(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2021 年 3 月 4 日 (04.03.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/036627 A1

(51) 国际专利分类号:
H04W 12/02 (2009.01)

(21) 国际申请号: PCT/CN2020/104598

(22) 国际申请日: 2020 年 7 月 24 日 (24.07.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910795258.8 2019年8月27日 (27.08.2019) CN
202010256020.0 2020年4月2日 (02.04.2020) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 李飞 (LI, Fei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。张博 (ZHANG, Bo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。何承东 (HE, Chengdong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,

(54) **Title:** COMMUNICATION SYSTEM, METHOD, AND APPARATUS

(54) **发明名称:** 一种通信系统、方法及装置

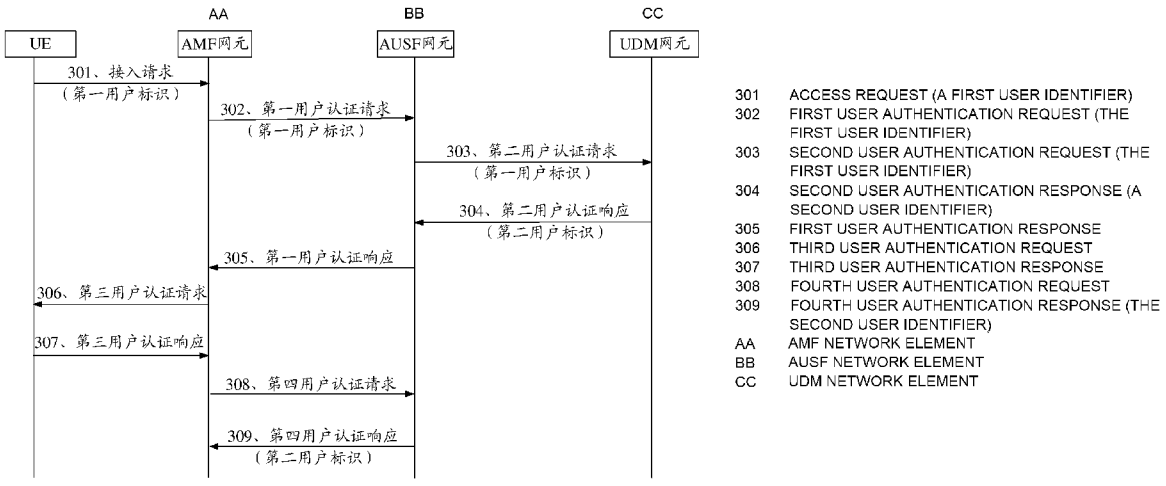

图 3

(57) **Abstract:** A communication system, method, and apparatus, relating to the technical field of communications. The communication system comprises a mobile management network element, an authentication service network element, and a data management network element. A terminal device is used for sending an access request to the mobile management network element, and the access request comprises a first user identifier; the mobile management network element is used for sending a first user authentication request to the authentication service network element in response to the access request, and the first user authentication request comprises the first user identifier; the authentication service network element is used for sending a second user authentication request to the data management network element in response to the first user authentication request, and the second user authentication request comprises the first user identifier; the data management network element is used for returning a second user authentication response to the authentication service network element in response to the second user authentication request, the second user authentication response comprises a

WO 2021/036627 A1

[见续页]

MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

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

本国际公布:

— 包括国际检索报告(条约第21条(3))。

second user identifier, and the second user identifier is an anonymization identity identifier of the terminal device. According to the technical solution, the second user identifier is introduced, thereby facilitating improving the security and reliability of communication.

(57) 摘要：一种通信系统、方法及装置，涉及通信技术领域。其中，该通信系统包括移动管理网元、认证服务网元和数据管理网元；终端设备用于向移动管理网元发送接入请求；接入请求包括第一用户标识；移动管理网元用于响应于接入请求，向认证服务网元发送第一用户认证请求；第一用户认证请求包括第一用户标识；认证服务网元用于响应于第一用户认证请求，向数据管理网元发送第二用户认证请求，第二用户认证请求包括第一用户标识；数据管理网元用于响应于第二用户认证请求，向认证服务网元返回第二用户认证响应，第二用户认证响应包括第二用户标识；第二用户标识为终端设备的匿名化身份标识。这种技术方案通过引入第二用户标识，有助于提高通信的安全性和可靠性。

一种通信系统、方法及装置

相关申请的交叉引用

本申请要求在2019年08月27日提交中国专利局、申请号为201910795258.8、申请名称为“一种通信系统、方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中；本申请要求在2020年04月02日提交中国专利局、申请号为202010256020.0、申请名称为“一种通信系统、方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，特别涉及一种通信系统、方法及装置。

背景技术

第五代（5th generation，5G）通信中，通常用户永久标识符（subscription permanent identifier，SUPI）应用于密钥 KAMF 的计算，因此 SUPI 属于敏感信息。而核心网中的各网元之间通信是采用用户永久标识符（subscription permanent identifier，SUPI）标识终端设备的，如果核心网中网元被攻击或网元中的数据被盗取，容易导致 SUPI 泄露，影响用户通信隐私性。

发明内容

本申请实施例提供一种通信系统、方法及装置，有助于提高通信的安全性和可靠性。

第一方面，本申请实施例提供的一种通信系统，包括移动管理网元、认证服务网元和数据管理网元；

终端设备用于向所述移动管理网元发送接入请求；所述接入请求包括第一用户标识，所述第一用户标识是对 SUPI 加密得到的，所述 SUPI 为所述终端设备的身份标识；

所述移动管理网元用于响应于所述接入请求，向所述认证服务网元发送第一用户认证请求；所述第一用户认证请求包括所述第一用户标识；

所述认证服务网元用于响应于所述第一用户认证请求，向所述数据管理网元发送第二用户认证请求，所述第二用户认证请求包括所述第一用户标识；

所述数据管理网元用于响应于所述第二用户认证请求，向所述认证服务网元返回第二用户认证响应，所述第二用户认证响应包括第二用户标识；所述第二用户标识为所述终端设备的匿名化身份标识；

所述认证服务网元还用于响应于所述第二用户认证响应，向所述移动管理网元返回第一用户认证响应。

本申请实施例通过引入第二用户标识，使得核心网中各网元可以通过第二用户标识标识终端设备，而第二用户标识为终端设备的匿名化身份标识，与现有技术中核心网中各网元通过 SUPI 标识终端设备相比，有助于提高通信的安全性和可靠性。

在一种可能的设计中，所述第一用户认证响应还包括所述第二用户标识。有助于简化移动管理网元获取第二用户标识的方式。

在一种可能的设计中，所述移动管理网元还用于响应于所述第一用户认证响应，从所述认证服务网元获取所述第二用户标识。便于移动管理网元获取第二用户标识。

在一种可能的设计中，所述第一用户认证请求还包括第一指示信息，则所述认证服务网元响应于所述第一用户认证请求，向所述数据管理网元发送的所述第二用户认证请求还包括所述第一指示信息；所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。有助于数据管理网元确定服务网络支持用户匿名化处理，从而返回第二用户标识。

需要说明的是，所述移动管理网元支持用户身份匿名化处理，还可以理解为：所述移动管理网元所在的网络支持用户身份匿名化处理，其中，所述移动管理网络所在的网络为终端设备请求接入的网络，用于为终端设备提供服务。其中该网络可以称之为服务网络。

在一种可能的设计中，所述第二用户认证响应还包括第二指示信息，则所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回的所述第一用户认证响应还包括所述第二指示信息；所述第二指示信息用于指示所述数据管理网元支持用户身份匿名化处理。有助于移动管理网元确定归属网络支持用户身份匿名化处理，从而获取第二用户标识。

需要说明的是，所述数据管理网元支持用户身份匿名化处理，还可以理解为：所述数据管理网元所在的网络支持用户身份匿名化处理，其中，所述数据管理网络所在的网络为用于提供终端设备注册相关信息（例如注册状态等）的网络。其中该网络可以称之为归属网络。

在一种可能的设计中，所述通信系统还包括第一网元；

所述数据管理网元还用于：向所述第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述第一用户标识，以及接收所述第一网元返回的所述第二用户标识；所述第一网元用于响应于所述匿名化用户标识获取请求，对所述第一用户标识解密，以得到所述 SUPI；根据所述 SUPI，获取所述第二用户标识，以及向所述数据管理网元返回所述第二用户标识。有助于简化实现方式。

在一种可能的设计中，所述通信系统还包括第一网元；

所述数据管理网元还用于：对所述第一用户标识解密，以得到所述 SUPI，并向所述第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述 SUPI，以及接收所述第一网元返回的所述第二用户标识；所述第一网元用于响应于所述匿名化用户标识获取请求，根据所述 SUPI，获取所述第二用户标识，以及向所述数据管理网元返回所述第二用户标识。有助于简化实现方式。

在一种可能的设计中，所述认证服务网元还用于：向所述第一网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；并接收所述第一网元返回的密钥 K_{AMF}，以及向所述移动管理网元发送所述密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥；所述第一网元用于响应于所述密钥获取请求，根据所述第二用户标识，生成所述密钥 K_{AMF}，并向所述认证服务网元返回所述密钥 K_{AMF}；所述移动管理网元还用于：接收所述认证服务网元发送的所述密钥 K_{AMF}。以便于移动管理网元能够通过密钥 K_{AMF} 实现与终端设备之间的安全通信。

在一种可能的设计中，所述第一网元用于根据所述第二用户标识获取所述 SUPI，并根据所述 SUPI 生成所述密钥 K_{AMF}。以便于移动管理网元能够通过密钥 K_{AMF} 实现与终端设备之间的安全通信。

在一种可能的设计中，所述移动管理网元，还用于向所述认证服务器发送第一参数；所述认证服务网元，还用于向所述第一网元发送所述第一参数；所述第一网元用于根据所述 SUPI 和所述第一参数生成所述密钥 K_{AMF}。有助于简化密钥 K_{AMF} 的生成方式。

在一种可能的设计中，所述数据管理网元还用于对所述第一用户标识解密，以得到所述 SUPI；根据所述 SUPI，获取所述第二用户标识。有助于简化实现方式。

在一种可能的设计中，所述移动管理网元还用于：根据所述第二用户标识，生成密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥。有助于简化实现方式。

在一种可能的设计中，所述认证服务网元还用于向所述数据管理网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；并接收所述数据管理网元返回的密钥 K_{AMF}，以及向所述移动管理网元发送所述密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥；所述数据管理网元，还用于响应于所述密钥获取请求，根据所述第二用户标识，生成所述密钥 K_{AMF}，并向所述认证服务网元返回所述密钥 K_{AMF}；所述移动管理网元还用于接收所述认证服务网元发送的所述密钥 K_{AMF}。有助于简化实现方式。

第二方面，本申请实施例提供的一种通信方法，所述方法包括：

移动管理网元接收到终端设备发送的接入请求，所述接入请求包括第一用户标识，所述第一用户标识是对 SUPI 加密得到的，所述 SUPI 为所述终端设备的身份标识；所述移动管理网元响应于所述接入请求，向所述认证服务网元发送第一用户认证请求，所述第一用户认证请求包括所述第一用户标识；所述移动管理网元接收认证服务网元响应于所述第一用户认证请求，返回的第一用户认证响应；

其中，所述第一用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识；或者，所述移动管理网元响应于所述第一用户认证响应，从所述认证服务网元获取所述第二用户标识。

在一种可能的设计中，所述第一用户认证请求还包括第一指示信息，所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。

在一种可能的设计中，第一用户认证响应还包括第二指示信息，所述第二指示信息用于指示所述数据管理网元支持用户身份匿名化处理。

在一种可能的设计中，所述移动管理网元根据所述第二用户标识，生成密钥 K_{AMF}；或者，所述移动管理网元接收所述认证服务网元返回的密钥 K_{AMF}；

所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥。

在一种可能的设计中，所述移动管理网元还向所述认证服务网元发送第一参数；所述第一参数用于生成所述密钥 K_{AMF}。

第三方面，本申请实施例提供的另一种通信方法，所述方法包括：

认证服务网元接收到移动管理网元发送的第一用户认证请求；所述第一用户认证请求包括第一用户标识，所述第一用户标识是对 SUPI 加密得到的，所述 SUPI 为终端设备的身份标识；所述认证服务网元响应于所述第一用户认证请求，向数据管理网元发送第二用户认证请求，所述第二用户认证请求包括所述第一用户标识；所述认证服务网元接收到所述数据管理网元响应于所述第二用户认证请求，返回的第二用户认证响应，所述第二用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识；所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回第一用户认证响应。

在一种可能的设计中，所述第一用户认证响应包括所述第二用户标识。

在一种可能的设计中，所述第一用户认证请求还包括第一指示信息，则所述认证服务网元响应于所述第一用户认证请求，向所述数据管理网元发送的所述第二用户认证请求还包括所述第一指示信息；所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。

在一种可能的设计中，所述第二用户认证响应还包括第二指示信息，则所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回的所述第一用户认证响应还包括所述第二指示信息；所述第二指示信息用于指示所述数据管理网元支持用户身份匿名化处理。

在一种可能的设计中，所述认证服务网元向第一网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；所述认证服务网元接收所述第一网元响应于所述密钥获取请求，返回的密钥 K_{AMF}，所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥 K_{AMF}；所述认证服务网元向所述移动管理网元发送的所述密钥 K_{AMF}。

在一种可能的设计中，所述认证服务网元接收所述移动管理网元发送的第一参数，并将所述第一参数发送给所述第一网元，所述第一参数用于生成所述密钥 K_{AMF}。

在一种可能的设计中，所述认证服务网元向所述数据管理网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；并接收所述数据管理网元响应于所述密钥获取请求返回的密钥 K_{AMF}，向所述移动管理网元发送的所述密钥 K_{AMF}，所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥 K_{AMF}。

第四方面，本申请实施例提供的另一种通信方法，所述方法包括:

数据管理网元接收到认证服务网元发送的第二用户认证请求，所述第二用户认证请求包括第一用户标识，所述第一用户标识是对 SUPI 加密得到的，所述 SUPI 为终端设备的身份标识；所述数据管理网元响应于所述第二用户认证请求，向所述认证服务网元返回第二用户认证响应，所述第二用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识。

在一种可能的设计中，所述数据管理网元向第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述第一用户标识；所述数据管理网元接收所述第一网元响应于所述匿名化用户标识获取请求返回的所述第二用户标识。

在一种可能的设计中，所述数据管理网元对所述第一用户标识解密，以得到所述 SUPI，并向第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述 SUPI；所述数据管理网元接收所述第一网元响应于所述匿名化用户标识获取请求返回的所述第二用户标识。

在一种可能的设计中，所述数据管理网元对所述第一用户标识解密，以得到所述 SUPI；并根据所述 SUPI，获取所述第二用户标识。

在一种可能的设计中，所述数据管理网元接收到所述认证服务网元发送的密钥获取请求，所述密钥获取请求包括第二用户标识；所述数据管理网元响应于所述密钥获取请求，向所述认证服务网元返回密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥。

第五方面，本申请提供的另一种通信方法，所述方法包括:

第一网元接收到数据管理网元发送的匿名化用户标识获取请求，所述匿名化用户标识获取请求包括第一用户标识或者 SUPI；所述第一用户标识是对所述 SUPI 加密得到的，所

述 SUPI 为终端设备的身份标识；所述第一网元响应于所述匿名化用户标识获取请求向数据管理网元返回所述第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识。

在一种可能的设计中，所述第一网元根据所述 SUPI，获取所述第二用户标识，所述 SUPI 是从所述匿名化用户标识获取请求中得到的，或者对所述第一用户标识解密得到的。

在一种可能的设计中，所述第一网元接收到认证服务网元发送的密钥获取请求，所述密钥获取请求包括所述第二用户标识；所述第一网元响应于所述密钥获取请求，根据所述第二用户标识，生成密钥 K_{AMF}，并向所述认证服务网元返回所述密钥 KAMF；所述密钥 KAMF 为所述终端设备与移动管理网元之间的密钥。

在一种可能的设计中，所述第一网元接收认证服务网元发送的第一参数；所述第一参数是移动管理网元发送给所述认证服务网元的；所述第一参数用于生成所述密钥 K_{AMF}。

第五方面，本申请提供的另一种通信系统，包括移动管理网元、认证服务网元和数据管理网元；

所述终端设备用于向所述移动管理网元发送接入请求；所述接入请求包括第一用户标识，所述第一用户标识是对 SUPI 加密得到的，所述 SUPI 为所述终端设备的身份标识；

所述移动管理网元用于响应于所述接入请求，向所述认证服务网元发送第一用户认证请求；所述第一用户认证请求包括所述第一用户标识；

所述认证服务网元用于响应于所述第一用户认证请求，向所述数据管理网元发送第二用户认证请求，所述第二用户认证请求包括所述第一用户标识；

所述数据管理网元用于响应于所述第二用户认证请求，向所述认证服务网元返回第二用户认证响应，所述第二用户认证响应中包括第二用户标识；

所述认证服务网元还用于接收到所述第二用户认证响应，向所述移动管理网元返回第一用户认证响应；示例的，第一用户认证响应包括第二用户标识。

所述移动管理网元还用于响应于所述第一用户认证响应，向所述终端设备发送第三用户认证请求，所述第三用户认证请求包括所述第一用户标识；

所述终端设备还用于响应于所述第三用户认证请求，根据 SUPI 得到所述第二用户标识，并根据所述第二用户标识，生成密钥 K_{AMF}；然后向所述移动管理网元返回第三用户认证响应；所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥；

所述移动管理网元还用于响应于所述第三用户认证响应，向所述认证服务网元发送第四用户认证请求；

所述认证服务网元响应于第四用户认证请求，向所述移动管理网元返回第四用户认证响应，所述第四用户认证响应包括所述第二用户标识；

所述移动管理网元响应于第四用户认证响应，根据所述第二用户标识，生成所述密钥 K_{AMF}。

第六方面，本申请实施例的通信装置，该装置可以是平台上实例化的虚拟化功能，也可以是硬件设备或硬件设备中的网络元件等。该装置具有实现上述各方面以及各方面可能设计的技术方案的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

在一种可能的设计中，该装置包括处理单元和通信单元，处理单元例如可以是处理器，通信单元例如可以是收发器，收发器可以包括射频电路。例如，处理单元用于响应于接入请求，触发通信单元向认证服务单元发送第一用户认证请求；再例如处理单元用于响应于

