(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 109389449 A
(43)申请公布日 2019.02.26

(21)申请号 201710669238.7

(22)申请日 2017.08.08

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市南山区高新区科技中一路腾讯大厦35层

(72)发明人 石彬 卓小亮

(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 张颖玲 李梅香

(51)Int.Cl.
G06Q 30/06(2012.01)
G06Q 20/12(2012.01)
G06Q 20/08(2012.01)
H04L 29/08(2006.01)

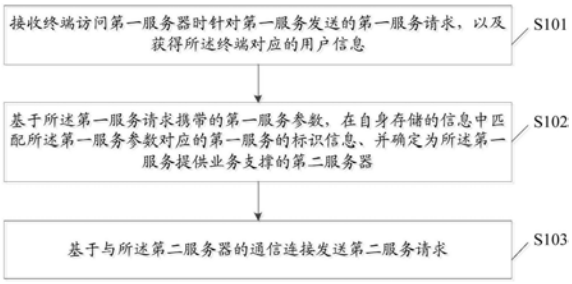
权利要求书2页 说明书15页 附图12页

(54)发明名称

一种信息处理方法、服务器及存储介质

(57)摘要

本发明实施例提供一种信息处理方法，包括：接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端对应的用户信息；基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器；基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。本发明实施例还提供另一种信息处理方法、服务器及存储介质。



CN 109389449 A

1.一种信息处理方法,其特征在于,包括:

接收终端访问第一服务器时针对第一服务发送的第一服务请求,以及获得所述终端的用户信息;

基于所述第一服务请求携带的第一服务参数,在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器;

基于与所述第二服务器的通信连接发送第二服务请求,所述第二服务请求包括所述用户信息和所述第一服务的标识信息,所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

2.根据权利要求1所述的方法,其特征在于,所述接收终端访问第一服务器时针对第一服务发送的第一服务请求之前,所述方法还包括:

获取并存储所述第二服务器能够提供服务的信息;

所述信息包括:服务参数、及与所述服务参数对应的标识信息。

3.根据权利要求1所述的方法,其特征在于,所述基于与所述第二服务器的通信连接发送第二服务请求之前,所述方法还包括:

所述第一服务器获得所述第二服务器发送的网络连接信息,基于所述网络连接信息建立与所述第二服务器的通信连接;

所述网络连接信息基于所述第二服务器完成对应与所述第一服务器的认证后发送。

4.一种信息处理方法,应用于第二服务器,其特征在于,包括:

基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求,所述第二服务请求包括用户信息和第一服务的标识信息;所述标识信息对应于第一服务参数;

当针对所述第二服务请求鉴权成功时,在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据。

5.根据权利要求4所述的方法,其特征在于,所述接收所述第一服务器发送的第二服务请求之前,所述方法还包括:

所述第二服务器获得所述第一服务器的认证信息,基于所述认证信息对所述第一服务器进行认证;所述认证信息包括以下信息的至少之一:校验信息、网络协议地址信息。

6.根据权利要求5所述的方法,其特征在于,所述接收所述第一服务器发送的第二服务请求之前,所述方法还包括:

基于所述第一服务器的认证完成,所述第二服务器向所述第一服务器发送网络连接信息,基于所述网络连接信息建立与所述第一服务器的通信连接。

7.根据权利要求5所述的方法,其特征在于,所述在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据之前,所述方法还包括:

判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致,得到第一判断结果;

在所述第一判断结果为是时,判断所述鉴权信息中携带的用户信息及所述第一服务的标识信息是否有效,得到第二判断结果;

在所述第二判断结果为是时,确认针对所述第二服务请求鉴权成功。

8.第一服务器,其特征在于,所述第一服务器包括:

第一接收单元,用于接收终端针对第一服务发送的第一服务请求,以及获得所述终端

的用户信息；

确定单元，用于基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器。

第一发送单元，用于基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

9.根据权利要求8所述的第一服务器，其特征在于，所述第一服务器还包括：

第二获取单元，用于获得所述第二服务器发送的网络连接信息，基于所述网络连接信息建立与所述第二服务器的通信连接；

所述网络连接信息基于所述第二服务器完成对应与所述第一服务器的认证后发送。

10.第二服务器，其特征在于，所述第二服务器包括：

第三接收单元，用于基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求，所述第二服务请求包括用户信息和第一服务的标识信息；所述标识信息对应于第一服务参数；

服务单元，用于在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据。

11.根据权利要求10所述的第二服务器，其特征在于，所述第二服务器还包括：

第三获取单元，用于获得所述第一服务器的认证信息，基于所述认证信息对所述第一服务器进行认证；所述认证信息包括以下信息的至少之一：校验信息、网络协议地址信息。

12.根据权利要求11所述的第二服务器，其特征在于，所述第二服务器还包括：

建立单元，用于基于所述第一服务器的认证完成，向所述第一服务器发送网络连接信息，基于所述网络连接信息建立与所述第一服务器的通信连接。

13.根据权利要求11所述的第二服务器，其特征在于，所述第二服务器还包括：

鉴权单元，用于对针对第一服务的请求进行鉴权；

所述鉴权单元，具体用于判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致，得到第一判断结果；

在所述第一判断结果为是时，判断所述鉴权信息中携带的网络协议地址信息、用户信息及所述第一服务的标识信息是否有效，得到第二判断结果；

在所述第二判断结果为是时，确认针对所述第二服务请求鉴权成功。

14.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现权利要求1至3任一项所述方法的步骤；

或，该程序被处理器执行时实现权利要求4至7任一项所述方法的步骤。

15.一种服务器，所述服务器包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现权利要求1至3任一项所述方法的步骤；

或，所述处理器执行所述程序时实现权利要求4至7任一项所述方法的步骤。

一种信息处理方法、服务器及存储介质

技术领域

[0001] 本发明涉及通信技术，尤其涉及一种信息处理方法、服务器及存储介质。

背景技术

[0002] 随着信息化的发展，用户可通过服务提供方自身的平台获得虚拟服务；还可通过第三方平台获得服务提供方提供的虚拟服务。第二种虚拟服务的获取方式的网络架构图，如图1所示，具体包括：用户从第三方平台获得虚拟服务对应的标识信息(例如CDKEY)，在通过服务提供方平台输入该标识信息从而获得相应的虚拟服务。

[0003] 这种方式的弊端在于：用户需要在第三方平台操作，获得标识信息后还需要在服务提供方提供的平台操作，过程复杂且繁琐。

发明内容

[0004] 有鉴于此，本发明实施例为解决现有技术中存在的问题而提供一种信息处理方法、服务器及存储介质，使得第二服务器对应的第三方商家能够根据用户的购买请求直接与服务提供方进行信息交互，用于为用户提供服务，简化了用户购买服务的流程。

[0005] 本发明实施例提供一种信息处理方法，包括：

[0006] 接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端的用户信息；

[0007] 基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器；

[0008] 基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

[0009] 上述方案中，所述接收终端访问第一服务器时针对第一服务发送的第一服务请求之前，所述方法还包括：

[0010] 获取并存储所述第二服务器能够提供服务的信息；

[0011] 所述信息包括：服务参数、及与所述服务参数对应的标识信息。

[0012] 上述方案中，所述基于与所述第二服务器的通信连接发送第二服务请求之前，所述方法还包括：

[0013] 所述第一服务器获得所述第二服务器发送的网络连接信息，基于所述网络连接信息建立与所述第二服务器的通信连接；

[0014] 所述网络连接信息基于所述第二服务器完成对应与所述第一服务器的认证后发送。

[0015] 本发明实施例还提供一种信息处理方法，应用于第二服务器，包括：

[0016] 基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求，所述第

二服务请求包括为用户提供第一服务的鉴权信息；

[0017] 用户信息和第一服务的标识信息；所述标识信息对应于第一服务参数；

[0018] 在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据。

[0019] 上述方案中，所述接收所述第一服务器发送的第二服务请求之前，所述方法还包括：

[0020] 所述第二服务器获得所述第一服务器的认证信息，基于所述认证信息对所述第一服务器进行认证；所述认证信息包括以下信息的至少之一：校验信息、网络协议地址信息。

[0021] 上述方案中，所述接收所述第一服务器发送的第二服务请求之前，所述方法还包括：

[0022] 基于所述第一服务器的认证完成，所述第二服务器向所述第一服务器发送网络连接信息，基于所述网络连接信息建立与所述第一服务器的通信连接。

[0023] 上述方案中，所述在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据之前，所述方法还包括：对针对第一服务的请求进行鉴权；

[0024] 所述对针对第一服务的请求进行鉴权，包括：

[0025] 判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致，得到第一判断结果；

[0026] 在所述第一判断结果为是时，判断所述鉴权信息中携带的用户信息及所述第一服务的标识信息是否有效，得到第二判断结果；

[0027] 在所述第二判断结果为是时，确认针对所述第二服务请求鉴权成功。

[0028] 本发明实施例还提供第一服务器，包括：

[0029] 第一接收单元，用于接收终端针对第一服务发送的第一服务请求，以及获得所述终端的用户信息；

[0030] 确定单元，用于基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器。

[0031] 第一发送单元，用于基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

[0032] 上述方案中，所述第一服务器还包括：

[0033] 第二获取单元，用于获得所述第二服务器发送的网络连接信息，基于所述网络连接信息建立与所述第二服务器的通信连接；

[0034] 所述网络连接信息基于所述第二服务器完成对应与所述第一服务器的认证后发送。

[0035] 本发明实施例还提供第二服务器，所述第二服务器包括：

[0036] 第三接收单元，用于基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求，所述第二服务请求包括用户信息和第一服务的标识信息；所述标识信息对应于第一服务参数；

[0037] 服务单元，用于在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据。

[0038] 上述方案中，所述第二服务器还包括：

[0039] 第三获取单元，用于获得所述第一服务器的认证信息，基于所述认证信息对所述第一服务器进行认证；所述认证信息包括以下信息的至少之一：校验信息、网络协议地址信息。

[0040] 上述方案中，所述第二服务器还包括：

[0041] 建立单元，用于基于所述第一服务器的认证完成，向所述第一服务器发送网络连接信息，基于所述网络连接信息建立与所述第一服务器的通信连接。

[0042] 上述方案中，所述第二服务器还包括：

[0043] 鉴权单元，用于对针对第一服务的请求进行鉴权；

[0044] 所述鉴权单元，具体用于判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致，得到第一判断结果；

[0045] 在所述第一判断结果为是时，判断所述鉴权信息中携带的网络协议地址信息、用户信息及所述第一服务的标识信息是否有效，得到第二判断结果；

[0046] 在所述第二判断结果为是时，确认针对所述第二服务请求鉴权成功。

[0047] 上述方案中，所述第二服务器还包括：

[0048] 第三发送单元，用于向所述第一服务器发送第二服务请求响应；

[0049] 在所述第二服务请求响应指示提供向所述用户提供所述第一服务失败时，所述第二服务请求响应包括：错误信息及错误信息对应的错误码。

[0050] 本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现上述方法的步骤。

[0051] 本发明实施例还提供一种服务器，所述服务器包括：存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述方法的步骤。

