



(12) 发明专利

(10) 授权公告号 CN 111625810 B

(45) 授权公告日 2023. 09. 05

(21) 申请号 202010470156.1

G06F 16/955 (2019.01)

(22) 申请日 2020.05.28

H04L 9/40 (2022.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 111625810 A

(56) 对比文件

CN 103609090 A, 2014.02.26

CN 110493352 A, 2019.11.22

CN 103269349 A, 2013.08.28

CN 103067378 A, 2013.04.24

CN 111200610 A, 2020.05.26

CN 109547402 A, 2019.03.29

CN 107634934 A, 2018.01.26

US 2010125652 A1, 2010.05.20

WO 2013001573 A1, 2013.01.03

WO 2014146446 A1, 2014.09.25

(43) 申请公布日 2020.09.04

(73) 专利权人 百度在线网络技术(北京)有限公司

地址 100085 北京市海淀区上地十街10号
百度大厦三层

专利权人 上海小度技术有限公司

(72) 发明人 龙飞

(74) 专利代理机构 北京品源专利代理有限公司
11332

专利代理师 赵翠香

刘文印、吴鸿文、李昕、凡帅、张启翔. 一种基于可信用户代理的多方闭环网络身份认证及管理机制.《信息安全研究》.2018,652-661.

(51) Int.Cl.

G06F 21/46 (2013.01)

审查员 胡燕清

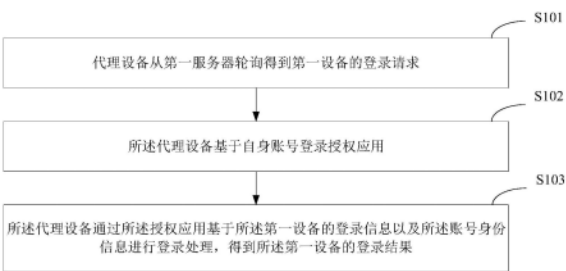
权利要求书3页 说明书12页 附图5页

(54) 发明名称

设备登录方法、设备及系统

(57) 摘要

本申请公开了设备登录方法、设备、系统及存储介质,涉及信息处理领域。具体实现方案为:代理设备从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;所述代理设备基于自身账号登录授权应用;所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。



1. 一种设备登录方法,包括:

代理设备从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

所述代理设备基于自身账号登录授权应用;

所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果;

所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,包括:

所述代理设备通过所述授权应用调用第一应用程序接口API,将所述第一设备的登录信息以及所述账号身份信息写入数据库,完成所述第一设备的登录信息以及所述账号身份信息的绑定。

2. 根据权利要求1所述的方法,所述方法还包括:

在所述第一设备登录成功的情况下,所述代理设备通过所述授权应用为所述第一设备从客控服务器侧获取针对第一服务的授权。

3. 根据权利要求1所述的方法,所述方法还包括:

所述代理设备获取到部署设备发来的针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息;

基于所述至少一个登录成功的设备的相关信息、所述第二服务的标识信息,从客控服务器侧获取针对至少一个登录成功的设备的第二服务的授权。

4. 一种设备登录方法,包括:

部署设备获取第一设备的登录统一资源定位符URL;

所述部署设备基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

所述部署设备将所述第一设备的登录信息上报至第一服务器;其中,所述第一服务器用于根据登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

5. 根据权利要求4所述的方法,其中,所述部署设备获取第一设备的登录URL,包括:

所述部署设备扫描包含登录URL的二维码;

或者,

所述部署设备通过与第一设备建立的通信连接,获取所述第一设备的登录URL。

6. 根据权利要求4所述的方法,所述方法还包括:

所述部署设备向代理设备发送针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息。

7. 一种代理设备,包括:

第一信息获取单元,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一

设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

管理单元,用于基于自身账号登录授权应用;以及通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果;

所述管理单元,用于:

所述代理设备通过所述授权应用调用第一应用程序接口API,将所述第一设备的登录信息以及所述账号身份信息写入数据库,完成所述第一设备的登录信息以及所述账号身份信息的绑定。

8. 根据权利要求7所述的代理设备,其中,所述管理单元,还用于在所述第一设备登录成功的情况下,通过所述授权应用为所述第一设备从客控服务器侧获取针对第一服务的授权。

9. 根据权利要求7所述的代理设备,其中,所述信息获取单元,还用于获取到部署设备发来的针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息;

所述管理单元,还用于基于所述至少一个登录成功的设备的相关信息、所述第二服务的标识信息,从客控服务器侧获取针对至少一个登录成功的设备的第二服务的授权。

10. 一种部署设备,包括:

第二信息获取单元,用于获取第一设备的登录URL;

信息生成单元,用于基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

信息发送单元,用于将所述第一设备的登录信息上报至第一服务器;所述第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;其中,所述第一服务器用于根据登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

11. 根据权利要求10所述的部署设备,其中,所述第二信息获取单元,用于扫描包含登录URL的二维码;

或者,

通过与第一设备建立的通信连接,获取所述第一设备的登录URL。

12. 根据权利要求10所述的部署设备,其中,所述信息发送单元,还用于向代理设备发送针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息。

13. 一种设备登录系统,包括:

代理设备,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;基于自身账号登录授权应用;以及通过所述授权应

用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果;

部署设备,用于获取第一设备的登录URL;基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;将所述第一设备的登录信息上报至第一服务器。

14.根据权利要求13所述的系统,所述系统还包括:

第一服务器,用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求。

15.根据权利要求13或14所述的系统,所述系统还包括:

第一设备,用于向第二服务器发起第一请求,接收所述第二服务器分配的登录URL;

第二服务器,用于根据第一设备发来的第一请求,为所述第一设备分配包含第一设备的相关信息的登录URL。

16.一种电子设备,包括:

至少一个处理器;以及

与所述至少一个处理器通信连接的存储器;其中,

所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行权利要求1-3或4-6中任一项所述的方法。

17.一种存储有计算机指令的非瞬时计算机可读存储介质,所述计算机指令用于使所述计算机执行权利要求1-3或4-6中任一项所述的方法。

设备登录方法、设备及系统

技术领域

[0001] 本申请涉及计算机技术领域,尤其涉及信息处理领域。本申请尤其涉及一种设备登录方法、设备、系统及存储介质。

背景技术

[0002] 随着通信设备的智能化程度越来越高,越来越多的设备可以通过连接网络为用户提供智能服务。这类设备需要通过设置账号才能够登录对应的服务器并进而获取到相应的服务。但是,相关技术中,需要用户手动进行操作,比如包括有账户的设置,才能够使得设备登录网络,如此,尤其是在针对大批量设备进行部署的场景中,按照相关技术逐台设备进行人工配置使得设备完成登录,就会出现耗时较长,出错率高等问题。

