

安全通信的方法和装置

5 本申请要求于 2021 年 8 月 6 日提交中国国家知识产权局、申请号为 202110904250.8、发明名称为“安全通信的方法和装置”的中国专利申请和 2021 年 9 月 14 日提交中国国家知识产权局、申请号为 202111073980.4、发明名称为“安全通信的方法和装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

10 技术领域

本申请涉及通信领域，并且更具体地，涉及一种安全通信的方法和装置。

背景技术

15 用户设备（user equipment, UE）可以通过有缝无线局域网分流（non-seamless ireless local area network offload, NSW0）的方式接入网络，实现 UE 通过非第三代合作伙伴计划（non-3rd generation partnership project, non-3GPP）技术接入网络。目前，该方式仅限于在第四代（4th generation, 4G）系统中应用。因此，如何扩展 NSW0 接入方式的应用范围成为亟待解决的问题。

20 发明内容

本申请提供一种安全通信的方法和装置，将 NSW0 场景应用到第五代（5th generation, 5G）系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与第五代核心网（5th generation core, 5GC）的鉴权流程。

25 第一方面，提供了一种适用于终端设备使用有缝的无线局域网分流 NSW0 的方式接入网络的场景的安全通信的方法，包括：统一数据管理实体接收来自鉴权服务功能实体的指示信息；该统一数据管理实体根据该指示信息在至少两种鉴权方式中选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。

30 上述方案，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

35 结合第一方面，在第一方面的某些实现方式中，该指示信息是网络接入标识 NAI 格式的用户隐藏标识 SUCI，或者是用户隐藏标识 SUCI 中的字段。

结合第一方面，在第一方面的某些实现方式中，该指示信息包括以下任意一个或多个：该鉴权服务功能实体的标识，或该终端设备所在网络的标识，或接入技术类型指示信息，或接入方法指示信息，该接入类型指示信息用于指示接入网络类型，该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：该统一数据管理实体存储标识该终端设备通过有缝的无线局域网分流 NSW0 的方式接入该网络的信息；或者，该统一数据管理实体存储标识该终端设备通过该 NSW0 的方式接入该网络的信息，以及该鉴权服务功能实体的标识。

5 上述方案，UDM 在记录鉴权成功状态时可以通过只记录通过 NSW0 鉴权成功的状态而不记录鉴权服务功能实体的 ID，维护简单，需要更改的网元较少，方便快捷商用；或者，可以将通过 NSW0 鉴权成功状态与鉴权服务功能实体的 ID 绑定，使得 UDM 记录的条目更为清晰。

结合第一方面，在第一方面的某些实现方式中，该终端设备通过有缝的无线局域网分
10 流 NSW0 的方式接入该网络的信息用于可扩展认证协议 EAP 重鉴权流程。

第二方面，提供了一种安全通信的方法，包括：终端设备接收来自无线访问接入点的消息；该终端设备根据该消息生成指示信息，该指示信息表示该终端设备处于有缝的无线局域网分流 NSW0 场景；该终端设备发送该指示信息。

上述方案，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，
15 并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：该终端设备根据该第
20 一消息 01 确定使用该 NSW0 的方式接入网络。

结合第二方面，在第二方面的某些实现方式中，该第一指示信息 01 包括用户隐藏标识(subscription concealed identifier, SUCI)，其中，该 SUCI 是网络接入标识(network access identifier, NAI) 格式的字段，或者，该 SUCI 是由该终端设备根据国际移动用户识别码
25 (International Mobile Subscriber Identity, IMSI) 类型的用户永久标识 SUPI 生成的、NAI 格式的字段，或者，该 SUCI 是该终端设备根据由 IMSI 类型的 SUPI 生成的、NAI 格式的字段，该 SUCI 包括第一字段，该第一字段用于指示选择该 EAP-AKA' 与该终端设备进行鉴权。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：该终端设备生成主会话密钥，该主会话密钥为用于生成该终端设备与网络通信的密钥的根密钥，该网络为该终端设备通过该 NSW0 的方式接入的网络。
30

上述方案，在鉴权成功后生成用于生成该终端设备与该网络通信的密钥的根密钥，以便于后续终端设备在 NSW0 场景下与网络之间的安全通信，进一步完善了 NSW0 场景下的鉴权和密钥分发的流程。

结合第二方面，在第二方面的某些实现方式中，该终端设备发送该指示信息，包括：
35 该终端设备向统一数据管理实体或鉴权服务功能实体或该无线访问接入点发送该指示信息。

第三方面，提供了一种安全通信的方法，其特征在于，包括：鉴权服务功能实体接收来自无线访问接入点的消息；该鉴权服务功能实体根据该消息生成指示信息，该指示信息用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权；该鉴权服务功能实体向该统一数据管理实体发送该指示信息。
40

上述方案，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的
5 开销。

结合第三方面，在第三方面的某些实现方式中，该指示信息包括以下任意一个或多个：该鉴权服务功能实体的标识，或该终端设备所在网络的标识，或接入技术类型指示信息，或接入方法指示信息，该接入类型指示信息用于指示接入网络类型，该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

10 结合第三方面，在第三方面的某些实现方式中，该方法还包括：该鉴权服务功能实体根据该消息确定该终端设备通过 NSW0 的方式接入网络。

结合第三方面，在第三方面的某些实现方式中，该方法还包括：该鉴权服务功能实体生成主会话密钥，该主会话密钥用于生成该终端设备与该网络通信的密钥；该鉴权服务功能实体向该无线访问接入点发送该主会话密钥。

15 上述方案，UDM 在记录鉴权成功状态时可以通过只记录通过 NSW0 鉴权成功的状态而不记录鉴权服务功能实体的 ID，维护简单，需要更改的网元较少，方便快捷商用；或者，可以将通过 NSW0 鉴权成功状态与鉴权服务功能实体的 ID 绑定，使得 UDM 记录的条目更为清晰。

20 第四方面，提供了一种安全通信的装置，包括：收发模块，用于接收来自无线访问接入点的消息；处理模块，用于根据该消息生成指示信息，该指示信息表示该终端设备处于有缝的无线局域网分流 NSW0 场景；该收发模块，还用于发送该指示信息。

上述方案，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的
25 开销。

结合第四方面，在第四方面的某些实现方式中，该处理模块，还用于根据该消息确定使用该 NSW0 的方式接入网络。

30 结合第四方面，在第四方面的某些实现方式中，该指示信息是网络接入标识 NAI 格式的用户隐藏标识 SUCI，或者是用户隐藏标识 SUCI 中的字段。

结合第四方面，在第四方面的某些实现方式中，该处理模块，还用于生成主会话密钥，该主会话密钥用于生成该终端设备与网络通信的密钥，该网络为该终端设备通过该 NSW0 的方式接入的网络。

35 结合第四方面，在第四方面的某些实现方式中，该收发模块，具体还用于向统一数据管理实体或鉴权服务功能实体或该无线访问接入点发送该指示信息。

第五方面，提供了一种适用于终端设备使用有缝的无线局域网分流 NSW0 的方式接入网络的场景的安全通信的装置，包括：收发模块，用于接收来自鉴权服务功能实体的指示信息；处理模块，用于根据该指示信息在至少两种鉴权方式中选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。

40 上述方案，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，

并通过指示 UDM 选择 EAP-AKA' 鉴权方法, 能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外, 在 NSW0 场景下, 终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF, 减轻了 AMF 的负担, 也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

5 结合第五方面, 在第五方面的某些实现方式中, 该指示信息是网络接入标识 NAI 格式的用户隐藏标识 SUCI, 或者是用户隐藏标识 SUCI 中的字段。

结合第五方面, 在第五方面的某些实现方式中, 该指示信息包括以下任意一个或多个: 该鉴权服务功能实体的标识, 或该终端设备所在网络的标识, 或接入技术类型指示信息, 或接入方法指示信息, 该接入类型指示信息用于指示接入网络类型, 该接入方法指示信息
10 用于指示该终端设备使用的接入技术的特征。

结合第五方面, 在第五方面的某些实现方式中, 该处理模块, 还用于存储标识该终端设备通过有缝的无线局域网分流 NSW0 的方式接入该网络的信息; 或者, 该处理模块, 还用于存储标识该终端设备通过该 NSW0 的方式接入该网络的信息, 以及该鉴权服务功能实体的标识。

15 结合第五方面, 在第五方面的某些实现方式中, 该终端设备通过有缝的无线局域网分流 NSW0 的方式接入该网络的信息用于可扩展认证协议 EAP 重鉴权流程。

第六方面, 提供了一种安全通信的装置, 包括: 收发模块, 用于接收来自无线访问接入点的消息; 该处理模块, 用于根据该消息生成指示信息, 该指示信息用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权; 该收发
20 模块, 还用于向该统一数据管理实体发送该指示信息。

上述方案, 将 NSW0 场景应用到 5G 系统中, 扩展了 NSW0 接入方式的应用范围, 并通过指示 UDM 选择 EAP-AKA' 鉴权方法, 能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外, 在 NSW0 场景下, 终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF, 减轻了 AMF 的负担, 也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的
25 开销。

结合第六方面, 在第六方面的某些实现方式中, 该鉴权服务功能实体的标识, 或该终端设备所在网络的标识, 或接入技术类型指示信息, 或接入方法指示信息, 该接入类型指示信息用于指示接入网络类型, 该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

30 结合第六方面, 在第六方面的某些实现方式中, 该处理模块, 还用于根据该消息确定该终端设备通过 NSW0 的方式接入网络。

结合第六方面, 在第六方面的某些实现方式中, 该处理模块, 还用于生成主会话密钥, 该主会话密钥用于生成该终端设备与该网络通信的密钥; 该收发模块, 还用于向该无线访问接入点发送该主会话密钥。

35 第七方面, 提供了一种通信装置, 其特征在于, 包括: 处理器和存储器; 该存储器, 用于存储计算机程序; 该处理器, 用于执行该存储器中存储的计算机程序, 以使得该通信装置执行第一方面至第三方面任一方面所述的通信方法。

第八方面, 提供了一种计算机可读存储介质, 其特征在于, 该计算机可读存储介质上存储有计算机程序, 当该计算机程序在计算机上运行时, 使得该计算机执行第一方面至第
40 三方面任一方面所述的通信方法。

第九方面，提供了一种芯片系统，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该芯片系统地通信设备执行第一方面至第三方面任一方面所述的通信方法。

第十方面，提供了一种安全通信的系统，其特征在于，包括：终端设备，用于接收无线访问接入的消息 01；还用于根据该消息生成指示信息 01，该指示信息 01 表示该终端设备处于有缝的无线局域网分流 NSWO 场景；还用于向鉴权服务功能实体发送指示信息 01；该鉴权服务功能实体，用于接收指示信息 01；还用于向统一数据管理实体发送指示信息 02，该指示信息 02 用于指示选择该 EAP-AKA' 与该终端设备进行鉴权；该统一数据管理实体，用于根据该指示信息 02 在至少两种鉴权方式中选择 EAP-AKA' 与终端设备进行鉴权。

第十一方面，提供了一种安全通信的系统，其特征在于，包括：鉴权服务功能实体，用于接收消息 02；还用于根据该消息 02 生成指示信息 02，该指示信息 02 用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权；还用于向统一数据管理实体发送指示信息 02；该统一数据管理实体，用于根据该指示信息 02 在至少两种鉴权方式中选择 EAP-AKA' 与终端设备进行鉴权。

附图说明

- 图 1 提供了 4G 中非 3GPP 接入架构的示意图。
- 图 2 示出了当前的 5G 网络架构。
- 图 3 示出了 SUCI 的结构。
- 图 4 示出了本申请提供的安全通信的方法 100 的示意性交互图。
- 图 5 示出了本申请提供的安全通信的方法 200 的示意性交互图。
- 图 6 示出了本申请提供的安全通信的方法 300 的示意性交互图。
- 图 7 示出了本申请提供的安全通信的方法 400 的示意性交互图。
- 图 8 示出了本申请生成 MSK 的密钥架构。
- 图 9 示出了本申请提供的安全通信的方法 500 的示意性交互图。
- 图 10 示出了本申请提供的安全通信的方法 600 的示意性交互图。
- 图 11 示出了本申请提供的安全通信的方法 700 的示意性交互图。
- 图 12 是本申请实施例提供的用于安全通信的通信装置的示意性框图。
- 图 13 为本申请实施例提供的安全通信的装置 20 的示意图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

本申请实施例提供的技术方案可以应用于各种通信系统，例如：长期演进（long term evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、第五代（5th generation, 5G）系统或新无线（new radio, NR）或者未来的 3GPP 系统等。

通常来说，传统的通信系统支持的连接数有限，也易于实现，然而，随着通信技术的

发展,移动通信系统将不仅支持传统的通信,还将支持例如,设备到设备(device to device, D2D)通信,机器到机器(machine to machine, M2M)通信,机器类型通信(machine type communication, MTC),车辆与万物(vehicle to everything, V2X)通信(也可以称为车辆网通信),例如,车辆与车辆(vehicle to vehicle, V2V)通信(也可以称为车到车通信)、
5 车辆与基础设施(vehicle to infrastructure, V2I)通信(也可以称为车到基础设施通信),车辆与行人(vehicle to pedestrian, V2P)通信(也可以称为车到人通信),车辆与网络(vehicle to network, V2N)通信(也可以称为车到网络通信)。

图1提供了4G中非3GPP接入架构的示意图。下面结合图1对本申请实施例中可能涉及各个网元分别进行说明。

10 非3GPP接入,是指UE通过非3GPP接入技术接入到运营商网络,使用运营商网络资源。非3GPP接入技术包括WLAN, CDMA等接入技术。

1、用户设备(user equipment, UE):可以称终端设备、终端、接入终端、用户单元、用户站、移动站、移动台、远方站、远程终端、移动设备、用户终端、无线通信设备、用户代理或用户装置。UE还可以是蜂窝电话、无绳电话、会话启动协议(session initiation
15 protocol, SIP)电话、无线本地环路(wireless local loop, WLL)站、个人数字助理(personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备,5G网络中的终端设备或者未来演进的公用陆地移动通信网络(public land mobile network, PLMN)中或者非陆地网络(non-terrestrial networks, NTN)的终端设备等,还可以是端设备,逻辑实体,智能设备,如手机,智能
20 终端等终端设备,或者服务器,网关,基站,控制器等通信设备,或者物联网设备,如传感器,电表,水表等物联网(internet of things, IoT)设备。还可以是具有通信功能的无人机(unmanned aerial vehicle 或 uncrewed aerial vehicle, UAV)。本申请实施例对此并不限定。

2、归属签约用户服务器(home subscriber server, HSS)是演进的分组系统(evolved packet system, EPS)中用于存储用户签约信息的服务器,主要负责管理用户的签约数据及移动用户的位置信息。

3、策略与计费规则功能单元(policy and charging rules function, PCRF)是业务数据流和网际互连协议(internet protocol, IP)承载资源的策略与计费控制策略决策点,它为策略与计费执行功能单元选择及提供可用的策略和计费控制决策。

30 4、公共数据网(public data network, PDN)网关:提供用户的会话管理和承载控制、数据转发、IP地址分配以及非3GPP用户接入等功能。它是3GPP接入和非3GPP接入公用数据网络PDN的锚点。

5、验证、授权和记账(authentication、authorization、accounting, AAA)服务器:是一个能够处理用户访问请求的服务器程序,提供验证授权以及帐户服务,主要目的是管理
35 用户访问网络服务器,对具有访问权的用户提供服务。AAA服务器通常同网络访问控制、网关服务器、数据库以及用户信息目录等协同工作。

