G 用户终端的 IP 地址及其身份标识的绑定信息是否相匹配，如果匹配，则该 2G 用户终端通过鉴权，否则该 2G 用户终端不能通过鉴权。

较佳地，所述 2G 用户终端发起的接入请求中还包括鉴权方式标识，

所述鉴权方式标识为早期的通用鉴权框架鉴权方式时，所述应用业务实体通过执行用户身份初始检查验证的实体 BSF 从 HSS 获取该 2G 用户终端的 IP 地址及其身份标识的绑定信息。

较佳地，所述应用业务实体通过 BSF 从 HSS 获取该 2G 用户终端的 IP 地址及其身份标识的绑定信息的过程包括以下步骤：

应用业务实体向 BSF 发送请求鉴权信息的消息，该请求消息中包含用户终端的身份标识，BSF 接收到该请求后，根据请求中的用户终端的身份标识向 HSS 请求该 2G 用户终端的 IP 地址及其身份标识的绑定信息，并将得

到的绑定信息直接返回给应用业务实体，应用业务实体保存接收到的绑定信息；

所述 BSF 向 HSS 请求绑定信息的消息中包含鉴权方案字段，该鉴权方案字段指示为 early IMS。

较佳地，所述 BSF 为早期的仅具备查询功能的 Early-BSF，或支持完全 3G 功能且具备 Early-BSF 功能的 BSF。

较佳地，当所述应用业务实体通过 BSF 向 HSS 请求绑定信息时，所述应用业务实体与已保存绑定信息的 HSS 属于相同或不同的归属网络。

较佳地，所述 2G 用户终端发起的接入请求中还包括鉴权方式标识，

所述鉴权方式标识为直接鉴权方式时，所述应用业务实体直接向 HSS 发送绑定信息请求消息，接收并保存 HSS 返回的该 2G 用户终端的 IP 地址及其身份标识的绑定信息。

较佳地，所述应用业务实体向 HSS 发送的请求消息由用户数据请求 UDR 消息承载，且该消息中的属性信息指明请求绑定信息；HSS 给应用业务实体返回的响应消息由用户数据应答 UDA 消息承载，且该消息中的属性信息指明请求绑定信息。

较佳地，当所述应用业务实体直接向 HSS 请求绑定信息时，所述应用业务实体与已保存绑定信息的 HSS 属于相同的归属网络。

较佳地，所述 2G 用户终端向应用业务实体发起的接入请求由基于 HTTP 协议的请求消息 HTTP GET 承载；

所述请求消息中的鉴权方式标识由 HTTP GET 中的用户代理 user agent 字段承载。

较佳地，所述接入请求中的身份标识为用户公共身份标识 IMPU；

所述应用业务实体从 HSS 获取的该 2G 用户终端的 IP 地址及其身份标识的绑定信息为：接入请求中所包含的 IMPU 和该 2G 用户终端的 IP 地址的对应关系；或发起接入请求的 2G 用户终端所拥有的所有 IMPU 和该 2G 用户终端的 IP 地址的对应关系。

较佳地，该方法进一步包括：2G 用户终端与应用业务实体之间建立传输层安全 TLS 隧道，然后再执行步骤 a。

较佳地，所述应用业务实体为应用服务器 AS 或应用服务器代理 AP。

本发明的关键是：应用业务实体接收到来自 2G 用户终端的包含用户身份标识的接入请求后，根据接入请求中的用户身份标识，从 HSS 获取该 2G 用户终端的 IP 地址及其身份标识的绑定信息；之后，应用业务实体判断自身保存的该 2G 用户终端的 IP 地址及其身份标识的绑定信息与发起接入请求的 2G 用户终端的 IP 地址及其身份标识的绑定信息是否相匹配，如果匹配，则该 2G 用户终端通过鉴权，否则该 2G 用户终端不能通过鉴权。应用本发明，实现了对直接接入应用业务实体的 2G 用户终端进行鉴权，既保证了合法的用户能够接入，又保证了网络的安全。特别对于早期应用的基于 IMS 的业务，能够正常部署和运行。