[0052] 本发明实施例中所提供的信息处理方法、服务器及存储介质，用户向第三方商家对应的第一服务器发送针对第一服务的第一服务请求及所述用户的用户信息；第一服务器基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器；基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息；第二服务器在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据，用于为所述用户提供所述第一服务。如此，通过第一服务器向第二服务器发送携带用户信息和第一服务的标识信息的第二服务请求，第二服务器在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据为所述用户提供所述第一服务；使得用户在购买服务时，无需用户在服务提供方的平台输入服务对应的标识信息，第二服务器对应的第三方商家能够根据用户的购买请求直接与服务提供方进行信息交互，用于为用户提供服务，简化了用户购买服务的流程。当有多个用户需要购买服务时，第二服务器对应的第三方商家能够同时接收多个用户发送的购买请求，并基于多个购买请求与服务提供方进行信息交互，用于为多个用户同时提供服务，提高了为用户提供服务的效率。

附图说明

[0053] 图1为本发明第三方商家代售服务的网络架构示意图；

[0054] 图2为本发明实施例所涉及的网络架构示意图；

[0055] 图3为本发明实施例的信息处理方法的处理流程示意图一；

[0056] 图4为本发明实施例的终端向第一服务器发送第一服务请求示意图一；

[0057] 图5为本发明实施例的终端向第一服务器发送第一服务请求示意图二；

[0058] 图6为本发明实施例的第一服务器与第二服务器建立通信连接的处理流程示意图；

[0059] 图7为本发明实施例的信息处理方法的处理流程示意图二；

[0060] 图8为本发明实施例的信息处理方法的处理流程示意图三；

[0061] 图9为本发明实施例的信息处理方法的处理流程示意图四；

[0062] 图10为本发明实施例的信息处理方法的处理流程示意图五；

[0063] 图11为本发明实施例的信息处理方法的处理流程示意图六；

[0064] 图12为本发明实施例的信息处理方法的处理流程示意图七；

[0065] 图13为本发明实施例的信息处理方法的处理流程示意图八；

[0066] 图14为本发明实施例的信息处理方法的处理流程示意图九；

[0067] 图15为本发明实施例的信息处理方法的处理流程示意图十；

[0068] 图16为本发明实施例的信息处理方法的处理流程示意图十一；

[0069] 图17为本发明实施例第一服务器的组成结构示意图；

[0070] 图18为本发明实施例第二服务器的组成结构示意图；

[0071] 图19为本发明实施例服务器的硬件组成结构示意图。

具体实施方式

[0072] 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，此处所提供的实施例仅仅用以解释本发明，并不用于限定本发明。另外，以下所提供的实施例是用于实施本发明的部分实施例，而非提供实施本发明的全部实施例，在不冲突的情况下，本发明实施例记载的技术方案可以任意组合的方式实施。

[0073] 本发明实施例中涉及的名词和术语适用于如下的解释。

[0074] 1)服务，这里的服务可以是包装为服务的虚拟资产(例如会员特权、商家优惠券、代金券、团购券、红包、外卖服务、保洁服务、家政服务等)，也可以是在网络上使用的服务(例如网络游戏点卡、网上影院电影票等)，也可以是线上和线下相结合的服务。

[0075] 2)第一服务器，是指能够为用户提供服务购买业务的服务器，第一服务器为第三方商家的设备，所述第三方商家是指与服务提供方合作的渠道商，第三方包括：天猫商铺、京东商铺、联通电信运营商等。

[0076] 3)第二服务器，是指能够为服务提供业务支撑的服务器，第二服务器为服务提供方的设备。

[0077] 4)标识信息，为供用户获取服务的凭证，由服务提供方生成；

[0078] 从呈现方式的角度，服务的标识信息呈现的形式包括：由字母和数字构成的固定位数的号码、二维码、条形码等形式。

[0079] 从应用场景的角度，服务的标识信息可以包括电子折扣券和电子代金券等类型的

电子优惠券，也可以为直接用于兑换服务的电子兑换券。

[0080] 在介绍本实施例之前，先介绍一下本发明实施例所涉及的网络架构，图2为本发明实施例中网络架构示意图，本实施例涉及三方的设备，第一设备为请求获取服务的用户的设备(终端10)，第二设备为第三方商家对应的设备20，第三设备为服务提供方对应的设备30。

[0081] 在实施的过程中，第二设备首先与第三设备建立基于服务的通信连接，使得第二设备能够调用第三设备中的服务充值系统，请求第三设备为用户提供服务。第一设备向第二设备发送获取服务的请求后，第二设备根据所述请求及与第三设备建立通信连接所使用的参数向第三设备发送获取服务的请求；第三设备针对接收到的请求进行鉴权，鉴权成功后为用户提供服务。

[0082] 本发明实施例的信息处理方法的处理流程示意图一，如图3所示，包括以下步骤：

[0083] 步骤S101，接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端的用户信息；

[0084] 具体地，终端向第一服务器发送第一服务请求，所述第一服务请求用于请求获取第一服务。

[0085] 所述第一服务请求中携带有第一服务参数，所述第一服务参数携带的必要信息包括：待获取的目标服务(第一服务)的信息，如名称、类型、序列号、期限等；所述第一服务参数携带的可选信息包括：提供目标服务(第一服务)的商家的信息，如商家名称、商家地址等。

[0086] 举例来说，所述第一服务为腾讯视频VIP服务时，所述第一服务携带的信息包括：商家名称为腾讯视频、第一服务类型为视频VIP服务、第一服务期限为六个月。所述第一服务为肯德基时，所述第一服务携带的信息包括：商家名称为肯德基、第一服务类型为全品类九折的电子折扣券。当然不限于上述列举的第一服务参数，其他多种服务参数也在本发明实施例的保护范围之内。

[0087] 在一个具体实施例中，终端向第一服务器发送第一服务请求的一种方式为：用户在终端显示界面上触发与第一服务器对应的第三方商家提供的“售卖第一服务”功能；具体地，如图4所示，用户首先触发终端界面上第三方商家提供的“充值”功能，进入服务选择界面；用户通过特定的操作方式，如单击或双击等在多个服务中选择需要购买的第一服务。

[0088] 在一个具体实施例中，终端向第一服务器发送第一服务请求的另一种方式为：用户参加与第一服务器对应的第三方商家赠送第一服务的活动；具体地，第三方商家发起促销活动，在第三方商家购物满足第一金额即可赠送第一服务，所述第一金额的值由第三方商家灵活设定；如图5所示，当用户在第三方商家购物满足第一金额时，终端显示界面提示“领取第一服务”；当用户触发“领取第一服务”时，即为向第一服务器发送第一服务请求。当然不限于上述终端向第一服务器发送第一服务请求的两种方式，其他可实现的终端向第一服务器发送第一服务请求的方式均在本发明实施例的保护范围之内。

[0089] 继续对前述实施例进行说明，作为对第一服务请求的响应，第一服务器向所述终端发送第一指令；所述第一指令用户指示所述终端发送对应的用户信息。终端接收到第一服务器发送的第一指令后，向所述服务器发送所述终端的用户信息。其中，所述用户信息是指用户消费所述服务时，所使用的账号信息，如QQ账号或微信账号等。

[0090] 步骤S102,基于所述第一服务请求携带的第一服务参数,在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器;

[0091] 具体地,第一服务器提取所述第一服务请求中携带的第一服务参数后,第一服务器在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息。

[0092] 这里,第一服务器需要预先接收第二服务器能够提供服务的信息,所述信息包括:服务参数、及与所述服务参数对应的标识信息;第一服务器可以加密邮件的形式将自身能够提供服务的信息发送至第一服务器。服务参数包括的内容与上述步骤S101中提及的第一服务参数包括的内容相同,标识信息呈现的形式可以为:由16位大小写字母和数字组成的一串号码、或二维码、或条形码等任何能够作为用户获取服务的凭证。对于一种服务,存在多个标识信息与之对应;也就是说,可以是多个用户利用多个标识信息获取同一种服务;因此,第一服务器可以同时接收多个用户发送的获取服务的请求,有效地提高了为用户提供服务的效率。

[0093] 继续对前述实施例进行说明,第一服务器将由第一服务请求中提取的第一服务参数在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息。由于与第一服务器对应的第三方商家可能会与多个服务提供方合作,代售多个服务提供方提供的服务;因此,第一服务器会根据所述第一服务请求中携带的第一服务参数确定为所述第一服务提供业务支撑的第二服务器。

[0094] 步骤S103,基于与所述第二服务器的通信连接发送第二服务请求;

[0095] 具体地,第一服务器需首先与第二服务器建立通信连接,基于已经建立的通信连接,第一服务器采用安全版超文本传输(Hyper Text Transfer Protocol over Secure Socket Lay,https)协议、利用POST模式向第二服务器发送第二服务请求;所述第二服务请求包括所述用户信息和所述第一服务的标识信息,所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

[0096] 本发明实施例中,第一服务器采用https协议、利用POST模式向第二服务器发送服务请求,能够保证网络传输过程的安全性。

[0097] 继续对前述实施例进行说明,第一服务器与第二服务器建立通信连接的处理流程示意图,如图6所示,包括以下步骤:

[0098] 步骤1a,当第二服务器对应的服务提供方与第一服务器对应的第三方商家进行服务售卖合作时,服务提供方为第三方商家分配用于唯一表征所述第一服务器的校验信息,所述校验信息包括第三方商家账号和第三方商家密码,将所述校验信息发送至第三方商家;同时,请求第三方商家提供网络协议(Internet Protocol,IP)地址信息,所述IP地址信息为第一服务器向第二服务器请求为用户提供服务时所使用的IP地址。

[0099] 步骤1b,第三方商家向服务提供方发送IP地址信息。

[0100] 步骤1c,服务提供方将服务的标识信息、所述校验信息及所述IP地址信息记录至自身的服务充值数据中;

[0101] 具体地,可以是服务提供方将服务的标识信息、所述校验信息及所述IP地址信息注册至服务提供方的服务充值系统中;可以理解,该过程即为第二服务器完成对应与所述第一服务器的认证过程。。

[0102] 这里,所述标识信息与所述第三方商家与所述服务提供方进行售卖合作的服务存在对应关系;所述校验信息和所述IP地址信息也与所述第三方商家与所述服务提供方进行售卖合作的服务存在对应关系。

[0103] 步骤1d,服务提供方向第三方商家发送基于所合作的服务进行交互的协议;

[0104] 这里,所述协议是指第三方商家向服务提供方发送为用户提供服务的请求格式、字段、及对应的含义,及第三方商家向服务提供方发送为用户提供服务的请求目的网络协议地址,所述目的网络协议地址即为网络连接信息。

[0105] 具体地,规定了第三方商家采用https协议、利用POST模式向服务提供方发送针对所合作服务的服务请求,即第三方商家调用服务提供方的服务充值系统的接口,用于请求为用户提供服务;其中,所述服务请求携带的JSON数据包所包括的参数及参数说明如表1所示;表1所述“参数”中的“qqid”和“wxid”为用户信息,“cdkey”为标识信息,“shop”为用于表征第三方商家的校验信息,“figure”为采用消息摘要算法第五版(Message Digest Algorithm,MD5)对qqid、cdkey、shop对应的数值及特殊约定字符串加密获得。

[0106]

参数	说明	是否必须
qqid	待充会员qq号	是
wxid	待充会员微信号(优先)	是
cdkey	待核销cdkey(16位字母)	是
shop	商铺标识	是
figure	指纹信息	是

[0107] 表1

[0108] 在一具体实施例中,第三方商家向服务提供方发送的服务请求为:

