

(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
2020 年 5 月 7 日 (07.05.2020)



(10) 国际公布号
WO 2020/087778 A1

(51) 国际专利分类号:

H04L 29/06 (2006.01)

(部位: 自编 01-03 和 08-12 单元) (仅限办公用途), Guangdong 510623 (CN)。

(21) 国际申请号:

PCT/CN2019/070885

(22) 国际申请日:

2019 年 1 月 8 日 (08.01.2019)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

201811302719.5 2018 年 11 月 2 日 (02.11.2018) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。

(72) 发明人: 方思行(FANG, Sixing); 中国广东省深圳市前海深港合作区前湾一路 1 号 A 栋 201 室, Guangdong 518052 (CN)。

(74) 代理人: 广州华进联合专利商标代理有限公司(ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区珠江东路 6 号 4501 房

(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, 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)。

(54) Title: MULTIPLE SYSTEM LOGIN METHOD, APPARATUS, COMPUTER DEVICE AND STORAGE MEDIUM

(54) 发明名称: 多系统登录方法、装置、计算机设备和存储介质

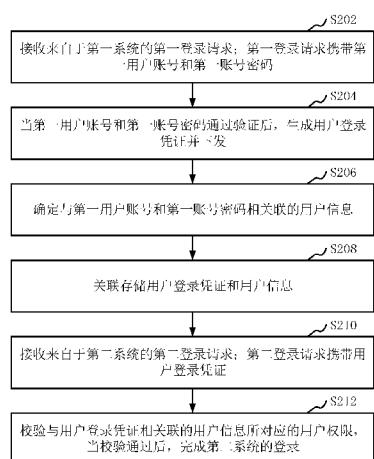


图 2

(57) Abstract: A multiple system login method, comprising: receiving a first login request from a first system; the first login request carrying a first user account number and a first account number password; after the first user account number and the first account number password pass verification, generating and issuing a user login certificate; determining user information associated with the first user account number and the first account number password; associatively storing the user login certificate and the user information; receiving a second login request from a second system; the second login request carrying a user login certificate; cross-checking a user permission corresponding to user information associated with the user login certificate, and after cross-checking is passed, completing login to the second system.

(57) 摘要: 一种多系统登录方法, 包括: 接收来自于第一系统的第一登录请求; 所述第一登录请求携带第一用户账号和第一账号密码; 当所述第一用户账号和第一账号密码通过验证后, 生成用户登录凭证并下发; 确定与所述第一用户账号和第一账号密码相关联的用户信息; 关联存储所述用户登录凭证和所述用户信息; 接收来自于第二系统的第二登录请求; 所述第二登录请求携带用户登录凭证; 及校验与所述用户登录凭证相关联的用户信息所对应的用户权限, 当校验通过后, 完成所述第二系统的登录。

- S202 Receive a first login request from a first system; the first login request carries a first user account number and a first account number password
- S204 After the first user account number and the first account number password pass verification, generate and issue a user login certificate
- S206 Determine user information associated with the first user account number and the first account number password
- S208 Associatively store the user login certificate and the user information
- S210 Receive a second login request from a second system; the second login request carries a user login certificate
- S212 Cross-check a user permission corresponding to user information associated with the user login certificate, and after cross-checking is passed, complete login to the second system

本国际公布：

- 包括国际检索报告(条约第21条(3))。

发明名称：多系统登录方法、装置、计算机设备和存储介质

相关申请的交叉引用

本申请要求于 2018 年 11 月 02 日提交中国专利局，申请号为 201811302719.5，申请名称为“多系统登录方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及一种多系统方法、装置、计算机设备和存储介质。

背景技术

随着计算机技术的发展，越来越多的业务都可通过计算机设备来实现和完成。对于不同的业务通常需要登录各自对应的业务系统，才能进行相应的操作。而每个业务系统的系统登录、鉴权和认证方法等通常是每个系统独立执行。

然而，发明人意识到，传统的多系统登录，通常是对于不同的业务系统，在登录时分别输入相应的用户账号和账号密码，在认证通过后，才能登录相应的业务系统。这样虽然可以登录多个业务系统，但是当用户需登录的业务系统过多的时候，登录每个业务系统都需要输入相应的用户名和密码，操作繁琐，导致多系统登录效率低。

发明内容

根据本申请公开的各种实施例，提供一种多系统登录方法、装置、计算机设备和存储介质。

一种多系统登录方法，由认证服务器执行，所述方法包括：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

一种多系统登录装置，包括：

接收模块，用于接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用

户账号和第一账号密码；

生成模块，用于当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定模块，用于确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储模块，用于关联存储所述用户登录凭证和所述用户信息；

所述接收模块还用于接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验模块，用于校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

一种计算机设备，包括存储器和一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述处理器执行时，使得所述一个或多个处理器执行以下步骤：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器执行以下步骤：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请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申请的一些实施例，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它的附图。

图 1 为根据一个或多个实施例中多系统登录方法的应用场景图。

图 2 为根据一个或多个实施例中多系统登录方法的流程示意图。

图 3 为根据一个或多个实施例中多系统登录方法的时序图。

图 4 为根据一个或多个实施例中多系统登录装置的框图。

图 5 为另一个实施例中多系统登录装置的框图。

图 6 为根据一个或多个实施例中计算机设备的框图。

具体实施方式

为了使本申请的技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

本申请提供的多系统登录方法，可以应用于如图 1 所示的应用环境中。终端 110 通过网络与业务系统 120 通过网络进行通信。业务系统 120 包括多个系统，如第一系统 121 和第二系统 122 等。业务系统 120 和认证服务器 130 通过网络连接。终端 110 向第一系统 121 发送携带有第一用户账号和第一账号密码的第一登录请求，第一系统 121 将第一登录请求转发至认证服务器 130。认证服务器 130 对第一用户账号和第一账号密码进行验证，验证通过后生成用户登录凭证并下发至终端 110。终端 110 向第二系统 122 发送携带有用户登录凭证的第二登录请求，第二系统 122 将第二登录请求转发至认证服务器 130。认证服务器 130 对与用户登录凭证关联的用户信息进行校验，校验通过后，完成第二系统的登录。

其中，终端 110 可以但不限于各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备。业务系统 120 可以是独立的服务器或服务器集群来实现。其中，第一系统和第二系统用来区分不同的业务系统，在不引起歧义的前提下第一系统和第二系统都可以称为业务系统。认证服务器 130 可以用独立的服务器或者是多个服务器组成的服务器集群来实现。

在一些实施例中，如图 2 所示，提供了一种多系统登录方法，以该方法应用于图 1 中的认证服务器 130 为例进行说明，包括以下步骤：

S202，接收来自于第一系统的第一登录请求；第一登录请求携带第一用户账号和第一账号密码。

其中，第一系统是业务系统，具体可以是第一业务服务器。第一登录请求是通过用户账号登录第一业务服务器时所触发的登录请求。认证服务器是与多个业务系统相对应的、

且用于提供对登录各系统的用户账号进行验证服务的服务器。

具体地，用户可通过终端触发登录第一系统的第一登录请求，第一系统将接收到的第一登录请求转发至认证服务器。认证服务器可通过网络连接接收来自于第一系统的第一登录请求。其中，第一登录请求携带第一用户账号和第一账号密码。

