(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109413096 B
(45)授权公告日 2019.08.09

(21)申请号 201811453442.6

(22)申请日 2018.11.30

(65)同一申请的已公布的文献号
申请公布号 CN 109413096 A

(43)申请公布日 2019.03.01

(73)专利权人 北京海泰方圆科技股份有限公司
地址 100094 北京市海淀区东北旺西路8号中关村软件园9号楼国际软件大厦E座一层、二层

(72)发明人 安晓江 胡伯良 蒋红宇

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 黄志华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/36(2013.01)

(56)对比文件
CN 106961447 A,2017.07.18,
CN 108023881 A,2018.05.11,
CN 104125485 A,2014.10.29,
CN 104253784 A,2014.12.31,
CN 108197480 A,2018.06.22,
CN 105162591 A,2015.12.16,
CN 106105091 A,2016.11.09,
CN 108200040 A,2018.06.22,
CN 105656922 A,2016.06.08,
CN 106778206 A,2017.05.31,

审查员 张洁

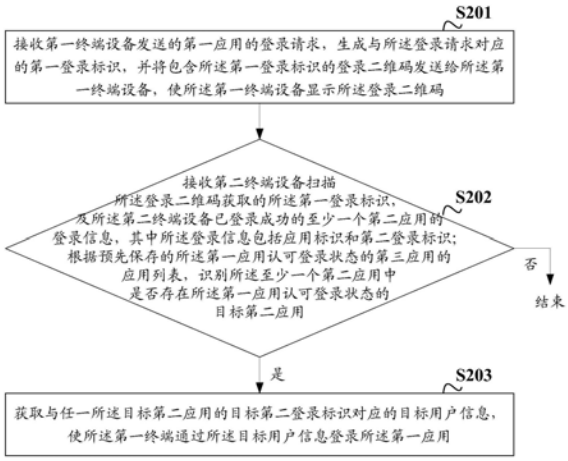
权利要求书3页 说明书12页 附图4页

(54)发明名称

一种多应用的登录方法及装置

(57)摘要

本发明公开了一种多应用的登录方法及装置，所述方法包括：第一验证服务器接收第一终端设备发送的第一应用的登录请求，生成包含与登录请求对应的第一登录标识的登录二维码；使第一终端设备显示登录二维码；接收第二终端设备扫描登录二维码获取的第一登录标识，及已登录成功的至少一个第二应用的登录信息，根据第一应用认可登录状态的第三应用的应用列表，识别到至少一个第二应用中存在第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。提供了一种不同应用间可以相互认证的登录方案。



CN 109413096 B

1.一种多应用的登录方法,其特征在于,应用于第一验证服务器,所述方法包括:

接收第一终端设备发送的第一应用的登录请求,生成与所述登录请求对应的第一登录标识,并将包含所述第一登录标识的登录二维码发送给所述第一终端设备,使所述第一终端设备显示所述登录二维码;

接收第二终端设备扫描所述登录二维码获取的所述第一登录标识,及所述第二终端设备已登录成功的至少一个第二应用的登录信息,其中所述登录信息包括应用标识和第二登录标识;根据预先保存的所述第一应用认可登录状态的第三应用的应用列表,识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用;

如果是,获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息,使所述第一终端通过所述目标用户信息登录所述第一应用;

其中,获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息包括:

向与目标第二应用对应的目标第二验证服务器发送包含目标第二应用的目标第二登录标识的用户信息请求;接收目标第二验证服务器发送的与目标第二登录标识绑定的目标用户信息。

2.如权利要求1所述的方法,其特征在于,如果预先配置有每个应用的公钥和私钥,所述登录信息还包括私钥签名,所述获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息之前,所述方法还包括:

根据所述目标第二应用的公钥,对所述目标第二应用的私钥签名进行验签;

如果验签通过,进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

3.一种多应用的登录方法,其特征在于,应用于第二终端设备,所述方法包括:

扫描第一终端设备显示的第一应用的登录二维码,获取所述登录二维码包含的第一登录标识,其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的;

向所述第一验证服务器发送所述第一登录标识,及所述第二终端设备中已登录成功的至少一个第二应用的登录信息,其中所述登录信息包括应用标识和第二登录标识;使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表,在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时,获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息,使所述第一终端通过所述目标用户信息登录所述第一应用;

其中,获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息包括:

向与目标第二应用对应的目标第二验证服务器发送包含目标第二应用的目标第二登录标识的用户信息请求;接收目标第二验证服务器发送的与目标第二登录标识绑定的目标用户信息。

4.如权利要求3所述的方法,其特征在于,如果预先配置有每个应用的公钥和私钥,所述登录信息还包括私钥签名。

5.如权利要求3所述的方法,其特征在于,所述向所述第一验证服务器发送所述第一登录标识,及所述第二终端设备中已登录成功的至少一个第二应用的登录信息之前,所述方法还包括:

针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

6.一种多应用的登录装置，其特征在于，应用于第一验证服务器，所述装置包括：

请求处理模块，接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

接收识别模块，用于接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用，并在识别结果为是时，触发登录控制模块；

登录控制模块，用于获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用；

其中，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息包括：

向与目标第二应用对应的目标第二验证服务器发送包含目标第二应用的目标第二登录标识的用户信息请求；接收目标第二验证服务器发送的与目标第二登录标识绑定的目标用户信息。

7.如权利要求6所述的装置，其特征在于，所述登录控制模块，具体用于如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名，根据所述目标第二应用的公钥，对所述目标第二应用的私钥签名进行验签；如果验签通过，进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

