



(12) 发明专利

(10) 授权公告号 CN 106910063 B

(45) 授权公告日 2020.10.27

(21) 申请号 201510973539.X

G06Q 20/40 (2012.01)

(22) 申请日 2015.12.22

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 102855560 A, 2013.01.02

申请公布号 CN 106910063 A

CN 104268746 A, 2015.01.07

(43) 申请公布日 2017.06.30

CN 101046870 A, 2007.10.03

CN 104240073 A, 2014.12.24

(73) 专利权人 卓望数码技术(深圳)有限公司

审查员 于芝枝

地址 518057 广东省深圳市南山区高新技

术产业园南区深港产学研基地大楼西

座六楼南翼

(72) 发明人 霍要峰 刘忠诚 王巍

(74) 专利代理机构 深圳市顺天达专利商标代理

有限公司 44217

代理人 李琴

(51) Int. Cl.

G06Q 20/38 (2012.01)

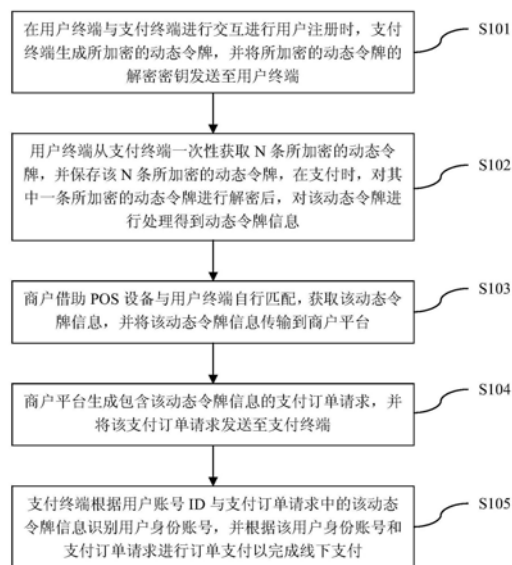
权利要求书2页 说明书6页 附图1页

(54) 发明名称

一种线下支付方法及系统

(57) 摘要

本发明提供了一种线下支付方法,该方法包括:支付终端生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端;用户终端从支付终端一次性获取N条所加密的动态令牌,并保存该N条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息;POS设备与用户终端自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台;商户平台生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端;支付终端根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付。本发明还提供了对应的线下支付系统。



1. 一种线下支付方法,其特征在于,所述方法包括:

S0、在用户终端与支付终端进行交互以进行用户注册时,支付终端生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端;

S1、用户终端从支付终端一次性获取多条所加密的动态令牌,并保存该多条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息并向商户展示该动态令牌信息;

S2、商户借助POS设备与用户终端自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台;

S3、商户平台生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端;

S4、支付终端根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付;

其中,所述方法还包括:在步骤S1中用户终端向商户展示该动态令牌信息之后,用户终端自动删除本地缓存的该条所加密的动态令牌。

2. 根据权利要求1中所述的线下支付方法,其特征在于,在所述步骤S0中,所述生成所加密的动态令牌的步骤包括:

为用户终端分配用户账户ID,并为该用户账户ID分配种子值;

根据该用户账户ID和该种子值预先生成N条动态令牌;

使用非对称加密算法的加密公钥对每个动态令牌进行加密。

3. 根据权利要求2中所述的线下支付方法,其特征在于,所述步骤S0进一步包括:

用户终端在接收到所加密的动态令牌的该解密密钥时通过对称加密算法将该解密密钥进行加密,并将生成的密文分段存储在不同位置,其中该解密密钥为非对称解密密钥。

4. 根据权利要求3中所述的线下支付方法,其特征在于,在所述步骤S1中,所述对其中一条所加密的动态令牌进行解密的步骤包括:

组合存储在不同位置的密文得到完整的密文;

通过对称加密算法对该完整的密文进行解密得到解密密钥;

使用该解密密钥来解密该所加密的动态令牌。

5. 根据权利要求1中所述的线下支付方法,其特征在于,所述动态令牌信息包括动态令牌以及由动态令牌同时转换的条形码和二维码。

6. 一种线下支付系统,其特征在于,所述线下支付系统包括用户终端、支付终端、商户平台和POS设备,其中:

所述支付终端用于在用户终端与支付终端进行交互以进行用户注册时,生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端;

