(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105897668 A
(43)申请公布日 2016.08.24

(21)申请号 201510694688.2

(22)申请日 2015.10.22

(71)申请人 乐视致新电子科技(天津)有限公司
地址 300467 天津市滨海新区生态城动漫中路126号动漫大厦B1区二层201-427

(72)发明人 牛云飞

(74)专利代理机构 北京邦信阳专利商标代理有限公司 11012
代理人 张伟杰

(51)Int.Cl.
*H04L 29/06*(2006.01)

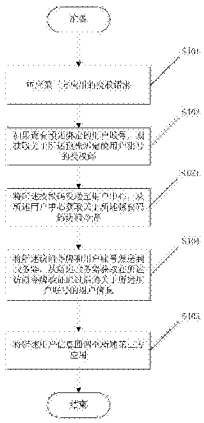
权利要求书4页 说明书10页 附图8页

(54)发明名称

一种第三方账号授权方法、设备、服务器及其系统

(57)摘要

本发明公开一种第三方账号授权方法、设备、服务器及其系统，方法包括：响应第三方应用的授权请求；如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；将所述用户信息回调至所述第三方应用。本发明通过提供一种能够将预先绑定的账号授权给第三方应用使用的方案，使得第三方应用能够获取该安全账号的授权，从而使得第三方应用能够采用该安全账号进行各种敏感操作，例如支付付费等。




CN 105897668 A

1.一种第三方账号授权方法，其特征在于，包括：

第三方授权响应步骤，包括：响应第三方应用的授权请求；

授权码获取步骤，包括：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

访问令牌获取步骤，包括：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

用户信息获取步骤，包括：将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；

信息回调步骤，包括：将所述用户信息回调至所述第三方应用。

2.根据权利要求1所述的第三方账号授权方法，其特征在于，所述获取关于所述预先绑定的用户账号的授权码，具体包括：

获取所述第三方应用的应用标识和应用密钥；

对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

3.根据权利要求1所述的第三方账号授权方法，其特征在于，所述授权码获取步骤，还包括：如果没有预先绑定的用户账号，则：

获取所述第三方应用的应用标识和应用密钥；

将所述应用标识和所述应用密钥发送到服务器；

显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行访问令牌获取步骤，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

4.根据权利要求1所述的第三方账号授权方法，其特征在于，所述访问令牌获取步骤中，获取所述访问令牌后与所述用户账号关联保存；

所述第三方授权响应步骤，具体包括：

当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述用户信息获取步骤，否则执行所述授权码获取步骤。

5.根据权利要求1所述的第三方账号授权方法，其特征在于，所述信息回调步骤，具体包括：

将所述用户信息进行哈希封装后回调至所述第三方应用。

6.根据权利要求1所述的第三方账号授权方法，其特征在于，所述第三方授权响应步骤，具体包括：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用Java基于安卓系统生成，且所述授权页面的显示资源来自以Java库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用Java的反射机制从安卓系统所提供的R文件中获取。

7.一种第三方账号授权方法，其特征在于，包括：

访问令牌接收步骤，包括：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于

所述授权码的访问令牌；

用户信息发送步骤，包括：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

8. 根据权利要求 7 所述的第三方账号授权方法，其特征在于，还包括，授权码发送步骤；

所述授权码发送步骤，包括：

接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

9. 一种第三方账号授权设备，其特征在于，包括：

第三方授权响应模块，用于：响应第三方应用的授权请求；

授权码获取模块，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

访问令牌获取模块，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

用户信息获取模块，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；

信息回调模块，用于：将所述用户信息回调至所述第三方应用。

10. 根据权利要求 9 所述的第三方账号授权设备，其特征在于，所述获取关于所述预先绑定的用户账号的授权码，具体用于：

获取所述第三方应用的应用标识和应用密钥；

对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

11. 根据权利要求 9 所述的第三方账号授权设备，其特征在于，所述授权码获取模块，还用于：如果没有预先绑定的用户账号，则：

获取所述第三方应用的应用标识和应用密钥；

将所述应用标识和所述应用密钥发送到服务器；

显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行访问令牌获取模块，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

12. 根据权利要求 9 所述的第三方账号授权设备，其特征在于，所述访问令牌获取模块中，获取所述访问令牌后与所述用户账号关联保存；

所述第三方授权响应模块，具体用于：

当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述用户信息获取模块，否则执行所述授权码获取模块。

13. 根据权利要求 9 所述的第三方账号授权设备，其特征在于，所述信息回调模块，具体用于：

将所述用户信息进行哈希封装后回调至所述第三方应用。

14. 根据权利要求 9 所述的第三方账号授权设备，其特征在于，所述第三方授权响应模块，具体用于：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用 Java 基于安卓系统生成，且所述授权页面的显示资源来自以 Java 库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用 Java 的反射机制从安卓系统所提供的 R 文件中获取。

15. 一种第三方账号授权服务器，其特征在于，包括：

访问令牌接收模块，用于：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌；

用户信息发送模块，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

16. 根据权利要求 15 所述的第三方账号授权服务器，其特征在于，还包括，授权码发送模块；

所述授权码发送模块，用于：

接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

17. 一种第三方账号授权系统，包括：设备端和服务器端；

所述设备端，包括：

设备端第三方授权响应模块，用于：响应第三方应用的授权请求；

设备端授权码获取模块，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

设备端访问令牌获取模块，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

设备端用户信息获取模块，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取关于所述用户账号的用户信息；

设备端信息回调模块，用于：将所述用户信息回调至所述第三方应用；

所述服务器端，包括：

服务器端访问令牌接收模块，用于：接收到来自设备的访问令牌和用户账号；

服务器端用户信息发送模块，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备。

# 一种第三方账号授权方法、设备、服务器及其系统

## 技术领域

[0001] 本发明涉及账号管理相关技术领域，特别是一种第三方账号授权方法、设备、服务器及其系统。

## 背景技术

[0002] 智能手机，是指像个人电脑一样，具有独立的操作系统，独立的运行空间，可以由用户自行安装软件、游戏、导航等第三方服务商提供的程序，并可以通过移动通讯网络来实现无线网络接入的手机类型。

