[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/02 (2006.01)
G06F 17/00 (2006.01)
G06Q 40/00 (2006.01)
H04L 29/02 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610086565.1

[45] 授权公告日 2008 年 11 月 26 日

[11] 授权公告号 CN 100438409C

[22] 申请日 2006.6.22

[21] 申请号 200610086565.1

[73] 专利权人 北京飞天诚信科技有限公司

地址 100083 北京市海淀区学院路 40 号研 7A 楼 5 层

[72] 发明人 陆 舟 于华章

[56] 参考文献

WO01/27779A1 2001.4.19

CN2929835Y 2007.8.1

WO2005/052801A1 2005.6.9

CN1773528A 2006.5.17

审查员 寇利敏

[74] 专利代理机构 北京中海智圣知识产权代理有限公司

代理人 曾永珠

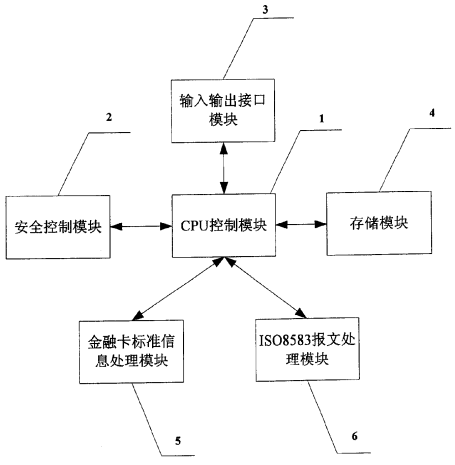
权利要求书 2 页 说明书 10 页 附图 5 页

[54] 发明名称

具有金融交易报文处理能力的智能卡及其工作方法

[57] 摘要

本发明公开了一种具有金融交易报文处理能力的智能卡，包括 CPU 控制模块、安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块和 ISO8583 报文处理模块，其中 CPU 控制模块分别连接并控制安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块、ISO8583 报文处理模块。本发明的工作方法，包括处理金融卡标准信息；ISO8583 报文信息。本发明将 ISO8583 报文处理功能集成到智能卡中以后，能够提高金融交易的安全性，有效防止利用金融交易终端安全漏洞牟取不义之财的非法行为；扩大金融卡的使用范围，使个人计算机受理金融卡交易成为可能，极大地方便了持卡人的各种金融交易活动。



1.一种具有金融交易报文处理能力的智能卡，包括 CPU 控制模块、安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块、CPU 控制模块分别连接并控制安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块，其特征在于：还包括 ISO8583 报文处理模块，CPU 控制模块连接并控制 ISO8583 报文处理模块，所述 ISO8583 报文处理模块对输入的原始数据进行组织、打包，并对接收到的 ISO8583 报文包进行解包和处理。

2. 根据权利要求 1 所述的具有金融交易报文处理能力的智能卡，其特征在于：所述智能卡是接触式智能卡或非接触式智能卡。

3. 根据权利要求 1 所述的具有金融交易报文处理能力的智能卡，其特征在于：所述智能卡集成在便携设备中。

4. 根据权利要求 3 所述的具有金融交易报文处理能力的智能卡，其特征在于：所述便携设备是手机、PDA、PocketPC、USB TOKEN、U 盘、MP3 播放器或移动存储器。

