

(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 3 月 30 日 (30.03.2017)



(10) 国际公布号
WO 2017/049598 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01) H04W 12/04 (2009.01)
- (21) 国际申请号: PCT/CN2015/090752
- (22) 国际申请日: 2015 年 9 月 25 日 (25.09.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 广东欧珀移动通信有限公司 (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。
- (72) 发明人: 曾元清 (ZENG, Yuanqing); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。 唐海 (TANG, Hai); 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。
- (74) 代理人: 广州三环专利代理有限公司 (GUANGZHOU SCIHEAD PATENT AGENT CO., LTD.); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, 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))。

(54) Title: TERMINAL AUTHENTICATION METHOD AND DEVICE

(54) 发明名称: 终端认证的方法及设备

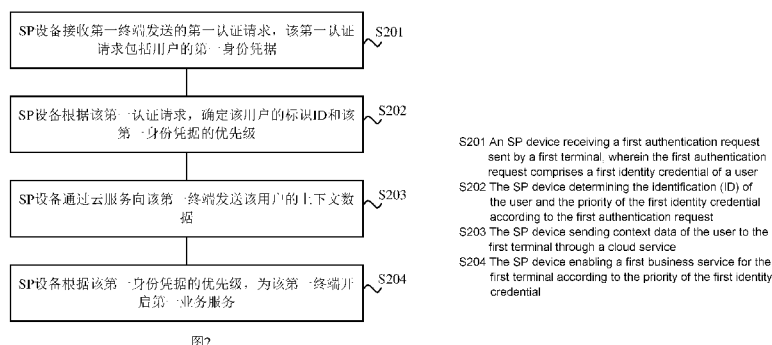


图2

(57) Abstract: Provided are a terminal authentication method and device. The method comprises: an SP device receiving a first authentication request sent by a first terminal, wherein the first authentication request comprises a first identity credential of a user; the SP device determining the identification (ID) of the user and the priority of the first identity credential according to the first authentication request; the SP device sending context data of the user to the first terminal through a cloud service; and the SP device enabling a first service for the first terminal according to the priority of the first identity credential. In the embodiments of the present invention, an SP device loads context data of a user for a terminal according to an identity credential of the user sent by the terminal and provides a corresponding service. Thus, a unified and secure identity authentication method can be realized, a seamless user experience is provided for the user, the usability can be improved, and better utilization of resources can be realized.

(57) 摘要: 本发明实施例提供了一种终端认证的方法和设备, 该方法包括: SP 设备接收第一终端发送的第一认证请求, 所述第一认证请求包括用户的第一身份凭据; SP 设备根据所述第一认证请求, 确定所述用户的标识 ID 和所述第一身份凭据的优先级; SP 设备通过云服务向所述第一终端发送所述用户的上下文数据; SP 设备根据所述第一身份凭据的优先级, 为所述第一终端开启第一服务。本发明实施例中, SP 设备根据终端发送的用户身份凭据, 为终端加载用户的上下文数据, 并提供相应的服务。这样能够实现统一安全的身份认证方式, 并为用户提供无缝的使用体验, 可以提高易用性, 并能实现资源的更优利用。

WO 2017/049598 A1

终端认证的方法及设备

技术领域

5 本发明实施例涉及通信领域，并且更具体地，涉及一种终端认证的方法及设备。

背景技术

在现有的移动通信系统中，运营商为用户提供 SIM 卡，蜂窝系统使用运营商提供的 SIM 卡进行身份认证。用户需要向不同的运营商分别申请 SIM
10 卡才能使用多个运营商提供的服务。并且，当 SIM 卡丢失或损坏时，用户无法接入运营商网络而导致无法使用服务。

另外，由于一个号码在同一时间只能使用一个终端设备，因此当用户想要更换终端设备时，必须同时转移 SIM 卡。然而目前不同的终端设备对于 SIM 卡的规格要求是不同的，因此，用户在更换终端设备时，可能需要到运
15 营商更换 SIM 卡或者使用转接器。这样容易给用户带来不便，造成用户开销大甚至可能会由于转接器的故障导致 SIM 卡或者终端设备损坏。

可见，现有的方式对用户使用运营商的服务造成了很多限制，给用户带来诸多不便，甚至还可能造成用户开销大。

20 发明内容

本发明实施例提供一种终端认证的方法和设备，可以为用户提供无缝的使用体验，提高易用性，并能实现资源的更优利用。

第一方面，提供了一种终端认证的方法，包括：

25 服务提供商 SP 设备接收第一终端发送的第一认证请求，所述第一认证请求包括用户的第一身份凭据；

所述 SP 设备根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级；

所述 SP 设备通过云服务向所述第一终端发送所述用户的上下文数据；

30 所述 SP 设备根据所述第一身份凭据的优先级，为所述第一终端开启第一服务。

第二方面，提供了一种终端认证的方法，包括：

终端生成请求接入服务提供商 SP 设备的认证请求，所述认证请求包括用户的身份凭据；

所述终端将所述认证请求发送至所述 SP 设备；

在所述认证请求通过时，所述终端获取并加载所述用户的上下文数据；

5 所述终端使用所述 SP 设备根据所述身份凭据的优先级，为所述终端提供的对应的服务。

第三方面，提供了一种服务提供商设备，包括：

接收单元，用于接收第一终端发送的第一认证请求，所述第一认证请求包括用户的第一身份凭据；

10 确定单元，用于根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级；

发送单元，用于通过云服务向所述第一终端发送所述用户的上下文数据；

15 处理单元，用于根据所述第一身份凭据的优先级，为所述第一终端开启第一服务。

第四方面，提供了一种终端，包括：

生成单元，用于生成请求接入服务提供商 SP 设备的认证请求，所述认证请求包括用户的身份凭据；

发送单元，用于将所述认证请求发送至所述 SP 设备；

20 获取单元，用于在所述认证请求通过时，获取并加载所述用户的上下文数据；

处理单元，用于使用所述 SP 设备根据所述身份凭据的优先级为所述终端提供的对应的服务。

25 本发明实施例通过 SP 设备根据终端发送的用户的身份凭据，为终端加载用户的上下文数据，并提供相应的服务。这样能够实现统一安全的身份认证方式，并为用户提供无缝的使用体验，可以提高易用性，并能实现资源的更优利用。

附图说明

30 为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图

仅仅是本发明的一些实施例，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。

图 1 是本发明一个实施例的终端认证的方法的示意性流程图。

图 2 是本发明另一个实施例的终端认证的方法的示意性流程图。

5 图 3 是本发明另一个实施例的终端认证的方法的示意性流程图。

图 4 是本发明一个实施例的用户身份认证的方法的示意性流程图。

图 5 是本发明一个实施例的终端呈现的选择界面的示意图。

图 6 是本发明另一个实施例的用户身份认证的方法的示意性流程图。

图 7 是本发明一个实施例的 SP 设备的示意性框图。

10 图 8 是本发明另一个实施例的 SP 设备的示意性框图。

图 9 是本发明一个实施例的终端的示意性框图。

图 10 是本发明另一个实施例的终端的示意性框图。

具体实施方式

15 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作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。

应注意，本发明实施例中，终端也可以称为用户设备（User Equipment, UE），包括但不限于具有无线通信功能的设备。例如，终端可以为手持终端、车载设备、可穿戴设备、家用智能设备、传感器等能够使用通信服务的设备。举例来说，可以为蜂窝电话，如智能手机等。

20 本发明实施例中，运营商可以通过服务提供商（Service Provider, SP）设备向用户提供服务。其中，所提供的服务包括但不限于：语音、视频、数据等传统通信服务，车联网、物联网、智能交通、智能家居、医疗监控、传感器网络等未来可能出现的服务。

图 1 是本发明一个实施例的终端认证的方法 100 的示意性流程图。图 1 中示出了第一终端 11、SP 设备 12 和第二终端 14。

30 本发明实施例中，假设第一终端 11 和第二终端 14 由同一用户使用，并且在初始状态均未处于使用状态，即用户既没有使用第一终端 11 接入移动网络，也没有使用第二终端 14 接入移动网络。

S101, 用户在欲使用第一终端 11 接入移动网络, 使用移动网络提供的服务时, 第一终端 11 生成第一认证请求, 请求接入 SP 设备 12。其中, 第一认证请求中包括用户的第一身份凭据。

本发明实施例中, 身份凭据是一种用户的身份的表征。身份凭据可以包括首要 (primary) 凭据和次级 (secondary) 凭据。其中, 首要凭据可以包括如下的至少一种: DNA、指纹、虹膜、声纹等。次级凭据可以包括如下的至少一种: 数字证书、数字签名、用户卡、口令等。并且, 身份凭据可以与其他证明进行身份捆绑认证。其中, 其他证明例如可以为权威机构颁发的证明。举例来说, 权威机构颁发的证明可以是身份证号码或者护照号码等。本发明
5 实施例中, 该其他证明可以作为用户的标识 (Identifier, ID)。

本发明实施例中, 不同的身份凭据可以具有不同的优先级。首要凭据的优先级可以高于次级凭据的优先级。并且, 具体地可以将 DNA 作为最高优先级, 将指纹作为第二优先级, 将虹膜作为第三优先级, 将声纹作为第四优先级, ...将口令作为最低优先级。

这里, DNA 可以通过采集血液或者唾液等确定。指纹可以是多个手指的指纹信息, 或者一个手指的指纹信息, 或者可以是一个手指的部分指纹信息; 并且, 多个手指的指纹的优先级可以高于一个手指的指纹的优先级。虹膜可以是双眼或单眼的虹膜。
15

举例来说, 用户卡可以是 SIM 卡。口令可以是长字符串或短字符串, 或者也可以是在图形上运动的顺序。
20

可理解, 由于不同的终端的硬件差异, 所能够支持输入的用户凭据也会有所不同。例如, 有的终端可以通过摄像头采集用户的虹膜信息; 有的终端可以通过特定区域采集用户的指纹信息; 等等。未来有的终端也可以通过特定的方式收集血液或唾液等进行 DNA 识别。

还可理解, 本发明实施例中, 用户的身份凭据可以是用户基于上述的方法向终端输入的; 也可以是经过运营商授权或者身份认证机构授权后存储在终端中的凭据 (例如客户识别模块 (Subscriber Identity Module, SIM) 卡); 还可以是从已经通过认证的其它终端或已经接入移动网络的其它终端 (例如第三终端, 图 1 中未示出) 获取的。
25

第一终端 11 从第三终端获取身份凭据可以通过向第三终端发送授权请求, 该授权请求用于请求加载用户的身份凭据; 在该授权请求通过时, 接收
30

并加载第三终端发送的用户的身份凭据。第一终端 11 向第三终端发送的授权请求可以包括指纹和/或口令等，第三终端验证通过指纹和/或口令后，将用户的身份凭据发送给第一终端 11。

可理解，第三终端向第一终端 11 发送的用户的身份凭据，可以直接发送，也可以使用特定时间范围内（例如 1 min 内）有效的密钥进行加密。具体而言，该密钥可以是根据用户的 ID 和/或终端的 ID 派生出的密钥。密钥可以在用户的身份凭据发送完毕后立即失效。本发明实施例对此不作限定。

此外，第三终端向第一终端 11 发送用户的身份凭据可以通过多种传输技术，例如可以通过无线保真（WiFi）、蓝牙（Bluetooth）、近距离无线通讯技术（Near Field Communication, NFC）、紫蜂协议（Zigbee）或 USB 1.0、USB 2.0、USB OTG 等有线连接等技术，本发明实施例对此不作限定。

S102，第一终端 11 将生成的包括第一身份凭据的第一认证请求发送至 SP 设备 12，相应地，SP 设备 12 接收第一终端 11 发送的第一认证请求。

具体地，第一认证请求中还可以包括第一终端 11 的标识，一方面便于 SP 设备 12 对身份凭据进行验证后将验证的结果反馈给第一终端 11；另一方面还可以根据第一终端 11 的标识将相应的数据发送给第一终端 11。

S103，SP 设备 12 根据该第一认证请求，确定该用户的标识 ID 和该第一身份凭据的优先级。

可选地，SP 设备 12 可以将第一认证请求发送至身份认证服务器；在身份认证服务器通过第一认证请求时，接收身份认证服务器发送的用户的 ID 和该第一身份凭据的优先级。

可选地，作为一例，身份认证服务器可以是由服务提供者（如运营商）搭建并维护的。也就是说，不同的运营商分别搭建并维护各自的身份认证服务器。

可选地，作为另一例，身份认证服务器可以是用户、运营商之外的第三方搭建的；例如，第三方可以为其他商定的第三方机构。例如，第三方为政府主管部门，也就是说，身份认证服务器可以为政府主管部门进行搭建并维护的。这样，能够保证用户的身份凭据的安全性。

若身份认证服务器是由第三方搭建的，那么，该身份认证服务器可以由至少一个运营商进行访问。这里，为了保证用户的身份凭据的安全性，可以设置运营商访问身份认证服务器的权限。

可选地，SP 设备 12 还可以根据自身预存储的对应关系，确定与该第一身份凭据对应的用户的 ID 和优先级。

例如，SP 设备 12 可以预存储用户 ID 与用户身份凭据以及身份凭据（优先级较低的部分用户凭据）的优先级之间的部分对应关系。

5 这样，SP 设备 12 可以首先判断该 SP 设备 12 上是否有预存储的部分对应关系。如果 SP 设备 12 没有存储部分对应关系，或者，如果 SP 设备 12 无法根据该部分对应关系确定身份凭据的优先级以及用户的 ID，那么，再将第一认证请求发送至身份认证服务器进行认证。如果 SP 设备 12 可以根据该部分对应关系确定身份凭据的优先级以及用户的 ID，那么，SP 设备 12 可
10 以根据该部分对应关系进行认证。这样，能够提高用户进行认证的效率。

