

认证方法、装置、介质和芯片

技术领域

本公开涉及通信技术领域，具体地，涉及一种认证方法、装置、介质和芯片。

背景技术

在无线通信系统中，3GPP（3rd Generation Partnership Project，第三代合作伙伴项目）定义了用户设备（User Equipment，UE）与应用功能之间的会话安全保护功能，并且提出了基于应用的密钥管理方法，简称为 AKMA（Authentication and Key Management for Applications based on 3GPP credentials，基于 3GPP 凭证的应用认证和密钥管理）。

在相关技术中，用户设备可以基于 AKMA 与应用功能 AF（Application Function）实体进行消息交互，确定该用户设备对该应用功能 AF 实体的访问权限，以便与应用功能 AF 实体建立安全会话，这会增加应用功能 AF 实体的负荷，降低 AF 实体的效率。

发明内容

为克服相关技术中存在的上述问题，本公开提供一种认证方法、装置、介质和芯片。

根据本公开实施例的第一方面，提供一种认证方法，应用于用户设备，所述方法包括：

从一个或多个第一实体中，确定请求通信的目标实体；

根据所述目标实体确定第一权限请求参数；

根据所述第一权限请求参数向第一代理实体发送应用会话建立请求消息；所述应用会话建立请求消息用于指示所述第一代理实体根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

响应于接收到所述第一代理实体发送的应用会话建立响应消息，确定所述用户设备与所述目标实体是否具有第一通信权限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，通过所述第一代理实体进行身份认证。

根据本公开实施例的第二方面，提供一种认证方法，应用于第一代理实体，所述方法包括：

接收用户设备发送的应用会话建立请求消息；所述应用会话建立请求消息包括第一权限请求参数，所述应用会话建立请求消息用于指示所述第一代理实体根据第一权限请求参数确定所述用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，向用户设备发送应用会话建立响应消息，以及，对所述用户设备进行身份认证。

根据本公开实施例的第三方面，提供一种认证方法，应用于第三实体，所述方法包括：

接收第一代理实体发送的第二权限请求参数；所述第二权限请求参数用于指示第三实

体确定用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能，所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；

根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，获取第一待认证密钥信息；将所述第一待认证密钥信息发送至所述第一代理实体。

根据本公开实施例的第四方面，提供一种认证方法，应用于一个或多个第一实体中的目标实体，所述方法包括：

获取第一代理实体对用户设备的认证结果，所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示所述用户设备与所述目标实体具有第一通信权限；所述第二认证结果用于指示所述用户设备与所述目标实体具有第二通信权限；所述第一实体包括提供应用功能的实体，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

根据所述认证结果与用户设备进行通信。

根据本公开实施例的第五方面，提供一种认证方法，应用于第二实体，所述方法包括：

获取第一代理实体对用户设备的认证结果；所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示用户设备与目标实体具有第一通信权限；所述第二认证结果用于指示用户设备与目标实体具有第二通信权限；所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

将所述认证结果发送至所述目标实体，以便所述目标实体根据所述认证结果与用户设备进行通信。

根据本公开实施例的第六方面，提供一种认证装置，应用于用户设备，所述装置包括：

目标实体确定模块，被配置为从一个或多个第一实体中，确定请求通信的目标实体；

参数确定模块，被配置为根据所述目标实体确定第一权限请求参数；

第一消息发送模块，被配置为根据所述第一权限请求参数向第一代理实体发送应用会话建立请求消息；所述应用会话建立请求消息用于指示所述第一代理实体根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第一消息接收模块，被配置为响应于接收到所述第一代理实体发送的应用会话建立响应消息，确定所述用户设备与所述目标实体是否具有第一通信权限；

认证模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，通过所述第一代理实体进行身份认证。

根据本公开实施例的第七方面，提供一种认证装置，应用于第一代理实体，所述装置包括：

第一代理接收模块，被配置为接收用户设备发送的应用会话建立请求消息；所述应用会话建立请求消息包括第一权限请求参数，所述应用会话建立请求消息用于指示所述第一代理实体根据第一权限请求参数确定所述用户设备与目标实体是否具有第一通信权限，所

述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第一代理确定模块，被配置为根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；

第一代理发送模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，向用户设备发送应用会话建立响应消息，以及，对所述用户设备进行身份认证。

根据本公开实施例的第八方面，提供一种认证装置，应用于第三实体，所述装置包括：

第三接收模块，被配置为接收第一代理实体发送的第二权限请求参数；所述第二权限请求参数用于指示第三实体确定用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能，所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；

第三确定模块，被配置为根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限；

第三密钥模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，获取第一待定密钥信息；

第三发送模块，被配置为将所述第一待定密钥信息发送至所述第一代理实体。

根据本公开实施例的第九方面，提供一种认证装置，应用于一个或多个第一实体中的目标实体，所述装置包括：

第一通信模块，被配置为获取第一代理实体对用户设备的认证结果，所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示所述用户设备与所述目标实体具有第一通信权限；所述第二认证结果用于指示所述用户设备与所述目标实体具有第二通信权限；所述第一实体包括提供应用功能的实体，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；根据所述认证结果与用户设备进行通信。

根据本公开实施例的第十方面，提供一种认证装置，应用于第二实体，所述装置包括：

第二接收模块，被配置为获取第一代理实体对用户设备的认证结果；所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示用户设备与目标实体具有第一通信权限；所述第二认证结果用于指示用户设备与目标实体具有第二通信权限；所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第二发送模块，被配置为将所述认证结果发送至所述目标实体，以便所述目标实体根据所述认证结果与用户设备进行通信。

根据本公开实施例的第十一方面，提供一种认证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行本公开第一方面所提供的认证方法的步骤。

根据本公开实施例的第十二方面，提供一种认证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行本公开第二方面所提供的认证方法的步骤。

根据本公开实施例的第十三方面，提供一种认证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行本公开第三方面所提供的认证方法的步骤。

根据本公开实施例的第十四方面，提供一种认证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行本公开第四方面所提供的认证方法的步骤。

根据本公开实施例的第十五方面，提供一种认证装置，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行本公开第五方面所提供的认证方法的步骤。

根据本公开实施例的第十六方面，提供一种计算机可读存储介质，其上存储有计算机程序指令，该计算机程序指令被处理器执行时实现本公开第一方面所提供的认证方法的步骤。

根据本公开实施例的第十七方面，提供一种计算机可读存储介质，其上存储有计算机程序指令，该计算机程序指令被处理器执行时实现本公开第二方面所提供的认证方法的步骤。

根据本公开实施例的第十八方面，提供一种计算机可读存储介质，其上存储有计算机程序指令，该计算机程序指令被处理器执行时实现本公开第三方面所提供的认证方法的步骤。

根据本公开实施例的第十九方面，提供一种计算机可读存储介质，其上存储有计算机程序指令，该计算机程序指令被处理器执行时实现本公开第四方面所提供的认证方法的步骤。

根据本公开实施例的第二十方面，提供一种计算机可读存储介质，其上存储有计算机程序指令，该计算机程序指令被处理器执行时实现本公开第五方面所提供的认证方法的步骤。

根据本公开实施例的第二十一方面，提供一种芯片，包括：处理器和接口；所述处理器用于读取指令以执行本公开第一方面所提供的认证方法的步骤。

根据本公开实施例的第二十二方面，提供一种芯片，包括：处理器和接口；所述处理器用于读取指令以执行本公开第二方面所提供的认证方法的步骤。

根据本公开实施例的第二十三方面，提供一种芯片，包括：处理器和接口；所述处理器用于读取指令以执行本公开第三方面所提供的认证方法的步骤。

根据本公开实施例的第二十四方面，提供一种芯片，包括：处理器和接口；所述处理器用于读取指令以执行本公开第四方面所提供的认证方法的步骤。

根据本公开实施例的第二十五方面，提供一种芯片，包括：处理器和接口；所述处理器用于读取指令以执行本公开第五方面所提供的认证方法的步骤。

本公开的实施例提供的技术方案可以包括以下有益效果：从一个或多个第一实体中，确定请求通信的目标实体；根据该目标实体确定第一权限请求参数；根据该第一权限请求参数向第一代理实体发送应用会话建立请求消息；响应于接收到第一代理实体发送的应用会话建立响应消息，确定用户设备与目标实体是否具有第一通信权限；在用户设备与目标实体具有第一通信权限的情况下，通过第一代理实体进行身份认证。其中，该应用会话建

立请求消息用于指示第一代理实体根据第一权限请求参数确定用户设备与目标实体是否具有第一通信权限；该第一实体可以包括提供应用功能的实体，该第一代理实体可以包括 3GPP 运营商域内的可信的提供认证功能的实体，该第一代理实体为该第一实体提供认证代理功能。这样，通过 3GPP 运营商域内的可信的第一代理实体可以确定用户设备与第一实体是否具有第一通信权限，并在具有第一通信权限的情况下进行用户设备的身份验证，可以将第一实体的一部分功能通过第一代理实体实现，从而降低第一实体的负荷，提高第一实体的效率，并且，用户设备通过统一的第一代理实体实现与一个或多个第一实体的权限认证与身份认证，也降低了用户设备进行认证的复杂度，提高了用户设备的效率。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

图 1 是根据一示例性实施例示出的一种本公开实施例适用的通信系统的示意图。

图 2 是根据一示例性实施例示出的另一种本公开实施例适用的通信系统的示意图。

图 3 是根据一示例性实施例示出的一种认证方法的流程图。

图 4 是根据一示例性实施例示出的一种认证方法的流程图。

图 5 是根据一示例性实施例示出的一种认证方法的流程图。

图 6 是根据一示例性实施例示出的一种认证方法的流程图。

图 7 是根据一示例性实施例示出的一种认证方法的流程图。

图 8 是根据一示例性实施例示出的一种认证方法的流程图。

图 9 是根据一示例性实施例示出的一种认证方法的流程图。

图 10 是根据一示例性实施例示出的一种认证方法的流程图。

图 11 是根据一示例性实施例示出的一种认证方法的流程图。

图 12 是根据一示例性实施例示出的一种认证方法的流程图。

图 13 是根据一示例性实施例示出的一种认证装置的框图。

图 14 是根据一示例性实施例示出的一种认证装置的框图。

图 15 是根据一示例性实施例示出的一种认证装置的框图。

图 16 是根据一示例性实施例示出的一种认证装置的框图。

图 17 是根据一示例性实施例示出的一种认证装置的框图。

图 18 是根据一示例性实施例示出的一种认证装置的框图。

图 19 是根据一示例性实施例示出的一种认证装置的框图。

图 20 是根据一示例性实施例示出的一种认证装置的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

需要说明的是，本公开中所有获取信号、信息或数据的动作都是在遵照所在地国家相应的数据保护法规政策的前提下，并获得由相应装置所有者给予授权的情况下进行的。

在本公开中，使用的术语如“第一”、“第二”等是用于区别类似的对象，而不必理

解为特定的顺序或先后次序。另外，在未作相反说明的情况下，在参考附图的描述中，不同附图中的同一标记表示相同的要素。

在本公开的描述中，除非另有说明，“多个”是指两个或两个以上，其它量词与之类似；“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；“和/或”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，其中A，B可以是单数或者复数。

在本公开实施例中尽管在附图中以特定的顺序描述操作，但是不应将其理解为要求按照所示的特定顺序或是串行顺序来执行这些操作，或是要求执行全部所示的操作以得到期望的结果。在特定环境中，多任务和并行处理可能是有利的。

在相关技术中，用户设备可以基于AKMA与应用功能AF（Application Function）实体进行消息交互，确定该用户设备对该应用功能AF实体的访问权限，以便与应用功能AF实体建立安全会话。但是，由于多个用户设备引起的消息交互会增加应用功能AF实体的负荷，降低应用功能AF实体的效率，并且，在网络中存在多个应用功能AF实体的情况下，UE直接与AF进行消息交互以确定访问权限，对于UE来讲，也会降低效率。

为了解决上述问题，本公开提供了一种认证方法、装置、介质和芯片。

下面首先介绍本公开实施例的实施环境。

本公开的实施例可以应用于4G（the 4th Generation，第四代）网络系统，例如长期演进(Long Term Evolution，LTE)系统，或者，也可以应用于在5G（the 5th Generation，第五代）网络系统，如采用新型无线接入技术(New Radio Access Technology, New RAT)的接入网；云无线接入网(Cloud Radio Access Network, CRAN)等通信系统。

图1是根据一示例性实施例示出的一种本公开实施例适用的通信系统的示意图，需要说明的是，本公开实施例并不限于图1所示的系统中，此外，图1中的实体可以是硬件，也可以是从功能上划分的软件或者以上二者结合后的结构。图1中所示的实体可以是任意通信网络架构中的实体，该通信网络可以是4G网络、5G网络或6G网络等。

如图1所示，该通信系统可以包括：第一实体101、第三实体103、第一代理实体110和用户设备160，其中，第一实体101可以为一个或多个，例如，该第一实体101可以包括：第一实体1011、第一实体1012、……、第一实体101n等。第一代理实体110可以与该一个或多个第一实体101相连接（例如，通过有线网络、无线网络或二者的结合相连接），该第一代理实体可以与第三实体相连接，该用户设备可以与第一代理实体和第三实体相连接。

在一些实施例中，该第一实体101可以包括3GPP运营商域内的可信的提供应用功能的实体，该第一代理实体110可以包括3GPP运营商域内的可信的提供认证代理功能的实体，该第三实体103可以包括提供AKMA授权及应用密钥推演功能的实体，例如该第三实体103可以是提供AKMA锚点功能并对用户设备与第一实体的通信权限进行认证的功能实体。

示例地，第一实体可以包括：应用功能AF（Application Function）实体或应用服务器SCS/AS（Services Capability Server/Application Server）；第一代理实体可以包括认证代理AP（AKMA Authentication Proxy）实体；第三实体可以包括：AKMA锚点功能AAnF（AKMA Anchor Function）实体。

在一些实施例中，第一实体可以包括3GPP运营商域内的可信的提供应用功能的实体，第一代理实体可以包括3GPP运营商域内的可信的提供认证功能的实体，该第一代理实体为第一实体提供认证代理功能，该第一实体可以包括一个或多个。

图 2 是根据一示例性实施例示出的另一种本公开实施例适用的通信系统的示意图, 如图 2 所示, 该通信系统可以包括: 第一实体 101、第二实体 122、第三实体 103、第一代理实体 110 和用户设备 160, 其中, 第一实体 101 可以为一个或多个。第二实体 102 可以与该一个或多个第一实体 101 相连接(例如, 通过有线网络、无线网络或二者的结合相连接), 该第一代理实体可以与第二实体和第三实体相连接, 该用户设备可以与第一代理实体和第三实体相连接。

在图 2 中, 该第一实体 101 可以包括 3GPP 运营商域外的非可信的提供应用功能的实体, 例如, 应用功能 AF(Application Function)实体或应用服务器 SCS/AS(Services Capability Server/Application Server); 该第一代理实体 110 可以包括 3GPP 运营商域内的可信的提供认证代理功能的实体, 例如, 认证代理 AP(AKMA Authentication Proxy)实体; 该第三实体 103 可以包括提供 AKMA 授权及应用密钥推演功能的实体, 例如, AKMA 锚点功能 AAnF(AKMA Anchor Function)实体。该第二实体可以包括提供网络开放功能的实体, 例如, 网络开放功能 NEF(Network Exposure Function)实体或业务能力开放功能 SCEF(Service Capability Exposure Function)实体。

图 3 是根据一示例性实施例示出的一种认证方法, 可以应用于上述通信系统中的用户设备。如图 3 所示, 该方法可以包括:

