



(12)发明专利申请

(10)申请公布号 CN 107342966 A

(43)申请公布日 2017.11.10

(21)申请号 201610285293.1

(22)申请日 2016.04.29

(71)申请人 北京京东尚科信息技术有限公司

地址 100080 北京市海淀区杏石口路65号
西杉创意园西区11C楼东段1-4层西段
1-4层

申请人 北京京东世纪贸易有限公司

(72)发明人 刘姗

(74)专利代理机构 北京英赛嘉华知识产权代理
有限责任公司 11204

代理人 王达佐 马晓亚

(51)Int.Cl.

H04L 29/06(2006.01)

H04L 9/06(2006.01)

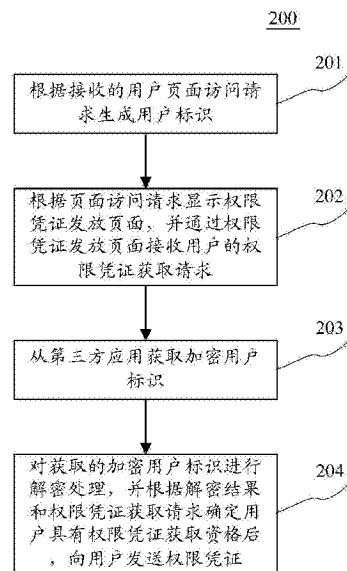
权利要求书2页 说明书9页 附图4页

(54)发明名称

权限凭证发放方法和装置

(57)摘要

本申请公开了权限凭证发放方法和装置。所述方法的具体实施方式包括：根据接收的用户页面访问请求生成用户标识，其中，所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的；根据所述页面访问请求显示权限凭证发放页面，并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求；从所述第三方应用获取加密用户标识，其中，所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的；对获取的加密用户标识进行解密处理，并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后，向所述用户发送权限凭证。该实施方式实现了权限凭证的安全发放。



1. 一种权限凭证发放方法,其特征在于,所述方法包括:

根据接收的用户页面访问请求生成用户标识,其中,所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的;

根据所述页面访问请求显示权限凭证发放页面,并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求;

从所述第三方应用获取加密用户标识,其中,所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的;

对获取的加密用户标识进行解密处理,并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后,向所述用户发送权限凭证。

2. 根据权利要求1所述的方法,其特征在于,所述方法还包括:

接收所述用户的页面分享请求,其中,所述页面分享请求包括目标用户的信息;

根据所述页面分享请求以及所述加密用户标识生成用于使目标用户获取权限凭证的分享链接;

并将所述分享链接发送给目标用户。

3. 根据权利要求2所述的方法,其特征在于,所述方法还包括:

统计所述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。

4. 根据权利要求1所述的方法,其特征在于,所述加密用户标识通过以下步骤生成:

使用通过RSA加密算法得到的加密对中的公钥对所述用户标识进行加密处理,生成加密用户标识。

5. 根据权利要求4所述的方法,其特征在于,所述对获取的加密用户标识进行解密处理,包括:

使用所述加密对中的私钥对获取的加密用户标识进行解密处理,得到解密后的用户标识。

6. 根据权利要求1所述的方法,其特征在于,所述权限凭证获取请求包括所述用户的IP地址;以及

所述根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格,包括:

确定所述用户的IP地址未包含在预先设定的IP地址灰名单中;

确定对所述加密用户标识解密处理后得到的用户标识未包含在预先设定的用户标识灰名单中;

确定对所述加密用户标识解密处理后得到的用户标识的领取次数没有超过预先设定的用户标识领取次数阈值;

对所述加密用户标识解密处理后得到的用户标识进行格式校验,如果校验通过,则确定所述用户具有权限凭证获取资格。

7. 根据权利要求6所述的方法,其特征在于,所述IP地址灰名单通过以下方式进行设置:

根据所述用户的IP地址判断所述用户对所述权限凭证发放页面的访问次数是否超过预先设定的IP地址访问次数阈值;

如果超过，则将所述用户的IP地址写入所述IP地址灰名单，其中，所述IP地址灰名单中的IP地址在设定时长内被禁止用于获取权限凭证。

8.根据权利要求6所述的方法，其特征在于，所述用户标识灰名单通过以下方式进行设置：

统计所述用户点击所述超链接与发送所述权限凭证获取请求之间的时间间隔小于预先设定的时间间隔阈值的次数；

如果统计得到的次数超过预先设定的次数阈值，则将解密处理后得到的用户标识写入所述用户标识灰名单，其中，所述用户标识灰名单中的用户标识在设定时长内被禁止用于获取权限凭证。

9.根据权利要求1所述的方法，其特征在于，所述权限凭证获取请求包括手机号码；以及

在所述向所述用户发送权限凭证之前，所述方法还包括：

确定所述用户输入的验证信息正确，其中，所述验证信息是通过图片或者短信的形式发送给所述用户的。

10.一种权限凭证发放装置，其特征在于，所述装置包括：

生成单元，用于根据接收的用户页面访问请求生成用户标识，其中，所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的；

显示和接收单元，用于根据所述页面访问请求显示权限凭证发放页面，并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求；

获取单元，用于从所述第三方应用获取加密用户标识，其中，所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的；

发放单元，用于对获取的加密用户标识进行解密处理，并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后，向所述用户发送权限凭证。

