(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 2 月 7 日 (07.02.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/024744 A1

(51) 国际专利分类号:
*H04W 8/26* (2009.01)

(21) 国际申请号: PCT/CN2018/097088

(22) 国际申请日: 2018 年 7 月 25 日 (25.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710643843.7 2017年7月31日 (31.07.2017) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 李赫 (LI, He); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
陈璟 (CHEN, Jing); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
李欢 (LI, Huan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京三高永信知识产权代理有限责任公司 (BEIJING SAN GAO YONG XIN INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国北京市海淀区学院路蓟门里和景园A座1单元102室, Beijing 100088 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) **Title:** METHOD AND DEVICE FOR ACQUIRING IDENTIFIER OF TERMINAL DEVICE

(54) **发明名称:** 获取终端设备的身份标识的方法及装置

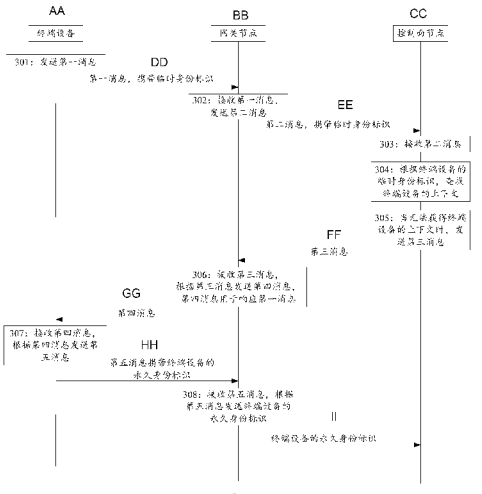


图 3

301: Transmit first message
302: Receive first message, transmit second message
303: Receive second message
304: Search for context of terminal device on the basis of temporary identifier of terminal device
305: When context of terminal device could not be acquired, transmit third message
306: Receive third message, transmit fourth message on the basis of third message, fourth message being used for responding to first message
307: Receive fourth message, transmit fifth message on the basis of fourth message
308: Receive fifth message, transmit permanent identifier of terminal device on the basis of fifth message
AA Terminal device
BB Gateway node
CC Control plane node
DD First message, carrying temporary identifier
EE Second message, carrying temporary identifier
FF Third message
GG Fourth message
HH Fifth message carrying permanent identifier of terminal device
II Permanent identifier of terminal device

(57) **Abstract:** The present application relates to the technical field of communications. Disclosed are a method and device for acquiring an identifier of a terminal device. The method comprises: a gateway node receives a first message transmitted by a terminal device and transmits a second message to a control plane node, both the first message and the second message carrying a temporary identifier of the terminal device; the gateway node receives a third message transmitted by the control plane node, the third message being transmitted by the control plane node when a permanent identifier of the terminal device could not be acquired; the gateway node transmits a fourth message to the terminal device on the basis of the third message; the gateway node receives a fifth message transmitted by the terminal device, the fifth message carrying the permanent identifier of the terminal device; and the gateway node transmits the permanent identifier to the control plane node on the basis of the fifth message. In the present application, even if a context of the terminal device is not acquired by the control plane node, same can be forwarded via the gateway node to acquire the permanent identifier, thus allowing the terminal device to be provided with the possibility of successfully accessing a network.

WO 2019/024744 A1

[见续页]

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

**(84) 指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

**本国际公布**:

— 包括国际检索报告(条约第21条(3))。

**(57) 摘要**：本申请公开了一种获取终端设备的身份标识的方法及装置，属于通信技术领域。该方法包括：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第一消息和第二消息中均携带终端设备的临时身份标识；网关节点接收控制面节点发送的第三消息，第三消息是控制面节点在无法获得终端设备的永久身份标识时发送的；网关节点根据第三消息向终端设备发送第四消息；网关节点接收终端设备发送的第五消息，第五消息携带终端设备的永久身份标识；网关节点根据第五消息向控制面节点发送永久身份标识。在本申请中，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到永久身份标识，从而使该终端设备具有成功接入网络的可能。

# 获取终端设备的身份标识的方法及装置

本申请要求于 2017 年 7 月 31 日提交中华人民共和国国家知识产权局、申请号为201710643843.7、申请名称为“获取终端设备的身份标识的方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

## 技术领域

本申请涉及通信技术领域，特别涉及一种获取终端设备的身份标识的方法及装置。

## 背景技术

当前，终端设备可以通过第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）技术接入网络，也可以通过非 3GPP 技术接入网络。其中，当终端设备接入 5G 网络时，无论是通过 3GPP 技术还是通过非 3GPP 技术接入，终端设备均需要接入和移动管理功能（Access and Mobility Management Function，AMF）节点。

在现有技术中，当终端设备通过非 3GPP 技术接入 5G 网络，且终端设备为再次注册而非首次注册时，终端设备可以与非 3GPP 合作功能（Non-3GPP Interworking Function，N3IWF）节点进行协商，以建立互联网协议安全性（Internet Protocol Security，IPsec）连接。之后，终端设备可以通过该 IPsec 连接向 N3IWF 节点发送该终端设备的临时身份标识和请求消息，其中，该请求消息是使用完整性密钥进行完整性保护的消息。N3IWF 节点根据该临时身份标识选择 AMF 节点，并将该请求消息发送至选择的 AMF 节点。AMF 节点在接收到该请求消息之后，可以对该请求消息进行完整性验证。如果选择的 AMF 节点对该完整性保护的请求消息的完整性验证通过，则说明该 AMF 节点中存储有终端设备的上下文，从而成功接入 5G 网络。其中，该上下文是指终端设备首次注册成功之后生成的信息，包括该终端设备的永久身份标识、以及安全上下文等信息。如果选择的 AMF 节点对该请求消息的完整性验证未通过，则说明该 AMF 节点未找到终端设备的上下文。在这种情况下，终端设备将无法成功接入 5G 网络。

由上述描述可知，当终端设备通过非 3GPP 技术接入 5G 网络，且终端设备为再次入网时，如果选择的 AMF 节点未找到终端设备的上下文，那么 AMF 节点无法确认终端设备的身份，那么，终端设备将无法成功接入网络。

## 发明内容

本申请实施例提供了一种获取终端设备的身份标识的方法及装置，可以用于解决相关技术中终端设备再次入网时，AMF 无法确认终端设备的身份的问题。所述技术方案如下：

第一方面，提供了一种获取终端设备的身份标识的方法，所述方法包括：

网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，所述第一消息和所述第二消息中均携带所述终端设备的临时身份标识；

所述网关节点接收所述控制面节点发送的第三消息，所述第三消息是所述控制面节点在无法获得所述终端设备的永久身份标识时发送的；

所述网关节点根据所述第三消息向所述终端设备发送第四消息，所述第四消息用于响应所述第一消息；

所述网关节点接收所述终端设备发送的第五消息，所述第五消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识。

在本申请实施例中，当控制面节点未能获取到终端设备的上下文时，可以向网关节点发送用于请求终端设备的永久身份标识的第三消息，之后，网关节点可以转发该第三消息给终端设备，从而将获取到的永久身份标识传回至该控制面节点。由此可见，在本申请实施例中，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一互联网协议安全性 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述身份请求消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

可选地，所述第五消息携带身份回复消息和所述关联参数，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，其中，所述第六消息携带所述身份回复消息和可扩展鉴权协议身份响应 EAP-AKA’/Identity-Response 消息，且所述身份回复消息和所述 EAP-AKA’/Identity-Response 消息均携带所述永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA’/Identity-Response 消息，所述 EAP-AKA’/Identity-Response 消息携带所述永久身份标识；或者，

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述终端设备的永久身份标识。

在本申请实施例中，网关节点可以直接向终端设备发送携带有身份请求消息的第四消息，来向终端设备请求永久身份标识，这样，当网关节点接收到终端设备发送的永久身份标识之后，就可以将该永久身份标识发送给控制面节点。也即是，通过网关节点的转发，

可以使控制面节点获取到永久身份标识。并且，该第四消息中还可以携带第一失败原因值，以使终端设备可以携带关联参数，进而使网关节点可以向该关联参数所指示的终端设备发送永久身份标识。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带可扩展鉴权协议身份请求 EAP-AKA’/Identity-Request 消息和第一失败原因值；

其中，所述 EAP-AKA’/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述第一失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

可选地，所述第五消息携带 EAP-AKA’/Identity-Response 消息和所述关联参数，所述 EAP-AKA’/Identity-Response 消息用于响应所述述 EAP-AKA’/Identity-Request 消息，所述 EAP-AKA’/Identity-Response 消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息；

其中，所述第六消息携带身份回复消息和所述 EAP-AKA’/Identity-Response 消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA’/Identity-Response 消息，所述 EAP-AKA’/Identity-Response 消息携带所述终端设备的永久身份标识。

网关节点可以根据身份请求消息生成 EAP-AKA’/Identity-Request 消息向终端设备请求永久身份标识，也即是，网关节点可以在触发鉴权的同时，向终端设备请求永久身份标识，将触发鉴权的过程和获取永久身份标识的过程合并在一起，减少了信令交互。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带失败消息和第一失败原因值；

其中，所述失败消息用于指示获取所述终端设备的上下文失败，所述第一失败原因值用于告知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

可选地，所述第五消息携带注册请求消息和所述关联参数，所述注册请求消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标

识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带可扩展鉴权协议身份请求 EAP-AKA’/Identity-Request 消息，所述可扩展鉴权协议身份请求 EAP-AKA’/Identity-Request 消息用于触发对所述终端设备的鉴权流程时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述可扩展鉴权协议身份请求 EAP-AKA’/Identity-Request 消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

可选地，所述第五消息携带可扩展鉴权协议身份响应 EAP-AKA’/Identity-Response 消息和所述关联参数，所述 EAP-AKA’/Identity-Response 消息用于响应所述 EAP-AKA’/Identity-Request 消息，所述 EAP-AKA’/Identity-Response 消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带所述 EAP-AKA’/Identity-Response 消息。

在本申请实施例中，控制面节点在获取终端设备的上下文失败之后，可以直接触发鉴权，将鉴权流程和获取终端设备的永久身份标识的过程合并，减少了信令交互。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息携带失败消息，且所述失败消息用于指示所述控制面节点无法确定终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述失败消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败。

可选地，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带通知消息，且所述通知消息用于向所述网关节点通知所述控制面节点无法确定所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带注册拒绝消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败。

可选地，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标

识，包括：

所述网关节点向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息；

或者，

所述网关节点向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息和 EAP-AKA’/Identity-Response 消息，所述 EAP-AKA’/Identity-Response 消息用于触发对所述终端设备的鉴权流程。

在本申请实施例中，网关节点可以将注册请求消息和 EAP-AKA’/Identity-Response 一起发，控制面节点可以在获取到终端设备的永久身份标识的同时，开始对终端设备鉴权，减少了信令交互。

第二方面，提供了一种获取终端设备的身份标识的方法，所述方法包括：

终端设备向网关节点发送第一消息，所述第一消息中携带所述终端设备的临时身份标识；

所述终端设备接收所述网关节点发送的第四消息，所述第四消息用于响应所述第一消息；

所述终端设备根据所述第四消息向所述网关节点发送第五消息，所述第五消息携带所述终端设备的永久身份标识。

在本申请实施例中，当终端设备接收到第四消息时，可以向网关节点回复携带有永久身份标识的第五消息，以便网关节点向控制面节点发送该永久身份标识，这样，终端设备即具有了成功接入网络的可能。

可选地，所述终端设备根据所述第四消息向所述网关节点发送第五消息，包括：

当所述第四消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带可扩展鉴权协议身份请求 EAP-AKA’/Identity-Request 消息，且所述 EAP-AKA’/Identity-Request 消息用于触发对所述终端设备的鉴权流程时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带可扩展鉴权协议身份响应 EAP-AKA’/Identity-Response 消息，所述 EAP-AKA’/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述可扩展鉴权协议身份 EAP-AKA’/Identity-Response 用于响应所述 EAP-AKA’/Identity-Request 消息，所述 EAP-AKA’/Identity-Response 消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带失败消息，且所述失败消息用于指示所述控制面节点无法确定所述终端设备的永久身份标识时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

可选地，所述第四消息中还携带第一失败原因值，所述第一失败原因值用于通知所述终端设备第一IPsec连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以，关联所述第一 IPsec 连接和第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后

建立的 IPsec 连接；

在所述终端设备向所述网关节点发送所述第五消息之前，还包括：

所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，并建立所述终端设备与所述网关节点之间的第二 IPsec 连接；

所述终端设备向所述网关节点发送所述第五消息，包括：

所述终端设备通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息还携带关联参数，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数。

可选地，所述关联参数为全球唯一临时用户设备标识 GUTI、安全参数索引 SPI 或者 Cookie。

可选地，所述终端设备根据所述第四消息向所述网关节点发送第五消息，包括：

当所述第四消息中携带第二失败原因值和失败消息，所述第二失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述失败消息用于通知所述终端设备所述控制面节点无法确定所述终端设备的永久身份标识时，所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，建立与所述网关节点的之间的第二 IPsec 连接，并通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带第二失败原因值和注册拒绝消息，所述第二失败原因值用于通知所述终端设备第一 IPsec 连接失败时，所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，建立与所述网关节点之间的第二 IPsec 连接，并通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

第三方面，提供了一种获取终端设备的身份标识的方法，所述方法包括：

控制面节点接收网关节点发送的第二消息，所述第二消息中携带终端设备的临时身份标识；

所述控制面节点根据所述临时身份标识查找所述终端设备的上下文；

当所述控制面节点未获取到所述终端设备的上下文时，向所述网关节点发送第三消息；

所述控制面节点接收所述网关节点发送的所述终端设备的永久身份标识。

在本申请实施例中，控制面节点在未获取到终端设备的上下文时，可以网关节点发送第三消息，以便网关节点根据该第三消息向终端设备请求永久身份标识。这样，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能。

第四方面，提供了一种获取终端设备的身份标识的装置，所述装置具有实现上述第一方面中获取终端设备的身份标识的方法行为的功能。所述装置包括至少一个模块，该至少一个模块用于实现上述第一方面所提供的获取终端设备的身份标识的方法。

第五方面，提供了一种获取终端设备的身份标识的装置，所述装置具有实现上述第二

方面中获取终端设备的身份标识的方法行为的功能。所述装置包括至少一个模块，该至少一个模块用于实现上述第二方面所提供的获取终端设备的身份标识的方法。

第六方面，提供了一种获取终端设备的身份标识的装置，所述装置具有实现上述第三方面中获取终端设备的身份标识的方法行为的功能。所述装置包括至少一个模块，该至少一个模块用于实现上述第一方面所提供的获取终端设备的身份标识的方法。

第七方面，提供了一种获取终端设备的身份标识的装置，所述装置的结构中包括处理器和存储器，所述存储器用于存储支持所述装置执行上述第一方面所提供的获取终端设备的身份标识的方法的程序，以及存储用于实现上述第一方面所提供的获取终端设备的身份标识的方法所涉及的数据。所述处理器被配置为用于执行所述存储器中存储的程序。所述存储设备的操作装置还可以包括通信总线，该通信总线用于该处理器与存储器之间建立连接。

第八方面，提供了一种获取终端设备的身份标识的装置，所述装置的结构中包括处理器和存储器，所述存储器用于存储支持所述装置执行上述第二方面所提供的获取终端设备的身份标识的方法的程序，以及存储用于实现上述第二方面所提供的获取终端设备的身份标识的方法所涉及的数据。所述处理器被配置为用于执行所述存储器中存储的程序。所述存储设备的操作装置还可以包括通信总线，该通信总线用于该处理器与存储器之间建立连接。

第九方面，提供了一种获取终端设备的身份标识的装置，所述装置的结构中包括处理器和存储器，所述存储器用于存储支持所述装置执行上述第三方面所提供的获取终端设备的身份标识的方法的程序，以及存储用于实现上述第三方面所提供的获取终端设备的身份标识的方法所涉及的数据。所述处理器被配置为用于执行所述存储器中存储的程序。所述存储设备的操作装置还可以包括通信总线，该通信总线用于该处理器与存储器之间建立连接。

第十方面，提供了一种计算机可读存储介质，所述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，使得计算机执行上述第一方面所述的获取终端设备的身份标识的方法。

第十一方面，提供了一种计算机可读存储介质，所述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，使得计算机执行上述第二方面所述的获取终端设备的身份标识的方法。

第十二方面，提供了一种计算机可读存储介质，所述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，使得计算机执行上述第三方面所述的获取终端设备的身份标识的方法。

第十三方面，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，使得计算机执行上述第一方面所述的获取终端设备的身份标识的方法。

第十四方面，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，使得计算机执行上述第二方面所述的获取终端设备的身份标识的方法。

第十五方面，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，使得计算机执行上述第三方面所述的获取终端设备的身份标识的方法。

上述第四至十五方面所获得的技术效果与第一方面、第二方面和第三方面中对应的技术手段获得的技术效果近似，在这里不再赘述。

本申请提供的技术方案带来的有益效果至少包括：在本申请实施例中，当控制面节点未能获取到终端设备的上下文时，可以向网关节点发送用于请求终端设备的永久身份标识的第三消息，之后，网关节点可以转发该第三消息给终端设备，从而将获取到的永久身份标识传回至该控制面节点。由此可见，在本申请实施例中，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。

## 附图说明

图 1 是本申请实施例提供的一种系统结构图；

图 2A 是本申请实施例提供的一种装置的结构示意图；

图 2B 是本申请实施例提供的一种终端设备的结构示意图；

图 3 是本申请实施例提供的一种获取终端设备的身份标识的流程图；

图 4 是本申请实施例提供的一种获取终端设备的身份标识的流程图；

图 5 是本申请实施例提供的一种获取终端设备的身份标识的流程图；

图 6 是本申请实施例提供的一种获取终端设备的身份标识的流程图；

图 7 是本申请实施例提供的一种获取终端设备的身份标识的流程图；

图 8 是本申请实施例提供的获取终端设备的身份标识的装置的结构示意图；

图 9 是本申请实施例提供的获取终端设备的身份标识的装置的结构示意图；

图 10 是本申请实施例提供的获取终端设备的身份标识的装置的结构示意图。

## 具体实施方式

为使本申请的目的、技术方案和优点更加清楚，下面将结合附图对本申请实施方式作进一步地详细描述。

在对本申请实施例进行详细的解释说明之前，先对本申请实施例涉及的应用场景予以介绍。

当前，终端设备可以通过 3GPP 技术接入网络，也可以通过非 3GPP 技术接入网络。其中，3GPP 技术是指通过 3GPP 标准制定的空口技术，如我们常用的 3G、4G 和 5G 网络的

空口接入技术即为 3GPP 技术。而剩余的不是通过 3GPP 标准制定的空口接入技术，即为非 3GPP 技术。例如，以无线保真接入节点（Wireless Fidelity Access Point， WIFI AP）为代表的空口技术。