可理解，分别对应上述的两个例子，SP 设备 12 或身份认证服务器中存储有用户 ID 与用户身份凭据以及身份凭据的优先级之间的对应关系。

举例来说，如表一所示，假设 SP 设备 12 或身份认证服务器收到的身份凭据为 DNA1，那么，SP 设备 12 或用户认证服务器可以确定对应的标识为
15 ID1，对应的优先级为 P1。即，此时，第一终端 11 的认证通过。

表一

优先级	P1	P2	P3	P4	P5		P9
ID1	DNA1	指纹 1	虹膜 1	声纹 1	证明 1		口令

S104，在认证通过时，第一终端 11 接收 SP 设备 12 通过云服务发送的该用户的上下文数据，并加载该用户的上下文数据。具体地，SP 设备 12 可以在自身的存储器中存储的数据中，根据用户的 ID 为该用户划分一块用于
20 存储上下文数据的空间；或者优选地，运营商可以搭建一个云服务器，用于存储各用户在服务使用过程中产生的上下文数据。在第一终端 11 的认证请求通过时，运营商将用户的上下文数据通过云服务发送给第一终端 11。

可理解，S104 不是必需的，第一终端 11 还可以向已经通过认证的其它终端或已经接入移动网络的其它终端（例如第三终端，图 1 中未示出）发送
25 数据请求，用于请求加载该用户的上下文数据；在该数据请求通过时，接收并加载第三终端发送的该用户的上下文数据。可选地，该数据请求可以通过指纹和/或口令的形式验证。

可理解，第一终端 11 接收第三终端发送的用户的上下文数据，也可以通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议

Zigbee 或 USB 1.0、USB 2.0、USB OTG 等有线连接等技术。

可理解,该用户的上下文数据包括该用户的通讯录、该用户的通话记录、该用户的短信记录、该用户的浏览记录、该用户使用的应用 APP 的数据、该用户的帐号-密码和该用户使用的用户界面中的至少一种。

- 5 可理解,该用户的上下文数据使用特定时间范围内有效的第一密钥进行加密。

这样,即使用户是第一次使用第一终端 11 或者最新更新数据时使用的不是第一终端 11,用户也可以快速地获取自己最新使用其它终端产生的上下文数据,使得用户能够获得完美无缝的使用体验。

- 10 S105, SP 设备 12 根据第一终端 11 的第一认证请求中的第一身份凭据的优先级,为第一终端 11 开启第一服务。

SP 设备 12 中存储有身份凭据的优先级与可用服务之间的对应关系。

具体地,运营商所支持的服务可以分为不同的等级,例如,服务的等级可以根据服务的重要性或者服务的资费等进行划分。

- 15 运营商可以设置不同等级的服务所需的身份凭据。举例来说,运营商可以设置如下规则: 1.用户需要最高优先级的身份凭据(例如, DNA)才可以修改注册时选择的服务; 2.用户需要第二优先级的身份凭据(例如, 指纹)才可以使用国际漫游通话服务。

该规则可以通过身份凭据的优先级与可用服务之间的对应关系来表示。

- 20 并且,运营商可以将该对应关系预先存储在 SP 设备 12 中,这样,在 S105 中, SP 设备 12 可以根据该对应关系确定相应的服务,并为终端 11 开启该相应的服务。

在 S105 之后,用户便可以通过第一终端 11 接入运营商的网络,并且能够使用与第一身份凭据对应的服务。

- 25 S106, 用户还欲使用第二终端 14 接入移动网络,使用移动网络提供的服务。如果第一终端 11 内存储有用户的一个或多个身份凭据(包括用户的第二身份凭据)时,第二终端 14 可以向第一终端 11 发送授权请求,用于请求加载用户的第二身份凭据。

- 30 S107, 第一终端 11 验证第二终端 14 发送的授权请求是否可以通过。当授权请求通过时,第一终端 11 向第二终端 14 发送第二身份凭据。

可理解, S106 和 S107 的具体实现方式已经在 S101 中进行描述,此处

不再进行赘述。而且，S106 和 S107 也不是必需的。第二终端 14 的第二身份凭据也可以是由用户向终端输入的，还可以是原本就存储在终端中的，本发明实施例对此不作限定。

S108, 第二终端 14 将包括第二身份凭据的第二认证请求发送至 SP 设备 12, 相应地, SP 设备 12 接收第二终端 14 发送的第二认证请求。

S109, SP 设备 12 验证第二认证请求, 并确定该用户的标识 ID 和该第二身份凭据的优先级。

S110, 在第二认证请求通过时, 第二终端 14 可以向通过认证的已经接入移动网络的第一终端 11 发送数据请求, 用于请求加载该用户的上下文数据; 在该数据请求通过时, 接收并加载第一终端 11 发送的该用户的上下文数据。可选地该数据请求可以通过指纹和/或口令的形式验证。

可替代 S110 地, 第二终端 14 可以通过云服务从 SP 设备 12 接收该用户的上下文数据。

S111, SP 设备 12 根据第二终端 14 的第二认证请求中的第二身份凭据的优先级, 为第二终端 14 开启第二服务。

在本发明实施例中, 同一个用户身份可以同时使用多个终端 (例如第一终端 11 和第二终端 14), 该多个终端可以是相同类型的, 也可以是不同类型的。例如, 一个用户可以同时使用两个手机, 或者既使用手机的同时使用平板电脑, 其中, 手机和平板电脑使用时均归属于同一个用户 ID。每一个终端内可以存储一个或多个不同等级的身份凭据。不同类型的终端可以存放和使用的最高身份凭据等级不同。例如, 不同类型的终端存放和使用的最高身份凭据等级按“家中固定设备>车载设备>手机>穿戴设备>监控设备>传感器”的顺序递减。

可理解, 同一个用户身份同时使用多个终端时, 可以根据终端的身份凭据的等级、用户偏好和终端能力等因素, 使不同的终端对应不同的服务。

例如, 同一个用户可以同时使用多部手机, 用户可以指定某一部或多部手机用于语音通话服务, 其它手机使用数据服务。其中, 每部手机中都可以存储有用户的身份凭据, 例如手机中可以具有用户身份识别卡等凭据。每部手机可使用的服务可以由用户通过设置身份凭据等级限定的。

再如, 同一个用户可以同时使用手机和平板电脑, 手机可以用于语音通话服务和数据服务, 由于终端能力的限制, 平板电脑则只能用于数据服务。

可理解，当本发明实施例中的终端为低成本的终端（例如传感器）时，其有可能以很大的数量存在于移动网络中。该低成本的终端一般不具备 SIM 卡、指纹识别等成本较高、体积和耗电较大的部件，因其功能较简单，产生的数据一般也不涉及较高级别的用户隐私。因此，该低成本的终端可以不需
5 要频繁进行认证，从而可以用特定的方式进行认证所需要的身份凭证的加载。

可选地，可以在终端出厂时，由制造商为用户定制预加载，即在终端中预加载使用该终端的用户的身份凭证。

可选地，可以在终端与服务提供商签约时，服务提供商向终端提供用户
10 的身份凭证，身份凭证可通过特定编程接口或硬件（例如 IC 卡等）加载。

可选地，可以由用户自行加载授权信息。例如，终端开机后，如终端内不存在（有效的）身份凭证时，或者通过特定操作将终端设置为身份凭证加载模式时，则用户可以进行加载身份凭证。

例如，用户可以通过自有通信网络（如 WLAN）广播发送身份凭证，终端接收后进行存储。用户还可以通过已经存储有身份凭证的其它终端（如手机），以 NFC、蓝牙等短距离无线电技术对不具备身份凭证的终端进行加载。
15 用户还可以使用数据线、存储卡等对不具备身份凭证的终端进行加载。

S112，当用户不想再通过第一终端 11 使用移动网络提供的服务时，用户可以通过第一终端 11 的相关系统或应用向 SP 设备 12 发送解除认证请求，
20 以用于请求 SP 设备 12 停止为第一终端 11 提供第一服务。

S113，SP 设备 12 在停止为该第一终端 11 提供该第一服务时，计算该第一终端 11 使用该第一服务所花费的流量和/或费用，即 SP 设备 12 根据用户的第一服务的使用情况，进行计费。

具体地，不同的服务类型可以采用不同的计费方式，例如，可以按次
25 （session based）计费，可以按时长计费，可以按所使用的网络资源（如流量）计费，可以按使用资源的类型计费等，本发明对此不作限定。

其中，按照使用资源的类型计费可以包括：优先级资源（如紧急通话）费用较高；广播类型的资源计费方式不同于单播（unicast）类型的资源计费方式，等等。

30 可选地，SP 设备 12 可以通过计费控制装置、策略与计费执行功能（Policy and Charging Enforcement Function, PCEF）、策略与计费规则功能（Policy and

Charging Rules Function, PCRF) 等进行计费。

可选地，用户可以在统一计费服务器设置与该用户的 ID 对应的计费账户。其中，用户的 ID 与计费账户一一对应。这样，不同的运营商均可以使用该计费账户，从而能够节省用户开销，减轻了用户缴费的压力，避免了用户由于忘记缴费导致停机带来的麻烦。

具体地，SP 设备 12 可以向该统一计费服务器发送计费请求，该计费请求包括所述 ID，并由所述统一计费服务器从用户的计费账户进行计费。

S114，第一终端 11 被停止使用第一服务，并且可以删除自身存储的用户的上下文数据和/或用户的身份凭据，以保证用户数据的安全。

10 本发明实施例中，运营商将其提供的服务分成不同的等级，并且需要用户使用相应的身份凭据才能使用对应的服务。用户使用终端时可以通过云服务或其它终端加载上下文数据，使用户获得无缝的服务体验。并且，用户可以同时以一个身份使用多个终端接入同一个服务提供商，能够提高用户使用相应的服务的灵活性。

15 图 2 是本发明另一个实施例的终端认证的方法 200 的示意性流程图。图 2 所示的方法由 SP 设备执行，包括：

S201，SP 设备接收第一终端发送的第一认证请求，该第一认证请求包括用户的第一身份凭据。

20 S202，SP 设备根据该第一认证请求，确定该用户的标识 ID 和该第一身份凭据的优先级。

S203，SP 设备通过云服务向该第一终端发送该用户的上下文数据。

S204，SP 设备根据该第一身份凭据的优先级，为该第一终端开启第一服务。

25 本发明实施例中，SP 设备根据终端发送的用户的身份凭据，为终端加载用户的上下文数据，并提供相应的服务。这样能够实现统一安全的身份认证方式，并为用户提供无缝的使用体验，可以提高易用性，并能实现资源的更优利用。

本发明实施例中，用户的第一身份凭据可以包括首要凭据或次级凭据。所述首要凭据的优先级高于所述次级凭据的优先级。

30 其中，所述首要凭据包括如下的至少一种：DNA、指纹、虹膜、声纹。其中，所述次级凭据包括如下的至少一种：数字证书、数字签名、用户卡、

口令。

本发明实施例中，所述第一身份凭据可以是所述第一终端与服务提供商签约时，所述服务提供商向所述第一终端提供的，所述第一身份凭据可通过特定编程接口或硬件加载。

- 5 本发明实施例中，所述第一身份凭据可以是已通过认证的终端向所述第一终端提供的。本发明实施例中，各个不同的身份凭据可以设定优先级顺序，具体地可以参见前述图 1 的实施例中关于优先级的描述，这里不再赘述。

可选地，S202 中，SP 设备可以根据预存储的对应关系，确定与所述第一身份凭据对应的所述 ID 和所述优先级。

- 10 可选地，作为另一个实施例，在 S202 中，SP 设备可以将所述第一认证请求发送至身份认证服务器，并接收所述身份认证服务器发送的所述 ID 和所述第一身份凭据的优先级。

其中，第一认证请求中的第一身份凭据可以是终端采用产生方法处理之后的身份凭据。

- 15 本发明实施例中，所述用户的上下文数据可以包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

- 20 可选地，作为一个实施例，在 S203 中，SP 设备可以使用特定时间范围内有效的密钥对所述用户的上下文数据进行加密；并通过云服务向所述第一终端发送经过加密后的用户的上下文数据。

可选地，作为一个实施例，密钥在用户的上下文数据发送完毕后失效。

- 25 可选地，作为一个实施例，密钥是根据用户的 ID 和/或第一终端的 ID 派生出的密钥。可选地，作为一个实施例，在 S204 中，SP 设备可以确定与所述第一身份凭据的优先级对应的服务，其中，不同的优先级对应的服务不同，且高优先级所对应的服务可以包括低优先级所对应的服务；并为所述第一终端开启与所述第一身份凭据的优先级对应的第一服务。

可理解，SP 设备中可以存储优先级与服务之间的对应关系。具体地，S204 可以参见图 1 的实施例中 S105 的描述，为避免重复，这里不再赘述。

- 30 进一步地，在 S204 之后，方法 200 还包括：

所述 SP 设备接收第二终端发送的第二认证请求，所述第二认证请求包

括用户的第二身份凭据；

所述 SP 设备根据所述第二认证请求，确定所述用户的标识 ID 和所述第二身份凭据的优先级；

所述 SP 设备通过云服务向所述第二终端发送所述用户的上下文数据；

5 所述 SP 设备根据所述第二身份凭据的优先级，为所述第二终端开启第二服务。

具体地，同一个用户可以同时使用多个终端接受同一个 SP 设备的服务。使用过程可以参见图 1 的实施例中 S106 至 S111 的描述，为避免重复，这里不再赘述。可选地，所述第一身份凭据的优先级与所述第二身份凭据的优先级不同，对应地，所述第一服务和所述第二服务不同。

可选地，作为一个实施例，所述方法 200 还可以包括：SP 设备根据所述用户的所述第一服务和所述第二服务的使用情况，进行计费。

具体地，SP 设备可以向统一计费服务器发送计费请求，以便于所述统一计费服务器从所述用户的计费账户进行计费。其中，所述计费请求包括所述 ID，且所述计费账户与所述 ID 一一对应。

