

(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 12 月 20 日 (20.12.2018)

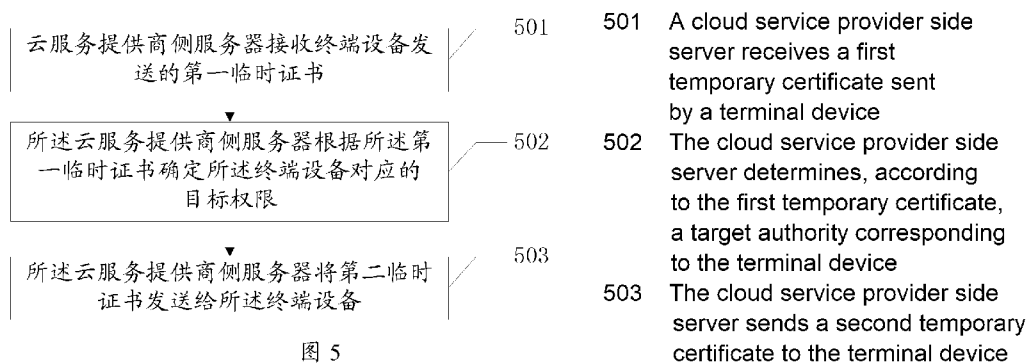
WIPO | PCT

(10) 国际公布号
WO 2018/228199 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01) H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2018/089039
- (22) 国际申请日: 2018 年 5 月 30 日 (30.05.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201710447707.0 2017年6月14日 (14.06.2017) CN
- (71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。
- (72) 发明人: 袁哲 (YUAN, Zhe); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。
- (74) 代理人: 深圳市深佳知识产权代理事务所(普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市国贸大厦 15 楼西座 1521 室, Guangdong 518014 (CN)。
- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,

(54) Title: AUTHORIZATION METHOD AND RELATED DEVICE

(54) 发明名称: 一种授权方法以及相关设备



(57) Abstract: Disclosed are an authorization method and a related device. The method in the embodiments of the present application comprises: a server receiving a first temporary certificate sent by a terminal device; the server determining a target authority according to the first temporary certificate; and the server sending a second temporary certificate to the terminal device, wherein the second temporary certificate is used to indicate the target authority, such that the terminal device accesses the target resource on the server by means of the second temporary certificate. It can be seen that the server can implement the refined authority management of the terminal device by means of the second temporary certificate, that is, the terminal device only has access to a target authority for the server, thereby guaranteeing the security and flexibility of the terminal device accessing the target resource on the server.

(57) 摘要: 本申请实施例公开了一种授权方法以及相关设备。本申请实施例方法包括: 服务器接收终端设备发送的第一临时证书, 所述服务器根据所述第一临时证书确定目标权限, 所述服务器将第二临时证书发送给所述终端设备, 所述第二临时证书用于指示所述目标权限, 以使所述终端设备通过所述第二临时证书访问所述服务器上的所述目标资源。可见, 所述服务器可通过所述第二临时证书实现对所述终端设备进行精细化的权限管理, 即使得所述终端设备对所述服务器仅具有目标权限的访问, 同时保证了终端设备访问所述服务器的目标资源的安全性和灵活性。

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))。

一种授权方法以及相关设备

本申请要求于 2017 年 06 月 14 日提交中国专利局、申请号为 2017104477070、发明名称为“一种授权方法以及相关设备”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。

5 技术领域

本申请涉及通信技术领域，尤其涉及的是一种授权方法以及相关设备。

背景技术

终端设备在访问资源时，需要资源拥有者的授权，终端设备在资源拥有者的授权下，即可进行资源的访问。

10 一般情况下，终端设备要访问资源时，会先向资源所有者发送请求消息，资源所有者将授权码发送给终端设备，终端设备通过该授权码向授权服务器请求访问令牌，授权服务器对终端设备进行验证，验证通过后向终端设备返回访问令牌，终端设备通过该访问令牌访问资源所有者上的资源，具体流程如图 1 所示。

15 上述方案中，所述资源所有者对所述终端设备的授权过程为实时授权，无法对终端设备定义精细化的权限需求，一般是把权限分成粗粒度的些类别，这种方式是无法满足云服务的精细化权限管理需求，而且以访问令牌来作为授权后访问资源的凭证，安全性较低。

发明内容

20 本申请实施例提供了一种授权方法以及相关设备。

本申请第一方面提供了一种授权方法，包括：

服务器接收终端设备发送的第一临时证书，所述第一临时证书用于请求访问所述服务器上的资源；

所述服务器根据所述第一临时证书确定所述终端对应的目标权限，所述目
25 标权限为访问所述服务器上的目标资源的权限；

所述服务器将第二临时证书发送给所述终端设备,以使所述终端设备通过所述第二临时证书访问所述目标资源。

本申请第二方面提供了一种授权方法,包括:

5 终端设备将第一临时证书发送给服务器,所述第一临时证书用于请求访问所述服务器上的资源,以使得所述服务器根据所述第一临时证书确定所述终端设备对应的目标权限,所述目标权限为访问所述服务器上的目标资源的权限;所述服务器为云服务提供商侧的服务器,所述终端设备为第三方服务商侧的服务器;

10 所述终端设备接收所述服务器发送的所述目标权限对应的第二临时证书;所述终端设备通过所述第二临时证书访问所述目标资源。

本申请第三方面提供了一种服务器,包括:

接收单元,用于接收终端设备发送的第一临时证书,所述第一临时证书用于请求访问所述服务器上的资源;

15 确定单元,用于根据所述第一临时证书确定所述终端设备对应的目标权限,所述目标权限为访问所述服务器上的目标资源的权限;

发送单元,用于将所述目标权限对应的第二临时证书发送给所述终端设备,以使所述终端设备通过所述第二临时证书访问所述目标资源。

本申请第四方面提供了一种终端设备,包括:

20 发送单元,用于将第一临时证书发送给服务器,所述第一临时证书用于请求访问所述服务器上的资源,以使得所述服务器根据所述第一临时证书确定所述终端设备对应的目标权限,所述目标权限为访问所述服务器上的目标资源的权限;

接收单元,用于接收所述服务器发送的所述目标权限对应的第二临时证书;

25 访问单元,用于通过所述第二临时证书访问所述目标资源。

本申请第五方面提供了一种服务器，包括：

一个或多个中央处理器、存储器、总线系统、以及一个或多个程序，所述中央处理器和所述存储器通过所述总线系统相连；

其中所述一个或多个程序被存储在所述存储器中，所述一个或多个程序包括指令，所述指令当被所述服务器执行时使所述服务器执行如本申请第一方面所提供的所述的授权方法。

本申请第六方面提供了一种终端设备，包括：

一个或多个处理器单元、存储单元、总线系统、以及一个或多个程序，所述处理器单元和所述存储单元通过所述总线系统相连；

其中所述一个或多个程序被存储在所述存储单元中，所述一个或多个程序包括指令，所述指令当被所述终端设备执行时使所述终端设备执行如本申请第二方面所示的所述的授权方法。

本申请第七方面提供了一种计算机存储介质，包括指令，当其在计算机上运行时，使得计算机执行如本申请第一方面所述的方法。

本申请第七方面提供了一种计算机存储介质，包括指令，当其在计算机上运行时，使得计算机执行如本申请第二方面所述的方法。

从以上技术方案可以看出，本申请实施例具有以下优点：

所述服务器可通过所述第二临时证书实现对所述终端设备进行精细化的权限管理，即使得所述终端设备对所述服务器仅具有目标权项的访问，同时保证了终端设备访问所述服务器的目标资源的安全性和灵活性。

附图说明

图1为一种授权方法的步骤流程示意图；

图2为本申请所提供的云服务系统的结构的一种实施例结构示意图；

图3为本申请所提供的云服务提供商侧服务器的一种实施例结构示意图；

图4为本申请所提供的终端设备的一种实施例结构示意图；

图5为本申请所提供的授权方法的一种实施例步骤流程图；

图6为本申请所提供的授权方法的另一种实施例步骤流程图；

图7为本申请所提供的授权方法的另一种实施例步骤流程图；

图8为本申请所提供的预选权限的创建示意图；

5 图9为本申请所提供的云服务提供商侧服务器另一种实施例结构示意图；

图10为本申请所提供的终端设备的另一种实施例结构示意图；

图11为本申请所提供的应用场景的一种示例图。

具体实施方式

本申请实施例提供了一种授权方法，用于对终端设备进行精细化的权限管
10 理。应理解，本申请实施例中的服务器具体可以是云服务提供商侧服务器，还
可以是其他类型的服务器，具体本申请不作限定，下面实施例将以云服务提供
商侧服务器为例对本申请实施例中的授权方法和相关设备进行介绍。

应理解，本实施例所示的授权方法可以基于云服务系统，本实施例所示的
云服务系统的结构可参见图2所示，其中，所述云服务系统包括云服务提供商
15 侧服务器201。且本实施例所示的云服务提供商侧服务器为云服务提供商的服
务平台侧的服务器。

本实施例所示的所述云服务系统还包括至少一个终端设备202，本实施例
以所述终端设备202的数目为一个为例进行示例性说明。

本实施例所示的终端设备202为第三方服务商侧的设备。

20 其中，所述第三方服务商为入驻云服务提供商建立的以云计算产品为基础
的服务平台，提供给云服务开发者的软件、服务、建站、企业应用服务，以帮
助用户更好的使用云计算产品和服务。

本实施例所示的所述云服务提供商侧服务器可为资源所有者（Resource
Owner，RO），或所述云服务提供商侧服务器可为资源服务器（Resource
25 Server），或所述云服务提供商侧服务器可为授权服务器（Authorization Server，

AS)。

本实施例中，所述终端设备 202 即可通过 OAUTH 协议向所述云服务提供商侧服务器请求授权。

以下结合图 3 所示对所述云服务提供商侧服务器 201 的结构进行可选的说明，具体的，本实施例对所述云服务提供商侧服务器结构的说明为可选的示例，不做限定，只要所述云服务提供商侧服务器 201 能够实现对所述终端设备 202 的授权，以使所述终端设备 202 能够根据授权访问所述云服务提供商侧服务器 201 上的资源即可。

所述云服务提供商侧服务器可因配置或性能不同而产生比较大的差异，可以包括一个或一个以上中央处理器 (central processing units, CPU) 301 (例如，一个或一个以上处理器) 和存储器 302，一个或一个以上存储应用程序 303 或数据 304 的存储介质 305 (例如一个或一个以上海量存储设备)。其中，存储器 302 和存储介质 305 可以是短暂存储或持久存储。存储在存储介质 305 的程序可以包括一个或一个以上模块 (图示没标出)，每个模块可以包括对服务器中的一系列指令操作。更进一步地，中央处理器 301 可以设置为与存储介质 305 通信，在云服务提供商侧服务器上执行存储介质 305 中的一系列指令操作。

