

(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
2023 年 11 月 9 日 (09.11.2023)



(10) 国际公布号
WO 2023/213301 A1

- (51) 国际专利分类号:
H04W 12/06 (2021.01)
- (21) 国际申请号: PCT/CN2023/092298
- (22) 国际申请日: 2023 年 5 月 5 日 (05.05.2023)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202210489884.6 2022年5月6日 (06.05.2022) 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: 李赫(LI, He); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴荣(WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,

(54) **Title:** AUTHENTICATION METHOD, COMMUNICATION APPARATUS, AND COMPUTER-READABLE STORAGE MEDIUM

(54) 发明名称: 鉴权方法、通信装置和计算机可读存储介质

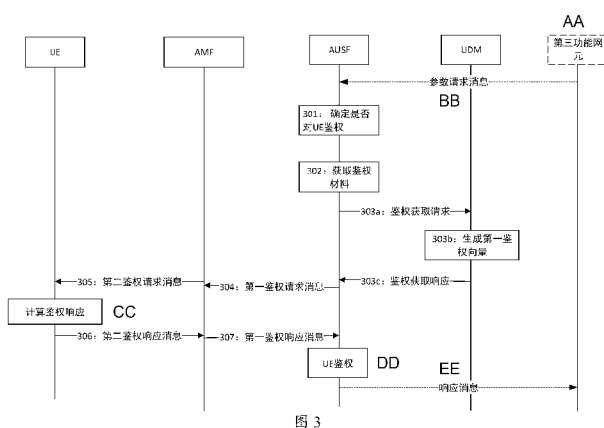


图 3

- 301 Determine whether to authenticate a UE
302 Acquire authentication material
303a Authentication acquisition request
303b Generate a first authentication vector
303c Authentication acquisition response
304 First authentication request message
305 Second authentication request message
306 Second authentication response message
307 First authentication response message
AA Third functional network element
BB Parameter request message
CC Calculate an authentication response
DD UE authentication
EE Response message

(57) **Abstract:** Embodiments of the present application disclose an authentication method, a communication apparatus, and a storage medium. The method comprises: a first functional network element of a home network determining whether a terminal needs to be authenticated; when the terminal needs to be authenticated, the first functional network element acquiring authentication material; the first functional network element acquiring a first authentication vector according to the authentication material; and the first functional network element sending a first authentication request message to an AMF, so as to trigger authentication of the terminal, the first authentication request message comprising the first authentication vector. In the present method, the first functional network element of the home network determines to trigger authentication of the terminal.

(57) 摘要: 本申请实施例公开了鉴权方法、通信装置和存储介质, 其中, 该方法包括归属网络的第一功能网元确定是否需要终端进行鉴权; 在需要对终端进行鉴权的情况下, 第一功能网元获取鉴权材料; 第一功能网元根据所述鉴权材料, 获取第一鉴权向量; 第一功能网元向AMF发送第一鉴权请求消息以触发对终端进行鉴权, 其中, 第一鉴权请求消息包括第一鉴权向量。该方法中通过归属网络的第一功能网元确定触发对终端进行鉴权。

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))。

鉴权方法、通信装置和计算机可读存储介质

- 5 本申请要求于 2022 年 05 月 06 日提交中国专利局、申请号为 202210489884.6、申请名称为“鉴权方法、通信装置和计算机可读存储介质”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

- 10 本申请涉及通信领域，并且更具体地，涉及通信领域中的鉴权方法和使用该鉴权方法的通信装置。

背景技术

目前，用户设备（user equipment, UE）接入 5G 网络，均需经过接入、鉴权的过程。当终端设备鉴权成功并进入连接态，用户设备可以与网络进行通信。

- 15 相关技术中，当用户设备接入 5G 网络，且终端是首次注册时，终端可以通过下一代基站(next generation node basestaion, gNB)或非 3GPP 合作功能(non-3GPPinterworking function, N3IWF)网元向核心网接入和移动管理(core access and mobility management function, AMF)实体发送该终端的身份信息。当 AMF 网元接收到终端的身份信息时，AMF 网元可以根据该用户设备的身份信息选择鉴权服务功能(authentication server function, AUSF)实体以触发鉴权流程，AUSF 向统一数据管理(unified data management, UDM)实体发送鉴权获取请求，UDM 根据鉴权获取请求计算鉴权向量，再返回鉴权向量至 AUSF 网元，AUSF 网元通过 AMF 网元向 UE 发送鉴权参数，UE 校验鉴权参数，校验成功则表明网络侧验证通过，UE 向 AMF 发送响应，AMF 向 AUSF 发送认证校验信息，AUSF 校验认证校验信息，校验成功则表明 UE 鉴权成功，由此完成鉴权流程。

- 20 在上述相关技术中，主鉴权流程是由服务网络的 AMF 网元发起，当前尚未发现由归属网络的功能网元触发主鉴权的方案。

发明内容

本申请提供一种由归属网络的功能网元发起鉴权的鉴权方法和使用该鉴权方法的通信装置。

- 30 第一方面，本申请实施例提供了一种鉴权方法，该方法包括：归属网络的第一功能网元确定是否需要终端进行鉴权；在需要对所述终端进行鉴权的情况下，所述第一功能网元获取鉴权材料；所述第一功能网元根据所述鉴权材料，获取第一鉴权向量；所述第一功能网元向 AMF 发送第一鉴权请求消息以触发对所述终端进行鉴权，其中，所述第一鉴权请求消息包括所述第一鉴权向量。

- 35 在该技术方案中，通过归属网络的第一功能网元确定是否需要终端进行鉴权，在需要进行鉴权的情况下，第一功能网元获取鉴权材料，根据鉴权材料，获取第一鉴权向量，第一功能网元再向 AMF 发送第一鉴权请求消息进而触发对终端进行鉴权，这样，鉴权流程的发起点在归属网络的第一功能网元，减少了 AMF 与第一功能网元之间的信令交互。

在一种实现方式中，第一功能网元为 AUSF，第一功能网元获取所述鉴权材料的具体方式可以为：第一功能网元从存储的上下文中获取所述鉴权材料；或者第一功能网元从第四功能网元获取鉴权材料，第四功能网元为存储有鉴权材料的网元。

5 在一种实现方式中，第一功能网元确定是否需要所述终端进行鉴权的具体方式可以为：所述第一功能网元接收来自第三功能网元的服务请求，所述服务请求用于向所述第一功能网元请求指定服务；响应于所述第三功能网元的服务请求，所述第一功能网元确定是否需要所述终端进行鉴权。

10 在一种实现方式中，第一功能网元根据所述鉴权材料，获取第一鉴权向量的具体方式可以为：AUSF 向 UDM 发送鉴权向量请求消息，其中，鉴权向量请求消息包括所述鉴权材料；所述 AUSF 接收来自所述 UDM 的鉴权向量响应消息，所述鉴权向量响应消息包括所述第一鉴权向量。

15 在一种实现方式中，第一功能网元为 UDM，第一功能网元获取所述鉴权材料的具体方式可以为：第一功能网元从存储的上下文中获取所述鉴权材料；或者，第一功能网元从第四功能网元获取所述鉴权材料，所述第四功能网元为存储有所述鉴权材料的网元。

在一种实现方式中，第一功能网元根据所述鉴权材料，获取第一鉴权向量的具体方式可以为：所述第一功能网元根据所述鉴权材料，生成所述第一鉴权向量。

在一种实现方式中，鉴权材料具体包括以下一种或多种：服务网络名称，服务网络标识，网络标识符，移动国家码或移动网号。

20 第二方面，本申请实施例提供一种通信装置，该通信装置的结构中包括：处理模块，用于确定是否需要所述终端进行鉴权；在需要对所述终端进行鉴权的情况下，所述处理模块获取鉴权材料；所述处理模块根据所述鉴权材料，获取第一鉴权向量；收发模块，用于向所述 AMF 发送第一鉴权请求消息以触发对所述终端进行鉴权，其中，所述第一鉴权请求消息包括所述第一鉴权向量。

25 在一种实现方式中，处理模块获取所述鉴权材料的具体方式可以为：所述处理模块从存储的上下文中获取所述鉴权材料；或者所述处理模块从第四功能网元获取所述鉴权材料，所述第四功能网元为存储有所述鉴权材料的网元。

30 在一种实现方式中，处理模块确定是否需要所述终端进行鉴权的具体方式可以为：处理模块接收来自第三功能网元的服务请求，所述服务请求用于向所述处理模块请求指定服务；响应于所述第三功能网元的服务请求，所述处理模块确定是否需要所述终端进行鉴权。

在一种实现方式中，处理模块根据所述鉴权材料，获取所述第一鉴权向量的具体方式可以为：所述处理模块向 UDM 发送鉴权向量请求消息，其中，所述鉴权向量请求消息包括所述鉴权材料；所述处理模块接收来自所述 UDM 的鉴权向量响应消息，所述鉴权向量响应消息包括所述第一鉴权向量。

35 在一种实现方式中，处理模块根据所述鉴权材料，获取所述第一鉴权向量的具体方式可以为：所述处理模块根据所述鉴权材料，生成所述第一鉴权向量。

在一种实现方式中，鉴权材料具体包括以下一种或多种：服务网络名称，服务网络标识，网络标识符，移动国家码或移动网号。

第三方面，本申请实施例提供另一种通信装置，该通信装置包括至少一个处理器，至

少一个处理器执行用于执行存储在存储器中的指令，使得该通信装置实现上述第一方面所述的方法示例中的操作。

第四方面，本发明实施例提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令被通信装置执行时使该通信装置执行上述第一方面的方法。

附图说明

图 1 是 5G 服务化架构的示意图。

图 2 是一种鉴权方法的流程示意图。

图 3 是本申请实施例提供的一种鉴权方法的流程示意图。

图 4 是本申请实施例提供的又一种鉴权方法的流程示意图。

图 5 是本申请实施例提供的又一种鉴权方法的流程示意图。

图 6 是本申请实施例提供的鉴权装置的结构示意图。

图 7 是本申请实施例提供的鉴权装置的另一结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。其中，在本申请的描述中，除非另有说明，“/”表示前后关联的对象是一种“或”的关系，例如，A/B 可以表示 A 或 B；本申请中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A、B 可以是单数或者复数。并且，在本申请的描述中，除非另有说明，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a，b，或 c 中的至少一项(个)，可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。另外，为了便于清楚描述本申请实施例的技术方案，在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并不限定一定不同。

本申请实施例的技术方案可以应用于各种通信系统，例如：第五代(5th Generation, 5G)移动通信系统中的新无线(New Radio, NR)以及未来的移动通信系统等。

(1) 第五代(5th generation, 5G)网络架构

如图 1 所示，为基于服务化架构的第五代(5th generation, 5G)网络架构示意图。该架构可包括接入网和核心网，可选的，还可以包括用户设备(user equipment, UE)。

UE 是一种具有无线收发功能的设备，可以部署在陆地上，包括室内或室外、手持、穿戴或车载；也可以部署在水面上(如轮船等)；还可以部署在空中(例如飞机、气球和卫星上等)。UE 可以是手机(mobile phone)、平板电脑(Pad)、带无线收发功能的电脑、虚拟现实(virtual reality, VR)终端设备、增强现实(augmented reality, AR)终端设备、工业控制(industrial control)中的无线终端、车载终端设备、无人驾驶(self driving)中的无线终端、远程医疗(remote medical)中的无线终端、智能电网(smart grid)中的无线终端、运输安全(transportation safety)中的无线终端、智慧城市(smart city)中的无

线终端、智慧家庭（smart home）中的无线终端、可穿戴终端设备等等。UE有时也可以称为终端、终端设备、接入终端设备、车载终端、工业控制终端、UE单元、UE站、移动站、移动台、远方站、远程终端设备、移动设备、UE代理或UE装置等。UE也可以是固定的或者移动的。

- 5 接入网可以包括接入网络设备，接入网络设备可以是为终端设备提供接入的设备，可以包括无线接入网（radio access network, RAN）设备。RAN设备主要负责空口侧的无线资源管理、服务质量（quality of service, QoS）管理、数据压缩和加密等功能。RAN设备可以包括各种形式的基站，例如宏基站，微基站（也可以称为小站），中继站，接入点，气球站等。在采用不同的无线接入技术的系统中，具备基站功能的设备的名称可能会有所不同，例如，在5G系统中，称为RAN或者下一代基站（next-generation Node basestation, gNB）；在长期演进（long term evolution, LTE）系统中，称为演进的节点B（evolved NodeB, eNB或eNodeB）。

