(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
2023 年 8 月 3 日 (03.08.2023)

WIPO | PCT

(10) 国际公布号
WO 2023/143251 A1

(51) 国际专利分类号:
H04W 12/041 (2021.01)

(21) 国际申请号: PCT/CN2023/072627

(22) 国际申请日: 2023 年 1 月 17 日 (17.01.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210114688.0 2022年1月30日 (30.01.2022) 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: 吴义壮(**WU, Yizhuang**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 雷骜(**LEI, Ao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李赫(**LI, He**); 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: 北京中博世达专利商标代理有限公司 (**BEIJING ZBSD PATENT & TRADEMARK AGENT LTD.**); 中国北京市海淀区交大东路31号11号楼8层, Beijing 100044 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ,

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

(54) 发明名称: 通信方法及装置

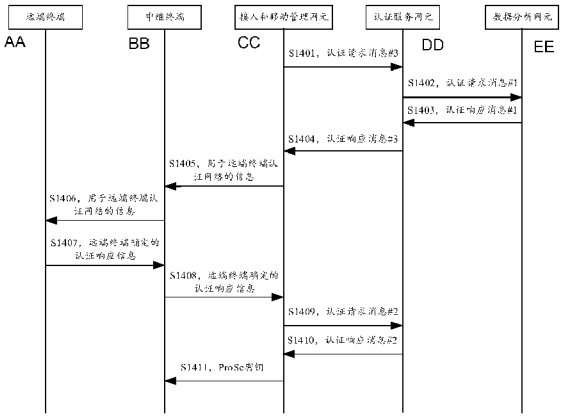

图 14

S1401, S1404 Authentication request message #3
S1402, S1403 Authentication request message #1
S1405, S1406 Information for a remote terminal to authenticate a terminal
S1407, S1408 Authentication response information determined by the remote terminal
S1409, S1410 Authentication request message #2
S1411 ProSe key
AA Remote terminal
BB Relay terminal
CC Access and mobility management network element
DD Authentication service network element
EE Data analysis network element

(57) **Abstract:** The present application relates to the field of communication, and provides a communication method and apparatus, for use in ensuring the security of proximity service relay communication. In the method, by means of proximity service authentication information #1 provided by a data management network element, a remote terminal and a network can authenticate each other and generate a proximity service key for communication between the remote terminal and a relay terminal; furthermore, a remote terminal device and a relay terminal device deduce a communication protection key of a PC5 connection (i.e., a connection between the remote

WO 2023/143251 A1

[见续页]

IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, 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, CV, 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, ME, 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))。

terminal and the relay terminal) on the basis of the proximity service key, wherein the communication protection key may comprise at least one of an encryption key and an integrity protection key, thereby ensuring the security of proximity service relay communication, and avoiding situations, such as user information leakage, caused by attacks.

(57) 摘要：本申请提供一种通信方法及装置，涉及通信领域，用以确保临近业务中继通信的安全。该方法中，通过数据管理网元提供的临近业务认证信息#1，远端终端和网络可以彼此认证对方并生成用于远端终端和中继终端通信的临近业务密钥，进一步的，远端终端设备和中继终端设备基于该临近业务密钥推演PC5连接(即远端终端和中继终端间的连接)的通信保护密钥，可以包含加密密钥和完整性保护密钥中的至少一个，以确保临近业务中继通信安全，避免出现因被攻击而导致用户信息泄露等情况。

通信方法及装置

本申请要求于2022年01月30日提交国家知识产权局、申请号为202210114688.0、申请名称为“通信方法及装置”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

本申请涉及通信领域，尤其涉及一种通信方法及装置。

背景技术

在通信系统中，如果某个用户设备（user equipment，UE）1 处于网络覆盖之外、或与接入网（radio access network，RAN）设备间通信信号不好、或需要其他 UE 协助传输数据时，UE1 可以通过另一个 UE（例如 UE2）的辅助，从网络侧获取业务。例如，UE1 与 UE2 在空口建立临近业务通信 5（ProSe communication 5，PC5）接口连接，以通过 PC5 连接与网络侧通信。这种情况下，UE1 可认为是临近业务（proximity based services，ProSe）远端（remote）UE，或者简称为远端 UE。UE2 可认为是临近业务 UE 到网络的中继（ProSe UE-to-network relay），或者简称为中继 UE。远端 UE 通过中继 UE 与网络侧之间的通信可以认为是 ProSe 中继通信。

然而，ProSe 中继通信存在安全风险，容易被攻击，导致用户信息泄露。

发明内容

本申请实施例提供一种通信方法及装置，用以确保 ProSe 中继通信的安全，避免出现因被攻击而导致用户信息泄露等情况。

为达到上述目的，本申请采用如下技术方案：

第一方面，提供一种通信方法。该通信方法包括：认证服务网元向数据管理网元发送认证请求消息#1，并接收来自数据管理网元的认证响应消息#1。认证请求消息#1 用于请求认证远端终端，认证响应消息#1 包括：临近业务 ProSe 认证信息#1，ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。在远端终端认证网络通过的情况下，认证服务网元接收来自接入和移动管理网元的认证请求消息#2，该认证请求消息#2 用于请求认证远端终端。如此，在认证远端终端通过的情况下，例如认证服务网元认证远端终端通过，或者认证服务网元和接入和移动管理网元都认证远端终端通过，认证服务网元向接入和移动管理网元发送认证响应消息#2。其中，认证请求消息#2 用于请求认证远端终端；认证响应消息#2 包括：ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

基于第一方面所述的方法可知，通过数据管理网元提供的 ProSe 认证信息#1，远端终端和网络可以彼此认证对方。在双方都认证通过的情况下，便可生成用于远端 UE 和中继 UE 通信的 ProSe 密钥，以便基于 ProSe 密钥推演 PC5 连接（即远端 UE 和中继 UE 间的连接）的通信保护密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全，避免出现因被攻击而导致用户信息泄露等情况。

可选地，远端终端和中继终端可以基于 ProSe 密钥推演 PC5 连接的通信保护密钥，例如，远端终端和中继终端可以基于 ProSe 密钥推演一个会话密钥，然后远端终端和中继终端基于会话密钥进一步推演通信保护密钥（如加密密钥和完整性保护密钥），本申请不限制。

一种可能的设计方案中，ProSe 认证信息#1 可以为如下至少一项：认证与密钥协商 AKA 的 ProSe 认证向量#1、或扩展认证协议请求 EAP-AKA’的 ProSe 的认证向量。也就是说，远端 UE 与网络之间的认证可以基于对已有认证方法，例如 5G AKA 或 EAP-AKA’增强实现，以实现在不引入新的认证方法的情况下，确保 ProSe 中继通信安全。

可选地，AKA 的 ProSe 认证向量#1 或 EAP-AKA’的 ProSe 的认证向量可以包括如下至少一项：用于远端终端认证网络的信息、用于认证服务网元认证远端终端的信息、或用于确定 ProSe 密钥的信息。可以看出，认证向量不仅可用于远端 UE 与网络之间的认证，还用于确定 ProSe 密钥。以便 AUSF 网元在确定认证通过的情况下，可以根据认证向量推演 ProSe 密钥，无需额外获取，以提高认证效率和密钥推演效率。

可选地，在认证服务网元向数据管理网元发送认证请求消息#1 之前，第一方面所述的方法还可以包括：认证服务网元接收来自接入和移动管理网元的认证请求消息#3。相应的，在认证服务网元接收来自数据管理网元的认证响应消息#1 之后，在认证服务网元接收来自接入和移动管理网元的认证请求消息#2 之前，第一方面所述的方法还可以包括：认证服务网元向接入和移动管理网元发送认证响应消息#3。认证响应消息#3 可以包括：ProSe 认证信息#2，ProSe 认证信息#2 包括：用于远端终端认证网络的信息。可选地，ProSe 认证信息#2 还可以包括：用于网络认证远端终端的信息。也就是说，ProSe 中继通信的认证可以由接入和移动管理网元触发，例如在业务有需求的情况下触发，以便认证服务网元可以有针对性地执行认证，确保认证的有效性。

进一步的，ProSe 认证信息#2 可根据 ProSe 认证信息#1 确定。ProSe 认证信息#2 可以为如下至少一项：AKA 的 ProSe 认证向量#2、或 EAP 请求消息或 AKA’挑战消息。例如，如果采用增强的 AKA 认证机制，则 AKA 的 ProSe 认证向量#2 可根据 AKA 的 ProSe 认证向量#1 确定，无需引入新的功能，从而降低网元复杂度。如果采用增强的 EAP-AKA’认证机制，则 EAP 请求消息或 AKA’挑战消息可根据 EAP-AKA’的 ProSe 的认证向量确定，无需引入新的功能，从而降低网元复杂度。

进一步的，AKA 的 ProSe 认证向量#2 可以包括：用于接入和移动管理网元认证远端终端的信息。如此，AKA 的 ProSe 认证向量#2 还可用于接入和移动管理网元从服务网的角度认证远端终端，从而可以提高认证的全面性，进一步确保 ProSe 中继通信安全。

可选地，认证请求消息#3 可用于请求认证远端终端。比如，请求认证服务网元认证远端终端，用以触发认证服务网元执行 ProSe 通信的认证流程，确保认证的可靠性。

进一步的，认证请求消息#3 可以包括如下至少一项：远端终端的用户隐藏标识 SUCI、服务网络名称、中继服务码 RSC、随机值#1、或 ProSe 中继通信指示信息。

其中，服务网络名称、RSC 或 ProSe 中继通信指示信息中的任一项可用于指示认证为 ProSe 中继通信的认证，以触发认证服务网元执行 ProSe 通信的认证流程，确保认证的准确性和可靠性，避免对现有流程的影响。服务网络名称、RSC、或随机值#1 中的任一项可用于确定 ProSe 密钥，以便 AUSF 网元在确定认证通过的情况下，可以直接根据这些参数推演 ProSe 密钥，无需额外获取，以提高密钥推演效率。

进一步的，在认证服务网元向接入和移动管理网元发送认证响应消息#2 之前，第一方面所述的方法还可以包括：若认证请求消息#3 中包括：RSC 和随机值#1，则认证服务网元保存 RSC 和随机值#1，以便后续密钥推演时可直接使用，无需再次获取，以进一步提高密钥推演效率。

进一步的，用于确定 ProSe 密钥的信息包括：中间密钥。在认证服务网元向接入和移动管理网元发送认证响应消息#2 之前，第一方面所述的方法还可以包括：在认证远端终端通过的情况下，认证服务网元根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密钥，确定 ProSe 密钥。也就是说，认证服务网元可以根据业务场景以及密钥隔离等需求，选择合适的参数来确定 ProSe 密钥，以适应更多业务场景。例如，根据 RSC、随机值#1、随机值#2 和中间密钥确定 ProSe 密钥。或者，根据服务网络名称、随机值#1、随机值#2 和中间密钥确定 ProSe 密钥。其中，中间密钥也可以是根据 ProSe 认证向量确定的。

一种可能的设计方案中，认证请求消息#2 可以包括如下至少一项：远端终端确定的认证响应信息、用于确定 ProSe 密钥的 RSC、或用于确定 ProSe 密钥的随机值#1。认证响应信息用于认证远端终端。也就是说，接入和移动管理网元可以在确定远端终端认证通过的情况下，才向认证服务网元发送用于推演 ProSe 密钥的参数，例如 RSC 和/或随机值#1，从而实现按需提供必要的参数，无需预存信息，防止资源浪费。

可选地，认证响应消息#2 可以包括：随机值#2。随机值#2 用于确定 ProSe 密钥，以便远端终端在确定认证通过的情况下，可以直接根据随机值#2 推演 ProSe 密钥，保证为远端 UE 的不同 ProSe 通信推演不同的密钥，实现密钥的隔离。

进一步地，认证响应消息#2 还可以包括如下至少一项：远端终端的用户隐藏标识 SUPI、或 EAP 成功消息。其中，EAP 成功消息可以用于指示网络认证远端终端成功。该远端终端的 SUPI 可以用于指示中继终端需要向网络上报远端 UE 的信息。

一种可能的设计方案中，认证服务网元跳过推演用于远端终端与网络之间通信的密钥，以防止生成冗余的信息，造成资源的浪费。

可选地，认证请求消息#1 可以包括如下至少一项：远端终端的 SUCI、或 ProSe 中继通信指示信息。ProSe 中继通信指示信息用于指示认证为 ProSe 中继通信的认证，以触发数据管理网元发选择 ProSe 中继通信对应的认证向量，确保 ProSe 中继通信认证的可靠性。

第二方面，提供一种通信方法。该通信方法包括：接入和移动管理网元向认证服务网元发送认证请求消息#3，并接收来自认证服务网元的认证响应消息#3。认证响应消息#3 包括：ProSe 认证信息#2，ProSe 认证信息#2 包括：用于远端终端认证网络的信息。可选地，ProSe 认证信息#2 还可以包括：用于网络认证远端终端的信息。如

此，在远端终端认证网络通过的情况下，接入和移动管理网元向认证服务网元发送认证请求消息#2，并在认证远端终端通过的情况下，接收来自认证服务网元的认证响应消息#2，以向中继终端发送 ProSe 密钥。其中，认证请求消息#2 用于请求认证远端终端。认证响应消息#2 包括：ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，ProSe 认证信息#2 可以为如下至少一项：AKA 的 ProSe 认证向量#2、或 EAP 请求消息或 AKA’挑战消息。

可选地，AKA 的 ProSe 认证向量#2 可包括如下至少一项：用于远端终端认证网络的信息、或用于接入和移动管理网元认证远端终端的信息。

可选地，EAP 请求消息或 AKA’挑战消息可包括：用于远端终端认证网络的信息。

一种可能的设计方案中，在接入和移动管理网元接收来自认证服务网元的认证响应消息#3 之后，在接入和移动管理网元向认证服务网元发送认证请求消息#2 之前，第二方面所述的方法还可以包括：接入和移动管理网元向中继终端发送用于远端终端认证网络的信息，接收来自中继终端的远端终端确定的认证响应信息，认证响应信息用于认证远端终端。其中，用于远端终端认证网络的信息可以用于指示中继终端向远端终端转发 ProSe 中继通信的认证数据，即用于远端终端认证网络的信息，避免中继终端执行其他操作，例如自行认证，确保 ProSe 中继通信认证的可靠性。

一种可能的设计方案中，在接入和移动管理网元向中继终端发送用于远端终端认证网络的信息之前，接入和移动管理网元跳过获取密钥集标识和反降级参数。或者接入和移动管理网元跳过生成密钥集标识和反降级参数。

可选地，在 ProSe 认证信息#2 可以包括：用于接入和移动管理网元认证远端终端的信息的情况下，在接入和移动管理网元接收来自中继终端的远端终端认证响应消息之后，在接入和移动管理网元向认证服务网元发送认证请求消息#2 之前，第二方面所述方法还可以包括：接入和移动管理网元根据远端终端确定的认证响应消息，以及用于接入和移动管理网元认证远端终端的信息，确定远端终端认证通过。

可选地，用于远端终端认证网络的信息和远端终端确定的认证响应信息为通过通信密钥保护的信息，通信密钥用于中继终端与网络的通信，以确保中继终端与网络之间的通信安全。例如，通信密钥为中继终端与接入和移动管理网元之间建立的非接入层安全密钥，该非接入层安全密钥可以包含加密密钥和完整性保护密钥。

可选地，认证请求消息#2 可以包括如下至少一项：远端终端确定的认证响应消息、用于确定 ProSe 密钥的 RSC、或用于确定 ProSe 密钥的随机值#1。该认证响应消息用于认证远端终端。

可选地，认证响应消息#2 可以包括：随机值#2，随机值#2 用于确定 ProSe 密钥。

进一步的，认证响应消息#2 还可以包括如下至少一项：远端终端的 SUPI、或 EAP 成功消息。

进一步的，在接入和移动管理网元接收来自认证服务网元的认证响应消息#2 之后，第二方面所述的方法还可以包括：接入和移动管理网元向中继终端发送随机值

#2。也就是说，接入和移动管理网元可以在网络认证远端终端通过后，才向远端终端发送用于推演 ProSe 密钥的参数，也即随机值#2，从而实现按需提供必要的参数，无需预存信息，防止资源浪费。

一种可能的设计方案中，在接入和移动管理网元向认证服务网元发送认证请求消息#3 之前，第二方面所述的方法还可以包括：接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥（如 KAUSF）。换言之，只有在远端终端没有执行过认证的情况下或不存在用于推演 ProSe 密钥的密钥，才执行 ProSe 中继通信的认证流程，避免因重复执行认证流程而导致资源浪费。当然，在对远端终端执行过认证的情况下，可使用认证服务网元上已有的密钥（如 KAUSF）推演 ProSe 密钥，无需再次执行 ProSe 中继通信认证。

可选地，接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥，可以包括：接入和移动管理网元接收来自中继终端的远端终端指示信息，远端终端指示信息用于指示远端终端未执行认证或不存在用于推演 ProSe 密钥的密钥。接入和移动管理网元根据远端终端指示信息，确定未对远端终端执行过 ProSe 中继通信的认证。

可选地，接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥，可以包括：接入和移动管理网元向数据管理网元发送认证服务网元获得请求消息，并接收来自数据管理网元的认证服务网元获得响应消息。其中，认证服务网元获得请求消息用于请求认证服务网元的标识，该认证服务网元用于远端终端的 ProSe 中继通信认证。认证服务网元获得响应消息未携带该认证服务网元的标识，用以表示未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥。接入和移动管理网元根据认证服务网元获得响应消息，确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥。

可以看出，在远端终端指示其是否执行过认证的情况下或不存在用于推演 ProSe 密钥的密钥，接入和移动管理网元可根据远端终端的指示信息，而不用再与其他网元交互，便可确定是否执行 ProSe 中继通信的认证。或者，远端终端可以不指示其是否执行过 ProSe 中继通信的认证，由接入和移动管理网元根据数据管理网元反馈的信息确定，如此可以降低远端终端与接入和移动管理网元之间的通信开销，提高通信效率。

此外，第二方面所述的方法的其他技术效果可以参考第一方面所述的方法中的技术效果，不再赘述。

第三方面，提供一种通信方法。该通信方法包括：数据管理网元接收来自认证服务网元的认证请求消息#1，并向认证服务网元发送认证响应消息#1。认证响应消息#1 包括：ProSe 认证信息#1。ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。

一种可能的设计方案中，ProSe 认证信息#1 可以为如下至少一项：AKA 的 ProSe 认证向量#1、或 EAP-AKA’的 ProSe 的认证向量。

可选地，AKA 的 ProSe 认证向量#1 或 EAP-AKA’的 ProSe 的认证向量可以包括如下至少一项：用于远端终端认证网络的信息、用于认证服务网元认证远端终端的信

息、或用于确定 ProSe 密钥的信息。

可选地，在数据管理网元接收来自认证服务网元的认证请求消息#1 之前，第三方面所述的方法还可以包括：数据管理网元接收来自接入和移动管理网元的认证服务网元获得请求消息， 并向接入和移动管理网元发送认证服务网元获得响应消息。其中，认证服务网元获得请求消息用于请求认证服务网元的标识，该认证服务网元用于远端终端的 ProSe 中继通信认证。认证服务网元获得响应消息未携带该认证服务网元的标识，用以表示未对远端终端执行过 ProSe 中继通信的认证。

一种可能的设计方案中，在数据管理网元向认证服务网元发送认证响应消息#1 之前，第三方面所述的方法还可以包括：数据管理网元确定远端终端授权获取中继服务。也就是说，在确定远端终端有中继通信的权限的基础上，才对其进行 ProSe 中继通信认证，避免无效认证。

一种可能的设计方案中，在数据管理网元向认证服务网元发送认证响应消息#1 之前，第三方面所述的方法还可以包括：数据管理网元根据认证请求消息#1，确定 ProSe 认证信息#1。

一种可能的设计方案中，在数据管理网元向认证服务网元发送认证响应消息#1 之前，第三方面所述的方法还可以包括：数据管理网元确定未对远端终端执行过认证，或确定不存在用于推演 ProSe 密钥的密钥，或确定不存在为远端终端服务的 AUSF 网元。换言之，只有在远端终端没有执行过认证，或不存在用于推演 ProSe 密钥的密钥，或不存在为远端终端服务的 AUSF 网元的情况下，才执行 ProSe 中继通信的认证流程，避免因重复执行认证流程而导致资源浪费。当然，在对远端终端执行过认证的情况下，数据管理网元可以请求认证服务网元使用已有的密钥（如 KAUSF）推演 ProSe 密钥，无需再次执行 ProSe 中继通信认证。

此外，第三方面所述的方法的其他技术效果，可以参考第一方面或第二方面所述的方法中的技术效果，不再赘述。

第四方面，提供一种通信方法。该通信方法包括：中继终端接收来自接入和移动管理网元的用于远端终端认证网络的信息，并向接入和移动管理网元发送远端终端确定的认证响应信息。远端终端确定的认证响应信息用于认证远端终端。如此，中继终端接收来自接入和移动管理网元的 ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，用于远端终端认证网络的信息和远端终端确定的认证响应信息为通过通信密钥保护的消息，通信密钥用于中继终端与网络的通信。例如，通信密钥为中继终端与接入和移动管理网之间建立的非接入层安全密钥，该非接入层安全密钥可以包含加密密钥和完整性保护密钥。

一种可能的设计方案中，在中继终端接收来自接入和移动管理网元的用于远端终端认证网络的信息之后，在中继终端向接入和移动管理网元发送远端终端确定的认证响应信息之前，第四方面所述的方法还可以包括：中继终端向远端终端发送用于远端终端认证网络的信息，并接收来自远端终端的远端终端确定的认证响应信息。也就是说，中继终端可以主动与远端终端交互，以确保远端终端能够认证网络，并向网络反馈自身的认证响应消息，确保网络也能够认证远端终端。

可选地，用于远端终端认证网络的信息承载在消息中，该消息的名称或携带的指示信息，可以指示需要由远端终端执行 ProSe 中继通信的认证流程或指示请求认证远端 UE。如此，中继终端向远端终端发送用于远端终端认证网络的信息，可以包括：中继终端根据消息，向远端终端发送用于远端终端认证网络的信息，以确保 ProSe 中继通信认证的可靠性。例如，中继终端根据该消息的名称或消息中包含的指示信息，向远端终端发送用于远端终端认证网络的信息。

一种可能的设计方案中，在中继终端向接入和移动管理网元发送的 ProSe 通信认证响应消息之后，第四方面所述的方法还可以包括：中继终端接收来自接入和移动管理网元的随机值#2，并向远端终端发送随机值#2。随机值#2 用于确定 ProSe 密钥。

此外，第四方面所述的方法的其他技术效果，可以参考第一方面或第二方面所述的方法中的技术效果，不再赘述。

第五方面，提供一种通信方法。该通信方法包括：远端终端接收来自中继终端的用于远端终端认证网络的信息。如此，在远端终端确定认证网络通过的情况下，远端终端向中继终端发送远端终端确定的认证响应信息，该认证响应信息用于认证远端终端。

一种可能的设计方案中，在远端终端向中继终端发送远端终端确定的认证响应信息之后，方法还包括：远端终端接收来自中继终端的随机值#2，以根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密钥，确定 ProSe 密钥，该 ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，在远端终端向中继终端发送远端终端确定的认证响应信息之后，方法还包括：远端终端跳过推演用于远端终端与网络通信的密钥，如跳过 KSEAF 的推演。

此外，第五方面所述的方法的其他技术效果，可以参考第一方面或第二方面所述的方法中的技术效果，不再赘述。

第六方面，提供一种通信装置。该通信装置包括：用于执行第一方面所述的通信方法的模块，例如接收模块和发送模块。

可选地，发送模块和接收模块也可以集成为一个模块，如收发模块。其中，收发模块用于实现第六方面所述的通信装置的发送功能和接收功能。

可选地，第六方面所述的通信装置还可以包括处理模块。其中，处理模块用于实现该通信装置的处理功能。

可选地，第六方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第一方面所述的通信方法。

需要说明的是，第六方面所述的通信装置可以是网络设备，例如认证服务网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，第六方面所述的通信装置的技术效果可以参考第一方面所述的通信方法的技术效果，此处不再赘述。

第七方面，提供一种通信装置。该通信装置包括：用于执行第二方面所述的通信

方法的模块，例如接收模块和发送模块。

可选地，发送模块和接收模块也可以集成为一个模块，如收发模块。其中，收发模块用于实现第七方面所述的通信装置的发送功能和接收功能。

可选地，第七方面所述的通信装置还可以包括处理模块。其中，处理模块用于实现该通信装置的处理功能。

可选地，第七方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第二方面所述的通信方法。

需要说明的是，第七方面所述的通信装置可以是网络设备，例如接入和移动管理网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，第七方面所述的通信装置的技术效果可以参考第二方面所述的通信方法的技术效果，此处不再赘述。

第八方面，提供一种通信装置。该通信装置包括：用于执行第三方面所述的通信方法的模块，例如接收模块和发送模块。

可选地，发送模块和接收模块也可以集成为一个模块，如收发模块。其中，收发模块用于实现第八方面所述的通信装置的发送功能和接收功能。

可选地，第八方面所述的通信装置还可以包括处理模块。其中，处理模块用于实现该通信装置的处理功能。

可选地，第八方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第三方面所述的通信方法。

需要说明的是，第八方面所述的通信装置可以是网络设备，例如数据管理网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，第八方面所述的通信装置的技术效果可以参考第三方面所述的通信方法的技术效果，此处不再赘述。

第九方面，提供一种通信装置。该通信装置包括：用于执行第四方面所述的通信方法的模块，例如接收模块和发送模块。

可选地，发送模块和接收模块也可以集成为一个模块，如收发模块。其中，收发模块用于实现第九方面所述的通信装置的发送功能和接收功能。

可选地，第九方面所述的通信装置还可以包括处理模块。其中，处理模块用于实现该通信装置的处理功能。

可选地，第九方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第四方面所述的通信方法。

需要说明的是，第九方面所述的通信装置可以是终端，例如中继终端，也可以是可设置于终端中的芯片（系统）或其他部件或组件，还可以是包含终端的装置，本申请对此不做限定。

此外，第九方面所述的通信装置的技术效果可以参考第四方面所述的通信方法的技术效果，此处不再赘述。

第十方面，提供一种通信装置。该通信装置包括：用于执行第五方面所述的通信方法的模块，例如接收模块和发送模块。

可选地，发送模块和接收模块也可以集成为一个模块，如收发模块。其中，收发模块用于实现第十方面所述的通信装置的发送功能和接收功能。

可选地，第十方面所述的通信装置还可以包括处理模块。其中，处理模块用于实现该通信装置的处理功能。

可选地，第十方面所述的通信装置还可以包括存储模块，该存储模块存储有程序或指令。当该处理模块执行该程序或指令时，使得该通信装置可以执行第五方面所述的通信方法。

需要说明的是，第十方面所述的通信装置可以是终端，例如远端终端，也可以是可设置于终端中的芯片（系统）或其他部件或组件，还可以是包含终端的装置，本申请对此不做限定。

此外，第十方面所述的通信装置的技术效果可以参考第五方面所述的通信方法的技术效果，此处不再赘述。

第十一方面，提供一种通信装置。该通信装置包括：处理器，该处理器用于执行第一方面至第五方面中任意一种可能的实现方式所述的通信方法。

在一种可能的设计方案中，第十一方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第十一方面所述的通信装置与其他通信装置通信。

在一种可能的设计方案中，第十一方面所述的通信装置还可以包括存储器。该存储器可以与处理器集成在一起，也可以分开设置。该存储器可以用于存储第一方面至第五方面中任一方面所述的通信方法所涉及的计算机程序和/或数据。

在本申请中，第十一方面所述的通信装置可以为第一方面、第二方面或第三方面中的网络设备，或第四方面或第五方面中的终端，或者可设置于该终端或网络设备中的芯片（系统）或其他部件或组件，或者包含该终端或网络设备的装置。

此外，第十一方面所述的通信装置的技术效果可以参考第一方面至第五方面中任意一种实现方式所述的通信方法的技术效果，此处不再赘述。

第十二方面，提供一种通信装置。该通信装置包括：处理器，该处理器与存储器耦合，该处理器用于执行存储器中存储的计算机程序，以使得该通信装置执行第一方面至第五方面中任意一种可能的实现方式所述的通信方法。

在一种可能的设计方案中，第十二方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第八方面所述的通信装置与其他通信装置通信。

在本申请中，第十二方面所述的通信装置可以为第一方面、第二方面或第三方面中的网络设备，或第四方面或第五方面中的终端，或者可设置于该终端或网络设备中的芯片（系统）或其他部件或组件，或者包含该终端或网络设备的装置。

此外，第十二方面所述的通信装置的技术效果可以参考第一方面至第五方面中任

意一种实现方式所述的通信方法的技术效果，此处不再赘述。

第十三方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机程序，当该处理器执行该计算机程序时，以使该通信装置执行第一方面至第五方面中的任意一种实现方式所述的通信方法。

在一种可能的设计方案中，第十三方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第十三方面所述的通信装置与其他通信装置通信。

在本申请中，第十三方面所述的通信装置可以为第一方面、第二方面或第三方面中的网络设备，或第四方面或第五方面中的终端，或者可设置于该终端或网络设备中的芯片（系统）或其他部件或组件，或者包含该终端或网络设备的装置。

此外，第十三方面所述的通信装置的技术效果可以参考第一方面至第五方面中任意一种实现方式所述的通信方法的技术效果，此处不再赘述。

第十四方面，提供了一种通信装置，包括：处理器；该处理器用于与存储器耦合，并读取存储器中的计算机程序之后，根据该计算机程序执行如第一方面至第五方面中的任意一种实现方式所述的通信方法。

在一种可能的设计方案中，第十四方面所述的通信装置还可以包括收发器。该收发器可以为收发电路或接口电路。该收发器可以用于第十四方面所述的通信装置与其他通信装置通信。

在本申请中，第十四方面所述的通信装置可以为第一方面、第二方面或第三方面中的网络设备，或第四方面或第五方面中的终端，或者可设置于该终端或网络设备中的芯片（系统）或其他部件或组件，或者包含该终端或网络设备的装置。

此外，第十四方面所述的通信装置的技术效果可以参考第一方面至第五方面中任意一种实现方式所述的通信方法的技术效果，此处不再赘述。

第十五方面，提供一种通信系统。该通信系统包括：第四方面或第五方面所述的一个或多个终端设备，例如中继终端和远程终端，以及第一方面、第二方面或第三方面所述一个或多个网络设备，例如认证服务网络、接入和移动管理网元和数据管理网元。

第十六方面，提供一种计算机可读存储介质，包括：计算机程序或指令；当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第五方面中任意一种可能的实现方式所述的通信方法。

第十七方面，提供一种计算机程序产品，包括计算机程序或指令，当该计算机程序或指令在计算机上运行时，使得该计算机执行第一方面至第五方面中任意一种可能的实现方式所述的通信方法。

附图说明

图 1 为 5G 的架构示意图；

图 2 为层 3 中继架构的架构示意图；

图 3 为层 2 中继架构的架构示意图；

图 4 为 ProSe 通信建立安全连接的流程示意图；

图 5 为主认证流程的流程示意图一；
图 6 为主认证流程的流程示意图二；
图 7 为本申请实施例提供的通信系统的架构示意图；
图 8 为本申请实施例提供的通信方法的流程示意图一；
图 9 为本申请实施例提供的通信方法的流程示意图二；
图 10 为本申请实施例提供的通信方法的流程示意图三；
图 11 为本申请实施例提供的通信方法的流程示意图四；
图 12 为本申请实施例提供的通信方法的流程示意图五；
图 13 为本申请实施例提供的通信方法的流程示意图六；
图 14 为本申请实施例提供的通信方法的流程示意图七；
图 15 为本申请实施例提供的通信装置的结构示意图一；
图 16 为本申请实施例提供的通信装置的结构示意图二。

具体实施方式

方便理解，下面先介绍本申请实施例所涉及的技术术语。

1、第五代（5th generation，5G）移动通信系统：

图 1 为 5G 系统的架构示意图，如图 1 所示，5G 系统包括：接入网（access network，AN）和核心网（core network，CN），还可以包括：终端。

上述终端可以为具有收发功能的终端，或为可设置于该终端的芯片或芯片系统。该终端也可以称为用户设备（uesr equipment，UE）、接入终端、用户单元（subscriber unit）、用户站、移动站（mobile station，MS）、移动台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。本申请的实施例中的终端可以是手机（mobile phone）、蜂窝电话（cellular phone）、智能电话（smart phone）、平板电脑（Pad）、无线数据卡、个人数字助理电脑（personal digital assistant，PDA）、无线调制解调器（modem）、手持设备（handset）、膝上型电脑（laptop computer）、机器类型通信（machine type communication，MTC）终端、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、车载终端、具有终端功能的路边单元（road side unit，RSU）等。本申请的终端还可以是作为一个或多个部件或者单元而内置于车辆的车载模块、车载模组、车载部件、车载芯片或者车载单元。

上述 AN 用于实现接入有关的功能，可以为特定区域的授权用户提供入网功能，并能够根据用户的级别，业务的需求等确定不同质量的传输链路以传输用户数据。AN 在终端与 CN 之间转发控制信号和用户数据。AN 可以包括：接入网设备，也可以称为无线接入网设备（radio access network，RAN）设备。

