(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
2011 年 3 月 24 日 (24.03.2011)

PCT

(10) 国际公布号
WO 2011/032515 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01) *H04L 9/32* (2006.01)
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2010/077085

(22) 国际申请日: 2010 年 9 月 19 日 (19.09.2010)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200910093828.5 2009 年 9 月 21 日 (21.09.2009) CN

(71) 申请人 (对除美国外的所有指定国): **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; 及

(75) 发明人/申请人 (仅对美国): **毕晓宇 (BI, Xiaoyu)** [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)。 **张爱琴 (ZHANG, Aiqin)** [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)。 **张冬梅 (ZHANG, Dongmei)** [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)。

(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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, 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, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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))。

[见续页]

(54) **Title**: METHOD AND DEVICE FOR AUTHENTICATION PROCESSING

(54) **发明名称** : 认证处理方法及装置

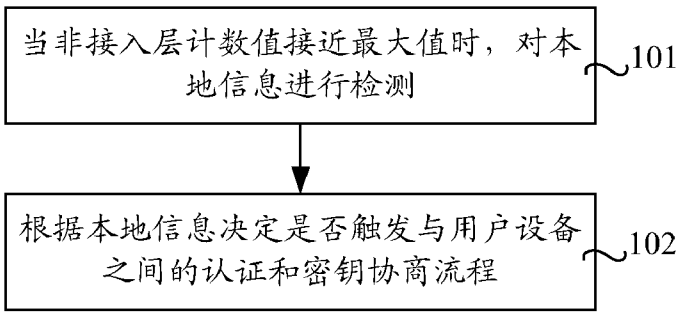

图 1 / FIG. 1

101 WHEN THE NON-ACCESS STRATUM (NAS) COUNT VALUE APPROACHES TO THE MAXIMUM VALUE, DETECTING THE LOCAL INFORMATION
102 DECIDING WHETHER TO TRIGGER AN AUTHENTICATION AND KEY AGREEMENT FLOW WITH A USER EQUIPMENT ACCORDING TO THE LOCAL INFORMATION

(57) **Abstract**: The embodiments of the invention disclose a method and device for authentication processing. The method includes: in the case of encountering failure during performing authentication and key agreement (AKA) flow on a user equipment (UE), determining whether the network policy supports non-authentication for the current service; if the network policy supports non-authentication for the current service, and the current service does not need authentication, keeping on executing the current service; or if the network policy supports non-authentication for the current service, and the UE does not have the capacity of executing AKA flow, keeping on executing the current service; or if the network policy supports non-authentication for the current service, and the UE does not have an inserted card, then keeping on executing the current service. In the embodiments of the invention, if performing Evolved Packet System (EPS) AKA flow encounters failure, the connection will not be released at once, but the connection is released or the current service keeps on being executed according to the local information and the network policy, thereby avoiding releasing the connections unnecessary to be released and saving resources.

[见续页]

WO 2011/032515 A1

(57) 摘要:

本发明实施例涉及一种认证处理方法及装置，包括：在对用户设备执行认证和密钥协商流程失败的情况下，确定网络策略是否支持当前业务不认证，若所述网络策略支持当前业务不认证，且所述当前业务为不需要进行认证的业务，则继续执行所述当前业务；或者若所述网络策略支持当前业务不认证，且所述用户设备不具有执行认证和密钥协商流程的能力，则继续执行所述当前业务；或者若所述网络策略支持当前业务不认证，且所述用户设备无插入卡，则继续执行所述当前业务。本发明实施例中，如果执行 EPS AKA 流程认证失败，不会立即释放连接，而是根据本地信息及网络策略释放连接或者继续执行当前业务，避免了释放没有必要进行释放的连接，节省了资源。

认证处理方法及装置

本申请要求于 2009 年 9 月 21 日提交中国专利局、申请号为 200910093828.5、发明名称为"认证处理方法及装置"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

本发明实施例涉及通信领域，尤其涉及一种认证处理方法及装置。

背景技术

非接入层（Non-Access Stratum，简称：NAS）计数（COUNT）是长期演进（Long Term Evolution，简称：LTE）系统中安全上下文的一部分。在 LTE 系统中，NAS 计数可作为密钥的生命周期，使密钥具有新鲜性；同时，NAS 计数可以保证用户设备（User Equipment，简称：UE）与网络侧密钥的同步，具有抗重放攻击的作用。每一套演进分组系统（Evolved Packet System，简称：EPS）安全上下文包含两个独立的 NAS 计数值：上行 NAS 计数值和下行 NAS 计数值。这两个 NAS 计数的计数器分别由 UE 和移动管理实体（Mobility Management Entity，简称：MME）来独立维护。

NAS 计数有 32 位，主要由两个部分组成：NAS 序列号（SQN）与 NAS 溢出值（OVERFLOW），其中 NAS 序列号为 8 位，NAS 溢出值为 16 位。NAS 序列号承载于每条 NAS 消息中，当每一个新的或是重传的受到安全保护的 NAS 消息发出后，发送端将会将 NAS 序列号的值增加 1；当 NAS 序列号增加到最大值，循环一圈时，NAS 溢出值增加 1。

现有技术中，当 MME 检测到下行的 NAS 计数值即将环绕的时候，也就是 NAS 计数值比较接近最大值 2^{24} 时，MME 将会触发一个新的 EPS 认证和密钥协商（Authentication and Key Agreement，简称：AKA）流程，建立新的安全上下文，并且当安全上下文被激活时将 NAS 计数值初始化为 0。

当 MME 检测到 UE 的上行 NAS 计数值也接近到最大值时，也就是即将环绕时，MME 会触发 EPS AKA 流程。

现有技术如果执行 EPS AKA 流程认证失败，就立即释放连接。这种安全处理过程浪费了资源。

发明内容

本发明实施例提供了一种认证处理方法及装置，用以节省资源。

本发明实施例提供了另一种认证处理方法，包括:

在对用户设备执行认证和密钥协商流程失败的情况下，无线通信网络侧设备确定网络策略是否支持当前业务不认证，

若所述网络策略支持当前业务不认证，且所述当前业务为不需要进行认证的业务，则继续执行所述当前业务；或者

若所述网络策略支持当前业务不认证，且所述用户设备不具有执行认证和密钥协商流程的能力，则继续执行所述当前业务；或者

若所述网络策略支持当前业务不认证，且所述用户设备无插入卡，则继续执行所述当前业务。

本发明实施例提供了另一种认证处理装置，包括:

执行模块，用于执行认证和密钥协商流程;

处理模块，位于无线通信网络侧设备内，包括:

第一判断单元，用于在对用户设备执行认证和密钥协商流程失败的情况下，确定网络策略是否支持当前业务不认证，

第二判断单元，用于在所述网络策略支持当前业务不认证的情况下，确定所述当前业务是否是需要进行认证的业务，或者所述用户设备是否具有执行认证和密钥协商流程的能力，或者所述用户设备是否具有插入卡;

执行单元，用于在所述第二判断单元判断为所述当前业务是不需要进行认证的业务，或者所述用户设备不具有执行认证和密钥协商流程的能力，

或者所述用户设备不具有插入卡的情况下况下，继续执行所述当前业务。

本发明实施例中，如果执行 EPS AKA 流程认证失败，不会立即释放连接，而是根据本地信息及网络策略释放连接或者继续执行当前业务，避免了释放没有必要进行释放的连接，节省了资源。

