(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 2 月 9 日 (09.02.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/020417 A1

(51) 国际专利分类号:
G06Q 20/20 (2012.01)

(21) 国际申请号: PCT/CN2015/091337

(22) 国际申请日: 2015 年 9 月 30 日 (30.09.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510466760.6 2015 年 7 月 31 日 (31.07.2015) CN

(71) 申请人: **宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: **张子敬 (ZHANG, Zijing)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 **张晴 (ZHANG, Qing)**; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: **北京友联知识产权代理事务所（普通合伙） (YOULINK INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区学清路 8 号科技财富中心 A 座 506 室尚志峰, Beijing 100192 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: METHOD FOR MOBILE PAYMENT AND WEARABLE DEVICE

(54) **发明名称** : 一种移动支付方法及可穿戴设备

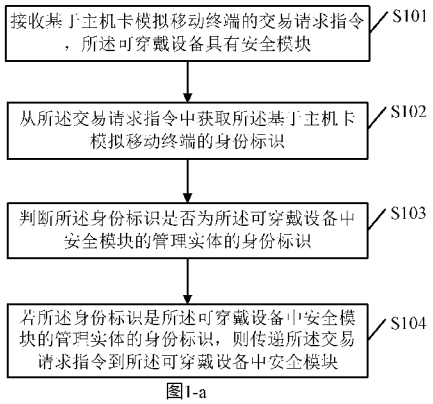


图1-a

S101 Receiving a transaction request instruction of host-based card emulation mobile terminal, the wearable device comprises security modules
S102 Obtaining an identity of the host-based card emulation mobile terminal from the transaction request instruction
S103 Judging whether the identity is the identity of a management entity of the security modules in the wearable device
S104 If the identity is the identity of a management entity of the security modules in the wearable device, transferring the transaction request instruction to the security modules in the wearable device

(57) **Abstract**: A method for mobile payment and a wearable device are provided, the method comprising: receiving a transaction request instruction of host-based card emulation mobile terminal, the wearable device comprises security modules (S101); obtaining an identity of the host-based card emulation mobile terminal from the transaction request instruction (S102); determining whether the identity is the identity of a management entity of the security modules in the wearable device (S103); if the identity is the identity of a management entity of the security modules in the wearable device, transmitting the transaction request instruction to the security modules in the wearable device (S104). By implementing the SE function of a HCE mobile terminal in the wearable device, thereby during a NFC transaction in the HCE mobile terminal, the security of the transaction could be improved, and the risk prevention is strong.

(57) **摘要**: 一种移动支付方法及可穿戴设备，所述方法，包括：接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备具有安全模块（S101）；从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识（S102）；判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识（S103）；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块（S104）。通过将 HCE 移动终端的 SE 功能在可穿戴设备中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

WO 2017/020417 A1

说 明 书

一种移动支付方法及可穿戴设备

技术领域

本发明涉及通信领域，具体涉及一种移动支付方法及可穿戴设备。

背景技术

目前，基于 Android4.4 的 NFC（Near Field Communication，近距离无线通讯技术）支付引入了一个新的开放式架构，即 HCE（Host-based Card Emulation，主机卡模拟）技术，从而在配备 NFC 功能的终端中实现卡模块后，HCE 移动终端不需要提供物理 SE（Security Elements，安全模块），使得 NFC 的应用更加简单与灵活。

但是 HCE 技术只是模拟了 NFC 和 SE 通信的协议和实现，也即以虚拟 SE 的方式完成 NFC 业务的安全保证，并没有实现 SE。现有基于 HCE 技术的 SE 解决方案，可以是通过基于主机软件模拟或者基于云端服务器来实现，但是基于主机软件模拟虽然简单但是安全性很差，比如在系统被 Root（获取超级用户权限）的情况下没有任何防范能力，所以需要一种安全性强的 SE 方案。

发明内容

本发明实施例提供了一种移动支付方法及可穿戴设备，以期可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性。

本发明实施例第一方面提供一种移动支付方法，应用于可穿戴设备，所述可穿戴设备具有安全模块，包括:

接收基于主机卡模拟移动终端的交易请求指令;

从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

本发明实施例第二方面提供一种可穿戴设备，所述可穿戴设备具有安全模块，包括：

接收模块，用于接收基于主机卡模拟移动终端的交易请求指令；

第一获取模块，用于从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识；

第一判断模块，用于判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；

传递模块，用于若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

可以看出，在本发明实施例提供的技术方案中，接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备具有安全模块；再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识；然后再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1-a 是本发明第一实施例提供的一种移动支付方法的流程示意图；

图 1-b 是本发明第五实施例提供的移动支付系统的示意图；

图 2-a 是本发明第二实施例提供的一种移动支付方法的流程示意图；

图 2-b 是本发明第二实施例提供的一种移动支付方法的交互流程示意图；

图 3-a 是本发明第三实施例提供的一种移动支付方法的流程示意图；

图 3-b 是本发明第三实施例提供的一种移动支付方法的流程示意图；

图 4 是本发明第四实施例提供的一种可穿戴设备的结构示意图；

图 5 是本发明第五实施例提供的一种可穿戴设备的结构示意图;

图 6 是本发明第六实施例提供一种可穿戴设备的结构示意图。

具体实施方式

本发明实施例提供了一种移动支付方法及可穿戴设备，以期可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性。

为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”和“第三”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

本发明实施例的一种移动支付方法，一种移动支付方法包括：接收基于主机卡模拟移动终端的交易请求指令；从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识；判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则响应所述交易请求与外部终端进行交易通信。

首先参见图 1-a 和图 1-b，图 1-a 是本发明第一实施例提供的一种移动支付方法的流程示意图，图 1-b 是本发明第五实施例提供的移动支付系统的示意图。其中，如图 1 所示，本发明第一实施例提供的一种移动支付方法可以包括:

S101、接收基于主机卡模拟移动终端的交易请求指令。

如图 1-b 所示，其中，HCE 移动终端为配备有 NFC 功能、HCE 功能以及对应的如蓝牙、无线网络等无线通信模块的移动终端，可以为手机，平板电脑等;但该 HCE 移动终端没有 SE 模块，其实现 SE 功能的模块放置在可穿戴设备上，也即 HCE 移动终端在进行非接触支付时，HCE 移动终端的 NFC 控制器会将支

付信息路由到可穿戴设备的 SE 模块来完成移动支付，该 SE 模块可以是通过硬件芯片来实现，也可以通过软件模拟实现。其中，可穿戴设备是指具有 SE 模块并支持对应的如蓝牙、无线网络等无线通信模块的可穿戴设备，可以为智能手环、智能手表以及戒指等，从而利用 HCE 移动终端与外部受理设备进行移动支付时，需要通过可穿戴设备上的 SE 模块来完成。其中，外部受理设备是指具有读写器功能的设备，如读卡器、POS（point of sales terminal，销售点情报管理系统）机等。

其中，HCE 移动终端和可穿戴设备之间通过蓝牙、无线网络等无线通信模块实现通信; HCE 移动终端利用 NFC 完成与外部受理设备之间的非接触移动支付通信。

其中，交易请求指令为 HCE 移动终端发送给可穿戴设备的用于请求支付交易的指令，该交易指令包括 HCE 移动终端的身份识别信息以及交易类型等。

可选地，在本发明一些可能的实施方式中，该交易请求指令还可以包括与交易相关的其它非敏感信息。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端靠近外部受理 POS 机时，HCE 移动终端的 NFC 控制器就会将交易路由到可穿戴设备的 SE 模块，HCE 移动终端向可穿戴设备发送用于请求支付交易的指令，从而可穿戴设备将接收到基于主机卡模拟移动终端的交易请求指令。

S102、从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识。

其中，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个。

其中，HCE 移动终端的身份标识为 HCE 移动终端的唯一身份标识，可以用该身份标识唯一确定该 HCE 移动终端。

可以理解，由于 HCE 移动终端的移动设备国际识别码（IMEI）、物理地址（MAC 地址）或近距离无线通讯芯片序列号（NFC 芯片 ID）中的任一可均可识别 HCE 移动终端，所以可通过 IMEI、MAC 地址或 NFC 芯片 ID 中的任一个或几个来识别 HCE 移动终端。

S103、判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识。

其中，可穿戴设备中 SE 模块的管理实体是指预先由用户设定的、对可穿戴设备中 SE 模块具有管理权限的管理实体，该管理实体可以是 HCE 移动终端。

可选地，在本发明的一些可能的实施方式中，该管理实体可以是一个。

可选地，在本发明的另一些可能的实施方式中，该管理实体可以是多个。

可以理解，由于身份标识可以唯一标识 HCE 移动终端，所以可以利用身份标识来判断该 HCE 移动终端是否为可穿戴设备中 SE 模块的管理实体。

S104、若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

举例说明，在本发明的一些可能的实施方式中，当 HCE 移动终端利用其自身的 NFC 功能与外部受理 POS 机进行支付交易时，NFC 控制器通过上述身份认证请求将交易路由到可穿戴设备中 SE 模块中，当利用 HCE 移动终端的身份标识通过身份认证后，可穿戴设备接收该交易请求指令，并将该交易请求指令传递至可穿戴设备中的安全模块，由可穿戴设备中安全模块实现 HCE 移动终端的 SE 功能，从而可以实现 HCE 移动终端和外部受理 POS 机之间的移动支付交易。

可选地，在本发明的一些可能的实施方式中，在移动支付的过程中，HCE 移动终端和可穿戴设备中 SE 模块之间通过蓝牙或 Wi-Fi 等无线通信方式完成敏感信息的读取。

可以看出，本实施例的方案中，可穿戴设备接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备具有安全模块；再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

可选地，在本发明的一些可能的实施方式中，所述方法还包括:

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

可以理解，如果 HEC 移动终端的身份标识不是由用户预设的可穿戴设备的管理实体的身份标识，为了安全起见，将禁止该 HCE 移动终端对可穿戴设备中 SE 模块进行访问。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户交易指令请求。

可选地，在本发明的一些可能的实施方式中，所述方法还包括:

接收用户的配对指令，所述配对指令用于为所述可穿戴设备选择配对的基于主机卡模拟移动终端;

确定所述基于主机卡模拟移动终端为所述可穿戴设备的管理实体，其中，所述可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

