[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06K 19/07 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910077144.6

[43] 公开日 2009 年 7 月 8 日

[11] 公开号 CN 101477607A

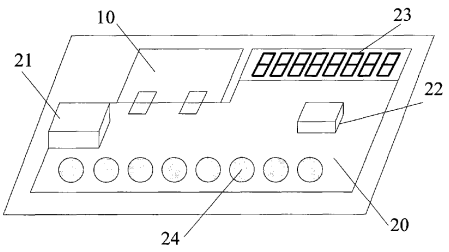
[22] 申请日 2009.1.16
[21] 申请号 200910077144.6
[71] 申请人 北京海升天达科技有限公司
地址 100102 北京市朝阳区望京西路 48 号金隅国际 C 座 2205 室
[72] 发明人 王科宇 谢涛令 张 徵
[74] 专利代理机构 北京市浩天知识产权代理事务所
代理人 许志勇 洪 缨
权利要求书 3 页 说明书 9 页 附图 4 页

[54] 发明名称

智能卡及其智能卡用户身份认证方法

[57] 摘要

本发明公开了一种智能卡及其智能卡用户身份认证的方法。 智能卡包括卡基和封装在卡基中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和柔性电池。 当柔性输入模块的按键较多、功能复杂，智能卡还包括封装在卡基中的输入驱动模块。 本发明的智能卡实现了片上读卡器的功能，使得不需要额外的读卡设备即可以读取智能卡上的信息，而且采用本发明的智能卡进行 CNP 环境下的智能卡用户身份认证时，不需要额外的读卡设备来产生用于认证时需要的认证信息，例如一次性的动态密码，智能卡本身可以根据需要生成用于实现 CNP 环境下的身份认证所需的认证信息。 此外，本发明还在传统智能卡上扩展新的应用，例如智能卡信息查询或者数字签名，提供了可能。



1、一种智能卡，包括卡基和封装在所述卡基中的智能卡芯片，其特征在于，还包括:

柔性显示模块，封装在所述卡基中，用于显示信息;

显示驱动模块，封装在所述卡基中，与所述柔性显示模块和智能卡芯片连接，用于驱动柔性显示模块;

柔性输入模块，封装在所述卡基中，与所述显示驱动模块或智能卡芯片连接，用于向所述智能卡输入信息;

柔性电池模块，封装在所述卡基中，用于向所述智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块提供电源。

2、如权利要求 1 所述的智能卡，其特征在于，所述显示驱动模块采用具有驱动所述柔性显示模块功能的微处理器芯片。

3、如权利要求 1 所述的智能卡，其特征在于，所述显示驱动模块集成在所述智能卡芯片中。

4、如权利要求 1 或 2 或 3 所述的智能卡，其特征在于，所述智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块安装在柔性电路板上，柔性电路板封装在所述卡基中。

5、如权利要求 1 所述的智能卡，其特征在于，所述柔性显示模块是柔性 LCD、柔性 LED、柔性 OLED 或者柔性双稳态显示装置。

6、如权利要求 1 所述的智能卡，其特征在于，所述柔性输入模块是柔性键盘或者柔性手写输入装置。

7、一种智能卡，包括卡基和封装在所述卡基中的智能卡芯片，其特征在于，还包括:

柔性显示模块，封装在所述卡基中，用于显示信息;

显示驱动模块，封装在所述卡基中，与所述柔性显示模块和智能卡芯片连接，用于驱动柔性显示模块;

柔性输入模块，封装在所述卡基中，用于向所述智能卡输入信息;

输入驱动模块，封装在所述卡基中，与所述柔性输入模块以及所述智能卡芯片或者显示驱动模块连接，用于驱动柔性输入模块;

柔性电池模块，封装在所述卡基中，用于向所述智能卡芯片、柔性显示

模块、显示驱动模块、柔性输入模块和输入驱动模块提供电源。

8、如权利要求 7 所述的智能卡，其特征在于，所述显示驱动模块和/或输入驱动模块采用具有驱动所述柔性显示模块和/或柔性输入模块功能的微处理器芯片。

9、如权利要求 7 所述的智能卡，其特征在于，所述显示驱动模块和/输入驱动模块集成在所述智能卡芯片中。

10、如权利要求 7 或 8 或 9 所述的智能卡，其特征在于，所述智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和输入驱动模块安装在柔性电路板上，柔性电路板封装在所述卡基中。

11、如权利要求 7 所述的智能卡，其特征在于，所述柔性显示模块是柔性 LCD、柔性 LED、柔性 OLED 或者柔性双稳态显示装置。

12、如权利要求 7 所述的智能卡，其特征在于，所述柔性输入模块是柔性键盘或者柔性手写输入装置。

13、一种智能卡用户身份认证的方法，其特征在于，包括步骤:

1）通过所述智能卡的柔性输入模块启动所述智能卡芯片生成用户身份认证信息，并通过柔性显示模块显示;

2）把用户信息和所述用户身份认证信息输入到网络环境中的用户身份认证平台;