[0109]
```
{
  “qq”:”545891183”,
  “wxid”:””
  “cdkey”:”DAEUNSSFYsdwrYNY”,
  “shop”:”tmall_shop_1”,
  “figure”:” 0b3fa34f401731dc3c57a046c8213cd4”
}
```

[0110] “figure”的计算方式为:Md5(${qq}&${cdkey}&${shop}&${特殊约定字符串})

[0111] 待加密字符串为:

[0112] 545891183&DAEUNSSFYsdwrYN&tmall_shop_1&tmall_shop_password。

[0113] 待加密字符串经Md5方式加密后的密文为:

[0114] 0b3fa34f401731dc3c57a046c8213cd4。

[0115] 在另一具体实施例中,第三方商家向服务提供方发送的服务请求为:

[0116]
```
{
  “qq”:”0”,
  “wxid”:”Runner802”
  “cdkey”:”DAEUNSSFYsdwrYNY”,
  “shop”:”tmall_shop_1”,
  “figure”:”dcbecbb860fa565db8444f9a11338f26”
}
```

[0118] “figure”的计算方式为:Md5(${wxid}&${cdkey}&${shop}&${特殊约定字符串})

[0119] 待加密字符串为:

[0120] Runner802&DAEUNSSFYsdwrYN&tmall_shop_1&tmall_shop_password

[0121] 待加密字符串经Md5方式加密后的密文为:

[0122] dcbecbb860fa565db8444f9a11338f26。

[0123] 本发明实施例的信息处理方法的处理流程示意图二,如图7所示,本实施例的方法与图3所示的方法相似,其不同之处在于,在步骤S103之后还包括:

[0124] 步骤S104,第一服务器接收所述第二服务器发送的第二服务请求响应;

[0125] 这里,在所述第二服务请求响应指示向所述终端的用户提供所述第一服务成功时,所述第二服务请求响应包括:提供服务成功;在所述第二服务请求响应指示向所述终端的用户提供所述第一服务失败时,所述第二服务请求响应包括:错误信息及错误信息对应的错误码。

[0126] 具体地,第二服务器向第一服务器返回一JSON数据包,所述JSON数据包携带的内容为:

[0127]
```
{
  “ret”:0
  “msg”:”success”
}
```

[0128] 在一具体实施例中,第二服务器向第一服务器发送的错误码定义如下所示:

[0129] 错误码“10000”表示非https请求,错误码“10001”表示参数错误,错误码“10002”表示商铺信息错误,错误码“10003”表示非白名单IP,错误码“10004”表示指纹校验失败,错误码“10005”表示CDKEY已使用过,错误码“10006”表示系统错误、错误信息减msg,错误码“10007”表示非本商铺商品,错误码“10008”表示微信号查询失败。

[0130] 本发明实施例的信息处理方法的处理流程示意图三,如图8所示,本实施例的方法与图7所示的方法相似,其不同之处在于,在步骤S104之后还包括:

[0131] 步骤S105,第一服务器再次向第二服务器发送第二服务请求;

[0132] 在步骤S104中,所述第二服务请求响应指示向所述终端的用户提供所述第一服务失败时,第一服务器根据所述第二服务请求响应携带的错误信息及错误信息对应的错误码修正相应的参数信息,基于修正后的参数信息再次向第二服务器发送第二服务请求,用于

请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

[0133] 本发明实施例的信息处理方法的处理流程示意图四，如图9所示，本实施例的方法与图3所示的方法相似，其不同之处在于，在步骤S102之后还包括：

[0134] 步骤S106，第一服务器确认第一服务对应的标识信息处于不安全状态时，向第二服务器发送标识信息更换请求；

[0135] 这里，所述标识信息处于不安全状态至少包括：第一服务器由于自身损坏等原因导致的所述表示信息丢失、其他服务器通过非常规手段(如窃取)获取所述标识信息等。

[0136] 其中，所述更换请求携带处于不安全状态的标识信息列表。

[0137] 步骤S107，接收第二服务器发送的更换请求响应；

[0138] 这里，第一服务器接收的所述更换请求响应携带新的标识信息，所述新的标识信息为供用户获取第一服务的凭证；同时，所述更换请求响应还用于表征已取消所述更换请求中携带的标识信息的有效状态。如此，第二服务器通过取消处于不安全状态的标识信息的有效状态，有效地避免了服务资产的遗失。

[0139] 本发明实施例的信息处理方法的处理流程示意图五，如图10所示，包括以下步骤：

[0140] 步骤201，基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求；

[0141] 由于本发明实施例应用于第二服务器，因此，该步骤为第二服务器

[0142] 基于与第一服务器的通信连接接收第二服务请求；所述第二服务请求包括用户信息和第一服务的标识信息；所述标识信息对应于第一服务参数；

[0143] 所述用户信息为待提供服务的用户的信息，如：qq账号或微信账号；所述第一服务参数携带的必要信息包括：待获取的目标服务(第一服务)的信息，如名称、类型、序列号、期限等；所述第一服务参数携带的可选信息包括：提供目标服务(第一服务)的商家的信息，如商家名称、商家地址等。

[0144] 具体地，第二服务器需首先与第一服务器建立通信连接，基于已经建立的通信连接，第二服务器接收第一服务器采用https协议、利用POST模式发送的第二服务请求；所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。第二服务器与第一服务器建立通信连接的具体处理流图，如上述图6所示，这里不再赘述。

[0145] 本发明实施例中，第一服务器采用https协议、利用POST模式向第二服务器发送服务请求，能够保证网络传输过程的安全性。

[0146] 步骤S202，当针对所述第二服务请求鉴权成功时，在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据；

[0147] 具体地，所述第二服务器在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据，用于为所述用户提供所述第一服务。

[0148] 本发明实施例的信息处理方法的处理流程示意图六，如图11所示，本实施例的方法与图10所示的方法相似，其不同之处在于，在步骤S201之后还包括对针对第二服务请求进行鉴权；对针对第二服务请求进行鉴权的具体实现过程，包括：

[0149] 步骤S203，判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致，得到第一判断结果；在第一判断结果为是时，执行步骤S204；在第一判断结果为

否时，结束流程；

[0150] 这里，第二服务器预先为第一服务器分配用于唯一表征所述第一服务器的校验信息，所述校验信息包括：与第一服务器对应的第三方商家账号和第三方商家密码。第二服务器还可以预先接收第一服务器发送的IP地址信息，所述IP地址信息为所述第一服务器向所述第二服务器发送服务请求所使用的地址信息。

[0151] 具体地，第二服务器判断所述第二服务请求携带的鉴权信息中的第三方商家账号与第二服务器预先为第一服务器分配的第三方商家账号是否一致；并判断所述第二服务请求携带的鉴权信息中的第三方商家密码与第二服务器预先为第一服务器分配的第三方商家密码是否一致；在上述判断结果均为是时，执行步骤S204。

[0152] 或第二服务器判断所述第二服务请求携带的鉴权信息中的第三方商家账号与第二服务器预先为第一服务器分配的第三方商家账号是否一致；并判断所述第二服务请求携带的鉴权信息中的第三方商家密码与第二服务器预先为第一服务器分配的第三方商家密码是否一致；再判断所述第二服务请求携带的IP地址信息与第二服务器内记录的第一服务器用于发送服务请求的IP地址信息是否一致；在上述判断结果均为是时，执行步骤S204。

[0153] 步骤S204，判断所述鉴权信息中携带的用户信息及所述第一服务的标识信息是否有效，得到第二判断结果；在第二判断结果为是时，执行步骤S202；在第二判断结果为否时，结束流程；

[0154] 具体地，第二服务器判断所述鉴权信息中携带的用户信息，如qqid、微信id是否有效，判断所述第一服务的标识信息是否处于有效状态；在上述判断结果均为是时，执行步骤S202。

[0155] 本发明实施例中，通过对唯一表征第一服务器的校验信息、第一服务器发送服务请求的IP地址信息、用户信息及标识信息的验证，来确保第三服务器请求的合法性。

[0156] 本发明实施例的信息处理方法的处理流程示意图七，如图12所示，本实施例的方法与图10所示的方法相似，其不同之处在于，在步骤S201之前还包括：

[0157] 步骤S200，向所述第一服务器发送所述第二服务器能够提供服务的信息；

[0158] 具体地，第二服务器向所述第一服务器发送所述第二服务器能够提供服务的信息。

[0159] 所述信息包括：服务参数、及与所述服务参数对应的标识信息；所述服务参数携带的必要信息包括：待获取的目标服务的信息，如名称、类型、序列号、期限等；所述服务参数携带的可选信息包括：提供目标服务的商家的信息，如商家名称、商家地址等。

[0160] 举例来说，所述服务为腾讯视频VIP服务时，所述服务携带的信息包括：商家名称为腾讯视频、服务类型为视频VIP服务、服务期限为六个月。所述服务为肯德基时，所述服务携带的信息包括：商家名称为肯德基、服务类型为全品类九折的电子折扣券。当然不限于上述列举的服务参数，其他多种服务参数也在本发明实施例的保护范围之内。

[0161] 本发明实施例的信息处理方法的处理流程示意图八，如图13所示，本实施例的方法与图10所示的方法相似，其不同之处在于，在步骤S202之后还包括：

[0162] 步骤S205，向所述第一服务器发送第二服务请求响应；

[0163] 这里，在所述第二服务请求响应指示向所述终端的用户提供所述第一服务成功时，所述第二服务请求响应包括：提供服务成功；在所述第二服务请求响应指示提供向所述

用户提供所述第一服务失败时，所述第二服务请求响应包括：错误信息及错误信息对应的错误码。

[0164] 具体地，第二服务器向第一服务器返回一JSON数据包，所述JSON数据包携带的内容为：

[0165]
```
{
  “ret”:0
  “msg”:”success”
}
```

[0166]

[0167] 在一具体实施例中，第二服务器向第一服务器发送的错误码定义如下所示：

[0168] 错误码“10000”表示非https请求，错误码“10001”表示参数错误，错误码“10002”表示商铺信息错误，错误码“10003”表示非白名单IP，错误码“10004”表示指纹校验失败，错误码“10005”标识CDKEY已使用过，错误码“10006”表示系统错误、错误信息减msg，错误码“10007”表示非本商铺商品，错误码“10008”表示微信号查询失败。

[0169] 本发明实施例的信息处理方法的处理流程示意图九，如图14所示，本实施例的方法与图13所示的方法相似，其不同之处在于，在步骤S205之后还包括：

[0170] 步骤S206，取消所述第二处理请求携带的标识信息的有效状态；

[0171] 在步骤S205中，所述第二服务请求响应指示向所述终端的用户提供所述第一服务成功时，第二服务器取消所述第三处理请求携带的标识信息的有效状态。

[0172] 具体地，第二服务器可以在自身记录的服务对应的标识信息中找到第一服务对应的标识信息，将所述第一服务对应的标识信息属性标记为不可用；或者第二服务器可以在自身记录的服务对应的标识信息中找到第一服务对应的标识信息，并在自身记录的服务对应的标识信息中删除第一服务对应的标识信息。如此，能够避免同一个标识信息的重复利用。

