(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 9 月 10 日 (10.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/177523 A1

(51) 国际专利分类号:
H04W 76/10 (2018.01) *H04W 24/02* (2009.01)

(21) 国际申请号: PCT/CN2020/075611

(22) 国际申请日: 2020 年 2 月 17 日 (17.02.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910160313.6 2019年3月4日 (04.03.2019) 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: 雷 中 定 (**LEI, Zhongding**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

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

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

WO 2020/177523 A1

(54) **Title:** REGISTRATION METHOD AND APPARATUS FOR TERMINAL DEVICE

(54) 发明名称: 终端设备的注册方法及装置

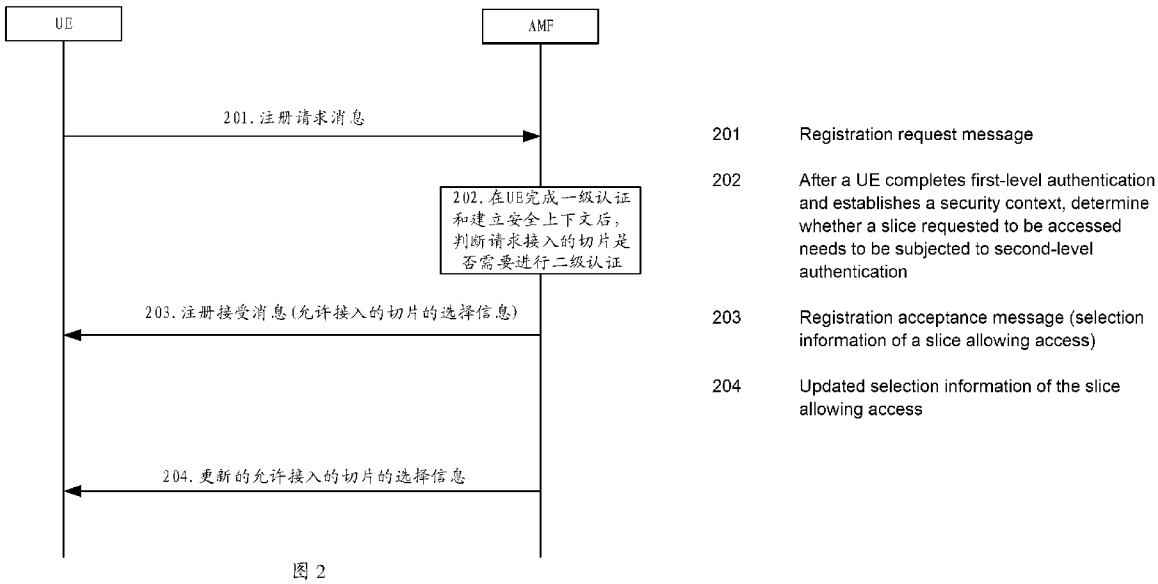

图 2

(57) **Abstract:** Provided are a registration method and apparatus for a terminal device. In the method, the time when a network sends a registration acceptance message is earlier than the time when a registration acceptance message is sent in a registration process in the prior art, i.e. in the present application, the registration acceptance message is sent once first-level authentication on a terminal device has been completed and a security context has been established, whereas in the prior art, the registration acceptance message is sent only after second-level authentication on all slices has been completed. In this way, not only can the problem caused by nested authentication be solved, access flexibility of a terminal device can also be greatly increased, so that the setting or management of a timer during registration becomes simpler. At this moment, the terminal device can determine, according to second-level authentication

[见续页]

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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

information fed back by the network, the time for which performing second-level authentication is more convenient for the terminal device. For example, according to a slice that has been authenticated successfully, the terminal device can access the slice, establish a session, and send and receive a data service. In addition, the terminal device then requests access to other slices when later being idle.

(57) 摘要：本申请提供终端设备的注册方法及装置。该方法中，网络发送注册接受消息比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对终端设备的一级认证和建立安全上下文之后就发送注册接受消息，而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，终端设备也大大增加了接入的灵活性，并且使得注册时的定时器的设置或管理变得更为简便。此时，终端设备可以根据网络反馈的二级认证信息，决定何时进行二级认证对终端设备更方便。比如，终端设备可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

终端设备的注册方法及装置

相关申请的交叉引用

本申请要求在2019年03月04日提交中国专利局、申请号为201910160313.6、申请名称为“终端设备的注册方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及移动通信技术领域，尤其涉及终端设备的注册方法及装置。

背景技术

终端设备在接入网络或切片之前，需要同切片进行双向认证并得到网络的授权。目前，终端设备和网络之间可能需要两级认证。其中，终端设备和运营商网络之间的认证称为一级认证，终端设备和运营商网络之外的第三方网络之间的认证称为二级认证。

目前，一种可能的认证方式为：终端设备发起注册请求->运营商网络的一级认证->第三方网络的二级认证->网络对终端设备接入的切片的授权->注册完成。

上述认证流程主要有以下缺点：

1)、注册、认证的计时器（timer）的设置、管理问题。由于二级认证是终端设备同第三方网络之间的认证，第三方网络负责认证的认证服务器计算资源可以大有不同，这也会造成完成二级认证所需的时间长短有别。再进一步，一次注册流程可以支持嵌套多次的二级认证，这将使得完成二级认证流程的时间大相径庭。然而，注册、认证流程在具体实现中，会针对总体流程以及每个关键步骤事先设定计时器，每个计时的步骤或流程如果超时，就会产生运行错误。另外，当进行二级认证时，网络也可以通过暂停、恢复注册流程的计时器来缓解计时器设定问题，但这由引入了计时器管理复杂的新问题。总之，由于上述因素造成的二级认证时间差异性，使得系统设定计时器问题变成了复杂而具有挑战的任务。

2)、整个注册流程由于二级认证的拖累，可能会被显著延长，造成用户体验等其他问题。终端设备或用户通常希望尽快使用可接入的服务，而不是长时间在注册流程中等待。

发明内容

本申请提供终端设备的注册方法及装置，用以解决终端设备的注册流程中存在的注册、认证的计时器难以设置或管理，注册流程时间较长的问题，以达到简化计时器的设置和缩短初始注册流程的时长的目的。

第一方面，终端设备向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；在所述终端设备完成一级认证和建立安全上下文后，所述终端设备接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择

信息；在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，所述终端设备接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

基于该方案，网络发送注册接受消息比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对终端设备的一级认证和建立安全上下文之后就发送注册接受消息（通过提前发送注册接受消息，初始注册流程可以尽早结束，不过这仅仅代表暂时（Interim）结束，而不是完全结束，因为还有二级认证没完成），而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，终端设备也大大增加了接入的灵活性，并且使得注册时的定时器的设置或管理变得更为简便。此时，终端设备可以根据网络反馈的二级认证信息，决定何时进行二级认证对终端设备更方便。比如，终端设备可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

在一种可能的实现方法中，所述第一注册接受消息还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片的选择信息、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识；其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

在一种可能的实现方法中，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述终端设备向所述移动性管理网元发送第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。所述终端设备接收更新的允许接入的切片的选择信息，包括：所述终端设备接收来自所述移动性管理网元的第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

在一种可能的实现方法中，所述终端设备接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，包括：所述终端设备接收来自所述移动性管理网元的配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述配置更新命令还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择

信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识；其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

第二方面，移动性管理网元接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；在所述终端设备完成一级认证和建立安全上下文后，所述移动性管理网元判断所述请求接入的切片是否需要进行二级认证；所述移动性管理网元向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息；在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，所述移动性管理网元向所述终端设备发送更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

基于该方案，网络发送注册接受消息比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对终端设备的一级认证和建立安全上下文之后就发送注册接受消息(通过提前发送注册接受消息，注册流程可以尽早结束，不过这仅仅代表暂时(Interim)结束，而不是完全结束，因为还有二级认证没完成)，而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，终端设备也大大增加了接入的灵活性，并且使得注册时的定时器的设置或管理变得更为简便。此时，终端设备可以根据网络反馈的二级认证信息，决定何时进行二级认证对终端设备更方便。比如，终端设备可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

在一种可能的实现方法中，所述第一注册接受消息还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片的选择信息、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识；其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的一个或多个切片的选择信息。

在一种可能的实现方法中，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述移动性管理网元接收来自所述终端设备的第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证；所述移动性管理网元向所述终端设备发送更新的允许接入的切片的选择信息，包括：所述移动性管理网元向所述终端设备发送第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；所述第二切片认证指

示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

在一种可能的实现方法中，所述移动性管理网元向所述终端设备发送更新的允许接入的切片的选择信息，包括：所述移动性管理网元向所述终端设备发送配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述配置更新命令还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识；其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

第三方面，终端设备向所述移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；在所述终端设备完成一级认证和建立安全上下文后，所述终端设备接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；所述终端设备向所述移动性管理网元发送第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；在所述需要进行二级认证的切片中的第一切片二级认证通过后，所述终端设备接收来自所述移动性管理网元的第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

基于该方案，网络发送注册接受消息比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对终端设备的一级认证和建立安全上下文之后就发送注册接受消息(通过提前发送注册接受消息，注册流程可以尽早结束，不过这仅仅代表暂时(Interim)结束，而不是完全结束，因为还有二级认证没完成)，而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，终端设备也大大增加了接入的灵活性，并且使得注册时的定时器的设置或管理变得更为简便。此时，终端设备可以根据网络反馈的二级认证信息，决定何时进行二级认证对终端设备更方便。比如，终端设备可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

在一种可能的实现方法中，所述需要进行二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息还包括所述分组信息指示了所述需要进行二级认证的切片的分组信息，所述分组信息指示了各分组进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二

注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

第四方面，移动性管理网元接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；在所述终端设备完成一级认证和建立安全上下文后，所述移动性管理网元向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；所述移动性管理网元接收来自所述终端设备的第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；在所述需要进行二级认证的切片中的第一切片二级认证通过后，所述移动性管理网元向所述终端设备发送第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

基于该方案，网络发送注册接受消息比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对终端设备的一级认证和建立安全上下文之后就发送注册接受消息(通过提前发送注册接受消息，注册流程可以尽早结束，不过这仅仅代表暂时(Interim)结束，而不是完全结束，因为还有二级认证没完成)，而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，终端设备也大大增加了接入的灵活性，并且使得注册时的定时器的设置或管理变得更为简便。此时，终端设备可以根据网络反馈的二级认证信息，决定何时进行二级认证对终端设备更方便。比如，终端设备可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

在一种可能的实现方法中，所述需要进行二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息还包括所述分组信息指示了所述需要进行二级认证的切片的分组信息，所述分组信息指示了各分组进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

第五方面，本申请提供一种通信装置，该装置具有实现上述任意方面或任意方面中的实现方法的功能。该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。该硬件或软件包括一个或多个与上述功能相对应的模块。

第六方面，本申请提供一种通信装置，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，以使该装置执行如上述任意方面或任意方面中的实现方法。

第七方面，本申请提供一种通信装置，包括：包括用于执行以上任意方面各个步骤的单元或手段（means）。

第八方面，本申请提供一种通信装置，包括处理器和接口电路，所述处理器用于通过

接口电路与其它装置通信，并执行以上任意方面提供的任意方法。该处理器包括一个或多个。

第九方面，本申请提供一种通信装置，包括处理器，用于与存储器相连，用于调用所述存储器中存储的程序，以执行上述任意方面的任意实现方式中的方法。该存储器可以位于该装置之内，也可以位于该装置之外。且该处理器包括一个或多个。

第十方面，本申请还提供一种计算机可读存储介质，所述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，使得处理器执行上述任意方面所述的方法。

第十一方面，本申请还提供一种包括指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述任意方面所述的方法。

第十二方面，本申请还提供一种芯片系统，包括：处理器，用于执行上述各方面所述的方法。

第十三方面，本申请还提供一种通信系统，包括用于执行上述第一方面或第一方面任一实现方法的终端设备和用于执行上述第二方面或第二方面任一实现方法的移动性管理网元。

第十四方面，本申请还提供一种通信系统，包括用于执行上述第三方面或第三方面任一实现方法的终端设备和用于执行上述第四方面或第四方面任一实现方法的移动性管理网元。

附图说明

图 1 为本申请提供的一种可能的网络架构示意图；
图 2 为本申请提供的一种终端设备的注册方法流程示意图；
图 3 为本申请提供的又一种终端设备的注册方法流程示意图；
图 4 为本申请提供的又一种终端设备的注册方法流程示意图；
图 5 为本申请提供的又一种终端设备的注册方法流程示意图；
图 6 为本申请提供的又一种终端设备的注册方法流程示意图；
图 7 为本申请提供的又一种终端设备的注册方法流程示意图；
图 8 为本申请提供的一种通信装置示意图；
图 9 为本申请提供的又一种通信装置示意图；
图 10 为本申请提供的又一种通信装置示意图。

具体实施方式

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

为了使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请作进一步地详细描述。方法实施例中的具体操作方法也可以应用于装置实施例或系统实施例中。其中，在本申请的描述中，除非另有说明，“多个”的含义是两个或两个以上。

如图 1 所示，为基于服务化架构的第五代（the 5th generation，5G）网络架构示意图。图 1 所示的 5G 网络架构中可包括三部分，分别是终端设备部分、数据网络（data network，

DN）和运营商网络部分。

其中，运营商网络可包括网络开放功能（network exposure function，NEF）网元、网络存储功能（network function repository function，NRF）网元、策略控制功能（policy control function，PCF）网元、统一数据管理（unified data management，UDM）网元、应用功能（application function，AF）网元、认证服务器功能（authentication server function，AUSF）网元、接入与移动性管理功能（access and mobility management function，AMF）网元、会话管理功能（session management function，SMF）网元、（无线）接入网（(radio)access network，(R)AN）以及用户面功能（user plane function，UPF）网元等。上述运营商网络中，除(无线)接入网部分之外部分，称为核心网络部分。为方便说明，后续以(R)AN 称为 RAN 为例进行说明。

本申请的终端设备（也可以称为用户设备（user equipment，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）。所述终端可以是手机（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、增强现实（augmented reality，AR）终端、工业控制（industrial control）中的无线终端、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）中的无线终端等。

上述终端设备可通过运营商网络提供的接口（例如 N1 等）与运营商网络建立连接，使用运营商网络提供的数据和/或语音等服务。终端设备还可通过运营商网络访问 DN，使用 DN 上部署的运营商业务，和/或第三方提供的业务。其中，上述第三方可为运营商网络和终端设备之外的服务方，可为终端设备提供他数据和/或语音等服务。其中，上述第三方的具体表现形式，具体可根据实际应用场景确定，在此不做限制。

RAN 是运营商网络的子网络，是运营商网络中业务节点与终端设备之间的实施系统。终端设备要接入运营商网络，首先是经过 RAN，进而可通过 RAN 与运营商网络的业务节点连接。本申请中的 RAN 设备，是一种为终端设备提供无线通信功能的设备，接入网设备包括但不限于：5G 中的下一代基站(g nodeB，gNB)、演进型节点 B（evolved node B，eNB）、无线网络控制器（radio network controller，RNC）、节点 B（node B，NB）、基站控制器（base station controller，BSC）、基站收发台（base transceiver station，BTS）、家庭基站（例如，home evolved nodeB，或 home node B，HNB）、基带单元（baseBand unit，BBU）、传输点(transmitting and receiving point，TRP)、发射点(transmitting point，TP)、移动交换中心等。

AMF 网元是由运营商网络提供的控制面网元，负责终端设备接入运营商网络的接入控制和移动性管理，例如包括移动状态管理，分配用户临时身份标识，认证和授权用户等功能。

SMF 网元是由运营商网络提供的控制面网元，负责管理终端设备的协议数据单元（protocol data unit，PDU）会话。 PDU 会话是一个用于传输 PDU 的通道，终端设备需要通过 PDU 会话与 DN 互相传送 PDU。PDU 会话由 SMF 网元负责建立、维护和删除等。SMF 网元包括会话管理（如会话建立、修改和释放，包含 UPF 和 AN 之间的隧道维护）、UPF 网元的选择和控制、业务和会话连续性（Service and Session Continuity，SSC）模式选

