

# (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  
2017 年 11 月 30 日 (30.11.2017)



(10) 国际公布号  
**WO 2017/201804 A1**

(51) 国际专利分类号:  
**H04W 12/06** (2009.01)

中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(21) 国际申请号: PCT/CN2016/087398

(22) 国际申请日: 2016 年 6 月 28 日 (28.06.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
201610370605.9 2016年5月27日 (27.05.2016) CN

(71) 申请人: 宇龙计算机通信科技(深圳)有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(72) 发明人: 钟焰涛(ZHONG, Yantao); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 傅文治(FU, Wenzhi); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 刘是泉(LIU, Shixiao);

(74) 代理人: 北京友联知识产权代理事务所(普通合伙) (YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路8号科技财富中心A座506室尚志峰, Beijing 100192 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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,

(54) Title: METHOD FOR ANTI-THEFT VERIFICATION OF TERMINAL, TERMINAL, AND SERVER

(54) 发明名称: 终端防盗验证方法、终端和服务

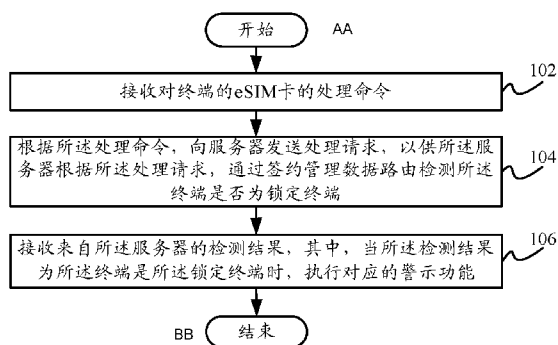


图 1

102 Receive a processing command for an eSIM card of a terminal

104 Send a processing request to a server according to the processing command so that the server detects whether the terminal is a locked terminal by means of subscription management data routing according to the processing request

106 Receive the detection result from the server, wherein a corresponding warning function is performed when the detection result is that the terminal is the locked terminal

AA Start

BB End

(57) Abstract: The present invention provides a method for anti-theft verification of a terminal, a terminal, and a server. The method for anti-theft verification of a terminal comprises: receiving a processing command for an eSIM card of a terminal; sending a processing request to a server according to the processing command so that the server detects whether the terminal is a locked terminal by means of subscription management data routing according to the processing request; and receiving the detection result from the server, wherein a corresponding warning function is performed when the detection result is that the terminal is the locked terminal. By means of the technical solution of the present invention, on the basis of the characteristic that an embedded universal integrated circuit card (eUICC) in an eSIM card terminal has a unique identification code, when the terminal receives a processing command for the eSIM card, the server can effectively determine whether the terminal has been reported lost or locked, so that the server can obtain various information from the terminal to determine a real-time status of the terminal, thereby facilitating recovery of the terminal and protecting the benefits of users.

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:** 本发明提出了一种终端防盗验证方法、一种终端和一种服务器, 其中, 终端防盗验证方法包括: 接收对终端的eSIM卡的处理命令; 根据所述处理命令, 向服务器发送处理请求, 以供所述服务器根据所述处理请求, 通过签约管理数据路由检测所述终端是否为锁定终端; 接收来自所述服务器的检测结果, 其中, 当所述检测结果为所述终端是所述锁定终端时, 执行对应的警示功能。通过本发明的技术方案, 利用eSIM卡终端中eUICC卡(嵌入式通用集成电路卡)具有唯一标识码的特性, 可以在终端接收到对eSIM卡的处理命令时通过服务器有效判断其是否已被挂失或锁定, 从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况, 便于寻回终端, 保障了用户的利益。

## 终端防盗验证方法、终端和服务

### 技术领域

5 本发明涉及终端技术领域，具体而言，涉及一种终端防盗验证方法、一种终端和一种服务器。

### 背景技术

10 目前，相关技术中提供了 eSIM 卡（嵌入式用户身份识别卡）以取代原有的 SIM 卡（用户身份识别卡），eSIM 卡本身为终端的一部分，在出厂时或用户经运营商进行变更时进行配置，避免了原有 SIM 卡手动拆卸不便的缺陷。

然而，如果 eSIM 卡的终端被盗时，由于被盗终端的 eSIM 卡很可能被重新配置，则对于被盗终端的信息安全保护及寻回非常不利。

15 因此，如何处理 eSIM 卡终端的防盗问题，成为目前亟待解决的技术问题。

### 发明内容

20 本发明正是基于上述问题，提出了一种新的技术方案，可以有效处理 eSIM 卡终端的防盗问题，增强 eSIM 卡终端的安全性，有效保障用户的利益。

有鉴于此，本发明的一方面提出了一种终端防盗验证方法，包括：接收对终端的 eSIM 卡的处理命令；根据所述处理命令，向服务器发送处理请求，以供所述服务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，以验证本终端是否为不具有对 eSIM 卡

的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

另外，在确定该终端为锁定终端时，对应的警示功能包括：禁止对 eSIM 卡的处理、上传终端的实时地理位置至服务器或其他关联终端、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面图图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功能，可以由终端出厂时自带，也可以由用户手动进行设置和更改，从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况，以便寻回终端，保护用户的财产安全。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，所述对终端的 eSIM 卡的处理命令包括：激活所述 eSIM 卡的用户配置文件的处理请求；或为所述 eSIM 卡下载新的用户配置文件的处理请求。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理请求时，即可开启防盗验证模式，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，所述处理命令中具有所述终端的

eUICC 卡的唯一标识码，以供所述服务器检测所述签约管理数据路由的数据库中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，这样，就可以在终端接收到对 eSIM 卡的处理命令时，通过服务器根据其 eUICC 卡的唯一标识码有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

本发明的另一方面提出了一种终端，包括：处理请求接收单元，接收对终端的 eSIM 卡的处理命令；发送单元，根据所述处理命令，向服务器发送处理请求，以供所述服务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；检测结果接收单元，接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，以验证本终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

另外，在确定该终端为锁定终端时，对应的警示功能包括：禁止对 eSIM 卡的处理、上传终端的实时地理位置至服务器或其他关联终端、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面部图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功

能，可以由终端出厂时自带，也可以由用户手动进行设置和更改，从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况，以便寻回终端，保护用户的财产安全。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，所述处理请求接收单元具体用于：接收激活所述 eSIM 卡的用户配置文件的处理请求；或接收为所述 eSIM 卡下载新的用户配置文件的处理请求。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理请求时，即可开启防盗验证模式，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，所述处理命令中具有所述终端的 eUICC 卡的唯一标识码，以供所述服务器检测所述签约管理数据路由的数据库中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，这样，就可以在终端接收到对 eSIM 卡的处理命令时，通过服务器根据其 eUICC 卡的唯一标识码有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

