

(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
2016 年 5 月 12 日 (12.05.2016)



(10) 国际公布号
WO 2016/070799 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2015/093729
- (22) 国际申请日: 2015 年 11 月 3 日 (03.11.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410643056.9 2014 年 11 月 7 日 (07.11.2014) CN
201410643670.5 2014 年 11 月 7 日 (07.11.2014) CN
201510054772.8 2015 年 2 月 3 日 (03.02.2015) CN
201510055973.X 2015 年 2 月 3 日 (03.02.2015) CN
- (71) 申请人: 天地融科技股份有限公司 (TENDYRON CORPORATION) [CN/CN]; 中国北京市海淀区学清路 38 号 B 座 1810, Beijing 100083 (CN)。
- (72) 发明人: 李东声 (LI, Dongsheng); 中国北京市海淀区学清路 38 号 B 座 1810, Beijing 100083 (CN)。
- (74) 代理人: 北京清亦华知识产权代理事务所 (普通合伙) (TSINGYIHUA INTELLECTUAL PROP-

ERTY LLC); 中国北京市海淀区清华园清华大学照澜院商业楼 301 室, Beijing 100084 (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)。

[见续页]

(54) Title: DATA INTERACTION METHOD AND SYSTEM

(54) 发明名称: 数据交互方法和系统

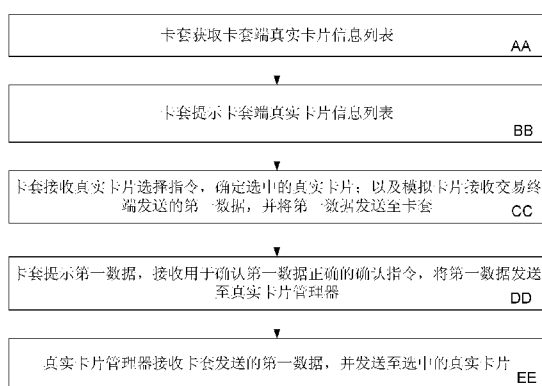


图 1 / FIG. 1

- AA A card sleeve acquires a card sleeve-end real card information list
- BB The card sleeve gives a prompt about the card sleeve-end real card information list
- CC The card sleeve receives a real card choosing instruction and determines a chosen real card; and a simulation card receives first data sent by a transaction terminal and sends the first data to the card sleeve
- DD The card sleeve gives a prompt about the first data, receives a confirmation instruction for confirming that the first data is correct, and sends the first data to a real card manager
- EE The real card manager receives the first data sent by the card sleeve and sends the first data to the chosen real card

(57) Abstract: A data secure interaction method and system, wherein the method comprises: a card sleeve acquiring a card sleeve-end real card information list, and the card sleeve giving a prompt about the card sleeve-end real card information list; the card sleeve receiving a real card choosing instruction and determining a chosen real card; and a simulation card receiving first data sent by a transaction terminal and sending the first data to the card sleeve; the card sleeve giving a prompt about the first data, receiving a confirmation instruction for confirming that the first data is correct, and sending the first data to a real card manager; the real card manager receiving the first data sent by the card sleeve and sending the first data to the chosen real card. Through this data interaction method, data interaction among the simulation card, the card sleeve and the real card manager can be realized, in order to provide a data interaction solution that is not only convenient for a user to carry, but also higher in security.

(57) 摘要: 一种数据安全交互方法和系统, 其中所述方法包括: 卡套获取卡套端真实卡片信息列表, 卡套提示卡套端真实卡片信息列表; 卡套接收真实卡片选择指令, 确定选中的真实卡片; 以及模拟卡片接收交易终端发送的第一数据, 并将第一数据发送至卡套; 卡套提示第一数据, 接收用于确认第一数据正确的确认指令, 将第一数据发送至真实卡片管理器; 真实卡片管理器接收卡套发送的第一数据, 并发送至选中的真实卡片。通过该数据交互方法可以提供一种既方便用户携带, 且安全性较高的数据

以实现模拟卡片、卡套与真实卡片管理器之间的数据交互, 交互解决方案。



WO 2016/070799 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

数据交互方法和系统

技术领域

本发明涉及电子信息安全技术领域，尤其涉及一种数据交互方法和系统。

5

背景技术

现有交易流程中，例如：取款或者购物刷卡，通常用户需要随身携带从银行办理的银行卡，用户随身携带银行卡存在一定的安全风险，一旦丢失，则容易对用户的资产造成损失。另外，由于银行卡种类多种多样，一个用户可能同时拥有多张不同银行的银行卡，如
10 需随身携带多张不同银行的银行卡，也不够便携，如果为了方便携带，仅携带了多张银行卡中的某些银行卡时，在使用这些银行卡进行取款或者购物刷卡时，可能存在跨行交易，导致交易中发生不必要的费用。

因此，现有技术中急需提供一种既方便用户携带，且安全性较高的交易解决方案。

15 发明内容

本发明旨在解决上述问题。

本发明的一个主要目的在于提供一种数据交互方法。

为达到上述目的，本发明的技术方案具体是这样实现的：

本发明一方面提供了一种数据交互方法，包括：卡套获取卡套端真实卡片信息列表，
20 其中，卡套端真实卡片信息列表为卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；卡套提示卡套端真实卡片信息列表；卡套接收真实卡片选择指令，确定选中的真实卡片；以及模拟卡片接收交易终端发送的第一数据，并将第一数据发送至卡套；卡套提示第一数据，接收用于确认第一数据正确的确认指令，将第一数据发送至真实
25 卡片管理器；真实卡片管理器接收卡套发送的第一数据，并发送至选中的真实卡片。

此外，数据交互方法还包括：卡套与模拟卡片建立安全连接，获得卡套与模拟卡片之间进行数据安全传输的卡套端第一安全传输密钥和模拟卡片端安全传输密钥。

此外，卡套与模拟卡片建立安全连接包括：卡套向模拟卡片发送用于指示建立安全连接的第一安全连接指令，其中，第一安全连接指令包括：卡套利用模拟卡片证书中的模拟
30 卡片公钥对卡套端第一绑定因子以及生成的第一连接随机因子进行加密获得的第一连接密文，卡套利用卡套私钥对卡套端第一绑定因子以及第一连接随机因子进行签名获得的第一

连接签名；模拟卡片接收第一安全连接指令，利用模拟卡片私钥对第一连接密文进行解密，获得卡套端第一绑定解密因子以及第一连接随机解密因子；模拟卡片利用卡套证书中的卡套公钥、卡套端第一绑定解密因子以及第一连接随机解密因子对第一连接签名进行验证；模拟卡片验证第一连接签名正确后，验证卡套端第一绑定解密因子与模拟卡片端绑定因子是否相同；模拟卡片验证卡套端第一绑定解密因子与模拟卡片端绑定因子相同后，生成第二连接随机因子；模拟卡片利用卡套证书中的卡套公钥对第一连接随机解密因子以及第二连接随机因子进行加密获得第二连接密文，利用模拟卡片私钥对第一连接随机解密因子以及第二连接随机因子进行签名获得第二连接签名；模拟卡片向卡套发送第一安全连接响应，其中，第一安全连接响应包括：第二连接密文以及第二连接签名；卡套接收第一安全连接响应，利用卡套私钥对第二连接密文进行解密，获得解密后的第一连接随机解密因子和第二连接随机解密因子；卡套利用模拟卡片证书中的模拟卡片公钥、解密后的第一连接随机解密因子和第二连接随机解密因子对第二连接签名进行验证；卡套验证第二连接签名正确后，验证解密后的第一连接随机解密因子与第一连接随机因子是否相同；卡套验证解密后的第一连接随机解密因子与第一连接随机因子相同后，至少利用第二连接随机解密因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片至少利用第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥。

此外，卡套与模拟卡片建立安全连接包括：卡套接收模拟卡片发送的模拟卡片生成的第三连接随机因子以及模拟卡片唯一标识；卡套向模拟卡片发送用于指示建立安全连接的第二安全连接指令，其中，第二安全连接指令包括：卡套唯一标识、卡套利用模拟卡片证书中的模拟卡片公钥对第三连接随机因子以及生成的第四连接随机因子进行加密获得的第三连接密文、卡套利用卡套私钥对第三连接随机因子以及第四连接随机因子进行签名获得的第三连接签名；模拟卡片接收第二安全连接指令，判断卡套唯一标识是否在模拟卡片端绑定列表中；如果卡套唯一标识在模拟卡片端绑定列表中，模拟卡片利用模拟卡片私钥对第三连接密文进行解密，获得第三连接随机解密因子以及第四连接随机解密因子；模拟卡片利用卡套证书中的卡套公钥、第三连接随机解密因子以及第四连接随机解密因子对第三连接签名进行验证；模拟卡片验证第三连接签名正确后，验证第三连接随机解密因子与第三连接随机因子是否相同；如果第三连接随机解密因子与第三连接随机因子相同，模拟卡片利用模拟卡片私钥对第三连接随机解密因子以及第四连接随机解密因子进行签名获得第四连接签名；模拟卡片向卡套发送第二安全连接响应，其中，第二安全连接响应包括：第四连接签名；卡套接收第二安全连接响应，利用模拟卡片证书中的模拟卡片公钥、第三连接随机因子和第四连接随机因子对第四连接签名进行验证；卡套验证第四连接签名正确后，

至少利用第四连接随机因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片至少利用第四连接随机解密因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥；卡套利用卡套端第一安全传输密钥对第三连接随机因子以及第四连接随机因子进行第一处理后发送至模拟卡片；模拟卡片利用模拟卡片端安全传输密钥对第三连接随机解密因子以及第四连接随机解密因子进行第一处理后发送至卡套；卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第三连接随机因子以及第四连接随机因子是否相同；模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第三连接随机解密因子以及第四连接随机解密因子是否相同。

此外，数据交互方法还包括：卡套与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥。

此外，卡套与真实卡片管理器建立安全连接包括：卡套向真实卡片管理器发送用于指示建立安全连接的第三安全连接指令，其中，第三安全连接指令包括：卡套利用真实卡片管理器证书中的真实卡片管理器公钥对卡套端第二绑定因子以及生成的第五连接随机因子进行加密获得的第五连接密文，卡套利用卡套私钥对卡套端第二绑定因子以及第五连接随机因子进行签名获得的第五连接签名；真实卡片管理器接收第三安全连接指令，利用真实卡片管理器私钥对第五连接密文进行解密，获得卡套端第二绑定解密因子以及第五连接随机解密因子；真实卡片管理器利用卡套证书中的卡套公钥、卡套端第二绑定解密因子以及第五连接随机解密因子对第五连接签名进行验证；真实卡片管理器验证第五连接签名正确后，验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子是否相同；真实卡片管理器验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子相同后，生成第六连接随机因子；真实卡片管理器利用卡套证书中的卡套公钥对第五连接随机解密因子以及第六连接随机因子进行加密获得第六连接密文，利用真实卡片管理器私钥对第五连接随机解密因子以及第六连接随机因子进行签名获得第六连接签名；真实卡片管理器向卡套发送第三安全连接响应，其中，第三安全连接响应包括：第六连接密文以及第六连接签名；卡套接收第三安全连接响应，利用卡套私钥对第六连接密文进行解密，获得解密后的第五连接随机解密因子和第六连接随机解密因子；卡套利用真实卡片管理器证书中的真实卡片管理器公钥、解密后的第五连接随机解密因子和第六连接随机解密因子对第六连接签名进行验证；卡套验证第六连接签名正确后，验证解密后的第五连接随机解密因子与第五连接随机因子是否

相同；卡套验证解密后的第五连接随机解密因子与第五连接随机因子相同后，至少利用第六连接随机解密因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器至少利用第六连接随机因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥。