第一用户认证请求，触发通信单元向数据管理单元发送第二用户认证请求等。

在另一种可能的设计中，该装置包括处理器和存储器，其中存储器用于存储程序，处理器用于调用存储器中存储的程序，以实现各方面以及各方面任意一项可能的设计中消息保护的方法。需要说明的是，处理器可以通过输入/输出接口、管脚或电路等发送或者接收数据。存储器可以为芯片内的寄存器、缓存等。此外，存储器还可以是终端设备内的位于芯片外部的存储单元，如只读存储器（read-only memory，ROM)、可存储静态信息和指令的其他类型的静态存储设备、随机存取存储器（random access memory，RAM)等。

其中，上述任一处提到的处理器，可以是一个通用的中央处理器（central processing unit，CPU），微处理器，特定应用集成电路（application-specific integrated circuit，ASIC)，或一个或多个用于控制执行上述各方面或者各方面任意一项可能设计的消息保护的方法的程序的集成电路。

第七方面，本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有程序，当该程序在计算机上运行时，使得计算机执行上述各方面所述的方法。

第八方面，本申请还提供一种包含程序的计算机程序产品，当其在计算机上运行时，使得计算机执行上述各方面所述的方法。

另外，第二方面至第九方面中任一种可能设计方式所带来的技术效果可参见第一方面中不同设计方式所带来的技术效果，此处不再赘述。

附图说明

图 1 为本申请实施例的一种通信系统的架构示意图；

图 2 为本申请实施例的另一通信系统的架构示意图；

图 3 为本申请实施例的一种通信方法的流程示意图；

图 4 为本申请实施例的另一通信方法的流程示意图；

图 5 为本申请实施例的另一通信方法的流程示意图；

图 6 为本申请实施例的一种通信方法的流程示意图；

图 7 为本申请实施例的另一通信方法的流程示意图；

图 8 为本申请实施例的另一通信方法的流程示意图；

图 9 为本申请实施例的另一通信方法的流程示意图；

图 10 为本申请实施例的一通信装置的结构示意图；

图 11 为本申请实施例的另一通信装置的结构示意图；

图 12 为本申请实施例的另一通信方法的流程示意图；

图 13 为本申请实施例的另一通信方法的流程示意图；

图 14 为本申请实施例的另一通信方法的流程示意图；

图 15 为本申请实施例的另一通信方法的流程示意图。

具体实施方式

本申请实施例中“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“和/或”，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 的情况，其中 A、B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“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 和 b，a 和 c，b 和 c，或 a、b 和 c，其中 a、b、c 中的每一个本身可以是元素，也可以是包含一个或多个元素的集合。

在本申请中，“示例的”“在一些实施例中”“在另一些实施例中”等用于表示作例子、例证或说明。本申请中被描述为“示例”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用示例的一词旨在以具体方式呈现概念。

本申请中“的（of）”，“相应的（corresponding，relevant）”和“对应的(corresponding)”有时可以混用，应当指出的是，在不强调其区别时，其所要表达的含义是一致的。本申请实施例中通信、传输有时可以混用，应当指出的是，在不强调区别是，其所表达的含义是一致的。例如传输可以包括发送和/或接收，可以为名词，也可以是动词。

需要指出的是，本申请实施例中涉及的“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

为解决背景技术提到的问题，本申请提供一种通信系统，如图 1 所示，该通信系统包括移动管理网元、认证服务网元、数据管理网元。此外，在一些实施例中该通信系统还包括第一网元。其中第一网元又可以命名为用户标识匿名化网元等，对第一网元的名称不作限定。

其中，移动管理网元、认证服务网元和数据管理网元为核心网中的网元。此外，对于终端设备来说，移动管理网元为服务网络中的网元，认证服务网元、数据管理网元、第一网元为归属网络中的网元。

示例地，移动管理网元用于在终端设备发起接入时，向认证服务网元发送第一用户认证请求，第一用户认证请求包括第一用户标识，该第一用户标识是对 SUPI 加密得到的，SUPI 为终端设备的身份标识；

认证服务网元用于响应于第一用户认证请求，向数据管理网元发送第二用户认证请求，第二用户认证请求包括第一用户标识；

数据管理网元用于响应于第二用户认证请求，向认证服务网元返回第二用户认证响应，第二用户认证响应包括第二用户标识，第二用户标识为终端设备的匿名化身份标识；

认证服务网元响应于第二用户认证响应，向移动管理网元返回第一用户认证响应。在一些实施例中，第一用户认证响应包括第二用户标识。或者，移动管理网元在接收到第一用户认证响应后，向认证服务网元获取第二用户标识。

在一些实施例中，第二用户标识可以是第一网元生成的，也可以是数据管理网元生成的。示例的，第二用户标识是第一网元生成的，数据管理网元用于响应于第一用户认证请求，向第一网元发送匿名化用户标识获取请求，第一网元用于响应于匿名化用户标识获取请求，向数据管理网元返回第二用户标识。数据管理网元在接收到第一网元返回的第二用户标识后，再向认证服务网元发送第二用户认证请求。例如，第一网元可以向数据管理网元返回匿名化用户标识获取响应，该匿名化用户标识获取响应中包括第二用户标识。

例如，匿名化用户标识获取请求包括第一用户标识，第一网元可以对第一用户标识解密，以得到 SUPI，并根据 SUPI，得到第二用户标识。再例如，匿名化用户标识获取请求包括 SUPI，第一网元可以根据 SUPI，得到第二用户标识。

示例的，第二用户标识是数据管理网元生成的，所述数据管理网元响应于第一用户认证请求，根据第一用户标识，得到第二用户标识，然后向认证服务网元返回第二用户认证

响应。例如，数据管理网元可以对第一用户标识解密，以得到 SUPI，然后根据 SUPI，得到第二用户标识。

本申请实施例通过引入第二用户标识，使得核心网中的各网元之间通信时可以通过第二用户标识标识终端设备，与现有技术中通过 SUPI 标识终端设备相比，有助于降低通信中用户隐私泄露的风险。

在一些实施例中，移动管理网元还可以用于通过认证服务网元向数据管理网元指示移动管理网元支持用户身份匿名化处理。示例的，移动管理网元向认证服务网元发送第一用户认证请求，第一用户认证请求包括第一用户标识和第一指示信息，第一指示信息用于指示移动管理网元支持用户身份匿名化处理。需要说明的是，移动管理网元支持用户身份匿名化处理，还可以理解为：移动管理网元所在的网络支持用户身份匿名化处理，其中，所述移动管理网络所在的网络为终端设备请求接入的网络，用于为终端设备提供服务。其中该网络可以称之为服务网络。认证服务网元接收到第一用户认证请求后，响应于第一用户认证请求，向数据管理网元发送第二用户认证请求，第二用户认证请求包括第一用户标识和第一指示信息，从而达到移动管理网元向数据管理网元指示终端设备的服务网络支持用户身份匿名化处理的目的。

在又一些实施例中，数据管理网元还可以用于通过认证服务网元向移动管理网元指示数据管理网元支持用户身份匿名化处理。示例的，数据管理网元用于响应于第二用户认证请求，向认证服务网元返回第二用户认证响应，第二用户认证响应包括第二用户标识和第二指示信息，第二指示信息用于指示数据管理网元支持用户身份匿名化处理。需要说明的是，数据管理网元支持用户身份匿名化处理，还可以理解为：数据管理网元所在的网络支持用户身份匿名化处理，其中，数据管理网络所在的网络为用于提供终端设备注册相关信息（例如注册状态等）的网络。其中该网络可以称之为归属网络。认证服务网元接收到第二用户认证响应，响应于该第二用户认证响应，向移动管理网元发送第一用户认证响应，第一用户认证响应包括第二指示信息，从而到达指示移动管理网元终端设备的归属网络支持用户身份匿名化处理的目的。

基于本申请实施例提供的通信系统，在不改变终端设备中生成密钥 K_{AMF} 的方式的情况下，为了避免移动管理网元根据第二用户标识从数据管理网元或第一网元获取 SUPI，来得到终端设备与移动管理网元之间的密钥 K_{AMF}，在一些实施例中，移动管理网元还可以用于根据第二用户标识，生成密钥 K_{AMF}，其中，移动管理网元根据第二用户标识，生成密钥 K_{AMF} 所使用的算法使得移动管理网元生成的密钥 K_{AMF} 与终端设备根据 SUPI 生成的密钥 K_{AMF} 相同。或者，在另一些实施例中，认证服务网元用于向第一网元发送密钥获取请求，密钥获取请求包括第二用户标识，第一网元用于响应于密钥获取请求，根据第二用户标识得到 SUPI，并根据 SUPI 得到密钥 K_{AMF}，然后将密钥 K_{AMF} 返回给认证服务网元，再由认证服务网元将密钥 K_{AMF} 发送给移动管理网元。或者，在又一些实施例中，认证服务网元用于向数据管理网元发送密钥获取请求，密钥获取请求包括第二用户标识，数据管理网元用于响应于密钥获取请求，根据第二用户标识得到 SUPI，并根据 SUPI 得到密钥 K_{AMF}，然后将密钥 K_{AMF} 返回给认证服务网元，再由认证服务网元将密钥 K_{AMF} 发送给移动管理网元。

示例的，第一网元可以根据第二用户标识和第一参数（例如 ABBA 参数等），得到密钥 K_{AMF}，例如，第一参数是由移动管理网元通过认证服务网元发送给第一网元的。例如

移动管理网元可以通过将第一参数携带在第一用户认证请求中发送给认证服务网元，再由认证服务网元将第一参数携带在第二用户认证请求中发送给数据管理网元。然后，由数据管理网元将第一参数携带在密钥获取请求中，发送给第一网元。

应理解，本申请实施例中的终端设备（terminal device），也可以称为用户设备（user equipment，UE），是一种具有无线收发功能的设备，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）。所述终端设备可以是手机（mobile phone）、平板电脑（pad）、带无线收发功能的电脑、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、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。以下将终端设备称之为UE进行介绍。

具体的，本申请实施例可以应用于5G通信系统中，也可以应用于其它通信系统中，比如第六代（6th generation，6G）通信系统等未来通信系统中。

示例的，如图2所示，为本申请实施例一种5G通信系统的网络架构的示意图。该5G通信系统的网络架构可以包括接入与移动性管理功能（access and mobility management function，AMF）网元、鉴权服务功能（authentication server function，AUSF)网元、统一数据管理（unified data management，UDM）网元、会话管理功能（session management function，SMF）网元、（无线）接入网（(radio)access network，(R)AN）以及用户面功能（user plane function，UPF）网元等。此外，5G通信系统的网络架构中还包括数据网络（data network，DN）、认证凭证存储和处理功能（Authentication Credential Repository and Processing Function，ARPF）网元、安全锚点功能（security anchor function，SEAF）网元、第一网元等。

RAN的主要功能是控制UE通过无线接入到移动通信网络。RAN是移动通信系统的一部分。它实现了一种无线接入技术。从概念上讲，它驻留某个设备之间（如移动电话、一台计算机，或任何远程控制机），并提供与其核心网的连接。RAN设备包括但不限于：5G中的(g nodeB，gNB)、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)、移动交换中心等，此外，还可以包括无线保真（wireless fidelity，wifi）接入点（access point，AP）等。

AMF网元负责UE的接入管理和移动性管理，在实际应用中，其包括了4G通信系统架构中移动管理实体（mobility management entity，MME）的移动性管理功能，并加入了接入管理功能。

AUSF网元具有鉴权服务功能，用于终结SEAF请求的认证功能。

UDM网元为控制面网元，负责存储签约用户的用户永久标识符(subscriber permanent identifier，SUPI)、信任状（credential）、安全上下文（security context）、用户签约数据等信息。UDM网元所存储的这些信息可用于UE接入5G网络的认证和授权。其中，上述签约用户具体可为使用5G网络提供的业务的用户。上述签约用户的SUPI可为该手机芯卡的号

码等。

SMF 网元负责会话管理，如用户的会话建立等。

UPF 网元是用户面的功能网元，主要负责连接外部网络，其包括了 4G 通信系统的网络架构中服务网关（serving gateway，S-GW）、分组数据网络网关（packet data network gateway，PDN gateway，P-GW）的相关功能。

DN 负责为 UE 提供服务的网络，如一些 DN 为终端设备提供上网功能，另一些 DN 为终端设备提供短信功能等等。

SEAF 网元于完成对 UE 的认证过程，在 5G 通信中，SEAF 的功能可以合并到 AMF 网元中。

ARPF 网元具有认证凭证存储和处理功能，用于存储 UE 的长期认证凭证，如永久密钥 K 等。在 5G 通信中，ARPF 网元的功能可以合并到 UDM 网元中。

可以理解的是，上述网元或者功能既可以是硬件设备中的网络元件，也可以是在专用硬件上运行软件功能，或者是平台(例如，云平台)上实例化的虚拟化功能。可选的，上述网元或者功能可以由一个设备实现，也可以由多个设备共同实现，还可以是一个设备内的一个功能模块，本申请实施例对此不作具体限定。

在本申请实施例中，图 1 中所示的移动管理网元可以为图 2 中所示的 AMF 网元，也可以为图 2 中未示出的 SEAF 网元，图 1 中所示的认证服务网元可以为图 2 中所示的 AUSF 网元，图 1 中所示的数据管理网元可以为图 2 中所示的 UDM 网元，也可以为图 2 中未示出的 ARPF 网元等。

为方便说明，以图 1 所示的 5G 通信系统的网络架构为例，对本申请实施例的通信方法进行详细说明。

示例的，如图 3 所示，为本申请实施例的一种通信方法的流程示意图，具体包括以下步骤。

301、UE 向 AMF 网元发送接入请求；接入请求包括第一用户标识，第一用户标识是对 SUPI 加密得到的，SUPI 为 UE 的身份标识。

在一些实施例中，第一用户标识可以用户隐藏标识（subscriber permanent identifier，SUCI），也可以对 SUPI 加密得到的不同于 SUCI 的用户标识，对此不作限定。

302、AMF 网元响应于接入请求，向 AUSF 网元发送第一用户认证请求；其中，该第一用户认证请求包括第一用户标识。

在一些实施例中，第一用户认证请求还包括第一指示信息，第一指示信息用于指示 AMF 网元支持用户身份匿名化处理。以达到通知 UDM 网元支持用户身份匿名或处理的目的，有助于简化实现方式。此外，AMF 网元还可以通过其它方式向 UDM 网元通知 AMF 网元支持用户身份匿名化处理，例如，AMF 网元可以将第一指示信息携带在自定义的消息中发送给 AUSF 网元，通过 AUSF 网元通知给 UDM 网元。其中，AMF 网元可以在发送第一用户认证请求之前或之后发送携带第一指示信息的自定义的消息，也可以同时发送第一用户认证请求、和携带第一指示信息的自定义的消息，对此不作限定。

303、AUSF 网元响应于第一用户认证请求，向 UDM 网元发送第二用户认证请求，第二用户认证请求包括第一用户标识。

在一些实施例中，第二用户认证请求还包括第一指示信息。例如，AUSF 网元在第一用户认证请求还包括第一指示信息时，则向 UDM 网元发送的第二用户认证请求还可以包

括第一指示信息，以指示 UDM 网元 AMF 网元支持用户身份匿名化处理。或者，AUSF 网元接收到其它包括第一指示信息的消息后，也可以在响应于第一用户认证请求，向 UDM 网元发送的第二用户认证请求中包括第一指示信息。第一指示信息的相关实现方式可以参见上述相关介绍，在此不再赘述。

304、UDM 网元响应于第二用户认证请求，向 AUSF 网元返回第二用户认证响应，第二用户认证响应中包括第二用户标识。第二用户标识为 UE 的匿名化身份标识。

其中，第二用户标识不同于 SUPI，可以与第一用户标识相同，也可以与第一用户标识不同，对此不作限定。

具体的，第二用户标识可以是由 UDM 网元得到的，也可以是由第一网元得到的。

在一些实施例中，UDM 网元响应于第二用户认证请求，根据第一用户标识，得到第二用户标识，然后向 AUSF 返回第二用户认证响应。例如，UDM 网元可以对第一用户标识解密，以得到 SUPI，然后根据 SUPI，得到第二用户标识。比如，UDM 网元根据对第一用户标识解密得到的 SUPI，从预先配置的 SUPI 和匿名化用户标识的对应关系中，查找第二用户标识。SUPI 和匿名化用户标识的对应关系可以通过协议预先定义，也可以通过其它方式预先配置在 UDM 中。再比如，UDM 网元还可以根据 SUPI，基于第一算法，得到第二用户标识，然后记录 SUPI 与第二用户标识的对应关系。第一算法可以是通过协议预定义的，也可以通过其它方式预配置的，如第二用户标识=f1（SUPI）。再例如，根据第一用户标识，基于预设算法，得到第二用户标识，如第二用户标识=f0（第一用户标识）。

在另一些实施例中，UDM 网元响应于第二用户认证请求，向第一网元发送匿名化用户标识获取请求，匿名化用户标识获取请求包括第一用户标识。第一网元响应于匿名化用户标识获取请求，向 UDM 网元返回第二用户标识，UDM 网元接收到第一网元返回的第二用户标识，再向 AUSF 网元返回第二用户认证响应。示例的，第一网元响应于匿名化用户标识获取请求，向 UDM 返回匿名化用户标识获取响应，匿名化用户标识获取响应包括第二用户标识。

需要说明的是，第一网元得到第二用户标识的具体实现方式可以参见 UDM 网元得到第二用户标识的方式，在此不再赘述。

在又另一些实施例中，UDM 网元响应于第二用户认证请求，对第一用户标识解密，得到 SUPI，并向第一网元发送匿名化用户标识获取请求，匿名化用户标识获取请求包括 SUPI。第一网元响应于匿名化用户标识获取请求，向 UDM 网元返回第二用户标识，UDM 网元接收到第一网元返回的第二用户标识，再向 AUSF 网元返回第二用户认证响应。需要说明的是，第一网元根据 SUPI 得到第二用户标识的具体实现方式可以参见 UDM 网元根据 SUPI 得到第二用户标识的方式，在此不再赘述。

在一些实施例中，第二用户认证响应还包括第二指示信息，第二指示信息用于指示 UDM 网元支持用户身份匿名化处理。以达到指示 AMF 网元 UDM 网元支持用户身份匿名化处理的目的。

