

用户识别卡及智能终端、用户识别卡应用方法

本申请要求了申请日为 2022 年 04 月 12 日、申请号为 202210383011.7、名称为“用户识别卡及智能终端、用户识别卡应用方法”的中国发明申请的优先权，并且通过参照上述中国发明申请的全部说明书、权利要求、附图和摘要的方式，将其引用于本申请。

技术领域

本发明涉及通信技术领域，特别涉及一种用户识别卡及智能终端、用户识别卡应用方法。

背景技术

传统用户识别卡（SIM，Subscriber Identity Module）是移动通讯系统中标识移动用户身份的集成电路（Integrated Circuit，IC）卡，用于运营商数据的安全存储及对用户身份鉴权和客户信息加密。用户识别卡广泛应用于手机、智能手表等智能终端。

在现有技术中，用户识别卡受功耗、成本等约束，其处理性能一般较低，且外部接口较少，并且与智能终端上的处理模块间的通信速率较低，制约了其在支持身份认证、金融交易等安全应用方面的能力发挥。同时，智能终端上的处理模块具有很强的处理性能，可以支持丰富的应用，但也由于其具有丰富的逻辑与物理通道，其运行环境复杂，易于受到安全攻击。

因此，希望能有一种新的用户识别卡及智能终端、用户识别卡应用方法，能够克服上述问题。

发明内容

鉴于上述问题，本发明的目的在于提供一种用户识别卡及智能终端、用户识别卡应用方法，特别是一种扩展用户识别卡支持应用能力的方法，

从而扩展用户识别卡的应用程序支持能力，提升应用程序运行的性能与安全性。

根据本发明的一方面，提供一种用户识别卡，包括第一通讯接口，所述第一通讯接口支持 7816 接口与 SPI+接口复用，其中，所述 SPI+接口的通讯速率高于所述 7816 接口的通讯速率；第一运行单元，与所述第一通讯接口相连接以传输数据，所述第一运行单元运行第一子程序来实现以下功能中的至少一种：安全启动、加密、解密和认证。

可选地，所述第一通讯接口与智能终端的第二通讯接口相连接以传输数据。

根据本发明的另一方面，提供一种智能终端，包括处理模块；所述处理模块包括：第二通讯接口，所述第二通讯接口支持 7816 接口与 SPI+接口复用，其中，所述 SPI+接口的通讯速率高于所述 7816 接口的通讯速率；第二运行单元，与所述第二通讯接口相连接以传输数据，并运行第二子程序以处理非敏感数据和/或进行人机交互实现；

可选地，所述第二通讯接口与用户识别卡的第一通讯接口相连接以传输数据。

可选地，所述第一通讯接口和/或所述第二通讯接口包括数据端口，用于数据的输入和/或输出；时钟端口，用于传递时钟信号，所述时钟信号的上升沿或下降沿作为数据的同步信号；以及复位端口，用于传递复位信号，所述复位信号高电平或低电平有效，其中，当所述处理模块向所述用户识别卡发出有效的复位信号时，所述用户识别卡进行冷复位；当所述用户识别卡向所述处理模块发出有效的复位信号时，所述处理模块对所述第二子程序进行热复位。

可选地，所述用户识别卡或所述处理模块均可作为主端发起通讯。

根据本发明的再一方面，提供一种用户识别卡应用方法，包括在用户识别卡上运行第一子程序以实现安全启动和/或加密和/或解密和/或认证；通过支持 7816 接口与 SPI+接口复用的通讯接口，建立所述用户识别卡与处理模块的通讯连接；以及在智能终端的所述处理模块上运行第二子程序。

可选地，所述用户识别卡应用方法还包括所述用户识别卡/处理模块以 7816 协议向所述处理模块/用户识别卡发起是否支持所述 SPI+接口的询问；在所述处理模块/用户识别卡支持所述 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 SPI+接口协议进行通讯；在所述处理模块/用户识别卡不支持所述 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 7816 接口协议进行通讯。

可选地，所述用户识别卡应用方法还包括所述用户识别卡向所述处理模块发送第一复位信号，所述处理模块获取所述第一复位信号后对所述应用程序进行热复位；或所述处理模块向所述用户识别卡发送第二复位信号，所述用户识别卡获取所述第二复位信号后进行冷复位。

可选地，建立所述用户识别卡与所述处理模块的通讯连接以进行数据交互；所述用户识别卡应用方法还包括：所述用户识别卡向所述处理模块发送时钟信号；或所述处理模块向所述用户识别卡发送时钟信号，其中，所述时钟信号的上升沿或下降沿作为所述数据交互的同步信号。

