

一种生成设备间通信的密钥的方法、系统和装置

5 技术领域

本申请涉及通信领域，并且更具体地，涉及一种生成远端设备和中继设备之间通信的密钥的方法、系统和装置。

背景技术

10 随着移动通信的高速发展，为了满足不同业务不同场景下的通信需求，提出了设备到设备的近距离业务（proximity-bases services, ProSe）通信模型，允许用户设备（user equipment, UE）与用户设备之间直接建立通信连接。其中一种通信模型是，一个 UE 通过另一个 UE 的辅助接入到运营商网络，从而与数据网络进行业务交互。

例如，远端用户设备（Remote UE）通过中继用户设备（UE-to-Network Relay）获取
15 业务的流程中，为了保证通信安全，Remote UE 和 UE-to-Network Relay 之间需要建立安全连接。然而通过 UE-to-Network Relay 建立通信连接是按需动态建立的，Remote UE 和 UE-to-Network Relay 之间无法预配置共享的安全信息并基于预配置的共享安全信息建立 Remote UE 和 UE-to-Network Relay 之间的安全连接。因此亟需一种方法动态建立 Remote
20 UE 和 UE-to-Network Relay 之间的安全连接。

发明内容

本申请提供一种生成设备间通信的密钥的方法、系统和装置，使得用户设备与用户设备之间动态地建立了安全的通信连接。

第一方面，提供了一种生成设备间通信的密钥的方法，该方法包括：第一用户设备基
25 于第一密钥，生成第一临时标识；所述第一用户设备向第二用户设备发送第一请求，所述第一请求用于建立所述第一用户设备和所述第二用户设备之间的通信连接；其中，所述第一请求包括所述第一临时标识和中继服务码；所述第一用户设备基于第二密钥和所述中继服务码，生成共享密钥；其中，所述共享密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接，所述第二密钥与所述第一密钥为鉴权流程中生成的密钥或者是基于
30 鉴权流程中生成的中间密钥推演得到的密钥。

其中，所述共享密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接。一种可能的实现方式包含，第一用户设备和第二用户设备分别基于生成的共享密钥推演一个中间密钥或会话密钥，进一步的，基于中间密钥或会话密钥推演第一用户设备和第二用户设备之间的消息或数据的加密密钥和/或完整保护密钥。所述加密密钥和/或完整保护密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接。另一种可能的实现方式包含，第一用户设备和第二用户设备分别基于生成的共享密钥推演第一用户设备和第二用户设备之间的消息或数据的加密密钥和/或完整保护密钥。所述加密密钥和/或完整保护密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接。
35

基于上述方案，第一用户设备生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥，使得用户设备与用户设备之间动态地建立了安全的通信连接。

5 结合第一方面，在第一方面的某些实现方式中，所述第二密钥与所述第一密钥相同，且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

结合第一方面，在第一方面的某些实现方式中，所述第二密钥与所述第一密钥不同，且所述第一密钥为所述鉴权流程中生成的密钥 Kausf；所述第二密钥为基于所述 Kausf 推演得到的密钥。

10 结合第一方面，在第一方面的某些实现方式中，所述第二密钥与所述第一密钥不同，且所述第二密钥为所述鉴权流程中生成的密钥 Kausf；所述第一密钥为基于所述 Kausf 推演得到的密钥。

结合第一方面，在第一方面的某些实现方式中，所述第一用户设备基于第一密钥，生成第一临时标识，包括：所述第一用户设备基于所述第一密钥、所述第一用户设备的网络标识和路由信息，生成所述第一临时标识；其中，所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息，所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

其中，与所述第一用户设备相关的核心网网元具体可以是第一用户设备鉴权流程中涉及的核心网网元，例如数据管理网元和近距离业务安全功能网元。

20 基于上述技术方案，第一用户设备基于第一密钥、第一用户设备的网络标识和路由信息生成第一临时标识，并将所述第一临时标识发给所述第二用户设备。第二用户设备向网络侧发送所述第一临时标识，使得与第一用户设备用户相关的核心网网元能够根据第一临时标识获取上述第二密钥，进一步的该核心网网元根据第二密钥确定共享密钥并发送给所述第二用户设备，从而使得第一用户设备和第二用户设备获取相同的共享密钥。基于该共享密钥，第一用户设备和第二用户设备能够动态建立安全的通信连接。

结合第一方面，在第一方面的某些实现方式中，所述第一用户设备基于所述第一密钥、所述第一用户设备的网络标识和路由信息，生成所述第一临时标识，包括：所述第一用户设备基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数，得到第二临时标识；将所述第二临时标识和所述路由信息进行拼接，得到所述第一临时标识。

30 结合第一方面，在第一方面的某些实现方式中，所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI；所述路由信息为路由指示。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：所述第一用户设备向移动管理网元发送非接入层 NAS 消息，所述 NAS 消息包括能力信息，所述能力信息用于指示所述第一用户设备支持作为远端用户设备。

35 基于上述技术方案，第一用户设备通过向网络侧发送包括能力信息的 NAS 消息，以便作为网络侧确定第一用户设备是否具有支持作为远端用户设备的能力的依据，从而有助于第一用户设备生成共享密钥，使得用户设备与用户设备之间动态地建立安全的通信连接。

结合第一方面,在第一方面的某些实现方式中,所述第一请求还包括第一新鲜性参数;所述第一用户设备基于所述第二密钥和所述中继服务码,生成所述共享密钥,包括:所述第一用户设备基于所述第二密钥、所述中继服务码和所述第一新鲜性参数,生成所述共享密钥。

- 5 基于上述技术方案,第一用户设备基于所述第二密钥、所述中继服务码和所述第一新鲜性参数,生成所述共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,使得用户设备与用户设备之间建立的安全通信连接更可靠。

- 10 结合第一方面,在第一方面的某些实现方式中,该方法还包括:所述第一用户设备接收来自所述第二用户设备的安全模式命令,所述安全模式命令包括第二新鲜性参数;所述第一用户设备基于所述第二密钥和所述中继服务码,生成所述共享密钥,包括:所述第一用户设备基于所述第二密钥、所述中继服务码和所述第二新鲜性参数,生成所述共享密钥。

- 15 基于上述技术方案,第一用户设备基于所述第二密钥、所述中继服务码和所述第二新鲜性参数,生成所述共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,使得用户设备与用户设备之间建立的安全通信连接更可靠。

- 20 结合第一方面,在第一方面的某些实现方式中,所述第一请求还包括第一新鲜性参数;该方法还包括:所述第一用户设备接收来自所述第二用户设备的安全模式命令,所述安全模式命令包括第二新鲜性参数;所述第一用户设备基于所述第二密钥和所述中继服务码,生成所述共享密钥,包括:所述第一用户设备基于所述第二密钥、所述中继服务码、所述第一新鲜性参数和所述第二新鲜性参数,生成所述共享密钥。

- 25 基于上述技术方案,第一用户设备基于所述第二密钥、所述中继服务码、所述第一新鲜性参数和所述第二新鲜性参数,生成所述共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,使得用户设备与用户设备之间建立的安全通信连接更可靠。

- 30 结合第一方面,在第一方面的某些实现方式中,所述安全模式命令还包括安全算法;该方法还包括:所述第一用户设备基于所述共享密钥和所述安全算法,得到通信密钥;所述通信密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接。具体的,所述第一用户设备基于所述共享密钥和所述安全算法,得到通信密钥,还包括:所述第一用户设备基于所述共享密钥生成中间密钥/会话密钥,基于中间密钥/会话密钥和所述安全算法的到通信密钥。

基于上述技术方案,所述第一用户设备基于所述共享密钥和所述安全算法,得到通信密钥,使得用户设备与用户设备之间建立的安全通信连接得到保护,从而更加可靠。

- 35 第二方面,提供了一种生成设备间通信的密钥的方法,该方法包括:第一网元基于第一密钥,生成第一临时标识;所述第一网元接收来自第二网元的密钥获取消息,所述密钥获取消息包括第一用户设备的标识和中继服务码,其中,所述第一用户设备的标识包括所述第一临时标识或者所述第一用户设备的网络标识,所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息;所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥;其中,所述共享密钥用于保护所述第一用户设备和第

二用户设备之间的通信连接,所述第二密钥与所述第一密钥为所述第一用户设备的鉴权流程中生成的密钥或者是基于所述第一用户设备的鉴权流程中生成的中间密钥推演得到的密钥;所述第一网元向所述第二网元发送所述共享密钥。进一步地,第二网元将所述共享密钥发送给第二用户设备。

- 5 基于上述技术方案,第一网元生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥,并发送给第二用户设备,使得第二用户设备与第一用户设备之间可以基于所述共享密钥动态地建立了安全的通信连接。

结合第二方面,在第二方面的某些实现方式中,所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:所述第一网元根据所述第一用户设备的标识获取所述第二密钥,所述第一网元根据所述第二密钥和所述中继服务码,生成所述共享密钥。

- 10 基于上述技术方案,第一网元根据所述第一用户设备的标识获取所述第二密钥,使得第一网元可以根据所述第二密钥和所述中继服务码,生成用于保护设备间通信连接的共享密钥,使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 15 结合第二方面,在第二方面的某些实现方式中,所述第二密钥与所述第一密钥相同,且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

结合第二方面,在第二方面的某些实现方式中,所述第二密钥与所述第一密钥不同,且所述第一密钥为所述鉴权流程中生成的密钥 Kausf;所述第二密钥为基于所述 Kausf 推演得到的密钥。

- 20 结合第二方面,在第二方面的某些实现方式中,所述第二密钥与所述第一密钥不同,且所述第二密钥为所述鉴权流程中生成的密钥 Kausf;所述第一密钥为基于所述 Kausf 推演得到的密钥。

结合第二方面,在第二方面的某些实现方式中,所述第一网元基于第一密钥,生成第一临时标识,包括:所述第一网元基于所述第一密钥、所述第一用户设备的网络标识和路由信息,生成所述第一临时标识;其中,所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息,所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

- 25 结合第二方面,在第二方面的某些实现方式中,所述第一网元基于第一密钥、所述第一用户设备的网络标识和路由信息,生成第一临时标识,包括:所述第一网元基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数,得到第二临时标识;将所述第二临时标识和所述路由信息进行拼接,得到所述第一临时标识。

结合第二方面,在第二方面的某些实现方式中,所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI;所述路由信息为路由指示。

- 30 结合第二方面,在第二方面的某些实现方式中,该方法还包括:在对所述第一用户设备进行鉴权流程中,所述第一网元接收来自第三网元的指示信息;响应于所述指示信息,所述第一网元基于所述第一密钥,生成所述第一临时标识。

基于上述技术方案,第一网元响应于第三网元发送的指示信息,从而生成第一临时标

识。然后第一网元将所述生成的第一临时标识与所述第二密钥关联存储起来。后续当第一网元接收来自第二网元的携带第一临时标识的密钥获取消息时，第一网元能够根据所述第一临时标识获取上述第二密钥，从而有利于第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备，使得第一用户设备与第二用户设备之间基于共享密钥动态地建立安全的通信连接。

结合第二方面，在第二方面的某些实现方式中，在对所述第一用户设备进行鉴权流程中，所述第一网元接收来自第三网元的指示信息；响应于所述指示信息，所述第一网元基于所述第一密钥，生成所述第一临时标识，包括：在对所述第一用户设备进行鉴权流程中，所述第一网元接收来自第四网元的能力信息，所述能力信息用于指示所述第一用户设备支持远端 UE 的能力；响应于所述指示信息和所述能力信息，所述第一网元基于所述第一密钥，生成所述第一临时标识。

基于上述技术方案，第一网元响应于第三网元发送的指示信息和第四网元发送的能力信息，从而生成第一临时标识。然后第一网元将所述生成的第一临时标识与所述第二密钥关联存储起来。后续当第一网元接收来自第二网元的携带第一临时标识的密钥获取消息时，第一网元能够根据所述第一临时标识获取上述第二密钥，从而有利于第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备，使得第一用户设备与第二用户设备之间基于共享密钥动态地建立了安全的通信连接。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：所述第一网元将所述第一临时标识发送给第三网元。

基于上述技术方案，第一网元将所述第一临时标识发送给第三网元，第三网元将所述第一临时标识和所述第一网元的标识存储在所述第一用户设备的上下文信息中。后续第二网元可以根据所述第一临时标识从第三网元获取所述第一网元的标识和所述第一用户设备的网络标识。继而第二网元能够基于所述第一用户设备的网络标识从所述第一网元获取上述共享密钥并发送给第二用户设备，使得第一用户设备与第二用户设备之间可以基于所述共享密钥动态地建立安全的通信连接。

结合第二方面，在第二方面的某些实现方式中，所述密钥获取消息还包括第一新鲜性参数；所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数，生成共享密钥。

基于上述技术方案，第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数，生成共享密钥，保证针对第二密钥相同、中继服务码相同，但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥，从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：所述第一网元生成第二新鲜性参数；所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第二新鲜性参数，生成共享密钥。

基于上述技术方案，第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第二新鲜性参数，生成共享密钥，保证针对第二密钥相同、中继服务码相同，

