

(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 11 月 9 日 (09.11.2017)



(10) 国际公布号
WO 2017/190633 A1

- (51) 国际专利分类号:
G06Q 20/40 (2012.01)
- (21) 国际申请号: PCT/CN2017/082457
- (22) 国际申请日: 2017 年 4 月 28 日 (28.04.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201610289386.1 2016 年 5 月 3 日 (03.05.2016) CN
- (71) 申请人: 广州广电运通金融电子股份有限公司 (GRG BANKING EQUIPMENT CO., LTD.) [CN/CN]; 中国广东省广州市高新技术产业开发区科学城科林路 9 号, Guangdong 510663 (CN)。
- (72) 发明人: 陈明宇 (CHEN, Mingyu); 中国广东省广州市高新技术产业开发区科学城科林

路 9 号, Guangdong 510663 (CN)。熊飞 (XIONG, Fei); 中国广东省广州市高新技术产业开发区科学城科林路 9 号, Guangdong 510663 (CN)。张云瑞 (ZHANG, Yunrui); 中国广东省广州市高新技术产业开发区科学城科林路 9 号, Guangdong 510663 (CN)。

(74) 代理人: 广州华进联合专利商标代理有限公司 (ADVANCE CHINA IP LAW OFFICE); 中国广东省广州市天河区花城大道 85 号 3901 房, Guangdong 510623 (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, DJ, 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, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR,

(54) Title: METHOD AND DEVICE FOR RELIABLY VERIFYING IDENTITY OF FINANCIAL CARD USER

(54) 发明名称: 验证金融卡用户身份可靠性的方法及装置

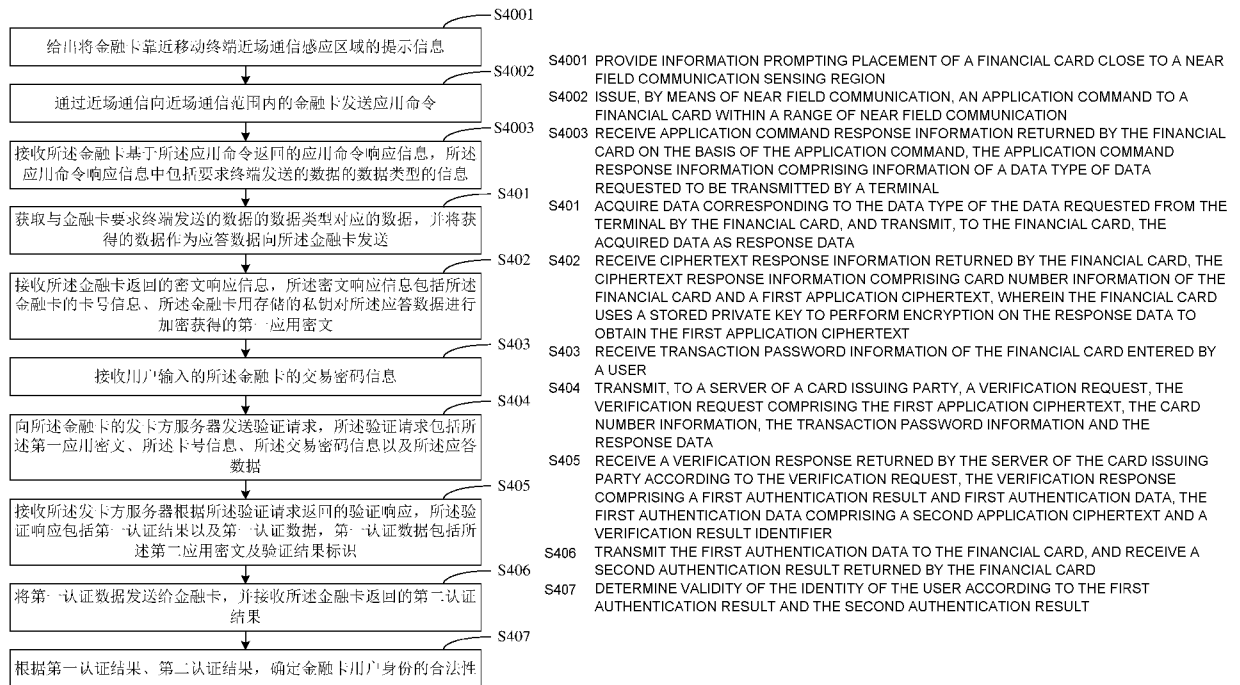


图 4

(57) Abstract: Provided are a method and device for reliably verifying the identity of a financial card user. The method comprises the following steps: transmitting, to a financial card, response data required by the financial card, interacting with the financial card to acquire ciphertext response information comprising card number information and a first application ciphertext, and receiving transaction password information entered by a user; and transmitting, to a server of a card issuing party, the ciphertext response information, the transaction password information and the response data, interacting with the server of the card issuing party to obtain a first authenti-

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))。

fication result and first authentication data, transmitting the first authentication data to the financial card, obtaining a second authentication result after the financial card has performed verification on the basis of the first authentication data, and determining validity of the identity of the user according to the first authentication result and the second authentication result. The solution disclosed in an embodiment of the invention can verify the identity of a user and issuance of a financial card in a convenient, fast and reliable manner without needing an additional hardware device, thereby preventing security risk imposed by frauds, and ensuring information security.

(57) 摘要: 一种验证金融卡用户身份可靠性的方法及装置, 该包括步骤: 将金融卡需要的应答数据发送给金融卡, 与金融卡交互获得包括卡号信息、第一应用密文的密文响应信息, 接收用户输入的交易密码信息; 将密文响应信息、交易密码信息以及应答数据发送给发卡方服务器, 与发卡方服务器进行交互获得第一认证结果以及第一认证数据, 将第一认证数据发送给金融卡, 获得金融卡基于该第一认证数据进行验证后获得的第二认证结果, 根据第一认证结果、第二认证结果, 确定用户身份的合法性。本发明实施例方案, 不需要额外的硬件设备, 即可方便、快捷、可靠地完成对用户身份和发行的验证, 避免了因欺诈所带来的安全风险, 保护了信息安全。

验证金融卡用户身份可靠性的方法及装置

技术领域

本发明涉及信息安全领域，特别是涉及一种验证金融卡用户身份可靠性的方法、一种
5 验证金融卡用户身份可靠性的装置。

背景技术

随着计算机网络的不断完善和互联网数据业务产业链的日益成熟，手机互联网用户不断增多，用户身份可靠性的验证也面临着严峻的挑战。例如，在金融领域，手机银行登录、
10 转账、查询、理财等交易都面临着身份合法性验证，目前部分银行在手机银行转账时是通过银行额外发行的 U 盾来验证用户身份的合法性，不仅增加了成本，而且 U 盾还需要随身携带，易丢失，增加了用户的使用难度。还有其它的领域，例如个人信用征信平台，其验证用户身份合法性需要银行卡、U 盾和手机，如果用户没有办理 U 盾就会存在一定的泄漏风险。此外，在移动支付领域，也同样面临用户身份合法性验证的难题。

15 对于移动设备端，手机网上银行、购物支付、转账等交易都面临用户身份合法性验证的问题，有些仅仅通过用户名和密码来实现验证，有些通过手机短信发送验证码来验证，这些方式都很容易被截取，手机也很容易被盗取，有些通过银行 U 盾或者发行加密模块验证用户身份的合法性，不仅增加了用户携带的难度，而且增加了用户的成本。

20 发明内容

基于此，本发明实施例的目的在于提供一种验证金融卡用户身份可靠性的方法、一种验证金融卡用户身份可靠性的装置，其可以快捷可靠地对金融卡用户的身份的合法性进行验证，保护信息安全。

为达到上述目的，本发明实施例采用以下技术方案：

25 一种验证金融卡用户身份可靠性的方法，包括步骤：

获取与金融卡要求终端发送的数据的数据类型对应的数据，并将获得的数据作为应答数据向所述金融卡发送；

接收所述金融卡返回的密文响应信息，所述密文响应信息包括所述金融卡的卡号信

息、所述金融卡用存储的私钥对所述应答数据进行加密获得的第一应用密文；

接收用户输入的所述金融卡的交易密码信息；

向所述金融卡的发卡方服务器发送验证请求，所述验证请求包括所述第一应用密文、所述卡号信息、所述交易密码信息以及所述应答数据；

- 5 接收所述发卡方服务器根据所述验证请求返回的验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括：所述发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文后、将该第二应用密文与所述第一应用密文进行比对获得的卡人一致性校验结果、对所述交易密码信息进行校验获得的密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证
- 10 结果标识；