择、漫游等会话相关的功能。

UPF 网元是由运营商提供的网关，是运营商网络与 DN 通信的网关。UPF 网元包括数据包路由和传输、包检测、业务用量上报、服务质量（Quality of Service, QoS）处理、合法监听、上行包检测、下行数据包存储等用户面相关的功能。

DN，也可以称为分组数据网络(packet data network，PDN)，是位于运营商网络之外的网络，运营商网络可以接入多个 DN，DN 上可部署多种业务，可为终端设备提供数据和/或语音等服务。例如，DN 是某智能工厂的私有网络，智能工厂安装在车间的传感器可为终端设备，DN 中部署了传感器的控制服务器，控制服务器可为传感器提供服务。传感器可与控制服务器通信，获取控制服务器的指令，根据指令将采集的传感器数据传送给控制服务器等。又例如，DN 是某公司的内部办公网络，该公司员工的手机或者电脑可为终端设备，员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。

UDM 网元是由运营商提供的控制面网元，负责存储运营商网络中签约用户的用户永久标识符(subscriber permanent identifier，SUPI)、信任状（credential）、安全上下文（security context）、签约数据等信息。UDM 网元所存储的这些信息可用于终端设备接入运营商网络的认证和授权。其中，上述运营商网络的签约用户具体可为使用运营商网络提供的业务的用户，例如使用中国电信的手机芯卡的用户，或者使用中国移动的手机芯卡的用户等。上述签约用户的永久签约标识（Subscription Permanent Identifier，SUPI）可为该手机芯卡的号码等。上述签约用户的信任状、安全上下文可为该手机芯卡的加密密钥或者跟该手机芯卡加密相关的信息等存储的小文件，用于认证和/或授权。上述安全上下文可为存储在用户本地终端（例如手机）上的数据（cookie）或者令牌（token）等。上述签约用户的签约数据可为该手机芯卡的配套业务，例如该手机芯卡的流量套餐或者使用网络等。需要说明的是，永久标识符、信任状、安全上下文、认证数据（cookie）、以及令牌等同认证、授权相关的信息，在本发明本申请文件中，为了描述方便起见不做区分、限制。如果不做特殊说明，本申请实施例将以用安全上下文为例进行来描述，但本申请实施例同样适用于其他表述方式的认证、和/或授权信息。

AUSF 网元是由运营商提供的控制面网元，通常用于一级认证，即终端设备（签约用户）与运营商网络之间的认证。AUSF 网元接收到签约用户发起的认证请求之后，可通过UDM 网元中存储的认证信息和/或授权信息对签约用户进行认证和/或授权，或者通过UDM 网元生成签约用户的认证和/或授权信息。AUSF 网元可向签约用户反馈认证信息和/或授权信息。

NEF 网元是由运营商提供控制面网元。NEF 网元以安全的方式对第三方开放运营商网络的对外接口。在 SMF 网元需要与第三方的网元通信时，NEF 网元可作为 SMF 网元与第三方的网元通信的中继。NEF 网元作为中继时，可作为签约用户的标识信息的翻译，以及第三方的网元的标识信息的翻译。比如，NEF 将签约用户的 SUPI 从运营商网络发送到第三方时，可以将 SUPI 翻译成其对应的外部身份标识（identity，ID）。反之，NEF 网元将外部 ID（第三方的网元 ID）发送到运营商网络时，可将其翻译成 SUPI。

PCF 网元是由运营商提供的控制面功能，用于向 SMF 网元提供 PDU 会话的策略。策略可以包括计费相关策略、QoS 相关策略和授权相关策略等。

网络切片选择功能（Network Slice Selection Function，NSSF）网元（图中未示出），负责确定网络切片实例，选择 AMF 网元等。

图 1 中 Nnef、Nausf、Nnrf、Npcf、Nudm、Naf、Namf、Nsmf、N1、N2、N3、N4，以及 N6 为接口序列号。这些接口序列号的含义可参见 3GPP 标准协议中定义的含义，在此不做限制。

本申请中的移动性管理网元可以是图 1 所示的 AMF 网元，也可以是未来通信系统中的具有上述 AMF 网元的功能的网元。或者，本申请中的移动性管理网元还可以是长期演进（long term evolution，LTE）中的移动性管理实体（mobility management entity，MME）等。

为方便说明，本申请后续，以移动性管理网元为 AMF 网元为例进行说明。进一步地，将 AMF 网元简称为 AMF，将终端设备称为 UE，即本申请后续所描述的 AMF 均可替换为移动性管理网元，UE 均可替换为终端设备。

为便于理解本申请内容，下面对本申请涉及的一些通信术语进行解释说明。需要说明的是，该部分内容也作为本申请发明内容的一部分。

一、切片

本申请中的“切片”也可以称为“网络切片”，或称为“网络切片实例”，三者具有相同的含义，这里统一说明，后续不再赘述。

目前，多种多样的场景对第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）生态系统提出了不同的需求，如计费、策略、安全、移动性等需求。3GPP 强调了网络切片之间不相互影响，例如突发的大量的抄表业务不应该影响正常的移动宽带业务。为了满足多样性需求和切片间的隔离，需要业务间相对独立的管理和运维，并提供量身定做的业务功能和分析能力。不同类型业务的实例部署在不同的网络切片上，相同业务类型的不同实例也可部署在不同的网络切片上。

5G 网络中的切片是一个虚拟的专用网络，它是由一组网络功能、子网络所构成。比如，图 1 中的 RAN、AMF、SMF、UPF 可以组成一个切片。图 1 中的每种网络功能只示意性地画出了一个，而在实际网络部署中，每种网络功能或子网络可以有多个、数十个或上百个。运营商网络中可以部署很多网络切片，每个切片可以有不同的性能来满足不同应用、不同垂直行业的需求。运营商可以根据不同垂直行业客户的需求，“量身定做”一个切片。运营商也可以允许一些行业客户享有较大的自主权，参与切片的部分管理、控制功能。其中，切片级的认证就是由行业客户参与的一种网络控制功能，即对终端用户接入切片进行认证和授权。

当核心网部署了网络切片，用户初始附着（或称为注册）到网络时，会触发网络切片的选择过程。切片的选择过程取决于用户的签约数据，本地配置信息，漫游协议，运营商的策略等等。在网络切片的选择过程中，需要综合考虑以上参数，才能为 UE 选择最佳的切片类型。

当 UE 需要接入到某个网络切片时，UE 可以提供请求的网络切片给核心网，用于核心网为 UE 选择网络切片实例。其中，UE 请求的网络切片，可以用请求的网络切片集合来表示，或者也可以表示为请求的网络切片选择辅助信息（requested network slice selection assistance information，requested NSSAI）。requested NSSAI 是由一个或多个单网络切片选择辅助信息（single network slice selection assistance information，S-NSSAI）来表示构成，每个 S-NSSAI 用于标识一个网络切片类型，也可以理解为，S-NSSAI 用于标识网络切片，或者可以理解为 S-NSSAI 是网络切片的标识信息。为了简单起见，在以下的描述中，对“网

络切片”或是“S-NSSAI”不做严格区分，可以同样适用。

UE 注册到网络之后，核心网网元（如 AMF 或 NSSF）根据 UE 的签约数据、UE 的 requested NSSAI、漫游协议以及本地配置等信息综合判断，为 UE 选择允许接入的网络切片集合。其中，允许接入的网络切片集合可以用允许的（allowed）NSSAI 来表示，allowed NSSAI 包含的 S-NSSAI 均为当前运营商网络允许接入的 S-NSSAI。

二、接入网络切片的认证与授权

UE 在接入网络或网络切片之前，需要同网络切片进行双向认证并得到网络的授权。目前在 5G 标准中，网络对 UE 的认证与授权都是由运营商网络直接进行，这类认证授权方法被称为 Primary Authentication（一级认证）。随着垂直行业和物联网的发展，可以预见，运营商网络之外的 DN（如服务于垂直行业的 DN），对于接入到该 DN 的 UE 同样有认证与授权的需求。比如，某商业公司提供了游戏平台，通过运营商网络，为游戏玩家提供游戏服务。一方面，由于玩家使用的 UE 是通过运营商网络接入游戏平台，运营商网络需要对该 UE 进行认证和授权，即一级认证。游戏玩家是商业公司的客户，该商业公司也需要对游戏玩家进行认证、授权，这种认证如果是基于网络切片的，或者它的颗粒度（granularity）是以切片为单位的，则该认证可以称为切片认证（slice authentication）或称为二级认证（secondary authentication），或称为基于切片的二级认证（slice-specific secondary authentication）。

需要说明的是，不管是上述一级认证，还是二级认证，都是针对 UE(及或使用该 UE 的某个用户)与网络（运营商网络或第三方网络）之间的认证。比如，针对一级认证，指的是 UE 与运营商网络之间的认证，如在 UE 的注册流程中运营商网络对 UE 执行一级认证，若一级认证通过则可以建立该 UE 的安全上下文。再比如，针对二级认证，指的是 UE（或使用该 UE 的用户）与运营商网络之外的网络（即第三方网络）之间的认证，第三方网络会将二级认证结果通知运营商网络，以便运营商网络授权或拒绝该 UE 接入为第三方网络服务的运营商网络。

需要说明的是，本申请后续有时也将二级认证称为对切片的二级认证，其具有的含义实际是：UE（或使用该 UE 的用户）与第三方网络之间执行的二级认证，其认证结果，将会决定运营商网络是否授权 UE 接入该切片。

在目前已经发布的 5G 标准中，只支持一级认证。UE 需要接入切片时，在一级认证之后，由网络（如 UDM、AMF 或 NSSF 等网络功能）根据存储在 UDM 的 UE 与网络的签约数据和其他信息，为 UE 选择适合的切片并由 AMF 把允许 UE 接入的切片的授权信息（即 allowed NSSAI）发送给 UE。

为了更好的支持垂直行业的应用，例如支持上述的游戏公司对玩家的认证与授权，3GPP 正在研究如何有效地同时支持这两种认证（即一级认证和二级认证）的机制。

在一种可能的实现方法中，以下给出了一种同时包括一级认证和二级认证的 UE 的注册流程的大致过程：

步骤 1，UE 向 AMF 发送接入网络的注册申请（如 UE 发送注册请求消息）。

步骤 2，AMF 根据 UE 的签约信息，发起同 UE 进行一级认证。

步骤 3，一级认证成功后，AMF 确定该 UE 是否还需要进一步的二级认证。

步骤 4，如果需要，AMF 发起二级认证流程，通知 UE 和 DN 进行二级认证，并转发 UE 和 DN 之间认证所需的各种交互信息。

步骤 5，当 UE 和 DN 的二级认证成功后，DN 向 AMF 发送认证成功消息。

步骤 6，AMF 根据认证成功消息以及其他网络信息，为 UE 选择切片，确定 allowed NSSAI。

步骤 7，AMF 将授权信息（即 allowed NSSAI）通过注册接受消息发送给 UE，完成注册流程。

上述注册流程，是一种被称之为“嵌套式”（nested）的流程。所谓“嵌套”，可以有两种理解：1）二级认证和一级认证被一起嵌套在初始注册流程中，即完整的注册流程是：注册请求->运营商网络的一级认证->第三方网络的二级认证->网络（运营商网络和第三方网络）对 UE 接入的切片的授权（allowed NSSAI）->注册完成；2）二级认证被嵌套在一级认证和网络授权过程中，即运营商网络的一级认证->第三方网络的二级认证->网络对 UE 接入的切片的授权（allowed NSSAI）。

上述嵌套式的二级认证流程主要有以下缺点：

1）、注册、认证的计时器（timer）的设置、管理问题。根据目前 3GPP 标准化的结论，二级认证可能会采用基于标准组织 IETF（Internet Engineering Task Force）制定的 EAP（Extensible Authentication Protocol）标准作为基本认证机制，并且支持多种 EAP 认证方法（EAP method）。由于不同的 EAP 认证方法，所需的认证流程、计算资源不同，完成认证所需的时间也有所不同。进一步，二级认证是 UE（或使用 UE 的用户）同外部网络之间的认证，外部网络负责认证的认证服务器计算资源可以大有不同，3GPP 网络与具有不同网络资源的网络之间信息交互的网络拥塞状况也会不同，这也会造成完成二级认证所需的时间长短有别。再进一步，一级注册流程可以支持嵌套多次的二级认证（分别对应多个不同的 S-NSSAI），综上因素，都可以使得完成二级认证流程的时间大相径庭。然而，注册、认证流程在具体实现中，会针对总体流程以及每个关键步骤事先设定计时器，每个计时的步骤或流程如果超时，就会产生运行错误。另外，当进行二级认证时，网络也可以以通过暂停、恢复注册流程的计时器来缓解计时器设定问题，但这又会引入计时器管理复杂等新问题。总之，由于上述因素造成的切片认证时间差异性，使得系统设定计时器问题变成了复杂而具有挑战的任务。

2）、整个注册流程由于二级认证的拖累，可能会被显著延长，造成用户体验等其他问题。UE 或用户通常希望尽快使用可接入的服务，而不是长时间在注册流程中等待。

3）、一级认证的独立性问题。在已经发布的 5G 标准中，只要运营商网络的一级认证成功，UE 就可以接入网络、建立会话连接等。而上述嵌套式的认证流程中，即使网络的一级认证成功，注册流程还需要等待外部网络的二级认证完成才可以被接入网络。

为解决上述问题，本申请提供多种 UE 的注册方法，下面具体说明。

基于图 1 所示的架构，如图 2 所示，为本申请提供的一种 UE 的注册方法流程示意图。该方法包括以下步骤：

步骤 201，UE 向 AMF 发送注册请求（registration request）消息，相应地，AMF 可以接收到该注册请求消息。

这里的注册请求消息在本申请中也可以称为第一注册请求消息。该注册请求消息用于请求注册至网络。

该注册请求消息包括请求接入的切片的选择信息，该请求接入的切片的选择信息可以称为 requested NSSAI, requested NSSAI 中包括一个或多个 S-NSSAI。作为示例，requested

NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI 5、S-NSSAI 6}，其中，S-NSSAI1 对应切片 1，S-NSSAI2 对应切片 2，S-NSSAI3 对应切片 3，S-NSSAI4 对应切片 4，S-NSSAI5 对应切片 5，S-NSSAI6 对应切片 6，即 UE 请求接入切片 1、切片 2、切片 3、切片 4、切片 5 和切片 6。

步骤 202，在 UE 完成一级认证和建立安全上下文后，AMF 判断请求接入的切片是否需要进行二级认证。

作为示例，requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，比如 AMF 确定 S-NSSAI1 对应的切片 1、S-NSSAI2 对应的切片 2、S-NSSAI3 对应的切片 3、S-NSSAI4 对应的切片 4 需要进行二级认证，S-NSSAI5 对应的切片 5 和 S-NSSAI6 对应的切片 6 不需要进行二级认证。

需要说明的是，步骤 201 中所述的建立安全上下文，可以是指非接入层（Non-Access Stratum，NAS）安全上下文的建立，也可以是指 NAS 安全上下文和接入层（Access Stratum ，AS）安全上文的建立。这里不做限定。需要进一步说明的是，这一点同样适用于本申请中其他处的描述，这里做统一说明，后续不再一一重复说明。

步骤 203，AMF 向 UE 发送注册接受（registration accept）消息，相应地，UE 可以接收到该注册接受消息。

这里的注册接受消息在本申请中也可以称为第一注册接受消息。

该注册接受消息包括允许接入的切片的选择信息，该允许接入的切片的选择信息比如可以是 allowed NSSAI, allowed NSSAI 中包括一个或多个 S-NSSAI。

具体的，该 allowed NSSAI 包括以下信息中的至少一个:

1）、请求接入的切片中已经完成二级认证的切片的选择信息。

请求接入的切片中已经完成二级认证的切片的选择信息，在一种实现方法中，还可以包括网络分配的与请求接入的切片的选择信息对应的切片的选择信息。

2）、请求接入的切片中不需要进行二级认证的切片的选择信息。

请求接入的切片中不需要进行二级认证的切片的选择信息，在一种实现方法中，还可以包括网络分配的与请求接入的切片的选择信息对应的切片的选择信息。

3）、网络分配的不需要进行二级认证的切片的选择信息。

这里的网络分配的不需要进行二级认证的切片的选择信息具体指的是：由网络分配的不包含在请求接入的切片的选择信息中的（或者由网络分配的不包含在与请求接入的切片的选择信息相对应的切片的选择信息中的）、且不需要进行二级认证的切片的选择信息。

下面结合上面的示例继续说明。即 requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，S-NSSAI1 对应的切片 1、S-NSSAI2 对应的切片 2、S-NSSAI3 对应的切片 3、S-NSSAI4 对应的切片 4 需要进行二级认证，S-NSSAI5 对应的切片 5 和 S-NSSAI6 对应的切片 6 不需要进行二级认证。

比如，UE 和运营商网络之间完成了一级认证、且对切片 5 和切片 6 通过了授权(不需要二级认证)，则 allowed NSSAI 可以包括 S-NSSAI5、S-NSSAI6。这里的 S-NSSAI5 和 S-NSSAI6 即为请求接入的切片中不需要进行二级认证的切片的选择信息。

再比如，在 UE 和运营商网络完成一级认证和建立安全上下文的过程之后，运营商网络认为切片 1 的认证过程短暂，并发起了对切片 1 的二级认证。当 UE 和运营商网络之外的第三方网络之间针对切片 1 成功完成了二级认证后，运营商网络允许对切片 1 通过授权，

则 allowed NSSAI 还可以包括 S-NSSAI1。这里的 S-NSSAI1 即为请求接入的切片中已经完成二级认证的切片的选择信息。

再比如，运营商网络（如 AMF）和 UE 完成了一级认证，运营商网络分配切片 7 让 UE 接入，即 AMF 确定可以将切片 7 授权给 UE 接入，且该切片 7 是不需要进行二级认证的切片，则 allowed NSSAI 还可以包括 S-NSSAI7（对应切片 7）。这里的 S-NSSAI7 即为网络分配的不需要进行二级认证的切片的选择信息。

综上，在上述示例中，allowed NSSAI 可以包括以下信息中的一个或多个：请求接入的切片中已经完成二级认证的切片的选择信息（即 S-NSSAI1）、请求接入的切片中不需要进行二级认证的切片的选择信息（即 S-NSSAI5 和 S-NSSAI6）、网络分配的不需要进行二级认证的切片的选择信息（即 S-NSSAI7）。

另外需要说明的是，作为一种实现方法，如果 allowed NSSAI 中包括了请求接入的切片中已经完成二级认证的切片的选择信息或者包括了请求接入的切片中不需要进行二级认证的切片的选择信息，那么网络也可以不用分配额外的切片的选择信息。相反，如果 allowed NSSAI 中不包括任何请求接入的切片中已经完成二级认证的切片的选择信息，或者不包括任何请求接入的切片中不需要进行二级认证的切片的选择信息，那么网络一定要基于一级认证，分配一个不需要进行二级认证的切片的选择信息。在上述例子中，allowed NSSAI 包括了 S-NSSAI1，S-NSSAI5 和 S-NSSAI6，这时，网络可以不再分配 S-NSSAI7 给 UE。相反，如果 S-NSSAI5 和 S-NSSAI6 也需要但还没进行切片认证，针对 S-NSSAI1 的切片认证也没完成，此时网络必须分配 S-NSSAI7 给 UE，保证通过一级认证的 UE 至少有一个 S-NSSAI 在 allowed NSSAI 中。

作为一种实现方法，上述注册请求消息中进一步还可以包括以下信息中的至少一个：

1）、请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息。

即 requested NSSAI 中的需要进行二级认证、且未完成二级认证的切片的 S-NSSAI，可以简称为待认证授权的 NSSAI（pending NSSAI），即可以在注册接受消息中增加一个项（IE），用于携带 pending NSSAI。

比如，针对上述示例，requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4 为需要进行二级认证的切片的选择信息，若 S-NSSAI1 对应的切片 1 已经完成了二级认证，则请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息为：S-NSSAI2、S-NSSAI3 和 S-NSSAI4，即 pending NSSAI={ S-NSSAI2、S-NSSAI3 和 S-NSSAI4}。

作为一种实现方法，请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息可以携带于一个切片选择信息列表（或切片选择信息 S-NSSAI 列表）中，切片选择信息列表（或切片选择信息 S-NSSAI 列表）中的切片的选择信息的顺序指示了切片选择信息列表（或切片选择信息 S-NSSAI 列表）中的切片进行二级认证的优先级。（为了描述简便，以下的“切片选择信息列表”,代表切片选择信息 S-NSSAI 列表，不再赘述。比如，注册请求消息包括切片选择信息列表 A，该切片选择信息列表 A={ S-NSSAI2、S-NSSAI3、S-NSSAI4}。一方面，该切片选择信息列表 A 指示了请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息包括 S-NSSAI2、S-NSSAI3 和 S-NSSAI4；另一方面，该切片选择信息列表 A 还指示了进行二级认证的优先顺序依次为：S-NSSAI2、S-NSSAI3、S-NSSAI4。

2）、请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间。

这里的预估时间可以使得 UE 在后续发起针对请求接入的切片中需要进行二级认证且未完成二级认证的切片的二级认证时，确定切片的二级认证的先后顺序，比如针对二级认证所需的预估时间较短的切片，则可以优先进行针对该切片的二级认证。UE 也可以根据预估时间只请求部分切片的二级认证，比如切片 2 的预估时间小于一个事先设定的值，UE 只把 S-NSSAI2 放入 requested NSSAI 列表中，从而只对切片 2（或对应的 S-NSSAI）进行切片认证。

3）、切片认证指示。该切片认证指示用于指示存在未完成二级认证的切片。

这里的切片认证指示在本申请中也可以称为第一切片认证指示。

需要说明的是，本申请中任意地方出现的切片认证指示也可以称为指示信息、或二级认证指示，因此，这里的切片认证指示也可以称为第一指示信息、或第一二级认证指示。

该“切片认证指示”还可以用于表示当前的注册接受消息不是最终版的，还有 S-NSSAI 需要认证才能完成所有切片的注册过程。

需要说明的是，在具体实现中，若注册接受消息中携带上述 pending NSSAI，则该 pending NSSAI 可以隐式指示存在未完成二级认证的切片及表示当前的注册接受消息不是最终版的，则此时该切片认证指示是可选的。

4）、请求接入的切片中不需要进行二级认证的切片的选择信息（non-slice authentication NSSAI）。

比如，针对上述示例，requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，S-NSSAI5、S-NSSAI6 为不需要进行二级认证的切片的选择信息，则 non-slice authentication NSSAI={S-NSSAI5、S-NSSAI6}。

UE 可以根据该参数（即 non-slice authentication NSSAI）在以后的注册申请时，参考优化 UE 携带的参数。

5）、请求接入的切片中被拒绝接入的切片的选择信息（rejected NSSAI）。

rejected NSSAI 指被拒绝的 S-NSSAI 的列表。比如，针对上述示例，requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，若 S-NSSAI2 因为某种原因被拒绝（如该 S-NSSAI 同 UE 不匹配，或签约情况变化，或没有通过二级认证等），则可以通过 Rejected NSSAI 携带被拒绝的 S-NSSAI。可选的，注册接受消息中还可以携带拒绝的原因。

在具体实现中，上述 “allowed NSSAI”、“pending NSSAI”、“non-slice authentication NSSAI”、“rejected NSSAI”等可以合并成一个 IE，或以某种组合方式合并成 2 个或多个 IE。

6）、至少一个临时标识。一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

这里的临时标识例如可以是 5G-全球唯一临时 UE 标识（5G- Globally Unique Temporary UE Identity，5G- GUTI）。

当有多个切片完成一级认证和二级认证时，一种方式是每个 5G-GUTI 对应一个或多个切片；另一种方式是，只有一个 5G-GUTI，该 5G-GUTI 对应所有的切片。

5G-GUTI 包含路由信息，在 UE 下次接入时，RAN 设备可以根据该信息选择合适的 AMF 来服务 UE。

步骤 204，在请求接入的切片中需要进行二级认证且未完成二级认证的第一切片的二级认证通过后，UE 接收来自 AMF 的更新的允许接入的切片的选择信息，更新的允许接入的切片的选择信息包括第一切片的选择信息或网络分配的与第一切片的选择信息对应的切片的选择信息。

需要说明的是，这里的“第一切片”可以指请求接入的切片中需要进行二级认证且未完成二级认证的切片中所有的切片，也可以指请求接入的切片中需要进行二级认证且未完成二级认证的切片中部分切片（如一个切片）。即，AMF 可以是在需要进行二级认证且未完成二级认证的切片中的所有切片均完成二级认证后，向 UE 发送更新的允许接入的切片的选择信息，也可以是在需要进行二级认证且未完成二级认证的切片中的部分切片完成二级认证后，向 UE 发送更新的允许接入的切片的选择信息。

比如，针对上述示例，requested NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6}，假设通过上述步骤 201-步骤 203，得到如下结果：

1）、S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4 为需要二级认证的切片的选择信息；

2）、S-NSSAI5、S-NSSAI6 为不需要二级认证的切片的选择信息；

3）、S-NSSAI1 对应的切片 1 已经通过了二级认证、且授权给 UE。

4）、S-NSSAI2 对应的切片 2 运营商网络不支持，即被拒绝；

5）、S-NSSAI3 对应的切片 3、S-NSSAI4 对应的切片 4 还未完成二级认证和授权。

6）、网络为 UE 分配的已经通过一级认证且授权、且不需要二级认证的切片 7 的选择信息（S-NSSAI7）。

因此，在上述步骤 203 的注册接受消息中的：

allowed NSSAI={S-NSSAI1、S-NSSAI5、S-NSSAI6、S-NSSAI7}；

pending NSSAI={S-NSSAI3、S-NSSAI4}；

non-slice authentication NSSAI={ S-NSSAI 5、S-NSSAI6、S-NSSAI7 }；

rejected NSSAI={ S-NSSAI2}。

则在上述步骤 204 中，需要继续二级认证的切片（requested NSSAI for slice authentication）即为{ S-NSSAI3、S-NSSAI4}。需要说明的是，requested NSSAI for slice authentication 中的 S-NSSAI 还可以指示二级认证的顺序，比如该 requested NSSAI for slice authentication 指示了二级认证的顺序依次为：S-NSSAI3、S-NSSAI4。

需要说明的是，作为又一种实现方法，在步骤 202 中，AMF 也可以不进行是否需要进行切片二级认证的判断。在这种实现方式下，AMF 根据一级认证的结果，在步骤 203 中发送的注册接受消息中携带网络分配的 allowed NSSAI，但无法在 allowed NSSAI 中包括并授权不需要进行切片二级认证的 S-NSSAI。

下面结合示例，给出上述步骤 204 的不同实现方法。

实现方法一、通过注册请求消息和注册接受消息实现需要继续二级认证的切片的二级认证流程。

基于该实现方法，在上述步骤 203 之后步骤 204 之前，还包括以下步骤 204a：

步骤 204a、UE 向 AMF 发送第一消息，相应地，AMF 可以接收到该第一消息。

需要说明的是，步骤 204a 中，AMF 接收到该第一消息后，还可以包括一个判断的动作，即判断请求接入的切片是否需要进行二级认证，这个判断的动作，类似于步骤 202 中的描述。

更进一步，在判断请求接入的切片是否需要进行二级认证之前，还可以判断是否需要进行一级认证并重新建立安全上下文，比如确认以前的一级认证已经失效或以前一级认证建立的安全上下文已经失效或被删除等情况发生时，则确认可以重新进行一级认证并重新建立安全上下文。一级认证和安全上下文的建立，类似于步骤 202 中关于一级认证和安全上下文建立的描述。

该第一消息用于请求对请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证，即第一消息用于请求对上述 requested NSSAI for slice authentication 进行二级认证。

这里的第一消息具体为注册请求消息。该注册请求消息在本申请中也可以称为第二注册请求消息。该注册请求消息与上述步骤 201 中的注册请求消息的作用及携带的信息不同。

该注册请求消息包括请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息（即上述 requested NSSAI for slice authentication），和/或，切片认证指示（本申请中也将该切片认证指示称为第二切片认证指示、或第二级认证指示、或指示信息）。

该切片认证指示用于请求对请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

在一种实现方法中，该注册请求消息包括 requested NSSAI for slice authentication，但不包括该切片认证指示，即 requested NSSAI for slice authentication 可以隐式请求对 requested NSSAI for slice authentication 进行二级认证。

在又一种实现方法中，该注册请求消息包括切片认证指示，但不包括 requested NSSAI for slice authentication，则由 AMF 根据切片认证指示，确定 requested NSSAI for slice authentication。

在又一种实现方法中，该注册请求消息包括切片认证指示和 requested NSSAI for slice authentication。

基于该实现方法，则上述步骤 204 具体实现为：AMF 向 UE 发送第二消息，相应地，UE 可以接收该第二消息，第二消息包括更新的允许接入的切片的选择信息。

该第二消息具体为注册接受消息，该注册接受消息在本申请中也可以称为第二注册接受消息，其与上述步骤 203 的注册接受消息（即第一注册接受消息）携带的信息不同。

这里的更新的允许接入的切片的选择信息（new allowed NSSAI）包括上述 requested NSSAI for slice authentication 中二级认证通过且授权的 NSSAI。比如针对上述示例，requested NSSAI for slice authentication ={S-NSSAI3、S-NSSAI4}，若 S-NSSAI3、S-NSSAI4 均二级认证通过且授权，则 new allowed NSSAI={S-NSSAI3、S-NSSAI4}。

进一步的，new allowed NSSAI 还可以包括更新前的 allowed NSSAI 中的 S-NSSAI。比如，针对上述示例，allowed NSSAI={S-NSSAI1、S-NSSAI5、S-NSSAI6、S-NSSAI7}，则 new allowed NSSAI={S-NSSAI1、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6、S-NSSAI7}。

需要说明的是，更新的允许接入的切片的选择信息包括的切片的选择信息可以是 requested NSSAI for slice authentication 中的 S-NSSAI，也可以是由网络分配的与该 S-NSSAI 对应的 S-NSSAI。比如，requested NSSAI for slice authentication 中的 S-NSSAI3 需要二级认证，在二级认证通过后，正常情况下，网络会反馈 S-NSSAI3 授权，但有些场景，网络不支持 S-NSSAI3，而是支持与 S-NSSAI3 具有类似特性的 S-NSSAI3a，这时，网络发送的授权的 S-NSSAI 则可以是 S-NSSAI3a，即 S-NSSAI3a 是与 S-NSSAI3 对应的 S-NSSAI，同时

还可以通知 UE: S-NSSAI3 与 S-NSSAI3a 之间的对应关系。

需要说明的是，上述步骤 204a-步骤 204 可以执行一次或多次。比如，针对 requested NSSAI for slice authentication ={S-NSSAI3、S-NSSAI4}，则有以下不同的实现方式:

1)、执行一次步骤 204a，携带的 requested NSSAI for slice authentication ={S-NSSAI3 }。

执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI3 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3。若 S-NSSAI3 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI3 或步骤 204 不携带 new allowed NSSAI。

再执行一次步骤 204a，携带的 requested NSSAI for slice authentication ={S-NSSAI4 }。

再执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI4 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI4。若 S-NSSAI4 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI4 或步骤 204 不携带 new allowed NSSAI。