- 10 核心网负责维护移动网络的签约数据，为UE提供会话管理、移动性管理、策略管理以及安全认证等功能。核心网可以包括如下网元：用户面功能（user plane function, UPF）、
15 认证服务功能（authentication server function, AUSF）、接入和移动性管理功能（access and mobility management function, AMF）、会话管理功能（session management function, SMF）、网络切片选择功能（network slice selection function, NSSF）、网络开放功能（network exposure function, NEF）、网络功能仓储功能（NF repository function, NRF）、策略控制功能（policy control function, PCF）、统一数据管理（unified data management, UDM）
20 和应用功能（application function, AF）、AKMA服务的锚点网元（AKMA anchor function, AAnF）。

- SMF网元，主要负责移动网络中的会话管理，例如会话建立、修改和释放。具体功能例如为用户分配互联网协议（internet protocol, IP）地址，选择提供报文转发功能的UPF等。UPF网元，主要负责用户数据的转发和接收，可以从数据网络接收用户数据，通过接
25 入网络设备传输给UE；还可以通过接入网络设备从UE接收用户数据，转发至数据网络。PCF网元，主要支持提供统一的策略框架来控制网络行为，提供策略规则给控制层网络功能，同时负责获取与策略决策相关的用户签约信息。PCF网元可以向AMF网元、SMF网元提供策略，例如服务质量（quality of service, QoS）策略、切片选择策略等。数据网络（data network, DN）用于为用户提供业务服务，可以是私有网络，例如局域网；也可以
30 是不受运营商管控的外部网络，例如互联网（Internet）；还可以是运营商共同部署的专有网络，例如提供IP多媒体子系统（IP multimedia subsystem, IMS）的网络。UE可通过建立的协议数据单元（protocol data unit, PDU）会话，来访问DN。

AMF网元，主要负责移动网络中的移动性管理，例如用户位置更新、用户注册网络、用户切换等。为描述方便，后文简称AMF。

- 35 AUSF网元，用于执行UE的安全认证。AUSF网元接收到UE发起的认证请求之后，可通过UDM网元中存储的认证和/或授权信息对UE进行认证和/或授权，或者通过统一数据管理功能生成签约用户的认证和/或授权信息。为描述方便，后文简称AUSF。

UDM网元，用于存储用户数据，例如签约数据、鉴权/授权数据等。服务网络（serving network, SN），是AMF、AUSF所在的位置。

服务网络 (serving network, SN), 也称拜访网络, 是一个终端使用 N1 接口连接的 AMF 所在的网络。服务网络是 AMF、SMF 所在的位置。

归属网络 (Home network, HN), 也称家乡网络, 是指存储 UE 的签约数据的网元所在的网络。家乡网络可以被标识符标识。家乡网络标识符包括移动国家码(Mobile Country Code, MCC)和移动网号(Mobile Network Code, MNC)。归属网络是 AUSF、UDM 所在的位置。

(2) 主鉴权

当前, UE 可以通过 3GPP 技术接入网络。当 UE 首次接入 5G 网络时, AMF 需要启动 UE 和网络之间的相互认证, 即主鉴权流程。并提供可在后续安全过程中在 UE 和服务网络之间使用的密钥材料, 从而保证 UE 和核心网之间的安全性。主鉴权和密钥认证生成锚密钥 K_{SEAF} , 锚密钥由归属网络的 AUSF 发送给服务网络的 AMF。

参考图 2 所示的一种主鉴权流程图, 包括但不限于如下步骤:

步骤 201: AMF 向 AUSF 发送第一鉴权请求消息。

当服务网络的 AMF 确定启动认证时, AMF 通过向 AUSF 发送第一鉴权请求消息 (UEAuthentication_Authenticate Request message), 用于触发主鉴权流程。

第一鉴权请求消息可以包括如下一个或多个参数: 用户身份标识、服务网络名称 (serving network name, SN-name)。其中, 用户身份标识用于标识用户设备, 服务网络名称用于标识对应的服务网络。

可选地, 用户身份标识为 SUPI 或 SUCI。SUPI 是用户的永久身份, 可以全网唯一标识一个用户。SUCI 是 UE 的匿名身份信息, 是一种临时身份, 用于保护 SUPI 不被暴露在空口, 进而保护用户隐私。SUCI 至少包括 SUPI 中除 SUPI 类型外的部分做加密后的结果。

步骤 202: AUSF 接收到第一鉴权请求消息后, 依据第一鉴权请求消息携带的服务网络名称确定是否为允许接入的服务网络, 当确定为允许接入的服务网络后, AUSF 发送第一获取请求消息 (UEAuthentication_Get Request) 至 UDM。

步骤 203: UDM 接收来自 AUSF 的第一获取请求消息, 根据接收的第一获取请求消息生成第一鉴权向量, 再发送响应于该第一获取请求消息的第一获取响应消息至 AUSF。

其中, 第一获取响应消息包括第一鉴权向量和用户身份标识。

一种实现方式中, 用户身份标识为 SUCI, UDM 解析 SUCI 以获得用户设备的永久身份标识 (SUPI), UDM 基于 SUPI 确定鉴权算法, 并生成第一鉴权向量。可选的, 鉴权算法为 EAP-AKA' 鉴权或 5G AKA。下面以 5G AKA 为例介绍。

UDM 基于 5G AKA 算法生成第一鉴权向量, 第一鉴权向量包括 RAND, AUTN, XRES* 和 K_{AUSF} 。其中, RAND 为随机数, K_{AUSF} 为归属网络中 AUSF 生成的中间密钥, XRES* 为期望响应, 根据秘钥生成函数(keyderivation functions, KDF)计算得到的, 是期望的 UE 鉴权响应参数, 用于与 UE 返回的响应 RES* 比较以确定鉴权是否成功; AUTN 为认证令牌, AUTN 为网络提供给 UE 以用于对归属网络进行鉴权的参数。

步骤 204: AUSF 接收来自 UDM 的第一获取响应消息, 生成第二鉴权向量, 发送第二鉴权响应消息至 AMF。其中, 第二鉴权响应消息包括第二鉴权向量。

AUSF 接收第一获取响应消息后, AUSF 临时存储 XRES* 和用户永久身份标识 SUPI, 计算第二鉴权向量, 再发送第二鉴权响应至 AMF。其中, 第二鉴权向量包括 RAND, AUTN,

HXRES*。

具体的，AUSF 基于 XRES* 计算得到 HXRES* 再使用 HXRES* 替换 XRES* 得到第二鉴权向量。

5 步骤 205: AMF 接收该第二鉴权响应消息，发送第二鉴权请求消息至 UE，其中，第二鉴权请求消息用于在 UE 侧触发和网络侧的双向鉴权，第二鉴权请求消息携带 RAND, AUTN。

步骤 206: UE 接收来自 AMF 的第二鉴权请求消息，UE 验证网络是否为真实的。当 UE 确定网络是真实的，UE 向 AMF 发送第二鉴权响应消息，该第二鉴权响应消息中包括鉴权响应 RES*。

10 步骤 207: AMF 接收到 RES* 后，向 AUSF 发送第三鉴权请求消息，该第三鉴权请求消息包括 AMF 从 UE 处接收到的 RES*。

基于 RES* 计算 HRES*，比较 HRES* 与存储的 HXRES*，若 HRES* 和 HXRES* 一致则认为 AMF 认为 UE 是真实的。之后，AMF 向 AUSF 发送第三鉴权请求消息用于将从 UE 处接收到的 RES* 发送至 AMF。

15 步骤 208: AUSF 接收到该第三鉴权请求消息后，将 RES* 与保存的 XRES* 比较，如果 RES* 与保存的 XRES* 一致，则认为 UE 鉴权成功。AUSF 可向 AMF 发送第三鉴权响应消息，该第三鉴权响应消息中包括 AUSF 的鉴权结果。

上述鉴权方法，服务网络的 AMF 可在与 UE 建立信令连接的任何过程中触发对 UE 的鉴权。

20 在一种实现方式中，AMF 接收用户设备的注册请求以发起对 UE 的鉴权。可选地，AMF 通过 RAN 接收来自用户设备的首次注册请求，首次注册请求中携带用户设备标识（例如，SUCI），AMF 基于 SUCI 确定对应的用户设备是否为被服务网络允许接入的用户设备。

25 在另一种实现方式中，AMF 预配置策略触发对 UE 的鉴权。例如，AMF 根据本地策略，在 NAS COUNT 即将翻转时触发对 UE 的鉴权。

在另一种实现方式中，例如 UE 从 4G 移动到 5G，且 AMF 设有 5G 原生安全上下文的时候，AMF 可触发主鉴权流程。

30 另一种触发对 UE 鉴权的方法，由 UDM 向为 UE 服务的 AMF 请求为 UE 发起鉴权，AMF 响应于该请求触发主鉴权流程。示例的，AMF 基于 UDM 的请求，按照上述步骤 201 至步骤 208 的方式执行鉴权流程。

另一种触发对 UE 鉴权的方法，由 AUSF 向为 UE 服务的 AMF 请求为 UE 发起鉴权，AMF 响应于该请求发起主鉴权流程。AMF 基于 AUSF 的请求，按照上述步骤 201 至步骤 208 的方式执行鉴权流程。与 UDM 向 AMF 请求对 UE 进行鉴权的不同之处在于，AUSF 向 AMF 请求对 UE 进行鉴权需要先向 UDM 获取为 UE 服务的 AMF 信息。

35 上述的鉴权方法，其本质都是由服务网络的 AMF 向 AUSF 发送消息以开始鉴权流程。当 AUSF 或者 UDM 请求 AMF 发起对 UE 进行鉴权时，鉴权流程较为复杂，信令开销较大。

鉴于此，本申请提供一种由归属网络的功能网元发送消息给 AMF，并直接开始对 UE 进行鉴权的方法。可以理解的，鉴权流程的发起点在归属网络的功能网元，而不再是服务

网络的 AMF。

对 UE 进行鉴权，是指核心网对 UE 进行安全认证，确定 UE 是真实可信的。同时，UE 也能认证网络是真实的。若归属网络确定需要对 UE 进行鉴权，则归属网络发起归属网络鉴权流程。具体地，归属网络鉴权流程是由归属网络功能网元直接开始对 UE 进行鉴权。具体地，指当归属网络确定需要对 UE 鉴权时，归属网主动发送鉴权向量给 AMF，并通过 AMF 发送给 UE 以执行鉴权的过程。

参考图 3 所示，本实施例提供的一种由归属网络的第一功能网元发起鉴权的方法，在该方法中第一功能网元为 AUSF，该方法包括但不限于：

步骤 301. AUSF 确定是否需要需要对 UE 进行鉴权。

AUSF 基于本地策略或第三功能网元的请求确定是否需要需要对 UE 进行鉴权。其中，第三功能网元为除 AUSF 以外的核心网网元。

在一种实现方式中，AUSF 根据本地策略确定是否需要需要对 UE 进行鉴权。

可选地，本地策略可以包括：当 AUSF 发现漫游指导（Steering of roaming, SoR）计数器值或者通过 UDM 更新 UE 参数（UE parameters update via UDM, UPU）计数器值即将翻转时，AUSF 确定需要对 UE 进行鉴权。

可选地，本地策略可以包括：当 AUSF 发现 K_{AUSF} 的使用时间超过或即将超过运营商策略所规定的时间，则 AUSF 确定需要对 UE 进行鉴权。具体的，通过计时器记录 K_{AUSF} 的使用时间，该计时器与 UE 的永久身份 SUPI 绑定，当该计时器记录的 K_{AUSF} 的使用时间超过或即将超过预设值时，AUSF 确定需要对 UE 进行鉴权。

可选地，本地策略可以包括：当 AUSF 发现距离前一次对 UE 鉴权成功的时间间隔超过或即将超过运营商策略所规定的时间，则 AUSF 确定需要对 UE 进行鉴权。具体的，可通过一个计时器记录距离前一次对 UE 鉴权成功的时间间隔，该计时器与 UE 的永久身份 SUPI 绑定。当 AUSF 确定 UE 鉴权成功后，计时器开始工作，当该计时器工作时间间隔超过或即将超过预设间隔值时，AUSF 确定需要对 UE 进行鉴权。

在又一种实现方式中，AUSF 接收来自第三功能网元的参数请求消息。该参数请求消息用于向 AUSF 请求参数，或者请求 AUSF 为 UE 进行鉴权。

其中，参数请求消息至少包括用户的永久身份 SUPI。比如，参数请求消息可以用于请求 K_{AKMA} 。再比如，参数请求消息用于请求 SoR 数据保护，或者请求 UPU 数据保护。

