(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 105103525 A
(43)申请公布日 2015.11.25

(21)申请号 201480018685.0

(22)申请日 2014.01.29

(30)优先权数据
61/758,107 2013.01.29 US

(85)PCT国际申请进入国家阶段日
2015.09.28

(86)PCT国际申请的申请数据
PCT/US2014/013685 2014.01.29

(87)PCT国际申请的公布数据
WO2014/171989 EN 2014.10.23

(71)申请人 玛丽·格蕾丝
地址 美国科罗拉多州

(72)发明人 玛丽·格蕾丝

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 范胜杰 李鹤松

(51)Int.Cl.
H04M 1/66(2006.01)

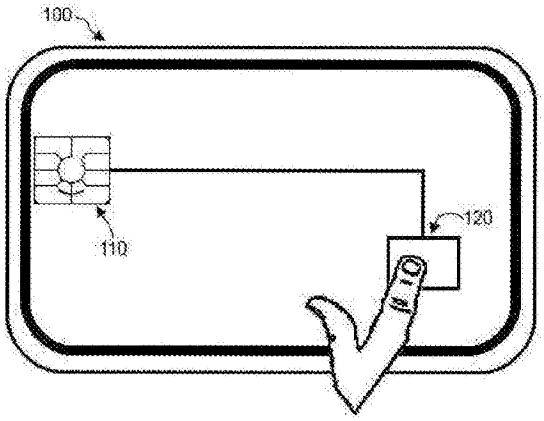
权利要求书1页 说明书8页 附图5页

(54)发明名称

具有增强的安全特性的智能卡和智能卡系统

(57)摘要

本发明涉及智能卡系统，并且特别涉及在智能卡系统中智能卡使用的安全和校验。以前，塑料卡可以传输个人数据而无需用户完成物理测试。这导致身份盗窃。本发明的实施例使用具有卡访问模块(110)和生物辨识模块(120)的智能卡(100)，其中在智能卡传输个人信息之前生物辨识模块验证用户的身份。



CN 105103525 A

1.一种智能卡,包括：

安全元件；

安全芯片；

路由器；

指纹处理器；

指纹图像传感器；

天线；

至少一个授权的指纹模板；

PCD 读取器 / 写入器；以及

软件,该软件被配置为从指纹图像传感器接收指纹图像并将指纹图像与至少一个授权的指纹模板比对并且只有在指纹图像与至少一个授权的模板匹配时才允许访问安全元件,而无需请求访问不在卡上的任何信息或系统。

2.一种存储程序的非暂态计算机可读介质,当其被智能卡的至少一个处理单元执行时,验证尝试访问在智能卡上所存储的信息的人的身份,所述程序包括用于以下步骤的指令的集合：

扫描手指以获取人的手指的指纹图像；

捕获人的所扫描的手指的指纹图像；

安全地检索指纹模板以比对所捕获的指纹；

将指纹的识别标记的集合与指纹模板的识别标记的集合进行比对；以及

设置用于访问在智能卡上所存储的信息的锁定属性,所述锁定属性仅设置为解锁或锁定其中之一,其中当指纹的识别标记的集合与指纹模板的识别标记的集合匹配时,将锁定属性设置为解锁,其中当指纹的识别标记的集合未与指纹模板的识别标记的集合匹配时,将锁定属性设置为锁定。

具有增强的安全特性的智能卡和智能卡系统

技术领域

[0001] 本文的实施例总体涉及智能卡系统，并且更具地涉及在智能卡系统中的智能卡使用的安全和校验。

背景技术

[0002] 智能卡、借记卡或银行卡、识别卡、奖励卡以及人可以携带或使用的任何其他的各种塑料卡将信息加密到卡中以便利于他们的使用。许多这些传统卡现在可以无需直接接触卡而被读取。换言之，当将卡置于邻近读取器时，读取器可能能够查询存储于卡上的信息并且提取完成交易或其它活动所需的信息。无需物理地接触卡而访问这些卡的能力已导致通过人在未察觉的卡持有者的范围内不正当地携带远程读取器或扫描仪所造成的身份盗窃和信息盗窃的很多实例。

[0003] 此外，当卡持有者不期望传送信息时，可以具有与卡的物理接触并且使用该接触从卡抓取信息。

[0004] 传统卡并没有对抗这些类型入侵的保护。虽然卡可以屏蔽可能试图抓取信息的无线资源并且保护与卡读取器的接触，但是如果这些信息抓取通道的任意一个获得与卡的接触，则他们可能能够无需卡持有者的同意而从卡中抓取信息。在物理和电子方面增强卡的安全的传统方法对于通过卡持有者的卡的期望便利使用具有不必要的妨碍。

[0005] 期望具有附加的安全特性，其将保护存储于卡上的信息而无需不必要的妨碍卡持有者针对合法和期望的交易使用卡的能力。

发明内容

[0006] 本公开涉及可能提供增强安全特性而无需不希望地妨碍通过使用者简单使用卡的改善的卡和卡安全系统。本公开的卡在处理以下问题时是高效的：身份盗窃；ID 和支付、借记卡、信用卡欺诈和盗窃；非法物理和逻辑访问；以及可以否认并阻止了对可能与在卡中包含的信息有关的电子邮件和机密电子和物理信息以及来自数据库的信息的访问和未授权移除。

[0007] 本发明的一些实施例提供了安全自身验证智能卡，其包括需要使用智能卡的、具有安全存储的信息的卡访问模块，在允许卡访问模块访问安全存储的信息之前验证人的身份的生物辨识模块，以及电源。在一些实施例中，生物辨识模块从与存储于智能卡的存储设备中的生物辨识模板比对的人接收生物辨识输入。

