(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 104272332 B
(45)授权公告日 2018.10.23

(21)申请号 201280069962.1
(22)申请日 2012.12.19
(65)同一申请的已公布的文献号
申请公布号 CN 104272332 A
(43)申请公布日 2015.01.07
(30)优先权数据
61/577,652 2011.12.19 US
13/448,193 2012.04.16 US
(85)PCT国际申请进入国家阶段日
2014.08.19
(86)PCT国际申请的申请数据
PCT/US2012/070683 2012.12.19
(87)PCT国际申请的公布数据
WO2013/096486 EN 2013.06.27
(73)专利权人 希昆软件公司
地址 美国加利福尼亚州
(72)发明人 D·布鲁德尼奇 M·卡拉夫特 H·瑞斯基斯 A·韦恩斯坦
(74)专利代理机构 北京市中伦律师事务所 11410
代理人 张思悦 贾媛媛
(51)Int.Cl.
G06Q 20/22(2012.01)
G06Q 20/32(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
(56)对比文件
US 2011/0153498 A1,2011.06.23,
US 2011/0218868 A1,2011.09.08,
US 2006/0122921 A1,2006.06.08,
CN 101960480 A,2011.01.26,
US 2008/0116264 A1,2008.05.22,
审查员 廖雯雯

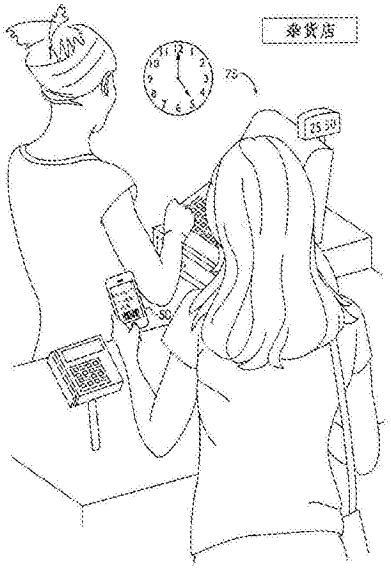
权利要求书3页 说明书13页 附图14页

(54)发明名称

用于便携式通信设备中动态临时支付授权的系统和方法

(57)摘要

一种用于使用动态临时凭证的系统，所述动态临时凭证与便携式通信设备用于与电子控制点(例如销售点、NFC访问点)的交易中来，所述便携式通信设备具有地理位置模块(例如GPS)。所述系统具有集中式模块，所述集中式模块接收所述便携式通信设备的当前地理位置，并发送所述动态临时凭证至所述便携式通信设备并且向与所述电子控制点可操作关联的授权系统提供预测的交易信息—包括所述动态临时凭证和便携式通信设备的地理位置。所述动态临时凭证具有预定的有效时间，其允许循环使用所述动态凭证，这样的循环使用可考虑到近期发布所述凭证的地理位置。也公开了一种采用便携式通信设备使用动态临时凭证的方法。



CN 104272332 B

1.一种用于发布动态临时凭证的系统，所述系统向便携式通信设备发布所述动态临时凭证，以在所述便携式通信设备与电子控制点之间的交易中使用，所述便携式通信设备具有提供所述便携式通信设备的当前地理位置的服务，所述系统包括：

与系统管理服务器可操作地相关联的装置，其用于存储用户唯一标识信息，所述用户唯一标识信息包括与所述便携式通信设备的用户相关联的用户名和密码信息；

所述系统管理服务器中的、用于从所述便携式通信设备接收包括由用户所输入的密码和所述便携式通信设备的当前地理位置的信息的装置；

所述系统管理服务器中的、用于认证所述便携式通信设备的用户的装置，所述认证包括验证由用户所输入的密码；

所述系统管理服务器中的、用于在验证所述密码之后使用所述便携式通信设备的当前地理位置确定可能的商家和用于所述可能的商家的电子控制点的类型的装置；

用于通过所述系统管理服务器生成动态临时凭证的装置；

用于将生成的所述动态临时凭证从所述系统管理服务器发送至所述便携式通信设备的装置；

用于将预测交易信息从所述系统管理服务器提供至与所述电子控制点可操作地关联的授权系统的装置，所述预测交易信息包括所述动态临时凭证、用于所述可能的商家的商家标识和用于所述动态临时凭证的预定到期时间；以及

所述授权系统中的、用于使用所述预测交易信息授权来自所述电子控制点的交易请求的装置，所述授权系统验证与所述电子控制点相关联的商家标识匹配所述预测交易信息中的所述可能的商家的商家标识和在授权所述交易请求之前在用于所述动态临时凭证的预定到期时间之前接收所述交易请求这两者。

2.如权利要求1所述的系统，其中所述便携式通信设备具有唯一的数字设备签名，用于存储用户唯一标识信息的装置还包括将所述便携式通信设备的唯一的数字设备签名与所述便携式通信设备的用户相关联，所述认证装置还通过确认所述唯一的数字设备签名和密码都与所述用户相关联来验证所述便携式通信设备的所述用户。

3.如权利要求2所述的系统，其中所述预测交易信息还包括所述便携式通信设备的唯一的数字设备签名。

4.如权利要求1所述的系统，其中所述用于将生成的所述动态临时凭证从所述系统管理服务器发送至所述便携式通信设备的装置还将所述一个或多个可能的商家传输至所述便携式通信设备，所述系统还包括查明装置，所述查明装置用于查明来自所述便携式通信设备的对所述一个或多个可能的商家中的一个的确认，在接收到不匹配的指示时所述查明装置选择其他一个或多个可能的商家。

5.如权利要求4所述的系统，其中所述用于将生成的所述动态临时凭证从所述系统管理服务器发送至所述便携式通信设备的装置还向所述便携式通信设备传输与所述一个或多个可能的商家中的每一个相关联的模拟方法。

6.如权利要求5所述的系统，其中所述预测交易信息还包括与所述一个或多个可能的商家中的每一个相关联的模拟方法。

7.如权利要求1所述的系统，其中所述电子控制点包括销售点终端，而所述认证系统包括具有验证映射网关的商家支付网络。

8.如权利要求7所述的系统，其中所述验证映射网关包括包含所述预测交易信息和传统支付数据的验证数据库。

9.如权利要求8所述的系统，其中所述验证映射网关可操作地连接至一个或多个发布方，所述系统还包括与所述验证映射网关相关联的装置，以在支付交易中，在发送所述支付交易至与所述传统支付数据相关联的发布方之前，用所述传统支付数据取代所述动态临时凭证。

10.如权利要求1所述的系统，其中所述便携式通信设备是第一便携式通信设备，所述动态临时凭证的预定到期时间是分钟数量级的，所述系统还包括第二便携式通信设备和用于循环使用所述动态临时凭证的循环使用装置，其中在预定的有效时间到期之后，当所述第二便携式通信设备位于相对于所述第一便携式通信设备的当前地理位置的第二不同地理位置时，所述循环使用装置使用所述第一便携式通信设备的当前地理位置、所述第二便携式通信设备的地理位置和与所述动态临时凭证相关联的所述预定到期时间，将所述动态临时凭证传输至所述第二便携式通信设备。

11.一种用于在便携式通信设备与电子控制点之间的交易中、与所述便携式通信设备一起使用动态临时凭证的方法，所述便携式通信设备具有提供所述便携式通信设备的当前地理位置的服务，所述方法包括：

在系统管理服务器中从所述便携式通信设备接收由所述便携式通信设备的用户所输入的密码和所述便携式通信设备的当前地理位置；

由所述系统管理服务器通过验证所接收的密码匹配唯一标识数据库中的与所述便携式通信设备的用户相关联的密码来认证所述用户，所述唯一标识数据库与所述系统管理服务器可操作地相关联；

由所述系统管理服务器在认证所述用户之后使用接收的所述便携式通信设备的当前地理位置和与所述系统管理服务器可操作地相关联的商家地理位置集合数据库确定可能的商家和用于所述可能的商家的电子控制点的类型；

生成所述动态临时凭证并将所述动态临时凭证从所述系统管理服务器发送至所述便携式通信设备；

由所述系统管理服务器将预测交易信息提供至与所述电子控制点可操作地关联的授权系统，所述预测交易信息包括所述动态临时凭证、用于所述可能的商家的商家标识和用于所述动态临时凭证的预定到期时间；以及

在所述授权系统处从所述电子控制点接收交易请求，所述交易请求包括商家标识；

其中，所述授权系统使用所述预测交易信息验证由所述电子控制点所发送的所述商家标识匹配所述预测交易信息中的所述可能的商家的商家标识和在授权所述交易请求之前在用于所述动态临时凭证的预定到期时间之前接收所述交易请求这两者。

12.如权利要求11所述的方法，其中所述便携式通信设备具有唯一的数字设备签名，所述唯一的数字设备签名被存储在与所述便携式通信设备的用户相关联的所述唯一标识数据库中，认证所述用户还包括验证所述用户和所述唯一的数字设备签名之间的关联。

13.如权利要求11所述的方法，其中所述方法还包括：

在验证所述商家标识匹配和所述动态临时凭证没有到期后，授权所请求的交易；

用交易记录中与所述便携式通信设备的所述用户相关联的传统卡支付数据取代所述

动态临时凭证;和

将所述交易记录传递至发布方授权系统以使用与所述用户相关联的所述传统卡支付数据进行支付。

用于便携式通信设备中动态临时支付授权的系统和方法

[0001] 本申请要求2011年12月19日提交的美国临时专利申请第61/577,652号和2012年4月16日提交的美国非临时专利申请第13/448,193号的优先权，其每一个通过引用全文并入本文。

技术领域

[0002] 本发明一般涉及使用安全信息完成无线交易，并且更具体地，涉及用于应便携式通信设备的请求处理一次性支付交易的系统和方法，其可基于现实世界地理位置信息。

背景技术

[0003] 使用基于RFID的感应卡的无线交易是相当普遍的。举例来说，许多工人使用RFID钥匙卡获准进入他们的工作场所，而在高速公路上驾驶员使用RFID通行证支付通行费。RFID，表示无线射频标识，为了识别目的而使用电磁波在终端和一些目标之间交换数据。最近，各公司一直在尝试使用移动电话所支持的RFID，以实现电子支付产品(例如信用卡和/或借记卡)。但是，基础RFID技术产生了许多安全问题，促使基础技术的改进。尽管如此，广泛采用RFID技术作为电子支付机制的进展缓慢。

[0004] 智能手机在消费者中的普及也迅速增长。已经出现如何使消费者能使用他们现有的手机进行电子支付的挑战。对于这一挑战，具有嵌入式安全元件的手机中的近场通信技术是一个潜在的解决方案。

[0005] 近场通信(NFC)是一种类似FID使用电磁波交换数据的另一种技术。NFC是指定调制方式、编码、传送速度和RF界面的开放标准(参见例如ISO/IEC18092)。不同于RFID，NFC波仅在短距离(几英寸的量级)并在高频率传输。因此，更广泛地采用NFC作为通信平台，因为它为金融交易和访问控制提供了更好的安全性。其他短距离通信协议是已知的并且可以获得接受用于在支持金融交易和访问控制中使用。

[0006] NFC设备已经被用于在某些销售点设备进行支付。但也有许多销售点设备未对NFC通信启用。因此，本发明的目的是提供一种解决方案，使任何智能手机能够在接受传统(legacy)电子支付的商家，用现有的销售点装备进行高度安全的电子支付。

[0007] 另一个问题是与可用的各种不同销售点终端相关联的无数通信协议。所以，举例来说，对与IBM销售点终端成功地无线通信来说必要的协议可以是与对于与NCR终端通信来说必要的协议非常不同的。因此，本发明的目的在于提供一种系统和方法，用于使用地理位置数据(如果可用)来尝试预先确定与便携式通信设备共同定位的零售机构中存在的可能的销售点终端设备。

[0008] 实体商家接受电子形式支付的能力已经在发达国家中大幅增长，并且在发展中国家中正在迅速增长。金融业已经对电子交易开发并部署了严格的系统、方法和要求，以减轻和减少欺诈行为。

[0009] 因此，如本领域普通技术人员应从他们面前的说明书理解的，本发明还寻求提供对前述的机会和相关问题的一种或多种解决方案。本发明的这些和其它的目的和优点对于

本领域技术人员来说也将是从他们面前的附图、说明书和权利要求而显而易见的。预期所有这样的另外的系统、方法、特征和优点包括在本文描述内，本公开内容的范围之内并且由所附权利要求保护。