8.一种多应用的登录装置，其特征在于，应用于第二终端设备，所述装置包括：

扫描模块，用于扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

发送模块，用于向所述第一验证服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用；

其中，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息包括：

向与目标第二应用对应的目标第二验证服务器发送包含目标第二应用的目标第二登录标识的用户信息请求；接收目标第二验证服务器发送的与目标第二登录标识绑定的目标用户信息。

9.如权利要求8所述的装置，其特征在于，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名。

10.如权利要求8所述的装置，其特征在于，所述装置还包括：

获取模块，用于针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

11.一种验证服务器，其特征在于，包括：处理器、通信接口、存储器和通信总线，其中，处理器，通信接口，存储器通过通信总线完成相互间的通信；

所述存储器中存储有计算机程序，当所述程序被所述处理器执行时，使得所述处理器执行权利要求1-2任一项所述方法的步骤。

12.一种终端设备，其特征在于，包括：处理器、通信接口、存储器和通信总线，其中，处理器，通信接口，存储器通过通信总线完成相互间的通信；

所述存储器中存储有计算机程序，当所述程序被所述处理器执行时，使得所述处理器执行权利要求3-5任一项所述方法的步骤。

13.一种计算机可读存储介质，其特征在于，其存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行权利要求1-2任一项所述方法的步骤。

14.一种计算机可读存储介质，其特征在于，其存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行权利要求3-5任一项所述方法的步骤。

一种多应用的登录方法及装置

技术领域

[0001] 本发明涉及计算机技术领域，尤其涉及一种多应用的登录方法及装置。

背景技术

[0002] 随着科学技术的发展和人们生活水平的不断提高，终端设备逐渐走进了人们的工作和生活，为人们的工作和生活带来了极大的便利。人们通过终端设备上的各种应用进行娱乐、学习、办公等，但是用户在终端设备上使用应用时通常需要登录应用，登录成功后才能实现对应用的使用。

[0003] 目前登录应用的常见登录方式就是用户名和密码登录，然而这种登录方式需要每次登录都输入用户名和密码，登录过程繁琐，影响了用户体验。为了简化登录过程，现有技术多采用二维码登录的方式，例如：在某一终端设备A上显示某一应用的登录二维码，如在电脑上显示微信的登录二维码；通过另一已登录该应用的终端设备B，扫描终端设备A上显示的某一应用的登录二维码，获取终端设备A上显示的某一应用的登录二维码中的登录标识，并将登录标识与终端设备B中已登录该应用的用户信息发送给验证服务器，验证服务器将终端设备A显示的二维码中包含的登录标识与终端设备B发送的用户信息绑定，实现在终端设备A上登录该应用。

[0004] 然而，现有技术中的登录方式仅依赖于同一应用间的认证登录，登录方式不灵活，影响了用户体验。

发明内容

[0005] 本发明提供一种多应用的登录方法及装置，用以解决现有技术中存在登录方式不灵活，影响用户体验的问题。

[0006] 第一方面，本发明公开了一种多应用的登录方法，应用于第一验证服务器，所述方法包括：

[0007] 接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

[0008] 接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用；

[0009] 如果是，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0010] 可选的，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括第二应用的私钥签名，所述获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息之前，所述方法还包括：

[0011] 根据所述目标第二应用的公钥，对所述目标第二应用的私钥签名进行验签；

[0012] 如果验签通过，进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

[0013] 第二方面，本发明公开了一种多应用的登录方法，应用于第二终端设备，所述方法包括：

[0014] 扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

[0015] 向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0016] 可选的，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名。

[0017] 可选的，所述向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息之前，所述方法还包括：

[0018] 针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

[0019] 第三方面，本发明公开了一种多应用的登录装置，应用于第一验证服务器，所述装置包括：

[0020] 请求处理模块，接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

[0021] 接收识别模块，用于接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用，并在识别结果为是时，触发登录控制模块；

[0022] 登录控制模块，用于获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0023] 可选的，所述登录控制模块，具体用于如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名，根据所述目标第二应用的公钥，对所述目标第二应用的私钥签名进行验签；如果验签通过，进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

[0024] 第四方面，本发明公开一种多应用的登录装置，应用于第二终端设备，所述装置包括：

[0025] 扫描模块，用于扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服

务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

[0026] 发送模块，用于向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0027] 可选的，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名。

[0028] 可选的，所述装置还包括：

[0029] 获取模块，用于针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

[0030] 第五方面，本发明公开了一种验证服务器，包括：处理器、通信接口、存储器和通信总线，其中，处理器，通信接口，存储器通过通信总线完成相互间的通信；

[0031] 所述存储器中存储有计算机程序，当所述程序被所述处理器执行时，使得所述处理器执行上述第一方面任一项所述方法的步骤。

[0032] 第六方面，本发明公开了一种终端设备，包括：处理器、通信接口、存储器和通信总线，其中，处理器，通信接口，存储器通过通信总线完成相互间的通信；

[0033] 所述存储器中存储有计算机程序，当所述程序被所述处理器执行时，使得所述处理器执行上述第二方面任一项所述方法的步骤。

[0034] 第七方面，本发明公开了一种计算机可读存储介质，其存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行上述第一方面任一项所述方法的步骤。

[0035] 第八方面，本发明公开了一种计算机可读存储介质，其存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行上述第二方面任一项所述方法的步骤。

[0036] 本发明有益效果如下：

[0037] 由于在本发明实施例中，第一验证服务器预先保存有第一应用认可登录状态的第三应用的应用列表，在扫描第一终端设备的第一应用对应的登录二维码的第二终端设备中存在第一应用认可登录状态的已登录成功的目标第二应用时，根据任一已登录成功的目标第二应用对应的目标用户信息使第一终端设备登录第一应用，实现了不同应用间的相互认证，提高了登录的灵活性，提高了用户体验。