11.根据权利要求10所述的装置，其特征在于，所述装置还包括分享单元，所述分享单元用于：

接收所述用户的页面分享请求，其中，所述页面分享请求包括目标用户的信息；

根据所述页面分享请求以及所述加密用户标识生成用于使目标用户获取权限凭证的分享链接；

并将所述分享链接发送给目标用户。

12.根据权利要求11所述的装置，其特征在于，所述装置还包括：

统计单元，用于统计所述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。

权限凭证发放方法和装置

技术领域

[0001] 本申请涉及计算机技术领域,具体涉及互联网技术领域,尤其涉及权限凭证发放方法和装置。

背景技术

[0002] 互联网技术的快速发展和终端设备的日益普及给人们的生活带来了极大的便利,例如,用户可以通过购物网站足不出户的购买到所需商品。在使用互联网的过程中,如果用户想要获取某些特殊的权限,往往需要具有针对该权限的电子权限凭证。例如,用户在某购物网站购买商品时想要获得价格优惠的权限,则需要具有该购物网站提供的优惠券。

[0003] 现有技术中,权限凭证发放者(例如购物网站)可以直接向用户发放权限凭证,也可以通过第三方应用向用户发放权限凭证。在通过第三方应用发放权限凭证时,往往存在较大的安全隐患,易发生不法之徒恶意领取事件(例如黑客模拟正常用户大量领取权限凭证)。

发明内容

[0004] 本申请的目的在于提出一种改进的权限凭证发放方法和装置,来解决以上背景技术部分提到的技术问题。

[0005] 第一方面,本申请提供了一种权限凭证发放方法,所述方法包括:根据接收的用户页面访问请求生成用户标识,其中,所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的;根据所述页面访问请求显示权限凭证发放页面,并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求;从所述第三方应用获取加密用户标识,其中,所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的;对获取的加密用户标识进行解密处理,并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后,向所述用户发送权限凭证。

[0006] 在一些实施例中,所述方法还包括:接收所述用户的页面分享请求,其中,所述页面分享请求包括目标用户的信息;根据所述页面分享请求以及所述加密用户标识生成用于使目标用户获取权限凭证的分享链接;并将所述分享链接发送给目标用户。

[0007] 在一些实施例中,所述方法还包括:统计所述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。

[0008] 在一些实施例中,所述加密用户标识通过以下步骤生成:使用通过RSA加密算法得到的加密对中的公钥对所述用户标识进行加密处理,生成加密用户标识。

[0009] 在一些实施例中,所述对获取的加密用户标识进行解密处理,包括:使用所述加密对中的私钥对获取的加密用户标识进行解密处理,得到解密后的用户标识。

[0010] 在一些实施例中,所述权限凭证获取请求包括所述用户的IP地址;以及所述根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格,包括:确定所述用户的IP地址未包含在预先设定的IP地址灰名单中;确定对所述加密用户标识解密处理后

得到的用户标识未包含在预先设定的用户标识灰名单中；确定对所述加密用户标识解密处理后得到的用户标识的领取次数没有超过预先设定的用户标识领取次数阈值；对所述加密用户标识解密处理后得到的用户标识进行格式校验，如果校验通过，则确定所述用户具有权限凭证获取资格。

[0011] 在一些实施例中，所述IP地址灰名单通过以下方式进行设置：根据所述用户的IP地址判断所述用户对所述权限凭证发放页面的访问次数是否超过预先设定的IP地址访问次数阈值；如果超过，则将所述用户的IP地址写入所述IP地址灰名单，其中，所述IP地址灰名单中的IP地址在设定时长内被禁止用于获取权限凭证。

[0012] 在一些实施例中，所述用户标识灰名单通过以下方式进行设置：统计所述用户点击所述超链接与发送所述权限凭证获取请求之间的时间间隔小于预先设定的时间间隔阈值的次数；如果统计得到的次数超过预先设定的次数阈值，则将解密处理后得到的用户标识写入所述用户标识灰名单，其中，所述用户标识灰名单中的用户标识在设定时长内被禁止用于获取权限凭证。

[0013] 在一些实施例中，所述权限凭证获取请求包括手机号码；以及在所述向所述用户发送权限凭证之前，所述方法还包括：确定所述用户输入的验证信息正确，其中，所述验证信息是通过图片或者短信的形式发送给所述用户的。

[0014] 第二方面，本申请提供了一种权限凭证发放装置，所述装置包括：生成单元，用于根据接收的用户页面访问请求生成用户标识，其中，所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的；显示和接收单元，用于根据所述页面访问请求显示权限凭证发放页面，并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求；获取单元，用于从所述第三方应用获取加密用户标识，其中，所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的；发放单元，用于对获取的加密用户标识进行解密处理，并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后，向所述用户发送权限凭证。

[0015] 在一些实施例中，所述装置还包括分享单元，所述分享单元用于：接收所述用户的页面分享请求，其中，所述页面分享请求包括目标用户的信息；根据所述页面分享请求以及所述加密用户标识生成用于使目标用户获取权限凭证的分享链接；并将所述分享链接发送给目标用户。

[0016] 在一些实施例中，所述装置还包括：统计单元，用于统计所述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。