附图说明

[0010] 为了更好地理解本发明，参照以下附图描述了非限制性和非穷尽的实施方案。在附图中，除非另有规定，类似的附图标记表示在所有不同附图中类似的部分。

[0011] 图1A示例性说明终端用户尝试使用她的便携式通信设备在销售点进行安全的支付交易；

[0012] 图1B示例性说明终端用户的智能手机(即便携式通信设备)和各种子系统包括系统管理后端之间的可操作的互连；

[0013] 图2是示例性说明可与本系统相关的便携式通信设备中的一些逻辑块的框图；

[0014] 图3A和图3B一起示例性说明一次性支付的过程的一个可能的实施方案的流程；

[0015] 图4是示例性说明与图3A和3B的一次性支付处理有关的便携式通信设备与支付生态系统的其余部分之间的信息流的框图；

[0016] 图5、图6和图6A是可布署在智能电话上的示例性钱包用户界面的示例性说明；

[0017] 图7A和7B是由代表性便携式通信设备上的示例性钱包用户界面生成一次性支付凭证的两个可能的实施方案的示例性说明；

[0018] 图8A是示例性说明可与本系统相关的便携式通信设备中的一些逻辑块的方框图；

[0019] 图8B的框图示例性说明可与本系统相关的图8 A的“一次性支付钱包”的框图其他细节；

[0020] 图9A和9B一起示例性说明可在示例性说明的智能手机上运行的用户界面的一个可能的实施方案，进一步示例性说明与联合钱包(federated wallet)相结合的一次性凭证功能的灵活性；

[0021] 图10是构成授权许可一次性支付应用程序查看、选择和/或更改支付子系统中存储的安全数据的系统的一个可能的实施方案的框图。

具体实施方式

[0022] 现在将在下文中参照附图更充分地描述本发明，其形成本发明的一部分，并且其显示，通过示例性说明的方式，可实行本发明的具体的示例性实施方案。但是，本发明也可以许多不同的形式体现并且不应被解释为仅限于本文所阐述的实施方案；更确切地说，提供这些实施方案使得本公开内容彻底和完整，并且向本领域技术人员充分地表达本发明的范围。除其他事项外，本发明可体现为方法或设备。因此，本发明和其要素可以采取全部硬件实施方案，全部软件实施方案或结合软件和硬件方面的实施方案的形式。因此，下面详细描述不应被视为具有限制意义。

[0023] 便携式通信设备

[0024] 本发明提供了可与各种不同的便携式通信设备一起使用的系统和方法，包括但不限于PDA、移动电话、智能电话、笔记本电脑、平板电脑以及优选地包括蜂窝语音和数据服务以及优选地访问消费者可下载的应用程序的其他移动设备。一个这样的便携式通信设备可

以是iPhone、摩托罗拉RAZR或DROID;然而,本发明优选是与平台和设备无关的。例如,便携式通信设备技术平台可以是Microsoft Windows Mobile、Microsoft Windows Phone7、Palm OS、RIM Blackberry OS、Apple OS、Android OS、Symbian、Java或任何其他技术平台。为了本公开内容的目的,已经按照采用通用平台为智能手机优化的特征和界面描述本发明,但本领域技术人员应当理解,所有这样的特征和界面也可以使用并适用于任何其它的平台和/或设备。

[0025] 便携式通信设备包括一个或多个短距离电磁通信设备,诸如NFC、RFID或蓝牙收发器。目前优选的是使用与NFC IP1标准(www.nfcforum.org)兼容的NFC基带,它在与便携式通信设备上的安全元件配对并呈现在"非接支付读卡器"面前(见下文销售点)时,提供了类似点对点数据交换、读写器模式(即,收集来自RFID标签的信息)和非接卡模拟(emulation)(每NFC IP 1和ISO14443标准)的标准功能。如面前有本说明书、附图和权利要求的本领域技术人员所应理解的,NFC IP1标准仅仅是目前的优选实施例,它可以被输出—整体或部分—与任何其它近距离通信标准关联使用。更优选的是,便携式通信设备包括NFC/RFID天线(符合NFC IP 1和ISO14443标准)以启用近场通信。不过,如应理解的,虽然存在甚至更短的范围以及可能的读取问题,但仍可以使用NFC/RFID通信。

[0026] 便携式通信设备还包括移动网络界面,来建立和管理与移动网络运营商的无线通信。移动网络界面使用一个或多个通信协议和技术,包括但不限于,用于移动通信的全球系统(GSM)、3G、4G,码分多址(CDMA)、时分多址(TDMA)、用户数据报协议(UDP)、传输控制协议/因特网协议(TCP/IP)、SMS、通用分组无线业务(GPRS)、WAP、超宽带(UWB)、IEEE 802.16全球微波接入互操作性(WiMAX)、SIP/RTP,或各种其它无线通信协议中的任一种来与移动网络运营商的移动网络进行通信。因此,移动网络界面可以包括收发器、收发设备、或网络界面卡(NIC)。可以预期的是,如面前有本说明书、附图和权利要求的本领域技术人员所应理解的,移动网络界面和短距离电磁通信设备可以共享收发器或收发设备。

[0027] 便携式通信设备还包括位置收发器,其通常可以将设备在地球表面上的物理坐标确定为纬度、经度和高度的函数。这种位置收发器优选使用GPS技术,所以它在本文中可以称为GPS收发器;然而,应当理解的是,位置收发器可另外(或可选地)采用其他地理定位机制,包括但不限于三角测量、辅助GPS(AGPS)、E-OTD、CI、SAI、ETA、BSS或类似机制,以确定便携式通信设备在地球表面上的物理位置。

[0028] 便携式通信设备还包括用户界面,其为消费者提供一些装置,以接收信息以及输入信息或以其他方式对所接收的信息作出响应。如目前理解的(未预期将本发明限制于此)这种用户界面可以包括麦克风、音频扬声器、触觉界面、图形显示器以及键区、键盘、指取设备和/或触摸屏。便携式通信设备还包括微处理器和大性能存储器。大性能存储器可以包括例如ROM、RAM以及一个或多个可移动存储卡。大性能存储器为计算机可读指令和其它数据提供存储,包括基本输入/输出系统("BIOS")和用于控制便携式通信设备的操作的操作系统。

[0029] 便携式通信设备还包括专用于识别设备的设备标识存储器,诸如SIM卡。如通常理解的,SIM卡包含设备的唯一序列号(ESN)、移动用户的国际唯一序号(IMSI)、安全认证和加密的信息、与本地网络相关的临时信息、用户已经访问的服务列表以及两个密码(通常使用的PIN码和解锁用的PUK码)。如面前有本说明书、附图和权利要求的本领域技术人员所应理

解的，其他信息可以根据设备的类型、其主要的网络类型、本地移动网络运营商等保留在设备标识存储器中。

[0030] 便携式通信设备可具有两个子系统：(1)“无线子系统”，其能够进行通信和其他数据应用程序，在现今移动电话的用户中已经变得普及，和(2)“安全交易子系统”，也可被称为“支付子系统”。安全交易子系统将包括安全元件和用于通信至管理和供应系统的相关联的设备软件，以及用于使用和管理存储在安全元件中的安全数据的面向用户的界面。可以预期的是这种安全交易子系统将优选包括安全元件，与作为全球平台2.1.X、2.2或2.2.X(www.globalplatform.org)的一部分所描述的相似(如果不相同)。安全元件已经被实现为专门的、独立的物理存储器，用于与行业普通销售点一起使用的存储支付卡磁道数据的行业通用实践；此外，也可以存储在安全元件中的其他安全凭证包括员工徽章凭证(employment badge credentials)(企业访问控制)、酒店及其他基于卡的访问系统以及通行凭证。

[0031] 移动网络运营商

[0032] 每个便携式通信设备都连接到至少一个移动网络运营商。移动网络运营商通常提供实体基础设施，其经由与每个手机发射塔的相关联区域(cell)内的多个便携式通信设备进行通信的多个手机发射塔，支持无线通信服务、数据应用程序和安全交易子系统。反过来，手机发射塔可与移动网络运营商的逻辑网络、POTS和因特网可操作地通信，以传送移动网络运营商自己的逻辑网络内，以及至包括那些其它移动网络运营商的外部网络的通信和数据。移动网络运营商通常提供对一个或多个通信协议和技术的支持，包括但不限于用于移动通信的全球系统(GSM)、3G、4G、码分多址(CDMA)、时分多址(TDMA)系统、用户数据报协议(UDP)、传输控制协议/因特网协议(TCP/IP)、SMS、通用分组无线业务(GPRS)、WAP、超宽带(UWB)、IEEE 802.16全球微波接入互操作性(WiMAX)、SIP/RTP或各种其它无线通信协议中的任一种，以与便携式通信设备进行通信。

[0033] 零售子系统

[0034] 现今的商家标准是互联网协议连接支付系统，允许对银行和商业服务提供商的借记卡、信用卡、预付费和礼品类产品进行交易处理。通过在销售点(或采购点)终端的磁性读取器刷磁条启用卡，卡内数据被传送至销售点装备并用于由发卡银行确认资金。这种销售点装备已开始包括作为附件的非接式智能卡读取器，允许支付卡数据在RF界面上呈现，以代替磁性读取器。数据通过RF界面由ISO14443标准和专有的支付应用程序类似PayPass和payWave传送至读取器，其传输来自卡以及未来包括支付子系统的移动设备的非接卡数据。

[0035] 零售商的销售点设备75可以通过无线或有线连接连接至商家支付网络。这种销售点网络除了局域网(LAN)、广域网(WAN)、直接连接(例如通过通用串行总线(USB)端口)、其它形式的计算机可读介质、或上述的任何组合之外，还可以包括因特网。在相互关联的一组LAN上，包括基于不同的架构和协议的那些，路由器起到LAN之间的链路作用，使信息能够从一个发送至另一个。另外，LAN内的通信链路通常包括双绞线对或同轴电缆，而网络之间的通信链路可以利用模拟电话线路，全部或部分专用数字线路，包括T1、T2、T3和T4，综合业务数字网(ISDN)，数字用户线路(DSL)，无线链路，包括卫星链路，或本领域技术人员已知的其它的通信链路。此外，远程计算机和其他相关电子设备可以通过调制解调器和临时电话链路远程连接至LAN或WAN。在本质上，销售点网络可利用允许信息在销售点设备和金融服务

提供商之间传播的任何通信方法，以便通过相同的金融服务提供商对在交易点的支付进行确认、认证并最终获得金融交易。

[0036] 系统管理后端

[0037] 系统包括系统管理后端。如图1B中所示，系统管理后端300经由至少一个移动网络运营商的基础设施连接至零售子系统(见销售点设备75)、安全交易子系统(由一个或多个金融服务提供商组成)310以及多个便携式通信设备50。系统管理后端300包括与一个或多个客户端设备可操作通信的服务器。服务器还与零售商子系统75、安全交易子系统310以及一个或多个便携式通信设备50可操作通信。任何类型的语音信道可与本发明关联使用，包括但不限于VoIP。

[0038] 系统管理后端300的服务器可以包括一个或多个通用计算机，该一个或多个通用计算机执行在同一台计算机上或者在分布在多个计算机上的本地或广域网络上串行或者并行运行系统后台所需的程序和功能，并且该一个或多个通用计算机甚至可以位于“云”中(优选遵守充分安全性的规定)。包括服务器的一个或多个计算机可被Linux、Windows®、Windows CE、Unix或基于Java®的操作系统等等所控制。系统管理后端服务器与存储程序代码和数据的大性能存储器可操作关联。数据可包括一个或多个数据库、文本、电子表格、文件夹、文件等等，其可以配置为保留并存储知识库，用户识别符(ESN、IMSI、PIN码、电话号码、电子邮件/即时消息地址、账单信息等等)。

[0039] 系统管理后端服务器可以支持案例管理系统，以在客户服务中心的客户端计算机上提供呼叫通信连通和分配。在使用VoIP的语音信道连通的优选方法中，案件管理系统是通过加利福尼亚的红木城的Contactual有限公司发布的。接触系统是用于基于VoIP的客户服务呼叫中心的标准CRM系统，对于处理同时支付和与手机有关的服务关注的服务问题时，其同样提供灵活性。如面前有本说明书、附图和权利要求的本领域技术人员所应理解的，可以在本发明中使用其他其他案例管理系统，例如Salesforce(加利福尼亚，旧金山，Salesforce.com有限公司)和Novo(弗吉尼亚州，弗吉尼亚海滩，Novo Solutions有限公司)。

