

通信方法、装置以及系统

5 本申请要求于2022年03月28日提交中国专利局、申请号为202210312676.9、申请名称为“通信方法、装置以及系统”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

10 本申请涉及通信领域，尤其涉及一种通信方法、装置以及系统。

背景技术

 随着用户交互体验的不断改进，出现了一种登录方式，即免密登录。免密登录是指不需要用户手工输入账号和密码就能够完成的登录。免密登录可以用于很多的场景，如用于
15 企业应用程序（application，APP）的注册、登录以及支付等业务场景。免密登录方式更好地满足了用户对交互体验的追求，该方式不仅可以加快登录速度，提高登录的效率，还可以避免用户忘记密码、输错密码等带来的麻烦。如何借助电信运营商的网络资源实现免密登录，是值得考虑的问题。

20 发明内容

 本申请实施例提供一种通信方法、装置以及系统，能够借助电信运营商的网络资源实现免密登录。

 第一方面，提供了一种通信方法，该方法可以由用户设备执行，或者，也可以由用户设备的组成部件（例如芯片或者电路）执行，对此不作限定。

25 该方法可以包括：用户设备向核心网设备发送第一免流量消息，第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息；用户设备从核心网设备接收第二免流量消息，第二免流量消息包括登录信息，登录信息为用户设备登录到应用服务器所需要的信息；用户设备向应用服务器发送登录信息，以登录到应用服务器；其中，第一免流量消息
30 和第二免流量消息均为通过基站传输且不产生待计费流量的消息。

 其中，待计费流量，是指电信网络中的数据网关（如用户面功能（user plane function，UPF）网元）检测到的应计费的数据流量。

 作为示例，第一免流量消息可以包括指示信息，该指示信息指示核心网设备向用户设备提供登录信息；或者，第一免流量消息也可以隐式指示（或者本身具有触发功能）核心网设备向用户设备提供登录信息，即核心网设备收到该第一免流量消息，可获知向用户设备
35 提供登录信息。

 基于上述技术方案，用户设备向核心网设备发送第一免流量消息，该第一免流量消息可用于触发核心网设备向用户设备发送第二免流量消息，该第二免流量消息中携带登录信息，用户设备收到该登录信息后，可以基于该登录信息登录应用服务器。其中，第一免流

量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息，这样，通过采用不产生待计费流量的消息获取登录应用服务器所需要的信息，不仅能够借助电信运营商的网络资源实现免密登录，还可以适用于更多的场景。比如，在用户的用户设备没有开启移动网络数据流量的情况下，也可以进行便捷且安全的免密登录。

5 结合第一方面，在第一方面的某些实现方式中，第一免流量消息指示核心网设备向用户设备提供登录信息。

一示例，第一免流量消息本身可指示核心网设备向用户设备提供登录信息。基于该示例，当核心网设备收到该第一免流量消息后，可确定要向用户设备提供登录信息。

另一示例，第一免流量消息包括指示信息，该指示信息指示核心网设备向用户设备提供登录信息。基于该示例，当核心网设备收到该第一免流量消息后，可根据该第一免流量消息中的指示信息确定要向用户设备提供登录信息。

结合第一方面，在第一方面的某些实现方式中，方法还包括：用户设备获取并显示第一标识信息；或者，用户设备获取并显示第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

15 示例地，第一标识信息为用户设备对应的用户的通信标识，如为该用户的手机号。

基于上述技术方案，用户设备获取第一标识信息或第二标识信息，从而可在登录页面上显示用户的标识信息，并且可便于用户获知用户设备将使用自己的标识进行免密登录。进而可决策是否要通过该第一标识信息或第二标识信息对应的标识登录。这样可提高用户的登录体验。此外，若登录页面显示的是第二标识信息，还可以进一步避免用户的用户标识泄露给第三方实体。

20 结合第一方面，在第一方面的某些实现方式中，用户设备获取第一标识信息，包括：用户设备从核心网设备发送的消息中获取第一标识信息；或者，用户设备获取第二标识信息，包括以下任一项：用户设备从核心网设备发送的消息中获取第二标识信息；或者，用户设备从核心网设备发送的消息中获取第一标识信息，并对第一标识信息进行脱敏处理得到第二标识信息。

25 基于上述技术方案，用户设备可以直接获取第二标识信息，或者也可以获取第一标识信息，并对第一标识信息进行脱敏处理得到第二标识信息。

结合第一方面，在第一方面的某些实现方式中，用户设备从核心网设备发送的消息中获取第一标识信息，包括：用户设备从第二免流量消息获取第一标识信息；或者，用户设备从核心网设备发送的消息中获取第二标识信息，包括：用户设备从第二免流量消息获取第二标识信息。

基于上述技术方案，登录信息和用户的标识信息（如用户的第一标识信息或用户的第二标识信息），可以通过一个信令传输，从而可节省信令开销。

35 结合第一方面，在第一方面的某些实现方式中，方法还包括：用户设备接收来自核心网设备的第三免流量消息，其中，第三免流量消息为通过基站传输且不产生待计费流量的消息，则：用户设备从核心网设备发送的消息中获取第一标识信息，包括：用户设备从第三免流量消息获取第一标识信息；或者，用户设备从核心网设备发送的消息中获取第二标识信息，包括：用户设备从第三免流量消息获取第二标识信息。

示例地，第三免流量消息可以为 SIP 查询响应消息或者 SIP 注册响应消息。

示例地，第三免流量消息可以为 NAS 注册接受消息。

示例地，第三免流量消息和第二免流量消息可以相同，也可以不同，不予限制。

结合第一方面，在第一方面的某些实现方式中，通过基站传输且不产生待计费流量的消息是：经过基站及用户面数据网关传输且不产生待计费流量的用户面（user plane）消息。

5 示例地，用户面数据网关，可以为第三代合作伙伴计划（3rd generation partnership project, 3GPP）标准规范中定义的用户面功能（user plane function, UPF）网元。

示例地，第一免流量消息、第二免流量消息、第三免流量消息均为经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。

10 示例地，经过基站及用户面数据网关传输且不产生待计费流量的用户面消息，也可以描述为经过基站及用户面数据网关传输且不产生待计费流量的用户面信令。

结合第一方面，在第一方面的某些实现方式中，经过基站及用户面数据网关传输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。

15 基于上述技术方案，由于 SIP 信令的传输可以不产生待计费流量。举例来说，SIP 信令属于核心网的用户面消息，SIP 信令可以由 UE 操作系统之下的底层软件发起、通过 IMS 接入点（access point name, APN）接入网络；该 SIP 信令经过 UPF 时，UPF 识别其类型后可统计流量但不会计费，即不产生待计费流量。因此用户设备与核心网设备之间通过 SIP 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户的用户设备没有开启移动网络数据流量的情况下，也可以进行便捷且安全的免密登录。

20 结合第一方面，在第一方面的某些实现方式中，第一免流量消息为 SIP 查询消息，第二免流量消息为 SIP 查询响应消息；或者，第一免流量消息为 SIP 注册消息，第二免流量消息为 SIP 注册响应消息。

示例地，SIP 查询消息例如可以为 SIP OPTIONS 消息。

25 基于上述技术方案，若第一免流量消息为 SIP 注册消息，第二免流量消息为 SIP 注册响应消息，则可以复用现有的流程，如在用户设备注册通过 SIP 协议注册到通信网络中时，获取登录信息，从而可节省信令开销。

结合第一方面，在第一方面的某些实现方式中，核心网设备为呼叫会话控制功能设备。

示例地，呼叫会话控制功能设备可以为服务-呼叫会话控制功能（serving-call session control function, S-CSCF）设备。

30 示例地，核心网设备（如呼叫会话控制功能设备）可校验应用服务器的身份。举例来说，应用服务器可以与核心网设备（如呼叫会话控制功能设备）预先协商一个密钥，该密钥可用于应用服务器向核心网设备请求验证登录信息时，核心网设备校验应用服务器的身份；当核心网设备校验完应用服务器的身份后，可开始验证登录信息。

示例地，核心网设备中还可能包括其他的功能网元，对此不予限制。

35 结合第一方面，在第一方面的某些实现方式中，通过基站传输且不产生待计费流量的消息是：经过基站且不经用户面数据网关传输的控制面（control plane）消息。

示例地，第一免流量消息、第二免流量消息、第三免流量消息均为经过基站且不经用户面数据网关传输的控制面消息。

示例地，经过基站且不经用户面数据网关传输的控制面消息，也可以描述为，经过

基站且不经用户面数据网关传输的控制面信令。

结合第一方面，在第一方面的某些实现方式中，经过基站且不经用户面数据网关传输的控制面消息是非接入层 NAS 消息。

- 5 基于上述技术方案，由于 NAS 信令属于控制面消息，控制面消息可不计入流量，因此不产生待计费流量，这样，用户设备与核心网设备之间通过 NAS 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户设备不支持 IMS 网络的情况下，也可以进行便捷且安全的免密登录。

结合第一方面，在第一方面的某些实现方式中，第一免流量消息为 NAS 注册消息，第二免流量消息为 NAS 注册接受消息。

- 10 结合第一方面，在第一方面的某些实现方式中，核心网设备为接入管理网元。

示例地，接入管理网元，可以为 3GPP 标准规范中定义的接入和移动性管理功能（access and mobility management function, AMF）网元。

- 15 示例地，核心网设备（如 AMF 网元）可校验应用服务器的身份。举例来说，应用服务器可以与核心网设备（如 AMF 网元）预先协商一个密钥，该密钥可用于应用服务器向核心网设备请求验证登录信息时，核心网设备校验应用服务器的身份；当核心网设备校验完应用服务器的身份后，可开始验证登录信息。

示例地，核心网设备还可以包括其他的功能网元，不予限制。

结合第一方面，在第一方面的某些实现方式中，第二免流量消息还包括所述登录信息的认证地址。

- 20 其中，登录信息的认证地址，可表示通过向该认证地址发送该登录信息，可实现对该登录信息的认证。例如，登录信息的认证地址为网络开放网元的地址，应用服务器向该网络开放网元发送登录信息，从而可实现对该登录信息的验证。举例来说，该网络开放网元可向核心网设备发送该登录信息，以便核心网设备对该登录信息进行验证。再例如，登录信息的认证地址为核心网设备自身的地址，应用服务器向该核心网设备发送登录信息，从而核心网设备对该登录信息进行验证。

- 25 基于上述技术方案，该第二免流量消息中还包括登录信息的认证地址。认证地址，可用于指示认证该登录信息的设备的地址，或者提供对该登录信息进行认证的接口服务的设备的地址，或者接收来自应用服务器的该登录信息的设备的地址。一种可能的形式，登录信息的认证地址为网络开放网元的地址；另一种可能的形式，登录信息的认证地址为其他地址信息，根据该其他地址信息可确定出网络开放网元的地址。

第二方面，提供了一种通信方法，该方法可以由核心网设备执行，或者，也可以由核心网设备的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由核心网设备执行为例进行说明。

- 35 该方法可以包括：核心网设备接收来自用户设备的第一免流量消息，第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息；核心网设备生成登录信息，登录信息为用户设备登录到应用服务器所需要的信息；核心网设备向用户设备发送第二免流量消息，第二免流量消息包括登录信息；其中，第一免流量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息。

结合第二方面，在第二方面的某些实现方式中，第一免流量消息指示核心网设备向用

户设备提供登录信息。

结合第二方面，在第二方面的某些实现方式中，方法还包括：核心网设备向用户设备发送第一标识信息或第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

- 5 结合第二方面，在第二方面的某些实现方式中，核心网设备向用户设备发送第二标识信息，包括：核心网设备对第一标识信息进行脱敏处理得到第二标识信息，并向用户设备发送第二标识信息。

结合第二方面，在第二方面的某些实现方式中，第二免流量消息包括第一标识信息或第二标识信息。

- 10 结合第二方面，在第二方面的某些实现方式中，核心网设备向用户设备发送第一标识信息或第二标识信息，包括：核心网设备向用户设备发送第三免流量消息，第三免流量消息包括第一标识信息或第二标识信息；其中，第三免流量消息为通过基站传输且不产生待计费流量的消息。

- 结合第二方面，在第二方面的某些实现方式中，通过基站传输且不产生待计费流量的消息是：经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。
- 15 结合第二方面，在第二方面的某些实现方式中，经过基站及用户面数据网关传输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。

- 结合第二方面，在第二方面的某些实现方式中，第一免流量消息为 SIP 查询消息，第二免流量消息为 SIP 查询响应消息；或者，第一免流量消息为 SIP 注册消息，第二免流量消息为 SIP 注册响应消息。
- 20 结合第二方面，在第二方面的某些实现方式中，核心网设备为呼叫会话控制功能设备。

结合第二方面，在第二方面的某些实现方式中，通过基站传输且不产生待计费流量的消息是：经过基站且不经用户面数据网关传输的控制面消息。

- 结合第二方面，在第二方面的某些实现方式中，经过基站且不经用户面数据网关传输的控制面消息是非接入层 NAS 消息。
- 25 结合第二方面，在第二方面的某些实现方式中，第一免流量消息为 NAS 注册消息，第二免流量消息为 NAS 注册接受消息。

结合第二方面，在第二方面的某些实现方式中，核心网设备为接入管理网元。

- 结合第二方面，在第二方面的某些实现方式中，第二免流量消息还包括认证登录信息的证地址。
- 30 结合第二方面，在第二方面的某些实现方式中，方法还包括：核心网设备接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；核心网设备向应用服务器发送用户的第三标识信息，用户的第三标识信息是基于登录信息确定的。

示例地，第三标识可识别用户。例如，第三标识为用户的通信号码。

- 35 结合第二方面，在第二方面的某些实现方式中，核心网设备向应用服务器发送用户的第三标识信息，包括：若核心网设备成功认证登录信息，则核心网设备向应用服务器发送用户的第三标识信息。

结合第二方面，在第二方面的某些实现方式中，方法还包括：核心网设备基于登录信息和对应关系，确定用户的第三标识信息，对应关系包括用户的第三标识信息与登录信息

之间的对应关系。

第二方面及各个可能的设计的有益效果可以参考第一方面相关的描述，在此不予赘述。

5 第三方面，提供了一种通信方法，该方法可以由通信系统执行，或者，也可以由通信系统的组成部件（例如芯片或者电路）执行，对此不作限定。下面以通信系统包括用户设备和核心网设备为例进行说明。

10 该方法可以包括：用户设备向核心网设备发送第一免流量消息，第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息；核心网设备接收第一免流量消息，并生成登录信息，登录信息为用户设备登录到应用服务器所需要的信息；核心网设备向用户设备发送第二免流量消息，第二免流量消息包括登录信息；用户设备接收第二免流量消息，并向应用服务器发送登录信息，以登录到应用服务器；其中，第一免流量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息。

关于第三方面中可能的实现方式以及效果可以参考前面第一方面以及第二方面中的描述，此处不再赘述。

15 第四方面，提供了一种通信方法，该方法可以由用户设备执行，或者，也可以由用户设备的组成部件（例如芯片或者电路）执行，对此不作限定。

20 该方法可以包括：用户设备向呼叫会话控制功能设备发送会话初始协议 SIP 消息；用户设备接收来自呼叫会话控制功能设备的 SIP 消息的响应，SIP 消息的响应包括登录信息，登录信息为用户设备登录到应用服务器所需要的信息；用户设备向应用服务器发送登录请求消息，登录请求消息中包括登录信息。

示例地，呼叫会话控制功能设备可以为 S-CSCF 设备。

25 基于上述技术方案，由于 SIP 信令的传输可以不需要用户的计费流量，因此，用户与呼叫会话控制功能设备之间通过 SIP 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户的用户设备没有开启移动网络数据流量的情况下，也可以进行便捷且安全的免密登录。

结合第四方面，在第四方面的某些实现方式中，SIP 消息为 SIP 查询消息，SIP 消息的响应为 SIP 查询响应消息；或者，SIP 消息为 SIP 注册消息，SIP 消息的响应为 SIP 注册响应消息。

30 结合第四方面，在第四方面的某些实现方式中，方法还包括：用户设备获取并显示第一标识信息；或者，用户设备获取并显示第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

35 结合第四方面，在第四方面的某些实现方式中，用户设备获取第一标识信息，包括：用户设备从呼叫会话控制功能设备发送的消息中获取第一标识信息；或者，用户设备获取第二标识信息，包括以下任一项：用户设备从呼叫会话控制功能设备发送的消息中获取第二标识信息；或者，用户设备从呼叫会话控制功能设备发送的消息中获取第一标识信息，并对第一标识信息进行脱敏处理得到第二标识信息。

结合第四方面，在第四方面的某些实现方式中，用户设备从呼叫会话控制功能设备发送的消息中获取第一标识信息，包括：用户设备从 SIP 消息的响应获取第一标识信息；或者，用户设备从呼叫会话控制功能设备发送的消息中获取第二标识信息，包括：用户设备

从 SIP 消息的响应获取第二标识信息。

结合第四方面，在第四方面的某些实现方式中，方法还包括：用户设备接收来自呼叫会话控制功能设备的第三免流量消息，其中，第三免流量消息为通过基站传输且不产生待计费流量的消息，则：用户设备从呼叫会话控制功能设备发送的消息中获取第一标识信息，
5 包括：用户设备从第三免流量消息获取第一标识信息；或者，用户设备从呼叫会话控制功能设备发送的消息中获取第二标识信息，包括：用户设备从第三免流量消息获取第二标识信息。

结合第四方面，在第四方面的某些实现方式中，SIP 消息的响应还包括登录信息的认证地址。

10 第四方面及各个可能的设计的有益效果可以参考第一方面相关的描述，在此不予赘述。

第五方面，提供了一种通信方法，该方法可以由呼叫会话控制功能设备执行，或者，也可以由呼叫会话控制功能设备的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由呼叫会话控制功能设备执行为例进行说明。