3）网络环境中的用户身份认证服务器进行用户身份认证，并把认证成功或失败的结果反馈给所述用户身份认证平台。

14、如权利要求 13 所述的方法，其特征在于，步骤 1)之前还包括步骤:通过柔性输入模块输入个人识别信息，若所述个人识别信息与所述智能卡内存储的识别信息一致，则继续；否则，退出。

15、如权利要求 13 或 14 所述的方法，其特征在于，步骤 1）中是根据所述智能卡芯片中存储的信息生成所述用户身份认证信息。

16、如权利要求 13 或 14 所述的方法，其特征在于，步骤 1)在生成所述用户身份认证信息之前还包括步骤: 通过柔性输入模块输入信息; 步骤 1）中是根据所述输入信息和智能卡芯片中存储的信息生成所述用户身份认证信息。

17、如权利要求 13 所述的方法，其特征在于，所述用户身份认证信息是一次性动态密码或者数字签名。

智能卡及其智能卡用户身份认证方法

技术领域

本发明涉及智能卡领域，尤其涉及一种带显示和输入装置的智能卡及其智能卡用户身份认证方法。

背景技术

EMV 标准是由国际三大银行卡组织-Europay、MasterCard 和 Visa 共同发起制定的银行卡从磁条卡向智能（集成电路）卡转移的技术标准，是基于智能卡的金融支付标准，已成为公认的全球统一标准。目前，中国也颁布了“中国金融集成电路（IC）卡规范”2.0 版（简称 PBOC 2.0 版），与国际 EMV2000 智能卡标准兼容。智能卡又称 IC（集成电路）卡，指在其中封装了集成电路芯片的卡片。智能卡具有存储容量大、数据安全性高、防伪性好、应用设备成本低、技术成熟等特点。

随着互联网应用广泛深入到社会的方方面面，越来越多的企业和个人在互联网上从事各种业务和交易活动，这些电子业务的开展有赖于安全的用户身份认证。此外，随着网络交易及在线银行的不断推广使用，越来越多的金融交易发生在银行交易柜台以外的环境下，即 CNP（Card-Not-Present，卡不在场）的金融交易环境下，而此时对于交易用户身份的认证，将比在柜台交易时更复杂。目前的认证方法有：

固定的用户名和密码，这种方法的安全性较差。

通过智能卡读卡器连接电脑，插入用户智能卡进行认证，但需要单独的读卡器，且无法在 CNP 环境下使用。

使用对应用户身份的 USB Key，插入电脑 USB 接口，进行认证，但无法在 CNP 环境下使用，且需要单独的硬件设备。

使用单独的 OTP（One-Time password，一次性密码）硬件，以产生

一次性密码用于认证，但需要单独的 OTP 硬件设备，无法结合用户已有的智能卡。

使用手持式的智能卡读卡器，插入用户身份/账户智能卡，通过智能卡芯片产生一次性 OTP 密码，用于 CNP 环境下的身份认证，同时通过读卡器的键盘输入交易信息，可对电子交易进行数字签名。这种方式需要使用智能卡和单独的智能卡读卡器，成本较高，用户携带不方便。

对于符合 EMV2000 的智能卡，其本身采用具有很高安全等级（经过特殊安全保护设计）的半导体智能芯片来存储用户的个人信息，然后将该芯片通过压接工艺嵌入到由诸如 PVC（Polyvinylchlorid，聚氯乙烯）材料所构成的塑料卡基材中。在此基础上，智能卡芯片内部采用高安全性的操作系统来管理所有用户存储信息，同时也依赖此操作系统来有效管理智能芯片对外的信息交互接口。当前，针对 EMV2000 的智能卡都需要在专用的金融读写工具的配合下，才能实现对智能卡芯片内信息的读取和生成用于认证的 OTP。而独立的金融读写工具本身的设计制造会涉及到很多部门及行业的标准，从而增加了产品的系统成本。此外，要实现金融读写工具无处不在，随时可以使用，这一点本身难以实现。市场上有部分公司采用了挂在钥匙扣上的便携型的读卡工具，以实现诸如 EMV 的 CAP（Chip Authentication Program）和 DPA(Dynamic Passcode Authentication)的基于智能卡存储信息的 CNP 环境下的身份认证方法。在这样的解决方案中，各公司设计了形状各异的读卡设备，在满足智能卡读写的同时，需要为读卡器留有足够的空间以放置键盘，键盘用以输入诸如 PIN（personal identification number，个人识别码）等用户所知道的信息。然而读卡器本身的尺寸是独立读卡器解决方案的关键之一。设计尺寸太大将影响携带的方便性。如果尺寸太小，会导致键盘区域较为拥挤，导致按键误触发。

CNP 环境下，目前符合 EMV2000/PBOC2.0 标准的金融智能卡使用的用户身份认证方法是：

有交易需求的用户将个人智能卡插入到信用卡发行商所提供的读卡器中，并按照提示，键入用户 PIN 码，读卡器显示由智能卡生成的用户身份认证信息，比如：一次性密码；

将用户信息和智能卡产生的用户身份认证信息输入到网络交易平台中的用户身份认证平台；

通过网络连接的身份认证服务器根据用用户信息和户身份认证信息进行用户身份认证，并将认证成功或失败的结果反馈给用户身份认证平台。

发明内容

针对现有技术中的智能卡和智能卡读卡器分离，需要采用单独的读卡器来显示智能卡内的信息以及生成用户身份认证的信息，本发明提供了一种智能卡，在智能卡上实现片上读卡器的功能，从而使智能卡用户的应用和携带更为方便。