[0173] 本发明实施例的信息处理方法的处理流程示意图十，如图15所示，本实施例的方法与图10所示的方法相似，其不同之处在于，在步骤S201之前还包括：

[0174] 步骤S207，第二服务器接收第一服务器发送的标识信息更换请求；

[0175] 这里，所述标识信息处于不安全状态至少包括：第一服务器由于自身损坏等原因导致的所述表示信息丢失、其他服务器通过非常规手段(如窃取)获取所述标识信息等。

[0176] 其中，所述更换请求携带处于不安全状态的标识信息列表。

[0177] 步骤S208，第二服务器向第一服务器发送更换请求响应；

[0178] 这里，所述更换请求响应携带新的标识信息，所述新的标识信息为供用户获取第一服务的凭证；同时，所述更换请求响应还用于表征已取消所述更换请求中携带的标识信息的有效状态。如此，第二服务器通过取消处于不安全状态的标识信息的有效状态，有效地避免了服务资产的遗失；

[0179] 具体地，第二服务器取消处于不安全状态的标识信息的有效状态的具体处理流程与上述步骤S206的具体操作流程相同，这里不再赘述。

[0180] 以用户通过第三方商家为指定的QQ号码购买服务期限为六个月的腾讯视频VIP服务为例，本发明实施例的信息处理方法的处理流程示意图十一，如图16所示，包括以下步

骤：

[0181] 步骤S301，第三方商家与腾讯公司建立服务售卖合作；

[0182] 具体地，腾讯公司为第三方商家分配用于表征第三方商家的店铺名称和店铺密码；第三方商家向腾讯公司发送IP地址信息，所述IP地址信息为第三方商家向腾讯公司发送为用户提供服务的请求时所使用的IP地址；腾讯公司将店铺名称、店铺密码及IP地址信息注册至自身的服务直充系统。

[0183] 步骤S302，服务直充系统向第三方商家发送自身能够提供的服务，及服务对应的标识信息；

[0184] 具体地，可通过加密邮件的形式向第三方商家发送服务及服务对应的标识信息。

[0185] 步骤S303，用户向第三方商家发送购买腾讯视频VIP服务的请求，并完成针对所购买的服务的支付；

[0186] 其中，所述请求携带购买腾讯视频VIP服务的QQ号码、购买腾讯视频VIP服务的期限为六个月。

[0187] 步骤S304，第三方商家在自身存储的标识信息中匹配用户购买的服务对应的标识信息(cdkey)。

[0188] 步骤S305，第三方商家调用服务直充系统，请求为用户提供相应的服务；

[0189] 具体地，第三方商家调用腾讯公司的服务直充系统是向服务直充系统的接口发送携带购买腾讯视频VIP服务的QQ号码、cdkey、店铺名称、店铺密码及IP地址信息的请求。

[0190] 步骤S306，服务直充系统对所述请求进行安全校验；

[0191] 具体地，将所述请求中携带的cdkey、店铺名称、店铺密码及IP地址信息与自身存储的cdkey、店铺名称、店铺密码及IP地址信息进行匹配，得到匹配结果，如果匹配结果一致，进一步判断购买腾讯视频VIP服务的QQ号码是否有效，判断结果为是时，安全校验通过。

[0192] 步骤S307，服务直充系统兑换腾讯视频VIP服务，并返回请求响应；

[0193] 具体地，在该QQ用户的账户下没有腾讯视频VIP服务数据时，通过兑换腾讯视频VIP服务，使得该用户成了腾讯视频VIP会员，并享受腾讯视频VIP会员的特权；在该QQ用户的账户下有腾讯视频VIP服务数据时，通过兑换腾讯视频VIP服务，使得的该用户延长了腾讯视频VIP会员的时限。

[0194] 为实现本发明上述信息处理方法实施例，本发明实施例还提供第一服务器，所述第一服务器的组成结构如图17所示，包括：

[0195] 第一接收单元100，用于接收终端针对第一服务发送的第一服务请求，以及获得所述终端的用户信息；

[0196] 确定单元101，用于基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器。

[0197] 第一发送单元102，用于基于与所述第二服务器的通信连接发送第二服务请求，所述第二服务请求包括所述用户信息和所述第一服务的标识信息，所述第二服务请求用于请求所述第二服务器向所述终端的用户提供所述第一服务的标识信息对应的第一服务。

[0198] 在一具体实施例中，所述第一服务器还包括：

[0199] 第一获取单元103，用于获取并存储所述第二服务器能够提供服务的信息；

[0200] 所述信息包括:服务参数、及与所述服务参数对应的标识信息。

[0201] 在一具体实施例中,所述第一服务器还包括:

[0202] 第二获取单元104,用于获得所述第二服务器分配的用于表征所述第一服务器的校验信息;

[0203] 所述第一发送单元102,还用于向所述第二服务器发送网络协议地址信息,以使所述第二服务器基于所述校验信息和所述网络协议地址信息建立与所述第一服务器的通信连接。

[0204] 在一具体实施例中,所述第一接收单元100,具体用于向所述终端发送第一指令;

[0205] 获取所述终端基于所述第一指令发送的所述终端的用户信息。

[0206] 在一具体实施例中,所述第一服务器还包括:

[0207] 第二接收单元105,用于接收所述第二服务器发送的第二服务请求响应;

[0208] 在所述第二服务请求响应指示向所述终端的用户提供所述第一服务失败时,所述第二服务请求响应包括:错误信息及错误信息对应的错误码。

[0209] 为实现本发明上述信息处理方法实施例,本发明实施例还提供第二服务器,所述第二服务器的组成结构如图18所示,包括:

[0210] 第三接收单元200,用于基于与第一服务器的通信连接接收所述第一服务器发送的第二服务请求,所述第二服务请求包括用户信息和第一服务的标识信息;所述标识信息对应于第一服务参数。

[0211] 服务单元201,用于在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据。

[0212] 在一具体实施例中,所述第二服务器还包括:

[0213] 第二发送单元202,用于向所述第一服务器发送所述第二服务器能够提供服务的信息;

[0214] 所述信息包括:服务参数、及与所述服务参数对应的标识信息。

[0215] 在一具体实施例中,所述第二服务器还包括:

[0216] 第三获取单元203,用于获得所述第一服务器的认证信息,基于所述认证信息对所述第一服务器进行认证;所述认证信息包括以下信息的至少之一:校验信息、网络协议地址信息。

[0217] 在一具体实施例中,所述第二服务器还包括:

[0218] 建立单元204,用于基于所述第一服务器的认证完成,向所述第一服务器发送网络连接信息,基于所述网络连接信息建立与所述第一服务器的通信连接。

[0219] 在一具体实施例中,所述第二服务器还包括:

[0220] 鉴权单元205,用于对针对第一服务的请求进行鉴权;

[0221] 鉴权单元205,具体用于判断鉴权信息中携带的校验信息与为所述第一服务器分配的校验信息是否一致,得到第一判断结果。

[0222] 在所述第一判断结果为是时,判断所述鉴权信息中携带的网络协议地址信息、用户信息及所述第一服务的标识信息是否有效,得到第二判断结果;

[0223] 在所述第二判断结果为是时,确认针对所述第二服务请求鉴权成功。

[0224] 在一具体实施例中,所述第二服务器还包括:

[0225] 第三发送单元206，用于向所述第一服务器发送第二服务请求响应；

[0226] 在所述第二服务请求响应指示提供向所述用户提供所述第一服务失败时，所述第二服务请求响应包括：错误信息及错误信息对应的错误码。

[0227] 本发明实施例中，构成所述第一服务器的第一接收单元100、确定单元101、第一发送单元102、第一获取单元103、第二获取单元104、第二接收单元105执行的功能可由位于服务器上的中央处理器(CPU)、或微处理器(MPU)、或数字信号处理器(DSP)、或可编程门阵列(FPGA)实现。

[0228] 本发明实施例中，构成所述第二服务器的第三接收单元200、服务单元201、第二发送单元202、第三获取单元203、建立单元204、鉴权单元205、第三发送单元206执行的功能可由位于服务器上的CPU、或MPU、或DSP或FPGA实现。

[0229] 本发明实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现上述方法的步骤。所述的计算机可读存储介质包括：移动存储设备、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0230] 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、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0231] 本发明实施例还提供一种服务器，所述服务器的硬件组成结构示意图，如图19所示，包括处理器701和存储器702，所述存储器702上存储有应用程序7022。

[0232] 上述本发明实施例揭示的方法可以应用于处理器701中，或者由处理器701实现。处理器701可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器701中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器701可以是通用处理器、DSP，或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。处理器701可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本发明实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于存储器702，处理器701读取存储器702中的信息，结合其硬件完成前述方法的步骤。

[0233] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备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，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0234] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显

示的部件可以是、或也可以不是物理单元，即可以位于一个地方，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全部单元来实现本实施例方案的目的。

[0235] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，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，也可以采用硬件加软件功能单元的形式实现。