- 5 此外，卡套与真实卡片管理器建立安全连接包括：卡套接收真实卡片管理器发送的真实卡片管理器生成的第七连接随机因子和真实卡片管理器唯一标识；卡套向真实卡片管理器发送用于指示建立安全连接的第四安全连接指令，其中，第四安全连接指令包括：卡套唯一标识、卡套利用真实卡片管理器证书中的真实卡片管理器公钥对第七连接随机因子以及生成的第八连接随机因子进行加密获得的第七连接密文、卡套利用卡套私钥对第七连接
- 10 随机因子以及第八连接随机因子进行签名获得的第七连接签名；真实卡片管理器接收第四安全连接指令，判断卡套唯一标识是否在真实卡片管理器端绑定列表中；如果卡套唯一标识在真实卡片管理器端绑定列表中，真实卡片管理器利用真实卡片管理器私钥对第七连接密文进行解密，获得第七连接随机解密因子以及第八连接随机解密因子；真实卡片管理器利用卡套证书中的卡套公钥、第七连接随机解密因子以及第八连接随机解密因子对第七连
- 15 接签名进行验证；真实卡片管理器验证第七连接签名正确后，验证第七连接随机解密因子与第七连接随机因子是否相同；如果第七连接随机解密因子与第七连接随机因子相同，真实卡片管理器利用真实卡片管理器私钥对第七连接随机解密因子以及第八连接随机解密因子进行签名获得第八连接签名；真实卡片管理器向卡套发送第四安全连接响应，其中，第四安全连接响应包括：第八连接签名；卡套接收第四安全连接响应，利用真实卡片管理器
- 20 证书中的真实卡片管理器公钥、第七连接随机因子和第八连接随机因子对第八连接签名进行验证；卡套验证第八连接签名正确后，至少利用第八连接随机因子以及卡套端第二绑定因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器至少利用第八连接随机解密因子以及真实卡片管理器端绑定因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥；卡套利用卡套端第二安全传输密钥对第七连接随机因子以
- 25 及第八连接随机因子进行第一处理后发送至真实卡片管理器；真实卡片管理器利用真实卡片管理器端安全传输密钥对第七连接随机解密因子以及第八连接随机解密因子进行第一处理后发送至卡套；卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机因子以及第八连接随机因子是否相同；真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全
- 30 传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机解密因子以及第八连接随机解密因子是否相同。

此外，在卡套与模拟卡片建立安全连接之前，数据交互方法还包括：卡套与模拟卡片执行绑定操作。

此外，卡套与模拟卡片执行绑定操作包括：卡套接收用于指示与模拟卡片进行绑定的触发命令；卡套向模拟卡片发送第一绑定指令，其中，第一绑定指令包括：卡套生成的第一绑定随机因子、卡套证书以及卡套唯一标识；模拟卡片接收第一绑定指令，利用根证书对卡套证书进行验证；模拟卡片验证卡套证书合法后，生成第二绑定随机因子；模拟卡片利用卡套证书中的卡套公钥对第一绑定随机因子以及第二绑定随机因子进行加密获得第一绑定密文，利用模拟卡片私钥对第一绑定随机因子以及第二绑定随机因子进行签名获得第一绑定签名；模拟卡片向卡套发送第一绑定响应，其中，第一绑定响应包括：第一绑定密文、第一绑定签名、模拟卡片证书以及模拟卡片唯一标识；卡套接收第一绑定响应，利用根证书对模拟卡片证书进行验证；卡套验证模拟卡片证书合法后，利用卡套私钥对第一绑定密文进行解密，获得第一绑定随机解密因子和第二绑定随机解密因子；卡套利用模拟卡片证书中的模拟卡片公钥、第一绑定随机解密因子以及第二绑定随机解密因子对第一绑定签名进行验证；卡套验证第一绑定签名正确后，验证第一绑定随机解密因子与第一绑定随机因子是否相同；卡套验证第一绑定随机解密因子与第一绑定随机因子相同后，提示模拟卡片唯一标识；卡套接收用于确认模拟卡片唯一标识正确的触发命令，利用卡套私钥对第一绑定随机因子以及第二绑定随机解密因子进行签名，获得第二绑定签名，以及存储模拟卡片唯一标识、模拟卡片证书以及卡套端第一绑定因子至卡套端第一绑定列表，其中，卡套端第一绑定因子为第二绑定随机解密因子；卡套向模拟卡片发送第二绑定签名；模拟卡片接收第二绑定签名，利用卡套证书中的卡套公钥、第一绑定随机因子以及第二绑定随机因子对第二绑定签名进行验证；模拟卡片验证第二绑定签名正确后，存储卡套唯一标识、卡套证书以及模拟卡片端绑定因子至模拟卡片端绑定列表，其中，模拟卡片端绑定因子为第二绑定随机因子。

此外，在卡套与真实卡片管理器建立安全连接之前，数据交互方法还包括：卡套与真实卡片管理器执行绑定操作。

此外，卡套与真实卡片管理器执行绑定操作包括：卡套接收用于指示与真实卡片管理器进行绑定的触发命令；卡套通过无线网络向真实卡片管理器发送第二绑定指令，其中，第二绑定指令包括：卡套生成的第三绑定随机因子、卡套证书以及卡套唯一标识；真实卡片管理器接收第二绑定指令，利用根证书对卡套证书进行验证；真实卡片管理器验证卡套证书合法后，生成第四绑定随机因子；真实卡片管理器利用卡套证书中的卡套公钥对第三绑定随机因子以及第四绑定随机因子进行加密获得第二绑定密文，利用真实卡片管理器私

钥对第三绑定随机因子以及第四绑定随机因子进行签名获得第三绑定签名；真实卡片管理器通过无线网络向卡套发送第二绑定响应，其中，第二绑定响应包括：第二绑定密文、第三绑定签名、真实卡片管理器证书以及真实卡片管理器唯一标识；卡套接收第二绑定响应，利用根证书对真实卡片管理器证书进行验证；卡套验证真实卡片管理器证书合法后，利用卡套私钥对第二绑定密文进行解密，获得第三绑定随机解密因子和第四绑定随机解密因子；卡套利用真实卡片管理器证书中的真实卡片管理器公钥、第三绑定随机解密因子以及第四绑定随机解密因子对第三绑定签名进行验证；卡套验证第三绑定签名正确后，验证第三绑定随机解密因子与第三绑定随机因子是否相同；卡套验证第三绑定随机解密因子与第三绑定随机因子相同后，提示真实卡片管理器唯一标识；卡套接收用于确认真实卡片管理器唯一标识正确的触发命令，利用卡套私钥对第三绑定随机因子以及第四绑定随机解密因子进行签名，获得第四绑定签名，以及存储真实卡片管理器唯一标识、真实卡片管理器证书以及卡套端第二绑定因子至卡套端第二绑定列表，其中，卡套端第二绑定因子为第四绑定随机解密因子；卡套向真实卡片管理器发送第四绑定签名；真实卡片管理器接收第四绑定签名，利用卡套证书中的卡套公钥、第三绑定随机因子以及第四绑定随机因子对第四绑定签名进行验证；真实卡片管理器验证第四绑定签名正确后，存储卡套唯一标识、卡套证书以及真实卡片管理器端绑定因子至真实卡片管理器端绑定列表，其中，真实卡片管理器端绑定因子为第四绑定随机因子。

此外，在卡套与真实卡片管理器建立安全连接之前，数据交互方法还包括：卡套向真实卡片管理器发送登录请求；在卡套与真实卡片管理器建立安全连接之后，数据交互方法还包括：卡套通过卡套端第二安全传输密钥对接收到的登录密码进行第一处理后发送至真实卡片管理器；真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性；真实卡片管理器在验证第二处理后的数据通过后，卡套登录真实卡片管理器。

此外，真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性包括：真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，获得待验证密码；真实卡片管理器判断待验证密码是否为报警密码；如果待验证密码为报警密码，则真实卡片管理器确定待验证密码验证通过，并执行报警操作；如果待验证密码不是报警密码且为登录密码，则真实卡片管理器确定待验证密码验证通过。

此外，数据交互方法还包括：真实卡片管理器对与真实卡片管理器连接的真实卡片进行检测；真实卡片管理器在检测到与真实卡片管理器连接的真实卡片后，获取真实卡片的

真实卡片信息，其中，真实卡片信息至少包括：卡号；真实卡片管理器获取真实卡片的真实卡片信息后，生成真实卡片管理器端真实卡片信息列表。

此外，数据交互方法还包括：真实卡片管理器还生成真实卡片管理器端标识列表，真实卡片管理器端标识列表中的标识与真实卡片管理器端真实卡片信息列表中的真实卡片信息一一对应。

此外，卡套登录真实卡片管理器后，数据交互方法还包括：卡套查找卡套端标识列表；如果卡套查找到卡套端标识列表，则利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同，如果不相同，则真实卡片管理器利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套，卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表；如果卡套未查找到卡套端标识列表，则利用卡套端第二安全传输密钥对预设标识进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，真实卡片管理器确定第二处理后的数据用于指示卡套端未存储卡套端标识列表时，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套，卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，卡套登录真实卡片管理器后，数据交互方法还包括：真实卡片管理器利用真实卡片管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；如果不相同，则卡套向真实卡片管理器发送更新请求；真实卡片管理器接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，卡套还包括心跳休眠模式，其中，心跳休眠模式为低功耗的非工作模式，数据交互方法还包括：卡套在心跳休眠模式下，每隔第一预设时间向真实卡片管理器发送检测信息；真实卡片管理器接收到检测信息，向卡套发送响应信息；如果卡套在第二预设时间内未收到响应信息，则断开卡套与真实卡片管理器之间的安全连接；如果卡套在第二预设

时间内收到响应信息，则保持卡套与真实卡片管理器建立的安全连接。

此外，如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，数据交互方法还包括：卡套存储更新提示信息；在卡套由心跳休眠模式进入工作模式后，卡套向真实卡片管理器发送更新触发请求；真实卡片管理器接收更新触发请求，利用真实卡片管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；如果不相同，则卡套向真实卡片管理器发送更新请求；真实卡片管理器接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，数据交互方法还包括：卡套存储更新提示信息；在卡套由心跳休眠模式进入工作模式后，卡套利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器；真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同；如果不相同，则真实卡片管理器利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，卡套接收真实卡片选择指令，确定选中的真实卡片；包括：卡套接收真实卡片选择指令，获取选中标识，其中，选中标识用于指示选中的真实卡片；卡套将选中标识发送至真实卡片管理器；真实卡片管理器根据选中标识从与真实卡片管理器连接的真实卡片中，确定与选中标识对应的选中的真实卡片。

此外，数据交互方法还包括：卡套至少将卡套证书发送至更新平台；更新平台生成第一更新加密密钥；更新平台利用第一更新加密密钥对卡套应用程序安装包进行加密获得第一安装包密文；更新平台利用更新平台私钥对第一安装包密文进行签名获得第一安装包签名；更新平台利用卡套证书中的卡套公钥加密第一更新加密密钥，获得第一更新加密密钥密文；更新平台将卡套更新信息发送至卡套，其中，卡套更新信息包括：更新平台证书、第一安装包密文、第一安装包签名以及第一更新加密密钥密文；卡套接收卡套更新信息，利用根证书验证更新平台证书；卡套验证更新平台证书通过后，利用更新平台证书中的更

新平台公钥对第一安装包签名进行验签；卡套验证第一安装包签名正确后，利用卡套私钥解密第一更新加密密钥密文，获得第一解密密钥；卡套利用第一解密密钥解密第一安装包密文，获得卡套应用程序安装包；卡套验证卡套应用程序安装包的数据格式是否正确；如果卡套验证卡套应用程序安装包的数据格式正确，卡套根据卡套应用程序安装包进行安装。

5 此外，数据交互方法还包括：卡套从模拟卡片中获取模拟卡片证书，至少将模拟卡片证书发送至更新平台；更新平台生成第二更新加密密钥；更新平台利用第二更新加密密钥对模拟卡片应用程序安装包进行加密获得第二安装包密文；更新平台利用更新平台私钥对第二安装包密文进行签名获得第二安装包签名；更新平台利用模拟卡片证书中的模拟卡片公钥加密第二更新加密密钥，获得第二更新加密密钥密文；更新平台将模拟卡片更新信息
10 发送至卡套，其中，模拟卡片更新信息包括：更新平台证书、第二安装包密文、第二安装包签名以及第二更新加密密钥密文；卡套接收模拟卡片更新信息，并发送至模拟卡片；模拟卡片接收卡套发送的模拟卡片更新信息，利用根证书验证更新平台证书；模拟卡片验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第二安装包签名进行验签；模拟卡片验证第二安装包签名正确后，利用模拟卡片私钥解密第二更新加密密钥密文，获
15 得第二解密密钥；模拟卡片利用第二解密密钥解密第二安装包密文，获得模拟卡片应用程序安装包；模拟卡片验证模拟卡片应用程序安装包的数据格式是否正确；如果模拟卡片验证模拟卡片应用程序安装包的数据格式正确，模拟卡片根据模拟卡片应用程序安装包进行安装。

