

安全策略处理方法以及通信设备

5           本申请要求于 2021 年 01 月 10 日提交中国专利局、申请号为 202110027552.1、申请名称为“安全策略处理方法以及通信设备”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           本申请实施例涉及通信领域，尤其涉及一种安全策略处理方法和通信设备。

背景技术

          用户面安全按需保护机制是第五代移动通信技术（5th generation mobile communication technology, 5G）网络中的一种安全机制，该用户面安全按需保护包含用户面加密保护和  
15    用户面完整性保护。该用户面安全按需保护机制要求接入网设备根据从核心网设备接收到的用户面安全策略判断是否开启与终端设备之间的用户面加密保护和/或用户面完整性保护。用户面安全按需保护机制能够为终端设备提供更加灵活的用户面安全保护。

          然而，现有的第四代移动通信技术（the 4th generation mobile communication technology, 4G）网络并不支持用户面安全按需保护机制。在4G网络中，接入网设备与终端设备的用户  
20    面安全是固定的，即用户面安全固定为用户面加密保护开启，用户面完整性保护不开启。

          在4G网络短期内不会退网的情况下，如何将前述用户面安全按需保护机制应用于4G网络中已经成为业界研究的热点。用户面安全按需保护机制对于网络中的接入网设备以及相关的核心网设备（如4G网络中的移动性管理实体（mobility management entity, MME）以及5G网络中的接入和移动性管理功能（access and mobility management function, AMF）  
25    实体等）的参与。

          而4G网络中可能存在未升级的接入网设备和未升级的核心网设备，前述未升级的接入网设备和未升级的核心网设备不支持用户面安全按需保护，因此，从而导致无法实现用户面安全按需保护的  
          目的。

          如何在同时存在升级和未升级的接入网设备/核心网设备的4G网络中，实现用户面安全  
30    按需保护的机制，是当前标准中亟需解决的问题。

发明内容

          本申请实施例提供了一种安全策略处理方法和通信设备，用于在存在不支持用户面安全按需保护的核心网网元的网络中，实现尽力而为的用户面安全按需开启机制。

35           第一方面，本申请实施例提供了一种安全策略处理方法，包括：目标接入网设备接收来自核心网设备#30-1的消息#50-2；其中，所述消息#50-2包含来自源接入网设备的容器信息；所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，所述用户面安全激活状态表征用户面加密保护是否开启和/或用户面完整性保护是

否开启。

一种可能的实现方式中，所述容器信息包括用户面安全策略#40-1；所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，包括：

5 所述目标接入网设备根据所述用户面安全策略#40-1，确定自身与终端设备之间的用户面安全激活状态。其中，容器信息是源接入网设备生成并通过核心网设备#30-1发送给目标接入网设备的，核心网设备#30-1不解析该容器信息，而是透传给目标接入网设备，因此，无论核心网设备#30-1是否升级，都可以保证目标接入网设备可以获得能够使用的用户面安全策略，进而保证目标接入网设备和终端设备之间可以实现用户面安全按需开启。

10 一种可能的实现方式中，所述消息#50-2还包括用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1；其中，用户面安全策略#40-2可以是核心网设备#30-1确定的所述终端设备对应的用户面安全策略（例如，可以是核心网设备#30-1自身保存的用户面安全策略，也可以是从其他核心网设备获取的用户面安全策略，例如终端设备的签约的用户面安全策略）。

15 所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，包括：所述目标接入网设备根据所述用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。

20 当目标接入网设备接收到多个用户面安全策略是，目标接入网设备可以优先使用优先级/安全等级高的用户面安全策略。本申请实施例中，目标接入网设备根据来自核心网设备#30-1的所述用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。可以有效的避免潜在的降质攻击。

此外，在一种可能的实现方式中，在所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态之前，所述方法还包括：

25 所述目标接入网设备判断所述用户面安全策略#40-2和所述用户面安全策略#40-1是否一致；在所述用户面安全策略#40-2和所述用户面安全策略#40-1一致的情况下，所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。

30 在所述用户面安全策略#40-2和所述用户面安全策略#40-1不一致的情况下，所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。还可以进一步的，生成告警信息，所述告警信息用于表征所述源接入网设备处于不安全的环境。可选的，所述目标接入网设备向所述核心网设备#30-1发送所述告警信息。后续目标接入网设备或者核心网设备#30-1执行相关操作时可以参考该告警信息。例如，在切换流程中，尽量避免切换到所述源接入网设备。

35 在一种可能的实现方式中，在所述消息#50-2中没有携带用户面安全策略且所述容器信息中也没有携带用户面安全策略的情况下，所述目标接入网设备根据预配置的用户面安全策略#40-3，确定自身与终端设备之间的用户面安全激活状态。

一种可能的实现方式中，所述消息#50-2为切换请求消息；所述切换请求消息用于请求所述目标接入网设备为所述终端设备准备切换资源。

一种可能的实现方式中，所述消息#50-2还包括指示信息；在所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态之前，所述方法

还包括：所述目标接入网设备根据所述指示信息确定所述终端设备支持用户面安全按需保护。

如果所述终端设备不支持用户面安全按需保护，则目标接入网设备可以不用确定自身与终端设备之间的用户面安全激活状态。

- 5       第二方面，本申请实施例提供了一种安全策略处理方法，包括：源接入网设备获取终端设备的用户面安全策略#40-1；所述源接入网设备向核心网设备#30-1 发送消息#50-1；所述消息#50-1 包括容器信息，所述容器信息包括所述用户面安全策略#40-1。其中，所述核心网设备#30-1 不解析所述容器信息中的内容。

- 10       一种可能的实现方式中，在所述源接入网设备获取终端设备的用户面安全策略#40-1 之前，所述方法还包括：所述源接入网设备确定所述终端设备支持用户面安全按需保护。

- 15       在终端设备不支持用户面安全按需保护，而源接入网设备支持用户面安全按需保护的情况下，源接入网设备可能会从核心网侧获得终端设备的用户面安全策略，并存储在终端设备的 AS 上下文里。如果终端设备不支持用户面安全按需保护，则源接入网设备可以不用获取 AS 上下文中的用户面安全策略，这样可以避免在网络中传递无用的信息，节约信令。

一种可能的实现方式中，所述方法还包括：所述源接入网设备确定所述终端设备需要切换到所述目标接入网设备。

- 20       上述各方面中，在切换场景下，所述消息#50-2 可以为切换请求消息；所述切换请求消息用于请求所述目标接入网设备为所述终端设备准备切换资源。所述消息#50-1 包括切换需求消息，所述切换需求消息用于目标接入网设备为所述终端设备准备切换资源。

- 25       一种可能的实现方式所述消息#50-2 还包括指示信息；在所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态之前，所述方法还包括：所述目标接入网设备根据所述指示信息确定所述终端设备支持用户面安全按需保护。所述指示信息由所述终端设备的安全能力的部分比特位表征，所述终端设备的安全能力用于指示所述终端设备支持使用的至少一个安全算法。其中，所述终端设备的安全能力为 UE 演进分组系统安全能力。

- 30       第三方面，本申请实施例提供了一种通信设备，该通信装置具有实现上述本申请实施例中各个网元用于实现相应的方法的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

- 35       第四方面，提供了一种装置，包括：处理器和存储器；该存储器用于存储计算机执行指令，当该装置运行时，该处理器执行该存储器存储的该计算机执行指令，以使该装置执行如上述第一方面和第二方面中任一所述的安全策略处理方法。该装置具体可以是第一方面中任一所述的安全策略处理方法中涉及的网元或者网元中的芯片。

第五方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第一方面和第二方面中任意一项所述的安全策略处理方法。

第六方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使

得计算机可以执行上述第一方面中任意一项所述的安全策略处理方法。

其中，第三方面至第六方面中任一种设计方式所带来的技术效果可参见第一方面中不同设计方式所带来的技术效果，此处不再赘述。

## 5 附图说明

为了更清楚地说明本申请实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例。

图 1A 为本申请实施例提供的一种安全策略处理方法适用的 4G 网络架构图；

图 1B 为本申请实施例提供的一种安全策略处理方法适用的 5G-4G 互通架构图

10 图 2 为本申请实施例提供的一种安全策略处理方法示意图；

图 3 为本申请实施例提供的一种安全策略处理方法在 S1 切换场景下的示例图；

图 4 为本申请实施例提供的一种安全策略处理方法在 5GS 到 EPS 切换场景下的一个示意图；

图 5 为本申请实施例提出的一种通信设备的结构示意图；

15 图 6 为本申请实施例提出的另一种通信设备的结构示意图。

## 具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。

20 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”以及其他各种术语标号等（如果存在）是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含