目前，非 3GPP 技术可以进一步分为可信非 3GPP 技术和非可信非 3GPP 技术。其中，可信非 3GPP 技术是指非 3GPP 接入节点和后面的网关节点是由同一个运营商部署的，例如，如图 1 所示的系统架构中，如果 Non-3GPP 接入节点和 N3IWF 节点均是由同一个运营商部署的，那么，该非 3GPP 技术即为可信非 3GPP 技术。而除此之外的非 3GPP 技术则均为非可信非 3GPP 技术，例如，如果图 1 所示的架构中 Non-3GPP 接入节点和 N3IWF 节点不是由同一个运营商部署的，那么，该非 3GPP 技术即为非可信非 3GPP 技术。

无论终端设备通过 3GPP 技术接入网络，还是通过非 3GPP 技术接入网络，终端设备均可以通过控制面节点进行鉴权。具体地，当终端设备通过控制面节点进行鉴权时，控制面节点需要获取终端设备的永久身份标识。

在现有技术中，当终端设备通过非 3GPP 技术接入网络，且终端设备为再次注册而非首次注册时，终端设备可以通过网关节点向控制面节点发送携带有临时身份标识的注册请求消息，并且该注册请求消息是经过完整性保护的。控制面节点可以根据该临时身份标识查找该终端设备的上下文。如果该控制面节点为终端设备首次注册时的控制面节点，且该终端设备首次注册时的控制面节点存储有该终端设备的上下文，那么，该控制面节点可以根据查找到的该终端设备的上下文对注册请求消息进行完整性验证，从而使终端设备成功接入网络。而如果由于终端设备移动的原因，当前选择的控制面节点中未存储有终端设备的上下文，也即是，该控制面节点并非终端设备首次注册时的控制面节点，此时，该控制面节点将无法获取到终端设备的上下文，显然，也就无法获取到终端设备的永久身份标识。而本申请实施例提供的获取终端设备的身份标识的方法即可以用于该种场景下，用于解决控制面节点未查找到终端设备上下文时如何获取该终端设备的永久身份标识的问题。

在对本申请实施例涉及的应用场景进行介绍之后，接下来，对本申请实施例涉及的系统架构进行介绍。

本申请实施例提供的获取终端设备的身份标识的方法可以应用于任何有获取终端设备身份标识需求的通信系统，例如，可以应用于图 1 所示的系统中。

如图 1 所示，该系统可以包括终端设备、非第三代合作伙伴计划（Non-3rd Generation Partnership Project，Non-3GPP）接入节点、N3IWF 节点、数据网络（data network，DN）以及下述多个网络功能（network functions，NF）节点：鉴权服务器功能（authentication server function，AUSF）节点、统一数据管理（unified data management，UDM）节点、接入和移动管理功能（Access and Mobility Management Function，AMF）节点、会话管理功能（Session Management Function，SMF）节点、PCF 节点、应用功能（application function，AF）节点、用户面功能（User Plane Function，UPF）节点。可理解的是，图 1 仅为示例性架构图，除图 1 所示功能节点之外，该系统还可以包括其他功能节点，本申请实施例对此不进行限定。

在图 1 所示的系统中，各功能节点之间可以通过下一代网络（next generation，NG）接口建立连接实现通信，如：终端设备可以通过 N 接口 1（简称 N1）与 AMF 节点建立控制面信令连接，AN/RAN 节点可以通过 N 接口 3（简称 N3）与 UPF 节点建立用户面数据连接，

N3IWF 节点可以通过 N 接口 2（简称 N2）与 AMF 节点建立控制面信令连接，UPF 节点可以通过 N 接口 4（简称 N4）与 SMF 节点建立控制面信令连接，UPF 节点可以通过 N 接口 6（简称 N6）与 DN 节点交互用户面数据，AMF 节点可以通过 N 接口 8（简称 N8）与 UDM 节点建立控制面信令连接，AMF 节点可以通过 N 接口 12（简称 N12）与 AUSF 节点建立控制面信令连接，AMF 节点可以通过 N 接口 11（简称 N11）与 SMF 节点建立控制面信令连接，SMF 节点可以通过 N 接口 7（简称 N7）与 PCF 节点建立控制面信令连接， PCF 节点可以通过 N 接口 5（简称 N5）与 AF 节点建立控制面信令连接，AUSF 节点可以通过 N 接口 13（简称 N13）与 UDM 节点建立控制面信令连接。

其中，图 1 中的终端设备可以为 UE，还可以为蜂窝电话、无绳电话、会话发起协议(session initiation protocol，SIP)电话、智能电话、无线本地环路(wireless local loop，WLL)站、个人数字助理(personal digital assistant，PDA)、膝上型计算机、手持式通信设备、手持式计算设备、卫星无线设备、无线调制解调器卡和/或用于在无线系统上进行通信的其它设备。Non-3GPP 节点为由多个节点组成的网络，用于实现无线物理层功能、资源调度和无线资源管理、无线接入控制以及移动性管理功能备。UDM 节点、AUSF 节点、PCF 节点、AMF 节点、SMF 节点、UPF 节点可统称为 NF 节点，其中，NF 节点中的 AMF 节点、PCF 节点可称为控制面（control plane，CP）节点，UPF 节点可以称为用户面功能（user plane function，UPF）节点。NF 节点中除 UPF 节点之外的节点可以独立工作，也可以组合在一起实现某些控制功能，如：这些节点组合在一起后可以完成终端设备的接入鉴权、安全加密、位置注册等接入控制和移动性管理功能，以及用户面传输路径的建立、释放和更改等会话管理功能，以及分析一些切片（slice）相关的数据（如拥塞）、终端设备相关的数据的功能。UPF 节点主要完成用户面数据的路由转发等功能，如：负责对终端设备的数据报文过滤、数据传输/转发、速率控制、生成计费信息等。

具体的，N3IWF 节点为终端设备从非 3GPP 技术接入时需要连接的节点，并且，N3IWF 节点可以与终端设备建立互联网协议安全性（Internet Protocol Security，IPsec）连接，并通过该 IPsec 连接传输信令。另外，N3IWF 节点可以将终端设备发送的 NAS 消息转发给 AMF 节点。AMF 节点主要负责移动性管理，当前， AMF 节点还集成有安全锚点功能（Security Anchor Function，SEAF）模块，该 SEAF 模块主要负责向 AUSF 节点发起鉴权请求，在演进分组系统鉴权过程中完成网络侧对终端的验证。AUSF 节点的主要功能是接收 SEAF 模块发送的鉴权请求，选择鉴权方法。当采用可扩展鉴权协议的鉴权方法的时候，AUSF 节点主要负责完成网络侧对终端的鉴权；并且，AUSF 节点可以向 ARPF 节点请求鉴权向量，并且回复鉴权响应给 SEAF 模块。ARPF 节点的主要功能是存储长期密钥，接收 AUSF 节点发送的鉴权向量请求，使用存储的长期密钥计算鉴权向量，并将鉴权向量发送至 AUSF 节点。

具体的，图 1 中 AMF 节点、UDM 节点、AUSF 节点、PCF 节点、SMF 节点和 UPF 节点均可称为网络功能节点，具体可以包含图 2A 所示的部件。图 2A 是本申请实施例提供的一种装置的结构示意图。该装置可以是图 1 中的各网络功能节点。参见图 2A，该装置可以包括至少一个处理器 201，通信总线 202，存储器 203 以及至少一个通信接口 204。需要说明的是，图 2A 示出的设备结构并不构成对网络功能节点的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，本申请实施例对此不进行限定。下

面结合图 2A 对网络功能节点的各个构成部件进行具体的介绍：

处理器 201 是该装置的控制中心，可以是一个处理器，也可以是多个处理元件的统称。例如，处理器 201 可以是一个通用中央处理器（Central Processing Unit，CPU），或特定应用集成电路（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，例如：一个或多个微处理器（digital signal processor，DSP），或，一个或者多个现场可编程门阵列（field programmable gate array，FPGA）。其中，处理器 201 可以通过运行或执行存储在存储器 203 内的软件程序，以及调用存储在存储器 203 内的数据，执行网络功能节点的各种功能。例如，图 3 所示的实施例中网关节点或控制面节点的动作即可以通过对应的网络功能节点的处理器调用存储器内的数据来执行。

在具体实现中，作为一种实施例，处理器 201 可以包括一个或多个 CPU，例如图 2A 中所示的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，网络功能节点可以包括多个处理器，例如图 2A 中所示的处理器 201 和处理器 205。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。

通信总线 202 可包括一通路，在上述组件之间传送信息。该通信总线 202 可以是工业标准体系结构(industry standard architecture, ISA)总线、外部设备互连(peripheral component, PCI）总线或扩展工业标准体系结构（extended industry standard architecture，EISA）总线等。该总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 2A 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 203 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它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它类型的动态存储设备，也可以是电可擦可编程只读存储器（Electrically Erasable Programmable Read-Only Memory，EEPROM）、只读光盘（Compact Disc Read-Only Memory，CD-ROM）或其它光盘存储、光碟存储（包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等）、磁盘存储介质或者其它磁存储设备、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它介质，但不限于此。存储器 203 可以是独立存在，通过通信总线 202 与处理器 201 相连接。存储器 203 也可以和处理器 201 集成在一起。其中，所述存储器 203 用于存储执行本申请实施例提供的方案的软件程序，并由处理器 201 来控制执行。

通信接口 204，用于与其他设备或通信网络通信，如以太网，RAN，无线局域网（wireless local area networks，WLAN）等。通信接口 33 可以包括接收单元实现接收功能，以及发送单元实现发送功能。

在具体实现中，作为一种实施例，网络功能节点还可以包括输出设备 206 和输入设备 207。输出设备 206 和处理器 201 通信，可以以多种方式来显示信息。例如，输出设备 206 可以是液晶显示器（liquid crystal display，LCD），发光二级管（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 207 和处理器 201 通信，可以以多种方式接收用户的输入。例如，输入设备 207 可以是鼠标、键盘、触摸屏设备或传感设备等。

上述的网络功能节点可以是一个通用计算机设备或者是一个专用计算机设备。在具体实现中，可以是台式机、便携式电脑、网络服务器等。

具体的，图 1 中的终端设备可以包含图 2B 所示的部件。图 2B 是本申请实施例提供的一种终端设备的结构示意图。该终端设备可以是图 1 中的终端设备。参见图 2B，该终端设备可以包括处理器、用户接口、一个或多个连接电路模块和存储器。需要说明的是，图 2B 示出的设备结构并不构成对网络功能节点的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，本申请实施例对此不进行限定。下面结合图 2B 对网络功能节点的各个构成部件进行具体的介绍：

处理器可以包括用于终端设备的音频/视频和逻辑功能的电路。例如，处理器可以包括数字信号处理器设备、微处理器设备、模数转换器、数模转换器等等。可以根据这些设备各自的能力而在这些设备之间分配移动设备的控制和信号处理功能。处理器还可以包括内部语音编码器 VC、内部数据调制解调器 DM 等等。此外，处理器可以包括操作一个或多个软件程序的功能，所述软件程序可以存储在存储器中。通常，处理器和所存储的软件指令可以被配置为使终端设备执行动作。例如，处理器和所存储的软件指令可以被配置为执行图 3 所示的实施例中终端设备所执行的动作。

终端设备还可以包括用户接口，其例如可以包括耳机或扬声器、麦克风、输出装置（例如显示器）、输入装置等等，其可操作地耦合到处理器。在这一点上，处理器可以包括用户接口电路，其被配置为至少控制所述用户接口的一个或多个元件(诸如扬声器、麦克风、显示器等等)的一些功能。处理器和/或包括处理器的用户接口电路可以被配置为通过存储在处理器可访问的存储器中的计算机程序指令(例如软件和/或固件)来控制用户接口的一个或多个元件的一个或多个功能。尽管并未示出，但是终端设备可以包括用于向与移动设备相关的各种电路供电的电池，所述电路例如为提供机械振动来作为可检测输出的电路。输入装置可以包括允许所述装置接收数据的设备，诸如小键盘、触摸显示器、游戏杆和/或至少一个其他输入设备等。

终端设备还可以包括用于共享和/或获得数据的一个或多个连接电路模块。例如，所述终端设备可以包括短距射频 RF 收发机和/或检测器，从而可以根据 RF 技术与电子设备共享和/或从电子设备获得数据。所述终端设备可以包括其他短距收发机，诸如例如红外 IR 收发机、使用收发机、无线通用串行总线 USB 收发机等等。蓝牙收发机能够根据低功耗或超低功耗蓝牙技术操作。在这一点上，终端设备并且更具体地是短距收发机能够向和/或从在所述装置附近(诸如在 10 米内)的电子设备发送和/或接收数据。尽管并未示出，所述终端设备能够根据各种无线联网技术来向和/或从电子设备发送和/或接收数据，这些技术包括: Wi-Fi、Wi-Fi 低功耗、WLAN 技术，诸如 IEEE 802.11 技术、IEEE 802.15 技术、IEEE 802.16 技术等等。

终端设备可以包括可存储与移动用户相关的信息元素的存储器，诸如用户身份模块 SIM。除了 SIM，所述装置还可以包括其他可移除和/或固定存储器。终端设备可以包括易失性存储器和/或非易失性存储器。例如，易失性存储器可以包括随机存取存储器 RAM，其包括动态 RAM 和/或静态 RAM、芯片上和/或芯片外高速缓冲存储器等等。非易失性存储器可以是嵌入式的和/或可移除的，其可以包括例如只读存储器、闪存存储器、磁性存储设备，

例如硬盘、软盘驱动器、磁带等等、光盘驱动器和/或介质、非易失性随机存取存储器 NVRAM 等等。类似于易失性存储器，非易失性存储器可以包括用于数据的暂时存储的高速缓冲区域。易失性和/或非易失性存储器的至少一部分可以嵌入到处理器中。存储器可以存储一个或多个软件程序、指令、信息块、数据等等，其可以由所述终端设备用来执行移动终端的功能。例如，图 3 所示的实施例中终端设备的动作即可以通过处理器调用存储器内的软件程序、指令、信息块、数据等来执行。具体的，例如，存储器可以包括能够唯一标识终端设备的标识符，诸如国际移动设备标志 IMEI 码，还可以存储有国际移动用户标识码 IMSI 等。

在对本申请实施例涉及的应用场景和系统架构进行介绍之后，接下来对本申请实施例的具体实现过程进行详细的解释说明。

图 3 是本申请实施例提供的一种获取终端设备的身份标识的方法的流程图。参见图 3，该方法包括以下步骤：

步骤 301：终端设备向网关节点发送第一消息，第一消息中携带终端设备的临时身份标识。

其中，终端设备可以为图 1 所示的系统架构中的终端设备，该网关节点可以用于与终端设备建立 IPsec 隧道连接，并将终端设备发送的 NAS 消息转发给控制面节点。其中，该控制面节点可以为图 1 中所示的 AMF 节点或者 LTE 系统中的 MME，或者其他 3GPP 系统中的负责接入和移动性管理的功能的网元或功能实体。

具体的，该网关节点可以为图 1 所示的 N3IWF 节点。

需要说明的是，该终端设备还可以为应用于 LTE 系统或其他 3GPP 系统中的终端设备，该网关节点同样可以为应用于 LTE 系统和其他 3GPP 系统中的网关节点，例如，该网关节点可以为 LTE 网络的 ePDG 节点。

其中，第一消息中可以携带有请求消息，该请求消息具体可以是注册请求消息，服务请求消息或者会话建立请求消息。该请求消息中携带终端设备的临时身份标识。

其中，第一消息具体可以是第二版本互联网密钥交换协议（Internet Key Exchange protocol Version 2，IKEv2）消息。例如，该消息为第二版本互联网密钥交换协议鉴权请求（Internet Key Exchange protocol Version 2- Authentication –Request，IKEv2-AUTH- Request）消息。终端设备的临时身份标识可以用于标识终端设备，是由 AMF、MME 在终端设备首次入网的时候分配给 UE，以避免终端设备的永久身份标识被过多的使用，造成隐私泄露。该临时身份标识可以包含有分配这个临时身份标识的控制面节点的地址信息。该临时身份标识具体可以是，如 5G 系统的临时身份标识，LTE 系统中的全球唯一用户设备标识（Globally Unique Temporary User Equipment Identity，GUTI），系统架构演进临时移动用户标识（System Architecture Evolution- Temporary Mobile Subscriber Identity，S-TMSI）。

例如，当终端设备再次注册到网络时，发送该第一消息，该第一消息携带有注册请求消息，该注册请求消息中携带临时身份标识；再例如，当终端设备请求网络提供服务时，发送该第一消息，该第一消息携带服务请求消息，该服务请求消息中携带临时身份标识，如 GUIT 或 S-TMSI；再例如，当终端设备请求建立会话时，发送该第一消息，该第一消息携带会话建立请求，该会话建立请求中携带定义临时身份标识。

可选地，在步骤 301 之前，还包括：终端设备和该网关节点协商建立 IPsec 连接。

进而，步骤 301 中通过该 IPsec 连接发送该第一消息。

示例性地，当终端设备通过非 3GPP 技术接入如图 1 所示的网络时，该网关节点和非 3GPP 接入节点，如 wifi AP 不是由同一个运营商部署的。在这种情况下，对于网关节点而言，该非 3GPP 接入节点是不可信的，所以，当终端设备和该网关节点进行信令交互之前，终端设备和网关节点之间可以协商建立 IPsec 连接，当建立 IPsec 连接之后，终端设备和网关节点之间可以通过该 IPsec 连接进行信令交互，从而起到对传输的信令保护的作用。

具体的，终端设备向网关节点发送第一消息的详细实现过程将通过下述实施例中步骤 401 中进行详细的解释说明。

步骤 302：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第二消息中携带终端设备的临时身份标识。

其中，该控制面节点可以为图 1 中所示的 AMF 节点或者 LTE 系统中的 MME，或者其他 3GPP 系统中的负责接入和移动性管理的功能的网元或功能实体。

示例性地，当网关节点接收到终端设备发送的第一消息时，可以将该第一消息中携带的请求消息作为第二消息中的消息的部分或全部发送至控制面节点。

其中，该第二消息可以包含前述第一消息中携带的请求消息，例如，第二消息可以包含注册请求消息或服务请求消息等消息。

具体的，本步骤的详细实现过程将通过下述实施例中的步骤 402 进行解释说明。

步骤 303：控制面节点接收网关节点发送的第二消息。

步骤 304：控制面节点根据终端设备的临时身份标识，查找该终端设备的上下文。

示例性地，控制面节点在接收到第二消息时，即可以确定终端设备所要请求的服务，如注册服务、服务请求等，此时，控制面节点可以根据该第二消息中的临时身份标识查找该终端设备的上下文，以便根据该终端设备的上下文对该终端设备进行验证并提供服务。

在一种可选的方案中，AMF 节点存储有该终端设备的上下文信息。具体地，AMF 可以根据终端设备的临时身份标识，获取终端设备的上下文信息。

在另一种可选的方案中，AMF 节点向其他控制面节点请求该终端设备的上下文信息。具体地，AMF 节点可以将前述的请求消息转发至其他控制面板节点，等待其他控制面节点回复响应消息，该响应消息中可以携带该终端设备的上下文信息。进一步地，AMF 节点可以根据该终端设备的临时身份标识确定其他控制面节点，从而从其他控制面节点获取该终端设备的上下文。