一方面，为了解决上述技术问题，本发明提供了一种智能卡，包括卡基和封装在所述卡基中的智能卡芯片，还包括:

柔性显示模块，封装在所述卡基中，用于显示信息；

显示驱动模块，封装在所述卡基中，与所述柔性显示模块和智能卡芯片连接，用于驱动柔性显示模块；

柔性输入模块，封装在所述卡基中，与所述显示驱动模块或智能卡芯片连接，用于向所述智能卡输入信息；

柔性电池模块，封装在所述卡基中，用于向所述智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块提供电源。

优选地，如上所述的智能卡中的显示驱动模块采用具有驱动所述柔性显示模块功能的微处理器芯片。

为了解决上述技术问题，本发明还提供了一种智能卡，包括卡基和封装在所述卡基中的智能卡芯片，还包括:

柔性显示模块，封装在所述卡基中，用于显示信息；

显示驱动模块，封装在所述卡基中，与所述柔性显示模块和智能卡芯片连接，用于驱动柔性显示模块；

柔性输入模块，封装在所述卡基中，用于向所述智能卡输入信息；

输入驱动模块，封装在所述卡基中，与所述柔性输入模块以及所述智能卡芯片或者显示驱动模块连接，用于驱动柔性输入模块。

柔性电池模块，封装在所述卡基中，用于向所述智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和输入驱动模块提供电源。

优选地，如上所述的智能卡中的显示驱动模块和/或输入驱动模块采用具有驱动所述柔性显示模块和/或柔性输入模块功能的微处理器芯片。

另一方面，本发明还提供了一种智能卡用户身份认证的方法，包括步骤：

1）通过所述智能卡的柔性输入模块启动所述智能卡芯片生成用户身份认证信息，并通过柔性显示模块显示；

2）把用户信息和所述用户身份认证信息输入到网络环境中的用户身份认证平台；

3）网络环境中的用户身份认证服务器进行用户身份认证，并把认证成功或失败的结果反馈给所述用户身份认证平台。

本发明提供了一种智能卡，实现了片上读卡器的功能，使得不需要额外的读卡设备即可以读取智能卡上的信息。采用本发明的智能卡进行 CNP 环境下的智能卡用户身份认证时，不需要额外的读卡设备来产生用于认证时需要的认证信息，智能卡本身可以根据需要生成用于实现 CNP 环境下的身份认证所需的认证信息，例如一次性的动态密码。本发明的智能卡使得用户的携带性和易用性得到保障，并可降低产品成本。目前世界上银行卡和信用卡正在向芯片卡转换，利用智能卡芯片实现 CNP 环境下的用户身份认证也成为发展的趋势，本发明可以实现 Visa 和 Mastercard 制定的 CAP/DPA 标准的功能要求，同时为在传统智能卡上扩展新的应用，例如智能卡信息查询或者数字签名，提供了可能。

附图说明

图 1 是本发明一实施例的智能卡的基本结构框图；

图 2 是本发明另一实施例的智能卡的基本结构框图；

图 3 是本发明又一实施例的智能卡的基本结构框图；

图 4 是本发明还一实施例的智能卡的基本结构框图；

图 5 是本发明一实施例的智能卡结构的示意图；

图 6 是本发明另一实施例的智能卡结构的示意图；

图 7 是本发明一实施例的智能卡用户身份认证方法的流程图。

具体实施方式

下面结合附图及具体实施方式对本发明技术方案做进一步的详细描述。

如图 1 和图 2 所示，智能卡包括卡基和封装在卡基中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和柔性电池。当柔性输入模块的输入按键较少、功能简单时，柔性输入模块不需要输入驱动。智能卡芯片是智能卡的核心，其上运行芯片内操作系统（COS，Chip Operating System），完成运算、存储和控制等功能；柔性输入模块用于和用户交互，输入相应信息；显示驱动模块用于驱动柔性显示模块；柔性显示模块用于和用户交互，显示用户输入的信息和智能卡输出的信息；柔性电池向智能卡中的智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块提供电源。

如图 1 所示，在本发明的一实施例中，显示驱动模块与智能卡芯片和柔性显示模块连接；柔性输入模块与显示驱动模块连接，通过显示驱动模块与智能卡芯片通信；柔性电池直接与智能卡中的智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块连接，用于向智能卡中的芯片和模块提供电源。柔性电池也可以不直接与柔性输入模块和/或柔性显示模块连接，而是通过与柔性输入模块和柔性显示模块连接的显示驱动模块向柔性输入模块和/或柔性显示模块提供电源。