将所述第一认证数据发送给所述金融卡，并接收所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定的第二认证结果；

根据所述第一认证结果、所述第二认证结果，确定金融卡用户身份的合法性。

- 15 一种验证金融卡用户身份可靠性的方法，包括步骤：

接收终端发送的应答数据，所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据；

用存储的私钥对所述应答数据进行加密获得第一应用密文，并向所述终端返回密文响应信息，所述密文响应信息包括存储的金融卡的卡号信息、所述第一应用密文；

- 20 接收所述终端发送的第一认证数据，所述第一认证数据包括第二应用密文以及验证结果标识；

将所述验证结果标识与所述第一应用密文进行处理获得过程数据，用存储的私钥对所述过程数据进行加密获得第二认证数据，并将所述第二认证数据与所述第一认证数据进行对比确定第二认证结果；

- 25 将所述第二认证结果向所述终端发送，由所述终端根据所述第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性。

一种验证金融卡用户身份可靠性的方法，包括步骤：

接收终端发送的验证请求，所述验证请求包括第一应用密文、金融卡的卡号信息、交

易密码信息以及应答数据；

获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文，并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果；

对所述交易密码信息进行校验获得密码正确性校验结果；

- 5 生成验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识；

- 10 向所述终端返回所述验证响应，由所述终端将所述第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据所述第一认证结果、所述第二认证结果确定金融卡用户身份的合法性。

一种验证金融卡用户身份可靠性的装置，包括：

数据获取模块，用于获取与金融卡要求终端发送的数据的数据类型对应的数据；

- 15 终端第一信息交互模块，用于将所述数据获取模块获得的数据作为应答数据向所述金融卡发送，并接收所述金融卡返回的密文响应信息，所述密文响应信息包括所述金融卡的卡号信息、所述金融卡用存储的私钥对所述应答数据进行加密获得的第一应用密文；将终端第二信息交互模块接收的第一认证数据发送给所述金融卡，并接收所述金融卡返回的第二认证结果；

密码信息接收模块，用于接收用户输入的所述金融卡的交易密码信息；

- 20 终端第二信息交互模块，用于向所述金融卡的发卡方服务器发送验证请求，所述验证请求包括所述第一应用密文、所述卡号信息、所述交易密码信息以及所述应答数据；并接收所述发卡方服务器根据所述验证请求返回的验证响应；

合法性判定模块，用于根据所述第一认证结果、所述第二认证结果，确定金融卡用户身份的合法性；

- 25 所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括：所述发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文后、将该第二应用密文与所述第一应用密文进行比对获得的卡人一致性校验结果、对所述交易密码信息进行校验获得的密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识；

第二认证结果由所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定。

一种验证金融卡用户身份可靠性的装置，包括：

- 5 卡端信息交互模块，接收终端发送的应答数据，所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据，并向所述终端返回密文响应信息，所述密文响应信息包括存储的金融卡的卡号信息、卡端加密模块生成的第一应用密文；以及接收所述终端发送的第一认证数据，所述第一认证数据包括第二应用密文以及验证结果标识，并将所述第二认证结果向所述终端发送，由所述终端根据认证模块
- 10 确定的第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性；

过程数据确定模块，用于将所述验证结果标识与所述第一应用密文进行处理，获得过程数据；

- 卡端加密模块，用于用存储的私钥对所述应答数据进行加密获得所述第一应用密文，
- 15 并用存储的所述私钥对所述过程数据进行加密获得第二认证数据；

认证模块，用于将所述第二认证数据与所述第一认证数据进行对比确定所述第二认证结果。

一种验证金融卡用户身份可靠性的装置，包括：

- 服务端信息交互模块，用于接收终端发送的验证请求，所述验证请求包括第一应用密文、金融卡的卡号信息、交易密码信息以及应答数据，并将验证响应生成模块生成的验证响应向所述终端发送，由所述终端将验证响应中的第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据验证响应中的第一认证结果、所述第二认证结果确定金融卡用户身份的合法性；
- 20

- 卡人一致性校验模块，用于获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文，并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果；
- 25

密码校验模块，用于对所述交易密码信息进行校验获得密码正确性校验结果；

验证响应生成模块，用于生成所述验证响应，所述验证响应包括第一认证结果以及第

一认证数据,所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果,所述第一认证数据包括所述第二应用密文及验证结果标识。

根据如上所述的本发明实施例的方案,其不需要额外的硬件设备,使用已有的金融卡结合终端(如智能手机),即可方便、快捷、可靠地完成对金融卡用户的身份和发行的验证,避免了因欺诈所带来的安全风险,保护了信息安全。本发明实施例的验证金融卡用户身份可靠性的方法和装置,可适用于移动支付等领域,结合 NFC 技术,实现对金融卡的用户身份进行验证,提高移动支付的安全性。

附图说明

- 10 图 1 是一个实施例中本发明方案的工作环境示意图;
图 2 是一个实施例中终端的组成结构示意图;
图 3 是一个实施例中发卡方服务器的组成结构示意图;
图 4 是一个实施例中本发明的验证金融卡用户身份可靠性的方法的流程示意图;
图 5 是另一个实施例中本发明的验证金融卡用户身份可靠性的方法的流程示意图;
15 图 6 是另一个实施例中本发明的验证金融卡用户身份可靠性的方法的流程示意图;
图 7 是一个具体示例的验证用户身份可靠性时的交互流程示意图;
图 8 是一个实施例中本发明的验证金融卡用户身份可靠性的装置的结构示意图。

具体实施方式

- 20 为使本发明的目的、技术方案及优点更加清楚明白,以下结合附图及实施例,对本发明进行进一步的详细说明。应当理解,此处所描述的具体实施方式仅仅用以解释本发明,并限定本发明的保护范围。

- 图1示出了本发明一个实施例中的工作环境示意图。该工作环境涉及金融卡101(如金融IC卡,或具有信息存储功能的金融卡片)、终端102(如智能手机)以及发卡方服务器103,同时还可能涉及云端支付平台100,金融卡101通过近场通信方式(NFC)与终端102进行交互,实现金融卡101方的身份可靠性的验证,终端102通过网络直接与发卡方服务器103进行交互,或者是经由云端支付平台100与发卡方服务器103进行交互,以实现发卡方服务器103方的身份可靠性验证。本发明实施例方案涉及的是终端102在需要使用金融卡

101时的对金融卡用户身份可靠性进行验证的方案。

终端102在一个实施例中的结构示意图如图2所示。该终端包括通过系统总线连接的处理器、供电模块、存储介质、内存、通信接口、显示屏幕和输入设备。其中，终端的存储介质中存储有操作系统和一种验证金融卡用户身份可靠性的装置，该验证金融卡用户身份可靠性的装置用于实现一种验证金融卡用户身份可靠性的方法。终端的通信接口用于与发卡方服务器103或者云端支付平台100连接通信。终端的输入设备用以接收用户的输入信息，例如本发明实施例中的交易密码信息。输入设备基于用户终端的类型不同可以有所不同。用户终端可以是移动终端，比如手机、平板电脑等；也可以是其它具有上述结构的设备。

发卡方服务器103在一个实施例中的结构示意图如图3所示。服务器103包括通过系统总线连接的处理器、供电模块、存储介质、内存和通信接口。其中，服务器103的存储介质存储有操作系统、数据库和一种验证金融卡用户身份可靠性的装置，该装置用于与终端102、金融卡101配合工作，并实现一种验证金融卡用户身份可靠性的方法。服务器103的通信接口用于与终端102或者云端支付平台100进行连接和通信。