其中，该终端设备的上下文中可以包括该终端设备的永久身份标识。

具体的，本步骤的详细实现过程将通过下述实施例中的步骤 404 进行解释说明。

步骤 305：当控制面节点无法获得终端设备的上下文时，向网关节点发送第三消息。

其中，第三消息可以用于通知终端设备无法确定该终端设备的永久身份标识。可替换地，第三消息可以用于向终端设备请求永久身份标识，或者，用于通知终端请求的服务失败；或者，用于通知终端设备无法获取到或无法查找到或未存储该终端设备的永久身份标识。

具体的，该第三消息可以为 N2 消息。

例如，当控制面节点未获取到终端设备的上下文（例如，自身未存储，或向其他控制

面节点请求该终端设备的上下文信息失败）时，表明该控制面节点无法确定所述终端设备的真实身份，因此，该控制面节点无法为该终端设备提供请求的服务。

其中，第三消息可以携带身份请求消息，或可扩展鉴权协议身份请求（Extensible Authentication Protocol /Identity-Request，EAP-AKA'/Identity-Request）消息，或失败消息，或通知消息中的一种或多种。该身份请求消息可以用于请求终端设备的永久身份标识；该EAP-AKA'/Identity-Request 消息可以用于触发对终端设备的鉴权流程，从而间接向终端设备请求永久身份标识；该失败消息可以用于通知该终端设备请求的服务失败。

可选地，失败消息携带有原因值，该终端设备可以通过查看该失败消息携带的原因值来确定请求的服务失败的原因。比如，请求的服务失败的原因可以是无法确定该终端设备的永久身份。

可选地，该通知消息可以用于向网关节点通知控制面节点无法获得终端设备的永久身份。具体的。该通知消息还可以向网关节点通知控制面节点发送的第三消息的内容或向网关节点通知应该采取的动作。比如，当控制面节点可以获取该终端设备的上下文的时候，该通知消息携带密钥信息，网关节点根据携带的密钥信息对该终端设备进行认证；当控制面节点无法获取该终端设备的上下文的时候，该通知消息不携带密钥信息，用于告知网关节点该控制面节点对该终端设备无法认证。再比如，该通知消息可以是原因值，进一步地，网关节点可以根据携带的原因值，在再次收到该终端设备发来的消息时，将接收到的该终端设备的消息发给该控制面节点。

可选地，当第三消息为 N2 消息时，该身份请求消息、EAP-AKA'/Identity-Request 消息和失败消息，可以放到该 N2 消息中的 NAS 容器中。

可选地，通知消息可以放到该 N2 消息的 NAS 容器外。

具体的，本步骤可以包括多种可能的实现方式，该多种可能的实现方式将分别通过后续实施例中的步骤 404，步骤 504，步骤 604，和步骤 704 进行详细的解释说明。

步骤 306：网关节点接收控制面节点发送的第三消息，并根据第三消息向终端设备发送第四消息，第四消息用于响应第一消息。

示例性地，当网关节点接收到控制面节点发送的第三消息时，根据该第三消息向终端设备发送第四消息，该第四消息可以用于请求终端设备的永久身份标识。

其中，该第四消息可以是第二版本互联网密钥交换协议鉴权响应（Internet Key Exchange protocol Version 2- Authentication –Request，IKEv2-AUTH- Response）消息，该 IKEv2-AUTH-Response 消息用于回复第一消息。

其中，该第四消息可以携带身份请求消息和第一失败原因值，或者可以携带EAP-AKA'/Identity-Request 消息和第一失败原因值，或者可以携带失败消息和第一失败原因值，或者可以携带失败消息和第二失败原因值，或者可以携带注册拒绝消息和第二失败原因值，其中，该注册拒绝消息可以是失败消息的一种。

需要说明的是，第一失败原因值可以用于通知终端设备第一 IPsec 连接失败，可选地，第一失败原因值还可以用于终端设备根据第一原因值确定关联参数，并发送关联参数给网关节点，网关节点根据关联参数关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后再次建立的 IPsec 连接。

其中，当第三消息中携带的内容不同时，第四消息也可以携带相应的不同的内容。具

体的，本步骤可能存在的具体实现方式将分别通过下述实施例中的步骤406、步骤506、步骤606和步骤706进行详细的解释说明。

步骤307：终端设备接收网关节点发送的第四消息，并根据第四消息向网关节点发送第五消息，第五消息携带终端设备的永久身份标识。

其中，第五消息可以是IKEv2-AUTH-Request消息，可以携带身份回复消息，该身份回复消息携带终端设备的永久身份标识；或者，该第五消息可以携带可扩展鉴权协议身份响应（Extensible Authentication Protocol /Identity-Response ，EAP-AKA'/Identity-Response）消息，该EAP-AKA'/Identity-Response携带终端设备的永久身份标识；或者可以携带注册请求消息，该注册请求消息携带终端设备的永久身份标识。

可选的，第五消息还可以携带关联参数，该关联参数用于关联第一 IPsec 连接和第二IPsec 连接，使网关节点可以将通过不同 IPsec 连接发送的消息发往同一个控制面节点。具体的，网关节点可以通过该关联参数确定将第五消息中携带永久身份标识的消息发往哪个控制面节点。比如，该关联参数可以是终端设备之前在第一消息中携带过的临时身份标识，还可以为建立第一 IPsec 连接时的安全索引参数（Security Parameter Index，SPI），或者Cookies。可选的，终端设备可以将该临时身份标识放到网络访问标识符（Network Access Identifier，NAI），中。网关节点可以根据临时身份标识中的信息，将携带永久身份标识的消息发给控制面节点。

其中，该终端设备的永久身份标识可以为该终端设备的国际移动用户识别码（International Mobile Subscriber Identification Number，IMSI），或者可以为永久签约身份（Subscriber permanent Identity, SUPI）。

在本步骤中，第五消息携带的内容可以有多种可能性，携带不同内容时对应的实现方式将分别通过后续实施例中的步骤407、步骤507、步骤607和步骤707进行详细的解释说明。

步骤308：网关节点接收终端设备发送的第五消息，根据第五消息向控制面节点发送终端设备的永久身份标识。

其中，网关节点可以根据第五消息携带的内容的不同，通过不同的方式向控制面节点发送终端设备的永久身份标识，具体的可能的实现方式将分别通过后续实施例中的步骤408、步骤508、步骤608和步骤708进行详细的解释说明。

在本申请实施例中，当控制面节点未能获取到终端设备的上下文时，可以向网关节点发送包含有用于请求终端设备的永久身份标识的第三消息，之后，网关节点可以转发该第三消息中的含有请求终端设备的永久身份标识的消息给终端设备，从而将获取到的永久身份标识传回至该控制面节点。由此可见，在本申请实施例中，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。

在第一种可能的实现方式中，当第三消息中携带身份请求消息，且身份请求消息用于请求终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一互联网协议安全性IPsec连接向终端设备发送第四消息，第四消息携带身份请求消息。

可选地，第四消息还携带第一失败原因值，其中，第一失败原因值用于通知终端设备

第一 IPsec 连接失败，第一失败原因值还用于关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

相应地，当第四消息中携带身份请求消息，且身份请求消息用于请求终端设备的永久身份标识时，终端设备向网关节点发送第五消息，第五消息携带身份回复消息，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识；

相应地，当第四消息还携带第一失败原因值时，在终端设备向网关节点发送第五消息之前，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，并建立终端设备与网关节点之间的第二 IPsec 连接；

终端设备通过第二 IPsec 连接向网关节点发送第五消息，第五消息还携带关联参数，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数。

相应地，当第五消息携带身份回复消息和关联参数时，网关节点向该关联参数所指示的控制面节点发送第六消息，其中，第六消息携带身份回复消息和可扩展鉴权协议身份响应 EAP-AKA'/Identity-Response 消息，且身份回复消息和 EAP-AKA'/Identity-Response 消息均携带永久身份标识；或者，第六消息携带身份回复消息，身份回复消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息携带永久身份标识；

或者，当第五消息携带身份回复消息和关联参数时，网关节点根据该关联参数向控制面节点发送第六消息，第六消息携带身份回复消息，身份回复消息携带终端设备的永久身份标识。

在该种实现方式中，网关节点可以直接向终端设备发送携带有身份请求消息的第四消息，来向终端设备请求永久身份标识，这样，当网关节点接收到终端设备发送的永久身份标识之后，就可以将该永久身份标识发送给控制面节点。也即是，通过网关节点的转发，可以使控制面节点获取到永久身份标识。并且，该第四消息中还可以携带第一失败原因值，以使终端设备可以携带关联参数，进而使网关节点可以向该关联参数所指示的终端设备发送永久身份标识。

在第二种可能的实现方式中，当第三消息中携带身份请求消息，且身份请求消息用于请求终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息和第一失败原因值。

其中，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程，第一失败原因值用于通知终端设备第一 IPsec 连接失败，第一失败原因值还用于终端设备根据第一原因值确定关联参数，并发送关联参数给网关节点，网关节点根据关联参数关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后再次建立的 IPsec 连接。

相应地，当第四消息中携带 EAP-AKA'/Identity-Request 消息，且 EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程时，终端设备向网关节点发送第五消息，第五消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程，可扩展鉴权协议身份 EAP-AKA'/Identity-Response 用于响应 EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识；

相应地，当第四消息还携带第一失败原因值时，在终端设备向网关节点发送第五消息之前，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，并建立终端设备与网关节点之间的第二 IPsec 连接。

进而，终端设备通过第二 IPsec 连接向网关节点发送第五消息，第五消息还携带关联参数，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数。

相应地，当第五消息携带 EAP-AKA'/Identity-Response 消息和关联参数，网关节点根据该关联参数向控制面节点发送第六消息；

其中，第六消息携带身份回复消息和 EAP-AKA'/Identity-Response 消息，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识；或者，第六消息携带身份回复消息，身份回复消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

在该种实现方式中，网关节点可以根据身份请求消息生成 EAP-AKA'/Identity-Request 消息向终端设备请求永久身份标识，也即是，网关节点可以在触发鉴权的同时，向终端设备请求永久身份标识，将触发鉴权的过程和获取永久身份标识的过程合并在一起，减少了信令交互。

在第三种可能的实现方式中，当所述第三消息携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带失败消息。

其中，失败消息用于指示获取终端设备的上下文失败，第一失败原因值用于告知终端设备第一 IPsec 连接失败，第一失败原因值还用于关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，第四消息还携带第一失败原因值，其中，第一失败原因值用于通知终端设备第一 IPsec 连接失败，第一失败原因值还用于关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

相应地，当第四消息还携带第一失败原因值时，在终端设备向网关节点发送第五消息之前，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，并建立终端设备与网关节点之间的第二 IPsec 连接；

终端设备通过可以第二IPsec连接向网关节点发送第五消息，第五消息还携带关联参数，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数。

相应地，当第五消息中携带失败消息和关联参数时，网关节点根据该关联参数向控制面节点发送第六消息，该第六消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识。

在第四种可能的实现方式中，当第三消息中携带 EAP-AKA'/Identity-Request 消息，且 EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息。

可选地，第四消息还携带第一失败原因值，第一失败原因值用于通知终端设备第一 IPsec

连接失败，第一失败原因值还用于终端设备根据第一原因值确定关联参数，并发送关联参数给网关节点，网关节点根据关联参数关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

相应地，当第四消息中携带 EAP-AKA'/Identity-Request 消息，且 EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程时，终端设备向网关节点发送第五消息，第五消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程，EAP-AKA'/Identity-Response 用于响应 EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

当第四消息还携带第一失败原因值时，在终端设备向网关节点发送第五消息之前，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，并建立终端设备与网关节点之间的第二 IPsec 连接；终端设备通过第二 IPsec 连接向网关节点发送第五消息，第五消息还携带关联参数，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数。

相应地，当第五消息中携带 EAP-AKA'/Identity-Response 消息和关联参数时，网关节点根据该关联参数向控制面节点发送第六消息，该第六消息携带 EAP-AKA'/Identity-Response 消息。

在该种实现方式中，控制面节点在获取终端设备的上下文失败之后，直接触发鉴权，将鉴权流程和获取终端设备的永久身份标识的过程合并，减少了信令交互。

在第五种可能的实现方式中，当第三消息携带失败消息，且失败消息用于指示控制面节点无法确定终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带失败消息。

其中，第四消息还携带第二失败原因值，第二失败原因值用于通知终端设备第一 IPsec 连接失败。

相应地，当第四消息中携带失败消息，且失败消息用于指示控制面节点无法确定终端设备的永久身份标识时，终端设备向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

当第四消息还携带第二失败原因值时，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，建立与网关节点的之间的第二 IPsec 连接，并通过第二 IPsec 连接向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

相应地，当第五消息携带注册请求消息时，网关节点向控制面节点发送第六消息，第六消息携带注册请求消息；或者，网关节点向控制面节点发送第六消息，第六消息携带注册请求消息和 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息用于触发对终端设备的鉴权流程。

在该种实现方式中，网关节点可以将注册请求消息和 EAP-AKA'/Identity-Response 一起发，控制面节点可以在获取到终端设备的永久身份标识的同时，开始对终端设备鉴权，减少了信令交互。

在第六种可能的实现方式中，当第三消息携带通知消息，且通知消息用于向网关节点

通知控制面节点无法获得终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带注册拒绝消息。

其中，第四消息还携带第二失败原因值，第二失败原因值用于通知终端设备第一 IPsec 连接失败。

相应地，当第四消息中携带注册拒绝消息时，终端设备向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

当第四消息还携带第二失败原因值时，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，建立与网关节点的之间的第二 IPsec 连接，并通过第二 IPsec 连接向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

相应地，当第五消息携带注册请求消息时，网关节点向控制面节点发送第六消息，第六消息携带注册请求消息；或者，网关节点向控制面节点发送第六消息，第六消息携带注册请求消息和 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息用于触发对终端设备的鉴权流程。

在本申请实施例中，控制面节点在未能获取终端设备的上下文时，可以向网关节点发送第三消息，该第三消息中可以携带不同类型的消息来请求终端设备的永久身份标识。根据该第三消息中携带的消息的不同，网关节点和终端设备的执行的操作也不同，也即是，该控制面节点获取到永久身份标识的方式也就不同。接下来将分别就不同的情况对本申请实施例进行详细的解释说明。首先，将结合图 4 介绍当第三消息中携带的是身份请求消息时，控制面节点获取终端设备的身份标识的具体实现过程。

图 4 是本申请实施例提供的一种获取终端设备的身份标识的方法的流程图。如图 4 所示，该方法包括以下步骤：

步骤 401：终端设备向网关节点发送第一消息，第一消息中携带终端设备的临时身份标识。

终端设备在接入网络时，可能是再次注册到网络，或者是请求服务，或者是与网络建立会话。此时，终端设备可以向网关节点发送携带有相应的请求消息的第一消息。例如，终端设备可以向网关节点发送携带有注册请求消息的第一消息，也可以发送携带有服务请求消息或者是会话建立请求的第一消息。其中，该请求消息中均可以携带终端设备的临时身份标识。

可选地，当终端设备通过非 3GPP 技术接入如图 1 所示的网络时，该网关节点和非 3GPP 接入节点，如 wifi AP 不是由同一个运营商部署的。在这种情况下，对于网关节点而言，该非 3GPP 接入节点是不可信的，所以，当终端设备和该网关节点进行信令交互之前，终端设备和网关节点之间可以协商建立 IPsec 连接，当建立 IPsec 连接之后，终端设备和网关节点之间可以通过该 IPsec 连接进行信令交互，从而起到对传输的信令保护的作用。

其中，当终端设备通过该第一 IPsec 连接发送第一消息时，该第一消息可以为 IKEv2-AUTH- Request 消息。

当第一消息为 IKEv2-AUTH-Request 消息时，该第一消息包括厂商标识（Vendor Identification，VID）载荷，上述请求消息即可以放在 VID 载荷中，并且，在本申请实施例中 VID 载荷可以用于携带非接入层（Non-Access Stratum，NAS）消息。另外，处于 VID 载

荷中的请求消息除了携带终端设备的临时身份标识之外，还可以携带密钥标识符、消息鉴权码（Message Authentication Code，MAC）等，由于网关节点可以不对 VID 载荷中的 NAS 消息进行解析，因此，为了网关节点能够根据终端设备的临时身份标识选择合适的控制面节点。具体的，在该第一消息的 VID 载荷之外，可以携带 NAI，该 NAI 中可以携带终端设备的临时身份标识。可选地，当第一消息为 IKEv2-AUTH-Request 消息，该第一消息中还可以携带鉴权载荷和/或通知载荷等。

需要说明的是，在本申请实施例中，网关节点可以通过检查第一消息中有没有鉴权载荷去判断要不要触发鉴权。另外，该鉴权载荷还可以用于网关节点对终端设备进行验证。

步骤 402：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第二消息中携带终端设备的临时身份标识。

当网关节点接收到终端设备发送的第一消息之后，可以向控制面节点发送第二消息，该第二消息包含第一消息的 VID 载荷中的 NAS 消息，也即是，该第二消息可以包含前述的各类请求消息中的一种。

例如，第一消息的 VID 载荷中携带的是注册请求消息，当网关节点接收到第一消息时，即将该 VID 载荷中的注册请求消息作为第二消息中的部分内容或全部内容发送至控制面节点。

可选地，当第一消息中携带鉴权载荷时，网关节点可以不发起鉴权流程。

步骤 403：控制面节点接收网关节点发送的第二消息。

步骤 404：控制面节点根据临时身份标识查找该终端设备的上下文。

当控制面节点接收到第二消息之后，对第二消息进行解析，之后，根据该第二消息中的临时身份标识查找该终端设备的上下文。

在一种可选的方案中，控制面节点如 AMF 节点中可以存储有该终端设备的上下文。具体地，该控制面节点可以根据终端设备的临时身份标识，确定该终端设备的上下文。

在另一种可选的方案中，当前的控制面节点可以向其他控制面节点请求该终端设备的上下文。具体地，该控制面节点可以将第二消息转发至其他控制面板节点，等待其他控制面节点回复响应消息，该响应消息中可以携带该终端设备的上下文信息。进一步地，控制面节点可以根据该终端设备的临时身份标识来确定要向其请求上下文的其他控制面节点。

步骤 405：当控制面节点无法获得终端设备的上下文时，向网关节点发送第三消息，该第三消息中携带身份请求消息，该身份请求消息用于请求终端设备的永久身份标识。

在本申请实施例中，控制面节点通常可以对第二消息进行处理，例如，控制面节点可以验证该第二消息的完整性保护，若验证通过，则说明该控制面节点可以获取该终端设备的永久身份标识。当控制面节点在自身存储中查找不到终端设备的永久身份标识或者是验证完整性保护的密钥，或者是当控制面节点无法从其他控制面节点处获取到该终端设备的永久身份标时，可以确定该控制面节点无法获得该终端设备的上下文。

当控制面节点确定无法获得该终端设备的上下文时，就表明该控制面节点无法确定终端设备的永久身份标识。在这种情况下，控制面节点可以向网关节点发送第三消息，该第三消息中携带身份请求消息，通过该身份请求消息来请求终端设备的永久身份标识。