RAN 设备可以是为终端提供接入的设备，主要负责空口侧的无线资源管理、服

务质量（quality of service，QoS）管理、数据压缩和加密等功能。RAN 设备可以包括 5G，如新空口（new radio，NR）系统中的 gNB，或，5G 中的基站的一个或一组（包括多个天线面板）天线面板，或者，还可以为构成 gNB、传输点（transmission and reception point，TRP 或者 transmission point，TP）或传输测量功能（transmission measurement function，TMF）的网络节点，如基带单元（building base band unit，BBU），或，集中单元（centralized unit，CU）或分布单元（distributed unit，DU）、具有基站功能的 RSU，或者有线接入网关，或者 5G 的核心网网元。或者，RAN 设备还可以包括无线保真（wireless fidelity，WiFi）系统中的接入点（access point，AP），无线中继节点、无线回传节点、各种形式的宏基站、微基站（也称为小站）、中继站、接入点、可穿戴设备、车载设备等等。或者，RAN 设备可以也可以包括下一代移动通信系统，例如 6G 的接入网设备，例如 6G 基站，或者在下一代移动通信系统中，该网络设备也可以有其他命名方式，其均涵盖在本申请实施例的保护范围以内，本申请对此不做任何限定。

CN 主要负责维护移动网络的签约数据，为终端提供会话管理、移动性管理、策略管理以及安全认证等功能。CN 主要包括如下网元：用户面功能（user plane function，UPF）网元、认证服务功能（authentication server function，AUSF）网元、接入和移动性管理功能（access and mobility management function，AMF）网元、会话管理功能（session management function，SMF）网元、网络切片选择功能（network slice selection function，NSSF）网元、网络开放功能（network exposure function，NEF）网元、网络功能仓储功能（NF repository function，NRF）网元、策略控制功能（policy control function，PCF）网元、统一数据管理（unified data management，UDM）网元、应用功能（application function，AF）网元、以及网络切片和独立非公共网络（standalone non-public network，SNPN）的鉴权授权功能（network slice-specific and SNPN authentication and authorization function，NSSAAF）网元。

其中，UPF 网元主要负责用户数据处理（转发、接收、计费等）。例如，UPF 网元可以接收来自数据网络（data network，DN）的用户数据，通过接入网设备向终端转发该用户数据。UPF 网元也可以通过接入网设备接收来自终端的用户数据，并向 DN 转发该用户数据。DN 网元指的是为用户提供数据传输服务的运营商网络。例如网际互连协议（internet protocol，IP）多媒体业务（IP multi-media srvice，IMS）、互联网（internet）等。DN 可以为运营商外部网络，也可以为运营商控制的网络，用于向终端设备提供业务服务。

AUSF 网元可用于执行终端的安全认证。

AMF 网元主要负责移动网络中的移动性管理。例如用户位置更新、用户注册网络、用户切换等。

SMF 网元主要负责移动网络中的会话管理。例如会话建立、修改、释放。具体功能例如为用户分配互联网协议（internet protocol，IP）地址，选择提供报文转发功能的 UPF 等。

PCF 网元主要支持提供统一的策略框架来控制网络行为，提供策略规则给控制层网络功能，同时负责获取与策略决策相关的用户签约信息。PCF 网元可以向 AMF 网

元、SMF 网元提供策略，例如服务质量（quality of service，QoS）策略、切片选择策略等。

NSSF 网元可用于为终端选择网络切片。

NEF 网元可用于支持能力和事件的开放。

UDM 网元可用于存储用户数据，例如签约数据、鉴权/授权数据等。

AF 网元主要支持与 CN 交互来提供服务，例如影响数据路由决策、策略控制功能或者向网络侧提供第三方的一些服务。

NSSAAF 网元可用于支持切片认证和授权，以及支持使用凭据持有者的凭据访问独立非公共网络。NSSAAF 网元可以通过认证、授权和计费代理（authentication，authorization，and accounting proxy，AAA-P）与认证、授权和计费服务器（authentication，authorization，and accounting server，AAA-S）交互。

SCP（Service Communication Proxy，服务通信代理）网元可用于实现网络功能之间的通信转发，还可以用于实现负载均衡和网络功能选择等。

2、近距离通信：

随着移动通信的高速发展，新业务类型，如视频聊天、虚拟现实（virtual reality，VR）/增强现实（augmented AR）等数据业务的普遍应用，提高了用户对带宽的需求。对此，近距离通信，例如设备到设备（device-to-device，D2D）通信是一种解决方案。

D2D 通信允许 UE 之间直接进行通信，例如通过 PC5 接口进行通信，实现数据面和控制面的信息传输。这样，用户在小区（cell）网络的控制下便可与其他小区用户共享频谱资源，有效提高频谱资源的利用率。D2D 通信包括：一对多通信（one to many communication），以及一对一通信（One to one communication）。一对多通信通常对应于组播和广播通信，一对一通信通常对应于单播通信。在一对一通信中，若发送方 UE 与接收方 UE 在近距离范围内，通过相互发现后可以直接通信。

3、临近业务（proximity based services，ProSe）通信：

ProSe 通信又称为近距离业务通信，是 D2D 通信中的一种典型业务场景。ProSe 通信可以包含临近业务直接通信、临近业务 UE 到网络中继通信。针对临近业务 UE 到网络中继通信（可简称 ProSe 中继通信），在某个 UE（记为 UE1）处于网络覆盖之外、或与 RAN 设备间的通信信号不好、或需要其他 UE（记为 UE2）协助传输数据的情况下，UE1 可以通过 UE2 的辅助，从网络获取业务。此时，UE1 可称为临近业务远端 UE（ProSe remote UE），或者 5G 临近业务远端 UE（5G ProSe remote UE），或者简称为远端 UE（remote UE）。UE2 可为称为临近业务 UE 到网络中继（ProSe UE-to-network relay），或者 5G 临近业务 UE 到网络中继（5G ProSe UE-to-network relay），或者简称为中继 UE（relay UE）。中继 UE 可用于提供支持远端 UE 连接到网络的 ProSe 功能，以便远端 UE 可通过中继 UE 提供的 ProSe 功能与 DN 通信，即 ProSe 中继通信。

为支持 ProSe 功能，第三代合作伙伴计划（3rd generation partnership project，3GPP）引入了层 3 中继架构和层 2 中继架构。下面分别介绍。

图 2 为层 3 中继架构的架构示意图。如图 2 所示，远端 UE 与中继 UE 建立 PC5

连接，中继 UE 通过 RAN 设备接入核心网（5GC）。这样，远端 UE 通过 PC5 连接，以及中继 UE 接入的核心网，从 DN 获得业务，实现 ProSe 通信。例如，中继 UE 可以建立或修改针对于远端 UE 的协议数据单元（protocol data unit，PDU）会话，并通知 SMF 网元将远端 UE 的相关信息存储在会话管理（session management，SM）上下文中。这样，远端 UE 便能够通过中继 UE 的 PDU 会话从 DN 获得业务，实现 ProSe 通信。或者，中继 UE 也可以建立或修改针对于远端 UE 的 PDU 会话，以便远端 UE 可通过该 PDU 会话进行密钥交换协议（internet key exchange, IKE）流程与非 3GPP 互通功能（non-3GPP interworking function, N3IWF）建立信令的互联网安全协议（internet protocol security，IPsec）隧道，并执行非接入层（non-access stratum，NAS）注册流程。这样，远端 UE 便能够通过中继 UE 建立的 PDU 会话和 N3IWF 建立远端 UE 的 PDU 会话，并从 DN 获得业务，实现 ProSe 中继通信。此外，中继 UE 可以位于家乡公共陆地移动网（public land mobile network，PLMN），也可以位于拜访 PLMN，对此不做具体限定。

图 3 为层 2 中继架构的架构示意图。如图 3 所示，远端 UE 与中继 UE 建立 PC5 连接，中继 UE 与 RAN 设备建立 Uu 口连接。RAN 设备可以与远端 UE 接入的核心网连接，以及也可以与中继 UE 接入的核心网连接。这种情况下，远端 UE 与中继 UE 建立 PC5 连接后，远端 UE 通过建立的 PC5 连接与 RAN 建立无线资源连接，进一步与核心网建立非接入层（non-stradum, NAS）连接，从而可以建立 PDU 会话，从 DN 获取业务，实现 ProSe 中继通信。例如，远端 UE 可通过中继 UE 接入网络并建立或修改远端 UE 自身的 PDU 会话，以通过该 PDU 会话从 DN 获得业务，实现 ProSe 中继通信。此外，远端 UE 接入的核心网与中继 UE 接入的核心网可以是相同的 PLMN，或者不同的 PLMN，对此不做具体限定。

需要说明的是，在层 2 中继架构中，远端 UE 可以称为 5G ProSe 层 2 远端 UE 、ProSe 层 2 远端 UE 、或层 2 远端 UE。类似的，在层 3 中继架构中，远端 UE 可以称为 5G ProSe 层 3 远端 UE、ProSe 层 3 远端 UE、或层 3 远端 UE。下文提到的远端 UE 可以理解为层 2 中继架构或层 3 中继架构中的远端 UE，其命名也可以相应替换。同理，在层 2 中继架构中，中继 UE 可以称为 5G ProSe 层 2 中继 UE、ProSe 层 2 中继 UE、或层 2 中继 UE。类似的，在层 3 中继架构中，中继 UE 可以称为 5G ProSe 层 3 中继 UE、ProSe 层 3 中继 UE 、或层 3 中继 UE。在没有特别说明的情况下，下文提到的中继 UE 可以理解为层 2 中继架构或层 3 中继架构中的中继 UE，其命名也可以相应替换。

4、ProSe 中继通信的安全：

为确保 ProSe 中继通信的安全，远端 UE 与中继 UE 之间应当建立安全的 PC5 连接。图 4 为建立安全的 ProSe 中继通信的流程示意图，如图 4 所示，该流程包括如下步骤：

S401，远端 UE 注册到网络，并与网络之间执行认证和授权。

S402，中继 UE 注册到网络，并与网络之间执行认证和授权。

需要指出的是，远端 UE 可以通过服务远端 UE 的 AMF 网元（记为远端 AMF 网元）注册到网络。中继 UE 可以通过服务中继 UE 的 AMF 网元（记为中继 AMF 网

元）注册到网络。远端 AMF 网元与中继 AMF 网元可以是相同的网元，或者不同的网元，对此不做具体限定。

S403，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，则通过执行中继发现流程来发现中继 UE。

S404，远端 UE 向中继 UE 发送直接通信请求（direct communication request）消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信。直接通信请求消息可包括远端 UE 的如下参数：安全能力、安全策略、用户隐藏标识（subscription concealed identifier，SUCI）、中继通信码（relay service code，RSC）、以及 Nonce_1。其中，安全能力用于指示远端 UE 支持的加密和/或完整性保护算法。安全策略用于指示是否开启安全保护，其中安全保护包含加密保护和/或完整性保护示。例如安全策略可以包含加密为必须的或推荐的或不需要的；和/或完整性保护为必须的，或推荐的或不需要的。RSC 用于标识中继 UE 可为远端 UE 提供的一个连接服务。Nonce_1 为由远端 UE 生成的随机数，用于推演远端 UE 和中继 UE 之间安全通信的密钥 K_{NR_ProSc}。远端 UE 和中继 UE 基于 K_{NR_ProSc} 生成用于通信的安全密钥，如加密密钥和/或完整性密钥。

S405，中继 UE 向中继 AMF 网元发送中继密钥请求（relay key request）消息。相应的，中继 AMF 网元接收来自中继 UE 向的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信，或者说请求 ProSe 通信的密钥。中继密钥请求消息可以包括：中继 UE 的标识、远端 UE 的 SUCI、RSC、以及 Nonce_1。

S406，中继 AMF 网元验证中继 UE。

中继 AMF 网元根据中继 UE 的标识验证中继 UE，以确定中继 UE 授权作为中继提供服务。

S407，中继 AMF 网元向远端 AUSF 网元发送 UE 认证请求（Kausf_UEAuthentication_Authenticate Request）消息。相应的，远端 AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息。

其中，UE 认证请求消息可以包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S408，远端 AUSF 网元执行 UE 认证获得（Nudm_UEAuthentication_Get）流程。

远端 AUSF 网元可以根据 UE 认证请求消息，执行 UE 认证获得流程，以从远端 UDM 网元获得认证向量。远端 UDM 网元可以是服务远端 UE 的 UDM 网元。

S409，远端 AUSF 网元执行针对远端 UE 的主认证流程（Primary authentication of Remote UE）。

S410，远端 UE 确定 5GPRUK 和 5GPRUK ID。

远端 UE 通过主认证流程认证网络通过后，可以确定 5GPRUK 和 5GPRUK ID。例如，远端 UE 可根据主认证流程中推演得到的密钥，例如 K_{AUSF} 推演得到 5GPRUK 和 5GPRUK ID。5GPRUK 用于推演远端 UE 和中继 UE 之间安全通信的密钥。5GPRUK ID 用于定位 5GPRUK。

S411，远端 AUSF 网元确定 5GPRUK 和 5GPRUK ID。

远端 AUSF 网元通过主认证流程认证远端 UE 通过后，也可以确定 5GPRUK 和 5GPRUK ID。例如，远端 AUSF 网元也可根据主认证流程中推演得到的密钥，例如 K_{AUSF} 推演得到 5GPRUK 和 5GPRUK ID。此外，S411 与 S410 的执行顺序不限定。

S412，远端 AUSF 网元推演 K_{NR_ProSe}。

远端 AUSF 网元通过主认证流程认证远端 UE 通过后，可根据 5GPRUK、Nonce_1 和 Nonce_2 推演 K_{NR_ProSe}。Nonce_2 为由远端 AUSF 网元生成的随机数。

S413，远端 AUSF 网元向中继 AMF 网元发送 UE 认证响应（Nausf_UEAuthentication_Authenticate response）消息。相应的，中继 AMF 网元接收来自远端 AUSF 网元的 UE 认证响应消息。

UE 认证响应消息为 UE 认证请求消息的响应消息，用于指示 ProSe 通信认证通过。UE 认证响应消息可以包括：K_{NR_ProSe}、5GPRUK ID、以及 Nonce_2。

S414，中继 AMF 网元向中继 UE 发送中继密钥响应（Relay Key Response）消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

其中，中继密钥响应消息主要用于为中继 UE 配置 K_{NR_ProSe}。中继密钥响应消息可以包括：K_{NR_ProSe}、5GPRUK ID、以及 Nonce_2。

S415，中继 UE 向远端 UE 发送直接安全模式命令（direct security mode commend）消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

直接安全模式命令消息用于指示远端 UE 确定 K_{NR_ProSe}。直接安全模式命令消息可以包括：5GPRUK ID、以及 Nonce_2。

S416，远端 UE 推演 K_{NR_ProSe}。

远端 UE 在接收到直接安全模式命令消息后，可以根据 5GPRUK ID 定位用于建立 PC5 连接的 5GPRUK，从而根据 5GPRUK、Nonce_1 和 Nonce_2 推演 K_{NR_ProSe}。

S417，远端 UE 向中继 UE 发送直接安全模式命令完成（direct security mode commend complete）消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令完成消息。

可以看出，3GPP 大致定义了 ProSe 通信的安全流程，即需要通过主认证流程来对 ProSe 通信进行认证，并在认证通过后推演 K_{NR_ProSe}，以确保 ProSe 通信安全。方便理解，下面介绍主认证流程。

图 5 为 3GPP 中主认证流程的流程示意图一，如图 5 所示，该流程包括如下步骤：

S501，UE 向安全锚点功能（security anchor function，SEAF）发送 N1 消息。相应的，SEAF 接收来自 UE 的 N1 消息。

SEAF 可以部署在 AMF 网元或者其他任何可能的网元上，或者独立部署，对此不做具体限定。N1 消息可以是注册请求（register request）消息，用于 UE 请求注册到网络。N1 消息中可以包括：UE 的标识，例如，SUCI，或者 5G-全球唯一临时 UE 标识（globally unique temporary UE identity，GUTI）。

S502，SEAF 向 AUSF 网元发送 UE 认证请求（Nausf_UEAuthentication_Authenticate Request）消息。相应的，AUSF 网元接收来

自 SEAF 的 UE 认证请求消息。

UE 认证请求消息用于请求 AUSF 网元执行认证流程。UE 认证请求消息中可以包括： SUCI 或用户永久标识（subscription permanent identifier，SUPI）、服务网络名称（service network name，SN-name）。

其中，SEAF 接收到 N1 消息后，可确定 5G-GUTI 有效，且需要重新认证 UE。那么，SEAF 应当在 UE 认证请求消息中携带 SUPI，否则应当携带 SUCI。

S503，AUSF 网元向 UDM 网元发送 UE 认证获得请求（Nudm_UEAuthentication_Get Request）消息。相应的，UDM 网元接收来自 AUSF 网元 UE 认证获得请求消息。

UE 认证获得请求消息用于请求 UDM 网元生成认证向量，以便后续认证使用。UE 认证获得请求消息中可以包括：SUCI 或 SUPI、服务网络名称。

其中，AUSF 网元接收到 UE 认证请求消息后，可验证服务网络名称，例如将 UE 认证请求消息中携带的服务网络名称与预期的服务网络名称比较。如果 UE 认证请求消息中携带的服务网络名称与预期的服务网络名称匹配，则 AUSF 网元确定 SEAF 有权使用该服务网络名称，向 UDM 网元发送 UE 认证获得请求消息。如果 UE 认证请求消息中携带的服务网络名称与预期的服务网络名称不匹配，则 AUSF 网元确定 SEAF 无权使用该服务网络名称，流程结束，并向 SEAF 发送消息，用以指示该服务网络未授权。

S504，UDM 网元选择认证方式。

如果 UE 认证获得请求消息中携带的是 SUCI，则 UDM 网元可以调用用户隐藏标识解密功能（subscription identifier de-concealing function，SIDF）解析 SUCI，获得 SUPI。UDM 网元，或者 UDM 网元可以调用认证凭证存储和处理功能（authentication credential repository and processing function，ARPF）根据 SUPI 选择签约用户数据里支持的认证方法。该流程中 UDM 网元/ARPF 确定选择 5G 认证与密钥协商（authentication and key agreement，AKA）机制。

S505，UDM 网元生成认证向量。

UDM 网元/ARPF 可以生成 5G AKA 机制对应的认证向量，例如 5G 家乡环境认证向量（5G home environment authentication vector，5G HE AV）。认证向量可以包括：随机数（RAND）、认证令牌（authentication token，AUTN）、XRES*和 K_{AUSF}。其中，RAND 和 AUTN 用于 UE 认证网络。XRES*可用于 AUSF 网元认证 UE。K_{AUSF} 可用于保护发送给的 UE 的信息，还可用于密钥推演，以获得后续用于通信的密钥，例如 K_{AMF}。XRES*和 K_{AUSF} 可由根密钥和 RAND 推演得到。

具体的，UDM 网元/ARPF 可以生成一些参数，包括：消息验证码（MAC）、期待的响应（XRES）、加密密钥（CK）、完整性密钥（IK）、以及匿名密钥（AK）。MAC 由序列号（SQN）、RAND、AMF 和根密钥经 f1 算法计算得到。XRES 由 RAND 和根密钥经算法 f2 计算得到。CK 由根密钥和 RAND 经 f3 算法计算得到。IK 由根密钥和 RAND 经 f4 算法计算得到。AK 由根密钥和 RAND 经 f5 算法计算得到。在此基础上，UDM 网元/ARPF 可以得到 AUTN，AUTN 包括：AK 与 SQN 异或（SQN 异或 AK）与 AMF 和 MAC 串联{AUTN=SQN ⊕ AK || AMF ||

MAC}。UDM 网元/ARPF 可以根据 XRES 和 RAND 推演 XRES*,推演的过程中还使用下面参数，如服务网络名称、服务网络名称的长度，RAND 的长度。UDM 网元/ARPF 还可以根据 IK 和 CK 推演 K_{AUSF}。至此，认证向量包含的参数均被推演出，也即生成认证向量。

S506，UDM 网元向 AUSF 网元发送 UE 认证获得响应（Nudm_UEAuthentication_Get Response）消息。相应的，AUSF 网元接收来自 UDM 网元的 UE 认证获得响应消息。

其中，UE 认证获得响应消息为上述 UE 认证获得请求消息的响应消息。UE 认证获得响应消息中可以包括：认证向量和指示信息，该指示信息用以指示该认证向量用于 5G AKA。可选地，如果 UE 认证获得请求消息中携带的是 SUCI，则 UE 认证获得响应消息中还可以包括：SUPI。

S507，AUSF 网元储存 XRES*，推演 HXRES*以及 K_{SEAF}。

AUSF 网元接收到 UE 认证获得响应消息后，可储存 XRES*，或者 XRES*和 SUPI，以便后续认证使用。AUSF 网元可根据 XRES*推演 HXRES*，该 HXRES*可用于 SEAF 认证 UE。AUSF 网元还可根据 K_{AUSF} 推演 K_{SEAF}，该 K_{SEAF} 可用于 SEAF 的密钥推演，以获得 K_{AMF}。

S508，AUSF 网元向 SEAF 发送 UE 认证响应（Nausf_UEAuthentication_Authenticate Response）消息。相应的，SEAF 接收来自 AUSF 网元的 UE 认证响应消息。

UE 认证响应消息为上述 UE 认证请求消息的响应消息。UE 认证响应消息中可以包括：认证向量，例如 5G 服务环境认证向量(5G serving environment authentication vector，5G SE AV)。认证向量可以包括：RAND、AUTN、以及 HXRES*。也就是说，AUSF 网元将认证向量中的 XRES*替换为 HXRES*，并移除认证向量中的 KAUSF，得到认证向量。

S509，SEAF 向 UE 发送认证请求（authenticate request）消息。相应的，UE 接收来自 SEAF 的认证请求消息。

认证请求消息可以是 NAS 消息，用于请求 UE 认证网络。认证请求消息可以包括：RAND、AUTN、5G 密钥集标识（key set identifier in 5G，ngKSI）、以及不同架构之间的反降级（anti-bidding down between architectures，ABBA）参数。ngKSI 可以由 SEAF 确定，用于 UE 和 AMF 网元标识 KAMF 和部分原生安全上下文。ABBA 参数可以由 SEAF 确定，用于推演 K_{AMF}。

S510，UE 推演 RES*。

RES*用于认证 UE。

其中，UE 可以包括：移动设备（mobile equipment，ME）和全球用户识别卡（universal subscriber identity module，USIM）。UE 接收到认证请求消息后，USIM 可根据 RAND 和自身的根密钥，验证 AUTN。如果 USIM 验证 AUTN 失败，则表示 UE 认证网络失败，流程结束。如果 USIM 验证 AUTN 通过，则表示 UE 认证网络通过。在此基础上，USIM 可以利用根密钥和 RAND 推演 RES、以及 CK 和 IK，并向 ME 发送 RES、以及 CK 和 IK。ME 可以根据 CK 和 IK 推演 K_{AUSF}，再根据 K_{AUSF} 推

演 K_{SEAF}。ME 还可以根据 RES 推演 RES*，然后执行 S511。

S511，UE 向 SEAF 发送认证响应（authenticate response）消息。相应的，SEAF 接收来自 UE 的认证响应消息。

认证响应消息可以是 NAS 消息，用于响应上述认证请求消息。认证响应消息中可以包括：RES*。

S512，SEAF 认证 UE。

SEAF 接收到认证响应消息后，可根据 RES*推演 HRES*，以比较 HRES*和先前获得的 HXRES*。如果 HRES*和 HXRES*不匹配，则表示认证 UE 失败，认证流程结束。如果 HRES*和 HXRES*匹配，则表示认证 UE 通过，或者说从服务网的角度认为认证通过，然后执行 S513。

S513，SEAF 向 AUSF 网元发送 UE 认证请求消息。相应的，AUSF 网元接收来自 SEAF 的 UE 认证请求消息。

UE 认证请求消息用于请求认证 UE。UE 认证请求消息中可以包括：RES*。

S514，AUSF 网元认证 UE。

AUSF 网元接收到 UE 认证请求消息后，可比较 RES*与先前保存的 XRES*。如果 RES*和 XRES*不匹配，则表示认证 UE 失败，流程结束。如果 RES*和 XRES*匹配，则表示认证 UE 通过，或者说从归属网的角度认为认证通过，然后执行 S515。AUSF 网元还可以根据本地网络运营商的策略确定存储 K_{AUSF}。

S515，AUSF 网元向 SEAF 发送 UE 认证响应消息。相应的，SEAF 接收来自 AUSF 网元的 UE 认证响应消息。

UE 认证响应消息为 UE 认证请求消息的响应消息，用于指示认证 UE 通过。UE 认证响应消息中可以包括：K_{SEAF}。可选地，如果 UE 认证请求消息中携带的是 SUCI，则 UE 认证响应消息中还可以包括：SUPI。其中，SEAF 接收到 UE 认证响应消息后，可根据 K_{SEAF}、ABBA 参数、以及 SUPI，推演 K_{AMF}，并向 AMF 网元发送 ngKSI 和 K_{AMF}。

如果 UE 认证请求消息中携带的是 SUCI，即 SUCI 用于此认证，则 SEAF 应当在接收到 UE 认证响应消息后，即包含 SUPI 的 UE 认证响应消息，才向 AMF 网元提供 ngKSI 和 K_{AMF}，以便在此之前，服务网不会为 UE 提供通信服务。

另外，UE 在确定认证通过后，也可根据 K_{SEAF}、ABBA 参数、以及 SUPI 自行推演 K_{AMF}。至此，UE 和 AMF 网元都获得了相同的密钥，即 K_{AMF}，双方可使用该密钥进一步推演加密密钥和/或完整性保护密钥，并使用推演的密钥用对 UE 与 AMF 网元之间的信息进行安全保护，保证通信安全。

图 6 为 3GPP 中主认证流程的流程示意图二，如图 6 所示，该流程包括如下步骤：

S601，UE 向 SEAF 发送 N1 消息。相应的，SEAF 接收来自 UE 的 N1 消息。

S602，SEAF 向 AUSF 网元发送 UE 认证请求消息。相应的，AUSF 网元接收来自 SEAF 的 UE 认证请求消息。

S603，AUSF 网元向 UDM 网元发送 UE 认证获得请求消息。相应的，UDM 网元接收来自 AUSF 网元 UE 认证获得请求消息。

其中，S601-S603 的具体实现原理与上述 S501-S503 类似，可参考理解，不再赘述。

S604，UDM 网元选择认证方式。

如果 UE 认证请求消息中携带的是 SUCI，则 UDM 网元可以调用 SIDF 解析 SUCI，获得 SUPI。UDM 网元，或者 UDM 网元可以调用 ARPF 根据 SUPI 选择签约用户数据里支持的认证方法。该流程中 UDM 网元/ARPF 确定选择扩展认证协议（extensible authentication protocol，EAP）-AKA’机制。

S605，UDM 网元生成认证向量。

UDM 网元/ARPF 可以生成 EAP-AKA’机制对应的认证向量，例如转换的认证向量 AV’(transformed authentication vector)。认证向量可以包括：RAND、AUTN、XRES、以及 CK’和 IK’。其中，RAND、AUTN 和 XRES 的具体实现原理可以参考上述 S505 中的相关介绍，不再赘述。CK’和 IK’可由根密钥和 RAND 推演得到。例如，UDM 网元/ARPF 推演出 CK 和 IK，再根据 CK 和 IK 推演 CK’和 IK’。 CK 和 IK 的具体实现原理可以参考上述 S505 中的相关介绍，不再赘述。

S606，UDM 网元向 AUSF 网元发送 UE 认证获得响应消息。相应的，AUSF 网元接收来自 UDM 网元的 UE 认证获得响应消息。

其中，UE 认证获得响应消息用于响应上述 UE 认证获得请求消息。UE 认证获得响应消息中可以包括：认证向量和指示信息，该指示信息用以指示该认证向量用于 EAP-AKA’。可选地，如果 UE 认证获得请求消息中携带的是 SUCI，则 UE 认证获得响应消息中还可以包括：SUPI。

S607，AUSF 网元向 SEAF 发送 UE 认证响应消息。相应的，SEAF 接收来自 AUSF 网元的 UE 认证响应消息。

UE 认证响应消息用于响应上述 UE 认证请求消息。UE 认证响应消息中可以包括：EAP 请求（EAP-Request）消息/ AKA’挑战（AKA'-Challenge）消息。EAP 请求消息/ AKA’挑战消息可以是根据 UE 认证获得响应消息确定的，消息中包括：RAND 和 AUTN。

S608，SEAF 向 UE 发送认证请求消息。相应的，UE 接收来自 SEAF 的认证请求消息。

认证请求消息可以是 NAS 消息，用于请求 UE 认证网络。认证请求消息中可以包括：EAP 请求消息/ AKA’挑战消息。也就是说，SEAF 接收到 UE 认证响应消息后，可以将 UE 认证响应消息中的 EAP 请求消息/ AKA’挑战消息继续封装到认证请求消息中，以向 UE 透传该 EAP 请求消息/ AKA’挑战消息。此外，SEAF 的认证请求消息中还可以包括：ngKSI、以及 ABBA 参数。ngKSI 和 ABBA 参数的具体实现原理与上述 S509 中类似，可参考理解，不再赘述。此外，在 EAP-AKA’认证过程中，SEAF 向 UE 发送的 ngKSI 值和 ABBA 参数不能更改。

S609，UE 推演 RES。

RES 用于认证 UE。

UE 可以包括： ME 和 USIM。UE 接收到认证请求消息后，USIM 可根据 RAND 和自身的根密钥，验证 AUTN。如果 USIM 验证 AUTN 失败，则表示 UE 认证网络失

败，认证流程结束。如果 USIM 验证 AUTN 通过，则表示 UE 认证网络通过。在此基础上，USIM 可以利用根密钥和 RAND，推演 RES、以及 CK 和 IK，并向 ME 发送 RES、以及 CK 和 IK。ME 可以根据 CK 和 IK 推演 CK'和 IK'。

S610，UE 向 SEAF 发送认证响应消息。相应的，SEAF 接收来自 UE 的认证响应消息。

认证响应消息可以是 NAS 消息，用于响应上述认证请求消息。认证响应消息中可以包括：EAP 响应（EAP-response）消息/ AKA'挑战消息。EAP 响应消息/ AKA'挑战消息中可以包括：RES。

S611，SEAF 向 AUSF 网元发送 UE 认证请求消息。相应的，AUSF 网元接收来自 SEAF 的 UE 认证请求消息。

UE 认证请求消息用于请求认证 UE。UE 认证请求消息中可以包括：EAP 响应消息/ AKA'挑战消息。也就是说，SEAF 接收到认证响应消息后，可以将认证响应消息中的 EAP 响应消息/ AKA'挑战消息继续封装到 UE 认证请求消息中，以向 AUSF 网元透传该 EAP 响应消息/ AKA'挑战消息。

S612，AUSF 网元认证 UE。

AUSF 网元接收到 UE 认证请求消息后，可将 EAP 响应消息/ AKA'挑战消息中的 RES 与本地保存的 XRES 比较。如果 RES 和 XRES 不匹配，则表示认证 UE 失败，认证流程结束。如果 RES 和 XRES 匹配，则表示认证 UE 通过，然后执行 S614。

S613，AUSF 网元向 SEAF 发送 UE 认证响应消息。相应的，SEAF 接收来自 AUSF 网元的 UE 认证响应消息。

UE 认证响应消息为 UE 认证请求消息的响应消息。UE 认证响应消息中可以包括：EAP 成功（EAP success）消息，用以指示认证通过，以及还可以包括：K_{SEAF}。可选地，如果 UE 认证请求消息中携带的是 SUCI，则 UE 认证响应消息中还可以包括：SUPI。可以理解，AUSF 网元确定认证通过后，可根据 CK'和 IK'推演 EMSK，根据 EMSK 确定 K_{SEAF}，具体的，AUSF 网元确定 EMSK 的前 256 位作为 K_{AUSF}，然后根据 K_{AUSF} 推演 K_{SEAF}。相应的，SEAF 接收到 UE 认证响应消息后，可根据 K_{SEAF}、ABBA 参数、以及 SUPI，推演 K_{AMF}，并向 AMF 网元发送 ngKSI 和 K_{AMF}。

需要指出的是，如果 UE 认证请求消息中携带的是 SUCI，即 SUCI 用于认证，则 SEAF 应当在接收到 UE 认证响应消息后，即包含 SUPI 的 UE 认证响应消息，才向 AMF 网元提供 ngKSI 和 K_{AMF}，以便在此之前，服务网不会为 UE 提供通信服务。

S614，SEAF 向 UE 发送 N1 消息。相应的，UE 接收来自 SEAF 的 N1 消息。

N1 消息中可以包括：EAP 成功消息、ngKSI 和 ABBA 参数。这样，UE 在确定认证通过后，也可根据 K_{SEAF}、ABBA 参数、以及 SUPI 自行推演 K_{AMF}。至此，UE 和 AMF 网元都获得了相同的密钥，即 K_{AMF}，双方可使用该密钥进一步推演加密密钥和/或完整性保护密钥，并使用推演的密钥用对 UE 与 AMF 网元之间的信息进行安全保护，保证通信安全。

如图 5 和图 6 所示，以上介绍了目前 3GPP 定义的主认证流程。该主认证流程主要定义了 UE 和网络如何执行认证并建立相同的密钥，如 K_{AMF}。如图 4 基于主认证流程的 ProSe 中继通信流程，有两个 UE，包括：远端 UE 和中继 UE。这种情况下，