5. 一种具有金融交易报文处理能力的智能卡的工作方法，包括以下步骤：

（1）在其内部处理金融卡标准信息；

（2）取得交易数据；

（3）生成上送 ISO8583 报文；

（4）将 ISO8583 报文传送到金融交易终端；

（5）将 ISO8583 报文传送到服务提供商的系统。

6. 根据权利要求 5 所述一种具有金融交易报文处理能力的智能卡的工作方法，其特征在于：还包括如下步骤：

（6）取得从金融交易终端和服务提供商的系统返回的报文包；

（7）解析 ISO8583 报文；

（8）解析交易信息；

（9）提取相应信息并传送到终端输出；

（10）更新卡内信息。

7. 根据权利要求 5 所述一种具有金融交易报文处理能力的智能卡的工作方法，其特征在于：所述金融卡标准信息为 EMV/PBOC 规范相关信息。

具有金融交易报文处理能力的智能卡及其工作方法

技术领域

本发明涉及金融电子交易系统，具体来说是涉及一种具有金融交易报文处理能力的智能卡及其方法。

背景技术

随着金融电子化的不断发展，智能卡的应用越来越普及。智能卡的名称来源于英文名词“Smartcard”，又称集成电路卡，即 IC 卡(Integrated Circuit card)。它将一个集成电路芯片镶嵌于塑料基片中，封装成卡的形式，其外形与覆盖磁条的磁卡相似。它一出现，就以其超小的体积、先进的集成电路芯片技术以及特殊的保密措施和无法破译及仿造的特点受到普遍欢迎。在智能卡使用的某些领域，它们只是仅仅提供受保护的非易失性存储。更高级的智能卡还有微处理器和内存，用于安全的处理和储存，并且可以用于使用公共密钥或者共享密钥算法的安全应用程序。智能卡上的非易失性存储是最宝贵的资源，可用于保存密钥和数字证书。一些智能卡有单独的加密协处理器，支持像 RSA、DES 和 3DES 这样的算法。智能卡不包含电池，只有在和读卡机连接的时候才被激活。当它被连接时，在执行一个复位序列之后，卡片处于非激活状态，等待接收来自客户端（主机）应用程序的命令请求。智能卡可以分为可接触和非可接触。可接触智能卡通过读卡器和智能卡的 8 个触点物理接触来通讯并工作，而非可接触智能卡依靠在小于 2 英尺（60.96 厘米）的一般距离之内的射频信号通讯。

非接触智能卡的射频通信基于类似于用于保存反盗窃和记录清单的射频标识符(RFID)标记的技术。随着技术的发展，智能卡也可以被集成到便携设备中了。手机、PDA、PocketPC、USB TOKEN、U盘、MP3 播放器和移动存储器等都属于便携设备。这些设备的一个共同特点就是体积小、易携带，因此受到了用户的青睐。目前，智能卡被广泛地应用于电话卡、金融卡、身份识别卡以及移动电话、付费电视等领域。

为了规范智能卡，国际标准化组织指定了一系列标准，其中ISO7816-3 规定了电源、信号结构以及智能卡与诸如终端这样的接口设备间的信息交换，包括信号速率、电压电平、电流数值、奇偶约定、操作规程、传输机制以及与智能卡的通信。可以说，该标准能够保证在智能卡与终端之间正确传输数据，防止智能卡与终端之间的通讯数据被非法窃取和篡改。

EMV 标准是三大信用卡国际组织（Europay、MasterCard、VISA）联合制定的银行芯片卡应用统一技术标准。符合 EMV 标准的银行卡（智能卡）具有强大的防欺诈功能，其中的个人信息很难被复制。与磁条卡相比，EMV 标准芯片卡内部的信息能够得到更好的保护，避免受到破坏和恶意窃取。芯片中加密的信息可以极大的减少持卡人、商户和银行的风险。同时，它还可以存储更多的信息，如会员信息、奖励积分，乃至饮食习惯和健康状况等个人信息。

目前，作为国内金融行业标准的《中国金融集成电路（IC）卡规范》（简称 PBOC 标准），是在符合国际金融 IC 卡发展趋势的前提下，

在兼容 EMV 规范的原则基础上，结合国内实际需求而制定的金融 IC 卡行业标准。目前，PBOC 2.0 是我国金融 IC 卡的最新标准。

国际标准化组织（ISO）在银行卡有关领域，制定了一系列标准和规范，从银行卡的物理特征到记录技术，以及银行使用银行卡的一些应用标准都已包括在内，其中 ISO8583 标准规定了银行卡应用系统间交换信息的规范及数据安全保密接口。银行卡交换中心与 ATM、EFT/POS 等金融终端之间的消息（Message）是根据《ISO 8583:1987 BANK CARD ORIGINATED MESSAGES -- INTERCHANGE MESSAGE SPECIFICATIONS -- CONTENT FOR FINANCIAL TRANSACTIONS》定义的，它规定了银行卡交易的消息交换规范。ISO8583 所规定的所有消息报文最多由 128 个字段域组成，每个域都有统一的规定，并有定长与变长之分。ISO8583 报文由以下三个部分组成：消息类型标识符（MESSAGE-TYPE-IDENTIFIER）、位图表（BITMAP）和一系列由位图表规定的数据元组成。位图表是 8583 包的核心，它是打包解包确定字段域的关键，而了解每个字段域的属性则是填写数据的基础。

