

(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
2015年7月9日 (09.07.2015)



(10) 国际公布号
WO 2015/100974 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01)
- (21) 国际申请号: PCT/CN2014/080713
- (22) 国际申请日: 2014年6月25日 (25.06.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310753800.6 2013年12月31日 (31.12.2013) 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: 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: 广州三环专利代理有限公司 (GUANG-ZHOU SCIHEAD PATENT AGENT CO., LTD); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, 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,

[见续页]

(54) Title: TERMINAL AUTHENTICATION METHOD, DEVICE AND SYSTEM

(54) 发明名称: 一种终端认证的方法、装置及系统

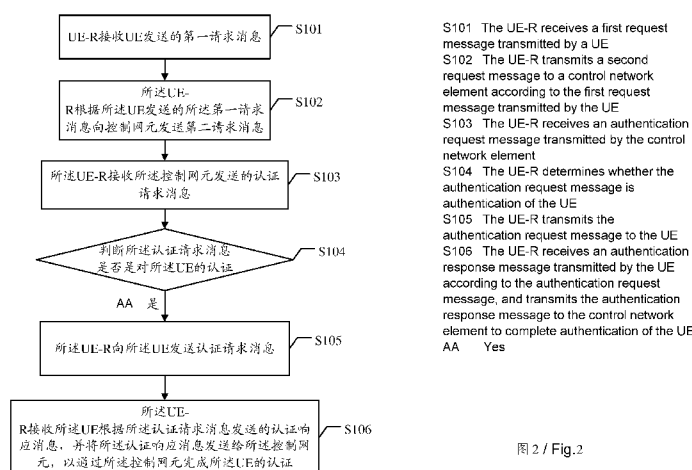


图2 / Fig.2

(57) Abstract: Disclosed in an embodiment of the present invention is a terminal authentication method, comprising: a user equipment to network relay (UE-R) receives a first request message transmitted by a user equipment (UE); the UE-R transmits a second request message to a control network element according to the first request message transmitted by the UE; the UE-R receives an authentication request message transmitted by the control network element and determines whether the authentication request message is authentication of the UE; if yes, then the UE-R transmits the authentication request message to the UE; the UE-R receives an authentication response message transmitted by the UE according to the authentication request message, and transmits the authentication response message to the control network element. Also disclosed in an embodiment of the present invention is a terminal authentication device. The present invention has the advantages of easy operation, reduced complexity and costs of the terminal, and improved terminal authentication efficiency and user experience.

(57) 摘要:

[见续页]

WO 2015/100974 A1



RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**

CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

本发明实施例公开了一种终端认证的方法，包括：用户设备中继 UE-R 接收用户设备 UE 发送的第一请求消息；所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息；所述 UE-R 接收所述控制网元发送的认证请求消息，判断所述认证请求消息是否是对所述 UE 的认证；若所述认证请求消息是对所述 UE 的认证，所述 UE-R 向所述 UE 发送认证请求消息；所述 UE-R 接收所述 UE 根据所述认证请求消息发送的认证响应消息，并将所述认证响应消息发送给所述控制网元。本发明实施例还公开了一种终端认证的装置。本发明具有操作简单，可降低终端的复杂性和成本，提高终端认证的效率和用户体验的优点。

一种终端认证的方法、装置及系统

技术领域

本发明涉及通信技术领域，尤其涉及一种终端认证的方法、装置及系统。

背景技术

近距离通信业务（Proximity Service, ProSe）技术主要是在两个距离较近的用户终端（User Equipment, UE）之间建立安全的通信信道，使得两个 UE 进行端到端的数据传输时数据能够进行安全的交换。ProSe 技术主要包括：ProSe Discovery 和 ProSe Communication 两部分，其中，在 ProSe 阶段，上述两个 UE 需要借助演进的通用陆地无线接入网（Evolved Universal Terrestrial Radio Access Network, E-UTRAN）或者其他非网络节点技术检测到对方，完成对双方身份的检验；在 ProSe Communication 阶段，上述两个 UE 需要借助 E-UTRAN 或者其他非网络节点技术建立安全的通信信道，建立安全的通信信道之后则可进行安全的数据通信。在 ProSe 技术的具体应用中，UE 可通过用户设备中继（UE-to-Network Relay, UE-R）接入到网络演进的分组核心（Evolved Packet Core, EPC），在一些具体的应用场景中，UE 可能没有被 EPC 网络信号覆盖，而 UE-R 有被 EPC 网络信号所覆盖，此时，UE 可通过 UE-R 接入到 EPC 网络中。在上述场景中，由于 UE 可通过 UE-R 接入到 EPC 网络，使得 UE 接入到 EPC 网络的过程中可能存在着未授权的 UE 接入到网络的安全威胁，故此，需要采取相应的安全措施来防止未授权的 UE 接入到网络中。

现有技术中主要是采用扩展认证协议-认证与密钥分配（Extensible Authentication Protocol- Authentication and Key Agreement, EAP-AKA）认证协议，通过验证、授权和账户（Authentication, Authorization and Accounting，AAA）Server（归属用户服务器）和 UE-R 完成远程 UE 与网络之间的认证，现有技术采用 EAP-AKA 协议对 UE 进行认证，使得 UE 需要支持演进的分组系统（Evolved Packet System，EPS）AKA 认证，也要支持 EAP-AKA 认证，增加了终端（即 UE）的复杂性和成本，对现有协议影响较大，UE-R 也需要新的协议栈来承载 Radius 协议或 Diameter 协议，增加了 UE-R 的复杂性和成

本。此外，现有技术采用 EAP-AKA 认证协议，通过 AAA Server 和 UE-R 完成远程 UE 与网络之间的认证时需要的消息流程较大，UE 认证的效率也较低，用户体验效果低。

发明内容

本发明实施例提供一种终端认证的方法、装置及系统，可采用 EPS AKA 认证完成对通过 UE-R 接入网络的 UE 的认证，操作简单，降低了终端的复杂度和成本，提高了 UE 认证的效率和用户体验。

本发明实施例第一方面提供了一种终端认证的方法，其可包括：

用户设备中继 UE-R 接收用户设备 UE 发送的第一请求消息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，以使所述控制网元根据所述第二请求消息向归属用户服务器 HSS 发送认证数据请求消息，其中，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述 UE-R 接收所述控制网元发送的认证请求消息，判断所述认证请求消息是否是对所述 UE 的认证；

若所述认证请求消息是对所述 UE 的认证，所述 UE-R 向所述 UE 发送认证请求消息，所述认证请求消息中包括所述 UE 的认证参数；

所述 UE-R 接收所述 UE 根据所述认证请求消息发送的认证响应消息，并将所述认证响应消息发送给所述控制网元，以通过所述控制网元完成所述 UE 的认证。

结合第一方面，在第一种可能的实现方式中，所述 UE 发送的第一请求消息中包含所述 UE 认证的标识信息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，包括：

所述 UE-R 将所述第一请求消息中携带的所述 UE 认证的标识信息添加到所述第二请求消息中，并将所述第二请求消息发送给所述控制网元。

结合第一方面或第一方面第一种可能的实现方式，在第二种可能的实现方式中，所述 UE 发送的第一请求消息不包含所述 UE 认证的标识信息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息, 包括:

所述 UE-R 在所述第二请求消息中添加所述 UE 认证的标识信息, 并将所述第二请求消息发送给所述控制网元。

结合第一方面至第一方面第二种可能的实现方式中任一种, 在第三种可能的实现方式中, 所述控制网元发送的认证请求消息中包括所述 HSS 根据所述 UE 认证的标识信息设定的对所述 UE 认证的认证标识信息;

所述判断所述认证请求消息是否是对所述 UE 的认证, 包括:

判断所述认证请求消息中是否包含认证标识信息;

若所述认证请求消息中包含所述认证标识信息, 则判断所述认证请求消息为对所述 UE 的认证。

本发明实施例第二方面提供了一种终端的认证方法, 其可包括:

HSS 接收控制网元发送的认证数据请求消息, 根据所述认证数据请求消息判断所述认证数据请求消息是否包括 UE 认证的标识信息;

若所述认证数据请求消息中包括所述 UE 认证的标识信息, 所述 HSS 在认证矢量中设定所述 UE 认证的认证标识信息;

所述 HSS 将所述认证矢量发送给所述控制网元, 以通过所述控制网元将所述认证标识信息发送给 UE-R, 以使所述 UE-R 根据所述认证标识信息判断是否是对所述 UE 的认证。

结合第二方面, 在第一种可能的实现方式中, 所述认证矢量中包括: RAND 参数、AUTN 参数、XRES 参数、和 Ksme 参数;

所述 HSS 在所述认证矢量中设定所述 UE 认证的认证标识信息, 包括:

所述 HSS 在所述认证矢量中的 AUTN 参数中的认证管理域 AMF 参数中设定所述认证标识信息。

结合第二方面或第二方面第一种可能的实现方式, 在第二种可能的实现方式中, 所述认证矢量中包括: RAND 参数、AUTN 参数、XRES 参数和 Ksme 参数;

所述 HSS 在所述认证矢量中设定所述 UE 认证的认证标识信息, 还包括:

所述 HSS 对所述认证矢量中的 RAND 参数进行加密;

所述 HSS 在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

本发明实施例第三方面提供了一种终端认证的方法，其可包括：

UE 向 UE-R 发送第一请求消息，以使所述 UE-R 根据所述第一请求消息向控制网元发送第二请求消息；

所述 UE 接收所述 UE-R 发送的认证请求消息，所述认证请求消息中携带所述 UE 认证标识信息；

所述 UE 对所述认证标识信息中的加密信息进行解密，并根据所述解密得到的信息计算认证响应；

所述 UE 将所述认证响应发送给所述 UE-R，以通过所述 UE-R 发送给控制网元对所述 UE 进行认证。

结合第三方面，在第一种可能的实现方式中，所述 UE 向 UE-R 发送的所述第一请求消息中包括所述 UE 认证的标识信息。

本发明实施例第四方面提供了一种终端认证的方法，其可包括：

控制网元接收 UE-R 发送的第二请求消息，判断所述第二请求消息是否包含 UE 认证的标识信息；

若所述第二请求消息包含所述 UE 认证的标识信息，所述控制网元向 HSS 发送认证数据请求消息，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述控制网元从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量；

所述控制网元将包含所述认证矢量信息的认证请求消息发送给所述 UE-R，以供所述 UE-R 判断所述认证请求消息是否是对 UE 的认证。

结合第四方面，在第一种可能的实现方式中，所述控制网元接收 UE-R 发送的第二请求消息之后，所述方法还包括：

判断所述第二请求消息是否为指定消息类型；

若所述第二请求消息为所述指定消息类型，所述控制网元向 HSS 发送认证数据请求消息。

结合第四方面或第四方面第一种可能的实现方式，在第二种可能的实现方

式中, 所述控制网元向 HSS 发送认证数据请求消息之前, 所述方法还包括:

所述控制网元添加所述 UE 认证的标识信息到所述认证数据请求消息中。

结合第四方面至第四方面第二种可能的实现方式中任一种, 在第三种可能的实现方式中, 所述控制网元将包含所述认证矢量的认证请求消息发送给所述 UE-R 之前, 所述方法还包括:

所述控制网元添加所述 UE 认证的标识信息到所述认证请求消息中。

本发明实施例第五方面提供了一种终端认证的中继设备, 其可包括:

接收模块, 用于接收 UE 发送的第一请求消息;

发送模块, 用于根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息, 以使所述控制网元根据所述第二请求消息向 HSS 发送认证数据请求消息, 其中, 所述认证数据请求消息中携带所述 UE 认证的标识信息;

所述接收模块, 用于接收所述控制网元发送的认证请求消息;

判断模块, 用于根据所述接收模块接收到的所述认证请求消息判断所述认证请求消息是否是对所述 UE 的认证;

所述发送模块, 用于在所述判断模块判断结果为是时, 向所述 UE 发送认证请求消息, 所述认证请求消息中包括所述 UE 的认证参数;

所述接收模块, 还用于接收所述 UE 根据所述发送模块发送的所述认证请求消息发送的认证响应消息;

所述发送模块, 用于将所述接收模块接收到的所述认证响应消息发送给所述控制网元, 以通过所述控制网元完成所述 UE 的认证。

结合第五方面, 在第一种可能的实现方式中, 所述接收模块接收到的所述 UE 发送的第一请求消息中包含所述 UE 认证的标识信息;

所述发送模块, 还具体用于:

将所述第一请求消息中携带的所述 UE 认证的标识信息添加到所述第二请求消息中, 并将所述第二请求消息发送给所述控制网元。

结合第五方面或第五方面第一种可能的实现方式, 在第二种可能的实现方式中, 所述接收模块接收到的所述 UE 发送的第一请求消息中不包含所述 UE 认证的标识信息;

所述发送模块, 具体用于:

在所述第二请求消息中添加所述 UE 认证的标识信息，并将所述第二请求消息发送给所述控制网元。

结合第五方面至第五方面第二种可能的实现方式中任一种，在第三种可能的实现方式中，所述接收模块接收到的所述控制网元发送的认证请求消息中包括所述 HSS 根据所述 UE 认证的标识信息设定的对所述 UE 认证的认证标识信息；

所述判断模块，具体用于：

判断所述认证请求消息是否包含认证标识信息；

若所述认证请求消息中包含所述认证标识信息，则判断所述认证请求消息为对所述 UE 的认证。

本发明实施例第六方面提供了一种终端认证的服务器，其可包括：

接收模块，用于接收控制网元发送的认证数据请求消息；

判断模块，用于根据所述接收模块接收到的所述认证数据请求消息判断所述认证数据请求消息是否包含 UE 认证的标识信息；

处理模块，用于在所述判断模块判断结果为是时，在认证矢量中设定所述 UE 认证的认证标识信息；

发送模块，用于所述处理模块处理得到的将所述认证矢量发送给所述控制网元，以通过所述控制网元将所述认证标识信息发送给 UE-R，以使所述 UE-R 根据所述认证标识信息判断是否是对所述 UE 的认证。

结合第六方面，在第一种可能的实现方式中，所述处理模块处理得到的所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数、和 K_{asme} 参数；

所述处理模块，具体用于：

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

结合第六方面或第六方面第一种可能的实现方式，在第二种可能的实现方式中，所述处理模块处理得到的所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数和 K_{asme} 参数；

所述处理模块，还具体用于：

对所述认证矢量中的 RAND 参数进行加密；

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

本发明实施例第七方面提供了一种终端认证的用户设备，其可包括：

发送模块，用于向 UE-R 发送第一请求消息，以使所述 UE-R 根据所述第一请求消息向控制网元发送第二请求消息；

接收模块，用于接收所述 UE-R 发送的认证请求消息，所述认证请求消息中携带 UE 认证的认证标识信息；

处理模块，用于对所述认证标识信息中的加密信息进行解密，并根据所述解密得到的信息计算认证响应。

结合第七方面，在第一种可能的实现方式中，所述发送模块发送的所述第一请求消息中包括所述 UE 认证的标识信息。

本发明实施例第八方面提供了一种终端认证的控制设备，其可包括：

接收模块，用于接收 UE-R 发送的第二请求消息；

处理模块，用于根据所述接收模块接收到的所述第二请求消息判断所述第二请求消息是否包含 UE 认证的标识信息；

发送模块，用于在所述处理模块判断结果为是时，向 HSS 发送认证数据请求消息，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述接收模块，用于从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量；

所述发送模块，还用于将所述接收模块接收到的包含所述认证矢量信息的认证请求消息发送给所述 UE-R，以供所述 UE-R 判断所述认证请求消息是否是对 UE 的认证。

结合第八方面，在第一种可能的实现方式中，所述控制设备，还包括：

判断模块，用于根据所述接收模块接收到的第二请求消息判断所述第二请求消息是否为指定消息类型，若所述第二请求消息为所述指定消息类型，则通知所述发送模块向 HSS 发送认证数据请求消息。

结合第八方面或第八方面第一种可能的实现方式，在第二种可能的实现方式中，所述发送模块，还具体用于：

添加所述 UE 认证的标识信息到所述认证数据请求消息中，并将所述认证

数据请求消息发送给所述 HSS。

结合第八方面至第八方面第二种可能的实现方式中任一种，在第三种可能的实现方式中，所述发送模块，还具体用于：

添加所述 UE 认证的标识信息到所述包含所述认证矢量的认证请求消息中，并将认证请求消息发送给所述 UE-R。

本发明实施例第九方面提供了一种终端认证的系统，其可包括：如本发明实施例第五方面提供的中继设备、本发明实施例第六方面提供的服务器、本发明实施例第七方面提供的用户设备和本发明实施例第八方面提供的控制设备。

在本发明实施例中，UE 通过 UE-R 接入网络时可通过 UE-R 将包括 UE 的标识信息的请求发送给控制网元，以通过控制网元获取 UE 的认证矢量消息，UE-R 可根据获取到的认证矢量消息判断该认证矢量消息是否为对 UE 的认证，若是，则将向 UE 发送认证请求，进而可通过控制网元完成 UE 的认证，操作简单，降低了终端的复杂度和成本，提高了 UE 认证的效率和用户体验。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是现有技术中采用 AKA 认证原理对 UE-R 进行认证的示意图；

图 2 是本发明实施例提供的终端认证的方法的第一实施例流程示意图；

图 3 是本发明实施例提供的终端认证的方法的第一交互示意图；

图 4 是本发明实施例提供的终端认证的方法的第二交互示意图；

图 5 是本发明实施例提供的终端认证的方法的第三交互示意图；

图 6 是本发明实施例提供的终端认证的方法的第二实施例流程示意图；

图 7 是本发明实施例提供的终端认证的方法的第四交互示意图；

图 8 是本发明实施例提供的终端认证的方法的第五交互示意图；

图 9 是本发明实施例提供的终端认证的方法的第六交互示意图；

图 10 是本发明实施例提供的终端认证的方法的第七交互示意图；

图 11 是本发明实施例提供的终端认证的方法的第八交互示意图；
图 12 是本发明实施例提供的终端认证的方法的第三实施例流程示意图；
图 13 是本发明实施例提供的终端认证的方法的第四实施例流程示意图；
图 14 是本发明实施例提供的终端认证的方法的第九交互示意图；
图 15 是本发明实施例提供的终端认证的中继设备的实施例结构示意图；
图 16 是本发明实施例提供的终端认证的服务器的实施例结构示意图；
图 17 是本发明实施例提供的终端认证的用户设备的实施例结构示意图；
图 18 是本发明实施例提供的终端认证的控制设备的实施例的一结构示意图；
图 19 是本发明实施例提供的终端认证的控制设备的实施例的另一结构示意图；
图 20 是本发明实施例提供的终端认证的系统的结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，下面所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

在 ProSe 技术中，当 UE 通过 UE-R 接入网络时，本发明实施例可采用 EPS AKA 认证原理对接入网络的 UE 进行认证，防止未授权的 UE 通过 UE-R 接入网络，对网络造成安全威胁。在 ProSe 技术中，当 UE-R 作为普通的长期演进（Long Term Evolution, LTE）UE 接入网络时，网络对 UE-R 进行认证时采用的正是 EPS AKA 认证。同样，基于通用引导架构（Generic Bootstrapping Architecture, GBA）的 AKA 引导过程（bootstrapping procedure）可以替换 EPS AKA 认证流程应用在以下描述的实施例中。本发明实施例中移动管理实体（Mobility Management Entity, MME）也可以为 ProSe Function（ProSe 业务中功能控制网元）。

参见图 1，是现有技术中网络采用 AKA 对 UE-R 进行认证的交互示意图，其可包括步骤：A1-A10。

A1, UE-R 向 MME 发送请求。

在现有技术中, UE-R 向 MME 发送的请求中包括 UE-R 的国际移动用户识别码 (International Mobile Subscriber Identity, IMSI)。

A2, MME 向 HSS 发送认证数据请求。

在现有技术中, MME 接收到 UE-R 发送的请求之后则可向归属用户服务器 (Home Subscriber Server, HSS) 发送认证数据请求, 其中, 上述认证数据请求中包括 UE-R 的 IMSI。