其中，配对指令用于用户在可穿戴设备上选择并设定与可穿戴设备进行配对连接的 HCE 移动终端，即设定允许访问可穿戴设备中 SE 模块的 HCE 移动终端。

可以理解，通过用户的配对指令，可以选择与可穿戴设备进行绑定的 HCE 移动终端，通过将 HCE 移动终端与可穿戴设备之间进行绑定，也即实现用户选择可穿戴设备中 SE 模块的管理实体，从而只允许设定的管理实体访问可穿戴设备中 SE 模块。在后续 HCE 移动终端向可穿戴设备发送交易请求指令时，只允许与可穿戴设备绑定的 HCE 移动终端做为可穿戴设备的管理实体传递交易指令给可穿戴设备中 SE 模块，增加交易的安全性。

可选地，在本发明的一些可能的实施方式中，该身份标识可以是 HCE 移动终端的唯一身份标识，如 IMEI、MAC 地址以及 NFC 芯片 ID 等。

可选地，在本发明的一些可能的实施方式中，所述传递所述交易请求到所述可穿戴设备中安全模块之前，所述方法还包括:

获取所述基于主机卡模拟移动终端和所述可穿戴设备之间的信号强度;

判断所述信号强度是否大于或等于预设信号强度;

若所述信号强度大于或等于所述预设信号强度，则触发传递所述交易请求指令到所述可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

可以理解，为了保证 HCE 移动终端和可穿戴设备之间的正常通信，需要预设两者之间的预设信号强度，从而确保 HCE 移动终端和可穿戴设备之间的无线信号强度，只有当两者之间信号强度达到预设信号强度时才传递交易请求指令至可穿戴设备中 SE 模块，HCE 移动终端也才能进一步完成 NFC 移动支付交易。而 HCE 移动终端和可穿戴设备之间是通过蓝牙或无线 Wi-Fi 进行通信的，所以两者之间的距离越近则通信信号越好，从而可在 HCE 移动终端和可穿戴设备之间的信号强度未达到预设信号强度时，则提醒用户两者距离太远，用户可以通过移动 HCE 终端或可穿戴设备，减少两者之间的距离，确保两者之间的信号强度，保证通信安全，从而保证交易的安全性，并且由于此种方式使得信号强度可控，所以使得该 NFC 交易不受支付环境的影响，用户体验更好。

可选地，在本发明的一些可能的实施方式中，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

可选地，在本发明的一些可能的实施方式中，预设信号强度可由用户设定，由用户在 HCE 移动终端和可穿戴设备之间选择一个合适的距离后，可穿戴设备自动检测此时的信号强度，并加上允许的干扰范围作为最后可进行交易的预设信号强度。

可选地，在本发明的另一些可能的实施方式中，预设信号强度可由可穿戴设备自学习完成，具体地，可穿戴设备自动统计每次交易时 HCE 移动终端和可穿戴设备之间无线通信信号强度，查找一段时间交易信号强度趋于较平稳范围，也即波动较小时取较低值并加上干扰范围作为可进行交易的预设信号强度。

可选地，在本发明的一些可能的实施方式中，所述方法还包括:

对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全

模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

可选地，在本发明的一些可能的实施方式中，若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理，并提醒用户。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端上的应用程序对可穿戴设备中 SE 模块卡片应用的访问控制包括对 SE 模块上卡片应用数据的下载、安装、删除、数据个人化等相关操作，也即可以对 SE 模块上卡片应用进行初始化以及中间对数据的修改、删除或增加等操作。

举例说明，在本发明一些可能的实施方式中，可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用的初始化，如第一次使用中国银行进行移动支付时，由于可穿戴设备中 SE 模块中并没有中国银行对应的卡片应用，所以需要对可穿戴设备中 SE 模块下载卡片应用数据，从而对中国银行对应的卡片应用进行初始化。

再举例说明，在本发明的一些可能的实施方式中，可以是 HCE 移动中端上的中国银行 APP 对可穿戴设备中 SE 模块卡片应用上面关于敏感信息的更改，如当用户在 APP 上进行余额转帐时，则 APP 对其相关 SE 模块中的中国银行的卡片应用上面的余额信息进行更改。

再举例说明，在本发明的另一些可能的实施方式中，还可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用中帐户的更改，如当增加或者删除帐户时，由于帐户等敏感信息存放在可穿戴设备中 SE 模块中，所以通过 APP 对可穿戴设备中 SE 模块卡片应用中的帐户信息进行更改。

可以理解，由于 HCE 移动终端上 APP 对可穿戴设备中 SE 模块卡片应用的访问控制为对敏感数据的访问控制，所以需要通过可穿戴设备对 HCE 移动终端上的应用程序进行访问控制鉴权，只有通过访问控制鉴权的 APP 才可以访问可穿戴设备中 SE 模块卡片应用，从而保证控制规则的安全性。

可选地，在本发明的一些可能的实施方式中，所述对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权之前，所述方法还包括:

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理请求指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则触发所述可穿戴设备对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权的步骤。

其中，身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个。

其中，该管理请求指令用于 HCE 移动终端请求对可穿戴设备进行访问控制等管理。

可以理解，由于可穿戴设备对访问其 SE 模块的管理实体进行设定，所以需要通过 HCE 移动终端的身份标识确定其是否为可穿戴设备中 SE 模块的管理实体，如果是，才允许该 HCE 移动终端管理可穿戴设备中 SE 模块，继而再对 HCE 移动终端上的 APP 访问可穿戴设备中 SE 模块卡片应用进行进一步访问控制鉴权，从而使得访问的安全性更高。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户的管理请求指令。

为了便于更好理解和实施本发明实施例的上述方案，下面结合一些具体的应用场景进行举例说明。

请参见图 2-a 和图 2-b，图 2-a 是本发明第二实施例提供的一种移动支付方法的流程示意图，图 2-b 是本发明第二实施例提供的一种移动支付方法的交互流程示意图，其中，如图 2 所示，本发明第二实施例提供的一种移动支付方法可以包括:

S201、接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端。

其中，HCE 移动终端为配备有 NFC 功能、HCE 功能以及对应的如蓝牙、无线网络等无线通信模块的移动终端，可以为手机，平板电脑等；但该 HCE 移动终端没有 SE 模块，其实现 SE 功能的模块放置在可穿戴设备上，也即 HCE 移动终端在进行非接触支付时，HCE 移动终端的 NFC 控制器会将支付信息路由到可穿戴设备的 SE 模块来完成移动支付，该 SE 模块可以是通过硬件芯片来实现，也可以通过软件模拟实现。其中，可穿戴设备是指具有 SE 模块并支持对应的如蓝牙、无线网络等无线通信模块的可穿戴设备，可以为智能手环、智能手表以及戒指等，从而利用 HCE 移动终端与外部受理设备进行移动支付时，需要通过可穿戴设备上的 SE 模块来完成。其中，外部受理设备是指具有读写器功能的设备，如读卡器、POS（point of sales terminal，销售点情报管理系统）机等。

其中，HCE 移动终端和可穿戴设备之间通过蓝牙、无线网络等无线通信模块实现通信；HCE 移动终端利用 NFC 完成与外部受理设备之间的非接触移动支付通信。

其中，配对指令用于用户在可穿戴设备上选择并设定与可穿戴设备进行配对连接的 HCE 移动终端，即设定允许访问可穿戴设备中 SE 模块的 HCE 移动终端。

可以理解，通过用户的配对指令，可以选择与可穿戴设备进行绑定的 HCE 移动终端，通过将 HCE 移动终端与可穿戴设备之间进行绑定，从而只允许设定的管理实体访问可穿戴设备中 SE 模块。在后续 HCE 移动终端向可穿戴设备发送交易请求指令时，只允许与可穿戴设备绑定的 HCE 移动终端做为可穿戴设备的管理实体传递交易指令给可穿戴设备中 SE 模块，增加交易的安全性。

S202、确定基于主机卡模拟移动终端为可穿戴设备的管理实体。

其中，可穿戴设备的管理实体通过基于主机卡模块移动终端的身份标识进行认证。

其中，可穿戴设备中 SE 模块的管理实体是指预先由用户设定的、对可穿戴设备中 SE 模块具有管理权限的管理实体，该管理实体可以是 HCE 移动终端。

可选地，在本发明的一些可能的实施方式中，该管理实体可以是一个。

可选地，在本发明的另一些可能的实施方式中，该管理实体可以是多个。

可以理解，由于身份标识可以唯一标识 HCE 移动终端，所以可以利用身份标识来判断该 HCE 移动终端是否为可穿戴设备中 SE 模块的管理实体。

可以理解，通过HCE移动终端的身份标识确定可穿戴设备的管理实体后，即实现用户选择可穿戴设备中SE模块的管理实体，从而只允许设定的管理实体访问可穿戴设备中SE模块。在后续HCE移动终端向可穿戴设备发送交易请求指令时，只允许与可穿戴设备绑定的HCE移动终端做为可穿戴设备的管理实体传递交易指令给可穿戴设备中SE模块，增加交易的安全性。

S203、接收基于主机卡模拟移动终端的交易请求指令。

其中，交易请求指令为HCE移动终端发送给可穿戴设备的用于请求支付交易的指令，该交易指令包括HCE移动终端的身份识别信息以及交易类型等。

可选地，在本发明一些可能的实施方式中，该交易请求指令还可以包括与交易相关的其它非敏感信息。

可选地，在本发明的一些可能的实施方式中，HCE移动终端靠近外部受理POS机时，HCE移动终端的NFC控制器就会将交易路由到可穿戴设备的SE模块，HCE移动终端向可穿戴设备发送用于请求支付交易的指令，从而可穿戴设备将接收到基于主机卡模拟移动终端的交易请求指令。

可选地，在本发明的一些可能的实施方式中，可穿戴设备接收HCE移动终端的交易请求指令之前，所述方法还包括:

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则所述可穿戴设备对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

可选地，在本发明的一些可能的实施方式中，该身份标识可以是HCE移动终端的唯一身份标识，如IMEI、MAC地址以及NFC芯片ID等。

可选地，在本发明的一些可能的实施方式中，若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理，并提醒用户。

可选地，在本发明的一些可能的实施方式中，HCE移动终端上的应用程序对可穿戴设备中SE模块卡片应用的访问控制包括对SE模块上卡片应用数据的下载、安装、删除、数据个人化等相关操作，也即可以对SE模块上卡片应用进行初始化以及中间对数据的修改、删除或增加等操作。

举例说明，在本发明第二实施例中，可以是HCE移动终端上的中国银行APP（Application，应用程序）对可穿戴设备中SE模块卡片应用的初始化，如第一次使用中国银行进行移动支付时，由于可穿戴设备中SE模块中并没有中国银行对应的卡片应用，所以需要对可穿戴设备中SE模块下载卡片应用数据，从而对中国银行对应的卡片应用进行初始化。

