(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
2018 年 9 月 27 日 (27.09.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/170617 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01) *H04W 8/26* (2009.01)

(21) 国际申请号: PCT/CN2017/077162

(22) 国际申请日: 2017 年 3 月 18 日 (18.03.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

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

(72) 发明人: 李赫(LI, He); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈璟(CHEN, Jing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李欢(LI, Huan); 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: 广 州 三 环 专 利 商 标 代 理 有 限 公 司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, 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,

(54) **Title:** NETWORK ACCESS AUTHENTICATION METHOD BASED ON NON-3GPP NETWORK, AND RELATED DEVICE AND SYSTEM

(54) 发明名称: 一种基于非3GPP网络的入网认证方法、相关设备及系统

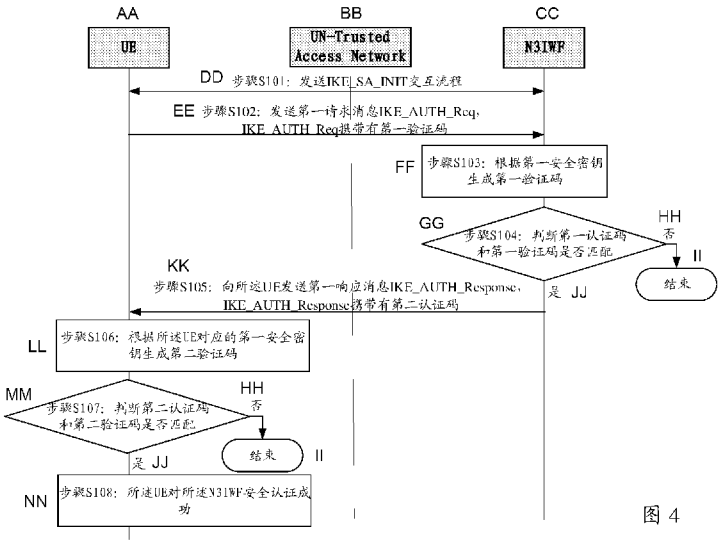


图 4

AA UE
BB UN-Trusted Access Network
CC N3IWF
DD Step S101: Send an IKE_SA_INIT interaction process
EE Step S102: Send a first request message IKE_AUTH_Req, the IKE_AUTH_Req carrying a first verification code
FF Step S103: Generate the first verification code according to a first security key
GG Step S104: Determine whether a first authentication code matches the first verification code
HH No
II End
JJ Yes
KK Step S105: Send a first response message IKE_AUTH_Response to UE, the IKE_AUTH_Response carrying a second authentication code
LL Step S106: Generate a second verification code according to the first security key corresponding to the UE
MM Step S107: Determine whether the second authentication code matches the second verification code
NN Step S108: Security authentication of the UE on an N3IWF is successful

(57) **Abstract:** Embodiments of the present invention disclose a network access authentication method based on a non-3GPP network, and a related device and system. The method comprises: a UE sending a first request message to an N3IWF, the first request message carrying a first authentication code, AMF indication information, and key identifier information, the first authentication code being used by the N3IWF to perform security authentication on the UE, and the key identifier information being used to acquire a first security key; receiving a first response message returned by the N3IWF on the basis of the first request message, the first response carrying a second authentication code, and the first response message being used to indicate that security authentication of the N3IWF on the UE is successful; and the UE performing integrity verification on the second authentication code, mutual security authentication between the UE and the N3IWF being realized after verification is successful. By adopting the present invention, once UE has successfully accessed a network, the UE can quickly re-access the network according to a non-3GPP protocol.

WO 2018/170617 A1

[见续页]

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

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本发明实施例公开了一种基于非3GPP网络的入网认证方法、相关设备及系统，所述方法包括：UE向N3IWF发送第一请求消息，所述第一请求消息携带有第一认证码、AMF指示信息和密钥标识信息，所述第一认证码用于所述N3IWF对所述UE进行安全认证，所述密钥标识信息用于获取所述第一安全密钥；接收所述N3IWF基于所述第一请求消息返回的第一响应消息，所述第一响应携带有第二认证码所述第一响应消息用于指示所述N3IWF对所述UE安全认证成功；然后UE对第二认证码进行完整性验证，验证成功后UE和N3IWF即可实现相互安全认证。采用本发明，能够在UE上一次成功入网后，实现UE通过non-3GPP的快速入网。

一种基于非 3GPP 网络的入网认证方法、相关设备及系统

技术领域

本发明涉及 5G 通信技术领域，尤其涉及一种基于非 3GPP 网络的入网认证方法、相关设备及系统。

背景技术

随着通信技术的不断发展，第三代合作伙伴计划 3GPP（3rd Generation Partnership Project，3GPP）和非 3GPP（non-3GPP）已经大规模部署和使用，特别是 non-3GPP，如 wifi 的使用，给用户带来更便利的通信服务和业务体验。同时随着用户设备（User equipmen，UE），如手机、平板等的大规模增加，给通信注入新的活力，也给运营带了挑战。特别是用户设备 UE 的入网认证过程中，现有技术中参见图 3 给出的 5G 网络框架示意图；UE 每次通过 non-3GPP 接入网络时，都需要通过 Untrusted non-3GPP access network and allocated IP address （可信的非 3GPP 接入网）接入核心网。入网鉴权流程中，信令控制面涉及到 UE 分别与非 3GPP 互通网元（non-3GPP Interworking Function，N3IWF）、接入和移动性管理网元（Access and Mobility Management Function，AMF）以及鉴权服务器（Authentication Server Function，AUSF）之间的相互认证鉴权过程。整个入网鉴权过程繁琐，且在鉴权过程中需要消耗比较长的鉴权等待时间。因此，针对 UE 上一次已经成功入网的情况，UE 再次通过 3GPP /non-3GPP 入网时，均需要再次重复进行 UE 和 3GPP/non-3GPP 网络侧之前的入网鉴权流程，消耗的鉴权时间较长，用户体验较差。

发明内容

本发明实施例公开了一种基于非 3GPP 网络的入网认证方法、相关设备及系统，可利用 UE 上次入网成功后存储的安全上下文信息来完成当前通过非 3GPP 的入网认证，减少现有技术中通过非 3GPP 进行入网认证的流程步骤，实现 UE 的快速入网。

第一方面，本发明实施例提供了一种基于非 3GPP 网络的入网认证方法，包括：

用户设备 UE 获取上一次成功入网后，所述 UE 的保留信息；

根据所述 UE 的保留信息，确定接入和移动性管理网元 AMF 指示信息和第一安全密钥；

根据所述第一安全密钥生成第一认证码；

向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥；

接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息。

本申请方案中用户设备 UE 获取上一次成功入网后所述 UE 的保留信息，根据所述 UE 的保留信息，确定接入和移动性管理网元 AMF 指示信息和第一安全密钥，然后根据所述第一安全密钥生成第一认证码，并向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥，

然后接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息；这样 UE 可利用上次入网成功后其内存储的安全上下文信息来完成当前通过非 3GPP 的再次入网认证，减少现有技术中通过非 3GPP 进行入网认证的流程步骤，实现 UE 的快速入网。

在一些可选的方案中，所述第一响应消息携带有第二认证码，所述第二认证码为所述 N3IWF 根据所述第一安全密钥生成的；所述方法还包括：

根据所述第一安全密钥生成第二验证码；

如果所述第二验证码与所述第二认证码匹配，则所述 UE 对所述 N3IWF 安全认证成功。

通过执行上述步骤，用户设备基于第二验证码的完整性验证，来完成 UE 对所述 N3IWF 的安全认证；也即是验证 N3IWF 是否为真的；这样帮助 UE 通过 non-3GPP 快速入网。

在一些可选的方案中，所述 UE 对所述 N3IWF 安全认证成功之后，还包括：

向所述 N3IWF 发送第四请求消息，所述第四请求消息承载在因特网安全 IPsec 协议，所述第四请求消息携带有第三认证码和所述密钥标识信息，所述第三认证码用于所述 AMF 指示信息所指示的第一 AMF 对所述 UE 进行安全认证；

接收所述 N3IWF 发送的第四响应消息，所述第四响应消息承载在因特网安全 IPsec 协议，所述第四响应消息用于指示所述 UE 注册成功。

通过执行上述步骤，用户设备将第四请求消息承载在 IPsec 协议发送给 N3IWF，以实现网络侧第一 AMF 对 UE 的安全认证。

在一些可选的方案中，所述第一请求消息还携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证。

在一些可选的方案中，所述方法还包括：

根据所述 UE 的保留信息，确定 NAS 完整性密钥；

根据所述 NAS 完整性密钥生成第三认证码，其中所述密钥标识信息还用于获取所述 NAS 完整性密钥。

通过执行上述步骤，用户设备从 UE 的保留信息中获取 NAS 完整性密钥，然后再利用 NAS 完整性密钥生成第三认证码，以便第一 AMF 根据密钥标识信息获取所述 NAS 完整性密钥，并基于对第三认证码的验证来完成第一 AMF 对 UE 的安全认证，进而实现 UE 的快速安全入网。

第二方面，本发明实施例提供了一种基于非 3GPP 网络的入网认证方法，包括：

N3IWF 接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息；

向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标识信息对应的所述第一安全密钥；

根据所述第一安全密钥生成第一验证码；

如果所述第一认证码和所述第一验证码匹配，则向所述 UE 发送第一响应消息。

本申请方案中 N3IWF 接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息，向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标识信息对应的所述第一安全密钥，根据所述第一安全密钥生成第一验证码，如果所述第一认证码和所述第一验证码匹配，则向所述 UE 发送第

一响应消息;这样 N3IWF 基于对第一认证码的完整性验证实现 N3IWF 对 UE 的安全认证，能够减少现有技术中通过非 3GPP 进行入网认证的流程步骤，实现 UE 的快速入网。

在一些可选的方案中，所述方法还包括:

根据所述第一安全密钥生成第二认证码;

将所述第二认证码发送给所述 UE，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。

通过执行上述步骤，N3IWF 利用接收的第一安全密钥生成第二认证码，并发送给 UE，以实现 UE 对 N3IWF 的安全认证。

在一些可选的方案中，所述向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体包括: 根据所述 AMF 指示信息，查找第一 AMF; 向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息; 所述接收所述密钥标识信息对应的所述第一安全密钥具体包括: 接收所述第一 AMF 发送的所述第一安全密钥。

通过执行上述步骤，N3IWF 直接向所述 AMF 指示信息所指示的第一 AMF 发送第二请求消息，以获取第一安全密钥，完成第一认证码的验证并生成第二认证码，以实现 UE 和 N3IWF 的相互认证。

在一些可选的方案中，所述向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体包括:

在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥;

所述接收所述密钥标识信息对应的所述第一安全密钥具体包括:

接收所述第二 AMF 发送的所述第一安全密钥; 所述第一安全密钥为所述第一 AMF 根据所述密钥标识信息确定的，或者所述第一安全密钥为所述第二 AMF 根据接收所述第一 AMF 发送的第一安全密钥信息生成的，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数。

通过执行上述步骤，N3IWF 无法找到所述 AMF 指示信息所指示的第一 AMF，通过向第二 AMF 发送第三请求消息，以使第二 AMF 向第一 AMF 发送第二请求消息，来获取第一安全密钥，完成第一认证码的验证、以及生成第二认证码，最终实现 UE 和 N3IWF 的相互认证。

在一些可选的方案中，所述向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体包括:

在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥; 还包括:

接收所述第一 AMF 通过所述第二 AMF 发送的重定向指示信息，所述重定向指示信息携带有所述第一 AMF 的地址信息，所述重定向指示信息用于指示所述 N3IWF 重新向所述

第一 AMF 发送第二请求消息;

根据所述重定向指示信息，向所述地址信息对应的第一 AMF 发送所述第二请求消息;

所述接收所述密钥标识信息对应的所述第一安全密钥具体包括:

接收所述第一 AMF 发送的所述第一安全密钥。

通过执行上述步骤，N3IWF 无法找到所述 AMF 指示信息所指示的第一 AMF，通过向第二 AMF 发送第三请求消息，以使第二 AMF 向第一 AMF 发送第二请求消息。在第一 AMF 接收到第二请求消息后，通过第二 AMF 向第一 AMF 发送重定向指示信息，以便 N3IWF 与第一 AMF 直接建立通信连接，从第一 AMF 中获取第一安全密钥，以实现 UE 和 N3IWF 的相互认证。

在一些可选的方案中，所述向所述 UE 发送第一响应消息之后，还包括:

接收所述 UE 发送的第四请求消息，该第四请求消息承载在因特网安全 IPsec 协议，所述第四请求消息携带有第三认证码和所述密钥标识信息，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证;

向所述第一 AMF 发送所述第四请求消息，并接收所述第一 AMF 基于所述第四请求消息返回的第四响应消息，该第四请求消息和该第四响应消息承载在 NG2 协议上;

向所述 UE 发送所述第四响应消息，该第四请求消息承载在因特网安全 IPsec 协议，所述第四响应消息用于指示所述 UE 注册成功。

通过执行上述步骤，N3IWF 接收 UE 承载在 IPsec 协议上的第四请求消息，并从中抽取出第四请求消息，再将第四请求消息承载在 NG2 协议上发送给第一 AMF，以完整第一 AMF 对 UE 的安全认证。同理，在第一 AMF 向 UE 发送第四响应消息时同样需要先承载在 IPsec 协议上传给 N3IWF，在承载在 NG2 协议最终发送给 UE，以实现第一 AMF 对 UE 的安全认证。

在一些可选的方案中，所述第一请求消息携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证，则所述方法还包括: 所述 N3IWF 向第一 AMF 发送第三认证码。

第三方面，本发明实施例提供了一种基于非 3GPP 网络的入网认证方法，包括:

第一 AMF 接收 N3IWF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息;

根据所述密钥标识信息，确定第一安全密钥;

向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。

本申请方案中第一 AMF 接收 N3IWF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息，然后根据所述密钥标识信息，确定第一安全密钥，最后向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥; 这样第一 AMF 基于 N3IWF 发送的密钥标识信息来确定出第一安全密钥，并将其发送给 N3IWF，以帮助 N3IWF 完成对 UE 的安全认证，实现 UE 快速入网。

在一些可选的方案中，所述第一 AMF 接收 N3IWF 发送的第二请求消息具体包括:

接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二 AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的;

所述向所述 N3IWF 发送第二响应消息具体包括:

向所述第二 AMF 发送的第三响应消息，以使所述第二 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息和所述第三响应消息分别携带有所述第一安全密钥。

通过执行上述步骤，在 N3IWF 无法查找到与 AMF 指示信息对应的第一 AMF 的情况下，第一 AMF 接收第二 AMF 发送的用于获取第一安全密钥的第二请求消息。在确定到第一安全密钥后，同样通过第二 AMF 将查找的第一安全密钥发送给 N3IWF，以帮助 N3IWF 完成对 UE 的安全认证，实现 UE 快速入网。

在一些可选的方案中，所述第一 AMF 接收 N3IWF 发送的第二请求消息具体包括:

接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二 AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的;

向所述 N3IWF 发送第二响应消息之前，还包括:

通过所述第二 AMF 向所述 N3IWF 发送重定向指示信息，所述重定向指示信息用于指示所述 N3IWF 向所述第一 AMF 发送所述第二请求消息;

接收所述 N3IWF 基于所述重定向指示信息发送的所述第二请求消息。

通过执行上述步骤，在 N3IWF 无法查找到与 AMF 指示信息对应的第一 AMF 的情况下，第一 AMF 接收到第二 AMF 发送的用于获取第一安全密钥的第二请求消息时，可以通过第二AMF向第一AMF发送重定向指示信息,以建立第一AMF与N3IWF直接通信连接，避免第一 AMF 与 N3IWF 再次进行消息传输时，需要经过第二 AMF，节省 UE 入网时间，实现 UE 的快速入网。

在一些可选的方案中，所述向所述 N3IWF 发送第二响应消息之后，还包括:

接收所述 N3IWF 发送的第四请求消息，所述第四请求消息携带有第三认证码和密钥标识信息，所述第三认证码用于所述第一 AMF 对所述 UE 进行安全认证;

根据所述密钥标识信息，确定 NAS 完整性密钥;

根据所述 NAS 完整性密钥生成第三验证码;

如果所述第三验证码和所述第三认证码匹配，则向所述 N3IWF 发送第四响应消息，所述第四响应消息用于指示所述 UE 注册成功。

通过执行上述步骤，第一 AMF 接收 UE 经过 N3IWF 发送来的第四请求消息，第四请求消息携带有第三认证码，基于第三认证码的验证来实现第一 AMF 对 UE 的安全认证，实现 UE 安全快速入网。

在一些可选的方案中，所述第二请求消息还携带有第三认证码；所述根据所述密钥标识信息，确定第一安全密钥之前，还包括:

根据所述密钥标识信息，确定 NAS 完整性密钥;

根据所述 NAS 完整性密钥生成第三验证码;

如果所述第三验证码和所述第三认证码匹配，则执行所述根据所述密钥标识信息，确定第一安全密钥的步骤。

通过执行上述步骤，如果第一 AMF 接收的第二请求消息中携带有第三认证码时，第一 AMF 会对第三认证码进行验证来实现第一 AMF 对 UE 的安全认证，减少入网认证流程的步骤，实现 UE 的安全快速入网。

第四方面，本发明实施例提供了一种基于非 3GPP 网络的入网认证方法，包括:

第一 AMF 接收第二 AMF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息；

根据所述密钥标识信息，确定用于派生第一安全密钥的派生参数；

向所述第二 AMF 发送第三响应消息，所述第三响应消息携带有所述用于派生第一安全密钥的派生参数，以使所述第二 AMF 根据接收的所述派生参数生成所述第一安全密钥。

本申请方案中第一 AMF 接收第二 AMF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息，根据所述密钥标识信息，确定用于派生第一安全密钥的派生参数，向所述第二 AMF 发送第三响应消息，所述第三响应消息携带有所述用于派生第一安全密钥的派生参数，以便第二 AMF 根据派生参数生成第一安全密钥，帮助 UE 和 N3IWF 之间完成相互安全认证，实现 UE 的安全快速入网。

第五方面，本发明实施例提供了一种基于非 3GPP 网络的入网认证方法，包括：

第二 AMF 接收 N3IWF 发送的第三请求消息，所述第三消息携带有 UE 临时标识和密钥标识信息，所述密钥标识信息用于获取第一安全密钥；

向所述 UE 临时标识对应的第一 AMF 发送第二请求消息，所述第二请求消息携带有所述 UE 临时标识和所述密钥标识信息；

接收所述第一 AMF 发送的第三响应消息，所述第三响应消息携带有用于派生第一安全密钥的派生参数；

根据所述派生参数生成第一安全密钥；

向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥，所述第一安全密钥用于所述 N3IWF 对所述 UE 进行安全认证。

本申请方案中第二 AMF 接收到 N3IWF 发送的第三请求消息后，向所述 UE 临时标识对应的第一 AMF 发送第二请求消息，所述第二请求消息和第三请求消息中携带有 UE 临时标识和密钥标识信息，接收所述第一 AMF 发送的第三响应消息，所述第三响应消息携带有用于派生第一安全密钥的派生参数，根据所述派生参数生成第一安全密钥，向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥，所述第一安全密钥用于所述 N3IWF 对所述 UE 进行安全认证；这样第二 AMF 根据派生参数生成第一安全密钥，帮助 UE 和 N3IWF 之间完成相互安全认证，实现 UE 的安全快速入网。

在一些可选的方案中，所述第二请求消息和所述第三请求消息还分别携带有第三认证码，所述第三认证码用于所述第一 AMF 对所述 UE 进行安全认证。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述第一安全密钥为所述 UE 的安全上下文信息中的 NAS 完整性密钥。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述第一安全密钥为根据所述 UE 的安全上下文信中的安全密钥和第一新鲜保护参数派生的密钥。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥，所述第一新鲜保护参数包括以下中的任意一项：计数器的计数值、第一随机数、UE 临时标识。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述 AMF 指示信息用于指示与所述 UE 进行相互安全认证的第一 AMF，所述 AMF 指示信息包括 UE

临时标识，或者根据 UE 临时标识生成的网络接入标识 NAI 信息。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述密钥标识信息包括 UE 临时标识，和/或，所述 UE 的安全上下文信息中的密钥标识符。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述第三认证码为根据所述 UE 的安全上下文信息中的 NAS 完整性密钥（即是所述 NAS 完整性密钥）和第二新鲜保护参数生成的。