305、AUSF 网元响应于第二用户认证响应，向 AMF 网元返回第一用户认证响应。示例的，第一用户认证响应包括第二用户标识。

在一些实施例中，AUSF 网元响应于的第二用户响应包括第二指示信息，则向 AMF 网元返回的第一用户认证响应也可以包括第二指示信息。

306、AMF 网元响应于第一用户认证响应，向 UE 发送第三用户认证请求。示例的，

第三用户认证请求用于向 UE 发起对网络的验证，例如，第三用户认证请求包括从 UDM 网元获取的网络的相关信息。

307、UE 响应于第三用户认证请求，向 AMF 网元返回第三用户认证响应。例如，UE 在对网络验证通过后，向 AMF 网元返回第三用户认证响应。再例如，UE 在对网络验证未通过时，不向 AMF 网元返回用户认证响应，也可以向 AMF 网元返回网络验证失败响应。

示例的，第三用户认证响应可以包括用于验证 UE 的相关信息，例如 RES、或 RES*。

308、AMF 网元响应于第三用户认证响应，向 AUSF 网元发送第四用户认证请求。示例的，第四用户认证请求用于发起对 UE 的验证。

309、AUSF 网元响应于第四用户认证请求，向 AMF 网元返回第四用户认证响应。示例的，第四用户认证响应包括第二用户标识。例如，AUSF 网元对 UE 验证通过后，向 AMF 网元返回第四用户认证响应。再例如，AUSF 网元对 UE 验证未通过时，可以不向 AMF 网元发送用户认证响应，也可以向 AMF 网元返回 UE 验证失败响应。

需要说明的是，第一用户认证响应包括第二用户标识时，第四用户认证响应可以不包括第二用户标识。或者，第四用户认证响应包括第二用户标识时，第一用户认证响应可以不包括第二用户标识。或者，第一用户认证响应和第四用户认证响应也可以均包括第二用户标识。

进一步的，在另一些实施例中，AUSF 网元响应于第四用户认证请求，向第一网元发送密钥获取请求，密钥获取请求包括第二用户标识。第一网元响应于密钥获取请求，向 AUSF 网元返回密钥 K_{AMF}。AUSF 网元接收到第一网元返回密钥 K_{AMF}，再向 AMF 网元返回第四用户认证响应。示例的，第四用户认证响应还包括密钥 K_{AMF}。从而使得 AMF 网元获取到密钥 K_{AMF}。示例的，第一网元可以根据第二用户标识，从预先配置的 SUPI 和匿名化用户标识对应关系，查找与第二用户标识对应的 SUPI，然后根据 SUPI，得到密钥 K_{AMF}。在一些实施例中，第一网元根据 SUPI 和第一参数，得到 K_{AMF}。其中，第一参数可以为 ABBA 参数，可以是 AMF 网元通过 AUSF 网元发送给第一网元的。例如，AMF 网元将第一参数携带在第四用户认证请求中发送给 AUSF 网元，AUSF 网元将第一参数携带在密钥获取请求中发送给第一网元。

示例的，根据 SUPI，得到密钥 K_{AMF} 的具体实现方式可以参见现有的得到密钥 K_{AMF} 的实现方式。

或者，AUSF 网元响应于第四用户认证请求，向 UDM 网元发送密钥获取请求，密钥获取请求包括第二用户标识。UDM 网元响应于密钥获取请求，向 AUSF 网元返回密钥 K_{AMF}。AUSF 网元接收到 UDM 网元返回密钥 K_{AMF}，再向 AMF 网元返回第四用户认证响应。示例的，第四用户认证响应还包括密钥 K_{AMF}。从而使得 AMF 网元获取到密钥 K_{AMF}。

需要说明的是，UDM 网元生成密钥 K_{AMF} 的具体实现方式，可以参见第一网元生成密钥 K_{AMF} 的具体实现方式，在此不再赘述。

或者，AMF 网元接收到第四用户认证响应后，根据第二用户标识，基于第二算法，得到密钥 K_{AMF}。

需要说明的是，上述实施例中 AMF 网元与 AUSF 网元之间用户认证请求又可以称之为 Nausf_UE Authentication_Authenticate Request，例如，第一用户认证请求和第四用户认证请求又可以称之为 Nausf_UE Authentication_Authenticate Request；AMF 网元与 AUSF 网

元之间的用户认证响应又可以称之为 Nausf_UE Authentication_Authenticate Response，例如，第一用户认证响应和第四用户认证响应。上述实施例中 AUSF 网元与 UDM 网元之间的用户认证请求又可以称之为 Nudm_UE Authentication_Get Request，例如第二用户认证请求；AUSF 网元与 UDM 网元之间的用户认证响应又可以称之为 Nudm_UE Authentication_Get Response，例如第二用户认证响应。上述实施例中 AMF 网元与 UE 之间的用户认证请求又可以称之为 Authentication-Request，例如第三用户认证请求；AUSF 网元与 UDM/ARPF 网元之间的用户认证响应又可以称之为 Authentication- Response，例如第三用户认证响应。本申请实施例对用户认证请求和用户认证响应的名称不作限定。

可以理解的是，图 3 所示的通信方法中还可以由 SEAF 网元执行 AMF 网元执行的步骤，和/或，由 ARPF 网元执行 UDM 网元执行的步骤。

以第二用户标识和密钥 K_{AMF} 是由第一网元得到的为例，示例的，本申请实施例的通信方法可以如图 4 所示，具体包括以下步骤。

401、UE 向 AMF 网元发送接入请求；接入请求包括 SUCI。

402、AMF 网元接收到接入请求，向 AUSF 网元发送 Nausf_UE Authentication_Authenticate Request1；Nausf_UE Authentication_Authenticate Request1 包括 SUCI 和指示信息 1，指示信息 1 用于指示 AMF 网元支持用户身份匿名化处理。

403、AUSF 网元接收到 Nausf_UE Authentication_Authenticate Request1，向 UDM 网元发送 Nudm_UE Authentication_Get Request，Nudm_UE Authentication_Get Request 包括 SUCI、和指示信息 1。

404、UDM 网元接收到 Nudm_UE Authentication_Get Request，在 UDM 网元支持用户身份匿名化处理时，向第一网元发送匿名化用户标识获取请求，该匿名化用户标识获取请求包括 SUCI。

405、第一网元接收到匿名化用户标识获取请求，对 SUCI 进行解密，得到 SUPI。然后根据 SUPI，从预先配置的 SUPI 与 SUPI*的对应关系中，得到与该 SUPI 对应的 SUPI*，并向 UDM 网元返回匿名化用户标识获取响应，该匿名化用户标识获取响应包括与 SUPI 对应的 SUPI*。

406、UDM 网元接收到匿名化用户标识获取响应，根据 SUPI*，从预先配置的 SUPI* 与用户签约数据的对应关系中，确定 UE 的用户签约数据，并根据用户签约数据，得到 XRES*，向 AUSF 网元返回 Nudm_UE Authentication_Get Response，该 Nudm_UE Authentication_Get Response 包括指示信息 2、SUPI*和 XRES*。指示信息 2 用于指示 UDM 网元支持用户身份匿名化处理。

407、AUSF 网元接收到 Nudm_UE Authentication_Get Response，向 AMF 网元返回 Nausf_UE Authentication_Authenticate Response1，Nausf_UE Authentication_Authenticate Response1 包括指示信息 2 和 XRES*。

408、AMF 网元接收到 Nausf_UE Authentication_Authenticate Response1，向 UE 发送 Authentication-Request。

409、UE 接收到 Authentication-Request，生成 RES*，并向 AMF 网元返回 Authentication-Response，Authentication-Response 包括 RES*。

410、AMF 网元接收到 Authentication-Response，判断 RES*和 XRES*相同，向 AUSF 网元发送 Nausf_UE Authentication_Authenticate Request2，Nausf_UE

Authentication_Authenticate Request2 包括 RES*。

411、AUSF 网元接收到 Nausf_UE Authentication_Authenticate Request2，根据 RES*，生成第一 HXRES*，判断第一 HXRES*与第二 HXRES*相同，向第一网元发送密钥获取请求，密钥获取请求包括 SUPI*和 ABBA 参数。示例的，密钥获取请求还可以包括 Kseaf 等。

示例的，ABBA 参数可以是 AMF 网元发送给 AUSF 网元的，例如，AMF 网元将 ABBA 参数携带在 Nausf_UE Authentication_Authenticate Request2 中发送给 AUSF 网元的，即 Nausf_UE Authentication_Authenticate Request2 还包括 ABBA 参数。

412、第一网元接收到密钥获取请求，根据 SUPI*，从预先配置的 SUPI*与 SUPI 的对应关系中，确定 UE 的 SUPI，并根据 SUPI 和 ABBA 参数，基于预设算法得到密钥 K_{AMF}，然后向 AUSF 网元返回密钥获取响应，该密钥获取响应包括 SUPI*和密钥 K_{AMF}。

413、AUSF 网元接收到密钥获取响应，向 AMF 网元返回 Nausf_UE Authentication_Authenticate Response2，Nausf_UE Authentication_Authenticate Response2 包括 SUPI*和密钥 K_{AMF}。

由于 UE 中也是根据 SUPI、ABBA 参数，基于预设算法，得到密钥 K_{AMF} 的，因此本申请实施例中可以基于密钥 K_{AMF} 实现 AMF 网元与 UE 的安全通信。

需要说明的是，第二用户标识和/或密钥 K_{AMF} 还可以由 UDM 网元得到。例如，第二用户标识由 UDM 网元得到，在这种情况下，将步骤 404~406 可以替换为：404A，UDM 网元接收到 Nudm_UE Authentication_Get Request，在 UDM 网元支持用户身份匿名化处理时，对 SUCI 解密，得到 SUPI，根据 SUPI，从预先配置的 SUPI 与 SUPI*的对应关系中，得到与该 SUPI 对应的 SUPI*，以及根据 SUPI，从预先配置的 SUPI 与用户签约数据的对应关系中，确定 UE 的用户签约数据，并根据用户签约数据，得到 XRES*，向 AUSF 网元返回 Nudm_UE Authentication_Get Response，该 Nudm_UE Authentication_Get Response 包括指示信息 2、SUPI*和 XRES*。

再例如，密钥 K_{AMF} 由 UDM 网元得到，在这种情况下，可以将步骤 411、步骤 412 中的第一网元替换为 UDM 网元。

再例如，第二用户标识和密钥 K_{AMF} 均是由 UDM 网元得到时，在这种情况下，将步骤 404~406 替换为：404B，UDM 网元接收到 Nudm_UE Authentication_Get Request，在 UDM 网元支持用户身份匿名化处理时，对 SUCI 解密，得到 SUPI；根据 SUPI，从预先配置的 SUPI 与 SUPI*的对应关系中，得到与该 SUPI 对应的 SUPI*，以及根据 SUPI，从预先配置的 SUPI 与用户签约数据的对应关系中，确定 UE 的用户签约数据，并根据用户签约数据，得到 XRES*；根据 SUPI，基于预设算法得到密钥 K_{AMF}，向 AUSF 网元返回 Nudm_UE Authentication_Get Response，该 Nudm_UE Authentication_Get Response 包括指示信息 2、SUPI*、XRES*和密钥 K_{AMF}。将步骤 411~413 可以替换为：411A、AUSF 网元接收到 Nausf_UE Authentication_Authenticate Request2，根据 RES*，生成第一 HXRES*，判断第一 HXRES*与第二 HXRES*相同，向 AMF 网元返回 Nausf_UE Authentication_Authenticate Response2，Nausf_UE Authentication_Authenticate Response2 包括 SUPI*和密钥 K_{AMF}。

以第二用户标识和密钥 K_{AMF} 是由 UDM 网元得到的为例，示例的，本申请实施例的通信方法可以如图 5 所示，具体包括以下步骤。

501、UE 向 AMF 网元发送接入请求；接入请求包括 SUCI。

502、AMF 网元接收到接入请求，向 AUSF 网元发送 Nausf_UE

Authentication_Authenticate Request1；Nausf_UE Authentication_Authenticate Request1 包括 SUCI、和指示信息 1，指示信息 1 携带 ABBA 参数，且用于指示 AMF 网元支持用户身份匿名化处理。

503、AUSF 网元接收到 Nausf_UE Authentication_Authenticate Request1，向 UDM 网元发送 Nudm_UE Authentication_Get Request，Nudm_UE Authentication_Get Request 包括 SUCI、和指示信息 1。

504、UDM 网元接收到 Nudm_UE Authentication_Get Request，在 UDM 网元支持用户身份匿名化处理时，对 SUCI 进行解密，得到 SUPI，根据 SUPI、ABBA 参数，基于第一算法，得到 SUPI*，并记录 SUPI 与 SUPI*的对应关系，以及根据 SUPI，从预先配置的 SUPI 与用户签约数据的对应关系中查找该 UE 的用户签约数据，根据该 UE 的用户签约数据生成 XRES*，以及向 AUSF 返回 Nudm_UE Authentication_Get Response，该 Nudm_UE Authentication_Get Response 包括指示信息 2、SUPI*和 XRES*。指示信息 2 用于指示 UDM 网元支持用户身份匿名化处理。

505、AUSF 网元接收到 Nudm_UE Authentication_Get Response，向 AMF 网元返回 Nausf_UE Authentication_Authenticate Response1，Nausf_UE Authentication_Authenticate Response1 包括指示信息 2 和 XRES*。

506、AMF 网元接收到 Nausf_UE Authentication_Authenticate Response1，向 UE 发送 Authentication-Request。

507、UE 接收到 Authentication-Request，生成 RES*，并向 AMF 网元返回 Authentication-Response，Authentication-Response 包括 RES*。

508、AMF 网元接收到 Authentication-Response，判断 RES*和 XRES*相同，向 AUSF 网元发送 Nausf_UE Authentication_Authenticate Request2，Nausf_UE Authentication_Authenticate Request2 包括 RES*。

509、AUSF 网元接收到 Nausf_UE Authentication_Authenticate Request2，根据 RES*，生成第一 HXRES*，判断第一 HXRES*与第二 HXRES*相同，向 AMF 网元返回 Nausf_UE Authentication_Authenticate Response2，Nausf_UE Authentication_Authenticate Response2 包括 SUPI*。

510、AMF 网元接收到 Nausf_UE Authentication_Authenticate Response2，根据 SUPI*、ABBA 参数，基于第二算法，得到密钥 K_{AMF}。

其中，根据 SUPI*、ABBA 参数基于第二算法得到的密钥 K_{AMF}，与 UE 根据 SUPI、ABBA 参数得到的密钥 K_{AMF} 相同，从而有助于基于密钥 K_{AMF} 实现 AMF 网元与 UE 的安全通信。

需要说明的是，图 4、图 5 所示的通信方法仅为示例性说明，并不构成对本申请的限定。

本申请实施例中由于在用户认证过程中可以得到第二用户标识，因此核心网中的网元通信时可以通过第二用户标识标识 UE。

示例的，如图 6 所示，为会话连接建立场景中使用第二用户标识标识 UE 的方法的流程示意图，具体包括以下步骤。

601、AMF 网元向 SMF 网元发送会话连接建立请求，会话连接建立请求中包括第二用

户标识。

602、SMF 网元接收到会话连接建立请求，根据第二用户标识寻址对应的 UDM 网元，并向该 UDM 网元发送用户签约数据查询请求，该用户签约数据查询请求包括第二用户标识。

603、UDM 网元接收到用户签约数据查询请求，根据第二用户标识，查询 UE 的用户签约数据。

示例的，UDM 网元可以根据第二用户标识，从预先配置的匿名化用户标识和用户签约数据的对应关系中，查询 UE 的用户签约数据。或者，UDM 网元可以对第二用户标识解密，得到 SUPI，根据 SUPI，从预先配置的 SUPI 与用户签约数据的对应关系中，查询 UE 的用户签约数据。

由于上述过程中 AMF 网元、SMF 网元和 UDM 网元在会话连接建立过程中查询用户签约数据时，是通过第二用户标识标识 UE 的，因而大大降低了通信过程中隐私泄露的风险。

示例的，如图 7 所示，为注册状态查询的场景中使用第二用户标识标识 UE 的方法的流程示意图，具体包括以下步骤。

701、AMF 网元根据第二用户标识寻址到对应的 UDM 网元，并向该 UDM 网元发送注册状态查询请求，注册状态查询请求包括第二用户标识。

702、UDM 网元接收到注册状态查询请求，记录第二用户标识标识的 UE 的注册状态。

示例的，UE 的注册状态包括去注册、注册等状态。

需要说明的是，第二用户标识还可以应用于其它场景中核心网的各网元通信时用于标识 UE，例如 AMF 网元和 PCF 网元、SMF 网元和 PCF 网元等通信时，可以采用第二用户标识标识 UE。

在一些实施例中，AMF 网元还可以记录全球唯一临时 UE 标识（globally unique temporary UE identity，GUTI）与第二用户标识的对应关系，以便于 AMF 网元在接收到 GUTI 时，便于查找第二用户标识。

此外，在一些实施例中，还可以通过改变 UE 计算密钥 K_{AMF} 时使用的参数，以 UE 计算密钥 K_{AMF} 时使用的参数为第二用户标识为例，示例的，本申请实施例提供的另一种通信方法，如图 8 所示，具体包括以下步骤。

801、UE 向 AMF 网元发送接入请求；接入请求包括第一用户标识。第一用户标识是对 SUPI 加密得到的，SUPI 为 UE 的身份标识。

示例的，第一用户标识为 SUCI。

在一些实施例中，接入请求还包括第一指示信息，第一指示信息用于指示 UE 支持用户身份匿名化处理。

802、AMF 网元响应于接入请求，向 AUSF 网元发送第一用户认证请求；第一用户认证请求包括第一用户标识。

示例的，接入请求包括第一指示信息时，第一用户认证请求也可以包括第一指示信息。

803、AUSF 网元响应于第一用户认证请求，向 UDM 网元发送第二用户认证请求，第二用户认证请求包括第一用户标识。

示例的，第一用户认证请求包括第一指示信息时，第二用户认证请求也可以包括第一指示信息。

804、UDM 网元响应于第二用户认证请求，向 AUSF 网元返回第二用户认证响应，第二用户认证响应中包括第二用户标识符；第二用户标识为 UE 的匿名化身份标识。例如，第二用户标识可以为 SUPI*。