6、演进型分组数据网关(evolved packet data gateway, ePDG)

7、IP多媒体系统(IP multimedia subsystem, IMS):是一种全新的多媒体业务形式,它能够满足的终端客户更新颖、更多样化多媒体业务的需求。

40 从图1中可以看出,4G系统中UE通过非3GPP接入网络时,经过HSS、AAA服务

器等网元，而不经核心网网元，如移动性管理实体（mobility management entity, MME）。例如，UE 通过有缝 WLAN 分流（non-seamless WLAN offload, NSW0）模式接入网络时，可以经过 WLAN 接入点（Wi-Fi AP）接入网络，而不经 MME。

在 5G 网络，已经标准化了 UE 可以通过 non-3GPP 接入技术接入到 5G 核心网。但是 5G 网络的标准化协议中，并没有考虑到 NSW0 接入方式的应用，即没有考虑 UE 不通过接入和移动管理功能网元（access and mobility management function, AMF）接入 5GC 的场景。

图 2 示出了当前的 5G 网络架构。下面结合图 2 对本申请实施例中可能涉及的各个网元分别进行说明。

10 1、UE：具体参见图 1 对应的描述。

2、接入网（access network, AN）：为特定区域的授权用户提供入网功能，并能够根据用户的级别，业务的需求等使用不同质量的传输隧道。接入网络可以为采用不同接入技术的接入网络。目前的无线接入技术有两种类型：3GPP 接入技术（例如 3G、4G 或 5G 系统中采用的无线接入技术和未来 3GPP 无线接入技术）和非第三代合作伙伴计划（non-3GPP）接入技术。3GPP 接入技术是指符合 3GPP 标准规范的接入技术，采用 3GPP 接入技术的接入网络称为无线接入网络（radio access network, RAN），其中，5G 系统中的接入网设备称为下一代基站节点（next generation Node Base station, gNB）。非 3GPP 接入技术是指不符合 3GPP 标准规范的接入技术，例如，以 Wi-Fi 中的接入点（access point, AP）为代表的空口技术。

20 基于无线通信技术实现接入网络功能的接入网可以称为无线接入网（radio access network, RAN）。无线接入网能够管理无线资源，为终端提供接入服务，进而完成控制信号和用户数据在终端和核心网之间的转发。

无线接入网例如可以是基站（NodeB）、演进型基站（evolved NodeB, eNB 或 eNodeB）、5G 移动通信系统中的基站（gNB）、未来移动通信系统中的基站或 Wi-Fi 系统中的 AP 等，还可以是云无线接入网络（cloud radio access network, CRAN）场景下的无线控制器，或者该接入网设备可以为中继站、接入点、车载设备、可穿戴设备以及未来 5G 网络中的网络设备或者未来演进的 PLMN 网络中的网络设备等。本申请的实施例对无线接入网设备所采用的具体技术和具体设备形态不做限定。

30 3、接入和移动管理功能（access and mobility management function, AMF）实体：主要用于移动性管理和接入管理等，可以用于实现移动性管理实体（mobility management entity, MME）功能中除会话管理之外的其它功能，例如，合法监听、或接入授权（或鉴权）等功能。

4、认证服务功能（authentication server function, AUSF）实体：主要用于用户鉴权等。

35 5、统一数据管理（unified data management, UDM）实体：用于处理用户标识、接入鉴权、注册、或移动性管理等。

在图 2 所示的网络架构中，N1 接口为终端与 AMF 实体之间的参考点；N2 接口为 AN 和 AMF 实体的参考点，用于非接入层（non-access stratum, NAS）消息的发送等；N3 接口为（R）AN 和用户平面功能（user plane function, UPF）实体之间的参考点，用于传输用户面的数据等；N4 接口为会话管理功能（session management function, SMF）实体和 UPF 实体之间的参考点，用于传输例如 N3 连接的隧道标识信息，数据缓存指示信息，以及下

行数据通知消息等信息；N6 接口为 UPF 实体和据网络（DN）之间的参考点，用于传输用户面的数据等。

应理解，上述图 2 所示的网络架构可以应用于本申请实施例，此外，适用本申请实施例的网络架构并不局限于此，任何能够实现上述各个网元的功能的网络架构都适用于本申请实施例。

还应理解，图 2 中所示的 AMF 实体、SMF 实体、UPF 实体、网络开放功能（network exposure function, NEF）、AUSF 实体、网络存储功能（network function (NF) repository function, NRF）实体、策略控制功能（policy control function, PCF）实体、UDM 实体可以理解为核心网中用于实现不同功能的网元，例如可以按需组合成网络切片。这些核心网网元可以各自独立的设备，也可以集成于同一设备中实现不同的功能，本申请对此不做限定。需要说明的是，上述“网元”也可以称为实体、设备、装置或模块等，本申请并未特别限定。

还应理解，上述命名仅为用于区分不同的功能，并不代表这些网元分别为独立的物理设备，本申请对于上述网元的具体形态不作限定，例如，可以集成在同一个物理设备中，也可以分别是不同的物理设备。此外，上述命名仅为便于区分不同的功能，而不对本申请构成任何限定，本申请并不排除在 5G 网络以及未来其它的网络中采用其他命名的可能。例如，在 6G 网络中，上述各个网元中的部分或全部可以沿用 5G 中的术语，也可能采用其他名称等。在此进行统一说明，以下不再赘述。

还应理解，图 2 中的各个网元之间基于服务化接口进行通信，例如各个网元之间使用服务化接口进行信息交互或调用服务。图 2 中的各个网元之间的接口名称只是一个示例，具体实现中接口的名称可能为其他的名称，本申请对此不作具体限定。此外，上述各个网元之间的所传输的消息（或信令）的名称也仅仅是一个示例，对消息本身的功能不构成任何限定。

在该网络架构中，RAN 支持 2 种接入技术，即 3GPP 接入技术和非 3GPP 接入技术。从图 2 中可以看出，UE 如果通过非 3GPP 技术接入到 5GC，是必须经过 AMF 的。事实上，在 3GPP 和非 3GPP 融合的背景下，UE 通过 3GPP 和非 3GPP 接入技术接入 5GC 并进行鉴权时都必须经过 AMF。在这种情况下，如果 UE 可以通过非 3GPP 接入完成用户面数据交互，那么需要接入 5GC 就会导致 AMF 处理、信令交互等负担较重，影响网络的通信效率。另外，UE 通过非 3GPP 技术接入到 5GC 的网络架构还未进行实际部署，而且部署该网络架构需要的花销非常大。

鉴于 4G 系统中 NSWO 模式下，UE 可以经过 WLAN 接入点而不经核心网网元（如 AMF）接入网络，且 UE 通过 NSWO 模式接入网络的架构已经基本部署完毕，且目前还没有关于 UE 通过 NSWO 模式接入 5GC 的方案，本申请提出一种安全通信的方法和装置，使得 UE 可以通过 NSWO 模式不经 AMF 接入 5GC，从而可以减轻 AMF 的负担，提高网络的通信效率，节省部署网络架构的花销。在 UE 通过 NSWO 模式接入 5GC 时，由于 5G 系统中 UDM 支持两种鉴权方法，即 EAP-AKA' 和 5G-AKA，而由于 NSWO 场景下只能使用 EAP-AKA'，因此 UDM 如何选择鉴权方法成为需要解决的问题。

为了更好地理解本申请实施例的技术方案，下面介绍一些相关概念。

用户永久标识（subscription permanent identifier, SUPI）包括 SUPI 类型（type）和值，其中，SUPI type 有 4 种：IMSI, NSI（network specific identifier），a Global Line Identifier

(GLI) or a Global Cable Identifier (GCI), SUPI 的值的格式有 2 种, 分别为: IMSI, NAI。其中, NAI 格式, 是一种通用格式, 其表现形式为 username@example.com。

为了不在空口暴露用户的 SUPI, 通过对 SUPI 中的除去 SUPI type 之外的部分进行计算得到一个结果, 该结果是用户隐藏标识 (subscription concealed identifier, SUCI) 的一部分。

图 3 示出了 SUCI 的结构。如图 3 所示, SUCI 主要包含的内容如下:

SUPI 类型: 0 代表 IMSI; 1 代表 NSI; 2 代表 GLI; 3 代表 GCI; 4 到 7 还没有被定义。

归属地网络标识符 (home network identifier) 用于识别 UE 的家乡网络。

当 SUPI type 是 IMSI 的时候, 归属地网络标识符为移动国家码 (mobile country code, MCC) 和移动网络码 (mobile network code, MNC)。当 SUPI 类型是 NSI 的时候, Home Network Identifier 是一个格式为 username@realm 的字符串。当 SUPI type 是 GCI 时, Home Network Identifier 的格式为 5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

为了便于理解本申请实施例, 下面将对本申请涉及一些概念进行解释说明。

1、本申请中, UE 可以通过 3GPP 或非 3GPP 方式接入网络, 而 UE 通过非 3GPP 接入网络时, 具体包括通过 NSWOW 接入和非 NSWOW 接入的方式网络。

2、无缝 WLAN 分流 (non-seamless WLAN offload, NSWOW) 是指 UE 使用运营商网络信任状与运营商网络执行完鉴权流程后, 直接使用本地 AP 将数据发送给外部网络, 该接入方法只需要运营商提供信任状, 并提供相应的鉴权流程, 不需要 AMF, SMF 等网元为 UE 创建 UE 的 3GPP 网络使用的上下文。也就是说, NSWOW 是一种借用 3GPP 信任状完成对 UE 身份的确认后, 不需要 3GPP 系统为其提供服务的一种传递用户数据的方法, 例如 UE 接入 Wi-Fi AP 且无需经过 3GPP 核心网传递用户数据的方法。

需要说明的是, 本申请中涉及的“NSWOW 模式”、“NSWOW 方式”、“NSWOW 技术”、“NSWOW 接入”、“NSWOW 接入方式”等多种表述, 均表达上述内容。

需要说明的是, 本申请中的 NSWOW 场景以及在 NSWOW 场景下的安全通信的方法不仅仅限于在 4G 系统中实现, 在 5G 或 NR, 或未来的 6G、7G 系统中均可以适用。

3、非 NSWOW 方式是指 UE 通过非 3GPP 接入技术接入到 5G 核心网的一种接入方式。该接入方式需要运营商提供信任状, 并提供相应的鉴权流程, 还需要 AMF, SMF 等网元为 UE 创建 UE 的 3GPP 网络使用的上下文。上述是 3GPP 在 Release 15 就标准化的一种标准化接入流程。

需要说明的是, 本申请中涉及的“非 NSWOW 模式”、“非 NSWOW 方式”、“非 NSWOW 技术”、“非 NSWOW 接入”、“非 NSWOW 接入方式”等多种表述, 均表达上述内容。

4、在本申请中, 无线访问接入点 (Wi-Fi AP) 又可以叫做 WLAN AP, 其可以只是一个接入节点, 也可以是包含有控制功能的接入节点。本申请实施例涉及 Wi-Fi AP 传递消息的情景中, 同样适用于以下几种方式:

方式一: Wi-Fi AP 作为接入节点直接传递消息给接收方。

方式二: Wi-Fi AP 将消息先传递给内部接入控制器 (access control, AC)。

方式三: Wi-Fi AP 将消息传递给外部 AC, 再由 AC 发送给接收方。

下面结合图 4, 对本申请提供的安全通信的方法 100 进行详细说明。图 4 是本申请的方法 100 的示意性交互图。方法 100 具体可以通过两个方案来实现。

方案一:

S101a, 无线访问接入点向终端设备发送消息 01, 相应地, 终端设备接收来自无线访问接入点的消息 01。

5 应理解, 消息 01 可以是终端设备与无线访问接入点之间建立连接过程中, 从无线访问接入点接收的消息。具体地, 终端设备与无线访问接入点之间建立连接过程中的信息交互可以参考电气电子工程师学会(institute of electrical and electronics engineer, IEEE)802.11 中的相关步骤。终端设备根据消息 01 可以确定使用 NSW0 的方式接入网络。

示例性, 关于终端设备如何根据消息 01 确定使用 NSW0 的方式接入网络, 可以参考 S201 中相关的内容。

10 S102a, 终端设备根据消息 01 生成指示信息 01, 指示信息 01 表示所述终端设备处于 NSW0 场景, 或者, 用于指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权。

其中, 用于指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权, 说明指示信息 01 的接收方可以根据该指示信息 01 获知需要指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权。当接收方是统一数据管理实体, 统一数据管理实体根据该指示信息 15 01 确定选择 EAP-AKA' 与终端设备进行鉴权。

具体地, 指示信息 01 可以是 SUCI, 也可以是承载在 SUCI 中的指示信息, 或者也可以是单独的指示信息, 本申请对此不做限定。

示例性地, 该指示信息 01 可以是 NAI 格式的 SUCI。

20 应理解, 该 NAI 格式的 SUCI 可以由不同类型的 SUPI 生成的, 例如由 IMSI 类型的 SUPI 生成的。由于一般情况下 IMSI 类型的 SUPI 生成的 SUCI 是 IMSI 格式的, 而根据 IMSI 格式的 SUPI 生成的 NAI 格式的 SUCI 与此有区别, 因此可以用来隐式地指示使用 EAP-AKA' 鉴权方法。具体实现方式可以参见方法 200 中的 S203。

示例性地, 指示信息 01 可以承载在 SUCI 中, 指示信息 01 可以是 SUCI 中的字段或者字符串或者数字, 本申请对其在 SUCI 中的位置不做限定。例如, 该指示信息 01 可以是字符串“NSW0”, 用来指示 UE 通过 NSW0 方式接入。具体实现方式可以参见方法 200 25 中的 S203。

示例性地, 指示信息 01 可以是单独的指示信息, 用于指示 UE 通过 NSW0 方式接入网络, 或者, 用于指示使用 EAP-AKA' 鉴权方法。

其中, 关于用于指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权的说明 30 可参考上述的描述。

其中, 用于指示 UE 通过 NSW0 方式接入, 说明指示信息 01 的接收方可以根据该指示信息 01 获知 UE 通过 NSW0 方式接入网络。当接收方是统一数据管理实体, 统一数据管理实体根据该指示信息 01 确定选择 EAP-AKA' 与终端设备进行鉴权。

35 S103, 终端设备发送指示信息 01, 包括: 终端设备向无线访问接入点或鉴权服务功能实体或统一数据管理实体发送指示信息 01, 相应地, 接收方为无线访问接入点时, 无线访问接入点接收指示信息 01 后将指示信息 01 转发给鉴权服务功能实体; 接收方为鉴权服务功能实体时, 鉴权服务功能实体接收指示信息 01 后转发给统一数据管理实体; 接收方为统一数据管理实体时, 统一数据管理实体接收来自终端设备的指示信息 01。

40 S104, 鉴权服务功能实体根据指示信息 01 向统一数据管理实体发送指示信息 02, 相应地, 统一数据管理实体从鉴权服务功能实体接收指示信息 02。

应理解，这里的指示信息 02 包括的内容可以与指示信息 01 相同，也可以不同。

示例性地，指示信息 02 包括的内容与指示信息 01 相同。鉴权服务功能实体转发指示信息 01 中的内容。具体可以参见方法 200 中的相关描述。

示例性地，指示信息 02 包括的内容与指示信息 01 不同，可以理解为指示信息 02 中除指示信息 01 外还包括其他指示信息。鉴权服务功能实体在指示信息 01 的基础上，又加入了自行生成的信息，为了方便描述，下面将该信息称为指示信息 03。例如，鉴权服务功能实体根据指示信息 01 的消息来源（如来自于 Wi-Fi AP）确定 UE 通过 NSW0 接入网络，从而生成指示信息 03。因此，指示信息 02 包括指示信息 01 和指示信息 03。