附图说明

图 1 所示为应用本发明的实施例一的流程示意图；

图 2 所示为应用本发明的实施例二的流程示意图。

具体实施方式

下面结合附图及具体实施例对本发明再做进一步地详细说明。

图 1 所示为应用本发明的实施例一的流程示意图。在本实施例中，2G 的 UE 已接入到 3GPP 分组域，并获得分组网络的分组网络网关节点（GGSN）为其分配的 IP 地址，同时 GGSN 将该 UE 的用户的电话号码（MSISDN）、分组域的国际移动用户身份标识（IMSI）及 IP 地址等相关信息发送给 HSS，HSS 通过用户的 MSISDN 或 IMSI 查找到用户在 IMS 系统中的身份标识 IMPI，并将该 UE 的 IMPI、该 IMPI 所对应的用户的公共身份标识（IMPU）、MSISDN 以及该 UE 的 IP 地址等信息进行绑定保存。本实施例以 2G 的 UE 接入 AS 为例进行说明。

步骤 101，2G 的 UE 向 AS 发起接入请求，该请求中包含该 UE 自身的身份标识，如 IMPU；该请求消息中还包含自身所支持的鉴权方式标识，在现有基于 Http 协议的 Ut 接口，可以利用 Http GET 消息中的用户代理（user agent）字段来承载该鉴权方式标识，在本实施例中，该 2G 的 UE 所支持的鉴权方式为早期应用 GAA 的 Ut 接口认证方式，在此，将该鉴权方式的标识记为早期的通用鉴权框架鉴权方式（Early-GAA-Ut），那么该鉴权方式标识 Early-GAA-Ut 将被添在 Http 消息中的 user agent 字段中。

步骤 102，AS 根据接收到的接入请求，判断出请求消息中的鉴权方式标识为 Early-GAA-Ut 后，AS 向执行用户身份初始检查验证的实体（BSF）发送请求鉴权信息的消息，该消息中包含该 AS 的用户身份标识，本步骤中的 BSF 可以为早期的仅具备查询功能的 Early-BSF，也可以是支持完全 3G 功能且具有 Earl y-BSF 功能的 BSF。

由于在 3G GAA 的执行过程中，AS 向 BSF 请求鉴权信息时，需要携带 BSF 分配的用户会话标识（B-TID），而在 Early-GAA-Ut 鉴权方式中是不存在 BSF 分配的 B-TID 的，因此对于支持完全 3G 功能且具备 Early-BSF 功能的 BSF，其接收到来自 AS 的请求鉴权信息的消息后，可以通过判断该消息中携带的是 B-TID 还是用户身份标识来区分是正常 3G GAA 的鉴权方式还是 Early-GAA-Ut 的鉴权鉴权方式。

步骤 103，BSF 收到 AS 的请求鉴权信息的消息，并确定该请求中携带的是用户身份标识后，向 HSS 请求该 UE 的 IP 地址及其身份标识的绑定信息。该请求信息中同样包含 UE 的身份标识，并且，该向 HSS 请求绑定信息的消息中包含鉴权方案字段，且该鉴权方案字段中指示为 early IMS。

步骤 104，HSS 根据接收到的请求信息中的用户身份标识，查询 BSF 所需的绑定信息，并将该绑定信息返回给 BSF。

通常 UE 所发接入请求中的用户身份标识为 IMPU，因此，HSS 查询绑定信息的过程为：HSS 通过收到的 IMPU 查找与该 IMPU 所对应的 IMPI，以及与该 IMPI 所对应的 IP 地址，所述返回的绑定信息是指 IMPU 与该 UE 的 IP 地址的

对应关系。

如果发起接入请求的 UE 所携带的用户身份标识是 IMPI 或 IMSI，则 HSS 返回的绑定信息是 IMPI 与 IP 地址的绑定信息或 IMSI 与 IP 地址的绑定信息，或根据其所应用的网络系统的需要返回需要的 IMPI 和/或 IMPU 与该用户终端 IP 地址的绑定的信息。也就是说，HSS 所返回的绑定信息是发起请求的 UE 的身份标识与该 UE 当前所拥有 IP 地址的对应信息。

