

(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
2020 年 2 月 13 日 (13.02.2020)



(10) 国际公布号
WO 2020/029730 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2019/094830

(22) 国际申请日: 2019 年 7 月 5 日 (05.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810904615.5 2018年8月9日 (09.08.2018) 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: 张博 (ZHANG, Bo); 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, 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, 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,

(54) Title: IDENTITY INFORMATION PROCESSING METHOD, DEVICE AND SYSTEM

(54) 发明名称: 一种身份信息处理方法、设备及系统

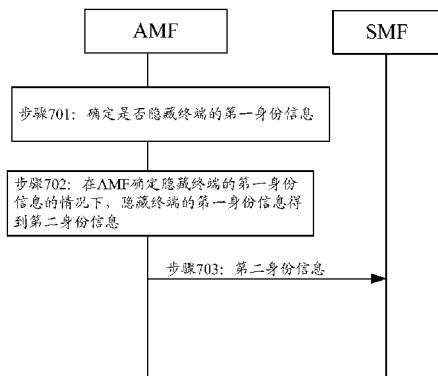


图 7

- Step 701 Determine whether to hide first identity information of a terminal
Step 702 In a case where the AMF determines to hide the first identity information of the terminal, hide the first identity information of the terminal to obtain second identity information
Step 703 Second identity information

(57) Abstract: Provided by the embodiments of the present application are an identity information processing method, device and system, used to solve the problem of identity information of a terminal being divulged. The method comprises: whether to hide first identity information of a terminal is determined, and when determined to hide the first identity information of the terminal, the first identity information is hidden, second identity information is acquired, and the second identity information is sent to a session management network element; the session management network element sends the second identity information to a third network element; and after receiving the second identity information of the terminal sent by the session management network element, the third network element sends to a decryption function entity a decryption request for requesting second identity information of a decryption terminal, receives decrypted identity information from the decryption function entity, acquires data corresponding to the decrypted identity information, and sends the data to the session management network element.

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))。

(57) 摘要：本申请实施例提供一种身份信息的处理方法、设备及系统，以解决终端的身份信息被泄露的问题。该方法包括：确定是否隐藏终端的第一身份信息，在确定隐藏终端的第一身份信息的情况下，隐藏第一身份信息，得到第二身份信息，向会话管理网元发送第二身份信息。后续，会话管理网元向第三网元发送第二身份信息，第三网元接收会话管理网元发送的终端的第二身份信息后，向解密功能实体发送用于请求解密终端的第二身份信息的解密请求，从解密功能实体接收解密后的身份信息，获取与解密后的身份信息对应的数据，向会话管理网元发送数据。

一种身份信息的方法、设备及系统

本申请要求于 2018 年 8 月 9 日提交中国国家知识产权局、申请号为 201810904615.5、
发明名称为“一种身份信息的方法、设备及系统”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

本申请涉及通信技术领域，尤其涉及一种身份信息的方法、设备及系统。

背景技术

随着无线通信技术的快速发展，第五代（Fifth Generation, 5G）移动通信网络（简称 5G 网络）应运而生，在 5G 网络中，为了满足不同客户（如业务提供商或者租户）的业务需求，提出了网络切片（Network Slice, NS）的概念。

其中，NS 是一个用于支持特定网络能力与网络特性的逻辑隔离的网络，可以提供端到端（end to end, E2E）的网络服务。例如，终端可以向网络切片发送携带有终端的身份信息（如：用户永久标识（Subscription Permanent Identifier, SUPI））的请求消息，请求网络切片中的网络功能（Network Function, NF）为终端建立承载在网络切片上的协议数据单元（protocol data unit, PDU）会话（Session），使终端通过 PDU session 接入数据网络（data network, DN）。

但是，不同网络切片所属域是不同的，当网络切片属于除运营商之外的域（如垂直行业安全域）时，将终端的身份信息发送至该网络切片，容易导致终端的身份信息泄露到垂直行业安全域的风险。

发明内容

本申请提供一种身份信息的方法、设备及系统，以解决终端的身份信息被泄露的问题。

为达到上述目的，本申请提供如下技术方案：

第一方面，本申请提供一种身份信息的方法，该方法包括：第一网元获取用于确定网络切片的所属域的第一参数，根据第一参数判断网络切片是否被运营商管理。基于该方法，可以判断网络切片是否被运营商管理，以便后续向该网络切片发送终端的身份信息时，根据该判断结果确定是否隐藏终端的身份信息，保护终端的身份信息不被泄露。如：在网络切片被运营商管理时，表示的身份信息是安全的，不用隐藏终端的身份信息；反之，在网络切片未被运营商管理时，则表示终端的网络切片位于垂直行业安全域，易泄露，需要隐藏终端的身份信息。需要说明的是，上述网络切片可以指支持终端接入的网络切片。

在第一方面的第一种可能的设计中，结合第一方面，第一网元为切片选择网元、网络贮存网元、接入和移动性管理网元中任一网元。如此，可以通过不同的网元来判断网络切片是

否被运营商管理，提高了判断的灵活性。

在第一方面的第二种可能的设计中，结合第一方面或第一方面的第一种可能的设计，当第一网元为切片选择网元或者网络贮存网元时，该方法还包括：第一网元向接入和移动性管理网元发送指示信息，该指示信息用于指示网络切片是否被运营商管理；或者，用于指示是否隐藏终端的第一身份信息；或者，用于指示网络切片的所属域是否与运营商安全域属于同一安全域。如此，接入和移动性管理网元可以通过其他网元发送的指示信息判断网络切片是否被运营商管理。

在第一方面的第三种可能的设计中，结合第一方面或第一方面的任一种可能的设计，第一参数包括：网络切片对应的 NSSAI、终端的 TAI、终端的业务类型中的至少一种参数。

其中，在第一网元为切片选择网元时，第一网元可以接收接入和移动性管理网元发送的第一参数，第一参数可以包括在切片选择请求中。

在第一网元为网络贮存网元时，第一网元可以接收接入和移动性管理网元发送的第一参数，第一参数可以包括在 NF 发现请求中。

在第一网元为接入和移动性管理网元时，第一网元可以接收终端发送的第一参数，其中，第一参数可以包括在会话建立请求或者会话更新请求或者注册请求中。

第二方面，本申请提供一种通信装置，该通信装置可以为通信网络中的第一网元，第一网元可以为切片选择网元或者切片选择网元中的芯片或者片上系统，还可以为网络贮存网元或者网络贮存网元中的芯片或者片上系统；也可以为接入和移动性管理网元或者接入和移动性管理网元中的芯片或者片上系统。该通信装置可以实现上述各方面或者各可能的设计中通信装置所执行的功能，所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个上述功能相应的模块。如：该通信装置可以包括：获取单元，判断单元；

获取单元，用于获取用于确定网络切片的所属域的第一参数；

判断单元，用于根据第一参数判断网络切片是否被运营商管理。

其中，通信装置的具体实现方式可以参考第一方面或第一方面的任一种可能的设计提供的身份信息的处理方法中通信装置的行为功能，在此不再重复赘述。因此，该提供的通信装置可以达到与第一方面或者第一方面的任一种可能的设计相同的有益效果。

第三方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机执行指令，当该通信装置运行时，该处理器执行该存储器存储的该计算机执行指令，以使该通信装置执行如上述第一方面或者第一方面的任一种可能的设计所述的身份信息的处理方法。

第四方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第一方面或者上述方面的任一种可能的设计所述的身份信息的处理方法。

第五方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面或者上述方面的任一种可能的设计所述的身份信息的处理方法。

第六方面，提供了一种芯片系统，该芯片系统包括处理器、通信接口，用于支持通信装置实现上述方面中所涉及的功能，例如处理器获取用于确定网络切片的所属域的第一参数，根据第一参数判断网络切片是否被运营商管理。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存通信装置必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第三方面至第六方面中任一种设计方式所带来的技术效果可参见上述第一方面或者第一方面的任一种可能的设计所带来的技术效果，不再赘述。

第七方面，本申请提供又一种身份信息的处理方法，该方法包括：第二网元确定是否隐藏终端的第一身份信息，在第二网元确定隐藏终端的第一身份信息的情况下，第二网元隐藏第一身份信息，得到第二身份信息，并向会话管理网元发送第二身份信息。基于该方法，第二网元可以将需要隐藏的终端的身份信息进行隐藏后发送至会话管理网元，保护终端的身份信息在发往垂直行业安全域时不被泄露。

在第七方面的第一种可能的设计中，结合第七方面，第二网元为接入和移动性管理网元、网络边缘保护代理、拜访地会话管理网元中任一网元。如此，可以通过不同网元隐藏终端的身份信息，提高了终端的身份信息隐藏的灵活性。

在第七方面的第二种可能的设计中，结合第七方面或第七方面的第一种可能的设计，第二网元确定是否隐藏终端的第一身份信息，包括：第二网元接收指示信息，根据指示信息确定是否隐藏终端的第一身份信息；指示信息用于指示网络切片是否被运营商管理；或者，指示信息用于指示是否隐藏终端的第一身份信息；或者，指示信息用于指示网络切片的所属域是否与运营商安全域属于同一安全域。

需要说明的是，当第二网元为接入和移动性管理网元时，第二网元自己可以判断网络切片是否被运营商管理，并根据自身的判断结果确定是否隐藏终端的第一身份信息。

在第七方面的第三种可能的设计中，根据第七方面或第七方面的任一种可能的设计，第二网元隐藏第一身份信息，得到第二身份信息，包括：第二网元利用公钥加密终端的第一身份信息，得到第二身份信息；或者，第二网元利用共享密钥加密终端的第一身份信息，得到第二身份信息；或者，第二网元根据共享密钥以及密钥推导函数得到新的密钥，利用新的密钥加密终端的第一身份信息，得到第二身份信息；或者，第二网元随机化终端的第一身份信息，得到第二身份信息；或者，第二网元将终端的第一身份信息对应的 GPSI 作为第二身份信息。如此，可以通过多种方式隐藏终端的身份信息，提高了隐藏的灵活性。

第八方面，本申请提供一种通信装置，该通信装置可以为通信网络中的第二网元，第二网元可以为网络边缘保护代理或者网络边缘保护代理中的芯片或者片上系统，还可以为拜访地会话管理网元或者拜访地会话管理网元中的芯片或者片上系统；也可以为接入和移动性管理网元或者接入和移动性管理网元中的芯片或者片上系统。该通信装置可以实现上述第七方面或者第七方面的各可能的设计中通信装置所执行的功能，所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个上述功能相应的模块。如：该通信装置可以包括：确定单元、隐藏单元、发送单元。

确定单元，用于确定是否隐藏终端的第一身份信息；

隐藏单元，用于确定隐藏终端的第一身份信息的情况下，隐藏第一身份信息，得到第二身份信息；

发送单元，用于向会话管理网元发送第二身份信息。

其中，通信装置的具体实现方式可以参考第七方面或第七方面的任一种可能的设计提供的身份信息的方法中通信装置的行为功能，在此不再重复赘述。因此，该提供的通信装置可以达到与第七方面或者第七方面的任一种可能的设计相同的有益效果。

第九方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机执行指令，当该通信装置运行时，该处理器执行该存储器存储的该计算机执行指令，以使该通信装置执行如上述第七方面或者第七方面的任一种可能的设计所述的身份信息的方法。

第十方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第七方面或者上述方面的任一种可能的设计所述的身份信息的方法。

第十一方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第七方面或者上述方面的任一种可能的设计所述的身份信息的方法。

第十二方面，提供了一种芯片系统，该芯片系统包括处理器、通信接口，用于支持通信装置实现上述方面中所涉及的功能，例如处理器确定是否隐藏终端的第一身份信息，在确定隐藏终端的第一身份信息的情况下，隐藏第一身份信息，得到第二身份信息，并通过通信接口向会话管理网元发送第二身份信息。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存通信装置必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第九方面至第十二方面中任一种设计方式所带来的技术效果可参见上述第七方面或者第七方面的任一种可能的设计所带来的技术效果，不再赘述。

第十三方面，本申请提供一种身份信息的方法，所述方法包括：第三网元接收会话管理网元发送的终端的身份信息以及用于指示终端的身份信息为隐藏后的身份信息的指示；第三网元根据指示向解密功能实体发送解密请求，其中，解密请求包括终端的身份信息，解密请求用于请求解密终端的身份信息；第三网元从解密功能实体接收解密后的身份信息，获取与解密后的身份信息对应的数据，向会话管理网元发送数据。基于该方法，在第三网元接收到的身份信息为隐藏后的身份信息的情况下，请求解密功能实体对隐藏后的身份信息进行解密，获取与解密后的身份信息对应的数据，并将获取到的数据发送给会话管理网元，以便会话管理网元根据接收的数据实现 PDU session 上的业务传输。如此，在终端的身份信息不被泄露的情况下，保证了业务传输的连续性。

在第十三方面的第一种可能的设计中，结合第十三方面，第三网元为策略控制网元、计费网元、数据管理网元中任一网元。如此，不同网元接收到隐藏后的身份信息后，可以请求其他网元解密终端的身份信息。

在第十三方面的第二种可能的设计中，结合第十三方面或者第十三方面的第一种可能的设计，解密功能实体为接入和移动性管理网元、数据管理网元、网络贮存网元、计费网元、

策略控制网元、认证鉴权网元中任一网元。如此，可以通过不同网元解密隐藏后的终端的身份信息，增加解密终端的身份信息的灵活性。

在第十三方面的第二种可能的设计中，结合第十三方面或者第十三方面的任一种可能的设计，所述方法还包括：第三网元向会话管理网元发送隐藏后的第二身份信息对应的信息，以便会话管理网元保存隐藏后的第二身份信息以及第二身份信息对应的信息。如此，可以在第三网元通知会话管理网元发送信息的情况下，直接向会话管理网元发送隐藏后的身份信息即可，无需通过解密功能实体解密隐藏后的身份信息后，再向会话管理网元发送信息，降低了第三网元的处理功耗以及与其他网元之间的信令开销。

第十四方面，本申请提供一种通信装置，该通信装置可以为通信网络中的第三网元，第三网元可以为策略控制网元或者策略控制网元中的芯片或者片上系统，还可以为计费网元或者计费网元中的芯片或者片上系统；也可以为数据管理网元或者数据管理网元中的芯片或者片上系统。该通信装置可以实现上述第十三方面或者第十三方面的各可能的设计中通信装置所执行的功能，所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个上述功能相应的模块。如：该通信装置可以包括：接收单元、发送单元、获取单元。

