(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 104980925 B
(45)授权公告日 2019.05.28

(21)申请号 201510292364.6

(22)申请日 2015.06.01

(65)同一申请的已公布的文献号
申请公布号 CN 104980925 A

(43)申请公布日 2015.10.14

(73)专利权人 走遍世界(北京)信息技术有限公司
地址 100035 北京市海淀区西直门北大街32号院2号楼8层807

(72)发明人 梁玮殷 祝宏

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 韩建伟 张永明

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 29/06(2006.01)

(56)对比文件
CN 104255007 A ,2014.12.31,说明书第[0010]-[0013]段,图1-3.

审查员 赵小植

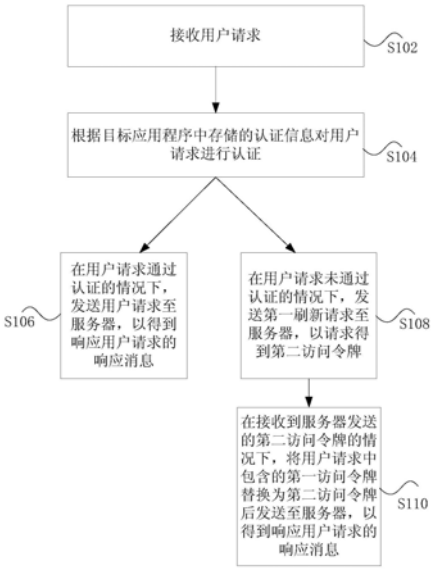
权利要求书3页 说明书16页 附图3页

(54)发明名称

用户请求的认证方法和装置

(57)摘要

本发明公开了一种用户请求的认证方法和装置。其中,用户请求的认证方法包括:接收用户请求;根据目标应用程序中存储的认证信息对用户请求进行认证;在用户请求通过认证的情况下,发送用户请求至服务器,以得到响应用户请求的响应消息;在用户请求未通过认证的情况下,发送第一刷新请求至服务器,以请求得到第二访问令牌;在接收到服务器发送的第二访问令牌的情况下,将用户请求中包含的第一访问令牌替换为第二访问令牌后发送至服务器,以得到响应用户请求的响应消息。通过本发明,解决了现有技术中对用户请求进行认证的方式较为繁琐,导致用户操作不便的问题,进而达到了简化对用户请求的认证过程,提高认证效率的效果。



CN 104980925 B

1.一种用户请求的认证方法,其特征在于,包括:

接收用户请求,其中,所述用户请求为用户接触设备屏幕中的当前显示页面时产生的请求,所述用户请求中包含第一访问令牌;

根据目标应用程序中存储的认证信息对所述用户请求进行认证,其中,所述目标应用程序为所述当前显示页面对应的应用程序;

在所述用户请求通过认证的情况下,发送所述用户请求至服务器,以得到响应所述用户请求的响应消息;

在所述用户请求未通过认证的情况下,发送第一刷新请求至所述服务器,以请求得到第二访问令牌,其中,所述第二访问令牌与所述第一访问令牌不同,所述第一刷新请求中包含所述认证信息中存储的刷新令牌;以及

在接收到所述服务器发送的所述第二访问令牌的情况下,将所述用户请求中包含的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器,以得到响应所述用户请求的响应消息;

其中,所述认证信息中存储的刷新令牌中包含三部分内容,一部分内容是由32位或者64位的字符、数字和特殊字符随机组成的序列,另一部分内容是申请刷新令牌的时间,还有一部分内容是刷新令牌的有效使用期限;

其中,在所述用户请求通过认证的情况下,发送所述用户请求至服务器之后,所述方法还包括:

判断是否接收到所述服务器发送的认证失败消息;

在判断出接收到所述认证失败消息的情况下,发送第二刷新请求至所述服务器,以请求第四访问令牌,其中,所述第四访问令牌与所述第一访问令牌不相同,所述第二刷新请求中包含所述刷新令牌;

判断是否接收到所述服务器发送的所述第四访问令牌;

在判断出接收到所述第四访问令牌的情况下,将所述用户请求中包含的所述第一访问令牌替换为所述第四访问令牌后发送至所述服务器,以得到响应所述用户请求的响应消息;

在判断出未接收到所述第四访问令牌的情况下,删除所述认证信息。

2.根据权利要求1所述的方法,其特征在于,所述认证信息中还存储有第三访问令牌,根据目标应用程序中存储的认证信息对所述用户请求进行认证包括:

所述目标应用程序中的应用程序编程接口将所述用户请求发送至对应的网络请求接口;

所述网络请求接口将所述用户请求发送至网络模块;

所述网络模块根据所述第三访问令牌判断所述第一访问令牌是否有效,

其中,在判断出所述第一访问令牌有效的情况下,所述用户请求通过认证;

在判断出所述第一访问令牌无效的情况下,所述用户请求未通过认证。

3.根据权利要求1或2所述的方法,其特征在于,在所述用户请求未通过认证的情况下,发送第一刷新请求至所述服务器之后,所述方法还包括:

判断是否接收到所述服务器发送的所述第二访问令牌;

在判断出未接收到所述第二访问令牌的情况下,删除所述认证信息。

4.根据权利要求1所述的方法，其特征在于，在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器之后，所述方法还包括：

判断是否接收到所述服务器发送的认证失败消息；

在判断出接收到所述认证失败消息的情况下，发送第二刷新请求至所述服务器，以请求第四访问令牌，其中，所述第四访问令牌与所述第一访问令牌、所述第二访问令牌均不相同，所述第二刷新请求中包含所述刷新令牌；

判断是否接收到所述服务器发送的所述第四访问令牌；

在判断出接收到所述第四访问令牌的情况下，将所述用户请求中包含的所述第二访问令牌替换为所述第四访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；

在判断出未接收到所述第四访问令牌的情况下，删除所述认证信息。

5.一种用户请求的认证装置，其特征在于，包括：

接收单元，用于接收用户请求，其中，所述用户请求为用户接触设备屏幕中的当前显示页面时产生的请求，所述用户请求中包含第一访问令牌；

认证单元，用于根据目标应用程序中存储的认证信息对所述用户请求进行认证，其中，所述目标应用程序为所述当前显示页面对应的应用程序；

第一发送单元，用于在所述用户请求通过认证的情况下，发送所述用户请求至服务器，以得到响应所述用户请求的响应消息；

第二发送单元，用于在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器，以请求得到第二访问令牌，其中，所述第二访问令牌与所述第一访问令牌不同，所述第一刷新请求中包含所述认证信息中存储的刷新令牌；以及

第三发送单元，用于在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中包含的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；

其中，所述认证信息中存储的刷新令牌中包含三部分内容，一部分内容是由32位或者64位的字符、数字和特殊字符随机组成的序列，另一部分内容是申请刷新令牌的时间，还有一部分内容是刷新令牌的有效使用期限；

其中，第二判断单元，用于在所述用户请求通过认证的情况下，发送所述用户请求至服务器之后，判断是否接收到所述服务器发送的认证失败消息；

第四发送单元，用于在判断出接收到所述认证失败消息的情况下，发送第二刷新请求至所述服务器，以请求第四访问令牌，其中，所述第四访问令牌与所述第一访问令牌不相同，所述第二刷新请求中包含所述刷新令牌；

第三判断单元，用于判断是否接收到所述服务器发送的所述第四访问令牌；

第五发送单元，用于在判断出接收到所述第四访问令牌的情况下，将所述用户请求中包含的所述第一访问令牌替换为所述第四访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；

第二删除单元，用于在判断出未接收到所述第四访问令牌的情况下，删除所述认证信息。

6.根据权利要求5所述的装置，其特征在于，所述认证信息中还存储有第三访问令牌，所述认证单元包括：

所述目标应用程序中的应用程序编程接口，用于将所述用户请求发送至对应的网络请求接口；

所述网络请求接口，用于将所述用户请求发送至网络模块；

所述网络模块，用于根据所述第三访问令牌判断所述第一访问令牌是否有效，

其中，在判断出所述第一访问令牌有效的情况下，所述用户请求通过认证；

在判断出所述第一访问令牌无效的情况下，所述用户请求未通过认证。

7.根据权利要求5或6所述的装置，其特征在于，所述装置还包括：

第一判断单元，用于在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器之后，判断是否接收到所述服务器发送的所述第二访问令牌；

第一删除单元，用于在判断出未接收到所述第二访问令牌的情况下，删除所述认证信息。

8.根据权利要求5所述的装置，其特征在于，所述装置还包括：

第四判断单元，用于在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器之后，判断是否接收到所述服务器发送的认证失败消息；