25 了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

本申请实施例提供的方法可以适用于任何存在不支持用户面安全按需保护的核心网网元的网络中，实现尽力而为的用户面安全按需开启机制。本申请实施例下面描述

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

示例性的，下面先介绍两个可能适用本申请提出的安全策略处理方法的系统架构

35 和应用场景。

本申请提出的安全策略处理方法适用的一种场景是 4G 网络场景。如图 1A 所示为当前长期演进（long term evolution, LTE）/系统架构演进（system architecture evolution, SAE）的网络构架。其中，核心网部分主要包括：移动管理实体（MME）、服务网关（serving gateway, SGW/S-GW）、分组数据网网关（packet data network

- gateway, PDN GW/PGW/ P-GW) 以及归属签约用户服务器 (home subscriber server, HSS)、服务 GPRS 支持节点 (serving GPRS support node, SGSN)、策略与计费规则功能单元 (policy and charging rules function, PCRF) 以及运营商的 IP 服务 (Operator's IP Services) (例如, IP 多媒体系统 (IP multimedia subsystem, IMS)、
- 5 分组交换业务 (packet switching service, PSS)) 等。其中, 核心网可以是演进型分组核心网 (evolved packet core, EPC)。此外, 图 1A 还包括接入网部分, 即 UMTS 演进陆地无线接入网 (evolution UMTS terrestrial radio access network, E-UTRAN)。该接入网部分主要包括: 接入网 (radio access network, RAN) 设备。此外, 图 1A 还可以包括终端设备, 例如, 用户设备 (user equipment, UE)。
- 10 其中, 移动管理实体 MME: 负责管理和存储终端设备的移动管理上下文 (例如, 终端设备的标识、移动性管理状态以及用户安全参数等), 对非接入层 (non-access stratum, NAS) 信令 (例如, 附着请求 (attach request)、位置更新请求 (update location request)、服务请求 (service request) 以及分组数据网连接请求 (PDN connectivity request) 等) 进行处理, 负责 NAS 信令的安全等。
- 15 服务网关 S-GW/SGW: 终结接入网用户面接口的网关, 执行合法监听、分组数据路由功能等。该服务网关 S-GW 与移动管理实体 MME 之间的接口是 S11 接口, 负责终端设备的会话控制信息等交互。
- 分组数据网网关 P-GW: 终结到分组数据网的 SGi 接口的网关, 用于提供用户的承载控制、数据转发、IP 地址分配以及非 3GPP 用户接入等功能, 是 3GPP
- 20 接入和非 3GPP 接入公用数据网 (public data network, PDN) 的锚点。P-GW 具有分组路由和转发的功能, 并负责策略计费增强功能、基于每个用户的分组过滤功能等。P-GW 通过 S5 接口与 S-GW 相连, 传递信息建立、修改和删除等控制信息, 以及分组数据路由等。此外, 该 P-GW 还通过 SGi 接口与运营商的 IP 服务相连。
- 25 归属签约用户服务器 HSS: 用户归属网络中存储用户信息的核心数据库。该 HSS 主要包含用户配置文件、用户签约数据、执行用户的身份验证和授权的相关信息以及有关用户物理位置的信息等。该 HSS 通过 S6a 接口与 MME 连接, 以使得 MME 可以从 HSS 获取前述用户配置文件、用户签约数据等信息。
- 策略与计费规则功能单元 PCRF: 业务数据流和 IP 承载资源的策略与计费控制策略决策点, 可以对用户和业务态服务质量 (quality of service, QoS) 进行控制, 为用户提供差异化的服务。该 PCRF 通过 Gx 与 P-GW 相连, 通过 Rx 与运营
- 30 商的 IP 服务相连。
- 此外, 前述 MME 通过 S1-MME 接口与 E-UTRAN 连接, S-GW 通过 S1-U 和 S11 分别与 E-UTRAN 和 MME 连接。同时 MME 通过 S3 接口, S-GW 通过 S4 接口
- 35 分别与 2G/3G 和 SGSN 连接, 分别负责终端设备在对应网络之间的移动性控制面锚点和用户面锚点功能。此外, S-GW 还通过 S12 接口与演进的通用陆地无线接入网络 (evolved universal terrestrial radio access network, UTRAN) 连接。

需要说明的是，上面的4G网络架构图只是示意性的，实际网络中，可能会存在多个同类网元，例如，可能存在多个接入网设备、多个MME以及多个PCRF等。其中，多个同类网元中，可能存在部分网元升级了（本申请各个实施例中，用“升级”表示网元支持用户面安全按需保护机制，下文不再赘述），而部分网元未升级（也可以这些网元称为传统的网元（legacy Network element, legacy NE），或者不支持用户面安全按需保护的NE）。例如，网络中可能同时存在升级的MME和未升级的MME。

本申请提出的安全策略处理方法适用的另外一种场景是4G网络和5G网络互通（Interworking）的场景。如图1B所示包括4G网络与5G网络共用的用户面功能（user plane function, UPF）实体+ PDN网关用户面功能（PDN gateway user plane function, PGW-U）实体、共用的会话管理功能（session management function, SMF）实体+ PDN网关控制面功能（PDN gateway control plane function, PGW-C）实体、共用的策略控制功能（policy control function, PCF）实体+策略和计费规则功能（policy and charging rules function, PCRF）实体、共用的归属签约用户服务器（home subscriber server, HSS）+统一数据管理（unified data management, UDM）实体。这里“+”表示合设，UPF为5G网络的用户面功能，PGW-U是与UPF对应的4G网络的网关用户面功能，SMF是5G网络的会话管理功能，PGW-C是与SMF对应的4G网络中的网关控制面功能，PCF是5G网络的策略控制功能、PCRF是与PCF对应的4G网络的策略计费规则功能。这里的“合设”可以表示同一个设备同时具备两个实体的功能。本申请实施例中，为方便表述，将HSS+UDM实体称之为用户数据管理实体，将PGW-C实体+SMF实体称之为控制面功能实体，在此进行统一说明，以下不再赘述。当然，上述合设后的网络设备也可以用其他名称，本申请实施例对此不作具体限定。

此外，如图1B所示，上述4G网络和5G网络互通架构中还可以包括MME和服务网关，以及5G网络中的接入和移动性管理功能（Access and Mobility Management Function, AMF）实体。

MME的功能同4G网络中的MME功能，这里不再赘述。

AMF实体：用于用户的接入和移动性管理，主要包含用户的注册管理、可达性管理、移动性管理、寻呼管理、接入认证和授权非接入层信令的加密和完整性保护等。

SMF实体：用于用户的会话管理，主要包含用户的会话建立、修改和释放，IP地址分配，会话策略管理等。

其中，终端设备通过演进型通用陆地无线接入网（evolved universal terrestrial radio access network, E-UTRAN）设备接入4G网络，终端通过下一代无线接入网（next generation radio access network, NG-RAN）设备接入5G网络。E-UTRAN设备通过S1-MME接口与MME通信，E-UTRAN设备通过S1-U接口与SGW通信，MME通过S11接口与SGW通信，MME通过S6a接口与用户数据管理实体通信，MME通过N26接口与AMF实体通信，SGW通过S5-U接口与PGW-U实体+UPF实体通信，SGW通过S5-C接口与PGW-C实体+SMF实体通信，PGW-U实体+UPF实体通过N3接口与NG-RAN设备通信，PGW-U实体+UPF实体通过N4接口与PGW-C实体+SMF实体通信，PGW-C实体+SMF实体通过N7接口与PCRF实体+PCF实体通信，HSS+UDM实体通过N10接口与PGW-C实体+SMF实体通信，HSS+UDM实体通过N8接口与AMF实体通信，PCRF实体+PCF实体通过N15接口与AMF实体通信，PGW-C实体+SMF实体通过N11接口与AMF实体通信，AMF实体通过N2接口与NG-RAN设备通信，AMF