第三功能网元为 AUSF 以外的核心网功能网元。比如，该第三功能网元为 AAnF, UDM, 或者 AF 等功能网元。

可选地，第三功能网元是 AAnF, AAnF 向 AUSF 发送 K_{AKMA} 更新请求消息，该更新请求消息用于请求一个新的 K_{AKMA} 密钥。比如，该更新请求消息为 Nausf_AKMA_AnchorKey_Refresh。AUSF 根据该更新请求消息确定是否需要更新 K_{AKMA} 。若确定需要更新 K_{AKMA} 则确定需要对 UE 进行鉴权。

可选地，第三功能网元是 UDM, UDM 向 AUSF 发送 SoR 保护请求消息或者 UPU 保护请求消息，该请求消息中携带的数据需要使用 K_{AUSF} 做安全保护。当 AUSF 发现需要更新 K_{AUSF} ，或者 AUSF 本地没有存储 K_{AUSF} 时，则确定需要对 UE 进行鉴权。具体的，该请求消息为 Nausf_SoRProtection message，或者 Nausf_UPUProtection message。

可选地，第三功能网元是 UDM, UDM 接收到 AAnF 请求更新 K_{AKMA} 请求时，UDM

向 AUSF 发送请求消息。此时，该请求消息用于请求更新 K_{AKMA} 。比如，该请求消息为 Nausf_AKMA_ K_{AKMA} _Refresh message。AUSF 确定是否需要更新 K_{AKMA} ，若确定需要更新 K_{AKMA} 则确定需要对 UE 进行鉴权。此时，可选地，Nausf_AKMA_ K_{AKMA} _Refresh 消息中还携带有 AAnF ID，该 AAnF ID 用于告知是哪个 AAnF 请求密钥更新，以便于后续 AUSF 直接发送更新后的 K_{AKMA} 给 AAnF。

可选地，第三功能网元是 UDM，UDM 接收到第四功能网元请求更新 K_{AF} 密钥的请求消息，UDM 向 AUSF 发送 K_{AF} 更新请求消息，该请求消息用于请求一个新的 K_{AF} 密钥，AUSF 确定需要更新 K_{AF} 对应的 K_{AKMA} 时，则确定需要对 UE 进行鉴权。示例的，第四功能网元为 AAnF，或者 3GPP 内部 AF 或者 3GPP 外部 AF，当第四功能网元为 3GPP 外部的 AF 时，该 AF 通过 NEF 请求更新 K_{AF} 。该更新请求消息为 Nausf_AKMA_ K_{AF} _Refresh message。

可选地，第三功能网元是 3GPP 内部 AF，或者用于 3GPP 外部 AF 使用的 NEF，AUSF 接收到 AF 或者 NEF 请求更新 K_{AF} 时，3GPP 内部 AF 或者 NEF 向 AUSF 发送请求消息。此时，该请求消息用于请求更新 K_{AF} 。AUSF 确定需要更新 K_{AF} 对应的 K_{AKMA} 时，则确定需要对 UE 进行鉴权。该更新请求消息为 Nausf_AKMA_ K_{AF} _Refresh message。

可选地，第三功能网元是 3GPP 内部 AF，或者用于 3GPP 外部 AF 使用的 NEF，AUSF 接收到来自 3GPP 内部 AF 或者 NEF 的请求消息。此时，该请求消息用于请求对 UE 进行鉴权，AUSF 响应于该请求消息，确定需要对 UE 进行鉴权。该请求消息为 Nausf_UEAuthentication_Authenticate Requestmessage。

可选地，第三功能网元是 UDM，UDM 接收到来自第四功能网元对 UE 进行鉴权的请求，则 UDM 确定需要对 UE 进行鉴权。示例的，第四功能网元为 AAnF，或者 3GPP 内部 AF 或者 3GPP 外部 AF，当第四功能网元为 3GPP 外部的 AF 时，该 AF 通过 NEF 请求对 UE 进行鉴权。

在第三种实现方式中，AUSF 可以根据本地策略和第三功能网元的请求消息综合判断是否需要对 UE 进行鉴权。

可选地，第三功能网元是 AAnF。AAnF 向 AUSF 发送 K_{AKMA} 更新请求消息。该更新请求消息用于请求一个新的 K_{AKMA} 密钥。比如，该更新请求消息为 Nausf_AKMA_AncorKey_Refresh 消息。AUSF 在接收到该更新请求消息后，AUSF 根据本地策略进一步判断是否对 UE 进行鉴权。

进一步地，本地策略为距离前次鉴权成功的时间间隔是否超过或即将超过运营商策略所规定的时间。AUSF 可以根据距离前次鉴权成功的时间间隔判断是否需要对 UE 进行鉴权。距离前次鉴权成功的时间间隔小于预设值，则确定无需对 UE 进行鉴权；若距离前次鉴权成功的时间间隔超过预设值时，则 AUSF 确定需要对 UE 进行鉴权。

进一步地，本地策略为比对本本地保存的 K_{AKMA} 与 AAnF 发送的 K_{AKMA} 是否一样来确定是否需要对 UE 进行鉴权。具体地，AUSF 根据 AAnF 发送的 K_{AKMA} 与本地保存的 K_{AKMA} 进行对比，若一样，则确定对 UE 进行鉴权；若不一样，则确定不对 UE 进行鉴权。

进一步地，本地策略为比对本本地保存的 K_{AKMA} 密钥标识符与 AAnF 发送的 K_{AKMA} 密钥标识符是否一样来确定是否需要对 UE 进行鉴权。具体的，AUSF 比对 AAnF 发送的 K_{AKMA} 密钥标识符与本地保存的 K_{AKMA} 密钥标识符，若一样，则确定对 UE 进行鉴权；若

不一样,则确定不对UE进行鉴权。其中, K_{AKMA} 密钥标识符由AUSF生成,用于标识 K_{AKMA} ,示例的,它可以为3bit长的密钥标识符,也可以是AKMA密钥标识符(AKMA Key Identifier,A-KID)。

可选地,第三功能网元是3GPP内部AF,或者用于3GPP外部AF使用的NEF。AUSF
5 接收到AF或者NEF请求对UE进行鉴权的鉴权请求消息。AUSF根据本地策略查看UE是否刚被鉴权过或者举例上次UE鉴权成功的时间间隔是否在有效期内,如果不在有效期内,则确定需要对UE进行鉴权。示例的,该消息为Nausf_UEAuthentication_Authenticate Request message。

步骤302.在需要对终端进行鉴权的情况下,AUSF获取鉴权材料。

10 需要说明的是,本实施例中,“获取”可理解为“主动获取”,包括但不限于AUSF主动从本地存储的上下文中获取或主动发起鉴权材料获取请求消息。可以理解的,“获取”亦可理解为AUSF可直接地或间接地从第四功能网元接收鉴权材料,第四功能网元为存储或生成鉴权材料的功能网元。

其中,鉴权材料是直接地或者间接地用于生成鉴权向量的材料。鉴权材料包括但不限于
15 于以下的一种或多种:服务网络名称(serving network name,SN name),服务网络标识(serving network identifier,SN ID),网络标识符(Network identifier,NID),MCC或MNC。

示例的,当鉴权材料为SN Name,SN Name可以直接用于生成鉴权向量。其中,SN Name是由SN ID生成的。比如,SN Name可以由SN ID与字符串“5G”使用“:”进行拼接得到:5G:SN ID。SN ID的格式可以是MCC与MNC拼接得到。网络标识符用于标识UE所在的网络。本实施例不限制SN Name的生成方法,也不限制SN ID的具体格式。

示例的,当鉴权材料为MCC和MNC,AUSF可以根据MCC和MNC得到SN Name。该SN Name最终用于获取鉴权向量。具体地,AUSF可以从UE的永久身份SUPI中获取
25 MCC和MNC。

示例的,当鉴权材料为MCC和MNC,AUSF可以使用MCC和MNC先获取SN ID,再使用SN ID与“5G”进行拼接,最终得到SN Name。

示例的,当鉴权用于私网场景时,则AUSF可以根据鉴权所在的场景构造出鉴权材料。例如,如果SN Name需要NID组成,那么AUSF可以从本地存储获取SUPI对应的NID。

30 在一种实现方式中,AUSF从本地存储的上下文中获取对UE进行鉴权所需的鉴权材料。例如,前一次鉴权中AMF发送AUSF的鉴权请求消息包括SN_name,将该SN_name存储在本地的上下文中。

在另一种实现方式中,AUSF从第四功能网元获取鉴权材料。其中,第四功能网元为存储鉴权材料的功能网元。

35 在一种具体实现方式中,第四功能网元为AMF,AUSF向UDM发送AMF ID请求消息。该AMF ID请求消息用于向UDM请求为UE服务的AMF信息。

该AMF ID请求消息携带需要鉴权的UE的用户的永久身份SUPI。

可选地,该AMF ID请求消息携带指示信息,该指示信息用于指示该请求消息是用于请求为UE服务的AMF ID。

可选地，该 AMF ID 请求消息本身就可以触发 UDM 知晓该消息的作用是用于请求为 UE 服务的 AMF ID。比如，该消息为 Nudm_UECM Request 消息，或者 Nudm_UEAuthentication Get Request 消息，或者 Nudm_HNAAuthentication Get Request 消息。其中，HNAAuthentication 代表家乡网络鉴权服务。该家乡网络鉴权服务在不同实施例中可以是不同网元使用的服务。比如，该家乡网络鉴权服务可以是 AMF 的服务。再比如，他

5 可以是 AUSF 的服务。再比如，他可以是 UDM 的服务。本实施例不做限定。

相应地，UDM 接收该 AMF ID 请求消息，根据 SUPI 确定 AMF ID 后，发送 AMF ID 响应消息给 AUSF。其中，该 AMF ID 响应消息中携带 AMF ID。该 AMF ID 响应消息为 Nudm_UECM Response 消息，或者 Nudm_UEAuthentication Get Response 消息，或者

10 Nudm_HNAAuthentication Get Response 消息。

AUSF 根据 AMF ID 确定 AMF，向该 AMF 发送 SN Name 获取请求消息。该 SN Name 获取请求消息用于获取鉴权材料，例如 SN Name。该 SN Name 获取请求消息中携带所述 SUPI。该 SN Name 获取请求消息为 Namf_UEAuthentication_Authenticate 消息，或者 Nausf_UEAuthentication_Authenticate Request 消息，或者

15 Nausf_HNAAuthentication_Authenticate Request 消息，或者 Namf_HNAAuthentication_Authenticate Request 消息，或者 Namf_HNAAuthentication_Get Request 消息。

AMF 在收到所述 SN Name 获取请求消息后，确定为该 SUPI 服务，则发送 SN Name 至 AUSF。

可选地，AMF 可通过响应于该 SN Name 获取请求消息的响应消息发送 SN Name 至 AUSF。比如，该响应消息为 Namf_UEAuthentication_Authenticate Response，或者 Nausf_UEAuthentication_Authenticate Response 消息，或者 Nausf_HNAAuthentication_Authenticate Response 消息，或者 Namf_HNAAuthentication_Authenticate Response 消息，或者 Namf_HNAAuthentication_Get

20 Response 消息。

可选地，该消息中还携带 SUPI。

可选地，AMF 也可以通过 AUSF 鉴权请求消息发送该 SN Name，比如，该消息为 Nausf_UEAuthentication_Authenticate Request。此时，该消息中还携带 SUPI。

上述过程可以理解的，在 AUSF 确定对终端进行鉴权的情况下，AUSF 向第四功能网元发送获取请求消息以获取鉴权材料，第四功能网元响应于该获取请求消息，将存储或生成的鉴权材料发送给 AUSF。

30

步骤 303. AUSF 根据鉴权材料，获取第一鉴权向量。

AUSF 根据鉴权材料从 UDM 获取第一鉴权向量。具体的，AUSF 发送鉴权材料至 UDM，UDM 根据鉴权材料生成第一鉴权向量再将该第一鉴权向量发送至 AUSF。在一种实现方式中，该步骤包括：

35

步骤 303a: AUSF 向 UDM 发送鉴权向量请求消息。该鉴权向量请求消息包括鉴权材料和 SUPI。具体的，鉴权材料可以为 SN_name。可选地，鉴权向量请求消息还携带有指示信息，指示信息指示获取 SUPI 的第一鉴权向量。

