(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 8 月 22 日 (22.08.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/157909 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01) *H04L 12/24* (2006.01)

(21) 国际申请号: PCT/CN2019/072529

(22) 国际申请日: 2019 年 1 月 21 日 (21.01.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810150774.0 2018年2月13日 (13.02.2018) CN

(71) 申请人: 华 为 技 术 有 限 公 司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 应江威(**YING, Jiangwei**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 谭仕勇(**TAN, Shiyong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 杨艳梅 (**YANG, Yanmei**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市海淀区宝盛南路1号院20号楼8层101-01, Beijing 100192 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** COMMUNICATION METHOD AND COMMUNICATION APPARATUS

(54) 发明名称: 一种通信方法及通信装置

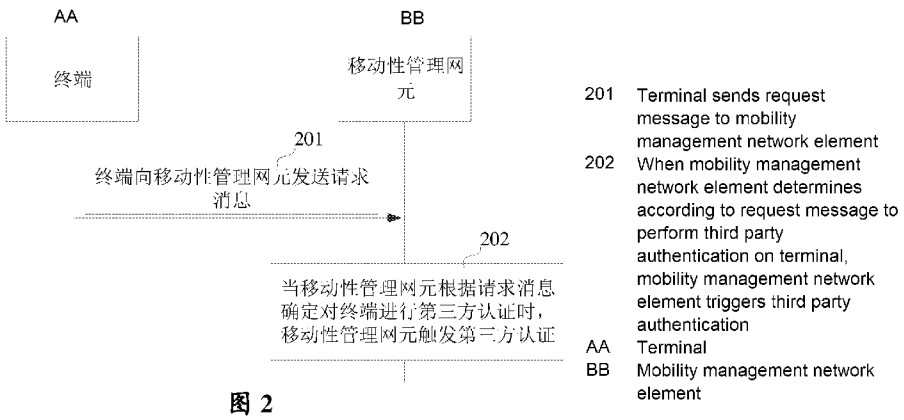

图 2

(57) **Abstract:** Provided are a communication method and a communication apparatus, used for achieving the goal of a terminal performing normal communication even in the case that local authentication is not performed. The method comprises: a mobility management network element receives a request message from a terminal used for requesting access to a network; when the mobility management network element determines according to the request message to perform third party authentication on the terminal, the mobility management network element triggers the third party authentication. Thus, after authentication between the terminal and a third party, even if local authentication is not performed, the terminal can still access the network to perform communication after undergoing the third party authentication.

(57) 摘要: 本申请实施例提供一种通信方法及通信装置，用于实现终端在未进行本地认证的情况下也可以进行正常通信的目的。本申请实施例中该方法包括: 移动性管理网元接收来自终端的用于请求接入网络的请求消息，当所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证时，所述移动性管理网元触发第三方认证，如此，终端与第三方之间认证之后，即使未进行本地认证，终端在经过第三方认证之后也可接入网络以进行通信。

WO 2019/157909 A1

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种通信方法及通信装置

本申请要求在 2018 年 2 月 13 日提交中华人民共和国知识产权局、申请号为201810150774.0、发明名称为“一种通信方法及通信装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信领域，尤其涉及一种通信方法及通信装置。

背景技术

移动通信系统中，为了保证系统的安全性，终端可以通过安全凭证与网络侧设备之间进行网络层的相互认证，并在认证成功后，终端与网络侧设备进行业务通信。在 4G 通信网络中，安全凭证可以是安装在终端上的通用集成电路卡(Universal Integrated Circuit Card，UICC)卡，终端可以基于 UICC 卡中的 USIM 与网络侧设备进行安全认证，例如，演进的分组系统（Evolved Packet System，EPS）认证和密钥协商（authentication and key agreement，AKA）安全认证。该安全认证可以称为本地认证，也可以称为网络层认证。

随着通信技术的发展，出现一些创新应用场景，例如，机器类通信（machine type communication，MTC）、工业控制、和智能交通系统（intelligent transportation system，ITS）等。相应地，在这些场景下，出现了一些成本较低、构造简单的终端，比如，无需安装 UICC 卡的 IoT 设备，上述基于网络层的安全认证无法满足需求。

发明内容

本申请实施例提供一种通信方法及通信装置，用于实现终端在未进行本地认证的情况下也可以进行正常通信的目的。

第一方面，提供了一种通信方法，该方法中移动性管理网元接收来自终端的请求消息，请求消息用于请求接入网络，当移动性管理网元根据请求消息确定对终端进行第三方认证时，移动性管理网元触发第三方认证。网络可以指运营商网络，具体可以包括无线接入网和核心网。如此，终端与第三方之间认证之后，即使未进行本地认证，终端在经过第三方认证之后也可接入网络以进行通信。

结合第一方面，在第一方面的第一种实施方式中，为了提供方案的灵活性，可以提供多种方式使移动性管理网元确定对终端进行第三方认证，比如，当请求消息中包括用于指示对终端进行第三方认证的指示信息时，移动性管理网元确定对终端进行第三方认证。再比如，当请求消息中包括应用标识时，移动性管理网元确定对终端进行第三方认证。再比如，当请求消息中包括终端的标识，且与终端的标识对应的认证方式为对终端进行第三方认证时，移动性管理网元确定对终端进行第三方认证。

结合第一方面的第一种实施方式，在第一方面的第二种实施方式中，所述请求消息还包括用户标识；或者，所述请求消息还包括用户标识和应用容器，应用容器用于对终端进行第三方认证。例如，通过请求消息中携带应用容器的方式将应用容器传输给应用服务器，一方面，可以避免应用服务器向终端请求应用容器，进而减少应用服务器与终端的信令交

互，另一方面，移动性管理网元可以将该应用容器发送给应用服务器，使得应用服务器可以基于该应用容器对终端进行第三方认证。

结合第一方面的第一种实施方式，在第一方面的第三种实施方式中，方法还包括：移动性管理网元根据请求消息向终端发送响应消息，响应消息包括用于指示终端通过控制面发送信息的指示信息。进一步地，移动性管理网元通过控制面接收用户标识。如此，终端可以通过控制面发送用户标识，从而可以避免终端发送失败。

结合第一方面的第三种实施方式，在第一方面的第四种实施方式中，方法还包括：移动性管理网元通过控制面接收应用容器，应用容器用于对终端进行第三方认证。如此，终端可以通过控制面发送应用容器，从而可以避免终端发送失败。

结合第一方面，在第一方面的第五种实施方式中，所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证，包括：当请求消息中包括用户标识时，移动性管理网元确定对终端进行第三方认证。如此，移动性管理网元可以通过简单的方式确定对终端进行第三方认证。

结合第一方面的第五种实施方式，在第一方面的第六种实施方式中，请求消息还包括应用容器，应用容器用于对终端进行第三方认证。例如，通过请求消息中携带应用容器的方式将应用容器传输给应用服务器，一方面，可以避免应用服务器向终端请求应用容器，进而减少应用服务器与终端的信令交互，另一方面，移动性管理网元可以将该应用容器发送给应用服务器，使得应用服务器可以基于该应用容器对终端进行第三方认证。

结合第一方面的第二种实施方式至第一方面的第六中实施方中的任一种实施方式，在第一方面的第七种实施方式中，为了提高方案的灵活性，移动性管理网元可以通过 AUSF 网元或 NEF 网元向应用服务器发送用户标识。

第二方面，提供了一种通信方法，包括：终端向移动性管理网元发送请求消息，请求消息中包括认证参考信息，认证参考信息用于移动性管理网元确定是否对终端进行第三方认证，终端接收来自移动性管理网元对请求消息的响应消息。该方法提供了一种新的认证方式，使得终端在第三方认证成功后即可接入网络，解决了终端在未进行本地认证的情况下无法接入网络的问题。

结合第二方面，在第二方面的第一种实施方式中，认证参考信息包括：用于指示对终端进行第三方认证的指示信息或应用标识，基于该指示信息或应用标识，移动性管理网元可以确定对终端进行第三方认证。如此，可以提高方案的灵活性。

结合第二方面的第一种实施方式，在第二方面的第二种实施方式中，请求消息还包括用户标识，使得应用服务器可以基于该用户标识对终端进行认证。

结合第二方面，在第二方面的第三种实施方式中，认证参考信息包括：用户标识。如此，移动性管理网元可以基于该用户标识确定对终端进行第三方认证。

结合第二方面的第二种实施方式或第二方面的第三种实施方式，在第二方面的第四种实施方式中，请求消息还包括应用容器，应用容器用于对终端进行第三方认证。例如，通过请求消息中携带应用容器的方式将应用容器传输给应用服务器，一方面，可以避免应用服务器向终端请求应用容器，减少应用服务器与终端的信令交互，另一方面，可以使得应用服务器基于该应用容器对终端进行认证。

结合第二方面的第一种实施方式，在第二方面的第五种实施方式中，响应消息包括用于指示终端通过控制面发送信息的指示信息，该方法还包括：终端通过控制面向移动性管

理网元发送用户标识。如此，终端可以通过控制面发送用户标识，从而可以避免终端发送失败。

结合第二方面的第五种实施方式，在第二方面的第六种实施方式中，方法还包括：终端通过控制面向移动性管理网元发送应用容器；其中，应用容器用于对终端进行第三方认证。进一步，移动性管理网元可以把应用容器传输给应用服务器，以使得应用服务器可以基于应用容器对终端进行第三方认证。

第三方面，提供了一种通信方法，该方法中，AUSF 网元接收来自移动性管理网元的用户标识；AUSF 网元向应用服务器请求用户标识对应的认证参数；AUSF 网元接收来自应用服务器的认证参数，认证参数用于对终端进行认证，例如，认证参数用于对终端进行本地认证，也可以用于对终端进行第三方认证。可见，为了兼容现有技术，AUSF 网元仍然具备对终端进行认证的功能，但是在这种情况下，AUSF 网元可以向应用服务器请求用户标识对应的认证参数，以便实现对终端的认证，提高了方案的灵活性。

结合第三方面，在第三方面的第一种实施方式中，方法还包括：AUSF 网元向应用服务器发送应用容器，应用容器用于应用服务器对终端进行第三方认证。如此，可以使应用服务器基于应用容器对终端进行认证，从而可以避免应用服务器再次向终端请求应用容器，从而可以减少应用服务器与终端的信令交互。

结合第三方面或第三方面的第一种实施方式，在第三方面的第二种实施方式中，为了兼容现有技术，方法还包括：AUSF 网元根据认证参数对终端进行认证，从而可以进一步提高了网络的安全性。

第四方面，提供了一种通信方法，该方法中，PCF 网元接收 SMF 网元发送的策略控制和计费 (Policy Control and Charging，PCC)策略建立请求消息，PCC 策略建立请求消息包括用户标识；PCF 网元根据用户标识，获得用户标识对应的 PCC 策略；PCF 网元向 SMF 网元发送 PCC 策略。如此，可以获得更细粒度的 PCC 策略，例如，应用级别的粒度或用户级别的粒度，提高了 PCC 策略的灵活性。

结合第四方面，在第四方面的第一种实施方式中，所述 PCC 策略还包括收费信息。如此，可以为第三方为终端提供付费服务，或者为用户制定个性化收费标准奠定基础。

第五方面，提供了一种通信方法，该方法中，SMF 网元向 PCF 网元发送 PCC 策略建立请求消息，PCC 策略建立请求消息包括用户标识；SMF 网元接收来自 PCF 网元的用户标识对应的 PCC 策略。在一种可选地实施方式中，PCC 策略建立请求消息中还包括应用标识。如此，可以获得更细粒度的 PCC 策略，比如可以将 PCC 策略制定为应用级别的粒度或用户级别的粒度，举个例子，为不同的应用设置不同的 PCC 策略，或者为同一个应用对应的不同的用户设置不同的 PCC 策略，可见，该方法可提高 PCC 策略设置的灵活性。

结合第五方面，在第五方面的第一种实施方式中，方法还包括：SMF 网元接收应用服务器发送的根密钥；SMF 网元根据根密钥与终端进行密钥协商。如此，在终端未进行本地认证的情况下，应用服务器可以为 SMF 网元分配根密钥，以便实现 SMF 网元与终端之间的安全保护。

第六方面，提供了一种通信装置，包括处理器，处理器与存储器耦合，存储器用于存储程序，处理器调用存储器存储的程序，以执行以上第一方面的方法。该通信装置可以是移动性管理网元，也可以是至少一个处理元件或芯片。

第七方面，提供了一种通信装置，包括处理器，处理器与存储器耦合，存储器用于存

储程序，处理器调用存储器存储的程序，以执行以上第二方面的方法。该通信装置可以是终端，也可以是至少一个处理元件或芯片。

第八方面，提供了一种通信装置，包括处理器，处理器与存储器耦合，存储器用于存储程序，处理器调用存储器存储的程序，以执行以上第三方面的方法。该通信装置可以是AUSF网元，也可以是至少一个处理元件或芯片。

第九方面，提供了一种通信装置，包括处理器，处理器与存储器耦合，存储器用于存储程序，处理器调用存储器存储的程序，以执行以上第四方面的方法。该通信装置可以是PCF网元，也可以是至少一个处理元件或芯片。

第十方面，提供了一种通信装置，包括处理器，处理器与存储器耦合，存储器用于存储程序，处理器调用存储器存储的程序，以执行以上第五方面的方法。该通信装置可以是SMF网元，也可以是至少一个处理元件或芯片。

第十一方面，提供了一种通信装置，包括用于执行以上第一方面的方法中各个步骤的单元或者手段（means）。该通信装置可以是移动性管理网元，也可以是至少一个处理元件或芯片。

第十二方面，提供了一种通信装置，包括用于执行以上第二方面的方法中各个步骤的单元或者手段（means）。该通信装置可以是终端，也可以是至少一个处理元件或芯片。

第十三方面，提供了一种通信装置，包括用于执行以上第三方面的方法中各个步骤的单元或者手段（means）。该通信装置可以是AUSF网元，也可以是至少一个处理元件或芯片。

第十四方面，提供了一种通信装置，包括用于执行以上第四方面的方法中各个步骤的单元或者手段（means）。该通信装置可以是PCF网元，也可以是至少一个处理元件或芯片。

第十五方面，提供了一种通信装置，包括用于执行以上第五方面的方法中各个步骤的单元或者手段（means）。该通信装置可以是SMF网元，也可以是至少一个处理元件或芯片。

第十六方面，本申请实施例提供一种通信系统，该通信系统包括移动性管理网元和终端，分别用于实现以上第一方面或第二方面提供的方法中的步骤。

结合第十六方面，在第十六方面的第一种实施方式中，该通信系统还可以包括AUSF网元、PCF网元和SMF网元中的任一个或任多个，分别用于实现以上方法中相应的步骤。

第十七方面，提供了一种程序，该程序在被处理器执行时用于执行以上第一方面至第五方面中的任一方面或任一方面的任一种实施方式中的方法。

第十八方面，提供了一种计算机可读存储介质，包括第十七方面的程序。

附图说明

图1为本申请实施例适用的一种通信系统结构示意图；

图2为本申请实施例提供的一种通信方法流程示意图；

图3为本申请实施例提供的另一种通信方法流程示意图；

图4为本申请实施例提供的另一种通信方法流程示意图；

图5为本申请实施例提供的另一种通信方法流程示意图；

图6为本申请实施例提供的另一种通信方法流程示意图；

图7为本申请实施例提供的另一种通信方法流程示意图；

图 8 为本申请实施例提供的另一种通信方法流程示意图；

图 9 为本申请实施例提供的一种移动性管理网元的结构示意图；

图 10 为本申请实施例提供的一种终端的结构示意图；

图 11 为本申请实施例提供的一种通信装置的结构示意图；

图 12 为本申请实施例提供的一种通信装置的结构示意图；

图 13 为本申请实施例提供的一种通信装置的结构示意图；

图 14 为本申请实施例提供的另一种通信装置的结构示意图；

图 15 为本申请实施例提供的另一种通信装置的结构示意图；

图 16 为本申请实施例提供的另一种通信装置的结构示意图；

图 17 为本申请实施例提供的另一种通信装置的结构示意图；

图 18 为本申请实施例提供的另一种通信装置的结构示意图；

图 19 为本申请实施例提供的一种通信系统结构示意图。

具体实施方式

图 1 示例性示出了本申请实施例适用的一种 5G 通信系统结构示意图，该通信系统结构可以应用于下一代通信系统。下面对该图 1 中所示的各个组成部分进行简单介绍。

终端：可以包括各种具有通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备，以及各种形式的终端，例如，移动台（mobile station，MS），终端（terminal），用户设备（user equipment，UE），软终端等等，举例来说有水表、电表、传感器、手机和 ipad 等。