附图说明

[0038] 为了更清楚地说明本发明实施例或现有技术中的技术方案，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。

[0039] 图1为本发明实施例提供的多应用的登录方法适用的一种通信架构示意图；

[0040] 图2为本发明实施例提供的一种多应用的登录过程示意图；

[0041] 图3为本发明实施例提供的一种多应用的登录过程示意图；

[0042] 图4为本发明实施例提供的一种多应用的登录装置结构示意图；

[0043] 图5为本发明实施例提供的一种多应用的登录装置结构示意图；

[0044] 图6为本发明实施例提供的一种验证服务器；

[0045] 图7为本发明实施例提供的一种终端设备。

具体实施方式

[0046] 为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0047] 需要理解的是，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。本申请中所涉及的多种，是指两种或两种以上。

[0048] 下面将结合附图，对本申请实施例进行详细描述。

[0049] 图1为本发明实施例提供的多应用的登录方法适用的一种通信架构示意图，如图1所示，包含第一终端设备、第二终端设备、用于对第一应用进行登录验证和管理的第一验证服务器、及与多个第二应用分别一一对应的进行登录验证和管理的第二验证服务器。在本发明实施例中，第一终端设备可以为手机、平板电脑、掌上电脑、个人电脑等设备；第二终端设备可以为具有二维码扫描功能的手机、平板电脑等设备；验证服务器可以为具有登录验证和管理功能的服务器或服务器集群等。以下结合具体实施例对本申请的登录过程进行说明。

[0050] 实施例1：

[0051] 图2为本发明实施例提供的一种多应用的登录过程示意图，该过程包括：

[0052] S201：接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码。

[0053] 在本发明实施例中，验证服务器针对接收到的每个应用的登录请求，均会生成一个与该登录请求唯一对应的登录标识，用以标识该登录请求，例如：登录请求标识中可以包含全局唯一标识符(Globally Unique Identifier，GUID)等用于保证登录请求标识的唯一性。

[0054] 另外，在实际应用中，用户可以通过点击显示在第一终端设备的第一应用的图标触发第一终端设备向与第一应用对应的第一验证服务器发送第一应用的登录请求；也可以是通过其它应用程序或事件触发第一终端设备向与第一应用对应的第一验证服务器发送第一应用的登录请求，在本发明实施例中不进行限定。

[0055] 具体的，第一验证服务器接收到第一终端设备发送的第一应用的登录请求后，生成与该登录请求对应的第一登录标识并存储，并生成包含该第一登录标识的登录二维码，将生成的该登录二维码发送给第一终端设备，使第一终端设备显示该登录二维码用于扫描二维码登录。

[0056] 较佳的，为了便于扫描登录二维码的终端设备，对与第一应用对应的第一验证服务器的信息的获知，第一登录标识中还包含第一验证服务器的标识信息，如：网络之间互连的协议(Internet Protocol，IP)地址、媒体访问控制地址(Media Access Control Address，MAC)地址、统一资源定位符(Uniform Resource Locator，URL)等，便于扫描登录二维码的终端设备对第一验证服务器的信息的获知；当然了，第一验证服务器也可以是生成包含第一登录标识和第一验证服务器的标识信息的登录二维码，便于扫描登录二维码的终端设备对第一验证服务器的信息的获知。具体的，在登录二维码中包含进行登录验证和管理的验证服务器的标识信息是本领域常规技术，不再进行赘述。

[0057] S202：接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用，如果是，进行S203，如果否，则结束。

[0058] 在第一验证服务器中预先保存有其进行登录验证的第一应用认可登录状态的第三应用的应用列表，其中第一应用认可登录状态的第三应用可以为一个也可以为多个，在应用列表中保存有第一应用认可登录状态的每个第三应用的应用标识，如应用名称、应用ID等，较佳的，在应用列表中还保存有应用列表中每个第三应用对应的验证服务器的标识信息，如：IP地址、MAC地址、URL等，便于第一验证服务器对与第三应用对应的验证服务器的信息的获知。其中，第一应用认可登录状态的第三应用的应用列表可由用户预先配置完成。

[0059] 具体的，在用户需要在第一终端设备登录第一应用时，通过第二终端设备扫描第一终端设备显示的第一应用的登录二维码，获取该登录二维码中包含的第一登录标识，并将获取的第一登录标识，及第二终端设备中已登录成功的至少一个第二应用的登录信息发送给与第一应用对应的第一验证服务器。

[0060] 第一验证服务器接收到第二终端发送的第一登录标识及第二终端设备已登录成功的至少一个第二应用的登录信息，根据每个第二应用的应用标识及预先保存的第一应用认可登录状态的第三应用的应用列表，识别第二终端设备已登录成功的至少一个第二应用中，是否存在位于第一应用认可登录状态的应用列表中的目标第二应用。

[0061] 在本发明实施例中，第二应用的第二登录标识，针对每次第二应用的登录也是唯一的，具体的，如果第二应用当前登录是通过扫描第二应用的登录二维码登录成功的，则第二终端中保存的第二应用的第二登录标识，与第二应用对应的第二验证服务器对该次登录生成的登录二维码中的第二登录标识相同；如果第二应用当前是通过用户名和密码等方式登录，第二验证服务器未生成与当前第二应用登录对应的登录二维码，则第二验证服务器会针对第二应用该次登录生成一个第二登录标识用于绑定本次登录第二应用的用户信息，并将生成的第二登录标识发送给第二终端。