其中，该指示信息 03 可以表示所述终端设备处于有缝的无线局域网分流 NSW0 场景，用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。指示信息 03 可以承载在服务网络名称（service network name，SN name）中，也可以是一个独立的指示信息。具体可以参见方法 300 中的 S306。

S105，统一数据管理实体根据指示信息 02 在至少两种鉴权方式中选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。

需要说明的是，终端设备使用 EAP-AKA' 与网络进行鉴权时，不需要经过核心网网元 AMF。

与 S104 中指示信息 02 相对应地，统一数据管理实体根据指示信息 02 的指示选择 EAP-AKA' 与终端设备进行鉴权。

示例性地，如果指示信息 02 与指示信息 01 的内容相同，具体参见方法 200 中的 S209，如果指示信息 02 包括指示信息 01 和指示信息 03，具体参见方法 200 中的 S209 和方法 300 中的 S309 对应的描述（例如，UDM 根据 SUCI 或指示信息 05，以及 SN name 或指示信息 06，选择 EAP-AKA'）。

本申请实施例，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。进一步地，通过 UE 生成的 SUCI 或通过指示信息指示 UDM 选择 EAP-AKA' 鉴权方法，完善了 NSW0 场景下的鉴权流程。

方案二：

S101b，无线访问接入点向鉴权服务功能实体发送消息 02，相应地，鉴权服务功能实体接收来自无线访问接入点的消息 02。

示例性地，鉴权服务功能实体可以通过消息 02 的来源或者消息名称确定终端设备通过 NSW0 接入网络，例如鉴权服务功能实体通过消息 02 来自于无线访问接入点确定，或者鉴权服务功能实体通过消息 02 的消息名称为 EAP-响应/身份认证（EAP response/identity）消息确定。

可选地，鉴权服务功能实体还可以通过消息 02 中的指示信息确定终端设备通过 NSW0 接入网络。例如，消息 02 中还可以包括指示信息 01，指示信息 01 具体可以参见方案 1 中的相关描述。

S102b，鉴权服务功能实体根据消息 02 生成指示信息 03。

示例性地，鉴权服务功能实体生成的指示信息 03 可以表示所述终端设备处于有缝的

无线局域网分流 NSWO 场景，或者，用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。指示信息 03 可以承载在 SN name 中，也可以是一个独立的指示信息。

其中，用于指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权，说明指示信息 03 的接收方可以根据该指示信息 03 获知需要指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权。当接收方是统一数据管理实体，统一数据管理实体根据该指示信息 03 确定选择 EAP-AKA' 与终端设备进行鉴权。

其中，表示所述终端设备处于有缝的无线局域网分流 NSWO 场景（或者说用于指示 UE 通过 NSWO 方式接入），说明指示信息 03 的接收方可以根据该指示信息 03 获知 UE 通过 NSWO 方式接入网络。当接收方是统一数据管理实体，统一数据管理实体根据该指示信息 03 确定选择 EAP-AKA' 与终端设备进行鉴权。

示例性的，该指示信息 03 可以包括以下任意一个或多个：该鉴权服务功能实体的标识，或该终端设备所在网络的标识，或接入技术类型指示信息，或接入方法指示信息，该接入类型指示信息用于指示接入网络类型，该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

应理解，这里的终端设备所在网络的标识可以包括服务网络的标识信息和接入网络的标识信息。

具体可以参见方法 300 中的 S306。

S104，鉴权服务功能实体向统一数据管理实体发送指示信息 02。

应理解，指示信息 02 包括的内容可以与指示信息 03 相同，也可以不完全相同。

作为一个示例，消息 02 中不包括指示信息 01，指示信息 02 包括的内容可以与指示信息 03 包括的内容相同。

作为另一个示例，消息 02 中包括指示信息 01，指示信息 02 可以包括指示信息 01 和指示信息 03。

S105，统一数据管理实体根据指示信息 02 在至少两种鉴权方式中选择 EAP-AKA' 与终端设备进行鉴权。

与 S104 中指示信息 02 相对应地，统一数据管理实体根据指示信息 02 的指示选择 EAP-AKA' 与终端设备进行鉴权。

示例性地，如果指示信息 02 与指示信息 03 的内容相同，具体参见方法 300 中的 S309，如果指示信息 02 包括指示信息 01 和指示信息 03，具体参见方法 200 中的 S209 和方法 300 中的 S309 对应的描述（例如，UDM 根据 SUCI 或指示信息 05，以及 SN name 或指示信息 06，选择 EAP-AKA' ）。

本申请实施例，将 NSWO 场景应用到 5G 系统中，扩展了 NSWO 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSWO 场景下 UE 与 5GC 的鉴权流程。另外，在 NSWO 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

可选地，该方法 100 还包括：

该统一数据管理实体存储该终端设备通过该 NSWO 的方式接入该网络，具体可以参见 S216 中的方式一或 S416 中的方式一。

或者，该统一数据管理实体存储该终端设备通过该 NSW0 的方式接入网络，以及该鉴权服务功能实体的标识，具体可参见 S216 中的方式二，或者 S416 中的方式二。

- 本申请实施例，UDM 在记录鉴权成功状态时可以通过只记录通过 NSW0 鉴权成功的状态而不记录鉴权服务功能实体的 ID，维护简单，需要更改的网元较少，方便快速商用；
- 5 或者，可以将通过 NSW0 鉴权成功状态与鉴权服务功能实体的 ID 绑定，使得 UDM 记录的条目更为清晰。

可选地，该方法 100 还包括：

- 所述鉴权服务功能实体生成主会话密钥，相应的，所述终端设备也生成相同的主会话密钥，所述主会话密钥为用于生成所述终端设备与所述网络通信的密钥的根密钥，所述网络为所述终端设备通过所述 NSW0 的方式接入的网络。
- 10

所述鉴权服务功能实体向所述无线访问接入点发送所述主会话密钥，相应地，所述无线访问接入点接收来自所述鉴权服务功能实体的所述主会话密钥。

关于如何生成主会话密钥具体可以参见方法 400 的 S418。

- 本申请实施例，在鉴权成功后生成用于生成所述终端设备与所述网络通信的密钥的根密钥，以便于后续终端设备在 NSW0 场景下与网络之间的安全通信，进一步完善了 NSW0 场景下的鉴权和密钥分发的流程。
- 15

下面结合图 5，对本申请提供的安全通信的方法 200 进行详细说明。图 5 是本申请的方法 200 的示意性交互图。在方法 200 中通过 UE 生成的 SUCI 或指示信息向 UDM 指示选择 EAP-AKA' 鉴权方法。

- 20 S201，UE 与非 3GPP 接入网元建立连接。

示例性地，这里的 UE 使用的非 3GPP 接入技术可以是 WLAN。若非 3GPP 接入技术是 WLAN，则非 3GPP 接入网元是一个 Wi-Fi AP。下面以 Wi-Fi AP 为例进行说明。

- 应理解，UE 所接入的 Wi-Fi AP 网络可以只支持 NSW0 方式或者只支持非 NSW0 方式，还可以既支持 NSW0 方式，也支持非 NSW0 方式，因此当一个 UE 收到来自 Wi-Fi AP 的消息的时候，要先判断是使用非 NSW0 方式还是 NSW0 方式接入。这里的消息属于 UE 与 Wi-Fi AP 之间建立连接的过程中，Wi-Fi AP 向 UE 发送的消息，UE 与 Wi-Fi AP 之间建立连接的过程的信息交互可以参考 IEEE802.11 中相关的信息交互。作为一个示例，在参考 IEEE802.11 中相关的信息交互时，可以直接延用其中的信息交互，并且将 Wi-Fi AP 发送给 UE 的消息作为触发 UE 判断是非 NSW0 方式还是 NSW0 方式接入网络的触发条件。或者，作为另一个示例，也可以在 IEEE802.11 中相关的信息交互的基础上，在 Wi-Fi AP 发送给 UE 的消息中加入指示 UE 判断是使用非 NSW0 方式还是 NSW0 方式接入网络的指示信息。
- 25
- 30

- 关于 UE 判断是使用非 NSW0 方式还是 NSW0 方式接入网络，可以通过如下方式，比如，UE 可以本地保存的列表，本地策略或者 UE 使用者手动选择等方式确定选择哪种接入方式。
- 35

- 作为一个示例，UE 本地保存有一张 Wi-Fi AP 或者服务集标识（service set identifier，SSID）或者 WLAN 网络的名称的列表，符合该列表的则优先使用非 NSW0 接入，或者优先使用 NSW0 接入。该列表运营商可以通过多种方式配置给 UE，例如空中下载（over the air，OTA），或者，通过 NAS 消息传递给 UE，比如 UE 参数更新（UE Parameters Update，UPU）流程等，或者还可以通过其他方式，本申请对此不做限定。
- 40

作为另一个示例，本地策略，可以是一种选网逻辑，或者一种选择接入方法的逻辑，其可以包括一种或多种策略形式，例如白名单、黑名单、接入方法优先级排序等。本地策略则可以是运营商通过 OTA 或者通过 NAS 消息传递给 UE，比如通过 NAS 消息传递 UE 路由选择策略（UE route selection policy, URSP），该 URSP 中可以指示当 UE 接入一个 Wi-Fi AP 的时候，是优先选择使用非 NSWO 接入还是 NSWO 接入方法。本地策略还可以指示 UE 优先使用非 NSWO 接入，在不成功后，才可以选择 NSWO 接入方法。本地的策略的配置方法可以有多种，其目的是使 UE 按照一定的入网逻辑接入网络。UE 的使用者可以通过手机屏幕选择一个网络，当该网络可以同时使用非 NSWO 和 NSWO 接入的时候，用户可以根据屏幕弹框选择想要的接入方式。

5 S202, Wi-Fi AP 向 UE 发送 EAP 请求/认证（EAP-Request/Identity）消息，用于触发 EAP 鉴权。

或者，该消息还可以是 EAP-Request/AKA'-Identity 消息。

10 S203, UE 忽略本地保存的安全上下文、5G 全局唯一的临时标识（5G-globally unique temporary identity, 5G-GUTI）等参数，使用 IMSI 生成 SUCI。

15 当 UE 已经通过 3GPP 或者非 NSWO 方式接入过网络，UE 本地可能保存着有效的 5G-GUTI、NAS 安全上下文。在此上述情形下，如果 UE 正在使用 3GPP 接入，那么 UE 本地不仅保存着有效的 5G-GUTI、NAS 安全上下文，还有接入层（access stratum, AS）安全上下文。当 UE 确定使用 NSWO 模式接入后，UE 不使用本地保存的 5G-GUTI 和有效的安全上下文，而是需要根据 SUPI 生成 SUCI。这是因为 5G-GUTI 对应的 SUPI 是保存在 AMF 上的，NSWO 接入方式，是不经过 AMF 的，如果要发送 5G-GUTI，则 UDM 要将 5G-GUTI 发给相应的 AMF，由相应的 AMF 发送 SUPI 给 UDM。为了指示 UDM 选择 EAP-AKA' 鉴权方法，这里 UE 可以采用以下两种指示方式，分别通过 SUCI 和 SUCI 之外的指示信息来指示 UDM 选择 EAP-AKA' 鉴权方法，或者，表示 UE 处于 NSWO 场景。

20 其中，用于指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权，以 SUCI 为例，说明 SUCI 的接收方可以根据该 SUCI 获知需要指示统一数据管理实体选择 EAP-AKA' 与终端设备进行鉴权。当接收方是统一数据管理实体，统一数据管理实体根据该 SUCI 确定选择 EAP-AKA' 与终端设备进行鉴权。

25 其中，表示 UE 处于 NSWO 场景（或者说用于指示 UE 通过 NSWO 方式接入），以 SUCI 以外的指示信息为例，说明该指示信息的接收方可以根据该指示信息获知 UE 通过 NSWO 方式接入网络。当接收方是统一数据管理实体，统一数据管理实体根据该指示信息确定选择 EAP-AKA' 与终端设备进行鉴权。

指示方式一，通过 SUCI 指示 UDM 选择 EAP-AKA' 鉴权方法。

UE 可以使用多种方式生成 SUCI，下面以两种实现方式为例进行说明。

30 实现方式一，通过 SUCI 向 UDM 指示当前的接入方法，使得 UDM 可以选择到 EAP-AKA'。

35 作为一个示例，若 UE 的 SUPI 是 IMSI 类型，则 UE 生成 NAI 格式的 SUCI，其构成包含安全保护结果的部分@ nai.5GC.mnc<MNC>.mcc<MCC>.3gppnetwork.org。也就是说，如果与 NAI 格式对应，那其中的 username 部分包括了安全保护结果。比如：IMSI 是 234150999999999，其中，MCC = 234，MNC = 15，MSISN = 0999999999。路由指示器（routing identifier）为 678，归属地网络公钥标识符（home network public key identifier）

为 27。那么, NAI 格式的 SUCI 的构成可以为:

type0.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of 0999999999>.mac<MAC tag value>@nai.5GC.mnc<MNC>.mcc<MCC>.3gppnetwork.org。

其中, type0.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key>.cip< encryption of 0999999999>.mac<MAC tag value>为 username 部分, 所述安全保护部分为: cip< encryption of 0999999999>.mac<MAC tag value>。

应理解, 对于图 3 中的 SUCI, 如果 SUPI 类型为 0, 即 IMSI, 那么目前的 SUCI 的格式不是 NAI 的格式, 而是 IMSI 的格式。

相应地, 后续步骤中 UDM 看到 NAI 格式的 SUCI, 则选择 EAP-AKA' 鉴权方法。

10 作为另一个示例, 若 UE 的 SUPI 是非 IMSI 类型, 则 UDM 可以配置 NAI 格式的 SUCI 均选择 EAP-AKA' 鉴权方法。此时, 只要 UDM 看到 SUCI 是 NAI 格式的, 那么 UDM 就会选择 EAP-AKA' 鉴权方法。一般情况下, 在 5G 系统中 UDM 可以基于 SUPI 去选择鉴权方法, 而本申请中 UDM 是基于 SUCI 的格式去选择。

综上所述, 在实现方式一中, 若 SUPI 格式是 IMSI, 那么通过生成用 NAI 格式的 SUCI 15 去向 UDM 指示选择 EAP-AKA' 鉴权方法, 若 SUPI 的格式是非 IMSI 类型, 则 UDM 可以配置 NAI 格式的 SUCI 均选择 EAP-AKA' 鉴权方法。

实现方式二, 在 SUCI 中增加指示信息 04, 该指示信息 04 用于指示需要使用 EAP-AKA' 鉴权方法, 或者该指示某种接入方式, 该接入方式不是 3GPP 或者非 NSW0 方式接入, 可以是 NSW0 的接入方式。即, 可以在 NAI 格式的 SUCI 中增加指示信息 04, 20 或者在非 NAI 格式的 SUCI 中增加指示信息 04。

需要说明的是, 增加的指示信息 04 可以在增加在 NAI 格式的 username 部分; 或者增加的指示信息 04 也可以在该 NAI 格式的 example 部分。本申请对此不做限定。