[0003] 智能手机中所运行的软件称为应用 (App)，通过 App 能够为智能手机带来非常多的功能。

[0004] 用户账号是用于标识用户身份，因此如何保证用户账号的安全非常重要。现有技术一般采用的是将用户账号保存到服务器，用户在登陆时通过用户密码进行验证。

[0005] 然而，当用户账号过多时，其很难保证其账号的安全性，因此 App 很难采用账号进行敏感操作，例如支付付费等。

## 发明内容

[0006] 基于此，有必要针对现有技术难以保证账号的安全性的技术问题，提供一种第三方账号授权方法、设备、服务器及其系统。

[0007] 本发明提供一种第三方账号授权方法，包括：

[0008] 第三方授权响应步骤，包括：响应第三方应用的授权请求；

[0009] 授权码获取步骤，包括：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0010] 访问令牌获取步骤，包括：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0011] 用户信息获取步骤，包括：将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；

[0012] 信息回调步骤，包括：将所述用户信息回调至所述第三方应用。

[0013] 进一步的，所述获取关于所述预先绑定的用户账号的授权码，具体包括：

[0014] 获取所述第三方应用的应用标识和应用密钥；

[0015] 对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

[0016] 进一步的，所述授权码获取步骤，还包括：如果没有预先绑定的用户账号，则：

[0017] 获取所述第三方应用的应用标识和应用密钥；

[0018] 将所述应用标识和所述应用密钥发送到服务器；

[0019] 显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

[0020] 获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行访问令牌获取步骤，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

[0021] 进一步的，所述访问令牌获取步骤中，获取所述访问令牌后与所述用户账号关联保存；

[0022] 所述第三方授权响应步骤，具体包括：

[0023] 当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述用户信息获取步骤，否则执行所述授权码获取步骤。

[0024] 进一步的，所述信息回调步骤，具体包括：

[0025] 将所述用户信息进行哈希封装后回调至所述第三方应用。

[0026] 进一步的，所述第三方授权响应步骤，具体包括：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用 Java 基于安卓系统生成，且所述授权页面的显示资源来自以 Java 库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用 Java 的反射机制从安卓系统所提供的 R 文件中获取。

[0027] 本发明提供一种第三方账号授权方法，包括：

[0028] 访问令牌接收步骤，包括：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌；

[0029] 用户信息发送步骤，包括：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

[0030] 进一步的，还包括，授权码发送步骤；

[0031] 所述授权码发送步骤，包括：

[0032] 接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

[0033] 如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

[0034] 如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

[0035] 本发明提供一种第三方账号授权设备，包括：

[0036] 第三方授权响应模块，用于：响应第三方应用的授权请求；

[0037] 授权码获取模块，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0038] 访问令牌获取模块，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0039] 用户信息获取模块，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；

[0040] 信息回调模块，用于：将所述用户信息回调至所述第三方应用。

[0041] 进一步的，所述获取关于所述预先绑定的用户账号的授权码，具体用于：

[0042] 获取所述第三方应用的应用标识和应用密钥；

[0043] 对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

[0044] 进一步的，所述授权码获取模块，还用于：如果没有预先绑定的用户账号，则：

[0045] 获取所述第三方应用的应用标识和应用密钥；

[0046] 将所述应用标识和所述应用密钥发送到服务器；

[0047] 显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

[0048] 获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行访问令牌获取模块，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

[0049] 进一步的，所述访问令牌获取模块中，获取所述访问令牌后与所述用户账号关联保存；

[0050] 所述第三方授权响应模块，具体用于：

[0051] 当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述用户信息获取模块，否则执行所述授权码获取模块。

[0052] 进一步的，所述信息回调模块，具体用于：

[0053] 将所述用户信息进行哈希封装后回调至所述第三方应用。

[0054] 进一步的，所述第三方授权响应模块，具体用于：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用 Java 基于安卓系统生成，且所述授权页面的显示资源来自以 Java 库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用 Java 的反射机制从安卓系统所提供的 R 文件中获取。

[0055] 本发明提供一种第三方账号授权服务器，包括：

[0056] 访问令牌接收模块，用于：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌；

[0057] 用户信息发送模块，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

[0058] 进一步的，还包括，授权码发送模块；

[0059] 所述授权码发送模块，用于：

[0060] 接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

[0061] 如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

[0062] 如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

[0063] 本发明提供一种第三方账号授权系统，包括：设备端和服务器端；

[0064] 所述设备端，包括：

[0065] 设备端第三方授权响应模块，用于：响应第三方应用的授权请求；

[0066] 设备端授权码获取模块，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0067] 设备端访问令牌获取模块，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0068] 设备端用户信息获取模块，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取关于所述用户账号的用户信息；

[0069] 设备端信息回调模块，用于：将所述用户信息回调至所述第三方应用；

[0070] 所述服务器端，包括：

[0071] 服务器端访问令牌接收模块，用于：接收到来自设备的访问令牌和用户账号；

[0072] 服务器端用户信息发送模块，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备。

[0073] 本发明通过提供一种能够将预先绑定的账号授权给第三方应用使用的方案，使得第三方应用能够获取该安全账号的授权，从而使得第三方应用能够采用该安全账号进行各种敏感操作，例如支付付费等。

## 附图说明

[0074] 图 1 为本发明应用于设备的一种第三方账号授权方法的工作流程图；

[0075] 图 2 为本发明应用于服务器的一种第三方账号授权方法的工作流程图；

[0076] 图 3 为本发明一种第三方账号授权设备的结构模块图；

[0077] 图 4 为本发明最佳实施例的设备结构示意图；

[0078] 图 5 为本发明一种第三方账号授权服务器的结构模块图；

[0079] 图 6 为本发明最佳实施例的服务器结构示意图；

[0080] 图 7 为本发明一种第三方账号授权系统的结构模块图；

[0081] 图 8 为本发明的最佳实施例的针对预先绑定用户账号的设备的工作流程图。

## 具体实施方式

[0082] 下面结合附图和具体实施例对本发明做进一步详细的说明。

[0083] 如图 1 所示为本发明一种第三方账号授权方法的工作流程图，包括：

[0084] 步骤 S101，包括：响应第三方应用的授权请求；

[0085] 步骤 S102，包括：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0086] 步骤 S103，包括：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0087] 步骤 S104，包括：将所述访问令牌和用户账号发送到服务器，从所述服务器获取