[0062] S203：获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0063] 具体的，如果第二终端设备已登录成功的至少一个第二应用中，存在位于第一应用认可登录状态的应用列表中的目标第二应用，第一验证服务器根据任一第一应用认可登录状态的目标第二应用，向与该目标第二应用对应的目标第二验证服务器发送包含该目标

第二应用的目标第二登录标识的用户信息请求;目标第二验证服务器接收到包含目标第二登录标识的用户信息请求后,将与目标登录标识绑定的目标用户信息发送给第一验证服务器,第一验证服务器接收到该目标用户信息后,将该目标用户信息与第一终端设备发送的第一应用的登录请求对应的第一登录标识绑定,使得第一终端设备通过该目标用户信息登录第一应用。

[0064] 另外,如果第二终端设备已登录成功的至少一个第二应用中,不存在位于第一应用认可登录状态的应用列表中的目标第二应用,则需要通过其它登录方式登录第一应用,如用户名和密码登录。

[0065] 此外,为了保证登录的可靠性,如果第二终端设备已登录成功的至少一个第二应用中,存在位于第一应用认可登录状态的应用列表中的多个目标第二应用时,如果第一验证服务器选择的某一目标第二应用的登录状态已失效,例如该目标第二应用对应的目标第二登录标识在与该目标第二应用对应的目标第二验证服务器中该目标第二登录标识与用户信息解除绑定,标识用户已退出登录状态,第一服务器可以继续轮询存在位于第一应用认可登录状态的应用列表中的其它目标第二应用,以保证登录的可靠性。

[0066] 较佳的,第一验证服务器在确定某一目标第二应用的登录状态已失效,还可以将包含该目标第二应用的应用标识的失效信息发送给第二终端,使第二终端删除该目标第二应用的登录信息。

[0067] 在本发明实施例中,第二终端设备进行的操作均可由第二终端设备中的某一特定应用实现,如认证应用不再进行赘述。

[0068] 由于在本发明实施例中,第一验证服务器预先保存有第一应用认可登录状态的第三应用的应用列表,在扫描第一终端设备的第一应用对应的登录二维码的第二终端设备中存在第一应用认可登录状态的已登录成功的目标第二应用时,根据任一已登录成功的目标第二应用对应的目标用户信息使第一终端设备登录第一应用,实现了不同应用间的相互认证,提高了登录的灵活性,提高了用户体验。

[0069] 实施例2:

[0070] 为了提高登录的可靠性,在上述实施例的基础上,在本发明实施例中,如果预先配置有每个应用的公钥和私钥,所述登录信息还包括私钥签名,所述获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息之前,所述方法还包括:

[0071] 根据所述目标第二应用的公钥,对所述目标第二应用的私钥签名进行验签;

[0072] 如果验签通过,进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

[0073] 在本发明实施例中,每个应用还可以配置有公钥和私钥,并对外公开公钥。

[0074] 具体的,第一验证服务器在通过与目标第二应用对应的目标第二验证服务器,获取与目标第二登录标识对应的目标用户信息之前,根据该目标第二应用的公钥对该目标第二应用的私钥签名进行验签,即根据该目标第二应用的公钥对该目标第二应用的私钥签名进行解密,如果解密成功,确定验签通过,通过与该目标第二应用对应的目标第二验证服务器,获取与该目标第二登录标识对应的目标用户信息,用于对第一应用的登录。

[0075] 如果验签不通过,则确定该目标第二应用不可用,第一验证服务器继续轮询存在位于第一应用认可登录状态的应用列表中的其它目标第二应用,以保证登录的可靠性。

[0076] 在本发明实施例中，第二终端设备可以根据第二应用的私钥对第二应用的应用ID、唯一登录标识等中的一种或多种进行加密，生成私钥签名，在本申请中不进行具体限定。

[0077] 实施例3：

[0078] 图3为本发明实施例提供的一种多应用的登录过程示意图，该过程包括：

[0079] S301：扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的。

[0080] 在本发明实施例中，验证服务器针对接收到的每个应用的登录请求，均会生成一个与该登录请求唯一对应的登录标识，用以标识该登录请求，例如：登录请求标识中可以包含GUID等用于保证登录请求标识的唯一性。

[0081] 具体的，第一验证服务器接收到第一终端设备发送的第一应用的登录请求后，生成与该登录请求对应的第一登录标识并存储，并生成包含该第一登录标识的登录二维码，将生成的该登录二维码发送给第一终端设备，使第一终端设备显示该登录二维码用于扫描二维码登录。在用户需要在第一终端设备登录第一应用时，通过第二终端设备扫描第一终端设备显示的第一应用的登录二维码，获取该登录二维码中包含的第一登录标识。

[0082] 较佳的，为了便于扫描登录二维码的终端设备对第一应用对应的第一验证服务器的信息的获知，第一登录标识中还包含第一验证服务器的标识信息，如：IP地址、MAC地址、URL等；具体的，在登录二维码中包含进行登录验证和管理的验证服务器的标识信息是本领域常规技术，不再进行赘述。

[0083] S302：向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0084] 在第一验证服务器中预先保存有其进行登录验证的第一应用认可登录状态的第三应用的应用列表，其中第一应用认可登录状态的第三应用可以为一个也可以为多个，在应用列表中保存有第一应用认可登录状态的每个第三应用的应用标识，如应用名称、应用ID等，较佳的，在应用列表中还保存有应用列表中每个第三应用对应的验证服务器的标识信息，如：IP地址、MAC地址、URL等，便于第一验证服务器对与第三应用对应的验证服务器的信息的获知。其中，第一应用认可登录状态的第三应用的应用列表可由用户预先配置完成。

