

(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 1 月 19 日 (19.01.2017)



(10) 国际公布号
WO 2017/008631 A1

- (51) 国际专利分类号:
G06F 21/82 (2013.01)
- (21) 国际申请号: PCT/CN2016/087468
- (22) 国际申请日: 2016 年 6 月 28 日 (28.06.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510405480.4 2015 年 7 月 10 日 (10.07.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 王磊 (WANG, Lei) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。 沈凌楠 (SHEN, Lingnan) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。 朱兴 (ZHU, Xing) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。

- (74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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: INFORMATION INPUT METHOD AND SYSTEM, USER EQUIPMENT, AND TERMINAL

(54) 发明名称: 信息输入方法和系统、用户设备和终端

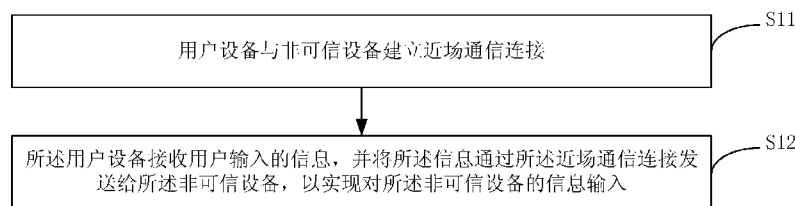


图 1

- S11 A user equipment establishes a near field communication connection with an untrusted device
- S12 The user equipment receives information entered by a user, and sends the information to the untrusted device through the near field communication connection, to implement inputting information to the untrusted device

(57) Abstract: This application provides an information input method and system, a user equipment, and a terminal. The information input method comprises: a user equipment establishes a near field communication connection with an untrusted device; the user equipment receives information entered by a user, and sends the information to the untrusted device through the near field communication connection, to implement inputting information to the untrusted device. This method can improve the security during information input, and reduce the possibility of user information being intercepted.

(57) 摘要: 本申请提出一种信息输入方法和系统、用户设备和终端, 该信息输入方法包括: 用户设备与非可信设备建立近场通信连接; 所述用户设备接收用户输入的信息, 并将所述信息通过所述近场通信连接发送给所述非可信设备, 以实现所述非可信设备的信息输入。该方法能够提高信息输入时的安全性, 降低用户信息被窃取的可能性。



WO 2017/008631 A1

信息输入方法和系统、用户设备和终端

技术领域

本申请涉及信息安全技术领域，尤其涉及一种信息输入方法和系统、用户
5 设备和终端。

背景技术

在实际的生产生活中，通过密码验证，实现各种访问控制、身份验证、权限授权的场景非常多。尤其对于像销售终端（Point Of Sale, POS），自动柜员
10 机（Automatic Teller Machine, ATM）等涉及资金的场景，密码输入安全显得极其重要。

现有技术中，用户采用他人提供的密码输入设备进行密码输入，但是他人的设备依然容易被攻击，破坏，改造等，例如，输入设备被改造后可能会在用户输入密码时，对密码进行拍摄，从而造成密码泄露。

15

发明内容

本申请旨在至少在一定程度上解决相关技术中的技术问题之一。

为此，本申请的一个目的在于提出一种信息输入方法，该方法可以提高信息输入时的安全性，降低用户信息被窃取的可能性。

20 本申请的另一个目的在于提出一种用户设备。

本申请的另一个目的在于提出一种终端。

本申请的另一个目的在于提出一种信息输入系统。

为达到上述目的，本申请第一方面实施例提出的信息输入方法，包括：用户设备与非可信设备建立近场通信连接；所述用户设备接收用户输入的信息，
25 并将所述信息通过所述近场通信连接发送给所述非可信设备，以实现对所述非可信设备的信息输入。

本申请第一方面实施例提出的信息输入方法，通过用户设备接收用户输入的信息并发送给非可信设备，可以将信息输入从传统的用户直接输入到非可信设备中，改变为用户通过用户设备输入到非可信设备中，由于用户不直接与非可信设备接触，与用户接触的是用户设备，由于用户设备是用户自己的，相对
30 于通常由他人提供的非可信设备，可以提高可信任度，从而可以提高信息输入时的安全性，降低用户信息被窃取的可能性。

为达到上述目的，本申请第二方面实施例提出的信息输入方法，包括：非可信设备与用户设备建立近场通信连接；所述非可信设备接收所述用户设备通过所述近场通信连接发送的输入信息，所述输入信息由用户通过用户设备输入。

5 本申请第二方面实施例提出的信息输入方法，非可信设备接收通过用户设备传输的用户输入的信息，由于信息是由用户输入到自己的用户设备而不是非可信设备内，从而可以提高信息的安全性。

为达到上述目的，本申请第三方面实施例提出的用户设备，包括：连接模块，用于与非可信设备建立近场通信连接；传输模块，用于接收用户输入的信息，并将所述信息通过所述近场通信连接发送给所述非可信设备，以实现对所
10 述非可信设备的信息输入。

本申请第二方面实施例提出的用户设备，通过用户设备接收用户输入的信息并发送给非可信设备，可以将信息输入从传统的用户直接输入到非可信设备中，改变为用户通过用户设备输入到非可信设备中，由于用户不直接与非可信
15 设备接触，与用户接触的是用户设备，由于用户设备是用户自己的，相对于通常由他人提供的非可信设备，可以提高可信度，从而可以提高信息输入时的安全性，降低用户信息被窃取的可能性。

为达到上述目的，本申请第四方面实施例提出的终端，所述终端属于非可信设备，所述终端包括：连接模块，用于与用户设备建立近场通信连接；接收
20 模块，用于接收所述用户设备通过所述近场通信连接发送的输入信息，所述输入信息由用户通过用户设备输入。

本申请第四方面实施例提出的终端，接收通过用户设备传输的用户输入的信息，由于信息是由用户输入到自己的用户设备而不是非可信设备内，从而可以提高信息的安全性。

25 为达到上述目的，本申请第五方面实施例提出的信息输入系统，包括：如第三方面所示的用户设备，以及，如第四方面所示的终端。

本申请第五方面实施例提出的信息输入系统，通过用户在用户设备上输入信息，用户设备将信息发送给非可信设备，可以避免用户直接与非可信设备接触，从而提高信息输入时的安全性，降低用户信息被窃取的可能性。

30 本申请附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本申请的实践了解到。

附图说明

本申请上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 是本申请一实施例提出的信息输入方法的流程示意图；