但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥，从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第二方面，在第二方面的某些实现方式中，所述密钥获取消息还包括第一新鲜性参数；该方法还包括：所述第一网元生成第二新鲜性参数；所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述所述第一网元根据所述第一用户设备的标识、所述中继服务码、所述第二密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥。

基于上述技术方案，第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥，保证针对第二密钥相同、中继服务码相同，但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥，从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第二方面，在第二方面的某些实现方式中，所述第一网元为鉴权功能网元。

结合第二方面，在第二方面的某些实现方式中，所述第二网元为移动管理网元、鉴权功能网元或近距离业务安全功能网元。

结合第二方面，在第二方面的某些实现方式中，所述第三网元为数据管理网元。

结合第二方面，在第二方面的某些实现方式中，所述第四网元为移动管理网元。

第三方面，提供了一种生成设备间通信的密钥的方法，该方法包括：第五网元获取第一临时标识和第三密钥，所述第三密钥为基于鉴权流程中生成的中间密钥推演得到的密钥；所述第五网元接收来自第六网元的密钥获取消息，所述密钥获取消息包括所述第一临时标识和中继服务码；所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥；其中，所述共享密钥用于保护所述第一用户设备和第二用户设备之间的通信连接；所述第五网元向所述第六网元发送所述共享密钥。

基于上述技术方案，第五网元生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥，使得用户设备与用户设备之间动态地建立了安全的通信连接。

结合第三方面，在第三方面的某些实现方式中，所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥；包括：所述第五网元根据所述第一临时标识获取所述第三密钥，所述第五网元根据所述第三密钥和中继服务码生成共享密钥。

基于上述技术方案，第五网元根据所述第一临时标识获取所述第三密钥，使得第五网元可以根据所述第三密钥和所述中继服务码，生成用于保护设备间通信连接的共享密钥，第五网元将共享密钥经由一或多个中间网元发送给第二用户设备，保证了第一用户设备和第二用户设备之间动态建立了共享密钥，基于共享密钥，使得用户设备与用户设备之间动态地建立了安全的通信连接。

结合第三方面，在第三方面的某些实现方式中，第五网元获取第一临时标识，包括：第五网元从所述第一网元接收到所述第一临时标识，所述第一临时标识是基于第一中间密钥生成的，所述第一中间密钥为对所述第一用户设备进行鉴权流程中生成的中间密钥或者是基于鉴权流程中生成的中间密钥推演得到的密钥；或者，第五网元基于第三中间密钥生成所述第一临时标识。

基于上述技术方案，第五网元获取所述第一临时标识，从而使得第五网元可以根据所述第一临时标识获取所述第三密钥，使得第五网元可以根据所述第三密钥和所述中继服务码，生成用于保护设备间通信连接的共享密钥，第五网元将共享密钥经由一或多个中间网元发送给第二用户设备，保证了第一用户设备和第二用户设备之间动态建立了共享密钥，

5 基于共享密钥，继而使得用户设备与用户设备之间动态地建立了安全的通信连接。

结合第三方面，在第三方面的某些实现方式中，所述第三密钥为基于所述鉴权流程中生成的密钥 Kausf 推演得到的密钥。

结合第三方面，在第三方面的某些实现方式中，所述第一临时标识是基于所述第一密钥生成的，包括：所述第一临时标识是基于所述第一密钥、所述第一用户设备的网络标识和路由信息生成的；其中，所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息，所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

10

结合第三方面，在第三方面的某些实现方式中，所述第一临时标识是基于所述第一密钥、所述第一用户设备的网络标识和路由信息生成的，包括：所述第二临时标识是基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数得到的；所述第一临时标识是将所述第二临时标识和所述路由信息进行拼接得到的。

15

结合第三方面，在第三方面的某些实现方式中，所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI；所述路由信息为路由指示。

结合第三方面，在第三方面的某些实现方式中，所述密钥获取消息还包括第一新鲜性参数；所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥和所述第一新鲜性参数，生成共享密钥。

20

基于上述技术方案，第五网元根据所述第一临时标识、所述中继服务码、第二密钥和所述第一新鲜性参数，生成共享密钥，保证针对第二密钥相同、中继服务码相同，但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥，从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

25

结合第三方面，在第三方面的某些实现方式中，该方法还包括：所述第五网元生成第二新鲜性参数；所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥和所述第二新鲜性参数，生成共享密钥。

30

基于上述技术方案，第五网元根据所述第一临时标识、所述中继服务码、第二密钥和所述第二新鲜性参数，生成共享密钥，保证针对第二密钥相同、中继服务码相同，但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥，从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第三方面，在第三方面的某些实现方式中，所述密钥获取消息还包括第一新鲜性参数；该方法还包括：所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥。

35

基于上述技术方案，第五网元根据所述第一临时标识、所述中继服务码、第二密钥、

第一临时标识和所述第二新鲜性参数,生成共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

5 结合第三方面,在第三方面的某些实现方式中,所述第五网元为第一近距离业务安全功能网元。

结合第三方面,在第三方面的某些实现方式中,所述第五网元为第一近距离业务安全功能网元。

结合第三方面,在第三方面的某些实现方式中,所述第六网元为第二近距离业务安全功能网元。

10 第四方面,提供了一种生成设备间通信的密钥的系统,该系统包括:第一网元,用于基于第一密钥生成第一临时标识;第二网元,用于向第一网元发送密钥获取消息,所述密钥获取消息包括第一用户设备的标识和中继服务码,其中,所述第一用户设备的标识包括所述第一临时标识或者所述第一用户设备的网络标识,所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息;所述第一网元还用于根据所述第一用户设备的标识、所述
15 中继服务码以及第二密钥,生成共享密钥;其中,所述共享密钥用于保护所述第一用户设备和第二用户设备之间的通信连接,所述第二密钥与所述第一密钥为所述第一用户设备的鉴权流程中生成的密钥或者是基于所述第一用户设备的鉴权流程中生成的中间密钥推演得到的密钥;所述第一网元向所述第二网元发送所述共享密钥。

20 基于上述技术方案,第一网元生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥,使得用户设备与用户设备之间动态地建立了安全的通信连接。

结合第四方面,在第四方面的某些实现方式中,所述第一网元还用于根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:所述第一网元还用于根据所述第一用户设备的标识获取所述第二密钥,所述第一网元还用于根据所述第二密
25 钥和所述中继服务码,生成所述共享密钥。

基于上述技术方案,第一网元根据所述第一用户设备的标识获取所述第二密钥,使得第一网元可以根据所述第二密钥和所述中继服务码,生成用于保护设备间通信连接的共享密钥,使得用户设备与用户设备之间动态地建立了安全的通信连接。

30 结合第四方面,在第四方面的某些实现方式中,所述第二密钥与所述第一密钥相同,且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

结合第四方面,在第四方面的某些实现方式中,所述第二密钥与所述第一密钥不同,且所述第一密钥为所述鉴权流程中生成的密钥 Kausf;所述第二密钥为基于所述 Kausf 推演得到的密钥。

35 结合第四方面,在第四方面的某些实现方式中,所述第二密钥与所述第一密钥不同,且所述第二密钥为所述鉴权流程中生成的密钥 Kausf;所述第一密钥为基于所述 Kausf 推演得到的密钥。

结合第四方面,在第四方面的某些实现方式中,所述第一网元,用于基于第一密钥,生成第一临时标识,包括:所述第一网元还用于,基于所述第一密钥、所述第一用户设备

的网络标识和路由信息,生成所述第一临时标识;其中,所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息,所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

5 基于上述技术方案,第一网元基于第一密钥、第一用户设备的网络标识和路由信息生成第一临时标识,使得与第一用户设备相关的核心网网元能够根据第一临时标识获取上述第二密钥,进一步地根据第二密钥确定共享密钥并发送给第二用户设备,保证第一用户设备和第二用户设备获取相同的共享密钥。基于该共享密钥,使得用户设备与用户设备之间动态地建立了安全的通信连接。

10 结合第四方面,在第四方面的某些实现方式中,所述第一网元还用于,基于所述第一密钥、所述第一用户设备的网络标识和路由信息,生成所述第一临时标识,包括:所述第一网元还用于,基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数,得到第二临时标识;将所述第二临时标识和所述路由信息进行拼接,得到所述第一临时标识。

15 基于上述技术方案,第一网元基于第一密钥、第一用户设备的网络标识和路由信息生成第一临时标识,使得与第一用户设备相关的核心网网元能够根据第一临时标识获取上述第二密钥,从而有利于第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

20 结合第四方面,在第四方面的某些实现方式中,所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI;所述路由信息为路由指示。

结合第四方面,在第四方面的某些实现方式中,该系统还包括:第三网元,在对所述第一用户设备进行鉴权流程中,所述第三网元用于向所述第一网元发送第一指示信息;响应于所述第一指示信息,所述第一网元用于,基于所述第一密钥,生成所述第一临时标识。

25 基于上述技术方案,第一网元响应于第三网元发送的指示信息,从而生成第一临时标识,使得第一网元能够根据第一临时标识获取上述第二密钥,从而有利于第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

30 结合第四方面,在第四方面的某些实现方式中,该系统还包括:第四网元,在对所述第一用户设备进行鉴权流程中,所述第四网元用于向所述第一网元发送能力信息,所述能力信息用于指示所述第一用户设备支持远端 UE 的能力;响应于所述第一指示信息和所述能力信息,所述第一网元用于,基于所述第一密钥,生成所述第一临时标识。

35 基于上述技术方案,第一网元响应于第三网元发送的指示信息和第四网元发送的能力信息,从而生成第一临时标识,使得第一网元能够根据第一临时标识获取上述第二密钥,从而有利于第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

结合第四方面,在第四方面的某些实现方式中,所述第一网元还用于将所述第一临时标识发送给所述第三网元。

基于上述技术方案,第一网元将所述第一临时标识发送给第三网元,第三网元将所述第一临时标识存储在所述第一用户设备的上下文信息中,以便于所述第三网元根据所述第

一临时标识从所述第一用户设备的上下文中确定所述第一网元的标识,继而使得第一网元能够根据第一临时标识获取上述第二密钥,从而使得第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 5 结合第四方面,在第四方面的某些实现方式中,所述第二网元还用于,向所述第三网元发送所述第一临时标识;所述第三网元还用于,向所述第二网元发送所述第一网元的标识。

10 基于上述技术方案,第二网元向第三网元发送所述第一临时标识(由第一用户设备经由一或多个中间网元发送给第二网元的第一临时标识),用于第三网元根据第一临时标识从所述第一用于设备的上下文中确定所述第一网元的标识,继而使得第一网元能够根据第一临时标识获取上述第二密钥,从而使得第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 15 结合第四方面,在第四方面的某些实现方式中,所述第三网元还用于,向所述第二网元发送所述第一网元的标识和第一用户设备的网络标识。

20 基于上述技术方案,第三网元向第二网元发送第一网元的标识和第一用户设备的网络标识,使得第二网元根据第一网元的标识找到第一网元,从而使得第一网元能够根据第一临时标识或第一用户设备的网络标识获取上述第二密钥,从而使得第一网元根据第二密钥确定共享密钥并经由一或多个中间网元发送给第二用户设备,使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 25 结合第四方面,在第四方面的某些实现方式中,所述密钥获取消息还包括第一新鲜性参数;所述第一网元用于,根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:所述第一网元用于,根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数,生成共享密钥。

30 基于上述技术方案,第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数,生成共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

- 35 结合第四方面,在第四方面的某些实现方式中,所述第一网元还用于,生成第二新鲜性参数;所述第一网元用于,根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:所述所述第一网元用于,根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第二新鲜性参数,生成共享密钥。

基于上述技术方案,第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第二新鲜性参数,生成共享密钥,保证针对第二密钥相同、中继服务码相同,但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥,从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第四方面,在第四方面的某些实现方式中,所述密钥获取消息还包括第一新鲜性参数;所述第一网元还用于,生成第二新鲜性参数;所述第一网元用于,根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:所述所述第一网元

用于, 根据所述第一用户设备的标识、所述中继服务码、第二密钥、所述第一新鲜性参数和所述第二新鲜性参数, 生成共享密钥。

- 5 基于上述技术方案, 第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥、所述第一新鲜性参数和所述第二新鲜性参数, 生成共享密钥, 保证针对第二密钥相同、中继服务码相同, 但第一用户设备在与不同的用户设备建立直接通信时生成不同的共享密钥, 从而使得用户设备与用户设备之间建立的安全通信连接更可靠。

结合第四方面, 在第四方面的某些实现方式中, 该系统还包括: 第一用户设备和第二用户设备。

- 10 结合第四方面, 在第四方面的某些实现方式中, 所述第一网元为鉴权功能网元。
结合第四方面, 在第四方面的某些实现方式中, 所述第二网元为移动管理网元、鉴权功能网元或近距离业务安全功能网元。

结合第四方面, 在第四方面的某些实现方式中, 所述第三网元为数据管理网元。

结合第四方面, 在第四方面的某些实现方式中, 所述第四网元为移动管理网元。

- 15 第五方面, 提供了一种生成设备间通信的密钥的装置, 该装置包括: 存储器, 用于存储计算机指令; 处理器, 用于执行所述存储器中存储的计算机指令, 使得所述装置执行第一方面或第一方面中任意一种可能的实现方式中所述的方法。

