(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 1 月 30 日 (30.01.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/020007 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01)

(21) 国际申请号: PCT/CN2019/096023

(22) 国际申请日: 2019 年 7 月 15 日 (15.07.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810824956.1 2018年7月25日 (25.07.2018) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 毛玉欣 (MAO, Yuxin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦由中兴通讯股份有限公司转交, Guangdong 518057 (CN)。

(74) 代理人: 隆天知识产权代理有限公司 (LUNG TIN INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路5号远大中心B座18层, Beijing 100101 (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,

(54) **Title:** NETWORK ACCESS METHOD AND DEVICE, TERMINAL, BASE STATION, AND READABLE STORAGE MEDIUM

(54) **发明名称**: 网络接入方法、装置、终端、基站和可读存储介质

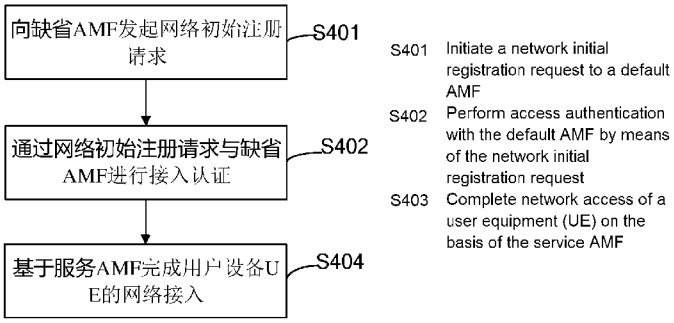

图 4

(57) **Abstract:** Embodiments of the present disclosure provide a network access method and device, a terminal, a base station, and a computer readable storage medium. A network initial registration request is initiated to a default AMF, and then, access authentication is performed with the default AMF by means of the network initial registration request; after the authentication is successful, a corresponding service AMF is determined; the service AMF is an AMF determined according to NSSAI sent to the default AMF; network access of a user equipment (UE) is completed on the basis of the service AMF. Therefore, after an authentication interaction with the default AMF is performed, processing of the NSSAI information is performed to determine the service AMF, so that message leakage possibly caused by directly sending the NSSAI is avoided, and the security of network access is improved.

(57) **摘要**: 本公开实施例提供了一种网络接入方法、装置、终端、基站和计算机可读存储介质，通过向缺省AMF发起网络初始注册请求，然后通过网络初始注册请求与缺省AMF进行接入认证；认证成功后，确定对应的服务AMF；服务AMF为根据发送给缺省AMF的NSSAI所确定的AMF；基于服务AMF完成用户设备UE的网络接入。从而通过与缺省AMF之间的认证交互之后，再进行NSSAI信息的处理过程确定服务AMF，避免了直接发送NSSAI可能造成的消息泄露，提升了网络接入的安全性。

WO 2020/020007 A1

[见续页]

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))。

网络接入方法、装置、终端、基站和可读存储介质

技术领域

本公开实施例涉及网络通信领域，尤其涉及一种网络接入方法、装置、终端、基站和计算机可读存储介质。

背景技术

5G 网络实现了软件和硬件解耦，在通用硬件资源上构建虚拟化网络提供网络服务。5G 网络可以根据需求对网络容量进行灵活弹缩。同时 5G 网络还打破了传统电信网络的封闭模式，将网络服务能力开放给第三方业务（如业务提供商、企业、垂直行业等），让第三方业务可以按需构建网络切片提供网络服务，以适应各种业务快速发展和不断变化的需求。、

3GPP（The 3rd Generation Partnership Project，第三代伙伴计划）定义了 5G 网络通信架构，如图 1 所示。5G 网络以网络切片形式为用户提供网络服务。网络切片是功能完整、逻辑独立、资源共享的虚拟网络。

不同业务对网络服务质量、安全等网络指标存在不同的需求。例如，车联网应用，要求超低时延，超高可靠性；物联网应用保证机器通信，要求高等级的安全保证，而普通的多媒体娱乐等数据业务，虽然对带宽有较高要求，但仅需要普通安全等级就能满足业务要求。5G 技术可通过为不同的业务定制不同的网络切片，以满足每种业务的需求。每个网络切片逻辑上是独立的一张网络，可为用户提供网络服务。虽然多个网络切片共用网络基础资源，但网络切片之间彼此是隔离的。网络切片以 NSSAI（Network Slice Selection Assistance Information， 网络切片选择辅助信息）标识。但是，在网络接入的过程中，NSSAI 信息传递过程未加以保护，容易被在消息传递路径上获取其信息，进而易受到其他人群针对此发起的攻击，瘫痪网络，影响用户和网络安全。

发明内容

本公开实施例提供了一种网络接入方法、装置、终端、基站和计算机可读存储介质，旨在解决先有技术中网络接入安全性差，易受到攻击的问题。

为了解决上述技术问题，本公开实施例提供了一种网络接入方法，包括：

向缺省接入和移动性管理功能 AMF 发起网络初始注册请求；

通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

认证成功后，确定对应的服务 AMF；所述服务 AMF 为根据发送给所述缺省 AMF 的网络切片选择辅助信息 NSSAI 所确定的 AMF；

基于所述服务 AMF 完成用户设备 UE 的网络接入。

本公开实施例还提供一种网络接入方法，包括：

接收 UE 发送的网络初始注册请求；

通过所述网络初始注册请求与所述 UE 进行接入认证；

认证成功后，根据接收到的由所述 UE 发送的 NSSAI 确定对应的服务 AMF；

通过所述服务 AMF 完成 UE 的网络接入。

本公开实施例还提供了一种网络接入装置，包括：

请求发起模块，设置为向 AMF 发起网络初始注册请求；

第一认证模块，设置为通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

第一 AMF 确认模块，设置为认证成功后，确定对应的服务 AMF；所述服务 AMF 为根据发送给所述缺省 AMF 的网络切片选择辅助信息 NSSAI 所确定的 AMF；

第一网络接入模块，设置为基于所述服务 AMF 完成用户设备 UE 的网络接入。

本公开实施例还提供一种网络接入装置，包括：

请求接收模块，设置为接收 UE 发送的网络初始注册请求；

第二认证模块，设置为通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

第二 AMF 确认模块，设置为认证成功后，根据接收到的由所述 UE 发送的 NSSAI 确定对应的服务 AMF；

第二网络接入模块，设置为通过所述服务 AMF 完成 UE 的网络接入。

本公开实施例还提供了一种终端，包括第一处理器、第一存储器和第一通信总线；

所述第一通信总线设置为实现所述第一处理器和第一存储器之间的连接通信；

所述第一处理器设置为执行所述第一存储器中存储的计算机程序，以实现上述的网络接入方法的步骤。

本公开实施例还提供了一种基站，包括第二处理器、第二存储器和第二通信总线；

所述第二通信总线设置为实现所述第二处理器和第二存储器之间的连接通信；

所述第二处理器设置为执行所述第二存储器中存储的计算机程序，以实现上述的网络接入方法的步骤。

本公开实施例还提供了一种计算机可读存储介质，计算机可读存储介质中存储有一个或者多个计算机程序，计算机程序可被一个或者多个处理器执行，以实现上述的网络接入方法的步骤。

本公开实施例的有益效果是：

本公开实施例提供了一种网络接入方法、装置、终端、基站和计算机可读存储介质，通过向缺省 AMF 发起网络初始注册请求，然后通过网络初始注册请求与缺省 AMF 进行接入认证；认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的 NSSAI 所确定的 AMF；基于服务 AMF 完成用户设备 UE 的网络接入。从而通过与缺省 AMF 之间的认证交互之后，再进行 NSSAI 信息的处理过程确定服务 AMF，避免了直接发送 NSSAI 可能造成的消息泄露，提升了网络接入的安全性。

本公开实施例其他特征和相应的有益效果在说明书的后面部分进行阐述说明，且应当

理解，至少部分有益效果从本公开说明书中的记载变的显而易见。

附图说明

图 1 为 5G 网络通信架构示意图；

图 2 为切片网络接入示意图；

图 3 为 3GPP 定义的网络接入方法信号流图；

图 4 为本公开第一实施例提供的一种网络接入方法流程图；

图 5 为本公开第二实施例提供的一种网络接入方法流程图；

图 6 为本公开第三实施例提供的一种网络接入方法信号流图；

图 7 为本公开第四实施例提供的一种网络接入方法信号流图；

图 8 为本公开第五实施例提供的一种网络接入方法信号流图；

图 9 为本公开第六实施例提供的一种网络接入装置组成示意图；

图 10 为本公开第七实施例提供的一种网络接入装置组成示意图；

图 11 为本公开第八实施例提供的一种终端组成示意图；

图 12 为本公开第九实施例提供的一种基站组成示意图。

具体实施方式

图 2 描述了用户接入 5G 网络，使用网络切片提供服务的示例。通过网络编排管理系统编排网络切片 1 为车联网业务提供服务，编排网络切片 2 为互联网业务提供服务，切片 1 与切片 2 之间逻辑隔离。公共网元域是被多个切片共享的公共网元，例如 AMF（Access and Mobility Management Function， 接入和移动性管理功能），NSSF（Network Slice Selection Function， 网络切片选择功能），AUSF（Authentication Server Function， 认证服务功能）等。用户 UE（User Equipment， 用户设备）如果使用车联网业务，就需要接入切片 1；如果使用互联网业务，就需要接入切片 2。不同业务对网络服务质量、安全等网络指标存在不同的需求。例如，车联网应用，要求超低时延，超高可靠性；物联网应用保证机器通信，要求高等级的安全保证，而普通的多媒体娱乐等数据业务，虽然对带宽有较高要求，但仅需要普通安全等级就能满足业务要求。5G 技术可通过为不同的业务定制不同的网络切片，以满足每种业务的需求。每个网络切片逻辑上是独立的一张网络，可为用户提供网络服务。虽然多个网络切片共用网络基础资源，但网络切片之间彼此是隔离的。

3GPP 定义了用户附着到网络，发起初次注册的流程，如图 3 所示。

S301、UE 发送注册请求消息，消息中包含：注册类型、SUPI/5G-GUTI（Subscription Permanent Identifier， 永久签约标识/5G-Globally Unique Temporary UE Identity， 5G 全球唯一临时 UE 标识）、安全参数、NSSAI 等信息。NSSAI 用于指示用户请求接入的网络切片。