实体通过N1接口与终端通信。

需要说明的是，图1B中的各个网元之间的接口名字只是一个示例，具体实现中接口名字可能为其他名字，本申请实施例对此不作具体限定。

当然，4G网络和5G网络互通架构中还可以有其它的网元，比如，4G网络中还可以包括通用分组无线系统（general packet radio system, GPRS）业务支撑节点（serving GPRS support node, SGSN）等，5G网络中还可以包括鉴权服务功能（authentication server function, AUSF）实体和网络切片选择功能（network slice selection function, NSSF）实体等，本申请实施例对此不作具体限定。

需要说明的是，上面的4G网络和5G网络互通架构只是示意性的，实际网络中，可能存在多个同类网元，例如，可能存在多个接入网设备以及多个MME等。其中，多个同类网元中，可能存在部分网元升级了，而部分网元未升级。例如，4G网络和5G网络互通架构中也可能同时存在升级的MME和未升级的MME。

本申请各个实施例涉及的接入网设备：是终端设备和核心网设备之间的桥梁，用于无线资源管理等。终端设备可以通过接入网设备接入网络。本申请中的接入网设备可以是4G无线接入网络设备，也可以是4G接入网中在空中接口上通过一个或多个小区与无线终端设备通信的设备。例如，前述接入网设备可以为长期演进LTE系统或演进的LTE系统（long term evolution advanced, LTE-A）中的演进型基站（evolutional node B, NodeB或eNB或e-NodeB）。也可以是5G无线接入网络设备，例如，可以包括NG-RAN，下一代演进型网络基站（Next Generation E-UTRAN NodeB, ng-eNB）或者5G基站（gNodeB, gNB）。应当注意的是，本申请中涉及的接入网设备可以是升级的接入网设备（例如，支持用户面安全按需保护的接入网设备）或未升级的接入网设备（例如，不支持用户面安全按需保护的接入网设备）。另外，根据为终端设备提供服务的先后顺序的不同，源接入网设备可以理解为切换流程之前为该终端设备提供服务的接入网设备，例如，可以是终端设备初始接入时为该终端设备提供服务的接入网设备；目标接入网设备可以理解为切换流程之后为该终端设备提供服务的接入网设备。一般地前述源接入网设备与目标接入网设备之间会有关于终端设备的上下文的传输。应当理解的是，本申请实施例中的接入网设备可以是上述任意一种设备或上述设备中的芯片，具体此处不做限定。无论作为设备还是作为芯片，该接入网设备都可以作为独立的产品进行制造、销售或者使用。在本实施例以及后续实施例中，以接入网设备为例进行介绍。

此外，本申请各个实施例涉及的终端设备：包括向用户提供语音和/或数据连通性的设备。例如，可以包括具有无线连接功能的手持式设备或连接到无线调制解调器的处理设备。该终端设备可以经无线接入网RAN（例如，前述源接入网设备或前述目标接入网设备）与核心网进行通信，可以与RAN交换语音和/或数据。该终端设备可以包括用户设备UE、无线终端设备、移动终端设备、用户单元（subscriber unit）、用户站（subscriber station），移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point, AP）、远程终端设备（remote terminal）、接入终端设备（access terminal）、用户终端设备（user terminal）、用户代理（user agent）、或用户装备（user device）等。此外，该终

端设备也可以为车载终端，例如，集成在车辆中的车载盒子（telematics box，T-Box）、域控制器（domain controller，DC）、多域控制器（multi domain controller，MDC）或车载单元（on board unit，OBU）。该终端设备还可以为穿戴设备，例如，眼镜、手套、手表、服饰及鞋，或者其他的可以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，

5 具体本申请不做限定。应当理解的是，本申请实施例中的终端设备可以是上述任意一种设备或芯片，具体此处不做限定。无论作为设备还是作为芯片，该终端设备都可以作为独立的产品进行制造、销售或者使用。在本实施例以及后续实施例中，仅以终端设备为例进行介绍。

由于网络中可能存在不支持用户面安全按需保护的核心网网元，所以在需要有核心网网元参与的用户面安全按需保护流程中，接入网设备可能无法获得用于实现用户面安全按需开启所必须的参数（如用户面安全策略等），从而无法实现自身与终端设备之间的用户面安全按需开启功能。

10

下面将对本申请各实施例涉及名称或术语进行介绍：

用户面安全策略，包括用户面加密保护策略和用户面完整性保护策略。其中，用户面加密保护策略用于指示是否开启用户面加密保护，用户面完整性保护策略用于指示是否开启用户面完整性保护。用户面加密保护策略存在三种可能的值，分别为 **not needed**、**preferred** 和 **required**，用户面完整性保护策略也存在三种可能的值，分别为 **not needed**、**preferred** 和 **required**。其中，**not needed** 表示不需要开启，**preferred** 表示可以开启也可以不开启，**required** 表示必须开启。上述三种可能的值可以采用 2 比特（bit）

15 来指示，例如 00 指示不需要开启，01 指示可以开启可以不开启，11 指示必须开启。用户面加密保护策略和用户面完整性保护策略具体采用何种方式对三种可能的值进行指示，在本申请实施例中不作限定。

20

用户面加密保护即保护数据在传输过程中的机密性（因此又可以被称作用户面机密性保护），机密性是指无法被直接看出真实内容。用户面完整性保护即保护数据在用户面传输过程中的完整性，完整性是指数据是原始的没有被篡改的。

25

在用户面安全按需保护机制下，接入网设备可以根据终端设备的用户面安全策略，确定是否按需自身与终端设备之间的用户面安全保护。当用户面加密保护策略/用户面完整性保护策略取值 **not needed** 时，则接入网设备根据用户面加密保护策略/用户面完整性保护策略，确定不开启自身与终端设备之间的用户面加密保护/用户面完整性保护；

30 当用户面加密保护策略/用户面完整性保护策略取值 **required** 时，则接入网设备根据用户面加密保护策略/用户面完整性保护策略，确定开启自身与终端设备之间的用户面加密保护/用户面完整性保护；当用户面加密保护策略/用户面完整性保护策略取值 **preferred** 时，则接入网设备根据用户面加密保护策略/用户面完整性保护策略以及其他信息（例如，自身的负荷情况），确定是否开启自身与终端设备之间的用户面加密保护/用户面完整性保护（例如，负荷大于阈值的情况下，不开启用户面加密保护/用户面完整性保护，反之，则开启用户面加密保护/用户面完整性保护）。

35

用户面安全激活状态，用于表征用户面加密保护是否开启和/或用户面完整性保护是否开启。可以理解为，用户面安全激活状态可以是接入网设备根据终端设备的用户面安全策略，确定用户面加密保护/用户面完整性保护开启或者不开启的结果。

当将用户面安全按需机制应用到 4G 网络时, MME 可能需要获取终端设备的用户面安全策略, 并传递给接入网设备。如果 MME 是传统的 MME, 则可能导致接入网设备无法获取终端设备的用户面安全策略, 从而无法实现用户面安全的按需开启。特别是在切换场景下, 可能会存在用户面安全保护强度下降的问题。

- 5           如图 2 所示, 提出的一种安全策略处理方法, 用以在切换场景下, 实现尽力而为的用户面安全按需开启机制。

S201、终端设备通过源接入网设备#10-1 接入网络#1; 以及源接入网设备#10-1 确定终端设备需要切换到目标接入网设备#20-1;

- 10           特别的, 该切换需要通过核心网设备进行, 例如, 该切换可以是 S1 切换, 5GS 到 EPS 切换。源接入网设备可以根据触发条件发起切换, 该条件例如可以包括: 与目标接入网没有 X2 连接, X2 切换失败, 源接入网设备根据当前运行状态策略; 以及当前无线网络状态较差, 负载均衡, 语音服务要求等。

- 15           当网络#1 为 4G 网络时, 源接入网设备#10-1 可以是 4G 网络中的接入网设备, 例如, 可以是演进型接入网 eNB 或者是演进型通用陆地无线接入网 E-UTRAN; 当网络#1 为 5G 网络时, 源接入网设备#10-1 可以是 5G 网络中的接入网设备, 例如, 可以是下一代无线接入网 NG-RAN。

需要说明的是, 在本申请实施例中该步骤为可选的。

S202、源接入网设备#10-1 向核心网设备#30-1 发送消息#50-1; 相应的, 核心网设备#30-1 接收来自源接入网设备#10-1 的消息#50-1。