发明内容

[0003] 本公开提供了一种设备登录方法、设备、系统及存储介质。

[0004] 根据本公开的一方面,提供了一种设备登录方法,包括:

[0005] 代理设备从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0006] 所述代理设备基于自身账号登录授权应用;

[0007] 所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0008] 根据本公开的另一方面,提供了一种设备登录方法,包括:

[0009] 部署设备获取第一设备的登录URL;

[0010] 所述部署设备基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0011] 所述部署设备将所述第一设备的登录信息上报至第一服务器;其中,所述第一服务器用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

[0012] 根据本公开的另一方面,提供了一种代理设备,包括:

[0013] 第一信息获取单元,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0014] 管理单元,用于基于自身账号登录授权应用;以及通过所述授权应用基于所述第

一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0015] 根据本公开的另一方面,提供了一种部署设备,包括:

[0016] 第二信息获取单元,用于获取第一设备的登录URL;

[0017] 信息生成单元,用于基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0018] 信息发送单元,用于将所述第一设备的登录信息上报至第一服务器;所述第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;其中,所述第一服务器用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

[0019] 根据本公开的另一方面,提供了一种设备登录系统,包括:

[0020] 代理设备,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;基于自身账号登录授权应用;以及通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0021] 部署设备,用于获取第一设备的登录URL;基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;将所述第一设备的登录信息上报至第一服务器。

[0022] 根据本公开的另一方面,提供了一种电子设备,包括:

[0023] 至少一个处理器;以及

[0024] 与所述至少一个处理器通信连接的存储器;其中,

[0025] 所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行前述方法。

[0026] 根据本公开的另一方面,提供了一种存储有计算机指令的非瞬时计算机可读存储介质,其特征在于,所述计算机指令用于使所述计算机执行前述方法。

[0027] 根据本申请的另一方面,提供了一种计算机程序产品,包括计算机程序,所述计算机程序在被处理器执行时实现如上所述的方法。

[0028] 根据本申请的技术在获取到第一设备的相关信息之后,分配账号以及基于账号对第一设备进行登录等激活处理均由网络侧的设备自动完成,从而减少了设备登录或激活处理中人工处理的参与程度,并且能够减少人工配置错误等问题,使得设备的部署更加快捷,提升了设备部署的效率。尤其在需要大批量部署设备的场景中,避免了逐台设备进行人工配置的处理,从而减少时间消耗提升部署效率。

[0029] 应当理解,本部分所描述的内容并非旨在标识本公开的实施例的关键或重要特征,也不用于限制本公开的范围。本公开的其它特征将通过以下的说明书而变得容易理解。

附图说明

- [0030] 附图用于更好地理解本方案,不构成对本申请的限定。其中:
- [0031] 图1是根据本申请实施例的设备登录方法流程示意图一;
- [0032] 图2是根据本申请实施例的设备登录方法流程示意图二;
- [0033] 图3是根据本申请实施例的设备登录方法流程示意图三;
- [0034] 图4是根据本申请实施例的设备登录方法流程示意图四;
- [0035] 图5是根据本申请实施例的设备登录方法流程示意图五;
- [0036] 图6是根据本申请实施例的代理设备组成结构示意图;
- [0037] 图7是根据本申请实施例的部署设备组成结构示意图;
- [0038] 图8是根据本申请实施例的设备登录系统组成结构示意图;
- [0039] 图9是用来实现本申请实施例的设备登录方法的电子设备的框图。

具体实施方式

[0040] 以下结合附图对本申请的示范性实施例做出说明,其中包括本申请实施例的各种细节以助于理解,应当将它们认为仅仅是示范性的。因此,本领域普通技术人员应当认识到,可以对这里描述的实施例做出各种改变和修改,而不会背离本申请的范围和精神。同样,为了清楚和简明,以下的描述中省略了对公知功能和结构的描述。

[0041] 本发明实施例提供了一种设备登录方法,如图1所示,包括:

[0042] S101:代理设备从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0043] S102:所述代理设备基于自身账号登录授权应用;

[0044] S103:所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0045] 上述代理设备从第一服务器轮询得到第一设备的登录请求之前,需要部署设备先向第一服务器发送第一设备的登录信息,基于此,本实施例还一种设备登录方法,如图2所示,包括:

[0046] S201:部署设备获取第一设备的登录URL (Uniform Resource Locator,统一资源定位符);

[0047] S202:所述部署设备基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0048] S203:所述部署设备将所述第一设备的登录信息上报至第一服务器;其中,所述第一服务器用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

[0049] 本实施例提供的方案中,第一设备可以为需要进行部署的多个设备中之一。当前需要部署的多个设备,可以为智能音箱,或智能终端等设备。

[0050] 一种优选的示例中,需要部署的多个设备,为用户在多个空间中不同的空间部署的不同的设备。举例来说,多个空间可以为一个建筑中的多个房间,比如,酒店中的每一个房间中部署一个智能音箱。

[0051] 一种示例中,第一设备在开机之后,会向第二服务器(可以称为passport云端服务器)发起第一请求;第二服务器收到第一请求后为第一设备分配一个登陆URL。

[0052] 其中,第一设备开启后可以周期性的发起第一请求,相应的,第二服务器会接收到第一请求后就分配一个新的登录URL。其中,周期长度可以根据实际情况配置,比如,可以为10s、20s等等,本实施例不对其进行限定。

[0053] 也就是说,不同次请求可以得到不同次的登录URL,如此,可以避免登录URL被盗的问题,提升系统安全性。

[0054] 基于此,当部署设备对多个需要部署的设备中的任意一个设备需要进行登录部署的时候,可以将该当前部署的设备作为第一设备,然后执行前述S201。

[0055] 具体来说,所述部署设备获取第一设备的登录URL,包括:

[0056] 所述部署设备扫描包含登录URL的二维码;

[0057] 或者,

[0058] 所述部署设备通过与第一设备建立的通信连接,获取所述第一设备的登录URL。

[0059] 上述两种情况分别来说,第一设备可以为有屏设备也可以为无屏设备。

[0060] 当第一设备为有屏设备的时候,比如有些智能终端有操作或显示屏幕,那么第一设备可以将当前获取到的登录URL以二维码的形式展示在屏幕上,相应的,部署设备可以通过自身安装的APP(可以称为部署APP)扫描包含登录URL的二维码以获取登录URL。

[0061] 当第一设备为无屏设备的时候,比如有些智能音箱没有交互屏幕,那么部署设备(通过自身安装的部署APP)控制通信模块与第一设备的通信模块建立连接之后,通过建立的通信连接,获取所述第一设备的登录URL。