如图 2 所示，在本发明的另一实施例中，显示驱动模块与智能卡芯片和柔性显示模块连接；柔性输入模块和智能卡芯片连接，把柔性输入模块输入的信息送到智能卡芯片，还通过智能卡芯片把需要显示的输入信息送到显示驱动模块，并在柔性显示模块上显示；柔性电池直接与智能卡中的智能卡芯片、柔性显示模块、显示驱动模块和柔性输入模块连接，用于向智能卡中的芯片和模块提供电源。柔性电池也可以不直接与柔性显示模块连接，而是通过与柔性显示模块连接的显示驱动模块向柔性显示模块提供电源；柔性电池还可以不直接与柔性输入模块连接，而是通过与柔性输入模块连接的智能卡芯片向柔性输入模块提供电源。

如图 3 和图 4 所示，智能卡包括卡基和封装在卡基中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块、输入驱动模块和柔性电池。当柔性输入模块输入按键较多、功能复杂时，柔性输入模块需要输入驱动。智能卡芯片是智能卡的核心，其上运行芯片内操作系统（COS，Chip Operating System），完成运算、存储和控制等功能；输入驱动模块用于驱动柔性输入模块；柔性输入模块用于和用户交互，输入相应信息；显示驱动模块用于驱动柔性显示模块；柔性显示模块用于和用户交互，显示用户输入的信息和智能卡输出的信息；柔性电池向智能卡中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和输入驱动模块提供电源。

如图 3 所示，在本发明的又一实施例中，显示驱动模块与智能卡芯片和柔性显示模块连接；输入驱动模块与柔性输入模块和显示驱动模块连接，输入驱动模块通过显示驱动模块与智能卡芯片通信；柔性电池直接与智能卡中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和输入驱动模块连接，用于向智能卡中的芯片和模块提供电源。柔性电池也可以不直接与柔性输入模块连接，而是通过与柔性输入模块连接的输入驱动模块向柔性输入模块提供电源；柔性电池还可以不直接与柔性显示模块连接，而是通过与柔性显示模块连接的显示驱动模块向柔性显示模块提供电源。

如图 4 所示，在本发明的还一实施例中，显示驱动模块与智能卡芯片和柔性显示模块连接；输入驱动模块与柔性输入模块和智能卡芯片连接，柔性输入模块通过输入驱动模块把柔性输入模块输入的信息送到智能卡芯片，还通过智能卡芯片把需要显示的输入信息送到显示驱动模块，并在柔性显示模块上显示；柔性电池直接与智能卡中的智能卡芯片、柔性显示模块、显示驱动模块、柔性输入模块和输入驱动模块连接，用于向智能卡中的芯片和模块提供电源。柔性电池也可以不直接与柔性输入模块连接，而是通过与柔性输入模块连接的输入驱动模块向柔性输入模块提供电源；柔性电池还可以不直接与柔性显示模块连接，而是通过与柔性显示模块连接的显示驱动模块向柔性显示模块提供电源。

图 5 是本发明一实施例的智能卡结构的示意图，包括柔性电池 10、智能卡芯片 21、显示驱动模块 22、柔性显示模块 23 和柔性输入模块 24，其

中，智能卡芯片 21、显示驱动模块 22、柔性显示模块 23 和柔性输入模块 24 安装在柔性电路板 20 上，柔性电路板 20 和智能卡芯片 21 都封装在卡基中。由于柔性输入模块 24 的按键较少、功能简单，因此不需要输入驱动。显示驱动模块 22 采用单独的显示驱动芯片。智能卡芯片 21 除符合 ISO7816/7810 和 EMV2000 标准的 8 个引脚外，具有单独的输入输出接口和显示驱动芯片连接，并通过此连接完成数据和指令的交换。智能卡芯片 21 的符合 ISO7816/7810 或 EMV2000 标准的 8 个引脚连接到外露在卡基表面的接触铜片上，用于实现和符合 ISO7816/7810 标准的读卡器之间的接触连接。将满足 CNP（卡不存在，即智能卡不和电脑直接连接）等具体认证方案，如 CAP/DPA（Chip Authentication Program/ Dynamic Passcode Authentication），的软件实现集成到智能卡芯片的操作系统（COS）中，智能卡芯片负责将计算所得的结果传递到显示器驱动芯片中，由该芯片负责显示内容的缓存及显示控制。

在本发明的一个实施例中，显示器驱动芯片采用具有显示驱动功能的微处理器芯片，例如 Elan 或 Holtek 的微处理器芯片。微处理器芯片本身具有独立的运算能力，加上柔性显示模块和柔性输入模块，在脱离智能卡芯片，即不需要智能卡芯片参与的情况下，可以实现一些功能和应用，例如：独立地生成本智能卡或第三方身份认证应用所需要的一次性动态密码（OTP）。而 OTP 应用本身是用户在 CNP 环境下（CNP，卡不在场，即智能卡不和计算机直接连接）应用非常广泛的身份认证方式之一。此外，可以将每次使用智能卡芯片的相关信息，比如：交易的金额、账户余额、账号积分等存储在微处理器芯片中，用户可以随时进行查询，而不必用到智能卡芯片，也无需外插读卡器终端。一般情况下，智能卡芯片的功耗远大于微处理器芯片，因此在这种应用中可以有效降低智能卡的功耗。在本发明的又一实施例中，当智能卡的柔性输入模块的按键较多、功能复杂而需要输入驱动时，输入驱动模块也可以采用微处理器芯片，并且显示驱动模块和输入驱动模块可采用一块微处理器芯片，也即是用一块微处理器芯片同时实现显示驱动模块和输入驱动模块的功能。