进一步的，在一些实施例中，第二用户认证响应还可以包括第二指示信息，第二指示信息用于指示 UDM 网元支持用户身份匿名化处理。

其中，第二用户标识可以是 UDM 网元得到的，也可以是第一网元得到的，具体实现方式可以参见上述相关介绍，在此不再赘述。

805、AUSF 网元响应于第二用户认证响应，向 AMF 网元返回第一用户认证响应。示例的，第一用户认证响应包括第二指示信息。或者，第一用户认证响应也可以包括第二用户标识。

806、AMF 网元响应于第一用户认证响应，向 UE 发送第三用户认证请求。示例的，第三用户认证请求还包括第二指示信息。例如，第三用户认证请求用于向 UE 发起对网络的验证。

807、UE 响应于第三用户认证请求，根据 SUPI 得到第二用户标识，并根据第二用户标识生成密钥 K_{AMF}；以及向 AMF 网元返回第三用户认证响应；

需要说明的是，根据 SUPI 得到第二用户标识、根据第二用户标识生成密钥 K_{AMF} 的具体实现方式可以参见上述各实施例中的相关介绍。

808、AMF 网元响应于第三用户认证响应，向 AUSF 网元发送第四用户认证请求。例如，第四用户认证请求可以用于发起对 UE 的验证。

809、AUSF 网元响应于第四用户认证请求，向 AMF 网元返回第四用户认证响应，第四用户认证响应中包括第二用户标识。

810、AMF 网元响应于第四用户认证响应，根据第二用户标识，生成密钥 K_{AMF}。从而使得 AMF 网元生成的密钥 K_{AMF} 与 UE 生成的密钥 K_{AMF} 相同，有助于实现安全通信。

在一些实施例中，第一用户认证响应包括第二用户标识时，AMF 网元可以响应于第一用户认证响应，根据第二用户标识，生成密钥 K_{AMF}，当接收到第四用户认证响应后，无需根据第二用户标识，生成密钥 K_{AMF}。

示例的，如图 9 所示，为本申请实施例还提供又一种通信方法，具体包括以下步骤。

901、配置在网元 1 上的第一用户标识转换模块接收到来自网元 2 的第一业务请求，第一业务请求包括用户标识 1，用户标识 1 为终端设备 A 的身份标识。例如，用户标识 1 可以为 SUPI，也可以为 SUCI、或者临时用户身份标识等。

902、第一用户标识转换模块对将第一业务请求中的用户标识 1 替换为用户标识 2，用户标识 2 为终端设备 A 的匿名化身份标识。例如，用户标识 2 可以为上述实施例中的第二用户标识。

例如，第一用户标识转化模块可以根据预先设置的用户标识 1 与用户标识 2 的对应关系，将第一业务请求中的用户标识 1 替换为对应的用户标识 2。再例如，第一用户标识转换模块还可以基于第一算法，对第一业务请求中的用户标识 1 进行相应的运算，得到

用户标识2，并将第一业务请求中的用户标识1替换为得到的用户标识2。

903、第一用户标识转换模块将用户标识1替换为用户标识2的第一业务请求发送给网元1。

904、网元1响应于第一业务请求，向配置在网元1上的第二用户标识转换模块发送第一业务响应，第一业务响应包括用户标识2，用户标识2为终端设备A的匿名化身份标识。

905、第二用户标识转换模块将第一业务响应中的用户标识2替换为用户标识1，用户标识1为终端设备A的身份标识。

第二用户标识转换模块将第一业务响应中的用户标识2替换为用户标识1，可以看做是将消息中的用户标识1替换为用户标识2的逆过程，例如，第一用户标识转换模块根据预先设置的用户标识1与用户标识2的对应关系，将第一业务请求中的用户标识1替换为对应的用户标识2，则第二用户标识转换模块也可以根据预先设置的用户标识1与用户标识2的对应关系，将第一业务响应中的用户标识2替换为对应的用户标识1。再例如，第一用户标识转换模块还可以基于第一算法和密钥1，对第一业务请求中的用户标识1进行相应的运算，得到用户标识2，并将第一业务请求中的用户标识1替换为得到的用户标识2。则第二用户标识转换模块可以基于第二算法和密钥2，对第一业务响应中的用户标识2进行相应的运算，得到用户标识1，并将第一业务响应中的用户标识2替换为得到的用户标识1。第二算法可以为第一算法的逆运算。需要说明的是，密钥1和密钥2可以相同，也可以不同。此外，第一算法、和密钥1可以预配置在第一用户标识转换模块，也可以是第一用户标识转换模块从其它网元（例如UDM网元、第一网元等）获取的，对此不作限定。第二算法和密钥2可以预配置在第二用户标识转换模块，也可以是第二用户标识转换模块从其它网元（例如UDM网元、第一网元等）获取的，对此不作限定。

另外，还需要说明的是，上述仅为用户标识1和用户标识2具体转换方法的示例性说明，本申请实施例对用户标识1和用户标识2转换的方式不作限定。

906、第二用户标识转换模块将用户标识2替换为用户标识1的第一业务响应返回给网元2。

需要说明的是，上述网元1可以为AMF网元、AUSF网元、SMF网元等核心网中的网元，对此不作限定。网元2可以为终端设备，也可以核心网中的网元，例如AMF网元、AUSF网元、SMF网元等。

需要说明的是，第一用户标识转换模块和第二用户标识转换模块可以为两个独立的模块，分别配置在网元1上，也可以为一个模块，配置在网元1上，例如，第一用户标识转换模块和第二用户标识转换模块对于网元1来说是可拆卸的。需要说明的是，第一用户标识转换模块和第二用户标识转换模块的生产商与网元1的生产商可以不同。

通过该技术方案，使得网元无法获取终端设备的身份标识，有助于提高通信的安全性。

以上各个实施例可以独立使用，也可以相互结合使用，以实现不同的技术效果。

上述主要从各个网元之间交互的角度对本申请提供的方案进行了介绍。可以理解的是，上述实现各网元为了实现上述功能，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，结合本申请中所公开的实施例描述的各示例的单元及算法步骤，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。

如图 10 所示，为本申请所涉及的装置的一种可能的示例性框图，该装置 1000 可以以软件或硬件的形式存在。装置 1000 可以包括：处理单元 1002 和通信单元 1001。作为一种实现方式，该通信单元 1001 可以包括接收单元和发送单元。处理单元 1002 用于对装置 1000 的动作进行控制管理。通信单元 1001 用于支持装置 1000 与其他网络实体的通信。

其中，处理单元 1002 可以是处理器或控制器，例如可以是通用中央处理器（central processing unit，CPU），通用处理器，数字信号处理（digital signal processing，DSP），专用集成电路（application specific integrated circuits，ASIC），现场可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包括一个或多个微处理器组合，DSP 和微处理器的组合等等。通信单元 1001 是一种该装置的接口电路，用于从其它装置接收信号。例如，当该装置以芯片的方式实现时，该通信单元 1001 是该芯片用于从其它芯片或装置接收信号的接口电路，或者， 是该芯片用于向其它芯片或装置发送信号的接口电路。

该装置 1000 可以为上述实施例中的移动管理网元、认证服务网元、数据管理网元或第一网元，还可以为用于移动管理网元、认证服务网元、数据管理网元或第一网元的芯片。例如，当装置 1000 为移动管理网元、认证服务网元、数据管理网元或第一网元时，该处理单元 1002 例如可以是处理器，该通信单元 1001 例如可以是收发器。可选的，该收发器可以包括射频电路，该存储单元例如可以是存储器。例如，当装置 1000 为用于移动管理网元、认证服务网元、数据管理网元或第一网元的芯片时，该处理单元 1002 例如可以是处理器，该通信单元 1001 例如可以是输入/输出接口、管脚或电路等。该处理单元 1002 可执行存储单元存储的计算机执行指令，示例的，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是该移动管理网元、认证服务网元、数据管理网元或第一网元内的位于该芯片外部的存储单元，如只读存储器（read-only memory，ROM)或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM)等。

在一实施例中，该装置 1000 为上述实施例中的移动管理网元。处理单元 1002，用于在通信单元 1001 接收到终端设备发送的接入请求时，响应于接入请求，触发通信单元 1001 向认证服务网元发送第一用户认证请求。通信单元 1001 还有于接收认证服务单元响应于第一用户认证请求，返回的第一用户认证响应。第一用户认证响应包括第二用户标识；或者，处理单元 1002 响应于第一用户认证响应，通过通信单元 1001 从认证服务单元获取第二用户标识。

在另一实施例中，该装置 1000 为上述实施例中的认证服务网元。处理单元 1002，用于在通信单元 1001 接收到移动管理网元发送的第一用户认证请求时，响应于第一用户认证请求，向数据管理网元发送第二用户认证请求。第一用户认证请求包括第一用户标识，通信单元 1001 还用于接收数据管理网元响应于第二用户认证请求，返回的第二用户认证响应，第二用户认证响应包括第二用户标识。处理单元 1002 还用于响应于第二用户认证

响应，向移动管理网元返回第一用户认证响应。

在另一实施例中，该装置 1000 为上述实施例中的数据管理网元。处理单元 1002，用于在通信单元 1001 接收到认证服务网元发送的第二用户认证请求时，响应于第二用户认证请求，触发通信单元 1001 向认证服务王艳返回第二用户认证响应，第二用户认证响应包括第二用户标识。

在另一实施例中，该装置 1000 为上述实施例中的会话管理网元。处理单元 1002，用于在通信单元 1001 接收到数据管理网元发送的匿名化用户标识获取请求，响应于匿名化用户标识获取请求，触发通信单元 1001 向数据管理网元返回第二用户标识。其中，匿名化用户标识获取请求包括第一用户标识或 SUPI。

可以理解的是，该装置 1000 执行本申请实施例通信方法的具体过程以及相应的有益效果，可以参考前述方法实施例中的相关描述，这里不再赘述。

若该装置是移动性管理网元、认证服务网元、数据管理网元或第一网元，则移动管理网元认证服务网元、数据管理网元或第一网元以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定 ASIC，电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。在一个简单的实施例中，本领域的技术人员可以想到该移动管理网元、认证服务网元、数据管理网元或第一网元可以采用图 11 所示的形式。

比如，图 11 中的处理器 1102 可以通过调用存储器 1101 中存储的程序指令，使得移动性管理网元、认证服务网元、数据管理网元或第一网元执行上述方法实施例中的方法。

具体的，图 10 中的通信单元 1001、处理单元 1002 的功能/实现过程可以通过图 11 中的处理器 1102 调用存储器 1101 中存储的计算机执行指令来实现。或者，图 10 中的处理单元 1002 的功能/实现过程可以通过图 11 中的处理器 1102 调用存储器 1101 中存储的计算机执行指令来实现，图 10 中的通信单元 1001 的功能/实现过程可以通过图 11 中的通信接口 1103 来实现。

可选的，当该装置 1000 是芯片或电路时，则通信单元 1001 的功能/实现过程还可以通过管脚或电路等来实现。

如图 11 所示，为本申请提供的又一种装置示意图，该装置可以是上述实施例中的移动管理网元、认证服务网元、数据管理网元或第一网元。该装置 1100 包括：处理器 1102 和通信接口 1103，可选的，装置 1100 还可以包括存储器 1101。可选的，装置 1100 还可以包括通信线路 1104。其中，通信接口 1103、处理器 1102 以及存储器 1101 可以通过通信线路 1104 相互连接；通信线路 1104 可以是外设部件互连标准（peripheral component interconnect，简称 PCI）总线或扩展工业标准结构（extended industry standard architecture，简称 EISA）总线等。所述通信线路 1104 可以分为地址总线、数据总线、控制总线等。为便于表示，图 11 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

处理器 1102 可以是一个 CPU，微处理器，ASIC，或一个或多个用于控制本申请方案程序执行的集成电路。

通信接口 1103，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，无线接入网（radio access network，RAN），无线局域网(wireless local area networks，WLAN)，有线接入网等。

存储器 1101 可以是 ROM 或可存储静态信息和指令的其他类型的静态存储设备，RAM

或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器（electrically erasable programmable read-only memory，EEPROM）、只读光盘（compact disc read-only memory，CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 1104 与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 1101 用于存储执行本申请方案的计算机执行指令，并由处理器 1102 来控制执行。处理器 1102 用于执行存储器 1101 中存储的计算机执行指令，从而实现本申请上述实施例提供的会话管理网元的选择方法。

可选的，本申请实施例中的程序指令也可以称之为应用程序代码、计算机程序、计算机指令等，本申请实施例对此不作具体限定。

在上述实施例中，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申请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、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（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能够存取的任何可用介质或者是包括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，DVD)、或者半导体介质（例如固态硬盘（Solid State Disk，SSD））等。

本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器，数字信号处理器，专用集成电路（ASIC），现场可编程门阵列（FPGA）或其它可编程逻辑装置，离散门或晶体管逻辑，离散硬件部件，或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器，可选地，该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现，例如数字信号处理器和微处理器，多个微处理器，一个或多个微处理器联合一个数字信号处理器核，或任何其它类似的配置来实现。

本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示例性地，存储媒介可以与处理器连接，以使得处理器可以从存储媒介中读取信息，并可以向存储媒介存写信息。可选地，存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于 ASIC 中。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方

框或多个方框中指定的功能的步骤。

尽管结合具体特征及其实施例对本申请进行了描述，显而易见的，在不脱离本申请的精神和范围的情况下，可对其进行各种修改和组合。相应地，本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明，且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。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，则本申请也意图包括这些改动和变型在内。

此外，在一些实施例中，还需要考虑 UE 是否支持匿名化处理，可以通过 UE 与网络交换指示的方式来确定是否进行匿名化处理，示例的，本申请实施例提供的另一种通信方法，如图 12 所示，具体包括以下步骤。

1201、UE 向 AMF 网元发送接入请求；接入请求包括第一用户标识。第一用户标识是对 SUPI 加密得到的，SUPI 为 UE 的身份标识。

示例的，第一用户标识为 SUCI。

在一些实施例中，接入请求还包括指示信息 1，指示信息 1 用于指示 UE 支持用户身份匿名化处理。

1202、AMF 网元响应于接入请求，向 AUSF 网元发送第一用户认证请求；第一用户认证请求包括第一用户标识和服务网络名称。

示例的，服务网络名称包含 PLMN ID 和/或网络标识（network identifier，NID）。其中，PLMN ID 和 NID 联合用于标识非公共网络（例如，独立组网的非公共网络（standalone non-public network，SNPN））。

在一些实施例中，AMF 网元或 AMF 网元所在的网络支持用户身份匿名化处理时，第一用户认证请求也可以包括指示信息 2，指示信息 2 用于指示 AMF 网元或 AMF 网元所在网络和/或 UE 支持用户身份匿名化处理。例如，在指示信息 2 用于指示 UE 支持用户身份匿名化处理的情况下，可以隐含向 UDM 网元指示 AMF 网元或 AMF 网元所在的网络也支持用户身份匿名化处理。

在一些实施例中，接入请求包括指示信息 1 时，第一用户认证请求也可以包括指示信息 1。

在一些实施例中，接入请求包括指示信息 1、且 AMF 网元或 AMF 网元所在网络支持用户身份匿名化处理时，第一用户认证请求也可以包括指示信息 1 和/或指示信息 2，指示信息 2 用于指示 AMF 网元或 AMF 网元所在网络和/或 UE 支持用户身份匿名化处理。

1203、AUSF 网元响应于第一用户认证请求，向 UDM 网元发送第二用户认证请求，第二用户认证请求包括第一用户标识和服务网络名称。

在一些实施例中，第一用户认证请求包括指示信息 1 时，用户认证请求也可以包括指示信息 1。

在一些实施例中，第一用户认证请求中包括指示信息 2 时，第二用户认证请求也可以包括指示信息 2。

1204、UDM 网元响应于第二用户认证请求，向 AUSF 网元返回第二用户认证响应，第二用户认证响应中包括第二用户标识；

示例的，第二用户标识为 UE 的 SUPI。又示例的，第二用户标识为 UE 的匿名化身份标识。例如第二用户标识为 SUPI*。此外，UDM 网元还记录 SUPI 与 SUPI*的对应关系。

例如，UDM 网元在第二用户认证请求包括指示信息 1 和/或指示信息 2 的情况下，第二用户标识为 UE 的匿名化身份标识。以 UE 的匿名化身份标识为 SUPI* 为例，UDM 网元还记录 SUPI 与 SPUI*的对应关系。

又例如，UDM 网元在第二用户认证请求包括指示信息 1 和/或服务网络名称包括 NID 的情况下，第二用户标识为 UE 的匿名化身份标识。以 UE 的匿名化身份标识为 SUPI* 为例，UDM 网元还记录 SUPI 与 SPUI*的对应关系。

又例如，UDM 网元在 UE 签约能力指示 UE 支持用户身份匿名化处理和/或第二用户认证请求包括指示信息 2 的情况下，第二用户标识为 UE 的匿名化身份标识。以 UE 的匿名化身份标识为 SUPI*为例，UDM 网元还记录 SUPI 与 SUPI*的对应关系。

又例如，UDM 网元在 UE 签约能力指示 UE 支持用户身份匿名化处理和/或第二用户认证请求包括的服务网络名称包含 NID 的情况下，第二用户标识为 UE 的匿名化身份标识。以 UE 的匿名化身份标识为 SUPI* 为例，UDM 网元还记录 SUPI 与 SPUI*的对应关系。

在一些实施例中，UE 的匿名化身份标识（例如 SUPI*）是由 UDM 网元根据以下参数中一种或者多种，基于某一算法或策略生成的：

新鲜性参数，包括但不限于：随机数（RAND）、序列号（sequence number，SQN）、计数（count）；其中，计数指的是 UE 和网络侧维护的计数器所计的数值，例如 NAS 计数器所计的值。

UE 的标识，包括但不限于：SUPI、5G 全球唯一临时标识符（5G globally unique temporary identifier, 5G-GUTI）、SUCI、通用公共订阅标识符（generic public subscription identifier，GPSI）等；

UE 和网络侧之间的共享密钥，包括但不限于：KAUSF、加密密钥 CK、完整性密钥 IK、匿名密钥 AK、长期密钥 K、以及由 KAUSF、KAKMA、CK、IK、AK 和 K 中的任意一项或多项生成的密钥，比如 SEAF 密钥 KSEAF 等。具体的，KSEAF 由 KAUSF 生成。

