(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 105245541 B
(45)授权公告日 2020.02.18

(21)申请号 201510711862.X

(22)申请日 2015.10.28

(65)同一申请的已公布的文献号
申请公布号 CN 105245541 A

(43)申请公布日 2016.01.13

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 任杰

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 张振伟 张颖玲

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

(56)对比文件
CN 104994073 A,2015.10.21,全文.
US 2006095788 A1,2006.05.04,全文.
CN 104506492 A,2015.04.08,说明书第[0050]-[00136]段.

审查员 易水英

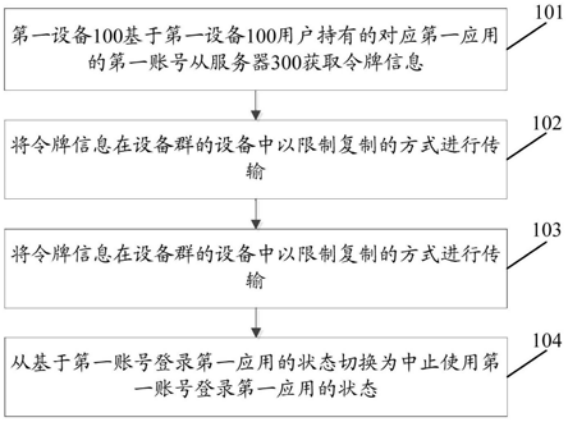
权利要求书4页 说明书12页 附图8页

(54)发明名称

鉴权方法、设备及系统

(57)摘要

本发明公开一种鉴权方法、设备和系统;方法包括:第一设备基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息;将令牌信息在设备群的设备中以限制复制的方式进行传输,令牌信息用于供服务器对设备群中具有所述令牌信息的第二设备进行鉴权,在鉴权通过时为第二设备分配第一账号的使用权限;确定第二设备基于第一账号的使用权限登录第一应用,从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。采用本发明,能够在多设备使用同一账号登录应用时,避免账号的密钥泄露以有效保障账号安全。



CN 105245541 B

1.一种鉴权方法,其特征在于,所述方法包括:

第一设备基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息,所述令牌信息为所述服务器基于所述第一账号生成,所述令牌信息中附有数字签名或数字证书,用于表征所述第一设备用户拥有所述第一账号的所有权;

将所述令牌信息在设备群的设备中以限制复制的方式进行传输,所述令牌信息还用于供所述服务器对所述设备群中具有所述令牌信息的第二设备进行鉴权,在鉴权通过时为所述第二设备分配所述第一账号的使用权限,以支持所述第二设备使用所述第一账号登录所述第一应用;

所述令牌信息中携带时限信息,用于供所述服务器检测所述第二设备获取的所述第一账号的使用权限是否处于有效期,并在超出有效期时中止分配给所述第二设备的所述第一账号的使用权限;

确定所述第二设备基于所述第一账号的使用权限登录所述第一应用,从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

2.如权利要求1所述的方法,其特征在于,所述第一设备基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息,包括:

所述第一设备通过令牌信息请求从所述服务器获取所述令牌信息,所述令牌信息请求用于供所述服务器生成对应所述第一账户的标识;

加密所述标识得到所述令牌信息,并维护所述第一账号与所述标识的对应关系。

3.如权利要求2所述的方法,其特征在于,

所述第一账号与所述标识的对应关系用于供所述服务器从所述令牌信息解密出所述标识、并基于所述对应关系确定与所述标识对应的所述第一账号,分配所述第一账号的使用权限给所述第二设备;或者,

所述令牌信息和所述第一账号的信息用于供所述第二设备发送至所述服务器,使所述服务器基于所述对应关系验证所述第二设备发送的所述第一账号与所述令牌信息中携带的所述标识是否匹配,在匹配时分配所述第一账号的使用权限给所述第二设备。

4.如权利要求1所述的方法,其特征在于,所述方法还包括:

向所述服务器发送针对所述令牌信息的回收请求,所述回收请求中携带的所述令牌信息用于供所述服务器确定所述第一设备用户拥有所述第一账号的所有权时,中止为所述第二设备分配的对应所述第一账号的使用权限;

从中止使用所述第一账号登录所述第一应用的状态切换为恢复使用所述第一账号登录所述第一应用的状态。

5.如权利要求1至4任一项所述的方法,其特征在于,所述方法还包括:

所述令牌信息还用于供所述服务器检测所述设备群中分配有对应所述第一账号的使用权限的所述第二设备是否具有所述令牌信息,在不具有时中止为所述第二设备分配的对应所述第一账号的使用权限。

6.一种鉴权方法,其特征在于,所述方法包括:

服务器基于第一设备用户持有的对应第一应用的第一账号,生成对应所述第一账号的令牌信息,所述令牌信息中附有数字签名或数字证书,所述令牌信息表征所述第一设备用户拥有所述第一账号的所有权;

将所述令牌信息发送至第一设备，所述令牌信息用于供所述第一设备在设备群的设备中以限制复制的方式进行传输；

基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；

基于所述令牌信息携带的时限信息检测所述第二设备获取的所述第一账号的使用权限是否处于有效期，并在超出有效期时，中止为所述第二设备分配的对应所述第一应用的使用权限；

确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，触发所述第一设备从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

7.如权利要求6所述的方法，其特征在于，

所述服务器基于第一设备用户持有的对应第一应用的第一账号，生成对应所述第一账号的令牌信息，包括：

接收所述第一设备发送的令牌信息请求时，生成对应所述第一账户的标识；

加密所述标识得到所述令牌信息，并维护所述第一账号与所述标识的对应关系。

8.如权利要求7所述的方法，所述基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，包括：

从所述第二设备发送的所述令牌信息解密出所述标识；

基于所述对应关系确定与所述标识对应的所述第一账号，分配所述第一账号的使用权限给所述第二设备；

所述基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，包括：

从所述第二设备发送的所述令牌信息解密出所述标识；

基于所述对应关系验证所述第二设备发送的所述第一账号与所述第二设备发送的所述令牌信息中携带的所述标识是否匹配，在匹配时分配所述第一账号的使用权限给所述第二设备。

9.如权利要求6所述的方法，其特征在于，所述方法还包括：

接收所述第一设备发送的针对所述令牌信息的回收请求，所述回收请求中携带所述令牌信息；

基于所述令牌信息确定所述第一设备用户拥有所述第一账号的所有权时，中止为所述第二设备分配的对应所述第一账号的使用权限；

触发所述第一设备从中止使用所述第一账号登录所述第一应用的状态切换为恢复使用所述第一账号登录所述第一应用的状态。

10.如权利要求6至9任一项所述的方法，其特征在于，所述方法还包括：

检测所述设备群中分配有对应所述第一账号的使用权限的所述第二设备是否具有所述令牌信息，

在不具有所述令牌信息时，中止为所述第二设备分配的对应所述第一账号的使用权限。

11.一种第一设备，其特征在于，所述第一设备包括：

获取单元，用于基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息，所述令牌信息为所述服务器基于所述第一账号生成，所述令牌信息中附有数字签名或数字证书，用于表征所述第一设备用户拥有所述第一账号的所有权；

第一传输单元，用于将所述令牌信息在设备群的设备中以限制复制的方式进行传输，所述令牌信息还用于供所述服务器对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；以及

用于基于所述令牌信息携带的时限信息供所述服务器检测所述第二设备获取的所述第一账号的使用权限是否处于有效期，并在超出有效期时中止分配给所述第二设备的所述第一账号的使用权限；

切换单元，用于确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

12.如权利要求11所述的第一设备，其特征在于，

所述获取单元，还用于通过令牌信息请求从所述服务器获取所述令牌信息，所述令牌信息请求用于供所述服务器生成对应所述第一账户的标识，加密所述标识得到所述令牌信息，并维护所述第一账号与所述标识的对应关系。