[0085] 第二终端将获取的第一登录标识，及第二终端设备中已登录成功的至少一个第二应用的登录信息发送给与第一应用对应的第一验证服务器。第一验证服务器接收到第二终端发送的第一登录标识及第二终端设备已登录成功的至少一个第二应用的登录信息，根据每个第二应用的应用标识及预先保存的第一应用认可登录状态的第三应用的应用列表，识别第二终端设备已登录成功的至少一个第二应用中，是否存在位于第一应用认可登录状态的应用列表中的目标第二应用。

[0086] 在本发明实施例中，第二应用的第二登录标识，针对每次第二应用的登录也是唯

一的，具体的，如果第二应用当前登录是通过扫描第二应用的登录二维码登录成功的，则第二终端中保存的第二应用的第二登录标识，与第二应用对应的第二验证服务器对该次登录生成的登录二维码中的第二登录标识相同；如果第二应用当前是通过用户名和密码等方式登录，第二验证服务器未生成与当前第二应用登录对应的登录二维码，则第二验证服务器会针对第二应用该次登录生成一个第二登录标识用于绑定本次登录第二应用的用户信息，并将生成的第二登录标识发送给第二终端。

[0087] 如果第二终端设备已登录成功的至少一个第二应用中，存在位于第一应用认可登录状态的应用列表中的目标第二应用，第一验证服务器根据任一第一应用认可登录状态的目标第二应用，向与该目标第二应用对应的目标第二验证服务器发送包含该目标第二应用的目标第二登录标识的用户信息请求；目标第二验证服务器接收到包含目标第二登录标识的用户信息请求后，将与目标登录标识绑定的目标用户信息发送给第一验证服务器，第一验证服务器接收到该目标用户信息后，将该目标用户信息与第一终端设备发送的第一应用的登录请求对应的第一登录标识绑定，使得第一终端设备通过该目标用户信息登录第一应用。

[0088] 另外，如果第二终端设备已登录成功的至少一个第二应用中，不存在位于第一应用认可登录状态的应用列表中的目标第二应用，则需要通过其它登录方式登录第一应用，如用户名和密码登录。

[0089] 此外，为了保证登录的可靠性，如果第二终端设备已登录成功的至少一个第二应用中，存在位于第一应用认可登录状态的应用列表中的多个目标第二应用时，如果第一验证服务器选择的某一目标第二应用的登录状态已失效，例如该目标第二应用对应的目标第二登录标识在与该目标第二应用对应的目标第二验证服务器中该目标第二登录标识与用户信息解除绑定，标识用户已退出登录状态，第一服务器可以继续轮询存在位于第一应用认可登录状态的应用列表中的其它目标第二应用，以保证登录的可靠性。

[0090] 较佳的，第一验证服务器在确定某一目标第二应用的登录状态已失效，还可以将包含该目标第二应用的应用标识的失效信息发送给第二终端，使第二终端删除该目标第二应用的登录信息。

[0091] 在本发明实施例中，第二终端设备进行的操作均可由第二终端设备中的某一特定应用实现，如认证应用不再进行赘述。

[0092] 较佳的，为了便于第一验证服务器对第二终端设备中已登录成功的各第二应用的合法性进行验证，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名，使第二终端设备能根据第二应用的公钥对第二应用的私钥签名进行验签，具体验签过程参见上述实施例2，不再进行赘述。

[0093] 实施例4：

[0094] 在上述各实施例的基础上，在本发明实施例中，所述向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息之前，所述方法还包括：

[0095] 针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

[0096] 具体的，在第二终端设备中每个第二应用登录成功后，第二终端设备获取该第二

应用的登录信息，并保存。具体的，第二终端设备可以直接在第二终端中每个第二应用登录成功后，直接读取第二终端设备中保存的该第二应用的登录信息，也可以是第二终端设备中每个第二应用登录成功后，该第二应用生成一个包含登录信息的登录信息二维码，第二终端设备可以根据该登录信息二维码获取该第二应用的登录信息并保存，其中应用的登录信息包括应用标识、对应的登录标识、私钥签名等。

[0097] 实施例5：

[0098] 图4为本发明实施例提供的一种多应用的登录装置结构示意图，应用于第一验证服务器，该装置包括：

[0099] 请求处理模块41，接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

[0100] 接收识别模块42，用于接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用，并在识别结果为是时，触发登录控制模块；

[0101] 登录控制模块43，用于获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0102] 所述登录控制模块43，具体用于如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名，根据所述目标第二应用的公钥，对所述目标第二应用的私钥签名进行验签；如果验签通过，进行获取与所述目标第二应用的目标第二登录标识对应的目标用户信息的步骤。

[0103] 实施例6：

[0104] 图5为本发明实施例提供的一种多应用的登录装置结构示意图，应用于第二终端设备，该装置包括：

[0105] 扫描模块51，用于扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

[0106] 发送模块52，用于向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0107] 优选地，如果预先配置有每个应用的公钥和私钥，所述登录信息还包括私钥签名。

[0108] 所述装置还包括：

[0109] 获取模块53，用于针对所述第二终端设备中每个已登录成功的第二应用，获取该第二应用的登录信息。

[0110] 实施例7：

[0111] 在上述各实施例的基础上，本发明实施例还提供了一种验证服务器，如图6所示，包括：处理器61、通信接口62、存储器63和通信总线64，其中，处理器61，通信接口62，存储器63通过通信总线64完成相互间的通信；

[0112] 所述存储器63中存储有计算机程序，当所述程序被所述处理器61执行时，使得所述处理器61执行以下步骤：

[0113] 接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

[0114] 接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用；

[0115] 如果是，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0116] 实施例8：

[0117] 在上述各实施例的基础上，本发明实施例还提供了一种终端设备，如图7所示，包括：处理器71、通信接口72、存储器73和通信总线74，其中，处理器71，通信接口72，存储器73通过通信总线74完成相互间的通信；