[0040] 系统管理后端服务器还支持发布引擎2010、用户唯一标识数据库2011、商家地理位置归类数据库2012和预测交易模块2015。这些元件将在本说明书下文说明。

[0041] 与系统管理后端服务器相关联的每台客户端计算机具有网络界面设备、图形用户界面和匹配由客户服务中心服务器支持的语音信道如VoIP的语音通信能力。每个客户端计算机可以请求便携式通信设备的蜂窝和安全交易子系统两者的状态。这种状态可以包括便携式通信设备的软存储器和核心性能，NFC组件：基带、NFC天线、安全元件的状态和标识的内容。

[0042] 支付子系统

[0043] 如图2中所示，每个便携式通信设备50可包含一次性支付钱包160、支付库110、安全元件120、NFC(或RF)基带、支付子系统150(即安全数据存储装置115和安全元件120)以及诊断代理170。一次性支付钱包160是使任何便携式通信设备能够请求并模拟因临时使用而下载到设备50(优选至支付子系统150中)的与NFC/RF基带相关联的凭证(例如卡、优惠券、访问控制和票数据)的电脑应用程序。应用程序也可以使用WAP、J2ME RTE和/或SMS通道在传统功能手机(非智能手机)上实现，以代替智能手机。如下文中将要更充分讨论地，凭证最

优选是基于NFC的，但也可以是基于RFID，2-D条代码或阿拉伯数字的。

[0044] 支付库110由一次性支付钱包160使用，以管理(并在其上进行家务)安全元件120，与系统管理后端300交流并且经由数据通信收发器(包括其SMS信道)在设备50上执行无线通信(over-the-air)(OTA)配置。可以预期的是，OTA数据通信会以某种方式被加密，并且加密密钥将被布署在与便携式通信设备50以及与支付子系统150可操作关联的卡服务模块中。在一个实施方案中，卡服务模块可操作连接至一次性支付钱包160(布署为如下所述的第三方应用程序)和支付子系统150。卡服务模块通常强制执行对存储在支付子系统150中的数据的访问控制，并且控制被允许在支付子系统150中运行的每个应用程序的功能。在一个实施方案中，卡服务模块验证在便携式通信设备上使用的每个第三方应用程序的作者/发布方(如下文一般描述)。支付子系统150可以被用来存储凭证，例如除了其他支付卡的临时一次性支付卡、优惠券、访问控制和票数据(例如，交通票数据、音乐会票数据等等)。这些凭证类型中的一些可以根据情况加至支付子系统和支付库。

[0045] 安全数据存储装置115提供便携式通信设备上安全的存储。可根据预期存储在安全数据存储装置115中的数据的性质提供不同的安全级别。举例来说，安全数据存储装置115可以简单地是设备50的操作系统级别的密码保护。如这些操作系统中已知的，密码可以是存储在存储装置50中某处的简单的字母数字或十六进制代码。可替代地，安全数据存储装置115中的数据是优选加密的。然而，更可能的是，所述安全数据存储装置115将以标题为“System and Method for Providing A Virtual Secure Element on a Portable Communication Device”的2011年10月21日提交并通过引用并入本文的美国专利申请号13/279147的共同未决的专利申请(由本申请的受让人拥有)中公开的方式设置为虚拟安全元件。

[0046] 经由智能手机的一次性支付

[0047] 由于一些销售点设备不接受NFC支付，而一些用户没有设立NFC账户，本发明使任何便携通信设备能够在接受传统的电子支付的商家经由他们现有的销售点装置进行高度安全的电子支付。

[0048] 为了使用该系统一次性支付给零售商，消费者应已经下载一次性支付钱包应用程序并且有指定银行的至少一个现有帐户。消费者也应已经注册了一次性支付发布方310(其也可以是指定银行)的至少一个帐户。此外，消费者也应具有他们智能电话(或便携式通信设备50)的移动数据服务。

[0049] 因凭证的临时性质及其与地理位置确认的结合，一次性支付钱包160可以消除凭证的存储、维护和使用中所涉及的一些复杂性。可以由一次性支付钱包160控制的可能行为是与以下相关联的行为：

[0050] a.钱包管理(例如，设置、重新设置或启用钱包密码；获得OTA服务器的URL；无线通信注册配置；设置支付时间；增加支付时间；设置默认卡；列出发布方、内存审计列表；确定存储凭证的SE；更新钱包状态)；

[0051] b.凭证管理(例如，添加凭证；查看凭证详细信息；删除凭证；激活凭证(赎回/支付)；停用凭证；锁定/解锁凭证；要求密码访问；获得凭证图像；设置访问密码)；和

[0052] c.安全元件(SE)管理(例如，获得凭证；更新凭证；更新元数据；删除凭证；钱包锁定/解锁；SE锁定/解锁)。

[0053] 图3A-3B一起示例性说明使用一次性支付钱包160获得并使用一次性支付凭证的过程的一个可能的实施方案(以及各种可能的替代)。消费者可携带他们的智能手机(即便携式通信设备50)进入实体零售店,并如常进行他们的购物体验。将一次性支付钱包160下载在他们的智能手机上,当消费者准备在实体零售商店结账时,通过打开能够解决(solution-enabled)的智能手机应用程序,消费者甚至可以使用他们采用传统系统的智能手机支付。

[0054] 消费者来到销售点75,打开智能手机50上的一次性支付钱包160,通过一次性支付屏幕上的用户界面输入消费者的口令/密码(参见图5)。一次性支付钱包160发送消费者的密码和地理位置坐标(由位置标识服务165生成,图2)至发布引擎2010(图4)。在一个实施方案中,在生成临时支付卡的信息之前,一次性支付钱包160还可以为消费者提供将即将发生的支付的估计量通信至发布引擎2010的能力。通过将关于一次性支付的估计量信息合并至确认进程,可以为一次性代码提供额外的安全性。

[0055] 发布引擎2010验证密码(例如,使用用户唯一标识数据库2011)。接收正确的通行码指示系统消费者将在短的预定时段内的进行支付(几分钟量级,在某些情况下可以延长)。发布引擎2010使用从便携式通信设备50接收到的地理位置坐标,来确定可能的商家并在与发布引擎2010可操作关联的数据库中查找商家的销售点详细信息(例如,商家地理位置集合数据库2012)。特别地,根据接收到的地理位置信息,发布引擎2010执行数据库查询,以确定消费者位置安装(或可能被安装)哪种非接式销售点终端。在优选实施方案中,便携式通信设备50还可以显示接下来所述便携式通信设备50可位于其中的最可能的零售商店的列表(例如,接下来前五个)(参见,例如图6A)。基于所识别的位置和/或销售点终端,便携式通信设备50的卡服务模块用对于该位置和/或销售点特定的数据格式和其他非接式销售点的数据配置支付系统150,以使得设备50得到卡、优惠券、票或访问控制模拟的支持或优化呈现。系统还可以识别可用于那个地理位置而消费者尚未在支付库110中下载的的消费者新卡产品。在一些实施方案中,系统可以加载所需的库。

[0056] 发布引擎2010包括所有电子支付受理商户的数据库(例如,商家地理位置集合数据库2012),其可能包括商家位置、传统电子支付中使用的商家标识号码、每个商家位置接受的传统支付方案,以及每个商家位置的销售点的设备性能性能性能(参见下面表1)。尽管商家地理位置集合数据库2012被描述为包括在发布引擎2010中或以其他方式为发布引擎2010的一部分,但设想商家地理位置集合数据库2012可以包括在便携式通信设备50、发布方310内,为便携式通信设备50、发布方310的一部分,或与便携式通信设备50、发布方310相关联,或者分别承载。

[0057] 表1-商家和一次性支付信息的实施例

[0058]

商家名称	商家位置GPS（纬度/经度）	商家位置地址	传统商家ID号	传统支付	装置性能
Grocery land	37.28N，122.24W	加州红木城海洋大道100号400室，94065	XQ24MZ122A	条形码	激光扫描仪
Appliance Land	37.28N，122.24W	加州红木城海洋大道110号400室，94065	YF234XY302	3-D条形码	3-D条形码读取器
Must Buy	37.28N，122.24W	加州红木城海洋大道120号400室，94065	MN343D	NFC	NFC读取器

[0059] 发布引擎2010之后生成一次性使用的临时支付卡，并将临时支付卡数据和可能商家的身份通过无线通信传输至便携式通信设备50。这种临时支付卡信息可以使用现有的标准和传统电子支付行业的惯例进行实时编排(formatted)，包括个人帐号、发布方标识号码、ISO/IEC7812(涉及使用发布方标识号码(IIN)的发布方标识，以在国际、行业间和/或行业内交换中操作)，ISO/IEC7813(涉及用于初始金融交易的磁道的数据结构和内容)，以及ISO 8583格式(这是企业消息协议，基于专有(proprietary)标准)。

[0060] 在一个优选的实施方案中，一次性支付钱包160基于便携式通信设备50的性能以及商家的销售点设备75的性能编排临时支付卡的格式。临时支付卡信息也可被编排为多种格式，以为消费者提供可以呈现给商家收银员的选项。图7A和图7B示例性说明可以传输至所述便携式通信设备50的两种可能类型的一次性支付码。图7A将一次性支付码描绘为2-D条形码。如本领域中普通技术人员应理解的，这种条形码可以是3-D或QR码。图7B将一次性支付码描绘为数字代码，其可以是16位数字或根据需要具有不同长度。

[0061] 临时支付卡信息可以在智能手机屏幕上显示的一种格式是ISO/IEC7813标准号(即PAN)，商家职员手动将其输入商家销售点。临时支付卡信息可以在智能手机屏幕上显示的另一种格式是条形码(ISO/IEC 15426-1)、2-D条码(ISO/IEC15426-2)、QR码(ISO/IEC 18004:2006)，或传输ASCII数据，之后由商家销售点的光学扫描仪捕获的其他类似方法。临时支付卡数据可以显示的还有一种格式，使用NFC的点对点模式(ISO/IEC18092)、NFC标签模拟(NDEF，ISO14443和Felica)或NFC卡模拟模式(ISO 14443卡模拟)或RFID模式。

[0062] 临时支付卡数据在短的预定时间段后到期，例如两(2)分钟，以提供更多的安全性。只要发布方愿意，这一时间可以延长。据信少于30分钟或者甚至少于20分钟或者甚至10分钟将是优选的。可以如所期望的使用和/或编程其他到期时间。

[0063] 便携式通信设备50从发布引擎2010接收临时凭证数据、可能的商家和模拟信息。在一个优选的实施方案中，所述便携式通信设备50确认从数据库2012中正确地选择可能的商家。在结合图6示例性说明的一个方法中，便携式通信设备请求用户确认位置。在该示例性说明的实施例中，IS用户界面询问位置是否为“Grocery land”？当消费者在图1中显示位于Grocery land，消费者应选择图6上的“是”按钮。如果系统已经选择了错误的零售商，则系统可提供备选方案以确保正确的零售商。例如，图6A描绘了实例中提供接近消费者附近的可能的商家列表，此处从被发布引擎2010识别为商场(或其他高密度商家群)的地方内要求一次性凭证。如面前有本说明书、附图和权利要求的本领域技术人员所应理解的，附近的商家的列表不必局限于单个商场中的那些商家。可以从与服务器接收到的地理位置地理地

相近的其他零售商选择替代方案。如还应理解的是替代方案可以下拉菜单或列表的形式呈现给终端用户。

[0064] 在其中消费者使用便携式设备50确认商家的实施方案中，对可能的商家的确认可被发布引擎2010接收。如果可能的商家被不正确识别，则发布引擎可以发布新的模拟信息至便携式通信设备50。一旦已知可能的商家，发布引擎2010的预测交易模块2015向验证映射网关2020传输该可能的商家的ID，与便携式通信设备50相关联的唯一用户ID，为交易产生的一次性使用记号(token)以及过期时间。

[0065] 验证映射网关2020可以由银行、发布方310或支付处理器网络实际主办，并可以布署为服务或安装并集成在现有的交易处理器、卡制度、财务机构和其他实体的子系统。当从预测交易模块2015接收数据时，接收的数据被存储在与验证映射网关相关联的数据库中。当这样的数据被提供时，临时数据可以与先前与唯一用户ID相关联的传统卡数据相关联。如果传统的卡唯一的用户ID关联存在，则其可由发布方310创建或者甚至在便携式通信设备50和由系统管理后端300安排的验证映射网关2020之间的电子交易中由消费者直接创建。