13.如权利要求11或12任一项所述的第一设备，其特征在于，所述第一设备还包括：

回收单元，用于向所述服务器发送针对所述令牌信息的回收请求，所述回收请求中携带所述令牌信息，所述令牌信息用于供所述服务器确定所述第一设备用户拥有所述第一账号的所有权时，中止为所述第二设备分配的对应所述第一账号的使用权限；

所述切换单元，还用于从中止使用所述第一账号登录所述第一应用的状态切换为使用所述第一账号登录所述第一应用的状态。

14.一种服务器，其特征在于，所述服务器包括：

令牌单元，用于基于第一设备用户持有的对应第一应用的第一账号，生成对应所述第一账号的令牌信息，所述令牌信息中附有数字签名或数字证书，所述令牌信息表征所述第一设备用户拥有所述第一账号的所有权；

第二传输单元，用于将所述令牌信息发送至第一设备，所述令牌信息用于供所述第一设备在设备群的设备中以限制复制的方式进行传输；

鉴权单元，用于基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；以及

用于基于所述令牌信息携带的时限信息检测所述第二设备获取的所述第一账号的使用权限是否在有效期，并在超出有效期时，中止为所述第二设备分配的对应所述第一应用的使用权限；

触发单元，用于确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，触发所述第一设备从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

15.如权利要求14所述的服务器，其特征在于，

所述令牌单元，包括：

接收模块，用于接收所述第一设备发送的令牌信息请求时，生成对应所述第一账户的标识；

加密模块，用于加密所述标识得到所述令牌信息，并维护所述第一账号与所述标识的对应关系。

16.如权利要求15所述的服务器，其特征在于，

所述鉴权单元包括：

解密模块，用于从所述第二设备发送的所述令牌信息解密出所述标识；

分配单元，用于基于所述对应关系确定与所述标识对应的所述第一账号，分配所述第一账号的使用权限给所述第二设备；或者，用于基于所述对应关系验证所述第二设备发送的所述第一账号与所述令牌信息中携带的所述标识是否匹配，在匹配时分配所述第一账号的使用权限给所述第二设备。

17.如权利要求14所述的服务器，其特征在于，

所述传输单元还用于接收所述第一设备发送的针对所述令牌信息的回收请求，所述回收请求中携带所述令牌信息；

所述鉴权单元，还用于基于所述令牌信息确定所述第一设备用户拥有所述第一账号的所有权时，中止为所述第二设备分配的对应所述第一账号的使用权限；

所述切换单元，还用于触发所述第一设备从中止使用所述第一账号登录所述第一应用的状态切换为使用所述第一账号登录所述第一应用的状态。

18.如权利要求14至17任一项所述的服务器，其特征在于，

所述鉴权单元还用于检测所述设备群中分配有对应所述第一账号的使用权限的所述第二设备是否具有所述令牌信息，在不具有所述令牌信息时，中止为所述第二设备分配的对应所述第一账号的使用权限。

19.一种鉴权系统，其特征在于，包括权利要求11至13任一项所述的第一设备、以及权利要求14至18任一项所述的服务器。

20.一种存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1-10任一项所述的鉴权方法。

鉴权方法、设备及系统

技术领域

[0001] 本发明涉及通信领域的安全控制技术，尤其涉及一种鉴权方法、设备及系统。

背景技术

[0002] 随着设备的智能化，人们除了拥有台式机、笔记本电脑等常规的设备，还拥有智能手机、平板电脑、智能眼镜(Google眼镜)、智能手表(Apple watch)等多种形式的智能设备，这些设备都具有强大的智能性，能够运行多种不同的应用，例如，可以运行提供多种形式服务，包括线上服务(如在线多媒体播放、网上银行、社交服务如微信、微博等)，还包括线下服务(网上预定家政服务、在线购买提供送花上门服务的商品，如外卖、家政服务、电子产品、服装等)。

[0003] 用户需要使用预先注册的账号和密钥登录在设备中运行的应用才能使用应用所提供的服务，但是在账号的管理上存在安全隐患。

[0004] 在一个典型的场景中，用户1往往拥有多台设备，如智能手机、平板电脑等，并且用户往往会使用所拥有的设备来使用相同的服务，例如用户1可能在不同的时刻分别使用智能手机和平板电脑来使用微信，这就需要用户1在所持有的设备中分别设置存储微信的账号和密钥，由于用户1一般只会随身携带智能手机，而不会总是随身携带平板电脑、笔记本电脑等设备，这就给用户1的账号安全带来了隐患，导致恶意用户2可能使用用户的设备而登录应用使用服务，给用户1带来损失；

[0005] 在另一个典型的场景中，用户1希望将自身的账号(例如淘宝账号)暂时让渡给用户3使用，这就需要用户1通过特定方式向用户3告知用户1的账号和密钥(如用户1通过口头方式告知用户3，或通过用户1持有的设备向用户3持有的设备发送信息的方式告知)，这对用户1的账号安全带来了巨大的安全隐患。

[0006] 综上所述，相关技术对于在多设备使用同一账号时，避免账号的密钥泄露以有效保障账号安全、尚无有效解决方案。

发明内容

[0007] 本发明实施例提供一种鉴权方法、设备及系统，能够在多设备使用同一账号登录应用时，避免账号的密钥泄露以有效保障账号安全。

[0008] 本发明实施例的技术方案是这样实现的：

[0009] 第一方面，本发明实施例提供一种鉴权方法，所述方法包括：

[0010] 第一设备基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息，所述令牌信息为所述服务器基于所述第一账号生成，用于表征所述第一设备用户拥有所述第一账号的所有权；

[0011] 将所述令牌信息在设备群的设备中以限制复制的方式进行传输，所述令牌信息还用于供所述服务器对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登

录所述第一应用；

[0012] 确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

[0013] 第二方面，本发明实施例提供一种鉴权方法，所述方法包括：

[0014] 服务器基于第一设备用户持有的对应第一应用的第一账号，生成对应所述第一账号的令牌信息，所述令牌信息表征所述第一设备用户拥有所述第一账号的所有权；

[0015] 将所述令牌信息发送至第一设备，所述令牌信息用于供所述第一设备在设备群的设备中以限制复制的方式进行传输；

[0016] 基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；

[0017] 确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，触发所述第一设备从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

[0018] 第三方面，本发明实施例提供一种第一设备，所述第一设备包括：

[0019] 获取单元，用于基于第一设备用户持有的对应第一应用的第一账号从服务器获取令牌信息，所述令牌信息为所述服务器基于所述第一账号生成，用于表征所述第一设备用户拥有所述第一账号的所有权；

[0020] 第一传输单元，用于将所述令牌信息在设备群的设备中以限制复制的方式进行传输，所述令牌信息还用于供所述服务器对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；

[0021] 切换单元，用于确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

[0022] 第四方面，本发明实施例提供一种服务器，包括：

[0023] 令牌单元，用于基于第一设备用户持有的对应第一应用的第一账号，生成对应所述第一账号的令牌信息，所述令牌信息表征所述第一设备用户拥有所述第一账号的所有权；

[0024] 第二传输单元，用于将所述令牌信息发送至第一设备，所述令牌信息用于供所述第一设备在设备群的设备中以限制复制的方式进行传输；

[0025] 鉴权单元，用于基于所述令牌信息对所述设备群中具有所述令牌信息的第二设备进行鉴权，在鉴权通过时为所述第二设备分配所述第一账号的使用权限，以支持所述第二设备使用所述第一账号登录所述第一应用；

[0026] 触发单元，用于确定所述第二设备基于所述第一账号的使用权限登录所述第一应用，触发所述第一设备从基于所述第一账号登录所述第一应用的状态切换为中止使用所述第一账号登录所述第一应用的状态。