本发明的再一方面提出了一种终端防盗验证方法，包括：接收来自终端的对所述终端的 eSIM 卡的处理请求；根据所述处理请求，通过签约管

理数据路由检测所述终端是否为锁定终端；当检测到所述终端为所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，由服务器来验证该终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时通过服务器有效判断其是否已被挂失或锁定，从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，所述处理请求包括：激活所述 eSIM 卡的用户配置文件的处理请求，或为所述 eSIM 卡下载新的用户配置文件的处理请求，以及所述处理请求中具有所述终端的 eUICC 卡的唯一标识码。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理命令时，即可开启防盗验证模式，向服务器发送对应的处理请求，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，所述通过签约管理数据路由检测所述终端是否为锁定终端，包括：根据所述处理请求，检测所述签约管理数据路

由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，就可以在终端接收到激活 eSIM 卡的用户配置文件的命令时，如果服务器根据其 eUICC 卡的唯一标识码有效判断已被挂失或锁定，即可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

在上述任一技术方案中，优选地，当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，所述通过签约管理数据路由检测所述终端是否为锁定终端，包括：对签约管理数据准备装置与签约管理数据路由进行相互认证；在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；根据所述 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，SIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，在终端接收到为 eSIM 卡下载新的用户配置文件的命令时，可以经 SM-DP（签约管理数据准备装置）向 SM-SR（签约管理数据路由）进行 eUICC 信息集检索，以检测 SM-SR 的数据库中是否存储了该终端的 eUICC 卡的唯一标识码，如果已存储，说明该终端已被挂失或锁定，服务器可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的

利益。

在上述任一技术方案中，优选地，还包括：在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测  
5 测到所述数据库中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

在该技术方案中，还可以对签约管理数据路由的数据库中的 eUICC 卡的唯一标识码进行删除，以对终端进行解锁，方便用户的使用。

本发明的还一方面提出了一种服务器，包括：处理请求接收单元，接收  
10 收来自终端的对所述终端的 eSIM 卡的处理请求；检测单元，根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；警示单元，当检测到所述终端为所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令  
15 时，可以向服务器发送处理请求，由服务器来验证该终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

20 其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时通过服务器有效判断其是否已被挂失或锁定，从而使服务器能够从终端中获取  
25 多样化的信息来确定该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，所述处理请求接收单元具体用于：接收激活所述 eSIM 卡的用户配置文件的处理请求，或接收为所述 eSIM 卡下载新的用户配置文件的处理请求；以及所述处理请求中具有所述终端的

eUICC 卡的唯一标识码。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理命令时，即可开启防盗验证模式，向服务器发送对应的处理请求，以便服务器验证本终端是否 5 是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，所述检测单元包括：第一检索单元，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，根据所述处理请求，检测所述签约管理数据路由的数据库中是否存储有所 10 述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务 15 器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，就可以在终端接收到激活 eSIM 卡的用户配置文件的命令时，如果服务器根据其 eUICC 卡的唯一标识码有效判断已被挂失或锁定，即可从终端中获取多样化的信息来确定该终端 20 的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

在上述任一技术方案中，优选地，所述检测单元包括：认证单元，当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，对签约管理数据准备装置与签约管理数据路由进行相互认证；检索请求发送单 25 元，在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；第二检索单元，根据所述 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，SIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，在终端接收到为 eSIM 卡下载新的用户配置文件的命令时，可以经 SM-DP（签约管理数据准备装置）向 SM-SR（签约管理数据路由）进行 eUICC 信息集检索，以检测 SM-SR 的数据库中是否存储了该终端的 eUICC 卡的唯一标识码，如果已存储，说明该终端已被挂失或锁定，服务器可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

在上述任一技术方案中，优选地，还包括：解锁定命令接收单元，在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；标识码删除单元，根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测到所述数据库中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

在该技术方案中，还可以对签约管理数据路由的数据库中的 eUICC 卡的唯一标识码进行删除，以对终端进行解锁，方便用户的使用。

通过以上技术方案，利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时通过服务器有效判断其是否已被挂失或锁定，从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

## 附图说明

图 1 示出了根据本发明的一个实施例的终端防盗验证方法的流程图；

图 2 示出了根据本发明的一个实施例的终端的框图；

图 3 示出了根据本发明的另一个实施例的终端防盗验证方法的流程图；

图 4 示出了根据本发明的一个实施例的服务器的框图；

图 5 示出了根据本发明的一个实施例的 eSIM 卡远程配置管理系统的架构图；

图 6 示出了根据本发明的一个实施例的进行终端挂失的流程图；

5 图 7 示出了根据本发明的一个实施例的触发防盗功能的流程图；

图 8 示出了根据本发明的另一个实施例的触发防盗功能的流程图；

图 9 示出了根据本发明的一个实施例的为终端进行解挂失的流程图。

### 具体实施方式

10 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的  
15 的保护范围并不受下面公开的具体实施例的限制。

图 1 示出了根据本发明的一个实施例的终端防盗验证方法的流程图。

如图 1 所示，根据本发明的一个实施例的终端防盗验证方法，包括：

步骤 102，接收对终端的 eSIM 卡的处理命令；

步骤 104，根据所述处理命令，向服务器发送处理请求，以供所述服  
20 务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

步骤 106，接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失  
25 或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，以验证本终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

30 其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可

以是指定的专用于终端防盗的其他类型的服务器。

另外，在确定该终端为锁定终端时，对应的警示功能包括：禁止对 eSIM 卡的处理、上传终端的实时地理位置至服务器或其他关联终端、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面  
5 图图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功能，可以由终端出厂时自带，也可以由用户手动进行设置和更改，从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该  
10 终端的实时状况，以便寻回终端，保护用户的财产安全。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的  
15 利益。

在上述技术方案中，优选地，所述对终端的 eSIM 卡的处理命令包括：激活所述 eSIM 卡的用户配置文件的处理请求；或为所述 eSIM 卡下载新的用户配置文件的处理请求。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的  
20 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理请求时，即可开启防盗验证模式，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，所述处理命令中具有所述终端的 eUICC 卡的唯一标识码，以供所述服务器检测所述签约管理数据路由的数据库  
25 中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电

路卡)，eUICC 卡具有唯一标识码也就是全球唯一编号 EID，这样，就可以在终端接收到对 eSIM 卡的处理命令时，通过服务器根据其 eUICC 卡的唯一标识码有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

图 2 示出了根据本发明的一个实施例的终端的框图。

如图 2 所示，根据本发明的一个实施例的终端 200，包括：处理请求接收单元 202、发送单元 204 和检测结果接收单元 206。

其中，处理请求接收单元 202 用于接收对终端的 eSIM 卡的处理命令；发送单元 204 用于根据所述处理命令，向服务器发送处理请求，以供所述服务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；检测结果接收单元 206 用于接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，以验证本终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