在所述访问令牌验证通过后的关于所述用户账号的用户信息；

[0088] 步骤S105，包括：将所述用户信息回调至所述第三方应用。

[0089] 本发明的方法可以采用软件开发工具包(Software Development Ki t，sdk)的形式提供给软件开发者。软件开发者所开发的软件应用，即第三方应用，通过调用sdk所提供的函数请求授权，触发步骤S101，从而响应授权请求。步骤S102中，获取预先绑定的用户账号的授权码，并将该授权码发送到用于实现对用户信息的综合管理的用户中心，该用户中心可以与设备一体，也可以是与服务器一体，还可以是单独设备。步骤S103中获取到访问令牌，并通过访问令牌发送到服务器，由于所发送的是访问令牌，因此其能很好地隐藏授权码，避免授权码被非法获取。在步骤S104中，服务器对访问令牌验证后即返回相关的用户信息，该用户信息通过第三方应用所提供的回调函数回调至第三方应用。

[0090] 本发明由于采用的用户账号是预先绑定的，因此其安全性较高，从而使得第三方应用能够采用该用户账号实现各种敏感操作，例如支付付费等。

[0091] 在其中一个实施例中，所述获取关于所述预先绑定的用户账号的授权码，具体包括：

[0092] 获取所述第三方应用的应用标识和应用密钥；

[0093] 对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

[0094] 本实施例进一步对第三方应用的应用标识和应用密钥进行验证，以保证该第三方应用具有相应的权限以取得预先绑定的用户账号的授权码，从而进一步提高安全。

[0095] 在其中一个实施例中，所述步骤S102，还包括：如果没有预先绑定的用户账号，则：

[0096] 获取所述第三方应用的应用标识和应用密钥；

[0097] 将所述应用标识和所述应用密钥发送到服务器；

[0098] 显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

[0099] 获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行步骤S103，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

[0100] 本实施例增加对没有预先绑定用户账号的支持，即如果用户采用的是一个预先绑定有用户账号的设备，则其可以直接在设备中获取授权码，然而，如果用户没有采用预先绑定有用户账号的设备，则其可以通过设备登陆服务器进而获取授权码，服务器对第三方应用的应用标识和应用密钥进行验证以确保其具有足够权限。

[0101] 在其中一个实施例中，所述步骤S103中，获取所述访问令牌后与所述用户账号关联保存；

[0102] 所述步骤S101，具体包括：

[0103] 当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述步骤S104，否则执行所述步骤S102。

[0104] 本实施例中，针对已经取得过用户信息的用户账号，可以直接采用已有的访问令牌，从而减少步骤流程，提高用户信息的获取速度，使得用户获得更好的用户体验。

[0105] 在其中一个实施例中，所述步骤S105，具体包括：

[0106] 将所述用户信息进行哈希封装后回调至所述第三方应用。

[0107] 本实施例通过哈希封装进行回调，从而提高回调速度。优选地，采用哈希地图，即HashMap方式对用户信息进行封装。

[0108] 在其中一个实施例中，所述步骤S101，具体包括：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用Java基于安卓系统生成，且所述授权页面的显示资源来自以Java库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用Java的反射机制从安卓系统所提供的R文件中获取。

[0109] 安卓系统，即Android系统，当采用java进行开发时，其中有一个R文件，即R.Java文件，用于保存资源文件，然而，由于同一个jar包中不能同时具有两个R文件，因此，本实施例的资源文件以l ibrary的形式提供，且将原R文件中，所有资源文件的资源文件标识，即资源文件id采用反射机制来取得，从而使得该sdk能够顺利的被Java开发者调用。

[0110] 如图2所示为本发明一种第三方账号授权方法的工作流程图，包括：

[0111] 步骤S201，包括：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌；

[0112] 步骤S202，包括：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

[0113] 本实施例应用于服务器中，服务器对访问令牌进行验证后返回用户账号的用户信息。

[0114] 在其中一个实施例中，还包括，授权码发送步骤；

[0115] 所述授权码发送步骤，包括：

[0116] 接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

[0117] 如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

[0118] 如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

[0119] 本实施例的步骤处理了用户在采用不预先绑定用户账号的设备时的登陆请求，并返回相应的授权码。

[0120] 如图8所示为本发明的最佳实施例的针对预先绑定用户账号的设备的工作流程图，设备为手机，具体包括：

[0121] 开发者采用本发明所提供的sdk时，首先需要在服务器申请授权的应用标识(appid)、应用密钥(appsecret)、openid和secret_key。

[0122] 步骤S801，将appid，appsecret传给置于手机rom的代理agent，如果appid与

appsecret 验证成功，直接打开登录界面，进行授权登录，登录成功将获得由 agent 返回的授权码 (code)，具体来说：

[0123] 将 openid 与 secret_key 传 给 agent 的 GuideActivity，根 据 startActivityForResult 去 启 动 内 置 在 手 机 rom 里 面 的 com.letv.android.agent.GuideActivity 页面，如果该页面授权成功会在 onActivityResult 中将 code 通过 Intent 回传，取到 code 之后，调用 getAccessToken(code) 来换取用户的 accesstoken；

[0124] 步骤 S802，通过 http 发送到用户中心，用户中心再根据该授权码，把对应该授权码的用户的访问令牌 (accesstoken) 返回，具体来说：

[0125] 将开发者传入的 appid、appsecrect、授权码 code、回调地址组合，成为一个 json 字串，通过 HttpClient 的 POST 发送 getAccessTokenFromServer 请求到用户中心，然后用 RequestCallback 的接口回调从用户中心取到返回的 Json 字段，对其用 JSONObject 解析，取到 accesstoken、uid 字段；

[0126] 步骤 S803，通过 accesstoken，取得用户的账户信息，具体来说：

[0127] 将 accesstoken、uid 传入 getUserBasicInfo 方法，在 getUserBasicInfo 方法中，将 appid、uid、accesstoken、uid 组合成一个 json 字符串，同理根据 HttpClient 的 Get 发送 getUserBasicInfoFromServer 请求，取得用户的基本信息，返回信息包括 :uid、nickname、accesstoken、file_300*300、file_200*200、file_70*70、file_50*50。

[0128] 然后将这些信息组合到回调接口中；

[0129] 步骤 S804，取得用户信息之后，通过 android 的 shareprefer，将 accesstoken 以及 uid、nickname 等存储到本地存储，将 uid 作为主键，如果是根据历史直接点击登录，则会取到所有 shareprefer 中的用户信息，进行展示，然后根据该用户信息取到用户的 accesstoken，然后执行步骤 S803，取到用户信息，将信息回调出去。

[0130] 步骤 S805，通过 sdk 提供的回调接口，将信息回传给第三方应用进行账户信息处理，回调接口将用户信息封装成 HashMap，然后开发者直接可以直接对 HashMap 对象进行操作，具体来说：

