

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 13/00 (2006.01)

G06Q 30/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 02803418. X

[45] 授权公告日 2007 年 1 月 24 日

[11] 授权公告号 CN 1296840C

[22] 申请日 2002.10.28 [21] 申请号 02803418. X

[30] 优先权

[32] 2001.11.2 [33] KR [31] 0068082/2001

[86] 国际申请 PCT/KR2002/002009 2002.10.28

[87] 国际公布 WO2003/038712 英 2003.5.8

[85] 进入国家阶段日期 2003.7.2

[73] 专利权人 SK 电信股份有限公司

地址 韩国首尔

[72] 发明人 丁银洙 成宽济 朴钟成 催昌浩

[56] 参考文献

CN1169786A 1998.1.7 G07F19/00

KR1998 - 054903A 1998.9.25 G06K19/00

US6016476A 2000.1.18 H04L9/32

KR10 - 0207596B1 1999.7.15 G06K17/00

审查员 高琛颢

[74] 专利代理机构 中原信达知识产权代理有限责任公司

代理人 顾红霞 钟 强

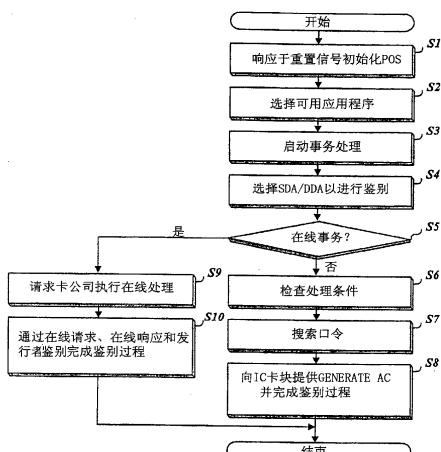
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

利用 IrFM 执行 EMV 支付过程的方法

[57] 摘要

本发明涉及最优化地利用移动终端和 POS (Point Of Sale) 终端之间的 IrFM (Infrared Financial Messaging) 执行 EMV (Europay, Master and Visa) 支付过程的方法。在本发明的方法中，如果基于写在装于移动终端中的卡芯片上的信息鉴别了购买者，则发送事务批准信息给 POS 终端，如果 POS 终端响应了一个批准，则该事务的数字收据被发送到该 POS 终端。然后如果 POS 终端请求结束事务，则释放连接会话。



1. 一种利用其中嵌有卡芯片的移动通讯终端基于 IrFM 执行 EMV 支付过程的方法，包括以下步骤：

(a) 选择一个被移动通讯终端中的卡芯片和支付处理终端支持的可用应用程序列表并启动事务处理；

(b) 在作为所述应用程序之一的卡外软件模块中，根据一个鉴别过程，检查嵌有卡芯片的移动通讯终端的用户口令，如果用户通过了鉴别，则响应于特定击键在移动通讯终端与支付处理终端之间建立一个无线链路，并通过所建立的无线链路接收来自支付处理终端的信用信息请求；

(c) 响应于所述信用信息请求，发送一个 ARQC 消息和成员资格信息给支付处理终端；

(d) 允许卡外软件模块从所述支付处理终端接收一个作为对该 ARQC 消息的响应的 ARPC 消息，并请求卡芯片鉴别发行者，并且如果该发行者通过了鉴别，则允许所述卡外软件模块发送一个从一个事务产生的数字收据到所述支付处理终端；以及

(e) 允许卡外软件模块从支付处理终端接收事务完成消息并释放该事务的连接的会话。

2. 如权利要求 1 中所述的方法，其特征在于步骤 (a) 向卡芯片提供一个用于同步的 GET PROCESSING OPTION 命令以通知事务处理已启动。

3. 如权利要求 1 中所述的方法，还包括的步骤是：

如果所述事务处理已经启动，允许包含在移动通讯终端中的卡外软件模块从卡芯片读取所述事务处理所需的数据并接收附加信息以鉴别用户。

4. 如权利要求 1 中所述的方法，其特征在于，当所述特定击键产生时，步骤 (b) 允许包含在移动通讯终端中的应用程序软件模块响应于一个连续地从支付处理终端发送的针对无线链路连接的连接请求消息，搜索一个通往支付处理终端的无线链路并将移动通讯终端连接到该无线链路。

