

一种密钥标识的生成方法以及相关装置

技术领域

本申请涉及通信技术领域，尤其涉及一种密钥标识的生成方法以及相关装置。

背景技术

随着网络技术的快速的发展，网络安全成为日益突出的问题。随着第五代移动通信(the 5th generation, 5G)的发展，目前用户设备(user equipment, UE)与应用服务器(application function, AF)之间可以采用应用的认证和密钥管理(authentication and key management for application, AKMA)流程。在 AKMA 流程中，鉴权管理功能(authentication server function, AUSF)向统一数据管理功能(Unified Data Management, UDM)发送鉴权向量获取请求消息(Numid_UEAuthentication Get Request)，该鉴权向量获取请求消息中携带永久身份标识(subscriber permanent identifier, SUPI)或签约隐藏标识符(subscription concealed identifier, SUCI)，该鉴权向量获取请求消息用于触发 UE 与网络侧(核心网)之间的主鉴权(Primary authentication)流程。

该鉴权向量获取请求消息中携带 SUPI 或 SUCI 由 AUSF 接收的鉴权向量请求消息确定，当该鉴权请求消息中携带 SUPI 时，该鉴权向量获取请求消息中携带 SUPI；当该鉴权请求消息中携带 SUCI 时，该鉴权向量获取请求消息中携带 SUCI。

在 AKMA 流程中，AUSF 需要生成 AKMA 密钥临时身份标识(AKMA-Key Identifier, A-KID)，A-KID 也称为认证和密钥管理-密钥临时身份标识。目前规定，A-KID 需要基于路由标识(Routing Indicator, RID)生成，该路由标识在标准 TS 23.003 中定义，具体的，该路由标识可用于 AUSF 或 UDM 选择。而 RID 是 SUCI 的一部分，SUPI 中不包括 RID。当鉴权请求消息中携带的是 SUPI 时，AUSF 无法获取 RID。进而 AUSF 无法生成 A-KID，造成 AKMA 流程的失败。

发明内容

本申请实施例第一方面提供了一种密钥标识的生成方法，包括：鉴权管理功能接收来自接入与移动性管理功能鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；根据认证和密钥管理指示信息，鉴权管理功能基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；鉴权管理功能保存路由标识。

具体的，签约隐藏标识符(SUCI)可以理解为是永久身份标识(SUPI)的一种加密形式，例如可以参考 3GPP TS33.501 第 6.12.2 章节以及 TS23.003 第 2.2B 章节所述。具体的，SUCI 中可以包括路由标识以及加密部分。加密部分为用户加密的身份信息。一种可能的实现方式中，SUPI 中除移动国家代码(mobile country code, MCC)之外的部分可以由全球

用户识别卡 (universal subscriber identity module, USIM) 或移动设备 (mobile equipment, ME) 进行加密计算得到该加密部分。

该鉴权请求消息#1 为 “Nausf_UEAuthentication_Authenticate Request”。

该认证和密钥管理指示信息本申请实施例中也称为 AKMA 业务指示信息，该 AKMA 业务指示信息可以是 “AKMA Indication” 或 “AKMA ID”，本申请实施例中不作限定。AKMA 业务指示信息用于指示 AUSF 需要为这个 UE 生成 AKMA 锚点密钥 K_{akma} 以及对应的密钥标识符 (如认证和密钥管理-密钥临时身份标识)。也可以理解为：该 AKMA 业务指示信息用于指示该 UE 支持 AKMA 业务。

UDM 再次发送 RID 是为了确保 AUSF 处有可以使用的 RID。

本申请实施例中，在 AKMA 流程中，鉴权管理功能 AUSF 保存路由标识 RID 相关的参数 (例如：SUCI、认证和密钥管理-密钥临时身份标识 A-KID 和/或 RID)。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时，AUSF 可以使用该 RID 相关的参数生成新的 A-KID，保证 AKMA 流程的成功执行。

在一种可能的实现方式中，还包括：鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#2；在鉴权请求消息#2 中携带永久身份标识的情况下，鉴权管理功能使用保存的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。具体的，AUSF 基于该 SUPI，确定中间密钥 K_{ausf}，并使用 K_{ausf} 生成 A-KID#2。AUSF 基于保存的 RID，在接收 SUPI 的情况下可以生成新的 A-KID，保证 UE 的 AKMA 业务顺利执行。

在一种可能的实现方式中，鉴权管理功能基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1，包括：鉴权管理功能基于对终端设备进行鉴权流程中生成的中间密钥，生成认证和密钥管理-密钥临时身份标识；鉴权管理功能将路由标识和认证和密钥管理-密钥临时身份标识进行拼接，得到认证和密钥管理-密钥临时身份标识#1。

具体的，基于 RID 生成 A-KID 具体如下：A-KID 格式为 “username@example”。“username” 部分包括路由标识，和认证和密钥管理-终端设备临时身份标识 (AKMA Temporary UE Identifier, A-TID)。“example” 部分包括家乡网络标识，例如：移动国家代码 (mobile country code, MCC) 和移动网络代码 (mobile network code, MNC)。A-TID 是基于 K_{ausf} 生成的一个临时标识。

在一种可能的实现方式中，鉴权管理功能保存路由标识，包括：鉴权管理功能保存认证和密钥管理-密钥临时身份标识#1。现有技术中，鉴权管理功能生成认证和密钥管理-密钥临时身份标识#1 之后，会将生成的认证和密钥管理-密钥临时身份标识#1 发送给其他网元 (如认证和密钥管理锚点功能)，然后删除生成的认证和密钥管理-密钥临时身份标识#1。由于 A-KID 中包括路由标识，鉴权管理功能后续收到基于 SUPI 的鉴权向量请求消息时，依然可以为终端设备生成对应的 A-KID，从而保证了 AKMA 流程的顺利进行。

在一种可能的实现方式中，鉴权向量获取响应消息#1 中还包括路由标识；鉴权管理功能基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1，包括：鉴权管理功能基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-密钥临时身份标识#1。AUSF 该可以基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-

密钥临时身份标识#1，提升了方案的实现灵活性。

在一种可能的实现方式中，鉴权管理功能保存路由标识，包括：鉴权管理功能保存签约隐藏标识符。提升了方案的实现灵活性。

在一种可能的实现方式中，鉴权管理功能保存路由标识之后，还包括：鉴权管理功能
5 删除认证和密钥管理-密钥临时身份标识#1。AUSF 保存路由标识之后，还可以删除认证和
密钥管理-密钥临时身份标识#1，以节省 AUSF 的存储空间。

在一种可能的实现方式中，鉴权管理功能基于保存的路由标识生成认证和密钥管理-密
钥临时身份标识#2 之后，还包括：鉴权管理功能删除认证和密钥管理-密钥临时身份标识#2；
鉴权管理功能继续保存路由标识。AUSF 保存的路由标识生成认证和密钥管理-密钥临时身
10 份标识#2 之后，还可以删除认证和密钥管理-密钥临时身份标识#2，以节省 AUSF 的存储空
间。AUSF 还可以继续保存路由标识，以确保 AKMA 业务的成功执行。

第二方面，本申请实施例提出一种密钥标识的生成方法，包括：鉴权管理功能接收来
自接入与移动性管理功能的鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签
约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；鉴权管理功能向统一
15 数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标
识符；鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获
取响应消息#1 包括认证和密钥管理指示信息和签约隐藏标识符中的路由标识；根据认证和
密钥管理指示信息，鉴权管理功能基于路由标识生成认证和密钥管理-密钥临时身份标识#1。

本申请实施例中，在 AKMA 流程中，AUSF 可以从 UDM 中获取 RID。以保证 AUSF
20 接收的鉴权向量获取请求消息中携带 SUPI 时，AUSF 可以使用该 RID 生成新的 A-KID，
保证 AKMA 流程的成功执行。

在一种可能的实现方式中，还包括：鉴权管理功能接收来自接入与移动性管理功能的
鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；鉴权管理功能向统一数据管理功能
发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；鉴权管理
25 功能接收来自统一数据管理功能的鉴权向量获取响应消息#2，鉴权向量获取响应消息#2 包
括路由标识；鉴权管理功能使用路由标识生成新的认证和密钥管理-密钥临时身份标识#2。
本实施例中，AUSF 可以从 UDM 中获取路由标识，提升了方案的实现灵活性。

在一种可能的实现方式中，还包括：鉴权管理功能接收来自接入与移动性管理功能的
鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；鉴权管理功能向统一数据管理功能
30 发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；鉴权管理
功能根据认证和密钥管理指示信息，从核心网网元获取路由标识；鉴权管理功能使用路由
标识生成新的认证和密钥管理-密钥临时身份标识#2。本实施例中，AUSF 可以从其它的核
心网网元中获取路由标识，以确保 AKMA 业务的成功执行，提升了方案的实现灵活性。

在一种可能的实现方式中，鉴权管理功能根据认证和密钥管理指示信息，从其他核心
35 网网元获取路由标识，包括：鉴权管理功能根据认证和密钥管理指示信息，确定需要生成
认证和密钥管理-密钥临时身份标识#2；在鉴权管理功能本地没有路由标识的情况下，鉴权
管理功能从核心网网元获取路由标识。

具体的，AUSF 还检测 AUSF 本地是否保存有 RID 相关的参数（例如 RID、SUCI 和/或 A-KID）。当检测结果为鉴权请求消息#2 中没有 RID（或者鉴权请求消息#2 没有 RID，且，AUSF 本地没有 RID 相关的参数），则 AUSF 从核心网网元获取路由标识。

可选的，核心网网元包括统一数据管理功能或者接入与移动性管理功能。

5 本实施例中，AUSF 在本地没有路由标识的情况下，从其它的核心网网元中获取路由标识，以确保 AKMA 业务的成功执行，提升了方案的实现灵活性。

在一种可能的实现方式中，在鉴权管理功能根据认证和密钥管理指示信息，从核心网网元获取路由标识之前，还包括：鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#2，鉴权向量获取响应消息#2 包括认证和密钥管理指示信息。AUSF 在接收认证和密钥管理指示信息的情况下，AUSF 才可以确认该 UE 支持 AKMA 业务。因此，在此之后 AUSF 才会从核心网网元获取路由标识，避免信令的浪费。

第三方面，本申请实施例提出一种密钥标识的生成方法，包括：鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；根据认证和密钥管理指示信息，鉴权管理功能基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#2；其中，鉴权请求消息#2 包括永久身份标识和路由标识；鉴权管理功能使用从接入与移动性管理功能接收到的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

本申请实施例中，在 AKMA 流程中，AMF 判断 UE 支持 AKMA 业务的情况下，AUSF 可以从 AMF 中获取 RID。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时，AUSF 可以使用该 RID 生成新的 A-KID，保证 AKMA 流程的成功执行。

25 在一种可能的实现方式中，在鉴权管理功能使用从接入与移动性管理功能接收到的路由标识生成新的认证和密钥管理-密钥临时身份标识#2 之前，还包括：鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#2，其中，鉴权向量获取请求消息#2 中携带永久身份标识；鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#2。本实施例中，AMF 可以在鉴权请求消息中携带 RID，AUSF 从该鉴权请求消息中获取 RID，提升了方案得实现灵活性。

30 在一种可能的实现方式中，在鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#2 之前，还包括：鉴权管理功能向接入与移动性管理功能发送第一鉴权请求响应；第一鉴权请求响应包括第一指示信息，第一指示信息用于指示终端设备支持应用的认证和密钥管理业务。本实施例中，AUSF 还可以通过其它指示信息（第一指示信息），通知 AMF 该 UE 支持 AKMA 业务，提升了方案得实现灵活性。

35 在一种可能的实现方式中，鉴权向量获取响应消息#1 中还包括路由标识；鉴权管理功能基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1，包括：鉴

权管理功能基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-密钥临时身份标识#1。本实施例中,AUSF还可以通过来着 AMF 的鉴权向量获取响应消息#1 中的 RID,生成认证和密钥管理-密钥临时身份标识#1,提升了方案得实现灵活性。

5 第四方面,本申请实施例提出一种密钥标识的生成方法,包括:鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#2;鉴权请求消息#2 包括永久身份标识;鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#2,鉴权向量获取请求消息#2 中携带永久身份标识;鉴权管理功能接收来自统一数据管理功能的鉴权向量获取响应消息#2,鉴权向量获取响应消息#2 包括认证和密钥管理指示信息;鉴权管理功能根据认证和密钥管理指示信息,确定需要生成认证和密钥管理-密钥临时身份标识;在鉴权管理功能本地没有路由标识的情况下,鉴权管理功能从核心网网元获取路由标识;鉴权管理功能使用路由标识生成认证和密钥管理-密钥临时身份标识#2。

具体的,AUSF 还检测 AUSF 本地是否保存有 RID 相关的参数(例如 RID、SUCI 和/或 A-KID)。当检测结果为鉴权请求消息#2 中没有 RID(或者鉴权请求消息#2 没有 RID,且,AUSF 本地没有 RID 相关的参数),则 AUSF 从核心网网元获取路由标识。

15 可选的,核心网网元包括统一数据管理功能或者接入与移动性管理功能。

本申请实施例中,在 AKMA 流程中,AUSF 可以从 UDM 或 AMF 等核心网网元中获取 RID。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时,AUSF 可以使用该 RID 生成新的 A-KID,保证 AKMA 流程的成功执行。

第五方面,本申请实施例提出一种通信装置,包括:

20 收发模块,用于接收来自接入与移动性管理功能鉴权请求消息#1,鉴权请求消息#1 中携带签约隐藏标识符,签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识;

收发模块,还用于向统一数据管理功能发送鉴权向量获取请求消息#1,鉴权向量获取请求消息#1 中携带签约隐藏标识符;

25 收发模块,还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1,鉴权向量获取响应消息#1 包括认证和密钥管理指示信息;

处理模块,用于根据认证和密钥管理指示信息,基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1;

处理模块,还用于保存路由标识。

30 在一种可能的实现方式中,收发模块,还用于接收来自接入与移动性管理功能的鉴权请求消息#2;

处理模块,还用于在鉴权请求消息#2 中携带永久身份标识的情况下,使用保存的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

35 在一种可能的实现方式中,处理模块,还用于基于对终端设备进行鉴权流程中生成的中间密钥,生成认证和密钥管理-密钥临时身份标识;

处理模块,还用于将路由标识和认证和密钥管理-密钥临时身份标识进行拼接,得到认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块，还用于保存认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，鉴权向量获取响应消息#1 中还包括路由标识；

处理模块，还用于基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1，包括：

处理模块，还用于基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块，还用于保存签约隐藏标识符。

在一种可能的实现方式中，处理模块，还用于删除认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块，还用于删除认证和密钥管理-密钥临时身份标识#2；

处理模块，还用于继续保存路由标识。

第六方面，本申请实施例提出一种通信装置，包括：

收发模块，用于接收来自接入与移动性管理功能的鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；

收发模块，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息和签约隐藏标识符中的路由标识；

处理模块，用于根据认证和密钥管理指示信息，基于路由标识生成认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，收发模块，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；

收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2，鉴权向量获取响应消息#2 包括路由标识；

处理模块，还用于使用路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，收发模块，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；

收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块，还用于根据认证和密钥管理指示信息，从核心网网元获取路由标识；