[0236] 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。

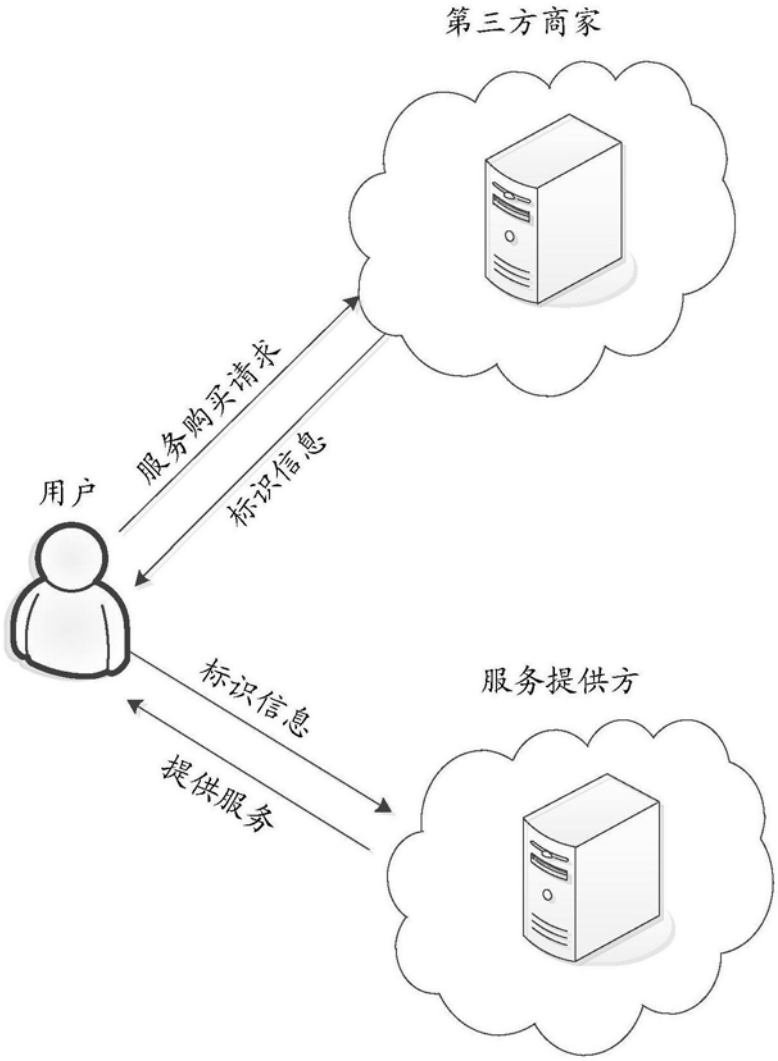


图1

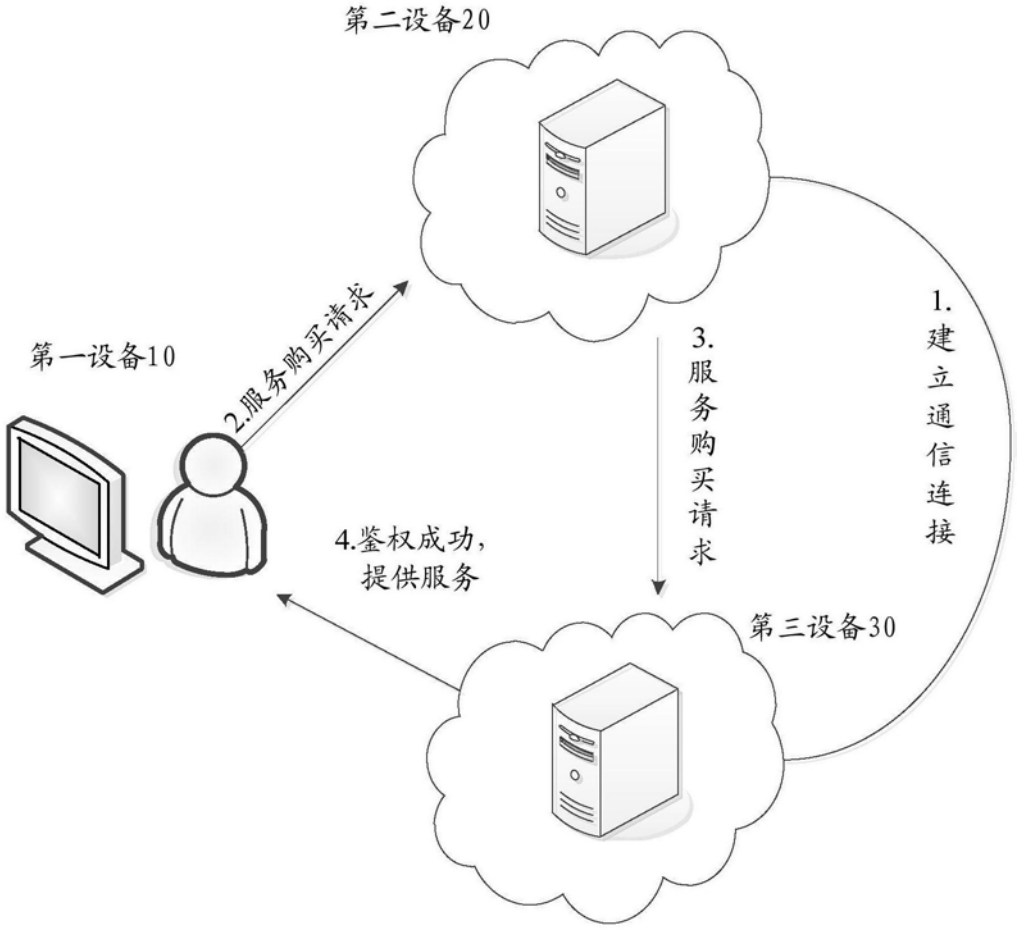

第二设备20
第一设备10
2.服务购买请求
3.
服
务
购
买
请
求
1.
建
立
通
信
连
接
4.鉴权成功，
提供服务
第三设备30

图2

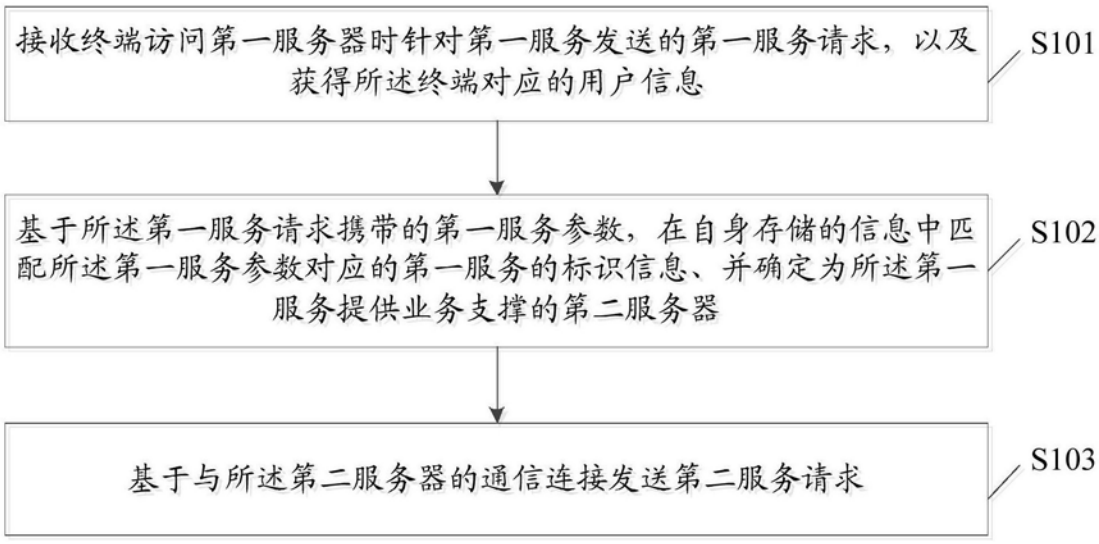

接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端对应的用户信息
S101
基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器
S102
基于与所述第二服务器的通信连接发送第二服务请求
S103

图3

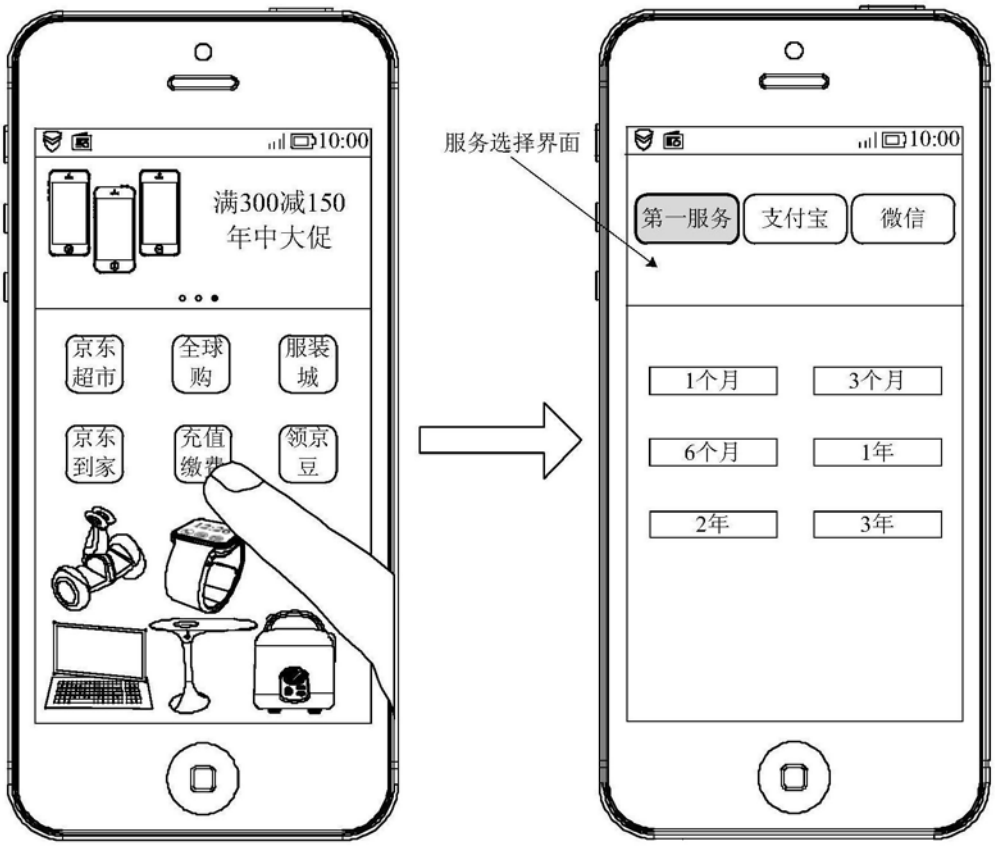

10:00
满300减150
年中大促
京东超市
全球购
服装城
京东到家
充值缴费
领京豆
服务选择界面
10:00
第一服务
支付宝
微信
1个月
3个月
6个月
1年
2年
3年