接收单元，用于接收会话管理网元发送的终端的身份信息以及用于指示终端的身份信息为隐藏后的身份信息的指示；

发送单元，用于根据指示向解密功能实体发送解密请求，其中，解密请求包括终端的身份信息，解密请求用于请求解密终端的身份信息；

接收单元，还用于从解密功能实体接收解密后的身份信息；

获取单元，用于获取与解密后的身份信息对应的数据；

发送单元，还用于向会话管理网元发送数据。

其中，通信装置的具体实现方式可以参考第十三方面或第十三方面的任一种可能的设计提供的身份信息的处理方法中通信装置的行为功能，在此不再重复赘述。因此，该提供的通信装置可以达到与第十三方面或者第十三方面的任一种可能的设计相同的有益效果。

第十五方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机执行指令，当该通信装置运行时，该处理器执行该存储器存储的该计算机执行指令，以使该通信装置执行如上述第十三方面或者第十三方面的任一种可能的设计所述的身份信息的处理方法。

第十六方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第十三方面或者上述方面的任一种可能的设计所述的身份信息的处理方法。

第十七方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第十三方面或者上述方面的任一种可能的设计所述的身份信息的处理方法。

第十八方面，提供了一种芯片系统，该芯片系统包括处理器、通信接口，用于支持通信装置实现上述方面中所涉及的功能，例如处理器接收会话管理网元发送的终端的身份信息以

及用于指示终端的身份信息为隐藏后的身份信息的指示，根据指示向解密功能实体发送解密请求，其中，解密请求包括终端的身份信息，解密请求用于请求解密终端的身份信息；从解密功能实体接收解密后的身份信息，获取与解密后的身份信息对应的数据，向会话管理网元发送数据。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存通信装置必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第十五方面至第十八方面中任一种设计方式所带来的技术效果可参见上述第十三方面或者第十三方面的任一种可能的设计所带来的技术效果，不再赘述。

第十九方面，本申请提供一种身份信息的处理系统，包括：如第二方面至第六方面所述的第一网元、如第八方面至第十二方面所述的第二网元、如第十四方面至第十八方面所述的第三网元。

附图说明

图 1 为本申请实施例提供的系统架构示意图；

图 2a 为本申请实施例提供的非漫游场景下的系统架构示意图；

图 2b 为本申请实施例提供的 L0B 漫游场景下的系统架构示意图；

图 2c 为本申请实施例提供的 home routed 漫游场景下的系统架构示意图；

图 3 为本申请实施例提供的一种通信装置的组成示意图；

图 4 为本申请实施例提供的一种身份信息的处理方法流程图；

图 5 为本申请实施例提供的又一种身份信息的处理方法流程图；

图 6 为本申请实施例提供的再一种身份信息的处理方法流程图；

图 7 为本申请实施例提供的再一种身份信息的处理方法流程图；

图 8 为本申请实施例提供的再一种身份信息的处理方法流程图；

图 9 为本申请实施例提供的一种通信装置的组成示意图；

图 10 为本申请实施例提供的又一种通信装置的组成示意图；

图 11 为本申请实施例提供的再一种通信装置的组成示意图。

具体实施方式

首先，为了便于理解本申请实施例，对本申请实施例涉及的一些技术术语进行描述：

NS：是一个具备特定网络特性的逻辑网络，不同网络切片之间逻辑上是隔离的，它可以按照需求方的要求灵活地提供一种或者多种网络服务。一个网络切片由单网络切片选择辅助信息（Single Network Slice Selection Assistance Information, S-NSSAI）来标识。

网络切片选择辅助信息 (network slice selection assistance information, NSSAI): 用于指示一个或者多个网络切片, NSSAI 中包括多个单 NSSAI (single NSSAI, S-NSSAI)。S-NSSAI 由服务类型 (slice/service type, SST) 和切片区分器 (slice differentiator, SD) 等参数组成。其中, SST 包括标准化和运营商自定义的类型; SD 是补充 SST 的可选信息, 以区分相同 SST 的多个网络切片。需要说明的是, 在本申请实施例中, 可以将 NSSAI 简称为网络切片信息。

运营商安全域: 运营商所管理的网络。

垂直行业安全域: 运营商安全域之外的其他网络, 即非运营商管理的网络。在本申请各实施例中, 垂直行业安全域可称为业务管理域或者业务安全域等。其中一种可能的部署方式为, 垂直行业安全域中与运营商安全域之间通过网络边缘保护代理 (Security Edge Protection Proxy, SEPP) 相互通信。如: 垂直行业安全域的边缘部署有 SEEP1, 运营商安全域的边缘部署有 SEEP2, 垂直行业安全域中的网络功能 (Network Function, NF) 可以通过 SEEP1 向运营商安全域中的 SEEP2 发送信息, SEEP2 接收到 SEEP1 发送的信息后, 将接收到的信息发送给运营商安全域中的 NF。

下面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。

本申请提供的技术方案可以应用于图 1 所示网络, 该网络可以为 5G 网络。如图 1 所示, 该网络可以包括: 终端、接入网设备、接入和移动性管理网元、多个网络切片 (如图 1 中的 NS-1 和 NS-2)、切片选择网元、策略控制网元、数据管理网元、计费网元、数据网络 (Data Network, DN) 等。其中, 每个网络切片由不同网络功能和物理资源集合而成, 可以用于承载 PDU session, 以便终端通过该 PDU session 接入数据网络。一种可能的结构中, 网络切片由网络贮存网元、多个管理网元、多个用户面网元组成。网络切片间相互隔离, 多个网络切片可以共享同一切片选择网元、接入和移动性管理网元、数据管理网元、策略控制网元、计费网元。在图 1 中, 不同网络切片可以均位于运营商安全域中, 被运营商所管理; 也可以部署在除运营商之外的网络中。例如, 图 1 中的 NS-1 位于运营商安全域, NS-2 位于垂直业务安全域。在图 1 中, 每个域的边缘可以部署有 SEEP, SEEP 为域的通信接口, 具有收发数据或信息的功能, 不同域中的 NF 可以通过 SEEP 相互通信。需要说明的是, 图 1 所示网络架构仅为示例性架构图, 虽然未示出, 但除图 1 所示网络功能外, 图 1 所示网络还可以包括其他功能, 如: 认证鉴权网元 (如: 认证服务器功能 (Authentication Server Function, AUSF))、认证信任状存储和处理功能 (Authentication credential Repository and Processing Function, ARPF) 等。

其中, 图 1 中的终端可以为用户设备 (User Equipment, UE), 还可以为各种具有无线或者有线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; 还可以包括用户单元 (subscriber unit)、蜂窝电话 (cellular phone)、智能电话 (smart phone)、无线数据卡、个人数字助理 (Personal Digital Assistant, PDA) 电脑、平板型电脑、无线调制解调器 (modem)、手持设备 (handheld)、膝上型电脑 (laptop computer)、无绳电话 (cordless phone) 或者无线本地环路 (Wireless Local Loop, WLL) 台、机器类型通信 (Machine Type Communication, MTC) 终端、移动台 (Mobile Station, MS) 等, 不予限制。

图 1 中的接入网设备主要用于实现物理层功能、资源调度和无线资源管理、接入控制以及移动性管理等功能；可以为下一代基站（generation nodeB, gNB）或某种其它任一接入单元；也可能为其他具体有线网络功能的接入网设备。

图 1 中的切片选择网元具备选择网络切片以及识别网络切片的属性的功能，主要用于根据终端请求的 NSSAI 和/或终端签约的 NSSAI 等信息为终端选择合适的网络切片、判断选择出的网络切片是否被运营商管理等。具体的，该切片选择网元可以为网络切片选择功能（Network Slice Selection Function, NSSF）。

图 1 中的接入和移动性管理网元主要实现对终端的接入控制和移动性管理功能，还可以用于保护终端的身份信息（如终端的 SUPI 等）。具体的，该接入和移动性管理网元可以为接入和移动管理功能（Access and Mobility Management Function, AMF）。

图 1 中的网络贮存网元保存有网络中各个网络功能（Network Function, NF）的概况（profile）、NF 支持的业务，主要用于发现 NF 以及判断其发现的 NF 所处的网络是否被运营商管理等。具体的，该网络贮存网元可以为网络仓库功能（Network Repository Function, NRF）。

图 1 中的会话管理网元主要用于实现用户面传输路径的建立、释放和更改等会话管理功能，还可以用于在会话管理网元为终端的拜访地会话管理网元的情况下，隐藏（hide）发往归属地会话管理网元的终端的身份信息。具体的，该会话管理网元可以为会话管理功能（Session Management, SMF）。

图 1 中的用户面网元主要负责用户面数据的路由转发等功能，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。具体的，该用户面网元可以为用户面功能（User Plane Function, UPF）。

图 1 中的策略控制网元主要用于制定与终端相关的策略与计费控制规则（Policy and Charging Control Rule, PCC rule），还可以用于在接收到会话管理网元发送的隐藏后的身份信息后，获取与隐藏后的身份信息对应的原身份信息，并向会话管理网元下发原身份信息对应的数据。具体的，该策略控制网元可以为策略控制功能（Policy Control Function, PCF）。

图 1 中的数据管理网元主要用于保存终端签约的数据和相关信息，还可以用于在接收到会话管理网元发送的隐藏后的身份信息后，获取与隐藏后的身份信息对应的原身份信息，并向会话管理网元下发原身份信息对应的数据。具体的，该数据管理网元可以为统一数据管理（unified data management, UDM）。

图 1 中的计费网元主要用于对终端的流量进行计费等，还可以用于在接收到会话管理网元发送的隐藏后的身份信息后，获取与隐藏后的身份信息对应的原身份信息，并向会话管理网元下发原身份信息对应的数据。具体的，该计费网元可以为计费控制功能（Charge Function, CHF）。

需要说明的是，上述各架构中的网元名字只是一个示例，具体实现中网元名字可能为其他名字，本申请实施例对此不作具体限定。下面以图 1 为 5G 网络，图 1 中的接入和移动性管理网元为 AMF，切片选择网元为 NSSF，网络贮存网元为 NRF，会话管理网

元为 AMF，策略控制网元为 PCF，数据管理网元为 UDM，计费网元为 CHF 为例，对本申请提供的身份信息的方法进行介绍。

如图 2a 所示，为终端处于非漫游场景下的系统架构图。在图 2a 中，终端位于归属公共陆地移动网络 (Home Public Land Mobile Network, HPLMN) (简称 hPLMN) 中，终端可以通过 hPLMN 中的 NS 接入 DN。例如：终端可以通过 hPLMN 中的 NS-2 接入 DN1。

由于终端设备的移动性，终端设备在 5G 网络中移动时，可能会处于图 2b 所示的本地分汇 (Local breakout, LBO) 漫游的场景或者图 2c 所示的归属地路由 (home routed) 漫游的场景，其中，LBO 漫游可以指漫游终端通过拜访地的网络切片接入网络获取相应的业务，业务的提供者可以是拜访公共陆地移动网络 (Public Land Mobile Network, PLMN) (简称 vPLMN)。例如，如图 2b 所示，终端通过 vPLMN 中的 SMF (即 vSMF) 接入 DN1 获取相应的业务，所有访问业务的终端面流量都经 vPLMN 中的 vSMF 上报给 hPLMN 中的 PCF (即 hPCF)，即：local breakout 漫游下为终端服务的 SMF 位于拜访地。

home routed 漫游是指经由归属地路由，通过拜访地的 SMF 与归属地 SMF 相连接，进行控制信令传输，并由归属地网络切片与数据网络相连接，如：图 2c 所示，vSMF 为拜访地 SMF，hSMF 为归属地 SMF，终端可以通过 vSMF 向 hSMF 发送消息，hSMF 可以将接收到的消息上传给 PCF 或者 CHF 或者 UDM 等。

在图 1~图 2c 所示系统中，为了避免终端的身份信息 (如 SUPI) 泄露到垂直行业安全域，在终端接入某个网络切片之前，判断该网络切片是否被运营商管理，在该网络切片被运营商管理的情况下 (如：网络切片位于垂直行业安全域的情况下)，隐藏终端的身份信息，即：加密终端的身份信息，后续向该网络切片发送终端的身份信息时，发送加密后的身份信息，保护终端的身份信息不被泄露到垂直行业安全域。当网络中的某些网元 (如 PCF 或 CHF 或 UDM) 接收到加密后的身份信息后，解密收到的身份信息，获取与解密后的身份信息对应的数据。上述隐藏终端的身份信息的操作可以为通过随机化的方式处理终端的身份信息。具体的，该方法可参照图 4~图 8 所示。

为了实现本申请实施例提供的身份信息的方法，上述网络中的各个网元可以包括图 3 所示部件。图 3 为本申请实施例提供的一种通信装置的组成示意图，如图 3 所示，该通信装置 300 包括至少一个处理器 301，通信线路 302，以及至少一个通信接口 304，还可以包括存储器 303。其中，处理器 301，存储器 303 以及通信接口 304 三者之间可以通过通信线路 302 连接。

处理器 301 可以是一个中央处理器 (Central Processing Unit, CPU)，也可以是特定集成电路 (Application Specific Integrated Circuit, ASIC)，或者是被配置成实施本申请实施例的一个或多个集成电路，例如：一个或多个数字信号处理器 (Digital Signal Processor, DSP)，或，一个或者多个现场可编程门阵列 (Field Programmable Gate Array, FPGA)。

通信线路 302 可包括一通路，用于在上述组件之间传送信息。

存储器 303 可以是只读存储器 (Read-Only Memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备, 随机存取存储器 (Random Access Memory, RAM) 或者可存储信息和指令的其他类型的动态存储设备, 也可以是电可擦可编程只读存储器 (Electrically Erasable Programmable Read-Only Memory, EEPROM)、只读光盘 (Compact Disc Read-Only Memory, CD-ROM) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。存储器 303 可以是独立存在, 通过通信线路 302 与处理器 301 相连接。存储器 303 也可以和处理器 301 集成在一起。其中, 存储器 303 用于存储执行指令或者应用程序代码, 并由处理器 301 来控制执行, 实现本申请下述实施例提供的身份信息的方法。