步骤 406：网关节点接收控制面节点发送的第三消息，并根据第三消息向终端设备发送第四消息，第四消息用于响应第一消息，该第四消息携带第一失败原因值，且该第四消息

中携带身份请求消息、EAP-AKA'/Identity-Request 消息和失败消息中的任一个。

当网关节点接收到第三消息之后，网关节点向终端设备请求永久身份标识。其中，网关节点和终端设备之间可以通过建立的第一 IPsec 连接进行通信的，终端设备发送的第一消息可以是 IKEv2-AUTH-Request 消息，那么，网关节点在向终端设备发送消息时，可以发送 IKEv2-AUTH-Response 消息，也即是第四消息。具体的，该第四消息中携带的内容可以有以下三种情况：

（1）第四消息携带第一失败原因值和身份请求消息。

当终端设备和网关节点之间完成一对消息对的传输之后，终端设备或网关节点可以将第一 IPsec 连接断开，终端设备发起建立第二 IPsec 连接请求，即再建立第二 IPsec 连接来传输消息。而如果断开第一 IPsec 连接之后，网关节点会将之前关于该终端设备的各种信息进行删除。这样，当终端设备再次通过下述步骤向网关节点发送永久身份标识时，网关节点将无法确定接收到的永久身份标识是不是发送第一消息的终端设备的永久身份标识，这样，网关节点也就无法回复控制面节点向其发送的身份请求消息，也即是，无法向控制面节点回复该永久身份标识。因此，网关节点可以在第四消息中携带第一失败原因值，终端设备可以根据该第一失败原因值确定网关节点需要将两次 IPsec 连接关联起来，以便网关节点可以确定两次接收到的来自终端设备的消息均是属于同一个终端设备。

需要说明的是，该第一失败原因值可以是终端设备和网关节点事先协商好的原因值。具体的，事先协商可以是通过消息协商，可以通过网管配置，也可以是在出厂设置的时候预配置的。当网关节点确定接收到的第三消息中携带有身份请求消息时，网关节点可以向控制面节点回复该身份请求消息，在这种情况下，网关节点可以关联两次 IPsec 连接，此时，网关节点可以在第四消息中携带第一失败原因值，以使终端设备携带关联参数，进而使网关节点可以根据该关联参数关联两次 IPsec 连接。

具体的，在本申请实施例中，第一失败原因值可以用于通知终端设备第一 IPsec 连接失败的原因，可选地，该第一失败原因值还可以用于指示终端设备发送关联参数，进而使网关节点可以根据该关联参数关联两次 IPsec 连接。具体关联时所需要采用的关联参数是由终端设备和网关节点事先协商好的。具体的，事先协商，可以是通过消息协商，可以通过网管配置，也可以是在出厂设置的时候预配置的。例如，该关联参数可以为建立 IPsec 连接时的安全参数索引（Security Parameter Index，SPI）、Cookies 或者终端设备的临时身份标识，如全球唯一临时用户设备标识（Globally Unique Temporary User Equipment Identity，GUTI）等。当该关联参数为上述的任一种时，在断开第一 IPsec 连接时，网关节点在删除关于该终端设备的部分信息时，则需要保留对应的参数。例如，假设该关联参数为 SPI，那么，网关节点在断开与终端设备之间的 IPsec 连接时就需要保留 SPI，并且终端设备在建立第二 IPsec 连接时或建立第二 IPsec 连接后携带 SPI。

另外，网关节点通过第四消息向终端设备请求永久身份标识，该第四消息中可以直接携带网关节点接收到的身份请求消息。具体的，由于第四消息为第一消息的响应消息，因此，当第一消息为 IKEv2-AUTH-Request 消息时，第四消息可以为 IKEv2-AUTH-Response 消息。另外，该身份请求消息可以为 NAS 消息，由第四消息中的 VID 载荷携带。还需要说明的是，第一失败原因值可以由第四消息中的鉴权载荷或通知载荷携带，也可以由其他载荷携带。

（2）第四消息携带第一失败原因值和 EAP-AKA'/Identity-Request 消息。

当网关节点接收到身份请求消息时，该网关节点可以确定控制面节点在请求终端设备的永久身份标识，此时，网关节点可以通过触发鉴权来向终端设备请求永久身份标识。具体的，网关节点可以生成 EAP-AKA'/Identity-Request 消息，该 EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程。之后，网关节点可以在第四消息中携带该 EAP-AKA'/Identity-Request 消息。

同样的，该第四消息可以是 IKEv2 响应消息，该 EAP-AKA'/Identity-Request 消息可以是 NAS 消息，由第四消息中的 VID 载荷携带，该第一失败原因值可以由第四消息中的鉴权载荷或通知载荷携带，也可以由其他载荷携带。

（3）第四消息携带第一失败原因值和失败消息。

当网关节点接收到身份请求消息时，该网关节点可以确定控制面节点在请求终端设备的永久身份标识，也就是说，网关节点可以认为控制面节点获取终端设备的上下文失败，此时，网关节点可以生成失败消息，该失败消息可以用来指示控制面节点无法确定终端设备的永久身份标识。在这种情况下，网关节点可以将该失败消息携带在第四消息中，以告知终端设备控制面节点获取上下文失败，从而请求终端设备的永久身份标识。

需要说明的是，第四消息可以是 IKEv2-AUTH-Response 消息，该失败消息可以由第四消息中的 VID 载荷携带，并且，第一失败原因值可以由第四消息中的鉴权载荷或通知载荷携带，也可以由其他载荷携带。

可选地，失败消息可以为注册失败消息、或者服务请求失败消息、或者验证完整性保护失败消息，会话建立失败消息等中的一种。

步骤 407：终端设备接收网关节点发送的第四消息，并根据第四消息向网关节点发送第五消息，第五消息携带终端设备的永久身份标识。

终端设备在接收到网关节点发送的第四消息时，可以对该第四消息进行处理。由步骤 406 可知，第四消息中携带的内容可以分为三种，终端设备根据第四消息中携带的内容的不同，可以进行不同的处理。

（1）当第四消息中携带的是第一失败原因值和身份请求消息时，终端设备可以断开第一 IPsec 连接，并且获取关联参数，该关联参数为终端设备存储的预先与网关节点协商好的用于关联第一 IPsec 连接和第二 IPsec 连接的参数。具体的，终端设备与网关节点协商的方法可以是通过信令交互进行协商，或者可以是网管提前配置，或者可以是由标准或规范定义好的。由于第四消息中携带的是身份请求消息，因此，终端设备可以响应该身份请求消息，生成身份回复消息，并由该身份回复消息携带永久身份标识。之后，终端设备可以与网关节点进行协商，建立第二 IPsec 连接，并通过第二 IPsec 连接向网关节点发送第五消息。此时，该第五消息中身份回复消息，该身份回复消息中携带永久身份标识。

可选地，该第五消息还可以携带关联参数，该关联参数用于关联第一 IPsec 连接和第二 IPsec 连接，使网关节点可以将同一个终端设备通过不同 IPsec 连接发送的消息发往同一个控制面节点。也即是，当第五消息携带关联参数时，网关节点可以通过该关联参数确定将第五消息中携带永久身份标识的消息发往哪个控制面节点。具体的，该关联参数可以是终端设备之前在第一消息中携带过的临时身份标识。可选的，终端设备可以将该临时身份标识放到网络访问标识符（Network Access Identifier，NAI）中。网关节点可以根据临时身份

标识中的信息，将携带永久身份标识的消息发给控制面节点。

可选地，当该第五消息不携带关联参数时，终端设备可以在建立第二 IPsec 连接的过程中携带关联参数，相应地，网关节点可以获取自身在建立第二 IPsec 连接时的参数作为关联参数。例如，假设终端设备在建立第二 IPsec 连接的过程中携带有 SPI，网关节点可以获取建立第二 IPsec 连接时产生的 SPI，之后网关节点可以将获取的 SPI 与终端设备携带的 SPI 做比较，并根据比较结果来进行下一步的操作。

需要说明的是，第五消息可以为 IKEv2-AUTH-Request 消息，该身份回复消息可以 NAS 消息，可以由第五消息中的 VID 载荷携带。

（2）当第四消息中携带的是第一失败原因值和 EAP-AKA'/Identity-Request 消息时，对于第一失败原因值的处理，可以参考上述（1）中的说明。对于 EAP-AKA'/Identity-Request 消息，终端设备可以生成响应该 EAP-AKA'/Identity-Request 消息的 EAP-AKA'/Identity-Response 消息，并且，由该 EAP-AKA'/Identity-Response 消息携带该永久身份标识。之后，终端设备可以建立与网关节点之间的第二 IPsec 连接，并通过第二 IPsec 连接向网关节点发送第五消息，此时，该第五消息中携带 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息携带永久身份标识。

可选地，该第五消息中还可以携带关联参数。具体的，第五消息中携带关联参数的情况可以参照步骤 307 以及上述（1）中的相关解释说明。

需要说明的是，第五消息可以为 IKEv2-AUTH-Request 消息，该 EAP-AKA'/Identity-Response 消息可以由第五消息中的 VID 载荷携带。

（3）当第四消息中携带的是第一失败原因值和失败消息时，终端设备可以断开第一 IPsec 连接，获取关联参数。第四消息中携带有失败消息，终端设备可以根据该失败消息获知控制面节点无法确定永久身份标识。在这种情况下，终端设备可以重新发起注册请求消息，该注册请求消息中携带终端设备的永久身份标识。之后，终端设备可以建立与网关节点之间的第二 IPsec 连接，并通过该第二 IPsec 连接向网关节点发送第五消息，此时，该第五消息携带注册请求消息，该注册请求消息中携带永久身份标识。

可选地，该第五消息中还可以携带关联参数，具体的，第五消息中携带关联参数的情况可以参照上述（1）中相关的解释说明。

需要说明的是，该第五消息可以为 IKEv2-AUTH-Request 消息，该注册请求消息可以为 NAS 消息，由第五消息的 VID 载荷携带。

另外，当第四消息中携带有失败消息时，终端设备可以确定第一消息中携带的请求消息所请求的服务失败。此时，从发送第一消息，到接收到关于第一消息的响应失败消息，终端设备完成了一套完整的状态机。而终端设备向网关节点再次发起注册请求消息，则表示终端设备又开始了一套新的状态机。

步骤 408：网关节点接收终端设备发送的第五消息，并根据第五消息向控制面节点发送第六消息，该第六消息携带身份回复消息，该身份回复消息携带终端设备的永久身份标识。

当网关节点接收到终端设备发送的第五消息之后，可以对第五消息进行处理，之后，根据该第五消息向控制面节点发送携带有该终端设备的永久身份标识的第六消息。

具体的，当网关节点确定该第五消息携带有关联参数时，网关节点可以根据第五消息中携带的关联参数来判断当前发送第五消息的终端设备是否为之前发送第一消息的终端设

备。具体的，当关联参数为 SPI 或 cookie 时，网关节点可以从存储的属于多个终端设备的关联参数中查找是否存在与第五消息中携带的关联参数相同的关联参数。如果网关节点查找到与第五消息中携带的关联参数相同的关联参数，那么，网关节点可以确定当前发送第五消息的终端设备就是之前发送第一消息的终端设备，此时，网关节点可以从存储的关联参数与控制面节点的对应关系中确定该关联参数对应的控制面节点，从而向确定的控制面节点发送该第六消息。当该关联参数为 NAI，且该 NAI 携带有前次使用的临时身份标识时，网关节点可以从存储的属于多个终端设备的临时身份标识中查找是否存在与第五消息中携带的临时身份标识相同的临时身份标识。如果网关节点查找到与第五消息中携带的临时身份标识相同的临时身份标识，那么，网关节点可以确定当前发送第五消息的终端设备就是之前发送第一消息的终端设备，此时，网关节点可以从存储的关联参数与控制面节点的对应关系中确定该关联参数对应的控制面节点，从而向确定的控制面节点发送该第六消息；或者，网关节点可以不对第五消息中携带的临时身份标识进行比对，而是直接根据该临时身份标识，向该临时身份标识所指示的控制面节点发送第六消息。具体的，网关节点可以直接根据该第五消息中携带的终端设备的永久身份标识来回复控制面节点发送的身份请求消息，也即是，网关节点可以直接将第五消息中携带有终端设备的永久身份标识的消息携带在第六消息中发送至控制面节点。

当网关节点确定控制面节点之后，网关节点可以根据该第五消息向控制面节点发送第六消息，该第六消息中携带终端设备的永久身份标识。具体的，根据第五消息携带的内容的不同，第六消息中携带的其他内容也会不同。其中，该第六消息可以为 N2 消息。

（1）当第五消息中携带的是身份回复消息时，网关节点可以直接用该身份回复消息来响应之前接收到的控制面节点发送的身份请求消息。也即是，网关节点可以直接将该身份回复消息携带在第六消息中发送至控制面节点。

可选地，网关节点还可以生成 EAP-AKA'/Identity-Response 消息来触发鉴权。在这种情况下，该第六消息中还可以携带该 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息中也可以携带有终端设备的永久身份标识。

可选地，该 EAP-AKA'/Identity-Response 消息可以携带在身份回复消息中，此时，该终端设备的永久身份标识由 EAP-AKA'/Identity-Response 消息来携带。也即是，该第六消息携带身份回复消息，该身份回复消息携带 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

（2）当第五消息中携带的是 EAP-AKA'/Identity-Response 消息时，网关节点可以生成身份回复消息来响应控制面节点发送的身份请求消息。之后，网关节点可以向控制面节点发送第六消息，该第六消息中可以携带身份回复消息和 EAP-AKA'/Identity-Response 消息，并且该身份回复消息中携带有永久身份标识。

可选地，该 EAP-AKA'/Identity-Response 消息可以由身份回复消息携带。也即是，该第六消息携带身份回复消息，该身份回复消息携带 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息携带永久身份标识。

（3）当第五消息中携带的是注册请求消息时，网关节点可以生成身份回复消息来响应控制面节点发送的身份请求消息。之后，网关节点可以向控制面节点发送第六消息，该第六消息中携带该身份回复消息，该身份回复消息中携带终端设备的永久身份标识。

可选地，网关节点还可以生成EAP-AKA'/Identity-Response消息来触发鉴权。在这种情况下，该第六消息中还可以携带该EAP-AKA'/Identity-Response消息，该EAP-AKA'/Identity-Response消息中也携带有终端设备的永久身份标识。或者，该EAP-AKA'/Identity-Response消息可以由身份回复消息携带，此时，该EAP-AKA'/Identity-Response消息中携带有永久身份标识。

需要说明的是，由步骤407中（3）的描述可知，终端设备接收到失败消息后，确定入网失败，完整了第一套状态机，而重新发起注册则又开始了另一套新的状态机。而控制面节点此时还在等待关于身份请求消息的响应消息，也即是，控制面节点此时还处于上第一套状态机。在这种情况下，由网关节点回复控制面节点身份回复消息，使控制面节点可以继续第一套状态机。由此可见，在本申请实施例中，通过网关节点可以使终端设备和控制面节点的状态机不同步，由网关节点分别维护终端设备和控制面节点两侧的状态机，这样，控制面节点就不必再结束第一套状态机，重新开始另一套状态机，减少了控制面节点的操作复杂性。

在本申请实施例中，控制面节点在未获取到终端设备的上下文时，可以向网关节点发送携带有身份请求消息的第三消息来请求终端设备的永久身份标识，网关节点在接收到该身份请求消息时，可以向终端设备发送用于关联第一IPsec连接和第二IPsec连接的第一失败原因值，同时，还可以向终端设备直接发送身份请求消息，或者可以向终端设备发送根据该身份请求消息生成的EAP-AKA'/Identity-Request消息或失败消息。之后，如果终端设备接收到的是身份请求消息，那么，终端设备可以自己回复携带有终端设备的永久身份标识的身份回复消息，网关节点只需将该身份回复消息转发给控制面节点即可。如果终端设备接收到的是EAP-AKA'/Identity-Request消息或者是失败消息，那么，终端设备即回复对应的携带有永久身份标识的消息，并由网关节点根据终端设备回复的消息生成身份回复消息，回复控制面节点的身份请求消息。由此可见，在本申请实施例中，即使控制面节点中未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。

另外，在本申请实施例中，网关节点还可以根据身份请求消息生成EAP-AKA'/Identity-Request消息向终端设备请求永久身份标识，也即是，网关节点可以在触发鉴权的同时，向终端设备请求永久身份标识，将触发鉴权的过程和获取永久身份标识的过程合并在一起，减少了信令交互。还需要说明的是，网关还可以根据身份请求消息生成失败消息向终端设备请求永久身份标识，这样，网关节点就需要分别维护终端设备和控制面节点两侧的状态机，使得终端设备和控制面节点两侧的状态机可以不一致，减少了控制面节点操作的复杂性。

上述实施例介绍了当第三消息携带的是身份请求消息时，控制面节点获取终端设备的身份标识的具体实现过程，接下来将结合附图5介绍当第三消息中携带的是EAP-AKA'/Identity-Request消息时，控制面节点获取终端设备的身份标识的具体实现过程。

步骤501：终端设备向网关节点发送第一消息，第一消息中携带终端设备的临时身份标

识。

本步骤可以参考前述实施例中的步骤401，本申请实施例不再赘述。

步骤502：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第二消息中携带终端设备的临时身份标识。

本步骤可以参考前述实施例中的步骤402，本申请实施例不再赘述。

步骤503：控制面节点接收网关节点发送的第二消息。

步骤504：控制面节点根据临时身份标识查找该终端设备的上下文。

本步骤可以参考前述实施例中的步骤404，本申请实施例不再赘述。

步骤505：当控制面节点无法获得终端设备的上下文时，向网关节点发送第三消息，该第三消息中携带EAP-AKA'/Identity-Request消息。

当控制面节点无法获得终端设备的上下文时，则表明当前的控制面节无法确定该终端设备的身份。此时，该控制面节点可以对该终端设备进行鉴权，从而使终端设备成功接入网络。基于此，控制面节点在无法获得终端设备的上下文时，可以直接触发鉴权，将触发鉴权和获取终端设备的永久身份标识的流程一起执行。具体的，控制面节点可以直接向网关节点发送携带由 EAP-AKA'/Identity-Request 消息的第三消息，通过触发鉴权来请求终端设备的永久身份标识。

步骤506：网关节点接收控制面节点发送的第三消息，并根据第三消息向终端设备发送第四消息，第四消息用于响应第一消息，该第四消息携带第一失败原因值和EAP-AKA'/Identity-Request消息。

当网关节点接收到控制面节点发送的第三消息时，可以直接向终端设备发送携带有该EAP-AKA'/Identity-Request消息的第四消息。

另外，第三消息中携带有 EAP-AKA'/Identity-Request 消息，表示控制面节点后续可以根据回复的永久身份标识对该终端设备继续进行鉴权，这样，网关节点需要保证其发送第四消息来请求永久身份标识的终端设备和后续返回永久身份标识的终端设备是同一个终端设备，而由前述实施例中的描述可知，第一 IPsec 连接断开之后，如果不将两次 IPsec 连接进行关联，那么，网关节点会将第一 IPsec 连接对应的终端设备的信息删除，这样，即使该终端设备通过第二 IPsec 连接返回永久身份标识，网关节点也无法确认返回的终端设备的永久身份标识是否是请求的终端设备的永久身份标识。这样，网关节点也就无法将第二 IPsec 连接中收到的第五消息中的永久身份标识，发往接收第二消息的控制面节点。在这种情况下，网关节点还可以在第四消息中携带第一失败原因值，以使终端设备携带关联参数，进而使网关节点可以根据该关联参数关联第一 IPsec 连接和第二 IPsec 连接。