无线接入网（radio access network，RAN）：可以由 5G-RAN 节点组成的网络，实现无线物理层功能、资源调度和无线资源管理、无线接入控制以及移动性管理功能。例如，5G-RAN 通过用户面接口 N3 和 UPF 网元相连，用于传送终端的数据；5G-RAN 通过控制面接口 N2 和接入和移动性管理功能（Access and Mobility Management Function，AMF）网元建立控制面信令连接，用于实现无线接入承载控制等功能。

认证服务功能（authentication server function，AUSF）网元：用于负责保证终端和网络之间的安全认证。

AMF 网元：负责移动性管理和接入管理等，用于实现 4G 系统中移动性管理实体（mobility management entity，MME）功能中除会话管理之外的其它功能。例如，负责维护和管理终端的状态信息，负责终端的认证，选择网络切片，或选择会话管理功能（session management function，SMF）网元。

SMF 网元：为终端建立会话，分配会话的 IP 地址，管理或终止会话；选择用户面功能（User plane function，UPF）网元；选择网络开放功能（network exposure function，NEF）网元。

NEF 网元：负责连接 SMF 网元与外部 DN 网络，可以包括第三方认证网元。

UPF 网元：提供会话和承载管理，IP 地址分配等功能；例如，负责对终端的数据报文过滤、数据传输/转发、速率控制、生成计费信息等。

统一数据管理功能（unified data management，UDM）网元：为网络网元分配参考信息，例如，为 SMF 网元或 NEF 网元分配参考信息。

策略控制功能（Policy Control Function，PCF）网元：为网络网元分配参考信息，例如，

为 SMF 网元或 NEF 网元分配参考信息。

第三方认证网元：外部数据网络的安全认证和授权功能网元，可以用于对终端进行安全认证和授权检查。例如，第三方认证网元可以为 DN 设备，DN 设备可以为 DN-AAA 服务器，AF，AF-AAA，应用服务器（Application-Server），Application-Server-AAA 的任意一种。举个例子，比如第三方认证网元可以是腾讯、阿里巴巴或支付宝等应用厂商。

需要指出的是，本申请各实施例中以第三方认证网元为应用服务器为例进行描述，涉及的应用服务器均可以替换为第三方认证网元，不予限制。

上述图 1 所示的各个组成部分可以通过下一代网路架构下的各个接口进行通信，例如，终端与 AMF 网元可以通过 N1 接口进行通信。

本申请实施例所提供的方案可以适用于如图 1 所示的 5G 通信系统，也可以适用于 4G 通信系统，还可以适用于 5G 的下一代通信系统，本申请实施例中的网元（比如移动性管理网元、AMF 网元、SMF 网元、NEF 网元、AUSF 网元和 UPF 网元等中的任一个网元）可以是一个物理设备上的功能模块，也可以是一个单独的物理设备。

需要指出的是，本申请中提及的“网络”可以指运营商网络，也可以指的是无线通信网络，具体可以包括无线接入网和核心网，其中，核心网可以是由运营商部署的设备中除无线接入网部分，例如，AMF 网元，SMF 网元，以及 UPF 网元等，不予限制。

本申请中提及的移动性管理网元为具有移动性管理功能的网元，例如，AMF 网元或 MME 网元。

此外，本申请的各实施例以第三方认证网元为应用服务器为例进行描述，所涉及的应用服务器均可以替换为第三方认证网元。

如图 2 所示，本申请实施例提供了一种通信方法，该方法包括：

步骤 201，终端向移动性管理网元发送请求消息。

相应地，移动性管理网元接收来自终端的请求消息。

其中，请求消息可以用于请求接入网络，该请求消息可以是注册请求（attach request）消息。

步骤 202，当移动性管理网元根据请求消息确定对终端进行第三方认证时，移动性管理网元触发第三方认证。

具体的，上述步骤 202 中的第三方认证可以是第三方认证网元对用户标识和密钥进行认证，若第三方认证网元对用户标识认证成功，则确定第三方认证网元对终端进行第三方认证成功，若第三方认证网元对用户标识认证失败，则确定第三方认证网元对终端进行第三方认证失败。

可选地，步骤 202 中移动性管理网元根据请求消息确定对终端进行第三方认证可以替换为：移动性管理网元根据请求消息确定跳过对终端进行本地认证，或者，根据指示信息确定不对终端进行本地认证，其实现方式可以参见下述第一种实施场景中的描述，不予限制。

通过上述实施例提供的方案，在终端未进行网络认证的情况下，也可以使终端进行通信，如此，不仅可以解决背景技术中提到的无安全凭证的终端的认证问题，也可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

需要说明的是，在对终端进行第三方认证的情况下，可以对该终端进行本地认证，也可以不对该终端进行本地认证。比如，为了提高安全性，在对终端进行本地认证成功后，

再对终端进行第三方认证。对终端的双重认证，可以大大提高了网络的安全性。再比如，仅对终端进行第三方认证，并在第三方认证成功后终端即可接入网络，能够提高了终端认证的灵活性，不但解决了背景技术中提及的场景下终端无法接入网络的问题，还能够解决未开通漫游的场景下终端无法接入网络的问题。

可选地，在上述实施例的第一种实施场景下，步骤 202 中移动性管理网元根据请求消息确定对终端进行第三方认证可以包括如下实现方式:

方式一、当所述请求消息中包括用于指示对所述终端进行第三方认证的指示信息时，所述移动性管理网元确定对所述终端进行第三方认证。

其中，请求消息中可以包括用于指示对终端进行第三方认证的指示信息。该指示信息可以称为受限服务指示（limited service indication）或者第三方认证指示（third party authentication indication）。

具体的，请求消息中可以包括认证参考信息，其中，认证参考信息可用于所述移动性管理网元确定是否对所述终端进行第三方认证。认证参考信息可以包括用于指示对终端进行第三方认证的指示信息。如此，移动性管理网元可以通过较为简单的方式确定出对终端进行第三方认证。

示例性地，终端可以在确定终端进行第三方认证时，将用于指示对终端进行第三方认证的指示信息携带于请求消息中。

其中，终端确定进行第三方认证的方式可以有多种方法，比如，可以预先设置该终端的认证方式为第三方认证方式；再比如，该终端在未检测到可用的 VPLMN 时（即终端无法正常接入 VPLMN 网络），确定该终端进行第三方认证；还比如，VPLMN 的广播消息中指示 VPLMN 支持终端受限接入（支持终端受限接入的意思是指支持终端进行第三方认证）或第三方认证时，确定该终端进行第三方认证；再比如，该终端在未检测到可用的 VPLMN 时（即终端没有开通在 VPLMN 的漫游，无法正常接入 VPLMN 网络），且 VPLMN 的广播消息中指示 VPLMN 支持 UE 受限接入或第三方认证时，确定该终端进行第三方认证。

方式二、当所述请求消息中包括应用标识时，所述移动性管理网元确定对所述终端进行第三方认证。

示例性地，可以在终端中预先设置进行第三方认证的应用标识（例如，预先设置一个或多个应用标识），终端可以从预先设置的进行第三方认证的应用标识中选取一个应用标识，并将该选取的应用标识通过请求消息发送给移动性管理网元，通过移动性管理网元触发该应用标识对应的应用服务器对终端进行第三方认证。

具体的，请求消息中可以包括认证参考信息，其中，认证参考信息可用于所述移动性管理网元确定是否对所述终端进行第三方认证。认证参考信息可以包括应用标识。如此，移动性管理网元可以通过较为简单的方式确定出对终端进行第三方认证。

其中，应用标识可以用于标识进行第三方认证的应用。

方式三、当所述请求消息中包括所述终端的标识，且与所述终端的标识对应的认证方式为对所述终端进行第三方认证时，所述移动性管理网元确定对所述终端进行第三方认证。

具体的，请求消息中可以包括认证参考信息，其中，认证参考信息可用于所述移动性管理网元确定是否对所述终端进行第三方认证。认证参考信息可以包括终端的标识。

其中，终端的标识可以用于标识终端，可以为全球唯一临时标识（global unique

temporary identity，GUTI），国际移动用户识别码（International Mobile Subscriber Identification，IMSI），或临时识别码（Temporary Mobile Subscriber Identity，TMSI）等。

示例性地，终端可以预先存储终端的标识和认证方式的对应关系，认证方式可以包括本地认证和第三方认证。一个终端的标识可以对应至少一种认证方式，一个终端的标识可以对应本地认证，或者一个终端的标识对应第三方认证，或者一个终端的标识对应本地认证和第三方认证。举个例子，终端为一个智能水表，该智能水表进行第三方认证，则终端的标识和认证方式的对应关系中可以包括：该智能水表的标识和第三方认证的对应关系。移动性管理网元可以根据终端的标识和认证方式的对应关系，确定出该终端是否进行第三方认证。

示例性地，移动性管理网元可以存储有终端类型与认证方式的对应关系，移动性管理网元先根据终端的标识确定出终端的类型，之后根据该终端的类型与认证方式之间的对应关系，确定该终端的认证方式为第三方认证。如此，移动性管理网元可以通过较为简单的方式确定出对终端进行第三方认证。

其中，终端的标识还可以是能够指示出终端类型的终端的标识或移动设备（mobile equipment，ME）标识。判断终端的类型具体可能有多种实现形式，比如判断该终端是否属于 IoT 类型，或者判断该终端是否属于预设的厂商，或者判断该终端是否属于预设的应用企业等等。

方式四、当所述请求消息中包括用户标识时，所述移动性管理网元确定对所述终端进行第三方认证。

具体的，请求消息中可以包括认证参考信息，其中，认证参考信息可用于所述移动性管理网元确定是否对所述终端进行第三方认证。认证参考信息可以包括用户的标识。

其中，用户标识也可以称为应用用户标识（Application User ID）。用户标识可以由进行第三方认证的应用服务器所分配的。用户标识与进行第三方认证的应用服务器相对应或相关联。

可选地，上述方式一、方式二、方式三和方式四中确定对终端进行第三方认证的方式可以单独使用，也可以组合使用。当请求消息中包括终端的标识、用于指示对终端进行第三方认证的指示信息、应用标识和用户标识中的任多个时，可以为上述方式一、方式二、方式三和方式四中的各个用于确定是否对终端进行第三方认证的方式设置优先级，之后根据优先级确定根据哪个信息确定对终端进行第三方认证。

需要说明的是，上述请求消息可以包括用户标识，也可以不包括用户标识。

进一步地，上述请求消息还可以包括应用容器（application container）。其中，应用容器可以用于应用服务器对终端进行第三方认证。可选地，应用容器也可以称为应用安全容器（application security container）或安全容器（security container）。应用容器中可以包括用于第三方认证的一些参数，比如，密钥相关信息(例如，安全挑战值)等。密钥相关信息可以是使用密钥生成的一个的安全挑战值。一种可选地实施方式中，若应用服务器成功验证了用户标识所对应的安全挑战值，则可以确认该用户标识对应的终端第三方认证成功，相对应地，若应用服务器对用户标识所对应的安全挑战值验证失败，则可以确认该用户标识对应的终端第三方认证失败。

可选地，移动性管理网元可以通过 NEF 网元或 AUSF 网元或 SMF 网元向应用服务器发送应用容器。通过请求消息中携带应用容器的方式将应用容器传输给应用服务器，一方

面，可以避免应用服务器向终端请求应用容器，进而减少应用服务器与终端的信令交互，另一方面，移动性管理网元可以将该应用容器发送给应用服务器，使得应用服务器可以基于该应用容器对终端进行第三方认证。

在第一个示例中，假设上述请求消息不包括用户标识，也不包括应用容器，那么上述方法还可以包括：移动性管理网元根据请求消息向终端发送响应消息，该响应消息包括用于指示所述终端通过控制面发送信息的指示信息；终端根据指示信息，通过控制面向移动性管理网元发送用户标识；相应地，移动性管理网元通过控制面接收该用户标识。例如，终端通过非接入层（Non-access Stratum，NAS）消息向移动性管理网元发送用户标识。

进一步地，还可以包括：终端根据指示信息，通过控制面向移动性管理网元发送应用容器；相应地，移动性管理网元通过控制面接收该应用容器。例如，终端通过 NAS 消息向移动性管理网元发送应用容器。其中，用户标识与应用容器可以携带在同一个 NAS 消息中，也可以携带在不同的 NAS 消息中，不予限制。

需要指出的是，终端通过控制面发送信息，可以避免终端发送失败，可以参见下述内容中图 5 所示实施例中的相关内容。

在第二个示例中，假设上述请求消息包括用户标识，不包括应用容器，那么上述方法还可以包括：移动性管理网元根据请求消息向终端发送响应消息，该响应消息包括用于指示所述终端通过控制面发送信息的指示信息；终端根据指示信息，通过控制面向移动性管理网元发送应用容器；相应地，移动性管理网元通过控制面接收应用容器。例如，终端通过 NAS 消息向移动性管理网元发送应用容器。

需要指出的是，终端通过控制面发送信息，可以避免终端发送失败，可以参见下述内容中图 5 所示实施例中的相关内容。

在第三个示例中，假设上述请求消息不包括用户标识，也不包括应用容器，那么上述方法还可以包括：移动性管理网元根据请求消息向终端发送响应消息；终端向移动性管理网元通过 NAS 消息发送用户标识。例如，用户标识可以携带在分组数据单元（Packet Data Unit，PDU）会话建立请求中，该 PDU 会话建立请求携带在该 NAS 消息中。再例如，NAS 消息包括用户标识和 PDU 会话建立请求。

进一步地，还可以包括：终端向移动性管理网元通过 NAS 消息发送应用容器。例如，应用容器可以携带在 PDU 会话建立请求中，该 PDU 会话建立请求携带在该 NAS 消息中。再例如，NAS 消息包括应用容器和 PDU 会话建立请求。

需要指出的是，终端通过 NAS 消息发送信息，可以更好的现有技术兼容，可以参见下述内容中图 6 和图 7 所示实施例中的相关内容。

在第四个示例中，假设上述请求消息包括用户标识，不包括应用容器，那么上述方法还可以包括：移动性管理网元根据请求消息向终端发送响应消息；终端向移动性管理网元通过 NASSM 消息发送应用容器。例如，应用容器可以携带在 PDU 会话建立请求中，该 PDU 会话建立请求携带在该 NAS 消息中。再例如，NAS 消息包括用户标识和 PDU 会话建立请求。

需要指出的是，终端通过 NAS 消息发送应用容器，可以更好地与现有技术兼容，可以参见下述内容中图 6 和图 7 所示实施例中的相关内容。

其中，当上述请求消息为注册请求，且移动性管理网元对终端注册成功时，上述各示例中的响应消息可以是注册接受消息；当上述请求消息为注册请求，且移动性管理网元对

终端注册失败时，上述响应消息可以是注册失败消息。

需要指出的是，当响应消息为注册失败消息时，该响应消息可以不包括上述指示信息，不予限制。

进一步可选地，上述方法还包括：移动性管理网元通过 AUSF 网元或 NEF 网元向应用服务器发送用户标识。

可选地，在上述实施例的第二种实施场景下，步骤 202 中移动性管理网元触发第三方认证可以采用如下方式实现。

方式 A、移动性管理网元向 NEF 网元发送第一信息，使得 NEF 网元向应用服务器发送第二信息，以使得该应用服务器基于第二信息对终端进行第三方认证。该方案可以参见图 3 和图 5 所示实施例中的相关描述。

其中，上述第一信息可以是用户标识，或应用容器，还可以是信令或消息，也可以是数据包，不予限制。第二信息可以是用户标识，或应用容器，还可以是信令或消息，也可以是数据包，上述第二信息与第一信息可以相同，也可以不同，不予限制。

在第一个示例中，移动性管理网元将从终端接收到的应用标识发送给 NEF 网元；NEF 网元根据该应用标识获得该应用标识对应的应用服务器的地址信息，并向该应用服务器发送信令，使得该应用服务器对终端进行第三方认证。例如，NEF 网元根据应用标识进行域名服务器（Domain Name Server，DNS）查询，获取应用服务器的地址信息。再例如，NEF 网元存储有应用标识与应用服务器的地址信息之间的对应关系，NEF 网元根据该应用标识查询出该应用标识对应的应用服务器的地址信息。如此可以使 NEF 网元确定出应用服务器，从而使应用服务器对终端进行第三方认证。