第六发送单元，用于在判断出接收到所述认证失败消息的情况下，发送第二刷新请求至所述服务器，以请求第四访问令牌，其中，所述第四访问令牌与所述第一访问令牌、所述第二访问令牌均不相同，所述第二刷新请求中包含所述刷新令牌；

第五判断单元，用于判断是否接收到所述服务器发送的所述第四访问令牌；

第七发送单元，用于在判断出接收到所述第四访问令牌的情况下，将所述用户请求中包含的所述第二访问令牌替换为所述第四访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；

第三删除单元，用于在判断出未接收到所述第四访问令牌的情况下，删除所述认证信息。

用户请求的认证方法和装置

技术领域

[0001] 本发明涉及认证领域，具体而言，涉及一种用户请求的认证方法和装置。

背景技术

[0002] 近年来，随着人们生活节奏的加快和手机功能的日益强大，手机已经融入人们生活的方方面面，人们越来越依赖手机。随着智能手机硬件配置和性能的不断提升，用户可以把大量的应用程序安装到手机上。

[0003] 现有技术中，当用户在手机上使用某个应用程序时，需要通过触摸手机屏幕或者按键来发送请求，上述应用程序在收到请求后，会对请求中的相关信息(如，访问令牌)进行认证，如果上述相关信息是有效的，则可通过认证，进而发送上述请求至服务器，服务器会响应该请求；如果上述相关信息是无效的，则需要用户至少重新发送一次上述请求至应用程序，才可能会得到关于上述请求的响应消息，通过上述描述可知，现有技术中对用户请求进行认证的方式较为复杂，同一请求可能需要用户多次发送，才可得到该请求的响应信息，容易给使用上述应用程序的用户带来操作的不便。

[0004] 针对现有技术中对用户请求进行认证的方式较为复杂，导致用户操作不便的问题，目前尚未提出有效的解决方案。

发明内容

[0005] 本发明提供一种用户请求的认证方法和装置，以解决现有技术中对用户请求进行认证的方式较为复杂，导致用户操作不便的问题。

[0006] 根据本发明实施例的一个方面，提供了一种用户请求的认证方法。根据本发明的用户请求的认证方法包括：接收用户请求，其中，所述用户请求为用户接触设备屏幕中的当前显示页面时产生的请求，所述用户请求中包含第一访问令牌；根据目标应用程序中存储的认证信息对所述用户请求进行认证，其中，所述目标应用程序为所述当前显示页面对应的应用程序；在所述用户请求通过认证的情况下，发送所述用户请求至服务器，以得到响应所述用户请求的响应消息；在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器，以请求得到第二访问令牌，其中，所述第二访问令牌与所述第一访问令牌不同，所述第一刷新请求中包含所述认证信息中存储的刷新令牌；以及在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中包含的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息。

[0007] 进一步地，所述认证信息中还存储有第三访问令牌，根据目标应用程序中存储的认证信息对所述用户请求进行认证包括：所述目标应用程序中的应用程序编程接口将所述用户请求发送至对应的网络请求接口；所述网络请求接口将所述用户请求发送至网络模块；所述网络模块根据所述第三访问令牌判断所述第一访问令牌是否有效，其中，在判断出所述第一访问令牌有效的情况下，所述用户请求通过认证；在判断出所述第一访问令牌无效的情况下，所述用户请求未通过认证。

[0008] 进一步地，在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器之后，所述方法还包括：判断是否接收到所述服务器发送的所述第二访问令牌；在判断出未接收到所述第二访问令牌的情况下，删除所述认证信息。

[0009] 进一步地，在所述用户请求通过认证的情况下，发送所述用户请求至服务器之后，所述方法还包括：判断是否接收到所述服务器发送的认证失败消息；在判断出接收到所述认证失败消息的情况下，发送第二刷新请求至所述服务器，以请求第四访问令牌，其中，所述第四访问令牌与所述第一访问令牌不相同，所述第二刷新请求中包含所述刷新令牌；判断是否接收到所述服务器发送的所述第四访问令牌；在判断出接收到所述第四访问令牌的情况下，将所述用户请求中包含的所述第一访问令牌替换为所述第四访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；在判断出未接收到所述第四访问令牌的情况下，删除所述认证信息。

[0010] 进一步地，在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器之后，所述方法还包括：判断是否接收到所述服务器发送的认证失败消息；在判断出接收到所述认证失败消息的情况下，发送第二刷新请求至所述服务器，以请求第四访问令牌，其中，所述第四访问令牌与所述第一访问令牌、所述第二访问令牌均不相同，所述第二刷新请求中包含所述刷新令牌；判断是否接收到所述服务器发送的所述第四访问令牌；在判断出接收到所述第四访问令牌的情况下，将所述用户请求中包含的所述第二访问令牌替换为所述第四访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息；在判断出未接收到所述第四访问令牌的情况下，删除所述认证信息。

[0011] 根据本发明实施例的另一方面，提供了一种用户请求的认证装置。根据本发明的用户请求的认证装置包括：接收单元，用于接收用户请求，其中，所述用户请求为用户接触设备屏幕中的当前显示页面时产生的请求，所述用户请求中包含第一访问令牌；认证单元，用于根据目标应用程序中存储的认证信息对所述用户请求进行认证，其中，所述目标应用程序为所述当前显示页面对应的应用程序；第一发送单元，用于在所述用户请求通过认证的情况下，发送所述用户请求至服务器，以得到响应所述用户请求的响应消息；第二发送单元，用于在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器，以请求得到第二访问令牌，其中，所述第二访问令牌与所述第一访问令牌不同，所述第一刷新请求中包含所述认证信息中存储的刷新令牌；以及第三发送单元，用于在接收到所述服务器发送的所述第二访问令牌的情况下，将所述用户请求中包含的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器，以得到响应所述用户请求的响应消息。

[0012] 进一步地，所述认证信息中还存储有第三访问令牌，所述认证单元包括：所述目标应用程序中的应用程序编程接口，用于将所述用户请求发送至对应的网络请求接口；所述网络请求接口，用于将所述用户请求发送至网络模块；所述网络模块，用于根据所述第三访问令牌判断所述第一访问令牌是否有效，其中，在判断出所述第一访问令牌有效的情况下，所述用户请求通过认证；在判断出所述第一访问令牌无效的情况下，所述用户请求未通过认证。

[0013] 进一步地，所述装置还包括：第一判断单元，用于在所述用户请求未通过认证的情况下，发送第一刷新请求至所述服务器之后，判断是否接收到所述服务器发送的所述第二

访问令牌;第一删除单元,用于在判断出未接收到所述第二访问令牌的情况下,删除所述认证信息。

[0014] 进一步地,所述装置还包括:第二判断单元,用于在所述用户请求通过认证的情况下,发送所述用户请求至服务器之后,判断是否接收到所述服务器发送的认证失败消息;第四发送单元,用于在判断出接收到所述认证失败消息的情况下,发送第二刷新请求至所述服务器,以请求第四访问令牌,其中,所述第四访问令牌与所述第一访问令牌不相同,所述第二刷新请求中包含所述刷新令牌;第三判断单元,用于判断是否接收到所述服务器发送的所述第四访问令牌;第五发送单元,用于在判断出接收到所述第四访问令牌的情况下,将所述用户请求中包含的所述第一访问令牌替换为所述第四访问令牌后发送至所述服务器,以得到响应所述用户请求的响应消息;第二删除单元,用于在判断出未接收到所述第四访问令牌的情况下,删除所述认证信息。

[0015] 进一步地,所述装置还包括:第四判断单元,用于在接收到所述服务器发送的所述第二访问令牌的情况下,将所述用户请求中的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器之后,判断是否接收到所述服务器发送的认证失败消息;第六发送单元,用于在判断出接收到所述认证失败消息的情况下,发送第二刷新请求至所述服务器,以请求第四访问令牌,其中,所述第四访问令牌与所述第一访问令牌、所述第二访问令牌均不相同,所述第二刷新请求中包含所述刷新令牌;第五判断单元,用于判断是否接收到所述服务器发送的所述第四访问令牌;第七发送单元,用于在判断出接收到所述第四访问令牌的情况下,将所述用户请求中包含的所述第二访问令牌替换为所述第四访问令牌后发送至所述服务器,以得到响应所述用户请求的响应消息;第三删除单元,用于在判断出未接收到所述第四访问令牌的情况下,删除所述认证信息。