可以理解，通过上述步骤对可穿戴设备中SE模块的卡片应用进行初始化，从而才能进行后续的NFC交易，并且通过上述步骤，实现对HCE移动终端的身份认证以及HCE移动终端上应用程序的访问控制鉴权，保证初始化工作的安全性，从而保证了后续交易的安全性。

S204、从交易请求指令中获取基于主机卡模拟移动终端的身份标识。

其中，身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个。

其中，HCE移动终端的身份标识为HCE移动终端的唯一身份标识，可以用该身份标识唯一确定该HCE移动终端。

可以理解，由于HCE移动终端的移动设备国际识别码（IMEI）、物理地址（MAC地址）或近距离无线通讯芯片序列号（NFC芯片ID）中的任一可均可识别HCE移动终端，所以可通过IMEI、MAC地址或NFC芯片ID中的任一个或几个来识别HCE移动终端。

S205、判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识。

可以理解，由于在步骤S201和S202设定了可穿戴设备的管理实体，所以利用上述设定的管理实体的身体标识来判断该HCE移动终端是否为可穿戴设备

中 SE 模块的管理实体，通过对 HCE 移动终端的身份进行认证，提高安全性。

S206、若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则获取基于主机卡模拟移动终端和可穿戴设备之间的信号强度。

可选地，在本发明的一些可能的实施方式中，所述方法还包括:

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户交易指令请求。

可以理解，如果 HEC 移动终端的身份标识不是由用户预设的可穿戴设备的管理实体的身份标识，为了安全起见，将禁止该 HCE 移动终端对可穿戴设备中 SE 模块进行访问。

可选地，在本发明的一些可能的实施方式中，在移动支付的过程中，HCE 移动终端和可穿戴设备中 SE 模块之间通过蓝牙或 Wi-Fi 等无线通信方式完成敏感信息的读取，所以为了保证通信的可靠性，需要进一步确定 HCE 移动终端和可穿戴设备中 SE 模块的信号强度是否足够。

S207、判断信号强度是否大于或等于预设信号强度。

可选地，在本发明的一些可能的实施方式中，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

可选地，在本发明的一些可能的实施方式中，预设信号强度可由用户设定，由用户在 HCE 移动终端和可穿戴设备之间选择一个合适的距离后，可穿戴设备自动检测此时的信号强度，并加上允许的干扰范围作为最后可进行交易的预设信号强度。

可选地，在本发明的另一些可能的实施方式中，预设信号强度可由可穿戴设备自学习完成，具体地，可穿戴设备自动统计每次交易时 HCE 移动终端和可穿戴设备之间无线通信信号强度，查找一段时间交易信号强度趋于较平稳范围，

也即波动较小时取较低值并加上干扰范围作为可进行交易的预设信号强度。

可以理解，为了保证 HCE 移动终端和可穿戴设备之间的正常通信，需要预设两者之间的预设信号强度，从而确保 HCE 移动终端和可穿戴设备之间的无线信号强度，只有当两者之间信号强度达到预设信号强度时才传递交易请求指令至可穿戴设备中 SE 模块，HCE 移动终端也才能进一步完成 NFC 移动支付交易。而 HCE 移动终端和可穿戴设备之间是通过蓝牙或无线 Wi-Fi 进行通信的，所以两者之间的距离越近则通信信号越好，从而可在 HCE 移动终端和可穿戴设备之间的信号强度未达到预设信号强度时，则提醒用户两者距离太远，用户可以通过移动 HCE 终端或可穿戴设备，减少两者之间的距离，确保两者之间的信号强度，保证通信安全，从而保证交易的安全性，并且由于此种方式使得信号强度可控，所以使得该 NFC 交易不受支付环境的影响，用户体验更好。

S208、若信号强度大于或等于所述预设信号强度，则触发传递交易请求指令到可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

可以理解，为了保证 HCE 移动终端和可穿戴设备之间的正常通信，需要预设两者之间的预设信号强度，从而确保 HCE 移动终端和可穿戴设备之间的无线信号强度，只有当两者之间信号强度达到预设信号强度时才传递交易请求指令至可穿戴设备中 SE 模块，HCE 移动终端也才能进一步完成 NFC 移动支付交易。而 HCE 移动终端和可穿戴设备之间是通过蓝牙或无线 Wi-Fi 进行通信的，所以两者之间的距离越近则通信信号越好，从而可在 HCE 移动终端和可穿戴设备之间的信号强度未达到预设信号强度时，则提醒用户两者距离太远，用户可以通过移动 HCE 终端或可穿戴设备，减少两者之间的距离，确保两者之间的信号强度，保证通信安全，从而保证交易的安全性，并且由于此种方式使得信号强度可控，所以使得该 NFC 交易不受支付环境的影响，用户体验更好。

S209、传递交易请求指令到可穿戴设备中安全模块。

举例说明，在本发明的一些可能的实施方式中，当 HCE 移动终端利用其自身的 NFC 功能与外部受理 POS 机进行支付交易时，NFC 控制器通过上述身份认证请求将交易路由到可穿戴设备中 SE 模块中，当利用 HCE 移动终端的身份标识通过身份认证后，可穿戴设备接收该交易请求指令，并将该交易请求指令

传递至可穿戴设备中的安全模块，由可穿戴设备中安全模块实现 HCE 移动终端的 SE 功能，从而可以实现 HCE 移动终端和外部受理 POS 机之间的移动支付交易。

可以看出，本实施例的方案中，可穿戴设备接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备具有安全模块；再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

请参见图 3-a 和图 3-b，图 3-a 是本发明第三实施例提供的一种移动支付方法的流程示意图，图 3-b 是本发明第三实施例提供的一种移动支付方法的流程示意图。其中，如图 3 所示，本发明第三实施例提供的一种移动支付方法可以包括：

S301、接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端。

S302、确定基于主机卡模拟移动终端为可穿戴设备的管理实体。

其中，可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

其中，步骤 S301 和步骤 S302 与步骤 S201 和步骤 S202 相同。

S303、接收基于主机卡模拟移动终端的管理请求指令。

其中，该管理请求指令用于 HCE 移动终端请求对可穿戴设备进行访问控制等管理。

S304、从管理请求指令中获取基于主机卡模拟移动终端的身份标识。

其中，身份标识包括主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个。

S305、判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识。

S306、若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则可

穿戴设备对基于主机卡模拟移动终端上的应用程序进行访问控制鉴权。

其中，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权。

可以理解，由于可穿戴设备对访问其 SE 模块的管理实体进行设定，所以需要通过 HCE 移动终端的身份标识确定其是否为可穿戴设备中 SE 模块的管理实体，如果是，才允许该 HCE 移动终端管理可穿戴设备中 SE 模块，继而再对 HCE 移动终端上的 APP 访问可穿戴设备中 SE 模块卡片应用进行进一步访问控制鉴权，从而使得访问的安全性更高。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户的管理请求指令。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端上的应用程序对可穿戴设备中 SE 模块卡片应用的访问控制包括对 SE 模块上卡片应用数据的下载、安装、删除、数据个人化等相关操作，也即可以对 SE 模块上卡片应用进行初始化以及中间对数据的修改、删除或增加等操作。

S307、若访问控制鉴权通过，则允许应用程序对可穿戴设备中安全模块卡片应用进行管理。

S308、若访问控制鉴权未通过，则禁止应用程序对可穿戴设备中安全模块卡片应用进行管理。

可以理解，步骤 S307 和步骤 S308 没有特定的执行先后顺序。

举例说明，在本发明一些可能的实施方式中，可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用的初始化，如第一次使用中国银行进行移动支付时，由于可穿戴设备中 SE 模块中并没有中国银行对应的卡片应用，所以需要对可穿戴设备中 SE 模块下载卡片应用数据，从而对中国银行对应的卡片应用进行初始化。

再举例说明，在本发明的一些可能的实施方式中，可以是 HCE 移动中端上的中国银行 APP 对可穿戴设备中 SE 模块卡片应用上面关于敏感信息的更改，

如当用户在 APP 上进行余额转帐时，则 APP 对其相关 SE 模块中的中国银行的卡片应用上面的余额信息进行更改。

再举例说明，在本发明的另一些可能的实施方式中，还可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用中帐户的更改，如当增加或者删除帐户时，由于帐户等敏感信息存放在可穿戴设备中 SE 模块中，所以通过 APP 对可穿戴设备中 SE 模块卡片应用中的帐户信息进行更改。

可以理解，由于 HCE 移动终端上 APP 对可穿戴设备中 SE 模块卡片应用的访问控制为对敏感数据的访问控制，所以需要通过可穿戴设备对 HCE 移动终端上的应用程序进行访问控制鉴权，只有通过访问控制鉴权的 APP 才可以访问可穿戴设备中 SE 模块卡片应用，从而保证控制规则的安全性。

可选地，在本发明的一些可能实施方式中，执行完 S301 至 S308 的步骤后，可进一步执行 S203 至 S209 的步骤，从而进一步完成 HCE 移动终端通过可穿戴设备中 SE 模块的 NFC 支付交易。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端中 APP 对可穿戴设备中 SE 模块卡片应用的管理可以在支付交易之前，如需要对可穿戴设备中 SE 模块卡片应用进行初始化，才能进行进一步地支付交易。

可选地，在本发明的另一些可能的实施方式中，HCE 移动终端中 APP 对可穿戴设备中 SE 模块卡片应用的管理可以在支付交易之中以及之后，如需要对可穿戴设备中 SE 模块卡片应用进行数据删除及更改等，例如，支付交易完成后，用户又想通过中国银行 APP 转帐，从而可利用 HCE 移动终端中 APP 对可穿戴设备中 SE 模块卡片应用的访问控制管理对 SE 模块卡片应用中的数据进行更改。

可以看出，本实施例的方案中，可穿戴设备接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备具有安全模块；再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备中实现，从而可以在 HCE 移动终端进行 NFC

交易的时候提高交易的安全性，风险防范性强。

本发明实施例还提供一种可穿戴设备，该可穿戴设备包括:

接收模块，用于接收基于主机卡模拟移动终端的交易请求指令;

第一获取模块，用于从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识;

第二判断模块，用于判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

传递模块，用于若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

具体的，请参见图 4，图 4 是本发明第四实施例提供的一种可穿戴设备的结构示意图，其中，如图 4 所示，本发明第四实施例提供的一种可穿戴设备 400 可以包括:

接收模块 410、第一获取模块 420、第一判断模块 430 和传递模块 440。

其中，接收模块 410，用于接收基于主机卡模拟移动终端的交易请求指令。

如图 1-b 所示，其中，HCE 移动终端为配备有 NFC 功能、HCE 功能以及对应的如蓝牙、无线网络等无线通信模块的移动终端，可以为手机，平板电脑等;但该 HCE 移动终端没有 SE 模块，其实现 SE 功能的模块放置在可穿戴设备上，也即 HCE 移动终端在进行非接触支付时，HCE 移动终端的 NFC 控制器会将支付信息路由到可穿戴设备的 SE 模块来完成移动支付，该 SE 模块可以是通过硬件芯片来实现，也可以通过软件模拟实现。其中，可穿戴设备是指具有 SE 模块并支持对应的如蓝牙、无线网络等无线通信模块的可穿戴设备，可以为智能手环、智能手表以及戒指等，从而利用 HCE 移动终端与外部受理设备进行移动支付时，需要通过可穿戴设备上的 SE 模块来完成。其中，外部受理设备是指具有读写器功能的设备，如读卡器、POS（point of sales terminal，销售点情报管理系统）机等。

其中，HCE 移动终端和可穿戴设备之间通过蓝牙、无线网络等无线通信模块实现通信; HCE 移动终端利用 NFC 完成与外部受理设备之间的非接触移动支付通信。

其中，交易请求指令为 HCE 移动终端发送给可穿戴设备的用于请求支付交易的指令，该交易指令包括 HCE 移动终端的身份识别信息以及交易类型等。

可选地，在本发明一些可能的实施方式中，该交易请求指令还可以包括与交易相关的其它非敏感信息。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端靠近外部受理 POS 机时，HCE 移动终端的 NFC 控制器就会将交易路由到可穿戴设备的 SE 模块，HCE 移动终端向可穿戴设备发送用于请求支付交易的指令，从而可穿戴设备将接收到基于主机卡模拟移动终端的交易请求指令。

第一获取模块 420，用于从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识。

其中，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个。

其中，HCE 移动终端的身份标识为 HCE 移动终端的唯一身份标识，可以用该身份标识唯一确定该 HCE 移动终端。

可以理解，由于 HCE 移动终端的移动设备国际识别码（IMEI）、物理地址（MAC 地址）或近距离无线通讯芯片序列号（NFC 芯片 ID）中的任一可均可识别 HCE 移动终端，所以可通过 IMEI、MAC 地址或 NFC 芯片 ID 中的任一个或几个来识别 HCE 移动终端。

第一判断模块 430，用于判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识。

其中，可穿戴设备中 SE 模块的管理实体是指预先由用户设定的、对可穿戴设备中 SE 模块具有管理权限的管理实体，该管理实体可以是 HCE 移动终端。

可选地，在本发明的一些可能的实施方式中，该管理实体可以是一个。

可选地，在本发明的另一些可能的实施方式中，该管理实体可以是多个。

可以理解，由于身份标识可以唯一标识 HCE 移动终端，所以可以利用身份标识来判断该 HCE 移动终端是否为可穿戴设备中 SE 模块的管理实体。

传递模块 440，用于若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

举例说明，在本发明的一些可能的实施方式中，当 HCE 移动终端利用其自身的 NFC 功能与外部受理 POS 机进行支付交易时，NFC 控制器通过上述身份认证请求将交易路由到可穿戴设备中 SE 模块中，当利用 HCE 移动终端的身份标识通过身份认证后，可穿戴设备接收该交易请求指令，并将该交易请求指令

传递至可穿戴设备中的安全模块，由可穿戴设备中安全模块实现 HCE 移动终端的 SE 功能，从而可以实现 HCE 移动终端和外部受理 POS 机之间的移动支付交易。

可选地，在本发明的一些可能的实施方式中，在移动支付的过程中，HCE 移动终端和可穿戴设备中 SE 模块之间通过蓝牙或 Wi-Fi 等无线通信方式完成敏感信息的读取。

可以理解的是，本实施例的可穿戴设备 400 的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

可以看出，本实施例的方案中，可穿戴设备 400 接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备 400 具有安全模块；可穿戴设备 400 再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后可穿戴设备 400 再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则可穿戴设备 400 传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备 400 中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

请参见图 5，图 5 是本发明第五实施例提供的一种可穿戴设备的结构示意图，其中，如图 5 所示，本发明第五实施例提供的一种可穿戴设备 500 可以包括：

接收模块 510、第一获取模块 520、第一判断模块 530 和传递模块 540。

其中，接收模块 510、第一获取模块 520、第一判断模块 530 和传递模块 540 的部分功能和本发明第四实施例的接收模块 410、第一获取模块 420、第一判断模块 430 和传递模块 440 功能一样，与本发明第四实施例相同的功能在此不再赘述，另外，本发明第五实施例的可穿戴设备 500 在本发明第四实施例的可穿戴设备 400 的基础上有所补充，详述如下。

可选地，在本发明的一些可能的实施方式中，所述第一判断模块 520 还用于：

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，

则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

可以理解，如果 HEC 移动终端的身份标识不是由用户预设的可穿戴设备的管理实体的身份标识，为了安全起见，将禁止该 HCE 移动终端对可穿戴设备中 SE 模块进行访问。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户交易指令请求。

可选地，在本发明的一些可能的实施方式中，所述可穿戴设备还包括:

配对模块 550，用于

接收用户的配对指令，所述配对指令用于为所述可穿戴设备选择配对的基于主机卡模拟移动终端;

确定所述基于主机卡模拟移动终端为所述可穿戴设备的管理实体，其中，所述可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

其中，配对指令用于用户在可穿戴设备上选择并设定与可穿戴设备进行配对连接的 HCE 移动终端，即设定允许访问可穿戴设备中 SE 模块的 HCE 移动终端。

可以理解，通过用户的配对指令，可以选择与可穿戴设备进行绑定的 HCE 移动终端，通过将 HCE 移动终端与可穿戴设备之间进行绑定，也即实现用户选择可穿戴设备中 SE 模块的管理实体，从而只允许设定的管理实体访问可穿戴设备中 SE 模块。在后续 HCE 移动终端向可穿戴设备发送交易请求指令时，只允许与可穿戴设备绑定的 HCE 移动终端做为可穿戴设备的管理实体传递交易指令给可穿戴设备中 SE 模块，增加交易的安全性。

可选地，在本发明的一些可能的实施方式中，该身份标识可以是 HCE 移动终端的唯一身份标识，如 IMEI、MAC 地址以及 NFC 芯片 ID 等。

可选地，在本发明的一些可能的实施方式中，所述可穿戴设备 500 还包括:

第二获取模块 560，用于获取所述基于主机卡模拟移动终端和所述可穿戴设

备之间的信号强度;

第二判断模块 570，用于判断所述信号强度是否大于或等于预设信号强度;

提示模块 580，用于若所述信号强度大于或等于所述预设信号强度，则触发所述传递模块传递所述交易请求指令到所述可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

可以理解，为了保证 HCE 移动终端和可穿戴设备之间的正常通信，需要预设两者之间的预设信号强度，从而确保 HCE 移动终端和可穿戴设备之间的无线信号强度，只有当两者之间信号强度达到预设信号强度时才传递交易请求指令至可穿戴设备中 SE 模块，HCE 移动终端也才能进一步完成 NFC 移动支付交易。而 HCE 移动终端和可穿戴设备之间是通过蓝牙或无线 Wi-Fi 进行通信的，所以两者之间的距离越近则通信信号越好，从而可在 HCE 移动终端和可穿戴设备之间的信号强度未达到预设信号强度时，则提醒用户两者距离太远，用户可以通过移动 HCE 终端或可穿戴设备，减少两者之间的距离，确保两者之间的信号强度，保证通信安全，从而保证交易的安全性，并且由于此种方式使得信号强度可控，所以使得该 NFC 交易不受支付环境的影响，用户体验更好。

可选地，在本发明的一些可能的实施方式中，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

可选地，在本发明的一些可能的实施方式中，预设信号强度可由用户设定，由用户在 HCE 移动终端和可穿戴设备之间选择一个合适的距离后，可穿戴设备自动检测此时的信号强度，并加上允许的干扰范围作为最后可进行交易的预设信号强度。

可选地，在本发明的另一些可能的实施方式中，预设信号强度可由可穿戴设备自学习完成，具体地，可穿戴设备自动统计每次交易时 HCE 移动终端和可穿戴设备之间无线通信信号强度，查找一段时间交易信号强度趋于较平稳范围，也即波动较小时取较低值并加上干扰范围作为可进行交易的预设信号强度。

可选地，在本发明的一些可能的实施方式中，所述可穿戴设备还包括:

第一管理模块 590，用于

对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访

问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

可选地，在本发明的一些可能的实施方式中，若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理，并提醒用户。

可选地，在本发明的一些可能的实施方式中，HCE 移动终端上的应用程序对可穿戴设备中 SE 模块卡片应用的访问控制包括对 SE 模块上卡片应用数据的下载、安装、删除、数据个人化等相关操作，也即可以对 SE 模块上卡片应用进行初始化以及中间对数据的修改、删除或增加等操作。

举例说明，在本发明一些可能的实施方式中，可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用的初始化，如第一次使用中国银行进行移动支付时，由于可穿戴设备中 SE 模块中并没有中国银行对应的卡片应用，所以需要对可穿戴设备中 SE 模块下载卡片应用数据，从而对中国银行对应的卡片应用进行初始化。

再举例说明，在本发明的一些可能的实施方式中，可以是 HCE 移动中端上的中国银行 APP 对可穿戴设备中 SE 模块卡片应用上面关于敏感信息的更改，如当用户在 APP 上进行余额转帐时，则 APP 对其相关 SE 模块中的中国银行的卡片应用上面的余额信息进行更改。

再举例说明，在本发明的另一些可能的实施方式中，还可以是 HCE 移动终端上的中国银行 APP（Application，应用程序）对可穿戴设备中 SE 模块卡片应用中帐户的更改，如当增加或者删除帐户时，由于帐户等敏感信息存放在可穿戴设备中 SE 模块中，所以通过 APP 对可穿戴设备中 SE 模块卡片应用中的帐户信息进行更改。