在一些实施例中，终端上运行有浏览器应用，终端可通过浏览器应用进入与第一系统所对应的登录界面。用户在登录界面中输入第一用户账号和第一账号密码。终端根据第一用户账号和第一账号密码生成登录请求。终端可检测触发发送登录请求的触发操作，当检测到触发操作时，向第一系统发送登录请求。

其中，其中，触发操作是作用于登录界面的预设操作，检测到触发操作将触发发送登录请求。触发操作具体可以是触摸操作、光标操作、按键操作或者语音操作。其中，触摸操作可以是触摸点击操作、触摸按压操作或者触摸滑动操作，触摸操作可以是单点触摸操作或者多点触摸操作；光标操作可以是控制光标进行点击的操作或者控制光标进行按压的操作；按键操作可以是虚拟按键操作或者实体按键操作等。

S204，当第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发。

其中，用户登录凭证是用于验证用户身份的凭证，具体可以字母、数字、汉字或字符串等。认证服务器接收来自于不同用户账号所对应的登录请求，生成不同的用户登录凭证。用户登录凭证可以是随机生成的，这样，可以保障认证服务器每接收一次第一登录请求，就生成唯一的用户登录凭证。

具体地，认证服务器在接收到携带有第一用户账号和第一账号密码的第一登录请求后，根据与存储的用户账号和相应的账号密码进行比对验证。当第一用户账号和第一账号密码通过账号验证后，认证服务器则随机生成相应的用户登录凭证。响应于第一登录请求，认证服务器将用户登录凭证下发至第一系统，第一系统再将用户登录凭证转发至终端。终端将接收到的用户登录凭证存储至浏览器的 cookie 中。

在一些实施例中，在用户注册账号时，认证服务器可将用户账号、账号密码、以及用户信息（比如，与用户账号绑定的手机号或用户的身份证后 6 位等信息）进行关联存储。当认证服务器接收到第一登录请求后，可根据预先存储的用户账号及账号密码进行核对。核对通过后才生成用户登录凭证。

S206，确定与第一用户账号和第一账号密码相关联的用户信息。

其中，用户信息是和用户身份相关的信息，具体可以是用户的手机号码、唯一身份证号、唯一身份证号的后六位、与用户唯一绑定的字符串等。具体地，在用户注册账号时，认证服务器可将用户账号、账号密码、以及用户信息进行关联，并存储至数据库中。认证服务器可从数据库中查找与第一用户账号和第一账号密码相关联的用户信息。

可以理解的是，用户信息是用户在注册多个相关联的系统时必须输入的信息，且对于同一个用户，在注册多个系统相对应的用户账号时，所输入的用户信息是一样的。这样，才便于后根据用户信息校验用户的身份。

S208, 关联存储用户登录凭证和用户信息。

具体地, 认证服务器在生成用户登录凭证后, 可获取与第一用户账号相关联的用户信息, 认证服务器可将用户登录凭证和相应的用户信息进行关联, 并将关联后的用户登录凭证及用户信息以 key-value (关键字-值) 的形式存储至 Redis 数据库 (Redis 数据库是一种 key-value 的存储系统) 中。其中, Redis 数据库可以架构在认证服务器中, 也可以架构在其他关联的服务器中。

S210, 接收来自于第二系统的第二登录请求; 第二登录请求携带用户登录凭证。

其中, 第二系统是业务系统, 具体可以是第二业务服务器。第二登录请求是通过用户登录凭证登录第二业务服务器时所触发的登录请求。具体地, 认证服务器可通过网络连接接收来自于第二系统的第二登录请求。其中, 第二登录请求携带用户登录凭证。

在一些实施例中, 终端上运行有浏览器应用, 终端可通过浏览器应用进入与第二系统所对应的登录界面。当用户通过浏览器应用登录第二系统时, 终端从浏览器的 cookie (缓存) 中获取用户登录凭证。终端向第二系统发送携带有用户登录凭证的第二登录请求。第二系统将该登录请求转发至认证服务器。

在一些实施例中, 第二登录请求的生成步骤包括: 终端接收认证服务器下发的用户登录凭证; 终端将用户登录凭证存储至浏览器缓存中; 终端接收用户通过浏览器触发的针对于第二系统的登录指令; 终端根据登录指令, 从浏览器缓存中查找用户登录凭证; 当终端查找到用户登录凭证时, 向认证服务器发送携带有用户登录凭证的第二登录请求。

在一些实施例中, 用户通过终端以第一用户账号成功登录第一系统时, 会接收认证服务器下发的用户登录凭证。终端可将用户登录凭证存储至浏览器缓存中。当用户通过浏览器登录第二系统时, 终端接收用户通过浏览器触发的针对于第二系统的登录指令, 并根据登录指令, 从浏览器缓存中查找用户登录凭证。查找到用户登录凭证时, 根据用户登录凭证生成第二登录请求。终端将第二登录请求发送至第二系统, 第二系统将第二登录请求转发至认证服务器。

上述实施例中, 通过浏览器登录第二系统时, 则无需用户输入相应的用户账号和账号密码, 只需终端查找到用户登录凭证, 通过用户登录凭证即可登录第二系统, 方便快捷。

S212, 校验与用户登录凭证相关联的用户信息所对应的用户权限, 当校验通过后, 完成第二系统的登录。

具体地, 认证服务器在接收到携带有用户登录凭证的第二登录请求时, 从第二登录请求中提取用户登录凭证。认证服务器在本地查找该用户登录凭证。当查找到该用户登录凭证后, 确定与该用户登录凭证相关联的用户信息。

进一步地, 认证服务器可确定与该用户信息所对应的用户权限, 当与该用户信息所对应的用户权限为允许访问权限时, 则校验通过, 完成第二系统的登录。并将校验通过的信息反馈至第二系统。第二系统接收到校验通过的信息后可允许该终端的访问。

在一些实施例中, 终端通过用户账号成功登录第一系统后, 认证服务器生成用户登

录凭证，且将用户登录凭证和用户信息关联存储至 Redis 数据库中。此时，可以认为 Redis 数据库中的用户登录凭证是有效的。与该用户信息相应的用户可直接通过用户登录凭证登录第二系统（登录后的用户账号是与用户信息相关联的第二用户账号）。因此，当认证服务器根据用户登录凭证在 Redis 数据库中查找到与用户登录凭证对应的用户信息时，即可认为该用户信息所对应的用户权限为允许访问权限。

在一些实施例中，步骤 S212，也就是校验与用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成第二系统的登录的步骤具体包括以下步骤：确定与第二登录请求所携带的用户登录凭证相关联的用户信息；根据用户信息，查找与第二系统相对应的第二用户账号和第二账号密码；当查找到第二用户账号和第二账号密码时，则判定校验通过并完成第二系统的登录。