2)、执行一次步骤 204a，携带的 requested NSSAI for slice authentication ={S-NSSAI3、S-NSSAI4 }。

执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI3 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3。若 S-NSSAI3 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI3 或步骤 204 不携带 new allowed NSSAI。

再执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI4 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI4。若 S-NSSAI4 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI4 或步骤 204 不携带 new allowed NSSAI。

3)、执行一次步骤 204a，携带的 requested NSSAI for slice authentication ={S-NSSAI3、S-NSSAI4 }。

执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI3、S-NSSAI4 均二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3 和 S-NSSAI4。若 S-NSSAI3 二级认证未通过、或未授权，S-NSSAI4 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI4，但不包括 S-NSSAI3。若 S-NSSAI4 二级认证未通过、或未授权，S-NSSAI3 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3，但不包括 S-NSSAI4。若 S-NSSAI3 和 S-NSSAI4 二级认证均未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI3 和 S-NSSAI4，或步骤 204 不携带 new allowed NSSAI。

实现方法二、通过配置更新命令实现需要继续二级认证的切片的二级认证流程

基于该实现方法，则上述步骤 204 具体实现为: AMF 向 UE 发送第二消息，相应地，UE 可以接收该第二消息，第二消息包括更新的允许接入的切片的选择信息。

该第二消息具体为配置更新命令 (UE Configuration Update Command)，该注册接受消息在本申请中也可以称为第二注册接受消息，其与上述步骤 203 的注册接受消息 (即第一注册接受消息) 携带的信息不同。

该实现方法二，与上述实现方法一的主要区别是: 该实现方法利用了注册流程中的注册接受消息 (即步骤 203)，以及利用到了配置更新命令 (步骤 204)，并且是由网络主动发起对请求接入的切片中需要进行二级认证且未完成二级认证的切片 (这里称为 NSSAI need for slice authentication) 进行二级认证，如针对上述示例，网络在上述步骤 203 之后主动发起针对 S-NSSAI3 和 S-NSSAI4 的二级认证流程，并通过配置更新命令向 UE 发送二级认证的结果。

其中，包括的更新的允许接入的切片的选择信息,这里的更新的允许接入的切片的选择信息（new allowed NSSAI）包括 NSSAI need for slice authentication 中二级认证通过且授权的 NSSAI。比如针对上述示例，NSSAI need for slice authentication ={ S-NSSAI3、S-NSSAI4}，若 S-NSSAI3、S-NSSAI4 均二级认证通过且授权，则 new allowed NSSAI={S-NSSAI3、S-NSSAI4}。

进一步的，new allowed NSSAI 还可以包括更新前的 allowed NSSAI 中的 S-NSSAI。比如，针对上述示例，allowed NSSAI={S-NSSAI1、S-NSSAI5、S-NSSAI6、S-NSSAI7}，则 new allowed NSSAI={S-NSSAI1、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6、S-NSSAI7}。

需要说明的是，new allowed NSSAI 包括的切片的选择信息可以是 NSSAI need for slice authentication 中的 S-NSSAI,也可以是由网络分配的与该 S-NSSAI 对应的 S-NSSAI。比如，NSSAI need for slice authentication 中的 S-NSSAI3 需要二级认证，在二级认证通过后，正常情况下，网络会反馈 S-NSSAI3 授权，但有些场景，网络不支持 S-NSSAI3，而是支持与 S-NSSAI3 具有类似特性的 S-NSSAI3a，这时，网络发送的授权的 S-NSSAI 则可以是 S-NSSAI3a,即 S-NSSAI3a 是与 S-NSSAI3 对应的 S-NSSAI,同时还可以通知 UE: S-NSSAI3 与 S-NSSAI3a 之间的对应关系。

进一步的，上述配置更新命令中还可以包括以下信息中的一个或多个:

1）、请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息。

比如，针对上述 NSSAI need for slice authentication ={S-NSSAI3、S-NSSAI4}，若 S-NSSAI3 二级认证未通过、或未授权，即 S-NSSAI3 被拒绝，则可以在配置更新命令中携带 rejected NSSAI, rejected NSSAI={ S-NSSAI3}，可选的，还可以携带拒绝原因（如该 S-NSSAI 同 UE 不匹配，或签约情况变化，或没有通过二级认证等）。

2）、更新后的请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息（即 new NSSAI need for slice authentication）。

比如，针对上述 NSSAI need for slice authentication ={S-NSSAI3、S-NSSAI4}，若 S-NSSAI4 二级认证通过且授权，则可以在配置更新命令中携带 new NSSAI need for slice authentication, new NSSAI need for slice authentication={S-NSSAI3}。

3）、至少一个临时标识，其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

该临时标识的具体含义和作用可以参考前述描述，这里不再赘述。

需要说明的是，上述步骤 204 可以执行一次或多次。比如，针对 NSSAI need for slice authentication={S-NSSAI3、S-NSSAI4}，则有以下不同的实现方式:

1）、执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI3 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3。若 S-NSSAI3 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI3 或步骤 204 不携带 new allowed NSSAI。

再执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI4 二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI4。若 S-NSSAI4 二级认证未通过、或未授权，则 new allowed NSSAI 不包括 S-NSSAI4 或步骤 204 不携带 new allowed NSSAI。

2）、执行一次步骤 204，携带 new allowed NSSAI。若 S-NSSAI3、S-NSSAI4 均二级认证通过且授权，则 new allowed NSSAI 包括 S-NSSAI3 和 S-NSSAI4。若 S-NSSAI3 二级认

证未通过、或未授权，S-NSSAI4二级认证通过且授权，则new allowed NSSAI包括S-NSSAI4，但不包括S-NSSAI3。若S-NSSAI4二级认证未通过、或未授权，S-NSSAI3二级认证通过且授权，则new allowed NSSAI包括S-NSSAI3，但不包括S-NSSAI4。若S-NSSAI3和S-NSSAI4二级认证均未通过、或未授权，则new allowed NSSAI不包括S-NSSAI3和S-NSSAI4，或步骤204不携带new allowed NSSAI。

实现方法三、通过新定义的消息实现需要继续二级认证的切片的二级认证流程

在一种实现方法中，可以将上述实现方法一中的步骤204a的注册请求消息（即第二注册请求消息）更换为一个新定义的消息，这里称为切片注册请求消息，将步骤204的注册接受消息（即第二注册接受消息）更换为一个定义的消息，这里称为切片注册接受消息，从而得到该实现方法三。

在又一种实现方法中，可以将上述实现方法二中的步骤204的配置更新命令更换为一个定义的消息，这里称为切片注册更新命令，从而得到该实现方法三。

基于图2实施例的方案，网络发送注册接受消息（即上述步骤203的注册接受消息）比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对UE的一级认证和建立安全上下文之后就发送注册接受消息（通过提前发送注册接受消息，注册流程可以尽早结束，不过这仅仅代表暂时（Interim）结束，而不是完全结束，因为还有二级认证没完成），而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，UE也大大增加了接入的灵活性，并且使得注册时的定时器的设置变得更为简便。此时，UE可以根据网络反馈的二级认证信息，决定何时进行二级认证对UE更方便。比如，UE可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

基于图1所示的架构，如图3所示，为本申请提供的又一种UE的注册方法流程示意图，本实施例与上述图2实施例的主要区别在于：本实施例以UE为主，根据其可获得的信息，通过优化注册请求消息中的参数来实现去嵌套的方法，而对网络协议不需要或者需要很小的改动。该方法包括以下步骤：

步骤301，UE向AMF发送注册请求（registration request）消息，相应地，AMF可以接收到该注册请求消息。

这里的注册请求消息在本申请中也可以称为第一注册请求消息。该注册请求消息用于请求注册至网络。

注册请求消息包括请求接入的切片的选择信息（requested NSSAI），请求接入的切片为不需要进行二级认证的切片。

在步骤301之前，UE可以事先获知哪些S-NSSAI需要二级认证，哪些S-NSSAI不需要二级认证，例如UE可以利用历史接入的情况来进行分析，并确定哪些S-NSSAI需要二级认证，哪些S-NSSAI不需要二级认证。又例如，UE可以预先配置可接入的S-NSSAI，并预先配置哪些S-NSSAI不需要二级认证，哪些需要二级认证。也可预先配置存储相关二级认证的特征，如采用哪种EAP方法，预估的二级认证所需时间等。

即UE可以将UE中的S-NSSAI分为两组，一组为需要二级认证的S-NSSAI，另一组为不需要二级认证的S-NSSAI。

或者，UE还可以将上述需要二级认证的S-NSSAI进一步的再分为N个组（N大于1），

比如，根据二级认证可能的时间长短，或根据需要接入切片的先后顺序进行分组。分组后，在 UE 注册至网络后的后续流程中，可以针对该 N 个组中的每个组发起一次注册申请。更进一步，也可以针对每个需要二级认证的 S-NSSAI 发起一次注册申请（即每个 S-NSSAI 是一个组），同样的，发起注册申请的先后顺序，可以事先进行排序。

在上述步骤 301 的 requested NSSAI，只携带不需要进行二级认证的切片，不携带需要进行二级认证的切片。

作为一个示例，UE 中的 S-NSSAI 包括 S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6，其中，UE 确定 S-NSSAI1 对应的切片 1、S-NSSAI2 对应的切片 2、S-NSSAI3 对应的切片 3、S-NSSAI4 对应的切片 4 需要进行二级认证，S-NSSAI5 对应的切片 5 和 S-NSSAI6 对应的切片 6 不需要进行二级认证。则该步骤 301 的 requested NSSAI={ S-NSSAI5、S-NSSAI6}。

进一步的，还可以将 S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4 进行分组，比如分为四个组，每个组包括一个 S-NSSAI，或者分为两个组等，并且不同的分组对应的二级认证的优先级不同。

步骤 302，在 UE 完成一级认证和建立安全上下文后，AMF 向 UE 发送注册接受消息，相应地，UE 可以接收到该注册接受消息。

该注册接受消息包括允许接入的切片的选择信息（allowed NSSAI），allowed NSSAI 包括以下信息中的一个或多个：

1）、请求接入的切片中的允许接入的切片的选择信息。

请求接入的切片中的允许接入的切片的选择信息即为 requested NSSAI 中不需要进行二级认证的 S-NSSAI。比如，上述 requested NSSAI 中的 S-NSSAI5S-NSSAI6，在一级认证通过后直接授权，则请求接入的切片中的允许接入的切片的选择信息即为{S-NSSAI5，S-NSSAI6}。

2）、网络分配的不需要进行二级认证的切片的选择信息。

这里的网络分配的不需要进行二级认证的切片的选择信息具体指的是：网络分配的已经完成一级认证、且不需要进行二级认证的切片的选择信息。

比如，网络（如 AMF）对 S-NSSAI7 对应的切片 7 完成了一级认证且授权通过，即 AMF 确定可以将切片 7 授权给 UE 接入，且该切片 7 是不需要进行二级认证的切片，则 allowed NSSAI 还可以包括 S-NSSAI7。这里的 S-NSSAI7 即为网络分配的已经完成一级认证、且不需要进行二级认证的切片的选择信息。

综上，在上述示例中，allowed NSSAI 可以包括以下信息中的一个或多个：请求接入的切片中的允许接入的切片的选择信息（即 S-NSSAI5 和 S-NSSAI6）、网络分配的不需要进行二级认证的切片的选择信息（即 S-NSSAI7）。

需要说明的是，在一种可能的实现方法中，如果 allowed NSSAI 中已经包括了请求接入的切片中的允许接入的切片的选择信息，那么网络也可以不用分配额外的切片的选择信息。相反，如果 allowed NSSAI 不包括任何请求接入的切片中的允许接入的切片的选择信息，网络就一定要分配给通过一级认证的 UE 至少一个 S-NSSAI。在上述例子中，allowed NSSAI 包括了 S-NSSAI5 和 S-NSSAI6，这时，网络可以不再分配 S-NSSAI7 给 UE。如果，S-NSSAI5 和 S-NSSAI6 也需要进行切片认证，网络才分配 S-NSSAI7 给通过一级认证的 UE，如此，可以保证至少有一个 S-NSSAI 在 allowed NSSAI 中。

步骤 303，UE 向 AMF 发送第一消息，相应地，AMF 可以接收到该第一消息。

第一消息包括需要进行二级认证的切片的选择信息（requested NSSAI for slice authentication），第一消息用于请求对需要进行二级认证的切片进行切片认证。例如，针对上述示例，requested NSSAI for slice authentication 例如包括 S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4。或者也可以多次发送第一消息，每次发起的第一消息中包括需要进行二级认证的切片的一个分组。

作为一种实现方法，需要进行二级认证的切片的选择信息可以携带于一个切片选择信息列表中，切片选择信息列表中的切片的选择信息的顺序指示了切片选择信息列表中的切片进行二级认证的优先级。比如，第一消息包括切片选择信息列表 A，该切片选择信息列表 A={ S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4}。一方面，该切片选择信息列表 A 指示了请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息包括 S-NSSAI1、S-NSSAI2、S-NSSAI3 和 S-NSSAI4；另一方面，该切片选择信息列表 A 还指示了进行二级认证的顺序依次为：S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4。

步骤 304，在需要进行二级认证的切片中的第一切片二级认证通过后，AMF 向 UE 发送第二消息，相应地，UE 接收来自 AMF 的第二消息。

该第二消息包括更新的允许接入的切片的选择信息（new allowed NSSAI），new allowed NSSAI 包括第一切片的选择信息或网络分配的与第一切片的选择信息对应的切片的选择信息。

需要说明的是，这里的“第一切片”可以指 requested NSSAI for slice authentication 中所有的切片，也可以指 requested NSSAI for slice authentication 中部分切片（如一个切片）。即，AMF 可以是在 requested NSSAI for slice authentication 中的所有切片均完成二级认证后，向 UE 发送 new allowed NSSAI，也可以是在 requested NSSAI for slice authentication 中的部分切片完成二级认证后，向 UE 发送 new allowed NSSAI。

下面结合具体示例，对上述过程进行说明。比如，UE 将 UE 中的 S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4、S-NSSAI5、S-NSSAI6 分为了两个分组，其中分组 1={S-NSSAI5、S-NSSAI6}，分组 2={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4}，其中分组 1 包括不需要二级认证的切片的选择信息，分组 2 包括需要二级认证的切片的选择信息。

上述步骤 303 的第一消息中的 requested NSSAI for slice authentication={S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4}，网络对 requested NSSAI for slice authentication 中的切片的选择信息对应的切片进行二级认证，比如对 S-NSSAI1、S-NSSAI2、S-NSSAI3 认证通过且授权，对 S-NSSAI4 拒绝，则上述第二消息中的 new allowed NSSAI={S-NSSAI1、S-NSSAI2、S-NSSAI3}，或者，new allowed NSSAI 中还可以包括上述步骤 302 的 allowed NSSAI 中的 S-NSSAI，比如 allowed NSSAI={S-NSSAI5、S-NSSAI7}，则 new allowed NSSAI={ S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI5、S-NSSAI7}。第二消息还可以携带 rejected NSSAI，该 rejected NSSAI={ S-NSSAI 4}，进一步地还可以携带拒绝接入的原因，具体可参考前述描述的各拒绝接入的原因。

需要说明的是，requested NSSAI for slice authentication 中的 S-NSSAI 还可以指示二级认证的顺序，比如该 requested NSSAI for slice authentication 指示了二级认证的顺序依次为：S-NSSAI1、S-NSSAI2、S-NSSAI3、S-NSSAI4。

需要说明的是，上述步骤 303-步骤 304 可以执行一次或多次。其具体实现过程类似于

上述图 2 实施例中的相关描述的方法，可参考前述描述。

需要说明的是，在一种实现方法中，上述第一消息是注册请求消息，第二消息是注册接受消息。在又一种实现方法中，上述第一消息是切片注册请求消息，第二消息是切片注册接受消息。