通信接口 304, 用于与其他设备或通信网络通信, 可以使用任何收发器一类的装置, 如以太网, 无线接入网 (Radio Access Network, RAN), 无线局域网 (Wireless Local Area Networks, WLAN) 等。

作为一种可实现方式, 处理器 301 可以包括一个或多个 CPU, 例如图 3 中的 CPU0 和 CPU1。作为另一种可实现方式, 通信装置 300 可以包括多个处理器, 例如图 3 中的处理器 301 和处理器 307。作为再一种可实现方式, 通信装置 300 还可以包括输出设备 305 和输入设备 306。

需要说明的是, 上述的通信装置 300 可以是一个通用设备或者是一个专用设备。例如, 通信装置 300 可以是台式机、便携式电脑、网络服务器、PDA、移动手机、平板电脑、无线终端、嵌入式设备或有图 3 中类似结构的设备。本申请实施例不限定通信装置 300 的类型。

下面结合图 2a~图 2c, 对本申请实施例提供的身份信息的处理方法进行具体阐述。需要说明的是, 本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例, 具体实现中也可以是其他的名字, 本申请实施例对此不作具体限定。

图 4 为本申请实施例提供的一种身份信息的处理方法流程图, 该方法可以应用于图 2a 或图 2b 或图 2c 所示场景中, 在该方法用于图 2a 所示场景中时, 该方法中的 AMF、NSSF 可以为归属地 AMF (即 hAMF)、归属地 NSSF (即 hNSSF)。在该方法用于图 2b 所示场景中时, 该方法中的 AMF、NSSF 可以为图 2b 中的拜访地 AMF (即 vAMF)、拜访地 NSSF (即 vNSSF)。在该方法用于图 2c 所示场景中时, 该方法中的 AMF、NSSF 可以为图 2c 中的拜访地 AMF (即 vAMF)、归属地 NSSF (即 hNSSF)。如图 4 所示, 该方法可以包括:

步骤 401: 终端向 AMF 发送第一请求消息。

其中, 该 AMF 可以为默认 AMF。终端可以通过接入网设备向 AMF 发送第一请求消息。

其中, 第一请求消息可以用于请求 AMF 为终端建立网络接入; 还可以用于指示 AMF 在网络切片位于垂直行业安全域的情况下, 隐藏发往网络切片的终端的身份信息。

第一请求消息可以为会话建立请求或者会话更新请求或者注册请求，不予限制。第一请求消息可以包括终端的第一身份信息以及终端请求的 NSSAI，还可以包括其他信息，如：终端的设备类型、终端的业务标识、终端的业务类型参数等；又可以包括隐藏指示，该隐藏指示可以用于指示 AMF 在网络切片位于垂直行业安全域的情况下，隐藏发往该网络切片

5 的终端的身份信息。需要说明的是，第一请求消息也可以不包括隐藏指示，当 AMF 接收到包括终端的第一身份信息的第一请求消息时，默认在网络切片位于垂直行业安全域的情况下，隐藏发往该网络切片的终端的第一身份信息。

本申请各实施例中，终端的第一身份信息可以为终端的用户永久标识 (Subscription Permanent Identifier, SUPI)，或者终端的国际移动用户识别码 (International Mobile Subscriber Identity, IMSI)，或者终端的全球唯一临时标识 (Globally Unique Temporary Identifier, GUTI)，或者终端的临时移动用户标识符 (Temporary Mobile Subscriber Identity, TMSI) (如：系统架构演进临时移动用户标识符 (S-TMSI) 或者移动管理功能临时移动用户标识符 (M-TMSI) 或者分组域用户临时标识符 (P-TMSI))，或者终端的 IP 多媒体私有标识 (IP Multimedia Private Identity, IMPI)，或者终端的 IP 多媒体共有标识 (IP Multimedia Public Identity, IMPU)，或者终端的国际移动台设备标识 (International Mobile Station Equipment Identity, IMEI) 等，不予限制。

10 15

步骤 402: AMF 接收第一请求消息，向 NSSF 发送切片选择请求。

其中，切片选择请求可以用于请求 NSSF 选择支持终端接入的网络切片，切片选择请求可以包括终端请求的 NSSAI，还可以包括终端的 SUPI 对应的公共陆地移动网标识 (Public Land Mobile Network Identity, PLMN ID)、终端的路由区域标识 (Tracking Area Identity, TAI)、终端的设备类型、终端的业务标识、终端的业务类型参数中的一种或多种信息。

20

可选的，步骤 402 中，当 AMF 接收到第一请求消息后，若 AMF 自身不能为终端选择出合适的网络切片，则向 NSSF 发送切片选择请求；若 AMF 自身可以为终端选择出合适的网络切片，则不向 NSSF 发送切片选择请求。具体的，AMF 可以通过现有技术判断自身是否可以为终端选择出合适的网络切片，本申请实施例对此不予赘述。

25

在图 4 所示方法应用于图 2a 或图 2b 所示场景下时，AMF 可以通过 AMF 与 NSSF 之间的通信接口 (如：服务化接口 Nnssf) 直接向 NSSF 发送切片选择请求。在图 4 所示方法应用于图 2c 所示场景下时，如图 2c 所示，AMF 可以向 vNSSF 发送切片选择请求，vNSSF 接收到切片选择请求后，向 hNSSF 转发该切片选择请求。需要说明的是，AMF 向 vNSSF 发送的切片选择请求与 vNSSF 向 hNSSF 发送的切片选择请求中均携带有终端请求的 NSSAI，除携带 NSSAI 之外，AMF 向 vNSSF 发送的切片选择请求中携带的信息可以与 vNSSF 向 hNSSF 发送的切片选择请求中携带的信息相同或不同。

30

步骤 403: NSSF 接收切片选择请求，判断网络切片是否被运营商管理。

其中，步骤 403 中所述的网络切片可以为 NSSF 选择的、支持终端接入的网络切片。具体的，NSSF 选择网络切片的过程可参照现有技术，本申请实施例对此不予赘述。

35

其中，网络切片是否被运营商管理可以指：网络切片是否位于运营商安全域或者网

络切片的所属域与运营商安全域是否属于同一安全域。如：若终端的网络切片位于运营商安全域中，则表示网络切片被运营商管理；反之，网络切片位于运营商安全域之外（即位于垂直行业安全域中），网络切片不被运营商管理。

需要说明的是，本申请中的下述几四种描述：网络切片是否被运营商管理、网络切片是否位于运营商安全域、发往网络切片的身份信息是否需要隐藏（或者保护）、发往（网络切片中的）NF（如：SMF）的身份信息是否需要隐藏（或者保护）、网络切片的所属域与运营商安全域是否属于同一安全域为同一概念，这四种描述形式之间可以相互替换。例如，“判断网络切片是否被运营商管理”可以描述为“判断发往（网络切片中的）NF（如：SMF）的身份信息是否需要隐藏”，还可以描述为“判断网络切片的所属域与运营商安全域是否属于同一安全域”，也可以描述为“判断网络切片是否位于运营商安全域”。此外，还可以用其他描述语言来间接表达“网络切片是否被运营商管理”，即用其可用于表达“网络切片是否被运营商管理”的语言描述也在本申请的保护范围之内。

一种可能的设计中，NSSF 根据 NSSAI 与网络切片所属域的对应关系，确定网络切片是否被运营商管理；其中，网络切片所属域包括运营商安全域或者垂直行业安全域。例如，NSSAI1 对应运营商安全域，NSSAI2 对应垂直行业安全域，当 NSSF 选择出的网络切片对应的 NSSAI 为 NSSAI2 时，则确定网络切片位于垂直行业安全域，不被运营商管理。或者，NSSAI 中包括 NSSAI 对应的网络切片是否属于运营商安全域的指示，NSSF 根据此指示可以直接确定网络切片是否被运营商管理，如：当该指示用于指示 NSSAI 对应的网络切片不属于运营商安全域时，NSSF 确定网络切片不位于运营商安全域，而是位于垂直行业安全域。

又一种可能的设计中，切片选择请求中包括终端的 TAI，若终端的 TAI 指示终端位于垂直行业安全域中，则 NSSF 根据终端的 TAI 确定网络切片属于被运营商管理，反之，则确定网络切片不被运营商管理。

再一种可能的设计中，切片选择请求中包括终端的业务类型，若终端的业务类型指示终端的业务属于垂直行业业务范畴，则 NSSF 根据终端的业务类型确定网络切片属于被运营商管理，反之，则确定网络切片不被运营商管理。

可选的，上述网络切片等价于网络切片内的 NF（如：SMF、UPF 等网络功能实体）。即本申请中所述的网络切片是否被运营商管理等同于网络切片中的 NF（如：SMF 或者 UPF）是否被运营商管理。

步骤 404：NSSF 向 AMF 发送指示信息。

其中，指示信息可以用于指示网络切片是否被运营商管理，或者用于指示是否隐藏终端的第一身份信息，或者用于指示网络切片的所属域是否与运营商安全域属于同一安全域。

以指示信息用于指示网络切片是否被运营商管理为例，该指示信息可以为二进制比特数“0”或“1”，其中，“0”表示网络切片未被运营商管理，“1”表示网络切片被运营商管理。或者，该指示信息为布尔值“true”或者“false”，“false”表示网络切片未被运营商管理，“true”表示网络切片被运营商管理。

在图 4 所示方法应用于图 2a 或图 2b 所示场景下时, NSSF 可以通过 NSSF 与 AMF 之间的通信接口 (如: 服务化接口 Namf) 直接向 AMF 发送指示信息。

在图 4 所示方法应用于图 2c 所示场景下时, hNSSF 向 vNSSF 发送指示信息, 由 vNSSF 向 AMF 发送指示信息。需要说明的是, hNSSF 向 vNSSF 发送的指示信息与 vNSSF 向 AMF 发送的指示信息可以相同, 也可以不同, 如: hNSSF 向 vNSSF 发送的指示信息可以用于指示网络切片不被运营商管理, vNSSF 向 AMF 发送的指示信息可以用于指示是否隐藏终端的身份信息。

需要说明的是, 在步骤 404 中, NSSF 还可以向 AMF 发送网络切片对应的 NSSAI 以及其他信息, 不予限制。

10 步骤 405: AMF 接收指示信息。

进一步可选的, AMF 接收到指示信息后, 可以由自身或者其他网元根据指示信息确定是否隐藏终端的第一身份信息。具体的, 根据指示信息确定是否隐藏终端的第一身份信息的过程可参照 7 中所示。

在图 4 所示的方法中, 可以通过 NSSF 判断网络切片是否被运营商管理, 并根据判断结果向 AMF 发送指示信息, 后续, 以便 AMF 或者其他网元根据该指示信息确定是否隐藏终端的身份信息, 保护终端的身份信息不被泄露。

与图 4 不同的是, 在又一种可实现方法中, 可以通过 NRF 判断为终端服务的会话管理网元是否被运营商管理, 具体的, 该方法可参照图 5 所示。

图 5 为本申请实施例提供的又一种身份信息的处理方法, 该方法可以应用于图 2a 或图 2b 或图 2c 所示场景中, 在该方法用于图 2a 所示场景中时, 该方法中的 AMF、NRF 可以为归属地 AMF (即 hAMF)、归属地 NRF (即 hNRF)。在该方法用于图 2b 所示场景中时, 该方法中的 AMF、NRF 可以为图 2b 中的拜访地 AMF (即 vAMF)、拜访地 NRF (即 vNRF)。在该方法用于图 2c 所示场景中时, 该方法中的 AMF、NRF 可以为图 2c 中的拜访地 AMF (即 vAMF)、归属地 NRF (即 hNRF)。如图 5 所示, 该方法可以包括:

25 步骤 501: 终端向 AMF 发送第一请求消息。

其中, 步骤 501 可参照步骤 401 所述, 不再赘述。

步骤 502: AMF 接收第一请求消息, 向 NRF 发送 NF 发现请求。

其中, NF 发现请求中可以包括网络切片对应的 NSSAI, 该网络切片可以为支持终端接入的网络切片。NF 发现请求可以用于请求 NRF 发现该 NSSAI 对应的网络切片中为终端服务的 SMF 以及判断该 SMF 是否被运营商管理。除包括 NSSAI 之外, NF 发现请求还可以包括终端的 SUPI 对应的 PLMN ID、终端的 TAI、终端的设备类型、终端的业务标识、终端的业务类型参数中的一种或多种信息。

可选的, 步骤 502 中, 当 AMF 接收到第一请求消息, 且选择出网络切片后, 若 AMF 自身不能从该网络切片中选择出为终端服务的 SMF, 则向 NRF 发送 NF 发现请求; 若 AMF 自身可以从该网络切片中选择出为终端服务的 SMF, 则不向 NSSF 发送切片选择请求。具体的, AMF 可以采用现有技术判断自身是否可以选择出为终端服务的 SMF, 本

申请实施例对此不予赘述。其中，在图 2c 所示场景下，AMF 选择出的网络切片为拜访地网络切片。

在图 5 所示方法应用于图 2a 或图 2c 所示场景下时，AMF 可以通过 AMF 与 NRF 之间的通信接口（如：服务化接口 Nnrf）直接向 NRF 发送 NF 发现请求。在图 4 所示方法应用于图 2c 所示场景下时，如图 2c 所示，AMF 可以向 vNRF 发送 NF 发现请求，vNRF 接收到 NF 发现请求后，向 hNRF 转发该 NF 发现请求；其中，vNRF 为 AMF 选择出的拜访地网络切片中的 NRF，hNRF 为与该拜访地网络切片相对应的归属地网络切片中的 NRF。需要说明的是，AMF 向 vNRF 发送的 NF 发现请求与 vNRF 向 hNRF 发送的 NF 发现请求中均携带有终端请求的 NSSAI，除携带 NSSAI 之外，AMF 向 vNRF 发送的 NF 发现请求中携带的信息可以与 vNRF 向 hNRF 发送的 NF 发现请求中携带的信息相同或者不同。