云服务提供商侧服务器还可以包括一个或一个以上电源 306，一个或一个以上有线或无线网络接口 307，一个或一个以上输入输出接口 308，和/或，一个或一个以上操作系统 309，例如 Windows Server™，Mac OS X™，Unix™，Linux™，FreeBSD™ 等等。

以下结合图 4 所示对本实施例所示的终端设备 202 的具体结构进行示例性说明。

所述终端设备包括输入单元 405、处理器单元 403、输出单元 401、通信单元 407、存储单元 404、射频电路 408 等组件。

这些组件通过一条或多条总线进行通信。本领域技术人员可以理解，图 4

中示出的终端设备的结构并不构成对本申请的限定，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。

在本申请实施方式中，所述终端设备可以是任何移动或便携式电子设备，
5 包括但不限于智能手机、移动电脑、平板电脑、个人数字助理 (Personal Digital Assistant, PDA)、媒体播放器、智能电视等。

所述终端设备包括：

输出单元 401，用于输出待显示的图像。

具体的，所述输出单元 401 包括但不限于影像输出单元 4011 和声音输出
10 单元 4012。

所述影像输出单元 4011 用于输出文字、图片和/或视频。所述影像输出单元 4011 可包括显示面板，例如采用液晶显示器 (英文全称：Liquid Crystal Display, 英文简称：LCD)、有机发光二极管 (英文全称：Organic Light-Emitting Diode, 英文简称：OLED)、场发射显示器 (英文全称：field emission display, 英文简称 FED) 等形式来配置的显示面板。或者所述影像输出单元 4011 可以包
15 括反射式显示器，例如电泳式 (electrophoretic) 显示器，或利用光干涉调变技术 (英文全称：Interferometric Modulation of Light) 的显示器。

所述影像输出单元 4011 可以包括单个显示器或不同尺寸的多个显示器。
在本申请的具体实施方式中，触摸屏亦可同时作为输出单元 401 的显示面板。

20 例如，当触摸屏检测到在其上的触摸或接近的手势操作后，传送给处理器单元 403 以确定触摸事件的类型，随后处理器单元 403 根据触摸事件的类型在显示面板上提供相应的视觉输出。虽然在图 4 中，输入单元 405 与输出单元 401 是作为两个独立的部件来实现终端设备的输入和输出功能，但是在某些实施例中，可以将触摸屏与显示面板集成一体而实现终端设备的输入和输出功
25 能。例如，所述影像输出单元 4011 可以显示各种图形化用户接口 (英文全称：

Graphical User Interface, 英文简称 GUI)以作为虚拟控制组件, 包括但不限于窗口、滚动轴、图标及剪贴簿, 以供用户通过触控方式进行操作。

在本申请具体实施方式中, 所述影像输出单元 4011 包括滤波器及放大器, 用来将处理器单元 403 所输出的视频滤波及放大。声音输出单元 4012 包括数字模拟转换器, 用来将处理器单元 403 所输出的音频信号从数字格式转换为模拟格式。

处理器单元 403, 用于运行相应的代码, 对接收信息进行处理, 以生成并输出相应的界面。

具体的, 所述处理器单元 403 为终端设备的控制中心, 利用各种接口和线路连接整个终端设备的各个部分, 通过运行或执行存储在存储单元内的软件程序和/或模块, 以及调用存储在存储单元内的数据, 以执行终端设备的各种功能和/或处理数据。所述处理器单元 403 可以由集成电路(英文全称: Integrated Circuit, 英文简称: 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, 所述处理器单元 403 可以仅包括中央处理器(英文全称: Central Processing Unit, 英文简称: CPU), 也可以是图形处理器(英文全称: Graphics Processing Unit, 英文简称: GPU), 数字信号处理器(英文全称: Digital Signal Processor, 英文简称: DSP)、及通信单元中的控制芯片(例如基带芯片)的组合。在本申请实施方式中, CPU 可以是单运算核心, 也可以包括多运算核心。

存储单元 404, 用于存储代码和数据, 代码供处理器单元 403 运行。

具体的, 存储单元 404 可用于存储软件程序以及模块, 处理器单元 403 通过运行存储在存储单元 404 的软件程序以及模块, 从而执行终端设备的各种功能应用以及实现数据处理。存储单元 404 主要包括程序存储区和数据存储区, 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, 比如

声音播放程序、图像播放程序等等；数据存储区可存储根据终端设备的使用所创建的数据（比如音频数据、电话本等）等。

在本申请具体实施方式中，存储单元 404 可以包括易失性存储器，例如非挥发性动态随机存取内存（英文全称：Nonvolatile Random Access Memory，英文简称 NVRAM）、相变化随机存取内存（英文全称：Phase Change RAM，英文简称 PRAM）、磁阻式随机存取内存（英文全称：Magnetoresistive RAM，英文简称 MRAM）等，还可以包括非易失性存储器，例如至少一个磁盘存储器件、电子可擦除可编程只读存储器（英文全称：Electrically Erasable Programmable Read-Only Memory，英文简称 EEPROM）、闪存器件，例如反或
5 闪存（英文全称：NOR flash memory）或是反及闪存（英文全称：NAND flash
10 memory）。

非易失存储器储存处理器单元 403 所执行的操作系统及应用程序。所述处理器单元 403 从所述非易失存储器加载运行程序与数据到内存并将数字内容储存于大量储存装置中。所述操作系统包括用于控制和管理常规系统任务，例如
15 如内存管理、存储设备控制、电源管理等，以及有助于各种软硬件之间通信的各种组件和/或驱动器。

在本申请实施方式中，所述操作系统可以是 Google 公司的 Android 系统、Apple 公司开发的 iOS 系统或 Microsoft 公司开发的 Windows 操作系统等，或者是 Vxworks 这类的嵌入式操作系统。

20 所述应用程序包括安装在终端设备上的任何应用，包括但不限于浏览器、电子邮件、即时消息服务、文字处理、键盘虚拟、窗口小部件（Widget）、加密、数字版权管理、语音识别、语音复制、定位（例如由全球定位系统提供的功能）、音乐播放等等。

输入单元 405，用于实现用户与终端设备的交互和/或信息输入到终端设备
25 中。

例如，所述输入单元 405 可以接收用户输入的数字或字符信息，以产生与用户设置或功能控制有关的信号输入。在本申请具体实施方式中，输入单元 405 可以是触摸屏，也可以是其他人机交互界面，例如实体输入键、麦克风等，还可是其他外部信息撷取装置，例如摄像头等。

5 本申请实施例所示的触摸屏，可收集用户在其上触摸或接近的操作动作。比如用户使用手指、触笔等任何适合的物体或附件在触摸屏上或接近触摸屏的位置的操作动作，并根据预先设定的程式驱动相应的连接装置。可选的，触摸屏可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸操作，并将检测到的触摸操作转换为电信号，以及将所述电信号传送给
10 触摸控制器；触摸控制器从触摸检测装置上接收所述电信号，并将它转换成触点坐标，再送给所述处理器单元 403。

所述触摸控制器还可以接收处理器单元 403 发来的命令并执行。此外，所述触摸屏可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触摸屏。

15 在本申请的其他实施方式中，所述输入单元 405 所采用的实体输入键可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。麦克风形式的输入单元 405 可以收集用户或环境输入的语音并将其转换成电信号形式的、处理器单元 403 可执行的命令。

20 在本申请的其他一些实施方式中，所述输入单元 405 还可以是各类传感器件，例如霍尔器件，用于侦测终端设备的物理量，例如力、力矩、压力、应力、位置、位移、速度、加速度、角度、角速度、转数、转速以及工作状态发生变化的时间等，转变成电量来进行检测和控制。其他的一些传感器件还可以包括重力感应计、三轴加速计、陀螺仪、电子罗盘、环境光传感器、接近传感器、温度传感器、湿度传感器、压力传感器、心率传感器、指纹识别器等。

25 通信单元 407，用于建立通信信道，使终端设备通过所述通信信道以连接

至远程服务器，并从所述远程服务器下媒体数据。所述通信单元 407 可以包括无线局域网（英文全称：Wireless Local Area Network，英文简称：wireless LAN）模块、蓝牙模块、基带模块等通信模块，以及所述通信模块对应的射频（英文全称：Radio Frequency，英文简称：RF）电路，用于进行无线局域网络通信、蓝牙通信、红外线通信及/或蜂窝式通信系统通信，例如宽带码分多重接入（英文全称：Wideband Code Division Multiple Access，英文简称：W-CDMA）及/或高速下行封包存取（英文全称：High Speed Downlink Packet Access，英文简称 HSDPA）。所述通信模块用于控制终端设备中的各组件的通信，并且可以支持直接内存存取。

在本申请的不同实施方式中，所述通信单元 407 中的各种通信模块一般以集成电路芯片（英文全称：Integrated Circuit Chip）的形式出现，并可进行选择性组合，而不必包括所有通信模块及对应的天线组。例如，所述通信单元 407 可以仅包括基带芯片、射频芯片以及相应的天线以在一个蜂窝通信系统中提供通信功能。经由所述通信单元 407 建立的无线通信连接，例如无线局域网接入或 WCDMA 接入，所述终端设备可以连接至蜂窝网（英文全称：Cellular Network）或因特网。在本申请的一些可选实施方式中，所述通信单元 407 中的通信模块，例如基带模块可以集成到处理器单元 403 中，典型的如高通（Qualcomm）公司提供的 APQ+MDM 系列平台。

射频电路 408，用于信息收发或通话过程中接收和发送信号。例如，将基站的下行信息接收后，给处理器单元 403 处理；另外，将设计上行的数据发送给基站。通常，所述射频电路 408 包括用于执行这些功能的公知电路，包括但不限于天线系统、射频收发机、一个或多个放大器、调谐器、一个或多个振荡器、数字信号处理器、编解码（Codec）芯片组、用户身份模块（SIM）卡、存储器等等。此外，射频电路 408 还可以通过无线通信与网络和其他设备通信。

所述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯

系统 (英文全称: Global System of Mobile communication, 英文简称: GSM)、通用分组无线服务(英文全称: General Packet Radio Service, 英文简称: GPRS)、码分多址 (英文全称: Code Division Multiple Access, 英文简称: CDMA)、宽带码分多址 (英文全称: Wideband Code Division Multiple Access, 英文简称: WCDMA)、高速上行链路分组接入技术(英文全称: High Speed Uplink Packet Access, 英文简称: HSUPA)、长期演进 (英文全称: Long Term Evolution, 英文简称: LTE)、电子邮件、短消息服务 (英文全称: Short Messaging Service, 英文简称: SMS) 等。