此外，数据交互方法还包括：真实卡片管理器至少将真实卡片管理器证书发送至更新
20 平台；更新平台生成第三更新加密密钥；更新平台利用第三更新加密密钥对真实卡片管理器应用程序安装包进行加密获得第三安装包密文；更新平台利用更新平台私钥对第三安装包密文进行签名获得第三安装包签名；更新平台利用真实卡片管理器证书中的真实卡片管理器公钥加密第三更新加密密钥，获得第三更新加密密钥密文；更新平台将真实卡片管理器更新信息发送至真实卡片管理器，其中，真实卡片管理器更新信息包括：更新平台证书、
25 第三安装包密文、第三安装包签名以及第三更新加密密钥密文；真实卡片管理器接收真实卡片管理器更新信息，利用根证书验证更新平台证书；真实卡片管理器验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第三安装包签名进行验签；真实卡片管理器验证第三安装包签名正确后，利用真实卡片管理器私钥解密第三更新加密密钥密文，获得第三解密密钥；真实卡片管理器利用第三解密密钥解密第三安装包密文，获得真实卡片
30 管理器应用程序安装包；真实卡片管理器验证真实卡片管理器应用程序安装包的数据格式是否正确；如果真实卡片管理器验证真实卡片管理器应用程序安装包的数据格式正确，真

实卡片管理器根据真实卡片管理器应用程序安装包进行安装。

此外，在卡套与模拟卡片建立安全连接之后，模拟卡片向卡套发送的第一数据利用模拟卡片端安全传输密钥进行第一处理后发送，卡套接收到第一处理后的第一数据，利用卡套端安全传输密钥进行第二处理；卡套向模拟卡片发送的第二数据利用卡套端安全传输密钥进行第一处理后发送，模拟卡片接收到第一处理后的第二数据，利用模拟卡片端安全传输密钥进行第二处理。

此外，在卡套与真实卡片管理器建立安全连接之后，卡套向真实卡片管理器发送的第一数据利用卡套端安全传输密钥进行第一处理后发送，真实卡片管理器接收到第一处理后的第一数据，利用真实卡片管理器端安全传输密钥进行第二处理；真实卡片管理器向卡套发送的第二数据利用真实卡片管理器端安全传输密钥进行第一处理后发送，卡套接收到第一处理后的第二数据，利用卡套端安全传输密钥进行第二处理。

此外，第一处理包括：加密处理，第二处理包括：解密处理；或者第一处理包括：校验计算处理，第二处理包括：校验验证计算处理；或者第一处理包括：加密和校验计算处理，第二处理包括：解密和校验验证计算处理。

此外，真实卡片管理器根据真实卡片的安全性等级，对与真实卡片管理器连接的真实卡片的真实卡片信息的读写权限进行开启和/或关闭的设置。

此外，卡套检测出模拟卡片超出卡套的有效通信范围时，进行安全提示。

此外，卡套为移动设备。

此外，卡套为移动设备和电子签名设备，或者卡套为电子签名设备。

本发明的另一主要目的在于提供一种数据交互系统。

为达到上述目的，本发明的技术方案具体是这样实现的：

本发明一方面提供了一种数据交互系统，包括：模拟卡片、卡套以及真实卡片管理器；卡套，用于获取卡套端真实卡片信息列表；提示卡套端真实卡片信息列表；接收真实卡片选择指令，确定选中的真实卡片，其中，卡套端真实卡片信息列表为卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；模拟卡片，用于接收交易终端发送的第一数据，并将第一数据发送至卡套；卡套，还用于提示第一数据，接收用于确认第一数据正确的确认指令，将第一数据发送至真实卡片管理器；真实卡片管理器，用于接收卡套发送的第一数据，并发送至选中的真实卡片。

此外，卡套，还用于与模拟卡片建立安全连接，获得卡套与模拟卡片之间进行数据安全传输的卡套端第一安全传输密钥；模拟卡片，还用于与卡套建立安全连接，获得卡套与

模拟卡片之间进行数据安全传输的模拟卡片端安全传输密钥。

此外，卡套，具体用于向模拟卡片发送用于指示建立安全连接的第一安全连接指令，其中，第一安全连接指令包括：卡套利用模拟卡片证书中的模拟卡片公钥对卡套端第一绑定因子以及生成的第一连接随机因子进行加密获得的第一连接密文，卡套利用卡套私钥对卡套端第一绑定因子以及第一连接随机因子进行签名获得的第一连接签名；模拟卡片，具体用于接收第一安全连接指令，利用模拟卡片私钥对第一连接密文进行解密，获得卡套端第一绑定解密因子以及第一连接随机解密因子；利用卡套证书中的卡套公钥、卡套端第一绑定解密因子以及第一连接随机解密因子对第一连接签名进行验证；验证第一连接签名正确后，验证卡套端第一绑定解密因子与模拟卡片端绑定因子是否相同；验证卡套端第一绑定解密因子与模拟卡片端绑定因子相同后，生成第二连接随机因子；利用卡套证书中的卡套公钥对第一连接随机解密因子以及第二连接随机因子进行加密获得第二连接密文，利用模拟卡片私钥对第一连接随机解密因子以及第二连接随机因子进行签名获得第二连接签名；向卡套发送第一安全连接响应，其中，第一安全连接响应包括：第二连接密文以及第二连接签名；卡套，具体还用于接收第一安全连接响应，利用卡套私钥对第二连接密文进行解密，获得解密后的第一连接随机解密因子和第二连接随机解密因子；利用模拟卡片证书中的模拟卡片公钥、解密后的第一连接随机解密因子和第二连接随机解密因子对第二连接签名进行验证；验证第二连接签名正确后，验证解密后的第一连接随机解密因子与第一连接随机因子是否相同；验证解密后的第一连接随机解密因子与第一连接随机因子相同后，至少利用第二连接随机解密因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片，具体还用于至少利用第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥。

此外，卡套，具体用于接收模拟卡片发送的模拟卡片生成的第三连接随机因子以及模拟卡片唯一标识；向模拟卡片发送用于指示建立安全连接的第二安全连接指令，其中，第二安全连接指令包括：卡套唯一标识、卡套利用模拟卡片证书中的模拟卡片公钥对第三连接随机因子以及生成的第四连接随机因子进行加密获得的第三连接密文、卡套利用卡套私钥对第三连接随机因子以及第四连接随机因子进行签名获得的第三连接签名；模拟卡片，具体用于接收第二安全连接指令，判断卡套唯一标识是否在模拟卡片端绑定列表中；如果卡套唯一标识在模拟卡片端绑定列表中，利用模拟卡片私钥对第三连接密文进行解密，获得第三连接随机解密因子以及第四连接随机解密因子；利用卡套证书中的卡套公钥、第三连接随机解密因子以及第四连接随机解密因子对第三连接签名进行验证；验证第三连接签名正确后，验证第三连接随机解密因子与第三连接随机因子是否相同；如果第三连接随机

解密因子与第三连接随机因子相同，利用模拟卡片私钥对第三连接随机解密因子以及第四连接随机解密因子进行签名获得第四连接签名；向卡套发送第二安全连接响应，其中，第二安全连接响应包括：第四连接签名；卡套，具体还用于接收第二安全连接响应，利用模拟卡片证书中的模拟卡片公钥、第三连接随机因子和第四连接随机因子对第四连接签名进行验证；验证第四连接签名正确后，至少利用第四连接随机因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片，具体还用于至少利用第四连接随机解密因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥；卡套，具体还用于利用卡套端第一安全传输密钥对第三连接随机因子以及第四连接随机因子进行第一处理后发送至模拟卡片；模拟卡片，具体还用于利用模拟卡片端安全传输密钥对第三连接随机解密因子以及第四连接随机解密因子进行第一处理后发送至卡套；卡套，具体还用于接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第三连接随机因子以及第四连接随机因子是否相同；模拟卡片，具体还用于接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第三连接随机解密因子以及第四连接随机解密因子是否相同。

此外，卡套，还用于与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥；真实卡片管理器，还用于与卡套建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的真实卡片管理器端安全传输密钥。

此外，卡套，具体用于向真实卡片管理器发送用于指示建立安全连接的第三安全连接指令，其中，第三安全连接指令包括：卡套利用真实卡片管理器证书中的真实卡片管理器公钥对卡套端第二绑定因子以及生成的第五连接随机因子进行加密获得的第五连接密文，卡套利用卡套私钥对卡套端第二绑定因子以及第五连接随机因子进行签名获得的第五连接签名；真实卡片管理器，具体用于接收第三安全连接指令，利用真实卡片管理器私钥对第五连接密文进行解密，获得卡套端第二绑定解密因子以及第五连接随机解密因子；利用卡套证书中的卡套公钥、卡套端第二绑定解密因子以及第五连接随机解密因子对第五连接签名进行验证；验证第五连接签名正确后，验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子是否相同；验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子相同后，生成第六连接随机因子；利用卡套证书中的卡套公钥对第五连接随机解密因子以及第六连接随机因子进行加密获得第六连接密文，利用真实卡片管理器私钥对第五连接随机解密因子以及第六连接随机因子进行签名获得第六连接签名；向卡套发送第三安全连接响应，其

中，第三安全连接响应包括：第六连接密文以及第六连接签名；卡套，具体还用于接收第三安全连接响应，利用卡套私钥对第六连接密文进行解密，获得解密后的第五连接随机解密因子和第六连接随机解密因子；利用真实卡片管理器证书中的真实卡片管理器公钥、解密后的第五连接随机解密因子和第六连接随机解密因子对第六连接签名进行验证；验证第六连接签名正确后，验证解密后的第五连接随机解密因子与第五连接随机因子是否相同；验证解密后的第五连接随机解密因子与第五连接随机因子相同后，至少利用第六连接随机解密因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器，具体还用于至少利用第六连接随机因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥。

此外，卡套，具体用于接收真实卡片管理器发送的真实卡片管理器生成的第七连接随机因子和真实卡片管理器唯一标识；向真实卡片管理器发送用于指示建立安全连接的第四安全连接指令，其中，第四安全连接指令包括：卡套唯一标识、卡套利用真实卡片管理器证书中的真实卡片管理器公钥对第七连接随机因子以及生成的第八连接随机因子进行加密获得的第七连接密文、卡套利用卡套私钥对第七连接随机因子以及第八连接随机因子进行签名获得的第七连接签名；真实卡片管理器，具体用于接收第四安全连接指令，判断卡套唯一标识是否在真实卡片管理器端绑定列表中；如果卡套唯一标识在真实卡片管理器端绑定列表中，利用真实卡片管理器私钥对第七连接密文进行解密，获得第七连接随机解密因子以及第八连接随机解密因子；利用卡套证书中的卡套公钥、第七连接随机解密因子以及第八连接随机解密因子对第七连接签名进行验证；验证第七连接签名正确后，验证第七连接随机解密因子与第七连接随机因子是否相同；如果第七连接随机解密因子与第七连接随机因子相同，利用真实卡片管理器私钥对第七连接随机解密因子以及第八连接随机解密因子进行签名获得第八连接签名；向卡套发送第四安全连接响应，其中，第四安全连接响应包括：第八连接签名；卡套，具体还用于接收第四安全连接响应，利用真实卡片管理器证书中的真实卡片管理器公钥、第七连接随机因子和第八连接随机因子对第八连接签名进行验证；验证第八连接签名正确后，至少利用第八连接随机因子以及卡套端第二绑定因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器，具体还用于至少利用第八连接随机解密因子以及真实卡片管理器端绑定因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥；卡套，具体还用于利用卡套端第二安全传输密钥对第七连接随机因子以及第八连接随机因子进行第一处理后发送至真实卡片管理器；真实卡片管理器，具体还用于利用真实卡片管理器端安全传输密钥对第七连接随机解密因子以及第八连接随机解密因子进行第一处理后发送至卡套；卡套，具体还用于接收真实卡片管理

器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机因子以及第八连接随机因子是否相同；真实卡片管理器，具体还用于接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机解密因子以及第八连接随机解密因子是否相同。