附图说明

图 1 为本发明实施例一认证处理方法的流程图；

图 2 为本发明实施例二认证处理方法的流程图；

图 3 为本发明实施例三认证处理方法的流程图；

图 4 为本发明实施例四认证处理方法的流程图；

图 5 为本发明实施例五认证处理方法的流程图；

图 6 为本发明实施例六认证处理方法的流程图；

图 7 为本发明实施例七认证处理方法的流程图；

图 8 为本发明实施例八认证处理装置的结构示意图；

图 9 为本发明实施例九认证处理装置的结构示意图；

图 10 为本发明实施例十认证处理装置的结构示意图；

图 11 为本发明实施例十一认证处理装置的结构示意图；

图 12 为本发明实施例十二认证处理装置的结构示意图；

图 13 为本发明实施例十三认证处理装置的结构示意图。

具体实施方式

下面通过附图和实施例，对本发明实施例的技术方案做进一步的详细描述。

图 1 为本发明实施例一认证处理方法的流程图。如图 1 所示，本实施例具体包括如下步骤：

步骤 101、当非接入层计数值接近最大值时，对本地信息进行检测；

步骤 102、根据本地信息决定是否触发与用户设备之间的认证和密钥协商流程。

其中 NAS 计数值接近最大值即为 NAS 计数值即将环绕的时候，认证和密钥协商流程可以为 EPS AKA 流程。

上述两步骤的执行主体可以为 MME，当下行或上行的 NAS 计数值即将环绕的时候，MME 对本地信息进行检测，根据检测结果决定是否触发 EPS AKA 流程。

以检测上行的 NAS 计数值为例，MME 接收 NAS 消息，NAS 计数值加 1；MME 检测 NAS 计数值是否接近最大值，具体地，MME 可以检测 NAS 计数值是否等于门限值，该门限值为预先设定的接近最大值的数值；若是，则对本地信息进行检测，根据检测结果决定是否触发认证和密钥协商流程；否则，继续接收 NAS 消息。

本实施例中 MME 不会一旦检测到 NAS 计数值即将环绕，就立即触发 EPS AKA 流程，减少了触发 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

下面在描述实施例二之前，预先介绍与实施例二相关的技术。

在 LTE 系统中，EPS 安全上下文有两种划分方式。按照使用状态，EPS 安全上下文可以分为当前 EPS 安全上下文（current EPS security context）和非当前 EPS 安全上下文（non-current EPS security context）。其中当前 EPS 安全上下文是指最新被激活的安全上下文，即当前正在使用的安全上下文。上述当前正在使用的安全上下文可以与一套非当前本地 EPS 安全上下文（non-current native EPS security context）同时存在。按照生成方式，EPS 安全上下文可以分为映射 EPS 安全上下文（mapped EPS security context）和本地 EPS 安全上下文（native EPS security context）。其中映射 EPS 安全上下文是指从其他系统映射过来的安全上下文，如从通用移动通信系统（Universal Mobile Telecommunications System，简称：UMTS）映射到 LTE

系统。本地 EPS 安全上下文是指在 LTE 系统中，经过 EPS AKA 生成的安全上下文。其中本地 EPS 安全上下文又分为部分本地 EPS 安全上下文（partial native EPS security context）和完整本地 EPS 安全上下文（full native EPS security context）。其主要区别是部分本地 EPS 安全上下文没有经过一个成功的 NAS 安全模式流程运行，因此在部分本地 EPS 安全上下文中只包含 UE 接入 LTE 网络中认证的根密钥 K_{ASME} 、密钥集标识（Key Set Identity，简称：KSI）、UE 的安全能力以及设置为 0 的 NAS 计数值；而完整本地 EPS 安全上下文是经过 EPS AKA 流程之后由一个成功的 NAS 安全模式命令（Security Mode Command，简称：SMC）流程激活的安全上下文，其包含一套完整 EPS NAS 安全上下文，因此完整本地 EPS 安全上下文会额外包含 NAS 层的完整性密钥 K_{NASint} 、加密密钥 K_{NASenc} 以及所选的 NAS 加密算法和完整性算法标识。

图 2 为本发明实施例二认证处理方法的流程图。本实施例中本地信息为本地保存的安全上下文，下述安全上下文均为本地 EPS 安全上下文。

如图 2 所示，本实施例具体包括如下步骤：

步骤 201、MME 接收 NAS 消息，NAS 计数值加 1。

步骤 202、MME 检测 NAS 计数值是否接近最大值，若是，则执行步骤 203；否则执行步骤 201。

具体地，可以预先设定一接近最大值的数值作为门限值，MME 检测 NAS 计数值是否等于门限值，若是，则执行步骤 203；否则执行步骤 201。

步骤 203、MME 检测本地保存的安全上下文除了当前安全上下文以外，是否还包括非当前安全上下文，若是，则执行步骤 204；否则触发 EPS AKA 流程。

步骤 204、激活该非当前安全上下文。

上述非当前安全上下文可通过成功运行 NAS SMC 流程来激活。成功运行的 NAS SMC 流程包括：MME 使用安全上下文对 NAS SMC 消息进行完整性保护，当 UE 对 NAS SMC 消息完整性验证成功，向 MME 发送 NAS

安全模式完成（Security Mode Complete）消息，MME 解密 NAS 安全模式完成消息并进行完整性验证。则 MME 可以获知与 UE 共享此安全上下文，且该安全上下文被激活。因此步骤 204 通过成功执行上述 NAS SMC 流程，激活非当前安全上下文。

进一步的，如果上述 NAS SMC 流程运行失败，则 MME 触发 EPS AKA 流程。

上述非当前本地安全上下文可以包括非当前部分本地安全上下文或非当前完整本地安全上下文，上述步骤 204 可以为：MME 激活非当前部分本地安全上下文或非当前完整本地安全上下文。

本实施例中，通过成功运行 MME 触发的 NAS SMC 流程，MME 与 UE 共享的非当前本地安全上下文被激活。当 MME 没有收到 UE 返回的 NAS 安全模式完成消息时，MME 触发 EPS AKA 流程。

下面通过两个具体的例子，说明本实施例的应用场景。

（1）当 MME 检测到 NAS 计数值接近最大值时，MME 通过检测安全上下文获知 MME 和 UMTS 用户身份模块集成电路卡（UMTS Subscriber Identity Module Integrated Circuit Card，简称：UICC）中保存了一套非当前部分安全上下文，MME 激活该非当前部分安全上下文，此时 NAS 计数值被初始化为 0，这样省去了 EPS AKA 流程。

与现有技术相比，该场景中 MME 没有立即触发 EPS AKA 流程，避免了非当前部分安全上下文资源的浪费，同时也避免了因执行没有必要的 EPS AKA 流程而造成的资源耗费。

（2）UE 在接入 EPS 的过程中建立了当前安全上下文，之后 UE 在从演进通用地面无线接入网络（Evolved Universal Terrestrial Radio Access Network，简称：E-UTRAN）切换到通用地面无线接入网络（Universal Terrestrial Radio Access Network，简称：UTRAN）或 GSM／EDGE 无线通讯网络（GSM EDGE Radio Access Network，简称：GERAN）的过程中保存这套在 E-UTRAN 中生成的本地安全上下文；然后，当该 UE 再切换回到

E-UTRAN 中时，使用的是映射安全上下文，该映射安全上下文成为当前安全上下文，之前 UE 和 MME 保存的在 E-UTRAN 网络中生成的安全上下文成为非当前完整安全上下文。在这种场景下，当 MME 检测到 NAS 计数值接近最大值时，MME 通过检测安全上下文获知本地保存有该非当前完整安全上下文，则 MME 激活该非当前完整安全上下文，这样省去了 EPS AKA 流程。

与现有技术相比，该场景中 MME 没有立即触发 EPS AKA 流程，避免了之前保存的非当前完整安全上下文资源的浪费，同时也避免了因执行没有必要的 EPS AKA 流程而造成的资源耗费。

本实施例中 MME 不会一旦检测到 NAS 计数值即将环绕，就立即触发 EPS AKA 流程，减少了触发 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