- 20 基于上述技术方案, 所述生成设备间通信的密钥的装置通过执行第一方面或第一方面中任意一种可能的实现方式中所述的方法, 使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥, 从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

第六方面, 提供了一种生成设备间通信的密钥的装置, 该装置包括: 存储器, 用于存储计算机指令; 处理器, 用于执行所述存储器中存储的计算机指令, 使得所述装置执行第二方面或第二方面中任意一种可能的实现方式中所述的方法。

- 25 基于上述技术方案, 所述生成设备间通信的密钥的装置通过执行第二方面或第二方面中任意一种可能的实现方式中所述的方法, 使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥, 从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 30 第七方面, 提供了一种生成设备间通信的密钥的装置, 该装置包括: 存储器, 用于存储计算机指令; 处理器, 用于执行所述存储器中存储的计算机指令, 使得所述装置执行第三方面或第三方面中任意一种可能的实现方式中所述的方法。

- 35 基于上述技术方案, 所述生成设备间通信的密钥的装置通过执行第三方面或第三方面中任意一种可能的实现方式中所述的方法, 使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥, 从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

第八方面, 提供了一种可读计算机存储介质, 其上存储有计算机程序, 所述计算机程序被通信装置执行时, 使得所述通信装置执行第一方面或第一方面中任意一种可能的实现方式中所述的方法。

基于上述技术方案, 所述可读计算机存储介质上存储有计算机程序, 所述计算机程序被生成设备间通信的密钥的装置执行时, 通过执行第一方面或第一方面中任意一种可能的

实现方式中所述的方法,使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥,从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 5 第九方面,提供了一种可读计算机存储介质,其上存储有计算机程序,所述计算机程序被通信装置执行时,使得所述通信装置执行第二方面或第二方面中任意一种可能的实现方式中所述的方法。

- 10 基于上述技术方案,所述可读计算机存储介质上存储有计算机程序,所述计算机程序被生成设备间通信的密钥的装置执行时,通过执行第二方面或第二方面中任意一种可能的实现方式中所述的方法,使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥,从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

第十方面,提供了一种可读计算机存储介质,其上存储有计算机程序,所述计算机程序被通信装置执行时,使得所述通信装置执行第三方面或第三方面中任意一种可能的实现方式中所述的方法。

- 15 基于上述技术方案,所述可读计算机存储介质上存储有计算机程序,所述计算机程序被生成设备间通信的密钥的装置执行时,通过执行第三方面或第三方面中任意一种可能的实现方式中所述的方法,使得所述装置生成了可用于保护所述第一用户设备和所述第二用户设备之间的通信连接的共享密钥,从而使得用户设备与用户设备之间动态地建立了安全的通信连接。

- 20 第十一方面,提供了一种芯片系统,所述芯片系统包括处理器,用于从存储器中调用并运行计算机程序,使得安装有所述芯片系统的设备执行第一方面或第一方面中任意一种可能的实现方式中所述的通信方法。

- 25 可选地,该芯片系统还可以包括存储器,该存储器中存储有指令,处理器用于执行存储器中存储的指令或源于其他的指令。当该指令被执行时,处理器用于实现上述第一方面或其任意可能的实现方式中的方法。

可选地,该芯片系统可以集成在用户设备上。

第十二方面,提供了一种芯片系统,所述芯片系统包括处理器,用于从存储器中调用并运行计算机程序,使得安装有所述芯片系统的设备执行第二方面或第二方面中任意一种可能的实现方式中所述的通信方法。

- 30 可选地,该芯片系统还可以包括存储器,该存储器中存储有指令,处理器用于执行存储器中存储的指令或源于其他的指令。当该指令被执行时,处理器用于实现上述第二方面或其任意可能的实现方式中的方法。

可选地,该芯片系统可以集成在网络设备上。

- 35 第十三方面,提供了一种芯片系统,所述芯片系统包括处理器,用于从存储器中调用并运行计算机程序,使得安装有所述芯片系统的设备执行第三方面或第三方面中任意一种可能的实现方式中所述的通信方法。

可选地,该芯片系统还可以包括存储器,该存储器中存储有指令,处理器用于执行存储器中存储的指令或源于其他的指令。当该指令被执行时,处理器用于实现上述第三方面或其任意可能的实现方式中的方法。

可选地，该芯片系统可以集成在网络设备上。

综上所述，基于上述技术方案，通过生成设备间的通信密钥，使得用户设备与用户设备之间动态地建立了安全的通信连接。

5 附图说明

图 1 是应用于本申请实施例的场景示意图

图 2 是应用于本申请实施例的网络架构示意图

图 3 是本申请实施例提供的一例的网络侧推演远端用户设备的临时标识的方法的示意性交互流程图

10 图 4 是本申请实施例提供的一例的远端用户设备通过中继用户设备接入网络的方法的示意性交互流程图

图 5 是本申请实施例提供的另一例的网络侧推演远端用户设备的临时标识的方法的示意性交互流程图

15 图 6 是本申请实施例提供的另一例的远端用户设备通过中继用户设备接入网络的方法的示意性交互流程图

图 7 是本申请实施例提供的另一例的网络侧推演远端用户设备的临时标识的方法的示意性交互流程图

图 8 是本申请实施例提供的另一例的远端用户设备通过中继用户设备接入网络的方法的示意性交互流程图

20 图 9 是本申请实施例提供的一例的通信装置的示意性框图

图 10 是本申请实施例提供的另一例的通信设备的示意性框图

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

25 本申请实施例提及的无线通信系统包括但不限于：全球移动通信（global system of mobile communication, GSM）系统、长期演进（long term evolution, LTE）频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）、宽带码分多址（wideband code division multiple access, WCDMA）系统、码分多址（code division multiple access, CDMA）系统、时分同步码分多址（time division-synchronous code division multiple access, TD-SCDMA）、通用分集无线业务（general packet radio service, GPRS）、LTE
30 系统、先进的长期演进（LTE-Advanced, LTE-A）系统、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、下一代通信系统（例如，5G 通信系统）、多种接入系统的融合系统，或演进系统、下一代 5G 移动通信系统的三大应用场景：增强移动
35 宽带（enhanced mobile broadband, eMBB）、极可靠低时延通信（ultra-reliable and low latency communication, URLLC）、和增强型机器类型通信（enhanced machine-type communication, eMTC）或者将来出现的新的通信系统。

通常来说，传统的通信系统支持连接数有限，也易于实现，然而，随着通信技术的发展，移动通信系统将不仅支持传统的通信，还将支持例如，设备到设备（Device to Device，

D2D)通信, 机器到机器 (Machine to Machine, M2M)通信, 机器类型通信 (Machine Type Communication, MTC), 车联网 (Vehicle To Everything, V2X)通信, 例如, 车到车 (Vehicle to Vehicle, V2V)通信、车到基础设施 (Vehicle to Infrastructure, V2I)通信, 车到行人 (Vehicle to Pedestrian, V2P)通信, 车道网络 (Vehicle to Network, V2N)通信。

5 本申请实施例中所涉及到的终端设备可以包括各种具有无线通信功能的接入终端、移动设备、用户终端、或用户装置。例如, 用户设备 (user equipment, UE)、手持终端、笔记本电脑、用户单元 (subscriber unit)、蜂窝电话 (cellular phone)、智能电话 (smart phone)、无线数据卡、个人数字助理 (personal digital assistant, PDA) 电脑、平板型电脑、无线调制解调器 (modem)、手持设备 (handheld)、膝上型电脑 (laptop computer)、
10 无绳电话 (cordless phone) 或者无线本地环路 (wireless local loop, WLL) 台、机器类型通信 (machine type communication, MTC) 终端或是其他可以接入网络的设备。终端设备与接入网设备之间采用某种空口技术相互通信。本申请的实施例对应用场景不做限定。

图 1 示出了应用于本申请实施例的场景示意图, 如图 1 所述, Remote UE 通过 UE-to-Network Relay 接入到运营商网络从而与数据网络进行业务交互。

15 应理解, 图 1 仅是为了便于理解, 对本申请实施例的应用场景的示意图的示例, 本申请实施例对此并不作任何限定, 以下对该示意图中涉及到的网元进行说明。

Remote UE: 一个具备近距离通信的 UE, 能通过中继设备与数据网络 (data network, DN) 通信。例如可以是具备通过另一个 UE 接入并访问网络的能力的 UE。

20 UE-to-Network Relay: 可以是具备为另一 UE 提供接入, 并为该 UE 提供访问网络功能的 UE。

(无线) 接入网络 (radio access network, (R)AN) 网元: 为终端设备提供接入的设备, 包含 RAN 设备和 AN 设备。RAN 设备主要是 3GPP 网络无线网络设备, AN 可以是 non-3GPP 定义的接入网设备, 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。所述接入网设备可以包括各种形式的基站, 例如: 宏基站,
25 微基站 (也称为小站), 中继站, 接入点等。在采用不同的无线接入技术的系统中, 具备基站功能的设备的名称可能会有所不同, 例如, 在第五代 (5th generation, 5G) 系统中, 称为 RAN 或者 gNB(5G NodeB); 在 LTE 系统中, 称为演进的节点 B (evolved NodeB, eNB 或者 eNodeB); 在第三代 (3rd generation, 3G) 系统中, 称为节点 B (Node B) 等。

30 网关: 主要负责对外连接到数据网络以及用户面的数据包路由转发、报文过滤、执行服务质量控制相关功能等。可以从数据网络接收用户数据, 通过接入网设备传输给终端设备, 还可以通过接入网设备从终端设备接收用户数据, 转发到数据网络。在 5G 通信系统中, 该用户面网元可以是用户面功能 (user plane function, UPF) 网元。在未来通信系统中, 用户面网元仍可以是 UPF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

35 图 2 示出了应用于本申请实施例的 5G 网络架构示意图。作为示例而非限定, 本申请实施例可应用于 5G 通信系统的网络架构, 以下对该网络架构中可能涉及的各个网元分别进行说明。

鉴权服务功能 (authentication server function, AUSF) 网元: 支持接入时的鉴权功能。在本申请实施例中, AUSF 网元用于实现 UE 接入网络时的鉴权, 用于生成密钥, 还可以用于对 Remote UE 的授权判定。

统一数据管理 (unified data management, UDM) 网元: 用于生成认证信任状, 用户标识处理 (如存储和管理用户永久身份等), 接入授权控制和签约数据管理等。在本申请实施例中, UDM 用于对 Remote UE 进行授权判定, 存储用户信息等。

策略控制功能 (policy control function, PCF) 网元: 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。

网络开放功能 (network exposure function, NEF) 网元: 用于安全地向外部开放由 3GPP 网络功能提供的业务和能力等。

应用功能网元 (application function, AF): 用于提供业务, 或者进行应用影响的数据路由, 接入网络开放功能网元, 或, 与 PCF 网元交互业务数据进行策略控制等。

网络鉴权功能 (network repository function, NRF) 网元, 用于网络中一个网络功能 (Network Function, NF) 网元发现另一个 NF 的网元, 例如, AMF、SMF、PCF 以及 UDM 等网络功能实体都称为 NF 网元。在本申请实施例中, NRF 用于根据 AUSF 的实例标识 (Instance ID) 找到其路由信息, 并发送给 PSF。

统一数据存储网元 (unified data repository, UDR): 即, 用于存储用户签约数据、业务策略数据、非结构化数据等。

移动性管理功能网元 (access and mobility management function, AMF) 网元: 主要用于移动性管理和接入管理等, 可以用于实现移动性管理实体 (mobility management entity, MME) 功能中除会话管理之外的其它功能, 例如, 终端移动性管理、终端鉴权与去鉴权、终端会话接入、终端的允许的切片接入选择、合法监听或接入授权 (或鉴权) 等功能。

会话管理功能网元 (session management function, SMF) 网元: 主要用于会话管理、终端设备的网际互连协议 (internet protocol, IP) 地址分配和管理、选择和管理用户平面功能、策略控制、收费功能接口的终结点或下行数据通知等。

用户面功能网元 (user plane function, UPF): 可用于分组路由和转发、或用户面数据的服务质量 (quality of service, QoS) 参数处理等。用户数据可通过该网元传输到数据网络 (data network, DN)。

PC5: 具备近距离通信能力的 UE 之间的参考点, 用于近距离通信直接发现 (ProSe Direct Discovery)、近距离通信直接通信 (ProSe Direct Communication) 和 UE-to-Network Relay 的控制面连接和用户面连接。

图 2 中, UE A 可以直接通过 Uu 接口接入网络, 也可以先通过 PC5 接口与 UE C 建立连接, 再通过 UE C 接入网络。UE B 先通过 PC5 接口与 UE A 建立连接, 再通过 UE A 接入网络; UE C 可以通过 Uu 接口接入网络, 也可以先通过 PC5 接口与 UE A 建立连接, 再通过 UE A 接入网络。