这里，计费账户可以是用户预先设置在统一计费服务器中的，并且该计费账户可以由多个运营商的 SP 设备分别进行访问。多个终端分别使用 SP 设备所提供的服务产生的费用可以在同一 ID 对应的计费账户中扣除。

可选地，作为一个实施例，所述方法 200 还可以包括：所述 SP 设备接收所述第一终端发送的解除认证请求，所述解除认证请求用于请求所述 SP 设备停止为所述第一终端提供所述第一服务；所述 SP 设备停止为所述第一终端提供所述第一服务。

具体地，SP 设备在停止为所述第一终端提供所述第一服务时，根据所述用户的所述第一服务的使用情况，进行计费。具体地，解除认证时的处理可以参见图 1 的实施例中 S112 至 S114 的描述，为避免重复，这里不再赘述。

可理解，方法 200 的各步骤可以参见前述图 1 的实施例中相应的步骤的描述，为避免重复，这里不再赘述。

图 3 是本发明另一个实施例的终端认证的方法 300 的示意性流程图。图 3 所示的方法由终端执行，包括：

30 S301，终端生成请求接入服务提供商 SP 设备的认证请求，所述认证请求包括用户的身份凭据。

S302, 终端将所述认证请求发送至所述 SP 设备。

S303, 在所述认证请求通过时, 终端获取并加载所述用户的上下文数据。

S304, 终端使用所述 SP 设备根据所述身份凭据的优先级, 为所述终端提供的对应的服务。

5 本发明实施例中, 终端通过用户的身份凭据, 经由 SP 设备进行身份认证, 并且获取并加载所述用户的上下文数据, 能够由 SP 设备为用户提供相应的服务。这样能够实现统一安全的身份认证方式, 并为用户提供无缝的使用体验, 可以提高易用性, 并能实现资源的更优利用。

10 本发明实施例中, 用户的身份凭据可以包括首要凭据或次级凭据。所述首要凭据的优先级高于所述次级凭据的优先级。

其中, 所述首要凭据包括如下的至少一种: DNA、指纹、虹膜、声纹。其中, 所述次级凭据包括如下的至少一种: 数字证书、数字签名、用户卡、口令。

15 可选地, 作为一个实施例, 用户的身份凭据可以是所述用户向所述终端输入的。

可选地, 作为一个实施例, 用户的身份凭据可以是所述终端与服务提供商签约时, 所述服务提供商向所述终端提供的, 所述身份凭据可通过特定编程接口或硬件加载。

20 可选地, 作为另一个实施例, 用户的身份凭据可以通过以下方式获取的, 向第三终端发送第一授权请求, 所述第一授权请求用于请求加载所述用户的身份凭据; 在所述第一授权请求通过时, 接收并加载所述第三终端发送的所述用户的身份凭据。其中, 终端可以通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接从所述第二终端接收所述身份凭据。

25 此外, 终端内可以存储有所述用户的身份凭据, 所述方法 300 还包括: 所述终端接收第四终端发送的第二授权请求, 所述第二授权请求用于请求加载所述用户的身份凭据; 所述终端验证所述第二授权请求是否通过; 在所述第二授权请求通过时, 所述终端向所述第四终端发送所述用户的身份凭据。

30 在本发明实施例中, 用户的身份凭据可以使用特定时间范围内有效的第二密钥进行加密。

可选地, 作为另一个实施例, 第二密钥在所述用户的身份凭据发送完毕

后失效。

可选地，作为另一个实施例，第二密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。本发明实施例中，各个不同的身份凭据可以设定优先级顺序，具体地可以参见前述图 1 的实施例中关于优先级的描述，这里不再赘述。

可选地，S303 中，终端可以接收所述 SP 设备通过云服务向所述终端发送的所述用户的上下文数据，并加载所述用户的上下文数据。

可选地，作为另一个实施例，在 S303 中，所述终端可以向第一终端发送第一数据请求，所述第一数据请求用于请求加载所述用户的上下文数据；在所述第一数据请求通过时，接收并加载所述第一终端发送的所述用户的上下文数据。

本发明实施例中，用户的上下文数据可以包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

用户的上下文数据可以使用特定时间范围内有效的第一密钥进行加密。其中第一密钥可以在所述用户的上下文数据发送完毕后失效。第一密钥可以是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。其中，终端可以通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接接收所述第一终端发送的所述用户的上下文数据。

在本发明实施例中，终端可以请求解除认证。具体地，终端向所述 SP 设备发送解除认证请求，所述解除认证请求用于请求所述 SP 设备停止为所述终端提供对应的服务；所述终端删除所加载的用户的上下文数据。

可理解，方法 300 的各步骤可以参见前述图 1 的实施例中相应的步骤的描述，为避免重复，这里不再赘述。

下面结合图 4 至图 6，详细介绍图 1 中涉及的第一终端 11 的用户的身份认证的方法。图 4 是本发明一个实施例的用户身份认证的方法的流程图。图 4 中示出了第一终端 11、SP 设备 12 和身份认证服务器 13。

本发明实施例中，假设第一终端 11 在初始状态未处于使用状态，即没有任一用户使用第一终端 11 接入移动网络。或者，可以是该第一终端 11 处于出厂设置的状态，或者可以是第一用户初次使用该第一终端 11。

S401, 在第一用户准备使用第一终端 11 时, 第一终端 11 呈现选择界面, 用于第一用户选择运营商。

例如, 第一终端 11 的界面可以显示第一列表(如图 5 所示为其中一例), 第一列表列出了多个运营商(如图 5 中示出了运营商 A、运营商 B 和运营商 C)。

S402, 第一终端 11 接收第一用户输入的选择信息, 该选择信息指示第一用户所选择的运营商。

具体地, 第一用户可以在 S401 所呈现的选择界面中选择至少一个运营商。

举例来说, 该选择信息可以是第一用户选择图 5 所示的运营商 A, 并点击“确定”按钮。

举例来说, 该选择信息也可以是第一用户选择图 5 所示的运营商 A 和运营商 C, 并点击“确定”按钮。

S403, 第一终端 11 呈现可支持的身份凭据列表。

本发明实施例中, 身份凭据是一种用户的身份的表征。身份凭据可以包括首要(primary)凭据和次级(secondary)凭据。其中, 首要凭据可以包括如下的至少一种: DNA、指纹、虹膜、声纹等。次级凭据可以包括如下的至少一种: 数字证书、数字签名、用户卡、口令等。并且, 身份凭据可以与其他证明进行身份捆绑认证。其中, 其他证明例如可以为权威机构颁发的证明。举例来说, 权威机构颁发的证明可以是身份证号码或者护照号码等。本发明实施例中, 该其他证明可以作为第一用户的标识(Identifier, ID)。

本发明实施例中, 不同的身份凭据可以具有不同的优先级。首要凭据的优先级可以高于次级凭据的优先级。并且, 具体地可以将 DNA 作为最高优先级, 将指纹作为第二优先级, 将虹膜作为第三优先级, 将声纹作为第四优先级, ...将口令作为最低优先级。

这里, DNA 可以通过采集血液或者唾液等确定。指纹可以是多个手指的指纹信息, 或者一个手指的指纹信息, 或者可以是一个手指的部分指纹信息; 并且, 多个手指的指纹的优先级可以高于一个手指的指纹的优先级。虹膜可以是双眼或单眼的虹膜。

举例来说, 用户卡可以是 SIM 卡。口令可以是长字符串或短字符串, 或者也可以是在图形上运动的顺序。

可理解, 由于不同的终端的硬件差异, 所能够支持输入的用户凭据也会有所不同。例如, 有的终端可以通过摄像头采集用户的虹膜信息; 有的终端可以通过特定区域采集用户的指纹信息; 等等。未来有的终端也可以通过特定的方式收集血液或唾液等进行 DNA 识别。

5 因此, S403 中第一终端 11 呈现的用户凭据列表与该第一终端 11 的硬件属性等有关。

应注意, 本发明实施例中, 该步骤 S403 是可选的, 非必须的。例如, 第一终端 11 为该第一用户所有, 其他用户只能在第一用户的同意或授权之后才能使用, 并且第一用户对该第一终端 11 的属性 (和对应的服务) 已经很熟悉, 那么第一用户可以设置该第一终端 11 不再呈现支持的身份凭据列表。

S404, 第一终端 11 接收第一用户输入的身份凭据。

举例来说, 第一用户可以通过第一终端 11 的键盘或者触摸屏输入口令。或者, 第一用户可以通过第一终端 11 的指纹采集模块输入指纹。或者, 第一用户可以通过第一终端 11 的摄像头输入虹膜。或者, 第一用户可以通过麦克输入声纹。等等。

本发明实施例中, 第一终端 11 不限定只由一个用户使用, 即可以有多个用户通过该第一终端 11 接入移动网络。那么, 第一终端 11 可以为不同的用户分配各自独立的存储区域。例如, 第一终端 11 内部可以具有多个物理上或者逻辑上独立的存储区域, 分别用于存储不同用户的信息。

具体地, 第一终端 11 可以为第一用户分配第一存储区域, 用于存储该第一用户的身份凭据。并在通过认证之后, 用于存储第一用户的用户数据 (包括用户界面) 和服务信息等。

S405, 第一终端 11 将第一用户的身份凭据发送至 SP 设备 12。

25 可理解, SP 设备 12 为 S402 中第一用户所选择的运营商的 SP 设备。

举例来说, 如果第一用户在 S402 选择的运营商为运营商 A, 那么 SP 设备 12 即为运营商 A 的 SP 设备。举例来说, 如果第一用户在 S402 选择的运营商为运营商 A 和运营商 B, 那么 SP 设备 12 包括运营商 A 的 SP 设备和运营商 B 的 SP 设备。

30 可选地, 如果第一用户的身份凭据的优先级比较高, 例如为 DNA 或虹膜等, 那么第一终端 11 可以先采用生成方法对第一用户的身份凭据进行处

理, 然后再将处理后的身份凭据发送至 SP 设备 12。也就是说, 第一终端 11 不直接传输 DNA、指纹、虹膜、声纹等用户身份凭据的原始数据, 而是传输经过某种产生方法 (例如使用某种单向映射的算法) 进行处理后的数据。这样, 用户可以保护自己的隐私不被运营商或者其他截获传输数据的第三方 (如黑客) 非法获取。

这里的产生方法可以理解为一种加密的方法。并且, 采用产生方法之后生成的可以为较低优先级的形式。例如, 针对 DNA, 采用生成方法处理后的可以为长度为 30 的字符串。针对指纹, 采用生成方法处理后的可以为长度为 25 的字符串。

10 S406, SP 设备 12 将第一用户的身份凭据发送至身份认证服务器 13。

可选地, 作为一例, 身份认证服务器 13 可以是由服务提供者 (如运营商) 搭建并维护的。也就是说, 不同的运营商分别搭建并维护各自的身份认证服务器。

15 可选地, 作为另一例, 身份认证服务器 13 可以是用户、运营商之外的第三方搭建的; 例如, 第三方可以为其他商定的第三方机构。例如, 第三方可以为政府主管部门, 也就是说, 身份认证服务器 13 可以为政府主管部门进行搭建并维护的。这样, 能够保证用户的身份凭据的安全性。

20 若身份认证服务器 13 是由第三方搭建的, 那么, 该身份认证服务器 13 可以由至少一个运营商进行访问。这里, 为了保证用户的身份凭据的安全性, 可以设置运营商访问身份认证服务器 13 的权限。

25 可选地, 在 S406 中, SP 设备 12 可以将第一用户的身份凭据进行再次处理后发送至身份认证服务器 13, 例如, 可以增加自身的数字签名或加密。这样, 不仅可以向身份认证服务器 13 表明消息的来源, 还可以保证 SP 设备 12 与身份认证服务器 13 之间的安全通信。可理解, SP 设备 12 所使用的数字签名或加密的方法等是 SP 设备 12 与身份认证服务器 13 预先约定的。

30 可理解, 若在 S405 中, SP 设备 12 从第一终端 11 接收到的是采用产生方法处理后的身份凭据, 那么, 在 S406 中, SP 设备 12 也将采用产生方法处理后的身份凭据发送至身份认证服务器 13。或者, 在 S406 中, SP 设备可以将采用产生方法处理后的身份凭据进行再次处理 (增加自身的数字签名或加密) 后再发送至身份认证服务器 13。由于 SP 设备 12 不知道第一终端 11 所采用的产生方法, 或者, 即使 SP 设备 12 知道产生方法却不知道用于加密

的密钥，因此 SP 设备 12 无法进行解密操作，从而 SP 设备 12 无法获取第一用户的优先级较高的身份凭据，这样能够提高身份凭据的安全性。

例如，第一用户输入第一终端 11 的身份凭据为 DNA 特征信息，SP 设备 12 从第一终端 11 获取的处理后的身份凭据为长度为 30 的字符串。相应地，SP 设备 12 将长度为 30 的字符串发送至身份认证服务器 13，或者 SP 设备 12 将长度为 30 的字符串再次处理后发送至身份认证服务器 13。

S407，身份认证服务器 13 根据第一用户的身份凭据，确定与该身份凭据对应的第一用户的标识（Identifier，ID）以及该身份凭据的优先级。

其中，第一用户的 ID 可以为权威机构颁发的证明，例如可以为第一用户的身份证号码或者护照号码等。

本发明实施例中，身份认证服务器 13 中存储有用户的 ID 与用户身份凭据以及身份凭据的优先级之间的对应关系。也就是说，身份凭据与其他证明之间的身份捆绑认证的信息存储在身份认证服务器 13 中。

举例来说，如表一所示，假设身份认证服务器 13 在 S406 中收到的身份凭据为 DNA1，那么，用户认证服务器 13 可以确定对应的标识为 ID1，对应的优先级为 P1。

