(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 101882233 A
(43)申请公布日 2010.11.10

(21)申请号 201010190929.7

(22)申请日 2010.06.02

(71)申请人 方亚南
地址 100036 北京市西城区金融大街 23 号平安大厦 11 楼
申请人 卢新华
潘松

(72)发明人 方亚南 卢新华 潘松

(74)专利代理机构 北京中北知识产权代理有限公司 11253
代理人 卢业强

(51)Int.Cl.
G06K 19/07(2006.01)
G07F 7/08(2006.01)

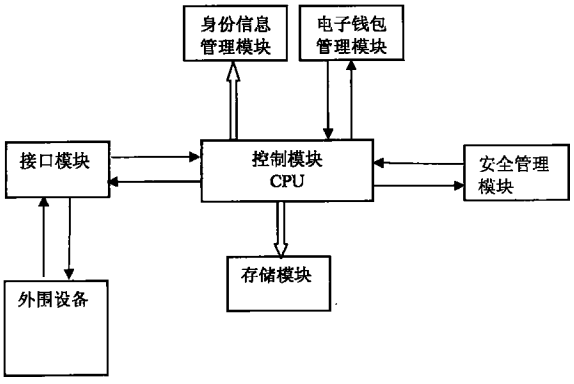
权利要求书 1 页 说明书 9 页 附图 1 页

(54)发明名称

一种多功能芯片卡

(57)摘要

本发明公开了一种多功能芯片卡，包括非接触式射频接口、USB 接口、SD 卡接口、身份信息管理模块、电子钱包管理模块、控制模块、安全管理模块和存储模块，所述芯片卡内存有用户 SIM 卡的序列号。其中，所述身份信息管理模块内置有用户身份信息；所述电子钱包管理模块对电子钱包的交易、余额、充值和消费等数据进行管理；所述安全管理模块对外部输入的信息进行安全监控。所述芯片卡进一步包括卡基接口。本发明不仅解决了支付卡在终端上可以近距离、中距离、远距离支付并存的问题，而且解决了支付卡的安全管理问题，实现金融卡和移动通信网络的有效结合，达到一卡多用的目的。



CN 101882233 A

1. 一种多功能芯片卡，其特征在于：包括非接触式射频接口、USB 接口、SD 卡接口、身份信息管理模块、电子钱包管理模块、控制模块、安全管理模块和存储模块，所述芯片卡内存有用户 SIM 卡的序列号；其中，

所述身份信息管理模块：内置有用户身份信息，在控制模块的控制下，其对用户身份信息进行验证；

所述电子钱包管理模块：在控制模块的控制下，对电子钱包的交易、余额、充值和消费等数据进行管理，并将处理结果反馈给控制模块；

所述控制模块：将外部输入的信息送入安全管理模块，根据安全管理模块的反馈结果控制身份信息管理模块、电子钱包管理模块和存储模块进行相应操作，或不进行任何操作；

所述安全管理模块：对外部输入的信息进行安全监控，若信息合法则允许控制模块执行相应操作，若信息不合法则禁止控制模块执行相应操作；还对安全信息进行初试化和修改设置；

所述存储模块：在控制模块的控制下，对信息进行存储。

2. 根据权利要求 1 所述的多功能芯片卡，其特征在于：所述芯片卡还包括卡基接口；所谓卡基，是指主要由射频天线和基础电路组成的一个类似于卡片的设备，此设备不能单独工作，必须与芯片卡结合才能工作。

3. 根据权利要求 2 所述的多功能芯片卡，其特征在于：所述芯片卡与所述卡基结合后的卡片频率为 13.56MHz。

4. 根据权利要求 1 或 2 所述的多功能芯片卡，其特征在于：所述芯片卡还包括数字证书模块，其由控制模块控制，用于网络银行支付的数字签名，所述网络包括有线网络和无线网络。

5. 根据权利要求 1 或 2 所述的多功能芯片卡，其特征在于：所述芯片卡还包括支付限制模块，其由控制模块控制，在无源模式下，若支付金额或支付次数超出参数限制的范围，则所述支付限制模块将临时锁定支付功能。