结合第一方面至第五方面中任一方面所述实施例中，在一些可选的方案中，所述第二新鲜保护参数包括以下中的任一项：计数器的计数值、第二随机数。

第六方面，本发明提供一种用户设备，所述用户设备包括用于执行上述第一方面的方法的功能单元。

第七方面，本发明提供一种非 3GPP 互通网元，所述非 3GPP 互通网元包括用于执行上述第二方面的方法的功能单元。

第八方面，本发明提供一种接入和移动性管理网元，所述接入和移动性管理网元包括用于执行上述第三方面至第五方面中任意一方面的方法的功能单元。

第九方面，本发明提供一种用户设备，包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行上述第一方面描述的方法。

第十方面，本发明提供一种非 3GPP 互通网元，包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行上述第二方面描述的方法。

第十一方面，本发明提供一种接入和移动性管理网元，包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行上述第三方面或第四方面或第五方面描述的方法。

第十二方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储了用于基于非 3GPP 网络的入网认证的程序代码。所述程序代码包括用于执行上述第一方面描述的方法的指令。

第十三方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储了用于基于非 3GPP 网络的入网认证的程序代码。所述程序代码包括用于执行上述第二方面描述的方法的指令。

第十四方面，提供了一种计算机可读存储介质，所述计算机可读存储介质存储了用于基于非 3GPP 网络的入网认证的程序代码。所述程序代码包括用于执行上述第三方面至第五方面中任一方面描述的方法的指令。

第十五方面，提供了一种计算机程序产品，该计算机程序产品包括程序指令，当该计算机程序产品被用户设备执行时，该用户设备执行上述第一方面描述的方法。该计算机程序产品可以为一个软件安装包，在需要使用上述第一方面描述的方法的情况下，可以下载该计算机程序产品并在用户设备上执行该计算机程序产品。

第十六方面，提供了一种计算机程序产品，该计算机程序产品包括程序指令，当该计

算机程序产品被非 3GPP 互通网元 N3IWF 执行时，该 N3IWF 执行上述第一方面描述的方法。该计算机程序产品可以为一个软件安装包，在需要使用上述第二方面描述的方法的情况下，可以下载该计算机程序产品并在非 3GPP 互通网元 N3IWF 上执行该计算机程序产品。

第十七方面，提供了一种计算机程序产品，该计算机程序产品包括程序指令，当该计算机程序产品被接入和移动性管理网元 AMF 执行时，该 AMF 执行上述第三方面至第五方面中任一方面所描述的方法。该计算机程序产品可以为一个软件安装包，在需要使用上述第三方面至第五方面中任一方面所描述的方法的情况下，可以下载该计算机程序产品并在接入和移动性管理网元 AMF 上执行该计算机程序产品。

通过实施本发明实施例，能够减少现有技术中 UE 上一次成功入网后当前通过 non-3GPP 进行入网认证的流程步骤，节省入网认证时间，实现 UE 的快速入网。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍。

图 1 是本发明实施例提供的一种 LTE 的 3GPP 网络框架示意图；

图 2 是本发明实施例提供的一种 LTE 的 non-3GPP 网络框架示意图；

图 3 是本发明实施例提供的一种 5G 网络框架示意图；

图 4-图 9 是本发明实施例提供的几种基于非 3GPP 网络的入网认证方法的流程示意图；

图 10-图 11 是本发明实施例提供的两种第一接入和移动性管理网元（第一 AMF）对 UE 进行安全认证方法的流程示意图；

图 12-14 是本发明实施例提供的几种用户设备 UE 的结构示意图；

图 15-17 是本发明实施例提供的几种非 3GPP 互通网元 N3IWF 的结构示意图；

图 18-20 是本发明实施例提供的几种接入和移动性管理网元 AMF 的结构示意图；

图 21 是本发明实施例提供的一种基于非 3GPP 网络的入网认证系统的结构示意图。

具体实施方式

下面将结合本发明的附图，对本发明实施例中的技术方案进行详细描述。

请参见图 1，图 1 是本发明实施例提供的一种 LTE 的 3GPP 网络框架示意图。该网络框架示意图包括用户设备 UE（User Equipment，UE）、UMTS 陆地无线接入网（UMTS Terrestrial Radio Access Network，E-UTRAN）、移动管理实体 MME（Mobility Management Entity，MME）、归属签约用户服务器 HSS（Home Subscriber Server，HSS）、服务网关 SGW（Serving Gateway）、分组数据网络网关 PDN-GW（Packet Data Network Gateway）、策略控制和计费规则功能 PCRF（Policy and Charging Rules Function，PCRF）和运营商提供的 IP 业务，图示为 Operator's IP Service。

应理解的是，E-UTRAN 是 LTE 中的空口接入部分，通常也称为演进的 NodeB（Evolved NodeB，eNodeB），为用户设备 UE 的接入提供无线资源。移动管理实体 MME 处于核心网，负责安全、移动性管理和会话管理，功能包括核心网的承载控制，对服务网关 SGW 和分

组数据网络网关 PDN-GW 选择，鉴权等。服务网关 SGW 负责 UE 用户平面数据的传送、转发和路由切换等。分组数据网络网关 PDN-GW 主要负责与 PDN 网络进行连接、为用户分配 IP 地址等。归属签约用户服务器 HSS 负责存储用户的签约信息和鉴权数据等。策略控制和计费规则功能 PCRF 实体负责跟进用户的签约信息、网际协议能力接入网络（IP Capability Access Network，IP-CAN）类型、IP-CAN 能力等信息产生用于承载建立的策略和计费规则信息。

基于图 1 所示的 3GPP 网络框架示意图，UE 通过 3GPP 连接网络，其入网认证流程为 UE—>E-UTRAN—>MME—>HSS。UE 会发送附着请求给 MME，MME 会向 HSS 请求用户的鉴权向量集，之后 UE 和 MME 之间进行基于 LTE 的鉴权和密钥协商 EPS-AKA（Evolved packet system - authentication and key agreement，EPS-AKA）认证，最后完成 UE 和 3GPP 网络侧之间的安全认证，实现 UE 接入 3GPP 网络。

请参见图 2，图 2 是本发明实施例提供的一种 LTE 的 non-3GPP 网络框架示意图。该网络框架示意图包括用户设备 UE（User Equipment，UE）、可信的非 3GPP IP 接入网（Untrusted non-3GPP IP Access）、演进的分组数据网络网关（Evolved PDN Gateway，ePDG）、3GPP 认证授权计费（3GPP Authentication Authorization Accounting server，3GPP AAA）服务器、归属签约用户服务器 HSS（Home Subscriber Server，HSS）、服务网关 SGW（Serving Gateway）、分组数据网络网关 PDN-GW（Packet Data Network Gateway）。

应理解的是，演进的分组数据网络网关 ePDG 具有 3GPP TS 23.234 中定义 PDN-GW 功能的实体，对 PDN-GW 功能的具体修改或拓展等功能。可信的非 3GPP IP 接入网 Untrusted non-3GPP IP Access，如无线局域网 WLAN（Wireless Local Area Network，WLAN），为 UE 的接入提供无线资源。3GPP AAA 服务器负责对 UE 进行认证授权。关于归属签约用户服务器 HSS、服务网关 SGW、分组数据网络网关 PDN-GW、策略控制和计费规则功能 PCRF 的相关说明，具体请参见图 1 实施例的相关阐述，这里不再赘述。

应理解的是，PDN-GW 支持通过 S2a 或 S2b 接口实现 non-3GPP（非 3GPP）的接入。其中 S2a 允许基于代理移动 IP（Proxy Mobile Internet Protocol，PMIP）协议和移动 IPV4 协议（Mobile IPV4，MIPV4）来通过 trusted non-3GPP（可信非 3GPP）接入，S2b 允许基于代理移动 IPv6（Proxy Mobile IPv6，PMIPv6）协议来通过 Untrusted non-3GPP（不可信非 3GPP）接入。

应理解的是，non-3GPP 网络可以包括 Wi-Fi（Wireless Fidelity，中文：无线保真）、WiMAX（Worldwide Interoperability for Microwave Access，中文：全球微波互联接入）等不属于 3GPP 制定规范的网络。

同理，基于图 2 所示 non-3GPP 网络框架图，UE 通过 non-3GPP 入网过程中，入网认证流程为：UE—>ePDG—>3GPP AAA 服务器—>HSS。UE 会和 ePDG 建立安全隧道，ePDG 会主动发起可扩展鉴权协议（Extensible Authentication Protocol，EAP）鉴权，3GPP AAA 服务器作为 EAP 服务器参与 EAP 鉴权流程，鉴权结束后即可完成 UE 和 3GPP 网络侧之间的安全认证，实现 UE 接入 3GPP 网络。

基于图 1 和图 2 所示的网络框架图可知，UE 通过 LTE 的 3GPP 和通过 LTE 的 non-3GPP 入网，其入网认证流程所使用的信令控制面网元没有完全相同，也没有完全不同；其各自入网流程并没有关联性。也即是，UE 无法利用 3GPP 接入的便利性为非 3GPP 的接入做准备。

为解决上述 LTE 的 3GPP 和 LTE 的 non-3GPP 入网没有关联性的问题，请参见图 3，图 3 是本发明实施例提供的一种 5G 网络框架示意图。该网络框架示意图包括用户设备 UE（User Equipment，UE）、接入网网元（Radio Access network，R-AN），图示为（R）AN、非 3GPP 接入方式（Non-3GPP）、非 3GPP 互通网元（non-3GPP Interworking Function，N3IWF）、接入和移动性管理网元（Access and Mobility Management Function，AMF）、会话管理网元（Session Management Function，SMF）、用户面功能网元（User Plane Function，UPF）和专用网络网元（Dedicated Network，DN）等网元。

应理解的是，（R）AN 是指 3GPP 网元，例如 LTE 中的 eNB，UMTS 中的 NB。Non-3GPP 接入技术是指 3GPP 以外的接入技术，如 wifi。N3IWF 类似于 LTE 中的 ePDG，在 5G 中用于 UE 通过非 3GPP 技术接入的时候，和 UE 建立 IPsec 隧道的网元。在未来 5G 定义中，其名字可能会更改。

接入和移动性管理网元 AMF 负责 UE 的接入管理和移动性管理，在实际应用中相当于 LTE 网络框架中移动管理实体 MME 里的移动性管理 MM，并加入了接入管理。

应理解的是，接入和移动性管理网元 AMF 中还可能合并有安全锚点功能网元（Security Anchor Function，SEAF）和安全上下文管理功能网元（Security Context Management Function，SCMF）；也即是 AMF 也具有 SEAF 和 SCMF 的功能。安全锚点功能网元（Security Anchor Function，SEAF）也肯能独立于接入和移动性管理网 AMF 网元是个独立的网元。认证凭证存储和处理功能网元（Authentication Credential Repository and Processing Function，ARPF）主要负责存储用户的签约信息，如长期密钥。鉴权服务器（Authentication Server Function，AUSF）与 ARPF 交互，并且终结来自 SEAF 的鉴权请求。其中，AUSF 和 ARPF 可以理解为 LTE 网络框架中 HSS 拆分出来的功能网元。SEAF 与 AUSF 同 UE 交互，在入网认证流程中接收中间密钥，其可理解为 LTE 网络框架中 MME 拆分出来的功能网元。SCMF 从 SEAF 中获取中间密钥进一步派生出其密钥。可选地，ARPF 合并到图示中的用户数据管理网元（User Data Management，UDM）中，作为 UDM 的一部分。可选地，还可将 SEAF、SCMF 和 AMF 独立分开，将其作为一个独立的鉴权功能网元（Authentication function，AUF）。

会话管理网元 SMF 负责会话管理，如用户的会话建立等，也即是移动管理网元 MME 里的会话管理功能。用户面功能网元 UPF 是 UE 用户面的功能网元，主要负责连接外部网络，相当于 LTE 中的服务网关 SGW 和 PDN 网关（PDN-GW）的合体。专用网络网元 DN 负责为 UE 提供服务的网络，如一些 DN 为 UE 提供上网功能，另一些 DN 为 UE 提供短信功能等等。需要说明的是，图示中的一部分功能网元/实体与本申请方案无关，这里将不再详述。

基于图 3 所示的 5G 网络架构示意图，5G 的 non-3GPP 入网认证流程为：UE—>non-3GPP—>N3IWF—>AMF; 5G 的 3GPP 入网认证流程为：UE—>(R)AN—>AMF。可知 AMF 作为 5G 下 3GPP 和 non-3GPP 在信令控制面的一个汇聚功能实体（汇聚网元），其解决了 LTE 下通过 3GPP 和 non-3GPP 入网无关联性的问题。然而，在实际应用中发现 UE 上次通过 3GPP 或 non-3GPP 入网成功后，再次通过 3GPP 或 non-3GPP 进行非首次入网时，UE 还是需要重新按照 3GPP 或 non-3GPP 的入网认证流程，重新完成 UE 和网络侧之间的相互认证，认证成功后才能成功接入网络。由于 3GPP 或 non-3GPP 的入网认证过程比较繁琐，将会消耗较长的鉴权认证时间，UE 不能及时成功入网，影响用户体验。

为解决上述 UE 上次通过 3GPP 或 non-3GPP 入网成功后，再通过 non-3GPP 入网时入网认证时间较长的问题。结合图 3 所示的 5G 网络框架示意图，请参见图 4，图 4 是本发明实施例提供的一种基于非 3GPP 网络的入网认证方法的流程示意图，该方法包括如下实施步骤。

步骤 S101、UE 向 N3IWF 发送 IKE_SA_INIT 请求消息。相应地，所述 N3IWF 接收所述 UE 基于所述 IKE_SA_INIT 请求消息返回的 IKE_SA_INIT 响应消息。

本申请方案中，UE 上一次不论通过 3GPP(如 2G/3G/4G/5G)还是 non-3GPP(如 Wi-Fi) 成功接入网络后，网络侧会为 UE 分配有对应的 UE 临时标识，同时 UE 还会自己生成对应的安全上下文信息、或者其他信息。也即是 UE 上一次成功入网后，UE 中会存储有上一次入网成功后的保留信息，所述保留信息可以包括有 UE 临时标识、安全上下文信息或者其他的一些 UE 或网络侧生成的信息。

应理解的是，UE 临时标识为 UE 接入网络时核心网为 UE 分配的身份标识，此 UE 临时标识可以用于 RAN 或 N3IWF 寻找对应的 AMF 信息，正如 LTE 中的 GUTI（Globally Unique Temporary UE Identity，中文：全球唯一临时 UE 标识）等等。安全上下文信息可以包括鉴权过程中生成的密钥和后续会继续使用的非接入层（Non-access stratum，NAS）密钥、无线资源控制(Radio Resource Control, RRC)密钥和用户面保护密钥，如 Kamf, Knas-int, Knas-enc，Krrc-int，Krrc-enc，Kup-int，Kup-enc 等，或者 5G 中的锚点密钥 Kseaf，AMF 密钥 Kamf，以及保护 NAS 层，AS 层，用户面的加解密密钥和完整性保护密钥。可选地，安全上下文信息还可以包括加密算法、完整性保护算法，或者上一次 UE 与网络侧协商和生成的其他密钥和其他算法等，本发明实施例不作限定。

需要说明的是，安全上下文信息，会随着新密钥的生成而不断扩充。密钥标识信息可以由网络侧分配，或者也可以由 UE 临时标识来代表/标识。如果密钥标识信息是 UE 临时标识时，则通过密钥标识信息获取密钥的过程为：UE 和网络侧通过 UE 临时标识找到安全上下文信息，从安全上下文中获得密钥。如果这个密钥标识信息标识所有密钥或基于密钥标识信息标识的密钥所派生的密钥，则此密钥标识信息也可标识所有新派生的密钥。比如 LTE 中，KSIasme 就标识 Kasme 和其相关的密钥；再如 5G 中可能用 KSIseaf 标识，或 KSIamf 标识，或 KSIseaf+KSAIamf 的形式标识。

在UE上一次成功接入网络后，UE再通过non-3GPP（如Wi-Fi）接入网络时，UE与N3IWF之间交互IKE_SA_INIT消息(Internet key exchange initial association，中文：互联网密钥交换初始关联消息)。也即是，UE向N3IWF发送IKE_SA_INIT请求消息（IKE_SA_INIT1消息），所述IKE_SA_INIT请求消息携带有所述UE支持建立的安全通道参数KEi和发起方UE生成的随机数Randi（Random number）。这里的KEi可以是指UE支持建立的一个或多个安全通道的参数。

相应地，N3IWF接收UE发送的IKE_SA_INIT请求消息（假设记为IKE_SA_INIT1消息），通过解析IKE_SA_INIT1消息得到对应的参数信息，如KEi、Randi等。N3IWF从KEi中选取出UE和网络侧协商所要建立的安全通道参数KEr，同时还会生成Randr。进一步地，N3IWF向UE发送的IKE_SA_INIT响应消息（IKE_SA_INIT2消息），所述IKE_SA_INIT响应消息携带有UE与网络侧所需建立的安全通道参数Ker和响应方N3IWF生成的随机数Randr。

应理解的是，IKE_SA_INIT请求消息还可以携带UE临时标识、或其他参数信息；IKE_SA_INIT响应消息还可以携带N3IWF的标识信息（如N3IWF的ID号、N3IWF的IP地址等）、或者其他参数信息等，本发明实施例不作限定。

实际应用中，IKE_SA_INIT请求消息携带的诸如KEi、Randi、UE临时标识等参数信息可以可以放到消息中的V载荷或N载荷中，即Vendor(厂商)载荷或Notification(通知)载荷。同理，IKE_SA_INIT响应消息携带的诸如Ker、Randr等参数信息同样可放到消息中的V载荷或N载荷中，即Vendor（厂商）载荷或Notification（通知）载荷，以进行传输。

步骤S102、所述UE向所述N3IWF发送第一请求消息，所述第一请求消息携带有第一认证码、AMF指示信息和密钥标识信息，所述第一认证码用于所述N3IWF对所述UE进行安全认证，所述密钥标识信息用于所述N3IWF获取验证所述第一认证码的第一安全密钥。相应地，所述N3IWF接收所述UE发送的第一请求消息。

在本发明的一个实施例中，所述UE向N3IWF发送第一请求消息之前，还包括：所述UE根据所述UE对应的第一安全密钥生成第一认证码。

在第一种实现方式中，UE利用其内存储的安全上下文信息中的第一安全密钥Ks生成第一认证码AUTH1。这里的第一安全密钥Ks可以是指UE上一次成功入网后，UE存储的安全上下文信息中的Kseaf密钥、Kamf密钥、NAS层保护密钥、用户面完整性保护密钥(也即是NAS完整性保护密钥，也称为NAS完整性密钥）或者其他密钥等安全密钥。举例来说，AUTH1=prf(prf(Ks，“Key Pad for IKEv2”)，<InitiatorSignedOctets>)。其中，prf是使用的算法，如哈希256等。Key Pad for IKEv2是作为互联网密钥交换IKEv2协议密钥的填补参数，通常用字符串表示，这里作为生成第一认证码的一个输入参数。<InitiatorSignedOctets>是根据IKE_SA_INIT1消息中的一些参数信息（如KEi）和一些参数信息的衍生参数计算出来，因为计算<InitiatorSignedOctets>属于现有技术，这里不做相关详述。

在第二种实现方式中，UE利用其内存储的安全上下文信息中的安全密钥和第一新鲜保

护参数生成该 UE 对应的第一安全密钥 Ks。进一步地，UE 根据第一安全密钥生成第一认证码 AUTH1。

应理解的是，这里的安全密钥可以是指 UE 对应安全上下文信息中的 Kseaf 密钥、Kamf 密钥、或者其他密钥信息。这里的第一新鲜保护参数可以是指以下中的任意一项：计数器的计数值（NAS uplink count）、第一随机数、UE 临时标识、N3IWF 的标识信息、或者其他新鲜保护参数。N3IWF 的标识信息用于标识 N3IWF 的身份信息，例如 N3IWF 的 IP 地址、N3IWF 的 ID 号等。