步骤 503：NRF 接收 NF 发现请求，判断 SMF 是否被运营商管理。

其中，步骤 503 中所述的 SMF 可以是 NRF 从支持终端接入的网络切片中选择出的、为终端服务的 SMF，也可以为其他能够为终端服务的 SMF。其中，NRF 选择为终端服务的 SMF 的过程可参照现有技术，本申请实施例对此不予赘述。需要说明的是，在图 2c 所示场景下，NRF 选择出的 SMF 为归属地 SMF（hSMF）。

在 SMF 是 NRF 从支持终端接入的网络切片中选择出的、为终端服务的 SMF 的情况下，NRF 判断 SMF 是否被运营商管理的过程可以包括：NRF 判断 NF 发现请求中包括的 NSSAI 对应的网络切片是否被运营商管理，若被运营商管理，则确定选择出的 SMF 被运营商管理，反之，则确定选择出的 SMF 不被运营商管理。NRF 判断 NF 发现请求中包括的 NSSAI 对应的网络切片是否被运营商管理的过程可参照步骤 403 中 NSSF 判断网络切片是否被运营商管理的过程，不再赘述。

在步骤 503 中的 SMF 为其他 SMF 的情况下，NRF 可以根据 SMF 的地址信息判断该 SMF 是否被运营商管理。如：NRF 可以查看运营商管理的所有地址信息，若该 SMF 的地址信息包括在运营商管理的地址信息的范围之内，则确定该 SMF 被运营商管理，反之，则确定该 SMF 不被运营商管理。其中，SMF 的地址信息用于标识该 SMF，可以为 SMF 的因特网协议（Internet Protocol，IP）地址，或者 SMF 全量域名（fully qualified domain name，FQDN），或者 SMF 实例的信息，或者 SMF 业务实例的地址等。

需要说明的是，SMF 是否被运营商管理、SMF 所在的网络切片是否被运营商管理、SMF 所在的网络切片是否位于运营商安全域、发往 SMF 的身份信息是否需要隐藏（或者保护）、发往 SMF 所在的网络切片的身份信息是否需要隐藏（或者保护）、SMF 所在的网络切片的所属域与运营商安全域是否属于同一安全域为同一概念，这几种描述形式之间可以相互替换。例如，以 SMF 为支持终端接入的网络切片中的 SMF 为例，“判断 SMF 是否被运营商管理”可以描述为“判断终端接入的网络切片是否被运营商管理”，还可以描述为“判断终端接入的网络切片与运营商安全域是否属于同一安全域”等，不予限制。此外，还可以用其他描述语言来间接表达“SMF 是否被运营商管理”，即用其可用于表达“SMF 是否被运营商管理”的语言描述也在本申请的保护范围之内。

步骤 504: NRF 向 AMF 发送 SMF 的地址信息以及指示信息。

其中, 步骤 504 中的指示信息可以用于指示 SMF 是否被运营商管理, 或者用于指示是否隐藏发往该 SMF 的终端的第一身份信息, 或者用于指示 SMF 的所属域是否与运营商安全域属于同一安全域。该指示信息的具体表示形式可参照步骤 404 中所述, 不再赘述。

在图 5 所示方法应用于图 2a 或图 2b 所示场景下时, NRF 可以通过 NRF 与 AMF 之间的通信接口 (如: 服务化接口 Namf) 直接向 AMF 发送 SMF 的地址信息以及指示信息。

在图 5 所示方法应用于图 2c 所示场景下时, hNRF 向 vNRF 发送 SMF 的地址信息以及指示信息, 由 vNRF 向 AMF 发送 SMF 的地址信息以及指示信息。需要说明的是, hNRF 向 vNRF 发送的指示信息与 vNRF 向 AMF 发送的指示信息可以相同, 也可以不同, 如: hNRF 向 vNRF 发送的指示信息可以用于指示 SMF 不被运营商管理, vNRF 向 AMF 发送的指示信息可以用于指示隐藏发往 SMF 的终端的第一身份信息。

步骤 505: AMF 接收 SMF 的地址信息以及指示信息。

进一步可选的, AMF 接收到指示信息后, 可以由自身或者其他网元根据指示信息确定是否隐藏终端的第一身份信息。具体的, 根据指示信息确定是否隐藏终端的第一身份信息的过程可参照 7 中所示。需要说明的是, 在图 5 所示方法中, NRF 也可以仅向 AMF 发送 SMF 的地址信息, 后续, AMF 接收到 SMF 的地址信息后, 根据 SMF 的地址信息确定 SMF 是否被运营商管理。如: 若 SMF 的地址信息包括在运营商所管理的地址信息的范围内, 则确定 SMF 被运营商管理, 反之, 则确定 SMF 不被运营商管理。

在图 5 所示的方法中, 可以通过 NRF 判断网络切片中的 SMF 是否被运营商管理, 并根据判断结果向 AMF 发送指示信息, 后续, 便于 AMF 或者其他网元根据该指示信息确定是否隐藏终端的身份信息, 保护终端的身份信息不被泄露。

与图 4 或图 5 所示方法不同的是, 再一种可实现方法中, 可以通过 AMF 自身判断网络切片是否被运营商管理。具体的, 该可实现方法可参照图 6 中所示。

图 6 为本申请实施例提供的再一种身份信息的处理方法, 该方法可以应用于图 2a 或图 2b 或图 2c 所示场景中, 在该方法用于图 2a 所示场景中时, 该方法中的 AMF、UDM 可以为归属地 AMF (即 hAMF)、归属地 UDM。在该方法用于图 2b 所示场景中时, 该方法中的 AMF 可以为图 2b 中的拜访地 AMF (即 vAMF), UDM 可以为归属地 UDM。在该方法用于图 2c 所示场景中时, 该方法中的 AMF 可以为图 2c 中的拜访地 AMF (即 vAMF), UDM 可以为归属地 UDM。如图 6 所示, 该方法可以包括:

步骤 601: 终端向 AMF 发送第一请求消息。

其中, 步骤 601 可参照步骤 401 所述, 不再赘述。

步骤 602: AMF 接收第一请求消息, 向 UDM 发送数据请求。

其中, 数据请求中可以包括终端的第一身份信息, 数据请求可以用于请求终端的签约数据。该数据请求可以为 Nudm 消息,

步骤 603: UDM 获取终端的签约数据, 向 AMF 发送获取到的终端的签约数据。

其中, 终端的签约数据可以包括终端签约的 NSSAI, 或者终端签约的数据网络的名
称 (Data Network Name, DNN), 或者, 终端签约的 NSSAI 以及终端签约的 NSSAI
是否被运营商管理间的对应关系, 或者终端签约的 DNN 以及终端签约的 DNN 是否被运
营管理间的对应关系。

步骤 604: AMF 接收终端签约的数据, 根据终端签约的数据以及终端请求的 NSSAI,
判断网络切片是否被运营商管理。

其中, 该网络切片可以为支持终端接入的网络切片。AMF 可以根据终端签约的数据
以及终端请求的 NSSAI 确定支持终端接入的网络切片, 其具体实现方式可参照现有技术,
不再赘述。

具体的, AMF 判断网络切片是否被运营商管理的过程可参照步骤 403 中 NSSF 判断
网络切片是否被运营商管理的过程, 不再赘述。除参照步骤 403 之外, AMF 还可以根据
网络切片对应的 DNN, 根据该 DNN 是否被运营商管理, 判断网络切片是否被运营商管
理, 如: 若 DNN 被运营商管理, 则确定网络切片被运营商管理, 反之, 则确定网络切片
不被运营商管理。

进一步可选的, AMF 判断网络切片是否被运营商管理后, 可以由自身或者其他网元
确定是否隐藏终端的第一身份信息。具体的, 确定是否隐藏终端的第一身份信息的过程
可参照 7 中所示。

在图 6 所示的方法中, 可以通过 AMF 判断网络切片是否被运营商管理, 后续, 便于
AMF 或者其他网元根据 AMF 的判断结果确定是否隐藏终端的身份信息, 保护终端的身
份信息不被泄露。

以上图 4~图 6 主要对网络切片或者 SMF 是否被运营商管理进行了描述。接下来,
在网络切片或者 SMF 被运营商管理的情况下, 隐藏终端的第一身份信息, 反之, 则直接
向网络切片中的 SMF 发送终端的第一身份信息。具体的, 该过程可参照图 7 所示。

图 7 为本申请提供的一种身份信息的处理方法流程示意图, 该方法可以应用于图 2a
或图 2b 或图 2c 所示场景中, 在该方法用于图 2a 所示场景中时, 该方法中的 AMF、SMF
可以为归属地 AMF (即 hAMF)、归属地 SMF。在该方法用于图 2b 所示场景中时, 该方
法中的 AMF 可以为图 2b 中的拜访地 AMF (即 vAMF), SMF 可以为拜访地 SMF (vSMF)。
在该方法用于图 2c 所示场景中时, 该方法中的 AMF 可以为图 2c 中的拜访地 AMF (即
vAMF), SMF 可以为归属地 SMF (hSMF)。如图 7 所示, 所述方法包括:

步骤 701: AMF 确定是否隐藏终端的第一身份信息。

一种可能的设计中, AMF 根据从 NSSF 或者 NRF 接收到的指示信息确定是否隐藏
终端的第一身份信息; 其中, 指示信息的相关描述可参照图 4 或图 5 中所述, 不再赘述。

例如, 若指示信息用于指示网络切片被运营商管理, 则确定不隐藏终端的第一身份
信息, 反之, 则确定隐藏终端的第一身份信息。或者, 若指示信息用于指示隐藏终端的
第一身份信息, 则直接确定隐藏终端的第一身份信息, 反之, 则确定不隐藏终端的第一

身份信息。

又一种可能的设计中, AMF 根据本地预设策略确定是否隐藏终端的第一身份信息, 如: AMF 可以采用图 6 所示方法确定是否隐藏终端的第一身份信息。

需要说明的是, 本申请不限制 AMF 确定是否隐藏终端的第一身份信息的实现方式。

5 步骤 702: 在 AMF 确定隐藏终端的第一身份信息的情况下, 隐藏终端的第一身份信息得到第二身份信息。

在本申请各实施例中, 隐藏可以指加密或者封装或者保护。第二身份信息可以为隐藏后的终端的身份信息, 第二身份信息可以与终端的第一身份信息对应。

具体的, AMF 可以通过下述几种方式隐藏终端的第一身份信息, 得到第二身份信息:

10 方式一: 利用公钥加密终端的第一身份信息, 得到第二身份信息。

方式二: 利用共享密钥加密终端的第一身份信息, 得到第二身份信息。其中, 共享密钥预先配置在隐藏终端的第一身份信息的网元 (如 AMF) 上和解密第二身份信息的网元上。

15 方式三: AMF 根据共享密钥衍生出新的密钥, 利用新的密钥加密终端的第一身份信息, 得到第二身份信息。

例如: 新的密钥 $K_{SST} = KDF(K)$, 或者 $K_{SST} = KDF(K, SST)$, 其中, K 为共享密钥, SST 为 NSSAI 包括的切片信息, KDF 为密钥推衍函数。共享密钥 K 预先配置在隐藏终端的第一身份信息的网元 (如 AMF) 上和解密第二身份信息的网元 (如图 8 中所示的解密功能实体) 上。

20 需要说明的是, 上述密钥推衍函数内的参数, 除了 K , SST 之外, 还可能包括切片 ID, 会话 ID 中的至少一项; 也可以包括时间, 计算器, 序列号, 随机数 (nonce) 等。在方式三中, AMF 需要将 AMF 与解密第二身份信息的网元间没有共享的参数 (如: 切片 ID, 时间, 计算器, 序列号, 随机数 (nonce) 等) 发送至 SMF, 以便 SMF 将这些没有共享的参数发送至解密第二身份信息的网元, 以使得解密第二身份信息的网元使用
25 相同推衍函数和推衍参数得到 K_{SST} , 进而根据 K_{SST} 解密第二身份信息, 得到终端的第一身份信息。

方式四: AMF 随机化终端的第一身份信息, 得到第二身份信息。

一种可能的设计中, AMF 根据 hash 类型函数随机化终端的第一身份信息。这里 hash 类型的函数可以为普通的 hash 类型函数 (如 SHA-256 等), 或者媒体接入控制 (Media Access Control, MAC) 消息验证码 (Message Authentication Code) 类型的函数 (如: 基于哈希算法的消息验证码 (Hashed Base Message Authentication, HMAC), 或者基于加密的验证码 (Cipher-based MAC, CMAC) 等), 不做限制。例如, 以终端的第一身份信息为 SUPI 为例, 隐藏后的身份信息 = $hash(SUPI, SST)$, 或者 $hash(SUPI, SST, (nonce, 序列号 (sequence number), 时间 (time) 中的至少一项))$ 。其中, 随机数
30 为 AMF 生成的任一数值。序列号为当前时刻的前一时刻 AMF 与 SMF 交互的信息的序号。时间为当前时刻 AMF 内定时器的时间。

又一种可能的设计中，第二身份信息由 AMF 的路由信息（routing information）以及 AMF 生成的随机数组成。例如，以终端的第一身份信息为 SUPI 为例， $\text{Hide}(\text{SUPI}) = \text{AMF routing information} || \text{random number}$ 。

在方式四中，AMF 保存隐藏后的第二身份信息与终端的第一身份信息的对应关系，以便后续 AMF 接收到解密第二身份信息的网元发送的解密请求后，根据该对应关系解密得到终端的第一身份信息。

方式五：AMF 将终端的第一身份信息对应的 GPSI 作为隐藏后的第二身份信息。

需要说明的是，本申请中所述隐藏终端的第一身份信息可以指：将终端的第一身份信息全部隐藏或者部分隐藏，其中，部分隐藏指隐藏终端的第一身份信息中的部分信息。以终端的第一身份信息为 SUPI 为例，SUPI 包括网络标识和身份标识两部分信息，网络标识可以为 MNC，MCC，身份标识可以为 MSIN，其中，网络标识可以不用隐藏，身份标识隐藏。

步骤 703：AMF 向 SMF 发送第二身份信息。

其中，第二身份信息可以包括在会话建立请求或者会话更新请求中向 SMF 发送。除第二身份信息之外，AMF 还可以向 SMF 发送第二身份信息为隐藏后的身份信息的指示，以便 SMF 接收到该指示后，将第二身份信息以及该指示一起发送给 PCF 或 CHF 或者 UDM 等。