此外，卡套，还用于在卡套与模拟卡片建立安全连接之前，与模拟卡片执行绑定操作。

此外，卡套，具体用于接收用于指示与模拟卡片进行绑定的触发命令；向模拟卡片发送第一绑定指令，其中，第一绑定指令包括：卡套生成的第一绑定随机因子、卡套证书以及卡套唯一标识；模拟卡片，具体用于接收第一绑定指令，利用根证书对卡套证书进行验证；验证卡套证书合法后，生成第二绑定随机因子；利用卡套证书中的卡套公钥对第一绑定随机因子以及第二绑定随机因子进行加密获得第一绑定密文，利用模拟卡片私钥对第一绑定随机因子以及第二绑定随机因子进行签名获得第一绑定签名；向卡套发送第一绑定响应，其中，第一绑定响应包括：第一绑定密文、第一绑定签名、模拟卡片证书以及模拟卡片唯一标识；卡套，具体还用于接收第一绑定响应，利用根证书对模拟卡片证书进行验证；验证模拟卡片证书合法后，利用卡套私钥对第一绑定密文进行解密，获得第一绑定随机解密因子和第二绑定随机解密因子；利用模拟卡片证书中的模拟卡片公钥、第一绑定随机解密因子以及第二绑定随机解密因子对第一绑定签名进行验证；验证第一绑定签名正确后，验证第一绑定随机解密因子与第一绑定随机因子是否相同；验证第一绑定随机解密因子与第一绑定随机因子相同后，提示模拟卡片唯一标识；接收用于确认模拟卡片唯一标识正确的触发命令，利用卡套私钥对第一绑定随机因子以及第二绑定随机解密因子进行签名，获得第二绑定签名，以及存储模拟卡片唯一标识、模拟卡片证书以及卡套端第一绑定因子至卡套端第一绑定列表，其中，卡套端第一绑定因子为第二绑定随机解密因子；向模拟卡片发送第二绑定签名；模拟卡片，具体还用于接收第二绑定签名，利用卡套证书中的卡套公钥、第一绑定随机因子以及第二绑定随机因子对第二绑定签名进行验证；验证第二绑定签名正确后，存储卡套唯一标识、卡套证书以及模拟卡片端绑定因子至模拟卡片端绑定列表，其中，模拟卡片端绑定因子为第二绑定随机因子。

此外，卡套，还用于在卡套与真实卡片管理器建立安全连接之前，与真实卡片管理器执行绑定操作。

此外，卡套，具体用于接收用于指示与真实卡片管理器进行绑定的触发命令；通过无线网络向真实卡片管理器发送第二绑定指令，其中，第二绑定指令包括：卡套生成的第三绑定随机因子、卡套证书以及卡套唯一标识；真实卡片管理器，具体用于接收第二绑定指

令，利用根证书对卡套证书进行验证；验证卡套证书合法后，生成第四绑定随机因子；利用卡套证书中的卡套公钥对第三绑定随机因子以及第四绑定随机因子进行加密获得第二绑定密文，利用真实卡片管理器私钥对第三绑定随机因子以及第四绑定随机因子进行签名获得第三绑定签名；通过无线网络向卡套发送第二绑定响应，其中，第二绑定响应包括：第二绑定密文、第三绑定签名、真实卡片管理器证书以及真实卡片管理器唯一标识；卡套，具体还用于接收第二绑定响应，利用根证书对真实卡片管理器证书进行验证；验证真实卡片管理器证书合法后，利用卡套私钥对第二绑定密文进行解密，获得第三绑定随机解密因子和第四绑定随机解密因子；利用真实卡片管理器证书中的真实卡片管理器公钥、第三绑定随机解密因子以及第四绑定随机解密因子对第三绑定签名进行验证；验证第三绑定签名正确后，验证第三绑定随机解密因子与第三绑定随机因子是否相同；验证第三绑定随机解密因子与第三绑定随机因子相同后，提示真实卡片管理器唯一标识；接收用于确认真实卡片管理器唯一标识正确的触发命令，利用卡套私钥对第三绑定随机因子以及第四绑定随机解密因子进行签名，获得第四绑定签名，以及存储真实卡片管理器唯一标识、真实卡片管理器证书以及卡套端第二绑定因子至卡套端第二绑定列表，其中，卡套端第二绑定因子为第四绑定随机解密因子；向真实卡片管理器发送第四绑定签名；真实卡片管理器，具体还用于接收第四绑定签名，利用卡套证书中的卡套公钥、第三绑定随机因子以及第四绑定随机因子对第四绑定签名进行验证；验证第四绑定签名正确后，存储卡套唯一标识、卡套证书以及真实卡片管理器端绑定因子至真实卡片管理器端绑定列表，其中，真实卡片管理器端绑定因子为第四绑定随机因子。

此外，卡套，还用于在卡套与真实卡片管理器建立安全连接之前，向真实卡片管理器发送登录请求；在卡套与真实卡片管理器建立安全连接之后，通过卡套端第二安全传输密钥对接收到的登录密码进行第一处理后发送至真实卡片管理器；真实卡片管理器，还用于接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性；在验证第二处理后的数据通过后，卡套登录真实卡片管理器。

此外，真实卡片管理器，具体用于利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，获得待验证密码；判断待验证密码是否为报警密码；如果待验证密码为报警密码，则确定待验证密码验证通过，并执行报警操作；如果待验证密码不是报警密码且为登录密码，则确定待验证密码验证通过。

此外，真实卡片管理器，还用于对与真实卡片管理器连接的真实卡片进行检测；在检测到与真实卡片管理器连接的真实卡片后，获取真实卡片的真实卡片信息；获取真实卡片

的真实卡片信息后，生成真实卡片管理器端真实卡片信息列表，其中，真实卡片信息至少包括：卡号。

此外，真实卡片管理器，还用于生成真实卡片管理器端标识列表，真实卡片管理器端标识列表中的标识与真实卡片管理器端真实卡片信息列表中的真实卡片信息一一对应。

- 5 此外，卡套，还用于在卡套登录真实卡片管理器后，查找卡套端标识列表；如果卡套查找到卡套端标识列表，则利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器；如果卡套未查找到卡套端标识列表，则利用卡套端第二安全传输密钥对预设标识进行第一处理后发送至真实卡片管理器；真实卡片管理器，还用于接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，
- 10 判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同，如果不相同，则利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；或者接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，确定第二处理后的数据用于指示卡套端未存储卡套端标识列表时，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；
- 15 卡套，还用于接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

- 此外，真实卡片管理器，还用于在卡套登录真实卡片管理器后，利用真实卡套管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；卡套，还用于接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二
- 20 处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；如果不相同，则向真实卡片管理器发送更新请求；真实卡片管理器，还用于接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；卡套，还用于接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

- 25 此外，卡套还包括心跳休眠模式，其中，心跳休眠模式为低功耗的非工作模式；卡套，还用于在心跳休眠模式下，每隔第一预设时间向真实卡片管理器发送检测信息；真实卡片管理器，还用于接收到检测信息，向卡套发送响应信息；卡套，还用于如果在第二预设时间内未收到响应信息，则断开卡套与真实卡片管理器之间的安全连接；如果在第二预设时间内收到响应信息，则保持卡套与真实卡片管理器建立的安全连接。

- 30 此外，卡套，还用于如果在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息时，存储更新提示信息；在卡套由心跳休眠模式进入工作模式后，向真实卡片管

理器发送更新触发请求；真实卡片管理器，还用于接收更新触发请求，利用真实卡片管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；卡套，还用于接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；如果不相同，
5 则向真实卡片管理器发送更新请求；真实卡片管理器，还用于接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；卡套，还用于接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，卡套，还用于如果在第二预设时间内收到响应信息，且响应信息中还包含更新
10 提示信息时，存储更新提示信息；在卡套由心跳休眠模式进入工作模式后，利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器；真实卡片管理器，还用于接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同；如果不相同，则利用真实卡片管理器端安全传输密钥对更新指令和更新数据
15 进行第一处理后发送至卡套；卡套，还用于接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。

此外，卡套，具体用于接收真实卡片选择指令，获取选中标识，其中，选中标识用于指示选中的真实卡片；将选中标识发送至真实卡片管理器；真实卡片管理器，具体用于根据选中标识从与真实卡片管理器连接的真实卡片中，确定与选中标识对应的选中的真实卡
20 片。

此外，数据交互系统还包括：更新平台；卡套，还用于至少将卡套证书发送至更新平台；

更新平台，用于生成第一更新加密密钥；利用第一更新加密密钥对卡套应用程序安装包进行加密获得第一安装包密文；利用更新平台私钥对第一安装包密文进行签名获得第一
25 安装包签名；利用卡套证书中的卡套公钥加密第一更新加密密钥，获得第一更新加密密钥密文；将卡套更新信息发送至卡套，其中，卡套更新信息包括：更新平台证书、第一安装包密文、第一安装包签名以及第一更新加密密钥密文；卡套，还用于接收卡套更新信息，利用根证书验证更新平台证书；验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第一安装包签名进行验签；验证第一安装包签名正确后，利用卡套私钥解密第一
30 更新加密密钥密文，获得第一解密密钥；利用第一解密密钥解密第一安装包密文，获得卡套应用程序安装包；验证卡套应用程序安装包的数据格式是否正确；如果卡套验证卡套应

用程序安装包的数据格式正确，根据卡套应用程序安装包进行安装。

此外，数据交互系统还包括：更新平台；卡套，还用于从模拟卡片中获取模拟卡片证书，至少将模拟卡片证书发送至更新平台；更新平台，用于生成第二更新加密密钥；利用第二更新加密密钥对模拟卡片应用程序安装包进行加密获得第二安装包密文；利用更新平台私钥对第二安装包密文进行签名获得第二安装包签名；利用模拟卡片证书中的模拟卡片公钥加密第二更新加密密钥，获得第二更新加密密钥密文；将模拟卡片更新信息发送至卡套，其中，模拟卡片更新信息包括：更新平台证书、第二安装包密文、第二安装包签名以及第二更新加密密钥密文；卡套，还用于接收模拟卡片更新信息，并发送至模拟卡片；模拟卡片，还用于接收卡套发送的模拟卡片更新信息，利用根证书验证更新平台证书；验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第二安装包签名进行验签；验证第二安装包签名正确后，利用模拟卡片私钥解密第二更新加密密钥密文，获得第二解密密钥；利用第二解密密钥解密第二安装包密文，获得模拟卡片应用程序安装包；验证模拟卡片应用程序安装包的数据格式是否正确；如果模拟卡片验证模拟卡片应用程序安装包的数据格式正确，根据模拟卡片应用程序安装包进行安装。

此外，数据交互系统还包括：更新平台；真实卡片管理器，还用于至少将真实卡片管理器证书发送至更新平台；更新平台，用于生成第三更新加密密钥；利用第三更新加密密钥对真实卡片管理器应用程序安装包进行加密获得第三安装包密文；利用更新平台私钥对第三安装包密文进行签名获得第三安装包签名；利用真实卡片管理器证书中的真实卡片管理器公钥加密第三更新加密密钥，获得第三更新加密密钥密文；将真实卡片管理器更新信息发送至真实卡片管理器，其中，真实卡片管理器更新信息包括：更新平台证书、第三安装包密文、第三安装包签名以及第三更新加密密钥密文；真实卡片管理器，还用于接收真实卡片管理器更新信息，利用根证书验证更新平台证书；验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第三安装包签名进行验签；验证第三安装包签名正确后，利用真实卡片管理器私钥解密第三更新加密密钥密文，获得第三解密密钥；利用第三解密密钥解密第三安装包密文，获得真实卡片管理器应用程序安装包；验证真实卡片管理器应用程序安装包的数据格式是否正确；如果真实卡片管理器验证真实卡片管理器应用程序安装包的数据格式正确，根据真实卡片管理器应用程序安装包进行安装。

此外，模拟卡片，还用于在卡套与模拟卡片建立安全连接之后，向卡套发送的第一数据利用模拟卡片端安全传输密钥进行第一处理后发送，卡套，还用于接收到第一处理后的第一数据，利用卡套端安全传输密钥进行第二处理；卡套，还用于在卡套与模拟卡片建立安全连接之后，向模拟卡片发送的第二数据利用卡套端安全传输密钥进行第一处理后发送，

模拟卡片，还用于接收到第一处理后的第二数据，利用模拟卡片端安全传输密钥进行第二处理。

此外，卡套，还用于在卡套与真实卡片管理器建立安全连接之后，向真实卡片管理器发送的第一数据利用卡套端安全传输密钥进行第一处理后发送，真实卡片管理器，还用于
5 接收到第一处理后的第一数据，利用真实卡片管理器端安全传输密钥进行第二处理；真实卡片管理器，还用于在卡套与真实卡片管理器建立安全连接之后，向卡套发送的第二数据利用真实卡片管理器端安全传输密钥进行第一处理后发送，卡套，还用于接收到第一处理后的第二数据，利用卡套端安全传输密钥进行第二处理。