在第二个示例中，移动性管理网元向 NEF 网元发送用户标识，NEF 网元根据用户标识获得应用标识。其中，该用户标识可以指示应用标识，或者，NEF 网元根据用户标识的格式可以确定出应用标识。比如，用户标识是完全合格域名（Fully Qualified Domain Name，FQDN）格式的标识，则可以根据 FQDN 格式的用户标识获取应用标识；又比如，用户标识是腾讯的邮箱地址，则可根据该应用标识确定应用服务器为腾讯。然后，NEF 网元可以根据该应用标识获得该应用标识对应的应用服务器的地址信息，并向该应用服务器发送信令，相关描述可以参见第一个示例，不再赘述。如此可以使 NEF 网元确定出应用服务器，从而使应用服务器对终端进行第三方认证。

在第三个示例中，移动性管理网元向 NEF 网元发送终端的标识，NEF 网元根据终端的标识确定出应用标识。例如，NEF 网元可以存储有终端的标识和应用标识的对应关系，NEF 网元可以根据该对应关系，确定出该终端的标识对应的应用标识。然后，NEF 网元可以根据该应用标识获得该应用标识对应的应用服务器的地址信息，并向该应用服务器发送信令，相关描述可以参见第一个示例，不再赘述。如此可以使 NEF 网元确定出应用服务器，从而使应用服务器对终端进行第三方认证。

在第四个示例中，移动性管理网元根据终端的标识确定出应用标识，并将应用标识发送给 NEF 网元，然后，NEF 网元可以根据该应用标识获得该应用标识对应的应用服务器的地址信息，并向该应用服务器发送信令，相关描述可以参见第一个示例，不再赘述。如此可以使 NEF 网元确定出应用服务器，从而使应用服务器对终端进行第三方认证。

方式 B、移动性管理网元向 AUSF 网元发送第一信息，使得 AUSF 网元向应用服务器发送第二信息，以使得该应用服务器基于第二信息对终端进行第三方认证。如此，可以更

好的兼容现有技术。该方案可以参见图 4 所示实施例中的相关描述。

其中，上述第一信息和第二信息可以参见方式 A 中的描述，不予限制。

示例性地，移动性管理网元将接收到的用户标识发送给 AUSF 网元，AUSF 网元通过 NEF 网元将用户标识发送给应用服务器，从而使应用服务器基于该用户标识对终端进行第三方认证。

进一步地，移动性管理网元可以将接收到的应用容器发送给 AUSF 网元，AUSF 网元通过 NEF 网元将应用容器发送给应用服务器，从而使应用服务器基于该应用容器对用户标识对应的终端进行第三方认证。

该方式 B 中，NEF 网元确定出应用标识的方式与上述方式 A 中的第一个示例至第四个示例类似，在此不再赘述。

方式 C、移动性管理网元向 SMF 网元发送第一信息，使得 SMF 网元向应用服务器发送第二信息，以使得该应用服务器基于第二信息对终端进行第三方认证。如此，可以更好的兼容现有技术。该方案可以参见图 6 或 7 所示实施例中的相关描述。

其中，上述第一信息和第二信息可以参见方式 A 中的描述，不予限制。

在一个示例中，移动性管理网元在确定对终端进行第三方认证之后，向终端发送请求消息的响应，以使得终端发送 NAS 消息，该 NAS 消息携带用户标识。移动性管理网元接收到终端发送的携带用户标识的 NAS 消息，并将 NAS 消息传输给 SMF 网元，以使得 SMF 网元通过 NEF 网元将 NAS 消息中的用户标识发送给应用服务器，从而使应用服务器基于该用户标识对终端进行第三方认证。

进一步地，上述 NAS 消息还可以携带应用容器，SMF 网元通过 NEF 网元将 NAS 消息中的应用容器发送给应用服务器，从而使应用服务器基于该用户标识对终端进行第三方认证。

此外，上述示例中，NEF 网元可以采用上述第二种实施场景的方式 A 中的第一个示例至第四个示例中的方法确定出应用服务器，在此不再赘述。

在另一个示例中以第三方认证网元为数据网络为例介绍，移动性管理网元在向终端发送对请求消息的响应之后，接收到终端发送的携带用户标识的 NAS 消息，移动性管理网元将 NAS 消息传输给 SMF 网元，SMF 网元通过 UPF 网元将 NAS 消息中的用户标识发送给数据网络，从而使数据网络基于该用户标识对终端进行第三方认证。

进一步地，上述 NAS 消息还可以携带应用容器，SMF 网元通过 UPF 网元将 NAS 消息中的应用容器发送给数据网络，从而使应用服务器基于该用户标识对终端进行第三方认证。

需要注意的是，上述第一种实施场景下的方式一、方式二、方式三或方式四中的任一种方式可以与上述第二种实施场景下的方式 A、方式 B 或方式 C 中的任一种方式结合使用。例如：当移动性管理网元采用上述第一种实施场景下的方式一、方式二、方式三或方式四中任一种方式确定对终端进行第三方认证时，移动性管理网元可以采用上述第二种实施场景下的方式 A 或方式 B 中的任一种方式结合使用。再例如，当移动性管理网元采用上述第一种实施场景下的方式一、方式二或方式三中任一种方式确定对终端进行第三方认证时，移动性管理网元可以采用上述第二种实施场景下的方式 C 结合使用。

图 3 提供了另一种通信方法流程示意图，如图 3 所示，该实施例中以移动性管理网元

为 AMF 网元，以请求消息为注册请求为例进行介绍，移动性管理网元可以通过 NEF 网元与应用服务器交互。该方法包括:

步骤 301，终端向 AMF 网元发送注册请求（registration request）。

其中，注册请求可以包括用户标识和用于指示对终端进行第三方认证的指示信息。

步骤 302，AMF 网元根据注册请求中的指示信息，确定对终端进行第三方认证。

可选地，步骤 302 替换为 AMF 网元根据指示信息确定跳过对终端的本地认证或确定不对终端进行本地认证。

步骤 303，AMF 网元向 NEF 网元发送用户标识。

示例性地，AMF 网元可以调用 NEF 网元的消息传递服务来实现向 NEF 网元发送用户标识的目的，消息传递服务例如可以是 NEF 通信消息传输，（NEF_communication_message transfer），调用消息传递服务具体可以是 AMF 网元向 NEF 网元发送消息传递请求，消息传递请求例如可以是 NEF 通信消息传输请求（NEF_communication_message transfer request），其中，消息传递请求中包括用户标识。

可选地，步骤 303 还包括: NEF 网元向 AMF 网元发送消息传递响应，例如，NEF 通信消息传输响应（NEF_communication_message transfer response）。

步骤 304，NEF 网元向应用服务器发送该用户标识。

步骤 305，应用服务器对用户标识对应的终端进行第三方认证。

具体地，应用服务器可以基于应用容器对该终端进行第三方认证，应用服务器可以通过下面两种方式获得该应用容器。

一种可选地实施方式中，在步骤 301 的注册请求中携带应用容器，从而通过 NEF 网元发送至应用服务器；另一种可选地实施方式中，在步骤 301 的注册请求中不携带应用容器，在步骤 304 之后，应用服务器从终端上获取应用容器，例如，应用服务器发送请求消息给终端，以获取应用容器。

步骤 306，应用服务器向 NEF 网元发送认证结果。

其中，认证结果可以包括认证成功或认证失败。

其中，认证成功可以表明允许终端进行常规数据传输（normal data transmission authorized）。

步骤 307，NEF 网元向 AMF 网元发送认证结果。

示例性地，NEF 网元调用 NEF 网元提供的消息通知服务，例如，NEF 通信消息通知（NEF_communication_message notify），即 NEF 网元发送消息通知，例如，NEF 消息通信消息通知（NEF_communication_message notify）给 AMF 网元，其中包括认证结果。

步骤 308，当认证结果为认证成功时，AMF 网元向终端发送注册接受（registration accept）。

图 3 示出的方案中，AMF 网元确定对终端进行第三方认证，并通过 NEF 网元实现触发应用服务器对终端进行第三方认证，实现了在终端未进行网络认证的情况下，也可以使终端进行通信，如此，不仅可以解决背景技术中提到的无安全凭证的终端的认证问题，也可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

图 4 提供了另一种通信方法流程示意图，图 4 所示的通信方法中可以基于 AUSF 网元

来实现对终端的第三方认证。如图 4 所示，该实施例中以移动性管理网元为 AMF 网元，以请求消息为注册请求为例进行介绍，移动性管理网元通过 AUSF 网元与应用服务器交互。该方法包括:

步骤 401，终端向 AMF 网元发送注册请求。

其中，注册请求中可以包括用户标识、应用容器和用于指示对终端进行第三方认证的指示信息。

步骤 402，AMF 网元根据注册请求中的指示信息，确定对终端进行第三方认证。

步骤 403，AMF 网元向 AUSF 网元发送终端认证请求。

其中，终端认证请求中可以包括用户标识、应用容器和用于指示对终端进行第三方认证的指示信息。

例如，AMF 网元可以调用 AUSF 网元提供的终端认证服务，实现向 AUSF 网元发送终端认证请求的目的。

步骤 404，AUSF 网元根据终端认证请求中的指示信息确定对该终端进行三方认证。

可替换地，步骤 401 中注册请求可以包括应用标识，或终端的标识，或用户标识，相应地，终端认证请求包括应用标识，或终端的标识，或用户标识，进一步地，步骤 404 可以替换为下述方式一至方式三种中的任一种方式:

方式一、当终端认证请求中包括应用标识时，AUSF 网元确定对终端进行第三方认证。

方式二、当终端认证请求中包括终端的标识，且与终端的标识对应的认证方式为对终端进行第三方认证时，AUSF 网元确定对所述终端进行第三方认证。

方式三、当终端认证请求中包括用户标识时，AUSF 网元确定对终端进行第三方认证。

该方式一至方式三种的涉及到的相关方案与上述第一种实施场景中的方式二至方式四类似，在此不再赘述。

步骤 405，AUSF 网元向 NEF 网元发送用户标识。

步骤 405 可以借鉴上述步骤 303 中 AMF 网元向 NEF 网元发送用户标识的内容，在此不再赘述。

步骤 406，NEF 网元向应用服务器发送该用户标识。

其中，NEF 网元可以采用图 2 所示实施例中提供的方案来确定出应用服务器，在此不再赘述。

步骤 407，应用服务器对用户标识对应的终端进行第三方认证。

具体地，在步骤 407 中，应用服务器可以基于应用容器对该终端进行第三方认证，应用服务器可以通过下面两种方式获得该应用容器。

一种可选地实施方式中，步骤 401 的注册请求中携带应用容器，从而 AUSF 网元和 NEF 网元发送至应用服务器；另一种可选地实施方式中，在步骤 401 的注册请求中不携带应用容器，在步骤 406 之后，应用服务器从终端获取应用容器。

步骤 408，应用服务器向 NEF 网元发送认证结果和用户标识对应的认证参数。

示例性的，认证参数可以是 5G 认证向量，也可以是 5G 认证向量（credential）中的参数，5G 认证向量可以是 EPS-AKA*对应的认证向量，也可以是 EAP-AKA'对应的认证向量，可以基于应用层的参数生成，例如用户标识，用户标识对应的密钥等。

步骤 409， NEF 网元向 AUSF 网元发送认证结果和将用户标识对应的认证参数。

在步骤 409 中，NEF 网元向 AUSF 网元发送信息的方式可以参见上述步骤 307，在此

步骤赘述。

可选地，在步骤 409 之后，AUSF 网元将认证结果发送给 AMF 网元。

步骤 410，AUSF 网元基于认证参数对终端进行本地认证。

上述步骤 410 中可以包括：AUSF 网元、AMF 网元和终端之间基于认证参数进行安全流程、进行空口安全协商、进行安全认证、进行网络层的认证或者进行本地认证等等，属于现有技术，不再赘述。

步骤 411，在认证结果为认证成功，且 AUSF 网元对终端的本地认证认证成功时，AMF 网元向终端发送注册接受。

在步骤 411 中，AUSF 网元在对终端的本地认证认证成功时，向 AMF 网元发送用于指示本地认证认证成功的指示信息。

相应地，AMF 网元根据该指示信息确定对终端的本地认证成功。

在上述步骤 408 中，应用服务器也可以不对终端进行第三方认证，则在步骤 408 和步骤 409 中仅向 AUSF 网元发送认证参数即可，这种情况下，在步骤 411 中，AMF 网元可以在确认 AUSF 网元对终端认证成功之后，向终端发送注册接受。

图 4 所提供的方案中，AMF 网元确定对终端进行第三方认证，并触发应用服务器向 AUSF 网元发送认证参数，用于 AUSF 网元进行本地认证，解决背景技术中提到的无安全凭证的终端的认证问题，保证了网络的安全性；此外，通过 AUSF 网元认证可以兼容现有技术。进一步地，AMF 网元确定对终端进行第三方认证，还可以触发应用服务器对终端进行第三方认证，双重认证，大大提高网络的安全性。另外，图 4 提供的方案还可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

图 5 提供了另一种通信方法流程示意图，如图 5 所示，该实施例中以移动性管理网元为 AMF 网元，以请求消息为注册请求为例进行介绍，移动性管理网元通过 NEF 网元与应用服务器交互。该方法包括：

步骤 501，终端向 AMF 网元发送注册请求。

其中，注册请求中可以包括用于指示对终端进行第三方认证的指示信息。

步骤 502，AMF 网元根据注册请求中的指示信息确定对终端进行第三方认证。

可替换地，步骤 501 中注册请求可以包括用户标识，或终端的标识，或应用标识，相应地，步骤 502 可以替换为图 2 所示实施例中步骤 202 中与注册请求相应的实现方式来确定对终端进行第三方认证，不再赘述。

步骤 503，AMF 网元对终端进行注册，向终端发送注册接受。

可选地，步骤 503 的注册过程与现有技术中的对终端进行注册的过程相比，并未包含对终端的本地认证的进程。注册接受即为请求消息对应的响应消息，该注册接受可以包括用于指示终端通过控制面发送信息的指示信息（Control Plane Only Indicator），该指示信息可以用于指示终端使用控制面传输信息，例如，消息或数据。

步骤 504，终端通过控制面向 AMF 网元发送用户标识。

示例性的，终端可以通过控制面发送携带用户标识的消息，例如，非接入层（Non-access Stratum，NAS）消息（message）。

需要指出的是，步骤 504 为可选步骤，当请求消息中包括用户标识时，可以不执行步骤 504，步骤 505 中的用户标识为请求消息中包括用户标识。

步骤 505，AMF 网元向 NEF 网元发送用户标识。

步骤 505 可以借鉴上述步骤 303 中的相关描述。

步骤 506，NEF 网元向应用服务器发送用户标识。

步骤 507，应用服务器对用户标识对应的终端进行第三方认证。

具体地，应用服务器可以基于应用容器对该终端进行第三方认证，应用服务器可以通过下面两种方式获得该应用容器。

一种可选地实施方式中，在步骤 504 中终端通过控制面向 AMF 网元发送应用容器，从而通过 NEF 网元发送至应用服务器；另一种可选地实施方式中，在步骤 506 之后，应用服务器从终端获取应用容器。

步骤 508，应用服务器向 NEF 网元发送认证结果。

步骤 508 可以借鉴上述步骤 306。

步骤 509，NEF 网元向 AMF 网元发送认证结果。

步骤 509 可以借鉴上述步骤 307。

步骤 510，当认证结果为认证成功时，AMF 网元向终端发送响应。

其中，在步骤 510 中的响应可以为终端通过控制面发送信息的消息对应的响应。

图 5 所提供的方案中，AMF 网元确定对终端进行第三方认证，并触发应用服务器对终端进行第三方认证，解决背景技术中提到的无安全凭证的终端的认证问题，提高了网络的安全性；此外，AMF 网元指示终端通过控制面发送信息，可以避免终端发送信息失败的情况。另外，图 5 提供的方案还可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

图 6 提供了另一种通信方法流程示意图，如图 6 所示，该实施例中以移动性管理网元为 AMF 网元，以请求消息为注册请求为例进行介绍。该方法包括:

步骤 601，终端向 AMF 网元发送注册请求。

其中，注册请求中可以包括用于指示对终端进行第三方认证的指示信息。

步骤 602，AMF 网元根据注册请求中的指示信息确定对终端进行第三方认证。

可替换地，步骤 601 中注册请求可以包括用户标识，或终端的标识，或应用标识，相应地，步骤 602 可以替换为图 2 所示实施例中步骤 202 中与注册请求相应的实现方式来确定对终端进行第三方认证，不再赘述。