图 6 是本发明另一实施例的智能卡结构的示意图，其中显示驱动模块集

成到智能卡芯片 21′中，使得智能卡芯片除具备传统智能卡芯片的功能外，还具备显示装置的驱动功能和接口，而芯片本身在安全、防防范外部干扰、侵扰方面仍然遵循和符合 ISO7816/7810 或 EMV2000 的标准，将满足 CNP 等具体认证方案，如 CAP/DPA（Chip Authentication Program/ Dynamic Passcode Authentication），的软件实现集成到智能卡芯片的操作系统（COS）中。集成了显示驱动模块的智能卡芯片除负责传统智能卡的有关计算和管理外，还负责显示的驱动和管理。在本发明的又一实施例中，当智能卡的柔性输入模块的按键较多、功能复杂而需要输入驱动时，可以把输入驱动模块也集成到智能卡芯片 21′中，使得智能卡芯片除具备传统智能卡芯片的功能外，还具备显示装置的驱动功能和接口以及输入装置的驱动功能和接口，从而除负责传统智能卡的有关计算和管理外，还负责显示的驱动和管理以及输入的驱动和管理。

本发明中的柔性显示模块采用柔性液晶显示装置（LCD，Liquid Crystal Display），其中也包括：环氧树脂系高分子分散液晶膜（PDLC）显示装置，或者可以采用柔性发光二极管（LED。Light Emitting Diode）以及柔性有机发光二极管（OLED，Organic Light Emitting Diode）显示装置，本发明或者还可以采用双稳态（bi-stable）柔性显示装置，例如：电子墨水（E-ink）显示装置，电泳显示装置（EPD，electro phoretic display）。

本发明中的柔性输入模块采用柔性键盘或者柔性手写输入装置。

本发明实施例的智能卡的卡体符合 ISO7816/7810 或 EMV2000 标准的要求，用于取代传统的银行卡/信用卡。但是本发明不限于 ISO7816/7810 或 EMV2000 的要求，其他的卡体形式也在本发明的保护范围之内。

如图 7 所示，采用本发明的智能卡，比如用于银行金融领域，用户进行 CNP 环境下交易时的身份认证方法的具体实施方式是：

1）有交易需求的用户利用智能卡上的键盘输入 PIN（personal identification number，个人识别码），如用户输入的 PIN 码与智能卡中存储的 PIN 码一致，则继续，否则，退出；

2）成功进入智能卡系统后，可以通过键盘和显示器，选择所需采用的功能，例如产生身份认证所需要的一次性动态密码或者数字签名，智能卡根

据智能卡内存储的信息，例如同步计数器的数值和用户的 OTP 密钥，生成一次性动态密码，或者根据智能卡内存储的信息，例如用户私钥和用户输入的信息，例如交易信息，生成数字签名；

3）把用户信息和智能卡产生的一次性动态密码或者数字签名输入到用户网络电子交易平台的用户身份认证平台；

4）网络中的身份认证服务器根据用户提交信息进行身份认证，并将认证成功或失败信息反馈给用户身份认证平台。

需要说明的是，以上所述仅为本发明较佳的具体实施例，而不是对本发明技术方案的限定，任何熟悉该技术的本领域普通技术人员在本发明所提示的技术范围内，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。

