

(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
2018 年 4 月 5 日 (05.04.2018)



(10) 国际公布号
WO 2018/058725 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01)

(21) 国际申请号: PCT/CN2016/103877

(22) 国际申请日: 2016 年 10 月 29 日 (29.10.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610866774.1 2016 年 9 月 29 日 (29.09.2016) 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: 郭辰 (GUO, Chen); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。 徐宇杰 (XU, Yujie); 中国广东

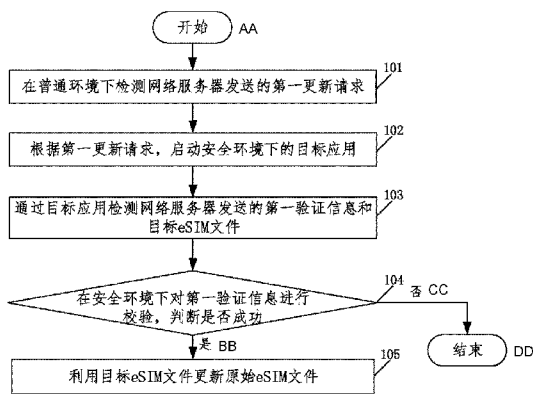
省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (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, JP, KE, KG, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) Title: METHOD FOR PREVENTING ESIM FILE FROM BEING TAMPERED WITH, AND MOBILE TERMINAL

(54) 发明名称: 一种防止eSIM文件被篡改的方法及移动终端



[Fig. 1]

- 101 DETECT, IN A COMMON ENVIRONMENT, A FIRST UPDATE REQUEST SENT BY A NETWORK SERVER
102 START, ACCORDING TO THE FIRST UPDATE REQUEST, A TARGET APPLICATION IN A SECURE ENVIRONMENT
103 DETECT, BY MEANS OF THE TARGET APPLICATION, FIRST VERIFICATION INFORMATION AND A TARGET ESIM FILE SENT BY THE NETWORK SERVER
104 CHECK, IN A SECURE ENVIRONMENT, THE FIRST VERIFICATION INFORMATION, AND DETERMINE WHETHER IT IS SUCCESSFUL
105 UPDATE AN ORIGINAL ESIM FILE USING THE TARGET ESIM FILE
AA START
BB YES
CC NO
DD END

(57) Abstract: Disclosed in the embodiments of the invention are a method for preventing an eSIM file from being tampered with, and a mobile terminal. The method comprises: a mobile terminal detecting, in a common environment, a first update request sent by a network server, the first update request being used for requesting to update an original embedded subscriber identification module (eSIM) file in the mobile terminal; according to the first update request, the mobile terminal starting a target application in a secure environment; the mobile terminal detecting, by means of the target application, first verification information and a target eSIM file sent by the network server, the first verification information being used for verifying the identity of the network server; the mobile terminal checking, in a secure environment, the first verification information; when the check by the mobile terminal of the first verification information in the secure environment is successful, the mobile terminal updating the original eSIM file using the target eSIM file. The implementation of the embodiments of the invention is able to efficiently prevent the eSIM file from being maliciously tampered with, improving the security of the mobile terminal.

(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: 本发明实施例公开了一种防止eSIM文件被篡改的方法及移动终端, 该方法包括: 移动终端在普通环境下检测网络服务器发送的第一更新请求, 第一更新请求用于请求更新移动终端中的原始嵌入式用户识别模块eSIM文件; 移动终端根据第一更新请求, 启动安全环境下的目标应用; 移动终端通过目标应用检测网络服务器发送的第一验证信息和目标eSIM文件, 其中, 第一验证信息为用于对网络服务器的身份进行验证的信息; 移动终端在安全环境下对第一验证信息进行校验; 当移动终端在安全环境下对第一验证信息校验成功时, 移动终端利用目标eSIM文件更新原始eSIM文件。实施本发明实施例, 能够有效防止eSIM文件被恶意篡改, 提高移动终端的安全性。

说明书

一种防止eSIM文件被篡改的方法及移动终端

- [1] 本申请要求于2016年9月29日提交中国专利局，申请号为201610866774.1、发明名称为“一种防止eSIM文件被篡改的方法及移动终端”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

- [2] 本发明涉及通信技术领域，尤其涉及一种防止eSIM文件被篡改的方法及移动终端。

背景技术

- [3] 随着移动通信的快速发展，已经逐渐出现将eSIM（embedded Subscriber Identification Module，嵌入式用户识别模块）取代传统的SIM卡应用于终端中。与传统的SIM卡相比，eSIM不是作为独立的可移除零部件加入终端中，而是直接嵌入到终端芯片中，eSIM的出现使得用户在无需购买新终端的提前下，即可以自由选择、随时切换运营商。
- [4] 由于eSIM通过终端与运营商建立连接，因此在实际应用中，可能会由于黑客的攻击，使得eSIM文件恶意地被篡改，因此用户的个人数据存在安全隐患，使得终端的安全性低下。

对发明的公开

发明内容

- [5] 本发明实施例公开了一种防止eSIM文件被篡改的方法及移动终端，能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。
- [6] 本发明实施例第一方面公开了一种防止eSIM文件被篡改的方法，移动终端包括普通环境和安全环境，其中，所述安全环境为所述移动终端运行在安全域TZ下的环境，所述方法包括：
- [7] 所述移动终端在所述普通环境下检测网络服务器发送的第一更新请求，所述第一更新请求用于请求更新所述移动终端中的原始嵌入式用户识别模块eSIM文件；

- [8] 所述移动终端根据所述第一更新请求，启动所述安全环境下的目标应用；
- [9] 所述移动终端通过所述目标应用检测所述网络服务器发送的第一验证信息和目标eSIM文件，其中，所述第一验证信息为用于对所述网络服务器的身份进行验证的信息；
- [10] 所述移动终端在所述安全环境下对所述第一验证信息进行校验；
- [11] 当所述移动终端在所述安全环境下对所述第一验证信息校验成功时，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。
- [12] 作为一种可选的实施方式，所述移动终端在所述安全环境下对所述第一验证信息校验成功之后，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件之前，所述方法还包括：
- [13] 所述移动终端在所述安全环境下获取第二验证信息，所述第二验证信息为用于对所述目标应用的安全性进行验证的信息；
- [14] 所述移动终端在所述安全环境下对所述第二验证信息进行校验；
- [15] 其中，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件，包括：
- [16] 若所述移动终端对所述第二验证信息校验成功，则所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。
- [17] 作为一种可选的实施方式，所述移动终端在所述安全环境下对所述第一验证信息校验成功之后，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件之前，所述方法还包括：
- [18] 所述移动终端输出第一验证指令，所述第一验证指令用于指示用户输入第一生物特征信息；
- [19] 所述移动终端判断用户输入的第一生物特征信息是否校验通过；
- [20] 其中，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件，包括：
- [21] 若所述移动终端判断用户输入的所述第一生物特征信息校验通过，则所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。
- [22] 作为一种可选的实施方式，所述方法还包括：
- [23] 所述移动终端将所述安全环境下的所述目标eSIM文件通过共享缓冲器映射至所述普通环境下，以更新所述普通环境下的eSIM文件。

- [24] 作为一种可选的实施方式，所述方法还包括：
- [25] 所述移动终端在所述安全环境下检测第二更新请求，其中，所述第二更新请求用于请求更新所述安全环境下的所述第二验证信息，所述第二更新请求携带有新的第二验证信息和第三验证信息；
- [26] 所述移动终端在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；
- [27] 当所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功时，所述移动终端利用所述新的第二验证信息更新所述第二验证信息。
- [28] 作为一种可选的实施方式，所述方法还包括：
- [29] 所述移动终端在所述安全环境下检测第三更新请求，其中，所述第三更新请求用于请求更新所述安全环境下的所述目标应用和所述第二验证信息，所述第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；
- [30] 所述移动终端在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；
- [31] 当所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功时，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。
- [32] 作为一种可选的实施方式，所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功之后，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，所述方法还包括：
- [33] 所述移动终端对所述新的目标应用进行签名信息验证；
- [34] 所述移动终端判断所述签名信息验证是否通过；
- [35] 其中，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息，包括：
- [36] 若所述移动终端判断所述签名信息验证通过，则所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