[0016] 根据本发明实施例,通过接收用户请求,其中,所述用户请求为用户接触设备屏幕中的当前显示页面时产生的请求,所述用户请求中包含第一访问令牌;根据目标应用程序中存储的认证信息对所述用户请求进行认证,其中,所述目标应用程序为所述当前显示页面对应的应用;在所述用户请求通过认证的情况下,发送所述用户请求至服务器,以得到响应所述用户请求的响应消息;在所述用户请求未通过认证的情况下,发送第一刷新请求至所述服务器,以请求得到第二访问令牌,其中,所述第二访问令牌与所述第一访问令牌不同,所述第一刷新请求中包含所述认证信息中存储的刷新令牌;以及在接收到所述服务器发送的所述第二访问令牌的情况下,将所述用户请求中的所述第一访问令牌替换为所述第二访问令牌后发送至所述服务器,以得到响应所述用户请求的响应消息,解决了现有技术中对用户请求进行认证的方式较为繁琐,导致用户操作不便的问题,进而达到了简化对用户请求的认证过程,提高认证效率的效果。此外,本发明实施例所提供的认证方式,还起到了简化用户操作的效果。

附图说明

[0017] 构成本申请的一部分的附图用来提供对本发明的进一步理解,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0018] 图1是根据本发明实施例的用户请求的认证方法的流程图;

[0019] 图2是根据本发明实施例可选的用户请求的认证方法的流程图;以及

[0020] 图3是根据本发明实施例的用户请求的认证装置的示意图。

具体实施方式

[0021] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，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，都应当属于本发明保护的范围。

[0022] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0023] 实施例1

[0024] 根据本发明实施例，提供了一种可以用于实施本申请装置实施例的方法实施例，需要说明的是，在附图的流程图示出的步骤可以在诸如一组计算机可执行指令的计算机系统中执行，并且，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0025] 在本发明实施例中，设备为具有触摸屏幕的，且可以安装应用程序的任何类型终端，例如手机、平板电脑等。

[0026] 根据本发明实施例，提供了一种用户请求的认证方法。图1是根据本发明实施例的用户请求的认证方法的流程图，如图1所示，该方法包括如下的步骤S102至步骤S110：

[0027] 步骤S102：接收用户请求，其中，用户请求为用户接触设备屏幕中的当前显示页面时产生的请求，用户请求中包含第一访问令牌。

[0028] 步骤S104：根据目标应用程序中存储的认证信息对用户请求进行认证，其中，目标应用程序为当前显示页面对应的应用。

[0029] 步骤S106：在用户请求通过认证的情况下，发送用户请求至服务器，以得到响应用户请求的响应消息。

[0030] 步骤S108：在用户请求未通过认证的情况下，发送第一刷新请求至服务器，以请求得到第二访问令牌，其中，第二访问令牌与第一访问令牌不同，第一刷新请求中包含认证信息中存储的刷新令牌。

[0031] 步骤S110：在接收到服务器发送的第二访问令牌的情况下，将用户请求中包含的第一访问令牌替换为第二访问令牌后发送至服务器，以得到响应用户请求的响应消息。

[0032] 在本发明实施例中，应用程序接收到用户请求后，根据其内存储的认证信息对上述用户请求进行本地认证。如果用户请求通过本地认证，则将用户请求发送至服务器，以得到该用户请求的响应消息；如果用户请求未通过本地认证，该应用程序会自动获取新的，有效的认证介质(即，访问令牌)，并将上述用户请求中已经失效的认证介质替换成新获取的

认证介质，即也同样认为完成了对该用户请求的本地认证，最后发送替换了认证介质后的用户请求至服务器。

[0033] 而相关技术中，在对用户请求进行认证时，如果应用程序对用户第一次发送的用户请求进行认证后，判断出第一次接收到的用户请求未通过认证，会提示该用户需要再次发送上述用户请求，以获取有效的认证介质。当该应用程序第二次接收到上述用户请求时，会通过服务器获取到有效的认证介质，但是在收到有效的认证介质后，仍会提示用户需要再一次(即第三次)发送上述用户请求，其中，再一次发送的用户请求中包含了有效的认证介质。由于第三次发送的用户请求中包含了有效的认证介质，所以上述用户请求可以通过本地认证，即完成了对用户请求的认证，这时应用程序会将用户请求转发至服务器。通过上述描述可知，现有技术中对用户请求进行认证时，认证过程较为繁琐，需要用户多次发生同一用户请求，才可得到上述用户请求的响应信息。

[0034] 通过以上对比，可以看出本发明实施例中，对用户请求进行认证时，即使用户请求没有通过本地认证，用户也只需发送一次用户请求即可完成对该用户请求的认证，解决了现有技术中对用户请求进行认证的方式较为繁琐，导致用户操作不便的问题，进而达到了简化对用户请求的认证过程，提高认证效率的效果。此外，本发明实施例所提供的认证方式，还起到了简化用户操作的效果。

[0035] 本发明上述实施例所提供的用户请求的认证方法可以应用到任一安装在终端设备中的应用程序中。

[0036] 此外，本发明上述实施例中，目标应用程序根据其内存储的认证信息对用户请求进行认证的过程，也就是应用程序对用户请求进行认证的过程，可以称为本地认证。

[0037] 可选地，第一访问令牌中包含由32位或者64位的字符、数字和特殊字符随机组成的序列。

[0038] 可选地，认证信息中存储的刷新令牌中包含三部分内容，一部分内容是由32位或者64位的字符、数字和特殊字符随机组成的序列，另一部分内容是申请刷新令牌的时间，还有一部分内容是刷新令牌的有效使用期限。在本发明实施例中，可以将刷新令牌的有效使用期限设置较为长久，例如：1年。那么，认证信息则持久化的存储在应用程序中，上述持久化的存储时长由刷新令牌的有效使用期限决定。

[0039] 可选地，认证信息中除了存储有刷新令牌外，还存储有第三访问令牌，根据目标应用程序中存储的认证信息对用户请求进行认证包括如下步骤S1041至步骤S1045：

[0040] 步骤S1041：目标应用程序中的应用程序编程接口将用户请求发送至对应的网络请求接口。

[0041] 其中，目标应用程序在接收到用户请求后，通过其内的应用程序编程接口调用与该用户请求对应的网络请求接口的方式，将上述用户请求发送至与其对应的网络请求接口。

[0042] 步骤S1043：网络请求接口将用户请求发送至网络模块。

[0043] 步骤S1045：网络模块根据第三访问令牌判断第一访问令牌是否有效，其中，在判断出第一访问令牌有效的情况下，用户请求通过认证；在判断出第一访问令牌无效的情况下，用户请求未通过认证。

[0044] 其中，网络模块为对基础网络请求模块进行认证权限扩展后的模块。网络模块用

于对用户请求进行认证，并将接收到的，且通过认证的用户请求继续转发至服务器。需要说明的是，不同的用户请求都是通过网络模块转发至服务器的，并且该网络模块是唯一的。不同用户请求之间的差异体现在各自用户请求URL链接以及每个用户请求所规定的参数。当接收到不同的用户请求时，对网络模块来说，只是不同参数的差异，对每个用户请求进行认证的处理流程都是相同的。

[0045] 可选地，第三访问令牌中也包含三部分内容，分别是由32位或者64位的字符、数字和特殊字符随机组成的序列、申请该访问令牌的时间以及该访问令牌的有效使用期限。

[0046] 进一步可选地，网络模块根据第三访问令牌判断第一访问令牌是否有效包括如下步骤：

[0047] 步骤S1：网络模块获取第三访问令牌中的有效使用期限。

[0048] 步骤S3：判断接收到第一访问令牌的时间是否超过有效使用期限，其中，在判断出接收到第一访问令牌的时间未超过有效使用期限的情况下，表示第一访问令牌有效，则确定用户请求通过认证；在判断出接收到第一访问令牌的时间已超过有效使用期限的情况下，表示第一访问令牌无效，则确定用户请求未通过认证。

[0049] 可选地，在用户请求未通过认证的情况下，发送第一刷新请求至服务器之后，本发明实施例所提供的用户请求的认证方法还包括如下步骤S112至步骤S114：

[0050] 步骤S112：判断是否接收到服务器发送的第二访问令牌。

[0051] 可以由网络模块将包含刷新令牌的第一刷新请求发送至服务器。由于刷新令牌也是有使用时间限制的，所以很有可能发送至服务器的第一刷新请求中包含的刷新令牌已经超过该令牌的有效使用期限，即该刷新令牌已经过期，那么服务器在接收到上述用于请求得到第二访问令牌的刷新请求后，会先判断刷新请求中的刷新令牌是否已经过期，如果判断出刷新令牌已经过期，则服务器不会发送第二访问令牌给目标应用程序，如果判断出刷新令牌未过期，则服务器会发送第二访问令牌给目标应用程序。