S302、RAN（Radio Access Network， 无线接入网络）根据 UE（User Equipment，用

户设备）提供的信息，例如 NSSAI 以及运营商策略，选择为用户接入服务的 AMF（Access and Mobility Management Function， 接入和移动性管理功能）。

S303、RAN 将所述注册请求消息路由至所述 AMF。

S304、如果 UE 注册请求消息中包含了 5G-GUTI，并且选择当前服务 AMF 与用户上一次注册所使用的 AMF 不同时，新的 AMF 和旧 AMF 交互，从旧 AMF 获取 SUPI 和移动性管理上下文信息。

S305、如果步骤 S301 或者步骤 S303 中没有向新 AMF 提供 SUPI，则新 AMF 向 UE 发起标识请求程序，请求 UE 提供 SUPI。

S306、UE 向新 AMF 提供 SUCI（Subscription Concealed Identifier，隐藏签约标识，经过加密的 SUPI）。

S307、新 AMF 发起 UE 接入认证过程，根据 SUCI 选择 AUSF（Authentication Server Function， 认证服务功能）。

S308、UE、新 AMF、AUSF、UDM（Unified Data Management， 统一数据管理）之间交互认证流程，完成 UE 和 AMF 之间的双向认证。

S309、认证成功之后，AMF 发起 NAS（Non-Access Stratum， 非接入层）安全通道建立程序，建立 NAS 安全通道，对 UE 和 AMF 交互的消息进行加密和完整性保护。

S310、认证完成之后，新 AMF 向旧 AMF 通知 UE 注册成功。

S311、如果步骤 S301 或者步骤 S303 中没有向新 AMF 提供 PEI（Permanent Equipment Identifier， 设备永久标识），则新 AMF 向 UE 发起标识请求程序，请求 UE 提供 PEI。AMF 和 EIR（Equipment Identity Register，设备标识寄存器）交互，对 PEI 进行认证。

S312、新 AMF 注册到 UDM，UDM 存储 AMF 标识，以及接入类型。新 AMF 从 UDM 获取接入和移动性签约数据、SMF（Session Management Function， 会话管理功能）选择签约数据等。获取这些信息之后，创建移动性管理上下文。新 AMF 向 UDM 订阅用户签约信息，当用户签约信息发生更改时，及时通知新 AMF，以便新 AMF 根据新的用户签约信息重新创建移动性管理上下文。

S303、UDM 通知旧 AMF 删除与所述 UE 相关的移动性管理上下文。旧 AMF 通知相关 SMF 所述 UE 已经从旧 AMF 去注册，释放相关的 PDU 会话。旧 AMF 从 UDM 上去注册之前的相关订阅事件。

S314、如果 AMF 发生改变，新 AMF 向每个 SMF 通知 UE 可达状态。如果 PDU 会话状态指示已经在 UE 侧释放，则 AMF 需要通知 SMF 释放和该 PDU 会话关联的网络资源。

S315、新 AMF 向 UE 返回注册接受消息，包含：5G-GUTI（新 AMF 为其分配的最新 5G-GUTI）、NSSAI（经过网络侧授权的允许 UE 请求使用的 NSSAI）等信息。

S316、UE 向新 AMF 发送注册完成消息。

上述图 3 中，在用户成功完成接入认证之后，用户和网络之间建立 NAS 安全通道，

保证UE和AMF之间交互的信息经过加密和完整性保护。而在所述NAS安全通道建立(步骤S309)之前，即步骤S301-S306消息均为明文传递，包括在此期间用户向网络发送注册请求消息时携带的IMSI（International Mobile Subscriber Identification Number， 国际移动用户识别码），以及用户请求接入的网络切片标识NSSAI信息都为明文。因此中间人在消息传递路径上很容易获取IMSI、NSSAI等关键用户信息。通过分析就可以推断出NSSAI对应的网络切片的作用，即提供何种服务，或者推断出使用网络切片的人群等，以便有针对性的向所述切片发起诸如DoS（Denial of Service，拒绝服务）等攻击，瘫痪网络，影响用户和网络安全。

为了使本公开的目的、技术方案及优点更加清楚明白，下面通过各实施方式结合附图对本公开实施例作进一步详细说明。应当理解，此处所描述的实施例仅仅用以解释本公开，并不用于限定本公开。

第一实施例

请参考图4，图4是本公开第一实施例提供的网络接入方法流程图，包括：

S401、向缺省接入和移动性管理功能AMF发起网络初始注册请求；

S402、通过网络初始注册请求与缺省AMF进行接入认证；

S403、认证成功后，确定对应的服务AMF；服务AMF为根据发送给缺省AMF的网络切片选择辅助信息NSSAI所确定的AMF；

S404、基于服务AMF完成用户设备UE的网络接入。

为了避免因NSSAI暴露而引发的网络攻击，需要在用户接入网络过程中，保证NSSAI传递的安全性，因此本实施例提出了一种用户接入网络的网络接入方法，通过对 NSSAI的加密传递，达到保护NSSAI的目的。

本实施例中所述的缺省AMF，所指的是系统默认状态下的AMF；由于本实施例中的网络接入过程中，UE没有直接在请求时提供明文的NSSAI信息，因此无法直接确认UE所要接入的服务AMF来完成网络的接入过程，所以UE的交互对象首先是缺省AMF，通过缺省AMF来为用户进行接入服务。

在UE与缺省AMF交互的过程中，缺省AMF的交互需要涉及到与UE之间的认证过程，认证过程中并不涉及到UE对服务AMF的选择，而是为了后续UE与缺省AMF之间交互NSSAI信息。本实施例为了提升NSSAI信息在传输过程中的安全性，示例性而言，NSSAI可以为通过非对称加密方式传送、对称加密方式传送以及NAS安全通道传送中的至少一种发送给缺省AMF。也就是说，NSSAI在UE和缺省AMF之间进行传输的手段，可以包括对NSSAI本身进行加密，或者是在安全的NAS安全通道内传输两种手段。而对NSSAI 进行加密，则可以通过非对称加密、对称加密等手段来实现。上述各加密手段之间可以单独实施，也可以组合进行，比如可通过非对称加密手段对NSSAI进行加密，然后再通过NAS安全通道进行传输；或者是通过对称加密手段对NSSAI进行加密，然后在

通过 NAS 安全通道进行传输等等。

在一些实施例中，NSSAI 为通过非对称加密方式传送可以包括：确定在 UE 和网络侧配置的运营商公钥和私钥；通过公钥对 NSSAI 进行加密；将加密后的 NSSAI 通过网络初始注册请求发送给缺省 AMF。其中，通过非对称加密方式传送，首先需要在 UE 侧以及网络侧配置匹配的运营商公钥和私钥；然后，UE 在发送 NSSAI 至网络侧时，则通过配置的运营商公钥，对 NSSAI 进行加密，然后发送加密的 NSSAI 至网络侧。而发送的过程可以通过网络初始注册请求，来携带加密的 NSSAI 并发送至网络侧。

相应的，认证成功后，确定对应的服务 AMF 可以包括：认证成功后，对 NSSAI 通过私钥进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。由于 NSSAI 通过运营商公钥进行了加密，为了保证其安全性，需要在 UE 和缺省 AMF 之间的认证通过后，方才通过运营商私钥对该加密的 NSSAI 进行解密，从而可得到明文 NSSAI。得到明文 NSSAI 之后，缺省 AMF 就可以根据该 NSSAI 的内容，来确定用户接入切片网络所需的服务 AMF。

在一些实施例中，NSSAI 为通过对称加密方式传送包括：认证成功后，根据根密钥和密钥材料产生密钥，通过密钥对 NSSAI 进行加密；将加密后的 NSSAI 发送给缺省 AMF。对称加密的过程可以在 UE 与缺省 AMF 认证成功之后进行；在认证成功后，根密钥 K 产生认证向量（包括 RAND（RANDom，随机数），AUTN（AUthentication TokeN，授权令牌），$K_{NSSAIenc}$ 等信息）。AUSF 将该认证向量发送给缺省 AMF。该缺省 AMF 保存认证向量，并将密钥材料 RAND，AUTN 等信息发送给 UE。UE 进行验证，并根据保存的根密钥 K 和密钥材料计算产生 $K_{NSSAIenc}$。

相应的，认证成功后，确定对应的服务 AMF 可以包括：根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥；将密钥发送给缺省 AMF；根据密钥，对加密后的 NSSAI 进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。在认证成功后，服务 AMF 根据加密该 NSSAI 的认证向量 $K_{NSSAIenc}$ 来相应的对 NSSAI 进行解密，从而得到明文 NSSAI，然后根据该明文 NSSAI 的内容，确定对应的服务 AMF，来实现 UE 的切片网络的接入。

在一些实施例中，NSSAI 为通过 NAS 安全通道传送还可以包括：认证成功后，在 UE 和缺省 AMF 之间建立 NAS 安全通道；通过 NAS 安全通道发送 NSSAI 给缺省 AMF。此时，不需要对 NSSAI 本身进行加密，而通过安全的 NAS 安全通道来发送 NSSAI，从而保证 NSSAI 的安全性，避免 NSSAI 被外界所窃取。

在一些实施例中，认证成功后，确定对应的服务 AMF 可以包括：根据 NSSAI，确定对应的服务 AMF；确定对应的服务 AMF 之后，拆除 UE 和缺省 AMF 之间的 NAS 安全通道。在确定了服务 AMF 之后，在 UE 和缺省 AMF 之间的 NAS 安全通道就没有必要继续保留了，可以直接拆除以节约网络资源。

本实施例提供了一种网络接入方法，通过向缺省 AMF 发起网络初始注册请求，然后通过网络初始注册请求与缺省 AMF 进行接入认证；认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的 NSSAI 所确定的 AMF；基于服务 AMF 完成用户设

备 UE 的网络接入。从而通过与缺省 AMF 之间的认证交互之后，再进行 NSSAI 信息的处理过程确定服务 AMF，避免了直接发送 NSSAI 可能造成的消息泄露，提升了网络接入的安全性。

第二实施例

请参考图 5，图 5 为本公开第二实施例提供的一种网络接入方法流程图，包括：

S501、接收 UE 发送的网络初始注册请求；

S502、通过网络初始注册请求与 UE 进行接入认证；

S503、认证成功后，根据接收到的由 UE 发送的 NSSAI 确定对应的服务 AMF；

S504、通过服务 AMF 完成 UE 的网络接入。

为了避免因 NSSAI 暴露而引发的网络攻击，需要在用户接入网络过程中，保证 NSSAI 传递的安全性，因此本实施例提出了一种用户接入网络的网络接入方法，通过对 NSSAI 的加密传递，达到保护 NSSAI 的目的。