- [37] 作为一种可选的实施方式，所述移动终端判断所述签名信息验证通过之后，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，所述方法还包括：
- [38] 所述移动终端输出第二验证指令，所述第二验证指令用于指示用户输入第二生物特征信息；
- [39] 所述移动终端判断用户输入的第二生物特征信息是否校验通过；
- [40] 其中，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息，包括：
- [41] 若所述移动终端判断所述第二生物特征信息校验通过，则所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。
- [42] 本发明实施例第二方面公开一种移动终端，所述移动终端包括普通环境和安全环境，其中，所述安全环境为所述移动终端运行在安全域TZ下的环境，所述移动终端包括：
- [43] 第一检测单元，设置为在所述普通环境下检测网络服务器发送的第一更新请求，所述第一更新请求用于请求更新所述移动终端中的原始嵌入式用户识别模块eSIM文件；
- [44] 启动单元，设置为根据所述第一更新请求，启动所述安全环境下的目标应用；
- [45] 所述第一检测单元，还设置为通过所述目标应用检测所述网络服务器发送的第一验证信息和目标eSIM文件，其中，所述第一验证信息为用于对所述网络服务器的身份进行验证的信息；
- [46] 校验单元，设置为在所述安全环境下对所述第一验证信息进行校验；
- [47] 第一更新单元，设置为当所述校验单元在所述安全环境下对所述第一验证信息校验成功时，利用所述目标eSIM文件更新所述原始eSIM文件。
- [48] 作为一种可选的实施方式，所述移动终端还包括：
- [49] 获取单元，设置为在所述校验单元在所述安全环境下对所述第一验证信息校验成功之后，所述第一更新单元利用所述目标eSIM文件更新所述原始eSIM文件之前，在所述安全环境下获取第二验证信息，所述第二验证信息为用于对所述目

标应用的安全性进行验证的信息；

[50] 所述校验单元，还设置为在所述安全环境下对所述第二验证信息进行校验；

[51] 所述第一更新单元具体设置为当所述校验单元对所述第二验证信息校验成功时，利用所述目标eSIM文件更新所述原始eSIM文件。

[52] 作为一种可选的实施方式，所述移动终端还包括：

[53] 第一输出单元，设置为当所述校验单元在所述安全环境下对所述第一验证信息校验成功之后，所述第一更新单元利用所述目标eSIM文件更新所述原始eSIM文件之前，输出第一验证指令，所述第一验证指令用于指示用户输入第一生物特征信息；

[54] 第一判断单元，设置为判断用户输入的第一生物特征信息是否校验通过；

[55] 所述第一更新单元具体设置为当所述第一判断单元判断用户输入的所述第一生物特征信息校验通过时，利用所述目标eSIM文件更新所述原始eSIM文件。

[56] 作为一种可选的实施方式，所述移动终端还包括：

[57] 映射单元，设置为将所述安全环境下的所述目标eSIM文件通过共享缓冲器映射至所述普通环境下，以更新所述普通环境下的eSIM文件。

[58] 作为一种可选的实施方式，所述移动终端还包括：

[59] 第二检测单元，设置为在所述安全环境下检测第二更新请求，其中，所述第二更新请求用于请求更新所述第二验证信息，所述第二更新请求携带有新的第二验证信息和第三验证信息；

[60] 所述校验单元，还设置为在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；

[61] 第二更新单元，设置为当所述校验单元对所述新的第二验证信息和所述第三验证信息均校验成功时，利用所述新的第二验证信息更新所述第二验证信息。

[62] 作为一种可选的实施方式，所述移动终端还包括：

[63] 第三检测单元，设置为在所述安全环境下检测第三更新请求，其中，所述第三更新请求用于请求更新所述目标应用和所述第二验证信息，所述第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；

[64] 所述校验单元，还设置为在所述安全环境下分别对所述新的第二验证信息和所

述第三验证信息进行校验；

[65] 第三更新单元，设置为当所述校验单元对所述新的第二验证信息和所述第三验证信息均校验成功时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[66] 作为一种可选的实施方式，所述校验单元，还设置为在对所述新的第二验证信息和所述第三验证信息均校验成功之后，所述第三更新单元利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，对所述新的目标应用进行签名信息验证；

[67] 所述移动终端还包括：

[68] 第二判断单元，设置为判断所述签名信息验证是否通过；

[69] 所述第三更新单元具体设置为当所述第二判断单元判断所述签名信息验证通过时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[70] 作为一种可选的实施方式，所述移动终端还包括：

[71] 第二输出单元，设置为在所述第二判断单元判断所述签名信息验证通过之后，所述第三更新单元利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，输出第二验证指令，所述第二验证指令用于指示用户输入第二生物特征信息；

[72] 所述第二判断单元，还设置为判断用户输入的第二生物特征信息是否校验通过；

[73] 所述第三更新单元具体设置为当所述第二判断单元判断所述第二生物特征信息校验通过时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[74] 与现有技术相比，本发明实施例具有以下有益效果：

[75] 本发明实施例中，移动终端在普通环境下通过检测网络服务器发送的第一更新请求，启动安全环境下的目标应用，从而通过目标应用检测网络服务器发送的第一验证信息，当在安全环境下对第一验证信息校验成功时，移动终端利用目标eSIM文件更新原始eSIM文件。可见，实施本发明实施例，当移动终端检测到

网络服务器发起的eSIM文件更新时，需在TZ环境下对网络服务器的身份信息校验成功后才能进行eSIM文件的更新，从而能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。

附图说明

[76] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[77] 图1是本发明实施例公开的一种防止eSIM文件被篡改的方法的流程示意图；

[78] 图2是本发明实施例公开的一种防止eSIM文件被篡改的具体原理示意图；

[79] 图3是本发明实施例公开的另一种防止eSIM文件被篡改的方法的流程示意图；

[80] 图4是本发明实施例公开的另一种防止eSIM文件被篡改的具体原理示意图；

[81] 图5是本发明实施例公开的一种移动终端的结构示意图；

[82] 图6是本发明实施例公开的另一种移动终端的结构示意图；

[83] 图7是本发明实施例公开的又一种移动终端的结构示意图；

[84] 图8是本发明实施例公开的又一种移动终端的结构示意图；

具体实施方式

[85] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[86] 本发明实施例公开了一种防止eSIM文件被篡改的方法及移动终端，能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。以下分别进行详细说明。

[87] 请参阅图1，图1是本发明实施例公开的一种防止eSIM文件被篡改的方法的流程示意图，该方法应用于移动终端，且移动终端包括普通环境和安全环境，其中，安全环境为移动终端运行在安全域TZ下的环境。如图1所示，该防止eSIM文件被篡改的方法可以包括以下步骤。

[88] 101、移动终端在普通环境下检测网络服务器发送的第一更新请求。

- [89] 本发明实施例中，该第一更新请求用于请求更新移动终端中的原始eSIM文件。移动终端可以包括移动手机、平板电脑、个人数字助理（Personal Digital Assistant, PDA）、移动互联网设备（Mobile Internet Device, MID）、智能穿戴设备（如智能手表、智能手环）等各种移动终端，本发明实施例不作限定。
- [90] 本发明实施例中，移动终端可以包括普通环境和安全环境，其中，安全环境又可称为TZ（TrustZone，安全域）环境，是移动终端运行在TZ下的一种环境，具体的，是基于TZ技术通过在嵌入式内核中开辟出一块可信代码区来构建安全运行的环境。普通环境是移动终端中原有的环境，是一种非TZ环境，如普通Android系统下用户可以正常进行各项操作（如打电话、上网、发信息等）的环境。普通环境和安全环境为移动终端中两个独立且互不干扰的工作环境。
- [91] 102、移动终端根据第一更新请求，启动安全环境下的目标应用。
- [92] 103、移动终端通过目标应用检测网络服务器发送的第一验证信息和目标eSIM文件。
- [93] 本发明实施例中，第一验证信息为用于对网络服务器的身份进行验证的信息，即用于验证网络服务器的真伪。第一验证信息可以是网络服务器下发的网络密钥cipher_key_A。
- [94] 104、移动终端在安全环境下对第一验证信息进行校验，若移动终端对第一验证信息校验成功，则执行步骤105；否则，结束本流程。
- [95] 本发明实施例中，移动终端在安全环境下将第一验证信息与预设的第一验证信息进行匹配验证，若匹配成功，则确定第一验证信息通过校验。第一验证信息可以是网络服务器下发的网络密钥cipher_key_A。具体的，移动终端将接收到的网络密钥与预设的网络密钥进行匹配验证，若匹配成功，则移动终端利用目标eSIM文件更新原始eSIM文件；同时，网络服务器下发的网络密钥可以用来验证网络服务器的真伪，若该网络密钥与预设的网络密钥匹配成功，则说明是真网络服务器下发的网络密钥；若匹配不成功，则可能是黑客伪装的网络服务器，则移动终端将不利用目标eSIM文件更新原始eSIM文件，即防止原始eSIM文件文件被篡改，以对原始eSIM文件进行保护。
- [96] 105、移动终端利用目标eSIM文件更新原始eSIM文件。