- 20           其中, 消息#50-1 包括终端设备的标识以及容器信息。终端设备的标识用于标识终端设备, 以使得核心网设备#30-1 根据该终端设备的标识获得终端设备的接入层 (Access Stratum, AS) 上下文。容器信息由源接入网设备生成#10-1, 并最终传递到目标接入网设备#20-1, 容器信息中的内容不被中间网元 (如核心网设备#2) 解析。例如, 容器信息可以是源 eNB 到目标 eNB 透明容器 (source eNB to target eNB transparent container)。容器信息可以包含终端设备的用户面安全策略#40-1。
- 25

消息#50-1 例如可以是切换需求消息, 用于请求目标接入网设备#20-1 为所述终端准备切换资源。

- 一种可能的实现方式中, 源接入网设备#10-1 可以根据终端设备是否支持用户面安全按需保护, 来确定是否在容器信息中携带用户面安全策略#40-1。例如, 只有在终端设备支持用户面安全按需保护的情况下, 源接入网设备#10-1 才会在容器信息中携带用户面安全策略#40-1。具体的, 源接入网设备#10-1 根据终端设备的 AS 上下文确定终端设备是否支持用户面安全按需保护。例如, 终端设备的 AS 上下文中包括的终端设备是否支持用户面安全按需保护的指示信息/能力信息; 也可以包括自身与终端设备当前的用户面安全激活状态信息。源接入网设备#10-1 可以根据终端设备 AS 上下文中包括的信息, 确定终端设备是否支持用户面安全按需保护。
- 30
- 35

可选的, 用户面安全策略#40-1 可以是源接入网设备#10-1 与所述终端设备当前使用的用户面安全策略。例如, 用户面安全策略#40-1 可以是源接入网设备#10-1 上所述终端设备上下文中的用户面安全策略。一种可能的实现方式中, 当终端设备通过源接

接入网设备#10-1 接入到网络#1 中时，源接入网设备#10-1 可以从网络侧获取该用户面安全策略#40-1，并将该用户面安全策略#40-1 存储在所述终端设备的 AS 上下文中。该用户面安全策略#40-1 例如可以是所述终端设备签约的用户面安全策略（subscribed UP security policy）。

- 5       当源接入网设备确定发起切换时，可以从终端设备的 AS 上下文中获取存储的用户面安全策略#40-1。

S203、核心网设备#30-1 获取所述终端设备的用户面安全策略#40-2；

其中，核心网设备#30-1 根据消息#50-1 中的终端设备的标识，从所述终端设备的非接入层（non-access stratum，NAS）上下文中获取用户面安全策略#40-2。

- 10       需要说明的，S203 是可选的。在一种可能的实现方式中，如果核心网设备#30-1 是传统的网元，即不支持用户面安全按需机制，则该步骤可能无法执行。

S204、核心网设备#30-1 向目标接入网设备#20-1 发送消息#50-2；相应的，目标接入网设备#20-1 接收来自核心网设备#30-1 的消息#50-2

- 15       其中，所述消息#50-2 包括所述容器信息。可选的，在 S203 被执行的情况下，所述消息#50-2 中还包括所述用户面安全策略#40-2。

- 20       可选的，消息#50-2 还包括指示信息，该指示信息用于指示所述终端设备是否指示用户面安全按需保护。可选的，该指示信息可以由该终端设备的安全能力的部分比特位表征，该终端设备的安全能力用于指示该终端设备支持使用的至少一个安全算法。示例性的，前述终端设备的安全能力为 UE 演进分组系统安全能力（UE EPS security capabilities），该指示信息可以用终端设备的安全能力中一个预留的比特位来指示，例如 EEA7 或者 EIA7。其中，EEA7 代表 UE 演进分组系统安全能力中为第八个加密算法预留的比特位，EIA7 代表 UE 演进分组系统安全能力中为第八个完整性算法预留的比特位，而本实施例将该比特位用于携带终端设备是否支持用户面安全按需保护的指示。

- 25       所述消息#50-2 可以为切换请求消息；所述切换请求消息用于请求所述目标接入网设备为所述终端设备准备切换资源。

S205、目标接入网设备#20-1 根据消息#50-2 激活用户面安全保护。

- 30       具体的，当消息#50-2 不包括用户面安全策略#40-2，但是所述容器信息包括用户面安全策略#40-1 时，目标接入网设备#20-1 根据容器信息中的用户面安全策略#40-1，确定自身与终端设备之间的用户面安全激活状态。

当消息#50-2 包括用户面安全策略#40-2 时，目标接入网设备#20-1 根据用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态；

- 35       可选的，当消息#50-2 包括用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1 时，目标接入网设备#20-1 忽略用户面安全策略#40-1，并根据用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。

可选的，当消息#50-2 包括用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1 时，目标接入网设备#20-1 比较用户面安全策略#40-2 和用户面安全策略#40-1 是否一致，如果用户面安全策略#40-2 和用户面安全策略#40-1 一致，则采用用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态，如果用户面安全

策略#40-2 和用户面安全策略#40-1 不一致，可以采取如下任一操作：

1. 取消切换流程，具体的，目标接入网设备#20-1 发送切换失败(handover failure)消息到核心网设备#30-1，以指示核心网设备#30-1 准备切换资源失败。可选的，可以在切换失败(handover failure)消息中携带原因值。该原因值可以用于指示切换失败的原因，例如，用户面安全策略错误或者存在安全风险等。
2. 依旧以用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态，并生成一个警告信息。可选的，目标接入网设备#20-1 可以将该告警信息通知给核心网设备#30-1。所述告警信息用于表征源接入网设备#10-1 的信任等级。可以理解的是，该告警信息可以表示源接入网设备#10-1 处于不安全的环境。后续目标接入网设备#20-1 或者核心网设备#30-1 执行相关操作时可以参考该告警信息。例如，在切换流程中，尽量避免切换到所述源接入网设备#10-1。
3. 选择用户面安全策略#40-1 和用户面安全策略#40-2 中安全级别更高的用户面安全策略，并确定自身与终端设备之间的用户面安全激活状态。其中认为“required”的安全级别最高，其次为“preferred”，“not needed”安全级别最低。
4. 选择用户面安全策略#40-1 和用户面安全策略#40-2 中对性能影响最低的用户面安全策略，并确定自身与终端设备之间的用户面安全激活状态。其中认为“not needed”的性能影响最低，其次为“preferred”，“preferred”的性能影响最大。
5. 选择用户面安全策略#40-1 和用户面安全策略#40-2 中最平衡的用户面安全策略，并确定自身与终端设备之间的用户面安全激活状态。其中认为“preferred”最平衡。

在另外一种可能的实现方式中，消息#50-2 中可能不包括用户面安全策略#40-2，容器信息中不包括用户面安全策略#40-1，此时，目标接入网设备#20-1 可以根据预配置的用户面安全策略#40-3，确定自身与终端设备之间的用户面安全激活状态。

- 25 在另外一种可能的实现方式中，所述目标接入网设备#20-1 还从核心网设备 30-1 接收到所述指示信息。只有在所述指示信息指示所述终端设备支持用户面安全按需保护的情况下，目标接入网设备#20-1 才会进一步采用上述方法（1）-（5）所述的方式确定自身与所述终端设备之间的用户面安全激活状态。

其中，所述用户面安全激活状态用于指示用户面加密保护和/或用户面完整性保护是否开启的状态。

- 30 需要说明的是，本申请实施例中的核心网设备#30-1 是一个概括性的概念，其可以指代核心网中的一个或者多个网元。例如，核心网设备#30-1 可以包括 4G 网络中的一个 MME，或者是包括 4G 网络中的两个 MME，也可以包括一个 4G 网络中的 MME 与一个 5G 网络中的 AMF，本申请各个实施例中对核心网设备#30-1 的表现形式不做限定。
- 35

在本申请实施例中，只要终端设备和目标接入网设备#20-1 支持用户面安全按需保护机制，无论核心网设备#30-1 是否升级（支持用户面安全按需保护机制），目标接入网设备#20-1 总是可以获取相应的用户面安全策略，用以确定自身与终端设备之间的用户面安全激活状态。特别地，采用本申请实施例的方案，还可以有效的避免降质攻击