目前，一般通过如下方式使用金融智能卡：智能卡负责处理 EMV/PBOC 标准信息，金融交易终端负责处理 ISO8583 报文，然后金融交易终端通过网络与服务提供商进行信息交互。这种方式使得交易的安全性很大程度上依赖于金融交易终端系统的安全性，一旦金融交易终端系统出现安全漏洞，就会给整个交易环节带来风险。犯罪分子可能会利用个人计算机系统的安全漏洞来牟取不义之财。此外，这

种方式的另一个弊端是金融卡只能由金融交易终端来受理，限制了金融卡的使用范围。

发明内容

为了克服上述缺点，本发明旨在提供一种具有金融交易报文处理能力的智能卡及其方法，可以在其内部处理 ISO8583 报文。

本发明通过以下方案实现：一种具有金融交易报文处理能力的智能卡，包括 CPU 控制模块、安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块和 ISO8583 报文处理模块，其中 CPU 控制模块分别连接并控制安全控制模块、输入输出接口模块、存储模块、金融卡标准信息处理模块、ISO8583 报文处理模块，所述 ISO8583 报文处理模块负责对输入的原始数据进行组织、打包，并对接收到的 ISO8583 报文包进行解包和处理。

所述智能卡可以是接触式智能卡，也可以是非接触式智能卡。

所述智能卡可以集成在便携设备中。

所述便携设备可以是手机、PDA、PocketPC、USB TOKEN、U 盘、MP3 播放器或移动存储器。

一种具有金融交易报文处理能力的智能卡的工作方法，包括以下步骤：

（1）在其内部处理金融卡标准信息；

（2）取得交易数据；

（3）生成上送报文；

（4）将报文传送到金融交易终端；

（5）将报文传送到服务提供商的系统。

上述方法还可以包括如下步骤：

（1）取得从金融交易终端和服务提供商的系统返回的报文包；

（2）解析报文；

（3）解析交易信息；

（4）提取相应信息并传送到终端输出；

（5）更新卡内信息。

所述金融卡标准为 EMV/PBOC 规范，所述金融卡标准信息为 EMV/PBOC 规范相关信息。

所述报文为 ISO8583 报文。

本发明的有益效果是：将 ISO8583 报文处理功能集成到智能卡中以后，能够提高金融交易的安全性，有效防止利用金融交易终端安全漏洞牟取不义之财的非法行为；扩大金融卡的使用范围，使个人计算机受理金融卡交易成为可能，极大地方便了持卡人的各种金融交易活动。

附图说明

图 1 为当前金融智能卡应用模式描述图。

图 2 为本发明应用模式描述图。

图 3 为本发明一种实施方式的示意图。

图 4 为本发明另一种实施方式的示意图。

图 5 为本发明的功能结构示意图。

图 6 为本发明中对报文信息进行打包流程图。

图 7 为本发明中对报文信息进行解包流程图。

具体实施方式

下面结合附图和具体实施例对本发明作进一步详细描述：

如图 1 所示，目前金融智能卡主要负责处理 EMV/PBOC 标准信息。金融交易终端主要负责处理 ISO8583 报文信息。两者通过网络与服务提供商进行信息交互。

如图 2 所示，本发明中所述智能卡既负责处理 EMV/PBOC 标准信息，又负责处理 ISO8583 报文信息，从而使金融交易终端和个人计算机均可以处理金融交易智能卡，扩大了其使用范围，方便了人们对其进行的各种金融应用，而且提高了金融交易的安全性。