[0052] 步骤S114：在判断出未接收到第二访问令牌的情况下，删除认证信息。

[0053] 进一步可选地，在判断出未接收到第二访问令牌的情况下，删除认证信息时，还可以发出异常提示消息。该异常提示消息可以体现在目标应用程序的系统日志中，用于向目标应用程序后台的工作人员反馈用户请求未能响应；还可以以文字的形式显示在设备屏幕中，用于提醒用户进行相应操作。例如，上述文字可以是：请检查网络设置。

[0054] 在用户请求通过本地认证之后，为了得到该用户请求的响应消息，目标应用程序还会继续将该用户请求发送给服务器，但是，服务器在接收到上述用户请求后，会再次对该用户请求进行认证。

[0055] 需要说明的是，在本地认证的过程中，可能只是检查用户请求中的访问令牌是否超过有效使用期限，即检查用户请求中的访问令牌是否有效，而服务器在对用户请求进行认证的过程中，检查的内容包括但不限于用户请求中访问令牌是否有效，还会对访问令牌进行其它内容的检查，例如，检查访问令牌是否合法等。如果服务器检查的全部内容，用户请求都是符合条件或要求的，那么服务器会返回响应该用户请求的响应消息给目标应用程序，如果服务器检查的全部内容中，用户请求中有至少一项不符合条件或者要求，则服务器会返回对用户请求认证失败的消息给目标应用程序。

[0056] 通过上述描述可知，目标应用程序对用户请求的认证与服务器对用户请求的认证

之间是相互独立的，互不影响的，即，服务器不会因为用户请求通过了目标应用程序对其的认证，而不再对上述用户请求进行认证。

[0057] 可选地，在用户请求通过认证的情况下，发送用户请求至服务器之后，本发明实施例所提供的用户请求的认证方法还包括如下步骤S116至步骤S124：

[0058] 步骤S116：判断是否接收到服务器发送的认证失败消息。

[0059] 其中，上述步骤S116中认证失败消息是指服务器对包含第一访问令牌的用户请求进行认证，所反馈的消息。

[0060] 步骤S118：在判断出接收到认证失败消息的情况下，发送第二刷新请求至服务器，以请求第四访问令牌，其中，第四访问令牌与第一访问令牌不同，第二刷新请求中包含刷新令牌。

[0061] 步骤S120：判断是否接收到服务器发送的第四访问令牌。

[0062] 步骤S122：在判断出接收到第四访问令牌的情况下，将用户请求包含中的第一访问令牌替换为第四访问令牌后发送至服务器，以得到响应用户请求的响应消息。

[0063] 步骤S124：在判断出未接收到第四访问令牌的情况下，删除认证信息。

[0064] 在发明实施例中，在包含了第一访问令牌的用户请求通过了目标应用程序对其的本地认证的情况下，目标应用程序会将通过本地认证的用户请求发送至服务器，在将上述用户请求发送至服务器后，目标应用程序还需判断是否接收到服务器发送的关于对用户请求认证失败的消息。其中，如果目标应用程序接收到服务器发送的关于用户请求认证失败的消息，则会向服务器发送包含刷新令牌的发送第二刷新请求。服务器在收到包含刷新请求后，会判断刷新令牌是否在有效使用期限内，如果服务器判断出刷新令牌在有效使用期限内的话，服务器会发送新的访问令牌(即第四访问令牌)给目标应用程序，目标应用程序在接收到第四访问令牌的情况下，会将之前用户请求中包含的第一访问令牌替换成第四访问令牌后，再次将用户请求发送给服务器。

[0065] 需要说明的是，上述步骤S118中的第四访问令牌可能与上述步骤S110中的第二访问令牌相同，也可能不同，但是与上述步骤S106中的第一访问令牌是不相同的。如果服务器判断出刷新令牌不在有效使用期限内的话，则不会发送第四访问令牌至目标应用程序，那么目标应用程序也就不会收到第四访问令牌，此时，也是会删除认证信息，并且在删除认证信息时，同样还可以发送异常提示消息。

[0066] 在本发明实施例中，在服务器对用户请求认证失败的情况下，目标应用程序也会自动获取新的，有效的认证介质(即，访问令牌)，并同样将上述用户请求中已经失效的认证介质替换成新获取的认证介质后再次发给服务器，使得在不需要用户重新发送用户请求的情况下，增加了一次服务器对用户请求的认证，进一步达到了在对用户请求进行认证时，简化用户操作的效果。

[0067] 可选地，在判断出接收到第四访问令牌的情况下，将用户请求包含中的第一访问令牌替换为第四访问令牌后发送至服务器之后，本发明实施例所提供的用户请求的认证方法还包括：需判断是否再次接收到服务器发送的认证失败消息。其中，上述认证失败消息是指：服务器对包含第四访问令牌的用户请求进行认证，所反馈的消息。其中，在判断出再次接收到服务器发送的认证失败消息的情况下，删除权证信息，并且在删除认证信息时，同样还可以发送异常提示消息；在判断出未再次接收到服务器发送的认证失败消息的情况下，

则接收到服务器发送的关于用户请求的响应消息。

[0068] 虽然，目标应用程序向服务器发送的是包含了由服务器返回的新的访问令牌的用户请求，但对于服务器而言，还是对接收到的上述用户请求进行正常的认证，所以上该用户请求还是存在没有通过服务器对其的验证的可能性。

[0069] 可选地，在接收到服务器发送的第二访问令牌的情况下，将用户请求中包含的第一访问令牌替换为第二访问令牌后发送至服务器之后，本发明实施例所提供的用户请求的认证方法还包括如下步骤S126至步骤S134：

[0070] 步骤S126：判断是否接收到服务器发送的认证失败消息。

[0071] 其中，上述步骤S126中认证失败消息是指服务器对包含第二访问令牌的用户请求进行认证，所反馈的消息。

[0072] 步骤S128：在判断出接收到认证失败消息的情况下，发送第二刷新请求至服务器，以请求第四访问令牌，其中，本发明实施例中的第四访问令牌与上述步骤S106中的第一访问令牌，以及上述步骤S110中的第二访问令牌均不相同，第二刷新请求中包含刷新令牌。

[0073] 步骤S130：判断是否接收到服务器发送的第四访问令牌。

[0074] 步骤S132：在判断出接收到第四访问令牌的情况下，将用户请求中包含的第二访问令牌替换为第四访问令牌后发送至服务器，以得到响应用户请求的响应消息。

[0075] 步骤S134：在判断出未接收到第四访问令牌的情况下，删除认证信息。

[0076] 即使目标应用程序向服务器发送的是包含了由服务器返回的新的访问令牌(即第二访问令牌)的用户请求，在发送上述用户请求后，目标应用程序还需判断是否接收服务器发送的关于对用户请求认证失败的消息。其中，如果目标应用程序接收到服务器发送的关于用户请求认证失败的消息，则会自动向服务器再一次(即第二次)发送包含刷新令牌的发送刷新请求。服务器在第二次收到上述刷新请求后，仍会判断此次接收到的刷新令牌是否在有效使用期限内，如果服务器判断出此次接收到的刷新令牌在有效使用期限内的话，服务器会再一次(即第二次)发送新的访问令牌(即第四访问令牌)给目标应用程序，目标应用程序在再次(即第二次)接收到新的访问令牌(即第四访问令牌)的情况下，会将之前用户请求中包含的访问令牌即第二访问令牌)再次替换，具体为将第二访问令牌替换成第四访问令牌，并将再次替换了访问令牌的用户请求再次发送给服务器。如果服务器判断出此次接收到的刷新令牌不在有效使用期限内的话，则不会再一次(即第二次)发送新的访问令牌(即第四访问令牌)给目标应用程序，那么目标应用程序也就不会收到第四访问令牌，此时，也是会删除认证信息，并且在删除认证信息时，同样还可以发送异常提示消息。

[0077] 在本发明实施例中，即使在之前用户请求没有通过本地认证的情况下，如果服务器对用户请求还是认证失败，目标应用程序则会再次(即第二次)自动获取新的，有效的认证介质(即访问令牌)，并同样在将上述用户请求中已经失效的认证介质替换成新获取的认证介质后再次发给服务器，使得在不需要用户重新发送用户请求的情况下，又增加了一次服务器对用户请求进行认证的次数，进一步达到了在对用户请求进行认证时，简化用户操作的效果。

[0078] 需要说明的是，不论本发明前述内容的实施例中什么情况下删除了认证信息，在删除认证信息后，如果用户想要再次发送用户请求至目标应用程序，则需重新登录该目标应用程序。其中，在用户重新输入正确的账户信息登录目标应用程序的过程中，该目标应用