基于图 3 实施例的方案，网络发送注册接受消息（即上述步骤 302 的注册接受消息）比现有技术的注册流程中发送注册接受消息的时间更早，即本申请只要完成了对 UE 的一级认证和建立安全上下文之后就发送注册接受消息（通过提前发送注册接受消息，注册流程可以尽早结束，不过这仅仅代表暂时（Interim）结束，而不是完全结束，因为还有二级认证没完成），而现有技术是等到所有的切片完成二级认证之后才发送注册接受消息，这样不仅可以解决嵌套式认证带来的问题，UE 也大大增加了接入的灵活性，并且使得注册时的定时器的设置变得更为简便。此时，UE 可以根据网络反馈的二级认证信息，决定何时进行二级认证对 UE 更方便。比如，UE 可以根据已经成功认证的切片，接入该切片，建立会话，发送接收数据服务。而在晚些时候空闲时，再请求接入其他切片。

本申请通过上述图 2 和图 3 两个实施例，给出了 UE 的两种注册方法，实现了“去嵌套化”的二级认证，即提供灵活的认证（注册）流程，使得一级认证和二级认证可以解耦，单一的或几个二级认证流程的长短，不会造成对一级认证以及其他二级认证造成显著影响，从而解决上述嵌套式认证流程所引入的问题。

注册流程中，与认证、授权强相关的流程可以先从功能上进行划分为：1）网络和 UE 之间的一级认证，2）网络对 UE 接入切片的 NSSAI 授权，3）UE 和 DN 之间的二级认证，4）NAS 或 AS 安全建立（即建立 UE 的安全上下文）。

其中，1）中的一级认证和 4）中的 NAS 和/或 AS 安全建立，都与 3）的二级认证不直接相关，它与 2）中切片的 NSSAI 授权行为也可以是相对独立的。一级认证是基于 UE 在运营商网络 UDM 中存储的签约数据（而不是二级认证的 DN AAA 是认证、授权和计费（Authentication、Authorization、Accounting，AAA）服务器），一级认证之后，NAS 安全中的密钥推衍和生成，也不受 NSSAI 的制约（NSSAI 不是密钥生成时所需参数）。也就是说，一级认证以及 NAS 和/或 AS 安全建立过程是可以从其他流程中分离出来的。而 2）和 3）强相关，而且通常有一一对应的关系。也就是说，一个切片的认证成功，会直接对应到一个 S-NSSAI 的授权，这样 2）和 3）是需要绑定的，但该绑定又是可以以一次（或一组）二级认证或一个（或一组）S-NSSAI 授权的为单位（颗粒度）进行，而不需要把所有的二级认证和 S-NSSAI 混在一起。

具体实现方法上，主要原则是尽可能的先完成注册流程中一级认证、NAS 安全建立等必选流程，然后再按照灵活可配置的安全策略进行二级认证。至于切片授权的 S-NSSAI 信息，可以每次二级认证成功及时发送给用户，或者一次性发送多个 S-NSSAI 的信息。与前述嵌套式二级认证相对应，总体流程可以简要概括为（省略 NAS 安全建立流程）:

步骤 1，UE 向网络（AMF）发送接入网络的注册申请。

步骤 2，网络（AMF）根据 UE 的签约信息（如 SUPI 等），同 UE 进行一级认证。

步骤 3，认证成功后，网络（AMF）确定该 UE 是否还需要进一步进行二级认证。

步骤 4，网络（AMF）将授权信息 allowed NSSAI（但还未进行二级认证）发送给 UE，完成“interim”注册流程。如果需要二级认证，网络（AMF）发起一个或者一组二级认证流程，通知 UE 和 DN 进行二级认证，并转发 UE 和 DN 之间认证所需的各种交互信息。

其中，allowed NSSAI根据网络存储信息(如UE存储在UDM或AMF的签约信息等)或授权信息（如通过与NSSF交互）来确定。allowed NSSAI可以包括网络分配的默认的S-NSSAI，和/或与待访问的不需要二级认证的切片相对应的S-NSSAI。选定哪个切片或哪一组二级认证，可以灵活配置、确定（根据UE注册请求信息、签约信息、DN信息等等）

步骤5，每完成一次二级认证，DN向网络（AMF）发送二级认证成功消息。

步骤6，针对每一次二级认证或者每一组二级认证，网络（AMF）根据二级认证是否成功，为UE选择（或通过NSSF等NF）相对应的切片，确定allowed NSSAI。

步骤7，网络（AMF）将更新的授权信息allowed NSSAI发送给UE，完成注册流程(步骤5-步骤7可以根据需要重复进行)。

在本申请上述认证（注册）流程，在具体实施例中，还需要进一步考虑以下几个方面：

1）、网络给UE发送allowed NSSAI信息的方法，比如，方法1：采用现有注册流程中的消息和流程，但需要定义新的IE（Information Element）及新的动作（behavior）。再比如，方法2：定义新的专用消息及相应的流程。

2）、如果是采用现有注册流程，备选消息有“registration accept”。

3)、发送“registration accept”（包括了授权信息“allowed NSSAI”）的时间点：可选的方案一，网络可以在一级认证之后(还没有与DN进行二级认证之前，或无需二级认证)，根据一级认证结果、存储在网络（UDM、AMF等）的签约信息、AMF与其他网络功能（如NSSF）交互的结果等信息，确定allowed NSSAI，并发送给UE。可选的方案二，网络可以在一级认证之后，并且完成了一部分的二级认证之后，发送“registration accept”。需要说明的是，方案二是一种局部的嵌套方案。

4)、“registration accept”消息中，除了可以包括“allowed NSSAI”之外，也需要包括指示信息，通知UE，哪些NSSAI需要进行二级认证。也可以指示多个二级认证的优选认证方式和优先顺序，即二级认证是一个认证完成后通知UE还是一组二级认证完成后通知UE。二级认证的认证顺序，可以根据所需时间长短排序。除了排序，也可以标示，每个二级认证所需时间的估计值。

5）、“registration accept”消息中，还可以进一步指示哪些S-NSSAI被拒绝，比如“rejected NSSAI”，哪些S-NSSAI不需要进行二级认证。指示的好处是，UE可以存储相应的状态，在下次请求接入的时候，可以避免重复申请接入被拒绝的S-NSSAI，或者进行其他操作，比如UE可以根据被拒绝的原因，通知UE上的应用程序或用户进行进一步处理。如，长期被拒绝，用户可以查询签约数据是否存在问题等。

6）、上述指示信息，可以是多个单独的IE，也可以是一个IE多种状态，这里不作限定。

7）、除了利用现有“registration accept”消息之外，网络还可以利用“UE Configuration Update Command”消息，通知UE需要进行二级认证。类似上述描述，在“UE Configuration Update Command”消息中，可以包括各种指示信息，触发UE来进行二级认证的后续步骤。

8）、除了利用现有消息之外，也可以定义新的消息，完成网络和UE之间的信息交互。主要是完成，网络通知UE已经被授权的Allowed NSSAI信息，待二级认证的S-NSSAI，被拒绝的NSSAI信息，不需要二级认证的NSSAI信息。这些信息可以多此发送，首先是在二级认证之前，之后是在每次二级认证之后，或是每组二级认证之后。

9）、本申请一方面可以通过网络侧来解决嵌套式认证问题，另一方面也可以通过增强

UE 的智能性和通过网络的协助来解决、缓解该问题。比如，如果 UE 可以获得、分析、预测到哪些 S-NSSAI 不需要二级认证，每种二级认证所需的时间，UE 可以在注册请求中，直接通知网络 UE 的选择，即，先进行单独一级认证和无需二级认证的注册申请，然后按顺序进行每个二级认证或每组二级认证。

以上是对上述实施例 2 和实施例 3 的总结说明，其中的每项内容的具体实现都已经在实施例中做了具体说明，可以参考前述描述。

下面结合具体示例，对图 2 和图 3 所示的实施例进行介绍说明。需要说明的是，以下图 4-图 6 中的 AAA-F 指的是 AAA 代理功能（AAA- proxy function）网元，AAA-S 指的是 AAA 服务器（AAA- proxy server），这里做统一说明。

如图 4 所示，为本申请提供的又一种 UE 的注册方法流程示意图。该实施例是对上述图 2 所示的实施例并结合其中的步骤 204 对应的实现方法一的一个具体示例。该方法包括以下步骤：

步骤 401，UE 向网络（AMF）发送注册请求消息，该注册请求消息中包括 requested NSSAI。

步骤 402，AMF 收到注册请求消息后，发起一级认证流程进行 UE 和网络的双向认证（包括 NAS 安全建立过程）。

步骤 403，一级认证成功后，AMF 判断请求接入的切片是否需要二级认证。

即判断 requested NSSAI 中的 S-NSSAI 对应的切片是否需要二级认证。

步骤 404，AMF 向 UE 发送注册接受消息，该注册接受消息包括以下一项或多项：“allowed NSSAI”、“Pending NSSAI”、“切片认证指示”、“non-slice authentication NSSAI”、“rejected NSSAI”、“5G-GUTI”。

步骤 405，UE 向 AMF 发送注册请求消息。该消息可以包括需要二级认证的 NSSAI 请求（“requested NSSAI for slice authentication”）、“切片认证指示”、“5G-GUTI”等。

步骤 406，网络与 UE 完成切片的二级认证。

即网络与 UE 完成 requested NSSAI for slice authentication 中的 S-NSSAI 对应的切片的二级认证的流程。

步骤 407，AMF 向 UE 发送注册接受消息，该消息包含了经过二级认证以后的更新了的“allowed NSSAI”，其中可以包括当前认证所授权的 S-NSSAI 和以前已经授权的 S-NSSAI，也可以只包括当前认证所授权的 S-NSSAI。

该实施例的上述步骤的具体实现细节可以参考图 2 所示的实施例的相关内容的描述，该实施例的有益效果的描述也可以参考图 2 所示的实施例的描述，这里不再赘述。

如图 5 所示，为本申请提供的又一种 UE 的注册方法流程示意图。该实施例是对上述图 2 所示的实施例并结合其中的步骤 204 对应的实现方法二的一个具体示例。该方法包括以下步骤：

步骤 501-步骤 504，与实施例 4 的步骤 401-步骤 404 相同，可参考前述描述。

步骤 505，网络发起并完成与 UE 的切片的二级认证。

即网络与 UE 完成 NSSAI need for slice authentication 中的 S-NSSAI 对应的切片的二级认证的流程。

步骤 506，AMF 向 UE 发送配置更新命令，该配置更新命令包含了经过二级认证以后的更新了的 “allowed NSSAI”，其中可以包括当前认证所授权的 S-NSSAI 和以前已经授权的 S-NSSAI，也可以只包括当前认证所授权的 S-NSSAI。

步骤 507，UE 向网络（AMF）发送配置更新完成消息。

该步骤 507 为可选步骤。

需要说明的是，上述步骤 505 和步骤 506 也可以执行多次，比如每次完成 NSSAI need for slice authentication 中的 S-NSSAI 对应的切片中的一个切片的二级认证的流程，并将授权的 S-NSSAI 通过步骤 506 发送给 UE。再比如，每次完成 NSSAI need for slice authentication 中的 S-NSSAI 对应的切片中的多个切片的二级认证的流程，并将授权的 S-NSSAI 通过步骤 506 发送给 UE。

该实施例的上述步骤的具体实现细节可以参考图 2 所示的实施例的相关内容的描述，该实施例的有益效果的描述也可以参考图 2 所示的实施例的描述，这里不再赘述。

如图 6 所示，为本申请提供的又一种 UE 的注册方法流程示意图。该实施例是对上述图 2 所示的实施例并结合其中的步骤 204 对应的实现方法三的一个具体示例。该方法包括以下步骤：

步骤 601-步骤 604，与实施例 4 的步骤 401-步骤 404 相同，可参考前述描述。

步骤 605，UE 向 AMF 发送切片注册请求消息。该消息可以包括需要二级认证的 NSSAI 请求（“requested NSSAI for slice authentication”）、“切片认证指示”、“5G-GUTI” 等。

步骤 606，网络与 UE 完成切片的二级认证。

即网络与 UE 完成 requested NSSAI for slice authentication 中的 S-NSSAI 对应的切片的二级认证的流程。

步骤 607，AMF 向 UE 发送切片注册接受消息，该消息包含了经过二级认证以后的更新了的 “allowed NSSAI”，其中可以包括当前认证所授权的 S-NSSAI 和以前已经授权的 S-NSSAI，也可以只包括当前认证所授权的 S-NSSAI。

该实施例与图 4 所示的实施例的主要区别是：步骤 605 采用新定义的切片注册请求消息，步骤 607 采用新定义的切片注册接受消息，其他都类似。

该实施例的上述步骤的具体实现细节可以参考图 2 所示的实施例的相关内容的描述，该实施例的有益效果的描述也可以参考图 2 所示的实施例的描述，这里不再赘述。

如图 7 所示，为本申请提供的又一种 UE 的注册方法流程示意图。该实施例是对上述图 3 所示的实施例的一个具体示例。该方法包括以下步骤：

步骤 701，UE 向网络（AMF）发送注册请求消息，该注册请求消息中包括 requested NSSAI。

其中，requested NSSAI 包括请求接入的不需要二级认证的切片的选择信息。

步骤 702，AMF 收到注册请求消息后，发起一级认证流程进行 UE 和网络的双向认证（包括 NAS 安全建立过程）。

步骤 703，一级认证成功后，AMF 判断请求接入的切片是否需要二级认证。

这里，AMF 判断的结果是：requested NSSAI 中的所有 S-NSSAI 对应的切片均不需要二级认证。

该步骤为可选步骤。

步骤 704，AMF 向 UE 发送注册接受消息，该注册接受消息包括以下一项或多项："allowed NSSAI"、"rejected NSSAI"、"5G-GUTI"。

步骤 705，UE 向 AMF 发送注册请求消息。该消息可以包括需要二级认证的 NSSAI 请求（"requested NSSAI for slice authentication"）、"切片认证指示"、"5G-GUTI" 等。

步骤 706，网络与 UE 完成切片的二级认证。

即网络与 UE 完成 requested NSSAI for slice authentication 中的 S-NSSAI 对应的切片的二级认证的流程。

步骤 707，AMF 向 UE 发送注册接受消息，该消息包含了经过二级认证以后的更新了的"allowed NSSAI"，其中可以包括当前认证所授权的 S-NSSAI 和以前已经授权的 S-NSSAI，也可以只包括当前认证所授权的 S-NSSAI。

需要说明的是，上述步骤 705 的注册请求消息也可以使用切片注册请求消息替代，上述步骤 707 的注册接受消息也可以使用切片注册接受消息替代。

该实施例的上述步骤的具体实现细节可以参考图 3 所示的实施例的相关内容的描述，该实施例的有益效果的描述也可以参考图 3 所示的实施例的描述，这里不再赘述。

上述主要从各个网元之间交互的角度对本申请提供的方案进行了介绍。可以理解的是，上述实现各网元为了实现上述功能，其包含了执行各个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，本发明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发明的范围。

如图 8 所示 ，为本申请所涉及的通信装置的一种可能的示例性框图，该通信装置 800 可以以软件或硬件的形式存在。通信装置 800 可以包括：处理单元 802 和通信单元 803。作为一种实现方式，该通信单元 803 可以包括接收单元和发送单元。处理单元 802 用于对通信装置 800 的动作进行控制管理。通信单元 803 用于支持通信装置 800 与其他网络实体的通信。通信装置 800 还可以包括存储单元 801，用于存储通信装置 800 的程序代码和数据。

其中，处理单元 802 可以是处理器或控制器，例如可以是通用中央处理器（central processing unit，CPU），通用处理器，数字信号处理（digital signal processing，DSP），专用集成电路（application specific integrated circuits，ASIC），现场可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。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。所述处理器也可以是实现计算功能的组合，例如包括一个或多个微处理器组合，DSP 和微处理器的组合等等。存储单元 801 可以是存储器。通信单元 803 是一种该装置的接口电路，用于从其它装置接收信号。例如，当该装置以芯片的方式实现时，该通信单元 803 是该芯片用于从其它芯片或装置接收信号的接口电路，或者， 是该芯片用于向其它芯片或装置发送信号的接口电路。