公私钥，包括但不限于：UE 的公钥、UE 的私钥、UE 的归属网络的公钥、UE 的归属网络的私钥等；

网络标识，包括但不限于：服务网络标识、服务网络名称、归属网络名称、路由参数 routing indicator 等；

其中 UDM 网元生成 UE 的匿名化身份标识所使用的算法或策略包括：推演，和/或拼接等，本申请实施例不作限定。

在一些实施例中，第二用户认证响应还可以包括指示信息 3，指示信息 3 用于指示 UDM 网元支持用户身份匿名化处理，其中，UDM 网元支持用户身份匿名化处理又可以表述为 UDM 网元进行了用户身份匿名化处理，和/或，UDM 网元所在归属网络支持用户身份匿名化处理。

在一些实施例中，第二用户认证响应还可以包括指示信息 4，指示信息 4 用于指示 UE 支持用户身份匿名化处理。

1205、AUSF 网元响应于第二用户认证响应，向 AMF 网元返回第一用户认证响应。示例的，第一用户认证响应包括指示信息 3 和/或第三用户标识。

在一些实施例中，AUSF 网元根据指示信息 1 和/或指示信息 4 和/或指示信息 2 和/或服务网络名称包含 NID，生成第三用户标识，第三用户标识为 UE 的匿名化身份标识。例如第三用户标识为 SUPI*。

其中，第三用户标识可以是第二用户标识，也可以 AUSF 网元根据第二用户标识计算得到的。具体计算包含的参数与 UDM 网元生成 SUPI*的方式一致，这里不再赘述。

1206、AMF 网元响应于第一用户认证响应，向 UE 发送第三用户认证请求，第三用户认证请求用于向 UE 发起认证。示例的，第三用户认证请求还可以包括指示信息 3。

在一些实施例中，指示信息 3 可以携带在认证令牌 AUTN 中。

1207、UE 响应于第三用户认证请求，向 AMF 网元返回第三用户认证响应，以及根据 SUPI 和/或指示信息 3 生成第二用户标识，并根据第二用户标识生成密钥 KAMF。

需要说明的是，UE 根据 SUPI 生成第二用户标识与上述 UDM 生成 SUPI*的方式一致。UE 根据第二用户标识生成密钥 KAMF 的具体实现方式可以参见上述各实施例中的相关介绍。

UE 可以在向 AMF 返回第三用户认证响应之后，生成第二用户标识和密钥 KAMF，也可以在返回第三用户认证响应之前生成第二用户标识和密钥 KAMF，对此不作限定。此外，UE 生成第二用户标识和密钥 KAMF 的方式可参见上述相关介绍，在此不再赘述。

在一些实施例中，生成密钥 KAMF 时只用 SUPI*除去 PLMN ID 和/或路由信息的部分。

1208、AMF 网元响应于第三用户认证响应，向 AUSF 网元发送第四用户认证请求。例如，第四用户认证请求可以用于发起对 UE 的验证。

1209、AUSF 网元响应于第四用户认证请求，向 AMF 网元返回第四用户认证响应，第四用户认证响应中也可以包括第三用户标识。

在一些实施例中，AUSF 网元根据指示信息 1 和/或指示信息 4 和/或指示信息 2 和/或服务网络名称包含 NID 生成第三用户标识，第三用户标识为 UE 的匿名化身份标识。例如第三用户标识为 SUPI*。

其中，第三用户标识可以是第二用户标识，也可以 AUSF 根据第二用户标识计算得到的。具体计算包含的参数与 UDM 网元生成 SUPI*的方式一致，这里不再赘述。

在一些实施例中，AUSF 网元在认证 UE 成功后，向 UDM 网元返回用户认证结果，其中用户认证结果包括第三用户标识和/或 SUPI。

1210、AMF 网元响应于第四用户认证响应，根据第三用户标识，生成密钥 KAMF。从而使得 AMF 网元生成的密钥 KAMF 与 UE 生成的密钥 KAMF 相同，有助于实现安全通信。

进一步的，在一些实施例中，在 UE 接入网络后，还可以由 AMF 网元主动发起用户认证，更新 UE 与网络之间通信交互所使用的 UE 的匿名化身份标识，例如 SUPI*。

示例的，AMF 网元可以在 UE 接入网络后周期性触发发起用户认证，也可以通过事件（例如小区切换、NAS COUNT wrap around 等）触发发起用户认证。

例如，以 UE 的匿名化用户标识为 SUPI*1 为例，如图 13 所示，为 AMF 网络主动发起用户认证时的通信方法，具体包括以下步骤。

1301、AMF 网元向 AUSF 网元发送第一用户认证请求；第一用户认证请求包括 SUPI*1 和服务网络名称。

示例的，服务网络名称包含 PLMN ID 和/或 NID。

在一些实施例中，AMF 网元或 AMF 网元所在的网络支持用户身份匿名化处理时，第一用户认证请求也可以包括指示信息 2，指示信息 2 用于指示 AMF 网元或 AMF 网元所在网络和/或 UE 支持用户身份匿名化处理。

在一些实施例中，当 UE 支持用户身份匿名化处理时，AMF 网元存储指示信息 1，指示信息 1 用于指示 UE 支持用户身份匿名化处理，在这种情况下，第一用户认证请求还可以包括指示信息 1。

1302、AUSF 网元响应于第一用户认证请求，向 UDM 网元发送第二用户认证请求，第二用户认证请求包括 SUPI*1 和服务网络名称。

在一些实施例中，第一用户认证请求包括指示信息 2 时，用户认证请求也可以包括指示信息 2。

1303、UDM 网元响应于第二用户认证请求，向 AUSF 网元返回第二用户认证响应，第二用户认证响应中包括 SUPI*1 和 SUPI*2;

在一些实施例中，第二用户认证响应包括指示信息 2、和/或 UDM 网元支持用户身份匿名化处理时，UDM 网元若根据 SUPI*1，从记录的 SUPI 与 SUPI*的对应关系中查找到与 SUPI*1 对应的 SUPI，则判断 UE 支持用户身份匿名化处理，生成 SUPI*2，以及记录 SUPI 与 SUPI*2 的对应关系。具体的，生成 SUPI*2 的方式可以参见上述步骤 1204 中生成第二用户标识的相关介绍，在此不再赘述。

进一步，示例的，在 UDM 网元判定判断 UE 支持用户身份匿名化处理的情况下，第二用户认证响应还可以包括指示信息 1，用于指示 UE 支持用户身份匿名化处理。以便于显示向 AMF 网元指示 UE 支持用户身份匿名化处理。

在另一些实施例中，UDM 网元若根据 SUPI*1，从记录的 SUPI 与 SUPI*的对应关系中未查找到与 SUPI*1 对应的 SUPI，则将 SUPI*1 作为 SUPI 处理。

在另一些实施例中，当 AMF 网元不支持用户身份匿名化处理时，UDM 网元响应于第二用户认证请求，向 AUSF 网元返回第二用户认证响应包括 SUPI，不包括指示信息 3，指示信息 3 用于指示 UDM 网元支持用户身份匿名化处理。

在一些实施例中，第二用户认证响应包括指示信息 2、和/或 UDM 网元支持用户身份匿名化处理时，第二用户认证响应还可以包括指示信息 3，其中，UDM 网元支持用户身份匿名化处理又可以表述为 UDM 网元进行了用户身份匿名化处理，和/或，UDM 网元所在归属网络支持用户身份匿名化处理。

1304、AUSF 网元响应于第二用户认证响应，向 AMF 网元返回第一用户认证响应。示例的，第一用户认证响应包括指示信息 3。

1305、AMF 网元响应于第一用户认证响应，向 UE 发送第三用户认证请求，第三用户认证请求用于向 UE 发起认证。示例的，第三用户认证请求还可以包括指示信息 3。

在一些实施例中，指示信息 3 可以携带在认证令牌 AUTN 中。

1306、UE 响应于第三用户认证请求，向 AMF 网元返回第三用户认证响应，以及根据 SUPI 和/或指示信息 3 生成 SUPI*2，并根据 SUPI*2 生成密钥 KAMF。

需要说明的是，UE 根据 SUPI 生成 SUPI*2 与上述 UDM 生成 SUPI*的方式一致。UE 根据 SUPI*2 生成密钥 KAMF 的具体实现方式可以参见上述各实施例中的相关介绍。

UE 可以在向 AMF 返回第三用户认证响应之后，生成 SUPI*2 和密钥 KAMF，也可以在返回第三用户认证响应之前生成 SUPI*2 和密钥 KAMF，对此不作限定。此外，UE 生成 SUPI*2 和密钥 KAMF 的方式可参见上述相关介绍，在此不再赘述。

1307、AMF 网元响应于第三用户认证响应，向 AUSF 网元发送第四用户认证请求。例如，第四用户认证请求可以用于发起对 UE 的验证。

1308、AUSF 网元响应于第四用户认证请求，向 AMF 网元返回第四用户认证响应，第四用户认证响应中可以包括第三用户标识、SUPI*2。在一些实施例中，第四用户认证响应中也可以包括 SUPI*1。

第三用户标识的相关介绍可以参见步骤 1209 中的描述，这里不再赘述。

1309、AMF 网元响应于第四用户认证响应，当 SUPI*2 与 SUPI*1 不同时，将 SUPI*1 替换为 SUPI*2，并记录 SUPI*1 与 SUPI*2 的对应关系，并根据 SUPI*2，生成密钥 KAMF。从而实现用户匿名身份标识的更新，有助于实现安全通信。

进一步的，AMF 网元还可以通过比较 SUPI*2 与 SUPI*1，当 SUPI*2 与 SUPI*1 不同时，判定 UE 支持用户身份匿名化处理。从而实现隐式判定 UE 支持用户身份匿名化处理。

又进一步的，在一些实施例中，如图 14 所示，AMF 网元在将 SUPI*1 替换为 SUPI*2 后，还包括:

1401、AMF 网元向 SMF 网元发送会话连接建立请求，该会话连接建立请求包括 SUPI*1 和 SUPI*2。

1402、SMF 网元在接收到会话建立连接请求后，将 SUPI*1 替换为 SUPI*2，以便于后续 SMF 网元通过 SUPI*2 标识 UE。

示例的，会话连接建立请求可以为 Nsmf_PDUSession_CreateSMContext Request。

上述是以 SMF 网元为例进行介绍的，也就是说，AMF 网元在针对某一 UE 更新用户身份匿名化标识后，可以通过与核心网中其它网元之间的业务消息中携带更新后的 UE 的用户身份匿名化标识，从而有助于节省资源开销。

此外，对于核心网中的除 AMF 网元以外的其它网元还可以在每次获取到 UE 的用户身份匿名化标识后，通过向 AMF 网元订阅，以使得 AMF 网元在再次更新 UE 的用户身份匿名化标识后，向其它网元发送更新后的 UE 的用户身份匿名化标识。

以 NF 网元 1 已获取到 UE 的用户身份匿名化标识为 SUPI*1 为例，本申请实施例订阅用户匿名化身份标识更新的方法可以如图 15 所示，具体包括以下步骤:

1501、NF 网元 1 向 AMF 网元发送订阅用户匿名化身份标识更新请求，其中订阅用户匿名化身份标识更新请求包括 SUPI*1。

例如，订阅用户匿名化身份标识更新请求为一个新定义的消息，例如 AMF_UEIdentifier_UpdateSubscribe。再例如，订阅用户匿名化身份标识更新请求可以为已有的业务消息。

1502、AMF 网元接收到订阅用户匿名化身份标识更新请求后，若将 SUPI*1 替换为 SUPI*2，则向 NF 网元 1 发送订阅用户匿名化身份标识更新响应，订阅用户匿名化身份标识更新响应中包括 SUPI*1 和 SUPI*2。

例如，订阅用户匿名化身份标识更新响应可以为一个新定义的消息，例如 AMF_UEIdentifier_UpdateNotification。再例如，订阅用户匿名化身份标识更新响应可以为已有的业务消息。

1503、NF 网元 1 接收到订阅用户匿名化身份标识更新响应后，将 SUPI*1 替换为 SUPI*2。

进一步的，为避免后续 AMF 网元再次更新 SUPI*2，NF 网元 1 将 SUPI*1 替换为 SUPI*2 后，再次向 AMF 网元发送订阅用户匿名化身份标识更新请求，或者，AMF 网元再将 SUPI*1 替换为 SUPI*2 后，将对 SUPI*1 的订阅替换为对 SUPI*2 的订阅。

此外，需要说明的是，本申请各实施例中涉及的接入请求可以理解为注册请求，即本申请实施例中涉及的接入请求可以替换为注册请求。

权 利 要 求

1、一种通信系统，其特征在于，包括移动管理网元、认证服务网元和数据管理网元；

所述移动管理网元用于接收终端设备发送的接入请求；所述接入请求包括第一用户标识，所述第一用户标识是对用户标识 SUPI 加密得到的，所述 SUPI 为所述终端设备的身份标识；

所述移动管理网元用于响应于所述接入请求，向所述认证服务网元发送第一用户认证请求；所述第一用户认证请求包括所述第一用户标识；

所述认证服务网元用于响应于所述第一用户认证请求，向所述数据管理网元发送第二用户认证请求，所述第二用户认证请求包括所述第一用户标识；

所述数据管理网元用于响应于所述第二用户认证请求，向所述认证服务网元返回第二用户认证响应，所述第二用户认证响应包括第二用户标识；所述第二用户标识为所述终端设备的匿名化身份标识；

所述认证服务网元还用于响应于所述第二用户认证响应，向所述移动管理网元返回第一用户认证响应。

2、如权利要求 1 所述的通信系统，其特征在于，所述第一用户认证响应还包括所述第二用户标识。

3、如权利要求 1 或 2 所述的通信系统，其特征在于，所述移动管理网元还用于：

响应于所述第一用户认证响应，从所述认证服务网元获取所述第二用户标识。

4、如权利要求 1 至 3 任一所述的通信系统，其特征在于，所述第一用户认证请求还包括第一指示信息，则所述认证服务网元响应于所述第一用户认证请求，向所述数据管理网元发送的所述第二用户认证请求还包括所述第一指示信息；所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。

5、如权利要求 1 至 4 任一所述的通信系统，其特征在于，所述第二用户认证响应还包括第二指示信息，则所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回的所述第一用户认证响应还包括所述第二指示信息；所述第二指示信息用于指示所述数据管理网元支持用户身份匿名化处理。

6、如权利要求 1 至 5 任一所述的通信系统，其特征在于，还包括第一网元；

所述数据管理网元还用于：

向所述第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述第一用户标识，以及接收所述第一网元返回的所述第二用户标识；

所述第一网元用于响应于所述匿名化用户标识获取请求，对所述第一用户标识解密，以得到所述 SUPI；根据所述 SUPI，获取所述第二用户标识，以及向所述数据管理网元返回所述第二用户标识。

7、如权利要求 1 至 5 任一所述的通信系统，其特征在于，还包括第一网元；

所述数据管理网元还用于：

对所述第一用户标识解密，以得到所述 SUPI，并向所述第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述 SUPI，以及接收所述第一网元返回的所述第二用户标识；

所述第一网元用于响应于所述匿名化用户标识获取请求，根据所述 SUPI，获取所述第

二用户标识，以及向所述数据管理网元返回所述第二用户标识。

8、如权利要求 6 或 7 所述的通信系统，其特征在于，所述认证服务网元还用于：

向所述第一网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；并接收所述第一网元返回的密钥 K_{AMF}，以及向所述移动管理网元发送所述密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥；

所述第一网元用于响应于所述密钥获取请求，根据所述第二用户标识，生成所述密钥 K_{AMF}，并向所述认证服务网元返回所述密钥 K_{AMF}；

所述移动管理网元还用于：接收所述认证服务网元发送的所述密钥 K_{AMF}。

9、如权利要求 8 所述的通信系统，其特征在于，所述第一网元用于根据所述第二用户标识获取所述 SUPI，并根据所述 SUPI 生成所述密钥 K_{AMF}。

10、如权利要求 9 所述的通信系统，其特征在于，

所述移动管理网元，还用于向所述认证服务器发送第一参数；

所述认证服务网元，还用于向所述第一网元发送所述第一参数；

所述第一网元用于根据所述 SUPI 和所述第一参数生成所述密钥 K_{AMF}。

11、如权利要求 1 至 5 任一所述的通信系统，其特征在于，所述数据管理网元，还用于：

对所述第一用户标识解密，以得到所述 SUPI；根据所述 SUPI，获取所述第二用户标识。

12、如权利要求 11 所述的通信系统，其特征在于，所述认证服务网元还用于：

向所述数据管理网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；并接收所述数据管理网元返回的密钥 K_{AMF}，以及向所述移动管理网元发送所述密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥；

所述数据管理网元，还用于：

响应于所述密钥获取请求，根据所述第二用户标识，生成所述密钥 K_{AMF}，并向所述认证服务网元返回所述密钥 K_{AMF}；

所述移动管理网元还用于：接收所述认证服务网元发送的所述密钥 K_{AMF}。

13、如权利要求 11 所述的通信系统，其特征在于，所述移动管理网元还用于：

根据所述第二用户标识，生成密钥 K_{AMF}；所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥。

14、一种通信方法，其特征在于，所述方法包括：

移动管理网元接收到终端设备发送的接入请求，所述接入请求包括第一用户标识，所述第一用户标识是对用户标识 SUPI 加密得到的，所述 SUPI 为所述终端设备的身份标识；

所述移动管理网元响应于所述接入请求，向所述认证服务网元发送第一用户认证请求，所述第一用户认证请求包括所述第一用户标识；

所述移动管理网元接收认证服务网元响应于所述第一用户认证请求，返回的第一用户认证响应；

其中，所述第一用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识；或者，所述移动管理网元响应于所述第一用户认证响应，从所述认证服务网元获取所述第二用户标识。