电源 409, 用于给终端设备的不同部件进行供电以维持其运行。作为一般性理解, 所述电源 409 可以是内置的电池, 例如常见的锂离子电池、镍氢电池等, 也包括直接向终端设备供电的外接电源, 例如 AC 适配器等。在本申请的一些实施方式中, 所述电源 409 还可以作更为广泛的定义, 例如还可以包括电源管理系统、充电系统、电源故障检测电路、电源转换器或逆变器、电源状态指示器 (如发光二极管), 以及与终端设备的电能生成、管理及分布相关联的其他任何组件。

基于图 1 至图 4 所示, 以下结合图 5 所示以云服务提供商侧服务器为执行主体对本申请实施例所提供的授权方法进行详细说明:

步骤 501、云服务提供商侧服务器接收终端设备发送的第一临时证书。

所述第一临时证书用于请求访问所述云服务提供商侧服务器上的资源;

具体的, 在所述终端设备需要向所述云服务提供商侧服务器请求访问所述云服务提供商侧服务器上的资源的情况下, 用户即可登录所述终端设备的目标网站, 所述目标网站为用于获取所述云服务提供商侧服务器授权的网站, 通过登录所述网站以使所述终端设备能够将所述第一临时证书发送给所述云服务提供商侧服务器。

在终端设备需要获取所述云服务提供商侧服务器授权的情况下, 所述终端

设备即可向所述云服务提供商侧服务器发送所述第一临时证书。

步骤 502、所述云服务提供商侧服务器根据所述第一临时证书确定终端设备对应的目标权限。

其中，所述目标权限为访问所述云服务提供商侧服务器上的目标资源的权限。

步骤 503、所述云服务提供商侧服务器将终端设备对应的第二临时证书发送给所述终端设备。

本实施例所示的所述第二临时证书是短期凭证。可将所述第二临时证书的有效时间配置几分钟到几小时。一旦第二临时证书的凭证到期，则云服务提供商侧服务器将不再识别所述第二临时证书，从而使得所述终端设备无法再通过所述第二临时证书访问所述云服务提供商侧服务器上的目标资源。

本实施例所示的云服务提供商侧服务器执行授权方法的具体执行过程，请详见图 7 所示的实施例。

基于图 1 至图 4 所示，以下结合图 6 所示以终端设备为执行主体对本申请实施例所提供的授权方法进行详细说明：

步骤 601、终端设备将第一临时证书发送给云服务提供商侧服务器。

所述第一临时证书的说明可参见图 5 所示的实施例，具体在本实施例中不做赘述。

步骤 602、所述终端设备接收所述云服务提供商侧服务器发送的第二临时证书。

所述第二临时证书的说明可参见图 5 所示的实施例，具体在本实施例中不做赘述。

步骤 603、所述终端设备通过所述第二临时证书访问所述云服务提供商侧服务器上的所述目标资源。

本实施例所示的终端设备执行授权方法的具体执行过程，请详见图 7 所示

的实施例。

以下结合图 7 所示对图 5 和图 6 所示的授权方法的执行流程进行具体的详细说明：

5 如图 7 所示，所述授权方法包括：

步骤 701、所述终端设备将请求信息发送给云服务提供商侧服务器。

本实施例所示的所述终端设备的具体说明，请详见上述实施例所示，具体在本实施例中不做赘述。

10 具体的，本实施例所示的所述请求信息包括所述终端设备已存储的第一令牌（Token）信息。

其中，所述第一令牌信息用于所述终端设备向所述云服务提供商侧服务器进行认证。

本实施例对所述第一令牌信息的类型可为多种，本实施例对所述第一令牌信息的类型不做限定。

15 本实施例所示的终端设备通过所述第一令牌信息向所述云服务提供商侧服务器请求认证，从而使得所述云服务提供商侧服务器能够基于所述第一令牌信息判断出所述终端设备是否伪造，是否越权，是否过期等。

20 更具体的，本实施例所示的所述终端设备可存储有云服务提供商侧服务器的统一资源定位符 URL 地址，则本实施例所示的所述终端设备即可根据所述统一资源定位符 URL 地址向所述云服务提供商侧服务器发送所述请求信息。

更具体的，本实施例所示的终端设备可根据所述 URL 地址将所述请求信息发送至所述云服务提供商侧服务器上用于对终端设备进行认证的网站。

步骤 702、所述云服务提供商侧服务器接收所述终端设备发送的请求信息。

25 具体的，所述云服务提供商侧服务器的具体说明请详见上述实施例所示，具体在本实施例中不做赘述。

步骤 703、所述云服务提供商侧服务器生成第四签名信息。

具体的，本实施例所示的所述云服务提供商侧服务器在接收到所述请求信息后，即可对第一密钥标识、所述第一令牌信息以及所述云服务提供商侧服务器所生成的随机回复信息（echoInfo）进行加密计算以生成第四签名信息。

5 具体的，本实施例所示的所述云服务提供商侧服务器根据已存储的长期密钥对第一密钥标识、所述第一令牌信息以及所述云服务提供商侧服务器所生成的随机回复信息进行加密计算以生成第四签名信息。

步骤 704、所述云服务提供商侧服务器将所述第四签名信息发送给所述终端设备。

10 步骤 705、所述终端设备判断所述第四签名信息是否满足第一条条件，若是，则执行步骤 706。

本实施例中，在终端设备接收到所述第四签名信息后，即可对所述第四签名信息进行解密计算以获取所述第四签名信息所包含的第一密钥标识、所述第一令牌信息以及所述云服务提供商侧服务器所生成的随机回复信息。

15 本实施例所示的所述第一条条件为：所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同。

本实施例中，若所述终端设备判断出所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同的情况下，即所述终端设备确定出所述第四签名信息满足所述第一条条件的情况下，则可继续执行步骤 20 骤 706。

步骤 706、所述终端设备将第五签名信息发送给所述云服务提供商侧服务器。

具体的，本实施例所示的终端设备将所述第四签名信息所包括的所述随机回复信息发送给所述云服务提供商侧服务器。

25 具体发送方式为，所述终端设备对所接收到的所述随机回复信息进行加密

计算以生成所述第五签名信息,即所述终端设备所生成的所述第五签名信息包括有所述随机回复信息。

本实施例所示的所述终端设备即可通过所述第五签名信息将所述随机回复信息发送给所述云服务提供商侧服务器。

5 本实施例中,所述终端设备可调用所述云服务提供商侧服务器的目标接口以实现所述终端设备与所述云服务提供商侧服务器之间的数据交互。

具体的,所述云服务提供商侧服务器的目标接口可为所述云服务提供商侧服务器的开放服务器授权(Open Service Auhorization)的应用程序编程接口(Application Programming Interface, API)。

10 本实施例所示的终端设备通过所述第五签名信息调用所述云服务提供商侧服务器的目标接口。

步骤 707、所述云服务提供商侧服务器获取第五签名信息所包括的所述随机回复信息。

具体的,所述云服务提供商侧服务器对所述第五签名信息进行解密计算以
15 获取所述第五签名信息所包括的所述随机回复信息。

步骤 708、所述云服务提供商侧服务器判断所述第五签名信息是否满足第二条件,若是,则执行步骤 709。

本实施例中,所述云服务提供商侧服务器在获取到所述第五签名信息所包括的所述随机回复信息后,即可判断所述第五签名信息是否满足第二条件。

20 其中,所述第二条件为:所述第五签名信息所包括的所述随机回复信息与所述云服务提供商侧服务器所生成的所述随机回复信息相同。

在所述云服务提供商侧服务器判断出所述第五签名信息所包括的所述随机回复信息与所述云服务提供商侧服务器所生成的所述随机回复信息相同,即所述第五签名信息满足所述第二条件的情况下,则所述云服务提供商侧服务器
25 与所述终端设备之间完成 URL 确认,则完成 URL 确认的所述云服务提供商侧

服务器与所述终端设备之间即可进行数据交互。

具体的，所述云服务提供商侧服务器与所述终端设备之间完成 URL 确认后，所述云服务提供商侧服务器的所述目标接口被所述终端设备成功调用。

步骤 709、所述云服务提供商侧服务器生成第一签名信息。

5 具体的，本实施例所示的所述云服务提供商侧服务器对加密票据进行加密计算以生成第一签名信息，其中，所述加密票据用于对所述终端设备进行认证。

步骤 710、所述云服务提供商侧服务器将所述第一签名信息发送给所述终端设备。

本实施例中，在所述云服务提供商侧服务器生成所述第一签名信息后，即可将已生成的所述第一签名信息发送给所述云服务提供商侧服务器。

步骤 711、所述终端设备将第二签名信息发送给所述云服务提供商侧服务器。

具体的，本实施例所示的所述终端设备在接收到所述第一签名信息后，即可对所述第一签名信息进行解密计算以获取所述第一签名信息所包括的所述加密票据。

更具体的，所述终端设备对所述加密票据进行加密计算以生成所述第二签名信息，可见，所述终端设备所生成的所述第二签名信息中包括所述加密票据。

步骤 712、所述云服务提供商侧服务器获取所述第二签名信息所包括的所述加密票据。

20 具体的，本实施例所示的所述云服务提供商侧服务器可接收所述终端设备所发送的所述第二签名信息，并对所述第二签名信息进行解密计算以获取所述第二签名信息所包括的所述加密票据。

步骤 713、所述云服务提供商侧服务器获取第三签名信息。

具体的，所述云服务提供商侧服务器在获取到所述第二签名信息所包括的所述加密票据后，即可对所述第二签名信息所包括的所述加密票据进行加密计

算以生成所述第三签名信息。

步骤 714、所述云服务提供商侧服务器在确定满足第三条件的情况下，将第一临时证书发送给所述终端设备。

5 具体的，本实施例所示的所述云服务提供商侧服务器判断所述第二签名信息和所述第三签名信息是否相同，若所述第二签名信息和所述第三签名信息相同，则所述云服务提供商侧服务器即可确定出满足所述第三条件，即本实施例所示的所述第三条件为：所述第三签名信息与所述第二签名信息相同。

10 可选的，所述终端设备可通过所述终端设备的长期密钥对所述加密票据进行加密计算，并通过加密计算后的加密票据向所述云服务提供商侧服务器请求所述第一临时证书，在所述终端设备获取到所述第一临时证书后，所述终端设备即可通过所述第一临时证书完成与所述云服务提供商侧服务器之间的认证环节，相互认证后的所述终端设备和所述云服务提供商侧服务器即可进行实时授权流程，其中，本实施例所示的所述实时授权流程的基础是 oAuth2.0 协议实时授权流程请详见下述实施例所示。