根据本发明实施例的用户识别卡及智能终端、用户识别卡应用方法，在用户识别卡上运行第一子程序以实现安全启动和/或加密和/或解密和/或认证，提升了应用程序运行的安全性。

进一步地，在处理模块上运行第二子程序以执行应用程序，扩展了用户识别卡对应用程序的支持能力。

进一步地，用户识别卡与处理模块之间的通讯接口为 7816 接口，并复用为 SPI+接口，传输兼容性好且效率高，适用范围广。

附图说明

通过以下参照附图对本发明实施例的描述，本发明的上述以及其他目的、特征和优点将更为清楚，在附图中：

图 1 示出了根据本发明实施例的用户识别卡的结构示意图；

图 2 示出了根据本发明实施例的智能终端的结构示意图；

图 3 示出了根据本发明实施例的智能终端的装置示意图；

图 4 示出了根据本发明实施例的时序示意图；

图 5 示出了根据本发明实施例的应用程序的功能分配示意图；

图 6 示出了根据本发明实施例的用户识别卡应用方法的方法流程图。

具体实施方式

以下将参照附图更详细地描述本发明的各种实施例。在各个附图中，相同的元件采用相同或类似的附图标记来表示。为了清楚起见，附图中的各个部分没有按比例绘制。此外，在图中可能未示出某些公知的部分。

下面结合附图和实施例，对本发明的具体实施方式作进一步详细描述。在下文中描述了本发明的许多特定的细节，例如部件的结构、材料、尺寸、处理工艺和技术，以便更清楚地理解本发明。但正如本领域的技术人员能够理解的那样，可以不按照这些特定的细节来实现本发明。

应当理解，在描述部件的结构时，当将一层、一个区域称为位于另一层、另一个区域“上面”或“上方”时，可以指直接位于另一层、另一个区域上面，或者在其与另一层、另一个区域之间还包含其它的层或区域。并且，如果将部件翻转，该一层、一个区域将位于另一层、另一个区域“下面”或“下方”。

图 1 示出了根据本发明实施例的用户识别卡的结构示意图。如图 1 所示，根据本发明实施例的用户识别卡 100 包括第一运行单元 110 和第一通讯接口 120。

具体地讲，第一运行单元 110 与第一通讯接口 120 相连接以传输数据，第一运行单元 110 运行第一子程序来实现以下功能中的至少一种：安全启动、加密、解密和认证。可选地，第一运行单元 110 运行小程序（Applet）以实现相应应用程序的安全启动、加解密及认证等安全功能。可选地，输入和/或输出的数据以及本文中提及的其它数据，可以是信号、命令等各种形式的信息。

在本发明的可选实施例中，第一通讯接口 120 用于数据的输入和/输出。第一通讯接口 120 为 7816 接口复用为 SPI+（特定串行外设接口）。可选地，第一运行单元 110 通过第一通讯接口 120 接收输入数据，运行第一子程序来实现以下功能中的至少一种：安全启动、加密、解密和认

证，并将第一子程序产生的输出数据通过第一通讯接口 120 输出。

图 2 示出了根据本发明实施例的智能终端的结构示意图。如图 2 所示，根据本发明实施例的智能终端例如为手机、电脑等设备（下文中以智能终端为手机举例），包括用户识别卡 100 和处理模块 200。其中，用户识别卡 100 包括第一运行单元 110 和第一通讯接口 120；处理模块 200 包括第二运行单元 210 和第二通讯接口 220。

具体地讲，第一运行单元 110 与第一通讯接口 120 相连接以输入和/或输出数据，第一运行单元 110 运行第一子程序来实现以下功能中的至少一种：安全启动、加密、解密和认证。

第二运行单元 210 与第二通讯接口 220 相连接以传输数据，并运行第二子程序，例如通过运行第二子程序以执行应用程序。可选地，第二运行单元 210 运行（执行）应用程序（APP），负责处理非敏感信息及人机交互等功能。第二通讯接口 220 为 7816 接口复用为 SPI+（特定串行外设接口）。