具体地，认证服务器可从 Redis 数据库中查找与该用户登录凭证相关联的用户信息。根据预先存储的用户账号和关联的用户信息，确定与该用户信息对应的第二用户账号和第二账号密码。其中，第二用户账号和第二账号密码用于登录第二系统。当认证服务器从本地查找到第二用户账号和第二账号密码时，则判定校验通过，向第二业务反馈认证通过的反馈信息，以完成第二系统的登录。

可以理解的是，第一系统和第二系统在不引起歧义的前提均下可以称作业务系统。其中，多个业务系统相关联，当用户以用户账号和账号密码登录多个相关联的业务系统中的一个业务系统时，该业务系统可以称作第一业务系统。当用户以用户登录凭证登录该多个系统中的其他业务系统时，该其他的业务系统可以称作第二系统。可以理解的是，第二系统可以有多个、且第一系统和第二系统并不唯一。

上述多系统登录方法，当第一系统通过登录验证后，认证服务器生成用户登录凭证并下发。认证服务器将用户信息与用户登录凭证关联存储，使得用户在登录第二系统时，可通过用户登录凭证来进行登录。这样，认证服务器只需校验与用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，即可完成第二系统的登录。这样，将业务系统和认证服务器独立开来，当用户需登录多个不同的系统时，无需在登录每个系统时都输入用户账号和账号密码，只需通过用户登录凭证即可登录多个系统，在保障多系统登录的安全性的前提下，减少了登录多个系统的操作，大大提高了多系统登录的效率。

在一些实施例中，在步骤 S202 之前，也就是接收来自于第一系统的第一登录请求的步骤之前，该多系统登录方法还包括账号注册的步骤，该步骤包括：分别接收来自于第一系统的第一账号注册请求、以及来自于第二系统的第二账号注册请求；第一账号注册请求携带第一用户账号、第一账号密码、以及用户信息；第二账号注册请求携带第二用户账号、第二账号密码、以及用户信息；验证第一用户账号、第一账号密码、以及用户信息的合法性；当验证通过后，将与第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储；验证第二用户账号、第二账号密码、以及用户信息的合法性；当验证通过后，将与第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。

具体地，用户在登录多系统中的任一系统之前，用户首先得持有该系统的用户账号。用户在初次登录多系统中的任一系统之前，需注册该系统的用户账号。当用户需注册多个关联系统中的任一系统所对应的账号时，用户可在终端展示的账号注册界面中输入用户账号、账号密码、以及用户信息。终端根据用户输入的用户账号、账号密码、以及用户信息生成账号注册请求，并发送至相应的业务系统。业务系统将账号注册请求转发至认证服务器。

可以理解的是，当用户注册与第一系统对应的账号时，用户可在第一系统提供的、且在终端展示的账号注册界面中输入第一用户账号、第一账号密码、以及用户信息。并通过终端，根据第一用户账号、第一账号密码、以及用户信息，生成第一账号注册请求，将第一账号注册请求发送至第一系统。第一系统将第一账号注册请求转发至认证服务器。

当用户注册与第二系统对应的账号时，用户可在第二系统提供的、且在终端展示的账号注册界面中输入第二用户账号、第二账号密码、以及用户信息。并通过终端，根据第二用户账号、第二账号密码、以及用户信息，生成第二账号注册请求，将第二账号注册请求发送至第二系统。第二系统将第二账号注册请求转发至认证服务器。

进一步地，当认证服务器分别接收到与第一业务系统和第二业务系统所对应的第一账号注册请求和第二账号注册请求后，验证相应的第一用户账号、第一账号密码和用户信息的合法性，以及验证相应的第二用户账号、第二账号密码和用户信息的合法性。

进一步地，当第一用户账号、第一账号密码、以及用户信息的合法性验证通过后，认证服务器可将与第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联，并存储在存储介质中。当第二用户账号、第二账号密码、以及用户信息的合法性验证通过后，认证服务器可将与第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联，并存储在存储介质中。

可以理解的是，当认证服务器接收到来自第一系统的第一账号注册请求后，即可验证第一用户账号、第一账号密码、以及用户信息的合法性，并在验证通过后，将与第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储。当认证服务器接收到来自第二系统的第二账号注册请求后，即可验证第二用户账号、第二账号密码、以及用户信息的合法性，并在验证通过后，将与第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。其中，对第一账号注册请求的验证步骤和存储步骤、与对第二账号注册请求的验证步骤和存储步骤的执行次序不做限定，对第一账号注册请求的验证步骤和存储步骤可以在与对第二账号注册请求的验证步骤和存储步骤之前、同时、或之后执行。

在一些实施例中，认证服务器可分别验证第一用户账号和/或第二用户账号是否与现有账号重复、第一账号密码和/或第二账号密码是否符合预设要求、用户信息否有误等。其中，账号密码是否符合预设要求，比如，账号密码是否含有数字、字母、字符等中的至少两种；或账号密码的位数是否达到预设位数等。用户信息否有误，比如，用户信息的位

数是否达到预设位数、用户信息是否真实等。

上述实施例中，在账号注册过程中，认证服务器可分别关联存储与第一系统对应的第一用户账号、第一账号密码和用户信息、以及与第二系统对应的第二用户账号、第二账号密码和用户信息，便于后续登录相应的系统时的登录验证。

在一些实施例中，步骤 S202，也就是当第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发的步骤具体包括以下步骤：当第一用户账号和第一账号密码通过验证后，确定第一系统所对应的系统级别；当系统级别为主系统级别时，则随机生成用户登录凭证；响应于第一登录请求，反馈用户登录凭证。

在一些实施例中，当第一用户账号和第一账号密码通过验证后，认证服务器可向第一系统反馈验证通过的反馈信息。并且，认证服务器可确定第一系统所属的系统级别。当第一系统为主系统时，才可生成用户登录凭证并下发。否则，仅仅反馈第一用户账号和第一账号密码验证通过的反馈信息。

在一些实施例中，认证服务器可预先设定各业务系统所对应的系统级别。其中系统级别包括主系统级别和辅系统级别等。也可根据各业务系统对应的业务内容制定更为详细的系统级别，本实施例在此不做限定。进而，认证服务器可以预先设定，只有通过用户账号和账号密码登录主系统级别的业务系统后，认证服务器才会生成用户登录凭证。也就是只有登录该主业务系统后才能免密访问其它关联的业务系统，如果初次登录的是辅业务系统，那么登录其它关联系统时将仍需输入用户账号和账号密码才能登录。

可以理解的是，处于主系统级别的业务系统可以有多个；处于辅系统级别的业务系统也可以有一个或多个，本实施例在此不做限定。

上述实施例中，认证服务器只有在验证通过主系统所对应的、且携带有用户账号和账号密码的登录请求后，才会生成用户登录凭证，这样，用户在登录其他的系统时才可使用免密快捷的登录方式，大大提高了多系统登录的安全性。