程序会向服务器请求新的认证信息，在接收到服务器发送的新的认证信息后，会将新的认证信息进行本地存储。

[0079] 可选地，在判断出接收到第四访问令牌的情况下，将用户请求中包含的第二访问令牌替换为第四访问令牌后发送至服务器之后，本发明实施例所提供的用户请求的认证方法还包括：判断是否再次接收到服务器发送的认证失败消息。其中，此处认证失败消息是指服务器对包含上述第四访问令牌的用户请求进行认证，所反馈的消息。其中，在判断出再次接收到服务器发送的认证失败消息的情况下，删除权证信息，并且在删除认证信息时，同样还可以发送异常提示消息；在判断出未再次接收到服务器发送的认证失败消息的情况下，则接收到服务器发送的关于用户请求的响应消息。

[0080] 图2是根据本发明实施例可选的用户请求的认证方法的流程图，如图2所示，该方法主要包括如下步骤S202至步骤S234：

[0081] 步骤S202：接收包含第一访问令牌的用户请求，该步骤同步骤S102，在此不再重复说明。

[0082] 步骤S204：对包含第一访问令牌的用户请求进行认证，该步骤同步骤S104，在此不再重复说明。具体地，可通过执行上述步骤S1041至步骤S1045完成对包含第一访问令牌的用户请求的认证。

[0083] 步骤S206：判断包含第一访问令牌的用户请求是否通过认证，其中，在判断出包含第一访问令牌的用户请求通过认证的情况下，执行步骤S218；在判断出包含第一访问令牌的用户请求未通过认证的情况下，执行步骤S208。

[0084] 步骤S208：发送第一刷新请求至服务器，该步骤同步骤S108，在此不再重复说明。

[0085] 步骤S210：在发送第一刷新请求至服务器后，判断是否接收到服务器发送的第二访问令牌，该步骤同步骤S112，在此不再重复说明。其中，在判断出接收到服务器发送的第二访问令牌的情况下，执行步骤S212；在判断出未接收到服务器发送的第二访问令牌的情况下，执行步骤S234。

[0086] 步骤S212：将用户请求中包含的第一访问令牌替换为第二访问令牌，并发送该用户请求至服务器，该步骤同步骤S110，在此不再重复说明。

[0087] 步骤S214：在将用户请求中包含的第一访问令牌替换为第二访问令牌，并发送该用户请求至服务器后，判断是否接收到服务器发送的认证失败消息，该步骤同步骤S126，在此不再重复说明。其中，在判断出接收到服务器发送的认证失败消息的情况下，执行步骤S216；在判断出未接收到服务器发送的认证失败消息的情况下，执行步骤S236。

[0088] 步骤S216：发送第二刷新请求至服务器，该步骤同步骤S128，在此不再重复说明。

[0089] 步骤S218：发送包含第一访问令牌的用户请求至服务器，该步骤同步骤S106，在此不再重复说明。

[0090] 步骤S220：在发送第二刷新请求至服务器后，判断是否接收到服务器发送的第四访问令牌，该步骤同步骤S130，在此不再重复说明。其中，在判断出接收到服务器发送的第四访问令牌的情况下，执行步骤S230；在判断出未接收到服务器发送的第四访问令牌的情况下，执行步骤S234。

[0091] 步骤S222：在发送包含第一访问令牌的用户请求至服务器后，判断是否接收到服务器发送的认证失败消息，该步骤同步骤S116。具体地，判断是否接收到服务器发送的对用

户请求认证失败的消息。其中，如果接收到服务器发送的对用户请求认证失败的消息，执行步骤S224；如果未接收到服务器发送的对用户请求认证失败的消息，会接收到服务器发送的关于用户请求的响应消息，也即执行步骤S236。需要说明的是，上述内容提到的用户请求中包含的是第一访问令牌。

[0092] 步骤S224：发送第二刷新请求至服务器，该步骤同步骤S118，在此不再重复说明。

[0093] 步骤S226：在发送第二刷新请求至服务器后，判断是否接收到服务器发送的第四访问令牌，该步骤同步骤S120，在此不再重复说明。其中，在判断出接收到服务器发送的第四访问令牌的情况下，执行步骤S228；在判断出未接收到服务器发送的第四访问令牌的情况下，执行步骤S234。

[0094] 步骤S228：将用户请求中包含的第一访问令牌替换为第四访问令牌，并发送该用户请求至服务器，该步骤同步骤S122，在此不再重复说明。

[0095] 步骤S230：将用户请求中包含的第二访问令牌替换为第四访问令牌，并发送该用户请求至服务器，该步骤同步骤S132，在此不再重复说明。

[0096] 步骤S232：在将用户请求中包含的第二访问令牌替换为第四访问令牌，并发送该用户请求至服务器后，或者在将用户请求中包含的第一访问令牌替换为第四访问令牌，并发送该用户请求至服务器后，判断是否接再次收到服务器发送的认证失败消息。具体地，本步骤中认证失败消息是指服务器对包含第四访问令牌的用户请求进行认证，所反馈的消息。其中，第四访问令牌可以是替换了第一访问令牌的第四访问令牌，还可以是替换了第二访问令牌的第四访问令牌。其中，在判断出未再次接收到服务器发送的认证失败消息的情况下，执行步骤S234；在判断出再次接收到服务器发送的认证失败消息的情况下，执行步骤S236。

[0097] 步骤S234：删除认证信息，并抛出异常。具体地，本步骤中的认证信息即为上述内容中提到存储在应用程序中的认证信息，该认证信息中包含访问令牌和刷新令牌，认证信息中的访问令牌即为上述发明实施例中的第三访问令牌。

[0098] 步骤S236：接收到服务器发送的响应消息，上述响应消息为用户请求的响应消息。

[0099] 同样的，不论本发明实施例中在什么情况下删除了认证信息，在删除认证信息后，如果用户想要再次发送用户请求至目标应用程序，则需重新登录该目标应用程序。其中，在用户重新输入正确的账户信息登录目标应用程序的过程中，该目标应用程序会向服务器请求新的认证信息，在接收到服务器发送的新的认证信息后，会将新的认证信息进行本地存储。

[0100] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0101] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储

介质(如ROM/RAM、磁碟、光盘)中,包括若干指令用以使得一台终端设备(可以是手机,计算机,服务器,或者网络设备等)执行本发明各个实施例所述的方法。

[0102] 实施例2

[0103] 根据本发明实施例,还提供了一种用于实施上述用户请求的认证方法的用户请求的认证装置,该用户请求的认证装置主要用于执行本发明实施例上述内容所提供的用户请求的认证方法,以下对本发明实施例所提供的用户请求的认证装置做具体介绍:

[0104] 在本发明实施例中,设备为具有触摸屏幕的,且可以安装应用程序的任何类型终端,例如手机、平板电脑等。

[0105] 图3是根据本发明实施例的用户请求的认证装置的示意图,如图3所示,该装置主要包括:接收单元10、认证单元20、第一发送单元30、第二发送单元40和第三发送单元50,其中:

[0106] 接收单元10用于接收用户请求,其中,用户请求为用户接触设备屏幕中的当前显示页面时产生的请求,用户请求中包含第一访问令牌。

[0107] 认证单元20用于根据目标应用程序中存储的认证信息对用户请求进行认证,其中,目标应用程序为当前显示页面对应的应用程序。

[0108] 第一发送单元30用于在用户请求通过认证的情况下,发送用户请求至服务器,以得到响应用户请求的响应消息。

[0109] 第二发送单元40用于在用户请求未通过认证的情况下,发送第一刷新请求至服务器,以请求得到第二访问令牌,其中,第二访问令牌与第一访问令牌不同,第一刷新请求中包含认证信息中存储的刷新令牌。

[0110] 第三发送单元50用于在接收到服务器发送的第二访问令牌的情况下,将用户请求中包含的第一访问令牌替换为第二访问令牌后发送至服务器,以得到响应用户请求的响应消息。

[0111] 在本发明实施例中,应用程序接收到用户请求后,根据其内存储的认证信息对上述用户请求进行本地认证。如果用户请求通过本地认证,则将用户请求发送至服务器,以得到该用户请求的响应消息;如果用户请求未通过本地认证,该应用程序会自动获取新的,有效的认证介质(即,访问令牌),并将上述用户请求中已经失效的认证介质替换成新获取的认证介质,即也同样认为完成了对该用户请求的本地认证,最后发送替换了认证介质后的用户请求至服务器。

[0112] 而相关技术中,在对用户请求进行认证时,如果应用程序对用户第一次发送的用户请求进行认证后,判断出第一次接收到的用户请求未通过认证,会提示该用户需要再次发送上述用户请求,以获取有效的认证介质。当该应用程序第二次接收到上述用户请求时,会通过服务器获取到有效的认证介质,但是在收到有效的认证介质后,仍会提示用户需要再一次(即第三次)发送上述用户请求,其中,再一次发送的用户请求中包含了有效的认证介质。由于第三次发送的用户请求中包含了有效的认证介质,所以上述用户请求可以通过本地认证,即完成了对用户请求的认证,这时应用程序会将用户请求转发至服务器。通过上述描述可知,现有技术中对用户请求进行认证时,认证过程较为繁琐,需要用户多次发生同一用户请求,才可得到上述用户请求的响应信息。