所述用户终端用于从支付终端一次性获取多条所加密的动态令牌,并保存该多条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息并向商户展示该动态令牌信息;

所述POS设备用于与用户终端自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台;

所述商户平台用于生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发

送至支付终端；

所述支付终端还用于根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付；

所述用户终端还用于在向商户展示该动态令牌信息之后,自动删除本地缓存的该条所加密的动态令牌。

7.根据权利要求6中所述的线下支付系统,其特征在于,所述支付终端包括身份认证服务平台,所述身份认证服务平台用于生成所加密的动态令牌的步骤包括:

为用户终端分配用户账户ID,并为该用户账户ID分配种子值;

根据该用户账户ID和该种子值预先生成N条动态令牌;

使用非对称加密算法的加密公钥对每个动态令牌进行加密。

8.根据权利要求7中所述的线下支付系统,其特征在于,所述用户终端还用于在接收到所加密的动态令牌的该解密密钥时通过对称加密算法将该解密密钥进行加密,并将生成的密文分段存储在不同位置,其中该解密密钥为非对称解密密钥。

9.根据权利要求8中所述的线下支付系统,其特征在于,所述用户终端上安装有安全认证组件,所述安全认证组件用于对其中一条所加密的动态令牌进行解密的步骤包括:

组合存储在不同位置的密文得到完整的密文;

通过对称加密算法对该完整的密文进行解密得到解密密钥;

使用该解密密钥来解密该所加密的动态令牌。

10.根据权利要求6中所述的线下支付系统,其特征在于,所述动态令牌信息包括动态令牌以及由动态令牌同时转换的条形码和二维码。

一种线下支付方法及系统

技术领域

[0001] 本发明涉及电子商务技术领域,更具体地说,涉及一种线下支付方法及系统。

背景技术

[0002] 当前移动电子商务线下消费交易日趋流行,在完成交易的支付过程中,用户身份识别主要是按照短信验证码、NFC(Near Field Communication,近场通信)等方式实现。

[0003] 短信验证码方式是业务系统服务器向用户手机推送短信验证码,用户向商家提供短信验证码,商家在终端设备上输入用户的短信验证码后,识别用户账户身份,将账户信息、交易信息组成订单,发到业务系统服务器,完成支付交易。整个用户识别的过程简单方便,但是无法防止暴力破解、黑客入侵等不安全因素,以及短信验证码下发延迟导致的用户体验不佳。

[0004] NFC方式是用户使用NFC手机在受理环境上刷手机,通过近场通信方式完成用户账户信息的获取,进而完成支付交易,但是NFC方式需要用户更换支持NFC的终端,甚至要更换NFC-SWP的SIM卡,用户使用门槛较高,商家需要改造受理环境,增加额外的成本。

[0005] 总之,在移动电子商务快速发展的新形势下,随着O2O模式的不断深入,移动终端能力的不断增强,简单的验证码方式识别或通过NFC设备近场通信技术实现的识别方法,已经不能满足这种线下电子商务的新模式,因此,为了保证用户、电子商务平台、商家的共同利益,促进产业链的可持续发展,寻求一种全新的、更加安全、更加方便快捷,有着更好用户体验的线下消费交易支付方法成为亟待解决的问题。

发明内容

[0006] 本发明要解决的技术问题在于,针对现有移动电子商务线下消费交易支付的上述缺陷,以及更加安全、方便的线下消费交易支付方法的必然性,提供一种线下支付方法及系统。

[0007] 本发明解决上述问题的技术方案是提供了一种线下支付方法,所述方法包括:

[0008] S0、在用户终端与支付终端进行交互以进行用户注册时,支付终端生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端;

[0009] S1、用户终端从支付终端一次性获取N条所加密的动态令牌,并保存该N条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息,其中N为正整数;

[0010] S2、商户借助POS设备与用户终端自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台;

[0011] S3、商户平台生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端;