可以理解，由于 HCE 移动终端上 APP 对可穿戴设备中 SE 模块卡片应用的访问控制为对敏感数据的访问控制，所以需要通过可穿戴设备对 HCE 移动终端上的应用程序进行访问控制鉴权，只有通过访问控制鉴权的 APP 才可以访问可

穿戴设备中 SE 模块卡片应用，从而保证控制规则的安全性。

可选地，在本发明的一些可能的实施方式中，所述可穿戴设备还包括:

第二管理模块 5100，用于

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则触发所述第一管理模块执行对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权的步骤。

其中，该管理请求指令用于 HCE 移动终端请求对可穿戴设备进行访问控制等管理。

其中，，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个。

可以理解，由于可穿戴设备对访问其 SE 模块的管理实体进行设定，所以需要通过 HCE 移动终端的身份标识确定其是否为可穿戴设备中 SE 模块的管理实体，如果是，才允许该 HCE 移动终端管理可穿戴设备中 SE 模块，继而再对 HCE 移动终端上的 APP 访问可穿戴设备中 SE 模块卡片应用进行进一步访问控制鉴权，从而使得访问的安全性更高。

可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此 HCE 移动终端加入黑名单，以防下次再接收到该用户的管理请求指令。

可以理解的是，本实施例的可穿戴设备 500 的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

可以看出，本实施例的方案中，可穿戴设备 500 接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备 500 具有安全模块；可穿戴设备 500 再

从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后可穿戴设备 500 再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则可穿戴设备 500 传递所述交易请求到所述可穿戴设备中安全模块。通过将 HCE 移动终端的 SE 功能在可穿戴设备 500 中实现，从而可以在 HCE 移动终端进行 NFC 交易的时候提高交易的安全性，风险防范性强。

参见图 6，图 6 是本发明第六实施例提供一种可穿戴设备的结构示意图。如图 6 所示，本发明第六实施例提供一种可穿戴设备 600 可以包括：至少一个总线 601、与总线相连的至少一个处理器 602 以及与总线相连的至少一个存储器 603。

其中，处理器 602 通过总线 601，调用存储器 603 中存储的代码以用于接收基于主机卡模拟移动终端的交易请求指令；从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识；判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则响应所述交易请求与外部终端进行交易通信。

其中，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片中的至少一个。

可选地，在本发明的一些可能的实施方式中，所述处理器 602 还用于：

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

可选地，在本发明的一些可能的实施方式中，所述处理器 602 还用于：

接收用户的配对指令，所述配对指令用于为所述可穿戴设备选择配对的基于主机卡模拟移动终端；

确定所述基于主机卡模拟移动终端为所述可穿戴设备的管理实体，其中，所述可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

可选地，在本发明的一些可能的实施方式中，所述传递所述交易请求到所述可穿戴设备中安全模块之前，所述处理器 602 还用于：

获取所述基于主机卡模拟移动终端和所述可穿戴设备之间的信号强度;

判断所述信号强度是否大于或等于预设信号强度;

若所述信号强度大于或等于所述预设信号强度，则触发传递所述交易请求指令到所述可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

可选地，在本发明的一些可能的实施方式中，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

可选地，在本发明的一些可能的实施方式中，所述处理器 602 还用于:

对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

可选地，在本发明的一些可能的实施方式中，若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理，并提醒用户。

可选地，在本发明的一些可能的实施方式中，所述可穿戴设备对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权之前，所述处理器 602 还用于:

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理指令中获取所述基于主机卡模拟移动终端的身份标识,;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则触发所述可穿戴设备对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权的步骤。

其中，该管理请求指令用于HCE移动终端请求对可穿戴设备进行访问控制等管理。可选地，在本发明的一些可能的实施方式中，若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问，并提醒用户有非法设备访问。

可选地，在本发明的一些可能的实施方式中，当提醒用户有非法设备访问后，用户可将此HCE移动终端加入黑名单，以防下次再接收到该用户的管理请求指令。

可以理解的是，本实施例的可穿戴设备 600 的各功能模块的功能可根据上述方法实施例中的方法具体实现，其具体实现过程可以参照上述方法实施例的相关描述，此处不再赘述。

可以看出，本实施例的方案中，可穿戴设备 600 接收基于主机卡模拟移动终端的交易请求指令，所述可穿戴设备 600 具有安全模块；可穿戴设备 600 再从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识，所述身份标识包括所述主机卡模拟移动终端的移动设备国际识别码、物理地址和近距离无线通讯芯片序列号中的至少一个；然后可穿戴设备 600 再判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识；若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则可穿戴设备 600 传递所述交易请求到所述可穿戴设备中安全模块。通过将HCE移动终端的SE功能在可穿戴设备600中实现，从而可以在HCE移动终端进行NFC交易的时候提高交易的安全性，风险防范性强。

本发明实施例还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时包括上述方法实施例中记载的任何移动支付方法的部分或全部步骤。

需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本发明的各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可为个人计算机、服务器或者网络设备等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括: U盘、只读存储器(ROM, Read-Only Memory)、随机存取存储器(RAM, Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权 利 要 求 书

1、一种移动支付方法，其特征在于，应用于可穿戴设备，所述可穿戴设备具有安全模块，所述方法包括:

接收基于主机卡模拟移动终端的交易请求指令;

从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

2、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

3、根据权利要求 1 或 2 所述的方法，其特征在于，所述传递所述交易请求指令到所述可穿戴设备中安全模块之前，所述方法还包括:

获取所述基于主机卡模拟移动终端和所述可穿戴设备之间的信号强度;

判断所述信号强度是否大于或等于预设信号强度;

若所述信号强度大于或等于所述预设信号强度，则触发所述传递所述交易请求指令到所述可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

4、根据权利要求 3 所述的方法，其特征在于，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

5、根据权利要求 1 或 2 所述的方法，其特征在于，所述方法还包括:

对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

6、根据权利要求 5 所述的方法，其特征在于，所述对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权之前，所述方法还包括:

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理请求指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则触发所述可穿戴设备对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权的步骤。

7、根据权利要求 1 所述的方法，其特征在于，所述方法还包括:

接收用户的配对指令，所述配对指令用于为所述可穿戴设备选择配对的基于主机卡模拟移动终端;

确定所述基于主机卡模拟移动终端为所述可穿戴设备的管理实体，其中，所述可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

8、一种可穿戴设备，其特征在于，所述可穿戴设备具有安全模块，所述可穿戴设备包括:

接收模块，用于接收基于主机卡模拟移动终端的交易请求指令;

第一获取模块，用于从所述交易请求指令中获取所述基于主机卡模拟移动终端的身份标识;

第一判断模块，用于判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

传递模块，用于若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则传递所述交易请求指令到所述可穿戴设备中安全模块。

9、根据权利要求 8 所述的可穿戴设备，其特征在于，所述第一判断模块还用于:

若所述身份标识不是所述可穿戴设备中安全模块的管理实体的身份标识，则禁止所述基于主机卡模拟移动终端对所述可穿戴设备中安全模块的访问。

10、根据权利要求 8 或 9 所述的可穿戴设备，其特征在于，所述可穿戴设备还包括:

第二获取模块，用于获取所述基于主机卡模拟移动终端和所述可穿戴设备之间的信号强度;

第二判断模块，用于判断所述信号强度是否大于或等于预设信号强度;

提示模块，用于若所述信号强度大于或等于所述预设信号强度，则触发所述传递模块执行所述传递所述交易请求指令到所述可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离。

11、根据权利要求 10 所述的可穿戴设备，其特征在于，所述预设信号强度由用户设定，或由所述可穿戴设备根据所述可穿戴设备与所述基于主机卡模拟移动终端之间的通信信号强度按照预设方式确定。

12、根据权利要求 8 或 9 所述的可穿戴设备，其特征在于，所述可穿戴设备还包括:

第一管理模块，用于

对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权，所述访问控制鉴权用于对所述应用程序访问所述可穿戴设备中安全模块卡片应用进行访问控制鉴权;

若所述访问控制鉴权通过，则允许所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理;

若所述访问控制鉴权未通过，则禁止所述应用程序对所述可穿戴设备中安全模块卡片应用进行管理。

13、根据权利要求 12 所述的可穿戴设备，其特征在于，所述可穿戴设备还包括:

第二管理模块，用于

接收基于主机卡模拟移动终端的管理请求指令;

从所述管理指令中获取所述基于主机卡模拟移动终端的身份标识;

判断所述身份标识是否为所述可穿戴设备中安全模块的管理实体的身份标识;

若所述身份标识是所述可穿戴设备中安全模块的管理实体的身份标识，则

触发所述第一管理模块执行所述对所述基于主机卡模拟移动终端上的应用程序进行访问控制鉴权的步骤。

14、根据权利要求 8 所述的可穿戴设备，其特征在于，所述可穿戴设备还包括:

配对模块，用于

接收用户的配对指令，所述配对指令用于为所述可穿戴设备选择配对的基于主机卡模拟移动终端;