5. 如权利要求 4 中所述的方法，其特征在于，提供所述特定键用以将操作模式切换到 IrFM 服务器模式，并且所述特定键从一个 PIN 提供。

6. 如权利要求 1 中所述的方法，还包括的步骤是：

如果从支付处理终端接收到一个批准的请求，允许所述卡外软件模块向所述卡芯片提供一个第一 GENERATE AC，以决定在线鉴别；以及

允许所述卡芯片响应于所述第一 GENERATE AC 向所述卡外软件模块提供在线鉴别判断的结果。

7. 如权利要求 1 中所述的方法，其特征在于从所述卡芯片选择并读取所述成员资格信息然后存储在一个存储器中。

8. 如权利要求 1 中所述的方法，还包括的步骤是：

如果所述 ARQC 消息和成员资格信息被发送到支付处理终端，允许支付处理终端将该成员资格信息提供给一个通讯服务提供商并将该 ARQC 消息提供给一个卡公司；以及

允许所述支付处理终端从所述卡公司接收 ARPC 消息并将该 ARPC 消息发送到包含于移动通讯终端中的卡外软件模块。

9. 如权利要求 1 中所述的方法，其特征在于，发行者鉴别通过一个检查过程来进行，该检查过程检查从支付处理终端接收的 ARPC 消息是否为具有授权批准的响应消息。

10. 如权利要求 9 所述的方法，还包括的步骤是：

如果所述 ARPC 消息是得到授权的，则向卡芯片提供一个第二 GENERATE AC 以终止与支付处理终端的事务；

允许所述卡芯片向所述卡外软件模块提供数字收据作为对第二 GENERATE AC 的响应；

允许卡外软件模块接收所述数字收据并询问所述卡芯片：与卡数据有关

的数据是否被改动；以及

如果有数据被改动，则根据改动的数据编辑所述数字收据。

11. 如权利要求 1 中所述的方法，其特征在于，如果从所述卡外软件模块接收到所述数字收据，则所述支付处理终端将该数字收据提供给一个银行服务器，从所述银行服务器电子地接收结算的金额，将事务完成消息发送到所述卡外软件模块，并释放连接的会话。

利用 IrFM 执行 EMV 支付过程的方法

发明领域

本发明涉及执行 EMV (Europay, Master and Visa) 支付过程的方法，特别涉及在移动通讯终端和作为支付处理终端的 POS (Point Of Sale) 终端之间执行最优的事务处理的方法。

现有技术

传统地，IrFM (Infrared Financial Messaging, 红外金融消息) 的基本概念与一个基于近距离无线连接方法 IrDA (Infrared Data Association, 红外数据关联) 的金融事务的简档 (profile) 相关。建议在各种环境中使用与 IrFM 相关的 PTD (Personal Trusted Device, 个人信任的设备) 金融支付方法。

IC (Integrated Circuit, 集成电路) 卡模块的操作通常通过 POS 终端执行，而且因为 IC 卡模块总是处于待命状态，所以持 IC 卡模块的购买者要命令 IC 卡模块发送响应数据，使得 IC 卡模块能响应来自 POS 终端的请求。

亦即，在基于 IrFM 执行传统 EMV 支付过程时，在 POS 终端和 IC 卡模块之间通过双向通讯执行几个事务（例如至少 9 或 10 个）。

下面参照图 1 说明在 POS 终端和 IC 卡模块之间通过双向通讯执行事务的情况。在步骤 S1 中，IC 卡模块插入 POS 终端时，响应于重置信号，POS 终端初始化或重置。

如果 POS 终端被重置，选择该 IC 卡模块支持的应用程序中用于该事务的应用程序以及 POS 终端。然后，创建可用应用程序的列表并且在步骤 S2 中从该列表中选择一个应用程序。

POS 终端然后向 IC 卡模块发出一个 GET PROCESSING OPTION 命令，例如一个同步命令，以通知 IC 卡模块，事务处理已经在步骤 S3 启动。此时，IC 卡模块响应于所述 GET PROCESSING OPTION 向 POS 终端发出一个 AFL (Application File Locator)。

然后 POS 终端从 IC 卡模块读取事务处理所需的应用程序数据。此时，在步骤 S4 确定数据是否必须用 SDA (Static Data Authentication) 或 DDA (Dynamic Data Authentication) 鉴别。

在步骤 S5，POS 终端确定是否请求了用于大笔金额在线事务的发行者鉴别，或者是否请求了用于防止通过周期性在线事务的非法使用，这在离线事务中不能检测到。

SDA 是一个对与 IC 卡模块相关的卡数据中的不可改变的数据进行鉴别的过程。执行 SDA 用于确定由发行者记录的数据是否被改动过。对 IC 卡模块执行 SDA 之后，执行 DDA 以鉴别由 IC 卡模块产生的签名。

在上述过程中，如果使用离线事务数据的 SDA，则在步骤 S6 中，POS 终端根据 POS 终端和 IC 卡模块的数据检查处理条件，包括在比较 POS 终端和 IC 卡模块的应用程序版本号时的一个条件，确定国家代码和异步传输模式是否可用并检查有效期。

在步骤 S7，POS 终端搜索从 PIN (Personal Identification Number，个人识别码) 输入的口令以确定 IC 卡模块的用户是否被授权。