A3, HSS 计算认证矢量。

在现有技术中, 当 HSS 接收到 MME 发送的认证数据请求时, HSS 则可计算对 UE-R 进行认证的认证矢量, 其中, 上述认证矢量中包括: RAND (RANDom number) 参数、AUTN (Authentication token) 参数、XRES (Expected user RESponse) 参数、Kasme 参数等。

A4, HSS 向 MME 发送认证数据响应。

具体的, HSS 向 MME 发送的认证数据响应中包括: RAND 参数、AUTN 参数、ARES 参数、Kasme 等。

A5, MME 存储认证数据响应。

在现有技术中, MME 接收到 HSS 发送的认证数据响应之后, 则可将接收到的认证数据响应存储起来, 并向 UE-R 发送认证请求。

A6, MME 向 UE-R 发送认证请求。

具体的, 上述 MME 向 UE-R 发送的认证请求中包括上述 RAND 参数和 AUTN 参数。

A7, UE-R 验证 AUTN, 并计算 RES (RESponse) 参数。

在现有技术中, UE-R 接收到 MME 发送的认证请求之后, 则可对上述认证请求中的 AUTN 进行验证, 验证 AUTN 正确之后, 则可计算 RES 参数, 进而可将上述 RES 参数发送给 MME。

A8, UE-R 向 MME 发送用户认证响应。

A9, MME 认证 UE。

A10, MME 向 UE-R 发送认证响应。

具体的, 上述用户认证响应中包括 RES 参数, MME 接收到 UE-R 发送的

RES 参数之后,则可上述 RES 参数与其存储的 XRES 参数进行比较,对 UE-R 进行认证。当 MME 比较得知 RES 和 XRES 一致时,则可通过 UE-R 的认证,完成对 UE-R 的认证,并将认证结果通过认证响应反馈给 UE-R。

本发明实施例在 UE 通过 UE-R 接入网络时,采用上述 EPS AKA 认证原理对 UE 进行认证,不需要新增协议(例如 EAP-AKA 协议)对 UE 进行认证,UE 只需要支持 EPS AKA 协议即可,无需同时支持 EPS AKA 协议和 EAP-AKA 协议,降低了终端的复杂度和成本。本发明实施例在 UE 通过 UE-R 接入网络时,通过 EPS AKA 协议对 UE 进行认证,UE-R 可直接支持 UE 的认证,无需在 UE 和 UE-R 之间建立新的协议栈来支撑新的协议,UE-R 支持 UE 认证的复杂性和成本低,操作便捷,认证效率高。下面将结合图 1 中所描述的 EPS AKA 的认证过程,对本发明实施中通过 EPS AKA 对 UE 进行认证的具体实现过程进行具体描述。

参见图 2,是本发明实施例提供的终端认证的方法的第一实施例流程示意图。本实施例中所描述的终端认证的方法,包括步骤:

S101, UE-R 接收 UE 发送的第一请求消息。

S102, 所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息。

在一些可行的实施方式中,上述 UE 发送的第一请求消息中可包括 UE 的识别码(IMSI)和 UE 的标识信息(Indication)(即 UE 认证的标识信息),其中,上述标识信息 Indication 可表示上述第一请求消息是 UE 通过 UE-R 接入网络而发送的请求。具体实现中,当 UE 通过 UE-R 接入网络并向 UE-R 发送了包含其 IMSI 和 Indication 的第一请求消息之后,UE-R 则可根据 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的,上述第二请求消息的消息类型可与上述第一请求消息的消息类型相同,也可不同,具体可根据 UE 认证的实际场景需求设定。

具体实现中,UE-R 向 MME 发送第二请求消息时,可在上述第二请求消息中添加 UE 认证的标识信息,其中,上述 UE 认证的标识信息用于标记上述第二请求消息是 UE 通过 UE-R 接入网络时,UE-R 向 MME 发送的请求消息。

具体的，当 UE-R 接收到 UE 发送的第一请求消息中包含 UE 认证的标识信息（即 Indication）时，UE-R 可将上述标识信息 Indication 作为 UE 认证的标识信息添加到上述第二请求消息中，也可以重新选择标识信息 Indication（与上述第一请求消息中包含的 UE 认证的标识信息功能相同），并将其作为 UE 认证的标识信息添加到上述第二请求消息中，其中上述重新选择的标识信息可以与上述第一请求消息中包含的 UE 认证的标识信息相同，也可不同；然后 UE-R 将上述第二请求消息发送给 MME（即控制网元）。如图 3，当 UE-R 接收到 UE 发送的第一请求消息时，若接收到的第一请求消息中包括 UE 的 IMSI 和 Indication 时，UE-R 则可将上述第一请求消息中包括的 UE 的 IMSI 和 Indication 添加到第二请求消息中，也可以重新选择 Indication，并将 IMSI 和重新选择的 Indication 添加到第二请求消息中，然后将上述第二请求消息发送给控制网元。网络侧的控制网元通过 UE-R 接收到上述 UE-R 发送的第二请求消息之后，则可根据第二请求消息中包含的 UE 的 Indication 判断得知当前需要进行认证的是通过 UE-R 接入网络的 UE，而非 UE-R 自身，进而 MME 可向 HSS 发送相应的用户认证数据请求消息。

在一些可行的实施方式中，如图 4，当上述 UE 发送的第一请求消息中仅包括 UE 的 IMSI，不包含上述 UE 认证的标识信息（Indication）时，当 UE 通过 UE-R 接入网络并向 UE-R 发送了包含其 IMSI 的第一请求消息之后，UE-R 则可根据 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的，上述第二请求消息的消息类型可与上述第一请求消息的消息类型相同，也可不同，具体可根据 UE 认证的实际场景需求设定。

具体实现中，如图 4，当 UE-R 接收到的上述第一请求消息中仅包含 UE 的 IMSI 时，UE-R 可在上述 UE 发送的第一请求消息中添加标识信息 Indication（即 UE 认证的标识信息），将上述 IMSI 和 Indication 添加到第二请求消息中，并将上述包括 UE 的 IMSI 和 Indication 的第二请求消息发送给控制网元。网络侧的控制网元通过 UE-R 接收到上述 UE-R 发送的第二请求消息之后，则可根据第二请求消息中包含的 UE 的 Indication 判断得知当前需要进行认证的是通过 UE-R 接入网络的 UE，而非 UE-R 自身。

具体实现中，如图 5，当上述 UE 发送的第一请求消息中仅包括 UE 的 IMSI

时,当 UE 通过 UE-R 接入网络并向 UE-R 发送了包含其 IMSI 的第一请求消息之后,UE-R 则可根据 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的,上述第二请求消息的消息类型可与上述第一请求消息的消息类型相同,也可不同,具体可根据 UE 认证的实际场景需求设定。

具体实现中,如图 5,当 UE-R 接收到的上述第一请求消息中仅包含 UE 的 IMSI 时,UE-R 可直接将上述第一请求消息中的 UE 的 IMSI 添加到第二请求消息中,并将上述包括 UE 的 IMSI 的第二请求消息发送给控制网元,即在上述实现方式中,UE-R 向控制网元发送的第二请求消息中包括的 UE 的 IMSI,不包含上述标识信息 Indication。具体实现中,在上述实现方式中,当 UE-R 将仅包含 UE 的 IMSI 的第二请求消息发送给网络侧的控制网元之后,由于上述第二请求消息中没有 Indication,控制网元无法直接从上述第二请求消息中获取 Indication,此时,控制网元可通过上述第二请求消息的消息类型判断上述请求是 UE 通过 UE-R 接入网络时发送的认证请求还是 UE-R 自身接入网络时 UE-R 发送的认证请求。具体的,控制网元可将接收到的上述第二请求消息的消息类型与预存的指定消息类型进行匹配,判断上述第二请求消息的消息类型是否属于上述指定消息类型,若判断得知上述第二请求消息的消息类型是上述指定消息类型,控制网元则可向 HSS 发送相应的用户认证数据请求消息,还可通过上述用户认证数据请求消息告知 HSS 是 UE 接入网络还是 UE-R 接入网络,即控制网元通过对上述第二请求消息的消息类型的判定来判断得知当前接收到的第二请求消息的消息类型是否是指定消息类型,以决定向 HSS 发送的用户认证数据请求消息中包含的内容,即可判断得知需要进行认证的是通过 UE-R 接入网络的 UE,而非 UE-R 自身。

在一些可行的实施方式中,网络侧接收到 UE-R 发送的第二请求消息之后,则可根据上述第二请求消息计算对 UE 进行认证的认证矢量。具体实现中,如图 3 或图 4,当网络侧的控制网元接收到的第二请求消息中包括标识信息 Indication 时,则可判断得知上述第二请求消息是 UE 通过 UE-R 接入网络而发送的请求,而非 UE-R 接入网络的请求,即当网络侧判断得知上述第二请求消息中包括 Indication 时,则可计算对 UE 进行认证的认证矢量。具体的,当网络侧判断得知上述第二请求消息中包括 Indication 时,可在计算对 UE 进行认

证的认证矢量中设定认证标识信息（即对 UE 认证的认证标识信息），用于表示上述认证矢量是对 UE 进行的认证，并将包含上述认证标识信息的认证矢量通过认证请求消息发送给 UE-R。具体的，网络侧设定对 UE 的认证的认证标识信息时可在上述认证矢量中的 AMF 参数中设定对 UE 的认证的认证标识信息，例如，可在认证矢量中的 AUTN 参数中置位 AMF 参数的第 X 比特为 1，其中，上述 $1 \leq X \leq 7$ ，即上述 AMF 参数的第 X 比特可以是 AMF 参数中空闲的 7 个比特中的任意一个，网络侧设定上述标志位并将包含上述标志位的认证矢量发送给 UE-R，UE-R 则可根据上述标志位来判断接收到的认证矢量是对 UE 的认证，而非对其自身的认证。

具体实现中，当网络侧接收到的第二请求消息中不包括上述标识信息 Indication 时，网络侧还可通过上述第二请求消息的消息类型判断得知上述第二请求消息的 UE 通过 UE-R 接入网络而发送的请求消息，而非 UE-R 接入网络而发送的请求消息。网络侧判断得知接收到的第二请求消息是 UE 通过 UE-R 接入网络而发送的请求消息时，则可计算对 UE 进行认证的认证矢量，并在上述认证矢量计算中设定对 UE 的认证的认证标识信息，进而将包含对 UE 的认证的认证标识信息的认证矢量参数 RAND、AUTN 发送给 UE-R。

S103，所述 UE-R 接收所述控制网元发送的认证请求消息。

S104，所述 UE-R 判断所述认证请求消息是否为对所述 UE 的认证，若判断结果为是，则执行步骤 S105。

S105，所述 UE-R 向所述 UE 发送认证请求消息。

在一些可行的实施方式中，UE-R 接收到网络侧的控制网元发送的认证请求消息之后，则可根据上述认证请求消息中包含的认证矢量的各参数信息判断上述认证请求消息是否是对 UE 的认证，如果判断得知上述认证请求消息是对 UE 的认证，UE-R 则向 UE 发送认证请求消息。具体实现中，当 UE-R 接收到控制网元发送的认证请求消息时，UE-R 则可判断上述认证请求消息中是否包含对 UE 的认证的认证标识信息，例如，UE-R 可判断上述认证请求消息中的认证矢量的 AMF 参数的第 X 比特是否为 1，如果 UE-R 判断得知上述认证矢量的 AMF 的第 X 比特是 1，则判断得知上述认证请求消息是对 UE 的认证；此外，如图 10，还可判断认证请求消息中是否包含标识信息 Indication2，若存

在标识信息 Indication2, 则判断得知上述认证请求消息是对 UE 的认证, UE-R 则可向 UE 发送认证请求消息, 并将上述认证矢量中的 AUTN 和 RAND 等参数发送给 UE, 以供 UE 进行验证。

S106, 所述 UE-R 接收所述 UE 根据所述认证请求消息发送的认证响应消息, 并将所述认证响应消息发送给所述控制网元, 以通过所述控制网元完成所述 UE 的认证。

在一些可行的实施方式中, UE-R 向 UE 发送认证请求消息时将从网络侧接收到的 RAND、AUTN 发送给 UE, UE 接收到 UE-R 发送的 RAND, AUTN 之后, 则可对 RAND、AUTN 参数进行验证, 验证 AUTN 参数的正确性。UE 验证 AUTN 正确之后, 则可计算 RES 参数, 并将计算得到的 RES 参数发送给 UE-R。UE-R 接收到 UE 发送的认证响应 (其中, 包括上述 RES 参数) 之后, 则可将上述认证响应发送给网络侧的控制网元, 以通过上述控制网元完成 UE 的认证。控制网元完成对 UE 的认证。

在本发明实施例中, UE-R 可接收 UE 发送的请求消息, 根据 UE 发送的请求消息向网络侧发送认证请求消息, 并从网络侧获取包含对 UE 认证的认证标识信息的认证矢量, UE-R 可根据网络侧发送的认证请求消息判断是对 UE 的认证还是对自身的认证, 进而将认证请求消息发送给 UE, 完成对 UE 的认证, 操作简单, 终端成本低, 提高了 UE 认证的效率和用户体验。

参见图 6, 是本发明实施例提供的终端认证的方法的第二实施例流程示意图。本实施例中所描述的终端认证的方法, 包括步骤:

S201, HSS 接收控制网元发送的认证数据请求消息。

S202, 判断所述认证数据请求消息是否包括 UE 认证的标识信息, 若判断结果为是, 则执行步骤 S203。

S203, 所述 HSS 在认证矢量中设定所述 UE 认证的认证标识信息。

S204, 所述 HSS 将所述认证矢量发送给所述控制网元。

在一些可行的实施方式中, 处于网络侧的 HSS 接收到控制网元发送的认证数据请求消息之后, 则可判断上述认证数据请求消息中是否包含 UE 认证的标识信息, 其中, 上述 UE 认证的标识信息具体可为 UE 向 UE-R 发送的第一

请求消息中携带的 Indication, UE-R 将上述第一请求消息中携带的 Indication 添加到第二请求消息中, 进而将上述第二请求消息发送给控制网元, 通过控制网元发送给 HSS; 上述 UE 认证的标识信息也可为 UE-R 根据上述第一请求消息在向控制网元发送第二请求消息时添加的 Indication, UE-R 在上述第二请求消息中添加 Indication 之后将上述第二请求消息发送给控制网元, 控制网元可将上述第二请求消息中携带的 Indication 发送给 HSS, 即上述第二请求消息中的 UE 认证的标识信息也可以为控制网元自己选择的 Indication。如图 3、图 4 或图 5, 当 HSS 接收到控制网元发送的认证数据请求消息之后, 则可判断上述认证数据请求消息中是否包含 UE 认证的标识信息, 即上述认证数据请求消息中是否存在 Indication, 若判断得知上述认证数据请求消息中包括 Indication, 则可判断得知上述认证数据请求消息的认证对象为 UE。具体实现中, 当 HSS 判断得知上述认证数据请求消息对应的认证对象是 UE 时, HSS 则可计算上述认证数据请求消息对应的认证矢量消息, 即对 UE 认证的认证矢量消息, 并可在上述认证矢量消息中设定对 UE 的认证的认证标识信息。具体的, 上述 HSS 计算的认证矢量消息中可包括 RAND、AUTN、XRES 和 K_{asme} 等参数, HSS 确定对 UE 认证的上述认证矢量中的参数时可在上述 AUTN 参数中的 AMF 参数中设定对 UE 认证的认证标识信息, 用于表示上述认证矢量是对 UE 进行的认证。如图 3、图 4 或图 5, HSS 可将 AMF 参数的第 X 比特设定为对 UE 的认证的标志位, 比如将上述 AMF 参数的第 X 比特设置为 1, 以此作为对 UE 认证的认证标识信息, 其中, 上述 AMF 参数的第 X 比特为 AMF 参数中空闲的 7 个比特中的任意一个, 即 $1 \leq X \leq 7$ 。

在一些可行的实施方式中, HSS 确定了对 UE 认证的认证矢量消息并设定对 UE 认证的认证标识信息之后, 则可将上述包含对 UE 认证的认证标识信息的认证矢量通过认证响应消息发送给控制网元, 以通过控制网元将上述认证矢量通过认证请求消息发送给 UE-R。UE-R 接收到控制网元发送的认证请求消息之后则可根据上述认证请求消息中包含的认证矢量中的对 UE 认证的认证标识信息判断得知上述认证矢量是对 UE 的认证, 而非对其自身的认证, 进而可将上述认证矢量中相应的认证参数发送给 UE, 实现对 UE 的认证。

在一些可行的实施方式中, 如图 7 或图 8, 当 HSS 接收到控制网元发送的

认证数据请求消息之后,若判断得知上述认证数据请求消息中包括上述 UE 认证的标识信息,即上述认证数据请求消息中存在 Indication,则可计算对 UE 认证的认证矢量,并将上述认证矢量的 AUTN 参数的 AMF 参数中第 X 比特置位,以此来设定对 UE 认证的认证标识信息。除此之外,如图 9,当 HSS 接收到控制网元发送的认证数据请求消息之后,若判断得知上述认证数据请求消息中包括上述 UE 认证的标识信息,即上述认证数据请求消息中存在 Indication, HSS 还可对上述认证矢量中的 RAND 参数进行加密,并将上述 AMF 参数的第 X 比特设定为对 RAND 参数进行加密的标志位,以上述 AMF 的第 X 比特设定为 1 作为对 RAND 参数进行加密的标识信息,得到加密后的 RAND 参数 RAND*。即,可将上述 AMF 参数的第 X 比特为 1 设定为对 RAND 参数进行加密以及对 UE 认证的认证标识信息添加到上述认证矢量中,当 UE-R 接收到上述认证矢量时,若判断得知上述认证矢量中的 AMF 参数的第 X 比特为 1,则可判断得知上述认证矢量是对 UE 认证的认证矢量,UE-R 则可向 UE 发送认证请求,将上述认证矢量中的 RAND*参数和 AUTN 参数发送给 UE; UE 接收到上述认证矢量的参数信息之后,若判断得知上述 AUTN 参数中的 AMF 参数的第 X 比特为 1,则可对 RAND*参数进行解密,再对 AUTN 进行验证。即 HSS 在计算对 UE 认证的认证矢量时,可通过置位的方法来设定对 UE 认证的认证标识信息,还可同时通过加密的方法来保护认证矢量中的参数 RAND,可提高对 UE 认证的效率和用户体验效果。

在一些可行的实施方式中,若 HSS 接收到控制网元发送的认证数据请求消息中不包含上述 UE 认证的标识信息,即不包含 Indication,如图 10 或图 11, HSS 则可按照对 UE-R 认证的方法计算对 UE 认证的认证矢量,并且不对上述认证矢量做置位或者加密,直接通过认证数据响应信息发送认证矢量给控制网元,以通过控制网元对上述认证数据响应消息进行处理并发送认证请求消息给 UE-R。UE-R 可根据通过控制网元进行处理的认证矢量来判断上述认证请求消息是对 UE 的认证还是对其自身的认证。

在本发明实施例中,处于网络侧的 HSS 接收到控制网元发送的认证数据请求之后则可根据接收到的认证数据请求计算对 UE 认证的认证矢量,还可对上述认证矢量中的参数进行置位来标识消息,或者对认证矢量中的参数进行加

密来保护上述参数, UE-R 可通过 HSS 发送的认证矢量确定上述认证矢量是对 UE 的认证还是对其自身的认证, 可提高 UE 认证的效率和用户体验, 降低 UE-R 和 HSS 等终端的复杂性和成本。

参见图 12, 是本发明实施例提供的终端认证的方法的第三实施例流程示意图。本实施例中所描述的终端认证的方法, 包括步骤:

S301, UE 向 UE-R 发送第一请求消息。

S302, 所述 UE 接收所述 UE-R 发送的认证请求消息。

S303, 所述 UE 对所述认证标识信息中的加密信息进行解密, 并根据所述解密得到的信息计算认证响应。

S304, 所述 UE 将所述认证响应发送给所述 UE-R。

在一些可行的实施方式中, 当 UE 没有被 EPC 网络信号覆盖, 而 UE-R 被 EPC 网络信号覆盖时, UE 可通过 UE-R 接入网络, 进而可实现与其他 UE 的近距离通信。

具体实现中, 当 UE 通过 UE-R 接入网络时, 网络需要对其进行验证, 通过验证之后 UE 才能被允许接入到网络。具体的, 网络侧对 UE 进行认证时, UE 可向 UE-R 发送请求消息, 即 UE 可向 UE-R 发送第一请求消息, 其中, 上述第一请求消息中可包括 UE 认证的标识信息 (即 Indication), 如图 3。UE 向 UE-R 发送请求消息之后, UE-R 则可根据 UE 发送的请求消息向网络侧的控制网元发送请求消息, 以将 UE 的标识信息 (如 Indication) 发送给网络侧的 HSS, 以供 HSS 设定对 UE 认证的认证矢量。

在一些可行的实施方式中, 当 HSS 接收到控制网元发送的认证数据请求消息之后, 判断得知上述认证数据请求消息是 UE 通过 UE-R 接入网络而发送的请求时, 则可计算对 UE 认证的认证矢量, 并通过对上述认证矢量中参数进行置位的方法来标识上述认证矢量的对 UE 的认证, 进而将包含对 UE 认证的认证标识信息的认证请求消息通过控制网元发送给 UE-R。UE-R 接收到控制网元发送的认证请求消息之后, 若判断得知上述认证请求消息是对 UE 的认证, 则可向 UE 发送认证请求消息, UE 接收到 UE-R 发送的认证请求消息之后, 则可根据上述认证请求消息得到 UE 的认证响应。具体实现中, 上述 UE-R 向

UE 发送的认证请求中可包括 UE-R 根据 UE 发送的第一请求消息向 HSS 请求的认证参数，即上述 HSS 根据控制网元发送的认证数据请求设定的对 UE 认证的认证矢量中包含的认证参数。如图 3，UE 接收到 UE-R 发送的认证请求消息之后，则可验证上述认证请求中的 AUTN 参数的正确性，并在验证上述 AUTN 正确之后计算出 RES 参数，其中，上述认证请求消息中携带认证标识信息，UE 可对上述认证标识信息进行验证，进而根据上述认证标识信息计算认证响应。UE 根据上述认证参数得到上述 RES 参数之后，则可将上述 RES 参数作为 UE 的认证响应消息发送给 UE-R，以通过 UE-R 将上述认证响应发送给控制网元，通过控制网元完成对 UE 的认证。

在一些可行的实施方式中，当 UE 从 UE-R 接收到的认证请求消息中包括的认证标识信息中的认证参数包括加密信息时，如图 7。UE 接收到 UE-R 发送的认证请求消息之后，则可对上述认证请求消息中的认证标识信息进行解析，判断上述认证标识信息中的 AUTN 参数中的 AMF 参数的第 X 比特是否为 1，若判断得知上述 AMF 参数的第 X 比特为 1，则可对上述认证参数中的加密信息 (RAND*参数) 进行解密，得知明文 RAND 参数，并对上述认证参数中的 AUTN 参数进行验证，进而根据上述解密得到的明文 RAND 参数和上述认证标识信息中的认证参数等信息计算得到认证响应。具体的，当 UE 对上述加密信息 (RAND*) 进行解密得到明文 RAND 参数，并对上述 AUTN 参数进行验证得知上述 AUTN 参数正确之后，则可计算出 RES 参数，并将上述 RES 参数作为 UE 的认证响应发送给 UE-R。

在本发明实施例中，UE 通过 UE-R 接入网络时可向 UE-R 发送请求消息，并通过 UE-R 获取网络侧发送的认证矢量中的认证参数等信息，在验证 UE-R 发送的认证参数的正确性之后计算出 RES 参数，再通过 UE-R 将 RES 参数发送网络侧，完成 UE 的认证；在本发明实施例中，当网络侧发送的认证参数中包含加密信息时，UE 还可在判断得知接收到的参数中包含加密信息时对加密信息进行解密得到明文，再对其他参数进行验证，进而根据解密得到的明文及上述认证参数计算认证响应，可提高 UE 认证的效率和安全性，而且 UE 和 UE-R 均无需支持新的协议，操作简单，降低 UE 和 UE-R 等终端的复杂性和成本。

参见图 13，是本发明实施例提供的终端认证的方法的第四实施例流程示意图。本实施例中所描述的终端认证的方法，包括步骤：

S401，控制网元接收 UE-R 发送的第二请求消息。

S402，判断所述第二请求消息是否包含 UE 认证的标识信息，若判断结果为是，则执行步骤 S403。

S403，所述控制网元向 HSS 发送认证数据请求消息。

在一些可行的实施方式中，本发明实施例中所描述的认证对象可包括 UE 和 UE-R，下面将以 UE 为例，对本发明实施例提供的终端认证的方法进行具体描述。本发明实施中所描述的控制网元即为本发明实施例中所描述的 MME，在一些可行的实施方式中，本发明实施中所描述的 MME 网元可为 Prose 业务中的功能控制网元，下面将控制网元为执行主体对本发明实施中所描述的终端认证的方法进行具体描述。

在一些可行的实施方式中，上述控制网元从 UE-R 接收到的第二请求消息中包括 UE 认证的标识信息（即 Indication）和 IMSI，如图 3，当控制网元从 UE-R 接收到的第二请求消息中包括 Indication 时，控制网元则可根据上述 IMSI 和 Indication 向 HSS 发送认证数据请求消息。当上述控制网元从 UE-R 接收到的第二请求消息中包括 UE 的识别码（IMSI）和上述第二请求消息的消息类型时，控制网元则可将上述第二请求消息的消息类型，与指定消息类型进行匹配，判断上述第二请求消息是否为指定消息类型，若上述第二请求消息的消息类型是指定消息类型，控制网元则可向 HSS 发送认证数据请求消息。控制网元确定上述第二请求消息的消息类型是指定消息类型之后，则可添加 UE 认证的标识信息到上述认证数据请求消息中，如图 5、图 9。其中，上述 UE 认证的标识信息可为上述第二请求消息中携带的 UE 认证的标识信息（Indication），也可为控制网元在确定上述第二请求消息的消息类型是指定消息类型之后，在上述认证数据请求消息中自行添加的标识信息（Indication），上述第二请求消息中携带的 Indication 可与控制网元在上述认证数据请求消息中添加的 Indication 为同一个 Indication，也可为不同的 Indication，但均可用于标记上述认证数据请求消息的 UE 通过 UE-R 接入网络而通过控制网元发送的认证数据请求消

息。

S404, 所述控制网元从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量。

S405, 所述控制网元将包含所述认证矢量信息的认证请求消息发送给所述 UE-R。

在一些可行的实施方式中, 如图 3, 当控制网元从 UE-R 接收到的第二请求消息中包含 Indication (UE 认证的标识信息) 时, 控制网元判断得知上述第二请求消息中包含 Indication 时, 则可向 HSS 发送认证数据请求消息, 或者如图 5、图 9, 当控制网元根据接收到的第二请求消息判断得知上述第二请求消息的消息类型是指定消息类型之后, 控制网元则可在上述认证数据请求消息中添加 UE 认证的标识信息 Indication, 进而将包含上述 UE 的 IMSI 和 Indication 的认证数据请求消息发送给 HSS, 并从 HSS 处获取 HSS 设定的包含对 UE 认证的认证标识信息的认证矢量。控制网元从 HSS 处获取了对 UE 认证的认证矢量之后, 则可向上述 UE-R 发送认证请求消息, 将上述认证请求消息发送给 UE-R, 以通过 UE-R 将上述对 UE 认证的认证请求消息发送给 UE。

在一些可行的实施方式中, 如图 10, 当控制网元从 UE-R 接收到的第二请求消息中包含 Indication1 (UE 认证的标识信息) 时, 控制网元根据上述第二请求消息判断得知上述第二请求消息中包含 UE 认证的标识信息 Indication1 之后, 则可将包含上述 UE 的 IMSI 的认证数据请求消息发送给 HSS, 即上述认证数据请求消息中不包括 UE 认证的标识信息 Indication1。HSS 接收到上述仅包含 UE 的 IMSI 的认证数据请求消息之后可直接按照对 UE-R 认证时计算认证矢量的方式计算认证矢量, 即此时 HSS 无法区别是对 UE 的认证还是对 UE-R 的认证, 故此 HSS 无法通过对计算得到的认证矢量进行置位做认证标识信息, 也不对认证矢量进行加密保护, 而是直接将处理得到的认证矢量发送给控制网元。控制网元接收到 HSS 发送的认证矢量之后, 为了使得 UE-R 能区分控制网元发送的认证矢量消息是对 UE 的认证, 而非对其自身的认证, 控制网元可在接收到 HSS 发送的认证矢量之后, 可将标识信息 (Indication2) 添加到上述 HSS 设定的认证矢量中, 进而将包括上述标识信息 Indication2 的认证请求消息发送给 UE-R。其中, 上述标识信息 Indication2 表示上述认证请求消

息是对 UE 认证的认证请求消息，具体的，上述 Indication2 可以是上述认证请求消息中新增的字段，也可以是上述认证请求消息中的空闲字段；Indication2 可以为 MME 新选择的标识信息，也可以为 UE 发送给 UE-R 的标识信息，或者 UE-R 发送给 MME 的标识信息，或者 MME 发送给 HSS 的标识信息。具体实现中，如图 14，当控制网元从 UE-R 接收到的第二请求消息中仅包括 UE 的 IMSI 不包含 UE 认证的标识信息 Indication（或 Indication1）时，控制网元可根据上述第二请求消息的消息类型确定上述第二请求消息的消息类型是否为指定消息类型。当控制网元确定上述第二请求消息中包含 UE 认证的标识信息（具体可为上述图 3 中的 Indication 或者上述图 10 中的 Indication1）或者上述第二请求消息的消息类型是指定消息类型之后，也可将认证数据请求消息发送给 HSS，其中，上述认证数据请求消息中不包含 UE 认证的标识信息。HSS 接收到上述仅包含 UE 的 IMSI（即不包含上述 UE 认证的标识信息）的认证数据请求消息之后可直接按照对 UE-R 认证时计算认证矢量的方式计算认证矢量，并将处理得到的认证矢量发送给控制网元。控制网元接收到 HSS 发送的包含认证矢量的认证响应消息之后，将上述认证矢量通过认证请求消息发送给 UE-R 之前可将标识信息（如 Indication2）添加到上述认证请求消息中，将上述包含上述标识信息 Indication2 的认证矢量等信息通过认证请求消息发送给 UE-R。如图 14，控制网元可在接收到 HSS 发送的认证矢量消息之后，将标识信息（Indication2）添加到上述 HSS 设定的认证请求消息中，并将包括 Indication2 和 HSS 设定的认证矢量（包括 RAND、AUTN）的认证请求消息发送给 UE-R，具体的，控制网元可将包含标识信息 Indication2 和认证矢量的认证请求发送给 UE-R，以通过上述 Indication2 告知 UE-R 上述认证请求消息是对 UE 认证的请求消息。

在一些可行的实施方式中，控制网元将对 UE 认证的认证请求消息发送给 UE-R 之后，UE-R 则可根据上述认证请求消息向 UE 发送认证请求消息，将上述 HSS 设定的 RAND、AUTN 等信息发送给 UE，UE 则可对上述认证请求消息中的认证矢量中包含的认证参数进行验证，并计算得到参数 RES，进而将 RES 参数通过认证响应发送给 UE-R。UE-R 接收到 UE 发送的认证响应消息之后，则可将上述包含 RES 参数的认证响应消息发送给控制网元，控制网元接

收到上述认证响应消息之后，则可将上述认证响应消息中的 RES 参数与预存的 HSS 发送的认证矢量中的 XRES 进行比较，判断上述 RES 与 XRES 是否一致，若判断结果为是，则可判断得知上述 UE 是被允许接入的 UE，即可通过 UE 的认证请求，完成对 UE 的认证。

在本发明实施例中，控制网元可根据 UE-R 发送的第二请求消息确定上述第二请求消息中是否包含 UE 认证的标识信息或者上述第二请求消息的消息类型是否为指定消息类型，在上述第二请求消息中包含 UE 认证的标识信息或者上述第二请求消息的消息类型为指定消息类型时向 HSS 发送认证数据请求消息，并从 HSS 处获取对 UE 认证的认证矢量等认证标识信息，进而将包含认证标识信息的认证请求消息发送给 UE-R，以通过 UE-R 将上述认证标识信息发送给 UE；在本发明实施例中控制网元可将包含 UE 认证的标识信息的认证数据请求消息发送给 HSS，或者将包含认证标识信息的认证请求消息发送给 UE-R，可提高网络对 UE 认证的效率，降低 UE-R 和 UE 等终端的复杂性和成本，增强 UE 认证的用户体验。

参见图 15，是本发明实施例提供的终端认证的中继设备的实施例结构示意图。本实施例中所描述的中继设备，包括：

接收模块 10，用于接收 UE 发送的第一请求消息。

发送模块 20，用于根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，以使所述控制网元根据所述第二请求消息向 HSS 发送认证数据请求消息，其中，所述认证数据请求消息中携带所述 UE 认证的标识信息。

所述接收模块 10，用于接收所述控制网元发送的认证请求消息。

判断模块 30，用于根据所述接收模块接收到的所述认证请求消息判断所述认证请求消息是否是对所述 UE 的认证。

所述发送模块 20，用于在所述判断模块判断结果为是时，向所述 UE 发送认证请求消息，所述认证请求消息中包括所述 UE 的认证参数。

所述接收模块 10，还用于接收所述 UE 根据所述发送模块发送的所述认证请求消息发送的认证响应消息。

所述发送模块 20，用于将所述接收模块接收到的所述认证响应消息发送

给所述控制网元，以通过所述控制网元完成所述 UE 的认证。

在一些可行的实施方式中，所述接收模块 10 接收到的所述 UE 发送的第一请求消息中包含所述 UE 认证的标识信息；

上述发送模块 20，还具体用于：

将所述第一请求消息中携带的所述 UE 认证的标识信息添加到所述第二请求消息中，并将所述第二请求消息发送给所述控制网元。

具体实现中，本发明实施例中所描述 UE-R 即为本发明实施例中所描述的终端认证的中继设备。

在一些可行的实施方式中，上述接收模块 10 接收到的 UE 发送的第一请求消息中可包括 UE 的识别码 (IMSI) 和 UE 的标识信息 (Indication) (即 UE 认证的标识信息)，其中，上述标识信息 Indication 可表示上述第一请求消息是 UE 通过 UE-R 接入网络而发送的请求。具体实现中，当 UE-R 的接收模块 10 接收到 UE 通过 UE-R 接入网络并向 UE-R 发送的包含其 IMSI 和 Indication 的第一请求消息之后，UE-R 的发送模块 20 则可根据接收模块 10 接收到的 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的，上述第二请求消息的消息类型可与上述第一请求消息的消息类型相同，也可不同，具体可根据 UE 认证的实际场景需求设定。具体实现中，发送模块 20 向 MME 发送第二请求消息时，可在上述第二请求消息中添加 UE 认证的标识信息，其中，上述 UE 认证的标识信息用于标记上述第二请求消息是 UE 通过 UE-R 接入网络时，UE-R 向 MME 发送的请求消息。具体的，当 UE-R 的接收模块 10 接收到的 UE 发送的第一请求消息中包含 UE 认证的标识信息 (即 Indication) 时，发送模块 20 可将上述标识信息 Indication 作为 UE 认证的标识信息添加到上述第二请求消息中；发送模块 20 也可以选择新的标识信息，并将新选择的标识信息作为 UE 认证的标识信息添加到上路第二请求消息中，进而将上述第二请求消息发送给 MME (即控制网元)。如图 3，当 UE-R 的接收模块 10 接收到 UE 发送的第一请求消息时，若上述接收模块 10 接收到的第一请求消息中包含 UE 的 IMSI 和 Indication 时，UE-R 的发送模块 20 则可将上述第一请求消息中包括的 UE 的 IMSI 和 Indication 添加到第二请求消息中，也可以重新选择 Indication，并将 IMSI 和重新选择的 Indication 添加到第二请求消息中，并将

上述第二请求消息发送给控制网元。网络侧的控制网元通过 UE-R 接收到上述 UE-R 发送的第二请求消息之后，则可根据第二请求消息中包含的 Indication 判断得知当前需要进行认证的是通过 UE-R 接入网络的 UE，而非 UE-R 自身，进而 MME 可向 HSS 发送相应的用户认证数据请求消息。

在一些可行的实施方式中，上述接收模块 10 接收到的所述 UE 发送的第一请求消息中不包含所述 UE 认证的标识信息；

所述发送模块 20，具体用于：

在所述第二请求消息中添加所述 UE 认证的标识信息，并将所述第二请求消息发送给所述控制网元。

在一些可行的实施方式中，如图 4，当接收模块 10 接收到的上述 UE 发送的第一请求消息中仅包括 UE 的 IMSI，不包含上述 UE 认证的标识信息（Indication）时，当 UE 通过 UE-R 接入网络并向 UE-R 发送了包含其 IMSI 的第一请求消息之后，UE-R 的发送模块 20 则可根据 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的，上述发送模块 20 发送的第二请求消息的消息类型可与上述第一请求消息的消息类型相同，也可不同，具体可根据 UE 认证的实际场景需求设定。具体实现中，如图 4，当 UE-R 的接收模块 10 接收到的上述第一请求消息中仅包含 UE 的 IMSI 时，UE-R 的发送模块 20 可在上述 UE 发送的第一请求消息中添加上述标识信息 Indication（即 UE 认证的标识信息），将上述 IMSI 和 Indication 添加到第二请求消息中，并将上述包括 UE 的 IMSI 和 Indication 的第二请求消息发送给控制网元。网络侧的控制网元通过 UE-R 接收到上述 UE-R 发送的第二请求消息之后，则可根据第二请求消息中包含的 UE 的 Indication 判断得知当前需要进行认证的是通过 UE-R 接入网络的 UE，而非 UE-R 自身。

具体实现中，如图 5，当上述 UE 发送的第一请求消息中仅包括 UE 的 IMSI 时，当接收模块 10 接收到 UE 通过 UE-R 接入网络并向 UE-R 发送的包含 UE 的 IMSI 的第一请求消息之后，UE-R 的发送模块 20 则可根据 UE 发送的第一请求消息向控制网元发送第二请求消息。具体的，上述发送模块 20 发送的第二请求消息的消息类型可与上述第一请求消息的消息类型相同，也可不同，具体可根据 UE 认证的实际场景需求设定。具体实现中，如图 5，当 UE-R 的接

收模块 10 接收到的上述第一请求消息中仅包含 UE 的 IMSI 时, UE-R 的发送模块 20 可直接将上述第一请求消息中的 UE 的 IMSI 添加到第二请求消息中, 并将上述包括 UE 的 IMSI 的第二请求消息发送给控制网元, 即在上述实现方式中, UE-R 的发送模块 20 向控制网元发送的第二请求消息中包括 UE 的 IMSI, 不包含上述 UE 认证的标识信息 Indication。在上述实现方式中, 当 UE-R 的发送模块 20 将仅包含 UE 的 IMSI 的第二请求消息发送给网络侧的控制网元之后, 由于上述第二请求消息中没有 Indication, 控制网元无法直接从上述第二请求消息中获取 Indication, 此时, 控制网元可通过上述第二请求消息的消息类型判断上述请求是 UE 通过 UE-R 接入网络时发送的认证请求还是 UE-R 自身接入网络时 UE-R 发送的认证请求。具体的, 控制网元可将接收到的上述发送模块 20 发送的第二请求消息的消息类型与预存的指定消息类型进行匹配, 判断上述第二请求消息的消息类型是否属于上述指定消息类型, 若判断得知上述第二请求消息的消息类型是上述指定消息类型, 控制网元的发送模块 20 则可向 HSS 发送相应的用户认证数据请求消息, 还可通过上述用户认证数据请求消息告知 HSS 是 UE 接入网络还是 UE-R 接入网络, 即控制网元通过对上述第二请求消息的消息类型的判定来判断得知当前接收到的第二请求消息的消息类型是否是指定消息类型, 以决定向 HSS 发送的用户认证数据请求消息中包含的内容, 即可判断得知需要进行认证的是通过 UE-R 接入网络的 UE, 而非 UE-R 自身。