举例来说，第一安全密钥 Ks= KDF(Kamf，N3IWF ID)，或者 Ks= KDF(Kseaf，N3IWF ID)；AUTH1=prf(prf(Ks，“Key Pad for IKEv2”)，<InitiatorSignedOctets>)。其中，KDF 是指使用的算法，如哈希 256 等。关于生成第一安全密钥 Ks 和生成第一认证码 AUTH1 中涉及的其他参数信息的说明请参见上述第一种实现方式的相关具体说明，这里不再赘述。

又如，第一安全密钥 Ks= KDF(Kamf，NAS uplink Count)、或 Ks= KDF(Kseaf，NAS uplink Count)、AUTH1=prf(prf(Ks，“Key Pad for IKEv2”)，<InitiatorSignedOctets>)。其中，NAS uplink Count 表示计数器统计并记录的当前数据。关于生成第一安全密钥 Ks 和生成第一认证码 AUTH1 中涉及的其他参数信息的说明请参见上述第一种实现方式的相关具体说明，这里不再赘述。

应理解的是，这里的第一安全密钥 Ks 可以由安全上下文信息中的安全密钥、第一新鲜保护参数、可选地还可加入其他参数信息（如注册类型指示信息、完整性保护算法等）生成的，本发明实施例不作限定。

应理解的是，密钥标识信息可以包括以下中的任意一项或多项：密钥标识符、密钥 ID 号、UE 临时标识、或者其他的用于标识密钥身份或用于标识 UE 的安全上下文信息的标识信息。

本申请方案中，UE 向 N3IWF 发送第一请求消息 IKE_AUTH_Req(Internet key exchange authentication request，中文又称为互联网密钥交换认证请求消息)。其中，IKE_AUTH_Req 消息携带有第一认证码 AUTH1、AMF 指示信息和密钥标识信息；第一认证码用于所述 N3IWF 对所述 UE 进行安全认证。

相应地，N3IWF 接收 UE 发送的第一请求 IKE_AUTH_Req 消息，并对 IKE_AUTH_Req 消息进行解析，获得 IKE_AUTH_Req 消息中携带的诸如第一认证码 AUTH1、密钥标识信息（如 UE 临时标识和/或密钥标识符）、AMF 指示信息等参数信息。接着，N3IWF 判断 IKE_AUTH_Req 中是否存在有第一认证码 AUTH1。在 N3IWF 判断到 N3IWF 消息携带有第一认证码 AUTH1 的情况下，决定不发起可扩展鉴权协议（Extensible Authentication Protocol，EAP）鉴权请求。并且由于 N3IWF 内部没有存储有用于验证第一认证码 AUTH1 的第一安全密钥 Ks，因此需要等待密钥。此时，N3IWF 可以利用 IKE_AUTH_Req 消息携带的 AMF 指示信息（如 UE 临时标识或 NAI 信息），并结合密钥标识信息从与 AMF 指示信息所指示的第一 AMF 处获取到用于验证第一认证码 AUTH1 的第一安全密钥 Ks，继续执行步骤 S103。

在 N3IWF 判断到 N3IWF 消息没有携带有第一认证码 AUTH1 的情况下，N3IWF 将发

起 EAP 鉴权流程，由于 EAP 鉴权流程属于现有技术，本发明实施例不作具体阐述。

实际应用中，AMF 指示信息用于标识 UE 上一次入网所接入的 AMF，其他网络中的设备（例如 eNB，NR，ePDG,N3IWF 等等）可以通过 AMF 指示信息找到该 AMF。这里的 AMF 指示信息可以包括 UE 对应的 UE 临时标识，或者包括根据 UE 临时标识生成的网络接入标识（Network Access Identifier，NAI）信息，或者 UE 上一次注册时收到的 AMF 标识信息，或者 UE 通过其他方法获得的 AMF 标识信息。其中，所述 NAI 信息是由 UE 临时标识中的 AMF 信息部分和 3GPP 网络的标识信息按照标准中定义的 NAI 的格式生成。

应理解的是，NAI 信息可以包括用户临时标识和 3GPP 网络地址，或者 AMF 标识信息和 3GPP 网络地址，或者其他的用于标识上次 UE 成功入网后与网络侧核心网元 AMF 进行相互认证的 AMF 身份信息。

应理解的是，AMF 指示信息和密钥标识信息可以是同一个信息。一个信息既可以是 AMF 指示信息，也可以是密钥标识信息。例如：AMF 指示信息和密钥标识信息均为 UE 临时标识的情况下，第一请求消息中携带的 UE 临时信息用于查找并确定与 UE 临时标识对应的第一 AMF，也可以用来查找 UE 的安全上下信息（也即是安全上下文信息中的相关密钥）。

应理解的是，第一请求消息 IKE_AUTH_Req 还可以携带有诸如 NAI 信息、计数器的计数值 NAS uplink Count、第一新鲜保护参数或者其他的用于 UE 入网认证的参数信息。如果是服务请求流程或者注册周期流程，则 IKE_AUTH_Req 就携带相应流程的 NAI 信息，计数器的计数值 NAS uplink Count 或者其他的用于相应流程的参数。

实际应用中，在第一请求消息 IKE_AUTH_Req 中可以将第一认证码 AUTH1 放到该消息的 Authentication（鉴权）载荷中，将 UE 临时标识、AMF 指示信息、NAI 信息等其中任意一个用于身份标识的参数信息放在消息的 IDi（Identity initial，中文：发起者身份标识）载荷中，将密钥标识信息（如密钥标识符）等参数信息放到消息的 V 载荷中。可选地，还可以将 UE 临时标识、密钥标识信息等参数信息都可以放在消息的 V 载荷或 N 载荷中。

或者，在第一请求消息 IKE_AUTH_Req 中可以将第一认证码 AUTH1 放在消息的 Authentication payload 部分；将 UE 临时标识、密钥标识信息、或者其他参数信息放在消息中的其他部分，如 V 载荷或 N 载荷中，本发明实施例不作限定。

此外，在第一请求消息 IKE_AUTH_Req 中通常可以将计数器的计数值（NAS uplink Count）携带在消息的 V 载荷中进行传输。

步骤 S103、所述 N3IWF 根据所述第一安全密钥生成第一验证码。

本申请实施例中，N3IWF 根据获取的第一安全密钥 Ks 生成第一验证码 AUTH1'。举例来说，AUTH1'= prf(prf(Ks, "Key Pad for IKEv2"), <ResponserSignedOctets>)。关于 AUTH1' 的生成过程以及涉及的参数介绍请具体参见上述步骤 S102 中的相关具体阐述，这里不再赘述。

步骤 S104、所述 N3IWF 判断所述第一认证码与所述第一验证码是否匹配。

步骤 S105、所述 N3IWF 在判断到所述第一认证码与所述第一验证码匹配的情况下，则向所述 UE 发送第一响应消息，所述入网响应消息携带有第二认证码，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。

本申请方案中，N3IWF 判断生成的第一验证码 AUTH1'和 IKE_AUTH_Req 携带的第一认证码 AUTH1 是否相同，若相同，则表示 N3IWF 对 UE 的安全认证成功，继续执行步骤 S105 向 UE 发送第一响应消息 IKE_AUTH_Response（又称为互联网密钥交换认证响应消息）。其中，所述第一响应消息 IKE_AUTH_Response 携带有第二认证码 AUTH2，所述第二认证码 AUTH2 用于所述 UE 对所述 N3IWF 进行认证。

在 N3IWF 判断到第一验证码 AUTH1'和第一认证码 AUTH1 不相同（不匹配）的情况下，结束流程，或者执行正常的 non-3GPP 入网认证流程，由于正常的 non-3GPP 入网认证流程属于现有技术，本发明实施例不再作具体阐述。

应理解的是，IKE_AUTH_Response 还可以携带有诸如密钥标识信息、UE 临时标识、N3IWF 的标识信息、第一新鲜保护参数等等信息，本发明实施例不作限定。

在本发明的一个实施例中，所述 N3IWF 向所述 UE 发送第一响应消息之前，还包括：所述 N3IWF 根据所述第一安全密钥生成第二认证码。

在 N3IWF 获取到第一安全密钥 Ks 后，N3IWF 可以根据第一安全密钥和发送的生成第二认证码 AUTH2。同理，N3IWF 可以根据第一安全密钥、可选地还可以加入一些其他参数信息（如 IKE_SA_INIT 响应消息携带的一些参数或一些参数的衍生参数等）一起来生成第二认证码 AUTH2。举例来说，AUTH2 = prf(prf(Ks，“Key Pad for IKEv2”)，<ResponserSignedOctets>)。其中，<ResponseSignedOctets>是根据 IKE_SA_INIT 响应消息(假设记为 IKE_SA_INIT2 消息）中的一些参数信息（如 KEr）和一些参数信息的衍生参数计算出来，因为计算<ResponseSignedOctets>属于现有技术，这里不做相关详述。关于生成第二认证码 AUTH2 过程中涉及的参数信息请具体参见上述步骤 S102 中的相关具体阐述，这里不再赘述。

步骤 S106、相应地，所述 UE 接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息，所述第一响应消息携带有第二认证码，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。所述 UE 根据所述 UE 对应的第一安全密钥生成第二验证码。

本申请方案中，UE 接收 N3IWF 发送的第一响应消息 IKE_AUTH_Response，通过消息解析得到 IKE_AUTH_Response 消息携带的诸如第二认证码 AUTH2 等参数信息。UE 可以根据上述第一安全密钥 Ks 生成对应的第二验证码 AUTH2'。同理，UE 可以根据第一安全密钥、可选地还可以加入一些其他参数信息（如 IKE_SA_INIT 响应消息携带的一些参数或一些参数的衍生参数等）一起来生成第二认证码 AUTH2。举例来说，AUTH2'=prf(prf(Ks，“Key Pad for IKEv2”)，<ResponserSignedOctets>)。关于生成第二验证码 AUTH2'的过程请具体参见上述步骤 S105 中的相关描述，这里不再赘述。

步骤 S107、所述 UE 判断所述第二认证码与所述第二验证码是否匹配。

本申请方案中，UE 判断第二认证码 AUTH2 与生成的第二验证码 AUTH2'是否相同，如果相同，则 UE 对 N3IWF 的安全认证成功；否则，结束流程，UE 对 N3IWF 的安全认证失败。可选地，UE 还可以通过正常的 non-3GPP 入网认证流程再次尝试入网，由于正常的 non-3GPP 入网认证流程属于现有技术，与本发明实施例无关，这里不再详述。

步骤 S108、所述 UE 对所述 N3IWF 安全认证成功。

应理解的是，执行到步骤 S108，此时 UE 和 N3IWF 已完成了相互之间的安全认证，同时，UE 和网络侧建立的安全通道（如 IPsec 隧道）也完成。

在本发明的一个实施例中，结合图 4 所述实施例，其中步骤 S102 之后，步骤 S103 之前，还可以包括如下实施步骤。具体可参见图 5，图 5 是本发明实施例提供的又一种基于非 3GPP 网络的入网认证方法的流程示意图。

步骤 S201、在所述 N3IWF 查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向所述 AMF 指示信息所指示的第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息。相应地，所述第一 AMF 接收所述 N3IWF 发送的所述第二请求消息。

本申请方案中，所述 N3IWF 向所述 AMF 指示信息所指示的第一 AMF 发送第一安全密钥请求消息之前，还包括步骤 S200a: 所述 N3IWF 根据所述第一请求消息中的 AMF 指示信息，确定与所述 AMF 指示信息所指示的第一 AMF。

应理解的是，AMF 指示信息可以包括有 UE 临时标识或 NAI 信息、或其他的用于指示确定与 UE 进行双向安全认证的 AMF 的信息。所述 UE 临时标识含有所述 UE 上次成功入网时使用的 AMF 的信息。所述 NAI 信息同样可以指示所述 UE 上次成功入网时使用的 AMF 的信息。所述 N3IWF 通过所述第一请求消息 IKE_AUTH_Req 中 IDi 内的 AMF 指示信息(如 UE 临时标识或 NAI 信息)，来查找并确定与所述 AMF 指示信息所指示的第一 AMF。

举例来说，在 LTE 中 UE 的临时标识为 GUTI，GUTI 中含有 MME 的身份信息，eNB 可以通过这个身份信息找到对应的 MME 或者 LTE 中 UE 会将 NAI 作为 IDi 发送给 ePDG,ePDG 通过 NAI 的内容查找 MME。5G 中类似，N3IWF 接收的 IKE_AUTH_Req 中已携带有 UE 的临时标识或 NAI 信息，那么 N3IWF 可以根据这个临时标识或 NAI 信息，找到相关的 AMF，也即是第一 AMF。

应理解的是，第二请求消息还可以携带有第一认证码 AUTH1、密钥标识符、第一新鲜保护参数，如 N3IWF 的标识信息，计数器的计数值（NAS Uplink Count）、注册类型指示信息（又称为入网类型指示信息），也即是 UE 当前通过 non-3GPP 为首次入网还是非首次入网、或者其他的参数信息，本发明实施例不作限定。

步骤 S202、所述第一 AMF 根据所述密钥标识信息，确定所述 UE 对应的第一安全密钥。

本申请方案中，由于第一 AMF 中可能存储有多个 UE（与 UE 临时标识对应）的多个安全上下文信息，每个 UE 可能对应有一个或多个安全上下文信息。若所述密钥标识信息不包括 UE 临时标识，则第二请求消息还需要携带有 UE 临时标识，在第一 AMF 接收到第二请求消息后，通过消息解析出第二请求消息携带的 UE 临时标识，可选地还可有密钥标识符等密钥标识信息、或其他参数信息。接着，第一 AMF 根据第二请求消息携带的 UE 临时标识从预存的多个 UE 的多个安全上下文信息中，查找出与所述 UE 临时标识对应的一个或多个安全上下文信息。接着，第一 AMF 根据密钥标识信息（假设为密钥标识符）从所述 UE 临时标识对应的一个或多个安全上下文信息中查找出与密钥标识信息对应的 UE 的安全上下文信息。

应理解的是，如果第一 AMF 中为每个 UE 存储有对应的一个安全上下文信息时，那么此时第一 AMF 可以直接根据第二请求消息携带的 UE 临时标识查找到与 UE 临时标识对应的 UE 的安全上下文信息。也即是 UE 上一次成功入网后，UE 中存储的安全上下文信息。

进一步地，第一 AMF 根据查找的 UE 的安全上下文信息，并结合第二请求消息携带的诸如第一新鲜保护参数（N3IWF 的标识信息或 NAS uplink count）等参数信息确定出对应的第一安全密钥信息，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数或者直接包括第一安全密钥。

应理解的是，在第一安全密钥信息包括用于派生第一安全密钥的派生参数的情况下，此场景适用于使用 Kamf 密钥派生第一安全密钥，或者当 AMF 和 SEAF 共同部署在一起的时候（此时 AMF 和 SEAF 的内部交互忽略，SEAF 看做是 AMF 的一部分）。如果 AMF 和 SEAF 没有共同部署，那么 AMF 查找到 UE 后，如果要使用 Kseaf 作为基础密钥衍生第一安全密钥 Ks，那么可能需要继续去 SEAF 处查找相关 UE 的密钥信息（也即是查找与 UE 的安全上下文信息），AMF 需要提供 UE 的身份信息（UE 临时标识）和其他密钥输入参数给 SEAF，如 N3IWF 的标识信息，或 NAS uplink count 等第一新鲜保护参数。SEAF 依据第一新鲜保护参数和基础密钥 Kseaf 衍生/派生出第一安全密钥 Ks，将第一安全密钥 Ks 发送给第一 AMF。

在第一种实现方式中，第一 AMF 将查找到的 UE 的安全上下文信息中的 NAS 完整性密钥或用户面完整性保护密钥直接作为第一安全密钥 Ks。

在第二种实现方式中，第一 AMF 将查找到的 UE 的安全上下文信息中的安全密钥和第一新鲜保护参数，可选地还可以加入一些其他参数信息确定为用于派生第一安全密钥的派生参数。进一步地，第一 AMF 依据该安全上下文信息中的安全密钥和第一新鲜保护参数等派生参数生成第一安全密钥 Ks。

应理解的是，第一 AMF 还可以为第一安全密钥 Ks 生成对应的第一密钥标识信息。所述第一密钥标识信息用于标识第一安全密钥、或者用于标识与第一安全密钥相同类型的某一类密钥，第一安全密钥标识信息可以是特定的字符串、或者几比特的数字等，其生成和具体实现有关，这里不作相关详述。

需要说明的是，关于第一安全密钥的生成过程具体可参见图 4 实施例中关于第一安全密钥生成的相关具体阐述，这里不再赘述。同理，关于安全密钥、第一新鲜保护参数的相关描述请具体参见图 4 所述实施例的相关具体描述，这里不再赘述。

步骤 S203、所述第一 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。相应地，所述 N3IWF 接收所述第一 AMF 发送的所述第二响应消息，所述第二响应消息携带有所述第一安全密钥。

应理解的是，第二响应消息可以携带有第一安全密钥 Ks、可选的还可以携带有与 Ks 对应的密钥标识信息 KSIks、第一 AMF 的标识信息、安全上下文信息中的安全密钥、N3IWF 的标识信息、计数器的计数值（NAS uplink count）、第一新鲜保护参数或者其他的参数信息等，本发明实施例不作限定。

在本发明的又一个实施例中，结合图 4 所述实施例，其中步骤 S102 之后，步骤 S103 之前，还可以包括如下实施步骤。具体可参见图 6，图 6 是本发明实施例提供的又一种基于非 3GPP 网络的入网认证方法的流程示意图。

步骤 S301、在所述 N3IWF 查找不到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，所述第三请求消息携带有所述密钥标识信息。

本申请方案中，由于网络配置原因，N3IWF 可以通信连接的 AMF 有数目限制或者范围限制，比如运营商可能配置允许 N3IWF 查找网络边缘的 AMF，不允许 N3IWF 连接网络深处的 AMF，因此可能会出现 N3IWF 不能查找到与所述 AMF 指示信息所指示的第一 AMF 的情况。

在本发明的一个实施例中，请参见图 7，图 7 是本发明实施例提供的又一种基于非 3GPP 网络的入网认证方法的流程示意图，步骤 S102 之后还包括步骤 S200a 和步骤 S200b。在所述 N3IWF 无法查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，此时可结束流程，或者 N3IWF 可以向 UE 发送第一响应失败消息 IKE_AUTH_Response（failure）。可选地，UE 在接收到 N3IWF 返回的 IKE_AUTH_Response（failure）消息后，可以按照正常的 non-3GPP 入网认证流程再次进行入网认证。

在本发明的又一个实施例中，在所述 N3IWF 查找不到所述 AMF 指示信息所指示的第一 AMF 的情况下，所述 N3IWF 向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述 AMF 指示信息所指示的第一 AMF 发送第二请求消息。

实际应用中，N3IWF 内部维护有预配置可连接的 AMF 列表，该 AMF 列表包括有 N3IWF 支持连接的一个或多个 AMF。N3IWF 可以从 AMF 列表中任意选取一个或多个 AMF 作为第二 AMF。或者，N3IWF 可以通过域名（Domain Name System，DNS）服务器查找到对应的第二 AMF。接着 N3IWF 可以向第二 AMF 发送第三请求消息，该第三请求消息可以携带有 UE 临时标识、密钥标识信息等参数信息。

步骤 S302、相应地，所述第二 AMF 接收所述 N3IWF 发送的所述第三请求消息，并根据所述第三消息携带的 UE 临时标识，查找与所述 UE 临时标识对应的第一 AMF。

相应地，第二 AMF 接收 N3IWF 发送的第三请求消息。同理若在所述密钥标识信息不包括 UE 临时信息的情况下，则第三请求消息还需携带有 UE 临时标识，并通过消息解析获得第三请求消息携带的 UE 临时标识、密钥标识信息等参数信息，可选地还有其他参数信息。接着，第二 AMF 判断 UE 临时标识对应的 AMF 是否为第二 AMF 自身；如果不是，那么第二 AMF 根据 UE 临时标识含有的 AMF 的标识信息，查找出与 UE 临时标识对应的第一 AMF。

需要说明的是，关于第一 AMF 的查找过程具体可参见图 5 所述实施例的相关具体阐述，这里不再赘述。

应理解的是，在第二 AMF 无法查找到与 UE 临时标识对应的第一 AMF 的情况下，结束流程或通过 N3IWF 向 UE 发送第一响应失败消息 IKE_AUTH_Response（failure）。同理，UE 在接收到 N3IWF 返回的 IKE_AUTH_Response（failure）消息后，可以再次按照正常的 non-3GPP 入网认证流程进行入网认证，尝试入网。