6. 根据权利要求 5 所述的多功能芯片卡，其特征在于：所述支付限制模块包含单笔消费限制、累计消费限制、累计消费次数限制、单日消费限制和单日消费次数限制参数。

7. 根据权利要求 1 或 2 所述的多功能芯片卡，其特征在于：所述用户 SIM 卡的序列号存储在所述存储模块或所述身份信息管理模块内。

8. 根据权利要求 1 或 2 所述的多功能芯片卡，其特征在于：所述安全信息主要是指密钥信息和操作的权限信息。

一种多功能芯片卡

技术领域

[0001] 本发明涉及一种芯片卡，属于半导体领域。

背景技术

[0002] 目前，移动电子商务蓬勃发展，移动支付已经成为新一代支付方式，手机银行、手机电子钱包在国内外蓬勃发展，银行、移动通信公司以及很多第三方企业都在移动互连网上投入巨大的资源研究和试点移动电子商务、移动支付和移动多应用系统，由于移动通信网络和金融网络相对独立，政府机关也是分别对移动通信服务业和金融服务业进行监管。因此，对于手机支付、手机银行等同时跨金融、通信体系的应用，目前的各种手机非接触技术很难解决之间的安全、应用管理方面的冲突和协作问题。比如说，金融体系的安全和通信系统的安全需求不同、金融信息在手机里的安全性保障、电子钱包的管理主体等。对于这些问题，目前不管是NFC技术、RFSIM技术、SIMPASS双界面卡技术、还是贴片卡技术，它们都不能从根本上解决以上问题，因此，严重限制和阻碍了我国的移动电子商务、移动电子支付的发展。

发明内容

[0003] 本发明的技术解决问题是：克服现有技术的不足，提供一种多功能芯片卡，不仅解决了支付卡在终端上可以近距离、中距离、远距离支付并存的问题，而且解决了支付卡的安全管理问题，实现金融卡和移动通信网络的有效结合，达到一卡多用的目的。

[0004] 本发明的技术解决方案是：本发明提供的一种多功能芯片卡，包括非接触式射频接口、USB接口、SD卡接口、身份信息管理模块、电子钱包管理模块、控制模块、安全管理模块和存储模块，所述芯片卡内存有用户SIM卡的序列号；其中，

[0005] 所述身份信息管理模块：内置有用户身份信息，在控制模块的控制下，其对用户身份信息进行验证；

[0006] 所述电子钱包管理模块：在控制模块的控制下，对电子钱包的交易、余额、充值和消费等数据进行管理，并将处理结果反馈给控制模块；

[0007] 所述控制模块：将外部输入的信息送入安全管理模块，根据安全管理模块的反馈结果控制身份信息管理模块、电子钱包管理模块和存储模块进行相应操作，或不进行任何操作；

[0008] 所述安全管理模块：对外部输入的信息进行安全监控，若信息合法则允许控制模块执行相应操作，若信息不合法则禁止控制模块执行相应操作；还对安全信息进行初试化和修改设置，所述安全信息主要是指密钥信息和操作的权限信息；

[0009] 所述存储模块：在控制模块的控制下，对信息进行存储。

[0010] 进一步地，所述芯片卡还包括卡基接口；所谓卡基，是指主要由射频天线和基础电路组成的一个类似于卡片的设备，此设备不能单独工作，必须与芯片卡结合才能工作。

[0011] 所述芯片卡与所述卡基结合后的卡片频率为13.56MHz。

[0012] 再进一步地，所述芯片卡还包括数字证书模块，其由控制模块控制，用于网络银行支付的数字签名，所述网络包括有线网络和无线网络。

[0013] 又进一步地，所述芯片卡还包括支付限制模块，其由控制模块控制，在无源模式下，若支付金额或支付次数超出参数限制的范围，则所述支付限制模块将临时锁定支付功能。

[0014] 所述支付限制模块包含单笔消费限制、累计消费限制、累计消费次数限制、单日消费限制和单日消费次数限制参数。

[0015] 所述用户 SIM 卡的序列号可以存储在所述存储模块内，也可以存储在所述身份信息管理模块内。

[0016] 本发明的设计构思是：由银行发行内置有金融信息的专用芯片卡，银行对芯片卡进行初始化，然后用户将芯片卡插入特定手机中（特定手机是指能够支持此芯片卡的手机），这样用户可以很方便地实现手机的现场支付、远程支付和电子钱包功能。用户也可以将此芯片卡与其它具备标准接口的计费设备或卡基相联，或者通过手机射频天线与带天线的计费设备相联，完成支付、电子商务、电子票券等功能。芯片卡内部还可以集成用户的身份信息，用于医疗、保险、身份认证、门禁识别等功能。芯片卡还可以利用手机的无线通信功能（短信、GPRS 等），实现 OTA 充值、无线网络应用支付、下载电子票券等。