在一些可行的实施方式中, 网络侧接收到 UE-R 的发送模块 20 发送的第二请求消息之后, 则可根据上述第二请求消息计算对 UE 进行认证的认证矢量。具体实现中, 如图 3 或图 4, 当网络侧的控制网元接收到 UE-R 的发送模块 20 发送的第二请求消息中包括标识信息 Indication 时, 则可判断得知上述第二请求消息是 UE 通过 UE-R 接入网络而发送的请求, 而非 UE-R 接入网络的请求, 即当网络侧判断得知上述第二请求消息中包括 Indication 时, 则可计算对 UE 进行认证的认证矢量。具体的, 当网络侧判断得知上述第二请求消息中包括 Indication 时, 可在计算对 UE 进行认证的认证矢量中设定认证标识信息 (即对 UE 认证的认证标识信息), 用于表示上述认证矢量是对 UE 进行的认证, 并将包含上述认证标识信息的认证矢量通过认证请求消息发送给 UE-R。网络

侧设定对 UE 认证的认证标识信息时可在上述认证矢量中的 AMF 参数中设定对 UE 的认证的认证标识信息, 例如, 可在认证矢量中的 AUTN 参数中置位 AMF 参数的第 X 比特为 1, 其中, 上述 $1 \leq X \leq 7$, 即上述 AMF 参数的第 X 比特可以是 AMF 参数中空闲的 7 个比特中的任意一个, 网络侧设定上述标志位并将包含上述标志位的认证矢量发送给 UE-R, UE-R 则可根据上述标志位来判断接收到的认证矢量是对 UE 的认证, 而非对其自身的认证。

具体实现中, 当网络侧接收到的第二请求消息中不包括上述标识信息 Indication 时, 网络侧还可通过上述第二请求消息的消息类型判断得知上述第二请求消息的 UE 通过 UE-R 接入网络而发送的请求消息, 而非 UE-R 接入网络而发送的请求消息。网络侧判断得知接收到的第二请求消息是 UE 通过 UE-R 接入网络而发送的请求消息时, 则可计算对 UE 进行认证的认证矢量, 并在上述认证矢量计算中设定对 UE 的认证的标识信息, 进而将包含对 UE 的认证的标识信息的认证矢量参数 RAND、AUTN 发送给 UE-R。

在一些可行的实施方式中, 上述接收模块 10 接收到的所述控制网元发送的认证请求消息中包括所述 HSS 根据所述 UE 认证的标识信息设定的对所述 UE 认证的认证标识信息;

所述判断模块 30, 具体用于:

判断所述认证请求消息是否包含认证标识信息;

若所述认证请求消息中包含所述认证标识信息, 则判断所述认证请求消息为对所述 UE 的认证。

在一些可行的实施方式中, UE-R 的接收模块 10 接收到网络侧的控制网元发送的认证请求消息之后, 判断模块 30 则可根据上述接收模块 10 接收到的认证请求消息中包含的认证矢量的各参数信息判断上述认证请求消息是否是对 UE 的认证, 如果判断模块 30 判断得知上述认证请求消息是对 UE 的认证, UE-R 的发送模块 20 则向 UE 发送认证请求消息。具体实现中, 当 UE-R 的接收模块 10 接收到控制网元发送的认证请求消息时, UE-R 的判断模块 30 则可判断上述认证请求消息中是否包含对 UE 的认证的认证标识信息, 例如, UE-R 的判断模块 30 可判断上述认证请求消息中的认证矢量的 AMF 参数的第 X 比特是否为 1, 如果判断模块 30 判断得知上述认证矢量的 AMF 的第 X 比特是 1,

则判断得知上述认证请求消息是对 UE 的认证；具体的，如图 10，UE-R 判断模块 30 还可判断认证请求消息中是否包含标识信息 Indication2，若存在标识信息 Indication2，则判断得知上述认证请求消息是对 UE 的认证；发送模块 20 则可向 UE 发送认证请求消息，并将上述认证矢量中的 AUTN 和 RAND 等参数发送给 UE，以供 UE 进行验证。

在一些可行的实施方式中，UE-R 的发送模块 20 向 UE 发送认证请求消息时可将从网络侧接收到的上述认证矢量发送给 UE，UE 接收到 UE-R 发送的认证矢量参数 RAND、AUTN 之后，则可对认证矢量中的 RAND、AUTN 参数进行验证，验证 AUTN 参数的正确性。UE 验证 AUTN 正确之后，则可计算 RES 参数，并将计算得到的 RES 参数发送给 UE-R。UE-R 接收到 UE 发送的认证响应（包括上述 RES 参数）之后，则可将上述认证响应发送给网络侧的控制网元，以通过上述控制网元完成 UE 的认证。

在本发明实施例中，UE-R 可接收 UE 发送的请求消息，根据 UE 发送的请求消息向网络侧发送认证请求消息，并从网络侧获取包含对 UE 的认证的认证标识信息的认证矢量，UE-R 可根据网络侧发送的认证请求消息判断是对 UE 的认证还是对自身的认证，进而将认证请求消息发送给 UE，完成对 UE 的认证，操作简单，终端成本低，提高了 UE 认证的效率和用户体验。

参见图 16，是本发明实施例提供的终端认证的服务器的实施例结构示意图。本实施例中所描述的服务器，包括：

接收模块 40，用于接收控制网元发送的认证数据请求消息。

判断模块 50，用于根据所述接收模块接收到的所述认证数据请求消息判断所述认证数据请求消息是否包含 UE 认证的标识信息。

处理模块 60，用于在所述判断模块判断结果为是时，在认证矢量中设定所述 UE 认证的认证标识信息。

发送模块 70，用于所述处理模块处理得到的将所述认证矢量消息发送给所述控制网元，以通过所述控制网元将所述认证标识信息发送给 UE-R，以使所述 UE-R 根据所述认证标识信息判断是否是对所述 UE 的认证。

在一些可行的实施方式中，上述所述处理模块 60 处理得到的所述认证矢

量中包括: RAND 参数、AUTN 参数、XRES 参数、和 Ksme 参数;

所述处理模块 60, 具体用于:

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

具体实现中, 本发明实施例中所描述的 HSS 即为本发明实施例中所描述的终端认证的服务器。

在一些可行的实施方式中, 处于网络侧的 HSS 的接收模块 40 接收到控制网元发送的认证数据请求消息之后, 判断模块 50 则可判断上述认证数据请求消息中是否包含 UE 认证的标识信息, 其中, 上述 UE 认证的标识信息具体可为 UE 向 UE-R 发送的第一请求消息中携带的 Indication, UE-R 将上述第一请求消息中携带的 Indication 添加到第二请求消息中, 进而将上述第二请求消息发送给控制网元, 通过控制网元发送给 HSS; 上述 UE 认证的标识信息也可为 UE-R 根据上述第一请求消息在向控制网元发送第二请求消息时添加的 Indication, UE-R 在上述第二请求消息中添加 Indication 之后将上述第二请求消息发送给控制网元, 控制网元可将上述第二请求消息中携带的 Indication 发送给 HSS; 上述 UE 认证的标识信息也可以为控制网元自己选择的 Indication。如图 3、图 4 或图 5, 当 HSS 通过接收模块 40 接收到控制网元发送的认证数据请求消息之后, 判断模块 50 则可判断上述认证数据请求消息中是否包含 UE 认证的标识信息, 即上述认证数据请求消息中是否存在 Indication, 若判断模块 50 判断得知上述认证数据请求消息中包括 Indication, 则可判断得知上述认证数据请求消息的认证对象为 UE。具体实现中, 当 HSS 的判断模块 50 判断得知上述认证数据请求消息对应的认证对象是 UE 时, 处理模块 60 则可计算上述认证数据请求消息对应的认证矢量消息, 即对 UE 认证的认证矢量消息, 并可在上述认证矢量消息中设定对 UE 的认证的认证标识信息。具体的, 上述处理模块 60 处理得到的认证矢量消息中可包括 RAND、AUTN、XRES 和 Ksme 等参数, HSS 的处理模块 60 确定对 UE 认证的上述认证矢量中的参数时可在上述 AUTN 参数中的 AMF 参数中设定对 UE 认证的认证标识信息, 用于表示上述认证矢量是对 UE 进行的认证。如图 3、图 4 或图 5, 处理模块 60 可将 AMF 参数的第 X 比特设定为对 UE 的认证的标志位, 比如将上述 AMF 参数的第 X

比特设置为 1，以此作为对 UE 的认证的认证标识信息，其中，上述 AMF 参数的第 X 比特为 AMF 参数中空闲的 7 个比特中的任意一个，即 $1 \leq X \leq 7$ 。

在一些可行的实施方式中，HSS 的处理模块 60 确定了对 UE 认证的认证矢量消息并设定对 UE 认证的认证标识信息之后，发送模块 70 则可将上述包含对 UE 认证的认证标识信息的认证矢量通过认证响应消息发送给控制网元，以通过控制网元将上述认证矢量通过认证请求消息发送给 UE-R。UE-R 接收到控制网元发送的认证请求消息之后则可根据上述认证请求消息中包含的认证矢量中的对 UE 认证的认证标识信息判断得知上述认证矢量是对 UE 的认证，而非对其自身的认证，进而可将上述认证矢量中相应的认证参数发送给 UE，实现对 UE 的认证。

在一些可行的实施方式中，上述处理模块 60 处理得到的所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数和 K_{asme} 参数；

所述处理模块 60，还具体用于：

对所述认证矢量中的 RAND 参数进行加密；

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

在一些可行的实施方式中，如图 7 或图 8，当 HSS 的接收模块 40 接收到控制网元发送的认证数据请求消息之后，若判断模块 50 判断得知上述认证数据请求消息中包括上述 UE 认证的标识信息，即上述认证数据请求消息中存在 Indication，处理模块 60 则可计算对 UE 认证的认证矢量，并对上述认证矢量的 AUTN 参数的 AMF 参数中第 X 比特置位，以此来设定对 UE 认证的认证标识信息。除此之外，如图 9，当 HSS 接收到控制网元发送的认证数据请求消息之后，若判断得知上述认证数据请求消息中包括上述 UE 认证的标识信息，即上述认证数据请求消息中存在 Indication，HSS 的处理模块 60 还可对上述认证矢量中的 RAND 参数进行加密，并将上述 AMF 参数的第 X 比特设定为对 RAND 参数进行加密的标志位，以上述 AMF 的第 X 比特设定为 1 作为对 RAND 参数进行加密的标识信息，得到加密后的 RAND 参数 (RAND*)。即，处理模块 60 可将上述 AMF 参数的第 X 比特为 1 设定为对 RAND 参数进行加密以及对 UE 认证的认证标识信息添加到上述认证矢量中，当 UE-R 接收到上述认

证矢量时, 若判断得知上述认证矢量中的 AMF 参数的第 X 比特为 1, 则可判断得知上述认证矢量是对 UE 认证的认证矢量, UE-R 则可向 UE 发送认证请求, 将上述认证矢量中的 RAND*参数和 AUTN 参数发送给 UE; UE 接收到上述认证矢量的参数信息之后, 若判断得知上述 AUTN 参数中的 AMF 参数的第 X 比特为 1, 则可对 RAND*参数进行解密, 再对 AUTN 进行验证。即 HSS 在计算对 UE 认证的认证矢量时, 可通过置位的方法来设定对 UE 认证的认证标识信息, 还可同时通过加密的方法来保护认证矢量中的参数 RAND, 可提高对 UE 认证的效率和用户体验效果。

在一些可行的实施方式中, 若 HSS 的接收模块 40 接收到控制网元发送的认证数据请求消息中不包含上述 UE 认证的标识信息, 即不包含 Indication, 如图 10 或图 11, HSS 的处理模块 60 则可按照对 UE-R 认证的方法计算对 UE 认证的认证矢量, 并且不对上述认证矢量做置位或者加密, 直接通过发送模块 70 发送包含上述认证矢量的认证数据响应消息给控制网元, 以通过控制网元对上述认证数据响应消息进行处理并发送认证请求消息给 UE-R。UE-R 可根据通过控制网元进行处理的认证矢量来判断上述认证请求消息是对 UE 的认证还是对其自身的认证。

在本发明实施例中, 本发明实施例中所描述的 HSS 接收到控制网元发送的认证数据请求之后则可根据接收到的认证数据请求计算对 UE 认证的认证矢量, 还可对上述认证矢量中的参数进行置位来标识消息, 或者对认证矢量中的参数进行加密来保护上述参数, UE-R 可通过 HSS 发送的认证矢量确定上述认证矢量是对 UE 的认证还是对其自身的认证, 可提高 UE 认证的效率和用户体验, 降低 UE-R 和 HSS 等终端的复杂性和成本。

参见图 17, 是本发明实施例提供的终端认证的用户设备的实施例结构示意图。本实施例中所描述的用户设备, 包括:

发送模块 100, 用于向 UE-R 发送第一请求消息, 以使所述 UE-R 根据所述第一请求消息向控制网元发送第二请求消息。

接收模块 200, 用于接收所述 UE-R 发送的认证请求消息, 所述认证请求消息中携带 UE 认证的认证标识信息。

处理模块 300，用于对所述认证标识信息中的加密信息进行解密，并根据所述解密得到的信息计算认证响应。

在一些可行的实施方式中，所述发送模块 100 发送的所述第一请求消息中包括所述 UE 认证的标识信息。

具体实现中，本发明实施例中所描述的 UE 即为本发明实施例中所描述的终端认证的用户设备。

在一些可行的实施方式中，当 UE 没有被 EPC 网络信号覆盖，而 UE-R 被 EPC 网络信号覆盖时，UE 可通过 UE-R 接入网络，进而可实现与其他 UE 的近距离通信。

具体实现中，当 UE 通过 UE-R 接入网络时，网络需要对其进行验证，通过验证之后 UE 才能被允许接入到网络。具体的，网络侧对 UE 进行认证时，UE 的发送模块 100 可向 UE-R 发送请求消息，即 UE 可向 UE-R 发送第一请求消息，其中，上述第一请求消息中可包括 UE 认证的标识信息（即 Indication），如图 3。UE 的发送模块 100 向 UE-R 发送请求消息之后，UE-R 则可根据 UE 发送的请求消息向网络侧的控制网元发送请求消息，以将 UE 的标识信息（如 Indication）发送给网络侧的 HSS，以供 HSS 设定对 UE 认证的认证矢量。

在一些可行的实施方式中，当 HSS 接收到控制网元发送的认证数据请求消息之后，判断得知上述认证数据请求消息是 UE 通过 UE-R 接入网络而发送的请求时，则可计算对 UE 认证的认证矢量，并通过对上述认证矢量中参数进行置位的方法来标识上述认证矢量的对 UE 的认证，进而将包含对 UE 认证的认证标识信息的认证请求消息通过控制网元发送给 UE-R。UE-R 接收到控制网元发送的请求消息之后，若判断得知上述认证请求消息是对 UE 的认证，则可向 UE 发送认证请求消息，UE 的接收模块 200 接收到 UE-R 发送的认证请求消息之后，则可根据上述认证请求消息得到 UE 的认证响应。具体实现中，上述 UE 的接收模块 200 接收到的 UE-R 向 UE 发送的认证请求中可包括 UE-R 根据 UE 发送的第一请求消息向 HSS 请求的认证参数，即上述 HSS 根据控制网元发送的认证数据请求设定的对 UE 认证的认证矢量中包含的认证参数。如图 3，UE 的接收模块 200 接收到 UE-R 发送的认证请求消息之后，处理模块 300 则可验证上述认证请求中的 AUTN 参数的正确性，并在验证上述 AUTN

正确之后计算出 RES 参数，其中，上述认证请求消息中携带认证标识信息，UE 可对上述认证标识信息进行验证，进而根据上述认证标识信息计算认证响应。UE 的处理模块 300 根据上述认证参数得知上述 RES 参数之后，则可通过发送模块 100 将上述 RES 参数作为 UE 的认证响应发送给 UE-R，以通过 UE-R 将上述认证响应发送给控制网元，通过控制网元完成对 UE 的认证。

在一些可行的实施方式中，当 UE 的接收模块 200 从 UE-R 接收到的认证请求消息中包括的认证标识信息中的认证参数包括加密信息时，如图 7，接收模块 200 接收到 UE-R 发送的认证请求消息之后，处理模块 300 则可判断上述认证请求消息中的认证标识信息进行解析，判断上述认证标识信息中的 AUTN 参数中的 AMF 参数的第 X 比特是否为 1，若处理模块 300 判断得知上述 AMF 参数的第 X 比特为 1，则可对上述认证参数中加密信息（RAND*参数）进行解密，得知明文 RAND 参数，并对上述认证参数中的 AUTN 参数进行验证，进而根据上述解密得到的明文 RAND 参数和上述认证标识信息中的认证参数等信息计算得到认证响应。具体的，当 UE 的处理模块 300 对上述加密信息（RAND*）进行解密得到明文 RAND 参数，并对上述 AUTN 参数进行验证得知上述 AUTN 参数正确之后，则可计算出 RES 参数，并将上述 RES 参数作为 UE 的认证响应，通过发送模块 100 发送给 UE-R。

本发明实施例中所描述的 UE 通过 UE-R 接入网络时可向 UE-R 发送请求消息，并通过 UE-R 获取网络侧发送的认证矢量中的认证参数等信息，在验证 UE-R 发送的认证参数的正确性之后计算出 RES 参数，再通过 UE-R 将 RES 参数发送网络侧，完成 UE 的认证；本发明实施例中所描述的 UE 接收到网络侧发送的认证参数中包含加密信息时，UE 还可在判断得知接收到的参数中包含加密信息时对加密信息进行解密得到明文，再对其他参数进行验证，进而根据解密得到的明文及上述认证参数计算认证响应，可提高 UE 认证的安全性，而且 UE 和 UE-R 均无需支持新的协议，操作简单，降低 UE 和 UE-R 等终端的复杂性和成本。

参见图 18，是本发明实施例提供的终端认证的控制设备的实施例的一结构示意图。本实施例中所描述的控制设备，包括：

接收模块 400，用于接收 UE-R 发送的第二请求消息。

处理模块 500，用于根据所述接收模块接收到的所述第二请求消息判断所述第二请求消息是否包含 UE 认证的标识信息。

发送模块 600，在所述处理模块判断结果为是时，向 HSS 发送认证数据请求消息，所述认证数据请求消息中携带所述 UE 认证的标识信息。

所述接收模块 400，用于从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量。

所述发送模块 600，还用于将所述接收模块接收到的包含所述认证矢量信息的认证请求消息发送给所述 UE-R，以供所述 UE-R 判断所述认证请求消息是否是对 UE 的认证。

在一些可行的实施方式中，所述控制设备（如图 19），还包括：

判断模块 700，用于根据所述接收模块接收到的第二请求消息判断所述第二请求消息是否为指定消息类型，若所述第二请求消息为所述指定消息类型，则通知所述发送模块向 HSS 发送认证数据请求消息。

具体实现中，本发明实施例提供的终端认证的控制设备可为本发明实施例中所描述的 MME，也可以是 Prose 业务中的功能控制网元，即本发明实施中所描述的控制网元即为本发明实施提供的终端认证的控制设备。下面将以 MME 为本发明实施例提供的终端认证的控制设备进行具体描述。

在一些可行的实施方式中，上述 MME 的接收模块 400 从 UE-R 接收到的第二请求消息中可包括 UE 的识别码（IMSI）和 UE 认证的标识信息（即 Indication），如图 3，当接收模块 400 从 UE-R 接收到的第二请求消息中包括 Indication 时，处理模块 500 则可根据上述 IMSI 和 Indication 向 HSS 发送认证数据请求消息。