的问题。例如，源接入网设备#10-1 可能被攻击，不向核心网设备#30-1 发送用户面安全策略#40-1，或者向核心网设备#30-1 发送安全等级较低的用户面安全策略（如指示用户面加密保护和完整性保护都不开启的用户面安全策略），此时，目标接入网设备#20-1 可以通过优先使用来自核心网设备#30-1 的用户面安全策略#40-2，避免相应的攻击。

如图 3 所示，基于图 1A 所述的架构，提出的一种安全策略处理方法，用以在切换场景下，实现尽力而为的用户面安全按需开启机制。

下面以如图 3 所示的 S1 切换流程为例进行进一步介绍。其中，4G 网络中的接入网设备（为便于描述，本申请实施例以目标 eNB 为例）为前述目标接入网设备#20-1 的一种实现方式，4G 网络中的另一个接入网设备（为便于描述，本申请实施例以源 eNB 为例）为前述源接入网设备#10-1 的一种实现方式、目标 MME 和源 MME 为前述核心网设备#30-1 的一种实现方式。并且，假设目标 eNB 为升级的 eNB（即支持用户面安全按需保护的 eNB）。前述各个设备将执行如下步骤：

S301、终端设备通过源 eNB 接入 4G 网络；以及源 eNB 确定发起基于 S1 接口的切换，以便于将终端设备切换到目标 eNB；

源 eNB 在终端设备接入 4G 网络的过程中，会从核心网侧获取终端设备的用户面安全策略，并使用用户面安全策略激活自身与终端设备之间的用户面安全。源 eNB 还将获取的用户面安全策略存储在终端设备的接入层（access stratum，AS）上下文中。

示例性的，终端设备会通过初始 eNB 向初始 MME 发送附着请求（attach request）消息。然后，初始 MME 通过位置更新请求（update location request）消息将终端设备的标识发送至 HSS，该 HSS 向初始 MME 发送位置更新响应（update location request acknowledge）消息，其中，该位置更新响应消息携带该终端设备的签约数据，该签约数据中包含终端设备的签约的用户面安全策略。初始 MME 将该签约的用户面安全策略保存在终端设备的非接入层（non-access stratum，NAS）上下文中。初始 MME 在初始上下文建立请求（initial context setup request）消息中将该签约的用户面安全策略发送给初始 eNB，初始 eNB 将该签约的用户面安全策略保存在终端设备的 AS 上下文中。

在终端设备接入 4G 网络之后，没有更换接入网设备的情况下，这里的初始 eNB 就是源 eNB；在更换接入网设备的情况下，这里的初始 eNB 和源 eNB 是不同的接入网设备。此时，源 eNB 可以从初始 eNB 获取终端设备的 AS 上下文。

在终端设备接入 4G 网络之后，没有更换 MME 的情况下，这里的初始 MME 就是源 MME；在更换 MME 的情况下，这里的初始 MME 和源 MME 是不同的 MME。此时，源 MME 可以从初始 MME 获取终端设备的 NAS 上下文。

从上述流程可知，在没有出现攻击或者上下文传递（接入网设备之间的 AS 上下文或者 MME 之间的 NAS 上下文）异常的情况下，源 eNB 上的用户面安全策略（即用户面安全策略#40-1）和源 MME 上的用户面安全策略（用户面安全策略#40-2）应该是一致的。导致异常的原因可能包括接入网设备或者 MME 没有升级。

其中，当源 eNB 确定需要将终端设备切换至目标 eNB 时，S1 切换可以是基于如

下条件触发：

- (1) 源 eNB 和目标 eNB 之间没有 X2 接口；
- (2) 源 eNB 执行到目标 eNB 的 X2 切换失败，且源 eNB 接收来自目标 eNB 的错误指示；
- 5 (3) 源 eNB 动态学习的信息，或者源 eNB 上的配置信息等。

S302、源 eNB 向源 MME 发送切换需求（handover required）消息。

其中，该切换需求消息携带终端设备的标识以及容器信息（source eNB to target eNB transparent container）。终端设备的标识用于获得终端设备的上下文，例如，eNB  
10 UE S1AP ID 和 MME UE S1AP ID。

容器信息由源 eNB 生成，并最终传递到目标 eNB，不被中间网元（如源 MME 和目标 MME）解析。

其中，容器信息可选的包含源 eNB 保存的终端设备的用户面安全策略（即用户面安全策略#40-1）。

15 具体情况，可以参考 S202 中的相关描述，这里不予赘述。

S303、源 MME 获取所述终端设备的用户面安全策略#40-2；

同 S203，这里不再赘述。

S304、源 MME 向目标 MME 发送转发重定位请求（forward relocation request）消  
20 息。

其中，该转发重定位请求消息携带所述容器信息。特别的，源 MME 不解析容器信息，直接转发该容器信息。

该转发重定位请求消息还可以携带源 MME 保存的终端设备的用户面安全策略（即用户面安全策略#40-2）。示例性的，源 MME 根据终端设备的标识获得终端设备的  
25 NAS 上下文，从终端设备的 NAS 上下文中获得用户面安全策略#40-2。

可选的，该转发重定位请求消息还包含指示信息，该指示信息用于指示所述终端设备是否指示用户面安全按需保护。可选的，如果源 MME 是传统的 MME，则源 MME 本地可能不会保存用户面安全策略，所以也不会向目标 MME 发送用户面安全策略。

相关内容，例如，指示信息的相关描述，可以参考 S204 相关描述，这里不再赘  
30 述。

S305、目标 MME 向目标 eNB 发送切换请求（handover request）消息。

其中，所述切换请求消息用于请求所述目标 eNB 为所述终端设备准备切换资源。

该切换请求消息携带所述容器信息。可选的，该切换请求消息还可以携带终端设备的用户面安全策略#40-2 以及可选的携带所述指示信息。

35 需要说明的是，如果目标 MME 为传统的 MME，则目标 MME 可能不会向目标 eNB 发送所述用户面安全策略#40-2。因为传统的 MME，可能无法识别该信元，从而丢弃或者无法处理该信元。

S306、目标 eNB 确定用户面安全激活状态，所述用户面安全激活状态用于指示是否开启用户面加密保护和/或用户面完整性保护。

在一种可选的实施方式（1）中，若所述切换请求消息携带终端设备的用户面安全策略#40-2，则目标 eNB 使用用户面安全策略 40-2 确定自身与所述终端设备之间的用户面安全激活状态。应理解，在所述切换请求消息携带终端设备的用户面安全策略#40-2 的情况下，即使容器信息携带用户面安全策略#40-1，目标 eNB 也将忽略用户面安全策略#40-1，目标 eNB 都将用户面安全策略#40-2 来确定自身与所述终端设备之间的用户面安全激活状态。

在一种可选的实施方式（2）中，若所述切换请求消息不携带终端设备的用户面安全策略#40-2，但是所述容器信息携带用户面安全策略#40-1，则目标 eNB 使用用户面安全策略#40-1 来确定自身与所述终端设备之间的用户面安全激活状态。

在一种可选的实施方式（3）中，若所述切换请求消息携带终端设备的用户面安全策略#40-2，且所述容器信息也携带用户面安全策略#40-1，目标 eNB 对比用户面安全策略#40-1 和用户面安全策略#40-2，若一致，则目标 eNB 使用用户面安全策略#40-2 来确定自身与所述终端设备之间的用户面安全激活状态；若不一致，则目标 eNB 将发起切换取消流程。

在另一种可选的实施方式（4）中，若所述切换请求消息不携带终端设备的用户面安全策略#40-2，所述容器信息也不携带用户面安全策略#40-1，且目标 eNB 中预配置了用户面安全策略#40-3，则目标 eNB 使用目标 eNB 配置的用户面安全策略来确定自身与所述终端设备之间的用户面安全激活状态。

在另一种可选的实施方式（5）中，所述目标 eNB 还从目标 MME 接收到所述指示信息。只有在所述指示信息指示所述终端设备支持用户面安全按需保护的情况下，目标 eNB 才会进一步采用上述方法（1）-（4）所述的方式确定自身与所述终端设备之间的用户面安全激活状态。

在另一种可选的实施方式（6）中，若切换请求消息不携带终端设备的用户面安全策略#40-2，所述容器信息也不携带用户面安全策略#40-1，则目标 eNB 可以用未升级的方式为终端设备确定用户面安全激活状态，即总是开启加密保护，但不开启完整性保护。