[0017] 本发明与现有技术相比具有如下优点：

[0018] (1) 现有技术主要有两大类，一类是基于手机内置 RFID 芯片技术，另外一类是基于 SIM 卡的 RFID 芯片技术，这两种技术都存在芯片上的金融信息的设置、安全、出现差错之后的纠纷无法解决的困难；因为维修的企业可能是手机厂商或者 SIM 卡商，芯片中的金融信息属于银行，但银行是没有能力完成手机和 SIM 卡的维修的。采用本方案以后，芯片卡上的信息安全出了问题，能够很好界定是 SIM 的问题、还是手机的问题，或是用户自己从其它渠道泄露的。本方案从根本上解决了上述问题，金融机构为芯片卡发卡机构，对芯片卡负责，手机厂商对手机负责、SIM 卡商对 SIM 卡负责。这样，若出了问题，则有明确的责任方负责，同时，金融机构可以独立对芯片卡进行安全管理、安全控制、初始化、信息改写等各种操作，从而确保芯片卡的信息安全。

[0019] (2) 现有技术不能解决手机与电脑支付合一的问题。现有的手机射频近距离支付技术均不能同时支持电脑支付。本发明的芯片卡支持 USB 标准接口，可以直接插在电脑上作为 USBKey(U 盘电子证书）使用，也可以通过 USB 接口直接扣电子钱包内的费用，或者进行充值、电子票券的交易（下载和使用）。

[0020] (3) 现有技术不支持物联网络支付技术。物联网是新兴的技术，目前没有统一的支付技术标准，本发明为物联网提供了多种标准的支付接口，如 USB 接口、SD 卡接口、卡基接口，可以为物联网提供符合金融标准的支付接口，未来的付费电视、水表、电表、煤气表、暖气表、加油表、停车表等等，均可以通过这样的接口完成收费。

[0021] (4) 现有技术不支持芯片与天线分离技术。现有的支付卡片基本上都是支付模块与射频天线集成在一张卡片上，不支持芯片与天线的分离。本发明的芯片卡可以插入带有射频天线的新型大卡的卡基中，共同组合成一张有支付能力、认证安全能力的非接触式射频卡。

[0022] (5) 本发明的芯片卡具备身份认证、电子钱包、电子票券、安全控件合一的功能，而

现有的手机支付技术无法解决卡的发行、多应用管理、密钥分散式管理、电子钱包的维修、芯片与天线的分离等问题。

[0023] (6) 本发明的芯片卡还可以应用于各类具有标准接口的计费设备，如水表、气表、电表、加油机等，其作为解决互联网支付的安全工具。

附图说明

[0024] 图 1 为本发明具体实施方式的多功能芯片卡框图。

具体实施方式

[0025] 以下将结合附图对本发明的实施例进行说明。

[0026] 具体实施方式中多功能芯片卡包括非接触式射频接口、USB 接口、SD 卡接口、身份信息管理模块、电子钱包管理模块、控制模块、安全管理模块和存储模块，所述芯片卡内存有用户 SIM 卡的序列号，SIM 卡的序列号可以存储在所述存储模块内，也可以存储在所述身份信息管理模块内。

[0027] 其中，SD 卡接口是所述芯片卡与手机的接口模块。非接触式射频接口采用国际标准 ISO14443 协议。非接触式射频接口实际上是芯片卡与手机终端内置射频天线的连接部分，此连接部分为基带芯片，芯片卡、基带、射频天线共同构成具有 RFID 能力的射频卡片。

[0028] 所述身份信息管理模块：内置有用户身份信息，在控制模块的控制下，其对用户身份信息进行验证；

[0029] 所述电子钱包管理模块：在控制模块的控制下，对电子钱包的交易、余额、充值和消费等数据进行管理，并将处理结果反馈给控制模块；

[0030] 所述控制模块：为芯片卡的核心处理模块；其将外部输入的信息送入安全管理模块，根据安全管理模块的反馈结果控制身份信息管理模块、电子钱包管理模块和存储模块进行相应操作，或不进行任何操作；