步骤 S303、所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息。相应地，所述第一 AMF 接收所述第二 AMF 发送的所述第二请求消息。

本申请方案中，第二 AMF 可以利用解析第三请求消息所得的如 UE 临时标识、密钥标识信息、以及其他参数信息、可选地还可以加入一些其他参数信息（如第二 AMF 的标识信息等）来生成对应的第二请求消息，并将该第二请求消息发送给 UE 临时标识对应的第一 AMF。相应地，第一 AMF 接收第二 AMF 发送过来的第二请求消息，该第二请求消息携带有密钥标识信息、UE 临时标识等参数信息。

应理解的是，第二请求消息和第三请求消息还可以携带有诸如第一认证码 AUTH1、第一新鲜保护参数、第一随机数、N3IWF 的标识信息（N3IWF 的 IP 地址或 N3IWF 的 ID 号等）、计数器的计数值（NAS_uplink Count Number）、注册类型指示信息（又称为入网类型指示信息），也即是 UE 当前通过 non-3GPP 为首次入网还是非首次入网、或者其他的参数信息，本发明实施例不作限定。

步骤 S304、所述第一 AMF 根据所述密钥标识信息，确定所述 UE 对应的第一安全密钥信息，所述第一安全密钥信息包括第一安全密钥，或者用于派生第一安全密钥的派生参数。

在第一种实现方式中，步骤 S304 的具体实现方式为步骤 S304a：第一 AMF 根据所述密钥标识信息，确定所述 UE 对应的第一安全密钥。关于第一安全密钥 Ks 的确定过程具体可参见图 5 所述实施例步骤 S202 的相关具体阐述，这里不再赘述。

在第二种实现方式中，步骤 S304 的具体实现方式为步骤 S304b：第一 AMF 根据所述密钥标识信息，确定所述 UE 对应的第一安全密钥信息，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数。关于第一安全密钥信息的确定过程具体可参见图 5 所述实施例步骤 S202 的相关具体阐述，这里不再赘述。

应理解的是，在第二请求消息和第三请求消息分别还携带有第一新鲜保护参数（如 N3IWF 的标识信息、NAS uplink count 等）的情况下，所述派生参数包括有 UE 的安全上下文信息（如安全密钥）、第一新鲜保护参数、可选地还可以包括一些其他的参数信息（如 NAS 算法）等，本发明实施例不作限定。

需要说明的是，这里的第一安全密钥信息或派生参数可以包括 UE 的安全上下文信息（诸如 UE 临时标识、密钥标识信息、安全密钥、安全算法等）、还可以包括 N3IWF 的标识信息或计数器的计数值（NAS uplink count）等第一新鲜保护参数、或者其他的参数信息，本发明实施例不作限定。

步骤 S305、所述第一 AMF 向所述第二 AMF 发送第三响应消息，所述第三响应消息携带有所述第一安全密钥信息。相应地，所述第二 AMF 接收所述第一 AMF 发送的所述第三响应消息。

本申请方案中，第一 AMF 利用上述确定的第一安全密钥信息生成对应的第三响应消息，该第三响应消息携带有第一安全密钥信息。第一 AMF 可以将第三响应消息发送给第二 AMF。相应地，第二 AMF 接收第一 AMF 发送过来的第三响应消息。

步骤 S306、所述第二 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息携带

有第一安全密钥。相应地，所述 N3IWF 接收所述第二 AMF 发送的所述第二响应消息。

实际应用中，结合步骤 S304 的第一种实现方式步骤 S304a，在所述第一安全密钥信息包括第一安全密钥的情况下，第二 AMF 可以直接将接收的第一 AMF 发送的第三响应消息，作为第二响应消息转发（发送）给 N3IWF。或者，第二 AMF 可以根据接收的第三响应消息中携带的第一安全密钥 Ks，可选地还可以加入一些其他参数信息（如第二 AMF 的标识信息等）一起来生成第二响应消息，然后将第二响应消息发送给 N3IWF。相应地，N3IWF 接收第二 AMF 发送的第二响应消息，该第二响应消息至少携带有第一安全密钥。

实际应用中，结合步骤 S304 的第二种实现方式步骤 S304b，在所述第一安全密钥信息包括用于派生第一安全密钥的派生参数的情况下，所述第二 AMF 向所述 N3IWF 发送第二响应消息之前，还包括步骤 S306'：所述第二 AMF 根据所述派生参数生成对应的第一安全密钥 Ks。关于第一安全密钥 Ks 的确定过程具体可参见图 5 所述实施例步骤 S202 的相关具体阐述，这里不再赘述。

在第二 AMF 生成第一安全密钥 Ks 后，第二 AMF 可以利用生成的第一安全密钥 Ks，可选地还可以加入一些其他参数信息（如安全上下文信息中的参数、第一新鲜保护参数等）一起生成对应的第二响应消息，并将第二响应消息发送给 N3IWF。相应地，N3IWF 接收第二 AMF 发送的第二响应消息，该第二响应消息至少携带有第一安全密钥，可选地还可以携带有其他参数信息。具体可参见图 8，图 8 是本发明实施例提供的又一种基于非 3GPP 网络的入网认证方法的流程示意图。

需要说明的是，关于第二响应消息的相关说明具体可参见图 5 所述实施例步骤 S203 的相关具体阐述，这里不再赘述。

在本发明的又一个实施例中，结合图 4 所述实施例，其中步骤 S102 之后，步骤 S103 之前，还可以包括如下实施步骤。具体可参见图 9，图 9 是本发明实施例提供的又一种基于非 3GPP 网络的入网认证方法的流程示意图。

步骤 S401、在所述 N3IWF 查找不到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，所述第三请求消息携带有所述密钥标识信息。

步骤 S402、相应地，所述第二 AMF 接收所述 N3IWF 发送的所述第三请求消息，并根据所述第三消息携带的 UE 临时标识，查找与所述 UE 临时标识的第一 AMF。

步骤 S403、所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息。相应地，所述第一 AMF 接收所述第二 AMF 发送的所述第二请求消息。

需要说明的是，关于步骤 S401-步骤 S403 的具体实施方式请具体参见图 6 所述实施例步骤 S301-步骤 S303 的相关具体阐述，这里不再赘述。

步骤 S404、所述第一 AMF 通过所述第二 AMF 向所述 N3IWF 发送重定向指示信息，所述重定向指示信息携带有所述第一 AMF 的地址信息，所述重定向指示信息用于指示所述 N3IWF 重新向所述第一核心网网元发送第二请求消息。

步骤 S405、相应地，所述 N3IWF 接收所述第二 AMF 转发所述第一 AMF 发送的所述重定向指示信息。所述 N3IWF 根据所述重定向指示信息，向所述第一 AMF 发送所述第二

请求消息，所述第二请求消息携带有所述密钥标识信息。

本申请方案中，在第一 AMF 接收到第二 AMF 发送的第二请求消息时，第一 AMF 可以通过第二 AMF 向 N3IWF 发送重定向指示信息 Identification Response，该重定向指示信息 Identification Response 用于指 N3IWF 重新与第一 AMF 建立通信连接，以重传第二请求消息。相应地，N3IWF 接收第一 AMF 通过第二 AMF 转发的重定向指示信息 Identification Response，根据 Identification Response 的指示，重新将第二请求消息发送给第一 AMF。

步骤 S406、相应地，所述第一 AMF 接收所述 N3IWF 发送的所述第二请求消息。所述第一 AMF 根据所述密钥标识信息，确定所述 UE 对应的第一安全密钥。

应理解的是，步骤 S406 中所述第一 AMF 根据所述 UE 临时标识和所述密钥标识信息，确定所述 UE 对应的第一安全密钥还可以在步骤 S403 之后执行，也可以在步骤 S405 所述第一 AMF 接收到所述 N3IWF 发送的所述第二请求消息之后执行，本发明实施例不作限定。

步骤 S407、所述第一 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。相应地，所述 N3IWF 接收所述第一 AMF 发送的所述第二响应消息，所述第二响应消息携带有所述第一安全密钥。

需要说明的是，关于第一安全密钥和第二响应消息的介绍具体可参见图 5 所述实施例的相关具体阐述，这里不再赘述。

在本发明的又一个实施例中，结合图 4-图 9 所述实施例，其中步骤 S108 之后，还可以包括如下实施步骤。具体可参见图 10，图 10 是本发明实施例提供的一种第一 AMF 对 UE 进行安全认证方法的流程示意图。

步骤 S501、所述 UE 向所述 NSIWF 发送第四请求消息，该第四请求消息承载在因特网安全 IPsec（Internet Protocol Security，IPsec）协议，所述第四请求消息携带有第三认证码和密钥标识信息，所述第三认证码用于所述第一 AMF 对所述 UE 进行安全认证。相应地，所述 NSIWF 接收所述 UE 发送的第四请求消息。

本申请方案中，UE 在安全通道（如 IPsec 隧道）中向 NSIWF 发送第四请求消息，以实现所述第一 AMF 对所述 UE 的安全认证。这里的第四请求消息属于 NAS 消息，承载在 IPsec 协议上进行传输。

应理解的是，这里的第四请求消息可以是注册请求消息 Registration request、服务请求 Service Request 消息、服务区更新（Tracking area update，TAU）请求消息、或者其他流程的请求消息等，本发明实施例不作限定。

示例地如，如果这里的第四请求消息为注册请求消息，那么注册请求消息可以包括有注册参数 Registration parameters，该注册参数可以包括诸如 UE 临时标识、密钥标识信息、注册类型指示信息 RT、第二新鲜保护参数或者其他的参数信息，同时该注册请求消息还携带有第三认证码 MAC、或其他参数信息，本发明实施例不作限定。实际应用中，注册参数可以放在消息的 V 载荷或 N 载荷中。

同理，如果第四请求消息为其他流程，包括但不限于注册请求 Registration request 流程，其区别仅在于第四请求消息中携带的是其他流程的参数，如 Service Request parameters，TAU parameters。

应理解的是，在其他流程的第四请求消息中已经包含有第三认证码和其他流程参数，而在注册请求流程中注册请求消息只包含有注册参数，并不包含第三认证码。因此，在第四请求消息为注册请求消息的情况下，第四请求消息除了包含有注册请求消息的注册参数之外，还需要包含/携带第三认证码。

本发明的一个实施例中，所述 UE 向所述 AMF 指示信息所指示的第一 AMF 发送第四请求消息之前，还包括：所述 UE 根据所述 UE 的安全上下文信息中的 NAS 完整性密钥生成第三认证码。

实际应用中，UE 可以利用 UE 临时标识、密钥标识信息、注册类型指示消息、可选地还可以加入一些其他参数性（如第二新鲜保护参数、UE 存储的安全上下文信息等）来生成第四请求消息（如注册请求消息 Registration request）。接着 UE 可以利用安全上下文信息中的第二安全密钥（如 NAS 完整性密钥、加密密钥等）对第四请求消息（如注册请求消息 Registration request）进行保护，生成并计算出第三认证码 MAC。也即是，UE 可以根据 UE 上一次成功入网后其内存储的安全上下文信息，如 UE 临时标识、密钥标识信息、第二安全密钥 Kq 和安全算法 f1 等，并结合当前 UE 通过 non-3GPP 入网的注册类型指示信息 RI（入网类型指示信息，首次入网或非首次入网），可选地还可加入一些其他参数信息（如第二新鲜保护参数等）来生成第三认证码 MAC（Message authentication code，又称为消息鉴权码）。举例来说，MAC=EIA1（NAS 完整性密钥，第二新鲜性保护参数（如，NAS uplink count），UE 和 AMF 共有的不被第三方知道的参数（如 GUTI，或 registration type，或者后续被新定义的参数，比如接入方式指示符））。又如，LTE 中的生成方法，MAC=EIA1（NAS 完整性密钥，Registration request 消息（含有第三认证码 AMC），计数器的计数值（NAS uplink count），消息方向，承载信息）。再如，MAC = EIA1（NAS 完整性保护密钥，注册参数）。其中，EIA 是指 EPS 网络使用的完整性保护算法（EPS Integrity Algorithm），如 EIA0，EIA1，EIA2，EIA3 等，消息方向是指 Registration request 消息为上行消息还是下行消息，通常可以用特定字符串表示，如“0”表示下行消息，“1”表示上行消息。承载消息是指消息的传输管道，也即是在哪个管道中传输。注册参数是指在所述第一请求消息中携带在 V 载荷或 N 载荷中的注册参数。

应理解的是，这里的安全上下文信息包括第二安全密钥 Kq 和安全算法，第二安全密钥可以是指安全上下文信息的 NAS 完整性密钥、加密密钥、NAS 密钥等等，安全算法可以是安全上下文信息的完整性保护算法、加密算法、NAS 算法，或者其他的算法，本发明实施例不作限定。

应理解的是，这里的第二新鲜保护参数可以包括第二随机数、计数器的计数值（NAS uplink count）等参数信息，上述的第一新鲜保护参数和第二新鲜保护参数可以是指相同的参数，也可以是指不同的参数，本发明实施例不作限定。

步骤 S502、所述 N3IWF 向所述第一 AMF 发送所述第四请求消息，该第四请求消息承载在 NG2 协议上。相应地，所述第一 AMF 接收所述 N3IWF 发送的所述第四请求消息。

本申请方案中，N3IWF 接收到 UE 承载在 IPsec 协议上发送过来的第四请求消息（NAS 消息）后，N3IWF 可以从中抽取出该第四请求消息。进一步地，N3IWF 将第四请求消息承载在 NG2（Next Generation interface Number 2）协议上，将其发送给第一 AMF。相应地，

第一 AMF 接收 N3IWF 承载在 NG2 协议上发送过来的第四请求消息。

应理解的是，NG2 为一个接口，用于连接 N3IWF 和 AMF，使 N3IWF 和 AMF 进行相互通信。

步骤 S503、所述第一 AMF 根据所述密钥标识信息确定所述 UE 的安全上下文信息中的 NAS 完整性密钥。

本申请方案中，第一 AMF 接收 N3IWF 发送的第四请求消息，通过消息解析获知第四请求消息中携带的诸如第三认证码 MAC、UE 临时标识、密钥标识信息、注册类型指示信息 RT、第二新鲜保护参数等参数信息。第一 AMF 可以根据 UE 临时标识和密钥标识信息，查找出所述 UE 的安全上下文信息。关于安全上下文信息的查找过程可参见上述图 5 步骤 S202 实施例中的相关具体阐述，这里不再赘述。

步骤 S504、所述第一 AMF 根据所述 UE 的安全上下文信息中的 NAS 完整性密钥生成第三验证码。

本申请方案中，第一 AMF 根据所述 UE 临时标识、所述密钥标识信息、所述第二安全密钥 Kq（如 NAS 完整性密钥）、所述安全算法 f1、所述注册类型指示信息 RT、第二新鲜保护参数、可选地还可加入一些其他参数信息来生成第三验证码 MAC'。

实际应用中，第一 AMF 利用上述解析第四请求消息所得的如 UE 临时标识、密钥标识信息、注册类型指示信息 RT、第二新鲜保护参数等必要参数信息，生成与 UE 或 N3IWF 发送来的第四请求消息相同的第四请求消息（如注册请求消息 Registration request）。然后，第一 AMF 利用安全上下文信息中的第二安全密钥（如 NAS 完整性密钥等）对生成的第四请求消息（如 Registration request）进行保护，同样会生成并计算出第三验证码 MAC'。举例来说，MAC' =EIA1（NAS 完整性密钥，第二新鲜性保护参数（如，NAS uplink count），UE 和 AMF 共有的不被第三方知道的参数（如 GUTI，或注册类型指示信息 registration type，或者后续被新定义的参数，比如接入方式指示符））。又如，LTE 中的生成方法，MAC' =EIA1（NAS 完整性密钥，Registration request 消息（含有第三认证码 AMC），计数器的计数值（NAS uplink count），消息方向，承载信息）。关于 MAC' 生成过程所涉及的参数信息具体可参见步骤 S501 中的相关具体阐述，这里不再赘述。

步骤 S505、所述第一 AMF 判断所述第三验证码和所述第三认证码是否匹配。

步骤 S506、在判断到所述第三验证码和所述第三认证码匹配，则向所述 N3IWF 发送第四响应消息，该第四响应消息承载在 NG2 协议上，所述第四响应消息用于指示所述 UE 注册成功。

步骤 S507、相应地，所述 N3IWF 接收所述第一 AMF 发送的所述第四响应消息。所述 N3IWF 向所述 UE 发送所述第四响应消息，该第四响应消息承载在 IPsec 协议上，所述第四响应消息用于指示所述 UE 注册成功。

本申请方案中，第一 AMF 判断第三认证码 MAC 与生成的第三验证码 MAC' 是否相同，如果相同，则在安全通道上向 NI3WF 发送第四响应消息（如 Registration response），所述第四响应消息用于指示 UE 注册成功，第一 AMF 对 UE 的安全认证成功；否则，结束流程或者向 UE 发送第四响应失败消息（如 Registration response failure），所述第四响应失败消息用于指示第一 AMF 对 UE 的安全认证失败，UE 注册失败。这里的第四响应消息或

第四响应失败消息需要承载在 NG2 协议上，进行传输。

同理，N3IWF 接收第一 AMF 发送的第四响应消息或第四响应失败消息，并将该第四响应消息或第四响应失败消息承载在 NG2 协议上发送给 UE，以告知 UE 是否注册成功。

通过实施本发明实施例，能够利用 UE 上次入网成功后存储的安全上下文信息来完成当前 UE 通过非 3GPP 的入网认证，减少现有技术中通过非 3GPP 进行入网认证的流程步骤，实现 UE 的快速入网。

在本发明的又一个实施例中，结合图 4-图 9 所述实施例，在所述第一请求消息和所述第二请求消息中分别还携带有第三认证码的情况下，步骤 S202 或 S304 或 S406 所述第一 AMF 根据所述所述密钥标识信息，确定所述 UE 对应的第一安全密钥或第一安全密钥信息之前，还包括如下实施步骤。具体可参见图 11，图 11 是本发明实施例提供的又一种第一 AMF 对 UE 进行安全认证方法的流程示意图。

步骤 S601、所述第一 AMF 根据所述密钥标识信息，确定所述 UE 的安全上下文信息。

本申请方案中，在所述第一请求消息（IKE_AUTH_Req）和所述第二请求消息中分别还携带有第三认证码（MAC）的情况下，步骤 S102 所述 UE 向所述 N3IWF 发送第一请求消息之前，还包括：所述 UE 根据所述 UE 的安全上下文信息中的 NAS 完整性密钥生成第三认证码。

应理解的是，同理参见图 10 所述实施例关于第三认证码的生成过程，UE 首先可以利用 UE 临时标识、密钥标识信息，可选地还可加入一些其他参数信息（如 UE 存储的安全上下文信息、第二新鲜保护参数、注册类型指示消息等）来生成注册请求消息 Registration request。然后利用安全上下文信息中的第二安全密钥（如 NAS 完整性密钥等）对注册请求消息 Registration request 进行保护，生成并计算出第三认证码 MAC。也可以 UE 不生成具体的 Registration request 消息，而是用第二请求消息中携带的 N3IWF 使用的用于生成 Registration request 的 Registration parameter 作为生成第三认证码 MAC 的输入。如果 UE 发其他流程，如服务请求（Service Request）流程、类似于 LTE 的服务区更新（Tracking area update，TAU）流程，则第二消息中携带相应流程的参数，用于 N3IWF 生成相应的消息。如携带 service request parameter，或 TAU parameter.如果 UE 构造了完整的 Registration Request 消息，再生成 MAC。则要求 N3IWF 要构造出和 UE 生成的完全相同的 Registration Request 消息，再发送给第一 AMF。这个要求也同样适用于其他流程，如 service request 或 TAU 流程。关于第三认证码的生成过程具体可参见图 10 所述实施例的相关具体阐述，这里不再赘述。