在图 7 所示方法应用于图 2a 或图 2b 所示场景下时，AMF 可以通过 AMF 与 SMF 之间的通信接口（如：服务化接口 Nsmf）直接向 SMF 发送第二身份信息；或者，AMF 向其所在域的第一 SEEP 发送第二身份信息，第一 SEEP 接收到第二身份信息后，向 SMF 所在域的第二 SEEP 发送第二身份信息，第二 SEEP 接收第二身份信息，向 SMF 发送接收到的第二身份信息。

在图 7 所示方法应用于图 2c 所示场景下时，hAMF 向 vSMF 发送第二身份信息，由 vSMF 向 hSMF 发送第二身份信息。

可选的，在 AMF 确定不隐藏终端的第一身份信息的情况下，AMF 直接向 SMF 发送终端的第一身份信息。其中，除发送终端的第一身份信息外，AMF 还可以向 SMF 发送第一身份信息为未隐藏的身份信息的指示。其中，AMF 向 SMF 发送第一身份信息的过程可参照 AMF 向 SMF 发送第二身份信息的过程，不再赘述。

在本申请中，可以用“0”或“1”来指示 AMF 向 SMF 发送的身份信息是否为隐藏后的身份信息。如：“0”指示 AMF 向 SMF 发送的身份信息未隐藏，“1”指示 AMF 向 SMF 发送的身份信息被隐藏。需要说明的是，向 SMF 发送终端的第一身份信息的同时，AMF 也可以不向 SMF 发送用于指示第一身份信息为未隐藏后的身份信息的指示，当 SMF 接收到仅包括终端的第一身份信息的信息时，默认接收到的身份信息为未隐藏后的身份信息。

可选的，在图 7 所示方法中，AMF 根据本地策略确定是否执行图 7 所示步骤 701 以及隐藏终端的第一身份信息的过程，其中，本地策略预先配置在 AMF 上，本地策略用于

规定 AMF 在向其他网元发送终端的身份信息之前, 开启或者关闭 AMF 的确定是否隐藏终端的身份信息的功能。在 AMF 确定不执行步骤 701 的情况下, 可以通过其他网元来隐藏终端的身份信息。具体如下:

在图 2a 或图 2b 的情况下, AMF 接收到 NSSF 或者 NRF 发送的指示信息, 或者 AMF 自身判断网络切片是否被运营商管理之后, 不执行步骤 702~步骤 703, 而是向其所在的第一 SEEP 或者 SMF 所在的第二 SEEP 发送隐藏终端的第一身份信息的指示信息以及终端的第一身份信息, 以便第一 SEEP 或者第二 SEEP 根据隐藏终端的第一身份信息的指示信息隐藏终端的第一身份信息, 得到第二身份信息, 并向 SMF 发送第二身份信息。其中, 第一 SEEP 或第二 SEEP 隐藏终端的第一身份信息的过程可参照 AMF 隐藏终端的第一身份信息的过程, 不再赘述。

在图 2c 的情况下, AMF 接收到 NSSF 或者 NRF 发送的指示信息, 或者 AMF 自身判断网络切片是否被运营商管理之后, AMF 不执行步骤 702~步骤 703, 而是向 vSMF 发送用于指示隐藏终端的第一身份信息的指示信息以及终端的第一身份信息, 以便 vSMF 根据隐藏终端的第一身份信息的指示信息隐藏终端的第一身份信息, 得到第二身份信息, 并向 hSMF 发送第二身份信息。其中, vSMF 隐藏终端的第一身份信息的过程可参照 AMF 隐藏终端的第一身份信息的过程, 不再赘述。AMF 接收到的指示信息与 AMF 向 vSMF 发送的指示信息可以相同, 也可以不同, 如: AMF 接收到的指示信息可以为网络切片不被运营商管理, AMF 向 vSMF 发送的指示信息可以为隐藏终端的第一身份信息。

在图 7 所示的方法中, 可以将需要隐藏的身份信息进行隐藏后发送至 SMF, 保护终端的身份信息在发往垂直行业安全域时不被泄露。

SMF 接收到终端的身份信息 (第一身份信息或者第二身份信息) 后, 可以将接收到的身份信息发送至 PCF 或 CHF 或 UDM, 以便 PCF 或 CHF 或 UDM 接收 SMF 发送的终端的身份信息, 并在终端的身份信息为隐藏后的第二身份信息的情况下, 请求解密功能实体解密第二身份信息得到第一身份, 并根据解密后的第一身份信息获取与终端相关的数据返回给 SMF。下面结合图 8, 以 SMF 向 PCF 发送其接收到的终端的身份信息为例, 对该过程进行介绍。其中, SMF 向 UDM 或者 CHF 发送终端的身份信息的过程可参照图 8 所示过程。

图 8 为本申请提供的一种身份信息处理方法流程图, 该方法可以应用于图 2a 或图 2b 或图 2c 所示场景中, 在该方法用于图 2a 所示场景中时, 该方法中的 SMF 可以为归属地 SMF, PCF 可以为归属地 PCF。在该方法用于图 2b 所示场景中时, 该方法中的 SMF 可以为拜访地 SMF (vSMF), PCF 可以为归属地 PCF。在该方法用于图 2c 所示场景中时, 该方法中的 SMF 可以为归属地 SMF (hSMF), PCF 可以为归属地 PCF。如图 8 所示, 所述方法包括:

步骤 801: SMF 接收终端的身份信息。

其中, SMF 接收到的身份信息可以为未隐藏的终端的第一身份信息或者隐藏后的第二身份信息。

可选的, 步骤 801 中, SMF 还接收到用于指示终端的身份信息是否为隐藏后的身份

信息的指示,以便 SMF 根据此指示可以判定接收到的身份信息是否为隐藏后的身份信息。或者,步骤 801 中,SMF 接收到第二身份信息以及用于指示终端的身份信息为隐藏后的身份信息的指示,以便 SMF 根据此指示可以判定接收到的身份信息为隐藏后的身份信息。

5 步骤 802: 在终端的身份信息为隐藏后的第二身份信息的情况下,SMF 向 PCF 发送第二身份信息以及用于指示第二身份信息为隐藏后的身份信息的指示。

可选的,SMF 通过 SEEP 向 PCF 发送第二身份信息以及用于指示第二身份信息为隐藏后的身份信息的指示,或者,通过其与 PCF 的通信接口(如:服务化接口 Npcf)向 PCF 发送第二身份信息以及用于指示第二身份信息为隐藏后的身份信息的指示。

10 可选的,指示第二身份信息为隐藏后的身份信息的指示也可不发。PCF 可以根据接收到的身份信息判定其是否为隐藏后的身份信息;或者 PCF 可以根据 SMF 的信息(例如源 SMF 的地址等)判定 SMF 发送的身份信息是否为隐藏后的身份信息,即 PCF 不需要指示就可以判定其接收到的身份信息是否为隐藏后的身份信息。

步骤 803: PCF 接收第二身份信息以及用于指示第二身份信息为隐藏后的身份信息的指示,向解密功能实体发送解密请求。

15 其中,解密请求中包括第二身份信息,解密请求可以用于请求解密隐藏后的第二身份信息。

其中,解密功能实体可以为 UDM、AMF、CHF、AUSF、ARPF、NRF、PCF 中任一网元。需要说明的是,当解密功能实体为除自身之外的其他功能时,其中一种可选方式为,PCF 获取解密功能实体的地址信息,根据解密功能实体的地址信息向解密发送解密请求。

20 解密功能实体的地址信息可以由解密功能实体发送给 SMF,由 SMF 发送给 PCF,如:以解密功能实体为 AMF 为例,解密功能实体的地址信息可以与第二身份信息包括在同一消息中发送给 PCF,也可以包括在不同消息中发送给 PCF。或者,PCF 中预先配置有解密功能实体的地址信息,当 PCF 接收到第二身份信息以及用于指示第二身份信息为隐藏后的身份信息的指示时,PCF 根据其内预先配置的解密功能实体的地址信息向解密功能实体发送解密请求。或者,在解密功能实体为 AMF,且 AMF 采用方式四隐藏终端的身份信息的情况下,PCF 可以根据隐藏的身份信息中 AMF 的路由信息来确定 AMF,并请求 AMF 解密隐藏后的身份信息。如:Hide(SUPI)=AMF routing information||random number,当 PCF 接收到 Hide(SUPI)后,PCF 根据 AMF routing information 确定 AMF 的地址信息,向 AMF 发送解密请求。

步骤 804: 解密功能实体接收解密请求,解密隐藏后的第二身份信息,得到终端的第一身份信息,向 PCF 发送终端的第一身份信息。

其中,在采用方式一隐藏终端的身份信息情况下,解密功能实体通过私钥解密隐藏后的第二身份信息,得到终端的第一身份信息。

35 在采用方式二隐藏终端的身份信息情况下,解密功能实体通过共享密钥解密隐藏后的第二身份信息,得到终端的第一身份信息。其中,共享密钥预先存储在解密功能实体

上。

在采用方式三隐藏终端的身份信息情况下，解密功能实体通过推衍函数和推衍参数得到共享密钥后，基于共享密钥解密隐藏后的第一身份信息，得到终端的第二身份信息。

5 在采用方式四隐藏终端的身份信息情况下，解密功能实体为 AMF，AMF 保存有隐藏后的第二身份信息与终端的第一身份信息的对应关系，根据此对应关系得到终端的第一身份信息。

在采用方式五隐藏终端的身份信息情况下，解密功能实体为 AMF 或 UDM，解密功能实体通过终端的身份信息与 GPSI 的对应关系解密隐藏后的第二身份信息，得到终端的第一身份信息。

10 步骤 805：PCF 接收终端的第一身份信息，获取与第一身份份信息对应的数据，并向 SMF 发送获取到的数据。

需要说明的是，在终端的身份信息为第一身份信息的情况下，SMF 向 PCF 发送第一身份信息。PCF 接收 SMF 发送的第一身份信息，不需要解密接收到的第一身份信息，直接获取与第一身份份信息对应的数据，并向 SMF 发送获取到的数据。

15 在图 8 所示方法中，在 PCF 接收到的身份信息为隐藏后的身份信息的情况下，请求解密功能实体对隐藏后的身份信息进行解密，获取与解密后的身份信息对应的数据，并将获取到的数据发送给 SMF，以便 SMF 根据接收的数据实现 PDU session 上的业务传输。如此，在终端的身份信息不被泄露的情况下，保证了业务传输的连续性。

进一步的，在图 8 所示方法中，PCF 可以向 SMF 发送隐藏后的第二身份信息对应的信息，以便 SMF 保存隐藏后的第二身份信息以及第二身份信息对应的信息。后续，当
20 PCF 需要向 SMF 发送消息（例如通知消息）时，向 SMF 发送隐藏后的第二身份信息，以使得 SMF 根据隐藏后的第二身份信息直接获取第二身份信息对应的信息，并根据获取到的信息执行相应操作。例如：更新用户对应的策略等，或者通知 UPF，或者向接入网设备发送服务质量（Quality of Service, QoS）变更等等。如此，可以在 PCF 通知 SMF
25 发送信息的情况下，直接向 SMF 发送隐藏后的身份信息即可，无需通过解密功能实体解密隐藏后的身份信息后，再向 SMF 发送信息，降低了第三网元的处理功耗以及与其他网元之间的信令开销。

上述主要从 AMF、SMF、NSSF、NRF 各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是，上述 AMF 为了实现上述功能，其包含了执行各个
30 功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，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。

35 本申请实施例可以根据上述方法示例对执行上述方法的通信装置进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能

模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，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。

图 9 示出了一种通信装置的结构图，该通信装置可以为切片选择网元（如 NSSF）或者切片选择网元中的芯片或者片上系统，还可以为网络贮存网元（如 NRF）或者网络贮存网元中的芯片或者片上系统；也可以为接入和移动性管理网元（如 AMF）或者接入和移动性管理网元中的芯片或者片上系统，该通信装置可以用于执行上述实施例中涉及的终端的功能。作为一种可实现方式，图 9 所示通信装置包括：获取单元 90，判断单元 91；

获取单元 90，用于获取用于确定网络切片的所属域的第一参数；如：获取单元 90 支持图 9 所示通信装置执行步骤 402 或者步骤 502 或者步骤 601。

判断单元 91，用于根据第一参数判断网络切片是否被运营商管理。如：判断单元 91 用于支持图 9 所示通信装置执行步骤 403 或者步骤 503 或者步骤 604。

进一步的，如图 9 所示，在通信装置为切片选择网元（如 NSSF）或者切片选择网元中的芯片或者片上系统，或者，为网络贮存网元（如 NRF）或者网络贮存网元中的芯片或者片上系统时，该通信装置还可以包括：发送单元 92；

发送单元 92，用于向接入和移动性管理网元发送指示信息，该指示信息的相关描述如前所述，不再赘述。如：发送单元 92 用于支持图 9 所示的通信装置执行步骤 404 和步骤 504。

需要说明的是，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。本申请实施例提供的通信装置，用于执行上述身份信息的方法中通信装置的功能，因此可以达到与上述身份信息的方法相同的效果。

作为又一种可实现方式，图 9 所示通信装置可以包括：处理模块和通信模块。获取单元 90 和判断单元 91 集成在处理模块中，发送单元 92 集成的通信模块中。处理模块用于对通信装置的动作进行控制管理，例如，处理模块用于支持该通信装置支持步骤 403 或者步骤 503 或者步骤 604 以及执行本文所描述的技术的其它过程。通信模块用于支持通信装置执行步骤 404 和步骤 504 以及与其他网络实体的通信，例如与图 1 示出的功能模块或网络实体之间的通信。进一步的，该通信装置还可以包括存储模块，用于存储通信装置的程序代码和数据。

其中，处理模块可以是处理器或控制器。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。通信模块可以是收发电路或通信接口等。存储模块可以是存储器。当处理模块为处理器，通信模块为通信接口，存储模块为存储器时，图 9 所示通信装置可以为图 3 所示通信装置。

图 10 示出了一种通信装置的结构图，该通信装置可以为网络边缘保护代理（如：SEEP）或者网络边缘保护代理中的芯片或者片上系统，还可以为拜访地会话管理网元（如：vSMF）或者拜访地会话管理网元中的芯片或者片上系统；也可以为接入和移动性管理网元（如：AMF）或者接入和移动性管理网元中的芯片或者片上系统。该通信装置可以用于执行上述实施例中涉及的终端的功能。作为一种可实现方式，图 10 所示通信装置包括：确定单元 100、隐藏单元 101、发送单元 102。