其中，第一失败原因值可以用于通知终端设备第一 IPsec 连接失败。

可选地，第一失败原因值还可以用于指示终端设备发送关联参数，以使网关节点可以根据该关联参数关联第一 IPsec 连接和第二 IPsec 连接。可选地，该第一失败原因值还可以用于

另外，第四消息可以为 IKEv2-AUTH-Response 消息，EAP-AKA'/Identity-Request 消息可以由第四消息中的 VID 载荷携带。还需要说明的是，第一失败原因值可以由第四消息中的鉴权载荷或通知载荷携带，也可以由其他载荷携带。

步骤507：终端设备接收网关节点发送的第四消息，并根据第四消息向网关节点发送第

五消息，第五消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

当终端设备接收到携带有第一失败原因值的第四消息，可以确定需要关联两次 IPsec，此时，终端设备断开与网关节点之间的第一 IPsec 连接，获取关联参数。之后，终端设备可以响应 EAP-AKA'/Identity-Request 消息，根据 EAP-AKA'/Identity-Request 消息生成 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息中携带终端设备的永久身份标识。之后，终端设备可以与网关节点之间进行协商，建立第二 IPsec 连接，并通过第二 IPsec 连接向网关节点发送第五消息。此时，该第五消息中可以携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息中携带终端设备的永久身份标识。

可选地，该第五消息中还可以携带关联参数，关于该关联参数的具体解释说明可以参考步骤 307 以及上述实施例中步骤 407（1）中的相关介绍，本申请实施例不再赘述。

需要说明的是，第五消息可以为 IKEv2-AUTH-Request 消息，该 EAP-AKA'/Identity-Response 消息可以由第五消息中的 VID 载荷携带。

步骤 508：网关节点接收终端设备发送的第五消息，并根据第五消息向控制面节点发送第六消息，该第六消息携带 EAP-AKA'/Identity-Response 消息，该 EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

当网关节点接收到第五消息时，可选地，网关节点可以根据第五消息中携带的关联参数将第一 IPsec 连接和第二 IPsec 连接进行关联，具体的实现过程可以参考前述实施例中步骤 408 中相关的解释说明。

可选地，网关节点可以根据第五消息向控制面节点发送第六消息。具体的，由于控制面节点发送的第三消息中携带的是 EAP-AKA'/Identity-Request 消息，因此，网关节点可以直接将该 EAP-AKA'/Identity-Response 消息携带在第六消息中，以响应控制面节点发送的 EAP-AKA'/Identity-Request 消息。其中，该第六消息可以为 N2 消息。具体的，EAP-AKA'/Identity-Response 消息可以放到 NAS 容器中。

在本申请实施例中，控制面节点在未获取到终端设备的上下文时，可以向网关节点发送携带有 EAP-AKA'/Identity-Request 消息的第三消息来请求终端设备的永久身份标识，网关节点在接收到该 EAP-AKA'/Identity-Request 消息时，可以向终端设备发送第四消息，该第四消息中携带用于关联第一 IPsec 连接和第二 IPsec 连接的第一失败原因值和该 EAP-AKA'/Identity-Request 消息，终端设备在接收到的第四消息时，获取关联参数，并生成回复该 EAP-AKA'/Identity-Request 消息的 EAP-AKA'/Identity-Response 消息，其中，该 EAP-AKA'/Identity-Response 消息中携带有终端设备的永久身份标识。之后，终端设备可以向网关节点发送第五消息，该第五消息携带关联参数和 EAP-AKA'/Identity-Response 消息，网关节点在接收到第五消息后，只需将该 EAP-AKA'/Identity-Response 消息消息转发给控制面节点即可。由此可见，在本申请实施例中，即使控制面节点中无法获得终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。另外，在本申请实施例中，控制面节点在获取终端设备的上下文失败之后，直接触发鉴权，将鉴权流程和

获取终端设备的永久身份标识的过程合并，减少了信令交互。

前述两个实施例分别介绍了当第三消息中只携带身份请求消息或者只携带EAP-AKA'/Identity-Request消息时的具体实现过程。在实际应用中，控制面节点可以在获取永久身份标识的同时触发鉴权流程。也即是，控制面节点可以在第三消息中同时携带身份请求消息和EAP-AKA'/Identity-Request消息。

当第三消息中同时携带有身份请求消息和EAP-AKA'/Identity-Request消息时，则可以不必再由网关节点生成EAP-AKA'/Identity-Request消息来触发鉴权流程。在这种情况下，网关节点可以向终端设备发送第四消息，该第四消息中可以携带身份请求消息、EAP-AKA'/Identity-Request消息和第一失败原因值。终端设备在接收到第四消息时，根据身份请求消息生成身份回复消息，根据EAP-AKA'/Identity-Request消息生成EAP-AKA'/Identity-Request消息，断开第一IPsec连接，获取关联参数，建立第二IPsec连接，其中，身份回复消息和EAP-AKA'/Identity-Response消息中可以均携带终端设备的永久身份标识。之后，终端设备向网关节点发送第五消息，该第五消息可以携带身份回复消息、EAP-AKA'/Identity-Response消息和关联参数。网关节点在接收到第五消息之后，可以根据关联参数关联第一IPsec连接和第二IPsec连接，并向控制面节点发送第六消息，该第六消息中携带身份回复消息和EAP-AKA'/Identity-Response消息。

上述实施例介绍了当第三消息携带的是EAP-AKA'/Identity-Request消息时，控制面节点获取终端设备的身份标识的具体实现过程，接下来将结合附图6介绍当第三消息中携带的是失败消息或通知消息时，控制面节点获取终端设备的身份标识的具体实现过程。

步骤601：终端设备向网关节点发送第一消息，第一消息中携带终端设备的临时身份标识。

本步骤可以参考前述实施例中的步骤401，本申请实施例不再赘述。

步骤602：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第二消息中携带终端设备的临时身份标识。

本步骤可以参考前述实施例中的步骤402，本申请实施例不再赘述。

步骤603：控制面节点接收网关节点发送的第二消息。

步骤604：控制面节点根据临时身份标识查找该终端设备的上下文。

本步骤可以参考前述实施例中的步骤404，本申请实施例不再赘述。

步骤605：当控制面节点无法获得终端设备的上下文时，向网关节点发送第三消息，该第三消息中携带失败消息或通知消息。

当控制面节点未查找到终端设备的上下文时，控制面节点也就无法响应终端设备的请求，也就是说，终端设备发起的请求是失败的。例如，假设终端设备在第一消息中发送的是注册请求消息，当控制面节点查找不到终端设备的上下文时，即可以确定此次注册失败。因此，控制面节点可以生成失败消息，该失败消息可以用于通知终端设备控制面节点无法确定该终端设备的永久身份标识。再比如，控制面节点找到终端设备的上下文，但是验证完整性保护失败，此时，控制面节点可以生成失败消息，该失败消息可以用于通知终端设备控制面节点验证完整性保护失败，无法确定该终端设备的永久身份标识。

需要说明的是，该失败消息中携带有原因值，并且控制面节点可以根据失败类型的不同，在失败消息中携带不同的原因值。例如，假设终端设备的请求消息是注册请求消息，那么，控制面节点中携带的原因值即为注册失败对应的原因值。这里，失败类型也就是注册失败。

在另一种可能的实现方式中，当控制面节点未获取到终端设备的上下文时，控制面节点可以直接根据具体的未获取到的信息生成携带有对应的原因值的通知消息，来通知网关节点未能确定终端设备的上下文。例如，假设控制面节点未查找到上下文中的永久身份标识，那么，控制面节点可以生成通知消息，该通知消息中携带有用于标识未查找到永久身份标识所的原因值。

需要说明的是，上述失败消息可以为 NAS 消息。上述通知消息不是可以是 NAS 消息，也可以不是 NAS 消息。

步骤 606：网关节点接收控制面节点发送的第三消息，并根据第三消息向终端设备发送第四消息，第四消息用于响应第一消息，该第四消息携带第二失败原因值，且该第四消息中携带失败消息。

当网关节点通过解析第三消息中的 NAS 消息确定第三消息中携带有失败消息时，网关节点可以直接向终端设备发送携带有失败消息的第四消息。并且，由于控制面节点已经确认终端设备的请求失败，因此，可以确定在控制面节点一侧，由终端设备的第一消息开始的第一套状态机已经结束。此时，网关节点则可以不再维护第一 IPsec 连接和后续的第二 IPsec 连接之间的关联，因此，网关节点可以在第四消息中携带第二失败原因值，该第二失败原因值用于告知终端设备第一 IPsec 连接失败，但是该第二失败原因值并不能通知终端设备关联第一 IPsec 连接和第二 IPsec 连接。

当确定第三消息中携带有通知消息时，网关节点可以根据该通知消息确定控制面节点无法确定该终端设备的身份，结合这个实施例，具体地为网关节点可以根据该通知消息确定终端设备的请求失败，也即是，控制面节点拒绝了终端设备的请求。此时，网关节点可以根据该通知消息生成注册拒绝消息，并向终端设备发送携带有该注册拒绝消息的第四消息，以告知终端设备注册请求被拒绝。同样的，由于控制面节点已确认获取上下文失败，并且，并未发出具体的其他请求消息，因此，可以确定在控制面节点一侧，由终端设备的第一消息开始的第一套状态机已经结束。此时，网关节点可以不再维护第一 IPsec 连接和后续的第二 IPsec 连接之间的关联，因此，网关节点可以在第四消息中携带第二失败原因值，以告知终端设备第一 IPsec 连接失败，但不告知终端设备关联两次 IPsec 连接。

需要说明的是，在本申请实施例中，注册拒绝消息可以是失败消息的一种。

步骤 607：终端设备接收网关节点发送的第四消息，并根据第四消息向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

由步骤 606 中的描述可知，当第三消息中携带失败消息或通知消息时，第四消息中可以携带有第二失败原因值。当终端设备确定第四消息中携带有第二失败原因值时，终端设备可以断开与网关节点之间的第一 IPsec 连接，并且确定不需要将第一 IPsec 连接和第二 IPsec 连接进行关联，显然，也就不需要获取关联参数，之后，终端设备可以与网关节点协商建立第二 IPsec 连接。

另外，不管第四消息携带的是失败消息还是注册拒绝消息，终端设备均可以根据该失

败消息或注册拒绝消息确定注册失败或请求的服务失败，此时，终端设备可以根据该失败消息或者注册拒绝消息生成注册请求消息，并向网关节点发送携带有该注册请求消息的第五消息，重新发起注册。其中，该注册请求消息中携带终端设备的永久身份标识。

可选地，第五消息可以为 IKEv2-AUTH-Request 消息，该注册请求消息可以由第五消息中的 VID 载荷携带。可选地，第五消息通过第二 IPsec 连接来传输。具体地，在第五消息发送前，终端设备和网关节点建立第二 IPsec 连接。

步骤 608：网关节点接收终端设备发送的第五消息，并根据第五消息向控制面节点发送第六消息，该第六消息携带终端设备的永久身份标识。

当网关节点接收到终端设备发送的第五消息之后，可以向控制面节点发送第六消息，该第六消息中携带有该注册请求消息。

可选地，网关节点可以发送只携带有注册请求消息的第六消息。或者，网关节点还可以生成 EAP-AKA'/Identity-Response 消息，并在第六消息中携带该 EAP-AKA'/Identity-Response 消息，以触发鉴权。也即是，该第六消息可以同时携带 EAP-AKA'/Identity-Response 消息和注册请求消息，且 EAP-AKA'/Identity-Response 消息和注册请求消息均可以携带有终端设备的永久身份标识。

在本申请实施例中，控制面节点在无法获得终端设备的上下文时，可以向网关节点发送携带有失败消息或通知消息的第三消息来请求终端设备的永久身份标识，网关节点在接收到该失败消息或通知消息时，可以向终端设备发送第四消息，其中，不管第三消息携带的失败消息还是通知消息，控制面节点一侧的状态机都已完成，此时，该第四消息中将携带第二失败原因值，用于告知终端设备不关联第一 IPsec 连接和第二 IPsec 连接，同时，如果第三消息中携带的失败消息，那么，网关节点可以直接将携带有该失败消息和第二失败原因值的第四消息发送至终端设备。如果第三消息中携带的是通知消息，网关节点可以根据该通知消息生成注册拒绝消息，从而向终端设备发送携带有该注册拒绝消息和第二失败原因值的第四消息。终端设备在接收到的第四消息时，无论第四消息中携带的是失败消息还是注册拒绝消息，终端设备均可以生成注册请求消息，并通过第二 IPsec 连接向网关节点发送该注册请求消息，重新发起注册。网关节点在接收到该注册请求消息时，可以直接向控制面节点发送携带有该注册请求消息的第六消息，也可以同时在该第六消息中 EAP-AKA'/Identity-Response 消息，来触发鉴权。由此可见，在本申请实施例中，即使控制面节点中未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能。

前述实施例分别介绍了第三消息携带身份请求消息、EAP-AKA'/Identity-Request 消息、失败消息和通知消息中的一个时，本申请实施例的具体实现过程。除此之外，控制面节点可以在第三消息中同时携带身份请求消息和通知消息，或者同时携带 EAP-AKA'/Identity-Request 消息和通知消息，或者同时携带失败消息和通知消息。接下来将结合附图 7 介绍当第三消息中同时携带身份请求消息和通知消息时，本申请实施例的具体实现过程。

步骤 701：终端设备向网关节点发送第一消息，第一消息中携带终端设备的临时身份标

识。

本步骤可以参考前述实施例中的步骤401，本申请实施例不再赘述。

步骤702：网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，第二消息中携带终端设备的临时身份标识。

本步骤可以参考前述实施例中的步骤402，本申请实施例不再赘述。

步骤703：控制面节点接收网关节点发送的第二消息。

步骤704：控制面节点根据临时身份标识查找该终端设备的上下文。

本步骤可以参考前述实施例中的步骤404，本申请实施例不再赘述。

步骤705：当控制面节点无法获得终端设备的上下文时，向网关节点发送第三消息，且该第三消息中携带身份请求消息和通知消息。

在这种情况下，该通知消息中可以携带第一原因值。网关节点可以根据携带的第一原因值，在再次收到该终端设备发来的消息时，将接收到的该终端设备的消息发给该控制面节点。

需要说明的是，该通知消息中携带的第一原因值同样可以用于第三消息中携带的是EAP-AKA'/Identity-Request消息的情况。

具体的，该通知消息中的原因值可以有多种可能。例如，该原因值可以是告知网关节点再次收到该终端设备发来的消息时，要将接收到的该终端设备的消息发给该控制面节点的原因值。

步骤706：网关节点接收控制面节点发送的第三消息，并根据第三消息向终端设备发送第四消息，第四消息用于响应第一消息，该第四消息携带第一失败原因值和身份请求消息。

网关节点在接收到第三消息之后，可以向终端设备发送携带有身份请求消息的第四消息，并且，网关节点可以根据通知消息中携带的第一原因值，确定关联第一IPsec连接和后续的第二IPsec连接。也即是，该第四消息中还可以携带第一失败原因值。

步骤707：终端设备接收网关节点发送的第四消息，并根据第四消息向网关节点发送第五消息，第五消息携带身份回复消息，身份回复消息携带终端设备的永久身份标识。

本步骤可以参考前述实施例中步骤407中（1）的解释说明，本申请实施例不再赘述。

步骤708：网关节点接收终端设备发送的第五消息，并根据第五消息向控制面节点发送第六消息，该第六消息携带身份回复消息，该身份回复消息携带终端设备的永久身份标识。

本步骤可以参考前述实施例中步骤408中（1）的解释说明，本申请实施例不再赘述。

在本申请实施例中，控制面节点在无法获取到终端设备的上下文时，可以向网关节点发送携带有通知消息和身份请求消息的第三消息来请求终端设备的永久身份标识，网关节点在接收到该通知消息和身份请求消息时，可以不对身份请求消息进行解析，根据该通知消息确定关联第一IPsec连接和第二IPsec连接。之后，网关节点向终端设备发送携带有身份请求消息和第一失败原因值的第四消息，从而向终端设备请求永久身份标识。由此可见，在本申请实施例中，即使控制面节点中未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。另外，本申请实施例将通知消息和身份请求消息一起发送至网关节点，网关节点不必对身份请求消息进行解析即可以完成后续流程，

减少了网关节点操作的复杂性。

上述实施例介绍了当第三消息中同时携带通知消息和身份请求消息时的具体实现过程。当第三消息中同时携带通知消息和 EAP-AKA'/Identity-Request 消息时，网关节点在接收到第三消息时的处理可也参考上述实施例中的步骤 706，之后，网关节点向终端设备发送的第四消息中可以携带第一失败原因值和 EAP-AKA'/Identity-Request 消息。终端设备在接收到第四消息之后，根据第四消息向网关节点发送第五消息，以及网关节点根据第五消息向控制面节点发送第六消息的具体实现过程可以分别参考前述实施例中的步骤 507 和 508，本申请实施例不再赘述。

当第三消息中同时携带通知消息和失败消息时，该通知消息中可以携带有第二原因值，网关节点在接收到第三消息时，可以根据通知消息中的第二原因值确定不关联两次 IPsec 连接，这样，网关节点可以向终端设备发送携带有第二失败原因值和失败消息的第四消息。终端设备在接收到第四消息之后，根据第四消息向网关节点发送第五消息，以及网关节点根据第五消息向控制面节点发送第六消息的具体实现过程可以分别参考前述实施例中的步骤 607 和 608，本申请实施例不再赘述。

在对本申请实施例的具体实现过程进行介绍之后，接下来对本申请实施例涉及的装置进行介绍。

参见图 8，本申请实施例提供了一种获取终端设备的身份标识的装置，该装置包含于网关节点中，该装置包括：

接收模块 801，用于执行上述实施例中的步骤 302、步骤 306 中接收控制面节点发送的第四消息的步骤、以及步骤 308 中接收终端设备发送的第五消息的步骤；

发送模块 802：用于执行上述实施例中的步骤 306 中接收控制面节点发送的第三消息的步骤和步骤 308 中向控制面节点发送永久身份标识的步骤。

可选地，发送模块 802 包括：

发送子模块，用于当第三消息中携带身份请求消息，身份请求消息用于请求终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一互联网协议安全性 IPsec 连接向终端设备发送第四消息，第四消息携带身份请求消息和第一失败原因值；

其中，第一失败原因值用于通知终端设备第一 IPsec 连接失败，该第一失败原因值还用于指示所述终端设备发送关联参数，以关联第一 IPsec 连接与第二 IPsec 连接，该关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，第五消息携带身份回复消息和关联参数，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识；

发送子模块用于：

根据关联参数，向控制面节点发送第六消息，其中，第六消息携带身份回复消息和 EAP-AKA'/Identity-Response 消息，且身份回复消息和 EAP-AKA'/Identity-Response 消息均携带永久身份标识；或者，第六消息携带身份回复消息，身份回复消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息携带永久身份标识；或