步骤 105，BSF 收到该绑定信息后，不进行保存而是将该绑定信息直接转发给 AS，这样做的好处是当 AS 再次向 BSF 请求绑定信息时，BSF 需要到 HSS 去查询，从而保证了 BSF 返回给 AS 的信息总是最新的。

步骤 106，AS 收到绑定信息后保存，之后判断自身保存的该 UE 的 IP 地址及其身份标识的绑定信息与该发起接入请求的 UE 的 IP 地址及其身份标识的绑定信息是否相匹配，即是否完全相同，如果匹配，则该 2G 的 UE 通过鉴权，否则该 2G 的 UE 不能通过鉴权。

对于上述实施例，当 UE 的 IP 地址改变或注销后，GGSN 将通知 HSS 更新该绑定信息或删除该绑定信息。而当 HSS 所保存的绑定信息变化后，HSS 不需要通知 BSF，因为通常在 IP 地址变化或注销后，基于连接的应用层协议就会断开并在以后重新建立连接，AS 在连接断开后将删除保存的绑定信息，当 UE 重新建立连接时，AS 会重新向 BSF 请求绑定信息。

对于上述实施例，接收到接入请求的 AS 与已保存绑定信息的 HSS 可以属于同一归属网络，也可以属于不同的归属网络。

图 2 所示为应用本发明的实施例二的流程示意图。在本实施例中，UE 已接入到 3GPP 分组域，并获得 GGSN 为其分配的 IP 地址，同时 GGSN 将该 UE 的 MSISDN、IMSI 及 IP 地址等相关信息发送给 HSS，HSS 通过用户的 MSISDN 或 IMSI 查找到用户在 IMS 系统中的身份标识 IMPI，并将该 UE 的 IMPI、该 IMPI 所对应的用户的公共身份标识（IMPU）、MSISDN 以及该 UE 的 IP 地址等信息进行绑定保存。本实施例以 2G 的 UE 接入 AS 为例进行说明。

步骤 201，2G 的 UE 向 AS 发起接入请求，该请求中包含该 UE 自身的身份

标识，如 IMPU；该请求的消息中还包含自身所支持的鉴权方式标识，在现有基于 Http 协议的 Ut 接口，可以利用 Http GET 消息中的 user agent 字段来承载该鉴权方式标识，在本实施例中，该 2G 的 UE 所支持的鉴权方式为应用 AS 与 HSS 之间 Sh 接口的直接鉴权方式，在此，将该鉴权方式的标识记为直接鉴权方式（Ut-Sh-Authentication），那么该鉴权方式标识 Ut-Sh-Authentication 将被添在 Http 消息中的 user agent 字段中。

步骤 202，AS 根据接收到的接入请求，判断出请求消息中的鉴权方式标识为 Ut-Sh-Authentication 后，直接通过 Sh 接口向 HSS 发送请求该 UE 的 IP 地址及其身份标识绑定信息的消息。该请求消息中同样包含用户身份标识信息。通常，AS 通过 Sh 接口向 HSS 发送的请求消息由用户数据请求（UDR，User-Data-Request）消息来承载，且通过该请求消息中的属性信息 Avp（Attribute-Value Pair）来描述请求用户的何种数据。在本实施例中，通过增加要求绑定地址信息的 Avp 属性，来实现通过 Sh 接口请求地址绑定信息。

步骤 203，HSS 根据接收到的请求信息中的用户身份标识，查询 AS 所需的绑定信息，并将该绑定信息直接返回给 AS。通常，HSS 在 Sh 接口中使用用户数据应答（UDA，User-Data-Answer）消息作为 UDR 消息的响应消息。在本实施例中，由于是对请求绑定消息的响应，因此该 UDA 消息中也使用步骤 202 中增加的 Avp 属性信息。