[0066] 在优选实施方案中，在一次性使用的凭证信息被传输至所述便携式通信设备50的同时，预测交易模块2015发送数据至验证映射网关2020。在这种方法中，验证映射网关2020可以预计经由商家支付网络的来自商家POS75的消费者交易。特别是，在这样一个实施方案中，验证映射网关2020可以使用从预测交易模块2015接收数据和从零售商销售点75接收交易之间的时间，将所存储的数据从大型数据库取出并放入存储器中，以提供更快的访问(相比于来自大型数据库的访问时间)以及所存储的数据与从商家支付网络接收到的数据之间的比较。在这种方法中，与以其他方式为了这种比较而从POS75接收交易后再需要定位和调取数据所需要的等待时间相比，在验证映射网关2020中增加该额外的验证步骤，将产生更少的等待时间。

[0067] 所以返回消费者，便携式设备50接收该临时凭证和模拟信息后，消费者之后可以点击或以其他方式在NFC允许点对点的销售点设备75上激活智能手机50，这将使得便携式通信设备使用服务器提供的模拟协议用一次性支付代码来模拟凭证。可以理解的是，代码可以在便携式通信设备50的屏幕上视觉地“模拟”。由于临时支付卡数据可以传统格式提供，所以临时支付卡数据可被现有商家销售点装置75所接受。

[0068] 之后，销售点设备75通过正常商家支付网络处理临时支付卡数据，如同它是标准的信用卡或借记凭证。但是，由于临时支付卡数据使用注册并映射到作为发布方的一次性支付系统供应商的发布方标识号码(ISO IEC7812)，数据将经由商家支付网络路由至验证映射网关2020。如果数据在临时凭证到期时间到期之前被验证映射网关2020接收并来自预期可能的商家，则验证映射网关2020可以核准该交易(服从资金可用性等)。验证映射网关2020还可以将支付卡数据被输入商家销售点设备75的方法(现有ISO8583指定域)与临时卡数据被提供给移动电话的方法(例如数字代码、条形码、NFC)进行比较。

[0069] 再次，如果所有所需的表征相匹配(例如临时代码、执行时间、商家ID以及模拟类型)，则验证映射网关可以通过商家支付网络以核准代码向商家返回确认。商家销售点75接收授权(即用核准代码确认支付接受)、打印收据，而消费者带着他们的新购物品离开商店。

[0070] 可选地，当验证临时支付卡信息(包括时间和可能的商家ID)时，系统具有转发等

效的支付交易请求至发布方310以核准该交易的选项。这被称为背对背(back-to-back)支付交易。以这种方式，消费者和商家将从消费者的传统银行信用卡或借记卡账户获得支付确认，而不是临时卡号。特别是，一旦一次性支付交易被确认，验证映射网关2020替代交易数据中的传统的卡支付数据，其之后连同标准的POS交易信息(例如商家ID和交易数额)以及—在某些实施方案中—显示交易使用经过验证的一次性使用凭证的标示(以显示另外的安全性措施)一起传递至发布方授权系统310。发布方310将审核传统的卡数据和交易信息，来确定是否以本领域公知或者附加交易已经具有上文指出的另外的安全性的信息的方式来授权交易。经由正常现有处理通道将发布方授权发送回商家销售点75。

[0071] 这种一次性使用凭证的解决方案可用于许多不同类型的凭证验证情况，包括：信用卡和借记卡支付、礼品卡、会员卡、优惠券和优惠、访问控制和实际环境中消费者提出凭证用于验证的其他环境中。

[0072] 而功能性可集成在一次性支付钱包160内，用户界面可以通过钱包用户界面来提供，而安全支付子系统的无线通信配置和管理以及访问由卡服务模块的功能支持。用户界面之下，卡服务模块便于无线通信配置、安全元件管理，以及在用户的移动设备50上的卡服务模块与适当的发布方服务器之间以如先前在本领域中已知的加密的方式直接交换密钥(用于将是发布引擎2010的一次性支付钱包160)。

[0073] 验证作为第三方应用程序的一次性支付应用程序

[0074] 如图8A-8B中示例性说明的，一次性支付钱包160可被布署为许多受信任的第三方应用程序200中的一个。在应用程序被允许访问便携式通信设备50上的安全元件120(或安全数据存储装置115以及甚至优选地元数据存储库，其存储，除了别的之外，卡图像数据和任何压印卡数据)以浏览、选择和/或改变存储在支付子系统150中的安全数据之前，卡服务模块验证应用程序200的受信任状态。这种验证可通过访问许可或受信任的应用程序的本地授权数据库来完成。在优选的方法中，本地授权数据库与一个或多个服务器相关联的远程授权数据库配合使用，一个或多个服务器与系统管理后端300相关联。

[0075] 图10是一个可能的组合本地和远程授权数据库以提高卡服务模块、安全元件120和支付子系统150的安全性的一个可能的实施方案的框图。如图10中所示，用户A/C注册表(或用户帐户注册表)可以与服务器相关联(或以其它方式布署在云中)。用户的A/C注册表可以存储设置在每个用户的便携式设备50中的安全元件120的标识。可在该过程的任何点为每个用户添加用户帐户注册表中的入口。

[0076] “发布方注册表”数据库是核准的发布方的数据库。发布方ID对每个类型的凭证是唯一的。换句话说，如果银行有多种类型的凭证(例如借记卡，信用卡，认同卡等)，每个凭证类型将有自己的发布方ID(例如I-BofA-II)。在优选的方法中，多种类型的凭证之间的发布方ID也有一些共同的元素，由此表明该凭证是至少相关的(例如I-BofA-I)。以这种方式，来自相同的发布方的应用程序可以与相同的“扩展”的发布方的其他应用程序共享数据。在优选的方法中，可以通过要求甚至是钱包用户界面(其是系统附带的)具有发布方ID(以及一个应用程序ID和编译记号)来简化卡服务模块。

[0077] “应用程序注册表”是已预先被操作系统提供商核准的应用程序(主要是第三方)数据库。像用户A/C注册表一样，“应用程序注册表”和“发布方注册表”数据库维护在与一次性支付应用程序可操作关联的服务器端(或以其他方式在云中)。如面前有本说明书的本领

域技术人员所应理解的，不同的注册表可以在单独的数据库或统一的数据库中执行。在钱包160的起始并且之后优选地以基本上规则的时间间隔(例如，每天)，存储在所述一次性支付钱包160的应用程序注册表中的数据被分配给具有待本地存储的钱包的设备。

[0078] 如图10中所示，应用程序注册表可包括，除其他的之外，应用程序ID(“App ID”)，发布方ID和编译ID或记号。编译ID是在对特定应用程序的鉴定进程中由与一次性支付钱包相关联的一个或多个进程为每个应用程序生成的全局常数。在其由唯一设备50的特定卡服务模块生成之后，编译记号被包括在应用程序中或以其他方式与应用程序关联。这种编译记号优选由设备的本地伪随机数字发生器生成，其使用预先确定的种子(seed)，例如应用程序ID、编译ID、发布方ID或它们的某种组合。

[0079] 当用户尝试用设备50上的卡服务模块鉴定应用程序时，与第三方应用程序相关的编译ID(数字记号)和应用程序ID(数字标识符)可以对存储在存储于设备50上的卡服务注册表中的编译ID和应用程序ID进行匹配(参见图10)。如面前有本说明书的本领域技术人员所应理解的，相同的编译和应用程序ID对也被传输至与系统相关联的其它设备50。如果编译ID/应用程序ID对匹配存储在设备上的卡服务注册表中的对中的一个，秘密记号ID优选地由伪随机数字生成器(例如与安全元件120相关联的一个)在设备50上生成，并且之后与编译ID/应用程序ID对相关联存储在设备50的卡服务注册表中。在一些情况下，编译ID可以预先选择并用于接种(seed)随机数字发生器。应理解的是，与卡服务注册表相关联的其他预先确定的数据的一个或多个块可以替代地预先选择为种子。卡服务注册表优选地存储在安全存储器中(而不是在安全元件120中，因为安全元件120具有有限的不动产(real estate))，而卡服务注册表还优选地使用标准的加密技术进行加密。秘密记号ID也嵌入设备50上的应用程序200或以其它方式与设备50上的应用程序200相关联，来代替用所述应用程序分配的编译ID。

[0080] 一次性支付钱包160已加载到卡服务注册表(和嵌入到应用程序中的秘密记号)中之后，一次性支付钱包160可以启动并可能会提示用户选择加入，以提供对验证的(或受信任)应用程序所需的发布方特定凭证的访问。在一次性支付钱包应用程序160每次随后的启动中，将嵌入式秘密记号和/或应用程序ID与设备上的卡服务注册表中的数据进行比较。如果匹配，则应用程序是受信任的并且可以通过卡服务模块访问支付子系统150。在这样的方式，可以看到，应用程序200或钱包用户界面也可以从卡服务注册表中删除，并且因此将不能访问支付子系统并可能共同地不能访问应用程序。

[0081] 卡服务模块还优选使用受信任的应用程序验证步骤，以确定允许一次性支付钱包160的适当水平的子系统的访问。例如，在一个实施方案中，应用程序可以被授权访问并显示支付子系统150中包含的所有数据，其中另一个应用程序可以仅被授权访问并显示支付子系统150中包含的数据的子集。在又一个实施方案中，应用程序可以仅被允许发送支付或交易请求至一次性支付钱包160，但本身未被允许访问支付子系统150中包含的任何数据。在一个方法中，将权限分配给应用程序可以被认为是如下的：

[0082]

	保留的	所有凭证	扩展的发布方凭证	自己的凭证
读取	0	0 或 1	0 或 1	0 或 1
写入	0	0 或 1	0 或 1	0 或 1
删除	0	0 或 1	0 或 1	0 或 1
激活/停用	0	0 或 1	0 或 1	0 或 1
下载凭证	0	0 或 1	0 或 1	0 或 1

[0083] 这些权限可以被用于以上文显示的从最显著到最不显著数字的顺序形成4个十六进制数。如在图10的示例卡服务注册表中所示，I-BofA-II发布方具有权限级别11111，这可以被认为是扩大到0001 0001 0001 0001 0001。换句话说，I-BofA-II应用程序读取、写入、删除、激活/停用并下载自己的凭证，但不扩展发布方凭证，更不用说所有凭证。如果BofA有另一个发布方代码(例如I- BofA -I)，那么这将是扩展的发布方应用程序。因此，如果与发布方ID“I-BofA-II”关联的应用程序的权限级别设置为0010 0001 0001 0010 0001(或21121十六进制)，则应用程序将能够读取和激活/停用与两个发布方ID都相关联的凭证。在另一个实施例中，钱包用户界面可被给予44444(即0100 0100 0100 0100 0100)权限级别。换句话说，钱包用户界面可以读取、写入、删除、激活/停用并下载所有凭证。如本领域的普通技术人员应当理解，这些仅仅是可以被授予应用程序的可能的权限的示例，预期其他的权限。例如，一些应用程序可具有读取扩展发布方凭证的能力，但仅写入、删除、激活并下载应用程序自己的凭据(如21111，其扩展到0010 0001 0001 0001 0001)。在另一个实施例中，应用程序可能仅被给予激活/停用和下载的权利(即0000 0000 0000 0001 0001或00011，十六进制)。在另一个实施例中，应用程序可以是失效的—但未从受信任应用程序数据库或信用卡服务注册表处删除—通过设置所有权利为零。

[0084] 在将一次性支付钱包应用程序160配置为受信任的第三方应用程序中的一种的实施方案中，它将必须注册以便访问打开的钱包100(或者甚至卡服务模块)。一次性支付钱包应用160由与发布引擎2010相关联的发布方开发。此外，一次性支付钱包应用程序可以模拟NFC凭证。因此，一次性支付钱包应用程序160应该被给予权限级别11111，这可以被认为是扩大到0001 0001 0001 00010001。换句话说，一次性支付钱包应用160可以读取、写入、删除、激活/停用并下载自己的凭证，而不是扩展的发布方凭证或其他任何凭证。

[0085] 前述描述和附图涉及一次性支付钱包160和一次性支付凭证或信息或在短的预定时间段之后过期的临时支付卡数据。但是，也认识到，一次性支付钱包160可以反而被认为是动态的临时钱包160，而一次性支付凭证/信息和临时支付卡数据可被视为动态临时凭证。这样，凭证可以(1)“再循环”并且在系统中被其他用户重复使用；(2)具有比“短的”预定时间段更长的预定有效时间，且(3)这些凭证可以用于不止简单地购买商品。还可以预期的是，虽然前述描述和附图主要是涉及与商家相关联的销售点设备75，但前述描述、附图和实