另外，在确定该终端为锁定终端时，对应的警示功能包括：禁止对 eSIM 卡的处理、上传终端的实时地理位置至服务器或其他关联终端、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面部图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功能，可以由终端出厂时自带，也可以由用户手动进行设置和更改，从而便

于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况，以便寻回终端，保护用户的财产安全。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，处理请求接收单元 202 具体用于：接收激活所述 eSIM 卡的用户配置文件的处理请求；或接收为所述 eSIM 卡下载新的用户配置文件的处理请求。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理请求时，即可开启防盗验证模式，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，所述处理命令中具有所述终端的 eUICC 卡的唯一标识码，以供所述服务器检测所述签约管理数据路由的数据库中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，这样，就可以在终端接收到对 eSIM 卡的处理命令时，通过服务器根据其 eUICC 卡的唯一标识码有效判断其是否已被挂失或锁定，从而使服务器能够通过多样化的途径获取该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

图 3 示出了根据本发明的另一个实施例的终端防盗验证方法的流程图。

如图 3 所示，根据本发明的另一个实施例的终端防盗验证方法，包

括：

步骤 302，接收来自终端的对所述终端的 eSIM 卡的处理请求；

步骤 304，根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

5 步骤 306，当检测到所述终端为所述锁定终端时，执行对应的警示功能。

在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，由服务器来验证该终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变更处理。

15 其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时通过服务器有效判断其是否已被挂失或锁定，从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，所述处理请求包括：激活所述 eSIM 卡的用户配置文件的处理请求，或为所述 eSIM 卡下载新的用户配置文件的处理请求，以及所述处理请求中具有所述终端的 eUICC 卡的唯一标识码。

25 在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理命令时，即可开启防盗验证模式，向服务器发送对应的处理请求，以便服务器验证本终端是

否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，步骤 304 具体包括：根据所述处理请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡  
5 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务  
10 器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，就可以在终端接收到激活 eSIM 卡的用户配置文件的命令时，如果服务器根据其 eUICC 卡的唯一标识码有效判断已被挂失或锁定，即可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利  
15 益。

在上述任一技术方案中，优选地，当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，步骤 304 包括：对签约管理数据准备装置与签约管理数据路由进行相互认证；在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；根据所述  
20 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，SIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务  
25 器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，在终端接收到为 eSIM 卡下载新的用户配置文件的命令时，可以经 SM-DP（签约管理数据准备装置）向 SM-SR（签约管理数据路由）进行 eUICC 信息集检索，以检测 SM-SR 的

数据库中是否存储了该终端的 eUICC 卡的唯一标识码，如果已存储，说明该终端已被挂失或锁定，服务器可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

5       在上述任一技术方案中，优选地，还包括：在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测到所述数据库中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

10       在该技术方案中，还可以对签约管理数据路由的数据库中的 eUICC 卡的唯一标识码进行删除，以对终端进行解锁，方便用户的使用。

图 4 示出了根据本发明的一个实施例的服务器的框图。

如图 4 所示，根据本发明的一个实施例的服务器 400，包括：处理请求接收单元 402、检测单元 404 和警示单元 406。

15       其中，处理请求接收单元 402 用于接收来自终端的对所述终端的 eSIM 卡的处理请求；检测单元 404 用于根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；警示单元 406 用于当检测到所述终端为所述锁定终端时，执行对应的警示功能。

20       在该技术方案中，锁定终端是指终端的合法用户在运营商处进行挂失或权限限制等操作后的终端，当普通终端接收到对 eSIM 卡的处理命令时，可以向服务器发送处理请求，由服务器来验证该终端是否为不具有对 eSIM 卡的处理权限的锁定终端，如果服务器验证结果为是，则说明本终端不具有对 eSIM 卡的处理权限，禁止其进行处理，并示警，只有在服务器验证结果为否时，才允许对终端的 eSIM 卡进行用户配置文件更改等变  
25       更处理。

其中，服务器可以是与终端的 eSIM 卡相关联的运营商服务器，也可以是指定的专用于终端防盗的其他类型的服务器。

该技术方案利用 eSIM 卡终端中 eUICC 卡（嵌入式通用集成电路卡）具有唯一标识码的特性，可以在终端接收到对 eSIM 卡的处理命令时通过

服务器有效判断其是否已被挂失或锁定，从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况，增强终端的安全性，便于寻回终端，有效保障了用户的利益。

在上述技术方案中，优选地，处理请求接收单元 402 具体用于：接收  
5 激活所述 eSIM 卡的用户配置文件的处理请求，或接收为所述 eSIM 卡下载新的用户配置文件的处理请求；以及所述处理请求中具有所述终端的 eUICC 卡的唯一标识码。

在该技术方案中，终端丢失或被盗后，非法用户一般都会对终端的 eSIM 卡进行激活用户配置文件或下载新的用户配置文件的操作，因此，  
10 为了有效防盗，保护用户的财产安全，每当终端接收到激活 eSIM 卡的用户配置文件或为 eSIM 卡下载新的用户配置文件的处理命令时，即可开启防盗验证模式，向服务器发送对应的处理请求，以便服务器验证本终端是否为锁定终端，从而便于进一步判断终端接收到的处理请求是否合法。

在上述任一技术方案中，优选地，检测单元 404 包括：第一检索单元  
15 4042，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，根据所述处理请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，eSIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，就可以在终端接收到激活 eSIM 卡的用户配置文件的命令时，如果服务器根据其 eUICC 卡的唯一标识码  
25 有效判断已被挂失或锁定，即可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

在上述任一技术方案中，优选地，检测单元 404 包括：认证单元 4044、检索请求发送单元 4046 和第二检索单元 4048。

其中，认证单元 4044 用于当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，对签约管理数据准备装置与签约管理数据路由进行相互认证；检索请求发送单元 4046 用于在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；第二检索单元 4048 用于根据所述 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

在该技术方案中，SIM 卡终端中具有 eUICC 卡（嵌入式通用集成电路卡），eUICC 卡具有唯一标识码也就是全球唯一编号 EID，在终端的有效用户发现终端遗失或被盗时，可以在通过身份验证后，向运营商等服务器请求锁定该终端，服务器即可将该终端的 eUICC 卡的唯一标识码记录在签约管理数据路由的数据库中。这样，在终端接收到为 eSIM 卡下载新的用户配置文件的命令时，可以经 SM-DP（签约管理数据准备装置）向 SM-SR（签约管理数据路由）进行 eUICC 信息集检索，以检测 SM-SR 的数据库中是否存储了该终端的 eUICC 卡的唯一标识码，如果已存储，说明该终端已被挂失或锁定，服务器可从终端中获取多样化的信息来确定该终端的实时状况，便于寻回终端，增强终端的安全性，有效保障了用户的利益。