步骤 S602、所述第一 AMF 根据所述 UE 的安全上下文信息中的 NAS 完整性密钥生成第三验证码。

步骤 S603、所述第一 AMF 判断所述第三验证码和所述第三认证码是否匹配。

步骤 S604、所述第一 AMF 在判断到所述第三验证码和所述第三认证码匹配的情况下，则所述第一 AMF 对所述 UE 安全认证成功。

本申请方案中，在第一 AMF 确定到第三验证码 MAC’ 和第三认证码 MAC 匹配的情

况下，则表示第一 AMF 对所述 UE 安全认证成功，可以对应继续执行上述实施例中步骤 S202、或步骤 S304、或步骤 S406 以及之后的相关流程步骤。

应理解的是，N3IWF 向第一 AMF 发送的第二请求消息中携带有第三认证码 MAC，可选地还可以携带有 UE 临时标识、密钥标识符（或密钥标识信息）、注册类型指示信息 RT、第二新鲜保护参数或者其他参数信息，本发明实施例不作限定。

应理解的是，结合图 10 所述实施例，这里的第二请求消息包括注册请求消息 Registration request 和第三认证码 MAC。关于上述步骤 S601-步骤 S603 可参见上述图 10 所述实施例中步骤 S501-步骤 S505 的相关具体阐述，这里不再赘述。

结合图 10 所述实施例，本申请实施例中第一请求消息携带有注册参数，该注册参数包括有密钥标识信息、UE 的临时标识和第三认证码（MAC）等参数信息，第二请求消息是由注册请求消息 Registration request 和密钥请求消息构成，所述密钥请求消息用于获取验证第一认证码 AUTH1 的第一安全密钥，所述注册请求消息是 N3IWF 用第一请求消息中的注册参数生成的，并且注册请求消息（或注册参数）包含在第一请求消息中。

需要说明的是，本发明实施例中涉及的 UE 临时标识、密钥标识信息、NAI 信息、注册类型指示消息、第二新鲜保护参数、计数器的计数值（NAS uplink Count）等参数信息可以放在对应消息的 V 载荷或 N 载荷中，以进行传输；本发明实施例涉及的第一认证码 AUTH1、第一验证码 AUTH1’、第二认证码 AUTH2 以及第二验证码 AUTH2’ 等参数信息可以放在对应消息的 Authentication 鉴权载荷中。

通过实施本发明实施例，能够利用 UE 上次入网成功后安全上下文信息来完成当前 UE 通过非 3GPP 的入网认证，减少现有技术中通过非 3GPP 进行入网认证的流程步骤，实现 UE 的快速入网。

基于同一发明构思，请参见图 12，图 12 是本发明实施例提供的一种用户设备的结构示意图。如图 12，该用户设备 12 包括收发器 501、存储器 502 和处理器 503（处理器 503 的数量可以一个或多个，图 12 中以一个处理器为例），在本发明的一些实施例中，收发器 501、存储器 502 和处理器 503 可通过总线或者其它方式连接，其中，图 12 中以通过总线连接为例。所述处理器 503 调用所述存储器 502 中的基于非 3GPP 网络的入网认证程序，用于执行如下操作：

获取上一次成功入网后，所述 UE 的保留信息；

根据所述 UE 的保留信息，确定接入和移动性管理网元 AMF 指示信息和第一安全密钥；

根据所述第一安全密钥生成第一认证码；

通过所述收发器向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥；

通过所述收发器接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息。

在一些可选的方案中，所述第一响应消息携带有第二认证码，所述第二认证码为所述 N3IWF 根据所述第一安全密钥生成的；所述处理器还用于：根据所述第一安全密钥生成第

二验证码；如果所述第二验证码与所述第二认证码匹配，则所述 UE 对所述 N3IWF 安全认证成功。

在一些可选的方案中，所述 UE 的保留信息包括安全上下文信息，所述第一安全密钥为所述安全上下文信息中的 NAS 完整性密钥。

在一些可选的方案中，所述 UE 的保留信息包括安全上下文信息，所述第一安全密钥为根据所述安全上下文信中的安全密钥和第一新鲜保护参数派生的密钥。

在一些可选的方案中，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥，所述第一新鲜保护参数包括以下中的任意一项：计数器的计数值、第一随机数、UE 临时标识。

在一些可选的方案中，所述 AMF 指示信息用于指示与所述 UE 进行相互安全认证的第一 AMF，所述 AMF 指示信息包括 UE 临时标识，或者根据 UE 临时标识生成的网络接入标识 NAI 信息。

在一些可选的方案中，所述密钥标识信息包括 UE 临时标识，和/或，所述 UE 的安全上下文信息中的密钥标识符。

在一些可选的方案中，所述 UE 对所述 N3IWF 安全认证成功之后，所述处理器还用于：通过所述收发器向所述 N3IWF 发送第四请求消息，所述第四请求消息承载在因特网安全 IPsec 协议，所述第四请求消息携带有第三认证码和所述密钥标识信息，所述第三认证码用于所述 AMF 指示信息所指示的第一 AMF 对所述 UE 进行安全认证；通过所述收发器接收所述 N3IWF 发送的第四响应消息，所述第四响应消息承载在因特网安全 IPsec 协议，所述第四响应消息用于指示所述 UE 注册成功。

在一些可选的方案中，所述第一请求消息还携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证。

在一些可选的方案中，所述处理器还用于：根据所述 UE 的保留信息，确定 NAS 完整性密钥；根据所述 NAS 完整性密钥生成第三认证码，其中所述密钥标识信息还用于获取所述 NAS 完整性密钥。

在采用集成的单元的情况下，图 13 示出了上述实施例中所涉及的用户设备的一种可能的结构示意图。用户设备 12 包括：获取单元 120、确定单元 121、生成单元 122、发送单元 123 和接收单元 124。其中上述获取单元 120、确定单元 121、生成单元 122、发送单元 123 和接收单元 124 分别用于执行文本所描述的相关步骤，例如所述获取单元 120 用于获取上一次成功入网后，所述 UE 的保留信息；所述确定单元 121 用于根据所述 UE 的保留信息，确定接入和移动性管理网元 AMF 指示信息和第一安全密钥；所述生成单元 122 用于根据所述第一安全密钥生成第一认证码；所述发送单元 123 用于向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥；所述接收单元 124 用于接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息等。可选地根据结构本身还可以增加其他功能单元。

请参见图 14，图 14 示出了上述实施例中所涉及的用户设备（UE）的另一种可能的结构示意图。该用户设备 12 包括通信单元 1201，处理单元 1202，存储单元 1203。该通信单

元 1201 用于支持用户设备与上述实施例中的 3GPP 网络接入网或 non-3GPP 网络接入网，WLAN 接入点之间收发信息。处理单元 1202 还执行图 4 至图 11 中涉及用户设备的处理过程和/或用于本申请所描述的技术的其他过程。作为示例，处理单元 1202 用于支持用户设备执行图 4 中的过程 S102、S106-S108,和/或用于本文所描述的技术的其他过程。存储单元 1203 用于存储用户设备的程序代码和数据。

需要说明的是，本发明实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。本发明实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。例如，上述实施例中，接收单元和发送单元可以是同一个单元，也不同的单元。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

需要说明的是，图 12-图 14 所示的用户设备的具体实现还可以对应参照图 4-图 11 所述方法实施例的相应描述，此处不再赘述。

请参见图 15，图 15 是本发明实施例提供的一种非 3GPP 互通网元的结构示意图。如图 15，该非 3GPP 互通网元 14 包括收发器 601、存储器 602 和处理器 603（处理器 603 的数量可以一个或多个，图 14 中以一个处理器为例），在本发明的一些实施例中，收发器 601、存储器 602 和处理器 603 可通过总线或者其它方式连接，其中，图 15 中以通过总线连接为例。所述处理器 603 调用所述存储器 602 中的基于非 3GPP 网络的入网认证程序，用于执行如下操作：

通过所述收发器接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息；

通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标识信息对应的所述第一安全密钥；

根据所述第一安全密钥生成第一验证码；

如果所述第一认证码和所述第一验证码匹配，则通过所述收发器向所述 UE 发送第一响应消息。

在一些可选的方案中，所述处理器还用于：根据所述第一安全密钥生成第二认证码；通过所述收发器将所述第二认证码发送给所述 UE，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。

在一些可选的方案中，所述处理器通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体为：根据所述 AMF 指示信息，查找第一 AMF；向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息；所述处理器通过所述收发器接收所述密钥标识信息对应的所述第一安全密钥具体为：通过所述收发器接收所述第一 AMF 发送的所述第一安全密钥。

在一些可选的方案中，所述处理器通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体为：

在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息

和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥；所述处理器通过所述收发器接收所述密钥标识信息对应的所述第一安全密钥具体为：通过所述收发器接收所述第二 AMF 发送的所述第一安全密钥；所述第一安全密钥为所述第一 AMF 根据所述密钥标识信息确定的，或者所述第一安全密钥为所述第二 AMF 根据接收所述第一 AMF 发送的第一安全密钥信息生成的，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数。

在一些可选的方案中，所述处理器通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体为：在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥；所述处理器还用于：

通过所述收发器接收所述第一 AMF 通过所述第二 AMF 发送的重定向指示信息，所述重定向指示信息携带有所述第一 AMF 的地址信息，所述重定向指示信息用于指示所述 N3IWF 重新向所述第一 AMF 发送第二请求消息；根据所述重定向指示信息，向所述地址信息对应的第一 AMF 发送所述第二请求消息；所述处理器通过所述收发器接收所述密钥标识信息对应的所述第一安全密钥具体包括：通过所述收发器接收所述第一 AMF 发送的所述第一安全密钥。

在一些可选的方案中，所述处理器通过所述收发器向所述 UE 发送第一响应消息之后，所述处理器还用于：通过所述收发器接收所述 UE 发送的第四请求消息，该第四请求消息承载在因特网安全 IPsec 协议，所述第四请求消息携带有第三认证码和所述密钥标识信息，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证；通过所述收发器向所述第一 AMF 发送所述第四请求消息，并接收所述第一 AMF 基于所述第四请求消息返回的第四响应消息，该第四请求消息和该第四响应消息承载在 NG2 协议上；通过所述收发器向所述 UE 发送所述第四响应消息，该第四请求消息承载在因特网安全 IPsec 协议，所述第四响应消息用于指示所述 UE 注册成功。

在一些可选的方案中，所述第一请求消息还携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证；所述处理器还用于：通过所述收发器向第一 AMF 发送第三认证码。

在一些可选的方案中，所述密钥标识信息用于标识所述 UE 的安全上下文信息，所述第一安全密钥为所述安全上下文信息中的 NAS 完整性密钥。

在一些可选的方案中，所述密钥标识信息用于标识所述 UE 的安全上下文信息，所述第二请求消息还携带有第一新鲜保护参数；所述第一安全密钥为根据所述安全上下文信息中的安全密钥和第一新鲜保护参数派生的密钥。

在一些可选的方案中，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥，所述第一新鲜保护参数包括以下中的任意一项：计数器的计数值、第一随机数、UE 临时标识。

在一些可选的方案中，所述 AMF 指示信息用于指示与所述 UE 进行相互安全认证的第一 AMF，所述 AMF 指示信息包括 UE 临时标识、或者根据 UE 临时标识生成的 NAI 信息。

在一些可选的方案中，所述密钥标识信息包括所述 UE 临时标识和/或所述 UE 的安全

上下文信息中的密钥标识符。

在采用集成的单元的情况下，图 16 示出了上述实施例中所涉及的非 3GPP 互通网元的一种可能的结构示意图。非 3GPP 互通网元 14 包括：接收单元 130、发送单元 131、生成单元 132。其中上述接收单元 130、发送单元 131、生成单元 132 分别用于执行文本所描述的相关步骤，例如所述接收单元 130 用于接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息；所述发送单元 131 用于向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标识信息对应的所述第一安全密钥；所述生成单元 132 用于根据所述第一安全密钥生成第一验证码；所述发送单元 131 还用于如果所述第一认证码和所述第一验证码匹配，则通过所述收发器向所述 UE 发送第一响应消息等等，可选地根据结构本身还可以增加其他功能单元。

请参见图 17，图 17 示出了上述实施例中所涉及的非 3GPP 互通网元（N3IWF）的另一种可能的结构示意图。该非 3GPP 互通网元 14 包括通信单元 1401，处理单元 1402，存储单元 1403。该通信单元 1401 用于支持非 3GPP 互通网元与上述实施例中的用户设备和 non-3GPP 网络接入网中核心网网元（如 AMF），WLAN 接入点之间收发信息。处理单元 1402 还执行图 4 至图 11 中涉及用户设备的处理过程和/或用于本申请所描述的技术的其他过程。作为示例，处理单元 1402 用于支持非 3GPP 互通网元执行图 4 中的过程 S103-S105，和/或用于本文所描述的技术的其他过程。存储单元 1403 用于存储非 3GPP 互通网元的程序代码和数据。

需要说明的是，本发明实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。本发明实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。例如，上述实施例中，接收单元和发送单元可以是同一个单元，也不同的单元。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

需要说明的是，图 16-图 17 所示的非 3GPP 互通网元的具体实现还可以对应参照图 4-图 11 所述方法实施例的相应描述，此处不再赘述。

请参见图 18，图 18 是本发明实施例提供的一种接入和移动性管理网元的结构示意图。如图 18，该接入和移动性管理网元 16 包括收发器 701、存储器 702 和处理器 703（处理器 703 的数量可以一个或多个，图 16 中以一个处理器为例），在本发明的一些实施例中，收发器 701、存储器 702 和处理器 703 可通过总线或者其它方式连接，其中，图 18 中以通过总线连接为例。所述处理器 703 调用所述存储器 702 中的基于非 3GPP 网络的入网认证程序，用于执行如下操作：

通过所述收发器接收 N3IWF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息；

根据所述密钥标识信息，确定第一安全密钥；

通过所述收发器向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。

在一些可选的方案中，所述处理器通过所述收发器接收 N3IWF 发送的第二请求消息具体为：通过所述收发器接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二

AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的；所述处理器通过所述收发器向所述 N3IWF 发送第二响应消息具体为：向所述第二 AMF 发送的第三响应消息，以使所述第二 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息和所述第三响应消息分别携带有所述第一安全密钥。

在一些可选的方案中，所述处理器通过所述收发器接收 N3IWF 发送的第二请求消息具体为：通过所述收发器接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二 AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的；所述处理器通过所述收发器向所述 N3IWF 发送第二响应消息之前，所述处理器还用于：通过所述收发器通过所述第二 AMF 向所述 N3IWF 发送重定向指示信息，所述重定向指示信息用于指示所述 N3IWF 向所述第一 AMF 发送所述第二请求消息；通过所述收发器接收所述 N3IWF 基于所述重定向指示信息发送的所述第二请求消息。

在一些可选的方案中，所述密钥标识信息用于标识所述 UE 的安全上下文信息，所述第一安全密钥为所述安全上下文信息中的 NAS 完整性密钥。

在一些可选的方案中，所述密钥标识信息用于标识所述 UE 的安全上下文信息，所述第二请求消息还携带有第一新鲜保护参数；所述第一安全密钥为根据所述安全上下文信息中的安全密钥和第一新鲜保护参数。

在一些可选的方案中，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥，所述第一新鲜保护参数包括以下中的任意一项：计数器的计数值、第一随机数、UE 临时标识。

在一些可选的方案中，所述处理器通过所述收发器向所述 N3IWF 发送第二响应消息之后，所述处理器还用于：通过所述收发器接收所述 N3IWF 发送的第四请求消息，所述第四请求消息携带有第三认证码和密钥标识信息，所述第三认证码用于所述第一 AMF 对所述 UE 进行安全认证；根据所述密钥标识信息，确定 NAS 完整性密钥；根据所述 NAS 完整性密钥生成第三验证码；

如果所述第三验证码和所述第三认证码匹配，则通过所述收发器向所述 N3IWF 发送第四响应消息，所述第四响应消息用于指示所述 UE 注册成功。

在一些可选的方案中，所述第二请求消息还携带有第三认证码；所述根据所述密钥标识信息，确定第一安全密钥之前，所述处理器还用于：根据所述密钥标识信息，确定 NAS 完整性密钥；根据所述 NAS 完整性密钥生成第三验证码；如果所述第三验证码和所述第三认证码匹配，则执行所述根据所述密钥标识信息，确定第一安全密钥的步骤。

在采用集成的单元的情况下，图 19 示出了上述实施例中所涉及的接入和移动性管理网元的一种可能的结构示意图。接入和移动性管理网元 16 包括：接收单元 140、确定单元 141 和发送单元 132。其中上述接收单元 140、确定单元 141 和发送单元 132 分别用于执行文本所描述的相关步骤，例如接收单元 140 用于接收 N3IWF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息；确定单元 141 用于根据所述密钥标识信息，确定第一安全密钥；发送单元 132 用于向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥等等。可选地根据结构本身还可以增加其他功能单元。

请参见图 20，图 20 示出了上述实施例中所涉及的接入和移动性管理网元（AMF）的另一种可能的结构示意图。该接入和移动性管理网元 16 包括通信单元 1601，处理单元 1602，

存储单元 1603。该通信单元 1601 用于支持接入和移动性管理网元与上述实施例中的用户设备，non-3GPP 网络接入网中的一些功能网元（如 N3IWF）之间收发信息。处理单元 1602 还执行图 4 至图 11 中涉及用户设备的处理过程和/或用于本申请所描述的技术的其他过程。作为示例，处理单元 1602 用于支持非 3GPP 互通网元执行图 5 中的过程 S202、S203,和/或用于本文所描述的技术的其他过程。存储单元 1603 用于存储接入和移动性管理网元的程序代码和数据。

需要说明的是，本发明实施例中对单元的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。本发明实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。例如，上述实施例中，接收单元和发送单元可以是同一个单元，也不同的单元。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

需要说明的是，图 18-图 20 所示的接入和移动性管理网元的具体实现还可以对应参照图 4-图 11 所述方法实施例的相应描述，此处不再赘述。

请参见图 21，图 21 是本发明实施例提供的一种基于非 3GPP 网络的入网认证系统的结构示意图。该系统 18 包括非 3GPP 互通网元 14 和接入和移动性管理网元 16；其中，

所述非 3GPP 互通网元 14 可以是图 15-图 17 任一实施例中所描述的的非 3GPP 互通网元，这里不再赘述；

所述接入和移动性管理网元 16 可以是图 18-图 20 任一实施例中所描述的接入和移动性管理网元，这里不再赘述。

在一些可选的方案中，该系统还包括用户设备 12；其中，所述用户设备 12 可以是图 12-图 14 任一实施例中所描述的用户设备，这里不再赘述。

通过实施本发明实施例，能够减少现有技术中 UE 上一次成功入网后当前通过 non-3GPP 进行入网认证的流程步骤，节省入网认证时间，实现 UE 的快速入网。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

权 利 要 求

1、一种基于非 3GPP 网络的入网认证方法，其特征在于，所述方法包括:

用户设备 UE 获取上一次成功入网后，所述 UE 的保留信息;

根据所述 UE 的保留信息，确定接入和移动性管理网元 AMF 指示信息和第一安全密钥;

根据所述第一安全密钥生成第一认证码;

向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥;

接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息。

2、根据权利要求 1 所述的方法，其特征在于，所述第一响应消息携带有第二认证码，所述第二认证码为所述 N3IWF 根据所述第一安全密钥生成的；所述方法还包括:

根据所述第一安全密钥生成第二验证码;

如果所述第二验证码与所述第二认证码匹配，则所述 UE 对所述 N3IWF 安全认证成功。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述 UE 的保留信息包括安全上下文信息，所述第一安全密钥为根据所述安全上下文信中的安全密钥和第一新鲜保护参数派生的密钥。

4、根据权利要求 3 所述的方法，其特征在于，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥，所述第一新鲜保护参数包括以下中的任意一项：计数器的计数值、第一随机数、UE 临时标识。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述 AMF 指示信息用于指示与所述 UE 进行相互安全认证的第一 AMF，所述 AMF 指示信息包括 UE 临时标识，或者根据 UE 临时标识生成的网络接入标识 NAI 信息。

6、根据权利要求 1-5 任一项所述的方法，其特征在于，所述密钥标识信息包括 UE 临时标识，和/或，所述 UE 的安全上下文信息中的密钥标识符。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述第一请求消息还携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证。

8、一种基于非 3GPP 网络的入网认证方法，其特征在于，所述方法包括:

N3IWF 接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息;

向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标

识信息对应的所述第一安全密钥;

根据所述第一安全密钥生成第一验证码;

如果所述第一认证码和所述第一验证码匹配，则向所述 UE 发送第一响应消息。

9、根据权利要求 8 所述的方法，其特征在于，所述方法还包括:

根据所述第一安全密钥生成第二认证码;