施方案，可以适用于各种其它电子控制点，例如酒店房间的收发器、办公室收发器、汽车租赁收发器等。例如，电子控制点可包括任何访问点，例如销售点设备、RFID收发器、条码收发器、NFC收发器等。

[0086] 特别地，凭证通常必须在整个较大商家支付系统内由发布方310或其他组织“支付”。这样，系统可以仅具有有限数量的凭证供使用。与支付凭证被多个用户在不同的时间循环使用，并且优选地在不同的地理位置循环使用以提供防止欺诈的额外的安全性的系统相比，对特定用户和交易仅使用一次性的这种凭证可导致不必要的高成本。例如，发布引擎2010可以追踪与位于第一地理位置(例如加利福尼亚州)操作第一便携式通信设备50的第一用户的凭证有关的发布和到期数据，并且凭证的到期日期和时间之后，重新分配完全相同的凭证给位于第二不同地理位置(例如福罗里达州)操作第二便携式通信设备50的第二用户。

[0087] 同样，凭证可能有较长有效时间，以允许在各种“销售点”或其他电子控制点使用凭证。例如，参考图9A和9B所示，在便携式通信设备50上显示了示例性的钱包用户界面。钱包160可以包括各种支付卡并与各种支付卡(例如，Master Charge、VISA，Charge-It等，如图9A中示例性说明的)关联，并且还可以包括各种其他非支付应用程序并与各种其他非支付应用程序(例如，酒店房间钥匙、办公室钥匙卡，租车租赁FOB等，如图9B中示例性说明的)关联。尽管“有效时间”周期在销售点销售的情况下优选是短的，以提供增强的安全性，但可以预期的是，在钱包与非支付应用程序如酒店房间钥匙相关联时，“有效时间”可以是明显较长的。在这样的实例中，钱包160可以被用于“打开”或“锁定”用户在酒店的房间。因此，“有效时间”应设置为与用户在酒店的逗留至少相同时间。同样，有效时间可以设置为一段时间内(如果必要的话无限)以允许设备50的用户使用设备50来访问办公室或汽车租赁。

[0088] 因此，也可以预期，系统管理后端300和发布方310可与非金融服务相关联，以允许非支付的钱包应用程序的使用。例如，系统管理后端300可以包括与非金融服务相关的数据(例如酒店位置，办公位置等)，以及发布方310可与非支付实体(例如，酒店实体，办公管理实体关联等)来往的数据。

[0089] 前述描述和附图仅仅解释和示例性说明本发明并且本发明不限于此。虽然相关于某些实施方式或实施方案描述了说明书，但许多细节是为了说明的目的而阐述的。因此，前述仅仅示例性说明本发明的原理。例如，本发明可以有其它的具体形式而不背离其精神或必要表征。所描述的布置是示例性说明而非限制性的。对那些本领域技术人员，本发明可以接受另外的实施方式或实施方案，并且在本申请中所描述的这些细节中的某些可以显着地变化而不脱离本发明的基本原理。因此，应当理解的是，虽然本文没有明确地描述或示出，本领域的技术人员将能够设计出体现了本发明的原理的各种布置，因此在其范围和精神之内。