本实施例中所述的缺省 AMF，所指的是系统默认状态下的 AMF；由于本实施例中的网络接入过程中，UE 没有直接在请求时提供明文的 NSSAI 信息，因此无法直接确认 UE 所要接入的服务 AMF 来完成网络的接入过程，所以 UE 的交互对象首先是缺省 AMF，通过缺省 AMF 来为用户进行接入服务。

在 UE 与缺省 AMF 交互的过程中，缺省 AMF 的交互需要涉及到与 UE 之间的认证过程，认证过程中并不涉及到 UE 对服务 AMF 的选择，而是为了后续 UE 与缺省 AMF 之间交互 NSSAI 信息。本实施例为了提升 NSSAI 信息在传输过程中的安全性，示例性而言，缺省 AMF 可以通过非对称加密方式传送、对称加密方式传送以及 NAS 安全通道传送中的至少一种方式接收 NSSAI。也就是说，NSSAI 在 UE 和缺省 AMF 之间进行传输的手段，可以包括对 NSSAI 本身进行加密，或者是在安全的 NAS 安全通道内传输两种手段。而对 NSSAI 进行加密，则可以通过非对称加密、对称加密等手段来实现。上述各加密手段之间可以单独实施，也可以组合进行，比如可通过非对称加密手段对 NSSAI 进行加密，然后再通过 NAS 安全通道进行传输；或者是通过对称加密手段对 NSSAI 进行加密，然后在通过 NAS 安全通道进行传输等等。

在一些实施例中，NSSAI 为通过非对称加密方式传送可以包括：确定在 UE 和网络侧配置的运营商公钥和私钥；通过公钥对 NSSAI 进行加密；接收加密后的 NSSAI。其中，通过非对称加密方式传送，首先需要在 UE 侧以及网络侧配置匹配的运营商公钥和私钥；然后，UE 在发送 NSSAI 至网络侧时，则通过配置的运营商公钥，对 NSSAI 进行加密，然后发送加密的 NSSAI 至网络侧。而发送的过程可以通过网络初始注册请求，来携带加密的 NSSAI 并发送至网络侧。

相应的，认证成功后，根据接收到的由 UE 发送的 NSSAI 确定对应的服务 AMF 可以包括：认证成功后，对 NSSAI 通过私钥进行解密；根据解密后的 NSSAI，确定对应的服

务 AMF。由于 NSSAI 通过运营商公钥进行了加密，为了保证其安全性，需要在 UE 和缺省 AMF 之间的认证通过后，方才通过运营商私钥对该加密的 NSSAI 进行解密，从而可得到明文 NSSAI。得到明文 NSSAI 之后，缺省 AMF 就可以根据该 NSSAI 的内容，来确定用户接入切片网络所需的服务 AMF。

在一些实施例中，NSSAI 为通过对称加密方式传送可以包括：认证成功后，根据根密钥和密钥材料和密钥材料计算产生用于 NSSAI 加密的密钥，通过密钥对 NSSAI 进行加密；接收加密后的 NSSAI。对称加密的过程可以在 UE 与缺省 AMF 认证成功之后进行；在认证成功后，根密钥 K 产生认证向量（包括 RAND（RANDom，随机数），AUTN（AUthentication TokeN，授权令牌），$K_{NSSAIenc}$ 等信息）。AUSF 将该认证向量发送给缺省 AMF。该缺省 AMF 保存认证向量，并将密钥材料 RAND，AUTN 等信息发送给 UE。UE 进行验证，并根据保存的根密钥 K 和密钥材料计算产生 $K_{NSSAIenc}$。

相应的，认证成功后，确定对应的服务 AMF 可以包括：根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥；接收密钥；根据该密钥，对加密后的 NSSAI 进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。在认证成功后，服务 AMF 根据加密该 NSSAI 的认证向量 $K_{NSSAIenc}$ 来相应的对 NSSAI 进行解密，从而得到明文 NSSAI，然后根据该明文 NSSAI 的内容，确定对应的服务 AMF，来实现 UE 的切片网络的接入。

在一些实施例中，NSSAI 为通过 NAS 安全通道传送可以包括：认证成功后，在 UE 和 NSSAI 之间建立 NAS 安全通道；通过 NAS 安全通道接收 NSSAI。此时，不需要对 NSSAI 本身进行加密，而通过安全的 NAS 安全通道来发送 NSSAI，从而保证 NSSAI 的安全性，避免 NSSAI 被外界所窃取。

本实施例提供了一种网络接入方法，通过向缺省 AMF 发起网络初始注册请求，然后通过网络初始注册请求与缺省 AMF 进行接入认证；认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的 NSSAI 所确定的 AMF；基于服务 AMF 完成用户设备 UE 的网络接入。从而通过与缺省 AMF 之间的认证交互之后，再进行 NSSAI 信息的处理过程确定服务 AMF，避免了直接发送 NSSAI 可能造成的消息泄露，提升了网络接入的安全性。

第三实施例

请参考图 6，图 6 为本实施例提供的一种网络接入方法信号流图，包括：

本实施例描述了一种用户接入网络过程中的优化注册流程，实现 NSSAI 的加密传递，保证 NSSAI 传递过程中的安全性。本实施例中用户接入网络初始选择的 AMF 为缺省 AMF，即根据 UE 提供的信息无法进行 AMF 选择时配置的 AMF。具体实施过程如下描述：

S601、在 UE 配置运营商公钥，用于 UE 向网络发送消息时，对需要保护的信息进行加密；网络侧 SIDF（Subscription Identifier De-concealing Function， 签约标识解密功能）

保存相应的运营商私钥，用于对从 UE 接收的信息的解密。

S602、UE 接入网络发起注册请求，将请求接入的网络切片标识 NSSAI 使用该公钥进行加密。

S603、UE 发起网络初始注册请求，请求消息中包含加密 NSSAI。由于 NSSAI 加密，根据 AMF 选择方法，无法为用户选择到 NSSAI 对应的 AMF。因此选择缺省 AMF 为用户接入服务。

S604、UE 和缺省 AMF 之间完成双向认证。

S605、认证过程中，加密 NSSAI 被传递至 SIDF。认证成功之后，SIDF 对加密 NSSAI 解密成明文，并将该明文 NSSAI 发送给缺省 AMF。

S606、该缺省 AMF 根据该明文 NSSAI 向 NSSF 发送切片选择请求。NSSF 对请求 NSSAI（即该明文 NSSAI）进行授权，向该缺省 AMF 返回该授权 NSSAI，以及 target AMF（目的 AMF）集。

S607、该缺省 AMF 向 NRF 发起 Target AMF（即服务 AMF）查询，获取服务 AMF 的 IP 地址/FQDN(Fully Qualified Domain Name， 全限定域名)信息。

S608、该缺省 AMF 向该 Target AMF 转发用户注册请求，并包含该 RAN 信息，以及认证成功之后缺省 AMF 上产生的移动性管理上下文等信息。

S609、该 Target AMF 向 RAN 发送 N2 会话消息。

S610、如果该 Target AMF 需要对 UE 进行再次认证，则发起接入认证过程。

S611、剩余接入注册过程，参考图 3 中的步骤 S304-306 以及 S309-316。

上述实现过程，保证了 NSSAI 在 UE 和网络之间以加密方式传递，避免中间人窃取 NSSAI 之后通过解析推断出切片作用，接入人群属性，进而发起网络攻击，保证了用户和网络安全。

第四实施例

请参考图 7，图 7 为本公开第四实施例提供的一种网络接入方法信号流图，包括：

本实施例描述了一种用户接入网络时的优化注册流程，通过 UE 和缺省 AMF 之间认证成功之后派生用于 NSSAI 加密密钥。通过该密钥加密 NSSAI 实现安全传递。具体实施过程如下描述：

S701、UE 接入网络，发起注册请求。初始注册请求消息不包含 NSSAI，因此无法选择合适的 AMF，使用缺省 AMF 为 UE 接入服务。

S702、缺省 AMF 接收该注册请求，如果没有获取到用户标识 SUPI，则发起标识获取流程，从 UE 获取 SUCI(经过加密的 SUPI)。

S703、UE 和缺省 AMF 之间完成接入认证。AUSF 根据 UE 签约信息中的根密钥 K 产生认证向量（包括 RAND（RANDom，随机数），AUTN（AUthentication TokeN，授权令牌）， $K_{NSSAIenc}$ 等信息）。AUSF 将该认证向量发送给缺省 AMF。该缺省 AMF 保存认

证向量，并将密钥材料 RAND，AUTN 等信息发送给 UE。UE 进行验证，并根据保存的根密钥 K 和密钥材料计算产生 $K_{NSSAIenc}$。

S704、UE 使用对 $K_{NSSAIenc}$ 对 NSSAI 进行加密。

S705、UE 将加密 NSSAI 发送给缺省 AMF。

S706、缺省 AMF 接收该加密 NSSAI 之后使用 $K_{NSSAIenc}$ 解密，得到明文 NSSAI。

S707、该缺省 AMF 根据该明文 NSSAI 向 NSSF 发送切片选择请求。NSSF 对请求 NSSAI（即该明文 NSSAI）进行授权，向该缺省 AMF 返回该授权 NSSAI，以及 target AMF 集。

S708、该缺省 AMF 向 RAN 发送 N2 会话消息，将 target AMF 集携带给 RAN

S709、该 RAN 向 NRF 发起 Target AMF（即服务 AMF）查询，获取服务 AMF 的 IP 地址/FQDN 信息。

S710、该 RAN 向该 Target AMF 转发用户注册请求。

S711、如果该 Target AMF 需要对 UE 进行再次认证，则发起接入认证过程。

S712、剩余接入注册过程，参考图 3 中的步骤 S304-306 以及 S309-316。

上述实现过程，首先通过 UE 和缺省 AMF 之间执行接入认证，并根据 UE 根密钥 K 产生共享密钥 $K_{NSSAIenc}$ 后对 NSSAI 进行加密传送，保证 NSSAI 传输过程中的安全性。

第五实施例

请参考图 8，图 8 为本公开第五实施例提供的一种网络接入方法信号流图，包括：

本实施例描述了一种用户接入网络时的优化注册流程，通过 UE 和缺省 AMF 之间建立 NAS 安全通道传递 NSSAI，并在选择到服务 AMF 之后，拆除该 NAS 通道的方式实现 NSSAI 安全传递。具体实施过程如下描述：