步骤 603，AMF 网元对终端进行注册，并向终端发送注册接受。

可选地，步骤 603 可以借鉴上述步骤 503。

步骤 604，终端向 AMF 网元发送用户标识。

可选地，用户标识携带在 NAS 消息中，例如，NAS 消息携带有 PDU 会话建立请求（PDU session establishment request），该 PDU 会话建立请求携带有用户标识。再例如，NAS 消息携带有 PDU 会话建立请求和用户标识。

具体来说，该 NAS 消息中还可以包括：会话管理-网络切片选择辅助信息（session management-network slice selection assistance information，S-NSSAI），PDU 会话标识（PDU session ID）和 N1 SM container 中的任一项或任多项。其中，PDU 会话建立请求也可以携带在 N1 SM container 中。

需要指出的是，步骤 604 为可选步骤，当请求消息中包括用户标识时，可以不执行步

骤 604，步骤 605 中的用户标识为请求消息中包括用户标识。

步骤 605，AMF 网元向 SMF 网元发送用户标识和用于指示对终端进行第三方认证的指示信息。

其中，用户标识和用于指示对终端进行第三方认证的指示信息可以携带在 PDU 会话建立请求中，也可以不携带在 PDU 会话建立请求中。

在上述步骤 605 中，AMF 网元还可以将终端的标识，数据网络名（data network name，DNN）和 PDU session ID 中的任一项或任多项随同 PDU 会话建立请求一起发送给 SMF 网元。

其中，步骤 604 还可以包括：终端向 AMF 网元发送应用容器，那么，步骤 605 中还可以包括 AMF 网元向 SMF 网元应用容器。

其中，应用容器可以携带在 NAS 消息中，例如，NAS 消息携带有 PDU 会话建立请求（PDU session establishment request），该 PDU 会话建立请求携带有应用容器。再例如，NAS 消息携带有 PDU 会话建立请求和应用容器。

步骤 606，SMF 网元向 NEF 网元发送用户标识。

步骤 606 可以借鉴上述步骤 303 中 AMF 网元向 NEF 网元发送用户标识的相关描述。

步骤 607，NEF 网元向应用服务器发送该用户标识。

步骤 608，应用服务器对用户标识对应的终端进行第三方认证。

具体地，应用服务器可以基于应用容器对该终端进行第三方认证，应用服务器可以通过下面两种方式获得该应用容器。

一种可选地实施方式中，在步骤 604 中终端向 AMF 网元发送应用容器，从而通过 NEF 网元发送至应用服务器；另一种可选地实施方式中，在步骤 607 之后，应用服务器从终端获取应用容器。

步骤 609，应用服务器向 NEF 网元发送认证结果。

步骤 609 可以借鉴上述步骤 306。

步骤 610，NEF 网元向 SMF 网元发送认证结果。

步骤 610 可以借鉴上述步骤 307。在步骤 610 之后可以进行 PDU 会话建立的其它进程。

图 6 所示的方法中，AMF 网元确定对终端进行第三方认证，并通过终端，SMF 网元等触发应用服务器对终端进行第三方认证，解决背景技术中提到的无安全凭证的终端的认证问题，提高了网络的安全性；此外，可以在 PDU 会话建立请求中进行终端的第三方认证，可以更好的兼容现有技术。另外，图 6 提供的方案还可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

图 7 提供了另一种通信方法流程示意图，如图 7 所示，该实施例中以移动性管理网元为 AMF 网元，以请求消息为注册请求为例进行介绍。该实施例中，应用服务器可以是数据网络（data network，DN）。该方法包括：

先执行上述图 6 中的步骤 601 至步骤 605，并在步骤 605 之后执行步骤 706。

步骤 706，SMF 网元将用户标识发送给 UPF 网元。

示例性的，SMF 网元可以向 UPF 网元发送认证/授权请求（authentication/authorization request），其中包括用户标识。

步骤 707，UPF 网元将用户标识发送给 DN。

示例性的，UPF 网元可以根据认证/授权请求的目的地址信息将数据传输消息路由至DN，其中，可选的，目的地址信息为 DN 设备的 IP 地址信息。

步骤 708，DN 对用户标识对应的终端进行第三方认证。

可选地，DN 对用户标识对应的终端进行第三方认证的方式可以参见上述第一种实施场景下应用服务器进行第三方认证的方式，在此不再赘述。

步骤 709，DN 通过 UPF 网元向 SMF 网元发送认证结果。

示例性的，DN 可以通过 UPF 网元向 SMF 网元发送认证/授权响应（authentication/authorization response），其中包括认证结果，认证结果包括认证成功或认证失败。在步骤 709 之后可以进行 PDU 会话建立的其它进程。

图 7 所示的方法中，AMF 网元确定对终端进行第三方认证，并触发 DN 对终端进行第三方认证，解决了背景技术中提到的无安全凭证的终端的认证问题，提高了网络的安全性；此外，可以在 PDU 会话建立请求中进行终端的第三方认证，可以更好的兼容现有技术。另外，图 7 提供的方案还可以解决终端由于停机等原因不能进行本地认证的场景下的认证问题等场景下无法接入网络的问题。

基于上述内容，本申请实施例还提供一种通信方法，图 8 提供了另一种通信方法的流程示意图，如图 8 所示，该方法包括:

步骤 801，SMF 网元向 PCF 网元发送 PCC 策略建立请求消息。

在步骤 801 中，PCC 策略建立请求消息也可以称为 PCF 提供的会话管理策略控制的获取请求（Npcf_SMPolicyControl_Get request）。

相应地，PCF 网元接收 SMF 网元发送的 PCC 策略建立请求消息。

其中，PCC 策略建立请求消息可以包括用户标识。

可选地，PCC 策略建立请求中还包括终端的标识，PDU 会话标识，DNN，终端的用户永久标识(subscriber permanent identifier，SUPI)，应用标识和用于指示对终端进行第三方认证的指示信息中的任一项或任多项等。

步骤 802，PCF 网元根据用户标识，获得用户标识对应的 PCC 策略。

示例性地，PCF 网元可以预先存储用户标识和 PCC 策略的对应关系，PCF 网元根据该对应关系，获得该用户标识对应的 PCC 策略；或者，PCF 网元可以预先存储应用标识和 PCC 策略的对应关系，PCF 网元可以根据该用户标识，获得其对应的应用标识，再根据该对应关系，获得该应用标识对应的 PCC 策略，并将该策略作为该用户标识对应的 PCC 策略。

在一种示例中，PCC 策略可以由应用服务器预先部署在 PCF 网元上。

具体来说，应用服务器可以为一个应用部署一套 PCC 策略，也可以为一个应用部署多套 PCC 策略，其中，一个应用对应的多个用户标识可以对应同一个 PCC 策略，也可以对应不同的 PCC 测量。如此，可以根据应用的特性，制定每个应用专属的 PCC 策略，也可以根据用户等级，为每个用户制定专属的 PCC 策略。

在另一种示例中，PCC 策略也可以由 PCF 网元基于用户标识对应的 PCC 规则信息生成。其中，用户标识对应的 PCC 规则信息中，上述用于生成 PCC 规则的信息中可以包括收费信息，该收费信息中可以包括用于指示应用服务器愿意为终端提供费用赞助（sponsor token）的指示信息。可选地，收费信息中还包括愿意为终端提供的赞助费用的额度。如此，

提供了一种新的计费模式，简化了数据交换方式，可以为应用服务器负责签约和管理终端奠定基础。

其中，PCC 策略可以包括业务质量（Quality of Service，QoS）参数（parameters）。应用服务器预先部署的 PCC 策略中也可以不包括 QoS 参数，这种情况下，PCF 网元可以获取用户标识对应的 QoS 参数，比如从应用服务器请求到用户标识对应的 QoS 参数。

其中，QoS 参数可以包括 5G QoS 标识（5G QoS identifier，5QI），分配和保留优先级（allocation and retention priority，ARP），受保障流比特率（Guaranteed Flow Bit Rate，GFBR），或最大流比特率（Maximum Flow Bit Rate，MFBR），等。

步骤 803，PCF 网元向 SMF 网元发送 PCC 策略。

相对应地，SMF 网元接收来自 PCF 网元的用户标识对应的 PCC 策略。

举个例子，比如，PCC 策略中可以只允许终端传输应用标识所对应的数据。再比如，PCC 策略中规定采用特殊的计费，应用按用户量或集团用户模式付费，这种场景下不需要 SMF 网元/UPF 网元统计终端使用的数据流量。

图 8 所提供的方法中，可以生成应用级别的粒度或用户级别的粒度的 PCC 策略，可以提高 PCC 策略的灵活性。

需要注意的是，前述的实施例中也可以采用上述步骤 802 中的方案，相类似的，上述图 3 至图 7 中也还可以包括 PCF 网元接收到收费信息，可以在上述图 3 的步骤 306 中由应用服务器向 NEF 发送收费信息，之后由 NEF 网元将收费信息发送给 PCF 网元，或者在上述图 4 的步骤 408 中由应用服务器向 NEF 发送收费信息，之后由 NEF 网元将收费信息发送给 PCF 网元，或者在上述图 5 的步骤 508 中由应用服务器向 NEF 发送收费信息，之后由 NEF 网元将收费信息发送给 PCF 网元，或者在上述图 6 的步骤 609 中由应用服务器向 NEF 发送收费信息，之后由 NEF 网元将收费信息发送给 PCF 网元。可选地，若是应用到图 7 的场景下，则 DN 可以在上述图 7 的步骤 709 中将收费信息发送给 UPF 网元，之后由 UPF 网元向 PCF 网元发送收费信息。

需要注意的是，前述的实施例中也可以采用上述步骤 801 至步骤 803 中的方案，相类似的，上述步骤 801 至步骤 803 可以发生在终端发起 PDU 会话建立请求之后，比如在图 3 的步骤 308 之后、在图 4 的步骤 411 之后和图 5 的步骤 501 之后，终端可以发起 PDU 会话建立进程，在 PDU 会话建立进程发起之后，SMF 网元可以执行上述步骤 801，向 PCF 网元发送 PCC 策略建立请求消息，之后执行步骤 802 和步骤 803。可选地，若是应用到图 6 和图 7 的场景下，上述步骤 801 至步骤 803 还可以发生在图 6 的步骤 610 之后，或图 7 的步骤 709 之后。

在前述图 2 至图 8 所示的任意实施例中，可选地，当应用服务器对终端进行第三方认证成功之后，应用服务器可以向 SMF 网元发送根密钥，相对应地，SMF 网元接收应用服务器发送的根密钥，SMF 网元根据根密钥与终端进行密钥协商。可选地，该根密钥可以用于进一步生成密钥，用于终端和 SMF 网元/UPF 网元之间的安全保护，从而可以提高控制面信令/用户面数据的安全性，其中，“/”可以表示和/或的意思。

示例性的，前述的实施例中采用上述方案时，可以在上述图 3 的步骤 306 中由应用服务器向 NEF 发送根密钥，之后由 NEF 网元将根密钥发送给 SMF 网元，或者在上述图 4 的步骤 408 中由应用服务器向 NEF 发送根密钥，之后由 NEF 网元将根密钥发送给 SMF 网元，

或者在上述图 5 的步骤 508 中由应用服务器向 NEF 发送根密钥，之后由 NEF 网元将根密钥发送给 SMF 网元，或者在上述图 6 的步骤 609 中由应用服务器向 NEF 发送根密钥，之后由 NEF 网元将根密钥发送给 SMF 网元。可选地，若是应用到图 7 的场景下，则 DN 可以在上述图 7 的步骤 709 中将根密钥发送给 UPF 网元，之后由 UPF 网元向 SMF 网元发送根密钥。

基于上述内容和相同构思，本申请提供一种通信装置，用于执行上述图 2 至图 8 所示方法中的移动性管理网元侧的任一个方案。图 9 提供了一种通信装置的结构示意图，如图 9 所示，通信装置 901 包括处理器 903、发送器 902、接收器 907、存储器 905 和通信接口 904；其中，处理器 903、发送器 902、接收器 907、存储器 905 和通信接口 904 通过总线 906 相互连接。可选地，收发器可以包括发送器 902 和接收器 907。该实施例中的通信装置 901 可以是上述内容中的移动性管理网元、MME 网元或 AMF 网元。

可选地，存储器 905 还可以用于存储程序指令，处理器 903 调用该存储器 905 中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选地实施方式，使得通信装置 901 实现上述方法中移动性管理网元的功能。

处理器 903 用于根据执行存储器存储的指令，并控制发送器 902 进行信号的发送，以及控制接收器 907 进行信号接收，当处理器 903 执行存储器存储的指令时，通信装置 901 中的接收器 907，用于接收来自终端的请求消息，请求消息用于请求接入网络；处理器 903，用于当根据请求消息确定对终端进行第三方认证时，触发第三方认证。

在一种可选地设计中，处理器 903，用于：当请求消息中包括用于指示对终端进行第三方认证的指示信息时，确定对终端进行第三方认证；或者，当请求消息中包括应用标识时，确定对终端进行第三方认证；或者，当请求消息中包括终端的标识，且与终端的标识对应的认证方式为对终端进行第三方认证时，确定对终端进行第三方认证。

在一种可选地设计中，请求消息还包括用户标识；或者；请求消息还包括用户标识和应用容器，应用容器用于应用服务器对终端进行第三方认证。

在一种可选地设计中，发送器 902，还用于：根据请求消息向终端发送响应消息，响应消息包括用于指示终端通过控制面发送信息的指示信息；接收器 907，还用于：通过控制面接收用户标识。

在一种可选地设计中，接收器 907，还用于：通过控制面接收应用容器，应用容器用于应用服务器对终端进行第三方认证。

在一种可选地设计中，处理器 903，用于：当请求消息中包括用户标识时，确定对终端进行第三方认证。

在一种可选地设计中，请求消息还包括应用容器，应用容器用于应用服务器对终端进行第三方认证。

在一种可选地设计中，发送器 902，用于：通过认证服务器功能 AUSF 网元或网络开放功能 NEF 网元向应用服务器发送用户标识。

基于上述内容和相同构思，本申请提供一种通信装置，用于执行上述图 2 至图 8 所示方法中的终端侧的任一个方案。图 10 提供了另一种通信装置的结构示意图，如图 10 所示，通信装置 1001 包括处理器 1003、发送器 1002、接收器 1007、存储器 1005 和通信接口 1004；其中，处理器 1003、发送器 1002、接收器 1007、存储器 1005 和通信接口 1004 通过总线

1006 相互连接。可选地，收发器可以包括发送器 1002 和接收器 1007。

可选地，存储器 1005 还可以用于存储程序指令，处理器 1003 调用该存储器 1005 中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选地实施方式，使得通信装置 1001 实现上述方法中终端的功能。

处理器 1003 用于根据执行存储器存储的指令，并控制发送器 1002 进行信号的发送，以及控制接收器 1007 进行信号接收，当处理器 1003 执行存储器存储的指令时，通信装置 1001 中的发送器 1002，用于向移动性管理网元发送请求消息，请求消息中包括认证参考信息，认证参考信息用于移动性管理网元确定是否对终端进行第三方认证；接收器 1007，用于接收来自移动性管理网元对请求消息的响应消息。

在一种可选地设计中，认证参考信息包括：用于指示对终端进行第三方认证的指示信息或应用标识。在一种可选地设计中，请求消息还包括用户标识。在一种可选地设计中，认证参考信息包括：用户标识。在一种可选地设计中，请求消息还包括应用容器，应用容器用于应用服务器对终端进行第三方认证。

在一种可选地设计中，响应消息包括用于指示终端通过控制面发送信息的指示信息，发送器 1002，还用于：通过控制面向移动性管理网元发送用户标识。

在一种可选地设计中，发送器 1002，还用于：通过控制面向移动性管理网元发送应用容器；其中，应用容器用于应用服务器对终端进行第三方认证。

基于上述内容和相同构思，本申请提供一种通信装置，用于执行上述图 2 至图 8 所示方法中的 AUSF 网元侧的任一个方案。图 11 提供了另一种通信装置的结构示意图，如图 11 所示，通信装置 1101 包括处理器 1103、发送器 1102、接收器 1107、存储器 1105 和通信接口 1104；其中，处理器 1103、发送器 1102、接收器 1107、存储器 1105 和通信接口 1104 通过总线 1106 相互连接。可选地，收发器可以包括发送器 1102 和接收器 1107。

可选地，存储器 1105 还可以用于存储程序指令，处理器 1103 调用该存储器 1105 中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选地实施方式，使得通信装置 1101 实现上述方法中 AUSF 网元的功能。