5 图 2 是本申请另一实施例提出的信息输入方法的流程示意图；

图 3 是本申请另一实施例提出的信息输入方法的流程示意图

图 4 是本申请另一实施例提出的用户设备的结构示意图；

图 5 是本申请另一实施例提出的用户设备的结构示意图；

图 6 是本申请另一实施例提出的终端的结构示意图；

10 图 7 是本申请另一实施例提出的终端的结构示意图；

图 8 是本申请另一实施例提出的信息输入系统的结构示意图。

具体实施方式

下面详细描述本申请的实施例，所述实施例的示例在附图中示出，其中自
15 始至终相同或类似的标号表示相同或类似的模块或具有相同或类似功能的模块。下面通过参考附图描述的实施例是示例性的，仅用于解释本申请，而不能理解为对本申请的限制。相反，本申请的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

图 1 是本申请一实施例提出的信息输入方法的流程示意图，该方法包
20 括：

S11：用户设备与非可信设备建立近场通信连接。

其中，用户设备是用户自己使用的设备，包括但不限于手机，或者，平板电脑等。

非可信设备是相对于用户来讲的安全性有待提高的设备，非可信设备通常
25 是非用户自己使用的设备，而是由第三方提供的设备。

非可信设备例如为：ATM 或者 POS。

本实施例中，以用户设备与非可信设备建立近场通信连接为例，可以理解
的是，用户设备可以与非可信设备建立其他形式的通信连接，例如，还可以建立
蓝牙连接，声波连接，wifi 连接等。以近场通信连接为例，可以分别在用户
30 设备和非可信设备中设置近场通信模块，以建立该通信连接。

可选的，所述用户设备与非可信设备建立近场通信连接，包括：

在所述用户设备进入所述非可信设备的近场感应区域后，所述用户设备向

所述非可信设备发送建立近场通信连接的触发指令，或者，所述用户设备接收所述非可信设备发送的建立近场通信连接的触发指令；

所述用户设备根据所述触发指令与所述非可信设备建立近场通信连接。

以用户设备是手机，非可信设备是 POS 为例，当手机进入 POS 的近场通信感应区后，手机可以主动向 POS 发送建立近场通信连接的触发指令，POS 同意建立后，手机和 POS 可以建立近场通信连接。或者，手机进入 POS 的近场通信感应区后，POS 可以主动向手机发送触发指令，手机同意后，手机和 POS 可以建立近场通信连接。具体的，可以在手机内安装预设的 app（如称为安全输入程序），手机通过用户在该 app 上的操作主动发起触发指令或接收触发指令。S12：所述用户设备接收用户输入的信息，并将所述信息通过所述近场通信连接发送给所述非可信设备，以实现与所述非可信设备的信息输入。

可选的，所述用户设备接收用户输入的信息，包括：

所述用户设备向所述用户展示信息输入界面，并接收所述用户在所述信息输入界面内输入的信息，所述信息输入界面是安全键盘。

其中，安全键盘是一种虚拟键盘，在需要信息输入时，可以弹出并展示在用户界面上，安全键盘上显示的按键排列顺序是动态改变的，从而提高安全性。

当然，可以理解的是，用户也可以通过用户设备上的物理按键或者用户设备提供的输入法键盘等进行信息输入。

另外，在用户设备与非可信设备建立通信连接后，可以在用户设备上显示提示界面，例如，提示用户请输入信息等。

当用户在所述提示界面中选择输入信息时，向用户展示信息输入界面。

例如，提示界面中可以包括用于输入信息的输入框，当用户看到提示界面，并点击该输入框后，如果用户使用用户设备上的物理按键输入，则可以直接采用物理按键输入；或者，如果信息输入界面是软件形式，例如输入法的输入界面或者安全键盘等，用户在点击输入框后，可以触发用户设备展示信息输入界面。

用户输入的信息例如为密码，验证码，身份证号等需要安全输入的信息。

以密码为例，现有技术中，用户直接在 ATM 上输入密码，如果 ATM 被恶意安装窃取密码的摄像头后，就会造成用户密码的丢失。

而本实施例中，用户在用户设备上输入密码，由于用户设备是用户自己的设备，相对于 POS，ATM 等非可信设备难以被恶意改造，或者用户很容易发

现自己的设备被恶意改造，因此，用户在用户设备上输入信息相对于在 POS，ATM 等非可信设备上输入信息可以提高信息输入的安全性。

另外，当本实施例输入的信息是要输入到非可信设备内进行验证的密码时，本实施例中的密码不限于通常采用的数字密码，还可以是图形，图片等形式的密码。

具体的，该方法可以应用于非可信设备的密码输入应用中，当非可信设备需要用户输入密码时，用户设备主动发起或根据非可信设备主动发起的连接触发指令，建立用户设备与非可信设备之间的连接。

例如，用户需要在 POS 内输入密码时，用户可以拿着手机进入 POS 的近场感应区域，在手机进入 POS 的近场感应区域后，手机和 POS 可以建立近场通信连接。在手机内已安装预定的 app（如安全输入程序）时，手机和 POS 建立连接后，在该 app 内可以弹出提示界面，提示用户可以安全输入，在用户确定采用安全输入后，可以再弹出信息输入界面（如安全键盘），之后，用户可以通过该安全键盘进行密码输入。

当然，可以理解的是，也可以采用其他触发方式触发信息输入界面的展示，例如，触发建立近场通信连接的触发指令中包含调用信息输入界面的指令，或者，在建立近场通信连接后，提示用户启动信息输入界面等。

其中，如上所示，

用户设备通过近场通信方式将用户输入的信息发送给非可信设备。

现有技术中，以非可信设备是 POS 为例，用户是直接将信息输入到 POS 中，而本申请实施例中，不再是用户直接向 POS 输入信息，而是用户将信息先输入到用户设备中，再由用户设备通过通信连接发送给 POS。

由于非可信设备是接收到的消息，并不是用户直接输入时的显式信息，因此，即使非可信设备被安装了恶意摄像头等也不能窃取到消息中传输的信息，从而提高了信息的安全性。

可选的，该方法还可以包括：

对所述用户输入的信息进行预设运算，得到预设格式的信息。

在得到预设格式的信息后，在信息发送时可以具体是将预设格式的信息发送给非可信设备。

其中，预设格式是用户设备和非可信设备预先协商的，该预设格式可以使用户设备运算后得到的预设格式的信息仅能被非可信设备识别。由于其他设备不能识别该信息，从而降低被窃取性，进一步提高安全性。