该鉴权向量请求消息为 Nudm_UEAuthentication_Get Request 消息，或者

Nudm_HNAuthentication Get Request 消息，或者 Nausf_HNAuthentication_Authenticate Request 消息。该消息中携带鉴权材料和 UE 的永久身份。

步骤 303b: UDM 根据 SUPI 生成第一鉴权向量。

UDM 根据 SUPI 确定鉴权方法，并根据鉴权材料生成第一鉴权向量。

5 可选的，鉴权方法为 EAP-AKA'鉴权或 5G AKA。

若为 5G-AKA 鉴权方法，则第一鉴权向量包括随机数 RAND，第一认证令牌 AUTN，第一期望响应 XRES*和认证服务密钥 K_{AUSF}。

若为 EAP-AKA'鉴权方法，则第一鉴权向量包括随机数 RAND，第二认证令牌 AUTN，第二期望响应 RES*，加密密钥 CK 和完整性密钥 IK。

10 可以理解的是，鉴权方法可以有很多种，本实施例只是以 EAP-AKA'和 5G AKA 进行举例。本实施例不对鉴权方法和第一鉴权向量做限定。

步骤 303c: AUSF 接收来自 UDM 的鉴权向量响应消息，所述鉴权向量响应消息包括第一鉴权向量。

所述鉴权获取响应消息可以为 Nudm_UEAuthentication_Get 消息，或者

15 Nudm_HNAuthentication Get Response 消息，或者 Nausf_HNAuthentication_Authenticate Request 消息。本实施例不限制具体的消息名称。

可选的，所述鉴权获取请求响应还包括 SUPI。

步骤 304. AUSF 接收来自 UDM 的鉴权获取响应消息后，向 AMF 发送第一鉴权请求消息，该第一鉴权请求消息用于触发服务网络对 UE 进行鉴权。其中，第一鉴权请求消息
20 包括第二鉴权向量。可选地，还携带用户的永久身份标识。

第一鉴权请求消息用于告知 AMF 执行对 UE 进行鉴权的流程，是一条服务化请求消息。比如，该消息是 N_{AMF}_UEAuthentication_Request 消息，或者 Nausf_UEAuthentication Authenticate Reques 消息，或者 Nausf_UEAuthentication Authenticate Response 消息，
Namf_HNAuthentication_Authenticate Request 消息，或者

25 Nausf_HNAuthentication_Authenticate Request 消息。

当第一鉴权请求消息为 Namf_HNAuthentication_Authenticate Request 时，表示 AUSF 使用的是 AMF 的家乡网络鉴权服务，该第一鉴权请求消息的是家乡网络请求对 UE 进行鉴权的操作。此时，AMF 需要检查该第一鉴权请求消息是否来自于归属网络的功能网元。比如，AMF 检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM。如果是，则 AMF 处理该消息，执行步骤 305；如果不是，则丢弃该消息。
30

当第一鉴权请求消息为 Nausf_HNAuthentication_Authenticate Request 时，表示 AUSF 使用的是自己的服务，该第一鉴权请求消息的是家乡网络请求对 UE 进行鉴权的操作。此时，AMF 需要检查该第一鉴权请求消息是否来自于归属网络的功能网元。比如，AMF 检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM。如果是，则 AMF 处理该消息，执行步骤 305；如果不是，则丢弃该消息。
35

当第一鉴权请求消息为 N_{AMF}_UEAuthentication_Request 时，表示 AUSF 使用的是 AMF 的服务，该第一鉴权请求消息的是请求对 UE 进行鉴权的操作。此时，AMF 需要检查该第一鉴权请求消息是否来自于归属网络的功能网元。比如，AMF 检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM。如果是，则 AMF 处理该消息，执行步骤 305；如果

不是，则丢弃该消息。

当第一鉴权请求消息是 Nausf_UEAuthentication Authenticate Request 消息时，表明该消息是 AUSF 的 UEAuthentication 服务，并且该消息是一条请求消息。因为 Nausf_UEAuthentication 服务是现有 AUSF 服务，因此为了兼容现有技术，避免开发复杂度，因此可以重用该服务。但是需要说明的是，在现有技术中，AUSF 使用的是该 Nausf_UEAuthentication Authenticate 服务的响应消息，即 Nausf_UEAuthentication Authenticate Response 消息，将第二鉴权向量发送给 AMF。而本实施例使用的是 Nausf_UEAuthentication Authenticate 服务的请求消息。AMF 接收该第一鉴权请求消息并检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM，是则执行步骤 305，否则丢弃该第一鉴权请求消息并触发告警信息。

第一鉴权请求消息也可以为 Nausf_UEAuthentication Authenticate Response 消息，与现有技术不同之处在于该第一鉴权请求消息不是作为请求消息的响应消息。

其中，所述第一鉴权向量与所述第二鉴权向量可能相同也可能不同。

例如，若步骤 303 中采用鉴权方法为 5G-AKA，第一鉴权向量与第二鉴权向量不同，第二鉴权向量包括 RAND, AUTN, HXRES*；HXRES*由 XRES*变化得到。

例如，若步骤 303 中采用鉴权方法为 EAP-AKA'，第一鉴权向量和第二鉴权向量相同。第二鉴权向量包括 RAND，第二认证令牌 AUTN，第二期望响应 RES*，加密密钥 CK 和完整性密钥 IK。在此步骤中，通过 AUSF 向 AMF 发起第一鉴权请求消息作为触发对 UE 进行鉴权的起点，执行后续的 UE 鉴权流程。而前述的鉴权方法中，由 AMF 作为触发对 UE 进行鉴权的起点。

AUSF 将 RES*保存在本地，作为保存的鉴权响应。

步骤 305. AMF 发送第二鉴权请求消息至 UE。

AMF 接收第一鉴权请求消息后，向该 UE 发送第二鉴权请求消息。其中，第二鉴权请求消息包括第二鉴权向量中的全部或部分参数。

具体地，可选地，在发送第二鉴权请求消息前，AMF 先确定该 AMF 仍然在为该 UE 服务。

在一种实现方式中，第二鉴权请求消息是 Authentication Request。

在另一种实现方式中，第二鉴权请求消息为 DL(Downlink)NAS Transport NAS 消息，用于传递第二鉴权向量。其中，第二鉴权向量携带有指示信息，用于指示 UE 该消息传递的是用于对 UE 进行鉴权的参数。该指示信息可以是二进制比特位信息，或者字符串指示信息。比如，当消息携带“authentication”时，则 UE 知道该 DL NAS Transport NAS 是为触发双向鉴权。

步骤 306. UE 根据接收的第二鉴权请求消息中携带的参数验证网络是否为真实的。当 UE 确定网络是真实的，UE 向 AMF 发送第二鉴权响应消息。其中，第二鉴权响应消息携带鉴权响应 RES*。

在一种实现方式中，第二鉴权响应消息是 Authentication Response。

在另一种实现方式中，第二鉴权请求消息为 UL(Uplink) NAS Transport NAS 消息。

步骤 307. AMF 接收到第二鉴权响应消息后，向 AUSF 发送响应于第一鉴权请求消息对应的第一鉴权响应消息，第一鉴权响应消息包括所述鉴权响应。

相应地, 该第二鉴权响应消息为 N_{AMF}_UEAuthentication_Response 消息, 或者 Nausf_UEAuthentication Authenticate Response 消息, 或者 Nausf_UEAuthentication Authenticate Request, 或者 Nausf_HNAuthentication_Authenticate Response 消息, 或者 Namf_HNAuthentication_Authenticate Response 消息。N_{AMF}_UEAuthentication 服务和 Nausf_UEAuthentication 参考步骤 304 中的相关描述。

步骤 308. AUSF 对 UE 进行鉴权。具体地, AUSF 将该鉴权响应与本地保存的鉴权响应比较, 若一致则认为 UE 鉴权成功。

步骤 305-步骤 308 根据所述第二鉴权向量确定 UE 鉴权成功的具体方法可以参考 3GPP 标准 TS 33.501 章节 6.1 中的相关描述。在此不再赘述。

步骤 301-步骤 308 中描述的鉴权方法, AUSF 响应于本地策略或者第三功能网元请求确定需要对终端进行鉴权的情况下, AUSF 主动从本地存储的上下文或者第四功能网元获取鉴权材料, 并进一步获取根据鉴权材料生成的鉴权向量后, 发送第一鉴权请求消息至 AMF 以触发对 UE 的鉴权。不同于前述方法中 AMF 发起鉴权流程的是, 本实施例中鉴权流程的发起点是在归属网络的 AUSF, 而不是来自 AMF 的请求。这样, AUSF 不再依赖 AMF 的请求才可以触发对 UE 进行鉴权, 减少了 AMF 与 AUSF 的信令交互。

可选地, 在步骤 301 中当 AUSF 接收第三功能网元的参数请求, 根据第三功能网元的参数请求消息确定对 UE 进行鉴权时, 需要返回该参数至该第三功能网元。

如果在该步骤 301 中, AUSF 接收来自第三功能网元的服务参数请求消息, AUSF 还需回复参数响应消息至第三功能网元。AUSF 还需回复参数响应消息至第三功能网元存在以下三种情况:

第一种情况, AUSF 直接发送参数响应消息给第三功能网元。该参数响应消息携带请求的参数或者鉴权结果。

示例的, 当第三功能网元是 AAnF, 并且参数请求消息用于请求一个新的 K_{AKMA} 密钥时, 则 AUSF 在对 UE 鉴权成功后, 使用该鉴权过程中生成的 K_{AUSF} 生成新的 K_{AKMA} 密钥, 并将新的 K_{AKMA} 密钥携带在该参数响应消息。

示例的, 当第三功能网元是 UDM, 并且 UDM 向 AUSF 发送的参数请求消息是请求对 SoR 或者 UPU 保护。AUSF 确定对 UE 进行鉴权, 在鉴权成功后, AUSF 利用新生成的 K_{AUSF} 对 SoR 数据或者 UPU 数据做安全保护, 之后将安全保护的结果通过该参数响应消息发送给 UDM。

示例的, 当第三功能网元是 UDM 时, 参数请求消息用于请求新 K_{AKMA} 时, 在 AUSF 决定对 UE 进行鉴权。AUSF 在对 UE 鉴权成功后, 使用该鉴权过程中生成的 K_{AUSF} 生成新的 K_{AKMA} 密钥, 之后将新的 K_{AKMA} 密钥通过返回参数消息发送给 UDM。如果 UDM 是从第四功能网元, 比如 AAnF 收到的请求更新 K_{AKMA} 时, UDM 要进一步地将收到的新的 K_{AKMA} 密钥发送给该 AAnF。

示例的, 当第三功能网元是 3GPP 内部 AF, 或者用于 3GPP 外部 AF 使用的 NEF。参数请求消息用于请求对 UE 进行鉴权。AUSF 决定对 UE 进行鉴权。在鉴权成功后, AUSF 发送返回参数消息发送给 UDM。可选地, 该消息中携带鉴权结果。

示例的, 当第三功能网元是 UDM, UDM 接收第四功能网元的请求消息用于请求对 UE 进行鉴权。AUSF 确定对 UE 进行鉴权。在鉴权成功后, AUSF 发送返回参数消息发送

给 UDM。可选地，该返回参数消息中携带鉴权结果。UDM 要进一步地将鉴权结果告知第四功能网元。

第二种情况，AUSF 发送参数响应消息给第三功能网元，该返回响应消息用于告知第三功能网元参数请求消息收到。AUSF 在对 UE 鉴权成功后，AUSF 直接发送参数消息请求的参数，或者鉴权结果发送给第四功能网元，或者与第四功能网元同类型的网元。

第一种示例为，当第三功能网元是 UDM 时，并且 UDM 向 AUSF 发送请求对 SoR 数据或者 UPU 数据进行保护的请求消息。AUSF 在接收到该请求消息后，因本地存储的 K_{AUSF} 失效或即将失效，或者本地没有存储 K_{AUSF} ，则确定对 UE 进行鉴权。同时，AUSF 向 UDM 发送参数响应消息。该参数响应消息用于告知 UDM 请求失败。可选地，返回参数消息中携带原因值，原因值用于告知 UDM 没有密钥 K_{AUSF} 或者 K_{AUSF} 失效或即将失效。UDM 可以在后续流程中可以重新发起该请求，比如在之后，UDM 确定对 UE 鉴权成功后。本实施例不限制 AUSF 决定对 UE 进行鉴权和 AUSF 回复失败消息的先后顺序，也不限制 UDM 如何确定 UE 鉴权成功。