如图 3 所示，这是本发明的一种实施方式，智能卡直接与个人计算机（也可以是金融交易终端）连接，然后通过网络接入服务提供商一端。所述智能卡既负责处理 EMV/PBOC 标准信息，又负责处理 ISO8583 报文信息。所述智能卡可以通过个人计算机和网络将处理后包含发送者、接受者、数额以及交易序列号等信息的报文传递到服务提供方。所述智能卡可以是接触式智能卡，也可以是非接触式智能卡（内嵌天线）。相应地，个人计算机上配有智能卡读卡器/刷卡器或接收智能卡发出的信号的装置。借助于个人计算机上的键盘，可以输入交易信息。

如图 4 所示，这是本发明的另一种实施方式，智能卡被集成到了便携式移动设备中，便携式移动设备通过无线网络接入服务提供商一端。此时，智能卡以类似于手机中的 SIM 卡的形式存在，而所述便

携式移动设备具有终端的功能。所述智能卡既负责处理 EMV/PBOC 标准信息，又负责处理 ISO8583 报文信息。所述智能卡可以通过网络将处理后包含发送者、接收者、数额以及交易序列号等信息的报文传递到服务提供商处。所述便携式移动设备能够读取并将智能卡上存储和产生的信息通过无线网络传递到服务提供商一方，也能够接收并处理从服务提供商一方发送过来的信息。用户借助于便携式移动设备的按键、手写或语音识别等方式输入交易信息或发出指令。交易结果显示在便携式移动设备的显示屏上。

当然，便携设备也可以通过有线或无线的方式连接到个人计算机，再通过个人计算机间接连接到网络，最后通过网络连接到服务提供商那里。这种实施方式类似于第二种实施方式，此处就不详细描述了。

如图 5 所示，智能卡主要包括以下功能模块：CPU 控制模块 1、安全控制模块 2、输入输出接口模块 3、存储模块 4、金融卡标准信息处理模块 5 和 ISO8583 报文处理模块 6。所述智能卡上含有卡片操作系统（COS）固件。所述存储模块 4 可以是 EEPROM（电可擦除可编程只读存储器）或 Flash Memory（快擦写存储器）等，可以存放持卡人个人数据，如身份证号码、银行帐号和有效期等。所述金融卡标准信息处理模块 5 负责处理 EMV/PBOC 标准信息。所述 ISO8583 报文处理模块 6 负责对输入的原始数据进行组织、打包，并通过通讯手段将 ISO8583 报文信息包发送到服务提供商那里，反过来也可以对接收到的 ISO8583 报文包进行解包、处理。

APDU（Application Protocol Data Units）是用于对智能卡进行操作的一套指令。为了实现本发明，需要对 APDU 指令集进行相应地扩展，以使其支持智能卡内的 ISO8583 报文处理。如增加在智能卡内对 ISO8583 报文进行打包、解包的命令等。

消息类型标识符（MESSAGE-TYPE-IDENTIFIER）是一个 4 位数字的字段，指明消息的交易类型，其定义事例如下：

0100 授权类请求消息（授权、撤消授权。余额查询等）

0110 授权类应答消息（授权、撤消授权。余额查询等）

位图表 BITMAP 就是对消息报文格式的描述，每一位用“0”或“1”来表示与该位对应的数据元不存在或存在，用来对其后的数据元进行索引。位图表的第一位设为“1”，表示使用扩展位图（128 个域），否则表示只使用基本位图（64 个域）。对于授权/撤消授权类交易只使用基本位图，因此位图表第一位设为“0”。

ISO8583 标准定义的数据元包括 A 字母、B 二进制位等。ISO8583 的标准文献中有对这些数据元更详细的描述，并且在应用中可对基本数据类型进行任意组合，从而构造出新的数据类型。

ISO8583 标准的程序实现包括如下步骤：

1、 数据元类型描述：根据 ISO8583 标准规定，用类 ISO_8583 来描述一个数据元的属性。

2、 数据元定义：为了实现通用的打包/解包接口，在对数据元进行定义时需要一种通用的数据元类型，这种类型应涵盖 ISO8583 标准中 128 个数据元所有可能出现的各种类型。