处理模块，还用于使用路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，处理模块，还用于根据认证和密钥管理指示信息，确定需

要生成认证和密钥管理-密钥临时身份标识#2;

收发模块,还用于在鉴权管理功能本地没有路由标识的情况下,从核心网网元获取路由标识。

5 在一种可能的实现方式中,核心网网元包括统一数据管理功能或者接入与移动性管理功能。

在一种可能的实现方式中,收发模块,还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2,鉴权向量获取响应消息#2包括认证和密钥管理指示信息。

第七方面,本申请实施例提出一种通信装置,包括:

10 收发模块,用于接收来自接入与移动性管理功能的鉴权请求消息#1,鉴权请求消息#1中携带签约隐藏标识符,签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识;

收发模块,还用于向统一数据管理功能发送鉴权向量获取请求消息#1,鉴权向量获取请求消息#1中携带签约隐藏标识符;

15 收发模块,还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1,鉴权向量获取响应消息#1包括认证和密钥管理指示信息;

处理模块,用于根据认证和密钥管理指示信息,基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1;

收发模块,还用于接收来自接入与移动性管理功能的鉴权请求消息#2;其中,鉴权请求消息#2包括永久身份标识和路由标识;

20 处理模块,还用于使用从接入与移动性管理功能接收到的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中,收发模块,还用于向统一数据管理功能发送鉴权向量获取请求消息#2,其中,鉴权向量获取请求消息#2中携带永久身份标识;

收发模块,还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2。

25 在一种可能的实现方式中,收发模块,还用于向接入与移动性管理功能发送第一鉴权请求响应;第一鉴权请求响应包括第一指示信息,第一指示信息用于指示终端设备支持应用的认证和密钥管理业务。

在一种可能的实现方式中,处理模块,还用于基于鉴权向量获取响应消息#1中的路由标识生成认证和密钥管理-密钥临时身份标识#1。

30 第八方面,本申请实施例提出一种通信装置,包括:

收发模块,用于接收来自接入与移动性管理功能的鉴权请求消息#2;鉴权请求消息#2包括永久身份标识;

收发模块,还用于向统一数据管理功能发送鉴权向量获取请求消息#2,鉴权向量获取请求消息#2中携带永久身份标识;

35 收发模块,还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2,鉴权向量获取响应消息#2包括认证和密钥管理指示信息;

处理模块,还用于根据认证和密钥管理指示信息,确定需要生成认证和密钥管理-密钥

临时身份标识；

收发模块，还用于在鉴权管理功能本地没有路由标识的情况下，从核心网网元获取路由标识；

处理模块，还用于使用路由标识生成认证和密钥管理-密钥临时身份标识#2。

- 5 在一种可能的实现方式中，核心网网元包括统一数据管理功能或者接入与移动性管理功能。

10 本申请实施例第九方面提供一种通信装置，通信装置包括：处理器、存储器以及与处理器连接的收发器。存储器中存储有计算机程序或计算机指令，处理器还用于调用并运行存储器中存储的计算机程序或计算机指令，使得处理器实现如第一方面至第四方面中的任一

10 一方面或第一方面至第四方面中的任一方面的任意一种实现方式。

 可选的，处理器用于控制收发器执行如第一方面至第四方面中的任一方面的第一方面至第四方面中的任一方面的任意一种实现方式。

 本申请实施例第十方面提供一种包括计算机指令的计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如第一方面至第四方面中的任一方面的第一方面至第四方面中的任一方面的任意一种实现方式。

15 本申请实施例第十一方面提供一种计算机可读存储介质，包括计算机指令，当计算机指令在计算机上运行时，使得计算机执行如第一方面至第四方面中的任一方面的第一方面至第四方面中的任一方面的任意一种实现方式。

20 本申请实施例第十二方面提供一种通信装置，通信装置包括网络设备、终端设备或芯片等实体，通信装置包括处理器，用于调用存储器中的计算机程序或计算机指令，以使得处理器执行上述第一方面至第四方面中的任一方面的第一方面至第四方面中的任一方面的任意一种实现方式。

 可选的，处理器通过接口与存储器耦合。

25 本申请实施例第十三方面提供一种通信系统，通信系统包括第五方面的通信装置、第六方面的通信装置、第七方面的通信装置和/或第八方面的通信装置。

30 本申请实施例第十四方面还提供一种处理器，用于执行上述各种方法。在执行这些方法的过程中，上述方法中有关发送上述信息和接收上述信息的过程，可以理解为由处理器输出上述信息的过程，以及处理器接收输入的上述信息的过程。在输出上述信息时，处理器将该上述信息输出给收发器，以便由收发器进行发射。该上述信息在由处理器输出之后，还可能需要进行其他的处理，然后才到达收发器。类似的，处理器接收输入的上述信息时，收发器接收该上述信息，并将其输入处理器。更进一步的，在收发器收到该上述信息之后，该上述信息可能需要进行其他的处理，然后才输入处理器。

35 基于上述原理，举例来说，前述方法中提及的接收来自 AMF 的鉴权请求消息#1 可以理解为处理器输入用于鉴权请求消息#1。又例如，发送该鉴权向量获取请求消息#1 可以理解为处理器输出鉴权向量获取请求消息#1。

 对于处理器所涉及的发射、发送和接收等操作，如果没有特殊说明，或者，如果未与其在相关描述中的实际作用或者内在逻辑相抵触，则均可以更加一般性的理解为处理器输

出和接收、输入等操作，而不是直接由射频电路和天线所进行的发射、发送和接收操作。

在实现过程中，上述处理器可以是专门用于执行这些方法的处理器，也可以是执行存储器中的计算机指令来执行这些方法的处理器，例如通用处理器。上述存储器可以为非瞬时性（non-transitory）存储器，例如只读存储器（read only memory，ROM），其可以与处
5 理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型以及存储器与处理器的设置方式不做限定。

本申请实施例第十五方面提供了一种芯片系统，该芯片系统包括处理器和接口，所述接口用于获取程序或指令，所述处理器用于调用所述程序或指令以实现或者支持网络设备实现第一、第二、第三和/或第四方面所涉及的功能，例如，确定或处理上述方法中所涉及
10 的数据和信息中的至少一种。

在一种可能的设计中，所述芯片系统还包括存储器，所述存储器，用于保存网络设备必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包括芯片和其他分立器件。

附图说明

- 15 图 1a 为一种通信系统的网络架构示意图；
图 2 为本申请实施例中通信装置的硬件结构示意图；
图 3 为 UE 通过转发的接入流程示意图；
图 4 为本申请实施例提出的一种密钥标识的生成方法的实施例示意图；
图 5 为本申请实施例中又一种密钥标识的生成方法的实施例示意图；
20 图 6 为本申请实施例中又一种密钥标识的生成方法的实施例示意图；
图 7 为本申请实施例中又一种密钥标识的生成方法的实施例示意图；
图 8 为本申请实施例中又一种密钥标识的生成方法的实施例示意图；
图 9 为本申请实施例中通信装置的一种实施例示意图；
图 10 为本申请实施例中通信装置的一种实施例示意图；
25 图 11 为本申请实施例中通信装置的一种实施例示意图；
图 12 为本申请实施例中通信装置的一种实施例示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地
30 描述。显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”以及相应术语标号等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的
35 术语在适当情况下可以互换，这仅仅是描述本申请的实施例中对相同属性的对象在描述时所采用的区分方式。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，以便包含一系列单元的过程、方法、系统、产品或设备不必限于那些单元，

而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它单元。

在本申请的描述中，除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本申请中的“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，在本申请的描述中，“至少一项”是指一项或者多项，“多项”是指两项或两项以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a,b,或 c 中的至少一项(个)，可以表示：a,b,c,a-b,a-c,b-c,或 a-b-c，其中 a,b,c 可以是单个，也可以是多个。

本申请实施例的技术方案可以应用于各种通信系统，例如：宽带码分多址（Wideband Code Division Multiple Access, WCDMA）系统，通用分组无线业务（general packet radio service, GPRS），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 NR 以及未来的第六代通信系统等。

各种通信系统中由运营者运营的部分可称为运营商网络。运营商网络也可称为公用陆地移动网（public land mobile network, PLMN）网络，是由政府或政府所批准的经营者，以为公众提供陆地移动通信业务为目的而建立和经营的网络，主要是移动网络运营商

（mobile network operator, MNO）为用户提供移动宽带接入服务的公共网络。本申请实施例中所述的运营商网络或 PLMN 网络，可以为符合第三代合作伙伴项目（3rd generation partnership project, 3GPP）标准要求的网络，简称 3GPP 网络。通常 3GPP 网络由运营商来运营，包括但不限于第五代移动通信（5th-generation, 5G）网络（简称 5G 网络），第四代移动通信（4th-generation, 4G）网络（简称 4G 网络）或第三代移动通信技术（3rd-generation, 3G）网络（简称 3G 网络）。还包括未来的 6G 网络。为了方便描述，本申请实施例中将以运营商网络（如移动网络运营商（mobile network operator, MNO）网络）为例进行说明。

为了便于理解本申请实施例，以图 1a 所示的 5G 网络架构为例对本申请使用的应用场景进行说明，可以理解的是对其他通信网络与 5G 网络架构相似，因此不做赘述。请参阅图 1a，图 1a 为一种通信系统的网络架构示意图，所述网络架构中可以包括：终端设备（也可以称为用户设备部分，运营商网络部分和数据网络（data network, DN）部分。

终端设备部分包括终端设备 110，终端设备 110 也可以称为用户设备（user equipment, UE）。本申请实施例中所涉及的终端设备 110 作为一种具有无线收发功能的设备，可以经（无线）接入网（(radio)access network, (R)AN）140 中的接入网设备与一个或多个核心网（core network, CN）进行通信。终端设备 110 也可称为接入终端，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，无线网络设备，用户代理或用户装置等。终端设备 110 可以部署在陆地上，包括室内或室外，手持或车载；也可以部署在水面上（如轮船等）；还可以部署在空中（例如飞机，气球和卫星上等）。终端设备 110 可以是蜂窝电话（cellular phone），无绳电话，会话启动协议（session initiation protocol,

SIP)电话, 智能电话 (smart phone), 手机 (mobile phone), 无线本地环路 (wireless local loop, WLL) 站, 个人数字处理 (personal digital assistant, PDA), 可以是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设备, 车载设备, 可穿戴设备, 无人机设备或物联网, 车联网中的终端, 第五代移动通信 (fifth generation, 5G) 网络以及

5 未来网络中的任意形态的终端, 中继用户设备或者未来演进的公用陆地移动通信网络 (public land mobile network, PLMN) 中的终端等, 其中, 中继用户设备例如可以是 5G 家庭网关 (residential gateway, RG)。例如终端设备 110 可以是虚拟现实 (virtual reality, VR) 终端, 增强现实 (augmented reality, AR) 终端, 工业控制 (industrial control) 中的无线终端, 无人驾驶 (self driving) 中的无线终端, 远程医疗 (remote medical) 中的无线终端, 10 智能电网 (smart grid) 中的无线终端, 运输安全 (transportation safety) 中的无线终端, 智慧城市 (smart city) 中的无线终端, 智慧家庭 (smart home) 中的无线终端等。本申请实施例对此并不限定。为方便说明, 本申请实施例中以终端设备 110 包括无人机和无人机遥控器为例进行说明。

需要说明的是, 本申请实施例中涉及的无人机还可以包括: 可以自主进行行驶的车辆 15 (vehicle), 或基于遥控器的控制指令进行行驶的车辆; 可以自主进行航行的船舶 (shipping), 或基于遥控器的控制指令进行航行的船舶等。

运营商网络可以包括统一数据管理 (unified data management, UDM) 134, 鉴权管理功能 (authentication server function, AUSF) 136, 接入和移动性管理功能 (access and mobility management function, AMF) 137, 会话管理功能 (session management function, SMF) 138, 20 用户面功能 (user plane function, UPF) 139 以及 (R)AN140 等。上述运营商网络中, 除 (R)AN 140 部分之外的其他部分可以称为核心网络 (core network, CN) 部分或核心网部分。为方便说明, 本申请实施例中以 (R)AN 140 为 RAN 为例进行说明。

数据网络 DN 120, 也可以称为协议数据网络 (protocol data network, PDN), 通常是位于运营商网络之外的网络, 例如第三方网络。运营商网络可以接入多个数据网络 DN 120, 25 数据网络 DN 120 上可部署多种业务, 可为终端设备 110 提供数据和/或语音等服务。例如, 数据网络 DN 120 可以是某智能工厂的私有网络, 智能工厂安装在车间的传感器可以是终端设备 110, 数据网络 DN 120 中部署了传感器的控制服务器, 控制服务器可为传感器提供服务。传感器可与控制服务器通信, 获取控制服务器的指令, 基于指令将采集的传感器数据传送给控制服务器等。又例如, 数据网络 DN 120 可以是某公司的内部办公网络, 该公司员 30 工的手机或者电脑可为终端设备 110, 员工的手机或者电脑可以访问公司内部办公网络上的信息, 数据资源等。

终端设备 110 可通过运营商网络提供的接口 (例如 N1 等) 与运营商网络建立连接, 使用运营商网络提供的数据和/或语音等服务。终端设备 110 还可通过运营商网络访问数据网络 DN 120, 使用数据网络 DN 120 上部署的运营商业, 和/或第三方提供的业务。其中, 35 上述第三方可为运营商网络和终端设备 110 之外的服务方, 可为终端设备 110 提供其他数据和/或语音等服务。其中, 上述第三方的具体表现形式, 具体可基于实际应用场景确定, 在此不做限制。

下面对运营商网络中的网络功能进行简要介绍。

(R)AN 140 可以看作是运营商网络的子网络，是运营商网络中业务节点与终端设备 110 之间的实施系统。终端设备 110 要接入运营商网络，首先是经过(R)AN 140，进而可通过 (R)AN 140 与运营商网络的业务节点连接。本申请实施例中的接入网设备 (RAN 设备)，是一种为终端设备 110 提供无线通信功能的设备，也可以称为网络设备，RAN 设备包括但不限于：5G 系统中的下一代基站节点 (next generation node base station, gNB)，长期演进 (long term evolution, LTE) 中的演进型节点 B (evolved node B, eNB)，无线网络控制器 (radio network controller, RNC)，节点 B (node B, NB)，基站控制器 (base station controller, BSC)，基站收发台 (base transceiver station, BTS)，家庭基站 (例如，home evolved nodeB，或 home node B, HNB)，基带单元 (base band unit, BBU)，传输点 (transmitting and receiving point, TRP)，发射点 (transmitting point, TP)，小基站设备 (pico)，移动交换中心，或者未来网络中的网络设备等。采用不同无线接入技术的系统中，具备接入网设备功能的设备的名称可能会有所不同。为方便描述，本申请所有实施例中，上述为终端设备 110 提供无线通信功能的装置统称为接入网设备或简称为 RAN 或 AN。应理解，本文对接入网设备的具体类型不作限定。

接入与移动性管理功能 AMF (也可以称为 AMF 网元，AMF 网络功能或 AMF 网络功能实体) 137 是由运营商网络提供的控制面网络功能，负责终端设备 110 接入运营商网络的接入控制和移动性管理，例如包括移动状态管理，分配用户临时身份标识，认证和授权用户等功能。