[0008] 在一些实施例中，卡访问模块包括安全元件和近场通讯 (NFC) 路由器并且生物辨识模块包括生物辨识传感器和生物辨识处理器。在一些实施例中，NFC 路由器使在智能卡上的信息通过使能的移动设备无线地读取。可以通过标准智能卡读取器通过接触或者无线地读取智能卡。没有其他智能卡能无需外部读取器无线地与移动设备通信。

[0009] 在一些实施例中，生物辨识模板是指纹模板，生物辨识传感器是扫描人的指纹的指纹图像传感器，并且生物辨识处理器是存储指纹模板并且将人的指纹与指纹模板比对的

指纹处理器。在一些实施例中，指纹处理器通过 NFC 路由器与安全元件非直接连接。在一些其他实施例中，指纹处理器与安全元件直接连接。

[0010] 在一些实施例中，生物辨识模块包括指纹图像传感器而没有指纹处理器。在一些这种实施例中，安全元件存储指纹样本并且将人的指纹与指纹模板比对。此外，在一些这种实施例中 NFC 路由器从所附的天线吸收功率并且将电流供应到安全元件。

[0011] 在一些实施例中，安全自身验证智能卡包括安全元件和生物辨识传感器。在一些实施例中，安全元件是双接口智能卡芯片，其向指纹传感器提供电流和时钟并且存储指纹模板并将用户的指纹与指纹模板比对。

[0012] 前述发明内容意在作用为本发明的一些实施例的简要介绍。其并不是对此说明书中公开的所有发明主题的介绍或总览。后续的详细描述和在详细描述中所参考的附图将进一步描述发明内容中描述的实施例以及其他实施例。相应地，为了理解通过此文档描述的所有实施例，需要发明内容、详细描述和附图的全面检讨。另外，所要求的主体不限于在发明内容、详细描述和附图中的示例性的细节，而是由所附权利要求定义，因为在不脱离主题的精神的情况下，可以以其他特定形式体现所要求的主题。

附图说明

[0013] 以通用术语描述了本发明，当前将参考标记做出到附图，其并非一定以比例绘制，并且其中：

[0014] 图 1 概念地示出了在一些实施例中安全自身验证智能卡的外部视图。

[0015] 图 2 概念地示出了在一些实施例中安全自身验证智能卡的架构。

[0016] 图 3 概念地示出了在一些实施例中安全智能卡的自身验证处理的时序图。

[0017] 图 4 概念地示出了在一些实施例中安全自身验证智能卡的另一个架构。

[0018] 图 5 概念地示出了在一些其他实施例中安全自身验证智能卡的架构。

[0019] 图 6 概念地示出了在至少一个实施例中安全自身验证智能卡的另一个架构。

[0020] 图 7 概念地示出了在至少一个其他实施例中安全自身验证智能卡的方框图。

[0021] 图 8 概念地示出了通过其实施本发明的一些实施例的电子系统。

具体实施方式

[0022] 在以下详细描述中，描述了本发明的若干示例和实施例。然而，要对本领域技术人员明确的是本发明不限于列出的实施例并且可以适于任何若干其他使用。

[0023] 本发明的一些实施例提供了安全自身验证智能卡，其包括具有需要使用智能卡的安全存储的信息的卡访问模块，在允许卡访问模块访问安全存储的信息之前验证人的身份的生物辨识模块，以及电源。在一些实施例中，生物辨识模块从与智能卡的存储设备中存储的生物辨识模板 (template) 比对的人获取生物辨识输入。

[0024] 通过示例方式，在图 1 中示出了安全自身验证智能卡，其概念地示出了在一些实施例中智能卡的外部视图。具体地，该图示出了具有卡访问模块 110 和生物辨识模块 120 的智能卡 100。在此示例中，生物辨识模块是指纹传感器 / 扫描仪。在指纹传感器 120 上显示了智能卡 100 的示例性用户的手指。当指纹与存储在智能卡 100 中的指纹模板匹配时，将为了使用而解锁在智能卡中的信息。由此，只有在指纹匹配的情况下用户将能够使用智

能卡。此安全特性确保丢失的卡不被未授权的用户滥用，这是因为智能卡必须首先证实用户的身份以访问在智能卡中的信息、程序或其他数据项。

[0025] 智能卡 100 可以将手指扫描仪或其他生物辨识扫描仪合并到生物识别模块 120 中以提供安全特性，其除非授权人将预先认可的生物辨识特征（诸如指纹）呈现到扫描仪，否则将阻止对于卡保持的信息的访问或传输卡保持的信息。例如，如果卡持有者想要具有仅授权卡持有者使用的个人卡，则可对生物辨识扫描仪编程以仅辨认卡持有者的生物辨识特征。除非卡持有者将生物辨识特征呈现到扫描仪，否则卡将锁定任何访问卡上所加密的信息的尝试。然而，在一些实施例中，预先通过在其中用户或卡持有者将手指接触到指纹扫描仪的自身验证处理，用户或者卡持有者可以将智能卡递交到终端。

[0026] 期望可以认可多于一个人的生物辨识特征并且一旦将适当的生物辨识特征呈现到扫描仪，则任何对于卡认可的人的生物辨识特征就可以使用卡。可以被扫描的生物辨识特征的示例包括手指、视网膜、虹状物、面部等。此外，指纹模板和授权用户的样本可以被安全地保持在智能卡中并且嵌入在智能卡上整体地被处理以便防止用户隐私的滥用和误用。

[0027] 在一些实施例中，卡访问模块包括安全元件和近场通讯 (NFC) 路由器并且生物辨识模块包括生物辨识传感器和生物辨识处理器。在一些实施例中，NFC 路由器使得在智能卡上的信息能被无线地传输并且由 NFC 使能移动设备读取。可以通过标准智能卡读取器通过接触或无线地读取智能卡。能够与移动电话无线地通信的传统生物辨识验证智能卡不存在。而且，没有能够与移动电话无线地通信的传统智能卡不需要外部读取器。