图 3 为本发明实施例三认证处理方法的流程图。本实施例中本地信息为定时器状态。本实施例中，MME 上预先设置了一定时器，该定时器的状态可以为运行和停止。当 NAS 计数器的计数值到达门限值且 EPS AKA 流程成功完成时，定时器的状态转为运行；当定时器的定时时间到达设定的时间门限值时，定时器的状态转为停止。

如图 3 所示，本实施例具体包括如下步骤:

步骤 301、MME 接收 NAS 消息，NAS 计数值加 1。

步骤 302、MME 检测 NAS 计数值是否接近最大值，若是，则执行步骤 303；否则执行步骤 301。

具体地，本实施例预先设定一接近最大值的数值作为门限值，如设为 2^{24}-100，MME 检测 NAS 计数值是否等于 2^{24}-100，若是，则执行步骤 303；否则执行步骤 301。

步骤 303、MME 检测定时器状态是否为运行，若是，则执行步骤 304；否则触发 EPS AKA 流程。

步骤 304、激活非当前安全上下文。

所述该非当前安全上下文是由一个成功的NAS SMC流程运行激活的。一个成功的NAS SMC流程包括：MME使用安全上下文对NAS SMC消息进行完整性保护，当UE对NAS SMC消息完整性验证成功，向MME发送NAS 安全模式完成消息，MME解密NAS安全模式完成消息并进行完整性验证。则MME可以获知与UE共享此安全上下文，且该安全上下文被激活。因此步骤304通过成功执行上述NAS SMC流程，激活非当前本地安全上下文。

进一步的，如果上述NAS SMC流程运行失败，则MME触发EPS AKA流程。

在实际应用中，下行NAS计数值和上行NAS计数值一般相差不大，当 MME 检测到下行 NAS 计数值即将环绕时，不久之后即将检测到上行NAS计数值即将环绕；并且，MME触发EPS AKA流程之后隔一段时间，MME触发NAS SMC流程，通过执行NAS SMC流程，NAS计数值被初始化为0。如果当 MME 检测到下行 NAS 计数值即将环绕时，MME 就触发EPS AKA流程，而在检测到上行NAS计数值即将环绕之前，没有触发NAS SMC流程激活新产生的安全上下文，此时NAS计数值没有被初始化，那么现有技术检测到上行NAS计数值即将环绕，又会再次触发EPS AKA流程。本实施例通过检测定时器状态可以获知距离上次EPS AKA流程成功完成的时间是否已经到达设定的时间门限值，该时间门限值是根据EPS AKA流程成功完成到触发NAS SMC之间的时间来确定的，当本次NAS计数值接近最大值距离上次EPS AKA流程成功完成的时间小于设定的时间门限值时，MME触发NAS SMC流程；当本次NAS计数值接近最大值距离上次EPS AKA流程成功完成的时间大于或等于设定的时间门限值时，MME触发EPS AKA流程。因此，针对上述实际应用的场景，本实施例避免了在检测到上行NAS计数值即将环绕之前，没有触发NAS SMC流程，就又会再次触发EPS AKA流程，减少了EPS AKA流程的次数，避免了因触发没有必要的EPS AKA流程导致的资源耗费，节省了资源。

图 4 为本发明实施例四认证处理方法的流程图。本实施例中本地信息为状态器状态。本实施例中，MME 上需预先设置状态器，该状态器的状态可以为运行和停止，具体地，可以用 0 来表示运行，可以用 1 来表示停止。其中，运行表示距离上次 EPS AKA 流程成功完成的时间小于设定的时间门限值，停止表示距离上次 EPS AKA 流程成功完成的时间大于或等于设定的时间门限值。状态器可以由定时器来触发。

如图 4 所示，本实施例具体包括如下步骤:

步骤 401、MME 接收 NAS 消息，NAS 计数值加 1。

步骤 402、MME 检测 NAS 计数值是否接近最大值，若是，则执行步骤 403；否则执行步骤 401。

具体地，本实施例预先设定一接近最大值的数值作为门限值，如设为 2^{24}-100，MME 检测 NAS 计数值是否等于 2^{24}-100，若是，则执行步骤 403；否则触发 EPS AKA 流程。

步骤 403、MME 检测状态器状态是否为 0，若是，则执行步骤 404；否则触发 EPS AKA 流程。

步骤 404、激活非当前安全上下文。

所述该非当前安全上下文是由一个成功的 NAS SMC 流程运行激活的。一个成功的 NAS SMC 流程包括：MME 使用安全上下文对 NAS SMC 消息进行完整性保护，当 UE 对 NAS SMC 消息完整性验证成功，向 MME 发送 NAS 安全模式完成消息，MME 解密 NAS 安全模式完成消息并进行完整性验证。则 MME 可以获知与 UE 共享此安全上下文，且该安全上下文被激活。因此步骤 404 通过成功执行上述 NAS SMC 流程，激活非当前本地安全上下文。

进一步的，如果上述 NAS SMC 流程运行失败，则 MME 触发 EPS AKA 流程。

在实际应用中，下行 NAS 计数值和上行 NAS 计数值一般相差不大，当 MME 检测到下行 NAS 计数值即将环绕时，不久之后即将检测到上行

NAS 计数值即将环绕；并且，MME 触发 EPS AKA 流程之后隔一段时间，MME 触发 NAS SMC 流程，通过执行 NAS SMC 流程，NAS 计数值被初始化为 0。如果当 MME 检测到下行 NAS 计数值即将环绕时，MME 就触发 EPS AKA 流程，而在检测到上行 NAS 计数值即将环绕之前，没有触发 NAS SMC，此时 NAS 计数值没有被初始化，那么现有技术检测到上行 NAS 计数值即将环绕，又会再次触发 EPS AKA 流程。本实施例通过检测状态器状态可以获知距离上次 EPS AKA 流程成功完成的时间是否已经到达设定的时间门限值，该时间门限值是根据 EPS AKA 流程成功完成到触发 NAS SMC 之间的时间来确定的，当本次 NAS 计数值接近最大值距离上次 EPS AKA 流程成功完成的时间小于设定的时间门限值时，MME 触发 NAS SMC；当本次 NAS 计数值接近最大值距离上次 EPS AKA 流程成功完成的时间大于或等于设定的时间门限值时，MME 触发 EPS AKA 流程。因此，针对上述实际应用的场景，本实施例避免了在检测到上行 NAS 计数值即将环绕之前，没有触发 NAS SMC，就又会再次触发 EPS AKA 流程，减少了 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

图 5 为本发明实施例五认证处理方法的流程图。本实施例中本地信息为当前业务类型、服务质量（Quality of Service，简称：QoS）或用户设备执行认证的能力。

如图 5 所示，本实施例具体包括如下步骤：

步骤 501、MME 接收 NAS 消息，NAS 计数值加 1。

步骤 502、MME 检测 NAS 计数值是否接近最大值，若是，则执行步骤 503；否则执行步骤 501。

具体地，可以预先设定一接近最大值的数值作为门限值，MME 检测 NAS 计数值是否等于门限值，若是，则执行步骤 503；否则执行步骤 501。

步骤 503、MME 通过检测当前业务类型，检测当前业务类型对应的 UE 请求的当前业务是否为需要进行认证的业务；或者，MME 通过检测 QoS，

检测 QoS 对应的 UE 请求的当前业务是否为需要进行认证的业务；或者，MME 通过检测 UE 执行认证的能力，检测 UE 是否具有执行 EPS AKA 流程的能力；

若是，则触发 EPS AKA 流程；否则执行步骤 504。

步骤 504、继续使用当前的安全上下文，或者对当前业务不进行安全保护，或者中断当前业务的连接。

举例来说，本实施例通过检测当前业务类型获知 UE 请求的业务为紧急呼叫（Emergency Call，简称：EMC）业务，则检测出 UE 请求的业务不是需要进行认证的业务，则不再触发 EPS AKA 流程，而忽略 NAS 计数值接近最大值的检测结果，可以继续使用当前的安全上下文，或者对当前业务不进行安全保护，或者中断当前业务的连接。