示例性地, 增加的指示信息 04 用于指示 UDM 需要根据接入场景选择合适的接入技术, 或者用于指示想要使用的主鉴权方法。在本实施例中, 该指示信息 04 用于指示 UDM 25 该接入方法是 NSW0 接入方法, 或者需要使用 EAP 鉴权方法, 则 UDM 根据指示信息选择 EAP-AKA' 鉴权方法。比如, 指示信息 04 可以是一个字符串, 比如“NSW0”、“non-3GPP”等, “NSW0”表示采用 NSW0 方式接入, “non-3GPP”表示使用非 NSW0 方法接入。例如, 在 SUCI 的前面加上指示信息 04“NSW0”, SUCI 的构成为: "NSW0" username@nai.5GC.mnc<MNC>.mcc<MCC>.3gppnetwork.org, 或者增加的指示信息还可以是其他内容, 本申请对此不做限定。再比如, 指示信息 04 可以是 0,1 等数字, 例如在本实施例中 30 SUCI 的构成可以为: 6username@ nai.5GC.mnc<MNC>.mcc<MCC>.3gppnetwork.org; 或者指示信息 04 可以是在 username 部分增加 method0,method1,method2, 用来表示分别需要采用 5G-AKA、EAP-AKA'、其他鉴权方法。在本实施例中, SUCI 的构成可以是 method1.username@example.com, 其中 method1 表示需要使用 EAP-AKA' 鉴权方法。再比 35 如, 指示信息可以是比特位指示信息, 比如, 即选用 2 个比特位用于指示, 该指示信息 00 用于指示需要使用 EAP-AKA' 鉴权方法或者指示某种接入方式, 该接入方式不是 3GPP 或者非 NSW0 方式接入。

指示方式二, 消息中传递指示信息 05, 该指示信息 05 用于表示接入方法或者倾向使用的鉴权方法, 例如该指示信息 05 用于指示 UDM 选择 EAP-AKA' 鉴权方法; 或者该指 40 示某种接入方式, 例如可以是 NSW0 的接入方式。

示例性地，按照目前生成 SUCI 的方式，在 S204 中承载该 SUCI 的 EAP 响应/身份认证消息中添加生成的指示信息 05。需要说明的是，该指示信息 05 可以放在 EAP 消息中，也可以放在 EAP 消息外，本申请对此不做限定。

在一种可能的实现方式中，在 UE 确定是 NSWO 方式接入后，UE 根据本地存储的路由标识（routing ID，RID），选择一个 NSWO 模式使用的 RID。RID 是用来组成 SUCI 的必要组成部分。其值可以是默认值，也可以是根据运营商配置的值。在现有技术中，RID 用来发现和选择 AUSF 和 UDM。在 5G 引入 NSWO 后，因为该 UE 只需要使用运营商提供的主鉴权功能，因此运营商可能使用专用处理 NSWO 鉴权的 AUSF 和 UDM。这样做的好处在于，既可以做到对现有网络架构影响最小，又可以使得 UE 在同时通过 NSWO 模式和非 NSWO 模式接入网络时分别使用的密钥不互相影响，即 UE 的 2 个模式在网络侧实施时不会相互影响。为了达到上述目的，可以通过引入专门处理 NSWO 鉴权的 AUSF 和 UDM 来实现。例如，运营商可以分别给 UE 配置 NSWO 模式使用的 RID 和非 NSWO 模式使用的 RID。其中，NSWO 模式使用的 RID 用于发现专用处理 NSWO 鉴权的 AUSF 和 UDM；非 NSWO 模式使用的 RID 则是用于找到可以为传统接入提供服务的 AUSF 和 UDM。因此，如果 UE 本地存储一个 NSWO 模式使用的 RID 和一个非 NSWO 模式使用的 RID，那么 UE 根据使用 NSWO 方式接入网络时，就可以选择 NSWO 模式对应的 RID，并使用该 RID 构建 SUCI。可以理解的是，该方式中的 NSWO 模式使用的 RID 可以是本申请实施例中的用于表示终端设备处于 NSWO 场景/用于指示选择 EAP-AKA' 鉴权方法的指示信息。

S204，UE 给 Wi-Fi AP 回复 EAP 响应/身份认证消息，Wi-Fi AP 将该消息转发给鉴权服务功能实体。

应理解，鉴权服务功能实体可以是一个网元或者多个网元组成。比如其可以包括 3GPP AAA 服务器、AUSF 中的至少 1 个。

示例性的，与 S203 中的指示方式一对应，UE 通过该消息，向鉴权服务功能实体发送 NAI 格式的 SUCI；或者，与 S203 中的指示方式二对应，UE 通过该消息，向鉴权服务功能实体发送指示信息 05。S205，鉴权服务功能实体基于 SUCI 中的 RID 选择 UDM。

S206，鉴权服务功能实体生成 SN name。

SN name 可以是 5G：服务网络 ID，也可以是其他形式。具体实现上可以参考方法 400-700。

可选地，当鉴权服务功能实体包括 1 个或多个功能，或者 1 个或多个网元的时候，生成 SN name 和选择 UDM 可以发生在不同的功能或网元，在具体实现上可以参考方法 400-700。

S207，鉴权服务功能实体发送 UE 认证获取请求（Nudm_UEAuthentication_Get Request）消息给 UDM。消息中携带有 SUCI 和 SN name，或者，携带 SUCI、步骤 S203 指示方式二的指示信息 05 和 SN name。

S208，UDM 对 SUCI 解密获得 SUPI。

S209，UDM 根据 SUCI 或者步骤 S203 指示方式二中的指示信息 05 确定选择 EAP-AKA' 鉴权方法。

与 S203 中指示方式一中的实现方式一对应，由于一般情况下，IMSI 类型的 SUPI 只会生成非 NAI 格式的 SUCI，因此如果 UDM 收到一个 NAI 格式的 SUCI，但是该 SUCI

的 SUPI 类型为 IMSI 时, 则 UDM 可以根据该选择 EAP-AKA' 鉴权方法。或者, UDM 根据 NAI 格式的 SUCI 确定选择 EAP-AKA' 鉴权方法。

或者, 与 S203 中指示方式一中的实现方式二对应, 当 UDM 接收到承载了指示信息 04 的 SUCI 时, 则 UDM 可以根据该 SUCI 中的指示信息 04 选择 EAP-AKA' 鉴权方法。

- 5 或者, 与 S203 中指示方式二对应, 当 UDM 接收单独的指示信息 05, 则根据该指示信息 05 选择 EAP-AKA' 鉴权方法。

可选地, 在 UDM 选择 EAP-AKA' 鉴权方法之前, UDM 验证该 UE 是否有权限使用 NSW0 模式。比如, UDM 根据 UE 的签约数据进行验证。如果 UDM 中记录该 UE 支持使用 NSW0 模式, 则授权验证成功。否则失败。如果 UE 授权验证成功, 则执行步骤 S210。

- 10 如果 UE 授权验证失败, 则向鉴权服务器发送拒绝消息, 并携带拒绝原因值。

S210, UDM 回复 UE 认证获取响应 (Nudm_UEAuthentication_Get Response) 消息给鉴权服务功能实体, 消息中携带 AV 和 SUPI。

S211, 鉴权服务功能实体保留 SUPI, 并确定使用 EAP 鉴权方法, 鉴权服务功能实体向 UE 发送 EAP 请求/ AKA' 邀请 (EAP Request/ AKA' -Challenge) 消息。

- 15 S212, UE 验证网络侧的真实性。验证成功后, UE 生成 MSK, 再进行下一步。

示例性的, 在 UE 验证网络侧的真实性前, UE 首先获取与网络侧相同的 SN Name。

UE 可以自己生成 SN Name, 或者在步骤 S211 中获取 SN Name。

可选地, 鉴权服务功能实体为 AUSF 或鉴权服务功能实体为包括 AUSF 在内的多个网元时, UE 进行下一步前还生成 Kausf。

- 20 UE 是否生成 Kausf 的处理可以有以下几种方法:

方式一: UE 在鉴权过程中生成 Kausf, 同时在收到 EAP-Success 的情况下保存 Kausf。

具体地, UE 在生成 Kausf 后, 首先将 Kausf 存储于缓存区域中。本申请实施例中, 将终端设备存储中间密钥 Kausf 的缓存区域称为第一存储空间。在收到 EAP-Success 消息后, 保存 Kausf。保存 Kausf 是用最近一次生成的 Kausf 替代已经保存的 Kausf。具体地,

- 25 UE 使用第一存储空间中新生成的 Kausf 替换第二存储空间中的之前保存的 Kausf。UE 后续在 SoR 或者 UPU 流程中使用该第二存储空间 (长期存储空间) 中的 Kausf 进行鉴权与通信。在另一种情况, 如果 NSW0 场景支持 EAP 重鉴权流程 (EAP re-authentication protocol, ERP) 流程, 则 UE 需要保存 Kausf 或者保存用于 ERP 鉴权的密钥。

方式二: UE 在鉴权过程中生成 Kausf, 但不保存 Kausf。

- 30 具体地, UE 要根据当前采用 NSW0 方式接入, 确定不需要保存 Kausf。UE 可以生成但是不保存 Kausf, 或者 UE 可以不生成 Kausf。不保存 Kausf 也可以在生成 Kausf 后立即删掉, 也可以在生成后过了一段时间后删掉, 比如在收到 EAP-Success 消息后删掉。

方式三: UE 在鉴权过程中生成 EMSK (Extended Master Session Key, 扩展的主会话密钥), 但是不将 EMSK 作为 Kausf 使用。

- 35 具体地, UE 判断是在 NSW0 流程中, 则 UE 不将 EMSK 的高 256bit 用作 Kausf。进一步地, 可选地 EMSK 按照本身的 EAP 流程进行使用。比如作为 ERP 流程的根密钥。

方式四: 如果网络侧的鉴权服务器不是 AUSF, 则不生成 Kausf。

或者, MSK 和 Kausf 也可以在步骤 S221 中生成。

- 40 S213, UE 发送 EAP 响应/ AKA' 邀请 (EAP Response / AKA' -Challenge) 消息给鉴权服务功能实体。

S214, 鉴权服务功能实体验证 UE 的真实性, 并生成 MSK, 可选地还生成 Kausf 和保存 Kausf。

示例性地, 当鉴权服务功能实体是 AUSF 的时候, 生成 Kausf 是对 AUSF 改动最小的方法。如果不追求改动最小, 则 AUSF 可以不生成 Kausf, 或者 AUSF 生成了 Kausf 但是
5 不保存 Kausf。不保存可以是在生成 Kausf 后立刻删掉, 也可以是过了一段时间后删掉。总之, AUSF 认为 UE 鉴权成功后不会保存 Kausf。

具体地, AUSF 是否生成 Kausf 的处理可以有以下几种方法:

方式一: AUSF 生成 Kausf, 但是不保存 Kausf。比如, AUSF 在判断是 NSW0 流程生成的 Kausf, 则 AUSF 不保存 Kausf。

10 方式二: 如果 AUSF 需要后续使用到 Kausf, 则可以保存 Kausf。比如, AUSF 支持 SoR, UpU 流程, 则 AUSF 保存 Kausf。

方式三: AUSF 不生成 Kausf。比如, AUSF 判断是 NSW0 接入, 则不生成 Kausf。具体地, AUSF 可以生成 EMSK, 但是不将 EMSK 的前 256bit 用于 Kausf。进一步地, 可选地 EMSK 按照本身的 EAP 流程进行使用。比如作为 ERP 流程的根密钥。

15 示例性地, 如果 NSW0 场景支持 EAP 重鉴权流程 (EAP re-authentication protocol, ERP) 流程, 则当鉴权服务功能实体是 AUSF 的时候, 需要保存 Kausf 或者生成 Kausf 的 EMSK。

示例性地, 当鉴权服务功能实体是 3GPP AAA 的时候, 则可以不生成 Kausf。

20 可选地, S215, 鉴权服务功能实体向 UDM 发送 UE 认证结果确认请求 (Nudm_UEAuthentication_ResultConfirmation Request) 消息。

应理解, 在标准或者场景需要保存 Kausf, 或者网络侧需要记录 UE 的鉴权结果的情形下, 则执行步骤 S215。相应地, 在一种可能的实现方式中, 如果鉴权功能实体判断该 UE 正在使用 NSW0 模式接入, 则鉴权功能实体在认证 UE 成功后, 不需要发起 S215-S217 流程。需要说明的是, 在需要保存 Kausf 的情况下, 该步骤一定发生。

25 具体地, 关于网络侧是否需要记录 UE 的鉴权结果, 根据运营商需求或者标准规定而确定。

可选地, S216, UDM 存储当前 UE 通过非 3GPP 接入的鉴权成功状态。或者, 更具体地, UDM 存储当前 UE 通过 WLAN 接入下的鉴权成功状态, 或者, UDM 存储当前 UE 通过 NSW0 接入的鉴权成功状态。

30 如果执行步骤 S215, 则执行该步骤。如果步骤 S215 未执行, 则该步骤也不执行。

下面以两种可能的方式为例对 UDM 的存储方式进行详细说明。

方式一, UDM 维护一条鉴权成功状态信息。即, UDM 复用非 NSW0 接入方式发生鉴权的条目。UDM 在确定 NSW0 接入方式的初始鉴权成功后, UDM 更新该条目。UDM 更新方式有 2 种可能: 第一种, 增加一条记录 NSW0 模式鉴权成功, 并新增 (比如, 在
35 UE 没有通过 3GPP 和非 NSW0 接入方接入过的情况下, 即没有任何鉴权发生过的情况下) 此次鉴权经过的鉴权服务功能实体的 ID 或者替换原有的鉴权服务功能实体的 ID; 第二种是在已有的条目中信息增加一个标识该鉴权成功状态为 NSW0 模式的信息, 但是不替换已有的鉴权服务功能实体的 ID 或者新增鉴权服务功能实体的 ID。此时该鉴权成功状态的相关信息中不包括 NSW0 接入模式下使用的鉴权服务功能实体的 ID。

40 应理解, 不存储为 NSW0 服务的鉴权功能实体 ID 是因为通过 NSW0 鉴权的 UE 不

需要网络侧为维护该 UE 的状态。该 UE 可能每次使用 NSWO 服务的时候重新发生鉴权流程，因此 UDM 也不需要维护该 UE 的鉴权相关的状态信息，比如是否鉴权成功。

方式二，UDM 可以维护两条鉴权状态信息，一条用于 3GPP 接入和非 NSWO 接入流程中发送的主鉴权流程，另一条用于 NSWO 接入发生的主鉴权流程。该两条鉴权成功状态的相关信息中均包括鉴权服务功能实体的 ID 和一个指示信息。其中，一条鉴权状态的相关信息中的记录当前 UE 通过 NSWO 接入方法发起鉴权的鉴权结果，或者可以指示 UE 通过 NSWO 方式发起鉴权的鉴权结果；另一条鉴权成功状态的相关信息中的该指示信息可以指示当前 UE 通过 5GC（或者更具体地，AMF）发起鉴权的鉴权结果，或者指示 UE 通过 3GPP 接入和非 NSWO 接入发起的鉴权的鉴权的结果。

应理解，存储鉴权服务功能实体的 ID 可以方便于 UDM 找到为 UE 在 NSWO 场景鉴权的鉴权服务功能实体，并可以使用鉴权服务功能实体保存的密钥。

方式三，UDM 只接收消息，不做任何处理。

S217，UDM 回复 UE 认证结果确认响应（Nudm_UEAuthentication_ResultConfirmation Response）消息给鉴权服务功能实体。

S218，鉴权服务功能实体与 UE 进行可选的多轮 EAP 交互。

需要说明的是，S215 和 S218 的编号的大小并不对执行顺序造成限定，即，S218 可以在 S215 之前执行，也可以在 S215 之后执行。S217 与 S218 可以没有任何关联关系。