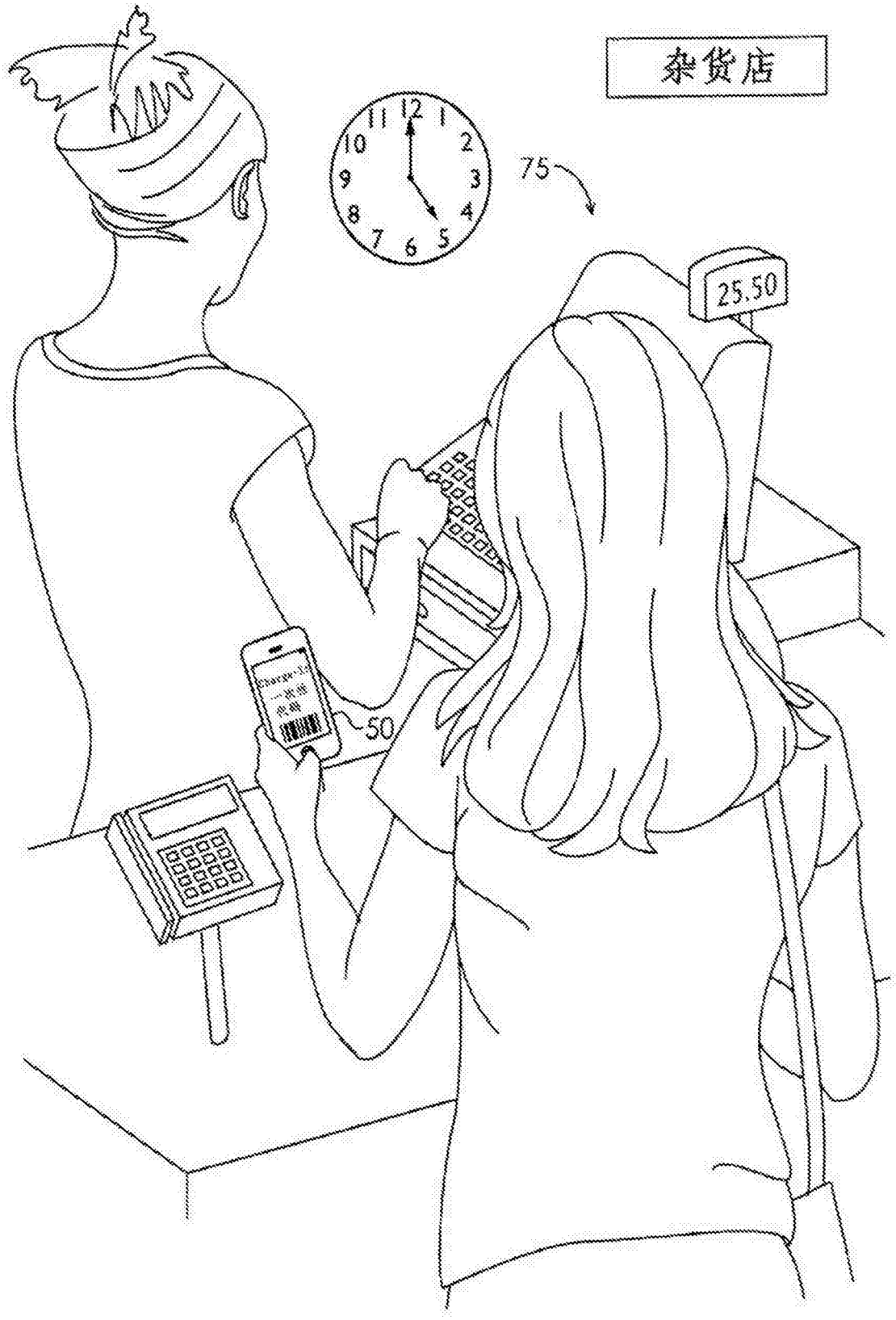


图1A

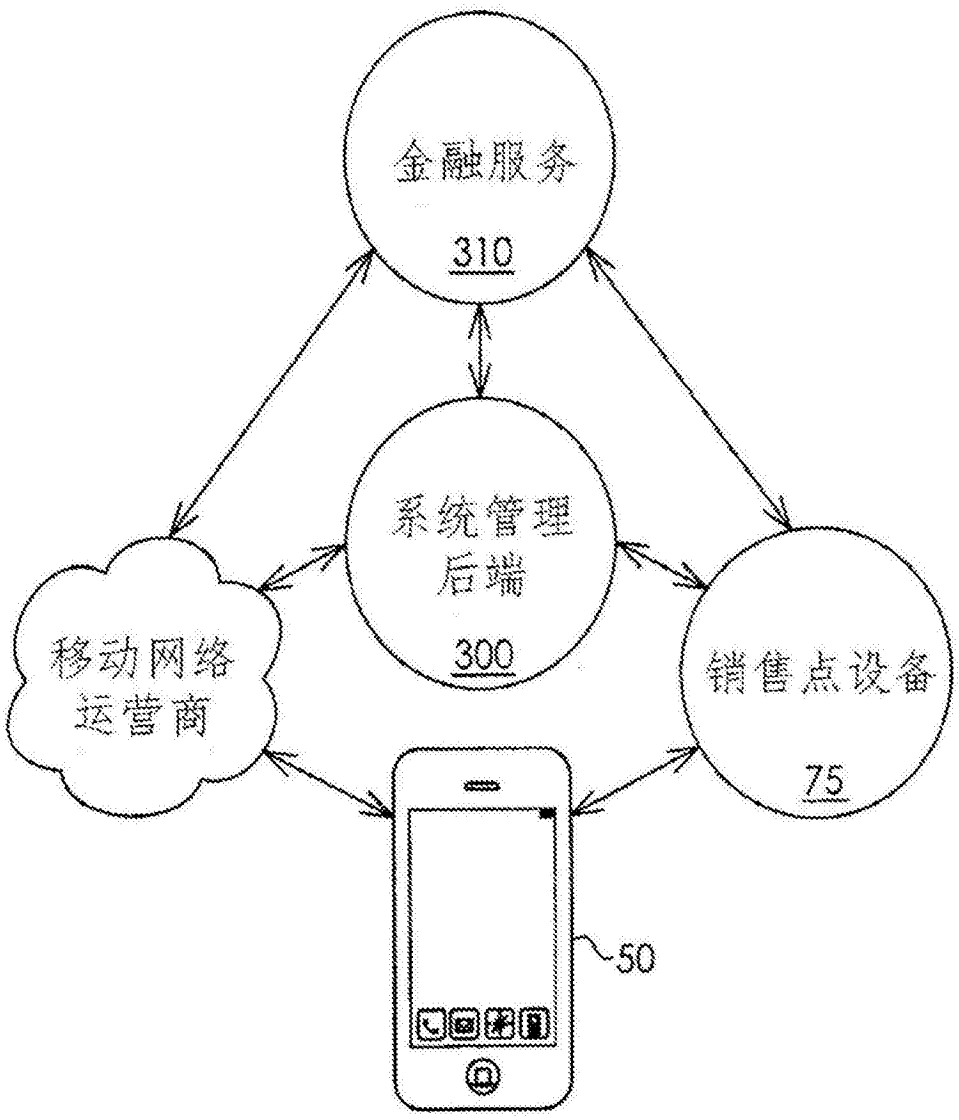


图1B

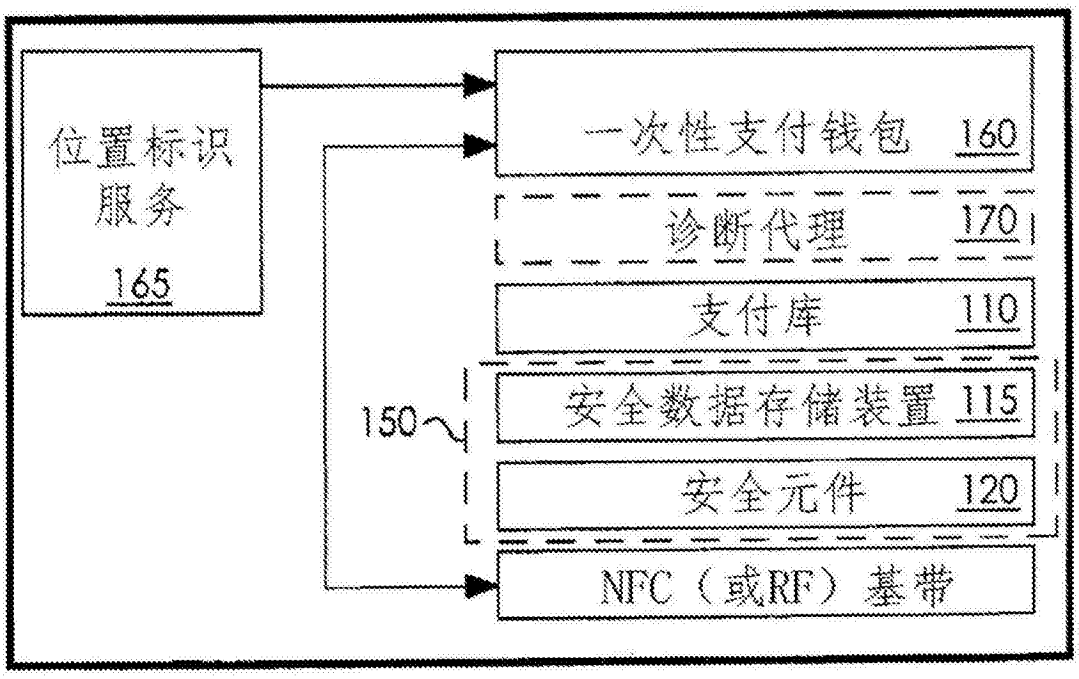

位置标识
服务
165
一次性支付钱包 160
诊断代理 170
支付库 110
150
安全数据存储装置 115
安全元件 120
NFC（或RF）基带

图2

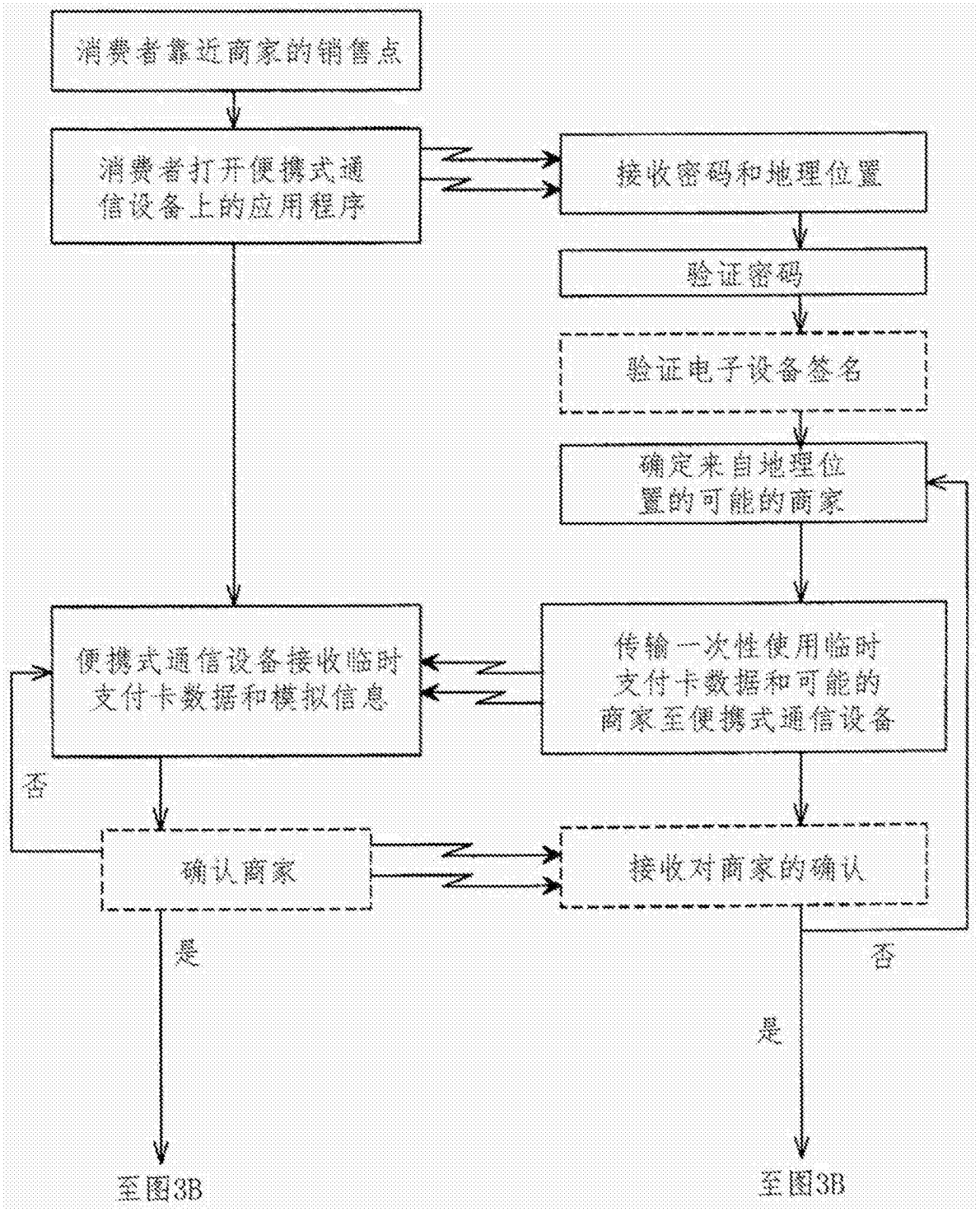

消费者靠近商家的销售点
消费者打开便携式通信设备上的应用程序
接收密码和地理位置
验证密码
验证电子设备签名
确定来自地理位置的可能的商家
便携式通信设备接收临时支付卡数据和模拟信息
传输一次性使用临时支付卡数据和可能的商家至便携式通信设备
否
确认商家
接收对商家的确认
是
否
是
至图3B
至图3B

图3A

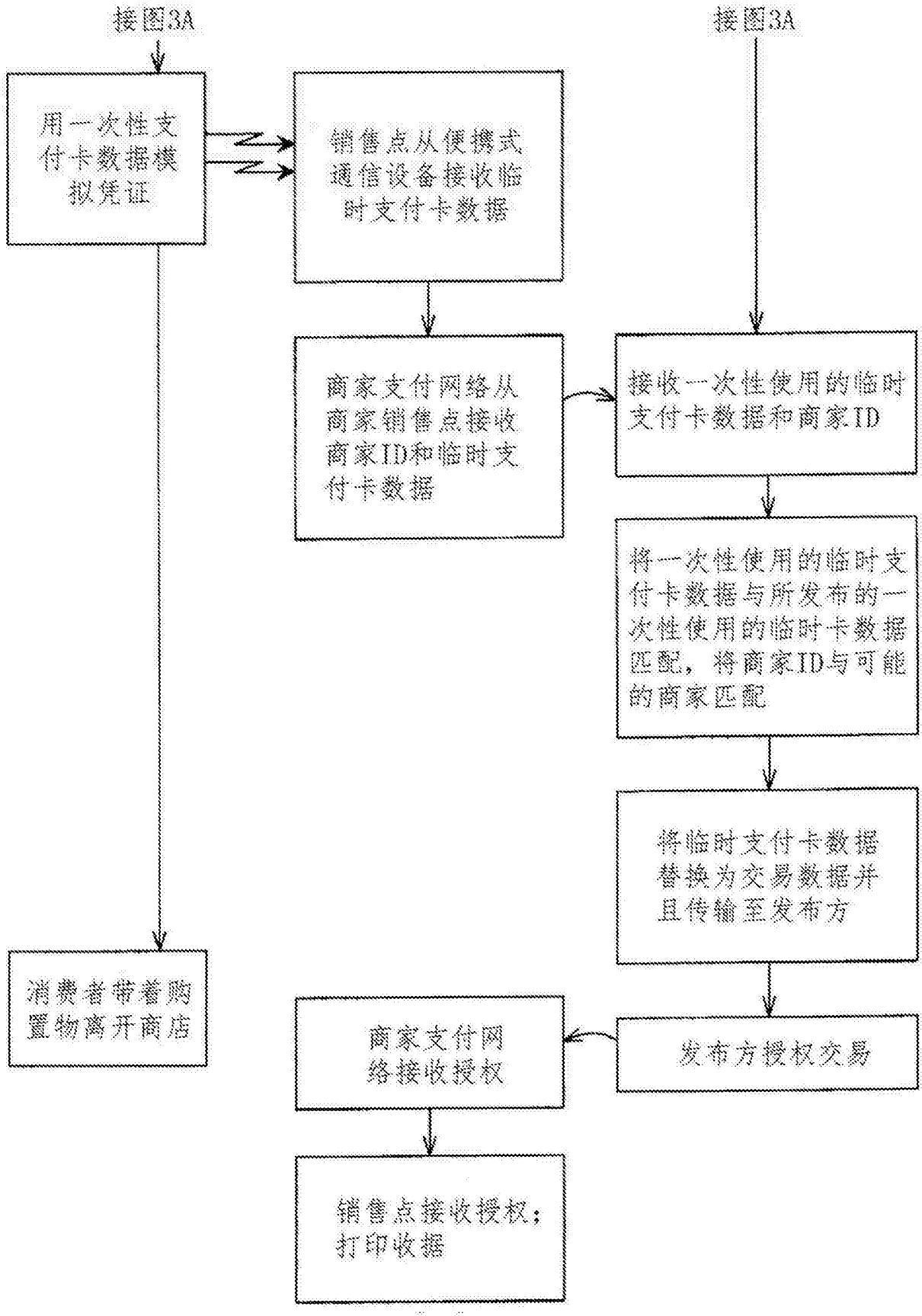

接图3A
接图3A
用一次性支付卡数据模拟凭证
销售点从便携式通信设备接收临时支付卡数据
商家支付网络从商家销售点接收商家ID和临时支付卡数据
接收一次性使用的临时支付卡数据和商家ID
将一次性使用的临时支付卡数据与所发布的一次性使用的临时卡数据匹配，将商家ID与可能的商家匹配
将临时支付卡数据替换为交易数据并且传输至发布方
消费者带着购置物离开商店
商家支付网络接收授权
发布方授权交易
销售点接收授权；打印收据

图3B

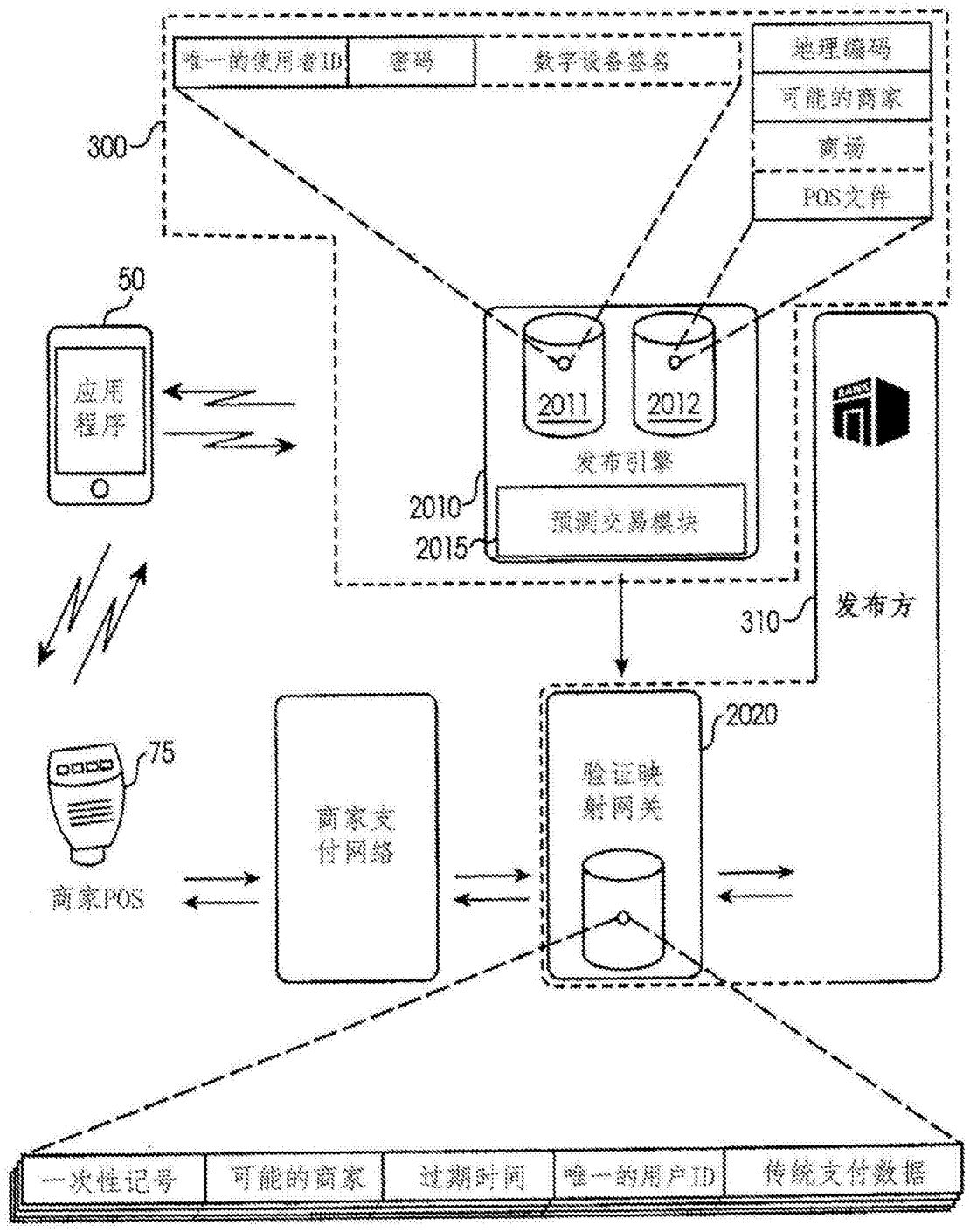

唯一的使用者ID
密码
数字设备签名
地理编码
可能的商家
商场
POS文件
300
50
应用程序
2011
2012
发布引擎
2010
预测交易模块
2015
发布方
310
2020
验证映射网关
商家支付网络
75
商家POS
一次性记号
可能的商家
过期时间
唯一的用户ID
传统支付数据