在一些实施例中，该多系统登录方法还包括清除用户登录凭证的步骤，该步骤具体包括：接收用户登录凭证清除指令；用户登录凭证清除指令携带待清除的用户登录凭证；根据用户登录凭证清除指令，从本地查找相应的用户登录凭证；响应于用户登录凭证清除指令，删除查找到的用户登录凭证、以及与用户登录凭证关联存储的用户信息。

具体地，用户登录凭证是有有效期的。当用户登录凭证的有效期到期后，终端可触发用户登录凭证清除指令。认证服务器可接收终端触发的用户登录凭证清除指令，该用户登录凭证清除指令携带待清除的用户登录凭证。认证服务器根据用户登录凭证清除指令，从 Redis 数据库中查找相应的用户登录凭证。当查找到用户登录凭证后，删除查找到的用户登录凭证、以及在 Redis 数据库中存储的与用户登录凭证关联存储的用户信息。

在一些实施例中，当终端接收到认证服务器下发的用户登录凭证后开始计时，当从当前时刻到开始计时的时刻之间的时间段达到预设时长时，可判定该用户登录凭证的有效期到期。此时，终端可自动触发用户登录凭证清除指令。

在一些实施例中，用户登录凭证清除指令的触发步骤包括：终端监测用户触发操作；当终端在预设时段内未检测到用户触发操作时，获取待清除的用户登录凭证；终端触发向认证服务器发送用户登录凭证清除指令的步骤；用户登录凭证清除指令携带待清除的用户登录凭证。

在一些实施例中，终端可定时或实时在浏览器界面中检测来自于用户的触发操作。当终端在预设时段内未检测到用户触发操作时，可从浏览器缓存中查找用户登录凭证，该用户登录凭证即为待清除的用户登录凭证。终端可自动触发向认证服务器发送用户登录凭证清除指令的步骤，其中，用户登录凭证清除指令携带待清除的用户登录凭证。这样，当终端在预设时段内未检测到用户触发操作时，才触发用户登录凭证清除指令，也就是当用户不使用业务系统时才触发用户登录凭证清除指令，保障了多系统使用的安全。

上述实施例中，可根据用户登录凭证清除指令，删除相应的用户登录凭证、以及用户登录凭证关联存储的用户信息，也就是当次的多系统快捷登录已失效，这样通过有限的时效性可以有效地保障快捷登录多系统时的安全性。

参考图 3，图 3 为多系统登录的时序图，在一个具体地实施例中，该多系统登录方法如下描述：首先用户可通过终端触发登录第一系统的第一登录请求，第一登录请求携带有用户账号和账号密码。第一系统将第一登录请求转发至认证服务器。认证服务器验证用户账号和账号密码，当验证通过后，生成用户登录凭证。认证服务器将用户登录凭证反馈至第一系统，第一系统转发至终端。用户通过终端触发登录第二系统的第二登录凭证，第二登录凭证携带有用户登录凭据。第二系统将第二登录请求转发至认证服务器，认证服务器查找与用户登录凭证关联的用户信息，当查找到用户信息时，返回验证通过的反馈信息。第二系统接收反馈信息，并授权终端访问，用户登录成功。

应该理解的是，虽然图 2 的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图 2 中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

在一些实施例中，如图 4 所示，提供了一种多系统登录装置 400，包括：接收模块 401、生成模块 402、确定模块 403、关联存储模块 404 和校验模块 405，其中：

接收模块 401，用于接收来自于第一系统的第一登录请求；第一登录请求携带第一用户账号和第一账号密码。

生成模块 402，用于当第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发。

确定模块 403，用于确定与第一用户账号和第一账号密码相关联的用户信息。

关联存储模块 404，用于关联存储用户登录凭证和用户信息。

接收模块 401 还用于接收来自于第二系统的第二登录请求；第二登录请求携带用户登录凭证。

校验模块 405，用于校验与用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成第二系统的登录。

在一些实施例中，接收模块 401 还用于分别接收来自于第一系统的第一账号注册请求、以及来自于第二系统的第二账号注册请求；第一账号注册请求携带第一用户账号、第一账号密码、以及用户信息；第二账号注册请求携带第二用户账号、第二账号密码、以及用户信息。

校验模块 405 还用于验证第一用户账号、第一账号密码、以及用户信息的合法性。

关联存储模块 404 还用于在验证通过后，将与第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储。

校验模块 405 还用于验证第二用户账号、第二账号密码、以及用户信息的合法性。

关联存储模块 404 还用于在验证通过后，将与第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。

在一些实施例中，生成模块 402 还用于当第一用户账号和第一账号密码通过验证后，确定第一系统所对应的系统级别；当系统级别为主系统级别时，则随机生成用户登录凭证；响应于第一登录请求，反馈用户登录凭证。

在一些实施例中，下发的用户登录凭证用于指示终端接收认证服务器下发的用户登录凭证；终端将用户登录凭证存储至浏览器缓存中；终端接收用户通过浏览器触发的针对于第二系统的登录指令；终端根据登录指令，从浏览器缓存中查找用户登录凭证；当终端查找到用户登录凭证时，向认证服务器发送携带有用户登录凭证的第二登录请求。

在一些实施例中，校验模块 405 还用于确定与第二登录请求所携带的用户登录凭证相关联的用户信息；根据用户信息，查找与第二系统相对应的第二用户账号和第二账号密码；当查找到第二用户账号和第二账号密码时，则判定校验通过并完成第二系统的登录。

在一些实施例中，如图 5 所示，该多系统登录装置 400 还包括查找模块 406、删除模块 407。

接收模块 401 还用于接收用户登录凭证清除指令；用户登录凭证清除指令携带待清除的用户登录凭证。

查找模块 406，用于根据用户登录凭证清除指令，从本地查找相应的用户登录凭证。

删除模块 407，用于响应于用户登录凭证清除指令，删除查找到的用户登录凭证、以及与用户登录凭证关联存储的用户信息。

在一些实施例中，下发的用户登录凭证用于指示终端监测用户触发操作；当终端在预设时段内未检测到用户触发操作时，获取待清除的用户登录凭证；终端触发向认证服务器

发送用户登录凭证清除指令的步骤；用户登录凭证清除指令携带待清除的用户登录凭证。

上述多系统登录装置，当第一系统通过登录验证后，认证服务器生成用户登录凭证并下发。认证服务器将用户信息与用户登录凭证关联存储，使得用户在登录第二系统时，可通过用户登录凭证来进行登录。这样，认证服务器只需校验与用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，即可完成第二系统的登录。这样，将业务系统和认证服务器独立开来，当用户需登录多个不同的系统时，无需在登录每个系统时都输入用户账号和账号密码，只需通过用户登录凭证即可登录多个系统，在保障多系统登录的安全性的前提下，减少了登录多个系统的操作，大大提高了多系统登录的效率。