[0017] 在一些实施例中，所述装置还包括：加密用户标识生成单元，用于使用通过RSA加密算法得到的加密对中的公钥对所述用户标识进行加密处理，生成加密用户标识。

[0018] 在一些实施例中，所述发放单元进一步用于：使用所述加密对中的私钥对获取的加密用户标识进行解密处理，得到解密后的用户标识。

[0019] 在一些实施例中，所述权限凭证获取请求包括所述用户的IP地址；以及所述发放单元进一步用于：确定所述用户的IP地址未包含在预先设定的IP地址灰名单中；确定对所述加密用户标识解密处理后得到的用户标识未包含在预先设定的用户标识灰名单中；确定对所述加密用户标识解密处理后得到的用户标识的领取次数没有超过预先设定的用户标识领取次数阈值；对所述加密用户标识解密处理后得到的用户标识进行格式校验，如果校

验通过，则确定所述用户具有权限凭证获取资格。

[0020] 在一些实施例中，所述装置还包括IP地址灰名单设置单元，所述IP地址灰名单设置单元用于：IP地址灰名单设置单元，用于根据所述用户的IP地址判断所述用户对所述权限凭证发放页面的访问次数是否超过预先设定的IP地址访问次数阈值；如果超过，则将所述用户的IP地址写入所述IP地址灰名单，其中，所述IP地址灰名单中的IP地址在设定时长内被禁止用于获取权限凭证。

[0021] 在一些实施例中，所述装置还包括用户标识灰名单设置单元，所述用户标识灰名单设置单元用于：统计所述用户点击所述超链接与发送所述权限凭证获取请求之间的时间间隔小于预先设定的时间间隔阈值的次数；如果统计得到的次数超过预先设定的次数阈值，则将解密处理后得到的用户标识写入所述用户标识灰名单，其中，所述用户标识灰名单中的用户标识在设定时长内被禁止用于获取权限凭证。

[0022] 在一些实施例中，所述权限凭证获取请求包括手机号码；以及所述装置还包括：确定单元，用于确定所述用户输入的验证信息正确，其中，所述验证信息是通过图片或者短信的形式发送给所述用户的。

[0023] 本申请提供的权限凭证发放方法和装置，根据用户通过第三方应用输入的页面访问请求显示权限凭证发放页面，之后通过该权限凭证发放页面接收用户的权限凭证获取请求，并从该第三方应用获取加密用户标识，而后对该加密用户标识进行解密处理，并根据解密结果和权限凭证获取请求确定该用户具有权限凭证领取资格之后在向该用户发送权限凭证，从而提高权限凭证发放的安全性。

附图说明

[0024] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0025] 图1是本申请可以应用于其中的示例性系统架构图；

[0026] 图2是根据本申请的权限凭证发放方法的一个实施例的流程图；

[0027] 图3是根据本申请的权限凭证发放方法的一个应用场景的示意图；

[0028] 图4是根据本申请的权限凭证发放装置的一个实施例的结构示意图；

[0029] 图5是适于用来实现本申请实施例的终端设备或服务器的计算机系统的结构示意图。

具体实施方式

[0030] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0031] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0032] 图1示出了可以应用本申请的权限凭证发放方法或权限凭证发放装置的实施例的示例性系统架构100。

[0033] 如图1所示，系统架构100可以包括终端设备101、102、103，网络104和服务器105。

网络104用以在终端设备101、102、103和服务器105之间提供通信链路的介质。网络104可以包括各种连接类型,例如有线、无线通信链路或者光纤电缆等等。

[0034] 用户可以使用终端设备101、102、103通过网络104与服务器105交互,以接收或发送消息等。终端设备101、102、103上可以安装有各种通讯客户端应用,例如网页浏览器应用、购物类应用、搜索类应用、即时通信工具、邮箱客户端、社交平台软件等。

[0035] 终端设备101、102、103可以是具有显示屏并且支持网页浏览的各种电子设备,包括但不限于智能手机、平板电脑、电子书阅读器、MP3播放器(Moving Picture Experts Group Audio Layer III,动态影像专家压缩标准音频层面3)、MP4(Moving Picture Experts Group Audio Layer IV,动态影像专家压缩标准音频层面4)播放器、膝上型便携计算机和台式计算机等等。

[0036] 服务器105可以是提供各种服务的服务器,例如对终端设备101、102、103上显示的网页提供支持的后台网页服务器。后台网页服务器可以对接收到的页面访问请求等数据进行分析等处理,并将处理结果(例如网页页面数据)反馈给终端设备。

[0037] 需要说明的是,本申请实施例所提供的权限凭证发放方法一般由服务器105执行,相应地,权限凭证发放装置一般设置于服务器105中。

[0038] 应该理解,图1中的终端设备、网络和服务器的数目仅仅是示意性的。根据实现需要,可以具有任意数目的终端设备、网络和服务器。

[0039] 继续参考图2,示出了根据本申请的权限凭证发放方法的一个实施例的流程200。所述的权限凭证发放方法,包括以下步骤:

[0040] 步骤201,根据接收的用户页面访问请求生成用户标识。

[0041] 在本实施例中,权限凭证发放方法运行于其上的电子设备(例如图1所示的服务器105)可以通过有线连接方式或者无线连接方式从用户所使用的终端接收页面访问请求,在这里上述电子设备可以是为权限凭证发放者提供各种服务的服务器,例如,当上述权限凭证发放者为购物网站时,上述服务器可以是为该购物网站提供服务的服务器,它可以指一台服务器,也可以指一个服务器集群。在本实施例中,上述页面访问请求可以是用户通过点击第三方应用中预先设定的超链接发送的,其中,上述第三方应用指的是与权限凭证发放者不同的应用,例如,当上述权限凭证发放者为购物网站或购物APP(Application,应用程序)时,上述第三方应用可以是不同于上述购物网站或购物APP的各种应用,如购物类应用、聊天类应用、网页浏览器应用等等。上述电子设备在接收到上述页面访问请求之后,可以根据该页面访问请求生成一个唯一的用户标识,该用户标识可以是各种形式的用户标识,例如,可以是一个随机生成的16位数字或者字母的字符串。需要指出的是,上述无线连接方式可以包括但不限于3G/4G连接、WiFi连接、蓝牙连接、WiMAX连接、Zigbee连接、UWB(ultra wideband)连接、以及其他现在已知或将来开发的无线连接方式。