确定所述基于主机卡模拟移动终端为所述可穿戴设备的管理实体，其中，所述可穿戴设备的管理实体通过所述基于主机卡模块移动终端的身份标识进行认证。

说 明 书 附 图

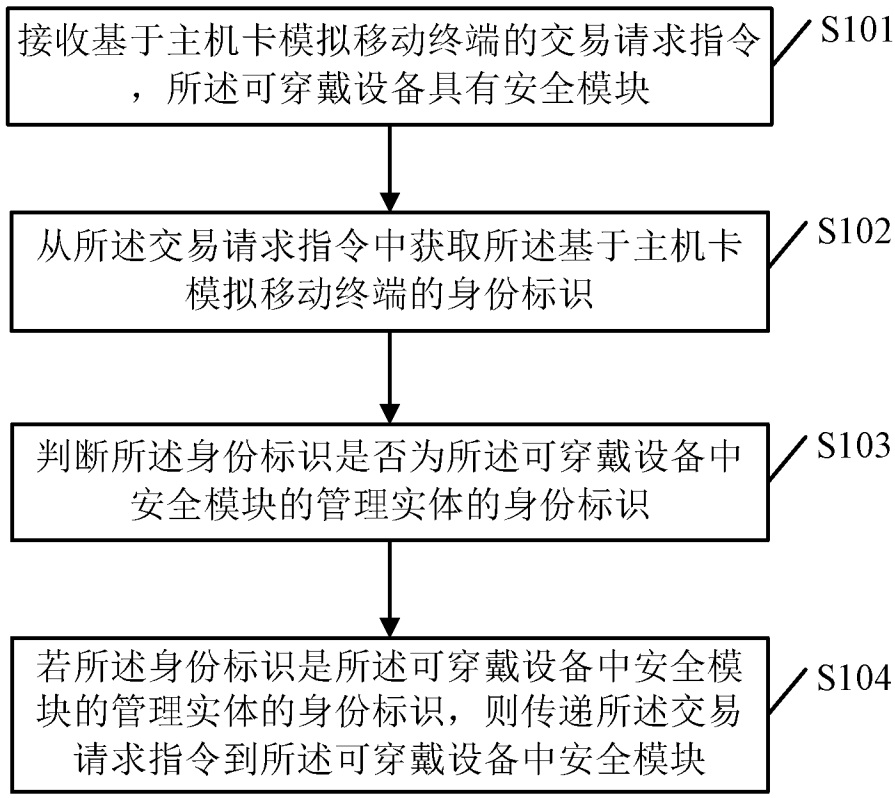


图 1-a

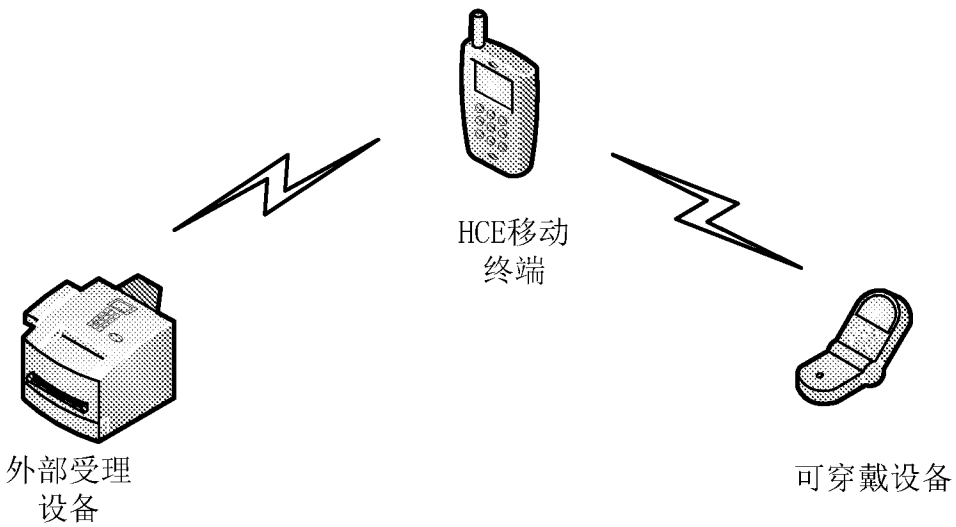


图 1-b

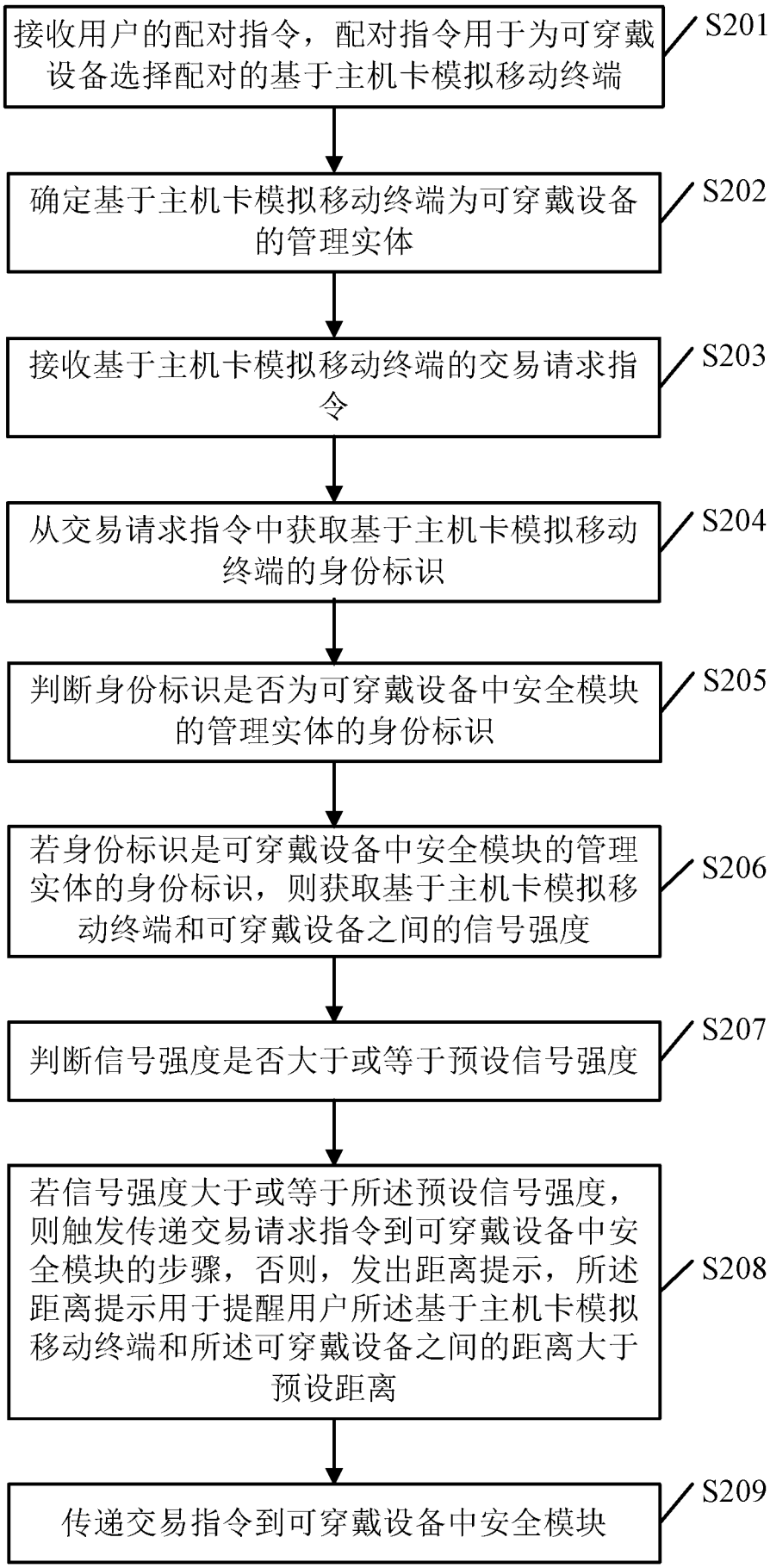

接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端
S201
确定基于主机卡模拟移动终端为可穿戴设备的管理实体
S202
接收基于主机卡模拟移动终端的交易请求指令
S203
从交易请求指令中获取基于主机卡模拟移动终端的身份标识
S204
判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识
S205
若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则获取基于主机卡模拟移动终端和可穿戴设备之间的信号强度
S206
判断信号强度是否大于或等于预设信号强度
S207
若信号强度大于或等于所述预设信号强度，则触发传递交易请求指令到可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离
S208
传递交易指令到可穿戴设备中安全模块
S209

图 2-a

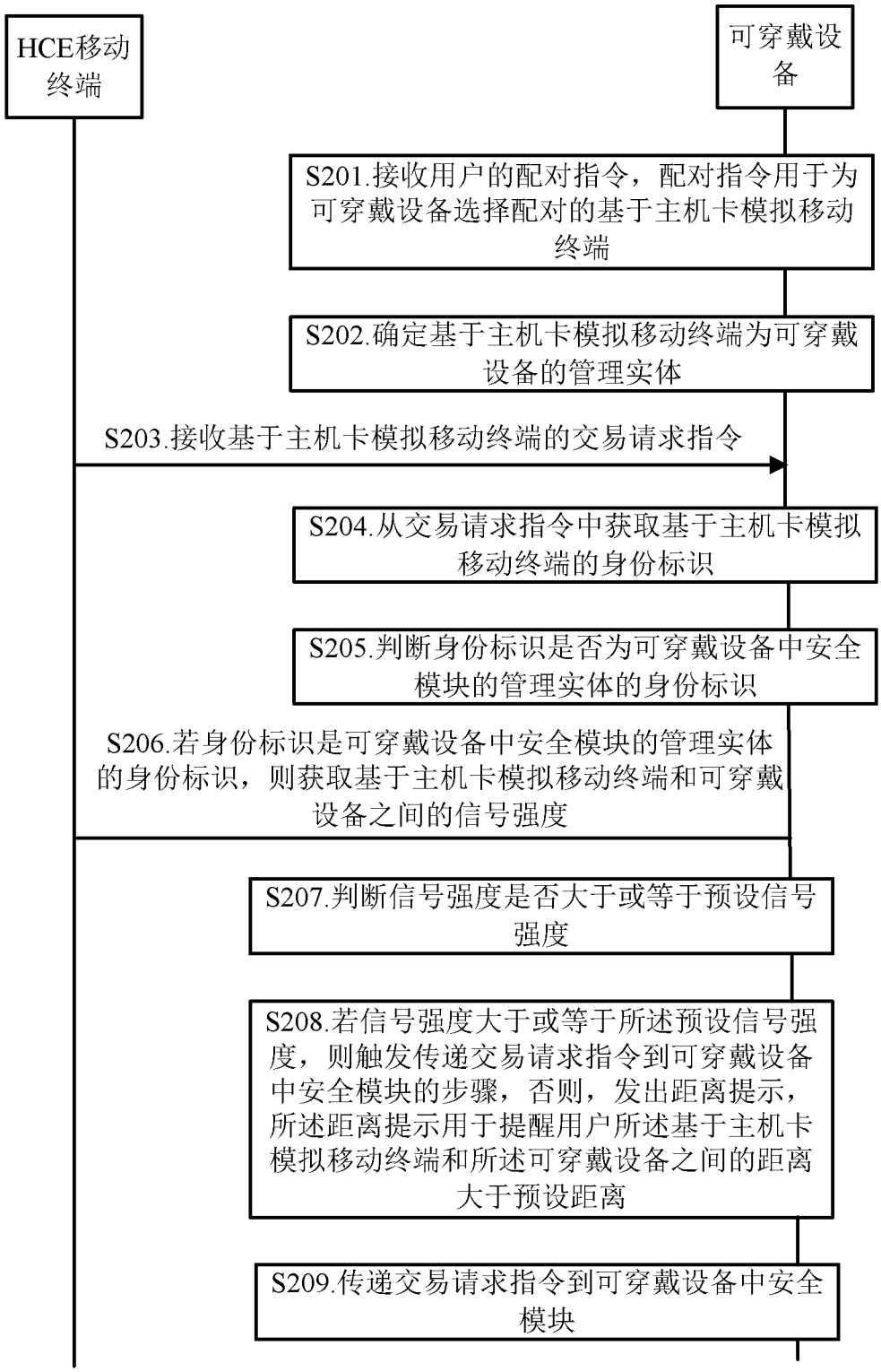

HCE移动终端
可穿戴设备
S201.接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端
S202.确定基于主机卡模拟移动终端为可穿戴设备的管理实体
S203.接收基于主机卡模拟移动终端的交易请求指令
S204.从交易请求指令中获取基于主机卡模拟移动终端的身份标识
S205.判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识
S206.若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则获取基于主机卡模拟移动终端和可穿戴设备之间的信号强度
S207.判断信号强度是否大于或等于预设信号强度
S208.若信号强度大于或等于所述预设信号强度，则触发传递交易请求指令到可穿戴设备中安全模块的步骤，否则，发出距离提示，所述距离提示用于提醒用户所述基于主机卡模拟移动终端和所述可穿戴设备之间的距离大于预设距离
S209.传递交易请求指令到可穿戴设备中安全模块