图4中示出了一个实施例中的验证金融卡用户身份可靠性的方法的流程示意图，该实施例中是以终端102的处理过程为例进行说明。

如图4所示，该实施例中的方法包括：

步骤 S401：获取与金融卡要求终端发送的数据的数据类型对应的数据，并将获得的数据作为应答数据向所述金融卡发送；

步骤 S402：接收所述金融卡返回的密文响应信息，所述密文响应信息包括所述金融卡的卡号信息、所述金融卡用存储的私钥对所述应答数据进行加密获得的第一应用密文；

步骤 S403：接收用户输入的所述金融卡的交易密码信息；

步骤 S404：向所述金融卡的发卡方服务器发送验证请求，所述验证请求包括所述第一应用密文、所述卡号信息、所述交易密码信息以及所述应答数据；

步骤 S405：接收所述发卡方服务器根据所述验证请求返回的验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括：所述发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文

后、将该第二应用密文与所述第一应用密文进行比对获得的卡人一致性（金融卡与持卡人一致）校验结果、对所述交易密码信息进行校验获得的密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识；

5 步骤 S406：将所述第一认证数据发送给所述金融卡，并接收所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定的第二认证结果；

步骤 S407：根据所述第一认证结果、所述第二认证结果，确定金融卡用户身份的合法性。

10 根据如上所述的本发明实施例的方案，其不需要额外的硬件设备，使用已有的金融卡结合终端，即可方便、快捷、可靠地完成对金融卡用户身份和发行的验证，避免了因欺诈所带来的安全风险，保护了信息安全。

考虑到终端与金融卡通信的安全性，在一个具体示例中，终端可以通过近场通信（Near Field Communication，缩写为 NFC，近距离无线通讯技术，）与金融卡进行交互。
15 而上述应答数据也可以基于金融卡的需求来获取。

据此，在一个具体示例中，如图 4 所示，在上述步骤 S401 之前，本实施例中的方法还可以包括：

步骤 S4002：通过近场通信向近场通信范围内的金融卡发送应用命令；

步骤 S4003：接收所述金融卡基于所述应用命令返回的应用命令响应信息，所述应用
20 命令响应信息中包括要求终端发送的数据的数据类型的信息。

可见，基于本实施例方案，终端与金融卡通过近场通信进行交互，进而可以确保金融卡与终端之间通信过程的安全性。此外，可以在需要时再让金融卡与终端进行通信。据此，如图 4 所示，在上述步骤 S4002 之前，还可以包括：

步骤 S4001：给出将金融卡靠近终端近场通信感应区域的提示信息。

25

图 5 中示出了另一个实施例中的验证金融卡用户身份可靠性的方法的流程示意图，该实施例中是以金融卡 101 的处理过程为例进行说明。

如图 5 所示，该实施例中的方法包括：

步骤 S501: 接收终端发送的应答数据, 所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据;

步骤 S502: 用存储的私钥对所述应答数据进行加密获得第一应用密文, 并向所述终端返回密文响应信息, 所述密文响应信息包括存储的金融卡的卡号信息、所述第一应用密文;

5 步骤 S503: 接收所述终端发送的第一认证数据, 所述第一认证数据包括第二应用密文以及验证结果标识;

步骤 S504: 将所述验证结果标识与所述第一应用密文进行处理获得过程数据, 用存储的私钥对所述过程数据进行加密获得第二认证数据, 并将该第二认证数据与所述第一认证数据进行对比确定第二认证结果;

10 步骤 S505: 将所述第二认证结果向所述终端发送, 由所述终端根据所述第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性。

考虑到终端与金融卡通信的安全性, 在一个具体示例中, 终端可以通过近场通信 (Near Field Communication, 缩写为 NFC, 近距离无线通讯技术,) 与金融卡进行交互。而上述应答数据也可以基于金融卡的需求来获取。

15 据此, 在一个具体示例中, 如图 5 所示, 在上述步骤 S501 之前, 本实施例中的方法还可以包括:

步骤 S5001: 接收终端通过近场通信发送的应用命令;

步骤 S5002: 根据所述应用命令向所述终端返回应用命令响应信息, 所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

20 图 6 中示出了另一个实施例中的验证金融卡用户身份可靠性的方法的流程示意图, 该实施例中是以发卡方服务器 103 的处理为例进行说明。

如图 6 所示, 该实施例中的方法包括:

25 步骤 S601: 接收终端发送的验证请求, 所述验证请求包括第一应用密文、金融卡的卡号信息、交易密码信息以及应答数据;

步骤 S602: 获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文, 并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果;

步骤 S603：对所述交易密码信息进行校验获得密码正确性校验结果；

步骤 S604：生成验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识；

5 步骤 S605：向所述终端返回所述验证响应，由所述终端将所述第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据所述第一认证结果、所述第二认证结果确定金融卡用户身份的合法性。

为了更好的理解发明实施例的方法，图 7 中示出了一个具体示例中验证用户身份可靠
10 性时的交互流程示意图。考虑到移动终端身份的可靠性验证的应用和需求较为普遍，在图 7 所示示例的说明中，是以终端 102 为移动终端为例进行说明，本领域技术人员可以理解，只要能够执行本发明实施例方案中的验证方案的相关功能，除了移动终端之外的其他终端同样适用。

在需要进行用户身份可靠性的验证时，例如在使用电子钱包等进行移动支付时，使用
15 金融终端过程中的安全验证时（例如手机银行 APP 软件等），购物类软件进行登陆或者进行购物时的身份验证时等等，如图 7 所示，移动终端可以先给出将金融卡靠近移动终端近场通信感应区域的提示信息，该提示信息可以采用任何可能的方式进行，例如在移动终端的相关显示界面上进行显示、通过语音进行语音提醒、显示界面的显示与语音提醒同时进行等等。

20 基于该提示信息，用户可将金融卡放置或者靠近移动终端近场通信的感应区域，移动终端通过近场通信向其近场通信范围内的金融卡发送应用命令。

金融卡接收到该应用命令后，激活移动终端所选择的相关应用，使金融卡处于开始状态，并向移动终端返回应用命令响应信息，该应用命令响应信息中包括要求终端发送的数据的数据类型的信息。在一个具体示例中，该应用命令响应信息中的数据类型的信息，可
25 以是以数据类型列表的方式发送。

以支付、购物等交易支付过程中的用户身份可靠性验证为例，在一个具体示例中，这里的数据类型可以是包括：交易时间、交易类型、交易金额、交易货币代码、随机数、终端性能。本领域技术人员可以理解，基于实际交易过程的需要，还可以是其他的数据类型。

移动终端接收到该命令响应信息后，获取与金融卡要求终端发送的数据的数据类型对应的数据，并将获得的数据组成应答数据向所述金融卡发送。如上所述，在发送应答数据发送时，也是通过近场通信（NFC）发送给金融卡。在一个具体示例中，所获得的数据，可以是以数据列表的方式作为应答数据发送给金融卡。

5 金融卡接收到该应答数据后，用金融卡自身存储的私钥对该应答数据进行加密获得应用密文（为便于与其他密文区分，在此称为第一应用密文），并向移动终端返回密文响应信息，该密文响应信息中包括有该金融卡存储的金融卡的卡号信息、以及上述第一应用密文。

10 移动终端接收到该密文响应信息后，可以给出让用户输入该金融卡的交易密码的提示信息，该提示信息可以通过语音进行提示，也可以是直接通过密码输入界面进行提示，也可以是密码输入界面与语音提示同时进行，并接收用户通过密码输入界面或者密码输入设备输入的该金融卡的交易密码信息。

15 随后，移动终端向该金融卡的发卡方服务器发送验证请求，在通过云端支付平台 100 进行支付交易的情况下，移动终端将该验证请求发送给该云端支付平台，由云端支付平台 15 发送给发卡方服务器。该验证请求中包括有：上述第一应用密文、上述卡号信息、上述交易密码信息以及上述应答数据。可以理解的是，为了加强移动终端与发卡方服务器通信过程的安全性，移动终端在发送该验证请求时，可以是加密之后在发送，相对应地，发卡方服务器在接收到该加密的验证请求后，再执行后续的操作。具体的加解密方式可以采用任何可能的加解密方式进行，本发明实施例不做具体限定。出于简便说明的目的，下述说明 20 中未对加解密过程进行说明。

25 发卡方服务器接收到该验证请求后，获取存储的与验证请求中的卡号信息对应的私钥，采用该私钥对验证请求中的应答数据进行加密获得应用密文（为便于区分，称之为第二应用密文），并将第二应用密文与验证请求中的第一应用密文进行比对，从而获得卡人一致性校验结果。可以理解的是，通常情况下，由于获得第一应用密文、第二应用密文的 25 加密方式是一样的，因此，正常情况下，所获得的第二应用密文应当是与第一应用密文是一致的，即在第二应用密文与第一应用密文一致的情况下，发卡方即可判定卡人是一致的，否则是不一致的。