在本发明的上述实施例中，提出了一种新的智能终端，能够扩展用户识别卡（SIM 卡）支持应用的能力。该智能终端采用用户识别卡及其上运行的 Applet 与处理模块及其上运行的 APP 结合的方式保证应用程序运行的性能与安全性。具体地，该智能终端包括用户识别卡及其上面运行的 Applet，处理模块及其上运行的 APP。用户识别卡及其上运行的 Applet 负责安全启动，加解密及认证等安全功能，处理模块及其上运行的 APP 负责处理非敏感信息及人机交互功能。处理模块及其上运行的 APP 对用户识别卡的处理能力进行扩展。

图 3 示出了根据本发明实施例的智能终端的装置示意图。如图 3 所示，根据本发明实施例的智能终端包括处理模块 200 和用户识别卡 100。

具体地讲，处理模块 200 中的第二运行单元 210 包括基带处理器和/或应用处理器，例如为手机基带/应用处理器。智能终端的基带/应用处理器上运行有应用程序（APP）以进行应用程序中非敏感数据处理、人机交互等功能。

用户识别卡 100 中的第一运行单元 110 上运行有小程序（Applet）

以实现应用程序的安全启动、加解密及认证功能等。

处理模块 200 上的第二通讯接口 220 与用户识别卡 100 上的第一通讯接口 120 相连接以传输数据。

如图 3 所示,第一通讯接口 120 包括数据端口(IO)、时钟端口(CLK)和复位端口(RST)。第二通讯接口 220 包括数据端口(IO)、时钟端口(CLK)和复位端口(RST)。数据端口(IO)用于数据的输入和/输出。时钟端口(CLK)用于传递时钟信号。复位端口(RST)用于传递复位信号。

在本发明的一个具体实施例中,手机基带/应用处理器通过三个物理端口(输入输出端口、时钟端口和复位端口)与用户识别卡相连接,同时支持 7816 接口与高速接口 SPI+接口复用,其中 7816 接口的 IO 端口被复用为 SPI+的双向数据接口 SPI_SDA; 7816 接口的时钟端口 CLK 被复用为 SPI+的时钟端口 SPI_CLK; 7816 接口的复位端口 RST 被复用为 SPI+的复位端口的 SPI_RST。需要说明的是,处理模块与用户识别卡的通讯接口为 7816 或 SPI+,且 7816 与 SPI+接口复用时,协议支持 7816、SPI+接口的协商,可选地,SPI+接口支持的通讯速率高于 7816 接口,7816 接口兼容现有用户识别卡。当然,端口的形式并不限于此。将三线接口变形为四线接口或更多接口,对 SPI+接口的端口进行轻微变形,如将 SPI+接口变形为输入 SPI_Datain,输出接口 SPI_Dataout, SPI_CLK,或者输入 SPI_Datain,输出接口 SPI_Dataout, SPI_CLK, SPI_RST(增加一个接口,将其映射到 7816 的未定义端口)均可实现本申请的技术方案。

SPI+接口的各接口定义如下:

SPI_SDA: 单工双向信号接口,手机基带/应用处理器与用户识别卡间的数据通道;

SPI_CLK: 时钟信号,上升沿或下降沿作为数据的同步信号;

SPI_RST: 复位信号,高电平或低电平有效。当手机基带/应用处理器向用户识别卡发出有效的复位信号时,用户识别卡进行冷复位;当用户识别卡向手机基带/应用处理器发出有效复位信号时,手机基带/应用处理器只对支持功能扩展的 APP 进行热复位。

参照图 4 所示的时序示意图, SPI+接口的第一个时钟沿发送新数据, 第二个时钟沿则是接收端口进行数据采集。第一个时钟沿可以为上升沿或下降沿, 第二个时钟沿可以为下降沿或上升沿。可选地, 手机基带/应用处理器和用户识别卡均可作为主端发起通讯。

在本发明的上述实施例中, 用户识别卡上运行有第一子程序, 智能终端上运行有第二子程序, 用户识别卡与智能终端的通讯接口为 7816 或 SPI+, 且 7816 与 SPI+接口复用, 协议支持 7816、SPI+接口的协商, 其中 SPI+接口支持的通讯速率高于 7816 接口的通讯速率, 7816 接口兼容现有用户识别卡; 用户识别卡及其上运行的第一子程序负责安全启动、加解密及认证等安全功能, 智能终端及其上运行的第二子程序负责处理非敏感信息及人机交互功能, 智能终端及其上运行的第二子程序对用户识别卡的处理能力进行扩展。

进一步地, 结合手机基带/应用处理器和用户识别卡各自的特点, 定义出两者的软硬件接口及工作流程, 扩展了用户识别卡的应用支持能力, 并且提升了应用运行的性能与安全性。