该通信装置 800 可以为上述任一实施例中的终端设备，还可以为用于终端设备的芯片。

例如，当通信装置 800 为终端设备时，该处理单元 802 例如可以是处理器，该通信单元 803 例如可以是收发器。可选的，该收发器可以包括射频电路，该存储单元例如可以是存储器。例如，当通信装置 800 为用于终端设备的芯片时，该处理单元 802 例如可以是处理器，该通信单元 803 例如可以是输入/输出接口、管脚或电路等。该处理单元 802 可执行存储单元存储的计算机执行指令，可选地，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是该终端设备内的位于该芯片外部的存储单元，如只读存储器（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)等。

在第一个实施例中，该通信装置 800 为终端设备，通信单元 803 包括发送单元和接收单元。发送单元，用于向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；接收单元，用于在所述终端设备完成一级认证和建立安全上下文后，接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息；接收单元，还用于在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

在一种可能的实现方法中，所述第一注册接受消息还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识；其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

在一种可能的实现方法中，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中发送单元，用于向所述移动性管理网元发送第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证；接收单元，具体用于接收来自所述移动性管理网元的第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

在一种可能的实现方法中，接收单元，用于接收来自所述移动性管理网元的配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述配置更新命令还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识；其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

在第二个实施例中，该通信装置 800 为终端设备，通信单元 803 包括发送单元和接收单元。发送单元，用于向所述移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；接收单元，用于在所述终端设备完成一级认证和建立安全上下文后，接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；所述发送单元，还用于向所述移动性管理网元发送第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；所述接收单元还用于在所述需要进行二级认证的切片中的第一切片二级认证通过后，接收来自所述移动性管理网元的第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

在一种可能的实现方法中，所述需要进行二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息还包括所述分组信息指示了所述需要进行二级认证的切片的分组信息，所述分组信息指示了各分组进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

可以理解的是，该通信装置用于上述终端设备的注册方法时的具体实现过程以及相应的有益效果，可以参考前述方法实施例中的相关描述，这里不再赘述。

如图 9 所示 ，为本申请所涉及的通信装置的一种可能的示例性框图，该通信装置 900 可以以软件或硬件的形式存在。通信装置 900 可以包括：处理单元 902 和通信单元 903。作为一种实现方式，该通信单元 903 可以包括接收单元和发送单元。处理单元 902 用于对通信装置 900 的动作进行控制管理。通信单元 903 用于支持通信装置 900 与其他网络实体的通信。通信装置 900 还可以包括存储单元 901，用于存储通信装置 900 的程序代码和数据。

其中，处理单元 902 可以是处理器或控制器，例如可以是 CPU，通用处理器，DSP，ASIC，FPGA 或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。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。所述

处理器也可以是实现计算功能的组合，例如包括一个或多个微处理器组合，DSP 和微处理器的组合等等。存储单元 901 可以是存储器。通信单元 903 是一种该装置的接口电路，用于从其它装置接收信号。例如，当该装置以芯片的方式实现时，该通信单元 903 是该芯片用于从其它芯片或装置接收信号的接口电路，或者， 是该芯片用于向其它芯片或装置发送信号的接口电路。

该通信装置 900 可以为上述任一实施例中的移动性管理网元，还可以为用于移动性管理网元的芯片。例如，当通信装置 900 为移动性管理网元时，该处理单元 902 例如可以是处理器，该通信单元 903 例如可以是收发器。可选的，该收发器可以包括射频电路，该存储单元例如可以是存储器。例如，当通信装置 900 为用于移动性管理网元的芯片时，该处理单元 902 例如可以是处理器，该通信单元 903 例如可以是输入/输出接口、管脚或电路等。该处理单元 902 可执行存储单元存储的计算机执行指令，可选地，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是该移动性管理网元内的位于该芯片外部的存储单元，如 ROM 或可存储静态信息和指令的其他类型的静态存储设备，RAM 等。

在第一个实施例中，该通信装置 900 为移动性管理网元，通信单元 803 包括发送单元和接收单元。接收单元，用于接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；处理单元，用于在所述终端设备完成一级认证和建立安全上下文后，所述移动性管理网元判断所述请求接入的切片是否需要进行二级认证；发送单元，用于向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息；发送单元，还用于在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，向所述终端设备发送更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

在一种可能的实现方法中，所述第一注册接受消息还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片的选择信息、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识；其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的一个或多个切片的选择信息。

在一种可能的实现方法中，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，接收单元，还用于接收来自所述终端设备的第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证；发送单元，用于向所述终端设备发送第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述第一消息包括所述请求接入的切片中需要进行二级认

证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

在一种可能的实现方法中，发送单元，用于向所述终端设备发送配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

在一种可能的实现方法中，所述配置更新命令还包括以下信息中的至少一个：所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识；其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

在第二个实施例中，该通信装置900为移动性管理网元，通信单元803包括发送单元和接收单元。接收单元，用于接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；发送单元，用于在所述终端设备完成一级认证和建立安全上下文后，向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；接收单元，还用于接收来自所述终端设备的第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；发送单元，还用于在所述需要进行二级认证的切片中的第一切片二级认证通过后，向所述终端设备发送第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

在一种可能的实现方法中，所述需要进行二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息还包括所述分组信息指示了所述需要进行二级认证的切片的分组信息，所述分组信息指示了各分组进行二级认证的优先级。

在一种可能的实现方法中，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息；或者，所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

可以理解的是，该通信装置用于上述终端设备的注册方法时的具体实现过程以及相应的有益效果，可以参考前述方法实施例中的相关描述，这里不再赘述。

如图 10 所示，为本申请提供的一种通信装置示意图，该通信装置可以是上述移动性管理网元、或终端设备。该通信装置 1000 包括：处理器 1002、通信接口 1003、存储器 1001。可选的，通信装置 1000 还可以包括通信线路 1004。其中，通信接口 1003、处理器 1002 以及存储器 1001 可以通过通信线路 1004 相互连接；通信线路 1004 可以是外设部件互连

标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。所述通信线路 1004 可以分为地址总线、数据总线、控制总线等。为便于表示，图 10 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。

处理器 1002 可以是一个 CPU，微处理器，ASIC，或一个或多个用于控制本申请方案程序执行的集成电路。

通信接口 1003，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，RAN，无线局域网(wireless local area networks，WLAN)，有线接入网等。

存储器 1001 可以是 ROM 或可存储静态信息和指令的其他类型的静态存储设备，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。存储器可以是独立存在，通过通信线路 1004 与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 1001 用于存储执行本申请方案的计算机执行指令，并由处理器 1002 来控制执行。处理器 1002 用于执行存储器 1001 中存储的计算机执行指令，从而实现本申请上述实施例提供的终端设备的注册方法。

可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

本领域普通技术人员可以理解：本申请中涉及的第一、第二等各种数字编号仅为描述方便进行的区分，并不用来限制本申请实施例的范围，也表示先后顺序。“和/或”，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。字符“/”一般表示前后关联对象是一种“或”的关系。“至少一个”是指一个或者多个。至少两个是指两个或者多个。“至少一个”、“任意一个”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、种），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。“多个”是指两个或两个以上，其它量词与之类似。此外，对于单数形式 “a”，“an”和“the” 出现的元素（element），除非上下文另有明确规定，否则其不意味着“一个或仅一个”，而是意味着“一个或多于一个”。例如，“a device”意味着对一个或多个这样的 device。

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。在计算机上加载和执行所述计算机程序指令时，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括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。

本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器，数字信号处理器，专用集成电路（ASIC），现场可编程门阵列（FPGA）或其它可编程逻辑装置，离散门或晶体管逻辑，离散硬件部件，或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器，可选地，该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现，例如数字信号处理器和微处理器，多个微处理器，一个或多个微处理器联合一个数字信号处理器核，或任何其它类似的配置来实现。

本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示例性地，存储媒介可以与处理器连接，以使得处理器可以从存储媒介中读取信息，并可以向存储媒介存写信息。可选地，存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于 ASIC 中。

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

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范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包括这些改动和变型在内。

权 利 要 求

1、一种终端设备的注册方法，其特征在于，包括:

终端设备向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息;

在所述终端设备完成一级认证和建立安全上下文后，所述终端设备接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个: 所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息;

在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，所述终端设备接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

2、如权利要求 1 所述的方法，其特征在于，所述第一注册接受消息还包括以下信息中的至少一个:

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识;

其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

3、如权利要求 2 所述的方法，其特征在于，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

4、如权利要求 1-3 任一所述的方法，其特征在于，还包括:

所述终端设备向所述移动性管理网元发送第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证;

所述终端设备接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，包括:

所述终端设备接收来自所述移动性管理网元的第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

5、如权利要求 4 所述的方法，其特征在于，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示;

所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

6、如权利要求 4 或 5 所述的方法，其特征在于，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息; 或者，

所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

7、如权利要求 1-3 任一所述的方法，其特征在于，所述终端设备接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，包括:

所述终端设备接收来自所述移动性管理网元的配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

8、如权利要求 7 所述的方法，其特征在于，所述配置更新命令还包括以下信息中的至少一个:

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识;

其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

9、一种终端设备的注册方法，其特征在于，包括:

移动性管理网元接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息;

在所述终端设备完成一级认证和建立安全上下文后，所述移动性管理网元判断所述请求接入的切片是否需要进行二级认证;

所述移动性管理网元向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个: 所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息;

在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，所述移动性管理网元向所述终端设备发送更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

10、如权利要求 9 所述的方法，其特征在于，所述第一注册接受消息还包括以下信息中的至少一个:

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片的选择信息、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识;

其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的一个或多个切片的选择信息。

11、如权利要求 10 所述的方法，其特征在于，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

12、如权利要求 9-11 任一所述的方法，其特征在于，还包括:

所述移动性管理网元接收来自所述终端设备的第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证;

所述移动性管理网元向所述终端设备发送更新的允许接入的切片的选择信息，包括:

所述移动性管理网元向所述终端设备发送第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

13、如权利要求 12 所述的方法，其特征在于，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；

所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

14、一种终端设备的注册方法，其特征在于，包括：

终端设备向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；

在所述终端设备完成一级认证和建立安全上下文后，所述终端设备接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；

所述终端设备向所述移动性管理网元发送第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；

在所述需要进行二级认证的切片中的第一切片二级认证通过后，所述终端设备接收来自所述移动性管理网元的第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

15、一种终端设备的注册方法，其特征在于，包括：

移动性管理网元接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；

在所述终端设备完成一级认证和建立安全上下文后，所述移动性管理网元向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息；

所述移动性管理网元接收来自所述终端设备的第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证；

在所述需要进行二级认证的切片中的第一切片二级认证通过后，所述移动性管理网元向所述终端设备发送第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

16、一种通信装置，其特征在于，包括发送单元和接收单元；

所述发送单元，用于向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；

所述接收单元，用于在所述装置完成一级认证和建立安全上下文后，接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中

已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息;

所述接收单元，还用于在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，接收来自所述移动性管理网元的更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

17、如权利要求 16 所述的装置，其特征在于，所述第一注册接受消息还包括以下信息中的至少一个:

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识;

其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

18、如权利要求 17 所述的装置，其特征在于，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

19、如权利要求 16-18 任一所述的装置，其特征在于，所述发送单元，还用于向所述移动性管理网元发送第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证;

所述接收单元，具体用于接收来自所述移动性管理网元的第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

20、如权利要求 19 所述的装置，其特征在于，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示;

所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

21、如权利要求 19 或 20 所述的装置，其特征在于，所述第一消息为第二注册请求消息，所述第二消息为第二注册接受消息; 或者，

所述第一消息为切片注册请求消息，所述第二消息为切片注册接受消息。

22、如权利要求 16-18 任一所述的装置，其特征在于，所述接收单元，具体用于接收来自所述移动性管理网元的配置更新命令，所述配置更新命令包括所述更新的允许接入的切片的选择信息。

23、如权利要求 22 所述的装置，其特征在于，所述配置更新命令还包括以下信息中的至少一个:

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片中被拒绝接入的切片的选择信息、更新后的所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、至少一个临时标识;

其中，一个临时标识对应完成二级认证的切片中的一个或多个切片的选择信息。

24、一种通信装置，其特征在于，包括发送单元、接收单元和处理单元;

所述接收单元，用于接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息；

处理单元，用于在所述终端设备完成一级认证和建立安全上下文后，判断所述请求接入的切片是否需要进行二级认证；

所述发送单元，用于向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括以下信息中的至少一个：所述请求接入的切片中已经完成二级认证的切片的选择信息、所述请求接入的切片中不需要进行二级认证的切片的选择信息、网络分配的不需要进行二级认证的切片的选择信息；

所述发送单元，还用于在所述请求接入的切片中需要进行二级认证且未完成二级认证的第一切片二级认证通过后，向所述终端设备发送更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

25、如权利要求 24 所述的装置，其特征在于，所述第一注册接受消息还包括以下信息中的至少一个：

所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息、所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证所需的预估时间、第一切片认证指示、所述请求接入的切片中不需要进行二级认证的切片的选择信息、所述请求接入的切片中被拒绝接入的切片的选择信息、至少一个临时标识；

其中，所述第一切片认证指示用于指示存在未完成二级认证的切片，一个临时标识对应完成二级认证的一个或多个切片的选择信息。

26、如权利要求 25 所述的装置，其特征在于，所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息携带于一个切片选择信息列表中，所述切片选择信息列表中的切片的选择信息的顺序指示了所述切片选择信息列表中的切片进行二级认证的优先级。

27、如权利要求 24-26 任一所述的装置，其特征在于，所述接收单元，还用于接收来自所述终端设备的第一消息，所述第一消息用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证；

所述发送单元，具体用于向所述终端设备发送第二消息，所述第二消息包括所述更新的允许接入的切片的选择信息。

28、如权利要求 27 所述的装置，其特征在于，所述第一消息包括所述请求接入的切片中需要进行二级认证且未完成二级认证的切片的选择信息，和/或，第二切片认证指示；

所述第二切片认证指示用于请求对所述请求接入的切片中需要进行二级认证且未完成二级认证的切片进行二级认证。

29、一种通信装置，其特征在于，包括发送单元和接收单元；

所述发送单元，用于向移动性管理网元发送第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片；

所述接收单元，用于在所述装置完成一级认证和建立安全上下文后，接收来自所述移动性管理网元的第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择

信息和/或网络分配的不需要进行二级认证的切片的选择信息;

所述发送单元，还用于向所述移动性管理网元发送第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证;

所述接收单元，还用于在所述需要进行二级认证的切片中的第一切片二级认证通过后，接收来自所述移动性管理网元的第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

30、一种通信装置，其特征在于，包括发送单元和接收单元;

所述接收单元，用于接收来自终端设备的第一注册请求消息，所述第一注册请求消息包括请求接入的切片的选择信息，所述请求接入的切片为不需要进行二级认证的切片;

所述发送单元，用于在所述终端设备完成一级认证和建立安全上下文后，向所述终端设备发送第一注册接受消息，所述第一注册接受消息包括允许接入的切片的选择信息，所述允许接入的切片的选择信息包括所述请求接入的切片中的允许接入的切片的选择信息和/或网络分配的不需要进行二级认证的切片的选择信息;

所述接收单元，还用于接收来自所述终端设备的第一消息，所述第一消息包括需要进行二级认证的切片的选择信息，所述第一消息用于请求对所述需要进行二级认证的切片进行切片认证;

所述发送单元，还用于在所述需要进行二级认证的切片中的第一切片二级认证通过后，向所述终端设备发送第二消息，所述第二消息包括更新的允许接入的切片的选择信息，所述更新的允许接入的切片的选择信息包括所述第一切片的选择信息或网络分配的与所述第一切片的选择信息对应的切片的选择信息。