15 该方法可以包括：呼叫会话控制功能设备接收来自用户设备的会话初始协议 SIP 消息；呼叫会话控制功能设备生成登录信息；呼叫会话控制功能设备向用户设备发送 SIP 消息的响应，SIP 消息的响应包括登录信息，登录信息为用户设备登录到应用服务器所需要的信息。

结合第五方面，在第五方面的某些实现方式中，SIP 消息为 SIP 查询消息，SIP 消息的响应为 SIP 查询响应消息；或者，SIP 消息为 SIP 注册消息，SIP 消息的响应为 SIP 注册响应消息。
20

结合第五方面，在第五方面的某些实现方式中，方法还包括：呼叫会话控制功能设备向用户设备发送第一标识信息或第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

25 结合第五方面，在第五方面的某些实现方式中，呼叫会话控制功能设备向用户设备发送第二标识信息，包括：呼叫会话控制功能设备对第一标识信息进行脱敏处理得到第二标识信息，并向用户设备发送第二标识信息。

结合第五方面，在第五方面的某些实现方式中，SIP 消息的响应包括第一标识信息或第二标识信息。

30 结合第五方面，在第五方面的某些实现方式中，呼叫会话控制功能设备向用户设备发送第一标识信息或第二标识信息，包括：呼叫会话控制功能设备向用户设备发送第三免流量消息，第三免流量消息包括第一标识信息或第二标识信息；其中，第三免流量消息为通过基站传输且不产生待计费流量的消息。

结合第五方面，在第五方面的某些实现方式中，SIP 消息的响应还包括登录信息的认证地址。
35

结合第五方面，在第五方面的某些实现方式中，方法还包括：呼叫会话控制功能设备接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；呼叫会话控制功能设备向应用服务器发送用户的第三标识信息，用户的第三标识信息是基于登录信息确定的。

结合第五方面，在第五方面的某些实现方式中，呼叫会话控制功能设备向应用服务器

发送用户的第三标识信息，包括：若呼叫会话控制功能设备成功认证登录信息，则呼叫会话控制功能设备向应用服务器发送用户的第三标识信息。

结合第五方面，在第五方面的某些实现方式中，方法还包括：呼叫会话控制功能设备基于登录信息和对应关系，确定用户的第三标识信息，对应关系包括用户的第三标识信息与登录信息之间的对应关系。

第五方面及各个可能的设计的有益效果可以参考第四方面相关的描述，在此不予赘述。

第六方面，提供了一种通信方法，该方法可以由用户设备执行，或者，也可以由用户设备的组成部件（例如芯片或者电路）执行，对此不作限定。

该方法可以包括：用户设备向核心网设备发送非接入层 NAS 消息；用户设备接收来自核心网设备的 NAS 消息的响应，NAS 消息的响应包括登录信息；用户设备向应用服务器发送登录请求消息，登录请求消息中包括登录信息。

基于上述技术方案，由于 NAS 信令的传输可以不需要用户的计费流量，因此，用户与核心网设备之间通过 NAS 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户设备不支持 IMS 网络的情况下，也可以进行便捷且安全的免密登录。

结合第六方面，在第六方面的某些实现方式中，NAS 消息为 NAS 注册消息，NAS 消息的响应为 NAS 注册接受消息。

结合第六方面，在第六方面的某些实现方式中，方法还包括：用户设备获取并显示第一标识信息；或者，用户设备获取并显示第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

结合第六方面，在第六方面的某些实现方式中，用户设备获取第一标识信息，包括：用户设备从接入管理网元发送的消息中获取第一标识信息；或者，用户设备获取第二标识信息，包括以下任一项：用户设备从接入管理网元发送的消息中获取第二标识信息；或者，用户设备从接入管理网元发送的消息中获取第一标识信息，并对第一标识信息进行脱敏处理得到第二标识信息。

结合第六方面，在第六方面的某些实现方式中，用户设备从接入管理网元发送的消息中获取第一标识信息，包括：用户设备从 NAS 消息的响应获取第一标识信息；或者，用户设备从接入管理网元发送的消息中获取第二标识信息，包括：用户设备从 NAS 消息的响应获取第二标识信息。

结合第六方面，在第六方面的某些实现方式中，方法还包括：用户设备接收来自接入管理网元的第三免流量消息，其中，第三免流量消息为通过基站传输且不产生待计费流量的消息，则：用户设备从接入管理网元发送的消息中获取第一标识信息，包括：用户设备从第三免流量消息获取第一标识信息；或者，用户设备从接入管理网元发送的消息中获取第二标识信息，包括：用户设备从第三免流量消息获取第二标识信息。

结合第六方面，在第六方面的某些实现方式中，NAS 消息的响应还包括登录信息的认证地址。

第六方面及各个可能的设计的有益效果可以参考第一方面相关的描述，在此不予赘述。

第七方面，提供了一种通信方法，该方法可以由接入管理网元执行，或者，也可以由接入管理网元的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由接入管理网元执行为例进行说明。

5 该方法可以包括：接入管理网元接收来自用户设备的 NAS 消息；接入管理网元生成登录信息；接入管理网元向用户设备发送 NAS 消息的响应，NAS 消息的响应包括登录信息，登录信息为用户设备登录到应用服务器所需要的信息。

结合第七方面，在第七方面的某些实现方式中，NAS 消息为 NAS 注册消息，NAS 消息的响应为 NAS 注册接受消息。

10 结合第七方面，在第七方面的某些实现方式中，方法还包括：接入管理网元向用户设备发送第一标识信息或第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

结合第七方面，在第七方面的某些实现方式中，接入管理网元向用户设备发送第二标识信息，包括：接入管理网元对第一标识信息进行脱敏处理得到第二标识信息，并向用户设备发送第二标识信息。

15 结合第七方面，在第七方面的某些实现方式中，NAS 消息的响应包括第一标识信息或第二标识信息。

结合第七方面，在第七方面的某些实现方式中，接入管理网元向用户设备发送第一标识信息或第二标识信息，包括：接入管理网元向用户设备发送第三免流量消息，第三免流量消息包括第一标识信息或第二标识信息；其中，第三免流量消息为通过基站传输且不产生待计费流量的消息。

20 结合第七方面，在第七方面的某些实现方式中，NAS 消息的响应还包括登录信息的认证地址。

结合第七方面，在第七方面的某些实现方式中，方法还包括：接入管理网元接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；接入管理网元向应用服务器发送用户的第三标识信息，用户的第三标识信息是基于登录信息确定的。

25 结合第七方面，在第七方面的某些实现方式中，接入管理网元向应用服务器发送用户的第三标识信息，包括：若接入管理网元成功认证登录信息，则接入管理网元向应用服务器发送用户的第三标识信息。

30 结合第七方面，在第七方面的某些实现方式中，方法还包括：接入管理网元基于登录信息和对应关系，确定用户的第三标识信息，对应关系包括用户的第三标识信息与登录信息之间的对应关系。

第七方面及各个可能的设计的有益效果可以参考第六方面相关的描述，在此不予赘述。

35 第八方面，提供了一种通信方法，该方法可以由应用服务器执行，或者，也可以由应用服务器的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由应用服务器执行为例进行说明。

该方法可以包括：应用服务器接收用户设备的登录请求消息，登录请求消息包括登录信息；应用服务器向核心网设备发送登录认证消息，登录认证消息包括登录信息，登录认证消息用于请求用户的第三标识信息；应用服务器接收来自核心网设备的用户的第三标识

信息。

结合第八方面，在第八方面的某些实现方式中，登录请求消息还包括登录信息的认证地址，应用服务器向核心网设备发送登录认证消息，包括：应用服务器通过认证地址，向核心网设备发送登录认证消息。

- 5 结合第八方面，在第八方面的某些实现方式中，认证地址用于指示网络开放网元的地址，应用服务器通过登录信息的认证地址，向核心网设备发送登录认证消息，包括：应用服务器通过网络开放网元，向核心网设备发送登录认证消息。

结合第八方面，在第八方面的某些实现方式中，登录认证消息还包括应用服务器的标识。

- 10 第九方面，提供了一种通信方法，该方法可以由核心网设备执行，或者，也可以由核心网设备的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由核心网设备执行为例进行说明。

- 15 该方法可以包括：核心网设备接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；核心网设备向应用服务器发送用户的第三标识信息，用户的第三标识信息是基于登录信息确定的。

结合第九方面，在第九方面的某些实现方式中，核心网设备向应用服务器发送用户的第三标识信息，包括：若核心网设备成功认证登录信息，则核心网设备向应用服务器发送用户的第三标识信息。

- 20 结合第九方面，在第九方面的某些实现方式中，方法还包括：核心网设备基于登录信息和对应关系，确定用户的第三标识信息，对应关系包括用户的第三标识信息与登录信息之间的对应关系。

结合第九方面，在第九方面的某些实现方式中，核心网设备为呼叫会话控制功能设备。

- 25 第十方面，提供了一种通信方法，该方法可以由网络开放网元执行，或者，也可以由网络开放网元的组成部件（例如芯片或者电路）执行，对此不作限定，为了便于描述，下面以由网络开放网元执行为例进行说明。

该方法可以包括：网络开放网元接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；网络开放网元向核心网设备发送登录认证消息；网络开放网元接收来自核心网设备的用户的第三标识信息，用户的第三标识信息是基于登录信息确定的；网络开放网元向应用服务器发送用户的第三标识信息。

- 30 结合第十方面，在第十方面的某些实现方式中，核心网设备为呼叫会话控制功能设备。

结合第一方面至第十方面，在某些实现方式中，登录信息包括核心网设备对以下至少一项信息进行加密或签名的结果：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的有效期。

- 35 结合第一方面至第十方面，在某些实现方式中，登录信息为根据以下至少一项生成的字符串：数字、字母、或符号。

第十一方面，提供一种通信的装置，该装置用于执行上述第一方面至第十方面任一种可能实现方式中的方法。具体地，该装置可以包括用于执行第一方面至第十方面任一种可能实现方式中的方法的单元和/或模块，如处理单元和/或通信单元。

在一种实现方式中，该装置为通信设备（如用户设备或核心网设备）。当该装置为通信设备时，通信单元可以是收发器，或，输入/输出接口；处理单元可以是至少一个处理器。可选地，收发器可以为收发电路。可选地，输入/输出接口可以为输入/输出电路。

5 在另一种实现方式中，该装置为用于通信设备（如用户设备或核心网设备）的芯片、芯片系统或电路。当该装置为用于通信设备的芯片、芯片系统或电路时，通信单元可以是该芯片、芯片系统或电路上的输入/输出接口、接口电路、输出电路、输入电路、管脚或相关电路等；处理单元可以是至少一个处理器、处理电路或逻辑电路等。

第十二方面，提供一种通信的装置，该装置包括：至少一个处理器，用于执行存储器存储的计算机程序或指令，以执行上述第一方面至第十方面任一种可能实现方式中的方法。可选地，该装置还包括存储器，用于存储的计算机程序或指令。可选地，该装置还包括通信接口，处理器通过通信接口读取存储器存储的计算机程序或指令。

在一种实现方式中，该装置为通信设备（如用户设备或核心网设备）。

在另一种实现方式中，该装置为用于通信设备（如用户设备或核心网设备）的芯片、芯片系统或电路。

15 第十三方面，提供一种处理器，用于执行上述各方面提供的方法。

对于处理器所涉及的发送和获取/接收等操作，如果没有特殊说明，或者，如果未与其在相关描述中的实际作用或者内在逻辑相抵触，则可以理解为处理器输出和接收、输入等操作，也可以理解为由射频电路和天线所进行的发送和接收操作，本申请对此不做限定。

第十四方面，提供一种计算机可读存储介质，该计算机可读介质存储用户设备执行的程序代码，该程序代码包括用于执行上述第一方面至第十方面任一种可能实现方式中的方法。

第十五方面，提供一种包含指令的计算机程序产品，当该计算机程序产品在计算机上运行时，使得计算机执行上述第一方面至第十方面任一种可能实现方式中的方法。

第十六方面，提供一种通信系统，包括前述的用户设备和/或核心网设备。

25

附图说明

图 1 是适用于本申请实施例的通信系统的示意图。

图 2 是免密登录的示意图。

图 3 是本申请实施例提供的一种通信方法 300 的示意图。

30 图 4 是本申请实施例提供的一种通信方法 400 的示意图。

图 5 是本申请实施例提供的一种通信方法 500 的示意图。

图 6 是本申请实施例提供的一种通信方法 600 的示意性流程图。

图 7 是本申请实施例提供的一种通信方法 700 的示意性流程图。

图 8 是本申请实施例提供的一种通信装置 800 的示意性图。

35 图 9 是本申请实施例提供另一种通信装置 900 的示意图。

具体实施方式

下面将结合附图，对本申请实施例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：第五代（5th generation，

5G) 或新无线 (new radio, NR) 系统、长期演进 (long term evolution, LTE) 系统、LTE 频分双工 (frequency division duplex, FDD) 系统、LTE 时分双工 (time division duplex, TDD) 系统等。本申请提供的技术方案还可以应用于未来的通信系统, 如第六代移动通信系统。本申请提供的技术方案还可以应用于设备到设备 (device to device, D2D) 通信, 5 车到万物 (vehicle-to-everything, V2X) 通信, 机器到机器 (machine to machine, M2M) 通信, 机器类型通信 (machine type communication, MTC), 以及物联网 (internet of things, IoT) 通信系统或者其他通信系统。

本申请实施例中的用户设备 (user equipment, UE) 也可以称为: 终端设备、接入终端、用户单元、用户站、移动站、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。

10 用户设备可以是一种向用户提供语音/数据的设备, 例如, 具有无线连接功能的手持式设备、车载设备等。目前, 一些终端的举例为: 手机 (mobile phone)、平板电脑、笔记本电脑、掌上电脑、移动互联网设备 (mobile internet device, MID)、可穿戴设备, 虚拟现实 (virtual reality, VR) 设备、增强现实 (augmented reality, AR) 设备、工业控制 (industrial control) 中的无线终端、无人驾驶 (self driving) 中的无线终端、远程手术 (remote medical surgery) 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、蜂窝电话、无绳电话、会话启动协议 (session initiation protocol, SIP) 电话、无线本地环路 (wireless local loop, WLL) 站、个人数字助理 (personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、可穿戴设备, 5G 网络中的终端设备或者未来演进的公用陆地移动通信网络 (public land mobile network, PLMN) 中的终端设备等, 本申请实施例对此并不限定。

20 作为示例而非限定, 在本申请实施例中, 该用户设备还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备, 是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称, 如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上, 或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备, 更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能, 例如: 智能手表或智能眼镜等, 以及只专注于某一类应用功能, 需要和其它设备如智能手机配合使用, 如各类进行体征监测的智能手环、智能首饰等。

30 本申请实施例中, 用于实现用户设备的功能的装置可以是用户设备, 也可以是能够支持用户设备实现该功能的装置, 例如芯片系统或芯片, 该装置可以被安装在用户设备中。本申请实施例中, 芯片系统可以由芯片构成, 也可以包括芯片和其他分立器件。

本申请实施例中的网络设备可以是用于与用户设备通信的设备。作为示例, 网络设备例如可以为用于为用户设备提供服务的通信网络中的设备。在本申请实施例中, 通信网络可包括运营商 IP 多媒体子系统 (IP multimedia subsystem, IMS) 网络, 也可包括搭建的通信网络, 或者也可包括其他通信网络, 对此不予限制。

作为示例, 网络设备例如可以包括以下一项或多项: 网络开放功能 (network exposure function, NEF) 网元、归属用户服务器 (home subscriber server, HSS)、服务-呼叫会话控

制功能 (serving-call session control function, S-CSCF) 设备、接入和移动性管理功能 (access and mobility management function, AMF) 网元、统一数据管理 (unified data management, UDM) 网元、应用服务器 (application server)。可以理解, 应用服务器可为用户设备提供应用层服务 (或者说为用户设备中的应用客户端提供服务), 如视频服务、导航服务、
5 电子商务服务或社交通信服务等, 具体是什么应用层服务, 本申请实施例不予限制。

本申请实施例中多次提及基站, 可以理解, 基站可以广义的覆盖如下中的各种名称, 或与如下名称进行替换, 比如: 节点 B (NodeB)、演进型基站 (evolved NodeB, eNB)、下一代基站 (next generation NodeB, gNB)、中继站、接入点、传输点 (transmitting and receiving point, TRP)、发射点 (transmitting point, TP)、主站、辅站、多制式无线 (multi-mode radio, MSR) 节点、家庭基站、网络控制器、接入节点、无线节点、接入点 (access point, AP)、传输节点、收发节点、基带单元 (baseband unit, BBU)、射频拉远单元 (remote radio unit, RRU)、有源天线单元 (active antenna unit, AAU)、射频头 (remote radio head, RRH)、中心单元 (central unit, CU)、分布式单元 (distributed unit, DU)、定位节点等。基站可以是宏基站、微基站、中继节点、施主节点或类似物, 或其组合。基站还可以
10 指用于设置于前述设备或装置内的通信模块、调制解调器或芯片。基站还可以是移动交换中心以及 D2D、V2X、M2M 通信中承担基站功能的设备、6G 网络中的网络侧设备、未来的通信系统中承担基站功能的设备等。基站可以支持相同或不同接入技术的网络。本申请的实施例对网络设备所采用的具体技术和具体设备形态不做限定。基站可以是固定的, 也可以是移动的。例如, 直升机或无人机可以被配置成充当移动基站, 一个或多个小区可以根据该移动基站的位置移动。在其他示例中, 直升机或无人机可以被配置成用作与另一基
15 站通信的设备。