AUSF 网元使用主认证流程认证 ProSe 中继通信场景下的远端 UE，根据现有流程 AUSF 网络在认证过程中可以为远端 UE 存储 K_{AUSF}，推演用于 UE 和网络安全通信的 K_{SEAF}。但在中继通信场景下，远端 UE 并不会与中继 AMF 网元建立非接入层连接，也不会通过中继 AMF 网元注册到网络，因此无需建立 UE 与网络之间的安全上下文。并且中继通信场景下，需要建立的是远端 UE 和中继 UE 的安全通信，即需要为中继 UE 推演需要的密钥，现有认证流程无法支持 AUSF 网元实现该功能。此外，中继通信场景下，远端 UE 与网络之间的认证流程是通过中继 UE 和中继 AMF 执行，在中继 UE 接收到认证请求时，根据现有的流程，中继 UE 会解析认证请求，并执行网络验证，由于认证参数是基于远端 UE 的根密钥确定，中继 UE 验证网络会失败，导致流程终结，导致无法建立通信连接。

综上，针对上述技术问题，本申请实施例提出了如下技术方案，用以实现建立安全的 ProSe 中继通信。下面将结合附图，对本申请中的技术方案进行描述。

本申请实施例的技术方案可以应用于各种通信系统，例如无线保真（wireless fidelity， WiFi）系统，车到任意物体（vehicle to everything，V2X）通信系统、设备间（device-todevie，D2D）通信系统、车联网通信系统、第 4 代（4th generation，4G）移动通信系统，如长期演进（long term evolution，LTE）系统、全球互联微波接入（worldwide interoperability for microwave access，WiMAX）通信系统、第五代（5th generation，5G）移动通信系统，如新空口（new radio，NR）系统，以及未来的通信系统，如第六代（6th generation，6G）移动通信系统等。

本申请将围绕可包括多个设备、组件、模块等的系统来呈现各个方面、实施例或特征。应当理解和明白的是，各个系统可以包括另外的设备、组件、模块等，并且/或者可以并不包括结合附图讨论的所有设备、组件、模块等。此外，还可以使用这些方案的组合。

另外，在本申请实施例中，“示例的”、“例如”等词用于表示作例子、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。

本申请实施例中，“信息（information）”，“信号（signal）”，“消息（message）”，“信道（channel）”、“信令（singaling）”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匹配的。“的（of）”，“相应的（corrEAPonding，relevant）”和“对应的（corrEAPonding）”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匹配的。此外，本申请提到的“/”可以用于表示“或”的关系。

本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

为便于理解本申请实施例，首先以图 7 中示出的通信系统为例详细说明适用于本申请实施例的通信系统。示例性的，图 7 为本申请实施例提供的通信方法所适用的一

种通信系统的架构示意图。

如图 7 所示，该通信系统可以适用于上述 5G 架构下的中继架构（层 2 中继架构或者层 3 中继架构），主要包括：远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元。其中，远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元的相关功能，可以参考上述 1、5G 移动通信系统、2、近距离通信、以及 3、ProSe 通信中的相关介绍，不再赘述。在本申请实施例的通信系统中，远端 UE 通过中继 UE 接入后，可触发 AUSF 网元对远端 UE 进行认证并建立安全通信。

下面将结合图 8-图 14，通过方法实施例具体介绍远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的交互流程。为方便理解，下面先介绍本申请实施例主要所涉及的一些信元，如下表 1 所示。

表 1

信元名称	信元功能
远端 UE 的 SUCI	可用于标识远端 UE，选择 AUSF 网元
中继 UE 的 5G GUTI	可用于标识中继 UE
Nonce_1	远端 UE 确定的随机值，可用于指示认证为 ProSe 中继通信的认证，还可用于推演 ProSe 密钥
RSC	可用于指示认证为 ProSe 中继通信的认证，还可用于推演 ProSe 密钥
服务网络名称	可用于指示认证为 ProSe 中继通信的认证，还可用于推演 ProSe 密钥
Nonce_2	AUSF 网元确定的随机值，可用于推演 ProSe 密钥
K_{AUSF}	AUSF 网元或 UDM 网元或 ARPF 确定的密钥，可用于推演 ProSe 密钥
IK 和 CK	UDM 网元确定的密钥，可用于推演 ProSe 密钥
IK'和 CK'	UDM 网元确定的密钥，可用于推演 ProSe 密钥
RAND	由 UDM 网元或 ARPF 推演得到，可用于远端 UE 认证网络
AUTN	由 UDM 网元或 ARPF 推演得到，可用于远端 UE 认证网络
期望响应（expected response，XRES）	由 UDM 网元或 ARPF 推演得到，可用于 AUSF 网元认证远端 UE
响应（response，RES）	由远端 UE 推演得到，可用于 AUSF 网元认证远端 UE
XRES*	由 UDM 网元或 ARPF 根据 XRES 推演得到，可用于 AUSF 网元认证远端 UE
哈希期望响应（hash expected response，HXRES）*	由 AUSF 网元根据 XRES*推演得到，可用于中继 AMF 网元认证远端 UE

RES*	由远端 UE 推演得到，可用于 AUSF 网元认证远端 UE
哈希响应（hash response，HRES）*	由中继 AMF 网元或 SEAF 根据 RES*推演得到，可用于中继 AMF 网元认证远端 UE

下面介绍本申请实施例所应用的各种场景。

场景 1：

示例性的，图 8 为本申请实施例提供的通信方法的流程示意图一。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以是远端 AUSF 网元，如 AUSF 网元是根据远端 UE 的标识确定的，用于支持对远端 UE 的认证，或者也可以其他任何可能形态的 AUSF 网元，对此不做具体限定。UDM 网元可以是远端 UDM 网元， 如该 UDM 网元是根据远端 UE 的标识确定的，用于为远端 UE 生成认证向量，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 1 中，UDM 根据来自的 AUSF 网元的请求确定基于 5G AKA 建立安全的 ProSe 中继通信（也可以称为 ProSe 中继通信的 5G AKA 流程，简称 5G ProSe AKA）。在增强的 5G AKA 的认证流程中，AMF 网元、AUSF 网元与 UDM 网元之间可通过使用已经服务操作（即 service operation）进行交互。

具体的，如图 8 所示，该通信方法的流程如下：

S801，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S802，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，ProSe 通信策略信息用于支持 UE 执行 ProSe 直接发现、建立 ProSe 直接通信、执行 ProSe 中继 UE 发现、建立中继通信连接中的一个或多个服务。S801 为可选步骤，即在执行中继通信流程中之前，远端 UE 可以执行 S801，获得 ProSe 通信策略信息，并基于该 ProSe 通信策略信息执行中继发现和建立直接通信连接。或者，在执行中继通信流程中之前，远端 UE 未接入网络获取 ProSe 通信策略信息，则远端 UE 基于本地预配置的 ProSe 通信策略信息执行中继发现和建立直接通信连接。

S803，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

S804，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S805，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信的密钥，或者说请求 ProSe 中继通信的密钥，请求包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选的，中继密钥请求消息中还可以包括：中继 UE 的标识，如 5G GUTI。

S806，中继 AMF 网元验证中继 UE。

具体的，中继 AMF 网元可根据来自 UDM 网元的中继 UE 的签约信息，判断中继 UE 是否授权作为中继提供服务。

其中，S803-S806 的具体实现原理与上述 S403-S406 类似，可参考理解，不再赘述。

S807，中继 AMF 网元向 AUSF 网元发送 UE 认证请求消息#1。相应的，AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息#1。

中继 AMF 网元可根据远端 UE 的 SUCI 选择 AUSF 网元，如中继 AMF 网元与 NRF 网元交互确定服务的 AUSF 网元，或者根据本地存储的 AUSF 网元信息确定服务的 AUSF 网元。如此，中继 AMF 网元可根据来自中继 UE 的中继密钥请求消息，确定向被选中的 AUSF 网元发送 UE 认证请求消息#1。例如，中继 AMF 网元可以根据消息名称，确定向 AUSF 网元发送 UE 认证请求消息#1。

UE 认证请求消息#1 可以为 Kausf_UEAuthentication_Authenticate Request 消息。UE 认证请求消息#1 可以用于请求触发建立 ProSe 中继通信安全的认证流程（简称为触发 ProSe 认证），以保证 AUSF 推演用于保护中继通信安全的密钥，避免 AUSF 执行错误的流程。该 ProSe 的认证用于远端 UE 通过中继 UE 与网络执行双向认证，并建立远端 UE 和中继 UE 之间安全通信的密钥。UE 认证请求消息#1 包含远端 UE 的 SUCI，服务网络名称，还可以包括如下至少一项： RSC、Nonce_1 或 ProSe 中继通信指示信息#1（例如，ProSe ind）。RSC 或 Nonce_1 或 ProSe 中继通信指示信息#1 或者服务网络名称都可用于指示请求的是 ProSe 认证，或者说指示认证用于认证远端 UE。也就是说，UE 认证请求消息#1 可以通过其携带的信元来指示请求触发 ProSe 认证。该信元可以是新的信元或者已有信元，针对已有信元，可以通过使用新的值来指示。

具体的，一种可能的方式中，UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、服务网络名称、以及 ProSe 中继通信指示信息#1，以通过 ProSe 中继通信指示信息#1 其用于请求或者说用于触发 ProSe 认证。在此基础上，中继 AMF 网元可以在后续确定远端 UE 认证通过的情况下，再向 AUSF 网元发送 RSC 和 Nonce_1，以使 AUSF 网元推演中继通信密钥，例如 ProSe 密钥。

或者，另一种可能的方式中，UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、RSC、Nonce_1、以及服务网络名称，以通过 RSC 和/或 Nonce_1 指示其用于请求 ProSe 认证。

或者，又一种可能的方式中，UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、服务网络名称、RSC、Nonce_1、以及 ProSe 中继通信指示信息#1，以通过显示的 ProSe 中继通信指示信息#1 请求 ProSe 认证。

上述三种可能的方式中，服务网络名称可以为 5G:SN ID 或 5G:ProSe 或者 5G:ProSe||SN ID。

或者，再一种可能的方式中，UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、服务网络名称、RSC、Nonce_1。服务网络名称设置为 5G:ProSe5G 或者 ProSe||SN ID，AUSF 网元可根据该特定的服务网络名称确定为 ProSe 认证。

或者，还一种可能的方式中，UE 认证请求消息#1 中可以包括：远端 UE 的

SUCI、服务网络名称。服务网络名称设置为 5G:ProSe 或 5G:ProSe||SN ID，AUSF 网元可根据该特定的服务网络名称确定为 ProSe 认证。这种方式中，中继 AMF 网元在接收到下述的 ProSe 通信认证响应消息后，再向 AUSF 网元发送 RSC 和 Nonce_1，以使 AUSF 网元推演 ProSe 密钥。

此外，若 AUSF 网元接收了来自 AMF 网元的 RSC 和 Nonce_1，则 AUSF 保存 RSC 和 Nonce_1，用于后续 ProSe 密钥推演。

可以理解，上述通过 SN 名的设置来指示的认证方式仅为一些示例，其具体的实现方式不限，下文中的相关介绍也可以参考理解，不再赘述。

S808，AUSF 网元向 UDM 网元发送 UE 认证获得请求消息。相应的，UDM 网元接收来自 AUSF 网元的 UE 认证获得请求消息。

AUSF 网元可以根据 UE 认证请求消息#1，向 UDM 网元发送 UE 认证获得请求消息。UE 认证获得请求消息可以为 Nudm_UEAuthentication_Request 请求消息。UE 认证获得请求消息可用于请求 ProSe 认证的数据。UE 认证获得请求消息中可以包括：远端 UE 的 SUCI、服务网络名称。

若 UE 认证请求消息#1 包括：远端 UE 的 SUCI、服务网络名称、以及 ProSe 中继通信指示信息#1，则 UE 认证获得请求消息还可以包含：ProSe 中继通信指示信息#2。ProSe 中继通信指示信息#2 用于请求 ProSe 认证的数据，或者说指示获取用于认证远端 UE 的认证数据。也即，UE 认证获得请求消息可以通过其携带显示的信元，例如 ProSe 中继通信指示信息#2，指示其用于请求 ProSe 认证的数据。其中，AUSF 网元可复用该 ProSe 中继通信指示信息#1，将其封装到 UE 认证获得请求消息中。此时，ProSe 中继通信指示信息#1 与 ProSe 中继通信指示信息#2 可以为同一指示信息。或者，AUSF 网元也可根据 UE 认证请求消息#1 中的 ProSe 中继通信指示信息#1，生成 ProSe 中继通信指示信息#2。此时，ProSe 中继通信指示信息#1 与 ProSe 中继通信指示信息#2 可以为不同的指示信息。

若 UE 认证请求消息#1 包括：远端 UE 的 SUCI、RSC、Nonce_1、以及服务网络名称，则 UE 认证获得请求消息还可以包含：RSC，Nonce_1、或 ProSe 中继通信指示信息#2。其中，RSC，Nonce_1 或 ProSe 中继通信指示信息#2 用于获取 ProSe 认证的数据，或者说用于获取认证远端 UE 的认证数据。

若 UE 认证请求消息#1 包括：远端 UE 的 SUCI、服务网络名称、RSC、Nonce_1、以及 ProSe 中继通信指示信息#1，则 UE 认证获得请求消息还可以包含：RSC，Nonce_1 或 ProSe 中继通信指示信息#2。其中，RSC，Nonce_1 或 ProSe 中继通信指示信息#2 用于获取 ProSe 认证的数据，或者说用于获取认证远端 UE 的认证数据。

若 UE 认证请求消息#1 包括：远端 UE 的 SUCI、服务网络名称、RSC、Nonce_1，服务网络名称设置为 5G:ProSe 或 5G:ProSe||SN ID，AUSF 网元根据该特定的服务网络名称确定为 ProSe 认证，则 UE 认证获得请求消息还可以包含：RSC，Nonce_1。此时，服务网络名称用于指示获取 ProSe 认证的数据，或者用于指示获取认证远端 UE 的认证数据。

若 UE 认证请求消息#1 包括：远端 UE 的 SUCI、服务网络名称，服务网络名称

设置为 5G:ProSe 或 5G:ProSe||SN ID，AUSF 根据该特定的服务网络名称确定为 ProSe 认证，则服务网络名称用于指示获取 ProSe 认证的数据，或者用于指示获取认证远端 UE 的认证数据。

可以理解，上述 UE 认证请求消息#1 中包括的各种参数组合仅为示例，不作为限定，其他组合也可以参考理解，不再赘述。

S809，UDM 网元生成 ProSe 中继通信的认证向量。

UDM 网元接收到 UE 认证获得请求消息后，可根据 ProSe 中继通信指示信息#2、或 RSC、或服务网络名称，确定获取 ProSe 认证的数据。

具体的，UDM 网元，或者 UDM 网元可以调用 SIDF，解析 SIDF 解析 SUCI 获取 SUPI。UDM 网元可以根据 SUPI 对应的签约用户数据和请求消息，确定 ProSe 中继通信的认证机制，例如确定使用 ProSe 中继通信的 5G AKA，也即 5G ProSe AKA。如此，UDM 网元可以生成 ProSe 中继通信的认证向量，例如，5G ProSe AKA 的认证向量#1（5G ProSe AKA HE AV）。5G ProSe AKA 的认证向量#1 可以包括：RAND、AUTN、XRES*、以及 K_{AUSF}。RAND 和 AUTN 可以由 UDM 网元确定，用于远端 UE 认证网络。其中 XRES*可由 UDM 网元或 ARPF 根据 XRES 推演得到，用于 AUSF 网元认证远端 UE。XRES 可由 UDM 网元或 ARPF 根据根密钥（K）和 RAND 推演得到。K_{AUSF} 由 UDM 网元或 ARPF 根据 IK、CK 和服务网络名称推演得到，用于推演 ProSe 密钥。

可以理解，上述介绍了 5G ProSe AKA 的认证向量#1 的一些实现方式，5G ProSe AKA 的认证向量#1 还可以替换为其他任何的可能的实现方式。例如，5G ProSe AKA 的认证向量#1 包括：RAND、AUTN、XRES 以及 K_{PROSE}。其中，XRES 仍可由 UDM 网元或 ARPF 根据根密钥和 RAND 推演得到。K_{PROSE} 可由 UDM 网元或 ARPF 根据 IK、CK、服务网络名称和字符串（PROSE）推演得到，用于推演 ProSe 密钥。或者，UDM 网元或 ARPF 先推演得到 K_{AUSF}，再根据 K_{AUSF} 推演 K_{PROSE}，具体的推演方法不限制。又例如，5G ProSe AKA 的认证向量#1 包括：RAND、AUTN、XRES*以及 K_{PROSE}。

可选地，UDM 网元确定 ProSe 中继通信的认证机制也可以为：如果 UE 认证获得请求消息中携带有新的信元（如 ProSe 中继通信指示信息#2 或 RSC），则 UDM 网元确定使用 5G ProSeAKA。或者通过携带新的 SN 名，如 5G：PROSE 或 5G:ProSe||SN ID，使得 UDM 网元确定使用 5G ProSe AKA。

可选地，在确定执行 ProSe 认证基础上，UDM 网元可以根据 SUPI 对应的签约用户数据，判断用户是否授权使用中继通信。如果确定用户授权使用中继通信，则授权检查通过，流程继续。否则，UDM 网元向 AUSF 网元发送用于指示认证失败的响应消息，流程结束。可以理解，UDM 网元执行判断用户是否授权使用中继通信的流程，与上述 UDM 网元执行确定 ProSe 中继通信的认证机制的流程之间的顺序可以不限定。

需要指出的是，ProSe 中继通信的 5G AKA 仅为本申请实施例中的一种示例性命名方式，其也可以替换为其他任何可能的命名方式，例如 5G ProSe 中继通信的 AKA、或 5G ProSe AKA 等，对此不做任何限定。同理，5G AKA 的 ProSe 认证向量

#1 也仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 5G AKA ProSe 认证向量#1、5G ProSe AKA 认证向量#1、或 5G ProSe AKA 的认证向量#1 等，对此不做任何限定。

S810，UDM 网元向 AUSF 网元发送 UE 认证获得响应消息。相应的，UDM 网元接收来自 AUSF 网元的 UE 认证获得响应消息。

UE 认证获得响应消息可以用于响应上述 UE 认证获得请求消息。UE 认证获得响应消息中可以包括：5G ProSe AKA 的认证向量#1，可选地，还可以包括：SUPI。UE 认证获得响应消息还可以指示：该 5G ProSe AKA 的认证向量#1 为用于 ProSe 中继通信的认证向量。例如，在 UE 认证获得响应消息已有指示信息指示认证向量用于 5G AKA 的基础上，可在 UE 认证获得响应消息中新增指示信息，用以指示 5G AKA 支持 ProSe 中继通信。或者，在 UE 认证获得响应消息中新增指示信息，用以指示认证向量用于 5G ProSe 认证和密钥管理。即认证向量用于远端 UE 与网络之间执行双向认证，以及建立远端 UE 和中继 UE 之间安全通信的密钥。

S811，AUSF 网元储存 XRES*，推演 HXRES*。

AUSF 网元接收到 UE 认证获得响应消息后，可储存 XRES*，可选地，还存储 SUPI。

一种可能的实现方式中，AUSF 网元可根据 XRES*推演 HXRES*，该 HXRES*可用于中继 AMF 网元认证远端 UE。在 ProSe 中继通信认证流程中，AUSF 网元不推演 K_{SEAF}，以防止生成冗余的信息，造成资源的浪费。

或者，另一种可能的实现方式中，AUSF 网元可以不推演 HXRES*，下述 S812 中发送给中继 AMF 网元的认证向量中可包含 AUTN 和 RAND，不包含 HXRES*，使得中继 AMF 网元后续可以不执行服务网的认证流程。或者，若来自 UDM 网元的认证向量中包含 XRES，下述 S812 中向中继 AMF 网元发送的认证向量中也可包含 AUTN 和 RAND，不包含 HXRES，使得中继 AMF 网元后续可以不执行服务网的认证流程。此处不限制。

可以理解，上述两种实现方式都可以防止网元资源的浪费。

S812，AUSF 网元向中继 AMF 网元发送 UE 认证响应消息#1。相应的，中继 AMF 网元接收来自 AUSF 网元的 UE 认证响应消息#1。

UE 认证响应消息#1 为上述 UE 认证请求消息#1 的响应消息。UE 认证响应消息#1 中可以包括：5G AKA 的 ProSe 认证向量#2（5G ProSe AKA SE AV）。5G AKA 的 ProSe 认证向量#1 可以包括：RAND、AUTN、以及 HXRES*。也就是说，AUSF 网元可以将 5G AKA 的 ProSe 认证向量#1 中的 XRES*替换为 HXRES*，以及移除 5G AKA 的 ProSe 认证向量#1 中的 K_{AUSF}，得到 5G AKA 的 ProSe 认证向量#2。

此外，根据上述 S811 中的介绍，一种可能的实现方式中，5G AKA 的 ProSe 认证向量#2 可以包括：RAND 和 AUTN，不包括：HXRES 或 HXRES*。

可选地，UE 认证响应消息#1 中也可以包括：指示信息，用以指示认证向量用于认证远端 UE。

需要指出的是，5G AKA 的 ProSe 认证向量#2 也仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 5G AKA ProSe 认证

向量#2、5G ProSe AKA 认证向量#2、或 5G ProSe AKA 的认证向量#2 等，对此不做任何限定。

S813，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息。相应的，中继 UE 接收来自中继 AMF 网元的 ProSe 通信认证请求消息。

ProSe 通信认证请求消息可用于指示对远端 UE 认证，或者说指示中继 UE 向远端 UE 发送认证数据，以避免中继 UE 接收到 ProSe 通信认证请求消息后自行执行认证，防止认证失败，无法建立通信连接。ProSe 通信认证请求消息可以通过其消息类型或其携带的指示信息进行指示。当然，也可通过已有消息（如认证请求消息）携带指示信息指示中继 UE 向远端 UE 发送认证数据，或指示对远端 UE 进行认证，此处不限制。ProSe 通信认证请求消息中可以包括：RAND 和 AUTN（认证数据），也即中继 AMF 网元可以从 5G ProSe AKA 的认证向量#2 中获得的 RAND 和 AUTN，并将其封装到 ProSe 通信认证请求消息中。RAND 和 AUTN 用于远端 UE 认证网络。

可选地，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息前，中继 AMF 跳过获取 ngKSI 和 ABBA 参数。或者，中继 AMF 网元跳过生成 ngKSI 和 ABBA 参数。中继 AMF 网元不向中继 UE 发送 ngKSI 和 ABBA 参数，也即 ProSe 通信认证请求消息不包含 ngKSI 和 ABBA 参数。

需要指出的是，ProSe 通信认证请求消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 ProSe 认证请求消息、远端 UE ProSe 认证请求消息、或已有的认证请求等等。此外，S813 的具体实现也可以是在已有消息中引入新的容器信元，容器中包含 RAND 和 AUTN。若中继 UE 接收到包含该容器的消息，则执行 S814。

S814，中继 UE 向远端 UE 发送远端 UE 认证请求消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证请求消息。

远端 UE 认证请求消息可用于指示认证远端 UE，或者说指示远端 UE 执行 ProSe 认证，确保远端 UE 与网络执行认证并推演 ProSe 密钥，建立远端 UE 和中继 UE 之间的安全通信。例如，远端 UE 认证请求消息可以通过其消息类型，或其携带的指示信息，指示远端 UE 执行 ProSe 认证。当然，也可通过已有消息携带指示信息来指示认证远端 UE，或者说指示远端 UE 执行 ProSe 认证，此处不限制。远端 UE 认证请求消息中可以包括：RAND 和 AUTN。也就是说，中继 UE 接收到 ProSe 通信认证请求消息后，可将 ProSe 通信认证请求消息携带的 RAND 和 AUTN，继续封装到远端 UE 认证请求消息中，以便远端 UE 认证使用。

需要指出的是，远端 UE 认证请求消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如远端 UE ProSe 通信认证请求消息、或远端 UE ProSe 认证请求消息等等。此外，若中继 UE 接收的为上述容器，则直接向远端 UE 转发该容器。

S815，远端 UE 推演 RES*。

其中，该 RES*可用于认证远端 UE。

远端 UE 可以包括：ME 和 USIM。远端 UE 接收到远端 UE 认证请求消息后，USIM 可根据 RAND 和自身的根密钥，验证 AUTN。如果 USIM 验证 AUTN 失败，

则表示 UE 认证网络失败，流程结束。如果 USIM 验证 AUTN 通过，则表示 UE 认证网络通过。在 UE 认证网络通过后，USIM 可以利用根密钥和 RAND 推演 RES、以及 CK 和 IK，并向 ME 发送 RES、以及 CK 和 IK。ME 可以根据 CK 和 IK 推演 K_{AUSF}，以及根据 RES 推演 RES*，然后执行 S816。在 ProSe 认证中，ME 可以不推演 K_{SEAF}，以提高认证效率。

需要说明的是，如上述 S809 和 S811 中的相关介绍可知，若网络侧使用新的密钥推演方法或新的认证参数的推演方法，则远端 UE 也使用和网络侧相同的方法执行密钥推演或认证参数推演，以及其他认证数据的生成。

S816，远端 UE 向中继 UE 发送远端 UE 认证响应消息。相应的，中继 UE 接收来自远端 UE 的远端 UE 认证响应消息。

远端 UE 认证响应消息为远端 UE 认证请求消息的响应消息。可选地，ProSe 通信认证响应消息可用于指示其为远端 UE 的认证响应消息，例如可以通过消息的类型或消息中包含的信元指示且为远端 UE 的认证响应消息。远端 UE 认证响应消息中可以包括：RES*。

需要指出的是，远端 UE 认证响应消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如远端 UE ProSe 通信认证响应消息、或远端 UE ProSe 认证响应消息等等。

S817，中继 UE 向中继 AMF 网元发送 ProSe 通信认证响应消息。相应的，中继 AMF 网元接收来自中继 UE 的 ProSe 通信认证响应消息。

ProSe 通信认证响应消息为上述 ProSe 通信认证请求消息的响应消息。ProSe 通信认证响应消息中可以包括：RES*。也就是说，中继 UE 可以从远端 UE 认证响应消息中获得 RES*，将其继续封装到 ProSe 通信认证响应消息中。

需要指出的是，ProSe 通信认证响应消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 ProSe 认证响应消息、或远端 UE ProSe 认证响应消息等等。

S818，中继 AMF 网元认证远端 UE。

中继 AMF 网元接收到 ProSe 通信认证响应消息后，可根据接收到的 RES*推演 HRES*，以比较 HRES*和 S812 获得的 HXRES*。如果 HRES*和 HXRES*不匹配，例如 HRES*和 HXRES*不相同，则表示认证远端 UE 失败，认证流程结束。如果 HRES*和 HXRES*匹配，例如 HRES*和 HXRES*相同，则表示认证 UE 通过，或者说从服务网的角度认为认证通过，然后执行 S819。

可以理解，若 S811 不推演 HXRES*，则中继 AMF 网元无需推演 HRES*，也无需执行服务网的认证。

S819，中继 AMF 网元向 AUSF 网元发送 UE 认证请求消息#2。相应的，AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息#2。

UE 认证请求消息#2 可用于请求对远端 UE 进行 ProSe 认证。例如，UE 认证请求消息#2 可以通过新的指示信息指示对远端 UE 进行认证。UE 认证请求消息#2 中可以包括：RES*。也就是说，中继 AMF 网元在认证远端 UE 通过后，可将 RES*封装到 UE 认证请求消息#2 中，然后向 AUSF 网元发送 UE 认证请求消息#2。可选地，如果

S807 中的 UE 认证请求消息#1 未携带 RSC 和 Nonce_1，则 UE 认证请求消息#2 中还可以包括：RSC 和 Nonce_1，即中继 AMF 网元还可以将 RSC 和 Nonce_1 封装到 UE 认证请求消息#2 中。或者，在 S807 中的 UE 认证请求消息#1 携带 RSC 和 Nonce_1 的情况下，UE 认证请求消息#2 中仍可以包括：RSC 和 Nonce_1。此时，RSC 和 Nonce_1 也可以用于指示对远端 UE 进行认证。

S820，AUSF 网元认证远端 UE。

AUSF 网元接收到 UE 认证请求消息#2 后，可比较 RES*与先前保存的 XRES*。如果 RES*和 XRES*不匹配，例如 RES*和 XRES*不相同，则表示认证远端 UE 失败，流程结束。如果 RES*和 XRES*匹配，例如 RES*和 XRES*相同，则表示认证远端 UE 通过，或者说从归属网的角度认为认证通过。在此基础上，AUSF 网元可以生成 Nonce_2，根据先前保存的 K_{AUSF}、RSC、Nonce_1 和 Nonce_2，推演 ProSe 密钥（K_{NR_ProSe}），用于远端 UE 与中继 UE 的通信使用。例如，AUSF 网元可以先根据 K_{AUSF} 和 RSC 推演一个中间密钥，再根据中间密钥、Nonce_1 和 Nonce_2 推演 ProSe 密钥。或者，AUSF 网元可以直接根据 K_{AUSF}、RSC、Nonce_1 以及 Nonce_2，推演 ProSe 密钥。或者，AUSF 网元还可以采用其他任何可能的方式推演 ProSe 密钥，对此不做具体限定。

可选地，AUSF 网元认证远端 UE 通过后，AUSF 网元可以根据认证为 ProSe 认证，确定跳过向 UDM 网元发送认证结果的流程，即不向 UDM 网元发送认证结果，而执行下述 S821，以向中继 AMF 网元发送 UE 认证响应消息#2，从而保证仅执行必要的流程，防止资源浪费。

可选地，在确定认证远端 UE 的情况下，AUSF 网元执行上述 ProSe 密钥推演的过程。

需要指出的是，ProSe 密钥仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 ProSe 通信密钥。此外，如果上述 5G AKA 的 ProSe 认证向量#1 中的密钥为 K_{PROSE}，则 AUSF 网元应当使用 K_{PROSE} 来推演 ProSe 密钥，即 K_{AUSF} 替换为 K_{PROSE}。

S821，AUSF 网元向中继 AMF 网元发送 UE 认证响应消息#2。相应的，中继 AMF 网元接收来自 AUSF 网元的 UE 认证响应消息#2。

UE 认证响应消息#2 为 UE 认证请求消息#2 的响应消息，可用于指示认证远端 UE 通过。UE 认证响应消息#2 中可以包括：ProSe 密钥和 Nonce_2。也就是说，AUSF 网元确定远端 UE 认证通过后，可将 ProSe 密钥和 Nonce_2 封装到 UE 认证响应消息#2 中，然后向中继 AMF 网元发送 UE 认证响应消息#2。

可选地，UE 认证响应消息#2 中还可以包括：远端 UE 的 SUPI。该远端 UE 的 SUPI 可用于指示中继 UE 向网络侧上报执行远端 UE 的信息。

S822，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

中继密钥响应消息为上述中继密钥请求消息的响应消息，可以包括：ProSe 密钥和 Nonce_2，可选地，还可以包括：远端 UE 的 SUPI。也就是说，中继 AMF 网元接收到 UE 认证响应消息#2 后，可根据 UE 认证响应消息#2，获得 ProSe 密钥和

Nonce_2，可选地，还可以获得远端 UE 的 SUPI，并将其封装到中继密钥响应消息中，以向中继 UE 发送中继密钥响应消息。相应的，中继 UE 可以存储 ProSe 密钥，可选地，还可以存储远端 UE 的 SUPI。

S823，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

直接安全模式命令消息可用于指示建立 PC5 安全。直接安全模式命令消息中可以包括：Nonce_2。也就是说，中继 UE 接收到中继密钥响应消息后，可从中获得 Nonce_2，然后将其封装到直接安全模式命令消息中，从而向远端 UE 发送直接安全模式命令消息。

S824，远端 UE 推演 ProSe 密钥。

远端 UE 可以使用与 AUSF 相同的方式推演 ProSe 密钥，即根据先前推演得到的 K_{AUSF}、RSC、Nonce_1 和 Nonce_2，推演 ProSe 密钥。此外，如果远端 UE 上述推演的密钥为 K_{PROSE}，则远端 UE 应当使用 K_{PROSE} 来推演 ProSe 密钥，即 K_{AUSF} 替换为 K_{PROSE}。

S825，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

直接安全模式命令完成消息为上述直接安全模式命令消息的响应消息，用以指示远端 UE 已确定 ProSe 密钥。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。由于中继 AMF 网元、AUSF 网元与 UDM 网元之间的交互可通过复用已有服务操作实现，在不引入新的服务操作的情况实现远端 UE 与网络之间的认证，以及生成中继 UE 和远端 UE 之间的安全通信的密钥。

需要指出的是，图 8 所示的流程中提到的消息#1、消息#2、向量#1、向量#2 等等，仅用于命名上的区分，不作为任何限定。

场景 2：

示例性的，图 9 为本申请实施例提供的通信方法的流程示意图二。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以是远端 AUSF 网元，如 AUSF 网元是根据远端 UE 的标识确定的，用于支持对远端 UE 的认证，或者也可以其他任何可能形态的 AUSF 网元，对此不做具体限定。UDM 网元可以是远端 UDM 网元，如该 UDM 网元是根据远端 UE 的标识确定的，用于为远端 UE 生成认证向量，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 2 中，根据来自的 AUSF 的请求确定基于增强的 5G AKA 建立安全的 ProSe 中继通信（也可以称为 ProSe 中继通信的 5G AKA 流程，简称 5G ProSe AKA）。在 ProSe 中继通信的 5G AKA 的认证流程中，AMF 网元、AUSF 网元与 UDM 网元之间可通过新的服务操作或新的服务名称进行交互。

具体的，如图 9 所示，该通信方法的流程如下：

S901，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S902，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，S901-S902 的具体实现原理与上述 S801-S802 类似，可参考理解，不再赘述。

S903，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

S904，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S905，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信，或者说请求 ProSe 中继通信的密钥，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选地，中继密钥请求消息中还可以包括：中继 UE 的标识，如 5G GUTI。