者，

根据关联参数，向控制面节点发送第六消息，第六消息携带身份回复消息，身份回复消息携带终端设备的永久身份标识。

可选地，发送模块 802，包括：

发送子模块，用于当第三消息中携带身份请求消息，身份请求消息用于请求终端设备的永久身份标识时，通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程，第一失败原因值用于通知终端设备第一 IPsec 连接失败，该第一失败原因值还用于指示所述终端设备发送关联参数，以关联第一 IPsec 连接与第二 IPsec 连接，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，第五消息携带 EAP-AKA'/Identity-Response 消息和关联参数，EAP-AKA'/Identity-Response 消息用于响应述 EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识；

发送子模块用于：

根据关联参数，向控制面节点发送第六消息；

其中，第六消息携带身份回复消息和 EAP-AKA'/Identity-Response 消息，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识；或者，第六消息携带身份回复消息，身份回复消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识。

可选地，发送模块 802 包括：

发送子模块，用于当第三消息携带身份请求消息，身份请求消息用于请求终端设备的永久身份标识时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带失败消息和第一失败原因值；

其中，失败消息用于指示获取终端设备的上下文失败，第一失败原因值用于通知终端设备第一 IPsec 连接失败，该第一失败原因值还用于指示所述终端设备发送关联参数，以关联第一 IPsec 连接与第二 IPsec 连接，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，第五消息携带注册请求消息和关联参数，注册请求消息携带终端设备的永久身份标识；

发送子模块用于：

根据关联参数，向控制面节点发送第六消息，第六消息携带身份回复消息，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识。

可选地，发送模块，包括：

当第三消息中携带 EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，第一失败原因值用于通知终端设备第一 IPsec 连接失败，该第一失败原因值还用

于指示所述终端设备发送关联参数，以关联第一 IPsec 连接与第二 IPsec 连接，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，第五消息携带 EAP-AKA'/Identity-Response 消息和关联参数，EAP-AKA'/Identity-Response 消息用于响应 EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识；

发送子模块用于：

根据关联参数，向控制面节点发送第六消息，第六消息携带 EAP-AKA'/Identity-Response 消息。

可选地，发送模块 802 包括：

发送子模块，用于当第三消息携带失败消息，失败消息用于指示控制面节点获取终端设备的上下文失败时，通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带失败消息和第二失败原因值；

其中，第二失败原因值用于通知终端设备第一 IPsec 连接失败，并关联第一 IPsec 连接与第二 IPsec 连接，第二 IPsec 连接是在断开第一 IPsec 连接之后建立的 IPsec 连接。

可选地，发送子模块还用于：

当第三消息中携带通知消息，且通知消息用于向网关节点通知控制面节点获取终端设备的上下文失败时，网关节点通过网关节点与终端设备之间的第一 IPsec 连接向终端设备发送第四消息，第四消息携带注册拒绝消息和第二失败原因值；

其中，第二失败原因值用于通知终端设备第一 IPsec 连接失败。

可选地，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识；

发送模块 802 包括：

发送子模块，用于向控制面节点发送第六消息，第六消息携带注册请求消息；或者，

该发送子模块还用于向控制面节点发送第六消息，第六消息携带注册请求消息和 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Response 消息用于触发对终端设备的鉴权流程。

参见图 9，本申请实施例提供了一种获取终端设备的身份标识的装置，该装置包含于终端设备中，该装置包括：

发送模块 901，用于执行上述实施例中步骤 301 以及步骤 307 中根据第四消息向网关节点发送第五消息的步骤。

接收模块 902，用于执行上述实施例中步骤 307 中接收网关节点发送的第四消息的步骤。

可选地，发送模块 901，包括：

发送子模块，用于当第四消息中携带身份请求消息时，向网关节点发送第五消息，第五消息携带身份回复消息，身份回复消息用于响应身份请求消息，身份回复消息携带终端设备的永久身份标识；或者，

发送子模块还用于当第四消息中携带 EAP-AKA'/Identity-Request 消息时，向网关节点发送第五消息，第五消息携带 EAP-AKA'/Identity-Response 消息，EAP-AKA'/Identity-Request 消息用于触发对终端设备的鉴权流程，EAP-AKA'/Identity-Response 用于响应

EAP-AKA'/Identity-Request 消息，EAP-AKA'/Identity-Response 消息携带终端设备的永久身份标识；或者，

发送子模块还用于当第四消息中携带失败消息时，向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

可选地，第四消息中还携带第一失败原因值，第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，第一失败原因值还用于指示终端设备发送关联参数，以关联第一 IPsec 连接和第二 IPsec 连接，关联参数为用于关联第一 IPsec 连接与第二 IPsec 连接的参数；

发送模块 901 还用于：

断开所述终端设备与所述网关节点之间的第一 IPsec 连接，并建立所述终端设备与所述网关节点之间的第二 IPsec 连接；

终端设备通过第二 IPsec 连接向网关节点发送第五消息，第五消息还携带关联参数。

可选地，关联参数为全球唯一临时用户设备标识 GUTI、安全参数索引 SPI 或者 Cookie。

可选地，发送模块 901 具体用于：

当第四消息中携带第二失败原因值时，终端设备断开终端设备与网关节点之间的第一 IPsec 连接，并建立终端设备与网关节点之间的第二 IPsec 连接；

当第四消息中还携带失败消息或注册拒绝消息时，终端设备通过第二 IPsec 连接向网关节点发送第五消息，第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识。

参见图 10，本申请实施例提供了一种获取终端设备的身份标识的装置，该装置包含于控制面节点中，该装置包括：

接收模块 1001，用于执行上述实施例中的步骤 303、403、503、603 和 703；

处理模块 1002，用于执行上述实施例中的步骤 304、404、504、604 和 704；

发送模块 1003，用于执行上述实施例中的步骤 305、405、505、605 和 705；

在本申请实施例中，当控制面节点未能获取到终端设备的上下文时，可以向网关节点发送用于请求终端设备的永久身份标识的第三消息，之后，网关节点可以转发该第三消息给终端设备，从而将获取到的永久身份标识传回至该控制面节点。由此可见，在本申请实施例中，即使控制面节点未获取到终端设备的上下文，也可以通过网关节点的转发，获取到该终端设备的永久身份标识，从而使该终端设备具有成功接入网络的可能，相较于现有技术中一旦接入失败即需要重新再次接入的接入流程，本申请实施例的提供的方法将使接入流程变得更加方便，更加合理。

需要说明的是：上述实施例提供的获取终端设备的身份标识的装置在获取终端设备的身份标识时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将设备的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的获取终端设备的身份标识的装置与获取终端设备的身份标识的方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意结合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如：同轴电缆、光纤、数据用户线（Digital Subscriber Line，DSL））或无线（例如：红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如：软盘、硬盘、磁带）、光介质（例如：数字通用光盘（Digital Versatile Disc，DVD））、或者半导体介质（例如：固态硬盘（Solid State Disk，SSD））等。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

以上所述为本申请提供的实施例，并不用以限制本申请，凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

# 权 利 要 求 书

1、一种获取终端设备的身份标识的方法，其特征在于，所述方法包括：

网关节点接收终端设备发送的第一消息，并向控制面节点发送第二消息，所述第一消息和所述第二消息中均携带所述终端设备的临时身份标识；

所述网关节点接收所述控制面节点发送的第三消息，所述第三消息是所述控制面节点在无法获得所述终端设备的永久身份标识时发送的；

所述网关节点根据所述第三消息向所述终端设备发送第四消息，所述第四消息用于响应所述第一消息；

所述网关节点接收所述终端设备发送的第五消息，所述第五消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识。

2、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一互联网协议安全性 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述身份请求消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

3、如权利要求 2 所述的方法，其特征在于，所述第五消息携带身份回复消息和所述关联参数，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，其中，所述第六消息携带所述身份回复消息和可扩展鉴权协议身份响应 EAP-AKA'/Identity-Response 消息，且所述身份回复消息和所述 EAP-AKA'/Identity-Response 消息均携带所述永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息携带所述永久身份标识；或者，

所述网关节点根据所述关联参数，向所述网关节点向所述控制面节点发送第六消息，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述终端设备的永久身份标识。

4、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端

设备发送第四消息，包括：

当所述第三消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述第一失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

5、如权利要求 4 所述的方法，其特征在于，所述第五消息携带 EAP-AKA'/Identity-Response 消息和所述关联参数，所述 EAP-AKA'/Identity-Response 消息用于响应所述述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息；

其中，所述第六消息携带身份回复消息和所述 EAP-AKA'/Identity-Response 消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识。

6、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带失败消息和第一失败原因值；

其中，所述失败消息用于指示获取所述终端设备的上下文失败，所述第一失败原因值用于告知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

7、如权利要求 6 所述的方法，其特征在于，所述第五消息携带注册请求消息和所述关联参数，所述注册请求消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识。

8、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息，所述可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

9、如权利要求 8 所述的方法，其特征在于，所述第五消息携带可扩展鉴权协议身份响应 EAP-AKA'/Identity-Response 消息和所述关联参数，所述 EAP-AKA'/Identity-Response 消息用于响应所述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带所述 EAP-AKA'/Identity-Response 消息。

10、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息携带失败消息，且所述失败消息用于指示所述控制面节点无法确定终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述失败消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败。

11、如权利要求 1 所述的方法，其特征在于，所述网关节点根据所述第三消息向所述终端设备发送第四消息，包括：

当所述第三消息中携带通知消息，且所述通知消息用于向所述网关节点通知所述控制面节点无法确定所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带注册拒绝消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败。

12、如权利要求 10 或 11 所述的方法，其特征在于，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识；

所述网关节点根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识，包括：

所述网关节点向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息；

或者，

所述网关节点向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息和 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息用于触发对所述终端设备的鉴权流程。

13、一种获取终端设备的身份标识的方法，其特征在于，所述方法包括：

终端设备向网关节点发送第一消息，所述第一消息中携带所述终端设备的临时身份标识；

所述终端设备接收所述网关节点发送的第四消息，所述第四消息用于响应所述第一消息；

所述终端设备根据所述第四消息向所述网关节点发送第五消息，所述第五消息携带所述终端设备的永久身份标识。

14、如权利要求 13 所述的方法，其特征在于，所述终端设备根据所述第四消息向所述网关节点发送第五消息，包括：

当所述第四消息中携带身份请求消息，且所述身份请求消息用于请求所述终端设备的永久身份标识时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带可扩展鉴权协议身份请求 EAP-AKA'/Identity-Request 消息，且所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带可扩展鉴权协议身份响应 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述可扩展鉴权协议身份 EAP-AKA'/Identity-Response 用于响应所述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带失败消息，且所述失败消息用于指示所述控制面节点无法确定所述终端设备的永久身份标识时，所述终端设备向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

15、如权利要求 14 所述的方法，其特征在于，所述第四消息中还携带第一失败原因值，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接和第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接；

在所述终端设备向所述网关节点发送所述第五消息之前，还包括：

所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，并建立所述终端设备与所述网关节点之间的第二 IPsec 连接；

所述终端设备向所述网关节点发送所述第五消息，包括：

所述终端设备通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息还携带所述关联参数。

16、如权利要求 15 所述的方法，其特征在于，所述关联参数为全球唯一临时用户设备标识 GUTI、安全参数索引 SPI 或者 Cookie。

17、如权利要求 13 所述的方法，其特征在于，所述终端设备根据所述第四消息向所述网关节点发送第五消息，包括：

当所述第四消息中携带第二失败原因值和失败消息，所述第二失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述失败消息用于通知所述终端设备所述控制面节点无法确定所述终端设备的永久身份标识时，所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，建立与所述网关节点的之间的第二 IPsec 连接，并通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识；或者，

当所述第四消息中携带第二失败原因值和注册拒绝消息，所述第二失败原因值用于通知所述终端设备第一 IPsec 连接失败时，所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，建立与所述网关节点之间的第二 IPsec 连接，并通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

18 一种获取终端设备的身份标识的方法，其特征在于，所述方法包括：

控制面节点接收网关节点发送的第二消息，所述第二消息中携带终端设备的临时身份标识；

所述控制面节点根据所述临时身份标识查找所述终端设备的上下文；

当所述控制面节点未获取到所述终端设备的上下文时，向所述网关节点发送第三消息；

所述控制面节点接收所述网关节点发送的所述终端设备的永久身份标识。

19、一种获取终端设备的身份标识的装置，所述装置包含于网关节点，其特征在于，所述装置包括：

接收模块，用于接收终端设备发送的第一消息，并向控制面节点发送第二消息，所述第一消息和所述第二消息中均携带所述终端设备的临时身份标识；

所述接收模块用于接收所述控制面节点发送的第三消息，所述第三消息用于向所述终端设备通知无法获得所述终端设备的永久身份标识；

发送模块，用于根据所述第三消息向所述终端设备发送第四消息，所述第四消息用于响应所述第一消息；

所述接收模块用于接收所述终端设备发送的第五消息，所述第五消息携带所述终端设备的永久身份标识；

所述发送模块用于根据所述第五消息向所述控制面节点发送所述终端设备的永久身份标识。

20、如权利要求 19 所述的装置，其特征在于，所述发送模块包括：

发送子模块，用于当所述第三消息中携带身份请求消息，所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一互联网协议安全性 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述身份请求消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

21、如权利要求 20 所述的装置，其特征在于，所述第五消息携带身份回复消息和所述关联参数，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；

所述发送子模块用于：

根据所述关联参数，向所述控制面节点发送第六消息，其中，所述第六消息携带所述身份回复消息和 EAP-AKA'/Identity-Response 消息，且所述身份回复消息和所述 EAP-AKA'/Identity-Response 消息均携带所述永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息携带所述永久身份标识；或者，

根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述终端设备的永久身份标识。

22、如权利要求 19 所述的装置，其特征在于，所述发送模块，包括：

发送子模块，用于当所述第三消息中携带身份请求消息，所述身份请求消息用于请求所述终端设备的永久身份标识时，通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述第一失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

23、如权利要求 22 所述的装置，其特征在于，所述第五消息携带

EAP-AKA'/Identity-Response 消息和所述关联参数，所述 EAP-AKA'/Identity-Response 消息用于响应所述述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；

所述发送子模块用于：

根据所述关联参数，向所述控制面节点发送第六消息；

其中，所述第六消息携带身份回复消息和所述 EAP-AKA'/Identity-Response 消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，所述第六消息携带所述身份回复消息，所述身份回复消息携带所述 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识。

24、如权利要求 19 所述的装置，其特征在于，所述发送模块，包括：

发送子模块，用于当所述第三消息携带身份请求消息，所述身份请求消息用于请求所述终端设备的永久身份标识时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带失败消息和第一失败原因值；

其中，所述失败消息用于指示获取所述终端设备的上下文失败，所述第一失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

25、如权利要求 24 所述的装置，其特征在于，所述第五消息携带注册请求消息和所述关联参数，所述注册请求消息携带所述终端设备的永久身份标识；

所述发送子模块用于：

根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识。

26、如权利要求 19 所述的装置，其特征在于，所述发送模块，包括：

当所述第三消息中携带 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述 EAP-AKA'/Identity-Request 消息和第一失败原因值；

其中，所述第一失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，所述第一失败原因值还用于指示终端设备发送关联参数，以关联所述第一 IPsec 连接与第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

27、如权利要求 26 所述的装置，其特征在于，所述第五消息携带 EAP-AKA'/Identity-Response 消息和关联参数，所述 EAP-AKA'/Identity-Response 消息用于响应所述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；

所述发送子模块用于：

根据所述关联参数，向所述控制面节点发送第六消息，所述第六消息携带所述 EAP-AKA'/Identity-Response 消息。

28、如权利要求 19 所述的装置，其特征在于，所述发送模块，包括：

发送子模块，用于当所述第三消息携带失败消息，所述失败消息用于指示所述控制面节点获取所述终端设备的上下文失败时，通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带所述失败消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败，并关联所述第一 IPsec 连接与第二 IPsec 连接，所述第二 IPsec 连接是在断开所述第一 IPsec 连接之后建立的 IPsec 连接。

29、如权利要求 28 所述的装置，其特征在于，所述发送子模块还用于：

当所述第三消息中携带通知消息，且所述通知消息用于向所述网关节点通知所述控制面节点获取所述终端设备的上下文失败时，所述网关节点通过所述网关节点与所述终端设备之间的第一 IPsec 连接向所述终端设备发送所述第四消息，所述第四消息携带注册拒绝消息和第二失败原因值；

其中，所述第二失败原因值用于通知所述终端设备所述第一 IPsec 连接失败。

30、如权利要求 28 或 29 所述的装置，其特征在于，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识；

所述发送模块，包括：

所述发送子模块，用于向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息；或者，

所述发送子模块，用于向所述控制面节点发送第六消息，所述第六消息携带所述注册请求消息和 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Response 消息用于触发对所述终端设备的鉴权流程。

31、一种获取终端设备的身份标识的装置，所述装置包含于终端设备中，其特征在于，所述装置包括：

发送模块，用于向网关节点发送第一消息，所述第一消息中携带所述终端设备的临时身份标识；

接收模块，用于所述终端设备接收所述网关节点发送的第四消息，所述第四消息用于响应所述第一消息；

所述发送模块，用于所述终端设备根据所述第四消息向所述网关节点发送第五消息，所

述第五消息携带所述终端设备的永久身份标识。

32、如权利要求 31 所述的装置，其特征在于，所述发送模块，包括：

发送子模块，用于当所述第四消息中携带身份请求消息时，向所述网关节点发送所述第五消息，所述第五消息携带身份回复消息，所述身份回复消息用于响应所述身份请求消息，所述身份回复消息携带所述终端设备的永久身份标识；或者，

所述发送子模块还用于当所述第四消息中携带 EAP-AKA'/Identity-Request 消息时，向所述网关节点发送所述第五消息，所述第五消息携带 EAP-AKA'/Identity-Response 消息，所述 EAP-AKA'/Identity-Request 消息用于触发对所述终端设备的鉴权流程，所述 EAP-AKA'/Identity-Response 用于响应所述 EAP-AKA'/Identity-Request 消息，所述 EAP-AKA'/Identity-Response 消息携带所述终端设备的永久身份标识；或者，

所述发送子模块还用于当所述第四消息中携带失败消息时，向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

33、如权利要求 32 所述的装置，其特征在于，所述第四消息中还携带第一失败原因值，所述第一失败原因值用于通知所述终端设备第一 IPsec 连接失败，所述第一失败原因值还用于指示所述终端设备发送关联参数，以关联所述第一 IPsec 连接和第二 IPsec 连接，所述关联参数为用于关联所述第一 IPsec 连接与所述第二 IPsec 连接的参数；

所述发送模块还用于：

断开所述终端设备与所述网关节点之间的第一 IPsec 连接，并建立所述终端设备与所述网关节点之间的第二 IPsec 连接；

所述终端设备通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息还携带所述关联参数。

34、如权利要求 33 所述的装置，其特征在于，所述关联参数为全球唯一临时用户设备标识 GUTI、安全参数索引 SPI 或者 Cookie。

35、如权利要求 31 所述的装置，其特征在于，所述发送模块具体用于：

当所述第四消息中携带第二失败原因值时，所述终端设备断开所述终端设备与所述网关节点之间的第一 IPsec 连接，并建立所述终端设备与所述网关节点之间的第二 IPsec 连接；