为便于理解本申请实施例, 首先结合图 1 详细说明适用于本申请实施例的通信系统。

图 1 是适用于本申请实施例的通信系统的示意图。如图 1 所示, 该通信系统可以包括一个或多个用户设备, 例如图 1 所示的用户设备 110。该通信系统还可以包括一个或多个
25 网络设备, 例如图 1 所示的网络设备 120。可选地, 该通信系统还包括应用服务器, 例如图 1 所示的应用服务器 130。用户设备与网络设备之间也可进行通信, 例如, 用户设备 110 可以与网络设备 120 通信。用户设备与应用服务器之间也可进行通信, 例如, 用户设备 110 可以与应用服务器 130 通信。网络设备与应用服务器之间也可进行通信。例如, 网络设备 120 与应用服务器 130 通信。

30 作为示例, 网络设备集合 120 中的设备例如可以为用于为用户设备提供服务的通信网络中的设备。网络设备集合 120 例如可以包括以下一项或多项: NEF 网元、HSS 设备、S-CSCF 设备、AMF 网元、UDM 网元。下面简单介绍各设备。

1、NEF 网元: 可用于安全地向外部开放由第三代合作伙伴计划 (3rd generation partnership project, 3GPP) 网络功能实体提供的业务和能力等。

35 2、HSS 设备: 可用于处理调用会话的 IMS 网络实体的主要用户数据库。

3、S-CSCF 设备: 可用于接收发送端发来的通信请求消息。

4、AMF 网元: 可用于接入控制、移动性管理、附着与去附着等功能。

5、UDM 网元: 可用于 UE 的签约数据管理, 包括 UE 标识的存储和管理, UE 的接入授权等。

可以理解，图 1 仅为便于理解而示例的简化示意图，本申请并未限定于此。

还可以理解，本申请中提及的核心网设备是指核心网中的网元，例如，S-CSCF 设备、AMF 设备等。作为示例，移动网络包括三个部分：基站子系统、网络子系统、以及系统支撑，核心网通常位于网络子系统内，核心网的功能主要包括提供用户连接、对用户的管理以及对业务完成承载，核心网可作为承载网络提供到外部网络（互联网）的接口。本申请实施例中，核心网设备还可以通过免流量消息向用户设备提供登录信息，对应用服务器发送的登录信息进行认证。

还可以理解，本申请实施例中提及的网元，如 AMF 网元、NEF 网元、UDM 网元等功能网元，可以理解为用于实现不同功能的网元，可以按需组合成网络切片。这些网元可以是各自独立的硬件设备，也可以集成于同一硬件设备中，或者可以是硬件设备中的网络元件，也可以是在专用硬件上运行的软件功能，或者是平台（例如，云平台）上实例化的虚拟化功能模块，本申请对于上述网元的具体形态不作限定。还可以理解，上述命名仅为便于区分不同的功能而定义，不对本申请构成任何限定。本申请并不排除在 6G 网络以及未来其它的网络中采用其他命名的可能。例如，上述 5G 网络的部分或全部网元有关的术语可以在 6G 网络中沿用。

随着用户交互体验的不断改进，出现了一种登录方式，即免密登录。免密登录是指不需要用户手工输入账号和密码就能够完成登录。免密登录可以用于很多的场景，如用于企业应用程序（application，APP）的注册、登录以及支付等业务场景。免密登录方式更好地满足了用户对交互体验的追求，该方式不仅可以加快登录速度，提高登录的效率，还可以避免用户忘记密码、输错密码等带来的麻烦。

图 2 是免密登录的示意图。如图 2 所示，一种可能的免密登录方式如下：在用户设备呈现免密登录页面后，用户可点击“通过手机号码一键登录”按钮，可完成免密登录。可选地，若免密登录页面上有服务协议，则用户可勾选该免密登录页面上的服务协议，并点击“通过手机号码一键登录”按钮，可完成免密登录。如此，可免去繁琐的输入环节，没有短信验证码，没有复杂难辨的图片验证码，点击一个按钮即可完成登录操作，给用户带来极大方便。

然而，在现有的免密登录流程中，需要使用用户订购的移动数据流量业务，若用户没有订购移动网络数据流量业务或者移动数据流量开关没有打开，则无法进行免密登录。

本申请提出一种方式，基于不产生待计费流量的信令，如会话初始协议（session initialization protocol，SIP）信令或非接入层（non-access stratum，NAS）信令，来获取登录所需要的信息。这样，不仅可以实现免密登录，还可以充分利用电信运营商的网络资源。

为便于理解本申请实施例，对本申请中涉及到的术语做简单说明。

1、通信号码

用户关联至少一个用户识别模块，用户识别模块例如可以为卡片（如上网卡，又如电话卡等等）。作为示例，用户识别模块例如可以为以下任一种：用户识别卡（subscriber identification module，SIM），通用用户识别卡（universal subscriber identification module，USIM），嵌入式 SIM 卡（Embedded-SIM，eSIM），用户识别模块（user identity model，UIM），IP 多媒体服务身份模块（IP multimedia service identity module），码分多址（code division multiple access，CDMA）用户识别模块（CDMA subscriber identity module，CSIM）

等等。

通信号码，为与用户识别模块（或者独立的通信单元）绑定的号码，通信号码可用于与其他用户进行通信。作为示例，通信号码，可以为当前广泛使用的电话号码或手机号码，是通信网络中的用户标识，用于与其他用户进行通信。通信号码可以为 N 位数字组成的号码，N 为大于 1 的整数。例如，N=11；再例如，N=4；再例如，N=8；再例如，N=12，等等。关于 N 的取值不予限制。可以理解，通信号码也可以是其他的表示形式，如字符串等，对此不予限制。

一种可能的形式，通信号码为移动台国际 ISDN 号码（mobile subscriber ISDN number, MSISDN）。其中，ISDN 为综合业务数字网（integrated service digital network, ISDN）。

在本申请中，对于一个用户来说，该用户通信号码的数量不予限制。一种可能的实现方式，用户通信号码的数量（如 MSISDN 的数量）与用户识别模块的数量相同。

2、通信号码掩码

在本申请实施例中，为便于描述，将隐匿了部分数字的通信号码称为通信号码掩码。假设通信号码为 N 位数值组成的号码，那么通信号码可以为将该 N 位数值中的 M 位数值隐匿，M 为大于 1 或等于 1，且 M 小于 N 的整数。举例来说，通信号码为 18612345678，则通信号码掩码例如可以是 186****5678。

在本申请中，对于一个用户来说，该用户通信号码掩码的数量不予限制。一种可能的实现方式，通信号码掩码的数量（如 MSISDN 掩码的数量）与通信号码的数量相同。

可以理解，通信号码掩码可以属于脱敏标识的一种，换句话说，下文中的通信号码掩码可替换为脱敏标识。

3、用户的标识

在介绍用户的标识之前，先简单介绍一下脱敏处理。

所谓脱敏处理，表示通过对信息的部分进行匿名化处理，例如，将信息的部分或全部变成“****”，以使该信息的真实内容不被完全暴露。

例如，用户的通信号码为 N 位数值组成的号码，那么对该通信号码脱敏处理，表示将该 N 位数值中的 M 位数值隐匿，M 为大于 1 或等于 1，且 M 小于 N 的整数。举例来说，通信号码为 18612345678，则对该通信号码脱敏处理后可得到：186****5678。

再例如，用户的昵称为“Alice”，那么对该用户的昵称脱敏处理，表示将该用户的昵称中部分信息隐匿，如对该用户的昵称脱敏处理后可得到：“*ice”。

在本申请实施例中，第一标识、第二标识、第三标识均为与用户设备对应的用户有关的标识。其中，第一标识可表示未经脱敏处理的用户标识，用于标识用户设备对应的用户，第二标识可表示对第一标识进行脱敏处理后得到的结果。作为示例，第一标识例如可以为：用户的通信号码、用户姓名、用户昵称、用户邮箱等等，相应地，第二标识可以是对上述标识进行脱敏处理后得到的标识。可以理解，上述关于第一标识的举例为示例说明，对此不予限制。

为便于说明，下面将第一标识和第二标识统称为显示标识，第三标识称为验证标识。可以理解，显示标识和验证标识是为区分做的命名，其命名不对本申请实施例的保护范围造成限定。下面介绍显示标识和验证标识。

1) 显示标识，表示用户设备登录应用服务器之前在登录页面显示的标识。通过在登

录页面上显示该显示标识，可便于用户获知用户设备将使用自己的哪一个标识进行免密登录，进而决策是否要通过该显示标识对应的标识登录，这样可提高用户的登录体验。此外，若在登录页面上显示的显示标识为第二标识，还可以进一步避免用户的用户标识泄露给第三方实体。

- 5 2) 验证标识（即第三标识），表示核心网设备对登录信息验证后向应用服务器返回的标识，该标识可标识用户。换句话说，应用服务器基于该验证标识可识别用户。

作为示例，验证标识为用户的通信号码（如 MSISDN），或者也可以为用户分配的标识，通过该标识可识别该用户。

- 10 可以理解，显示标识和验证标识功能不同。还可以理解，显示标识和验证标识可以相同，也可以不同，不予限制。

4、待计费流量

在本申请实施例中的“待计费流量”，是指电信网络中的数据网关（如 UPF 网元）检测到的应计费的数据流量。

5、移动数据流量业务

- 15 本申请实施例中的“移动数据流量业务”，是指运营商为用户提供的网络业务，用户设备（如手机）通过该网络业务访问数据网络（如互联网）的过程中，在运营商的数据网关可以检测到应计费的数据流量，即待计费流量。

- 20 可以理解，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。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

上面对本申请中涉及到的术语做了简单说明，下文实施例中不再赘述。

下文将结合附图详细说明本申请实施例提供的方法。

图 3 是本申请实施例提供的一种通信方法 300 的示意图。方法 300 可以包括如下步骤。

- 25 301，用户设备向核心网设备发送第一免流量消息，第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息。

可选地，第一免流量消息指示核心网设备向用户设备提供登录信息。其中，登录信息为用户设备登录到应用服务器所需要的信息。

一示例，第一免流量消息本身可指示核心网设备向用户设备提供登录信息。基于该示例，当核心网设备收到该第一免流量消息后，可确定要向用户设备提供登录信息。

- 30 另一示例，第一免流量消息包括指示信息，该指示信息指示核心网设备向用户设备提供登录信息。基于该示例，当核心网设备收到该第一免流量消息后，可根据该第一免流量消息中的指示信息确定要向用户设备提供登录信息。指示信息可通过一个或多个比特来实现。例如，假设通过 1 比特来指示核心网设备向用户设备提供登录信息，若第一免流量消息中的该比特设置为“1”，则表示第一免流量消息指示核心网设备向用户设备提供登录信息。应理解，上述仅是一种示例性说明，不予限制。

可以理解，第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息，也可以替换为，第一免流量消息用于触发核心网设备向用户设备发送登录信息。

302，用户设备从核心网设备接收第二免流量消息，第二免流量消息包括登录信息。

303，用户设备向应用服务器发送登录信息，以登录到应用服务器。

其中，第一免流量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息。

可选地，方法 300 还包括步骤 304：应用服务器向核心网设备发送登录信息，以验证该登录信息。

5 例如，应用服务器向核心网设备发送登录认证消息，该登录认证消息包括登录信息。可以理解，应用服务器可以直接向核心网设备发送登录信息，或者也可以间接向核心网设备发送登录信息。应用服务器间接向核心网设备发送登录信息，表示应用服务器通过其他设备或网元（如 NEF 网元）向核心网设备发送登录信息。例如，应用服务器向 NEF 网元发送登录信息，NEF 网元向核心网设备发送该登录信息。

10 基于本申请实施例，用户设备向核心网设备发送第一免流量消息，该第一免流量消息可用于触发核心网设备向用户设备发送登录信息，用户设备接收来自核心网设备的第二免流量消息，该第二免流量消息中携带登录信息，从而用户设备可以基于该登录信息登录应用服务器。其中，第一免流量消息和第二免流量消息不产生待计费流量，因此通过采用不产生待计费流量的消息获取登录应用服务器所需要的信息。这样，不仅能够借助电信运营

15 商的网络资源实现免密登录，还可以适用于更多的场景。

示例性地，本申请实施例方案至少适用于以下两种场景。

场景 1：用户在运营商中订购了移动数据流量业务，但是在用户设备中关闭了移动数据流量的开关或者移动数据流量业务已经欠费。

20 场景 2：用户在运营商中未订购移动数据流量业务，用户关联的用户识别模块（如 SIM 卡）可能仅用来语音通话，不能用来通过移动数据流量业务上网。这种情况常见于“双卡双待”的手机，其中的一张 SIM 卡可能未订购移动数据流量业务，但用户可能仍然想通过该 SIM 卡对应的手机号码实现免密登录。

可以理解，本申请实施例适用范围不限于上述两种场景。只要是用户设备无法通过移动数据流量业务获取登录信息的场景，本申请实施例都适用。

25 下面详细描述本申请实施例的方案。

示例性地，关于第一免流量消息和第二免流量消息，至少包括以下两种方案。

方案 1，第一免流量消息和第二免流量消息为用户面（user plane）消息。

30 用户面消息（或者用户面信令），即表示经过用户面数据网关的消息或信令。作为示例，用户面消息可以包括两种：一种是产生待计费流量的消息，一种是不产生待计费流量的消息。在本申请实施例中，第一免流量消息和第二免流量消息均为经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。示例地，用户面数据网关，可以为 3GPP 标准规范中定义的 UPF 网元。可以理解，在 5G 通信系统中，该用户面数据网关可以是 UPF 网元。在未来通信系统中，该用户面数据网关仍可以是 UPF 网元，或者，还可以有其它的名称，本申请不做限定。

35 可选地，第一免流量消息和第二免流量消息为 SIP 消息（也称为 SIP 信令）。作为示例，核心网设备为呼叫会话控制功能设备，该呼叫会话控制功能设备例如可以为 S-CSCF 设备。SIP 信令可以由 UE 发起、通过 IMS 接入点（access point, AP）接入网络；SIP 信令经过 UPF 时，UPF 识别信令类型为 SIP 信令后可不统计该 SIP 信令产生的流量或者统计该 SIP 信令产生的流量但不算入待计费流量，总之，不产生待计费流量。下面介绍两种

可能的形式。

一种可能的形式，第一免流量消息为 SIP 请求消息（如 SIP 查询消息），相应地，第二免流量消息为 SIP 请求消息的响应（如 SIP 查询消息的响应）。示例地，SIP 请求消息（如 SIP 查询消息）例如可以为 SIP OPTIONS 消息。在该形式下，在步骤 301 中，用户设备向核心网设备（如呼叫会话控制功能设备）发送 SIP 请求消息。具体地，后面结合方法 400 详细描述。

另一种可能的形式，第一免流量消息为 SIP 注册（SIP Register）消息，相应地，第二免流量消息为 SIP 注册响应（SIP Register Response）消息。在该形式下，步骤 301 中用户设备向核心网设备发送 SIP 注册消息（如呼叫会话控制功能设备）；步骤 302 中用户设备从核心网设备接收 SIP 注册响应消息。

方案 2，第一免流量消息和第二免流量消息为控制面（control plane）消息。

控制面消息（或者信令）可不计入流量，故也不产生待计费流量。因此，在本申请实施例中，第一免流量消息和第二免流量消息可以是控制面消息。或者也可以理解为，第一免流量消息和第二免流量消息为经过基站且不经用户面数据网关传输的控制面消息。

可选地，第一免流量消息和第二免流量消息为 NAS 消息。作为示例，核心网设备为接入管理网元，如 AMF 网元。可以理解，在 5G 通信系统中，该接入管理网元可以是 AMF 网元。在未来通信系统中，该接入管理网元仍可以是 AMF 网元，或者，还可以有其它的名称，本申请不做限定。下面介绍两种可能的形式。

一种可能的形式，第一免流量消息为 NAS 请求消息，相应地，第二免流量消息为 NAS 请求消息的响应。NAS 信令属于核心网的控制面消息。在该形式下，在步骤 301 中，用户设备向核心网设备（如 AMF 网元）发送 NAS 请求消息。具体地，后面结合方法 500 详细描述。

另一种可能的形式，第一免流量消息为 NAS 注册（NAS Register）消息，相应地，第二免流量消息为 NAS 注册接受（NAS Register Accept）消息。在该形式下，步骤 301 中用户设备向核心网设备发送 NAS 注册消息；步骤 302 中用户设备从核心网设备（如 AMF 网元）接收 NAS 注册接受消息。

可选地，第二免流量消息中还包括登录信息的认证地址。登录信息的认证地址，可用于指示认证该登录信息的设备的地址，或者提供对该登录信息进行认证的接口服务的设备的地址，或者接收来自应用服务器的该登录信息的设备的地址。一种可能的形式，登录信息的认证地址为网络开放网元的地址；另一种可能的形式，登录信息的认证地址为其他地址信息，根据该其他地址信息可确定出网络开放网元的地址。在上述两种可能的形式下，应用服务器可以基于该登录信息的认证地址向该网络开放网元发送登录信息，进而由该网络开放网元发送给核心网设备，由核心网设备进行验证。可以理解，上述为示例性说明，本申请实施例不限于此。例如，登录信息的认证地址为核心网设备自身的地址，应用服务器向该核心网设备发送登录信息，从而核心网设备对该登录信息进行验证。

在本申请实施例中，登录信息可用于用户设备登录应用服务器。举例来说，用户设备向应用服务器发送登录请求消息，在该登录请求消息中携带登录信息；应用服务器收到该登录信息后，可对该登录信息进行验证；若验证通过，则可允许（或者同意）用户设备登录。作为示例，登录信息例如可以为令牌（token）（或者也可称为票据）。