将所述第二认证码发送给所述 UE，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。

10、根据权利要求 8 所述的方法，其特征在于，所述向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体包括:

根据所述 AMF 指示信息，确定第一 AMF;

向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息;

所述接收所述密钥标识信息对应的所述第一安全密钥具体包括:

接收所述第一 AMF 发送的所述第一安全密钥。

11、根据权利要求 8 所述的方法，其特征在于，所述向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体包括:

在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥;

所述接收所述密钥标识信息对应的所述第一安全密钥具体包括:

接收所述第二 AMF 发送的所述第一安全密钥; 所述第一安全密钥为所述第一 AMF 根据所述密钥标识信息确定的，或者所述第一安全密钥为所述第二 AMF 根据接收所述第一 AMF 发送的第一安全密钥信息生成的，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数。

12、根据权利要求 8-11 任一项所述的方法，其特征在于，所述第一请求消息携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证; 则所述方法还包括:向第一 AMF 发送第三认证码。

13、一种基于非 3GPP 网络的入网认证方法，其特征在于，所述方法包括:

第一 AMF 接收 N3IWF 发送的第二请求消息,所述第二请求消息携带有密钥标识信息;

根据所述密钥标识信息，确定第一安全密钥;

向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。

14、根据权利要求 13 所述的方法，其特征在于，所述第一 AMF 接收 N3IWF 发送的

第二请求消息具体包括:

接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二 AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的;

所述向所述 N3IWF 发送第二响应消息具体包括:

向所述第二 AMF 发送的第三响应消息，以使所述第二 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息和所述第三响应消息分别携带有所述第一安全密钥。

15、根据权利要求 13 或 14 所述的方法，其特征在于，所述第二请求消息还携带有第三认证码；所述根据所述密钥标识信息，确定第一安全密钥之前，还包括:

根据所述密钥标识信息，确定 NAS 完整性密钥;

根据所述 NAS 完整性密钥生成第三验证码;

如果所述第三验证码和所述第三认证码匹配，则执行所述根据所述密钥标识信息，确定第一安全密钥的步骤。

16、一种用户设备，其特征在于，所述用户设备包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行如下操作:

获取上一次成功入网后，所述 UE 的保留信息;

根据所述 UE 的保留信息,确定接入和移动性管理网元 AMF 指示信息和第一安全密钥;

根据所述第一安全密钥生成第一认证码;

通过所述收发器向非 3GPP 互通网元 N3IWF 发送第一请求消息，所述第一请求消息携带有所述第一认证码、所述 AMF 指示信息和密钥标识信息，所述第一认证码用于所述 N3IWF 对所述 UE 进行安全认证，所述密钥标识信息用于获取所述第一安全密钥;

通过所述收发器接收所述 N3IWF 基于所述第一请求消息返回的第一响应消息。

17、根据权利要求 16 所述的用户设备，其特征在于，所述第一响应消息携带有第二认证码，所述第二认证码为所述 N3IWF 根据所述第一安全密钥生成的；所述处理器还用于:

根据所述第一安全密钥生成第二验证码;

如果所述第二验证码与所述第二认证码匹配,则所述 UE 对所述 N3IWF 安全认证成功。

18、根据权利要求 16 或 17 所述的用户设备，其特征在于，所述 UE 的保留信息包括安全上下文信息，所述第一安全密钥为根据所述安全上下文信中的安全密钥和第一新鲜保护参数派生的密钥。

19、根据权利要求 18 所述的用户设备，其特征在于，所述安全密钥包括 Kseaf 密钥或 Kamf 密钥,所述第一新鲜保护参数包括以下中的任意一项:计数器的计数值、第一随机数、UE 临时标识。

20、根据权利要求 16-19 任一项所述的用户设备，其特征在于，所述 AMF 指示信息用于指示与所述 UE 进行相互安全认证的第一 AMF，所述 AMF 指示信息包括 UE 临时标识，或者根据 UE 临时标识生成的网络接入标识 NAI 信息。

21、根据权利要求 16-20 任一项所述的用户设备，其特征在于，所述密钥标识信息包括 UE 临时标识，和/或，所述 UE 的安全上下文信息中的密钥标识符。

22、根据权利要求 16-21 任一项所述的用户设备，其特征在于，所述第一请求消息还携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证。

23、一种非 3GPP 互通网元，其特征在于，所述非 3GPP 互通网元包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行如下操作：

通过所述收发器接收 UE 发送的第一请求消息，所述第一请求消息携带有第一认证码、AMF 指示信息和密钥标识信息；

通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息，并接收所述密钥标识信息对应的所述第一安全密钥；

根据所述第一安全密钥生成第一验证码；

如果所述第一认证码和所述第一验证码匹配，则通过所述收发器向所述 UE 发送第一响应消息。

24、根据权利要求 23 所述的非 3GPP 互通网元，其特征在于，所述处理器还用于：

根据所述第一安全密钥生成第二认证码；

通过所述收发器将所述第二认证码发送给所述 UE，所述第二认证码用于所述 UE 对所述 N3IWF 进行安全认证。

25、根据权利要求 23 所述的非 3GPP 互通网元，其特征在于，所述处理器通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体为：

根据所述 AMF 指示信息，确定第一 AMF；

向所述第一 AMF 发送第二请求消息，所述第二请求消息携带有所述密钥标识信息；

所述处理器通过所述收发器接收所述密钥标识信息对应的所述第一安全密钥具体为：

通过所述收发器接收所述第一 AMF 发送的所述第一安全密钥。

26、根据权利要求 23 所述的非 3GPP 互通网元，其特征在于，所述处理器通过所述收发器向所述 AMF 指示信息所指示的第一 AMF 发送所述密钥标识信息具体为：

在没有查找到所述 AMF 指示信息所指示的第一 AMF 的情况下，向第二 AMF 发送第三请求消息，以使所述第二 AMF 向所述第一 AMF 发送第二请求消息，所述第二请求消息

和所述第三请求消息分别携带有所述密钥标识信息，所述第二请求消息用于获取验证所述第一认证码的第一安全密钥；

所述处理器通过所述收发器接收所述密钥标识信息对应的所述第一安全密钥具体为：

通过所述收发器接收所述第二 AMF 发送的所述第一安全密钥；所述第一安全密钥为所述第一 AMF 根据所述密钥标识信息确定的，或者所述第一安全密钥为所述第二 AMF 根据接收所述第一 AMF 发送的第一安全密钥信息生成的，所述第一安全密钥信息包括用于派生第一安全密钥的派生参数。

27、根据权利要求 23-26 任一项所述的非 3GPP 互通网元，其特征在于，所述第一请求消息携带有第三认证码，所述第三认证码用于第一 AMF 对所述 UE 进行安全认证；所述处理器还用于：

通过所述收发器向第一 AMF 发送第三认证码。

28、一种接入和移动性管理网元，其特征在于，所述接入和移动性管理网元包括处理器、存储器以及收发器，其中，所述存储器用于存储基于非 3GPP 网络的入网认证程序代码，所述处理器用于调用所述基于非 3GPP 网络的入网认证程序代码来执行如下操作：

通过所述收发器接收 N3IWF 发送的第二请求消息，所述第二请求消息携带有密钥标识信息；

根据所述密钥标识信息，确定第一安全密钥；

通过所述收发器向所述 N3IWF 发送第二响应消息，所述第二响应消息携带有所述第一安全密钥。

29、根据权利要求 28 所述的接入和移动性管理网元，其特征在于，所述处理器通过所述收发器接收 N3IWF 发送的第二请求消息具体为：

通过所述收发器接收第二 AMF 发送的第二请求消息，所述第二请求消息为所述第二 AMF 根据接收的所述 N3IWF 发送的第三请求消息所发出的；

所述处理器通过所述收发器向所述 N3IWF 发送第二响应消息具体为：

向所述第二 AMF 发送的第三响应消息，以使所述第二 AMF 向所述 N3IWF 发送第二响应消息，所述第二响应消息和所述第三响应消息分别携带有所述第一安全密钥。

30、根据权利要求 28 或 29 所述的接入和移动性管理网元，其特征在于，所述第二请求消息还携带有第三认证码；所述根据所述密钥标识信息，确定第一安全密钥之前，所述处理器还用于：

根据所述密钥标识信息，确定 NAS 完整性密钥；

根据所述 NAS 完整性密钥生成第三验证码；

如果所述第三验证码和所述第三认证码匹配，则执行所述根据所述密钥标识信息，确定第一安全密钥的步骤。

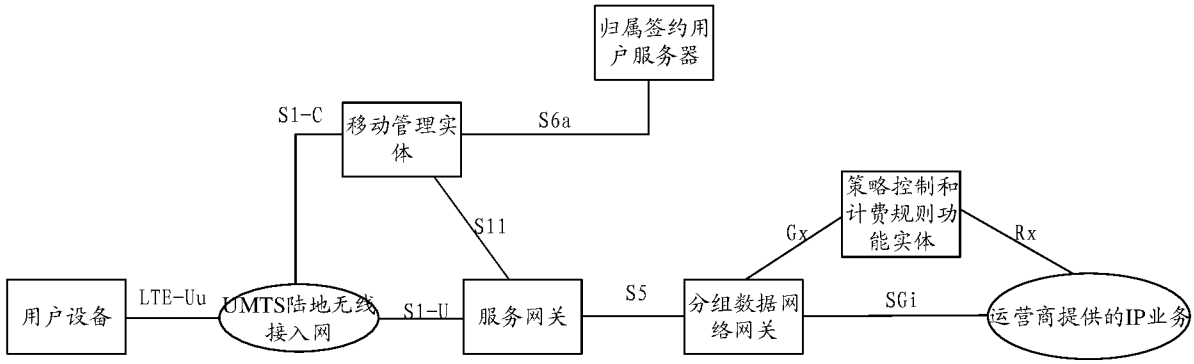

归属签约用户服务器
S1-C
移动管理实体
S6a
S11
策略控制和计费规则功能实体
Gx
Rx
用户设备
LTE-Uu
UMTS陆地无线接入网
S1-U
服务网关
S5
分组数据网络网关
SGi
运营商提供的IP业务

图 1

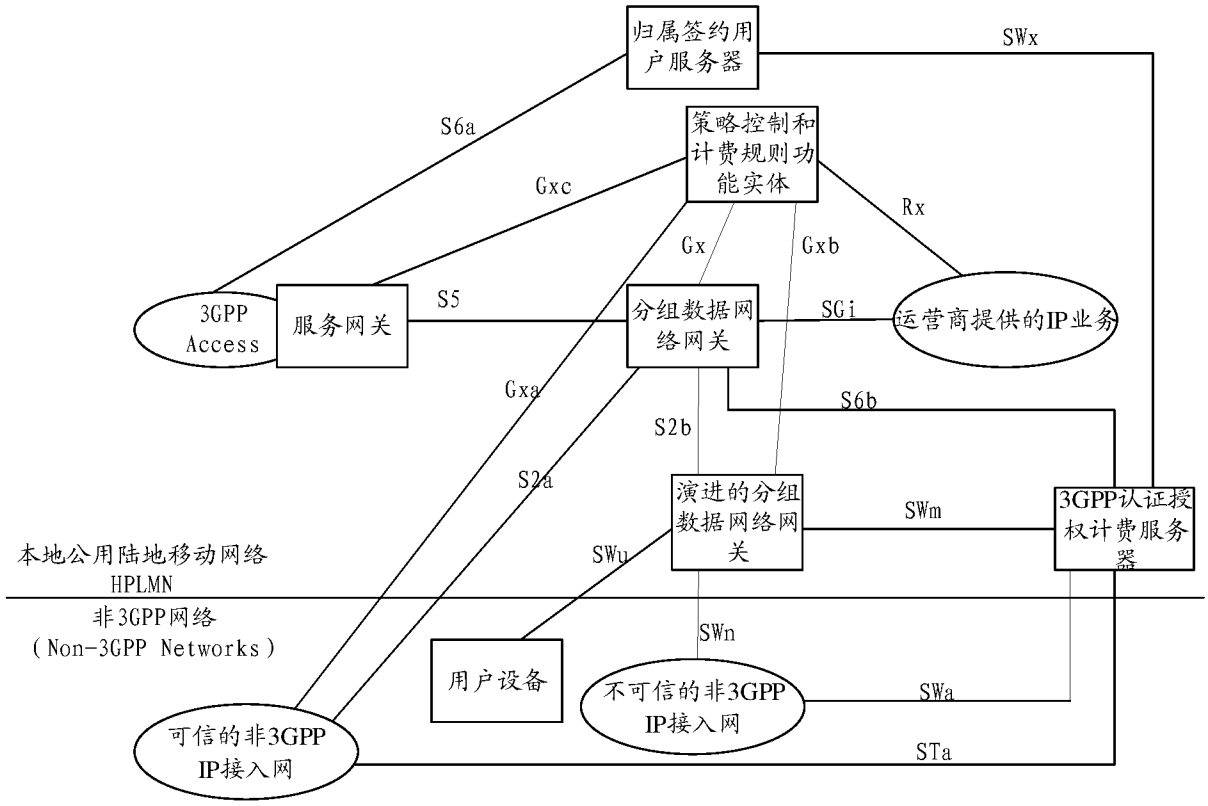

归属签约用户服务器
SWx
S6a
策略控制和计费规则功能实体
Gxc
Rx
Gx
Gxb
3GPP Access
服务网关
S5
分组数据网络网关
SGi
运营商提供的IP业务
Gxa
S6b
S2b
S2a
演进的分组数据网络网关
SWm
3GPP认证授权计费服务器
本地公用陆地移动网络
HPLMN
SWu
非3GPP网络
(Non-3GPP Networks)
SWn
用户设备
不可信的非3GPP IP接入网
SWa
可信的非3GPP IP接入网
STa

图 2

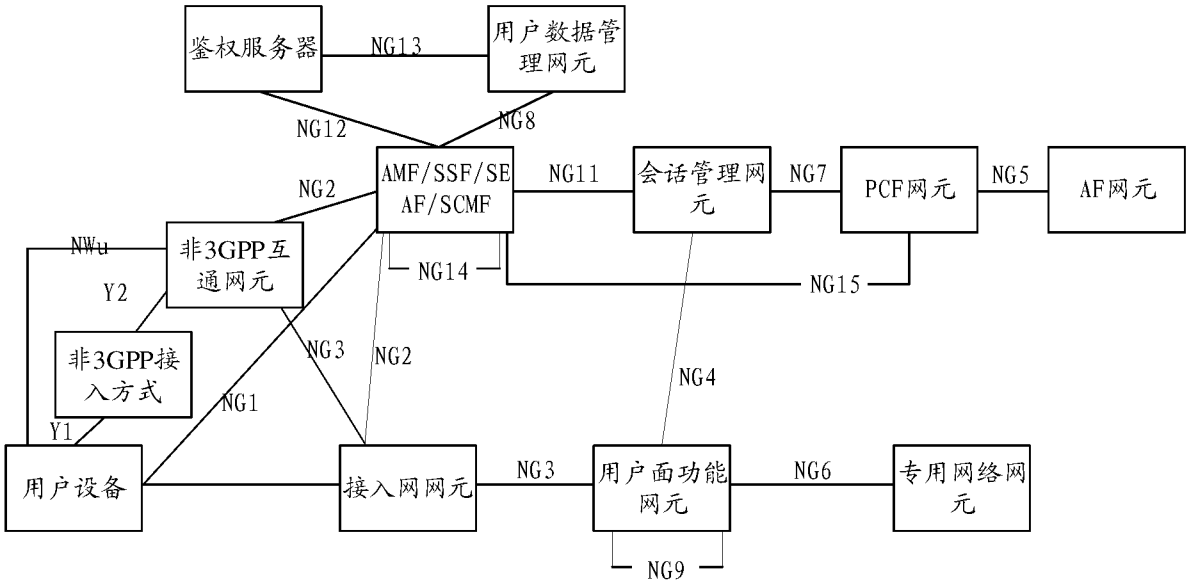

鉴权服务器
NG13
用户数据管理网元
NG12
NG8
AMF/SSF/SEAF/SCMF
NG11
会话管理网元
NG7
PCF网元
NG5
AF网元
NG2
NWu
非3GPP互通网元
NG14
NG15
Y2
非3GPP接入方式
NG3
NG2
NG4
NG1
Y1
用户设备
接入网网元
NG3
用户面功能网元
NG6
专用网络网元
NG9

图 3

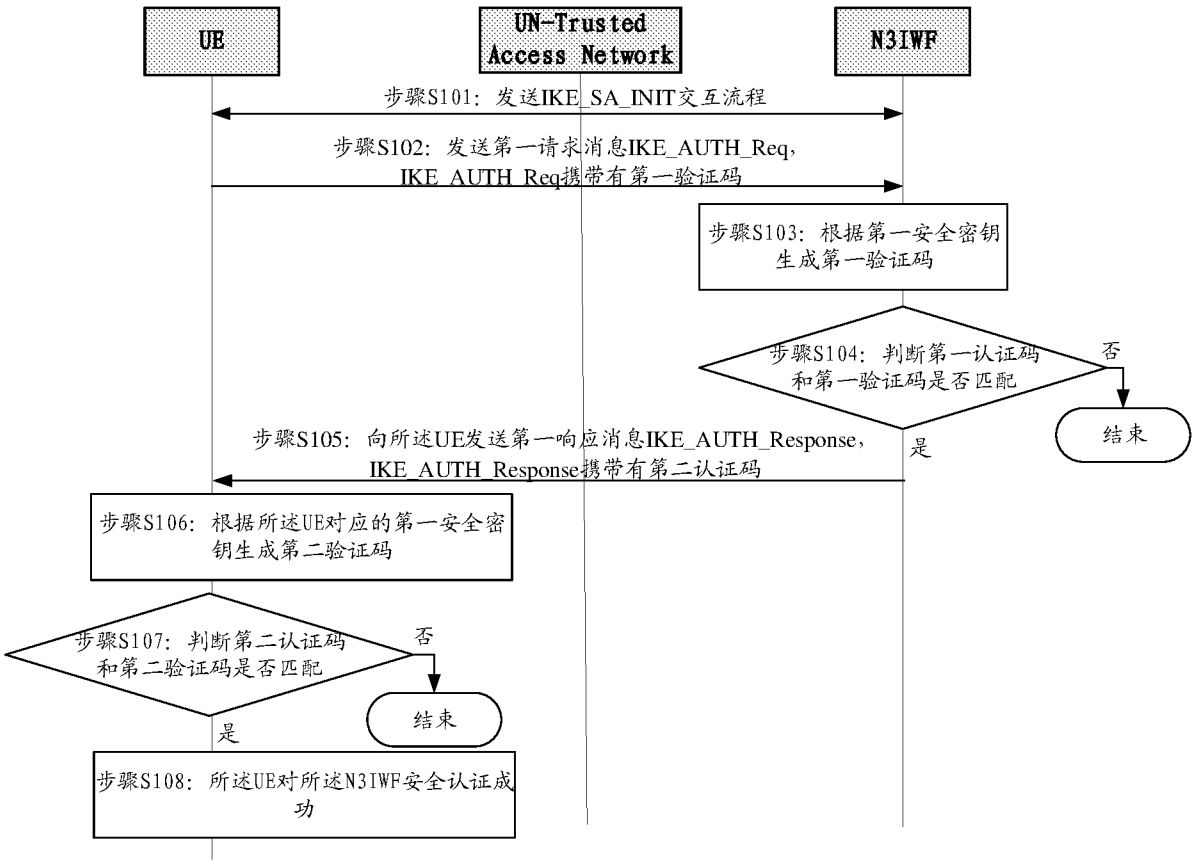

UE
UN-Trusted Access Network
N3IWF
步骤S101：发送IKE_SA_INIT交互流程
步骤S102：发送第一请求消息IKE_AUTH_Req，IKE_AUTH_Req携带有第一验证码
步骤S103：根据第一安全密钥生成第一验证码
步骤S104：判断第一认证码和第一验证码是否匹配
否
结束
是
步骤S105：向所述UE发送第一响应消息IKE_AUTH_Response，IKE_AUTH_Response携带有第二认证码
步骤S106：根据所述UE对应的第一安全密钥生成第二验证码
步骤S107：判断第二认证码和第二验证码是否匹配
否
结束
是
步骤S108：所述UE对所述N3IWF安全认证成功