[0062] 再进一步来说,通信连接可以通过蓝牙通信模块建立,或者可以通过WIFI模块建立,这里不进行穷举。

[0063] 在完成步骤S201之后,部署设备执行S202生成登录信息。

[0064] 其中,部署设备可以通过自身安装的部署APP,对第一设备所处空间的相关信息输入。

[0065] 这里,第一设备所处空间的相关信息,可以包括有建筑的名称、房间的编号等等。举例来说,第一设备所处空间的相关信息,可以为酒店名称、房间号等。

[0066] 另外,第一设备的相关信息可以包括有登录URL、第一设备的设备标识、第一设备的MAC(Media Access Control,媒体访问控制)地址、IP(Internet Protocol,是指互联网协议)地址等信息中至少之一。其中,第一设备的设备标识可以为第一设备的CUID、和/或SN(序列号)。

[0067] 也就是,在S202中,部署设备收集更多的第一设备的信息生成登录信息,然后执行S203,将第一设备的登录信息上报至第一服务器。

[0068] 其中,第一服务器可以与第二服务器相同,也可以与第二服务器不同。如果第一服务器与第二服务器不同,则第二服务器可以为passport云端服务器,第一服务器可以为ToB云端服务器。

[0069] 需要指出的是,第一服务器在收到第一设备的登录信息时,所述第一服务器还会根据登录信息为第一设备生成对应的账号身份信息。

[0070] 其中,账号身份信息中可以包括有用户名、密码等信息。

[0071] 然后第一服务器可以将登录信息以及账号身份信息作为登录请求。

[0072] 还需要理解的是,账号身份信息由于为服务器临时为第一设备分配的,因此进一步可以保证第一设备登录过程的安全性。

[0073] 前述S101中,代理设备可以在第一服务器轮询,得到第一设备的登录请求。

[0074] 代理设备可以为一个全天开启的设备或服务器,可以按照一定时间间隔或者可以为实时的对第一服务器进行轮询,检测是否存在新的登录请求。

[0075] 然后执行S102,也就是代理设备可以控制通过自身账号登录自身安装的授权应用。需要理解的是,代理设备中可以安装有授权应用,该授权应用可以为基于代理设备中预配置的多个特殊账号中任意之一登录的。

[0076] 前述S102执行完成后,代理设备(的授权应用)还可以向第一服务器发送自登录成功的通知。

[0077] 然后第一服务器还可以将代理设备的授权应用的自登录成功的通知传该第二服务器,使得第二服务器获知授权应用登录的状态。

[0078] 登录授权应用之后,就可以通过授权应用对第一设备的登录请求进行后续处理,也就是执行S103,根据登录请求中包含的内容对第一设备进行登录处理,得到登录结果。

[0079] 具体来说,所述代理设备通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,包括:

[0080] 所述代理设备通过所述授权应用调用第一应用程序接口API,将所述第一设备的登录信息以及所述账号身份信息写入数据库,完成所述第一设备的登录信息以及所述账号身份信息的绑定。

[0081] 其中第一API可以为第一应用调用passSDK API。相应的,前述处理可以理解为:授权应用通过调用passSDK API进行登录URL的写入,使得第一设备基于分配的账号身份信息完成登录。

[0082] 也就是说,前述登录处理可以认为是将登录信息中包含的登录URL、第一设备的设备标识、第一设备所处空间的相关信息、以及所述账号身份信息写入数据库进行绑定,以完成登录处理。

[0083] 这里,还需要指出的是,如果第一设备原始自带相关服务(或技能),可以在登录信息中还包括有第一设备的服务标识或技能标识,那么在登录处理的时候,可以将登录URL、第一设备的设备标识、第一设备所处空间的相关信息、以及所述账号身份信息、服务标识(或技能标识)一起写入数据库进行绑定以完成登录处理。

[0084] 完成S103之后,代理设备的授权应用还可以向第一服务器(也就是ToB云端服务器)发送第一设备登录成功的通知(或者可以为第一设备扫码成功的通知),不论通知的名称为什么但是其作用可以认为是通知第一设备登录成功;相应的,第一服务器可以将扫码成功的通知或登录成功的通知传输至第二服务器(也就是PASSPORT云端服务器);第一设备会轮询第二服务器,一旦轮询到登录成功的通知就可以确定自身已经登录成功。

[0085] 还需要理解的是,在第一设备登录成功后,如图3所示,本实施例提供方案还可以

包括S104:在所述第一设备登录成功的情况下,所述代理设备通过所述授权应用为所述第一设备从客控服务器侧获取针对第一服务的授权。

[0086] 也就是说,第一设备登录成功之后,授权应用可以直接从客控服务器侧为第一设备的第一服务获取相应的授权。

[0087] 具体来说,在确定第一设备登录成功的处理中,还可以包括:第一设备在轮询到自身登录成功(或扫码成功)的通知后,可以上报自身的标识给第一服务器;

[0088] 代理设备可以轮询第一服务器,接收到第一设备的设备标识后,从数据库中保存的信息来判断第一设备的设备标识是否为登录成功的设备标识,如果是,则确定所述第一设备登录成功。

[0089] 进而,代理设备在确定第一设备登录成功之后,可以根据数据库中保存的信息确定第一设备的服务标识(或技能标识),这里将获取到的服务标识或技能标识对应的服务称为第一服务。这里,第一服务可以理解为在第一设备中安装的某一功能或某一应用。也就是,第一设备登录成功之后,还需要对其中包含的服务获取相应的授权才可以使用其中的服务。

[0090] 代理设备可以向第一服务所对应的服务器申请授权。具体来说,代理设备可以利用第一设备的登录态,跳转至第一服务的客控服务器授权的网页(web)页面抓取对应的元素以对处于登录态的第一设备进行针对第一服务的授权。

[0091] 如果第一服务需要相应的账号和密码登录才可以使用的情况下,代理设备的授权应用还需要将第一设备的设备标识结合第一服务对应的账号和密码从对应的可控服务器获取授权,最终得到授权结果。然后,代理设备将授权结果上传到第一服务器。

[0092] 相应的,部署设备轮询到第一服务器上的第一服务的授权结果之后,确定第一设备的第一服务授权成功。

[0093] 至此,针对第一设备的登录以及服务绑定完成一次处理。

[0094] 另外,上述针对的场景为,第一设备存在原始安装(或预配置)的第一服务的情况下,登录完成之后直接对第一服务进行授权。但是,在实际应用中,很可能存在需要对当前登录成功或部署成功的多台设备进行服务升级的情况,比如,提供智能家居服务或其他第三方服务,针对这种情况,本实施例会针对多台已经登录成功的设备提供第三方服务批量授权的处理,具体可以包括:

[0095] 所述部署设备向代理设备发送针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息。

[0096] 相应的,所述代理设备获取到部署设备发来的针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息;

[0097] 基于所述至少一个登录成功的设备的相关信息、所述第二服务的标识信息,从客控服务器侧获取针对至少一个登录成功的设备的第二服务的授权。

[0098] 其中,登录成功的设备的相关信息,可以包括有设备的标识信息、不同设备对应的空间相关信息等等。

[0099] 第二服务的标识信息可以为服务ID、应用ID、技能ID中至少之一。

[0100] 也就是说,如果在部署完成多台设备之后,后期需要绑定新的第三方服务的时候,可以直接在部署设备选取多台设备进行服务绑定,进而将选取的多台设备的相关信息以及第三方服务的相关信息发送给代理设备;由代理设备通过授权应用从第三方服务的授权服务器获取对应的授权。如此,可以实现针对已经部署成功或登录完成的多台设备批量的进行第三方服务的绑定的处理,提升了处理效率。

[0101] 总的来说,本申请实施例提供了双app模式的处理方案,提供部署设备(具体可以为部署设备的部署应用(APP))给现场实施工作者,该部署设备(具体可以为部署设备的部署应用(APP))关联了用户账号下管理的酒店、设备及技能,数据跟行业管理平台联动,实施者可以很方便的在部署设备(具体可以为部署设备的部署应用(APP))选择酒店、填写房间、选择技能(比如智能家居的服务)、扫描音箱二维码提交进行登录激活等处理;

[0102] 代理设备的授权app收到部署app提交的任务,自动分配百度账号,自动在内部模拟用户进行登录,然后根据部署app上报的二维码,调用pass接口模拟扫描登录,同时进行qq音箱授权、客控技能授权等一系列功能。当代理设备的授权app处理完成后,设备(比如音箱)轮询到登录态自动登录成功。

[0103] 另外,还提供针对无屏设备在不切换百度账号的情况下通过蓝牙等通信连接实现配置或重配置,以及后期可以根据实际需求通过客控针对第三方服务补授权流程等处理,都提供了完善的tob场景的处理。

[0104] 一种示例中,结合图4进行说明:

[0105] 原始流程中,针对酒店中某一个房间安装的设备进行激活,需要在设备中执行申请账号、标记账号、绑定服务、恢复账号、登录账号最终完成激活等处理。

[0106] 而本示例中,申请账号、标记账号、绑定服务、恢复账号、登录账号的处理不需要设备本身参与操作,仅需要通过部署设备中的部署APP,对登录URL进行获取,就可以后续由代理设备的授权APP、服务器等进行自动交互,完成上述处理,直至设备完成激活。并且,部署设备可以支持有屏扫码、无屏连接蓝牙中任意之一的功能。从而能够实现部署设备扫描设备或连接设备后对设备一键激活,如此,用户不用学习理解账号概念,10-20s就能完成一台设备的激活,为规模化部署提供高效的处理工具。

[0107] 具体来说,代理设备通过授权APP(应用)可以构建内部服务代理机制,申请账号-分配账号-获取账号-登陆账号等处理全部内部自动完成。这里过程中,彻底摒弃手工环节、解决账号安全问题、输入易出错及出错后依赖百度方处理的问题。

[0108] 另外,本示例还避免了原始处理流程中在绑定项目(即绑定第三方服务)的处理中,需要手工录入的处理,也就是建立了激活的设备自动绑定到项目后台的逻辑,完全省去手工单个录入设备的步骤。

[0109] 再结合图4来说,在需要对激活的多个设备进行第三方服务的绑定的时候,可以直接通过部署设备(中的部署APP)选择酒店以及设备,以实现设备自动批量绑定。从而实现了第三方服务绑定与设备激活流程解耦,设备激活后随时批量绑定第三方服务。从而,使得流程更灵活,尤其适用于设备登录或部署完成后才会引入第三方服务的部分场景。

[0110] 又一示例,结合图5对本申请实施例的流程进行说明,本示例中,第一设备为音箱,第一服务器为ToB云端服务器、第二服务器为PASSPORT云端,具体可以包括:

[0111] 音箱向PASSPORT云端进行端上请求,得到PASSPORT云端返回的登录URL;

[0112] 部署设备(通过部署APP)扫描获取登录URL,将房间号和登录URL发送至ToB云端,然后ToB云端为登录请求分配用户名和密码作为账号身份信息;

[0113] 代理设备轮询ToB云端是否存在新的登录请求,基于轮询处理获取到新的登录请求后,使用分配的账号和密码自行登录授权APP,这里,分配的账号和密码为代理设备获取到的用于登录授权APP的账号信息,与前述ToB云端为登录请求分配的用户名和密码不同。

[0114] 代理设备的授权APP登录成功后,通知ToB云端APP自身登录成功,ToB云端通知PASSPORT云端,使得PASSPORT云端记录APP登录;

[0115] 代理设备的授权APP调用passSDK API将登录URL填入数据库,使得音箱以自己的账号身份登录。从而完成音箱的登录处理。并且,代理设备还会通知ToB云端登录成功,也就是扫描成功;ToB云端将扫码成功的通知发送至PASSPORT云端,由音箱轮询得到扫码结果。

[0116] 音箱会上报设备自身CUID至ToB云端;代理设备的授权APP得到音箱的CUID后,会判断设备是否登录成功,若成功,则利用pass webview的登录态跳转客控授权的web页面抓取元素进行第一服务的自动授权,完成后,向ToB云端通知授权结果;如果需要对第一服务进行登录,则需要根据设备CUID进一步获取到针对第一服务的登录态的授权,并向ToB反馈第一服务授权结果。部署设备(部署APP)通过轮询从ToB云端获知登录授权第一服务的状态。

[0117] 本发明实施例提供了一种代理设备,如图6所示,包括:

[0118] 第一信息获取单元61,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0119] 管理单元62,用于基于自身账号登录授权应用;以及通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0120] 上述代理设备从第一服务器轮询得到第一设备的登录请求之前,需要部署设备先向第一服务器发送第一设备的登录信息,基于此,本实施例还一种部署设备,如图7所示,包括:

[0121] 第二信息获取单元71,用于获取第一设备的登录URL;

[0122] 信息生成单元72,用于基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;

[0123] 信息发送单元73,用于将所述第一设备的登录信息上报至第一服务器;所述第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;其中,所述第一服务器用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求以使得所述授权设备针对所述第一设备进行登录处理。

[0124] 本实施例提供的方案中,第一设备可以为需要进行部署的多个设备中之一。当前需要部署的多个设备,可以为智能音箱,或智能终端等设备。

[0125] 具体来说,所述第二信息获取单元71,用于扫描包含登录URL的二维码;