在步骤 S8 中，如果口令有效，则 POS 终端根据 IC 卡模块确定的事务机制向 IC 卡模块提供一个 GENERATE AC (Application Cryptogram，应用程序密码)，从而完成鉴别过程。

在上述过程中，如果使用在线事务数据的 SDA，则在步骤 S9 中，POS

终端根据一个 ARQC (Authorization Request Cryptogram, 授权请求密码) 通过一个 VAN (Value Added Network, 增值网) 请求一个卡公司来执行在线处理。

在步骤 S10 中, 一个卡公司的主机通过在线请求、在线响应和发行者鉴别这三个步骤完成鉴别过程, 以确定是必须允许还是要拒绝该事务。

如上所述, 如果 IC 卡模块的支付过程基于 EMV, 该事务在 IC 卡模块与 POS 终端有关的状态下完成。但是, 存在无线链路断开的可能性因为 IC 卡模块与 POS 终端之间事务处理的数量增加而增高的问题。类似的, 如果传统的 IC 卡模块和 POS 终端之间的事务处理被应用到移动通讯终端使得鉴别过程和和事务能通过移动终端完成, 则事务处理数量也会增加。因此, 用户将因为用于完成移动通讯终端与 POS 终端之间的事务所需的时间太长而感到不方便。

发明内容

因此, 本发明针对上述问题。本发明的一个目的是提供一种方法, 用于利用 IrFM 来执行 EMV 支付过程, 该方法能够通过在 POS 终端与具有嵌入式 IC 的移动通讯终端之间执行一个最优事务处理来迅速执行事务和鉴别过程。

根据本发明的一个方面, 上述及其它目的能通过提供一种利用其中嵌有卡芯片的移动通讯终端基于 IrFM 执行 EMV 支付过程的方法来实现, 其步骤包括: (a) 选择一个被移动通讯终端中的卡芯片和支付处理终端支持的可用应用程序列表并启动事务处理; (b) 在作为所述应用程序之一的卡外软件模块中, 根据一个鉴别过程, 识别嵌有卡芯片的移动通讯终端的用户口令, 如果用户通过了鉴别, 则响应于特定击键将移动通讯终端连接到一个无线链路, 并通过该无线链路接收来自支付处理终端的信用信息请求; (c) 响应于所述信用信息请求, 发送一个 ARQC 消息和成员资格信息给支付处理终端; (d) 允许卡外软件模块接收一个作为对该 ARQC 消息的响应的 ARPC

(Authorization Response Cryptogram, 授权响应密码) 消息，并请求卡芯片鉴别发行者，并且如果该发行者通过了鉴别，则允许卡外软件模块发送一个与事务关联的数字收据到支付处理终端；以及 (e) 允许卡外软件模块从支付处理终端接收事务完成消息并释放连接的会话。

通过经无线链路连接在 POS 终端与嵌有 IC 的移动通讯终端之间执行更少——例如仅两个——基于 EMV 的过程，具有上述特征的本发明能快速执行事务和鉴别过程，降低无线链路断开的可能性并缩短移动通讯终端与 POS 终端之间的事务从开始到结束所需的时间。

附图简述

图 1 是显示一种用于执行传统 EMV 支付过程的流程图；

图 2 是本发明利用 IrFM 执行 EMV 支付过程的系统的框图；

图 3a 和 3b 是显示本发明的用于利用 IrFM 执行 EMV 支付过程的详细流程图。

具体实施方式

下面参照附图详细说明本发明的优选实施例。

图 2 是本发明利用 IrFM 执行 EMV 支付过程的系统的框图。该系统包括一个移动通讯终端 10 和一个 POS 终端 20。

移动通讯终端 10 是由普通用户使用的移动电话。移动通讯终端 10 中嵌有一个 IC 卡芯片 14。移动通讯终端 10 还包括一个卡外软件模块 12 以及一个 IrFM 应用程序软件模块 16 作为软件模块。

卡外软件模块 12 从 IC 卡芯片 14 选择并读取用户的成员资格信息，并将所读的成员资格信息临时地存储到存储器（未图示）中。卡外软件模块 12 从 IC 卡芯片 14 和 POS 终端 20 所支持的应用程序中选择要用于所述事务的应用程序，创建一个可用应用程序列表，并从所述列表中选择一个应用程序。

卡外软件模块 12 通知 IC 卡芯片 14 事务处理已通过发送一条 GET PROCESSING OPTION 命令——即用于同步的命令——而启动。

卡外软件模块 12 确定从 PIN 输入的口令是否有效来得知嵌有 IC 卡芯片 14 的移动通讯终端 10 的用户是授权的卡用户。如果移动通讯终端 10 的用户是授权的，则卡外软件模块 12 从用户使用的 PIN 接收一个特定的击键以将操作模式切换到 IrFM 服务器模式，并执行控制操作使得通往 POS 终端 20 的无线链路被搜索然后连接到 IrFM 应用程序软件模块 16。