当插入用户标识模块（Subscriber Identity Module，简称：SIM 卡）的 UE 从 UMTS 网络的紧急呼叫切换到 LTE 网络，MME 从通用分组无线业务（General Packet Radio Service，简称：GPRS）服务支持节点（Service GPRS Support Node，简称：SGSN）得到安全参数 Kc，并且进一步根据加密密钥（Cipher Key，简称：CK）和完整性密钥（Integrity Key，简称：IK）得到 K_{ASME}。NAS 计数值从 0 开始。此时，UE 在 LTE 网络中的安全保护是由 K_{ASME} 所派生的子密钥所保护的。当 NAS 计数值即将环绕时，MME 可以根据 Kc 检测出 UE 是 SIM 卡用户，不具有执行 EPS AKA 流程的能力，则 MME 不再触发 EPS AKA 流程，而忽略 NAS 计数值接近最大值的检测结果，可以继续使用当前的安全上下文，或者对当前业务不进行安全保护，或者中断当前业务的连接。

本实施例在 UE 请求的业务不是需要进行认证的业务或 UE 不具有执行认证和密钥协商流程的能力时，不触发 EPS AKA 流程，减少了 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

图 6 为本发明实施例六认证处理方法的流程图。如图 6 所示，本实施

例具体包括如下步骤:

步骤 601、MME 接收 NAS 消息，NAS 计数值加 1。

步骤 602、MME 检测 NAS 计数值是否接近最大值，若是，则执行步骤 603；否则执行步骤 601。该 NAS 计数值可以为上行 NAS 计数值，也可以为下行 NAS 计数值。

具体地，可以预先设定一接近最大值的数值作为门限值，MME 检测 NAS 计数值是否等于门限值，若是，则执行步骤 603；否则执行步骤 601。

步骤 603、MME 触发 EPS AKA 流程，同时 MME 触发 NAS SMC，激活 AKA 流程产生的安全上下文，NAS 计数值被初始化为 0。

本实施例将 EPS AKA 流程与 NAS SMC 的执行绑定在一起，避免了因检测到不同方向（上行方向和下行方向）NAS 计数值即将环绕，重复触发 EPS AKA 流程，减少了 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

图 7 为本发明实施例七认证处理方法的流程图。如图 7 所示，本实施例具体包括如下步骤:

步骤 801、MME 发起 EPS AKA 流程;

步骤 802、在执行 EPS AKA 流程失败的情况下，根据本地信息及网络策略决定释放连接或者继续执行当前业务。

进一步的，上述步骤 801 中 MME 发起 EPS AKA 流程可以在若干种条件下进行，例如：可以当 NAS 计数值接近最大值时，MME 发起 EPS AKA 流程；也可以由运营商的策略触发 EPS AKA 流程，具体地，运营商可以设置一定的本次策略，由 MME 来触发对其下 UE 的 EPS AKA，这可以是运营商基于一定的安全策略或者其他需求而制定的策略;还可以当 UE 进行网络间切换时，触发 EPS AKA 流程，具体地，当 UE 从安全级别较低的网络（如 GSM 或 UMTS 网络）切换（包括激活态的切换和空闲态移动）到安全级别较高的网络（如 LTE 网络）时，由网络侧触发 EPS AKA 流程。

本地信息可以包括以下信息的至少之一：当前业务类型，服务质量，

用户设备执行认证的能力，网络策略，用户识别模块类型或用户设备是否插入卡的信息。其中，当前业务类型指明了当前业务的类型信息，MME 可以根据当前业务类型确定当前业务是否为需要进行认证的业务。服务质量能够标识无需进行认证的业务，所以 MME 也可以根据服务质量确定当前业务是否为需要进行认证的业务。UE 执行认证的能力指明了 UE 是否具有执行 EPS AKA 的能力的相关信息，MME 可以根据 UE 执行认证的能力确定 UE 是否具有执行 EPS AKA 的能力。SIM 卡类型也指明了 UE 是否具有执行 EPS AKA 的能力的相关信息，MME 可以根据 SIM 卡类型确定 UE 是否具有执行 EPS AKA 的能力。由于认证需要在 UE 插入卡的情况下进行，如果 UE 插入卡后执行 EPS AKA 流程失败，那么就应该释放 NAS 信令连接；如果 UE 没有插入卡，则根据网络策略确定是否释放连接。网络策略是网络侧设备设定的策略，其可以支持当前业务是否进行认证。

根据以上本地信息及网络策略的内容，上述步骤 802 可以具体包括：

MME 若确定网络策略不支持当前业务不认证，则释放当前业务的连接；

MME 若确定网络策略支持当前业务不认证，且 MME 若根据本地信息中的当前业务类型或服务质量确定当前业务为不需要进行认证的业务，或者且 MME 若根据本地信息中的用户设备执行认证的能力或用户识别模块类型确定用户设备不具有执行认证和密钥协商流程的能力，或者且用户设备无插入卡，则继续执行当前业务；

MME 若确定网络策略支持当前业务不认证，且 MME 若根据本地信息中的当前业务类型或服务质量确定当前业务为需要进行认证的业务，或者且 MME 若根据本地信息中的用户设备执行认证的能力或用户识别模块类型确定用户设备具有执行认证和密钥协商流程的能力，或者且用户设备存在插入卡，则释放当前业务的连接。

举例来说，在 MME 确定网络策略支持当前业务不认证的场景下，MME 通过检测当前业务类型，获知 UE 请求的业务为 EMC 业务或公共报警业务，

由于 EMC 业务或公共报警业务不是需要进行认证的业务，且网络策略支持未认证的 EMC 或公共报警业务，则 MME 和 UE 继续执行当前业务。

如果当前业务为 NAS 信令连接中的单一业务，则可以通过释放 NAS 信令连接来实现释放当前业务的连接。如果 NAS 信令连接中承载了多个业务，且根据当前业务类型确定该多个当前业务均需要进行认证，则释放 NAS 信令连接。如果当前既包括需要认证的业务又包括不需要认证的业务（如 EMC），则释放上述需要认证的业务所对应的 EPS 承载，而保持不需要认证的业务的 EPS 承载（如 EMC 承载）。上述 EPS 承载是建立在 NAS 信令连接基础上的。

本实施例在认证失败，UE 请求的业务不是需要进行认证的业务或 UE 不具有执行 EPS AKA 流程的能力或用户设备未插入卡，且网络策略支持当前业务不认证的情况下仍然能继续执行当前业务，避免了当前业务执行中断的问题，节省了系统的资源。

图 8 为本发明实施例八认证处理装置的结构示意图。如图 8 所示，本实施例具体包括检测模块 11 和处理模块 12。其中，检测模块 11 用于当非接入层计数值接近最大值时，对本地信息进行检测；处理模块 12 用于根据检测结果决定是否触发与 UE 之间的认证和密钥协商流程。

本实施例提供的认证处理装置可以按照上述实施例一提供的方法来工作。

图 9 为本发明实施例九认证处理装置的结构示意图。如图 9 所示，本实施例在上述实施例八的基础上，本地信息为安全上下文，处理模块 12 具体包括第一激活单元 21 和第一触发单元 22。其中，第一激活单元 21 用于当检测模块 11 确定安全上下文包括非当前安全上下文，则激活非当前安全上下文；第一触发单元 22 用于当检测模块 11 确定安全上下文不包括非当前安全上下文，则触发认证和密钥协商流程。

本实施例处理模块 12 还可以包括收发单元 23，该收发单元 23 用于向 UE 发送 NAS SMC，并接收 NAS 安全模式执行成功的消息，向处理模块

12 中的第一激活单元 21 发送触发其动作的信息。第一激活单元 21 根据触发信息激活非当前安全上下文。当收发单元 23 没有接收到 UE 返回的 NAS 安全模式执行成功的消息时，第一触发单元 22 触发认证和密钥协商流程。