图4

图5

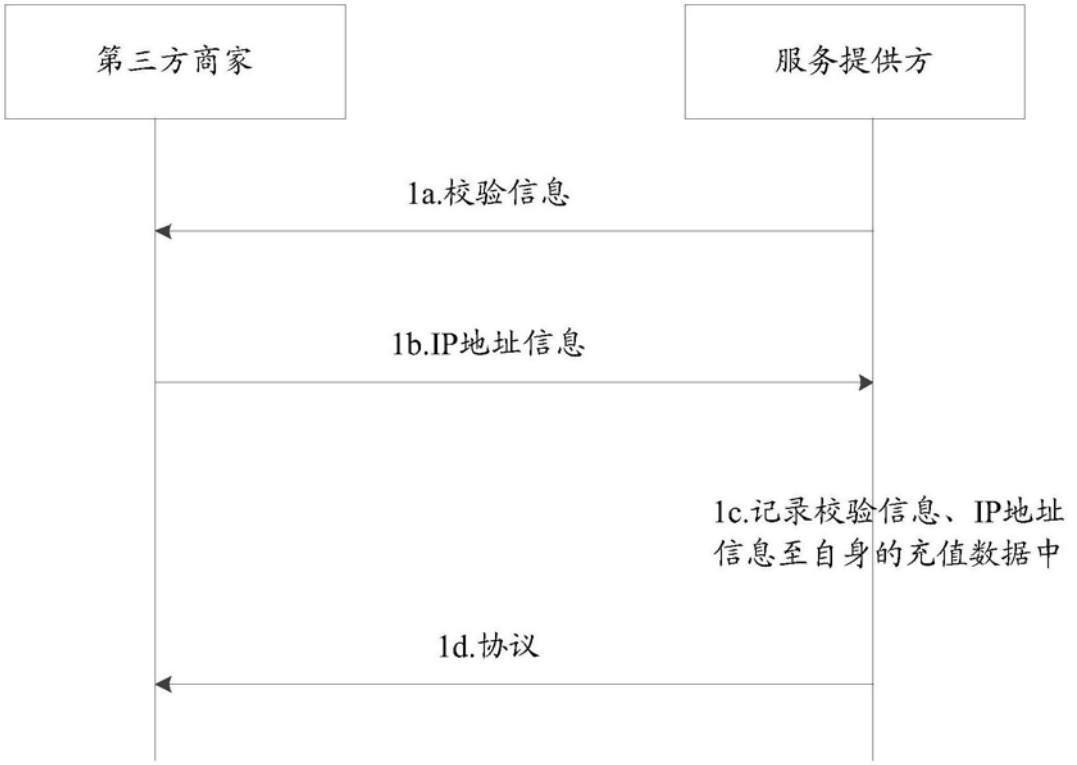

第三方商家
服务提供方
1a.校验信息
1b.IP地址信息
1c.记录校验信息、IP地址信息至自身的充值数据中
1d.协议

图6

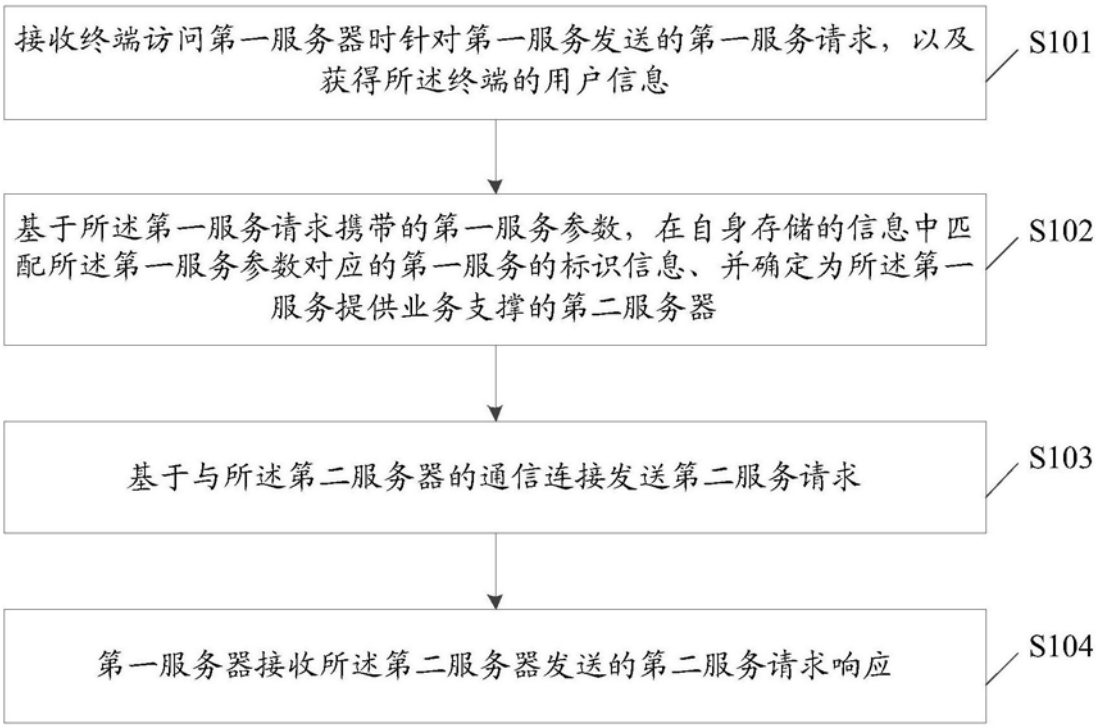

接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端的用户信息
S101
基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器
S102
基于与所述第二服务器的通信连接发送第二服务请求
S103
第一服务器接收所述第二服务器发送的第二服务请求响应
S104

图7

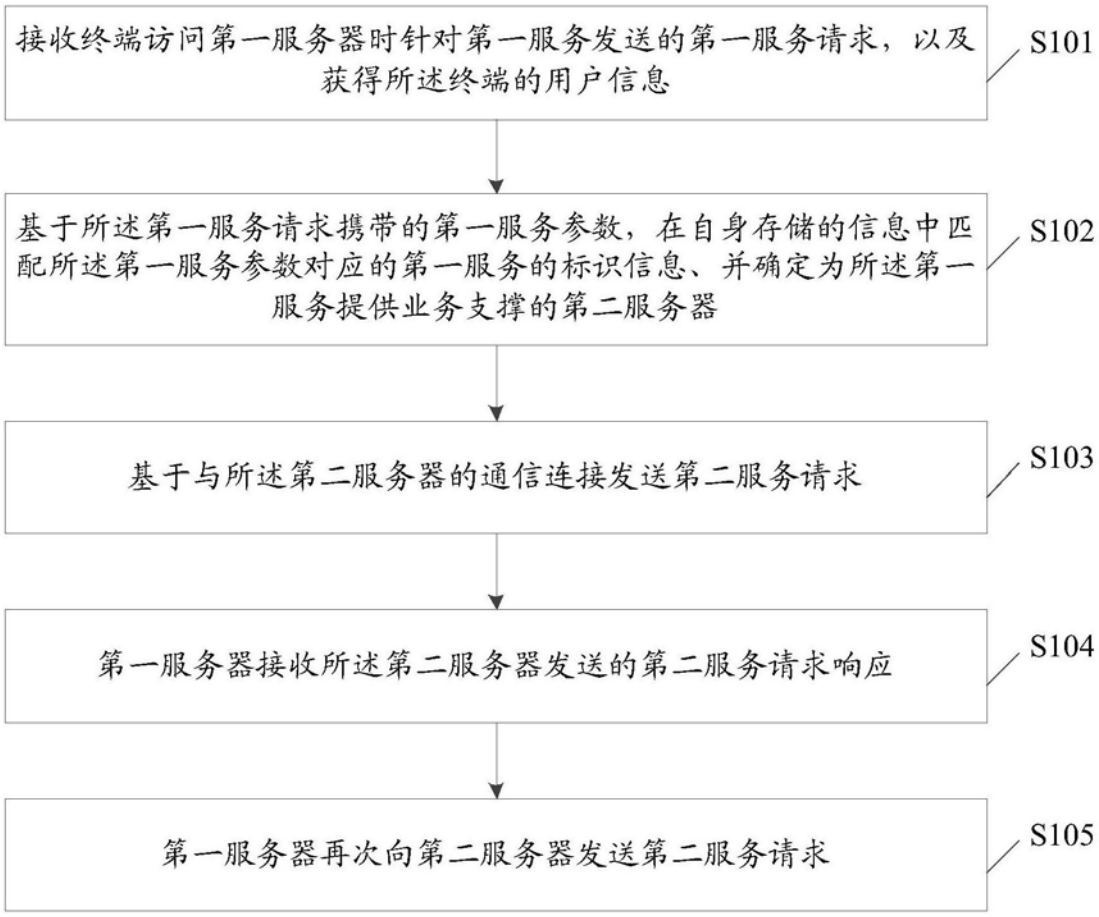

接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端的用户信息
S101
基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器
S102
基于与所述第二服务器的通信连接发送第二服务请求
S103
第一服务器接收所述第二服务器发送的第二服务请求响应
S104
第一服务器再次向第二服务器发送第二服务请求
S105

图8

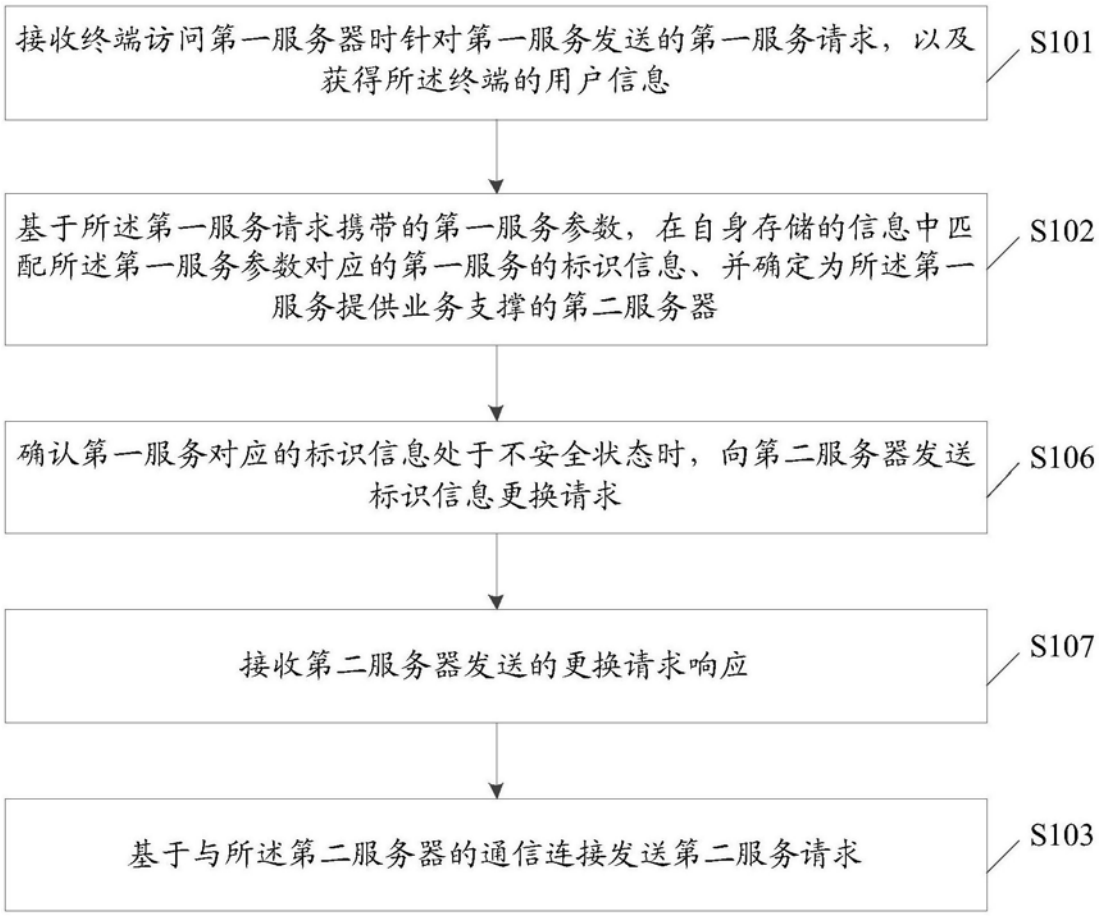

接收终端访问第一服务器时针对第一服务发送的第一服务请求，以及获得所述终端的用户信息
S101
基于所述第一服务请求携带的第一服务参数，在自身存储的信息中匹配所述第一服务参数对应的第一服务的标识信息、并确定为所述第一服务提供业务支撑的第二服务器
S102
确认第一服务对应的标识信息处于不安全状态时，向第二服务器发送标识信息更换请求
S106
接收第二服务器发送的更换请求响应
S107
基于与所述第二服务器的通信连接发送第二服务请求
S103

图9

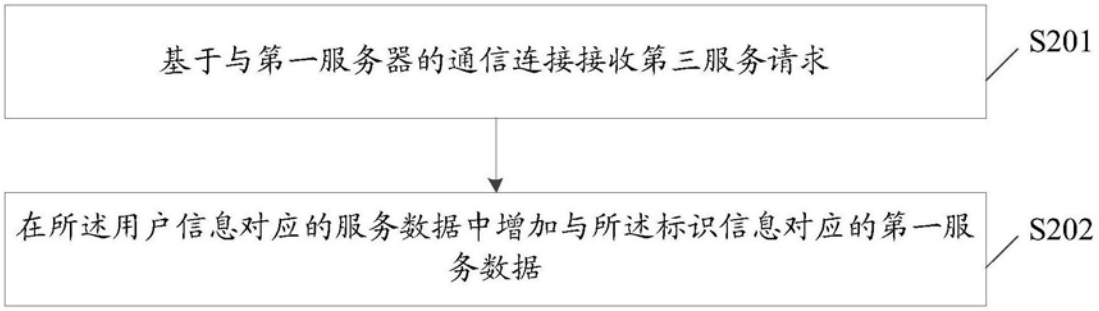

基于与第一服务器的通信连接接收第三服务请求
S201
在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据
S202