第二种示例为，当第三功能网元是 UDM，请求消息用于请求更新 K_{AKMA} 时。AUSF 可在收到该请求消息后，AUSF 确定对 UE 进行鉴权。同时，AUSF 也向 UDM 发送返回参数消息。该参数响应消息用于告知 UDM 接收到参数请求消息。AUSF 在对 UE 鉴权成功后，使用该鉴权过程中生成的 K_{AUSF} 生成新的 K_{AKMA} 密钥，并将新的 K_{AKMA} 密钥直接发送给 AAnF。该 AAnF 可以是向该 UDM 请求密钥 K_{AKMA} 的 AAnF，也可以是其他 AAnF。如果 UDM 在参数请求消息中携带了 AAnF ID，则 AUSF 可以发送 K_{AUSF} 给该 AAnF ID 对应的 AAnF。本实施例不限制 AUSF 决定对 UE 进行鉴权和参数响应消息的先后顺序。

第三种示例为，当第三功能网元是 UDM 时，UDM 接收第四功能网元的请求消息用于请求对 UE 进行鉴权。AUSF 决定对 UE 进行鉴权。在鉴权成功后，AUSF 发送返回参数消息发送给 UDM，该返回参数消息用于告知 UDM 接收到参数请求消息。

参考图 4 所示，本申请提供另一种由归属网络的功能网元触发鉴权的方法，与图 3 所示方法的不同之处在于，在本实施中，UDM 获取鉴权材料。该方法包括但不限于：

步骤 401. AUSF 确定是否需要到 UE 进行鉴权。

该步骤可参考步骤 301，在此不再赘述。

步骤 402. 在确定需要对终端进行鉴权的情况下，AUSF 向 UDM 发送获取请求消息，该获取请求消息用于获取第一鉴权向量。其中，该获取请求消息包括 SUPI。

可选地，该获取请求消息还包括指示信息，所述指示信息用于指示 UDM 需要对 UE 进行鉴权。指示信息可以是比特位指示信息，也可以是一个预先确定的 SN-Name 值。比如 SN-Name 的比特位为全 0 或者全 1。

示例的，该获取请求消息为 Nudm_UEAuthentication_Get Request message，为或者 Nudm_HNAuthentication Get Request 消息。

步骤 403. UDM 接收该获取请求消息后，获取鉴权材料。

可选地，在 UDM 接收该获取请求消息后，获取鉴权材料前，UDM 确定该 UE 需要鉴权。具体地，可以参考后文步骤 501 的相关描述。

UDM 可以直接根据本地存储的信息获得鉴权材料，或者 UDM 可以从第四功能网元获取鉴权材料。例如，第四功能网元为 AMF。

在一种实现方式中,UDM 本地存储鉴权材料,UDM 从本地存储获取鉴权材料。例如,前一次鉴权中使用的 SN_name 存储在 UDM 本地的上下文中。

再比如,UDM 根据本地存储的与 SUPI 对应的上下文确定为 UE 服务的服务网络信息,比如,AMF ID 或者 PLMN ID。从该服务网络信息中获取 MCC 和 MNC,根据 MCC 和 MNC 生成 SN Name。

在另一种实现方式中,UDM 从第四功能网元获取鉴权材料。其中,第四功能网元为存储鉴权材料的功能网元。

在一种具体实现方式中,第四功能网元为 AMF,UDM 从 SUPI 对应的上下文中获取正在为 UE 服务的 AMF 信息,比如 AMF ID。UDM 根据 AMF ID 确定 AMF,向该 AMF 发送 SN Name 获取请求消息。该 SN Name 获取请求消息用于获取鉴权材料,例如 SN Name。该 SN Name 获取请求消息中携带所述 SUPI。该 SN Name 获取请求消息为 Namf_UEAuthentication_AuthenticateRequest 消息,或者 Namf_HNAAuthentication_Get Request 消息。

AMF 在收到所述 SN Name 获取请求消息后,确定为该 SUPI 服务,则发送 SN Name 至 AUSF。

可选地,AMF 可通过响应于该 SN Name 获取请求消息的响应消息发送 SN Name 至 AUSF。比如,该响应消息为 Namf_UEAuthentication_Authenticate Response,或者 Nausf_UEAuthentication_Authenticate Response 消息,或者 Namf_HNAAuthentication_Get Response 消息。可选地,该消息中还携带 SUPI。

可选地,AMF 也可以通过 AUSF 鉴权请求消息发送该 SN Name,比如,该消息为 Nausf_UEAuthentication_Authenticate Request。此时,该消息中还携带 SUPI。

上述过程可以理解的,UDM 向第四功能网元发送获取请求消息以获取鉴权材料,第四功能网元响应于该获取请求消息,将存储或生成的鉴权材料发送给 UDM。

上述过程可以理解的,UDM 向第四功能网元发送获取请求消息以获取鉴权材料,第四功能网元响应于该获取请求消息,将存储或生成的鉴权材料发送给 UDM。

步骤 404.UDM 根据获取的鉴权材料生成第一鉴权向量。

UDM 根据 SUPI 确定鉴权方法,并根据鉴权材料生成第一鉴权向量。

步骤 405.UDM 向 AUSF 发送获取响应消息,所述获取响应消息包括第一鉴权向量。该步骤可参考步骤 303c,在此不再赘述。

步骤 406.AUSF 接收来自 UDM 的鉴权获取响应消息后,向 AMF 发送第一鉴权请求消息,该消息用于触发对 UE 进行鉴权。其中,第一鉴权请求消息包括第二鉴权向量。可选地,还携带用户的永久身份标识。

该步骤可参考步骤 304,在此不再赘述。

步骤 407-步骤 409 执行后续的鉴权流程,其实现后续鉴权流程的方法与步骤 305-308 相同,这里不再赘述。

参考图 5 所示,本申请提供的另一种由归属网络的功能网元触发鉴权的方法,在该方法中第一功能网元为 UDM,该方法包括但不限于:

步骤 501.UDM 确定是否需要 UE 进行鉴权。

UDM 根据本地策略或第三功能网元的请求确定是否需要 UE 进行鉴权。其中,第

三功能网元为除 UDM 以外的核心网网元。

在一种实现方式中，UDM 根据本地策略确定是否需要 UE 进行鉴权。

可选地，本地策略可以包括：UDM 根据本地是否存储有 AUSF ID 来确定是否需要 UE 进行鉴权。当 UDM 要发送漫游指导（Steering of roaming, SoR）数据或者 UPU 数据给 UE，但是 UDM 没有存储对应的 AUSF ID 时，UDM 无法找到对应的 AUSF 为 SoR 数据或者 UPU 数据提供安全保护，则 UDM 确定需要对 UE 进行鉴权。即，在 UDM 确定本地没有存储 AUSF ID 的情况下，UDM 决定对 UE 进行鉴权。

可选地，本地策略可以包括：UDM 根据 UE 是否被 5G 网络鉴权来确定是否需要 UE 进行鉴权。比如，UE 首次接入的是 4G 核心网，后来，在有 5G 网络覆盖的情况下，UE 从 4G 网络移动到 5G 网络，并开始使用 5G 网络。根据现有标准，该过程中，AMF 是可以不发起鉴权的。也就是说，UE 在接入 5G 网络后，并没有被 5G 网络鉴权过。因此，UDM 可以根据 UE 未被 5G 网络鉴权过，来确定对 UE 进行鉴权。

可选地，本地策略可以包括：UDM 根据距离前一次鉴权成功的时间间隔是否满足预设值，确定是否需要 UE 进行鉴权。若 UDM 发现前一次对 UE 鉴权成功的时间间隔超过或即将超过运营商策略规定时间，则 UDM 确定需要对 UE 进行鉴权。具体的，可通过一个计时器记录距离前一次对 UE 鉴权成功的时间间隔，该计时器与 UE 的永久身份 SUPI 绑定。当 AUSF 确定 UE 鉴权成功后，计时器开始计时，当该计时器记录的时间间隔超过或即将超过预设间隔值时，AUSF 确定需要对 UE 进行鉴权。

在又一种实现方式中，UDM 接收来自第三功能网元的参数请求消息，该参数请求消息用于向 UDM 请求参数，或者请求 UDM 为 UE 进行鉴权。该参数请求消息至少包括用户的永久身份。

比如，参数请求消息可以用于请求 K_{AKMA} 。再比如，参数请求消息是请求发送 SoR 数据或者 UPU 数据的保护消息的响应消息，该响应消息用于表示请求失败。AUSF 在接收参数请求消息后，因为本地存储的 K_{AUSF} 失效或即将失效，或者本地没有存储 K_{AUSF} ，则回复响应消息告知 UDM 请求失败。

第三功能网元为除 UDM 以外的核心网功能网元。该第三功能网元为 AAnF，AUSF，或者 AF 等功能网元。

示例的，当第三功能网元是 AAnF 时，AAnF 向 UDM 发送 K_{AKMA} 更新请求消息。该 K_{AKMA} 更新请求消息用于请求一个新的 K_{AKMA} 密钥。AUSF 确定需要更新 K_{AKMA} 则确定需要对 UE 进行鉴权。具体的，该 K_{AKMA} 更新请求消息为 Nudm_AKMA_AnchorKey_Refresh message。

示例的，当第三功能网元是 AUSF 时，AUSF 向 UDM 发送 SoR 数据或者 UPU 数据保护失败的结果。比如，该消息为 Nausf_SoRProtection Response 消息，或者 Nausf_UPUProtection Response message。当 UDM 收到该消息时，UDM 确定需要对 UE 进行鉴权。可选地，Nausf_SoRProtection Response 消息，或者 Nausf_UPUProtection Response 消息携带失败原因值。比如，失败原因值用于指示没有密钥 K_{AUSF} 。UDM 根据失败原因值确定需要对 UE 进行鉴权。

示例的，当第三功能网元是 AUSF 时，AUSF 接收来自第四功能网元的请求消息，比如来自 AAnF 的 K_{AKMA} 更新请求消息，AUSF 向 UDM 发送参数请求消息。此时，参数请

求消息用于请求对 UE 进行鉴权。UDM 根据该参数请求消息确定需要对 UE 进行鉴权。具体的，参数请求消息为 Nudm_UEAuthentication Get Request message。

示例的，当第三功能网元是 AUSF 时，AUSF 接收来自第四功能网元的请求消息，比如来自 NEF 或者 3GPP 内部 AF 请求更新 K_{AF} 时，AUSF 会向 UDM 发送请求消息，UDM 确定需要更新 K_{AF} 对应的 K_{AKMA} 时，则确定需要对 UE 进行鉴权。具体的，该请求消息为 Nudm_UEAuthentication Get Request message。

示例的，当第三功能网元是 NEF 或者 3GPP 内部的 AF，AF 或者 NEF 向 UDM 发送请求消息。此时，该请求消息用于请求更新 K_{AF} 。UDM 确定需要更新 K_{AF} 对应的 K_{AKMA} 时，则确定需要对 UE 进行鉴权。比如，该消息为 Nudm_UEAuthentication Authenticate Request 消息。

示例的，当第三功能网元是 AUSF，AUSF 接收来自第四功能网元的鉴权请求消息，例如来自 NEF 或者 3GPP 内部的 AF 的鉴权请求消息，具体的，该鉴权请求消息为 Nausf_UEAuthentication_Authenticate Request 消息。之后，AUSF 向 UDM 发送用于请求对 UE 进行鉴权的请求消息，UDM 根据该请求消息确定需要对 UE 进行鉴权。具体的，该鉴权请求消息为 Nudm_UEAuthentication Get Request 消息。

在又一种实现方式中，UDM 可以根据本地策略和第三功能网元的请求综合判断是否需要鉴权。一个示例为，当第三功能网元是 AUSF 时，AUSF 向 UDM 发送参数请求消息。此时，参数请求消息用于请求对 UE 进行鉴权。比如，该参数请求消息为 Nausf_UEAuthentication_Authenticate Request。UDM 在收到该参数请求消息后，UDM 根据本地策略进一步判断是否对 UE 进行鉴权。比如，本地策略为距离前一次鉴权成功的时间间隔是否超过或即将超过运营商策略所规定的时间来确定是否需要鉴权。若距离前一次鉴权成功的时间间隔小于预设值，则确定不对 UE 进行鉴权；距离前一次鉴权成功的时间间隔超过预设值，则确定对 UE 进行鉴权。