15 步骤 715、所述终端设备向所述云服务提供商侧服务器发送的第一临时证书。

其中，所述第一临时证书用于请求访问所述云服务提供商侧服务器上的资源。

20 本实施例所示的所述第一临时证书向所述终端设备已调用的目标接口请求获取预授权码（precode）。

通过本实施例所示的所述预授权码能够有效的防止恶意或假冒的终端设备向所述云服务提供商侧服务器获取授权，从而有效的提升了实时授权过程的安全。

步骤 716、所述云服务提供商侧服务器将预授权码发送给所述终端设备。

25 具体的，本实施例所示的所述云服务提供商侧服务器在获取到所述第一临

时证书后,即可判断所述云服务提供商侧服务器所存储的第一临时证书和当前所接收到的所述第一临时证书是否相同,若是,则所述云服务提供商侧服务器即可将所述预授权码发送给所述终端设备。

步骤 717、所述终端设备获取用户提交的认证信息。

5 具体的,本实施例所示的所述终端设备在接收到所述预授权码后,即可将所述目标网站进行跳转,从而使得所述目标网站跳转到包含有所述预授权码的所述云服务提供商侧服务器的登录页面中。

具体的,本实施例所示的所述登录页面中还包括有密钥标识。

本实施例所示的所述登录页面即可接收用户输入的用于进行登录的用户
10 名和密码以进行身份认证。

具体的,本实施例以所述认证信息包括所述用户的用户名和密码为例进行示例性的说明,在具体应用中,所述认证信息还可包括用于认证的其他信息,具体在本实施例中不做限定。

本实施例中,所述云服务提供商侧服务器可预先存储有多个用户名以及与
15 各所述用户名对应的密码,所述用户可通过所述终端设备向所述云服务提供商侧服务器的登录页面输入所述认证信息,若所述云服务提供商侧服务器确定出所述用户当前所输入的所述认证信息已存储在所述云服务提供商侧服务器上,则确定所述用户经过了认证。

步骤 718、所述云服务提供商侧服务器获取已选定权限。

20 本实施例中,在所述云服务提供商侧服务器根据所述用户所提交的所述认证信息确定出所述用户已经过认证,则所述云服务提供商侧服务器即可向用户提供权限列表。

具体的,所述权限列表包括多个待选定权限。

所述用户通过所述权限列表即可在所述多个待选定权限中选定需要的权
25 限。

具体的,所述云服务提供商侧服务器通过所述权限列表接收用户输入的选定操作。

所述云服务提供商侧服务器确定已选定权限,所述已选定权限为所述选定操作在所述权限列表中所选定的所述多个待选定权限中的至少一个权限。

5 例如,在所述权限列表中有一个待选定权限为通过 QQ 登录微博,若用户在所述权限列表中选定了通过 QQ 登录微博的权限,则所述云服务提供商侧服务器即可确定通过 QQ 登录微博的权限为已选定权限。

具体的,在所述云服务提供商侧服务器获取到所述已选定权限后,即可将已选定权限与用户的认证信息进行绑定,则在后续用户通过该认证信息进行登
10 录时,可获取到与认证信息绑定的所述已选定权限,从而避免了用户的重复选定。

步骤 719、所述云服务提供商侧服务器确定预选权限。

所述预选权限为所述终端设备在所述云服务提供商侧服务器上已选定的权限。

15 具体的,本实施例所示的预选权限为用户实现定义好策略,所述策略为所述终端设备在所述云服务提供商侧服务器上所能够访问的资源。

如图 8 所示,所述策略为包括权限和授权对象,权限包括效力、资源、授权接口、授权条件等,授权对象为权限所对应的用户,即本实施例所示的所述
20 云服务提供商侧服务器在确定所述预选权限的过程中,所述云服务提供商侧服务器可通过权限和授权对象实现对预选权限的配置。

具体的,所述云服务提供商侧服务器可根据终端设备所注册的行业领域或服务领域对所述策略进行创建。

具体的,所述云服务提供商侧服务器创建好策略之后,所述终端设备就默认可以执行预授权策略里描述的资源了。

25 步骤 720、所述云服务提供商侧服务器确定所述终端设备对应的目标权

限。

具体的,所述云服务提供商侧服务器确定所述已选定权限和所述预选权限的交集为所述目标权限。

在实施例 5 中,若本实施例 5 中所述终端设备没有经由所述权限列表获取已选定权限,则本实施例 5 所示的所述目标权限为所述预选权限。

具体的,所述终端设备在注册后,会根据所注册的行业领域或服务领域,给与云服务提供商侧服务器的默认授权策略。这样用户进入终端设备的站点后,在不选择其他策略的情况下,将默认允许终端使用默认的预选权限约束所述终端设备访问所述云服务提供商侧服务器的资源。

10 在实施例 10 中,若所述终端设备经由所述权限列表获取已选定权限,则本实施例 10 所示的所述目标权限为所述已选定权限和所述预选权限的交集。

即所述目标权限同时包括在所述已选定权限和所述预选权限中。

通过本实施例 15 所示的实时授权流程,能够使得使用所述终端设备的用户被所述云服务提供商侧服务器授予所述目标权限,从而使得所述云服务提供商侧服务器控制所述终端设备对所述云服务提供商侧服务器访问,使得所述终端设备只能够访问所述云服务提供商侧服务器上的所述目标资源,且所述云服务提供商侧服务器还能够控制用户访问所述目标资源的访问方式以及时机等,具体在本实施例 15 中不做限定。

以下结合图 11 所示结合具体应用场景对目标权限进行说明:

20 如图 11 所示,本实施例 20 所示的预选权限为“云主机管理权限(云主机重启、申请、查看等)”,即本实施例 20 所示的所述预选权限为云服务提供商侧服务器默认委托给所述终端设备的权限。

图 11 所示的已选定权限为“开发商自定义第三方角色”,云服务提供商侧服务器通过所述已选定权限对所述终端设备进行精细化的权限管理。

25 采用如图 11 所示的应用场景,所述终端设备能够在用户的操作下,通过

微信登录大众点评网,而且所述云服务提供商侧服务器能够通过目标权限对通过微信登录大众点评网的权限进行限定,例如,可限定通过微信登录所述大众点评网的时间,次数等,具体在本实施例中不做限定。

步骤 721、所述云服务提供商侧服务器将授权码发送给所述终端设备。

- 5 具体的,本实施例中,在所述云服务提供商侧服务器确定出所述目标权限的情况下,所述云服务提供商侧服务器将所述云服务提供商侧服务器已存储的授权码发送给所述终端设备。

步骤 722、所述终端设备将第六签名信息发送给所述云服务提供商侧服务器。

- 10 其中,所述终端设备接收到所述云服务提供商侧服务器发送的所述授权码后,即可对所述授权码和所述第一临时证书进行加密计算以生成的第六签名信息。

步骤 723、所述云服务提供商侧服务器判断所述第六签名信息是否满足第四条件,若是,则将目标访问参数发送给所述终端设备。

- 15 具体的,所述云服务提供商侧服务器在接收到所述第六签名信息的情况下,所述云服务提供商侧服务器即可对所述第六签名信息进行解密计算以获取所述第六签名信息所包括的所述授权码和所述第一临时证书。

所述第四条件为:所述第六签名信息所包括的所述授权码和所述云服务提供商侧服务器已存储的所述授权码相同。

- 20 所述第四条件还可为,所述第六签名信息所包括的所述第一临时证书和所述云服务提供商侧服务器已存储的所述第一临时证书相同。

在所述云服务提供商侧服务器判断出所述第六签名信息满足所述第四条件的情况下,所述云服务提供商侧服务器即可将用于访问所述目标资源的目标访问参数发送给所述终端设备。

- 25 所述目标访问参数包括第二令牌信息、第二密钥标识以及第二临时证书。

本实施例所示的所述第二临时证书是短期凭证。可将所述第二临时证书的有效时间配置几分钟到几小时。一旦第二临时证书的凭证到期，则云服务提供商侧服务器将不再识别所述第二临时证书，从而使得所述终端设备无法再通过所述第二临时证书访问所述云服务提供商侧服务器上的目标资源。

5 步骤 724、所述云服务提供商侧服务器将所述目标访问参数发送给所述终端设备。

本实施例中，所述终端设备即可通过已接收到的所述目标访问参数对所述云服务提供商侧服务器上的目标资源进行访问，具体的访问过程如下：

10 步骤 725、所述终端设备将第七签名信息发送给所述云服务提供商侧服务器。

其中，所述终端设备在接收到所述目标访问参数的情况下，所述终端设备即可对所述目标访问参数进行加密计算以生成的第七签名信息。

步骤 726、所述云服务提供商侧服务器生成第八签名信息。

15 其中，所述云服务提供商侧服务器对所述云服务提供商侧服务器所生成的所述目标访问参数进行加密计算以生成第八签名信息。

步骤 727、所述云服务提供商侧服务器确定所述终端设备具有访问所述目标资源的权限。

20 具体的，若所述云服务提供商侧服务器确定出所述第七签名信息与所述第八签名信息相同，则所述云服务提供商侧服务器确定所述终端设备具有访问所述目标资源的权限，即终端设备具有目标权限。

所述云服务提供商侧服务器根据确定所述终端设备具有目标权限后，所述终端设备即可访问所述云服务提供商侧服务器上的目标资源。

25 可见，采用本实施例所示的授权方法，则所述云服务提供商侧服务器可对所述终端设备进行精细化的权限管理，从而使得所述云服务提供商侧服务器即可向所述终端设备开放接入的能力，同时保证了终端设备访问所述云服务提供

商侧服务器的目标资源的安全性和灵活性,而且所述云服务提供商侧服务器与所述终端设备之间通过签名信息进行数据交互,从而提升了数据交互过程中的安全。

以下结合图 9 所示对本申请实施例所提供的云服务提供商侧服务器的具体结构进行详细说明:

本实施例所示的所述云服务提供商侧服务器用于执行图 9 所示的授权方法,具体执行过程请详见图 9 所示,具体在本实施例中不做赘述。

本实施例所示的所述云服务提供商侧服务器包括:

第一处理单元 901,用于对加密票据进行加密计算以生成第一签名信息,将所述第一签名信息发送给所述终端设备,接收所述终端设备发送的第二签名信息,所述第二签名信息包括所述终端设备对所述第一签名信息进行解密计算以获取到的所述加密票据,对所述第二签名信息进行解密计算以获取所述第二签名信息所包括的所述加密票据,对所述加密票据进行加密计算以生成第三签名信息,若确定出所述第三签名信息与所述第二签名信息相同,则将所述第一临时证书发送给所述终端设备。