如果身份认证服务器 13 接收到的处理后的身份凭据（第一终端 11 采用产生方法处理后的身份凭据），那么，在 S407 中，身份认证服务器 13 可以先采用验证方法恢复出身份凭据，然后再确定对应的优先级和用户的 ID。可理解，验证方法为一种解密的方法。并且，SP 设备 12 无法获取该验证方法。

可理解，本发明实施例中，产生方法和验证方法是第一终端 11 与身份认证服务器 13 事先约定的。例如，产生方法可以是第一终端 11 出厂设置所包括的。

可选地，在另一实施例中，如果身份认证服务器 13 接收到的不是 DNA、指纹、声纹、虹膜等身份凭据的原始数据，而是第一终端 11 经产生方法处理后的序列，那么身份认证服务器 13 可以根据经产生方法处理后的特征序列确定用户的 ID 已经身份凭据的优先级。例如，身份认证服务器 13 中也可以存储产生方法。身份认证服务器 13 可以将 DNA、指纹、声纹、虹膜等原始数据采用产生方法生成特征序列。这样，身份认证服务器 13 可以将该特征序列与接收到的序列进行比对，从而能够确定接收到的身份凭据的优先级

以及对应的用户的 ID。

另外，本发明实施例中，身份认证服务器 13 可以从特定部分获取用户的身份凭据，或者，也可以由用户主动上传身份凭据。假设身份认证服务器 13 是由政府主管部门进行搭建并维护的，那么，政府主管部门可以从公安部门获取用户的指纹与身份证号码/护照号码之间的对应关系等，可以从特定的医院获取用户的 DNA 和虹膜特征信息与身份证号码/护照号码之间的对应关系等，可以由用户自己上传用户卡和口令等。

S408，身份认证服务器 13 将身份凭据的优先级和第一用户的 ID 发送至 SP 设备 12。

10 这样，SP 设备 12 可以根据第一用户的 ID 获取用户的注册信息。其中，注册信息也称为签约信息。

可理解，第一用户需要在运营商进行注册之后才可以使用运营商提供的服务。在本发明实施例之前，第一用户已经在运营商进行了签约服务。例如，第一用户可以在签约的时候，选择运营商提供的至少一种服务，并可以设置至少一种服务分别所需的用户凭据。例如，第一用户可以选择或不选择国际漫游服务。第一用户可以与运营商约定国际漫游服务所需的用户凭据为指纹。

S409，SP 设备 12 为第一终端 11 开启相应的服务。

20 SP 设备 12 中存储有身份凭据的优先级与可用服务之间的对应关系。其中，该对应关系也可以理解为签约信息。

例如，该对应关系可以包括：口令对应的服务包括部分通话；用户卡对应的服务包括短信和全部通话；……，指纹对应的服务包括短信、全部通话和一定阈值下的网络流量；……，DNA 对应的服务包括所有可用的服务；等等。这里不再一一罗列。

25 也就是说，用户只有输入了相应的或者更高优先级的身份凭据才能使用对应的服务。如果用户输入的身份凭据的优先级低于服务对应的身份凭据的优先级，那么，第一终端 11 可以拒绝用户使用服务。

具体地，S408 之后，SP 设备 12 可以根据第一用户的 ID 获取第一用户的签约信息，进一步地，可以根据签约信息确定与身份凭据的优先级对应的服务。从而可以在 S409 中为第一用户所使用的第一终端 11 开启对应的服务。

具体地，运营商所支持的服务可以分为不同的等级，例如，服务的等级

可以根据服务的重要性或者服务的资费等进行划分。

运营商可以设置不同等级的服务所需的身份凭据。举例来说，运营商可以设置如下规则：1.用户需要最高优先级的身份凭据（例如，DNA）才可以修改注册时选择的服务；2.用户需要第二优先级的身份凭据（例如，指纹）

5 才可以使用国际漫游通话服务。

该规则可以通过身份凭据的优先级与可用服务之间的对应关系来表示。并且，运营商可以将该对应关系预先存储在 SP 设备 12 中，这样，在 S409 中，SP 设备 12 可以根据该对应关系确定相应的服务，并为第一终端 11 开启该相应的服务。

10 可选地，在 S408 之后，SP 设备 12 也可以将身份凭据的优先级与第一用户的 ID 发送至第一终端 11（图 4 中未示出），这样，第一终端 11 可以将身份凭据，身份凭据的优先级与第一用户的 ID 之间的对应关系进行存储，具体地，可以存储在第一存储区域。

在 S409 之后，第一用户便可以通过第一终端 11 接入运营商的网络，并且能够使用与第一用户输入的身份凭据对应的服务。

可理解，在此过程中，第一用户可以使用 S409 中所开启的服务。如果第一用户想要使用该所开启的服务之外的其他服务，那么，第一终端 11 可以显示拒绝告警或者提示第一用户需要输入高优先级的身份凭据。

20 举例来说，假设第一用户在 S404 中输入的身份凭据为口令，且在 S409 中所开启的服务包括本地通话。如果第一用户想要使用国际漫游通话，那么第一终端 11 可以呈现告警界面，拒绝第一用户的国际漫游通话的服务请求；或者，第一终端 11 可以呈现指示信息界面，指示第一用户需要高优先级的身份凭据“指纹”才可以使用该服务。

25 可选地，作为一个实施例，SP 设备 12 中可以预存储一部分用户凭据的优先级的信息，例如，可以预存储用户 ID 与用户身份凭据（优先级较低的部分用户凭据）以及身份凭据的优先级之间的部分对应关系。

这样，在 S405 之后，SP 设备 12 可以首先判断该 SP 设备 12 上是否有预存储的部分对应关系。如果 SP 设备 12 没有存储部分对应关系，或者，如果 SP 设备 12 无法根据该部分对应关系确定身份凭据的优先级以及用户的 ID，那么，在 S405 之后，继续执行 S406。

如果 SP 设备 12 可以根据该部分对应关系确定身份凭据的优先级以及用

户的 ID, 那么, 在 S405 之后, SP 设备 12 可以根据该部分对应关系进行认证, 且在认证之后直接执行 S409 (即, 无需执行 S406 至 S408)。这样, 能够提高用户进行认证的效率。

本发明实施例中, 假设 SP 设备 12 所在的运营商为运营商 A。在 S409 之后, 第一用户通过第一终端 11 接入到运营商 A 的网络, 并且可以通过第一终端 11 使用运营商 A 提供的服务。

在该过程中, 还可以进一步包括: SP 设备 12 根据第一用户的服务使用情况, 进行计费。具体地, 不同的服务类型可以采用不同的计费方式, 例如, 可以按次 (session based) 计费, 可以按时长计费, 可以按所使用的网络资源 (如流量) 计费, 可以按使用资源的类型计费等, 本发明对此不作限定。

其中, 按照使用资源的类型计费可以包括: 优先级资源 (如紧急通话) 费用较高; 广播类型的资源计费方式不同于单播 (unicast) 类型的资源计费方式, 等等。

可选地, SP 设备 12 可以通过计费控制装置、策略与计费执行功能 (Policy and Charging Enforcement Function, PCEF)、策略与计费规则功能 (Policy and Charging Rules Function, PCRF) 等进行计费。

可选地, 用户可以在统一计费服务器设置与该用户的 ID 对应的计费账户。其中, 用户的 ID 与计费账户一一对应。这样, 不同的运营商均可以使用该计费账户, 从而能够节省用户开销, 减轻了用户缴费的压力, 避免了用户由于忘记缴费导致停机带来的麻烦。

具体地, SP 设备 12 可以向该统一计费服务器发送计费请求, 该计费请求包括所述 ID, 并由所述统一计费服务器从用户的计费账户进行计费。

进一步地, 在该过程中, 如果第一用户想要使用其他运营商的服务 (例如运营商 B), 此时, 在图 4 所示的方法之后还可以包括 (图 4 中未示出):

S410, 第一终端 11 接收第一用户的特定指令, 该特定指令指示需要重新选择运营商。

具体地, 第一用户可以通过第一终端 11 的特定按钮重新选择运营商, 例如, 第一用户可以通过第一终端 11 的特定菜单使得第一终端 11 显示如图 5 所示的界面。即在 S410 之后, 可以执行 S401 和 S402。假设在该 S402 中, 第一用户再次选择的运营商为运营商 B。

举例来说, 假设某种服务 S1 只由运营商 B 提供, 或者第一用户只在与

运营商 B 进行签约时包括服务 S1。则在 S409 之后，若第一用户想要使用服务 S1，第一终端 11 会提示拒绝的告警信息。此时，可以执行 S410，即第一用户可以通过第一终端 11 重新选择运营商。

5 本发明实施例中，在 S409 之后，第一用户在服务使用过程中，可以在第一终端 11 的“服务设置”菜单中设置某些服务所连接的运营商。并且，该信息可以存储在第一终端 11 的第一存储区域中，这样，第一用户可以在后续利用该设置使用某些服务。例如，第一用户可以设置服务 S1 使用的运营商的顺序为：运营商 B、运营商 A、运营商 C。这样，服务 S1 优先使用运营商 B，只有在运营商 B 连接失败（如无信号）时才使用运营商 A，在运营商 B 和运营商 A 都连接失败时才使用运营商 C。例如，第一用户可以设置服务 S2 使用的运营商的顺序为：运营商 A、运营商 C。

可见，第一用户在使用第一终端 11 的过程中，不同的服务可以是不同的运营商所提供的。也就是说，第一用户可以同时使用多个运营商提供的服务。

15 S411，第一终端 11 将第一用户的身份凭据发送至运营商 B 的 SP 设备。

可理解，第一用户的身份凭据是第一终端 11 在 S404 中所获取的，且存储在第一终端 11 的第一存储区域中的。或者，该第一用户的身份凭据可以是第一用户在 S410 之后重新输入的。例如，如果只由运营商 B 提供的服务 S1 所需的身份凭据为 DNA，那么，在 S411 之前，第一用户可以输入 DNA。

20 在此之后，运营商 B 的 SP 设备可以执行与 SP 设备 12 类似的过程，这里不再赘述。

可选地，作为一例，在上述所示的方法之后，还可以包括：第一终端 11 接收第一用户的临时退出指令。该临时退出指令指示第一用户暂时不再使用该第一终端 11，并需临时冻结（suspend）该第一用户的相关信息。随后，25 第一终端 11 可以根据该临时退出指令，将第一用户的用户数据进行冻结。也就是说，该第一用户的用户数据处于不活动状态。其中，用户数据可以包括用户的 profile、用户的应用程序（Application，APP）以及用户的用户界面等。

当后续第一用户需要继续使用第一终端 11 时，第一用户可以输入激活指令。也就是说，第一终端 11 可以接收第一用户的激活指令，并将冻结的30 该第一用户的用户数据激活。具体地，第一终端 11 可以根据激活的用户数

据, 加载该第一用户的 profile, 并呈现第一用户的用户界面。其中, 该用户界面可以呈现第一用户的 APP 信息。

对于第一用户通过临时退出指令冻结的第一终端 11, 第一用户再次使用时, 如图 6 所示, 可以包括如下步骤:

5 S501, 第一终端 11 接收第一用户输入的激活指令。

其中, 该激活指令可以是第一用户的身份凭据, 例如为身份凭据 P1。

S502, 第一终端 11 获取第一用户的 ID 以及身份凭据 P1 的优先级。

可选地, 如果第一终端 11 中存储有第一用户的身份凭据 P1 的信息, 那么, S502 中, 第一终端 11 可以根据存储的信息确定该第一用户的 ID 以及
10 输入的身份凭据 P1 的优先级。

举例来说, 若第一终端 11 的第一存储区域存储有相关的信息, 那么, 第一终端 11 可以自行确定第一用户的 ID 以及输入的身份凭据 P1 的优先级。

可选地, 如果第一终端 11 中没有存储第一用户的身份凭据 P1 的信息(例如第一终端 11 只存储有身份凭据 P2 的信息), 那么, 第一终端 11 在 S501
15 之后可执行 S405 的步骤并从 SP 设备获取该第一用户的 ID 以及身份凭据 P1 的优先级。具体的描述如前所述, 这里不再赘述。

S503, 第一终端 11 根据第一用户的 ID, 获取第一存储区域中的用户信息。

这里, 第一存储区域如前所述, 为第一终端 11 为第一用户分配的独立的
20 的存储区域。

具体的, S503 中, 第一终端 11 呈现第一存储区域所存储的第一用户的用户界面 (User Interface, UI), 并且 UI 可显示第一用户的 APP 等。

S504, 第一用户通过第一终端 11 再次进行数据通信。

另外, 如果第一用户在前述的 S409 之后通过“服务设置”菜单设置了服务所使用的供应商 (或运营商的顺序), 那么, 在 S504 中第一用户可以直接
25 根据先前的设置使用服务。

可选地, 假设第一用户想要使用服务 S2, 而服务 S2 所需的身份凭据为 P2。如果第一用户在 S501 输入的身份凭据 S1 的优先级低于身份凭据 P2 的优先级, 那么, 第一终端 11 可以拒绝第一用户使用服务 S2。或者, 第一终端 11 可以呈现通知消息以便第一用户输入身份凭据 P2。或者, 第一终端 11
30 可以呈现选择界面以使用户决定是否将第一存储区域中所存储的身份凭据

P2 (如果存储的话) 发送至提供服务 S2 的运营商的 SP 设备。本发明对此不作限定。

可选地, 作为另一例, 在上述所示的方法之后 (S409 之后或者 S504 之后), 还可以包括: 第一终端 11 接收第一用户的永久停用指令。随后, 第一终端 11 可以根据该永久停用指令, 删除第一用户的用户数据。也就是说, 第一终端 11 可以根据永久停用指令, 将第一存储区域中的信息全部删除。