[0042] 通常,权限凭证发放者(例如购物网站)在与第三方应用合作发放权限凭证(例如优惠券)时,会为第三方应用提供一个页面的超链接,用户可以通过点击第三方应用中的该超链接向权限凭证发放者的服务器发送页面访问请求。

[0043] 步骤202,根据页面访问请求显示权限凭证发放页面,并通过权限凭证发放页面接收用户的权限凭证获取请求。

[0044] 在本实施例中,上述电子设备可以根据步骤201中接收的页面访问请求显示权限

凭证发放页面，并通过该权限凭证发放页面接收用户输入的权限凭证获取请求。在这里，权限凭证可以是用来证明用户具有某种权限的凭证，比如，购物网站的优惠券可以是用来证明用户在该购物网站具有享受优惠价格权限的凭证。

[0045] 步骤203，从第三方应用获取加密用户标识。

[0046] 在本实施例中，上述电子设备可以从上述第三方应用中获取加密用户标识，其中，上述加密用户标识可以是上述电子设备将步骤201中生成的用户标识采用加密算法进行加密后生成的，其中，上述加密算法可以是各种加密算法，例如高级加密标准(AES, Advanced Encryption Standard), DES(Data Encryption Algorithm, 数据加密算法)等等。上述电子设备可以将加密后生成的加密用户标识发送给上述第三方应用由该第三方应用预先进行存储的。在这里，上述第三方应用可以将上述加密用户标识存储在内嵌浏览器的Cookie中。

[0047] 在本实施例的一些可选的实现方式中，上述加密用户标识可以通过以下步骤生成：使用通过RSA加密算法得到的加密对中的公钥对所述用户标识进行加密处理，生成加密用户标识。RSA加密算法是一种公钥加密算法，它通常先生成一对RSA密钥，其中之一是保密密钥(即私钥)；另一个为公开密钥(即公钥)，可对外公开。上述电子设备可以使用加密对中的公钥对上述用户标识进行加密，加密后生成的加密用户标识只有使用上述加密对中的私钥才能进行解密。

[0048] 步骤204，对获取的加密用户标识进行解密处理，并根据解密结果和权限凭证获取请求确定用户具有权限凭证获取资格后，向用户发送权限凭证。

[0049] 在本实施例中，上述电子设备可以将步骤204中获取的加密用户标识进行解密处理，解密处理之后可以得到用户标识，上述电子设备可以对解密得到的用户标识进行校验，例如长度校验、格式校验等等，并根据校验结果判断该用户是否合法。上述电子设备还可以根据步骤202中接收的权限凭证获取请求判断上述用户是否具有权限凭证获取资格，如果确定该用户具有获取资格，则向该用户发送权限凭证。

[0050] 在本实施例的一些可选的实现方式中，上述对获取的加密用户标识进行解密处理，包括：上述电子设备使用上述加密对中的私钥对获取的加密用户标识进行解密处理，得到解密后的用户标识。

[0051] 在本实施例的一些可选的实现方式中，上述权限凭证获取请求包括上述用户的IP地址；以及上述根据解密结果和上述权限凭证获取请求确定所述用户具有权限凭证获取资格，包括：首先，上述电子设备可以将上述权限凭证获取请求中包括的上述用户的IP地址与预先设定的IP地址灰名单中的IP地址进行对比，确定上述用户的IP地址未包含在预先设定的IP地址灰名单中；其次，上述电子设备可以将对上述加密用户标识解密处理后得到的用户标识与预先设定的用户标识灰名单中的用户标识进行对比，确定对上述加密用户标识解密处理后得到的用户标识未包含在预先设定的用户标识灰名单中；然后，上述电子设备可以确定对上述加密用户标识解密处理后得到的用户标识的领取次数没有超过预先设定的用户标识领取次数阈值；最后，上述电子设备可以将对上述加密用户标识解密处理后得到的用户标识进行格式校验，如果校验通过，则确定该用户具有权限凭证获取资格。

[0052] 可选的，上述IP地址灰名单通过以下方式进行设置：上述电子设备可以根据上述用户的IP地址判断上述用户对上述权限凭证发放页面的访问次数是否超过预先设定的IP地址访问次数阈值；如果超过，则上述电子设备将上述用户的IP地址写入上述IP地址灰名

单,其中,上述IP地址灰名单中的IP地址在设定时长内(例如5分钟内)被禁止用于获取权限凭证。

[0053] 可选的,上述用户标识灰名单通过以下方式进行设置:上述电子设备可以统计上述用户点击上述超链接与发送上述权限凭证获取请求之间的时间间隔小于预先设定的时间间隔阈值的次数;如果统计得到的次数超过预先设定的次数阈值,则上述电子设备可以将解密处理后得到的用户标识写入上述用户标识灰名单,其中,上述用户标识灰名单中的用户标识在设定时长内(例如5分钟内)被禁止用于获取权限凭证。