示例性的, 图 2 中, UE A 和 UE C 都可以通过 Uu 接口直接接入网络。UE A 还可以先通过 PC5 接口与 UE C 建立连接, 再通过 UE C 接入网络 (此时, UE A 称为 Remote UE, UE C 称为 UE-to-Network Relay); UE C 也可以先通过 PC5 接口与 UE A 建立连接, 再通过 UE A 接入网络 (此时, UE C 称为 Remote UE, UE A 称为 UE-to-Network Relay)。UE B 先通过 PC5 接口与 UE A 建立连接, 再通过 UE A 接入网络 (此时, UE B 称为 Remote UE, UE A 称为 UE-to-Network Relay)。

其中，UE A 和 UE C 既可以认为是具有为另一个 Remote UE 提供网络连接功能的 UE-to-Network Relay，也可以认为是具有通过另一个 UE-to-Network Relay 接入并访问网络能力的 Remote UE。

5 UE B 可以认为是具有通过另一个 UE-to-Network Relay 接入并访问网络能力的 Remote UE，通过 UE-to-Network Relay A 接入网络。

图 3 示出了本申请实施例 UE#1（即，第一用户设备的一例）鉴权过程中或之后，网络侧推演 Remote UE#1 的临时标识的示意性流程图，包括以下步骤：

在该流程中，UDM 生成指示信息，并向 AUSF#1 发送，例如可以列举以下实现方式：方式 1，如下述 S400a~S440a：

10 S400a，UE#1 向 AMF#1 上报能力信息，该能力信息用于指示该 UE#1 是否支持作为 Remote UE 的能力。

例如，UE 侧向网络侧上报能力信息可以在 UE#1 向 AMF#1（即，第四网元的一例）发送非接入层 NAS 消息（例如，是注册请求消息）中携带。

S410a，AMF#1 向 AUSF#1 发送 UE#1 的能力信息。

15 例如，AMF#1 向 AUSF#1 发送 UE#1 的能力信息，可以在 AMF#1 向 AUSF#1 发送的鉴权请求消息（例如 Nausf_UEAuthentication_Authenticate Request）中携带。

S420a，AUSF#1 接收到 S410 发送的能力信息，并向 UDM（即，第三网元的一例）发送该能力信息。

20 例如，AUSF#1 可以向 UDM 发送包含 UE#1 的能力信息的鉴权请求消息（例如 Nudm_UEAuthentication Request 消息）。

S430a，UDM 根据所述能力信息和 UE#1 的签约数据生成指示信息#1，所述指示信息#1 用于指示是否生成 UE#1 的用于近距离通信的信息，例如该信息用于标识 UE#1；

应理解，为了便于描述，以下实施例以临时标识#1（即，第一临时标识的一例）作为 UE#1 的用于近距离通信的信息为例进行阐述，但本申请实施例对此不做任何限定。

25 作为实施例而非限定，UDM 可以根据携带能力信息的鉴权请求消息获取 UE#1 的签约信息，根据 UE#1 的签约数据和 UE#1 的能力信息确定指示信息#1。

其中，UDM 根据 UE#1 的能力信息和 UE#1 的签约数据确定指示信息#1 包括：

30 若 UE#1 的签约数据指示 UE#1 被授权作为 Remote UE 通过中继用户设备与数据网络进行通信，且 UE#1 的能力信息表示 UE#1 具备作为 Remote UE 的能力，则 UDM 指示 AUSF#1 生成指示信息#1。若其中任一条件不满足，则 UDM 不向 AUSF 发送指示信息#1 或指示信息#1 指示 AUSF#1 不生成临时标识#1。

S440a：UDM 向 AUSF#1 发送指示信息#1。

例如，所述指示信息#1 可以在鉴权过程中 UDM 向 AUSF#1 发送的鉴权响应消息中携带（例如，Nudm_UEAuthentication response），也可以在鉴权请求过程后发送。

35 方式 2，如下述 S400b~S440b：

S400b~S410b 与上述 S400a~S410a 相同，为简洁此处不再赘述。

S420b，AUSF#1 向 UDM 发送鉴权请求消息，其中鉴权请求消息与现有技术相同或类似；

S430b，UDM 根据鉴权请求消息获取 UE#1 签约数据，生成指示信息#2，所述指示信

息#2 用于指示 UE#1 是否被授权作为 Remote UE;

S440b, UDM 向 AUSF#1 发送指示信息#2。

例如, 所述指示信息#2 可以在鉴权过程中 UDM 向 AUSF#1 发送的鉴权响应消息中携带 (例如, Nudm_UEAuthentication response), 也可以在鉴权过程后发送。

5 方式 3, 如下述 S400c~S440c:

S400c, UE#1 向 AMF#1 发送注册请求消息, 其中注册请求消息与现有技术相同或类似;

S410c, AMF#1 向 AUSF#1 发送鉴权请求消息, 其中鉴权请求消息与现有技术相同或类似;

10 S420c~S440c 与上述 S420b~S440b 相同, 此处不再赘述。

S450, AUSF#1 根据以下三种情况中的任何一种确定生成临时标识#1:

情况 1: 与上述方式 1 相对应, AUSF#1 接收到指示信息#1, 且所述指示信息#1 指示生成临时标识#1。

15 情况 2: 与上述方式 2 相对应, AUSF#1 接收到所述能力信息和指示信息#2, 所述能力信息和指示信息#2 都指示 UE#1 可以作为 Remote UE。

情况 3: 与上述方式 3 相对应, AUSF#1 接收到指示信息#2, 且指示信息#2 指示 UE#1 被授权作为 Remote UE。

其中, 生成临时标识#1 的过程可以根据密钥#1 (即, 第一密钥的一例) 和 Remote UE#1 的网络标识生成临时标识#1, 例如可以列举以下实现方式:

20 在一种实现方式中, AUSF#1 根据 AMF#1 在鉴权流程中发送的 Remote UE#1 的网络标识和 AUSF#1 在鉴权流程中生成的密钥#1, 生成临时标识#1, 生成过程所使用的算法可以与现有技术相同或相似, 为了避免赘述未详细说明。

在另一种实现方式中, AUSF#1 根据临时标识#1 (即, 第二临时标识的一例) 和 UDM 的路由信息拼接得到临时标识#1' (即, 第一临时标识的另一例)

25 其中, Remote UE 的网络标识可以列举如下: 用户永久标识 (subscription permanent identifier, SUPI) 或者国际移动用户识别码 (international mobile subscriber identity, IMSI) 或者 (generic public subscription identifier, GPSI)

其中, 路由信息可以列举如下: 路由指示 (Routing indicator)。

30 应理解, 在本申请实施例中, AUSF#1 可以存储临时标识#1 及其与密钥#1 的对应关系; 也可以不存储临时标识#1, 存储 Remote UE#1 的网络标识和密钥#1 的对应关系。

其中, 密钥#1 可以是对 UE#1 进行鉴权流程中生成的密钥或者是基于鉴权流程中生成的中间密钥推演得到的密钥。

例如, 密钥#1 可以是基于鉴权过程中生成的密钥 Kausf#1, 也可以是基于 Kausf#1 推演的密钥 Kpru#1。

35 作为实施例而非限定, AUSF#1 根据临时标识#1 和 UDM 的路由信息拼接得到临时标识#1', 包括以下实现方式:

一种可能的实现方式: 临时标识#1 可以用 X 位来表示, 其中, 高 Y 位用于表示所述路由信息; 剩余的低(X-Y)位用于表示所述临时标识#1', 其中 X 和 Y 为正整数;

另一种可能的实现方式: 临时标识#1 可以用 X 位来表示, 其中, 低 Y 位用于表示所

述路由信息；剩余的高(X-Y)位用于表示所述临时标识#1'，其中X和Y为正整数。

应理解，AUSF#1还可以在生成临时标识#1后，生成基于鉴权流程中生成的中间密钥推演得到的密钥，例如Kpru#1。本申请实施例对此不作任何限定。

S460，AUSF向UDM发送临时标识#1。

- 5 具体的，AUSF#1将临时标识#1和Remote UE#1的网络标识发送给UDM，UDM根据Remote UE#1的网络标识将临时标识#1存储在Remote UE#1的上下文信息中。

其中，UE的上下文中还包含AUSF的标识。

图4示出了本申请实施例Remote UE#1通过UE-to-Network Relay#1（即，第二用户设备的一例）接入网络阶段的示意性流程图，包括以下步骤：

- 10 S470，Remote UE#1发现一个或多个UE-to-Network Relay，并从中选择一个UE-to-Network Relay（计作UE-to-Network Relay#1，即第二用户设备的一例）进行通信，Remote UE#1选择UE-to-Network Relay#1的方式与现有技术相同或类似，本申请实施例对此不作任何限定。

S480，Remote UE#1生成临时标识#1'（即，第一临时标识的一例）。

- 15 Remote UE#1生成临时标识#1'的方式与S450中AUSF生成临时标识#1'的方式相同，即Remote UE#1根据临时标识#1和UDM的路由信息拼接得到临时标识#1'，为避免赘述，此处不再详细说明。

- S490，Remote UE#1向UE-to-Network Relay#1发送请求消息#1（即，第一请求的一例），该请求消息#1用于请求建立所述Remote UE#1和UE-to-Network Relay#1之间的通信连接，例如直连通信请求（direct communication request，DCR）消息。请求消息#1包括临时标识#1'和中继服务码Relay service code。
- 20

应理解，Relay service code可以是UE侧预配置的，还可以是网络侧发送给UE的，例如例如TS23.502中定义的UE Configuration Update流程。

- 其中，Relay service code用于标识支持ProSe服务的UE-to-Network Relay提供的连接服务，以及标识支持ProSe服务的UE-to-Network Relay提供服务的授权用户，并且可以选择相关的安全策略或信息。
- 25

在一种可能的实现方式中，请求消息#1还可以包括新鲜性参数#1（即，第一新鲜性参数的一例）。

- 在另一种可能的实现方式中，请求消息#1还可以包括完整性消息认证码（message authentication code for integrity，MAC-I）（计作MAC-I#1）。
- 30

具体地，Remote UE#1将Relay service code作为输入参数，基于密钥#1根据特定算法生成出密钥#A，Remote UE#1使用密钥#A加密临时标识#1'和Relay service code后，生成MAC-I#1，用于验证请求消息#1的完整性保护，防止请求消息#1被攻击者篡改。

- 作为实施例而非限定，以下S4100~S4130，S4150中，网元#2（即，第二网元）可以是PSF#1，可以是AMF#2，也可以是AUSF#2。
- 35

应理解，AMF#2可以是与AMF#1相同的AMF，也可以是与AMF#1不同的AMF。

其中，AMF#1可以为服务remote UE#1的AMF，AMF#2可以为服务UE-to-Network Relay#1的AMF。

应理解，AUSF#2可以是与AUSF#1相同的AUSF，也可以是与AUSF#1不同的AUSF。

其中, AUSF#1 可以为服务 remote UE#1 的 AUSF, AUSF#2 可以为服务 UE-to-Network Relay#1 的 AUSF。

应理解, AMF#2 可以是与 AMF#1 相同的 AMF, 也可以是与 AMF#1 不同的 AMF。

例如, AMF#1 可以为服务 remote UE#1 的 AMF, AMF#2 可以为服务 UE-to-Network
5 Relay#1 的 AMF。

S4100, UE-to-Network Relay#1 向网元#2 发送临时标识 1' 和 Relay service code。

在一种可能的实现方式中, 网元#2 获取的信息还可以包括新鲜性参数#1。

在另一种可能的实现方式中, 网元#2 获取的信息还可以包括 MAC-I#1。

本申请实施例对此不作任何限定。

10 S4110, 网元#2 根据临时标识#1' 中的路由信息确定对应的 UDM。

S4120, 网元#2 向 UDM 发送临时标识#1'。

S4130, UDM 根据临时标识#1' 确定临时标识#1, 从上述 S460 中 UDM 保存的临时标识#1 和 Remote UE#1 的网络标识对应关系获取 Remote UE#1 的网络标识, 接着根据 Remote UE#1 的网络标识从 Remote UE#1 的上下文信息中获取 AUSF#1 的标识, 并向网元
15 #2 发送 AUSF#1 的标识。

在一种可能的实现方式中, 向网元#2 发送的信息还可以包括 Remote UE#1 的网络标识。

具体地, 在该步骤中, UDM 从 Remote UE#1 的上下文信息中获取 AUSF#1 的标识包
括:

20 UDM 从 Remote UE#1 的上下文信息中查找 AUSF#1 的 Instance ID, 网元#2 据此找到 AUSF#1。

可选地, S4140, 若网元#2 是 PSF, 则 PSF 对 Remote UE#1 进行授权检查。

具体地, PSF 存储有每个 UE 对应的授权信息执行授权检查。PSF 根据 Remote UE#1 的网络标识检查 Remote UE#1 是否授权作为 Remote UE, 从而通过 UE-to-Network Relay#1
25 获取 Relay service code 对应的连接服务。若授权检查通过则继续执行下述步骤; 若授权检查不通过, PSF 向 AUSF#2 发送失败响应消息, 该响应消息包括授权失败的原因值 (例如授权检查不通过, 缺乏必要参数等)。