会话管理功能 SMF (也可以称为 SMF 网元，SMF 网络功能或 SMF 网络功能实体) 138 是由运营商网络提供的控制面网络功能，负责管理终端设备 110 的协议数据单元 (protocol data unit, PDU) 会话。PDU 会话是一个用于传输 PDU 的通道，终端设备需要通过 PDU 会话与数据网络 DN 120 互相传送 PDU。PDU 会话由 SMF 网络功能 138 负责建立，维护和删除等。SMF 网络功能 138 包括会话管理 (如会话建立，修改和释放，包含用户面功能 UPF 139 和(R)AN 140 之间的隧道维护)，UPF 网络功能 139 的选择和控制，业务和会话连续性 (service and session continuity, SSC) 模式选择，漫游等会话相关的功能。

用户面功能 UPF (也可以称为 UPF 网元，UPF 网络功能或 UPF 网络功能实体) 139 是由运营商提供的网关，是运营商网络与数据网络 DN 120 通信的网关。UPF 网络功能 139 包括数据包路由和传输，数据包检测，业务用量上报，服务质量 (quality of service, QoS) 处理，合法监听，上行数据包检测，下行数据包存储等用户面相关的功能。

统一数据管理网元 UDM (也可以称为 UDM 网元，UDM 网络功能或 UDM 网络功能实体) 134 是由运营商提供的控制面功能，负责存储运营商网络中签约用户的永久身份标识 (subscriber permanent identifier, SUPI)，签约用户的公开使用的签约标识 (generic public subscription identifier, GPSI)，信任状 (credential) 等信息。其中 SUPI 在传输过程中会先进行加密，加密后的 SUPI 被称为隐藏的用户签约标识符 (subscription concealed identifier, SUCI)。UDM 134 所存储的这些信息可用于终端设备 110 接入运营商网络的认证和授权。其中，上述运营商网络的签约用户具体可为使用运营商网络提供的业务的用户，例如使用

“中国电信”的手机芯卡的用户，或者使用“中国移动”的手机芯卡的用户等。上述签约用户的信任状可以是：该手机芯卡存储的长期密钥或者跟该手机芯卡加密相关的信息等存储的小文件，用于认证和/或授权。需要说明的是，永久标识符，信任状，安全上下文，认证数据（cookie），以及令牌等同验证/认证，授权相关的信息，在本申请实施例中，为了描述方便起见不做区分限制。

鉴权管理功能（authentication server function, AUSF）（也可以称为 AUSF 网元、AUSF 网络功能或 AUSF 网络功能实体）136 是由运营商提供的控制面功能，通常用于主认证，即终端设备 110（签约用户）与运营商网络之间的认证。AUSF 136 接收到签约用户发起的认证请求之后，可通过 UDM 网络功能 134 中存储的认证信息和/或授权信息对签约用户进行认证和/或授权，或者通过 UDM 网络功能 134 生成签约用户的认证和/或授权信息。AUSF 网络功能 136 可向签约用户反馈认证信息和/或授权信息。在认证和密钥管理（Authentication and key management for Application, AKMA）场景中，会为认证和密钥管理锚点功能

（Authentication and key management for Application (AKMA) Anchor Function, AAnF）130 生成 AKMA 锚点密钥 Kakma（该秘钥管理密钥也称为 AKMA 根密钥），并且负责为应用功能（application Function, AF）135 生成 AF 135 使用的密钥 Kaf 和 Kaf 的有效时间。

网络开放功能（Network Exposure Function, NEF）131，做为中间网元为外部应用功能（application Function, AF）135 和核心网内部的认证和密钥管理锚点功能（Authentication and key management for Application (AKMA) Anchor Function, AAnF）130 提供交互服务。

网络存储功能（Network Repository Function, NRF）132，用于进行网络功能（Network Function, NF）登记、管理，或状态检测，实现所有 NF 的自动化管理，每个 NF 启动时，必须要到 NRF 进行注册登记才能提供服务，登记信息包括 NF 类型、地址，或服务列表等。

策略控制实体（policy control function, PCF）133，PCF 133 与 AF 135 交互获得服务质量（Quality of Service, Qos）参数，或者提供 QoS 参数给 AF 135，进而实现一种可以影响应用程序数据传输的作用。

应用功能 AF 135，AF 135 与第三代合作伙伴计划（3rd Generation Partnership Project, 3GPP）核心网交互用于提供应用层服务。比如：提供关于应用层数据路由，提供接入网络能力。AF 135 可以与 NEF 131 交互，可以与 PCF 133 交互。在认证和密钥管理（Authentication and key management for Application, AKMA）场景中，AF135 需要与 AAnF 130 交互，获得 AF 根密钥（Kaf）和 Kaf 的有效时间。AF 135 的位置可以在 5G 核心网内部，也可以在 5G 核心网外部。如果 AF 在 5G 核心网内部，那么他可以直接与 PCF 133 交互。如果 AF 135 在 5G 核心网外部，则 NEF 131 作为中间节点转发 AF 135 与 PCF 133 的交互内容。比如通过 NEF 转发。

认证和密钥管理 AKMA 锚点功能 AAnF 130，AAnF 130 会跟 AUSF 136 交互获得 AKMA 根密钥（Kakma），并且负责为 AF 135 生成 AF 135 使用的密钥 Kaf 和 Kaf 的有效时间。

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

不做赘述。需要说明的是，图 1a 中仅以终端设备 110 为 UE 作出了示例性说明，图 1a 中的各个网络功能之间的接口名称也仅仅是一个示例，在具体实现中，该系统架构的接口名称还可能为其他名称，本申请实施例对此不做具体限定。

为方便说明，本申请实施例中以移动性管理网络功能为 AMF 网络功能 137 为例进行说明。它也可以是未来通信系统中的具有上述 AMF 网络功能 137 的其他网络功能。或者，本申请中的移动性管理网络功能还可以是 LTE 中的移动管理网元(Mobility Management Entity, MME)等。进一步地，将 AMF 网络功能 137 简称为 AMF，将终端设备 110 称为 UE，将即本申请实施例中后文所描述的 AMF 均可替换为移动性管理网络功能，UE 均可替换为终端设备。

本申请提供的一种密钥标识的生成方法可以应用于各类通信系统中，例如，可以是物联网(internet of things, IoT)、窄带物联网(narrow band internet of things, NB-IoT)、长期演进(long term evolution, LTE)，也可以是第五代(5G)通信系统，还可以是 LTE 与 5G 混合架构、也可以是 5G 新无线(new radio, NR)系统以及未来通信发展中出现的新的通信系统等。本申请的 5G 通信系统可以包括非独立组网(non-standalone, NSA)的 5G 通信系统、独立组网(standalone, SA)的 5G 通信系统中的至少一种。通信系统还可以是公共陆地移动网络(public land mobile network, PLMN)网络、设备到设备(device-to-device, D2D)网络、机器到机器(machine to machine, M2M)网络或者其他网络。

此外，本申请实施例还可以适用于面向未来的其他通信技术，例如 6G 等。本申请描述的网络架构以及业务场景是为了更加清楚的说明本申请的技术方案，并不构成对本申请提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请涉及的各个网络功能可能发生变更，本申请提供的技术方案对于类似的技术问题，同样适用。

图 2 为本申请实施例中通信装置的硬件结构示意图。该通信装置可以是本申请实施例中网络设备或终端设备的一种可能的实现方式。如图 2 所示，通信装置至少包括处理器 204，存储器 203，和收发器 202，存储器 203 进一步用于存储指令 2031 和数据 2032。可选的，该通信装置还可以包括天线 206，I/O(输入/输出, Input/Output)接口 210 和总线 212。收发器 202 进一步包括发射器 2021 和接收器 2022。此外，处理器 204，收发器 202，存储器 203 和 I/O 接口 210 通过总线 212 彼此通信连接，天线 206 与收发器 202 相连。

处理器 204 可以是通用处理器，例如但不限于，中央处理器(Central Processing Unit, CPU)，也可以是专用处理器，例如但不限于，数字信号处理器(Digital Signal Processor, DSP)，应用专用集成电路(Application Specific Integrated Circuit, ASIC)和现场可编程门阵列(Field Programmable Gate Array, FPGA)等。该处理器 204 还可以是神经网络处理单元(neural processing unit, NPU)。此外，处理器 204 还可以是多个处理器的组合。特别的，在本申请实施例提供的技术方案中，处理器 204 可以用于执行，后续方法实施例中密钥标识的生成方法的相关步骤。处理器 204 可以是专门设计用于执行上述步骤和/或操作的处理器，也可以是通过读取并执行存储器 203 中存储的指令 2031 来执行上述步骤和/或操作的处理器，处理器 204 在执行上述步骤和/或操作的过程中可能需要用到数据 2032。

收发器 202 包括发射器 201 和接收器 202, 在一种可选的实现方式中, 发射器 201 用于通过天线 206 发送信号。接收器 202 用于通过天线 206 之中的至少一根天线接收信号。特别的, 在本申请实施例提供的技术方案中, 发射器 201 具体可以用于通过天线 206 之中的至少一根天线执行, 例如, 后续方法实施例中密钥标识的生成方法应用于网络设备或终端设备时, 网络设备或终端设备中接收模块或发送模块所执行的操作。

在本申请实施例中, 收发器 202 用于支持通信装置执行前述的接收功能和发送功能。将具有处理功能的处理器视为处理器 204。接收器 202 也可以称为输入口、接收电路等, 发射器 201 可以称为发射器或者发射电路等。

处理器 204 可用于执行该存储器 203 存储的指令, 以控制收发器 202 接收消息和/或发送消息, 完成本申请方法实施例中通信装置的功能。作为一种实现方式, 收发器 202 的功能可以考虑通过收发电路或者收发的专用芯片实现。本申请实施例中, 收发器 202 接收消息可以理解为收发器 202 输入消息, 收发器 202 发送消息可以理解为收发器 202 输出消息。

存储器 203 可以是各种类型的存储介质, 例如随机存取存储器(Random Access Memory, RAM), 只读存储器(Read Only Memory, ROM), 非易失性 RAM(Non-Volatile RAM, NVRAM), 可编程 ROM(Programmable ROM, PROM), 可擦除 PROM(Erasable PROM, EPROM), 电可擦除 PROM(Electrically Erasable PROM, EEPROM), 闪存, 光存储器和寄存器等。存储器 203 具体用于存储指令 2031 和数据 2032, 处理器 204 可以通过读取并执行存储器 203 中存储的指令 2031, 来执行本申请方法实施例中所述的步骤和/或操作, 在执行本申请方法实施例中操作和/或步骤的过程中可能需要用到数据 2032。

可选的, 该通信装置还可以包括 I/O 接口 210, 该 I/O 接口 210 用于接收来自外围设备的指令和/或数据, 以及向外围设备输出指令和/或数据。

下面, 介绍本申请实施例涉及的一些背景技术。

(1)、AKMA。

为了便于理解, 请参阅图 3, 图 3 为 UE 通过转发的接入流程示意图。以图 3 为例说明 AKMA 流程, 具体的:

301、UE 与核心网之间进行主鉴权流程。

步骤 301 中, UE 与核心网之间进行主鉴权 (Primary authentication) 流程。该主鉴权流程需要使用鉴权向量(authentication vector, AV), 该鉴权向量用于主鉴权流程中传递主鉴权流程的验证参数。具体的, 通过步骤 302, AUSF 获取该鉴权向量。

本申请实施例中, 该主鉴权流程也称为鉴权流程, 此处不作限制。

302、AUSF 向 UDM 发送鉴权向量获取请求消息。

步骤 302 中, AUSF 向 UDM 发送鉴权向量获取请求消息, 该鉴权向量获取请求消息例如 “Numd_UEAuthentication Get Request”。该鉴权向量获取请求消息用于向 UDM 请求鉴权向量。该鉴权向量获取请求消息中携带 SUPI 或 SUCI。具体的, 当 AMF 向 AUSF 发送的消息中携带 SUPI 时, 该鉴权向量获取请求消息中携带 SUPI; 当 AMF 向 AUSF 发送的消息中携带 SUCI 时, 该鉴权向量获取请求消息中携带 SUCI。

SUCI 可以理解为是 SUPI 的一种加密形式。SUCI 的具体生成方法可以参考 3GPP 标

准 TS 33.501。概括地说，SUPI 中除移动国家代码（mobile country code, MCC）之外的部分可以由全球用户识别卡（universal subscriber identity module, USIM）或移动设备（mobile equipment, ME）进行加密计算得到 SUCI 中的加密部分。SUCI 除了加密部分，还包括 RID, MCC, MNC 等内容。

5 303、AUSF 接收 UDM 发送的鉴权向量获取响应消息。

步骤 303 中，UDM 收到步骤 302 的鉴权向量获取请求消息后，UDM 确定对应的鉴权向量。UDM 向 AUSF 发送鉴权向量获取响应消息，该鉴权向量获取响应消息中携带鉴权向量。该鉴权向量获取响应消息例如：“Num_UEAuthentication_Get Response”。

10 可选的，UDM 基于 SUPI 对应的用户签约数据判断该主鉴权流程对应的 UE 是否支持 AKMA 业务。当该 UE 支持 AKMA 业务，则该鉴权向量获取响应消息中携带 AKMA 业务指示信息，该 AKMA 业务指示信息可以是“AKMA Indication”或“AKMA ID”，本申请实施例中不作限定。AKMA 业务指示信息用于指示 AUSF 需要为这个 UE 生成 AKMA 锚点密钥 Kakma。也可以理解为：该 AKMA 业务指示信息用于指示该 UE 支持 AKMA 业务。当该 UE 不支持 AKMA 业务，则该鉴权向量获取请求消息中不携带 AKMA 业务指示信息。

15 需要说明的是：AKMA indication 与 AKMA ID 可以采用相同的信元，也可以采用不同信元，此处不作限制。

304a、UE 基于 AUSF 根密钥生成 AKMA 锚点密钥 Kakma。

20 步骤 304a 中，当 UE 的主鉴权流程成功完成后，UE 基于与 AUSF 使用的相同的根密钥（Kausf）生成 AKMA 锚点密钥（Kakma）。可选的，进一步地，UE 要发起 AKMA 业务前，UE 基于与 AUSF 使用的相同的根密钥（Kausf）生成 AKMA 锚点密钥（Kakma）。

304b、UE 生成认证和密钥管理-密钥临时身份标识 A-KID。

25 步骤 304b 中，当 UE 的主鉴权流程成功完成后，UE 要发起 AKMA 业务前，UE 基于与 AUSF 使用的相同的根密钥（Kausf）生成认证和密钥管理-密钥临时身份标识（AKMA-Key Identifier, A-KID）。A-KID 用于标识 UE 的 AKMA 锚点密钥 Kakma。可选的，进一步地，UE 要发起 AKMA 业务前，UE 基于与 AUSF 使用的相同的根密钥（Kausf）生成 A-KID。具体地，UE 基于基于与 AUSF 使用的相同的根密钥（Kausf）生成 A-KID 中的密钥管理-密钥临时身份标识（AKMA Temporary UE Identifier, A-TID）部分。

30 具体的，基于 RID 生成 A-KID。A-KID 格式为“username@exmaple”。“username”部分包括路由标识，和认证和密钥管理-密钥临时身份标识（AKMA Temporary UE Identifier, A-TID）。“example”部分包括家乡网络标识，例如：移动国家代码（mobile country code, MCC）和移动网络代码（mobile network code, MNC）。A-TID 是基于 Kausf 生成的一个临时标识。