3、 消息处理：提供ISO8583的打包和解释报文的函数功能，不同的银行可以定义不同的交易报文格式。用类ISO_8583_MESSAGE实现消息处理，简化了ISO8583消息操作的复杂性，为应用提供了一个通用的打包和解包的接口。解包和打包处理在程序实现中类似于两个互逆的操作过程。在解包时进行如下处理：首先进行预处理，即将收到的消息中的报文类型标识符和位图表去掉，其余部分作为一个原封不动的字符串保留在一个定义的用于存放解包数据的存储区域中，并不进行继续解包。而实际上当某个应用需要对数据元进行具体访问时，真正的解包操作才发生，并且处理函数只为该应用解释它要访问的那个位域。

一笔交易的基本过程是这样的：智能卡或集成了智能卡的便携设备接收原始数据，作基本的合法性检查和预处理，组成交易请求报文，传送到服务提供商系统，服务提供商系统接收到交易请求，根据交易控制信息驱动相应的应用模块，处理相应的业务，处理结果返回终端系统和智能卡。

对 ISO8583 报文信息的打包和解包操作都是在智能卡内部完成的。

如图6所示，这是一个对ISO8583报文进行打包的过程。首先，步骤 61，获取交易数据。所述交易数据可以来自用户输入，也可以是由系统生成的，包括具体的交易信息。然后，步骤 62，生成上送报文。其中，包括组成 BITMAP（即上文所述的位图表）、填写交易

信息域和计算 MAC（Message Authentication Code，消息验证码）域等子步骤。之后，步骤 63，将报文传送到金融交易终端。最后，步骤 64，将报文传送到服务提供商的系统，从而完成通讯。

解包基本是一个与打包相反的过程，参见图 7。首先，步骤 71，取得从金融交易终端和服务提供商的系统返回的报文包。然后，步骤 72，解析报文。相应地，其中包括解析 BITMAP、验证 MAC 域等子步骤。接下来，步骤 73，解析交易信息。之后，步骤 74，提取相应信息并传送到终端输出。最后，步骤 75，对卡内的信息进行相应的更新，并且在金融交易终端输出相应信息。