S301、用户设备从一个或多个第一实体中, 确定请求通信的目标实体。

示例地, 该第一实体可以包括提供应用功能的实体, 例如应用功能 AF 实体。用户设备可以根据用户功能需求确定请求通信的 AF 实体。

S302、用户设备根据该目标实体确定第一权限请求参数。

在一些实施例中, 可以首先获取目标实体的第一目标实体标识, 根据该第一目标实体标识确定第一权限参数。

示例地, 该第一目标实体标识可以包括目标实体的 FQDN(Fully Qualified Domain Name, 全限定域名)、IP(Internet Protocol, 网际互连协议)地址和端口号(PortNumber)中的一项或多项。

在一些实施例中, 可以根据该第一目标实体标识和表征用户设备身份的用户设备标识, 获取该第一权限请求参数。

其中, 该用户设备标识可以包括用户设备对应的密钥标识 A-KID, 该密钥标识 A-KID 可以是用户设备在注册接入该通信系统时, 根据用户设备的硬件信息和通信系统发送的注册信息生成的, 该密钥标识 A-KID 可以在该通信系统中唯一标识一个用户设备。

示例地, 可以将该第一目标实体标识和该用户设备对应的密钥标识 A-KID, 作为该第一权限请求参数。

S303、用户设备根据该第一权限请求参数向第一代理实体发送应用会话建立请求消息。

其中, 该应用会话建立请求消息可以用于指示第一代理实体根据该第一权限请求参数确定用户设备与目标实体是否具有第一通信权限。

在一些实施例中, 第一代理实体与一个或多个第一实体相连接。示例地, 可以在一个信任域或一个边缘节点中设置统一的第一代理实体, 该第一代理实体可以与该信任域或该边缘节点中的每个第一实体相连接。在用户设备请求与该信任域或该边缘节点中的目标实体通信的情况下, 可以想该第一代理实体发送应用会话建立请求消息(例如 Application Session Establishment Request message)。

在一些实施例中, 第一实体可以包括提供应用功能的实体(例如, 可以是 3GPP 运营商域内的可信的提供应用功能的实体, 或者, 3GPP 运营商域外的非可信的提供应用功能的实体), 第一代理实体可以包括 3GPP 运营商域内的可信的提供认证功能的实体, 该第一代理实体为第一实体提供认证代理功能, 该第一实体可以包括一个或多个。

在一些实施例中，用户设备可以预先配置了第一代理实体的代理域名（例如 FQDN），通过该 FQDN，用户设备可以与第一代理实体进行消息交互或数据传输。

S304、用户设备响应于接收到第一代理实体发送的应用会话建立响应消息，确定用户设备与目标实体是否具有第一通信权限。

在一些实施例中，用户设备可以在接收到该应用会话建立响应消息的情况下，确定用户设备与目标实体具有第一通信权限。

反之，若用户设备在预设时间内未接收到该应用会话建立响应消息，则可以确定用户设备与目标实体不具有第一通信权限。

在另一些实施例中，用户设备可以在接收到应用会话建立响应消息，且该应用会话建立响应消息中包含成功指示信息的情况下，确定用户设备与目标实体具有第一通信权限。

反之，若用户设备接收到的该应用会话建立响应消息中未包含成功指示信息，或者包含失败指示信息，则可以确定用户设备与目标实体不具有第一通信权限。该成功指示信息可以是预先设置的任意指示信息。

在另外一些实施例中，用户设备可以在接收到应用会话建立响应消息，且该应用会话建立响应消息中不包含失败指示信息的情况下，确定用户设备与目标实体具有第一通信权限。

反之，若用户设备接收到的该应用会话建立响应消息中包含失败指示信息，则可以确定用户设备与目标实体不具有第一通信权限。该失败指示信息可以是预先设置的任意错误码。

S305、在用户设备与目标实体具有第一通信权限的情况下，用户设备通过第一代理实体进行身份认证。

示例地，用户设备可以根据目标实体的 FQDN 生成该目标实体对应的实体密钥 K_{AF} ，并根据该实体密钥 K_{AF} 与第一代理实体进行身份认证。

需要说明的是，用户设备进行身份认证的方式可以参考相关技术中的实现，例如可以根据目标实体对应的实体密钥信息进行身份认证，也可以根据用户设备对应的用户密钥信息和目标实体对应的实体密钥信息进行身份认证，本公开对此不作限定。

采用上述方法，从一个或多个第一实体中，确定请求通信的目标实体；根据该目标实体确定第一权限请求参数；根据该第一权限请求参数向第一代理实体发送应用会话建立请求消息；响应于接收到第一代理实体发送的应用会话建立响应消息，确定用户设备与目标实体是否具有第一通信权限；在用户设备与目标实体具有第一通信权限的情况下，通过第一代理实体进行身份认证。其中，该应用会话建立请求消息用于指示第一代理实体根据第一权限请求参数确定用户设备与目标实体是否具有第一通信权限；该第一实体可以包括提供应用功能的实体，该第一代理实体可以包括 3GPP 运营商域内的可信的提供认证功能的实体，该第一代理实体为该第一实体提供认证代理功能。这样，通过 3GPP 运营商域内的可信的第一代理实体可以确定用户设备与第一实体是否具有第一通信权限，并在具有第一通信权限的情况下进行用户设备的身份验证，可以将第一实体的一部分功能通过第一代理实体实现，从而降低第一实体的负荷，提高第一实体的效率，并且，用户设备通过统一的第一代理实体实现与一个或多个第一实体的权限认证与身份认证，也降低了用户设备进行认证的复杂度，提高了用户设备的效率。

在一些实施例中，上述第一通信权限可以包括以下一项或多项：

权限一、用户设备对目标实体具有访问权限。

权限二、用户设备对第一代理实体具有访问权限。

权限三、第一代理实体对目标实体具有代理权限。

权限四、目标实体对用户设备的用户标识具有获取权限。

示例地，可以在确定用户设备对目标实体具有访问权限的情况下，确定用户设备与目标实体具有第一通信权限；也可以在确定用户设备对第一代理实体具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第一通信权限；也可以在确定用户设备对目标实体具有访问权限、用户设备对第一代理实体具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第一通信权限。

在一些实施例中，用户设备与目标实体具有第一通信权限可以包括：用户设备对第一代理实体具有访问权限，且第一代理实体对目标实体具有代理权限；例如，在第一代理实体与目标实体的 FQDN 相同的情况下，可以使用该第一通信权限。

在另一些实施例中，用户设备与目标实体具有第一通信权限可以包括：用户设备对目标实体具有访问权限，和，用户设备对第一代理实体具有访问权限，和，第一代理实体对目标实体具有代理权限；例如，在第一代理实体与目标实体的 FQDN 不同的情况下，可以使用该第一通信权限。

在一些实施例中，上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体。

在一些实施例中，上述第一实体可以包括 3GPP 运营商域内的可信的提供应用功能的实体。示例地，该第一实体可以包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体。

在另一些实施例中，上述第一实体可以包括 3GPP 运营商域外的非可信的提供应用功能的实体，该第一代理实体可以通过第二实体与第一实体进行通信；该第二实体可以包括提供网络开放功能的实体。示例地，该第一实体可以包括：3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体；该第二实体包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

这样，用户设备可以通过 AP 与运营商域外的 AF 实体进行通信。

在一些实施例中，在通过第一代理实体进行身份认证成功之后，用户设备即可以与目标实体进行通信。

示例地，用户设备可以直接与目标实体通信，也可以通过第一代理实体与目标实体进行通信，例如通过第一代理实体转发用户设备与目标实体之间的通信消息。

在另一些实施例中，在通过第一代理实体进行身份认证成功之后，用户设备还可以确定第一代理实体的代理域名与目标实体的第一域名是否相同，在代理域名与第一域名不同的情况下，可以与目标实体进行通信。

反之，在代理域名与第一域名相同的情况下，可以通过用户设备与代理实体之间的安全会话进一步确定用户设备与目标实体是否具有第二通信权限；在具有第二通信权限的情况下，可以与目标实体进行通信。

需要说明的是，上述代理域名可以为该第一代理实体对应的全限定域名 FQDN，第一域名可以为该目标实体对应的全限定域名 FQDN。在某些场景下，第一代理实体与目标实体可以使用相同的 FQDN，而使用不同的 IP 地址或端口号，在该场景下，上述第一通信权限能够表征用户设备对该 FQDN 具有访问权限，但并不一定能够表征用户设备对 IP 地址或端口号对应的目标实体具有访问权限，此时，可以通过用户设备与代理实体之间的安全会话进一步确定用户设备与目标实体是否具有第二通信权限。

图 4 是根据一示例性实施例示出的一种认证方法，可以应用于用户设备。如图 4 所示，该方法可以包括：

S401、在用户设备与目标实体具有第一通信权限的情况下，用户设备通过第一代理实体进行身份认证。

S402、在通过第一代理实体进行身份认证成功之后，用户设备与第一代理实体建立安全会话。

示例地，该安全会话可以是 TLS（Transport Layer Security，传输层安全性）会话，通过 TLS 会话可以对用户设备与第一代理实体之间的通信实现保密性和数据完整性。

S403、用户设备获取第一代理实体的代理域名和目标实体的第一域名。

在一些实施例中，该代理域名可以为该第一代理实体对应的全限定域名 FQDN，该第一域名可以为该目标实体对应的全限定域名 FQDN。

S404、在代理域名与第一域名相同的情况下，用户设备通过安全会话确定用户设备与目标实体是否具有第二通信权限。

S405、在确定用户设备与目标实体具有第二通信权限的情况下，用户设备与目标实体进行通信。

同样地，用户设备可以直接与目标实体通信，也可以通过第一代理实体与目标实体进行通信，例如通过第一代理实体转发用户设备与目标实体之间的通信消息。

这样，通过对第一通信权限和第二通信权限的认证，在第一代理实体与目标实体的 FQDN 相同的情况下，也可以确定该用户设备对目标实体具有访问权限，从而进一步增强安全性。

在一些实施例中，上述 S404 步骤中通过安全会话确定用户设备与目标实体是否具有第二通信权限，可以包括以下步骤：

首先，用户设备通过上述安全会话，向第一代理实体发送目标实体服务请求消息。

示例地，该目标实体服务请求消息可以包括第二目标实体标识，该第二目标实体标识为用户设备根据第一目标实体标识获取的受保护的实体标识；该目标实体服务请求消息用于指示第一代理实体根据第二目标实体标识确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，上述第二目标实体标识为根据安全会话（例如 TLS 会话）的要求，对目标实体对应的第一目标实体标识进行保护后确定的标识。

在另一些实施例中，也可以直接将该第一目标实体标识作为该第二目标实体标识，将该第二目标实体标识通过安全会话进行传输，以实现对该第一目标实体标识的保护，以避免实体标识在传输过程中被篡改。

然后，用户设备响应于接收到第一代理实体发送的目标实体服务响应消息，确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，用户设备可以在接收到该目标实体服务响应消息的情况下，确定用户设备与目标实体具有第二通信权限。

反之，若用户设备在预设时间内未接收到该目标实体服务响应消息，则可以确定用户设备与目标实体不具有第二通信权限。

在另一些实施例中，用户设备可以在接收到目标实体服务响应消息，且该目标实体服务响应消息中包含成功指示信息的情况下，确定用户设备与目标实体具有第二通信权限。

反之，若用户设备接收到的该目标实体服务响应消息中未包含成功指示信息，或者包含失败指示信息，则可以确定用户设备与目标实体不具有第二通信权限。该成功指示信息可以是预先设置的任意指示信息。

在另外一些实施例中，用户设备可以在接收到目标实体服务响应消息，且该目标实体服务响应消息中不包含失败指示信息的情况下，确定用户设备与目标实体具有第二通信权限。

反之，若用户设备接收到的该目标实体服务响应消息中包含失败指示信息，则可以确定用户设备与目标实体不具有第二通信权限。该失败指示信息可以是预先设置的任意错误

码。该失败指示信息可以是预先设置的任意错误码。

这样，用户设备可以通过安全会话确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，上述第二通信权限可以包括以下权限中的一项或多项：

权限六、用户设备对目标实体具有访问权限。

权限七、第一代理实体对目标实体具有代理权限。

权限八、目标实体对用户设备的用户标识具有获取权限。

这样，可以通过用户设备与第一代理实体之间的安全会话，确定用户设备与目标实体是否具有第二通信权限，进一步提高认证的可靠性。

图 5 是根据一示例性实施例示出的一种认证方法，可以应用于上述通信系统中的第一代理实体。如图 5 所示，该方法可以包括：

S501、第一代理实体接收用户设备发送的应用会话建立请求消息。

其中，应用会话建立请求消息包括第一权限请求参数，应用会话建立请求消息用于指示第一代理实体根据第一权限请求参数确定用户设备与目标实体是否具有第一通信权限，目标实体为用户设备从一个或多个第一实体中确定的请求通信的实体，第一实体可以包括提供应用功能的实体，第一代理实体可以包括 3GPP 运营商域内的可信的提供认证功能的实体，该第一代理实体为第一实体提供认证代理功能，该第一实体可以包括一个或多个。

S502、第一代理实体根据第一权限请求参数确定用户设备与目标实体是否具有第一通信权限。

这样，通过 3GPP 运营商域内的可信的第一代理实体可以确定用户设备与第一实体是否具有第一通信权限，并在具有第一通信权限的情况下进行用户设备的身份验证，可以将第一实体的一部分功能通过第一代理实体实现，从而降低第一实体的负荷，提高第一实体的效率，并且，用户设备通过统一的第一代理实体实现与一个或多个第一实体的权限认证与身份认证，也降低了用户设备进行认证的复杂度，提高了用户设备的效率。

在一些实施例中，第一代理实体可以通过与第三实体的消息交互确定用户设备与目标实体是否具有第一通信权限。例如，可以包括以下步骤：

首先，第一代理实体根据第一权限请求参数确定第二权限请求参数。

在一些实施例中，可以将第一权限请求参数和第一代理实体对应的代理实体标识，作为第二权限请求参数。示例地，若第一权限请求参数包括目标实体的第一目标实体标识和用户设备对应的密钥标识 A-KID，则第二权限请求参数可以包括第一目标实体标识、密钥标识 A-KID 和第一代理实体对应的代理实体标识。

在另一些实施例中，可以将该第一权限请求参数作为第二权限请求参数。

其次，第一代理实体向第三实体发送第二权限请求参数。

示例地，该第三实体可以包括提供 AKMA 授权及应用密钥推演功能的实体。该第二权限请求参数可以用于指示第三实体确定用户设备与目标实体是否具有第一通信权限。

再次，第一代理实体获取第三实体发送的第一待定密钥信息。

该第一待定密钥信息为第三实体根据第二权限请求参数获取的密钥信息。

在一些实施例中，该第一待定密钥信息可以包括目标实体对应的应用密钥 K_{AF} 。

在另一些实施例中，该第一待定密钥信息可以包括目标实体对应的应用密钥 K_{AF} 和密钥有效时间 K_{AF} expiration time。

在一些实施例中，第一代理实体可以通过第一密钥请求消息，向第三实体发送第二权限请求参数；第一密钥请求消息用于指示第三实体获取第一待定密钥信息和用户设备的用户标识；第一代理实体还可以接收第三实体发送的第一密钥响应消息；并获取第一密钥响应消息中包含的第一待定密钥信息。

进一步地，第一密钥响应消息中还可以包括用户设备对应的第二用户标识，第一代理

实体可以根据接收到的第一密钥响应消息，获取第二用户标识。该第二用户标识可以包括用户设备对应的用户永久标识 SUPI (Subscription Permanent Identifier)。