[0027] 第五方面，本发明实施例提供一种鉴权系统，包括前述的第一设备以及服务器。

[0028] 本发明实施例中，第一设备基于第一应用的第一账号获取令牌信息，将令牌信息作为设备群中的设备使用第一账号登录第一应用的鉴权凭证，在第一设备用户不必告知设备群中的设备用户与第一账号相应的密钥的前提下，即可对具有令牌信息的第二设备进行鉴权认证，避免了第一账号的密钥泄露的风险；同时，在第二设备基于第一账号登录第一应用时，第一设备还暂停使用第一账号登录第一应用以避免第一账号的登录冲突问题。

附图说明

[0029] 图1是本发明实施例中鉴权系统的结构示意图；

[0030] 图2是本发明实施例中鉴权方法的流程示意图一；

[0031] 图3是本发明实施例中鉴权方法的流程示意图二；

[0032] 图4是本发明实施例中鉴权方法的流程示意图三；

[0033] 图5是本发明实施例中鉴权方法的流程示意图四；

[0034] 图6是本发明实施例中鉴权方法的流程示意图五；

[0035] 图7是本发明实施例中第一设备运行的第一应用处于不可操作的状态示意图；

[0036] 图8是本发明实施例中操作第一设备回收第一账号的使用权限的示意图；

[0037] 图9是本发明实施例中第一设备的结构示意图；

[0038] 图10是本发明实施例中服务器的结构示意图。

具体实施方式

[0039] 以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0040] 本发明实施例记载一种鉴权方法，可以应用基于第一账号登录应用第一应用)的第一设备100中，上述的第一应并非特指第一设备100中运行的某一个应用，而是指基于账号和密钥对用户进行鉴权，在鉴权通过时允许第一设备100相应服务的应用，例如微信、QQ、以及提供第三方服务(包括线上的社交、购物、外卖等服务、以及线下的家政等服务)的各种应用，同理，上述的第一设备100也并非特指某一个或某一类设备，而是指能够运行上述应用并具备通信能力的设备，并与设备群的设备进行区分。

[0041] 上述的第一设备100以及设备群中的设备可以是智能手机、平板电脑或穿戴式设备(如智能眼镜、智能手表等)，还可以是智能汽车、智能家电(如智能冰箱、智能电池、机顶盒等)；智能手机的操作系统可以是安卓操作系统、IOS操作系统或其他任意第三方开发的可以运行于微型计算机结构(至少包括处理器和内存)的操作系统(如移动版Linux系统、黑莓QNX操作系统等)。

[0042] 第一设备100以及设备群中的设备可以内置各种通信模块以支持设备之间的通信，如近场通信(NFC)模块、蓝牙通信模块、红外通信模块、WiFi通信模块、蜂窝通信模块(支持2/3/4G下各种制式如CDMA/WCDMA/TD-SCDMA下的通信)；当设备群中的设备需要与目标设备进行通信时，可以在近距离通信的有效范围内探测是否能够与目标设备进行近距离方式的通信(如蓝牙、WiFi，以WiFi为例，可以通过向目标设备发送回声请求消息，如果接收到目标设备返回的数据包，则表明处于近距离的有效通信范围内)；如果在近距离的有效范围内没有探测到设备，则可以基于远程通信方式(如蜂窝通信)与目标设备建立通信。

[0043] 本发明实施例中还涉及服务器300，服务器300是可以是为实施本发明实施例而专门设置的服务器(也可以采用服务器集群的方式)，当然，服务器300也可以是第一应用的后台服务器，例如，当第一应用为微信时，相应的服务器300可以为微信的后台服务器；当第一应用为QQ时，相应的服务器300可以为QQ的后台服务器。

[0044] 基于上述记载的第一设备100、设备群和服务器300，参见图2，在步骤101中，第一设备100基于第一设备100用户持有的对应第一应用的第一账号从服务器300获取令牌信息；令牌信息为服务器300基于第一账号生成，用于表征第一设备100用户拥有第一账号的所有权；在步骤102中，第一设备100将令牌信息在设备群的设备中以限制复制的方式进行传输；令牌信息还用于供服务器300对设备群中具有令牌信息的第二设备200进行鉴权，在鉴权通过时为第二设备200分配第一账号的使用权限，以支持第二设备200使用第一账号登录第一应用；在步骤103中，第一设备100确定第二设备200基于第一账号的使用权限登录第一应用，相应地，在步骤104中，从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。

[0045] 上述方案中，第一设备100基于第一应用的第一账号获取令牌信息，将令牌信息作为设备群中的设备使用第一账号登录第一应用的鉴权凭证，在第一设备100用户不必告知设备群中的设备用户与第一账号相应的密钥的前提下，即可对具有令牌信息的第二设备200进行鉴权认证，避免了第一账号的密钥泄露的风险；同时，在第二设备200基于第一账号登录第一应用时，第一设备100还暂停使用第一账号登录第一应用以避免第一账号的登录冲突问题；同时，令牌信息在设备群中是不可复制的方式传递的，这就有效杜绝了多个设备持有令牌并基于第一账号登录第一应用的情况。

[0046] 基于上述记载的第一设备100、设备群、服务器300以及鉴权方法，提出以下各具体实施例。

[0047] 实施例一

[0048] 本实施例针对以下场景中的问题提出解决的技术方案，参见图1，第一设备100中运行第一应用，第一设备100用户通过第一设备100注册了使用第一应用所提供服务的账号信息，包括：第一账号以及相应的密钥信息；当第一设备100用户希望将第一账号临时给第二设备200(第二设备200用户可以与第一设备100用户为同一用户，也可以为不同的用户)使用，而又不希望泄露对应第一账号的密钥给第二设备200。

[0049] 参见图3示出的鉴权方法，包括以下步骤：

[0050] 步骤201，第一设备100向服务器300发送令牌信息请求。

[0051] 令牌信息请求携带第一设备100用户注册的对应第一应用的第一账户的信息。

[0052] 步骤202，服务器300接收到第一设备100发送的令牌信息请求时，生成对应第一账户的标识，加密标识得到对应的令牌信息。

[0053] 服务器300可以采用非对称加密算法(或对称加密算法)对标识进行加密，为放置令牌信息被恶意更改，令牌信息中还可以附有数字签名或数字证书，第一设备100利用数字签名来验证令牌信息的可靠性。

[0054] 步骤203，服务器300维护第一账号与标识的对应关系。

[0055] 对于不同的第一设备100发送令牌信息请求时，服务器300均根据各第一设备100中的运行的第一应用的账号对应生成标识(针对不同的第一账号生成的标识不同)，并维护

各第一账号与对应生成的标识的对应关系;具体实施时,可以采用任意具有单一映射功能的函数对第一账号进行计算得到对应的标识,也可以不利用第一账号进行计算,而是利用

[0056] 令牌信息用于表征第一设备100用户拥有第一账号的所有权。

[0057] 步骤204,服务器300传递令牌信息至第一设备100。

[0058] 步骤205,第一设备100将令牌信息在设备群的设备中以限制复制的方式进行传输。

[0059] 第一设备100可以主动发起令牌信息在设备群的传递,或者,在接收到设备群中的设备(设为第二设备200)使用第一账号登录第一应用的请求时,传递令牌信息至第二设备200,当第二设备200获取到令牌信息时,可以基于令牌信息向服务器300请求使用第一账号登录第一应用的使用权限,在使用完毕时以限制复制的方式传递令牌信息至设备群中的其他设备;当然,第二设备200也可以在获取到令牌信息时不向服务器300请求第一账号的使用权限,而是直接将令牌信息以限制复制的方式传递至设备群中的其他设备;由于令牌信息在设备群中是以限制复制方式传递的,因此,在第二设备200传递令牌信息至设备群中的其他设备之后,第二设备200没有保留令牌信息,也就是说,一旦令牌信息在设备群中传递,在任一个时刻设备群中只有一个设备具有令牌信息。

[0060] 后续以设备群中的第二设备200基于令牌信息请求基于第一账号登录第一应用的使用权限进行说明。

[0061] 步骤206,设备群中的第二设备200基于令牌信息向服务器300请求登录第一应用。

[0062] 第二设备200向服务器300发送的请求中携带令牌信息;本实施例中,第一设备100仅仅将令牌信息传递给第二设备200,也就是说,第二设备200不具有第一设备100用户所具有的第一应用第一账号,在第二设备200使用第一账号之前,确保了第一设备100用户的账号安全。