5 登录信息为用户设备登录到应用服务器所需要的信息。登录信息可以是核心网设备向用户设备提供的（如核心网设备生成的）。核心网设备可校验应用服务器的身份。举例来说，应用服务器可以与核心网设备预先协商一个密钥，该密钥可用于应用服务器向核心网设备请求验证登录信息时，核心网设备校验应用服务器的身份；当核心网设备校验完应用服务器的身份后，可开始验证登录信息；且在核心网设备验证完登录信息后，可向应用服务器返回验证标识（如用户的通信号码）。

关于登录信息（如 token）的形式，本申请实施例不予限制。

一种可能的形式，登录信息为字符串（如随机生成的字符串）的形式。该字符串如可以包含字母、数字等。该字符串的长度可以为 X。X 为大于 1 的整数，如 X=32。

10 另一种可能的形式，登录信息中可以包括以下至少一项信息和/或核心网设备对以下至少一项信息进行加密或签名的结果：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的验证信息、登录信息的有效期。其中，核心网设备对上述至少一项信息进行加密或签名，从而可以提高上述至少一项信息的安全。举例来说，上述信息可携带核心网设备的数字签名；核心网设备收到上述信息后，
15 可先基于核心网设备的密钥验证上述数字签名，若验证通过，则可获得上述信息，进而可以对上述信息进行验证；若验证未通过，则可认为验证失败。。

其中每一项介绍如下。

- 用户设备的信息可表示使用登录信息的用户设备的信息；
- 用户设备对应的用户的信息可表示使用登录信息的用户的信息；
- 20 -登录信息的认证地址可用于指示验证的执行主体，即谁来接收该登录信息；
- 登录信息的适用范围（scope），用于指示该登录信息的作用范围；
- 登录信息的有效期，或者登录信息的过期（expiration）信息，用于指示该登录信息的有效使用期限。作为示例，登录信息的有效期可以为 T 分钟（T 为大于 0 的数，如 T 为 1，又如 T 为 5），且是一次性的。
- 25 -登录信息的验证信息，可表示用于验证该登录信息是否为核心网设备生成的。其中，验证信息例如可以是约定的验证码（或者说约定的暗号）。

作为一种可能的情形，登录信息包括登录信息的适用范围，且登录信息的适用范围为“用于向核心网设备请求获取用户的通信号码”。在该情形下，用户设备向应用服务器发送登录请求消息，在该登录请求消息中携带登录信息；应用服务器收到该登录信息后，
30 向核心网设备发送该登录信息；核心网设备收到该登录信息后，可基于该登录信息的适用范围，获知向应用服务器发送该用户的通信号码。

作为另一种可能的情形，登录信息包括登录信息的验证信息，且登录信息的验证信息为核心网设备提供的验证码（如 1234）。在该情形下，用户设备向应用服务器发送登录请求消息，在该登录请求消息中携带登录信息以及验证码 1234；应用服务器收到该登录信息后，
35 向核心网设备发送该登录信息以及验证码 1234；核心网设备收到该登录信息后，可基于该验证码 1234，获知该登录信息是核心网设备提供的登录信息。

作为另一种可能的情形，登录信息中包括登录信息的有效期。在该情形下，用户设备向应用服务器发送登录请求消息，在该登录请求消息中携带登录信息；应用服务器收到该登录信息后，向核心网设备发送该登录信息；核心网设备收到该登录信息后，可基于登录

信息的有效期判断该登录信息是否有效；若有效，则验证成功，并可通知应用服务器验证成功；若登录信息已过期，则验证失败，并可通知应用服务器验证失败。

可以理解，上述为举例说明，在实际应用中，可以根据实际情况，在登录信息中携带更多的信息。

5 还可以理解，关于登录信息的具体生成方式本申请实施例不予限制。例如，核心网设备对以下至少一项信息进行加密或签名：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的验证信息、登录信息的有效期；然后向用户设备发送加密或签名后的上述信息。再例如，核心网设备对上述至少一项信息进行编码，然后向用户设备发送编码后的上述信息。

10 作为示例，下面以列举核心网设备生成登录信息的可能方式。例如，登录信息可包括三部分：头部（Header）、载荷（Payload）、签名（Signature）。其中，Header 的格式可以为 json 格式，Header 中包括登录信息的属性，例如包括签名算法、登录信息类型（如 token 类型）。Payload 的格式可以为 json 格式，如可包括以下至少一项信息：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的验证信息、登录信息的有效期。再例如，登录信息为“字符串 1.字符串 2.字符串 3”，其中，字符串 1=Base64_encode(Header)（即字符串 1 可采用 Base64 编码方式编码），字符串 2=Base64_encode(Payload)，字符串 3=Sign(字符串 1.字符串 2, 密钥)（即字符串 3 为使用密钥对字符串 1 和字符串 2 进行签名得到的）。可以理解，上述为示例性说明，关于如何生成登录信息以及登录信息的具体形式，本申请实施例不予限制。

20 此外，关于解析登录信息的方式也有很多，对此不予限制。作为示例，核心网设备在解析登录信息时，可执行如下步骤：（1）获取登录信息的属性：例如使用 Base64_decode（如上述字符串 1）得到登录信息的属性信息；（2）计算签名：字符串 4=Sign(字符串 1.字符串 2, 密钥)；（3）验证签名：将字符串 4 与登录信息里的字符串 3 进行比较，一致则签名验证通过；（4）Base64_decode（如上述字符串 2）得到上述信息（如用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的验证信息、登录信息的有效期中的至少一项）；（5）对上述信息进行验证。

可以理解，关于如何生成登录信息以及如何解析登录信息，本申请实施例不予限制。

30 可选地，方法 300 还包括：用户设备获取显示标识。作为示例，显示标识可以携带于第三免流量消息。关于第三免流量消息可以参考前面的第一免流量消息和第二免流量消息，此处不再赘述。可以理解，第三免流量消息与第二免流量消息可以相同，即显示标识和登录信息可以通过同一免流量消息传输，从而节省信令开销；或者，第三免流量消息与第二免流量消息可以不同，即显示标识和登录信息可以通过不同免流量消息传输。

35 显示标识信息，可以用于在用户设备登录应用服务器时，在登录页面显示。通过在登录页面上显示显示标识信息，可便于用户获知用户设备将使用自己的哪一个标识（假设用户有多个标识）进行免密登录，进而用户决策是否要通过该显示标识对应的标识登录，这样可提高用户的登录体验。

第一种可能的情形，显示标识信息为用户的通信号码。在该情形下，用户设备登录应用服务器时，登录页面显示该用户的通信号码，进而提高用户的登录体验。

可选地，在该情形下，用户设备收到用户的通信号码后，可生成用户的通信号码掩码，

这样，登录页面显示该用户的通信号码掩码，不仅可提高用户的登录体验，还可以进一步避免用户的用户标识泄露给第三方实体。

在该情形下，可选地，显示标识可以携带于第二免流量消息中，或者也可以携带于其他免流量消息中（如下文所述的注册消息），不予限制。

- 5 第二种可能的情形，显示标识信息为用户的通信号码掩码。在该情形下，用户设备登录应用服务器时，登录页面显示该用户的通信号码掩码，不仅可提高用户的登录体验，还可以进一步避免用户的用户标识泄露给第三方实体。

10 在该情形下，可选地，用户设备获取显示标识，包括：用户设备从核心网设备接收显示标识；或者，用户设备接收用户标识；用户设备对该用户标识进行脱敏处理得到显示标识。其中，用户标识或显示标识可以携带于第二免流量消息中，或者也可以携带于其他免流量消息中（如下文所述的注册消息），不予限制。

可以理解，上述为示例性说明，对此不予限制。

- 15 可选地，方法 300 还包括：用户设备向核心网设备发送注册消息，注册消息用于将用户设备注册到通信网络；用户设备接收来自核心网设备的注册消息的响应，该注册消息的响应包括显示标识信息，显示标识信息用于用户设备登录到应用服务器前显示。其中，注册消息和注册消息的响应均为通过基站传输且不产生待计费流量的消息。

20 第一种可能的情形，显示标识信息为用户的通信号码。可选地，在该情形下，用户设备收到用户的通信号码后，可生成用户的通信号码掩码，这样，可在登录页面显示该用户的通信号码掩码，不仅可提高用户的登录体验，还可以进一步避免用户的用户标识泄露给第三方实体。

第二种可能的情形，显示标识信息为用户的通信号码掩码。在该情形下，用户设备登录应用服务器时，可在登录页面显示该用户的通信号码掩码，不仅可提高用户的登录体验，还可以进一步避免用户的用户标识泄露给第三方实体。

- 25 可选地，方法 300 还包括：核心网设备接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；核心网设备向应用服务器发送验证标识，验证标识是基于登录信息确定的。应用服务器收到用户的登录请求消息后，可向核心网设备发送登录认证消息。

验证标识可用于识别出该用户，换句话说，应用服务器基于该验证标识可识别用户。例如，验证标识为用户的通信号码（如 MSISDN）。可以理解，上述为示例性说明，对此不予限制。例如，也可以为用户分配一标识，通过该标识可识别该用户。

- 30 一种可能的实现方式，若核心网设备成功认证登录信息，则核心网设备向应用服务器发送验证标识。核心网设备认证（或者校验）登录信息，即表示核心网设备校验登录信息的有效性。作为示例，核心网设备校验登录信息，例如可以包括以下至少一项：核心网设备校验登录信息是否已过期、核心网设备校验是否是自己校验该登录信息。例如，若登录信息未过期，则可认为校验通过；若登录信息过期，则可认为校验未通过。再例如，若核心网设备确定自己校验该登录信息，则可认为校验通过；若核心网设备确定自己无权校验该登录信息，则可认为校验未通过。

可选地，核心网设备可以基于登录信息和对应关系，确定验证标识。其中，对应关系包括验证标识与登录信息之间的对应关系。

一种可能的实现方式，核心网设备存储登录信息和验证标识之间的对应关系。在该情

况下，核心网设备收到来自应用服务器的登录认证消息后，可以基于本地存储的对应关系，以及登录认证消息中携带的登录信息，确定验证标识。

另一种可能的实现方式，其他设备存储登录信息和验证标识之间的对应关系。在该情况下，例如，核心网设备收到来自应用服务器的登录认证消息后，可以向该其他设备请求该对应关系；其他设备收到该请求后，向核心网设备发送该对应关系；核心网设备基于收到的对应关系以及登录认证消息中携带的登录信息，确定验证标识。再例如，核心网设备收到来自应用服务器的登录认证消息后，可以向该其他设备请求验证标识，在该请求中可携带登录信息；其他设备收到该请求后，基于对应关系和该登录信息，确定验证标识，并向核心网设备发送该验证标识。

作为示例，登录信息与验证标识之间具有对应关系。作为示例，以登录信息为 token 为例，登录信息与验证标识之间的对应关系可以以表 1 的形式存在。

表 1

token	验证标识
token#1	标识#1
token#2	标识#2
token#3	标识#3

可以理解，表 1 仅是示例性说明，对此不予限制，任何属于表 1 的变形，都适用于本申请。例如，表 1 中还可以包括更多数量的 token 和验证标识。

图 4 是本申请实施例提供的一种通信方法 400 的示意图。作为示例，方法 400 可以用于实现方法 300 中的方案 1。方法 400 中涉及到的术语可以参考术语部分以及方法 300 中的描述，此处不再赘述。假设第一免流量消息和第二免流量消息为 SIP 信令，方法 400 可以包括如下步骤。

401，用户设备向呼叫会话控制功能设备发送 SIP 请求消息，SIP 请求消息指示呼叫会话控制功能设备向用户设备提供登录信息。

其中，登录信息为用户设备登录到应用服务器所需要的信息。登录信息例如为 token。

在步骤 401 中，用户设备向呼叫会话控制功能设备发送 SIP 请求消息。作为示例，呼叫会话控制功能设备为 S-CSCF 设备。

402，用户设备接收来自呼叫会话控制功能设备的 SIP 请求消息的响应，SIP 请求消息的响应包括登录信息。

在步骤 402 中，用户设备接收来自呼叫会话控制功能设备的 SIP 请求消息的响应。

403，用户设备向应用服务器发送登录请求消息，登录请求消息中包括登录信息。

在步骤 403 中，用户设备向应用服务器发送登录请求消息。

可选地，方法 400 还包括步骤 404：应用服务器向呼叫会话控制功能设备发送登录信息，以验证该登录信息。可以理解，应用服务器可以直接向呼叫会话控制功能设备发送登录信息，或者也可以间接向呼叫会话控制功能设备发送登录信息。应用服务器间接向呼叫会话控制功能设备发送登录信息，表示应用服务器通过其他设备或网元（如 NEF 网元）向呼叫会话控制功能设备发送登录信息。例如，应用服务器向 NEF 网元发送登录信息，NEF 网元向呼叫会话控制功能设备发送该登录信息。

基于本申请实施例，由于 SIP 信令的传输可以不产生待计费流量，因此，用户设备与呼叫会话控制功能设备之间通过 SIP 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户的用户设备没有开启移动网络数据流量的情况下，也可以进行便捷且安全的免密登录。

5 可选地，方法 400 还包括：用户设备向呼叫会话控制功能设备发送注册消息，注册信息用于通过 SIP 协议将用户设备注册到通信网络；用户设备接收来自呼叫会话控制功能设备的注册消息的响应，注册消息的响应包括显示标识。用户与呼叫会话控制功能设备之间可通过 SIP 信令的交互，来获得显示标识。关于显示标识可参考方法 300 中的描述，此处不再赘述。

10 可选地，方法 400 还包括：呼叫会话控制功能设备接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；呼叫会话控制功能设备向应用服务器发送验证标识，验证标识是基于登录信息确定的。可以理解，呼叫会话控制功能设备向应用服务器提供的验证标识，用于应用服务器识别该用户。该验证标识，与用户设备向呼叫会话控制功能设备注册时收到的显示标识，可以相同，也可以不同。

15 举例来说，应用服务器收到用户的登录请求后，可以确定登录信息的认证地址（如运营商网络中的 NEF 网元的地址），进而向该 NEF 网元发送登录认证消息，该 NEF 网元向呼叫会话控制功能设备转发该登录认证消息。一种可能的实现方式，登录请求中包括登录信息的认证地址，应用服务器基于该登录请求，可直接获得登录信息的认证地址。可以理解，上述实现方式为示例性说明，本申请实施例不限于此。例如，应用服务器基于登录请求中的登录信息，去查询该登录信息的认证地址。

20 一种可能的实现方式，若呼叫会话控制功能设备成功认证登录信息，则呼叫会话控制功能设备向应用服务器发送验证标识。作为示例，呼叫会话控制功能设备基于登录信息和对应关系，确定验证标识，对应关系包括验证标识与登录信息之间的对应关系。具体的可以参考方法 300 中的描述，此处不再赘述。

25 可以理解，方法 400 为示例性说明，本申请实施例不限于此。例如，方法 400 中的 SIP 请求消息可替换为 SIP 注册消息，SIP 请求消息的响应可替换为 SIP 注册响应消息。再例如，方法 400 中的 SIP 请求消息可替换为 SIP 消息（或者 SIP 查询消息），SIP 请求消息的响应可替换为 SIP 消息的响应（或者 SIP 查询响应消息）。

30 图 5 是本申请实施例提供的一种通信方法 500 的示意图。作为示例，方法 500 可以用于实现方法 300 中的方案 2。方法 500 中涉及到的术语可以参考术语部分以及方法 300 中的描述，此处不再赘述。假设第一免流量消息和第二免流量消息为 NAS 信令，方法 500 可以包括如下步骤。

501，用户设备向接入管理网元发送 NAS 请求消息，NAS 请求消息指示接入管理网元向用户设备提供登录信息。

35 其中，登录信息为用户设备登录到应用服务器所需要的信息。登录信息例如为 token。

在步骤 501 中，用户设备向接入管理网元发送 NAS 请求消息。作为示例，接入管理网元为 AMF 网元。

502，用户设备接收来自接入管理网元的 NAS 请求消息的响应，NAS 请求消息的响应包括登录信息。

在步骤 502 中，用户设备接收来自接入管理网元的 NAS 请求消息的响应。

503，用户设备向应用服务器发送登录请求消息，登录请求消息中包括登录信息。

在步骤 503 中，用户设备向应用服务器发送登录请求消息。

可选地，方法 500 还包括步骤 504：应用服务器向接入管理网元发送登录信息，以验证该登录信息。可以理解，应用服务器可以直接向接入管理网元发送登录信息，或者也可以间接向接入管理网元发送登录信息。应用服务器间接向接入管理网元发送登录信息，表示应用服务器通过其他设备或网元（如 NEF 网元）向接入管理网元发送登录信息。例如，应用服务器向 NEF 网元发送登录信息，NEF 网元向接入管理网元发送该登录信息。

基于本申请实施例，由于 NAS 信令的传输可以不产生待计费流量，因此，用户与接入管理网元之间通过 NAS 信令的交互，来获得登录应用服务器所需要的登录信息，不仅可以实现免密登录，还可以适用于更多的场景。比如，在用户的用户设备没有开启移动网络数据流量的情况下，也可以进行便捷且安全的免密登录。

可选地，方法 500 还包括：用户设备向接入管理网元发送 NAS 注册消息；终端发送被接收来自接入管理网元的 NAS 注册消息的响应，NAS 注册消息的响应包括显示标识。用户与接入管理网元之间可通过 NAS 信令的交互，来获得显示标识。关于显示标识可参考方法 300 中的描述，此处不再赘述。