S4150, 网元#2 向 AUSF#1 发送密钥获取消息。

一种可能的实现方式, 密钥获取消息包括临时标识#1' (即, 第一用户设备的标识的一例) 和 Relay service code。
30

另一种可能的实现方式, 若在 S4130 中, 网元#2 获取了 UDM 发送的 Remote UE#1 的网络标识 (即, 第一用户设备的标识的一例), 则密钥获取消息包括 Remote UE#1 的网络标识和 Relay service code。

在一种可能的实现方式中, 密钥获取消息还可以包括新鲜性参数#1。

35 在另一种可能的实现方式中, 密钥获取消息还可以包括 MAC-I#1。

S4160, AUSF#1 根据密钥#2 (即, 第二密钥的一例)、Relay service code、至少一个新鲜性参数确定 Remote UE#1 和 UE-to-Network Relay#1 之间的共享密钥 (例如 Kr)。

一种可能的实现方式, AUSF#1 获取 S4150 中网元#2 发送的临时标识#1', 且 S450 中 AUSF#1 存储了临时标识#1 和密钥#1 的对应关系, 则 AUSF#1 根据临时标识#1' 确定临时

标识#1, 根据临时标识#1 和密钥的对应关系找到密钥#1。

另一种可能的实现方式, AUSF#1 获取 S4150 中网元#2 发送的 Remote UE#1 的网络标识, 且 S450 中, AUSF#1 存储了 Remote UE#1 的网络标识和密钥#1 的对应关系, 则 AUSF#1 根据 Remote UE#1 的网络标识和该对应关系找到密钥#1。

- 5 其中, 密钥#2 为鉴权流程中生成的密钥或者是基于鉴权流程中生成的中间密钥推演得到的密钥, 例如可以列举以下三种情况:

情况 1: 密钥#2 与密钥#1 相同, 且密钥#2 和密钥#1 为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

- 10 情况 2: 密钥#2 与密钥#1 不同, 且所述密钥#1 为所述鉴权流程中生成的密钥 Kausf; 所述密钥#1 为基于所述 Kausf 推演得到的密钥。

情况 3: 密钥#2 与密钥#1 不同, 且所述密钥#2 为所述鉴权流程中生成的密钥 Kausf; 所述密钥#1 为基于所述 Kausf 推演得到的密钥。

- 15 应理解, 如果 S450 中生成并使用了 Kpru#1, 则在该步骤密钥#2 是 Kpru#1; 如果 S450 中没有生成或使用 Kpru#1, 则在该步骤中密钥#2 可以是 Kausf#1, 也可以是在该步骤中生成并使用的 Kpru#1。

其中, 至少一个新鲜性参数可以列举如下实施方式:

一种可能的实现方式, 至少一个新鲜参数可以是 S4150 发送的新鲜性参数#1 (即, Remote UE 生成的新鲜性参数#1);

- 20 另一种可能的实现方式中, 至少一个新鲜参数可以是 AUSF#1 自行生成的新鲜性参数#2 (即, 第二新鲜性参数的一例);

另一种可能的实现方式中, 至少一个新鲜参数可以是 Remote UE#1 生成的新鲜性参数#1 和 AUSF#1 自行生成的新鲜性参数#2。

本申请实施例对新鲜性参数的数量不作任何限定。

- 25 应理解, 若在 S4150 中, 接收的信息中包括 MAC-I#1, 则 AUSF#1 根据 MAC-I#1、Relay service code 和临时标识#1 验证消息的完整性, 与 S480 中 Remote UE#1 生成 MAC-I#1 所示的方法一致, AUSF#1 将 Relay service code 作为输入参数, 基于密钥#1 根据特定算法生成出密钥#A, Remote UE#1 使用密钥#A 加密临时标识#1 和 Relay service code 后, 生成 MAC-I#1', 若 MAC-I#1 与 MAC-I#1' 不一致, 则表示传输过程中信息内容丢失或被攻击, 若 MAC-I#1 与 MAC-I#1' 一致, 则推演共享密钥。

- 30 在一种可能的实现方式中, 上述生成密钥#A 的输入参数还可以包括新鲜性参数#1。

S4170, AUSF#1 向网元#2 发送共享密钥, 网元#2 向 UE-to-Network Relay#1 发送共享密钥。

其中, 网元#2 向 UE-to-Network Relay#1 发送共享密钥可以有以下实现方式:

- 35 一种可能的实现方式, 网元#2 通过用户面向 UE-to-Network Relay#1 发送;

另一种可能的实现方式, 网元#2 通过信令面向 UE-to-Network Relay#1 发送。

应理解, 所述共享密钥可以经过一个或者多个其他网元转发到 UE-to-Network Relay#1。

应理解, 若 S4160 中, 至少一个新鲜参数包括新鲜性参数#2, 则在该步骤中, AUSF#1 向 UE-to-Network Relay#1 发送新鲜性参数#2。

S4180, UE-to-Network Relay#1 向 Remote UE#1 发送安全模式命令。

其中, 所述安全模式命令包括安全算法, 安全算法可以包括加密算法和/或完整性保护算法。

在一种可能的实现方式中, 所述安全模式命令还可以包括新鲜性参数#2。

5 S4190, Remote UE#1 基于密钥、Relay service code、至少一个新鲜性参数, 采用与 S4160 中 AUSF#1 生成共享密钥同样的方法在该步骤中生成共享密钥。

S4200, Remote UE#1 和 UE-to-network Relay#1 基于共享密钥, 安全算法得到通信密钥。

其中, 得到通信密钥可以包括以下实现方式:

10 一种可能的实现方式中, Remote UE#1 和 UE-to-network Relay#1 基于生成的共享密钥推演一个中间密钥或会话密钥, 进一步的, 基于中间密钥或会话密钥推演 Remote UE#1 和 UE-to-network Relay#1 间的信令面和用户面的加密密钥(例如, NR PC5 Encryption Key, NRPEK)和/或完整性保护密钥(例如 NR PC5 Integrity Key, NRPIK)。

15 另一种可能的实现方式中, Remote UE#1 和 UE-to-network Relay#1 分别基于生成的共享密钥推演 Remote UE#1 和 UE-to-network Relay#1 之间的消息或数据的加密密钥和/或完整保护密钥。

通信密钥的具体生成方式与现有技术相同或类似, 例如 TS23.303 和 TS33.536 中的密钥生成方式。

20 S4210, UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#1, 用于响应 S4180 中的安全模式命令, 该响应消息#1 表示通信安全已经建立完成。

S4220, UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#2, 用于响应 S490 中的请求消息#1, 该响应消息#2 表示直连通信已建立完成。

图 5 示出了本申请实施例 UE#1 鉴权过程中, 网络侧授权 UE#1 作为 Remote UE#1(即, 第一用户设备的一例)阶段的示意性流程图, 包括以下步骤:

25 其中, 方式 1 中的 S500a~S540a 与上述 S400a~S440a 中的方法类似, 方式 2 中的 S500b~S540b 与上述 S400b~S440b 中的方法类似, 方式 3 中的 S500c~S540c 与上述 S400c~S440c 中的方法类似, 此处不再赘述。

PSF 获取密钥#3(即, 第三密钥的一例)和临时标识#1 可以列举以下实现方式:

方式 A:

30 S550a, AUSF#1 生成临时标识#1 和密钥#3。

其中, 生成临时标识#1 的具体过程与上述 S450 相同, 为避免赘述, 此处不再详细说明。

S560a, AUSF#1 向 PSF 发送临时标识#1 和密钥#3, 同时 PSF 存储临时标识#1 及其与密钥#3 的对应关系。

35 作为实施例而非限定, 密钥#3 可以为基于鉴权流程中生成的中间密钥推演得到的密钥。

例如, 密钥#3 可以是鉴权流程中生成的密钥 Kausf#1 推演得到的密钥 Kpru#1。

应理解, 当密钥#1 是基于鉴权流程中生成的中间密钥推演得到的密钥(例如, Kpru#1)时, 密钥#1 和密钥#3 相同。

方式 B:

S550b, AUSF#1 根据上述 S450 所述的三种情况确定生成密钥#3, 同时确定由 PSF 生成临时标识#1。

5 S560b, AUSF#1 向 PSF 发送 Remote UE#1 的网络标识和发送密钥#3, 可用于指示由 PSF 生成临时标识#1。

S565b, PSF 根据 Remote UE#1 的网络标识和密钥#3 生成临时标识#1, 可列举以下实现方式:

在一种实现方式中, PSF 根据 Remote UE#1 的网络标识和密钥#3 生成临时标识#1 (即, 第一临时标识的一例)。

10 另一种实现方式中, PSF 根据临时标识#1 和 UDM 的路由信息拼接得到临时标识#1' (即, 第二临时标识的一例)。

应理解, 在本申请实施例中, PSF 存储临时标识#1 及其与密钥#3 的对应关系。

图 6 示出了本申请实施例 Remote UE#1 通过 UE-to-Network Relay 接入网络阶段的示意性流程图, 包括以下步骤:

15 S570 与上述 S470 的方法相同或类似, Remote UE#1 发现一个或多个 UE-to-Network Relay, 并从中选择一个 UE-to-Network Relay (计作 UE-to-Network Relay#1, 即第二用户设备的一例) 进行通信。

S580 与上述 S480 的方法相同或类似, Remote UE#1 生成临时标识#1'。

20 Remote UE#1 生成临时标识#1' 的方式与 S540 中 AUSF#1 生成临时标识#1' 的方式相同。

作为实施例而非限定, AUSF#1 根据临时标识#1 和 PSF 的路由信息拼接得到临时标识#1', 包括以下实现方式:

一种可能的实现方式: 临时标识#1 可以用 X 位来表示, 其中, 高 Y 位用于表示所述路由信息; 剩余的低(X-Y)位用于表示所述临时标识#1', 其中 X 和 Y 为正整数;

25 另一种可能的实现方式: 临时标识#1 可以用 X 位来表示, 其中, 低 Y 位用于表示所述路由信息; 剩余的高(X-Y)位用于表示所述临时标识#1', 其中 X 和 Y 为正整数。

其中, 特定算法与现有技术相同或类似, 例如标准中规定的基本密钥派生方法。

应理解, S560、S570 和 S580 的序号大小顺序并不代表步骤执行的先后顺序, 本申请实施例对步骤执行的先后顺序不作任何限定, 本领域技术人员可根据需求灵活设定

30 S590, 与上述 S490 的方法相同或类似, Remote UE#1 向 UE-to-Network Relay#1 发送请求消息#1 (即, 第一请求的一例), 该请求消息#1 用于请求通过 UE-to-Network Relay#1 接入网络, 例如直连通信请求 (direct communication request, DCR) 消息。请求消息#1 携带信息#2, 请求消息#1 包括临时标识#1' 和 Relay service code。

35 应理解, Relay service code 可以是 UE 侧预配置的, 还可以是网络侧发送给 UE 的, 例如例如 TS23.502 中定义的 UE Configuration Update 流程。

其中, Relay service code 用于标识支持 ProSe 服务的 UE-to-Network Relay 提供的连接服务, 以及标识支持 ProSe 服务的 UE-to-Network Relay 提供服务的授权用户, 并且可以选择相关的安全策略或信息。

在一种可能的实现方式中, 请求消息#1 还可以包括新鲜性参数#1。

在另一种可能的实现方式中，请求消息#1 还可以包括 MAC-I#2。

- 具体地，Remote UE#1 将 Relay service code 作为输入参数，基于密钥#3 根据特定算法生成出密钥#A，Remote UE#1 使用密钥#A 加密临时标识#1'和 Relay service code 后，生成完整性消息认证码（message authentication code for integrity, MAC-I）（计作 MAC-I#2），
- 5 用于验证请求消息#1 的完整性保护，防止请求消息#1 被攻击者篡改。

S5100，UE-to-Network Relay#1 向网络侧 PSF 发送临时标识#1'和 Relay service code。

在一种可能的实现方式中，PSF 从 UE-to-Network Relay#1 获取的信息还可以包括新鲜性参数#1。

- 在另一种可能的实现方式中，PSF 从 UE-to-Network Relay#1 获取的信息还可以包括
- 10 MAC-I#2。

应理解，UE-to-Network Relay#1 可以经过一个或者多个其他网元向 PSF 发送临时标识 1'和 Relay service code。

可选地，S5110，与 S4140 的方法相同或类似，PSF 对 Remote UE#1 进行授权检查。

- 具体地，PSF 存储有每个 UE 对应的授权信息执行授权检查。PSF 根据临时标识#1'检查 Remote UE#1 是否授权作为 Remote UE，从而通过 UE-to-Network Relay#1 获取 Relay service code 对应的连接服务。若授权检查通过则继续执行下述步骤；若授权检查不通过，PSF 向 AUSF#2 发送失败响应消息，该响应消息包括授权失败的原因值（例如授权检查不通过，缺乏必要参数等）。
- 15

- S5120，与上述 S4160 的方法相同或类似，PSF 根据密钥#3、Relay service code、至少一个新鲜参数确定 Remote UE#1 和 UE-to-Network Relay#1 之间的共享密钥（例如 Kr）。
- 20