在一些实施例中，第一代理实体可以通过第二密钥请求消息，向第三实体发送第二权限请求参数；第二密钥请求消息用于表征第一代理实体请求获取第一待定密钥信息；第一代理实体还可以接收第三实体发送的第二密钥响应消息；获取第二密钥响应消息中包含的第一待定密钥信息。最后，第一代理实体根据第一待定密钥信息，确定用户设备与目标实体是否具有第一通信权限。

示例地，在该第一待定密钥信息包括目标实体对应的应用密钥 K_{AF} 的情况下，可以确定用户设备与目标实体具有第一通信权限。反之，在该第一待定密钥信息不包括目标实体对应的应用密钥 K_{AF} ，或者，该第一待定密钥信息不包括有效的应用密钥 K_{AF} ，或者，在预设时间内未收到该第一待定密钥信息的情况下，可以确定用户设备与目标实体不具有第一通信权限。

这样，第一代理实体通过与第三实体进行交互，可以确定用户设备与目标实体是否具有第一通信权限。

在另一些实施例中，在该第一代理实体存储有用户设备通信权限策略的情况下，可以直接根据第一权限请求参数确定用户设备与目标实体是否具有第一通信权限。

S503、在用户设备与目标实体具有第一通信权限的情况下，第一代理实体向用户设备发送应用会话建立响应消息，以及，对用户设备进行身份认证。

在一些实施例中，第一代理实体可以通过发送该应用会话建立响应消息，指示用户设备与目标实体具有第一通信权限；反之，通过不发送该应用会话建立响应消息，指示用户设备与目标实体不具有第一通信权限。

在另一些实施例中，第一代理实体可以在该应用会话建立响应消息中包含成功指示信息，通过该成功指示信息，指示用户设备与目标实体具有第一通信权限；反之，通过在该应用会话建立响应消息中不包含成功指示信息，指示用户设备与目标实体不具有第一通信权限。其中该成功指示信息可以是预先设置的任意指示信息。

在另外一些实施例中，在用户设备与目标实体不具有第一通信权限的情况下，第一代理实体可以在该应用会话建立响应消息中包含失败指示信息，指示用户设备与目标实体不具有第一通信权限；反之，在用户设备与目标实体具有第一通信权限的情况下，第一代理实体可以通过在该应用会话建立响应消息中不包含失败指示信息，指示用户设备与目标实体具有第一通信权限。

采用上述方法，可以基于第一代理实体实现对用户设备与第一实体的通信权限的认证，从而可以减少第一实体进行权限认证引起的负荷过高的问题。

在一些实施例中，上述第一通信权限可以包括以下一项或多项：

权限一、用户设备对目标实体具有访问权限；

权限二、用户设备对第一代理实体具有访问权限；

权限三、第一代理实体对目标实体具有代理权限。

权限四、目标实体对用户设备的用户标识具有获取权限。

在一些实施例中，上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体。

在一些实施例中，上述第一实体可以包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体

在一些实施例中，上述第二实体可以包括：网络开放功能 NEF 实体或业务能力开放功

能 SCEF 实体。

在一些实施例中，上述第三实体可以包括：AKMA 锚点功能 AAnF 实体。

在一些实施例中，在第一代理实体对用户设备进行身份认证成功的情况下，第一代理实体可以将身份认证的第一认证结果通知目标实体。其中，该第一认证结果用于指示目标实体与用户设备具有通信权限。

例如，在目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，第一代理实体可以向目标实体发送第一通知消息，该第一通知消息可以包括第一认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第一密钥响应消息获取到第二用户标识），第一通知消息还可以包括第二用户标识。

再例如，在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，第一代理实体可以根据第一认证结果向第二实体发送第二通知消息，以指示第二实体向目标实体发送第一认证结果。同样地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第一密钥响应消息获取到第二用户标识），第二通知消息还可以包括第二用户标识。

进一步地，该认证结果通知消息还可以包括用户设备对应的第一用户标识，示例地，在第一密钥响应消息中包括用户设备对应的第一用户标识的情况下，第一代理实体可以通过认证结果通知消息，向目标实体发送第一用户标识。

需要说明的是，该第一用户标识可以是用于表征用户设备的任意标识，例如，可以为用户设备对应的通用公共用户标识 GPSI。

这样，第一代理实体可以对用户设备与第一实体的通信权限进行验证，在用户设备与第一实体具有通信权限的情况下，指示用户设备与第一实体进行通信。

在另一些实施例中，在第一代理实体对用户设备进行身份认证成功的情况下，第一代理实体可以获取第一代理实体的代理域名和目标实体的第一域名；在代理域名与第一域名不同的情况下，将第一认证结果通知目标实体，以便指示目标实体与用户设备具有通信权限或者进行通信。

反之，在代理域名与第一域名相同的情况下，第一代理实体则暂时不将第一认证结果通知目标实体；先等待用户设备与目标实体是否具有第二通信权限，在确定用户设备与目标实体具有第二通信权限后，再将第二认证结果通知目标实体。

示例地，第一代理实体可以根据用户设备发送的目标实体服务请求消息，进一步确定用户设备与目标实体是否具有第二通信权限。

同样需要说明的是，上述代理域名可以是该第一代理实体对应的全限定域名 FQDN，第一域名可以是该目标实体对应的全限定域名 FQDN。在某些场景下，第一代理实体与目标实体可以使用相同的 FQDN，而使用不同的 IP 地址或端口号，在该场景下，上述第一通信权限能够表征用户设备对该 FQDN 具有访问权限，但并不一定能够表征用户设备对 IP 地址或端口号对应的目标实体具有访问权限，此时，可以通过用户设备与代理实体之间的安全会话进一步确定用户设备与目标实体是否具有第二通信权限。

图 6 是根据一示例性实施例示出的一种认证方法，可以应用于第一代理实体。如图 6 所示，该方法可以包括：

S601、在对用户设备进行身份认证成功之后，第一代理实体与用户设备建立安全会话。

示例地，该安全会话可以是 TLS（Transport Layer Security，传输层安全性）会话，通过 TLS 会话可以对第一代理实体与用户设备之间的通信实现保密性和数据完整性。

S602、第一代理实体通过安全会话，接收用户设备发送的目标实体服务请求消息。

目标实体服务请求消息包括第二目标实体标识，第二目标实体标识为用户设备根据目标实体的第一目标实体标识获取的受保护的实体标识，目标实体服务请求消息为用户设备

在确定第一代理实体的代理域名与目标实体的第一域名相同的情况下发送的消息。

S603、第一代理实体根据第二目标实体标识确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，在第二目标实体标识与第一目标实体标识相同的情况下，可以确定用户设备与目标实体具有第二通信权限。

在另一些实施例中，在第二目标实体标识与第一目标实体标识不同的情况下，第一代理实体可以通过与第三实体的消息交互确定用户设备与目标实体是否具有第二通信权限。

S604、第一代理实体向用户设备发送目标实体服务响应消息。

该目标实体服务响应消息用于指示用户设备与目标实体是否具有第二通信权限。

在一些实施例中，第一代理实体可以通过发送该目标实体服务响应消息，指示用户设备与目标实体具有第二通信权限；反之，通过不发送该目标实体服务响应消息，指示用户设备与目标实体不具有第二通信权限。

在另一些实施例中，第一代理实体可以在该目标实体服务响应消息中包含成功指示信息，通过该成功指示信息，指示用户设备与目标实体具有第二通信权限；反之，通过在该目标实体服务响应消息中不包含成功指示信息，指示用户设备与目标实体不具有第二通信权限。其中该成功指示信息可以是预先设置的任意指示信息。

在另外一些实施例中，在用户设备与目标实体不具有第二通信权限的情况下，第一代理实体可以在该目标实体服务响应消息中包含失败指示信息，指示用户设备与目标实体不具有第二通信权限；反之，在用户设备与目标实体具有第二通信权限的情况下，第一代理实体可以通过在该目标实体服务响应消息中不包含失败指示信息，指示用户设备与目标实体具有第二通信权限。该失败指示信息可以是预先设置的任意错误码。

这样，第一代理实体可以通过安全会话确定用户设备与目标实体是否具有第二通信权限，并将权限认证结果发送至目标设备。

在另一些实施例中，第一代理实体可以通过与第三实体的消息交互确定用户设备与目标实体是否具有第二通信权限。

图 7 是根据一示例性实施例示出的一种认证方法，可以应用于第一代理实体。如图 7 所示，在第二目标实体标识与第一目标实体标识不同的情况下，该第一代理实体可以根据该方法确定用户设备与目标实体是否具有第二通信权限，该方法可以包括：

S701、第一代理实体根据第二目标实体标识确定第三权限请求参数。

S702、第一代理实体向第三实体发送第三权限请求参数。

S703、第一代理实体获取第三实体发送的授权结果参数。

S704、第一代理实体根据授权结果参数确定用户设备与目标实体是否具有第二通信权限。

通过该方法，在第二目标实体标识与第一目标实体标识不同的情况下，第一代理实体可以通过与第三实体的消息交互确定用户设备与目标实体是否具有第二通信权限。

其中，第三权限请求参数可以用于指示第三实体确定用户设备与目标实体是否具有第二通信权限；授权结果参数可以用于表征用户设备与目标实体是否具有第二通信权限。示例地，该第三权限请求参数可以包括密钥标识 A-KID、第二目标实体标识和第一代理实体对应的代理实体标识；该第三权限请求参数可以用于指示第三实体确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，第一代理实体可以通过第三密钥请求消息，向第三实体发送第三权限请求参数；第三密钥请求消息用于指示第三实体获取授权结果参数和用户设备的用户标识。第一代理实体还可以接收第三实体发送的第三密钥响应消息；获取第三密钥响应消息中包含的授权结果参数。

进一步地，第三密钥响应消息还包括用户设备对应的第二用户标识，第一代理实体还可以根据接收到的第三密钥响应消息，获取第二用户标识。该第二用户标识可以包括用户设备对应的用户永久标识 SUPI (Subscription Permanent Identifier)。

在一些实施例中，该第三密钥请求消息可以包括授权指示参数。该授权指示参数可以用于指示第三实体根据第三密钥请求消息确定用户设备与目标实体是否具有第二通信权限。同样地，该第三密钥响应消息也可以包括授权指示参数，用于表征该第三密钥响应消息是对该第三密钥请求消息的响应。

在另一些实施例中，第一代理实体可以通过第四密钥请求消息，向第三实体发送第三权限请求参数；第四密钥请求消息用于表征第一代理实体请求获取授权结果参数。第一代理实体还可以接收第三实体发送的第四密钥响应消息；获取第四密钥响应消息中包含的授权结果参数。

在一些实施例中，该第四密钥请求消息还包括授权指示参数，授权指示参数用于指示第三实体根据第四密钥请求消息确定用户设备与目标实体是否具有第二通信权限。同样地，该第四密钥响应消息也可以包括授权指示参数，用于表征该第四密钥响应消息是对该第四密钥请求消息的响应。

在一些实施例中，该授权结果参数可以用于指示授权成功或授权失败。第一代理实体根据该授权结果参数确定用户设备与目标实体是否具有第二通信权限。示例地，在该授权结果参数为授权成功的情况下，可以确定用户设备与目标实体具有第二通信权限；反之，在该授权结果参数为授权失败，或者，上述密钥响应消息（例如第三密钥响应消息或第四密钥响应消息）未包括授权结果参数的情况下，可以确定用户设备与目标实体不具有第二通信权限。

在一些实施例中，上述第二通信权限可以包括以下权限中的一项或多项：

权限六、用户设备对目标实体具有访问权限。

权限七、第一代理实体对目标实体具有代理权限。

权限八、目标实体对用户设备的用户标识具有获取权限。

这样，可以通过用户设备与第一代理实体之间的安全会话，确定用户设备与目标实体是否具有第二通信权限，进一步提高认证的可靠性。

在一些实施例中，在根据授权结果参数确定用户设备与目标实体具有第二通信权限的情况下，第一代理实体可以将第二认证结果通知目标实体。

其中，该第二认证结果用于指示目标实体与用户设备具有通信权限。

例如，在目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，第一代理实体可以向目标实体发送第三通知消息，第三通知消息包括第二认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第三密钥响应消息获取到第二用户标识），第三通知消息还可以包括第二用户标识。

再例如，在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，第一代理实体可以根据第一认证结果向第二实体发送第四通知消息，以指示第二实体向目标实体发送第一认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第三密钥响应消息获取到第二用户标识），第四通知消息还可以包括第二用户标识。

这样，第一代理实体可以通过安全会话对用户设备与第一实体的第二通信权限进行验证，进一步提高认证的可靠性，并在用户设备与第一实体具有第二通信权限的情况下，指示用户设备与第一实体进行通信。

图 8 是根据一示例性实施例示出的一种认证方法，可以应用于第三实体。如图 8 所示，该方法可以包括：

S801、第三实体接收第一代理实体发送的第二权限请求参数。

其中，第二权限请求参数用于指示第三实体确定用户设备与目标实体是否具有第一通信权限，目标实体为用户设备从一个或多个第一实体中确定的请求通信的实体，第一实体包括提供应用功能的实体，第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，第一代理实体为第一实体提供认证代理功能，第三实体包括提供 AKMA 授权及应用密钥推演功能的实体。

S802、第三实体根据第二权限请求参数，确定用户设备与目标实体是否具有第一通信权限。

在一些实施例中，该第二权限请求参数可以包括第一代理实体对应的代理实体标识。第三实体接收到第二权限请求参数后，可以根据第一预设策略确定第三实体是否具有为第一代理实体服务的权限。该第一预设策略可以包括预先配置的参数。

在确定第三实体具有为第一代理实体服务的权限的情况下，根据该第二权限请求参数，确定用户设备与目标实体是否具有第一通信权限。

反之，在确定第三实体不具有为第一代理实体服务的权限的情况下，可以终止流程，不再检查不再用户设备与目标实体是否具有第一通信权限。此时，第三实体可以向第一代理实体发送失败指示，以便第一代理实体进行相应的失败处理；或者，第三实体也直接停止处理，不发送任何消息。

在一些实施例中，第二权限请求参数包括用户设备对应的密钥标识 A-KID、目标实体的第一目标实体标识和第一代理实体对应的代理实体标识。在本步骤中，确定用户设备与目标实体是否具有第一通信权限的方式包括以下一项或多项：

方式一、根据密钥标识 A-KID 和第一目标实体标识，确定用户设备对目标实体是否具有访问权限。

方式二、根据密钥标识 A-KID 和代理实体标识，确定用户设备对第一代理实体是否具有访问权限。

方式三、根据代理实体标识和第一目标实体标识，确定第一代理实体对目标实体是否具有代理权限。

方式四、根据密钥标识 A-KID 和第一目标实体标识，确定目标实体对用户设备的用户标识是否具有获取权限。

方式五、根据密钥标识 A-KID 确定用户设备是否具有使用 AKMA 的权限。

在一些实施例中，第三实体可以在确定用户设备对第一代理实体和目标实体均具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第一通信权限。

在另一些实施例中，第三实体可以在确定用户设备对目标实体均具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第一通信权限。