可选地，方法 500 还包括：接入管理网元接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；接入管理网元向应用服务器发送验证标识，验证标识是基于登录信息确定的。可以理解，接入管理网元向应用服务器提供的验证标识，用于应用服务器识别该用户。该验证标识，与用户通过用户设备向接入管理网元注册时收到的验证标识，可以相同，也可以不同。

举例来说，应用服务器收到用户的登录请求后，可以确定登录信息的认证地址（如运营商网络中的 NEF 网元的地址），进而向该 NEF 网元发送登录认证消息，该 NEF 网元向接入管理网元转发该登录认证消息。一种可能的实现方式，登录请求中包括登录信息的认证地址，应用服务器基于该登录请求，可直接获得登录信息的认证地址。可以理解，上述实现方式为示例性说明，本申请实施例不限于此。例如，应用服务器基于登录请求中的登录信息，去查询该登录信息的认证地址。

一种可能的实现方式，若接入管理网元成功认证登录信息，则接入管理网元向应用服务器发送验证标识。作为示例，接入管理网元基于登录信息和对应关系，确定验证标识，对应关系包括验证标识与登录信息之间的对应关系。具体的可以参考方法 300 中的描述，此处不再赘述。

可以理解，方法 500 为示例性说明，本申请实施例不限于此。例如，方法 500 中的 NAS 请求消息可替换为 NAS 注册消息，NAS 请求消息的响应可替换为 NAS 注册接受消息。再例如，方法 500 中的 NAS 请求消息可替换为 NAS 消息（或者 NAS 查询消息），NAS 请求消息的响应可替换为 NAS 消息的响应（或者 NAS 查询响应消息）。

下文为便于理解，以显示标识和验证标识均为通信号码 MSISDN，通信网络为运营商 IMS 网络，登录信息为 token，为例进行示例性说明。为区分，将用户设备对应的用户的 MSISDN 称为目标 MSISDN，将用户设备对应的用户的登录信息称为目标 token。

图 6 是本申请实施例提供的一种通信方法 600 的示意性流程图。该方法 600 可以用于实现上述方法 300 或方法 400 的方案。在该方法 600 中，核心网设备为 S-CSCF 设备。该方法 600 可以包括如下步骤。

601, IMS 客户端 (IMS Client) 向 S-CSCF 设备发送 SIP 注册 (register) 请求。

5 其中, IMS 客户端为 UE 中的 IMS 客户端。IMS 客户端可以安装于 (或者装载于) UE 基带芯片中。

在步骤 601 中, UE 中的 IMS 客户端向运营商 IMS 网络发起 SIP 注册请求, 该 SIP 注册请求经过路由之后到达 S-CSCF 设备。其中, 该 SIP 注册请求表示通过 SIP 协议进行 IMS 注册。可选地, 该 SIP 注册请求还可包括指示信息, 该指示信息用于指示 S-CSCF 设备向
10 用户设备提供目标 token。

602, S-CSCF 设备向 HSS 发送多媒体授权请求 (multimedia authorization request, MAR)。

S-CSCF 设备接收到来自 UE 的 SIP 注册请求后, 可向 HSS 发起多媒体授权请求, 以请求鉴权。

15 603, HSS 向 S-CSCF 设备返回多媒体授权应答 (multimedia authorization answer, MAA)。

可选地, 该 MAA 中包括注册与鉴权相关的信息。作为示例, 该 MAA 中包括目标 MSISDN。目标 MSISDN 表示用户 (即 UE 的用户) 的 MSISDN。

604, S-CSCF 设备向 IMS 客户端发送 SIP 注册响应。

20 该 SIP 注册响应, 可以认为是步骤 601 中 SIP 注册请求的响应。可选地, 若步骤 601 中的 SIP 注册请求还可包括指示信息, 该指示信息用于指示 S-CSCF 设备向用户设备提供目标 token; 则步骤 604 中, S-CSCF 设备向 IMS 客户端发送的 SIP 注册响应还可以包含目标 token。为便于说明, 方法 600 中主要介绍步骤 601 中的 SIP 注册请求不包括上述指示信息的情况, 即用户设备通过步骤 610 中的 SIP 请求消息来请求目标 token 为例进行示
25 例性说明。

其中, 该 SIP 注册响应中包括目标 MSISDN 或者目标 MSISDN 掩码。如前所述, MSISDN 为手机号码, MSISDN 掩码是指隐藏了部分数字的手机号码。其中, 目标 MSISDN 或者目标 MSISDN 掩码的数量可以是一个, 也可以是多个。举例来说, 若 UE 支持双卡双待, 且有双卡, 则该目标 MSISDN 可以有 2 个, 或者则该目标 MSISDN 掩码可以有 2 个。

30 目标 MSISDN 或者目标 MSISDN 掩码, 可以复用 SIP 注册响应中的现有字段, 或者也可以新增一字段。

第一种可能的方式, 该 SIP 注册响应中包括关联统一资源标识符 (uniform resource identifier, URI) (P-Associated-URI), 其中, P-Associated-URI 包含目标 MSISDN 或者目标 MSISDN 掩码。其中, P-Associated-URI, 可用于表示 UE 注册地址的所有关联 URI。

35 可以理解, 该 SIP 注册响应中还可以包括其他信息, 对此不予限制。作为一种可能的情形, 该 SIP 注册响应为 SIP 200 OK 响应。以 SIP 注册响应为 SIP 200 OK 响应, SIP 注册响应的一种可能形式如下。

SIP/2.0 200 OK

Service-Route: <sip:orig@test1.xxxx.com;lr;ca=ffffffff;TYPE=V4;IP=10.44.174.44;PORT

=53064>

P-Associated-URI: <186**5678>** //目标 MSISDN 掩码

Path: <sip:term@test2.xxxx.com;lr:ssn;TYPE=V4;IP=10.44.174.44;PORT=53064>

Accept-Resource-Priority: wps.4

5 Content-Length: 0

在上述示例中，SIP 200 OK 响应可包括目标 MSISDN 掩码，且目标 MSISDN 掩码携带于“P-Associated-URI”字段中，具体地，该目标 MSISDN 掩码为 186****5678。可以理解，“P-Associated-URI”字段还可能包括其他的信息，对此不予限制。

第二种可能的方式，该 SIP 注册响应中新增一字段，如称为“X-MSISDN-Mask”字段，该“X-MSISDN-Mask”字段中包含目标 MSISDN 或者目标 MSISDN 掩码。作为一种可能的情形，该 SIP 注册响应为 SIP 200 OK 响应。以 SIP 注册响应为 SIP 200 OK 响应，SIP 注册响应的一种可能形式如下。

SIP/2.0 200 OK

Service-Route: <sip:orig@test1.xxxx.com;lr;ca=ffffff;TYPE=V4;IP=10.44.174.44;PORT=53064>

P-Associated-URI: <sip:+8618612345678@xxxx.com;user=phone> //与用户身份相关的 URI

Path: <sip:term@test2.xxxx.com;lr:ssn;TYPE=V4;IP=10.44.174.44;PORT=53064>

Accept-Resource-Priority: wps.4

20 **X-MSISDN-Mask: 186****5678** //目标 MSISDN 掩码

Content-Length: 0

在上述示例中，SIP 200 OK 响应可包括目标 MSISDN 掩码，且目标 MSISDN 掩码通过“X-MSISDN-Mask”字段携带，具体地，该目标 MSISDN 掩码为 186****5678。

605，IMS 客户端获取目标 MSISDN 掩码。

25 可选地，IMS 客户端保存该目标 MSISDN 掩码。

IMS 客户端基于 SIP 注册响应获取目标 MSISDN 掩码，并保存该目标 MSISDN 掩码。该目标 MSISDN 掩码，可用于在授权页面（如步骤 608）呈现，具体地，后面结合步骤 608 详细说明。

可选地，IMS 客户端可以基于以下任一方式获取目标 MSISDN 掩码。

30 一种可能的方式，IMS 客户端基于目标 MSISDN，生成目标 MSISDN 掩码。

具体地，若步骤 604 中 S-CSCF 设备向 IMS 客户端发送的 SIP 注册响应中包括目标 MSISDN，则 IMS 客户端可根据目标 MSISDN 生成目标 MSISDN 掩码。

举例来说，在步骤 604 中，S-CSCF 设备向 IMS 客户端发送 SIP 200 OK 响应，且 SIP 200 OK 响应中包括“P-Associated-URI”字段，“P-Associated-URI”字段包含目标 MSISDN；IMS 客户端从 SIP 200 OK 响应中的“P-Associated-URI”字段里提取出目标 MSISDN，生成目标 MSISDN 掩码，并保存该目标 MSISDN 掩码。

另一种可能的方式，IMS 客户端直接获取目标 MSISDN 掩码。

具体地，若步骤 604 中 S-CSCF 设备向 IMS 客户端发送的 SIP 注册响应中包括目标 MSISDN 掩码，则 IMS 客户端可直接获取目标 MSISDN 掩码。其中，SIP 注册响应中包

- 括目标 MSISDN 掩码,例如可以是在 SIP 注册响应中新增头域(如称为 X-MSISDN-Mask),并将该头域的值设置为目标 MSISDN 掩码,如参考步骤 604 中 SIP 注册响应的示例;再例如, P-Associated-URI 包含目标 MSISDN 掩码。举例来说,在步骤 604 中, S-CSCF 设备向 IMS 客户端发送 SIP 200 OK 响应,且 SIP 200 OK 响应中包括“P-Associated-URI”字段,“P-Associated-URI”字段包含目标 MSISDN 掩码;IMS 客户端从 SIP 200 OK 响应中的“P-Associated-URI”字段里提取出目标 MSISDN 掩码,并保存该目标 MSISDN 掩码。
- 606, 用户设备呈现登录页面。
- UE 中的 APP 客户端 (APP Client) 呈现登录页面。
- 607, APP 客户端从 IMS 客户端获取目标 MSISDN 掩码。
- 10 在步骤 605 中, UE 中的 IMS 客户端保存目标 MSISDN 掩码,因此, APP 客户端可从 IMS 客户端获取目标 MSISDN 掩码。
- 举例来说, UE 操作系统可通过调用 IMS 客户端接口,获取 MSISDN 掩码;进一步地, APP 客户端通过调用该 UE 操作系统开放的接口,获取 MSISDN 掩码。
- 608, UE 中的 APP 客户端呈现授权页面,该授权页面上显示目标 MSISDN 掩码。
- 15 举例来说, APP 客户端弹出授权页面,并且在该授权页面上显示(或者展示,或者呈现)步骤 607 中获取的 MSISDN 掩码。此外,若 MSISDN 掩码的数量为多个,则授权页面上可显示该多个 MSISDN 掩码。举例来说,若 UE 中有双卡且支持双卡双待,则授权页面中展示两个 MSISDN 掩码。
- 可选地,该授权页面中还显示服务协议和登录按钮。若 MSISDN 掩码的数量为多个,且不同的 MSISDN 掩码对应的服务协议不同,则授权页面上可显示该多个 MSISDN 掩码对应的服务协议。
- 20 关于授权页面的来源可以有很多实现方式,对此不予限制。下面简单列举两种可能的方式。
- 一种可能的方式, APP 客户端集成了运营商的软件开发工具包 (software development kit, SDK), SDK 提供基础的授权页面, APP 客户端基于该基础的授权页面进行修改(或者调整),进而得到最终呈现的授权页面。
- 25 另一种可能的方式, UE 操作系统从 IMS 客户端获取基础的授权页面给 APP 客户端, APP 客户端基于该基础的授权页面进行修改(或者调整),进而得到最终呈现的授权页面。
- 在本申请实施例,通过在授权页面上显示目标 MSISDN 掩码,可便于用户获知自己将使用自己的号码进行免密登录。若授权页面上显示目标 MSISDN 掩码,则用户可以决策(或者判断,或者确定)是否要登录。若用户决策要登录,则可进行后续的登录操作;若用户决策不要登录,则可拒绝登录。
- 30 在授权页面上显示目标 MSISDN 掩码,可有助增强用户的登录体验,提高安全性。具体来说, MSISDN 是用户重要的数据,若用户不愿意(或者不同意)使用 MSISDN 进行免密登录,此时若在授权页面上呈现 MSISDN 是不合适的,且是不安全的。
- 35 609, APP 客户端确定用户授权。
- APP 客户端确定用户授权,或者 APP 客户端获知用户授权登录,表示基于用户的操作, APP 客户端可确定可以登录。
- 举例来说,在步骤 608 中的授权页面中显示有服务协议和登录按钮,若 APP 客户端

可通过用户选择（或者勾选，或者同意）该服务协议，点击登录按钮，确定用户授权。

610，APP 客户端通过 IMS 客户端向 S-CSCF 设备发送 SIP 请求消息。

该 SIP 请求消息用于请求目标 token。可选地，该 SIP 请求消息用于指示 S-CSCF 设备向用户设备提供目标 token。例如，该 SIP 请求消息本身可用于触发 S-CSCF 设备向用户设备提供目标 token；再例如，该 SIP 请求消息包括指示信息，该指示信息用于指示 S-CSCF 设备向用户设备提供目标 token。

举例来说，APP 客户端可调用 UE 操作系统开放的接口，请求目标 token；进一步地，UE 操作系统可调用 IMS 客户端接口去请求目标 token，即 IMS 客户端向 S-CSCF 设备发送 SIP 请求消息，该 SIP 请求消息用于请求目标 token。

其中，SIP 请求消息的形式例如可以为 SIP OPTIONS 消息。具体地，IMS 客户端向 S-CSCF 设备发送 SIP OPTIONS 消息，该 SIP OPTIONS 消息用于请求目标 token，该 SIP OPTIONS 消息中的 Accept 字段可携带：application/login-token 等信息。关于 SIP 请求消息，可以包括如下几种方式。

第一种可能的方式，通过 SIP OPTIONS 消息中的已有字段请求目标 token。作为示例，满足该方式的 SIP OPTIONS 消息形式如下。

```
OPTIONS sip: test1@xxxx.com
To: <sip:test1@xxxx.com>
From: Alice <sip:test2@xxxx.com>;tag=1928301774
Accept: application/login-token
Content-Length: 0
```

在上述示例中，用户设备可通过 SIP OPTIONS 消息中的“Accept”字段及其取值“application/login-token”指示 S-CSCF 设备向用户设备提供目标 token，或者用户设备通过“Accept”字段及其取值“application/login-token”指示 S-CSCF 设备向用户设备提供“application/login-token”类型的数据。其中，“application/login-token”类型的数据可表示登录应用所需要的信息（如目标 token）。

第二种可能的方式，通过 SIP OPTIONS 消息的起始行（或请求行）中的参数请求目标 token。作为示例，满足该方式的 SIP OPTIONS 消息形式如下。

```
OPTIONS sip: test1@huawei.com;type=login-token SIP/2.0
To: <sip:test1@huawei.com>
From: Alice <sip:test2@huawei.com>;tag=1928301774
Accept: application/json
Content-Length: 0
```

在上述示例中，用户设备可通过 SIP OPTIONS 消息的起始行中新增的“type=login-token”参数来指示 S-CSCF 设备向用户设备提供目标 token，或者用户设备通过“type=login-token”参数指示 S-CSCF 设备向用户设备提供“login-token”类型的数据。其中，“login-token”类型的数据可表示登录应用所需要的信息（如目标 token）。

可以理解，上述为示例性说明，对此不予限制。例如，“application/json”也可以是其他的类型，比如“application/text”。

第三种可能的方式，通过其他消息（如 SIPGET 消息）请求目标 token。作为示例，

SIPGET 消息形式如下。

GET sip: test1@huawei.com;type=login-token SIP/2.0

To: <sip:test1@huawei.com>

From: Alice <sip:test2@huawei.com>;tag=1928301774

5 Accept: application/json

Content-Length: 0

在上述示例中，用户设备可通过 SIP GET 消息的起始行（或请求行）中的“type=login-token”参数来指示 S-CSCF 设备向用户设备提供目标 token，或者用户设备通过“type=login-token”参数指示 S-CSCF 设备向用户设备提供“login-token”类型的数据。其中，“login-token”类型的数据可表示登录应用所需要的信息（如目标 token）。

10

611，S-CSCF 设备分配目标 token。

S-CSCF 设备可先确定目标 MSISDN，进而再分配目标 token。举例来说，S-CSCF 设备根据 SIP 请求消息中的信息（如 SIP OPTIONS 消息中的“From”字段的信息）确定用户的目标 MSISDN，进而生成 token，并将该 token 分配给目标 MSISDN，以完成目标 token 的分配操作。关于 token 的描述，可以参考方法 300 中关于登录信息的相关描述，此处不再赘述。

15

一种可能的情形，S-CSCF 设备保存（或者维护）目标 token 与目标 MSISDN 之间的对应关系，如以表 1 的形式保存。

另一种可能的情形，S-CSCF 设备可以向其他网元（如 UDM 网元发送目标 token 与目标 MSISDN 之间的对应关系，该其他网元保存该对应关系，如以表 1 的形式保存。

20

612，S-CSCF 设备通过 IMS 客户端向 APP 客户端发送目标 token。

可选地，S-CSCF 设备通过 IMS 客户端向 APP 客户端发送目标 token 的认证地址。其中，目标 token 和目标 token 的认证地址可以携带于同一信令中，也可以携带于不同信令中，不予限制。

25

举例来说，S-CSCF 设备向 IMS 客户端返回 SIP 响应消息，该 SIP 响应消息包括目标 token 和目标 token 的认证地址；UE 操作系统将 IMS 客户端获取到的目标 token 和目标 token 的认证地址，返回给 APP 客户端。

其中，S-CSCF 设备向 IMS 客户端返回的 SIP 响应消息的方法及字段名不予限制。例如，SIP 响应消息为 SIP 200 OK 响应，举例来说，S-CSCF 设备向 IMS 客户端返回 SIP 200 OK 响应，通过 SIP 200 OK 响应中的“X-Login-Token”字段携带目标 token，通过 SIP 200 OK 响应中的“X-Token-Auth-Addr”字段携带目标 token 的认证地址。

30

以步骤 610 中的第一种可能的方式为例，作为示例，SIP 200 OK 响应的形式如下。

SIP/2.0 200 OK

To: <sip:test1@xxxx.com>;tag=93810874

35

From: Alice <sip:test2@xxxx.com>;tag=1928301774

Accept: application/login-token

X-Login-Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjpbeyJ0b29sdHQiOiJodHRwczovL3Rvb2x0dC5jb20ifV0sImhhdCI6MTY0ODA4NTQ2NswiZXhwIjoxNjQ4MTM3NTk5LCJhdWQiOiJBbGJlZSIsImZyI6InRlc3QiLCJzdWIiOiJsb2dpbiJ9.