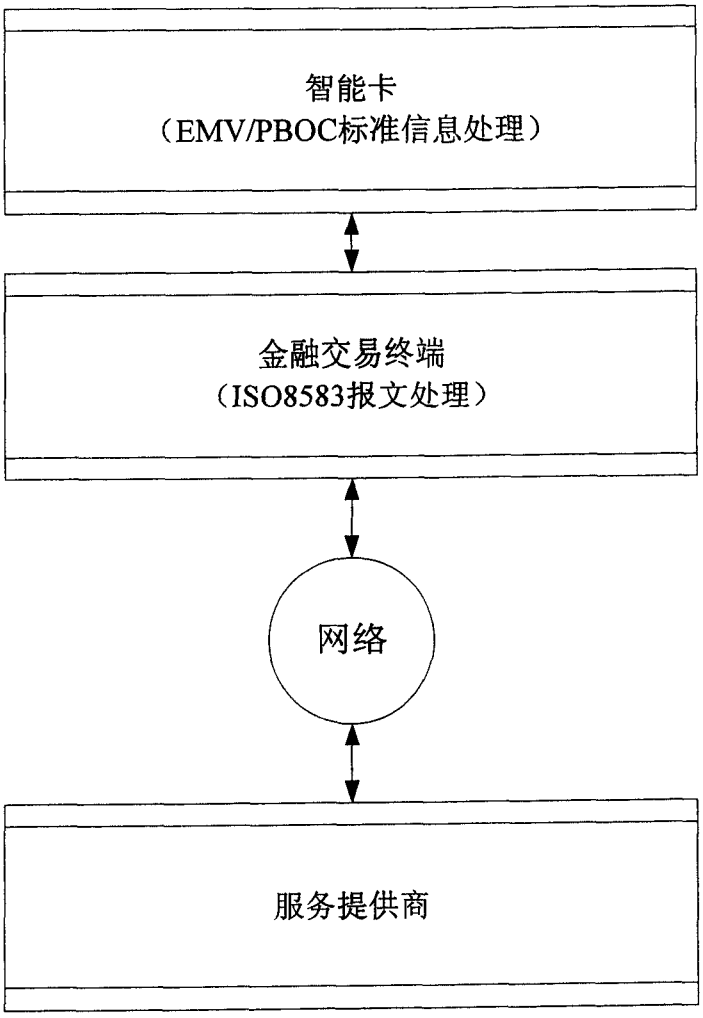


图 1

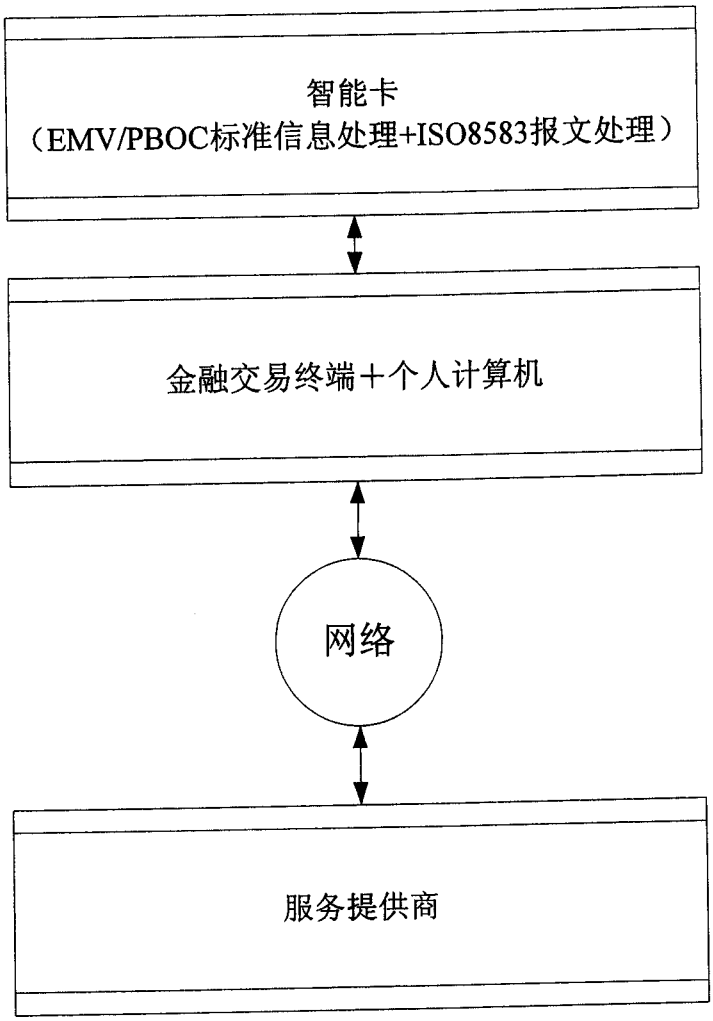

智能卡
（EMV/PBOC标准信息处理+ISO8583报文处理）
金融交易终端＋个人计算机
网络
服务提供商

图 2