确定单元 100，用于确定是否隐藏终端的第一身份信息；如：确定单元 100 用于支持图 10 所示的通信装置执行步骤 701。

隐藏单元 101，用于在确定隐藏终端的第一身份信息的情况下，隐藏第一身份信息，得到第二身份信息；如：隐藏单元 101 用于支持图 10 所示的通信装置执行步骤 702。

5 发送单元 102，用于向会话管理网元发送第二身份信息。如：发送单元 102 用于支持图 10 所示的通信装置执行步骤 703。

进一步的，如图 10 所示，该通信装置还可以包括：接收单元 103；

所述接收单元 103，用于接收切片选择网元或者网络贮存网元发送的指示信息，该指示信息的相关描述如前所述，不再赘述。

10 确定单元 100，具体用于根据该指示信息确定是否隐藏终端的第一身份信息。

需要说明的是，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。本申请实施例提供的通信装置，用于执行上述身份信息的处理方法中通信装置的功能，因此可以达到与上述身份信息的处理方法相同的效果。

15 作为又一种可实现方式，图 10 所示通信装置可以包括：处理模块和通信模块。处理模块集成有确定单元 100、隐藏单元 101；通信模块集成有接收单元 103、发送单元 102。处理模块用于对通信装置的动作进行控制管理，例如，处理模块用于支持该通信装置支持步骤 701、步骤 702 以及执行本文所描述的技术的其它过程。通信模块用于支持通信装置执行步骤 703 以及与其他网络实体的通信，例如与图 1 示出的功能模块或网络实体之间的通信。进一步的，该通信装置还可以包括存储模块，用于存储通信装置的程序代码和数据。

其中，处理模块可以是处理器或控制器。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。通信模块可以是收发电路或通信接口等。存储模块可以是存储器。当处理模块为处理器，通信模块为通信接口，存储模块为存储器时，图 10 所示通信装置可以为图 3 所示通信装置。

图 11 示出了一种通信装置的结构图，该通信装置可以为策略控制网元（如：PCF）或者策略控制网元中的芯片或者片上系统，还可以为计费网元（如 CHF）或者计费网元中的芯片或者片上系统；也可以为数据管理网元（如 UDM）或者数据管理网元中的芯片或者片上系统。该通信装置可以用于执行上述实施例中涉及的终端的功能。作为一种可实现方式，图 11 所示通信装置包括：接收单元 110、发送单元 111、获取单元 112。

接收单元 110，用于接收会话管理网元发送的终端的身份信息以及用于指示终端的身份信息为隐藏后的身份信息的指示；如：接收单元 110 用于支持图 11 所示的通信装置执行步骤 802。

35 发送单元 111，用于根据指示向解密功能实体发送解密请求，其中，解密请求包括终端的身份信息，解密请求用于请求解密终端的身份信息；如：发送单元 111 用于支持

图 11 所示的通信装置执行步骤 803。

接收单元 110，还用于从解密功能实体接收解密后的身份信息；如：接收单元 110 用于支持图 11 所示的通信装置执行步骤 804。

获取单元 112，用于获取与解密后的身份信息对应的数据。

5 发送单元 111，还用于向会话管理网元发送数据。如：发送单元 111 用于支持图 11 所示的通信装置执行步骤 805。

需要说明的是，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。本申请实施例提供的通信装置，用于执行上述身份信息的处理方法中通信装置的功能，因此可以达到与上述身份信息的处理方法相同的效果。

10 作为又一种可实现方式，图 11 所示通信装置可以包括：处理模块和通信模块。处理模块集成有获取单元 112；通信模块集成有接收单元 110、发送单元 111。处理模块用于对通信装置的动作进行控制管理，例如，处理模块用于支持该通信装置获取与解密后的身份信息对应的数据以及执行本文所描述的技术的其它过程。通信模块用于支持通信装置执行步骤 802、步骤 803、步骤 804、步骤 805 以及与其他网络实体的通信，例如与图 1 示出的功能模块或网络实体之间的通信。进一步的，该通信装置还可以包括存储模块，用于存储通信装置的程序代码和数据。

其中，处理模块可以是处理器或控制器。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP 和微处理器的组合等等。通信模块可以是收发电路或通信接口等。存储模块可以是存储器。当处理模块为处理器，通信模块为通信接口，存储模块为存储器时，图 11 所示通信装置可以为图 3 所示通信装置。

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来实现。该计算机程序产品包括一个或多个计算机指令。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、服务器或者数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line, 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以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。

尽管在此结合各实施例对本申请进行了描述，然而，在实施所要求保护的本申请过程中，本领域技术人员通过查看所述附图、公开内容、以及所附权利要求书，可理解并

实现所述公开实施例的其他变化。在权利要求中，“包括”（comprising）一词不排除其他组成部分或步骤，“一”或“一个”不排除多个的情况。单个处理器或其他单元可以实现权利要求中列举的若干项功能。相互不同的从属权利要求中记载了某些措施，但这并不表示这些措施不能组合起来产生良好的效果。

5 尽管结合具体特征及其实施例对本申请进行了描述，显而易见的，在不脱离本申请的精神和范围的情况下，可对其进行各种修改和组合。相应地，本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明，且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利
10 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。

15

20

25

30

权 利 要 求

1、一种身份信息的方法，其特征在于，所述方法包括：

第一网元获取第一参数；所述第一参数用于确定网络切片的所属域；

5 所述第一网元根据所述第一参数判断所述网络切片是否被运营商管理。

2、根据权利要求 1 所述的身份信息的方法，其特征在于，

所述第一网元为切片选择网元、网络贮存网元、接入和移动性管理网元中任一网元。

3、根据权利要求 2 所述的身份信息的方法，其特征在于，当所述第一网元为切片选择网元或者网络贮存网元时，所述方法还包括：

10 所述第一网元向所述接入和移动性管理网元发送指示信息；

其中，所述指示信息用于指示所述网络切片是否被运营商管理；或者，

所述指示信息用于指示是否隐藏所述终端的第一身份信息；或者，

所述指示信息用于指示所述网络切片的所属域是否与运营商安全域属于同一安全域。

4、根据权利要求 1-3 任一项所述的身份信息的方法，其特征在于，

15 所述第一参数包括：所述网络切片对应的网络切片选择辅助信息 NSSAI、所述终端的路由区域标识 TAI、所述终端的业务类型中的至少一种参数。

5、一种身份信息的方法，其特征在于，所述方法包括：

第二网元确定是否隐藏终端的第一身份信息；

20 在所述第二网元确定隐藏所述终端的第一身份信息的情况下，所述第二网元隐藏所述第一身份信息，得到第二身份信息，并向会话管理网元发送所述第二身份信息。

6、根据权利要求 5 所述的身份信息的方法，其特征在于，

所述第二网元为接入和移动性管理网元、网络边缘保护代理、拜访地会话管理网元中任一网元。

25 7、根据权利要求 5 或 6 所述的身份信息的方法，其特征在于，在所述第二网元确定是否隐藏终端的第一身份信息之前，所述方法还包括：

所述第二网元接收指示信息，其中，所述指示信息用于指示所述网络切片是否被运营商管理；或者，所述指示信息用于指示是否隐藏所述终端的第一身份信息；或者，所述指示信息用于指示所述网络切片的所属域是否与运营商安全域属于同一安全域；

30 所述第二网元确定是否隐藏终端的第一身份信息，包括：根据所述指示信息确定是否隐藏终端的第一身份信息。

8、根据权利要求 5-7 任一项所述的身份信息的方法，其特征在于，所述第二网元

隐藏所述第一身份信息，得到第二身份信息，包括：

所述第二网元利用公钥加密所述终端的第一身份信息，得到第二身份信息；或者，

所述第二网元利用共享密钥加密所述终端的第一身份信息，得到第二身份信息；或者，

5 所述第二网元根据共享密钥以及密钥推衍函数得到新的密钥，利用所述新的密钥加密所述终端的第一身份信息，得到第二身份信息；或者，

所述第二网元随机化所述终端的第一身份信息，得到第二身份信息；或者，

所述第二网元将所述终端的第一身份信息对应的广义公共用户标识 GPSI 作为所述第二身份信息。

9、一种身份信息的处理方法，其特征在于，所述方法包括：

10 第三网元接收会话管理网元发送的终端的身份信息以及用于指示所述终端的身份信息为隐藏后的身份信息的指示；

所述第三网元根据所述指示向解密功能实体发送解密请求，其中，所述解密请求包括所述终端的身份信息，所述解密请求用于请求解密所述终端的身份信息；

15 所述第三网元从所述解密功能实体接收解密后的身份信息，获取与所述解密后的身份信息对应的数据，向所述会话管理网元发送所述数据。

10、根据权利要求 9 所述的身份信息的处理方法，其特征在于，

所述第三网元为策略控制网元、计费网元、数据管理网元中任一网元。

11、根据权利要求 9 或 10 所述的身份信息的处理方法，其特征在于，

20 所述解密功能实体为接入和移动性管理网元、所述数据管理网元、网络贮存网元、所述计费网元、所述策略控制网元、认证鉴权网元中任一网元。

12、一种通信装置，其特征在于，所述通信装置包括：

获取单元，用于获取第一参数；所述第一参数用于确定网络切片的所属域；

判断单元，用于根据所述第一参数判断所述网络切片是否被运营商管理。

13、根据权利要求 12 所述的通信装置，其特征在于，

25 所述通信装置为切片选择网元、网络贮存网元、接入和移动性管理网元中任一网元。

14、根据权利要求 13 所述的通信装置，其特征在于，当所述通信装置为切片选择网元或者网络贮存网元时，所述通信装置还包括：

发送单元，用于向所述接入和移动性管理网元发送指示信息；

其中，所述指示信息用于指示所述网络切片是否被运营商管理；或者，

30 所述指示信息用于指示是否隐藏所述终端的第一身份信息；或者，

所述指示信息用于指示所述网络切片的所属域是否与运营商安全域属于同一安全域。

15、根据权利要求 12-14 任一项所述的通信装置，其特征在于，

所述第一参数包括：所述网络切片对应的网络切片选择辅助信息 NSSAI、所述终端的路由区域标识 TAI、所述终端的业务类型中的至少一种参数。

5 16、一种通信装置，其特征在于，所述通信装置包括：

确定单元，用于确定是否隐藏终端的第一身份信息；

隐藏单元，用于在所述确定单元确定隐藏所述终端的第一身份信息的情况下，隐藏所述第一身份信息，得到第二身份信息；

发送单元，用于向会话管理网元发送所述第二身份信息。

10 17、根据权利要求 16 所述的通信装置，其特征在于，

所述通信装置为接入和移动性管理网元、网络边缘保护代理、拜访地会话管理网元中任一网元。

18、根据权利要求 16 或 17 所述的通信装置，其特征在于，所述通信装置，还包括：

15 接收单元，用于接收指示信息；所述指示信息用于指示所述网络切片是否被运营商管理；或者，所述指示信息用于指示是否隐藏所述终端的第一身份信息；或者，所述指示信息用于指示所述网络切片的所属域是否与运营商安全域属于同一安全域；

所述确定单元，具体用于根据所述指示信息确定是否隐藏终端的第一身份信息。

19、根据权利要求 16-18 任一项所述的通信装置，其特征在于，所述隐藏单元，具体用于：

20 利用公钥加密所述终端的第一身份信息，得到第二身份信息；或者，

利用共享密钥加密所述终端的第一身份信息，得到第二身份信息；或者，

根据共享密钥以及密钥推衍函数得到新的密钥，利用所述新的密钥加密所述终端的第一身份信息，得到第二身份信息；或者，

随机化所述终端的第一身份信息，得到第二身份信息；或者，

25 将所述终端的第一身份信息对应的广义公共用户标识 GPSI 作为所述第二身份信息。

20、一种通信装置，其特征在于，所述通信装置包括：

接收单元，用于接收会话管理网元发送的终端的身份信息以及用于指示所述终端的身份信息为隐藏后的身份信息的指示；

30 发送单元，用于根据所述指示向解密功能实体发送解密请求，其中，所述解密请求包括所述终端的身份信息，所述解密请求用于请求解密所述终端的身份信息；

所述接收单元，还用于从所述解密功能实体接收解密后的身份信息；

获取单元，用于获取与所述解密后的身份信息对应的数据；

所述发送单元，还用于向所述会话管理网元发送所述数据。

21、根据权利要求 20 所述的通信装置，其特征在于，

所述通信装置为策略控制网元、计费网元、数据管理网元中任一网元。

5 22、根据权利要求 20 或 21 所述的通信装置，其特征在于，

所述解密功能实体为接入和移动性管理网元、所述数据管理网元、网络贮存网元、所述计费网元、所述策略控制网元、认证鉴权网元中任一网元。

23、一种包含指令的计算机程序产品，当所述指令在计算机上运行时，使得所述计算机执行如权利要求 1-4 任一项所述的身份信息的处理方法，或者如权利要求 5-8 任一项所述的身份信息的处理方法，或者如权利要求 9-11 任一项所述的身份信息的处理方法。

10 24、一种计算机存储介质，其特征在于，所述计算机存储介质包括计算机指令，当所述计算机指令在计算机上运行时，使得所述计算机执行如权利要求 1-4 任一项所述的身份信息的处理方法，或者如权利要求 5-8 任一项所述的身份信息的处理方法，或者如权利要求 9-11 任一项所述的身份信息的处理方法。