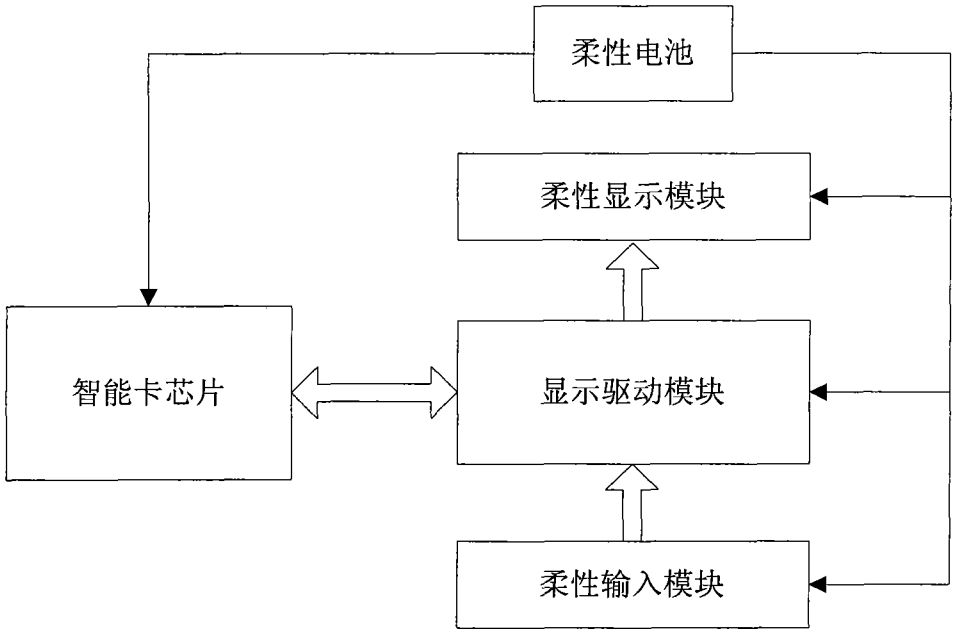

柔性电池
柔性显示模块
智能卡芯片
显示驱动模块
柔性输入模块

图 1

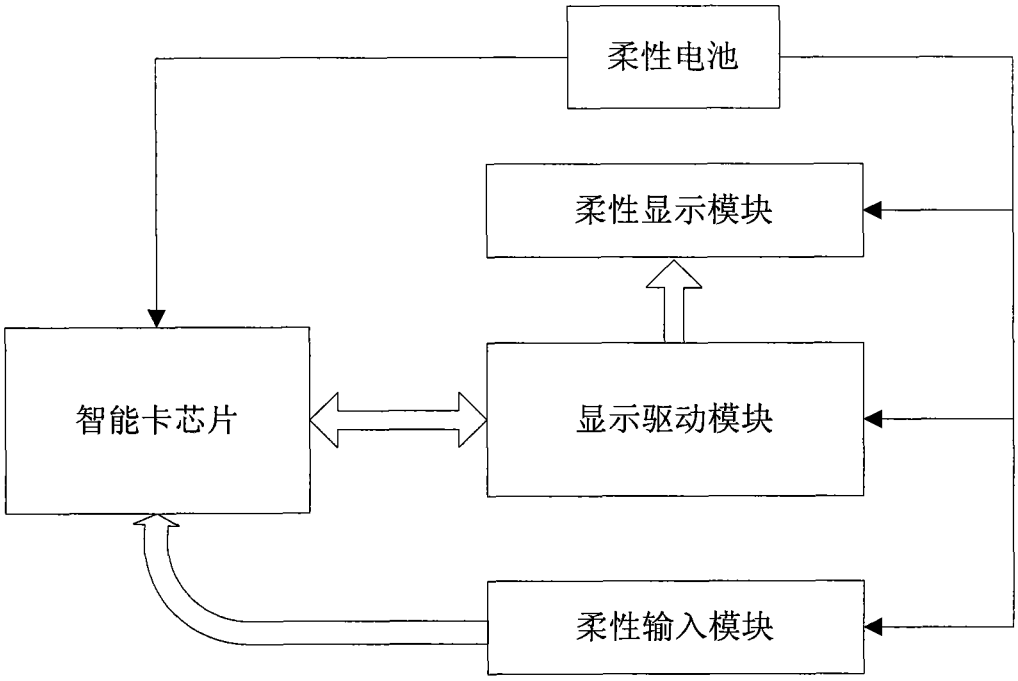

柔性电池
柔性显示模块
智能卡芯片
显示驱动模块
柔性输入模块

图 2

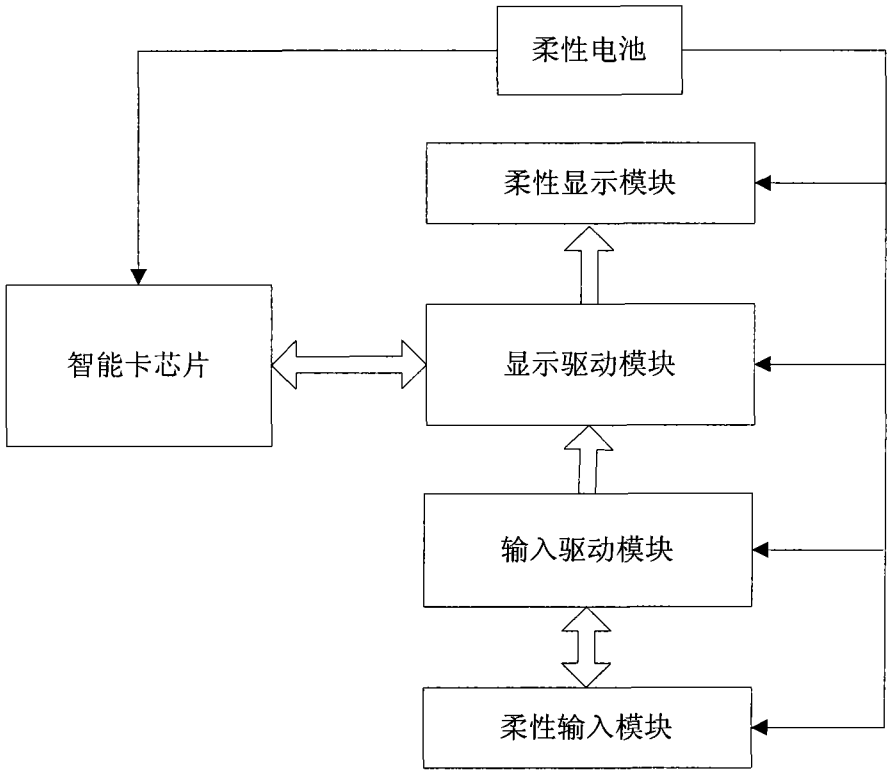