15、如权利要求 14 所述的方法，其特征在于，所述第一用户认证请求还包括第一指

示信息，所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。

16、如权利要求 14 或 15 所述的方法，其特征在于，第一用户认证响应还包括第二指示信息，所述第二指示信息用于指示数据管理网元支持用户身份匿名化处理。

17、如权利要求 14 至 15 任一所述的方法，其特征在于，所述方法还包括：

所述移动管理网元根据所述第二用户标识，生成密钥 K_{AMF}；或者，

所述移动管理网元接收所述认证服务网元返回的密钥 K_{AMF}；

所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥。

18、如权利要求 17 所述的方法，其特征在于，所述方法还包括：

所述移动管理网元还向所述认证服务网元发送第一参数；所述第一参数用于生成所述密钥 K_{AMF}。

19、一种通信方法，其特征在于，所述方法包括：

认证服务网元接收到移动管理网元发送的第一用户认证请求；所述第一用户认证请求包括第一用户标识，所述第一用户标识是对用户标识 SUPI 加密得到的，所述 SUPI 为终端设备的身份标识；

所述认证服务网元响应于所述第一用户认证请求，向数据管理网元发送第二用户认证请求，所述第二用户认证请求包括所述第一用户标识；

所述认证服务网元接收到所述数据管理网元响应于所述第二用户认证请求，返回的第二用户认证响应，所述第二用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识；

所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回第一用户认证响应。

20、如权利要求 19 所述的方法，其特征在于，所述第一用户认证响应包括所述第二用户标识。

21、如权利要求 19 或 20 所述的方法，其特征在于，所述第一用户认证请求还包括第一指示信息，则所述认证服务网元响应于所述第一用户认证请求，向所述数据管理网元发送的所述第二用户认证请求还包括所述第一指示信息；所述第一指示信息用于指示所述移动管理网元支持用户身份匿名化处理。

22、如权利要求 19 至 21 任一所述的方法，其特征在于，所述第二用户认证响应还包括第二指示信息，则所述认证服务网元响应于所述第二用户认证响应，向所述移动管理网元返回的所述第一用户认证响应还包括所述第二指示信息；所述第二指示信息用于指示所述数据管理网元支持用户身份匿名化处理。

23、如权利要求 19 至 22 任一所述的方法，其特征在于，所述方法还包括：

所述认证服务网元向第一网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识；

所述认证服务网元接收所述第一网元响应于所述密钥获取请求返回的密钥 K_{AMF}，所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥 K_{AMF}；

所述认证服务网元向所述移动管理网元发送的所述密钥 K_{AMF}。

24、如权利要求 23 所述的方法，其特征在于，所述方法还包括：

所述认证服务网元接收所述移动管理网元发送的第一参数，并将所述第一参数发送给所述第一网元，所述第一参数用于生成所述密钥 K_{AMF}。

25、如权利要求 23 所述的方法，其特征在于，所述方法还包括:

所述认证服务网元向所述数据管理网元发送密钥获取请求，所述密钥获取请求包括所述第二用户标识;

所述认证服务网元接收所述数据管理网元响应于所述密钥获取请求返回的密钥 K_{AMF}，所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥 K_{AMF};

所述认证服务网元向所述移动管理网元发送的所述密钥 K_{AMF}。

26、一种通信方法，其特征在于，所述方法包括:

数据管理网元接收到认证服务网元发送的第二用户认证请求，所述第二用户认证请求包括第一用户标识，所述第一用户标识是对用户标识 SUPI 加密得到的，所述 SUPI 为终端设备的身份标识;

所述数据管理网元响应于所述第二用户认证请求，向所述认证服务网元返回第二用户认证响应，所述第二用户认证响应包括第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识。

27、如权利要求 26 所述的方法，其特征在于，所述方法还包括:

所述数据管理网元向第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述第一用户标识;

所述数据管理网元接收所述第一网元响应于所述匿名化用户标识获取请求返回的所述第二用户标识。

28、如权利要求 26 所述的方法，其特征在于，所述方法还包括:

所述数据管理网元向第一网元发送匿名化用户标识获取请求，所述匿名化用户标识获取请求包括所述 SUPI;

所述数据管理网元接收所述第一网元响应于所述匿名化用户标识获取请求返回的所述第二用户标识。

29、如权利要求 26 所述的方法，其特征在于，所述方法还包括:

所述数据管理网元根据所述 SUPI，获取所述第二用户标识。

30、如权利要求 26~29 任一所述的方法，其特征在于，所述方法还包括:

所述数据管理网元接收到所述认证服务网元发送的密钥获取请求，所述密钥获取请求包括第二用户标识;

所述数据管理网元响应于所述密钥获取请求，向所述认证服务网元返回密钥 K_{AMF};所述密钥 K_{AMF} 为所述终端设备与所述移动管理网元之间的密钥。

31、一种通信方法，其特征在于，所述方法包括:

第一网元接收到数据管理网元发送的匿名化用户标识获取请求，所述匿名化用户标识获取请求包括第一用户标识或者用户标识 SUPI; 所述第一用户标识是对所述 SUPI 加密得到的，所述 SUPI 为终端设备的身份标识;

所述第一网元响应于所述匿名化用户标识获取请求向数据管理网元返回所述第二用户标识，所述第二用户标识为所述终端设备的匿名化身份标识。

32、如权利要求 31 所述的方法，其特征在于，所述方法还包括:

所述第一网元根据所述 SUPI，获取所述第二用户标识，所述 SUPI 是从所述匿名化用户标识获取请求中得到的，或者对所述第一用户标识解密得到的。

33、如权利要求 31 或 32 所述的方法，其特征在于，所述方法还包括:

所述第一网元接收到认证服务网元发送的密钥获取请求，所述密钥获取请求包括所述第二用户标识;

所述第一网元响应于所述密钥获取请求，向所述认证服务网元返回所述密钥 K_{AMF}; 所述密钥 K_{AMF} 为所述终端设备与移动管理网元之间的密钥。

34、如权利要求 33 所述的方法，其特征在于，所述方法还包括:

所述第一网元接收所述认证服务网元发送的第一参数; 所述第一参数是移动管理网元发送给所述认证服务网元的; 所述第一参数用于生成所述密钥 K_{AMF}。

35、一种通信装置，其特征在于，包括处理器和存储器，其中:

所述存储器存储有程序指令;

所述处理器用于调用所述存储器中存储的程序指令，执行如权利要求 14 至 18 任一所述的方法。

36、一种通信装置，其特征在于，包括处理器和存储器，其中:

所述存储器存储有程序指令;

所述处理器用于调用所述存储器中存储的程序指令，执行如权利要求 19 至 25 任一所述的方法。

37、一种通信装置，其特征在于，包括处理器和存储器，其中:

所述存储器存储有程序指令;

所述处理器用于调用所述存储器中存储的程序指令，执行如权利要求 26 至 30 任一所述的方法。

38、一种通信装置，其特征在于，包括处理器和存储器，其中:

所述存储器存储有程序指令;

所述处理器用于调用所述存储器中存储的程序指令，执行如权利要求 31 至 34 任一所述的方法。

39、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存储有程序，所述程序在计算机上运行时，使得所述计算机执行如权利要求 14 至 34 任一所述的方法。

通信系统

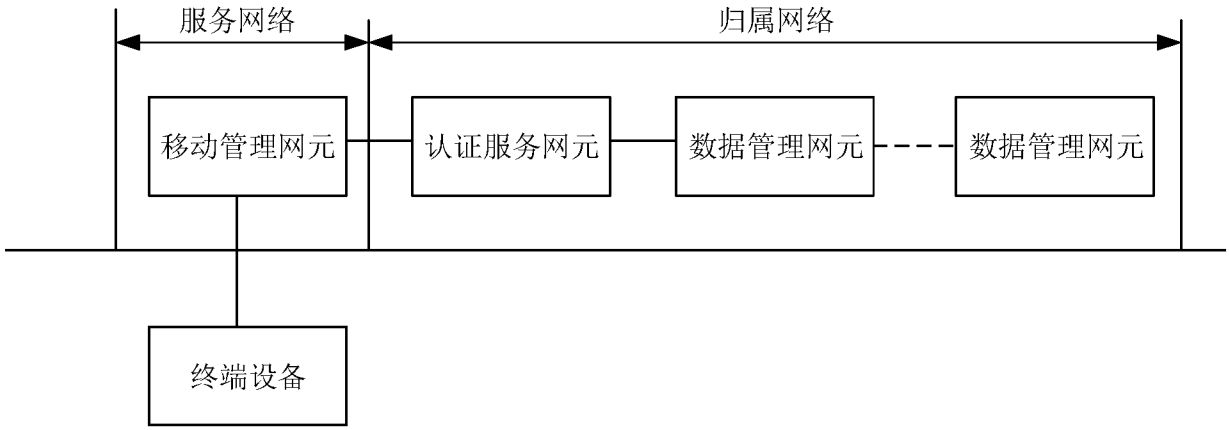
服务网络
归属网络
移动管理网元
认证服务网元
数据管理网元
数据管理网元
终端设备

图 1

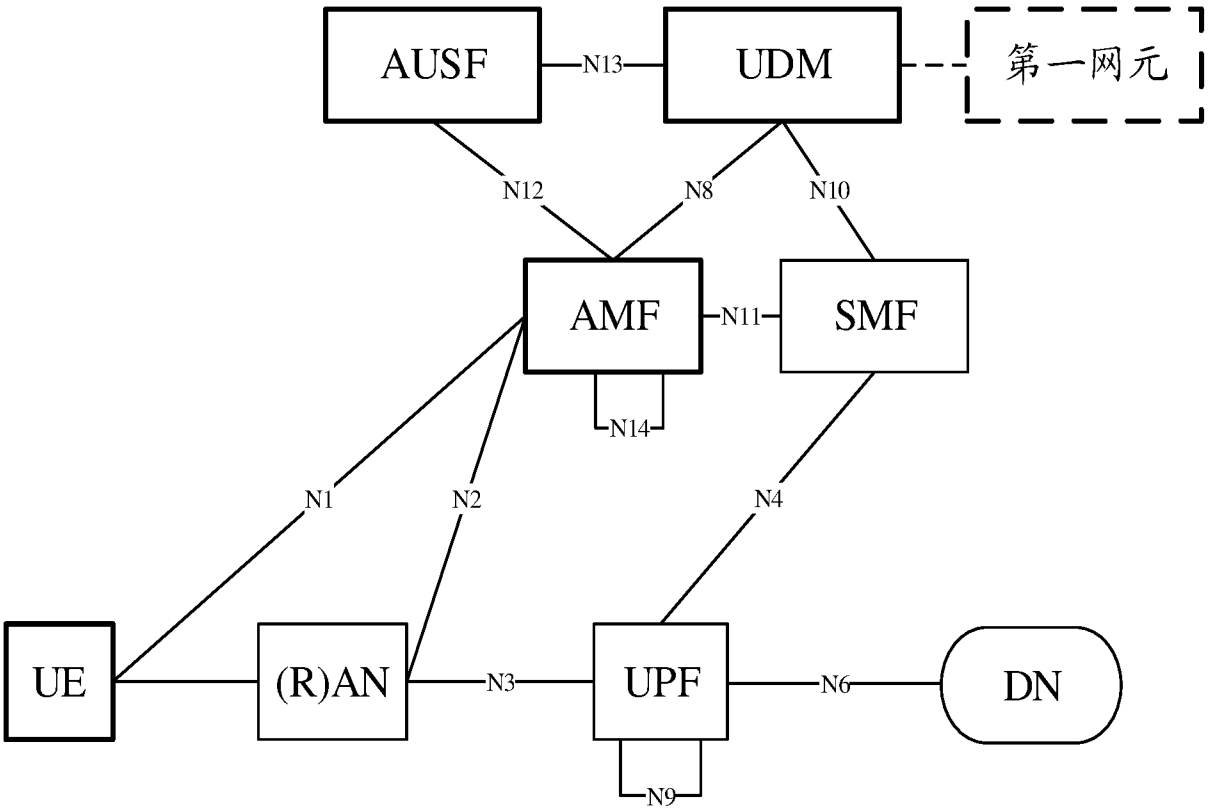
AUSF
N13
UDM
第一网元
N12
N8
N10
AMF
N11
SMF
N14
N1
N2
N4
UE
(R)AN
N3
UPF
N6
DN
N9

图 2

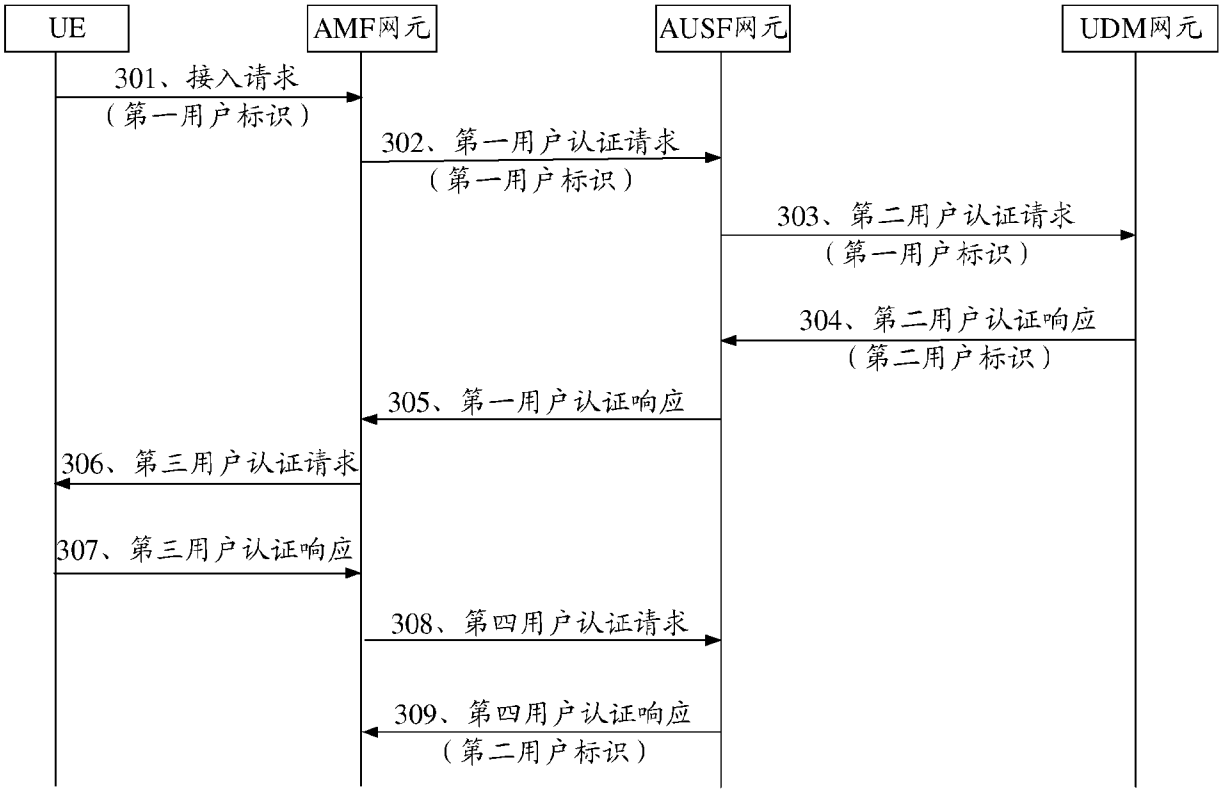
UE
AMF网元
AUSF网元
UDM网元
301、接入请求
（第一用户标识）
302、第一用户认证请求
（第一用户标识）
303、第二用户认证请求
（第一用户标识）
304、第二用户认证响应
（第二用户标识）
305、第一用户认证响应
306、第三用户认证请求
307、第三用户认证响应
308、第四用户认证请求
309、第四用户认证响应
（第二用户标识）

图 3

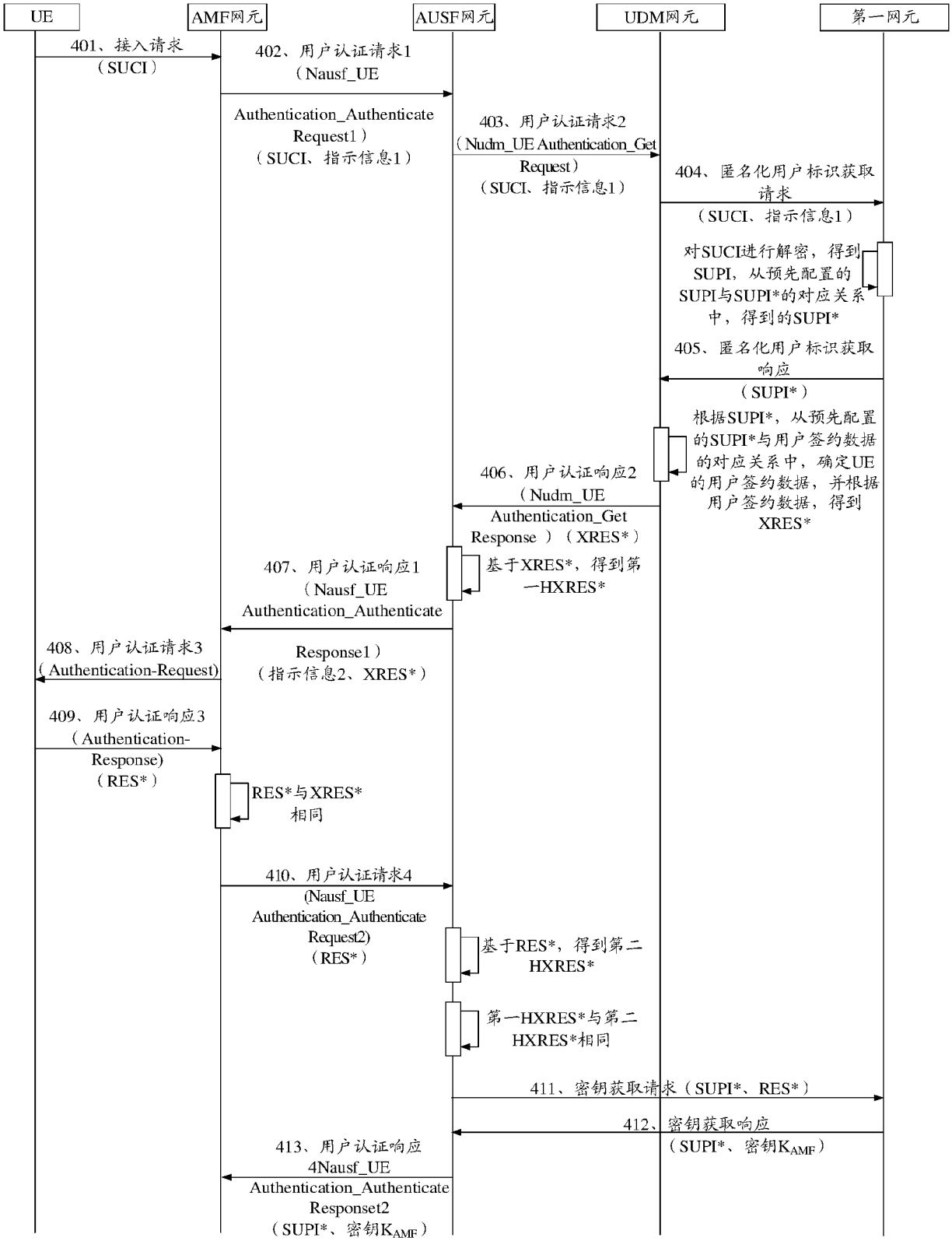
UE
AMF网元
AUSF网元
UDM网元
第一网元
401、接入请求
（SUCI）
402、用户认证请求1
（Nausf_UE
Authentication_Authenticate
Request1）
（SUCI、指示信息1）
403、用户认证请求2
（Nudm_UE Authentication_Get
Request）
（SUCI、指示信息1）
404、匿名化用户标识获取
请求
（SUCI、指示信息1）
对SUCI进行解密，得到
SUPI，从预先配置的
SUPI与SUPI*的对应关系
中，得到的SUPI*
405、匿名化用户标识获取
响应
（SUPI*）
根据SUPI*，从预先配置
的SUPI*与用户签约数据
的对应关系中，确定UE
的用户签约数据，并根据
用户签约数据，得到
XRES*
406、用户认证响应2
（Nudm_UE
Authentication_Get
Response ）（XRES*）
基于XRES*，得到第
一HXRES*
407、用户认证响应1
（Nausf_UE
Authentication_Authenticate
Response1）
（指示信息2、XRES*）
408、用户认证请求3
（Authentication-Request)
409、用户认证响应3
（Authentication-
Response)
（RES*）
RES*与XRES*
相同
410、用户认证请求4
(Nausf_UE
Authentication_Authenticate
Request2)
（RES*）
基于RES*，得到第二
HXRES*
第一HXRES*与第二
HXRES*相同
411、密钥获取请求（SUPI*、RES*）
412、密钥获取响应
（SUPI*、密钥K_{AMF}）
413、用户认证响应
4Nausf_UE
Authentication_Authenticate
Responset2
（SUPI*、密钥K_{AMF}）