关于多系统登录装置的具体限定可以参见上文中对于多系统登录方法的限定，在此不再赘述。上述多系统登录装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一些实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图6所示。该计算机设备包括通过系统总线连接的处理器、存储器、网络接口和数据库。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性计算机可读存储介质、内存储器。该非易失性计算机可读存储介质存储有操作系统、计算机可读指令和数据库。该内存储器为非易失性计算机可读存储介质中的操作系统和计算机可读指令的运行提供环境。该计算机设备的数据库用于存储数据。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机可读指令被处理器执行时以实现一种多系统登录方法。

本领域技术人员可以理解，图6中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

一种计算机设备，包括存储器和一个或多个处理器，存储器中存储有计算机可读指令，计算机可读指令被处理器执行时实现本申请任意一个实施例中提供的多系统登录方法的步骤。

一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，计算机可读指令被一个或多个处理器执行时，使得一个或多个处理器实现本申请任意一个实施例中提供的多系统登录方法的步骤。

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，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读存储介质中，该计算机可读指令在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器

(ROM)、可编程 ROM (PROM)、电可编程 ROM (EPROM)、电可擦除可编程 ROM (EEPROM) 或闪存。易失性存储器可包括随机存取存储器 (RAM) 或者外部高速缓冲存储器。作为说明而非局限, RAM 以多种形式可得, 诸如静态 RAM (SRAM)、动态 RAM (DRAM)、同步 DRAM (SDRAM)、双数据率 SDRAM (DDRSDRAM)、增强型 SDRAM (ESDRAM)、同步链路 (Synchlink) DRAM (SLDRAM)、存储器总线 (Rambus) 直接 RAM (RDRAM)、直接存储器总线动态 RAM (DRDRAM)、以及存储器总线动态 RAM (RDRAM) 等。

以上实施例的各技术特征可以进行任意的组合, 为使描述简洁, 未对上述实施例中的各个技术特征所有可能的组合都进行描述, 然而, 只要这些技术特征的组合不存在矛盾, 都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式, 其描述较为具体和详细, 但并不能因此而理解为对发明专利范围的限制。应当指出的是, 对于本领域的普通技术人员来说, 在不脱离本申请构思的前提下, 还可以做出若干变形和改进, 这些都属于本申请的保护范围。因此, 本申请专利的保护范围应以所附权利要求为准。

权利要求书

1、一种多系统登录方法，由认证服务器执行，所述方法包括：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

2、根据权利要求1所述的方法，其特征在于，还包括：

分别接收来自于所述第一系统的第一账号注册请求、以及来自于所述第二系统的第二账号注册请求；所述第一账号注册请求携带第一用户账号、第一账号密码、以及用户信息；所述第二账号注册请求携带第二用户账号、第二账号密码、以及用户信息；

验证所述第一用户账号、第一账号密码、以及用户信息的合法性；

在验证通过后，将与所述第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储；

验证所述第二用户账号、第二账号密码、以及用户信息的合法性；及

在验证通过后，将与所述第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。

3、根据权利要求1所述的方法，其特征在于，所述当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发，包括：

当所述第一用户账号和第一账号密码通过验证后，确定所述第一系统所对应的系统级别；

当所述系统级别为主系统级别时，则随机生成用户登录凭证；及

响应于所述第一登录请求，反馈所述用户登录凭证。

4、根据权利要求1所述的方法，其特征在于，所述第二登录请求的生成步骤包括：

终端接收所述认证服务器下发的用户登录凭证；

所述终端将所述用户登录凭证存储至浏览器缓存中；

所述终端接收用户通过浏览器触发的针对于所述第二系统的登录指令；

所述终端根据所述登录指令，从所述浏览器缓存中查找用户登录凭证；及

当所述终端查找到所述用户登录凭证时，向所述认证服务器发送携带有用户登录凭证的第二登录请求。

5、根据权利要求2所述的方法，其特征在于，所述校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录，包括：

确定与所述第二登录请求所携带的用户登录凭证相关联的用户信息；
根据所述用户信息，查找与所述第二系统相对应的第二用户账号和第二账号密码；及
当查找到所述第二用户账号和第二账号密码时，则判定校验通过并完成所述第二系统的登录。

6、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，还包括：

接收用户登录凭证清除指令；所述用户登录凭证清除指令携带待清除的用户登录凭证；

根据所述用户登录凭证清除指令，从本地查找相应的用户登录凭证；及

响应于所述用户登录凭证清除指令，删除查找到的用户登录凭证、以及与所述用户登录凭证关联存储的所述用户信息。

7、根据权利要求 6 所述的方法，其特征在于，所述用户登录凭证清除指令的触发步骤包括：

终端监测用户触发操作；

当所述终端在预设时段内未检测到所述用户触发操作时，获取待清除的用户登录凭证；及

所述终端触发向所述认证服务器发送用户登录凭证清除指令的步骤；所述用户登录凭证清除指令携带所述待清除的用户登录凭证。

8、一种多系统登录装置，包括：

接收模块，用于接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

生成模块，用于当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定模块，用于确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储模块，用于关联存储所述用户登录凭证和所述用户信息；

所述接收模块还用于接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验模块，用于校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

9、一种计算机设备，包括存储器及一个或多个处理器，所述存储器中储存有计算机可读指令，所述计算机可读指令被所述一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

10、根据权利要求 9 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

分别接收来自于所述第一系统的第一账号注册请求、以及来自于所述第二系统的第二账号注册请求；所述第一账号注册请求携带第一用户账号、第一账号密码、以及用户信息；所述第二账号注册请求携带第二用户账号、第二账号密码、以及用户信息；

验证所述第一用户账号、第一账号密码、以及用户信息的合法性；

在验证通过后，将与所述第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储；

验证所述第二用户账号、第二账号密码、以及用户信息的合法性；及

在验证通过后，将与所述第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。

11、根据权利要求 9 所述的计算机设备，其特征在于，所述计算机可读指令使得所述处理器在执行所述当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发时执行以下步骤：

当所述第一用户账号和第一账号密码通过验证后，确定所述第一系统所对应的系统级别；

当所述系统级别为主系统级别时，则随机生成用户登录凭证；及

响应于所述第一登录请求，反馈所述用户登录凭证。

12、根据权利要求 9 所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

终端接收所述认证服务器下发的用户登录凭证；

所述终端将所述用户登录凭证存储至浏览器缓存中；

所述终端接收用户通过浏览器触发的针对于所述第二系统的登录指令；

所述终端根据所述登录指令，从所述浏览器缓存中查找用户登录凭证；及

当所述终端查找到所述用户登录凭证时，向所述认证服务器发送携带有用户登录凭证的第二登录请求。

13、根据权利要求 10 所述的计算机设备，其特征在于，所述计算机可读指令使得所述处理器在执行所述校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录时执行以下步骤：