[0028] 除了通过机载扫描仪使能安全特性之外，期待智能卡也可以经由卡中的 NFC 路由器直接通信，其使卡能够被移动电话无线地读取而无需外部读取器。添加安全特性可以帮助防止移动电话上的盗窃以及 ID 和支付欺诈。一旦已经通过扫描仪授权访问卡上的信息，本公开的卡也可以通过标准智能卡读取器被优先地无线读取以提供增强的安全而仍利用标准卡读取器。

[0029] 图 2 概念地示出了在一些实施例中安全自身验证智能卡的架构 200。在该图中的卡访问模块 110 是可以或不可从卡的表面可视的安全芯片。换言之，安全芯片是允许访问智能卡的接触板，例如通过仿真智能卡读取器的应用或智能卡读取器。此外，在该图中的智能卡包括安全元件 210 和具有促进在终端（例如，专用智能卡读取设备、使能 NFC 并且包括可以读取智能卡的应用的移动设备等）和智能卡之间的无线通信的天线 230 的 NFC 路由器 220。

[0030] 通过参考图 1 在上面描述的生物辨识模块 120 在图 2 中被表示为两个分离的集成电路 (IC) 芯片，即指纹处理器 240 和指纹传感器 250。此外，智能卡架构 200 示出了一旦通过生物辨识扫描仪授权访问卡上的信息，针对任何一种使用任何一种标准协议的信息处设备的通信和资源管理。例如，智能卡可以使用 ISO7816 和 ISO14443 协议与外部终端安全地通信。也可以在本公开的范围内使用私有协议。然而，数据传送以及资源共享（即，功率、地、时钟等）依赖于卡的授权用户的手指，当其由指纹传感器 250 被扫描或由指纹处理器 240 被匹配时，将打开卡并且允许对在卡上所包含的信息访问或者通信。与此相反，当扫描到未授权的人的手指时，卡将不工作。

[0031] 在一些实施例中，生物辨识模板是指纹模板，生物辨识传感器是扫描人的指纹的指纹图像传感器，并且生物辨识处理器是存储指纹模板并且将人的指纹与指纹样本比对的

指纹处理器。在一些实施例中，指纹处理器经由 NFC 路由器不直接地连接到安全元件。在一些其他实施例中，指纹处理器直接连接到安全元件。

[0032] 期待可以将根据本公开的安全自身验证智能卡用作访问控制卡以监视通过卡持有者的访问并且将其限制到安全访问区域。还期待可以将根据本公开的卡用作金融支付和现金卡。可以将如此卡用作医疗信息卡以安全地并且安心地保持卡持有者的关键的、私人的以及其他医疗信息。可以将根据本公开的卡用作组合卡，诸如但不限于使持卡者能够在单个卡上接收全部政府和其他支付的组合政府 ID 和支付卡。可以将根据本公开的卡用于对于政府机构、公司、银行和其他实体的所有支付的会计控制。可以将卡用于证券和衍生品等交易者的实时交易结算以识别交易者并且作用为防止失控、未授权和内部交易。本公开许可创建针对地铁、公车、飞机、汽车生成运输 ID 和支付卡以及针对危险品和跨境汽车的运输和物品和个人的运输的驾驶员识别。

[0033] 提出根据本公开的可能使用卡的上述示例仅作为示例性的并且不期望限制如此卡的可能使用。尽管通过参照上述图 1 和图 2 描述了示例，但是一些实施例的安全自身验证智能卡包括以下示例性元件。不期望这是部件的穷尽型或排他型列表并且呈现此列表以提供根据本公开的卡的示例性实施例。

[0034] 1. 安全元件

[0035] 2. 安全芯片

[0036] 3. NFC 路由器

[0037] 4. 无源部件

[0038] 5. 指纹处理器

[0039] 6. 指纹图像传感器

[0040] 7. 天线

[0041] 8. 指纹模板

[0042] 9. 功率控制设备 (PCD) 读取器 / 写入器

[0043] 10. 存储器

[0044] 11. 软件

[0045] 12. 算法

[0046] 以保持关联安全智能卡的整体操作的方式相互关联各种示例性部件。为了更好地理解整个方式，其中，安全智能卡的不同组件通过生物辨识匹配、在图 3 中概念性地示出的时序图执行自身验证，其提供了可以在一些实施例中使用智能卡期间执行的识别匹配和验证处理中的事件的示例。如此图中所示，NFC 路由器 320 经由 NFC 天线调节从功率控制设备 (PCD)310 所传送的功率。PCD 310 也可以将功率分发到安全元件 330 和指纹处理器 340。在一些实施例中，NFC 路由器 320 作用为在 PCD 读取器 / 写入器 310、安全元件 330 和指纹处理器 340 之间的切换。

[0047] 安全元件 330 可以处理密码计算 (cryptographic computation)，并且处理通过外部实体发布的外部验证。安全元件 330 可以与存储设备（例如，EEPROM 非易失性永久存储器）协作以安全地存储密钥和数据。例如，安全元件可以存储在非对称密码系统中使用的私钥，诸如 RSA 或 DES。安全元件 330 也可以处理外部验证，其可以通过尝试访问卡的信息的外部实体被发布（例如，经由密码令牌接口库和 Cryptoki API 调用）。

[0048] 指纹处理器 340 可以是被配置为从指纹图像传感器读出指纹图像并且尝试将图像数据与存储用于识别授权用户或卡持有者的指纹图像模板匹配的基于安全处理器的单元。指纹图像传感器可以被配置为根据指纹处理器 340 的请求抓取或者接收指纹并且可以发送背部图像数据以便与用于授权用户或卡持有者的存储的指纹图像模板评估。

[0049] 虽然参照图 1-3 描述的示例提供了根据本公开的智能卡的安全自身验证系统的概观，但是附加配置和和架构的以下示例进一步突出了一些实施例的安全自身验证智能卡的方面和细节。