此外，第一处理包括：加密处理，第二处理包括：解密处理；或者第一处理包括：校
10 验计算处理，第二处理包括：校验验证计算处理；或者第一处理包括：加密和校验计算处理，第二处理包括：解密和校验验证计算处理。

此外，真实卡片管理器，还用于根据真实卡片的安全性等级，对与真实卡片管理器连接的真实卡片的真实卡片信息的读写权限进行开启和/或关闭的设置。

此外，卡套，还用于检测出模拟卡片超出卡套的有效通信范围时，进行安全提示。

此外，卡套为移动设备。

此外，卡套为移动设备和电子签名设备，或者卡套为电子签名设备。

由上述本发明提供的技术方案可以看出，通过本发明的数据交互方法和系统可以实现模拟卡片、卡套与真实卡片管理器之间的数据交互，以提供一种新型的既方便用户携带，且安全性较高的交易解决方案。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例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，对于本领域的普通技术人员来讲，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附
25 图。

图 1 为本发明实施例提供的数据交互方法的流程图；

图 2 示出了本发明实施例提供的数据交互系统的结构示意图；

图 3 为本发明实施例的数据更新方法方式一的流程图；

图 4 为本发明实施例的数据更新方法方式二的流程图；

图 5 为本发明实施例的数据更新方法方式三的流程图；

图 6 为本发明实施例的数据更新方法方式四的流程图；

图 7 为本发明实施例的卡套与模拟卡片建立安全连接方式一的流程图；

图 8 为本发明实施例的卡套与模拟卡片建立安全连接方式二的流程图；

图 9 为本发明实施例的卡套与真实卡片管理器建立安全连接方式一的流程图；

图 10 为本发明实施例的卡套与真实卡片管理器建立安全连接方式二的流程图；

5 图 11 为本发明实施例的卡套与模拟卡片执行绑定操作的流程图；

图 12 为本发明实施例的卡套与真实卡片管理器执行绑定操作的流程图；

图 13 为本发明实施例的卡套应用程序更新的流程图；

图 14 为本发明实施例的模拟卡片应用程序更新的流程图；

图 15 为本发明实施例的真实卡片管理器应用程序更新的流程图。

10

具体实施方式

下面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实施例，而不是全部的实施例。基于本发明的实施例，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，
15 都属于本发明的保护范围。

在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不
20 能理解为对本发明的限制。此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或数量或位置。

在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，
25 可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

下面将结合附图对本发明实施例作进一步地详细描述。

本发明提供了一种数据交互的架构，以提供既方便用户携带，且安全性较高的交易解决方案。该数据交互架构包括：模拟卡片、卡套以及真实卡片管理器。
30

其中：

模拟卡片，可以包括一张或多张，且该模拟卡片可以为单独制造的卡片也可以为预留

有模拟卡片功能的真实卡片。该模拟卡片与现有银行卡大小相同，在本数据交互架构中，替代真实卡片完成交易。模拟卡片具有接触式和/或非接触式接口，以便配合现有的交易终端（例如 ATM 机、POS 机、公交卡充值机等）完成交易。模拟卡片还具有无线接口，模拟卡片可以通过该无线接口与卡套进行数据交互。其中，接触式接口可以为触点等，非接触式接口可以为 NFC 接口等，该无线接口可以为蓝牙接口、红外接口、2.4GHz 接口、WIFI 接口、RFID 接口等。

卡套，可以包括一个或多个卡套，且该卡套可以管理一张或多张模拟卡片，每张模拟卡片只能属于一个卡套并被其管理。该卡套可以为单独制造为卡片外套形状的设备，也可以为具有本数据架构中提供的卡套功能的移动设备，包括：智能手机、平板电脑（PAD）、PDA（例如掌上电脑、学习机）、笔记本电脑、电子书阅读装置、可穿戴设备（例如智能手表、智能眼镜等）等。卡套可以具有接触式和/或非接触式接口，以便配合模拟卡片的接触式和/或非接触式接口进行数据交互，卡套也可以具有无线接口，以便通过该无线接口与模拟卡片相应的接口进行数据交互，其中，接触式接口可以为触点等，非接触式接口可以为 NFC 接口等，该无线接口可以为蓝牙接口、红外接口、2.4GHz 接口、WIFI 接口、RFID 接口等；卡套还具有网络接口，以便通过该网络接口与真实卡片管理器相应的网络接口进行数据交互，其中，该网络接口可以为 WIFI 接口、移动互联网接口（例如 3G、4G 网络）等。另外，卡套还可以为移动设备和电子签名设备的组合，其中卡套的网络接口借助于移动设备的网络接口实现，其他接口（例如无线接口、接触式和/或非接触式接口等）可以均位于电子签名设备上，或者该其他接口也可以均位于移动设备上，或者该其他接口中部分接口位于电子签名设备上，部分接口位于移动设备上；卡套执行的处理操作均在电子签名设备上执行；卡套还可以仅为电子签名设备。其中，电子签名设备可以为 key 设备，例如工行 U 盾，农行 K 宝等。

真实卡片管理器，可以管理多个卡套，且该真实卡片管理器具有多个接触式（例如卡槽等）接口和/或非接触式（例如 NFC 等）接口，以方便真实卡片管理器可以通过不同方式连接不同种类的真实卡片，其中，真实卡片管理器与至少一个真实卡片相连接，并存储有真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息，该真实卡片信息可以包括：卡号、卡片认证信息等信息，该卡片认证信息为认证真实卡片是否为正规渠道（例如银行、公交公司等）发行的卡片信息；该真实卡片可以为功能卡（例如公交卡、饭卡、购物卡、会员卡、积分卡等）或者银行颁发的银行卡；可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，以便用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，

从而保证这些真实卡片的安全性。真实卡片管理器还具有网络接口，以便通过该网络接口与卡套相应的网络接口进行数据交互，其中，该网络接口可以为 WIFI 接口、移动互联网接口（例如 3G、4G 网络）等。

在本数据交互架构中，模拟卡片以及真实卡片为智能芯片卡。

5 以下，对本发明中的术语进行说明：

第一处理包括：加密处理，第二处理包括：解密处理；具体地，单纯加密保证数据传输安全性，在待传输数据安全级别要求较高时，可以采用此种方式进行处理。或者

10 第一处理包括：校验计算处理，第二处理包括：校验验证计算处理；具体地，单纯校验保证数据传输完整性，防止篡改，在对待传输数据完整性要求较高时，可以采用此种方式进行处理。或者

第一处理包括：加密和校验计算处理，第二处理包括：解密和校验验证计算处理。具体地，采用加密和校验混合方式保证数据传输安全及完整，在对待传输数据安全级别要求最高时，可以采用此种方式进行处理。

15 基于上述数据交互架构，通过本发明的数据交互方法，可以实现模拟卡片、卡套与真实卡片管理器之间的数据交互，以提供一种新型的既方便用户携带，且安全性较高的交易解决方案。

图 1 示出了本发明实施例提供的数据交互方法的流程图，参见图 1，本发明的数据交互方法，包括：

20 卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；

卡套提示卡套端真实卡片信息列表；

卡套接收真实卡片选择指令，确定选中的真实卡片；以及模拟卡片接收交易终端发送的第一数据，并将第一数据发送至卡套；

25 卡套提示第一数据，接收用于确认第一数据正确的确认指令，将第一数据发送至真实卡片管理器；

真实卡片管理器接收卡套发送的第一数据，并发送至选中的真实卡片。

30 图 2 示出了本发明实施例提供的数据交互系统的结构示意图，参见图 2，本发明的数据交互系统，包括：模拟卡片、卡套以及真实卡片管理器；

卡套，用于获取卡套端真实卡片信息列表；提示卡套端真实卡片信息列表；接收真实卡片选择指令，确定选中的真实卡片，其中，卡套端真实卡片信息列表为卡套从真实卡片

管理器中获取的真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；

模拟卡片，用于接收交易终端发送的第一数据，并将第一数据发送至卡套；

卡套，还用于提示第一数据，接收用于确认第一数据正确的确认指令，将第一数据发
5 送至真实卡片管理器；

真实卡片管理器，用于接收卡套发送的第一数据，并发送至选中的真实卡片。

以下，针对上述数据交互方法或系统，进行详细说明，应当理解的是，下述的实施例均适用于方法或系统实施例。具体地，该数据交互方法或系统可以包含以下几个方面：

10 一、真实卡片管理器端真实卡片信息列表生成及更新：

在卡套获取卡套端真实卡片信息列表之前，真实卡片管理器通过如下方式进行真实卡片管理器端真实卡片信息列表的生成，当然，本发明并不局限于此：

真实卡片管理器对与真实卡片管理器连接的真实卡片进行检测；具体地，真实卡片管理器对其上设置的接触式接口和/或非接触式接口进行检测，以确定是否有真实卡片与真实
15 卡片管理器进行连接，可以依次检测是否有与其连接的真实卡片，也可以同时检测是否有与其连接的真实卡片。可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，以便用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

20 真实卡片管理器在检测到与真实卡片管理器连接的真实卡片后，获取真实卡片的真实卡片信息，其中，真实卡片信息至少包括：卡号；具体地，真实卡片管理器在检测到有真实卡片与其进行连接时，读取与其连接的真实卡片中存储的真实卡片信息，并最终获取全部与真实卡片管理器连接的真实卡片的真实卡片信息。此外，真实卡片信息除了包含卡号外，还可以包含卡片认证信息、真实卡片的颁发者标识等信息。

25 真实卡片管理器获取真实卡片的真实卡片信息后，生成真实卡片管理器端真实卡片信息列表。具体地，在真实卡片管理器获取了与其连接的真实卡片的真实卡片信息后，生成真实卡片管理器端真实卡片信息列表，以便后续卡套可以获取该真实卡片管理器端真实卡片信息列表，方便后续使用。可选的，真实卡片管理器可以获取到的是用户设置为允许被获取的真实卡片的真实卡片信息。

30 此外，真实卡片管理器除了生成真实卡片管理器端真实卡片信息列表外，还生成真实卡片管理器端标识列表，该真实卡片管理器端标识列表中的标识与真实卡片管理器端真实卡片信息列表中的真实卡片信息一一对应。具体地，该真实卡片管理器标识列表中的标识

可以唯一标识相应的真实卡片，该标识可以为：表明接触式接口和/或非接触式接口处是否有真实卡片连接的标识（例如 1 代表有真实卡片，0 代表无真实卡片），或者该标识可以为真实卡片的颁发者编码（例如真实卡片为银行卡时，该编码为银行编码）、真实卡片的卡号的尾号、真实卡片的卡号的校验值（例如 CRC 校验值等）等信息中的一种或其任意组合。

- 5 真实卡片管理器生成该真实卡片管理器端标识列表，可以方便后续卡套进行真实卡片信息列表的更新。

当然，真实卡片管理器可以在每次真实卡片管理器开机后，均重新检测并生成真实卡片管理器端真实卡片信息列表；或者也可以通过真实卡片管理器提供的功能按键（物理按键或者虚拟按键）触发对真实卡片检测后，重新生成真实卡片管理器端真实卡片信息列表；
10 或者还可以在真实卡片管理器每次检测到有真实卡片进行插拔或者进行入场出场时，对真实卡片信息列表执行增加和/或删除真实卡片信息的操作。

可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，以使用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。
15

具体地，真实卡片管理器可以将接触式接口和/或非接触式接口进行分区，根据对使用安全系数的不同分为普通卡片区域和重要卡片区域。例如：将用户的小额卡、副卡、公交卡等涉及金额较小的真实卡片放置在普通卡片区域，而将用户的大额卡、信用卡主卡等涉及金额较大的真实卡片放置在重要卡片区域。

- 20 在真实卡片管理器对接触式接口和/或非接触式接口进行分区后，可以对允许获取真实卡片的真实卡片信息的普通卡片区域进行读取，以获取在普通卡片区域进行连接的真实卡片的真实卡片信息；并无法对不允许获取真实卡片的真实卡片信息的重要卡片区域进行读取，无法获取在重要卡片区域进行连接的真实卡片的真实卡片信息。由此，真实卡片管理器生成的真实卡片管理器端真实卡片信息列表中只能包含在普通卡片区域连接的真实卡片的真实卡片信息，卡套可以获取在普通卡片区域连接的真实卡片的真实卡片信息，无法获取在重要卡片区域连接的真实卡片的真实卡片信息，例如：在普通卡片区域内的真实卡片对于卡套可见，卡套可以与其直接进行连接使用；在重要卡片区域内的真实卡片对于卡套不可见，卡套不可以与其直接进行连接使用，如需对重要卡片区域内的真实卡片进行连接使用，则需要采用如下方式之一对该重要卡片区域内的卡片进行设置，以便卡套可以与该
25
30 重要卡片区域内的全部或部分真实卡片进行连接使用：