图4

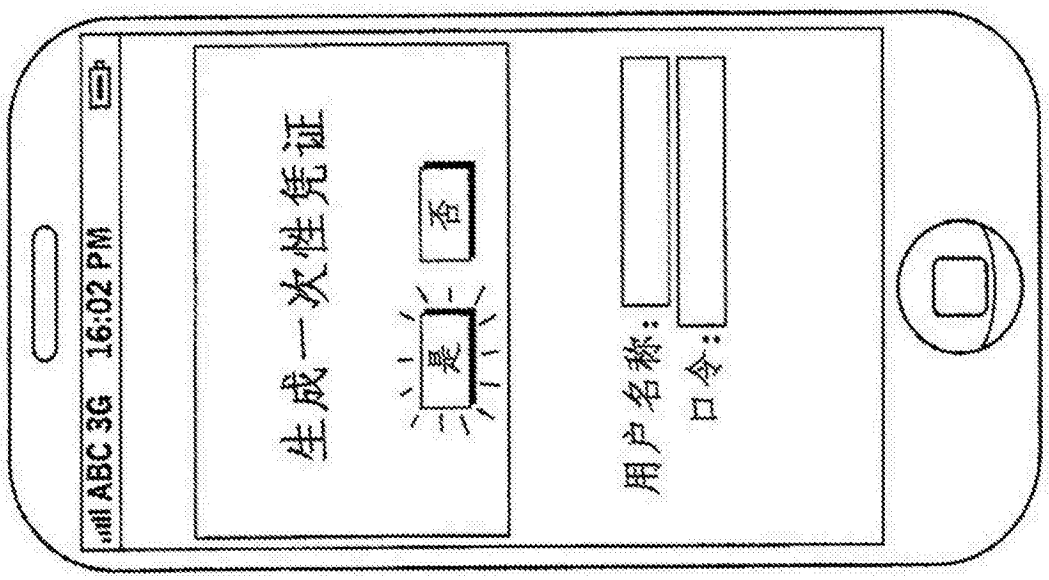


图5

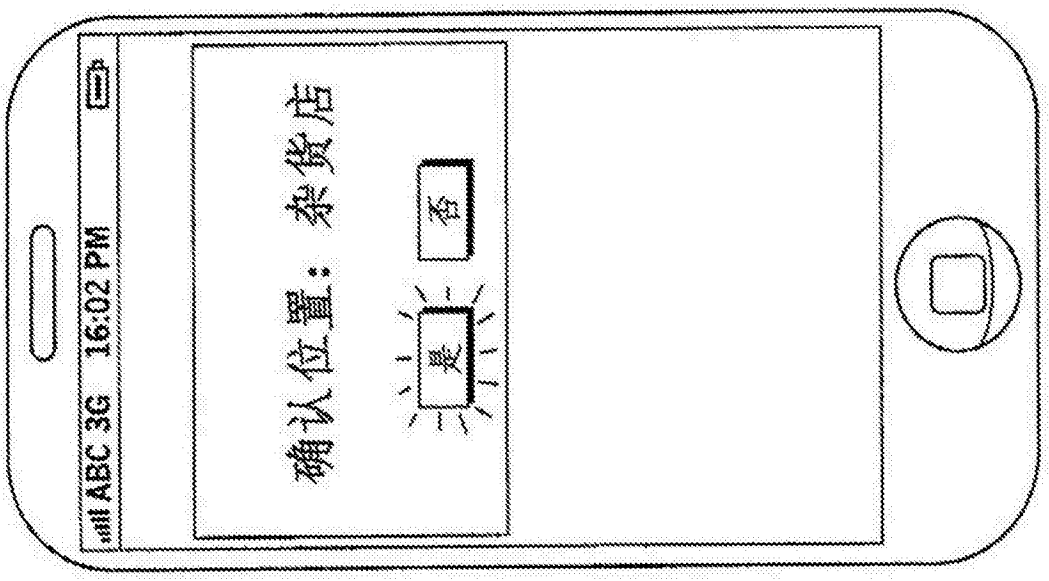


图6

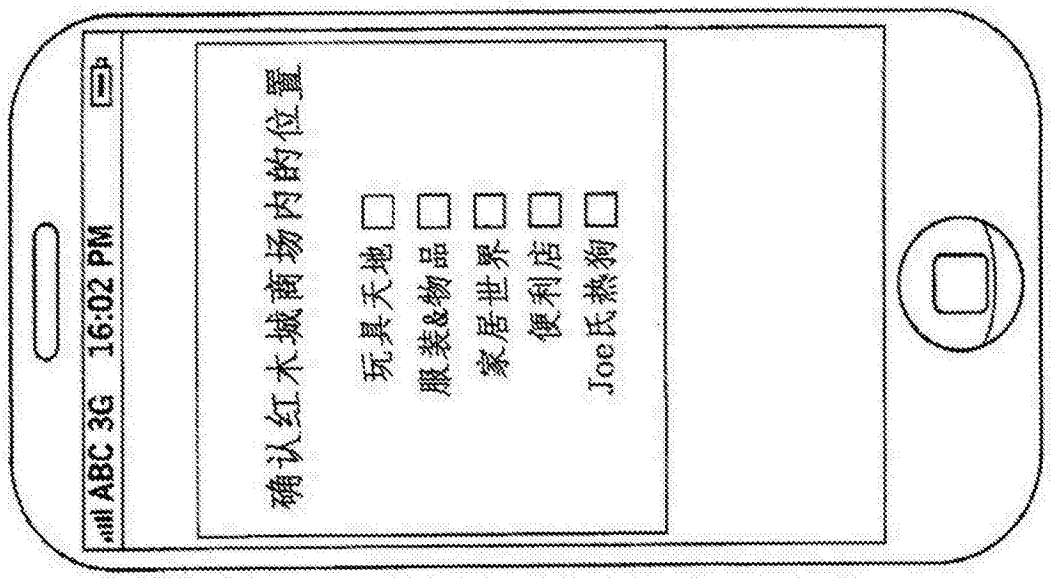


图6A

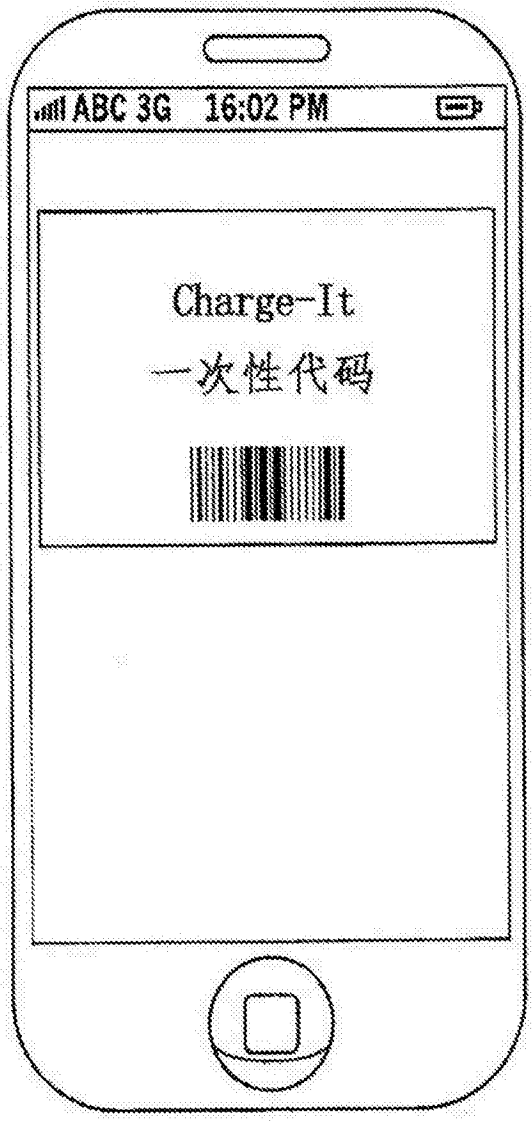


图7A

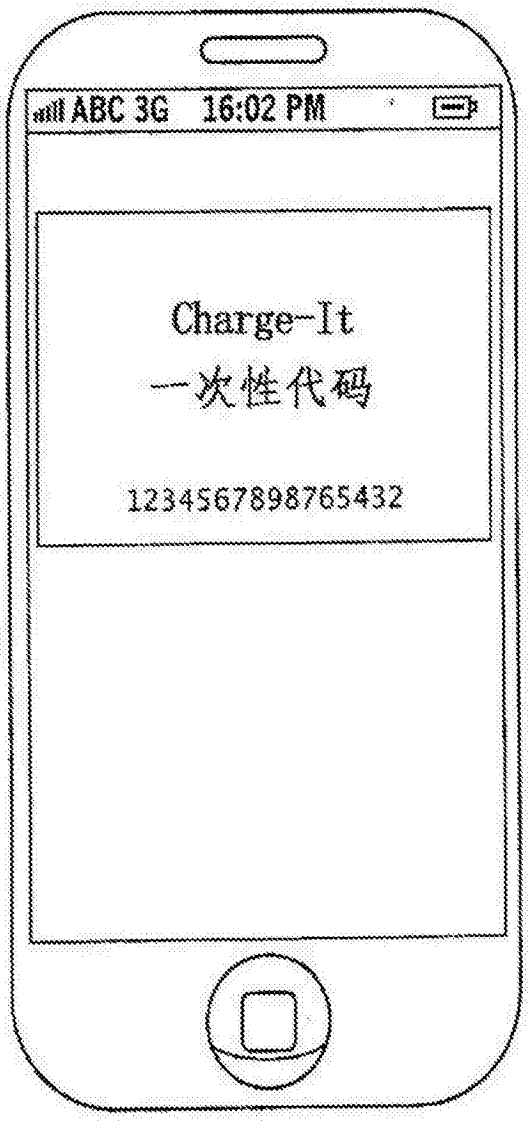


图7B

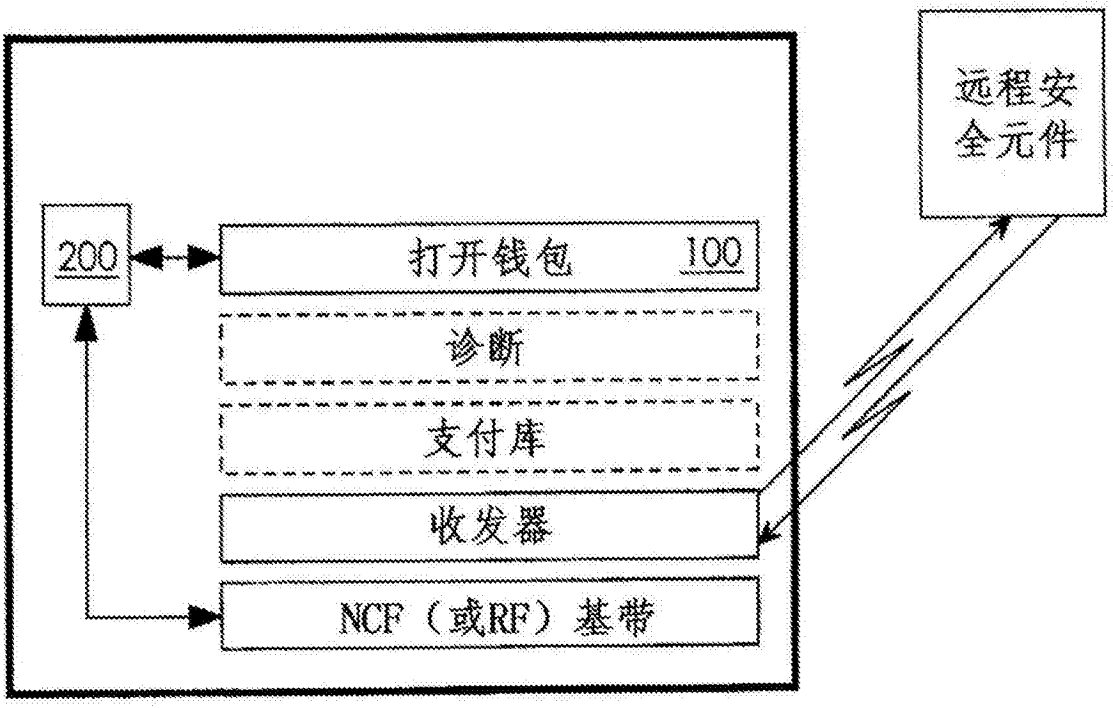

远程安全元件
200
打开钱包 100
诊断
支付库
收发器
NCF（或RF）基带

图8A

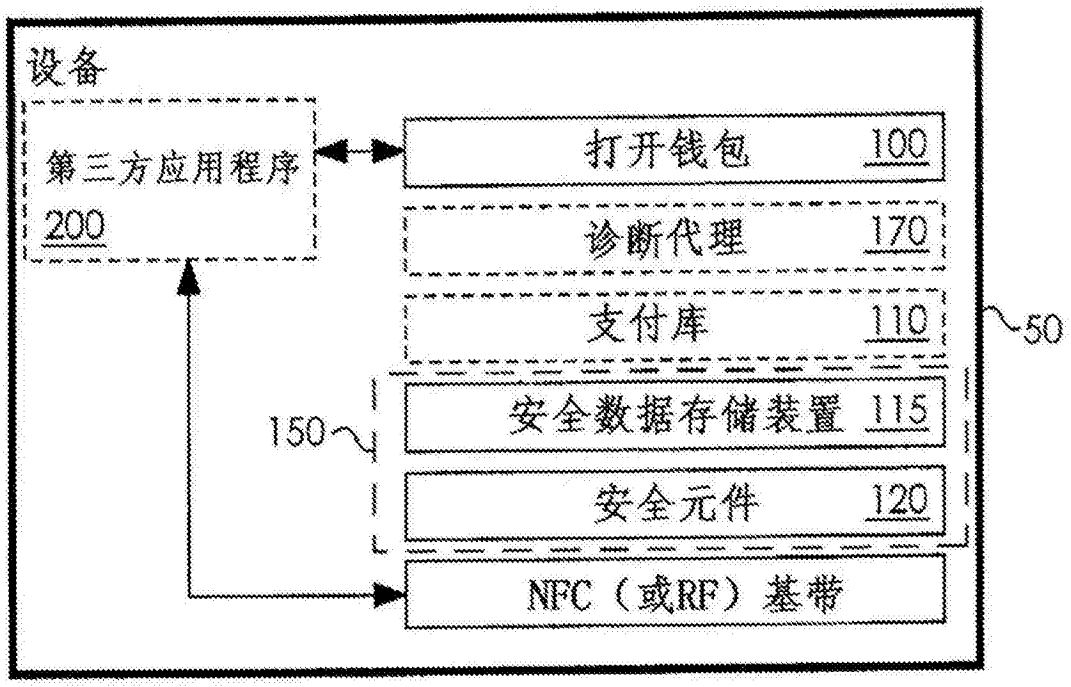

设备
第三方应用程序 200
打开钱包 100
诊断代理 170
支付库 110
50
150
安全数据存储装置 115
安全元件 120
NFC（或RF）基带

图8B

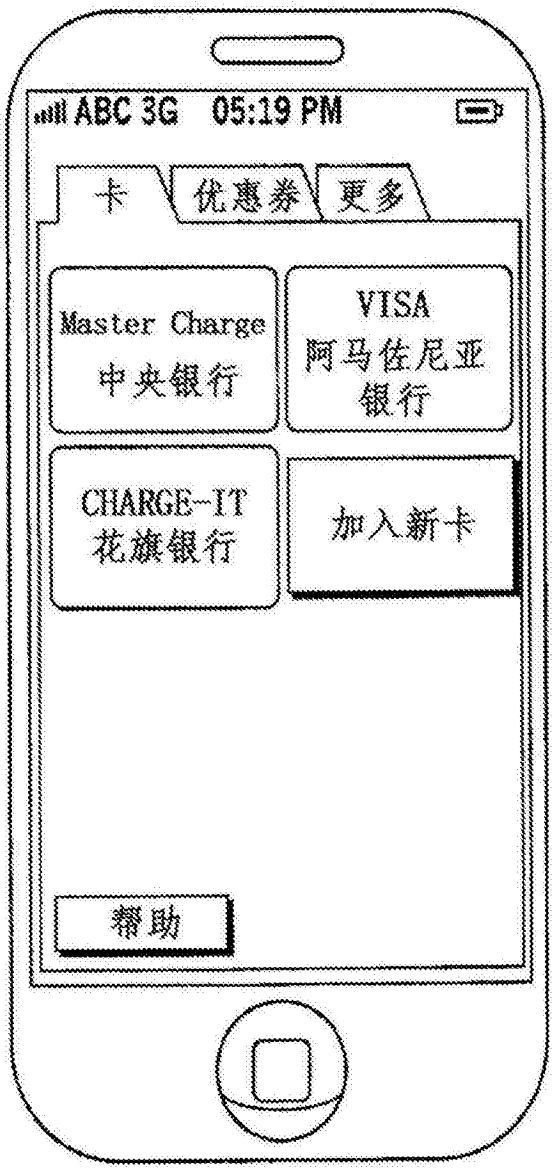

ABC 3G 05:19 PM
卡
优惠券
更多
Master Charge
中央银行
VISA
阿马佐尼亚
银行
CHARGE-IT