- [97] 作为一种可选的实施方式，移动终端在安全环境下对第一验证信息校验成功之后，以及移动终端利用目标eSIM文件更新原始eSIM文件之前，图1描述的方法还包括以下步骤：
- [98] 11) 移动终端在安全环境下获取第二验证信息，第二验证信息为用于对目标应用的安全性进行验证的信息；
- [99] 12) 移动终端在安全环境下对第二验证信息进行校验，若校验通过，则执行步骤105；否则，结束本流程。
- [100] 该实施方式中，第二验证信息为用于对目标应用的安全性进行验证的信息。第二验证信息可以是应用安全密钥HMAC_key_A，可以用来验证目标应用当前是否处于安全状态，且应用安全密钥可以是移动终端预先存储的，也可以是从运营商安全工具中获取的，本发明实施例不作限定。
- [101] 作为一种可选的实施方式，移动终端在安全环境下对第一验证信息校验成功之后，以及移动终端利用目标eSIM文件更新原始eSIM文件之前，图1描述的方法还包括以下步骤：
- [102] 13) 移动终端输出第一验证指令，第一验证指令用于指示用户输入第一生物特征信息；
- [103] 14) 移动终端判断用户输入的第一生物特征信息是否校验通过，若通过，则执行步骤105；否则，结束本流程。
- [104] 该实施方式中，第一生物特征信息可以是用户的指纹信息、虹膜信息、声纹信息、脸像信息、视网膜信息等，该实施方式不作限定。举例来说，第一生物特征信息可以是用户的指纹信息，用户在进行eSIM文件更新时，输出验证指令，用户输入指纹，当用户的指纹与预设指纹匹配时，则可以进行eSIM文件的更新；若不匹配，则不能进行eSIM文件的更新。
- [105] 该实施方式中，由于用户需要输入生物特征信息，并且验证成功，移动终端才能利用目标eSIM文件更新原始eSIM文件，从而能够防止eSIM文件被恶意篡改，提高移动终端的安全性。
- [106] 作为一种可选的实施方式，图1描述的方法还包括以下步骤：
- [107] 15) 移动终端将安全环境下的目标eSIM文件通过共享缓冲器映射至普通环境下

，以更新所述普通环境下的eSIM文件。

[108] 该实施方式中，将安全环境下的eSIM文件与普通环境下的eSIM文件相隔离，黑客进行恶意篡改时，移动终端可以进行安全恢复流程，从而来防止eSIM文件的恶意篡改。

[109] 请参阅图2，图2是本发明实施例公开的一种防止eSIM文件被篡改的具体原理示意图，以图2所示的原理示意图为例，来说明本发明实施例公开的一种防止eSIM文件被篡改的方法，移动终端包括普通环境（Non-secure world）和安全环境（Secure world）。

[110] 如图2所示，具体实施例的流程步骤与图2标注的步骤一致，具体流程如下：

[111] （1）网络(真/伪)服务器发送请求（即第一更新请求）到普通环境下的eSimApp应用；

[112] （2）eSimApp应用通知单片机驱动程序SCM Driver，网络请求更新eSIM文件；

[113] （3）SCM Driver通知监测器Monitor有网络更新；

[114] （4）移动终端进入TZ环境，并且启动Sec-eSimApp应用（即目标应用），通知SCM Driver模块Sec-eSimApp应用准备就绪；

[115] （5）SCM Driver模块通知eSimApp应用，Sec-eSimApp应用准备就绪；

[116] （6）eSimApp应用通知网络服务器，并进行以下操作；

[117] （7）网络服务器下发网络密钥cipher_key_A（即第一验证信息）；

[118] （8）移动终端发送网络密钥cipher_key_A和应用安全密钥HMAC_key_A（即第二验证信息）到Crypto模块进行有效性验证（即进行校验）；

[119] 具体地，应用安全密钥可以是移动终端预先存储的，也可以是从运营商安全工具中获取的。

[120] （9）若Crypto模块对网络密钥以及应用安全密钥的有效性验证失败，通知Sec-eSimApp应用效验失败不再进行后续操作；

[121] 有效性验证失败，则说明服务器可能为伪服务器或服务器异常，从而结束更新流程。

[122] （10）Crypto模块对网络密钥以及应用安全密钥的有效性验证成功，通知Sec-e

SimApp应用效验成功，并进行后续操作；

- [123] (11) Sec-eSimApp应用通知网络服务器，并进行下步操作；
- [124] (12) 网络服务器下发eSIM文件（即目标eSIM文件）到Sec-eSimApp应用；
- [125] (13) 文件服务器FileService将eSIM文件保存为临时eSIM文件；
- [126] (14) FileService通知安全识别模块进行安全效验流程；
- [127] (15) 安全识别模块启动生物识别APP；
- [128] (16) 生物识别APP通知用户进行生物特征信息的确认；
- [129] (17) 用户输入生物特征信息（即第一生物特征信息）确认操作；
- [130] (18) 生物识别APP把用户输入的生物特征信息传输给生物识别模块；
- [131] (19) 生物识别模块判断用户输入的所述第一生物特征信息校验通过，则通知FileService用户输入的生物特征信息验证成功；
- [132] (20) FileService把临时eSIM文件作为正式安全eSIM文件保存到SFS（Security Files System，安全文件系统）系统中；
- [133] (21) SFS系统中的安全eSIM文件在共享buffer中做安全文件映射，映射生成普通环境下的eSIM文件；
- [134] (22) 其它需要使用eSIM功能的模块通过EFS（Encrypting File System，加密文件系统）系统使用eSIM文件。
- [135] 本发明实施例通过生物识别技术校验用户的选择及修改权限，大大加强了安全性，有效防止因为设备丢失或误操作的产生。并且，当遇到黑客进行恶意篡改eSIM文件时，移动终端可以做安全恢复流程，从而来防止黑客的恶意篡改。
- [136] 可见，实施图1所描述的方法，用户需要进行eSIM文件的更新时，移动终端需要在安全环境下进行第一验证信息的校验，当校验成功时，移动终端才可以利用目标eSIM文件更新原始eSIM文件。可见，实施本发明实施例，能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。
- [137] 请参阅图3，图3是本发明实施例公开的另一种防止eSIM文件被篡改的方法的流程图示意图，该方法应用于移动终端，且移动终端包括普通环境和安全环境，其中，安全环境为移动终端运行在安全域TZ下的环境。如图3所示，该防止eSIM文件被篡改的方法可以包括以下步骤。

- [138] 301、移动终端在普通环境下检测网络服务器发送的第一更新请求。
- [139] 本发明实施例中，该第一更新请求用于请求更新移动终端中的原始eSIM文件。
- [140] 302、移动终端根据第一更新请求，启动安全环境下的目标应用。
- [141] 303、移动终端通过目标应用检测网络服务器发送的第一验证信息和目标eSIM文件。
- [142] 本发明实施例中，第一验证信息为用于对网络服务器的身份进行验证的信息。第一验证信息可以是网络服务器下发的网络密钥cipher_key_A。
- [143] 304、移动终端在安全环境下对第一验证信息进行校验，若移动终端对第一验证信息校验成功，则执行步骤305；否则，结束本流程。
- [144] 本发明实施例中，移动终端在安全环境下将第一验证信息与预设的第一验证信息进行匹配验证，若匹配成功，则确定第一验证信息通过校验。
- [145] 305、移动终端在安全环境下获取第二验证信息。
- [146] 本发明实施例中，第二验证信息为用于对目标应用的安全性进行验证的信息。第二验证信息可以是应用安全密钥HMAC_key_A，可以用来验证目标应用当前是否处于安全状态，且应用安全密钥可以是移动终端预先存储的，也可以是从运营商安全工具中获取的，本发明实施例不作限定。
- [147] 306、移动终端在安全环境下对第二验证信息进行校验，若校验成功，则执行步骤307；否则，结束本流程。
- [148] 本发明实施例中，移动终端在安全环境下将第二验证信息与预设的第二验证信息进行匹配验证，若匹配成功，则确定第二验证信息通过校验。
- [149] 307、移动终端利用目标eSIM文件更新原始eSIM文件。
- [150] 本发明实施例中，移动终端需要进行第一验证信息的校验以及第二验证信息的校验，并且两者均校验成功后，才能利用目标eSIM文件更新原始eSIM文件，从而能够有效提高移动终端的安全性。
- [151] 作为一种可选的实施方式，图3描述的方法还包括以下步骤：
- [152] 31) 移动终端在安全环境下检测第二更新请求，第二更新请求用于请求更新安全环境下的第二验证信息，第二更新请求携带有新的第二验证信息和第三验证信息；