[0054] 在本实施例的一些可选的实现方式中,上述权限凭证获取请求包括手机号码;以及在向上述用户发送权限凭证之前,上述方法还可以包括:上述电子设备可以接收用户输入的验证信息,并确定上述用户输入的验证信息正确,其中,上述验证信息是通过图片或者短信的形式发送给上述用户的。例如,在上述电子设备接收到包括手机号码的权限凭证获取请求之后,上述电子设备可以向该手机号码发送包括验证信息的短信,该验证信息可以为各种形式的信息,例如包含字母和/或数字的字符串,用户接收到短信之后,可以将短信中包含的验证信息输入到终端,以便上述电子设备进行接收和验证。

[0055] 在本实施例的一些可选的实现方式中,上述电子设备还可以接收上述用户的页面分享请求,其中,上述页面分享请求包括目标用户的信息,例如目标用户的用户名、昵称、账号等等;然后,上述电子设备可以根据上述页面分享请求以及上述加密用户标识生成用于使目标用户获取权限凭证的分享链接,例如,上述电子设备可以将上述用户的用户标识进行加密后拼接到上述超链接中,从而生成分享链接;最后,上述电子设备可以将所述分享链接发送给目标用户。目标用户通过点击上述分享链接可以访问上述权限凭证发放页面。

[0056] 可选的,上述电子设备还可以统计上述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。

[0057] 继续参见图3,图3是根据本实施例的权限凭证发放方法的应用场景的一个示意图。在图3的应用场景中,用户首先通过点击聊天类应用中的预先设定的超链接向购物网站的服务器发起一个页面访问请求;之后,该服务器根据接收到的页面访问请求通过用户所使用的终端设备向用户显示优惠券发放页面,如图3显示的页面,用户可以通过文本框301输入手机号码,并通过点击按钮302向上述服务器发送优惠券获取请求;然后,上述服务器可以从上述聊天类应用的内嵌浏览器Cookie中获取加密用户标识;最后,上述服务器对获取的加密用户标识进行解密处理,并根据解密结果和上述优惠券获取请求确定该用户具有优惠券获取资格后,向该用户发送优惠券。

[0058] 本申请的上述实施例提供的方法通过对加密用户标识和权限凭证获取请求包括的信息的验证判断用户是否具有权限凭证获取资格,从而保证了权限凭证发放的安全性。

[0059] 进一步参考图4,作为对上述各图所示方法的实现,本申请提供了一种权限凭证发放装置的一个实施例,该装置实施例与图2所示的方法实施例相对应,该装置具体可以应用于各种电子设备中。

[0060] 如图4所示,本实施例所述的权限凭证发放装置400包括:生成单元401、显示和接收单元402、获取单元403和发放单元404。其中,生成单元401用于根据接收的用户页面访问请求生成用户标识,其中,上述页面访问请求是上述用户通过点击第三方应用中预设的超链接发送的;显示和接收单元402用于根据上述页面访问请求显示权限凭证发放页面,并通

过上述权限凭证发放页面接收上述用户的权限凭证获取请求；获取单元403用于从上述第三方应用获取加密用户标识，其中，上述加密用户标识是将上述用户标识进行加密后生成并发送给上述第三方应用由上述第三方应用进行存储的；发放单元404用于对获取的加密用户标识进行解密处理，并根据解密结果和上述权限凭证获取请求确定上述用户具有权限凭证获取资格后，向上述用户发送权限凭证。

[0061] 在本实施例中，生成单元401、显示和接收单元402、获取单元403和发放单元404的具体处理可以参考图2对应实施例步骤201、步骤202和步骤203的详细描述，在此不再赘述。

[0062] 在本实施例的一些可选的实现方式中，上述装置还包括分享单元（未示出），上述分享单元用于：接收上述用户的页面分享请求，其中，上述页面分享请求包括目标用户的信息；根据上述页面分享请求以及上述加密用户标识生成用于使目标用户获取权限凭证的分享链接；并将上述分享链接发送给目标用户。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0063] 可选的，上述装置还包括：统计单元（未示出），用于统计上述用户的分享次数、分享链接被目标用户打开的次数、以及向目标用户发送权限凭证的次数。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0064] 在本实施例的一些可选的实现方式中，上述装置还包括：加密用户标识生成单元（未示出），用于使用通过RSA加密算法得到的加密对中的公钥对上述用户标识进行加密处理，生成加密用户标识。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0065] 在本实施例的一些可选的实现方式中，上述发放单元404进一步用于：使用上述加密对中的私钥对获取的加密用户标识进行解密处理，得到解密后的用户标识。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0066] 在本实施例的一些可选的实现方式中，上述权限凭证获取请求包括上述用户的IP地址；以及上述发放单元404进一步用于：确定上述用户的IP地址未包含在预先设定的IP地址灰名单中；确定对上述加密用户标识解密处理后得到的用户标识未包含在预先设定的用户标识灰名单中；确定对上述加密用户标识解密处理后得到的用户标识的领取次数没有超过预先设定的用户标识领取次数阈值；对上述加密用户标识解密处理后得到的用户标识进行格式校验，如果校验通过，则确定上述用户具有权限凭证获取资格。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0067] 在本实施例的一些可选的实现方式中，上述装置还包括IP地址灰名单设置单元（未示出），上述IP地址灰名单设置单元用于：根据上述用户的IP地址判断上述用户对上述权限凭证发放页面的访问次数是否超过预先设定的IP地址访问次数阈值；如果超过，则将上述用户的IP地址写入上述IP地址灰名单，其中，上述IP地址灰名单中的IP地址在设定时长内被禁止用于获取权限凭证。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述，在此不再赘述。