[0050] 具体地，安全智能卡的一些实施例包括匹配并且验证用户身份的指纹传感器，其如果成功匹配并验证，则打开智能卡以便在智能卡上的安全芯片能够与外部读取器通信。在一些此实施例中，通过在智能卡中植入的一个或更多的程序来执行匹配的操作。

[0051] 图 4 概念性地示出了安全自身验证智能卡的架构 400，其中指纹传感器 250 接收用户的手指以扫描并且指纹处理器 240 将捕获的用户的指纹图像与存储的指纹的模板图像比对，并且如果成功匹配，则经由 NFC 路由器 220 间接地打开智能卡从而允许安全芯片 110 与外部读取器通信。

[0052] 图 5 概念地示出了安全自身验证智能卡的另一个架构 500，其中指纹处理器 240 经由到安全元件 210 的直接接口打开智能卡。

[0053] 在一些实施例中，指纹传感器 / 扫描仪可以安装于连接到安全元件的智能卡上并且安全芯片位于卡的相同塑料体上。图 6 和图 7 概念地示出了安全自身验证智能卡的附加架构 600 和 700，其中指纹传感器 250 直接连接到卡上的安全元件 210。在图 6 中所示的示例架构 600 只包括三个 IC 芯片，具体地是安全元件 210、NFC 路由器 220 和指纹传感器 / 扫描仪 250。在这些实施例中，安全元件 210 执行指纹处理以匹配并验证用户的身份。

[0054] 而且，如图 7 所示，指纹传感器 / 扫描仪 250 与安全元件直接通信。由于在指纹传感器 250 和安全元件 210 之间的直接接口，所以此配置消除了 NFC 路由器。这也在指纹图像和其他智能卡存储信息的传输上提供了显著的安全性，其在数据传送期间完全地被压缩于卡内。另外，在图 7 中所示的架构 700 中，功率的来源是处理机载安全元件并且完全从不需要电池的电源获得（例如，感应）。

[0055] 在一些实施例中，可以以自身充电和无电池之一或这两者来配置智能卡。尤其是，通过参照图 4 和图 5 描述的示例架构所关联的电源基于电池电源。另一方面，通过参照图 6 和图 7 描述的示例架构所关联的电源基于非电池源，诸如感应。智能卡也可以使用经由 ISO7816 和 ISO1443RF 功率从终端接收的功率来操作。

[0056] 为了根据本公开使用智能卡，授权用户或卡持有者可以用以下一种或更多的模式配置智能卡：通过使用无线地将卡放到移动电话或标准无线智能卡读取器附近，针对物理或逻辑访问作为安全访问卡、作为安全 ID 卡，针对借记卡或信用卡作为安全支付卡。用户可以使用具有指纹传感器的智能卡以匹配和验证他们的身份，其随后将打开卡以便在智能卡上的安全芯片可以与外部读取器通信来验证他们的身份。该匹配优选地全部在可以进一步保护隐私和安全性的卡上完成。

[0057] 另外，可以在智能卡上安装人会向其接触他们的登记手指的指纹传感器 / 扫描仪，其可能与位于卡的相同塑料主体上的智能元件和安全芯片连接。

[0058] 此外，可以在全部需要积极识别的领域使用根据本公开的智能卡，诸如但不限于

驾驶员的驾照、护照、医疗保险和社会保险支付以及全部政府识别卡，在所有访问的领域、在所有支付的领域、在交易平台上交易者的数量和交易者的验证方面以及安全性，其可以被用于安全计算机和数据库访问和控制以及阻止黑客行为和 / 或未授权访问和移除信息。本公开的智能卡可以用作许多不同类型的访问控制卡、许多不同类型的金融支付和提款卡、具有用户鉴定和其他医疗信息的许多不同类型的医疗 ID 卡，组合卡，诸如但不限于使用户在其卡上接收所有政府和其他支付的政府 ID 和支付卡的政府 ID 和支付卡的其中之一。智能卡可以用于针对政府机构、公司和银行的所有支付的会计控制。

[0059] 一些实施例的智能卡可能符合来自以下未穷尽的标准列表的一个或更多的标准：

[0060] ISO/IEC 7816

[0061] ISO/IEC 14443

[0062] ISO 18092

[0063] NFC 论坛定义标准

[0064] EMV

[0065] 维萨波 (VisaWave)，拍立购 (PayPass)

[0066] FIPS140-1、2、3

[0067] FIPS121

[0068] 全球平台 (GlobalPlatform)

[0069] Java 卡 (JavaCard)

[0070] 虽然通过参照一个或更多附图已经描述了本发明的若干实施例，要理解的是本发明并不限制于上面所列出的特定实施例。由此，认识到本领域技术人员将理解可以在不脱离本发明的精神和意图的情况下做出特定替代、选择、修改和省略。

[0071] 而且，将实施一些上述特征和应用作为被指定作为在计算机可读存储介质（也称为计算机可读介质或机器可读介质）上记录的指令集的软件处理。当通过一个或更多的处理单元（例如，一个或更多的处理器或其它处理单元）执行指令时，他们使处理单元执行在指令中指示的行动。计算机可读介质的示例包括但不限于 CD-ROM、闪存驱动器、RAM、硬盘驱动器、EPROM、EEPROM 等。计算机可读介质不包括无线传播或通过有线连接的电子信号和载波。

[0072] 在此说明书中，术语“软件”意为包括存在于只读存储器的固件或存储在磁存储器中的应用，可以将其读入通过处理器处理的存储器。而且，在一些实施例中，多个软件发明可以被实施为较大程序的子部分同时保持区别软件发明。在一些实施例中，多个软件发明也可以实施为分离的软件。最后，此处描述的一齐实施软件发明的分离的软件的组合是在本发明的范围之内。在一些实施例中，当安装以操作一个或更多的电子系统时，软件程序定义一个或更多的执行并且实行软件程序的操作的特定机器实施方式。