此外，发卡方服务器还基于验证请求中的账号信息对验证请求中的交易密码信息进行

校验，判断校验请求中的交易密码是否与存储的该账号信息对应的信息是否一致，从而获得密码正确性校验结果。对密码进行校验的方式，可以采用目前已有以及以后可能出现的任何方式进行。

随后，发卡方服务器生成验证响应，并将该验证响应向移动终端发送，或者是通过云端交易平台发送给移动终端。该验证响应中包括有第一认证结果以及第一认证数据，其中，第一认证结果包括上述卡人一致性校验结果、上述密码正确性校验结果，第一认证数据包括上述第二应用密文及生成的验证结果标识。其中，该第一认证数据中，第二应用密文和验证结果标识的组合方式，可以是任何可能的方式，例如验证结果标识可以是第一认证数据中的在后的字节或者是在前的字节。

移动终端接收到该验证响应后，将第一认证数据发送给金融卡。

金融卡接收到该验证响应后，将第一认证数据中的验证结果标识与上述自身生成的第一应用密文进行处理获得过程数据，并用金融卡自身存储的私钥对该过程数据进行加密获得第二认证数据，并将该第二认证数据与上述第一认证数据进行对比，确定第二认证结果，并将该第二认证结果发送给移动终端。金融卡可以采用任何方式对验证结果标识与第一应用密文进行处理获得过程数据，在一个具体示例中，可以是将验证结果标识与第一应用密文进行异或处理获得上述过程数据。

移动终端在接收到第二认证结果后，将第二认证结果与第一认证结果结合，确定用户身份的合法性。其中，第一认证结果代表了发卡方服务器对卡人一致性的认证结果，第二认证结果代表了金融卡对卡人一致性的认证结果，二者的结合进一步加强了金融卡用户身份合法性验证的可靠性。

在用在交易支付系统的情况下，在确认了金融卡用户身份的合法性之后，移动终端可以进一步确定交易支付结果，并将交易支付结果进行显示，以告知用户认证结果和交易支付结果。

基于与上述方法相同的思想，本发明实施例还提供一种验证金融卡用户身份可靠性的装置，图 8 中示出了一个具体示例中的装置的结构示意图。在图 8 所示的结构示意图中，是以结合了设置在金融卡上的装置 81、设置在终端上的装置 82 以及设置在发卡方服务器上的装置 83 为例进行说明。

如图 8 所示，在一个具体示例中，设置在终端 82 上的验证金融卡用户身份可靠性的装置包括：

数据获取模块 822，用于获取与金融卡 81 要求终端 82 发送的数据的数据类型对应的数据；

5 终端第一信息交互模块 823，用于将数据获取模块 822 获得的数据作为应答数据向金融卡 81 发送，并接收金融卡 81 返回的密文响应信息，该密文响应信息包括金融卡 81 的卡号信息、金融卡 81 用存储的私钥对所述应答数据进行加密获得的第一应用密文；还用于将终端第二信息交互模块 825 接收的第一认证数据发送给金融卡 81，并接收金融卡 81 返回的第二认证结果；

10 密码信息接收模块 824，用于接收用户输入的金融卡 81 的交易密码信息；

终端第二信息交互模块 825，用于向金融卡的发卡方服务器 83 发送验证请求，该验证请求包括上述第一应用密文、上述卡号信息、上述交易密码信息以及上述应答数据；并接收发卡方服务器 83 根据该验证请求返回的验证响应；

合法性判定模块 826，用于根据上述第一认证结果、上述第二认证结果，确定金融卡
15 用户身份的合法性。

其中，上述验证响应包括第一认证结果以及第一认证数据，第一认证结果包括：发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对应答数据进行加密获得第二应用密文后、将该第二应用密文与第一应用密文进行比对获得的卡人一致性校验结果、对交易密码信息进行校验获得的密码正确性校验结果，上述第一认证数据包括所述第二应
20 用密文及验证结果标识；

上述第二认证结果由所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定。

相对应地，如图 8 所示，在该具体示例中，设置在金融卡 81 的验证金融卡用户身份
25 可靠性的装置包括：

卡端信息交互模块 811，接收终端 82 发送的应答数据，所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据，并向所述终端返回密文响应信息，所述密文响应信息包括存储的金融卡的卡号信息、卡端加密模块生

成的第一应用密文；以及接收所述终端发送的第一认证数据，所述第一认证数据包括第二应用密文以及验证结果标识，并将所述第二认证结果向所述终端发送，由所述终端根据认证模块确定的第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性；

- 5 过程数据确定模块 812，用于将所述验证结果标识与所述第一应用密文进行处理，获得过程数据；

卡端加密模块 813，用于用存储的私钥对所述应答数据进行加密获得所述第一应用密文，并用存储的所述私钥对所述过程数据进行加密获得第二认证数据；

- 10 认证模块 814，用于将所述第二认证数据与所述第一认证数据进行对比确定所述第二认证结果。

相对应地，如图 8 所示，在该具体示例中，设置在发卡方服务器 83 的验证金融卡用户身份可靠性的装置包括：

- 15 服务端信息交互模块 831，用于接收终端发送的验证请求，所述验证请求包括第一应用密文、金融卡的卡号信息、交易密码信息以及应答数据，并将验证响应生成模块生成的验证响应向所述终端发送，由所述终端将验证响应中的第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据验证响应中的第一认证结果、所述第二认证结果确定金融卡用户身份的合法性；

- 20 卡人一致性校验模块 832，用于获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文，并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果；

密码校验模块 833，用于对所述交易密码信息进行校验获得密码正确性校验结果；

验证响应生成模块 834，用于生成所述验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识。

- 25 考虑到终端与金融卡通信的安全性，在一个具体示例中，终端可以通过近场通信（Near Field Communication，缩写为 NFC，近距离无线通讯技术，）与金融卡进行交互。而上述应答数据也可以基于金融卡的需求来获取。

据此，在一个具体示例中：

上述终端第一信息交互模块 823，还通过近场通信向近场通信范围内的金融卡发送应用命令；并接收所述金融卡基于所述应用命令返回的应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

5 相对应地，上述卡端信息交互模块 811，还用于接收终端通过近场通信发送的应用命令；并根据所述应用命令向所述终端返回应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

可见，基于本实施例方案，终端与金融卡通过近场通信进行交互，进而可以确保金融卡与终端之间通信过程的安全性。

10 此外，可以在需要时再让金融卡与终端进行通信，据此，如图 8 所示，设置在终端 82 上的验证金融卡用户身份可靠性的装置还可以包括：

信息提示模块 821，用于给出将金融卡靠近终端近场通信感应区域的提示信息。

15 如上所述的本发明实施例的装置，可以应用到任何需要结合金融卡对金融卡用户身份的合法性和可靠性进行验证的领域，例如交易支付。以交易支付为例，在交易支付的应用场景，上述应答数据可以包括：交易时间、交易类型、交易金额、交易货币代码、随机数、终端性能信息。

此时，结合图 8 所示，在此情况下，设置在终端 82 上的验证金融卡用户身份可靠性的装置还可以包括：

交易结果确定模块 827，用于根据合法性判定模块 826 确定的金融卡用户身份的合法性确定交易支付结果，并将交易支付结果进行显示。

20 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一非易失性的计算机可读取存储介质中，如本发明实施例中，该程序可存储于计算机系统的存储介质中，并被该计算机系统至少一个处理器执行，以实现包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

25

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛

盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范

5 围。因此，本发明的保护范围应以所附权利要求为准。

权利要求书

1、一种验证金融卡用户身份可靠性的方法，其特征在于，包括步骤：

获取与金融卡要求终端发送的数据的数据类型对应的数据，并将获得的数据作为应答数据向所述金融卡发送；

5 接收所述金融卡返回的密文响应信息，所述密文响应信息包括所述金融卡的卡号信息、所述金融卡用存储的私钥对所述应答数据进行加密获得的第一应用密文；

接收用户输入的所述金融卡的交易密码信息；

向所述金融卡的发卡方服务器发送验证请求，所述验证请求包括所述第一应用密文、所述卡号信息、所述交易密码信息以及所述应答数据；

10 接收所述发卡方服务器根据所述验证请求返回的验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括：所述发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文后、将该第二应用密文与所述第一应用密文进行比对获得的卡人一致性校验结果、对所述交易密码信息进行校验获得的密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证
15 结果标识；