[0113] 通过以上对比,可以看出本发明实施例中,对用户请求进行认证时,即使用户请求

没有通过本地认证，用户也只需发送一次用户请求即可完成对该用户请求的认证，解决了现有技术中对用户请求进行认证的方式较为繁琐，导致用户操作不便的问题，进而达到了简化对用户请求的认证过程，提高认证效率的效果。此外，本发明实施例所提供的认证方式，还起到了简化用户操作的效果。

[0114] 发明上述实施例所提供的用户请求的认证装置可以应用到任一安装在终端设备中的应用程序中。

[0115] 此外，本发明上述实施例中，目标应用程序根据其内存储的认证信息对用户请求进行认证的过程，也就是应用程序对用户请求进行认证的过程，可以称为本地认证。

[0116] 可选地，第一访问令牌中包含由32位或者64位的字符、数字和特殊字符随机组成的序列。

[0117] 可选地，认证信息中存储的刷新令牌中包含三部分内容，一部分内容是由32位或者64位的字符、数字和特殊字符随机组成的序列，另一部分内容是申请刷新令牌的时间，还有一部分内容是刷新令牌的有效使用期限。在本发明实施例中，可以将刷新令牌的有效使用期限设置较为长久，例如：1年。那么，认证信息则持久化的存储在应用程序中，上述持久化的存储时长由刷新令牌的有效使用期限决定。

[0118] 可选地，认证信息中除了存储有刷新令牌外，还存储有第三访问令牌，认证单元20包括目标应用程序中的应用程序编程接口、网络请求接口和网络模块，其中：

[0119] 目标应用程序中的应用程序编程接口用于将用户请求发送至对应的网络请求接口。

[0120] 其中，目标应用程序在接收到用户请求后，通过其内的应用程序编程接口调用与该用户请求对应的网络请求接口的方式，将上述用户请求发送至与其对应的网络请求接口。

[0121] 网络请求接口用于将用户请求发送至网络模块。

[0122] 网络模块用于根据第三访问令牌判断第一访问令牌是否有效，其中，在判断出第一访问令牌有效的情况下，用户请求通过认证；在判断出第一访问令牌无效的情况下，用户请求未通过认证。

[0123] 其中，网络模块为对基础网络请求模块进行认证权限扩展后的模块。网络模块用于对用户请求进行认证，并将接收到的，且通过认证的用户请求继续转发至服务器。需要说明的是，不同的用户请求都是通过网络模块转发至服务器的，并且该网络模块是唯一的。不同用户请求之间的差异体现在各自用户请求URL链接以及每个用户请求所规定的参数。当接收到不同的用户请求时，对网络模块来说，只是不同参数的差异，对每个用户请求进行认证的处理流程都是相同的。

[0124] 可选地，第三访问令牌中也包含三部分内容，分别是由32位或者64位的字符、数字和特殊字符随机组成的序列、申请该访问令牌的时间以及该访问令牌的有效使用期限。

[0125] 进一步可选地，网络模块包括获取子模块和判断子模块，其中，获取子模块用于网络模块获取第三访问令牌中的有效使用期限；判断子模块用于判断接收到第一访问令牌的时间是否超过有效使用期限，其中，在判断出接收到第一访问令牌的时间未超过有效使用期限的情况下，表示第一访问令牌有效，则确定用户请求通过认证；在判断出接收到第一访问令牌的时间已超过有效使用期限的情况下，表示第一访问令牌无效，则确定用户请求未

通过认证。

[0126] 可选地，本发明实施例所提供用户请求的认证装置还包括第一判断单元和第一删除单元，其中：

[0127] 第一判断单元用于在用户请求未通过认证的情况下，发送第一刷新请求至服务器之后，判断是否接收到服务器发送的第二访问令牌。

[0128] 可以由网络模块将包含刷新令牌的第一刷新请求发送至服务器。由于刷新令牌也是有使用时间限制的，所以很有可能发送至服务器的第一刷新请求中包含的刷新令牌已经超过该令牌的有效使用期限，即该刷新令牌已经过期，那么服务器在接收到上述用于请求得到第二访问令牌的刷新请求后，会先判断刷新请求中的刷新令牌是否已经过期，如果判断出刷新令牌已经过期，则服务器不会发送第二访问令牌给目标应用程序，如果判断出刷新令牌未过期，则服务器会发送第二访问令牌给目标应用程序。

[0129] 第一删除单元用于在判断出未接收到第二访问令牌的情况下，删除认证信息。

[0130] 进一步可选地，第一删除单元还用于在判断出未接收到第二访问令牌的情况下，删除认证信息时，发出异常提示消息。该异常提示消息可以体现在目标应用程序的系统日志中，用于向目标应用程序后台的工作人员反馈用户请求未能响应；还可以以文字的形式显示在设备屏幕中，用于提醒用户进行相应操作。例如，上述文字可以是：请检查网络设置。

[0131] 在用户请求通过本地认证之后，为了得到该用户请求的响应消息，目标应用程序还会继续将该用户请求发送给服务器，但是，服务器在接收到上述用户请求后，会再次对该用户请求进行认证。

[0132] 需要说明的是，在本地认证的过程中，可能只是检查用户请求中的访问令牌是否超过有效使用期限，即检查用户请求中的访问令牌是否有效，而服务器在对用户请求进行认证的过程中，检查的内容包括但不限于用户请求中访问令牌是否有效，还会对访问令牌进行其它内容的检查，例如，检查访问令牌是否合法等。如果服务器检查的全部内容，用户请求都是符合条件或要求的，那么服务器会返回响应该用户请求的响应消息给目标应用程序，如果服务器检查的全部内容中，用户请求中有至少一项不符合条件或者要求，则服务器会返回对用户请求认证失败的消息给目标应用程序。

[0133] 通过上述描述可知，目标应用程序对用户请求的认证与服务器对用户请求的认证之间是相互独立的，互不影响的，即，服务器不会因为用户请求通过了目标应用程序对其的认证，而不再对上述用户请求进行认证。

[0134] 可选地，本发明实施例所提供的用户请求的装置还包括第二判断单元、第四发送单元、第三判断单元、第五发送单元和第二删除单元，其中：

[0135] 第二判断单元用于在用户请求通过认证的情况下，发送用户请求至服务器之后，判断是否接收到服务器发送的认证失败消息。

[0136] 其中，上述第二判断单元中认证失败消息是指服务器对包含第一访问令牌的用户请求进行认证，所反馈的消息。

[0137] 第四发送单元用于在判断出接收到认证失败消息的情况下，发送第二刷新请求至服务器，以请求第四访问令牌，其中，第四访问令牌与第一访问令牌不相同，第二刷新请求中包含刷新令牌。

[0138] 第三判断单元用于判断是否接收到服务器发送的第四访问令牌。

[0139] 第五发送单元用于在判断出接收到第四访问令牌的情况下，将用户请求中包含的第一访问令牌替换为第四访问令牌后发送至服务器，以得到响应用户请求的响应消息。

[0140] 第二删除单元用于在判断出未接收到第四访问令牌的情况下，删除认证信息。

[0141] 在发明实施例中，在包含了第一访问令牌的用户请求通过了目标应用程序对其的本地认证的情况下，目标应用程序会将通过本地认证的用户请求发送至服务器，在将上述用户请求发送至服务器后，目标应用程序还需判断是否接收到服务器发送的关于对用户请求认证失败的消息。其中，如果目标应用程序接收到服务器发送的关于用户请求认证失败的消息，则会向服务器发送包含刷新令牌的发送第二刷新请求。服务器在收到包含刷新请求后，会判断刷新令牌是否在有效使用期限内，如果服务器判断出刷新令牌在有效使用期限内的话，服务器会发送新的访问令牌(即第四访问令牌)给目标应用程序，目标应用程序在接收到第四访问令牌的情况下，会将之前用户请求中包含的第一访问令牌替换成第四访问令牌后，再次将用户请求发送给服务器。

[0142] 需要说明的是，上述第五发送单元中的第四访问令牌可能与上述第三发送单元50中的第二访问令牌相同，也可能不同，但是与上述第一发送单元30中的第一访问令牌是不相同的。如果服务器判断出刷新令牌不在有效使用期限内的话，则不会发送第四访问令牌至目标应用程序，那么目标应用程序也就不会收到第四访问令牌，此时，也是会删除认证信息，并且在删除认证信息时，同样还可以发送异常提示消息。