[0031] 所述安全管理模块：对外部输入的信息进行安全监控，若信息合法则允许控制模块执行相应操作，若信息不合法则禁止控制模块执行相应操作；还对安全信息进行初试化和修改设置，这里的安全信息，主要是指密钥信息和操作权限信息；

[0032] 所述存储模块：在控制模块的控制下，对信息进行存储。

[0033] 在实践中，芯片卡可以划分为多个应用区域，每个区域可以存储多个应用文件，如身份信息、电子钱包以及存储区域；每个应用区域是相互独立的，互相之间不能访问，存在安全访问控制。

[0034] 芯片卡的核心部分实际上是一个微型的操作系统，芯片中的应用分区管理、密钥控制以及信息的存储等都是用操作系统中的控制模块执行的，安全管理模块主要是对交易安全、通信安全、身份认证信息等进行安全管理。

[0035] 为了扩展芯片卡的功能，所述芯片卡还包括卡基接口。所谓卡基，是指主要由射频天线和基础电路组成的一个类似于卡片的设备，此设备不能单独工作，必须与芯片卡结合才能工作，结合后的卡片频率为 13.56MHz，在无源状态下工作，可以当做公交卡、银行卡、社保卡、校园卡、企业内部员工卡等使用。

[0036] 为了扩展芯片卡的功能，所述芯片卡还包括数字证书模块，数字证书模块固化在

存储硬件中，其由控制模块控制，用于网络银行支付的数字签名，增加数字证书模块是为了确保安全性，所述网络包括有线网络和无线网络。芯片卡存在银行数字证书，当用户进行网银支付时，数字证书模块保证用户密码及数据报文的加密，从而保证数据安全和交易安全。

[0037] 为了扩展芯片卡的功能，所述芯片卡还包括支付限制模块，支付限制模块固化在存储硬件中。其由控制模块控制，在无源模式下，若支付金额或支付次数超出参数限制的范围，则所述支付限制模块将临时锁定支付功能。所述支付限制模块可以包含单笔消费限制、累计消费限制、累计消费次数限制、单日消费限制和单日消费次数限制参数。

[0038] 芯片卡与手机终端结合后，在手机终端没电的情况下，芯片卡将在无源模式下进行交易，具体交易的安全性由芯片卡的支付限制模块决定，支付限制模块中存在单笔消费限制、累计消费限制、累计消费次数限制、单日消费限制、单日消费次数限制等参数，一旦支付金额或支付次数达到任何一个参数限制，则芯片卡将临时锁定支付功能，直至手机终端重新开机并成功经过安全认证，通过安全认证后，手机终端会将芯片卡中的金额或次数计数器重新清零。

[0039] 实施例一：本发明的芯片卡作为支付卡使用

[0040] 如图 1 所示，用芯片卡进行支付的过程为：

[0041] (1) 外围设备通过接口模块向芯片卡的控制模块（芯片卡的核心处理模块）发送支付请求 APDU(Application Protocol Data Unit，应用协议数据单元）指令。指令内容为：805401000F0000000120100412160000AD8FE92B。

[0042] 具体地，若外围设备为手机终端，则手机终端通过非接触式接口和 SD 卡接口向芯片卡的控制模块发送指令；若外围设备为卡基，则卡基通过非接触式接口向芯片卡的控制模块发送指令；若外围设备为 USB 设备，则 USB 设备通过 SD 卡接口或 USB 接口向芯片卡的控制模块发送指令。

[0043] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是参照中国人民银行制定的 PBOC2.0 规范中所规定的 APDU 指令，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集。

[0044] 芯片卡在进行支付交易过程中，具体的支付指令内容是由控制模块进行预检和解析的，主要包括对支付初始化、具体支付两个过程进行处理。下面分别就这两个过程进行详细的叙述。

[0045] a、支付初始化

[0046] 控制模块接收到支付初始化指令以后，首先对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持命令中提供的密钥索引号。如果不支持，则回送状态字‘9403’（不支持的密钥索引），但不回送其他数据。具体的支付初始化指令为：805001020B01000001000000000000000F。

[0047] b、支付

[0048] 控制模块在接收到具体的支付指令以后，对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，如果格式正确，则控制模块将对具体的数据进行解析，主要是对 DATA 数据域的数据进行验证，检查数据域数据是否是由 4 字节的终端交易序号 +4 字节交易日期 +3 字节交易时间 +4 字节的 MAC1 组成，对不符合的指令，安全控制模块将直