柔性电池
柔性显示模块
智能卡芯片
显示驱动模块
输入驱动模块
柔性输入模块

图 3

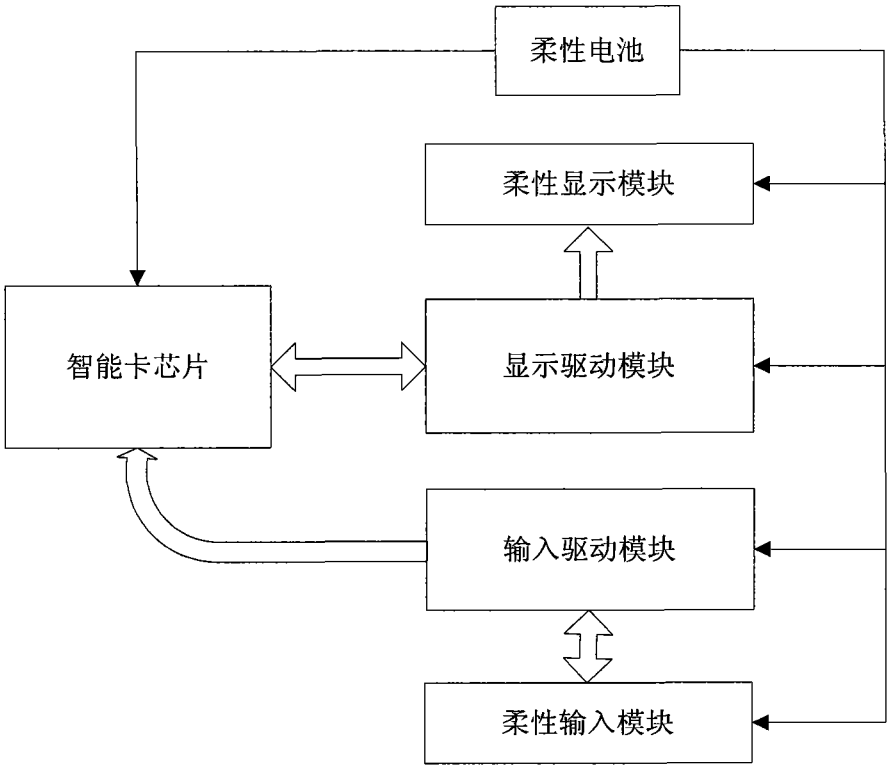

柔性电池
柔性显示模块
智能卡芯片
显示驱动模块
输入驱动模块
柔性输入模块

图 4

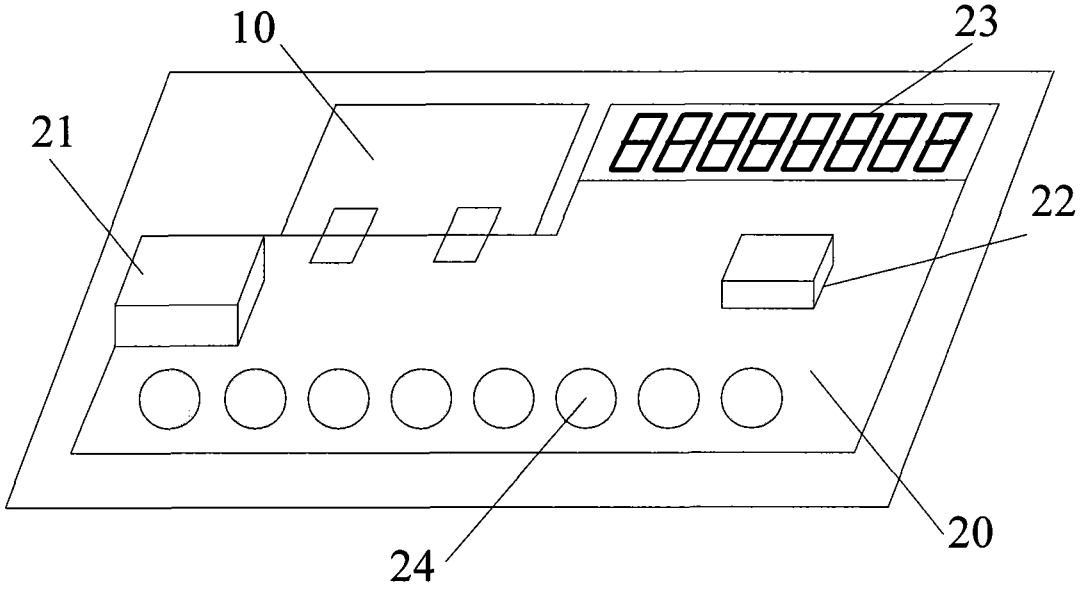


图 5