可理解, 在此之后, 如果第一用户再次使用该第一终端 11, 其过程与第一用户首次使用该第一终端 11 的流程相同, 这里不再赘述。

举例来说, 如果第一用户在某公共场所 (如图书馆、网吧等地) 使用公共设备, 那么可以在使用之后输入永久停用指令以及时清除个人数据, 这样能够保证用户数据的安全性。

可理解, 在第一用户临时退出或者永久停用该第一终端 11 之后, 另一用户 (例如第二用户) 可以使用该第一终端 11 接入数据通信网络。其中, 第二用户使用该第一终端 11 的过程与第一用户的过程类似, 这里不再赘述。

可选地, 在第一用户使用第一终端 11 的过程中, 第二用户也可以通过类似的方式使用该第一终端 11。并且第一用户的用户数据存储在第一存储区域, 第二用户的用户数据存储在第二存储区域。也就是说, 第一终端 11 可以同时由多个用户使用。

举例来说, 第一终端 11 可以将显示屏 (如触摸屏) 划分为两部分, 分别呈现第一用户的 UI 和第二用户的 UI。第一用户和第二用户分别通过各自的 UI 使用该终端。

举例来说, 第一终端 11 可以将显示屏呈现第一用户的 UI, 第二用户的 UI 在后台运行。第一用户可以通过其 UI 使用该终端, 第二用户可以通过蓝牙使用该终端进行通话等。

应注意, 本发明实施例中, 第一终端 11 可以由多个用户使用, 并且, 多个用户的用户数据分别存储在第一终端 11 中的各自独立的存储区域中。也就是说, 不同用户的用户数据是分别进行存储的, 一般地, 某个用户无法访问其他用户的用户数据。但是, 经过授权的用户数据可以由其他的用户进行访问。

举例来说, 第一用户可以授权将其用户数据中的一部分 (如用户数据块 DATA1) 的权限设置为公开, 这样, 其他的用户可以访问该授权的用户数据

块 DATA1。

举例来说，第一用户可以设置附条件的授权，例如，将用户数据中的一部分（如用户数据块 DATA2）的权限设置为半公开，在设置过程中只允许部分用户（如可以通过限定用户的 ID 的方式）访问该用户数据块 DATA2。

5 这样，只有第一用户所限定的用户可以访问该用户数据块 DATA2。

本发明实施例中，运营商将其提供的服务分成不同的等级，并且需要用户使用相应的身份凭据才能使用对应的服务。这样，用户可以使用身份凭据通过任何可用的终端接入运营商的网络，能够提高用户使用相应的服务的灵活性。

10 图 7 是本发明一个实施例的 SP 设备的示意性框图。图 7 所示的 SP 设备 600 包括接收单元 601、确定单元 602、发送单元 603 和处理单元 604。

接收单元 601，用于接收第一终端发送的第一认证请求，所述第一认证请求包括用户的第一身份凭据；

15 确定单元 602，用于根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级；

发送单元 603，用于通过云服务向所述第一终端发送所述用户的上下文数据；

处理单元 604，用于根据所述第一身份凭据的优先级，为所述第一终端开启第一服务。

20 本发明实施例中，SP 设备根据终端发送的用户的身份凭据，为终端加载用户的上下文数据，并提供相应的服务。这样能够实现统一安全的身份认证方式，并为用户提供无缝的使用体验，可以提高易用性，并能实现资源的更优利用。

25 其中，用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

可选地，作为一个实施例，发送单元 603 具体用于：

使用特定时间范围内有效的密钥对所述用户的上下文数据进行加密；

通过云服务向所述第一终端发送经过加密后的用户的上下文数据。

30 本发明实施例中，密钥可以在所述用户的上下文数据发送完毕后失效。密钥可以是根据所述用户的 ID 和/或所述第一终端的 ID 派生出的密钥。

本发明实施例中，用户的第一身份凭据可以包括首要凭据或次级凭据；其中，所述首要凭据可以包括如下的至少一种：DNA、指纹、虹膜、声纹；

其中，所述次级凭据可以包括如下的至少一种：数字证书、数字签名、

5 用户卡、口令。

其中，首要凭据的优先级高于所述次级凭据的优先级。

并且，第一身份凭据可以是所述第一终端与服务提供商签约时，所述服务提供商向所述第一终端提供的，所述第一身份凭据可通过特定编程接口或硬件加载。第一身份凭据也可以是已通过认证的终端向所述第一终端提供的。此时，第一终端可以为传感器。

可选地，作为一个实施例，接收单元 601 还用于接收第二终端发送的第二认证请求，所述第二认证请求包括用户的第二身份凭据；

确定单元 602 还用于根据所述第二认证请求，确定所述用户的标识 ID 和所述第二身份凭据的优先级；

15 发送单元 603 还用于通过云服务向所述第二终端发送所述用户的上下文数据；

处理单元 604 还用于根据所述第二身份凭据的优先级，为所述第二终端开启第二服务。

其中，所述第一服务和所述第二服务可以不同。

20 本发明实施例中，确定单元 602 具体可以用于：

根据预存储的对应关系，确定与所述第一身份凭据对应的所述 ID 和所述优先级。

或者，确定单元 602 具体可以用于：

将所述第一认证请求发送至身份认证服务器；

25 接收所述身份认证服务器发送的所述 ID 和所述第一身份凭据的优先级。

可选地，作为一个实施例，处理单元 604 还可以用于：

根据所述用户的所述第一服务和所述第二服务的使用情况，进行计费。

可选地，作为一个实施例，所述发送单元 603 还用于：

30 向统一计费服务器发送计费请求，以便于所述统一计费服务器从用户账户进行计费；

其中,所述计费请求包括所述 ID,且所述用户账户与所述 ID 一一对应。

本发明实施例中,第一身份凭据的优先级与所述第二身份凭据的优先级可以不同。

可选地,作为一个实施例,接收单元 601 还用于:

- 5 接收所述第一终端发送的解除认证请求,所述解除认证请求用于请求所述 SP 设备停止为所述第一终端提供所述第一服务;

处理单元 604 还用于:

停止为所述第一终端提供所述第一服务。

可选地,作为一个实施例,处理单元 604 还用于:

- 10 在停止为所述第一终端提供所述第一服务时,根据所述用户的所述第一服务的使用情况,进行计费。

应注意,本发明实施例中,接收单元 601 可以由接收器实现,发送单元 603 可以由发送器实现,确定单元 602 和处理单元 604 可以由处理器实现。

- 15 如图 8 所示,SP 设备 700 可以包括处理器 701、接收器 702、发送器 703 和存储器 704。其中,存储器 704 可以用于存储用户的签约信息,还可以用于存储处理器 701 执行的代码等。

SP 设备 700 中的各个组件通过总线系统 705 耦合在一起,其中总线系统 705 除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。

- 20 图 7 所示的 SP 设备 600 或图 8 所示的 SP 设备 700 能够实现前述图 1 至图 6 的实施例中由 SP 设备所实现的各个过程,为避免重复,这里不再赘述。

- 25 应注意,本发明上述方法实施例可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器 (Digital Signal Processor, DSP)、专用集成电路 (Application Specific Integrated Circuit, ASIC)、现场可编程门阵列 (Field Programmable Gate Array, FPGA) 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。
- 30 通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行

完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

5 可以理解，本发明实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(Read-Only Memory, ROM)、可编程只读存储器(Programmable ROM, PROM)、可擦除可编程只读存储器(Erasable PROM, EPROM)、电可擦除可编程只读存储器(Electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(Random Access Memory, RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(Static RAM, SRAM)、动态随机存取存储器(Dynamic RAM, DRAM)、同步动态随机存取存储器(Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(Double Data Rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(Synchlink DRAM, SLDRAM)和直接内存总线随机存取存储器(Direct Rambus RAM, DR RAM)。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

20 图9是本发明一个实施例的终端的示意性框图。图9所示的终端800包括生成单元801、发送单元802、获取单元803和处理单元804。

生成单元801，用于生成请求接入服务提供商SP设备的认证请求，所述认证请求包括用户的身份凭据；

发送单元802，用于将所述认证请求发送至所述SP设备；

25 获取单元803，用于在所述认证请求通过时，获取并加载所述用户的上下文数据；

处理单元804，用于使用所述SP设备根据所述身份凭据的优先级为所述终端提供的对应的服务。

30 本发明实施例中，终端通过用户的身份凭据，经由SP设备进行身份认证，并且获取并加载所述用户的上下文数据，能够由SP设备为用户提供相应的服务。这样能够实现统一安全的身份认证方式，并为用户提供无缝的使

用体验,可以提高易用性,并能实现资源的更优利用。

其中,用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

- 5 可理解,用户的上下文数据可以使用特定时间范围内有效的第一密钥进行加密。其中,第一密钥可以在所述用户的上下文数据发送完毕后失效。并且,第一密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

本发明实施例中,用户的身份凭据可以包括首要凭据或次级凭据;

- 10 其中,所述首要凭据可以包括如下的至少一种: DNA、指纹、虹膜、声纹;

其中,所述次级凭据可以包括如下的至少一种: 数字证书、数字签名、用户卡、口令。

其中,首要凭据的优先级高于所述次级凭据的优先级。

- 15 并且,用户的身份凭据可以是所述用户向所述终端输入的;用户的身份凭据也可以是是所述终端与服务提供商签约时,所述服务提供商向所述终端提供的,所述身份凭据可通过特定编程接口或硬件加载。用户的身份凭据还可以是已通过认证的终端向所述终端提供的。此时,终端可以为传感器。

可选地,作为一个实施例,获取单元 803 具体用于:

- 20 接收所述 SP 设备通过云服务向所述终端发送的所述用户的上下文数据,并加载所述用户的上下文数据。

可选地,作为一个实施例,发送单元 802 还可以用于:

向第一终端发送第一数据请求,所述第一数据请求用于请求加载所述用户的上下文数据;

获取单元 803 具体可以用于:

- 25 在所述第一数据请求通过时,接收并加载所述第一终端发送的所述用户的上下文数据。

本发明实施例中,获取单元 803 具体可以用于:

通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接接收所述第一终端发送的所述用户的上下文数据。

- 30 本发明实施例中,所述获取单元 803 还可以用于:

接收第二终端发送的第二数据请求,所述第二数据请求用于请求加载所

述用户的上下文数据;

所述处理单元 804 还用于:

验证所述第二数据请求是否通过;

所述发送单元 802 还用于:

- 5 在所述第二数据请求通过时,向所述第二终端发送所述用户的上下文数据。

可选地,作为一个实施例,发送单元 802 还可以用于:

向第三终端发送第一授权请求,所述第一授权请求用于请求加载所述用户的身份凭据;

- 10 所述获取单元 803 还可以用于:

在所述第一授权请求通过时,接收并加载所述第三终端发送的所述用户的身份凭据。

可选地,作为一个实施例,所述终端还包括存储单元,用于存储所述用户的身份凭据,所述获取单元 803 还可以用于:

- 15 接收第四终端发送的第二授权请求,所述第二授权请求用于请求加载所述用户的身份凭据;

所述处理单元 804 还用于:

所述终端验证所述第二授权请求是否通过;

所述发送单元 802 还用于:

- 20 在所述第二授权请求通过时,向所述第四终端发送所述用户的身份凭据。

其中,所述用户的身份凭据可以使用特定时间范围内有效的第二密钥进行加密。所述第二密钥可以在所述用户的身份凭据发送完毕后失效。所述第二密钥可以是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

- 25 可选地,作为一个实施例,所述获取单元 803 具体可以用于:通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接从所述第三终端接收所述身份凭据。

可选地,作为一个实施例,所述发送单元 802 还可以用于:

- 30 向所述 SP 设备发送解除认证请求,所述解除认证请求用于请求所述 SP 设备停止为所述终端提供对应的服务;

所述处理单元 804 还用于:

删除所加载的用户的上下文数据。

应注意，本发明实施例中，获取单元 803 的部分功能可以由接收器实现，发送单元 802 可以由发送器实现，生成单元 801 和处理单元 804 可以由处理器实现。如图 10 所示，终端 900 可以包括处理器 901、接收器 902、发送器 903 和存储器 904。其中，存储器 904 可以用于存储用户信息，还可以用于存储处理器 901 执行的代码等。

具体的，可以是存储器 904 中的一个逻辑存储区域用于存储所述用户信息，包括用户的身份凭据、签约信息、用户界面等。

终端 900 中的各个组件通过总线系统 905 耦合在一起，其中总线系统 905 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。

图 9 所示的终端 800 或图 10 所示的终端 900 能够实现前述图 1 至图 6 的实施例中由终端所实现的各个过程，为避免重复，这里不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

权利要求

1、一种终端认证的方法，其特征在于，包括：

服务提供商 SP 设备接收第一终端发送的第一认证请求，所述第一认证请求包括用户的第一身份凭据；

5 所述 SP 设备根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级；

所述 SP 设备通过云服务向所述第一终端发送所述用户的上下文数据；

所述 SP 设备根据所述第一身份凭据的优先级，为所述第一终端开启第一服务。

10 2、根据权利要求 1 所述的方法，其特征在于，所述用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述通过云服务向
15 所述第一终端发送所述用户的上下文数据，包括：

使用特定时间范围内有效的密钥对所述用户的上下文数据进行加密；

通过云服务向所述第一终端发送经过加密后的用户的上下文数据。

4、根据权利要求 3 所述的方法，其特征在于，所述密钥在所述用户的上下文数据发送完毕后失效。

20 5、根据权利要求 3 或 4 所述的方法，其特征在于，所述密钥是根据所述用户的 ID 和/或所述第一终端的 ID 派生出的密钥。

6、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述第一身份凭据是所述第一终端与服务提供商签约时，所述服务提供商向所述第一终端提供的，所述第一身份凭据可通过特定编程接口或硬件加载。

25 7、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述第一身份凭据是已通过认证的终端向所述第一终端提供的。