[0012] S4、支付终端根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付。

- [0013] 在上述线下支付方法中,在所述步骤S0中,所述生成所加密的动态令牌的步骤包括:
- [0014] 为用户终端分配用户账户ID,并为该用户账户ID分配种子值;
- [0015] 根据该用户账户ID和该种子值预先生成N条动态令牌;
- [0016] 使用非对称加密算法的加密公钥对每个动态令牌进行加密。
- [0017] 在上述线下支付方法中,所述步骤S0进一步包括:
- [0018] 用户终端在接收到所加密的动态令牌的该解密密钥时通过对称加密算法将该解密密钥进行加密,并将生成的密文分段存储在不同位置,其中该解密密钥为非对称解密密钥。
- [0019] 在上述线下支付方法中,在所述步骤S1中,所述对其中一条所加密的动态令牌进行解密的步骤包括:
- [0020] 组合存储在不同位置的密文得到完整的密文;
- [0021] 通过对称加密算法对该完整的密文进行解密得到解密密钥;
- [0022] 使用该解密密钥来解密该所加密的动态令牌。
- [0023] 在上述线下支付方法中,所述动态令牌信息包括动态令牌以及由动态令牌同时转换的条形码和二维码。
- [0024] 本发明还提供了一种线下支付系统,所述线下支付系统包括用户终端、支付终端、商户平台和POS设备,其中:
- [0025] 所述支付终端用于在用户终端与支付终端进行交互以进行用户注册时,生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端;
- [0026] 所述用户终端用于从支付终端一次性获取N条所加密的动态令牌,并保存该N条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息;
- [0027] 所述POS设备用于与用户终端自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台;
- [0028] 所述商户平台用于生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端;
- [0029] 所述支付终端还用于根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付。
- [0030] 在上述线下支付系统中,所述支付终端包括身份认证服务平台,所述身份认证服务平台用于生成所加密的动态令牌的步骤包括:
- [0031] 为用户终端分配用户账户ID,并为该用户账户ID分配种子值;
- [0032] 根据该用户账户ID和该种子值预先生成N条动态令牌;
- [0033] 使用非对称加密算法的加密公钥对每个动态令牌进行加密。
- [0034] 在上述线下支付系统中,所述用户终端还用于在接收到所加密的动态令牌的该解密密钥时通过对称加密算法将该解密密钥进行加密,并将生成的密文分段存储在不同位置,其中该解密密钥为非对称解密密钥。
- [0035] 在上述线下支付系统中,所述用户终端上安装有安全认证组件,所述安全认证组件用于对其中一条所加密的动态令牌进行解密的步骤包括:

- [0036] 组合存储在不同位置的密文得到完整的密文；
- [0037] 通过对称加密算法对该完整的密文进行解密得到解密密钥；
- [0038] 使用该解密密钥来解密该所加密的动态令牌。
- [0039] 在上述线下支付系统中，所述动态令牌信息包括动态令牌以及由动态令牌同时转换的条形码和二维码。
- [0040] 本发明的线下支付方法及系统的有益效果有：通过支付终端生成所加密的动态令牌，用户终端一次性从支付终端获取N条所解密的动态令牌，增强了线下支付交易的便捷性，使消费验证流程简单快速，用户体验良好。支付终端生成所加密的动态令牌，用户终端对动态令牌的解密密钥进行加密处理，增强线下支付交易的用户账户信息的安全，可靠，避免资金风险。通过用户注册时的用户账户ID与动态令牌的匹配，快速识别用户账户，降低线下支付用户身份识别的验证成本，进而降低线上电子商务与线下消费的成本投入。

附图说明

- [0041] 图1是本发明的线下支付系统的结构示意图。
- [0042] 图2是本发明的线下支付方法实施例的流程图。

具体实施方式

- [0043] 为了使本发明的目的、技术方案及优点更加清楚明白，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用以解释本发明，并不用于限定本发明。
- [0044] 如图1所示，是本发明的线下支付系统的结构示意图。该系统包括支付终端10、用户终端20、POS设备30和商户平台40。
- [0045] 其中，支付终端10用于在用户终端与支付终端进行交互以进行用户注册时，生成所加密的动态令牌，并将所加密的动态令牌的解密密钥发送至用户终端。支付终端10包括支付平台101和身份认证服务平台102，该支付平台101与该身份认证服务平台102交互，该身份认证服务平台102用于提供集中统一的身份认证鉴权服务接口，生成所加密的动态令牌，并将所加密的动态令牌的解密密钥发送至用户终端20。
- [0046] 支付终端10还用于根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号，并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付。具体地，该身份认证服务平台102还用于根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号，即通过动态令牌与用户账户ID的匹配，完成用户账号身份的识别；该支付平台101为银行的核心系统，根据该用户身份账号和支付订单请求进行订单支付，完成支付交易。
- [0047] 用户终端20用于从支付终端10一次性获取N条所加密的动态令牌，并保存该N条所加密的动态令牌，在支付时，对其中一条所加密的动态令牌进行解密后对该动态令牌经常处理得到动态令牌信息。用户终端20上安装有支付APP 201和安全认证组件202，该支付APP 201支持在线远程、近程支付，该安全认证组件202通过SDK与该支付APP 201集成，用于接收和存储所加密的动态令牌，并在使用所加密的动态令牌时，对所加密的动态令牌进行解密；支付APP 201展示动态令牌，接收POS设备的扫描，进而将代表用户账号身份的动态令牌传