通常 UE 所发接入请求中的用户身份标识为 IMPU，因此，HSS 查询绑定信息的过程为：HSS 通过收到的 IMPU 查找与该 IMPU 所对应的 IMPI，以及与该 IMPI 所对应的 IP 地址，所述返回的绑定信息是指 IMPU 与该 UE 的 IP 地址的对应关系。

如果发起接入请求的 UE 所携带的用户身份标识是 IMPI 或 IMSI，则 HSS 返回的绑定信息是 IMPI 与 IP 地址的绑定信息或 IMSI 与 IP 地址的绑定信息，或根据其所应用的网络系统的需要返回需要的 IMPI 和/或 IMPU 与该用户终端 IP 地址的绑定的信息。也就是说，HSS 所返回的绑定信息是发起请求的 UE 的身份标识与该 UE 当前所拥有 IP 地址的对应信息。

步骤204，AS收到绑定信息后保存，之后，判断自身保存的该UE的IP地址及其身份标识的绑定信息与该发起接入请求的UE的IP地址及其身份标识的绑定信息是否相匹配，即是否完全相同，如果匹配，则该2G的UE通过鉴权，否则该2G的UE不能通过鉴权。

对于上述实施例，当UE的IP地址改变或注销后，GGSN将通知HSS更新该绑定信息或删除该绑定信息。而当HSS所保存的绑定信息变化后，HSS不需要通知AS，因为通常在IP地址变化或注销后，基于连接的应用层协议就会断开并在以后重新建立连接，AS在连接断开后将删除保存的绑定信息，当UE重新建立连接时，AS会重新向HSS请求绑定信息。

对于上述实施例，接收到接入请求的AS与已保存绑定信息的HSS必须属于同一归属网络。

以上所述实施例均是以UE接入AS为例进行说明的，当然，上述所有实施例中的AS均可以直接替换为AP，由该AP代理AS完成对接入的UE进行鉴权的操作，且一个AP的后面可以有一个或一个以上的AS。在此，将所有类似AS或AP的实体称为应用业务实体。

再有，众所周知，用户的公共身份标识IMPU与私有标识IMPI对应关系是多对一的关系，因此针对上述两个实施例而言，在HSS返回绑定信息时，也可以返回这个IMPI所关联的所有IMPU与该UE的IP地址的绑定信息。这样做的好处是，UE连接到AS后，其后面消息有可能变化为使用其它的IMPU，因此AS需要保存该UE所有IMPU与该IP地址的对应关系。当上述实施例中的AS被替换为AP时，这样的处理尤为有用，因为AP后面可以有多个AS，且由AP替这些AS完成鉴权功能，则UE向不同的AS发出请求的时候使用的IMPU很可能是不同的，这时，如果AP已经保存了该UE所有IMPU与该UE的IP地址的对应关系，则可以迅速准确的完成其代理的鉴权的操作，而不必向HSS进行多次查询。

在上面两个实施例执行之前，UE和AS可以先建立基于传输层保护的传输层安全（TLS Transport Layer Security）隧道，由于TLS就是一种传输层保护协

议，因此在建立这个隧道后，再执行上面两个实施例中描述的基于应用层的认证过程，可以使 UE 和 AS 之间的应用层通信得到充分的安全保护。

以上所述实施例均是让网络侧来适应 UE，即让网络侧能够对 2G 的 UE 进行鉴权。当然，也可以让 UE 来适应网络侧，即让 2G 的用户加载一软件模块，从而使得该 2G 的 UE 能够完全地支持 3G 的功能，也就是使 2G 的 UE 能够支持 3G 的鉴权方式。这样，网络侧可以仍然采用标准的 3G 的鉴权方式对该 UE 进行鉴权。该软件模块可以从网上下载，也可以从运营商处直接获得。

以上所述实施例中的鉴权方式，既可以在 2G 的 UE 直接接入 AS 时应用，也可以在该接入的 UE 后续发送的消息中应用。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