S801、UE 接入网络，发起注册请求。初始注册请求消息不包含 NSSAI，因此无法选择合适的 AMF，使用缺省 AMF 为 UE 接入服务。

S802、缺省 AMF 接收该注册请求，如果没有获取到用户标识 SUPI，则发起标识获取流程，从 UE 获取 SUCI(经过加密的 SUPI)。

S803、UE 和缺省 AMF 之间完成接入认证。

S804、UE 和缺省 AMF 之间建立 NAS 安全通道。

S805、UE 使用该 NAS 安全通道将 NSSAI 发送给该缺省 AMF。该 NAS 安全通道是对 UE 和缺省 AMF 之间发送的整条消息进行加密和完整性保护。

S806、缺省 AMF 获取该 NSSAI，根据该 NSSAI 向 NSSF 发送切片选择请求。NSSF 对请求 NSSAI 进行授权，向该缺省 AMF 返回该授权 NSSAI，以及 target AMF 集。

S807、该缺省 AMF 向 NRF 发起 Target AMF（即服务 AMF）查询，获取服务 AMF 的 IP 地址/FQDN 信息。

S808、该缺省 AMF 向该 Target AMF 转发用户注册请求，并包含该 RAN 信息，以及

认证成功之后缺省 AMF 上产生的移动性管理上下文等信息。

S809、该 Target AMF 向 RAN 发送 N2 会话消息。

S810、缺省 AMF 拆除 NAS 安全通道。

S811、如果该 Target AMF 需要对 UE 进行再次认证，则发起接入认证过程。

S812、Target AMF 和 UE 建立 NAS 安全通道。

S813、剩余接入注册过程，参考图 3 中的步骤 S304-306 以及 S310-316。

上述实现过程，首先通过 UE 和缺省 AMF 之间完成接入认证之后，建立临时 NAS 安全通道用于 NSSAI 的安全传递。在缺省 AMF 根据该 NSSAI 发现服务 AMF 之后，拆除 UE 和缺省 AMF 之间的 NAS 安全通道，以此保证 NSSAI 传输过程中的安全性。

第六实施例

请参考图 9，图 9 为本公开第六实施例提供的一种网络接入装置组成示意图，包括：

请求发起模块 91，设置为向 AMF 发起网络初始注册请求；

第一认证模块 92，设置为通过网络初始注册请求与缺省 AMF 进行接入认证；

第一 AMF 确认模块 93，设置为认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的网络切片选择辅助信息 NSSAI 所确定的 AMF；

第一网络接入模块 94，设置为基于服务 AMF 完成用户设备 UE 的网络接入。

为了避免因 NSSAI 暴露而引发的网络攻击，需要在用户接入网络过程中，保证 NSSAI 传递的安全性，因此本实施例提出了一种用户接入网络的网络接入方法，通过对 NSSAI 的加密传递，达到保护 NSSAI 的目的。

本实施例中所述的缺省 AMF，所指的是系统默认状态下的 AMF；由于本实施例中的网络接入过程中，UE 没有直接在请求时提供明文的 NSSAI 信息，因此无法直接确认 UE 所要接入的服务 AMF 来完成网络的接入过程，所以 UE 的交互对象首先是缺省 AMF，通过缺省 AMF 来为用户进行接入服务。

在 UE 与缺省 AMF 交互的过程中，缺省 AMF 的交互需要涉及到与 UE 之间的认证过程，认证过程中并不涉及到 UE 对服务 AMF 的选择，而是为了后续 UE 与缺省 AMF 之间交互 NSSAI 信息。本实施例为了提升 NSSAI 信息在传输过程中的安全性，示例性而言，NSSAI 可以为通过非对称加密方式传送、对称加密方式传送以及 NAS 安全通道传送中的至少一种发送给缺省 AMF。也就是说，NSSAI 在 UE 和缺省 AMF 之间进行传输的手段，可以包括对 NSSAI 本身进行加密，或者是在安全的 NAS 安全通道内传输两种手段。而对 NSSAI 进行加密，则可以通过非对称加密、对称加密等手段来实现。上述各加密手段之间可以单独实施，也可以组合进行，比如可通过非对称加密手段对 NSSAI 进行加密，然后再通过 NAS 安全通道进行传输；或者是通过对称加密手段对 NSSAI 进行加密，然后在通过 NAS 安全通道进行传输等等。

在一些实施例中，NSSAI 为通过非对称加密方式传送可以包括：确定在 UE 和网络侧

配置的运营商公钥和私钥；通过公钥对 NSSAI 进行加密；将加密后的 NSSAI 通过网络初始注册请求发送给缺省 AMF。其中，通过非对称加密方式传送，首先需要在 UE 侧以及网络侧配置匹配的运营商公钥和私钥；然后，UE 在发送 NSSAI 至网络侧时，则通过配置的运营商公钥，对 NSSAI 进行加密，然后发送加密的 NSSAI 至网络侧。而发送的过程可以通过网络初始注册请求，来携带加密的 NSSAI 并发送至网络侧。

相应的，认证成功后，确定对应的服务 AMF 可以包括：认证成功后，对 NSSAI 通过私钥进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。由于 NSSAI 通过运营商公钥进行了加密，为了保证其安全性，需要在 UE 和缺省 AMF 之间的认证通过后，方才通过运营商私钥对该加密的 NSSAI 进行解密，从而可得到明文 NSSAI。得到明文 NSSAI 之后，缺省 AMF 就可以根据该 NSSAI 的内容，来确定用户接入切片网络所需的服务 AMF。

在一些实施例中，NSSAI 为通过对称加密方式传送包括：认证成功后，根据根密钥和密钥材料产生密钥，通过密钥对 NSSAI 进行加密；将加密后的 NSSAI 发送给缺省 AMF。对称加密的过程可以在 UE 与缺省 AMF 认证成功之后进行；在认证成功后，根据根密钥 K 产生认证向量 $K_{NSSAIenc}$，缺省 AMF 将认证参数发送给 UE，UE 根据根密钥 K 以及认证参数产生 $K_{NSSAIenc}$。UE 使用 $K_{NSSAIenc}$ 加密 NSSAI 并发送给缺省 AMF。

相应的，认证成功后，确定对应的服务 AMF 可以包括：将密钥发送给缺省 AMF；根据密钥，对加密后的 NSSAI 进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。在认证成功后，服务 AMF 根据加密该 NSSAI 的认证向量 $K_{NSSAIenc}$ 来相应的对 NSSAI 进行解密，从而得到明文 NSSAI，然后根据该明文 NSSAI 的内容，确定对应的服务 AMF，来实现 UE 的切片网络的接入。

在一些实施例中，NSSAI 为通过 NAS 安全通道传送还可以包括：认证成功后，在 UE 和 NSSAI 之间建立 NAS 安全通道；通过 NAS 安全通道发送 NSSAI 给缺省 AMF。此时，不需要对 NSSAI 本身进行加密，而通过安全的 NAS 安全通道来发送 NSSAI，从而保证 NSSAI 的安全性，避免 NSSAI 被外界所窃取。

本实施例提供了一种网络接入装置，通过向缺省 AMF 发起网络初始注册请求，然后通过网络初始注册请求与缺省 AMF 进行接入认证；认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的 NSSAI 所确定的 AMF；基于服务 AMF 完成用户设备 UE 的网络接入。从而通过与缺省 AMF 之间的认证交互之后，再进行 NSSAI 信息的处理过程确定服务 AMF，避免了直接发送 NSSAI 可能造成的消息泄露，提升了网络接入的安全性。

第七实施例

请参考图 10，图 10 为本公开第七实施例提供的一种网络接入装置组成示意图，包括：

请求接收模块 101，设置为接收 UE 发送的网络初始注册请求；

第二认证模块 102，设置为通过网络初始注册请求与缺省 AMF 进行接入认证；

第二 AMF 确认模块 103，设置为认证成功后，根据接收到的由 UE 发送的 NSSAI 确定对应的服务 AMF；

第二网络接入模块 104，设置为通过服务 AMF 完成 UE 的网络接入。

为了避免因 NSSAI 暴露而引发的网络攻击，需要在用户接入网络过程中，保证 NSSAI 传递的安全性，因此本实施例提出了一种用户接入网络的网络接入方法，通过对 NSSAI 的加密传递，达到保护 NSSAI 的目的。

本实施例中所述的缺省 AMF，所指的是系统默认状态下的 AMF；由于本实施例中的网络接入过程中，UE 没有直接在请求时提供明文的 NSSAI 信息，因此无法直接确认 UE 所要接入的服务 AMF 来完成网络的接入过程，所以 UE 的交互对象首先是缺省 AMF，通过缺省 AMF 来为用户进行接入服务。

在 UE 与缺省 AMF 交互的过程中，缺省 AMF 的交互需要涉及到与 UE 之间的认证过程，认证过程中并不涉及到 UE 对服务 AMF 的选择，而是为了后续 UE 与缺省 AMF 之间交互 NSSAI 信息。本实施例为了提升 NSSAI 信息在传输过程中的安全性，示例性而言，缺省 AMF 可以通过非对称加密方式传送、对称加密方式传送以及 NAS 安全通道传送中的至少一种方式接收 NSSAI。也就是说，NSSAI 在 UE 和缺省 AMF 之间进行传输的手段，可以包括对 NSSAI 本身进行加密，或者是在安全的 NAS 安全通道内传输两种手段。而对 NSSAI 进行加密，则可以通过非对称加密、对称加密等手段来实现。上述各加密手段之间可以单独实施，也可以组合进行，比如可通过非对称加密手段对 NSSAI 进行加密，然后再通过 NAS 安全通道进行传输；或者是通过对称加密手段对 NSSAI 进行加密，然后在通过 NAS 安全通道进行传输等等。

在一些实施例中，NSSAI 为通过非对称加密方式传送可以包括：确定在 UE 和网络侧配置的运营商公钥和私钥；通过公钥对 NSSAI 进行加密；接收加密后的 NSSAI。其中，通过非对称加密方式传送，首先需要在 UE 侧以及网络侧配置匹配的运营商公钥和私钥；然后，UE 在发送 NSSAI 至网络侧时，则通过配置的运营商公钥，对 NSSAI 进行加密，然后发送加密的 NSSAI 至网络侧。而发送的过程可以通过网络初始注册请求，来携带加密的 NSSAI 并发送至网络侧。