输至商户平台40。

[0048] POS设备30为线下支付受理环境,支持条形码、二维码等扫描来采集输入用户信息,用于与用户终端20自行匹配,获取动态令牌信息,并将该动态令牌信息传输至商户平台40。

[0049] 商户平台40与POS设备30交互,接收POS设备30传输的动态令牌信息,并输入交易信息,用于生成包含动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端10。

[0050] 如图2所示,是本发明的线下支付方法实施例的流程图。参考图2,将结合上述图1中的线下支付系统,对线下支付方法进行详细说明,该方法包括以下步骤:

[0051] 在步骤S101中,在用户终端20与支付终端10进行交互进行用户注册时,支付终端10生成所加密的动态令牌,并将所加密的动态令牌的解密密钥发送至用户终端。其中,用户终端20的安全认证组件202与支付终端10的身份认证服务平台102交互进行用户注册,并且,支付终端10生成所加密的动态令牌的步骤包括:首先,支付终端10为该用户终端20分配用户账户ID,并为该用户账户ID分配种子值。随后,支付终端10根据该用户账户ID和种子值预先生成N条动态令牌。具体地,每个动态令牌是由支付终端10的安全认证服务平台102生成固定长度的数字串,在本发明的实施例中,每个动态令牌的有效期为 $\text{TokenCode} = H(\text{Seed} + \text{ID} + \text{Time})$,其中,Seed表示种子值,ID表示用户账户ID,Time表示时间戳,通过动态令牌可以查询定位到用户账户ID、时效周期等。最后,支付终端10使用非对称加密算法的加密公钥对每个动态令牌进行加密,其中非对称加密算法可以为RSA、SM2等。

[0052] 进一步地,在本发明的一些实施例中,用户终端20在接收到所加密的动态令牌的解密密钥时,通过对称加密算法将解密密钥进行加密,并将生成的密文分段存储在不同位置。具体地,用户终端20的安全认证组件202通过对称加密算法将解密密钥进行加密,其中对称加密算法可以为DES、SM4等。

[0053] 进一步地,为了有效避免了因用户终端被逆向工程后而导致的算法及密钥泄漏,用户终端20将对称加密算法的解密方法文件加密成dat文件,以实现逻辑隐藏,此时用户终端的源代码中看不到动态令牌的解密方法及密钥,这样可避免对称加密算法及其对应的密钥泄漏。并且,该dat文件存放在库文件.so中,并对该库文件.so进行加固处理,可防止破解反编译,保障解密方法及密钥的安全性。

[0054] 在步骤S102中,用户终端20从支付终端10一次性获取N条所加密的动态令牌,并保存该N条所加密的动态令牌,在支付时,对其中一条所加密的动态令牌进行解密后,对该动态令牌进行处理得到动态令牌信息。具体地,用户终端20的安全认证组件202与支付终端10的身份认证服务平台102进行交互来获取N条所加密的动态令牌。其中,N为正整数,可以根据具体的情况任意设定。

[0055] 在本发明的实施例中,用户终端20在支付时使用其中一条所加密的动态令牌,先对该所加密的动态令牌进行解密,具体地,首先组合存储在不同位置的密文得到完整的密文,接着,通过对称加密算法对该完整的密文进行解密得到解密密钥,最后,使用该解密密钥来解密该所加密的动态令牌。对所加密的动态令牌进行解密的解密密钥对应于支付终端生成所加密的动态令牌时所采用的加密算法,在生成所加密的动态令牌时,采用非对称加密算法的加密密钥对动态令牌进行加密,则对所加密的动态令牌进行解密的解密密钥为非