[0131] 其封装格式为：

[0132] HashMap<String,Object>userInfo = new HashMap<String,Object>()

[0133] userInfo.put("letv_uid",/* 用户 uid*/)；

[0134] userInfo.put("nickname",/* 昵称 */)；

[0135] userInfo.put("access_token",/* 授权 access token*/)；

[0136] userInfo.put("file_300*300",/*300*300 头像 */)；

[0137] userInfo.put("file_200*200",/*200*200 头像 */)；

[0138] userInfo.put("file_70*70",/*70*70 头像 */)；

[0139] userInfo.put("file_50*50",/*50*50 头像 */)；

[0140] 然后将该 HashMap 对象直接回调给开发者。

[0141] 本发明的最佳实施例的针对非预先绑定用户账号的设备，具体包括：

[0142] 调用 html5 的登录页面，输入账户跟密码，点击登录，登录成功后在回调地址里会回传授权码 code，然后后续与针对预先绑定用户账号的设备的工作流程相同，即与步骤 S802-S805 一致，其登陆页面的生成，具体如下：

[0143] 根据 appid，appsecret 及回调地址，拼出来一个调起登录的 url，其格式如下：

[0144] "https://aaa.xxx.com/oauthopen/authorize ? scope = user_basic_show&display = mobile&client_id = "

[0145] +AccountOathSDK.appid+"&force_login = 1&state = &response_type = code&cl ient_secret = "

[0146] +AccountOathSDK.appsecret+"&redirect_uri = "+AccountOathSDK.redirect_uri ;

[0147] 然后通过 WebView 的 loadurl 来打开该登录页面，如果登录成功，则会将授权码 code 附在回调地址 redirect_uri 后面，如 https://aaa.xxx.com/oauth_default.html ? code = 1，然后通过 WebView 的 onPageFinish 方法，可以截取到 code 值，将该值传入 getAccessToken(code) 中。

[0148] 本发明最佳实施例的 sdk 由于资源文件在 jar 中用 R 文件直接访问会有冲突，所以所有资源文件的访问都采用 java 的反射机制来获得。具体提供一个 Mresource 类以根据资源类的类名 (className) 以及资源文件名 (name) 来获取资源文件 id。

[0149] 在 Mresource 中 会 提 供 一 个 getIdByName(Context context,String className,String name)，该方法会根据 className 以及 id 名称 name 来取得对应的 id。会先根据包名 (package name) 来反射出对应的 R 文件，然后在该 R 文件中遍历类，如果找到该资源类，则把该资源类中对用的 name 值所对应的 id 直接返回。

[0150]

```
r = Class.forName(packageName + ".R");
Class[] classes = r.getClasses();
Class desireClass = null;
for (int i = 0; i < classes.length; ++i) {
 if (classes[i].getName().split("\\$")[1].equals(className))
{
    desireClass = classes[i];
     break;
      }
}
if (desireClass != null)
id = desireClass.getField(name).getInt(desireClass);
```

[0151] 如图 3 所示为本发明一种第三方账号授权设备的结构模块图，包括：

[0152] 第三方授权响应模块 301，用于：响应第三方应用的授权请求；

[0153] 授权码获取模块 302，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0154] 访问令牌获取模块 303，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0155] 用户信息获取模块 304，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息；

[0156] 信息回调模块 305，用于：将所述用户信息回调至所述第三方应用。

[0157] 在其中一个实施例中，所述获取关于所述预先绑定的用户账号的授权码，具体用于：

[0158] 获取所述第三方应用的应用标识和应用密钥；

[0159] 对所述应用标识和所述应用密钥进行验证，如果验证通过，获取关于所述预先绑定的用户账号的授权码。

[0160] 在其中一个实施例中，所述授权码获取模块 302，还用于：如果没有预先绑定的用户账号，则：

[0161] 获取所述第三方应用的应用标识和应用密钥；

[0162] 将所述应用标识和所述应用密钥发送到服务器；

[0163] 显示所述服务器对所述应用标识和所述应用密钥进行验证后所返回的登陆页面；

[0164] 获取所述服务器对用户账号和用户密码验证通过后所返回的关于所述用户账号的授权码，执行访问令牌获取模块，所述用户账号和所述用户密码由所述服务器通过所述登陆页面接收得到。

[0165] 在其中一个实施例中，所述访问令牌获取模块 303 中，获取所述访问令牌后与所述用户账号关联保存；

[0166] 所述第三方授权响应模块 301，具体用于：

[0167] 当响应于第三方应用的授权请求时，如果保存有与所述用户账号关联保存的访问令牌，则直接执行所述用户信息获取模块 304，否则执行所述授权码获取模块 302。

[0168] 在其中一个实施例中，所述信息回调模块 305，具体用于：

[0169] 将所述用户信息进行哈希封装后回调至所述第三方应用。

[0170] 在其中一个实施例中，所述第三方授权响应模块 301，具体用于：显示授权页面，响应由所述授权页面所触发的第三方应用的授权请求，所述授权页面采用 Java 基于安卓系统生成，且所述授权页面的显示资源来自以 Java 库形式保存的至少一个资源文件，且每个所述资源文件的资源文件标识采用 Java 的反射机制从安卓系统所提供的 R 文件中获取。

[0171] 如图 4 所示为本发明的设备的结构框图，其主要包括：处理器 401、存储器 402、通信组件 403 及显示屏 404 等。一般来说，本发明的设备优选为智能手机、平板电脑和智能电视等。

[0172] 其中存储器 402 中存储前述方法的具体代码，由处理器 401 具体执行，通过显示屏 404 显示授权界面，以及通过通信组件 403 向服务器发送访问令牌和用户账号，以及接收用户信息并通过处理器 401 回调至第三方应用。

[0173] 如图 5 所示为本发明一种第三方账号授权服务器的结构模块图，包括：

[0174] 访问令牌接收模块 501，用于：接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述

预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌；

[0175] 用户信息发送模块502，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用。

[0176] 在其中一个实施例中，还包括，授权码发送模块；

[0177] 所述授权码发送模块，用于：

[0178] 接收到设备判断没有与所述设备绑定的用户账号时，所发送的应用标识和应用密钥，所述应用标识和所述应用密钥为所述设备所获取的所述第三方应用的应用标识和应用密钥；