如果卡外软件模块 12 连接到所述无线链路，则其从 POS 终端 20 接收信用信息请求。卡外软件模块 12 向 IC 卡芯片 14 提供第一 GENERATE AC，使得能够决定在线/离线鉴别。在决定在线鉴别的情况下，储存在存储器中的 ARQC 消息和成员资格信息被同时发送到 POS 终端 20。

从 POS 终端 20 接收作为对 ARQC 消息的响应的 ARPC 消息后，卡外软件模块 12 请求 IC 卡芯片 14 执行发行者鉴别以确定该 ARPC 消息是具有授权批准的响应消息。

从 IC 卡芯片 14 接收具有授权批准的响应消息之后，卡外软件模块 12 向 IC 卡芯片 14 提供第二 GENERATE AC，这是用于终止与 POS 终端 20 的事务的事务完成消息。卡外软件模块 12 在事务完成的时候接收从 IC 卡芯片 14 产生的数字收据。卡外软件模块 12 请求 IC 卡芯片 14 检查是否存在与卡数据有关的改动数据。如果没有改动的数据，卡外软件模块 12 发送该数字收据用于 POS 终端 20 记帐。

IC 卡芯片 14 从卡外软件模块 12 接收用于同步的 GET PROCESSING OPTION 命令，并执行控制操作以启动事务处理。响应于从卡外软件模块 12 接收的 GENERATE AC，IC 卡芯片 14 向卡外软件模块 12 提供一个表示在线鉴别请求的信号。

然后，IC 卡芯片 14 响应于从卡外软件模块 12 接收的发行者鉴别请求，向卡外软件模块 12 提供具有授权批准的响应消息。而且，IC 卡芯片 14 响应于第二 GENERATE AC 向卡外软件模块 12 提供在事务完成时产生的数字收据。

如果 IrFM 应用程序软件模块 16 从用户使用的 PIN 接收特定击键以将操作模式切换到 IrFM 服务器模式，其搜索一个无线链路以将自身连接到 POS 终端 20。当从 POS 终端 20 接收作为事务完成消息的 IrFM 截止请求消息时，IrFM 应用程序软件模块 16 截止 IrFM 然后释放所有连接的会话。

POS 终端 20 具有至少一个嵌入式 IC 卡插槽，并具有诸如基本 EMV 终端键盘的用户界面，字符 LCD (Liquid Crystal Display) 单元，PIN 键盘和与 LCD 单元分开的另一显示单元。POS 终端 20 发送一个用于无线链路连接的 IrFM 连接请求消息到嵌在移动通讯终端 10 中的卡外软件模块 12。POS 终端 20 还向卡外软件模块 12 发送信用信息请求。

然后，POS 终端 20 从卡外软件模块 12 接收 ARQC 消息和成员资格信息，将所接收的成员资格信息提供给一个通讯服务提供商 ‘A’，同时通过一个 VAN ‘B’ 将 ARQC 消息提供给一个卡公司 ‘C’。

然后，POS 终端 20 从卡公司 ‘C’ 接收 ARPC 消息并将其发送到卡外软件模块 12。从卡外软件模块 12 接收数字收据后，POS 终端 20 将该数字收据提供给银行服务器（未图示）并从银行服务器电子地接收预定数量的金额。最后，POS 终端 20 将 IrFM 截止请求消息发送到卡外软件模块 12 以关闭所有会话。

下面参照图 3a 和 3b 详细说明根据本发明的利用 IrFM 执行 EMV 支付过程的方法。

首先，如果利用 IrFM 在移动通讯终端 10 和 POS 终端之间基于 IC 卡芯片 14 执行 EMV 支付过程，则通过双向通讯进行在线事务。换言之，为了利用移动通讯终端 10 作为支付设备来购买某产品，用户利用移动通讯终端 10 执行一个最优双向事务，其中移动通讯终端 10 嵌有卡外软件模块 12 和 IrFM 应用程序软件模块作为其软件模块。

下面详细说明最优的双向事务。移动通讯终端 10 的卡外软件模块 12 从 IC 卡芯片 14 选择并读取使用移动通讯终端 10 的用户的成员资格信息，然后将所读的成员资格信息临时地存储在一个存储器（未图示）中。然后，在 IC 卡芯片 14 和 POS 终端支持的应用程序中选择要用于事务的应用程序。然后，创建一个选择的应用程序列表并且从该列表中选择一个应用程序，此为步骤 301。