8、根据权利要求 6 或 7 所述的方法，其特征在于，所述第一终端为传感器。

9、根据权利要求 1 至 8 中任一项所述的方法，其特征在于，所述方法
30 还包括：

所述 SP 设备接收第二终端发送的第二认证请求，所述第二认证请求包

括用户的第二身份凭据；

所述 SP 设备根据所述第二认证请求，确定所述用户的标识 ID 和所述第二身份凭据的优先级；

所述 SP 设备通过云服务向所述第二终端发送所述用户的上下文数据；

5 所述 SP 设备根据所述第二身份凭据的优先级，为所述第二终端开启第二服务。

10、根据权利要求 9 所述的方法，其特征在于，所述第一服务和所述第二服务不同。

11、根据权利要求 1 至 10 中任一项所述的方法，其特征在于，所述根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级，包括：

根据预存储的对应关系，确定与所述第一身份凭据对应的所述 ID 和所述优先级。

12、根据权利要求 1 至 10 中任一项所述的方法，其特征在于，所述根据所述第一认证请求，确定所述用户的标识 ID 和所述第一身份凭据的优先级，包括：

将所述第一认证请求发送至身份认证服务器；

接收所述身份认证服务器发送的所述 ID 和所述第一身份凭据的优先级。

20 13、根据权利要求 9 或 10 所述的方法，其特征在于，所述方法还包括：所述 SP 设备根据所述用户的所述第一服务和所述第二服务的使用情况，进行计费。

14、根据权利要求 13 所述的方法，其特征在于，所述方法还包括：

25 所述 SP 设备向统一计费服务器发送计费请求，以便于所述统一计费服务器从用户账户进行计费；

其中，所述计费请求包括所述 ID，且所述用户账户与所述 ID 一一对应。

15、根据权利要求 1 至 14 任一项所述的方法，其特征在于，所述用户的第一身份凭据包括首要凭据或次级凭据；

其中，所述首要凭据包括如下的至少一种：DNA、指纹、虹膜、声纹；

30 其中，所述次级凭据包括如下的至少一种：数字证书、数字签名、用户卡、口令。

16、根据权利要求 15 所述的方法，其特征在于，所述首要凭据的优先级高于所述次级凭据的优先级。

17、根据权利要求 9 或 10 所述的方法，其特征在于，所述第一身份凭据的优先级与所述第二身份凭据的优先级不同。

5 18、根据权利要求 1 至 17 任一项所述的方法，其特征在于，所述方法还包括：

所述 SP 设备接收所述第一终端发送的解除认证请求，所述解除认证请求用于请求所述 SP 设备停止为所述第一终端提供所述第一服务；

所述 SP 设备停止为所述第一终端提供所述第一服务。

10 19、根据权利要求 18 所述的方法，其特征在于，所述方法还包括：

所述 SP 设备在停止为所述第一终端提供所述第一服务时，根据所述用户的所述第一服务的使用情况，进行计费。

20、一种终端认证的方法，其特征在于，包括：

15 终端生成请求接入服务提供商 SP 设备的认证请求，所述认证请求包括用户的身份凭据；

所述终端将所述认证请求发送至所述 SP 设备；

在所述认证请求通过时，所述终端获取并加载所述用户的上下文数据；

所述终端使用所述 SP 设备根据所述身份凭据的优先级，为所述终端提供的对应的服务。

20 21、根据权利要求 20 所述的方法，其特征在于，所述用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

25 22、根据权利要求 20 或 21 所述的方法，其特征在于，所述用户的上下文数据使用特定时间范围内有效的第一密钥进行加密。

23、根据权利要求 22 所述的方法，其特征在于，所述第一密钥在所述用户的上下文数据发送完毕后失效。

24、根据权利要求 22 或 23 所述的方法，其特征在于，所述第一密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

30 25、根据权利要求 20 至 24 中任一项所述的方法，其特征在于，所述获取并加载所述用户的上下文数据，包括：

接收所述 SP 设备通过云服务向所述终端发送的所述用户的上下文数据，并加载所述用户的上下文数据。

26、根据权利要求 20 至 24 中任一项所述的方法，其特征在于，所述获取并加载所述用户的上下文数据，包括：

- 5 向第一终端发送第一数据请求，所述第一数据请求用于请求加载所述用户的上下文数据；

在所述第一数据请求通过时，接收并加载所述第一终端发送的所述用户的上下文数据。

- 10 27、根据权利要求 26 所述的方法，其特征在于，所述接收所述第一终端发送的所述用户的上下文数据，包括：

通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接接收所述第一终端发送的所述用户的上下文数据。

28、根据权利要求 20 至 27 中任一项所述的方法，其特征在于，所述方法还包括：

- 15 所述终端接收第二终端发送的第二数据请求，所述第二数据请求用于请求加载所述用户的上下文数据；

所述终端验证所述第二数据请求是否通过；

在所述第二数据请求通过时，所述终端向所述第二终端发送所述用户的上下文数据。

- 20 29、根据权利要求 20 至 28 中任一项所述的方法，其特征在于，所述用户的身份凭据是所述用户向所述终端输入的。

30、根据权利要求 20 至 28 中任一项所述的方法，其特征在于，所述用户的身份凭据是所述终端与服务提供商签约时，所述服务提供商向所述终端提供的，所述身份凭据可通过特定编程接口或硬件加载。

- 25 31、根据权利要求 30 所述的方法，其特征在于，所述终端为传感器。

32、根据权利要求 20 至 31 中任一项所述的方法，其特征在于，所述方法还包括：

向第三终端发送第一授权请求，所述第一授权请求用于请求加载所述用户的身份凭据；

- 30 在所述第一授权请求通过时，接收并加载所述第三终端发送的所述用户的身份凭据。

33、根据权利要求 20 至 32 中任一项所述的方法，其特征在于，所述终端内存储有所述用户的身份凭据，所述方法还包括：

所述终端接收第四终端发送的第二授权请求，所述第二授权请求用于请求加载所述用户的身份凭据；

5 所述终端验证所述第二授权请求是否通过；

在所述第二授权请求通过时，所述终端向所述第四终端发送所述用户的身份凭据。

34、根据权利要求 32 或 33 所述的方法，其特征在于，所述用户的身份凭据使用特定时间范围内有效的第二密钥进行加密。

10 35、根据权利要求 34 所述的方法，其特征在于，所述第二密钥在所述用户的身份凭据发送完毕后失效。

36、根据权利要求 34 或 35 所述的方法，其特征在于，所述第二密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

15 37、根据权利要求 32 所述的方法，其特征在于，所述接收第三终端发送的身份凭据，包括：

通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接从所述第三终端接收所述身份凭据。

38、根据权利要求 20 至 37 中任一项所述的方法，其特征在于，所述用户的身份凭据包括首要凭据或次级凭据；

20 其中，所述首要凭据包括如下的至少一种：DNA、指纹、虹膜、声纹；
其中，所述次级凭据包括如下的至少一种：数字证书、数字签名、用户卡、口令。

39、根据权利要求 38 所述的方法，其特征在于，所述首要凭据的优先级高于所述次级凭据的优先级。

25 40、根据权利要求 20 至 39 任一项所述的方法，其特征在于，所述方法还包括：

所述终端向所述 SP 设备发送解除认证请求，所述解除认证请求用于请求所述 SP 设备停止为所述终端提供对应的服务；

所述终端删除所加载的用户的上下文数据。

30 41、一种服务提供商设备，其特征在于，包括：

接收单元，用于接收第一终端发送的第一认证请求，所述第一认证请求

包括用户的第一身份凭据;

确定单元, 用于根据所述第一认证请求, 确定所述用户的标识 ID 和所述第一身份凭据的优先级;

5 发送单元, 用于通过云服务向所述第一终端发送所述用户的上下文数据;

处理单元, 用于根据所述第一身份凭据的优先级, 为所述第一终端开启第一服务。

42、根据权利要求 41 所述的服务提供商设备, 其特征在于, 所述用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。

43、根据权利要求 41 或 42 所述的服务提供商设备, 其特征在于, 所述发送单元具体用于:

15 使用特定时间范围内有效的密钥对所述用户的上下文数据进行加密;
通过云服务向所述第一终端发送经过加密后的用户的上下文数据。

44、根据权利要求 43 所述的服务提供商设备, 其特征在于, 所述密钥在所述用户的上下文数据发送完毕后失效。

45、根据权利要求 43 或 44 所述的服务提供商设备, 其特征在于, 所述密钥是根据所述用户的 ID 和/或所述第一终端的 ID 派生出的密钥。

20 46、根据权利要求 41 至 45 中任一项所述的服务提供商设备, 其特征在于, 所述第一身份凭据是所述第一终端与服务提供商签约时, 所述服务提供商向所述第一终端提供的, 所述第一身份凭据可通过特定编程接口或硬件加载。

25 47、根据权利要求 41 至 45 中任一项所述的服务提供商设备, 其特征在于, 所述第一身份凭据是已通过认证的终端向所述第一终端提供的。

48、根据权利要求 46 或 47 所述的服务提供商设备, 其特征在于, 所述第一终端为传感器。

49、根据权利要求 41 至 48 中任一项所述的服务提供商设备, 其特征在于:

30 所述接收单元还用于接收第二终端发送的第二认证请求, 所述第二认证请求包括用户的第二身份凭据;

所述确定单元还用于根据所述第二认证请求，确定所述用户的标识 ID 和所述第二身份凭据的优先级；

所述发送单元还用于通过云服务向所述第二终端发送所述用户的上下文数据；

5 所述处理单元还用于根据所述第二身份凭据的优先级，为所述第二终端开启第二服务。

50、根据权利要求 49 所述的服务提供商设备，其特征在于，所述第一服务和所述第二服务不同。

10 51、根据权利要求 41 至 50 中任一项所述的服务提供商设备，其特征在于，所述确定单元具体用于：

根据预存储的对应关系，确定与所述第一身份凭据对应的所述 ID 和所述优先级。

52、根据权利要求 41 至 50 中任一项所述的服务提供商设备，其特征在于，所述确定单元具体用于：

15 将所述第一认证请求发送至身份认证服务器；

接收所述身份认证服务器发送的所述 ID 和所述第一身份凭据的优先级。

53、根据权利要求 49 或 50 所述的服务提供商设备，其特征在于，所述处理单元还用于：

20 根据所述用户的所述第一服务和所述第二服务的使用情况，进行计费。

54、根据权利要求 53 所述的服务提供商设备，其特征在于，所述发送单元还用于：

向统一计费服务器发送计费请求，以便于所述统一计费服务器从用户账户进行计费；

25 其中，所述计费请求包括所述 ID，且所述用户账户与所述 ID 一一对应。

55、根据权利要求 41 至 54 任一项所述的服务提供商设备，其特征在于，所述用户的第一身份凭据包括首要凭据或次级凭据；

其中，所述首要凭据包括如下的至少一种：DNA、指纹、虹膜、声纹；

30 其中，所述次级凭据包括如下的至少一种：数字证书、数字签名、用户卡、口令。

56、根据权利要求 55 所述的服务提供商设备，其特征在于，所述首要

凭据的优先级高于所述次级凭据的优先级。

57、根据权利要求 49 或 50 所述的服务提供商设备，其特征在于，所述第一身份凭据的优先级与所述第二身份凭据的优先级不同。

58、根据权利要求 41 至 57 任一项所述的服务提供商设备，其特征在于，
5 所述接收单元还用于：

接收所述第一终端发送的解除认证请求，所述解除认证请求用于请求所述 SP 设备停止为所述第一终端提供所述第一服务；

所述处理单元还用于：

停止为所述第一终端提供所述第一服务。

10 59、根据权利要求 58 所述的服务提供商设备，其特征在于，所述处理单元还用于：

在停止为所述第一终端提供所述第一服务时，根据所述用户的所述第一服务的使用情况，进行计费。

60、一种终端，其特征在于，包括：

15 生成单元，用于生成请求接入服务提供商 SP 设备的认证请求，所述认证请求包括用户的身份凭据；

发送单元，用于将所述认证请求发送至所述 SP 设备；

获取单元，用于在所述认证请求通过时，获取并加载所述用户的上下文数据；

20 处理单元，用于使用所述 SP 设备根据所述身份凭据的优先级为所述终端提供的对应的服务。

61、根据权利要求 60 所述的终端，其特征在于，所述用户的上下文数据包括所述用户的通讯录、所述用户的通话记录、所述用户的短信记录、所述用户的浏览记录、所述用户使用的应用 APP 的数据、所述用户的帐号-密码和所述用户使用的用户界面中的至少一种。
25

62、根据权利要求 60 或 61 所述的终端，其特征在于，所述用户的上下文数据使用特定时间范围内有效的第一密钥进行加密。

63、根据权利要求 62 所述的终端，其特征在于，所述第一密钥在所述用户的上下文数据发送完毕后失效。

30 64、根据权利要求 62 或 63 所述的终端，其特征在于，所述第一密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

65、根据权利要求 60 至 64 中任一项所述的终端，其特征在于，所述获取单元具体用于：

接收所述 SP 设备通过云服务向所述终端发送的所述用户的上下文数据，并加载所述用户的上下文数据。

5 66、根据权利要求 60 至 64 中任一项所述的终端，其特征在于，所述发送单元还用于：

向第一终端发送第一数据请求，所述第一数据请求用于请求加载所述用户的上下文数据；

所述获取单元具体用于：

10 在所述第一数据请求通过时，接收并加载所述第一终端发送的所述用户的上下文数据。

67、根据权利要求 66 所述的终端，其特征在于，所述获取单元具体用于：

15 通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接接收所述第一终端发送的所述用户的上下文数据。

68、根据权利要求 60 至 67 中任一项所述的终端，其特征在于，所述获取单元还用于：

接收第二终端发送的第二数据请求，所述第二数据请求用于请求加载所述用户的上下文数据；

20 所述处理单元还用于：

验证所述第二数据请求是否通过；

所述发送单元还用于：

在所述第二数据请求通过时，向所述第二终端发送所述用户的上下文数据。

25 69、根据权利要求 60 至 68 中任一项所述的终端，其特征在于，所述用户的身份凭据是所述用户向所述终端输入的。

70、根据权利要求 60 至 68 中任一项所述的终端，其特征在于，所述用户的身份凭据是所述终端与服务提供商签约时，所述服务提供商向所述终端提供的，所述身份凭据可通过特定编程接口或硬件加载。