S906，中继 AMF 网元验证中继 UE。

具体的，中继 AMF 网元根据来自 UDM 网元的中继 UE 的签约信息，判断中继 UE 是否授权作为中继提供服务。

其中，S903-S906 的具体实现原理与上述 S403-S406 类似，可参考理解，不再赘述。

S907，中继 AMF 网元向 AUSF 网元发送 ProSe UE 认证请求（Nausf_ProSeUEAuthentication_Authenticate Request 或 Nausf_UEAuthentication_ProSeAuthenticate Request）消息#1。相应的，AUSF 网元接收来自中继 AMF 网元的 ProSe UE 认证请求消息#1。

中继 AMF 网元可根据远端 UE 的 SUCI 选择 AUSF 网元，如中继 AMF 网元与 NRF 网元交互确定服务的 AUSF 网元，或者根据本地存储的 AUSF 网元信息确定服务的 AUSF 网元。如此，中继 AMF 网元可根据来自中继 UE 的中继密钥请求消息，确定向被选中的 AUSF 网元发送 ProSe UE 认证请求消息#1。例如，中继 AMF 网元可以根据消息名称，确定向 AUSF 网元发送 ProSe UE 认证请求消息#1。

ProSe UE 认证请求消息#1 可以用于请求建立 ProSe 中继通信安全的认证流程（可简称触发 ProSe 认证），或者说触发 ProSe 认证，以保证 AUSF 推演用于保护中继通信安全的密钥，避免 AUSF 执行错误的流程。例如，ProSe UE 认证请求消息#1 可以通过自身服务类型、服务操作、或服务名称，指示其用于请求 ProSe 认证。该 ProSe 认证用于远端 UE 通过中继 UE 与网络执行双向认证，并建立远端 UE 和中继 UE 之间安全通信的密钥。ProSe UE 认证请求消息#1 可以包括如下至少一项：远端 UE 的 SUCI、RSC、Nonce_1、或服务网络名称。

具体的，一种可能的方式中，ProSe UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、以及服务网络名称。在此基础上，中继 AMF 网元可以在后续确定远端 UE 认证通过的情况下，再向 AUSF 网元发送 RSC 和 Nonce_1，以进一步按需提供参

数。或者，另一种可能的方式中，ProSe UE 认证请求消息#1 中可以包括：远端 UE 的 SUCI、RSC、Nonce_1、以及服务网络名称。

上述服务网络名称可以为 5G:SN ID 或 5G:ProSe 或者 5G:ProSe||SN ID。若使用 5G:ProSe 或者 5G:ProSe||SN ID，可以保证 AV 向量与直接认证的不同，达到安全隔离的密钥。

需要指出的是，通过 ProSe UE 认证请求消息这一名称指示新的服务名称或服务操作仅为一种示例，其也可以替换为其他任何可能的命名，例如 5G ProSe UE 认证请求消息、ProSe 通信 UE 认证请求消息、或 5G ProSe 通信 UE 认证请求消息等等，对此不做任何限定。

S908，AUSF 网元向 UDM 网元发送 ProSe UE 认证获得请求（Nudm_ProSeUEAuthentication_Get Request 或 Nudm_UEAuthentication_GetProSeAV）消息。相应的，UDM 网元接收来自 AUSF 网元的 ProSe UE 认证获得请求消息。

AUSF 网元可以根据 ProSe UE 认证请求消息#1，向 UDM 网元发送 ProSe UE 认证获得请求消息。ProSe UE 认证获得请求消息可用于请求 ProSe 认证（触发 ProSe 认证）。例如，ProSe UE 认证获得请求消息可以通过自身服务类型、服务操作、或服务名称，指示其用于请求 ProSe 认证。ProSe UE 认证获得请求消息中可以包括：远端 UE 的 SUCI。

可以理解，ProSe UE 认证获得请求消息的上述实现方式仅为一些示例，不作为限定。例如，ProSe UE 认证获得请求消息仍可以携带上述 ProSe 中继通信指示信息#2，以通过 ProSe 中继通信指示信息#2 指示其用于请求 ProSe 认证。ProSe 中继通信指示信息#2 的具体实现原理可以参考上述 S808 中的相关介绍，不再赘述。

需要指出的是，通过 ProSe UE 认证获得请求消息这一名称指示新的服务名称或服务操作仅为一种示例，其也可以替换为其他任何可能的命名，例如 5G ProSe UE 认证获得请求消息、ProSe 通信 UE 认证获得请求消息、或 5G ProSe 通信 UE 认证获得请求消息等等，对此不做任何限定。

S909，UDM 网元生成 ProSe 中继通信的认证向量。

UDM 网元可根据 ProSe UE 认证获得请求消息，确定执行 ProSe 认证。在此基础上，UDM 网元，或者 UDM 网元可以调用 SIDF，解析 SIDF 解析 SUCI 获取 SUPI。UDM 网元可以根据 SUPI 对应的签约用户数据，确定 ProSe 中继通信的认证机制，例如确定使用 ProSe 中继通信的 5G AKA，也即 5G ProSe AKA。如此，UDM 网元可以生成 ProSe 中继通信的认证向量，具体实现原理可以参考上述 S809 中的相关介绍，不再赘述。

可选地，在确定执行 ProSe 认证的基础上，UDM 网元可以根据 SUPI 对应的签约用户数据，判断用户是否授权使用中继通信，具体实现原理也可以参考上述 S809 中的相关介绍，不再赘述。

S910，UDM 网元向 AUSF 网元发送 ProSe UE 认证获得响应（Nudm_ProSeUEAuthentication_Get Response 或 Nudm_ProSeUEAuthentication_GetProSeAV Response）消息。相

应的，UDM 网元接收来自 AUSF 网元的 ProSe UE 认证获得响应消息。

ProSe UE 认证获得响应消息为上述 ProSe UE 认证获得请求消息的响应消息。ProSe UE 认证获得响应消息中可以包括：5G ProSe AKA 的认证向量#1，可选地，还可以包括：SUPI。ProSe UE 认证获得响应消息还可以指示该 5G ProSe AKA 的认证向量#1 为支持 ProSe 中继通信的 5G AKA 认证向量。例如，ProSe UE 认证获得响应消息可以通过自身消息类型、服务操作、或服务名称，指示认证向量用于 5G AKA，5G AKA 支持 ProSe 中继通信。或者，ProSe UE 认证获得响应消息也可以通过携带的指示信息，指示认证向量用于 5G AKA，5G AKA 支持 ProSe 中继通信。

需要指出的是，通过 ProSe UE 认证获得响应消息这一名称指示新的服务名称或服务操作仅为一种示例，其也可以替换为其他任何可能的命名方式，例如 5G ProSe UE 认证响应请求消息、ProSe 通信 UE 认证获得响应消息、或 5G ProSe 通信 UE 认证获得响应消息等等，对此不做任何限定。

S911，AUSF 网元储存 XRES*，推演 HXRES*。

其中，S911 的具体实现原理与上述 S811 类似，可参考理解，不再赘述。

S912，AUSF 网元向中继 AMF 网元发送 ProSe UE 认证响应（Nausf_ProSeUEAuthentication_Authenticate response 或 Nausf_UEAuthentication_ProSeAuthenticate response）消息#1。相应的，中继 AMF 网元接收来自 AUSF 网元的 ProSe UE 认证响应消息#1。

ProSe UE 认证响应消息#1 为上述 ProSe UE 认证请求消息#1 的响应消息。ProSe UE 认证响应消息#1 中可以包括：5G ProSe AKA 的认证向量#2，具体实现原理可以参考上述 S812 中的相关介绍，不再赘述。ProSe UE 认证响应消息#1 还可以指示该 5G ProSe AKA 的认证向量#2 为支持 ProSe 中继通信的 5G AKA。例如，ProSe UE 认证响应消息#1 可以通过自身消息类型、服务操作、或服务名称，指示认证向量用于 5G AKA，5G AKA 支持 ProSe 中继通信。或者，ProSe UE 认证响应消息#1 也可以通过携带的指示信息，指示认证向量用于 5G AKA，5G AKA 支持 ProSe 中继通信。

需要指出的是，通过 ProSe UE 认证响应消息这一名称指示新的服务名称或服务操作仅为一种示例，其也可以替换为其他任何可能的命名方式，例如 5G ProSe UE 认证响应消息、ProSe 通信 UE 认证响应消息、或 5G ProSe 通信 UE 认证响应消息等等，对此不做任何限定。

S913，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息。相应的，中继 UE 接收来自中继 AMF 网元的 ProSe 通信认证请求消息。

S914，中继 UE 向远端 UE 发送远端 UE 认证请求消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证请求消息。

S915，远端 UE 推演 RES*。

S916，远端 UE 向中继 UE 发送远端 UE 认证响应消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证响应消息。

S917，中继 UE 向中继 AMF 网元发送 ProSe 通信认证响应消息。相应的，中继 AMF 网元接收来自中继 UE 的 ProSe 通信认证响应消息。

S918，中继 AMF 网元认证远端 UE。

其中，S913-S918 的具体实现原理与 S813-S818 类似，可以参考理解，不再赘述。

S919，中继 AMF 网元向 AUSF 网元发送 ProSe UE 认证请求消息#2。相应的，AUSF 网元接收来自中继 AMF 网元的 ProSe UE 认证请求消息#2。

ProSe UE 认证请求消息#2 可用于请求对远端 UE 进行 ProSe 认证，包括：RES*。也就是说，中继 AMF 网元在认证远端 UE 通过后，可将 RES*封装到 ProSe UE 认证请求消息#2 中，然后向 AUSF 网元发送 ProSe UE 认证请求消息#2。可选地，如果 S907 中的 UE 认证请求消息#1 未携带 RSC 和 Nonce_1，则 ProSe UE 认证请求消息#2 中还可以包括：RSC 和 Nonce_1，即中继 AMF 网元还可以将 RSC 和 Nonce_1 封装到 ProSe UE 认证请求消息#2 中。或者，在 S907 中的 ProSe UE 认证请求消息#1 携带 RSC 和 Nonce_1 的情况下，ProSe UE 认证请求消息#2 中仍可以包括：RSC 和 Nonce_1。

S920，AUSF 网元认证远端 UE。

其中，S920 的具体实现原理与 S820 类似，可以参考理解，不再赘述。

S921，AUSF 网元向中继 AMF 网元发送 ProSe UE 认证响应消息#2。相应的，中继 AMF 网元接收来自 AUSF 网元的 ProSe UE 认证响应消息#2。

ProSe UE 认证响应消息#2 为 ProSe UE 认证请求消息#2 的响应消息，可用于指示认证远端 UE 通过。ProSe UE 认证响应消息#2 中可以包括：ProSe 密钥和 Nonce_2。

S922，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

S923，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

S924，远端 UE 推演 ProSe 密钥。

S925，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

其中，S921-S925 的具体实现原理与 S821-S825 类似，可以参考理解，不再赘述。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。由于中继 AMF 网元、AUSF 网元与 UDM 网元之间的交互可通过新的信令实现，实现与已有认证流程解耦，避免认证流程对 ProSe 认证产生影响。

需要指出的是，图 9 所示的流程中提到的消息#1、消息#2、向量#1、向量#2 等等，仅用于命名上的区分，不作为任何限定。

场景 3：

示例性的，图 10 为本申请实施例提供的通信方法的流程示意图三。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以是远端 AUSF 网元，如 AUSF 网

元是根据远端 UE 的标识确定的，用于支持对远端 UE 的认证，或者也可以其他任何可能形态的 AUSF 网元，对此不做具体限定。UDM 网元可以是远端 UDM 网元，如该 UDM 网元是根据远端 UE 的标识确定的，用于为远端 UE 生成认证向量，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 3 中，UDM 网元根据来自的 AUSF 网元的请求确定基于 EAP AKA' 建立安全的 ProSe 中继通信（也可以称为 ProSe 中继通信的 EAP- AKA'流程，简称 ProSe EAP- AKA'）。在 ProSe 中继通信的 EAP-AKA'的认证流程中，AMF 网元、AUSF 网元与 UDM 网元之间可通过使用已有服务操作进行交互。

具体的，如图 10 所示，该通信方法的流程如下：

S1001，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S1002，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，S1001-S1002 的具体实现原理与上述 S801-S802 类似，可参考理解，不再赘述。

S1003，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

S1004，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S1005，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信的密钥，或者说请求 ProSe 中继通信的密钥，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选地，中继密钥请求消息中还可以包括：中继 UE 的标识，如 5G GUTI。

S1006，中继 AMF 网元验证中继 UE。

具体的，中继 AMF 网元可根据来自 UDM 网元的中继 UE 的签约信息，判断中继 UE 是否授权作为中继提供服务。

其中，S1003-S1006 的具体实现原理与上述 S403-S406 类似，可参考理解，不再赘述。

S1007，中继 AMF 网元向 AUSF 网元发送 UE 认证请求消息#1。相应的，AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息#1。

S1008，AUSF 网元向 UDM 网元发送 UE 认证获得请求消息。相应的，UDM 网元接收来自 AUSF 网元的 UE 认证获得请求消息。

其中，S1007-S1008 的具体实现原理与上述 S807-S808 类似，可参考理解，不再赘述。

S1009，UDM 网元生成 ProSe 中继通信的认证向量。

UDM 网元可根据 UE 认证获得请求消息，确定获取 ProSe 认证的数据。具体的，UDM 网元，或者 UDM 网元可以调用 SIDF，解析 SIDF 解析 SUCI 获取 SUPI。UDM 网元可以根据 SUPI 对应的签约用户数据和请求消息，确定 ProSe 中继通信的认

证机制，例如确定使用 ProSe 中继通信的 EAP-AKA'。如此，UDM 网元可以生成 ProSe 中继通信的认证向量，例如，EAP-AKA'的 ProSe 认证向量（EAP-AKA' ProSe AV）。EAP-AKA'的 ProSe 认证向量可以包括：RAND、AUTN、XRES、以及 CK'和 IK'。其中，RAND、AUTN 以及 XRES 的具体实现原理可以参考上述 S809 中的相关介绍，不再赘述。CK'和 IK'可由根密钥和 RAND 推演得到，用于推演 ProSe 密钥。例如，UDM 网元/ARPF 可以根密钥和 RAND 推演 CK 和 IK，再根据 CK 和 IK 推演 CK'和 IK'。可以理解，采用 CK'和 IK'仅为一种示例，CK'和 IK 也可以替换其他任何可能的密钥，例如根据 CK 和 IK，以及新的 SN 或新的参数，如 PROSE 字符推演 K_{PROSE}。

可选地，UDM 网元确定 ProSe 中继通信的认证机制也可以为：如果 UE 认证获得请求消息中携带有 ProSe 中继通信指示信息#2，则 UDM 网元确定使用 ProSe 中继通信的 EAP-AKA'。这种情况下，UDM 网元无需查询签约用户数据，可提高认证效率。

可选地，在确定执行 ProSe 认证的基础上，UDM 网元可以根据 SUPI 对应的签约用户数据，判断用户是否授权使用中继通信，具体实现原理也可以参考上述 S809 中的相关介绍，不再赘述。

需要指出的是，ProSe 中继通信的 EAP-AKA'仅为本申请实施例中的一种示例性命名方式，其也可以替换为其他任何可能的命名方式，例如 5G ProSe 中继通信的 EAP-AKA'、或 5G ProSe EAP-AKA'等，对此不做任何限定。同理，EAP-AKA'的 ProSe 认证向量也仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 EAP-AKA'ProSe 认证向量、ProSe EAP-AKA'认证向量、或 ProSe 中继通信的 EAP-AKA'认证向量等，对此不做任何限定。

S1010，UDM 网元向 AUSF 网元发送 UE 认证获得响应消息。相应的，UDM 网元接收来自 AUSF 网元的 UE 认证获得响应消息。

UE 认证获得响应消息为上述 UE 认证获得请求消息的响应消息。UE 认证获得响应消息中可以包括：EAP-AKA'的 ProSe 认证向量，可选地，还可以包括：SUPI。UE 认证获得响应消息还可以指示：该 EAP-AKA'的 ProSe 认证向量为支持 ProSe 中继通信的 5G AKA 认证向量。例如，在 UE 认证获得响应消息已有指示信息指示认证向量用于 EAP-AKA'基础上，可在 UE 认证获得响应消息中新增指示信息，用以指示 EAP-AKA'支持 ProSe 中继通信。或者，在 UE 认证获得响应消息中新增指示信息，用以指示认证向量用于 EAP-AKA'， EAP-AKA'支持 ProSe 中继通信。

S1011，AUSF 网元储存 XRES。

AUSF 网元接收到 UE 认证获得响应消息后，可储存 XRES，可选地，还存储 SUPI，以便后续认证使用。在 ProSe 认证中，AUSF 网元可以不推演 K_{SEAF}，以防止生成冗余的信息，造成资源的浪费。

S1012，AUSF 网元向中继 AMF 网元发送 UE 认证响应消息#1。相应的，中继 AMF 网元接收来自 AUSF 网元的 UE 认证响应消息#1。

UE 认证响应消息#1 为上述 UE 认证请求消息#1 的响应消息。UE 认证响应消息#1 中可以包括：EAP 请求消息/ AKA'挑战消息。EAP 请求消息/ AKA'挑战消息可以

是根据 UE 认证获得响应消息#1 确定的 NAS 消息，包括：RAND 和 AUTN。

S1013，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息。相应的，中继 UE 接收来自中继 AMF 网元的 ProSe 通信认证请求消息。

ProSe 通信认证请求消息可用于指示用于对远端 UE 进行认证，或者说指示中继 UE 向远端 UE 发送认证数据，以避免中继 UE 接收到 ProSe 通信认证请求消息后自行执行认证，防止认证失败，无法建立通信连接。例如，ProSe 通信认证请求消息可以通过其消息类型，或其携带的指示信息，指示中继 UE 向远端 UE 发送认证数据，或者说指式对远端 UE 进行认证。当然，也可通过已有消息（如认证请求消息）携带指示信息来指示中继 UE 向远端 UE 发送认证数据，此处不限制。ProSe 通信认证请求消息中可以包括：EAP 请求消息/ AKA'挑战消息（认证数据）。也就是说，中继 AMF 网元接收到 UE 认证响应消息#1 后，可将 UE 认证响应消息#1 中的 EAP 请求消息/ AKA'挑战消息，继续封装到 ProSe 通信认证请求消息中，从而向中继 UE 透传该 EAP 请求消息/ AKA'挑战消息。

可选地，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息前，中继 AMF 跳过获取 ngKSI 和 ABBA 参数。或者，中继 AMF 网元跳过生成 ngKSI 和 ABBA 参数。中继 AMF 网元不向中继 UE 发送 ngKSI 和 ABBA 参数，也即 ProSe 通信认证请求消息不包含 ngKSI 和 ABBA 参数。

S1014，中继 UE 向远端 UE 发送远端 UE 认证请求消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证请求消息。

远端 UE 认证请求消息可用于指示远端 UE 执行 ProSe 认证，或者说认证远端 UE，确保远端 UE 与网络执行认证并推演 ProSe 密钥，建立远端 UE 和中继 UE 之间的安全通信。例如，ProSe 通信认证请求消息可以通过其消息类型，或其携带的指示信息，指示远端 UE 执行 ProSe 认证，或者说认证远端 UE。当然，也可通过已有消息携带指示信息来指示远端 UE 执行 ProSe 认证，此处不限制。ProSe 通信认证请求消息中可以包括：EAP 请求消息/ AKA'挑战消息，以便远端 UE 执行 ProSe 认证使用。也就是说，中继 UE 接收到 ProSe 通信认证请求消息后，可将 ProSe 通信认证请求消息中的 EAP 请求消息/ AKA'挑战消息，继续封装到远端 UE 认证请求消息中，以向远端 UE 透传该 EAP 请求消息/ AKA'挑战消息，以便远端 UE 认证使用。

S1015，远端 UE 推演 RES。

其中，远端 UE 可以包括：ME 和 USIM。UE 接收到远端 UE 认证请求消息后，USIM 可根据 RAND 和自身的根密钥，验证 AUTN。如果 USIM 验证 AUTN 失败，则表示远端 UE 认证网络失败，流程结束。如果 USIM 验证 AUTN 通过，则表示远端 UE 认证网络通过。在此基础上，USIM 可以利用根密钥和 RAND，推演 RES、以及 CK 和 IK，并向 ME 发送 RES、以及 CK 和 IK。ME 可以根据 CK 和 IK 推演 CK'和 IK'，然后执行 S1016。

需要说明的是，如上述 S1009 和 S1111 中的相关介绍可知，若网络侧使用新的密钥推演方法或新的认证参数的推演方法，则远端 UE 也使用和网络侧相同的方法执行密钥推演或认证参数推演，以及其他认证数据的生成。

S1016，远端 UE 向中继 UE 发送远端 UE 认证响应消息。相应的，远端 UE 接收

来自中继 UE 的远端 UE 认证响应消息。

远端 UE 认证响应消息为上述远端 UE 认证请求消息的响应消息。可选地，ProSe 通信认证响应消息可用于指示其为远端 UE 的认证响应消息。例如，ProSe 通信认证响应消息可以通过消息的类型或消息中包含的信元，指示其为远端 UE 的认证响应消息。远端 UE 认证响应消息中可以包括：EAP 响应消息/ AKA'挑战消息。EAP 响应消息/ AKA'挑战消息中可以包括：RES。

S1017，中继 UE 向中继 AMF 网元发送 ProSe 通信认证响应消息。相应的，中继 AMF 网元接收来自中继 UE 的 ProSe 通信认证响应消息。

ProSe 通信认证响应消息为上述 ProSe 通信认证请求消息的响应消息。可选地，ProSe 通信认证响应消息用于指示其为远端 UE 的认证响应消息。例如，ProSe 通信认证响应消息可以通过消息的类型或消息中包含的信元，指示其为远端 UE 的认证响应消息。ProSe 通信认证响应消息中可以包括：EAP 响应消息/ AKA'挑战消息。也就是说，中继 UE 可以从远端 UE 认证响应消息中获得 EAP 响应消息/ AKA'挑战消息，将其继续封装到 ProSe 通信认证响应消息中，以向 AUSF 网元透传该 EAP 响应消息/ AKA'挑战消息。

S1018，中继 AMF 网元向 AUSF 网元发送 UE 认证请求消息#2。相应的，AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息#2。

UE 认证请求消息#2 可用于请求对远端 UE 进行认证。例如，UE 认证请求消息#2 可以通过新的指示信息指示对远端 UE 进行认证。UE 认证请求消息#2 中可以包括：EAP 响应消息/ AKA'挑战消息。也就是说，中继 AMF 网元可以从 ProSe 通信认证响应消息中获得 EAP 响应消息/ AKA'挑战消息，将其封装到 UE 认证请求消息#2 中，以向 AUSF 网元透传该 EAP 响应消息/ AKA'挑战消息。可选地，如果 S1007 中的 UE 认证请求消息#1 未携带 RSC 和 Nonce_1，则 UE 认证请求消息#2 中还可以包括：RSC 和 Nonce_1，即中继 AMF 网元还可以将 RSC 和 Nonce_1 封装到 UE 认证请求消息#2 中。或者，在 S1007 中的 UE 认证请求消息#1 携带 RSC 和 Nonce_1 的情况下，UE 认证请求消息#2 中仍可以包括：RSC 和 Nonce_1。此时，RSC 和 Nonce_1 也可以用于指示对远端 UE 进行认证。

S1019，AUSF 网元认证远端 UE。

AUSF 网元接收到 UE 认证请求消息#2 后，可从中获得 EAP 响应消息/ AKA'挑战消息，并进一步获得 RES。AUSF 网元可以比较 RES 与先前保存的 XRES。如果 RES 和 XRES 不匹配，例如 RES 和 XRES 不相同，则表示认证远端 UE 失败，流程结束。如果 RES 和 XRES 匹配，例如 RES 和 XRES*相同，则表示认证远端 UE 通过。在此基础上，AUSF 网元可以生成 Nonce_2，根据先前保存的 CK'、IK'、RSC、Nonce_1 以及 Nonce_2，推演 ProSe 密钥，用于远端 UE 与中继 UE 的通信使用。

具体的，AUSF 网元可以根据 CK'和 IK'推演 EMSK，根据 EMSK 确定 K_{AUSF}，例如确定 EMSK 的前 256 位作为 K_{AUSF}，且不推演 K_{SEAF}。AUSF 网元可以根据 K_{AUSF}、RSC、Nonce_1 以及 Nonce_2，推演 ProSe 密钥。例如，AUSF 网元可以先根据 K_{AUSF} 和 RSC 推演一个中间密钥，再根据中间密钥、Nonce_1 和 Nonce_2 推演 ProSe 密钥。或者，AUSF 网元可以直接根据 K_{AUSF}、RSC、Nonce_1 以及 Nonce_2，

推演 ProSe 密钥。或者，AUSF 网元还可以采用其他任何可能的方式推演 ProSe 密钥，对此不做具体限定。

可选地，在确定认证远端 UE 的情况下，AUSF 网元执行上述 ProSe 密钥推演的过程。

S1020，AUSF 网元向中继 AMF 网元发送 UE 认证响应消息#2。相应的，中继 AMF 网元接收来自 AUSF 网元的 UE 认证响应消息#2。

UE 认证响应消息#2 为 UE 认证请求消息#2 的响应消息。UE 认证响应消息#2 中可以包括：EAP 成功消息，用以指示认证通过，以及还可以包括：ProSe 密钥和 Nonce_2。也就是说，AUSF 网元确定远端 UE 认证通过后，可生成 EAP 成功消息，并将 EAP 成功消息、ProSe 密钥和 Nonce_2 封装到 UE 认证响应消息#2 中，然后向中继 AMF 网元发送 UE 认证响应消息#2。

可选地，UE 认证响应消息#2 中还可以包括：远端 UE 的 SUPI。该远端 UE 的 SUPI 可用于指示中继 UE 向网络侧上报执行远端 UE 的信息。

S1021，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

中继密钥响应消息为上述中继密钥请求消息的响应消息，可以包括：EAP 成功消息、ProSe 密钥和 Nonce_2，可选地，还可以包括：远端 UE 的 SUPI。也就是说，中继 AMF 网元接收到 UE 认证响应消息#2 后，可根据 UE 认证响应消息#2，获得 EAP 成功消息、ProSe 密钥和 Nonce_2，可选地，还可以获得远端 UE 的 SUPI，并将其封装到中继密钥响应消息中，以向中继 UE 发送中继密钥响应消息。相应的，中继 UE 可以存储 ProSe 密钥，可选地，还可以存储远端 UE 的 SUPI。

S1022，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

直接安全模式命令消息可用于建立 PC5 安全。直接安全模式命令消息中可以包括：EAP 成功消息和 Nonce_2。也就是说，中继 UE 接收到中继密钥响应消息后，可从中获得 EAP 成功消息和 Nonce_2，然后将其封装到直接安全模式命令消息中，从而向远端 UE 发送直接安全模式命令消息。

S1023，远端 UE 推演 ProSe 密钥。

远端 UE 可以使用与 AUSF 相同的方式推演 ProSe 密钥，即根据先前推演得到的 CK'和 IK'，以及 RSC、Nonce_1 和 Nonce_2，推演 ProSe 密钥。

S1024，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

直接安全模式命令完成消息为上述直接安全模式命令消息的响应消息，用以指示远端 UE 已确定 ProSe 密钥。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。由于中继 AMF 网元、AUSF 网元与 UDM 网元之间的交互可通过复用已有服务操作实现，在不引入新的服务操作的情况实现远端 UE 与网络之间的认证，以及生成中继 UE 和远端 UE 之间的安全通信的密钥。

需要指出的是，图 10 所示的流程中提到的消息#1、消息#2 等等，仅用于命名上的区分，不作为任何限定。

场景 4：

示例性的，图 11 为本申请实施例提供的通信方法的流程示意图四。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以是远端 AUSF 网元，如 AUSF 网元是根据远端 UE 的标识确定的，用于支持对远端 UE 的认证，或者也可以其他任何可能形态的 AUSF 网元，对此不做具体限定。UDM 网元可以是远端 UDM 网元，如该 UDM 网元是根据远端 UE 的标识确定的，用于为远端 UE 生成认证向量，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 4 中，UDM 网元根据来自的 AUSF 网元的请求确定基于 EAP AKA’ 建立安全的 ProSe 中继通信（也可以称为 ProSe 中继通信的 EAP- AKA’流程，简称 ProSe EAP-AKA’）或者新的 EAP AKA。在 ProSe 中继通信的 5G EAP-AKA’的认证流程中，AMF 网元、AUSF 网元与 UDM 网元之间可通过新的服务操作或服务名称进行交互。

具体的，如图 11 所示，该通信方法的流程如下：

S1101，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S1102，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，S1101-S1102 的具体实现原理与上述 S801-S802 类似，可参考理解，不再赘述。

S1103，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

S1104，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S1105，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信，或者说请求 ProSe 中继通信的密钥，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选地，中继密钥请求消息中还可以包括：中继 UE 的标识，如 5G GUTI。

S1106，中继 AMF 网元验证中继 UE。

具体的，中继 AMF 网元可根据来自 UDM 网元的中继 UE 的签约信息，判断中继 UE 是否授权作为中继提供服务。

其中，S1103-S1106 的具体实现原理与上述 S403-S406 类似，可参考理解，不再赘述。

S1107，中继 AMF 网元向 AUSF 网元发送 ProSe UE 认证请求消息#1。相应的，AUSF 网元接收来自中继 AMF 网元的 ProSe UE 认证请求消息#1。

S1108，AUSF 网元向 UDM 网元发送 ProSe UE 认证获得请求消息。相应的，

UDM 网元接收来自 AUSF 网元的 ProSe UE 认证获得请求消息。

其中，S1107-S1108 的具体实现原理与上述 S907-S908 类似，可参考理解，不再赘述。

S1109，UDM 网元生成 ProSe 中继通信的认证向量。

UDM 网元可根据 ProSe UE 认证获得请求消息，确定执行 ProSe 认证。在此基础上，UDM 网元，或者 UDM 网元可以调用 SIDF，解析 SIDF 解析 SUCI 获取 SUPI。UDM 网元可以根据 SUPI 对应的签约用户数据，确定 ProSe 中继通信的认证机制，例如确定使用 ProSe 中继通信的 EAP-AKA'。如此，UDM 网元可以生成 ProSe 中继通信的认证向量，具体实现原理可以参考上述 S1109 中的相关介绍，不再赘述。

可选地，在确定执行 ProSe 认证的基础上，UDM 网元可以根据 SUPI 对应的签约用户数据，判断用户是否授权使用中继通信，具体实现原理也可以参考上述 S809 中的相关介绍，不再赘述。

S1110，UDM 网元向 AUSF 网元发送 ProSe UE 认证获得响应消息。相应的，UDM 网元接收来自 AUSF 网元的 ProSe UE 认证获得响应消息。

ProSe UE 认证获得响应消息为应上述 ProSe UE 认证获得请求消息的响应消息。ProSe UE 认证获得响应消息中可以包括：EAP-AKA'的 ProSe 认证向量，可选地，还可以包括：SUPI。ProSe UE 认证获得响应消息还可以指示：该 EAP-AKA'的 ProSe 认证向量为支持 ProSe 中继通信的 EAP-AKA'认证向量。例如，ProSe UE 认证获得响应消息可以通过自身消息类型，指示认证向量用于 EAP-AKA'，EAP-AKA'支持 ProSe 中继通信。或者，ProSe UE 认证获得响应消息也可以通过携带的指示信息，指示认证向量用于 EAP-AKA'，EAP-AKA'支持 ProSe 中继通信。

S1111，AUSF 网元储存 XRES。

AUSF 网元接收到 ProSe UE 认证获得响应消息后，可储存 XRES，可选地，还存储 SUPI，以便后续认证使用。在 ProSe 认证中，AUSF 网元可以不推演 K_{SEAF}，以防止生成冗余的信息，造成资源的浪费。

S1112，AUSF 网元向中继 AMF 网元发送 ProSe UE 认证响应消息#1。相应的，中继 AMF 网元接收来自 AUSF 网元的 ProSe UE 认证响应消息#1。

ProSe UE 认证响应消息#1 为上述 ProSe UE 认证请求消息#1 的响应消息。ProSe UE 认证响应消息#1 中可以包括：EAP 请求消息/ AKA'挑战消息。EAP 请求消息/ AKA'挑战消息可以是根据 UE 认证获得响应消息#1 确定的 NAS 消息，包括：RAND 和 AUTN。

S1113，中继 AMF 网元向中继 UE 发送 ProSe 通信认证请求消息。相应的，中继 UE 接收来自中继 AMF 网元的 ProSe 通信认证请求消息。

S1114，中继 UE 向远端 UE 发送远端 UE 认证请求消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证请求消息。

S1115，远端 UE 推演 RES。

S1116，远端 UE 向中继 UE 发送远端 UE 认证响应消息。相应的，远端 UE 接收来自中继 UE 的远端 UE 认证响应消息。

S1117，中继 UE 向中继 AMF 网元发送 ProSe 通信认证响应消息。相应的，中继

AMF 网元接收来自中继 UE 的 ProSe 通信认证响应消息。

其中，S1113-S1117 的具体实现原理与 S1013-S1017 类似，可以参考理解，不再赘述。

S1118，中继 AMF 网元向 AUSF 网元发送 ProSe UE 认证请求消息#2。相应的，AUSF 网元接收来自中继 AMF 网元的 ProSe UE 认证请求消息#2。