确定与所述第二登录请求所携带的用户登录凭证相关联的用户信息；

根据所述用户信息，查找与所述第二系统相对应的第二用户账号和第二账号密码；及

当查找到所述第二用户账号和第二账号密码时，则判定校验通过并完成所述第二系统的登录。

14、根据权利要求 9 至 13 中任一项所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

接收用户登录凭证清除指令；所述用户登录凭证清除指令携带待清除的用户登录凭证；

根据所述用户登录凭证清除指令，从本地查找相应的用户登录凭证；及

响应于所述用户登录凭证清除指令，删除查找到的用户登录凭证、以及与所述用户登录凭证关联存储的所述用户信息。

15、一个或多个存储有计算机可读指令的非易失性计算机可读存储介质，所述计算机可读指令被一个或多个处理器执行时，使得所述一个或多个处理器执行以下步骤：

接收来自于第一系统的第一登录请求；所述第一登录请求携带第一用户账号和第一账号密码；

当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发；

确定与所述第一用户账号和第一账号密码相关联的用户信息；

关联存储所述用户登录凭证和所述用户信息；

接收来自于第二系统的第二登录请求；所述第二登录请求携带用户登录凭证；及

校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录。

16、根据权利要求 15 所述的存储介质，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

分别接收来自于所述第一系统的第一账号注册请求、以及来自于所述第二系统的第二账号注册请求；所述第一账号注册请求携带第一用户账号、第一账号密码、以及用户信息；所述第二账号注册请求携带第二用户账号、第二账号密码、以及用户信息；

验证所述第一用户账号、第一账号密码、以及用户信息的合法性；

在验证通过后，将与所述第一系统对应的第一用户账号、第一账号密码、以及用户信息进行关联存储；

验证所述第二用户账号、第二账号密码、以及用户信息的合法性；及

在验证通过后，将与所述第二系统对应的第二用户账号、第二账号密码、以及用户信息进行关联存储。

17、根据权利要求 15 所述的存储介质，其特征在于，所述计算机可读指令使得所述处理器在执行所述当所述第一用户账号和第一账号密码通过验证后，生成用户登录凭证并下发时执行以下步骤：

当所述第一用户账号和第一账号密码通过验证后，确定所述第一系统所对应的系统级别；

当所述系统级别为主系统级别时，则随机生成用户登录凭证；及
响应于所述第一登录请求，反馈所述用户登录凭证。

18、根据权利要求 15 所述的存储介质，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

终端接收所述认证服务器下发的用户登录凭证；

所述终端将所述用户登录凭证存储至浏览器缓存中；

所述终端接收用户通过浏览器触发的针对于所述第二系统的登录指令；

所述终端根据所述登录指令，从所述浏览器缓存中查找用户登录凭证；及

当所述终端查找到所述用户登录凭证时，向所述认证服务器发送携带有用户登录凭证的第二登录请求。

19、根据权利要求 16 所述的存储介质，其特征在于，所述计算机可读指令使得所述处理器在执行所述校验与所述用户登录凭证相关联的用户信息所对应的用户权限，当校验通过后，完成所述第二系统的登录时执行以下步骤：