当所述第四消息中还携带失败消息或注册拒绝消息时，所述终端设备通过所述第二 IPsec 连接向所述网关节点发送所述第五消息，所述第五消息携带注册请求消息，所述注册请求消息携带所述终端设备的永久身份标识。

36、一种获取终端设备的身份标识的装置，所述装置包含于控制面节点中，其特征在于，所述装置包括：

接收模块，用于接收网关节点发送的第二消息，所述第二消息中携带终端设备的临时身份标识；

处理模块，用于根据所述临时身份标识查找所述终端设备的上下文；

发送模块，用于当所述处理模块未获取到所述终端设备的上下文时，向所述网关节点发送第三消息，所述第三消息用于请求所述终端设备的永久身份标识；

所述接收模块还用于接收所述网关节点发送的所述终端设备的永久身份标识。

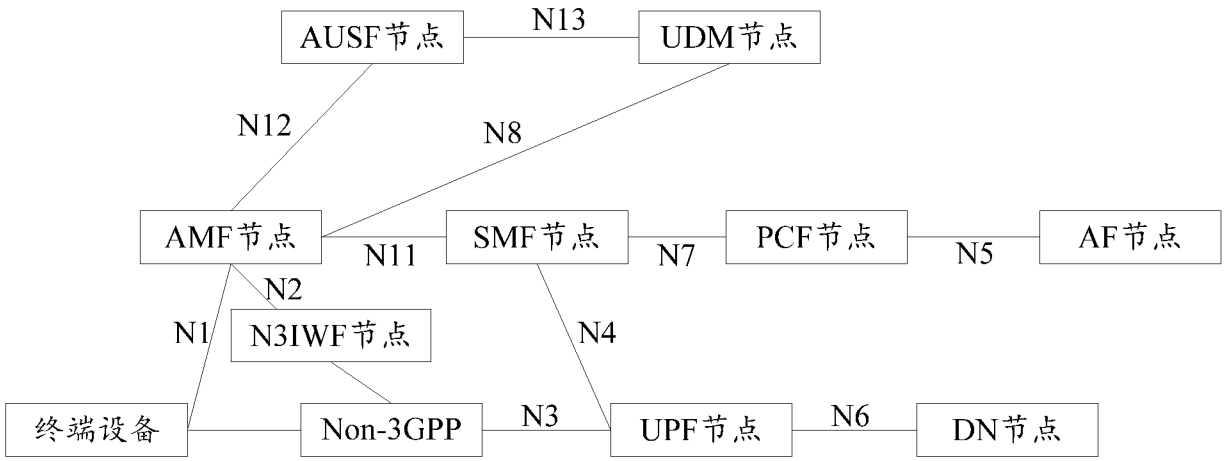
AUSF节点
N13
UDM节点
N12
N8
AMF节点
N11
SMF节点
N7
PCF节点
N5
AF节点
N2
N1
N3IWF节点
N4
终端设备
Non-3GPP
N3
UPF节点
N6
DN节点

图 1

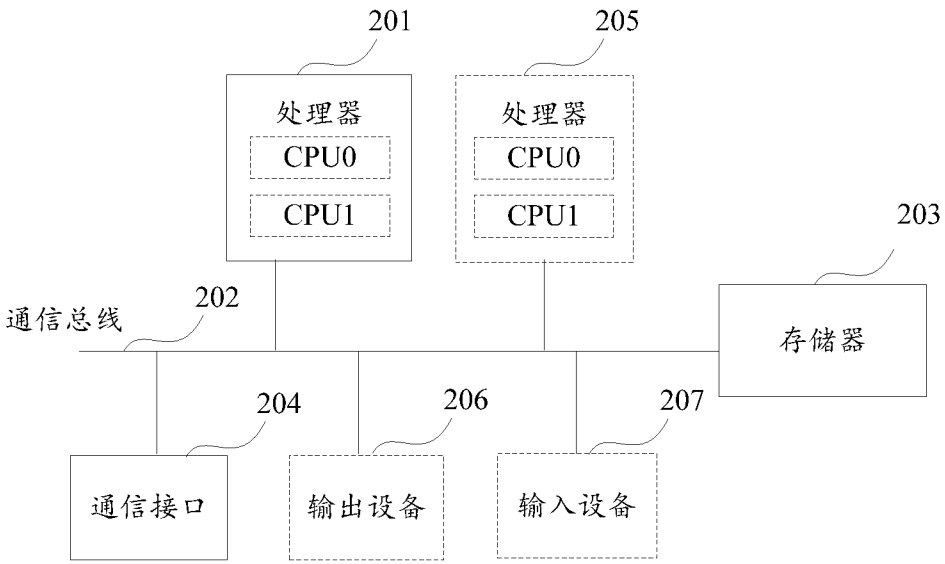
201
205
处理器
CPU0
CPU1
处理器
CPU0
CPU1
203
202
通信总线
存储器
204
206
207
通信接口
输出设备
输入设备

图 2A

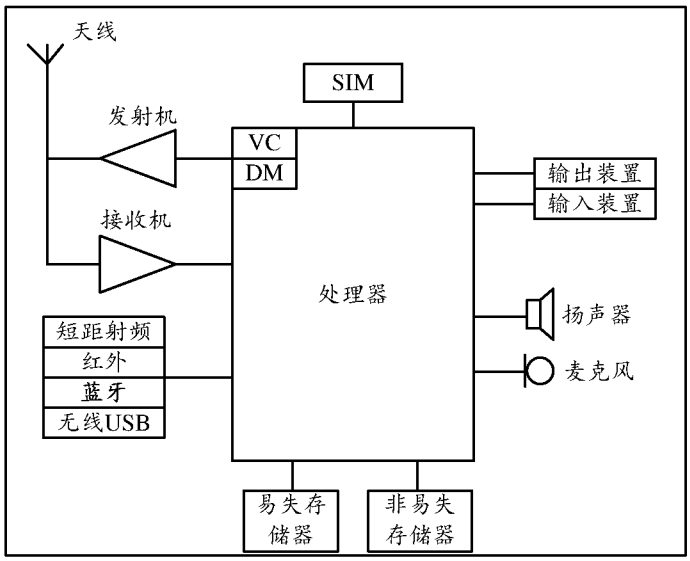
天线
SIM
发射机
VC
DM
输出装置
输入装置
接收机
处理器
扬声器
麦克风
短距射频
红外
蓝牙
无线USB
易失存储器
非易失存储器

图 2B

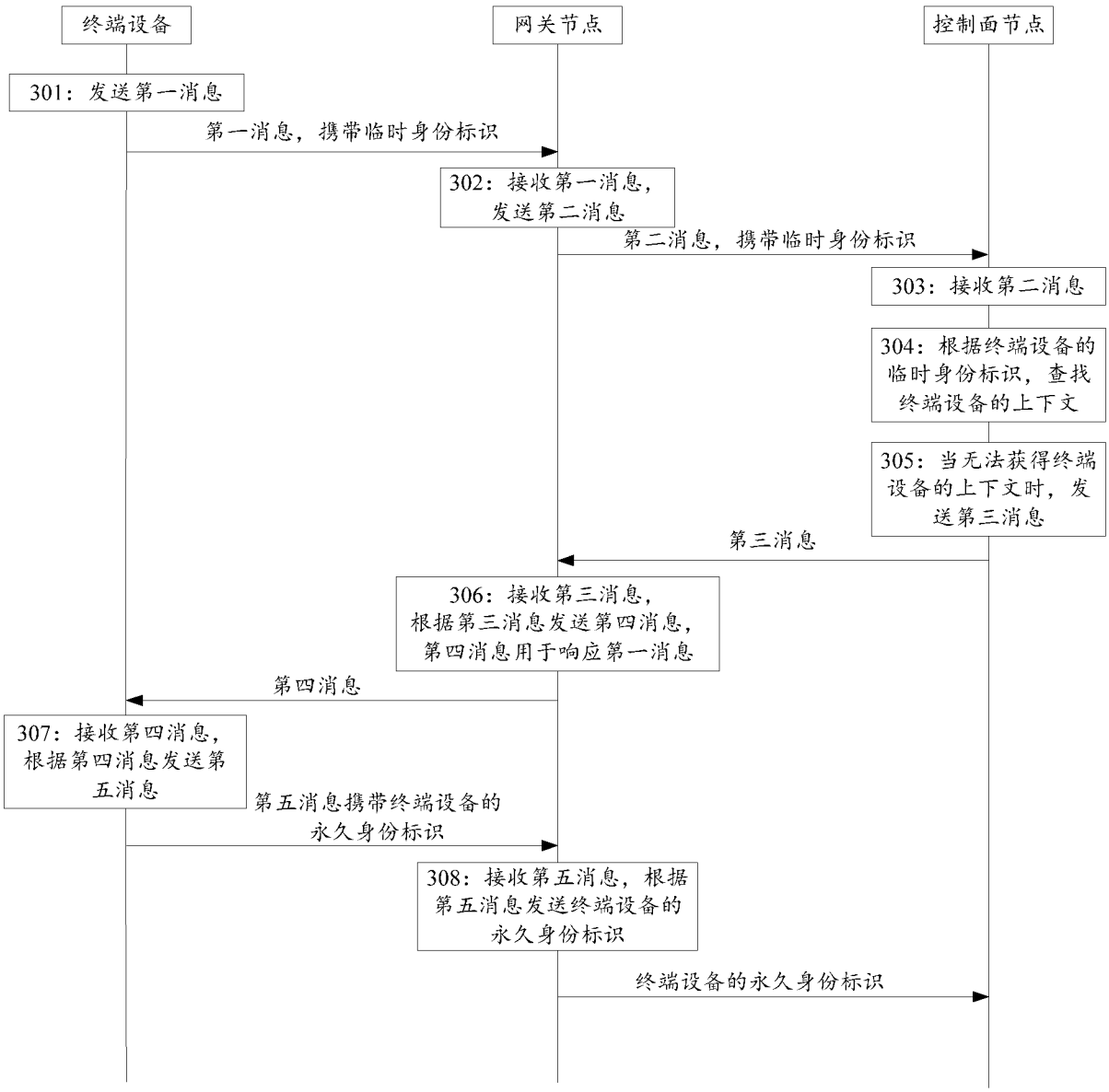
终端设备
网关节点
控制面节点
301：发送第一消息
第一消息，携带临时身份标识
302：接收第一消息，发送第二消息
第二消息，携带临时身份标识
303：接收第二消息
304：根据终端设备的临时身份标识，查找终端设备的上下文
305：当无法获得终端设备的上下文时，发送第三消息
第三消息
306：接收第三消息，根据第三消息发送第四消息，第四消息用于响应第一消息
第四消息
307：接收第四消息，根据第四消息发送第五消息
第五消息携带终端设备的永久身份标识
308：接收第五消息，根据第五消息发送终端设备的永久身份标识
终端设备的永久身份标识

图 3

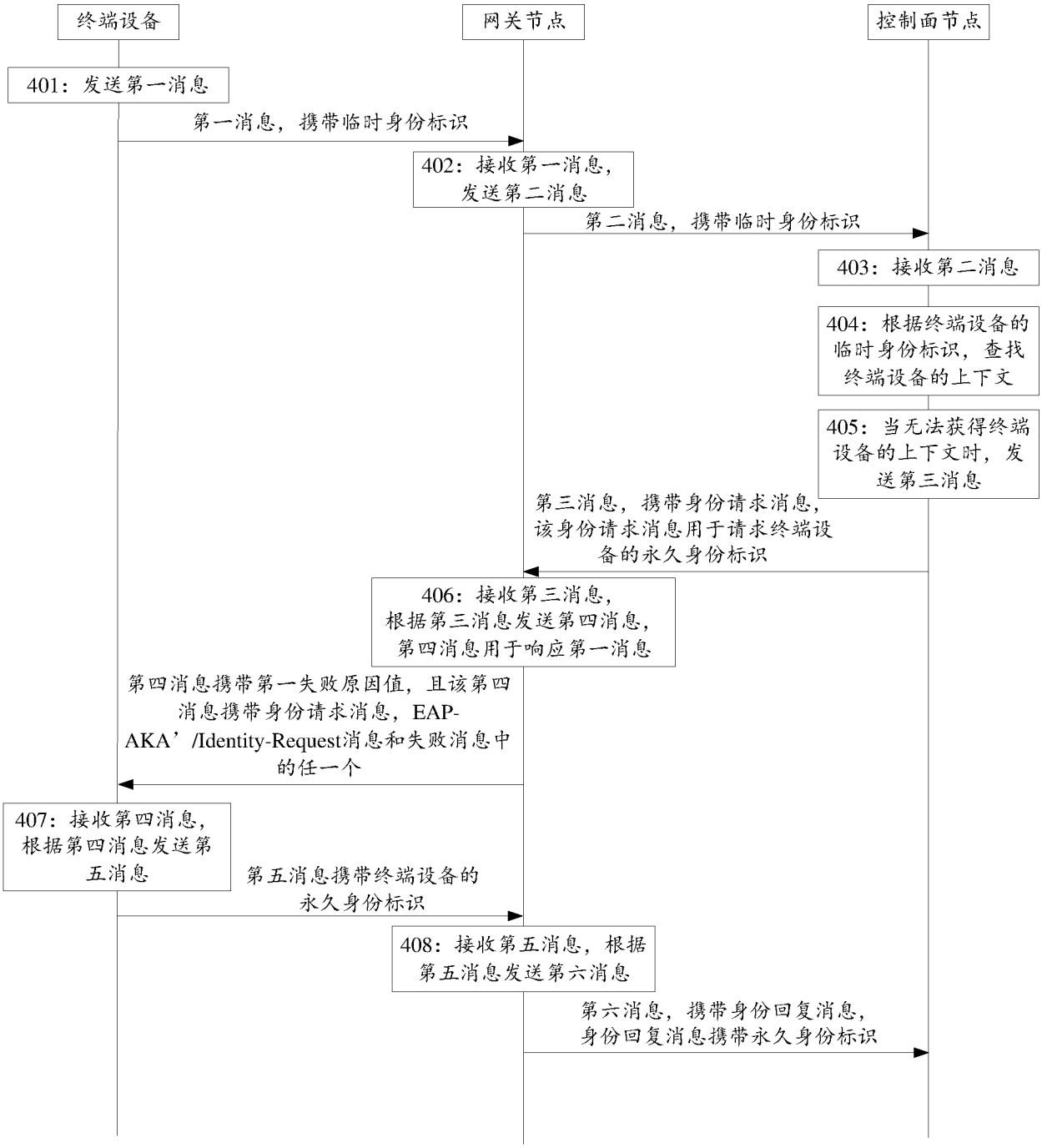
终端设备
网关节点
控制面节点
401：发送第一消息
第一消息，携带临时身份标识
402：接收第一消息，发送第二消息
第二消息，携带临时身份标识
403：接收第二消息
404：根据终端设备的临时身份标识，查找终端设备的上下文
405：当无法获得终端设备的上下文时，发送第三消息
第三消息，携带身份请求消息，该身份请求消息用于请求终端设备的永久身份标识
406：接收第三消息，根据第三消息发送第四消息，第四消息用于响应第一消息
第四消息携带第一失败原因值，且该第四消息携带身份请求消息，EAP-AKA'/Identity-Request消息和失败消息中的任一个
407：接收第四消息，根据第四消息发送第五消息
第五消息携带终端设备的永久身份标识
408：接收第五消息，根据第五消息发送第六消息
第六消息，携带身份回复消息，身份回复消息携带永久身份标识

图 4

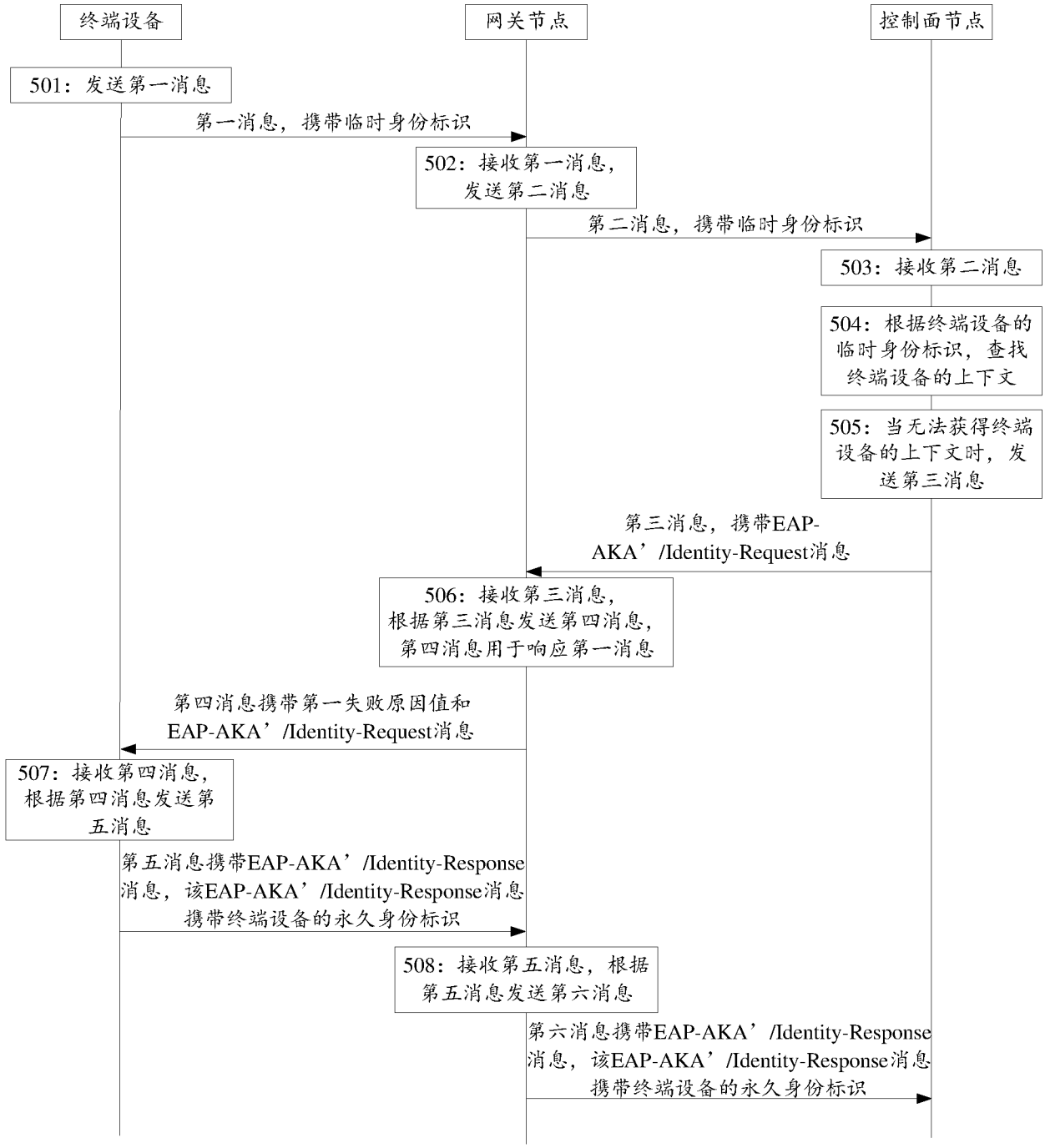
终端设备
网关节点
控制面节点
501：发送第一消息
第一消息，携带临时身份标识
502：接收第一消息，发送第二消息
第二消息，携带临时身份标识
503：接收第二消息
504：根据终端设备的临时身份标识，查找终端设备的上下文
505：当无法获得终端设备的上下文时，发送第三消息
第三消息，携带EAP-AKA’/Identity-Request消息
506：接收第三消息，根据第三消息发送第四消息，第四消息用于响应第一消息
第四消息携带第一失败原因值和EAP-AKA’/Identity-Request消息
507：接收第四消息，根据第四消息发送第五消息
第五消息携带EAP-AKA’/Identity-Response消息，该EAP-AKA’/Identity-Response消息携带终端设备的永久身份标识
508：接收第五消息，根据第五消息发送第六消息
第六消息携带EAP-AKA’/Identity-Response消息，该EAP-AKA’/Identity-Response消息携带终端设备的永久身份标识