图10

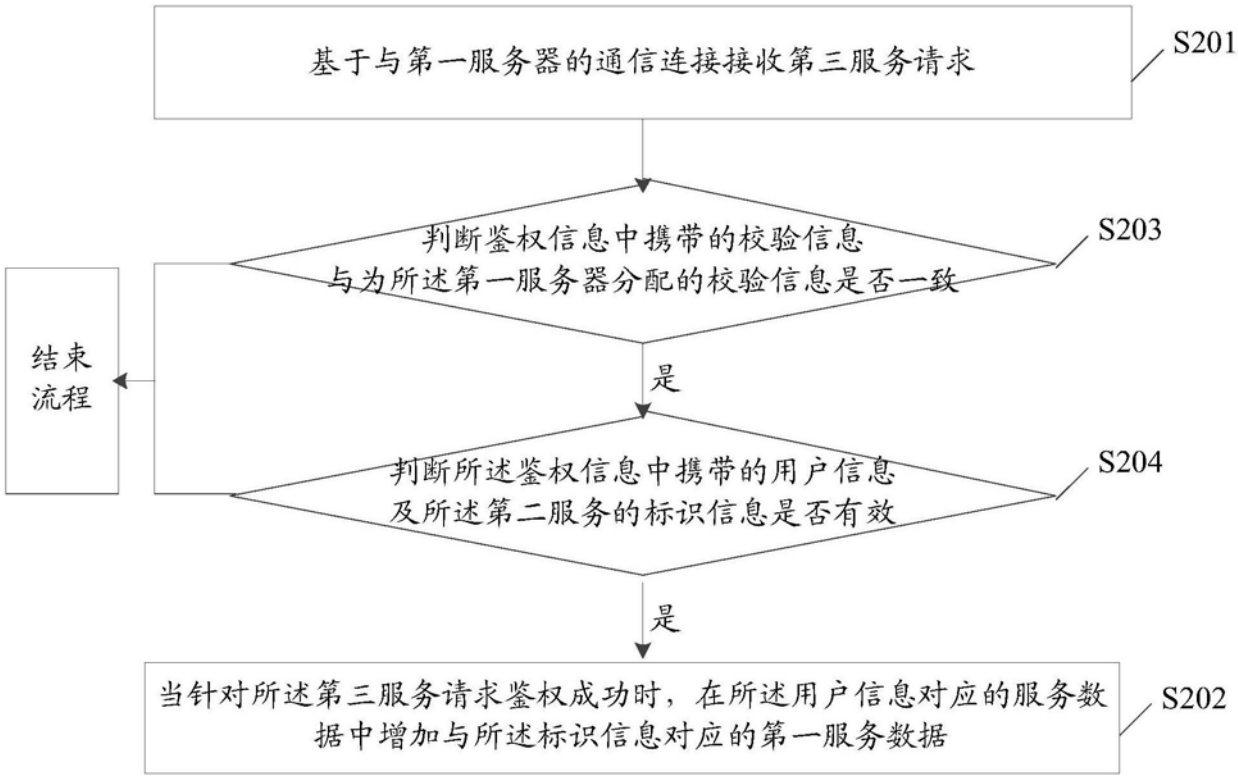

基于与第一服务器的通信连接接收第三服务请求
S201
判断鉴权信息中携带的校验信息
与为所述第一服务器分配的校验信息是否一致
S203
结束
流程
是
判断所述鉴权信息中携带的用户信息
及所述第二服务的标识信息是否有效
S204
是
当针对所述第三服务请求鉴权成功时，在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据
S202

图11

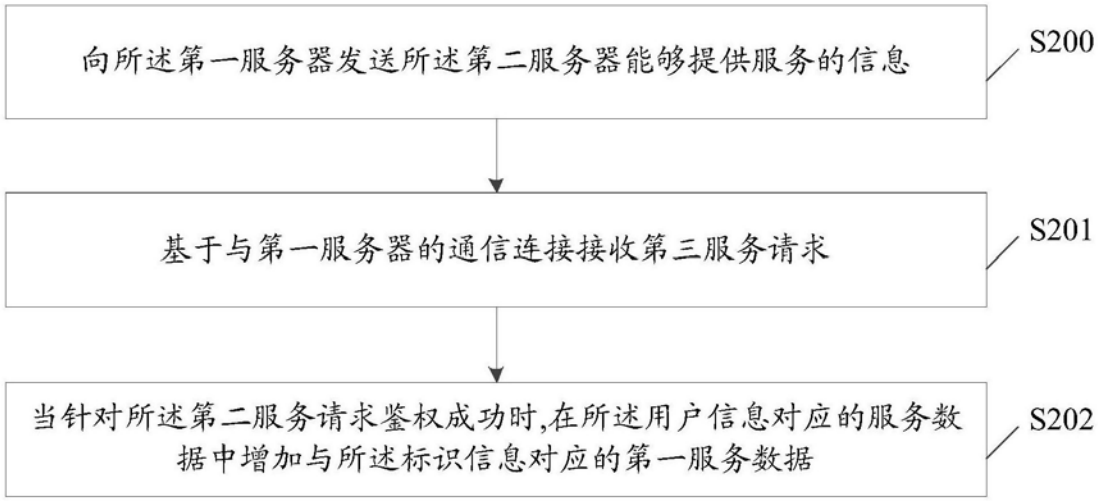

向所述第一服务器发送所述第二服务器能够提供服务的信息
S200
基于与第一服务器的通信连接接收第三服务请求
S201
当针对所述第二服务请求鉴权成功时,在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据
S202

图12

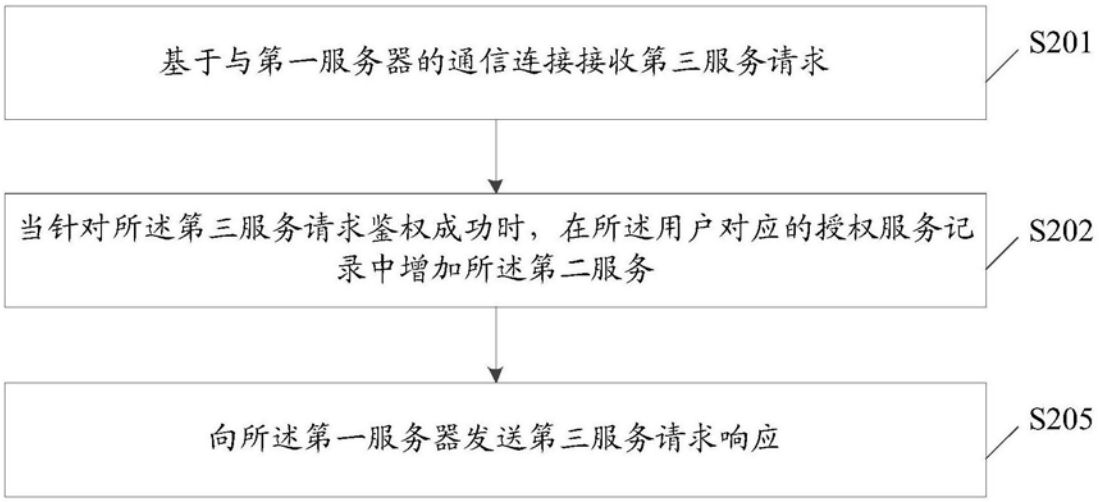

基于与第一服务器的通信连接接收第三服务请求
S201
当针对所述第三服务请求鉴权成功时，在所述用户对应的授权服务记录中增加所述第二服务
S202
向所述第一服务器发送第三服务请求响应
S205

图13

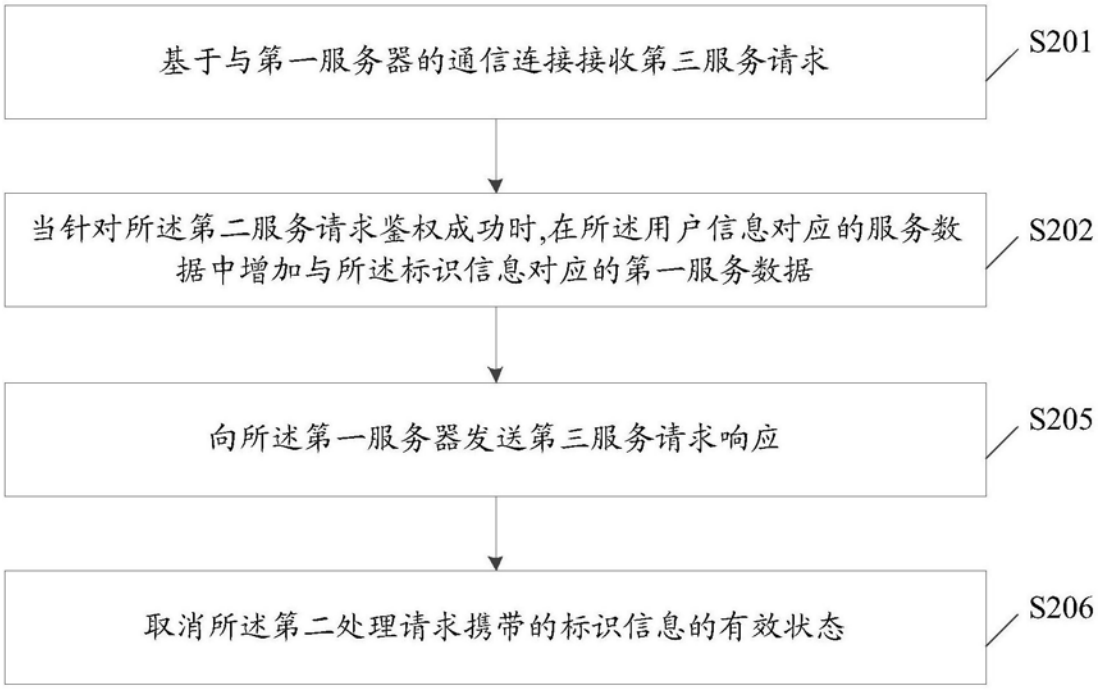

基于与第一服务器的通信连接接收第三服务请求
S201
当针对所述第二服务请求鉴权成功时,在所述用户信息对应的服务数据中增加与所述标识信息对应的第一服务数据
S202
向所述第一服务器发送第三服务请求响应
S205
取消所述第二处理请求携带的标识信息的有效状态
S206