[0179] 如果所述应用标识和所述应用密钥验证通过则向所述设备返回登陆页面，并通过所述登陆页面获取用户账号和用户密码；

[0180] 如果对所述用户账号和所述用户密码验证通过，则向所述设备返回关于所述用户账号的授权码。

[0181] 如图6所示为本发明的服务器的结构框图。服务器可以为一台电脑，也可以是多台电脑所组成的集群，其主要包括：处理器601、存储器602以及通信组件603等。

[0182] 其中存储器602中存储前述方法的具体代码，由处理器601具体执行，通过通信组件603接收设备发送的访问令牌和用户账号，并由处理器601从存储器602中查询得到用户信息后，通过通信组件603向设备返回用户信息。

[0183] 如图7所示为本发明一种第三方账号授权系统的结构模块图，包括：设备端71和服务器端72；

[0184] 所述设备端71，包括：

[0185] 设备端第三方授权响应模块711，用于：响应第三方应用的授权请求；

[0186] 设备端授权码获取模块712，用于：如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码；

[0187] 设备端访问令牌获取模块713，用于：将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌；

[0188] 设备端用户信息获取模块714，用于：将所述访问令牌和用户账号发送到服务器，从所述服务器获取关于所述用户账号的用户信息；

[0189] 设备端信息回调模块715，用于：将所述用户信息回调至所述第三方应用；

[0190] 所述服务器端72，包括：

[0191] 服务器端访问令牌接收模块721，用于：接收到来自设备的访问令牌和用户账号；

[0192] 服务器端用户信息发送模块722，用于：对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备。

[0193] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本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，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

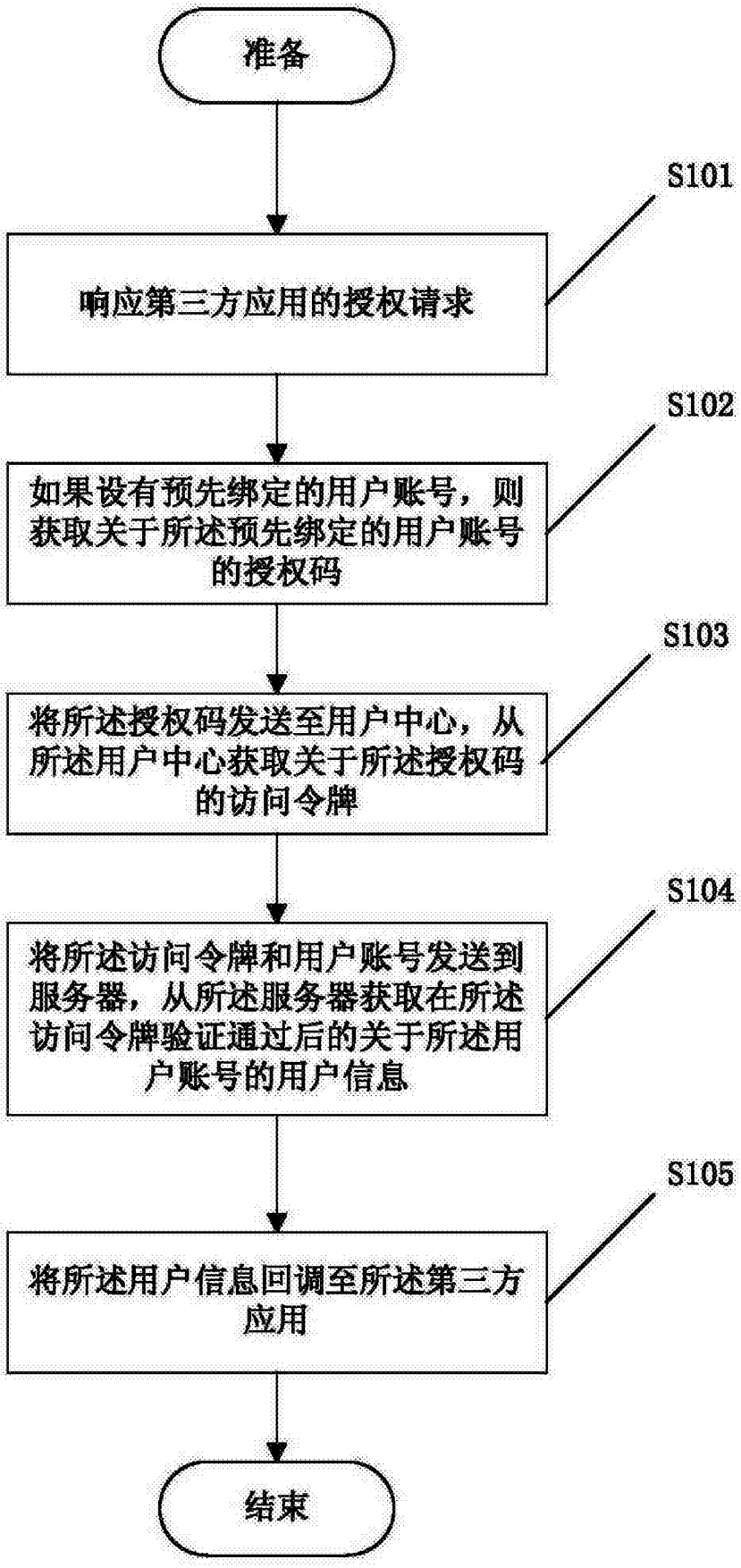

准备
S101
响应第三方应用的授权请求
S102
如果设有预先绑定的用户账号，则获取关于所述预先绑定的用户账号的授权码
S103
将所述授权码发送至用户中心，从所述用户中心获取关于所述授权码的访问令牌
S104
将所述访问令牌和用户账号发送到服务器，从所述服务器获取在所述访问令牌验证通过后的关于所述用户账号的用户信息
S105
将所述用户信息回调至所述第三方应用
结束