S803、第三实体在用户设备与目标实体具有第一通信权限的情况下，获取第一待定密钥信息。

示例地，可以根据目标实体对应的实体密钥信息，获取第一待定密钥信息。

在一些实施例中，该目标实体对应的实体密钥信息中可以包括目标实体对应的应用密钥 K_{AF} 。

在另一些实施例中，该目标实体对应的实体密钥信息中可以包括目标实体对应的应用密钥 K_{AF} 和密钥有效时间 K_{AF} expiration time。

S804、第三实体将第一待定密钥信息发送至第一代理实体。

以便第一代理实体根据第一待定密钥信息确定用户设备与目标实体是否具有第一通

信权限。

在一些实施例中，第三实体可以通过第一密钥请求消息，接收第一代理实体发送的第二权限请求参数；第一密钥请求消息用于指示第三实体获取第一待密钥信息和用户设备的用户标识。第三实体还可以通过第一密钥响应消息，向第一代理实体发送第一待密钥信息。

进一步地，第三实体还可以在确定所述目标实体具有获取用户标识的权限的情况下，通过第一密钥响应消息，向所述第一代理实体发送第一待密钥信息和用户设备对应的第二用户标识。

示例地，第三实体在确定目标实体具有获取用户标识的权限的情况下，通过第三密钥响应消息，向所述第一代理实体发送第一待密钥信息和用户设备对应的第二用户标识。例如，获取用户设备对应的第二用户标识，并将该第二用户标识和授权结果参数，通过第三密钥响应消息发送给至第一代理实体。

在一些实施例中，该第二用户标识可以是在 3GPP 运营商域内表征该用户设备的标识；示例地，该第二用户标识可以是用户设备对应的用户永久标识 SUPI。

在另一些实施例中，第三实体可以通过第二密钥请求消息，接收第一代理实体发送的第二权限请求参数；第二密钥请求消息用于指示第三实体获取第一待密钥信息。第三实体还可以通过第二密钥响应消息，向第一代理实体发送第一待密钥信息。

这样，第三实体可以确定用户设备与目标实体是否具有第一通信权限，并通过第一待密钥信息通知第一代理实体。

在一些实施例中，上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体。

在一些实施例中，上述第一实体可以包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

在一些实施例中，上述第三实体可以包括：AKMA 锚点功能 AAnF 实体。

图 9 是根据一示例性实施例示出的一种认证方法，可以应用于第三实体。如图 9 所示，在向第二实体发送第三密钥响应消息之后，该方法还可以包括：

S901、第三实体接收第一代理实体发送的第三权限请求参数。

S902、第三实体根据第三权限请求参数确定用户设备与目标实体是否具有第二通信权限。

S903、第三实体向第一代理实体发送授权结果参数。

其中，该授权结果参数可以用于通知第一代理实体用户设备与目标实体是否具有第二通信权限。

在一些实施例中，第三权限请求参数可以包括第一代理实体对应的代理实体标识。第三实体接收到第四密钥请求消息后，可以根据第一预设策略确定第三实体是否具有为第一代理实体服务的权限。该第一预设策略可以包括预先配置的参数。

在确定第三实体具有为第一代理实体服务的权限的情况下，根据第四密钥请求消息，确定用户设备与目标实体是否具有第二通信权限。

反之，在确定第三实体不具有为第一代理实体服务的权限的情况下，可以终止流程，不再检查不再用户设备与目标实体是否具有第一通信权限。此时，第三实体可以向第二实体发送失败指示，以便第二实体进行相应的失败处理；或者，第三实体也直接停止处理，不发送任何消息。

在一些实施例中，第三权限请求参数可以包括密钥标识 A-KID、第二目标实体标识和

第一代理实体对应的代理实体标识，第二目标实体标识为用户设备根据目标实体的第一目标实体标识获取的受保护的实体标识；上述 S902 步骤确定用户设备与目标实体是否具有第二通信权限的方式可以包括以下一项或多项：

方式六、根据密钥标识 A-KID 和第二目标实体标识，确定用户设备对目标实体是否具有访问权限。

方式七、根据代理实体标识和第二目标实体标识，确定第一代理实体对目标实体是否具有代理权限。

方式八、根据密钥标识 A-KID 和第一目标实体标识，确定目标实体对用户设备的用户标识是否具有获取权限。

在一些实施例中，第三实体可以在确定用户设备对目标实体具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第二通信权限。

在一些实施例中，第三实体可以通过第三密钥请求消息，接收第一代理实体发送的第三权限请求参数；第三密钥请求消息用于指示第三实体获取授权结果参数和用户设备的用户标识。第三实体还可以通过第三密钥响应消息，向第一代理实体发送授权结果参数。

进一步地，第三密钥请求消息可以包括授权指示参数，授权指示参数用于指示第三实体根据第三密钥请求消息确定用户设备与目标实体是否具有第二通信权限。同样地，第三密钥响应消息中也可以包括授权指示参数。

进一步地，第三实体还可以在确定所述目标实体具有获取用户标识的权限的情况下，通过第三密钥响应消息，向所述第一代理实体发送授权结果参数和所述用户设备对应的第二用户标识。

示例地，第三实体在确定目标实体具有获取用户标识的权限的情况下，通过第三密钥响应消息，向所述第一代理实体发送授权结果参数和所述用户设备对应的第二用户标识。例如，获取用户设备对应的第二用户标识，并将该第二用户标识和授权结果参数，通过第三密钥响应消息发送给至第一代理实体。

示例地，该第二用户标识可以包括用户设备对应的用户永久标识 SUPI。

在另一些实施例中，第三实体可以通过第四密钥请求消息，接收第一代理实体发送的第三权限请求参数；第四密钥请求消息用于指示第三实体获取授权结果参数。第三实体还可以通过第四密钥响应消息，向第一代理实体发送授权结果参数。

进一步地，第四密钥请求消息还可以包括授权指示参数，授权指示参数用于指示第三实体根据第三密钥请求消息确定用户设备与目标实体是否具有第二通信权限。同样地，该第四密钥响应消息也可以包括授权指示参数，用于表征该第四密钥响应消息是对该第四密钥请求消息的响应。

在一些实施例中，该授权结果参数可以用于指示授权成功或授权失败。示例地，第三实体可以根据用户设备与目标实体是否具有第二通信权限，确定该授权结果参数的取值。例如，第三实体在确定用户设备与目标实体具有第二通信权限的情况下，可以将该授权结果参数设置为授权成功（例如 1）；在确定用户设备与目标实体不具有第二通信权限的情况下，可以将该授权结果参数的取值设置为授权失败（例如 0）。

在另一些实施例中，第三实体可以通过在上述密钥响应消息（例如第三密钥响应消息或第四密钥响应消息）不包含该授权结果信息以指示用户设备与目标实体不具有第二通信权限。例如，在第三实体确定用户设备与目标实体不具有第二通信权限的情况下，可以在上述密钥响应消息中不包含该授权结果信息；反之，在确定用户设备与目标实体具有第二通信权限的情况下，可以在上述密钥响应消息中包含该授权结果信息。

图 10 是根据一示例性实施例示出的一种认证方法，可以应用于第一实体。如图 10 所示，该方法还可以包括：

S1001、第一实体获取第一代理实体对用户设备的认证结果。

S1002、第一实体根据认证结果与用户设备进行通信。

其中，认证结果包括第一认证结果或第二认证结果，第一认证结果用于指示用户设备与目标实体具有第一通信权限；第二认证结果用于指示用户设备与目标实体具有第二通信权限；目标实体为用户设备从一个或多个第一实体中确定的请求通信的实体，第一实体包括提供应用功能的实体，第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，第一代理实体为第一实体提供认证代理功能。

需要说明的是，第一实体可以等待用户设备发起通信；第一实体也可以主动与用户设备发起通信，本公开对此不作限定。

在一些实施例中，认证结果通知消息包括用户设备的第一用户标识。该第一用户标识可以是 3GPP 运营商域外表征该用户设备的标识。示例地，该第一用户标识为该用户设备对应的通用公共用户标识 GPSI。

在目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，目标实体可以接收第一代理实体发送的第一通知消息，第一通知消息包括第一认证结果；或者，接收第一代理实体发送的第三通知消息，第三通知消息包括第二认证结果。

进一步地，第一通知消息或第三通知消息中还包括用户设备对应的第二用户标识。第二用户标识包括可以用用户设备对应的用户永久标识 SUPI。

在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，目标实体可以接收第二实体发送的第五通知消息；其中，第五通知消息包括第一认证结果，第五通知消息为第二实体响应于接收到第二通知消息后发送的消息；或者，接收第二实体发送的第六通知消息；其中，第六通知消息包括第二认证结果，第五通知消息为第二实体响应于接收到第四通知消息后发送的消息。

进一步地，第五通知消息或第六通知消息中还包括用户设备的第一用户标识。第一用户标识可以为用户设备对应的通用公共用户标识 GPSI。

在一些实施例中，上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体。

在一些实施例中，上述第一实体可以包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

在一些实施例中，上述第二实体可以包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

这样，第一实体可以根据第一代理实体的认证结果通知消息，确定用户设备与第一实体是否具有第一通信权限，从而可以降低第一实体的负荷，提高第一实体的效率。

图 11 是根据一示例性实施例示出的一种认证方法，可以应用于第二实体。如图 11 所示，该方法可以包括：

S1101、第二实体获取第一代理实体对用户设备的认证结果。

认证结果包括第一认证结果或第二认证结果，第一认证结果用于指示用户设备与目标实体具有第一通信权限；第二认证结果用于指示用户设备与目标实体具有第二通信权限；目标实体为用户设备从一个或多个第一实体中确定的请求通信的实体，第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，第一代理实体为第一实体提供认证代理功能。

S1102、第二实体将认证结果发送至目标实体。

以便目标实体根据认证结果与用户设备进行通信。

采用上述方法，可以通过第二实体实现 3GPP 运营商域内的第一代理实体与 3GPP 运营商域外的第一实体之间的通信。

在一些实施例中，上述第二实体可以包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体；上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体；上述第一实体可以包括：3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

在一些实施例中，第二实体可以接收第一代理实体发送的第二通知消息；根据第二通知消息获取第一认证结果；根据第一认证结果向第一实体发送第五通知消息。其中，第二通知消息为第一代理实体在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，根据第一认证结果向第二实体发送的消息。

进一步地，在第二通知消息中包括用户设备对应的第二用户标识的情况下，第二实体可以根据第二用户标识获取用户设备对应的第一用户标识；根据第一认证结果和第一用户标识，向第一实体发送第五通知消息。

在另一些实施例中，第二实体可以接收第一代理实体发送的第四通知消息；根据第二通知消息获取第二认证结果；根据第二认证结果向第一实体发送第六通知消息。其中，第四通知消息为第一代理实体在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，根据第二认证结果向第二实体发送的消息。

进一步地，在第四通知消息中包括用户设备对应的第二用户标识的情况下，第二实体可以根据第二用户标识获取用户设备对应的第一用户标识；根据第二认证结果和第一用户标识，向第一实体发送第六通知消息。

在一些实施例中，该第二用户标识可以是在 3GPP 运营商域内表征该用户设备的标识；该第一用户标识可以是 3GPP 运营商域外表征该用户设备的标识。示例地，该第二用户标识可以是用户设备对应的用户永久标识 SUPI（Subscription Permanent Identifier）；该第一用户标识可以是用户设备对应的通用公共用户标识 GPSI（Generic Public Subscription Identifier）。

第二实体可以根据预设标识对应关系，确定第二用户标识对应的第一用户标识；该预设标识对应关系包括第二用户标识与第一用户标识的对应关系。

图 12 是根据一示例性实施例示出的一种认证方法，如图 12 所示，该方法可以包括：S1201、用户设备向第一代理实体发送应用会话建立请求消息。

示例地，该应用会话建立请求消息可以包括第一权限请求参数，该第一权限请求参数可以包括用户设备的密钥标识 A-KID 和目标实体的第一目标实体标识 Target AF ID。该目标实体可以是用户设备从一个或多个第一实体中确定的请求通信的实体。

在一些实施例中，用户设备可以通过通信系统中的预设功能实体获取密钥标识 A-KID，该预设功能实体可以包括鉴权服务功能 AUSF（Authentication Server Function）实体

S1202、第一代理实体响应于接收到该应用会话建立请求消息，向第三实体发送第二权限请求参数。

在一些实施例中，第一代理实体可以接收用户设备发送的应用会话建立请求消息，根据该应用会话建立请求消息中的第一权限请求参数确定第二权限请求参数。

示例地，在第一权限请求参数包括用户设备的密钥标识 A-KID 和目标实体的第一目标实体标识 Target AF ID 的情况下，可以确定第二权限请求参数包括密钥标识 A-KID、第一目标实体标识 Target AF ID 和该第一代理实体的代理实体标识。

在一些实施例中，第一代理实体可以通过第一密钥请求消息，向第三实体发送第二权限请求参数；第一密钥请求消息用于指示第三实体获取第一待认证密钥信息和用户设备的用户标识。示例地，该第一密钥请求消息可以为 Naanf_AKMA_ApplicationKey_Get

Requestmessage。

在另一些实施例中，第一代理实体可以通过第二密钥请求消息，向第三实体发送第二权限请求参数；第二密钥请求消息用于表征第一代理实体请求获取第一待定密钥信息。示例地，该第二密钥请求消息可以为 Naanf_AKMA_ApplicationKey_AnonUser_Get Request message。

S1203、第三实体在根据第二权限请求参数确定用户设备与目标实体具有第一通信权限的情况下，获取第一待定密钥信息。

其中，该第三实体可以基于预设权限策略对用户设备和目标实体的通信权限进行认证，以确定用户设备与目标实体是否具有第一通信权限，示例地：

在一些实施例中，第三实体确定用户设备与目标实体是否具有第一通信权限的方式可以包括以下一项或多项：

方式一、根据密钥标识 A-KID 和第一目标实体标识，确定用户设备对目标实体是否具有访问权限。

方式二、根据密钥标识 A-KID 和代理实体标识，确定用户设备对第一代理实体是否具有访问权限。

方式三、根据代理实体标识和第一目标实体标识，确定第一代理实体对目标实体是否具有代理权限。

方式四、根据密钥标识 A-KID 和第一目标实体标识，确定目标实体对用户设备的用户标识是否具有获取权限。

方式五、根据密钥标识 A-KID 确定用户设备是否具有使用 AKMA 的权限。

在另一些实施例中，第三实体可以在确定用户设备对目标实体均具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第一通信权限。示例地，第三实体可以通过以下步骤确定用户设备与目标实体是否具有第一通信权限：

S11、根据代理实体标识和第一目标实体标识，确定第一代理实体对目标实体是否具有代理权限。

若确定第一代理实体对目标实体不具有代理权限，则直接确定用户设备与目标实体不具有第一通信权限，不再执行 S12 步骤。反之，若确定第一代理实体对目标实体具有代理权限，则继续执行是 S12 步骤。

S12、根据密钥标识 A-KID 和第一目标实体标识，确定用户设备对目标实体是否具有访问权限。

若确定用户设备对目标实体不具有访问权限，则直接确定用户设备与目标实体不具有第一通信权限，不再执行 S13 步骤。反之，若确定用户设备对目标实体具有访问权限，则继续执行是 S13 步骤。

S13、根据密钥标识 A-KID 确定用户设备是否具有使用 AKMA 的权限。

在确定用户设备具有使用 AKMA 的权限的情况下，可以确定用户设备与目标实体具有第一通信权限。反之，在确定用户设备不具有使用 AKMA 的权限的情况下，可以确定用户设备与目标实体不具有第一通信权限。