在上述任一技术方案中，优选地，还包括：解锁定命令接收单元 408，在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；标识码删除单元 410，根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测到所述数据库中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

在该技术方案中，还可以对签约管理数据路由的数据库中的 eUICC 卡的唯一标识码进行删除，以对终端进行解锁，方便用户的使用。

图 5 示出了根据本发明的一个实施例的 eSIM 卡远程配置管理系统的架构图。

如图 5 所示，eSIM 卡远程配置管理系统是根据 eSIM 技术的标准规程

构建的。每个 eUICC 卡刚出厂的时候就会在 SM-SR（签约管理数据路由）处注册，从而 eUICC 的完整生命周期相关数据都在 SM-SR 数据库中有保存；另一方面，每次终端下载一个 eSIM 信息时，都需要 SM-SR 判断对应的终端是否有下载 eSIM 的能力。

5       本方案充分利用 SM-SR 和 SM-DP（签约管理数据准备装置）对 eUICC 的管理能力，同时利用了 eUICC 存在唯一标识码的特点，当用户挂失终端后，通过在 SM-SR 数据库中注明该 eUICC 对应终端为被盗终端，可以实现锁定设备，使该终端无法使用 eSIM 功能，当有非法用户尝试使用该被盗终端下载新的 eSIM 时，系统自动报警，并定位终端位置。

10       图 6 示出了根据本发明的一个实施例的进行终端挂失的流程图。

如图 6 所示，根据本发明的一个实施例的进行终端挂失的流程包括：

步骤 6.1，用户向 MNO（运营商）发送挂失请求，请求挂失某终端，此处，用户可以是生物个体，直接请求运营商进行挂失服务，也可以指其他经身份验证后的终端，向运营商服务器发送挂失请求。

15       步骤 6.2，MNO 向 SM-DP（签约管理数据准备装置）进行挂失处理。

步骤 6.3，SM-DP 与 SM-SR（签约管理数据路由）进行相互认证。

步骤 6.4，认证完成后，SM-SR 将挂失信息记入数据库中，具体来说，是将该终端的 eUICC 卡的唯一标识码打上挂失的标记。

20       步骤 6.5.1，SM-SR 向 SM-DP 反馈挂失确认。

步骤 6.5.2，SM-SR 向 MNO 反馈挂失确认。其中，步骤 6.5.1 和步骤 6.5.2 可以同时执行，也可以先执行其中任一个步骤，再执行另一个。

步骤 6.6，MNO 向用户反馈挂失确认。

SM-SR 触发的内容不仅限于上传位置信息，还可以是其他警示功能，比如，禁止对 eSIM 卡的处理、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面图图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功能，可以由终端出厂时自带，也可以

25

由用户手动进行设置和更改，从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况，以便寻回终端，保护用户的财产安全。

通过将终端挂失，可以在该终端的 eUICC 卡的唯一标识码打上挂失的标记，以便服务器接收到该终端的 eSIM 卡处理命令时，通过验证其对应的 eUICC 卡的唯一标识码为挂失状态来确定其为挂失终端，从而便于进一步禁止其 eSIM 卡相关的操作并获取该终端的实时位置信息等内容，有利于终端的寻回。

图 7 示出了根据本发明的一个实施例的触发防盗功能的流程图。

如图 7 所示，根据本发明的一个实施例，触发防盗功能的过程如下：

步骤 7.1，MNO 在接收到终端的 Profile（用户配置文件）下载命令后，向 SM-SR 发送 Profile 激活请求，其中，Profile 为 eSIM 卡的用户配置文件。

步骤 7.2，查找数据库发现激活请求中的 EID（eUICC 卡的唯一标识码）属于被盗终端，这里的数据库指的是 SM-SR 的数据库。

步骤 7.3.1，由 SM-SR 向 MNO 发送终端被盗提示。

步骤 7.3.2，SM-SR 触发终端的定位功能。步骤 7.3.1 与步骤 7.3.2 可以同时执行，也可以先执行其中任一个步骤，再执行另一个。

步骤 7.4，终端向 SM-SR 上报位置信息。

其中，上报位置信息可以是上传终端的实时地理位置至服务器或其他关联终端，但 SM-SR 触发的内容不仅限于上传位置信息，还可以是其他警示功能，比如，禁止对 eSIM 卡的处理、拨打预定警示电话（如报警电话），还可以使用前置摄像头拍摄操作者的面图图像或虹膜图像，如果终端具有指纹识别功能，还可以实时采集操作者的指纹，并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用，也可以结合使用，具体选择何种警示功能，可以由终端出厂时自带，也可以由用户手动进行设置和更改，从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况，以便寻回终端，保护用户的财产安全。

图 8 示出了根据本发明的另一个实施例的触发防盗功能的流程图。

如图 8 所示, 根据本发明的另一个实施例, 触发防盗功能的过程包括:

步骤 8.1, MNO 在接收到终端的 Profile (用户配置文件) 下载命令后, 向 SM-DP 发送 Profile 下载请求, 其中, Profile 为 eSIM 卡的用户配置文件。

步骤 8.2, SM-SR 与 SM-DP 相互认证。

步骤 8.3, 认证通过后, SM-DP 向 SM-SR 发送 EIS (eUICC 信息集) 请求, 请求进行检索终端的 eUICC 卡的唯一标识码。

10 步骤 8.4, 检索 EIS, 发现该终端为被盗终端, 即在检索到 SM-SR 的数据库中具有该终端的 eUICC 卡的唯一标识码时, 说明该终端为被盗终端。

步骤 8.5.1, SM-SR 向 SM-DP 发送终端被盗提示。

15 步骤 8.5.2, SM-SR 向 MNO 发送终端被盗提示。步骤 8.5.1 与步骤 8.5.2 可以同时执行, 也可以先执行其中任一个步骤, 再执行另一个。

步骤 8.6, SM-SR 触发终端的定位功能。

步骤 8.7, 终端向 SM-SR 上报位置信息。

20 同样, 上报位置信息可以是上传终端的实时地理位置至服务器或其他关联终端, 但 SM-SR 触发的内容不仅限于上传位置信息, 还可以是其他警示功能, 比如, 禁止对 eSIM 卡的处理、拨打预定警示电话 (如报警电话), 还可以使用前置摄像头拍摄操作者的面图图像或虹膜图像, 如果终端具有指纹识别功能, 还可以实时采集操作者的指纹, 并将上述一种或多种生物信息上传至服务器或其他关联终端。以上多种警示功能可以单独使用, 也可以结合使用, 具体选择何种警示功能, 可以由终端出厂时自带, 25 也可以由用户手动进行设置和更改, 从而便于在终端的合法用户挂失该终端后使服务器能够通过多样化的途径获取该终端的实时状况, 以便寻回终端, 保护用户的财产安全。