在一些可行的实施方式中，当上述接收模块 400 从 UE-R 接收到的第二请求消息中包括 UE 的识别码（IMSI）和上述第二请求消息的消息类型时，判断模块 700 则可将上述第二请求消息的消息类型，与指定消息类型进行匹配，判断上述第二请求消息是否为指定消息类型，若上述第二请求消息的消息类型是指定消息类型，控制网元则可向 HSS 发送认证数据请求消息。判断模块 700 确定上述第二请求消息的消息类型是指定消息类型之后，发送模块 600 则可添

加 UE 认证的标识信息到上述认证数据请求消息中, 如图 5、图 9, 其中, 上述 UE 认证的标识信息可为上述第二请求消息中携带的 UE 认证的标识信息 (Indication), 也可为控制网元在确定上述第二请求消息的消息类型是指定消息类型之后, 在上述认证数据请求消息中添加的标识信息 (Indication), 上述第二请求消息中携带的 Indication 可与控制网元在上述认证数据请求消息中添加的 Indication 为同一个 Indication, 也可为不同的 Indication, 但均可用于标记上述认证数据请求消息的 UE 通过 UE-R 接入网络而通过控制网元发送的认证数据请求消息。

在一些可行的实施方式中, 上述发送模块 600, 具体用于:

添加所述 UE 认证的标识信息到所述认证数据请求消息中, 并将所述认证数据请求消息发送给所述 HSS。

在一些可行的实施方式中, 如图 3, 当接收模块 400 从 UE-R 接收到的第二请求消息中包括 Indication (UE 认证的标识信息) 时, 处理模块 500 判断得知上述第二请求消息中包含 Indication 时, 则可向 HSS 发送认证数据请求消息, 或者如图 5、图 9, 当判断模块 700 根据接收到的第二请求消息判断得知上述第二请求消息的消息类型是指定消息类型之后, 发送模块 600 则可在上述认证数据请求消息中添加 UE 认证的标识信息 Indication, 进而将包含上述 UE 的 IMSI 和 Indication 的认证数据请求消息发送给 HSS, 并通过接收模块 400 从 HSS 处获取 HSS 设定的包含对 UE 认证的认证标识信息的认证矢量。接收模块 400 从 HSS 处获取了对 UE 认证的认证矢量之后, 则可通过发送模块 600 向上述 UE-R 发送认证请求消息, 将上述认证请求消息发送给 UE-R, 以通过 UE-R 将上述对 UE 认证的认证请求消息发送给 UE。

在一些可行的实施方式中, 上述发送模块 600, 具体用于:

添加所述 UE 认证的标识信息到所述包含所述认证矢量的认证请求消息中, 并将认证请求消息发送给所述 UE-R。

在一些可行的实施方式中, 如图 10, 当接收模块 400 从 UE-R 接收到的第二请求消息中包括 Indication1 (UE 认证的标识信息) 时, 处理模块 500 根据上述第二请求消息判断得知上述第二请求消息中包含 UE 认证的标识信息 Indication1 之后, 则可通过发送模块 600 将包含上述 UE 的 IMSI 的认证数据

请求消息发送给 HSS, 即上述认证数据请求消息中不包括 UE 认证的标识信息 Indication1。HSS 接收到上述仅包含 UE 的 IMSI 的认证数据请求消息之后可直接按照对 UE-R 认证时计算认证矢量的方式计算认证矢量, 即此时 HSS 无法区别是对 UE 的认证还是对 UE-R 的认证, 故此 HSS 无法通过对计算得到的认证矢量进行置位做认证标识信息, 也不对认证矢量进行加密保护, 而是直接将处理得到的认证矢量发送给控制网元。MME 的接收模块 400 接收到 HSS 发送的认证矢量之后, 为了使得 UE-R 能区分控制网元发送的认证矢量消息是对 UE 的认证, 而非对其自身的认证, MME 的处理模块 500 可在接收模块 400 接收到 HSS 发送的认证矢量之后, 可将标识信息 (Indication2) 添加到上述接收模块 400 接收到的 HSS 设定的认证矢量中, 并通过发送模块 600 将包括上述标识信息 Indication2 的认证请求消息发送给 UE-R。其中, 上述标识信息 Indication2 表示上述认证请求消息是对 UE 认证的认证请求消息, 具体的, 上述 Indication2 可以是上述认证请求消息中新增的字段, 也可以是上述认证请求消息中的空闲字段; Indication2 可以为 MME 新选择的标识信息, 也可以为 UE 发送给 UE-R 的请求消息中包含的标识信息, 或者 UE-R 发送给 MME 的请求消息中包含的标识信息, 又或者 MME 发送给 HSS 的认证数据请求消息中包含的标识信息。具体实现中, 如图 14, 当 MME 的接收模块 400 从 UE-R 接收到的第二请求消息中仅包括 UE 的 IMSI 不包含 UE 认证的标识信息 Indication (或 Indication1) 时, 处理模块 500 可根据上述第二请求消息的消息类型确定上述第二请求消息的消息类型是否为指定消息类型。当处理模块 500 确定上述第二请求消息中包含 UE 认证的标识信息 (具体可为上述图 3 中的 Indication 或者上述图 9 中的 Indication1) 或者上述第二请求消息的消息类型是指定消息类型之后, 发送模块 600 可将包含上述认证数据请求消息发送给 HSS, 其中, 上述认证数据请求消息中不包含 UE 认证的标识信息。HSS 接收到上述仅包含 UE 的 IMSI (即不包含上述 UE 认证的标识信息) 的认证数据请求消息之后可直接按照对 UE-R 认证时计算认证矢量的方式计算认证矢量, 并将处理得到的认证矢量发送给 MME。MME 的接收模块 400 接收到 HSS 发送的包含认证矢量的认证响应消息之后, 发送模块 600 将上述认证矢量通过认证请求消息发送给 UE-R 之前, 处理模块 500 则可将 UE 认证的标识信息 (如

Indication2) 添加到上述认证请求消息中, 通过发送模块 600 将上述包含标识信息 Indication2 的认证矢量等信息发送给 UE-R。如图 14, 处理模块 500 可在接收模块 400 接收到 HSS 发送的认证矢量消息之后, 将标识信息(Indication2) 添加到上述 HSS 设定的认证请求消息中, 并通过发送模块 600 将包括 Indication2 和 HSS 设定的认证矢量中 (RAND、AUTN) 的认证请求消息发送给 UE-R, 具体的, 发送模块 600 可将包含 Indication2 和 AUTN、RAND 通过认证请求消息发送给 UE-R, 以通过上述 Indication2 告知 UE-R 上述认证请求消息是对 UE 认证的请求消息。

在一些可行的实施方式中, MME 的发送模块 600 将对 UE 认证的认证请求消息发送给 UE-R 之后, UE-R 则可根据上述认证请求消息向 UE 发送认证请求消息, 将上述 HSS 设定的 RAND、AUTN 等信息发送给 UE, UE 则可对上述认证请求消息中的认证矢量中包含的认证参数进行验证, 并计算得到参数 RES, 进而将 RES 参数通过认证响应发送给 UE-R。UE-R 接收到 UE 发送的认证响应消息之后, 则可将上述包含 RES 参数的认证响应消息发送给 MME, MME 接收到上述认证响应消息之后, 则可将上述认证响应消息中的 RES 参数与预存的 HSS 发送的认证矢量中的 XRES 进行比较, 判断上述 RES 与 XRES 是否一致, 若判断结果为是, 则可判断得知上述 UE 是被允许接入的 UE, 即可通过 UE 的认证请求, 完成对 UE 的认证。

本发明实施例中所描述的控制网元 (MME) 可根据 UE-R 发送的第二请求消息确定上述第二请求消息中是否包含 UE 认证的标识信息或者上述第二请求消息的消息类型是否为指定消息类型, 在上述第二请求消息中包含 UE 认证的标识信息或者上述第二请求消息的消息类型为指定消息类型时向 HSS 发送认证数据请求消息, 并从 HSS 处获取对 UE 认证的认证矢量等认证标识信息, 进而将包含认证标识信息的认证请求消息发送给 UE-R, 以通过 UE-R 将上述认证标识信息发送给 UE; 在本发明实施例中 MME 可将包含对 UE 认证的标识信息的认证数据请求消息发送给 HSS, 或者将包含认证标识信息的认证请求消息发送给 UE-R, 可提高网络对 UE 认证的效率, 降低 UE-R 和 UE 等终端的复杂性和成本, 增强 UE 认证的用户体验。

参见图 20，是本发明实施提供的终端认证的系统的实施例结构示意图。本实施例中所描述的终端认证的系统，包括：上述本发明实施例提供的终端认证的用户设备 1000，上述本发明实施例提供的终端认证的中继设备 2000，上述本发明实施例提供的终端认证的控制设备 3000 和上述本发明实施例提供的终端认证的服务器 4000。

具体实现中，本发明上述提供的终端认证的系统的具体实现过程可参见上述本发明实施例提供的终端认证的方法或者装置（包括 UE、UE-R、MME 和 HSS）的具体实现过程，在此不再赘述。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）或随机存储记忆体（Random Access Memory, RAM）等。

以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权 利 要 求

1、一种终端认证的方法，其特征在于，包括：

用户设备中继 UE-R 接收用户设备 UE 发送的第一请求消息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，以使所述控制网元根据所述第二请求消息向归属用户服务器 HSS 发送认证数据请求消息，其中，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述 UE-R 接收所述控制网元发送的认证请求消息，判断所述认证请求消息是否是对所述 UE 的认证；

若所述认证请求消息是对所述 UE 的认证，所述 UE-R 向所述 UE 发送认证请求消息，所述认证请求消息中包括所述 UE 的认证参数；

所述 UE-R 接收所述 UE 根据所述认证请求消息发送的认证响应消息，并将所述认证响应消息发送给所述控制网元，以通过所述控制网元完成所述 UE 的认证。

2、如权利要求 1 所述的方法，其特征在于，所述 UE 发送的第一请求消息中包含所述 UE 认证的标识信息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，包括：

所述 UE-R 将所述第一请求消息中携带的所述 UE 认证的标识信息添加到所述第二请求消息中，并将所述第二请求消息发送给所述控制网元。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述 UE 发送的第一请求消息不包含所述 UE 认证的标识信息；

所述 UE-R 根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，包括：

所述 UE-R 在所述第二请求消息中添加所述 UE 认证的标识信息，并将所述第二请求消息发送给所述控制网元。

4、如权利要求 1-3 任意一项所述的方法，其特征在于，所述控制网元发送的认证请求消息中包括所述 HSS 根据所述 UE 认证的标识信息设定的对所述 UE 认证的认证标识信息；

所述判断所述认证请求消息是否是对所述 UE 的认证，包括：

判断所述认证请求消息中是否包含认证标识信息；

若所述认证请求消息中包含所述认证标识信息，则判断所述认证请求消息为对所述 UE 的认证。

5、一种终端认证的方法，其特征在于，包括：

HSS 接收控制网元发送的认证数据请求消息，根据所述认证数据请求消息判断所述认证数据请求消息是否包括 UE 认证的标识信息；

若所述认证数据请求消息中包括所述 UE 认证的标识信息，所述 HSS 在认证矢量中设定所述 UE 认证的认证标识信息；

所述 HSS 将所述认证矢量发送给所述控制网元，以通过所述控制网元将所述认证标识信息发送给 UE-R，以使所述 UE-R 根据所述认证标识信息判断是否是对所述 UE 的认证。

6、如权利要求 5 所述的方法，其特征在于，所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数、和 Ksme 参数；

所述 HSS 在所述认证矢量中设定所述 UE 认证的认证标识信息，包括：

所述 HSS 在所述认证矢量中的 AUTN 参数中的认证管理域 AMF 参数中设定所述认证标识信息。

7、如权利要求 5 或 6 所述的方法，其特征在于，所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数和 Ksme 参数；

所述 HSS 在所述认证矢量中设定所述 UE 认证的认证标识信息，还包括：

所述 HSS 对所述认证矢量中的 RAND 参数进行加密；

所述 HSS 在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认

证标识信息。

8、一种终端认证的方法，其特征在于，包括：

UE 向 UE-R 发送第一请求消息，以使所述 UE-R 根据所述第一请求消息向控制网元发送第二请求消息；

所述 UE 接收所述 UE-R 发送的认证请求消息，所述认证请求消息中携带所述 UE 认证的认证标识信息；

所述 UE 对所述认证标识信息中的加密信息进行解密，并根据所述解密得到的信息计算认证响应；

所述 UE 将所述认证响应发送给所述 UE-R，以通过所述 UE-R 发送给控制网元对所述 UE 进行认证。

9、如权利要求 8 所述的方法，其特征在于，所述 UE 向 UE-R 发送的所述第一请求消息中包括所述 UE 认证的标识信息。

10、一种终端认证的方法，其特征在于，包括：

控制网元接收 UE-R 发送的第二请求消息，判断所述第二请求消息是否包含 UE 认证的标识信息；

若所述第二请求消息包含所述 UE 认证的标识信息，所述控制网元向 HSS 发送认证数据请求消息，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述控制网元从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量；

所述控制网元将包含所述认证矢量信息的认证请求消息发送给所述 UE-R，以供所述 UE-R 判断所述认证请求消息是否是对 UE 的认证。

11、如权利要求 10 所述的方法，其特征在于，所述控制网元接收 UE-R 发送的第二请求消息之后，所述方法还包括：

判断所述第二请求消息是否为指定消息类型；

若所述第二请求消息为所述指定消息类型，所述控制网元向 HSS 发送认证数据请求消息。

12、如权利要求 10 或 11 所述的方法，其特征在于，所述控制网元向 HSS 发送认证数据请求消息之前，所述方法还包括：

所述控制网元添加所述 UE 认证的标识信息到所述认证数据请求消息中。

13、如权利要求 10-12 任意一项所述的方法，其特征在于，所述控制网元将包含所述认证矢量的认证请求消息发送给所述 UE-R 之前，所述方法还包括：
所述控制网元添加所述 UE 认证的标识信息到所述认证请求消息中。

14、一种终端认证的中继设备，其特征在于，包括：

接收模块，用于接收 UE 发送的第一请求消息；

发送模块，用于根据所述 UE 发送的所述第一请求消息向控制网元发送第二请求消息，以使所述控制网元根据所述第二请求消息向 HSS 发送认证数据请求消息，其中，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述接收模块，用于接收所述控制网元发送的认证请求消息；

判断模块，用于根据所述接收模块接收到的所述认证请求消息判断所述认证请求消息是否是对所述 UE 的认证；

所述发送模块，用于在所述判断模块判断结果为是时，向所述 UE 发送认证请求消息，所述认证请求消息中包括所述 UE 的认证参数；

所述接收模块，还用于接收所述 UE 根据所述发送模块发送的所述认证请求消息发送的认证响应消息；

所述发送模块，用于将所述接收模块接收到的所述认证响应消息发送给所述控制网元，以通过所述控制网元完成所述 UE 的认证。

15、如权利要求 14 所述的中继设备，其特征在于，所述接收模块接收到的所述 UE 发送的第一请求消息中包含所述 UE 认证的标识信息；

所述发送模块，还具体用于：

将所述第一请求消息中携带的所述UE认证的标识信息添加到所述第二请求消息中，并将所述第二请求消息发送给所述控制网元。

16、如权利要求 14 或 15 所述的中继设备，其特征在于，所述接收模块接收到的所述UE发送的第一请求消息中不包含所述UE认证的标识信息；

所述发送模块，具体用于：

在所述第二请求消息中添加所述UE认证的标识信息，并将所述第二请求消息发送给所述控制网元。

17、如权利要求 14-16 任意一项所述的中继设备，其特征在于，所述接收模块接收到的所述控制网元发送的认证请求消息中包括所述HSS根据所述UE认证的标识信息设定的对所述UE认证的认证标识信息；

所述判断模块，具体用于：

判断所述认证请求消息是否包含认证标识信息；

若所述认证请求消息中包含所述认证标识信息，则判断所述认证请求消息为对所述UE的认证。

18、一种终端认证的服务器，其特征在于，包括：

接收模块，用于接收控制网元发送的认证数据请求消息；

判断模块，用于根据所述接收模块接收到的所述认证数据请求消息判断所述认证数据请求消息是否包含UE认证的标识信息；

处理模块，用于在所述判断模块判断结果为是时，在认证矢量中设定所述UE认证的认证标识信息；

发送模块，用于将所述处理模块处理得到的所述认证矢量发送给所述控制网元，以通过所述控制网元将所述认证标识信息发送给UE-R，以使所述UE-R根据所述认证标识信息判断是否是对所述UE的认证。

19、如权利要求 18 所述的服务器，其特征在于，所述处理模块处理得到的所述认证矢量中包括：RAND 参数、AUTN 参数、XRES 参数、和 K_{asme}

参数;

所述处理模块,具体用于:

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

20、如权利要求 18 或 19 所述的服务器,其特征在于,所述处理模块处理得到的所述认证矢量中包括: RAND 参数、AUTN 参数、XRES 参数和 Ksme 参数;

所述处理模块,还具体用于:

对所述认证矢量中的 RAND 参数进行加密;

在所述认证矢量中的 AUTN 参数中的 AMF 参数中设定所述认证标识信息。

21、一种终端认证的用户设备,其特征在于,包括:

发送模块,用于向 UE-R 发送第一请求消息,以使所述 UE-R 根据所述第一请求消息向控制网元发送第二请求消息;

接收模块,用于接收所述 UE-R 发送的认证请求消息,所述认证请求消息中携带 UE 认证的认证标识信息;

处理模块,用于对所述认证标识信息中的加密信息进行解密,并根据所述解密得到的信息计算认证响应。

22、如权利要求 21 所述的用户设备,其特征在于,所述发送模块发送的所述第一请求消息中包括所述 UE 认证的标识信息。

23、一种终端认证的控制设备,其特征在于,包括:

接收模块,用于接收 UE-R 发送的第二请求消息;

处理模块,用于根据所述接收模块接收到的所述第二请求消息判断所述第二请求消息是否包含 UE 认证的标识信息;

发送模块,用于在所述处理模块判断结果为是时,向 HSS 发送认证数据

请求消息，所述认证数据请求消息中携带所述 UE 认证的标识信息；

所述接收模块，用于从所述 HSS 处获取所述 HSS 根据所述认证数据请求消息确定的认证矢量；

所述发送模块，还用于将所述接收模块接收到的包含所述认证矢量信息的认证请求消息发送给所述 UE-R，以供所述 UE-R 判断所述认证请求消息是否是对 UE 的认证。

24、如权利要求 23 所述的控制设备，其特征在于，所述控制设备，还包括：

判断模块，用于根据所述接收模块接收到的第二请求消息判断所述第二请求消息是否为指定消息类型，若所述第二请求消息为所述指定消息类型，则通知所述发送模块向 HSS 发送认证数据请求消息。

25、如权利要求 23 或 24 所述的控制设备，其特征在于，所述发送模块，还具体用于：

添加所述 UE 认证的标识信息到所述认证数据请求消息中，并将所述认证数据请求消息发送给所述 HSS。

26、如权利要求 23-25 任一项所述的控制设备，其特征在于，所述发送模块，还具体用于：

添加所述 UE 认证的标识信息到所述包含所述认证矢量的认证请求消息中，并将认证请求消息发送给所述 UE-R。

27、一种终端认证的系统，其特征在于，包括：如上述权利要求 14-17 所述的中继设备、如上述权利要求 18-20 所述的服务器、如上述权利要求 21-22 所述的用户设备和如权利要求 23-26 所述的控制设备。