图14

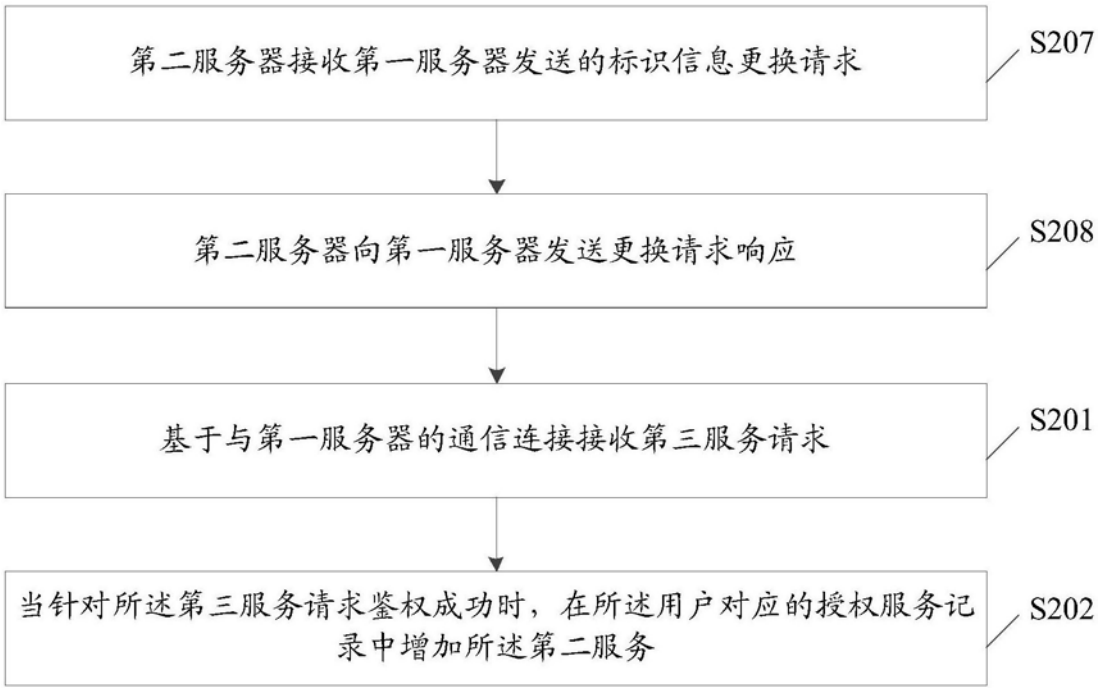

第二服务器接收第一服务器发送的标识信息更换请求
S207
第二服务器向第一服务器发送更换请求响应
S208
基于与第一服务器的通信连接接收第三服务请求
S201
当针对所述第三服务请求鉴权成功时，在所述用户对应的授权服务记录中增加所述第二服务
S202

图15

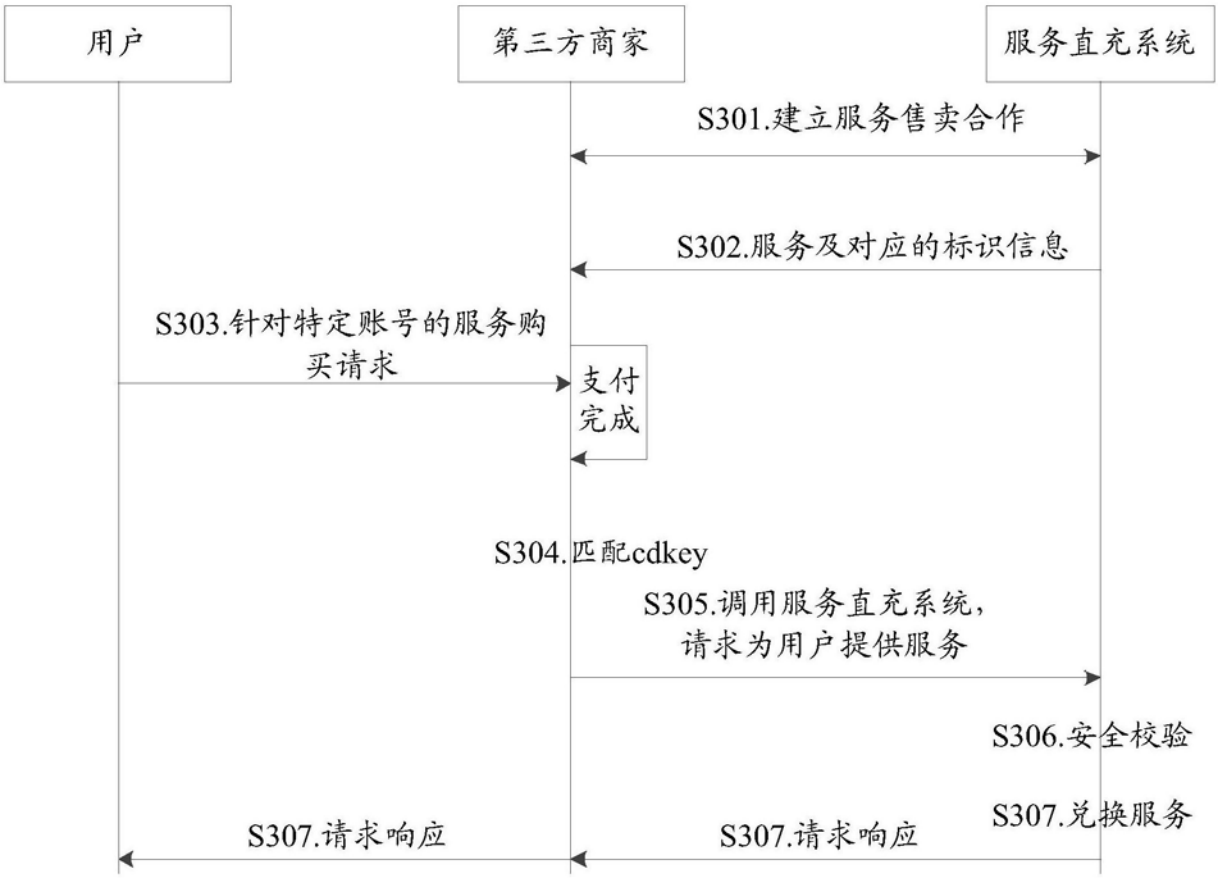

用户
第三方商家
服务直充系统
S301.建立服务售卖合作
S302.服务及对应的标识信息
S303.针对特定账号的服务购买请求
支付完成
S304.匹配cdkey
S305.调用服务直充系统，请求为用户提供服务
S306.安全校验
S307.兑换服务
S307.请求响应
S307.请求响应

图16

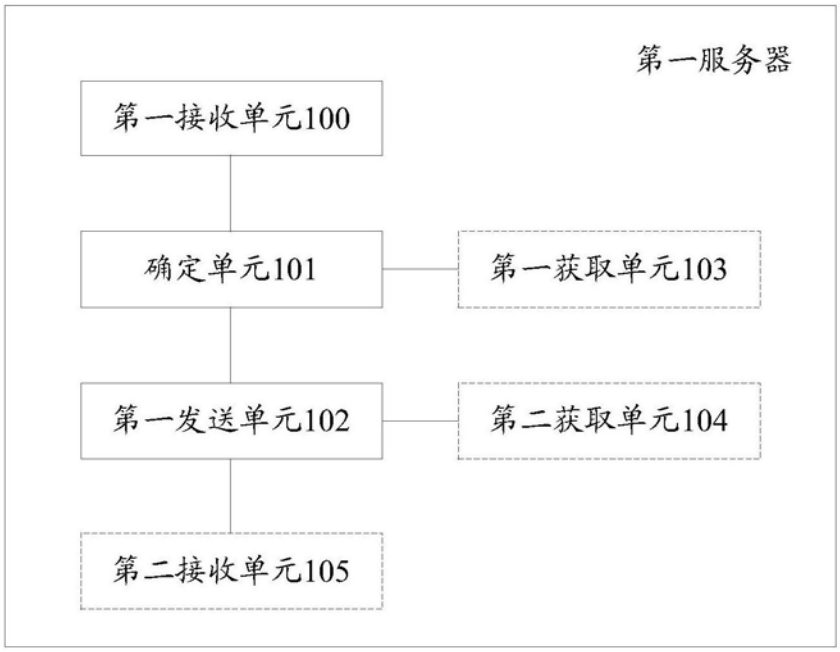

第一服务器
第一接收单元100
确定单元101
第一获取单元103
第一发送单元102
第二获取单元104
第二接收单元105

图17

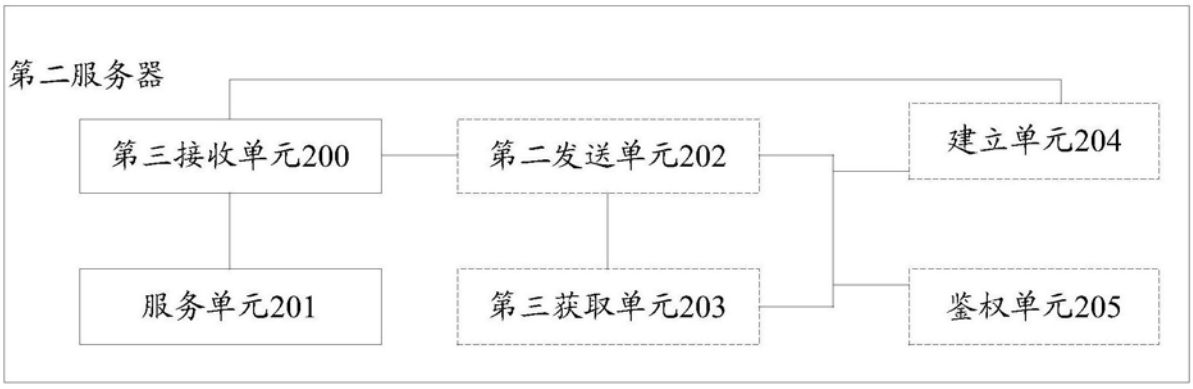

第二服务器
第三接收单元200
第二发送单元202
建立单元204
服务单元201
第三获取单元203
鉴权单元205

图18

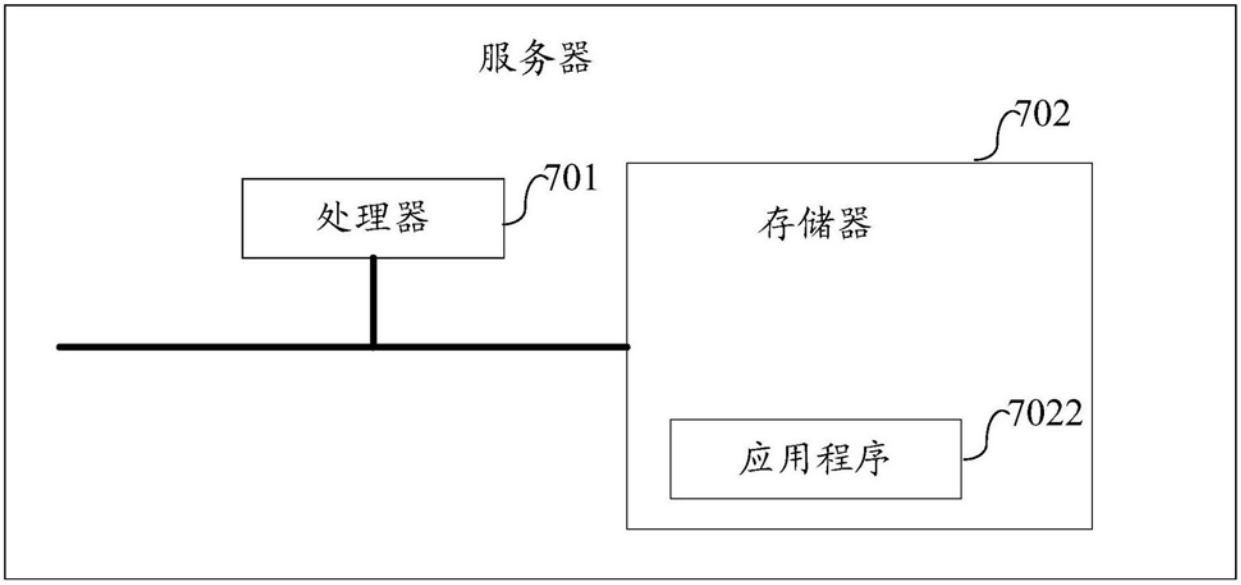


图19