[0126] 或者,

[0127] 通过与第一设备建立的通信连接,获取所述第一设备的登录URL。

[0128] 具体来说,管理单元62,用于通过所述授权应用调用第一应用程序接口API,将所述第一设备的登录信息以及所述账号身份信息写入数据库,完成所述第一设备的登录信息以及所述账号身份信息的绑定。

[0129] 其中第一API可以为第一应用调用passSDK API。相应的,前述处理可以理解为:授权应用通过调用passSDK API进行登录URL的写入,使得第一设备基于分配的账号身份信息完成登录。

[0130] 也就是说,前述登录处理可以认为是将登录信息中包含的登录URL、第一设备的设备标识、第一设备所处空间的相关信息、以及所述账号身份信息写入数据库进行绑定,以完成登录处理。

[0131] 管理单元62,用于在所述第一设备登录成功的情况下,通过所述授权应用为所述第一设备从客控服务器侧获取针对第一服务的授权。

[0132] 本实施例会针对多台已经登录成功的设备提供第三方服务批量授权的处理,具体可以包括:

[0133] 所述信息发送单元73,还用于向代理设备发送针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息。

[0134] 相应的,所述代理设备的所述信息获取单元,还用于获取到部署设备发来的针对至少一个登录成功的设备的第二服务的授权请求;其中,所述授权请求中包括:至少一个登录成功的设备的相关信息,以及第二服务的标识信息;

[0135] 所述管理单元,还用于基于所述至少一个登录成功的设备的相关信息、所述第二服务的标识信息,从客控服务器侧获取针对至少一个登录成功的设备的第二服务的授权。

[0136] 其中,登录成功的设备的相关信息,可以包括有设备的标识信息、不同设备对应的空间相关信息等等。

[0137] 本申请实施例还提供了一种设备登录系统,如图8所示包括:

[0138] 代理设备81,用于从第一服务器轮询得到第一设备的登录请求;其中,所述第一设备的登录请求中包括:部署设备上报的第一设备的登录信息,以及所述第一服务器分配的账号身份信息;其中,所述部署设备上报的第一设备的登录信息中包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;基于自身账号登录授权应用;以及通过所述授权应用基于所述第一设备的登录信息以及所述账号身份信息进行登录处理,得到所述第一设备的登录结果。

[0139] 部署设备82,用于获取第一设备的登录URL;基于获取的所述第一设备的登录URL生成第一设备的登录信息;所述第一设备的登录信息包括:所述第一设备的相关信息,所述第一设备所处空间的相关信息;将所述第一设备的登录信息上报至第一服务器。

[0140] 所述系统还包括:

[0141] 第一服务器83,用于根据所述登录请求分配账号身份信息,并向授权设备发送包含所述账号身份信息以及第一设备的登录信息的登录请求。

[0142] 所述系统还包括:

[0143] 第一设备84,用于向第二服务器发起第一请求,接收所述第二服务器分配的登录URL;

[0144] 第二服务器85,用于根据第一设备发来的第一请求,为所述第一设备分配包含第一设备的相关信息的登录URL。

[0145] 关于系统中上述设备或服务器的处理与前述实施例相同,因此这里不再进行赘述。

[0146] 通过采用上述方案,可以仅需要获取到第一设备的相关信息之后,分配账号以及基于账号对第一设备进行登录等激活处理均由网络侧的设备自动完成,从而减少了设备登录或激活处理中人工处理的参与程度,并且能够减少人工配置错误等问题,使得设备的部署更加快捷,提升了设备部署的效率。尤其在需要大批量部署设备的场景中,避免了逐台设备进行人工配置的处理,从而减少时间消耗提升部署效率。

[0147] 根据本申请的实施例,本申请还提供了一种电子设备、一种可读存储介质和一种计算机程序产品。

[0148] 如图9所示,是根据本申请实施例的设备登录方法的电子设备的框图。该电子设备可以为前述部署设备或代理设备。电子设备旨在表示各种形式的数字计算机,诸如,膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置,诸如,个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅仅作为示例,并且不意在限制本文中描述的和/或者要求的本申请的实现。

[0149] 如图9所示,该电子设备包括:一个或多个处理器901、存储器902,以及用于连接各部件的接口,包括高速接口和低速接口。各个部件利用不同的总线互相连接,并且可以被安装在公共主板上或者根据需要以其它方式安装。处理器可以对在电子设备内执行的指令进行处理,包括存储在存储器中或者存储器上以在外部输入/输出装置(诸如,耦合至接口的显示设备)上显示GUI的图形信息的指令。在其它实施方式中,若需要,可以将多个处理器和/或多条总线与多个存储器和多个存储器一起使用。同样,可以连接多个电子设备,各个设备提供部分必要的操作(例如,作为服务器阵列、一组刀片式服务器、或者多处理器系统)。图9中以一个处理器901为例。

[0150] 存储器902即为本申请所提供的非瞬时计算机可读存储介质。其中,所述存储器存储有可由至少一个处理器执行的指令,以使所述至少一个处理器执行本申请所提供的设备登录方法。本申请的非瞬时计算机可读存储介质存储计算机指令,该计算机指令用于使计算机执行本申请所提供的设备登录方法。

[0151] 存储器902作为一种非瞬时计算机可读存储介质,可用于存储非瞬时软件程序、非瞬时计算机可执行程序以及模块,如本申请实施例中的设备登录方法对应的程序指令/模块(例如,附图6所示的第一信息获取单元61、管理单元62,图7所示的第二信息获取单元71、信息生成单元72、信息发送单元73)。处理器901通过运行存储在存储器902中的非瞬时软件程序、指令以及模块,从而执行服务器的各种功能应用以及数据处理,即实现上述方法实施例中的设备登录方法。

[0152] 存储器902可以包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需要的应用程序;存储数据区可存储根据电子设备的使用所创建的数

据等。此外,存储器902可以包括高速随机存取存储器,还可以包括非瞬时存储器,例如至少一个磁盘存储器件、闪存器件、或其他非瞬时固态存储器件。在一些实施例中,存储器902可选包括相对于处理器901远程设置的存储器,这些远程存储器可以通过网络连接至电子设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0153] 设备登录方法的电子设备(部署设备或代理设备)还可以包括:输入装置903和输出装置904。处理器901、存储器902、输入装置903和输出装置904可以通过总线或者其他方式连接,图9中以通过总线连接为例。

[0154] 输入装置903可接收输入的数字或字符信息,以及产生与电子设备的用户设置以及功能控制有关的键信号输入,例如触摸屏、小键盘、鼠标、轨迹板、触摸板、指示杆、一个或者多个鼠标按钮、轨迹球、操纵杆等输入装置。输出装置904可以包括显示设备、辅助照明装置(例如,LED)和触觉反馈装置(例如,振动电机)等。该显示设备可以包括但不限于,液晶显示器(LCD)、发光二极管(LED)显示器和等离子体显示器。在一些实施方式中,显示设备可以是触摸屏。