需要说明的是，步骤 304a 与步骤 304b 执行顺序不作限制。

305a、AUSF 基于 AUSF 根密钥生成 AKMA 锚点密钥 Kakma。

35 步骤 305a 与前述步骤 304a 类似，不作赘述。与 304a 不同的地方在于，AUSF 在收到所述鉴权向量获取响应消息后，如果消息中携带有 AKMA 业务指示信息，则 AUSF 使用 AUSF 获取到的 Kausf 生成 Kakma 和 A-KID。如果所述鉴权向量获取响应消息没有携带有

AKMA 业务指示信息，则 AUSF 可以不生成 Kakma 和 A-KID。

305b、AUSF 生成认证和密钥管理-密钥临时身份标识 A-KID。

步骤 305b 中，当步骤 303 中，UDM 发送的鉴权向量获取响应消息中携带 AKMA 标识信息时，AUSF 基于该 AKMA 标识信息确定需要生成 A-KID。步骤 302 中，AMF 向 AUSF 提供 SUCI 时，步骤 305b 中，AUSF 基于该 SUCI 中的 RID 生成 A-KID。

306、AUSF 向 AAnF 发送 AKMA 锚密钥注册请求消息。

步骤 306 中，AUSF 选择一个 AAnF 后，AUSF 向该 AAnF 发送 AKMA 锚密钥注册请求消息。AKMA 锚密钥注册请求消息例如：“Naanf_AKMA_AnchorKey_Register Request”。具体的，该 AKMA 锚密钥注册请求消息中携带 SUPI、A-KID 和 Kakma。

307、AUSF 接收 AAnF 发送的 AKMA 锚密钥注册响应消息。

步骤 307 中，AAnF 基于步骤 306 的 AKMA 锚密钥注册请求消息，向 AUSF 发送 AKMA 锚密钥注册响应消息。该 AKMA 锚密钥注册响应消息例如：

“Naanf_AKMA_AnchorKey_Register Response”。

308、AUSF 删除 Kakma 和 A-KID。

步骤 308 中，当 AUSF 接收来自 AAnF 发送的 AKMA 锚密钥注册响应消息后，AUSF 删除 Kakma 和 A-KID。

(2)、路由标识 RID。

SUCI 中包括 RID。当前标准规定，RID 用于 AMF 查找 AUSF，AUSF 查找 UDM。在 AKMA 流程中，RID 用于生成 A-KID。RID 还用于选择 AAnF。

在 5G 全球用户识别卡 (Universal Subscriber Identity Module, USIM) 中，RID 存储在 USIM 中。当 5G UE 使用 5G USIM 时，5G UE 从该 5G USIM 中获取需要使用的 RID。该 RID 的值可以是一个非缺省值，也可以是一个缺省值。

而在 4G USIM 中不存在 RID，因此，如果一个 5G UE 使用了 4G USIM，那么 SUCI 中的 RID 会被填充为缺省值。

在 AMF 中，关于 UE 的上下文中包括 RID。可以理解为，AMF 从 SUCI 中获取 RID 后，将该 RID 存储在 AMF 中。在图 3 所示的 AKMA 流程中，当步骤 302 中，AMF 向 AUSF 提供的是 SUPI 时，该 SUPI 中不包括 RID。而当前标准规定，AUSF 不存储 UE 的 RID。因此，当步骤 302 中，AMF 向 AUSF 提供的是 SUPI 的前提下，在步骤 305b 中 AUSF 无法生成 A-KID (RID 是生成 A-KID 的必要参数)。因此造成 AKMA 流程的失败。

示例性的，当 UE 在注册请求消息中向 AMF 发送 5G 全局唯一的临时 UE 标识 (5G Globally Unique Temporary UE Identity, 5G-GUTI) 时，AMF 可以基于本地策略决定是否对 UE 进行鉴权。当 AMF 决定对 UE 进行鉴权，即发起主鉴权流程时，AMF 向 AUSF 发送的用于触发对 UE 鉴权的鉴权请求消息中携带 SUPI (步骤 302)。此时，AUSF 无法获取 RID。进而，AUSF 无法生成 A-KID。对 UE 鉴权的请求消息比如为

“Nausf_UEAuthentication_Authenticate Request” 消息。

基于此，本申请实施例提出一种密钥标识的生成方法，以确保 AUSF 可以获取 RID，进而保证 AUSF 生成 A-KID，进而确保 UE 的 AKMA 业务顺利执行。下面在介绍具体实施

例前进行简要描述, 根据 RID 来源的不同, 本申请实施例可以细分为:

1、AUSF 保存 RID, 该 RID 来自 AMF 或者 UDM。具体的, 请参阅图 4 所示的实施例。

2、AUSF 从核心网网元获取 RID。其中, 该核心网网元包括 AMF 或 UDM。

5 2.1、具体的, AUSF 从 AMF 获取 RID。请参阅图 5 所示的实施例和/或图 6 所示的实施例。

2.2、具体的, AUSF 从 UDM 获取 RID。请参阅图 7 所示的实施例和/或图 8 所示的实施例。

需要说明的是, 本申请各个实施例中, 为了便于区分, 将 SUCI 中携带的 RID 称为 RID#1, 来自 UDM 的 RID 称为 RID#2, 来自 AMF 的 RID 称为 RID#3, AUSF 中存储的 RID 称为 RID#4。可以理解的是, RID#1、RID#2、RID#3 和 RID#4 可能是相同的取值, 因此, 后续实施例中可能会出现标号混用。

首先介绍 AUSF 保存 RID 的方案, 请参阅图 4, 图 4 为本申请实施例提出的一种密钥标识的生成方法的实施例示意图。本申请实施例提出的一种密钥标识的生成方法, 包括:

15 401、AUSF 接收 AMF 发送的鉴权请求消息#1, 该鉴权请求消息#1 中携带 SUCI。

AUSF 接收 AMF 发送的鉴权请求消息#1, 该鉴权请求消息#1 中携带 SUCI。具体的, 该鉴权请求消息#1 为 “Nausf_UEAuthentication_Authenticate Request”。

该 SUCI 中携带的 RID 为 RID#1。

402、AUSF 向 UDM 发送鉴权向量获取请求消息#1, 该鉴权向量获取请求消息#1 中携带 SUCI。

AUSF 收到 AMF 发送的鉴权请求消息#1 后, AUSF 向 UDM 发送鉴权向量获取请求消息#1, 该鉴权向量获取请求消息#1 中携带 SUCI。

示例性的, 该鉴权向量获取请求消息#1 可以是:

“Nudm_UE_Authentication_Get_Request”。

25 403、AUSF 存储 SUCI, 或存储 SUCI 中的 RID#1。

步骤 401 后, AUSF 可以存储该 SUCI 至 AUSF 本地, AUSF 也可以存储 SUCI 中的 RID#1 至 AUSF 本地, 此处不作限制。

步骤 403 为可选步骤。

步骤 403 可以发生在步骤 402 之前, 即 AUSF 收到携带有 SUCI 的鉴权请求消息#1 后, AUSF 先存储 SUCI, 或存储 SUCI 中的 RID#1, 再执行步骤 402。

另一种理解是, 该步骤为暂时存储, 暂时存储是为了当 AUSF 收到鉴权向量响应消息后, 如果 AUSF 确定该 UE 支持 AKMA 业务, 则可以使用 SUCI 中的 RID#1 生成 A-KID#1。如果 AUSF 确定该 UE 不支持 AKMA 业务 (即没有收到 AKMA indication), 则该 AUSF 可以在后续流程中删除 SUCI, 或删除 RID#4。

35 AUSF 获取 SUCI 中的 RID#1 后, 将该 RID#1 存储至本地, 此时本地的该 RID 称为 RID#4。

404、AUSF 接收 UDM 发送的鉴权向量获取响应消息#1。

可选的, 该鉴权向量获取响应消息#1 中携带 RID#2。

步骤 402 后, UDM 接收 AUSF 发送的鉴权向量获取请求消息#1 后。当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#1 后, AUSF 对该 UE(与该鉴权请求消息#1 对应的 UE)进行鉴权操作。鉴权操作方式为进行主鉴权流程, 主鉴权流程可以参考标准 TS 33.501 中的章节 6 中的相关描述。

5 该鉴权向量获取响应消息#1 中还携带鉴权向量(authentication vector, AV)。

 可选的, 该鉴权向量获取响应消息#1 中还携带认证和密钥管理指示信息 AKMA indication。

 示例性的, 该鉴权向量获取响应消息#1 为“Nudm_UE_Authentication_Get_Response”。当鉴权成功, 则 AUSF 向 AMF 发送鉴权请求响应(authentication success)。

10 可选的, 该鉴权向量获取响应消息#1 中还可以携带 RID#1, 此时该鉴权向量获取响应消息#1 中还携带 AKMA INDICATION 和 AV。进一步地, UDM 在确定 UE 支持 AKMA 业务后, 确定 RID#2, 并将该 RID#2 携带在该鉴权向量获取响应消息#1 中。UDM 再次发送 RID#2 是为了确保 AUSF 处有可以使用的 RID。比如, 如果 AUSF 没有执行步骤 403, 那么 AUSF 就只能通过步骤 404 获得 RID#2, 并使用 RID#2 生成 A-KID#1。

15 405、当 AUSF 对该 UE 鉴权成功后, AUSF 向 AMF 发送第一鉴权请求响应。

 示例性的, 第一鉴权请求响应为“Nausf_UEAuthentication_Authenticate Response”消息, 消息携带可拓展认证协议-成功(extensible authentication protocol-success, EAP-success)消息或者携带告知 AMF 是否对 UE 鉴权成功的指示信息。

 406、AUSF 基于 RID 生成 A-KID#1。

20 AUSF 接收来自 UDM 的鉴权向量获取响应消息#1 后, AUSF 基于 AKMA 业务指示信息判断该 UE 支持 AKMA 业务, 则 AUSF 生成认证和密钥管理-密钥临时身份标识 A-KID#1。

 在一种可选的实现方式中, 当步骤 403 执行时, AUSF 基于本地存储的 SUCI 中的 RID#1, 或者, AUSF 基于本地存储的 RID#4 生成 A-KID#1。也可以理解为, AUSF 基于步骤 401 中鉴权请求消息#1 携带的 SUCI 中的 RID#1 生成 A-KID#1。

25 在另一种可选的实现方式中, 当步骤 403 不执行时, 当步骤 404 可选的发送 RID#2 方法执行时, AUSF 基于 UDM 发送的 RID#2 生成 A-KID#1。

 如果 AUSF 在步骤 404 中没有收到 AKMA indication, 并且如果步骤 403 执行时, AUSF 删除本地存储的 SUCI 或 SUCI 中的 RID#1。

 当 AUSF 生成 A-KID#1 后, AUSF 可以向 AAnF 发送 A-KID#1、SUPI 和 Kakma。具体的, 可以通过“Naanf_AnchorKey_Register Request”向 AAnF 发送。AAnF 接收该消息后, 向 AUSF 回复“Naanf_AKMA_Register Response”。

 进一步的, AUSF 基于该 SUCI, 生成 Kakma。为了区分, 这里生成的 Kakma 称为 Kakma-1。

 407、AUSF 存储 RID。

35 进一步地, AUSF 判断该 UE 支持 AKMA 业务后(即收到 AKMA indication 后), 确定存储 RID#1。具体的, AUSF 接收该 UE 的 AKMA indication 后, 表明 AUSF 需要生成 Kakma 和 A-KID, 则 AUSF 确定该 UE 支持 AKMA 业务。

 步骤 407 中 AUSF 存储的 RID, 根据 RID 来源的不同, 该 RID 可以是 RID#1, 也可以

是 RID#2。

需要说明的是，如果步骤 403 执行，则 AUSF 判断该 UE 支持 AKMA 业务后，继续存储 SUCI，或者存储 SUCI 中的 RID#1。

需要说明的是，如果步骤 403 没有执行，步骤 404 可选的发送 RID#2 方法执行时，则
5 AUSF 判断该 UE 支持 AKMA 业务后，AUSF 存储 RID#2。

步骤 407 中，AUSF 存储 RID#1 相关的参数存在多种可选的实现方式，下面分别进行说明。需要说明的是，RID#1 相关的参数包括但不限于：RID#1、SUCI、和/或 A-KID#1。

方案一：AUSF 存储 SUCI 中的 RID#1 和，RID#1 与 SUPI 的关联关系。示例性地，存储 RID#1、SUPI。存储 RID#1 与 SUPI 的关联关系是为了当 AUSF 收到 SUPI 的时候，基
10 于 SUPI 确定 RID#1。

方案二：AUSF 存储 SUCI，即 AUSF 不单独存储 RID#1。进一步地，AUSF 存储 SUCI 和，SUCI 与 SUPI 的关联关系。

方案三：AUSF 存储 RID#1，SUCI，和 RID#1、SUCI 和 SUPI 三者的关联关系。

需要说明的是，步骤 407 与步骤 406 的执行顺序，此处不作限定。具体的，AUSF 可
15 以首先生成 A-KID#1，其次再存储 RID#1 或存储 SUCI。AUSF 也可以存储 RID#1 或存储 SUCI 后，再生成 A-KID#1，此处不作限制。

可选的，若 AUSF 在生成 A-KID#1 后删除了 RID#1 和/或 SUCI，则 AUSF 存储 A-KID#1。那么步骤 410 中，AUSF 基于该 A-KID#1 生成 A-KID#2。具体地，AUSF 基于 A-KID#1 中的 RID#1 生成 A-KID#2 进一步地，AUSF 存储 A-KID#1 与 SUPI 的关联关系。可选的，当
20 RID#1 的值为缺省值时，步骤 407 中 AUSF 可以不存储 RID#1。则步骤 410 中，AUSF 使用缺省的 RID#1 值生成 A-KID#2。

需要说明的是，如果步骤 403 执行，则步骤 407 不需要重复存储。可以理解为，步骤 407 是步骤 403 的一个延续，即如果发生了步骤 403，那么 AUSF 只需要再判断 UE 支持 AKMA 业务后，执行步骤 407 时只需要进一步与 SUPI 的关联关系。

需要说明的是，如果步骤 403 没有执行，步骤 404 可选的发送 RID#2 方法执行时，则
25 步骤 407 不需要重复存储。可以理解为，步骤 407 是步骤 404 的一个延续，即如果发生了步骤 404 可选的发送 RID#1 方法执行时，并且在 AUSF 判断 UE 支持 AKMA 业务后，那么步骤 407 只需要进一步存储 RID#1 与 SUPI 的关联关系。

408、AUSF 删除 SUCI。

步骤 408 为可选步骤。具体的，步骤 403 中 AUSF 存储 SUCI 后，当 AUSF 还存储 RID#4
30 和/或 A-KID#1 时，AUSF 可以删除 SUCI。

AUSF 保存多个 RID#1 相关的参数（例如 RID#1、SUCI 和 A-KID#1）时，AUSF 可以仅保存其中一个参数，其他冗余的参数则可以考虑删除。比如本步骤 408 中提及的 SUCI，以及前序步骤提及的 A-KID#1，可以理解为是相对于 RID#1 冗余的参数。以便后续在 AUSF
35 无法获得 RID#1 的情况下再次生成新的 A-KID。