相应的，认证成功后，根据接收到的由 UE 发送的 NSSAI 确定对应的服务 AMF 可以包括：认证成功后，对 NSSAI 通过私钥进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。由于 NSSAI 通过运营商公钥进行了加密，为了保证其安全性，需要在 UE 和缺省 AMF 之间的认证通过后，方才通过运营商私钥对该加密的 NSSAI 进行解密，从而可得到明文 NSSAI。得到明文 NSSAI 之后，缺省 AMF 就可以根据该 NSSAI 的内容，来确定用户接入切片网络所需的服务 AMF。

在一些实施例中，NSSAI 为通过对称加密方式传送可以包括：认证成功后，根据根密钥和密钥材料产生密钥，通过密钥对 NSSAI 进行加密；接收加密后的 NSSAI。对称加密的过程可以在 UE 与缺省 AMF 认证成功之后进行；在认证成功后，根据根密钥和密钥

材料 K 产生认证向量 $K_{NSSAIenc}$，缺省 AMF 将认证参数发送给 UE，UE 根据根密钥和密钥材料 K 以及认证参数产生 $K_{NSSAIenc}$。UE 使用 $K_{NSSAIenc}$ 加密 NSSAI 并发送给缺省 AMF。

相应的，认证成功后，确定对应的服务 AMF 可以包括：接收密钥；根据密钥，对加密后的 NSSAI 进行解密；根据解密后的 NSSAI，确定对应的服务 AMF。在认证成功后，服务 AMF 根据加密该 NSSAI 的认证向量 $K_{NSSAIenc}$ 来相应的对 NSSAI 进行解密，从而得到明文 NSSAI，然后根据该明文 NSSAI 的内容，确定对应的服务 AMF，来实现 UE 的切片网络的接入。

在一些实施例中，NSSAI 为通过 NAS 安全通道传送可以包括：认证成功后，在 UE 和 NSSAI 之间建立 NAS 安全通道；通过 NAS 安全通道接收 NSSAI。此时，不需要对 NSSAI 本身进行加密，而通过安全的 NAS 安全通道来发送 NSSAI，从而保证 NSSAI 的安全性，避免 NSSAI 被外界所窃取。

本实施例提供了一种网络接入装置，通过向缺省 AMF 发起网络初始注册请求，然后通过网络初始注册请求与缺省 AMF 进行接入认证；认证成功后，确定对应的服务 AMF；服务 AMF 为根据发送给缺省 AMF 的 NSSAI 所确定的 AMF；基于服务 AMF 完成用户设备 UE 的网络接入。从而通过与缺省 AMF 之间的认证交互之后，再进行 NSSAI 信息的处理过程确定服务 AMF，避免了直接发送 NSSAI 可能造成的消息泄露，提升了网络接入的安全性。

第八实施例

请参考图 11，图 11 为本公开第八实施例提供的一种终端组成示意图，包括第一处理器 111、第一存储器 112 和第一通信总线 113；

第一通信总线 113 设置为实现第一处理器 111 和第一存储器 112 之间的连接通信；

第一处理器 111 设置为执行第一存储器 112 中存储的计算机程序，以实现本公开上述各实施例中的网络接入方法的流程，这里不再赘述。

第九实施例

请参考图 12，图 12 为本实施例提供的一种基站组成示意图，包括第二处理器 121、第二存储器 122 和第二通信总线 123；

第二通信总线 123 设置为实现第二处理器 121 和第二存储器 122 之间的连接通信；

第二处理器 121 设置为执行第二存储器 122 中存储的计算机程序，以实现本公开上述各实施例中的网络接入方法的流程，这里不再赘述。

第十实施例

本实施例提供了一种计算机可读存储介质，该计算机可读存储介质中存储有一个或者多个计算机程序，计算机程序可被一个或者多个处理器执行，以实现前述各实施例中的网

络接入方法，这里不再赘述。

显然，本领域的技术人员应该明白，上述本公开的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储介质（ROM/RAM、磁碟、光盘）中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。所以，本公开不限制于任何特定的硬件和软件结合。

以上内容是结合具体的实施方式对本公开所作的进一步详细说明，不能认定本公开的具体实施只局限于这些说明。对于本公开所属技术领域的普通技术人员来说，在不脱离本公开构思的前提下，还可以做出若干简单推演或替换，都应当视为属于本公开的保护范围。

权利要求

1.一种网络接入方法，包括：

向缺省接入和移动性管理功能 AMF 发起网络初始注册请求；

通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

认证成功后，确定对应的服务 AMF；所述服务 AMF 为根据发送给所述缺省 AMF 的网络切片选择辅助信息 NSSAI 所确定的 AMF；

基于所述服务 AMF 完成用户设备 UE 的网络接入。

2.如权利要求 1 所述的网络接入方法，其中，所述 NSSAI 为通过非对称加密方式传送、对称加密方式传送以及 NAS 安全通道传送中的至少一种发送给所述缺省 AMF。

3.如权利要求 2 所述的网络接入方法，其中，所述 NSSAI 为通过非对称加密方式传送包括：

确定在 UE 和网络侧配置的运营商公钥和私钥；

通过所述公钥对所述 NSSAI 进行加密；

将加密后的 NSSAI 通过所述网络初始注册请求发送给缺省 AMF。

4.如权利要求 3 所述的网络接入方法，其中，所述认证成功后，确定对应的服务 AMF 包括：

认证成功后，对所述 NSSAI 通过所述私钥进行解密；

根据解密后的所述 NSSAI，确定对应的所述服务 AMF。

5.如权利要求 2 所述的网络接入方法，其中，所述 NSSAI 为通过对称加密方式传送包括：

认证成功后，根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥，通过所述密钥对 NSSAI 进行加密；

将加密后的所述 NSSAI 发送给缺省 AMF。

6.如权利要求 5 所述的网络接入方法，其中，所述认证成功后，确定对应的服务 AMF 包括：

所述缺省 AMF 根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥；

根据所述密钥，对加密后的所述 NSSAI 进行解密；

根据解密后的所述 NSSAI，确定对应的所述服务 AMF。

7.如权利要求 2 所述的网络接入方法，其中，所述 NSSAI 为通过 NAS 安全通道传送包括：

认证成功后，在 UE 和所述缺省 AMF 之间建立 NAS 安全通道；

通过所述 NAS 安全通道发送所述 NSSAI 给所述缺省 AMF。

8.如权利要求 7 所述的网络接入方法，其中，所述认证成功后，确定对应的服务 AMF 包括：

根据所述 NSSAI，确定对应的所述服务 AMF；

确定对应的所述服务 AMF 之后，拆除 UE 和所述缺省 AMF 之间的 NAS 安全通道。

9.一种网络接入方法，包括：

接收 UE 发送的网络初始注册请求；

通过所述网络初始注册请求与所述 UE 进行接入认证；

认证成功后，根据接收到的由所述 UE 发送的 NSSAI 确定对应的服务 AMF；

通过所述服务 AMF 完成 UE 的网络接入。

10.如权利要求 9 所述的网络接入方法，其中，所述 NSSAI 为通过非对称加密方式传送、对称加密方式传送以及 NAS 安全通道传送中的至少一种接收。

11.如权利要求 10 所述的网络接入方法，其中，所述 NSSAI 为通过非对称加密方式传送包括：

确定在 UE 和网络侧配置的运营商公钥和私钥；

通过所述公钥对所述 NSSAI 进行加密；

接收加密后的所述 NSSAI。

12.如权利要求 11 所述的网络接入方法，其中，所述认证成功后，根据接收到的由所述 UE 发送的 NSSAI 确定对应的服务 AMF 包括：

认证成功后，对所述 NSSAI 通过所述私钥进行解密；

根据解密后的所述 NSSAI，确定对应的所述服务 AMF。

13.如权利要求 10 所述的网络接入方法，其中，所述 NSSAI 为通过对称加密方式传送包括：

认证成功后，根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥，通过所述密钥对 NSSAI 进行加密；

接收加密后的所述 NSSAI。

14.如权利要求 13 所述的网络接入方法，其中，所述认证成功后，确定对应的服务 AMF 包括：

根据根密钥和密钥材料计算产生用于 NSSAI 加密的密钥；

根据所述密钥，对加密后的所述 NSSAI 进行解密；

根据解密后的所述 NSSAI，确定对应的所述服务 AMF。

15.如权利要求 10 所述的网络接入方法，其中，所述 NSSAI 为通过 NAS 安全通道传送包括：

认证成功后，在 UE 和所述缺省 AMF 之间建立 NAS 安全通道；

通过所述 NAS 安全通道接收所述 NSSAI。

16.一种网络接入装置，包括：

请求发起模块，设置为向 AMF 发起网络初始注册请求；

第一认证模块，设置为通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

第一 AMF 确认模块，设置为认证成功后，确定对应的服务 AMF；所述服务 AMF 为根据发送给所述缺省 AMF 的网络切片选择辅助信息 NSSAI 所确定的 AMF；

第一网络接入模块，设置为基于所述服务 AMF 完成用户设备 UE 的网络接入。

17.一种网络接入装置，其中，包括：

请求接收模块，设置为接收 UE 发送的网络初始注册请求；

第二认证模块，设置为通过所述网络初始注册请求与所述缺省 AMF 进行接入认证；

第二 AMF 确认模块，设置为认证成功后，根据接收到的由所述 UE 发送的 NSSAI 确定对应的服务 AMF；

第二网络接入模块，设置为通过所述服务 AMF 完成 UE 的网络接入。

18.一种终端，其中，包括第一处理器、第一存储器和第一通信总线；

所述第一通信总线设置为实现所述第一处理器和第一存储器之间的连接通信；

所述第一处理器设置为执行所述第一存储器中存储的计算机程序，以实现如权利要求 1-7 任一项所述网络接入方法的步骤。

19.一种基站，其中，包括第二处理器、第二存储器和第二通信总线；

所述第二通信总线设置为实现所述第二处理器和第二存储器之间的连接通信；

所述第二处理器设置为执行所述第二存储器中存储的计算机程序，以实现如权利要求 8-14 任一项所述网络接入方法的步骤。

20.一种计算机可读存储介质，其中，所述计算机可读存储介质中存储有一个或者多个计算机程序，所述计算机程序可被一个或者多个处理器执行，以实现如权利要求 1-8 任一项所述网络接入方法的步骤，或如权利要求 9-15 任一项所述的网络接入方法的步骤。