[0063] 步骤207,服务器300对设备群中具有令牌信息的第二设备200进行鉴权,在鉴权通过时为第二设备200分配第一账号的使用权限。

[0064] 服务器300接收到第二设备200的请求时,利用令牌信息的数字签名(或数字证书)验证令牌信息是否为服务器300下发并且未经修改,之后解密出令牌信息中的标识,利用服务器300所维护的标识与第一账号的对应关系,确定第二设备200所请求使用的第一账号,并为第二设备200分配第一账号的使用权限,将第二设备200中运行的第一应用的状态置为基于第一账号的登录状态,从而使第二设备200用户获得了第一账号的使用权限。

[0065] 上述过程中第一设备100用于不需要将第一账号的密钥告知第二设备200,就可以实现让第二设备200基于第一账号登录第一应用的目的,避免了密钥泄露给第二十设备而可能导致的账号的风险。

[0066] 步骤208,服务器300触发第一设备100从基于第一账号登录第一应用的状态,切换为中止使用第一账号登录第一应用的状态。

[0067] 服务器300在为第二设备200分配第一账号的使用权限(也就是使第二设备200基于第二账号登录的第一应用)之后,将第一设备100基于第一账号的使用状态切换为中止使用的状态,第一设备100的显示界面上可以显示当前不可操作的提示,以支持第二设备200用户基于第一账号使用第一应用提供的服务。

[0068] 针对上述的提出的场景,参见图1,第一设备100用户基于自身的第一账号登录第

一应用后，在第一应用的图形界面发起向服务器300申请令牌信息的操作，在接收到服务器300下发的令牌信息时，将令牌信息发送到第二设备200，第二设备200基于令牌信息向服务器300请求第一账号的使用权限，服务器300基于令牌信息鉴权成功后，为第二设备200分配第一账号的使用权限，第二设备200运行的第一应用处于基于第一账号登录的状态，第一设备100中运行的第一应用处于中止基于第一账号登录的状态。

[0069] 实施例二

[0070] 实施例一中第二设备200在请求第一账号的使用权限时，仅具有令牌信息，而不具有第一账号的信息(如名称)，由服务器300基于维护的标识与第一账号的对应关系确定；本实施例中，第二设备200在请求第一账号的使用权限时，具有令牌信息以及第一账号的信息(如名称)，第二设备200基于名称和令牌信息请求第一账号的使用权限，由服务器300进行账号和令牌的双重验证，提升了鉴权的安全性。

[0071] 参见图4示出的鉴权方法，包括以下步骤：

[0072] 步骤301，第一设备100向服务器300发送令牌信息请求。

[0073] 令牌信息请求携带第一设备100用户注册的对应第一应用的第一账户的信息。

[0074] 步骤302，服务器300接收到第一设备100发送的令牌信息请求时，生成对应第一账户的标识，加密标识得到对应的令牌信息。

[0075] 服务器300可以采用非对称加密算法(或对称加密算法)对标识进行加密，为放置令牌信息被恶意更改，令牌信息中还可以附有数字签名或数字证书，第一设备100利用数字签名来验证令牌信息的可靠性。

[0076] 步骤303，服务器300维护第一账号与标识的对应关系。

[0077] 具体处理与实施例一的记载相同，这里不再赘述。

[0078] 步骤304，服务器300传递令牌信息至第一设备100。

[0079] 后续以第一设备100用户将令牌信息传递给第二设备200，以使第二设备200基于第一账号登录第一应用为例说明。

[0080] 步骤305，第一设备100将令牌信息和第一账号传递给第二设备200。

[0081] 为了避免数据传递被恶意拦截而导致令牌信息和第一账号泄露的问题，第一设备100可以将令牌信息和第一账号分别传递至第二设备200，由于后续服务器300是基于第一账号和令牌信息进行鉴权的，即使第一账号和令牌信息中的一个被恶意获取，也无法通过服务器300的鉴权。

[0082] 步骤306，设备群中的第二设备200基于令牌信息和第一账号向服务器300请求登录第一应用。

[0083] 第二设备200向服务器300发送的请求中携带令牌信息和第一账号的信息；本实施例中，第一设备100将令牌信息和第一应用的信息传递给第二设备200，也就是说，第二设备200具有第一应用第一账号的名称。

[0084] 步骤307，服务器300对设备群中具有令牌信息的第二设备200进行鉴权，在鉴权通过时为第二设备200分配第一账号的使用权限。

[0085] 服务器300接收到第二设备200的请求时，利用令牌信息的数字签名(或数字证书)验证令牌信息是否为服务器300下发并且未经修改，之后解密出令牌信息中的标识，利用服务器300所维护的标识与第一账号的对应关系，确定令牌信息中的标识所对应的第一账号

与第二设备200发送的请求携带的第一账号是否一致，如果一致则为第二设备200分配第一账号的使用权限，将第二设备200中运行的第一应用的状态置为基于第一账号的登录状态，从而使第二设备200获得第一账号的使用权限。

[0086] 上述过程中第一账号的密钥不需要泄露给第二设备200用户，就可以实现让第二设备200基于第一账号登录第一应用的目的，避免了密钥泄露的风险。

[0087] 步骤308，服务器300触发第一设备100从基于第一账号登录第一应用的状态，切换为中止使用第一账号登录第一应用的状态。

[0088] 服务器300在为第二设备200分配第一账号的使用权限(也就是使第二设备200基于第二账号登录的第一应用)之后，将第一设备100基于第一账号的使用状态切换为中止使用的状态，第一设备100的显示界面上可以显示当前不可操作的提示，以支持第二设备200基于第一账号使用第一应用提供的服务。

[0089] 需要指出的是，前述实施例中是以第二设备200具有令牌信息为例进行说明的，第二设备200可以将令牌信息在设备群中以限制复制的方式传递，对于设备群中的第三设备400(不同于第二设备200的其他设备)具有令牌信息并向服务器300请求第一账号的使用权限时，服务器300进行的鉴权处理与前述实施例中服务器300对第二设备200的鉴权处理相同，这里不再赘述。

[0090] 另外，前述实施例以使第一设备100和设备群中的设备归属于不同的用户为例进行说明，通过向设备群中的设备传递令牌信息，可以在设备群中的设备不具有第一账号的密钥的前提下使用第一账号登录第一应用，从而不需要向其他设备用户(也就设备群中的设备用户)透露第一账号的密钥信息。

[0091] 实施例三

[0092] 本实施例基于实施例一和实施例二，在前述实施例中，第二设备200获取到第一账号的使用权限之后，服务器300需要确定分配给第二设备200的使用权限何时中止；可以通过以下方式结合判断：

[0093] 1)第二设备200具有令牌信息，当第二设备200不具有令牌信息时，说明令牌信息在设备群中发生了限制复制的传递，并为设备群中的其他设备所具有，此时应当中止第二设备200的对应第一账号的使用权限；

[0094] 实际实施时，在采用方式1)进行判断的基础上，还可以结合方式2)进行判断：

[0095] 2)第二设备200具有令牌信息，且令牌信息没有超出有效期限；

[0096] 在前述实施例中，服务器300向第一设备100下发的令牌信息没有有效期的限制，也就是说，令牌信息在设备群中以限制复制的方式传递时，传递的时间没有时间上的限制；实际实施时，可能需要令牌信息在一段时间内有效，当令牌信息在设备群中传递而超出有效期限时，令牌信息即失效，即使设备群中的设备具有令牌也无法获得第一账号的使用权限。

[0097] 本实施例记载的鉴权方法对前述实施例中第二设备200获取到第一账号的使用权限(也就是基于第一账号登录第一应用)之后的处理进行说明；本实施例中，设定在前述实施例中服务器300向第一设备100下发的令牌信息中还具有时限信息，例如当令牌信息中携带数字证书时，时限信息可以以数字证书的有效期来设定。