图 9 示出了根据本发明的一个实施例的为终端进行解挂失的流程图。

如图 9 所示, 为终端进行解挂失的步骤如下:

步骤 9.1, 用户向 MNO 发送解挂失请求。此处, 用户可以是生物个体, 直接请求运营商进行解挂失服务, 也可以指其他经身份验证后的终端, 向运营商服务器发送解挂失请求。

步骤 9.2, MNO 调用 SM-DP 进行解挂失处理。

5 步骤 9.3, SM-SR 与 SM-DP 相互认证。

步骤 9.4, 认证通过后, SM-SR 在数据库中消除对应的挂失数据, 即消除对该终端的 eUICC 卡的唯一标识码的挂失标记。

步骤 9.5.1, SM-SR 向 SM-DP 发送解挂失确认。

步骤 9.5.2, SM-SR 向 MNO 发送解挂失确认。

10 步骤 9.6, MNO 向用户发送解挂失确认, 这里的用户可以是其他经身份验证后的终端, 也可以是已寻回的解挂失终端。

以上结合附图详细说明了本发明的技术方案, 通过本发明的技术方案, 利用 eSIM 卡终端中 eUICC 卡 (嵌入式通用集成电路卡) 具有唯一标识码的特性, 可以在终端接收到对 eSIM 卡的处理命令时通过服务器有效  
15 判断其是否已被挂失或锁定, 从而使服务器能够从终端中获取多样化的信息来确定该终端的实时状况, 增强终端的安全性, 便于寻回终端, 有效保障了用户的利益。

以上所述仅为本发明的优选实施例而已, 并不用于限制本发明, 对于本领域的技术人员来说, 本发明可以有各种更改和变化。凡在本发明的精神  
20 和原则之内, 所作的任何修改、等同替换、改进等, 均应包含在本发明的保护范围之内。

## 权利要求书

1. 一种终端防盗验证方法，其特征在于，包括：

接收对终端的 eSIM 卡的处理命令；

5 根据所述处理命令，向服务器发送处理请求，以供所述服务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

2. 根据权利要求 1 所述的终端防盗验证方法，其特征在于，所述对  
10 终端的 eSIM 卡的处理命令包括：

激活所述 eSIM 卡的用户配置文件的处理请求；或

为所述 eSIM 卡下载新的用户配置文件的处理请求。

3. 根据权利要求 1 或 2 所述的终端防盗验证方法，其特征在于，所述处理命令中具有所述终端的 eUICC 卡的唯一标识码，以供所述服务器  
15 检测所述签约管理数据路由的数据库中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

4. 一种终端，其特征在于，包括：

处理请求接收单元，接收对终端的 eSIM 卡的处理命令；

20 发送单元，根据所述处理命令，向服务器发送处理请求，以供所述服务器根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

检测结果接收单元，接收来自所述服务器的检测结果，其中，当所述检测结果为所述终端是所述锁定终端时，执行对应的警示功能。

25 5. 根据权利要求 4 所述的终端，其特征在于，所述处理请求接收单元具体用于：

接收激活所述 eSIM 卡的用户配置文件的处理请求；或

接收为所述 eSIM 卡下载新的用户配置文件的处理请求。

6. 根据权利要求 4 或 5 所述的终端，其特征在于，所述处理命令中

具有所述终端的 eUICC 卡的唯一标识码，以供所述服务器检测所述签约管理数据路由的数据库中是否存储有所述唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

7. 一种终端防盗验证方法，其特征在于，包括：

5 接收来自终端的对所述终端的 eSIM 卡的处理请求；

根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

当检测到所述终端为所述锁定终端时，执行对应的警示功能。

10 8. 根据权利要求 7 所述的终端防盗验证方法，其特征在于，所述处理请求包括：激活所述 eSIM 卡的用户配置文件的处理请求，或为所述 eSIM 卡下载新的用户配置文件的处理请求，以及所述处理请求中具有所述终端的 eUICC 卡的唯一标识码。

15 9. 根据权利要求 8 所述的终端防盗验证方法，其特征在于，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，所述通过签约管理数据路由检测所述终端是否为锁定终端，包括：

根据所述处理请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

20 10. 根据权利要求 8 或 9 所述的终端防盗验证方法，其特征在于，当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，所述通过签约管理数据路由检测所述终端是否为锁定终端，包括：

对签约管理数据准备装置与签约管理数据路由进行相互认证；

在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；

25 根据所述 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

11. 根据权利要求 8 或 9 所述的终端防盗验证方法，其特征在于，还包括：

在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；

根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测到所述数据库中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

5 12. 一种服务器，其特征在于，包括：

处理请求接收单元，接收来自终端的对所述终端的 eSIM 卡的处理请求；

检测单元，根据所述处理请求，通过签约管理数据路由检测所述终端是否为锁定终端；

10 警示单元，当检测到所述终端为所述锁定终端时，执行对应的警示功能。

13. 根据权利要求 12 所述的服务器，其特征在于，所述处理请求接收单元具体用于：

15 接收激活所述 eSIM 卡的用户配置文件的处理请求，或接收为所述 eSIM 卡下载新的用户配置文件的处理请求；以及

所述处理请求中具有所述终端的 eUICC 卡的唯一标识码。

14. 根据权利要求 13 所述的服务器，其特征在于，所述检测单元包括：

20 第一检索单元，当所述处理请求为激活所述 eSIM 卡的用户配置文件的处理请求时，根据所述处理请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

15. 根据权利要求 13 或 14 所述的服务器，其特征在于，所述检测单元包括：

25 认证单元，当所述处理请求为所述 eSIM 卡下载新的用户配置文件的处理请求时，对签约管理数据准备装置与签约管理数据路由进行相互认证；

检索请求发送单元，在认证通过后，通过签约管理数据准备装置向签约管理数据路由发送 eUICC 信息集检索请求；

第二检索单元，根据所述 eUICC 信息集检索请求，检测所述签约管理数据路由的数据库中是否存储有所述终端的 eUICC 卡的唯一标识码，其中，当所述数据库中存储有所述唯一标识码时，确定所述终端是所述锁定终端。

5           16. 根据权利要求 13 或 14 所述的服务器，其特征在于，还包括：

解锁定命令接收单元，在所述终端为所述锁定终端时，接收对所述终端的解锁定命令；

          标识码删除单元，根据所述解锁定命令，在所述签约管理数据路由的数据库中删除所述终端对应的所述唯一标识码，以供在检测到所述数据库  
10   中不具有所述唯一标识码时，确定所述终端不是所述锁定终端。