[0155] 此处描述的系统和技术各种实施方式可以在数字电子电路系统、集成电路系统、专用ASIC(专用集成电路)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括:实施在一个或者多个计算机程序中,该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释,该可编程处理器可以是专用或者通用可编程处理器,可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令,并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0156] 这些计算程序(也称作程序、软件、软件应用、或者代码)包括可编程处理器的机器指令,并且可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。如本文使用的,术语“机器可读介质”和“计算机可读介质”指的是用于将机器指令和/或数据提供给可编程处理器的任何计算机程序产品、设备、和/或装置(例如,磁盘、光盘、存储器、可编程逻辑装置(PLD)),包括,接收作为机器可读信号的机器指令的机器可读介质。术语“机器可读信号”指的是用于将机器指令和/或数据提供给可编程处理器的任何信号。

[0157] 为了提供与用户的交互,可以在计算机上实施此处描述的系统和技术,该计算机具有:用于向用户显示信息的显示装置(例如,CRT(阴极射线管)或者LCD(液晶显示器)监视器);以及键盘和指向装置(例如,鼠标或者轨迹球),用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互;例如,提供给用户的反馈可以是任何形式的传感反馈(例如,视觉反馈、听觉反馈、或者触觉反馈);并且可以用任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0158] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如,作为数据服务器)、或者包括中间件部件的计算系统(例如,应用服务器)、或者包括前端部件的计算系统(例如,具有图形用户界面或者网络浏览器的用户计算机,用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网

(LAN)、广域网(WAN)和互联网。

[0159] 计算机系统可以包括客户端和服务端。客户端和服务端一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务端的关系。

[0160] 根据本申请实施例的技术方案,可以仅需要获取到需要部署的设备的相关信息之后,分配账号以及基于账号对设备进行登录等激活处理均在设备的应用中自动完成,从而减少了设备登录或激活处理中人工处理的参与,使得设备的部署更加快捷,并且减少了配置错误等问题,提升了设备部署的效率,尤其在需要大批量部署设备的场景中,避免了逐台设备进行人工配置使得设备完成登录的处理,实现了减少时间消耗提升部署效率的效果。

[0161] 应该理解,可以使用上面所示的各种形式的流程,重新排序、增加或删除步骤。例如,本申请中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行,只要能够实现本申请公开的技术方案所期望的结果,本文在此不进行限制。

[0162] 上述具体实施方式,并不构成对本申请保护范围的限制。本领域技术人员应该明白的是,根据设计要求和因素,可以进行各种修改、组合、子组合和替代。任何在本申请的精神和原则之内所作的修改、等同替换和改进等,均应包含在本申请保护范围之内。