S219-S220，鉴权服务功能实体通过 Wi-Fi AP 发送 EAP 成功（EAP-Success）消息给 UE。在步骤 S219 中，鉴权服务功能实体将生成的 MSK 发送给 Wi-Fi AP。

S221，UE 认证鉴权服务功能实体的真实性。

可选地，UE 生成 Kausf。如果鉴权服务功能实体为 AUSF 或包括 AUSF，且步骤 S212 没有生成 Kausf，则他们在此步生成。具体生成方式可以参见 S212 中相应的描述。

S222，UE 与 Wi-Fi AP 完成安全建立。

示例性地，UE 基于 MSK 生成 kwlan，基于 kwlan 进行安全建立。Kwlan 可以是用于 UE 后续与网络侧通信的密钥，或者，后续 UE 和网络侧还可以根据 kwlan 继续派生出用于通信的密钥。

本申请实施例，将 NSWO 场景应用到 5G 系统中，扩展了 NSWO 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSWO 场景下 UE 与 5GC 的鉴权流程。另外，在 NSWO 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。同时，UDM 在记录鉴权成功状态时可以通过只记录通过 NSWO 鉴权成功的状态而不记录鉴权服务功能实体的 ID，维护简单，需要更改的网元较少，方便快捷商用；或者，可以将通过 NSWO 鉴权成功状态与鉴权服务功能实体的 ID 绑定，使得 UDM 记录的条目更为清晰。

下面结合图 6，对本申请提供的安全通信的方法 300 进行详细说明。图 6 是本申请的方法 300 的示意性交互图。方法 300 中通过鉴权服务功能实体生成的 SN name 或指示信息向 UDM 指示选择 EAP-AKA' 鉴权方法。

S301 可以参考 S201 中的相关描述，S302 可以参考 S202 中的相关描述。

S303，UE 生成 SUCI，具体实现可以参考目前 UE 生成 SUCI 的方法。

S304 可以参考 S204 中的相关描述，S305 可以参考 S205 中的相关描述。

S306, 鉴权服务功能实体生成 SN name。

为了指示 UDM 选择 EAP-AKA' 鉴权方法, 这里鉴权服务功能实体可以采用以下两种指示方式, 分别通过 SN name 指示或通过 SN name 之外的指示信息来指示接入方法或鉴权方法。

- 5 指示方式一, 鉴权服务功能实体生成 SN name 或者从接收到的消息中获取 SN name 的全部或者部分信息。

鉴权服务功能实体生成的 SN name 可以包括以下至少一项: 鉴权服务功能实体的标识, 或终端设备所在网络的标识, 或接入技术类型指示信息, 或接入方法指示信息等。

- 10 其中, (1) 这里的终端设备所在网络的标识包括服务网络的标识或接入网络的标识。这里的接入网络的标识可以理解为 Wi-Fi AP 所在网络的标识。一般情况下, 服务网络的标识理解为 AMF 所在网络的标识, 由于本申请实施例不经过 AMF, 这里的服务网络的标识可以理解为 proxy (如果 UE 接入的网络架构中包括 proxy) 的标识, 或者可以理解为接入网络的标识 (如果 UE 接入的网络架构中不包括 proxy)。(2) 技术类型指示信息用于指示 UE 使用的接入技术的类型, 比如接入技术可以是 3GPP 接入技术, 非 3GPP 接入技术, WLAN 接入技术, 蓝牙接入技术, 微波接入技术等。(3) 接入方法指示信息用于指示 UE 计划使用的接入网络的方法, 比如是使用 NSW0 方法, 非 NSW0 接入方法, 3GPP 接入方法, 微波接入方法。不管是技术类型指示信息还是接入方法指示信息, 其作用是给网络提供一种信息, 供网络获取 UE 当前的特征, 以影响网络对 UE 的鉴权方法的决定。

- 20 应理解, 接入类型指示信息、或者接入方法指示信息可以由鉴权服务功能实体自己生成, 也可以在接收消息中获取。比如, 接入类型指示信息、或者接入方法指示信息可以由 Wi-Fi AP 添加, 那么 Wi-Fi AP 可以在步骤 S204 中, 在 Wi-Fi AP 将该消息转发给鉴权服务功能实体传递 EAP 消息的同时将接入类型指示信息、或者接入方法指示信息携带在消息中。再比如, 接入类型指示信息、或者接入方法指示信息可以由 UE 添加, 那么 UE 在步骤 S204 中, 随着 EAP 消息发送给鉴权服务功能实体。

- 25 需要说明的是, 在本申请实施例中, 技术类型指示信息和接入方法指示信息用来指示 UE 当前使用的是 NSW0 接入方法, 最终目的是让 UDM 参考所述指示信息, 并最终选择到 EAP-AKA' 鉴权方法。

- 30 一方面, 鉴权服务功能实体可以根据消息来源或者消息中携带的信元, 确定接入方法, 生成 SN name。比如, 当鉴权服务功能实体从 AMF 收到需要对 UE 进行鉴权的消息的时候, 鉴权服务功能实体可以确定是 3GPP 接入方法或者是非 NSW0 接入方法。再比如, 如果信元中可以携带网络功能类型, 鉴权服务功能实体可以根据网络功能类型确定消息发送方是一个 AMF, 还是 Wi-Fi-AP 或者是一个 Proxy。

- 35 示例性地, 当鉴权服务功能实体从 Wi-Fi AP, 或者非 AMF 功能实体收到需要对 UE 进行鉴权的消息时, 鉴权服务功能实体确定是 NSW0 接入, 或者确定不是非 NSW0 接入。之后, 鉴权服务功能实体用接入网络标识 (access network identity) 或者接入网络类型 (access network type) 等具有区分接入方法的标识符来标识具体的接入方法, 并根据上述标识符生成 SN name。

- 40 另一方面, 接入网络标识 (access network identity), 或者接入网络类型 (access network type) 也可以是由鉴权服务功能实体从 UE 或者 Wi-Fi AP 获取。例如, UE 在步骤 S204 中, 将 access network identity 或 access network type 随着 EAP 消息发送给鉴权服务功能实体,

或者，Wi-Fi AP 可以在步骤 S204 中将 access network identity 或 access network type 加在发送给鉴权服务功能实体的 EAP 响应/AKA' 身份认证消息中。

5 在一个示例中，鉴权服务功能实体根据消息来源或者指示信息确定接入方法后，获取或者生成 access network identity, access network type。比如，access network identity 可以是 Wi-Fi AP 所在网络的 ID，可以是 Wi-Fi AP 自己的 ID，也可以是蓝牙 ID，或者为一种 UDM 可以识别的与目前的服务网络名称进行区分的 ID。应理解，该目前的服务网络可以理解为 AMF 所在的服务网络或者运营商服务网络，本申请中服务网络名称 (SN name) 10 通过与该目前的服务网络名称进行区分，从而可以使得 UDM 根据 SN name 中的 ID 判断出 UE 从哪个服务网络接入 access network type 可以指示接入网络类型，接入网络类型用于指示具体的无线空口技术，比如“WLAN”，或“WLAN access network”，或“NSWO”，或“Bluetooth”，或“microwave”，或 Restrictive non-3GPP access network type I, 或 Restrictive non-3GPP access network type II, 或 Restrictive non-3GPP access network type I。为了与已有的 SN name 拥有相同的格式，可以依然在 SN name 前加上 5G，比如是 5G: access network identity, 5G: access network type。再比如还可以是 5G: WLAN, 5G: Wi-Fi AP 等格式。15 或者，也可以不考虑与已有 SN name 拥有相同格式关联，比如只传递接收到的或者生成的 access network identity，或者只传递接收到的或者生成的 access network type。本申请实施例对具体的格式不做限制。

因此，本申请实施例中鉴权服务功能实体生成的 SN name 与 3GPP 接入和非 NSWO 接入情况下使用的 SN name 进行区别，以具有指示作用。

20 指示方式二，鉴权服务功能实体得到或者生成一个指示信息 06，该指示信息 06 用于指示 UDM 选择 EAP-AKA' 鉴权方法。

或者，该指示信息 06 也可以用于指示 UE 在 NSWO 场景下接入，或者 UE 使用 NSWO 方式接入，以便于 UDM 根据指示信息 06 选择 EAP-AKA' 鉴权方法。

25 在一定场景下，可能存在指示信息 05 和指示信息 06 合并在一起传递。例如，可以将指示信息 05 和指示信息 06 合并在一起后通过 SN name 对应的信元 (information element, IE) 进行传递，这样做可以减少因为新引入功能而带来的改动。

30 作为一个示例，上述 SN name 可以是 5G:NSWO.mnc015.mcc234.3gppnetwork.org.NSWO indicator。作为另一个示例，上述 SN name 还可以是 5G:mnc015.mcc234.3gppnetwork.org.NSWO。或者，该 SN name 还可以是其他的格式，本申请实施例对具体的格式不做限制。

示例性地，指示信息 06 可以由鉴权服务功能实体根据消息来源生成，或者根据收到的 SN name 的部分或全部生成，或者由鉴权服务功能实体从 Wi-Fi AP 传递的消息中获得。指示信息 06 可以通过 UE 认证获取请求消息发给 UDM。认证获取请求消息可以是 Nudm_UEAuthentication_Get Request 消息。

35 S307 可以参考 S207 中的相关描述，S308 可以参考 S208 中的相关描述。

S309，UDM 根据 SN name 或指示信息 06 选择 EAP-AKA' 鉴权方法。

与 S306 中的指示方式一对应，UDM 判断 SN name 中的具体内容，例如是接入网络类型，或者接入网络标识信息，则 UDM 选择 EAP-AKA' 鉴权方法。

40 示例性地，UDM 根据 SN name 确定终端设备在 NSWO 场景下接入网络，从而选择 EAP-AKA' 与终端设备进行鉴权。

与 S306 中的指示方式二对应, UDM 收到 SN name 和用于指示 UDM 接入方式或者指示 UDM 需要选择 EAP-AKA' 鉴权方法的指示信息 06, 确定选择 EAP-AKA' 鉴权方法。

可选地, 在 UDM 选择选择 EAP-AKA' 鉴权方法之前, UDM 验证该 UE 是否有权限使用 NSW0 模式。比如, UDM 验证 UE 是否有权限使用 SN Name 表示的服务网络。再比如, UDM 根据 UE 的签约数据进行验证。再比如, UDM 先根据 UE 的签约数据进行验证, 验证成功后, 再验证 UE 是否有权限使用 SN Name 表示的服务网络。如果 UE 授权验证成功, 则执行步骤 S310。如果 UE 授权验证失败, 则向鉴权服务器发送拒绝消息, 并携带拒绝原因值。

在 UDM 选择 EAP-AKA' 鉴权方法后, 生成 EAP-AKA' 相关的鉴权向量 AV。在 SN name 包括指示信息 05 和指示信息 06 的情况下, UDM 可以直接使用包括指示信息 05 和指示信息 06 的 SN name 获得 EAP-AKA' 相关的鉴权向量, 或者, UDM 也可以只使用指示信息 05 相关的部分作为 SN name。比如, 当 SN name 为 5G:NSWO.mnc015.mcc234.3gppnetwork.org. NSW0 indicator, 则 UDM 使用 5G:NSWO.mnc015.mcc234.3gppnetwork.org 作为 SN Name, 或者使用 5G:NSWO 作为 SN name。

S310-S322 可以分别参考 S210-S222 中的相关描述。

需要额外说明的是, 步骤 S312, UE 可以自己获取 SN name, 也可以通过步骤 S311 获取 SN name。UE 得到的 SN name 的类型可以参考步骤 S306 的相关描述。UE 在 EAP-AKA' 中使用 SN name 的方法可以参考步骤 S309 中的相关描述。

本申请实施例, 将 NSW0 场景应用到 5G 系统中, 扩展了 NSW0 接入方式的应用范围, 并通过指示 UDM 选择 EAP-AKA' 鉴权方法, 能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外, 在 NSW0 场景下, 终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF, 减轻了 AMF 的负担, 也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。同时, 相对于目前 UDM 保存的鉴权状态而言, 可以通过只记录鉴权成功的状态而不记录鉴权服务功能实体的 ID, 维护简单, 需要更改的网元较少, 方便快捷商用; 或者, 可以在鉴权成功状态与鉴权服务功能实体绑定的基础上添加与是否经过 NSW0 方式发起鉴权的指示信息, 使得 UDM 记录的条目更为清晰。

可选地, 在 S306 中, 鉴权服务功能实体除了通过上述 SN name 或者指示信息 06 向 UDM 指示选择 EAP-AKA' 鉴权方法外, 还可以有其他的实现方式。示例性地, 鉴权服务功能实体向 UDM 指示的接入方法可以是 NSW0 接入还是非 NSW0 接入, 鉴权方法可以是 5G-AKA 还是 EAP-AKA'。相应地, 当鉴权服务功能实体向 UDM 指示接入方法的时候, UDM 可以根据接入方法进一步决定要选择的鉴权方法。比如, 如果指示 NSW0 接入, 则 UDM 选择 EAP 鉴权方法。如果指示 3GPP 或者非 NSW0 接入, 则 UDM 基于 SUPI 选择鉴权方法。当鉴权服务功能实体向 UDM 指示鉴权方法的时候, UDM 可以直接确定鉴权方法。

可选的, 如果在 S307 中, UDM 收到的 SN name 不是 S306 中的 SN name, 也没有收到 S306 中的指示信息 06, 则 UDM 可以按照目前 5G 网络中 UDM 选择鉴权方式的方法确定鉴权方法, 即根据 SUPI 选择鉴权方法。或者, UDM 也可以根据 SN name 是 AMF 所在的服务网络的名称, 确定是 3GPP 接入还是非 NSW0 接入, 然后再根据 SUPI 选择鉴权方法。这样的话, UDM 相当于可以根据不同的 SN name 为其选择合适的鉴权方法。

需要说明的是, 指示 UDM 选择 EAP-AKA' 鉴权方法的方式可以单独使用, 例如方

法 200 或方法 300, 也可以结合使用, 例如将方法 300 中 S303 替换成方法 200 中的 S203 的部分或全部方案, 并且将方法 200 中 S209 中与 S203 中对应的方案添加进方法 300 的 S309 中, 或者还可以以其他的方式进行结合使用, 本申请对此不做限定。

下面结合图 7, 对本申请提供的安全通信的方法 400 进行详细说明。图 7 是本申请的方法 400 的示意性交互图。

如图 7 所示, 在方法 400 中, 鉴权服务功能实体由 2 个网元组成: 代理和 AUSF。

S401 具体参见上述 S201 的描述, S402 具体参见上述 S202 的描述。

S403, 根据 SUPI 生成 SUCI, 或者生成指示信息 02。

可能的实现方式一, 具体可以参见 S203 中的描述。

可能的实现方式二, 具体可以参见 S303 中的描述。

S404 具体参见上述 S204 的描述。

S405, Wi-Fi AP 将 S404 中的从 UE 接收的消息转发给代理 (proxy)。

具体地, Wi-Fi AP 根据预配置的信息, 或者根据 SUCI 中的 Home Network Identifier 找到 Proxy, 并将 EAP-Response/Identity 消息发送给 Proxy。Proxy 作为下一个网元的前一跳, Proxy 转发消息给哪个网元, 就是哪个网元的 Proxy。

应理解, 在方法 400 中, 加入 proxy 的目的或作用可以包括以下几点:

(1) 为了找到 UE 对应的 AUSF: 该 Proxy 的下一跳是 AUSF, 在方法 400 中, 该 Proxy 的下一跳是 AUSF, 因此可以称为是 AUSF Proxy, 或者, 又可以称为 AUSF-P。

(2) 降低下一跳网元的暴露面, 或者在 Wi-Fi AP 无法直接找到下一跳网元的情况下起到中转消息的作用。下面以方法 400 的 AUSF 为例进行解释说明。因为 AUSF 是处理鉴权相关的网元, 需要保存 UE 的密钥 Kausf, 如果 AUSF 被攻击者控制, 那么攻击者就可以拿到很多 UE 的密钥。因此 AUSF 要尽量减少被非核心网网元直接找到的可能性。因为 Wi-Fi AP 是一个网际互连协议 (Internet Protocol, IP) 网元, 可能是一个不被运营商信任的网元, 因此 Wi-Fi AP 直接连接 AUSF 对于 AUSF 的安全性会造成严重威胁。因此, 在这种情况下, 需要一个 Proxy 先接收来自 Wi-Fi AP 的消息。

(3) Proxy 也可能有一些安全功能, 比如拦截被篡改的要发给 AUSF 的数据包。

(4) 进行服务化消息和非无服务化消息的转换。

需要说明的是, 在具体实现中, Proxy 可以是一个单独的网元, 也可以跟非 3GPP 互通功能 (non-3GPP interworking function, N3IWF)、演进型分组数据网关 (evolved packet data gateway, ePDG)、可信 WLAN 合作功能 (trusted WLAN interworking function, TWIF)、3Gpp-AAA 服务器等网元进行合设。也就是说, N3IWF、ePDG、TWIF、3Gpp-AAA 服务器本身就具有 Proxy 的功能。

S406, 生成 SN name, 或者接收用于生成 SN name 或组成 SN name 的部分参数, 或者, 生成指示信息 03。

具体地, 方法 200 和方法 300 中的鉴权服务功能实体在方法 400 中由代理和 AUSF 构成, 因此 S406 也可以由代理或 AUSF 执行。S406 具体实现中可以有多种方式, 比如下文的 S406a 或 S406b。

S406a, 代理生成 SN name, 或者从 Wi-Fi AP 接收用于生成 SN name 或组成 SN name 的部分参数, 或者生成指示信息 03。

或者, 代理还可以将用于生成 SN name 或组成 SN name 的部分参数发送给 AUSF。

具体地, 关于代理生成 SN name 或指示信息 03 可以由多种实现方式。

可能的实现方式一, 与 S403 中可能的实现方式一对应, S406a 具体可以参考 S206 中关于鉴权服务功能实体的描述。

5 应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, 那么 S406a 中参考 S206 按照一般情况生成 SN name, 那么在 S411 中参考 S209, 通过 UE 生成的 SUCI 或指示信息 05 向 UDM 指示鉴权方法。

可能的实现方式二, 与 S403 中可能的实现方式二对应, S406a 具体可以参考 S306 中关于鉴权服务功能实体的描述。

10 应理解, S403 中按照一般情况生成 SUCI, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S309, 通过代理生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

可能的实现方式三, 与 S403 中可能的实现方式一对应, S406a 具体可以参考 S306 中关于鉴权服务功能实体的描述。

15 应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S209 和 S309, 通过 UE 生成的 SUCI 或指示信息 05, 以及代理生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

示例性地, 代理根据自己的 network ID 生成 SN name。再比如, 代理根据从 UE 收到的组成 SN name 的参数生成 SN name。

20 进一步地, 可选地, 代理可以根据 RID 的值在本地选择、或者通过 NRF 选择支持 NSWO 鉴权功能的 AUSF。

S406b, AUSF 生成 SN name, 或者从代理接收用于生成 SN name 或组成 SN name 的部分参数, 或者生成指示信息 03。

具体地, 关于 AUSF 生成 SN name 和指示信息 03 可以由多种实现方式。

25 可能的实现方式一, 与 S403 中可能的实现方式一对应, S406b 具体可以参考 S206 中关于鉴权服务功能实体的描述。

应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, 那么 S406a 中参考 S206 按照一般情况生成 SN name, 那么在 S411 中参考 S209, 通过 UE 生成的 SUCI 或指示信息 05 向 UDM 指示鉴权方法。

30 可能的实现方式二, 与 S403 中可能的实现方式二对应, S406b 具体可以参考 S306 中关于鉴权服务功能实体的描述。

应理解, S403 中按照一般情况生成 SUCI, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S309, 通过 AUSF 生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

35 可能的实现方式三, 与 S403 中可能的实现方式一对应, S406b 具体可以参考 S306 中关于鉴权服务功能实体的描述。

应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S209 和 S309, 通过 UE 生成的 SUCI 或指示信息 05, 以及 AUSF 生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

40 示例性地, AUSF 从代理接收代理的 network ID, 并根据该 network ID 生成 SN name。再比如, AUSF 从代理接收的参数可以是代理从 UE 或 Wi-Fi-AP 接收到的用于组成或生成

SN name 的部分参数, AUSF 据此生成 SN name, 例如是 AUSF 根据从代理处接收的接入网络标识 (access network identity) 或者接入网络类型 (access network type) 生成 SN name。

S407, 代理发送 UE 认证请求 (Nausf_UEAuthentication_Authenticate Request) 消息给 AUSF。消息中携带有 SUCI。可选地, 如果 S406 按照 S406a 进行实现, 则该消息中还包
5 括代理生成的 SN name。

S408, AUSF 基于 SUCI 选择 UDM。

可选地, 如果 S407 中 AUSF 接收的消息中没有携带 SN name, S406 按照 S406b 实现。

S409 具体参见 S207 的描述, S410 具体参见 S208 的描述。

S411, UDM 选择 EAP-AKA' 作为鉴权方法。

10 可能的实现方式一, 与 S406 中可能的实现方式一对应, S411 具体可以参考 S209 中关于鉴权服务功能实体的描述。

应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, 那么 S406a 中参考 S206 按照一般情况生成 SN name, 那么在 S411 中参考 S209, 通过 UE 生成的 SUCI 或指示信息 05 向 UDM 指示鉴权方法。

15 可能的实现方式二, 与 S406 中可能的实现方式二对应, S411 具体可以参考 S309 中关于鉴权服务功能实体的描述。

应理解, S403 中按照一般情况生成 SUCI, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S309, 通过 AUSF 或代理生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

20 可能的实现方式三, 与 S406 中可能的实现方式三对应, S411 具体可以参考 S209 和 S309 中关于鉴权服务功能实体的描述。

应理解, S403 中生成 S203 中的 SUCI 或指示信息 05, S406a 中参考 S306 生成 SN name 或指示信息 06, 那么在 S411 中参考 S209 和 S309, 通过 UE 生成的 SUCI 或指示信息 05, 以及 AUSF 或代理生成的 SN name 或指示信息 06 向 UDM 指示鉴权方法。

25

S412, UDM 回复认证获取响应 (Nudm_UEAuthentication_Get Response) 消息给 AUSF。消息中携带鉴权向量 AV 和 SUPI。

S413, AUSF 回复 UE 认证响应 (Nausf_UEAuthentication_Authenticate Response) 消息给 Proxy。

30 S414, 代理通过 EAP 请求 (EAP Request) 消息转发 AV 和生成的 SN Name 给 UE。或者, 这里的 EAP Request 还可以是 AKA' -Challenge 消息。

S415 具体参见 S212 的描述。

S416, UE 发送 EAP 响应 (EAP Response) 消息给代理。或者, 这里的 EAP Response 还可以是 AKA' -Challenge 消息。

35 S417, 代理发送 UE 认证请求 (Nausf_UEAuthentication_Authenticate Request) 消息给 AUSF。

S418, AUSF 验证 UE 的真实性, 并生成 MSK。

如图 8 所示, AUSF 可以通过如下密钥架构通过多种方法生成 MSK。

图 8 中的 (a) 所示的密钥架构中, 网络侧, UDM 根据 K 生成 CK 和 IK, 随后将 CK 和 IK 发送给 AUSF, AUSF 收到 CK' 和 IK' 后, 生成 MSK 和 EMSK。其中, EMSK 的
40

高 256bit 将被作为 Kausf。AUSF 在将 MSK 发送给 Wi-Fi AP, Wi-Fi AP 根据 MSK 生成 kwlan。类似的, 在 UE 侧, 由全球用户识别卡 (universal subscriber identity module, USIM) 和移动设备 (mobile equipment, ME) 执行与网络侧相同的步骤。

5 第一种方法, 在 AUSF 收到 CK' 和 IK' 后, 生成 MSK 和 EMSK。其中, EMSK 的高 256bit 将被作为 Kausf。因为 MSK 目前没有被使用, 因此 AUSF 直接发送 MSK 给 Wi-Fi AP。

10 如果 UDM 在步骤 S426 中保存条目采用方式一, 则可以不保存 Kausf, 或者也可以保存 Kausf, 覆盖上一次鉴权过程中的 Kausf。其中, 如果不保存 Kausf, 可以避免与非 NSW0 场景下的 Kausf 混淆, 因为 SOR, UPU 等流程只会在非 NSW0 场景下发生, 而不会在 NSW0 场景下发生。如果保存 Kausf, 覆盖上一次鉴权过程中的 Kausf, 则与目前 AUSF 保存 UE 鉴权成功的条目兼容, 即不管是什么场景发生的鉴权, 只要生成 Kausf, 就需要保存。在另一种可能中, 如果 NSW0 场景支持 ERP 鉴权, 则需要生成并保存 Kausf。

如果 UDM 在保存条目采用方式二, 则 AUSF 可以保存 Kausf。

15 图 8 中的 (b) 示出了另一种密钥架构, 与第一种密钥架构的区别在于由 Kausf 进一步生成 MSK。

20 第二种方法, 由 Kausf 进一步生成 MSK。Kausf 生成 MSK 的方法可以有多种。例如, 将 SN name 作为输入参数生成 MSK, 或者, 将 "WLAN" 作为输入参数生成 MSK, 或者, 将 SUPI 作为输入参数生成 MSK。进一步地, 还可以引入区分符, 不同的接入场景使用不同的值进行区分。比如 MSK = KDF (Kausf, 区分符, 区分符长度, SUPI, SUPI 长度)。使用区分符可以减少 Kausf, 适应将来的开发逻辑, 减少开发工作量, 加快商用速度。

另外, 对于 Kausf 的保存参考第一种方法中的描述。

25 图 8 中的 (c) 所示的密钥架构与图 8 中的 (a) 所示的密钥架构区别在于将 EMSK 的低 256bit 作为基础密钥, 直接作为 MSK 或者作为根密钥生成新的 MSK。

第三种方法, 将 EMSK 的低 256bit 作为基础密钥, 直接作为 MSK 或者作为根密钥生成新的 MSK。生成新的 MSK 的方法, 可以参考第二种方法的描述。对于 Kausf 的保存方法, 参考第一种方法描述。使用第 256bit 作为基础密钥的好处是防止密钥混淆。EMSK 的高 256bit 密钥作为 AMF 要参与鉴权的密钥根密钥, 低 256bit 密钥则作为其他鉴权发生时的根密钥。

30 S419 具体参见 S218 中的描述。

S420, AUSF 向代理发送 UE 认证响应 (Nausf_UEAuthentication_Authenticate Response) 消息。该消息中不携带 UE 的 SUPI。

可以理解的是, 在该场景中, Wi-Fi AP 无法感知 UE 的 SUPI, 也没有任何其他网元需要感知 UE 的 SUPI, 因此 AUSF 在该消息中不携带 UE 的 SUPI。

35 而在 UE 经过 AMF 进行鉴权时, 如果 AUSF 收到的是 SUCI, 则该步骤一定要携带 SUPI, 因为 SUPI 要发给 AMF。

S421-S424 可以参见 S219 至 S222。

需要说明的是, S423 中, UE 要生成与步骤 S418 中相同的 MSK。其中, MSK 的生成方法、Kausf 的保存均可以参考步骤 S418 的描述。

40 S425 可以参见 S215 的描述。其中, 用于执行鉴权功能实体的网元为 AUSF。与 S215

中类似地，在一种可能的实现方式中，如果鉴权功能实体判断该 UE 正在使用 NSW0 模式接入，则 AUSF 在认证 UE 成功后，不需要发起 S425-S427 流程。

S426，UDM 保存 UE 通过非 3GPP 接入的认证状态。

UDM 会记录 UE 鉴权成功的状态，可以采取以下两种可能的方式进行记录。

5 方式一，UDM 只为 UE 维护一个条目。

可能的情况一，如果该 AUSF 与 UE 之前发生过鉴权，那么该 UDM 使用本次鉴权使用的 AUSF ID 覆盖之前鉴权成功后保存的 AUSF ID。在这种情况下，AUSF 和 UE 都需要生成和存储 Kausf。如果有非 NSW0 鉴权，则 NSW0 鉴权使用的 AUSF ID 可以覆盖也可以不覆盖之前的非 NSW0 鉴权。若 NSW0 鉴权可以覆盖 AUSF ID，那么则是遵循目前的一般情况，即要求 UDM 只保存最后一次鉴权的 AUSF 对应的 Kausf。

10

示例性地，UDM 维护的条目如表 1 所示。

表 1

UE ID = SUPI	NSWO 鉴权	成功	AUSF ID(使用 NSW0 鉴权的 AUSF ID 替换已有的 AUSF ID)
--------------	---------	----	--

可能的情况二，UDM 只记录非 NSW0 鉴权时使用的 AUSF ID。在这种情况下，AUSF 和 UE 均不需要生成 Kausf，或者生成 Kausf 但不需要存储 Kausf。在这种情况下，也可以理解为若 NSW0 鉴权不覆盖 AUSF ID，那么是因为 UPU 和漫游选择(steering of roaming, SoR)流程只可以通过 AMF 发生，因此通过 AMF 鉴权发生后，才可能需要 UPU 和 SoR。换句话说，NSWO 鉴权因为不通过 AMF，因此与 UPU 和 SoR 没有任何关系。所以在这种理解下，NSWO 鉴权使用的 AUSF ID 和生成的 Kausf，是不需要被后续使用的。

15

示例性地，UDM 维护的条目如表 2 所示，结合第二列与第四列表示 UE 通过 NSW0 鉴权成功，结合第三列与第四列标识 UE 通过非 NSW0 鉴权成功，第五列的 AUSF ID 为非 NSW0 鉴权成功时记录的 AUSF ID。

20

表 2

UE ID = SUPI	NSWO 鉴权	非 NSW0 鉴权	成功	AUSF ID
--------------	---------	-----------	----	---------

方式二，UDM 为 UE 维护 2 条鉴权成功的条目。

其中，UDM 记录的一个条目标记为 WLAN 鉴权或 NSW0 鉴权，用来与 UE 经过 AMF 与 AUSF 鉴权生成的上下文进行区分。如果 UE 在通过 WLAN 接入前经过 AMF 与 AUSF 已经进行过鉴权并生成了安全上下文 Kausf，则 AUSF 还记录另一个条目，并将该条目标记为是通过 AMF 鉴权。此时，当 UDM 发起 SoR 流程或者 UE 参数更新(UE parameter update, UPU)流程的时候，UDM 要使用通过 AMF 鉴权生成的 Kausf 对 SoR 和 UPU 流程需要保护的参数进行保护。当 UDM 发起对 NSW0 场景 ERP 重鉴权的时候，要使用 NSW0 接入场景下鉴权过程中的 Kausf。即，此时 Kausf 可以用于 ERP 流程。