需要说明的是，该第一待定密钥信息可以包括目标实体对应的实体密钥信息。

在一些实施例中，该目标实体对应的实体密钥信息中可以包括目标实体对应的应用密钥 K_{AF} 。

在另一些实施例中，该目标实体对应的实体密钥信息中可以包括目标实体对应的应用密钥 K_{AF} 和密钥有效时间 K_{AF} expiration time。

S1204、第三实体将该第一待定密钥信息发送至第一代理实体。

在一些实施例中，第三实体可以通过第一密钥响应消息，向第一代理实体发送第一待

定密钥信息。示例地，该第一密钥响应消息可以为 Naanf_AKMA_ApplicationKey_Get Responsemessage。

在另一些实施例中，第三实体可以通过第二密钥响应消息，向第一代理实体发送第一待 定 密 钥 信 息 。 示 例 地 ， 该 第 二 密 钥 响 应 消 息 可 以 为 Naanf_AKMA_ApplicationKey_AnonUser_Get Responsemessage。

在一些实施例中，该第一密钥响应消息还可以包括用户设备的第二用户标识，该第二用户标识可以是在 3GPP 运营商域内表征该用户设备的标识；示例地，该第二用户标识可以是用户设备对应的用户永久标识 SUPI。

S1205、第一代理实体向用户设备发送应用会话建立响应消息。

第一代理实体获取该第一密钥响应消息中的应用密钥 K_{AF} 的情况下，可以确定用户设备与目标实体具有第一通信权限，此时，第一代理实体可以向用户设备发送应用会话建立响应消息。

S1206、用户设备通过第一代理实体进行身份认证。

用户设备可以在确定用户设备与目标实体具有第一通信权限的情况下，通过第一代理实体进行身份认证。示例地，用户设备可以根据目标实体的 FQDN 生成该目标实体对应的实体密钥 K_{AF} ，并根据该实体密钥 K_{AF} 与第一代理实体进行身份认证。

S1207a、第一代理实体将第一认证结果通知目标实体。

该第一认证结果可以用于指示目标实体与用户设备具有通信权限

在一些实施例中，在目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，第一代理实体可以向目标实体发送第一通知消息，该第一通知消息可以包括第一认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第一密钥响应消息获取到第二用户标识），第一通知消息还可以包括第二用户标识。

在另一些实施例中，在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，第一代理实体可以根据第一认证结果向第二实体发送第二通知消息，以指示第二实体向目标实体发送第一认证结果。同样地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第一密钥响应消息获取到第二用户标识），第二通知消息还可以包括第二用户标识。

在一些实施例中，在第一代理实体对用户设备进行身份认证成功的情况下，第一代理实体可以将第一认证结果通知目标实体（执行该 S1207a 步骤，不再继续执行 S1207b 及之后的步骤）。

在另一些实施例中，在第一代理实体对用户设备进行身份认证成功的情况下，第一代理实体可以获取第一代理实体的代理域名和目标实体的第一域名；在代理域名与第一域名不同的情况下，将第一认证结果通知目标实体（执行该 S1207a 步骤，不再继续执行 S1209b 及之后的步骤），以便指示目标实体与用户设备具有通信权限或者进行通信。

在另一些实施例中，在代理域名与第一域名相同的情况下，第一代理实体可以则暂时不向目标实体发送认证结果通知消息；先等待用户设备与目标实体是否具有第二通信权限，在确定用户设备与目标实体具有第二通信权限后，再将第一认证结果通知目标实体。也就是不执行 S1207a 步骤，继续执行 S1207b 及之后的步骤。

S1207b、用户设备与第一代理实体建立安全会话。

该安全会话可以包括 TLS 会话。

S1208、用户设备向第一代理实体发送目标实体服务请求消息。

其中，该目标实体服务请求消息包括第二目标实体标识，第二目标实体标识为用户设备根据目标实体的第一目标实体标识获取的受保护的实体标识。

在一些实施例中，该目标实体服务请求消息可以包括密钥标识 A-KID 和第二目标实体

标识。

在一些实施例中，在第二目标实体标识与第一目标实体标识相同的情况下，可以确定用户设备与目标实体具有第二通信权限，则可以向目标实体发送认证结果通知消息，并向用户设备发送目标实体服务响应消息。也就是执行该 S1209a 和 S1213 步骤，无需执行 S1209b 步骤至 S1212 步骤。

在另一些实施例中，在第二目标实体标识与第一目标实体标识不同的情况下，第一代理实体可以通过与第二实体的密钥请求消息交互确定用户设备与目标实体是否具有第二通信权限。也就是不执行 S1209a 步骤，继续执行 S1209b 及之后的步骤。

S1209a、第一代理实体将第一认证结果通知目标实体。

S1209b、第一代理实体向第三实体发送第三权限请求参数。

在一些实施例中，该第三权限请求参数可以包括密钥标识 A-KID、第二目标实体标识和第一代理实体对应的代理实体标识；该第三权限请求参数可以用于指示第三实体确定用户设备与目标实体是否具有第二通信权限。

在一些实施例中，第一代理实体可以通过第三密钥请求消息，向第三实体发送第三权限请求参数；第三密钥请求消息用于指示第三实体获取授权结果参数和用户设备的用户标识。示例地，该第三密钥请求消息可以为 Naanf_AKMA_ApplicationKey_Get Request message。

在另一些实施例中，第一代理实体可以通过第四密钥请求消息，向第三实体发送第三权限请求参数；第四密钥请求消息用于表征第一代理实体请求获取授权结果参数。示例地，该第四密钥请求消息可以为 Naanf_AKMA_ApplicationKey_AnonUser_Get Request message。

S1210、第三实体根据第三权限请求参数确定用户设备与目标实体是否具有第二通信权限。

示例地，第三实体确定用户设备与目标实体是否具有第二通信权限的方式可以包括以下一项或多项：

方式六、根据密钥标识 A-KID 和第二目标实体标识，确定用户设备对目标实体是否具有访问权限；

方式七、根据代理实体标识和第二目标实体标识，确定第一代理实体对目标实体是否具有代理权限。

方式八、根据密钥标识 A-KID 和第一目标实体标识，确定目标实体对用户设备的用户标识是否具有获取权限。

在一些实施例中，第三实体可以在确定用户设备对目标实体具有访问权限，且第一代理实体对目标实体具有代理权限的情况下，确定用户设备与目标实体具有第二通信权限。

S1211、第三实体向第一代理实体发送授权结果参数。

该授权结果参数可以用于通知第一代理实体用户设备与目标实体是否具有第二通信权限。

在一些实施例中，第三实体可以通过第三密钥响应消息，向第一代理实体发送授权结果参数。示例地，该第三密钥响应消息可以为 Naanf_AKMA_ApplicationKey_Get Response message。

在另一些实施例中，第三实体可以通过第四密钥响应消息，向第一代理实体发送授权结果参数。示例地，该第四密钥响应消息可以为 Naanf_AKMA_ApplicationKey_AnonUser_Get Response message。

在一些实施例中，第三实体在确定目标实体具有获取用户标识的权限的情况下，还可以在该第三密钥响应消息中包含用户设备的第二用户标识。同样地，该第四密钥响应消息中也可以包括用户设备的第二用户标识。该第二用户标识可以是用户设备对应的用户永久

标识 SUPI。

S1212、第一代理实体将第二认证结果通知目标实体。

其中，该第二认证结果可以用于指示目标实体与用户设备具有通信权限

例如，在目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，第一代理实体可以向目标实体发送第三通知消息，第三通知消息包括第二认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第三密钥响应消息获取到第二用户标识），第三通知消息还可以包括第二用户标识。

再例如，在目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，第一代理实体可以根据第一认证结果向第二实体发送第四通知消息，以指示第二实体向目标实体发送第一认证结果。进一步地，在第一代理实体获取到用户设备的第二用户标识的情况下（例如，通过第三密钥响应消息获取到第二用户标识），第四通知消息还可以包括第二用户标识。

在一些实施例中，该第二用户标识可以是用户设备对应的用户永久标识 SUPI。

S1213、第一代理实体向用户设备发送目标实体服务响应消息。

该目标实体服务响应消息用于指示用户设备与目标实体是否具有第二通信权限。

在一些实施例中，上述第一代理实体可以包括 3GPP 运营商域内的可信的认证代理 AP 实体。

在一些实施例中，上述第一实体可以包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体

在一些实施例中，上述第二实体可以包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

在一些实施例中，上述第三实体可以包括：AKMA 锚点功能 AAnF 实体。

这样，针对第一实体，通过 3GPP 运营商域内的可信的第一代理实体确定用户设备与第一实体是否具有通信权限，并在具有第一通信权限的情况下进行用户设备的身份验证，可以将第一实体的一部分功能通过第一代理实体实现，从而降低第一实体的负荷，提高第一实体的效率，并且，用户设备通过统一的第一代理实体实现与一个或多个第一实体的权限认证与身份认证，也降低了用户设备进行认证的复杂度，提高了用户设备的效率。

图 13 是根据一示例性实施例示出的一种认证装置 1300 的框图，该认证装置可以应用于用户设备。如图 13 所示，该装置 1300 可以包括：

目标实体确定模块 1301，被配置为从一个或多个第一实体中，确定请求通信的目标实体；

参数确定模块 1302，被配置为根据该目标实体确定第一权限请求参数；

第一消息发送模块 1303，被配置为根据该第一权限请求参数向第一代理实体发送应用会话建立请求消息；该应用会话建立请求消息用于指示该第一代理实体根据该第一权限请求参数确定该用户设备与该目标实体是否具有第一通信权限；该第一实体包括提供应用功能的实体，该第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，该第一代理实体为该第一实体提供认证代理功能；

第一消息接收模块 1304，被配置为响应于接收到该第一代理实体发送的应用会话建立响应消息，确定该用户设备与该目标实体是否具有第一通信权限；

认证模块，被配置为在该用户设备与该目标实体具有第一通信权限的情况下，通过该第一代理实体进行身份认证。

可选地，该参数确定模块 1302，被配置为将该目标实体的第一目标实体标识和该用户

设备对应的密钥标识 A-KID 作为该第一权限请求参数。

可选地，该第一通信权限包括以下一项或多项：

该用户设备对该目标实体具有访问权限；

该用户设备对该第一代理实体具有访问权限；

该第一代理实体对该目标实体具有代理权限；

所述目标实体对所述用户设备的用户标识具有获取权限。

图 14 是根据一示例性实施例示出的一种认证装置 1300 的框图，如图 14 所示，该装置还可以包括：

用户通信模块 1305，被配置为在通过该第一代理实体进行身份认证成功之后，与该第一代理实体建立安全会话；获取该第一代理实体的代理域名和该目标实体的第一域名；在该代理域名与该第一域名相同的情况下，通过该安全会话确定该用户设备与该目标实体是否具有第二通信权限；在确定该用户设备与该目标实体具有第二通信权限的情况下，与该目标实体进行通信。

可选地，该用户通信模块 1305，被配置为通过该安全会话，向该第一代理实体发送目标实体服务请求消息；该目标实体服务请求消息包括第二目标实体标识，该第二目标实体标识为该用户设备根据该第一目标实体标识获取的受保护的实体标识，该目标实体服务请求消息用于指示该第一代理实体根据该第二目标实体标识确定该用户设备与该目标实体是否具有第二通信权限；响应于接收到该第一代理实体发送的目标实体服务响应消息，确定该用户设备与该目标实体是否具有第二通信权限。

可选地，该第二通信权限包括以下一项或多项：

该用户设备对该目标实体具有访问权限；

该第一代理实体对该目标实体具有代理权限；

该目标实体对用户设备的用户标识具有获取权限。

可选地，该第一消息接收模块 1304，被配置为在接收到该应用会话建立响应消息的情况下，确定该用户设备与该目标实体具有第一通信权限；或者，在接收到该应用会话建立响应消息，且该会话建立响应消息中包含成功指示信息的情况下，确定该用户设备与该目标实体具有第一通信权限。

可选地，所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

可选地，所述第一实体包括 3GPP 运营商域内的可信的提供应用功能的实体。

可选地，所述第一实体包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体。

可选地，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体通过第二实体与所述第一实体进行通信；所述第二实体包括提供网络开放功能的实体。

可选地，所述第一实体包括：3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

可选地，所述第二实体包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

图 15 是根据一示例性实施例示出的一种认证装置 1500 的框图，该认证装置可以应用于第一代理实体。如图 15 所示，该装置 1500 可以包括：

第一代理接收模块 1501，被配置为接收用户设备发送的应用会话建立请求消息；所述应用会话建立请求消息包括第一权限请求参数，所述应用会话建立请求消息用于指示所述第一代理实体根据第一权限请求参数确定所述用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提

供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第一代理确定模块 1502，被配置为根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；

第一代理发送模块 1503，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，向用户设备发送应用会话建立响应消息，以及，对所述用户设备进行身份认证。

可选地，所述第一权限请求参数包括所述目标实体的第一目标实体标识和所述用户设备对应的密钥标识 A-KID。

可选地，所述第一通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；

所述用户设备对所述第一代理实体具有访问权限；

所述第一代理实体对所述目标实体具有代理权限；

所述目标实体对所述用户设备的用户标识具有获取权限。

可选地，所述第一代理确定模块 1502，被配置为根据所述第一权限请求参数确定第二权限请求参数；向第三实体发送所述第二权限请求参数；所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；所述第二权限请求参数用于指示所述第三实体确定所述用户设备与所述目标实体是否具有第一通信权限；获取所述第三实体发送的第一待定密钥信息，所述第一待定密钥信息为所述第三实体根据所述第二权限请求参数获取的密钥信息；根据所述第一待定密钥信息，确定所述用户设备与所述目标实体是否具有第一通信权限。

可选地，所述第一代理确定模块 1502，被配置为将所述第一权限请求参数和所述第一代理实体对应的代理实体标识，作为所述第二权限请求参数。

可选地，所述第一代理确定模块 1502，被配置为通过第一密钥请求消息，向第三实体发送所述第二权限请求参数；所述第一密钥请求消息用于指示所述第三实体获取第一待定密钥信息和所述用户设备的用户标识；接收所述第三实体发送的第一密钥响应消息；获取所述第一密钥响应消息中包含的第一待定密钥信息。

可选地，所述第一密钥响应消息还包括所述用户设备对应的第二用户标识，所述第一代理确定模块 1502，被配置为根据接收到的第一密钥响应消息，获取所述第二用户标识。

可选地，所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

可选地，所述第一代理确定模块 1502，被配置为通过第二密钥请求消息，向第三实体发送所述第二权限请求参数；所述第二密钥请求消息用于表征第一代理实体请求获取所述第一待定密钥信息；接收所述第三实体发送的第二密钥响应消息；获取所述第二密钥响应消息中包含的第一待定密钥信息。

可选地，所述第一代理确定模块 1502，被配置为在所述第一待定密钥信息包括所述目标实体对应的实体密钥信息的情况下，确定所述用户设备与所述目标实体具有第一通信权限。

可选地，在对所述用户设备进行身份认证成功的情况下，所述第一代理发送模块 1503，被配置为将所述身份认证的第一认证结果通知所述目标实体。

可选地，所述第一代理发送模块 1503，被配置为获取所述第一代理实体的代理域名和所述目标实体的第一域名；在所述代理域名与所述第一域名不同的情况下，将所述第一认证结果通知所述目标实体。

可选地，在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，所述第一代理发送模块 1503，被配置为向所述目标实体发送第一通知消息，所述第一通知消息包括所述第一认证结果。

可选地，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第一通知消息还包括所述第二用户标识。

可选地，在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，所述第一代理发送模块 1503，被配置为根据所述第一认证结果向所述第二实体发送第二通知消息，以指示所述第二实体向所述目标实体发送所述第一认证结果。