所述第一处理单元 901 将所述第一签名信息发送给所述终端设备之前,所述第一处理单元具体用于,接收所述终端设备发送的请求信息,所述请求信息包括所述终端设备已存储的第一令牌信息,对第一密钥标识、所述第一令牌信息以及所述云服务提供商侧服务器所生成的随机回复信息进行加密计算以生成第四签名信息,将所述第四签名信息发送给所述终端设备,以使在所述终端设备确定出所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同的情况下,所述终端设备将第五签名信息发送给所述云服务提供商侧服务器,所述第五签名信息包括所述随机回复信息,对所述第五签名信息进行解密计算以获取所述第五签名信息所包括的所述随机回复信息,确定出所述第五签名信息所包括的所述随机回复信息与所述云服务提

供商侧服务器所生成的所述随机回复信息相同的情况下，则触发执行将所述第一签名信息发送给所述终端设备步骤。

接收单元 902，用于接收终端设备发送的第一临时证书，所述第一临时证书用于请求访问所述云服务提供商侧服务器上的资源；

5 确定单元 903，用于根据所述第一临时证书确定所述终端设备对应的目标权限，所述目标权限为访问所述云服务提供商侧服务器上的目标资源的权限；

其中，所述确定单元 903 用于根据所述第一临时证书生成权限列表，所述权限列表包括多个待选定权限，通过所述权限列表接收用户输入的选定操作，确定已选定权限，所述已选定权限为所述选定操作在所述权限列表中所选定的
10 所述多个待选定权限中的至少一个权限，确定预选权限，所述预选权限为所述终端设备在所述云服务提供商侧服务器上已选定的权限，确定所述已选定权限和所述预选权限的交集为所述目标权限。

发送单元 904，用于将所述目标权限对应的第二临时证书发送给所述终端设备，以使所述终端设备通过所述第二临时证书访问所述目标资源。

15 其中，所述发送单元 904 用于将所述云服务提供商侧服务器已存储的授权码发送给所述终端设备，接收所述终端设备发送第六签名信息，所述第六签名信息为所述终端设备对所述授权码和所述第一临时证书进行加密计算以生成的签名信息，若判断所述第六签名信息所包括的所述授权码和所述云服务提供商侧服务器已存储的所述授权码相同，则将用于访问所述目标资源的目标访问
20 参数发送给所述终端设备，所述目标访问参数包括第二令牌信息、第二密钥标识以及所述第二临时证书。

第二处理单元 905，用于接收所述终端设备发送的用于访问所述目标资源的第七签名信息，所述第七签名信息为所述终端设备对所述目标访问参数进行加密计算以生成的签名信息，对所述云服务提供商侧服务器所生成的所述目标
25 访问参数进行加密计算以生成第八签名信息，若确定出所述第七签名信息与所

述第八签名信息相同，则确定所述终端设备具有访问所述目标资源的权限。

以下结合图 10 所示对本申请实施例所提供的终端设备的具体结构进行详细说明：

本实施例所示的所述云服务提供商侧服务器用于执行图 5 所示的授权方法，具体执行过程请详见图 5 所示，具体在本实施例中不做赘述。

本实施例所示的所述终端设备包括：

第一处理单元 1001，用于接收所述云服务提供商侧服务器发送的第一签名信息，所述第一签名信息为所述云服务提供商侧服务器对加密票据进行加密计算以生成的签名信息，对所述第一签名信息进行解密计算以获取所述加密票据，对所述加密票据进行加密计算以获取第二签名信息，将所述第二签名信息发送给所述云服务提供商侧服务器，以使所述云服务提供商侧服务器在确定出第三签名信息和第二签名信息相同的情况下，所述云服务提供商侧服务器将所述第一临时证书发送给所述终端设备，所述第三签名信息包括所述加密票据，接收所述云服务提供商侧服务器发送的所述第一临时证书。

所述第一处理单元 1001 在接收所述云服务提供商侧服务器发送的第一签名信息的过程中，具体用于向所述云服务提供商侧服务器发送请求信息，所述请求信息包括所述终端设备已存储的第一令牌信息，以使所述云服务提供商侧服务器向所述终端设备发送第四签名信息，其中，所述第四签名信息包括第一密钥标识、所述第一令牌信息以及所述云服务提供商侧服务器所生成的随机回复信息，接收所述第四签名信息，若确定出所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同的情况下，则对所述随机回复信息进行加密计算以生成第五签名信息，将所述第五签名信息发送给所述云服务提供商侧服务器，以使在所述云服务提供商侧服务器确定出所述第五签名信息所包括的所述随机回复信息与所述云服务提供商侧服务器所生成的所述随机回复信息相同的情况下，将所述第一签名信息发送给所述终端设

备。

发送单元 1002, 用于将第一临时证书发送给云服务提供商侧服务器, 所述
第一临时证书用于请求访问所述云服务提供商侧服务器上的资源;

其中, 所述发送单元 1002 用于, 接收所述云服务提供商侧服务器发送的
5 所述云服务提供商侧服务器已存储的授权码, 对所述授权码和所述第一临时证
书进行加密计算以生成的第六签名信息, 将所述第六签名信息发送给所述云服
务提供商侧服务器, 以使若所述云服务提供商侧服务器判断出所述第六签名信
息所包括的所述授权码和所述云服务提供商侧服务器已存储的所述授权码相
同, 则将用于访问所述目标资源的目标访问参数发送给所述终端设备, 所述目
10 标访问参数包括第二令牌信息、第二密钥标识以及所述第二临时证书, 接收所
述目标访问参数。

接收单元 1003, 用于接收所述云服务提供商侧服务器发送所述目标权限
对应的第二临时证书;

访问单元 1004, 用于通过所述第二临时证书访问所述云服务提供商侧服
15 务器上的所述目标资源。

第二处理单元 1005, 用于对所述目标访问参数进行加密计算以生成第七
签名信息, 将所述第七签名信息发送给所述云服务提供商侧服务器, 以使若所
述云服务提供商侧服务器确定出所述第七签名信息与第八签名信息相同, 则确
定所述终端设备具有访问所述目标资源的权限, 所述第八签名信息为所述云服
20 务提供商侧服务器对所述云服务提供商侧服务器所生成的所述目标访问参数
进行加密计算以生成的签名信息。

基于图 3 所示的云服务提供商侧服务器可知, 所述云服务提供商侧服务器
包括:

一个或多个所述中央处理器 301、存储器 302、总线系统、以及一个或多
25 个程序, 所述中央处理器 301 和所述存储器 302 通过所述总线系统相连。

其中所述一个或多个程序被存储在所述存储器 302 中,所述一个或多个程序包括指令,所述指令当被所述云服务提供商侧服务器执行时使所述云服务提供商侧服务器执行如图 5、图 6 或图 7 所示的方法,具体执行流程在本实施例中不做赘述。

5 基于图 4 所示的终端设备可知,所述终端设备包括一个或多个处理器单元 403、存储单元 404、总线系统、以及一个或多个程序,所述处理器单元 403 和所述存储单元 404 通过所述总线系统相连;

10 其中所述一个或多个程序被存储在所述存储单元 404 中,所述一个或多个程序包括指令,所述指令当被所述终端设备执行时使所述终端设备执行如图 5 所示的方法,具体执行过程在本实施例中不做赘述。

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。

15 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,20 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。

25 另外,在本申请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。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售
5 或使用,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,本申请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全部或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
10 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)执行本申请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(ROM, Read-Only Memory)、
随机存取存储器(RAM, Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述,以上实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,本领域的普通技术人员应当理
15 解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质的脱离本申请各实施例技术方案的精神和范围。

权 利 要 求

1、一种授权方法，其特征在于，包括：

服务器接收终端设备发送的第一临时证书，所述第一临时证书用于请求访问所述服务器上的资源；

5 所述服务器根据所述第一临时证书确定所述终端设备对应的目标权限，所述目标权限为访问所述服务器上的目标资源的权限；

所述服务器将所述目标权限对应的第二临时证书发送给所述终端设备，以使所述终端设备通过所述第二临时证书访问所述目标资源。

2、根据权利要求1所述的授权方法，其特征在于，所述服务器接收终端
10 设备发送的第一临时证书之前，所述方法还包括：

所述服务器对加密票据进行加密计算以生成第一签名信息；

所述服务器将所述第一签名信息发送给所述终端设备；

所述服务器接收所述终端设备发送的第二签名信息，所述第二签名信息包括所述终端设备对所述第一签名信息进行解密计算以获取到的所述加密票据；

15 所述服务器对所述第二签名信息进行解密计算以获取所述第二签名信息所包括的所述加密票据；

所述服务器对所述加密票据进行加密计算以生成第三签名信息；

若所述服务器确定出所述第三签名信息与所述第二签名信息相同，则所述服务器将所述第一临时证书发送给所述终端设备。

20 3、根据权利要求2所述的授权方法，其特征在于，所述服务器将所述第一签名信息发送给所述终端设备之前，所述方法还包括：

所述服务器接收所述终端设备发送的请求信息，所述请求信息包括所述终端设备已存储的第一令牌信息；

所述服务器对第一密钥标识、所述第一令牌信息以及所述服务器所生成的
25 随机回复信息进行加密计算以生成第四签名信息；

所述服务器将所述第四签名信息发送给所述终端设备,以使在所述终端设备确定出所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同的情况下,所述终端设备将第五签名信息发送给所述服务器,所述第五签名信息包括所述随机回复信息;

5 所述服务器对所述第五签名信息进行解密计算以获取所述第五签名信息所包括的所述随机回复信息;

若所述服务器确定出所述第五签名信息所包括的所述随机回复信息与所述服务器所生成的所述随机回复信息相同的情况下,触发执行所述服务器将所述第一签名信息发送给所述终端设备步骤。

10 4、根据权利要求 1 至 3 任一项所述的授权方法,其特征在于,所述服务器根据所述第一临时证书确定目标权限包括:

所述服务器根据所述第一临时证书生成权限列表,所述权限列表包括多个待选定权限;

所述服务器通过所述权限列表接收用户输入的选定操作;

15 所述服务器确定已选定权限,所述已选定权限为所述选定操作在所述权限列表中所选定的所述多个待选定权限中的至少一个权限;

所述服务器确定所述已选定权限和所述预选权限的交集为所述目标权限,所述预选权限为默认授权策略对应的权限。

20 5、根据权利要求 1 所述的授权方法,其特征在于,所述服务器将第二临时证书发送给所述终端设备包括:

所述服务器将所述服务器已存储的授权码发送给所述终端设备;

所述服务器接收所述终端设备发送第六签名信息,所述第六签名信息为所述终端设备对所述授权码和所述第一临时证书进行加密计算以生成的签名信息;