- [153] 32) 移动终端在安全环境下分别对新的第二验证信息和第三验证信息进行校验，若校验成功，则执行步骤33)；否则，结束本流程。
- [154] 33) 移动终端利用新的第二验证信息更新第二验证信息。
- [155] 该实施方式中，第三验证信息可以用于对第二更新请求的来源的安全性进行验证。第二更新请求可以是运营商安全工具下发的，由于运营商安全工具可能是黑客伪造的，所以可以通过第三验证信息来对运营商安全工具的身份进行校验。
- [156] 该实施方式中，移动终端可以在第一验证信息验证通过之后，进行第二验证信息的验证；也可以先进行第二验证信息的验证，再进行第一验证信息的验证；还可以将第一验证信息与第二验证信息同时进行验证，本实施方式不作限定。
- [157] 该实施方式中，第三验证信息可以用于对第二更新请求的来源的安全性进行验证。第二更新请求可以是运营商安全工具下发的，由于运营商安全工具可能是黑客伪造的，所以可以通过第三验证信息来对运营商安全工具的身份进行校验。
- [158] 该实施方式中，新的第二验证信息以及第三验证信息均需要通过验证后，移动终端才能进行新的第二验证信息的更新，从而可以防止第二验证信息被恶意修改，进而提高了移动终端的安全性。
- [159] 请参阅图4，图4是本发明实施例公开的另一种防止eSIM文件被篡改的具体原理示意图，以图4所示的原理示意图为例，来说明本发明实施例公开的另一种防止eSIM文件被篡改的方法，移动终端包括普通环境（Non-secure world）和安全环境（Secure world）。
- [160] 如图4所示，举例来说，当移动终端收到运营商安全工具下发的更新应用安全密钥的请求（即第二更新请求）时，从运营商安全工具获取新的应用安全密钥HMAC_key_A（即新的第二验证信息），以及获取运营商安全工具下发的网络密钥（即第三验证信息）；
- [161] Sec-eSimApp应用将从运营商安全工具获取的新的应用安全密钥HMAC_key_A和网络密钥发送至至Crypto模块中，以进行安全性验证；
- [162] 若运营商安全工具下发的网络密钥与移动终端中预先存储的匹配成功，则说明

该运营商安全工具是安全的，同时进行新的应用安全密钥HMAC_key_A的验证，若均验证成功，则进行应用安全密钥的更新，即利用从运营商安全工具中下载的安全密钥覆盖掉原先的安全密钥。可选的，在应用安全密钥和网络密钥均验证成功，在更新应用安全密钥之前，还可以采集用户的生物特征信息对用户的身份进行验证。

[163] 作为一种可选的实施方式，图3描述的方法还包括以下步骤：

[164] 34) 移动终端在安全环境下检测第三更新请求，第三更新请求用于请求更新安全环境下的目标应用和第二验证信息，且第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；

[165] 35) 移动终端在安全环境下分别对新的第二验证信息和第三验证信息进行校验，若校验成功，则执行步骤36；否则，结束本流程。

[166] 36) 所述移动终端利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。

[167] 该实施方式中，第三验证信息可以用于对第三更新请求的来源的安全性进行验证。第三更新请求可以是运营商安全工具下发的，由于运营商安全工具可能是黑客伪造的，所以可以通过第三验证信息来对运营商安全工具的身份进行校验。

[168] 作为一种可选的实施方式，在执行完步骤35)之后，在执行步骤36)之前，图3描述的方法还包括以下步骤：

[169] 37) 移动终端对新的目标应用进行签名信息验证，若验证通过，则执行步骤36)；否则，结束本流程。

[170] 该实施方式中，签名信息可以用来验证新的目标应用的安全性；若新的目标应用的签名信息未通过，则说明新的目标应用可能存在安全隐患，从而结束本流程；若新的目标应用的签名信息通过验证，则说明新的目标应用是安全的，可以进行下一步操作。

[171] 作为一种可选的实施方式，在执行完步骤37)之后，在执行步骤36)之前，图3描述的方法还包括以下步骤：

[172] 38) 移动终端输出第二验证指令，第二验证指令用于指示用户输入第二生物特

征信息;

[173] 39) 移动终端判断用户输入的第二生物特征信息是否校验通过, 若校验通过, 则执行步骤310; 否则结束本流程。

[174] 310) 移动终端利用新的目标应用更新目标应用, 以及利用新的第二验证信息更新第二验证信息。

[175] 请参阅图4, 图4是本发明实施例公开的另一种防止eSIM文件被篡改的具体原理示意图, 以图4所示的原理示意图为例, 来说明本发明实施例公开的另一种防止eSIM文件被篡改的方法, 移动终端包括普通环境 (Non-secure world) 和安全环境 (Secure world) 。

[176] 如图4所示, 具体实施例的流程步骤与图4标注的步骤一致, 具体流程如下:

[177] (1) 通过运营商安全工具下载Sec-eSimApp应用和应用安全密钥HMAC_key_A (即第三更新请求), 且将其保存为临时文件;

[178] 具体地, 还可以从运营商安全工具获取网络密钥 (即第三验证信息) 。

[179] (2) 发送网络密钥cipher_key_A和应用安全密钥HMAC_key_A 到Crypto模块中, 以进行有效性验证;

[180] (3) 若Crypto模块对网络密钥以及应用安全密钥的有效性验证失败, 通知Sec-eSimApp应用效验失败, 从而删除临时Sec-eSimApp应用和应用安全密钥HMAC_key_A文件, 结束更新流程;

[181] (4) 若Crypto模块对网络密钥以及应用安全密钥的有效性验证成功, 则将下载的临时Sec-eSimApp应用相关的证书信息传递到TZ PIL中, 且进行以下流程;

[182] (5) 在Fuse模块中进行Sec-eSimApp应用签名信息的验证;

[183] 该实施方式中, 通过TZ技术和签名熔丝, 防止了黑客通过物理连接来更新破解Sec-eSimApp应用。

[184] (6) Fuse模块将验证结果通知安全识别模块;

[185] (7) 若签名不匹配, 通知Sec-eSimApp应用效验失败, 从而删除临时Sec-eSimApp应用和HMAC_key_A文件, 结束更新流程;

[186] (8) 若签名匹配, 安全识别模块通知生物识别APP启动;

[187] (9) 生物识别APP通知用户进行生物特征信息的确认;

- [188] (10) 用户输入生物特征信息确认操作;
- [189] (11) 生物识别APP把用户输入的生物特征信息传输给生物识别模块;
- [190] (12) 若生物识别模块验证成功, 则进行以下流程;
- [191] (13) 安全识别模块通知文件服务器FileService安全流程效验全部完成;
- [192] (14) FileService把临时Sec-eSimApp应用和HMAC_key_A文件覆盖之前早期文件, 以实现Sec-eSimApp应用和应用安全密钥HMAC_key_A的更新;
- [193] (15) FileService通知SCM;
- [194] (16) SCM通知Monitor;
- [195] (17) Monitor通知SCM Driver已完成安全环境下Sec-eSimApp应用的更新;
- [196] (18) SCMDriver通知eSimApp应用进行更新;
- [197] (19) eSimApp应用连接网络服务器请求更新;
- [198] (20) 下载最新eSimApp应用, 以完成普通环境下eSimApp应用的更新。
- [199] 可见, 实施图3描述的方法, 用户在进行eSIM文件、目标应用和新的第二验证信息的更新时, 需要进行第一验证信息和第二验证信息的校验, 并且均校验成功后, 通过生物特征信息的验证, 才能进行eSIM文件、目标应用和新的第二验证信息的更新。可见, 实施本发明实施例, 能够有效防止eSIM文件被恶意篡改, 提高移动终端的安全性。
- [200] 请参阅图5, 图5是本发明实施例公开的一种移动终端的结构示意图, 可以用于执行本发明实施例公开的防止eSIM文件被篡改的方法。如图5所示, 该移动终端包括普通环境和安全环境, 其中, 安全环境为移动终端运行在安全域TZ环境下的环境, 该移动终端可以包括:
- [201] 第一检测单元501, 设置为在所述普通环境下检测网络服务器发送的第一更新请求, 所述第一更新请求用于请求更新所述移动终端中的原始嵌入式用户识别模块eSIM文件;
- [202] 启动单元502, 设置为根据第一更新请求, 启动安全环境下的目标应用;
- [203] 上述第一检测单元501, 还设置为通过目标应用检测网络服务器发送的第一验证信息和目标eSIM文件, 其中, 第一验证信息为用于对网络服务器的身份进行验证的信息;