处理器 1103 用于根据执行存储器存储的指令，并控制发送器 1102 进行信号的发送，以及控制接收器 1107 进行信号接收，当处理器 1103 执行存储器存储的指令时，通信装置 1101 中的接收器 1107，用于接收来自移动性管理网元的用户标识，接收来自应用服务器的认证参数；处理器 1103，用于向应用服务器请求用户标识对应的认证参数。

在一种可选地设计中，发送器 1102，还用于：向应用服务器发送应用容器，应用容器用于应用服务器对终端进行第三方认证。

在一种可选地设计中，处理器 1103，还用于：根据认证参数对终端进行认证。

基于上述内容和相同构思，本申请提供一种通信装置，用于执行上述图 2 至图 8 所示方法中的 PCF 网元侧的任一个方案。图 12 提供了另一种通信装置的结构示意图，如图 12 所示，通信装置 1201 包括处理器 1203、发送器 1202、接收器 1207、存储器 1205 和通信接口 1204；其中，处理器 1203、发送器 1202、接收器 1207、存储器 1205 和通信接口 1204 通过总线 1206 相互连接。可选地，收发器可以包括发送器 1202 和接收器 1207。

可选地，存储器 1205 还可以用于存储程序指令，处理器 1203 调用该存储器 1205 中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选地实施方式，使得通信装置 1201 实现上述方法中 PCF 网元的功能。

处理器 1203 用于根据执行存储器存储的指令，并控制发送器 1202 进行信号的发送，以及控制接收器 1207 进行信号接收，当处理器 1203 执行存储器存储的指令时，通信装置 1201 中的接收器 1207 用于接收 SMF 网元发送的 PCC 策略建立请求消息，PCC 策略建立请求消息包括用户标识；处理器 1203 用于根据预设 PCC 策略，获得用户标识对应的 PCC 策略；发送器 1202 用于向 SMF 网元发送 PCC 策略。如此，可以获得更细粒度的 PCC 策略，提高了 PCC 策略的灵活性。

在一种可选地实施方式中，PCC 策略建立请求消息中还包括应用标识。可选地，处理器 1203 用于根据预设 PCC 策略，获得与用户标识以及应用标识对应的 PCC 策略。在一种可选地实施方式中，预设 PCC 策略中至少存在两个第一 PCC 策略，两个第一 PCC 策略对应两个不同的应用标识；当应用标识对应的至少两个 PCC 策略时，至少两个 PCC 策略中至少存在两个第二 PCC 策略，两个第二 PCC 策略对应两个不同的用户标识。如此，可以将 PCC 策略制定为应用级别的粒度或用户级别的粒度，比如为不同的应用设置不同的 PCC 策略，或者为同一个应用对应的不同的用户设置不同的 PCC 策略，提高了 PCC 策略设置的灵活性。

在一种可选地实施方式中，预设 PCC 策略还包括收费信息。如此，可以为应用服务器为终端提供付费服务，或者为用户制定个性化收费标准奠定基础。

基于上述内容和相同构思，本申请提供一种通信装置，用于执行上述图 2 至图 8 所示方法中的 SMF 网元侧的任一个方案。图 13 提供了另一种通信装置的结构示意图，如图 13 所示，通信装置 1301 包括处理器 1303、发送器 1302、接收器 1307、存储器 1305 和通信接口 1304；其中，处理器 1303、发送器 1302、接收器 1307、存储器 1305 和通信接口 1304 通过总线 1306 相互连接。可选地，收发器可以包括发送器 1302 和接收器 1307。

可选地，存储器 1305 还可以用于存储程序指令，处理器 1303 调用该存储器 1305 中存储的程序指令，可以执行上述方案中所示实施例中的一个或多个步骤，或其中可选地实施方式，使得通信装置 1301 实现上述方法中 SMF 网元的功能。

处理器 1303 用于根据执行存储器存储的指令，并控制发送器 1302 进行信号的发送，以及控制接收器 1307 进行信号接收，当处理器 1303 执行存储器存储的指令时，通信装置 1301 中的发送器 1302 用于向 PCF 网元发送 PCC 策略建立请求消息，PCC 策略建立请求消息包括用户标识；接收器 1307 用于接收来自 PCF 网元的用户标识对应的 PCC 策略。在一种可选地实施方式中，PCC 策略建立请求消息中还包括应用标识。如此，可以获得更细粒度的 PCC 策略，比如可以将 PCC 策略制定为应用级别的粒度或用户级别的粒度，举个例子，为不同的应用设置不同的 PCC 策略，或者为同一个应用对应的不同的用户设置不同的 PCC 策略，可见，该方法可提高 PCC 策略设置的灵活性。

在一种可选地实施方式中，接收器 1307 还用于接收应用服务器发送的根密钥；SMF 网元根据根密钥与终端进行密钥协商。如此，在终端未进行本地认证的情况下，应用服务器可以为 SMF 网元分配根密钥，以便实现 SMF 网元与终端之间的安全保护。

在上述图 9、图 10、图 11、图 12 和图 13 中，总线 906、总线 1006、总线 1106、总线 1206 和总线 1306 中的任一个总线可以是外设部件互连标准（peripheral component interconnect，PCI）总线或扩展工业标准结构（extended industry standard architecture，EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 9、图 10、图 11、图 12 和图 13 中均仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

在上述图 9、图 10、图 11、图 12 和图 13 中，存储器 905、存储器 1005、存储器 1105、存储器 1205 和存储器 1305 中的任一个存储器可以包括易失性存储器（volatile memory），例如随机存取存储器（random-access memory，RAM）；存储器也可以包括非易失性存储器（non-volatile memory），例如快闪存储器（flash memory），硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）；存储器还可以包括上述种类的存储器的组合。

在上述图 9、图 10、图 11、图 12 和图 13 中，通信接口 904、通信接口 1004、通信接口 1104、通信接口 1204 和通信接口 1304 中的任一个通信接口可以为有线通信接入口，无线通信接口或其组合，其中，有线通信接口例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线通信接口可以为 WLAN 接口。

在上述图 9、图 10、图 11、图 12 和图 13 中，处理器 903、处理器 1003、处理器 1103、处理器 1203、处理器 1303 中的任一个处理器可以是中央处理器（central processing unit，CPU），网络处理器（network processor，NP）或者 CPU 和 NP 的组合。处理器还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路（application-specific integrated circuit，ASIC），可编程逻辑器件（programmable logic device，PLD）或其组合。上述 PLD 可以是复杂可编程逻辑器件（complex programmable logic device，CPLD），现场可编程逻辑门阵列（field-programmable gate array，FPGA），通用阵列逻辑（generic array logic, GAL）或其任意组合。

基于相同构思，本申请实施例提供一种通信装置，用于执行上述方法流程中的移动性管理网元侧的任一个方案。图 14 提供了另一种通信装置的结构示意图，如图 14 所示，通信装置 1401 包括发送单元 1402、处理单元 1403 和接收单元 1404。该实施例中的通信装置 1401 可以是上述的移动性管理网元，AMF 网元，或 MME，可以执行上述图 2 至图 8 对应的方案。

接收单元 1404，用于接收来自终端的请求消息，请求消息用于请求接入网络；处理单元 1403，用于当根据请求消息确定对终端进行第三方认证时，触发第三方认证。

应理解，以上网络设备的单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，图 14 中发送单元 1402 可以由上述图 9 的发送器 902 实现，图 14 中接收单元 1404 可以由上述图 9 的接收器 907 实现，图 14 中处理单元 1403 可以由上述图 9 的处理器 903 实现。也就是说，本申请实施例中发送单元 1402 可以执行上述图 9 的发送器 902 所执行的方案，本申请实施例中接收单元 1404 可以执行上述图 9 的接收器 907 所执行的方案，本申请实施例中处理单元 1403 可以执行上述图 9 的处理器 903 所执行的方案，其余内容可以参见上述内容，在此不再赘述。如上述图 9 所示，通信装置 901 包括的存储器 905 中可以用于存储该通信装置 901 包括的处理器 903 执行方案时的代码，该代码可为通信装置 901 出厂时预装的程序/代码。

基于相同构思，本申请实施例提供一种通信装置，用于执行上述方法流程中的终端侧的任一个方案。图 15 提供了另一种通信装置的结构示意图，如图 15 所示，通信装置 1501 包括发送单元 1502、处理单元 1503 和接收单元 1504。该实施例中的通信装置 1501 可以执行上述图 2 至图 8 对应的方案。

发送单元 1502，用于向移动性管理网元发送请求消息，请求消息中包括认证参考信息，认证参考信息用于移动性管理网元确定是否对终端进行第三方认证；接收单元 1504，用于

接收来自移动性管理网元对请求消息的响应消息。

应理解，以上网络设备的单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，图 15 中发送单元 1502 可以由上述图 10 的发送器 1002 实现，图 15 中接收单元 1504 可以由上述图 10 的接收器 1007 实现，图 15 中处理单元 1503 可以由上述图 10 的处理器 1003 实现。也就是说，本申请实施例中发送单元 1502 可以执行上述图 10 的发送器 1002 所执行的方案，本申请实施例中接收单元 1504 可以执行上述图 10 的接收器 1007 所执行的方案，本申请实施例中处理单元 1503 可以执行上述图 10 的处理器 1003 所执行的方案，其余内容可以参见上述内容，在此不再赘述。如上述图 10 所示，通信装置 1001 包括的存储器 1005 中可以用于存储该通信装置 1001 包括的处理器 1003 执行方案时的代码，该代码可为通信装置 1001 出厂时预装的程序/代码。

基于相同构思，本申请实施例提供一种通信装置，用于执行上述方法流程中的 AUSF 网元侧的任一个方案。图 16 提供了另一种通信装置的结构示意图，如图 16 所示，通信装置 1601 包括发送单元 1602、处理单元 1603 和接收单元 1604。该实施例中的通信装置 1601 可以执行上述图 2 至图 8 对应的方案。

接收单元 1604，用于接收来自移动性管理网元的用户标识，接收来自应用服务单元的认证参数；处理单元 1603，用于向应用服务单元请求用户标识对应的认证参数。

应理解，以上网络设备的单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，图 16 中发送单元 1602 可以由上述图 11 的发送器 1102 实现，图 16 中接收单元 1604 可以由上述图 11 的接收器 1107 实现，图 16 中处理单元 1603 可以由上述图 11 的处理器 1103 实现。也就是说，本申请实施例中发送单元 1602 可以执行上述图 11 的发送器 1102 所执行的方案，本申请实施例中接收单元 1604 可以执行上述图 11 的接收器 1107 所执行的方案，本申请实施例中处理单元 1603 可以执行上述图 11 的处理器 1103 所执行的方案，其余内容可以参见上述内容，在此不再赘述。如上述图 11 所示，通信装置 1101 包括的存储器 1105 中可以用于存储该通信装置 1101 包括的处理器 1103 执行方案时的代码，该代码可为通信装置 1101 出厂时预装的程序/代码。

基于相同构思，本申请实施例提供一种通信装置，用于执行上述方法流程中的 PCF 网元侧的任一个方案。图 17 提供了另一种通信装置的结构示意图，如图 17 所示，通信装置 1701 包括发送单元 1702、处理单元 1703 和接收单元 1704。该实施例中的通信装置 1701 可以执行上述图 2 至图 8 对应的方案。

接收单元 1704 用于接收 SMF 网元发送的 PCC 策略建立请求消息，PCC 策略建立请求消息包括用户标识；处理单元 1703 用于根据预设 PCC 策略，获得用户标识对应的 PCC 策略；发送单元 1702 用于向 SMF 网元发送 PCC 策略。

应理解，以上网络设备的单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，图 17 中发送单元 1702 可以由上述图 12 的发送器 1202 实现，图 17 中接收单元 1704 可以由上述图 12 的接收器 1207 实现，图 17 中处理单元 1703 可以由上述图 12 的处理器 1203 实现。也就是说，本申请实施例中发送单元 1702 可以执行上述图 12 的发送器 1202 所执行的方案，本申请实施例中接收单元 1704 可以执行上述图 12 的接收器 1207 所执行的方案，本申请实

施例中处理单元 1703 可以执行上述图 12 的处理器 1203 所执行的方案，其余内容可以参见上述内容，在此不再赘述。如上述图 12 所示，通信装置 1201 包括的存储器 1205 中可以用于存储该通信装置 1201 包括的处理器 1203 执行方案时的代码，该代码可为通信装置 1201 出厂时预装的程序/代码。

基于相同构思，本申请实施例提供一种通信装置，用于执行上述方法流程中的 SMF 网元侧的任一个方案。图 18 提供了另一种通信装置的结构示意图，如图 18 所示，通信装置 1801 包括发送单元 1802、处理单元 1803 和接收单元 1804。该实施例中的通信装置 1801 可以执行上述图 2 至图 8 对应的方案。

发送单元 1802 用于向 PCF 网元发送 PCC 策略建立请求消息，PCC 策略建立请求消息包括用户标识；接收单元 1804 用于接收来自 PCF 网元的用户标识对应的 PCC 策略。

应理解，以上网络设备的单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。本申请实施例中，图 18 中发送单元 1802 可以由上述图 13 的发送器 1302 实现，图 18 中接收单元 1804 可以由上述图 13 的接收器 1307 实现，图 18 中处理单元 1803 可以由上述图 13 的处理器 1303 实现。也就是说，本申请实施例中发送单元 1802 可以执行上述图 13 的发送器 1302 所执行的方案，本申请实施例中接收单元 1804 可以执行上述图 13 的接收器 1307 所执行的方案，本申请实施例中处理单元 1803 可以执行上述图 13 的处理器 1303 所执行的方案，其余内容可以参见上述内容，在此不再赘述。如上述图 13 所示，通信装置 1301 包括的存储器 1305 中可以用于存储该通信装置 1301 包括的处理器 1303 执行方案时的代码，该代码可为通信装置 1301 出厂时预装的程序/代码。

基于相同构思，本申请实施例提供一种通信系统，用于执行上述方法流程中的方案。图 19 示例性示出了本申请实施例提供的一种通信系统的结构示意图，如图 19 所示，该通信系统 1900 可以包括移动性管理网元 1901 和终端 1902。可选地，该通信系统还可以包括 AUSF 网元 1903、PCF 网元 1904 和 SMF 网元 1905 中的任一个或任多个，分别用于实现以上图 2 至图 8 的方法中相应的步骤。

终端 1902，用于向移动性管理网元 1901 发送请求消息，所述请求消息中包括认证参考信息，所述认证参考信息用于所述移动性管理网元确定是否对所述终端进行第三方认证；所述终端接收来自所述移动性管理网元对所述请求消息的响应消息。移动性管理网元 1901 接收来自终端 1902 的请求消息，所述请求消息用于请求接入网络；当所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证时，所述移动性管理网元触发第三方认证。

应理解，该通信系统 1900 中的移动性管理网元 1901 可以执行上述图 14 的通信装置 1401 所执行的方案，也可以执行上述图 9 的通信装置 901 所执行的方案，可选地，也可以是上述图 1 中的 AMF 网元，也可以是 MME 网元。该通信系统 1900 中的移动性管理网元 1901 可以执行上述图 14 的通信装置 1401 所执行的方案，也可以执行上述图 9 的通信装置 901 所执行的方案，可选地，也可以是上述图 1 中的 AMF 网元，也可以是 MME 网元。该通信系统 1900 中的终端 1902 可以执行上述图 15 的通信装置 1501 所执行的方案，也可以执行上述图 10 的通信装置 1001 所执行的方案，可选地，也可以是上述图 1 中的终端。该通信系统 1900 中的 AUSF 网元 1903 可以执行上述图 16 的通信装置 1601 所执行的方案，也可以执行上述图 11 的通信装置 1101 行的方案，可选地，也可以是上述图 1 中的 AUSF

网元。该通信系统 1900 中的 PCF 网元 1904 可以执行上述图 17 的通信装置 1701 所执行的方案，也可以执行上述图 12 的通信装置 1201 所执行的方案，可选地，也可以是上述图 1 中的 PCF 网元。该通信系统 1900 中的 SMF 网元 1905 可以执行上述图 18 的通信装置 1801 所执行的方案，也可以执行上述图 13 的通信装置 1301 所执行的方案，可选地，也可以是上述图 1 中的 SMF 网元。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件程序实现时，可以全部或部分地以计算机程序产品的形式实现。计算机程序产品包括一个或多个指令。在计算机上加载和执行计算机程序指令时，全部或部分地产生按照本申请实施例的流程或功能。计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。指令可以存储在计算机存储介质中，或者从一个计算机存储介质向另一个计算机存储介质传输，例如，指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。计算机存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。可用介质可以是磁性介质，（例如，软盘、硬盘、磁带、磁光盘（MO）等）、光介质（例如，CD、DVD、BD、HVD 等）、或者半导体介质（例如 ROM、EPROM、EEPROM、非易失性存储器（NAND FLASH）、固态硬盘（Solid State Disk，SSD））等。