409、AUSF 接收 AMF 发送的鉴权请求消息#2。

AUSF 接收 AMF 发送的鉴权请求消息#2，该鉴权请求消息#2 用于触发对 UE 的鉴权操

作。

该鉴权请求消息#2 可以是“Nausf_UEAuthentication_Authenticate Request”。当该鉴权请求消息#2 中携带的是 SUPI 时，进入步骤 410。

5 可选的，当该鉴权请求消息#2 中携带的是 SUCI，则后续方法与步骤 402-408 类似，此处不作赘述。

在另一种可选的实现方式中，当该鉴权请求消息#2 中携带的是 SUCI，后续执行步骤 410。

当 AUSF 接收鉴权请求消息#2 后，AUSF 可以向 UDM 发送鉴权向量获取请求消息#2 “Nudm_UE_Authentication_Get_Request”，该鉴权向量获取请求消息#2 中携带鉴权请求消息#2 中的 SUPI。UDM 基于 SUPI 确定该 UE 支持 AKMA 业务时，UDM 回复鉴权向量获取响应消息#2 “Nudm_UE_Authentication_Get_Response”中携带 AKMA 业务指示信息（例如 AKMA indication）。

步骤 409 后，当 AUSF 对该 UE 鉴权成功后，AUSF 向 AMF 发送第二鉴权请求响应。该第二鉴权请求响应例如“Nausf_UEAuthentication_Authenticate Response”。

15 410、当鉴权请求消息#2 中携带 SUPI 时，AUSF 生成 A-KID#2。

AUSF 基于该 SUPI，确定 Kausf，并使用 Kausf 生成 Kakma。为了区分，这里的 Kausf 称为 Kausf-2，这里生成的 Kakma 称为 Kakma-2。

AUSF 基于鉴权请求消息#2 中携带的 SUPI，确定 RID 相关的参数。AUSF 再基于 RID 相关的参数确定 RID，AUSF 基于 RID 生成 A-KID#2。下面分别描述各种实现方式：

20 在一种实现方式中，当鉴权请求消息#2 中携带 SUPI 时，AUSF 基于 RID#4 生成 A-KID#2。具体的，该 RID#4 来自 AUSF 本地。具体地，AUSF 基于 SUPI 确定与 SUPI 关联的 RID#4 再基于 RID#4 生成 A-KID#2。

在另一种实现方式中，当鉴权请求消息#2 中携带 SUPI 时，AUSF 基于 SUCI 中的 RID#4 生成 A-KID#2。具体的，该 SUCI 来自 AUSF 本地。具体地，AUSF 基于 SUPI 确定与 SUPI 关联的 SUCI，再基于 SUCI 中的 RID#1 生成 A-KID#2。

在另一种实现方式中，当鉴权请求消息#2 中携带 SUPI 时，AUSF 基于 A-KID#1 中的 RID#4 生成 A-KID#2。具体的，该 A-KID#1 来自 AUSF 本地。具体地，AUSF 基于 SUPI 确定与 SUPI 关联的 A-KID#1，再基于 A-KID#1 中的 RID#4 生成 A-KID#2。

30 在另一种实现方式中，当鉴权请求消息#2 中携带 SUPI 时，如果鉴权向量获取响应消息#2 中携带了 RID#2，则 AUSF 基于收到的 RID#2 生成 A-KID#2。

在另一种实现方式中，当鉴权请求消息#2 中携带 SUPI 时，并且 AUSF 本地没有保存有任何 RID#4 相关的参数（比如，SUCI，A-KID，和/或 RID#4），同时 AUSF 没有从 UDM 收到 RID#2 相关的参数，那么 AUSF 使用 RID 的缺省值生成 A-KID#2。可选的，当 AUSF 生成 A-KID#2 后，AUSF 可以向 AAnF 发送 A-KID#2、SUPI 和 Kakma-2。具体的，可以通过“Naanf_AnchorKey_Register Request”向 AAnF 发送。AAnF 接收该消息后，向 AUSF 回复“Naanf_AKMA_Register Response”。

411、AUSF 删除 Kakma-2。

412、AUSF 继续保存 RID#4 相关的参数。

在一种实现方法中, AUSF 继续保存 RID#4 或者 AUSF 继续保存 SUCI, 或者 A-KID#1。并且删除其他冗余参数。比如, 当 AUSF 删除 A-KID#2 后, 可以继续保存 RID#4。

在另一种实现方法中, 如果 AUSF 收到了 SUCI#2(该 SUPI#2 与步骤 401 中接收的 SUCI 不一致), 则 AUSF 保存 RID#3, 其中 SUPI#2 中的 RID 称为 RID#5, 或者 AUSF 保存 SUCI#2。
5 可以理解为, AUSF 保存 RID#5 相关的参数(例如 SUCI#2 和/或 RID#5), 不需要继续保存 RID#4 相关的参数。具体操作可以是直接覆盖, 或者先删除再存储, 或者先存储再删除。本申请不做具体限制。

在另一种实现方法中, 如果 AUSF 之前保存了 A-KID#1。在生成 A-KID#2 后, 则 AUSF
10 保存 A-KID#2。可以理解为, AUSF 保存 A-KID#2, 不需要继续保存 A-KID#1。具体操作可以是直接覆盖, 或者先删除再存储, 或者先存储再删除。本申请不做具体限制。

本申请实施例中, 在 AKMA 流程中, AUSF 保存 RID 相关的参数(例如: SUCI、A-KID 和/或 RID)。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时, AUSF 可以使用该 RID 相关的参数生成新的 A-KID, 保证 AKMA 流程的成功执行。

15 在前述实施例的基础上, 请参阅图 5, 图 5 为本申请实施例中又一种密钥标识的生成方法的实施例示意图。本申请实施例提出的一种密钥标识的生成方法, 包括:

501、AUSF 接收 AMF 发送的鉴权请求消息#1, 该鉴权请求消息#1 中携带 SUCI。

步骤 501 与前述步骤 401 类似, 此处不作赘述。

502、AUSF 生成 A-KID#1。

20 在一种可能的实现方式中, AUSF 接收鉴权请求消息#1 后, AUSF 基于该鉴权请求消息#1 中的 SUCI 中的 RID#1, 生成 A-KID#1。在 AUSF 生成 A-KID#1 前, AUSF 接收鉴权请求消息#1 后, AUSF 可以向 UDM 发送鉴权向量获取请求消息#1, 该鉴权向量获取请求消息#1 携带该 SUCI。该鉴权向量获取请求消息可以是:

“Nudm_UE_Authentication_Get_Request”。UDM 接收 AUSF 发送的鉴权向量获取请求消息
25 #1 后。UDM 向 AUSF 发送鉴权向量获取响应消息#1, 该鉴权向量获取响应消息#1 中携带鉴权向量(authentication vector, AV)。

可选的, 在 UDM 确定 SUCI 对应的 UE 支持 AKMA 业务的情况下, 该鉴权向量获取响应消息#1 中还携带认证和密钥管理指示信息 AKMA indication。可选的, 该鉴权向量获取响应消息#1 中携带 RID#1。

30 在另一种可能的实现方式中, AUSF 接收鉴权向量获取响应消息#1 后, AUSF 基于该鉴权向量获取响应消息#1 中的 RID#1, 生成 A-KID#1。

比如, 在 UDM 确定 SUCI 对应的 UE 支持 AKMA 业务的情况下, 才携带 RID#2。示例性的, 该鉴权向量获取响应消息#1 为“Nudm_UE_Authentication_Get_Response”。当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#1 后, AUSF 对该 UE(与该鉴权请求消息#1 对
35 应的 UE)进行鉴权操作。当鉴权成功, 则 AUSF 向 AMF 发送第一鉴权请求响应。

可选的, 该第一鉴权请求响应包括第一指示信息(indication), 该第一指示信息用于指示 UE 支持 AKMA 业务。需要说明的是, 该第一指示信息与 AKMA 业务指示信息可以采

用相同的信元，也可以采用不同的信元，此处不作限制。

进一步的，当 AUSF 收到 AKMA indication 后，AUSF 生成 Kakma。为了区分，这里生成的 Kakma 称为 Kakma-1。

当 AUSF 生成 A-KID#1 后，AUSF 可以向 AAnF 发送 A-KID#1、SUPI 和 Kakma。具体的，可以通过“Naanf_AnchorKey_Register Request”向 AAnF 发送。AAnF 接收该消息后，向 AUSF 回复“Naanf_AKMA_Register Response”。AUSF 收到“Naanf_AKMA_Register Response”后，产生 Kakma-1 和 A-KID#1。

AUSF 可以在收到步骤 501 消息后，暂时存储该 SUCI 或 SUCI 中的 RID#1，等到确定有 AKMA 业务指示信息后，并且生成 Kakma-1 和 A-KID#1 后，删除该 SUCI 或 SUCI 中的 RID#1。

503、AUSF 接收 AMF 发送的鉴权请求消息#2。

AUSF 接收 AMF 发送的鉴权请求消息#2。该鉴权请求消息#2 中携带 SUPI，则进入步骤 504。

可选的，AUSF 接收鉴权请求消息#2 后，AUSF 可以向 UDM 发送鉴权向量获取请求消息#2，该鉴权向量获取请求消息#2 携带该 SUPI。该鉴权向量获取请求消息#2 可以是：

“Nudm_UE_Authentication_Get_Request”。UDM 接收 AUSF 发送的鉴权向量获取请求消息#2 后。UDM 向 AUSF 发送鉴权向量获取响应消息#2，该鉴权向量获取响应消息#2 中携带鉴权向量(authentication vector, AV)。可选的，在 UDM 确定 SUPI 对应的 UE 支持 AKMA 业务的情况下，该鉴权向量获取响应消息#2 中还携带 AKMA indication。示例性的，该鉴权向量获取响应消息#2 为“Nudm_UE_Authentication_Get_Response”。当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#2 后，AUSF 确定该 UE 支持 AKMA 业务。AUSF 确定需要生成该 UE 的 A-KID。AUSF 对该 UE（与该鉴权请求消息#2 对应的 UE）进行鉴权操作。当鉴权成功，则 AUSF 向 AMF 发送鉴权请求响应（authentication success）。

可选的，该鉴权请求消息#2 中可以携带 RID#3。该步骤可选的，是因为现有技术中 RID 本身就是可选的通过鉴权请求消息从 AMF 传递给 AUSF。但是现有技术中传递 RID 的作用是方便 AUSF 通过 RID 快速查找到可以为 UE 服务的 UDM。

在一种可能的实现方式中，若鉴权请求消息#2 中携带的是 SUPI，则该鉴权请求消息#2 中还要携带 RID#3。这样做是为了确保 AUSF 有可以使用的 RID，以避免当 AUSF 确定该 SUPI 对应的 UE 支持 AKMA 业务的时候，没有可用的 RID 生成 A-KID。

504、AUSF 向 AMF 发送第一请求，第一请求中携带 SUPI。

AUSF 接收 AMF 发送的鉴权请求消息#2 后，AUSF 检测鉴权请求消息#2 中是否携带有 RID。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。

如果鉴权请求消息#2 没有 RID 相关的参数，则 AUSF 向 AMF 发送第一请求，该第一请求用于请求 RID。该第一请求中携带 SUPI，该 SUPI 为鉴权请求消息#2 中携带的 SUPI。进一步地，如果鉴权请求消息#2 和 AUSF 本地均没有 RID 相关的参数，则 AUSF 向 AMF 发送第一请求，该第一请求用于请求 RID。

可选的，第一请求中携带一个需要 RID 的指示信息。

具体地，AUSF 在接收 UDM 发送的鉴权向量获取响应消息#2 后，AUSF 确定该 UE 支持 AKMA 业务后，AUSF 没有在鉴权请求消息#2 中收到 RID#4，和/或 AUSF 本地没有保存有 RID#4，则 AUSF 向 AMF 发送该第一请求。

5 步骤 504 中，AUSF 接收 AMF 发送的鉴权请求消息#2 后，存在两种可选的实现方案，下面分别进行描述：

方案一：AUSF 每次接收鉴权请求消息#2 后，检测该鉴权请求消息#2 中是否携带 RID。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。当检测结果为鉴权请求消息#2 中没有 RID#3（或者鉴权请求消息#2 没有 RID，且，AUSF 本地没有 RID#4 相关的参数），则 AUSF 向 AMF 发送第一请求。步骤 506 中，AUSF 不保存来自 AMF 的第一响应中携带的 RID#3。即 AUSF 每次接收鉴权请求消息#2 后，都会检测该鉴权请求消息#2 中是否携带 RID，如果不携带，则 AUSF 向 AMF 发送第一请求。

15 方案二：AUSF 接收鉴权请求消息#2 后，检测该鉴权请求消息#2 中是否携带 RID。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。当检测结果为鉴权请求消息#2 中没有 RID#3（或者鉴权请求消息#2 没有 RID，且 AUSF 本地没有 RID#4 相关的参数），则 AUSF 向 AMF 发送第一请求。步骤 506 中，AUSF 保存来自 AMF 的第一响应中携带的 RID#3。即 AUSF 第一次接收到不携带 RID 的鉴权请求消息#2 后，AUSF 向 AMF 发送第一请求。步骤 506 中 AUSF 会保存 AMF 基于该第一请求返回的 RID#3。后续步骤中当 AUSF 再次接收到不携带 RID 的鉴权请求消息#2 时，AUSF 可以基于本地保存的 RID#4（步骤 506 中保存的）进行后续动作。示例性的，第一请求为“Nudm_UE_AKMA_Get_Request”。

AUSF 接收 AMF 发送的鉴权请求消息#2 后，AUSF 判断鉴权请求消息#2 中是否携带有 RID。如果携带有 RID，则执行步骤 507。

25 AUSF 接收 AMF 发送的鉴权请求消息#2 后，AUSF 确定本地保存有 RID 相关的参数的情况下，则执行步骤 507。

505、AMF 基于第一请求中携带的 SUPI，确定 RID#3。

AMF 接收第一请求后，基于该第一请求中携带的 SUPI，确定该 SUPI 对应的 RID#3。

30 在另一种实现方式中，AMF 接收第一请求后，首先，基于第一请求中携带的 SUPI，确定该 SUPI 对应的 RID#3。其次，AMF 基于该 RID#3 构造 SUCI，为了便于区分，将基于 RID#2 构造的 SUCI 称为 SUCI#3。具体地，AMF 使用归属网络（HPLMN）的公钥和 UE 的 SUPI 按照与 UE 相同的方式生成 SUCI#3。此时，要求 AMF 本地存储或者可以获得 HPLMN 的公钥、公钥标识符等生成 SUCI 的必要参数。

506、AMF 向 AUSF 发送第一响应，第一响应中携带 RID#3。

35 AMF 向 AUSF 发送第一响应，该第一响应中携带 RID#3。

在另一种实现方式中，AMF 向 AUSF 发送的第一响应中携带步骤 505 中构造的 SUCI#3。此时，该第一响应中不携带 RID。

示例性的，第一响应为“Nudm_UE_AKMA_Get_Response”。

507、AUSF 基于该 RID#3 生成 A-KID#2。

进一步的，AUSF 生成 Kakma。为了区分，这里生成的 Kakma 称为 Kakma-2。

可选的，当 AUSF 生成 A-KID#2 后，AUSF 可以向 AAnF 发送 A-KID#2、SUPI 和 Kakma-2。

5 具体的，可以通过“Naanf_AnchorKey_Register Request”向 AAnF 发送。AAnF 接收该消息后，向 AUSF 回复“Naanf_AKMA_Register Response”。