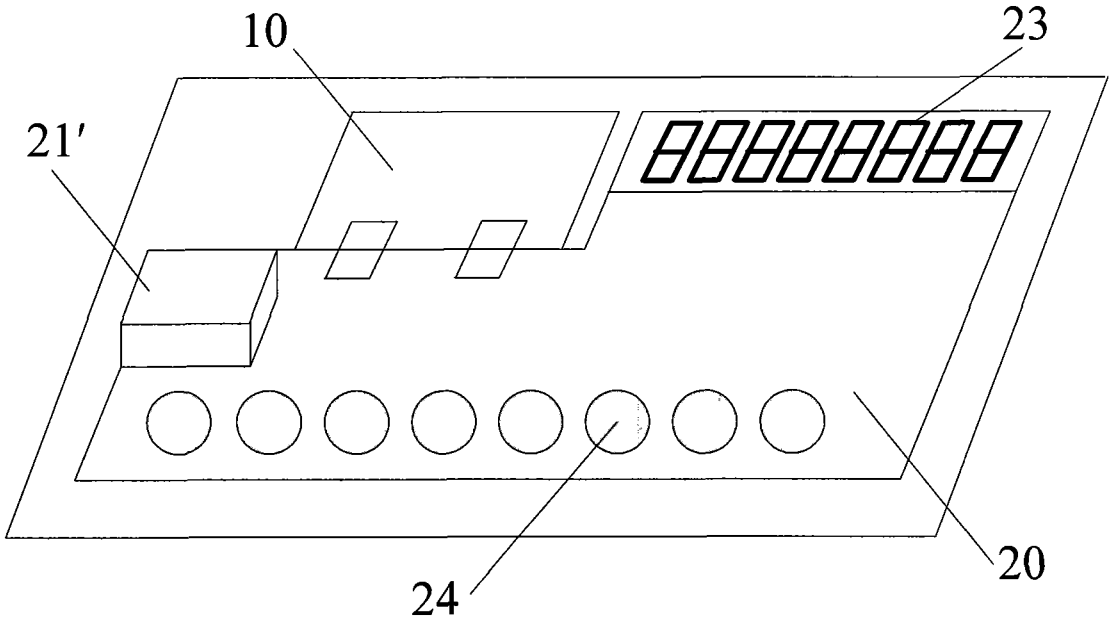


图 6

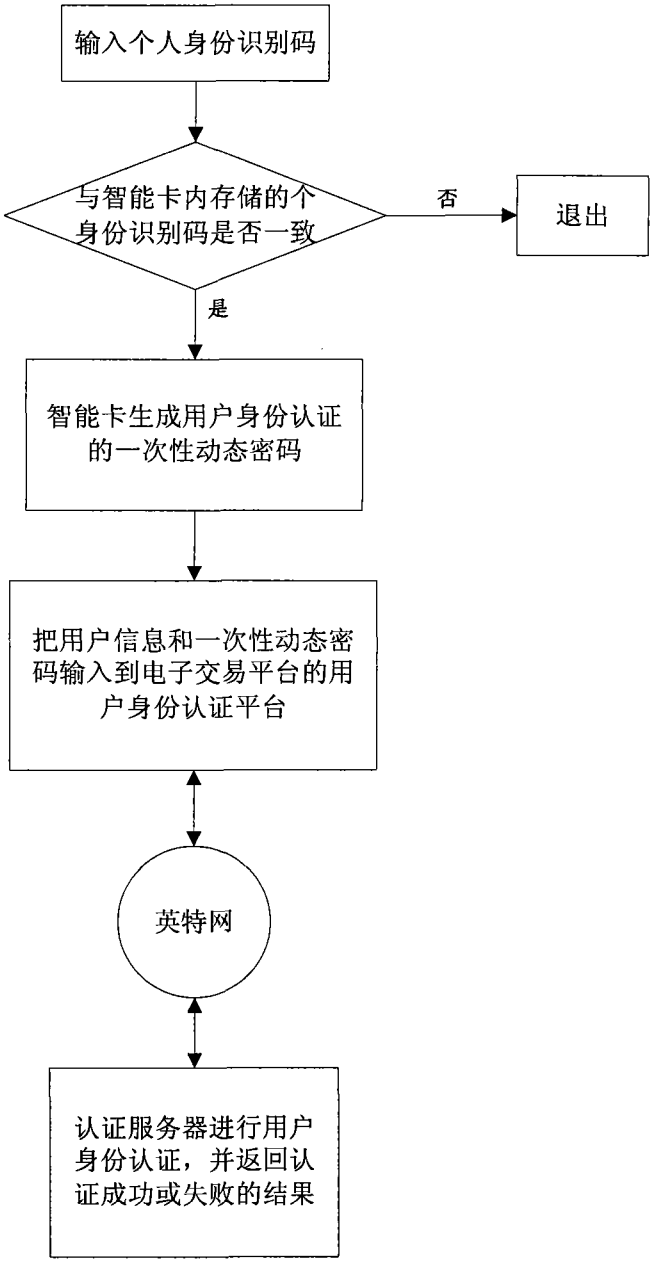

输入个人身份识别码
与智能卡内存储的个身份识别码是否一致
否
退出
是
智能卡生成用户身份认证的一次性动态密码
把用户信息和一次性动态密码输入到电子交易平台的用户身份认证平台
英特网
认证服务器进行用户身份认证，并返回认证成功或失败的结果

图 7