本实施例中，通过用户设备接收用户输入的信息并发送给非可信设备，可以将信息输入从传统的用户直接输入到非可信设备中，改变为用户通过用户设备输入到非可信设备中，由于用户不直接与非可信设备接触，与用户接触的是用户设备，由于用户设备是用户自己的，相对于通常由他人提供的非可信设备，可以提高可信度，从而可以提高信息输入时的安全性，降低用户信息被窃取的可能性。

图 2 是本申请另一实施例提出的信息输入方法的流程示意图，该方法包括：

S21：非可信设备与用户设备建立近场通信连接；

例如，在所述用户设备进入所述非可信设备的近场感应区域后，所述非可信设备向所述用户设备发送建立近场通信连接的触发指令，或者，所述非可信设备接收所述用户设备发送的建立近场通信连接的触发指令；所述非可信设备根据所述触发指令与所述用户设备建立近场通信连接。

非可信设备例如为 POS 或者 ATM，用户设备是指用户自己的设备，如手机。

S22：所述非可信设备接收所述用户设备通过所述近场通信连接发送的输入信息，所述输入信息由用户通过用户设备输入。

其中，所述输入信息是需要安全输入的信息。例如，输入信息是密码，身份证号，或者，验证码等。

以密码为例，非可信设备与用户设备建立近场通信连接的流程可以具体包括：当非可信设备需要用户输入密码时，向所述用户设备发起触发连接触发指令或者接收所述用户设备发起的连接触发指令，并根据所述触发指令建立用户设备与非可信设备之间的近场通信连接。

另一实施例中，该方法还可以包括：

所述非可信设备将所述输入信息发送给服务器，以使所述服务器对所述输入信息进行处理。

例如，用户将密码输入到手机中，手机将密码发送给 POS，之后 POS 将密码发给相应的服务器进行密码验证，得到密码验证结果。当验证成功后，允许用户进行后续操作。

本实施例中，非可信设备接收通过用户设备传输的用户输入的信息，由于信息是由用户输入到自己的用户设备而不是非可信设备内，从而可以提高信息的安全性。

图 3 是本申请另一实施例提出的信息输入方法的流程示意图。本实施例中，以信息为密码为例，假设用户设备是用户自己的手机，非可信设备是 POS 或者 ATM（简称为 POS/ATM），结合用户设备和非可信设备描述密码验证流程。

以用户设备与非可信设备之间的通信采用近场通信为例，近场通信技术（Near Field Communication, NFC）通常指近距离的无线通信技术。当前，最典型的基于近场通信基于近距离高频无线通信技术实现，可用距离大致在 10 厘米。其近距离的特点使其具有防信号干扰、通信冲突等优点，被大范围用于电子身份识别或者数据传输。市面上大量基于 NFC 的卡片附带安全单元（Security Element, SE）实现安全的本地信息存储，防止卡内信息篡改、拷贝等。这些技术特点使得近场通信技术使用范围广泛，不仅适合普通的电子标签，也满足金融 IC 卡等高安全要求场景。

随着近场通信技术应用和发展，如今近场通信技术也被应用于越来越多的移动设备、消费类电子产品、PC 和智能控制工具间进行近距离无线通信。例如，越来越多的 POS、ATM 等终端开始支持近场支付，越来越多的移动手机开始支持近场通信技术。

如图 3 所示，用户设备可以包括安全输入模块和近场通信模块，安全输入模块用于向用户显示密码输入界面以及接收用户输入的密码，并生成验证密码等，近场通信模块用于与非可信设备建立近场通信连接，并采用近场通信技术与非可信设备进行通信。非可信设备可以包括近场通信模块和 POS/ATM 系统，近场通信模块用于与用户设备建立近场通信连接，并采用近场通信技术与用户设备进行通信，POS/ATM 系统用于对用户设备发送的验证密码进行验证。

参见图 2，本实施例的信息输入方法包括：

S31：通信握手。

具体可以包括：

1.1，用户手机靠近 POS/ATM 近场通信感应区。

例如，当用户需要进行安全输入时，用户将自己的手机靠近 POS/ATM 近场通信感应区。

1.2，建立近场通信连接。

例如，用户可以在手机上安装安全输入程序，当手机进入 POS/ATM 近场通信感应区后，用户可以启动安全输入程序，通过安全输入程序触发两者的近场通信模块建立近场通信连接。

1.3, 进行安全通信握手。

在安全通信握手时,两者可以交换本次安全输入采用的通信协议、传输过程采用的安全相关的算法,典型的包括加密、签名等算法,以及其他应用相关的必要参数。此时,安全输入程序与 POS/ATM 进入等待安全输入状态。

5 需要说明的是,本申请实施例不限制具体的近场通信技术和通信模式。只要能够实现数据传输即可。理论上采用蓝牙、声波等其他通信手段同样可以达到期望的效果。

本申请实施例不限制握手过程中协商的加密、签名等安全算法,这些算法已经具备完整、成熟的体系,可根据实际的需要按需选择。

10 本申请实施例不限制手机端和 POS/ATM 端具体实现方案。

S32: 安全输入

具体可以包括:

2.1, 弹出安全密码输入提示。

例如,用户手机中的安全输入程序弹出提示,提示用户可以进行安全输入。

15 2.2, 弹出安全输入键盘。

例如,安全输入程序根据应用、环境的信息产生动态的安全键盘。典型的安全键盘具有被扰乱的按键排列等特征。如果需要安全输入程序在进行安全输入前可能对用户进行进一步的身份的确认或者访问的控制。

2.3, 用户进行密码输入。

20 例如,用户通过自己手机的安全输入键盘输入本次 POS/ATM 应用的密码信息。

需要说明的是,本申请实施例不限制手机安全键盘的特征。应用中可以根据实际的需要选择安全键盘的特征。

S33: 安全传输

25 具体可以包括:

3.1, 密码信息运算。

例如,安全输入程序根据实际应用规范的密码需求对输入密码进行运算,生成应用可验证的密码安全信息。生成的安全信息无法只能被应用的验证方识别和验证。

30 3.2, 根据握手的结果进行安全传输。

例如,安全输入程序根据步骤 S31 中与 POS/ATM 终端协商的通信协议、安全算法将生成的密码信息通过近场通信模块传输给 POS/ATM 系统。

S34: 安全验证

具体可以包括:

4.1, 密码验证。

例如, POS/ATM 对安全输入程序传输过来的密码信息进行验证。

5 4.2, 结果通知。

例如, POS/ATM 系统可以将验证结果通过近场通信模块通知用户手机。如果验证成功, 用户可以正常进行如支付等相关操作。如果验证失败, 可以重新开始执行 S32 重新进行密码输入, 或者验证失败, 中断业务。

本实施例中, 用户可以在自己的用户设备上输入密码, 用户设备可以通过
10 近场通信将密码传输给验证设备, 实现基于近场通信的安全密码输入, 提高安全性, 保护用户隐私数据。

图 4 是本申请另一实施例提出的用户设备的结构示意图, 用户设备 40 包括:

连接模块 41, 用于与非可信设备建立近场通信连接;

15 其中, 用户设备是用户自己使用的设备, 包括但不限于手机, 或者, 平板电脑等。

非可信设备是相对于用户来讲的安全性有待提高的设备, 非可信设备通常是非用户自己使用的设备, 而是由第三方提供的设备。

非可信设备例如为: ATM 或者 POS。

20 本实施例中, 以用户设备与非可信设备建立近场通信连接为例, 可以理解的是, 用户设备可以与非可信设备建立其他形式的通信连接, 例如, 还可以建立蓝牙连接, 声波连接, wifi 连接等。

以近场通信连接为例, 可以分别在用户设备和非可信设备中设置近场通信模块, 以建立该通信连接。其中, 近场通信模块在本实施例中具体是指连接模
25 块。

可选的, 所述连接模块 41 具体用于:

在所述用户设备进入所述非可信设备的近场感应区域后, 向所述非可信设备发送建立近场通信连接的触发指令, 或者, 接收所述非可信设备发送的建立近场通信连接的触发指令;

30 根据所述触发指令与所述非可信设备建立近场通信连接。

以用户设备是手机, 非可信设备是 POS 为例, 当手机进入 POS 的近场通信感应区后, 手机可以主动向 POS 发送建立近场通信连接的触发指令, POS

同意建立后,手机和POS可以建立近场通信连接。或者,手机进入POS的近场通信感应区后,POS可以主动向手机发送触发指令,手机同意后,手机和POS可以建立近场通信连接。具体的,可以在手机内安装预设的app(如称为安全输入程序),手机通过用户在该app上的操作主动发起触发指令或接收触发指令。

传输模块42,用于接收用户输入的信息,并将所述信息通过所述近场通信连接发送给所述非可信设备,以实现所述非可信设备的信息输入。

可选的,参见图5,所述传输模块42包括:

第一单元421,用于向所述用户展示信息输入界面,并接收所述用户在所述信息输入界面内输入的信息,所述信息输入界面是安全键盘。

其中,安全键盘是一种虚拟键盘,在需要信息输入时,可以弹出并展示在用户界面上,安全键盘上显示的按键排列顺序是动态改变的,从而可以提高安全性。

当然,可以理解的是,用户也可以通过用户设备上的物理按键或者用户设备提供的输入法键盘等进行信息输入。

另外,在用户设备与非可信设备建立通信连接后,可以在用户设备上显示提示界面,例如,提示用户请输入信息等。

当用户在所述提示界面中选择输入信息时,向用户展示信息输入界面。

例如,提示界面中可以包括用于输入信息的输入框,当用户看到提示界面,并点击该输入框后,如果用户使用用户设备上的物理按键输入,则可以直接采用物理按键输入;或者,如果信息输入界面是软件形式,例如输入法的输入界面或者安全键盘等,用户在点击输入框后,可以触发用户设备展示信息输入界面。

可选的,所述传输模块42包括:

第二单元422,用于对所述用户输入的信息进行预设运算,得到预设格式的信息;

第三单元423,用于将所述预设格式的信息发送给所述非可信设备。

其中,预设格式是用户设备和非可信设备预先协商的,该预设格式可以使用户设备运算后得到的预设格式的信息仅能被非可信设备识别。由于其他设备不能识别该信息,从而降低被窃取性,进一步提高安全性。

用户输入的信息例如为密码,验证码,身份证号等需要安全输入的信息。

可选的,所述信息是需要输入到所述非可信设备中的密码,所述连接模块

41 具体用于:

在所述非可信设备需要用户输入密码时,主动发起或接收所述非可信设备发起的连接触发指令,并根据所述触发指令建立与非可信设备之间的近场通信连接。

5 以密码为例,现有技术中,用户直接在 ATM 上输入密码,如果 ATM 被恶意安装窃取密码的摄像头后,就会造成用户密码的丢失。

而本实施例中,用户在用户设备上输入密码,由于用户设备是用户自己的设备,相对于 POS, ATM 等非可信设备难以被恶意改造,或者用户很容易发现自己的设备被恶意改造,因此,用户在用户设备上输入信息相对于在 POS, 10 ATM 等非可信设备上输入信息可以提高信息输入的安全性。

另外,当本实施例输入的信息是要输入到非可信设备内进行验证的密码时,本实施例中的密码不限于通常采用的数字密码,还可以是图形,图片等形式的密码。

具体的,该方法可以应用于非可信设备的密码输入应用中,当非可信设备 15 需要用户输入密码时,用户设备主动发起或根据非可信设备主动发起的连接触发指令,建立用户设备与非可信设备之间的连接。

例如,用户需要在 POS 内输入密码时,用户可以拿着手机进入 POS 的近场感应区域,在手机进入 POS 的近场感应区域后,手机和 POS 可以建立近场通信连接。在手机内已安装预定的 app (如安全输入程序) 时,手机和 POS 20 建立连接后,在该 app 内可以弹出提示界面,提示用户可以安全输入,在用户确定采用安全输入后,可以再弹出信息输入界面(如安全键盘),之后,用户可以通过该安全键盘进行密码输入。

当然,可以理解的是,也可以采用其他触发方式触发信息输入界面的展示,例如,触发建立近场通信连接的触发指令中包含调用信息输入界面的指令,或者, 25 在建立近场通信连接后,提示用户启动信息输入界面等。

本实施例中,通过用户设备接收用户输入的信息并发送给非可信设备,可以将信息输入从传统的用户直接输入到非可信设备中,改变为用户通过用户设备输入到非可信设备中,由于用户不直接与非可信设备接触,与用户接触的是用户设备,由于用户设备是用户自己的,相对于通常由他人提供的非可信设备, 30 可以提高可信度,从而可以提高信息输入时的安全性,降低用户信息被窃取的可能性。