25 若所述服务器判断所述第六签名信息所包括的所述授权码和所述服务器

已存储的所述授权码相同,则所述服务器将用于访问所述目标资源的目标访问参数发送给所述终端设备,所述目标访问参数包括第二令牌信息、第二密钥标识以及所述第二临时证书。

6、根据权利要求5所述的授权方法,其特征在于,所述方法还包括:

5 所述服务器接收所述终端设备发送的用于访问所述目标资源的第七签名信息,所述第七签名信息为所述终端设备对所述目标访问参数进行加密计算以生成的签名信息;

所述服务器对所述服务器所生成的所述目标访问参数进行加密计算以生成第八签名信息;

10 若所述服务器确定出所述第七签名信息与所述第八签名信息相同,则所述服务器确定所述终端设备具有访问所述目标资源的权限。

7、一种授权方法,其特征在于,包括:

终端设备将第一临时证书发送给服务器,所述第一临时证书用于请求访问所述服务器上的资源,以使得所述服务器根据所述第一临时证书确定所述终端设备对应的目标权限,所述目标权限为访问所述服务器上的目标资源的权限;

15 所述终端设备接收所述服务器发送的所述目标权限对应的第二临时证书,所述第二临时证书用于指示目标权限,所述目标权限用于指示具有访问所述服务器上的目标资源的权限;

所述终端设备通过所述第二临时证书访问所述目标资源。

20 8、根据权利要求7所述的授权方法,其特征在于,所述终端设备将第一临时证书发送给服务器之前,所述方法还包括:

所述终端设备接收所述服务器发送的第一签名信息,所述第一签名信息为所述服务器对加密票据进行加密计算以生成的签名信息;

所述终端设备对所述第一签名信息进行解密计算以获取所述加密票据;

25 所述终端设备对所述加密票据进行加密计算以获取第二签名信息;

所述终端设备将所述第二签名信息发送给所述服务器,以使所述服务器在确定出第三签名信息和第二签名信息相同的情况下,所述服务器将所述第一临时证书发送给所述终端设备,所述第三签名信息包括所述加密票据;

所述终端设备接收所述服务器发送的所述第一临时证书。

- 5 9、根据权利要求 8 所述的授权方法,其特征在于,所述终端设备接收所述服务器发送的第一签名信息之前,所述方法还包括:

所述终端设备向所述服务器发送请求信息,所述请求信息包括所述终端设备已存储的第一令牌信息,以使所述服务器向所述终端设备发送第四签名信息,其中,所述第四签名信息包括第一密钥标识、所述第一令牌信息以及所述
10 服务器所生成的随机回复信息;

所述终端设备接收所述第四签名信息;

若所述终端设备确定出所述第四签名信息所包括的所述第一令牌信息与所述终端设备已存储的所述第一令牌信息相同的情况下,则所述终端设备对所述随机回复信息进行加密计算以生成第五签名信息;

- 15 所述终端设备将所述第五签名信息发送给所述服务器,以使在所述服务器确定出所述第五签名信息所包括的所述随机回复信息与所述服务器所生成的所述随机回复信息相同的情况下,将所述第一签名信息发送给所述终端设备。

10、根据权利要求 7 所述的授权方法,其特征在于,所述终端设备接收所述服务器发送的第二临时证书包括:

- 20 所述终端设备接收所述服务器发送的所述服务器已存储的授权码;

所述终端设备对所述授权码和所述第一临时证书进行加密计算以生成的第六签名信息;

- 所述终端设备将所述第六签名信息发送给所述服务器,以使若所述服务器判断出所述第六签名信息所包括的所述授权码和所述服务器已存储的所述授
25 权码相同,则将用于访问所述目标资源的目标访问参数发送给所述终端设备,

所述目标访问参数包括第二令牌信息、第二密钥标识以及所述第二临时证书；
所述终端设备接收所述目标访问参数。

11、根据权利要求 10 所述的授权方法，其特征在于，所述方法还包括：
所述终端设备对所述目标访问参数进行加密计算以生成第七签名信息；

5 所述终端设备将所述第七签名信息发送给所述服务器，以使若所述服务器确定出所述第七签名信息与第八签名信息相同，则确定所述终端设备具有访问所述目标资源的所述目标权限，所述第八签名信息为所述服务器对所述服务器所生成的所述目标访问参数进行加密计算以生成的签名信息。

12、一种服务器，其特征在于，包括：

10 接收单元，用于接收终端设备发送的第一临时证书，所述第一临时证书用于请求访问所述服务器上的资源；

确定单元，用于根据所述第一临时证书确定所述终端设备对应的目标权限，所述目标权限为访问所述服务器上的目标资源的权限；

15 发送单元，用于将所述目标权限对应的第二临时证书发送给所述终端设备，以使所述终端设备通过所述第二临时证书访问所述目标资源。

13、一种终端设备，其特征在于，包括：

20 发送单元，用于将第一临时证书发送给服务器，所述第一临时证书用于请求访问所述服务器上的资源，以使得所述服务器根据所述第一临时证书确定所述终端设备对应的目标权限，所述目标权限为访问所述服务器上的目标资源的权限；

接收单元，用于接收所述服务器发送的所述目标权限对应的第二临时证书；

访问单元，用于通过所述第二临时证书访问所述目标资源。

14、一种服务器，其特征在于，包括：

25 一个或多个中央处理器、存储器、总线系统、以及一个或多个程序，所述

中央处理器和所述存储器通过所述总线系统相连;

其中所述一个或多个程序被存储在所述存储器中,所述一个或多个程序包括指令,所述指令当被所述服务器执行时使所述服务器执行如权利要求 1 至 6 任一项所述的授权方法。

5 15、一种终端设备,其特征在于,包括:

一个或多个处理器单元、存储单元、总线系统、以及一个或多个程序,所述处理器单元和所述存储单元通过所述总线系统相连;

其中所述一个或多个程序被存储在所述存储单元中,所述一个或多个程序包括指令,所述指令当被所述终端设备执行时使所述终端设备执行如权利要求
10 7 至 11 任一项所述的授权方法。