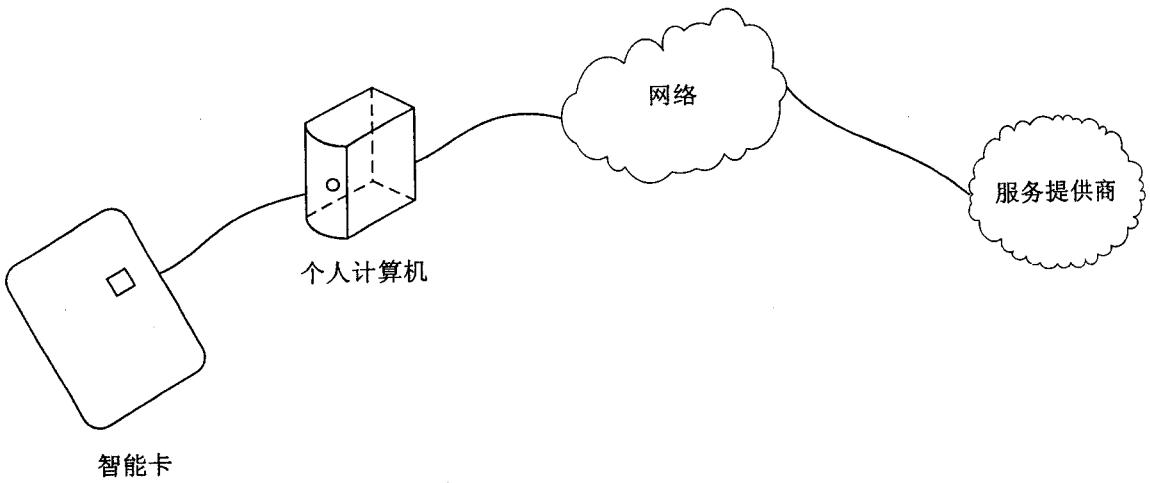

网络
服务提供商
个人计算机
智能卡

图 3

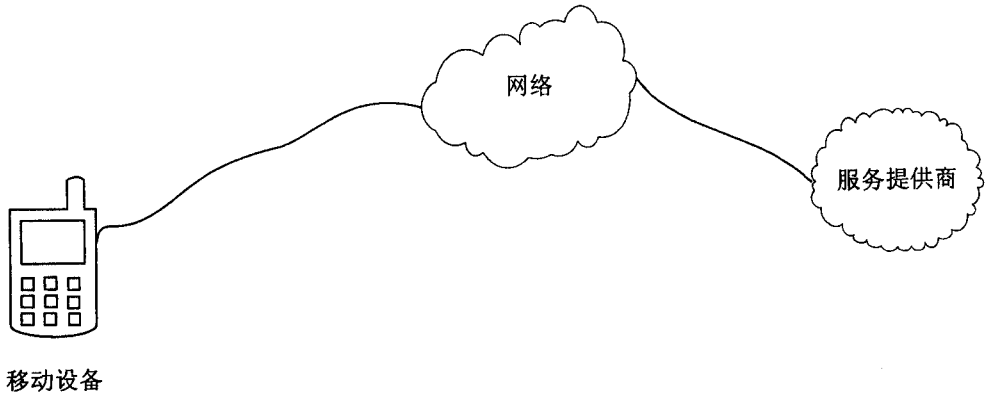

网络
服务提供商
移动设备

图 4

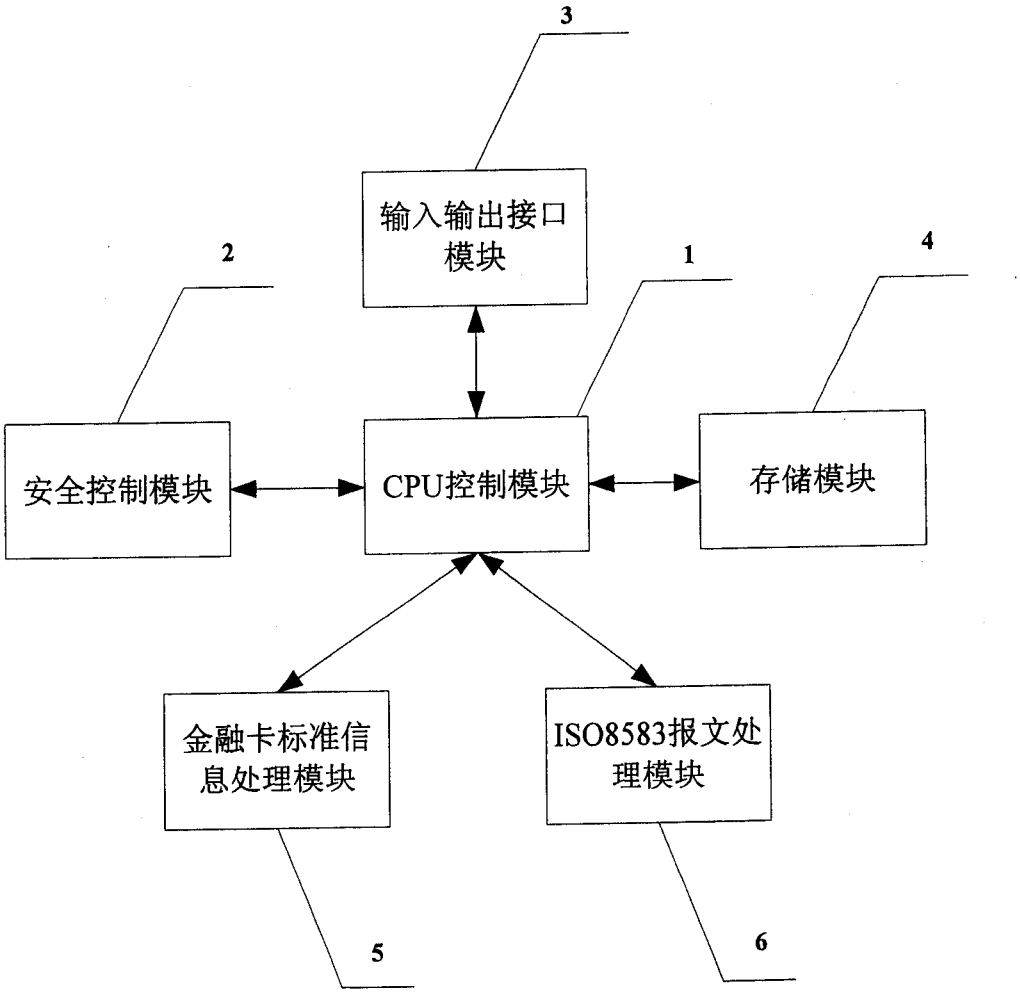

3