[0118] 所述存储器73中存储有计算机程序，当所述程序被所述处理器71执行时，使得所述处理器71执行以下步骤：

[0119] 扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

[0120] 向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0121] 实施例9：

[0122] 在上述各实施例的基础上，本发明实施例还提供了一种计算机存储可读存储介质，所述计算机可读存储介质内存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行时实现如下步骤：

[0123] 接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码；

[0124] 接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所

述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用；

[0125] 如果是，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0126] 实施例10：

[0127] 在上述各实施例的基础上，本发明实施例还提供了一种计算机存储可读存储介质，所述计算机可读存储介质内存储有可由电子设备执行的计算机程序，当所述程序在所述电子设备上运行时，使得所述电子设备执行时实现如下步骤：

[0128] 扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的；

[0129] 向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用。

[0130] 对于系统/装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0131] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0132] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0133] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0134] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0135] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优

选实施例以及落入本申请范围的所有变更和修改。

[0136] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

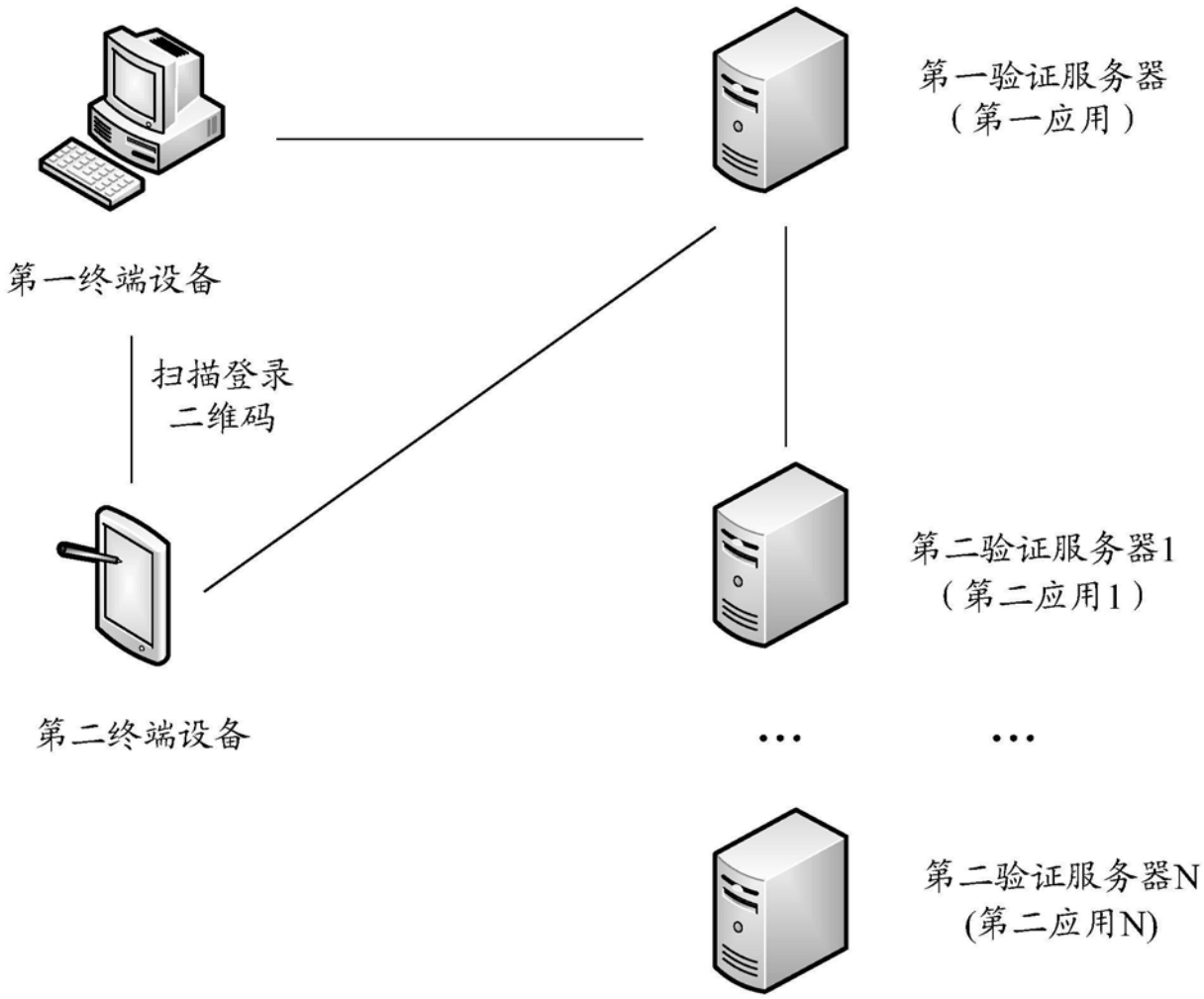

第一验证服务器
（第一应用）
第一终端设备
扫描登录
二维码
第二验证服务器1
（第二应用1）
第二终端设备
...
...
第二验证服务器N
(第二应用N)