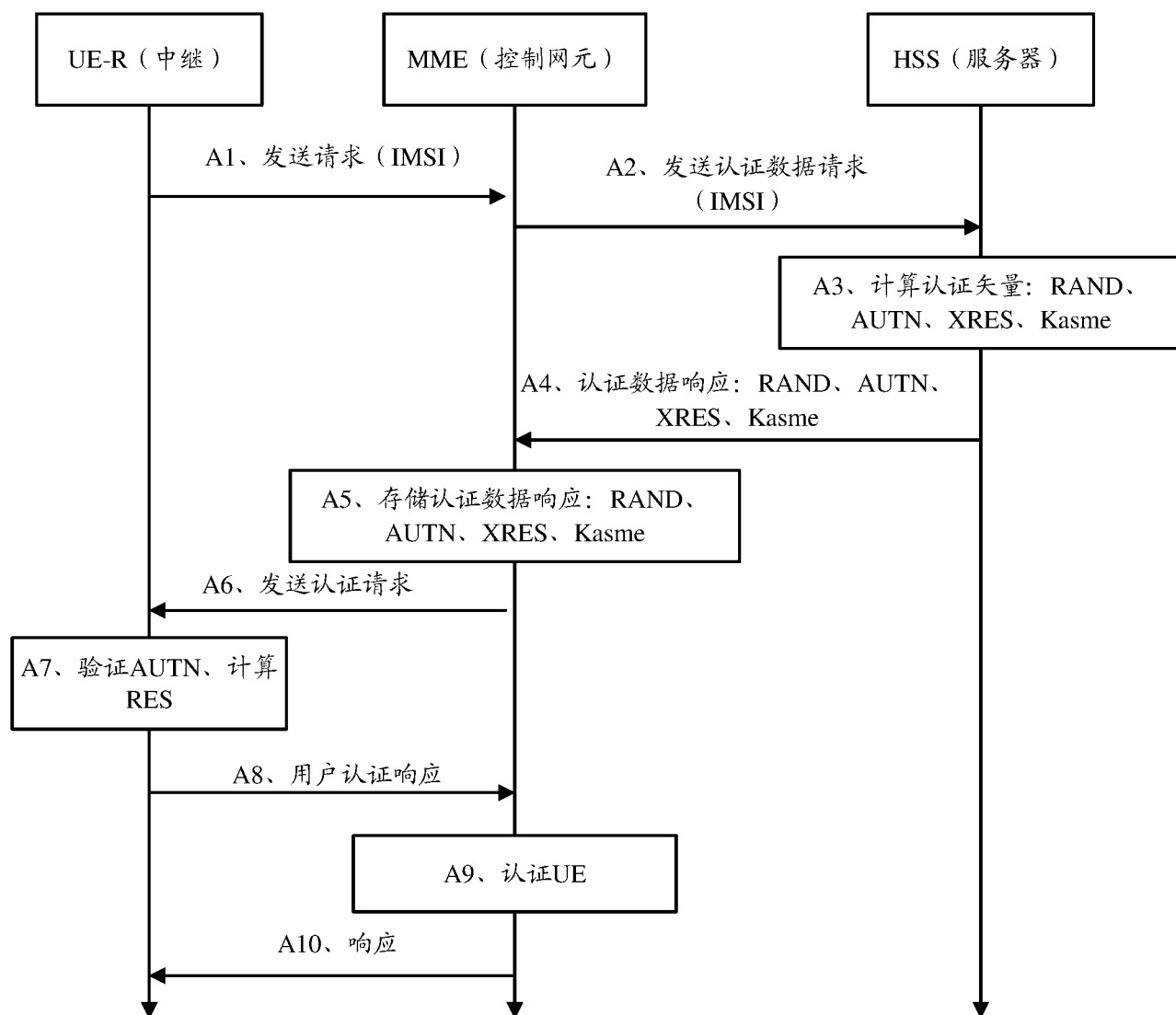


图 1

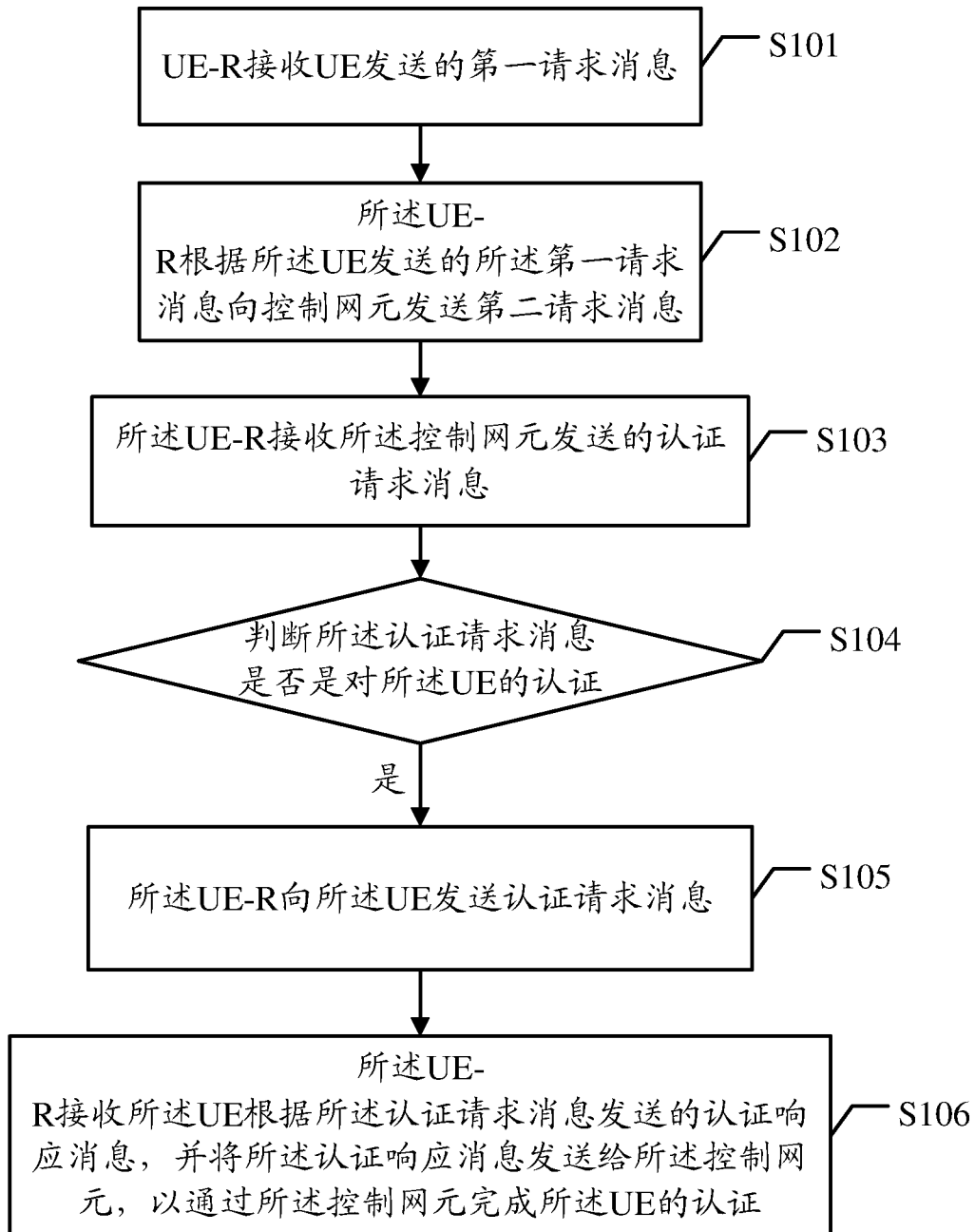


图 2

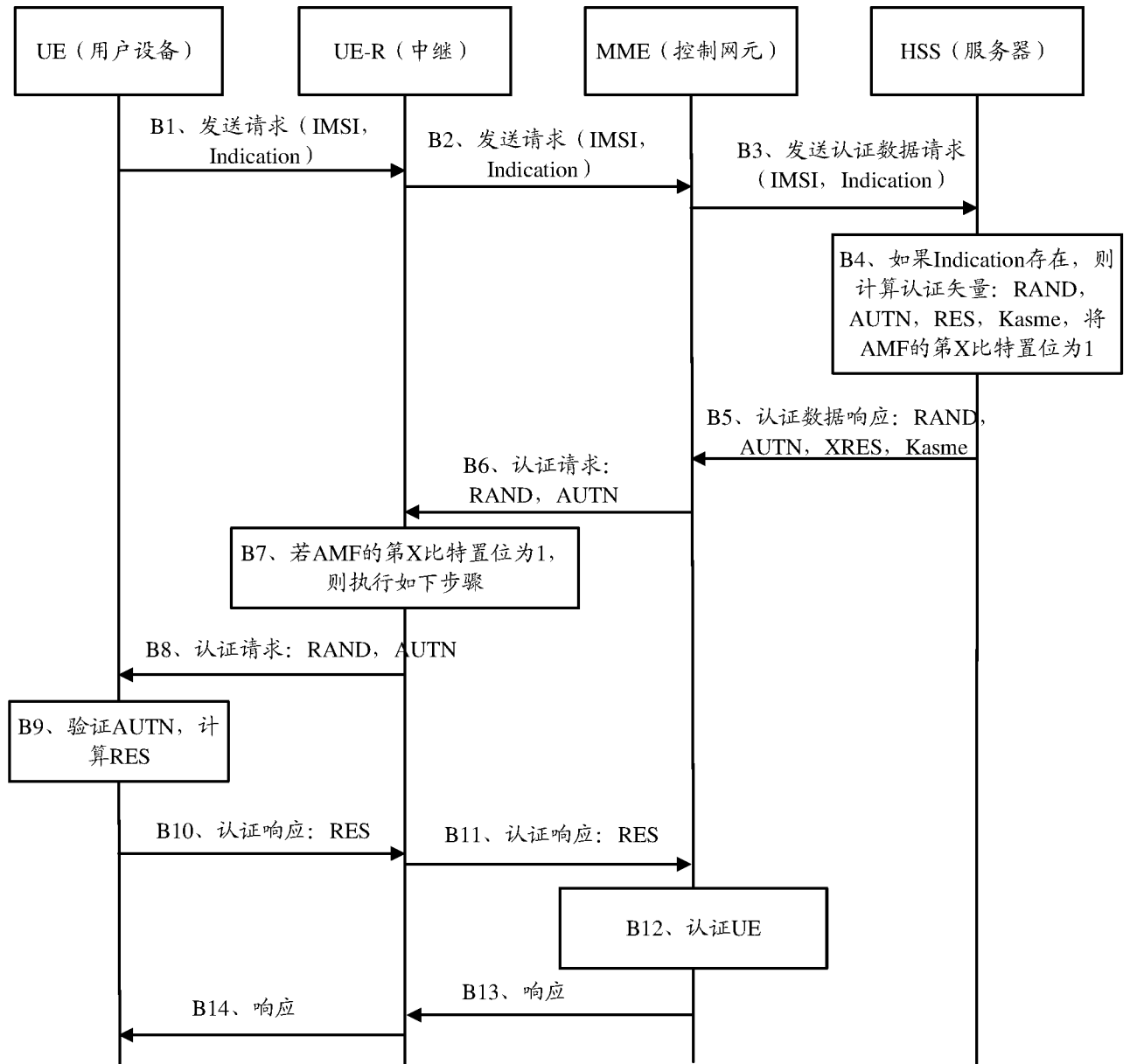


图 3

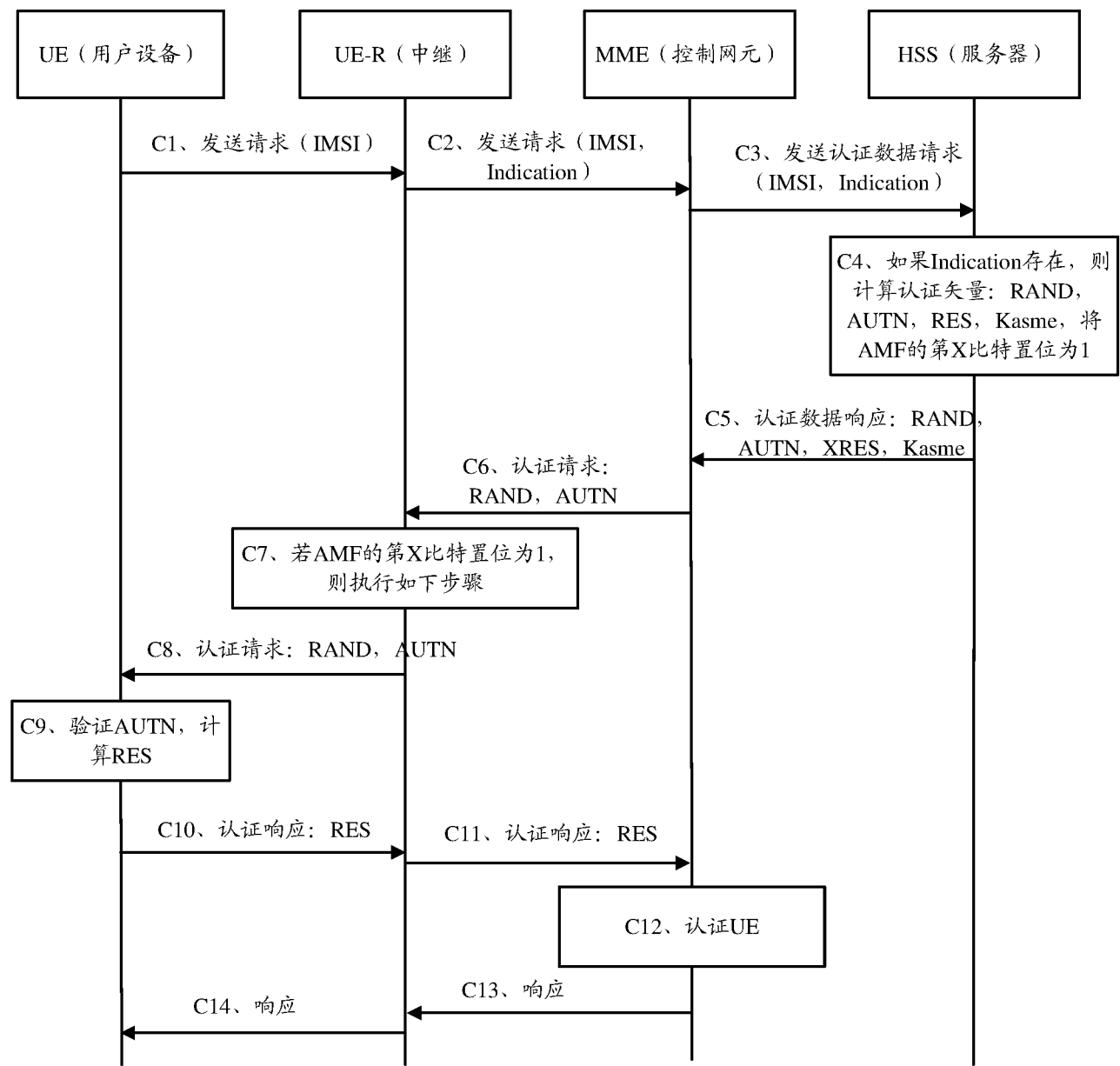


图 4

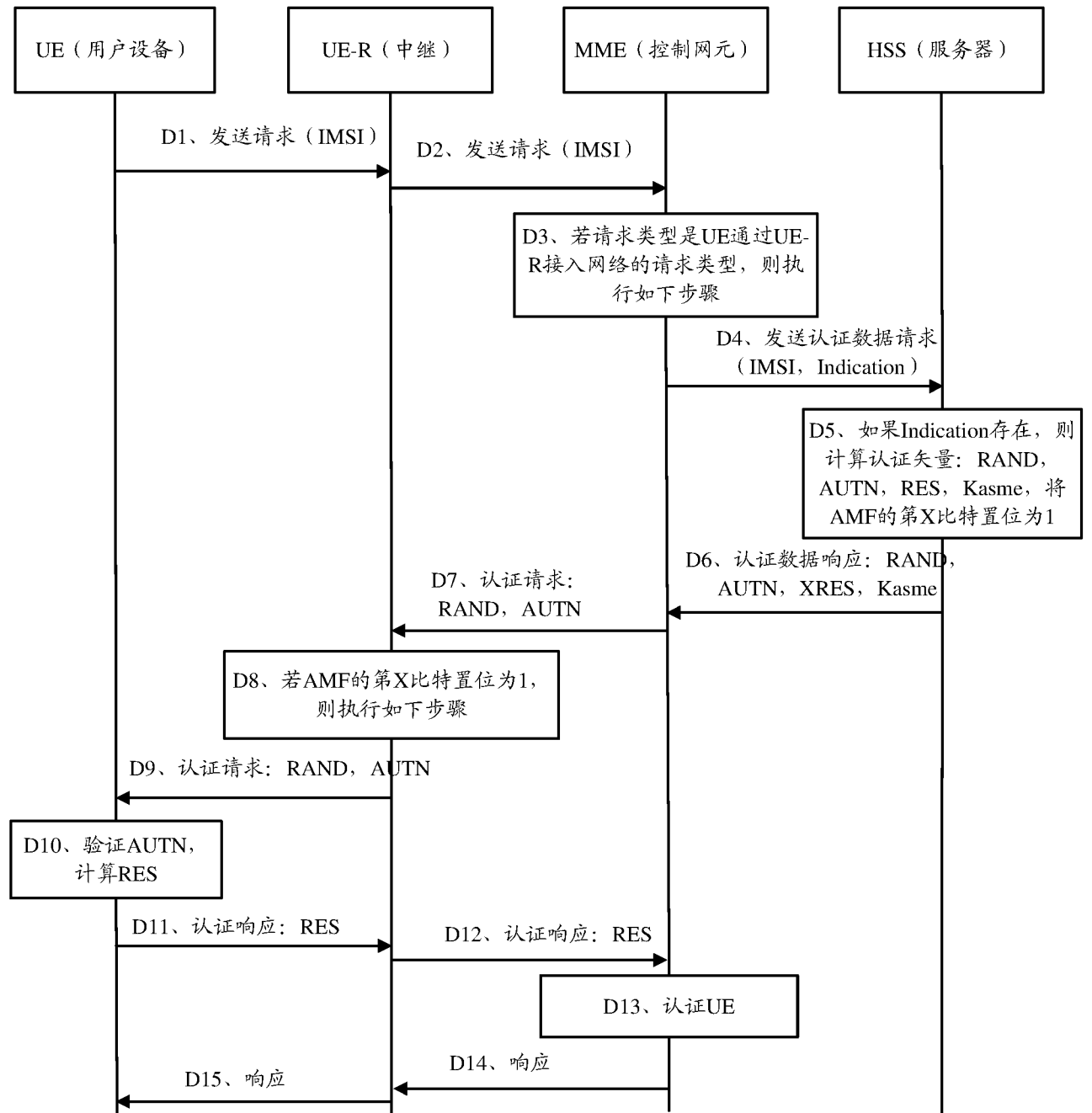


图 5

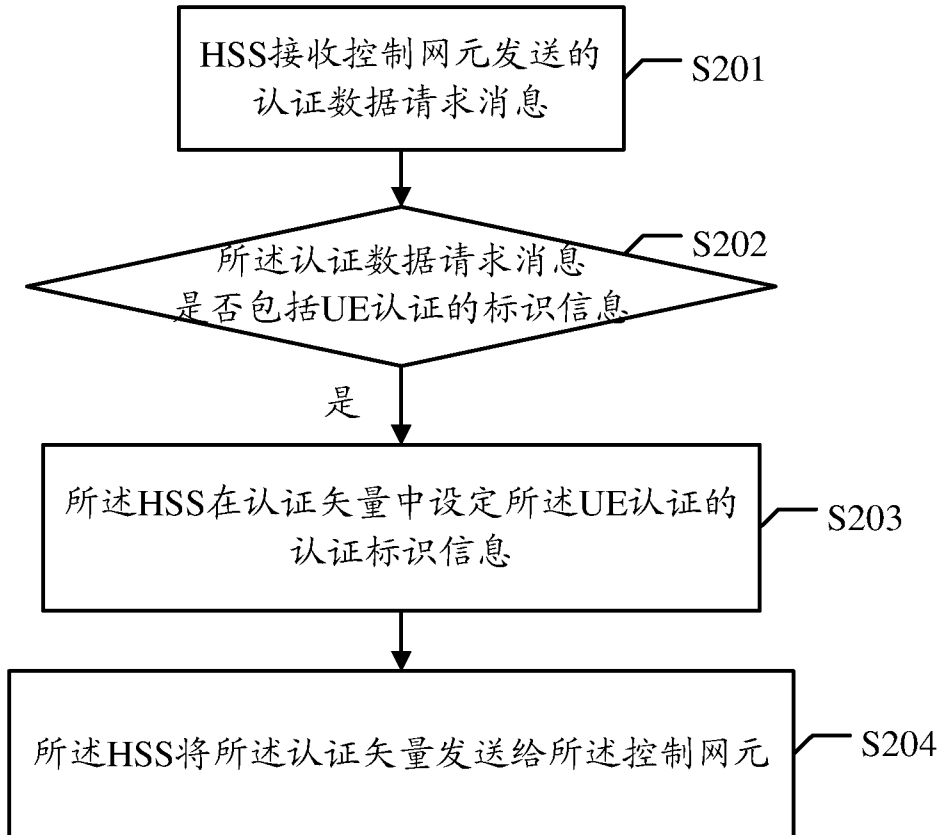


图 6

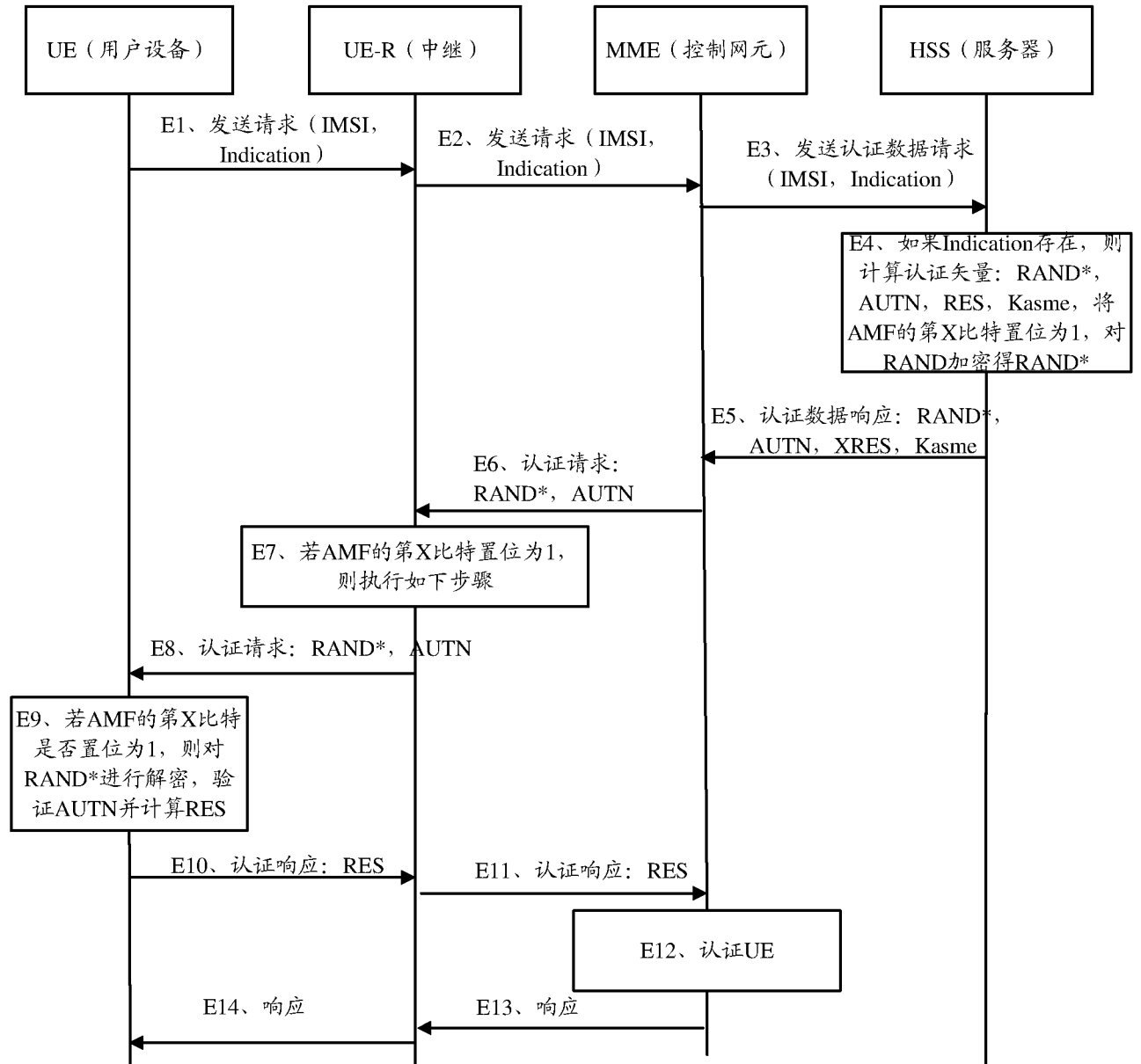


图 7

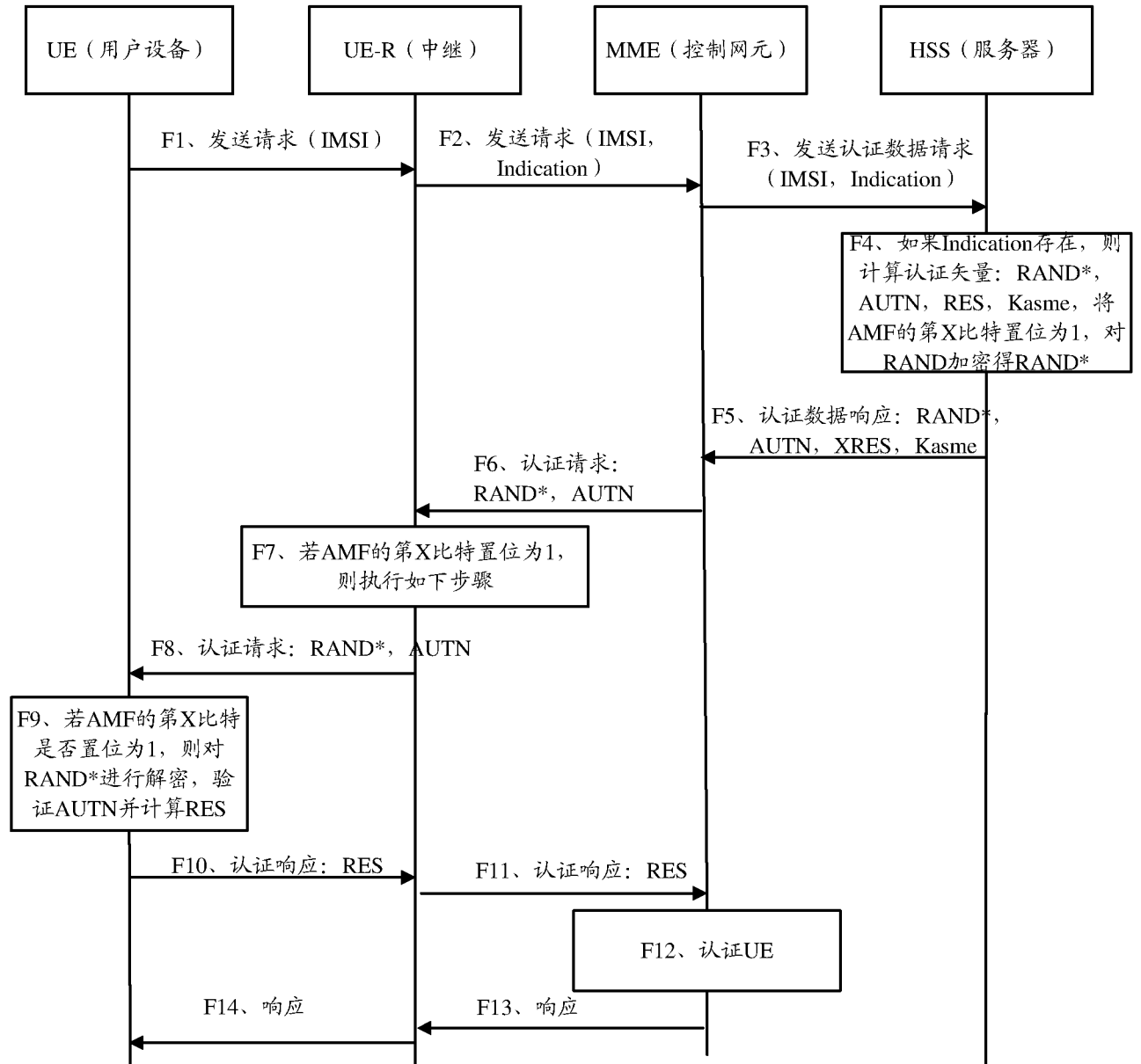


图 8

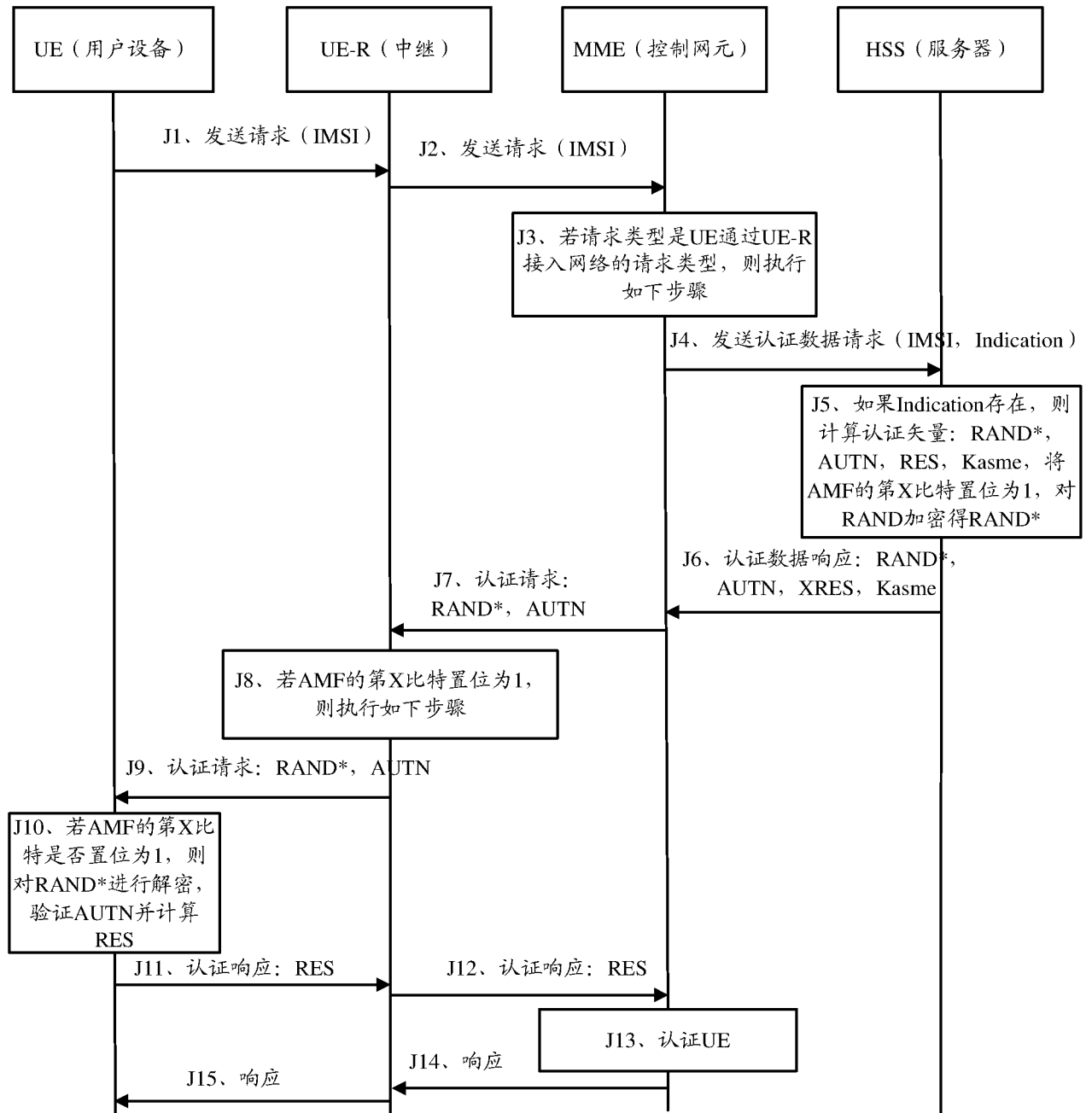


图 9

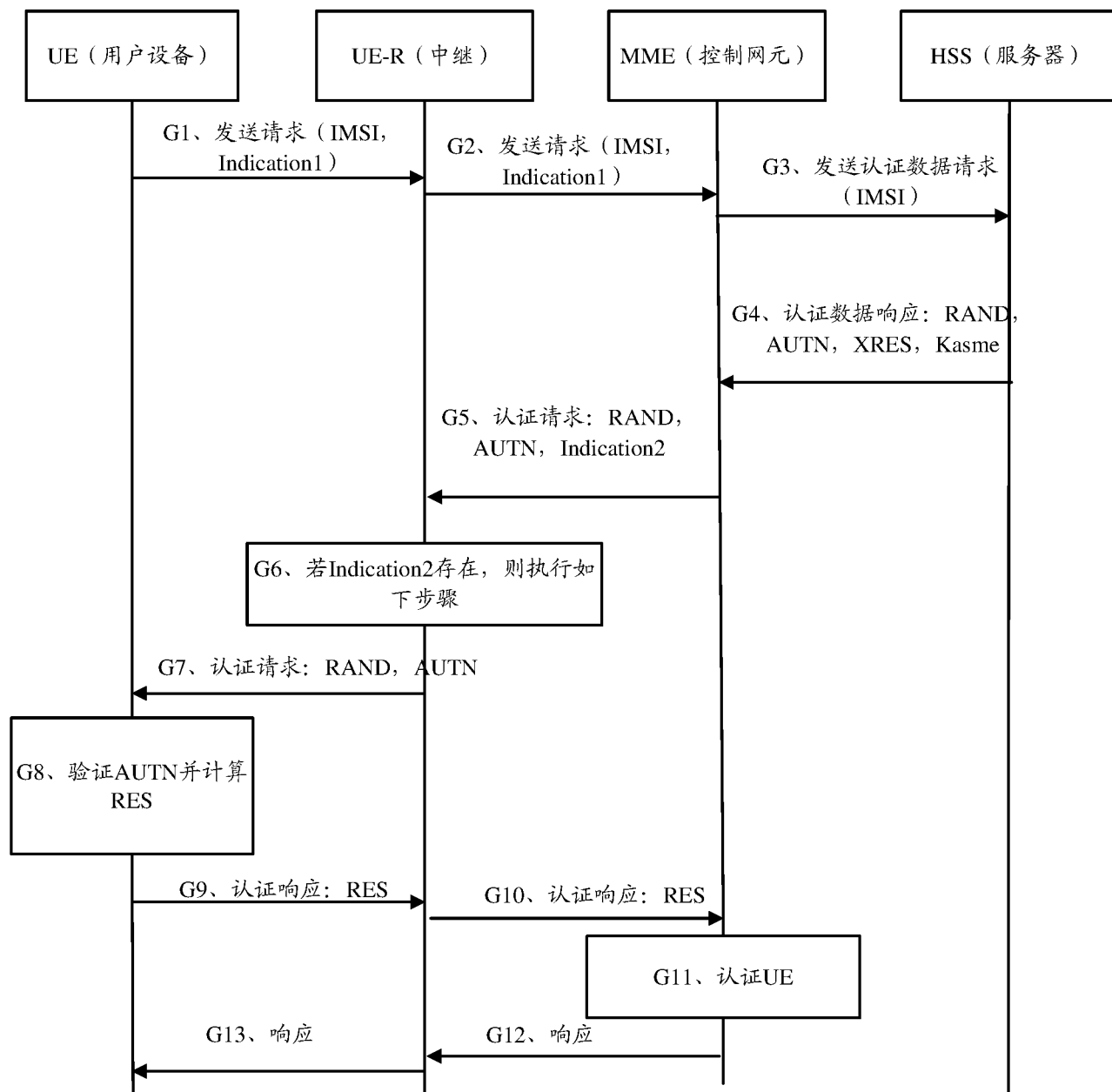


图 10

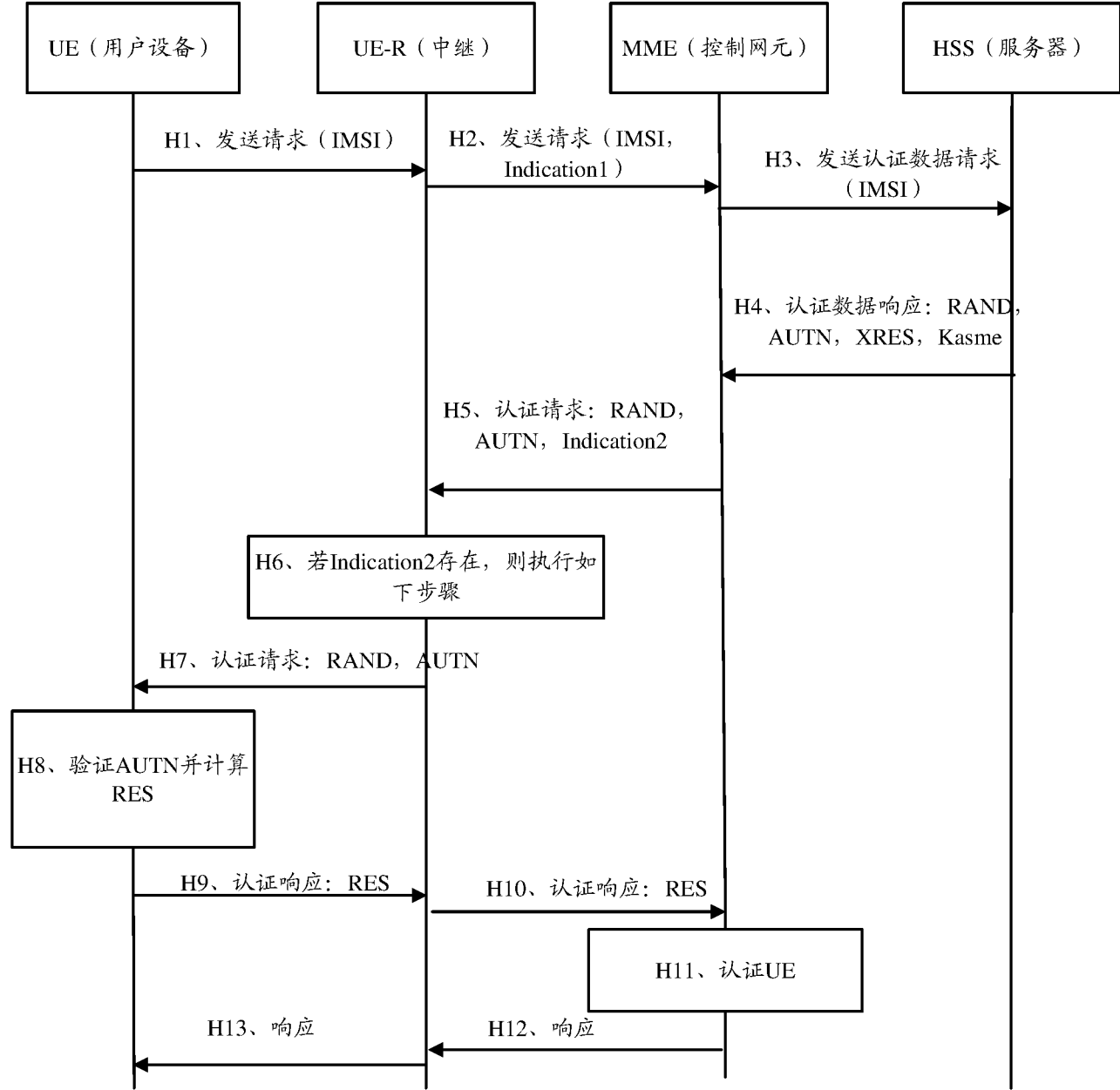


图 11

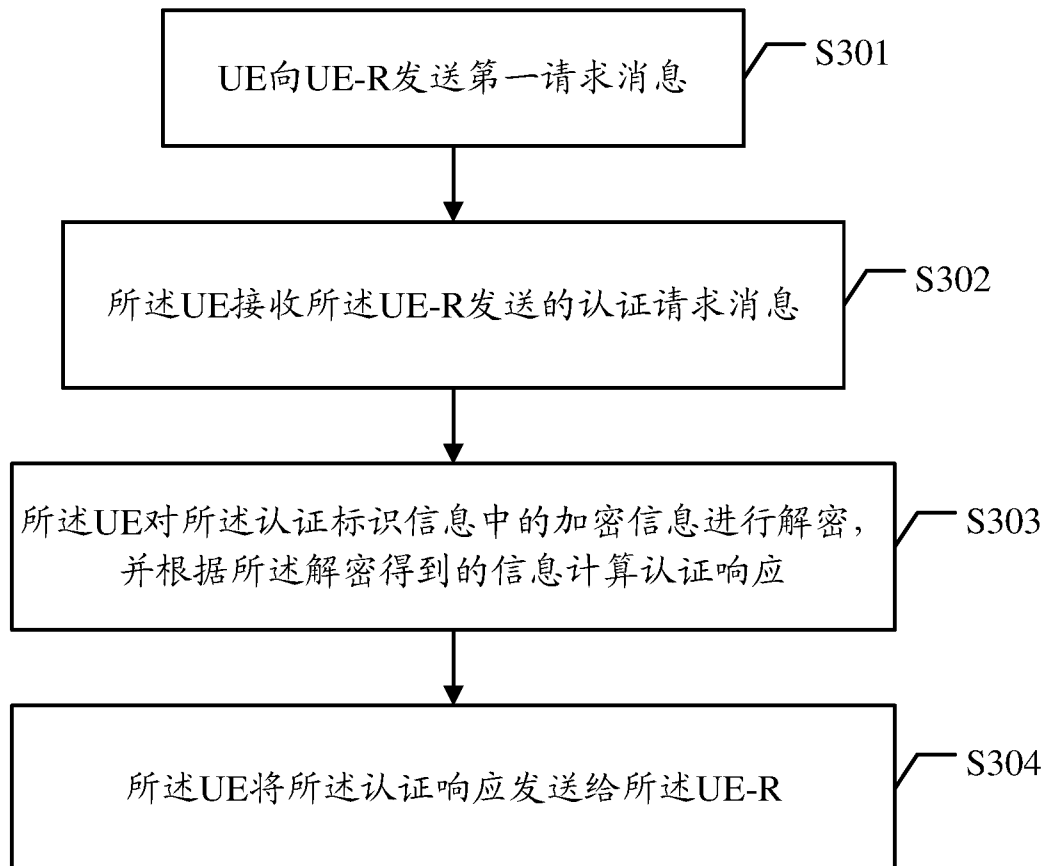


图 12

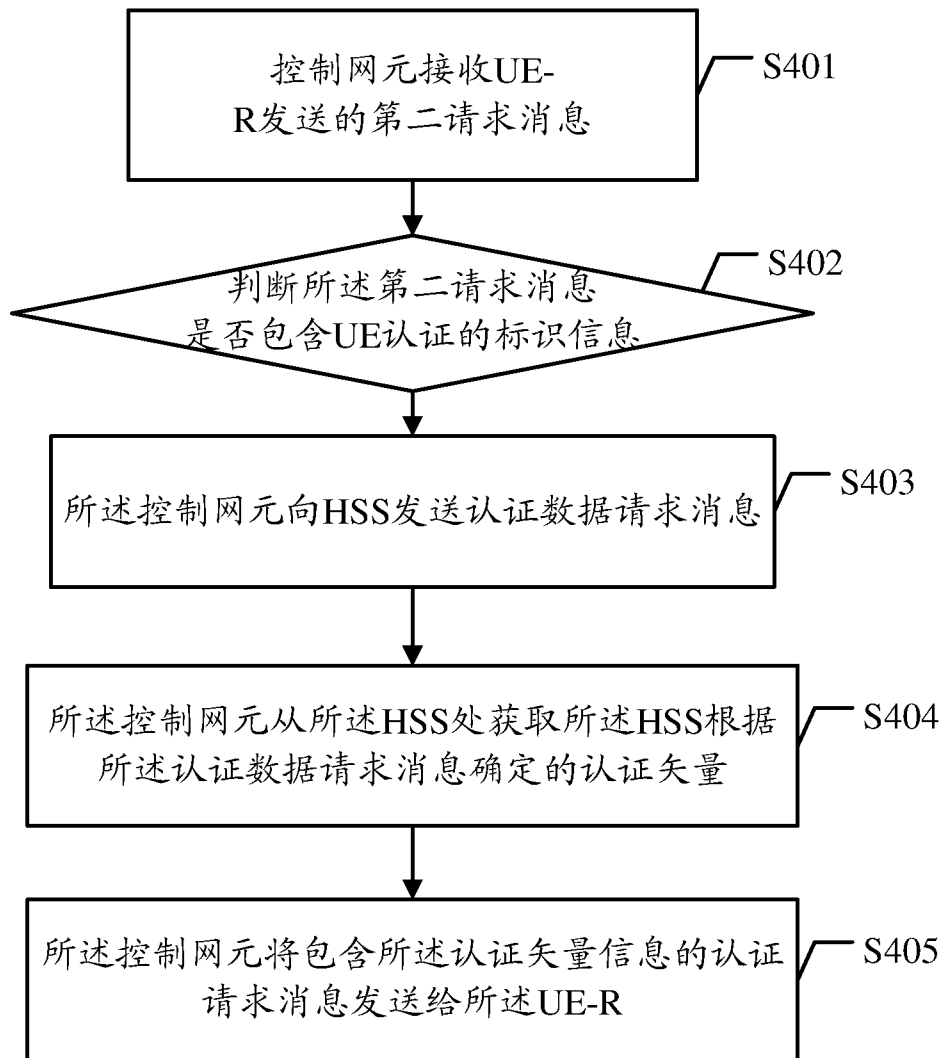


图 13

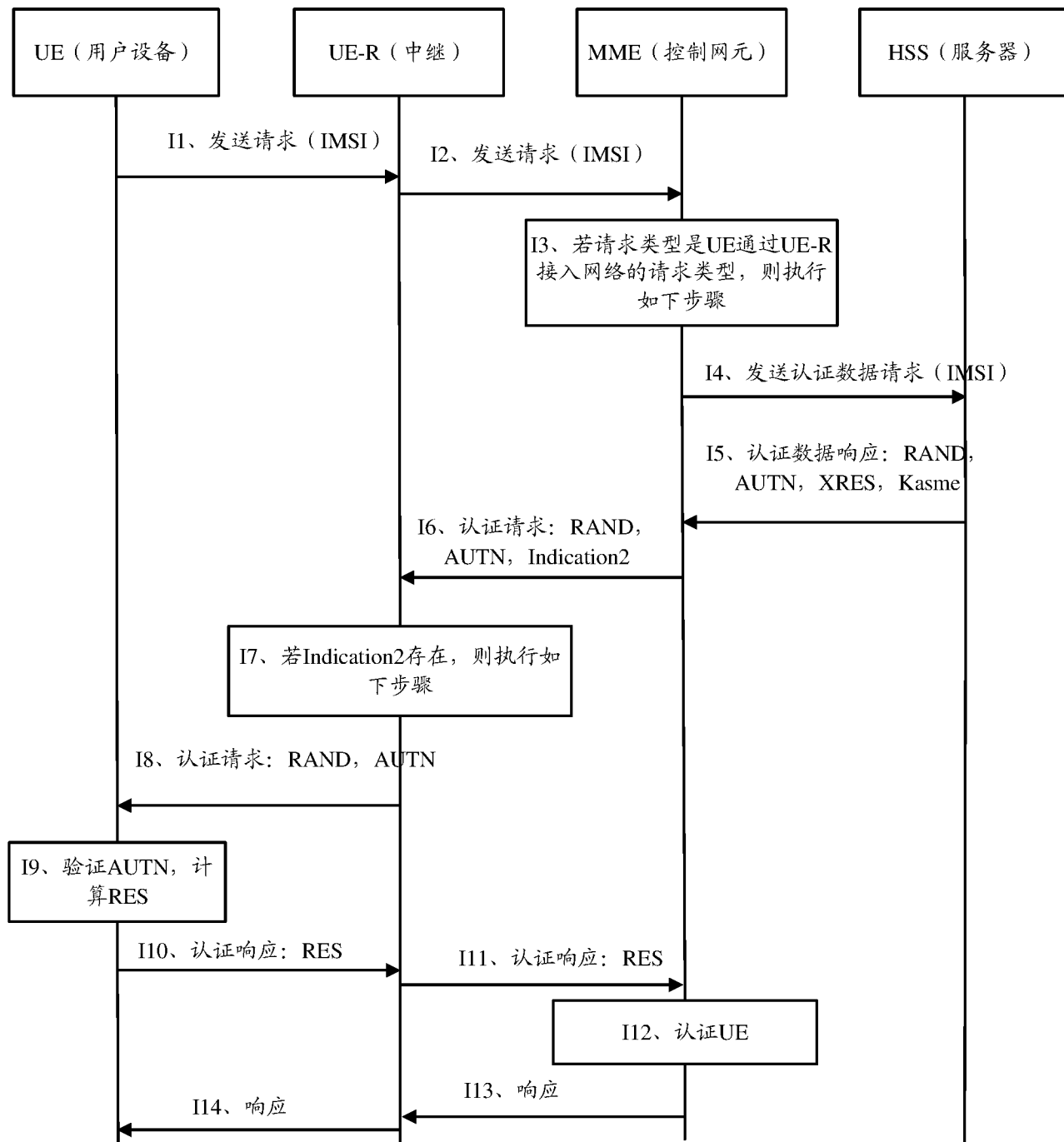


图 14

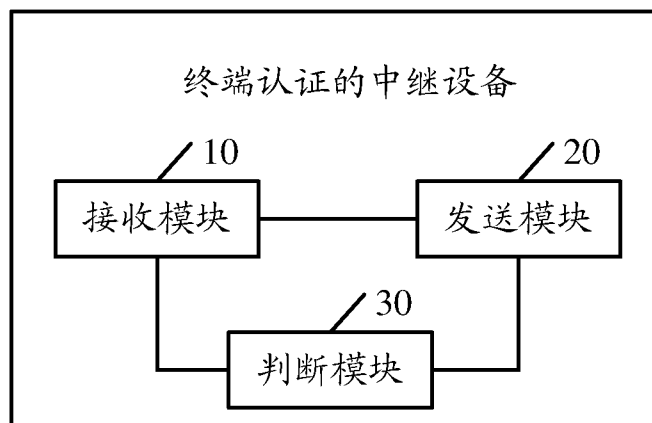


图 15

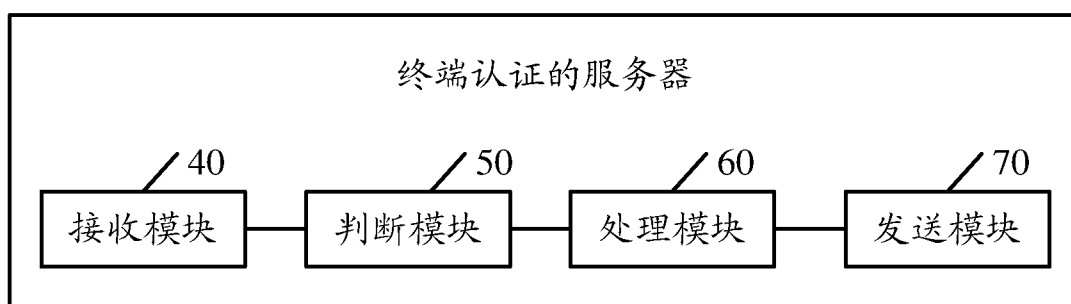


图 16

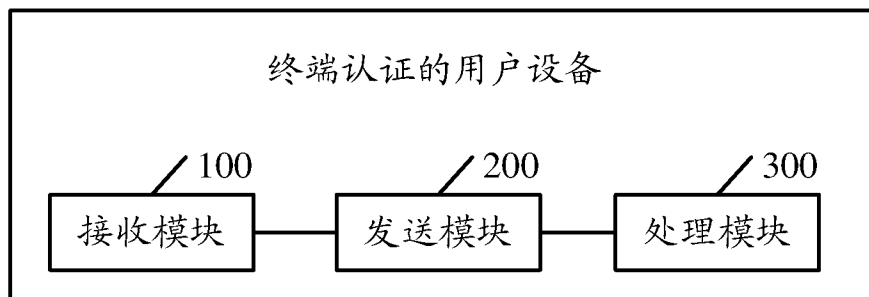


图 17

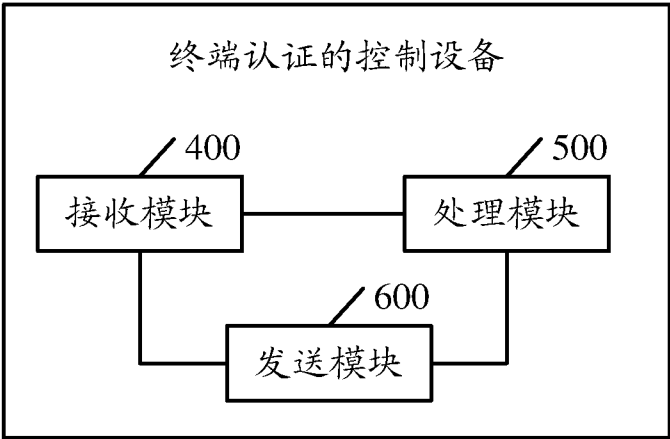


图 18

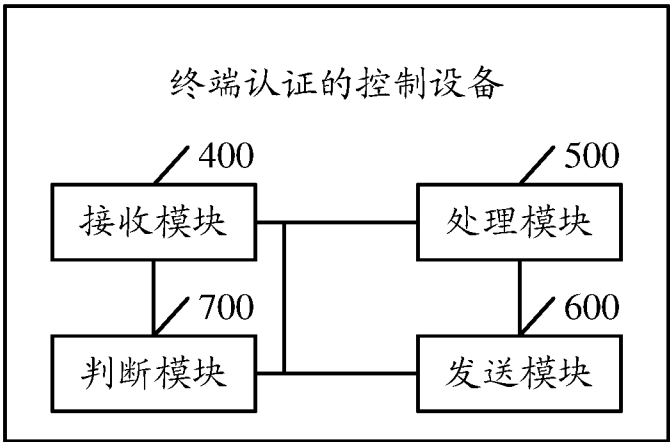


图 19

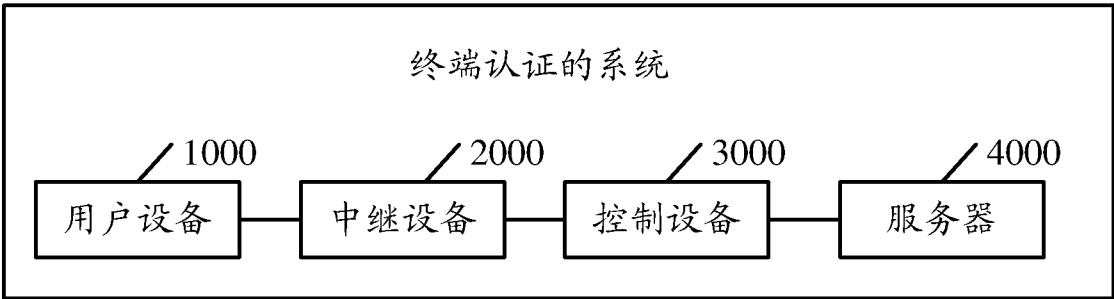


图 20

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/080713**A. CLASSIFICATION OF SUBJECT MATTER**

H04W 12/06 (2009.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W, H04Q, H04L, H04B

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)

WPI, EPODOC, CNKI, CNPAT: mobile terminal, protocol, short distance, mobile, terminal, handset, authentication, authorization, accounting, relay, RN, add, proximity, prose, eap, eps, aka, packet, core