[0143] 在本发明实施例中，在服务器对用户请求认证失败的情况下，目标应用程序也会自动获取新的，有效的认证介质(即访问令牌)，并同样将上述用户请求中已经失效的认证介质替换成新获取的认证介质后再次发给服务器，使得在不需要用户重新发送用户请求的情况下，增加了一次服务器对用户请求的认证，进一步达到了在对用户请求进行认证时，简化用户操作的效果。

[0144] 可选地，本发明实施例所提供的用户请求的认证装置还包括第六判断单元，其中，第六判断单元用于在判断出接收到第四访问令牌的情况下，将用户请求包含中的第一访问令牌替换为第四访问令牌后发送至服务器之后，判断是否再次接收到服务器发送的认证失败消息。其中，上述认证失败消息是指：服务器对包含第四访问令牌的用户请求进行认证，所反馈的消息。其中，在再次判断出接收到服务器发送的认证失败消息的情况下，删除权证信息，并且在删除认证信息时，同样还可以发送异常提示消息；在判断出未再次接收到服务器发送的认证失败消息的情况下，则接收到服务器发送的关于用户请求的响应消息。

[0145] 虽然，目标应用程序向服务器发送的是包含了由服务器返回的新的访问令牌的用户请求，但对于服务器而言，还是对接收到的上述用户请求进行正常的认证，所以上该用户请求还是存在没有通过服务器对其的验证的可能性。

[0146] 可选地，本发明实施例所提供的用户请求的认证装置还包括第四判断单元、第六发送单元、第五判断单元、第七发送单元和第三删除单元，其中：

[0147] 第四判断单元用于在接收到服务器发送的第二访问令牌的情况下，将用户请求中的第一访问令牌替换为第二访问令牌后发送至服务器之后，判断是否接收到服务器发送的认证失败消息。

[0148] 其中，上述第四判断单元中认证失败消息服务器对包含第二访问令牌的用户请求进行认证，所反馈的消息。

[0149] 第六发送单元用于在判断出接收到认证失败消息的情况下，发送第二刷新请求至服务器，以请求第四访问令牌，其中，本发明实施例中的第四访问令牌与上述接收单元10中的第一访问令牌，以及上述第三发送单元50中的第二访问令牌均不相同，第二刷新请求中包含刷新令牌。

[0150] 第五判断单元用于判断是否接收到服务器发送的第四访问令牌。

[0151] 第七发送单元用于在判断出接收到第四访问令牌的情况下，将用户请求中包含的第二访问令牌替换为第四访问令牌后发送至服务器，以得到响应用户请求的响应消息。

[0152] 第三删除单元用于在判断出未接收到第四访问令牌的情况下，删除认证信息。

[0153] 即使目标应用程序向服务器发送的是包含了由服务器返回的新的访问令牌(即第二访问令牌)的用户请求，在发送上述用户请求后，目标应用程序还需判断是否接收服务器发送的关于对用户请求认证失败的消息。其中，如果目标应用程序接收到服务器发送的关于用户请求认证失败的消息，则会自动向服务器再一次(即第二次)发送包含刷新令牌的发送刷新请求。服务器在第二次收到上述刷新请求后，仍会判断此次接收到的刷新令牌是否在有效使用期限内，如果服务器判断出此次接收到的刷新令牌在有效使用期限内的话，服务器会再一次(即第二次)发送新的访问令牌(即第四访问令牌)给目标应用程序，目标应用程序在再次(即第二次)接收到新的访问令牌(即第四访问令牌)的情况下，会将之前用户请求中包含的访问令牌即第二访问令牌)再次替换，具体为将第二访问令牌替换成第四访问令牌，并将再次替换了访问令牌的用户请求再次发送给服务器。如果服务器判断出此次接收到的刷新令牌不在有效使用期限内的话，则不会再一次(即第二次)发送新的访问令牌(即第四访问令牌)给目标应用程序，那么目标应用程序也就不会收到第四访问令牌，此时，也是会删除认证信息，并且在删除认证信息时，同样还可以发送异常提示消息。

[0154] 在本发明实施例中，即使在之前用户请求没有通过本地认证的情况下，如果服务器对用户请求还是认证失败，目标应用程序则会再次(即第二次)自动获取新的，有效的认证介质(即访问令牌)，并同样在将上述用户请求中已经失效的认证介质替换成新获取的认证介质后再次发给服务器，使得在不需要用户重新发送用户请求的情况下，又增加了一次服务器对用户请求进行认证的次数，进一步达到了在对用户请求进行认证时，简化用户操作的效果。

[0155] 需要说明的是，不论本发明前述内容的实施例中什么情况下删除了认证信息，在删除认证信息后，如果用户想要再次发送用户请求至目标应用程序，则需重新登录该目标应用程序。其中，在用户重新输入正确的账户信息登录目标应用程序的过程中，该目标应用程序会向服务器请求新的认证信息，在接收到服务器发送的新的认证信息后，会将新的认证信息进行本地存储。

[0156] 可选地，本发明实施例所提供的用户请求的认证装置还包括第七判断单元，其中，第七判断单元用于在判断出接收到第四访问令牌的情况下，将用户请求中包含的第二访问令牌替换为第四访问令牌后发送至服务器之后，判断是否再次接收到服务器发送的认证失败消息。其中，此处的认证失败的消息是指服务器对包含上述第四访问令牌的用户请求进行认证，所反馈的消息。其中，在判断出再次接收到服务器发送的认证失败消息的情况下，删除权证信息，并且在删除认证信息时，同样还可以发送异常提示消息；在判断出未再次接收到服务器发送的认证失败消息的情况下，则接收到服务器发送的关于用户请求的响应消

息。

[0157] 从以上的描述中，可以看出，本发明解决了现有技术中对用户请求进行认证的方式较为繁琐，导致用户操作不便的问题，进而达到了简化对用户请求的认证过程，提高认证效率的效果。

[0158] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0159] 在本发明的上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0160] 在本申请所提供的几个实施例中，应该理解到，所揭露的客户端，可通过其它的方式实现。其中，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，单元或模块的间接耦合或通信连接，可以是电性或其它的形式。

[0161] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0162] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0163] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0164] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