ProSe UE 认证请求消息#2 可用于请求对远端 UE 进行 ProSe 认证，包括：EAP 响应消息/ AKA'挑战消息。也就是说，中继 AMF 网元可以从 ProSe 通信认证响应消息中获得 EAP 响应消息/ AKA'挑战消息，将其封装到 ProSe UE 认证请求消息#2 中，以向 AUSF 网元透传该 EAP 响应消息/ AKA'挑战消息。可选地，如果 S1107 中的 ProSe UE 认证请求消息#1 未携带 RSC 和 Nonce_1，则 ProSe UE 认证请求消息#2 中还可以包括：RSC 和 Nonce_1，即中继 AMF 网元还可以将 RSC 和 Nonce_1 封装到 ProSe UE 认证请求消息#2 中。或者，在 S1107 中的 ProSe UE 认证请求消息#1 携带 RSC 和 Nonce_1 的情况下，ProSe UE 认证请求消息#2 中仍可以包括：RSC 和 Nonce_1。

S1119，AUSF 网元认证远端 UE。

其中，S1119 的具体实现原理与 S1019 类似，可以参考理解，不再赘述。

S1120，AUSF 网元向中继 AMF 网元发送 ProSe UE 认证响应消息#2。相应的，中继 AMF 网元接收来自 AUSF 网元的 ProSe UE 认证响应消息#2。

ProSe UE 认证响应消息#2 为 ProSe UE 认证请求消息#2 的响应消息。ProSe UE 认证响应消息#2 中可以包括：EAP 成功消息，用以指示认证通过，以及还可以包括：ProSe 密钥和 Nonce_2。也就是说，AUSF 网元确定远端 UE 认证通过后，可生成 EAP 成功消息，并将 EAP 成功消息、ProSe 密钥和 Nonce_2 封装到 ProSe UE 认证响应消息#2 中，然后向中继 AMF 网元发送 ProSe UE 认证响应消息#2。

S1121，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

S1122，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

S1123，远端 UE 推演 ProSe 密钥。

S1124，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。由于中继 AMF 网元、AUSF 网元与 UDM 网元之间的交互可通过新的信令实现，实现与已有认证流程解耦，避免认证流程对 ProSe 认证产生影响。

需要指出的是，图 11 所示的流程中提到的消息#1、消息#2 等等，仅用于命名上的区分，不作为任何限定。

场景 5：

示例性的，图 12 为本申请实施例提供的通信方法的流程示意图五。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通

信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以是中继 AUSF 网元，或者也可以其他任何可能形态的 AUSF 网元，对此不做具体限定。UDM 网元可以是中继 UDM 网元，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 5 中，远端 UE 或者中继 AMF 网元可以判断是否执行过 ProSe 认证。在执行过对远端 UE 认证的情况下，可使用中继 AUSF 网元上已有的密钥（如 K_{AUSF}）推演 ProSe 密钥，无需再次执行 Prose 认证。

具体的，如图 12 所示，该通信方法的流程如下：

S1201，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S1202，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，S1101-S1102 的具体实现原理与上述 S801-S802 类似，可参考理解，不再赘述。

S1203，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

其中，S1102 的具体实现原理与上述 S403 类似，可参考理解，不再赘述。

S1204，远端 UE 确定认证指示信息。

认证指示信息可以用于指示远端 UE 是否与网络执行过主认证流程，或者用于确定是否执行 ProSe 认证。例如，认证指示信息包括：1 比特（bit）。这 1 比特的取值为 1，表示远端 UE 执行过主认证流程，或确定无需执行 ProSe 认证，或确定使用现有的 K_{AUSF}。这 1 比特的取值为 0，表示远端 UE 未执行过主认证，或确定执行 ProSe 认证。或者，这 1 比特的取值为 1，表示远端 UE 未执行主认证，或确定执行 ProSe 认证流程。这 1 比特的取值为 0，表示远端 UE 执行过主认证，或确定无需执行 ProSe 认证，或确定使用现有的 K_{AUSF}。

其中，远端 UE 通过中继发现流程发现中继 UE 后，可判断本地是否储存有上述用于推演 ProSe 密钥的密钥，例如 K_{AUSF}。如果储存有上述 K_{AUSF}，则表示远端 UE 执行过 ProSe 认证，生成对应取值的认证指示信息。否则，如果未储存上述 K_{AUSF}，则表示远端 UE 未执行 ProSe 认证，生成对应取值的认证指示信息。

可选地，用于推演 ProSe 密钥的密钥为 K_{AUSF} 仅为一种示例，K_{AUSF} 可替换为其他的密钥，例如上述 K_{PROSE}。或者，用于推演 ProSe 密钥的密钥也可以分别存储在远端 UE 和网络中。例如，在远端 UE 与网络执行 ProSe 认证之后，该密钥便可以分别存储在远端 UE 和网络中。此处不限制。

S1204 为可选步骤，即远端 UE 通过认证指示信息直接指示其是否执行过认证，其仅为一种示例性的方式。例如，可选地，远端 UE 也可通过是否生成指示认证指示信息，来对应指示其是否执行过认证。这种情况下，后续的设备可通过信令中是否携带认证指示信息，来判断远端 UE 是否执行过认证。如果信令中携带有认证指示信息，则用以显示指示远端 UE 执行过认证。如果信令中未携带认证指示信息，则用以隐式指示远端 UE 未执行认证。或者，如果信令中携带有认证指示信息，则用以显示指示远端 UE 未执行认证。如果信令中未携带认证指示信息，则用以隐式指示远端 UE 执行过认证。又例如，可选地，远端 UE 可以不指示其是否执行过 ProSe 认证，

由中继 AMF 网元自行确定。

需要指出的是，通过认证指示信息这一命名来指示其是否执行过认证仅为一种示例，其也可以替换为其他任何可能的命名，例如指示信息、或 ProSe 指示信息等等，对此不做任何限定。

S1205，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选地，直接通信请求消息中还可以包括：认证指示信息。

S1206，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信，或者说请求 ProSe 中继通信的密钥，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。可选地，中继密钥请求消息中还可以包括中继 UE 的标识，如 5G GUTI。远端 UE 的 SUCI、RSC 以及 Nonce_1 可以参考上述 S405 中的相关介绍，不再赘述。可选地，在直接通信请求消息中携带有认证指示信息的情况下，中继密钥请求消息中还可以包括：认证指示信息。也就是说，中继 UE 接收到直接通信请求消息，并从中获得认证指示信息后，可将认证指示信息继续封装到中继密钥请求消息中，然后向中继 AMF 网元发送中继密钥请求消息。

S1207，中继 AMF 网元验证中继 UE。

其中，S1207 的具体实现原理与上述 S406 类似，可参考理解，不再赘述。

S1208，中继 AMF 网元确定是否发起 ProSe 认证。

中继 AMF 网元可以根据中继密钥请求消息中的认证指示信息，或者根据中继密钥请求消息中是否有携带认证指示信息，确定是否发起 ProSe 认证。这种情况下，如果中继 AMF 网元确定不发起 ProSe 认证，则从 UDM 网元获得 AUSF 网元的标识，以从 AUSF 网元获得 ProSe 密钥，也即 S1209-S1216。否则，如果中继 AMF 网元确定发起 ProSe 认证，则执行 ProSe 认证，也即 S1217。

可以理解，S1208 为可选步骤，在远端 UE 未指示其是否执行过认证的情况下，中继 AMF 网元可跳过 S1208 执行 S1209，以根据是否能够从 UDM 网元获得 AUSF 网元的标识，确定远端 UE 是否执行过认证或网络有可用的密钥（如 K_{AUSF}），也即确定是否发起 ProSe 通信认证。如果中继 AMF 网元确定不发起 ProSe 认证，则执行 S1211-S1216。否则，如果中继 AMF 网元确定发起 ProSe 认证，则执行 S1217。

S1209，中继 AMF 网元向 UDM 网元发送 AUSF 获得请求（Nudm_AUSFIdGet Request）消息。相应的，UDM 网元接收来自中继 AMF 网元的 AUSF 获得请求消息。

其中，AUSF 获得请求消息用于请求 UDM 网元反馈 AUSF 网元的标识，例如 AUSF 网元的 ID（instance Id），或 AUSF 网元的 IP 地址（如 IPv4 地址、IPv6 地址或前缀）。AUSF 获得请求消息中可以包括：远端 UE 的 SUCI。如此，UDM 网元可以从中获得远端 UE 的 SUCI，以根据该 SUCI 查找 AUSF 网元的标识。例如，UDM

网元，或者 UDM 网元可以调用 SIDF 解析该 SUCI 获得 SUPI，从而根据 SUPI 获取存储在 UDM 网元中的远端 UE 的上下文，以判断是否能够从上下文中获取 AUSF 网元的标识。

可选的，UDM 网元也可以根据 SUPI 对应的签约用户数据，判断用户是否授权使用中继通信，具体实现原理也可以参考上述 S809 中的相关介绍，不再赘述。

需要指出的是，AUSF 获得请求消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 AUSF 标识获得请求消息、或 AUSF 地址获得请求消息等等，对此不做任何限定。

S1210，UDM 网元向中继 AMF 网元发送 AUSF 获得响应（Nudm_AUSFIdGet Response）消息。相应的，UDM 网元接收来自中继 AMF 网元的 AUSF 获得响应消息。

AUSF 获得响应消息为上述 AUSF 获得请求消息的响应消息。AUSF 获得响应消息中可以包括：AUSF 网元的标识，可选地，还可以包括：SUPI。

其中，如果远端 UE 执行过认证，或者说远端 UE 本地存储了 K_{AUSF}，那么远端 UE 的上下文中应当储存有当初认证远端 UE 的 AUSF 网元的标识。这种情况下，UDM 网元能够从远端 UE 的上下文中获取 AUSF 网元的标识，并将其封装到 AUSF 获得响应消息中，然后向中继 AMF 网元发送该 AUSF 获得响应消息。否则，如果远端 UE 未执行 ProSe 认证，那么远端 UE 的上下文中没有 AUSF 网元的标识。这种情况下，UDM 网元无法从远端 UE 的上下文中获取 AUSF 网元的标识，而直接向中继 AMF 网元发送 AUSF 获得响应消息。

可以理解，在远端 UE 指示其执行过主认证的情况下，通过执行 S1209-S1210，中继 AMF 网元应当能够获得 AUSF 网元的标识。

需要指出的是，AUSF 获得响应消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 AUSF 标识获得响应消息、或 AUSF 地址获得响应消息等等，对此不做任何限定。

S1211，中继 AMF 网元向 AUSF 网元发送 ProSe 密钥请求（Nausf_ProSe_Key Request）消息。相应的，AUSF 网元接收来自中继 AMF 网元的 ProSe 密钥请求消息。

中继 AMF 网元可以根据 AUSF 网元的标识，向 AUSF 网元发送 ProSe 密钥请求消息。ProSe 密钥请求消息主要用于请求 ProSe 密钥，包括：SUPI、RSC 以及 Nonce_1。AUSF 网元接收到 ProSe 密钥请求消息后，可从中获得 RSC 以及 Nonce_1。这样，AUSF 网元可以根据先前认证远端 UE 时确定 K_{AUSF}、本次生成的 Nonce_2、以及 RSC 和 Nonce_1，推演 ProSe 密钥。其中，推演 ProSe 密钥的具体实现原理可以参考上述 S820 中的相关介绍，不再赘述。

需要指出的是，ProSe 密钥请求消息仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 ProSe 通信密钥请求消息，对此不做任何限定。

S1212，AUSF 网元向中继 AMF 网元发送 ProSe 密钥响应（Nausf_ProSe_Key Response）消息。相应的，中继 AMF 网元接收来自 AUSF 网元的 ProSe 密钥响应消

息。

ProSe 密钥响应消息为上述 ProSe 密钥请求消息的响应消息，包括：ProSe 密钥和 Nonce_2。此外，ProSe 密钥响应消息也仅为本申请实施例中的一种示例性的命名方式，其也可以替换为其他任何可能的命名方式，例如 ProSe 通信密钥响应消息，对此不做任何限定。

S1213，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

S1214，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

S1215，远端 UE 推演 ProSe 密钥。

S1216，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

其中，S1213-S1216 的具体实现原理与 S822-S825 类似，可参考理解，不再赘述。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。此外，在远端 UE 执行过 ProSe 认证的情况，AUSF 网元无需认证即可推演 ProSe 密钥，以有效提高设备运行效率。

S1217，ProSe 认证。

通过执行 ProSe 认证可建立中继 UE 和远端 UE 的安全通信。

其中，S1217 可以为场景 1 中的 S807-S822、或者场景 2 中的 S907-S922、或者场景 3 中的 S1007-S1021、或者场景 4 中的 S1107-S1121，具体实现原理与场景 1-场景 4 类似，可参考理解，不再赘述。

场景 6：

示例性的，图 13 为本申请实施例提供的通信方法的流程示意图六。该通信方法主要适用于远端 UE、中继 UE、AMF 网元、AUSF 网元、以及 UDM 网元之间的通信。AMF 网元可以包括：中继 AMF 网元和远端 AMF 网元，二者可以是同一或不同的 AMF 网元，对此不做具体限定。AUSF 网元可以包括：中继 AUSF 网元和远端 AUSF 网元，二者可以是不同的 AUSF 网元。UDM 网元可以是远端 UDM 网元，或者也可以其他任何可能形态的 UDM 网元，对此不做具体限定。在场景 6 中，UDM 网元可以判断远端 UE 是否执行过认证。在执行过认证的情况下，可直接推演 ProSe 密钥，无需再次认证。

具体的，如图 13 所示，该通信方法的流程如下：

S1301，远端 UE 注册到网络，从网络获取 ProSe 通信策略信息。

S1302，中继 UE 注册到网络，从网络获取 ProSe 通信策略信息。

其中，S1301-S1302 的具体实现原理与上述 S801-S802 类似，可参考理解，不再赘述。

S1303，远端 UE 执行中继发现流程。

远端 UE 若要采用 ProSe 中继通信，可通过执行中继发现流程来发现中继 UE。

S1304，远端 UE 向中继 UE 发送直接通信请求消息。相应的，中继 UE 接收来自远端 UE 的直接通信请求消息。

直接通信请求消息可用于远端 UE 请求与中继 UE 通信，包括：远端 UE 的 SUCI、RSC、以及 Nonce_1。

S1305，中继 UE 向中继 AMF 网元发送中继密钥请求消息。相应的，中继 AMF 网元接收来自中继 UE 的中继密钥请求消息。

中继密钥请求消息主要用于中继 UE 请求中继通信，或者说请求 ProSe 中继通信的密钥，包括：中继 UE 的 SUCI、远端 UE 的 SUCI、RSC、以及 Nonce_1。

S1306，中继 AMF 网元验证中继 UE。

其中，S1303-S1306 的具体实现原理与上述 S403-S406 类似，可参考理解，不再赘述。

S1307，中继 AMF 网元向中继 AUSF 网元 UE 认证请求消息/发送 ProSe UE 认证请求消息。相应的，中继 AUSF 网元接收来自中继 AMF 网元的 UE 认证请求消息#1/ProSe UE 认证请求消息#1。

其中，UE 认证请求消息的具体实现原理可以参考上述 S807 中的相关介绍，ProSe UE 认证请求消息的具体实现原理可以参考上述 S1007 中的相关介绍，不再赘述。

S1308，中继 AUSF 网元向 UDM 网元发送 UE 认证获得请求消息/ProSe UE 认证获得请求消息。相应的，UDM 网元接收来自中继 AUSF 网元的 UE 认证获得请求消息/ProSe UE 认证获得请求消息。

其中，UE 认证获得请求消息的具体实现原理可以参考上述 S808 中的相关介绍，ProSe UE 认证获得请求消息的具体实现原理可以参考上述 S1008 中的相关介绍，不再赘述。

S1309，UDM 网元确定远端 UE 是否执行过认证，或确定是否有服务的 AUSF 实例。

UDM 网元接收到 UE 认证获得请求消息/ProSe UE 认证获得请求消息，可从中获得远端 UE 的 SUCI，以根据该 SUCI 查找远端 AUSF 网元的标识。例如，UDM 网元，或者 UDM 网元可以调用 SIDF 解析该 SUCI 获得 SUPI，从而根据 SUPI 获取存储在 UDM 网元中的远端 UE 的上下文，以判断是否能够从上下文中获取远端 AUSF 网元的标识。这种情况下，如果 UDM 网元能够获取远端 AUSF 网元的标识，则表示远端 UE 执行过认证，有服务的 AUSF 实例，可直接从该远端 AUSF 网元获得 ProSe 密钥，即 S1310-S1317，无需再次认证。否则，如果 UDM 网元无法获取远端 AUSF 网元的标识，则表示远端 UE 未执行主认证，没有服务的 AUSF 实例，需要执行 ProSe 认证，即 S1318。

S1310，UDM 网元向远端 AUSF 网元发送 ProSe 密钥请求消息。相应的，远端 AUSF 网元接收来自 UDM 网元的 ProSe 密钥请求消息。

UDM 网元可以根据远端 AUSF 网元的标识，向远端 AUSF 网元发送 ProSe 密钥请求消息。ProSe 密钥请求消息主要用于请求 ProSe 密钥，包括：SUPI、RSC 以及 Nonce_1。远端 AUSF 网元接收到 ProSe 密钥请求消息后，可从中获得 RSC 以及

Nonce_1。这样，远端 AUSF 网元可以根据先前认证远端 UE 时确定 K_{AUSF}、本次生成的 Nonce_2、以及 RSC 和 Nonce_1，推演 ProSe 密钥。其中，推演 ProSe 密钥的具体实现原理可以参考上述 S820 中的相关介绍，不再赘述。

S1311，远端 AUSF 网元向 UDM 网元发送 ProSe 密钥响应消息。相应的，UDM 网元接收来自远端 AUSF 网元的 ProSe 密钥响应消息。

ProSe 密钥响应消息为上述 ProSe 密钥请求消息的响应消息，可以包括：ProSe 密钥和 Nonce_2。

S1312，UDM 网元向中继 AUSF 网元发送 UE 认证获得响应消息/ProSe UE 认证获得响应消息。相应的，中继 A USF 网元接收来自 UDM 网元的 UE 认证获得响应消息/ProSe UE 认证获得响应消息。

UE 认证获得响应消息/ProSe UE 认证获得响应消息中可以包括：ProSe 密钥和 Nonce_2。UE 认证获得响应消息的具体实现原理也可以参考上述 S810 中的相关介绍，ProSe UE 认证获得响应消息的具体实现原理也可以参考上述 S1010 中的相关介绍，不再赘述。

S1313，中继 AUSF 网元向中继 AMF 网元发送 UE 认证响应消息/ProSe UE 认证响应消息。相应的，中继 AMF 网元接收来自中继 AUSF 网元的 UE 认证响应消息/ProSe UE 认证响应消息。

UE 认证响应消息/ProSe UE 认证响应消息中可以包括：ProSe 密钥和 Nonce_2。UE 认证响应消息的具体实现原理也可以参考上述 S812 中的相关介绍，ProSe UE 认证响应消息的具体实现原理也可以参考上述 S1012 中的相关介绍，不再赘述。

S1314，中继 AMF 网元向中继 UE 发送中继密钥响应消息。相应的，中继 UE 接收来自中继 AMF 网元的中继密钥响应消息。

S1315，中继 UE 向远端 UE 发送直接安全模式命令消息。相应的，远端 UE 接收来自中继 UE 的直接安全模式命令消息。

S1316，远端 UE 推演 ProSe 密钥。

S1317，远端 UE 向中继 UE 发送直接安全模式命令完成消息。相应的，中继 UE 接收来自远端 UE 的直接安全模式命令完成消息。

其中，S1314-S1317 的具体实现原理与 S822-S825 类似，可参考理解，不再赘述。

至此，远端 UE 和中继 UE 都获得了相同的 ProSe 密钥，可以基于 ProSe 密钥推演 PC5 连接的会话密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全。此外，在远端 UE 执行过 ProSe 认证的情况，远端 AUSF 网元无需认证即可推演 ProSe 密钥，以有效提高设备运行效率。

S1318，ProSe 认证。

通过执行 ProSe 认证可建立中继 UE 和远端 UE 的安全通信。

其中，S1318 可以为场景 1 中的 S809-S822、或者场景 2 中的 S909-S922、或者场景 3 中的 S1009-S1021、或者场景 4 中的 S1109-S1121，具体实现原理与场景 1-场景 4 类似，可参考理解，不再赘述。

以上结合场景 1-场景 6 介绍了本申请实施例提供的通信方法在各个场景下的具体

流程。下面结合图 14 介绍本申请实施例提供的通信方法在各个场景下的整体流程。

示例性的，图 14 为本申请实施例提供的通信方法的流程示意图七。该通信方法可以适用于远端终端、中继终端、接入和移动管理网元、认证服务网元、以及数据管理网元之间的通信。其中，远端终端可以是上述场景 1-场景 6 中的远端 UE。中继终端可以是上述场景 1-场景 6 中的中继 UE。接入和移动管理网元可以是上述场景 1-场景 6 中的中继 AMF 网元。认证服务网元可以是上述场景 1-场景 6 中的 AUSF 网元。数据管理网元可以是上述场景 1-场景 6 中的 UDM 网元。

如图 14 所示，该通信方法的流程如下：

S1401，接入和移动管理网元向认证服务网元发送认证请求消息#3。相应的，认证服务网元接收来自接入和移动管理网元的认证请求消息#3。

认证请求消息#3 可用于请求认证远端终端。比如，请求认证服务网元认证远端终端，用以触发认证服务网元执行 ProSe 通信的认证流程，确保认证的正确性和可靠性。认证请求消息#3 包括：远端终端的 SUCI，还可以包括如下至少一项：服务网络名称、RSC、随机值#1（例如上述 Nonce_1）或 ProSe 中继通信指示信息（例如上述 ProSe 中继通信指示信息#1）。其中，服务网络名称、RSC 或 ProSe 中继通信指示信息中的任一项可用于指示认证为 ProSe 中继通信的认证，以触发认证服务网元执行 ProSe 通信的认证流程，确保认证的准确性和可靠性，避免对现有流程的影响。服务网络名称、RSC、或随机值#1 中的任一项可用于确定 ProSe 密钥，以便 AUSF 网元在确定认证通过的情况下，可以直接根据这些参数推演 ProSe 密钥，无需额外获取，以提高密钥推演效率。认证请求消息#3 具体可以为上述 UE 认证请求消息#1，或者 ProSe UE 认证请求消息#1，具体实现原理可以参考上述 S807、S907、S1007、或 S1107 中的相关介绍，不再赘述。

可选地，若认证请求消息#3 中包括：RSC 和随机值#1，则认证服务网元还可以保存 RSC 和随机值#1，以便后续密钥推演时可直接使用，无需再次获取，以进一步提高密钥推演效率。

S1402，认证服务网元向数据管理网元发送认证请求消息#1。相应的，数据管理网元接收来自认证服务网元的认证请求消息#1。

认证请求消息#1 可以用于请求认证远端终端。例如，认证请求消息#1 包括如下至少一项：远端终端的 SUCI、服务网络名称、RSC 或 ProSe 中继通信指示信息，例如 ProSe 中继通信指示信息为上述 ProSe 中继通信指示信息#2，ProSe 中继通信指示信息用于指示认证为 ProSe 中继通信的认证。如此，认证请求消息#1 触发数据管理网元获取 ProSe 中继通信对应的认证向量，确保 ProSe 中继通信认证的正确性和可靠性。认证请求消息#1 可以为上述 UE 认证获得请求消息，或者 ProSe UE 认证获得请求消息，具体实现原理可以参考上述 S808、S908、S1008、或 S1108 中的相关介绍，不再赘述。

可选地，认证服务网元向数据管理网元发送认证请求消息#1 还可以包括：认证服务网元根据来自移动与接入管理网元的认证请求消息#3 生成认证请求消息#1，然后向数据管理网元发送认证请求消息#1。

S1403，数据管理网元向认证服务网元发送认证响应消息#1。相应的，认证服务

网元接收来自数据管理网元的认证响应消息#1。

认证响应消息#1 可以为上述 UE 认证获得响应消息，或者 ProSe UE 认证获得响应消息。认证响应消息#1 包括：ProSe 认证信息#1。ProSe 认证信息#1 可以包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。

具体的，ProSe 认证信息#1 可以为如下至少一项：AKA 的 ProSe 认证向量#1（例如 5G AKA 的 ProSe 认证向量#1）、或 EAP-AKA’的 ProSe 的认证向量。也就是说，远端 UE 与网络之间的认证可以基于对已有认证方法，例如 5G AKA 或 EAP-AKA’增强实现，以实现在不引入新的认证方法的情况下，确保 ProSe 中继通信安全。

在 ProSe 认证信息#1 为 AKA 的 ProSe 认证向量#1 的情况下，其可以包括如下至少一项：用于远端终端认证网络的信息，例如上述 RAND 和 AUTN、用于认证服务网元认证远端终端的信息，例如上述 XRES*、或用于确定 ProSe 密钥的信息，例如上述 K_{AUSF}。

或者，在 ProSe 认证信息#1 为 EAP-AKA’的 ProSe 的认证向量的情况下，其可以包括如下至少一项：用于远端终端认证网络的信息，例如上述 RAND 和 AUTN、用于认证服务网元认证远端终端的信息，例如上述 XRES、或用于确定 ProSe 密钥的信息，例如上述 CK 和 IK。

可选地，认证响应消息#1 还可以包括：指示信息，用于指示 ProSe 认证信息#1 为认证方法对应的认证信息，如指示认证信息为 EAP-AKA’机制的认证信息或 5G AKA 机制的认证信息。可选地，该指示信息还用于指示认证信息为用于 ProSe 通信的认证信息，或者说支持 ProSe 通信的认证。也就是说，该指示信息可以用于指示认证信息为支持的 ProSe 中继通信的 EAP-AKA’或 5G AKA 的认证信息，也即增强的 EAP-AKA’或 AKA 的认证信息。其中，增强的 EAP-AKA’机制或 5G AKA 机制可以理解为：在认证流程中，有任一参与认证的网元使用新的认证向量生成方法确定认证向量、使用新的消息、使用新的服务操作、或者新增信元，则可认为是增强的 EAP-AKA’机制或 5G AKA 机制。

可选地，在 S1403 之前，数据管理网元还可以确定远端终端授权获取中继服务。也就是说，在确定远端终端有使用中继通信的权限的基础上，才对其进行 ProSe 中继通信认证，避免无效认证。以及，在 S1403 之前，数据管理网元可以根据认证请求消息#1，确定 ProSe 认证信息#1。

可选地，在 S1403 之前，若触发 ProSe 中继通信的认证，或者说认证远端终端的流程，则数据管理网元可以选择支持的 ProSe 中继通信的 EAP-AKA’机制或 5G AKA 机制，也即增强的 EAP-AKA’机制或 AKA 机制。数据管理网元也可以选择已有的 EAP-AKA’机制或 5G AKA 机制，保证针对 ProSe 中继通信场景，相关网元仅需要支持一种流程的增强逻辑即可实现，降低复杂度。其中，数据管理网元选择的已有的 EAP-AKA’机制或 5G AKA 机制可以理解为：数据管理网元使用已有的方法推演认证向量和使用已有的服务操作等。

此外，S1403 的具体实现原理可以参考上述 S809-S810、S909-S910、S1009-S1010、或 S1109-S1110 中的相关介绍，不再赘述。

S1404，认证服务网元向接入和移动管理网元发送认证响应消息#3。相应的，接入和移动管理网元接收来自认证服务网元的认证响应消息#3。

认证响应消息#3 可以为上述 UE 认证响应消息#1，或者 ProSe UE 认证响应消息#1。认证响应消息#3 包括：ProSe 认证信息#2。ProSe 认证信息#2 包括：用于远端终端认证网络的信息。可选地，ProSe 认证信息#2 还可以包括：用于网络认证远端终端的信息。也就是说，ProSe 中继通信的认证可以由接入和移动管理网元触发，例如在业务有需求的情况下触发，以便认证服务网元可以有针对性地执行认证，确保认证的有效性。

具体的，ProSe 认证信息#2 可根据 ProSe 认证信息#1 确定。ProSe 认证信息#2 可以为如下至少一项：AKA 的 ProSe 认证向量#2（例如 5G AKA 的 ProSe 认证向量#2）、或 EAP 请求消息或 AKA’挑战消息。例如，如果采用已有的 AKA 认证机制，则 AKA 的 ProSe 认证向量#2 可根据 AKA 的 ProSe 认证向量#1 确定，无需引入新的功能，从而降低网元复杂度。如果采用增强的 EAP-AKA’认证机制，则 EAP 请求消息或 AKA’挑战消息可根据 EAP-AKA’的 ProSe 的认证向量确定，无需引入新的功能，从而降低网元复杂度。

在 ProSe 认证信息#2 为 AKA 的 ProSe 认证向量#2 的情况下，其可包括如下至少一项：用于远端终端认证网络的信息，例如 RAND 和 AUTN、或用于接入和移动管理网元认证远端终端的信息，例如上述 HXRES*。如此，AKA 的 ProSe 认证向量#2 不仅可用于远端终端认证网络，还可用于接入和移动管理网元从服务网的角度认证远端终端，从而可以提高认证的全面性，进一步确保 ProSe 中继通信安全。

或者，在 ProSe 认证信息#2 为 EAP 请求消息或 AKA’挑战消息的情况下，其可包括：用于远端终端认证网络的信息，例如 RAND 和 AUTN。也就是说，认证服务网元将 ProSe 认证信息#1 中用于远端终端认证网络的信息，封装到 EAP 请求消息或 AKA’挑战消息中，可实现将该消息作为容器向接入和移动管理网元发送，以便接入和移动管理网元直接透传该消息，以提高处理效率，降低开销。

可选地，认证服务网元跳过推演用于远端终端与网络之间通信的密钥，例如 K_{SEAF}，以防止生成冗余的信息，造成资源的浪费或对现有机制的影响。例如，认证服务网元可以根据本地存储的信息（如 RSC 或 Nonce_1）或接收到的认证响应消息#1，确定跳过推演用于远端终端与网络通信的密钥。

此外，S1404 的具体实现原理可以参考上述 S811-S812、S911-S912、S1011-S1012、或 S1111-S1112 中的相关介绍，不再赘述。

S1405，接入和移动管理网元向中继终端发送用于远端终端认证网络的信息。相应的，中继终端接收来自接入和移动管理网元的用于远端终端认证网络的信息。

用于远端终端认证网络的信息可以包括：RAND 和 AUTN 的 EAP 请求消息/AKA’挑战消息，或者直接包括：RAND 和 AUTN，或者包括：容器，该容器中包括：RAND 和 AUTN。用于远端终端认证网络的信息可以承载在消息中。例如，ProSe 通信认证请求消息，或者其他任何可能的消息中，对此不做具体限定。该消息的名称或携带的指示信息，可用于指示需要由远端终端执行 ProSe 中继通信的认证流程。如此，中继终端可以根据该消息，向远端终端发送用于远端终端认证网络的信

息，避免中继终端执行其他操作，例如自行认证，确保 ProSe 中继通信认证的可靠性。此外，该消息为通过通信密钥保护的消息，也即该用于远端终端认证网络的信息为通过通信密钥保护的信息。该通信密钥用于中继终端与网络的通信，以确保中继终端与网络之间的通信安全。

可选地，接入和移动管理网元向中继终端发送远端终端认证网络的信息前，接入和移动管理网元跳过获取 ngKSI 和 ABBA 参数，或者接入和移动管理网元跳过生成密钥集标识和反降级参数。接入和移动管理网元不向中继终端发送 ngKSI 和 ABBA 参数。

此外，S1405 的具体实现原理可以参考上述 S813、S913、S1013、或 S1113 中的相关介绍，不再赘述。

S1406，中继终端向远端终端发送用于远端终端认证网络的信息。相应的，远端终端接收来自中继终端的用于远端终端认证网络的信息。

用于远端终端认证网络的信息可以包括：携带有 RAND 和 AUTN 的 EAP 请求消息/ AKA’挑战消息，或者直接包括：RAND 和 AUTN，或者包括：容器，该容器中包括：RAND 和 AUTN。用于远端终端认证网络的信息可以承载在消息中，例如远端终端认证请求消息，或者其他任何可能的消息中，对此不做具体限定。可选地，该消息的名称或携带的指示信息，可以指示需要由远端终端执行 ProSe 中继通信的认证流程或指示请求认证远端 UE。如此，中继终端向远端终端发送用于远端终端认证网络的信息，可以包括：中继终端根据消息，向远端终端发送用于远端终端认证网络的信息，以确保 ProSe 中继通信认证的可靠性。例如，中继终端根据该消息的名称或消息中包含的指示信息，向远端终端发送用于远端终端认证网络的信息。此外，该消息可以为上述远端 UE 认证请求消息，具体实现原理可以参考上述 S814、S914、S1014、或 S1114 中的相关介绍，不再赘述。

S1407，远端终端向中继终端发送远端终端确定的认证响应信息。相应的，中继终端接收来自远端终端的认证响应信息。

远端终端确定的认证响应信息用于认证远端终端，例如上述 RES 或 RES*。也就是说，中继终端可以主动与远端终端交互，以确保远端终端能够认证网络，并向网络反馈自身的认证响应消息，确保网络也能够认证远端终端。该远端终端确定的认证响应信息可以承载在远端终端认证响应消息，或者其他任何可能的消息中，对此不做具体限定。远端终端认证响应消息可以为上述远端 UE 认证响应消息，具体实现原理可以参考上述 S815-S816、S915-S916、S1015-S1016、或 S1115-S1116 中的相关介绍，不再赘述。

可选地，远端终端跳过推演用于远端终端与网络之间通信的密钥，例如 K_{SEAF}。

S1408，中继终端向接入和移动管理网元发送远端终端确定的认证响应信息。相应的，接入和移动管理网元接收来自中继终端的远端终端确定的认证响应信息。

远端终端确定的认证响应信息用于认证远端终端，例如上述 RES 或 RES*。该远端终端确定的认证响应信息可以承载在 ProSe 通信认证响应消息，或者其他任何可能的消息中，对此不做具体限定。ProSe 通信认证响应消息为通过通信密钥保护的消息，也即该远端终端确定的认证响应信息为通过通信密钥保护的信息，以确保中继终