本领域内的技术人员应明白，本申请实施例可提供为方法、系统、或计算机程序产品。因此，本申请实施例可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请实施例是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求

1、一种通信方法，其特征在于，包括:

移动性管理网元接收来自终端的请求消息，所述请求消息用于请求接入网络;

当所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证时，所述移动性管理网元触发第三方认证。

2、如权利要求 1 所述的方法，其特征在于，所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证，包括:

当所述请求消息中包括用于指示对所述终端进行第三方认证的指示信息时，所述移动性管理网元确定对所述终端进行第三方认证; 或者，

当所述请求消息中包括应用标识时，所述移动性管理网元确定对所述终端进行第三方认证; 或者，

当所述请求消息中包括所述终端的标识，且与所述终端的标识对应的认证方式为对所述终端进行第三方认证时，所述移动性管理网元确定对所述终端进行第三方认证。

3、如权利要求 2 所述的方法，其特征在于，所述请求消息还包括用户标识; 或者;

所述请求消息还包括用户标识和应用容器，所述应用容器用于对所述终端进行第三方认证。

4、如权利要求 2 所述的方法，其特征在于，所述方法还包括:

所述移动性管理网元根据所述请求消息向所述终端发送响应消息，所述响应消息包括用于指示所述终端通过控制面发送信息的指示信息;

所述移动性管理网元通过控制面接收所述用户标识。

5、如权利要求 4 所述的方法，其特征在于，所述方法还包括:

所述移动性管理网元通过所述控制面接收应用容器，所述应用容器用于对所述终端进行第三方认证。

6、如权利要求 1 所述的方法，其特征在于，所述移动性管理网元根据所述请求消息确定对所述终端进行第三方认证，包括:

当所述请求消息中包括用户标识时，所述移动性管理网元确定对所述终端进行第三方认证。

7、如权利要求 6 所述的方法，其特征在于，所述请求消息还包括应用容器，所述应用容器用于对所述终端进行第三方认证。

8、一种通信方法，其特征在于，包括:

终端向移动性管理网元发送请求消息，所述请求消息中包括认证参考信息，所述认证参考信息用于所述移动性管理网元确定是否对所述终端进行第三方认证;

所述终端接收来自所述移动性管理网元对所述请求消息的响应消息。

9、如权利要求 8 所述的方法，其特征在于，所述认证参考信息包括: 用于指示对所述终端进行第三方认证的指示信息或应用标识。

10、如权利要求 9 所述的方法，其特征在于，所述请求消息还包括用户标识。

11、如权利要求 8 所述的方法，其特征在于，所述认证参考信息包括: 用户标识。

12、如权利要求 10 或 11 所述的方法，其特征在于，所述请求消息还包括应用容器，所述应用容器用于对所述终端进行第三方认证。

13、如权利要求 9 所述的方法，其特征在于，所述响应消息包括用于指示所述终端通过控制面发送信息的指示信息，所述方法还包括:

所述终端通过控制面向所述移动性管理网元发送所述用户标识。

14、一种通信方法，其特征在于，包括:

认证服务器功能 AUSF 网元接收来自移动性管理网元的用户标识;

所述 AUSF 网元向应用服务器请求所述用户标识对应的认证参数;

所述 AUSF 网元接收来自所述应用服务器的所述认证参数，所述认证参数用于对终端进行认证。

15、如权利要求 14 所述的方法，其特征在于，所述方法还包括:

所述 AUSF 网元向所述应用服务器发送应用容器，所述应用容器用于所述应用服务器对所述终端进行第三方认证。

16、一种通信装置，其特征在于，包括:

接收器，用于接收来自终端的请求消息，所述请求消息用于请求接入网络;

处理器，用于当根据所述请求消息确定对所述终端进行第三方认证时，触发第三方认证。

17、如权利要求 16 所述的通信装置，其特征在于，所述处理器还用于:

当所述请求消息中包括用于指示对所述终端进行第三方认证的指示信息时，确定对所述终端进行第三方认证; 或者，

当所述请求消息中包括应用标识时，确定对所述终端进行第三方认证; 或者，

当所述请求消息中包括所述终端的标识，且与所述终端的标识对应的认证方式为对所述终端进行第三方认证时，确定对所述终端进行第三方认证。

18、如权利要求 17 所述的通信装置，其特征在于，所述请求消息还包括用户标识; 或者;

所述请求消息还包括用户标识和应用容器，所述应用容器用于对所述终端进行第三方认证。

19、如权利要求 17 所述的通信装置，其特征在于，所述通信装置还包括发送器;

所述发送器，用于根据所述请求消息向所述终端发送响应消息，所述响应消息包括用于指示所述终端通过控制面发送信息的指示信息;

所述接收器，还用于通过控制面接收所述用户标识。

20、如权利要求 19 所述的通信装置，其特征在于，所述接收器还用于:

通过所述控制面接收应用容器，所述应用容器用于对所述终端进行第三方认证。

21、如权利要求 16 所述的通信装置，其特征在于，所述处理器还用于:

当所述请求消息中包括用户标识时，确定对所述终端进行第三方认证。

22、如权利要求 21 所述的通信装置，其特征在于，所述请求消息还包括应用容器，所述应用容器用于对所述终端进行第三方认证。

23、一种通信装置，其特征在于，包括:

发送器，用于向移动性管理网元发送请求消息，所述请求消息中包括认证参考信息，所述认证参考信息用于所述移动性管理网元确定是否对终端进行第三方认证;

接收器，用于接收来自所述移动性管理网元对所述请求消息的响应消息。

24、如权利要求 23 所述的通信装置，其特征在于，所述认证参考信息包括: 用于指

示对所述终端进行第三方认证的指示信息或应用标识。

25、如权利要求 24 所述的通信装置，其特征在于，所述请求消息还包括用户标识。

26、如权利要求 23 所述的通信装置，其特征在于，所述认证参考信息包括：用户标识。

27、如权利要求 25 或 26 所述的通信装置，其特征在于，所述请求消息还包括应用容器，所述应用容器用于对所述终端进行第三方认证。

28、如权利要求 24 所述的通信装置，其特征在于，所述响应消息包括用于指示所述终端通过控制面发送信息的指示信息，所述发送器，还用于：

通过控制面向所述移动性管理网元发送所述用户标识。

29、一种通信装置，其特征在于，包括：

接收器，用于接收来自移动性管理网元的用户标识；

处理器，用于向应用服务器请求所述用户标识对应的认证参数；

所述接收器，还用于接收来自所述应用服务器的认证参数，所述认证参数用于对终端进行认证。

30、如权利要求 29 所述的通信装置，其特征在于，所述发送器，还用于：

向所述应用服务器发送应用容器，所述应用容器用于所述应用服务器对所述终端进行第三方认证。

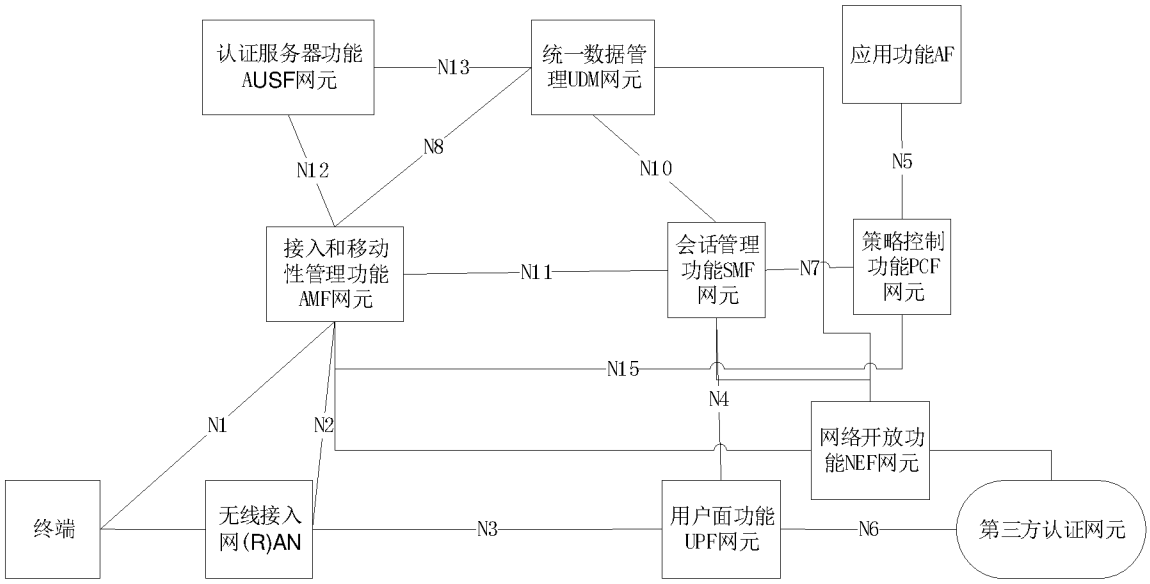
认证服务器功能AUSF网元
N13
统一数据管理UDM网元
应用功能AF
N12
N8
N10
N5
接入和移动性管理功能AMF网元
N11
会话管理功能SMF网元
N7
策略控制功能PCF网元
N15
N4
N1
N2
网络开放功能NEF网元
终端
无线接入网(R)AN
N3
用户面功能UPF网元
N6
第三方认证网元

图 1

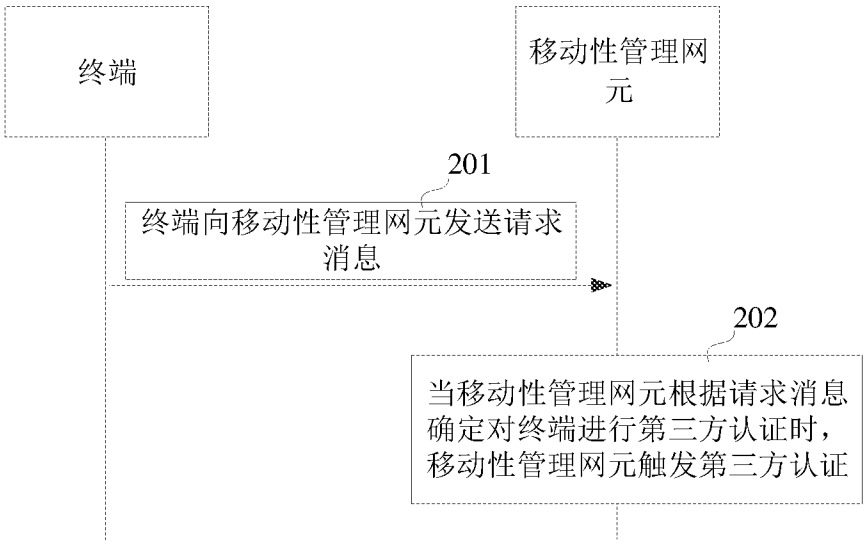
终端
移动性管理网元
201
终端向移动性管理网元发送请求消息
202
当移动性管理网元根据请求消息确定对终端进行第三方认证时，移动性管理网元触发第三方认证

图 2

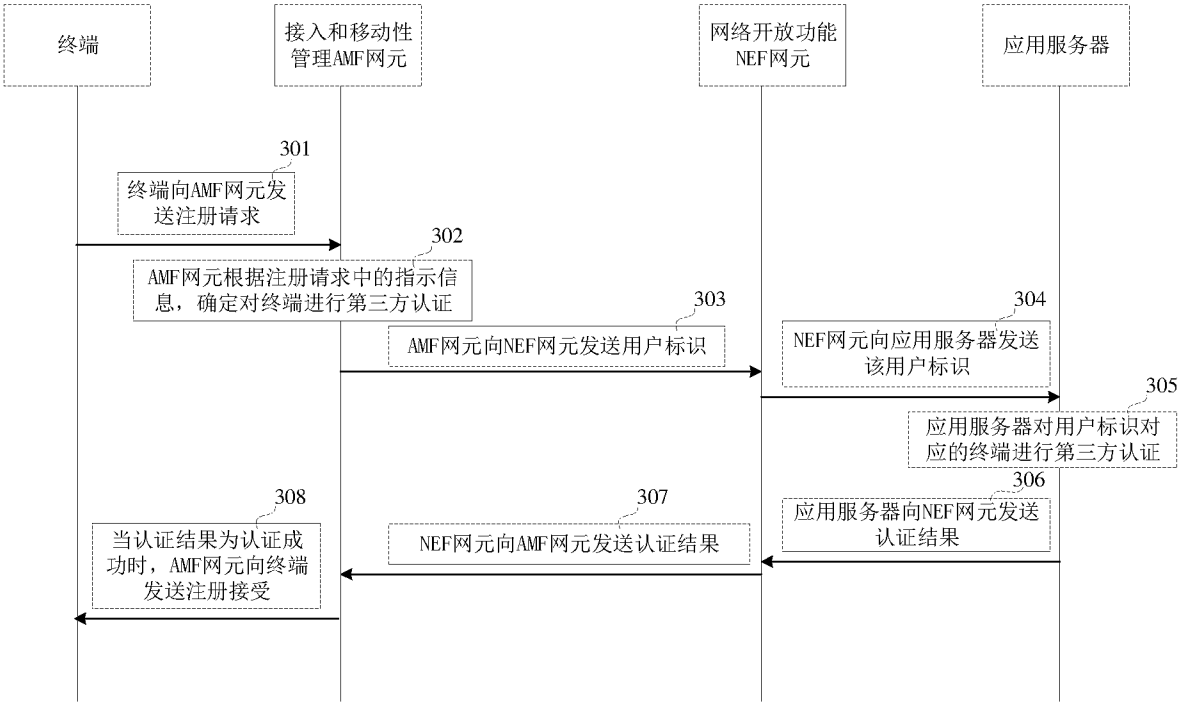
终端
接入和移动性管理AMF网元
网络开放功能NEF网元
应用服务器
301
终端向AMF网元发送注册请求
302
AMF网元根据注册请求中的指示信息，确定对终端进行第三方认证
303
AMF网元向NEF网元发送用户标识
304
NEF网元向应用服务器发送该用户标识
305
应用服务器对用户标识对应的终端进行第三方认证
306
应用服务器向NEF网元发送认证结果
307
NEF网元向AMF网元发送认证结果
308
当认证结果为认证成功时，AMF网元向终端发送注册接受