目标 eNB 确定用于自身与终端设备的用户面安全策略的方法，除了上面 6 种实现方式外，具体的实现中，还可以参考 S205 中的相关描述，这里不再赘述。

S307、目标 eNB 向目标 MME 发送切换请求响应（handover request acknowledge）消息。

其中，切换请求响应消息中包含无线资源控制 RRC 重配置（RRC connection reconfiguration），该 RRC 重配置由目标 eNB 构造。

可选的，RRC 重配置中携带配置信息，所述配置信息用于指示终端设备是否开启用户面加密保护和/或用户面完整性保护。可选的，配置信息由 S306 中用户面安全激活状态确定。

具体的，若配置信息中封装了禁用加密（ciphering disabled）字段，则终端设备不开启加密保护；若配置信息中未封装禁用加密（ciphering disabled）字段，则终端设备开启加密保护。若配置信息中封装了完整性保护（integrity protection）字段，则终端设备开启完整性保护；若配置信息中未封装完整性保护（integrity protection）字段，

则终端设备不开启完整性保护。

应理解，目标 eNB 将用户面安全激活状态通过所述配置信息的方式封装于 RRC 重配置中，通过切换请求响应发送至源 eNB，再由源 eNB 将封装了用户面安全激活状态的 RRC 重配置转发至终端设备。

- 5           S308、目标 MME 向源 MME 发送转发重定位回复（forward relocation response）消息。

该转发重定位回复消息包含上述 RRC 重配置，该 RRC 重配置携带所述配置信息。

S309、源 MME 向源 eNB 发送切换命令（handover command）消息。

该切换命令消息包含上述 RRC 重配置，该 RRC 重配置携带所述配置信息。

- 10          S310、源 eNB 向终端设备发送 RRC 重配置。

也就是说，该源 eNB 将从目标 eNB 中收到的 RRC 重配置转发至终端设备。

具体的，终端设备根据 RRC 重配置中的携带的所述配置信息确定是否开启自身与所述目标 eNB 之间的用户面安全加密保护/用户面完整性保护。

- 15          示例性的，当终端设备确定该配置信息未封装禁用加密（ciphering disabled）字段且未封装完整性保护（integrity protection）字段。于是，该终端设备便开启加密保护，但不开启完整性保护。当终端设备确定配置信息封装禁用加密（ciphering disabled）字段但未封装完整性保护（integrity protection）字段。于是，该终端设备便不开启该 DRB 的加密保护，也不开启该 DRB 的完整性保护。当终端设备确定该配置信息未封装禁用加密（ciphering disabled）字段但封装完整性保护（integrity protection）字段。于是，  
20          该终端设备便开启加密保护，也开启完整性保护。当终端设备确定该配置信息封装了禁用密码（ciphering disabled）字段也封装完整性保护（integrity protection）字段。于是，该终端设备便不开启加密保护，但开启完整性保护。

S311、终端设备向目标 eNB 发送 RRC 重配置完成消息。

- 25          其中，该 RRC 重配置完成（RRC connection reconfiguration Complete）消息用于指示目标 eNB 该终端设备已完成 RRC 重配置流程，该终端设备成功从源 eNB 切换至目标 eNB。此后，该终端设备可以与直接目标 eNB 进行通信。

- 30          本申请实施例中，不管源eNB或源MME或目标MME是否升级，目标eNB都能够获得可使用的用户面安全策略，并根据获得的用户面安全策略确定与终端设备之间的用户面安全保护状态。避免了在4G网络中由于源eNB或源MME或目标MME中部分网元未升级导致的用户面安全策略丢失，导致无法实现用户面安全按需机制的问题。此外，本申请实施例还可以尽最大可能使目标eNB可以获得一个优先级更高的安全策略，以尽最大努力保障在切换过程中的以最优选的用户面安全策略为终端设备开启或不开启用户面安全保护，避免了潜在的降质攻击。

- 35          如图 4 所示，基于图 1B 所述的架构，提出的一种安全策略处理方法，用以在 5GS 到 EPS 切换场景下，实现尽力而为的用户面安全按需开启机制。

其中，4G 网络中的接入网设备（为便于描述，本申请实施例以目标 eNB 为例，本实施例中下文简称 eNB）为前述目标接入网设备的一种实现方式，5G 网络中的接入网设备（为便于描述，本申请实施例以源 NG-RAN 为例，本实施例中下文简称 NG-RAN）为前述源接入网设备的一种实现方式，5G 网络中的核心网

设备（为便于描述，本申请实施例以源 AMF 为例，本实施例中下文简称源 AMF）和 4G 网络中的核心网设备（为便于描述，本申请实施例以目标 MME 为例，本实施例中下文简称 MME）为前述核心网设备#30-1 的一种实现方式。并且，假设 eNB 为升级的 eNB（即支持用户面安全按需保护的 eNB）。前述各个设备将执行如下步骤：

S401、终端设备通过 NG-RAN 接入 5G 网络；以及 NG-RAN 确定发起 5GS 到 EPS 切换，以便于将终端设备切换到 4G 网络中的 eNB；

NG-RAN 在终端设备接入 5G 网络的过程中，会从核心网侧获取终端设备的用户面安全策略，并使用用户面安全策略激活自身与终端设备之间的用户面安全。NG-RAN 还将获取的用户面安全策略存储在终端设备的接入层（access stratum, AS）上下文中。

示例性的，终端设备向 NG-RAN 发送协议数据单元（protocol data unit, PDU）会话建立请求消息。NG-RAN 通过 AMF 向 PWG-C+SMF 发送 PDU 会话建立请求。PWG-C+SMF 可以从 HSS+UDM 中获得终端设备签约的用户面安全策略，也可以从 PWG-C+SMF 的本地配置信息中获得用户面安全策略。其中，PWG-C+SMF 获取的用户面安全策略为终端设备的用户面安全策略，具体可以为针对该 PDU 会话的用户面安全策略。PWG-C+SMF 可以将从 HSS+UDM 获取的签约的用户面安全策略保存在终端设备的上下文中。PWG-C+SMF 将获取的用户面安全策略通过 AMF 发送给 NG-RAN。NG-RAN 将该签约的用户面安全策略保存在终端设备的 AS 上下文中。

因此，正常情况下，NG-RAN 中保存的用户面安全策略应该与 PWG-C+SMF 中保存的用户面安全策略一致。

其中，当源 NG-RAN 确定需要将终端设备切换至目标 eNB 时，5GS 到 EPS 切换可以是基于如下条件触发：

- （1）当前无线网络状态较差；
- （2）负载均衡；
- （3）语音服务要求。

S402、NG-RAN 向 AMF 发送切换需求（handover required）消息。

其中，该切换需求消息携带终端设备的标识以及容器信息。终端设备的标识用于获得终端设备的上下文，例如，RAN UE NGAP ID、AMF UE NGAP ID。

容器信息由 NG-RAN 生成，并最终传递到 eNB，不被中间网元解析，中间网元包含 AMF 以及 MME。相关描述可以参考 S202 和 S302 中的相关描述，这里不予赘述。

S403、AMF 向 PGW-C+SMF 发送 PDU 会话上下文请求消息。

PDU 会话上下文请求消息可以包含终端设备的上下文标识，终端设备的上下文标识可以根据终端设备的标识获得的，例如，会话管理上下文标识（Session Management Context ID）。

S404、PGW-C+SMF 获取终端设备的用户面安全策略#40-3；

具体的，PGW-C+SMF 根据终端设备的上下文标识获得终端设备的用户面安全策略#40-3。用户面安全策略#40-3 可以是终端设备上下文中存储的用户面安全策略，也可以是根据终端设备上下文中存储的用户面安全策略映射得到的用户面安全策略。