端与网络之间的通信安全。例如，通信密钥为中继终端与接入和移动管理网元之间建立的非接入层安全密钥，该非接入层安全密钥可以包含加密密钥和完整性保护密钥。此外，S1408 的具体实现原理可以参考上述 S817、S917、S1017、或 S1117 中的相关介绍，不再赘述。

S1409，接入和移动管理网元向认证服务网元发送认证请求消息#2。相应的，认证服务网元接收来自接入和移动管理网元的认证请求消息#2。

认证请求消息#2 用于请求认证远端终端。认证请求消息#2 可以包括如下至少一项：远端终端确定的认证响应信息、用于确定 ProSe 密钥的 RSC、或用于确定 ProSe 密钥的随机值#1，认证响应消息用于认证远端终端。也就是说，接入和移动管理网元可以在确定远端终端认证通过的情况下，才向认证服务网元发送用于推演 ProSe 密钥的参数，例如 RSC 和/或随机值#1，从而实现按需提供必要的参数，无需预存信息，防止资源浪费。认证请求消息#2 可以为上述 UE 认证请求消息#2，或者 ProSe UE 认证请求消息#2，具体实现原理可以参考上述 S819、S919、S1018、或 S1118 中的相关介绍，不再赘述。

可选地，在 S1409 之前，认证服务网元还可以保存 RSC 和随机值#1，以便后续密钥推演时可直接使用，无需再次获取，以进一步提高密钥推演效率。例如，用于确定 ProSe 密钥的信息包括中间密钥，例如 K_{AUSF}，或者 CK'和 IK'，或者 K_{PROSE}。在认证远端终端通过的情况下，认证服务网元根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密钥，确定 ProSe 密钥。也就是说，认证服务网元可以根据业务场景以及密钥隔离等需求，选择合适的参数来确定 ProSe 密钥，以适应更多业务场景。例如，根据 RSC、随机值#1、随机值#2 和中间密钥确定 ProSe 密钥。例如，根据服务网络名称、随机值#1、随机值#2 和中间密钥确定 ProSe 密钥。例如，根据中间密钥、RSC 和远端终端的 SUPI 推演临近业务中间密钥，再根据临近业务中间密钥、随机值#1 和随机值#2 确定 ProSe 密钥，或者还可以通过其他组合方式确定 ProSe 密钥，这里不一一列举。

S1410，认证服务网元向接入和移动管理网元发送认证响应消息#2。相应的，接入和移动管理网元接收来自认证服务网元的发送认证响应消息#2。

认证响应消息#2 中包括：ProSe 密钥。该 ProSe 密钥用于中继终端与远端终端的通信。可选地，认证响应消息#2 中还可以包括：随机值#2。随机值#2 用于确定 ProSe 密钥，以便远端终端在确定认证通过的情况下，可以直接根据随机值#2 推演 ProSe 密钥，保证为远端 UE 的不同 ProSe 通信推演不同的密钥，实现密钥的隔离。认证请求消息#2 可以为上述 UE 认证响应消息#2，或者 ProSe UE 认证响应消息#2，具体实现原理可以参考上述 S820-S821、S920-S921、S1019-S1020、或 S1119-S1120 中的相关介绍，不再赘述。

可选地，认证响应消息#2 中还可以包括如下至少一项：远端终端的用户隐藏标识 SUPI、或 EAP 成功消息。EAP 成功消息可以用于指示网络认证远端终端成功。该远端终端的 SUPI 用于指示中继终端需要向网络上报远端 UE 的信息。

S1411，接入和移动管理网元向中继终端发送 ProSe 密钥。相应的，中继终端接收来自接入和移动管理网元的 ProSe 密钥。

可选地，接入和移动管理网元还可以向中继终端发送远端终端的 SUPI，用以指示中继终端需要向网络上报远端 UE 的信息。

可选地，接入和移动管理网元还可以向中继终端发送 EAP 成功消息，用以指示网络认证远端终端成功。

其中，S1411 的具体实现原理可以参考上述 S822、S922、S1021、或 S1121 中的相关介绍，不再赘述。

之后，可选地，远端终端和中继终端可以基于 ProSe 密钥推演 PC5 连接的通信保护密钥，例如，远端终端和中继终端可以基于 ProSe 密钥推演一个会话密钥，然后远端终端和中继终端基于会话密钥进一步推演通信保护密钥（如加密密钥和完整性保护密钥），本申请不限制。

可选地，第一种可能的应用场景，如果为 AKA 的 ProSe 认证，则在 S1408 之后，以及在 S1409 之前，接入和移动管理网元可以根据远端终端确定的认证响应消息（上述基于 RES*推演的 XRES*），以及用于接入和移动管理网元认证远端终端的信息（上述 HXRES*），确定远端终端认证通过。即实现接入和移动管理网元从服务网的角度认证远端终端，从而可以提高认证的全面性，进一步确保 ProSe 中继通信安全。第一种可能的应用场景的具体实现原理，也可以参考上述 S818 或 S918 中的相关介绍，不再赘述。

可选地，第二可能的应用场景，在 S1410 之后，接入和移动管理网元可以向中继终端发送随机值#2。相应的，中继终端可以接收来自接入和移动管理网元的随机值#2。如此，中继终端可以向远端终端发送随机值#2，以便远端终端接收来自中继终端的随机值#2，以根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密钥，确定 ProSe 密钥。可以看出，接入和移动管理网元可以在网络认证远端终端通过后，才向远端终端发送用于推演 ProSe 密钥的参数，也即随机值#2，避免这些参数在认证通过前提前暴露，确保认证通过前的通信安全。此外，第二可能的应用场景的具体实现原理，也可以参考上述 S822-S825、S922-S925、S1021-S1023、或 1121-S1124 中的相关介绍，不再赘述。

可选地，第三可能的应用场景，在 S1401 之前，接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥（如 K_{AUSF}）。换言之，只有在远端终端没有执行过认证的情况下或不存在用于推演 ProSe 密钥的密钥，才执行 ProSe 中继通信的认证流程，避免因重复执行认证流程而导致资源浪费。当然，在对远端终端执行过认证的情况下，可使用认证服务网元上已有的密钥（如 K_{AUSF}）推演 ProSe 密钥，无需再次执行 ProSe 中继通信认证。

具体的，接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥，可以包括：接入和移动管理网元接收来自中继终端的远端终端指示信息，远端终端指示信息用于指示远端终端未执行认证或不存在用于推演 ProSe 密钥的密钥。接入和移动管理网元根据远端终端指示信息，确定未对远端终端执行过 ProSe 中继通信的认证。

或者，接入和移动管理网元确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥，可以包括：接入和移动管理网元向数据管理网元发送认证服务网

元获得请求消息，并接收来自数据管理网元的认证服务网元获得响应消息。其中，认证服务网元获得请求消息用于请求认证服务网元的标识，该认证服务网元用于远端终端的 ProSe 中继通信认证。认证服务网元获得响应消息未携带该认证服务网元的标识，用以表示未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥。接入和移动管理网元根据认证服务网元获得响应消息，确定未对远端终端执行过认证或不存在用于推演 ProSe 密钥的密钥。

可以看出，在远端终端指示其是否执行过认证的情况下或不存在用于推演 ProSe 密钥的密钥，接入和移动管理网元可根据远端终端的指示信息，而不用再与其他网元交互，便可确定是否执行 ProSe 中继通信的认证。或者，远端终端可以不指示其是否执行过 ProSe 中继通信的认证，由接入和移动管理网元根据数据管理网元反馈的信息确定，如此可以降低远端终端与接入和移动管理网元之间的通信开销，提高通信效率。

此外，第三可能的应用场景的具体实现原理，也可以参考上述场景 5 中的相关介绍，不再赘述。

可选地，第四可能的应用场景，在 S1403 之前， 数据管理网元确定未对远端终端执行过认证，或确定不存在用于推演 ProSe 密钥的密钥，或确定为远端终端服务的 AUSF 网元。换言之，只有在远端终端没有执行过认证，或不存在用于推演 ProSe 密钥的密钥，或不存在为远端终端服务的 AUSF 网元的情况下，才执行 ProSe 中继通信的认证流程，避免因重复执行认证流程而导致资源浪费。当然，在对远端终端执行过认证的情况下，数据管理网元可以请求认证服务网元使用已有的密钥（如 K_{AUSF}）推演 ProSe 密钥，无需再次执行 ProSe 中继通信认证。

此外，第四可能的应用场景的具体实现原理，也可以参考上述场景 6 中的相关介绍，不再赘述。

综上，基于图 8-图 14 中任一项所示的通信方法，通过数据管理网元提供的 ProSe 认证信息#1，远端终端和网络可以彼此认证对方。在双方都认证通过的情况下，便可生成用于远端 UE 和中继 UE 通信的 ProSe 密钥，以便基于 ProSe 密钥推演 PC5 连接（即远端 UE 和中继 UE 间的连接）的通信保护密钥，例如加密密钥和完整性保护密钥，以确保 ProSe 中继通信安全，避免出现因被攻击而导致用户信息泄露等情况。

以上结合图 8-图 14 详细说明了本申请实施例提供的通信方法。以下结合图 15-图 16 详细说明用于执行本申请实施例提供的通信方法的通信装置。

示例性地，图 15 是本申请实施例提供的通信装置的结构示意图一。如图 15 所示，通信装置 1500 包括：接收模块 1501 和发送模块 1502。为了便于说明，图 15 仅示出了该通信装置的主要部件。

一些实施例中，通信装置 1500 可适用于图 7 中所示出的通信系统中，执行图 8-图 13 中所示出的通信方法中 AUSF 网元的功能，或者适用于图 7 中所示出的通信系统中，执行图 14 中所示出的通信方法中认证服务网元的功能。

其中，发送模块 1502，用于向数据管理网元发送认证请求消息#1。接收模块 1501，用于接收来自数据管理网元的认证响应消息#1。认证请求消息#1 用于请求认

证远端终端，认证响应消息#1 包括：临近业务 ProSe 认证信息#1，ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。如此，在远端终端认证网络通过的情况下，接收模块 1501，还用于接收来自接入和移动管理网元的认证请求消息#2，并在认证远端终端通过的情况下，发送模块 1502，还用于向接入和移动管理网元发送认证响应消息#2。其中，认证请求消息#2 用于请求认证远端终端；认证响应消息#2 包括：ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，ProSe 认证信息#1 可以为如下至少一项：第 5 代通信系统认证与密钥协商 AKA 的 ProSe 认证向量#1、或扩展认证协议请求 EAP-AKA’的 ProSe 的认证向量。

可选地，AKA 的 ProSe 认证向量#1 或 EAP-AKA’的 ProSe 的认证向量可以包括如下至少一项：用于远端终端认证网络的信息、用于认证服务网元认证远端终端的信息、或用于确定 ProSe 密钥的信息。

可选地，接收模块 1501，还用于在发送模块 1502 向数据管理网元发送认证请求消息#1 之前，接收来自接入和移动管理网元的认证请求消息#3。相应的，在认证服务网元接收来自数据管理网元的认证响应消息#1 之后，发送模块 1502，还用于在接收模块 1501 接收来自接入和移动管理网元的认证请求消息#2 之前，向接入和移动管理网元发送认证响应消息#3。认证响应消息#3 可以包括：ProSe 认证信息#2，ProSe 认证信息#2 包括：用于远端终端认证网络的信息。

进一步的，ProSe 认证信息#2 可根据 ProSe 认证信息#1 确定。ProSe 认证信息#2 可以为如下至少一项：AKA 的 ProSe 认证向量#2、或 EAP 请求消息或 AKA’挑战消息。其中，AKA 的 ProSe 认证向量#2 可根据 AKA 的 ProSe 认证向量#1 确定。EAP 请求消息或 AKA’挑战消息可根据 EAP-AKA’的 ProSe 的认证向量确定。

进一步的，AKA 的 ProSe 认证向量#2 可以包括如下至少一项：用于远端终端认证网络的信息、或用于接入和移动管理网元认证远端终端的信息。

进一步的，EAP 请求消息或 AKA’挑战消息可以包括：用于远端终端认证网络的信息。

可选地，认证请求消息#3 可用于请求认证远端终端。

进一步的，认证请求消息#3 可以包括如下至少一项：远端终端的用户隐藏标识 SUCI、服务网络名称、中继服务码 RSC、随机值#1、或 ProSe 中继通信指示信息。其中，服务网络名称、RSC 或 ProSe 中继通信指示信息中的任一项可用于指示认证为 ProSe 中继通信的认证。服务网络名称、RSC、或随机值#1 中的任一项可用于确定 ProSe 密钥。

进一步的，通信装置 1500 还可以包括：处理模块（图 15 中未示出）。处理模块，用于在发送模块 1502 向接入和移动管理网元发送认证响应消息#2 之前，若认证请求消息#3 中包括：RSC 和随机值#1，则保存 RSC 和随机值#1。

进一步的，用于确定 ProSe 密钥的信息包括：中间密钥。处理模块，还用于在发送模块 1502 向接入和移动管理网元发送认证响应消息#2 之前，在认证远端终端通过的情况下，根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密

钥，确定 ProSe 密钥。

一种可能的设计方案中，认证请求消息#2 可以包括如下至少一项：远端终端确定的认证响应信息、用于确定 ProSe 密钥的 RSC、或用于确定 ProSe 密钥的随机值#1，认证响应消息用于认证远端终端。

可选地，认证响应消息#2 可以包括：随机值#2。随机值#2 用于确定 ProSe 密钥。

进一步的，认证响应消息#2 还可以包括如下至少一项：远端终端的 SUPI、或 EAP 成功消息。

一种可能的设计方案中，认证服务网元跳过推演用于远端终端与网络之间通信的密钥。

可选地，接收模块 1501 和发送模块 1502 也可以集成为一个模块，如收发模块（图 15 中未示出）。其中，收发模块用于实现通信装置 1500 的发送功能和接收功能。

可选地，通信装置 1500 还可以包括存储模块（图 15 中未示出），该存储模块存储有程序或指令。当处理模块执行该程序或指令时，使得通信装置 1500 可以执行图 8-图 13 中任一项所示出的通信方法中 AUSF 网元的功能，或者执行图 14 所示出的通信方法中认证服务网元的功能。

应理解，通信装置 1500 中涉及的处理模块可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1500 可以是网络设备，例如 AUSF 网元或者认证服务网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，通信装置 1500 的技术效果可以参考图 8-图 14 中任一项所示出的通信方法的技术效果，此处不再赘述。

另一些实施例中，通信装置 1500 可适用于图 7 中所示出的通信系统中，执行图 8-图 13 中所示出的通信方法中中继 AMF 网元的功能，或者适用于图 7 中所示出的通信系统中，执行图 14 中所示出的通信方法中接入和移动管理网元的功能。

其中，发送模块 1502，用于向认证服务网元发送认证请求消息#3，接收模块 1501，用于接收来自认证服务网元的认证响应消息#3。认证响应消息#3 包括：ProSe 认证信息#2，ProSe 认证信息#2 包括：用于远端终端认证网络的信息。如此，在远端终端认证网络通过的情况下，发送模块 1502，还用于向认证服务网元发送认证请求消息#2，并在认证远端终端通过的情况下，接收模块 1501，还用于接收来自认证服务网元的认证响应消息#2，以便发送模块 1502 向中继终端发送 ProSe 密钥。其中，认证请求消息#2 用于请求认证远端终端。认证响应消息#2 包括：ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，ProSe 认证信息#2 可以为如下至少一项：AKA 的 ProSe 认证向量#2、或 EAP 请求消息或 AKA’挑战消息。

可选地，AKA 的 ProSe 认证向量#2 可包括如下至少一项：用于远端终端认证网

络的信息、或用于接入和移动管理网元认证远端终端的信息。

可选地，EAP 请求消息或 AKA’挑战消息可包括：用于远端终端认证网络的信息。

一种可能的设计方案中，在接收模块 1501 接收来自认证服务网元的认证响应消息#3 之后，在发送模块 1502 向认证服务网元发送认证请求消息#2 之前，发送模块 1502，还用于向中继终端发送用于远端终端认证网络的信息，接收模块 1501，还用于接收来自中继终端的远端终端确定的认证响应信息。该认证响应信息用于认证远端终端。

可选地，在 ProSe 认证信息#2 可以包括：用于接入和移动管理网元认证远端终端的信息的情况下，通信装置 1500 还可以包括：处理模块（图 15 中未示出）。处理模块，还用于在接收模块 1501 接收来自中继终端的远端终端认证响应消息之后，以及在发送模块 1502 向认证服务网元发送认证请求消息#2 之前，根据远端终端确定的认证响应消息，以及用于接入和移动管理网元认证远端终端的信息，确定远端终端认证通过。

可选地，用于远端终端认证网络的信息和远端终端确定的认证响应信息为通过通信密钥保护的信息，通信密钥用于中继终端与网络的通信。

可选地，认证请求消息#2 可以包括如下至少一项：远端终端确定的认证响应消息、用于确定 ProSe 密钥的 RSC、或用于确定 ProSe 密钥的随机值#1，认证响应消息用于认证远端终端。

可选地，认证响应消息#2 可以包括：随机值#2，随机值#2 用于确定 ProSe 密钥。

进一步的，认证响应消息#2 还可以包括如下至少一项：远端终端的 SUPI、或 EAP 成功消息。

进一步的，发送模块 1502，还用于在接收模块 1501 接收来自认证服务网元的认证响应消息#2 之后，向中继终端发送随机值#2。

一种可能的设计方案中，处理模块，还用于在发送模块 1502 向认证服务网元发送认证请求消息#3 之前，确定未对远端终端执行过 ProSe 中继通信的认证。

可选地，接收模块 1501，还用于接收来自中继终端的远端终端指示信息，远端终端指示信息用于指示远端终端未执行 ProSe 执行通信的认证。处理模块，还用于根据远端终端指示信息，确定未对远端终端执行过 ProSe 中继通信的认证。

可选地，发送模块 1502，还用于向数据管理网元发送认证服务网元获得请求消息，接收模块 1501，还用于接收来自数据管理网元的认证服务网元获得响应消息。其中，认证服务网元获得请求消息用于请求认证服务网元的标识，该认证服务网元用于远端终端的 ProSe 中继通信认证。认证服务网元获得响应消息未携带该认证服务网元的标识，用以表示未对远端终端执行过 ProSe 中继通信的认证。如此，处理模块，还用于根据认证服务网元获得响应消息，确定未对远端终端执行过 ProSe 中继通信的认证。

可选地，接收模块 1501 和发送模块 1502 也可以集成为一个模块，如收发模块（图 15 中未示出）。其中，收发模块用于实现通信装置 1500 的发送功能和接收功

能。

可选地，通信装置 1500 还可以包括存储模块（图 15 中未示出），该存储模块存储有程序或指令。当处理模块执行该程序或指令时，使得通信装置 1500 可以执行图 8-图 13 中任一项所示出的通信方法中中继 AMF 网元的功能，或者执行图 14 所示出的通信方法中接入和移动管理网元的功能。

应理解，通信装置 1500 中涉及的处理模块可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1500 可以是网络设备，例如中继 AMF 网元或者接入和移动管理网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，通信装置 1500 的技术效果可以参考图 8-图 14 中任一项所示出的通信方法的技术效果，此处不再赘述。

又一些实施例中，通信装置 1500 可适用于图 7 中所示出的通信系统中，执行图 8-图 13 中所示出的通信方法中 UDM 网元的功能，或者适用于图 7 中所示出的通信系统中，执行图 14 中所示出的通信方法中数据管理网元的功能。

其中，接收模块 1501，用于接收来自认证服务网元的认证请求消息#1，发送模块 1502，用于向认证服务网元发送认证响应消息#1。认证响应消息#1 包括：ProSe 认证信息#1。ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。

一种可能的设计方案中，ProSe 认证信息#1 可以为如下至少一项：AKA 的 ProSe 认证向量#1、或 EAP-AKA’的 ProSe 的认证向量。

可选地，AKA 的 ProSe 认证向量#1 或 EAP-AKA’的 ProSe 的认证向量可以包括如下至少一项：用于远端终端认证网络的信息、用于认证服务网元认证远端终端的信息、或用于确定 ProSe 密钥的信息。

可选地，在接收模块 1501 接收来自认证服务网元的认证请求消息#1 之前，第三方面所述的方法还可以包括：接收模块 1501，还用于接收来自接入和移动管理网元的认证服务网元获得请求消息，发送模块 1502，还用于向接入和移动管理网元发送认证服务网元获得响应消息。其中，认证服务网元获得请求消息用于请求认证服务网元的标识，该认证服务网元用于远端终端的 ProSe 中继通信认证。认证服务网元获得响应消息未携带该认证服务网元的标识，用以表示未对远端终端执行过 ProSe 中继通信的认证。

一种可能的设计方案中，通信装置 1500 还可以包括：处理模块（图 15 中未示出）。处理模块，还用于在发送模块 1502 向认证服务网元发送认证响应消息#1 之前，确定远端终端授权获取中继服务。

一种可能的设计方案中，处理模块，还用于在发送模块 1502 向认证服务网元发送认证响应消息#1 之前，根据认证请求消息#1，确定 ProSe 认证信息#1。

一种可能的设计方案中，处理模块，还用于在发送模块 1502 向认证服务网元发送认证响应消息#1 之前，确定未对远端终端执行过 ProSe 中继通信的认证。

可选地，接收模块 1501 和发送模块 1502 也可以集成为一个模块，如收发模块（图 15 中未示出）。其中，收发模块用于实现通信装置 1500 的发送功能和接收功能。

可选地，通信装置 1500 还可以包括存储模块（图 15 中未示出），该存储模块存储有程序或指令。当处理模块执行该程序或指令时，使得通信装置 1500 可以执行图 8-图 13 中任一项所示出的通信方法中 UDM 网元的功能，或者执行图 14 所示出的通信方法中数据管理网元的功能。

应理解，通信装置 1500 中涉及的处理模块可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1500 可以是网络设备，例如 UDM 网元或者数据管理网元，也可以是可设置于网络设备中的芯片（系统）或其他部件或组件，还可以是包含网络设备的装置，本申请对此不做限定。

此外，通信装置 1500 的技术效果可以参考图 8-图 14 中任一项所示出的通信方法的技术效果，此处不再赘述。

再一些实施例中，通信装置 1500 可适用于图 7 中所示出的通信系统中，执行图 8-图 13 中所示出的通信方法中中继 UE 的功能，或者适用于图 7 中所示出的通信系统中，执行图 14 中所示出的通信方法中中继终端的功能。

其中，接收模块 1501，用于接收来自接入和移动管理网元的用于远端终端认证网络的信息，发送模块 1502，用于向接入和移动管理网元发送远端终端确定的认证响应信息。该认证响应信息用于认证远端终端。如此，接收模块 1501，还用于接收来自接入和移动管理网元的 ProSe 密钥，ProSe 密钥用于中继终端与远端终端的通信。

一种可能的设计方案中，用于远端终端认证网络的信息和远端终端确定的认证响应信息为通过通信密钥保护的信息，通信密钥用于中继终端与网络的通信。

一种可能的设计方案中，在接收模块 1501 接收来自接入和移动管理网元的用于远端终端认证网络的信息之后，在发送模块 1502 向接入和移动管理网元发送远端终端确定的认证响应信息之前，发送模块 1502，还用于向远端终端发送用于远端终端认证网络的信息，接收模块 1501，还用于接收来自远端终端的远端终端确定的认证响应信息。

可选地，用于远端终端认证网络的信息可以承载在消息中，该消息的名称或携带的指示信息，可以指示需要由远端终端执行 ProSe 中继通信的认证流程。如此，处理模块，还用于根据消息，控制发送模块 1502 向远端终端发送用于远端终端认证网络的信息。

一种可能的设计方案中，在发送模块 1502 向接入和移动管理网元发送的 ProSe 通信认证响应消息之后，接收模块 1501，还用于接收来自接入和移动管理网元的随机值#2，发送模块，还用于向远端终端发送随机值#2。随机值#2 用于确定 ProSe 密钥，该 ProSe 密钥用于中继终端与远端终端的通信。

可选地，接收模块 1501 和发送模块 1502 也可以集成为一个模块，如收发模块

（图 15 中未示出）。其中，收发模块用于实现通信装置 1500 的发送功能和接收功能。

可选地，通信装置 1500 还可以包括处理模块（图 15 中未示出），该处理模块用于实现该通信装置 1500 的处理功能。

可选地，通信装置 1500 还可以包括存储模块（图 15 中未示出），该存储模块存储有程序或指令。当处理模块执行该程序或指令时，使得通信装置 1500 可以执行图 8-图 13 中任一项所示出的通信方法中中继 UE 的功能，或者执行图 14 所示出的通信方法中中继终端的功能。

应理解，通信装置 1500 中涉及的处理模块可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1500 可以是终端，例如中继 UE 或者中继终端，也可以是可设置于终端中的芯片（系统）或其他部件或组件，还可以是包含终端的装置，本申请对此不做限定。

此外，通信装置 1500 的技术效果可以参考图 8-图 14 中任一项所示出的通信方法的技术效果，此处不再赘述。

还一些实施例中，通信装置 1500 可适用于图 7 中所示出的通信系统中，执行图 8-图 13 中所示出的通信方法中远端 UE 的功能，或者适用于图 7 中所示出的通信系统中，执行图 14 中所示出的通信方法中远端终端的功能。

其中，接收模块 1501，用于接收来自中继终端的用于远端终端认证网络的信息。如此，在确定认证网络通过的情况下，发送模块 1502，用于向中继终端发送远端终端确定的认证响应信息，该认证响应信息用于认证远端终端。

一种可能的设计方案中，通信装置 1500 还可以包括：处理模块（图 15 中未示出）。在发送模块 1502 向中继终端发送远端终端确定的认证响应信息之后，接收模块 1501，还用于接收来自中继终端的随机值#2，处理模块，还用于根据如下至少一项：服务网络名称、RSC、随机值#1、随机值#2 和中间密钥，确定 ProSe 密钥。

可选地，接收模块 1501 和发送模块 1502 也可以集成为一个模块，如收发模块（图 15 中未示出）。其中，收发模块用于实现通信装置 1500 的发送功能和接收功能。

可选地，通信装置 1500 还可以包括存储模块（图 15 中未示出），该存储模块存储有程序或指令。当处理模块执行该程序或指令时，使得通信装置 1500 可以执行图 8-图 13 中任一项所示出的通信方法中远端 UE 的功能，或者执行图 14 所示出的通信方法中远端终端的功能。

应理解，通信装置 1500 中涉及的处理模块可以由处理器或处理器相关电路组件实现，可以为处理器或处理单元；收发模块可以由收发器或收发器相关电路组件实现，可以为收发器或收发单元。

需要说明的是，通信装置 1500 可以是终端，例如远端 UE 或者远端终端，也可以是可设置于终端中的芯片（系统）或其他部件或组件，还可以是包含终端的装置，本申请对此不做限定。

此外，通信装置 1500 的技术效果可以参考图 8-图 14 中任一项所示出的通信方法的技术效果，此处不再赘述。

示例性地，图 16 为本申请实施例提供的通信装置的结构示意图二。该通信装置可以是终端或网络设备，也可以是可设置于终端或网络设备的芯片（系统）或其他部件或组件。如图 16 所示，通信装置 1600 可以包括处理器 1601。可选地，通信装置 1600 还可以包括存储器 1602 和/或收发器 1603。其中，处理器 1601 与存储器 1602 和收发器 1603 耦合，如可以通过通信总线连接。

下面结合图 16 对通信装置 1600 的各个构成部件进行具体的介绍：

其中，处理器 1601 是通信装置 1600 的控制中心，可以是一个处理器，也可以是多个处理元件的统称。例如，处理器 1601 是一个或多个中央处理器（central processing unit，CPU），也可以是特定集成电路（application specific integrated circuit，ASIC），或者是被配置成实施本申请实施例的一个或多个集成电路，例如：一个或多个微处理器（digital signal processor，DSP），或，一个或者多个现场可编程门阵列（field programmable gate array，FPGA）。

可选地，处理器 1601 可以通过运行或执行存储在存储器 1602 内的软件程序，以及调用存储在存储器 1602 内的数据，执行通信装置 1600 的各种功能，例如执行上述图 8-图 14 所示的通信方法。

在具体的实现中，作为一种实施例，处理器 1601 可以包括一个或多个 CPU，例如图 16 中所示出的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，通信装置 1600 也可以包括多个处理器，例如图 16 中所示的处理器 1601 和处理器 1604。这些处理器中的每一个可以是一个单核处理器（single-CPU），也可以是一个多核处理器（multi-CPU）。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

其中，所述存储器 1602 用于存储执行本申请方案的软件程序，并由处理器 1601 来控制执行，具体实现方式可以参考上述方法实施例，此处不再赘述。

可选地，存储器 1602 可以是只读存储器（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）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 1602 可以和处理器 1601 集成在一起，也可以独立存在，并通过通信装置 1600 的接口电路（图 16 中未示出）与处理器 1601 耦合，本申请实施例对此不作具体限定。

收发器 1603，用于与其他通信装置之间的通信。例如，通信装置 1600 为终端，收发器 1603 可以用于与网络设备通信，或者与另一个终端设备通信。又例如，通信装置 1600 为网络设备，收发器 1603 可以用于与终端通信，或者与另一个网络设备通信。

可选地，收发器 1603 可以包括接收器和发送器（图 16 中未单独示出）。其中，接收器用于实现接收功能，发送器用于实现发送功能。

可选地，收发器 1603 可以和处理器 1601 集成在一起，也可以独立存在，并通过通信装置 1600 的接口电路（图 16 中未示出）与处理器 1601 耦合，本申请实施例对此不作具体限定。

需要说明的是，图 16 中示出的通信装置 1600 的结构并不构成对该通信装置的限定，实际的通信装置可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

此外，通信装置 1600 的技术效果可以参考上述方法实施例所述的通信方法的技术效果，此处不再赘述。

本申请实施例提供一种通信系统。该通信系统包括上述方法实施例中的一个或多个终端，以及上述方法实施例中一个或多个网络设备。

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

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

上述实施例，可以全部或部分地通过软件、硬件（如电路）、固件或其他任意组合来实现。当使用软件实现时，上述实施例可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令或计算机程序。在计算机上加载或执行所述计算机指令或计算机程序时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以为通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如红外、无线、微波等）方式

向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集合的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质。半导体介质可以是固态硬盘。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A,B 可以是单数或者复数。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系，但也可能表示的是一种“和/或”的关系，具体可参考前后文进行理解。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项（个）或复数项（个）的任意组合。例如，a,b,或 c 中的至少一项（个），可以表示：a, b, c, a-b, a-c, b-c, 或 a-b-c，其中 a,b,c 可以是单个，也可以是多个。

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

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出

来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory，ROM）、随机存取存储器（random access memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1.一种通信方法，其特征在于，所述方法包括：

认证服务网元向数据管理网元发送认证请求消息#1，所述认证请求消息#1 用于请求认证远端终端的信息；

所述认证服务网元接收来自所述数据管理网元的认证响应消息#1，所述认证响应消息#1 包括：临近业务 ProSe 认证信息#1，所述 ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证所述远端终端的信息；

在所述远端终端认证网络通过的情况下，所述认证服务网元接收来自接入和移动管理网元的认证请求消息#2，所述认证请求消息#2 用于请求认证所述远端终端；

在认证所述远端终端通过的情况下，所述认证服务网元向所述接入和移动管理网元发送认证响应消息#2，所述认证响应消息#2 包括：ProSe 密钥，所述 ProSe 密钥用于中继终端与所述远端终端的通信。

2.根据权利要求 1 所述的方法，其特征在于，所述 ProSe 认证信息#1 为如下至少一项：认证与密钥协商 AKA 的 ProSe 认证向量#1、或扩展认证协议请求 EAP-AKA’的 ProSe 的认证向量。

3.根据权利要求 2 所述的方法，其特征在于，所述 AKA 的 ProSe 认证向量#1 或所述 EAP-AKA’的 ProSe 的认证向量包括如下至少一项：用于所述远端终端认证网络的信息、用于所述认证服务网元认证所述远端终端的信息、或用于确定所述 ProSe 密钥的信息。

4.根据权利要求 2 或 3 所述的方法，其特征在于，在所述认证服务网元向数据管理网元发送认证请求消息#1 之前，所述方法还包括：

所述认证服务网元接收来自所述接入和移动管理网元的认证请求消息#3；

相应的，在所述认证服务网元接收来自所述数据管理网元的认证响应消息#1 之后，在所述认证服务网元接收来自接入和移动管理网元的认证请求消息#2 之前，所述方法还包括：

所述认证服务网元向所述接入和移动管理网元发送认证响应消息#3，所述认证响应消息#3 包括：ProSe 认证信息#2，所述 ProSe 认证信息#2 包括：用于所述远端终端认证网络的信息。

5.根据权利要求 4 所述的方法，其特征在于，所述 ProSe 认证信息#2 根据所述 ProSe 认证信息#1 确定，所述 ProSe 认证信息#2 为如下至少一项：AKA 的 ProSe 认证向量#2、或 EAP 请求消息或 AKA’挑战消息；所述 AKA 的 ProSe 认证向量#2 根据所述 AKA 的 ProSe 认证向量#1 确定，所述 EAP 请求消息或 AKA’挑战消息根据所述 EAP-AKA’的 ProSe 的认证向量确定。