图 6 是本申请另一实施例提出的终端的结构示意图,该终端属于非可信设

备, 终端 60 包括:

连接模块 61, 用于与用户设备建立近场通信连接;

可选的, 所述连接模块 61 具体用于:

5 在所述用户设备进入所述终端的近场感应区域后, 向所述用户设备发送建立近场通信连接的触发指令, 或者, 接收所述用户设备发送的建立近场通信连接的触发指令; 根据所述触发指令与所述用户设备建立近场通信连接。

非可信设备例如为 POS 或者 ATM, 用户设备是指用户自己的设备, 如手机。

10 接收模块 62, 用于接收所述用户设备通过所述近场通信连接发送的输入信息, 所述输入信息由用户通过用户设备输入。

其中, 所述输入信息是需要安全输入的信息。例如, 输入信息是密码, 身份证号, 或者, 验证码等。

可选的, 所述连接模块 61 具体用于:

15 当所述终端需要用户输入密码时, 向所述用户设备发起连接触发指令或者接收所述用户设备发起的连接触发指令, 并根据所述触发指令建立所述近场通信连接。

以密码为例, 非可信设备与用户设备建立近场通信连接的流程可以具体包括: 当非可信设备需要用户输入密码时, 向所述用户设备发起触发连接触发指令或者接收所述用户设备发起的连接触发指令, 并根据所述触发指令建立用户设备与非可信设备之间的近场通信连接。

20

另一实施例中, 参见图 7, 该装置 60 还包括:

发送模块 63, 用于将所述输入信息发送给服务器, 以使所述服务器对所述输入信息进行处理。

25 例如, 用户将密码输入到手机中, 手机将密码发送给 POS, 之后 POS 将密码发给相应的服务器进行密码验证, 得到密码验证结果。当验证成功后, 允许用户进行后续操作。

本实施例中, 非可信设备接收通过用户设备传输的用户输入的信息, 由于信息是由用户输入到自己的用户设备而不是非可信设备内, 从而可以提高信息的安全性。

30 图 8 是本申请另一实施例提出的信息输入系统的结构示意图, 该系统 80 包括: 用户设备 81 和非可信设备 82, 用户设备 81 接收用户输入的信息, 并发送给非可信设备 82。

用户设备 81 例如为手机, 平板电脑等, 非可信设备 82 例如为 POS, ATM 等。

具体的用户设备的组成可以参见图 4 或图 5 所示, 具体的非可信设备的组成可以参见图 6 或图 7 所示, 在此不再赘述。

5 本实施例中, 通过用户在用户设备上输入信息, 用户设备将信息发送给非可信设备, 可以避免用户直接与非可信设备接触, 从而提高信息输入时的安全性, 降低用户信息被窃取的可能性。

需要说明的是, 在本申请的描述中, 术语“第一”、“第二”等仅用于描述目的, 而不能理解为指示或暗示相对重要性。此外, 在本申请的描述中, 除非另有说明, “多个”的含义是两个或两个以上。

10 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为, 表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分, 并且本申请的优选实施方式的范围包括另外的实现, 其中可以不按所示出或讨论的顺序, 包括根据所涉及的功能按基本同时的方式或按相反的顺序, 来执行功能, 这应被本申请的实施例所属技术领域的技术人员所理解。

应当理解, 本申请的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中, 多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如, 如果用硬件来实现, 和在另一实施方式中一样, 可用本领域公知的下列技术中的任一项或他们的组合来实现: 具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路, 具有合适的组合逻辑门电路的专用集成电路, 可编程门阵列(PGA), 现场可编程门阵列(FPGA)等。

25 本技术领域的普通技术人员可以理解实现上述实施例方法携带的全部或部分步骤是可以通程序来指令相关的硬件完成, 所述的程序可以存储于一种计算机可读存储介质中, 该程序在执行时, 包括方法实施例的步骤之一或其组合。

30 此外, 在本申请各个实施例中的各功能单元可以集成在一个处理模块中, 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模块中。上述集成的模块既可以采用硬件的形式实现, 也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用, 也可以存储在一个计算机可读取存储介质中。

上述提到的存储介质可以是只读存储器，磁盘或光盘等。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

尽管上面已经示出和描述了本申请的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本申请的限制，本领域的普通技术人员在本申请的范围内可以对上述实施例进行变化、修改、替换和变型。

权 利 要 求 书

1、一种信息输入方法，其特征在于，包括：

用户设备与非可信设备建立近场通信连接；

5 所述用户设备接收用户输入的信息，并将所述信息通过所述近场通信连接发送给所述非可信设备，以实现所述非可信设备的信息输入。

2、根据权利要求 1 所述的方法，其特征在于，所述用户设备与非可信设备建立近场通信连接，包括：

10 在所述用户设备进入所述非可信设备的近场感应区域后，所述用户设备向所述非可信设备发送建立近场通信连接的触发指令，或者，所述用户设备接收所述非可信设备发送的建立近场通信连接的触发指令；

所述用户设备根据所述触发指令与所述非可信设备建立近场通信连接。

3、根据权利要求 1 所述的方法，其特征在于，所述用户设备接收用户输入的信息，包括：

15 所述用户设备向所述用户展示信息输入界面，并接收所述用户在所述信息输入界面内输入的信息，所述信息输入界面是安全键盘。

4、根据权利要求 1 所述的方法，其特征在于，所述将所述信息通过所述近场通信连接发送给所述非可信设备之前，所述方法还包括：

对所述用户输入的信息进行预设运算，得到预设格式的信息；

20 所述将所述信息通过所述近场通信连接发送给所述非可信设备，包括：将所述预设格式的信息发送给所述非可信设备。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述信息是需要安全输入的信息。

6、根据权利要求 1-4 任一项所述的方法，其特征在于，所述方法应用于非可信设备的密码输入应用中；

25 所述用户设备与非可信设备建立近场通信连接，具体包括：

所述用户设备在所述非可信设备需要用户输入密码时，主动发起或接收所述非可信设备发起的连接触发指令，并根据所述触发指令建立与非可信设备之间的近场通信连接。

30 7、根据权利要求 1-4 任一项所述的方法，其特征在于，所述非可信设备包括：ATM 或者 POS。

8、一种信息输入方法，其特征在于，包括：

非可信设备与用户设备建立近场通信连接；

所述非可信设备接收所述用户设备通过所述近场通信连接发送的输入信息，所述输入信息由用户通过用户设备输入。

9、根据权利要求 8 所述的方法，其特征在于，所述非可信设备与用户设备建立近场通信连接，包括：

5 在所述用户设备进入所述非可信设备的近场感应区域后，所述非可信设备向所述用户设备发送建立近场通信连接的触发指令，或者，所述非可信设备接收所述用户设备发送的建立近场通信连接的触发指令；