[0073] 图 8 概念地示出了通过其实施本发明的一些实施例的电子系统 800。电子系统 800 可以是计算机、电话、PDA 或任何其他类型的电子设备。如此电子系统包括各种类型的计算机可读介质和用于各种类型计算机可读介质的接口。电子设备 800 包括总线 805、处理单元 810、系统存储器 815、只读 820、永久存储设备 825、输入设备 830、输出设备 835 和网络 840。

[0074] 总线 805 集合性地代表通信地连接电子系统 800 的多个内部设备的所有系统、外

围设备以及芯片总线。例如，总线 85 将处理单元 810 通信地连接于只读 820、系统存储器 815 以及永久存储设备 825。

[0075] 根据这些各种存储单元，处理单元 810 提取执行的指令和处理的数据以便执行本发明的处理。在不同实施例中处理单元可以是单处理器或多核处理器。

[0076] 只读存储器 (ROM)820 存储处理单元 810 和电子系统的其他模块需要的指令和静态数据。另一方面，永久存储器设备 825 是读写存储设备。该设备是即便电子系统 800 关闭也存储指令和数据的非易失性存储单元。本发明的一些实施例使用大容量存储设备（诸如磁盘或光盘以及其对应的盘驱动器）作为永久存储设备 825。

[0077] 其他实施例使用可移除存储设备（诸如软盘和闪盘驱动器）作为永久存储设备 825。与永久存储设备 825 类似，系统存储器 815 是读写存储器设备。然而，与永久存储设备 825 不同的是，系统存储器 815 是易失性读取存储器，诸如随机存取存储器。系统存储器 815 存储处理器在运行时间需要的指令和数据。在一些实施例中，在系统存储器 815、永久存储设备 825 和 / 或只读 820 中存储本发明的处理。例如，各种存储单元包括用于根据一些实施例的可显示符号的处理外观选择的指令。处理单元 810 从这些各种存储器单元检索执行的指令和处理的数据以便执行一些实施例的处理。

[0078] 总线 805 还与输入设备 830 和输出设备 835 连接。输入设备使得用户能够向电子系统通信信息并且选择指令。输入设备 830 包括字母数字键盘和指示设备（也称作“指针控制设备”）。输出设备 835 显示通过电子系统 800 所生成的图像。输出设备 835 包括指示器和显示设备，诸如阴极射线管 (CRT) 或液晶显示器 (LCD)。一些实施例包括诸如作用为输入设备和输出设备这两者的触摸屏。

[0079] 最终，如图 8 所示，总线 805 还通过网络适配器（未示出）将电子系统 800 附接到网络 840。以此种模式，计算机可以是计算机的网络的一部分（诸如局域网（“LAN”）、广域网（“WAN”）或互联网），或者网络（诸如互联网）的网络。电子系统 800 的所有或全部部件可以用于结合到本发明。

[0080] 可以以数字电子电路、计算机软件、固件或者硬件实施上述这些功能。可以使用一个或更多的计算机程序产品实施技术。可编程处理器和计算机可以被打包或者包括于移动设备中。可以通过一个或更多的可编程处理器以及通过一个或多个集合的可编程逻辑电路执行处理和逻辑流。可以通过通信网络内接通用和特殊目的计算和存储设备。

[0081] 一些实施例包括电子部件，诸如微处理器、以机器可读或计算机可读介质（可选地，称作计算机可读存储介质、机器可读介质或机器可读存储介质）存储计算机程序指令的存储设备和存储器。如此计算机可读介质的一些示例包括 RAM、ROM、只读光盘 (CD-ROM)、可记录光盘 (CD-R)、可重写光盘 (CD-RW)、只读数字通用光盘（例如，DVD-ROM、双层 DVD-ROM），各种可记录 / 可重写 DVD（例如，DCD-RAM、DCD-RW、DVD+RW 等），闪存存储器（例如，SD 卡、迷你 SD 卡、微型 SD 卡等），磁或者固态硬盘驱动器、只读和可记录蓝光 (Blu-Ray) ®光盘，超密度光盘，任何其他光或磁介质，以及软盘。计算机可读介质可以存储通过至少一个处理单元可执行的计算机程序并且包括用于执行各种操作的指令集。计算机程序和计算机代码的示例包括例如通过编译器生成的机器代码以及包含通过计算机、电子部件或使用解译器的微处理器所执行的高级代码的文件。