步骤 507 后，可选的，AUSF 可以删除 A-KID#2。

步骤 507 后，可选的，在 AUSF 保存 A-KID#2 以方便获得 RID#2 的情况下，AUSF 可以不删除 A-KID#2。

10 步骤 507 后，AUSF 可以删除 Kakma-2。

步骤 507 后，可选的，当 AUSF 删除 A-KID#2 后，可以保存 SUPI 和/或 RID#3。

本申请实施例中，在 AKMA 流程中，AUSF 可以从 AMF 中获取 RID。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时，AUSF 可以使用该 RID 生成新的 A-KID，保证 AKMA 流程的成功执行。

15 在前述实施例的基础上，请参阅图 6，图 6 为本申请实施例中又一种密钥标识的生成方法的实施例示意图。本申请实施例提出的一种密钥标识的生成方法，包括：

601、AUSF 接收 AMF 发送的鉴权请求消息#1，该鉴权请求消息#1 中携带 SUCI。

602、AUSF 基于 SUCI 中的 RID#1 生成 A-KID#1。

步骤 601-602 与前述步骤 501-502 类似，此处不作赘述。

20 603、AUSF 基于鉴权请求消息#1 向 AMF 发送第一鉴权请求响应，第一鉴权请求响应携带 AKMA 业务指示信息。

AUSF 基于鉴权请求消息#1 进行该 UE 的鉴权操作。当鉴权成功，则 AUSF 向 AMF 发送第一鉴权请求响应，该第一鉴权请求响应中携带用于指示该 UE 支持 AKMA 业务的指示信息（indication），该指示信息（indication）可以由 AUSF 自己生成。该指示信息也可以将从

25 UDM 收到的指示信息直接转发给 AMF，比如将 AKMA ID（或 AKMA indication）发给 AMF。该指示信息可以为值为 0 或者 1 的指示信息，比如当值为 1 时表示支持 AKMA 业务，当值为 0 时表示不支持 AKMA 业务。再比如，当值为 1 时表示支持 AKMA 业务，当不出现的时候表示不支持 AKMA 业务。也可以为字符串形式“AKMA”，或者枚举类型<AKMA enable>，<AKMA disable>。其可以通过是否出现表示是否支持 AKMA 业务，也可以通过具体含义指示是否支持 AKMA 业务。

30 示例性的，该第一鉴权请求响应为“Nausf_UEAuthentication_Authenticate Response”，该消息携带 EAP-success 消息或者携带告知 AMF 是否对 UE 鉴权成功的指示信息。

604、AMF 确定 UE 是否支持 AKMA 业务。

AMF 获取该第一鉴权请求响应后，AMF 保存该 AKMA 业务指示信息。比如，保存该
35 AKMA 业务指示信息与该 UE 的 SUPI 的关联关系。

605、AUSF 接收 AMF 发送的鉴权请求消息#2，鉴权请求消息#2 携带 SUPI 和 RID。

AMF 向 AUSF 发送鉴权请求消息#2 前，AMF 检查该 UE 是否支持 AKMA 业务，如果

确定该 UE 支持 AKMA 业务，则该鉴权请求消息#2 中携带 RID#2。该 RID#2 由 AMF 基于该 UE 的 SUPI 确定。AMF 基于该本地是否保存有 AKMA 业务指示信息确定 UE 是否支持 AKMA 业务。具体地，如果 AMF 本地保存有 AKMA 业务指示信息，则确定该 UE 支持 AKMA 业务。如果 AMF 本地没有保存 AKMA 业务指示信息，则确定该 UE 不支持 AKMA 业务。

在 AMF 确定 UE 支持 AKMA 业务的情况下，继续执行步骤 606。

在另一种实现方式中，AMF 确定该 SUPI 对应的 RID。其次，AMF 基于该 RID 构造 SUCI。在鉴权请求消息#2 中携带该构造的 SUCI#3。可选的，此时该鉴权请求消息#2 中不携带 SUCI 和 RID。具体地，AMF 使用 HPLMN 的公钥和 UE 的 SUPI 按照与 UE 相同的方式生成 SUCI#3。此时，要求 AMF 本地存储或者可以获得 HPLMN 的公钥、公钥标识符等生成 SUCI 的必要参数。

示例性的，鉴权请求消息#2 为 “Nausf_UEAuthentication_Authenticate request”。

606、AUSF 向 AMF 发送第二鉴权请求响应，第二鉴权请求响应携带 AKMA 业务指示信息。

当 AUSF 基于鉴权请求消息#2 完成该 UE 的鉴权操作后，AUSF 向 AMF 发送第二鉴权请求响应，该第二鉴权请求响应携带 AKMA 业务指示信息。此方法又称为显式的携带，显式的携带意味着每次都要发 AKMA 业务指示信息给 AMF，AMF 并进行检查该 UE 的 AKMA 业务指示信息是否依然存在，如果存在则可以更新已有的 UE 上下文信息，或者重新存储 AKMA 业务指示信息。如果 AKMA 业务指示信息不存在，则 AMF 可以认为该 UE 不再支持 AKMA 业务，则可以删除 UE 上下文中的 AKMA 业务指示信息。

可选的，该第二鉴权请求响应中也可以不携带 AKMA 业务指示信息。则 AMF 可以理解为该 UE 一直支持 AKMA 业务。当 UE 不再支持 AKMA 业务的时候，AUSF 发送一个 AKMA 业务取消指示信息，该指示信息表示 UE 不再支持 AKMA 业务。该 AKMA 业务取消指示信息可以与 AKMA 业务指示信息共同一个比特位信息。比如当值为 0 时，表示 UE 不支持 AKMA 业务，当值为 1 时，表示 UE 支持 AKMA 业务。AMF 在收到 AKMA 业务取消指示信息后，AMF 更新 UE 上下文信息，删除 AKMA 业务指示信息。该方法可以简化 AUSF 传递给 AMF 消息的复杂度，也同时降低了 AMF 处理的复杂度。

607、当鉴权请求消息#2 中携带 SUPI 和 RID#3 时，AUSF 基于该 RID#3 生成 A-KID#2。

步骤 607 后，进一步的，AUSF 生成 Kakma。为了区分，这里生成的 Kakma 称为 Kakma-2。

可选的，当 AUSF 生成 A-KID#2 后，AUSF 可以向 AAnF 发送 A-KID#2、SUPI 和 Kakma-2。具体的，可以通过 “Naanf_AnchorKey_Register Request” 向 AAnF 发送。AAnF 接收该消息后，向 AUSF 回复 “Naanf_AKMA_Register Response”。

步骤 607 后，可选的，AUSF 可以删除 Kakma-2。

本申请实施例中，在 AKMA 流程中，AMF 判断 UE 支持 AKMA 业务的情况下，AMF 可以在鉴权请求消息中携带 RID，AUSF 从该鉴权请求消息中获取 RID。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时，AUSF 可以使用该 RID 生成新的 A-KID，保证 AKMA 流程的成功执行。

在前述实施例的基础上，还可以由 UDM 提供 RID。具体的，请参阅图 7，图 7 为本申请实施例中又一种密钥标识的生成方法的实施例示意图。本申请实施例提出的一种密钥标识的生成方法，包括：

701、AUSF 接收 AMF 发送的鉴权请求消息#1，该鉴权请求消息#1 中携带 SUCI。

5 步骤 701 与前述步骤 501 类似，此处不作赘述。

702、AUSF 向 UDM 发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带 SUCI。

AUSF 接收 AMF 发送的鉴权请求消息#1 后，AUSF 向 UDM 发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带 SUCI。该鉴权向量获取请求消息#1 用于获取 RID#2。

10 示例性的，该鉴权向量获取请求消息#1 为“Nudm_UE_Authentication_Get_Request”。

703、UDM 向 AUSF 发送鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 不携带 RID。

UDM 接收该鉴权向量获取请求消息#1 后，UDM 向 AUSF 发送鉴权向量获取响应消息#1，该鉴权向量获取响应消息#1 中不携带 RID。

15 示例性的，该鉴权向量获取响应消息#1 为“Nudm_UE_Authentication_Get_Response”。当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#1 后，AUSF 对该 UE（与该鉴权请求消息#1 对应的 UE）进行鉴权操作。当鉴权成功，则 AUSF 向 AMF 发送鉴权请求响应（authentication success）。

可选的，该鉴权向量获取响应消息#1 中还携带鉴权向量(authentication vector, AV)。

20 可选的，该鉴权向量获取响应消息#1 中还携带认证和密钥管理指示信息 AKMA indication。

示例性的，该鉴权向量获取响应消息#1 为“Nudm_UE_Authentication_Get_Response”。当鉴权成功，则 AUSF 向 AMF 发送鉴权请求响应（authentication success）。

704、AUSF 生成 A-KID#1。

25 步骤 704 与前述步骤 502 类似，此处不作赘述。

705、AUSF 接收 AMF 发送的鉴权请求消息#2。

AUSF 接收 AMF 发送的鉴权请求消息#2。该鉴权请求消息#2 中携带 SUPI，则进入步骤 706。

30 可选的，AUSF 接收鉴权请求消息#2 后，AUSF 可以向 UDM 发送鉴权向量获取请求消息#2，该鉴权向量获取请求消息#2 携带该 SUPI。该鉴权向量获取请求消息#2 可以是：

“Nudm_UE_Authentication_Get_Request”。

UDM 接收 AUSF 发送的鉴权向量获取请求消息#2 后。AUSF 根据该鉴权向量获取响应消息#2 中携带的认证和密钥管理指示信息，确定该 UE 支持 AKMA 业务。AUSF 确定需要生成该 UE 的 A-KID。UDM 向 AUSF 发送鉴权向量获取响应消息#2，该鉴权向量获取响应消息#2 中携带鉴权向量(authentication vector, AV)。该鉴权向量获取响应消息#2 中不携带 RID。

可选的，该鉴权向量获取响应消息#2 中还携带认证和密钥管理指示信息 AKMA

indication。

示例性的，该鉴权向量获取响应消息#2 为“Nudm_UE_Authentication_Get_Response”。

当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#2 后，AUSF 对该 UE（与该鉴权请求消息#2 对应的 UE）进行鉴权操作。当鉴权成功，则 AUSF 向 AMF 发送鉴权请求响应

5 (authentication success)。

进一步的，AUSF 基于该 SUPI，生成 Kakma。

706、AUSF 向 UDM 发送第二请求，第二请求中携带 SUPI。

可选的，第二请求中携带一个需要 RID 的指示信息。

AUSF 接收鉴权请求消息#2 后，AUSF 向 UDM 发送第二请求，该第二请求用于向 UDM
10 请求 RID#2。

可选的，AUSF 在生成生成 Kakma 后，AUSF 向 UDM 发送第二请求。

可选的，AUSF 向 AMF 发送鉴权请求响应后，即 AUSF 完成 UE 的鉴权后，AUSF 向 UDM 发送第二请求。

示例性的，该第二请求为“Nudm_UE_AKMA_Get_Request”。

15 AUSF 接收 AMF 发送的鉴权请求消息#2 后，AUSF 检测鉴权请求消息#2 中是否携带有 RID#2。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。

如果鉴权请求消息#2 没有 RID#3 相关的参数，则 AUSF 向 UDM 发送第二请求，该第二请求用于请求 RID。该第二请求中携带 SUPI，该 SUPI 为鉴权请求消息#2 中携带的 SUPI。

20 可选的，进一步地，如果鉴权请求消息#2 和 AUSF 本地均没有 RID（RID#3 与 RID#4）相关的参数，则 AUSF 向 UDM 发送第二请求，该第二请求用于请求 RID。

可选的，第二请求中携带一个需要 RID 的指示信息。

具体地，AUSF 在接收 UDM 发送的鉴权向量获取响应消息#2 后，AUSF 确定该 UE 支持 AKMA 业务后，AUSF 没有在鉴权请求消息#2 中收到 RID#3，和/或 AUSF 本地没有保存有 RID#4，则 AUSF 向 UDM 发送该第二请求。
25

步骤 706 中，AUSF 接收 AMF 发送的鉴权请求消息#2 后，存在两种可选的实现方案，下面分别进行描述：

方案一：AUSF 每次接收鉴权请求消息#2 后，检测该鉴权请求消息#2 中是否携带 RID。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。当检测结果为鉴权请求消息#2 中没有 RID#3（鉴权请求消息#2 中没有 RID
30 且，AUSF 本地没有 RID#4 相关的参数），则 AUSF 向 UDM 发送第二请求。步骤 708 中，AUSF 不保存来自 UDM 的第二响应中携带的 RID#1。即 AUSF 每次接收鉴权请求消息#2 后，都会检测该鉴权请求消息#2 中是否携带 RID#3，如果不携带，则 AUSF 向 UDM 发送第二请求。

35 方案二：AUSF 接收鉴权请求消息#2 后，检测该鉴权请求消息#2 中是否携带 RID。可选的，AUSF 还检测 AUSF 本地是否保存有 RID#4 相关的参数（例如 RID#4、SUCI 和/或 A-KID#1）。当检测结果为鉴权请求消息#2 中没有 RID#3（或者鉴权请求消息#2 中没有

RID#1, 且 AUSF 本地没有 RID#4 相关的参数), 则 AUSF 向 UDM 发送第二请求。步骤 708 中, AUSF 保存来自 UDM 的第二响应中携带的 RID#2。即 AUSF 第一次接收到不携带 RID 的鉴权请求消息#2 后, AUSF 向 UDM 发送第二请求。步骤 708 中 AUSF 会保存 AMF 基于该第二请求返回的 RID#3。后续步骤中当 AUSF 再次接收到不携带 RID 的鉴权请求消息#2 时, AUSF 可以基于本地保存的 RID#4 (步骤 708 中保存的) 进行后续动作。示例性的, 第二请求为 “Nudm_UE_AKMA_Get_Request”。

AUSF 接收 AMF 发送的鉴权请求消息#2 后, AUSF 判断鉴权请求消息#2 中是否携带有 RID#3。如果携带有 RID#3, 则执行步骤 709。

AUSF 接收 AMF 发送的鉴权请求消息#2 后, AUSF 判断本地保存有 RID#4 相关的参数的情况下, 则执行步骤 709。

707、UDM 基于第二请求中携带的 SUPI, 确定 RID#2。

UDM 接收第一请求后, 基于该第二请求中携带的 SUPI, 确定该 SUPI 对应的 RID#2。

708、UDM 向 AUSF 发送第二响应, 第二响应携带 RID#2。

UDM 向 AUSF 发送第二响应, 该第二响应中携带 RID#2。

示例性的, 第二响应为 “Nudm_UE_AKMA_Get_Response”。

709、当鉴权请求消息#2 中携带 SUPI 时, AUSF 基于 RID#2 生成 A-KID#2。

进一步的, AUSF 基于生成 Kakma。为了区分, 这里生成的 Kakma 称为 Kakma-2。

可选的, 当 AUSF 生成 A-KID#2 后, AUSF 可以向 AAnF 发送 A-KID#2、SUPI 和 Kakma-2。具体的, 可以通过 “Naanf_AnchorKey_Register Request” 向 AAnF 发送。AAnF 接收该消息后, 向 AUSF 回复 “Naanf_AKMA_Register Response”。