花旗银行
加入新卡
帮助

图9A

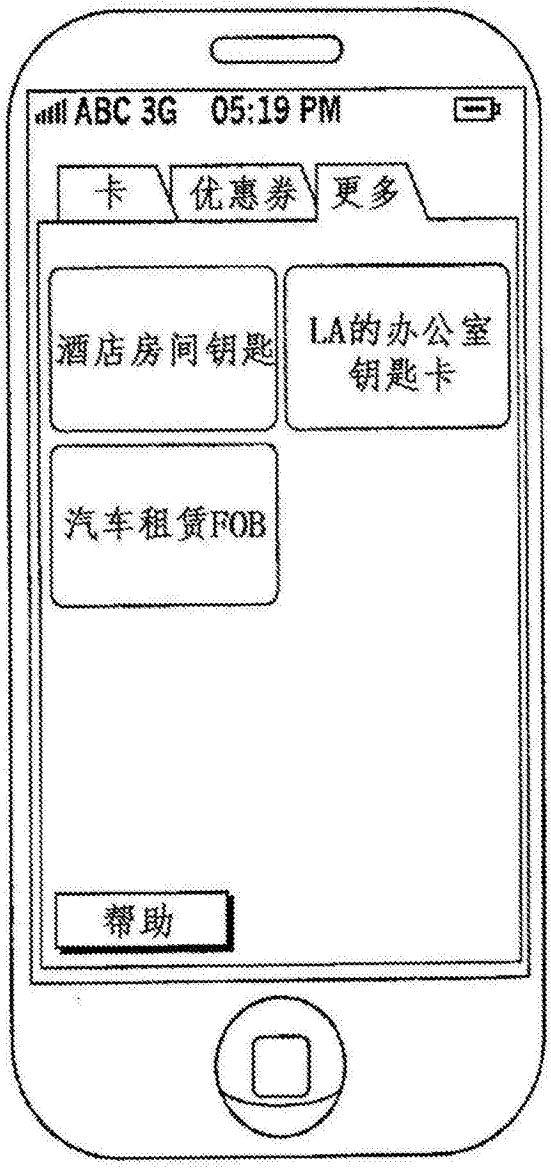


图9B

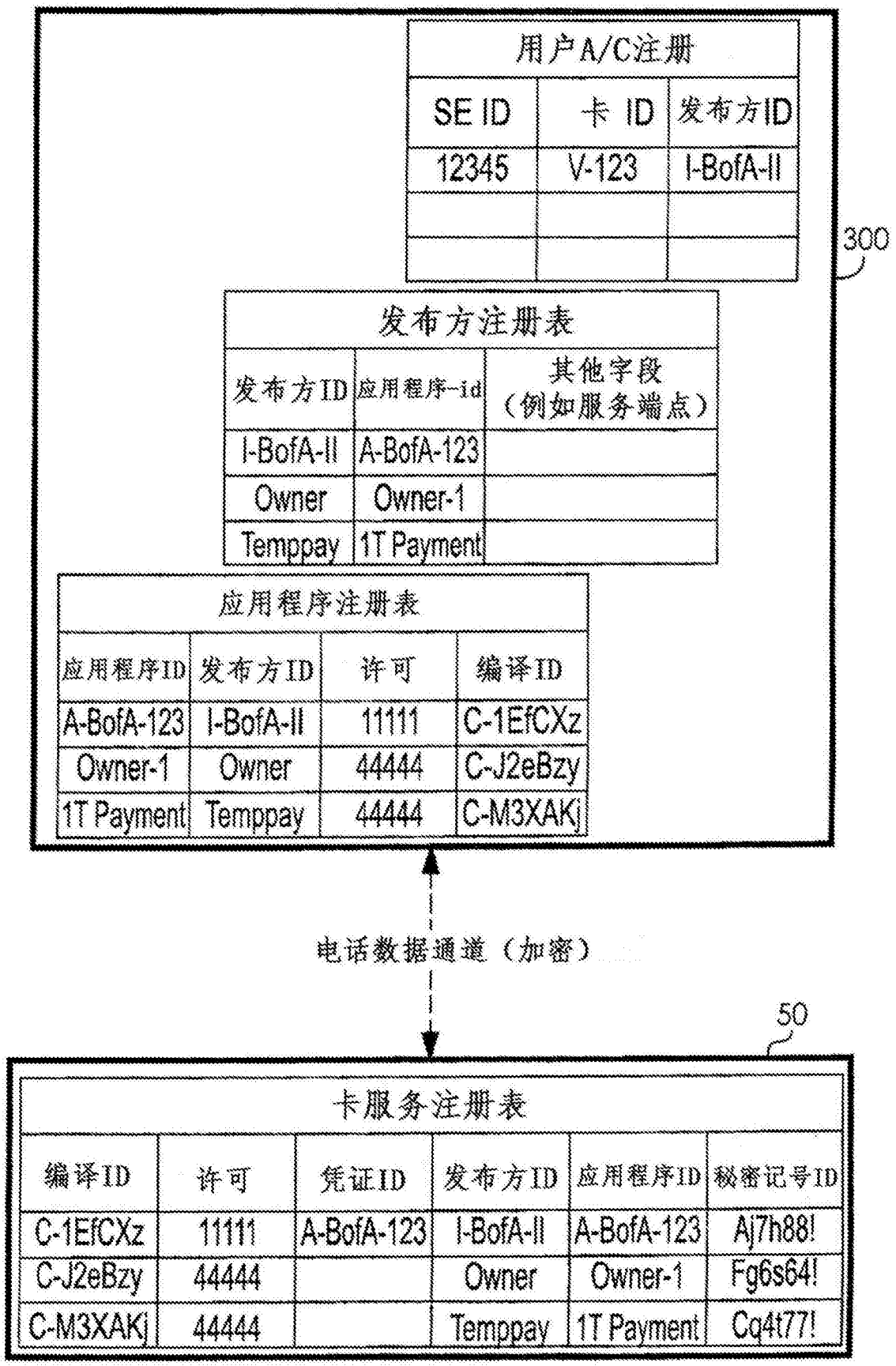

用户A/C注册
SE ID
卡 ID
发布方ID
12345
V-123
I-BofA-II
300
发布方注册表
发布方ID
应用程序-id
其他字段（例如服务端点）
I-BofA-II
A-BofA-123
Owner
Owner-1
Temppay
1T Payment
应用程序注册表
应用程序ID
发布方ID
许可
编译ID
A-BofA-123
I-BofA-II
11111
C-1EfCXz
Owner-1
Owner
44444
C-J2eBzy
1T Payment
Temppay
44444
C-M3XAKj
电话数据通道（加密）
50
卡服务注册表
编译ID
许可
凭证ID
发布方ID
应用程序ID
秘密记号ID
C-1EfCXz
11111
A-BofA-123
I-BofA-II
A-BofA-123
Aj7h88!
C-J2eBzy
44444
Owner
Owner-1
Fg6s64!
C-M3XAKj
44444
Temppay
1T Payment
Cq4t77!

图10