图 1

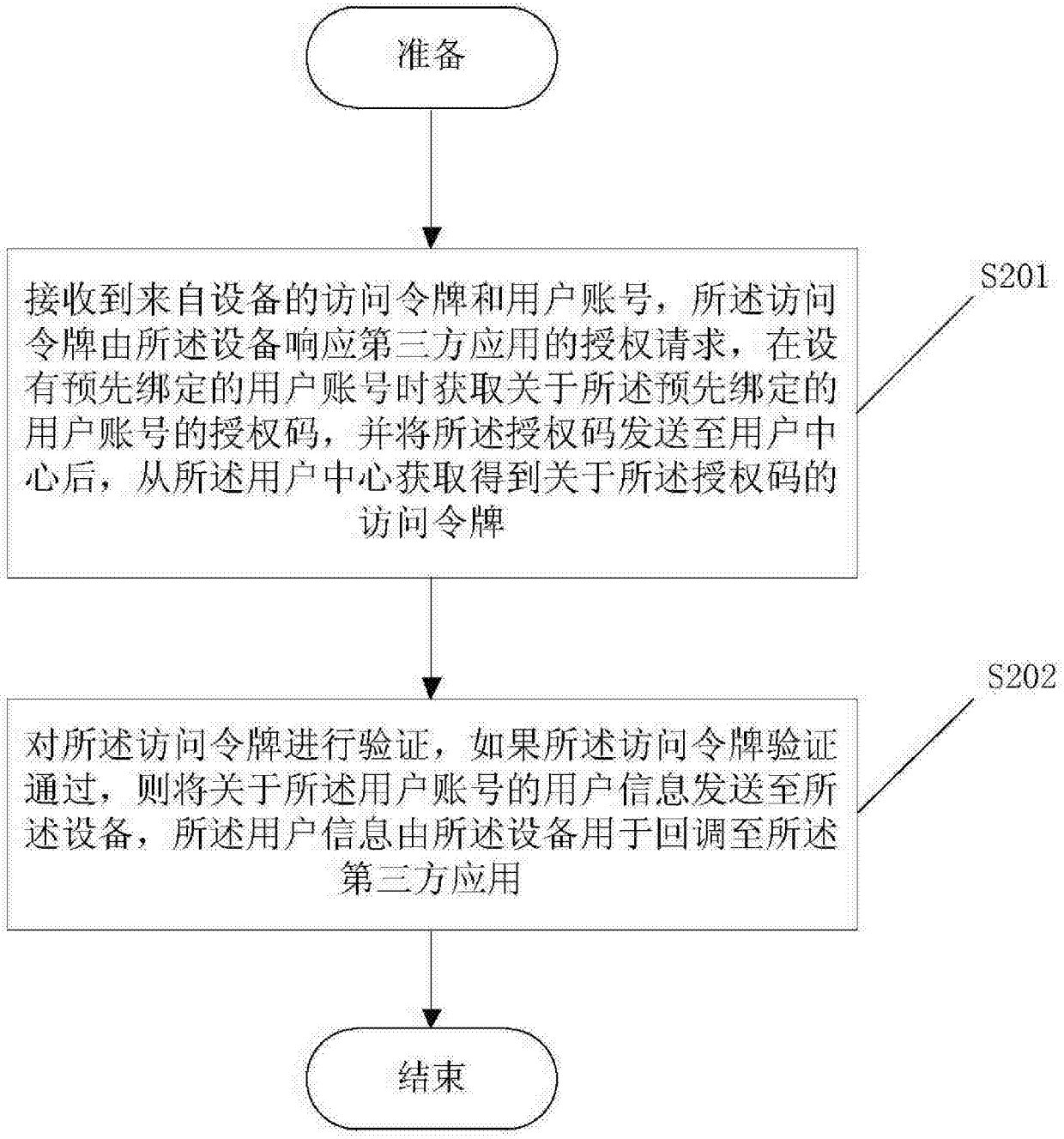

准备
接收到来自设备的访问令牌和用户账号，所述访问令牌由所述设备响应第三方应用的授权请求，在设有预先绑定的用户账号时获取关于所述预先绑定的用户账号的授权码，并将所述授权码发送至用户中心后，从所述用户中心获取得到关于所述授权码的访问令牌
S201
对所述访问令牌进行验证，如果所述访问令牌验证通过，则将关于所述用户账号的用户信息发送至所述设备，所述用户信息由所述设备用于回调至所述第三方应用
S202
结束