步骤 709 后, AUSF 可以删除 A-KID#2。

步骤 709 后, 可选的, AUSF 可以删除 Kakma-2。

本申请实施例中, 在 AKMA 流程中, AUSF 可以从 UDM 中获取 RID。以保证 AUSF 接收的鉴权向量获取请求消息中携带 SUPI 时, AUSF 可以使用该 RID 生成新的 A-KID, 保证 AKMA 流程的成功执行。

在前述实施例的基础上, 请参阅图 8, 图 8 为本申请实施例中又一种密钥标识的生成方法的实施例示意图。本申请实施例提出的一种密钥标识的生成方法, 包括:

801、AUSF 接收 AMF 发送的鉴权请求消息#1, 该鉴权请求消息#1 中携带 SUCI。

802、AUSF 向 UDM 发送鉴权向量获取请求消息#1, 鉴权向量获取请求消息#1 中携带 SUCI。

步骤 801-802 与前述步骤 701-702 类似, 此处不作赘述。

803、UDM 基于鉴权向量获取请求消息#1 中携带的 SUCI, 确定 RID#1。

UDM 基于该鉴权向量获取请求消息#1 中携带的 SUCI 确定 RID#1 后, UDM 存储该 RID#1, UDM 中存储的 RID#1 称为 RID#2。

进一步地, UDM 存储 RID#2 和, RID#2 与 SUPI 的关联关系。

可选的, UDM 存储 RID#2, SUCI, 和, RID#1 与 SUCI 的关联关系。进一步地, UDM 存储 RID#2 与 SUCI 与 SUPI 的关联关系。

可选的, UDM 存储 SUCI, 即 UDM 不单独存储 RID#2。进一步地, UDM 存储 SUCI 和, SUCI 与 SUPI 的关联关系。

可选的, 当 RID 的值为缺省值时, 步骤 803 中 UDM 可以不存储 RID#1。则步骤 805 中 AUSF 基于该缺省值生成 A-KID#1。

5 804、UDM 向 AUSF 发送鉴权向量获取响应消息#1, 鉴权向量获取响应消息#1 携带 RID#2。

进一步地, UDM 在确定该 UE 支持 AKMA 业务后, 在鉴权向量获取响应消息#1 中携带 RID#2。UDM 向 AUSF 发送鉴权向量获取响应消息#1, 该鉴权向量获取响应消息#1 携带 RID#2。

10 可选的, 该鉴权向量获取响应消息#1 不携带 RID。

AUSF 接收鉴权请求消息#1 后, AUSF 可以向 UDM 发送鉴权向量获取请求消息#1, 该鉴权向量获取请求消息#1 携带该 SUCI。该鉴权向量获取请求消息#1 可以是:

“Nudm_UE_Authentication_Get_Request”。

UDM 接收 AUSF 发送的鉴权向量获取请求消息#1 后。UDM 向 AUSF 发送鉴权向量获取响应消息#1, 该鉴权向量获取响应消息#1 中携带 RID#2。该鉴权向量获取响应消息#1 中还携带鉴权向量(authentication vector, AV)。可选的, 该鉴权向量获取响应消息#1 中还携带认证和密钥管理指示信息 AKMA indication。可选的, AUSF 记录该 UE 支持 AKMA 业务, 比如 AUSF 存储 AKMA indication。进一步地, AUSF 存储 AKMA indication 和 SUPI 的关联关系。示例性的, 该鉴权向量获取响应消息#1 为“Nudm_UE_Authentication_Get_Response”。

20 当 AUSF 接收来自 UDM 的鉴权向量获取响应消息#1 后, AUSF 对该 UE (与该鉴权请求消息#1 对应的 UE) 进行鉴权操作。当鉴权成功, 则 AUSF 向 AMF 发送鉴权请求响应 (authentication success)。

805、AUSF 基于 RID 生成 A-KID#1。

AUSF 接收鉴权请求消息#1 后, AUSF 基于该鉴权请求消息#1 中的 SUCI 中的 RID#1, 生成 A-KID#1。

可选的, AUSF 基于鉴权向量获取响应消息#1 中携带的 RID#2, 生成 A-KID#1。

进一步的, AUSF 基于生成 Kakma。为了区分, 这里生成的 Kakma 称为 Kakma-2。

可选的, 当 AUSF 生成 A-KID#1 后, AUSF 可以向 AAnF 发送 A-KID#1、SUPI 和 Kakma。具体的, 可以通过 “Naanf_AnchorKey_Register Request” 向 AAnF 发送。AAnF 接收该消息后, 向 AUSF 回复 “Naanf_AKMA_Register Response”。

30 806、AUSF 接收 AMF 发送的鉴权请求消息#2。

示例性的, 鉴权请求消息#2 为 “Nausf_UEAuthentication_Authenticate Request”。

807、AUSF 向 UDM 发送鉴权向量获取请求消息#2, 鉴权向量获取请求消息#2 中携带 SUPI。

35 AUSF 接收鉴权请求消息#2 后, AUSF 向 UDM 发送鉴权向量获取请求消息#2, 该鉴权向量获取请求消息#2 携带该 SUPI。该鉴权向量获取请求消息可以是:

“Nudm_UE_Authentication_Get_Request”。

鉴权向量获取请求消息#2中携带指示信息,该指示信息用于向UDM请求下发RID#2。具体地,AUSF查看是否有存储记录该UE支持AKMA业务,如果确定该UE支持AKMA业务,则在鉴权向量获取请求消息#2中携带指示信息。

具体地,AUSF接收AMF发送的鉴权请求消息#2后,AUSF检测鉴权请求消息#2中是否携带有RID#3。可选的,AUSF还检测AUSF本地是否保存有RID#4相关的参数(例如RID#4、SUCI和/或A-KID#1)。

如果鉴权请求消息#2没有RID相关的参数,并且AUSF存储有该UE支持AKMA业务,则AUSF向UDM发送鉴权向量获取请求消息#2,该鉴权向量获取请求消息#2用于请求鉴权向量和RID。具体的,该鉴权向量获取请求消息#2中携带SUPI和指示信息。该指示信息用于向UDM请求下发RID#2。

808、UDM基于鉴权向量获取请求消息#2中携带的SUPI,确定RID#2。

UDM接收AUSF发送的鉴权向量获取请求消息#2后。UDM基于该鉴权向量获取请求消息#2中携带的SUPI,确定RID#2。

UDM根据该鉴权向量获取请求消息#2中携带的指示信息,确定该SUPI对应的RID#2。

809、UDM向AUSF发送鉴权向量获取响应消息#2,鉴权向量获取响应消息#2携带RID#2。

UDM向AUSF发送鉴权向量获取响应消息#2,该鉴权向量获取响应消息#2中携带RID#2。

该鉴权向量获取响应消息#2中还携带鉴权向量(authentication vector, AV)。

可选的,该鉴权向量获取响应消息#2中还携带认证和密钥管理指示信息AKMA indication。示例性的,该鉴权向量获取响应消息#2为“Nudm_UE_Authentication_Get_Response”。

当AUSF接收来自UDM的鉴权向量获取响应消息#2后,AUSF对该UE(与该鉴权请求消息#1对应的UE)进行鉴权操作。当鉴权成功,则AUSF向AMF发送鉴权请求响应(authentication success)。

810、当鉴权请求消息#2中携带SUPI时,AUSF基于该鉴权向量获取响应消息#2中的RID#2生成A-KID#2。

当鉴权请求消息#2中携带SUPI,AUSF基于该鉴权向量获取响应消息#2中的RID#2生成A-KID#2。该RID#2来自UDM发送的鉴权向量获取响应消息#2。

可选的,当AUSF生成A-KID#2后,AUSF可以向AAnF发送A-KID#2、SUPI和Kakma-2。具体的,可以通过“Naanf_AnchorKey_Register Request”向AAnF发送。AAnF接收该消息后,向AUSF回复“Naanf_AKMA_Register Response”。

本申请实施例中,在AKMA流程中,AUSF可以从UDM中获取RID。UDM在现有的鉴权向量获取响应消息中携带该RID。以保证AUSF接收的鉴权向量获取请求消息中携带SUPI时,AUSF可以使用该RID生成新的A-KID,保证AKMA流程的成功执行。

上述主要以方法的角度对本申请实施例提供的方案进行了介绍。可以理解的是,通信装置为了实现上述功能,其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技

术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的模块及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

本申请实施例可以根据上述方法示例对通信装置进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

下面对本申请中的通信装置进行详细描述，请参阅图 9，图 9 为本申请实施例中通信装置的一种实施例示意图。通信装置可以部署于网络设备中，通信装置包括：

收发模块 901，用于接收来自接入与移动性管理功能鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

收发模块 901，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；

收发模块 901，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；

处理模块 902，用于根据认证和密钥管理指示信息，基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

处理模块 902，还用于保存路由标识。

在一种可能的实现方式中，收发模块 901，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；

处理模块 902，还用于在鉴权请求消息#2 中携带永久身份标识的情况下，使用保存的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，处理模块 902，还用于基于对终端设备进行鉴权流程中生成的中间密钥，生成认证和密钥管理-密钥临时身份标识；

处理模块 902，还用于将路由标识和认证和密钥管理-密钥临时身份标识进行拼接，得到认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块 902，还用于保存认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，鉴权向量获取响应消息#1 中还包括路由标识；

处理模块 902，还用于基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1，包括：

处理模块 902，还用于基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块 902，还用于保存签约隐藏标识符。

在一种可能的实现方式中，处理模块 902，还用于删除认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，处理模块 902，还用于删除认证和密钥管理-密钥临时身份标识#2；

处理模块 902，还用于继续保存路由标识。

请参阅图 10，图 10 为本申请实施例中通信装置的一种实施例示意图。通信装置可以部署于网络设备中，通信装置包括：

收发模块 1001，用于接收来自接入与移动性管理功能的鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

收发模块 1001，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；

收发模块 1001，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息和签约隐藏标识符中的路由标识；

处理模块 1002，用于根据认证和密钥管理指示信息，基于路由标识生成认证和密钥管理-密钥临时身份标识#1。

在一种可能的实现方式中，收发模块 1001，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；

收发模块 1001，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块 1001，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2，鉴权向量获取响应消息#2 包括路由标识；

处理模块 1002，还用于使用路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，收发模块 1001，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；

收发模块 1001，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块 1001，还用于根据认证和密钥管理指示信息，从核心网网元获取路由标识；

处理模块 1002，还用于使用路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，处理模块 1002，还用于根据认证和密钥管理指示信息，确定需要生成认证和密钥管理-密钥临时身份标识#2；

收发模块 1001，还用于在鉴权管理功能本地没有路由标识的情况下，从核心网网元获取路由标识。

在一种可能的实现方式中，核心网网元包括统一数据管理功能或者接入与移动性管理功能。

在一种可能的实现方式中，收发模块 1001，还用于接收来自统一数据管理功能的鉴权

向量获取响应消息#2，鉴权向量获取响应消息#2 包括认证和密钥管理指示信息。

请参阅图 11，图 11 为本申请实施例中通信装置的一种实施例示意图。通信装置可以部署于网络设备中，通信装置包括：

收发模块 1101，用于接收来自接入与移动性管理功能的鉴权请求消息#1，鉴权请求消息#1 中携带签约隐藏标识符，签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

收发模块 1101，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，鉴权向量获取请求消息#1 中携带签约隐藏标识符；

收发模块 1101，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#1，鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；

处理模块 1102，用于根据认证和密钥管理指示信息，基于签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

收发模块 1101，还用于接收来自接入与移动性管理功能的鉴权请求消息#2；其中，鉴权请求消息#2 包括永久身份标识和路由标识；

处理模块 1102，还用于使用从接入与移动性管理功能接收到的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，收发模块 1101，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，其中，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块 1101，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2。

在一种可能的实现方式中，收发模块 1101，还用于向接入与移动性管理功能发送第一鉴权请求响应；第一鉴权请求响应包括第一指示信息，第一指示信息用于指示终端设备支持应用的认证和密钥管理业务。

在一种可能的实现方式中，处理模块 1102，还用于基于鉴权向量获取响应消息#1 中的路由标识生成认证和密钥管理-密钥临时身份标识#1。

请参阅图 12，图 12 为本申请实施例中通信装置的一种实施例示意图。通信装置可以部署于网络设备中，通信装置包括：

收发模块 1201，用于接收来自接入与移动性管理功能的鉴权请求消息#2；鉴权请求消息#2 包括永久身份标识；

收发模块 1201，还用于向统一数据管理功能发送鉴权向量获取请求消息#2，鉴权向量获取请求消息#2 中携带永久身份标识；

收发模块 1201，还用于接收来自统一数据管理功能的鉴权向量获取响应消息#2，鉴权向量获取响应消息#2 包括认证和密钥管理指示信息；

处理模块 1202，还用于根据认证和密钥管理指示信息，确定需要生成认证和密钥管理-密钥临时身份标识；

收发模块 1201，还用于在鉴权管理功能本地没有路由标识的情况下，从核心网网元获取路由标识；

处理模块 1202，还用于使用路由标识生成认证和密钥管理-密钥临时身份标识#2。

在一种可能的实现方式中，核心网网元包括统一数据管理功能或者接入与移动性管理功能。

可选地，上述通信装置还可以包括存储单元，该存储单元用于存储数据和/或指令（也可以称为代码或者程序）。上述各个单元可以和存储单元交互或者耦合，以实现对应的方法或者功能。例如，处理模块 1202 可以读取存储单元中的数据或者指令，使得通信装置实现上述实施例中的方法。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。

本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，另外，在本申请各个实施例中的各功能模块可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上模块集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

在一个例子中，以上任一通信装置中的单元可以是配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路（application specific integrated circuit, ASIC），或，一个或多个微处理器（digital signal processor, DSP），或，一个或者多个现场可编程门阵列（field programmable gate array, FPGA），或这些集成电路形式中至少两种的组合。再如，当通信装置中的单元可以通过处理元件调度程序的形式实现时，该处理元件可以是通用处理器，例如中央处理器（central processing unit, CPU）或其它可以调用程序的处理器。再如，这些单元可以集成在一起，以片上系统（system-on-a-chip, SOC）的形式实现。

本申请还提供一种通信系统，其包括网络设备或终端设备中的至少一种或多种。

本申请实施例还提供的一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机控制网络设备或终端设备执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供的一种计算机程序产品，计算机程序产品包括计算机程序代码，当计算机程序代码在计算机上运行时，使得计算机执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供一种芯片系统，包括存储器和处理器，存储器用于存储计算机程序，处理器用于从存储器中调用并运行计算机程序，使得芯片执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供一种芯片系统，包括处理器，处理器用于调用并运行计算机程序，使得芯片执行如前述方法实施例所示任一项实现方式。

本申请实施例提供的技术方案可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、AI 节点、接入网设备、终端设备或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line, DSL））或

无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机可以存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，数字视频光盘（digital video disc, DVD））、或者半导体介质等。