6.根据权利要求 5 所述的方法，其特征在于，所述 AKA 的 ProSe 认证向量#2 包括：用于所述接入和移动管理网元认证所述远端终端的信息。

7.根据权利要求 4-6 中任一项所述的方法，其特征在于，所述认证请求消息#3 用于请求认证所述远端终端。

8.根据权利要求 7 所述的方法，其特征在于，所述认证请求消息#3 包括如下至少

一项：所述远端终端的用户隐藏标识 SUCI、服务网络名称、中继服务码 RSC、随机值#1、或 ProSe 中继通信指示信息；所述服务网络名称、所述 RSC 或所述 ProSe 中继通信指示信息中的任一项用于指示认证为 ProSe 中继通信的认证；所述服务网络名称、所述 RSC 或所述随机值#1 中的任一项用于确定所述 ProSe 密钥。

9.根据权利要求 8 所述的方法，其特征在于，在所述认证服务网元向所述接入和移动管理网元发送认证响应消息#2 之前，所述方法还包括：

若所述认证请求消息#3 中包括：所述 RSC 和所述随机值#1，则所述认证服务网元保存所述 RSC 和所述随机值#1。

10.根据权利要求 9 所述的方法，其特征在于，所述用于确定所述 ProSe 密钥的信息包括：中间密钥，在所述认证服务网元向所述接入和移动管理网元发送认证响应消息#2 之前，所述方法还包括：

在认证所述远端终端通过的情况下，所述认证服务网元根据如下至少一项：所述服务网络名称、所述 RSC、所述随机值#1、随机值#2 和所述中间密钥，确定所述 ProSe 密钥。

11.根据权利要求 1-7 中任一项所述的方法，其特征在于，所述认证请求消息#2 包括如下至少一项：所述远端终端确定的认证响应消息、用于确定所述 ProSe 密钥的 RSC、或用于确定所述 ProSe 密钥的随机值#1，所述认证响应消息用于认证所述远端终端。

12.根据权利要求 1-9、11 中任一项所述的方法，其特征在于，所述认证响应消息#2 包括：随机值#2，所述随机值#2 用于确定所述 ProSe 密钥。

13.根据权利要求 12 所述的方法，其特征在于，所述认证响应消息#2 还包括如下至少一项：远端终端的用户隐藏标识 SUPI、或 EAP 成功消息。

14.根据权利要求 1-7 中任一项所述的方法，其特征在于，所述认证请求消息#1 包括如下至少一项：所述远端终端的 SUCI、或 ProSe 中继通信指示信息，所述 ProSe 中继通信指示信息用于指示认证为 ProSe 中继通信的认证。

15.根据权利要求 1-14 中任一项所述的方法，其特征在于，所述认证服务网元跳过推演用于远端终端与网络之间通信的密钥。

16.一种通信方法，其特征在于，所述方法包括：

中继终端接收来自接入和移动管理网元的用于远端终端认证网络的信息；

所述中继终端向所述接入和移动管理网元发送所述远端终端确定的认证响应信息，所述认证响应信息用于认证所述远端终端；

所述中继终端接收来自所述接入和移动管理网元的 ProSe 密钥，所述 ProSe 密钥用于所述中继终端与所述远端终端的通信。

17.根据权利要求 16 所述的方法，其特征在于，所述远端终端认证网络的信息和所述远端终端确定的认证响应信息为通过通信密钥保护的信息，所述通信密钥用于所述中继终端与网络的通信。

18.根据权利要求 16 或 17 所述的方法，其特征在于，在所述中继终端接收来自接入和移动管理网元的用于所述远端终端认证网络的信息之后，在所述中继终端向所述接入和移动管理网元发送所述远端终端确定的认证响应信息之前，所述方法还包

括：

所述中继终端向所述远端终端发送所述用于所述远端终端认证网络的信息；

所述中继终端接收来自所述远端终端的所述认证响应信息。

19.根据权利要求 18 所述的方法，其特征在于，所述用于所述远端终端认证网络的信息承载在消息中，所述中继终端向所述远端终端发送所述用于所述远端终端认证网络的信息，包括：

所述中继终端根据所述消息，向所述远端终端发送所述用于所述远端终端认证网络的信息。

20.根据权利要求 16-19 中任一项所述的方法，其特征在于，在所述中继终端向所述接入和移动管理网元发送所述远端终端确定的认证响应信息之后，所述方法还包括：

所述中继终端接收来自所述接入和移动管理网元的随机值#2；

所述中继终端向所述远端终端发送所述随机值#2，所述随机值#2 用于确定所述 ProSe 密钥。

21.一种通信方法，其特征在于，所述方法包括：

远端终端接收来自中继终端的用于所述远端终端认证网络的信息；

在所述远端终端确定认证网络通过的情况下，所述远端终端向所述中继终端发送所述远端终端确定的认证响应信息，所述认证响应信息用于认证所述远端终端。

22.根据权利要求 21 所述的方法，其特征在于，在所述远端终端向所述中继终端发送所述远端终端确定的认证响应信息之后，所述方法还包括：

所述远端终端接收来自所述中继终端的随机值#2；

所述远端终端根据如下至少一项：服务网络名称、RSC、随机值#1、所述随机值#2 和中间密钥，确定 ProSe 密钥，所述 ProSe 密钥用于所述中继终端与所述远端终端的通信。

23.一种通信方法，其特征在于，所述方法包括：

数据管理网元接收来自认证服务网元的认证请求消息#1，所述认证请求消息#1 用于请求认证远端终端的信息；

所述数据管理网元向所述认证服务网元发送认证响应消息#1，所述认证响应消息#1 包括：临近业务 ProSe 认证信息#1；所述 ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证远端终端的信息。

24.根据权利要求 23 所述的方法，其特征在于，所述 ProSe 认证信息#1 为如下至少一项：认证与密钥协商 AKA 的 ProSe 认证向量#1、或扩展认证协议请求 EAP-AKA’的 ProSe 的认证向量。

25.根据权利要求 24 所述的方法，其特征在于，所述 AKA 的 ProSe 认证向量#1 或所述 EAP-AKA’的 ProSe 的认证向量包括如下至少一项：用于所述远端终端认证网络的信息、用于所述认证服务网元认证所述远端终端的信息、或用于确定所述 ProSe 密钥的信息。

26.根据权利要求 23-25 中任一项所述的方法，其特征在于，在所述数据管理网元向所述认证服务网元发送认证响应消息#1 之前，所述方法还包括：

所述数据管理网元确定所述远端终端授权获取中继服务。

27.一种通信方法，其特征在于，所述方法包括：

认证服务网元向数据管理网元发送认证请求消息#1，所述认证请求消息#1 用于请求认证远端终端的信息；

所述数据管理网元接收来自认证服务网元的认证请求消息#1，并向所述认证服务网元发送认证响应消息#1，所述认证响应消息#1 包括：临近业务 ProSe 认证信息#1，所述 ProSe 认证信息#1 包括如下至少一项：用于远端终端认证网络的信息、或用于认证所述远端终端的信息；

所述认证服务网元接收来自所述数据管理网元的认证响应消息#1；

在所述远端终端认证网络通过的情况下，接入和移动管理网元向所述认证服务网元发送认证请求消息#2，所述认证请求消息#2 用于请求认证所述远端终端；

所述认证服务网元接收来自所述接入和移动管理网元的所述认证请求消息#2；

在认证所述远端终端通过的情况下，所述认证服务网元向所述接入和移动管理网元发送认证响应消息#2，所述认证响应消息#2 包括：ProSe 密钥，所述 ProSe 密钥用于中继终端与所述远端终端的通信；

所述接入和移动管理网元接收来自所述认证服务网元的所述认证响应消息#2。

28.根据权利要求 27 所述的方法，其特征在于，所述 ProSe 认证信息#1 为如下至少一项：认证与密钥协商 AKA 的 ProSe 认证向量#1、或扩展认证协议请求 EAP-AKA'的 ProSe 的认证向量。

29.根据权利要求 28 所述的方法，其特征在于，所述 AKA 的 ProSe 认证向量#1 或所述 EAP-AKA'的 ProSe 的认证向量包括如下至少一项：用于所述远端终端认证网络的信息、用于所述认证服务网元认证所述远端终端的信息、或用于确定所述 ProSe 密钥的信息。

30.一种通信方法，其特征在于，所述方法包括：

中继终端接收来自接入和移动管理网元的用于远端终端认证网络的信息；

所述远程终端接收来自所述中继终端的用于所述远端终端认证网络的信息；

在所述远端终端确定认证网络通过的情况下，所述远端终端向所述中继终端发送所述远端终端确定的认证响应信息，所述认证响应信息用于认证所述远端终端；

所述中继终端向所述接入和移动管理网元发送所述远端终端确定的认证响应信息，并接收来自所述接入和移动管理网元的临近业务 ProSe 密钥，所述 ProSe 密钥用于所述中继终端与所述远端终端的通信。

31.根据权利要求 30 所述的方法，其特征在于，所述远端终端认证网络的信息和所述远端终端确定的认证响应信息为通过通信密钥保护的信息，所述通信密钥用于所述中继终端与网络的通信。

32.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求 1-15 中任一项所述的通信方法的模块。

33.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求 16-20 中任一项所述的通信方法的模块。

34.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求 21 或

22 所述的通信方法的模块。

35.一种通信装置，其特征在于，所述通信装置包括：用于执行如权利要求 23 或 26 所述的通信方法的模块。

36.一种通信装置，其特征在于，所述通信装置包括：处理器；其中，

所述处理器，用于执行如权利要求 1-26 中任一项所述的通信方法。

37.一种通信装置，其特征在于，所述通信装置包括：处理器和存储器；所述存储器用于存储计算机指令，当所述处理器执行该指令时，以使所述通信装置执行如权利要求 1-26 中任一项所述的通信方法。

38.一种通信系统，其特征在于，所述通信系统包括：如权利要求 1-13 中任一项所述的认证服务网元、如权利要求 13-18 中任一项所述的中继终端、以及如权利要求 21 或 22 所述的远端终端。

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包括计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求 1-26 中任一项所述的通信方法。

40.一种计算机程序产品，其特征在于，所述计算机程序产品包括：计算机程序或指令，当所述计算机程序或指令在计算机上运行时，使得所述计算机执行如权利要求 1-26 中任一项所述的通信方法。

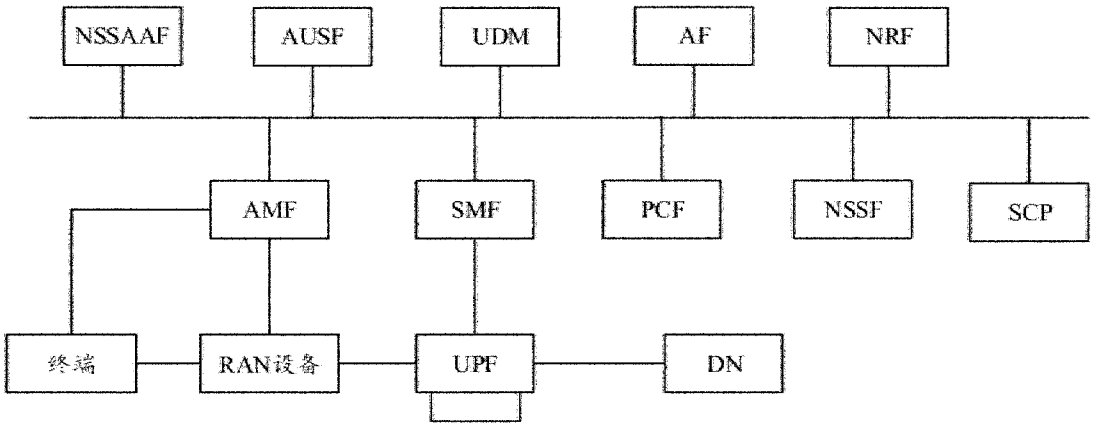
NSSAAF
AUSF
UDM
AF
NRF
AMF
SMF
PCF
NSSF
SCP
终端
RAN设备
UPF
DN

图 1


远端UE
中继UE
RAN设备
5GC
DN

图 2

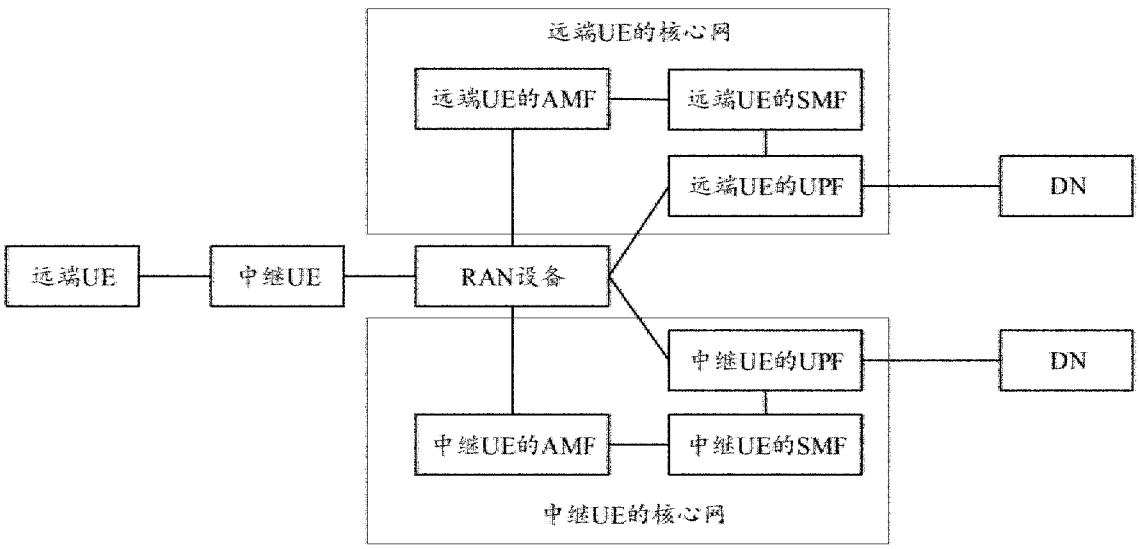
远端UE的核心网
远端UE的AMF
远端UE的SMF
远端UE的UPF
DN
远端UE
中继UE
RAN设备
中继UE的UPF
DN
中继UE的AMF
中继UE的SMF
中继UE的核心网

图 3

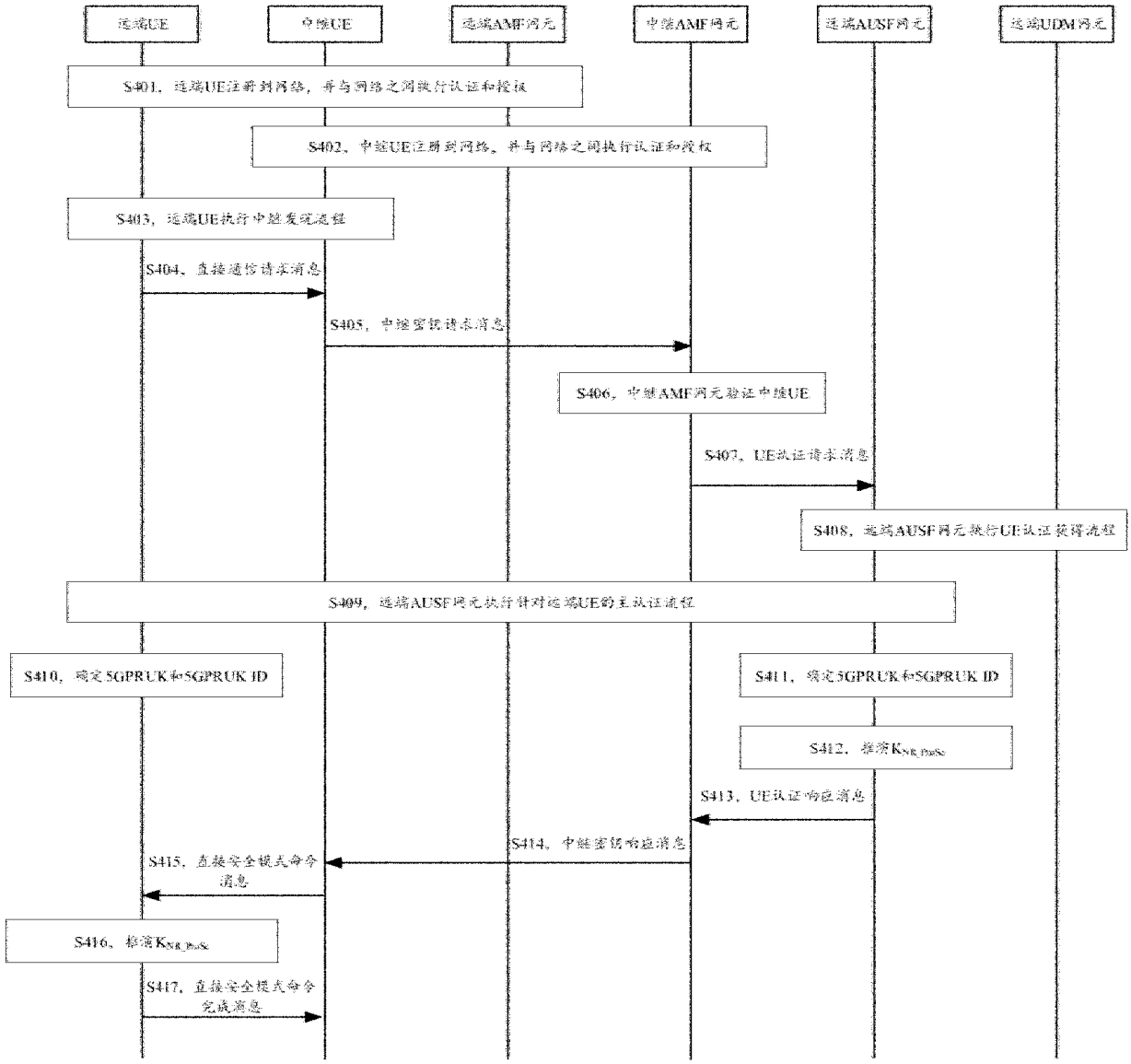
远端UE
中继UE
远端AMF网元
中继AMF网元
远端AUSF网元
远端UDM网元
S401，远端UE注册到网络，并与网络之间执行认证和授权
S402，中继UE注册到网络，并与网络之间执行认证和授权
S403，远端UE执行中继发现流程
S404，直接通信请求消息
S405，中继密钥请求消息
S406，中继AMF网元验证中继UE
S407，UE认证请求消息
S408，远端AUSF网元执行UE认证获得流程
S409，远端AUSF网元执行针对远端UE的主认证流程
S410，确定5GPRUK和5GPRUK ID
S411，确定5GPRUK和5GPRUK ID
S412，推演K_{NR_PaSe}
S413，UE认证响应消息
S414，中继密钥响应消息
S415，直接安全模式命令消息
S416，推演K_{NR_PaSe}
S417，直接安全模式命令完成消息

图 4

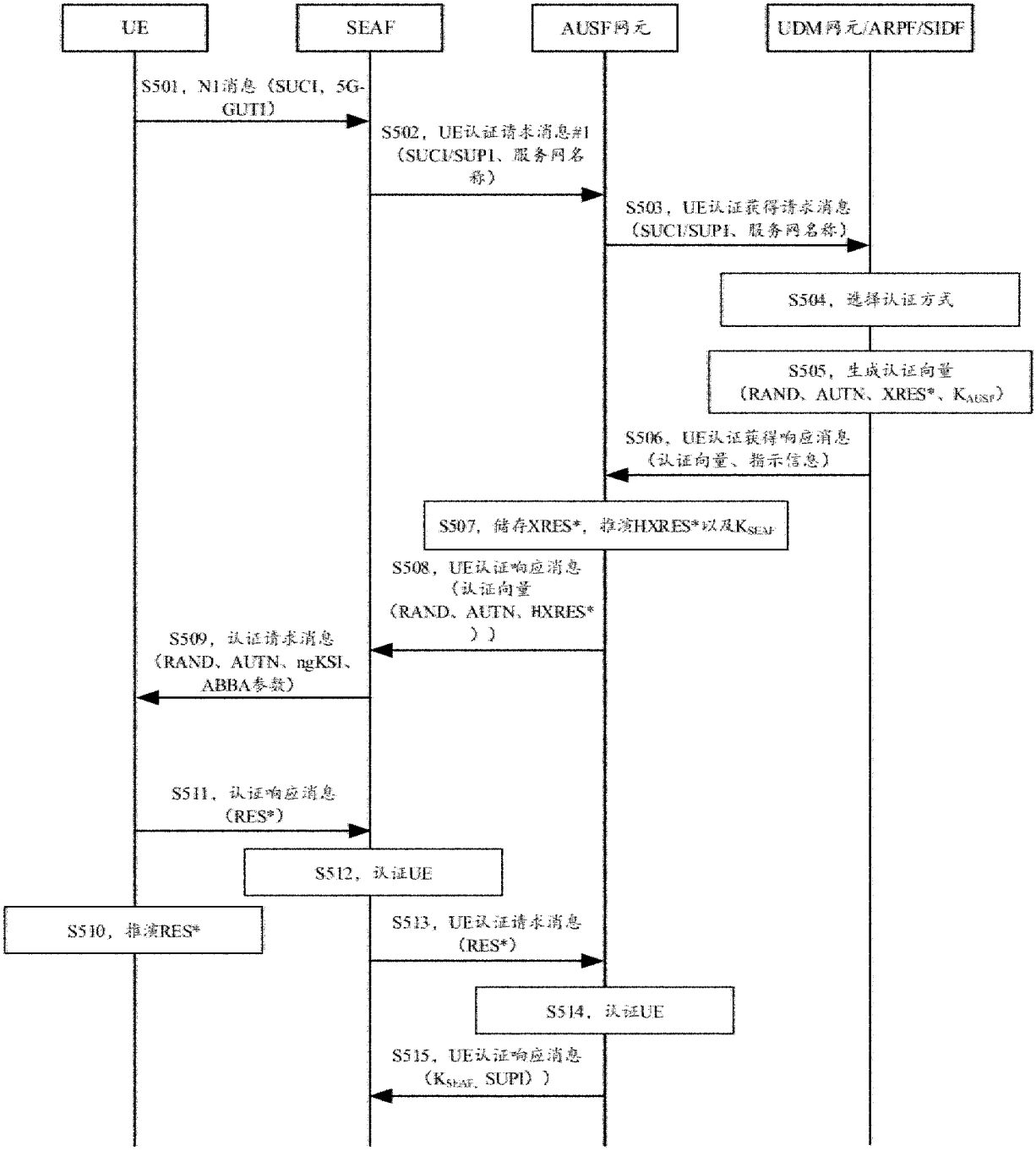
UE
SEAF
AUSF网元
UDM网元/ARPF/SIDF
S501，N1消息（SUCI，5G-GUTI）
S502，UE认证请求消息#1（SUCI/SUPI、服务网名称）
S503，UE认证获得请求消息（SUCI/SUPI、服务网名称）
S504，选择认证方式
S505，生成认证向量（RAND、AUTN、XRES*、K_{AUSF}）
S506，UE认证获得响应消息（认证向量、指示信息）
S507，储存XRES*，推演HXRES*以及K_{SEAF}
S508，UE认证响应消息（认证向量（RAND、AUTN、HXRES*））
S509，认证请求消息（RAND、AUTN、ngKSI、ABBA参数）
S511，认证响应消息（RES*）
S512，认证UE
S510，推演RES*
S513，UE认证请求消息（RES*）
S514，认证UE
S515，UE认证响应消息（K_{SEAF}、SUPI）

图 5

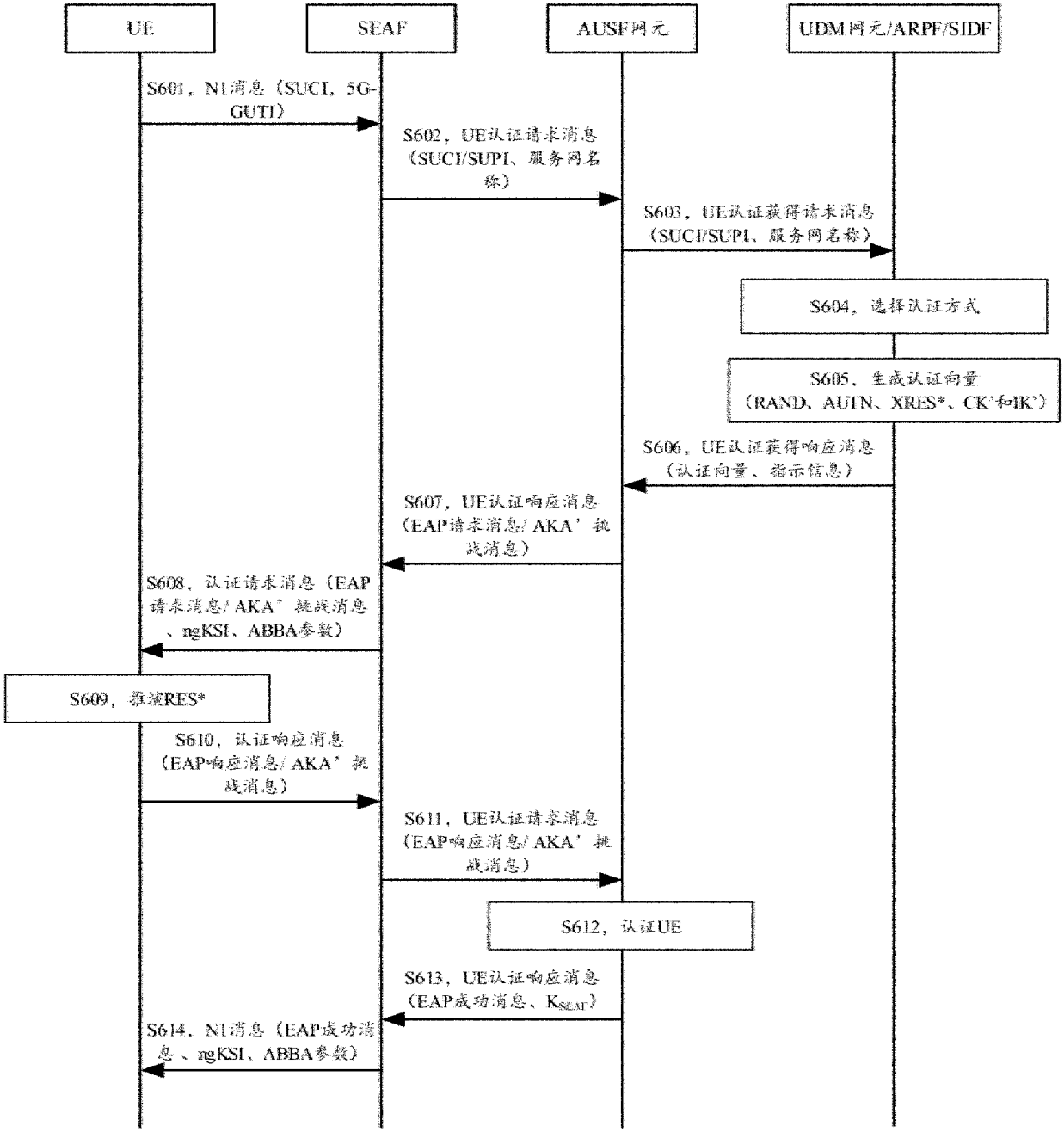
UE
SEAF
AUSF网元
UDM网元/ARPF/SIDF
S601，N1消息（SUCI，5G-GUTI）
S602，UE认证请求消息（SUCI/SUPI、服务网名称）
S603，UE认证获得请求消息（SUCI/SUPI、服务网名称）
S604，选择认证方式
S605，生成认证向量（RAND、AUTN、XRES*、CK'和IK'）
S606，UE认证获得响应消息（认证向量、指示信息）
S607，UE认证响应消息（EAP请求消息/ AKA' 挑战消息）
S608，认证请求消息（EAP请求消息/ AKA' 挑战消息、ngKSI、ABBA参数）
S609，推演RES*
S610，认证响应消息（EAP响应消息/ AKA' 挑战消息）
S611，UE认证请求消息（EAP响应消息/ AKA' 挑战消息）
S612，认证UE
S613，UE认证响应消息（EAP成功消息、K_{SEAF}）
S614，N1消息（EAP成功消息、ngKSI、ABBA参数）

图 6

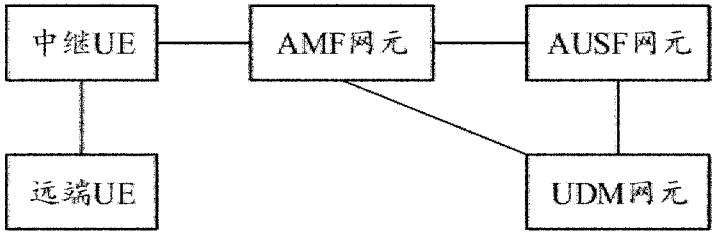
中继UE
AMF网元
AUSF网元
远端UE
UDM网元

图 7

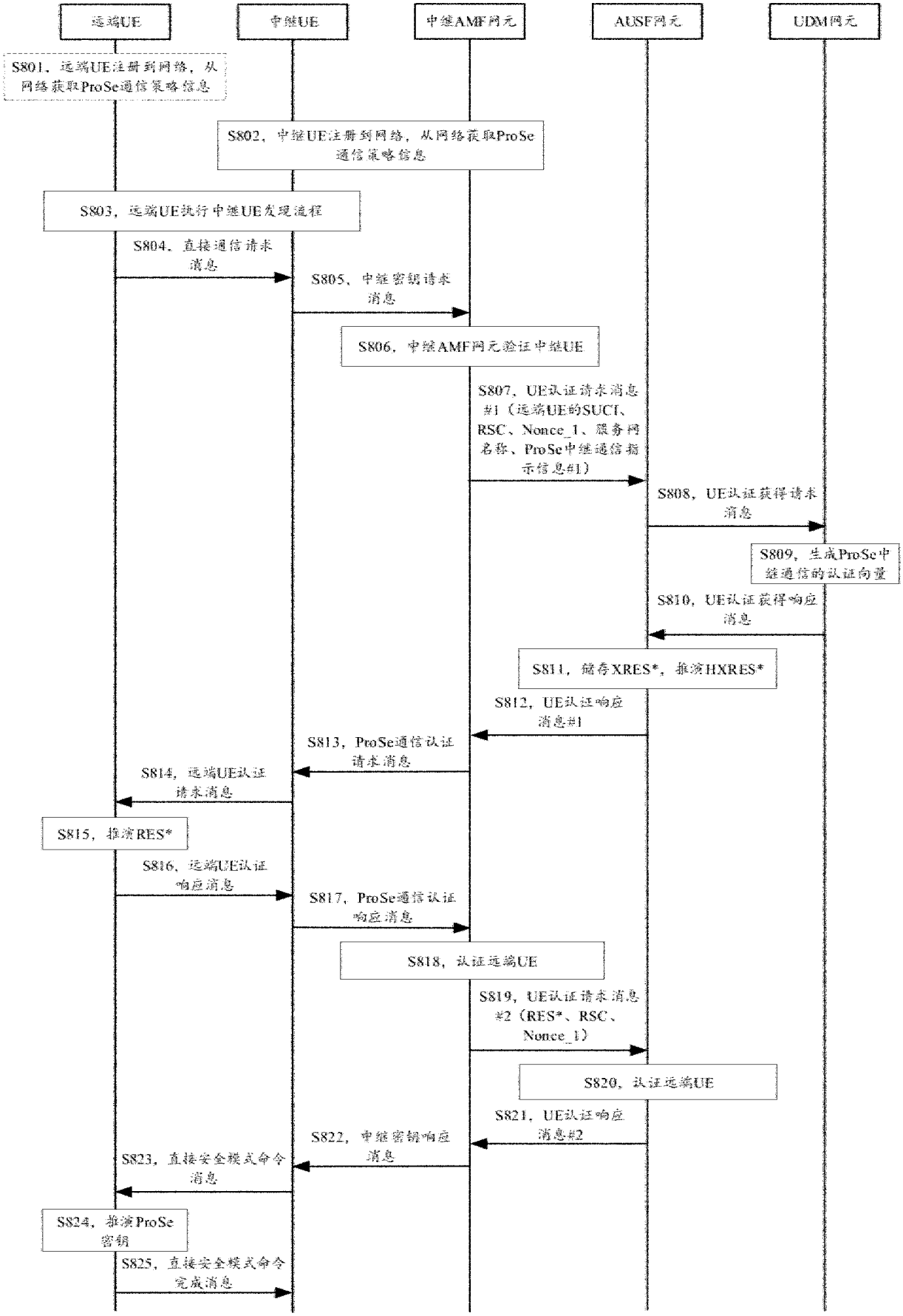
远端UE
中继UE
中继AMF网元
AUSF网元
UDM网元
S801，远端UE注册到网络，从网络获取ProSe通信策略信息
S802，中继UE注册到网络，从网络获取ProSe通信策略信息
S803，远端UE执行中继UE发现流程
S804，直接通信请求消息
S805，中继密钥请求消息
S806，中继AMF网元验证中继UE
S807，UE认证请求消息#1（远端UE的SUCI、RSC、Nonce_1、服务网名称、ProSe中继通信指示信息#1）
S808，UE认证获得请求消息
S809，生成ProSe中继通信的认证向量
S810，UE认证获得响应消息
S811，储存XRES*，推演HXRES*
S812，UE认证响应消息#1
S813，ProSe通信认证请求消息
S814，远端UE认证请求消息
S815，推演RES*
S816，远端UE认证响应消息
S817，ProSe通信认证响应消息
S818，认证远端UE
S819，UE认证请求消息#2（RES*、RSC、Nonce_1）
S820，认证远端UE
S821，UE认证响应消息#2
S822，中继密钥响应消息
S823，直接安全模式命令消息
S824，推演ProSe密钥
S825，直接安全模式命令完成消息