输入输出接口模块
2
1
4
安全控制模块
CPU控制模块
存储模块
金融卡标准信息处理模块
ISO8583报文处理模块
5
6

图 5

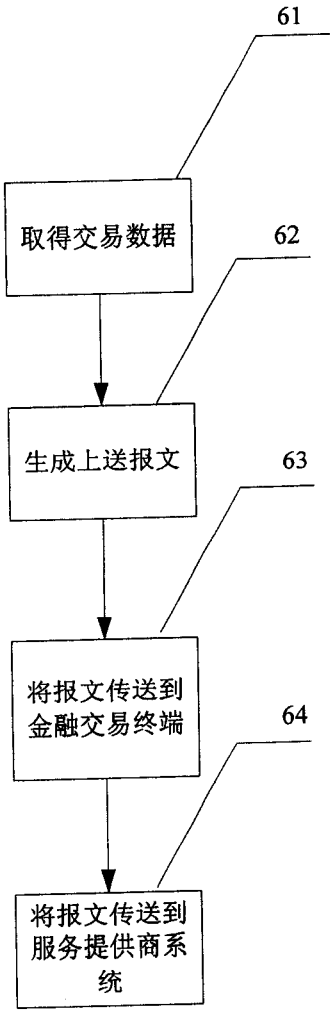


图 6

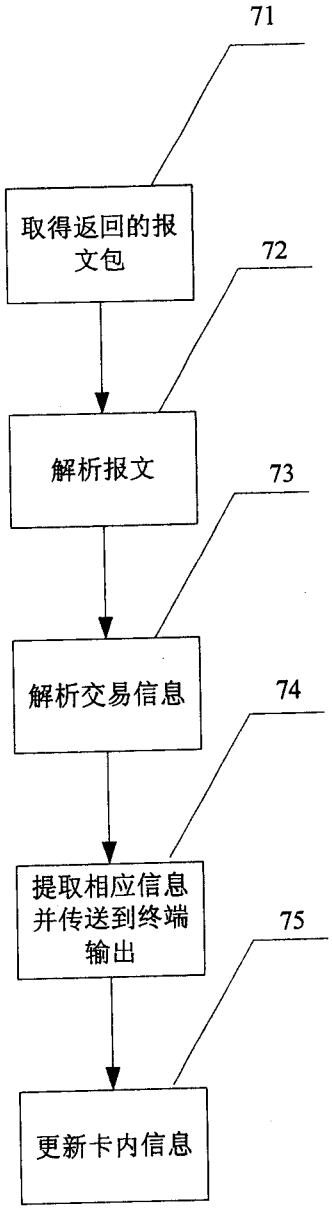


图 7