图 4

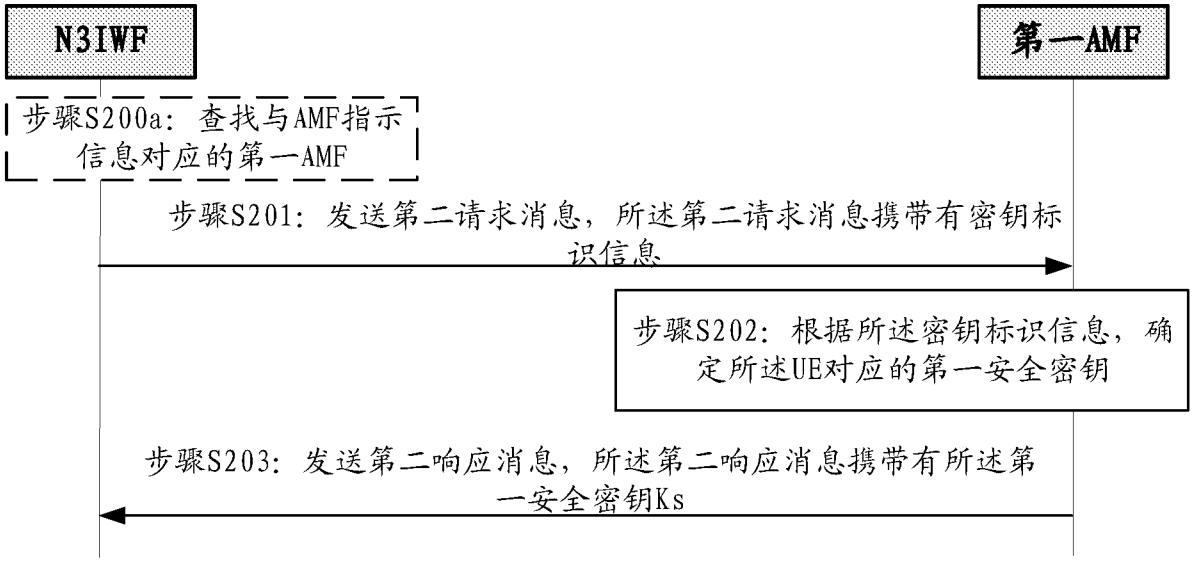

N3IWF
第一AMF
步骤S200a：查找与AMF指示信息对应的第一AMF
步骤S201：发送第二请求消息，所述第二请求消息携带有密钥标识信息
步骤S202：根据所述密钥标识信息，确定所述UE对应的第一安全密钥
步骤S203：发送第二响应消息，所述第二响应消息携带有所述第一安全密钥Ks

图 5

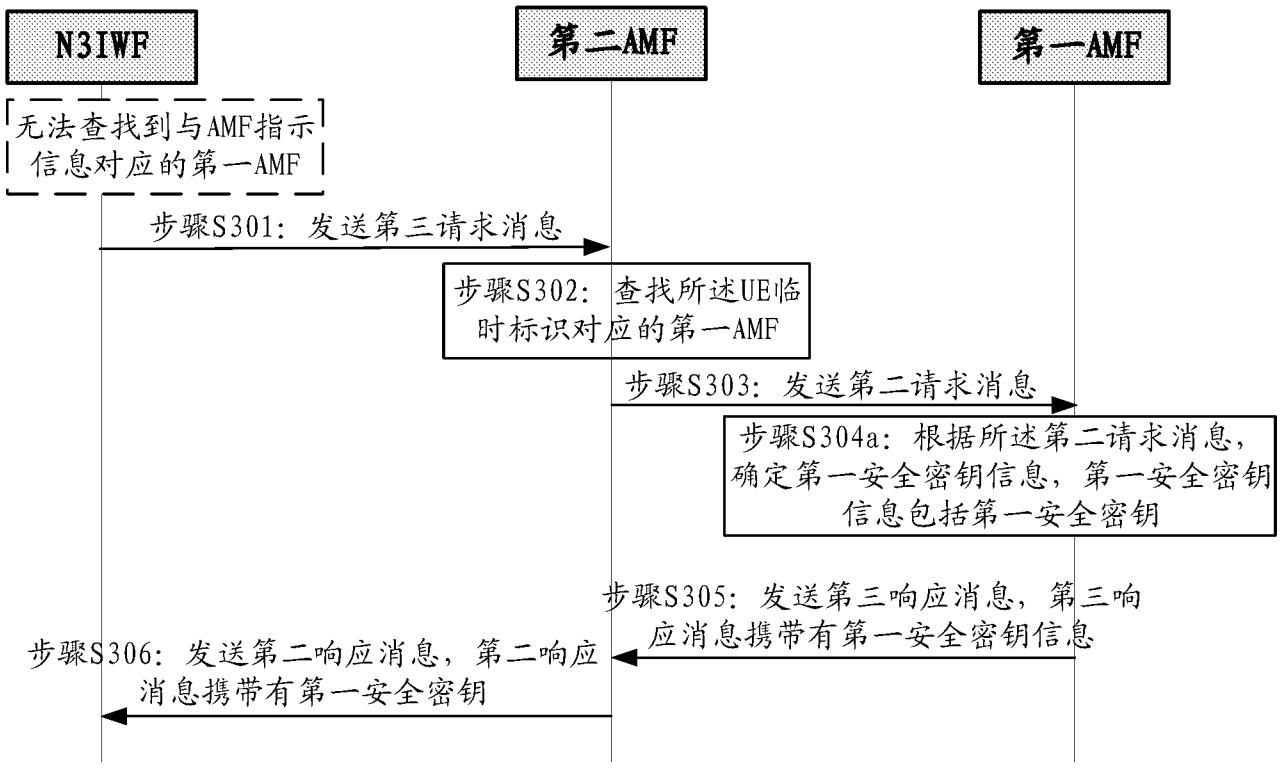

N3IWF
第二AMF
第一AMF
无法查找到与AMF指示信息对应的第一AMF
步骤S301：发送第三请求消息
步骤S302：查找所述UE临时标识对应的第一AMF
步骤S303：发送第二请求消息
步骤S304a：根据所述第二请求消息，确定第一安全密钥信息，第一安全密钥信息包括第一安全密钥
步骤S305：发送第三响应消息，第三响应消息携带有第一安全密钥信息
步骤S306：发送第二响应消息，第二响应消息携带有第一安全密钥

图 6

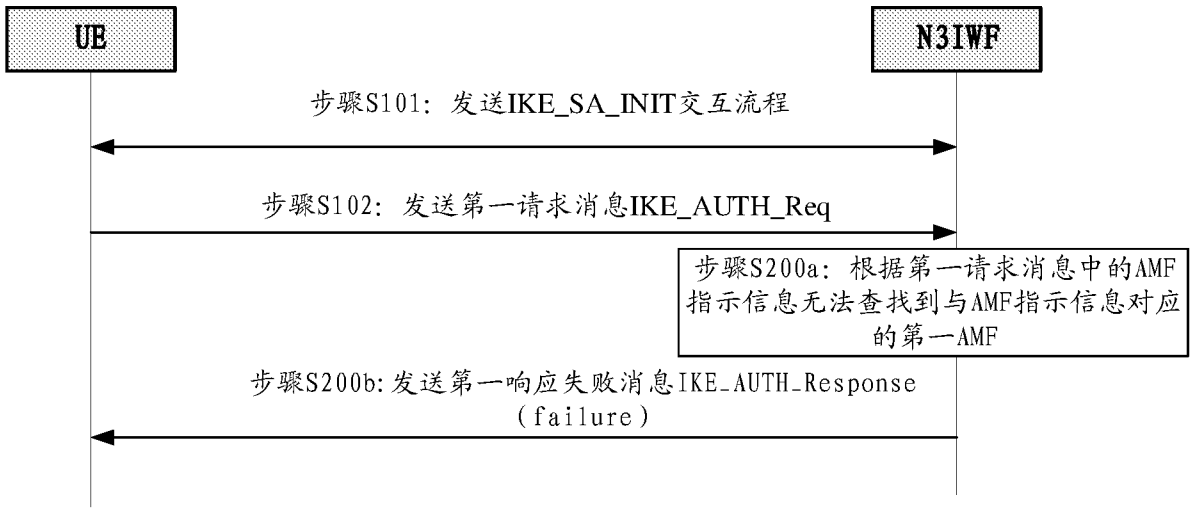

UE
N3IWF
步骤S101：发送IKE_SA_INIT交互流程
步骤S102：发送第一请求消息IKE_AUTH_Req
步骤S200a：根据第一请求消息中的AMF指示信息无法查找到与AMF指示信息对应的第一AMF
步骤S200b:发送第一响应失败消息IKE_AUTH_Response (failure)

图 7

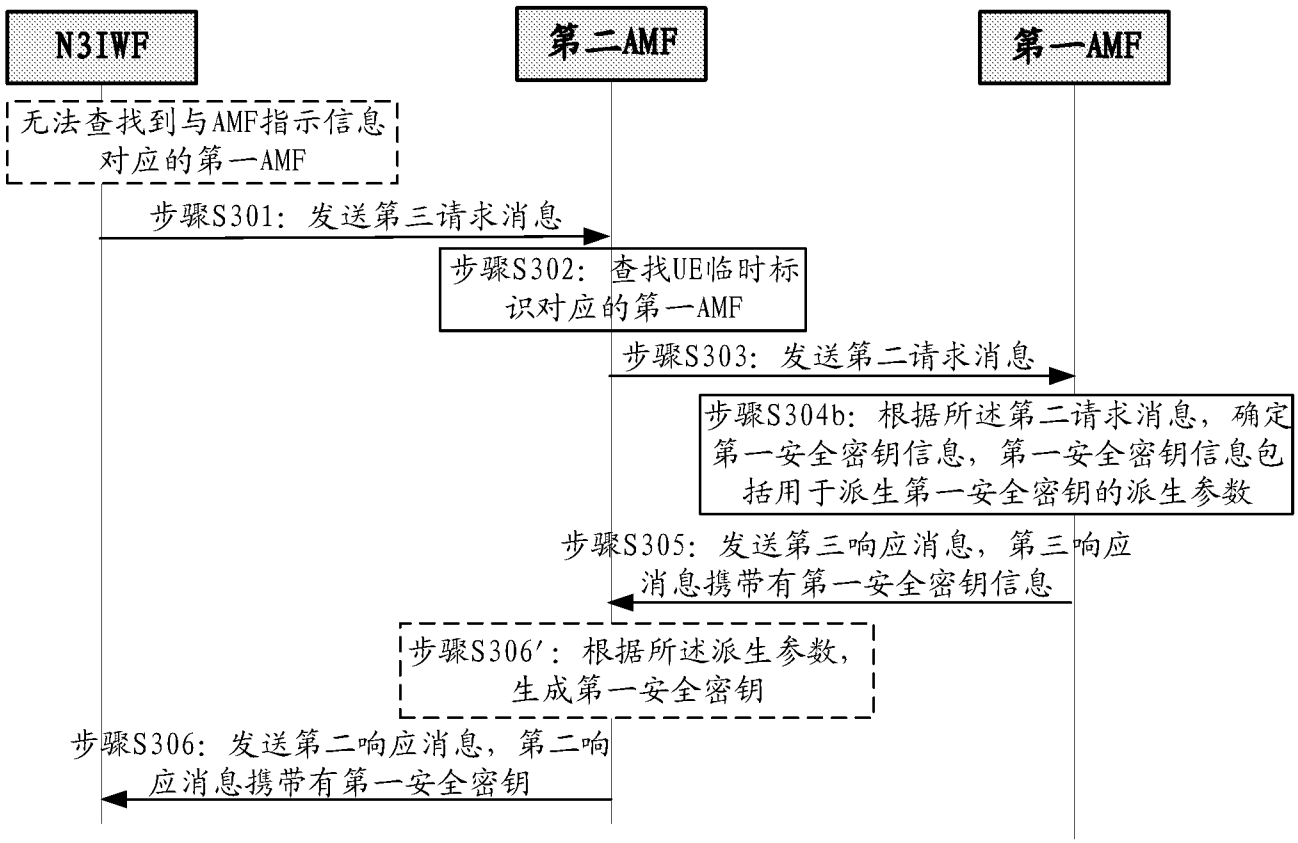

N3IWF
第二AMF
第一AMF
无法查找到与AMF指示信息对应的第一AMF
步骤S301：发送第三请求消息
步骤S302：查找UE临时标识对应的第一AMF
步骤S303：发送第二请求消息
步骤S304b：根据所述第二请求消息，确定第一安全密钥信息，第一安全密钥信息包括用于派生第一安全密钥的派生参数
步骤S305：发送第三响应消息，第三响应消息携带有第一安全密钥信息
步骤S306′：根据所述派生参数，生成第一安全密钥
步骤S306：发送第二响应消息，第二响应消息携带有第一安全密钥

图 8

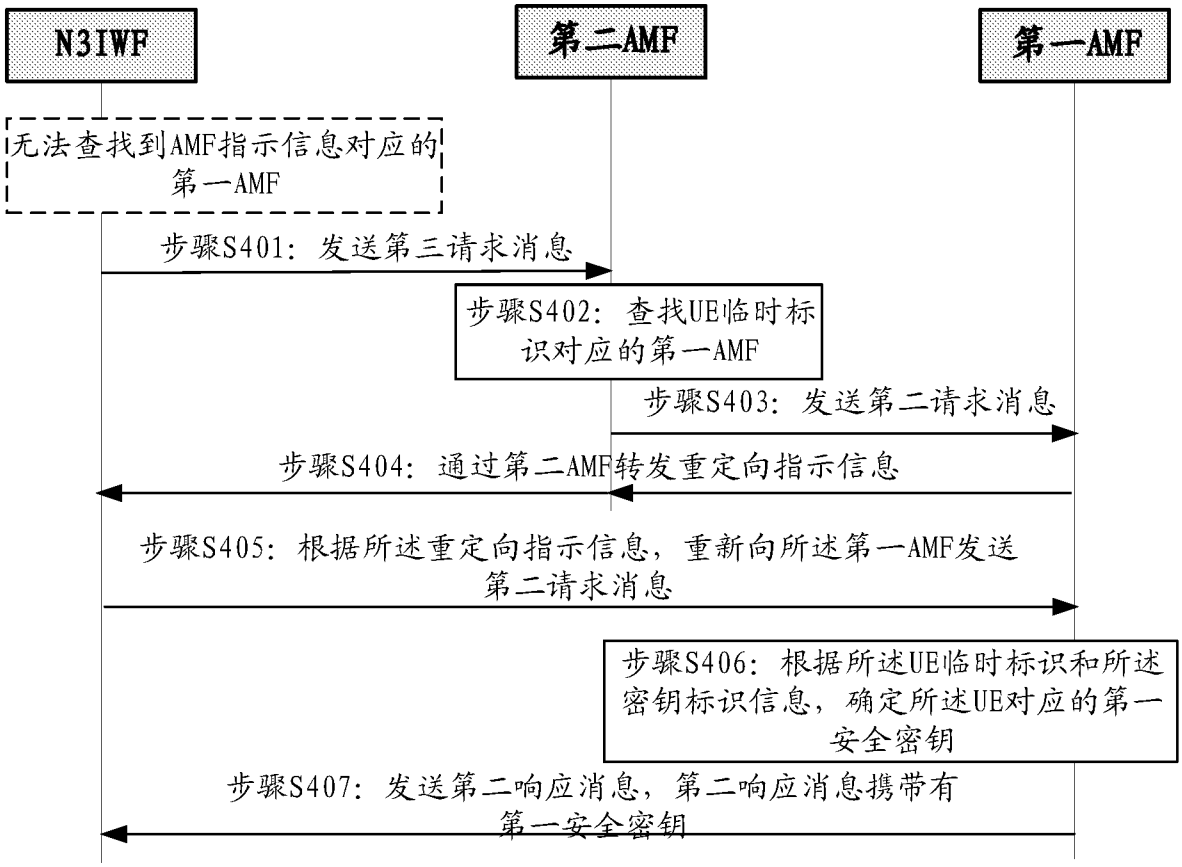

N3IWF
第二AMF
第一AMF
无法查找到AMF指示信息对应的第一AMF
步骤S401：发送第三请求消息
步骤S402：查找UE临时标识对应的第一AMF
步骤S403：发送第二请求消息
步骤S404：通过第二AMF转发重定向指示信息
步骤S405：根据所述重定向指示信息，重新向所述第一AMF发送第二请求消息
步骤S406：根据所述UE临时标识和所述密钥标识信息，确定所述UE对应的第一安全密钥
步骤S407：发送第二响应消息，第二响应消息携带有第一安全密钥

图 9

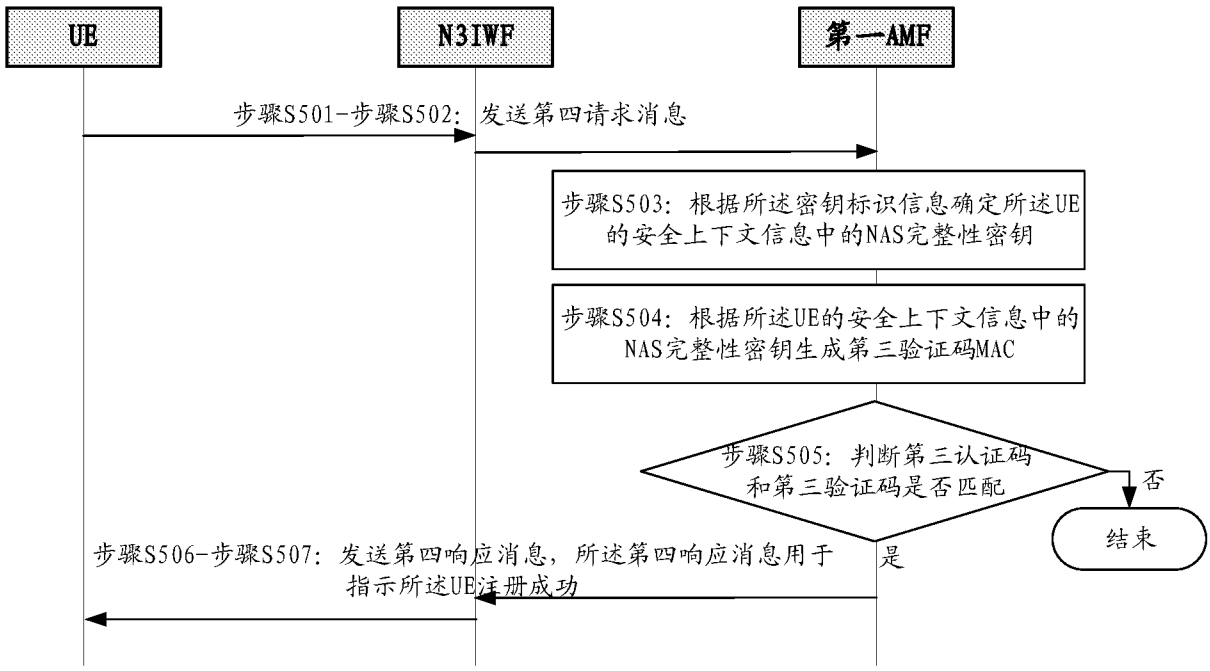

UE
N3IWF
第一AMF
步骤S501-步骤S502：发送第四请求消息
步骤S503：根据所述密钥标识信息确定所述UE的安全上下文信息中的NAS完整性密钥
步骤S504：根据所述UE的安全上下文信息中的NAS完整性密钥生成第三验证码MAC
步骤S505：判断第三认证码和第三验证码是否匹配
否
结束
是
步骤S506-步骤S507：发送第四响应消息，所述第四响应消息用于指示所述UE注册成功