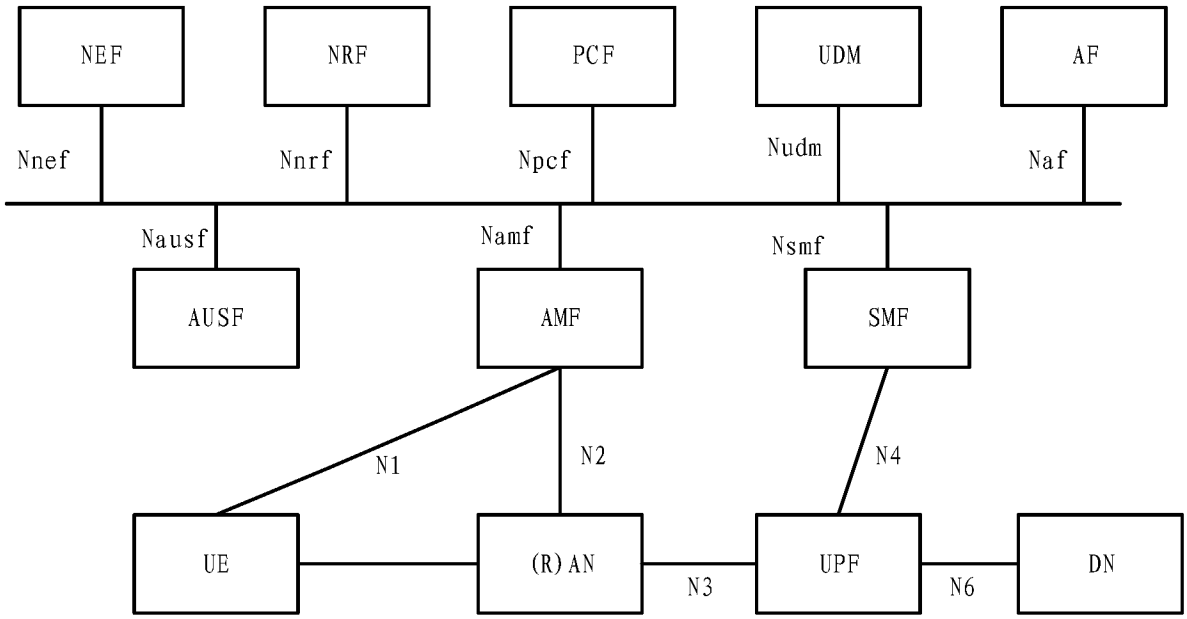
NEF
NRF
PCF
UDM
AF
Nnef
Nnrf
Npcf
Nudm
Naf
Nausf
Namf
Nsmf
AUSF
AMF
SMF
N1
N2
N4
UE
(R)AN
UPF
DN
N3
N6

图 1

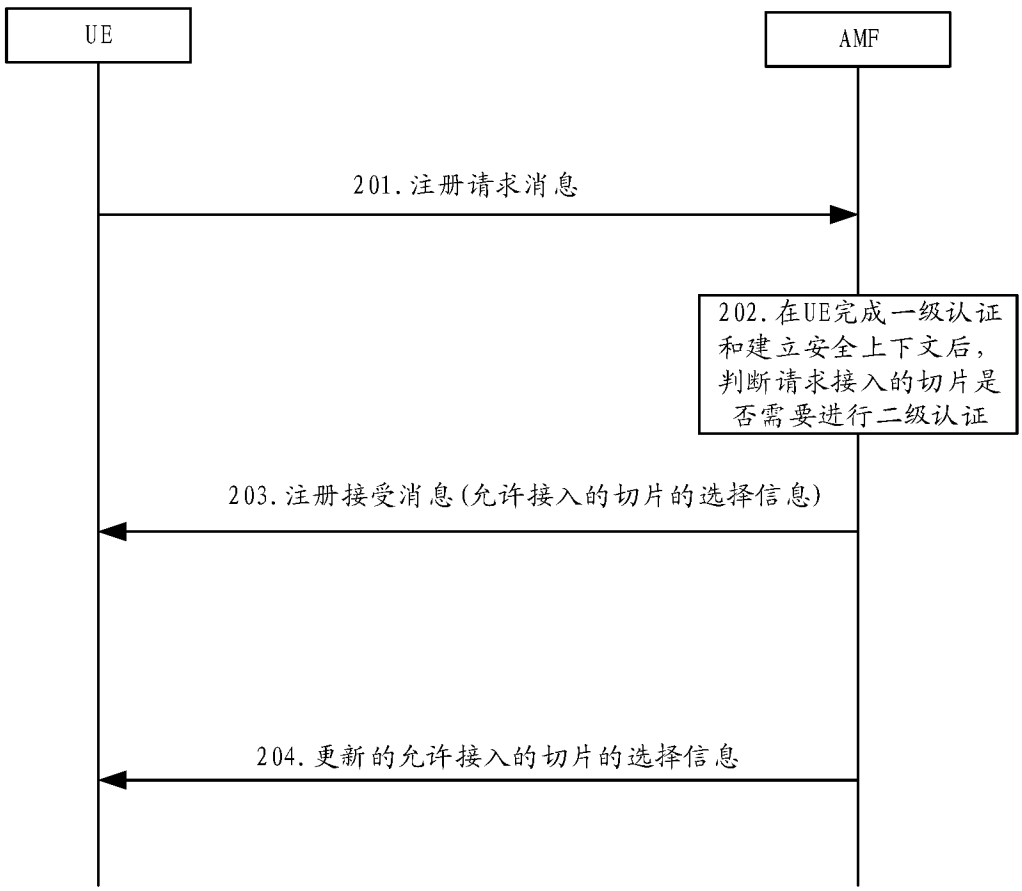
UE
AMF
201.注册请求消息
202.在UE完成一级认证和建立安全上下文后，判断请求接入的切片是否需要进行二级认证
203.注册接受消息(允许接入的切片的选择信息)
204.更新的允许接入的切片的选择信息

图 2

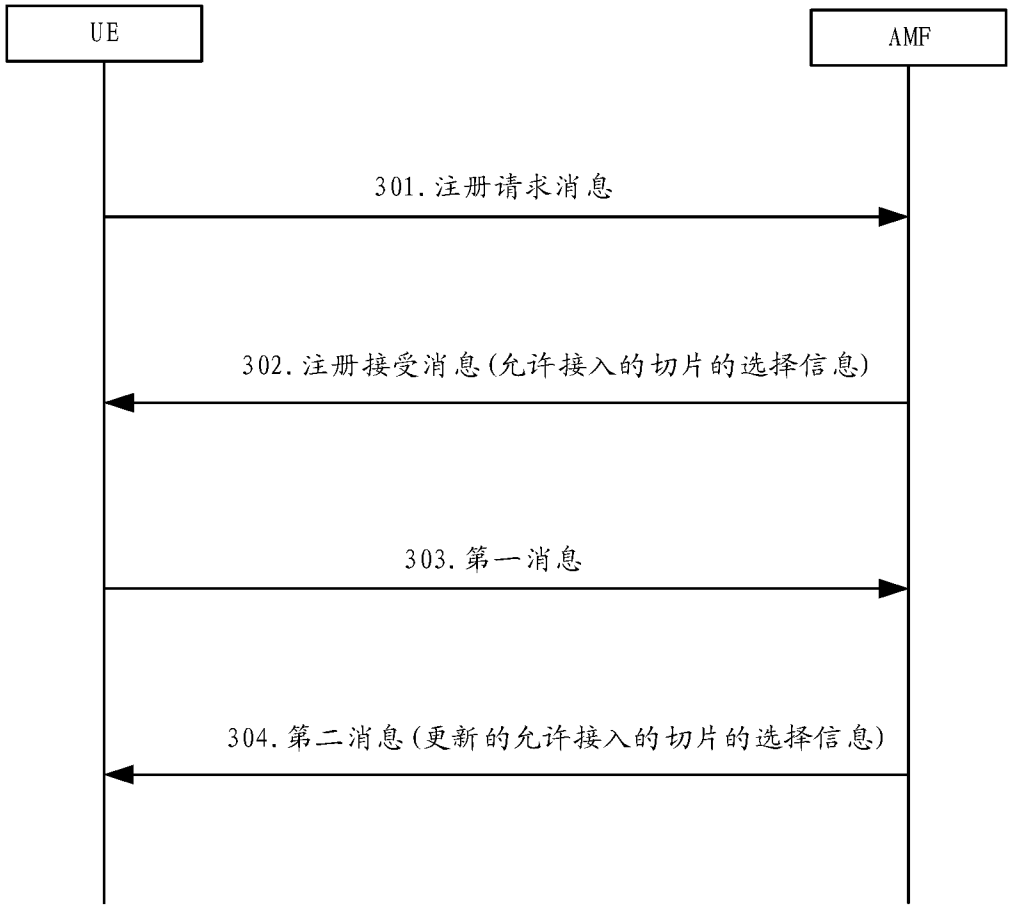
UE
AMF
301. 注册请求消息
302. 注册接受消息(允许接入的切片的选择信息)
303. 第一消息
304. 第二消息(更新的允许接入的切片的选择信息)

图 3

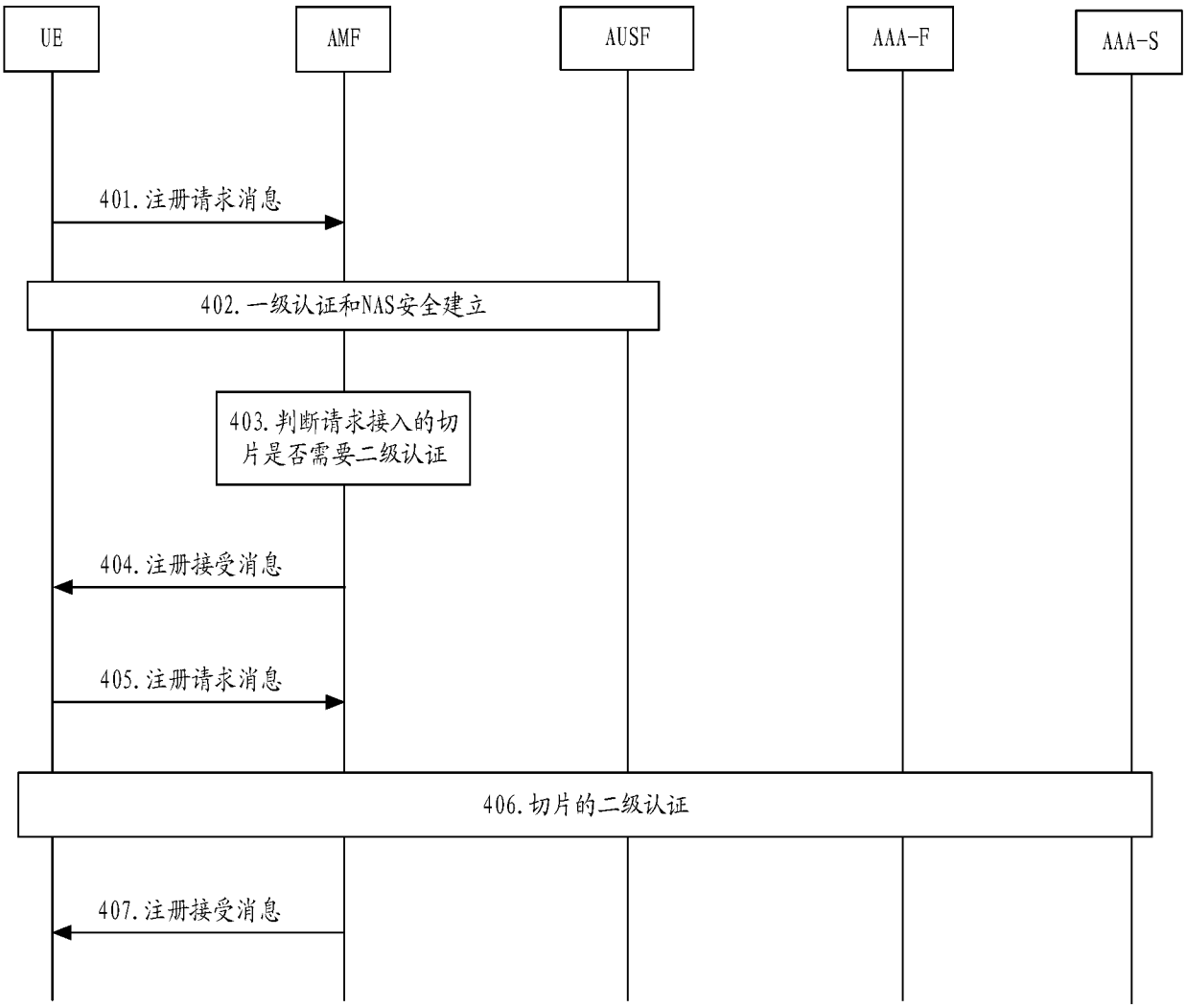
UE
AMF
AUSF
AAA-F
AAA-S
401. 注册请求消息
402. 一级认证和NAS安全建立
403. 判断请求接入的切片是否需要二级认证
404. 注册接受消息
405. 注册请求消息
406. 切片的二级认证
407. 注册接受消息

图 4

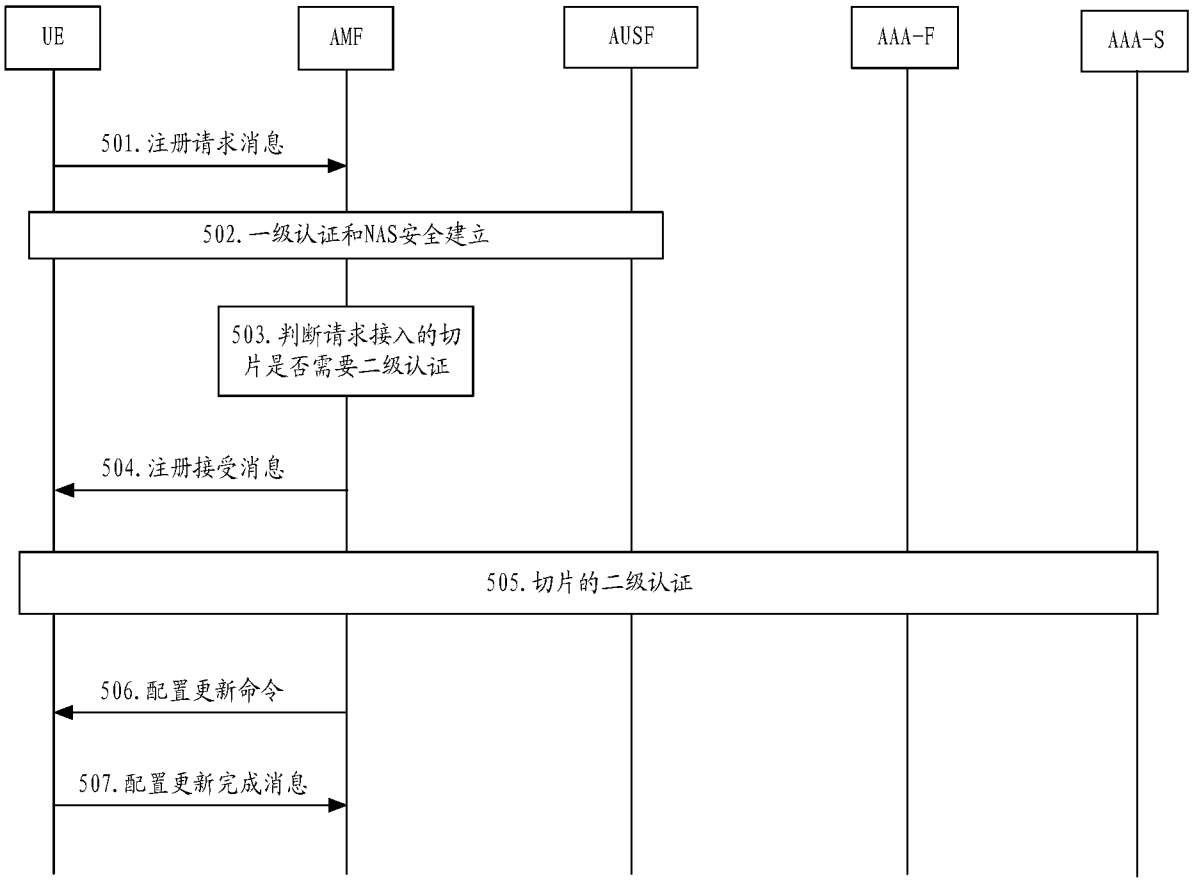
UE
AMF
AUSF
AAA-F
AAA-S
501. 注册请求消息
502. 一级认证和NAS安全建立
503. 判断请求接入的切片是否需要二级认证
504. 注册接受消息
505. 切片的二级认证
506. 配置更新命令
507. 配置更新完成消息