图 2-b

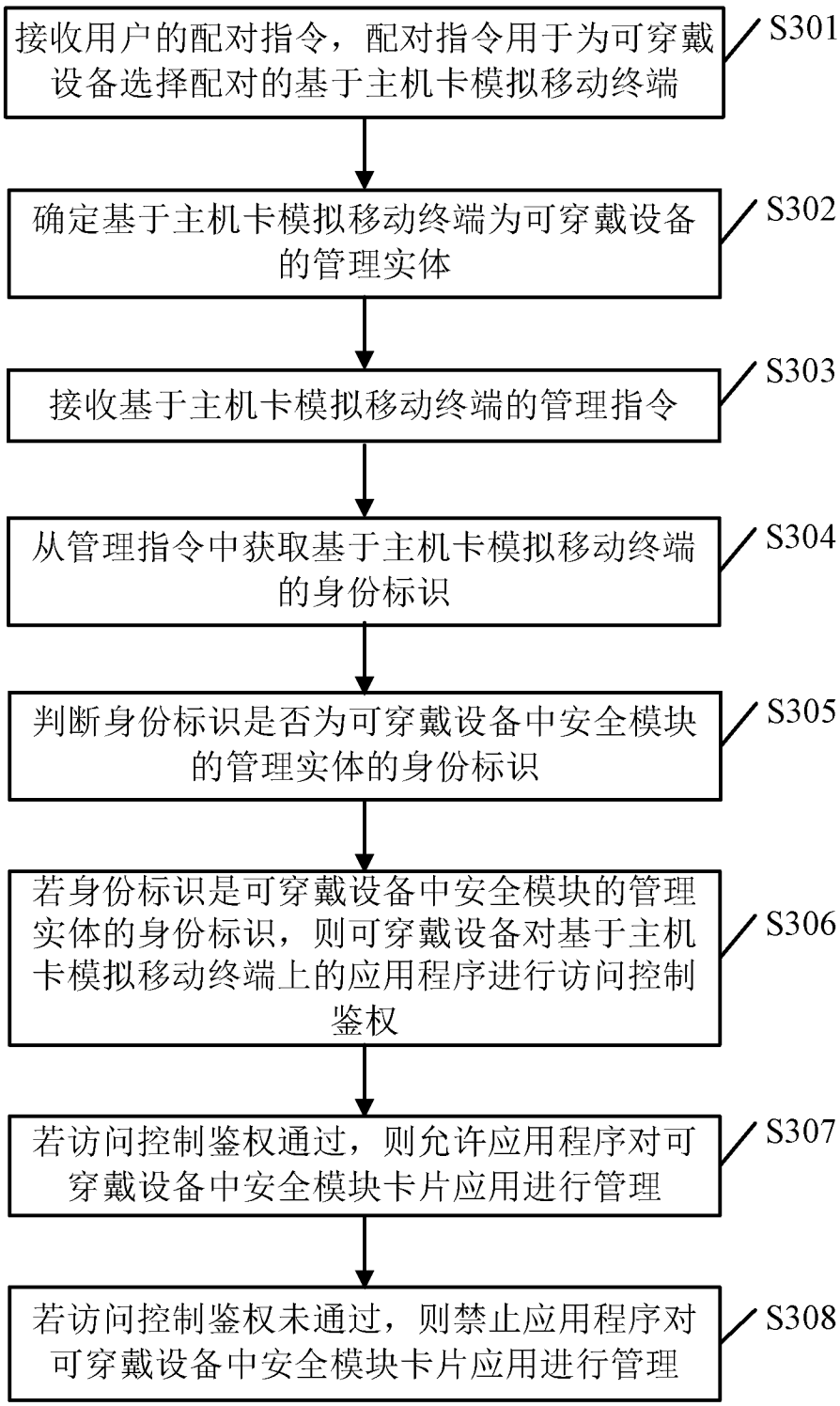

接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端
S301
确定基于主机卡模拟移动终端为可穿戴设备的管理实体
S302
接收基于主机卡模拟移动终端的管理指令
S303
从管理指令中获取基于主机卡模拟移动终端的身份标识
S304
判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识
S305
若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则可穿戴设备对基于主机卡模拟移动终端上的应用程序进行访问控制鉴权
S306
若访问控制鉴权通过，则允许应用程序对可穿戴设备中安全模块卡片应用进行管理
S307
若访问控制鉴权未通过，则禁止应用程序对可穿戴设备中安全模块卡片应用进行管理
S308

图 3-a

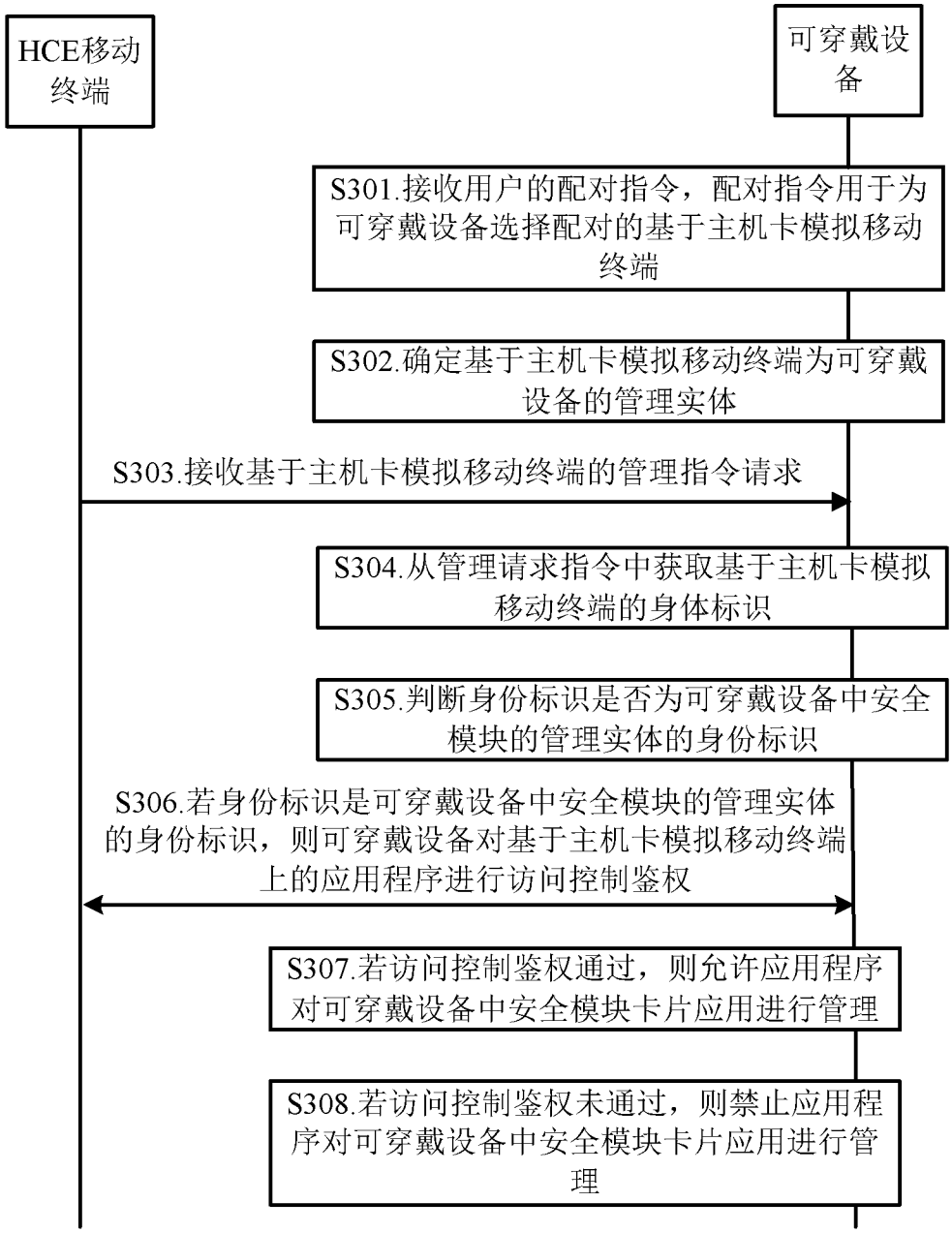

HCE移动终端
可穿戴设备
S301.接收用户的配对指令，配对指令用于为可穿戴设备选择配对的基于主机卡模拟移动终端
S302.确定基于主机卡模拟移动终端为可穿戴设备的管理实体
S303.接收基于主机卡模拟移动终端的管理指令请求
S304.从管理请求指令中获取基于主机卡模拟移动终端的身体标识
S305.判断身份标识是否为可穿戴设备中安全模块的管理实体的身份标识
S306.若身份标识是可穿戴设备中安全模块的管理实体的身份标识，则可穿戴设备对基于主机卡模拟移动终端上的应用程序进行访问控制鉴权
S307.若访问控制鉴权通过，则允许应用程序对可穿戴设备中安全模块卡片应用进行管理
S308.若访问控制鉴权未通过，则禁止应用程序对可穿戴设备中安全模块卡片应用进行管理