选择应用程序之后，卡外软件模块 12 向 IC 卡芯片 14 提供一个用于同步的 GET PROCESSING OPTION 命令，以通知 IC 卡芯片 14 事务处理已经启动，此为步骤 302。

通知之后，卡外软件模块 12 从 IC 卡模块 14 中读取事务处理所需的数据，此为步骤 303。

在在线鉴别中，卡外软件模块 12 确定嵌有 IC 卡芯片 14 的移动通讯终端的用户是否得到了授权。如果从 PIN 输入的口令有效，则卡外软件模块 12 从用户所使用的 PIN 接收一个特定击键以将操作模式切换到 IrFM 服务器模式，并执行控制操作使得通往 POS 终端 20 的无线链路被搜索而 IrFM 应用程序软件模块 16 能通过所发现的无线链路连接，此为步骤 304。

如果从用户使用的 PIN 接收到用于切换操作模式到 IrFM 服务器模式的特定击键，IrFM 应用程序软件模块 16 响应于一个连续地从 POS 终端 20 发送的针对无线链路连接的 IrFM 连接请求消息，搜索无线链路以连接到 POS 终端 20，此为步骤 305。

无线链路连接之后，卡外软件模块 12 响应于从 POS 终端 20 接收到的信用信息请求，向 IC 卡芯片 14 提供一个第一 GENERATE AC，以确定在线还是离线鉴别，此为步骤 306。

IC 卡芯片 14 响应于从卡外软件模块 12 接收到的 GENERATE AC，提供在线鉴别判断结果给卡外软件模块 12，步骤 307。

当从 IC 卡芯片 14 接收在线鉴别判断的结果时，卡外软件模块 12 同时发送一个 ARQC 消息和存储于存储器中的成员资格信息给 POS 终端 20，此为步骤 308。

从卡外软件模块 12 接收 ARQC 消息和成员资格信息之后，POS 终端 20 将成员资格信息提供给通讯服务提供商 ‘A’，此为步骤 309，并通过 VAN ‘B’ 将 ARQC 消息提供给卡公司 ‘C’，此为步骤 310。

然后，POS 终端 20 从卡公司 ‘C’ 接收一个 ARPC 消息并将该 ARPC 消息发送给卡外软件模块 12，此为步骤 311。

从 POS 终端 20 接收作为 ARQC 消息的响应的 ARPC 消息之后，卡外软件模块 12 请求 IC 卡芯片 14 执行发行者鉴别以确定该 ARPC 消息是否为具有授权批准的响应消息，此为步骤 312。

响应于从卡外软件模块 12 接收到的发行者鉴别请求，IC 卡芯片 14 向卡外软件模块 12 提供该具有授权批准的响应消息，此为步骤 313。

从 IC 卡芯片 14 接收具有授权批准的响应消息之后，卡外软件模块 12 向 IC 卡芯片 14 提供一个第二 GENERATE AC，其为事务完成消息，用以结束当前事务，此为步骤 314。

响应于从卡外软件模块 12 接收的第二 GENERATE AC, IC 卡芯片 14 向卡外软件模块 12 提供一个在事务完成时产生的数字收据, 此为步骤 315。

卡外软件模块 12 从 IC 卡芯片 14 接收所产生的数字收据然后请求 IC 卡芯片 14 确定是否有与卡数据相关的数据被改动。如果数据被改动, 则卡外软件模块 12 编辑数字收据为数据被改动。否则, 卡外软件模块 12 将数字收据发送到 POS 终端 20, 此为步骤 316。

从卡外软件模块 12 接收数字收据后, POS 终端 20 将该数字收据提供给银行服务器(未图示)以结算该事务, 然后从银行服务器电子地接收结算的金额。POS 终端 20 将一个 IrFM 截至请求消息发送到卡外软件模块 12 以释放所有连接的会话, 此为步骤 317。

当从 POS 终端 20 接收 IrFM 截至请求消息时, 卡外软件模块 12 截至 IrFM 并关闭其打开的会话, 此为步骤 318。

利用嵌有 IC 卡芯片的移动通讯终端, 支付过程可以在加油站、售货机、收费站以及停车处的控制设备上执行, 使得利用 IrFM 执行 EMV 支付过程的移动通讯终端能应用于各种应用领域。