具体地，PSF 根据临时标识#1'确定临时标识#1，由上述方式 A 中 S560a 存储的临时标识#1 和密钥#3 的对应关系，或者

由上述方式 B 中 S565b 存储的临时标识#1 和密钥#3 的对应关系查找密钥#3。

- 作为实施例而非限定，在该步骤中，密钥#3 可以为基于鉴权流程中生成的中间密钥推演得到的密钥。
- 25

例如，密钥#3 可以是鉴权流程中生成的密钥 Kausf#1 推演得到的密钥 Kpru#1。

其中，至少一个新鲜性参数生成方式可以列举如下：

- 一种可能的实现方式，至少一个新鲜参数可以是 S590 发送的新鲜性参数#1（即，Remote UE 生成的新鲜性参数#1）；
- 30 另一种可能的实现方式中，至少一个新鲜参数可以是 PSF 自行生成的新鲜性参数#2；
- 另一种可能的实现方式中，至少一个新鲜参数可以是 Remote UE 生成的新鲜性参数#1 和 PSF 自行生成的新鲜性参数#2。

本申请实施例对新鲜性参数的数量不作任何限定。

- 应理解，若在 S5100 中，PSF 获取的信息还可以包括 MAC-I#2，则 AUSF#1 根据
- 35 MAC-I#2、Relay service code 和临时标识#1 验证消息的完整性，验证方式与 S580 的方法相同或类似，AUSF#1 将 Relay service code 作为输入参数，基于密钥#3 根据特定算法生成出密钥#A，Remote UE#1 使用密钥#A 加密临时标识#1 和 Relay service code 后，生成 MAC-I#2'，若 MAC-I#2 与 MAC-I#2'不一致，则表示传输过程中信息内容丢失或被攻击，若 MAC-I#2 与 MAC-I#2'一致，则推演共享密钥。

在一种可能的实现方式中，上述生成密钥#A 的输入参数还可以包括新鲜性参数#1。

S5130，PSF 向 UE-to-Network Relay#1 发送共享密钥。

一种可能的实现方式，PSF 通过用户面向 UE-to-Network Relay#1 发送；

另一种可能的实现方式，PSF 通过信令面向 UE-to-Network Relay#1 发送。

5 应理解，所述共享密钥可以经过一个或者多个其他网元转发到 UE-to-Network Relay#1。

应理解，若 S5120 中，至少一个新鲜参数包括新鲜性参数#2，则在该步骤中，AUSF-2 向 UE-to-Network Relay#1 发送新鲜性参数#2。

10 S5140，与上述 S4180 的方法相同或类似，UE-to-Network Relay#1 向 Remote UE#1 发送安全模式命令。

其中，所述安全模式命令包括安全算法，安全算法可以包括加密算法和/或完整性保护算法。

在一种可能的实现方式中，所述安全模式命令还可以包括新鲜性参数#2。

15 S5150，与上述 S4190 的方法相同或类似，Remote UE#1 基于密钥#3、Relay service code、至少一个新鲜参数，采用与 S5120 同样的方法生成共享密钥。

S5160，与上述 S4200 的方法相同或类似，Remote UE#1 基于共享密钥和安全算法得到通信密钥。

其中，得到通信密钥可以包括以下实现方式：

20 一种可能的实现方式中，Remote UE#1 和 UE-to-network Relay#1 基于生成的共享密钥推演一个中间密钥或会话密钥，进一步的，基于中间密钥或会话密钥推演 Remote UE#1 和 UE-to-network Relay#1 间的信令面和用户面的加密密钥（例如，NR PC5 Encryption Key，NRPEK）和/或完整性保护密钥（例如 NR PC5 Integrity Key，NRPIK）。

25 另一种可能的实现方式中，Remote UE#1 和 UE-to-network Relay#1 分别基于生成的共享密钥推演 Remote UE#1 和 UE-to-network Relay#1 之间的消息或数据的加密密钥和/或完整保护密钥。

通信密钥的具体生成方式与现有技术相同或类似，例如 TS23.303 和 TS33.536 中的密钥生成方式。。

30 S5170，与上述 S4210 的方法相同或类似，UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#1，用于响应 S5160 中的安全模式命令，该响应消息#1 表示通信安全已经建立完成。

S5180，与上述 S4220 的方法相同或类似，UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#2，用于响应 S590 中的请求消息#1，该响应消息#2 表示直连通信已建立完成。

图 7 示出了本申请实施例 UE#1 认证授权作为 Remote UE#1（即，第二用户设备的一例）阶段的示意性流程图，包括以下步骤：

35 其中，方式 1 中的 S600a~S640a 与上述 S500a~S540a 中的方法类似，方式 2 中的 S600b~S640b 与上述 S500b~S540b 中的方法类似，方式 3 中的 S600c~S640c 与上述 S500c~S540c 中的方法类似，方式 A 中的 S650a~S660a 与上述 S550a~S560a 中的方法类似，方式 B 中的 S650b~S665b 与上述 S550b~S565b 中的方法类似，S670~S690 与上述 S570~S590 中的方法类似，此处不再赘述。

应理解,下述步骤中,PSF#1(即,第五网元的一例)可以是 Remote PSF,PSF#2(即,第六网元的一例)可以是服务 UE-to-Network Relay#1 的 PSF。

S6100,UE-to-Network Relay #1 向 PSF#2 发送临时标识#1'和 Relay Service Code。

5 应理解,UE-to-Network Relay#1 可以经过一个或者多个其他网元向 PSF 发送临时标识 1'和 Relay service code。

在一种可能的实现方式中,PSF#2 从 UE-to-Network Relay #1 获取的信息还可以包括新鲜性参数#1。

在另一种可能的实现方式中,PSF#2 从 UE-to-Network Relay #1 获取的信息还可以包括 MAC-I#1。

10 S6110,PSF#2 根据临时标识#1'(即,第一临时标识的一例)中的路由信息确定对应的 PSF#1。

S6120,PSF#1 获取临时标识#1'和 Relay service code。

在一种可能的实现方式中,PSF#1 获取的信息还可以包括新鲜性参数#1。

在一种可能的实现方式中,PSF#1 获取的信息还可以包括 MAC-I#1。

15 可选地,S6130,与上述 S5110 的方法相同或类似,PSF#1 对 Remote UE#1 进行授权检查。

PSF#1 根据临时标识#1'检查 Remote UE#1 是否授权作为 Remote UE,从而通过 UE-to-Network Relay#1 获取 Relay service code 对应的连接服务。若授权检查通过则继续执行下述步骤;若授权检查不通过,PSF#1 向 AUSF#2 发送失败响应消息,该响应消息包括
20 授权失败的原因值(例如授权检查不通过,缺乏必要参数等)。

S6140,与上述 S5120 的方法类似,PSF#1 根据密钥#3、Relay service code、至少一个新鲜参数确定 Remote UE#1 和 UE-to-Network Relay#1 之间通信的共享密钥(例如 Kr)。为避免赘述,此处不再详细说明。

25 应理解,若在 S6100 中,PSF#1 获取的信息还包括 MAC-I#1,则 AUSF#1 根据 MAC-I#1、Relay service code 和临时标识#1(即,第一临时标识的一例)验证消息的完整性,验证方式与 S5120 的方法相同或类似,此处不再赘述。

S6150,PSF#1 向 PSF#2 发送共享密钥。

一种可能的实现方式,PSF#1 通过用户面向 UE-to-Network Relay#1 发送;

另一种可能的实现方式,PSF#1 通过信令面向 UE-to-Network Relay#1 发送。

30 应理解,所述共享密钥可以经过一个或者多个其他网元转发到 UE-to-Network Relay#1。

应理解,若在 S6140 中,至少一个新鲜参数包括新鲜性参数#2,则在该步骤中,PSF#1 向 PSF#2 发送新鲜性参数#2。

35 S6160,与上述 S5130 的方法相同或类似,PSF#2 向 UE-to-Network Relay#1 发送共享密钥。

应理解,若在 S6150 中,PSF#2 接收到新鲜性参数#2,则 PSF#2 向 UE-to-Network Relay#1 发送新鲜性参数#2。

S6170,与上述 S5140 的方法相同或类似,UE-to-Network Relay#1 向 Remote UE#1 发送安全模式命令。

其中，所述安全模式命令包括安全算法，安全算法可以包括加密算法和/或完整性保护算法。

在一种可能的实现方式中，所述安全模式命令还可以包括新鲜性参数#2。

5 S6180,与上述 S5150 的方法相同或类似,Remote UE#1 基于密钥#3、Relay service code、至少一个新鲜参数，采用与 S6150 同样的方法生成共享密钥。

S6190,与上述 S5160 的方法相同或类似， Remote UE#1 基于共享密钥和安全算法得到通信密钥。

其中，得到通信密钥可以包括以下实现方式：

10 一种可能的实现方式中，Remote UE#1 和 UE-to-network Relay#1 基于生成的共享密钥推演一个中间密钥或会话密钥，进一步的，基于中间密钥或会话密钥推演 Remote UE#1 和 UE-to-network Relay#1 间的信令面和用户面的加密密钥（例如，NR PC5 Encryption Key，NRPEK）和/或完整性保护密钥（例如 NR PC5 Integrity Key，NRPIK）。

15 另一种可能的实现方式中，Remote UE#1 和 UE-to-network Relay#1 分别基于生成的共享密钥推演 Remote UE#1 和 UE-to-network Relay#1 之间的消息或数据的加密密钥和/或完整保护密钥。

通信密钥的具体生成方式与现有技术相同或类似，例如 TS23.303 和 TS33.536 中的密钥生成方式。

20 S6200,与上述 S5170 的方法相同或类似，UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#1，用于响应 S6190 中的安全模式命令，该响应消息#1 表示通信安全已经建立完成。

S6210,与上述 S5180 的方法相同或类似，UE-to-Network Relay#1 向 Remote UE#1 发送响应消息#2，用于响应 S690 中的请求消息#1（即，第一请求的一例），该响应消息#2 表示直接通信已建立完成。

25 应理解，上述实施例中，第一用户设备的标识（即，包括 Remote UE 的网络标识和第一用户设备的网络标识）用于识别所述第一用户设备的信息，本申请实施例对第一用户设备的标识不做任何限定，本领域技术人员为了达到识别所述第一用户设备的目的，可根据具体情况灵活限定。

应理解，上述实施例中，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，而不对本申请实施例的实施过程构成任何限定。

30 现有技术中，Remote UE 通过 UE-to-Network Relay 与网络建立会话的过程如下所述：

Remote UE 和 UE-to-Network Relay 分别接入网络，并从网络获取授权和配置信息。其中，授权和配置信息用于建立 ProSe 通信连接。Remote UE 发现一个或多个 UE-to-Network Relay，并从中选择一个 UE-to-Network Relay，接受其提供的连接服务信息。Remote UE 与所选择的 UE-to-Network Relay 建立一对一直接通信的连接。UE-to-Network Relay 向会话管理网元上报中继相关的协议数据单元（protocol data unit，PDU）会话的远端用户设备报告（Remote UE Report），例如（远端用户标识远（Remote User ID），远端用户信息（Remote UE info））。

在该 Remote UE 通过 UE-to-Network Relay 获取业务的过程中，为了保证通信安全，Remote UE 和 UE-to-Network Relay 之间需要建立安全连接。然而，由于 Remote UE 通过

UE-to-Network Relay 建立通信连接是按需动态建立的, 例如, Remote UE 在发现过程中, 发现的 UE-to-Network Relay 不是固定的。比如第一发现的, 可能是 UE-to-Network Relay#1, 第二发现的可能是 UE-to-Network Relay#1。Remote UE 在不同时候不同地点, 发现的 UE-to-Network Relay 可能都不一样, 且不可预知。因此无法在 Remote UE 和 UE-to-Network Relay 之间预配置共享的安全参数 (例如, 共享密钥) 用于 Remote UE 和 UE-to-Network Relay 之间安全通信。

基于本申请实施例提供的上述技术方案, 本申请实施例生成了设备间通信的密钥, 使得用户设备与用户设备之间动态地建立了安全的通信连接, 与上述现有技术中具有本质区别, 解决了上述现有技术存在的问题。

以上, 结合图 3 至图 8 详细说明了本申请实施例提供的方法。下面结合图 9 至图 10 介绍本申请实施例提供的通信装置。应理解, 装置实施例的描述与方法实施例的描述相互对应, 因此, 未详细描述的内容可以参见上文方法实施例, 为了简洁, 这里不再赘述。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。可以理解的是, 各个网元, 为了实现上述功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该可以意识到, 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, 本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行, 取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能, 但是这种实现不应认为超出本申请的范围。

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

图 9 是本申请实施例提供的通信装置 100 的示意性框图。如图所示, 该通信装置 100 可以包括: 收发单元 110 和处理单元 120。

在一种可能的设计中, 该通信装置 100 可以是上文方法实施例中的远端用户设备, 也可以是用于实现上文方法实施例中远端用户设备的功能的芯片。

应理解, 该通信装置 100 可对应于根据本申请实施例的方法 400、方法 500、方法 600、方法 700、方法 800 和方法 900 中的远端用户设备, 该通信装置 100 可以包括用于执行图 3 中的方法 400、图 4 中的方法 500、图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 中的远端用户设备执行的方法的单元。并且, 该通信装置 100 中的各单元和上述其他操作和/或功能分别为了实现图 3 中的方法 400、图 4 中的方法 500、图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 的相应流程。应理解, 各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明, 为了简洁, 在此不再赘述。