将所述第一认证数据发送给所述金融卡，并接收所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定的第二认证结果；

根据所述第一认证结果、所述第二认证结果，确定金融卡用户身份的合法性。

20 2、根据权利要求 1 所述的验证金融卡用户身份可靠性的方法，其特征在于，在获取与金融卡要求终端发送的数据的数据类型对应的数据之前，还包括步骤：

通过近场通信向近场通信范围内的金融卡发送应用命令；

接收所述金融卡基于所述应用命令返回的应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

25 3、根据权利要求 1 或 2 所述的验证金融卡用户身份可靠性的方法，其特征在于，还包括步骤：根据确定的金融卡用户身份的合法性确定交易支付结果，并将交易支付结果进行显示。

4、一种验证金融卡用户身份可靠性的方法，其特征在于，包括步骤：

接收终端发送的应答数据，所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据；

用存储的私钥对所述应答数据进行加密获得第一应用密文，并向所述终端返回密文响应信息，所述密文响应信息包括存储的金融卡的卡号信息、所述第一应用密文；

- 5 接收所述终端发送的第一认证数据，所述第一认证数据包括第二应用密文以及验证结果标识；

将所述验证结果标识与所述第一应用密文进行处理获得过程数据，用存储的私钥对所述过程数据进行加密获得第二认证数据，并将该第二认证数据与所述第一认证数据进行对比确定第二认证结果；

- 10 将所述第二认证结果向所述终端发送，由所述终端根据所述第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性。

5、根据权利要求 4 所述的验证金融卡用户身份可靠性的方法，其特征在于，在接收终端发送的应答数据之前，还包括步骤：

接收终端通过近场通信发送的应用命令；

- 15 根据所述应用命令向所述终端返回应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

6、一种验证金融卡用户身份可靠性的方法，其特征在于，包括步骤：

接收终端发送的验证请求，所述验证请求包括第一应用密文、金融卡的卡号信息、交易密码信息以及应答数据；

- 20 获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文，并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果；

对所述交易密码信息进行校验获得密码正确性校验结果；

生成验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果，所述第一认证数据包括所述

- 25 第二应用密文及验证结果标识；

向所述终端返回所述验证响应，由所述终端将所述第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据所述第一认证结果、所述第二认证结果确定金融卡用户身份的合法性。

7、一种验证金融卡用户身份可靠性的装置，其特征在于，包括：

数据获取模块，用于获取与金融卡要求终端发送的数据的数据类型对应的数据；

终端第一信息交互模块，用于将所述数据获取模块获得的数据作为应答数据向所述金融卡发送，并接收所述金融卡返回的密文响应信息，所述密文响应信息包括所述金融卡的卡号信息、所述金融卡用存储的私钥对所述应答数据进行加密获得的第一应用密文；将终端第二信息交互模块接收的第一认证数据发送给所述金融卡，并接收所述金融卡返回的第二认证结果；

密码信息接收模块，用于接收用户输入的所述金融卡的交易密码信息；

终端第二信息交互模块，用于向所述金融卡的发卡方服务器发送验证请求，所述验证请求包括所述第一应用密文、所述卡号信息、所述交易密码信息以及所述应答数据；并接收所述发卡方服务器根据所述验证请求返回的验证响应；

合法性判定模块，用于根据所述第一认证结果、所述第二认证结果，确定金融卡用户身份的合法性；

所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括：所述发卡方服务器获取存储的与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文后、将该第二应用密文与所述第一应用密文进行比对获得的卡人一致性校验结果、对所述交易密码信息进行校验获得的密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识；

第二认证结果由所述金融卡将所述验证结果标识与所述第一应用密文进行处理获得过程数据、用存储的私钥对所述过程数据进行加密获得第二认证数据后、将所述第二认证数据与所述第一认证数据进行对比确定。

8、根据权利要求7所述的验证金融卡用户身份可靠性的装置，其特征在于，

所述终端第一信息交互模块，还通过近场通信向近场通信范围内的金融卡发送应用命令；并接收所述金融卡基于所述应用命令返回的应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

9、根据权利要求7或8所述的验证金融卡用户身份可靠性的装置，其特征在于，还包括：

交易结果确定模块，用于根据所述合法性判定模块确定的金融卡用户身份的合法性确

定交易支付结果，并将交易支付结果进行显示。

10、一种验证金融卡用户身份可靠性的装置，其特征在于，包括：

卡端信息交互模块，接收终端发送的应答数据，所述应答数据包括所述终端根据金融卡要求终端发送的数据的数据类型获取的与所述数据类型对应的数据，并向所述终端返回
5 密文响应信息，所述密文响应信息包括存储的金融卡的卡号信息、卡端加密模块生成的第一应用密文；以及接收所述终端发送的第一认证数据，所述第一认证数据包括第二应用密文以及验证结果标识，并将所述第二认证结果向所述终端发送，由所述终端根据认证模块确定的第二认证结果以及发卡方服务器返回的第一认证结果确定金融卡用户身份的合法性；

10 过程数据确定模块，用于将所述验证结果标识与所述第一应用密文进行处理，获得过程数据；

卡端加密模块，用于用存储的私钥对所述应答数据进行加密获得所述第一应用密文，并用存储的所述私钥对所述过程数据进行加密获得第二认证数据；

15 认证模块，用于将所述第二认证数据与所述第一认证数据进行对比确定所述第二认证结果。

11、根据权利要求 10 所述的验证金融卡用户身份可靠性的装置，其特征在于：

所述卡端信息交互模块，还用于接收终端通过近场通信发送的应用命令；并根据所述应用命令向所述终端返回应用命令响应信息，所述应用命令响应信息中包括要求终端发送的数据的数据类型的信息。

20 12、一种验证金融卡用户身份可靠性的装置，其特征在于，包括：

服务端信息交互模块，用于接收终端发送的验证请求，所述验证请求包括第一应用密文、金融卡的卡号信息、交易密码信息以及应答数据，并将验证响应生成模块生成的验证响应向所述终端发送，由所述终端将验证响应中的第一认证数据发送给金融卡、接收到金融卡返回的第二认证结果后，根据验证响应中的第一认证结果、所述第二认证结果确定金融卡用户身份的合法性；
25

卡人一致性校验模块，用于获取与所述卡号信息对应的私钥、采用该私钥对所述应答数据进行加密获得第二应用密文，并将该第二应用密文与所述第一应用密文进行比对获得卡人一致性校验结果；

密码校验模块，用于对所述交易密码信息进行校验获得密码正确性校验结果；

验证响应生成模块，用于生成所述验证响应，所述验证响应包括第一认证结果以及第一认证数据，所述第一认证结果包括所述卡人一致性校验结果、所述密码正确性校验结果，所述第一认证数据包括所述第二应用密文及验证结果标识。