30 71、根据权利要求 70 所述的终端，其特征在于，所述终端为传感器。

72、根据权利要求 60 至 71 中任一项所述的终端，其特征在于，所述发

送单元还用于：

向第三终端发送第一授权请求，所述第一授权请求用于请求加载所述用户的身份凭据；

所述获取单元还用于：

- 5 在所述第一授权请求通过时，接收并加载所述第三终端发送的所述用户的身份凭据。

73、根据权利要求 60 至 72 中任一项所述的终端，其特征在于，所述终端还包括存储单元，用于存储所述用户的身份凭据，所述获取单元还用于：

- 10 接收第四终端发送的第二授权请求，所述第二授权请求用于请求加载所述用户的身份凭据；

所述处理单元还用于：

所述终端验证所述第二授权请求是否通过；

所述发送单元还用于：

- 15 在所述第二授权请求通过时，向所述第四终端发送所述用户的身份凭据。

74、根据权利要求 72 或 73 所述的终端，其特征在于，所述用户的身份凭据使用特定时间范围内有效的第二密钥进行加密。

75、根据权利要求 74 所述的终端，其特征在于，所述第二密钥在所述用户的身份凭据发送完毕后失效。

- 20 76、根据权利要求 74 或 75 所述的终端，其特征在于，所述第二密钥是根据所述用户的 ID 和/或所述终端的 ID 派生出的密钥。

77、根据权利要求 72 所述的终端，其特征在于，所述获取单元具体用于：

- 25 通过无线保真 WiFi、蓝牙 Bluetooth、近距离无线通讯技术 NFC、紫蜂协议 Zigbee 或有线连接从所述第三终端接收所述身份凭据。

78、根据权利要求 60 至 77 中任一项所述的终端，其特征在于，所述用户的身份凭据包括首要凭据或次级凭据；

其中，所述首要凭据包括如下的至少一种：DNA、指纹、虹膜、声纹；

- 30 其中，所述次级凭据包括如下的至少一种：数字证书、数字签名、用户卡、口令。

79、根据权利要求 78 所述的终端，其特征在于，所述首要凭据的优先

级高于所述次级凭据的优先级。

80、根据权利要求 60 至 79 任一项所述的终端，其特征在于，所述发送单元还用于：

- 向所述 SP 设备发送解除认证请求，所述解除认证请求用于请求所述 SP
- 5 设备停止为所述终端提供对应的服务；
- 所述处理单元还用于：
- 删除所加载的用户的上下文数据。