图 3

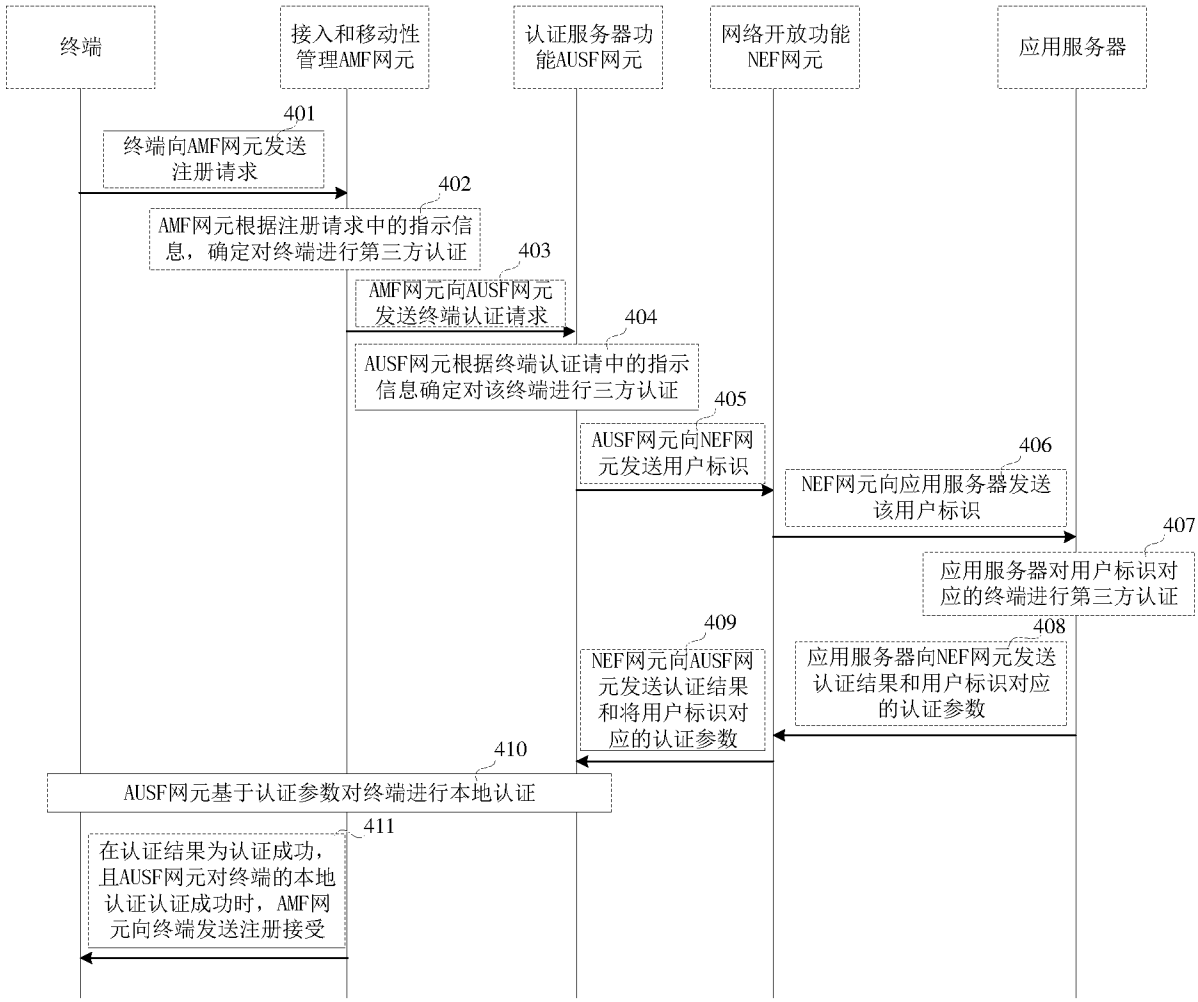
终端
接入和移动性管理AMF网元
认证服务器功能AUSF网元
网络开放功能NEF网元
应用服务器
401
终端向AMF网元发送注册请求
402
AMF网元根据注册请求中的指示信息，确定对终端进行第三方认证
403
AMF网元向AUSF网元发送终端认证请求
404
AUSF网元根据终端认证请中的指示信息确定对该终端进行三方认证
405
AUSF网元向NEF网元发送用户标识
406
NEF网元向应用服务器发送该用户标识
407
应用服务器对用户标识对应的终端进行第三方认证
408
应用服务器向NEF网元发送认证结果和用户标识对应的认证参数
409
NEF网元向AUSF网元发送认证结果和将用户标识对应的认证参数
410
AUSF网元基于认证参数对终端进行本地认证
411
在认证结果为认证成功，且AUSF网元对终端的本地认证认证成功时，AMF网元向终端发送注册接受

图 4

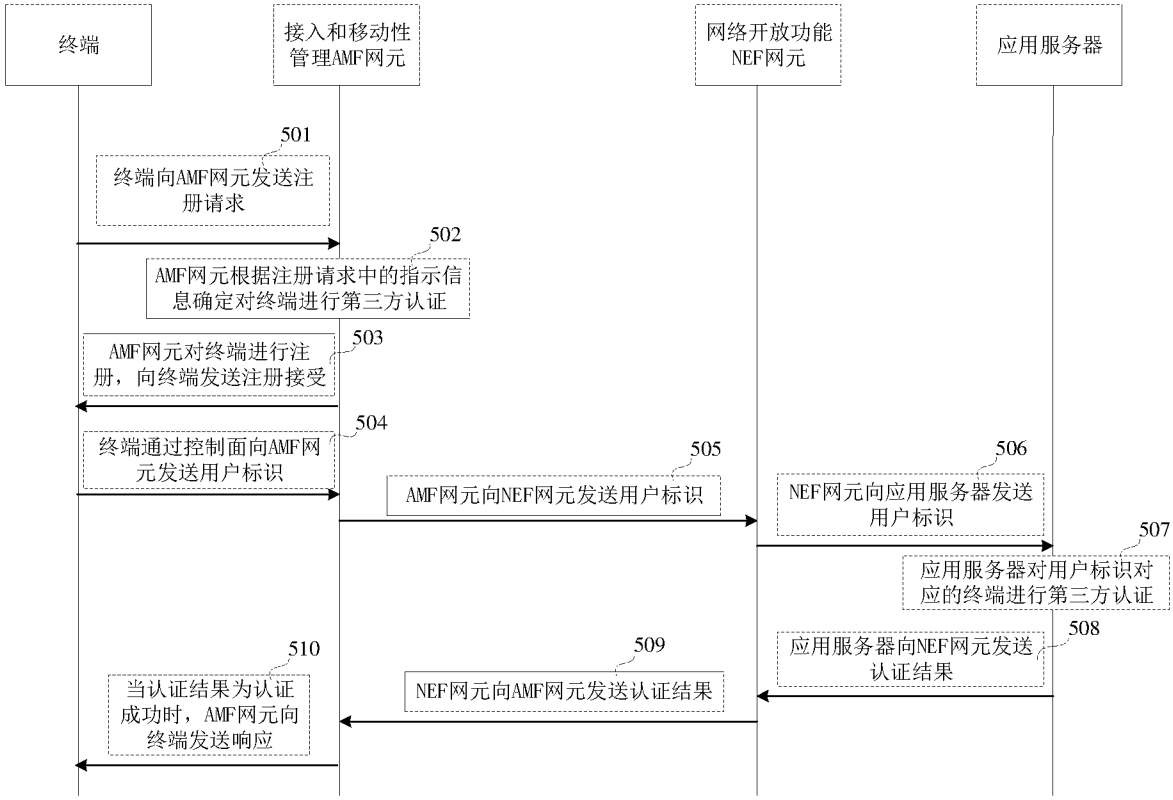
终端
接入和移动性管理AMF网元
网络开放功能NEF网元
应用服务器
501
终端向AMF网元发送注册请求
502
AMF网元根据注册请求中的指示信息确定对终端进行第三方认证
503
AMF网元对终端进行注册，向终端发送注册接受
504
终端通过控制面向AMF网元发送用户标识
505
AMF网元向NEF网元发送用户标识
506
NEF网元向应用服务器发送用户标识
507
应用服务器对用户标识对应的终端进行第三方认证
508
应用服务器向NEF网元发送认证结果
509
NEF网元向AMF网元发送认证结果
510
当认证结果为认证成功时，AMF网元向终端发送响应

图 5

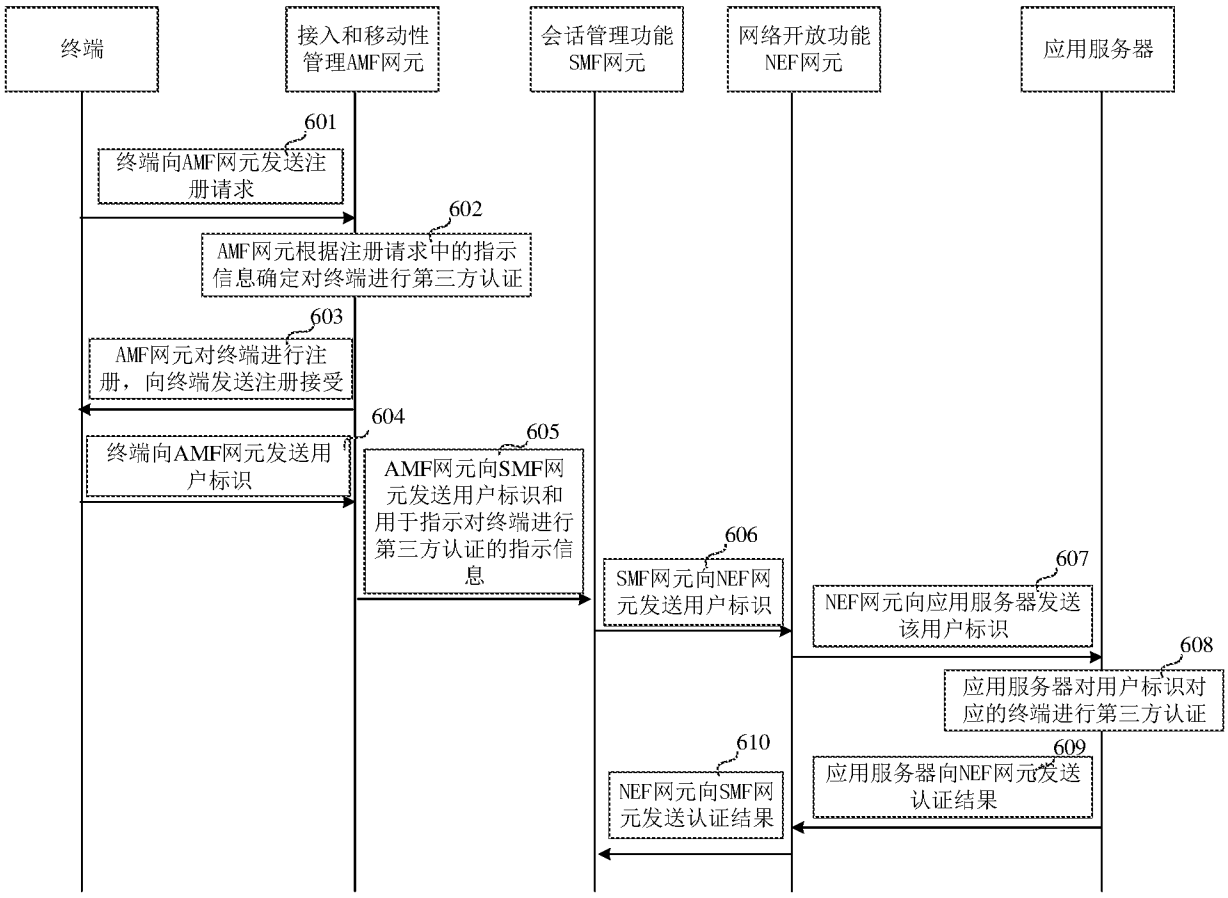
终端
接入和移动性管理AMF网元
会话管理功能SMF网元
网络开放功能NEF网元
应用服务器
601
终端向AMF网元发送注册请求
602
AMF网元根据注册请求中的指示信息确定对终端进行第三方认证
603
AMF网元对终端进行注册，向终端发送注册接受
604
终端向AMF网元发送用户标识
605
AMF网元向SMF网元发送用户标识和用于指示对终端进行第三方认证的指示信息
606
SMF网元向NEF网元发送用户标识
607
NEF网元向应用服务器发送该用户标识
608
应用服务器对用户标识对应的终端进行第三方认证
609
应用服务器向NEF网元发送认证结果
610
NEF网元向SMF网元发送认证结果

图 6

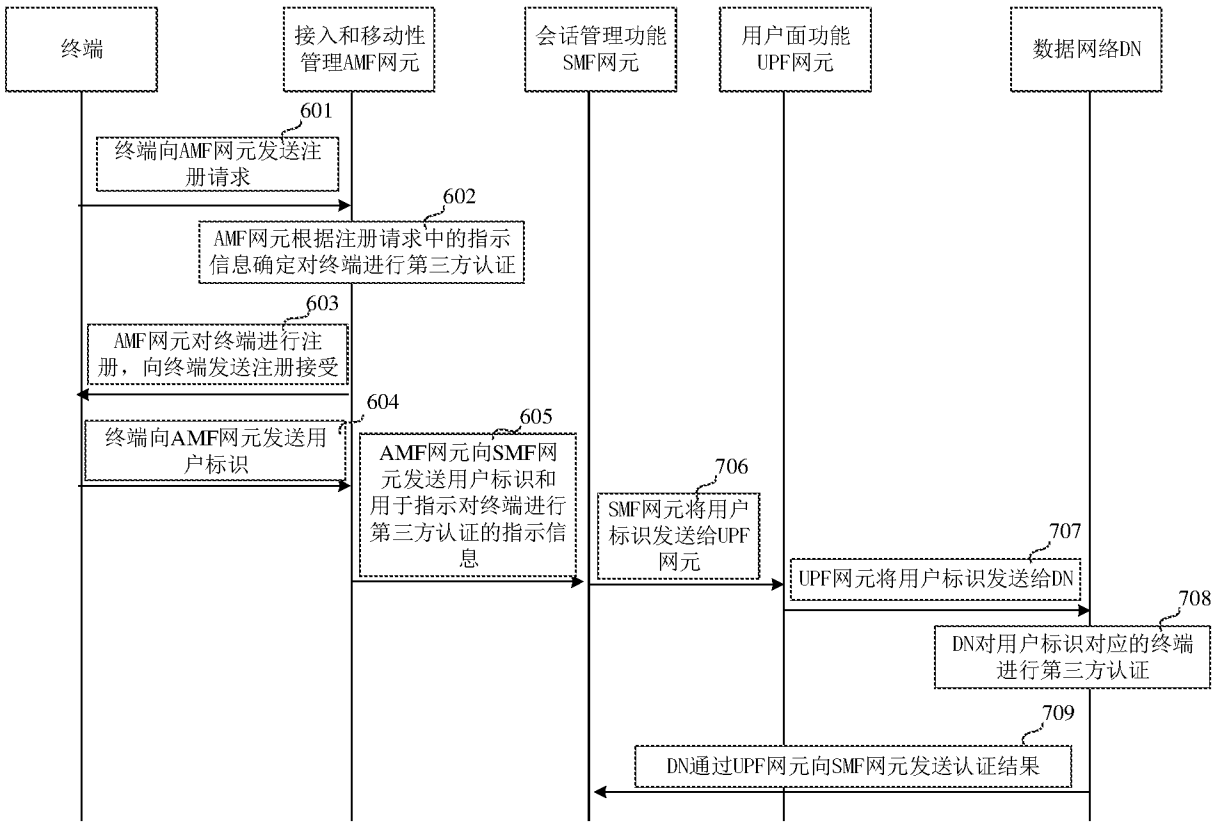
终端
接入和移动性管理AMF网元
会话管理功能SMF网元
用户面功能UPF网元
数据网络DN
601
终端向AMF网元发送注册请求
602
AMF网元根据注册请求中的指示信息确定对终端进行第三方认证
603
AMF网元对终端进行注册，向终端发送注册接受
604
终端向AMF网元发送用户标识
605
AMF网元向SMF网元发送用户标识和用于指示对终端进行第三方认证的指示信息
706
SMF网元将用户标识发送给UPF网元
707
UPF网元将用户标识发送给DN
708
DN对用户标识对应的终端进行第三方认证
709
DN通过UPF网元向SMF网元发送认证结果

图 7

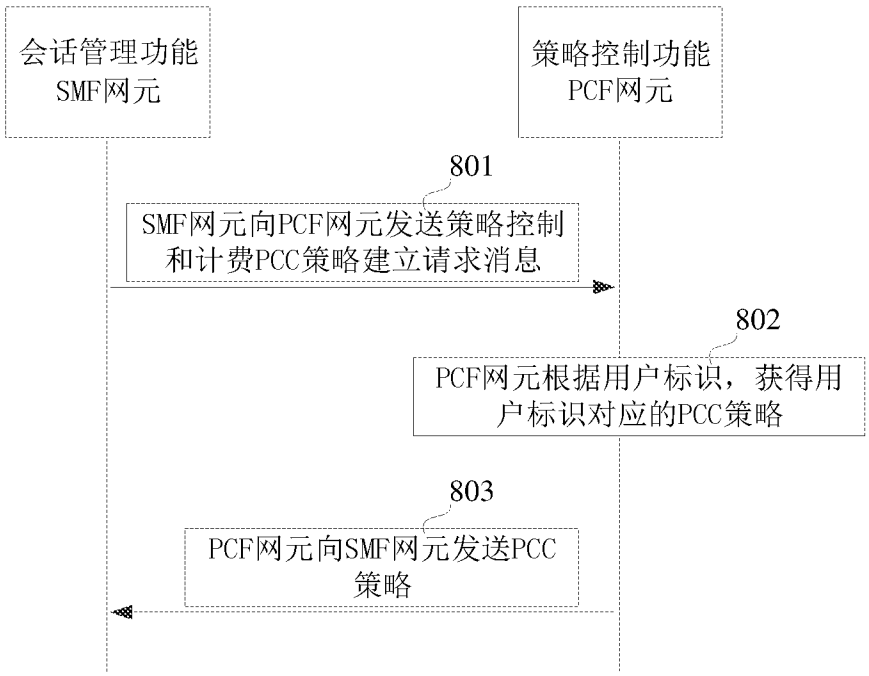
会话管理功能SMF网元
策略控制功能PCF网元
801
SMF网元向PCF网元发送策略控制和计费PCC策略建立请求消息
802
PCF网元根据用户标识，获得用户标识对应的PCC策略
803
PCF网元向SMF网元发送PCC策略