尽管用优选实施例对本发明进行说明, 本发明一般技术人员应理解, 不脱离权利要求所披露的本发明的范围和精神, 也可以作出各种修改、变化和替换。

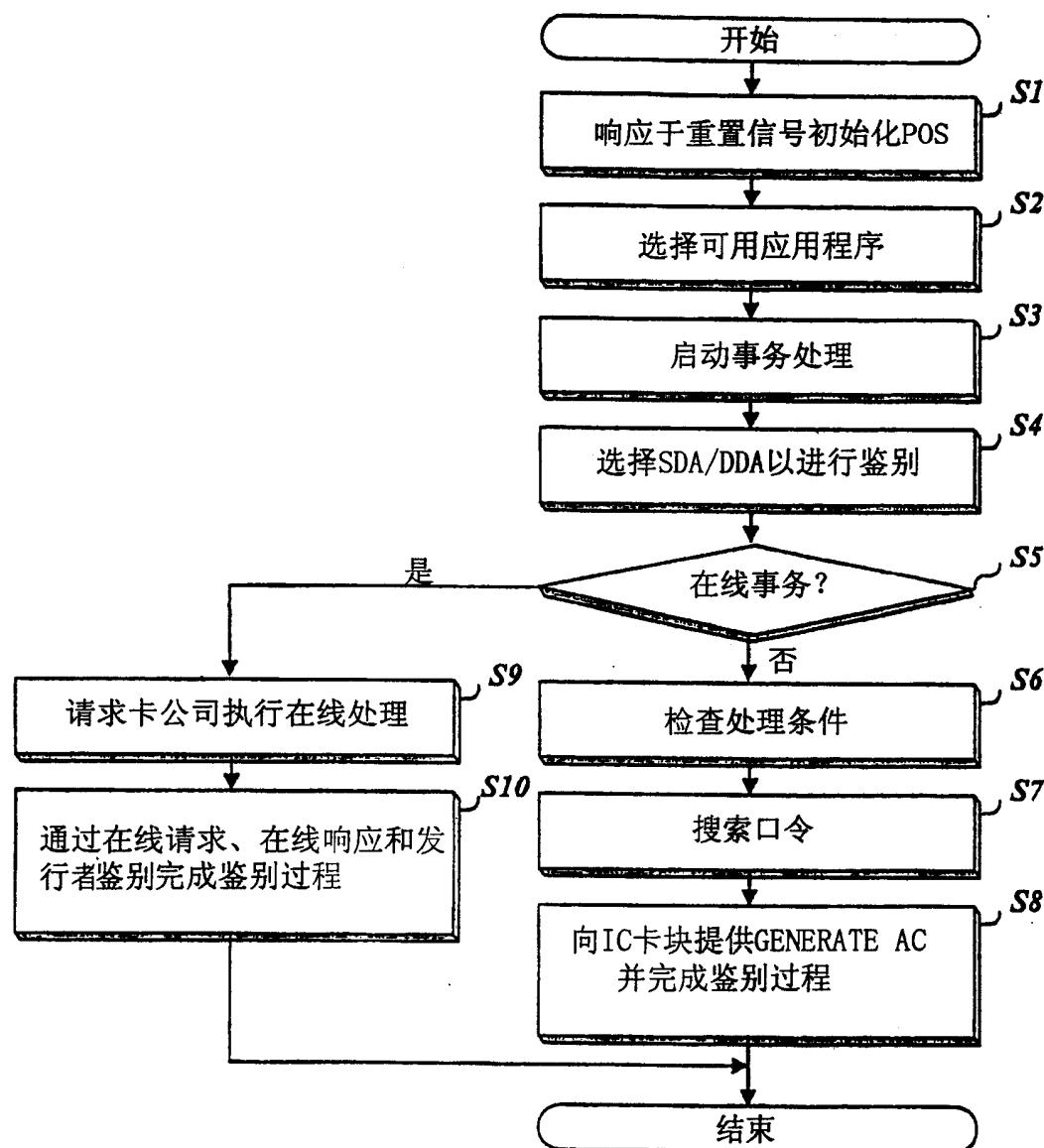


图 1

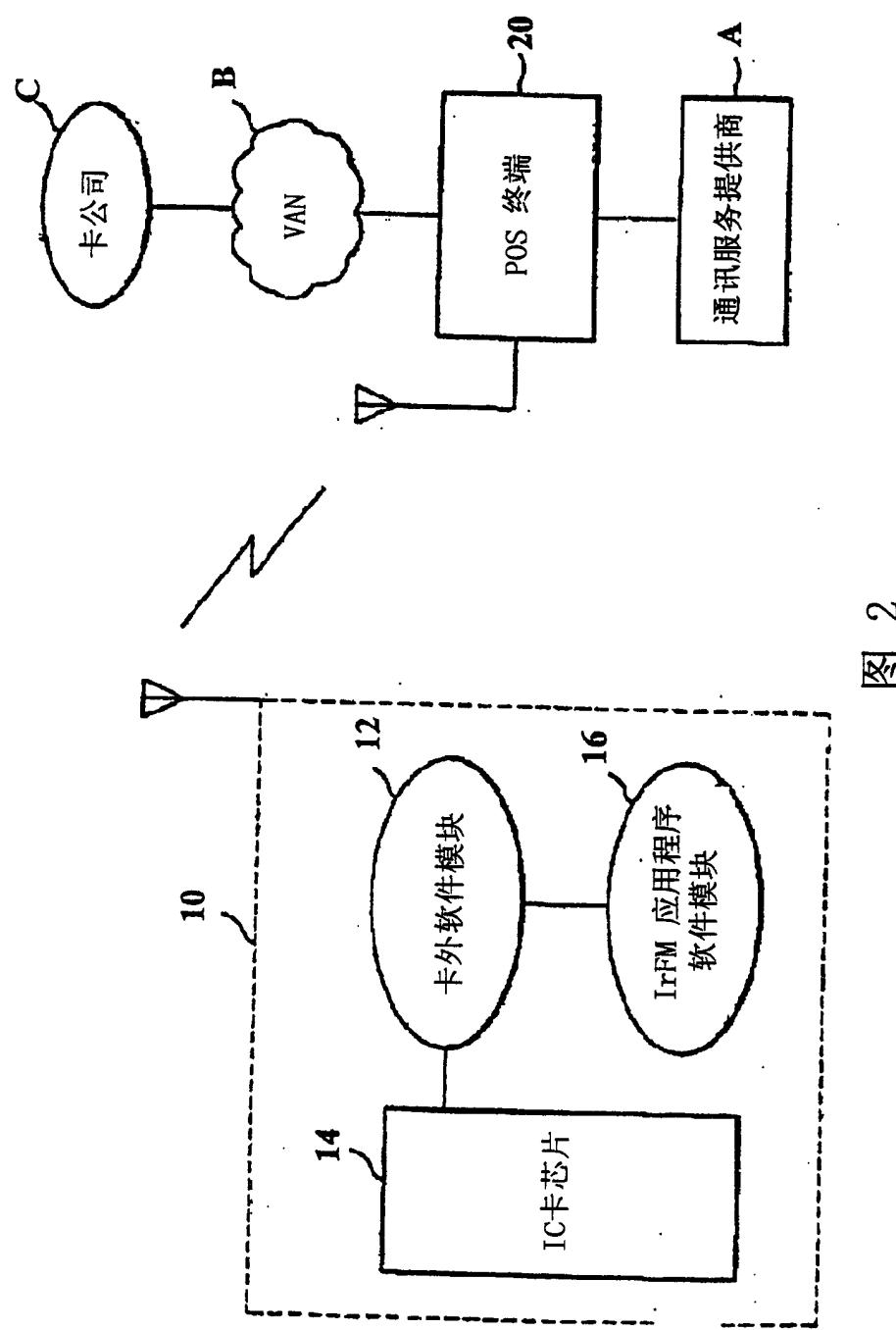


图 2