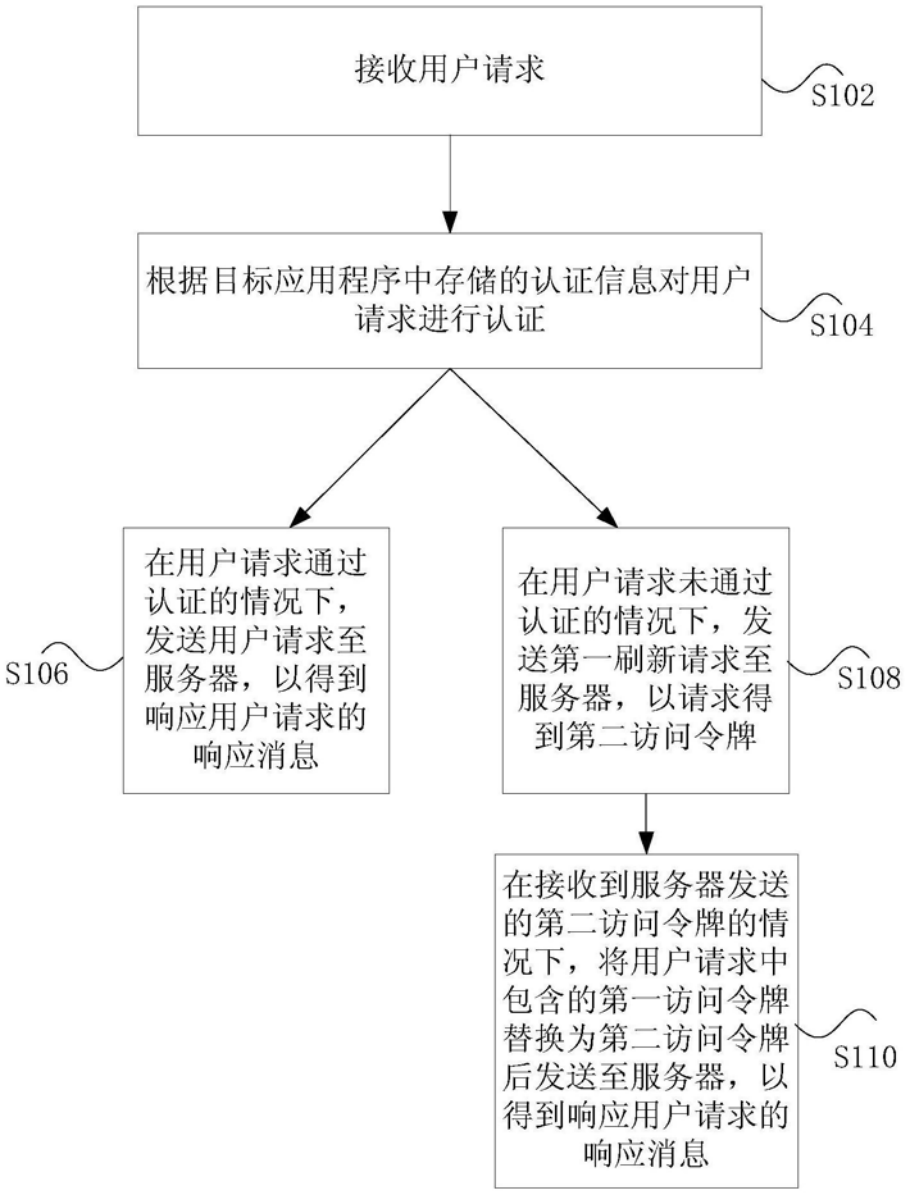

接收用户请求
S102
根据目标应用程序中存储的认证信息对用户请求进行认证
S104
在用户请求通过认证的情况下，发送用户请求至服务器，以得到响应用户请求的响应消息
S106
在用户请求未通过认证的情况下，发送第一刷新请求至服务器，以请求得到第二访问令牌
S108
在接收到服务器发送的第二访问令牌的情况下，将用户请求中包含的第一访问令牌替换为第二访问令牌后发送至服务器，以得到响应用户请求的响应消息
S110

图1

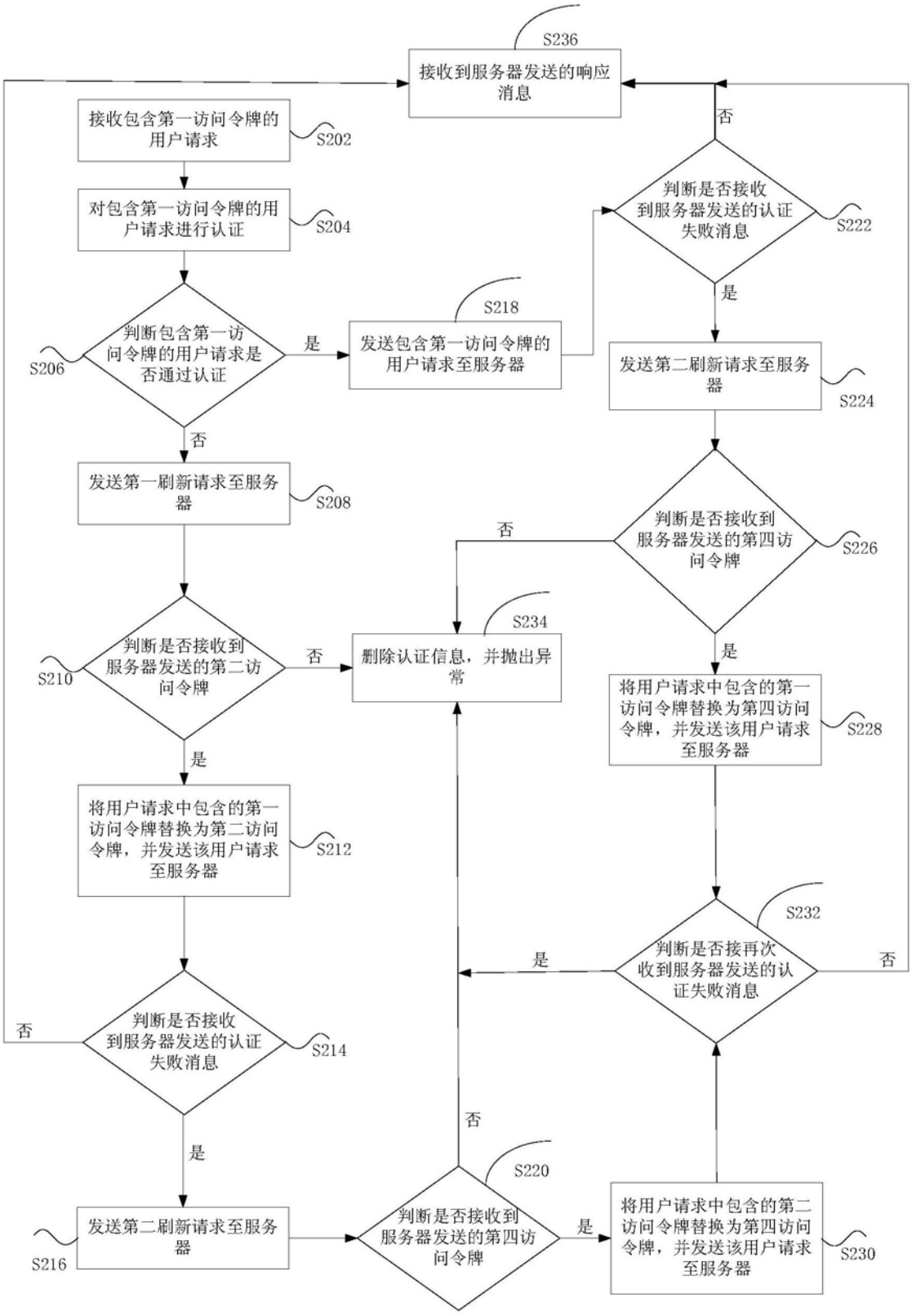

S236
接收到服务器发送的响应消息
接收包含第一访问令牌的用户请求
S202
对包含第一访问令牌的用户请求进行认证
S204
判断包含第一访问令牌的用户请求是否通过认证
S206
是
否
S218
发送包含第一访问令牌的用户请求至服务器
发送第一刷新请求至服务器
S208
判断是否接收到服务器发送的第二访问令牌
S210
否
是
S234
删除认证信息，并抛出异常
将用户请求中包含的第一访问令牌替换为第二访问令牌，并发送该用户请求至服务器
S212
判断是否接收到服务器发送的认证失败消息
S214
否
是
发送第二刷新请求至服务器
S216
判断是否接收到服务器发送的第四访问令牌
S220
否
是
判断是否接收到服务器发送的认证失败消息
S222
否
是
发送第二刷新请求至服务器
S224
判断是否接收到服务器发送的第四访问令牌
S226
否
是
将用户请求中包含的第一访问令牌替换为第四访问令牌，并发送该用户请求至服务器
S228
判断是否接再次收到服务器发送的认证失败消息
S232
是
否
将用户请求中包含的第二访问令牌替换为第四访问令牌，并发送该用户请求至服务器
S230

图2

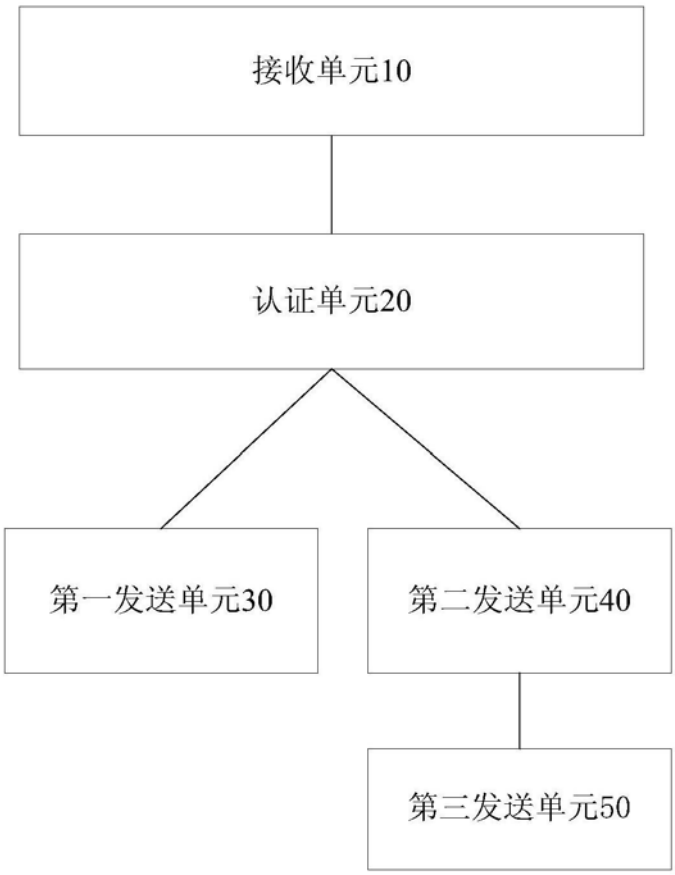


图3