图 2

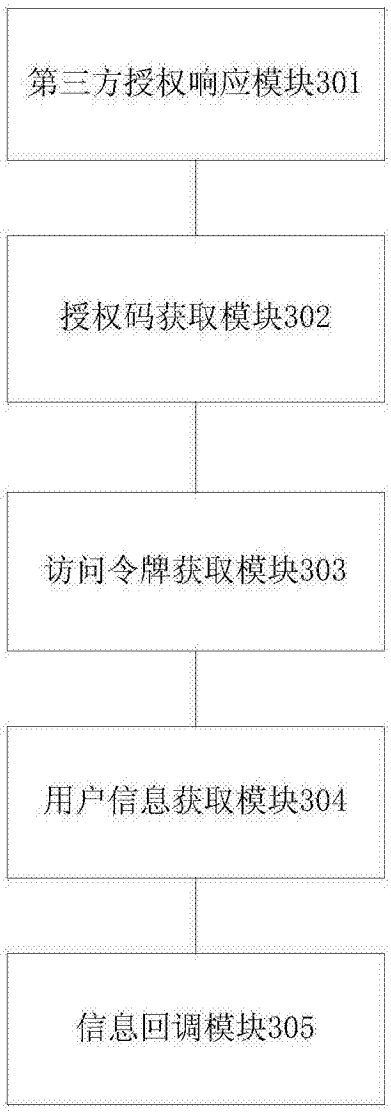

第三方授权响应模块301
授权码获取模块302
访问令牌获取模块303
用户信息获取模块304
信息回调模块305

图 3

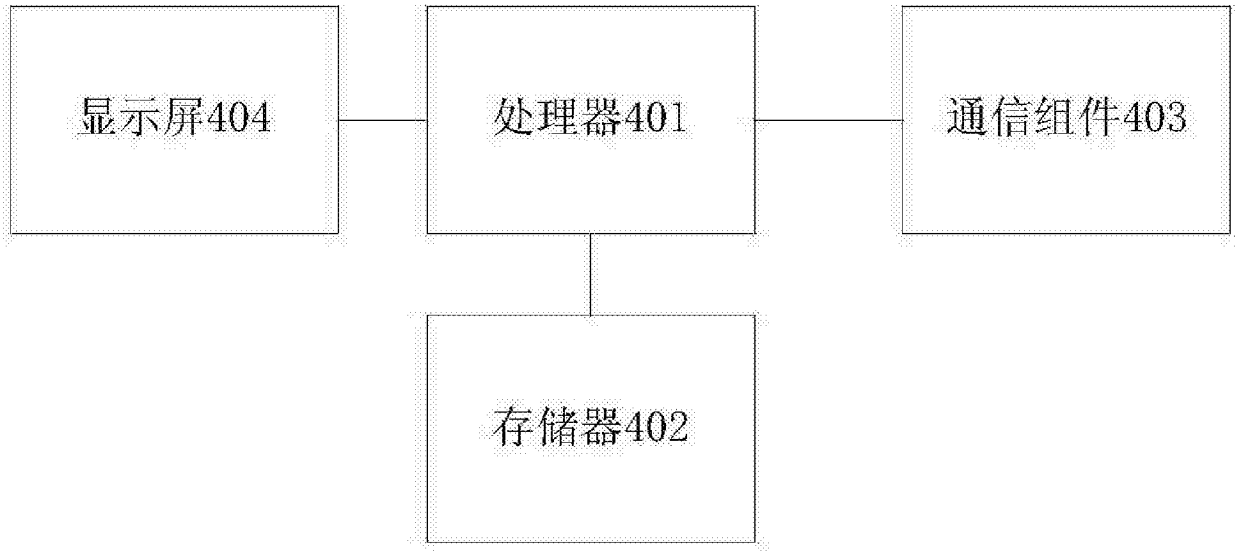



图 4


图 5

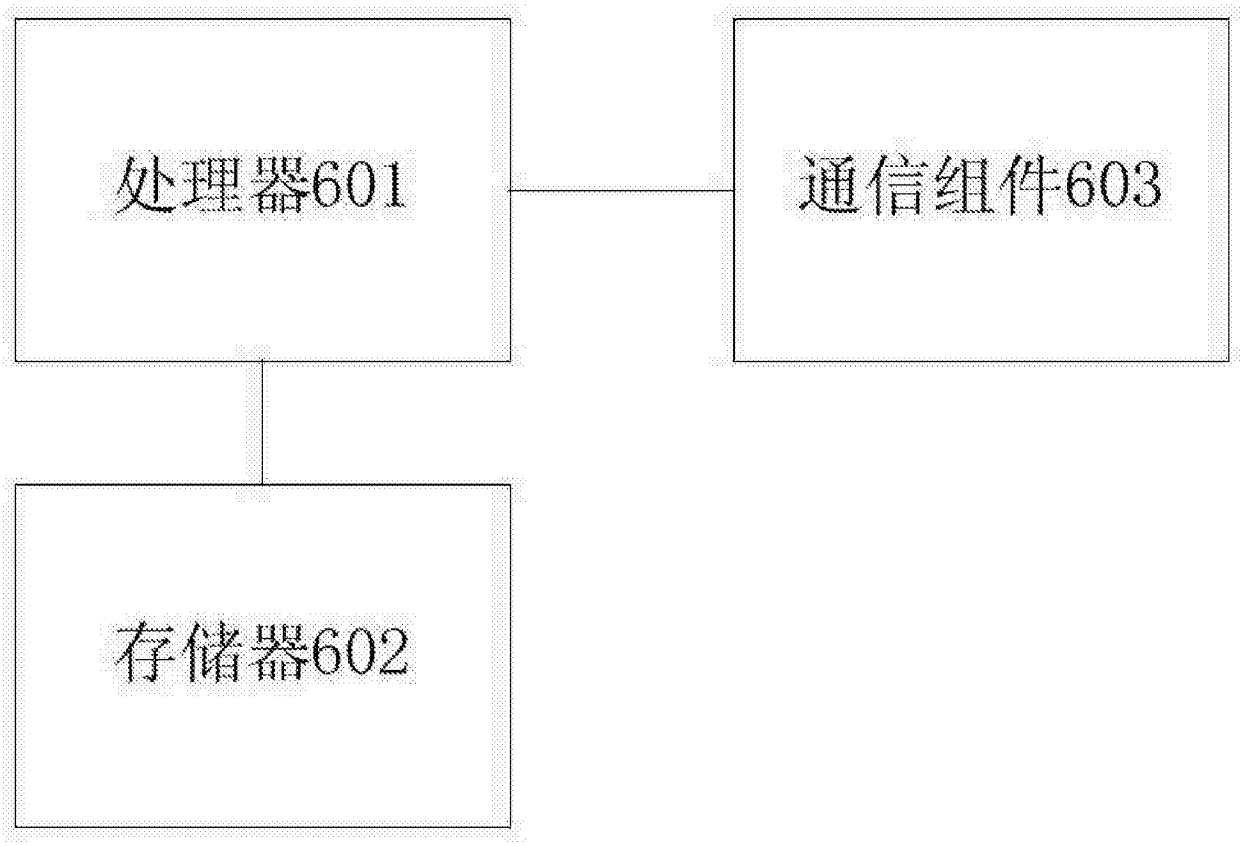



图 6

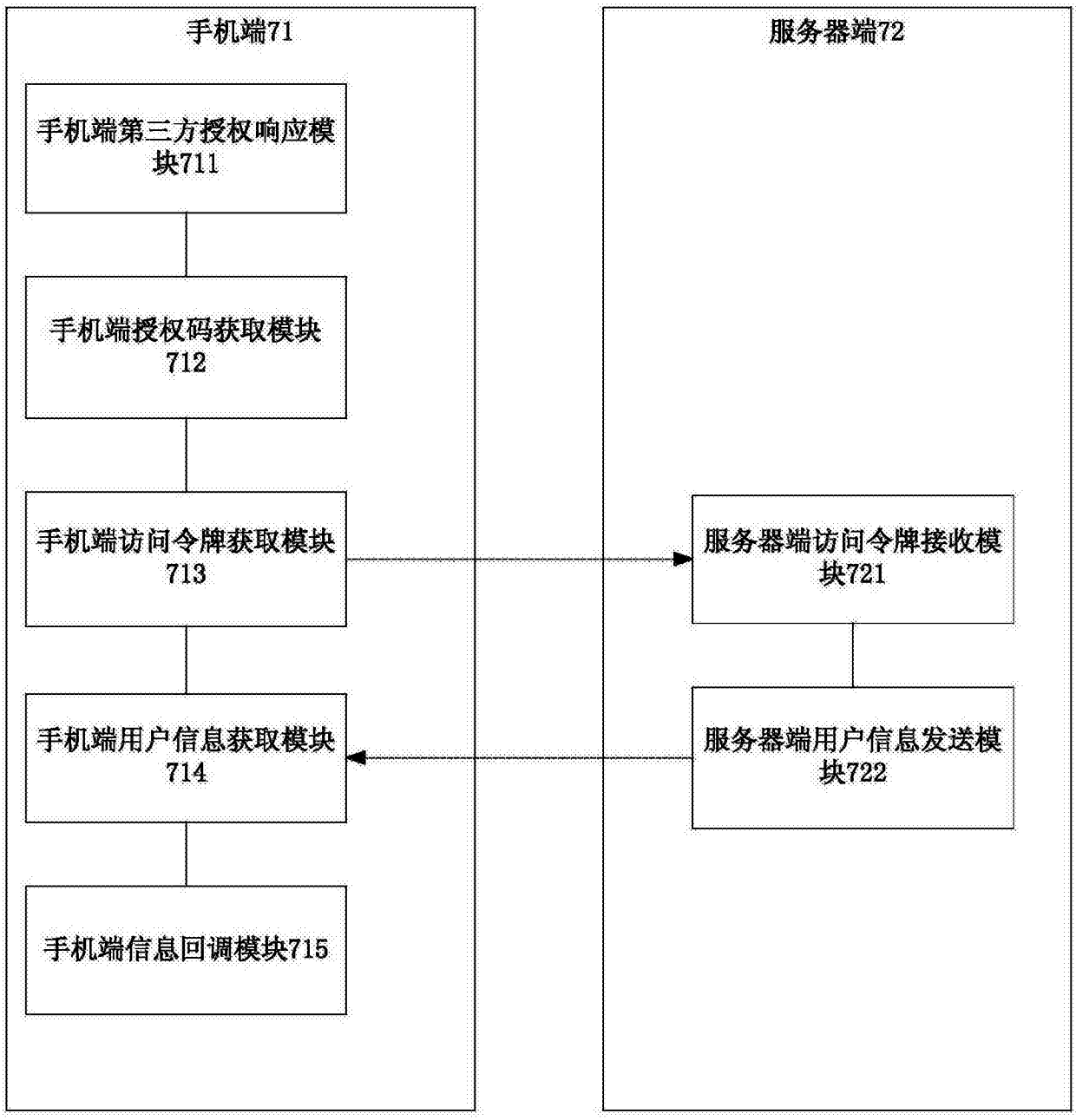

手机端71
手机端第三方授权响应模块711
手机端授权码获取模块712
手机端访问令牌获取模块713
手机端用户信息获取模块714
手机端信息回调模块715
服务器端72
服务器端访问令牌接收模块721