图1

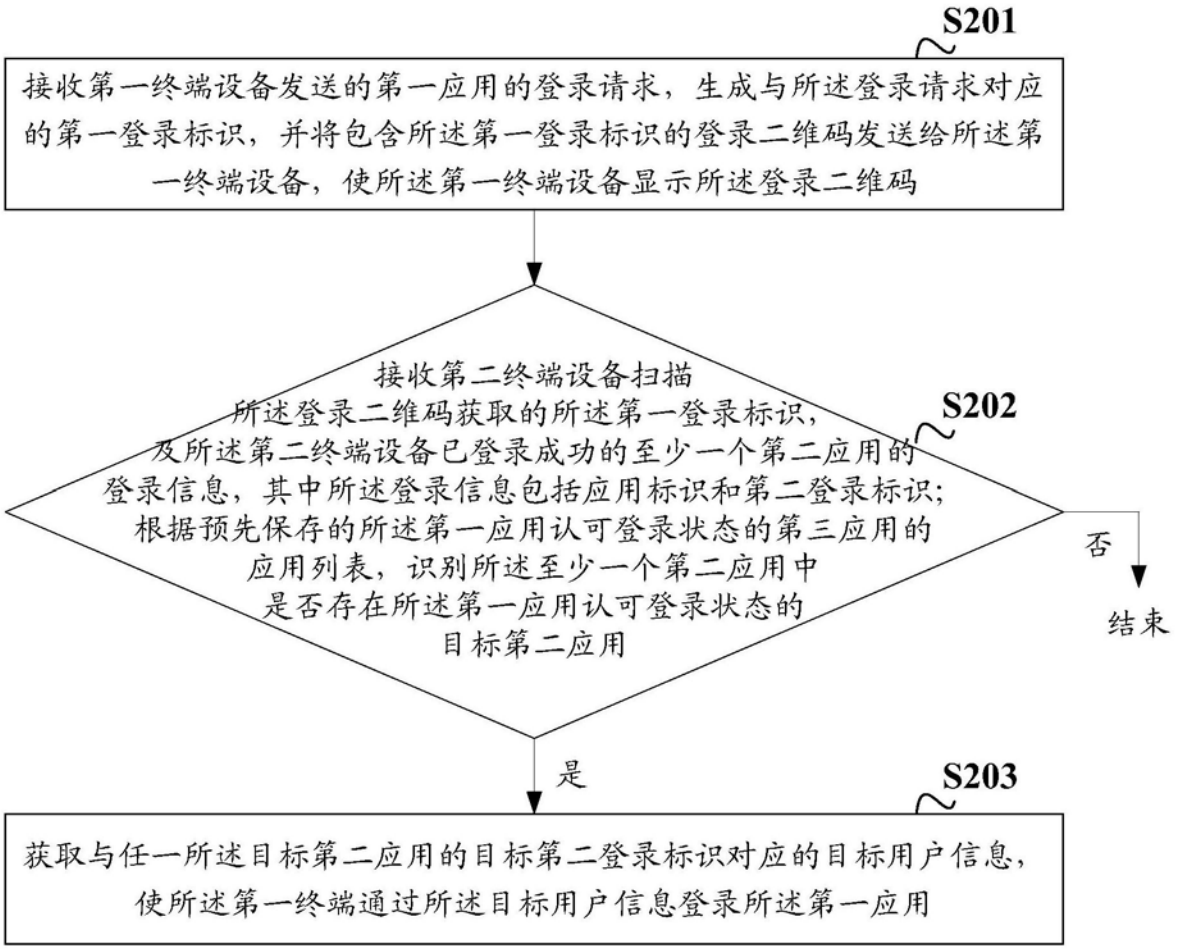

S201
接收第一终端设备发送的第一应用的登录请求，生成与所述登录请求对应的第一登录标识，并将包含所述第一登录标识的登录二维码发送给所述第一终端设备，使所述第一终端设备显示所述登录二维码
S202
接收第二终端设备扫描所述登录二维码获取的所述第一登录标识，及所述第二终端设备已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，识别所述至少一个第二应用中是否存在所述第一应用认可登录状态的目标第二应用
否
结束
是
S203
获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用