[0098] 参见图5示出的鉴权方法，包括以下步骤：

[0099] 步骤401，服务器300检测第二设备200是否具有令牌信息，如果具有，则执行步骤402；否则，执行步骤403。

[0100] 步骤402，服务器300检测第二设备200获取的第一账号的使用权限是否处于有效期，如果未超出，则返回步骤401；否则，执行步骤403。

[0101] 步骤403，服务器300中止分配给第二设备200的对应第一账号的使用权限。

[0102] 步骤404，服务器300触发第一设备100从基于第一账号登录第一应用的状态，切换为中止使用第一账号登录第一应用的状态。

[0103] 对于设备群中具有令牌信息的任意设备在基于令牌信息获取到第一账号的使用权限之后，服务器300都会检测具有第一账号的使用权限的设备是否具有令牌信息以及令牌信息是否超出有效期限的操作，实现了对令牌信息在设备群中传递的监测，确保了第一账号的使用安全。

[0104] 实施例四

[0105] 针对以下场景的处理进行说明：

[0106] 1)第一设备100和设备群中设备属于同一用户，第二设备200获取到第一账号的使用权限之后，用户需要使用第一设备100并基于第一账号来登录第一应用(此时第二设备200往往是临时用作第一应用的登录设备)。

[0107] 2)第一设备100和设备群中的设备属于不同的用户，当第一设备100用户的对应第一应用的第一账号的使用权限分配给第二设备200用户之后，第一设备100用户需要使用第一账号登录第一应用，也就是希望停止第二设备200用户在第二设备200上使用第一账号登录第一应用的行为。

[0108] 在上述两个场景中，服务器300有必要回收分配给第二设备200的对应第一账号的使用权限，以使第一设备100能够基于第一账号登录第一应用。

[0109] 参见图6示出的鉴权方法，包括以下步骤：

[0110] 步骤501，第一设备100向服务器300发送携带令牌信息的回收请求。

[0111] 回收请求中携带第一设备100从服务器请求的令牌信息，请求从设备群中具有令牌信息的设备中回收第一账号的使用权限，以使用户能够在第一设备基于第一账号登录第一应用。

[0112] 参见图7，第一设备100中止基于第一账号登录第一应用的状态时，第一应用的显示窗口处于不可操作的状态，相当于对用户的输入的操作进行了屏蔽接收，并可以提供如图8所示的回收第一应用的使用权限的虚拟按钮，当该虚拟按钮被触发时，第一设备100对应执行上述步骤501，以触发服务器300回收所分配的第一账号的使用权限，使第一设备100中第一应用的显示窗口重新处于可以操作的状态。

[0113] 步骤502，服务器300判断第一设备100是否拥有第一账号的所有权，如果使则执行步骤503；否则，停止处理。

[0114] 步骤503，中止为第二设备200分配的对应第一账号的使用权限。

[0115] 令牌信息中具有加密的标识，标识与第一账号对应，服务器300可以维护的标识与第一设备100的标识(如产品序列号，可以在向服务器300请求令牌信息时发送至服务器300，由服务器300将对应第一账号的标识、以及第一设备100标识加密形成令牌信息；也就是说，本实施例中。令牌信息中可以携带加密的以下标识：对应第一账号的标识；第一设备

100的标识。

[0116] 服务器300可以通过以下方式确定第一设备100是否具有第一账号的所有权:解密出令牌信息中的第一设备100的标识,与回收请求中携带的明文的第一设备100的标识匹配,如果匹配成功,则确定发送回收请求的设备具有第一账号的所有权。

[0117] 步骤504,服务器300触发第一设备100从中止基于第一账号登录第一应用的状态,切换为使用第一账号登录第一应用的状态。

[0118] 本实施例中通过令牌信息对发送回收请求的第一设备100进行验证,确定具有第一账号的所有权时,中止为第二设备200分配的对应第一账号的使用权限,并恢复第一设备100使用第一账号登录第一应用的状态,便于基于第一设备100使用第一应用。

[0119] 实施例五

[0120] 与前述实施例的记载相对应,本实施例还记载一种第一设备,参见图9,包括:

[0121] 获取单元110,用于基于第一设备100用户持有的对应第一应用的第一账号从服务器300获取令牌信息,令牌信息为服务器300基于第一账号生成,用于表征第一设备100用户拥有第一账号的所有权;

[0122] 第一传输单元120,用于将令牌信息在设备群的设备中以限制复制的方式进行传输,令牌信息还用于供服务器300对设备群中具有令牌信息的第二设备200进行鉴权,在鉴权通过时为第二设备200分配第一账号的使用权限,以支持第二设备200使用第一账号登录第一应用;

[0123] 切换单元130,用于确定第二设备200基于第一账号的使用权限登录第一应用,从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。

[0124] 获取单元110,还用于通过令牌信息请求从服务器300获取令牌信息,令牌信息请求用于供服务器300生成对应第一账户的标识,加密标识得到令牌信息,并维护第一账号与标识的对应关系;

[0125] 第一账号与标识的对应关系用于供服务器300从令牌信息解密出标识、并基于对应关系确定与标识对应的第一账号,分配第一账号的使用权限给第二设备200。

[0126] 获取单元110,还用于通过令牌信息请求从服务器300获取令牌信息,令牌信息请求用于供服务器300加密标识得到令牌信息;

[0127] 令牌信息和第一账号的信息还用于供第二设备200发送至服务器300,使服务器300验证第一账号与令牌信息中携带的标识是否匹配,在匹配时分配第一账号的使用权限给第二设备200。

[0128] 令牌信息中携带时限信息,用于供服务器300检测第二设备200获取的第一账号的使用权限是否处于有效期,并在超出有效期时中止分配给第二设备200的第一账号的使用权限。

[0129] 第一设备100还包括:

[0130] 回收单元140,用于向服务器300发送针对令牌信息的回收请求,回收请求中携带令牌信息,令牌信息用于供服务器300确定第一设备100用户拥有第一账号的所有权时,中止为第二设备200分配的对应第一账号的使用权限;

[0131] 切换单元130,还用于从中止使用第一账号登录第一应用的状态切换为使用第一账号登录第一应用的状态。

[0132] 令牌信息还用于供服务器300检测设备群中分配有对应第一账号的使用权限的第二设备200是否具有令牌信息，在不具有时中止为第二设备200分配的对应第一账号的使用权限。

[0133] 实际实施时，第一设备100中的各单元执行的逻辑处理功能可以由第一设备100中的处理器、微处理器(MCU)、专用集成电路(ASIC)或逻辑可编程门阵列(FPGA)实现，第一设备100中与第二设备200、以及与服务器300的通信功能可由第一设备100中的WiFi通信芯片、蜂窝通信芯片以及相应的外围电路和天线实现。

[0134] 实施例六

[0135] 与前述实施例的记载相对应，本实施例还记载一种服务器300，参见图10，包括：

[0136] 令牌单元310，用于基于第一设备100用户持有的对应第一应用的第一账号，生成对应第一账号的令牌信息，令牌信息表征第一设备100用户拥有第一账号的所有权；

[0137] 第二传输单元320，用于将令牌信息发送至第一设备100，令牌信息用于供第一设备100在设备群的设备中以限制复制的方式进行传输；

[0138] 鉴权单元330，用于基于令牌信息对设备群中具有令牌信息的第二设备200进行鉴权，在鉴权通过时为第二设备200分配第一账号的使用权限，以支持第二设备200使用第一账号登录第一应用；

[0139] 切换触发单元340，用于确定第二设备200基于第一账号的使用权限登录第一应用，触发第一设备100从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。

[0140] 令牌单元310，包括：接收模块，用于接收第一设备100发送的令牌信息请求时，生成对应第一账户的标识；加密模块，用于加密标识得到令牌信息，并维护第一账号与标识的对应关系。