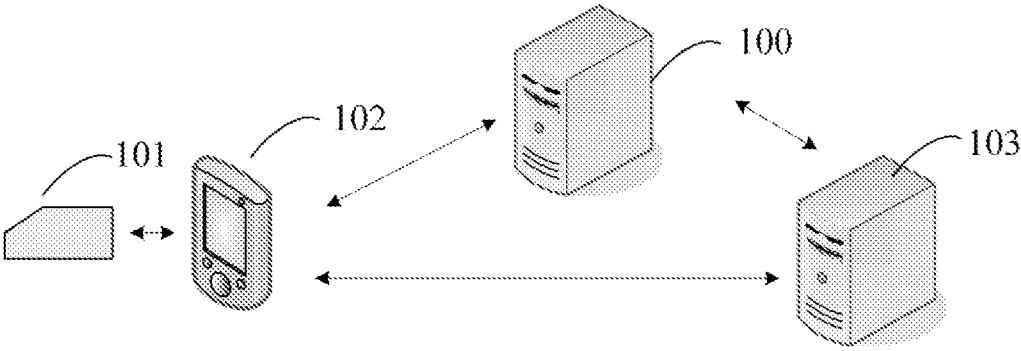


图 1

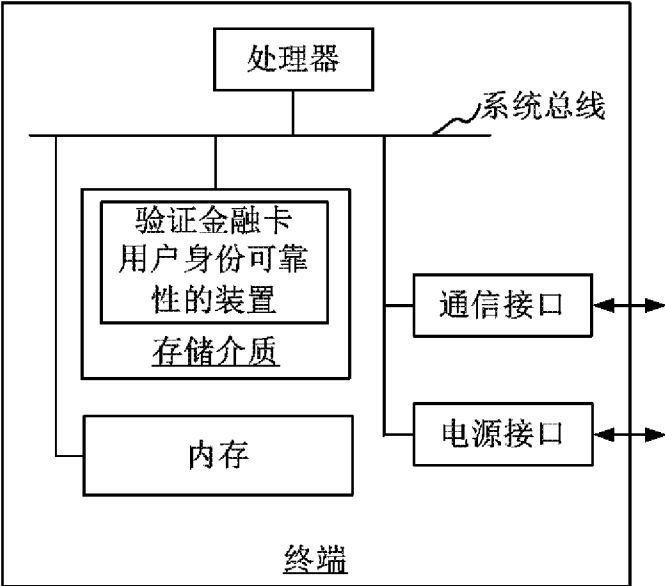


图 2

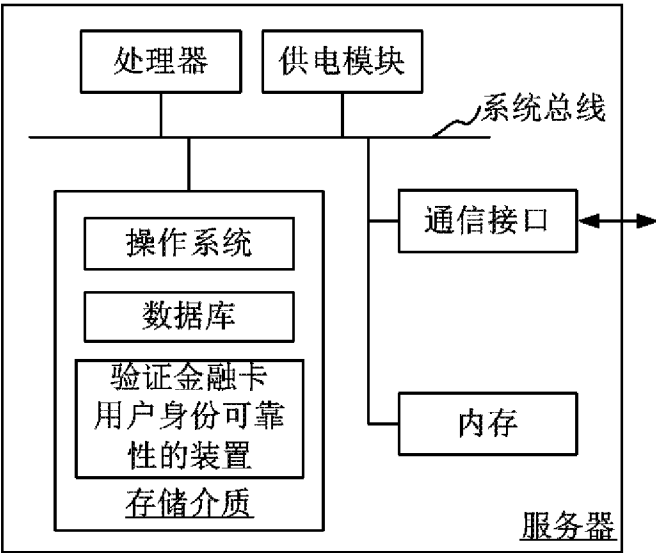


图 3

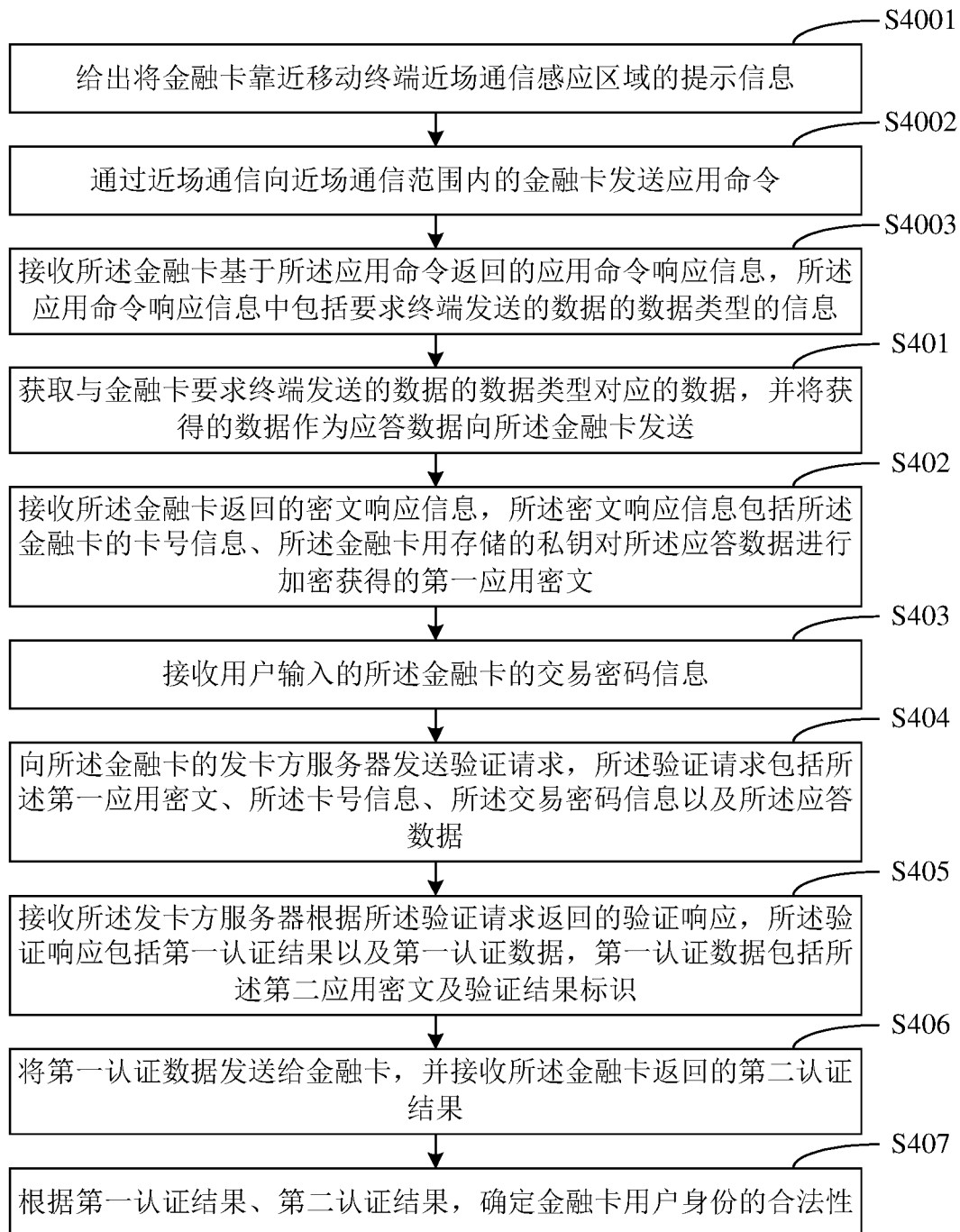


图 4

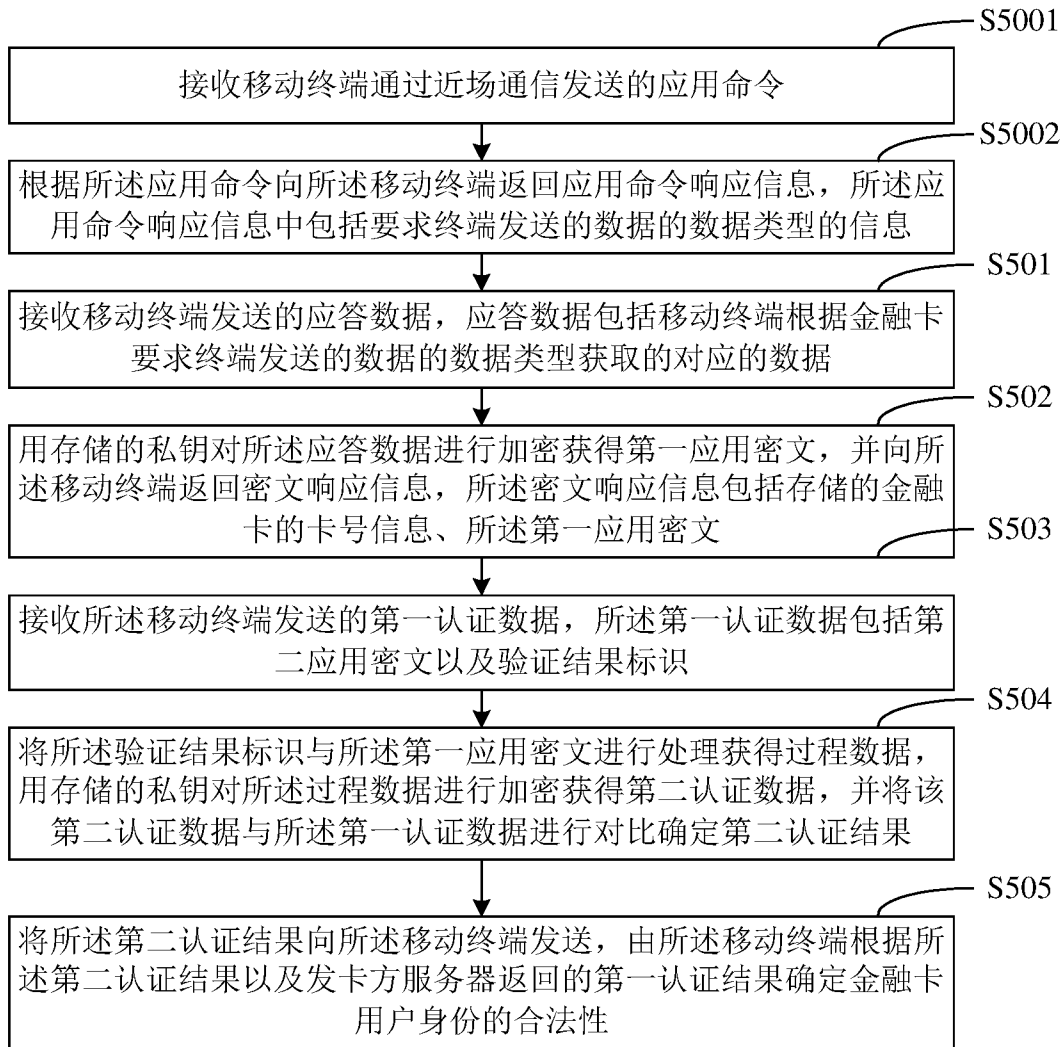


图 5

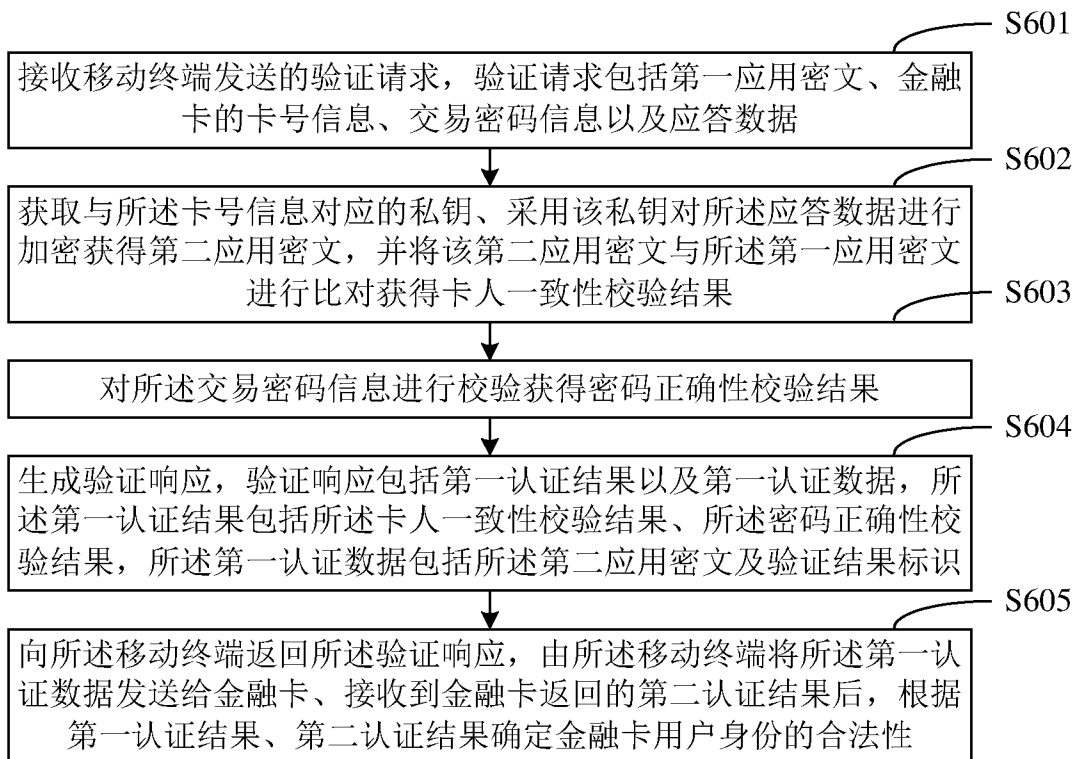


图 6

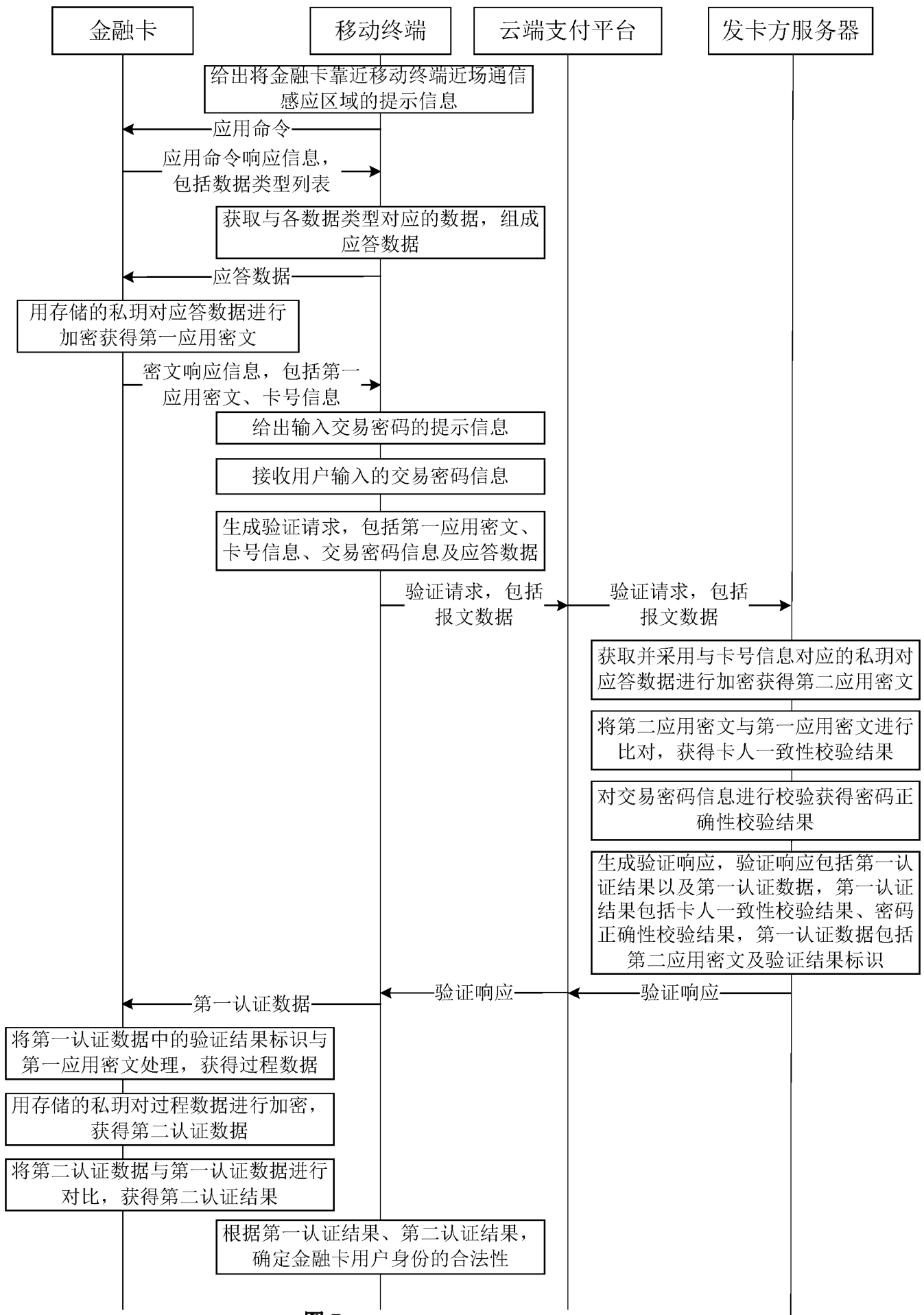


图 7

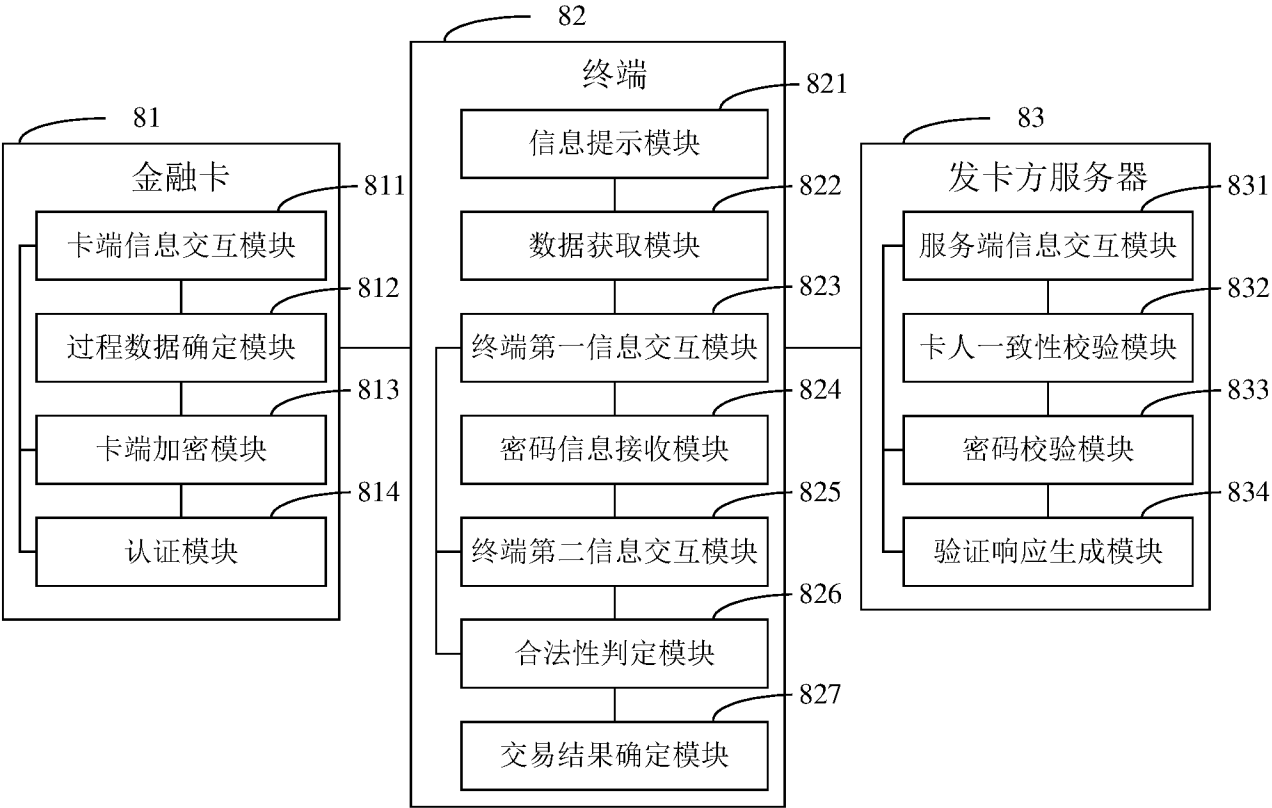


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2017/082457

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40 (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)

H04L; 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)

CPRSABS;CNTXT;CNKI;VEN:ciphertext, password, decryption, encryption, near field, transaction, card-issuing party, card issuer, card number, legal, NFC, key, pay, trade, deal, card, issu+, verif+, authentic+, valid+, identifi+, respons+, request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105897721 A (GRG BANKING EQUIPMENT CO., LTD.), 24 August 2016 (24.08.2016), claims 1-12	1-12
A	CN 104021473 A (LIU, Jintong), 03 September 2014 (03.09.2014), the whole document	1-12
A	CN 101710433 A (SHENZHEN NETCOM ELECTRONICS CO., LTD. et al.), 19 May 2010 (19.05.2010), the whole document	1-12
A	CN 104408620 A (DATA ASSURANCE & COMMUNICATION SECURITY RESEARCH CENTER, CHINESE ACADEMY OF SCIENCES), 11 March 2015 (11.03.2015), the whole document	1-12
A	CN 101162535 A (CHINA UNIONPAY CO., LTD.), 16 April 2008 (16.04.2008), the whole document	1-12
A	EP 2889823 A1 (GEMALTO SA), 01 July 2015 (01.07.2015), the whole document	1-12