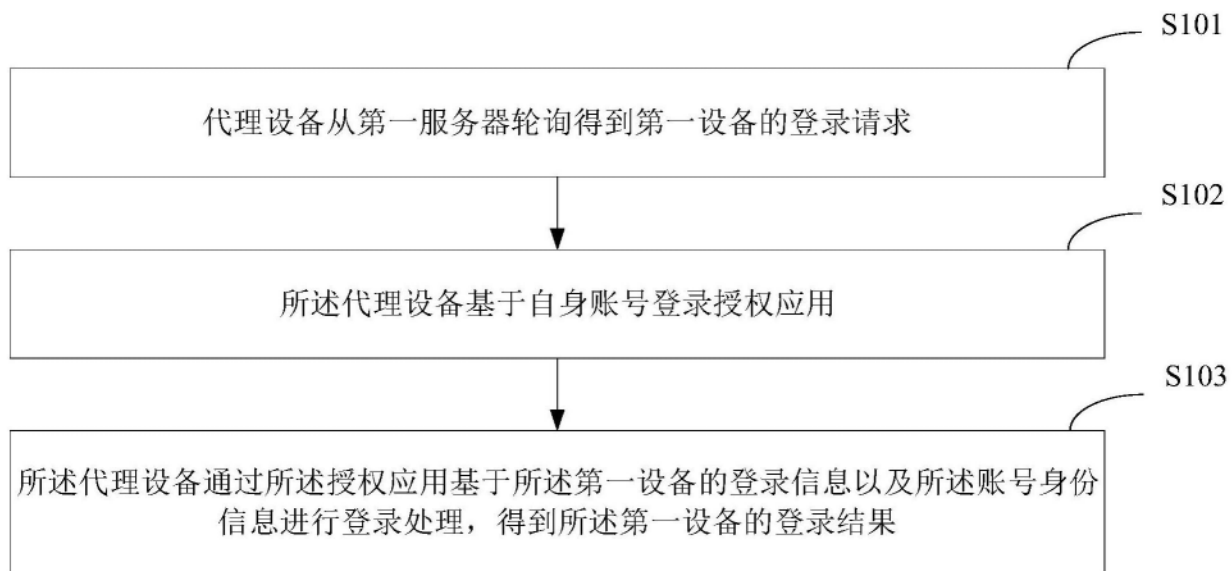


图1

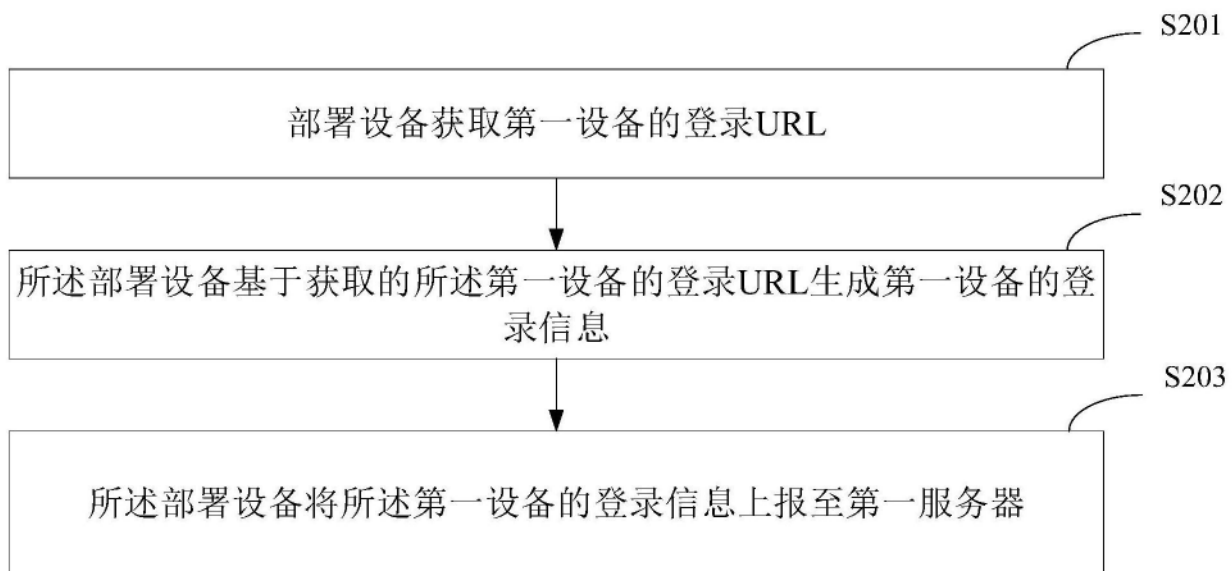


图2

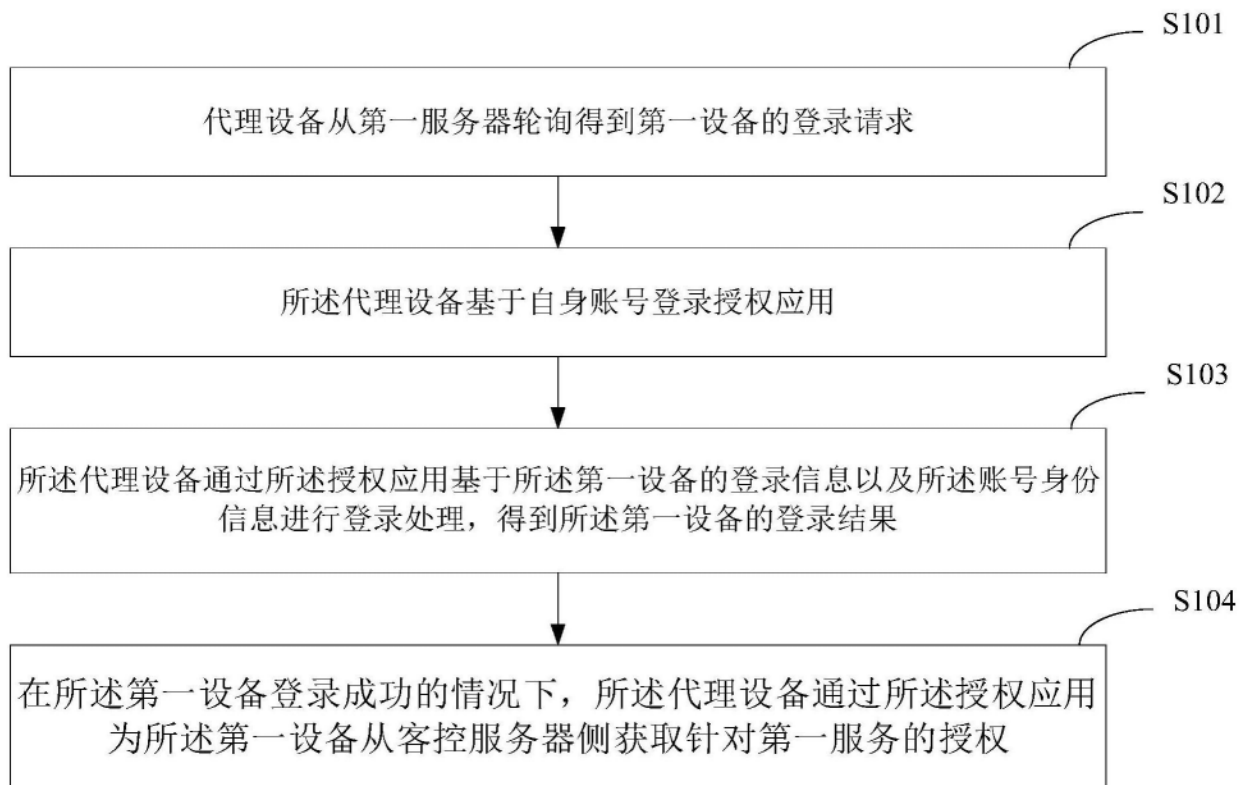


图3

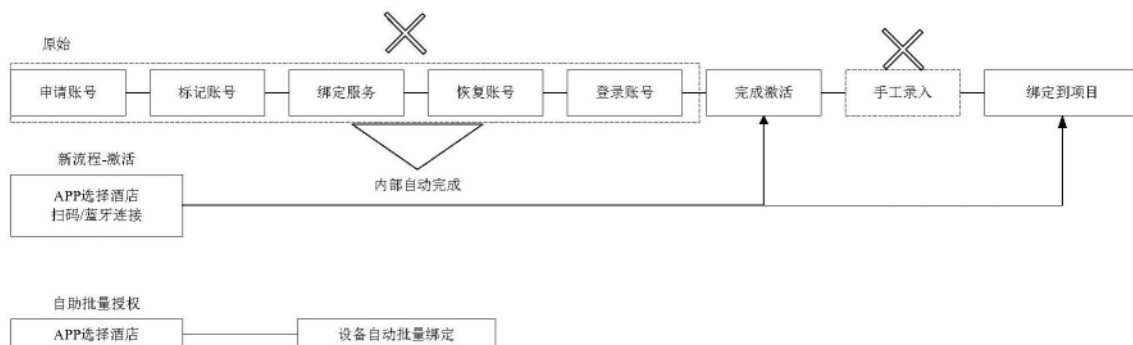


图4

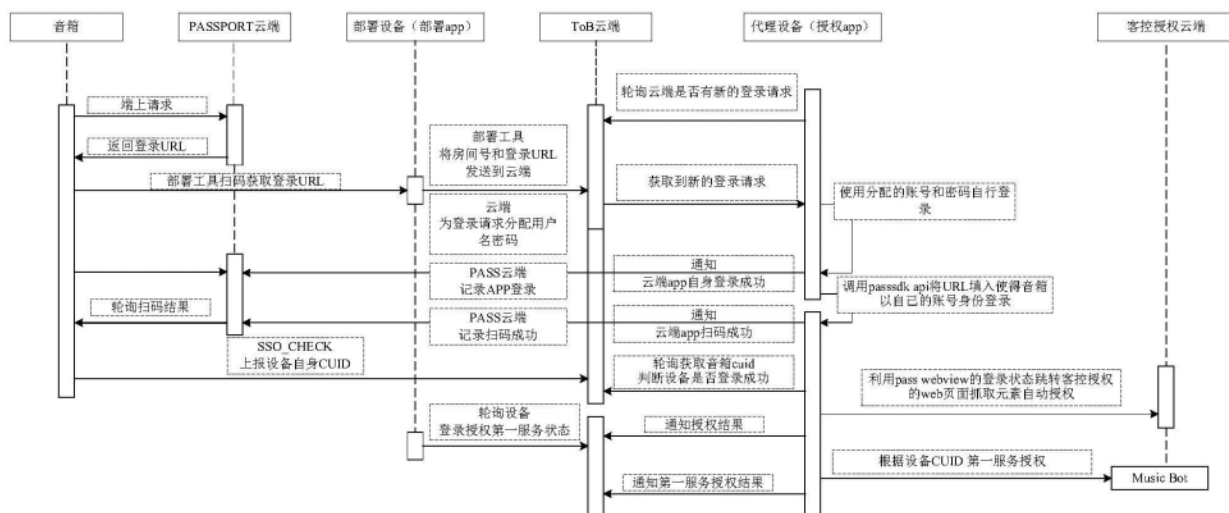