图 8

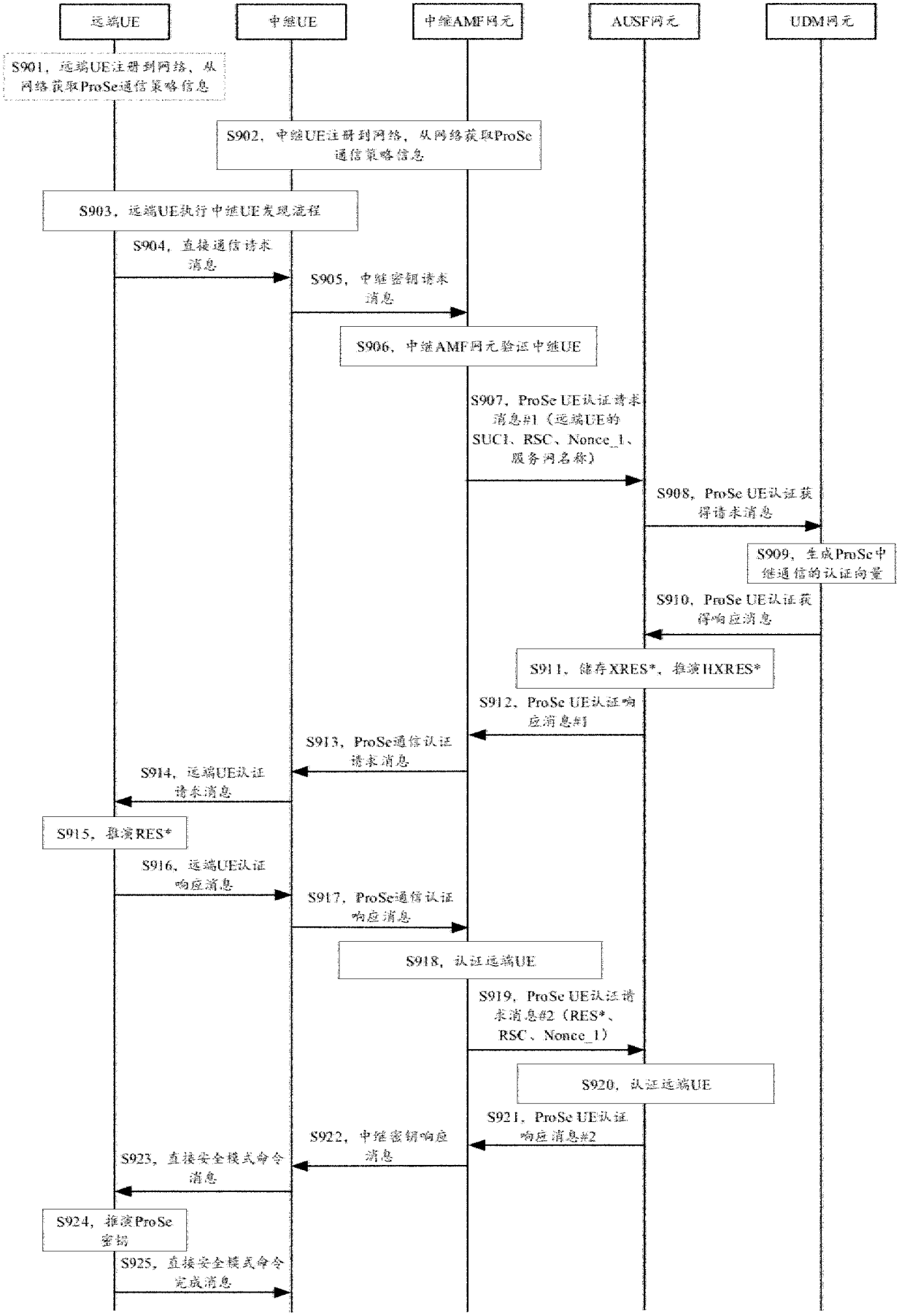
远端UE
中继UE
中继AMF网元
AUSF网元
UDM网元
S901，远端UE注册到网络，从网络获取ProSe通信策略信息
S902，中继UE注册到网络，从网络获取ProSe通信策略信息
S903，远端UE执行中继UE发现流程
S904，直接通信请求消息
S905，中继密钥请求消息
S906，中继AMF网元验证中继UE
S907，ProSe UE认证请求消息#1（远端UE的SUCI、RSC、Nonce_1、服务网名称）
S908，ProSe UE认证获得请求消息
S909，生成ProSe中继通信的认证向量
S910，ProSe UE认证获得响应消息
S911，储存XRES*，推演HXRES*
S912，ProSe UE认证响应消息#1
S913，ProSe通信认证请求消息
S914，远端UE认证请求消息
S915，推演RES*
S916，远端UE认证响应消息
S917，ProSe通信认证响应消息
S918，认证远端UE
S919，ProSe UE认证请求消息#2（RES*、RSC、Nonce_1）
S920，认证远端UE
S921，ProSe UE认证响应消息#2
S922，中继密钥响应消息
S923，直接安全模式命令消息
S924，推演ProSe密钥
S925，直接安全模式命令完成消息

图 9

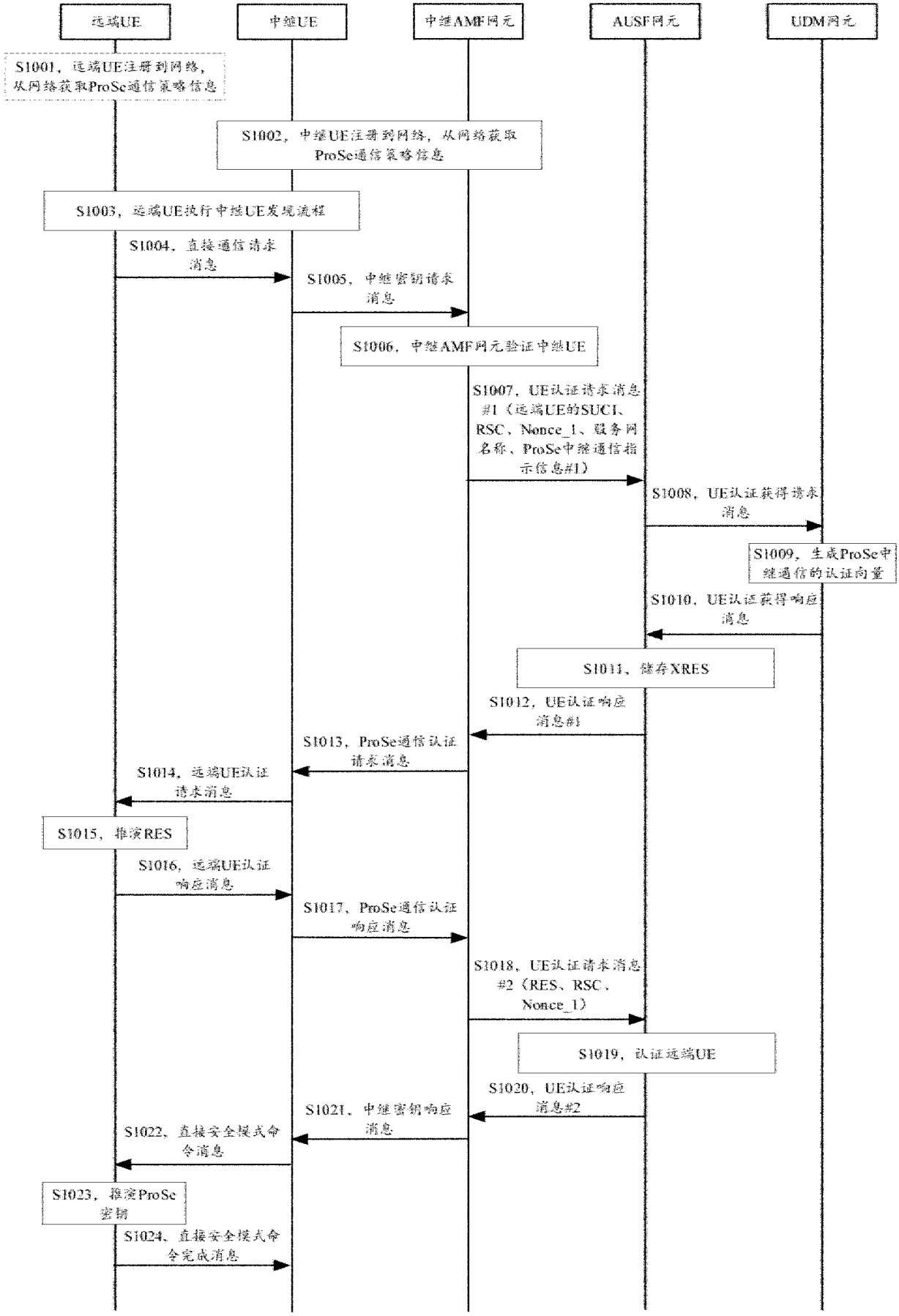
远端UE
中继UE
中继AMF网元
AUSF网元
UDM网元
S1001，远端UE注册到网络，从网络获取ProSe通信策略信息
S1002，中继UE注册到网络，从网络获取ProSe通信策略信息
S1003，远端UE执行中继UE发现流程
S1004，直接通信请求消息
S1005，中继密钥请求消息
S1006，中继AMF网元验证中继UE
S1007，UE认证请求消息#1（远端UE的SUCI、RSC、Nonce_1、服务网名称、ProSe中继通信指示信息#1）
S1008，UE认证获得请求消息
S1009，生成ProSe中继通信的认证向量
S1010，UE认证获得响应消息
S1011，储存XRES
S1012，UE认证响应消息#1
S1013，ProSe通信认证请求消息
S1014，远端UE认证请求消息
S1015，推演RES
S1016，远端UE认证响应消息
S1017，ProSe通信认证响应消息
S1018，UE认证请求消息#2（RES、RSC、Nonce_1）
S1019，认证远端UE
S1020，UE认证响应消息#2
S1021，中继密钥响应消息
S1022，直接安全模式命令消息
S1023，推演ProSe密钥
S1024，直接安全模式命令完成消息

图 10

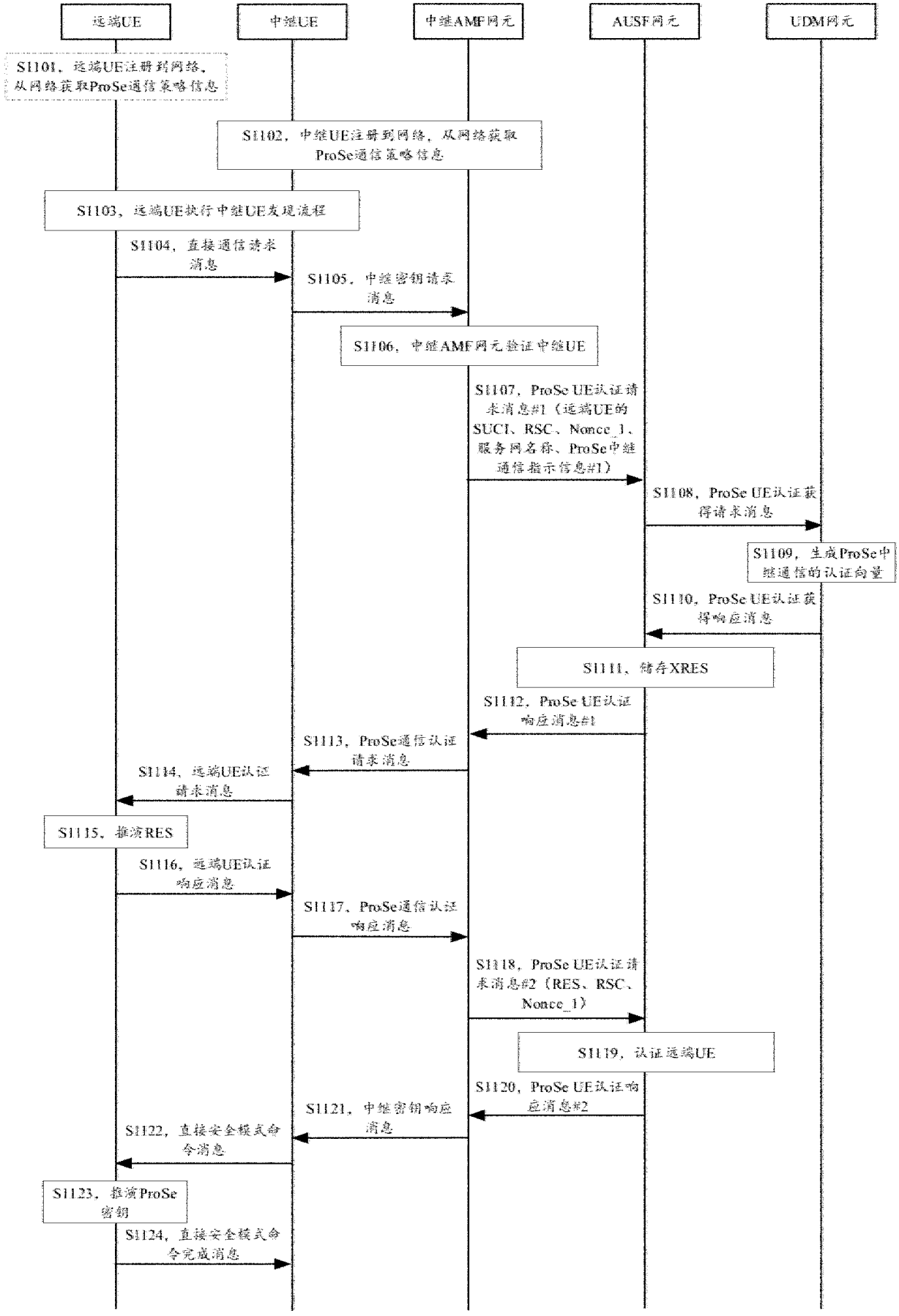
远端UE
中继UE
中继AMF网元
AUSF网元
UDM网元
S1101，远端UE注册到网络，从网络获取ProSe通信策略信息
S1102，中继UE注册到网络，从网络获取ProSe通信策略信息
S1103，远端UE执行中继UE发现流程
S1104，直接通信请求消息
S1105，中继密钥请求消息
S1106，中继AMF网元验证中继UE
S1107，ProSe UE认证请求消息#1（远端UE的SUCI、RSC、Nonce_1、服务网名称、ProSe中继通信指示信息#1）
S1108，ProSe UE认证获得请求消息
S1109，生成ProSe中继通信的认证向量
S1110，ProSe UE认证获得响应消息
S1111，储存XRES
S1112，ProSe UE认证响应消息#1
S1113，ProSe通信认证请求消息
S1114，远端UE认证请求消息
S1115，推演RES
S1116，远端UE认证响应消息
S1117，ProSe通信认证响应消息
S1118，ProSe UE认证请求消息#2（RES、RSC、Nonce_1）
S1119，认证远端UE
S1120，ProSe UE认证响应消息#2
S1121，中继密钥响应消息
S1122，直接安全模式命令消息
S1123，推演ProSe密钥
S1124，直接安全模式命令完成消息

图 11

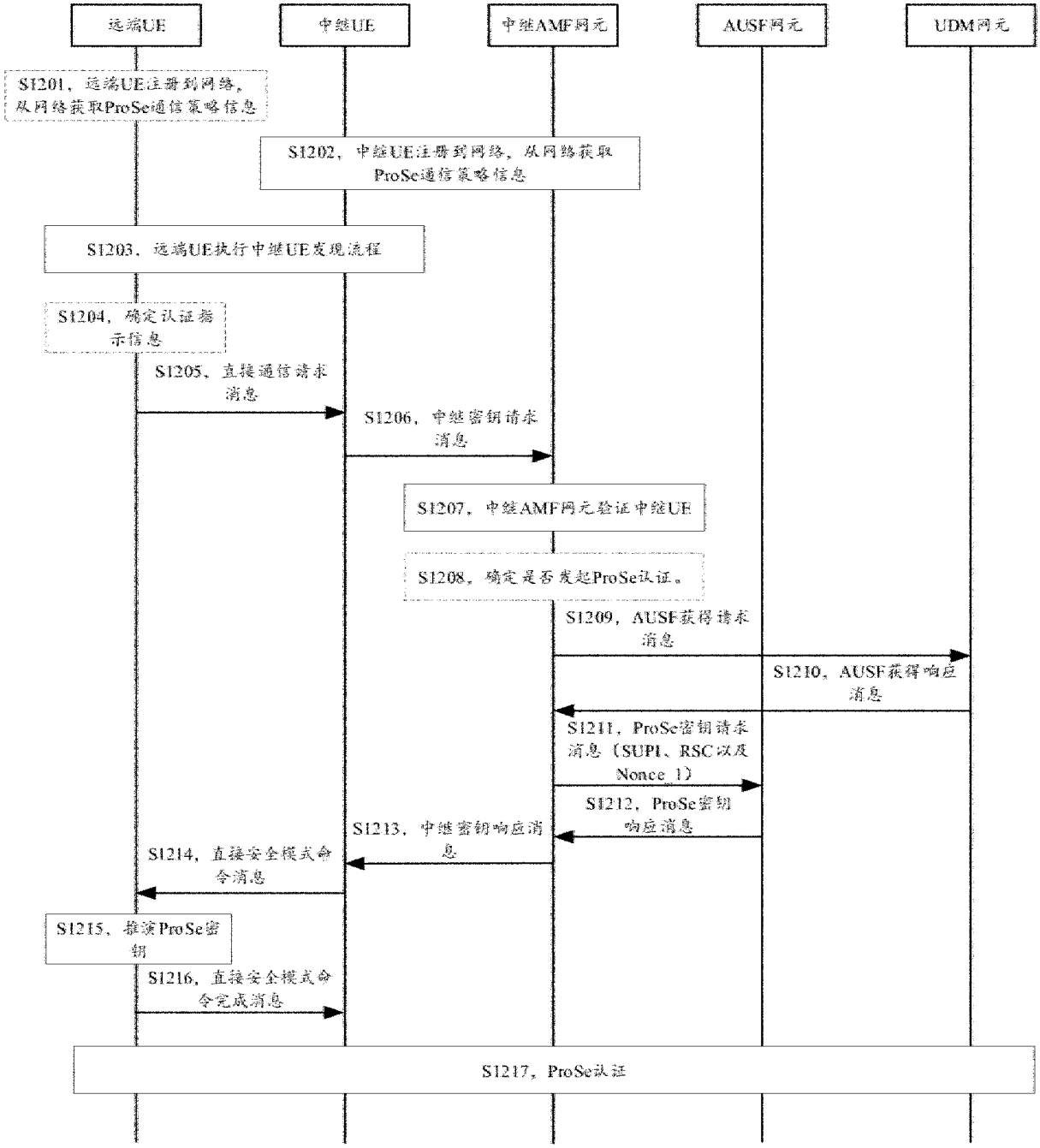
远端UE
中继UE
中继AMF网元
AUSF网元
UDM网元
S1201，远端UE注册到网络，从网络获取ProSe通信策略信息
S1202，中继UE注册到网络，从网络获取ProSe通信策略信息
S1203，远端UE执行中继UE发现流程
S1204，确定认证指示信息
S1205，直接通信请求消息
S1206，中继密钥请求消息
S1207，中继AMF网元验证中继UE
S1208，确定是否发起ProSe认证。
S1209，AUSF获得请求消息
S1210，AUSF获得响应消息
S1211，ProSe密钥请求消息（SUPI、RSC以及Nonce_1）
S1212，ProSe密钥响应消息
S1213，中继密钥响应消息
S1214，直接安全模式命令消息
S1215，推演ProSe密钥
S1216，直接安全模式命令完成消息
S1217，ProSe认证

图 12

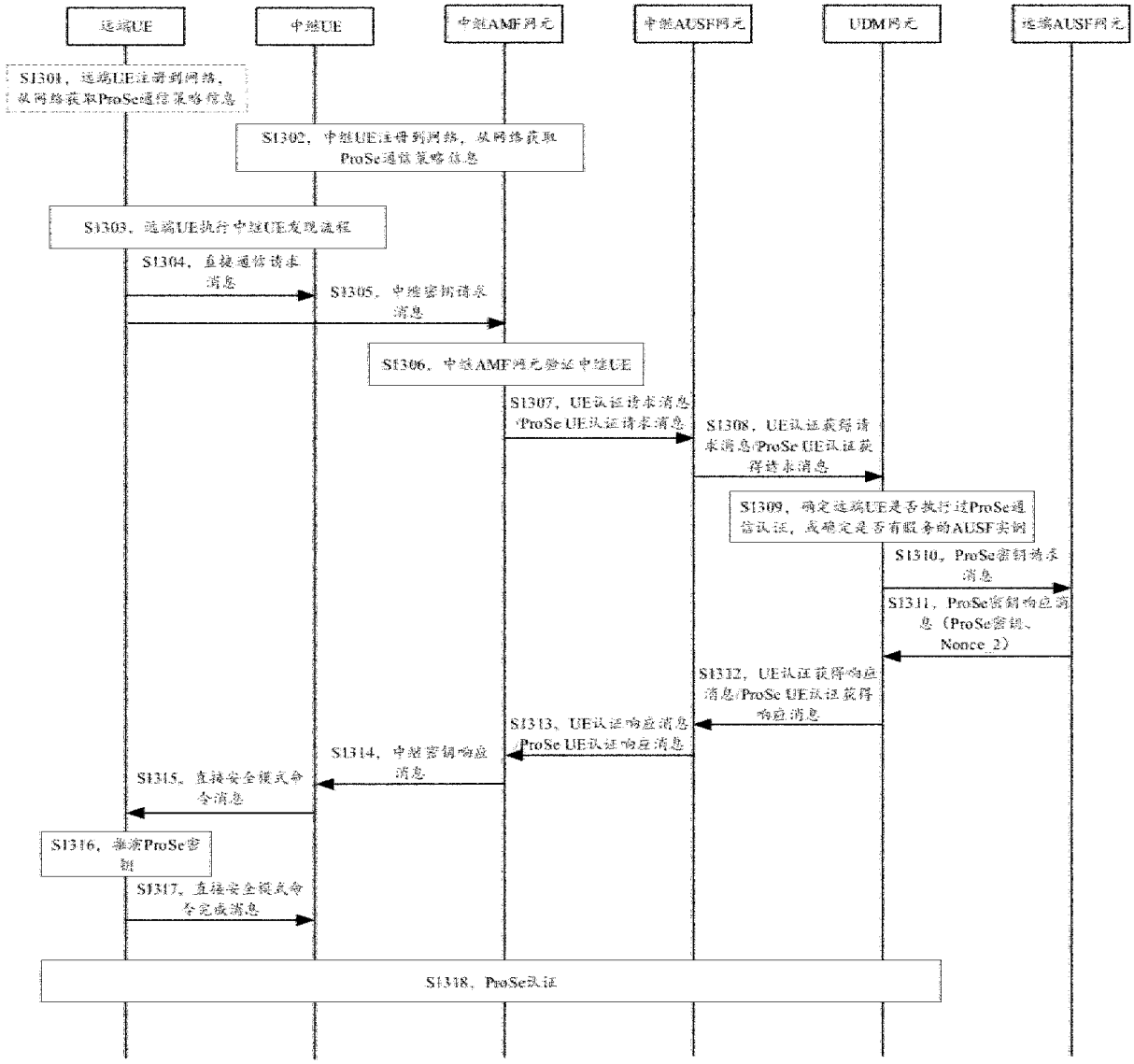
远端UE
中继UE
中继AMF网元
中继AUSF网元
UDM网元
远端AUSF网元
S1301，远端UE注册到网络，从网络获取ProSe通信策略信息
S1302，中继UE注册到网络，从网络获取ProSe通信策略信息
S1303，远端UE执行中继UE发现流程
S1304，直接通信请求消息
S1305，中继密钥请求消息
S1306，中继AMF网元验证中继UE
S1307，UE认证请求消息/ProSe UE认证请求消息
S1308，UE认证获得请求消息/ProSe UE认证获得请求消息
S1309，确定远端UE是否执行过ProSe通信认证，或确定是否有服务的AUSF实例
S1310，ProSe密钥请求消息
S1311，ProSe密钥响应消息（ProSe密钥、Nonce_2）
S1312，UE认证获得响应消息/ProSe UE认证获得响应消息
S1313，UE认证响应消息/ProSe UE认证响应消息
S1314，中继密钥响应消息
S1315，直接安全模式命令消息
S1316，推演ProSe密钥
S1317，直接安全模式命令完成消息
S1318，ProSe认证

图 13

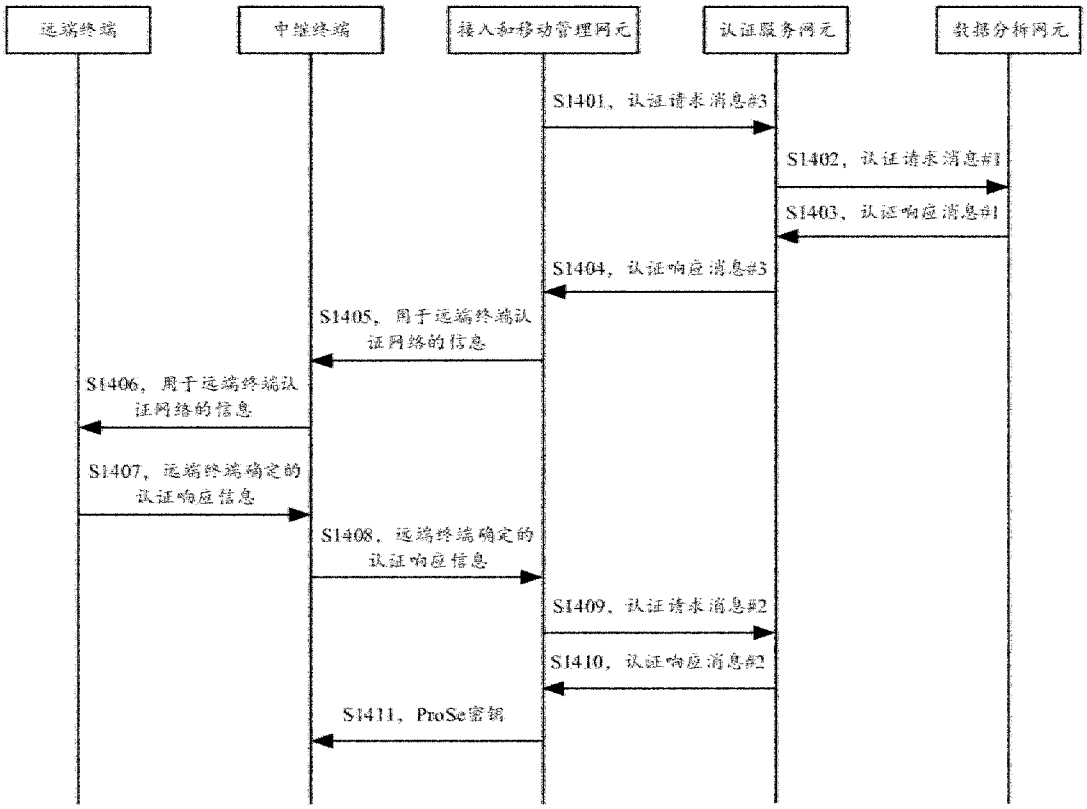
远端终端
中继终端
接入和移动管理网元
认证服务网元
数据分析网元
S1401，认证请求消息#3
S1402，认证请求消息#1
S1403，认证响应消息#1
S1404，认证响应消息#3
S1405，用于远端终端认证网络的信息
S1406，用于远端终端认证网络的信息
S1407，远端终端确定的认证响应信息
S1408，远端终端确定的认证响应信息
S1409，认证请求消息#2
S1410，认证响应消息#2
S1411，ProSe密钥

图 14

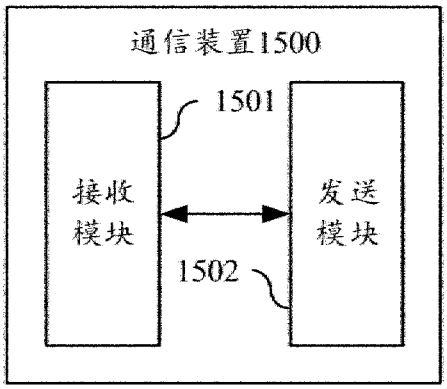
通信装置1500
1501
接收模块
发送模块
1502

图 15

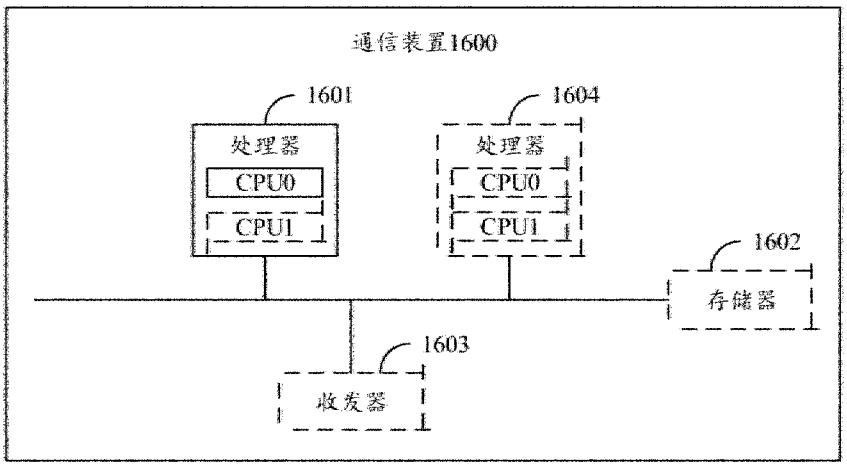
通信装置1600
1601
处理器
CPU0
CPU1
1604
处理器
CPU0
CPU1
1602
存储器
1603
收发器

图 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/072627

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/041(2021.01)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,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)

CJFD, CNABS, CNTXT, DWPI, ENTXT, ENTXTC, VEN, 3GPP: 加密, 近距离服务, 近距离通信, 近距离业务, 临近业务, 密钥, 认证, 消息, 信息, 远端终端, 中继, encrption, poximity, sevice, proximity, communication, nearby, sevice, key, authentication, message, information, remote, terminal, relay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 112219415 A (NOKIA TECHNOLOGIES OY) 12 January 2021 (2021-01-12) description, paragraphs [76]-[98]	21, 22, 34
Y	CN 112219415 A (NOKIA TECHNOLOGIES OY) 12 January 2021 (2021-01-12) description, paragraphs [76]-[98]	1-3, 11-15, 23-29, 32, 35-37, 39-40
Y	WO 2022019627 A1 (SAMSUNG ELECTRONICS CO., LTD.) 27 January 2022 (2022-01-27) description paragraphs [093]-[145]	1-3, 11-15, 23-29, 32, 35-37, 39-40
A	CN 113543121 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 October 2021 (2021-10-22) entire document	1-40
A	US 2021400475 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 23 December 2021 (2021-12-23) entire document	1-40
A	WO 2020091281 A1 (LG ELECTRONICS INC.) 07 May 2020 (2020-05-07) entire document	1-40

☐ 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
"D" document cited by the applicant in the international application
"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
21 March 2023	**23 March 2023**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/072627

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112219415	A	12 January 2021	WO	2019193107	A1	10 October 2019
				EP	3777011	A1	17 February 2021
				US	2021120409	A1	22 April 2021
WO	2022019627	A1	27 January 2022		None		
CN	113543121	A	22 October 2021		None		
US	2021400475	A1	23 December 2021	EP	3881580	A1	22 September 2021
				WO	2020099148	A1	22 May 2020
WO	2020091281	A1	07 May 2020		None		

国际检索报告

国际申请号
PCT/CN2023/072627

A. 主题的分类

H04W12/041(2021.01)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,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））

CJFD,CNABS,CNTXT,DWPI,ENTXT,ENTXTC,VEN,3GPP:加密,近距离服务,近距离通信,近距离业务,临近业务,密钥,认证,消息，信息，远端终端，中继，encrption,poximity,sevice,proximity,communication,nearby,sevice,key,authentication,message,information,remote,terminal,relay

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 112219415 A (诺基亚技术有限公司) 2021年1月12日 (2021-01-12) 说明书第[76]段至第[98]段	21,22,34
Y	CN 112219415 A (诺基亚技术有限公司) 2021年1月12日 (2021-01-12) 说明书第[76]段至第[98]段	1-3,11-15,23-29,32,35-37,39-40
Y	WO 2022019627 A1 (SAMSUNG ELECTRONICS CO LTD) 2022年1月27日 (2022-01-27) 说明书第[093]至第[145]段	1-3,11-15,23-29,32,35-37,39-40
A	CN 113543121 A (华为技术有限公司) 2021年10月22日 (2021-10-22) 全文	1-40
A	US 2021400475 A1 (ERICSSON TELEFON AB L M) 2021年12月23日 (2021-12-23) 全文	1-40
A	WO 2020091281 A1 (LG ELECTRONICS INC.) 2020年5月7日 (2020-05-07) 全文	1-40

☐ 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

"D" 申请人在国际申请中引证的文件

"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
2023年3月21日	2023年3月23日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	颜燕
传真号 (86-10)62019451	电话号码 (+86) 010-62089959

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/072627

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	112219415	A	2021年1月12日	WO	2019193107	A1	2019年10月10日
				EP	3777011	A1	2021年2月17日
				US	2021120409	A1	2021年4月22日
WO	2022019627	A1	2022年1月27日		无		
CN	113543121	A	2021年10月22日		无		
US	2021400475	A1	2021年12月23日	EP	3881580	A1	2021年9月22日
				WO	2020099148	A1	2020年5月22日
WO	2020091281	A1	2020年5月7日		无		