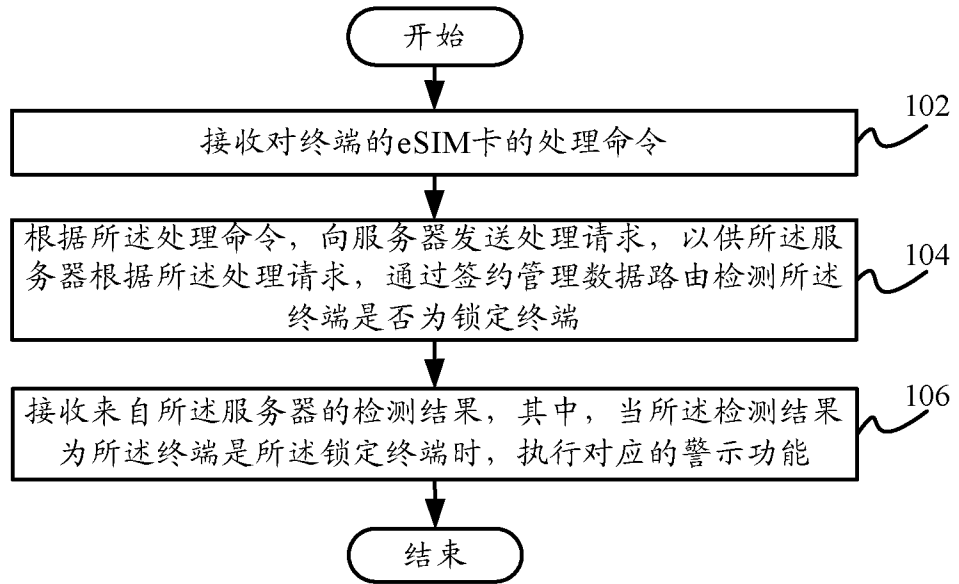


图 1

5



图 2

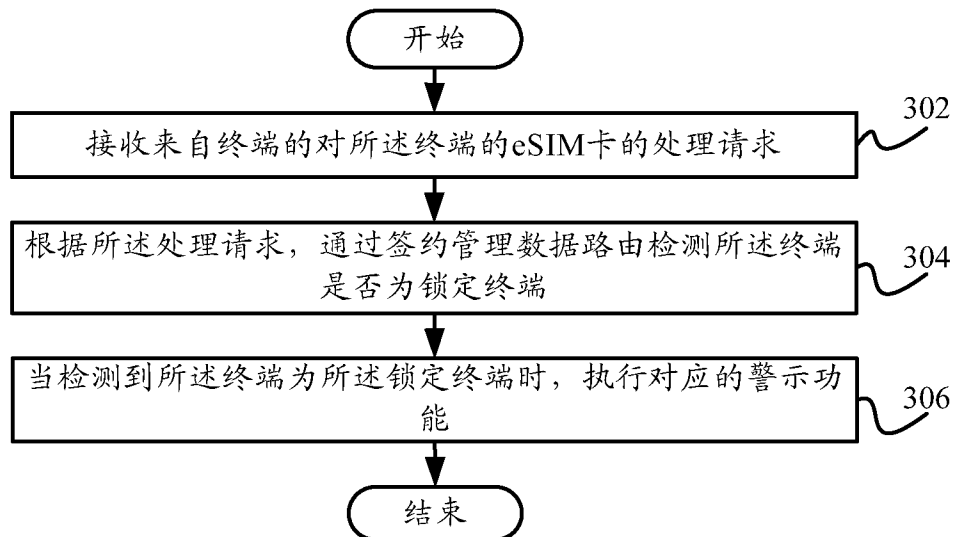


图 3

10



图 4

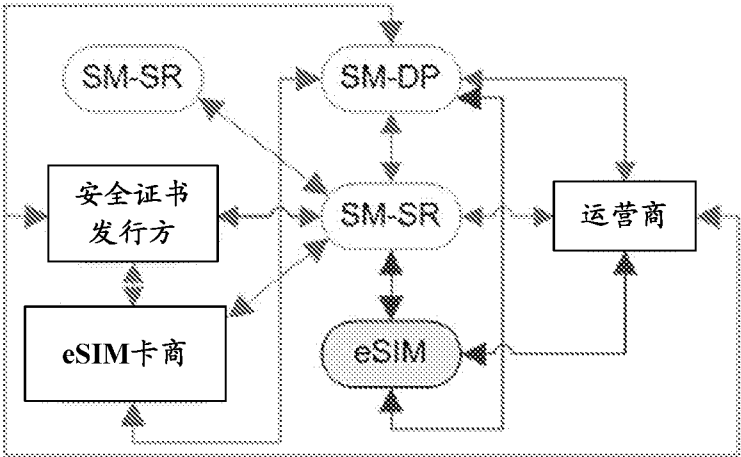


图 5

5

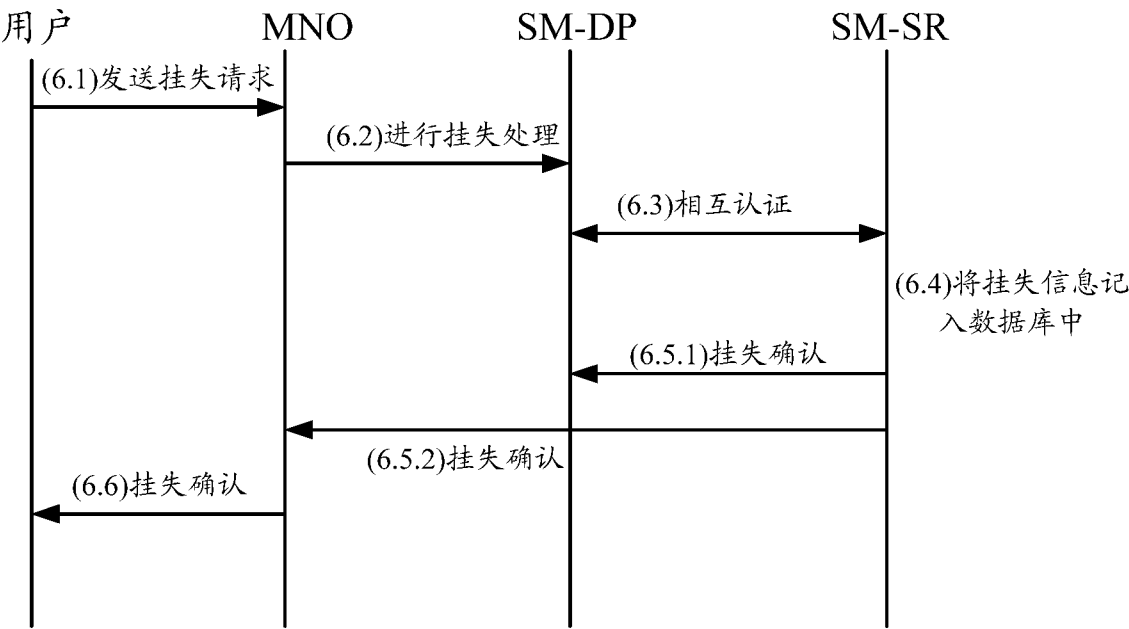


图 6