图 5

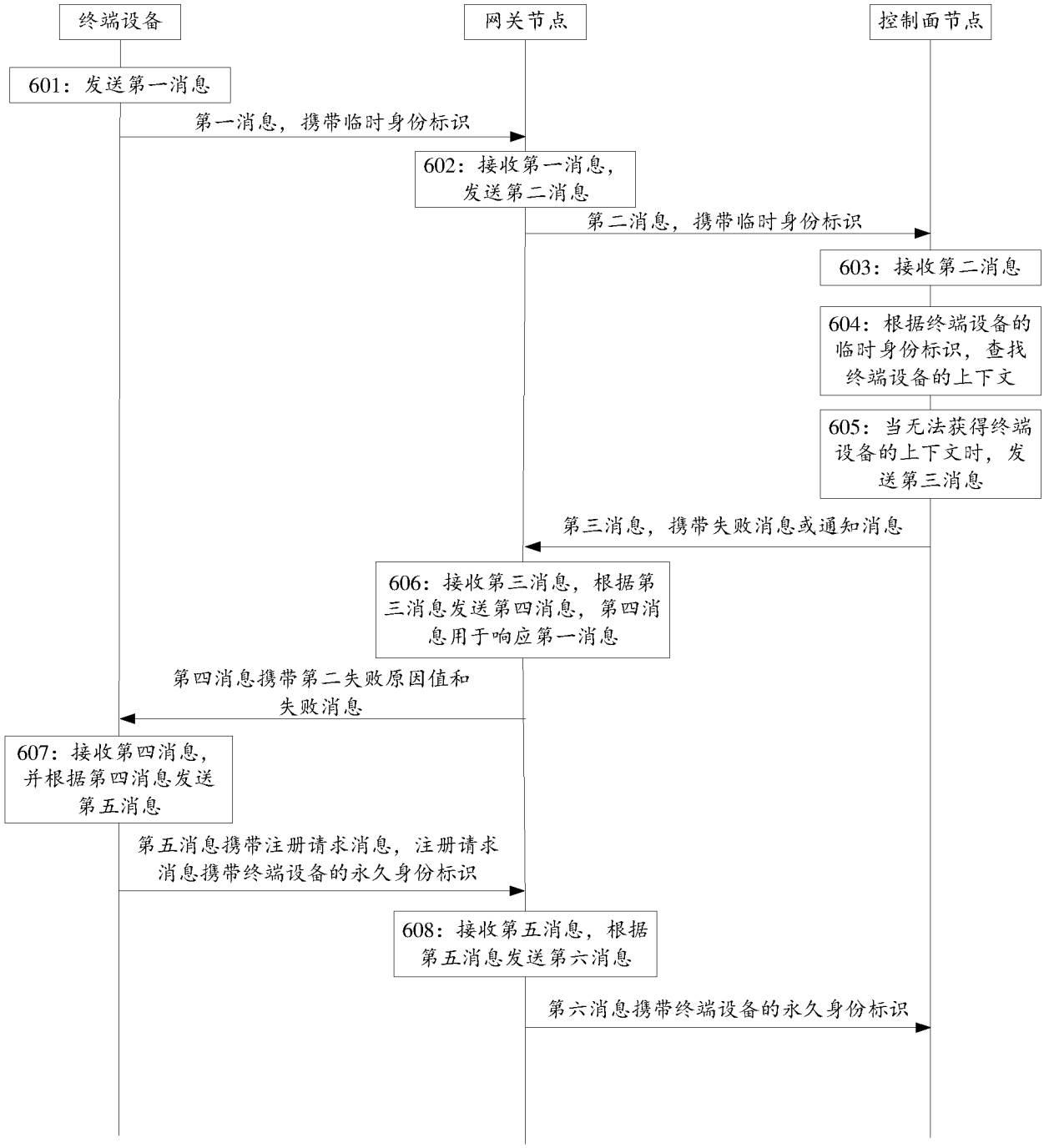
终端设备
网关节点
控制面节点
601：发送第一消息
第一消息，携带临时身份标识
602：接收第一消息，发送第二消息
第二消息，携带临时身份标识
603：接收第二消息
604：根据终端设备的临时身份标识，查找终端设备的上下文
605：当无法获得终端设备的上下文时，发送第三消息
第三消息，携带失败消息或通知消息
606：接收第三消息，根据第三消息发送第四消息，第四消息用于响应第一消息
第四消息携带第二失败原因值和失败消息
607：接收第四消息，并根据第四消息发送第五消息
第五消息携带注册请求消息，注册请求消息携带终端设备的永久身份标识
608：接收第五消息，根据第五消息发送第六消息
第六消息携带终端设备的永久身份标识

图 6

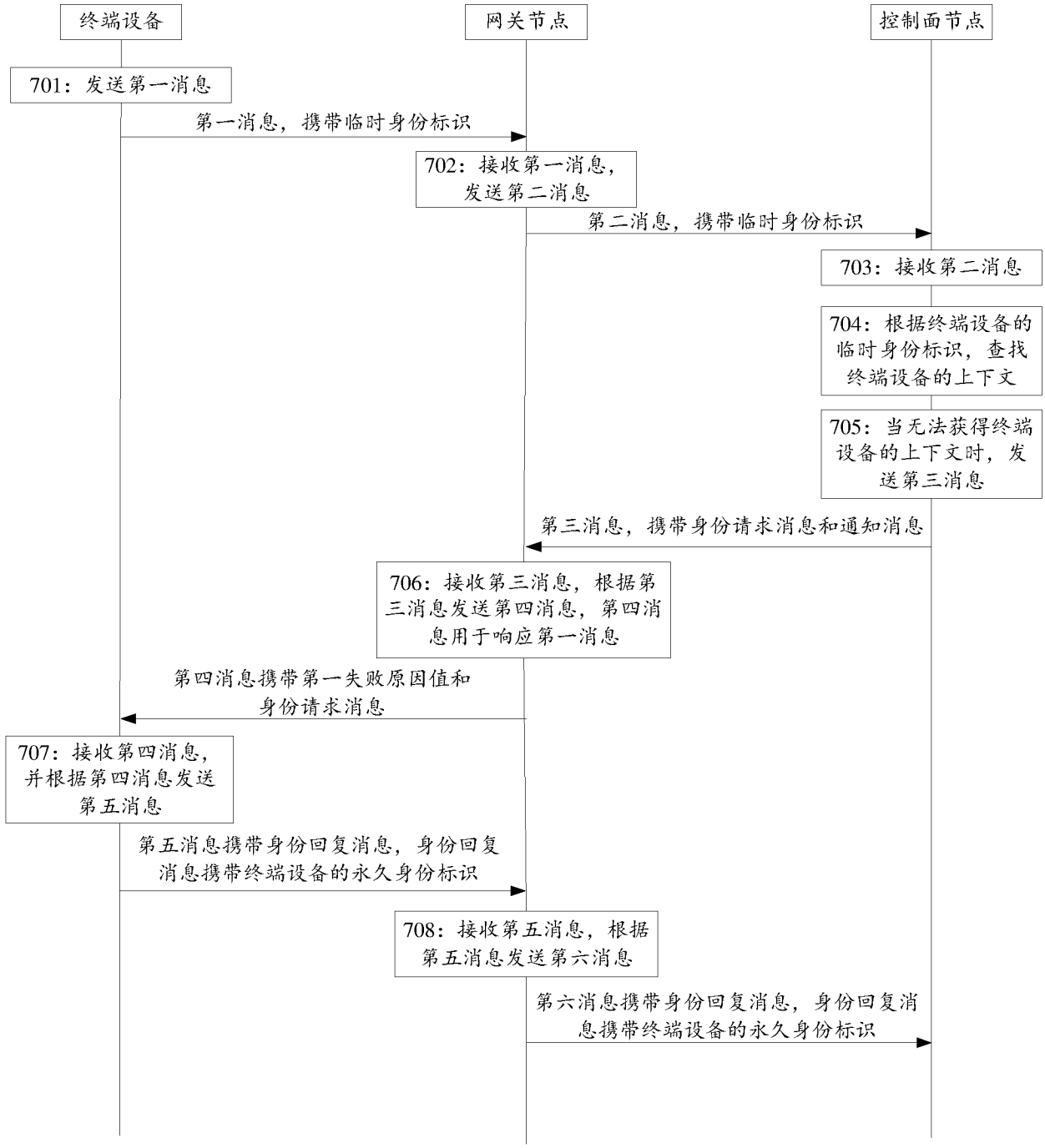
终端设备
网关节点
控制面节点
701：发送第一消息
第一消息，携带临时身份标识
702：接收第一消息，发送第二消息
第二消息，携带临时身份标识
703：接收第二消息
704：根据终端设备的临时身份标识，查找终端设备的上下文
705：当无法获得终端设备的上下文时，发送第三消息
第三消息，携带身份请求消息和通知消息
706：接收第三消息，根据第三消息发送第四消息，第四消息用于响应第一消息
第四消息携带第一失败原因值和身份请求消息
707：接收第四消息，并根据第四消息发送第五消息
第五消息携带身份回复消息，身份回复消息携带终端设备的永久身份标识
708：接收第五消息，根据第五消息发送第六消息
第六消息携带身份回复消息，身份回复消息携带终端设备的永久身份标识

图 7

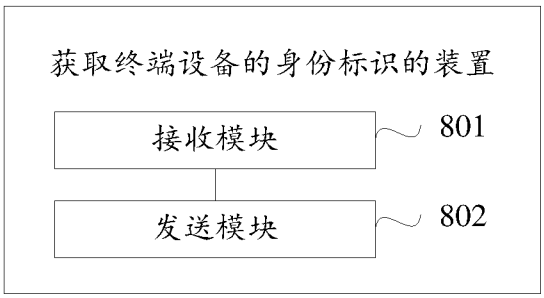
获取终端设备的身份标识的装置
接收模块
801
发送模块
802

图 8

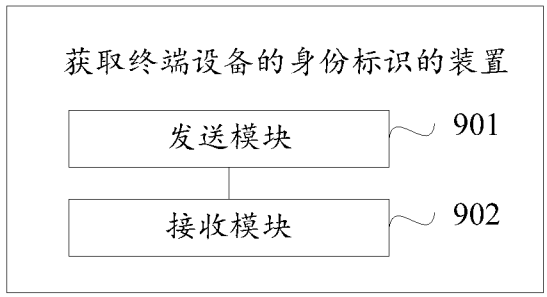
获取终端设备的身份标识的装置
发送模块
901
接收模块
902

图 9

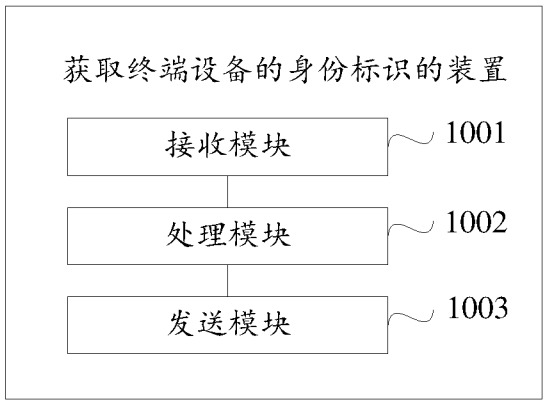
获取终端设备的身份标识的装置
接收模块
1001
处理模块
1002
发送模块
1003

图 10

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2018/097088**

## A. CLASSIFICATION OF SUBJECT MATTER

H04W 8/26(2009.01)i

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

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; CNABS; VEN; DWPI; 3GPP; WOTXT, EPTXT, USTXT: 临时身份标识, 永久身份标识, 互联网协议安全, 非3GPP, AMF, N3IWF, International Mobile Subscriber Identity, IPsec, Temporary Mobile Subscriber Identity, TMSI, EAP, IMSI

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 102724649 B (ZTE CORPORATION) 05 April 2017 (2017-04-05)<br>description, paragraphs 0105-0121, and figure 4 | 1, 18, 19, 36 |
| X | CN 101400054 A (HUAWEI TECHNOLOGIES CO., LTD.) 01 April 2009 (2009-04-01)<br>description, page 9, line 8 to page 10, line 8, and figure 5 | 13, 31 |
| A | CN 101034982 A (HUAWEI TECHNOLOGIES CO., LTD.) 12 September 2007 (2007-09-12)<br>entire document | 1-36 |
| A | CN 101039181 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 September 2007 (2007-09-19)<br>entire document | 1-36 |
| A | CN 101090358 A (HUAWEI TECHNOLOGIES CO., LTD.) 19 December 2007 (2007-12-19)<br>entire document | 1-36 |

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| **20 September 2018** | **28 September 2018** |

| Name and mailing address of the ISA/CN | Authorized officer |
|---|---|
| **State Intellectual Property Office of the P. R. China**<br>**No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing**<br>**100088**<br>**China** | |
| Facsimile No. **(86-10)62019451** | Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2018/097088**

| Patent document cited in search report | | | Publication date (day/month/year) | Patent family member(s) | | | Publication date (day/month/year) |
|---|---|---|---|---|---|---|---|
| CN | 102724649 | B | 10 October 2012 | CN | 102724649 | B | 05 April 2017 |
| CN | 101400054 | A | 01 April 2009 | CN | 101400054 | B | 17 October 2012 |
| CN | 101034982 | A | 12 September 2007 | | None | | |
| CN | 101039181 | A | 19 September 2007 | EP | 2560342 | A3 | 12 June 2013 |
| | | | | EP | 2723037 | A1 | 23 April 2014 |
| | | | | ES | 2481046 | T3 | 29 July 2014 |
| | | | | US | 2012246464 | A1 | 27 September 2012 |
| | | | | EP | 1995908 | A1 | 26 November 2008 |
| | | | | US | 8230213 | B2 | 24 July 2012 |
| | | | | US | 2014181930 | A1 | 26 June 2014 |
| | | | | US | 2009013184 | A1 | 08 January 2009 |
| | | | | EP | 2560342 | B1 | 14 May 2014 |
| | | | | EP | 1995908 | A4 | 25 November 2009 |
| | | | | WO | 2007104248 | A1 | 20 September 2007 |
| | | | | US | 8707041 | B2 | 22 April 2014 |
| | | | | CN | 101039181 | B | 08 September 2010 |
| | | | | EP | 1995908 | B1 | 17 July 2013 |
| | | | | EP | 2560342 | A2 | 20 February 2013 |
| CN | 101090358 | A | 19 December 2007 | WO | 2007147344 | A1 | 27 December 2007 |
| | | | | CN | 101090358 | B | 02 February 2011 |

# 国际检索报告

国际申请号
PCT/CN2018/097088

A. 主题的分类

H04W 8/26(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W H04L H04B

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT;CNABS;VEN;DWPI;3GPP;WOTXT,EPTXT,USTXT: 临时身份标识，永久身份标识，互联网协议安全，非3GPP，AMF，N3IWF，International Mobile Subscriber Identity，IPsec，Temporary Mobile Subscriber Identity，TMSI，EAP，IMSI

C. 相关文件

| 类 型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| X | CN 102724649 B (中兴通讯股份有限公司) 2017年 4月 5日 (2017-04-05)<br>说明书第0105-0121段，附图4 | 1，18，19，36 |
| X | CN 101400054 A (华为技术有限公司) 2009年 4月 1日 (2009-04-01)<br>说明书第9页第8行-第10页第8行，附图5 | 13，31 |
| A | CN 101034982 A (华为技术有限公司) 2007年 9月 12日 (2007-09-12)<br>全文 | 1-36 |
| A | CN 101039181 A (华为技术有限公司) 2007年 9月 19日 (2007-09-19)<br>全文 | 1-36 |
| A | CN 101090358 A (华为技术有限公司) 2007年 12月 19日 (2007-12-19)<br>全文 | 1-36 |

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

| 国际检索实际完成的日期 | 国际检索报告邮寄日期 |
|---|---|
| 2018年 9月 20日 | 2018年 9月 28日 |

| ISA/CN的名称和邮寄地址 | 受权官员 |
|---|---|
| 中华人民共和国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451 | 金曦<br>电话号码 86-(010)-62089554 |

# 国际检索报告
## 关于同族专利的信息

国际申请号
PCT/CN2018/097088

| 检索报告引用的专利文件 | | | 公布日（年/月/日） | 同族专利 | | | 公布日（年/月/日） |
|---|---|---|---|---|---|---|---|
| CN | 102724649 | B | 2012年 10月 10日 | CN | 102724649 | B | 2017年 4月 5日 |
| CN | 101400054 | A | 2009年 4月 1日 | CN | 101400054 | B | 2012年 10月 17日 |
| CN | 101034982 | A | 2007年 9月 12日 | | 无 | | |
| CN | 101039181 | A | 2007年 9月 19日 | EP | 2560342 | A3 | 2013年 6月 12日 |
| | | | | EP | 2723037 | A1 | 2014年 4月 23日 |
| | | | | ES | 2481046 | T3 | 2014年 7月 29日 |
| | | | | US | 2012246464 | A1 | 2012年 9月 27日 |
| | | | | EP | 1995908 | A1 | 2008年 11月 26日 |
| | | | | US | 8230213 | B2 | 2012年 7月 24日 |
| | | | | US | 2014181930 | A1 | 2014年 6月 26日 |
| | | | | US | 2009013184 | A1 | 2009年 1月 8日 |
| | | | | EP | 2560342 | B1 | 2014年 5月 14日 |
| | | | | EP | 1995908 | A4 | 2009年 11月 25日 |
| | | | | WO | 2007104248 | A1 | 2007年 9月 20日 |
| | | | | US | 8707041 | B2 | 2014年 4月 22日 |
| | | | | CN | 101039181 | B | 2010年 9月 8日 |
| | | | | EP | 1995908 | B1 | 2013年 7月 17日 |
| | | | | EP | 2560342 | A2 | 2013年 2月 20日 |
| CN | 101090358 | A | 2007年 12月 19日 | WO | 2007147344 | A1 | 2007年 12月 27日 |
| | | | | CN | 101090358 | B | 2011年 2月 2日 |