步骤 502. 在需要对终端进行鉴权的情况下，UDM 获取鉴权材料。

需要说明的是，本实施例中，“获取”可理解为“主动获取”，包括但不限于 UDM 主动从本地存储或主动发起获取鉴权材料的请求消息。可以理解的，“获取”亦可理解为 UDM 可直接地或间接地从第四功能网元接收鉴权材料，第四功能网元为存储有或者能生成鉴权材料的功能网元。

鉴权材料的相关描述参考步骤 302 的相关描述，在此不再赘述。

UDM 获取鉴权向量的描述参考步骤 403 的相关描述，再次不再赘述。

在一种实现方式中，UDM 从本地存储的上下文中直接获取对 UE 进行鉴权所需的鉴权材料。例如，前一次鉴权中存储在 UDM 本地上下文中的 SN_name。

在另一种实现方式中，UDM 从本地存储的上下文中间接地获取对 UE 进行鉴权所需的鉴权材料，即根据本地存储的上下文生成鉴权材料。比如，当鉴权材料是 SN Name 时，UDM 可以根据 UE 的永久身份 SUPI 中获取 MCC 和 MNC，使用 MCC 和 MNC 生成 SN Name。再比如，当鉴权材料是 SN Name 时，UDM 可以使用存储的 SUPI 对应的 PLMN ID 中，获取 MCC 和 MNC，再使用 MCC 和 MNC 进一步获得 SN Name。再比如，当鉴权用于私网景时，则 UDM 可以根据鉴权所在的场景构造出鉴权材料。例如，如果 SN Name 需要 NID 组成，那么 UDM 可以从本地存储的上下文获取 SUPI 对应的 NID。使用 MCC

和 MNC 获得 SN Name 的方法可以参考步骤 302 中的项目描述, 在此不再赘述。

在另一种实现方式中, UDM 直接从第四功能网元获取对 UE 进行鉴权所需的鉴权材料。其中, 第四功能网元为存储鉴权材料的功能网元。

5 可选地, 当第四功能网元为 AMF 时, UDM 从 SUPI 对应的上下文中获取正在为 UE 服务的 AMF 信息, 比如 AMF ID。UDM 根据 AMF ID 确定 AMF, 向 AMF 发送第一请求消息。该第一请求消息携带需要鉴权的 UE 的用户的永久身份 SUPI。

10 可选地, 该第一请求消息为 Namf_UEAuthentication_Authenticate 消息, 或者 Nudm_SDM_Get_Response 消息, 或者 Namf_HNAAuthentication_Get Request 消息。AMF 在收到第一请求消息后, 回复第一响应消息, 第一响应消息携带鉴权材料。示例的, 鉴权材料是 SN Name。具体的, 该第一响应消息为 Namf_UEAuthentication_Authenticate Response message, 或者 Nudm_SDM_Info message, 或者 Namf_HNAAuthentication_Get Response 消息。

15 在另一种实现方式中, UDM 在确定需要对 UE 进行鉴权后, UDM 向第五功能网元发送第一请求消息, 该第一请求消息携带需要鉴权的 UE 的用户永久身份 SUPI。第一请求消息用于请求服务网络对 UE 进行鉴权。

可选地, UDM 可以在本地没有存储 AUSF ID 的情况下, 向第五功能网元发送第一请求消息。

20 可选地, UDM 知晓鉴权材料存储在第五功能网元, UDM 向第五功能网元发送第一请求消息, 但是 UDM 从第四功能网元获取对 UE 进行鉴权所需的鉴权材料。具体地, 第五功能网元响应于第一请求消息, 向第四功能网元发送第二鉴权请求消息, 所述第二鉴权请求消息携带鉴权材料。示例的, 第四功能网元是 AUSF, 第五功能网元是 AMF。第一请求消息为 Namf_UEAuthentication_Authenticate 消息, 或者 Nudm_SDM_Get_Response 消息, 或者 Namf_HNAAuthentication_Get Request 消息; AMF 在收到 Namf_UEAuthentication_Authenticate 消息, 或者 Nudm_SDM_Get_Response 消息, 或者 25 Namf_HNAAuthentication_Get Request 消息后, AMF 向 AUSF 发送第二鉴权请求消息, 第二鉴权请求消息为 Nausf_UEAuthentication_Authenticate Request 消息。所述 Nausf_UEAuthentication_Authenticate Request 消息中携带有 SN Name 和 SUPI。AUSF 在收到 Nausf_UEAuthentication_Authenticate Request 消息后, AUSF 向 UDM 发送 Nudm_UEAuthentication Get Request。该 Nudm_UEAuthentication Get Request 消息中携带 30 SUPI 和 SN Name。需要说明的是, 该方法可以发生在以下情况中: UDM 在确定对 UE 进行鉴权, 但是本地没有存储 AUSF ID 的情况下。UDM 只能根据本地存储的 SUPI 对应的 AMF 信息, 比如 AMF ID, 向为 UE 服务的 AMF 请求对 UE 进行鉴权。那么 AMF 在收到请求消息后, 根据 SUPI 选择一个 AUSF, 并开始执行步骤 201 至步骤 208 所述流程。

35 可选地, 第五功能网元在收到第一请求消息后, 回复第一响应消息至 UDM。该第一响应消息用于告知 UDM 收到第一请求消息。该第一响应消息可以不携带任何内容。比如, 第一响应消息为 Namf_UEAuthentication_Authenticate Response 消息, 或者 Nudm_SDM_Info 消息。本实施例不限制第五功能网元发送第一响应消息和第二鉴权请求消息的顺序。

本实施例不限制鉴权材料的获取方法。本实施例不对消息名称做限定。

步骤 503. UDM 根据鉴权材料生成第一鉴权向量。

参考步骤 303, 在此不再赘述。

步骤 504. UDM 生成第一鉴权向量后, 向 AUSF 发送第一消息。相应的, AUSF 接收第一消息。其中, 第一消息包括第一鉴权向量

5 可选地, 还可能包括用户身永久份标识。

在一种可能的实现方法中, 在 UDM 没有收到 AUSF 鉴权获取请求消息的情况下, UDM 先根据本地存储的 AUSF ID 确定 AUSF, 再向所述 AUSF 发送第一消息。比如, UDM 根据本地存储获取鉴权材料或者从 AMF 直接获得鉴权材料, 并且 UDM 根据本地策略决定 UE 需要鉴权。第一消息是 Nudm_UEAuthentication Get Request 或者

10 Nausf_UEAuthentication_Authenticate Request 或者 Nausf_HNAuthentication_Authenticate Request。

在另一种可能的实现方法中, UDM 根据接收的第三功能网元的请求消息确定需要对 UE 进行鉴权, 且该第三功能网元不是 AUSF 的情况下, 第一消息是 Nudm_UEAuthentication Get Request 或者 Nausf_UEAuthentication_Authenticate Request 或者

15 Nausf_HNAuthentication_Authenticate Request。

在另一种可能的实现方法中, UDM 根据接收的第三功能网元的请求消息确定需要对 UE 进行鉴权, 且该第三功能网元不是 AUSF 的情况下, UDM 向 AMF 发送第三鉴权请求消息, 第三鉴权请求消息用于告知 AMF 执行对 UE 进行鉴权的流程, 是一条服务化请求消息。比如, 该消息是 N_{AMF}_UEAuthentication_Request 消息, 或者 Nudm_UEAuthentication Authenticate Reques 消息, 或者 Nudm_UEAuthentication Authenticate Response 消息, 或者 Namf_HNAuthentication_Authenticate Request 消息。

当第三鉴权请求消息为 Namf_HNAuthentication_Authenticate Request 时, 表示 UDM 使用的是 AMF 的家乡网络鉴权服务, 该第一鉴权请求消息的是家乡网络请求对 UE 进行鉴权的操作。此时, AMF 需要检查该第一鉴权请求消息是否来自于归属网络的功能网元。比如, AMF 检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM。如果是, 则 AMF 处理该消息, 执行步骤 506; 如果不是, 则丢弃该消息。

当第三鉴权请求消息为 N_{AMF}_UEAuthentication_Request 时, 表示 UDM 使用的是 AMF 的服务, 该第一鉴权请求消息的是请求对 UE 进行鉴权的操作。此时, AMF 需要检查该第一鉴权请求消息是否来自于归属网络的功能网元。比如, AMF 检查该第一鉴权请求消息是否来自于 AUSF 或者 UDM。如果是, 则 AMF 处理该消息, 执行步骤 506; 如果不是, 则丢弃该消息。

当第三鉴权请求消息是 Nudm_UEAuthentication Authenticate Request 消息时, 表明该消息是 UDM 的 UEAuthentication 服务, 并且该消息是一条请求消息。

UDM 向 UE 发送第三鉴权请求消息后, AMF 开始执行步骤 201, UDM 可以在步骤 35 202 中收到 AUSF 的请求消息。该鉴权获取请求消息可以是 Nudm_UEAuthentication Get Request 消息。所述鉴权获取响应消可以是 Nudm_UEAuthentication Get Response 消息。

在另一种可能的实现方式中, 在 UDM 接收到 AUSF 发送的鉴权获取请求消息的情况下, UDM 响应于该鉴权获取请求消息, 回复第一消息给该 AUSF, 此时, 第一消息为鉴权获取响应消息。

本实施例不对具体的消息名称做限定。

步骤 505. AUSF 向 AMF 发送第一鉴权请求消息，第一鉴权请求消息用于触发对 UE 进行鉴权。第一鉴权请求消息包括第一鉴权向量。可选地，第一鉴权请求消息还携带用户永久身份标识。

5 参考步骤 304 相关描述，在此不再赘述。步骤 506-步骤 508 执行后续的鉴权流程，其实现后续鉴权流程的方法与步骤 305-308 相同，这里不再赘述。

此外，若步骤 501 中 UDM 收来自第三功能网元的服务参数请求消息的情况下，所述 UDM 还需回复参数响应消息给第三功能网元。若第三功能网元是 AUSF，则参数响应消息可以是鉴权获取响应消息，或者一条单独的，用于告知收到的消息。若第三功能网元是 AAnF 或者 AF，或者外部 AF 使用的 NEF，并且参数请求消息是用于请求对 UE 的鉴权，
10 则参数响应消息可以用于告知消息收到，也可以用于传递鉴权结果的指示信息。用于告知第三功能网元鉴权成功还是失败。

需要说明的是，UDM 何时向外部网元发送参数请求响应本申请不做具体限制。

对应于上述方法实施例给出的方法，本申请实施例还提供了相应的装置，包括用于执行上述实施例相应的模块。所述模块可以是软件，也可以是硬件，或者是软件和硬件结合。
15

参见图 6，为本申请实施例提供的一种鉴权装置的结构示意图，该鉴权装置 600 包括：处理模块 610 和收发模块 620。所述收发模块 620 用于执行上述图 2-5 实施例中发送和接收消息相关的操作，处理模块 610 可以用于执行上述图 2-5 实施例中除了发送和接收消息以外相关的操作。

20 该通信装置可以作为 AUSF 网元，用于实现图 3 所示实施例中的鉴权方法。当该鉴权装置作为 AUSF 网元，执行图 3 中所示的方法实施例时，例如，处理模块 610 用于确定是否需要终端进行鉴权；在需要对所述终端进行鉴权的情况下，获取鉴权材料；根据所述鉴权材料获取鉴权向量；收发模块 620，可以用于向 AMF 发送第一鉴权请求消息以触发对终端进行鉴权，其中，第一鉴权请求消息包括所述鉴权向量。

25 当鉴权装置作为 UDM，执行图 5 中所示的方法实施例时，当该鉴权装置作为 UDM，执行图 5 中所示的方法实施例时，例如，处理模块 610 用于确定是否需要终端进行鉴权；在需要对所述终端进行鉴权的情况下，获取鉴权材料；根据所述鉴权材料获取鉴权向量；收发模块用于向 AMF 发送第一鉴权请求消息以触发对终端进行鉴权，其中，第一鉴权请求消息包括所述鉴权向量。

30 本实施例还提供另一种鉴权装置。如图 7 所示，该鉴权装置 700 包括处理器 710、存储器 720 和收发器 730。本申请实施例中不限定上述处理器 710 以及收发器 720 之间的具体连接介质。图 7 中以处理器 710 以及收发器 720 之间通过总线 730 连接为例，总线 740 在图中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线 740 可以分为地址总线、数据总线、控制总线等。为便于表示，图 7 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。
35

处理器 710 可以具有数据收发功能，能够与其他设备进行通信，在如图 7 所示的装置中，也可以设置独立的数据收发模块，例如收发器 730，用于收发数据；处理器 710 在与其他设备进行通信时，可以通过收发器 730 进行数据传输。