25

30

示例性的，表 3 示出了 AUSF 维护的同一个 UE 的 2 条鉴权成功的条目。其中，通过第二列“NSWO 鉴权”和“非 NSW0 鉴权”来区分是否经过 AMF 接入 AUSF 进行鉴权，第四列的 AUSF ID 用于指示哪个 AUSF 在存储 Kausf，所以这里的两种方案最主要的目的是，让 UDM 明确应该使用哪个 AUSF 与 UE 通过非 3GPP 进行通信，这样就可以确定用哪个密钥去做保护。此时，当 UDM 发起 SoR 流程或者 UPU 流程的时候，UDM 要使用表 3 中的非 NSW0 鉴权条目中的 AUSF ID 对应的 AUSF 存储的 Kausf 对 SoR 和 UPU 流程需要保护的参数进行保护。当 UDM 发起对 NSW0 场景 ERP 重鉴权的时候，要使用 NSW0

35

接入场景下鉴权过程中的 Kausf。UDM 要使用 NSW0 鉴权条目中的 AUSF ID 对应的 AUSF 存储的 Kausf 或者 EMSK 进行重鉴权流程。

表 3

UE ID = SUPI	NSWO 鉴权	成功	AUSF ID
	非 NSW0 鉴权	成功	AUSF ID

需要说明的是，本申请实施例是以 AUSF 执行鉴权功能为例进行说明，因此 UDM 记录的鉴权服务功能实体的 ID 均为 AUSF ID，如果鉴权服务功能实体为其他网元，则 UDM 记录的鉴权服务功能实体的 ID 即为其他网元的 ID，本申请对此不做限定。示例性地，鉴权服务功能实体为 AAA 服务器，则鉴权服务功能实体记录的 ID 为 AAA ID。

S427 可以参见 S217 的描述。

本申请实施例，将 NSW0 场景应用到 5G 系统中，扩展了 NSW0 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSW0 场景下 UE 与 5GC 的鉴权流程。另外，在 NSW0 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。同时，相对于目前 UDM 保存的鉴权状态而言，可以通过只记录鉴权成功的状态而不记录鉴权服务功能实体的 ID，维护简单，需要更改的网元较少，方便快捷商用；或者，可以在鉴权成功状态与鉴权服务功能实体绑定的基础上添加与是否经过 NSW0 方式发起鉴权的指示信息，使得 UDM 记录的条目更为清晰。另外，通过由代理和 AUSF 组成鉴权服务功能实体，减少 AUSF 的暴露面，进一步提高安全性能；通过兼容目前的密钥架构生成用于 UE 和网络侧通信的密钥的根密钥，完善鉴权和密钥分发机制，减少开发工作量，加快商用速度。

下面结合图 9，对本申请提供的安全通信的方法 500 进行详细说明。图 9 是本申请的方法 500 的示意性交互图。

方法 500 相对于方法 400 而言，区别在于：

(1) 将方法 400 中的 AUSF 替换成 AAA 服务器，从而使得方法 400 中的密钥架构也需要做相应更改。因为 AAA 服务器不需要生成 Kasuf，因此 AAA 服务器在第 18 步，直接生成 MSK 和 EMSK，不需要将 EMSK 的高 256bit 当做 Kausf。AAA 服务器然后将 MSK 发送给 Wi-Fi AP。

(2) 在 S526 中，如果 UDM 采用方式二记录 UE 鉴权成功的条目，那么条目需要包含 AAA 服务器的标识，即 AAA ID，以此来基于 UE 通过哪个 AAA 服务器鉴权成功。

本申请实施例，在方法 400 的有益效果的基础上，能够实现 NSW0 场景下鉴权通过 AAA 服务器，非 NSW0 场景下的鉴权通过 AUSF，通过网元的不同实现天然的分离，使得两种鉴权方式更加独立和清晰。

方法 500 中除上述区别外的步骤均可以参见方法 400 中的相关步骤。

下面结合图 10，对本申请提供的安全通信的方法 600 进行详细说明。图 10 是本申请的方法 600 的示意性交互图。

方法 600 相对于方法 500，区别在于：

(1) 将方法 500 中的代理替换为 AAA 服务器，将方法 500 中的 AUSF 替换为 AAA 协议和服务化协议的转换网元，有缝 WLAN 分流鉴权和授权功能 (non-seamless WLAN Offload authentication and authorization function, NSW0AAF)。该 NSW0AAF 专门处理

NSWO 场景下的鉴权流程，是鉴权服务功能实体。方法 600 中的鉴权过程、密钥生成过程可以发送 AAA 服务器上，具体可以参考方法 500 中的相应描述。而在鉴权过程中，NSWOAAF 做协议转换使用。其中，NSWOAAF 可以是一个单独的功能或网元或实体，也可以是 AUSF 的一部分。

5 (2) S607 中与 S507 中的消息内容一样，消息名称可以不一样，例如，S607 中的消息名称可以是请求 AKA 认证 (request AKA vector)。

 (3) S613 中与 S513 中的消息内容一样，消息名称可以不一样，例如，S613 中的消息名称可以是返回 AKA 认证 (return AKA vector)。

 本申请实施例，将 NSWO 场景应用到 5G 系统中，扩展了 NSWO 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSWO 场景下 UE 与 5GC 的鉴权流程。另外，在 NSWO 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

 下面结合图 11，对本申请提供的安全通信的方法 700 进行详细说明。图 11 是本申请的方法 700 的示意性交互图。

 方法 700 相对于方法 400，区别在于：

 将方法 400 中的代理替换为 AAA 服务器，该 AAA 服务器负责 AAA 协议和服务化协议的转换，并在架构中添加 AAA 代理，该 AAA 代理负责在 Wi-Fi AP 无法直接找到 AAA 服务器时找到 3GPP AAA 服务器，AUSF 负责鉴权和密钥衍生。

20 方法 700 中的信息交互可以参考方法 400 中类似的步骤，AAA 代理与 AAA 服务器之间的交互步骤如图 11 所示。

 本申请实施例，将 NSWO 场景应用到 5G 系统中，扩展了 NSWO 接入方式的应用范围，并通过指示 UDM 选择 EAP-AKA' 鉴权方法，能够完善 NSWO 场景下 UE 与 5GC 的鉴权流程。另外，在 NSWO 场景下，终端设备可以在通过非 3GPP 接入技术接入 5GC 时不经过 AMF，减轻了 AMF 的负担，也节省了部署 UE 通过非 3GPP 技术接入到 5GC 的架构的开销。

 以上，结合图 1 至图 11 详细说明了本申请实施例提供的方法。以下，结合图 12 至图 13 详细说明本申请实施例提供的装置。

30 图 12 是本申请实施例提供的用于安全通信的通信装置的示意性框图。如图 12 所示，该通信装置 10 可以包括收发模块 11 和处理模块 12。

 其中，收发模块 11 可以用于接收其他装置发送的信息，还可以用于向其他装置发送信息。比如，接收第一消息或发送第一指示信息。处理模块 12 可以用于进行装置的内容处理，比如，根据第一消息生成第一指示信息。

 在一种可能的设计中，该通信装置 10 可对应于上述方法实施例中的终端设备。

35 具体地，该通信装置 10 可对应于根据本申请实施例的方法 100 至方法 700 中任一方法中的终端设备或 UE，该通信装置 10 可以包括用于执行相应方法中由终端设备所执行的操作的模块，并且，该通信装置 10 中的各单元分别为了实现相应方法中由终端设备所执行的操作。

 示例性的，在该通信装置 10 对应于方法 100 中的终端设备时，收发模块 11 用于执行步骤 S101、S103，处理模块 12 用于执行 S102。

示例性的，在该通信装置 10 对应于方法 200 中的 UE 时，收发模块 11 用于执行步骤 S201、S202、S204、S211、S213、S218、S220、S222，处理模块 12 用于执行 S203、S212、S221。

5 示例性的，在该通信装置 10 对应于方法 300 中的 UE 时，收发模块 11 用于执行步骤 S301、S302、S304、S311、S313、S318、S320、S322，，处理模块 12 用于执行 S303、S312、S321。

示例性的，在该通信装置 10 对应于方法 400 中的 UE 时，收发模块 11 用于执行步骤 S401、S402、S404、S414、S416、S419、S422、S424，处理模块 12 用于执行 S403、S415、S423。

10 示例性的，在该通信装置 10 对应于方法 500 中的 UE 时，收发模块 11 用于执行步骤 S501、S502、S504、S514、S516、S519、S522、S524，处理模块 12 用于执行 S503、S515、S523。

示例性的，在该通信装置 10 对应于方法 600 中的 UE 时，收发模块 11 用于执行步骤 S601、S602、S604、S614、S616、S619、S622、S624，处理模块 12 用于执行 S603、S615、15 S623。

示例性的，在该通信装置 10 对应于方法 700 中的 UE 时，收发模块 11 用于执行步骤 S701、S702、S704、S714、S716、S719、S722、S724，处理模块 12 用于执行 S703、S715、S723。

具体地，在一种可能的实施例中，收发模块 11，收发模块，用于接收来自无线访问接入点的消息；处理模块 12，用于根据该消息生成指示信息，该指示信息表示该终端设备处于有缝的无线局域网分流 NSW0 场景；该收发模块，还用于发送该指示信息。

其中，该处理模块 12，还用于根据该消息确定使用该 NSW0 的方式接入网络。

其中，该指示信息是网络接入标识 NAI 格式的用户隐藏标识 SUCI，或者是用户隐藏标识 SUCI 中的字段。

25 其中，该处理模块 12，还用于生成主会话密钥，该主会话密钥用于生成该终端设备与网络通信的密钥，该网络为该终端设备通过该 NSW0 的方式接入的网络。

其中，该收发模块 11，具体还用于向统一数据管理实体或鉴权服务功能实体或该无线访问接入点发送该指示信息。

30 在另一种可能的设计中，该通信装置 10 可对应于上述方法实施例中的统一数据管理实体或 UDM。

具体地，该通信装置 10 可对应于根据本申请实施例的方法 100 至方法 700 中任一方法中的统一数据管理实体或 UDM，该通信装置 10 可以包括用于执行相应方法中由统一数据管理实体或 UDM 所执行的操作的模块，并且，该通信装置 10 中的各单元分别为了实现相应方法中由统一数据管理实体或 UDM 所执行的操作。

35 示例性的，在该通信装置 10 对应于方法 100 中的统一数据管理实体时，收发模块 11 用于执行步骤 S106，处理模块 12 用于执行步骤 S107。

示例性的，在该通信装置 10 对应于方法 200 中的 UDM 时，收发模块 11 用于执行步骤 S207、S210、S215、S217，处理模块 12 用于执行步骤 S208、S209、S216。

40 示例性的，在该通信装置 10 对应于方法 300 中的 UDM 时，收发模块 11 用于执行步骤 S307、S310、S315、S317，处理模块 12 用于执行步骤 S308、S309、S316。

示例性的, 在该通信装置 10 对应于方法 400 中的 UDM 时, 收发模块 11 用于执行步骤 S409、S412、S425、S427, 处理模块 12 用于执行步骤 S410、S411、S426。

示例性的, 在该通信装置 10 对应于方法 500 中的 UDM 时, 收发模块 11 用于执行步骤 S509、S512、S525、S527, 处理模块 12 用于执行步骤 S510、S511、S526。

5 示例性的, 在该通信装置 10 对应于方法 600 中的 UDM 时, 收发模块 11 用于执行步骤 S609、S612、S624、S626, 处理模块 12 用于执行步骤 S610、S611、S625。

示例性的, 在该通信装置 10 对应于方法 700 中的 UDM 时, 收发模块 11 用于执行步骤 S709、S712、S725、S727, 处理模块 12 用于执行步骤 S710、S711、S726。

具体地, 在一种可能的实施例中, 收发模块 11, 用于接收来自鉴权服务功能实体的指示信息; 处理模块 12, 用于根据该指示信息在至少两种鉴权方式中选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权。

其中, 该指示信息是网络接入标识 NAI 格式的用户隐藏标识 SUCI, 或者是用户隐藏标识 SUCI 中的字段。

15 其中, 该指示信息包括以下任意一个或多个: 该鉴权服务功能实体的标识, 或该终端设备所在网络的标识, 或接入技术类型指示信息, 或接入方法指示信息, 该接入类型指示信息用于指示接入网络类型, 该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

其中, 该处理模块 12, 还用于存储标识该终端设备通过有缝的无线局域网分流 NSW0 的方式接入该网络的信息; 或者, 该处理模块 12, 还用于存储标识该终端设备通过该 NSW0 的方式接入该网络的信息, 以及该鉴权服务功能实体的标识。

其中, 该终端设备通过有缝的无线局域网分流 NSW0 的方式接入该网络的信息用于可扩展认证协议 EAP 重鉴权流程。

在另一种可能的设计中, 该通信装置 10 可对应于上述方法实施例中的鉴权服务实体或 AUSF 或 proxy 或 AAA 服务器或 NSW0AAF。

25 具体地, 该通信装置 10 可对应于根据本申请实施例的方法 100 至方法 700 中任一方法中的鉴权服务实体或 AUSF 或 proxy 或 AAA 服务器或 NSW0AAF, 该通信装置 10 可以包括用于执行相应方法中由鉴权服务实体或 AUSF 或 proxy 或 AAA 服务器或 NSW0AAF 所执行的操作的模块, 并且, 该通信装置 10 中的各单元分别为了实现相应方法中由鉴权服务实体或 AUSF 或 proxy 或 AAA 服务器或 NSW0AAF 所执行的操作。

30 示例性的, 在该通信装置 10 对应于方法 100 中的鉴权服务功能实体时, 收发模块 11 用于执行步骤 S103, S104, S106, 处理模块 12 用于执行步骤 S105。

示例性的, 在该通信装置 10 对应于方法 200 中的鉴权服务功能实体时, 收发模块 11 用于执行步骤 S204、S207、S210、S211、S213、S215、S217、S218、S219, 处理模块 12 用于执行步骤 S205、S206、S214。

35 示例性的, 在该通信装置 10 对应于方法 300 中的鉴权服务功能实体时, 收发模块 11 用于执行步骤 S304、S307、S310、S311、S313、S315、S317、S318、S319, 处理模块 12 用于执行步骤 S305、S306、S314。

40 示例性的, 在该通信装置 10 对应于方法 400 中的 AUSF 时, 收发模块 11 用于执行步骤 S407、S409、S4122、S413、S417、S418、S420、S425、S427, 处理模块 12 用于执行步骤 S408、S406b、S418。

示例性的，在该通信装置 10 对应于方法 500 中的 AAA 服务器时，收发模块 11 用于执行步骤 S507、S509、S512、S513、S517、S520、S525、S527，处理模块 12 用于执行步骤 S508、S506b、S518。

5 示例性的，在该通信装置 10 对应于方法 600 中的 AAA 服务器时，收发模块 11 用于执行步骤 S502、S504，处理模块 12 用于执行步骤 S606、S617。

示例性的，在该通信装置 10 对应于方法 700 中的 AUSF 时，收发模块 11 用于执行步骤 S707、S709、S701、S713、S717、S720、S725、S727，处理模块 12 用于执行步骤 S708、S706b、S718。

10 具体地，在一种可能的实施例中，收发模块 11，用于接收来自无线访问接入点的消息；该处理模块 12，用于根据该消息生成指示信息，该指示信息用于指示统一数据管理实体选择可扩展认证协议-认证和密钥协商 EAP-AKA' 与终端设备进行鉴权；该收发模块 11，还用于向该统一数据管理实体发送该指示信息。