图 10

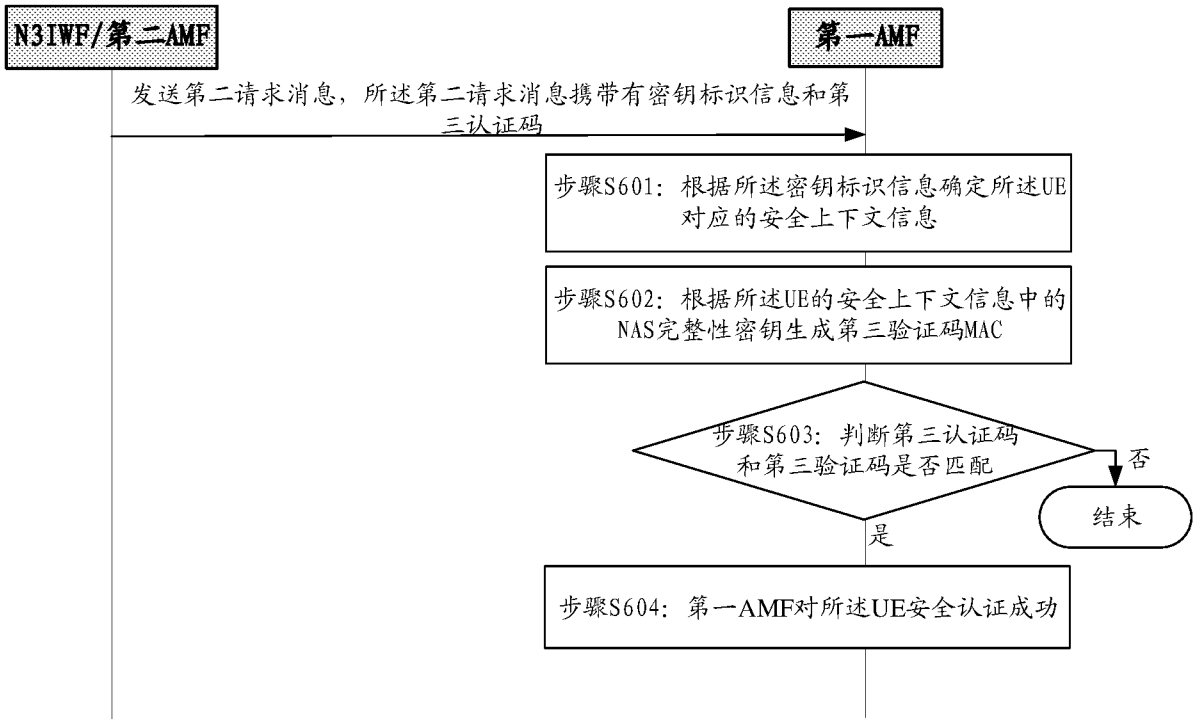

N3IWF/第二AMF
第一AMF
发送第二请求消息，所述第二请求消息携带有密钥标识信息和第三认证码
步骤S601：根据所述密钥标识信息确定所述UE对应的安全上下文信息
步骤S602：根据所述UE的安全上下文信息中的NAS完整性密钥生成第三验证码MAC
步骤S603：判断第三认证码和第三验证码是否匹配
否
结束
是
步骤S604：第一AMF对所述UE安全认证成功

图 11

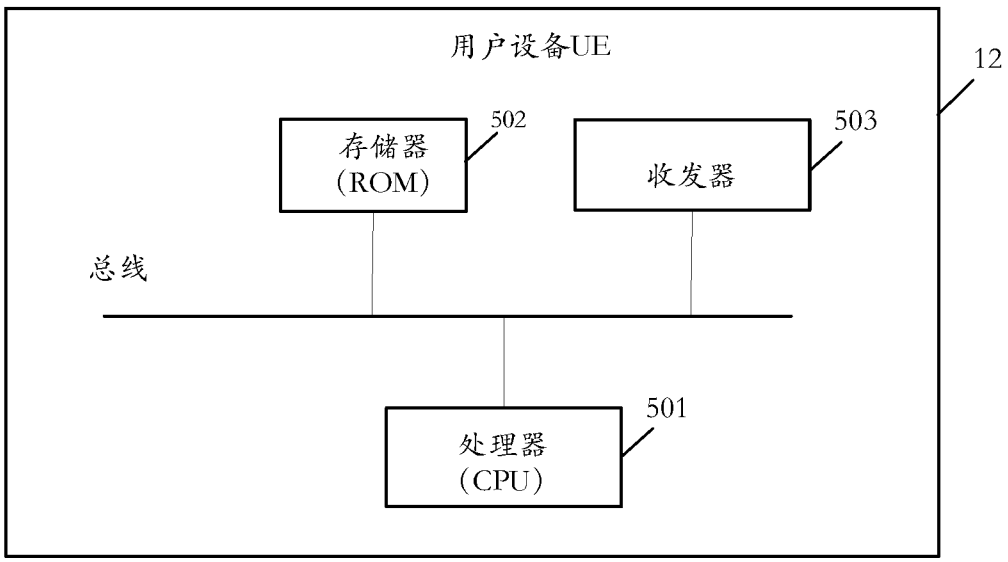

用户设备UE
12
存储器
(ROM)
502
收发器
503
总线
处理器
(CPU)
501

图 12

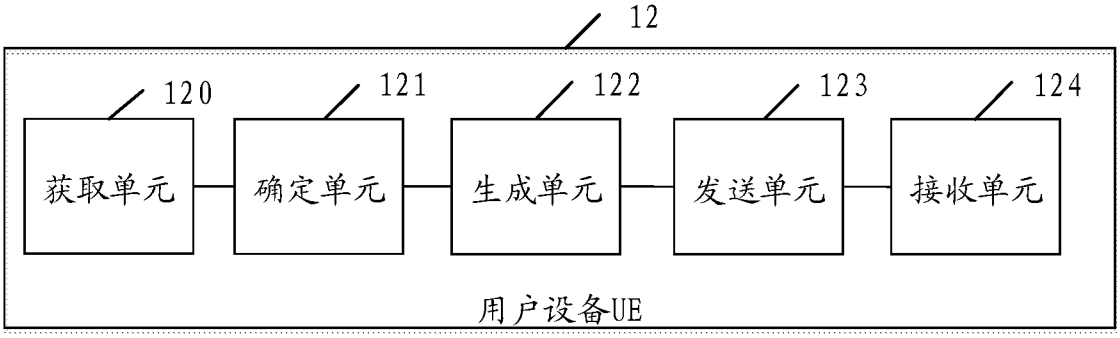

12
120
121
122
123
124
获取单元
确定单元
生成单元
发送单元
接收单元
用户设备UE

图 13

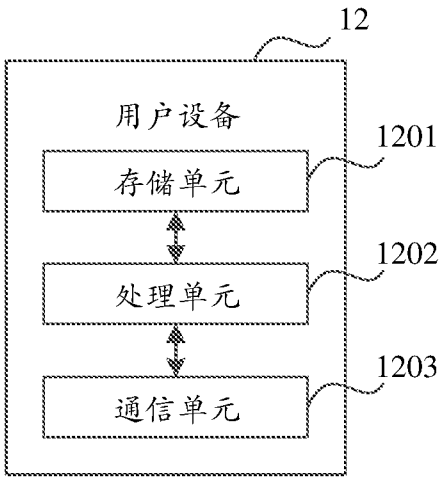

12
用户设备
1201
存储单元
1202
处理单元
1203
通信单元

图 14

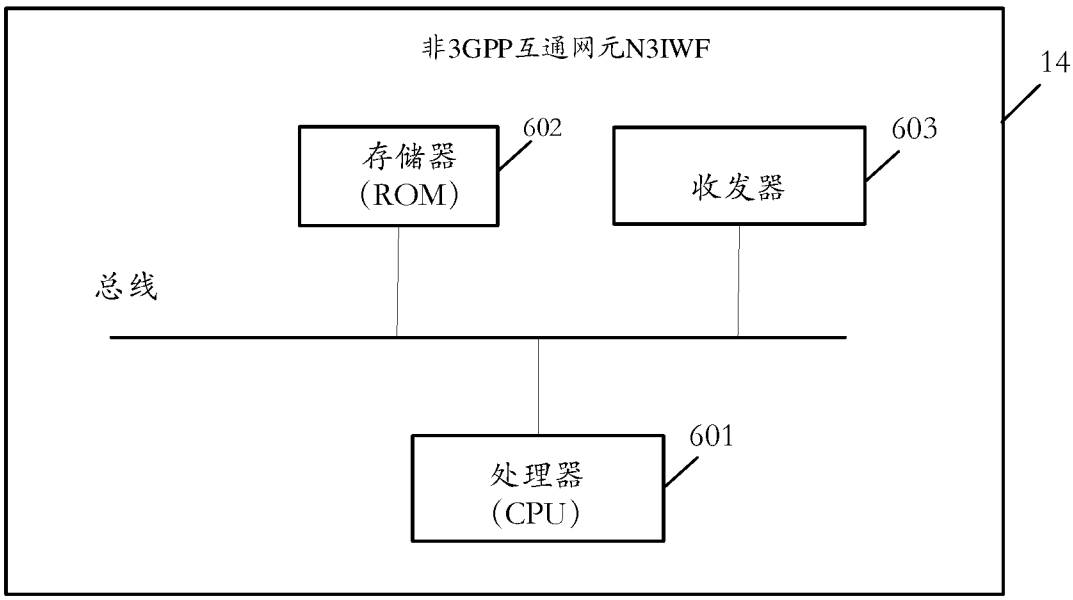

非3GPP互通网元N3IWF
14
602
存储器
(ROM)
603
收发器
总线
601
处理器
(CPU)

图 15

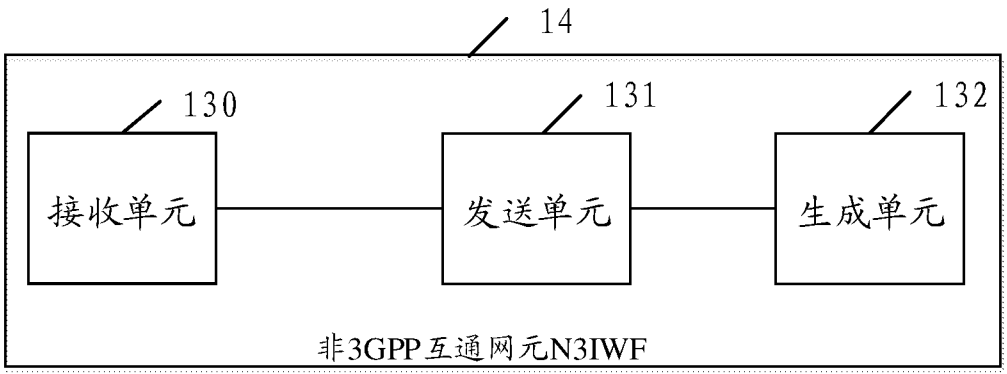

14
130
接收单元
131
发送单元
132
生成单元
非3GPP互通网元N3IWF

图 16

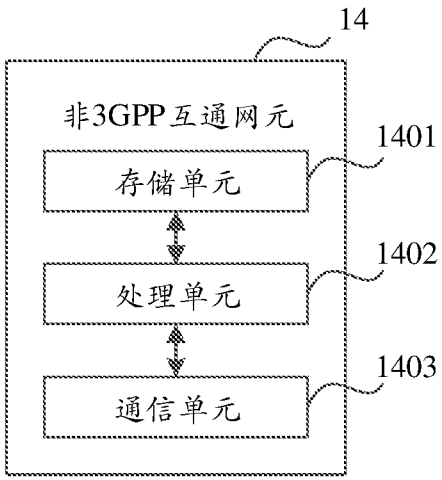

14
非3GPP互通网元
1401
存储单元
1402
处理单元
1403
通信单元

图 17

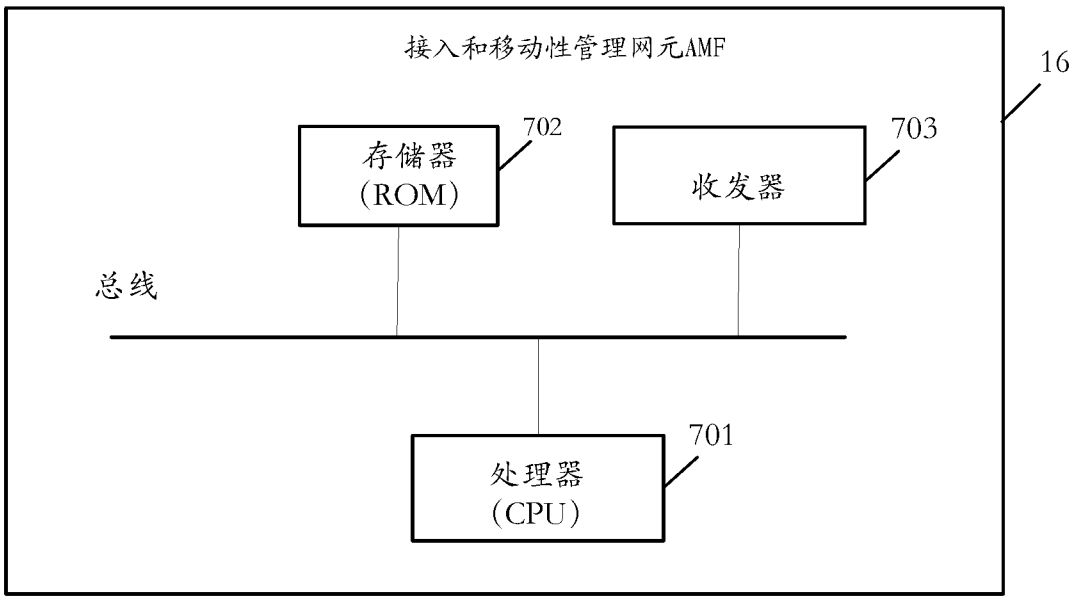

接入和移动性管理网元AMF
16
存储器
(ROM)
702
收发器
703
总线
处理器
(CPU)
701

图 18

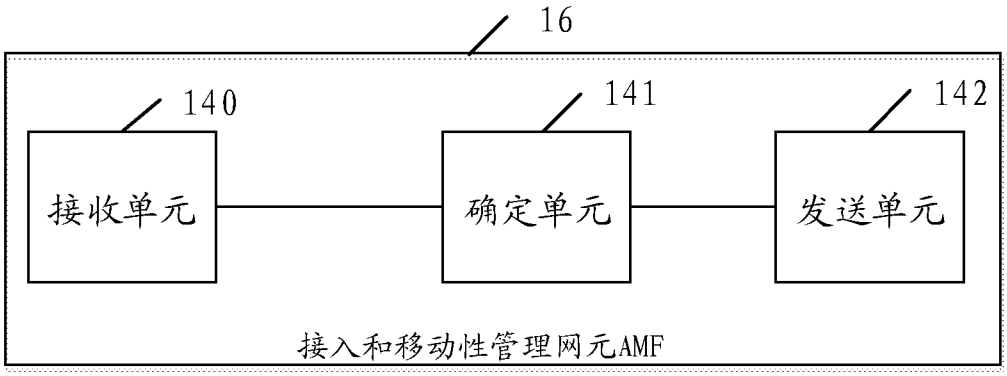

16
140
141
142
接收单元
确定单元
发送单元
接入和移动性管理网元AMF

图 19

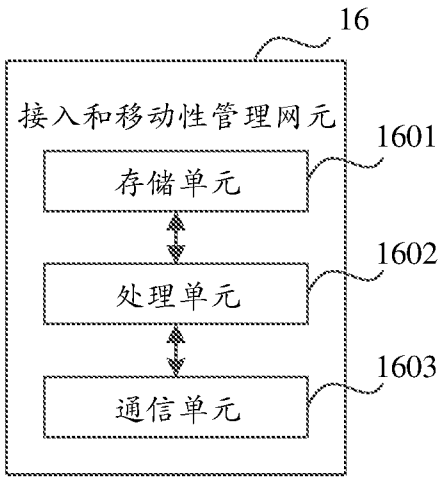

16
接入和移动性管理网元
1601
存储单元
1602
处理单元
1603
通信单元

图 20

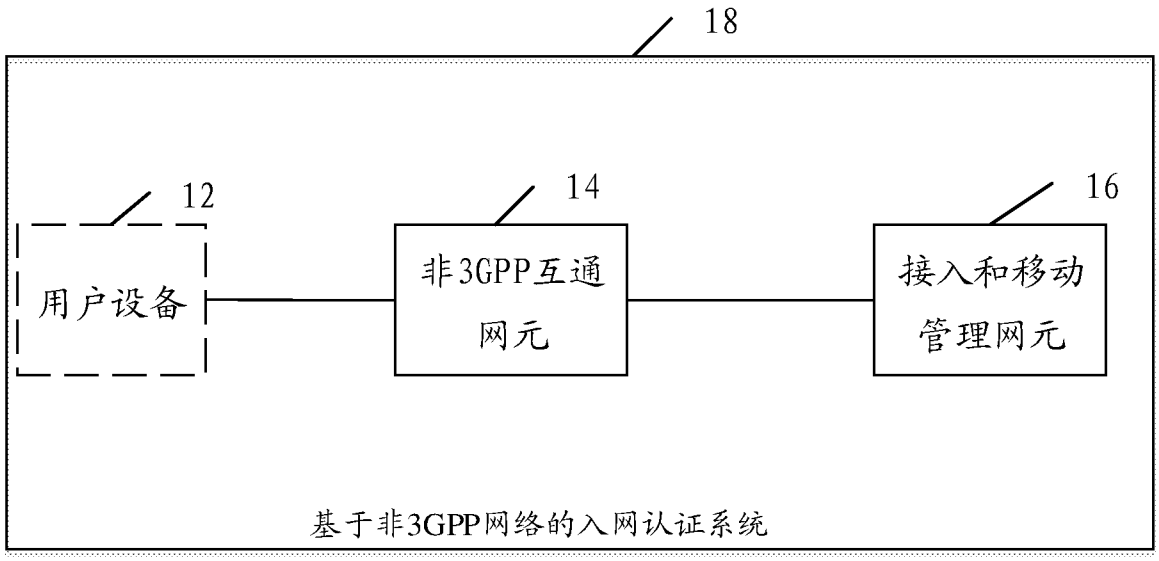

18
12
用户设备
14
非3GPP互通网元
16
接入和移动管理网元
基于非3GPP网络的入网认证系统

图 21

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/077162

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; H04W 8/26 (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)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 认证, 授权, 验证, 非 3GPP, 网络, 接入, 密钥, 移动, N3IWF, AMF, non, 3GPP, access, key, mobile

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, "Mobility Management Model for Non-3GPP Accesses: Procedures", S2-170739 SA WG 2 Meeting #S2-119, 17 February 2017 (17.02.2017), section 4.12.2	13-15, 28-30
A	QUALCOMM INCORPORATED, "Mobility Management Model for Non-3GPP Accesses: Procedures", S2-170739 SA WG 2 Meeting #S2-119, 17 February 2017 (17.02.2017), section 4.12.2	1-12, 16-27
A	CN 106304038 A (XU, Chengqi), 04 January 2017 (04.01.2017), entire document	1-30
A	CN 102348193 A (ZTE CORP.), 08 February 2012 (08.02.2012), entire document	1-30
A	EP 2166798 A1 (ALCATEL LUCENT), 24 March 2010 (24.03.2010), 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
30 October 2017	01 December 2017

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

Authorized officer
RAN, Jian'guo
Telephone No. (86-10) 62413873

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/077162

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106304038 A	04 January 2017	None	
CN 102348193 A	08 February 2012	WO 2012013103 A1	02 February 2012
EP 2166798 A1	24 March 2010	None	

国际检索报告

国际申请号
PCT/CN2017/077162

A. 主题的分类

H04W 12/06(2009.01)i; H04W 8/26(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））

CNPAT,CNKI,WPI,EPODOC,3GPP: 认证，授权，验证，非3GPP，网络，接入，密钥，移动，N3IWF,AMF,non,3GPP,access,key,mobile

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. "Mobility management model for non-3GPP accesses:procedures" S2-170739 SA WG2 Meeting #S2-119, 2017年 2月 17日 (2017-02-17), 第4.12.2节	13-15，28-30
A	QUALCOMM INCORPORATED. "Mobility management model for non-3GPP accesses:procedures" S2-170739 SA WG2 Meeting #S2-119, 2017年 2月 17日 (2017-02-17), 第4.12.2节	1-12，16-27
A	CN 106304038 A (徐成琦) 2017年 1月 4日 (2017-01-04) 全文	1-30
A	CN 102348193 A (中兴通讯股份有限公司) 2012年 2月 8日 (2012-02-08) 全文	1-30
A	EP 2166798 A1 (ALCATEL LUCENT) 2010年 3月 24日 (2010-03-24) 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
2017年 10月 30日	2017年 12月 1日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 冉建国 电话号码 (86-10)62413873

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/077162

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 106304038 A	2017年 1月 4日	无	
CN 102348193 A	2012年 2月 8日	WO 2012013103 A1	2012年 2月 2日
EP 2166798 A1	2010年 3月 24日	无	