接通知芯片核心处理模块，指令错误。具体的支付指令为：805401000F00000001201005061 61010E193F23A08。

[0049] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否拥有操作电子钱包管理模块的权限，并将判断结果反馈至控制模块；若指令拥有操作电子钱包管理模块的权限，则反馈结果为“是”，若指令不拥有操作电子钱包管理模块的权限，则反馈结果为“否”。

[0050] 安全管理模块检查控制模块发来的指令是否拥有操作电子钱包的权限信息。是否符合对电子钱包模块进行只读信息、只可添加的信息、只可更新的信息、无法读取的信息四个方面的限制；同时，对于大额支付，安全管理模块将限制支付请求，需要用户提供 PIN(Personal Identification Number，个人识别码缩写）认证，PIN 码是 4 到 8 位的数字，只有输入的数字通过认证，才允许对卡进行操作，如果输入的数字认证错误 3 次，则卡片将被锁定；安全管理模块验证支付指令满足必须的权限限制后，控制模块才可以对电子钱包进行支付操作。否则，安全管理模块将提示权限不足的错误信息。

[0051] (4) 控制模块根据安全管理模块的反馈结果，决定是否向电子钱包管理模块发送支付请求。

[0052] (5) 若反馈结果为“是”，则控制模块向电子钱包管理模块发送支付请求，电子钱包管理模块根据控制模块送来的指令进行支付处理，并将处理结果以指令流的方式返回给控制模块。

[0053] (6) 若反馈结果为“否”，则控制模块不向电子钱包管理模块发送支付请求。

[0054] (7) 控制模块将支付结果通过非接触式射频接口返回给外围设备，支付流程结束。

[0055] 此处的非接触式射频接口实际上是芯片和外围设备之间通过电磁波感应以电磁波方式传输的。

[0056] 实施例二：对本发明的芯片卡进行充值

[0057] 如图 1 所示，用芯片卡进行充值的过程为：

[0058] (1) 外围设备通过接口模块向芯片卡的控制模块（芯片卡的核心处理模块）发送充值请求 APDU(Application Protocol Data Unit，应用协议数据单元）指令。指令内容为：805200000B20100412160000AD8FE92B04。

[0059] 具体地，若外围设备为手机终端，则手机终端通过非接触式接口和 SD 卡接口向芯片卡的控制模块发送指令；若外围设备为卡基，则卡基通过非接触式接口向芯片卡的控制模块发送指令；若外围设备为 USB 设备，则 USB 设备通过 SD 卡接口或 USB 接口向芯片卡的控制模块发送指令。

[0060] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是参照中国人民银行制定的 PBOC2.0 规范中所规定的 APDU 指令，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集。

[0061] 芯片卡在进行充值交易过程中，具体的充值指令内容是由控制模块进行预检和解析的，主要包括对充值初始化、具体充值两个过程进行处理。下面分别就这两个过程进行详细的叙述。

[0062] a、充值初始化

[0063] 控制模块接收到充值初始化指令以后，首先对 APDU 指令进行预检，查看是否符合

CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持命令中提供的密钥索引号。如果不支持，则回送状态字‘9403’（不支持的密钥索引），但不回送其他数据。具体的支付初始化指令为：805000020B01000000100000000000010。

[0064] b、充值

[0065] 控制模块在接收到具体的充值指令以后，对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，如果格式正确，则控制模块将对具体的数据进行解析，主要是对 DATA 数据域的数据进行验证，检查数据域数据是否是由 4 字节的终端交易序号 +4 字节交易日期 +3 字节交易时间 +4 字节的 MAC2 组成，对不符合的指令，安全控制模块将直接通知芯片核心处理模块，指令错误。具体的支付指令为：805200000B20100506161010F901E2AC04。

[0066] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否拥有操作电子钱包管理模块的权限，并将判断结果反馈至控制模块；若指令拥有操作电子钱包管理模块的权限，则反馈结果为“是”，若指令不拥有操作电子钱包管理模块的权限，则反馈结果为“否”。