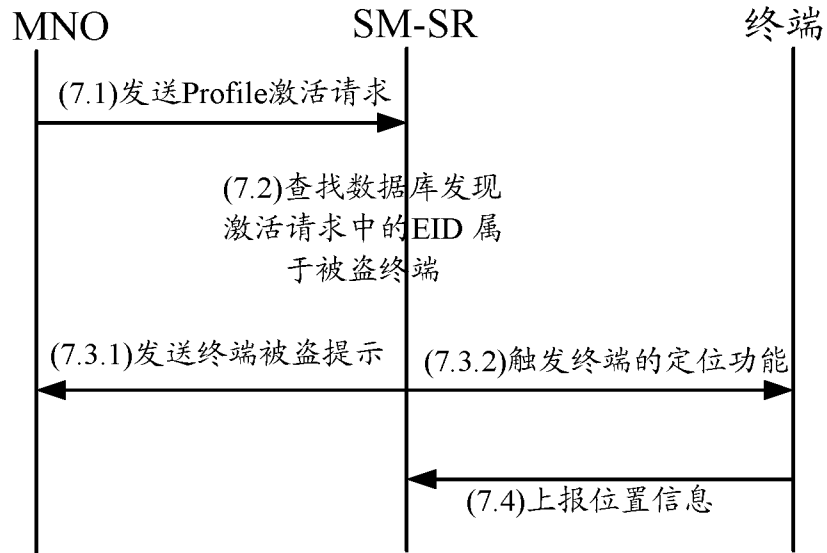


图 7

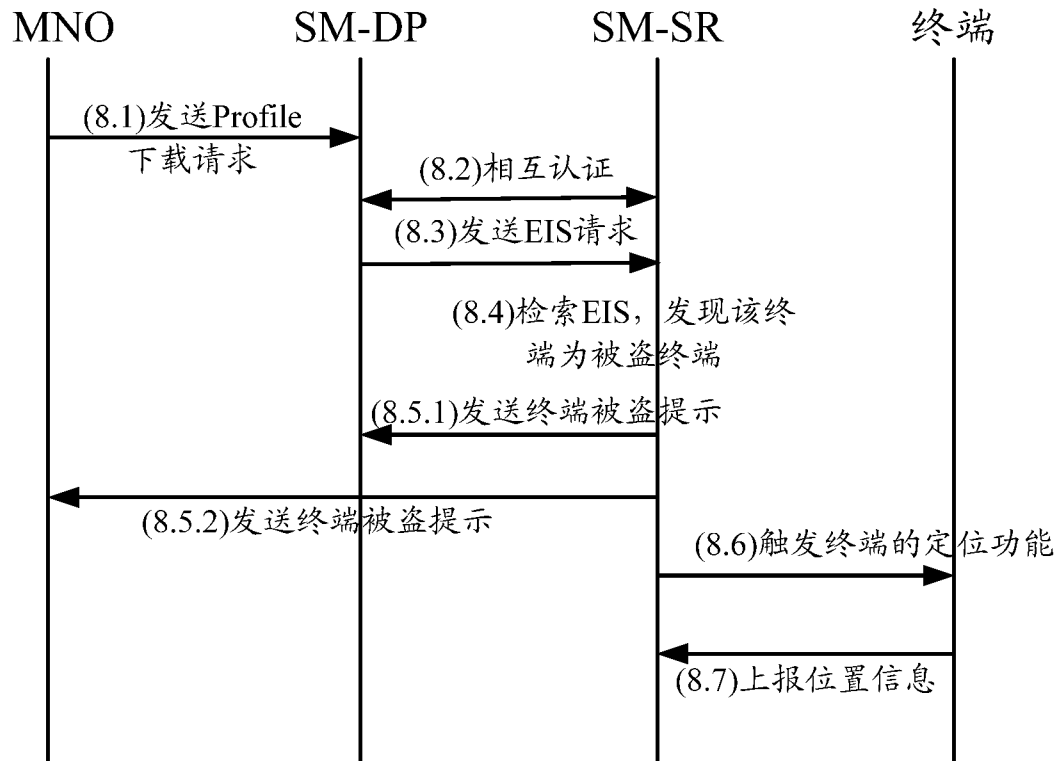


图 8

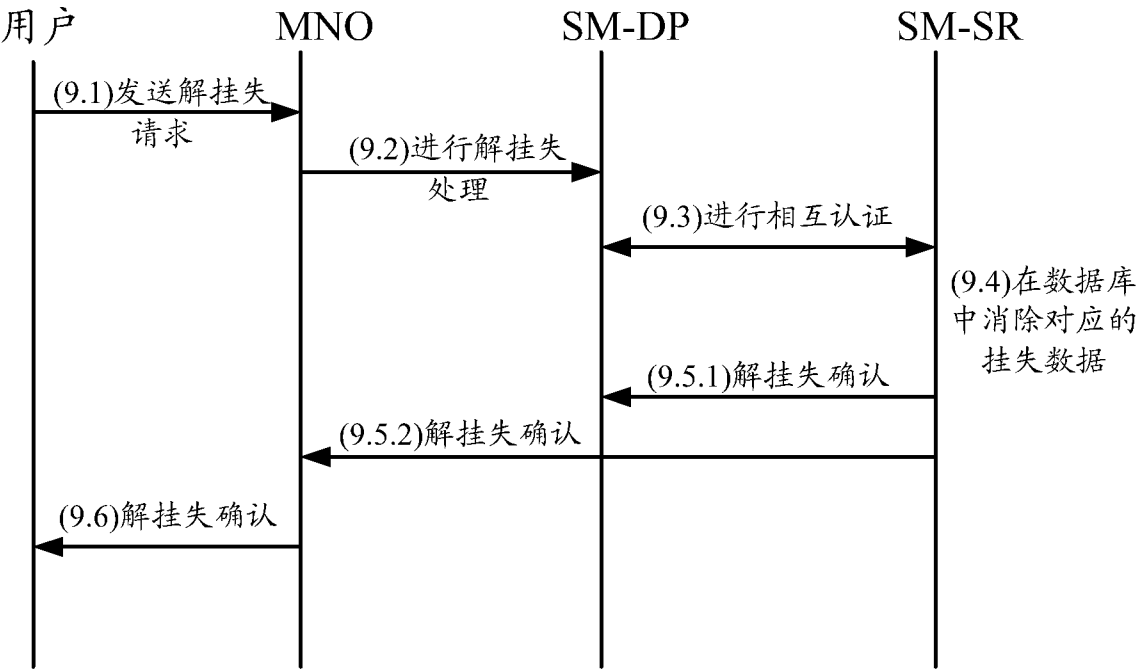


图 9

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2016/087398****A. CLASSIFICATION OF SUBJECT MATTER**