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101931955 A (ZTE CORP.), 29 December 2010 (29.12.2010), description, page 7, and figure 5	1-27
A	CN 101977378 A (ZTE CORP.), 16 February 2011 (16.02.2011), the whole document	1-27
A	CN 103379490 A (HUAWEI TECHNOLOGIES CO., LTD.), 30 October 2013 (30.10.2013), the whole document	1-27
A	WO 2012137643 A1 (NTT DOCOMO, INC. et al.), 11 October 2012 (11.10.2012), the whole document	1-27

☐ 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

10 September 2014 (10.09.2014)

Date of mailing of the international search report

10 October 2014 (10.10.2014)

Name and mailing address of the ISA/CN:

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

Authorized officer

FENG, MeiyuTelephone No.: (86-10) **62413205**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/080713

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101931955 A	29 December 2010	WO 2012028010 A1	08 March 2012
CN 101977378 A	16 February 2011	None	
CN 103379490 A	30 October 2013	WO 2013152740 A1	17 October 2013
WO 2012137643 A1	11 October 2012	JP 2012217110 A	08 November 2012
		CN 103460743 A	18 December 2013
		US 2014094145 A1	03 April 2014
		KR 20130137037 A	13 December 2013
		MX 2013011315 A	06 December 2013
		AU 2012239436 A1	31 October 2013
		EP 2696616 A1	12 February 2014
		INK OLNP201303127 P2	14 February 2014

A. 主题的分类		
H04W 12/06 (2009.01) i		
按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献 (标明分类系统和分类号)		