图5

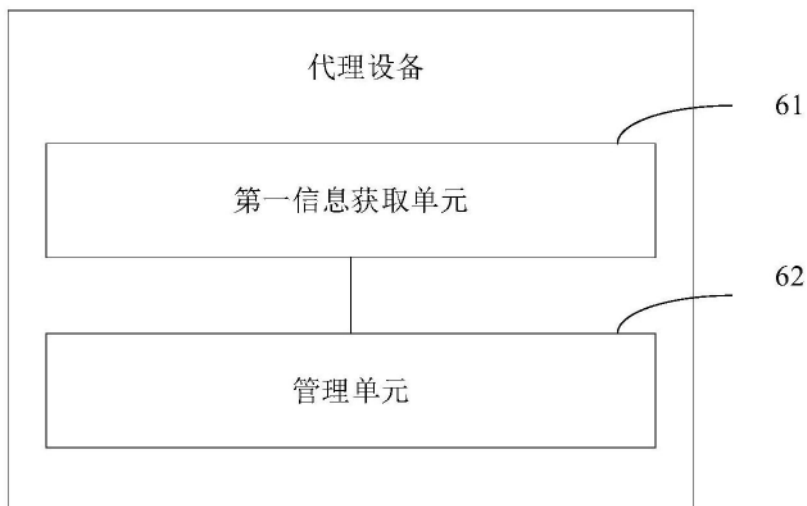


图6

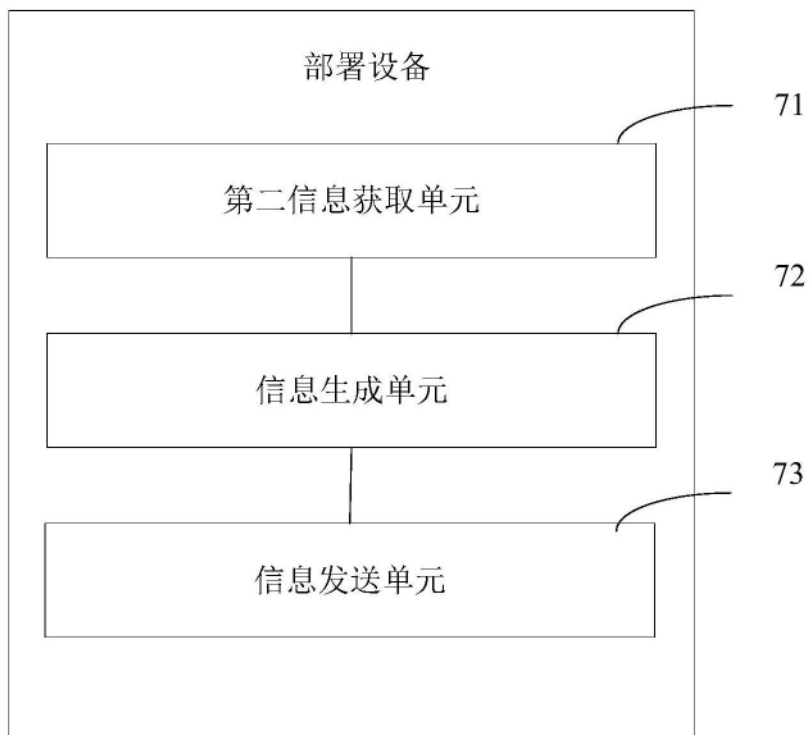


图7

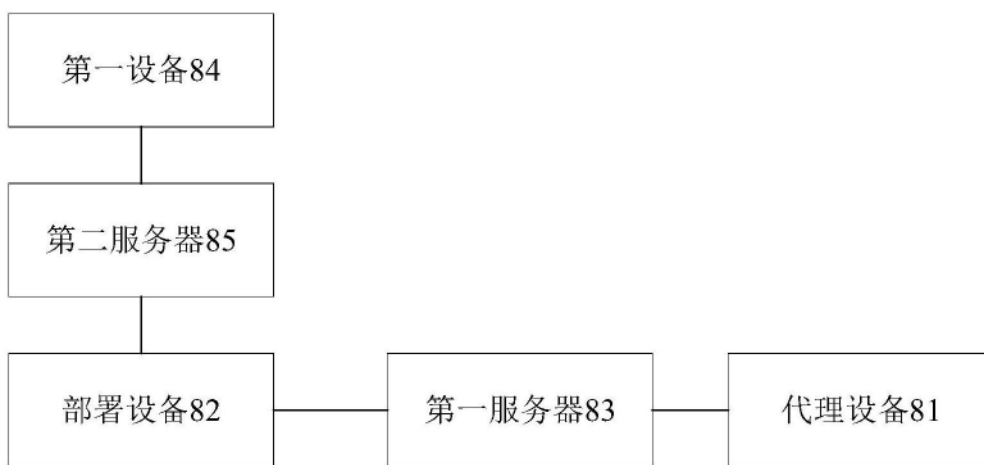


图8

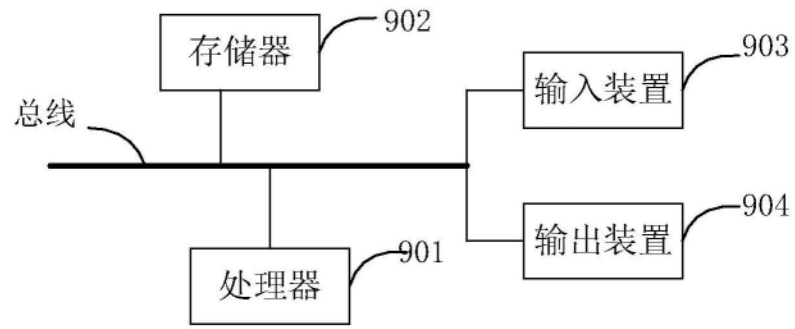


图9