15

1/6

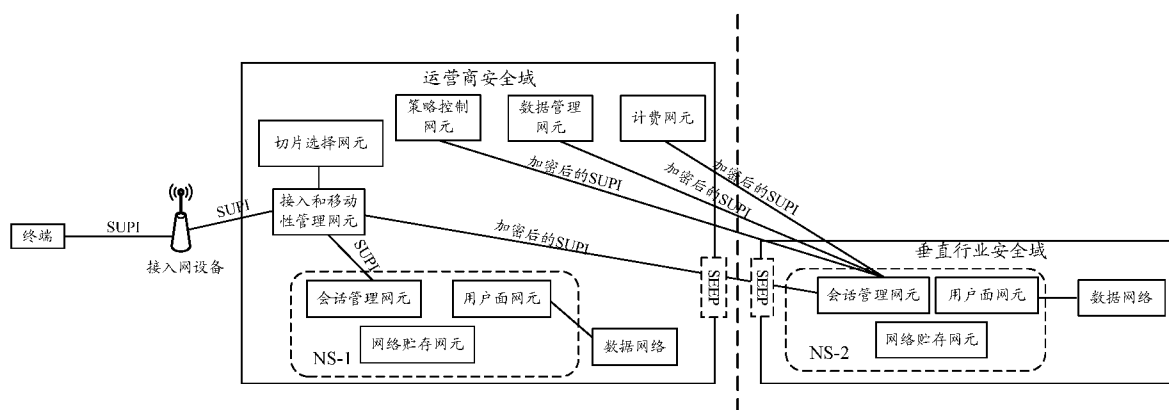


图 1

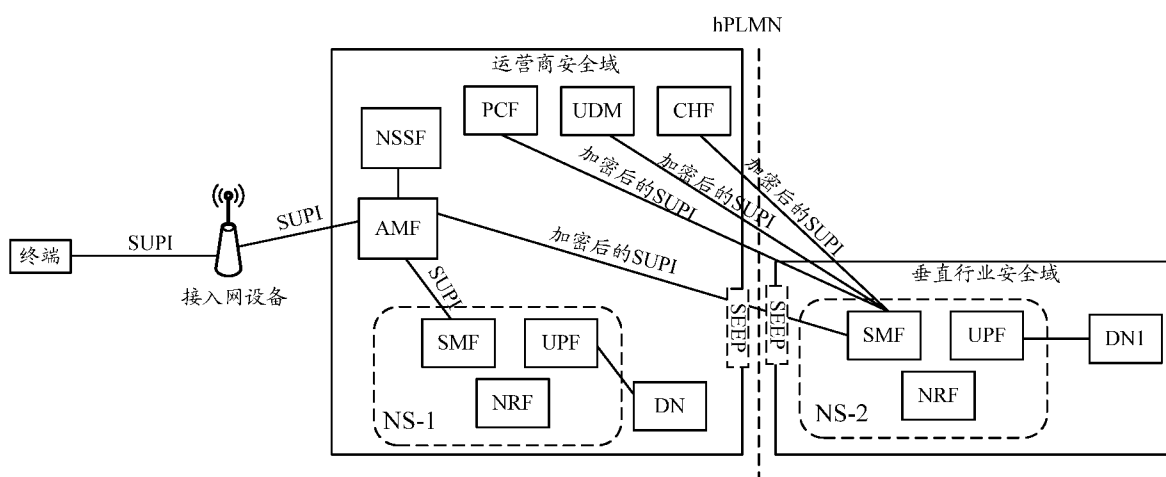


图 2a

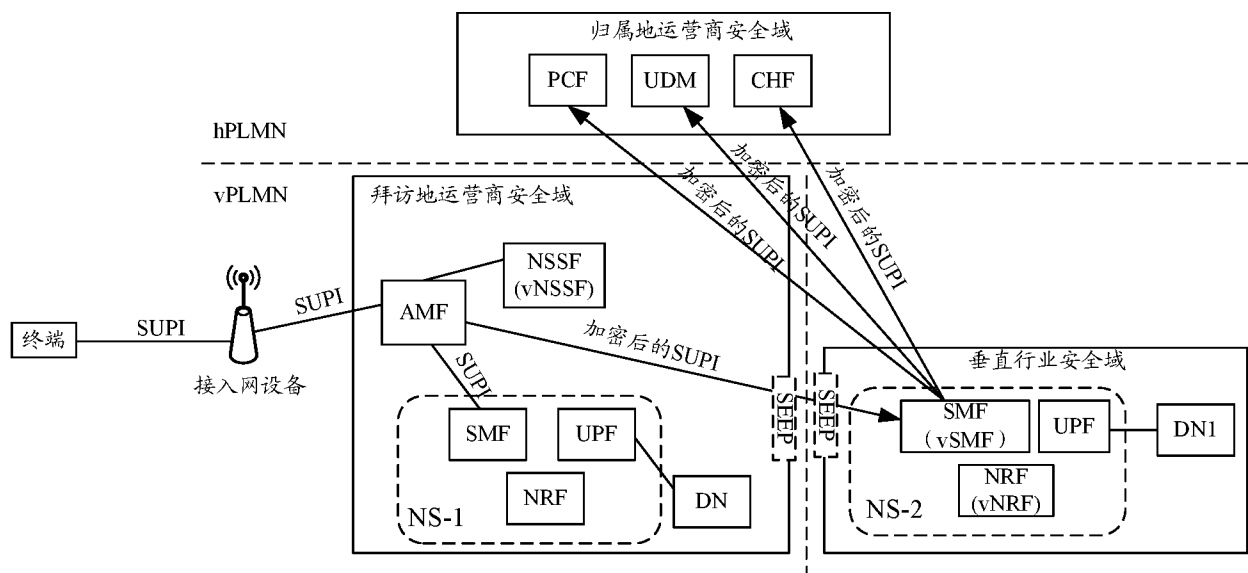


图 2b

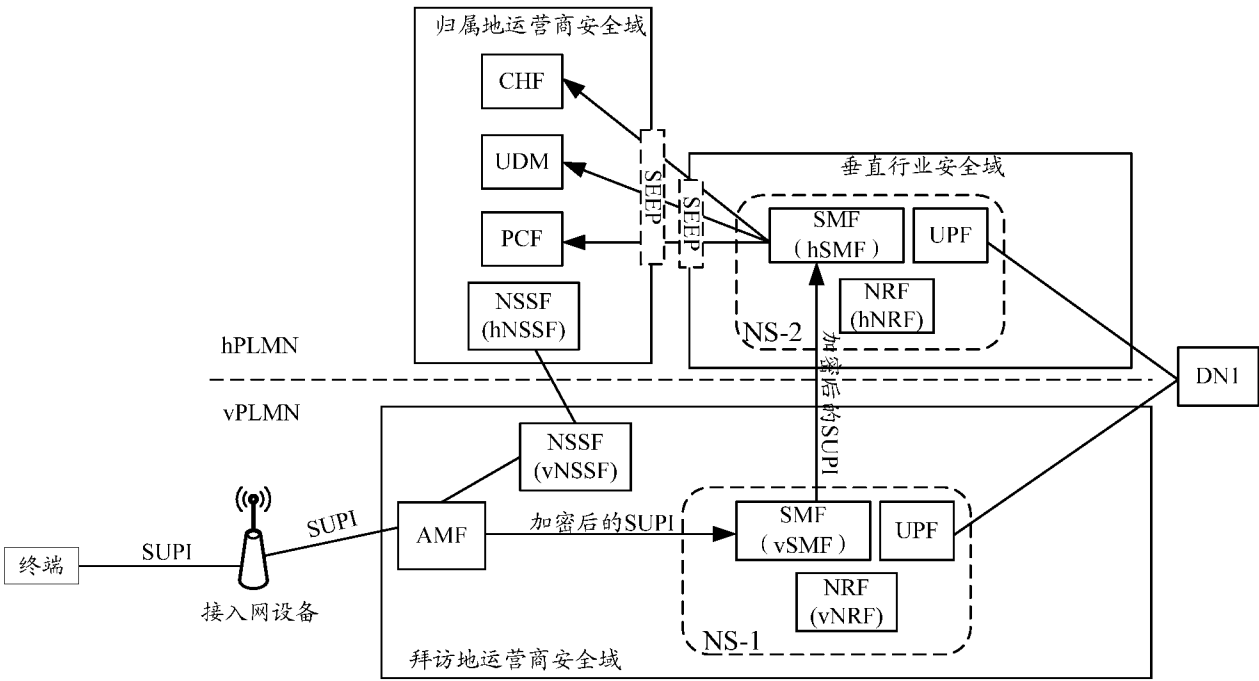


图 2c

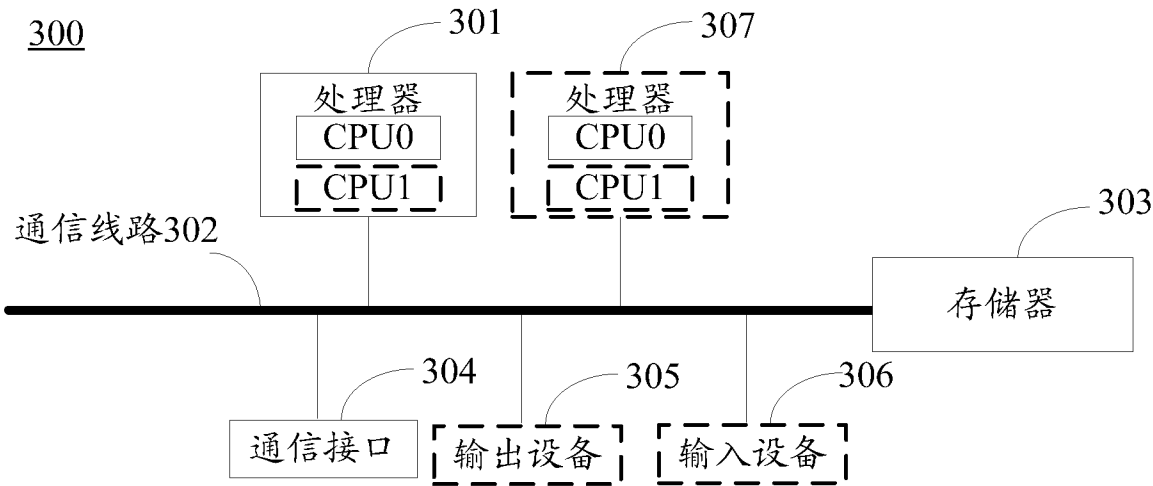


图 3

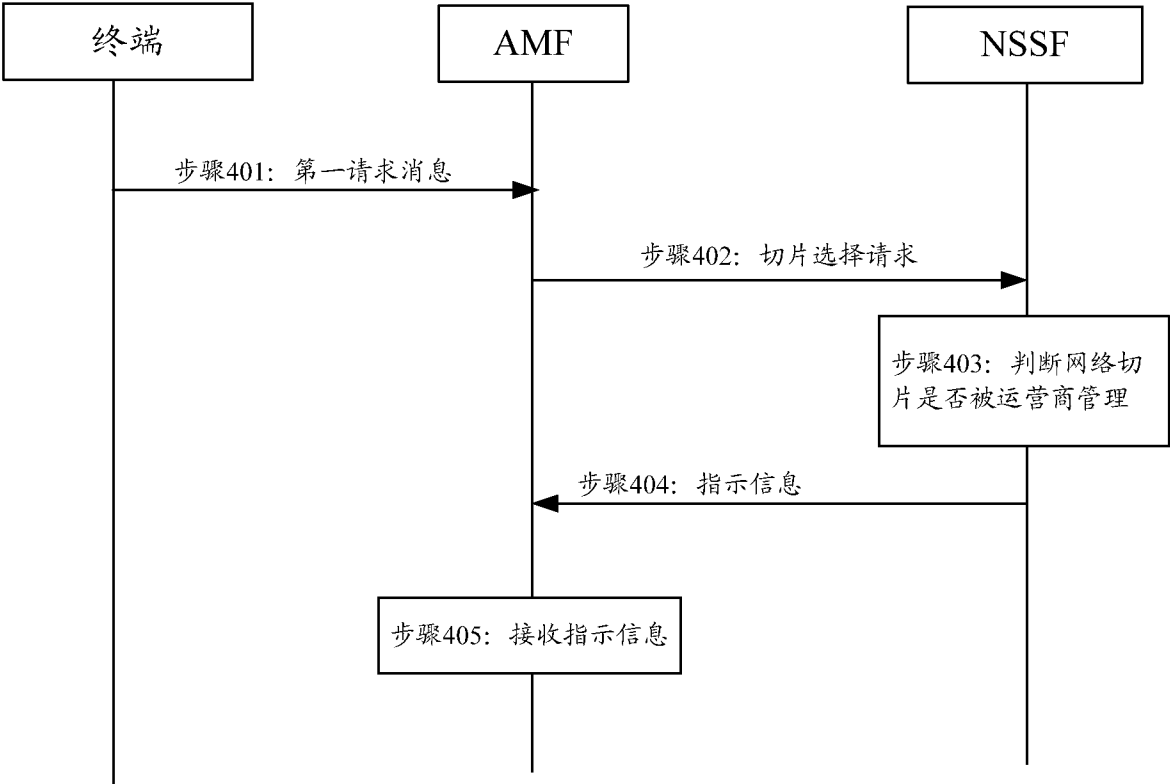


图 4

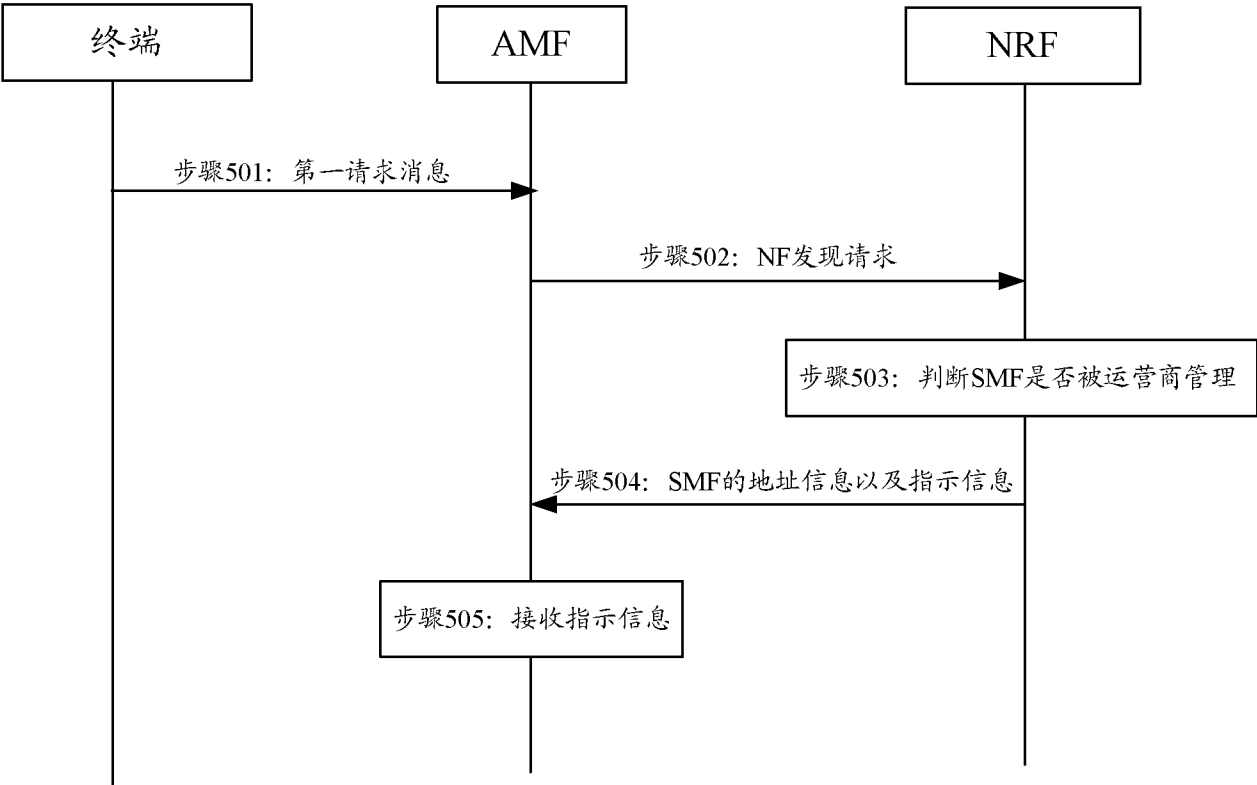


图 5

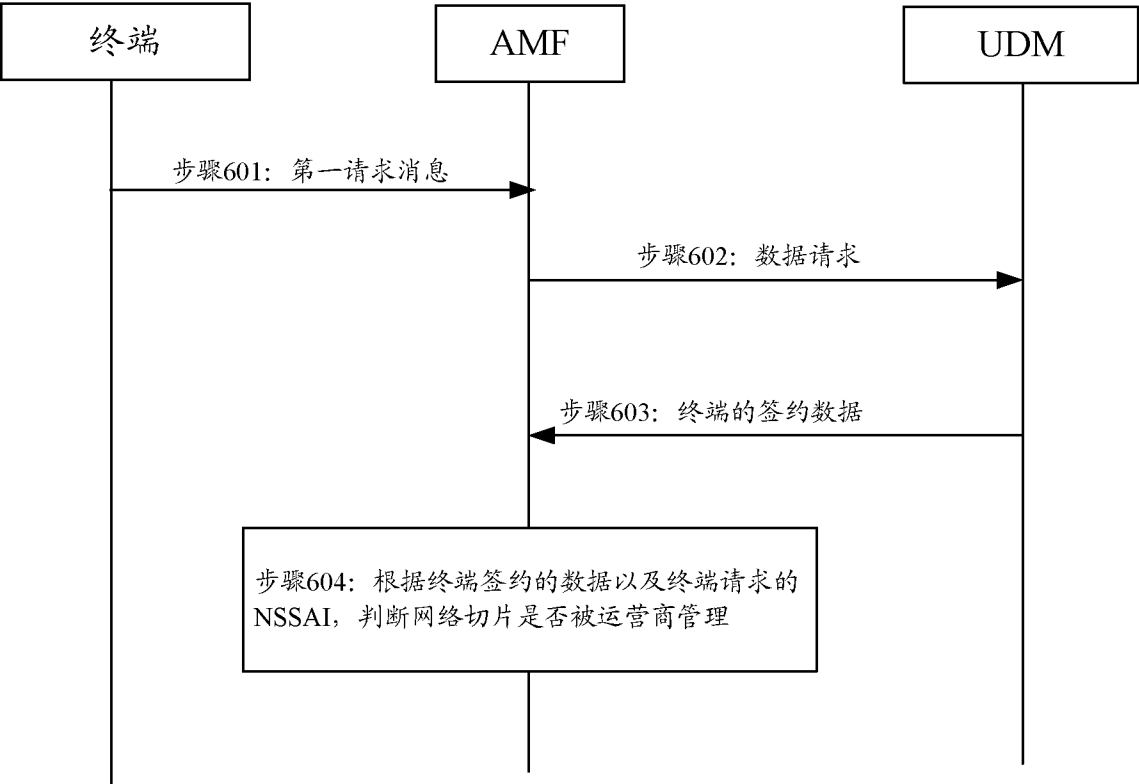


图 6

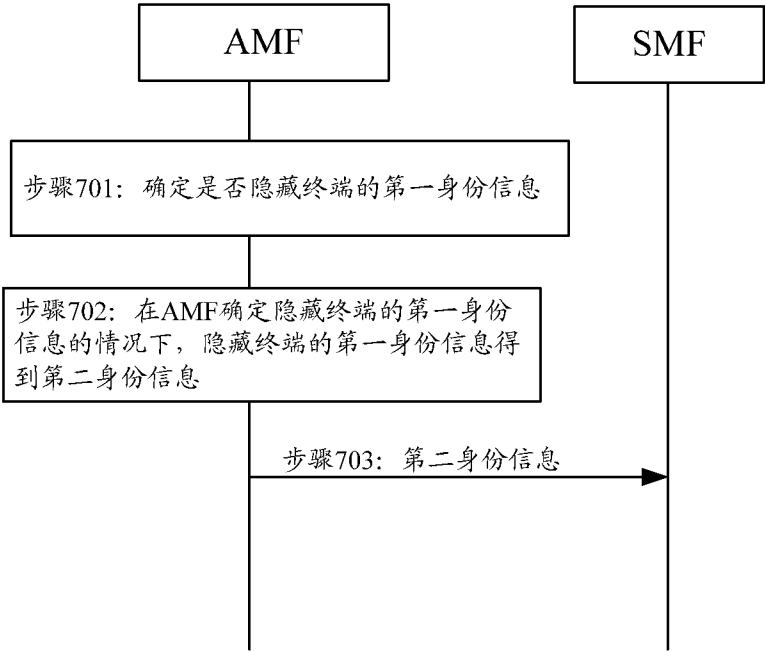


图 7

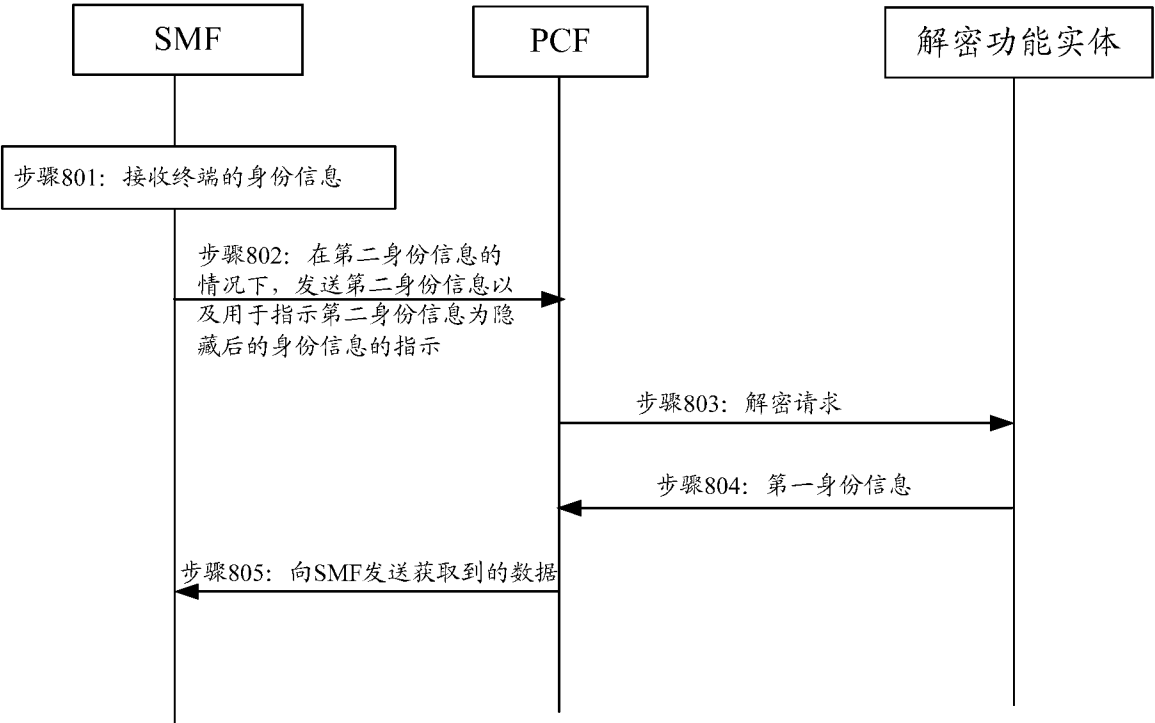


图 8

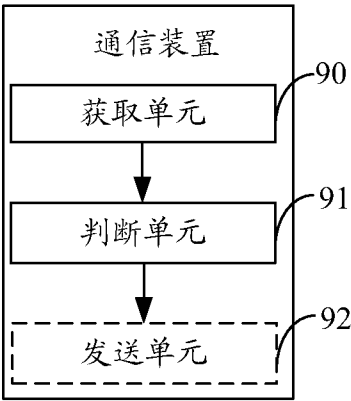


图 9

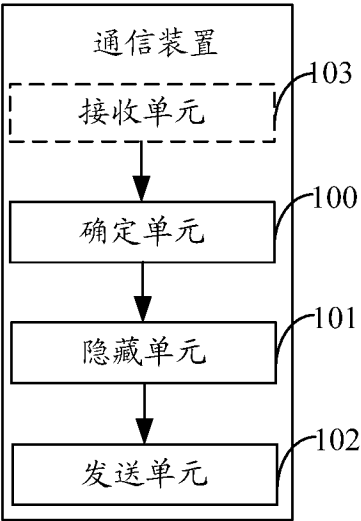


图 10

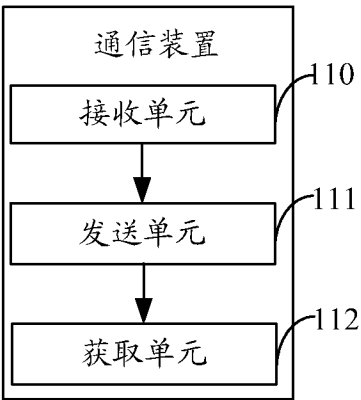


图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/094830

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)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)

CNABS, CNTXT, CNKI, EPTXT, USTXT, WOTXT, VEN: 网络切片, 运营商, 第三方, 垂直行业, 判断, 是否, 身份, 标识, 标志, 标记, 加密, 隐藏, 参数, network slice, operator, the third party, determine, whether, identification, encryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108012267 A (HUAWEI TECHNOLOGIES CO., LTD.) 08 May 2018 (2018-05-08) description, paragraphs [0128]-[0182], and figure 7	1-24
A	CN 108141756 A (SWEDEN TELEFONAKTIEBOLAGET LM ERICSSON) 08 June 2018 (2018-06-08) entire document	1-24
A	CN 107819595 A (TSINGHUA UNIVERSITY) 20 March 2018 (2018-03-20) entire document	1-24
A	WO 2017113109 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 06 July 2017 (2017-07-06) entire document	1-24

☐ 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

20 September 2019

Date of mailing of the international search report

27 September 2019

Name and mailing address of the ISA/CN

**China National Intellectual Property Administration (ISA/
CN)**
**No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
 100088**
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/094830

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108012267	A	08 May 2018	WO	2018077232	A1	03 May 2018