图 5 示出了根据本发明实施例的应用程序的功能分配示意图。如图 5 所示, 用户识别卡上的 Applet 负责安全启动、加解密及认证等安全相关功能, 手机基带/应用处理器则负责非敏感数据处理、人机交互功能。手机基带/应用处理器和用户识别卡均可作为主端发起通讯。

在一个具体实施例中, 智能终端上运行一个应用程序时, 首先在用户识别卡上进行应用程序的安全启动。然后在手机基带/应用处理器上进行应用程序的非敏感信息处理、人机交互功能等。在涉及到加密、认证等安全功能时, 由用户识别卡进行相应的加密、认证。用户识别卡与手机基带/应用处理器通过通讯接口进行数据交互。当然, 本发明并不限于此。用户识别卡执行的功能可以根据具体需求设置。手机基带/应用处理器执行的功能可以根据具体需求设置。用户识别卡与手机基带/应用处理器之间功能的配合、执行流程也可以根据具体需求进行设计。

图 6 示出了根据本发明实施例的用户识别卡应用方法的方法流程图。如图 6 所示, 根据本发明实施例的用户识别卡应用方法包括以下步骤:

在步骤 S101 中，在所述用户识别卡上运行第一子程序以实现安全启动和/或加密和/或解密和/或认证；

在用户识别卡上运行第一子程序以实现安全启动和/或加密和/或解密和/或认证。可选地，用户识别卡上的第一运行单元通过第一通讯接口接收启动信号、加密信号、解密信号和认证信号中的至少一种，并基于收到的信号运行第一子程序来实现相应的安全启动、加密、解密和认证，并通过第一通讯接口将第一子程序产生的输出数据输出。

在步骤 S102 中，通过支持 7816 接口与 SPI+接口复用的通讯接口，建立所述用户识别卡与处理模块的通讯连接；

通过支持 7816 接口与 SPI+接口复用的通讯接口，建立用户识别卡与处理模块的通讯连接，以进行用户识别卡与处理模块之间的数据交互。可选地，处理模块中的第二运行单元通过第二通讯接口传输数据，用户识别卡中的第一运行单元通过第一通讯接口传输数据。

在步骤 S103 中，在所述处理模块上运行第二子程序。

在处理模块上运行第二子程序，例如通过运行第二子程序以实现应用程序的非敏感信息处理、人机交互等功能。可选地，处理模块接收用户识别卡输出的输出数据，并根据接收到的输出数据运行第二子程序。

在本发明的可选实施例中，用户识别卡应用方法还包括以下步骤：

所述处理模块以 7816 协议向所述用户识别卡发起是否支持 SPI+接口的询问；

在所述用户识别卡支持 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 SPI+接口协议进行通讯；

在所述用户识别卡不支持 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 7816 接口协议进行通讯。

具体地讲，为了扩展对原有用户识别卡的兼容，采用 7816 通讯接口与 SPI+接口协商协议进行通讯接口协商。即用户识别卡上电完成安全启动后，手机基带/应用处理器作为主端发起协议的协商，即手机基带/应用处理器与用户识别卡进行通讯协议协商。具体协商方法包括：手机基带/AP 处理器先以 7816 协议向用户识别卡发起是否支持 SPI 接口的询问；

如果用户识别卡支持 SPI+接口则回复支持，手机基带/AP 处理器与用户识别卡之间则从下一条指令开始采用 SPI+接口协议进行通讯；如果不支持，手机下一条指令仍采用 7816 接口协议进行通讯。可选地，用户识别卡上电完成安全启动后，用户识别卡作为主端发起协议的协商，即用户识别卡与手机基带/应用处理器进行通讯协议协商。具体协商方法包括：用户识别卡先以 7816 协议向手机基带/应用处理器发起是否支持 SPI+接口的询问；如果手机基带/应用处理器支持 SPI+接口则回复支持，用户识别卡与手机基带/应用处理器之间则从下一条指令开始采用 SPI+接口协议进行通讯；如果不支持，下一条指令仍采用 7816 接口协议进行通讯。

可选地，用户识别卡应用方法还包括：

所述用户识别卡向所述处理模块发送第一复位信号，所述处理模块获取所述第一复位信号后对所述应用程序进行热复位；或

所述处理模块向所述用户识别卡发送第二复位信号，所述用户识别卡获取所述第二复位信号后进行冷复位。

在本发明的可选实施例中，建立所述用户识别卡与所述处理模块的通讯连接以进行数据交互。所述用户识别卡应用方法还包括所述用户识别卡向所述处理模块发送时钟信号；或所述处理模块向所述用户识别卡发送时钟信号，其中，所述时钟信号的上升沿或下降沿作为所述数据交互的同步信号。用户识别卡和处理模块均可作为主端进行通讯。在用户识别卡作为主端时，用户识别卡向处理模块发送时钟信号。在处理模块作为主端时，处理模块向用户识别卡发送时钟信号。