可选地，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第二通知消息还包括所述第二用户标识。

可选地，在对所述用户设备进行身份认证成功之后，所述装置还包括：

图 16 是根据一示例性实施例示出的一种认证装置 1500 的框图，如图 16 所示，该装置还可以包括：

第一代理通信模块 1504，被配置为与所述用户设备建立安全会话；通过所述安全会话，接收所述用户设备发送的目标实体服务请求消息；所述目标实体服务请求消息包括第二目标实体标识，所述第二目标实体标识为用户设备根据所述目标实体的第一目标实体标识获取的受保护的实体标识，所述目标实体服务请求消息为所述用户设备在确定所述第一代理实体的代理域名与所述目标实体的第一域名相同的情况下发送的消息；根据所述第二目标实体标识确定所述用户设备与所述目标实体是否具有第二通信权限；向所述用户设备发送的目标实体服务响应消息；所述目标实体服务响应消息用于指示所述用户设备与所述目标实体是否具有第二通信权限。

可选地，所述第二通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；

所述第一代理实体对所述目标实体具有代理权限；

该目标实体对用户设备的用户标识具有获取权限。

可选地，所述第一代理通信模块 1504，被配置为在所述第二目标实体标识与所述第一目标实体标识相同的情况下，确定所述用户设备与所述目标实体具有第二通信权限。

可选地，所述第一代理通信模块 1504，被配置为在所述第二目标实体标识与所述第一目标实体标识不同的情况下，根据所述第二目标实体标识确定第三权限请求参数；向第三实体发送所述第三权限请求参数；所述第三权限请求参数用于指示所述第三实体确定所述用户设备与所述目标实体是否具有第二通信权限；获取所述第三实体发送的授权结果参数；所述授权结果参数用于表征所述用户设备与所述目标实体是否具有第二通信权限；根据所述授权结果参数确定所述用户设备与所述目标实体是否具有第二通信权限。

可选地，所述第一代理通信模块 1504，被配置为将所述第二目标实体标识、所述用户设备对应的密钥标识 A-KID 和所述第一代理实体对应的代理实体标识，作为所述第三权限请求参数。

可选地，所述第一代理通信模块 1504，被配置为通过第三密钥请求消息，向第三实体发送所述第三权限请求参数；所述第三密钥请求消息用于指示所述第三实体获取授权结果参数和所述用户设备的用户标识；接收所述第三实体发送的第三密钥响应消息；获取所述第三密钥响应消息中包含的授权结果参数。

可选地，所述第三密钥响应消息还包括所述用户设备对应的第二用户标识，所述第一代理通信模块 1504，被配置为根据接收到的第三密钥响应消息，获取所述第二用户标识。

可选地，所述第三密钥请求消息还包括授权指示参数，所述授权指示参数用于指示所述第三实体根据所述第三密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

可选地，所述第一代理通信模块 1504，被配置为通过第四密钥请求消息，向第三实体发送所述第三权限请求参数；所述第四密钥请求消息用于表征第一代理实体请求获取所述授权结果参数；接收所述第三实体发送的第四密钥响应消息；获取所述第四密钥响应消息中包含的授权结果参数。

可选地,所述第四密钥请求消息还包括授权指示参数,所述授权指示参数用于指示所述第三实体根据所述第四密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

可选地,所述第一代理通信模块 1504,被配置为在根据所述授权结果参数确定所述用户设备与所述目标实体具有第二通信权限的情况下,将第二认证结果通知所述目标实体;所述第二认证结果用于指示所述目标实体与所述用户设备具有通信权限。

可选地,所述第一代理通信模块 1504,被配置为在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下,向所述目标实体发送第三通知消息,所述第三通知消息包括所述第二认证结果。

可选地,在所述第一代理实体获取到所述用户设备的第二用户标识的情况下,所述第三通知消息还包括所述第二用户标识。

可选地,所述第一代理通信模块 1504,被配置为在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下,根据所述第一认证结果向所述第二实体发送第四通知消息,以指示所述第二实体向所述目标实体发送所述第一认证结果。

可选地,在所述第一代理实体获取到所述用户设备的第二用户标识的情况下,所述第四通知消息还包括所述第二用户标识。

可选地,在所述第一待密钥信息包括应用密钥 KAF 和密钥有效时间。

可选地,所述第二实体包括:网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

可选地,所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

可选地,所述第一实体包括:3GPP 运营商域内的可信的应用功能 AF 实体,或者,3GPP 运营商域内的可信的应用服务器 SCS/AS 实体,或者,3GPP 运营商域外的非可信的应用功能 AF 实体,或者,3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

图 17 是根据一示例性实施例示出的一种认证装置 1700 的框图,该认证装置可以应用于第二实体。如图 17 所示,该装置 1700 可以包括:

第二接收模块 1701,被配置为获取第一代理实体对用户设备的认证结果;所述认证结果包括第一认证结果或第二认证结果,所述第一认证结果用于指示用户设备与目标实体具有第一通信权限;所述第二认证结果用于指示用户设备与目标实体具有第二通信权限;所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体,所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体,所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体,所述第一代理实体为所述第一实体提供认证代理功能;

第二发送模块 1702,被配置为将所述认证结果发送至所述目标实体,以便所述目标实体根据所述认证结果与用户设备进行通信。

可选地,所述第二接收模块 1701,被配置为接收所述第一代理实体发送的第二通知消息;所述第二通知消息为所述第一代理实体在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下,根据所述第一认证结果向所述第二实体发送的消息;根据所述第二通知消息获取所述第一认证结果;

所述第二发送模块 1702,被配置为根据所述第一认证结果向所述目标实体发送第五通知消息。

可选地,在所述第二通知消息中包括所述用户设备对应的第二用户标识的情况下,所述第二发送模块 1702,被配置为根据所述第二用户标识获取所述用户设备对应的第一用户标识;根据所述第一认证结果和所述第一用户标识,向所述目标实体发送第五通知消息。

可选地,所述第一用户标识为所述用户设备对应的通用公共用户标识 GPSI;所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

可选地,所述第二接收模块 1701,被配置为接收所述第一代理实体发送的第四通知消息;所述第四通知消息为所述第一代理实体在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下,根据所述第二认证结果向所述第二实体发送的消息;根据所述第二通知消息获取所述第二认证结果;

所述第二发送模块 1702,被配置为根据所述第二认证结果向所述目标实体发送第六通知消息。

可选地,在所述第四通知消息中包括所述用户设备对应的第二用户标识的情况下,所述所述第二发送模块 1702,被配置为根据所述第二用户标识获取所述用户设备对应的第一用户标识;根据所述第二认证结果和所述第一用户标识,向所述目标实体发送第六通知消息。

可选地,所述第二实体包括:网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

图 18 是根据一示例性实施例示出的一种认证装置 1800 的框图,该认证装置可以应用于第三实体。如图 18 所示,该装置 1800 可以包括:

第三接收模块 1801,被配置为接收第一代理实体发送的第二权限请求参数;所述第二权限请求参数用于指示第三实体确定用户设备与目标实体是否具有第一通信权限,所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体,所述第一实体包括提供应用功能的实体,所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体,所述第一代理实体为所述第一实体提供认证代理功能,所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体;

第三确定模块 1802,被配置为根据所述第二权限请求参数,确定所述用户设备与所述目标实体是否具有第一通信权限;

第三密钥模块 1803,被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下,获取第一待定密钥信息;

第三发送模块 1804,被配置为将所述第一待定密钥信息发送至所述第一代理实体。

可选地,所述第二权限请求参数包括所述用户设备对应的密钥标识 A-KID、目标实体的第一目标实体标识和所述第一代理实体对应的代理实体标识;所述第三确定模块 1802,被配置为通过以下一项或多项,确定所述用户设备与所述目标实体是否具有第一通信权限:

根据所述密钥标识 A-KID 和所述第一目标实体标识,确定所述用户设备对所述目标实体是否具有访问权限;

根据所述密钥标识 A-KID 和所述代理实体标识,确定所述用户设备对所述第一代理实体是否具有访问权限;

根据所述代理实体标识和所述第一目标实体标识,确定所述第一代理实体对所述目标实体是否具有代理权限。

可选地,所述第三密钥模块 1803,被配置为

根据所述目标实体对应的实体密钥信息,获取所述第一待定密钥信息。

可选地,所述第三接收模块 1801,被配置为通过第一密钥请求消息,接收第一代理实体发送的所述第二权限请求参数;所述第一密钥请求消息用于指示所述第三实体获取第一待定密钥信息和所述用户设备的用户标识;

所述第三发送模块 1804,被配置为通过第一密钥响应消息,向所述第一代理实体发送所述第一待定密钥信息。

可选地,所述第三发送模块 1804,被配置为在确定所述目标实体具有获取用户标识的权限的情况下,通过第一密钥响应消息,向所述第一代理实体发送第一待定密钥信息和所述用户设备对应的第二用户标识。

可选地,所述第二用户标识为所述用户设备对应的用户永久标识 SUPI。

可选地,所述第三接收模块 1801,被配置为通过第二密钥请求消息,接收第一代理实体发送的所述第二权限请求参数;所述第二密钥请求消息用于指示所述第三实体获取第一待密钥信息;

所述第三发送模块 1804,被配置为通过第二密钥响应消息,向所述第一代理实体发送所述第一待密钥信息。

可选地,所述第三确定模块 1802,被配置为在将所述第一待密钥信息发送至所述第一代理实体之后,接收所述第一代理实体发送的第三权限请求参数;根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限;向所述第一代理实体发送授权结果参数;所述授权结果参数用于通知所述第一代理实体所述用户设备与所述目标实体是否具有第二通信权限。

可选地,所述第三权限请求参数包括所述密钥标识 A-KID、第二目标实体标识和所述第一代理实体对应的代理实体标识,所述第二目标实体标识为所述用户设备根据目标实体的第一目标实体标识获取的受保护的实体标识;所述第三确定模块 1802,被配置为通过以下一项或多项,确定所述用户设备与所述目标实体是否具有第二通信权限:

根据所述密钥标识 A-KID 和所述第二目标实体标识,确定所述用户设备对所述目标实体是否具有访问权限;

根据所述代理实体标识和所述第二目标实体标识,确定所述第一代理实体对所述目标实体是否具有代理权限。

可选地,所述第三确定模块 1802,被配置为通过第三密钥请求消息,接收第一代理实体发送的所述第三权限请求参数;所述第三密钥请求消息用于指示所述第三实体获取授权结果参数和所述用户设备的用户标识;通过第三密钥响应消息,向所述第一代理实体发送授权结果参数。

可选地,所述第三密钥请求消息还包括授权指示参数,所述授权指示参数用于指示所述第三实体根据所述第三密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

可选地,所述第三确定模块 1802,被配置为在确定所述目标实体具有获取用户标识的权限的情况下,通过第三密钥响应消息,向所述第一代理实体发送授权结果参数和所述用户设备对应的第二用户标识。

可选地,所述第二用户标识为所述用户设备对应的用户永久标识 SUPI。

可选地,所述第三确定模块 1802,被配置为通过第四密钥请求消息,接收第一代理实体发送的所述第三权限请求参数;所述第四密钥请求消息用于指示所述第三实体获取授权结果参数;通过第四密钥响应消息,向所述第一代理实体发送所述授权结果参数。

可选地,所述第三确定模块 1802,被配置为根据第一预设策略确定所述第三实体是否具有为第一代理实体服务的权限;在所述第三实体是否具有为第一代理实体服务的权限的情况下,根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限。

可选地,所述第三确定模块 1802,被配置为根据第一预设策略确定所述第三实体是否具有为第一代理实体服务的权限;在所述第三实体是否具有为第一代理实体服务的权限的情况下,根据所述第二权限请求参数,确定所述用户设备与所述目标实体是否具有第一通信权限。

可选地,所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体;所述第三实体包括: AKMA 锚点功能 AAnF 实体。

可选地,所述第一实体包括: 3GPP 运营商域内的可信的应用功能 AF 实体,或者, 3GPP 运营商域内的可信的应用服务器 SCS/AS 实体,或者, 3GPP 运营商域外的非可信的应用功

能 AF 实体, 或者, 3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

图 19 是根据一示例性实施例示出的一种认证装置 1900 的框图, 该认证装置可以应用于第一实体。如图 19 所示, 该装置 1900 可以包括:

第一通信模块 1901, 被配置为获取第一代理实体对用户设备的认证结果, 所述认证结果包括第一认证结果或第二认证结果, 所述第一认证结果用于指示所述用户设备与所述目标实体具有第一通信权限; 所述第二认证结果用于指示所述用户设备与所述目标实体具有第二通信权限; 所述第一实体包括提供应用功能的实体, 所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体, 所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体, 所述第一代理实体为所述第一实体提供认证代理功能; 根据所述认证结果与用户设备进行通信。

可选地, 所述第一通信模块 1901, 被配置为在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下, 接收所述第一代理实体发送的第一通知消息, 所述第一通知消息包括所述第一认证结果; 或者, 接收所述第一代理实体发送的第三通知消息, 所述第三通知消息包括所述第二认证结果。

可选地, 所述第一通知消息或所述第三通知消息中还包括所述用户设备对应的第二用户标识。

可选地, 所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

可选地, 所述第一通信模块 1901, 被配置为在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下, 接收所述第二实体发送的第五通知消息; 其中, 所述第五通知消息包括所述第一认证结果, 所述第五通知消息为所述第二实体响应于接收到所述第二通知消息后发送的消息; 或者, 接收所述第二实体发送的第六通知消息; 其中, 所述第六通知消息包括所述第二认证结果, 所述第五通知消息为所述第二实体响应于接收到所述第四通知消息后发送的消息。

可选地, 所述第五通知消息或所述第六通知消息中还包括所述用户设备的第一用户标识。

可选地, 所述第一用户标识为所述用户设备对应的通用公共用户标识 GPSI。

可选地, 所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

可选地, 所述第一实体包括: 3GPP 运营商域内的可信的应用功能 AF 实体, 或者, 3GPP 运营商域内的可信的应用服务器 SCS/AS 实体, 或者, 3GPP 运营商域外的非可信的应用功能 AF 实体, 或者, 3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

关于上述实施例中的装置, 其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述, 此处将不做详细阐述说明。

图 20 是根据一示例性实施例示出的一种认证装置的框图。示例地, 该认证装置 2000 可以是终端设备, 例如移动电话, 计算机, 数字广播终端, 消息收发设备, 游戏控制台, 平板设备, 医疗设备, 健身设备, 个人数字助理等; 该认证装置 2000 也可以是服务器, 例如本地服务器或云服务器; 该认证装置 2000 也可以是图 1 所示的用户设备、该认证装置 2000 也可以是图 1 所示通信系统中的任一网络实体, 例如第一实体、第一代理实体、第二实体或第三实体。

参照图 20, 该装置 2000 可以包括以下一个或多个组件: 处理组件 2002, 存储器 2004, 以及通信组件 2006。

处理组件 2002 通常控制装置 2000 的整体操作, 诸如与显示, 电话呼叫, 数据通信, 相机操作和记录操作相关联的操作。处理组件 2002 可以包括一个或多个处理器 2020 来执行指令, 以完成上述的认证方法的全部或部分步骤。此外, 处理组件 2002 可以包括一个或多个模块, 便于处理组件 2002 和其他组件之间的交互。例如, 处理组件 2002 可以包括

多媒体模块，以方便多媒体组件和处理组件 2002 之间的交互。

存储器 2004 被配置为存储各种类型的数据以支持在装置 2000 的操作。这些数据的示例包括用于在装置 2000 上操作的任何应用程序或方法的指令，联系人数据，电话簿数据，消息，图片，视频等。存储器 2004 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。