所述非可信设备根据所述触发指令与所述用户设备建立近场通信连接。

10、根据权利要求 8 所述的方法，其特征在于，还包括：

10 所述非可信设备将所述输入信息发送给服务器，以使所述服务器对所述输入信息进行处理。

11、根据权利要求 8-10 任一项所述的方法，其特征在于，所述输入信息是需要安全输入的信息。

12、根据权利要求 8-10 任一项所述的方法，其特征在于，所述非可信设备与用户设备建立近场通信连接包括：

当非可信设备需要用户输入密码时，向所述用户设备发起触发连接触发指令或者接收所述用户设备发起的连接触发指令，并根据所述触发指令建立用户设备与非可信设备之间的近场通信连接。

13、根据权利要求 8-10 任一项所述的方法，其特征在于，所述非可信设备包括：ATM 或者 POS。

14、一种用户设备，其特征在于，包括：

连接模块，用于与非可信设备建立近场通信连接；

传输模块，用于接收用户输入的信息，并将所述信息通过所述近场通信连接发送给所述非可信设备，以实现所述非可信设备的信息输入。

25 15、根据权利要求 14 所述的设备，其特征在于，所述连接模块具体用于：在所述用户设备进入所述非可信设备的近场感应区域后，向所述非可信设备发送建立近场通信连接的触发指令，或者，接收所述非可信设备发送的建立近场通信连接的触发指令；

根据所述触发指令与所述非可信设备建立近场通信连接。

30 16、根据权利要求 14 所述的设备，其特征在于，所述传输模块包括：

第一单元，用于向所述用户展示信息输入界面，并接收所述用户在所述信息输入界面内输入的信息，所述信息输入界面是安全键盘。

17、根据权利要求 14 所述的设备，其特征在于，所述传输模块包括：
第二单元，用于对所述用户输入的信息进行预设运算，得到预设格式的信息；

第三单元，用于将所述预设格式的信息发送给所述非可信设备。

5 18、根据权利要求 14-17 任一项所述的设备，其特征在于，所述信息是需要输入到所述非可信设备中的密码，所述连接模块具体用于：

在所述非可信设备需要用户输入密码时，主动发起或接收所述非可信设备发起的连接触发指令，并根据所述触发指令建立与非可信设备之间的近场通信连接。

10 19、一种终端，所述终端属于非可信设备，其特征在于，所述终端包括：
连接模块，用于与用户设备建立近场通信连接；
接收模块，用于接收所述用户设备通过所述近场通信连接发送的输入信息，所述输入信息由用户通过用户设备输入。

20、根据权利要求 19 所述的终端，其特征在于，所述连接模块具体用于：
15 在所述用户设备进入所述终端的近场感应区域后，向所述用户设备发送建立近场通信连接的触发指令，或者，接收所述用户设备发送的建立近场通信连接的触发指令；