应当说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、

物品或者设备中还存在另外的相同要素。

依照本发明的实施例如上文所述，这些实施例并没有详尽叙述所有的细节，也不限制该发明仅为所述的具体实施例。显然，根据以上描述，可作很多的修改和变化。本说明书选取并具体描述这些实施例，是为了更好地解释本发明的原理和实际应用，从而使所属技术领域技术人员能很好地利用本发明以及在本发明基础上的修改使用。本发明仅受权利要求书及其全部范围和等效物的限制。

权利要求书

1、一种用户识别卡，其特征在于，包括：

第一通讯接口，所述第一通讯接口支持 7816 接口与 SPI+接口复用，其中，所述 SPI+接口的通讯速率高于所述 7816 接口的通讯速率；

第一运行单元，与所述第一通讯接口相连接以传输数据，所述第一运行单元运行第一子程序来实现以下功能中的至少一种：安全启动、加密、解密和认证。

2、根据权利要求 1 所述的用户识别卡，其特征在于，所述第一通讯接口与智能终端的第二通讯接口相连接以传输数据。

3、一种智能终端，其特征在于，包括处理模块；所述处理模块包括：

第二通讯接口，所述第二通讯接口支持 7816 接口与 SPI+接口复用，其中，所述 SPI+接口的通讯速率高于所述 7816 接口的通讯速率；

第二运行单元，与所述第二通讯接口相连接以传输数据，并运行第二子程序以处理非敏感数据和/或进行人机交互实现；

4、根据权利要求 3 所述的智能终端，其特征在于，

所述第二通讯接口与用户识别卡的第一通讯接口相连接以传输数据。

5、根据权利要求 4 所述的智能终端，其特征在于，所述第一通讯接口和/或所述第二通讯接口包括：

数据端口，用于数据的输入和/或输出；

时钟端口，用于传递时钟信号，所述时钟信号的上升沿或下降沿作为数据的同步信号；以及

复位端口，用于传递复位信号，所述复位信号高电平或低电平有效，

其中，当所述处理模块向所述用户识别卡发出有效的复位信号时，所述用户识别卡进行冷复位；

当所述用户识别卡向所述处理模块发出有效的复位信号时，所述处理模块对所述第二子程序进行热复位。

6、根据权利要求 4 所述的智能终端，其特征在于，所述用户识别卡或所述处理模块均可作为主端发起通讯。

7、一种用户识别卡应用方法，其特征在于，包括：

在用户识别卡上运行第一子程序以实现安全启动和/或加密和/或解密和/或认证；通过支持 7816 接口与 SPI+接口复用的通讯接口，建立所述用户识别卡与处理模块的通讯连接；以及

在智能终端的所述处理模块上运行第二子程序。

8、根据权利要求 7 所述的用户识别卡应用方法，其特征在于，所述用户识别卡应用方法还包括：

所述用户识别卡/处理模块以 7816 协议向所述处理模块/用户识别卡发起是否支持所述 SPI+接口的询问；

在所述处理模块/用户识别卡支持所述 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 SPI+接口协议进行通讯；

在所述处理模块/用户识别卡不支持所述 SPI+接口的情况下，所述处理模块与所述用户识别卡采用 7816 接口协议进行通讯。

9、根据权利要求 7 所述的用户识别卡应用方法，其特征在于，所述用户识别卡应用方法还包括：

所述用户识别卡向所述处理模块发送第一复位信号，所述处理模块获取所述第一复位信号后对所述应用程序进行热复位；或

所述处理模块向所述用户识别卡发送第二复位信号，所述用户识别卡获取所述第二复位信号后进行冷复位。

10、根据权利要求 7 所述的用户识别卡应用方法，其特征在于，建立所述用户识别卡与所述处理模块的通讯连接以进行数据交互；

所述用户识别卡应用方法还包括：

所述用户识别卡向所述处理模块发送时钟信号；或

所述处理模块向所述用户识别卡发送时钟信号，

其中，所述时钟信号的上升沿或下降沿作为所述数据交互的同步信号。