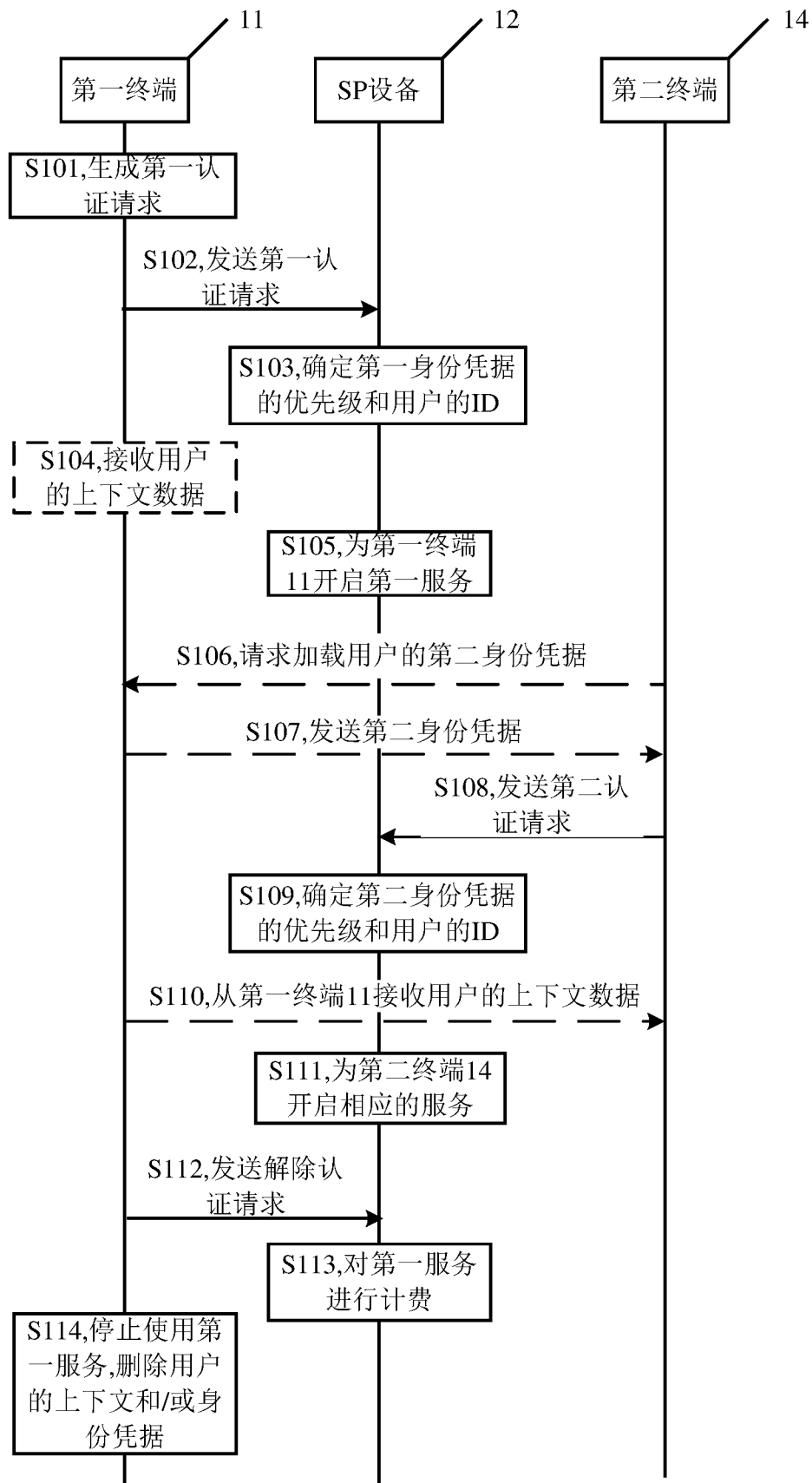


图1

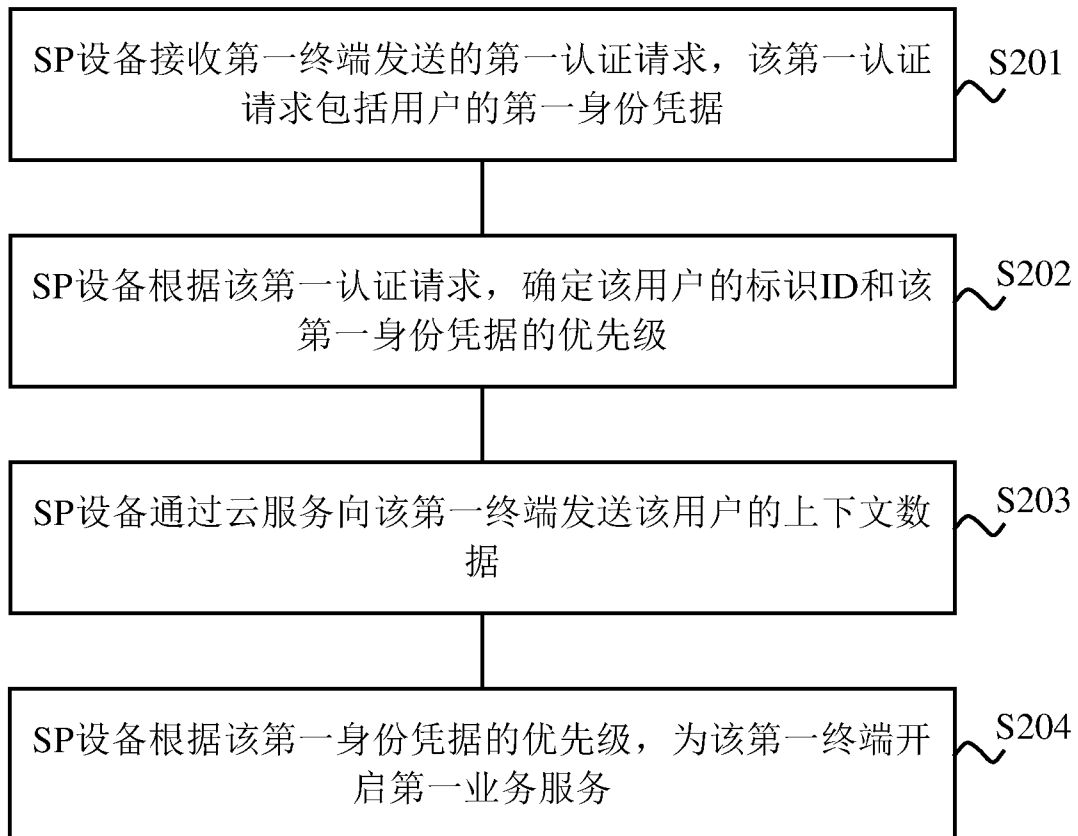


图2

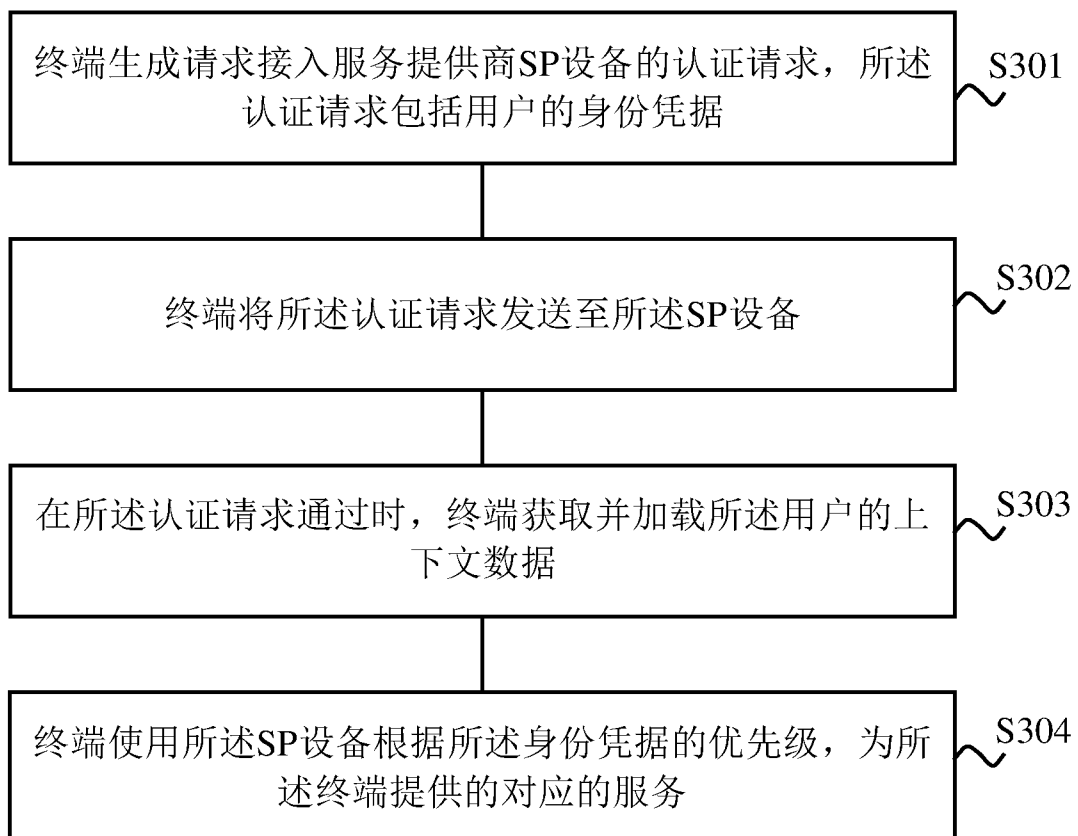


图3

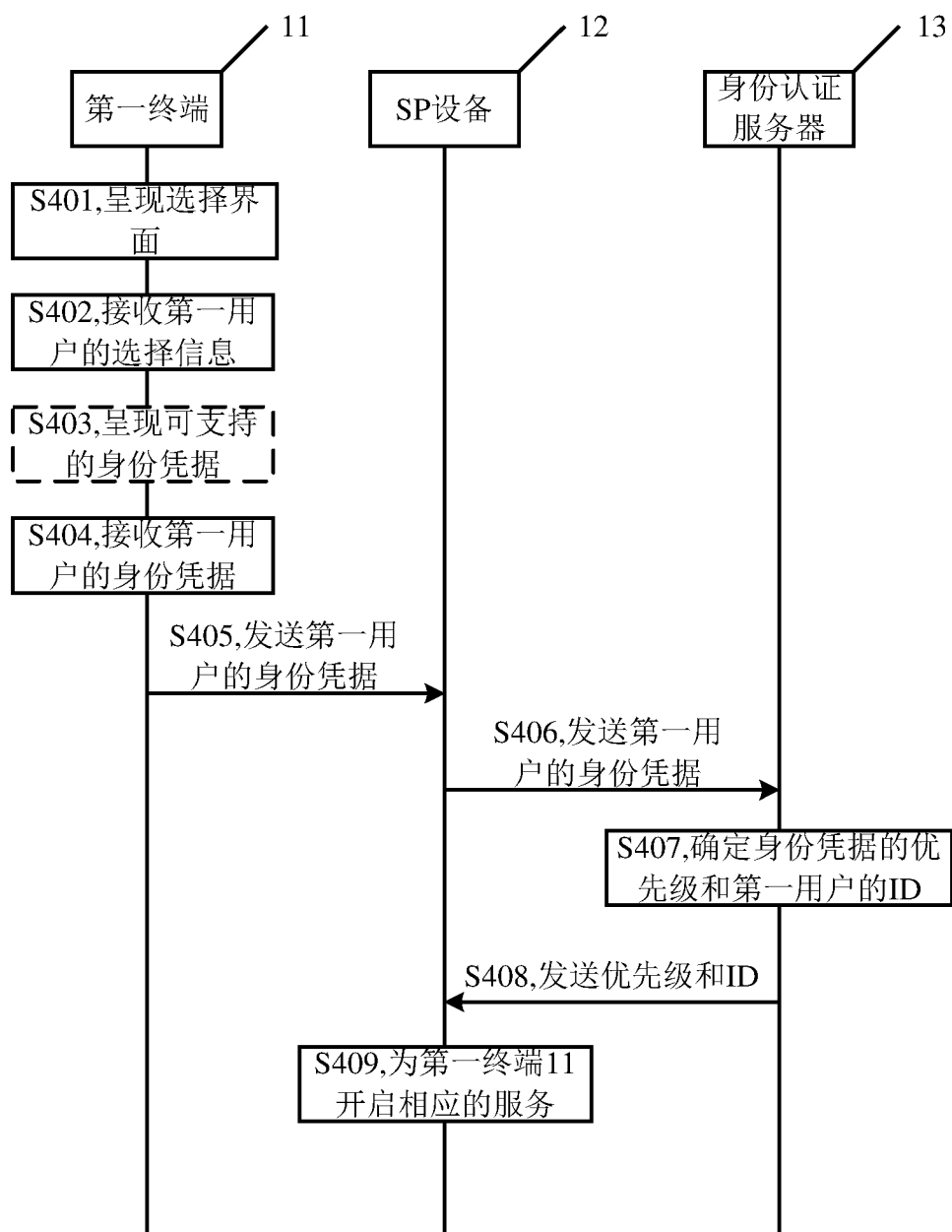


图4

请选择要接入的运营商

☐ 运营商A

☐ 运营商B

☐ 运营商C

图5

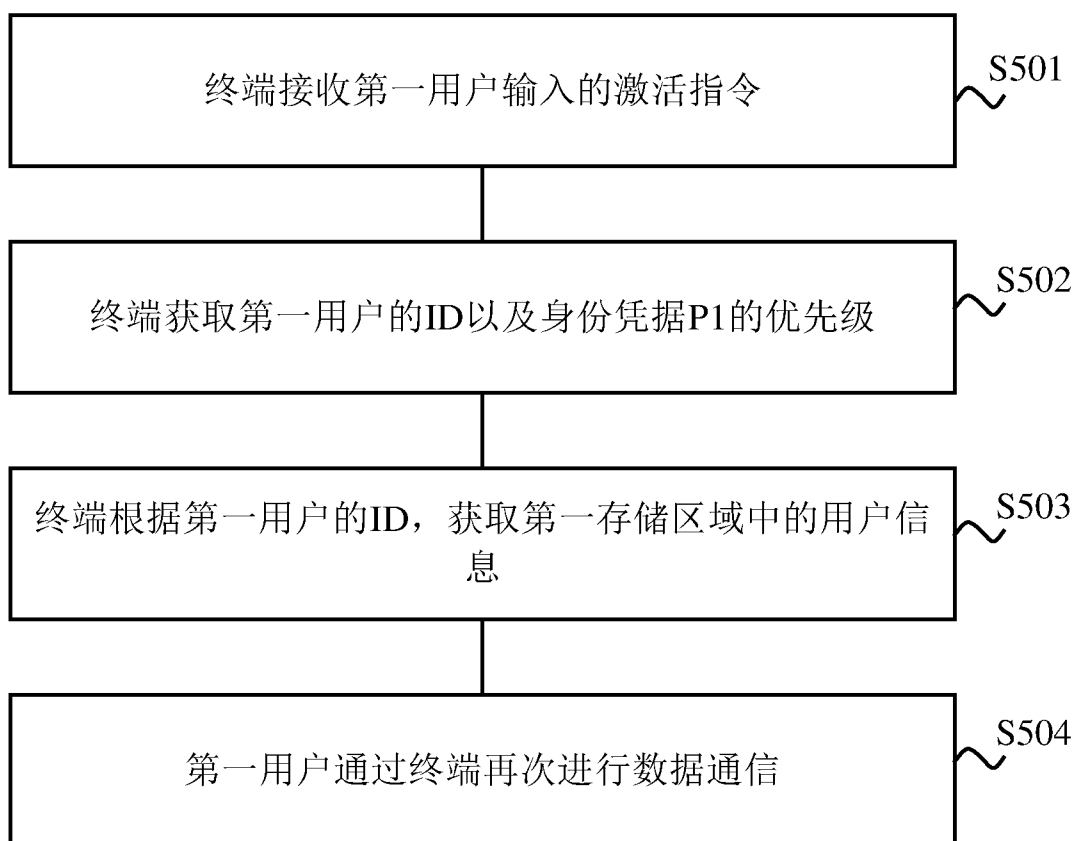


图6

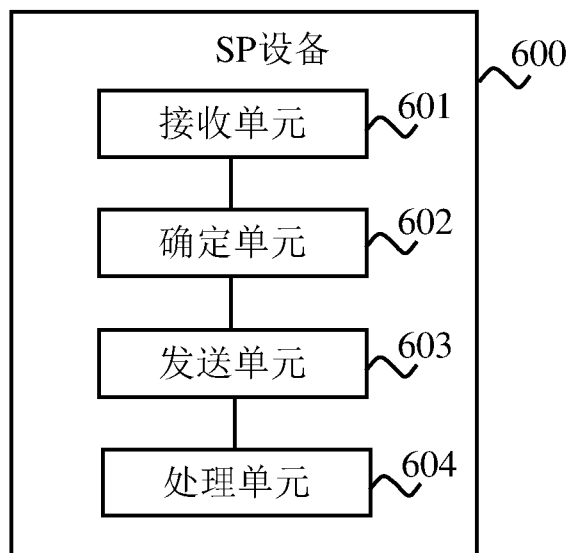


图7

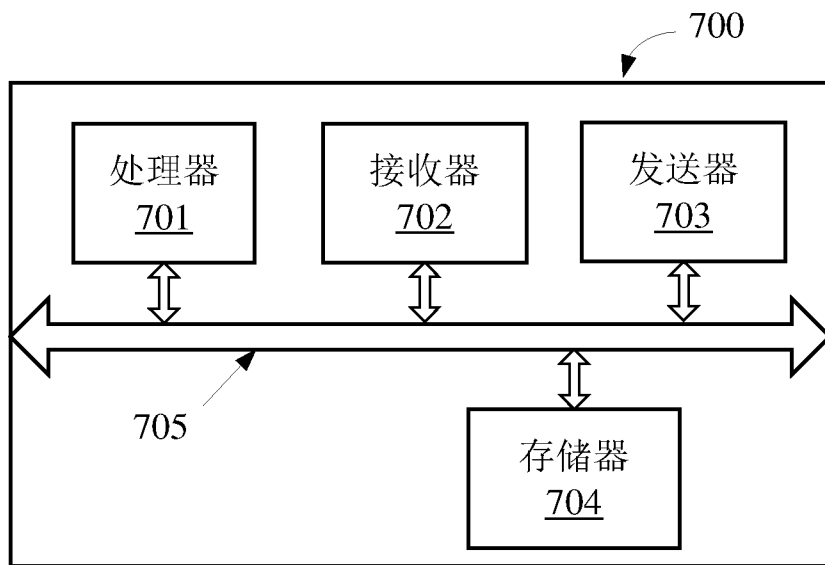


图8

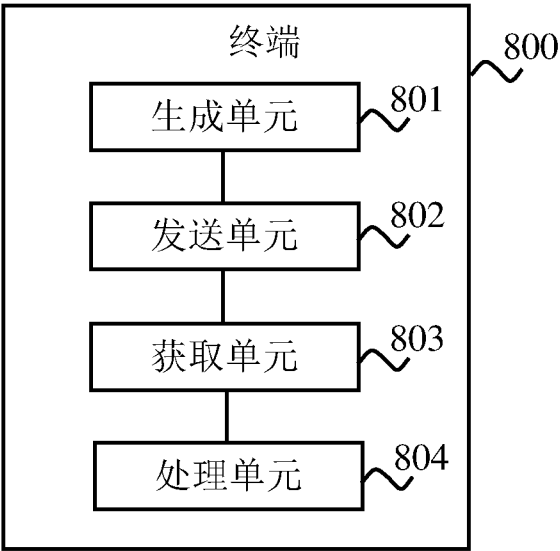


图9

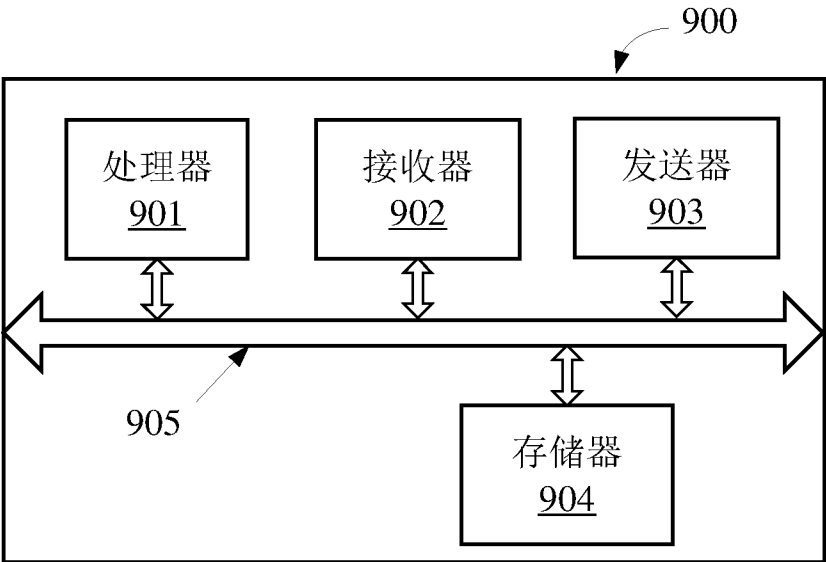


图10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/090752

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i; H04W 12/04 (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

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: mobile phone, key, encryption, cloud service, priority, credential, identity, context, identification, SIM, identify+, terminal, auth+, access, certify, code, password, fingerprint, mobile, communicate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104469765 A (BEIJING BAICELLS TECHNOLOGIES CO., LTD.), 25 March 2015 (25.03.2015), claims 1-16, and description, pages 6-10	1-80
X	CN 104469766 A (BEIJING BAICELLS TECHNOLOGIES CO., LTD.), 25 March 2015 (25.03.2015), claims 1-18, and description, pages 6-10	1-80
A	EP 2854433 A1 (ZTE CORP.), 01 April 2015 (01.04.2015), the whole document	1-80
A	CN 102149170 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 10 August 2011 (10.08.2011), the whole document	1-80

☐ 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 31 May 2016 (31.05.2016)	Date of mailing of the international search report 22 June 2016 (22.06.2016)
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) 62019451	Authorized officer LI, Kai Telephone No.: (86-10) 62413120

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/090752

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104469765 A	25 March 2015	WO 2016015509 A1	04 February 2016
CN 104469766 A	25 March 2015	WO 2016015510 A1	04 February 2016
EP 2854433 A1	01 April 2015	CN 103428696 A	04 December 2013
		US 2015172922 A1	18 June 2015
		WO 2013174185 A1	28 November 2013
CN 102149170 A	10 August 2011	None	

国际检索报告

国际申请号

PCT/CN2015/090752

A. 主题的分类

H04W 12/06(2009.01)i; H04W 12/04(2009.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W; H04Q

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, WPI, EPODOC: 终端, 手机, 认证, 鉴权, 接入, 授权, 密码, 密钥, 加密, 口令, 云服务, 优先级, 凭据, 身份, 上下文, 标识, SIM, identify+, terminal, auth+, access, certify, code, password, fingerprint, mobile, communicate

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 104469765 A (北京佰才邦技术有限公司) 2015年 3月 25日 (2015 - 03 - 25) 权利要求1-16, 说明书第6-10页	1-80
X	CN 104469766 A (北京佰才邦技术有限公司) 2015年 3月 25日 (2015 - 03 - 25) 权利要求1-18, 说明书第6-10页	1-80
A	EP 2854433 A1 (ZTE CORP.) 2015年 4月 1日 (2015 - 04 - 01) 全文	1-80
A	CN 102149170 A (宇龙计算机通信科技深圳有限公司) 2011年 8月 10日 (2011 - 08 - 10) 全文	1-80

☐ 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

2016年 5月 31日

国际检索报告邮寄日期

2016年 6月 22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

授权官员

李凯

传真号 (86-10) 62019451

电话号码 (86-10) 62413120

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/090752

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	104469765	A	2015年 3月 25日	WO	2016015509	A1	2016年 2月 4日
CN	104469766	A	2015年 3月 25日	WO	2016015510	A1	2016年 2月 4日
EP	2854433	A1	2015年 4月 1日	CN	103428696	A	2013年 12月 4日
				US	2015172922	A1	2015年 6月 18日
				WO	2013174185	A1	2013年 11月 28日
CN	102149170	A	2011年 8月 10日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)