本实施例提供的认证处理装置可以按照上述实施例二提供的方法来工作。

图 10 为本发明实施例十认证处理装置的结构示意图。如图 10 所示，本实施例在上述实施例八的基础上，本地信息为定时器状态，处理模块 12 具体包括第二激活单元 31 和第二触发单元 32。其中，第二激活单元 31 用于当检测模块 11 检测出定时器状态为运行时，激活非当前安全上下文；第二触发单元 32 用于当检测模块 11 检测出定时器状态为停止时，触发认证和密钥协商流程。

进一步的，本实施例处理模块 12 还可以包括收发单元 33，该收发单元 33 用于向 UE 发送 NAS SMC，并接收 NAS 安全模式执行成功的消息，向处理模块 12 中的第二激活单元 31 发送触发其动作的信息。第二激活单元 31 根据触发信息激活非当前安全上下文。当收发单元 33 没有接收到 UE 返回的 NAS 安全模式执行成功的消息时，第二触发单元 32 触发认证和密钥协商流程。

本实施例提供的认证处理装置可以按照上述实施例三提供的方法来工作。

图 11 为本发明实施例十一认证处理装置的结构示意图。如图 11 所示，本实施例在上述实施例八的基础上，本地信息为状态器状态，处理模块 12 具体包括第三激活单元 41 和第三触发单元 42。其中，第三激活单元 41 用于当检测模块 11 检测出状态器状态为运行时，激活非当前安全上下文；第三触发单元 42 用于当检测模块 11 检测出状态器状态为停止时，触发认证和密钥协商流程。

进一步的，本实施例处理模块 12 还可以包括收发单元 43，该收发单元 43 用于向 UE 发送 NAS SMC，并接收 NAS 安全模式执行成功的消息，向

处理模块 12 中的第三激活单元 41 发送触发其动作的信息。第三激活单元 41 根据触发信息激活非当前安全上下文。当收发单元 43 没有接收到 UE 返回的 NAS 安全模式执行成功的消息时，第三触发单元 42 触发认证和密钥协商流程。

本实施例提供的认证处理装置可以按照上述实施例四提供的方法来工作。

图 12 为本发明实施例十二认证处理装置的结构示意图。如图 12 所示，本实施例在上述实施例八的基础上，本地信息为当前的业务类型、或服务质量、或用户设备执行认证的能力，处理模块 12 具体包括第四触发单元 51 和处理单元 52。该第四触发单元 51 用于如果检测模块 11 确定当前业务类型对应的业务为需要进行认证的业务，或者确定服务质量对应的业务为需要进行认证的业务，或者确定用户设备执行认证的能力具有执行认证和密钥协商流程的能力，则触发认证和密钥协商流程。处理单元 52 用于如果检测模块 11 确定当前业务类型对应的业务不是需要进行认证的业务，或者确定服务质量对应的业务不是需要进行认证的业务，或者确定用户设备执行认证的能力不具有执行认证和密钥协商流程的能力，则继续使用当前的安全上下文，或者对当前业务不进行安全保护；或者中断当前业务的连接。

本实施例提供的认证处理装置可以按照上述实施例五提供的方法来工作。

上述装置实施例中不会一旦检测到 NAS 计数值即将环绕，就立即触发 EPS AKA 流程，减少了触发 EPS AKA 流程的次数，避免了因触发没有必要的 EPS AKA 流程导致的资源耗费，节省了资源。

图 13 为本发明实施例十三认证处理装置的结构示意图。如图 13 所示，本实施例具体包括执行模块 61 和处理模块 62。其中，执行模块 61 用于执行认证和密钥协商流程；处理模块 62 用于在执行模块 61 执行认证和密钥协商流程失败的情况下，根据本地信息及网络策略决定释放连接或者继续执行当前业务。

进一步的，本实施例还可以包括触发模块 63，该触发模块 63 用于在非接入层计数值接近最大值、运营商策略或用户设备进行网络间切换的触发条件下，触发执行模块 61 执行认证和密钥协商流程。

上述处理模块 62 可以进一步包括：第一判断单元 64、第一释放单元 65、第二判断单元 66、第二释放单元 67 和执行单元 68。其中，第一判断单元 64 用于在执行模块 61 执行认证和密钥协商流程失败的情况下，判断网络策略是否支持当前业务不认证；第一释放单元 65 用于在第一判断单元 64 判断为否的情况下，释放当前业务的连接；第二判断单元 66 用于在第一判断单元 64 判断为是的情况下，根据本地信息中的当前业务类型或服务质量判断当前业务是否为需要进行认证的业务，或者，根据本地信息中的用户设备执行认证的能力或用户识别模块类型判断用户设备是否具有执行认证和密钥协商流程的能力，或者，判断用户设备是否存在插入卡；第二释放单元 67 用于在第二判断单元 66 判断为是的情况下，释放当前业务的连接；执行单元 68 用于在第二判断单元 66 判断为否的情况下，继续执行当前业务。

本实施例提供的认证处理装置可以按照上述实施例七提供的方法来工作。

本实施例在认证失败，UE 请求的业务不是需要进行认证的业务或 UE 不具有执行 EPS AKA 流程的能力或用户设备未插入卡，且网络策略支持当前业务不认证的情况下仍然能继续执行当前业务，避免了当前业务执行中断的问题，节省了系统的资源。

本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤，而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上实施例仅用以说明本发明实施例的技术方案，

而非对其限制；尽管参照前述实施例对本发明实施例进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明实施例各实施例技术方案的精神和范围。

权利要求

1. 一种认证处理方法，其特征在于包括:

在对用户设备执行认证和密钥协商流程失败的情况下，无线通信网络侧设备确定网络策略是否支持当前业务不认证，

若所述网络策略支持当前业务不认证，且所述当前业务为不需要进行认证的业务，则继续执行所述当前业务；或者

若所述网络策略支持当前业务不认证，且所述用户设备不具有执行认证和密钥协商流程的能力，则继续执行所述当前业务；或者

若所述网络策略支持当前业务不认证，且所述用户设备无插入卡，则继续执行所述当前业务。

2. 根据权利要求 1 所述的方法，其特征在于，还包括:

若所述网络策略不支持当前业务不认证，则释放所述当前业务的连接。

3、根据权利要求 1 或 2 所述的方法，其特征在于，还包括:

若所述网络策略支持所述当前业务不认证，且当所述前业务为需要进行认证的业务，则释放所述当前业务的连接；或者

若所述网络策略支持所述当前业务不认证，且所述用户设备具有执行认证和密钥协商流程的能力，则释放所述当前业务的连接；或者

若所述网络策略支持所述当前业务不认证，且所述用户设备存在插入卡，则释放所述当前业务的连接。

4. 根据权利要求 1 至 3 任意一项所述的方法，其特征在于，还包括根据当前业务类型或服务质量确定当前业务是否为需要进行认证的业务。

5. 根据权利要求 1 至 3 任意一项所述的方法，其特征在于，还包括根据用户设备执行认证的能力或用户识别模块类型确定用户设备是否具有执行认证和密钥协商流程的能力。

6. 根据权利要求 2 至 5 任意一项所述的方法，其特征在于，所述释放所述当前业务的连接包括:

如果所述当前业务为非接入层信令连接中的单一业务，则释放非接入层信令连接；或者

如果非接入层信令连接中承载了多余一个业务，且根据所述当前业务类型确定所述多个当前业务均需要进行认证，则释放非接入层信令连接。

7. 根据权利要求 2 至 5 任意一项所述的方法，其特征在于，所述释放所述当前业务的连接包括:

如果非接入层信令连接中承载了多余一个业务，且根据所述当前业务类型确定所述当前业务既包括需要认证的业务又包括不需要认证的业务，则释放所述需要认证的业务的演进的分组系统承载，并且保持所述不需要认证的业务的演进的分组系统承载。