图 3-b

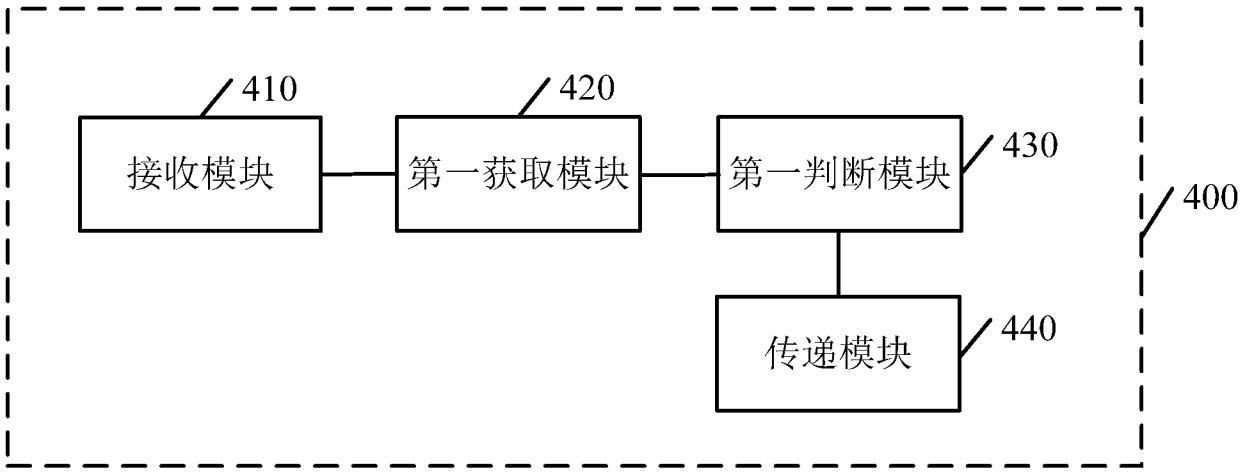

410
420
接收模块
第一获取模块
第一判断模块
430
400
传递模块
440

图 4

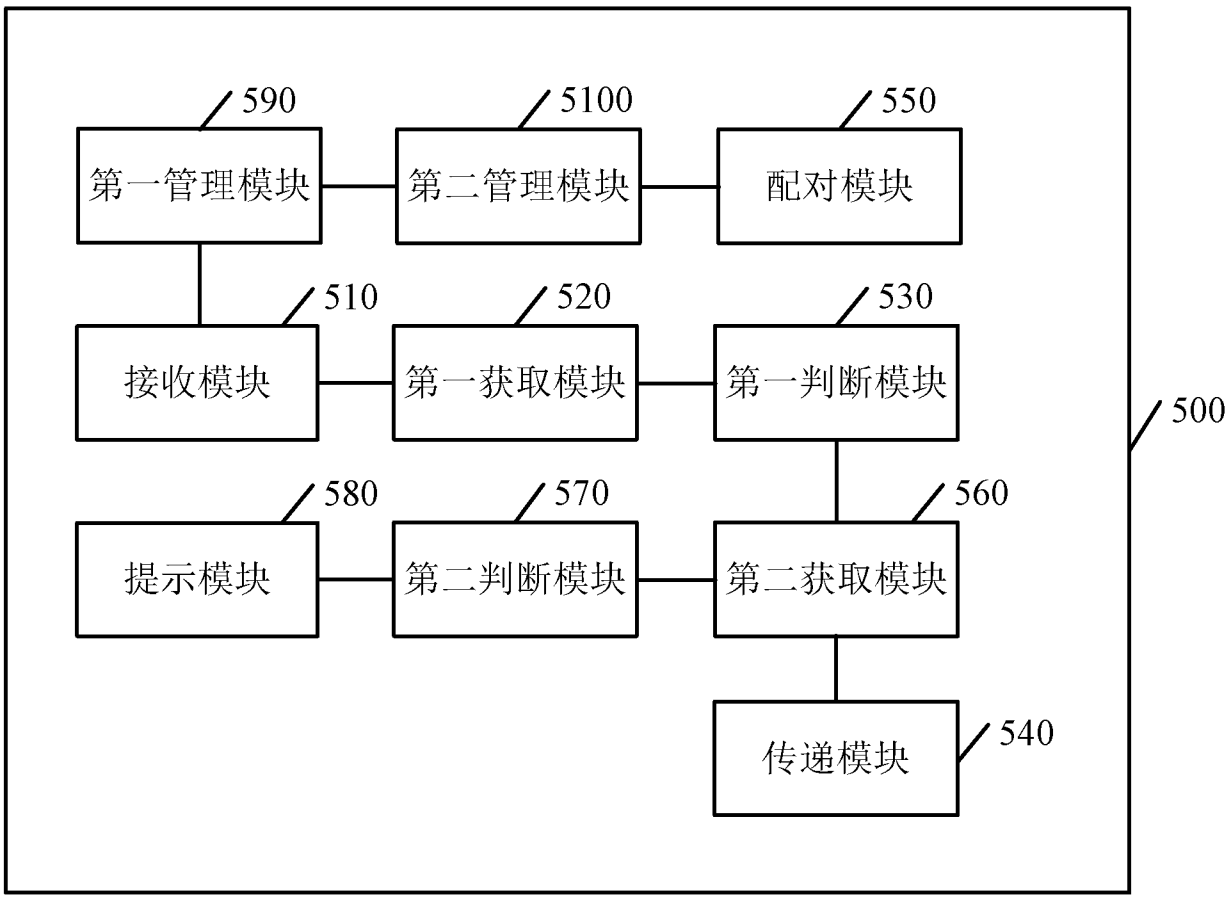

590
5100
550
第一管理模块
第二管理模块
配对模块
510
520
530
接收模块
第一获取模块
第一判断模块
500
580
570
560
提示模块
第二判断模块
第二获取模块
传递模块
540

图 5

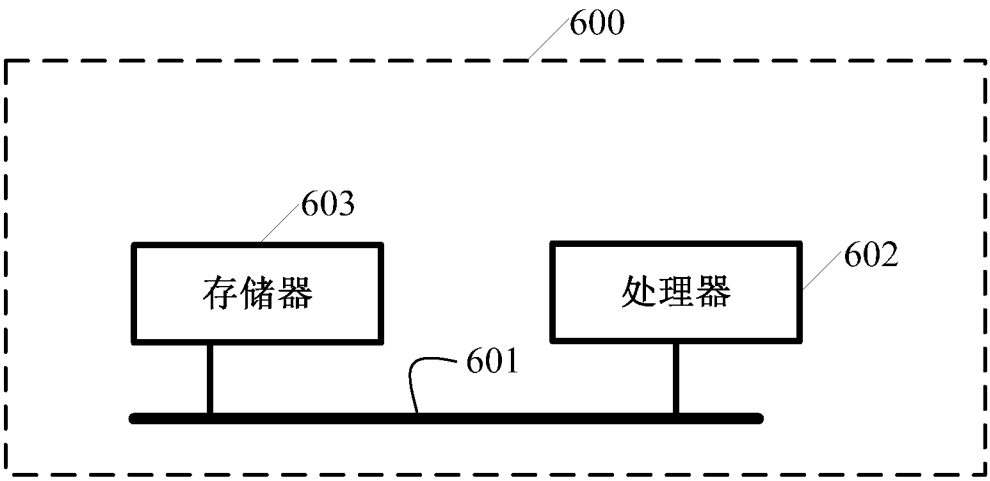


图 6

u

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/091337

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/20 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; WPI; EPODOC; CNKI; GOOGLE SCHOLAR; IEEE: mobile, payment, transaction, security, identi+, ID, wearable

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 204117191 U (BEIJING DAMING WUZHOU SCIENCE AND TECHNOLOGY INC.), 21 January 2015 (21.01.2015), description, paragraphs [0027]-[0039], and figures 1-3	1-14
A	CN 102685073 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 19 September 2012 (19.09.2012), the whole document	1-14
A	CN 102968722 A (BEIJING HUIYIN TONGLIAN SCIENCE AND TECHNOLOGY CO., LTD.), 13 March 2013 (13.03.2013), the whole document	1-14
A	CN 101154281 A (LENOVO (BEIJING) CO., LTD.), 02 April 2008 (02.04.2008), the whole document	1-14
A	US 2005187882 A1 (SOVIO, S. et al.), 25 August 2005 (25.08.2005), the whole document	1-14

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 March 2016 (01.03.2016)	**28 April 2016 (28.04.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **JIN, Xia** Telephone No.: (86-10) **62414438**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/091337

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 204117191 U	21 January 2015	None	
CN 102685073 A	19 September 2012	None	
CN 102968722 A	13 March 2013	None	
CN 101154281 A	02 April 2008	None	
US 2005187882 A1	25 August 2005	KR 20060114029 A	03 November 2006
		EP 1719322 A1	08 November 2006
		WO 2005086456 A1	15 September 2005
		CN 1926836 A	07 March 2007
		IN CHENP200603500 E	15 June 2007

国际检索报告

国际申请号 PCT/CN2015/091337

A. 主题的分类

G06Q 20/20(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT;WPI;EPODOC;CNKI;GOOGLE SCHOLAR;IEEE: 移动，支付，交易，安全，标识，身份，穿戴，mobile，payment，transaction，security，identi+，ID，wearable

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 204117191 U (北京大明五洲科技有限公司) 2015年 1月 21日 (2015-01-21) 说明书第[0027]-[0039]段，图1-3	1-14
A	CN 102685073 A (中国移动通信集团公司) 2012年 9月 19日 (2012-09-19) 全文	1-14
A	CN 102968722 A (北京惠银通联科技有限公司) 2013年 3月 13日 (2013-03-13) 全文	1-14
A	CN 101154281 A (联想北京有限公司) 2008年 4月 2日 (2008-04-02) 全文	1-14
A	US 2005187882 A1 (SOVIO, SAMPO 等) 2005年 8月 25日 (2005-08-25) 全文	1-14

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 3月 1日	2016年 4月 28日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	金霞
传真号 (86-10)62019451	电话号码 (86-10)62414438

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/091337

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	204117191	U	2015年 1月 21日	无			
CN	102685073	A	2012年 9月 19日	无			
CN	102968722	A	2013年 3月 13日	无			
CN	101154281	A	2008年 4月 2日	无			
US	2005187882	A1	2005年 8月 25日	KR	20060114029	A	2006年 11月 3日
				EP	1719322	A1	2006年 11月 8日
				WO	2005086456	A1	2005年 9月 15日
				CN	1926836	A	2007年 3月 7日
				IN	CHENP200603500	E	2007年 6月 15日