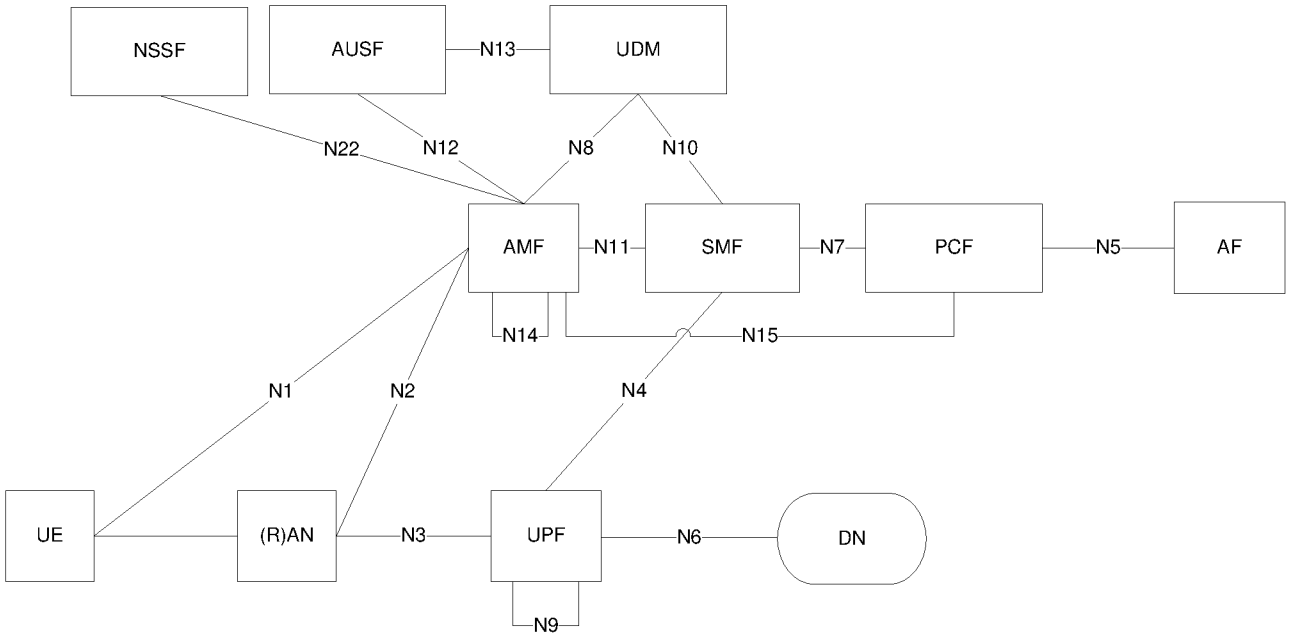
NSSF
AUSF
N13
UDM
N22
N12
N8
N10
AMF
N11
SMF
N7
PCF
N5
AF
N14
N15
N1
N2
N4
UE
(R)AN
N3
UPF
N6
DN
N9

图 1

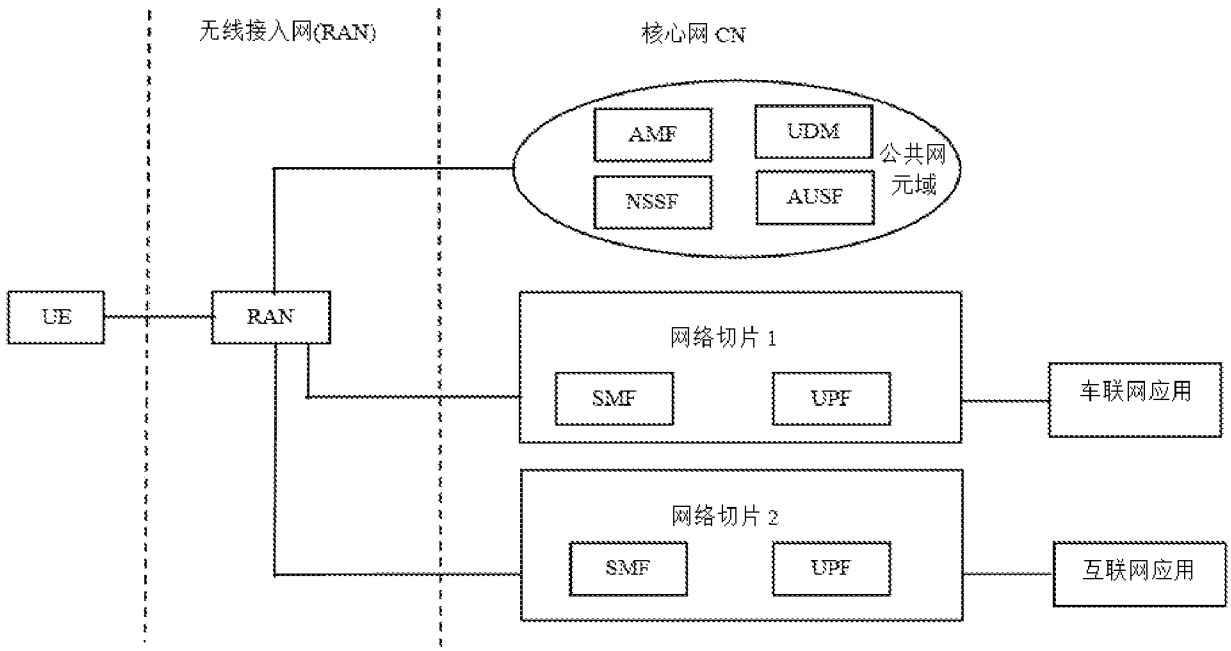
无线接入网(RAN)
核心网 CN
AMF
UDM
公共网
元域
NSSF
AUSF
UE
RAN
网络切片 1
SMF
UPF
车联网应用
网络切片 2
SMF
UPF
互联网应用

图 2

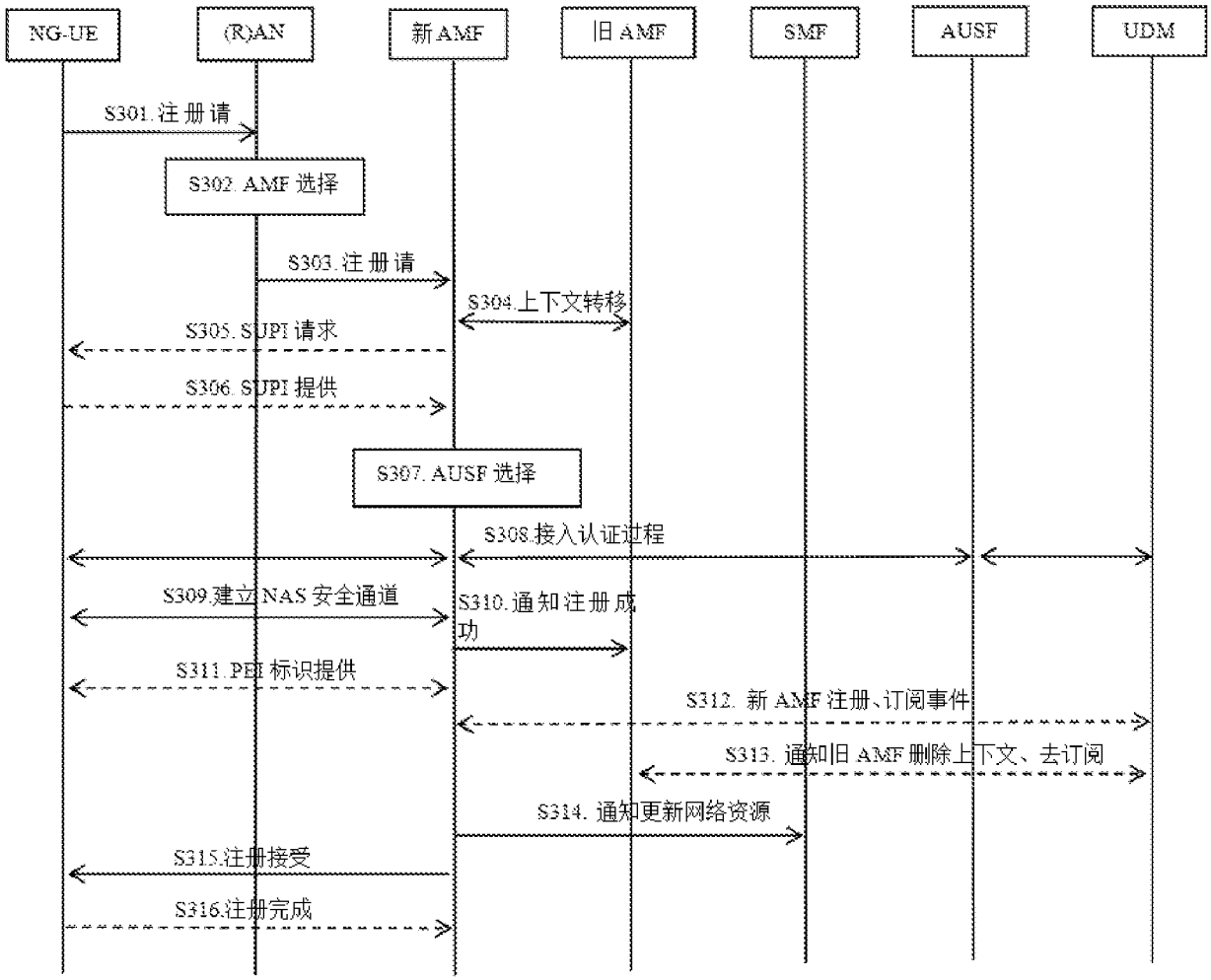
NG-UE
(R)AN
新AMF
旧AMF
SMF
AUSF
UDM
S301.注册请求
S302. AMF选择
S303.注册请求
S304.上下文转移
S305. SUPI请求
S306. SUPI提供
S307. AUSF选择
S308.接入认证进程
S309.建立NAS安全通道
S310.通知注册成功
S311. PEI标识提供
S312. 新AMF注册、订阅事件
S313. 通知旧AMF删除上下文、去订阅
S314. 通知更新网络资源
S315.注册接受
S316.注册完成