对称解密密钥,同样地,采用对称加密算法的加密密钥对动态令牌进行加密,则对所加密的动态令牌进行解密的解密密钥为对称解密密钥。

[0056] 进一步地,对动态令牌进行处理得到动态令牌信息的步骤包括:首先将该动态令牌同时转换为条形码和二维码,该动态令牌信息包括该条形码、二维码以及该动态令牌;随后,通过用户终端20的支付APP 201向商户展示该动态令牌、条形码和二维码。此时,支付APP 201展示了该动态令牌,用户终端20则自动删除本地缓存,这样,在每次线下支付时支付APP均展示不同的动态令牌。

[0057] 进一步地,在本发明的另一实施例中,用户终端20间隔预设时间自动与支付终端交互更新所加密的动态令牌。当然用户也可手动建立用户终端与支付终端的交互以更新所加密的动态令牌。进一步地,在用户终端从支付终端获取到一条新的所加密的动态令牌,则自动删除其中一条旧的所加密的动态令牌,这样保证每个用户终端有且仅有N条有效动态令牌可用,保证线下支付的安全性。

[0058] 在步骤S103中,商户借助POS设备30与用户终端20自行匹配,获取该动态令牌信息,并将该动态令牌信息传输到商户平台40。例如,商户可以手动输入用户终端20的支付APP 201展示的固定长度的数字串,也可通过扫描方式来扫描条形码或二维码。在本发明的一些实施例中,在用户终端处于网络状态时,商户借助POS设备获取该动态令牌信息后,用户终端与支付终端进行交互,并将POS设备获取到的动态令牌信息设置为失效状态。

[0059] 在步骤S104中,商户平台40生成包含该动态令牌信息的支付订单请求,并将该支付订单请求发送至支付终端10,该支付订单请求包含上述动态令牌信息、支付金额、商户的收款账号信息等等。在本发明的一些实施例中,商户平台40可与支付终端10建立HTTP连接,通过该HTTP连接将该支付订单请求发送至支付终端。在发送完毕之后,商户平台等候来自支付终端的应答。

[0060] 在步骤S105中,支付终端10根据用户账户ID与支付订单请求中的该动态令牌信息识别用户身份账号,并根据该用户身份账号和支付订单请求进行订单支付以完成线下支付。

[0061] 在本发明的另一实施例中,在用户终端进行了M次线下支付时,意味着已经使用了M条动态令牌,其中,M小于N,该线下支付方法还包括:在用户终端开启网络时,用户终端的安全认证组件自动联网与支付终端的安全认证服务平台交互,并增加M条所加密的动态令牌。

[0062] 在用户终端进行了N次线下支付时,此时所加密的动态令牌已被使用完,该线下支付方法还包括:提示用户开启用户终端的网络以重新获取N条所加密的动态令牌。

[0063] 本发明的线下支付方法及系统,首先,通过支付终端生成所加密的动态令牌,用户终端一次性从支付终端获取N条所解密的动态令牌,增强了线下支付交易的便捷性,使消费验证流程简单快速,用户体验良好。其次,支付终端生成所加密的动态令牌,用户终端对动态令牌的解密密钥进行加密处理,增强线下支付交易的用户账户信息的安全,可靠,避免资金风险。最后,通过用户注册时的用户账户ID与动态令牌的匹配,快速识别用户账户,降低线下支付用户身份识别的验证成本,进而降低线上电子商务与线下消费的成本投入。

[0064] 以上所述,仅为本发明较佳的具体实施方式,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,可轻易想到的变化或替换,