在另一种可能的设计中, 该通信装置 100 可以是上文方法实施例中的鉴权功能网元,

也可以是用于实现上文方法实施例中鉴权功能网元的芯片。

应理解，该通信装置 100 可对应于根据本申请实施例方法 400、方法 500 中的鉴权功能网元，该通信装置 100 可以包括用于执行图 3 中的方法 400、图 4 中的方法 500 中的鉴权功能网元执行的方法的单元。并且，该通信装置 100 中的各单元和上述其他操作和/或功能分别为了实现图 3 中的方法 400、图 4 中的方法 500 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在另一种可能的设计中，该通信装置 100 可以是上文方法实施例中的近距离业务安全功能网元，也可以是用于实现上文方法实施例中近距离业务安全功能网元的功能的芯片。

应理解，该通信装置 100 可对应于根据本申请实施例方法 600、方法 700、方法 800 和方法 900 中的近距离业务安全功能网元，该通信装置 100 可以包括用于执行图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 中的近距离业务安全功能网元执行的方法的单元。并且，该通信装置 100 中的各单元和上述其他操作和/或功能分别为了实现图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

还应理解，该通信装置 100 中的收发单元可对应于图 10 中示出的通信设备 200 中的收发器 210，该通信装置 100 中的处理单元 120 可对应于图 10 中示出的通信设备 200 中的收发器 220。

还应理解，当该通信装置 100 为芯片时，该芯片包括收发单元和处理单元。其中，收发单元可以是输入输出电路或通信接口；处理单元可以为该芯片上集成的处理器或者微处理器或者集成电路。

收发单元 110 用于实现通信装置 100 的信号的收发操作，处理单元 120 用于实现通信装置 100 的信号的处理操作。

可选地，该通信装置 100 还包括存储单元 130，该存储单元 130 用于存储指令。

图 10 是本申请实施例提供的通信设备 200 的示意性框图。如图所示，该通信设备 200 包括：至少一个处理器 210 和收发器 220。该处理器 210 与存储器耦合，用于执行存储器中存储的指令，以控制收发器 220 发送信号和/或接收信号。可选地，该通信设备 200 还包括存储器 230，用于存储指令。

应理解，上述处理器 210 和存储器 230 可以合成一个处理装置，处理器 210 用于执行存储器 230 中存储的程序代码来实现上述功能。具体实现时，该存储器 230 也可以集成在处理器 210 中，或者独立于处理器 210。

还应理解，收发器 220 可以包括接收器（或者称，接收机）和发射器（或者称，发射机）。收发器还可以进一步包括天线，天线的数量可以为一个或多个。收发器 220 有可以是通信接口或者接口电路。

在一种可能的设计中，该通信设备 200 可以是上文方法实施例中的远端用户设备，也可以是用于实现上文方法实施例中远端用户设备的功能的芯片。

具体地，该通信设备 200 可对应于根据本申请实施例的方法 400、方法 500、方法 600、方法 700、方法 800 和方法 900 中的远端用户设备，该通信设备 200 可以包括用于执行图 3 中的方法 400、图 4 中的方法 500、图 5 中的方法 600、图 6 中的方法 700、图 7 中的方

法 800 和图 8 中的方法 900 中的远端用户设备执行的方法的单元。并且，该通信设备 200 中的各单元和上述其他操作和/或功能分别为了实现图 3 中的方法 400、图 4 中的方法 500、图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在一种可能的设计中，该通信设备 200 可以是上文方法实施例中的近距离业务安全功能网元，也可以是用于实现上文方法实施例中近距离业务安全功能网元的功能的芯片。

具体地，该通信设备 200 可对应于根据本申请实施例的方法 400、方法 500 中的近距离业务安全功能网元，该通信设备 200 可以包括用于执行图 3 中的方法 400、图 4 中的方法 500 中的近距离业务安全功能网元执行的方法的单元。并且，该通信设备 200 中的各单元和上述其他操作和/或功能分别为了实现图 3 中的方法 400、图 4 中的方法 500 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在一种可能的设计中，该通信设备 200 可以是上文方法实施例中的鉴权功能网元，也可以是用于实现上文方法实施例中鉴权功能网元的功能的芯片。

具体地，该通信设备 200 可对应于根据本申请实施例的方法 600、方法 700、方法 800 和方法 900 中的鉴权功能网元，该通信设备 200 可以包括用于执行图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 中的鉴权功能网元执行的方法的单元。并且，该通信设备 200 中的各单元和上述其他操作和/或功能分别为了实现图 5 中的方法 600、图 6 中的方法 700、图 7 中的方法 800 和图 8 中的方法 900 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

当该通信设备 200 为芯片时，该芯片包括收发单元和处理单元。其中，收发单元可以是输入输出电路或通信接口；处理单元可以为该芯片上集成的处理器或者微处理器或者集成电路。本申请实施例还提供了一种处理装置，包括处理器和接口。所述处理器可用于执行上述方法实施例中的方法应理解，上述处理装置可以是一个芯片。例如，该处理装置可以是现场可编程门阵列（field programmable gate array, FPGA），可以是专用集成芯片（application specific integrated circuit, ASIC），还可以是系统芯片（system on chip, SoC），还可以是中央处理器（central processor unit, CPU），还可以是网络处理器（network processor, NP），还可以是数字信号处理电路（digital signal processor, DSP），还可以是微控制器（micro controller unit, MCU），还可以是可编程控制器（programmable logic device, PLD）或其他集成芯片。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。

在实现过程中,上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

可以理解,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(dynamic RAM, 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(synch-link DRAM, SLD RAM)和直接内存总线随机存取存储器(direct ram-bus RAM, DR RAM)。应注意,本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

根据本申请实施例提供的方法,本申请还提供一种计算机程序产品,该计算机程序产品包括:计算机程序代码,当该计算机程序代码在计算机上运行时,使得该计算机执行图3或图4或图5所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法,本申请还提供一种计算机可读介质,该计算机可读介质存储有程序代码,当该程序代码在计算机上运行时,使得该计算机执行图3或图4或图5所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法,本申请还提供一种系统,其包括前述的装置或设备。在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(digital subscriber line, DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机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成的服务器、数据中心等

数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，高密度数字视频光盘（digital video disc, DVD））、或者半导体介质（例如，固态硬盘（solid state disc, SSD））等。

5 上述各个装置实施例中网络侧设备与终端设备和方法实施例中的网络侧设备或终端设备对应，由相应的模块或单元执行相应的步骤，例如通信单元（收发器）执行方法实施例中接收或发送的步骤，除发送、接收外的其它步骤可以由处理单元（处理器）执行。具体单元的功能可以参考相应的方法实施例。其中，处理器可以为一个或多个。

10 在本说明书中使用的术语“部件”、“模块”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如，部件可以是但不限于，在处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示，在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中，部件可位于一个计算机上和/或分布在 2 个或更多个计算机之间。此外，这些部件可从在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组（例如来自与本地系统、分布式系统和/或网络间的另一部件交互的二个部件的数据，例如通过信号与其它系统交互的互联网）的信号通过本地和/或远程进程来通信。

20 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。

所述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。

25 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。

30 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。

35 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，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。

- 5 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、一种生成设备间通信的密钥的方法，其特征在于，包括：
第一用户设备基于第一密钥，生成第一临时标识；
- 5 所述第一用户设备向第二用户设备发送第一请求，所述第一请求用于建立所述第一用户设备和所述第二用户设备之间的通信连接；其中，所述第一请求包括所述第一临时标识和中继服务码；
- 所述第一用户设备基于第二密钥和所述中继服务码，生成共享密钥；其中，所述共享密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接，所述第二密钥与所述第一密钥为鉴权流程中生成的密钥或者是基于鉴权流程中生成的中间密钥推演得到的密钥。
- 10 2、根据权利要求1所述的方法，其特征在于，所述第二密钥与所述第一密钥相同，且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。
- 15 3、根据权利要求1所述的方法，其特征在于，所述第二密钥与所述第一密钥不同，且所述第一密钥为所述鉴权流程中生成的密钥 Kausf；所述第二密钥为基于所述 Kausf 推演得到的密钥。
- 4、根据权利要求1所述的方法，其特征在于，所述第二密钥与所述第一密钥不同，且所述第二密钥为所述鉴权流程中生成的密钥 Kausf；所述第一密钥为基于所述 Kausf 推演得到的密钥。
- 20 5、根据权利要求1-4中任一所述的方法，其特征在于，所述第一用户设备基于第一密钥，生成第一临时标识，包括：
所述第一用户设备基于所述第一密钥、所述第一用户设备的网络标识和路由信息，生成所述第一临时标识；其中，所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息，所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。
- 25 6、根据权利要求5所述的方法，其特征在于，所述第一用户设备基于所述第一密钥、所述第一用户设备的网络标识和路由信息，生成所述第一临时标识，包括：
所述第一用户设备基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数，得到第二临时标识；
- 30 将所述第二临时标识和所述路由信息进行拼接，得到所述第一临时标识。
- 7、根据权利要求5或6所述的方法，其特征在于，所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI；所述路由信息为路由指示。
- 8、根据权利要求1-7中任一所述的方法，其特征在于，所述方法还包括：
- 35 所述第一用户设备向移动管理网元发送非接入层 NAS 消息，所述 NAS 消息包括能力信息，所述能力信息用于指示所述第一用户设备支持作为远端用户设备。
- 9、根据权利要求1-8中任一所述的方法，其特征在于，所述第一请求还包括第一新鲜性参数；

所述第一用户设备基于所述第二密钥和所述中继服务码，生成所述共享密钥，包括：
所述第一用户设备基于所述第二密钥、所述中继服务码和所述第一新鲜性参数，生成所述共享密钥。

10、根据权利要求 1-8 中任一所述的方法，其特征在于，所述方法还包括：

- 5 所述第一用户设备接收来自所述第二用户设备的安全模式命令，所述安全模式命令包括第二新鲜性参数；

所述第一用户设备基于所述第二密钥和所述中继服务码，生成所述共享密钥，包括：
所述第一用户设备基于所述第二密钥、所述中继服务码和所述第二新鲜性参数，生成所述共享密钥。

- 10 11、根据权利要求 1-8 中任一所述的方法，其特征在于，所述第一请求还包括第一新鲜性参数；

所述方法还包括：

所述第一用户设备接收来自所述第二用户设备的安全模式命令，所述安全模式命令包括第二新鲜性参数；

- 15 所述第一用户设备基于所述第二密钥和所述中继服务码，生成所述共享密钥，包括：
所述第一用户设备基于所述第二密钥、所述中继服务码、所述第一新鲜性参数和所述第二新鲜性参数，生成所述共享密钥。

12、根据权利要求 11 所述的方法，其特征在于，所述安全模式命令还包括安全算法；

所述方法还包括：

- 20 所述第一用户设备基于所述共享密钥和所述安全算法，得到通信密钥；所述通信密钥用于保护所述第一用户设备和所述第二用户设备之间的通信连接。

13、一种生成设备间通信的密钥的方法，其特征在于，包括：

第一网元基于第一密钥，生成第一临时标识；

- 25 所述第一网元接收来自第二网元的密钥获取消息，所述密钥获取消息包括第一用户设备的标识和中继服务码，其中，所述第一用户设备的标识包括所述第一临时标识或者所述第一用户设备的网络标识，所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息；

所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥；其中，所述共享密钥用于保护所述第一用户设备和第二用户设备之间的通信连接，
30 所述第二密钥与所述第一密钥为所述第一用户设备的鉴权流程中生成的密钥或者是基于所述第一用户设备的鉴权流程中生成的中间密钥推演得到的密钥；

所述第一网元向所述第二网元发送所述共享密钥。

14、根据权利要求 13 所述的方法，其特征在于，所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：

- 35 所述第一网元根据所述第一用户设备的标识获取所述第二密钥，所述第一网元根据所述第二密钥和所述中继服务码，生成所述共享密钥。

15、根据权利要求 13 或 14 所述的方法，其特征在于，所述第二密钥与所述第一密钥相同，且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

16、根据权利要求 13 或 14 所述的方法，其特征在于，所述第二密钥与所述第一密钥不同，且所述第一密钥为所述鉴权流程中生成的密钥 Kausf；所述第二密钥为基于所述 Kausf 推演得到的密钥。

5 17、根据权利要求 13 或 14 所述的方法，其特征在于，所述第二密钥与所述第一密钥不同，且所述第二密钥为所述鉴权流程中生成的密钥 Kausf；所述第一密钥为基于所述 Kausf 推演得到的密钥。

18、根据权利要求 13-17 中任一项所述的方法，其特征在于，所述第一网元基于第一密钥，生成第一临时标识，包括：

10 所述第一网元基于所述第一密钥、所述第一用户设备的网络标识和路由信息，生成所述第一临时标识；其中，所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息，所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