应理解，若 PGW-C+SMF 是未升级的核心网设备，则 PGW-C+SMF 可能不会执行

S404。

S405、PGW-C+SMF 向 AMF 发送 PDU 会话上下文回复消息。

PDU 会话上下文回复消息包含终端设备的用户面安全策略#40-3。

应理解，若 PGW-C+SMF 是未升级的核心网设备，则 PDU 会话上下文回复消息

5 可能不会携带用户面安全策略#40-3。

S406、AMF 向 MME 发送转发重定位请求（forward relocation request）消息。

S407、MME 向 eNB 发送切换请求（handover request）消息。

S408、eNB 确定用户面安全激活状态。

S409、eNB 向 MME 发送切换请求响应（handover request acknowledge）消息。

10 S410、MME 向 AMF 发送转发重定位回复（forward relocation response）消息。

S411、AMF 向 eNB 发送切换命令（handover command）消息。

S412、NG-RAN 向终端设备发送 RRC 重配置。

S413、终端设备向 eNB 发送 RRC 重配置完成消息。

上述 S406-S413 的相关描述同 S304-S311，请参考上述描述，这里不再赘述。

15 本申请实施例中，不管 PGW-C+SMF 和 MME 是否升级，eNB 都能够获得可使用的用户面安全策略，并根据获得的用户面安全策略确定与终端设备之间的用户面安全保护状态。避免了在 4G 网络中由于源 eNB 或源 MME 或目标 MME 中部分网元未升级导致的用户面安全策略丢失，导致无法实现用户面安全按需机制的问题。此外，本申请实施例还可以尽最大可能使目标 eNB 可以获得一个优先级更高的安全策略，以尽  
20 最大努力保障在切换过程中的以最优选的用户面安全策略为终端设备开启或不开启用户面安全保护，避免了潜在的降质攻击。

图 5 所示为本申请实施例提供的通信设备的硬件结构示意图。该通信设备 500 包括至少一个处理器 501，通信线路 502，存储器 503 以及至少一个通信接口 504。

25 处理器 501 可以是一个通用中央处理器（central processing unit，CPU），微处理器，特定应用集成电路（application-specific integrated circuit，ASIC），或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路 502 可包括一通路，在上述组件之间传送信息。

30 通信接口 504，使用任何收发器一类的装置，用于与其他设备或通信网络通信，如以太网，无线接入网（radio access network，RAN），无线局域网(wireless local area networks，WLAN)等。

存储器 503 可以是只读存储器（read-only memory，ROM）或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器（random access memory，RAM）或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器

35 （electrically erasable programmable read-only memory，EEPROM）、只读光盘（compact disc read-only memory，CD-ROM）或其他光盘存储、光碟存储（包括压缩光碟、激光光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过通信线路 502 与处理器相连接。存储器也可以和处理器集成在一起。

其中，存储器 503 用于存储执行本申请方案的计算机执行指令，并由处理器 501 来控制执行。处理器 501 用于执行存储器 503 中存储的计算机执行指令，从而实现本申请上述实施例提供的安全策略处理方法。

5 可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

在具体实现中，作为一种实施例，处理器 501 可以包括一个或多个 CPU，例如图 5 中的 CPU0 和 CPU1。

10 在具体实现中，作为一种实施例，通信设备 500 可以包括多个处理器，例如图 5 中的处理器 501 和处理器 508。这些处理器中的每一个可以是一个单核（single-CPU）处理器，也可以是一个多核（multi-CPU）处理器。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（例如计算机程序指令）的处理核。

15 在具体实现中，作为一种实施例，通信设备 500 还可以包括输出设备 505 和输入设备 506。输出设备 505 和处理器 501 通信，可以以多种方式来显示信息。例如，输出设备 505 可以是液晶显示器（liquid crystal display, LCD），发光二极管（light emitting diode, LED）显示设备，阴极射线管（cathode ray tube, CRT）显示设备，或投影仪（projector）等。输入设备 506 和处理器 501 通信，可以以多种方式接收用户的输入。例如，输入设备 506 可以是鼠标、键盘、触摸屏设备或传感设备等。

20 上述的通信设备 500 可以是一个通用设备或者是一个专用设备。在具体实现中，通信设备 500 可以是上述图 2-图 4 实施例中的任一网元，如源接入网设备、目标接入网设备、AMF、MME、PGW-C+SMF 等。本申请实施例不限定通信设备 500 的类型。

25 上述图 2-图 4 主要以方法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，通信装置为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的模块及算法步骤，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。

30 本申请实施例可以根据上述方法示例对通信装置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。

35 下面对本申请中的通信装置进行详细描述，请参阅图 6，图 6 为本申请实施例中通信装置的一种实施例示意图。通信装置可以是图 2-图 4 实施例中的任一网元，如源接入网设备、目标接入网设备、AMF、MME、PGW-C+SMF 等。该通信装置包括：通信模块 601 和处理模块 602。其中，所述通信模块 601 用于实现消息的接收和发送功能，所述处理模块 602 用于执行相关的处理功能。

当所述通信装置为源接入网设备时：

所述通信模块 601，用于执行上述图 2-图 4 中 S202、S302、S402、S309、S310、

S411 和 S412 相关内容。

特别地，所述处理模块 602，用于获取所述终端设备的用户面安全策略#40-1；

可选的，所述处理模块 602，还用于根据终端设备是否支持用户面安全按需保护，来确定是否在容器信息中携带用户面安全策略#40-1。

5 当所述通信装置为目标接入网设备时：

所述通信模块 601，用于接收来自核心网设备#30-1 的消息#50-2；其中，所述消息#50-2 包含来自源接入网设备的容器信息；

10 所述处理模块 602，用于设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，所述用户面安全激活状态表征用户面加密保护是否开启和/或用户面完整性保护是否开启。

一种可能的实现方式中，所述容器信息包括用户面安全策略#40-1；所述处理模块 602，具体用于根据所述用户面安全策略#40-1，确定自身与终端设备之间的用户面安全激活状态。

15 一种可能的实现方式中，所述消息#50-2 还包括用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1；所述处理模块 602，具体用于根据所述用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。具体的，所述处理模块 602，用于忽略所述用户面安全策略#40-1，直接使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。

20 一种可能的实现方式中，所述处理模块 602，还用于判断所述用户面安全策略#40-2 和所述用户面安全策略#40-1 是否一致。

一种可能的实现方式中，所述处理模块 602，还用于生成告警信息，所述告警信息用于表征源接入网设备#10-1 处于不安全的环境。可选的，所述通信模块 601，还用于向所述核心网设备#30-1 发送所述告警信息。

25 一种可能的实现方式中，所述处理模块 602，还用于在所述消息#50-2 中没有携带用户面安全策略且所述容器信息中也没有携带用户面安全策略的情况下，根据预配置的用户面安全策略，确定自身与终端设备之间的用户面安全激活状态。

一种可能的实现方式中，所述消息#50-2 还包括指示信息，所述处理模块 602，还用于根据所述指示信息确定所述终端设备支持用户面安全按需保护。

30 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，另外，在本申请各个实施例中的各功能模块可以集成在一个处理器中，也可以是单独物理存在，也可以两个或两个以上模块集成在一个模块中。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。

35 在一个例子中，以上任一通信装置中的单元可以是配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路(application specific integrated circuit, ASIC)，或，一个或多个微处理器(digital signal processor, DSP)，或，一个或者多个现场可编程门阵列(field programmable gate array, FPGA)，或这些集成电路形式中至少两种的组合。再如，当通信装置中的单元可以通过处理元件调度程序的形式实现时，该处理元件可以是通用处理器，例如中央处理器(central processing unit, CPU)或其它可以调用程序的处理器。再如，这些单元可以集成在一起，以片上系统

(system-on-a-chip, SOC) 的形式实现。

本申请还提供一种通信系统，其包括网络设备或终端设备中的至少一种或多种。

本申请实施例还提供的一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机控制网络设备或终端设备执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供的一种计算机程序产品，计算机程序产品包括计算机程序代码，当计算机程序代码在计算机上运行时，使得计算机执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供一种芯片系统，包括存储器和处理器，存储器用于存储计算机程序，处理器用于从存储器中调用并运行计算机程序，使得芯片执行如前述方法实施例所示任一项实现方式。

本申请实施例还提供一种芯片系统，包括处理器，处理器用于调用并运行计算机程序，使得芯片执行如前述方法实施例所示任一项实现方式。

本申请实施例提供的技术方案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发明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、AI 节点、接入网设备、终端设备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可以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，数字视频光盘（digital video disc, DVD））、或者半导体介质等。

在本申请实施例中，在无逻辑矛盾的前提下，各实施例之间可以相互引用，例如方法实施例之间的方法和/或术语可以相互引用，例如装置实施例之间的功能和/或术语可以相互引用，例如装置实施例和方法实施例之间的功能和/或术语可以相互引用。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