- [204] 校验单元503, 设置为在安全环境下对第一验证信息进行校验;
- [205] 第一更新单元505, 设置为当校验单元503在安全环境下对第一验证信息校验成功时, 利用目标eSIM文件更新原始eSIM文件。
- [206] 请一并参阅图6, 图6是本发明实施例公开的另一种移动终端的结构示意图。其中, 图6所示的移动终端是在图5所示的移动终端的基础上进一步优化得到的。与图5所示的移动终端相比, 图6所示的移动终端中还可以包括:
- [207] 获取单元505, 设置为在校验单元503在安全环境下对第一验证信息校验成功之后, 第一更新单元504利用目标eSIM文件更新原始eSIM文件之前, 在安全环境下获取第二验证信息, 第二验证信息为用于对目标应用的安全性进行验证的信息;
- [208] 校验单元503, 还设置为在安全环境下对第二验证信息进行校验;
- [209] 第一更新单元504具体设置为当校验单元503对第二验证信息校验成功时, 利用目标eSIM文件更新原始eSIM文件。
- [210] 作为一种可选的实施方式, 图6所述的移动终端还可以包括:
- [211] 第一输出单元506, 设置为当校验单元503在安全环境下对第一验证信息校验成功之后, 第一更新单元504利用目标eSIM文件更新原始eSIM文件之前, 输出第一验证指令, 该第一验证指令用于指示用户输入第一生物特征信息;
- [212] 第一判断单元507, 设置为判断用户输入的第一生物特征信息是否校验通过;
- [213] 相应地, 第一更新单元504具体设置为当第一判断单元507判断用户输入的第一生物特征信息校验通过时, 利用目标eSIM文件更新原始eSIM文件。
- [214] 作为一种可选的实施方式, 图6所示的移动终端还可以包括:
- [215] 映射单元508, 设置为将安全环境下的目标eSIM文件通过共享缓冲映射至普通环境下。
- [216] 作为一种可选的实施方式, 图6所示的移动终端还可以包括:
- [217] 第二检测单元509, 设置为在所述安全环境下检测第二更新请求, 其中, 第二更新请求用于请求更新第二验证信息, 第二更新请求携带有新的第二验证信息和第三验证信息;
- [218] 校验单元503, 还设置为在安全环境下分别对新的第二验证信息和第三验证信

息进行校验；

[219] 第二更新单元510，设置为当校验单元503对新的第二验证信息和第三验证信息均校验成功时，利用新的第二验证信息更新第二验证信息。

[220] 请一并参阅图7，图7是本发明实施例公开的又一种移动终端的结构示意图。其中，图7所示的移动终端是在图5所示的移动终端的基础上进一步优化得到的。与图5所示的移动终端相比，图7所示的移动终端中还可以包括：

[221] 第三检测单元511，设置为在所述安全环境下检测第三更新请求，其中，第三更新请求用于请求更新目标应用和第二验证信息，第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；

[222] 校验单元503，还设置为在安全环境下分别对新的第二验证信息和第三验证信息进行校验；

[223] 第三更新单元512，设置为当校验单元503对新的第二验证信息和第三验证信息均校验成功时，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。

[224] 作为一种可选的实施方式，校验单元503，还设置为在对新的第二验证信息和第三验证信息均校验成功之后，第三更新单元512利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息之前，对新的目标应用进行签名信息验证；

[225] 所述移动终端还包括：

[226] 第二判断单元513，设置为判断所述签名信息验证是否通过；

[227] 相应地，第三更新单元512具体设置为当第二判断单元513判断签名信息验证通过时，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。

[228] 作为一种可选的实施方式，图7所示的移动终端还包括：

[229] 第二输出单元514，设置为在第二判断单元513判断签名信息验证通过之后，第三更新单元512利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息之前，输出第二验证指令，第二验证指令用于指示用户输入第二生物特征信息；

[230] 所述第二判断单元513，还设置为判断用户输入的第二生物特征信息是否校验通过；

[231] 相应地，第三更新单元512具体设置为当第二判断单元513判断第二生物特征信息校验通过时，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。

[232] 可见，实施图5、图6和图7所示的移动终端，用户在进行eSIM文件、目标应用和新的第二验证信息的更新时，需要进行第一验证信息和第二验证信息的校验，并且均校验成功后，通过生物特征信息的验证，才能进行eSIM文件、目标应用和新的第二验证信息的更新。可见，实施本发明实施例，能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。

[233] 请参阅图8，图8是本发明实施例公开的另一种移动终端的结构示意图，可以用于执行本发明实施例公开的防止eSIM文件被篡改的方法。如图8所示，该移动终端800可以包括：至少一个处理器801，至少一个输入装置802，至少一个输出装置803，存储器804等组件。其中，这些组件可以通过一条或多条总线805进行通信连接。本领域技术人员可以理解，图8中示出的移动终端的结构并不构成对本发明实施例的限定，它既可以是总线形结构，也可以是星型结构，还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。其中：

[234] 处理器801为移动终端的控制中心，利用各种接口和线路连接整个移动终端的各个部分，通过运行或执行存储在存储器804内的程序和/或模块，以及调用存储在存储器804内的数据，以执行移动终端的各种功能和处理数据。处理器801可以由集成电路（Integrated Circuit，简称IC）组成，例如可以由单颗封装的IC所组成，也可以由连接多颗相同功能或不同功能的封装IC而组成。举例来说，处理器801可以仅包括中央处理器（Central Processing Unit，简称CPU），也可以是CPU、数字信号处理器（Digital Signal Processor，简称DSP）、图形处理器（Graphic Processing Unit，简称GPU）及各种控制芯片的组合。在本发明实施方式中，CPU可以是单运算核心，也可以包括多运算核心。

[235] 输入装置802可以包括标准的触摸屏、键盘等，也可以包括有线接口、无线接

口等，可以用于与网络服务器进行交互。

[236] 输出装置803可以包括显示屏、扬声器等，也可以包括有线接口、无线接口等。

[237] 存储器804可用于存储软件程序以及模块，处理器801、输入装置802以及输出装置803通过调用存储在存储器804中的软件程序以及模块，从而执行移动终端的各项功能应用以及实现数据处理。存储器804主要包括程序存储区和数据存储空间，其中，程序存储区可存储操作系统、至少一个功能所需的应用程序等；数据存储空间可存储根据移动终端的使用所创建的数据等。在本发明实施例中，操作系统可以是Android系统、iOS系统或Windows操作系统等等。

[238] 在图8所示的移动终端中，包括普通环境和安全环境，其中，安全环境为所述移动终端运行在安全域TZ环境下的环境，处理器801调用存储在存储器804中的应用程序，用于执行以下操作：

[239] 在普通环境下检测网络服务器发送的第一更新请求，第一更新请求用于请求更新移动终端中的原始嵌入式用户识别模块eSIM文件；

[240] 根据第一更新请求，启动安全环境下的目标应用；

[241] 通过目标应用检测网络服务器发送的第一验证信息和目标eSIM文件，其中，第一验证信息为用于对网络服务器的身份进行验证的信息；

[242] 在安全环境下对第一验证信息进行校验；

[243] 当在安全环境下对第一验证信息校验成功时，利用目标eSIM文件更新原始eSIM文件。

[244] 一个实施例中，处理器801在安全环境下对第一验证信息校验成功之后，以及利用目标eSIM文件更新原始eSIM文件之前，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：