图 3

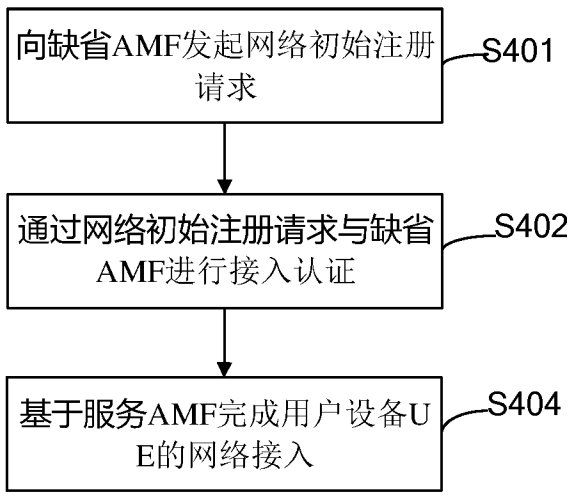
向缺省AMF发起网络初始注册请求
S401
通过网络初始注册请求与缺省AMF进行接入认证
S402
基于服务AMF完成用户设备UE的网络接入
S404

图 4

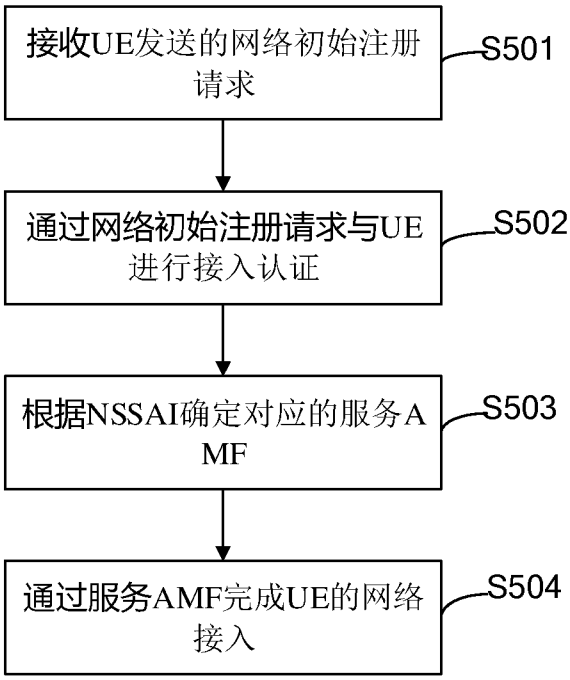
接收UE发送的网络初始注册请求
S501
通过网络初始注册请求与UE进行接入认证
S502
根据NSSAI确定对应的服务AMF
S503
通过服务AMF完成UE的网络接入
S504

图 5

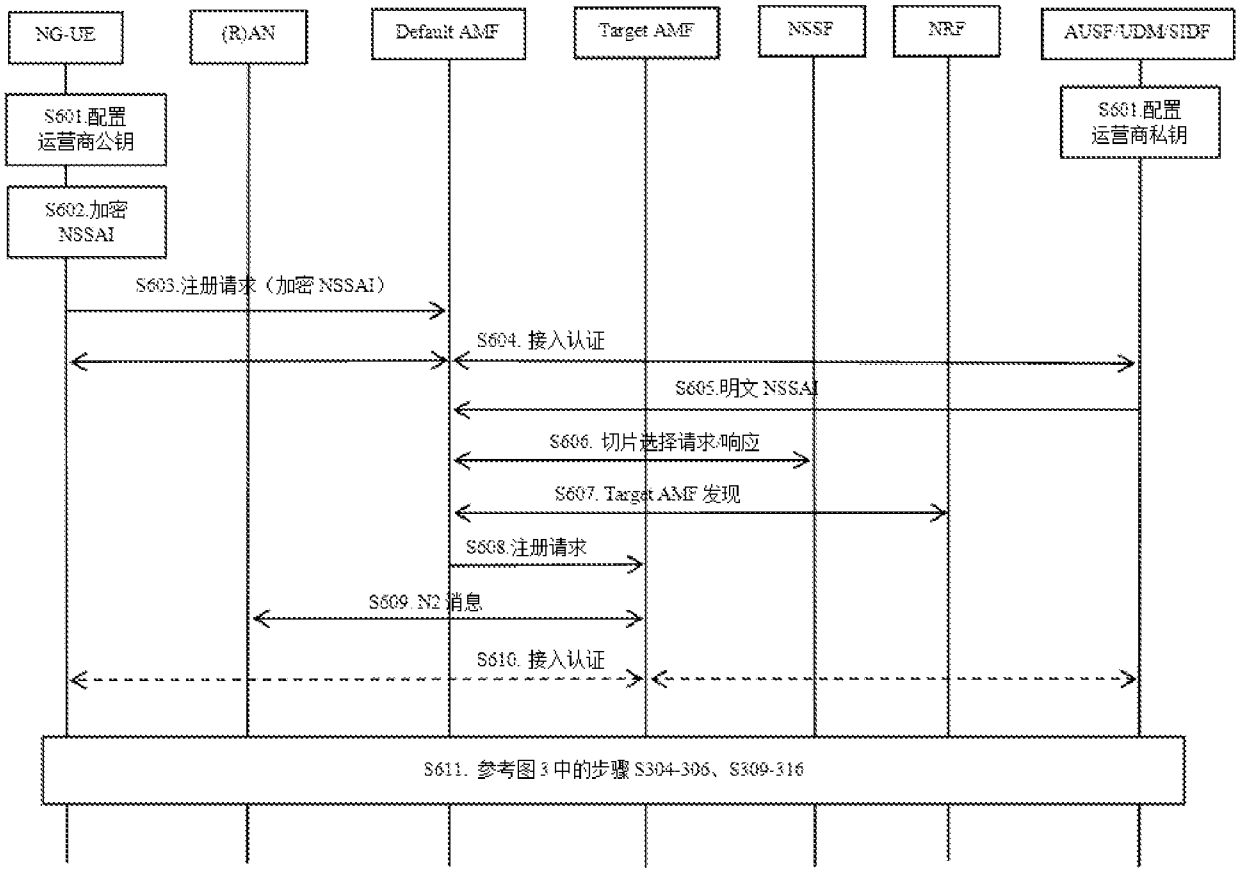
NG-UE
(R)AN
Default AMF
Target AMF
NSSF
NRF
AUSF/UDM/SIDF
S601.配置运营商公钥
S601.配置运营商私钥
S602.加密NSSAI
S603.注册请求（加密NSSAI）
S604. 接入认证
S605.明文NSSAI
S606. 切片选择请求/响应
S607. Target AMF发现
S608.注册请求
S609. N2消息
S610. 接入认证
S611. 参考图3中的步骤S304-306、S309-316

图 6

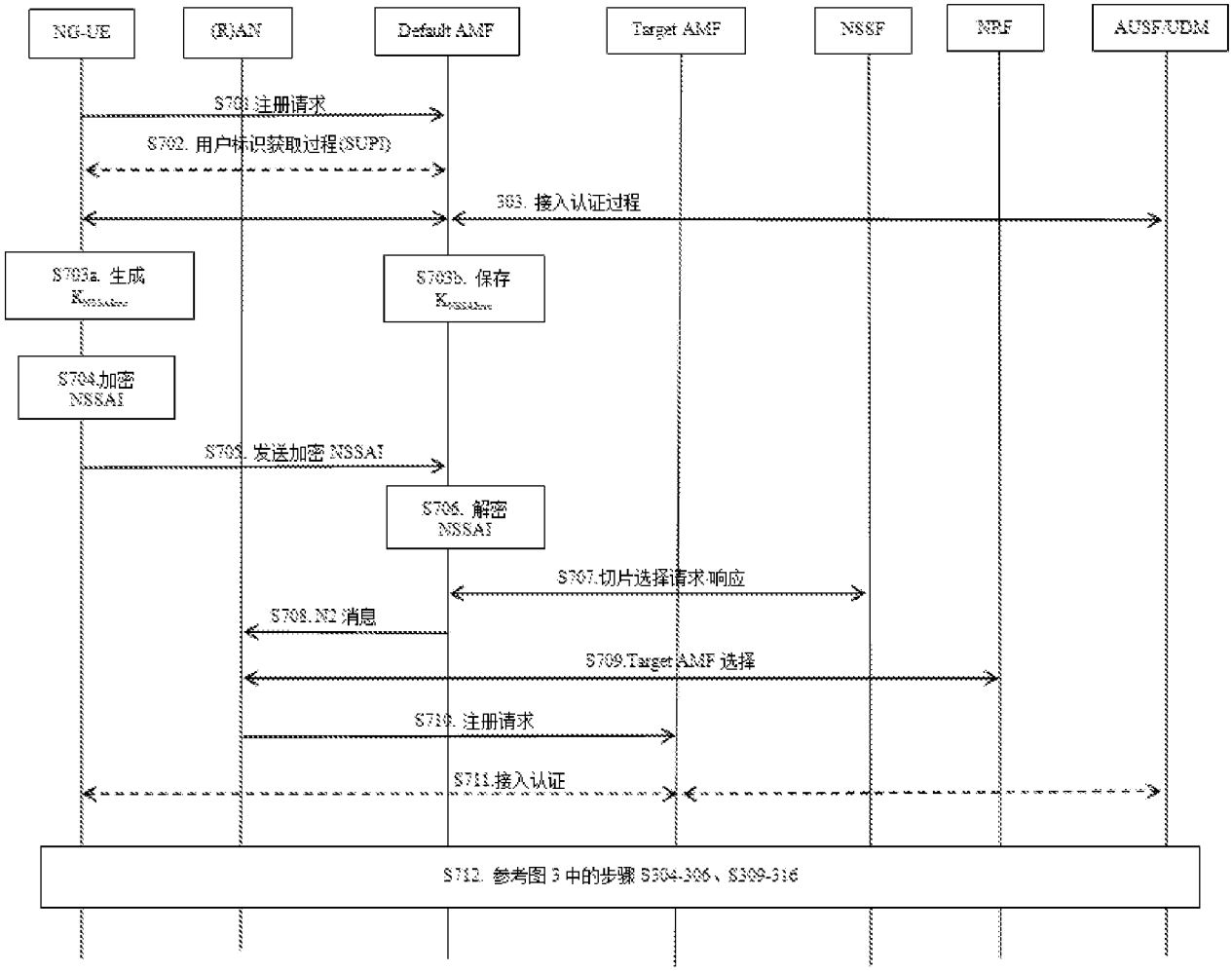
NG-UE
(R)AN
Default AMF
Target AMF
NSSF
NRF
AUSF/UDM
S701. 注册请求
S702. 用户标识获取过程(SUPI)
S703. 接入认证过程
S703a. 生成
S703b. 保存
S704.加密
NSSAI
S705. 发送加密 NSSAI
S706. 解密
NSSAI
S707.切片选择请求/响应
S708.N2 消息
S709.Target AMF 选择
S710. 注册请求
S711.接入认证
S712. 参考图 3 中的步骤 S304-306、S309-316