H04W 12/06 (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; H04Q; H04M

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: subscriber identity module, embedded, report the loss, SIM, eSIM, steal, stolen, lost, report, change, alter, replace, download

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                          | Relevant to claim No. |
|-----------|-------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 101835143 A (ZTE CORP.), 15 September 2010 (15.09.2010), description, paragraphs 0025-0081, and figure 2 | 1-16                  |
| A         | CN 103731821 A (HUAWEI DEVICE CO., LTD.), 16 April 2014 (16.04.2014), the whole document                    | 1-16                  |
| A         | WO 2012154600 A1 (APPLE INC.), 15 November 2012 (15.11.2012), the whole document                            | 1-16                  |

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

|                                                                                                                                                                         |                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Special categories of cited documents:                                                                                                                                | “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                                              |
| “A” document defining the general state of the art which is not considered to be of particular relevance                                                                | “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                                                                     |
| “E” earlier application or patent but published on or after the international filing date                                                                               | “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 |
| “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) | “&” document member of the same patent family                                                                                                                                                                                                    |
| “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                                                                  |                                                                                                                                                                                                                                                  |

Date of the actual completion of the international search  
30 December 2016 (30.12.2016)Date of mailing of the international search report  
**14 February 2017 (14.02.2017)**Name and mailing address of the ISA/CN:  
State Intellectual Property Office of the P. R. China  
No. 6, Xitucheng Road, Jimenqiao  
Haidian District, Beijing 100088, China  
Facsimile No.: (86-10) 62019451Authorized officer  
**HE, Xijia**  
Telephone No.: (86-10) **62413281**

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

International application No.

**PCT/CN2016/087398**

| Patent Documents referred<br>in the Report | Publication Date  | Patent Family    | Publication Date |
|--------------------------------------------|-------------------|------------------|------------------|
| CN 101835143 A                             | 15 September 2010 | WO 2011137605 A1 | 10 November 2011 |
|                                            |                   | EP 2509375 A1    | 10 October 2012  |
|                                            |                   | US 2012276924 A1 | 01 November 2012 |
| CN 103731821 A                             | 16 April 2014     | EP 2836052 A1    | 11 February 2015 |
|                                            |                   | US 2015067351 A1 | 05 March 2015    |
|                                            |                   | WO 2014056302 A1 | 17 April 2014    |
| WO 2012154600 A1                           | 15 November 2012  | US 2013122864 A1 | 16 May 2013      |

| <b>A. 主题的分类</b><br>H04W 12/06 (2009.01) i<br><br>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>B. 检索领域</b><br>检索的最低限度文献 (标明分类系统和分类号)<br>H04W; H04Q; H04M<br><br>包含在检索领域中的除最低限度文献以外的检索文献<br><br>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))<br>CNPAT, CNKI, WPI, EPDOC: 用户识别模块, 嵌入式, 盗, 窃, 偷, 丢, 挂失, 报失, 更换, 下载, SIM, eSIM, steal, stolen, lost, report, change, alter, replace, download                                                                                                                                                                                                                     |                                                                                |                                              |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| <b>C. 相关文件</b> <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101835143 A (中兴通讯股份有限公司) 2010年 9月 15日 (2010 - 09 - 15)<br/>说明书第0025-0081段、图2</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 103731821 A (华为终端有限公司) 2014年 4月 16日 (2014 - 04 - 16)<br/>全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>WO 2012154600 A1 (APPLE INC.) 2012年 11月 15日 (2012 - 11 - 15)<br/>全文</td> <td>1-16</td> </tr> </tbody> </table> |                                                                                |                                              | 类 型* | 引用文件, 必要时, 指明相关段落 | 相关的权利要求 | X | CN 101835143 A (中兴通讯股份有限公司) 2010年 9月 15日 (2010 - 09 - 15)<br>说明书第0025-0081段、图2 | 1-16 | A | CN 103731821 A (华为终端有限公司) 2014年 4月 16日 (2014 - 04 - 16)<br>全文 | 1-16 | A | WO 2012154600 A1 (APPLE INC.) 2012年 11月 15日 (2012 - 11 - 15)<br>全文 | 1-16 |
| 类 型*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 引用文件, 必要时, 指明相关段落                                                              | 相关的权利要求                                      |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | CN 101835143 A (中兴通讯股份有限公司) 2010年 9月 15日 (2010 - 09 - 15)<br>说明书第0025-0081段、图2 | 1-16                                         |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | CN 103731821 A (华为终端有限公司) 2014年 4月 16日 (2014 - 04 - 16)<br>全文                  | 1-16                                         |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | WO 2012154600 A1 (APPLE INC.) 2012年 11月 15日 (2012 - 11 - 15)<br>全文             | 1-16                                         |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| <input type="checkbox"/> 其余文件在C栏的续页中列出。 <input checked="" type="checkbox"/> 见同族专利附件。                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                |                                              |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| * 引用文件的具体类型:<br>“A” 认为不特别相关的表示了现有技术一般状态的文件<br>“E” 在国际申请日的当天或之后公布的在先申请或专利<br>“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)<br>“O” 涉及口头公开、使用、展览或其他方式公开的文件<br>“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<br>“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<br>“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<br>“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<br>“&” 同族专利的文件                                                                                                           |                                                                                |                                              |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| 国际检索实际完成的日期<br><br>2016年 12月 30日                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                | 国际检索报告邮寄日期<br><br>2017年 2月 14日               |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |
| ISA/CN的名称和邮寄地址<br><br>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                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                | 受权官员<br><br>贺希佳<br><br>电话号码 (86-10) 62413281 |      |                   |         |   |                                                                                |      |   |                                                               |      |   |                                                                    |      |

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2016/087398

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |            |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|------------|----|----------------|
| CN          | 101835143  | A  | 2010年 9月 15日   | WO   | 2011137605 | A1 | 2011年 11月 10日  |
|             |            |    |                | EP   | 2509375    | A1 | 2012年 10月 10日  |
|             |            |    |                | US   | 2012276924 | A1 | 2012年 11月 1日   |
| CN          | 103731821  | A  | 2014年 4月 16日   | EP   | 2836052    | A1 | 2015年 2月 11日   |
|             |            |    |                | US   | 2015067351 | A1 | 2015年 3月 5日    |
|             |            |    |                | WO   | 2014056302 | A1 | 2014年 4月 17日   |
| WO          | 2012154600 | A1 | 2012年 11月 15日  | US   | 2013122864 | A1 | 2013年 5月 16日   |