存储器中 720 存储指令或程序，处理器 710 用于执行存储器中存储的指令或程序。存

存储器中存储的指令或程序被执行时，该处理器 710 用于执行上述方法实施例中处理模块执行的操作，通信接口用于执行上述实施例中收发模块执行的操作。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各种说明性逻辑块（illustrative logical block）和步骤（step），能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以基于前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

在上述实施例中，各功能单元的功能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。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令（程序）。在计算机上加载和执行所述计算机程序指令（程序）时，全部或部分地产生按照本申请实施例所述的流程或功能。所述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。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机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。所述计算机可读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。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘（solid state disk，SSD））等。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存

取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

5 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种鉴权方法，其特征在于，所述方法包括：

归属网络的第一功能网元确定是否需要终端进行鉴权；

在需要对所述终端进行鉴权的情况下，所述第一功能网元获取鉴权材料；

5 所述第一功能网元根据所述鉴权材料，获取第一鉴权向量；

所述第一功能网元向接入和移动管理网元发送第一鉴权请求消息以触发对所述终端进行鉴权，其中，所述第一鉴权请求消息包括所述第一鉴权向量。

10 2、根据权利要求1所述的鉴权方法，其特征在于，所述第一功能网元确定是否需要终端进行鉴权，包括：

所述第一功能网元接收来自第三功能网元的服务请求，所述服务请求用于向所述第一功能网元请求指定服务；

响应于所述第三功能网元的服务请求，所述第一功能网元确定是否需要终端进行鉴权。

15 3、根据权利要求1所述的鉴权方法，其特征在于，所述第一功能网元为鉴权服务功能网元，所述第一功能网元获取所述鉴权材料，包括：

所述第一功能网元从存储的上下文中获取所述鉴权材料；

20 或者所述第一功能网元从第四功能网元获取所述鉴权材料，所述第四功能网元为存储有所述鉴权材料的网元。

4、根据权利要求3所述的鉴权方法，其特征在于，所述第一功能网元根据所述鉴权材料，获取第一鉴权向量，包括：

25 所述鉴权服务功能网元向统一数据管理网元发送鉴权向量请求消息，其中，所述鉴权向量请求消息包括所述鉴权材料；

所述鉴权服务功能网元接收来自所述统一数据管理网元的鉴权向量响应消息，所述鉴权向量响应消息包括所述第一鉴权向量。

30 5、根据权利要求1所述的鉴权方法，其特征在于，所述第一功能网元为统一数据管理网元，所述第一功能网元获取所述鉴权材料，包括：

所述第一功能网元从存储的上下文中获取所述鉴权材料；

或者，所述第一功能网元从第四功能网元获取所述鉴权材料，所述第四功能网元为存储有所述鉴权材料的网元。

35 6、根据权利要求5所述的鉴权方法，其特征在于，所述第一功能网元根据所述鉴权材料，获取第一鉴权向量，包括：

所述第一功能网元根据所述鉴权材料，生成所述第一鉴权向量。

7、根据权利要求 1-6 任一项所述的鉴权方法，其特征在于，所述鉴权材料包括以下一种或多种：服务网络名称，服务网络标识，网络标识符，移动国家码或移动网号。

8、一种通信装置，其特征在于，包括：

5 处理模块，用于确定是否需要终端进行鉴权；在需要对所述终端进行鉴权的情况下，获取鉴权材料；根据所述鉴权材料，获取第一鉴权向量；

收发模块，用于向接入和移动管理网元发送第一鉴权请求消息以触发对所述终端进行鉴权，其中，所述第一鉴权请求消息包括所述第一鉴权向量。

10 9、根据权利要求 8 所述的通信装置，其特征在于，所述处理模块，用于确定是否需要终端进行鉴权，具体为：

接收来自第三功能网元的服务请求，所述服务请求用于请求指定服务；

响应于所述服务请求，确定是否需要终端进行鉴权。

15 10、根据权利要求 8 所述的通信装置，其特征在于，所述处理模块，用于获取所述鉴权材料，具体为：

从存储的上下文中获取所述鉴权材料；

或者从第四功能网元获取所述鉴权材料，所述第四功能网元为存储有所述鉴权材料的网元。

20

11、根据权利要求 8 所述的通信装置，其特征在于，所述处理模块，用于根据所述鉴权材料，获取所述第一鉴权向量，具体为：

向统一数据管理网元发送鉴权向量请求消息，其中，所述鉴权向量请求消息包括所述鉴权材料；

25 接收来自所述统一数据管理网元的鉴权向量响应消息，所述鉴权向量响应消息包括所述第一鉴权向量。

12、根据权利要求 8 所述的通信装置，其特征在于，所述处理模块，用于根据所述鉴权材料，获取所述第一鉴权向量，具体为：

30 根据所述鉴权材料，生成所述第一鉴权向量。

13、根据权利要求 8-12 任一所述的通信装置，其特征在于，所述鉴权材料包括以下一种或多种：服务网络名称，服务网络标识，网络标识符，移动国家码或移动网号。

35 14、一种通信装置，其特征在于，包括：一个处理器，所述至少一个处理器执行用于执行存储在存储器中的指令，使得所述通信装置进行如权利要求 1-7 任一项所述的方法的操作。