通信组件 2006 被配置为便于装置 2000 和其他设备之间有线或无线方式的通信。装置 2000 可以接入基于通信标准的无线网络，如 WiFi，2G 或 3G，或它们的组合。在一个示例性实施例中，通信组件 2006 经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中，所述通信组件 2006 还包括近场通信(NFC)模块，以促进短程通信。例如，在 NFC 模块可基于射频识别(RFID)技术，红外数据协会(IrDA)技术，超宽带(UWB)技术，蓝牙(BT)技术和其他技术来实现。

在示例性实施例中，装置 2000 可以被一个或多个应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现，用于执行上述认证方法。

上述装置 2000 除了可以是独立的电子设备外，也可以是独立电子设备的一部分，例如在一种实施例中，该电子设备可以是集成电路(Integrated Circuit, IC)或芯片，其中该集成电路可以是一个 IC，也可以是多个 IC 的集合；该芯片可以包括但不限于以下种类：GPU(Graphics Processing Unit, 图形处理器)、CPU(Central Processing Unit, 中央处理器)、FPGA(Field Programmable Gate Array, 可编程逻辑阵列)、DSP(Digital Signal Processor, 数字信号处理器)、ASIC(Application Specific Integrated Circuit, 专用集成电路)、SOC(System on Chip, SoC, 片上系统或系统级芯片)等。上述的集成电路或芯片中可以用于执行可执行指令(或代码)，以实现上述认证方法。其中该可执行指令可以存储在该集成电路或芯片中，也可以从其他的装置或设备获取，例如该集成电路或芯片中包括处理器、存储器，以及用于与其他的装置通信的接口。该可执行指令可以存储于该处理器中，当该可执行指令被处理器执行时实现上述认证方法；或者，该集成电路或芯片可以通过该接口接收可执行指令并传输给该处理器执行，以实现上述认证方法。

在示例性实施例中，还提供了一种包括指令的非临时性计算机可读存储介质，例如包括指令的存储器 2004，上述指令可由装置 2000 的处理器 2020 执行以完成上述认证方法。例如，所述非临时性计算机可读存储介质可以是 ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

在另一示例性实施例中，还提供一种计算机程序产品，该计算机程序产品包含能够由可编程的装置执行的计算机程序，该计算机程序具有当由该可编程的装置执行时用于执行上述认证方法的代码部分。

本领域技术人员在考虑说明书及实践本公开后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

应当理解的是，本公开并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本公开的范围仅由所附的权利要求来限制。

权利要求书

1、一种认证方法，其特征在于，应用于用户设备，所述方法包括：

从一个或多个第一实体中，确定请求通信的目标实体；

根据所述目标实体确定第一权限请求参数；

根据所述第一权限请求参数向第一代理实体发送应用会话建立请求消息；所述应用会话建立请求消息用于指示所述第一代理实体根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

响应于接收到所述第一代理实体发送的应用会话建立响应消息，确定所述用户设备与所述目标实体是否具有第一通信权限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，通过所述第一代理实体进行身份认证。

2、根据权利要求 1 所述的方法，其特征在于，所述根据所述目标实体确定第一权限请求参数包括：

将所述目标实体的第一目标实体标识和所述用户设备对应的密钥标识 A-KID 作为所述第一权限请求参数。

3、根据权利要求 1 所述的方法，其特征在于，所述第一通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；

所述用户设备对所述第一代理实体具有访问权限；

所述第一代理实体对所述目标实体具有代理权限；

所述目标实体对所述用户设备的用户标识具有获取权限。

4、根据权利要求 1 所述的方法，其特征在于，在通过所述第一代理实体进行身份认证成功之后，所述方法还包括：

与所述第一代理实体建立安全会话；

获取所述第一代理实体的代理域名和所述目标实体的第一域名；

在所述代理域名与所述第一域名相同的情况下，通过所述安全会话确定所述用户设备与所述目标实体是否具有第二通信权限；

在确定所述用户设备与所述目标实体具有第二通信权限的情况下，与所述目标实体进行通信。

5、根据权利要求 4 所述的方法，其特征在于，所述通过所述安全会话确定所述用户设备与所述目标实体是否具有第二通信权限包括：

通过所述安全会话，向所述第一代理实体发送目标实体服务请求消息；所述目标实体服务请求消息包括第二目标实体标识，所述第二目标实体标识为所述用户设备根据所述第一目标实体标识获取的受保护的实体标识，所述目标实体服务请求消息用于指示所述第一代理实体根据所述第二目标实体标识确定所述用户设备与所述目标实体是否具有第二通信权限；

响应于接收到所述第一代理实体发送的目标实体服务响应消息，确定所述用户设备

与所述目标实体是否具有第二通信权限。

6、根据权利要求 4 所述的方法，其特征在于，所述第二通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；
所述第一代理实体对所述目标实体具有代理权限；
所述目标实体对所述用户设备的用户标识具有获取权限。

7、根据权利要求 1 所述的方法，其特征在于，所述响应于接收到所述第一代理实体发送的应用会话建立响应消息，确定所述用户设备与所述目标实体是否具有第一通信权限包括：

在接收到所述应用会话建立响应消息的情况下，确定所述用户设备与所述目标实体具有第一通信权限；或者，

在接收到所述应用会话建立响应消息，且所述会话建立响应消息中包含成功指示信息的情况下，确定所述用户设备与所述目标实体具有第一通信权限。

8、根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

9、根据权利要求 8 所述的方法，其特征在于，所述第一实体包括 3GPP 运营商域内的可信的提供应用功能的实体。

10、根据权利要求 9 所述的方法，其特征在于，所述第一实体包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体。

11、根据权利要求 8 所述的方法，其特征在于，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体通过第二实体与所述第一实体进行通信；所述第二实体包括提供网络开放功能的实体。

12、根据权利要求 11 所述的方法，其特征在于，所述第一实体包括：3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

13、根据权利要求 11 所述的方法，其特征在于，所述第二实体包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

14、一种认证方法，其特征在于，应用于第一代理实体，所述方法包括：

接收用户设备发送的应用会话建立请求消息；所述应用会话建立请求消息包括第一权限请求参数，所述应用会话建立请求消息用于指示所述第一代理实体根据第一权限请求参数确定所述用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权

限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，向用户设备发送应用会话建立响应消息，以及，对所述用户设备进行身份认证。

15、根据权利要求 14 所述的方法，其特征在于，所述第一权限请求参数包括所述目标实体的第一目标实体标识和所述用户设备对应的密钥标识 A-KID。

16、根据权利要求 14 所述的方法，其特征在于，所述第一通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；

所述用户设备对所述第一代理实体具有访问权限；

所述第一代理实体对所述目标实体具有代理权限；

所述目标实体对所述用户设备的用户标识具有获取权限。

17、根据权利要求 14 所述的方法，其特征在于，所述根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限包括：

根据所述第一权限请求参数确定第二权限请求参数；

向第三实体发送所述第二权限请求参数；所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；所述第二权限请求参数用于指示所述第三实体确定所述用户设备与所述目标实体是否具有第一通信权限；

获取所述第三实体发送的第一待定密钥信息，所述第一待定密钥信息为所述第三实体根据所述第二权限请求参数获取的密钥信息；

根据所述第一待定密钥信息，确定所述用户设备与所述目标实体是否具有第一通信权限。

18、根据权利要求 17 所述的方法，其特征在于，所述根据所述第一权限请求参数确定第二权限请求参数包括：

将所述第一权限请求参数和所述第一代理实体对应的代理实体标识，作为所述第二权限请求参数。

19、根据权利要求 17 所述的方法，其特征在于，所述向第三实体发送所述第二权限请求参数包括：

通过第一密钥请求消息，向第三实体发送所述第二权限请求参数；所述第一密钥请求消息用于指示所述第三实体获取第一待定密钥信息和所述用户设备的用户标识；

所述获取所述第三实体发送的第一待定密钥信息包括：

接收所述第三实体发送的第一密钥响应消息；

获取所述第一密钥响应消息中包含的第一待定密钥信息。

20、根据权利要求 19 所述的方法，其特征在于，所述第一密钥响应消息还包括所述用户设备对应的第二用户标识，所述方法还包括：

根据接收到的第一密钥响应消息，获取所述第二用户标识。

21、根据权利要求 20 所述的方法，其特征在于，所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

22、根据权利要求 17 所述的方法，其特征在于，所述向第三实体发送所述第二权限请求参数包括：

通过第二密钥请求消息，向第三实体发送所述第二权限请求参数；所述第二密钥请求消息用于表征第一代理实体请求获取所述第一待密钥信息；

所述获取所述第三实体发送的第一待密钥信息包括：

接收所述第三实体发送的第二密钥响应消息；

获取所述第二密钥响应消息中包含的第一待密钥信息。

23、根据权利要求 17 所述的方法，其特征在于，所述根据所述第一待密钥信息，确定所述用户设备与所述目标实体是否具有第一通信权限包括：

在所述第一待密钥信息包括所述目标实体对应的实体密钥信息的情况下，确定所述用户设备与所述目标实体具有第一通信权限。

24、根据权利要求 17 所述的方法，其特征在于，在对所述用户设备进行身份认证成功的情况下，所述方法还包括：

将所述身份认证的第一认证结果通知所述目标实体。

25、根据权利要求 24 所述的方法，其特征在于，所述将所述身份认证的第一认证结果通知所述目标实体包括：

获取所述第一代理实体的代理域名和所述目标实体的第一域名；

在所述代理域名与所述第一域名不同的情况下，将所述第一认证结果通知所述目标实体。

25、根据权利要求 24 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，所述将所述身份认证的第一认证结果通知所述目标实体包括：

向所述目标实体发送第一通知消息，所述第一通知消息包括所述第一认证结果。

26、根据权利要求 25 所述的方法，其特征在于，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第一通知消息还包括所述第二用户标识。

27、根据权利要求 24 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，所述将所述身份认证的第一认证结果通知所述目标实体包括：

根据所述第一认证结果向所述第二实体发送第二通知消息，以指示所述第二实体向所述目标实体发送所述第一认证结果。

28、根据权利要求 27 所述的方法，其特征在于，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第二通知消息还包括所述第二用户标识。

29、根据权利要求 14 所述的方法，其特征在于，在对所述用户设备进行身份认证成功之后，所述方法还包括：

与所述用户设备建立安全会话；

通过所述安全会话，接收所述用户设备发送的目标实体服务请求消息；所述目标实

体服务请求消息包括第二目标实体标识，所述第二目标实体标识为用户设备根据所述目标实体的第一目标实体标识获取的受保护的实体标识，所述目标实体服务请求消息为所述用户设备在确定所述第一代理实体的代理域名与所述目标实体的第一域名相同的情况下发送的消息；

根据所述第二目标实体标识确定所述用户设备与所述目标实体是否具有第二通信权限；

向所述用户设备发送的目标实体服务响应消息；所述目标实体服务响应消息用于指示所述用户设备与所述目标实体是否具有第二通信权限。

30、根据权利要求 29 所述的方法，其特征在于，所述第二通信权限包括以下一项或多项：

所述用户设备对所述目标实体具有访问权限；

所述第一代理实体对所述目标实体具有代理权限；

所述目标实体对所述用户设备的用户标识具有获取权限。

31、根据权利要求 29 所述的方法，其特征在于，所述根据所述第二目标实体标识确定所述用户设备与所述目标实体是否具有第二通信权限包括：

在所述第二目标实体标识与所述第一目标实体标识相同的情况下，确定所述用户设备与所述目标实体具有第二通信权限。

32、根据权利要求 29 所述的方法，其特征在于，所述根据所述第二目标实体标识确定所述用户设备与所述目标实体是否具有第二通信权限包括：

在所述第二目标实体标识与所述第一目标实体标识不同的情况下，根据所述第二目标实体标识确定第三权限请求参数；

向第三实体发送所述第三权限请求参数；所述第三权限请求参数用于指示所述第三实体确定所述用户设备与所述目标实体是否具有第二通信权限；

获取所述第三实体发送的授权结果参数；所述授权结果参数用于表征所述用户设备与所述目标实体是否具有第二通信权限；

根据所述授权结果参数确定所述用户设备与所述目标实体是否具有第二通信权限。

33、根据权利要求 32 所述的方法，其特征在于，所述根据所述第二目标实体标识确定第三权限请求参数包括：

将所述第二目标实体标识、所述用户设备对应的密钥标识 A-KID 和所述第一代理实体对应的代理实体标识，作为所述第三权限请求参数。

34、根据权利要求 32 所述的方法，其特征在于，所述向第三实体发送所述第三权限请求参数包括：

通过第三密钥请求消息，向第三实体发送所述第三权限请求参数；所述第三密钥请求消息用于指示所述第三实体获取授权结果参数和所述用户设备的用户标识；

所述获取所述第三实体发送的授权结果参数包括：

接收所述第三实体发送的第三密钥响应消息；

获取所述第三密钥响应消息中包含的授权结果参数。

35、根据权利要求 34 所述的方法，其特征在于，所述第三密钥响应消息还包括所述

用户设备对应的第二用户标识，所述方法还包括：

根据接收到的第三密钥响应消息，获取所述第二用户标识。

36、根据权利要求 34 所述的方法，其特征在于，所述第三密钥请求消息还包括授权指示参数，所述授权指示参数用于指示所述第三实体根据所述第三密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

37、根据权利要求 33 所述的方法，其特征在于，所述向第三实体发送所述第三权限请求参数包括：

通过第四密钥请求消息，向第三实体发送所述第三权限请求参数；所述第四密钥请求消息用于表征第一代理实体请求获取所述授权结果参数；

所述获取所述第三实体发送的授权结果参数包括：

接收所述第三实体发送的第四密钥响应消息；

获取所述第四密钥响应消息中包含的授权结果参数。

38、根据权利要求 37 所述的方法，其特征在于，所述第四密钥请求消息还包括授权指示参数，所述授权指示参数用于指示所述第三实体根据所述第四密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

39、根据权利要求 31 所述的方法，其特征在于，在根据所述授权结果参数确定所述用户设备与所述目标实体具有第二通信权限的情况下，所述方法还包括：

将第二认证结果通知所述目标实体；所述第二认证结果用于指示所述目标实体与所述用户设备具有通信权限。

40、根据权利要求 39 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，所述将第二认证结果通知所述目标实体包括：向所述目标实体发送第三通知消息，所述第三通知消息包括所述第二认证结果。

41、根据权利要求 40 所述的方法，其特征在于，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第三通知消息还包括所述第二用户标识。

42、根据权利要求 39 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，所述将第二认证结果通知所述目标实体包括：

根据所述第一认证结果向所述第二实体发送第四通知消息，以指示所述第二实体向所述目标实体发送所述第一认证结果。

43、根据权利要求 43 所述的方法，其特征在于，在所述第一代理实体获取到所述用户设备的第二用户标识的情况下，所述第四通知消息还包括所述第二用户标识。

44、根据权利要求 17 所述的方法，其特征在于，在所述第一待选密钥信息包括应用密钥 K_{AF} 和密钥有效时间。

45、根据权利要求 17 所述的方法，其特征在于，所述第二实体包括：网络开放功能

NEF 实体或业务能力开放功能 SCEF 实体。

46、根据权利要求 14 至 45 中任一项所述的方法，其特征在于，所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

47、根据权利要求 14 至 45 中任一项所述的方法，其特征在于，所述第一实体包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

48、一种认证方法，其特征在于，应用于第三实体，所述方法包括：

接收第一代理实体发送的第二权限请求参数；所述第二权限请求参数用于指示第三实体确定用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能，所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；