8. 根据权利要求 1 至 7 任意一项所述的方法，其特征在于，执行认证和密钥协商流程通过以下条件触发：非接入层计数值达到计数门限值，或运营商策略，或用户设备进行网络间切换。

9、根据权利要求 1 至 7 任意一项所述的方法，其特征在于，所述当前业务包括紧急呼叫业务，和/或公共报警业务。

10、如权利要求 9 所述的方法，其特征在于，

所述紧急呼叫业务为不需要进行认证的紧急呼叫业务或需要进行认证的紧急呼叫业务;

所述公共报警业务为不需要进行认证的公共报警业务或需要进行认证的公共报警业务。

11、如权利要求 1 至 10 任意一项所述的方法，其特征在于，所述无线通信网络侧设备包括移动管理实体。

12. 一种认证处理装置，其特征在于包括:

执行模块，用于执行认证和密钥协商流程;

处理模块，位于无线通信网络侧设备内，包括:

第一判断单元，用于在对用户设备执行认证和密钥协商流程失败的情

况下，确定网络策略是否支持当前业务不认证，

第二判断单元，用于在所述网络策略支持当前业务不认证的情况下，确定所述当前业务是否是需要进行认证的业务，或者所述用户设备是否具有执行认证和密钥协商流程的能力，或者所述用户设备是否具有插入卡；

执行单元，用于在所述第二判断单元判断为所述当前业务是不需要进行认证的业务，或者所述用户设备不具有执行认证和密钥协商流程的能力，或者所述用户设备不具有插入卡的情况下况下，继续执行所述当前业务。

13. 根据权利要求 12 所述的装置，其特征在于，所述处理模块还包括：

第一释放单元，用于在所述第一判断单元判断为不支持当前业务不认证的情况下，释放所述当前业务的连接。

14、根据权利要求 12 或 13 所述的装置，其特征在于，所述处理模块还包括：

第二释放单元，用于在所述第二判断单元判断为所述当前业务是需要进行认证的业务，或者所述用户设备具有执行认证和密钥协商流程的能力，或者所述用户设备具有插入卡的情况下，释放所述当前业务的连接。

15. 根据权利要求 12 至 14 任意一项所述的装置，其特征在于，所述第二判断单元用于在所述网络策略支持当前业务不认证的情况下，根据当前业务类型或服务质量确定当前业务是否为需要进行认证的业务，或者所述用户设备是否具有执行认证和密钥协商流程的能力，或者所述用户设备是否具有插入卡。

16. 根据权利要求 12 至 14 任意一项所述的装置，其特征在于，所述第二判断单元用于在所述网络策略支持当前业务不认证的情况下，确定当前业务是否为需要进行认证的业务，或者根据用户设备执行认证的能力或用户识别模块类型确定用户设备是否具有执行认证和密钥协商流程的能力，或者所述用户设备是否具有插入卡。

17. 根据权利要求 13 至 16 任意一项所述的装置，其特征在于，所述

第一释放单元或第二释放单元用于:

如果所述当前业务为非接入层信令连接中的单一业务，则释放非接入层信令连接；或者

如果非接入层信令连接中承载了多余一个业务，且根据所述当前业务类型确定所述多个当前业务均需要进行认证，则释放非接入层信令连接。

18. 根据权利要求 13 至 16 任意一项所述的装置，其特征在于，所述第一释放单元或第二释放单元用于:

如果非接入层信令连接中承载了多余一个业务，且根据所述当前业务类型确定所述当前业务既包括需要认证的业务又包括不需要认证的业务，则释放所述需要认证的业务的演进的分组系统承载，并且保持所述不需要认证的业务的演进的分组系统承载。

19. 根据权利要求 12 至 18 任意一项所述的装置，其特征在于，还包括:

触发模块，用于在非接入层计数值达到计数门限值、或运营商策略，或用户设备进行网络间切换的触发条件下，触发所述执行模块执行所述认证和密钥协商流程。

20、根据权利要求 12 至 18 任意一项所述的装置，其特征在于，所述当前业务包括紧急呼叫业务，和/或公共报警业务。

21、如权利要求 20 所述的装置，其特征在于，

所述紧急呼叫业务为不需要进行认证的紧急呼叫业务或需要进行认证的紧急呼叫业务;

所述公共报警业务为不需要进行认证的公共报警业务或需要进行认证的公共报警业务。

22、如权利要求 12 至 21 任意一项所述的装置，其特征在于，所述无线通信网络侧设备包括移动管理实体。

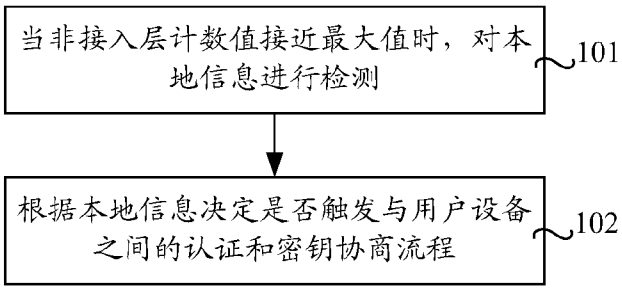
当非接入层计数值接近最大值时，对本地信息进行检测
101
根据本地信息决定是否触发与用户设备之间的认证和密钥协商流程
102

图 1

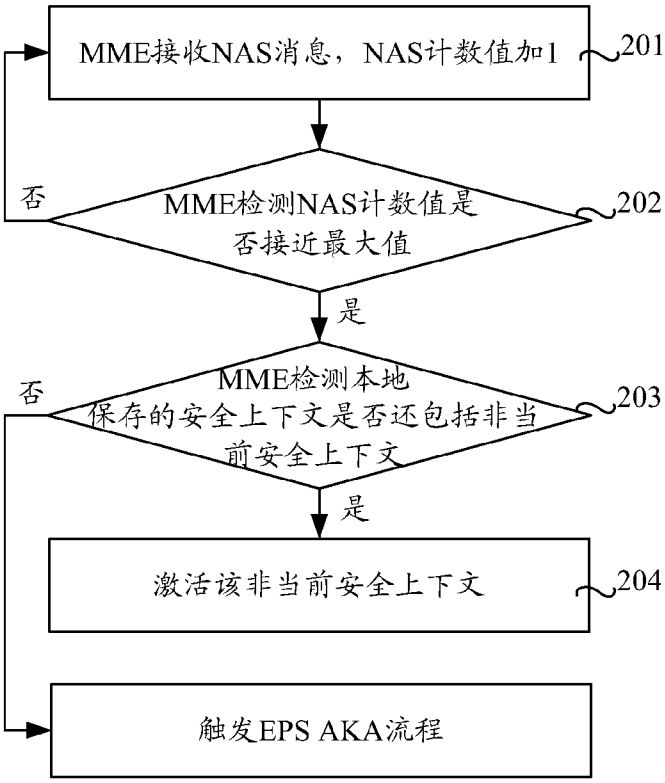
MME接收NAS消息，NAS计数值加1
201
否
MME检测NAS计数值是否接近最大值
202
是
否
MME检测本地保存的安全上下文是否还包括非当前安全上下文
203
是
激活该非当前安全上下文
204
触发EPS AKA流程