确定与所述第二登录请求所携带的用户登录凭证相关联的用户信息；

根据所述用户信息，查找与所述第二系统相对应的第二用户账号和第二账号密码；及

当查找到所述第二用户账号和第二账号密码时，则判定校验通过并完成所述第二系统的登录。

20、根据权利要求 15 至 19 中任一项所述的存储介质，其特征在于，所述处理器执行所述计算机可读指令时还执行以下步骤：

接收用户登录凭证清除指令；所述用户登录凭证清除指令携带待清除的用户登录凭证；

根据所述用户登录凭证清除指令，从本地查找相应的用户登录凭证；及

响应于所述用户登录凭证清除指令，删除查找到的用户登录凭证、以及与所述用户登录凭证关联存储的所述用户信息。

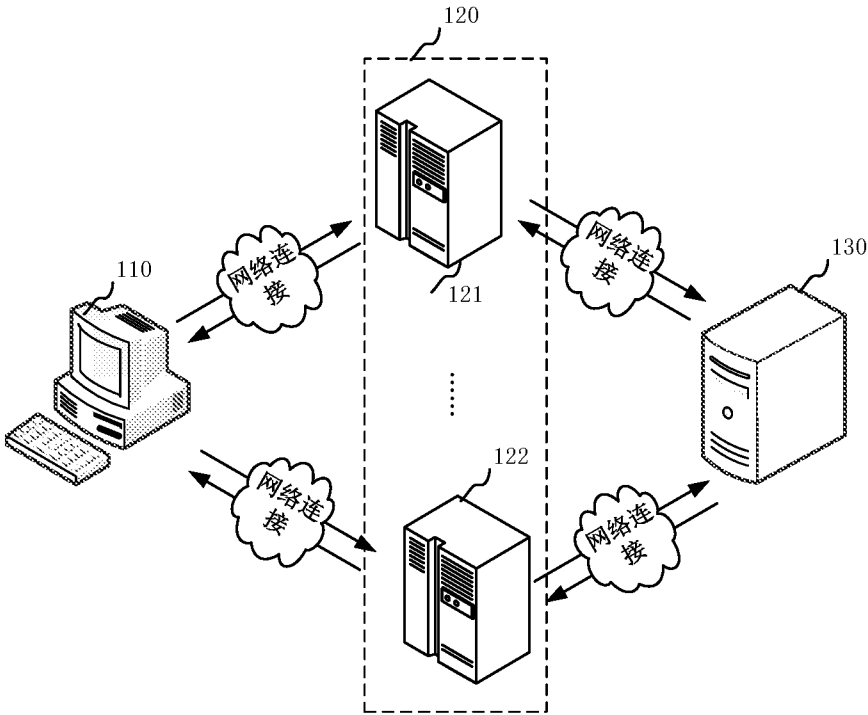


图 1

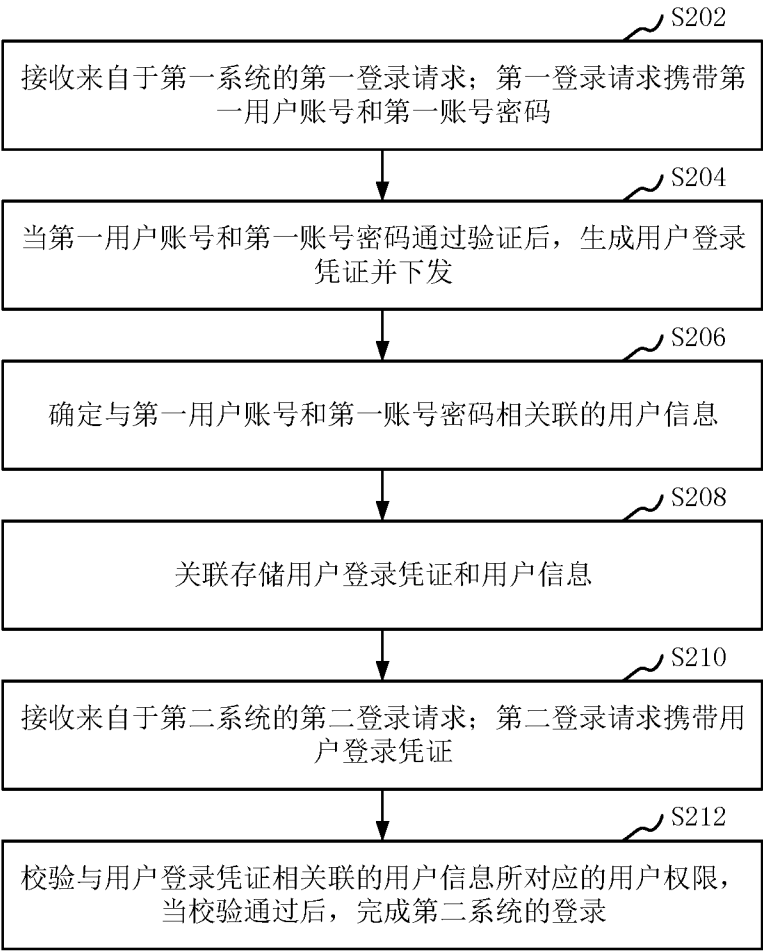


图 2

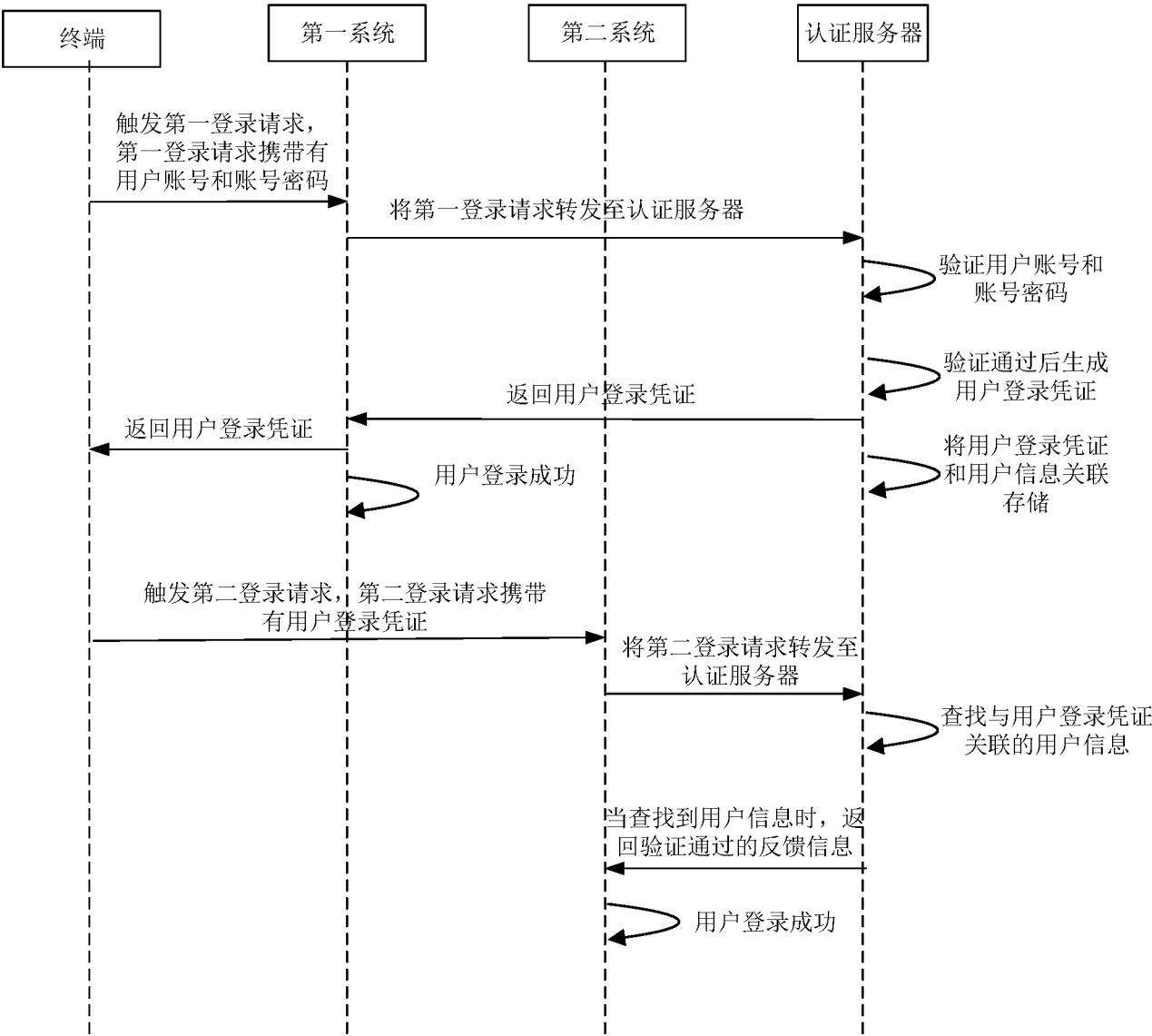


图 3

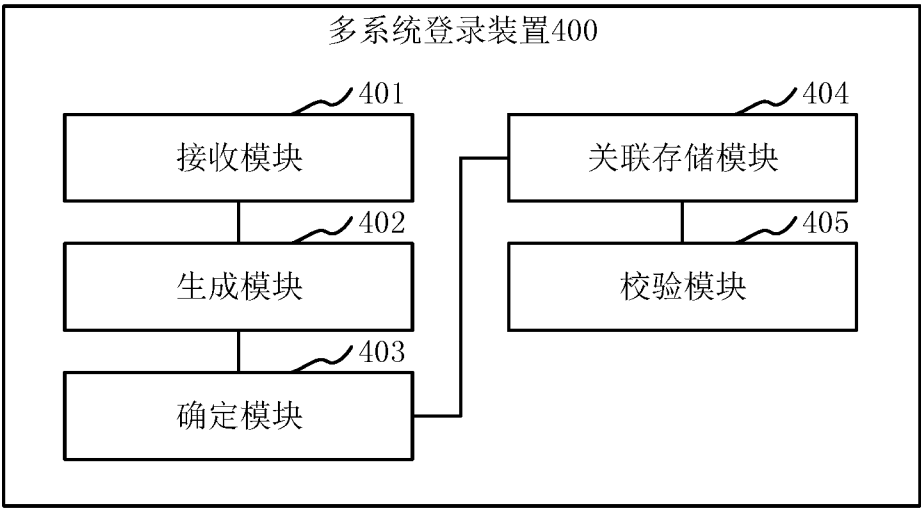


图 4

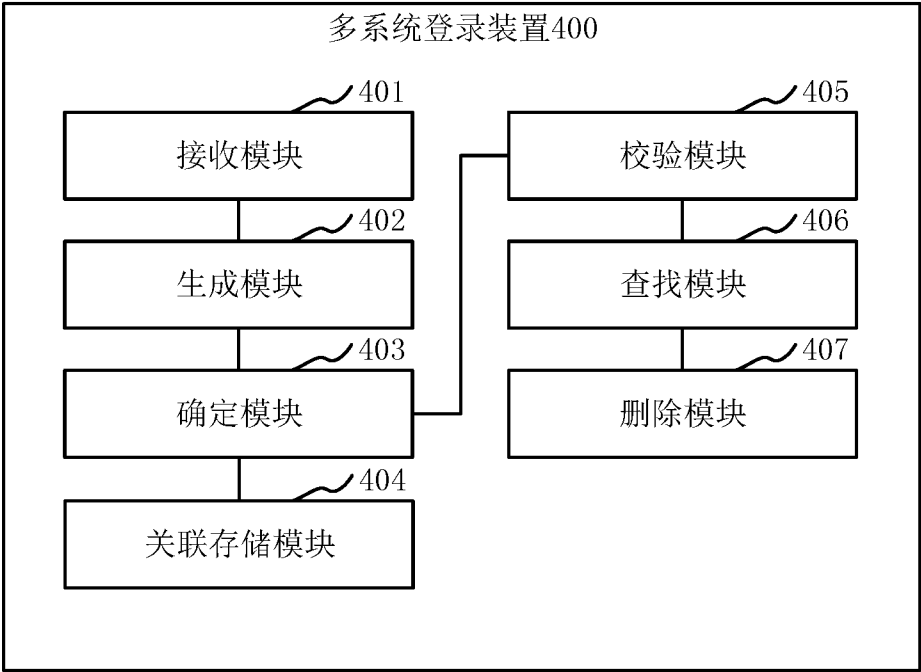


图 5

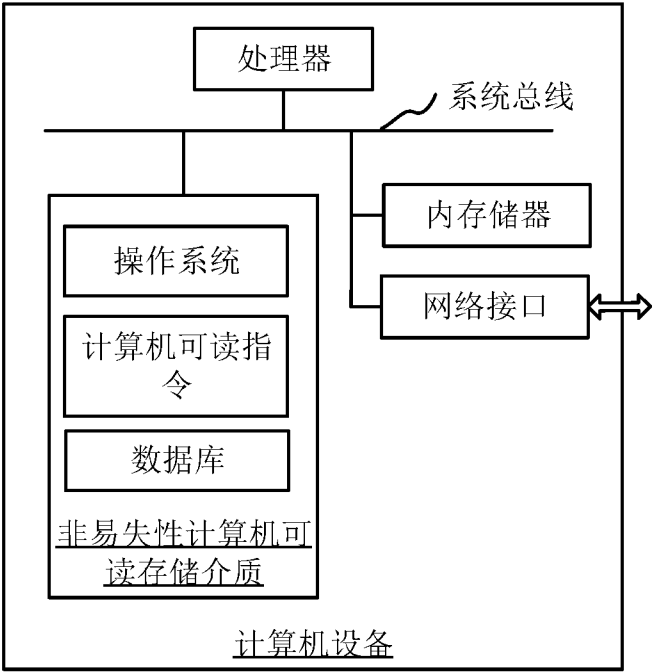


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/070885

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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)

H04L

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)

CNABS, CNTXT, VEN, USTXT, WOTXT, EPTXT: 登录请求, 凭证, 单点登录, 校验, 验证, login request, credentials, single sign on, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101355527 A (SHENZHEN ZTE MOBILE TELECOM CO., LTD.) 28 January 2009 (2009-01-28) description, page 4, and figure 2	1-20
X	CN 102469075 A (ZHONGKE ZHENGYANG INFORMATION SAFETY TECHNOLOGY CO., LTD.) 23 May 2012 (2012-05-23) claim 1	1-20
A	US 2014181944 A1 (CELLCO PARTNERSHIP DBA VERIZON) 26 June 2014 (2014-06-26) entire document	1-20
A	CN 105592003 A (BEIJING TRS INFORMATION TECHNOLOGY CO., LTD.) 18 May 2016 (2016-05-18) description, paragraphs [0026]-[0041]	1-20



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

“D” document cited by the applicant in the international application

“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

20 July 2019

Date of mailing of the international search report

05 August 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
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/CN2019/070885

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101355527	A	28 January 2009	None			
CN	102469075	A	23 May 2012	None			
US	2014181944	A1	26 June 2014	US	8959608	B2	17 February 2015
CN	105592003	A	18 May 2016	None			

国际检索报告

国际申请号

PCT/CN2019/070885