[0141] 鉴权单元330包括：

[0142] 解密模块，用于从第二设备200发送的令牌信息解密出标识；

[0143] 分配单元，用于基于对应关系确定与标识对应的第一账号，分配第一账号的使用权限给第二设备200；或者，

[0144] 分配单元用于基于对应关系验证第二设备200发送的第一账号与令牌信息中携带的标识是否匹配，在匹配时分配第一账号的使用权限给第二设备200。

[0145] 令牌信息中携带时限信息；鉴权单元330还用于基于时限信息检测为第二设备200获取的第一账号的使用权限是否处于有效期；超出有效期时，中止为第二设备200分配的对应第一应用的使用权限。

[0146] 传输单元320还用于接收第一设备100发送的针对令牌信息的回收请求，回收请求中携带令牌信息；鉴权单元330，还用于基于令牌信息确定第一设备100用户拥有第一账号的所有权时，中止为第二设备200分配的对应第一账号的使用权限；切换单元，还用于触发第一设备100从中止使用第一账号登录第一应用的状态切换为使用第一账号登录第一应用的状态。

[0147] 鉴权单元330还用于检测设备群中分配有对应第一账号的使用权限的第二设备200是否具有令牌信息，在不具有令牌信息时，中止为第二设备200分配的对应第一账号的使用权限。

[0148] 实际实施时，服务器300中的各单元执行的逻辑处理功能可以由服务器300中的处理器、微处理器(MCU)、专用集成电路(ASIC)或逻辑可编程门阵列(FPGA)实现，服务器300中与第二设备200、以及与第一设备100的通信功能可由服务器300的WiFi通信芯片、蜂窝通信芯片以及相应的外围电路和天线实现。

[0149] 实施例七

[0150] 本发明实施例还记载一种图2所示的鉴权系统，包括前述的第一设备100、以及服务器300。

[0151] 实施例八

[0152] 本实施例记载一种计算机可读介质，可以为ROM(例如，只读存储器、FLASH存储器、转移装置等)、磁存储介质(例如，磁带、磁盘驱动器等)、光学存储介质(例如，CD-ROM、DVD-ROM、纸卡、纸带等)以及其他熟知类型的程序存储器；计算机可读介质中存储有计算机可执行指令(例如腾讯视频等投射应用的二进制可执行指令)，当执行指令时，引起第一设备100至少一个处理器执行包括以下的操作：

[0153] 基于第一设备100用户持有的对应第一应用的第一账号从服务器300获取令牌信息，令牌信息为服务器300基于第一账号生成，用于表征第一设备100用户拥有第一账号的所有权；

[0154] 将令牌信息在设备群的设备中以限制复制的方式进行传输，令牌信息还用于供服务器300对设备群中具有令牌信息的第二设备200进行鉴权，在鉴权通过时为第二设备200分配第一账号的使用权限，以支持第二设备200使用第一账号登录第一应用；

[0155] 确定第二设备200基于第一账号的使用权限登录第一应用，从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。

[0156] 实施例九

[0157] 本实施例记载一种计算机可读介质，可以为ROM(例如，只读存储器、FLASH存储器、转移装置等)、磁存储介质(例如，磁带、磁盘驱动器等)、光学存储介质(例如，CD-ROM、DVD-ROM、纸卡、纸带等)以及其他熟知类型的程序存储器；计算机可读介质中存储有计算机可执行指令(例如腾讯视频等投射应用的二进制可执行指令)，当执行指令时，引起服务器300至少一个处理器执行包括以下的操作：

[0158] 基于第一设备100用户持有的对应第一应用的第一账号，生成对应第一账号的令牌信息，令牌信息表征第一设备100用户拥有第一账号的所有权；

[0159] 将令牌信息发送至第一设备100，令牌信息用于供第一设备100在设备群的设备中以限制复制的方式进行传输；

[0160] 基于令牌信息对设备群中具有令牌信息的第二设备200进行鉴权，在鉴权通过时为第二设备200分配第一账号的使用权限，以支持第二设备200使用第一账号登录第一应用；

[0161] 确定第二设备200基于第一账号的使用权限登录第一应用，触发第一设备100从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态。

[0162] 综上所述，第一设备基于第一应用的第一账号获取令牌信息，将令牌信息作为设备群中的设备使用第一账号登录第一应用的鉴权凭证，在第一设备用户不必告知设备群中的设备用户与第一账号相应的密钥的前提下，即可对具有令牌信息的第二设备进行鉴权认

证，避免了第一账号的密钥泄露的风险；同时，在第二设备基于第一账号登录第一应用时，第一设备还暂停使用第一账号登录第一应用以避免第一账号的登录冲突问题。

[0163] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、随机存取存储器(RAM，Random Access Memory)、只读存储器(ROM，Read-Only Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0164] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也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，本发明实施例的技术方案本质上或者说对相关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中，包括若干指令用以使得一台计算机设备(可以是个人计算机、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。而前述的存储介质包括：移动存储设备、RAM、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0165] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