[0082] 虽然参照许多特定细节描述了本发明，但是本领域普通技术人员将认识到在不脱

离本发明的精神的情况下，可以以其他特定形式体现本发明。由此，本领域普通技术人员应理解本范围并不通过上述示例性的细节和示例受到限制，而是通过所附权利要求被定义。

[0083] 工业实用性

[0084] 本发明的实施例的一个目的是从指纹图像传感器接收指纹图像并且将指纹图像与至少一个授权指纹模板比对。此信息可以被用于向受限空间提供或者限制访问。

[0085] 本发明的实施例的另一个目的是设置用于访问在智能卡上所存储的信息的锁定属性。这许可当正确地完成测试时访问智能卡上的信息。

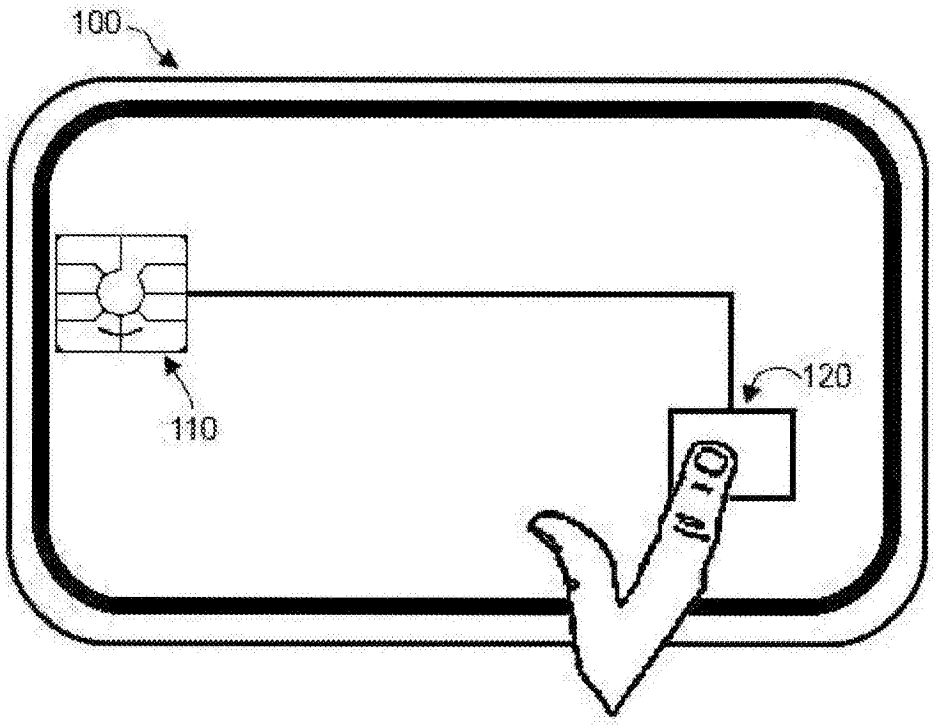

100
110
120

图 1

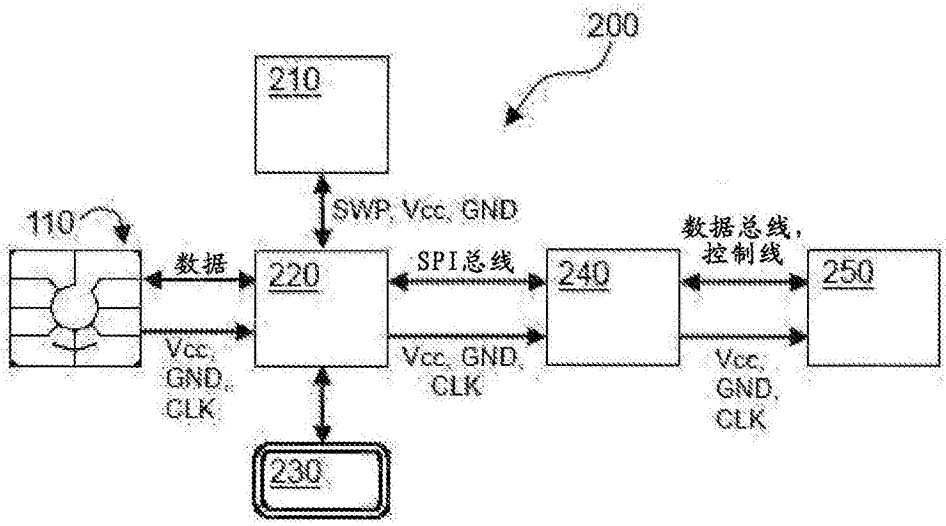

200
210
SWP, Vcc, GND
110
数据
220
SPI总线
240
数据总线，
控制线
250
Vcc,
GND,
CLK
Vcc, GND,
CLK
Vcc,
GND,
CLK
230