图 8

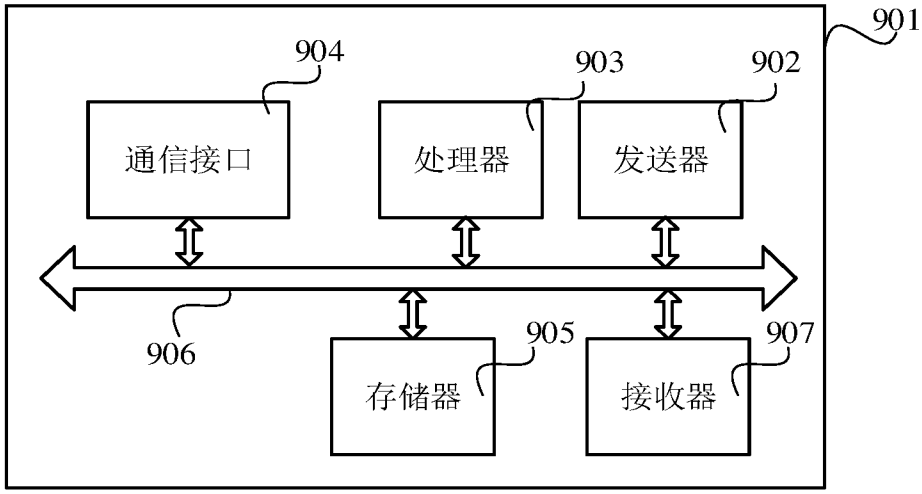
901
904
903
902
通信接口
处理器
发送器
906
905
907
存储器
接收器

图 9

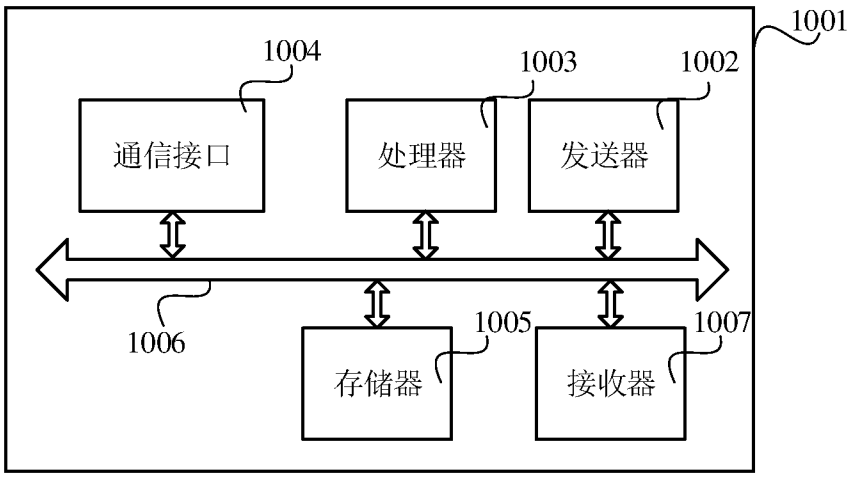
1001
1004
1003
1002
通信接口
处理器
发送器
1006
1005
1007
存储器
接收器

图 10

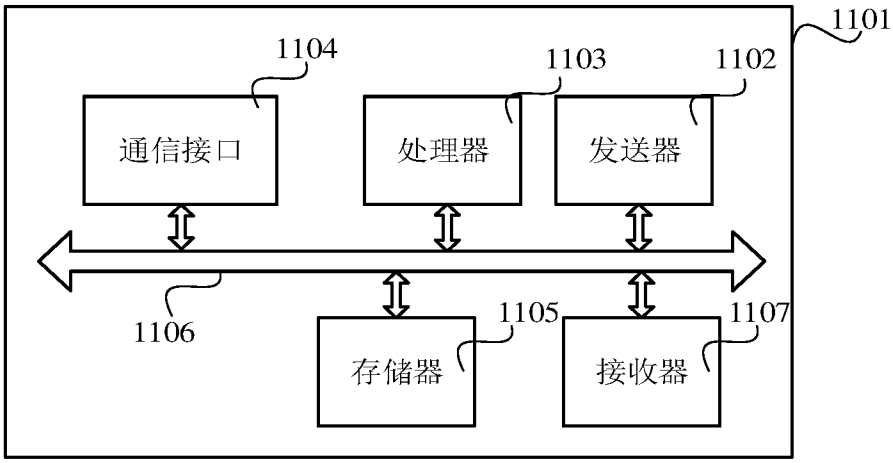
1101
1104
1103
1102
通信接口
处理器
发送器
1106
1105
1107
存储器
接收器

图 11

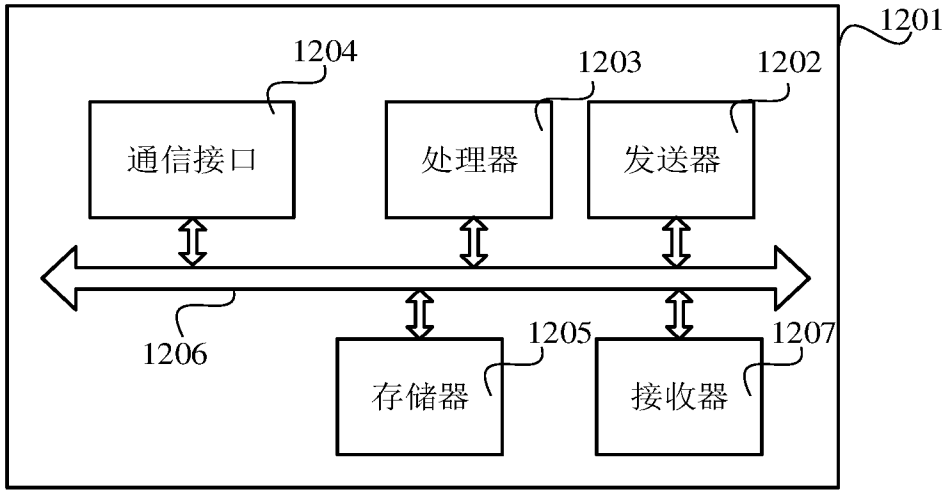
1201
1204
1203
1202
通信接口
处理器
发送器
1206
1205
1207
存储器
接收器

图 12

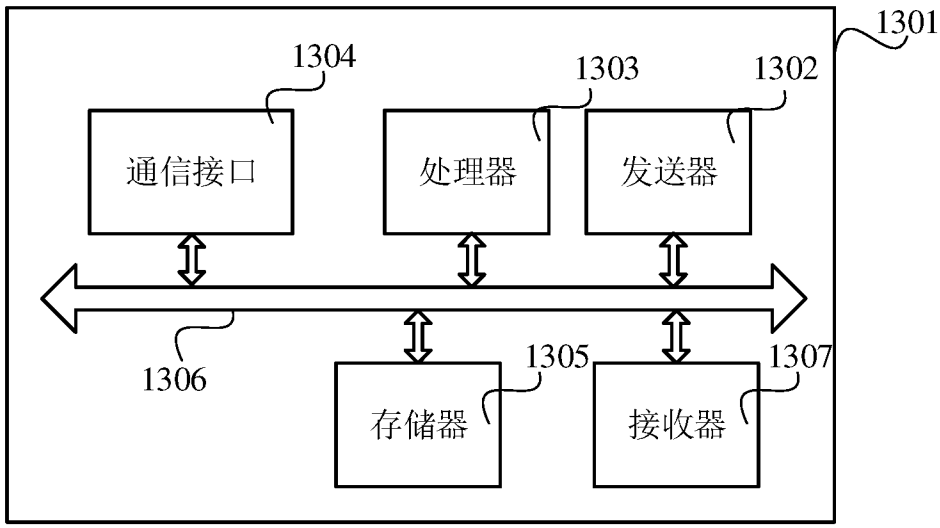
1301
1304
1303
1302
通信接口
处理器
发送器
1306
1305
1307
存储器
接收器

图 13

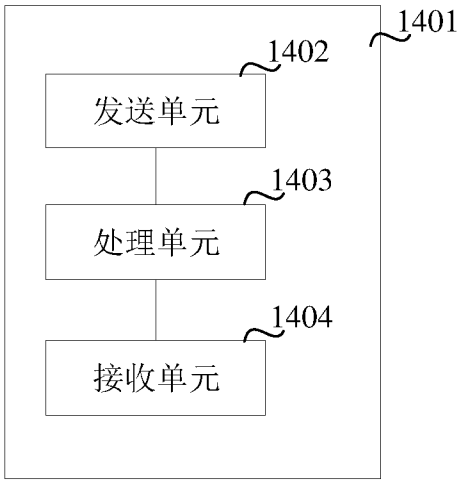
1401
1402
发送单元
1403
处理单元
1404
接收单元

图 14

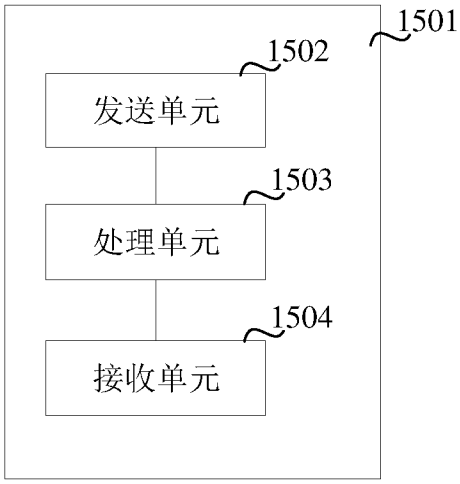
1501
1502
发送单元
1503
处理单元
1504
接收单元

图 15

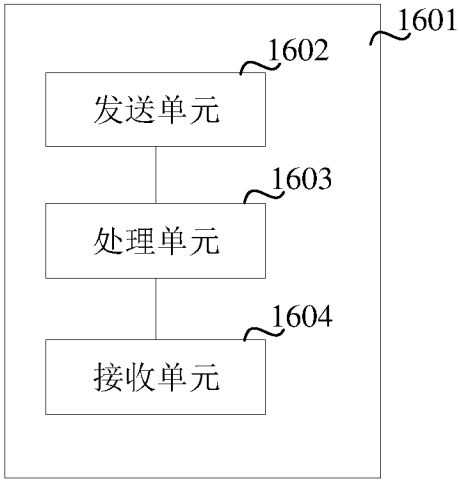
1601
1602
发送单元
1603
处理单元
1604
接收单元

图 16

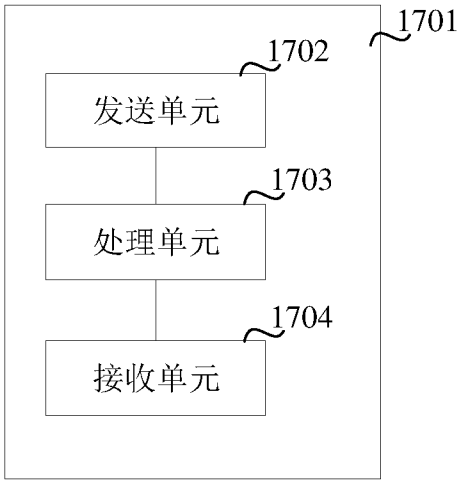
1701
1702
发送单元
1703
处理单元
1704
接收单元

图 17

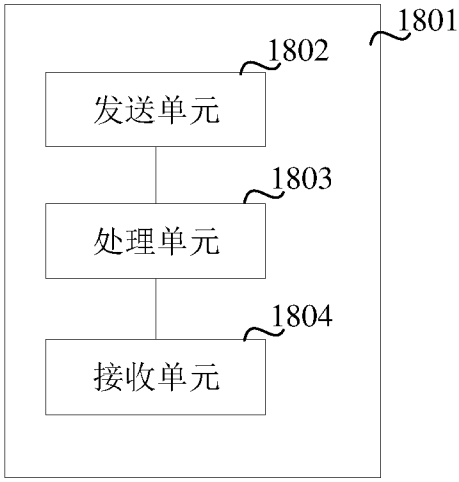
1801
1802
发送单元
1803
处理单元
1804
接收单元

图 18

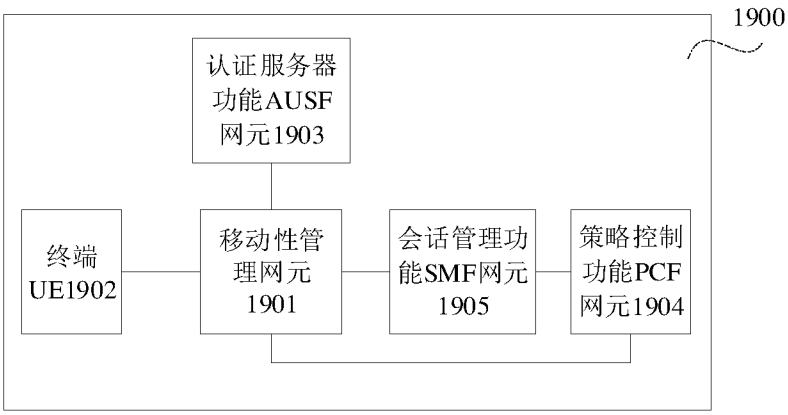
1900
认证服务器功能AUSF网元1903
终端UE1902
移动性管理网元1901
会话管理功能SMF网元1905
策略控制功能PCF网元1904

图 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/072529

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)i; H04L 12/24(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; CNKI; 3GPP: 5G, AMF, SMF, AAA, UDM, 第三方认证, 注册, 请求, 应用容器, 标识, registration, third party, authenticate, container, request, ID, flag

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NOKIA et al. "Network Slice Access Subscription Management by a Third Party" *SA WG2 Meeting #122bis S2-175693*, 25 August 2017 (2017-08-25), sections 2, 3 and 5.15.x	1-30
A	CN 107637019 A (HUAWEI TECHNOLOGIES CO., LTD.) 26 January 2018 (2018-01-26) entire document	1-30
A	CN 107579948 A (HUAWEI TECHNOLOGIES CO., LTD.) 12 January 2018 (2018-01-12) entire document	1-30
A	CN 106912047 A (ZTE CORPORATION) 30 June 2017 (2017-06-30) entire document	1-30
A	CN 104267958 A (NETQIN MOBILE INC.) 07 January 2015 (2015-01-07) entire document	1-30

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 March 2019	**19 April 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/072529

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 107637019 A	26 January 2018	US 2016360408 A1	08 December 2016
		KR 20180014097 A	07 February 2018
		EP 3311530 A4	22 August 2018
		WO 2016192635 A1	08 December 2016
		EP 3311530 A1	25 April 2018
CN 107579948 A	12 January 2018	WO 2018006626 A1	11 January 2018
CN 106912047 A	30 June 2017	WO 2017107745 A1	29 June 2017
CN 104267958 A	07 January 2015	None	

国际检索报告

国际申请号
PCT/CN2019/072529

A. 主题的分类

H04W 12/06(2009.01)i; H04L 12/24(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT; WPI; EPODOC; CNKI; 3GPP: 5G, AMF, SMF, AAA, UDM, 第三方认证，注册，请求，应用容器，标识，registration, third party, authenticate, container, request, ID, flag

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	NOKIA等. "Network Slice access subscription management by a third party" SA WG2 Meeting #122bis S2-175693, 2017年 8月 25日 (2017-08-25), 第2、3、5.15.x节	1-30
A	CN 107637019 A (华为技术有限公司) 2018年 1月 26日 (2018-01-26) 全文	1-30
A	CN 107579948 A (华为技术有限公司) 2018年 1月 12日 (2018-01-12) 全文	1-30
A	CN 106912047 A (中兴通讯股份有限公司) 2017年 6月 30日 (2017-06-30) 全文	1-30
A	CN 104267958 A (北京网秦天下科技有限公司) 2015年 1月 7日 (2015-01-07) 全文	1-30

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 3月 20日	2019年 4月 19日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 向琳 电话号码 86-10-53961566

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/072529

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	107637019	A	2018年 1月 26日	US	2016360408	A1	2016年 12月 8日
				KR	20180014097	A	2018年 2月 7日
				EP	3311530	A4	2018年 8月 22日
				WO	2016192635	A1	2016年 12月 8日
				EP	3311530	A1	2018年 4月 25日
CN	107579948	A	2018年 1月 12日	WO	2018006626	A1	2018年 1月 11日
CN	106912047	A	2017年 6月 30日	WO	2017107745	A1	2017年 6月 29日
CN	104267958	A	2015年 1月 7日		无		