## 权 利 要 求 书

- 1、一种安全策略处理方法，其特征在于，包括：
- 目标接入网设备接收来自核心网设备#30-1的消息#50-2；其中，所述消息#50-2包含来自源接入网设备的容器信息；
- 5       所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，所述用户面安全激活状态表征用户面加密保护是否开启和/或用户面完整性保护是否开启。
- 2、根据权利要求1所述的方法，其特征在于，所述容器信息包括用户面安全策略#40-1；
- 10       所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，包括：
- 所述目标接入网设备根据所述用户面安全策略#40-1，确定自身与终端设备之间的用户面安全激活状态。
- 3、根据权利要求1所述的方法，其特征在于，所述消息#50-2还包括用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1；
- 15       所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，包括：
- 所述目标接入网设备根据所述用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。
- 20       4、根据权利要求3所述的方法，其特征在于，所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态，包括：
- 所述目标接入网设备忽略所述用户面安全策略#40-1，直接使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。
- 5、根据权利要求3所述的方法，其特征在于，在所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态之前，所述方法还包括：
- 25       所述目标接入网设备判断所述用户面安全策略#40-2和所述用户面安全策略#40-1是否一致；
- 在所述用户面安全策略#40-2和所述用户面安全策略#40-1一致的情况下，所述目标接入网设备使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。
- 30       6、根据权利要求5所述的方法，其特征在于，在所述用户面安全策略#40-2和所述用户面安全策略#40-1不一致的情况下，所述还包括：
- 所述目标接入网设备生成告警信息，所述告警信息用于表征所述源接入网设备处于不安全的环境。
- 35       7、根据权利要求6所述的方法，其特征在于，还包括：
- 所述目标接入网设备向所述核心网设备#30-1发送所述告警信息。
- 8、根据权利要求1所述的方法，其特征在于，所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，包括：

在所述消息#50-2 中没有携带用户面安全策略且所述容器信息中也没有携带用户面安全策略的情况下，所述目标接入网设备根据预配置的用户面安全策略#40-3，确定自身与终端设备之间的用户面安全激活状态。

9、根据权利要求 1-8 任一所述的方法，其特征在于，所述容器信息为源 eNB 到目标 eNB 透明容器（source eNB to target eNB transparent container）。

10、根据权利要求 1-9 任一所述的方法，其特征在于，所述消息#50-2 为切换请求消息；所述切换请求消息用于请求所述目标接入网设备为所述终端设备准备切换资源。

11、根据权利要求 1-10 任一所述的方法，其特征在于，所述消息#50-2 还包括指示信息；在所述目标接入网设备根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态之前，所述方法还包括：

所述目标接入网设备根据所述指示信息确定所述终端设备支持用户面安全按需保护。

12、根据所述权利要求 11 所述的方法，其特征在于，所述指示信息由所述终端设备的安全能力的部分比特位表征，所述终端设备的安全能力用于指示所述终端设备支持使用的至少一个安全算法。

13、根据所述权利要求 12 所述的方法，其特征在于，所述终端设备的安全能力为 UE 演进分组系统安全能力。

14、一种安全策略处理方法，其特征在于，包括：

源接入网设备获取终端设备的用户面安全策略#40-1；

20 所述源接入网设备向核心网设备#30-1 发送消息#50-1；所述消息#50-1 包括容器信息，所述容器信息包括所述用户面安全策略#40-1。

15、根据权利要求 14 所述的方法，其特征在于，在所述源接入网设备获取终端设备的用户面安全策略#40-1 之前，所述方法还包括：

所述源接入网设备确定所述终端设备支持用户面安全按需保护。

25 16、根据权利要求 14 或 15 所述的方法，其特征在于，所述消息#50-1 包括切换需求消息，所述切换需求消息用于目标接入网设备为所述终端设备准备切换资源。

17、根据权利要求 16 所述的方法，其特征在于，所述方法还包括：

所述源接入网设备确定所述终端设备需要切换到所述目标接入网设备。

18、一种接入网设备，其特征在于，包括：

30 通信模块，用于接收来自核心网设备#30-1 的消息#50-2；其中，所述消息#50-2 包含来自源接入网设备的容器信息；

处理模块，用于根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态，所述用户面安全激活状态表征用户面加密保护是否开启和/或用户面完整性保护是否开启。

35 19、根据权利要求 18 所述的接入网设备，其特征在于，所述容器信息包括用户面安全策略#40-1；

所述处理模块，具体用于根据所述用户面安全策略#40-1，确定自身与终端设备之间的用户面安全激活状态。

20、根据权利要求 18 所述的接入网设备，其特征在于，所述消息#50-2 还包括用

用户面安全策略#40-2，且所述容器信息包括用户面安全策略#40-1；

所述处理模块，具体用于根据所述用户面安全策略#40-2，确定自身与终端设备之间的用户面安全激活状态。

- 21、根据权利要求 20 所述的接入网设备，其特征在于，所述处理模块，具体用于：  
5 忽略所述用户面安全策略#40-1，直接使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。

- 22、根据权利要求 20 所述的接入网设备，其特征在于，所述处理模块，还用于：  
在使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态之前，判断所述用户面安全策略#40-2 和所述用户面安全策略#40-1 是否一致；  
10 在所述用户面安全策略#40-2 和所述用户面安全策略#40-1 一致的情况下，使用所述用户面安全策略#40-2，确定自身与所述终端设备之间的用户面安全激活状态。

- 23、根据权利要求 22 所述的接入网设备，其特征在于，所述处理模块，还用于：  
在所述用户面安全策略#40-2 和所述用户面安全策略#40-1 不一致的情况下，生成告警信息，所述告警信息用于表征所述源接入网设备处于不安全的环境。

- 15 24、根据权利要求 23 所述的接入网设备，其特征在于，所述通信模块，还用于向所述核心网设备#30-1 发送所述告警信息。

- 25、根据权利要求 18 所述的接入网设备，其特征在于，所述处理模块，具体用于：  
在所述消息#50-2 中没有携带用户面安全策略且所述容器信息中也没有携带用户面安全策略的情况下根据预配置的用户面安全策略#40-3，确定自身与终端设备之间的  
20 用户面安全激活状态。

26、根据权利要求 18-25 任一所述的接入网设备，其特征在于，所述容器信息为源 eNB 到目标 eNB 透明容器（source eNB to target eNB transparent container）。

- 27、根据权利要求 18-26 任一所述的接入网设备，其特征在于，所述消息#50-2 为切换请求消息；所述切换请求消息用于请求所述接入网设备为所述终端设备准备切换  
25 资源。

28、根据权利要求 18-27 任一所述的接入网设备，其特征在于，所述消息#50-2 还包括指示信息；所述处理模块，还用于：

在根据所述消息#50-2，确定自身与终端设备之间的用户面安全激活状态之前，根据所述指示信息确定所述终端设备支持用户面安全按需保护。

- 30 29、根据所述权利要求 28 所述的接入网设备，其特征在于，所述指示信息由所述终端设备的安全能力的部分比特位表征，所述终端设备的安全能力用于指示所述终端设备支持使用的至少一个安全算法。

30、根据所述权利要求 29 所述的接入网设备，其特征在于，所述终端设备的安全能力为 UE 演进分组系统安全能力。

35

31、一种接入网设备，其特征在于，包括：

处理模块，用于获取终端设备的用户面安全策略#40-1；

通信模块，用于向核心网设备#30-1 发送消息#50-1；所述消息#50-1 包括容器信息，所述容器信息包括所述用户面安全策略#40-1。

32、根据权利要求 31 所述的接入网设备，其特征在于，所述处理模块，还用于：在获取终端设备的用户面安全策略#40-1 之前，确定所述终端设备支持用户面安全按需保护。

5 33、根据权利要求 31 或 32 所述的接入网设备，其特征在于，所述消息#50-1 包括切换需求消息，所述切换需求消息用于目标接入网设备为所述终端设备准备切换资源。

34、根据权利要求 33 所述的接入网设备，其特征在于，所述处理模块，还用于：确定所述终端设备需要切换到所述目标接入网设备。

10 35、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有指令，当所述指令在计算机上运行时，以使得计算机执行如权利要求 1 至 17 中任意一项所述的方法。

36、一种包含指令的计算机程序产品，其特征在于，当所述指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 17 中任意一项所述的方法。