[0067] 安全管理模块检查控制模块发来的指令是否拥有操作电子钱包的权限信息。是否符合对电子钱包模块进行只读信息、只可添加的信息、只可更新的信息、无法读取的信息四个方面的限制；安全管理模块验证支付指令满足必须的权限限制后，控制模块才可以对电子钱包进行充值操作。否则，安全管理模块将提示权限不足的错误信息。

[0068] (4) 控制模块根据安全管理模块的反馈结果，决定是否向电子钱包管理模块发送充值请求；

[0069] (5) 若反馈结果为“是”，则控制模块向电子钱包管理模块发送充值请求，电子钱包管理模块根据控制模块送来的指令进行充值处理，并将处理结果以指令流的方式返回给控制模块；

[0070] (6) 若反馈结果为“否”，则控制模块不向电子钱包管理模块发送充值请求；

[0071] (7) 控制模块将充值结果通过非接触式射频接口返回给外围设备，充值流程结束。

[0072] 实施例三：本发明的芯片卡作为身份卡使用

[0073] 如图 1 所示，身份信息的获取过程为：

[0074] (1) 外围设备通过接口模块向芯片卡的控制模块（芯片卡的核心处理模块）发送充值请求 APDU(Application Protocol Data Unit，应用协议数据单元）指令。指令内容为：00B0C001000000。

[0075] 具体地，若外围设备为手机终端，则手机终端通过非接触式接口和 SD 卡接口向芯片卡的控制模块发送指令；若外围设备为卡基，则卡基通过非接触式接口向芯片卡的控制模块发送指令；若外围设备为 USB 设备，则 USB 设备通过 SD 卡接口或 USB 接口向芯片卡的控制模块发送指令。

[0076] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是参照中国人民银行制定的 PBOC2.0 规范中所规定的 APDU 指令，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集；

[0077] 芯片卡在进行信息获取过程当中，具体的信息获取指令内容是由控制模块进行预

检和解析的，控制模块接收到信息获取指令以后，首先对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持命令中提供的文件数据块控制参数。如果支持，则允许访问指定的文件数据块，否则返回错误提示信息。具体的信息获取指令为 :00B0C001000000。

[0078] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否拥有操作身份信息管理模块的权限，并将判断结果反馈至控制模块 ;若指令拥有操作身份信息管理模块的权限，则反馈结果为“是”，若指令不拥有操作身份信息管理模块的权限，则反馈结果为“否”。

[0079] 安全管理模块检查控制模块发送的指令是否拥有操作身份信息模块的权限信息，从限制芯片卡用户的范围方面，主要包括卡体本身的保护，如公共信息的获取等 ;从限制读取智能卡信息的方式上，可以分为只读信息、只可添加的信息、只可更新的信息、无法读取的信息等四个方面。安全管理模块判断指令是否满足上述的权限限制，如果满足，则对身份信息模块进行所在范围的信息获取操作，否则，安全管理模块将返回权限不足的错误提示信息。

[0080] (4) 控制模块根据安全管理模块的反馈结果，决定是否向身份信息管理模块发送信息获取请求 ;

[0081] (5) 若反馈结果为“是”，则控制模块向身份信息管理模块发送信息获取请求，身份信息管理模块根据控制模块送来的指令进行信息获取处理，并将处理结果以指令流的方式返回给控制模块 ;

[0082] (6) 若反馈结果为“否”，则控制模块不向身份信息管理模块发送信息获取请求 ;

[0083] (7) 控制模块将信息获取结果通过非接触式射频接口返回给外围设备，充值流程结束。

[0084] 身份信息的更改流程为 :

[0085] (1) 外围设备通过接口模块向芯片卡的控制模块 (芯片卡的核心处理模块) 发送充值请求 APDU(Application Protocol Data Unit，应用协议数据单元) 指令。指令内容为 :

[0086] 04D6C0010A 身份证 AD8FE92B00

[0087] 具体地，若外围设备为手机终端，则手机终端通过非接触式接口和 SD 卡接口向芯片卡的控制模块发送指令 ;若外围设备为卡基，则卡基通过非接触式接口向芯片卡的控制模块发送指令 ;若外围设备为 USB 设备，则 USB 设备通过 SD 卡接口或 USB 接口向芯片卡的控制模块发送指令。

[0088] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是参照中国人民银行制定的 PBOC2.0 规范中所规定的 APDU 指令，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集 ;