LrLUGSaNeepmq0EfPpLxN_o3cJQm3D_oV_11t_DTmQ //登录信息
X-Token-Auth-Addr: https://test3.xxx.com/verification //认证地址
Content-Length: 0

5 可以理解,上述“X-Login-Token”字段中携带的登录信息,可以是经过编码后的信息。举例来说,S-CSCF设备对以下至少一项信息采用Base64编码方式编码:用户设备的信息、用户设备对应的用户的信息、目标token的认证地址、目标token的适用范围、目标token的有效期、目标token的验证信息、目标token的有效期,编码后的目标token如上述示例。可以理解,关于是否编码,以及编码时采用何种编码方式,本申请实施例不予限制。

10 以步骤610中的第二种可能的方式为例,作为示例,SIP 200 OK响应的形式如下。

SIP/2.0 200 OK
To: <sip:test1@xxxx.com>;tag=93810874
From: Alice <sip:test2@xxxx.com>;tag=1928301774
15 Content-Code: application/json
Content-Length: 314

{
20 "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjpbeyJ0b29sdHQiOiJodHRwczovL3Rvb2x0dC5jb20ifV0sImldCI6MTY0ODA4NTQ2NSwiZXhwIjoxNjQ4MTM3NTk5LCJhdWQiOiJBbGJjZSIsImZcyI6InRlc3QiLCJzdWl0IjpbJ2dpbiJ9.LrLUGSaNeepmq0EfPpLxN_o3cJQm3D_oV_11t_DTmQ", //登录信息
"auth_addr": "https://test3.xxx.com/verification//认证地址"
25 }

目标token的认证地址为https://test3.xxx.com/verification。

作为示例,上述步骤601-612可以认为是登录前的准备,下面步骤613-619可以认为是登录以及登录的认证。

613, APP客户端向应用服务器发送登录请求消息。

30 其中,该登录请求消息中包括目标token。可选地,该登录请求消息中还包括目标token的认证地址。

614,应用服务器向NEF网元发送登录认证消息。

35 其中,该登录认证消息包括目标token,该登录认证消息用于请求验证标识。其中,验证标识与用户一一对应,验证标识可用于标识用户,换句话说,基于该验证标识可以识别出该用户。作为示例,验证标识为目标MSISDN。下面主要以目标MSISDN为例进行示例性说明。

应用服务器收到登录请求后,可以确定目标token的认证地址(如运营商网络中的NEF网元的地址),进而向该NEF网元发送登录认证消息。

一种可能的实现方式,登录请求中包括目标token的认证地址,应用服务器基于该登

录请求，可直接获得目标 token 的认证地址。可以理解，上述实现方式为示例性说明，本申请实施例不限于此。例如，应用服务器基于登录请求中的目标 token，去查询该目标 token 的认证地址。

5 可选地，登录认证消息还可以携带 APP ID。举例来说，应用服务器预先获取 APP ID，如应用服务器可向运营商网络请求 APP ID，当应用服务器向 NEF 网元发送登录认证消息时，在该登录认证消息中携带提前获取的 APP ID，进而运营商网络可以识别该应用服务器。

10 可选地，登录认证消息可进行加密和/或防篡改保护。一种可能的实现方式，该登录认证消息可使用 APP 密钥（key）进行加密。举例来说，应用服务器预先获取 APPkey，如应用服务器可向运营商网络请求 APPkey，当应用服务器向 NEF 网元发送登录认证消息时，该登录认证消息可使用 APPkey 进行加密，进而提高安全性。

615，NEF 网元向 S-CSCF 设备转发登录认证消息。

可选地，NEF 网元向 S-CSCF 设备转发登录认证消息，包括：若 NEF 网元成功认证登录认证消息，则 NEF 网元向 S-CSCF 设备转发登录认证消息。

15 举例来说，应用服务器向 NEF 网元发送的登录认证消息包括目标 token 和 APP ID，且该登录认证消息使用 APP key 进行加密；NEF 网元使用与 APP ID 相对应的 APP key 校验该登录认证消息；在校验成功后，NEF 网元向 S-CSCF 设备转发该登录认证消息。

616，S-CSCF 设备基于目标 token，查找目标 MSISDN。

20 一种可能的情形，若 S-CSCF 设备本地保存目标 token 与目标 MSISDN 之间的对应关系，则 S-CSCF 设备基于该对应关系查找该目标 token 对应的目标 MSISDN。以表 1 为例，若请求消息#1 中包括的目标 token 为 token#1，则 S-CSCF 设备确定该目标 token 对应的目标 MSISDN 为 MSISDN#1。

另一种可能的情形，若其他网元保存目标 token 与目标 MSISDN 之间的对应关系，则 S-CSCF 设备可以向其他网元请求该目标 token 对应的目标 MSISDN。

25 可选地，S-CSCF 设备基于目标 token，查找目标 MSISDN，包括：若 S-CSCF 设备成功认证目标 token（或者 S-CSCF 设备对目标 token 校验通过），则 S-CSCF 设备基于目标 token，查找目标 MSISDN。

30 S-CSCF 设备认证（或者校验）目标 token，即表示 S-CSCF 设备校验目标 token 的有效性。作为示例，S-CSCF 设备校验目标 token，例如可以包括以下至少一项：S-CSCF 设备校验目标 token 是否已过期、S-CSCF 设备校验是否是自己校验该目标 token。例如，若目标 token 未过期，则可认为校验通过；若目标 token 过期，则可认为校验未通过。再例如，若 S-CSCF 设备确定自己校验该目标 token，则可认为校验通过；若 S-CSCF 设备确定自己无权校验该目标 token，则可认为校验未通过。例如，以步骤 612 中的示例为例，S-CSCF 设备收到目标 token（即登录信息）后，可以先进行解码，获得该目标 token 中的上述至少
35 一项信息，进而再对上述至少一项信息进行校验。再例如，S-CSCF 设备收到携带数字签名的目标 token（即登录信息）后，可以先基于 S-CSCF 设备的密钥验证该数字签名，若验证通过，则可进行解码，获得该目标 token 中的上述至少一项信息，然后对上述至少一项信息进行校验。具体可以方法 300 中的相关描述，此处不再赘述。

617，S-CSCF 设备向 NEF 网元发送目标 MSISDN。

举例来说，S-CSCF 设备查找到目标 MSISDN 后，向 NEF 网元发送登录认证消息的响应，该响应携带目标 MSISDN。

618，NEF 网元向应用服务器发送目标 MSISDN。

5 举例来说，NEF 网元从 S-CSCF 设备接收到登录认证消息的响应后，向应用服务器转发该登录认证消息的响应。

619，应用服务器通知 APP 客户端登录成功。

经过上述步骤，用户可实现免密登录。

可选地，S-CSCF 设备对目标 token 进行处理。作为示例，S-CSCF 设备可对目标 token 进行以下至少一项处理：S-CSCF 设备记录 APP ID 使用目标 token 成功获取目标 MSISDN 的次数（如用于计费）、S-CSCF 设备将目标 token 标记为失效。

可以理解，图 6 所示实施例主要以通过 SIP 请求消息请求目标 token 为例进行示例性说明，对此不予限制。例如，用户设备也可以通过 SIP 注册请求获取目标 token，S-CSCF 设备向 IMS 客户端发送的 SIP 注册响应中携带该目标 token。

15 上文结合图 6 所示的步骤 601- 619 示例地介绍了通过 UE 与运营商 IMS 网络之间的 SIP 信令来完成登录的场景。基于上述实施例，借助运营商 IMS 网络，通过 SIP 信令可实现免密登录，可支持更多场景下的免密登录，且不依赖移动网络数据流量。此外，通过上述方式登录，可以使得用户在较短时间（如 1~2 秒内）完成免密登录，用户体验较好。此外，在某些步骤中，UE 与运营商 IMS 网络之间可通过认证和密钥协商（authentication and key agreement, AKA）鉴权认证，安全性高。

20 图 7 是本申请实施例提供的一种通信方法 700 的示意性流程图。该方法 700 可以用于实现上述方法 300 或方法 500 的方案。在该方法 700 中，核心网设备可包括 AMF 网元。该方法 700 可以包括如下步骤。

701，调制解调器（Modem）向 AMF 网元发送 NAS 注册（register）请求。

25 其中，Modem 为 UE 中的 Modem。Modem 可以安装于（或者装载于）UE 基带芯片中。

在步骤 701 中，UE 中的 Modem 向运营商网络发起 NAS 注册请求，该请求经过路由之后到达 AMF 网元。可选地，该 NAS 注册请求还可包括指示信息，该指示信息用于指示 AMF 网元向用户设备提供目标 token。

702，AMF 网元从 UDM 网元获取签约数据。

30 AMF 网元收到 UE 的 NAS 注册请求后，可以向 UDM 网元发起注册，并获取该 UE 的签约数据。

其中，该签约数据包括目标 MSISDN。

703，AMF 网元向 Modem 返回 NAS 注册响应。

35 该 NAS 注册响应，可以认为是步骤 701 中 NAS 注册请求的响应。作为示例，该 NAS 注册响应为注册接受（registration accept）响应。可选地，若步骤 701 中的 NAS 注册请求还可包括指示信息，该指示信息用于指示 AMF 网元向用户设备提供目标 token；则步骤 703 中，AMF 网元向 IMS 客户端发送的 NAS 注册响应还可以包含目标 token。为便于说明，方法 700 中主要介绍步骤 701 中的 NAS 注册请求不包括上述指示信息的情况，即用户设备通过步骤 709 中的 NAS 请求消息来请求目标 token 为例进行示例性说明。

其中, 该 NAS 注册响应中包括目标 MSISDN 或者目标 MSISDN 掩码。如前所述, MSISDN 为手机号码, MSISDN 掩码是指隐藏了部分数字的手机号码。其中, 目标 MSISDN 或者目标 MSISDN 掩码的数量可以是一个, 也可以是多个。举例来说, 若 UE 支持双卡双待, 且有双卡, 则该目标 MSISDN 可以有 2 个, 或者则该目标 MSISDN 掩码可以有 2 个。

5 作为一种可能的情形, 该 NAS 注册响应的形式如下。

```
registrationAccept
  nGS-registration-result
    spare: 0x0
    sms-allowed-flag: sms-over-NAS-not-allowed
10    ngs-registration-result-value: the-3GPP-access
    ng-GUTI
      ...
    tai-list
      ...
15    ...
    am-data
      msisdn-mask: 186****5678 //目标 MSISDN 掩码
```

在上述示例中, 该 NAS 注册响应可包括目标 MSISDN 掩码, 且目标 MSISDN 掩码为 186****5678。

20 作为另一种可能的情形, 该 NAS 注册响应的形式如下。

```
registrationAccept
  nGS-registration-result
    spare: 0x0
    sms-allowed-flag: sms-over-NAS-not-allowed
25    ngs-registration-result-value: the-3GPP-access
    ng-GUTI
      ...
    tai-list
      ...
30    ...
    am-data
      msisdn: 18612345678 //目标 MSISDN
```

在上述示例中, 可以在 NAS 注册响应中包括目标 MSISDN, 即 18612345678, 用户设备收到该目标 MSISDN 后可生成目标 MSISDN 掩码。

35 704, Modem 获取目标 MSISDN 掩码。

可选地, Modem 保存该目标 MSISDN 掩码。

举例来说, Modem 基于 NAS 注册响应获取目标 MSISDN 掩码, 并保存该目标 MSISDN 掩码。该目标 MSISDN 掩码, 可用于在授权页面呈现 (如步骤 707), 具体地, 后面结合步骤 707 详细说明。

可选地, Modem 可以基于以下任一方式获取目标 MSISDN 掩码。

一种可能的方式, Modem 基于目标 MSISDN, 生成目标 MSISDN 掩码。

具体地, 若步骤 703 中 AMF 网元向 Modem 发送的 NAS 注册响应中包括目标 MSISDN, 则 Modem 可根据目标 MSISDN 生成目标 MSISDN 掩码。

5 另一种可能的方式, Modem 直接获取目标 MSISDN 掩码。

具体地, 若步骤 703 中 AMF 网元向 Modem 发送的 NAS 注册响应中包括目标 MSISDN 掩码, 则 Modem 可直接获取目标 MSISDN 掩码。其中, NAS 注册响应中包括目标 MSISDN 掩码。

705, 用户设备呈现登录页面。

10 UE 中的 APP 客户端呈现登录页面。

706, APP 客户端从 Modem 获取目标 MSISDN 掩码。

在步骤 704 中, UE 中的 Modem 保存目标 MSISDN 掩码, 因此, APP 客户端可从 Modem 获取目标 MSISDN 掩码。举例来说, UE 操作系统可通过调用 Modem 接口, 获取 MSISDN 掩码; 进一步地, APP 客户端通过调用该 UE 操作系统开放的接口, 获取 MSISDN 掩码。

15 707, UE 中的 APP 客户端呈现授权页面, 该授权页面上显示目标 MSISDN 掩码。

关于授权页面的来源可以有很多实现方式, 对此不予限制。下面简单列举两种可能的方式。

一种可能的方式, APP 客户端集成了运营商的 SDK, SDK 提供基础的授权页面, APP 客户端基于该基础的授权页面进行修改 (或者调整), 进而得到最终呈现的授权页面。

20 另一种可能的方式, UE 操作系统从 Modem 获取基础的授权页面给 APP 客户端, APP 客户端基于该基础的授权页面进行修改 (或者调整), 进而得到最终呈现的授权页面。

其中, 步骤 707 与步骤 608 相似, 此处不再赘述。

708, APP 客户端确定用户授权。

步骤 708 与步骤 609 相似, 此处不再赘述。

25 709, APP 客户端通过 Modem 向 AMF 网元发送 NAS 请求消息。

该 NAS 请求消息用于请求目标 token。可选地, 该 NAS 请求消息用于指示 AMF 网元向用户设备提供目标 token。例如, 该 NAS 请求消息本身可用于触发 AMF 网元向用户设备提供目标 token; 再例如, 该 NAS 请求消息包括指示信息, 该指示信息用于指示 AMF 网元向用户设备提供目标 token。

30 举例来说, APP 客户端可调用 UE 操作系统开放的接口, 请求目标 token; 进一步地, UE 操作系统可调用 Modem 接口去请求目标 token, 即 Modem 向 AMF 网元发送 NAS 请求消息, 该 NAS 请求消息用于请求目标 token。

其中, NAS 请求消息的形式例如可以为上行 NAS 传输 (UL NAS transport) 请求。

作为示例, NAS 请求消息的一种可能形式如下。

35 loginTokenRequest

...

ng-guti

type-of-identity: ng-guti

...

5 ng-guti-body
 mcc-mnc: 0x64f030
 amf-region-id: 0x0
 amf-set-id-h: 0x0
 amf-pointer: 0x1
 amf-set-id-l: 0x0
 ng-tmsi: 0x79

...

710, AMF 网元分配目标 token。

10 AMF 网元可先确定目标 MSISDN, 进而生成目标 token, 再将目标 token 分配给目标 MSISDN, 如此完成目标 token 的分配操作。举例来说, AMF 网元根据 NAS 请求消息中的信息确定用户, 进而可以确定该用户的目标 MSISDN, 并分配 token。其中, AMF 网元确定用户的方式很多, 不予限制。例如, AMF 网元可以根据 NAS 请求消息中的全球临时 UE 标识 (globally unique temporary UE identity, GUTI) 识别用户, 如上述 NAS 请求消息

15 中的 ng-guti-body 确定用户。

一种可能的情形, AMF 网元保存 (或者维护) 目标 token 与目标 MSISDN 之间的对应关系, 如以表 1 的形式保存。

另一种可能的情形, AMF 网元可以向其他网元 (如 UDM 网元发送目标 token 与目标 MSISDN 之间的对应关系, 该其他网元保存该对应关系, 如以表 1 的形式保存。

20 711, AMF 网元通过 Modem 向 APP 客户端发送目标 token。

可选地, AMF 网元通过 Modem 向 APP 客户端发送目标 token 的认证地址。其中, 目标 token 和目标 token 的认证地址可以携带于同一信令中, 也可以携带于不同信令中, 不予限制。

举例来说, AMF 网元向 Modem 返回 NAS 响应消息, 该 NAS 响应消息包括目标 token 和目标 token 的认证地址; UE 操作系统将 Modem 获取到的目标 token 和目标 token 的认证地址, 返回给 APP 客户端。其中, NAS 响应消息例如可以为下行 NAS 传输 (DL NAS transport) 响应。

作为示例, NAS 响应消息的一种可能形式如下。

loginTokenResponse
30 ...
 login-token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjpbeyJ0b29sdHQiOiJodHRwczovL3Rvb2x0dC5jb20ifV0sImIhdCI6MTY0ODA4NTQ2NSwiZXhwIjoxNjQ4MTM3NTk5LCJhdWQiOiJBbGJZSIsImIzcyI6InRlc3QiLCJzdWIiOiJsb2dpbiJ9.LrLUGSaNcepmq0EfPpLxN_o3cJQm3D_oV_11t_DTmQ //登录信息
35 token-auth-addr: https://test.xxx.com/verification //认证地址
 ...