服务器端用户信息发送模块722

图 7

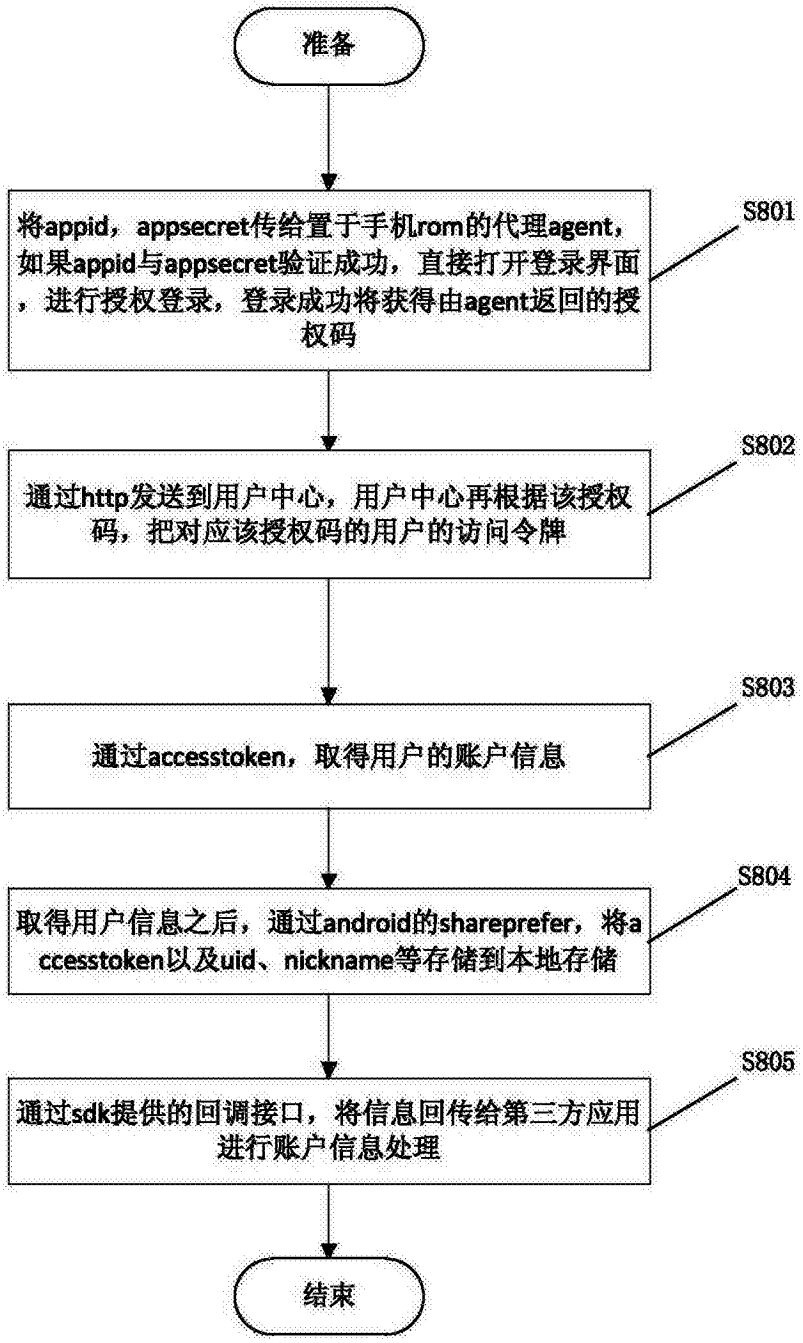

准备
将appid，appsecret传给置于手机rom的代理agent，如果appid与appsecret验证成功，直接打开登录界面，进行授权登录，登录成功将获得由agent返回的授权码
S801
通过http发送到用户中心，用户中心再根据该授权码，把对应该授权码的用户的访问令牌
S802
通过accesstoken，取得用户的账户信息
S803
取得用户信息之后，通过android的shareprefer，将accesstoken以及uid、nickname等存储到本地存储
S804
通过sdk提供的回调接口，将信息回传给第三方应用进行账户信息处理
S805
结束

图 8