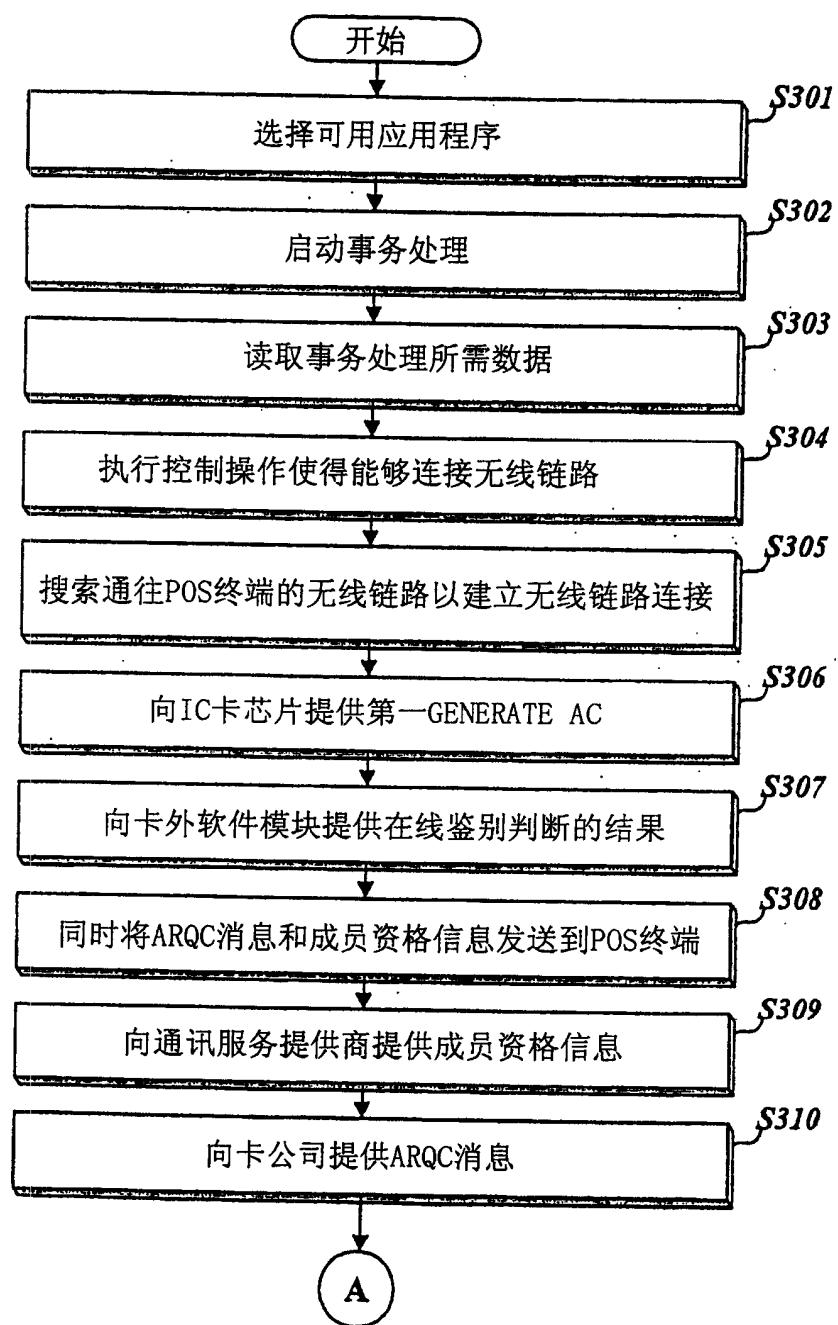


图 3a

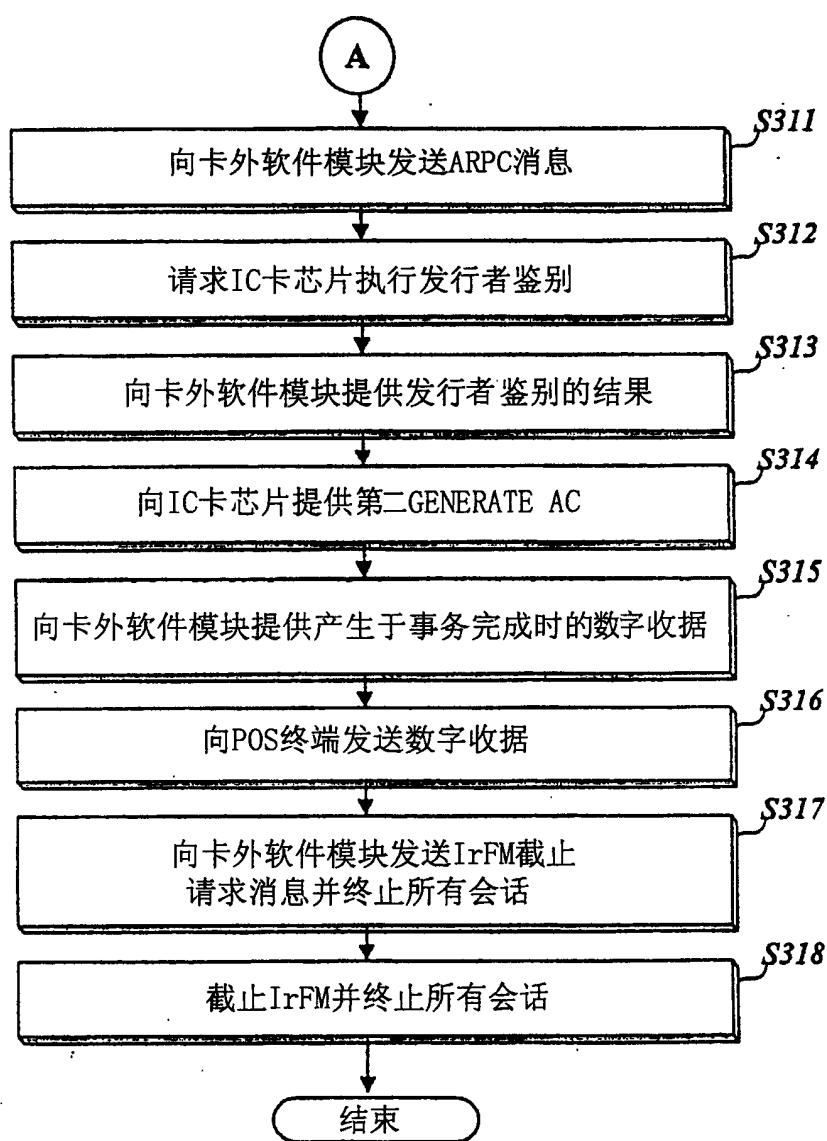


图 3b