可以理解, 上述 “login-token” 字段中携带的登录信息, 可以是经过编码后的信息。举例来说, AMF 网元对以下至少一项信息采用 base64 编码方式编码: 用户设备的信息、

用户设备对应的用户的信息、目标 token 的认证地址、目标 token 的适用范围、目标 token 的有效期、目标 token 的验证信息、目标 token 的有效期，编码后的目标 token 如上述示例。可以理解，关于是否编码，以及编码时采用何种编码方式，本申请实施例不予限制。

5 作为示例，上述步骤 701-711 可以认为是登录前的准备，下面步骤 712-718 可以认为是登录以及登录的认证。

712，APP 客户端向应用服务器发送登录请求消息。

其中，该登录请求消息中包括目标 token。可选地，该登录请求消息中还包括目标 token 的认证地址。

713，应用服务器向 NEF 网元发送登录认证消息。

10 步骤 713 与步骤 614 类似，此处不再赘述。

714，NEF 网元向 AMF 网元转发登录认证消息。

可选地，NEF 网元向 AMF 网元转发登录认证消息，包括：若 NEF 网元成功认证登录认证消息，则 NEF 网元向 AMF 网元转发登录认证消息。

15 举例来说，应用服务器向 NEF 网元发送的登录认证消息包括目标 token 和 APP ID，且该登录认证消息使用 APP key 进行加密；NEF 网元使用与 APP ID 相对应的 APP key 校验该登录认证消息；在校验成功后，NEF 网元向 AMF 网元转发该登录认证消息。

715，AMF 网元基于目标 token，查找目标 MSISDN。

一种可能的情形，若 AMF 网元本地保存目标 token 与目标 MSISDN 之间的对应关系，则 AMF 网元基于该对应关系查找该目标 token 对应的目标 MSISDN。以表 1 为例，若登
20 录认证消息中包括的目标 token 为 token#2，则 AMF 网元确定该目标 token 对应的目标 MSISDN 为 MSISDN#2。

另一种可能的情形，若其他网元（如 UDM 网元保存目标 token 与目标 MSISDN 之间的对应关系，则 AMF 网元可以向其他网元请求该目标 token 对应的目标 MSISDN。

25 可选地，AMF 网元基于目标 token，查找目标 MSISDN，包括：若 AMF 网元成功认证目标 token（或者 AMF 网元对目标 token 校验通过），则 AMF 网元基于目标 token，查找目标 MSISDN。

AMF 网元认证（或者校验）目标 token，即表示 AMF 网元校验目标 token 的有效性。作为示例，AMF 网元校验目标 token，例如可以包括以下至少一项：AMF 网元校验目标 token 是否已过期、AMF 网元校验是否是自己校验该目标 token。例如，若目标 token 未过
30 期，则可认为校验通过；若目标 token 过期，则可认为校验未通过。再例如，若 AMF 网元确定自己校验该目标 token，则可认为校验通过；若 AMF 网元确定自己无权校验该目标 token，则可认为校验未通过。例如，以步骤 711 中的示例为例，若 AMF 网元收到目标 token（即登录信息）后，可以先进行解码，获得该目标 token 中的上述至少一项信息，进而再对上述至少一项信息进行校验。再例如，AMF 网元收到携带数字签名的目标 token（即登
35 录信息）后，可以先基于 AMF 网元的密钥验证该数字签名，若验证通过，则可进行解码，获得该目标 token 中的上述至少一项信息，然后对上述至少一项信息进行校验。具体可以方法 300 中的相关描述，此处不再赘述。

716，AMF 网元向 NEF 网元发送目标 MSISDN。

举例来说，AMF 网元查找到目标 MSISDN 后，向 NEF 网元发送登录认证消息的响应，

该响应携带目标 MSISDN。

717, NEF 网元向应用服务器发送目标 MSISDN。

举例来说, NEF 网元从 AMF 网元接收到登录认证消息的响应后, 向应用服务器转发该登录认证消息的响应。

5 718, 应用服务器通知 APP 客户端登录成功。

经过上述步骤, 用户可实现免密登录。

可选地, AMF 网元对目标 token 进行处理。作为示例, AMF 网元可对目标 token 进行以下至少一项处理: AMF 网元记录 APP ID 使用目标 token 成功获取目标 MSISDN 的次数 (如用于计费)、AMF 网元将目标 token 标记为失效。

10 可以理解, 图 7 所示实施例主要以通过 NAS 请求消息请求目标 token 为例进行示例性说明, 对此不予限制。例如, 用户设备也可以通过 NAS 注册请求获取目标 token, AMF 网元向 IMS 客户端发送的 NAS 注册响应中携带该目标 token。

上文结合图 7 所示的步骤 701- 718 示例地介绍了通过 UE 与核心网之间的 NAS 信令来完成登录的场景。基于上述实施例, 借助核心网, 通过 NAS 信令可实现免密登录, 可支持更多场景下的免密登录, 且不依赖移动网络数据流量。此外, 通过上述方式登录, 可以使得用户在较短时间 (如 1~2 秒内) 完成免密登录, 用户体验较好。此外, 在某些步骤中, UE 与核心网之间可通过 AKA 鉴权认证, 安全性高。

可以理解, 本申请实施例中的图 6 至图 7 中的例子仅仅是为了便于本领域技术人员理解本申请实施例, 并非要将本申请实施例限于例示的具体场景。本领域技术人员根据图 6 至图 7 的例子, 显然可以进行各种等价的修改或变化, 这样的修改或变化也落入本申请实施例的范围内。例如, 上述图 6 至图 7 中的网元或设备, 可以更换为其他可以执行上述功能的网元或设备。再例如, 若方法 600 中通过 SIP 注册请求消息请求目标 token, 则步骤 601 中的该 SIP 注册请求还可包括指示信息, 该指示信息用于指示 S-CSCF 设备向用户设备提供目标 token; S-CSCF 设备收到该 SIP 注册请求后, 基于该 SIP 注册请求中的指示信息分配目标 token (如参考步骤 611); 步骤 604 中, S-CSCF 设备向 IMS 客户端发送的 SIP 注册响应还可以包含目标 token, 此时方法 600 可以不包括步骤 610 和 612。再例如, 若方法 700 中通过 NAS 注册请求消息请求目标 token, 则步骤 701 中的该 NAS 注册请求还可包括指示信息, 该指示信息用于指示 AMF 网元向用户设备提供目标 token; AMF 网元收到该 NAS 注册请求后, 基于该 NAS 注册请求中的指示信息分配目标 token (如参考步骤 710); 步骤 703 中, AMF 网元向 Modem 发送的 NAS 注册响应还可以包含目标 token, 此时方法 700 可以不包括步骤 709 和 711。

还可以理解, 上述图 6 至图 7 中各个步骤仅是示例性说明, 对此不作严格限定。此外, 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。

35 还可以理解, 在上述一些实施例中, 主要以显示标识和验证标识为用户的通信号码为例进行示例性说明, 对此不予限制。例如, 验证标识可以替换为任何能够识别用户的其它标识。再例如, 显示标识可以替换为用户的昵称等。此外, 验证标识可以替换为第三标识。显示标识可以替换为第一标识或第二标识。

还可以理解, 在上述一些实施例中, 主要以 IMS 客户端或 Modem 为例进行示例性说

明，IMS 客户端或 Modem 也可以替换为移动操作系统（mobile OS）。

还可以理解，在本申请的各实施例中涉及到一些消息名称，其命名不对本申请实施例的保护范围造成限定。

还可以理解，在上述一些实施例中提到了消息（如 SIP 消息或 NAS 消息）的可能的形式，可以理解，上述仅为示例性说明，对此不予限制。任何属于上述消息的变形，都适用于本申请实施例。

还可以理解，本申请的各实施例中的一些可选的特征，在某些场景下，可以不依赖于其他特征，也可以在某些场景下，与其他特征进行结合，不作限定。

还可以理解，在本申请的各实施例中的各种数字序号的大小并不意味着执行顺序的先后，仅为描述方便进行的区分，不应对本申请实施例的实施过程构成任何限定。

还可以理解，上述各个方法实施例中，由设备实现的方法和操作，也可以由可由设备的组成部件（例如芯片或者电路）来实现，不作限定。

相应于上述各方法实施例给出的方法，本申请实施例还提供了相应的装置，所述装置包括用于执行上述各个方法实施例相应的模块。该模块可以是软件，也可以是硬件，或者是软件和硬件结合。可以理解的是，上述各方法实施例所描述的技术特征同样适用于以下装置实施例。

图 8 是本申请实施例提供的一种通信装置 800 的示意图。该装置 800 包括收发单元 810 和处理单元 820。收发单元 810 可以用于实现相应的通信功能。收发单元 810 还可以称为通信接口或通信单元。处理单元 820 可以用于进行处理操作，如分配 token，验证 token 等。

可选地，该装置 800 还包括存储单元，该存储单元可以用于存储指令和/或数据，处理单元 820 可以读取存储单元中的指令和/或数据，以使得装置实现前述各个方法实施例中核心网设备或用户设备的动作。

在第一种设计中，该装置 800 可以是前述实施例中的用户设备，也可以是用户设备的组成部件（如芯片）。该装置 800 可实现对应于上文方法实施例中的用户设备执行的步骤或者流程。其中，收发单元 810 可用于执行上文方法实施例中用户设备的收发相关的操作（如发送和/或接收数据或消息的操作），例如，收发单元 810 可用于执行图 3 中的步骤 301 中向核心网设备发送第一免流量消息的操作、步骤 302 中接收来自核心网设备的第二免流量消息的操作、步骤 303 中向应用服务器发送登录信息的操作，还可以用于执行图 4 中的步骤 401 中向呼叫会话控制功能设备发送 SIP 请求消息的操作、步骤 402 中接收来自呼叫会话控制功能设备的 SIP 请求消息的响应的操作、步骤 403 中向应用服务器发送登录请求消息的操作，还可以用于执行图 5 中的步骤 501 中向接入管理网元发送 NAS 请求消息的操作、步骤 502 中接收来自接入管理网元的 NAS 请求消息的响应的操作、步骤 503 中向应用服务器发送登录请求消息的操作，还可以用于执行图 6 以及图 7 中 UE 中的发送和/或接收数据或消息的操作。处理单元 820 可用于执行上文方法实施例中用户设备的处理相关的操作，或者除收发之外的操作（如发送和/或接收数据或消息之外的操作），例如，处理单元 820 可用于生成第一免流量消息。再例如，处理单元 820 可用于执行图 6 中的步骤 606 至 609 中的操作、执行图 7 中的步骤 705 至 708 中的操作。

一种可能的实现方式，收发单元 810，用于向核心网设备发送第一免流量消息，第一

免流量消息用于触发核心网设备向用户设备发送第二免流量消息；收发单元 810，还用于从核心网设备接收第二免流量消息，第二免流量消息包括登录信息，登录信息为用户设备登录到应用服务器所需要的信息；收发单元 810，还用于向应用服务器发送登录信息，以登录到应用服务器；其中，第一免流量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息。可选地，处理单元 820 用于处理第二免流量消息，获取登录信息。可选地，处理单元 820 用于生成第一免流量消息。

示例地，第一免流量消息指示核心网设备向用户设备提供登录信息。

可选地，处理单元 820 用于获取并显示第一标识信息；或者，用户设备获取并显示第二标识信息；其中，第一标识信息标识用户设备对应的用户，第二标识信息为第一标识信息经脱敏处理得到的结果。

可选地，处理单元 820 具体用于从核心网设备发送的消息中获取第一标识信息；或者，从核心网设备发送的消息中获取第二标识信息；或者，从核心网设备发送的消息中获取第一标识信息，并对第一标识信息进行脱敏处理得到第二标识信息。

可选地，处理单元 820 具体用于从第二免流量消息获取第一标识信息；或者，从第二免流量消息获取第二标识信息。

可选地，收发单元 810，还用于接收来自核心网设备的第三免流量消息，其中，第三免流量消息为通过基站传输且不产生待计费流量的消息，则：处理单元 820 具体用于从第三免流量消息获取第一标识信息；或者，从第三免流量消息获取第二标识信息。

示例地，通过基站传输且不产生待计费流量的消息是：经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。

示例地，经过基站及用户面数据网关传输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。

示例地，第一免流量消息为 SIP 查询消息，第二免流量消息为 SIP 查询响应消息；或者，第一免流量消息为 SIP 注册消息，第二免流量消息为 SIP 注册响应消息。

示例地，核心网设备为呼叫会话控制功能设备。

示例地，通过基站传输且不产生待计费流量的消息是：经过基站且不经过用户面数据网关传输的控制面消息。

示例地，经过基站且不经过用户面数据网关传输的控制面消息是非接入层 NAS 消息。

示例地，第一免流量消息为 NAS 注册消息，第二免流量消息为 NAS 注册接受消息。

示例地，核心网设备为接入管理网元。

示例地，第二免流量消息还包括登录信息的认证地址。

示例地，登录信息包括核心网设备对以下至少一项信息进行加密或签名的结果：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的有效期。

在第二种设计中，该装置 800 可以是前述实施例中的核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的 S-CSCF 设备，图 7 中的 AMF 网元），也可以是核心网设备的组成部件（如芯片）。该装置 800 可对应于上文方法实施例中的核心网设备执行的步骤或者流程。其中，收发单元 810 可用于执行上文方法实施例中核心网设备的收发相关的操作（如发送和/或接收数据或消息的操

作), 例如, 收发单元 810 可用于执行图 3 中的步骤 301 中接收来自用户设备的第一免流量消息的操作、步骤 302 中向用户设备发送第二免流量消息的操作、步骤 304 中接收来自应用服务器的登录信息的操作, 还可以用于执行图 4 中的步骤 401 中接收来自用户设备的 SIP 请求消息的操作、步骤 402 中向用户设备发送 SIP 请求消息的响应的操作、步骤 404 中接收来自应用服务器的登录信息的操作, 图 5 中的步骤 501 中接收来自用户设备的 NAS 请求消息的操作、步骤 502 中向用户设备发送 NAS 请求消息的响应的操作、步骤 504 中接收来自应用服务器的登录信息的操作, 还可以用于执行图 6 中的 S-CSCF 设备发送和/或接收数据或消息的操作, 还可以用于执行图 7 中的 AMF 网元发送和/或接收数据或消息的操作。处理单元 820 可用于执行上文方法实施例中核心网设备的数据和/或信息处理相关的操作, 或者除收发之外的操作 (如发送和/或接收数据或消息之外的操作), 例如, 处理单元 820 可用于执行图 6 中的步骤 611 和步骤 616 的操作, 还可以用于执行图 7 中的步骤 710 和步骤 715 的操作。

一种可能的实现方式, 收发单元 810, 用于接收来自用户设备的第一免流量消息, 第一免流量消息用于触发核心网设备向用户设备发送第二免流量消息; 处理单元 820, 用于生成登录信息, 登录信息为用户设备登录到应用服务器所需要的信息; 收发单元 810, 还用于向用户设备发送第二免流量消息, 第二免流量消息包括登录信息; 其中, 第一免流量消息和第二免流量消息均为通过基站传输且不产生待计费流量的消息。

示例地, 第一免流量消息指示核心网设备向用户设备提供登录信息。

可选地, 收发单元 810, 还用于向用户设备发送第一标识信息或第二标识信息; 其中, 第一标识信息标识用户设备对应的用户, 第二标识信息为第一标识信息经脱敏处理得到的结果。

可选地, 处理单元 820, 还用于对第一标识信息进行脱敏处理得到第二标识信息; 收发单元 810, 用于向用户设备发送第二标识信息。

示例地, 第二免流量消息包括第一标识信息或第二标识信息。

可选地, 收发单元 810, 具体用于向用户设备发送第三免流量消息, 第三免流量消息包括第一标识信息或第二标识信息; 其中, 第三免流量消息为通过基站传输且不产生待计费流量的消息。

示例地, 通过基站传输且不产生待计费流量的消息是: 经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。

示例地, 经过基站及用户面数据网关传输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。

示例地, 第一免流量消息为 SIP 查询消息, 第二免流量消息为 SIP 查询响应消息; 或者, 第一免流量消息为 SIP 注册消息, 第二免流量消息为 SIP 注册响应消息。其中, SIP 查询消息例如可以为 SIP OPTIONS 消息。

示例地, 核心网设备为呼叫会话控制功能设备。

示例地, 通过基站传输且不产生待计费流量的消息是: 经过基站且不过用户面数据网关传输的控制面消息。

示例地, 经过基站且不过用户面数据网关传输的控制面消息是非接入层 NAS 消息。

示例地, 第一免流量消息为 NAS 注册消息, 第二免流量消息为 NAS 注册接受消息。

示例地，核心网设备为接入管理网元。

示例地，第二免流量消息还包括登录信息的认证地址。

5 可选地，收发单元 810，还用于接收来自应用服务器的登录认证消息，登录认证消息包括登录信息；向应用服务器发送用户的第三标识信息，用户的第三标识信息是基于登录信息确定的。