图 4

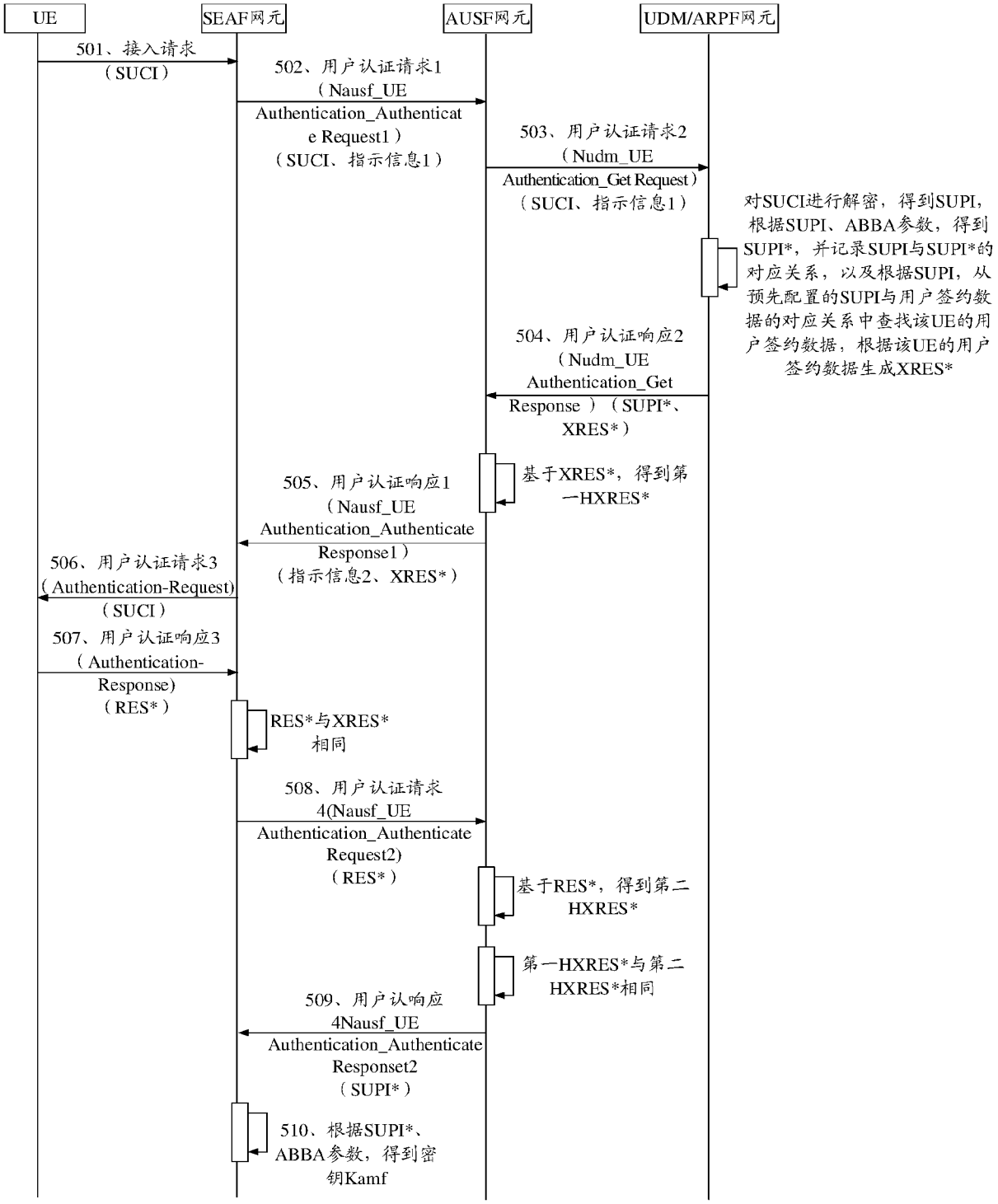
UE
SEAF网元
AUSF网元
UDM/ARPF网元
501、接入请求
（SUCI）
502、用户认证请求1
（Nausf_UE
Authentication_Authenticat
e Request1）
（SUCI、指示信息1）
503、用户认证请求2
（Nudm_UE
Authentication_Get Request）
（SUCI、指示信息1）
对SUCI进行解密，得到SUPI，
根据SUPI、ABBA参数，得到
SUPI*，并记录SUPI与SUPI*的
对应关系，以及根据SUPI，从
预先配置的SUPI与用户签约数
据的对应关系中查找该UE的用
户签约数据，根据该UE的用户
签约数据生成XRES*
504、用户认证响应2
（Nudm_UE
Authentication_Get
Response ）（SUPI*、
XRES*）
基于XRES*，得到第
一HXRES*
505、用户认证响应1
（Nausf_UE
Authentication_Authenticate
Response1）
（指示信息2、XRES*）
506、用户认证请求3
（Authentication-Request)
（SUCI）
507、用户认证响应3
（Authentication-
Response)
（RES*）
RES*与XRES*
相同
508、用户认证请求
4(Nausf_UE
Authentication_Authenticate
Request2)
（RES*）
基于RES*，得到第二
HXRES*
第一HXRES*与第二
HXRES*相同
509、用户认响应
4Nausf_UE
Authentication_Authenticate
Responset2
（SUPI*）
510、根据SUPI*、
ABBA参数，得到密
钥Kamf

图 5

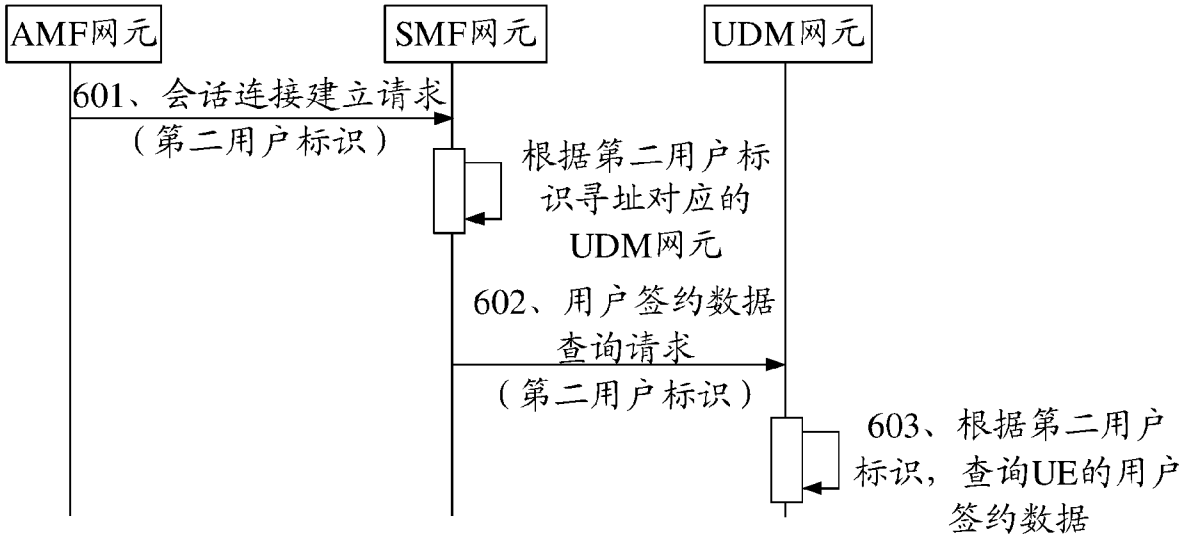
AMF网元
SMF网元
UDM网元
601、会话连接建立请求
（第二用户标识）
根据第二用户标识寻址对应的UDM网元
602、用户签约数据查询请求
（第二用户标识）
603、根据第二用户标识，查询UE的用户签约数据

图 6

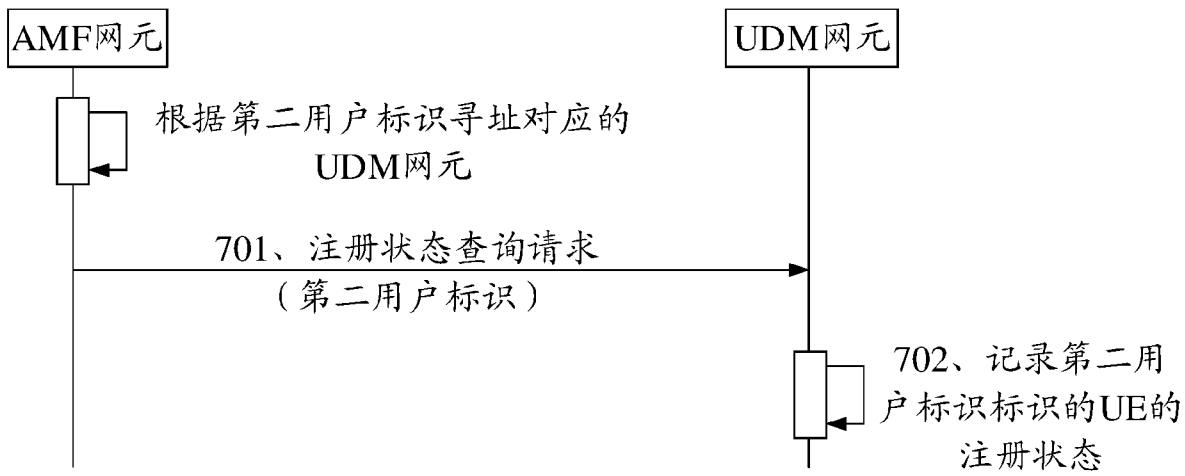
AMF网元
UDM网元
根据第二用户标识寻址对应的UDM网元
701、注册状态查询请求
（第二用户标识）
702、记录第二用户标识标识的UE的注册状态

图 7

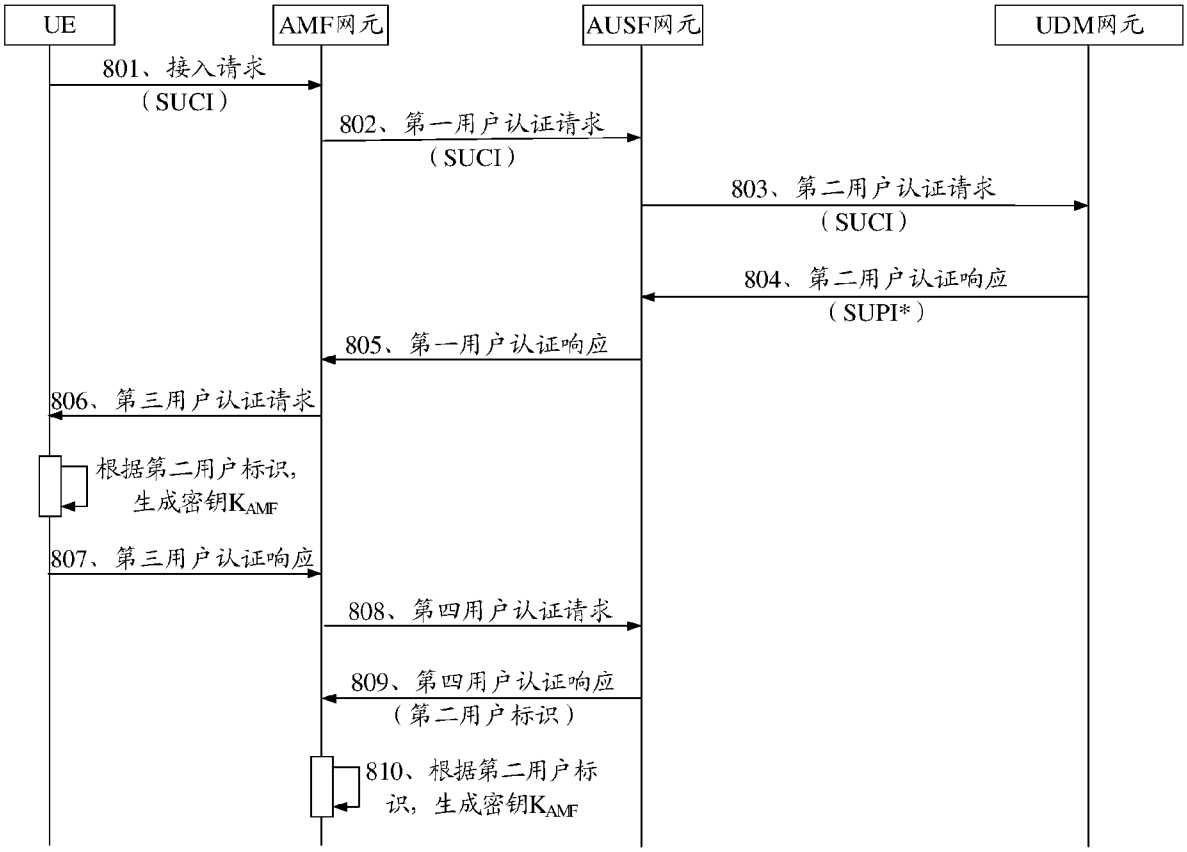
UE
AMF网元
AUSF网元
UDM网元
801、接入请求
（SUCI）
802、第一用户认证请求
（SUCI）
803、第二用户认证请求
（SUCI）
804、第二用户认证响应
（SUPI*）
805、第一用户认证响应
806、第三用户认证请求
根据第二用户标识，
生成密钥K_{AMF}
807、第三用户认证响应
808、第四用户认证请求
809、第四用户认证响应
（第二用户标识）
810、根据第二用户标
识，生成密钥K_{AMF}

图 8

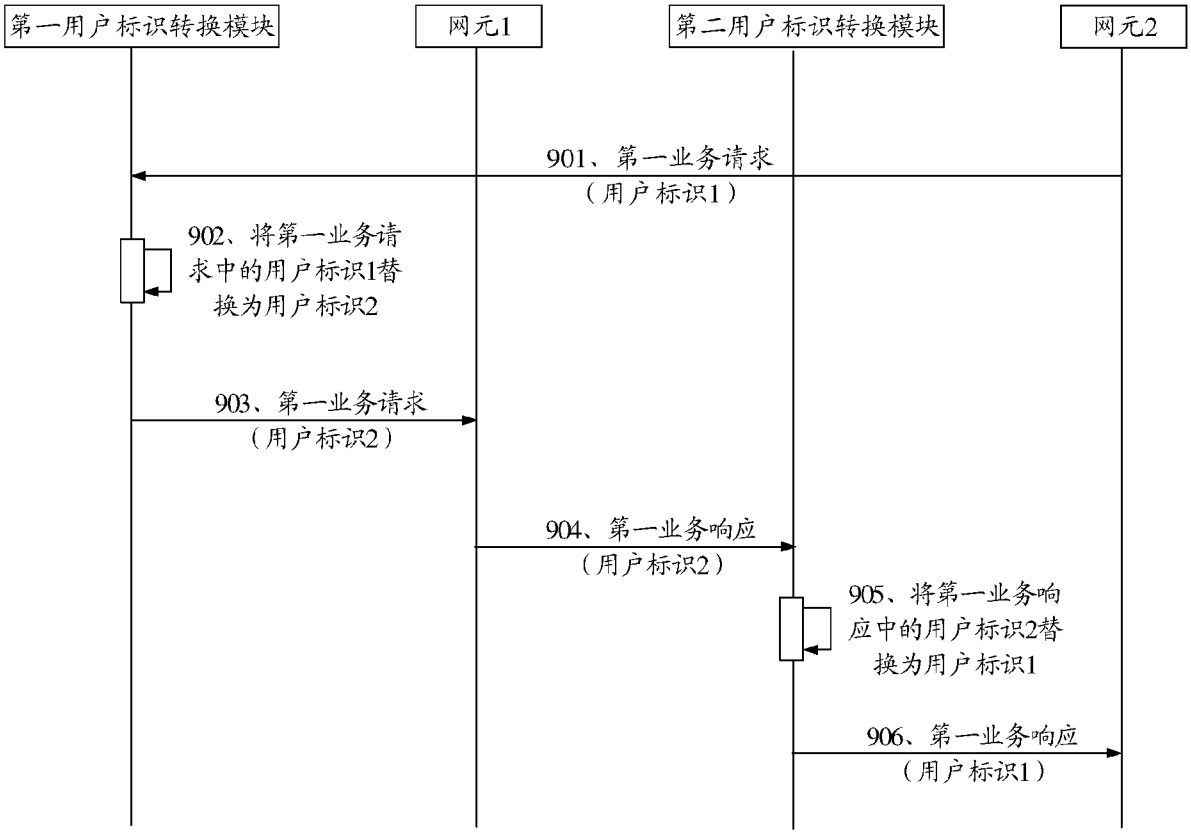
第一用户标识转换模块
网元1
第二用户标识转换模块
网元2
901、第一业务请求
（用户标识1）
902、将第一业务请求中的用户标识1替换为用户标识2
903、第一业务请求
（用户标识2）
904、第一业务响应
（用户标识2）
905、将第一业务响应中的用户标识2替换为用户标识1
906、第一业务响应
（用户标识1）