[245] 在安全环境下获取第二验证信息，该第二验证信息为用于对目标应用的安全性进行验证的信息；

[246] 在安全环境下对第二验证信息进行校验；

[247] 其中，处理器801利用目标eSIM文件更新原始eSIM文件的具体实施方式可以为：

- [248] 当在安全环境下对第二验证信息校验成功时，利用目标eSIM文件更新原始eSIM文件。
- [249] 一个实施例中，处理器801在安全环境下对第一验证信息校验成功之后，以及利用目标eSIM文件更新原始eSIM文件之前，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [250] 触发输出装置803输出第一验证指令，该第一验证指令用于指示用户通过输入装置802输入第一生物特征信息；
- [251] 判断用户输入的第一生物特征信息是否校验通过；
- [252] 其中，处理器801利用目标eSIM文件更新原始eSIM文件的具体实施方式可以为：
- [253] 当判断用户输入的第一生物特征信息校验通过时，利用目标eSIM文件更新原始eSIM文件。
- [254] 一个实施例中，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [255] 将安全环境下的目标eSIM文件通过共享缓冲器映射至普通环境下。
- [256] 一个实施例中，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [257] 在安全环境下检测第二更新请求，其中，该第二更新请求用于请求更新第二验证信息，且第二更新请求携带有新的第二验证信息和第三验证信息；
- [258] 在安全环境下分别对新的第二验证信息和第三验证信息进行校验；
- [259] 当对新的第二验证信息和第三验证信息均校验成功时，利用新的第二验证信息更新第二验证信息。
- [260] 一个实施例中，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [261] 在安全环境下检测第三更新请求，其中，第三更新请求用于请求更新目标应用和第二验证信息，第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；
- [262] 在安全环境下分别对新的第二验证信息和第三验证信息进行校验；

- [263] 当对新的第二验证信息和第三验证信息均校验成功时，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。
- [264] 一个实施例中，处理器801对新的第二验证信息和第三验证信息均校验成功之后，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息之前，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [265] 对新的目标应用进行签名信息验证；
- [266] 判断签名信息验证是否通过；
- [267] 其中，处理器801利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息的具体实施方式可以为：
- [268] 若判断签名信息验证是否通过，则利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。
- [269] 一个实施例中，处理器判断签名信息通过之后，利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息之前，处理器801还可以调用存储在存储器804中的应用程序，并执行以下操作：
- [270] 触发输出装置803输出第二验证指令，该第二验证指令用于指示用户通过输入装置802输入第二生物特征信息；
- [271] 判断用户输入的第二生物特征信息是否校验通过；
- [272] 其中，处理器801利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息的具体实施方式可以为：
- [273] 若判断用户输入的第二生物特征信息校验通过，则利用新的目标应用更新目标应用，以及利用新的第二验证信息更新第二验证信息。
- [274] 可见，实施图8所示的移动终端，用户在进行eSIM文件、目标应用和新的第二验证信息的更新时，需要进行第一验证信息和第二验证信息的校验，并且均校验成功后，通过生物特征信息的验证，才能进行eSIM文件、目标应用和新的第二验证信息的更新。可见，实施本发明实施例，能够有效防止eSIM文件被恶意篡改，提高移动终端的安全性。
- [275] 本发明所有实施例中的模块或单元，可以通过通用集成电路，例如CPU，或通

过ASIC (Application Specific Integrated Circuit, 专用集成电路) 来实现。

[276] 需要说明的是, 对于前述的各个方法实施例, 为了简单描述, 故将其都表述为一系列的动作组合, 但是本领域技术人员应该知悉, 本发明并不受所描述的动作顺序的限制, 因为依据本发明, 某一些步骤可以采用其他顺序或者同时进行。其次, 本领域技术人员也应该知悉, 说明书中所描述的实施例均属于优选实施例, 所涉及的动作和模块并不一定是本发明所必须的。

[277] 本发明实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

[278] 本发明实施例移动终端中的单元可以根据实际需要进行合并、划分和删减。

[279] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程, 是可以通过计算机程序来指令相关的硬件来完成, 所述的程序可存储于一计算机可读取存储介质中, 该程序在执行时, 可包括如上述各方法的实施例的流程。其中, 所述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory, ROM) 或随机存取存储器 (Random Access Memory, 简称RAM) 等。

[280] 以上对本发明实施例公开的一种防止eSIM文件被篡改的方法及移动终端进行了详细介绍, 本文中应用了具体个例对本发明的原理及实施方式进行了阐述, 以上实施例的说明只是用于帮助理解本发明的方法及其核心思想; 同时, 对于本领域的一般技术人员, 依据本发明的思想, 在具体实施方式及应用范围上均会有改变之处, 综上所述, 本说明书内容不应理解为对本发明的限制。

权利要求书

- [权利要求 1] 一种防止eSIM文件被篡改的方法，其特征在于，移动终端包括普通环境和安全环境，其中，所述安全环境为所述移动终端运行在安全域TZ下的环境，所述方法包括：
- 所述移动终端在所述普通环境下检测网络服务器发送的第一更新请求，所述第一更新请求用于请求更新所述移动终端中的原始嵌入式用户识别模块eSIM文件；
- 所述移动终端根据所述第一更新请求，启动所述安全环境下的目标应用；
- 所述移动终端通过所述目标应用检测所述网络服务器发送的第一验证信息和目标eSIM文件，其中，所述第一验证信息为用于对所述网络服务器的身份进行验证的信息；
- 所述移动终端在所述安全环境下对所述第一验证信息进行校验；
- 当所述移动终端在所述安全环境下对所述第一验证信息校验成功时，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，所述移动终端在所述安全环境下对所述第一验证信息校验成功之后，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件之前，所述方法还包括：
- 所述移动终端在所述安全环境下获取第二验证信息，所述第二验证信息为用于对所述目标应用的安全性进行验证的信息；
- 所述移动终端在所述安全环境下对所述第二验证信息进行校验；
- 其中，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件，包括：
- 若所述移动终端对所述第二验证信息校验成功，则所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。
- [权利要求 3] 根据权利要求1所述的方法，其特征在于，所述移动终端在所述安

全环境下对所述第一验证信息校验成功之后，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件之前，所述方法还包括：

所述移动终端输出第一验证指令，所述第一验证指令用于指示用户输入第一生物特征信息；

所述移动终端判断用户输入的第一生物特征信息是否校验通过；

其中，所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件，包括：

若所述移动终端判断用户输入的所述第一生物特征信息校验通过，则所述移动终端利用所述目标eSIM文件更新所述原始eSIM文件。

[权利要求 4] 根据权利要求1~3任一项所述的方法，其特征在于，所述方法还包括：

所述移动终端将所述安全环境下的所述目标eSIM文件通过共享缓冲器映射至所述普通环境下，以更新所述普通环境下的eSIM文件。

[权利要求 5] 根据权利要求2所述的方法，其特征在于，所述方法还包括：

所述移动终端在所述安全环境下检测第二更新请求，其中，所述第二更新请求用于请求更新所述第二验证信息，所述第二更新请求携带有新的第二验证信息和第三验证信息；

所述移动终端在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；

当所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功时，所述移动终端利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 6] 根据权利要求2所述的方法，其特征在于，所述方法还包括：

所述移动终端在所述安全环境下检测第三更新请求，其中，所述第三更新请求用于请求更新所述目标应用和所述第二验证信息，

所述第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；

所述移动终端在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；

当所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功时，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 7]

根据权利要求6所述的方法，其特征在于，所述移动终端对所述新的第二验证信息和所述第三验证信息均校验成功之后，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，所述方法还包括：

所述移动终端对所述新的目标应用进行签名信息验证；

所述移动终端判断所述签名信息验证是否通过；

其中，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息，包括：若所述移动终端判断所述签名信息验证通过，则所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 8]

根据权利要求7所述的方法，其特征在于，所述移动终端判断所述签名信息验证通过之后，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，所述方法还包括：

所述移动终端输出第二验证指令，所述第二验证指令用于指示用户输入第二生物特征信息；

所述移动终端判断用户输入的第二生物特征信息是否校验通过；

其中，所述移动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息，包括：若所述移动终端判断所述第二生物特征信息校验通过，则所述移

动终端利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 9]

一种移动终端，其特征在于，所述移动终端包括普通环境和安全环境，其中，所述安全环境为所述移动终端运行在安全域TZ下的环境，所述移动终端包括：

第一检测单元，设置为在所述普通环境下检测网络服务器发送的第一更新请求，所述第一更新请求用于请求更新所述移动终端中的原始嵌入式用户识别模块eSIM文件；

启动单元，设置为根据所述第一更新请求，启动所述安全环境下的目标应用；

所述第一检测单元，还设置为通过所述目标应用检测所述网络服务器发送的第一验证信息和目标eSIM文件，其中，所述第一验证信息为用于对所述网络服务器的身份进行验证的信息；

校验单元，设置为在所述安全环境下对所述第一验证信息进行校验；

第一更新单元，设置为当所述校验单元在所述安全环境下对所述第一验证信息校验成功时，利用所述目标eSIM文件更新所述原始eSIM文件。

[权利要求 10]