可选地，收发单元 810，具体用于若核心网设备成功认证登录信息，则向应用服务器发送用户的第三标识信息。

可选地，处理单元 820，还用于基于登录信息和对应关系，确定用户的第三标识信息，对应关系包括用户的第三标识信息与登录信息之间的对应关系。

10 示例地，登录信息包括核心网设备对以下至少一项信息进行加密或签名的结果：用户设备的信息、用户设备对应的用户的信息、登录信息的认证地址、登录信息的适用范围、登录信息的有效期。

可以理解，各单元执行上述相应步骤的具体过程在上述各方法实施例中已经详细说明，为了简洁，在此不再赘述。

15 还可以理解，这里的装置 800 以功能单元的形式体现。这里的术语“单元”可以指应用特有集成电路（application specific integrated circuit, ASIC）、电子电路、用于执行一个或多个软件或固件程序的处理器（例如共享处理器、专有处理器或组处理器等）和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。在一个可选例子中，本领域技术人员可以理解，装置 800 可以具体为上述实施例中的用户设备，可以用于执行上述各方法
20 实施例中与用户设备对应的各个流程和/或步骤，例如，图 3 中的步骤 301-303，图 4 中的步骤 401-403，图 5 中的步骤 501-503，图 6 中的步骤 601、604、605-610、612、613、619，图 7 中的步骤 701、703、704-709、711、712、718；或者，装置 800 可以具体为上述实施例中的呼叫会话控制功能设备，可以用于执行上述各方法实施例中与核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的
25 S-CSCF 设备，图 7 中的 AMF 网元）对应的各个流程和/或步骤，例如，图 3 中的步骤 301-302、304，图 4 中的步骤 401-402、404，图 5 中的步骤 501-502、504，图 6 中的步骤 601-604、610-612、615-617、图 7 中的步骤 701-703、709-711、714-716。为避免重复，在此不再赘述。

上述各个方案的装置 800 具有实现上述方法中用户设备所执行的相应步骤的功能，或者，
30 上述各个方案的装置 800 具有实现上述方法中核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的 S-CSCF 设备，图 7 中的 AMF 网元）所执行的相应步骤的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块；例如收发单元可以由收发机替代（例如，收发单元中的发送单元可以由发送机替代，收发单元
35 中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

此外，上述收发单元 810 还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。

需要指出的是，图 8 中的装置可以是前述实施例中的设备，也可以是芯片或者芯片系统，例如：片上系统（system on chip, SoC）。其中，收发单元可以是输入输出电路、通信接口；处理单元为该芯片上集成的处理器或者微处理器或者集成电路。在此不做限定。

图 9 是本申请实施例提供另一种通信装置 900 的示意图。该装置 900 包括处理器 910，
5 处理器 910 用于执行存储器 920 存储的计算机程序或指令，或读取存储器 920 存储的数据，以执行上文各方法实施例中的方法。可选地，处理器 910 为一个或多个。

可选地，如图 9 所示，该装置 900 还包括存储器 920，存储器 920 用于存储计算机程序或指令和/或数据。该存储器 920 可以与处理器 910 集成在一起，或者也可以分离设置。可选地，存储器 920 为一个或多个。

10 可选地，如图 9 所示，该装置 900 还包括收发器 930，收发器 930 用于信号的接收和/或发送。例如，处理器 910 用于控制收发器 930 进行信号的接收和/或发送。

作为一种方案，该装置 900 用于实现上文各个方法实施例中由用户设备执行的操作。

作为另一种方案，该装置 900 用于实现上文各个方法实施例中由核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的
15 S-CSCF 设备，图 7 中的 AMF 网元）执行的操作。

可以理解，本申请实施例中提及的处理器可以是中央处理单元（central processing unit, CPU），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。
20

还可以理解，本申请实施例中提及的存储器可以是易失性存储器和/或非易失性存储器。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）。例如，RAM 可以用作外部高速缓存。作为示例而非限定，RAM 包括如下多种形式：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（synchlink DRAM, SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM, DR RAM）。
25
30

需要说明的是，当处理器为通用处理器、DSP、ASIC、FPGA 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件时，存储器（存储模块）可以集成在处理器中。
35

还需要说明的是，本文描述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。

本申请实施例还提供一种计算机可读存储介质，其上存储有用于实现上述各方法实施例中由用户设备或核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，

图 5 中的接入管理网元，图 6 中的 S-CSCF 设备，图 7 中的 AMF 网元）执行的方法的计算机指令。

本申请实施例还提供一种计算机程序产品，包含指令，该指令被计算机执行时以实现上述各方法实施例中由用户设备或核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的 S-CSCF 设备，图 7 中的 AMF 网元）执行的方法。

本申请实施例还提供一种通信系统，包括前述的用户设备和核心网设备（如图 3 中的核心网设备，图 4 中的呼叫会话控制功能设备，图 5 中的接入管理网元，图 6 中的 S-CSCF 设备，图 7 中的 AMF 网元）。

上述提供的任一种装置中相关内容的解释及有益效果均可参考上文提供的对应的方法实施例，此处不再赘述。

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。此外，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。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。例如，所述计算机可以是个人计算机，服务器，或者网络设备等。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包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，DVD）、或者半导体介质（例如固态硬盘（solid state disk, SSD）等。例如，前述的可用介质包括但不限于：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，包括：
 用户设备向核心网设备发送第一免流量消息，所述第一免流量消息用于触发所述核心网设备向所述用户设备发送第二免流量消息；
 所述用户设备从所述核心网设备接收所述第二免流量消息，所述第二免流量消息包括登录信息，所述登录信息为所述用户设备登录到应用服务器所需要的信息；
 所述用户设备向所述应用服务器发送所述登录信息，以登录到所述应用服务器；
 其中，所述第一免流量消息和所述第二免流量消息均为通过基站传输且不产生待计费流量的消息。
2. 根据权利要求1所述的方法，其特征在于，所述第一免流量消息指示所述核心网设备向所述用户设备提供所述登录信息。
3. 根据权利要求1或2所述的方法，其特征在于，所述方法还包括：
 所述用户设备获取并显示第一标识信息；或者，
 所述用户设备获取并显示第二标识信息；
 其中，所述第一标识信息标识所述用户设备对应的用户，所述第二标识信息为所述第一标识信息经脱敏处理得到的结果。
4. 根据权利要求3所述的方法，其特征在于：
 所述用户设备获取所述第一标识信息，包括：所述用户设备从所述核心网设备发送的消息中获取所述第一标识信息；或者，
 所述用户设备获取所述第二标识信息，包括以下任一项：所述用户设备从所述核心网设备发送的消息中获取所述第二标识信息；或者，所述用户设备从所述核心网设备发送的消息中获取所述第一标识信息，并对所述第一标识信息进行脱敏处理得到所述第二标识信息。
5. 根据权利要求4所述的方法，其特征在于，所述方法还包括：
 所述用户设备接收来自所述核心网设备的第三免流量消息，其中，所述第三免流量消息为通过基站传输且不产生待计费流量的消息，则：
 所述用户设备从所述核心网设备发送的消息中获取所述第一标识信息，包括：所述用户设备从所述第三免流量消息获取所述第一标识信息；或者，所述用户设备从所述核心网设备发送的消息中获取所述第二标识信息，包括：所述用户设备从所述第三免流量消息获取所述第二标识信息。
6. 根据权利要求1至5中任一项所述的方法，其特征在于，
 所述通过基站传输且不产生待计费流量的消息是：经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。
7. 根据权利要求6所述的方法，其特征在于，所述经过基站及用户面数据网关传输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。
8. 根据权利要求7所述的方法，其特征在于，
 所述第一免流量消息为 SIP 查询消息，所述第二免流量消息为 SIP 查询响应消息；或

者，

所述第一免流量消息为 SIP 注册消息，所述第二免流量消息为 SIP 注册响应消息。

9. 根据权利要求 6 至 8 中任一项所述的方法，其特征在于，所述核心网设备为呼叫会话控制功能设备。

5 10. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于，

所述通过所述基站传输且不产生待计费流量的消息是：经过基站且不经过用户面数据网关传输的控制面消息。

11. 根据权利要求 10 所述的方法，其特征在于，所述经过基站且不经过用户面数据网关传输的控制面消息是非接入层 NAS 消息。

10 12. 根据权利要求 11 所述的方法，其特征在于，

所述第一免流量消息为 NAS 注册消息，所述第二免流量消息为所述 NAS 注册接受消息。

13. 根据权利要求 10 至 12 中任一项所述的方法，其特征在于，所述核心网设备为接入管理网元。

15 14. 根据权利要求 1 至 13 中任一项所述的方法，其特征在于，所述第二免流量消息还包括所述登录信息的认证地址。

15. 根据权利要求 1 至 14 中任一项所述的方法，其特征在于，所述登录信息包括所述核心网设备对以下至少一项信息进行加密或签名的结果：所述用户设备的信息、所述用户设备对应的用户的信息、所述登录信息的认证地址、所述登录信息的适用范围、所述登录信息的有效期。

20 16. 一种通信方法，其特征在于，包括：

核心网设备接收来自用户设备的第一免流量消息，所述第一免流量消息用于触发所述核心网设备向所述用户设备发送第二免流量消息；

25 所述核心网设备生成登录信息，所述登录信息为所述用户设备登录到应用服务器所需要的信息；

所述核心网设备向所述用户设备发送所述第二免流量消息，所述第二免流量消息包括所述登录信息；

其中，所述第一免流量消息和所述第二免流量消息均为通过基站传输且不产生待计费流量的消息。

30 17. 根据权利要求 16 所述的方法，其特征在于，所述第一免流量消息指示所述核心网设备向所述用户设备提供所述登录信息。

18. 根据权利要求 17 所述的方法，其特征在于，所述方法还包括：

所述核心网设备向所述用户设备发送第一标识信息或第二标识信息；

35 其中，所述第一标识信息标识所述用户设备对应的用户，所述第二标识信息为所述第一标识信息经脱敏处理得到的结果。

19. 根据权利要求 18 所述的方法，其特征在于，所述核心网设备向所述用户设备发送所述第二标识信息，包括：

所述核心网设备对所述第一标识信息进行脱敏处理得到所述第二标识信息，并向所述用户设备发送所述第二标识信息。

20. 根据权利要求 19 所述的方法, 其特征在于, 所述核心网设备向所述用户设备发送第一标识信息或第二标识信息, 包括:
- 所述核心网设备向所述用户设备发送第三免流量消息, 所述第三免流量消息包括所述第一标识信息或所述第二标识信息;
- 5 其中, 所述第三免流量消息为通过基站传输且不产生待计费流量的消息。
21. 根据权利要求 16 至 20 中任一项所述的方法, 其特征在于,
- 所述通过基站传输且不产生待计费流量的消息是: 经过基站及用户面数据网关传输且不产生待计费流量的用户面消息。
22. 根据权利要求 21 所述的方法, 其特征在于, 所述经过基站及用户面数据网关传
- 10 输且不产生待计费流量的用户面消息是会话初始协议 SIP 消息。
23. 根据权利要求 22 所述的方法, 其特征在于,
- 所述第一免流量消息为 SIP 查询消息, 所述第二免流量消息为 SIP 查询响应消息; 或者,
- 所述第一免流量消息为 SIP 注册消息, 所述第二免流量消息为 SIP 注册响应消息。
- 15 24. 根据权利要求 21 至 23 中任一项所述的方法, 其特征在于, 所述核心网设备为呼叫会话控制功能设备。
25. 根据权利要求 16 至 20 中任一项所述的方法, 其特征在于,
- 所述通过基站传输且不产生待计费流量的消息是: 经过基站且不经用户面数据网关传输的控制面消息。
- 20 26. 根据权利要求 25 所述的方法, 其特征在于, 所述经过基站且不经用户面数据网关传输的控制面消息是非接入层 NAS 消息。
27. 根据权利要求 26 所述的方法, 其特征在于,
- 所述第一免流量消息为 NAS 注册消息, 所述第二免流量消息为所述 NAS 注册接受消息。
- 25 28. 根据权利要求 25 至 27 中任一项所述的方法, 其特征在于, 所述核心网设备为接入管理网元。
29. 根据权利要求 16 至 28 中任一项所述的方法, 其特征在于, 所述第二免流量消息还包括所述登录信息的认证地址。
30. 根据权利要求 16 至 29 中任一项所述的方法, 其特征在于, 所述方法还包括:
- 30 所述核心网设备接收来自所述应用服务器的登录认证消息, 所述登录认证消息包括所述登录信息;
- 所述核心网设备向所述应用服务器发送所述用户的第三标识信息, 所述用户的第三标识信息是基于所述登录信息确定的。
31. 根据权利要求 30 所述的方法, 其特征在于, 所述核心网设备向所述应用服务器
- 35 发送所述用户的第三标识信息, 包括:
- 若所述核心网设备成功认证所述登录信息, 则所述核心网设备向所述应用服务器发送所述用户的第三标识信息。
32. 根据权利要求 30 或 31 所述的方法, 其特征在于, 所述方法还包括:
- 所述核心网设备基于所述登录信息和对应关系, 确定所述用户的第三标识信息, 所述

对应关系包括所述用户的第三标识信息与所述登录信息之间的对应关系。

33. 根据权利要求 16 至 31 中任一项所述的方法，其特征在于，所述登录信息包括所述核心网设备对以下至少一项信息进行加密或签名的结果：所述用户设备的信息、所述用户设备对应的用户的信息、能够验证所述登录信息的设备的信息、所述登录信息的适用范围、所述登录信息的有效期。

34. 一种通信方法，其特征在于，包括：

用户设备向核心网设备发送第一免流量消息，所述第一免流量消息用于触发所述核心网设备向所述用户设备发送第二免流量消息；

所述核心网设备生成登录信息，所述登录信息为所述用户设备登录到应用服务器所需的信息；

所述核心网设备向所述用户设备发送所述第二免流量消息，所述第二免流量消息包括所述登录信息；

所述用户设备向所述应用服务器发送所述登录信息，以登录到所述应用服务器；

其中，所述第一免流量消息和所述第二免流量消息均为通过基站传输且不产生待计费流量的消息。

35. 根据权利要求 34 所述的方法，其特征在于，所述方法还包括：

所述核心网设备向所述用户设备发送第一标识信息或第二标识信息；

其中，所述第一标识信息标识所述用户设备对应的用户，所述第二标识信息为所述第一标识信息经脱敏处理得到的结果。

36. 根据权利要求 35 所述的方法，其特征在于，所述核心网设备向所述用户设备发送所述第二标识信息，包括：

所述核心网设备对所述第一标识信息进行脱敏处理得到所述第二标识信息，并向所述用户设备发送所述第二标识信息。

37. 根据权利要求 35 所述的方法，其特征在于，所述核心网设备向所述用户设备发送第一标识信息或第二标识信息，包括：

所述核心网设备向所述用户设备发送第三免流量消息，所述第三免流量消息包括所述第一标识信息或所述第二标识信息；

其中，所述第三免流量消息为通过基站传输且不产生待计费流量的消息。

38. 根据权利要求 34 至 37 中任一项所述的方法，其特征在于，所述方法还包括：

所述应用服务器向所述核心网设备发送登录认证消息，所述登录认证消息包括所述登录信息；

所述核心网设备向所述应用服务器发送所述用户的第三标识信息，所述用户的第三标识信息是基于所述登录信息确定的。

39. 根据权利要求 38 所述的方法，其特征在于，所述核心网设备向所述应用服务器发送所述用户的第三标识信息，包括：

若所述核心网设备成功认证所述登录信息，则所述核心网设备向所述应用服务器发送所述用户的第三标识信息。

40. 根据权利要求 38 或 39 所述的方法，其特征在于，所述方法还包括：

所述核心网设备基于所述登录信息和对应关系，确定所述用户的第三标识信息，所述

对应关系包括所述用户的第三标识信息与所述登录信息之间的对应关系。

41. 一种通信装置，其特征在于，包括执行如权利要求 1 至 40 中任一项所述方法的单元或模块。

5 42. 一种通信装置，其特征在于，包括至少一个处理器，所述至少一个处理器用于执行存储器中存储的计算机程序，以使得所述装置执行如权利要求 1 至 15 中任一项所述的方法，或者以使得所述装置执行如权利要求 16 至 33 中任一项所述的方法，或者以使得所述装置执行如权利要求 34 至 40 中任一项所述的方法。

43. 根据权利要求 42 所述的装置，其特征在于，所述装置还包括所述存储器和/或通信接口，所述通信接口与所述处理器耦合，

10 所述通信接口，用于输入和/或输出信息。

44. 根据权利要求 42 或 43 所述的装置，其特征在于，所述装置为芯片。

45. 一种通信系统，其特征在于，包括用户设备和核心网设备，

其中，所述用户设备用于执行如权利要求 1 至 15 中任一项所述的方法，所述核心网设备用于执行如权利要求 16 至 33 中任一项所述的方法。

15 46. 一种计算机可读存储介质，其特征在于，包括计算机程序，

当所述计算机程序在计算机上运行时，使得所述计算机执行如权利要求 1 至 15 中任一项所述的方法；或者，

当所述计算机程序在计算机上运行时，使得所述计算机执行如权利要求 16 至 33 中任一项所述的方法；或者，

20 当所述计算机程序在计算机上运行时，使得所述计算机执行如权利要求 34 至 40 中任一项所述的方法。

47. 一种计算机程序产品，其特征在于，所述计算机程序产品中包括计算机程序代码，其特征在于：

25 当所述计算机程序代码在计算机上运行时，使得计算机实现上述权利要求 1 至 15 中任一项所述的方法；或者，

当所述计算机程序代码在计算机上运行时，使得计算机实现上述权利要求 16 至 33 中任一项所述的方法；或者，

当所述计算机程序代码在计算机上运行时，使得计算机实现上述权利要求 34 至 40 中任一项所述的方法。

30