16、一种计算机存储介质,包括指令,当其在计算机上运行时,使得计算机执行如权利要求 1 至 6 任意一项所述的方法。

17、一种计算机存储介质,包括指令,当其在计算机上运行时,使得计算机执行如权利要求 7 至 11 任意一项所述的方法。

15

20

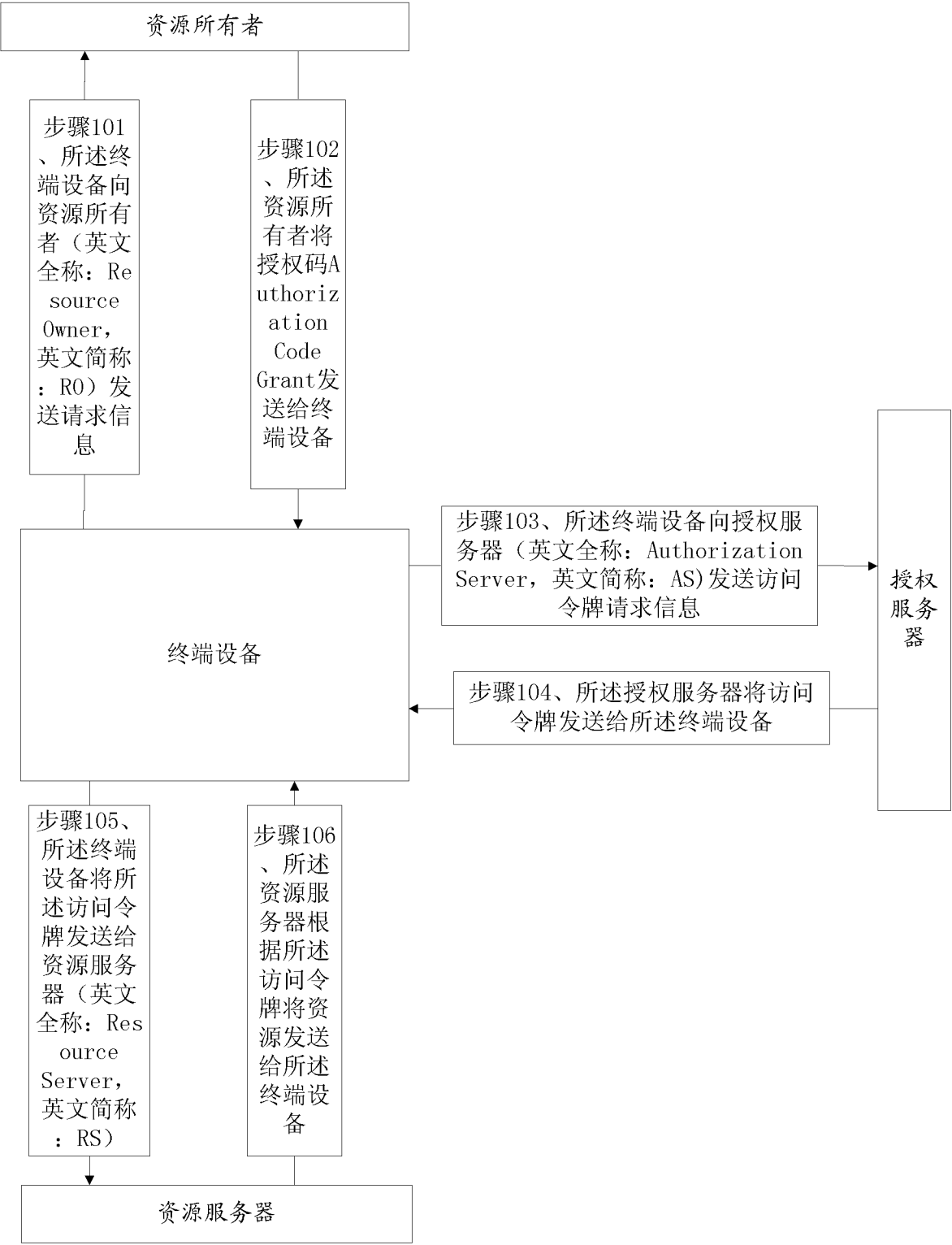


图 1

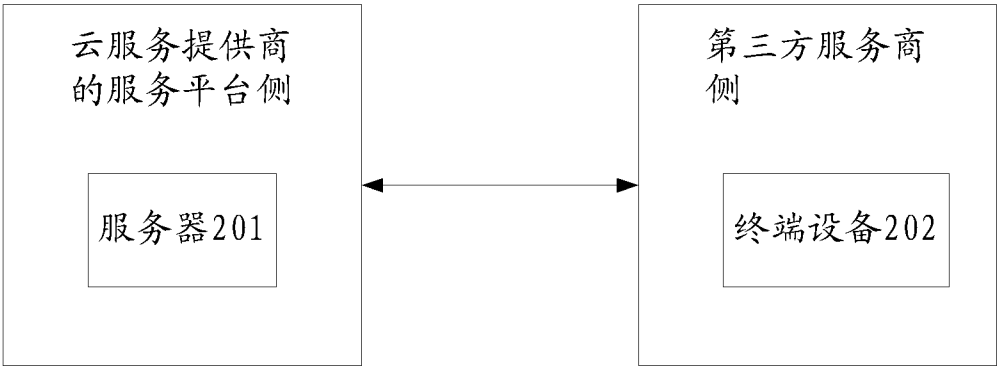


图 2

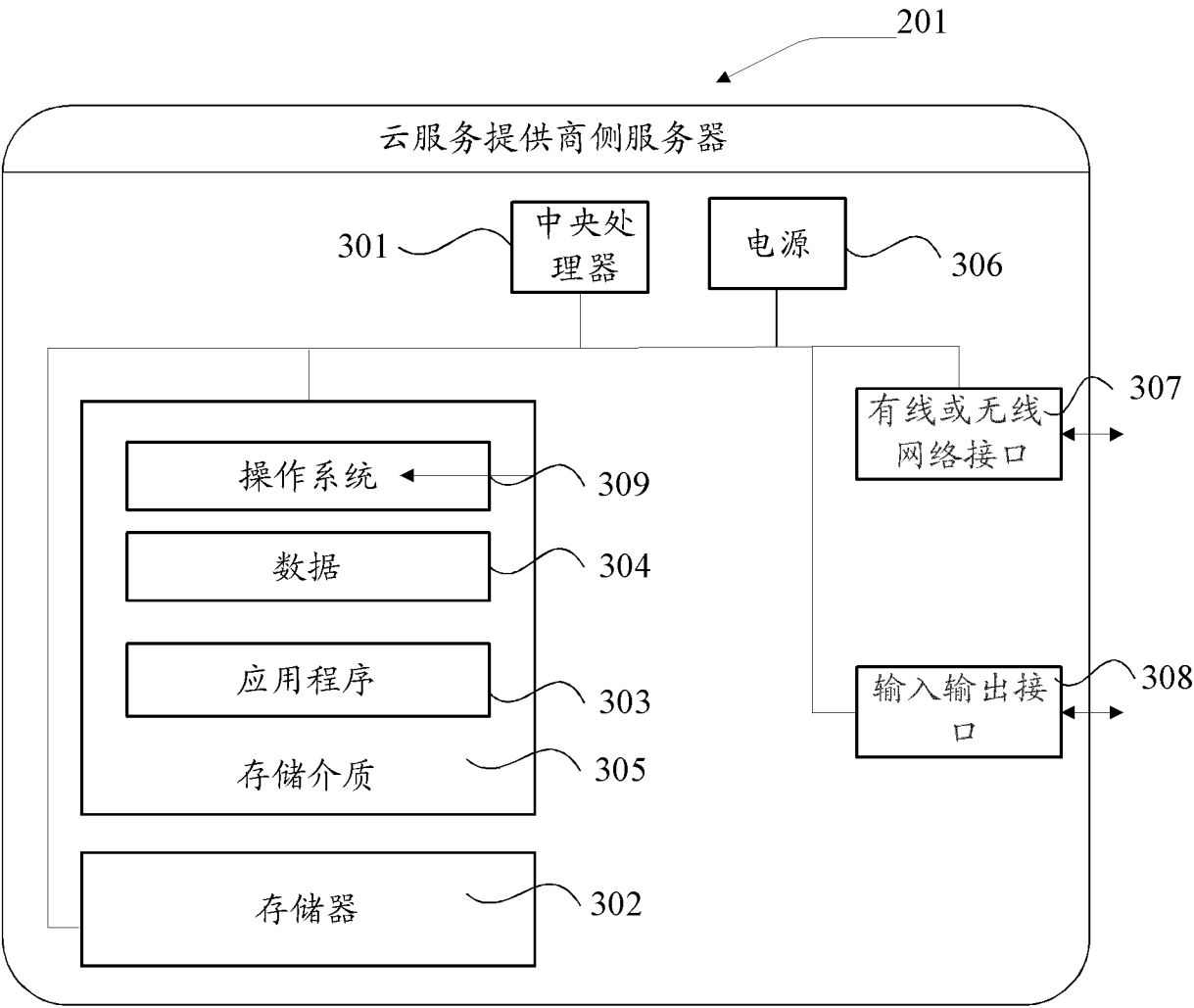


图 3

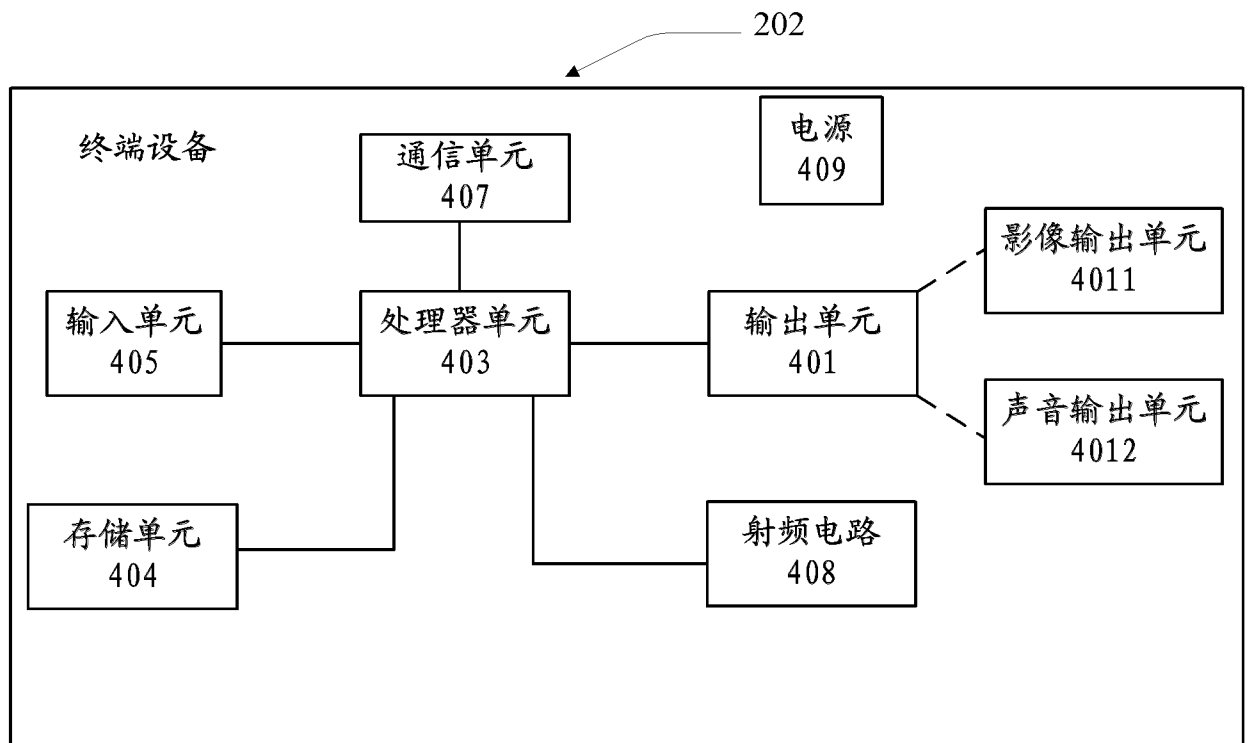


图 4

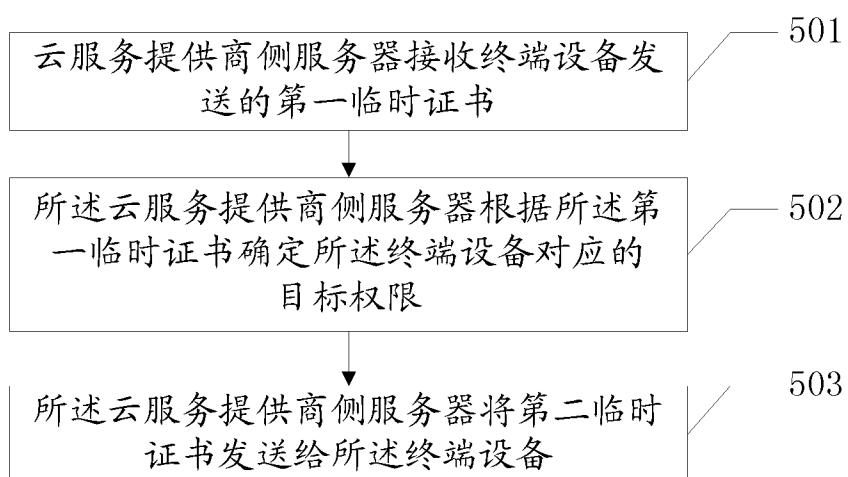


图 5

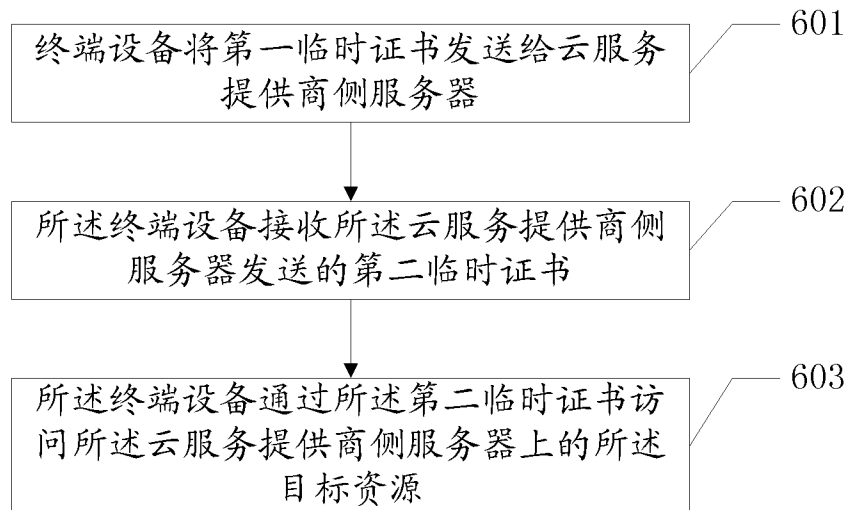


图 6

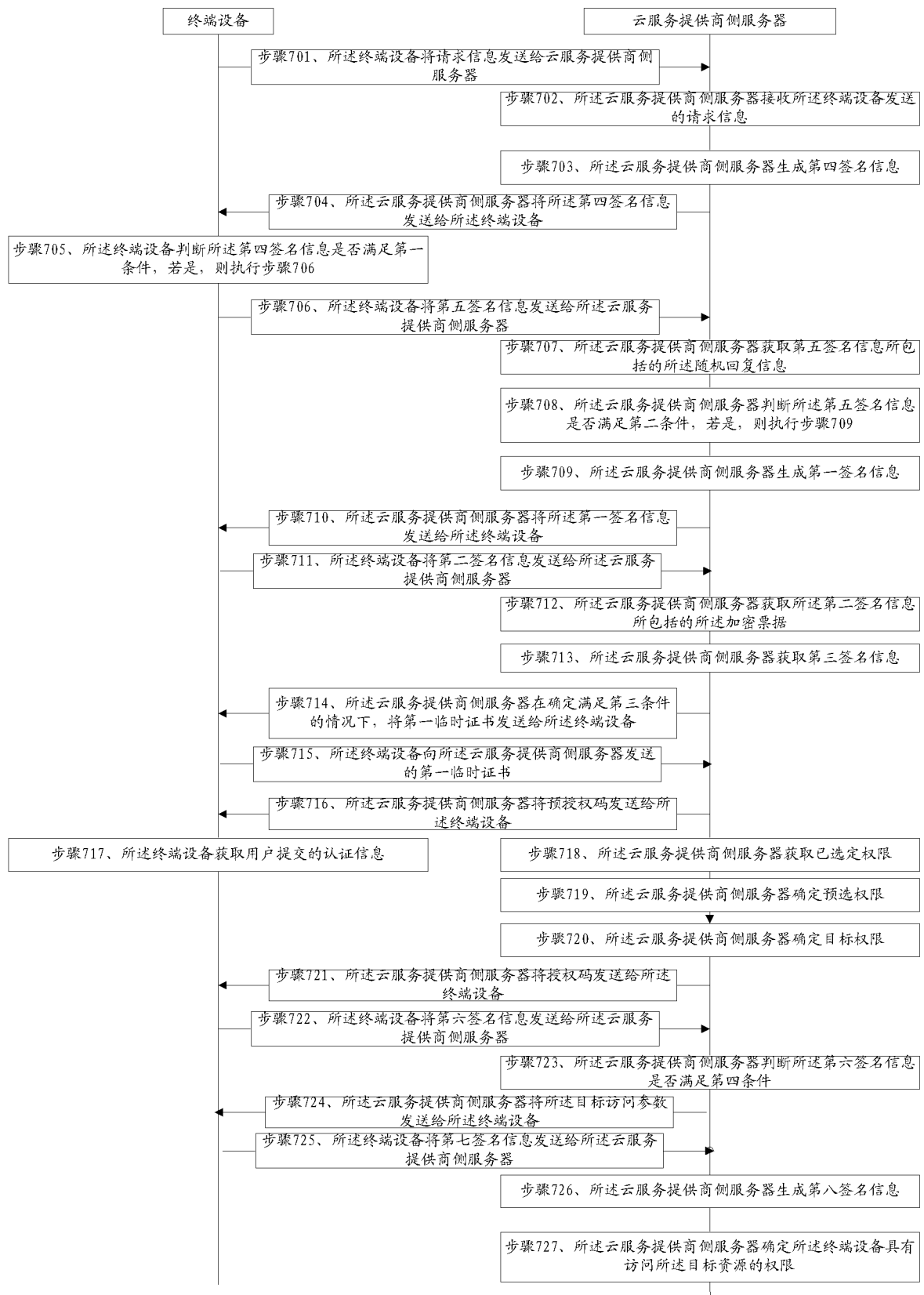


图 7

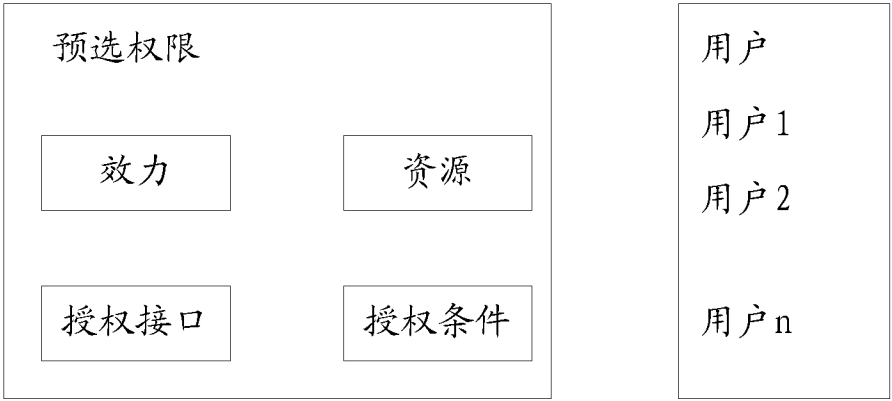


图 8

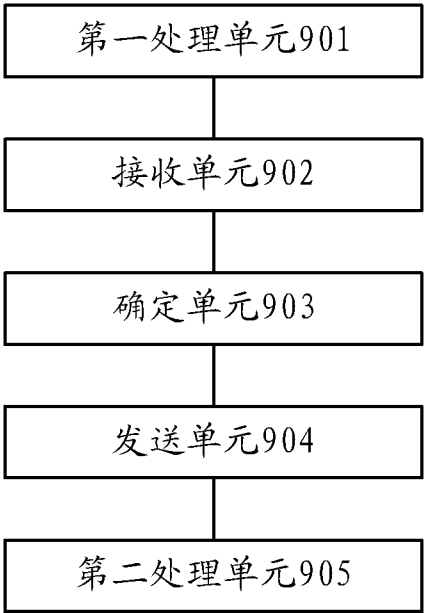


图 9

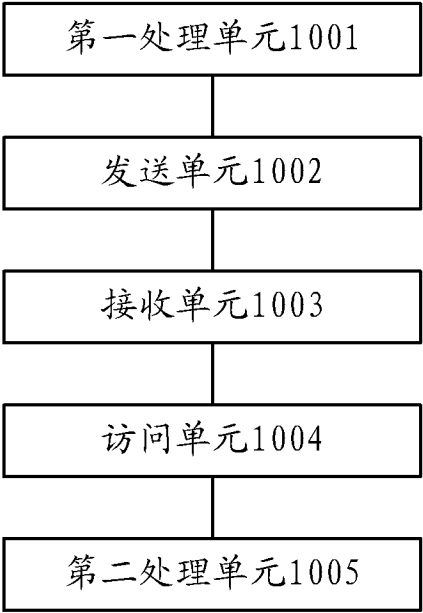


图 10

微信登录

该网页由大众点评开发，向其提供以下
权限即可继续操作

☐

云主机管理权限（云主机重启、申请、查看等）

☐

开发商自定义第三方角色

图 11

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/089039

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)n

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)

H04L; G06F

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)

VEN; SIPOABS; CNTXT; CNABS; CNKI; EPTXT; WOTXT; USTXT: 临时, 期限, 有效, 时间, 证书, 内容, 子, 请求, 权限, temp+, period, time, certificat+, content, domain, request, authori+, CPC: G06F21/10

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 107222485 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 29 September 2017 (2017-09-29) claims 1-15, and description, paragraphs 243-244	1-17
X	CN 101043403 A (XIDIAN UNIVERSITY) 26 September 2007 (2007-09-26) description, page 6, paragraph 3 to page 8, paragraph 4	1-17
A	CN 102057382 A (MICROSOFT CORPORATION) 11 May 2011 (2011-05-11) entire document	1-17
A	US 2003125012 A1 (ALLEN, L.S. ET AL.) 03 July 2003 (2003-07-03) entire document	1-17

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

“&” document member of the same patent family

Date of the actual completion of the international search

13 August 2018

Date of mailing of the international search report

22 August 2018

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

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/089039

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107222485	A	29 September 2017	None			