A. 主题的分类 H04L 29/06 (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) H04L 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)) CNABS, CNTXT, VEN, USTXT, WOTXT, EPTXT: 登录请求、凭证、单点登录、校验、验证, login request, credentials, single sign on, verify																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101355527 A (深圳市中兴移动通信有限公司) 2009年 1月 28日 (2009 - 01 - 28) 说明书第4页、图2</td> <td>1-20</td> </tr> <tr> <td>X</td> <td>CN 102469075 A (中科正阳信息安全技术有限公司) 2012年 5月 23日 (2012 - 05 - 23) 权利要求1</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2014181944 A1 (CELLCO PARTNERSHIP DBA VERIZON) 2014年 6月 26日 (2014 - 06 - 26) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 105592003 A (北京拓尔思信息技术股份有限公司) 2016年 5月 18日 (2016 - 05 - 18) 说明书第[0026]-[0041]段</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101355527 A (深圳市中兴移动通信有限公司) 2009年 1月 28日 (2009 - 01 - 28) 说明书第4页、图2	1-20	X	CN 102469075 A (中科正阳信息安全技术有限公司) 2012年 5月 23日 (2012 - 05 - 23) 权利要求1	1-20	A	US 2014181944 A1 (CELLCO PARTNERSHIP DBA VERIZON) 2014年 6月 26日 (2014 - 06 - 26) 全文	1-20	A	CN 105592003 A (北京拓尔思信息技术股份有限公司) 2016年 5月 18日 (2016 - 05 - 18) 说明书第[0026]-[0041]段	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
X	CN 101355527 A (深圳市中兴移动通信有限公司) 2009年 1月 28日 (2009 - 01 - 28) 说明书第4页、图2	1-20															
X	CN 102469075 A (中科正阳信息安全技术有限公司) 2012年 5月 23日 (2012 - 05 - 23) 权利要求1	1-20															
A	US 2014181944 A1 (CELLCO PARTNERSHIP DBA VERIZON) 2014年 6月 26日 (2014 - 06 - 26) 全文	1-20															
A	CN 105592003 A (北京拓尔思信息技术股份有限公司) 2016年 5月 18日 (2016 - 05 - 18) 说明书第[0026]-[0041]段	1-20															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
<table border="0"> <tr> <td> * 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 </td> <td> “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 </td> </tr> </table>			* 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													
* 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 2019年 7月 20日		国际检索报告邮寄日期 2019年 8月 5日															
ISA/CN的名称和邮寄地址 中国国家知识产权局 (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		授权官员 张雪凌 电话号码 86-(010)-62411265															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/070885

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	101355527	A	2009年 1月 28日	无	
CN	102469075	A	2012年 5月 23日	无	
US	2014181944	A1	2014年 6月 26日	US 8959608 B2	2015年 2月 17日
CN	105592003	A	2016年 5月 18日	无	