[0089] 芯片卡在进行信息更改过程当中，具体的信息更改指令内容是由控制模块进行预检和解析的，控制模块接收到信息更改指令以后，首先对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持命令

中提供的文件数据块控制参数。如果支持，则允许访问指定的文件数据块，否则返回错误提示信息。具体的信息更改指令为 :04D6C0010A123456789012A0B1C2D300。

[0090] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否拥有操作身份信息管理模块的权限，并将判断结果反馈至控制模块 ;若指令拥有操作身份信息管理模块的权限，则反馈结果为“是”，若指令不拥有操作身份信息管理模块的权限，则反馈结果为“否”。

[0091] 安全管理模块检查控制模块发送的指令是否拥有更新身份信息模块的权限信息，首先验证是否已经通过 PIN 验证，PIN 验证主要是指用户输入 4 到 8 位的数字，只有输入的数字通过认证，才允许对卡进行操作，如果输入的数字认证错误 3 次，则卡片将被锁定 ;其次是验证是否通过发卡行认证，主要是指卡片必须通过 16-32 位的密码认证，即外部认证之后，才可以对身份信息模块进行更改 ;最后从限制读取智能卡信息的方式上，验证是否符合满足只读信息、只可添加的信息、只可更新的信息、无法读取的信息等四个方面限制。安全管理模块判断指令是否满足上述的权限限制，如果满足，则对身份信息模块进行所在范围的更改操作，否则，安全管理模块将返回权限不足的错误提示信息。

[0092] (4) 控制模块根据安全管理模块的反馈结果，决定是否向身份信息管理模块发送信息更改请求 ;

[0093] (5) 若反馈结果为“是”，则控制模块向身份信息管理模块发送信息更改请求，身份信息管理模块根据控制模块送来的指令进行信息更改处理，并将处理结果以指令流的方式返回给控制模块 ;

[0094] (6) 若反馈结果为“否”，则控制模块不向身份信息管理模块发送信息更改请求 ;

[0095] (7) 控制模块将信息更新结果通过非接触式射频接口返回给外围设备，充值流程结束。

[0096] 实施例四 :本发明的芯片卡作为 U 盘使用

[0097] 如图 1 所示，芯片卡作为 U 盘存储使用的过程为 :

[0098] (1) 外围设备 (如 USB 设备) 通过 USB 接口向芯片卡的控制模块 (芯片卡的核心处理模块) 发送信息存储应用请求 APDU 指令，指令内容为 :00B00000010000。

[0099] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是验证 USB 操作指令是否符合 APDU 指令格式，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集 ;

[0100] 集成了芯片卡的 USB 设备在插入计算机等外围设备以后，芯片卡内部的控制模块在受到外围 USB 接口的请求，将主动向控制模块发送一条指令，指令内容为 00B00000010000，此指令是请求外部设备是否可以访问存储模块 ;控制模块接收到指令以后，首先对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持此命令，同时检查存储管理模块是否允许访问。如果支持，则允许访问指定的存储文件，否则返回错误提示信息。

[0101] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否拥有操作存储模块的权限，并将判断结果反馈至控制模块 ;若指令拥有存储模块的权限，则反馈结果为“是”，若指令不拥有操作存储模块的权限，则反馈结果为“否”。

[0102] 安全管理模块检查控制模块发来的指令是否拥有操作存储模块的权限信息。是否符合对存储模块进行只读信息、只可添加的信息、只可更新的信息、无法读取的信息四个方面的限制；安全管理模块判断指令是否满足上述的权限限制，如果满足，则对存储模块进行所在范围的操作，否则，安全管理模块将返回权限不足的错误提示信息。

[0103] (4) 控制模块再将反馈结果通过 USB 接口返回给外围设备，外围设备根据反馈结果判定是否可以访问芯片卡的存储区域；

[0104] (5) 若反馈结果为“是”，则控制模块向存储模块发送读写请求，存储模块根据控制模块送来的指令进行读写处理；

[0105] (6) 若反馈结果为“否”，则控制模块不向存储模块发送读写请求；

[0106] (7) 控制模块将读写结果通过 USB 接口返回给外围设备，访问流程结束。

[0107] 实施例五：本发明的芯片卡作为网银认证使用

[0108] 如图 1 所示，芯片卡作为网银认证使用的过程为：

[0109] (1) 外围设备（如 USB 设备）通过 USB 接口向芯片卡的控制模块（芯片卡的核心处理模块）发送信息数据签名的应用请求 APDU 指令，指令内容为：00D00000010000。