方式一、用户在输入登录密码后，卡套仅具有对普通卡片区域内的全部真实卡片进行连接使用的权限，不具有对重要卡片区域内的真实卡片进行连接使用的权限，如需对重要

卡片区域内的真实卡片进行连接使用，则可以在真实卡片管理器上设置物理按键、或者在真实卡片管理器上设置虚拟按键、或者在真实卡片管理器上设置功能菜单，以便用户可以在真实卡片管理器上设置卡套对重要卡片区域内的真实卡片进行连接使用的权限。例如：用户可以通过手动方式，按下物理按键、虚拟按键或者功能菜单中的选项，启动卡套对该重要卡片区域内的全部或者部分真实卡片进行连接使用的权限，从而使得卡套可以与该重要卡片区域内开放权限的真实卡片进行连接使用。

方式二、用户在输入登录密码后，卡套仅具有对普通卡片区域内的全部真实卡片进行连接使用的权限，不具有对重要卡片区域内的真实卡片进行连接使用的权限，如需对重要卡片区域内的真实卡片进行连接使用，则可以在真实卡片管理器上设置客户端，或者设置与真实卡片管理器连接的控制终端（例如：PC 机、智能手机、平板电脑等），并在控制终端上设置客户端，用户通过登录客户端进行权限设置，以开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限，以便使得卡套可以与该重要卡片区域内开放权限的真实卡片进行连接使用。

方式三、用户在输入登录密码后，卡套仅具有对普通卡片区域内的全部真实卡片进行连接使用的权限，不具有对重要卡片区域内的真实卡片进行连接使用的权限，如需对重要卡片区域内的真实卡片进行连接使用，则可以在真实卡片管理器上设置权限密码，用户可以通过卡套对真实卡片管理器发起权限设置请求，真实卡片管理器只有在接收到权限设置请求以及接收到用户输入的权限密码，并在验证用户输入的权限密码正确后，才可以开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限，以便使得卡套可以与该重要卡片区域内开放权限的真实卡片进行连接使用。其中，权限密码与登录密码以及报警密码不同。当然，如果真实卡片管理器验证用户输入的权限密码不正确，则不执行对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限的设置。

二、卡套端真实卡片信息列表的获取和更新：

本发明中，卡套获取的卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表。

卡套端真实卡片信息列表更新可以包括如下方式：

方式一、真实卡片管理器判断是否需要进行卡套端真实卡片信息列表的更新操作：

图 3 示出了本发明的数据更新方法中的方式一的方案，应当理解的是，该数据更新方法的方式一可以通过数据交互方法或数据交互系统实现。参见图 3，本发明的数据更新方法包括：

卡套查找卡套端标识列表；具体地，卡套端标识列表为卡套从真实卡片管理器中获取

的真实卡片管理器端标识列表。

如果卡套查找到卡套端标识列表，则将卡套端标识列表发送至真实卡片管理器，真实卡片管理器接收卡套发送的卡套端标识列表后，判断接收到的卡套端标识列表与真实卡片管理器存储的真实卡片管理器端标识列表是否相同，如果不相同，则真实卡片管理器将更新指令和更新数据发送至卡套，卡套接收到更新指令和更新数据后，更新卡套端真实卡片信息列表；具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

如果卡套未查找到卡套端标识列表，则将预设标识发送至真实卡片管理器，真实卡片管理器接收卡套发送的预设标识，确定预设标识用于指示卡套端未存储卡套端标识列表时，将更新指令和更新数据发送至卡套，卡套接收到更新指令和更新数据后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括存储指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行存储操作。

基于本发明的上述方案，卡套通过将卡套端标识列表发送至真实卡片管理器进行判断是否一致，由于卡套端标识列表数据量远小于卡套端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了真实卡片管理器的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，发送预设标识至真实卡片管理器，以便真实卡片管理器下发真实卡片管理器端标识列表以及真实卡片管理器端真实卡片信息列表至卡套，该预设标识可以为空标识、预定义数值、或者预定义字符等。

当然，本发明并不局限于方式一的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

由卡套向真实卡片管理器直接发送卡套端真实卡片信息列表，以便真实卡片管理器进行比对后判断是否更新；或者

由卡套向真实卡片管理器发送卡套端真实卡片信息列表的列表编号，以便真实卡片管

理器比对列表编号是否相同判断是否更新；或者

由真实卡片管理器接收到用户输入的更新指令后，真实卡片管理器将真实卡片管理器端真实卡片信息列表发送至卡套。

当然，在真实卡片管理器判断出需要进行更新后，还可以发送更新询问请求至卡套，

5 卡套提示该更新询问请求给用户，以使用户确认是否进行更新。

方式二、卡套判断是否需要进行卡套端真实卡片信息列表更新操作的流程：

图 4 示出了本发明的数据更新方法的方式二的方案，应当理解的是，该数据更新方法的方式二可以通过数据交互方法或数据交互系统实现。参见图 4，本发明的数据更新方法包括：

10 真实卡片管理器将真实卡片管理器端标识列表发送至卡套；

卡套接收真实卡片管理器发送的真实卡片管理器端标识列表，判断接收到的真实卡片管理器端标识列表与卡套存储的卡套端标识列表是否相同；具体地，如果卡套第一次使用或从未成功下载真实卡片管理器端标识列表，并未存储卡套端标识列表，则直接判定为不同即可。

15 如果不相同，则卡套向真实卡片管理器发送更新请求；

真实卡片管理器接收更新请求，将更新指令和更新数据发送至卡套；

卡套接收到真实卡片管理器发送的更新指令和更新数据后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，

20 卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

基于本发明的上述方案，真实卡片管理器通过将真实卡片管理器端标识列表发送至卡套进行判断是否一致，由于真实卡片管理器端标识列表数据量远小于真实卡片管理器端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了卡套的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，接收到真实卡片管理器下发真实卡片管理器端标识列表后，直接发送更新请求以便真实卡片管理器发送真实卡片管理器端真实卡片信息列表至卡套。

当然，本发明并不局限于方式二的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

由真实卡片管理器直接向卡套发送真实卡片管理器端真实卡片信息列表，以便卡套直接存储；或者

5 由真实卡片管理器向卡套发送真实卡片管理器端真实卡片信息列表的列表编号，以便卡套比对列表编号是否相同判断是否更新；或者

由卡套接收到用户输入的更新指令后，卡套发送更新请求至真实卡片管理器，以便真实卡片管理器直接下发真实卡片管理器端真实卡片信息列表发送至卡套。

当然，在卡套判断出需要进行更新后，还可以提示用户确认是否进行更新，并在用户
10 确认进行更新后，执行后续更新操作。

本发明的卡套除了具备正常工作模式之外，还具有心跳休眠模式，其中，心跳休眠模式为低功耗的非工作模式，即关闭一些不必要的耗电程序等。具体地，卡套可以在预设时间内没有操作后进入心跳休眠模式，也可以由用户的操作控制进入心跳休眠模式。

方式三、卡套处于心跳休眠模式下，卡套判断是否需要进行卡套端真实卡片信息列表
15 更新操作的流程：

图 5 示出了本发明的数据更新方法方式三的方案，应当理解的是，该数据更新方法的方式三可以通过数据交互方法或数据交互系统实现。参见图 5，本发明的数据更新方法包括：

卡套在心跳休眠模式下，每隔第一预设时间向真实卡片管理器发送检测信息；
20 真实卡片管理器接收到检测信息，向卡套发送响应信息；

如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，则卡套存储更新提示信息；其中，更新提示信息为真实卡片管理器告知卡套真实卡片管理器有真实卡片管理器端真实卡片信息列表更新的提示信息。

在卡套由心跳休眠模式进入工作模式后，卡套向真实卡片管理器发送更新触发请求；
25 具体地，卡套可以通过如下方式由心跳休眠模式进入工作模式：卡套收到更新提示信息后自动进入工作模式，或者卡套接收用户输入的操作指令（例如用户进行按键输入的操作指令等）后，进入工作模式。

真实卡片管理器接收更新触发请求，将真实卡片管理器端标识列表发送至卡套；

卡套接收真实卡片管理器发送的真实卡片管理器端标识列表，判断接收到的真实卡片
30 管理器端标识列表与卡套存储的卡套端标识列表是否相同；具体地，如果卡套第一次使用或从未成功下载真实卡片管理器端标识列表，并未存储卡套端标识列表，则直接判定为不同即可。

如果不相同，则卡套向真实卡片管理器发送更新请求；

真实卡片管理器接收更新请求，将更新指令和更新数据发送至卡套；

卡套接收到真实卡片管理器发送的更新指令和更新数据后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

其中的第一预设时间可以与第二预设时间相同或者不同。

基于本发明的上述方案，真实卡片管理器通过将真实卡片管理器端标识列表发送至卡套进行判断是否一致，由于真实卡片管理器端标识列表数据量远小于真实卡片管理器端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了卡套的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，接收到真实卡片管理器下发真实卡片管理器端标识列表后，直接发送更新请求以便真实卡片管理器发送真实卡片管理器端真实卡片信息列表至卡套。

当然，本发明并不局限于方式三的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

由真实卡片管理器直接向卡套发送真实卡片管理器端真实卡片信息列表，以便卡套直接存储；或者

由真实卡片管理器向卡套发送真实卡片管理器端真实卡片信息列表的列表编号，以便卡套比对列表编号是否相同判断是否更新；或者

由卡套接收到用户输入的更新指令后，卡套发送更新请求至真实卡片管理器，以便真实卡片管理器直接下发真实卡片管理器端真实卡片信息列表发送至卡套。

当然，在真实卡片管理器判断出需要进行更新后，还可以发送更新询问请求至卡套，卡套提示该更新询问请求给用户，以便用户确认是否进行更新。

方式四、卡套处于心跳休眠模式下，真实卡片管理器判断是否需要进行卡套端真实卡片信息列表更新操作的流程：

图 6 示出了本发明的数据更新方法方式四的方案，应当理解的是，该数据更新方法的

方式四可以通过数据交互方法或数据交互系统实现。参见图 6，本发明的数据更新方法包括：

卡套在心跳休眠模式下，每隔第一预设时间向真实卡片管理器发送检测信息；

真实卡片管理器接收到检测信息，向卡套发送响应信息；

- 5 如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，则卡套存储更新提示信息；其中，更新提示信息为真实卡片管理器告知卡套真实卡片管理器有真实卡片管理器端真实卡片信息列表更新的提示信息。

- 10 在卡套由心跳休眠模式进入工作模式后，卡套将卡套端标识列表发送至真实卡片管理器；具体地，卡套可以通过如下方式由心跳休眠模式进入工作模式：卡套收到更新提示信息后自动进入工作模式，或者卡套接收用户输入的操作指令（例如用户进行按键输入的操作指令等）后，进入工作模式。如果卡套为第一次使用或者从未成功下载真实卡片管理器端标识列表，则卡套中并未存储卡套端标识列表，此时，卡套利用卡套端第二安全传输密钥对预设标识进行第一处理后发送至真实卡片管理器。

- 15 真实卡片管理器接收卡套发送的卡套端标识列表，判断接收到的卡套端标识列表与真实卡片管理器存储的真实卡片管理器端标识列表是否相同；具体地，真实卡片管理器接收到预设标识，也判断为不相同。

如果不相同，则真实卡片管理器将更新指令和更新数据发送至卡套；

- 20 卡套接收到真实卡片管理器发送的更新指令和更新数据后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

其中的第一预设时间可以与第二预设时间相同或者不同。

- 30 基于本发明的上述方案，卡套通过将卡套端标识列表发送至真实卡片管理器进行判断是否一致，由于卡套端标识列表数据量远小于卡套端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了真实卡片管理器的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，发送预设标识至真实卡片管