图 2

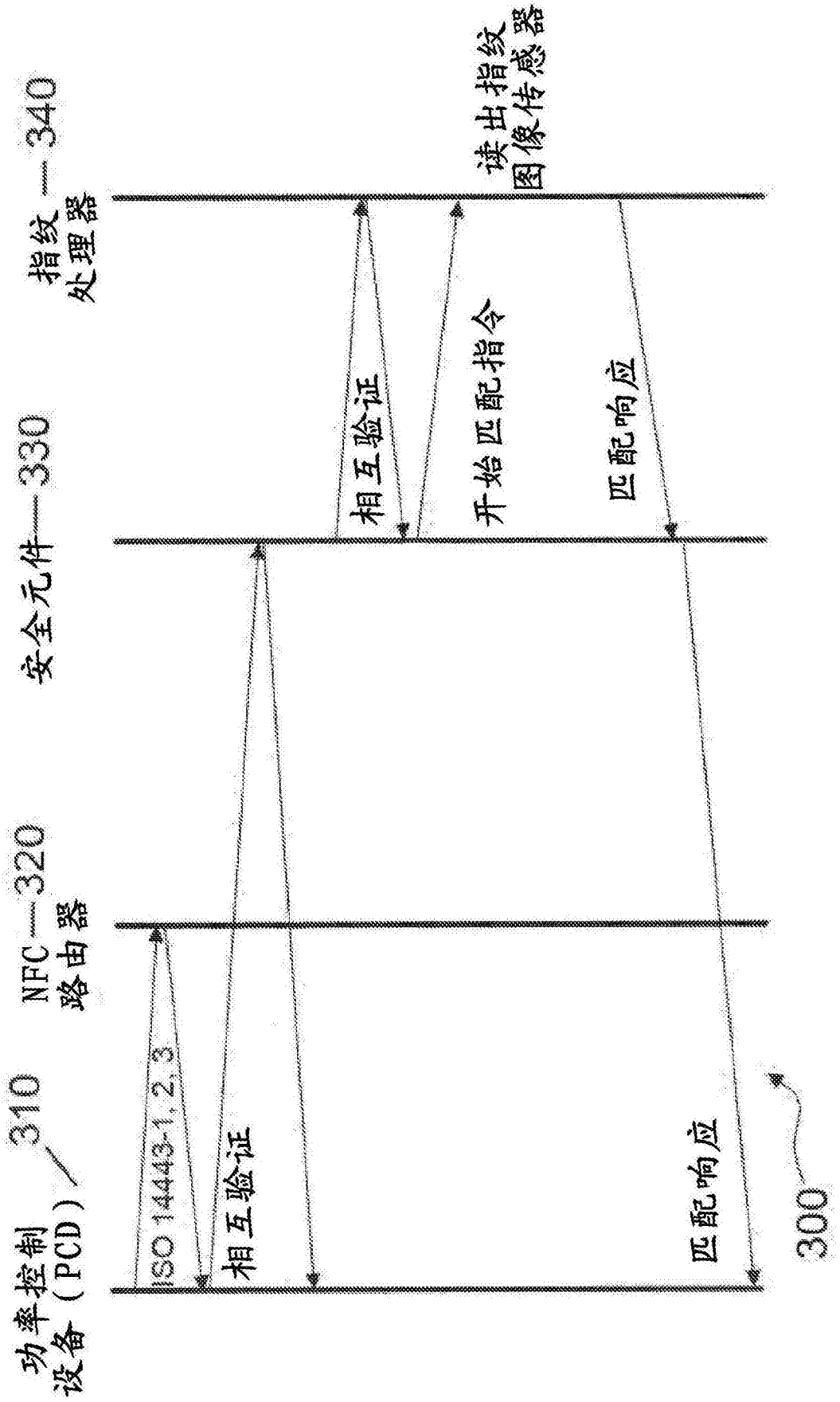

功率控制设备（PCD）
310
NFC—320
路由器
安全元件—330
指纹—340
处理器
读出指纹图像传感器
ISO 14443-1, 2, 3
相互验证
相互验证
开始匹配指令
匹配响应
匹配响应
300

图 3

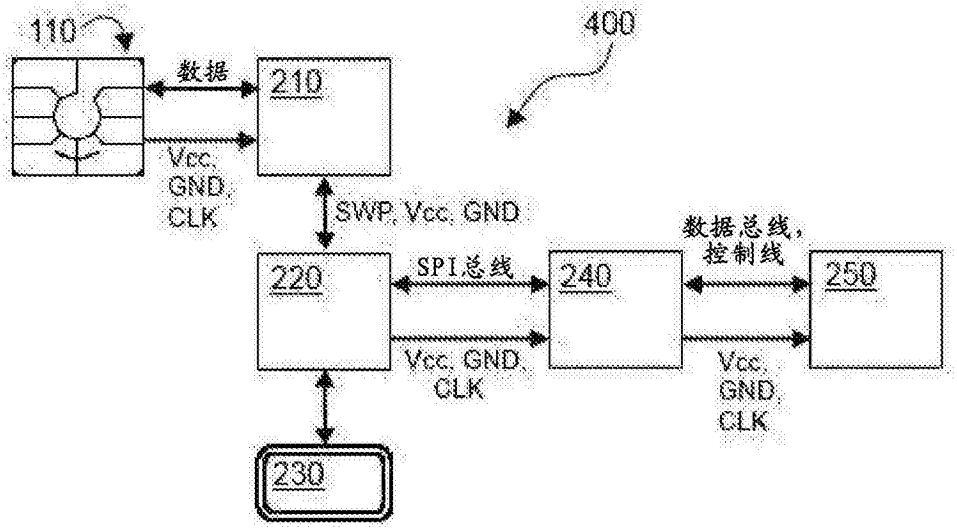

110
数据
210
400
Vcc,
GND,
CLK
SWP, Vcc, GND
数据总线，
控制线
220
SPI总线
240
250
Vcc, GND,
CLK
Vcc,
GND,
CLK
230

图 4

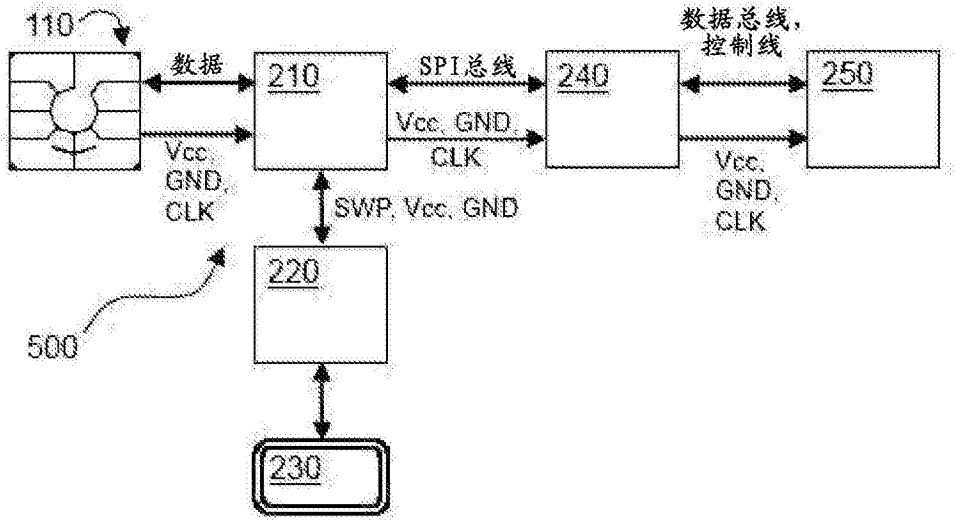

110
数据
210
SPI总线
240
数据总线，
控制线
250
Vcc,
GND,
CLK
Vcc, GND,
CLK
Vcc,
GND,
CLK
SWP, Vcc, GND
500
220
230