☐ 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 15 June 2017 (15.06.2017)	Date of mailing of the international search report 28 July 2017 (28.07.2017)
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 MAO, Yunnan Telephone No.: (86-10) 62089144

International application No.
PCT/CN2017/082457

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 G06Q 20/40(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) H04L; 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)) CPRSABS;CNTXT;CNKI;VEN:密文, 密码, 解密, 加密, 近场, 支付, 交易, 发卡方, 发卡机构, 卡号, 校验, 验证, 合法, 标识, 响应, 请求, NFC, key, pay, trade, deal, card, issu+, verif+, authentic+, valid+, identifi+, respons+, request																							
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 105897721 A (广州广电运通金融电子股份有限公司) 2016年 8月 24日 (2016 - 08 - 24) 权利要求1-12</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 104021473 A (刘劲彤) 2014年 9月 3日 (2014 - 09 - 03) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 101710433 A (深圳市江波龙电子有限公司等) 2010年 5月 19日 (2010 - 05 - 19) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 104408620 A (中国科学院数据与通信保护研究教育中心) 2015年 3月 11日 (2015 - 03 - 11) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 101162535 A (中国银联股份有限公司) 2008年 4月 16日 (2008 - 04 - 16) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>EP 2889823 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 全文</td> <td>1-12</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 105897721 A (广州广电运通金融电子股份有限公司) 2016年 8月 24日 (2016 - 08 - 24) 权利要求1-12	1-12	A	CN 104021473 A (刘劲彤) 2014年 9月 3日 (2014 - 09 - 03) 全文	1-12	A	CN 101710433 A (深圳市江波龙电子有限公司等) 2010年 5月 19日 (2010 - 05 - 19) 全文	1-12	A	CN 104408620 A (中国科学院数据与通信保护研究教育中心) 2015年 3月 11日 (2015 - 03 - 11) 全文	1-12	A	CN 101162535 A (中国银联股份有限公司) 2008年 4月 16日 (2008 - 04 - 16) 全文	1-12	A	EP 2889823 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 全文	1-12
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																					
PX	CN 105897721 A (广州广电运通金融电子股份有限公司) 2016年 8月 24日 (2016 - 08 - 24) 权利要求1-12	1-12																					
A	CN 104021473 A (刘劲彤) 2014年 9月 3日 (2014 - 09 - 03) 全文	1-12																					
A	CN 101710433 A (深圳市江波龙电子有限公司等) 2010年 5月 19日 (2010 - 05 - 19) 全文	1-12																					
A	CN 104408620 A (中国科学院数据与通信保护研究教育中心) 2015年 3月 11日 (2015 - 03 - 11) 全文	1-12																					
A	CN 101162535 A (中国银联股份有限公司) 2008年 4月 16日 (2008 - 04 - 16) 全文	1-12																					
A	EP 2889823 A1 (GEMALTO SA) 2015年 7月 1日 (2015 - 07 - 01) 全文	1-12																					
☐ 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 2017年 6月 15日		国际检索报告邮寄日期 2017年 7月 28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		授权官员 毛韵楠 电话号码 (86-10)62089144																					

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/082457

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	105897721	A	2016年 8月 24日	无			
CN	104021473	A	2014年 9月 3日	WO	2015180578	A1	2015年 12月 3日
CN	101710433	A	2010年 5月 19日	EP	2204782	A1	2010年 7月 7日
				US	2010163618	A1	2010年 7月 1日
CN	104408620	A	2015年 3月 11日	无			
CN	101162535	A	2008年 4月 16日	CN	101162535	B	2011年 1月 12日
EP	2889823	A1	2015年 7月 1日	WO	2015101439	A1	2015年 7月 9日