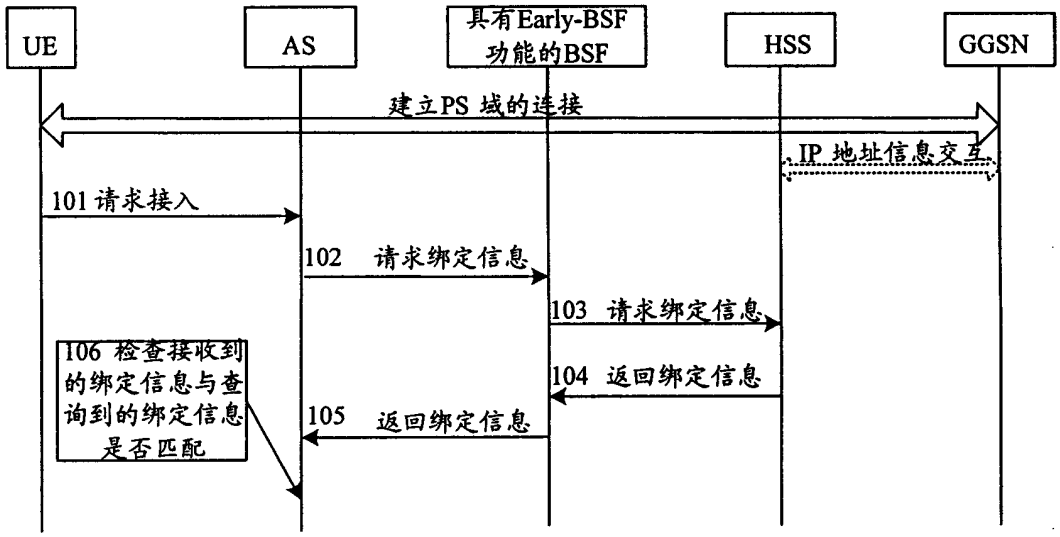

UE
AS
具有Early-BSF功能的BSF
HSS
GGSN
建立PS 域的连接
IP 地址信息交互
101 请求接入
102 请求绑定信息
103 请求绑定信息
104 返回绑定信息
105 返回绑定信息
106 检查接收到的绑定信息与查询到的绑定信息是否匹配

图 1

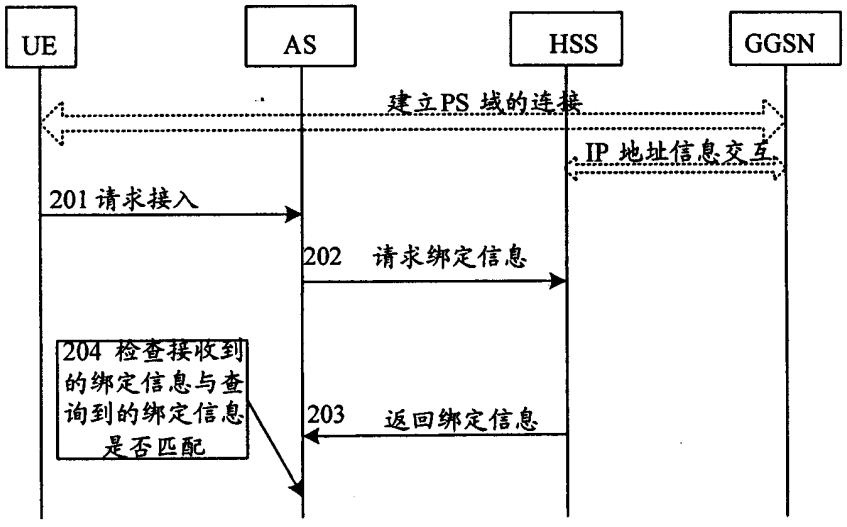

UE
AS
HSS
GGSN
建立PS 域的连接
IP 地址信息交互
201 请求接入
202 请求绑定信息
203 返回绑定信息
204 检查接收到的绑定信息与查询到的绑定信息是否匹配

图 2