根据所述触发指令与所述用户设备建立近场通信连接。

21、根据权利要求 19 所述的终端，其特征在于，还包括：
20 发送模块，用于将所述输入信息发送给服务器，以使所述服务器对所述输入信息进行处理。

22、根据权利要求 19-21 任一项所述的终端，其特征在于，所述连接模块具体用于：

25 当所述终端需要用户输入密码时，向所述用户设备发起连接触发指令或者接收所述用户设备发起的连接触发指令，并根据所述触发指令建立所述近场通信连接。

23、根据权利要求 19-21 任一项所述的终端，其特征在于，所述终端是 ATM 或者 POS。

24、一种信息输入系统，其特征在于，包括：
30 如权利要求 14-18 任一项所述的设备；以及，
如权利要求 19-23 任一项所述的终端。

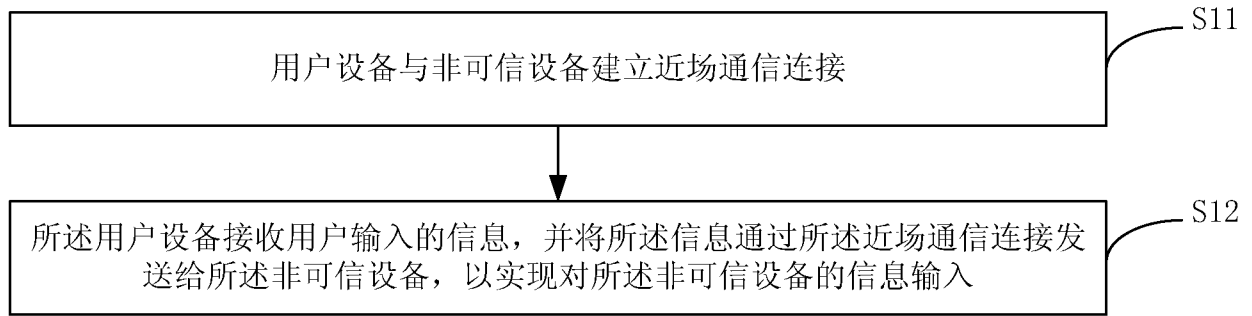


图 1

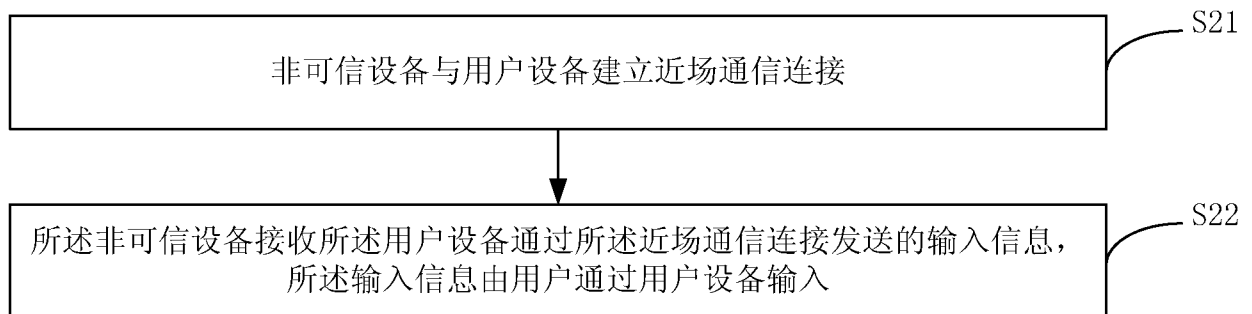


图 2

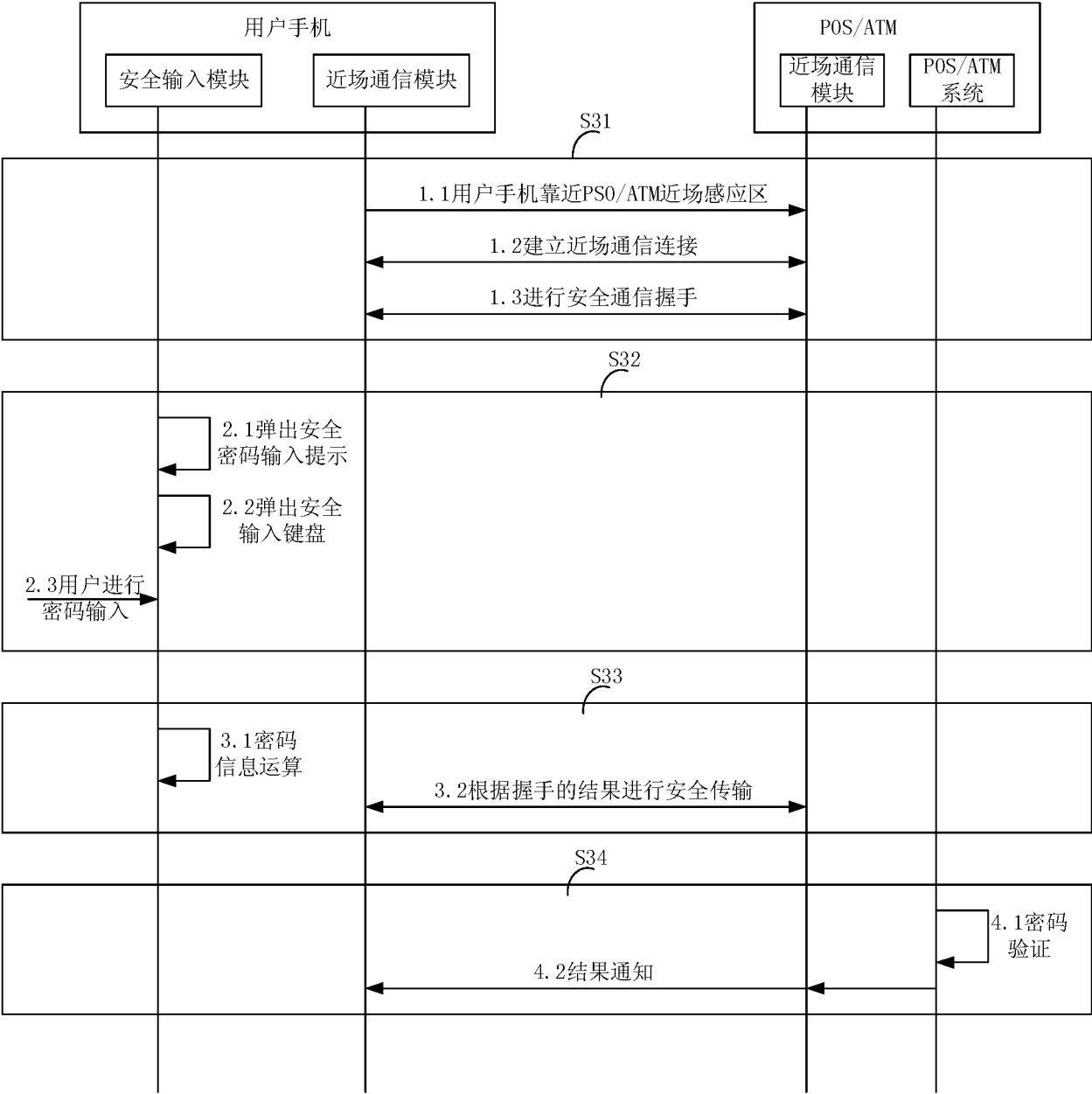


图 3

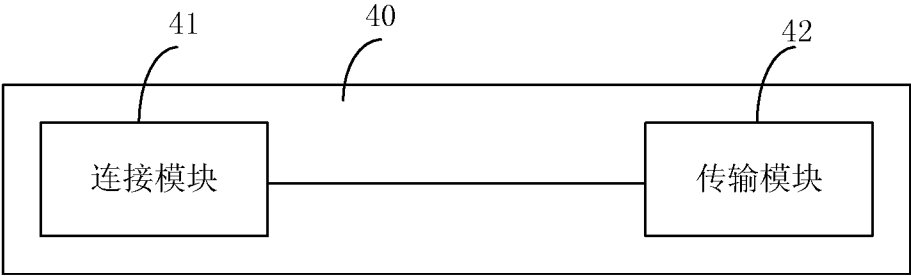


图 4

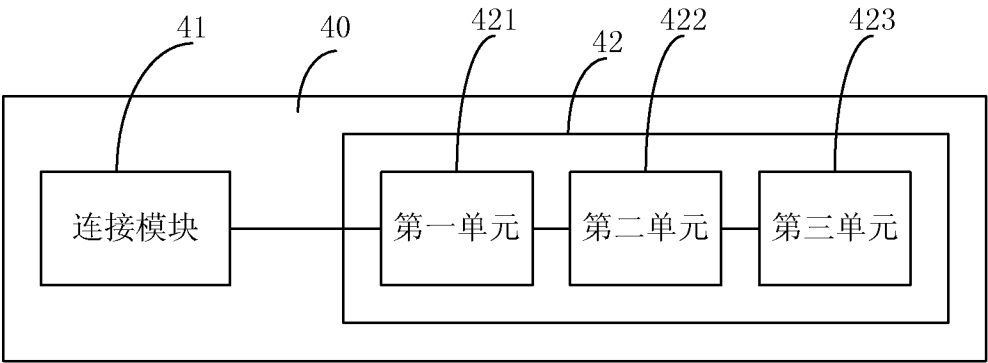


图 5

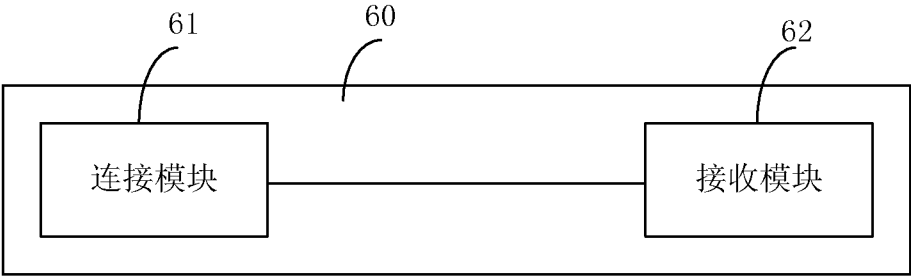


图 6

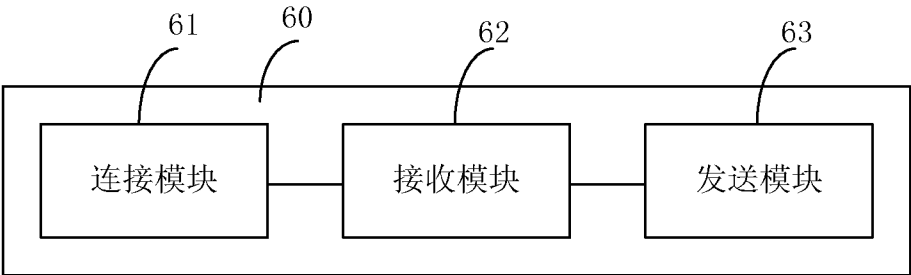


图 7

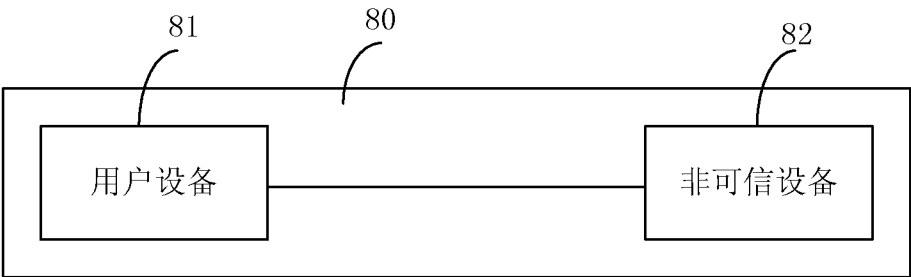


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/087468

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/82 (2013.01) 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)

G06F 21/+

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)

CPRSABS; VEN; CNKI: confident, near field, short range, user equipment, mobile phone, information, password, key, input, enter, secure, security, safety, authentic+, NFC, near filed communication, near, short, bluetooth, wifi, connect, ATM, automatic teller machine, POS, point of sale, mobile, phone, smartphone, terminal, portable, handheld, tablet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103164911 A (NATIONZ TECHNOLOGIES INC.), 19 June 2013 (19.06.2013), description, paragraphs [0029]-[0036]	1-24
X	CN 101123454 A (BEIJING JIAOTONG UNIVERSITY), 13 February 2008 (13.02.2008), claim 1	1-24
X	CN 103927655 A (XIE, Yujie), 16 July 2014 (16.07.2014), description, paragraph [0011]	1-24
X	CN 103455913 A (TENDYRON CORPORATION), 18 December 2013 (18.12.2013), description, paragraphs [0011]-[0033]	1-24
X	US 2011238573 A1 (COMPUTER ASS THINK INC.), 29 September 2011 (29.09.2011), description, paragraphs [0032]-[0039], and claims 11-15	1-24
A	CN 102054316 A (CHINA UNIONPAY CO., LTD.), 11 May 2011 (11.05.2011), the whole document	1-24

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
26 September 2016 (26.09.2016)

Date of mailing of the international search report
12 October 2016 (12.10.2016)

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
WU, Guangping