[0068] 在本实施例的一些可选的实现方式中，上述装置还包括用户标识灰名单设置单元（未示出），上述用户标识灰名单设置单元用于：统计上述用户点击上述超链接与发送上述权限凭证获取请求之间的时间间隔小于预先设定的时间间隔阈值的次数；如果统计得到的次数超过预先设定的次数阈值，则将解密处理后得到的用户标识写入上述用户标识灰名

单,其中,上述用户标识灰名单中的用户标识在设定时长内被禁止用于获取权限凭证。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述,在此不再赘述。

[0069] 在本实施例的一些可选的实现方式中,上述权限凭证获取请求包括手机号码;以及上述装置还包括:确定单元(未示出),用于确定上述用户输入的验证信息正确,其中,上述验证信息是通过图片或者短信的形式发送给上述用户的。该实现方式可参考上述图2对应实施例中相应实现方式的详细描述,在此不再赘述。

[0070] 下面参考图5,其示出了适于用来实现本申请实施例的终端设备或服务器的计算机系统500的结构示意图。

[0071] 如图5所示,计算机系统500包括中央处理单元(CPU)501,其可以根据存储在只读存储器(ROM)502中的程序或者从存储部分508加载到随机访问存储器(RAM)503中的程序而执行各种适当的动作和处理。在RAM 503中,还存储有系统500操作所需的各种程序和数据。CPU 501、ROM 502以及RAM 503通过总线504彼此相连。输入/输出(I/O)接口505也连接至总线504。

[0072] 以下部件连接至I/O接口505:包括键盘、鼠标等的输入部分506;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分507;包括硬盘等的存储部分508;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分509。通信部分509经由诸如因特网的网络执行通信处理。驱动器510也需要连接至I/O接口505。可拆卸介质511,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器510上,以便于从其上读出的计算机程序根据需要被安装入存储部分508。

[0073] 特别地,根据本公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,所述计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分509从网络上被下载和安装,和/或从可拆卸介质511被安装。在该计算机程序被中央处理单元(CPU)501执行时,执行本申请的方法中限定的上述功能。

[0074] 附图中的流程图和框图,图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0075] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中,例如,可以描述为:一种处理器包括生成单元、显示和接收单元、获取单元和发放单元。其中,这些单元的名称在某种情况下并不构成对该单元本身的限定,例如,生成单元还可以被描述为“根据接收的用户页面访问请求生成用户标识的单元”。

[0076] 作为另一方面,本申请还提供了一种非易失性计算机存储介质,该非易失性计算机存储介质可以是上述实施例中所述装置中所包含的非易失性计算机存储介质;也可以是单独存在,未装配入终端中的非易失性计算机存储介质。上述非易失性计算机存储介质存储有一个或者多个程序,当所述一个或者多个程序被一个设备执行时,使得所述设备:根据接收的用户页面访问请求生成用户标识,其中,所述页面访问请求是所述用户通过点击第三方应用中预设的超链接发送的;根据所述页面访问请求显示权限凭证发放页面,并通过所述权限凭证发放页面接收所述用户的权限凭证获取请求;从所述第三方应用获取加密用户标识,其中,所述加密用户标识是将所述用户标识进行加密后生成并发送给所述第三方应用由所述第三方应用进行存储的;对获取的加密用户标识进行解密处理,并根据解密结果和所述权限凭证获取请求确定所述用户具有权限凭证获取资格后,向所述用户发送权限凭证。

[0077] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离所述发明构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