在本申请实施例中，在无逻辑矛盾的前提下，各实施例之间可以相互引用，例如方法实施例之间的方法和/或术语可以相互引用，例如装置实施例之间的功能和/或术语可以相互引用，例如装置实施例和方法实施例之间的功能和/或术语可以相互引用。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。

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

权 利 要 求

1、一种密钥标识的生成方法，其特征在于，包括：

鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

所述鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1中携带所述签约隐藏标识符；

所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1包括认证和密钥管理指示信息；

根据所述认证和密钥管理指示信息，所述鉴权管理功能基于所述签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

所述鉴权管理功能保存所述路由标识。

2、根据权利要求1所述的方法，其特征在于，所述方法还包括：

所述鉴权管理功能接收来自所述接入与移动性管理功能的鉴权请求消息#2；

在所述鉴权请求消息#2中携带所述永久身份标识的情况下，所述鉴权管理功能使用所述保存的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

3、根据权利要求1或2所述的方法，其特征在于，所述鉴权管理功能基于所述签约隐藏标识符中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1，包括：

所述鉴权管理功能基于对所述终端设备进行鉴权流程中生成的中间密钥，生成认证和密钥管理-终端设备临时标识；

所述鉴权管理功能将所述路由标识和所述认证和密钥管理-终端设备临时标识获得所述认证和密钥管理-密钥临时身份标识#1。

4、根据权利要求3所述的方法，其特征在于，所述鉴权管理功能保存所述路由标识，包括：

所述鉴权管理功能保存所述认证和密钥管理-密钥临时身份标识#1。

5、根据权利要求1或2所述的方法，其特征在于，所述鉴权向量获取响应消息#1中还包括所述路由标识；

所述鉴权管理功能基于所述签约隐藏标识符中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1，包括：

所述鉴权管理功能基于所述鉴权向量获取响应消息#1中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1。

6、根据权利要求1或2所述的方法，其特征在于，所述鉴权管理功能保存所述路由标识，包括：

所述鉴权管理功能保存所述签约隐藏标识符。

7、根据权利要求1-6中任一项所述的方法，其特征在于，所述鉴权管理功能保存所述路由标识之后，所述方法还包括：

所述鉴权管理功能向删除所述认证和密钥管理-密钥临时身份标识#1。

8、根据权利要求 2-7 中任一项所述的方法，其特征在于，所述鉴权管理功能基于所述保存的路由标识生成所述认证和密钥管理-密钥临时身份标识#2 之后，所述方法还包括：

所述鉴权管理功能删除所述认证和密钥管理-密钥临时身份标识#2；

所述鉴权管理功能继续保存所述路由标识。

5 9、一种密钥标识的生成方法，其特征在于，包括：

鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1 中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

10 所述鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1 中携带所述签约隐藏标识符；

所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1 包括认证和密钥管理指示信息和所述签约隐藏标识符中的路由标识；

15 根据所述认证和密钥管理指示信息，所述鉴权管理功能基于所述路由标识生成认证和密钥管理-密钥临时身份标识#1。

10、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

所述鉴权管理功能接收来自所述接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括所述永久身份标识；

20 所述鉴权管理功能向所述统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，所述鉴权向量获取响应消息#2 包括所述路由标识；

所述鉴权管理功能使用所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

11、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：

25 所述鉴权管理功能接收来自所述接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括所述永久身份标识；

所述鉴权管理功能向所述统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

30 所述鉴权管理功能根据所述认证和密钥管理指示信息，从核心网网元获取所述路由标识；

所述鉴权管理功能使用所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

12、根据权利要求 11 所述的方法，其特征在于，所述鉴权管理功能根据所述认证和密钥管理指示信息，从其他核心网网元获取所述路由标识，包括：

35 所述鉴权管理功能根据所述认证和密钥管理指示信息，确定需要生成所述认证和密钥管理-密钥临时身份标识#2；

在所述鉴权管理功能本地没有所述路由标识的情况下，所述鉴权管理功能从所述核心网网元获取所述路由标识。

13、根据权利要求 11 或 12 所述的方法，其特征在于，所述核心网网元包括所述统一数据管理功能或者所述接入与移动性管理功能。

14、根据权利要求 11 所述的方法，其特征在于，在所述鉴权管理功能根据所述认证和密钥管理指示信息，从所述核心网网元获取路由标识之前，所述方法还包括：

5 所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，所述鉴权向量获取响应消息#2 包括所述认证和密钥管理指示信息。

15、一种密钥标识的生成方法，其特征在于，包括：

 鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1 中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；
10

 所述鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1 中携带所述签约隐藏标识符；

 所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；

15 根据所述认证和密钥管理指示信息，所述鉴权管理功能基于所述签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

 所述鉴权管理功能接收来自所述接入与移动性管理功能的鉴权请求消息#2；其中，所述鉴权请求消息#2 包括所述永久身份标识和所述路由标识；

 所述鉴权管理功能使用从所述接入与移动性管理功能接收到的所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。
20

16、根据权利要求 15 所述的方法，其特征在于，在所述鉴权管理功能使用从所述接入与移动性管理功能接收到的所述路由标识生成新的所述认证和密钥管理-密钥临时身份标识#2 之前，所述方法还包括：

 所述鉴权管理功能向所述统一数据管理功能发送鉴权向量获取请求消息#2，其中，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；
25

 所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#2。

17、根据权利要求 15 或 16 所述的方法，其特征在于，在所述鉴权管理功能接收来自所述接入与移动性管理功能的所述鉴权请求消息#2 之前，所述方法还包括：

 所述鉴权管理功能向所述接入与移动性管理功能发送第一鉴权请求响应；所述第一鉴权请求响应包括第一指示信息，所述第一指示信息用于指示所述终端设备支持应用的认证和密钥管理业务。
30

18、根据权利要求 15-17 任一所述的方法，其特征在于，所述鉴权向量获取响应消息#1 中还包括所述路由标识；

 所述鉴权管理功能基于所述签约隐藏标识符中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1，包括；
35

 所述鉴权管理功能基于所述鉴权向量获取响应消息#1 中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1。

19、一种密钥标识的生成方法，其特征在于，包括：

鉴权管理功能接收来自接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括永久身份标识；

5 所述鉴权管理功能向统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述鉴权管理功能接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，所述鉴权向量获取响应消息#2 包括认证和密钥管理指示信息；

所述鉴权管理功能根据所述认证和密钥管理指示信息，确定需要生成认证和密钥管理-密钥临时身份标识；

10 在所述鉴权管理功能本地没有路由标识的情况下，所述鉴权管理功能从核心网网元获取所述路由标识；

所述鉴权管理功能使用所述路由标识生成认证和密钥管理-密钥临时身份标识#2。

20、根据权利要求 19 所述的方法，其特征在于，所述核心网网元包括所述统一数据管理功能或者所述接入与移动性管理功能。

15 21、一种通信装置，其特征在于，包括：

收发模块，用于接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1 中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

20 所述收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1 中携带所述签约隐藏标识符；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；

处理模块，用于根据所述认证和密钥管理指示信息，基于所述签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

25 所述处理模块，还用于保存所述路由标识。

22、根据权利要求 21 所述的通信装置，其特征在于，

所述收发模块，还用于接收来自所述接入与移动性管理功能的鉴权请求消息#2；

所述处理模块，还用于在所述鉴权请求消息#2 中携带所述永久身份标识的情况下，使用所述保存的路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

30 23、根据权利要求 21 或 22 所述的通信装置，其特征在于，

所述处理模块，还用于基于对所述终端设备进行鉴权流程中生成的中间密钥，生成认证和密钥管理-终端设备临时标识；

所述处理模块，还用于将所述路由标识和所述认证和密钥管理-终端设备临时标识获得所述认证和密钥管理-密钥临时身份标识#1。

35 24、根据权利要求 23 所述的通信装置，其特征在于，

所述处理模块，还用于保存所述认证和密钥管理-密钥临时身份标识#1。

25、根据权利要求 21 或 22 所述的通信装置，其特征在于，所述鉴权向量获取响应消

息#1 中还包括所述路由标识；

所述处理模块，还用于基于所述签约隐藏标识符中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1，包括：

所述处理模块，还用于基于所述鉴权向量获取响应消息#1 中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1。

26、根据权利要求 21 或 22 所述的通信装置，其特征在于，

所述处理模块，还用于保存所述签约隐藏标识符。

27、根据权利要求 21-26 中任一项所述的通信装置，其特征在于，所

所述处理模块，还用于删除所述认证和密钥管理-密钥临时身份标识#1。

28、根据权利要求 22-27 中任一项所述的通信装置，其特征在于，

所述处理模块，还用于删除所述认证和密钥管理-密钥临时身份标识#2；

所述处理模块，还用于继续保存所述路由标识。

29、一种通信装置，其特征在于，包括：

收发模块，用于接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1 中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

所述收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1 中携带所述签约隐藏标识符；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1 包括认证和密钥管理指示信息和所述签约隐藏标识符中的路由标识；

处理模块，用于根据所述认证和密钥管理指示信息，基于所述路由标识生成认证和密钥管理-密钥临时身份标识#1。

30、根据权利要求 29 所述的通信装置，其特征在于，

所述收发模块，还用于接收来自所述接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括所述永久身份标识；

所述收发模块，还用于向所述统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，

所述鉴权向量获取响应消息#2 包括所述路由标识；

所述处理模块，还用于使用所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

31、根据权利要求 29 所述的通信装置，其特征在于，

所述收发模块，还用于接收来自所述接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括所述永久身份标识；

所述收发模块，还用于向所述统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述收发模块，还用于根据所述认证和密钥管理指示信息，从核心网网元获取所述路由标识；

所述处理模块，还用于使用所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

5 32、根据权利要求 31 所述的通信装置，其特征在于，

所述处理模块，还用于根据所述认证和密钥管理指示信息，确定需要生成所述认证和密钥管理-密钥临时身份标识#2；

所述收发模块，还用于在鉴权管理功能本地没有所述路由标识的情况下，从所述核心网网元获取所述路由标识。

10 33、根据权利要求 31 或 32 所述的通信装置，其特征在于，所述核心网网元包括所述统一数据管理功能或者所述接入与移动性管理功能。

34、根据权利要求 31 所述的通信装置，其特征在于，

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，所述鉴权向量获取响应消息#2 包括所述认证和密钥管理指示信息。

15 35、一种通信装置，其特征在于，包括：

收发模块，用于接收来自接入与移动性管理功能的鉴权请求消息#1，所述鉴权请求消息#1 中携带签约隐藏标识符，所述签约隐藏标识符为基于终端设备的永久身份标识生成的用户隐藏标识；

20 所述收发模块，还用于向统一数据管理功能发送鉴权向量获取请求消息#1，所述鉴权向量获取请求消息#1 中携带所述签约隐藏标识符；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#1，所述鉴权向量获取响应消息#1 包括认证和密钥管理指示信息；

处理模块，用于根据所述认证和密钥管理指示信息，基于所述签约隐藏标识符中的路由标识生成认证和密钥管理-密钥临时身份标识#1；

25 所述收发模块，还用于接收来自所述接入与移动性管理功能的鉴权请求消息#2；其中，所述鉴权请求消息#2 包括所述永久身份标识和路由标识；

所述处理模块，还用于使用从所述接入与移动性管理功能接收到的所述路由标识生成新的认证和密钥管理-密钥临时身份标识#2。

36、根据权利要求 35 所述的通信装置，其特征在于，

30 所述收发模块，还用于向所述统一数据管理功能发送鉴权向量获取请求消息#2，其中，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#2。

37、根据权利要求 35 或 36 所述的通信装置，其特征在于，

35 所述收发模块，还用于向所述接入与移动性管理功能发送第一鉴权请求响应；所述第一鉴权请求响应包括第一指示信息，所述第一指示信息用于指示所述终端设备支持应用的认证和密钥管理业务。

38、根据权利要求 35-37 任一所述的通信装置，其特征在于，

所述处理模块，还用于基于所述鉴权向量获取响应消息#1 中的所述路由标识生成所述认证和密钥管理-密钥临时身份标识#1。

39、一种通信装置，其特征在于，包括：

收发模块，用于接收来自接入与移动性管理功能的鉴权请求消息#2；所述鉴权请求消息#2 包括永久身份标识；

所述收发模块，还用于向所述统一数据管理功能发送鉴权向量获取请求消息#2，所述鉴权向量获取请求消息#2 中携带所述永久身份标识；

所述收发模块，还用于接收来自所述统一数据管理功能的鉴权向量获取响应消息#2，所述鉴权向量获取响应消息#2 包括认证和密钥管理指示信息；

所述处理模块，还用于根据所述认证和密钥管理指示信息，确定需要生成认证和密钥管理-密钥临时身份标识；

所述收发模块，还用于在所述鉴权管理功能本地没有路由标识的情况下，从核心网网元获取所述路由标识；

所述处理模块，还用于使用所述路由标识生成认证和密钥管理-密钥临时身份标识#2。
40、根据权利要求 39 所述的通信装置，其特征在于，所述核心网网元包括所述统一数据管理功能或者所述接入与移动性管理功能。

41、一种通信装置，其特征在于，所述通信装置包括：处理器；

所述处理器，用于执行存储器中存储的计算机程序或指令，以使所述通信装置执行如权利要求 1-8 中任一项所述的方法。

42、一种通信装置，其特征在于，所述通信装置包括：处理器；

所述处理器，用于执行存储器中存储的计算机程序或指令，以使所述通信装置执行如权利要求 9-14 中任一项所述的方法。

43、一种通信装置，其特征在于，所述通信装置包括：处理器；

所述处理器，用于执行存储器中存储的计算机程序或指令，以使所述通信装置执行如权利要求 15-18 中任一项所述的方法。

44、一种通信装置，其特征在于，所述通信装置包括：处理器；

所述处理器，用于执行存储器中存储的计算机程序或指令，以使所述通信装置执行如权利要求 19-20 中任一项所述的方法。

45、一种通信系统，其特征在于，包括：权利要求 21-28 中任一项所述的通信装置和权利要求 41 所述的通信装置。

46、一种通信系统，其特征在于，包括：权利要求 29-34 中任一项所述的通信装置和权利要求 42 所述的通信装置。

47、一种通信系统，其特征在于，包括：权利要求 35-38 中任一项所述的通信装置和权利要求 43 所述的通信装置。

48、一种通信系统，其特征在于，包括：权利要求 39-40 中任一项所述的通信装置和权利要求 44 所述的通信装置。

49、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质具有程序指令，

当所述程序指令被直接或者间接执行时，使得如权利要求 1-7，权利要求 8-15，权利要求 9-14，权利要求 15-18，和/或权利要求 19-20 中任一所述的方法被实现。

50、一种芯片系统，其特征在于，所述芯片系统包括至少一个处理器，所述处理器用于执行存储器中存储的计算机程序或指令，当所述计算机程序或所述指令在所述至少一个
5 处理器中执行时，使得如权利要求 1-7，权利要求 8-15，权利要求 9-14，权利要求 15-18，和/或权利要求 19-20 中任一所述的方法被实现。

51、一种计算机程序产品，其特征在于，包括指令，当所述指令在计算机上运行时，使得计算机执行权利要求 1-7，权利要求 8-15，权利要求 9-14，权利要求 15-18，和/或权利要求 19-20 中任一项所述的方法。

10