Telephone No.: (86-10) **62411829**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/087468

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103164911 A	19 June 2013	CN 103164911 B	03 February 2016
CN 101123454 A	13 February 2008	CN 101123454 B	20 April 2011
CN 103927655 A	16 July 2014	None	
CN 103455913 A	18 December 2013	None	
US 2011238573 A1	29 September 2011	WO 2011119389 A2	29 September 2011
		WO 2011119389 A3	15 December 2011
CN 102054316 A	11 May 2011	None	

国际检索报告

国际申请号

PCT/CN2016/087468

A. 主题的分类

G06F 21/82 (2013.01) 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)

G06F 21/+

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))

CPRSABS;VEN;CNKI: 信息, 密码, 口令, 输入, 安全, 可信, 近场, 近程, 蓝牙, 连接, 自动柜员机, 销售终端, 用户设备, 手机, 终端, 移动, 便携, 平板, information, password, key, input, enter, secure, security, safety, authentic+, NFC, near filed communication, near, short, bluetooth, wifi, connect, ATM, automatic teller machine, POS, point of sale, mobile, phone, smartphone, terminal, portable, handheld, tablet

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 103164911 A (国民技术股份有限公司) 2013年 6月 19日 (2013 - 06 - 19) 说明书第【0029】-【0036】段	1-24
X	CN 101123454 A (北京交通大学) 2008年 2月 13日 (2008 - 02 - 13) 权利要求1	1-24
X	CN 103927655 A (谢宇杰) 2014年 7月 16日 (2014 - 07 - 16) 说明书第【0011】段	1-24
X	CN 103455913 A (天地融科技股份有限公司) 2013年 12月 18日 (2013 - 12 - 18) 说明书第【0011】-【0033】段	1-24
X	US 2011238573 A1 (COMPUTER ASS THINK INC) 2011年 9月 29日 (2011 - 09 - 29) 说明书第【0032】-【0039】段, 权利要求11-15	1-24
A	CN 102054316 A (中国银联股份有限公司) 2011年 5月 11日 (2011 - 05 - 11) 全文	1-24

☐ 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

2016年 9月 26日

国际检索报告邮寄日期

2016年 10月 12日

ISA/CN的名称和邮寄地址

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

传真号 (86-10) 62019451

受权官员

吴广平

电话号码 (86-10) 62411829

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/087468

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	103164911	A	2013年 6月 19日	CN	103164911	B	2016年 2月 3日
CN	101123454	A	2008年 2月 13日	CN	101123454	B	2011年 4月 20日
CN	103927655	A	2014年 7月 16日	无			
CN	103455913	A	2013年 12月 18日	无			
US	2011238573	A1	2011年 9月 29日	WO	2011119389	A2	2011年 9月 29日
				WO	2011119389	A3	2011年 12月 15日
CN	102054316	A	2011年 5月 11日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)