图 2

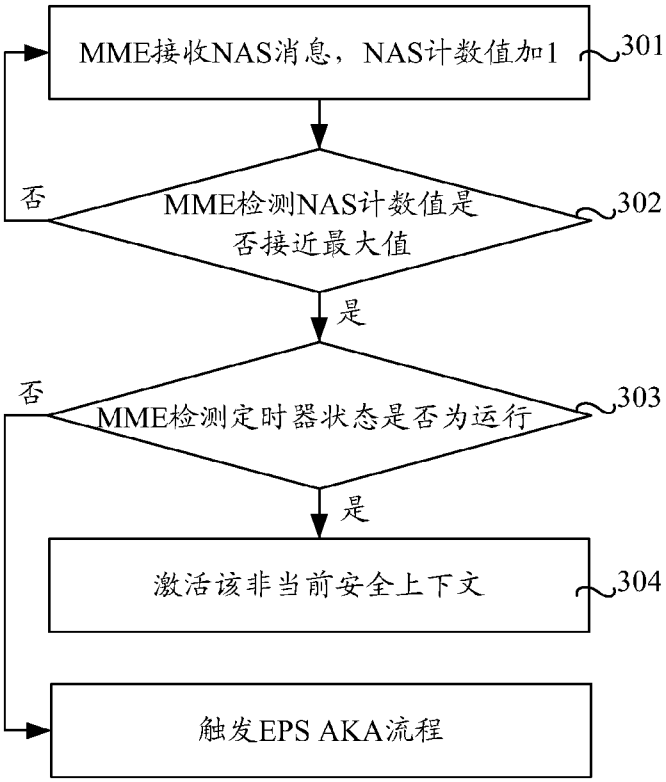
MME接收NAS消息，NAS计数值加1
301
MME检测NAS计数值是否接近最大值
302
否
是
MME检测定时器状态是否为运行
303
否
是
激活该非当前安全上下文
304
触发EPS AKA流程

图 3

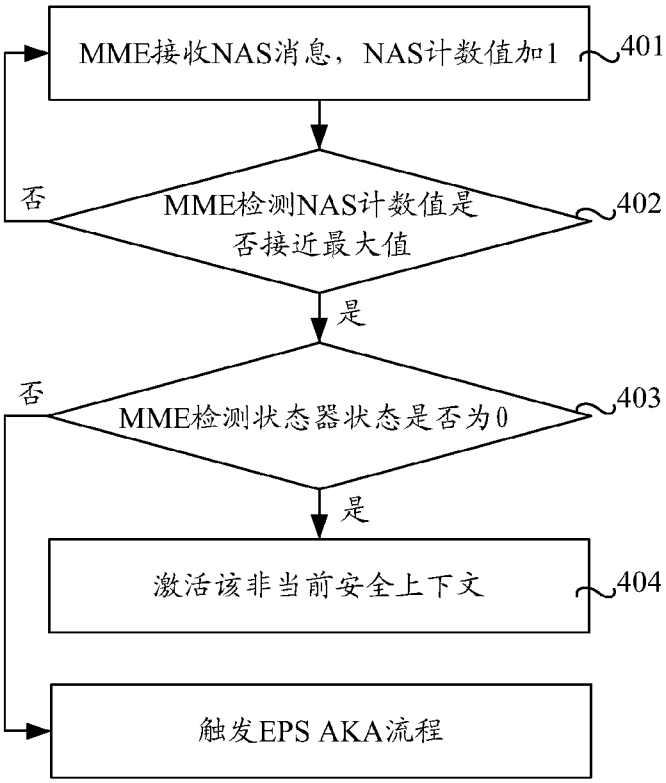
MME接收NAS消息，NAS计数值加1
401
MME检测NAS计数值是否接近最大值
402
否
是
MME检测状态器状态是否为0
403
否
是
激活该非当前安全上下文
404
触发EPS AKA流程

图 4

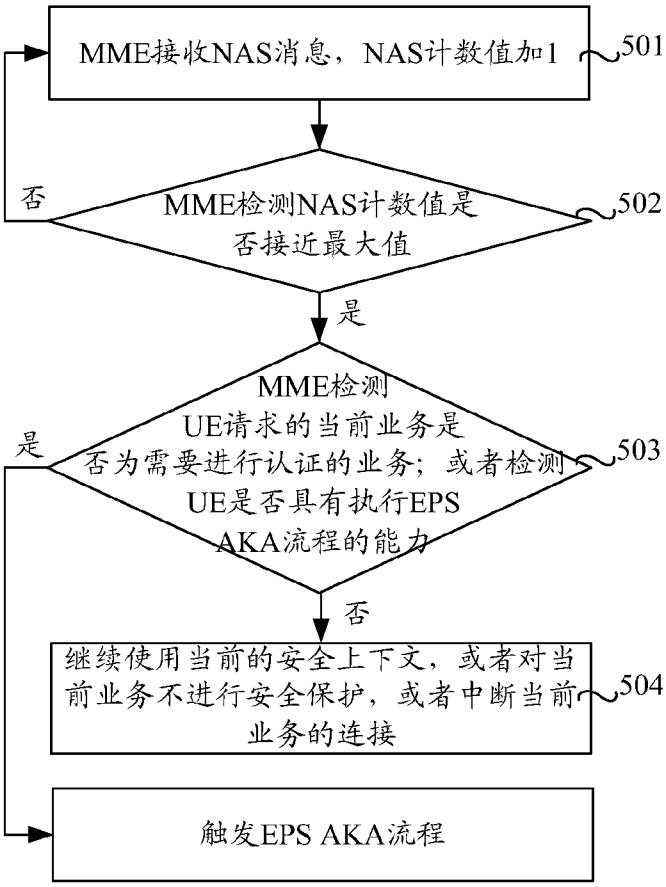
MME接收NAS消息，NAS计数值加1
501
MME检测NAS计数值是否接近最大值
502
否
是
MME检测UE请求的当前业务是否为需要进行认证的业务；或者检测UE是否具有执行EPS AKA流程的能力
503
是
否
继续使用当前的安全上下文，或者对当前业务不进行安全保护，或者中断当前业务的连接
504
触发EPS AKA流程

图 5

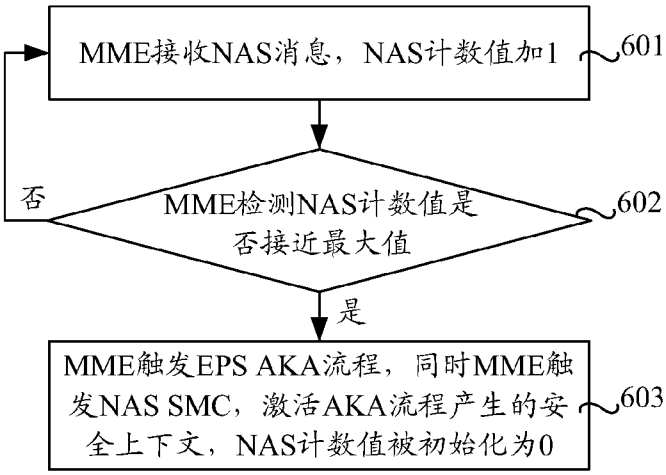
MME接收NAS消息，NAS计数值加1
601
MME检测NAS计数值是否接近最大值
602
否
是
MME触发EPS AKA流程，同时MME触发NAS SMC，激活AKA流程产生的安全上下文，NAS计数值被初始化为0
603

图 6

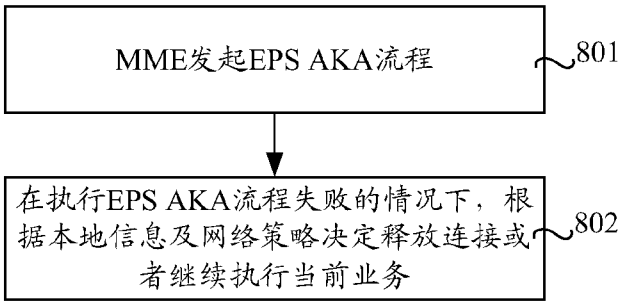
MME发起EPS AKA流程
801
在执行EPS AKA流程失败的情况下，根据本地信息及网络策略决定释放连接或者继续执行当前业务
802