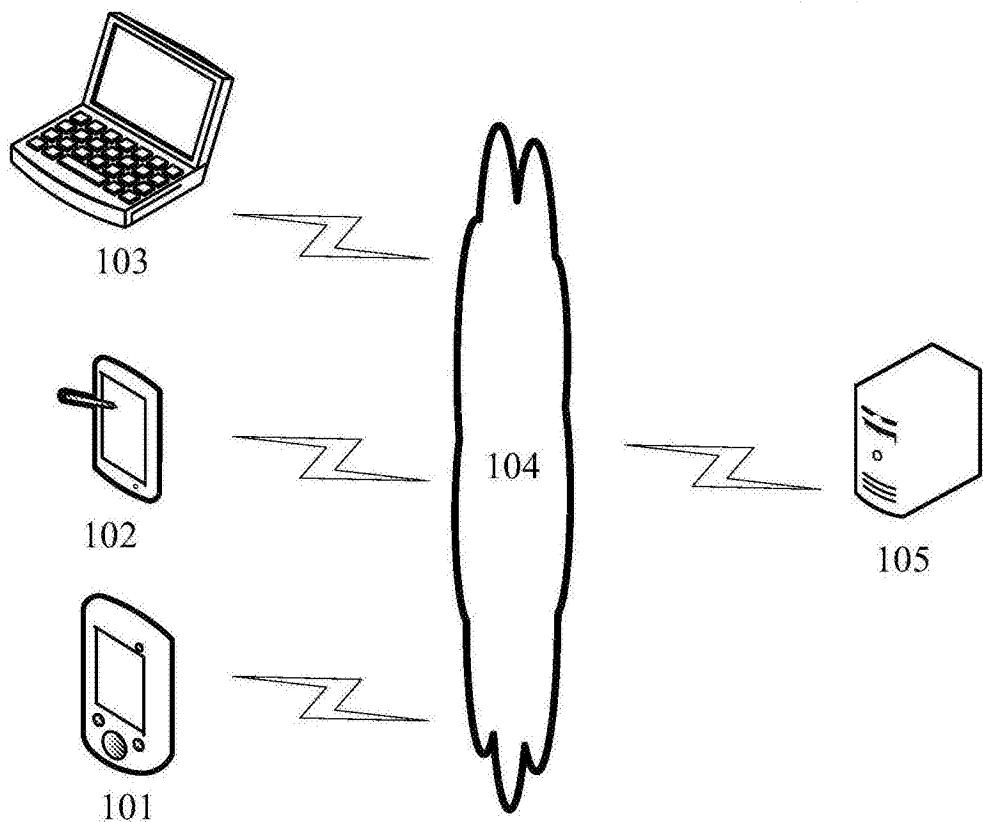
100

图1

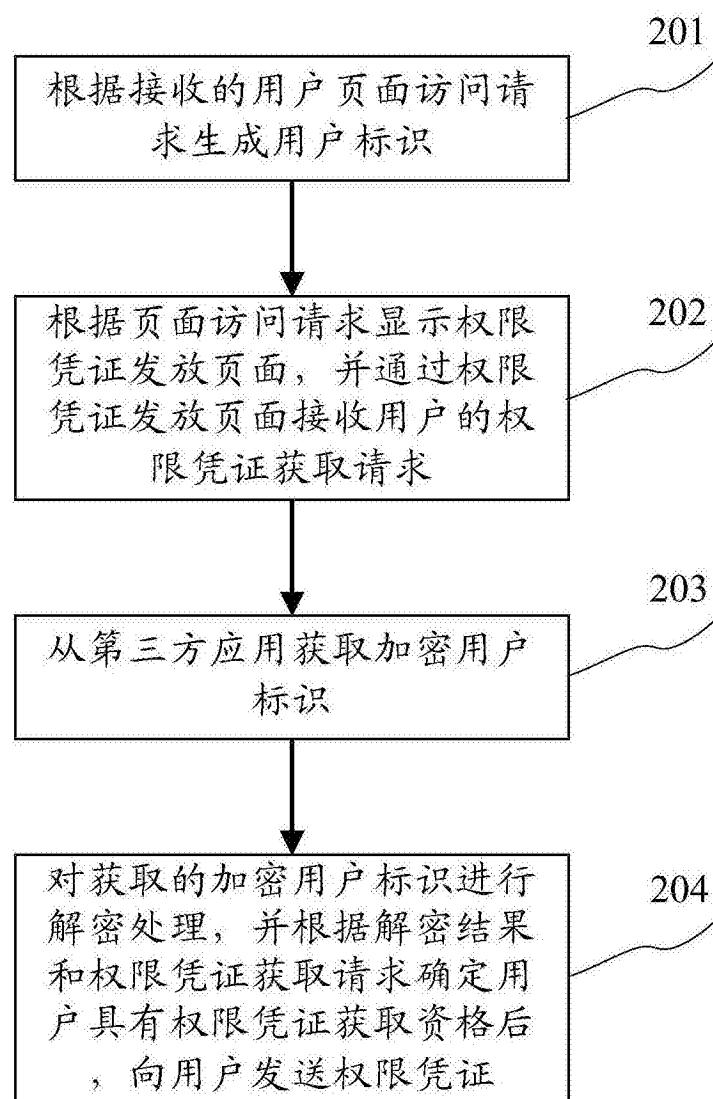
200

图2

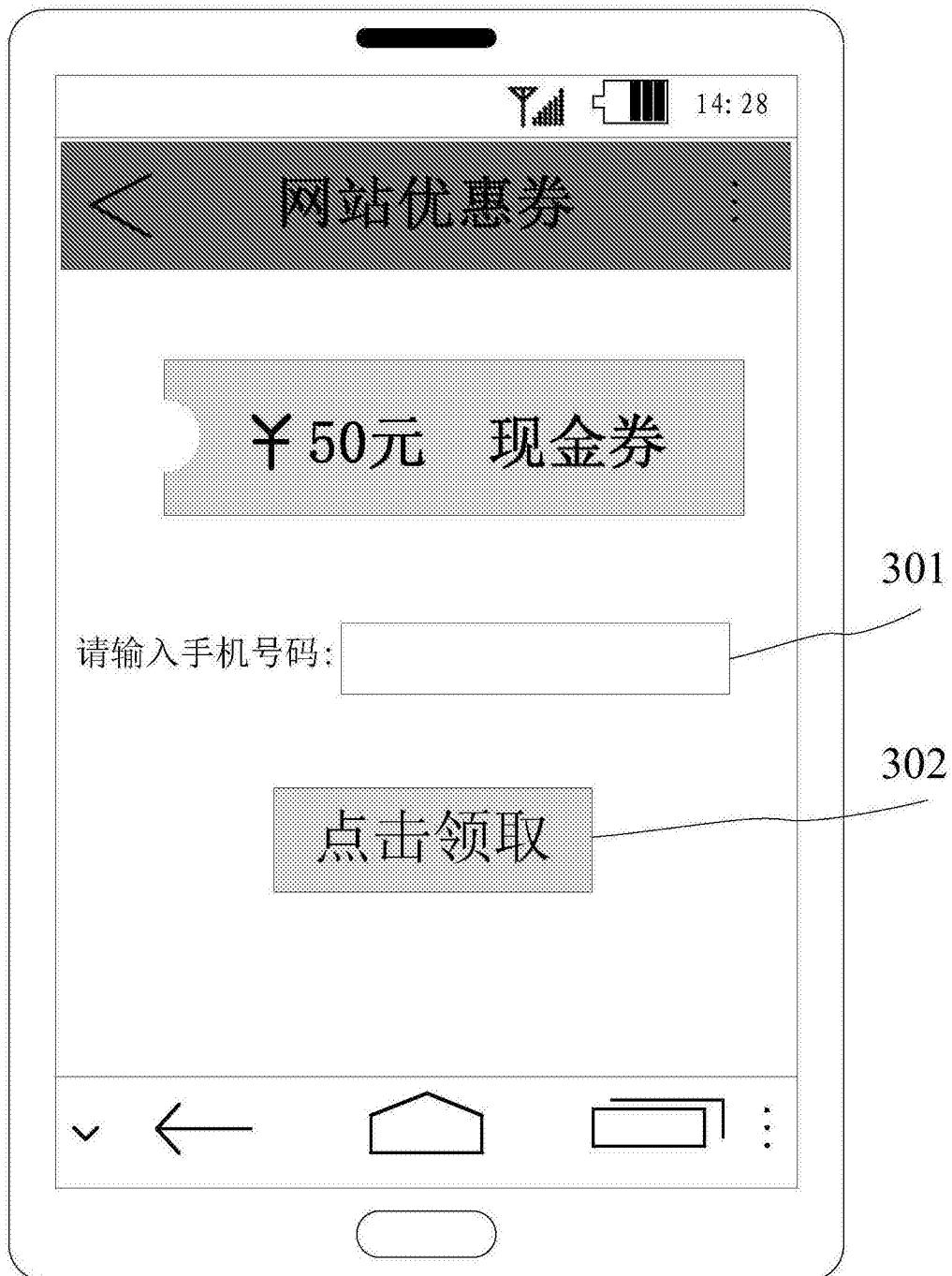