理器，以便真实卡片管理器下发真实卡片管理器端标识列表以及真实卡片管理器端真实卡片信息列表至卡套，该预设标识可以为空标识、预定义数值、或者预定义字符等。

当然，本发明并不局限于方式四的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

5 由卡套向真实卡片管理器直接发送卡套端真实卡片信息列表，以便真实卡片管理器进行比对后判断是否更新；或者

由卡套向真实卡片管理器发送卡套端真实卡片信息列表的列表编号，以便真实卡片管理器比对列表编号是否相同判断是否更新；或者

10 由真实卡片管理器接收到用户输入的更新指令后，真实卡片管理器将真实卡片管理器端真实卡片信息列表发送至卡套。

当然，在卡套判断出需要进行更新后，还可以提示用户确认是否进行更新，并在用户确认进行更新后，执行后续更新操作。

15 可选的，在真实卡片管理器开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限后，由于真实卡片管理器端真实卡片信息列表进行了更新，因此，真实卡片管理器会将开放了卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限的真实卡片信息发送至卡套，以便卡套更新卡套端真实卡片信息列表；或者在真实卡片管理器开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限后，触发卡套端真实卡片信息列表更新的流程，更新方式可以参照上述方式一和方式二

20 的更新方式，在此不再详述。

以上真实卡片管理器发送的更新数据中除了包含真实卡片管理器端真实卡片信息列表之外，还包含真实卡片管理器端标识列表，以便卡套获取最新的标识列表。

三、确定选中的真实卡片：

25 卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，可选的，在本步骤之前，还可以执行卡套开机、卡套登录真实卡片管理器的操作，在此不再赘述，具体可以参见上述有关卡套开机和卡套登录真实卡片管理器的相关描述。在本步骤中，卡套获取卡套端真实卡片信息列表，还可以包括卡套更新卡套端真实卡片信息列表的步骤，在此也不再赘述，

30 具体可以参见上述卡套更新卡套端真实卡片信息列表的相关描述。卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表后，将其存储在卡套的存储区域中，作为卡套端真实卡片信息列表，在卡套需要提示（例如显示或者语音播放等）卡套端真实卡片信

息列表时，可以从本地直接获取该卡套端真实卡片信息列表，提高卡套的处理速度。

卡套提示卡套端真实卡片信息列表；具体地，卡套利用自身的显示装置或者借助外部显示装置显示卡套端真实卡片信息列表，或者卡套利用自身的语音播放装置或者借助外部语音播放装置语音播放（例如喇叭播放或者通过耳机听筒播放等）卡套端真实卡片信息列表，以供用户根据卡套端真实卡片信息列表来选择进行交易时需要使用的真实卡片，方便用户选择，增强用户体验。

卡套接收真实卡片选择指令，确定选中的真实卡片；具体地，卡套接收的真实卡片选择指令可以为单独设置在卡套上的选择物理按键生成的，或者可以为卡套的触屏上的选择虚拟按键生成的，或者可以为在卡套屏幕上显示的菜单中选中表示选择功能的菜单项生成的。卡套接收真实卡片选择指令，确定选中的真实卡片，卡套经由真实卡片管理器与选中的真实卡片实现数据传输。另外，可以通过如下方式实现确定选中的真实卡片：卡套接收真实卡片选择指令，获取选中标识，其中，选中标识用于指示选中的真实卡片；卡套将选中标识发送至真实卡片管理器；真实卡片管理器根据选中标识从与真实卡片管理器连接的真实卡片中，确定与选中标识对应的选中的真实卡片；其中，选中标识可以为真实卡片信息中的部分或全部信息，例如：卡号和/或真实卡片管理器读写端口标识；真实卡片管理器接收到选中标识后，可以在真实卡片管理器端真实卡片信息列表中查找到与选中标识对应的真实卡片管理器读写端口标识，以便真实卡片管理器确定其读写端口，从而通过该读写端口与选中的真实卡片进行数据交互。

四、数据交互：

模拟卡片接收交易终端发送的第一数据，并将第一数据发送至卡套；具体地，在数据交互过程中，将模拟卡片与交易终端（例如 ATM 机、POS 机、公交卡充值机等）进行连接（接触式接口或者非接触式接口），模拟卡片接收交易终端发送的第一数据，该第一数据可以为待处理的数据（例如取款金额、扣款金额、真实卡片信息获取请求等）。

卡套提示第一数据，接收用于确认第一数据正确的确认指令，将第一数据发送至真实卡片管理器；具体地，卡套可以显示第一数据，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）第一数据，以供用户确认该第一数据是否正确，只有在正确后，接收用户输入的确认第一数据正确的确认指令后，才将该第一数据发送至真实卡片管理器；如果用户确认该第一数据不正确，则可以直接取消该次数据交互，以此，提高数据交互的安全性。卡套接收的用于确认第一数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确

认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

真实卡片管理器接收卡套发送的第一数据，并发送至选中的真实卡片。具体地，真实卡片管理器将第一数据发送至选中的真实卡片，以便选中的真实卡片对第一数据进行处理。选中的真实卡片接收到第一数据后，可以对第一数据进行处理，该处理为现有智能卡的处理的方案，在此不再赘述。

基于上述数据交互流程，可以通过一张模拟卡片可以实现多种不同种类的真实卡片的功能，用户进行数据交互时，只需携带模拟卡片及卡套，无需携带真实卡片即可以完成，提高便捷性和安全性。

卡套可以将数据交互过程中需要确认的信息进行提示，由此，用户可以对数据交互过程中的需要确认的信息进行确认后再执行交互，从而保证数据交互的真实性，提高安全性。

此外，由于可以选择使用与交易终端匹配的真实卡片，可以解决现有技术中用户未携带与交易终端匹配的真实卡片而产生的不必要的费用支出（例如银行跨行取款手续费等）。

当然，上述具体实现仅公开了从交易终端至真实卡片的单次数据交互，在实际应用中，可能存在多次数据交互，交互流程与上述单次数据交互相似，在多次数据交互中，可以根据交互的数据是否需要确认来设置在卡套处是否提示交互的数据来保证交互数据的真实性。

五、安全连接建立：

卡套获取卡套端真实卡片信息列表之前，本发明还可以包括卡套与模拟卡片建立安全连接，获得卡套与模拟卡片之间进行数据安全传输的卡套端第一安全传输密钥和模拟卡片端安全传输密钥的流程。

当然，也可以包括卡套与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥的流程。

当然，上述两个流程可以同时执行，也可以不同时执行，可以仅执行一个流程，也可以两个流程均执行。

1、卡套与模拟卡片建立安全连接，获得卡套与模拟卡片之间进行数据安全传输的卡套端第一安全传输密钥和模拟卡片端安全传输密钥：

在本发明中，卡套与模拟卡片可以通过如下方式建立安全连接：

方式一、卡套与模拟卡片互相认证对方身份（例如互相认证对方签名数据），并在互相

认证对方身份的过程中，比较双方存储的绑定因子是否相同，在比较双方存储的绑定因子相同且互相认证对方身份通过后，生成卡套与模拟卡片之间进行数据安全传输的安全传输密钥（卡套端第一安全传输密钥和模拟卡片端安全传输密钥）。

值得说明的是，如果在卡套与模拟卡片建立安全连接之前，执行了上述卡套与模拟卡片互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子的绑定操作，则在本方式一中，卡套与模拟卡片互相认证对方身份即为卡套与模拟卡片再次互相认证对方身份。

以下，本发明提供方式一的一种具体实现：

图 7 示出了本发明实施例中卡套与模拟卡片建立安全连接方式一的流程图，应当理解的是，该建立安全连接方式一可以通过数据交互方法或数据交互系统实现。参见图 7，卡套与模拟卡片建立安全连接包括：

卡套向模拟卡片发送用于指示建立安全连接的第一安全连接指令，其中，第一安全连接指令包括：卡套利用模拟卡片证书中的模拟卡片公钥对卡套端第一绑定因子以及生成的第一连接随机因子进行加密获得的第一连接密文，卡套利用卡套私钥对卡套端第一绑定因子以及第一连接随机因子进行签名获得的第一连接签名；具体地，在使用卡套与模拟卡片进行数据交互之前，可选的，在卡套与模拟卡片之间建立安全连接，以提高后续数据交互的安全性。其中，卡套接收的用于指示建立安全连接的第一安全连接指令可以为单独设置在卡套上的连接物理按键生成的，或者可以为卡套的触屏上的连接虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为将模拟卡片从卡套拔出后生成的，或者可以为在卡套屏幕上显示的菜单中选择连接功能生成的，或者可以为在卡套获得卡套端真实卡片信息列表，用户从中选择真实卡片后生成的。当然，还可以为其他任何方式生成的，在本发明中并不作限制。其中，第一连接随机因子可以为卡套生成的随机数、随机字符或其组合，当然，在生成第一连接随机因子后，还可以对第一连接随机因子的随机性进行验证，以提高第一连接随机因子的随机性，防止被破解；具体地，卡套利用模拟卡片公钥对卡套端第一绑定因子以及第一连接随机因子进行加密以保证卡套端第一绑定因子以及第一连接随机因子传输的安全性，卡套利用卡套私钥对卡套端第一绑定因子以及第一连接随机因子进行签名，以保证后续模拟卡片可以对卡套身份的合法性进行认证。将卡套端第一绑定因子发送至模拟卡片，以便后续模拟卡片对卡套端第一绑定因子是否与其存储的绑定因子相同进行判断，从而判断该卡套是否与该模拟卡片进行绑定。可选的，在本步骤之前，卡套检测到模拟卡片之后，卡套可以判断模拟卡片是否在卡套端第一绑定列表中，例如：可通过如下方式进行判断：卡套在检测到模拟卡片后，接收模拟卡片发送的模拟卡片信息（例如模拟卡片唯一标识和/或模拟卡片证书等），根据接收到的模拟卡片信息，判断该模

拟卡片是否在卡套端第一绑定列表中；和/或也可以由模拟卡片判断卡套是否在模拟卡片端绑定列表中，例如：可通过如下方式进行判断：卡套在检测到模拟卡片后，将卡套信息（例如卡套唯一标识和/或卡套证书等）发送至模拟卡片，模拟卡片根据接收到的卡套信息，判断该卡套是否在模拟卡片端绑定列表中；只有在判断对方在自身的绑定列表中后，才执行后续流程，优化了流程，提高了效率。

模拟卡片接收第一安全连接指令，利用模拟卡片私钥对第一连接密文进行解密，获得卡套端第一绑定解密因子以及第一连接随机解密因子；具体地，利用模拟卡片私钥对第一连接密文进行解密，如果在数据传输中发生了数据传输错误，或者在数据传输中发生了篡改，则将导致无法成功解密，或者解密出的卡套端第一绑定解密因子以及第一连接随机解密因子与卡套端第一绑定因子以及第一连接随机因子不同。而通过模拟卡片公钥进行加密，只有模拟卡片私钥可以成功解密，从而也可以保证数据解密的安全性。

模拟卡片利用卡套证书中的卡套公钥、卡套端第一绑定解密因子以及第一连接随机解密因子对第一连接签名进行验证；具体地，模拟卡片利用卡套公钥对卡套发送的签名进行验证，以确保数据的合法来源。

模拟卡片验证第一连接签名正确后，验证卡套端第一绑定解密因子与模拟卡片端绑定因子是否相同；具体地，模拟卡片还验证解密出的卡套端第一绑定解密因子是否与模拟卡片自身存储的模拟卡片端绑定因子是否相同，如果相同，则说明该卡套在与模拟卡片建立安全连接之前，已经完成了绑定的操作，基于此，模拟卡片可以判断卡套是否与模拟卡片进行了绑定。

模拟卡片验证卡套端第一绑定解密因子与模拟卡片端绑定因子相同后，生成第二连接随机因子；具体地，第二连接随机因子可以为模拟卡片生成的随机数、随机字符或其组合，当然，在生成第二连接随机因子后，还可以对第二连接随机因子的随机性进行验证，以提高第二连接随机因子的随机性，防止被破解。

模拟卡片利用卡套证书中的卡套公钥对第一连接随机解密因子以及第二连接随机因子进行加密获得第二连接密文，利用模拟卡片私钥对第一连接随机解密因子以及第二连接随机因子进行签名获得第二连接签名；具体地，模拟卡片利用卡套公钥对第一连接随机解密因子以及第二连接随机因子进行加密以保证第一连接随机解密因子以及第二连接随机因子传输的安全性，模拟卡片利用模拟卡片私钥对第一连接随机解密因子以及第二连接随机因子进行签名，以保证后续卡套可以对模拟卡片身份的合法性进行认证。

模拟卡片向卡套发送第一安全连接响应，其中，第一安全连接响应包括：第二连接密文以及第二连接签名；具体地，模拟卡片将第二连接密文和第二连接签名发送至卡套，以便卡套对接收到的数据进行解密和验证。