根据权利要求9所述的移动终端，其特征在于，所述移动终端还包括：

获取单元，设置为在所述校验单元在所述安全环境下对所述第一验证信息校验成功之后，所述第一更新单元利用所述目标eSIM文件更新所述原始eSIM文件之前，在所述安全环境下获取第二验证信息，所述第二验证信息为用于对所述目标应用的安全性进行验证的信息；

所述校验单元，还设置为在所述安全环境下对所述第二验证信息进行校验；

所述第一更新单元具体设置为当所述校验单元对所述第二验证信

息校验成功时，利用所述目标eSIM文件更新所述原始eSIM文件。

[权利要求 11]

根据权利要求9所述的移动终端，其特征在于，所述移动终端还包括：

第一输出单元，设置为当所述校验单元在所述安全环境下对所述第一验证信息校验成功之后，所述第一更新单元利用所述目标eSIM文件更新所述原始eSIM文件之前，输出第一验证指令，所述第一验证指令用于指示用户输入第一生物特征信息；

第一判断单元，设置为判断用户输入的第一生物特征信息是否校验通过；

所述第一更新单元具体设置为当所述第一判断单元判断用户输入的所述第一生物特征信息校验通过时，利用所述目标eSIM文件更新所述原始eSIM文件。

[权利要求 12]

根据权利要求9~11任一项所述的移动终端，其特征在于，所述移动终端还包括：

映射单元，设置为将所述安全环境下的所述目标eSIM文件通过共享缓冲器映射至所述普通环境下，以更新所述普通环境下的eSIM文件。

[权利要求 13]

根据权利要求10所述的移动终端，其特征在于，所述移动终端还包括：

第二检测单元，设置为在所述安全环境下检测第二更新请求，其中，所述第二更新请求用于请求更新所述第二验证信息，所述第二更新请求携带有新的第二验证信息和第三验证信息；

所述校验单元，还设置为在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；

第二更新单元，设置为当所述校验单元对所述新的第二验证信息和所述第三验证信息均校验成功时，利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 14]

根据权利要求10所述的移动终端，其特征在于，所述移动终端还

包括：

第三检测单元，设置为在所述安全环境下检测第三更新请求，其中，所述第三更新请求用于请求更新所述目标应用和所述第二验证信息，所述第三更新请求携带有新的目标应用、新的第二验证信息和第三验证信息；

所述校验单元，还设置为在所述安全环境下分别对所述新的第二验证信息和所述第三验证信息进行校验；

第三更新单元，设置为当所述校验单元对所述新的第二验证信息和所述第三验证信息均校验成功时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 15]

根据权利要求14所述的移动终端，其特征在于，

所述校验单元，还设置为在对所述新的第二验证信息和所述第三验证信息均校验成功之后，所述第三更新单元利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，对所述新的目标应用进行签名信息验证；
所述移动终端还包括：

第二判断单元，设置为判断所述签名信息验证是否通过；

所述第三更新单元具体设置为当所述第二判断单元判断所述签名信息验证通过时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

[权利要求 16]

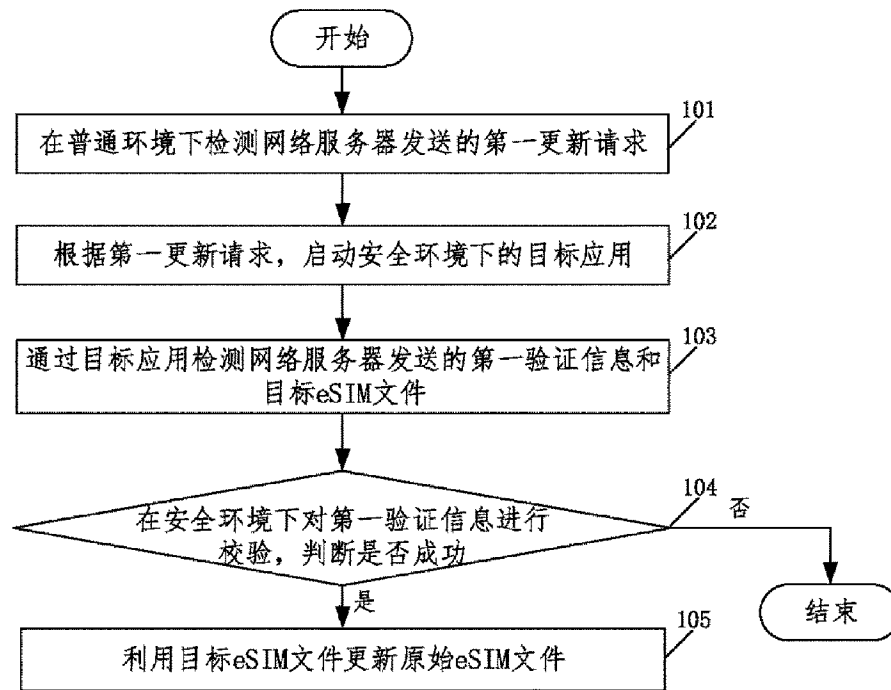
根据权利要求15所述的移动终端，其特征在于，所述移动终端还包括：

第二输出单元，设置为在所述第二判断单元判断所述签名信息验证通过之后，所述第三更新单元利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息之前，输出第二验证指令，所述第二验证指令用于指示用户输入第二生物特征信息；

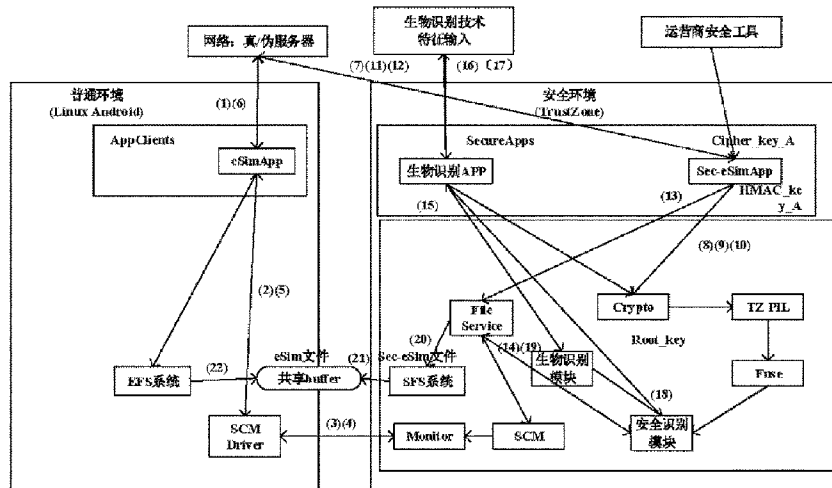
所述第二判断单元，还设置为判断用户输入的第二生物特征信息是否校验通过；

所述第三更新单元具体设置为当所述第二判断单元判断所述第二生物特征信息校验通过时，利用所述新的目标应用更新所述目标应用，以及利用所述新的第二验证信息更新所述第二验证信息。

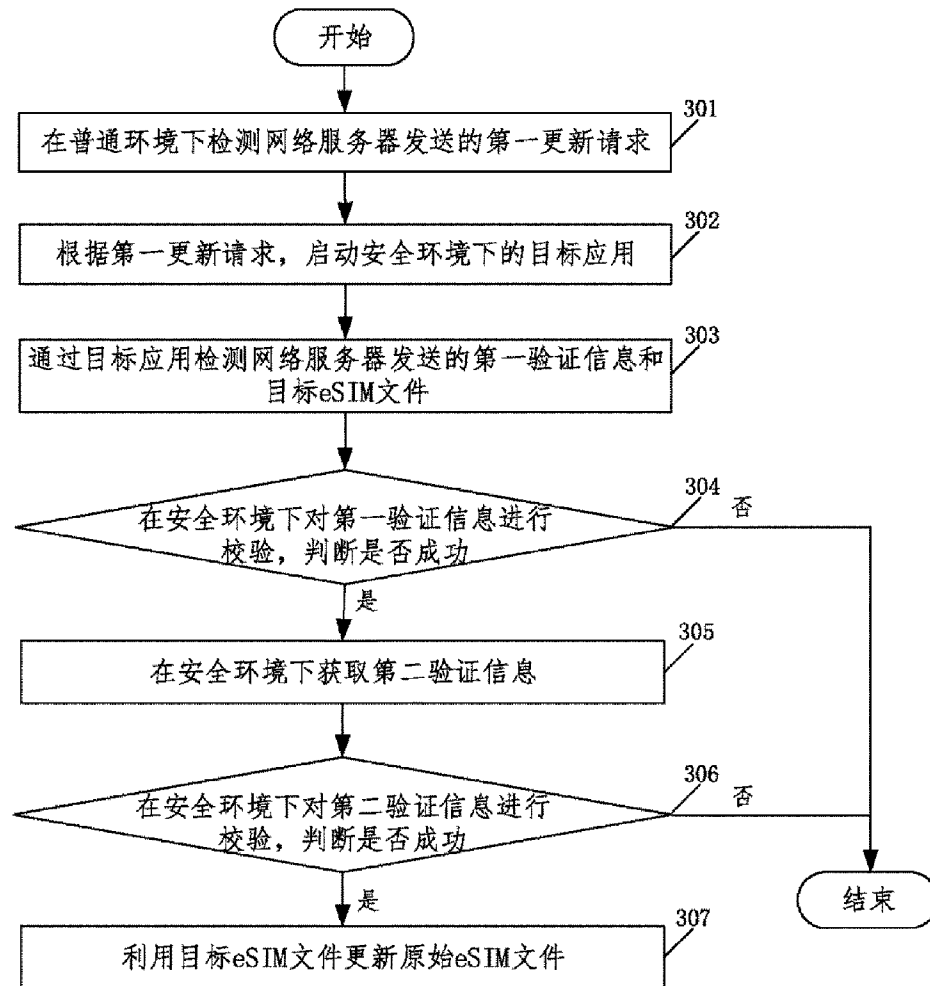
[Fig. 1]