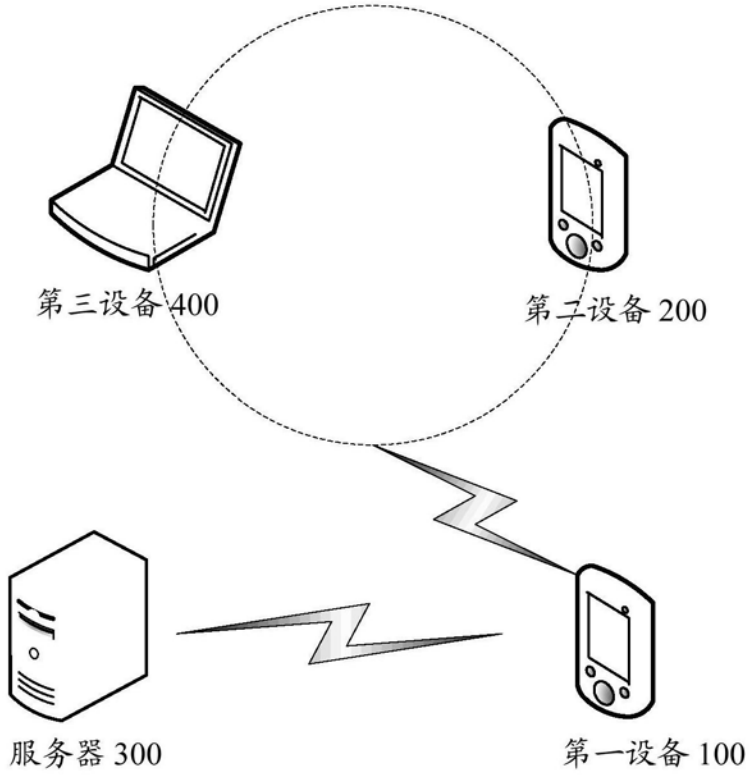

第三设备 400
第二设备 200
服务器 300
第一设备 100

图1

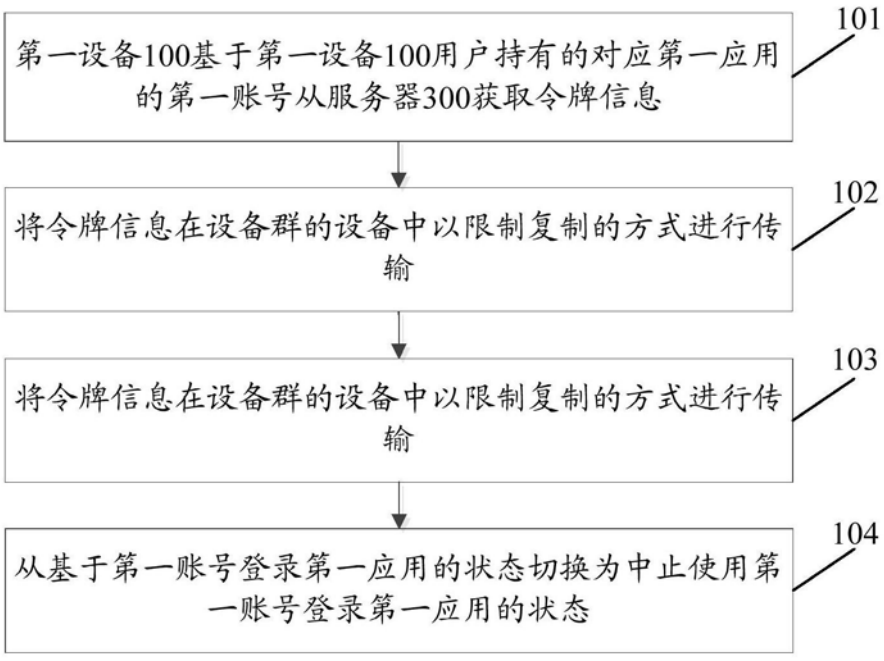

第一设备100基于第一设备100用户持有的对应第一应用的第一账号从服务器300获取令牌信息
101
将令牌信息在设备群的设备中以限制复制的方式进行传输
102
将令牌信息在设备群的设备中以限制复制的方式进行传输
103
从基于第一账号登录第一应用的状态切换为中止使用第一账号登录第一应用的状态
104

图2

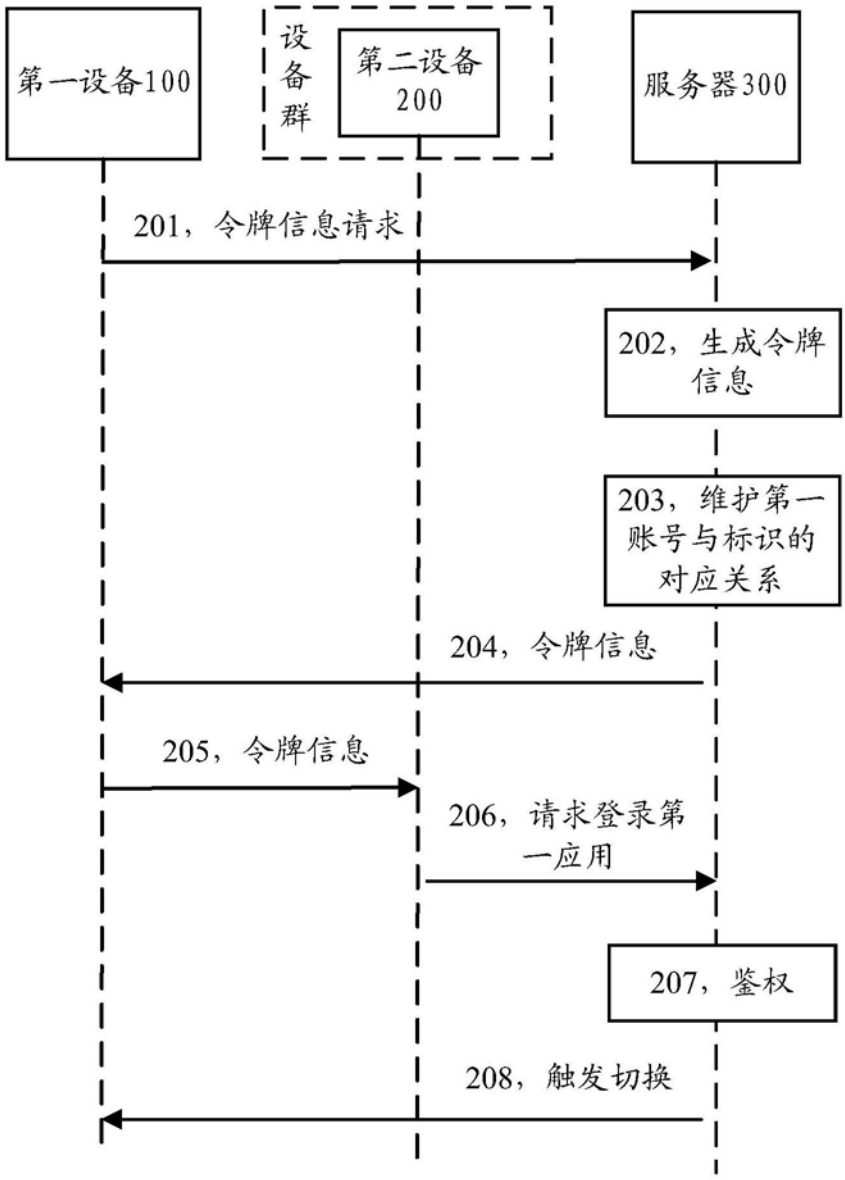

第一设备100
设备群
第二设备200
服务器300
201，令牌信息请求
202，生成令牌信息
203，维护第一账号与标识的对应关系
204，令牌信息
205，令牌信息
206，请求登录第一应用
207，鉴权
208，触发切换

图3

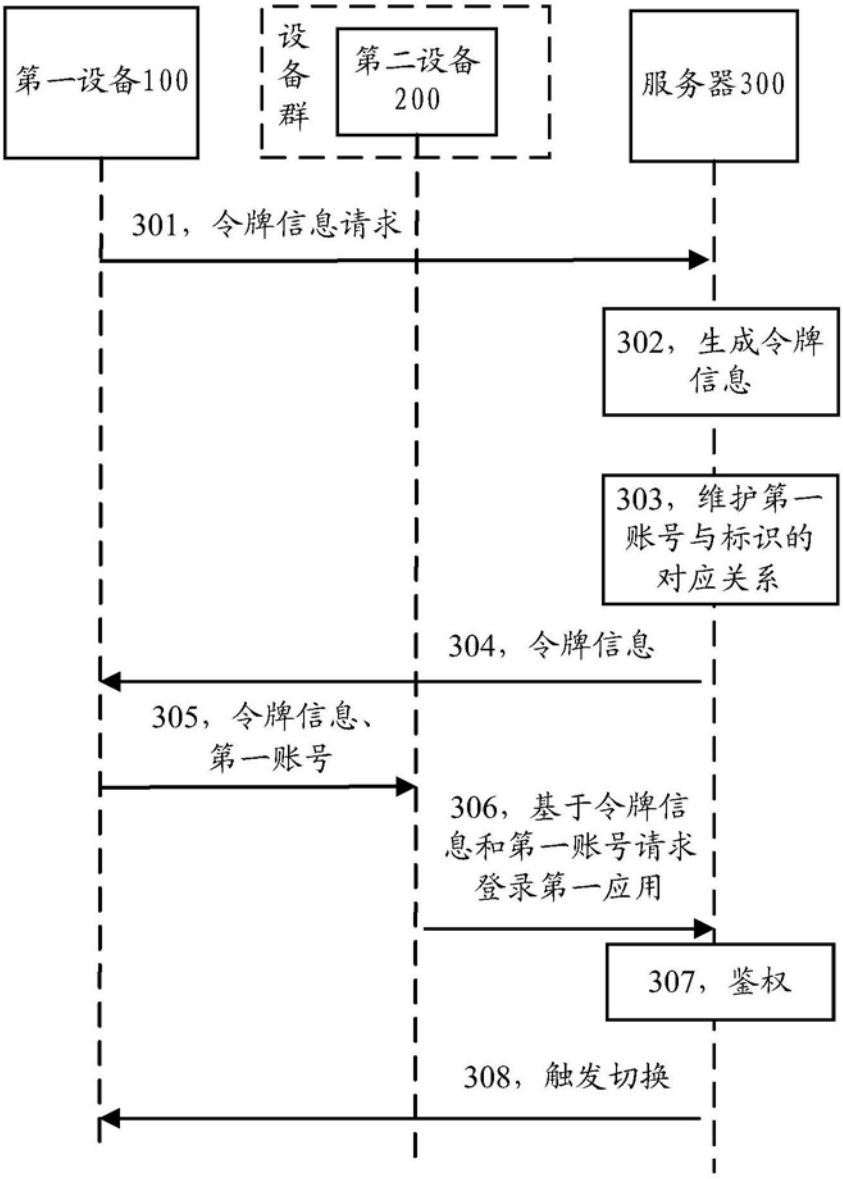

第一设备100
设备群
第二设备200
服务器300
301，令牌信息请求
302，生成令牌信息
303，维护第一账号与标识的对应关系
304，令牌信息
305，令牌信息、第一账号
306，基于令牌信息和第一账号请求登录第一应用
307，鉴权
308，触发切换