图 7

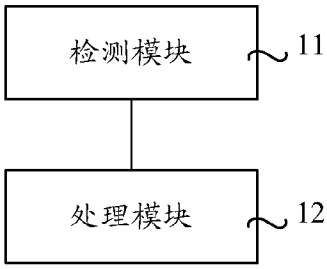
检测模块
11
处理模块
12

图 8

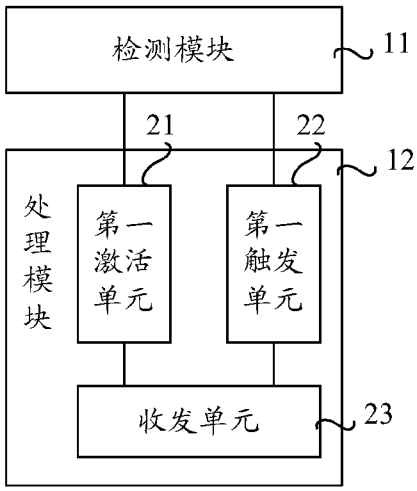
检测模块
11
21
22
12
处理模块
第一激活单元
第一触发单元
收发单元
23

图 9

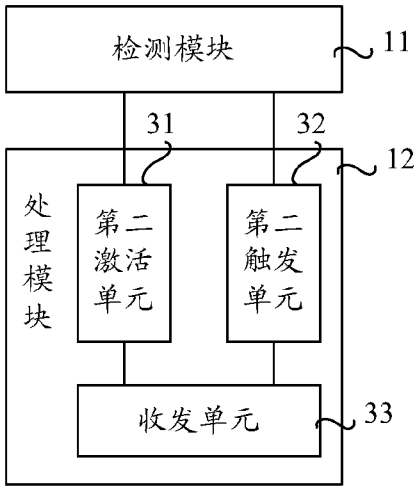
检测模块
11
31
32
12
处理模块
第二激活单元
第二触发单元
收发单元
33

图 10

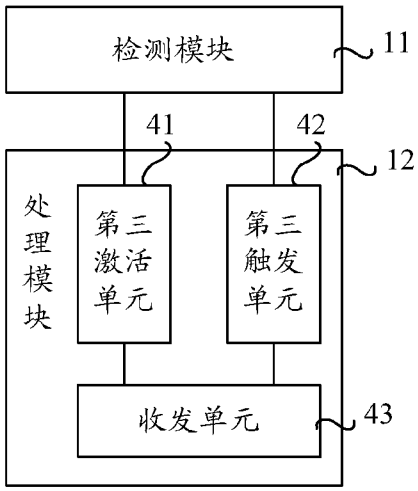
检测模块
11
41
42
12
处理模块
第三激活单元
第三触发单元
收发单元
43

图 11

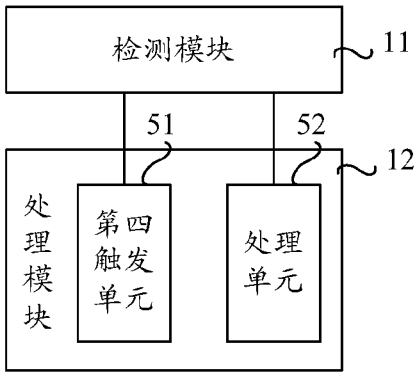
检测模块
11
51
52
12
处理模块
第四触发单元
处理单元

图 12

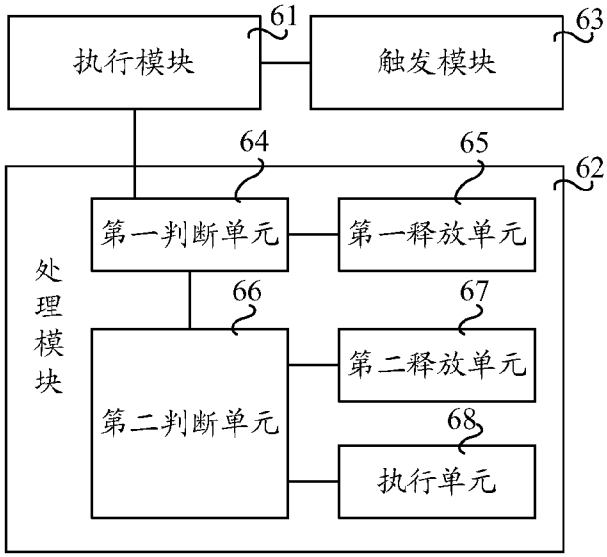
61
63
执行模块
触发模块
64
65
62
处理模块
第一判断单元
第一释放单元
66
67
第二判断单元
第二释放单元
68
执行单元

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/077085

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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)

IPC: H04W 12/-; H04L 9/32; H04L29/06; H04Q 7/-

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)

CNPAT, CNKI, WPI, EPODOC: authentication, verification, key, agreement, AKA, service, fail+, error, card, SIM, USIM, MME, emergence, inserted

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2009103728A1 (PATEL) 23 April 2009 (23.04.2009) the whole document	1-22
A	CN101237334A (HUAWEI TECHNOLOGIES CO LTD) 06 Aug. 2008(06.08.2008) the whole document	1-22
A	CN101272251A (HUAWEI TECHNOLOGIES CO LTD) 24 Sep. 2008(24.09.2008) the whole document	1-22
A	CN101119381A (ZTE COMMUNICATION CO LTD) 06 Feb. 2008(06.02.2008) the whole document	1-22

☐ 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
01 Dec. 2010(01.12.2010)	**23 Dec. 2010 (23.12.2010)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer Su, Yulei Telephone No. (86-10)62411515

Form PCT/ISA /210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/077085

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2009103728A1	23.04.2009	WO2009048574A2	16.04.2009
		WO2009048574A3	28.05.2009
		AU2008311306A1	16.04.2009
		MXPA10003677A	30.04.2010
		KR20100068279A	22.06.2010
		EP2210437A2	28.07.2010
CN101237334A	06.08.2008	WO2008095433A1	14.08.2008
CN101272251A	24.09.2008	WO2008113299A1	25.09.2008
		US2010011220A1	14.01.2010
CN101119381A	06.02.2008	None	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2010/077085

H04W 12/04 (2009.01) i
H04L 29/06 (2006.01) i
H04L 9/32 (2009.01) i

国际检索报告

国际申请号
PCT/CN2010/077085

A. 主题的分类

见附加页

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)

IPC: H04W 12/-; H04L 9/32; H04L29/06; H04Q7/-

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）)

CNPAT, CNKI: 认证, 密钥, 协商, 业务, 服务, 失败, 出错, 卡, SIM, USIM, MME,紧急,插入

WPI, EPODOC: authentication, verification, key, agreement, AKA, service, fail+, error, card, SIM, USIM, MME, emergence, inserted

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
A	US2009103728A1 (PATEL) 23.4 月 2009 (23.04.2009) 全文	1-22
A	CN101237334A (华为技术有限公司) 06.8 月 2008(06.08.2008) 全文	1-22
A	CN101272251A (华为技术有限公司) 24.9 月 2008(24.09.2008) 全文	1-22
A	CN101119381A (中兴通讯股份有限公司) 06.2 月 2008(06.02.2008) 全文	1-22

☐ 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
01.12 月 2010(01.12.2010)	**23.12 月 2010 (23.12.2010)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 苏玉磊 电话号码：(86-10) **62411515**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/077085

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2009103728A1	23.04.2009	WO2009048574A2	16.04.2009
		WO2009048574A3	28.05.2009
		AU2008311306A1	16.04.2009
		MXPA10003677A	30.04.2010
		KR20100068279A	22.06.2010
		EP2210437A2	28.07.2010
CN101237334A	06.08.2008	WO2008095433A1	14.08.2008
CN101272251A	24.09.2008	WO2008113299A1	25.09.2008
		US2010011220A1	14.01.2010
CN101119381A	06.02.2008	无	

H04W 12/04 (2009.01) i

H04L 29/06 (2006.01) i

H04L 9/32 (2009.01) i