19、根据权利要求 18 所述的方法，其特征在于，所述第一网元基于第一密钥、所述第一用户设备的网络标识和路由信息，生成第一临时标识，包括：

15 所述第一网元基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数，得到第二临时标识；

将所述第二临时标识和所述路由信息进行拼接，得到所述第一临时标识。

20、根据权利要求 13-19 中任一项所述的方法，其特征在于，

所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI；所述路由信息为路由指示。

20 21、根据权利要求 13-20 中任一所述的方法，其特征在于，所述方法还包括：

在对所述第一用户设备进行鉴权流程中，所述第一网元接收来自第三网元的指示信息；

响应于所述指示信息，所述第一网元基于所述第一密钥，生成所述第一临时标识。

22、根据权利要求 21 所述的方法，其特征在于，

25 在对所述第一用户设备进行鉴权流程中，所述第一网元接收来自第三网元的指示信息；

响应于所述指示信息，所述第一网元基于所述第一密钥，生成所述第一临时标识，包括：

30 在对所述第一用户设备进行鉴权流程中，所述第一网元接收来自第四网元的能力信息，所述能力信息用于指示所述第一用户设备支持远端 UE 的能力；

响应于所述指示信息和所述能力信息，所述第一网元基于所述第一密钥，生成所述第一临时标识。

23、根据权利要求 13-22 中任一所述的方法，其特征在于，所述方法还包括：

所述第一网元将所述第一临时标识发送给第三网元。

35 24、根据权利要求 13-23 中任一项所述的方法，其特征在于，所述密钥获取消息还包括第一新鲜性参数；

所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述第一网元根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数，生成共享密钥。

- 25、根据权利要求 13-23 中任一项所述的方法，其特征在于，所述方法还包括：
所述第一网元生成第二新鲜性参数；
所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述所述第一网元根据所述第一用户设备的标识、所述中继服务码、第二
5 密钥和所述第二新鲜性参数，生成共享密钥。
- 26、根据权利要求 13-23 中任一项所述的方法，其特征在于，所述密钥获取消息还包括第一新鲜性参数；
所述方法还包括：
所述第一网元生成第二新鲜性参数；
10 所述第一网元根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述所述第一网元根据所述第一用户设备的标识、所述中继服务码、所述第二密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥。
- 27、根据权利要求 13-26 中任一项所述的方法，其特征在于，
所述第一网元为鉴权功能网元。
- 15 28、根据权利要求 13-27 中任一项所述的方法，其特征在于，
所述第二网元为移动管理网元、鉴权功能网元或近距离业务安全功能网元。
- 29、根据权利要求 13-28 中任一项所述的方法，其特征在于，
所述第三网元为数据管理网元。
- 30、根据权利要求 13-29 中任一项所述的方法，其特征在于，
20 所述第四网元为移动管理网元。
- 31、一种生成设备间通信的密钥的方法，其特征在于，包括：
第五网元获取第一临时标识和第三密钥，所述第三密钥为基于鉴权流程中生成的中间
密钥推演得到的密钥；
所述第五网元接收来自第六网元的密钥获取消息，所述密钥获取消息包括所述第一临时
25 标识和中继服务码；
所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥；
其中，所述共享密钥用于保护所述第一用户设备和第二用户设备之间的通信连接；
所述第五网元向所述第六网元发送所述共享密钥。
- 32、根据权利要求 31 所述的方法，其特征在于，所述第五网元根据所述第一临时标
30 识、所述中继服务码以及第三密钥，生成共享密钥，包括：
所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥；
包含：
所述第五网元根据所述第一临时标识获取所述第三密钥，所述第五网元根据所述第三
密钥和中继服务码生成共享密钥。
- 35 33、根据权利要求 31 所述的方法，其特征在于，第五网元获取第一临时标识，包括：
第五网元从所述第一网元接收到所述第一临时标识，所述第一临时标识是基于第一中
间密钥生成的，所述第一中间密钥为对所述第一用户设备进行鉴权流程中生成的中间密钥
或者是基于鉴权流程中生成的中间密钥推演得到的密钥；
或者，第五网元基于第三中间密钥生成所述第一临时标识。

34、根据权利要求 31-33 中任一项所述的方法，其特征在于，所述第三密钥为基于所述鉴权流程中生成的密钥 Kausf 推演得到的密钥。

35、根据权利要求 33 所述的方法，其特征在于，所述第一临时标识是基于所述第一密钥生成的，包括：

- 5 所述第一临时标识是基于所述第一密钥、所述第一用户设备的网络标识和路由信息生成的；其中，所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息，所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

36、根据权利要求 35 所述的方法，其特征在于，所述第一临时标识是基于所述第一密钥、所述第一用户设备的网络标识和路由信息生成的，包括：

- 10 所述第二临时标识是基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数得到的；

 所述第一临时标识是将所述第二临时标识和所述路由信息进行拼接得到的。

37、根据权利要求 31-36 中任一项所述的方法，其特征在于，

- 15 所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI；所述路由信息为路由指示。

38、根据权利要求 31-37 中任一项所述的方法，其特征在于，所述密钥获取消息还包括第一新鲜性参数；

- 20 所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥和所述第一新鲜性参数，生成共享密钥。

39、根据权利要求 31-37 中任一项所述的方法，其特征在于，所述方法还包括：

 所述第五网元生成第二新鲜性参数；

- 25 所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述所述所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥和所述第二新鲜性参数，生成共享密钥。

40、根据权利要求 31-37 中任一项所述的方法，其特征在于，所述密钥获取消息还包括第一新鲜性参数；

 所述方法还包括：

- 30 所述第五网元根据所述第一临时标识、所述中继服务码以及第三密钥，生成共享密钥，包括：所述所述所述第五网元根据所述第一临时标识、所述中继服务码、第三密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥。

41、根据权利要求 31-40 中任一项所述的方法，其特征在于，

 所述第五网元为第一近距离业务安全功能网元。

42、根据权利要求 31-41 中任一项所述的方法，其特征在于，

- 35 所述第六网元为第二近距离业务安全功能网元。

43、一种生成设备间通信的密钥的系统，其特征在于，包括：

 第一网元，用于基于第一密钥生成第一临时标识；

 第二网元，用于向第一网元发送密钥获取消息，所述密钥获取消息包括第一用户设备的标识和中继服务码，其中，所述第一用户设备的标识包括所述第一临时标识或者所述第

一用户设备的网络标识,所述第一用户设备的网络标识用于网络侧识别第一用户设备的信息;

所述第一网元还用于根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥;其中,所述共享密钥用于保护所述第一用户设备和第二用户设备之间的通信连接,所述第二密钥与所述第一密钥为所述第一用户设备的鉴权流程中生成的密钥或者是基于所述第一用户设备的鉴权流程中生成的中间密钥推演得到的密钥;

所述第一网元向所述第二网元发送所述共享密钥。

44、根据权利要求 43 所述的系统,其特征在于,所述第一网元还用于根据所述第一用户设备的标识、所述中继服务码以及第二密钥,生成共享密钥,包括:

所述第一网元还用于根据所述第一用户设备的标识获取所述第二密钥,所述第一网元还用于根据所述第二密钥和所述中继服务码,生成所述共享密钥。

45、根据权利要求 43 或 44 所述的系统,其特征在于,所述第二密钥与所述第一密钥相同,且所述第二密钥和所述第一密钥为所述鉴权流程中生成的密钥 Kausf 或者基于所述 Kausf 推演得到的密钥。

46、根据权利要求 43 或 44 所述的系统,其特征在于,所述第二密钥与所述第一密钥不同,且所述第一密钥为所述鉴权流程中生成的密钥 Kausf;所述第二密钥为基于所述 Kausf 推演得到的密钥。

47、根据权利要求 43 或 44 所述的系统,其特征在于,所述第二密钥与所述第一密钥不同,且所述第二密钥为所述鉴权流程中生成的密钥 Kausf;所述第一密钥为基于所述 Kausf 推演得到的密钥。

48、根据权利要求 43-47 中任一项所述的系统,其特征在于,所述第一网元,用于基于第一密钥,生成第一临时标识,包括:

所述第一网元还用于,基于所述第一密钥、所述第一用户设备的网络标识和路由信息,生成所述第一临时标识;其中,所述第一用户设备的网络标识用于网络侧识别所述第一用户设备的信息,所述路由信息为用于确定与所述第一用户设备相关的核心网网元的信息。

49、根据权利要求 48 所述的系统,其特征在于,所述第一网元还用于,基于所述第一密钥、所述第一用户设备的网络标识和路由信息,生成所述第一临时标识,包括:

所述第一网元还用于,基于所述第一密钥和所述第一用户设备的网络标识作为第一预设算法的输入参数,得到第二临时标识;

将所述第二临时标识和所述路由信息进行拼接,得到所述第一临时标识。

50、根据权利要求 43-49 中任一项所述的系统,其特征在于,

所述第一用户设备的网络标识为用户永久标识 SUPI 或者国际移动用户识别码 IMSI 或者通用公共订阅标识符 GPSI;所述路由信息为路由指示。

51、根据权利要求 43-50 中任一项所述的系统,其特征在于,所述系统还包括:

第三网元,在对所述第一用户设备进行鉴权流程中,所述第三网元用于向所述第一网元发送第一指示信息;

响应于所述第一指示信息,所述第一网元用于,基于所述第一密钥,生成所述第一临时标识。

52、根据权利要求 51 中任一项所述的系统，其特征在于，所述系统还包括：

第四网元，在对所述第一用户设备进行鉴权流程中，所述第四网元用于向所述第一网元发送能力信息，所述能力信息用于指示所述第一用户设备支持远端 UE 的能力；

5 响应于所述第一指示信息和所述能力信息，所述第一网元用于，基于所述第一密钥，生成所述第一临时标识。

53、根据权利要求 43-52 中任一项所述的系统，其特征在于，
所述第一网元还用于将所述第一临时标识发送给所述第三网元。

54、根据权利要求 43-53 中任一项所述的系统，其特征在于，
所述第二网元还用于，向所述第三网元发送所述第一临时标识；
10 所述第三网元还用于，向所述第二网元发送所述第一网元的标识。

55、根据权利要求 43-54 中任一项所述的系统，其特征在于，

所述第三网元还用于，向所述第二网元发送所述第一网元的标识和第一用户设备的网络标识。

56、根据权利要求 43-55 中任一项所述的系统，其特征在于，所述密钥获取消息还包括第一新鲜性参数；

所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第一新鲜性参数，生成共享密钥。

57、根据权利要求 43-55 中任一项所述的系统，其特征在于，
20 所述第一网元还用于，生成第二新鲜性参数；

所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码、第二密钥和所述第二新鲜性参数，生成共享密钥。

58、根据权利要求 43-55 中任一项所述的系统，其特征在于，所述密钥获取消息还包括第一新鲜性参数；

所述第一网元还用于，生成第二新鲜性参数；

所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码以及第二密钥，生成共享密钥，包括：所述所述第一网元用于，根据所述第一用户设备的标识、所述中继服务码、第二密钥、所述第一新鲜性参数和所述第二新鲜性参数，生成共享密钥。

59、根据权利要求 43-58 中任一项所述的系统，其特征在于，所述系统还包括：
第一用户设备和第二用户设备。

60、根据权利要求 43-59 中任一项所述的系统，其特征在于，
所述第一网元为鉴权功能网元。

61、根据权利要求 43-60 中任一项所述的系统，其特征在于，
35 所述第二网元为移动管理网元、鉴权功能网元或近距离业务安全功能网元。

62、根据权利要求 43-61 中任一项所述的系统，其特征在于，
所述第三网元为数据管理网元。

63、根据权利要求 43-62 中任一项所述的系统，其特征在于，
所述第四网元为移动管理网元。

- 64、一种生成设备间通信的密钥的装置，其特征在于，包括：
存储器，用于存储计算机指令；
处理器，用于执行所述存储器中存储的计算机指令，使得所述通信装置执行如权利要求 1 至 12 中任一项所述的方法。
- 65、一种生成设备间通信的密钥的装置，其特征在于，包括：
存储器，用于存储计算机指令；
处理器，用于执行所述存储器中存储的计算机指令，使得所述装置执行如权利要求 13 至 30 中任一项所述的方法。
- 66、一种生成设备间通信的密钥的装置，其特征在于，包括：
存储器，用于存储计算机指令；
处理器，用于执行所述存储器中存储的计算机指令，使得所述通信装置执行如权利要求 31 至 42 中任一项所述的方法。
- 67、一种计算机可读存储介质，其特征在于，其上存储有计算机程序，所述计算机程序被通信装置执行时，使得所述通信装置执行如权利要求 1 至 12 中任一项所述的方法。
- 68、一种计算机可读存储介质，其特征在于，其上存储有计算机程序，所述计算机程序被通信装置执行时，使得所述通信装置执行如权利要求 13 至 30 中任一项所述的方法。
- 69、一种计算机可读存储介质，其特征在于，其上存储有计算机程序，所述计算机程序被通信装置执行时，使得所述通信装置执行如权利要求 31 至 42 中任一项所述的方法。