				EP	3506669	A4	21 August 2019
				BR	112019006352	A2	18 June 2019
				US	2019261180	A1	22 August 2019
				EP	3506669	A1	03 July 2019
CN	108141756	A	08 June 2018	EP	3357267	A1	08 August 2018
				US	2017164212	A1	08 June 2017
				WO	2017058067	A1	06 April 2017
CN	107819595	A	20 March 2018	None			
WO	2017113109	A1	06 July 2017	EP	3398305	A4	09 January 2019
				EP	3398305	A1	07 November 2018
				US	2018352501	A1	06 December 2018

国际检索报告

国际申请号

PCT/CN2019/094830

A. 主题的分类

H04W 12/06 (2009.01) 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))

CNABS, CNTXT, CNKI, EPTXT, USTXT, WOTXT, VEN: 网络切片, 运营商, 第三方, 垂直行业, 判断, 是否, 身份, 标识, 标志, 标记, 加密, 隐藏, 参数, network slice, operator, the third party, determine, whether, identification, encryption

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	CN 108012267 A (华为技术有限公司) 2018年 5月 8日 (2018 - 05 - 08) 说明书第[0128]-[0182]段, 附图7	1-24
A	CN 108141756 A (瑞典爱立信有限公司) 2018年 6月 8日 (2018 - 06 - 08) 全文	1-24
A	CN 107819595 A (清华大学) 2018年 3月 20日 (2018 - 03 - 20) 全文	1-24
A	WO 2017113109 A1 (TELEFONAKTIEBOLAGET LM ERICSSON PUBL) 2017年 7月 6日 (2017 - 07 - 06) 全文	1-24

☐ 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

2019年 9月 20日

国际检索报告邮寄日期

2019年 9月 27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

授权官员

李俊洁

电话号码 86-(010)-62412275

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/094830

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	108012267	A	2018年 5月 8日	WO	2018077232	A1	2018年 5月 3日
				EP	3506669	A4	2019年 8月 21日
				BR	112019006352	A2	2019年 6月 18日
				US	2019261180	A1	2019年 8月 22日
				EP	3506669	A1	2019年 7月 3日
CN	108141756	A	2018年 6月 8日	EP	3357267	A1	2018年 8月 8日
				US	2017164212	A1	2017年 6月 8日
				WO	2017058067	A1	2017年 4月 6日
CN	107819595	A	2018年 3月 20日	无			
WO	2017113109	A1	2017年 7月 6日	EP	3398305	A4	2019年 1月 9日
				EP	3398305	A1	2018年 11月 7日
				US	2018352501	A1	2018年 12月 6日