图 5

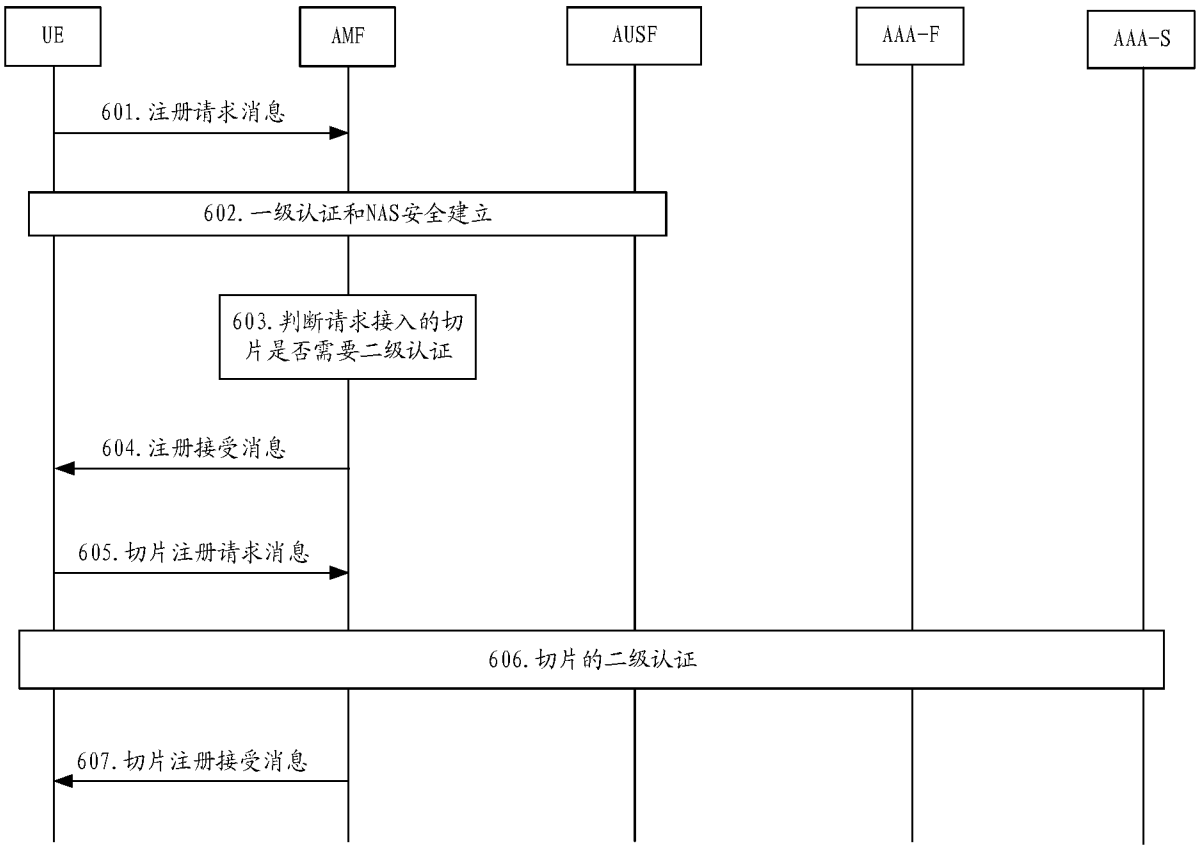
UE
AMF
AUSF
AAA-F
AAA-S
601. 注册请求消息
602. 一级认证和NAS安全建立
603. 判断请求接入的切片是否需要二级认证
604. 注册接受消息
605. 切片注册请求消息
606. 切片的二级认证
607. 切片注册接受消息

图 6

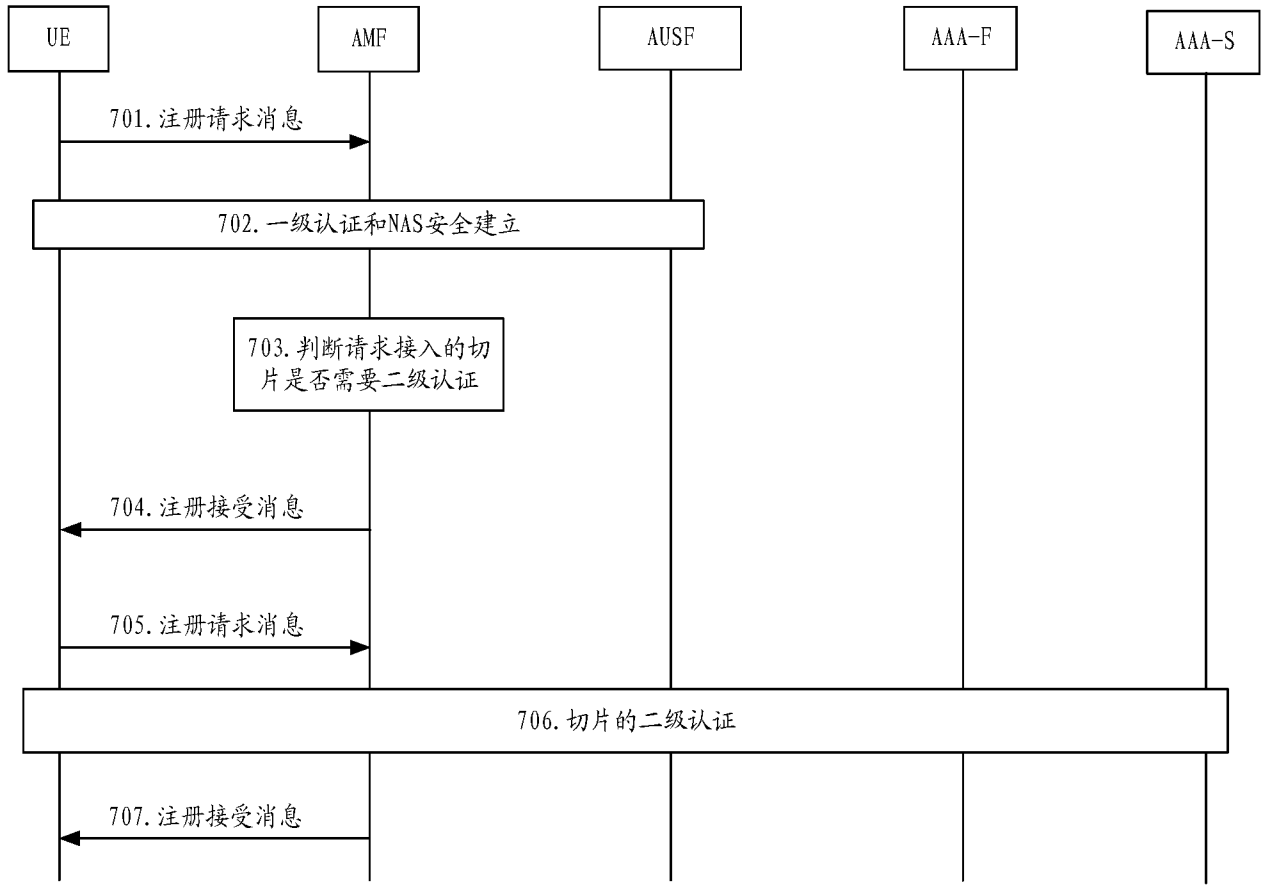
UE
AMF
AUSF
AAA-F
AAA-S
701. 注册请求消息
702. 一级认证和NAS安全建立
703. 判断请求接入的切片是否需要二级认证
704. 注册接受消息
705. 注册请求消息
706. 切片的二级认证
707. 注册接受消息

图 7

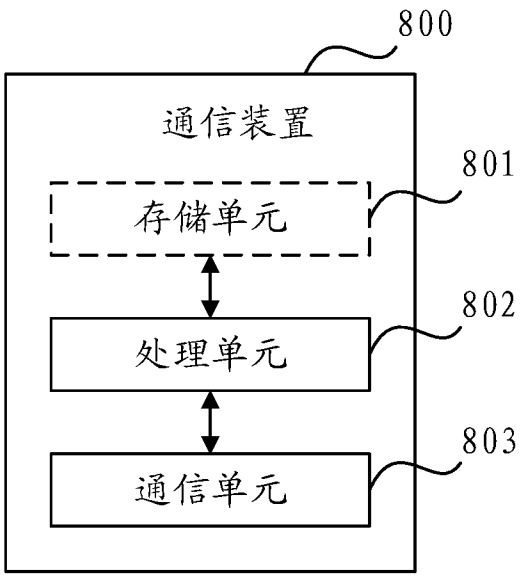
800
通信装置
801
存储单元
802
处理单元
803
通信单元

图 8

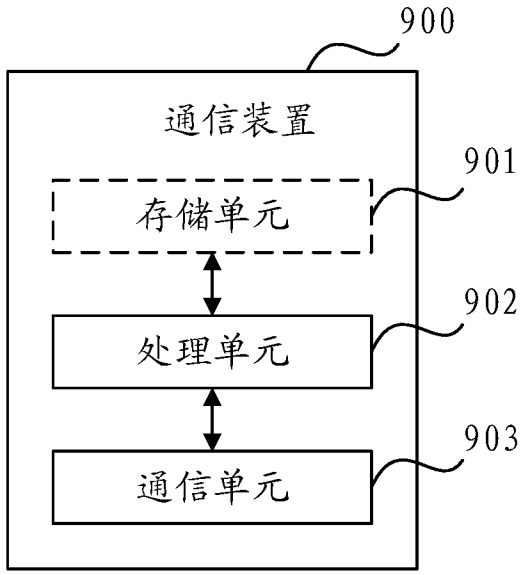
900
通信装置
901
存储单元
902
处理单元
903
通信单元

图 9

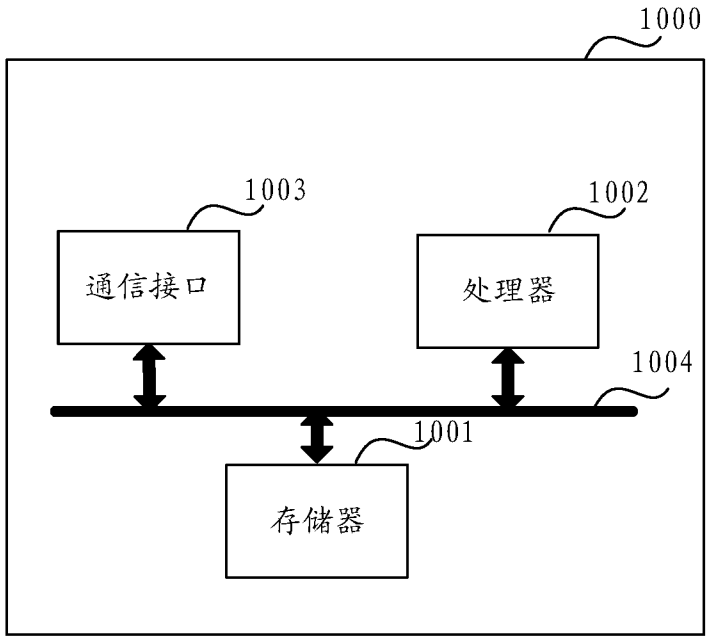
1000
1003
通信接口
1002
处理器
1004
1001
存储器

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/075611

A. CLASSIFICATION OF SUBJECT MATTER

H04W 76/10(2018.01)i; H04W 24/02(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)

CNPAT; CNKI; WPI; EPODOC; IEEE; 3GPP: 会话管理, 注册, 终端, 二次, 二级, 辅助, 认证, 授权, 延时, UE, AMF, request +, NSSAI, secondary, authent+, delay, timer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	QUALCOMM INCORPORATED et al. "TS 23.502: support of secondary slice authentication" *3GPP TSG-SA WG2 Meeting #131 S2-1902882*, 01 March 2019 (2019-03-01), section 4.2.2.2.2	1-30
A	CN 109417709 A (SAMSUNG ELECTRONICS CO., LTD.) 01 March 2019 (2019-03-01) entire document	1-30
A	US 2018317086 A1 (TELEFONAKTIEBOLAGET L M ERICSSON PUBL) 01 November 2018 (2018-11-01) entire document	1-30
A	WO 2018174383 A1 (LG ELECTRONICS INC.) 27 September 2018 (2018-09-27) entire document	1-30

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2020	**20 May 2020**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/075611

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109417709	A	01 March 2019	EP	3466135	A4	20 November 2019
				KR	20190016540	A	18 February 2019
				EP	3466135	A1	10 April 2019
				US	2019261178	A1	22 August 2019
				WO	2018008983	A1	11 January 2018
US	2018317086	A1	01 November 2018	JP	2020506578	A	27 February 2020
				EP	3501155	A1	26 June 2019
				WO	2018137873	A1	02 August 2018
				CN	110235423	A	13 September 2019
				US	2019230510	A1	25 July 2019
				IN	201817006106	A	29 November 2019
WO	2018174383	A1	27 September 2018	US	2020053562	A1	13 February 2020

国际检索报告

国际申请号
PCT/CN2020/075611

A. 主题的分类

H04W 76/10(2018.01)i; H04W 24/02(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））

CNPAT;CNKI;WPI;EPODOC;IEEE;3GPP:会话管理，注册，终端，二次，二级，辅助，认证，授权，延时，UE, AMF, request+, NSSAI, secondary, authent+, delay, timer

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	QUALCOMM INCORPORATED等. "TS 23.502: support of secondary slice authentication" 3GPP TSG-SA WG2 Meeting #131 S2-1902882, 2019年 3月 1日 (2019-03-01), 第4.2.2.2.2节	1-30
A	CN 109417709 A (三星电子株式会社) 2019年 3月 1日 (2019-03-01) 全文	1-30
A	US 2018317086 A1 (TELEFONAKTIEBOLAGET LM ERICSSONPUBL) 2018年 11月 1日 (2018-11-01) 全文	1-30
A	WO 2018174383 A1 (LG ELECTRONICS INC.) 2018年 9月 27日 (2018-09-27) 全文	1-30

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

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

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 4月 27日	2020年 5月 20日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 仝红红 电话号码 86-(10)-53961595

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/075611

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	109417709	A	2019年 3月 1日	EP	3466135	A4	2019年 11月 20日
				KR	20190016540	A	2019年 2月 18日
				EP	3466135	A1	2019年 4月 10日
				US	2019261178	A1	2019年 8月 22日
				WO	2018008983	A1	2018年 1月 11日
US	2018317086	A1	2018年 11月 1日	JP	2020506578	A	2020年 2月 27日
				EP	3501155	A1	2019年 6月 26日
				WO	2018137873	A1	2018年 8月 2日
				CN	110235423	A	2019年 9月 13日
				US	2019230510	A1	2019年 7月 25日
				IN	201817006106	A	2019年 11月 29日
WO	2018174383	A1	2018年 9月 27日	US	2020053562	A1	2020年 2月 13日