图 9

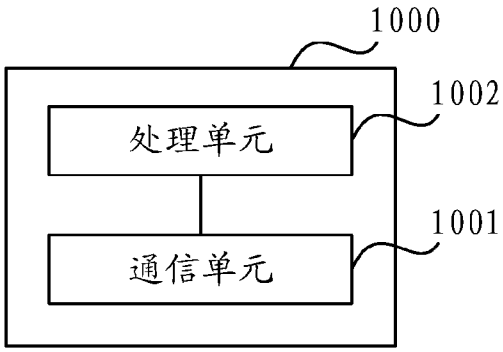
1000
1002
处理单元
1001
通信单元

图 10

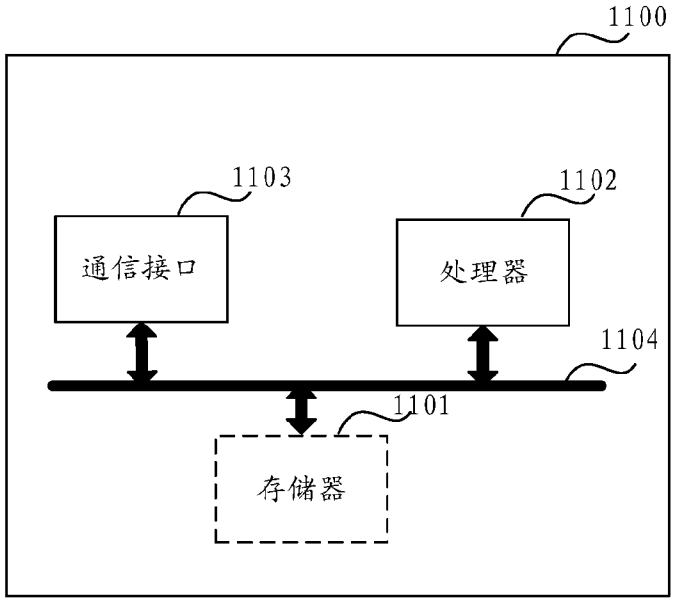
1100
1103
通信接口
1102
处理器
1104
1101
存储器

图 11

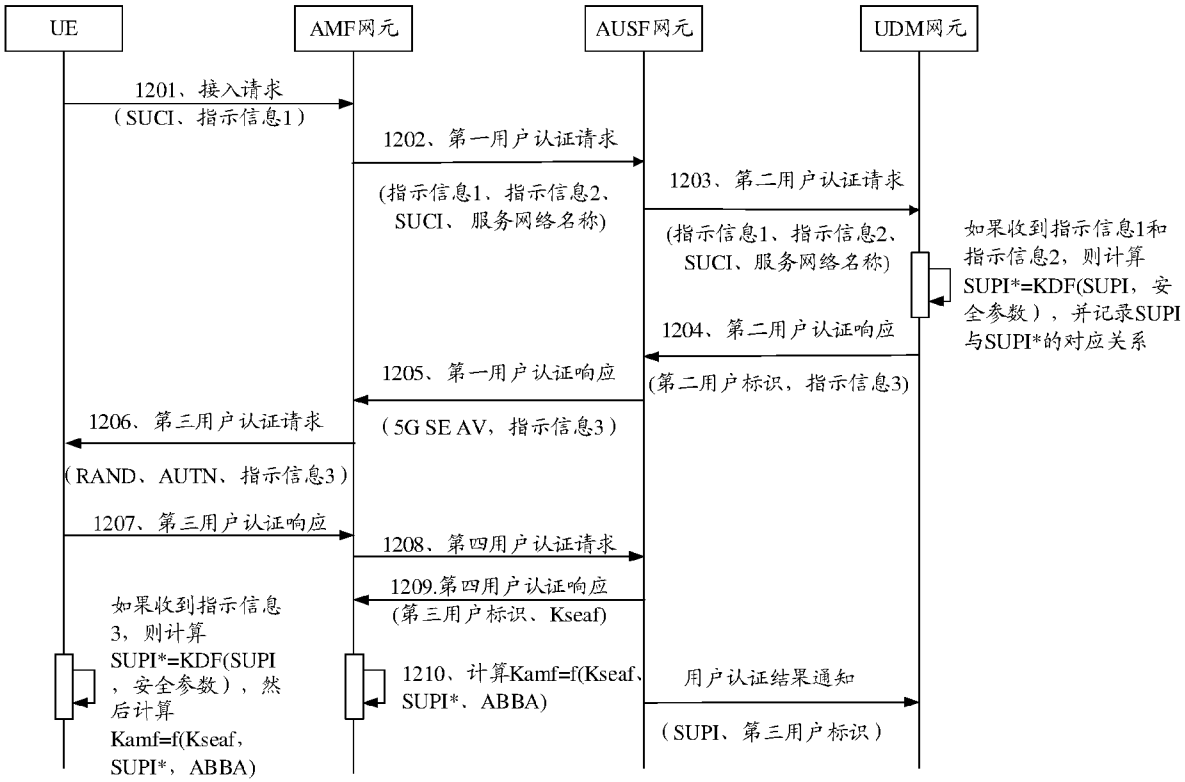
UE
AMF网元
AUSF网元
UDM网元
1201、接入请求
（SUCI、指示信息1）
1202、第一用户认证请求
(指示信息1、指示信息2、
SUCI、服务网络名称)
1203、第二用户认证请求
(指示信息1、指示信息2、
SUCI、服务网络名称)
如果收到指示信息1和
指示信息2，则计算
SUPI*=KDF(SUPI，安
全参数），并记录SUPI
与SUPI*的对应关系
1204、第二用户认证响应
(第二用户标识，指示信息3)
1205、第一用户认证响应
（5G SE AV，指示信息3）
1206、第三用户认证请求
（RAND、AUTN、指示信息3）
1207、第三用户认证响应
1208、第四用户认证请求
1209.第四用户认证响应
(第三用户标识、Kseaf)
如果收到指示信息
3，则计算
SUPI*=KDF(SUPI
，安全参数），然
后计算
Kamf=f(Kseaf，
SUPI*，ABBA)
1210、计算Kamf=f(Kseaf、
SUPI*、ABBA)
用户认证结果通知
（SUPI、第三用户标识）

图 12

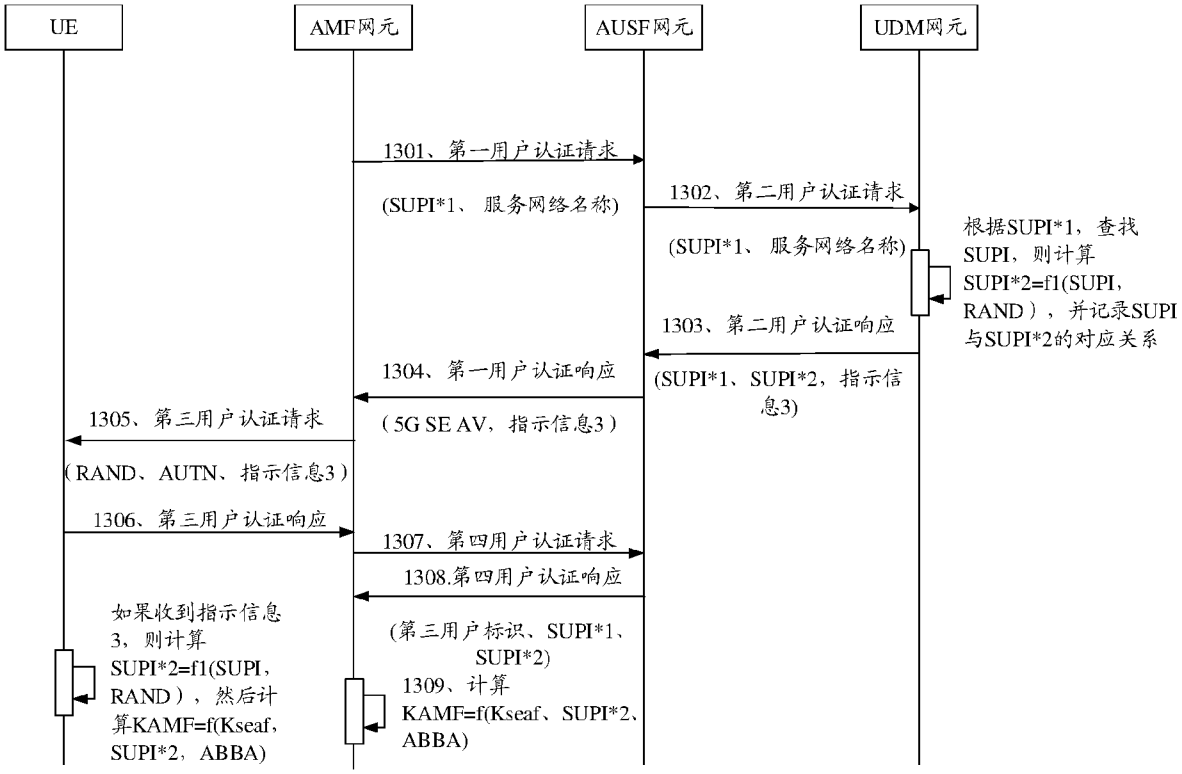
UE
AMF网元
AUSF网元
UDM网元
1301、第一用户认证请求
(SUPI*1、 服务网络名称)
1302、第二用户认证请求
(SUPI*1、 服务网络名称)
根据SUPI*1，查找SUPI，则计算SUPI*2=f1(SUPI，RAND），并记录SUPI与SUPI*2的对应关系
1303、第二用户认证响应
(SUPI*1、SUPI*2，指示信息3)
1304、第一用户认证响应
（5G SE AV，指示信息3）
1305、第三用户认证请求
（RAND、AUTN、指示信息3）
1306、第三用户认证响应
1307、第四用户认证请求
1308.第四用户认证响应
(第三用户标识、SUPI*1、SUPI*2)
如果收到指示信息3，则计算SUPI*2=f1(SUPI，RAND），然后计算KAMF=f(Kseaf，SUPI*2，ABBA)
1309、计算KAMF=f(Kseaf、SUPI*2、ABBA)

图 13

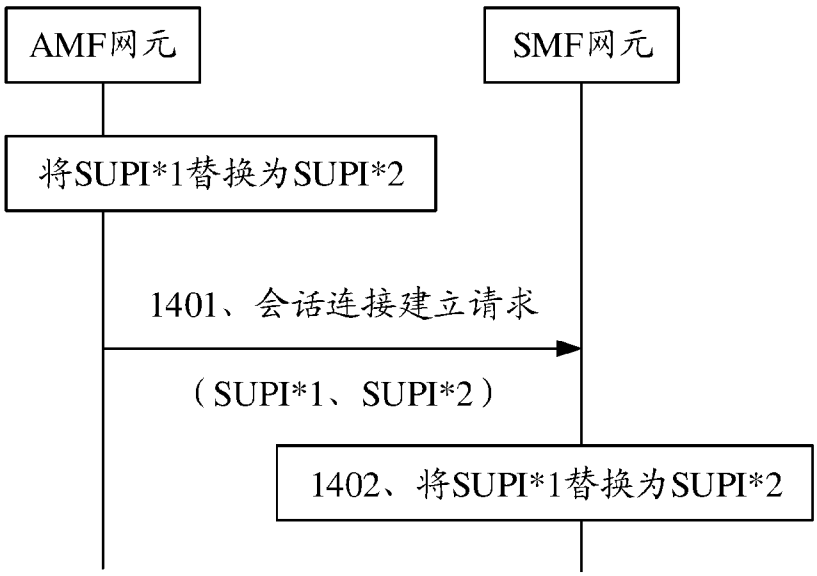
AMF网元
SMF网元
将SUPI*1替换为SUPI*2
1401、会话连接建立请求
（SUPI*1、SUPI*2）
1402、将SUPI*1替换为SUPI*2

图 14

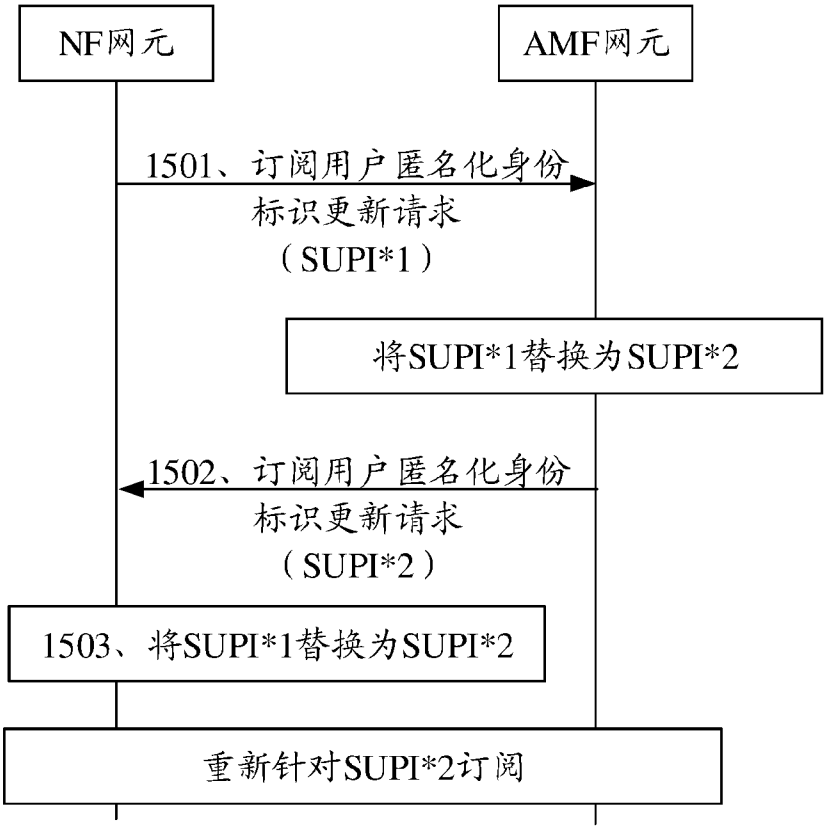
NF网元
AMF网元
1501、订阅用户匿名化身份标识更新请求（SUPI*1）
将SUPI*1替换为SUPI*2
1502、订阅用户匿名化身份标识更新请求（SUPI*2）
1503、将SUPI*1替换为SUPI*2
重新针对SUPI*2订阅

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/104598

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/02(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04M; H04Q; H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPTXT; USTXT; WOTXT; CNTXT; VEN; CNABS; CNKI; 3GPP: 加密, 盗用, 用户永久标识符, 匿名化身份标识, 移动管理网元, 认证服务网元, 数据管理网元, 追踪, 安全, 网络, SUPI, SUCI, authentication, encrypt+, AUSF, AMF, UDM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 108848502 A (XINGTANG COMMUNICATION TECHNOLOGY CO., LTD.) 20 November 2018 (2018-11-20) description paragraph [0063]- paragraph [0090]	1-39
A	CN 108683510 A (XINGTANG COMMUNICATION SCIENCE & TECHNOLOGY CO., LTD.) 19 October 2018 (2018-10-19) entire document	1-39
A	CN 108848495 A (XINGTANG COMMUNICATION SCIENCE & TECHNOLOGY CO., LTD.) 20 November 2018 (2018-11-20) entire document	1-39
A	US 10299128 B1 (CISCO TECHNOLOGY INC.) 21 May 2019 (2019-05-21) entire document	1–39

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 September 2020	**29 September 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/104598

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108848502 A	20 November 2018	None	
CN 108683510 A	19 October 2018	None	
CN 108848495 A	20 November 2018	None	
US 10299128 B1	21 May 2019	US 2019379544 A1	12 December 2019
		WO 2019236454 A1	12 December 2019
		US 2019380031 A1	12 December 2019
		US 10361843 B1	23 July 2019
		US 10673618 B2	02 June 2020

国际检索报告

国际申请号
PCT/CN2020/104598

A. 主题的分类

H04W 12/02(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04M; H04Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

EPTXT;USTXT;WOTXT;CNTXT;VEN;CNABS;CNKI;3GPP:加密，盗用，用户永久标识符,匿名化身份标识， 移动管理网元, 认证服务网元， 数据管理网元， 追踪， 安全，网络，SUPI, SUCI, authentication，encrypt+， AUSF, AMF, UDM

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 108848502 A (兴唐通信科技有限公司) 2018年 11月 20日 (2018-11-20) 说明书第[0063]段-第[0090]段	1-39
A	CN 108683510 A (兴唐通信科技有限公司) 2018年 10月 19日 (2018-10-19) 全文	1-39
A	CN 108848495 A (兴唐通信科技有限公司) 2018年 11月 20日 (2018-11-20) 全文	1-39
A	US 10299128 B1 (思科技术公司) 2019年 5月 21日 (2019-05-21) 全文	1-39

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

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

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 9月 23日	2020年 9月 29日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王菊
传真号 (86-10)62019451	电话号码 86-(010)-62411392

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/104598

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	108848502	A	2018年 11月 20日	无			
CN	108683510	A	2018年 10月 19日	无			
CN	108848495	A	2018年 11月 20日	无			
US	10299128	B1	2019年 5月 21日	US	2019379544	A1	2019年 12月 12日
				WO	2019236454	A1	2019年 12月 12日
				US	2019380031	A1	2019年 12月 12日
				US	10361843	B1	2019年 7月 23日
				US	10673618	B2	2020年 6月 2日