CN	101043403	A	26 September 2007	None			
CN	102057382	A	11 May 2011	CN	102057382	B	03 December 2014
				JP	2011525014	A	08 September 2011
				EP	2308005	A2	13 April 2011
				RU	2010149880	A	10 June 2012
				KR	20110036529	A	07 April 2011
				EP	2308005	A4	21 June 2017
				WO	2009149019	A3	25 February 2010
				WO	2009149019	A2	10 December 2009
				US	2009307759	A1	10 December 2009
				JP	5491499	B2	14 May 2014
				IN	201007746	P4	26 August 2011
US	2003125012	A1	03 July 2003	JP	2003281234	A	03 October 2003

国际检索报告

国际申请号

PCT/CN2018/089039

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)n

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)

H04L; G06F

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))

VEN;SIPOABS;CNTXT;CNABS;CNKI;EPTXT;WOTXT;USTXT:临时, 期限, 有效, 时间, 证书, 内容, 子, 请求, 权限, temp+, period, time, certificat+, content, domain, request, authori+, CPC: G06F21/10

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
PX	CN 107222485 A (腾讯科技深圳有限公司) 2017年 9月 29日 (2017 - 09 - 29) 权利要求1-15, 说明书第243-244段	1-17
X	CN 101043403 A (西安电子科技大学) 2007年 9月 26日 (2007 - 09 - 26) 说明书第6页第3段-第8页第4段	1-17
A	CN 102057382 A (微软公司) 2011年 5月 11日 (2011 - 05 - 11) 全文	1-17
A	US 2003125012 A1 (ALLEN, L. S. 等) 2003年 7月 3日 (2003 - 07 - 03) 全文	1-17

☐ 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

2018年 8月 13日

国际检索报告邮寄日期

2018年 8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

受权官员

蔡茹辛

传真号 (86-10)62019451

电话号码 86-(010)-62089151

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/089039

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	107222485	A	2017年 9月 29日	无			
CN	101043403	A	2007年 9月 26日	无			
CN	102057382	A	2011年 5月 11日	CN	102057382	B	2014年 12月 3日
				JP	2011525014	A	2011年 9月 8日
				EP	2308005	A2	2011年 4月 13日
				RU	2010149880	A	2012年 6月 10日
				KR	20110036529	A	2011年 4月 7日
				EP	2308005	A4	2017年 6月 21日
				WO	2009149019	A3	2010年 2月 25日
				WO	2009149019	A2	2009年 12月 10日
				US	2009307759	A1	2009年 12月 10日
				JP	5491499	B2	2014年 5月 14日
				IN	201007746	P4	2011年 8月 26日
US	2003125012	A1	2003年 7月 3日	JP	2003281234	A	2003年 10月 3日

表 PCT/ISA/210 (同族专利附件) (2015年1月)