15、一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得所述计算机

执行如权利要求 1-7 任一项所述的方法。

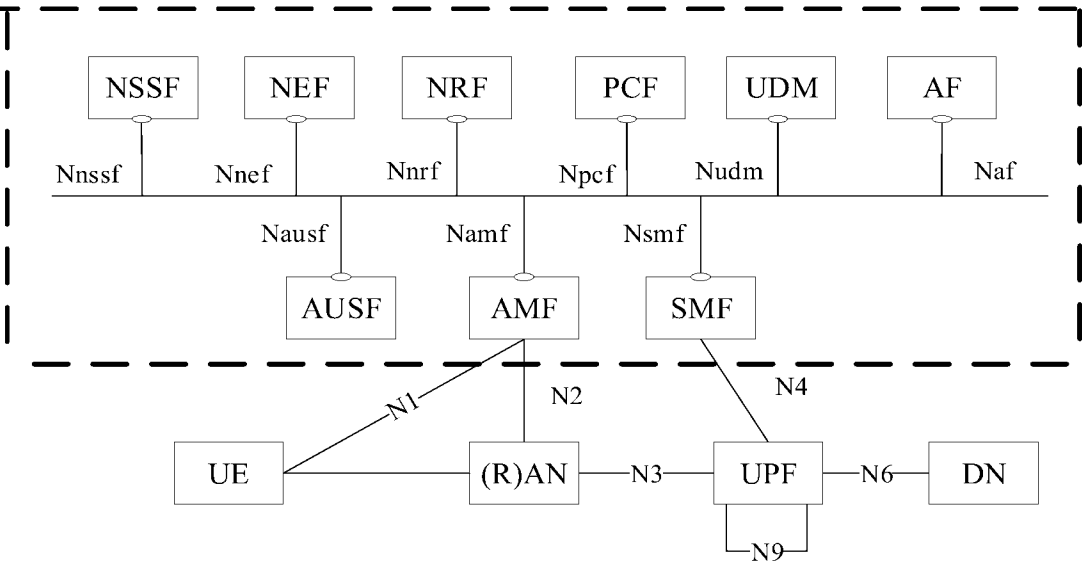


图 1

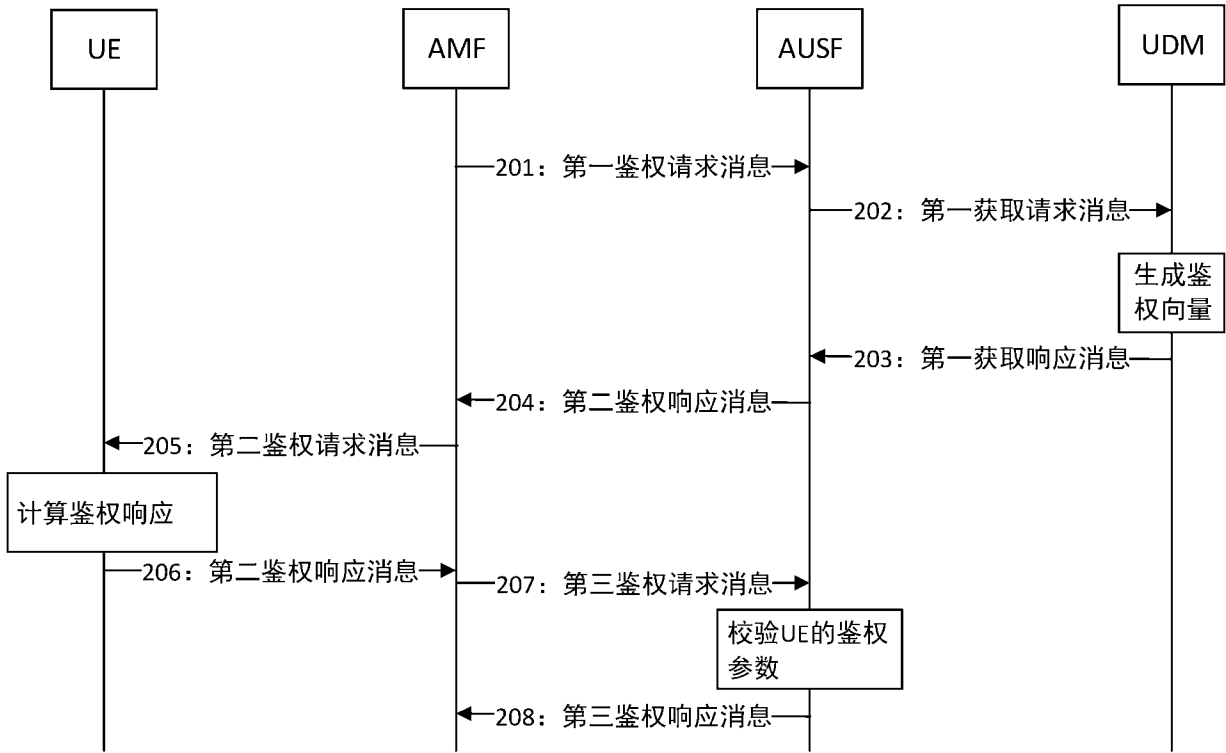


图 2

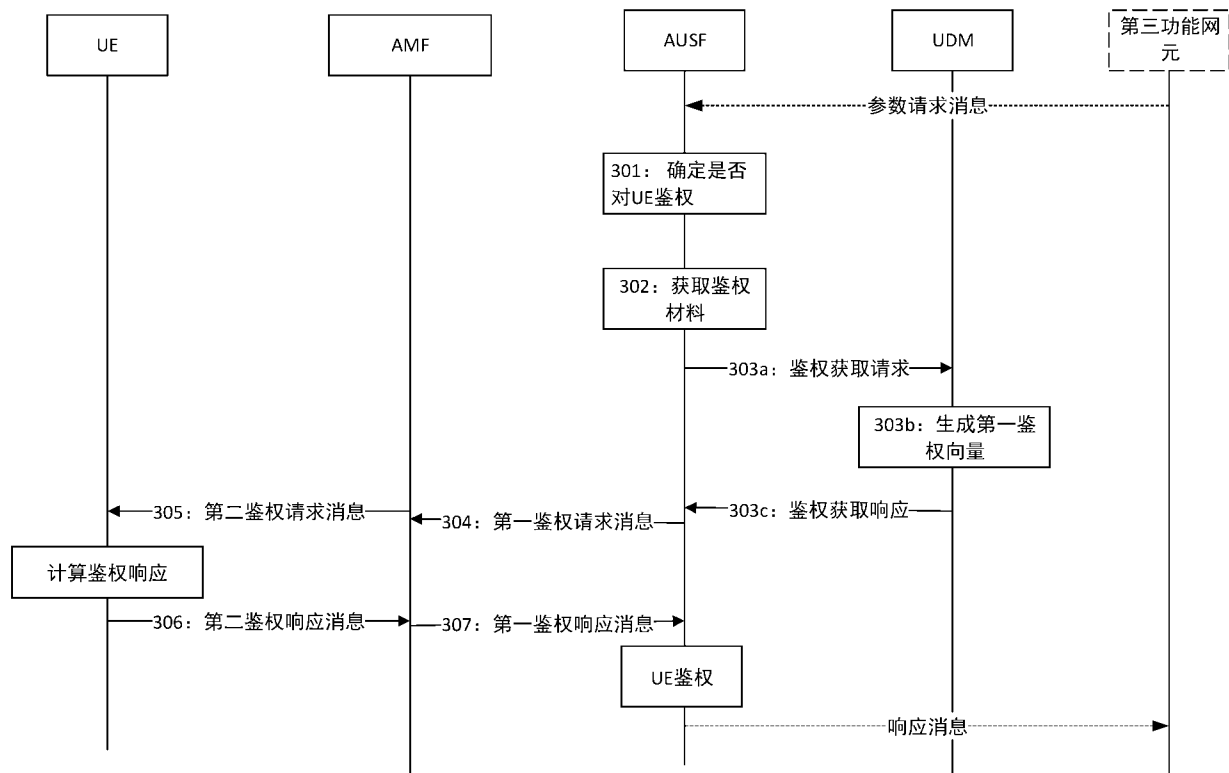


图 3

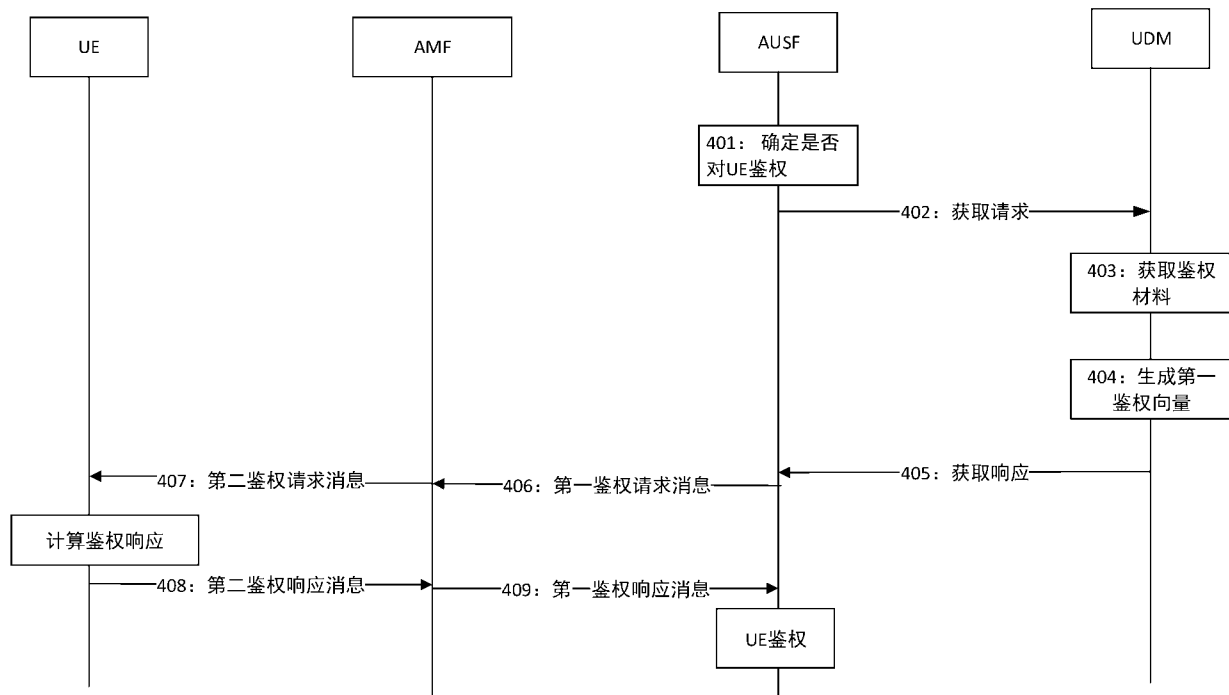


图 4

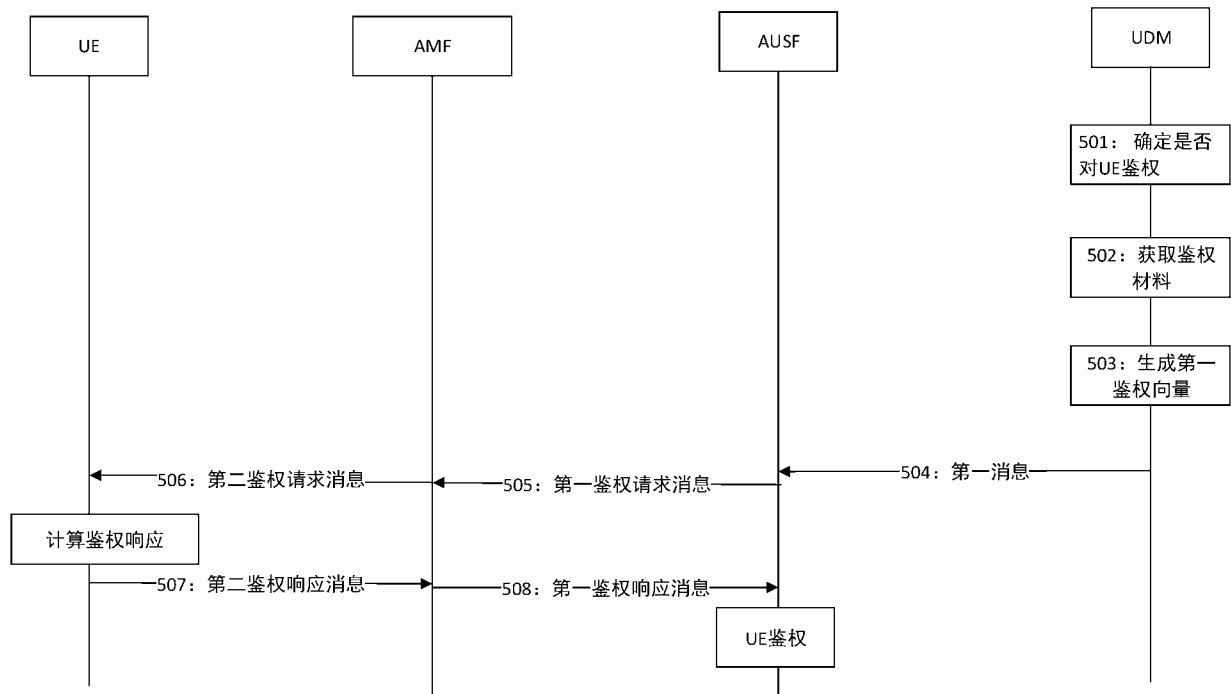


图 5

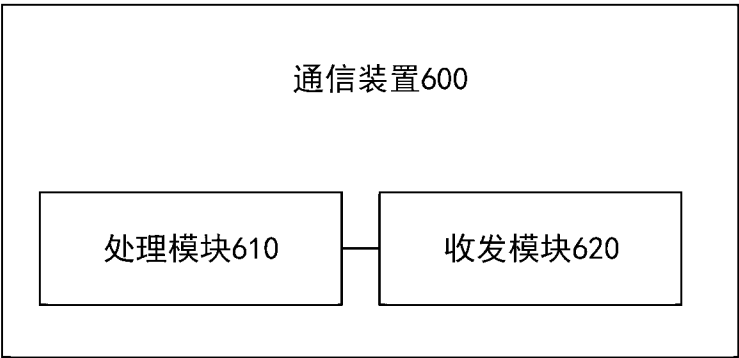


图 6

通信装置700

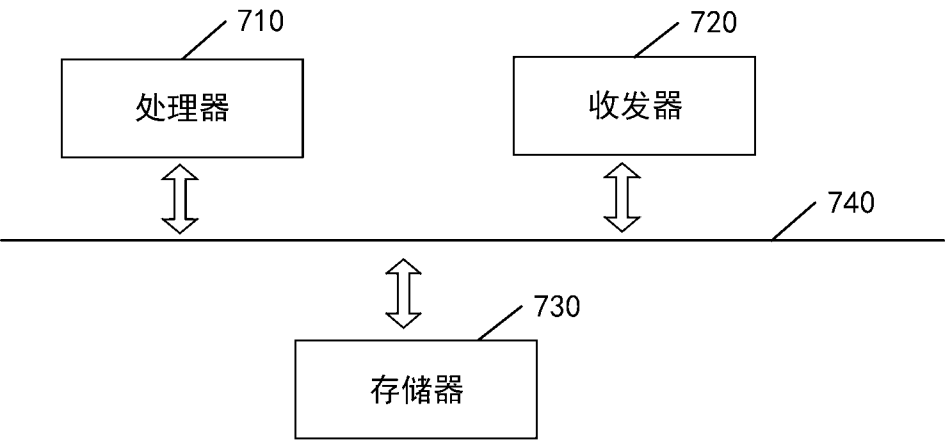


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2023/092298

A. CLASSIFICATION OF SUBJECT MATTER H04W 12/06(2021.01)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) IPC: H04W 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) CNTXT, ENTXTC, VEN, CNKI, 3GPP: 归属网络, 家乡网络, 触发, 发起, 启动, 鉴权, 认证, 服务功能, 服务器功能, 矢量, 向量, 接入和移动管理, 信令, 统一数据管理, home network, HPLMN, trigger, initiate, authentication, access and mobility management, AMF, unified data management, authentication server function, AUSF, UDM, vector, primary		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2021094109 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 20 May 2021 (2021-05-20) description, paragraphs [0004]-[0078]	1-15
A	WO 2021201558 A1 (SAMSUNG ELECTRONICS CO., LTD.) 07 October 2021 (2021-10-07) entire document	1-15
A	CN 110891271 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) 17 March 2020 (2020-03-17) entire document	1-15
A	CN 111404944 A (NO. 30 INSTITUTE OF CHINA ELECTRONIC TECHNOLOGY GROUP CORP. et al.) 10 July 2020 (2020-07-10) entire document	1-15
A	CN 114339745 A (CHINA TELECOM CORP., LTD.) 12 April 2022 (2022-04-12) entire document	1-15
☐ 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 “D” document cited by the applicant in the international application “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 12 July 2023		Date of mailing of the international search report 31 July 2023
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2023/092298

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
WO	2021094109	A1	20 May 2021	EP	4059248	A1	21 September 2022
				US	2022408249	A1	22 December 2022
WO	2021201558	A1	07 October 2021	EP	4111722	A1	04 January 2023
				KR	20220159991	A	05 December 2022
CN	110891271	A	17 March 2020	None			
CN	111404944	A	10 July 2020	None			
CN	114339745	A	12 April 2022	None			

国际检索报告

国际申请号

PCT/CN2023/092298

A. 主题的分类 H04W 12/06 (2021.01) 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) IPC: H04W 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)) CNTXT, ENTXTC, VEN, CNKI, 3GPP: 归属网络, 家乡网络, 触发, 发起, 启动, 鉴权, 认证, 服务功能, 服务器功能, 矢量, 向量, 接入和移动管理, 信令, 统一数据管理, home network, HPLMN, trigger, initiate, authentication, access and mobility management, AMF, unified data management, authentication server function, AUSF, UDM, vector, primary				
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		
A	WO 2021094109 A1 (ERICSSON TELEFON AB L M) 2021年5月20日 (2021 - 05 - 20) 说明书第[0004]-[0078]段	1-15		
A	WO 2021201558 A1 (SAMSUNG ELECTRONICS CO LTD) 2021年10月7日 (2021 - 10 - 07) 全文	1-15		
A	CN 110891271 A (大唐移动通信设备有限公司) 2020年3月17日 (2020 - 03 - 17) 全文	1-15		
A	CN 111404944 A (中国电子科技集团公司第三十研究所 等) 2020年7月10日 (2020 - 07 - 10) 全文	1-15		
A	CN 114339745 A (中国电信股份有限公司) 2022年4月12日 (2022 - 04 - 12) 全文	1-15		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。				
<table><tr><td>* 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 “D” 申请人在国际申请中引证的文件 “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</td><td>“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</td></tr></table>			* 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 “D” 申请人在国际申请中引证的文件 “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
* 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 “D” 申请人在国际申请中引证的文件 “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 2023年7月12日		国际检索报告邮寄日期 2023年7月31日		
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088		授权官员 孙凤 电话号码 (+86) 0512-88996138		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2023/092298

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)
WO	2021094109	A1	2021年5月20日	EP	4059248	A1	2022年9月21日
				US	2022408249	A1	2022年12月22日
WO	2021201558	A1	2021年10月7日	EP	4111722	A1	2023年1月4日
				KR	20220159991	A	2022年12月5日
CN	110891271	A	2020年3月17日	无			
CN	111404944	A	2020年7月10日	无			
CN	114339745	A	2022年4月12日	无			