图4

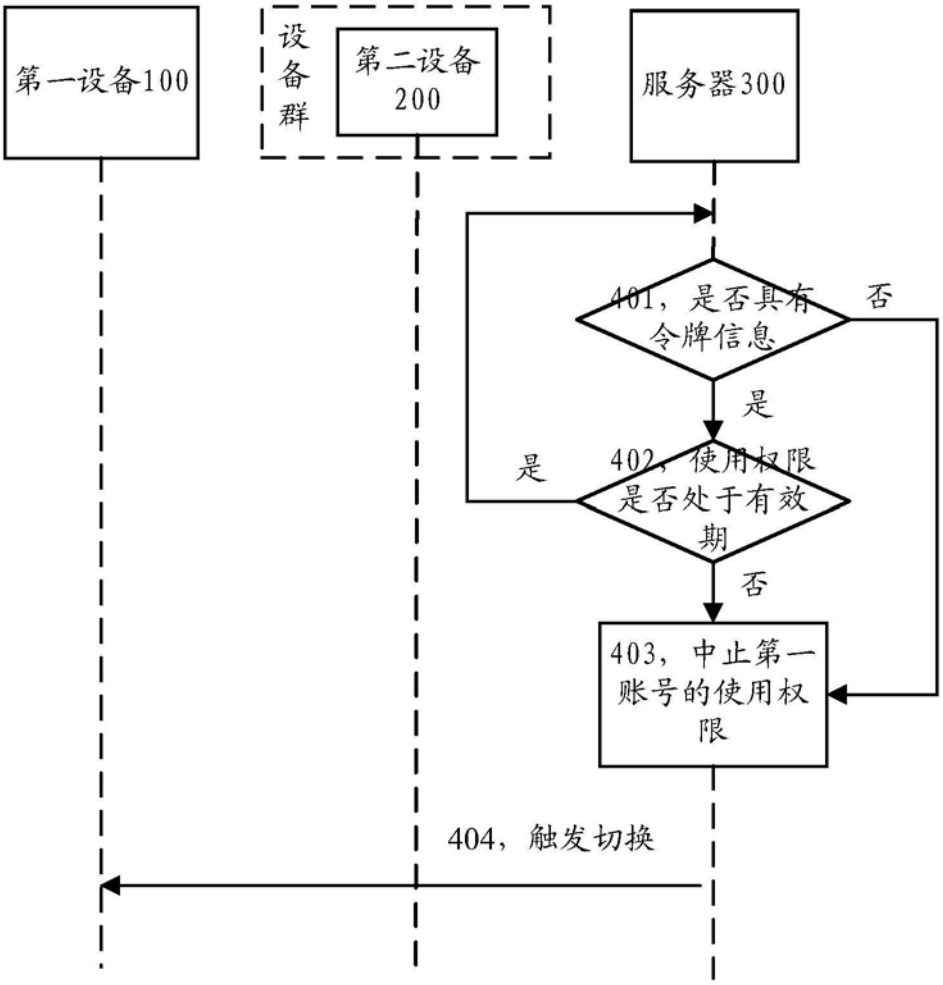

第一设备100
设备群
第二设备200
服务器300
401，是否具有令牌信息
否
是
402，使用权限是否处于有效期
是
否
403，中止第一账号的使用权限
404，触发切换

图5

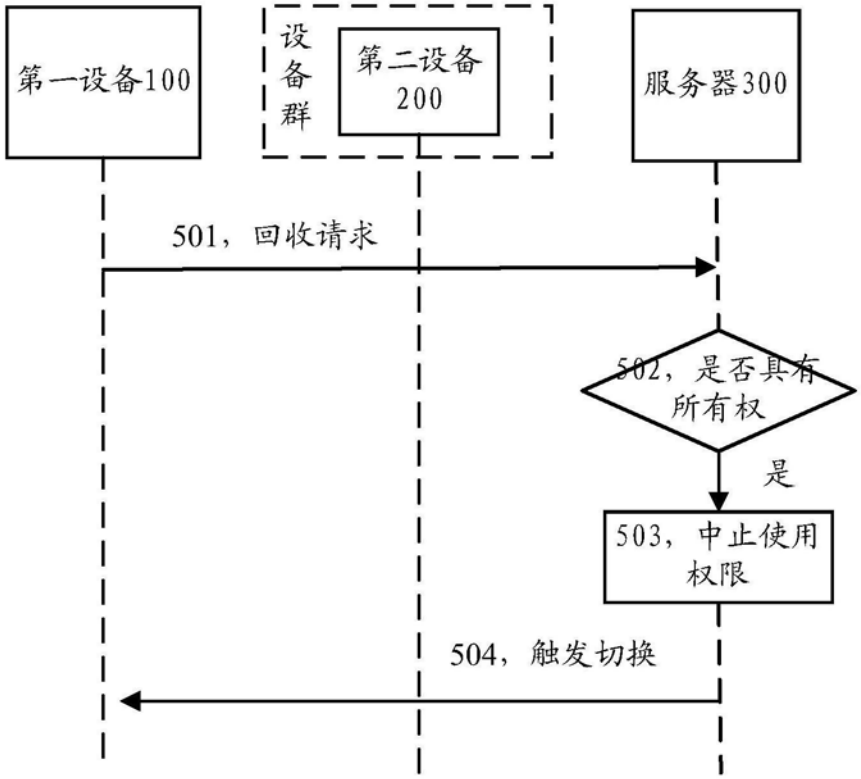

第一设备100
设备群
第二设备200
服务器300
501，回收请求
502，是否具有所有权
是
503，中止使用权限
504，触发切换

图6

图7

图8

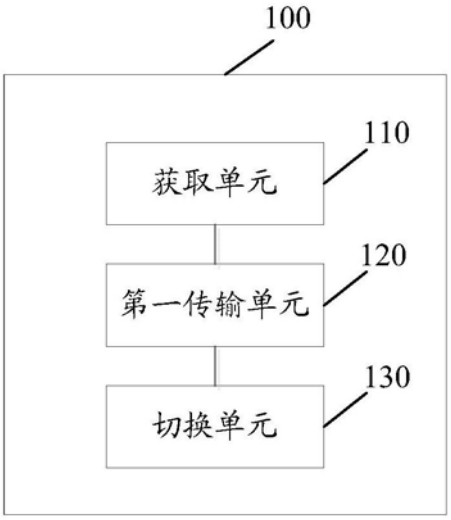


图9

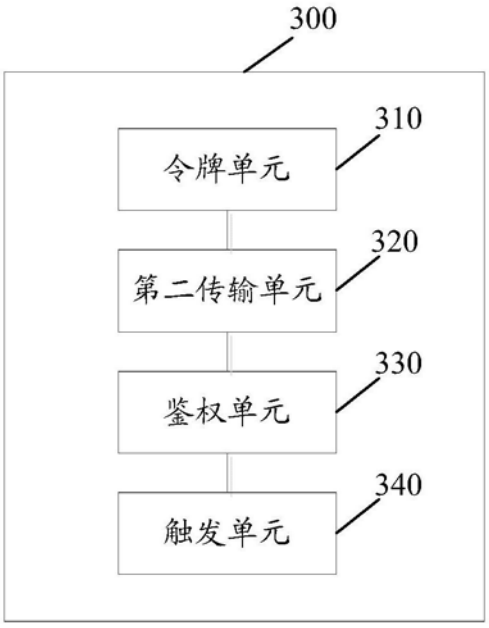


图10