图2

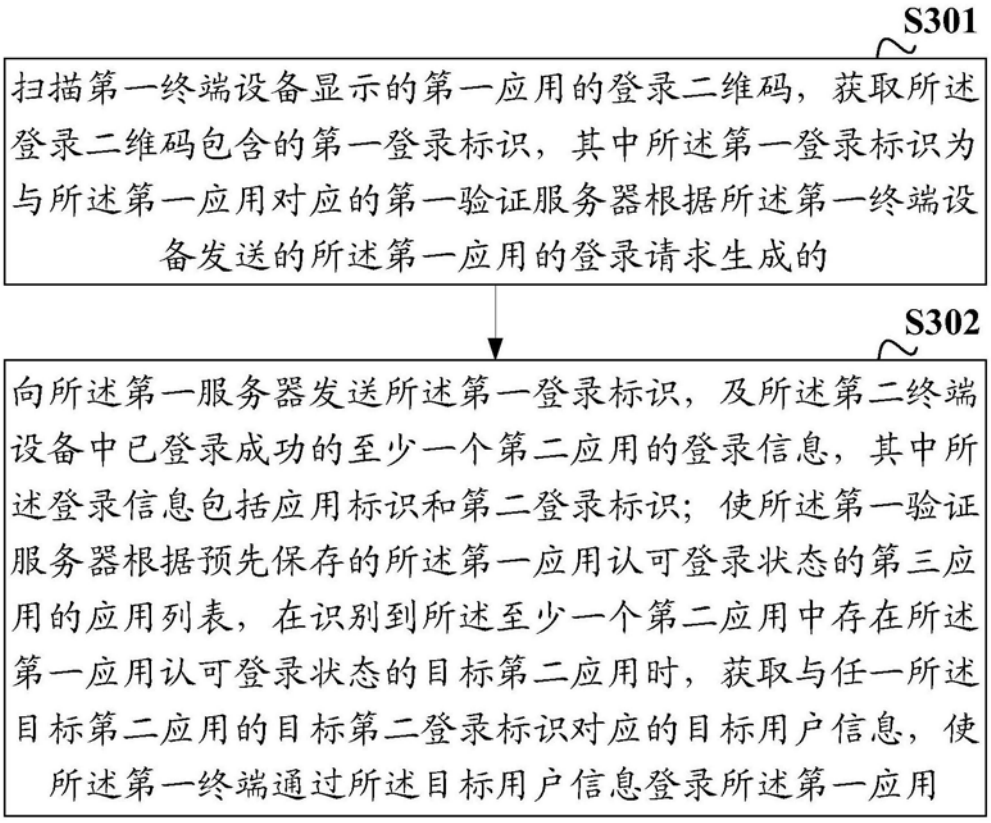

S301
扫描第一终端设备显示的第一应用的登录二维码，获取所述登录二维码包含的第一登录标识，其中所述第一登录标识为与所述第一应用对应的第一验证服务器根据所述第一终端设备发送的所述第一应用的登录请求生成的
S302
向所述第一服务器发送所述第一登录标识，及所述第二终端设备中已登录成功的至少一个第二应用的登录信息，其中所述登录信息包括应用标识和第二登录标识；使所述第一验证服务器根据预先保存的所述第一应用认可登录状态的第三应用的应用列表，在识别到所述至少一个第二应用中存在所述第一应用认可登录状态的目标第二应用时，获取与任一所述目标第二应用的目标第二登录标识对应的目标用户信息，使所述第一终端通过所述目标用户信息登录所述第一应用

图3

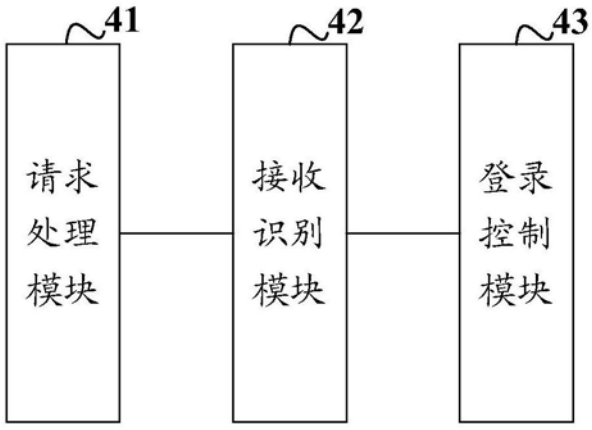

41
42
43
请求处理模块
接收识别模块
登录控制模块

图4

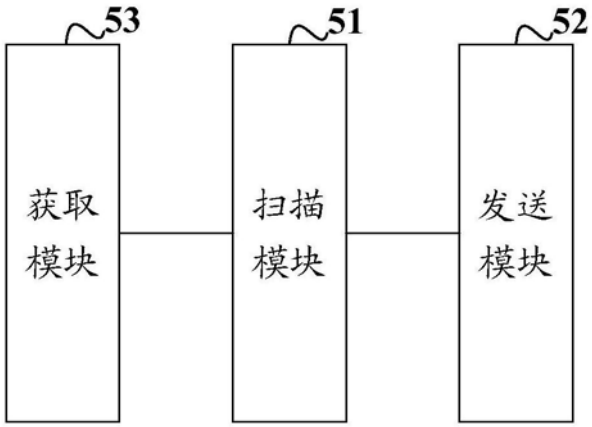

53
51
52
获取模块
扫描模块
发送模块

图5

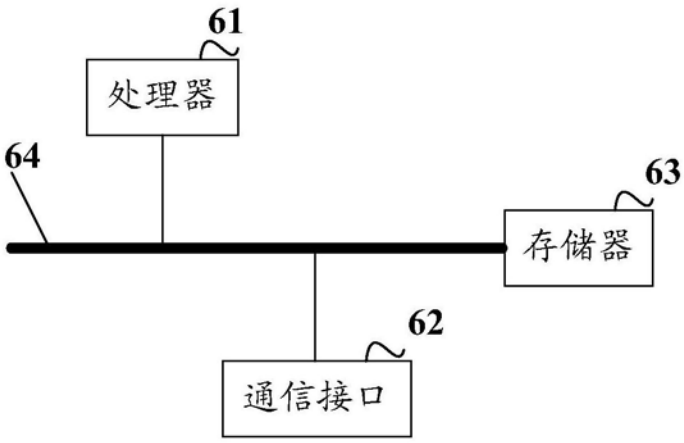

61
处理器
64
63
存储器
62
通信接口

图6

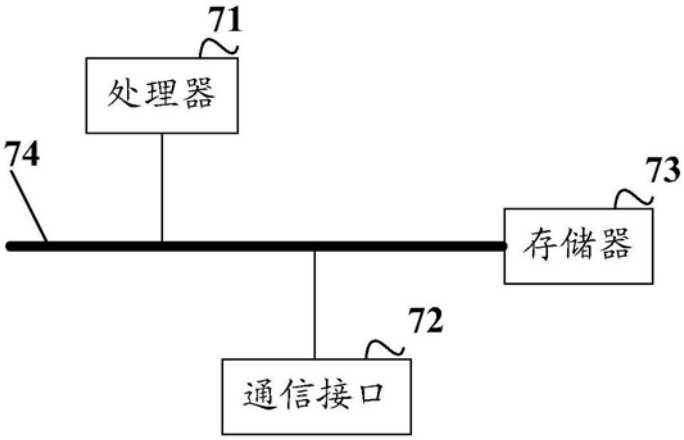

71
处理器
74
73
存储器
72
通信接口

图7