[0110] (2) 控制模块对指令内容进行解析，判断指令是否规范，并将解析后的指令送给安全管理模块。解析方式主要是验证 USB 操作指令是否符合 APDU 指令格式，控制模块分析指令是否合法，同时是否属于芯片中 COS 已存在的指令集；

[0111] 集成了芯片卡的 USB 设备在插入计算机等外围设备以后，计算机中的外围软件通过接口模块向芯片卡的控制模块发送信息数据签名的请求 APDU 指令，指令通过核心处理模块先到控制模块进行预处理和解析，具体的指令内容为 00D00000010000，此指令是对外围数据内容通过指定银行证书进行数据签名，控制模块接收到指令以后，首先对 APDU 指令进行预检，查看是否符合 CLA、INS、P1、P2、LC、DATA、LE 格式，对不符合的指令将直接提示指令格式错误。指令格式预检正确之后，将对指令内容进行解析并检查，主要检查的是控制模块中是否支持此命令，同时检查指定的银行证书索引是否存在。如果存在，则允许访问指定的银行证书，否则返回错误提示信息。

[0112] (3) 安全管理模块对控制模块送来的指令进行验证，判断指令是否可以使用指定的银行证书，并是否拥有操作权限，并将判断结果反馈至控制模块；若指令拥有存储模块的权限，则反馈结果为“是”，若指令不拥有操作存储模块的权限，则反馈结果为“否”。

[0113] 安全管理模块检查控制模块发来的指令是否拥有操作指定银行证书的权限信息。是否符合对存储模块进行只读信息、只可添加的信息、只可更新的信息、无法读取的信息四个方面的限制；安全管理模块判断指令是否满足上述的权限限制，如果满足，则对银行证书进行所在范围的操作，否则，安全管理模块将返回权限不足的错误提示信息。

[0114] (4) 控制模块根据安全管理模块的反馈结果，将数据用指定的金融证书进行签名并将签名数据通过 USB 接口返回给外围设备；

[0115] (5) 获取数据签名流程结束。

[0116] 本发明说明书中未作详细描述的内容属于本领域专业技术人员公知技术。

[0117] 上述实施例用来解释说明本发明，而不是对本发明进行限制，在本发明的精神和权利要求的保护范围内，对本发明作出的任何修改和改变，都落入本发明的保护范围。

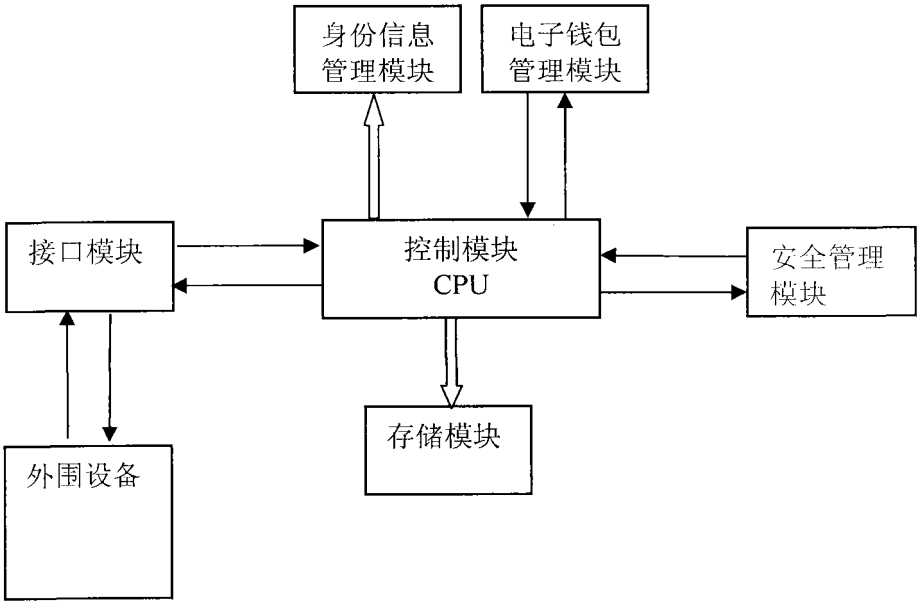


图 1