图 5

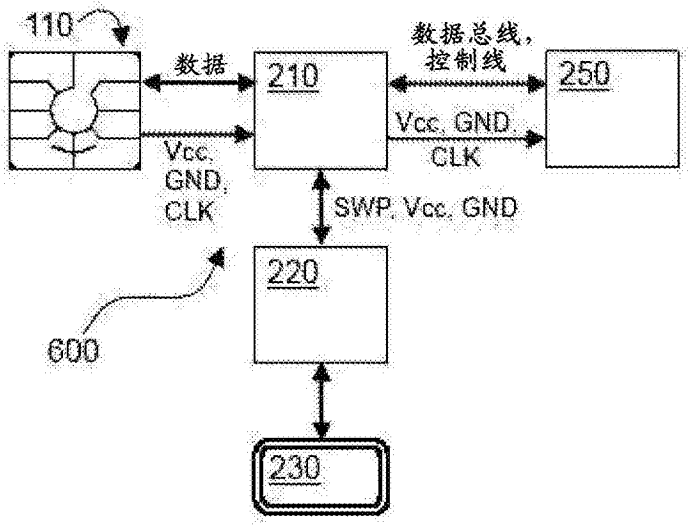

110
数据
210
数据总线，
控制线
250
Vcc, GND,
CLK
Vcc,
GND,
CLK
SWP, Vcc, GND
220
600
230

图 6

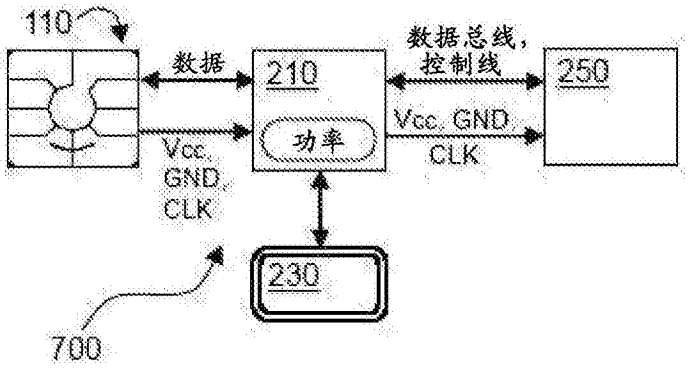

110
数据
210
数据总线，
控制线
250
功率
Vcc, GND,
CLK
Vcc,
GND,
CLK
230
700

图 7

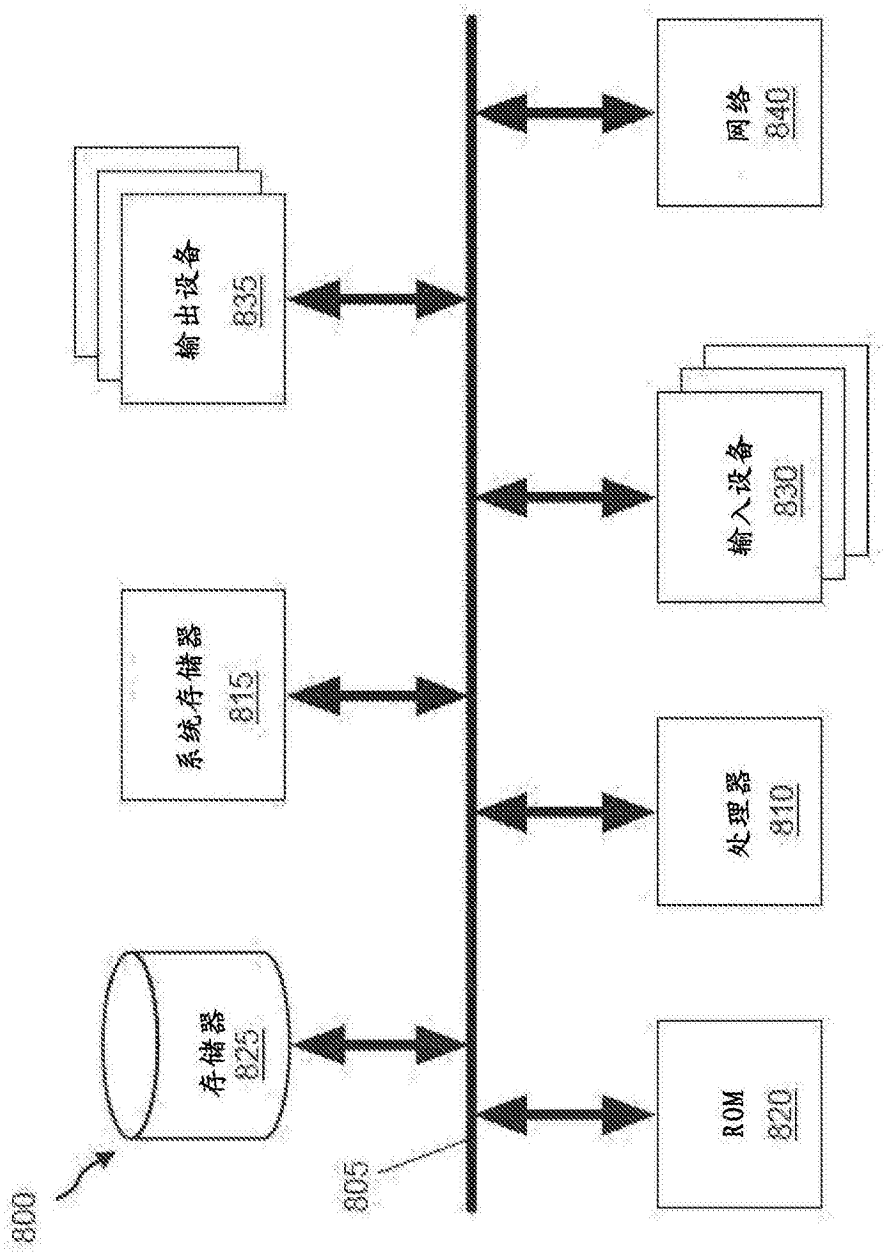

网络
840
输出设备
835
输入设备
830
系统存储器
815
处理器
810
存储器
825
ROM
820
800
805

图 8