根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限；

在所述用户设备与所述目标实体具有第一通信权限的情况下，获取第一待定密钥信息；

将所述第一待定密钥信息发送至所述第一代理实体。

49、根据权利要求 48 所述的方法，其特征在于，所述第二权限请求参数包括所述用户设备对应的密钥标识 A-KID、目标实体的第一目标实体标识和所述第一代理实体对应的代理实体标识；所述根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限包括以下一项或多项：

根据所述密钥标识 A-KID 和所述第一目标实体标识，确定所述用户设备对所述目标实体是否具有访问权限；

根据所述密钥标识 A-KID 和所述代理实体标识，确定所述用户设备对所述第一代理实体是否具有访问权限；

根据所述代理实体标识和所述第一目标实体标识，确定所述第一代理实体对所述目标实体是否具有代理权限；

根据所述密钥标识 A-KID 和所述第一目标实体标识，确定所述目标实体对所述用户设备的用户标识是否具有获取权限。

50、根据权利要求 48 所述的方法，其特征在于，所述获取第一待定密钥信息包括：根据所述目标实体对应的实体密钥信息，获取所述第一待定密钥信息。

51、根据权利要求 48 所述的方法，其特征在于，所述接收第一代理实体发送的第二权限请求参数包括：

通过第一密钥请求消息，接收第一代理实体发送的所述第二权限请求参数；所述第一密钥请求消息用于指示所述第三实体获取第一待定密钥信息和所述用户设备的用户标识；

所述将所述第一待定密钥信息发送至所述第一代理实体包括：
通过第一密钥响应消息，向所述第一代理实体发送所述第一待定密钥信息。

52、根据权利要求 51 所述的方法，其特征在于，所述通过第一密钥响应消息，向所述第一代理实体发送所述第一待定密钥信息包括：

在确定所述目标实体具有获取用户标识的权限的情况下，通过第一密钥响应消息，向所述第一代理实体发送第一待定密钥信息和所述用户设备对应的第二用户标识。

53、根据权利要求 52 所述的方法，其特征在于，所述第二用户标识为所述用户设备对应的用户永久标识 SUPI。

54、根据权利要求 48 所述的方法，其特征在于，所述接收第一代理实体发送的第二权限请求参数包括：

通过第二密钥请求消息，接收第一代理实体发送的所述第二权限请求参数；所述第二密钥请求消息用于指示所述第三实体获取第一待定密钥信息；

所述将所述第一待定密钥信息发送至所述第一代理实体包括：

通过第二密钥响应消息，向所述第一代理实体发送所述第一待定密钥信息。

55、根据权利要求 48 所述的方法，其特征在于，在将所述第一待定密钥信息发送至所述第一代理实体之后，所述方法还包括：

接收所述第一代理实体发送的第三权限请求参数；

根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限；

向所述第一代理实体发送授权结果参数；所述授权结果参数用于通知所述第一代理实体所述用户设备与所述目标实体是否具有第二通信权限。

56、根据权利要求 55 所述的方法，其特征在于，所述第三权限请求参数包括所述密钥标识 A-KID、第二目标实体标识和所述第一代理实体对应的代理实体标识，所述第二目标实体标识为所述用户设备根据目标实体的第一目标实体标识获取的受保护的实体标识；所述根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限包括以下一项或多项：

根据所述密钥标识 A-KID 和所述第二目标实体标识，确定所述用户设备对所述目标实体是否具有访问权限；

根据所述代理实体标识和所述第二目标实体标识，确定所述第一代理实体对所述目标实体是否具有代理权限；

根据所述密钥标识 A-KID 和所述第二目标实体标识，确定所述目标实体对所述用户设备的用户标识是否具有获取权限。

57、根据权利要求 53 所述的方法，其特征在于，所述接收所述第一代理实体发送的第三权限请求参数包括：

通过第三密钥请求消息，接收第一代理实体发送的所述第三权限请求参数；所述第三密钥请求消息用于指示所述第三实体获取授权结果参数和所述用户设备的用户标识；

所述向所述第一代理实体发送授权结果参数包括：

通过第三密钥响应消息，向所述第一代理实体发送授权结果参数。

58、根据权利要求 57 所述的方法，其特征在于，所述第三密钥请求消息还包括授权指示参数，所述授权指示参数用于指示所述第三实体根据所述第三密钥请求消息确定所述用户设备与所述目标实体是否具有第二通信权限。

59、根据权利要求 57 所述的方法，其特征在于，所述通过第三密钥响应消息，向所述第一代理实体发送授权结果参数包括：

在确定所述目标实体具有获取用户标识的权限的情况下，通过第三密钥响应消息，向所述第一代理实体发送授权结果参数和所述用户设备对应的第二用户标识。

60、根据权利要求 59 所述的方法，其特征在于，所述第二用户标识为所述用户设备对应的用户永久标识 SUPI。

61、根据权利要求 53 所述的方法，其特征在于，所述接收所述第一代理实体发送的第三权限请求参数包括：

通过第四密钥请求消息，接收第一代理实体发送的所述第三权限请求参数；所述第四密钥请求消息用于指示所述第三实体获取授权结果参数；

所述将所述授权结果参数发送至所述第一代理实体包括：

通过第四密钥响应消息，向所述第一代理实体发送所述授权结果参数。

62、根据权利要求 55 所述的方法，其特征在于，在根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限之前，所述方法还包括：

根据第一预设策略确定所述第三实体是否具有为第一代理实体服务的权限；

所述根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限包括：

在所述第三实体是否具有为第一代理实体服务的权限的情况下，根据所述第三权限请求参数确定所述用户设备与所述目标实体是否具有第二通信权限。

63、根据权利要求 48 所述的方法，其特征在于，在根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限之前，所述方法还包括：

根据第一预设策略确定所述第三实体是否具有为第一代理实体服务的权限；

所述根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限包括：

在所述第三实体是否具有为第一代理实体服务的权限的情况下，根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限。

64、根据权利要求 48 至 63 中任一项所述的方法，其特征在于，所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体；所述第三实体包括：AKMA 锚点功能 AAnF 实体。

65、根据权利要求 48 至 63 中任一项所述的方法，其特征在于，所述第一实体包括：3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

66、一种认证方法，其特征在于，应用于一个或多个第一实体中的目标实体，所述方法包括：

获取第一代理实体对用户设备的认证结果，所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示所述用户设备与所述目标实体具有第一通信权限；所述第二认证结果用于指示所述用户设备与所述目标实体具有第二通信权限；所述第一实体包括提供应用功能的实体，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

根据所述认证结果与用户设备进行通信。

67、根据权利要求 66 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域内的可信的提供应用功能的实体的情况下，所述获取第一代理实体对用户设备的认证结果包括：

接收所述第一代理实体发送的第一通知消息，所述第一通知消息包括所述第一认证结果；或者，

接收所述第一代理实体发送的第三通知消息，所述第三通知消息包括所述第二认证结果。

68、根据权利要求 67 所述的方法，其特征在于，所述第一通知消息或所述第三通知消息中还包括所述用户设备对应的第二用户标识。

69、根据权利要求 68 所述的方法，其特征在于，所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

70、根据权利要求 66 所述的方法，其特征在于，在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，所述获取第一代理实体对用户设备的认证结果包括：

接收所述第二实体发送的第五通知消息；其中，所述第五通知消息包括所述第一认证结果，所述第五通知消息为所述第二实体响应于接收到所述第二通知消息后发送的消息；或者，

接收所述第二实体发送的第六通知消息；其中，所述第六通知消息包括所述第二认证结果，所述第五通知消息为所述第二实体响应于接收到所述第四通知消息后发送的消息。

71、根据权利要求 70 所述的方法，其特征在于，所述第五通知消息或所述第六通知消息中还包括所述用户设备的第一用户标识。

72、根据权利要求 71 所述的方法，其特征在于，所述第一用户标识为所述用户设备对应的通用公共用户标识 GPSI。

73、根据权利要求 66 至 72 中任一项所述的方法，其特征在于，所述第一代理实体包括 3GPP 运营商域内的可信的认证代理 AP 实体。

74、根据权利要求 66 至 72 中任一项所述的方法，其特征在于，所述第一实体包括：

3GPP 运营商域内的可信的应用功能 AF 实体，或者，3GPP 运营商域内的可信的应用服务器 SCS/AS 实体，或者，3GPP 运营商域外的非可信的应用功能 AF 实体，或者，3GPP 运营商域外的非可信的应用服务器 SCS/AS 实体。

75、一种认证方法，其特征在于，应用于第二实体，所述方法包括：

获取第一代理实体对用户设备的认证结果；所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示用户设备与目标实体具有第一通信权限；所述第二认证结果用于指示用户设备与目标实体具有第二通信权限；所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

将所述认证结果发送至所述目标实体，以便所述目标实体根据所述认证结果与用户设备进行通信。

76、根据权利要求 75 所述的方法，其特征在于，所述获取第一代理实体对用户设备的认证结果包括：

接收所述第一代理实体发送的第二通知消息；所述第二通知消息为所述第一代理实体在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，根据所述第一认证结果向所述第二实体发送的消息；

根据所述第二通知消息获取所述第一认证结果；

所述将所述认证结果发送至所述目标实体包括：

根据所述第一认证结果向所述目标实体发送第五通知消息。

77、根据权利要求 76 所述的方法，其特征在于，在所述第二通知消息中包括所述用户设备对应的第二用户标识的情况下，所述根据所述第一认证结果向所述目标实体发送第五通知消息包括：

根据所述第二用户标识获取所述用户设备对应的第一用户标识；

根据所述第一认证结果和所述第一用户标识，向所述目标实体发送第五通知消息。

78、根据权利要求 77 所述的方法，其特征在于，所述第一用户标识为所述用户设备对应的通用公共用户标识 GPSI；所述第二用户标识包括所述用户设备对应的用户永久标识 SUPI。

79、根据权利要求 75 所述的方法，其特征在于，所述获取第一代理实体对用户设备的认证结果包括：

接收所述第一代理实体发送的第四通知消息；所述第四通知消息为所述第一代理实体在所述目标实体为 3GPP 运营商域外的非可信的提供应用功能的实体的情况下，根据所述第二认证结果向所述第二实体发送的消息；

根据所述第二通知消息获取所述第二认证结果；

所述将所述认证结果发送至所述目标实体包括：

根据所述第二认证结果向所述目标实体发送第六通知消息。

80、根据权利要求 79 所述的方法，其特征在于，在所述第四通知消息中包括所述用户设备对应的第二用户标识的情况下，所述根据所述第二认证结果向所述目标实体发送

第六通知消息包括：

根据所述第二用户标识获取所述用户设备对应的第一用户标识；
根据所述第二认证结果和所述第一用户标识，向所述目标实体发送第六通知消息。

81、根据权利要求 66 至 80 中任一项所述的方法，其特征在于，所述第二实体包括：网络开放功能 NEF 实体或业务能力开放功能 SCEF 实体。

82、一种认证装置，其特征在于，应用于用户设备，所述装置包括：

目标实体确定模块，被配置为从一个或多个第一实体中，确定请求通信的目标实体；

参数确定模块，被配置为根据所述目标实体确定第一权限请求参数；

第一消息发送模块，被配置为根据所述第一权限请求参数向第一代理实体发送应用会话建立请求消息；所述应用会话建立请求消息用于指示所述第一代理实体根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第一消息接收模块，被配置为响应于接收到所述第一代理实体发送的应用会话建立响应消息，确定所述用户设备与所述目标实体是否具有第一通信权限；

认证模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，通过所述第一代理实体进行身份认证。

83、一种认证装置，其特征在于，应用于第一代理实体，所述装置包括：

第一代理接收模块，被配置为接收用户设备发送的应用会话建立请求消息；所述应用会话建立请求消息包括第一权限请求参数，所述应用会话建立请求消息用于指示所述第一代理实体根据第一权限请求参数确定所述用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第一代理确定模块，被配置为根据所述第一权限请求参数确定所述用户设备与所述目标实体是否具有第一通信权限；

第一代理发送模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，向用户设备发送应用会话建立响应消息，以及，对所述用户设备进行身份认证。

84、一种认证装置，其特征在于，应用于第三实体，所述装置包括：

第三接收模块，被配置为接收第一代理实体发送的第二权限请求参数；所述第二权限请求参数用于指示第三实体确定用户设备与目标实体是否具有第一通信权限，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能，所述第三实体包括提供 AKMA 授权及应用密钥推演功能的实体；

第三确定模块，被配置为根据所述第二权限请求参数，确定所述用户设备与所述目标实体是否具有第一通信权限；

第三密钥模块，被配置为在所述用户设备与所述目标实体具有第一通信权限的情况下，获取第一待定密钥信息；

第三发送模块，被配置为将所述第一待定密钥信息发送至所述第一代理实体。

85、一种认证装置，其特征在于，应用于一个或多个第一实体中的目标实体，所述装置包括：

第一通信模块，被配置为获取第一代理实体对用户设备的认证结果，所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示所述用户设备与所述目标实体具有第一通信权限；所述第二认证结果用于指示所述用户设备与所述目标实体具有第二通信权限；所述第一实体包括提供应用功能的实体，所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；根据所述认证结果与用户设备进行通信。

86、一种认证装置，其特征在于，应用于第二实体，所述装置包括：

第二接收模块，被配置为获取第一代理实体对用户设备的认证结果；所述认证结果包括第一认证结果或第二认证结果，所述第一认证结果用于指示用户设备与目标实体具有第一通信权限；所述第二认证结果用于指示用户设备与目标实体具有第二通信权限；所述目标实体为所述用户设备从一个或多个第一实体中确定的请求通信的实体，所述第一实体包括 3GPP 运营商域外的非可信的提供应用功能的实体，所述第一代理实体包括 3GPP 运营商域内的可信的提供认证功能的实体，所述第一代理实体为所述第一实体提供认证代理功能；

第二发送模块，被配置为将所述认证结果发送至所述目标实体，以便所述目标实体根据所述认证结果与用户设备进行通信。

87、一种认证装置，其特征在于，所述装置包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行权利要求 1 至 13 中任一项所述方法的步骤，或者，所述处理器被配置为执行权利要求 14 至 47 中任一项所述方法的步骤，或者，所述处理器被配置为执行权利要求 48 至 65 中任一项所述方法的步骤，或者，所述处理器被配置为执行权利要求 66 至 74 中任一项所述方法的步骤，或者，所述处理器被配置为执行权利要求 75 至 81 中任一项所述方法的步骤。

88、一种计算机可读存储介质，其上存储有计算机程序指令，其特征在于，所述计算机程序指令被处理器执行时实现权利要求 1 至 13 中任一项所述方法的步骤，或者，所述计算机程序指令被处理器执行时实现权利要求 14 至 47 中任一项所述方法的步骤，或者，所述计算机程序指令被处理器执行时实现权利要求 48 至 65 中任一项所述方法的步骤，或者，所述计算机程序指令被处理器执行时实现权利要求 66 至 74 中任一项所述方法的步骤，或者，所述计算机程序指令被处理器执行时实现权利要求 75 至 81 中任一项所述方法的步骤。

89、一种芯片，其特征在于，包括处理器和接口；所述处理器用于读取指令以执行权利要求 1 至 13 中任一项所述方法的步骤，或者，所述处理器用于读取指令以执行权利要求 14 至 47 中任一项所述方法的步骤，或者，所述处理器用于读取指令以执行权利要求 48 至 65 中任一项所述方法的步骤，或者，所述处理器用于读取指令以执行权利要求 66 至 74 中任一项所述方法的步骤，或者，所述处理器用于读取指令以执行权利要求 75 至 81 中任一项所述方法的步骤。