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该以权利要求的保护范围为准。

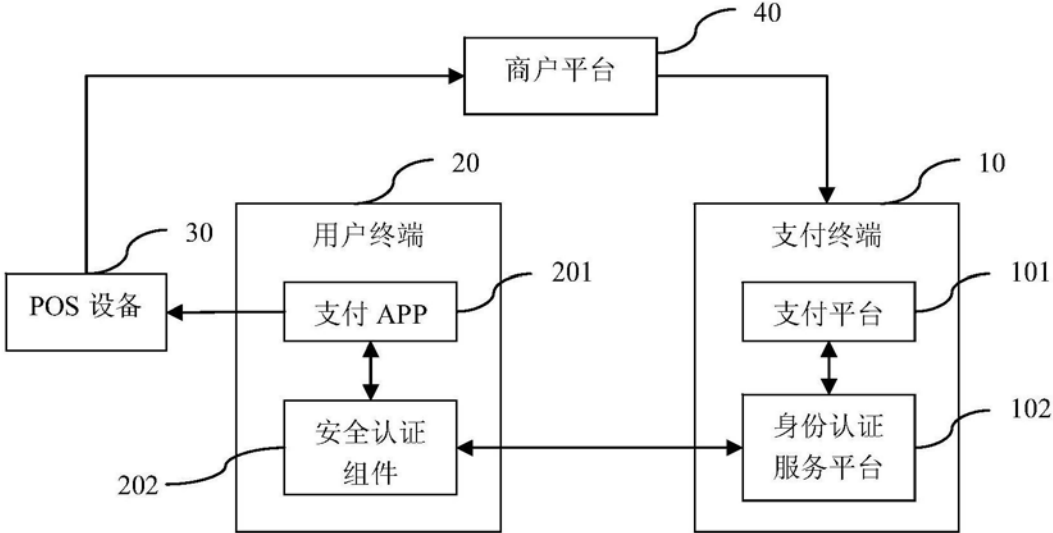


图1

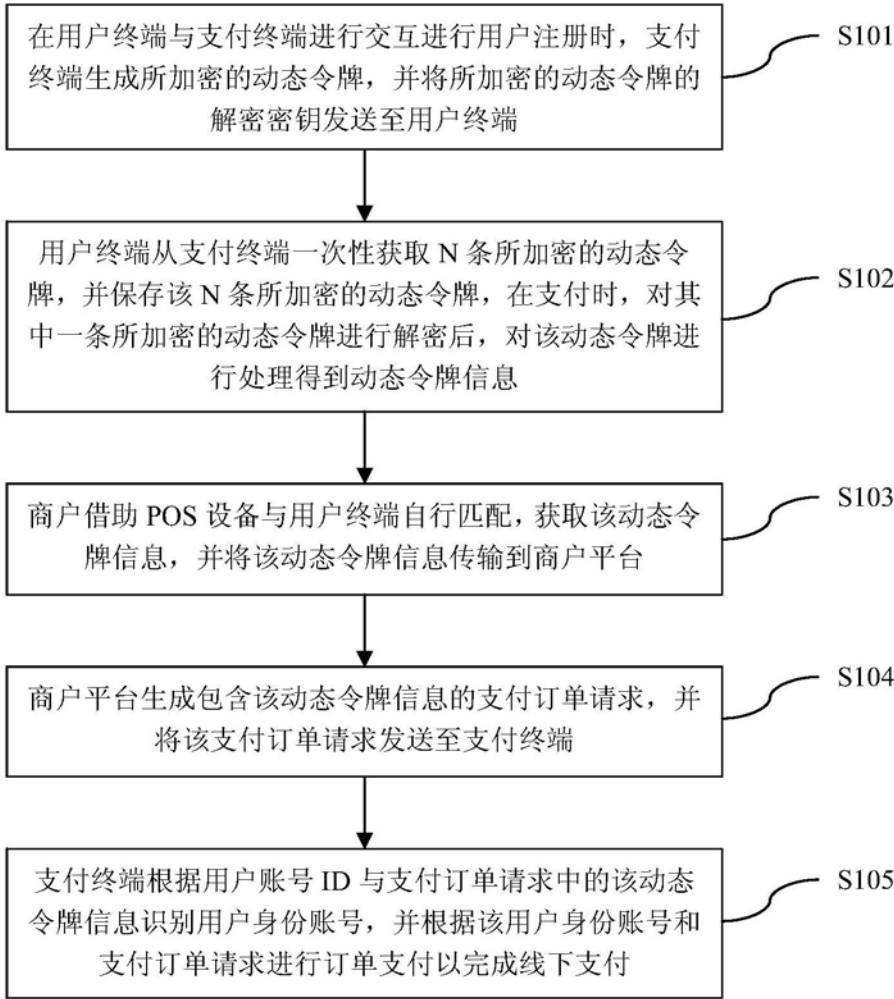


图2