图 7

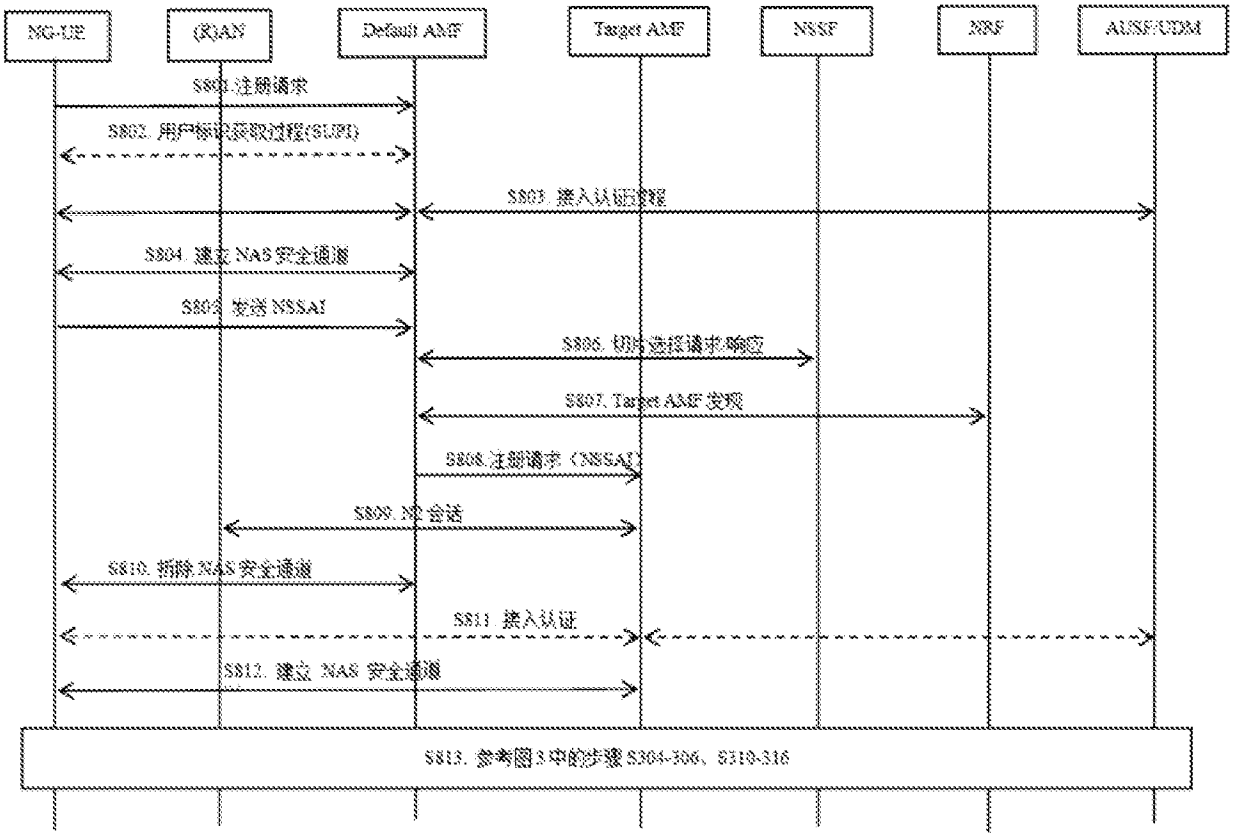
NG-UE
(R)AN
Default AMF
Target AMF
NSSF
NRF
AUSF/UDM
S801. 注册请求
S802. 用户标识获取过程(SUPI)
S803. 接入认证过程
S804. 建立 NAS 安全通道
S805. 发送 NSSAI
S806. 切片选择请求响应
S807. Target AMF 发现
S808. 注册请求（NSSAI）
S809. PDU 会话
S810. 释放 NAS 安全通道
S811. 接入认证
S812. 建立 NAS 安全通道
S813. 参考图3中的步骤 S304-306、S310-316

图 8

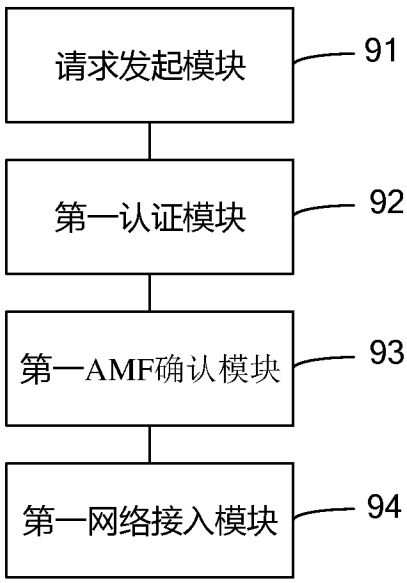
请求发起模块
91
第一认证模块
92
第一AMF确认模块
93
第一网络接入模块
94

图 9

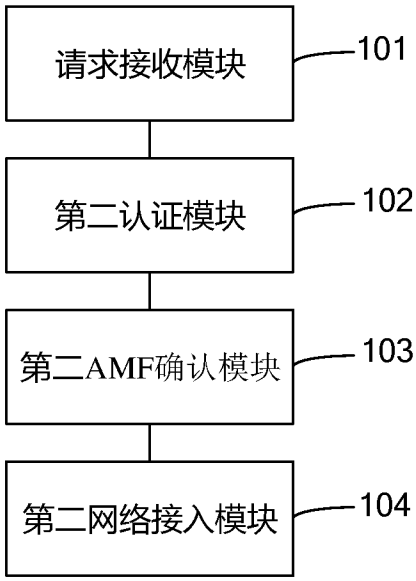
请求接收模块
101
第二认证模块
102
第二AMF确认模块
103
第二网络接入模块
104

图 10

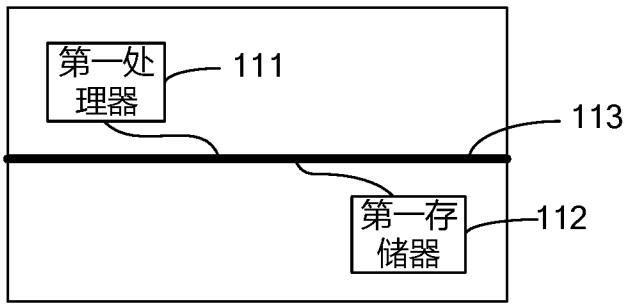
第一处理器
111
113
第一存储器
112

图 11

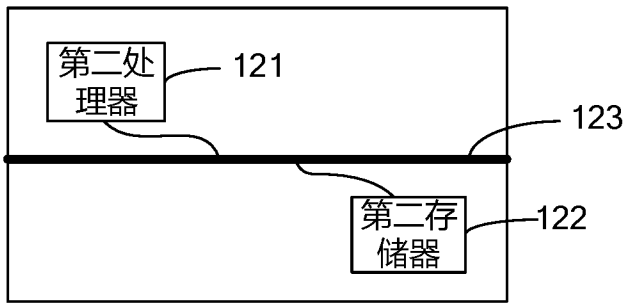
第二处理器
121
123
第二存储器
122

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/096023

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; H04Q; 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)

CNKI, CNPAT, WPI, EPODOC, 3GPP: 接入和移动性管理功能, 缺省, 默认, 注册请求, 认证, 授权, 网络切片选择辅助信息, 服务, 重定向, 新, 旧, AMF, default, registration request, authentication, authorization, NSSAI, serving, redirect, new, old

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017303259 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 19 October 2017 (2017-10-19) description, paragraphs [0122]-[0146] and [0322]-[0325], and figure 5	1, 2, 7-10, 15-20
A	CN 107580324 A (NO. 30 INSTITUTE OF CHINA ELECTRONICS TECHNOLOGY GROUP CORPORATION) 12 January 2018 (2018-01-12) entire document	1-20
A	CN 106982458 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 July 2017 (2017-07-25) entire document	1-20
A	HUAWEI et al. "TS23.502: Clarifications on Registration, PDU Session Establishment Procedures and Network Slicing" *3GPP TSG SA WG2 Meeting #119 S2-1701038*, 17 February 2017 (2017-02-17), entire document	1-20

☐ 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
18 September 2019	**26 September 2019**

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/CN2019/096023

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2017303259 A1	19 October 2017	US 2019098618 A1	28 March 2019
		KR 20170119296 A	19 October 2017
CN 107580324 A	12 January 2018	None	
CN 106982458 A	25 July 2017	WO 2018161803 A1	13 September 2018

国际检索报告

国际申请号
PCT/CN2019/096023

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; H04Q; 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））

CNKI,CNPAT,WPI,EPODOC,3GPP: 接入和移动性管理功能，缺省，默认，注册请求，认证，授权，网络切片选择辅助信息，服务，重定向，新，旧，AMF，default，registration request，authentication，authorization，NSSAI，serving，redirect，new，old

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	US 2017303259 A1 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 2017年 10月 19日 (2017-10-19) 说明书第[0122]-[0146]、[0322]-[0325]段，图5	1-2，7-10，15-20
A	CN 107580324 A (中国电子科技集团公司第三十研究所) 2018年 1月 12日 (2018-01-12) 全文	1-20
A	CN 106982458 A (华为技术有限公司) 2017年 7月 25日 (2017-07-25) 全文	1-20
A	HUAWEI等. "TS23.502: Clarifications on Registration, PDU Session Establishment Procedures and Network Slicing" 3GPP TSG SA WG2 Meeting #119 S2-1701038, 2017年 2月 17日 (2017-02-17), 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

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

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 9月 18日	2019年 9月 26日

ISA/CN的名称和邮寄地址	受权官员
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	刘丽
传真号 (86-10)62019451	电话号码 86-(10)-53961799

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/096023

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)
US	2017303259	A1	2017年 10月 19日	US	2019098618	A1	2019年 3月 28日
				KR	20170119296	A	2017年 10月 19日
CN	107580324	A	2018年 1月 12日		无		
CN	106982458	A	2017年 7月 25日	WO	2018161803	A1	2018年 9月 13日