图3

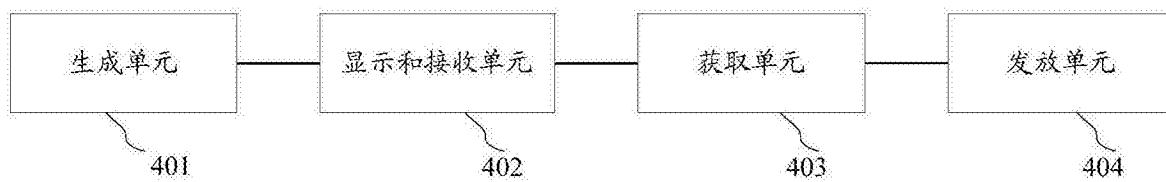
400

图4

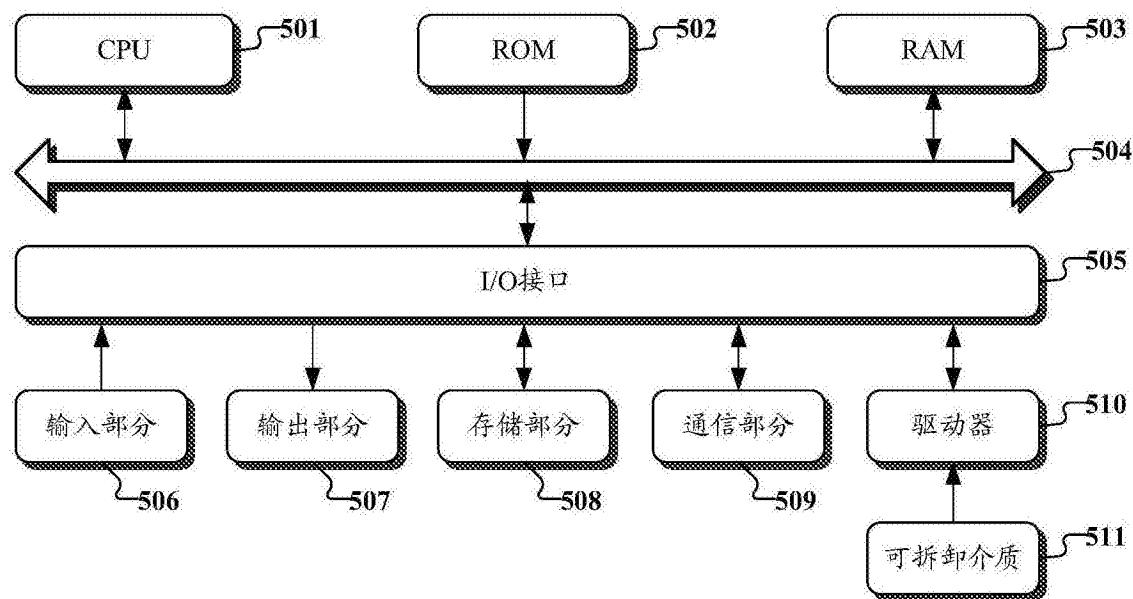
500

图5