H04W, H04Q, H04L, H04B		
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))		
WPI, EPDOC, CNKI, CNPAT: 移动终端, 认证, 中继, 协议, 增加, 近距离, 分组, 核心, mobile, terminal, handset, authentication, authorization, accounting, relay, RN, add, proximity, prose, eap, eps, aka, packet, core		
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
A	CN 101931955 A (中兴通讯股份有限公司) 2010年 12月 29日 (2010 - 12 - 29) 说明书第7页, 图5	1-27
A	CN 101977378 A (中兴通讯股份有限公司) 2011年 2月 16日 (2011 - 02 - 16) 全文	1-27
A	CN 103379490 A (华为技术有限公司) 2013年 10月 30日 (2013 - 10 - 30) 全文	1-27
A	WO 2012137643 A1 (NTT DOCOMO, INC. 等) 2012年 10月 11日 (2012 - 10 - 11) 全文	1-27
☐ 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
2014年 9月 10日		2014年 10月 10日
ISA/CN的名称和邮寄地址		授权官员
中华人民共和国国家知识产权局 (ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国		冯美玉
传真号 (86-10)62019451		电话号码 (86-10)62413205

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/080713

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	101931955	A	2010年 12月 29日	WO	2012028010	A1	2012年 3月 08日
CN	101977378	A	2011年 2月 16日	无			
CN	103379490	A	2013年 10月 30日	WO	2013152740	A1	2013年 10月 17日
WO	2012137643	A1	2012年 10月 11日	JP	2012217110	A	2012年 11月 08日
				CN	103460743	A	2013年 12月 18日
				US	2014094145	A1	2014年 4月 03日
				KR	20130137037	A	2013年 12月 13日
				MX	2013011315	A	2013年 12月 06日
				AU	2012239436	A1	2013年 10月 31日
				EP	2696616	A1	2014年 2月 12日
				INK	OLNP201303127	P2	2014年 2月 14日