其中，该鉴权服务功能实体的标识，或该终端设备所在网络的标识，或接入技术类型指示信息，或接入方法指示信息，该接入类型指示信息用于指示接入网络类型，该接入方法指示信息用于指示该终端设备使用的接入技术的特征。

其中，该处理模块 12，还用于根据该消息确定该终端设备通过 NSW0 的方式接入网络。

其中，该处理模块 12，还用于生成主会话密钥，该主会话密钥用于生成该终端设备与该网络通信的密钥；该收发模块，还用于向该无线访问接入点发送该主会话密钥。

20 图 13 为本申请实施例提供的安全通信的装置 20 的示意图。

在一种可能的设计中，该装置 20 可以为统一数据管理实体，也可以为位于统一数据管理实体上的芯片或芯片系统等。

在一种可能的设计中，该装置 20 可以为鉴权服务功能实体，也可以为位于鉴权服务功能实体上的芯片或芯片系统等。

25 在一种可能的设计中，该装置 20 可以为终端设备包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备，以及各种形式的终端，移动台，终端，用户设备，软终端等等，也可以为位于终端设备上的芯片或芯片系统等。

30 该装置 20 可以包括处理器 21（即，处理模块的一例）和存储器 22。该存储器 22 用于存储指令，该处理器 21 用于执行该存储器 22 存储的指令，以使该装置 20 实现如图 4 至图 11 中对应的方法中上述各种可能的设计中的设备执行的步骤。

35 进一步地，该装置 20 还可以包括输入口 23（即，收发模块的一例）和输出口 24（即，收发模块的另一例）。进一步地，该处理器 21、存储器 22、输入口 23 和输出口 24 可以通过内部连接通路互相通信，传递控制和/或数据信号。该存储器 22 用于存储计算机程序，该处理器 21 可以用于从该存储器 22 中调用并运行该计算机程序，以控制输入口 23 接收信号，控制输出口 24 发送信号，完成上述方法中终端设备或无线接入网设备或 UE 或基站的步骤。该存储器 22 可以集成在处理器 21 中，也可以与处理器 21 分开设置。

40 可选地，若该报文传输的装置 20 为通信设备，该输入口 23 为接收器，该输出口 24 为发送器。其中，接收器和发送器可以为相同或者不同的物理实体。为相同的物理实体时，可以统称为收发器。

可选地，若该装置 20 为芯片或电路，该输入口 23 为输入接口，该输出口 24 为输出接口。

作为一种实现方式，输入口 23 和输出口 34 的功能可以考虑通过收发电路或者收发的专用芯片实现。处理器 21 可以考虑通过专用处理芯片、处理电路、处理器或者通用芯片实现。

作为另一种实现方式，可以考虑使用通用计算机的方式来实现本申请实施例提供的设备。即将实现处理器 21、输入口 23 和输出口 24 功能的程序代码存储在存储器 22 中，通用处理器通过执行存储器 22 中的代码来实现处理器 21、输入口 23 和输出口 24 的功能。

其中，装置 20 中各模块或单元可以用于执行上述方法中进行随机接入的设备（例如，终端设备）所执行的各动作或处理过程，这里，为了避免赘述，省略其详细说明。

该装置 20 所涉及的与本申请实施例提供的技术方案相关的概念，解释和详细说明及其他步骤请参见前述方法或其他实施例中关于这些内容的描述，此处不做赘述。

应理解，本申请实施例中，该处理器可以为中央处理单元（CPU，central processing unit），该处理器还可以是其他通用处理器、数字信号处理器（DSP，digital signal processor）、专用集成电路（application specific integrated circuit，ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

本申请实施例还提供一种计算机可读存储介质，其上存储有用于实现上述方法实施例中由鉴权服务功能实体或统一数据管理实体或终端设备执行的方法的计算机指令。

例如，该计算机程序被计算机执行时，使得该计算机可以实现上述方法实施例中由鉴权服务功能实体或统一数据管理实体或终端设备执行的方法。

本申请实施例还提供一种计算机可读存储介质，其上存储有用于实现上述方法实施例中由鉴权服务功能实体或统一数据管理实体或终端设备执行的方法的计算机指令。

例如，该计算机程序被计算机执行时，使得该计算机可以实现上述方法实施例中由鉴权服务功能实体或统一数据管理实体或终端设备执行的方法。

还应理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory，ROM）、可编程只读存储器（programmable ROM，PROM）、可擦除可编程只读存储器（erasable PROM，EPROM）、电可擦除可编程只读存储器（electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（static RAM，SRAM）、动态随机存取存储器（DRAM）、同步动态随机存取存储器（synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM，DR RAM）。

上述实施例，可以全部或部分地通过软件、硬件、固件或其他任意组合来实现。当使用软件实现时，上述实施例可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令

或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质。半导体介质可以是固态硬盘。

10 应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

15 应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

30 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

40 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖

在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

权 利 要 求 书

1. 一种安全通信的方法，其特征在于，包括：
终端设备和无线访问接入点建立连接；
所述终端设备接收来自所述无线访问接入点的可扩展认证协议 EAP 请求或认证消息；
5 所述终端设备使用国际移动用户识别码 IMSI 生成网络接入标识 NAI 格式的用户隐藏标识 SUCI，其中，所述 SUCI 包括指示信息，所述指示信息用于指示有缝的无线局域网分流 NSWO 的接入方式；
所述终端设备向所述无线访问接入点发送 EAP 响应或身份认证消息，所述 EAP 响应或身份认证消息包括所述 SUCI。
- 10 2. 根据权利要求 1 所述的方法，其特征在于，所述终端设备和所述无线访问接入点建立连接包括：
在所述终端设备和所述无线访问接入点建立连接过程中，所述终端设备接收到来自所述无线访问接入点的消息，确定所述终端设备使用所述 NSWO 方式接入网络。
3. 根据权利要求 2 所述的方法，其特征在于，所述终端设备确定所述终端设备使用
15 所述 NSWO 方式接入网络包括：
所述终端设备根据本地保存的服务集标识 SSID 的列表，确定符合所述列表的 SSID 使用 NSWO 方式。
4. 根据权利要求 1-3 中任一项所述的方法，其特征在于，所述指示信息在所述 NAI 格式的域名 example 部分。
- 20 5. 根据权利要求 1-4 中任一项所述的方法，其特征在于，还包括：
所述终端设备验证网络侧的真实性；
验证成功后，所述终端设备生成主会话密钥 MSK；
所述终端设备根据所述 NSWO 方式接入网络，不生成中间密钥 Kausf。
6. 根据权利要求 1-5 中任一项所述的方法，其特征在于，所述终端设备在生成所述
25 SUCI 时忽略本地保存的安全上下文和 5G 全局唯一的临时标识 5G-GUTI。
7. 一种安全通信的方法，其特征在于，包括：
认证服务功能实体的代理接收来自无线访问接入点的消息；
所述代理生成服务网络名称，所述服务网络名称包括接入网络的标识和接入方法指示
30 信息，所述接入网络为所述无线访问接入点所在的网络，所述接入方法指示信息用于指示终端设备使用的接入网络的方式为有缝的无线局域网分流 NSWO；
所述代理向所述认证服务功能实体发送终端设备认证请求消息，所述终端设备认证请求消息包括所述终端设备的用户隐藏标识 SUCI 和所述服务网络名称。
8. 根据权利要求 7 所述的方法，其特征在于，所述方法还包括：
所述代理接收来自所述认证服务功能实体的终端设备认证响应消息。
- 35 9. 根据权利要求 7 或 8 所述的方法，其特征在于，所述方法还包括：
所述代理通过可扩展认证协议 EAP 请求消息向所述终端设备转发鉴权向量和所述服务网络名称；
所述代理接收来自所述终端设备的 EAP 响应消息。

10. 一种安全通信的方法，其特征在于，包括：
鉴权服务功能实体接收来自终端设备的可扩展认证协议 EAP 响应或认证和密钥协商 AKA' 邀请消息；
所述鉴权服务功能实体验证所述终端设备的真实性，并生成主会话密钥 MSK；
5 所述鉴权服务功能实体判断所述终端设备使用有缝的无线局域网分流 NSW0 的方式接入网络，则不生成中间密钥 Kausf；
所述鉴权服务功能实体通过无线访问接入点发送 EAP 成功消息给所述终端设备；
所述鉴权服务功能实体将所述 MSK 发送给所述无线访问接入点。
11. 根据权利要求 10 所述的方法，其特征在于，所述方法还包括：
10 所述鉴权服务功能实体向统一数据管理实体发送终端设备认证结果确认请求消息；
所述鉴权服务功能实体接收来自所述统一数据管理实体的终端设备认证结果确认响应消息。
12. 根据权利要求 10 或 11 所述的方法，其特征在于，所述方法还包括：
所述鉴权服务功能实体与所述终端设备进行可选的多轮 EAP 交互。
13. 一种安全通信的装置，其特征在于，包括：
15 至少一个处理器；以及
存储器，耦合到所述至少一个处理器，用于存储所述至少一个处理器执行的指令，以指示所述至少一个处理器：
和无线访问接入点建立连接；
20 接收来自所述无线访问接入点的可扩展认证协议 EAP 请求或认证消息；
使用国际移动用户识别码 IMSI 生成网络接入标识 NAI 格式的用户隐藏标识 SUCI，其中，所述 SUCI 包括指示信息，所述指示信息用于指示有缝的无线局域网分流 NSW0 的接入方式；
向所述无线访问接入点发送 EAP 响应或身份认证消息，所述 EAP 响应或身份认证消息包括所述 SUCI。
14. 根据权利要求 13 所述的装置，其特征在于，所述指令还指示所述至少一个处理器：
在和所述无线访问接入点建立连接过程中，接收到来自所述无线访问接入点的消息，确定所述装置使用 NSW0 方式接入网络。
15. 根据权利要求 14 所述的装置，其特征在于，所述指令还指示所述至少一个处理器：
30 根据本地保存的服务集标识 SSID 的列表，确定符合所述列表的 SSID 使用 NSW0 方式。
16. 根据权利要求 13-15 中任一项所述的装置，其特征在于，所述指示信息在所述 NAI 格式的域名 example 部分。
17. 根据权利要求 13-16 中任一项所述的装置，其特征在于，所述指令还指示所述至少一个处理器：
验证网络侧的真实性；
验证成功后，生成主会话密钥 MSK；
40 根据所述 NSW0 方式接入网络，不生成中间密钥 Kausf。

18. 根据权利要求 13-17 中任一项所述的装置, 其特征在于, 所述至少一个处理器在生成所述 SUCI 时忽略本地保存的安全上下文和 5G 全局唯一的临时标识 5G-GUTI。

19. 一种安全通信的装置, 其特征在于, 包括:

至少一个处理器; 以及

5 存储器, 耦合到所述至少一个处理器, 用于存储所述至少一个处理器执行的指令, 以指示所述至少一个处理器:

接收来自无线访问接入点的消息;

生成服务网络名称, 所述服务网络名称包括接入网络的标识和接入方法指示信息, 所述接入网络为所述无线访问接入点所在的网络, 所述接入方法指示信息用于指示终端设备使用的接入网络的方式为有缝的无线局域网分流 NSWO;

10 向所述认证服务功能实体发送终端设备认证请求消息, 所述终端设备认证请求消息包括所述终端设备的用户隐藏标识 SUCI 和所述服务网络名称。

20. 根据权利要求 19 所述的装置, 其特征在于, 所述指令还指示所述至少一个处理器:

15 接收来自所述认证服务功能实体的终端设备认证响应消息。

21. 根据权利要求 19 或 20 所述的装置, 其特征在于, 所述指令还指示所述至少一个处理器:

通过可扩展认证协议 EAP 请求消息向所述终端设备转发鉴权向量和所述服务网络名称;

20 接收来自所述终端设备的 EAP 响应消息。

22. 一种安全通信的装置, 其特征在于, 包括:

至少一个处理器; 以及

存储器, 耦合到所述至少一个处理器, 用于存储所述至少一个处理器执行的指令, 以指示所述至少一个处理器:

25 接收来自终端设备的可扩展认证协议 EAP 响应或认证和密钥协商 AKA' 邀请消息; 验证所述终端设备的真实性, 并生成主会话密钥 MSK;

判断所述终端设备使用有缝的无线局域网分流 NSWO 的方式接入网络, 则不生成中间密钥 Kausf;

通过无线访问接入点发送 EAP 成功消息给所述终端设备;

30 将所述 MSK 发送给所述无线访问接入点。

23. 根据权利要求 22 所述的装置, 其特征在于, 所述指令还指示所述至少一个处理器:

向统一数据管理实体发送终端设备认证结果确认请求消息;

接收来自所述统一数据管理实体的终端设备认证结果确认响应消息。

35 24. 根据权利要求 22 或 23 所述的装置, 其特征在于, 所述指令还指示所述至少一个处理器:

与所述终端设备进行可选的多轮 EAP 交互。

25. 一种安全通信的方法, 其特征在于, 包括:

认证服务功能实体的代理接收来自无线访问接入点的消息;

40 所述代理生成服务网络名称, 所述服务网络名称包括接入网络的标识和接入方法指示

信息,所述接入网络为所述无线访问接入点所在的网络,所述接入方法指示信息用于指示终端设备使用的接入网络的方式为有缝的无线局域网分流 NSW0;

所述代理向所述认证服务功能实体发送终端设备认证请求消息,所述终端设备认证请求消息包括所述终端设备的用户隐藏标识 SUCI 和所述服务网络名称;

5 所述认证服务功能实体接收来自所述代理的所述终端设备认证请求消息。

26. 根据权利要求 25 所述的方法,其特征在于,所述方法还包括:

所述代理接收来自所述认证服务功能实体的终端设备认证响应消息。

27. 根据权利要求 25 或 26 所述的方法,其特征在于,所述方法还包括:

10 所述代理通过可扩展认证协议 EAP 请求消息向所述终端设备转发鉴权向量和所述服务网络名称;

所述代理接收来自所述终端设备的 EAP 响应消息。

28. 一种安全通信的方法,其特征在于,包括:

鉴权服务功能实体接收来自终端设备的可扩展认证协议 EAP 响应或认证和密钥协商 AKA' 邀请消息;

15 所述鉴权服务功能实体验证所述终端设备的真实性,并生成主会话密钥 MSK;

所述鉴权服务功能实体判断所述终端设备使用有缝的无线局域网分流 NSW0 的方式接入网络,则不生成中间密钥 Kausf;

所述鉴权服务功能实体通过无线访问接入点发送 EAP 成功消息给所述终端设备;

所述无线访问接入点将所述 EAP 成功消息发给所述终端设备;

20 所述鉴权服务功能实体将所述 MSK 发送给所述无线访问接入点;

所述无线访问接入点接收所述 MSK。

29. 根据权利要求 28 所述的方法,其特征在于,所述方法还包括:

所述鉴权服务功能实体向统一数据管理实体发送终端设备认证结果确认请求消息;

25 所述鉴权服务功能实体接收来自所述统一数据管理实体的终端设备认证结果确认响应消息。

30. 根据权利要求 28 或 29 所述的方法,其特征在于,所述方法还包括:

所述鉴权服务功能实体与所述终端设备进行可选的多轮 EAP 交互。

31. 一种安全通信的系统,其特征在于,包括如权利要求 19 至 21 中任一项所述的装置和如权利要求 22 至 24 中任一项所述的装置。

30 32.一种计算机可读存储介质,其特征在于,所述存储介质中存储有计算机程序或指令,当所述计算机程序或指令被通信装置执行时,实现如权利要求 1 至 12 中任一项所述的方法。