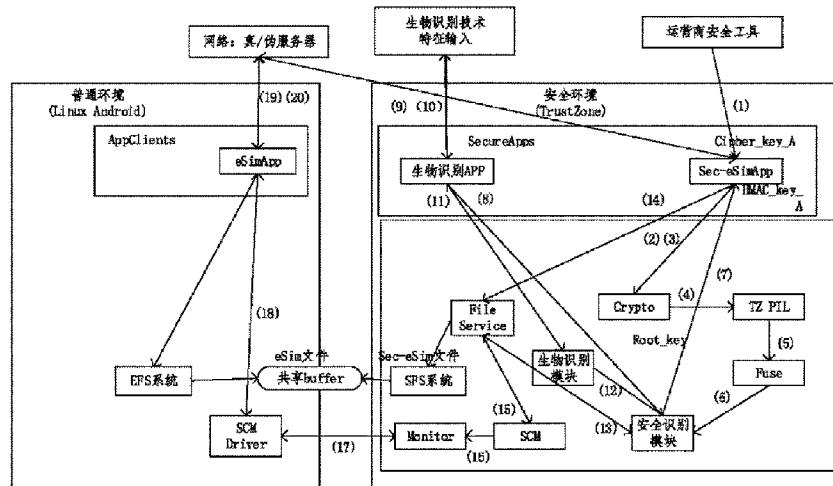
[Fig. 2]



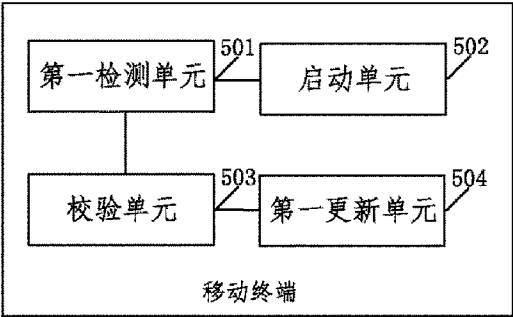
[Fig. 3]



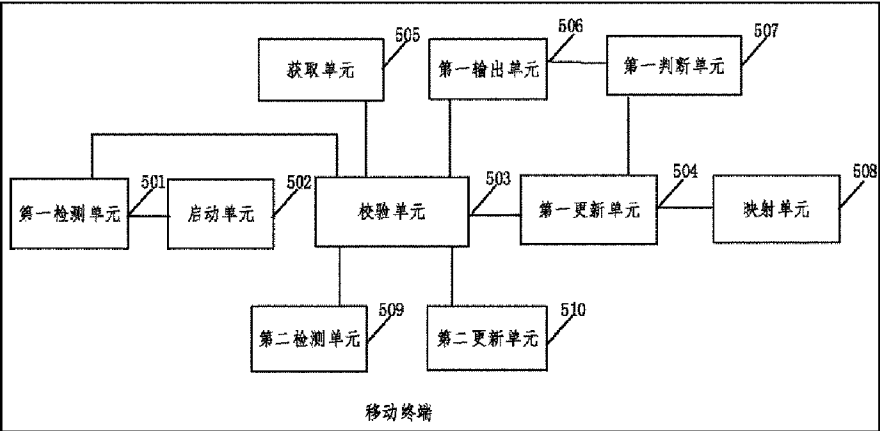
[Fig. 4]



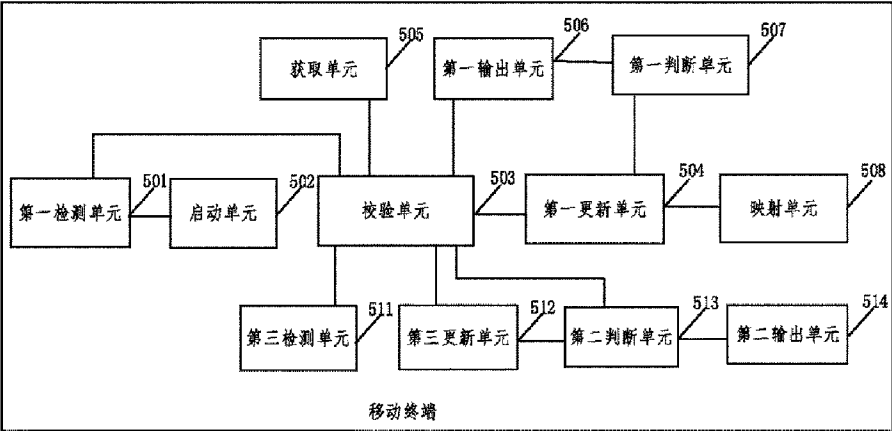
[Fig. 5]



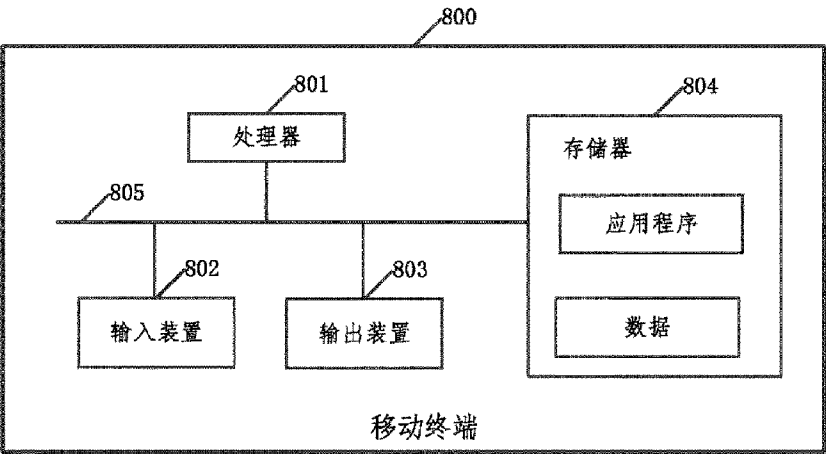
[Fig. 6]



[Fig. 7]



[Fig. 8]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/103877

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08 (2006.01) 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)

H04

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)

CNXTX, CNKI, CPRSABS, VEN: 嵌入式用户识别模块, 安全域, 嵌入式 sim, esim, 安全环境, sim 文件, sim, 篡改, 更新

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105100098 A (CHINA UNITED NETWORK COMMUNICATIONS CORPORATION LIMITED), 25 November 2015 (25.11.2015), description, pages 1 and 4-7	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 21 February 2017	Date of mailing of the international search report 27 March 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZHU, Shaohua Telephone No. (86-10) 62089391

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/103877

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105100098 A	25 November 2015	None	

A. 主题的分类 H04L 29/08 (2006.01) 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) H04 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, CNKI, CPRSABS, VEN: 嵌入式用户识别模块, 安全域, 嵌入式sim, esim, 安全环境, sim文件, sim, 篡改, 更新		
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 105100098 A (中国联合网络通信集团有限公司) 2015年 11月 25日 (2015 - 11 - 25) 说明书第1, 4-7页	1-16
☐ 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 2017年 2月 21日	国际检索报告邮寄日期 2017年 3月 27日	
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 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 朱少华 电话号码 (86-10) 62089391	

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/103877

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 105100098 A	2015年 11月 25日	无	