卡套接收第一安全连接响应，利用卡套私钥对第二连接密文进行解密，获得解密后的第一连接随机解密因子和第二连接随机解密因子；具体地，利用卡套私钥对第二连接密文进行解密，如果在数据传输中发生了数据传输错误，或者在数据传输中发生了篡改，则将导致无法成功解密，或者解密后的第一连接随机解密因子和第二连接随机解密因子与第一连接随机因子和第二连接随机因子不同。而通过卡套公钥进行加密，只有卡套私钥可以成功解密，从而也可以保证数据解密的安全性。

卡套利用模拟卡片证书中的模拟卡片公钥、解密后的第一连接随机解密因子和第二连接随机解密因子对第二连接签名进行验证；具体地，卡套利用模拟卡片公钥对模拟卡片发送的签名进行验证，以确保数据的合法来源。

卡套验证第二连接签名正确后，验证解密后的第一连接随机解密因子与第一连接随机因子是否相同；具体地，卡套验证自身生成的第一连接随机因子与解密后的第一连接随机解密因子相同，可以保证数据并未被篡改，且加密的数据来源确实为卡套发送第一连接随机因子的对象。

卡套验证解密后的第一连接随机解密因子与第一连接随机因子相同后，至少利用第二连接随机解密因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片至少利用第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥。具体地，卡套可以利用第二连接随机解密因子生成卡套与模拟卡片间的卡套端第一安全传输密钥，也可以利用第一连接随机因子、第二连接随机解密因子生成卡套与模拟卡片间的卡套端第一安全传输密钥，还可以利用第一连接随机因子、第二连接随机解密因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；同样的，模拟卡片也可以利用第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥，也可以利用第一连接随机解密因子、第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥，还可以利用第一连接随机解密因子、第二连接随机因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥；只要卡套与模拟卡片采用相同的参数相同的算法生成安全传输密钥即可。由此可见，在本发明中，安全传输密钥因子在卡套端可以为第二连接随机解密因子，或者第二连接随机解密因子以及第一连接随机因子；安全传输密钥因子在模拟卡片端可以为第二连接随机因子，或者第二连接随机因子以及第一连接随机解密因子。另外，安全传输密钥可以包括加解密密钥和/或校验密钥，使用加解密密钥可以参与数据传输可以保证数据传输的安全性，使用校验密钥参与数据传输可以保证数据传输的完整性，在本发明中，可以根据传输数据的安全性等级选择性地使用安全传输密钥。

当然，本发明中，模拟卡片至少利用第二连接随机因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥的步骤并不局限于本方式一中的步骤，还可以在模拟卡片生成第二连

接随机因子之后生成模拟卡片端安全传输密钥，也可以在卡套验证解密后的第一连接随机解密因子与第一连接随机因子相同后，接收卡套发送的成功信息后生成模拟卡片端安全传输密钥。

由此可见，基于上述卡套与模拟卡片建立的安全连接，可以提高数据传输的安全性，
5 同时，还可以验证双方是否进行了绑定，进一步提高了安全性。

如果卡套与模拟卡片建立安全连接之前，执行了上述手动绑定并存储绑定因子等操作，则在本方式一中，卡套与模拟卡片除了互相认证对方身份之外，还需要互相认证对方证书。

此外，本发明并不局限于上述卡套发起安全连接的建立，还可以由卡套触发模拟卡片发起安全连接的建立，此时，由模拟卡片发送第一安全连接指令至卡套，其他流程与上述
10 流程实施主体相反即可实现，在此不再一一赘述。

方式二、卡套与模拟卡片互相认证对方身份（例如互相认证对方签名数据），并在互相认证对方身份过程中生成安全传输密钥因子，在互相认证对方身份通过后，至少利用存储的绑定因子和安全传输密钥因子生成卡套与模拟卡片之间进行数据安全传输的安全传输密钥（卡套端第一安全传输密钥和模拟卡片端安全传输密钥），并验证双方生成的安全传输密
15 钥是否相同。

值得说明的是，如果在卡套与模拟卡片建立安全连接之前，执行了上述卡套与模拟卡片互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子的绑定操作，则在本方式二中，卡套与模拟卡片互相认证对方身份即为卡套与模拟卡片再次互相认证对方身份。

20 以下，本发明提供方式二的一种具体实现：

图 8 示出了本发明实施例中卡套与模拟卡片建立安全连接方式二的流程图，应当理解的是，该建立安全连接方式二可以通过数据交互方法或数据交互系统实现。参见图 8，卡套与模拟卡片建立安全连接包括：

卡套接收模拟卡片发送的模拟卡片生成的第三连接随机因子以及模拟卡片唯一标识；
25 具体地，第三连接随机因子可以为模拟卡片生成的随机数、随机字符或其组合，当然，在生成第三连接随机因子后，还可以对第三连接随机因子的随机性进行验证，以提高第三连接随机因子的随机性，防止被破解。在本步骤之前，模拟卡片生成第三连接随机因子，在卡套检测到该模拟卡片后，模拟卡片将该第三连接随机因子以及模拟卡片唯一标识发送至卡套。

30 卡套向模拟卡片发送用于指示建立安全连接的第二安全连接指令，其中，第二安全连接指令包括：卡套唯一标识、卡套利用模拟卡片证书中的模拟卡片公钥对第三连接随机因子以及生成的第四连接随机因子进行加密获得的第三连接密文、卡套利用卡套私钥对第三

连接随机因子以及第四连接随机因子进行签名获得的第三连接签名；具体地，在使用卡套与模拟卡片进行数据交互之前，可选的，在卡套与模拟卡片之间建立安全连接，以提高后续数据交互的安全性。其中，卡套接收的用于指示建立安全连接的第二安全连接指令可以为单独设置在卡套上的连接物理按键生成的，或者可以为卡套的触屏上的连接虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为将模拟卡片从卡套拔出后生成的，或者可以为在卡套屏幕上显示的菜单中选择连接功能生成的，或者可以为在卡套获得卡套端真实卡片信息列表，用户从中选择真实卡片后生成的。当然，还可以为其他任何方式生成的，在本发明中并不作限制。具体地，卡套利用模拟卡片公钥对第三连接随机因子以及生成的第四连接随机因子进行加密以保证第三连接随机因子以及生成的第四连接随机因子传输的安全性，卡套利用卡套私钥对第三连接随机因子以及生成的第四连接随机因子进行签名，以保证后续模拟卡片可以对卡套身份的合法性进行认证。另外，第四连接随机因子可以为卡套生成的随机数、随机字符或其组合，当然，在生成第四连接随机因子后，还可以对第四连接随机因子的随机性进行验证，以提高第四连接随机因子的随机性，防止被破解；可选的，在本步骤之前，卡套接收到模拟卡片唯一标识之后，卡套可以根据模拟卡片唯一标识判断模拟卡片是否在卡套端第一绑定列表中，只有在判断模拟卡片在卡套端第一绑定列表中后，才执行后续流程，优化了流程，提高了效率。

模拟卡片接收第二安全连接指令，判断卡套唯一标识是否在模拟卡片端绑定列表中；具体地，模拟卡片根据接收到的卡套唯一标识，判断该卡套是否在模拟卡片端绑定列表中；只有在判断卡套在模拟卡片端绑定列表中后，才执行后续流程，优化了流程，提高了效率。

如果卡套唯一标识在模拟卡片端绑定列表中，模拟卡片利用模拟卡片私钥对第三连接密文进行解密，获得第三连接随机解密因子以及第四连接随机解密因子；具体地，利用模拟卡片私钥对第三连接密文进行解密，如果在数据传输中发生了数据传输错误，或者在数据传输中发生了篡改，则将导致无法成功解密，或者获得的第三连接随机解密因子以及第四连接随机解密因子与第三连接随机因子以及第四连接随机因子不同。而通过模拟卡片公钥进行加密，只有模拟卡片私钥可以成功解密，从而也可以保证数据解密的安全性。

模拟卡片利用卡套证书中的卡套公钥、第三连接随机解密因子以及第四连接随机解密因子对第三连接签名进行验证；具体地，模拟卡片利用卡套公钥对卡套发送的签名进行验证，以确保数据的合法来源。

模拟卡片验证第三连接签名正确后，验证第三连接随机解密因子与第三连接随机因子是否相同；具体地，模拟卡片验证自身生成的第三连接随机因子与第三连接随机解密因子相同，可以保证数据并未被篡改，且加密的数据来源确实为模拟卡片发送第三连接随机因子的对象。

如果第三连接随机解密因子与第三连接随机因子相同，模拟卡片利用模拟卡片私钥对第三连接随机解密因子以及第四连接随机解密因子进行签名获得第四连接签名；具体地，模拟卡片利用模拟卡片私钥对第三连接随机解密因子以及第四连接随机解密因子进行签名，以保证后续卡套可以对模拟卡片身份的合法性进行认证。

- 5 模拟卡片向卡套发送第二安全连接响应，其中，第二安全连接响应包括：第四连接签名；具体地，模拟卡片将第四连接签名发送至卡套，以便卡套对接收到的数据进行验证。

卡套接收第二安全连接响应，利用模拟卡片证书中的模拟卡片公钥、第三连接随机因子和第四连接随机因子对第四连接签名进行验证；具体地，卡套利用模拟卡片公钥对模拟卡片发送的签名进行验证，以确保数据的合法来源。

- 10 卡套验证第四连接签名正确后，至少利用第四连接随机因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；模拟卡片至少利用第四连接随机解密因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥；具体地，卡套可以利用第四连接随机因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥，也可以利用第三连接随机因子、第四连接随机因子以及卡套端第一绑定因子生成卡套与模拟卡片间的卡套端第一安全传输密钥；同样的，模拟卡片也可以利用第四连接随机解密因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥，也可以利用第三连接随机因子、第四连接随机解密因子以及模拟卡片端绑定因子生成卡套与模拟卡片间的模拟卡片端安全传输密钥；只要卡套与模拟卡片采用相同的参数相同的算法生成安全传输密钥即可。由此可见，在本发明中，安全传输密钥因子在卡套端可以为第四连接随机因子，或者第三连接随机因子以及第四连接随机因子；安全传输密钥因子在模拟卡片端可以为第四连接随机解密因子，或者第三连接随机因子以及第四连接随机解密因子。另外，安全传输密钥可以包括加解密密钥和/或校验密钥，使用加解密密钥可以参与数据传输可以保证数据传输的安全性，使用校验密钥参与数据传输可以保证数据传输的完整性，在本发明中，可以根据传输数据的安全性等级选择性地使用安全传输密钥。

- 25 卡套利用卡套端第一安全传输密钥对第三连接随机因子以及第四连接随机因子进行第一处理后发送至模拟卡片；模拟卡片利用模拟卡片端安全传输密钥对第三连接随机解密因子以及第四连接随机解密因子进行第一处理后发送至卡套；具体地，双方利用各自生成的安全传输密钥对数据进行第一处理后发送至对方，以便对方验证双方生成的安全传输密钥是否相同。

- 30 卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第三连接随机因子以及第四连接随机因子是否相同；模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二

处理，比较第二处理后的数据与第三连接随机解密因子以及第四连接随机解密因子是否相同。具体地，双方利用各自生成的安全传输密钥对接收到的数据进行第二处理后，各自比较第二处理后的数据是否与各自发送的数据相同，如果相同，则说明双方生成的安全传输密钥相同，以便保证双方后续可以利用各自生成的安全传输密钥进行数据安全传输。另外，
5 在验证双方生成的安全传输密钥相同的同时，也可以验证各自存储的绑定因子相同，进一步验证对方为真实的绑定对象，进一步提高后续数据传输的安全性。

当然，本发明中，模拟卡片生成模拟卡片端安全传输密钥的步骤并不局限于本方式二中的步骤，还可以在解密获得第四连接随机解密因子后生成模拟卡片端安全传输密钥，也可以在卡套验证模拟卡片发送的第四连接签名无误后，接收卡套发送的成功信息后生成模拟卡片端安全传输密钥；卡套生成卡套端第一安全传输密钥的步骤也不局限于本方式二中的步骤，还可以在卡套生成第四连接随机因子后生成卡套端第一安全传输密钥。
10

由此可见，基于上述卡套与模拟卡片建立的安全连接，可以提高数据传输的安全性，同时，还可以验证双方是否进行了绑定，进一步提高了安全性。

如果卡套与模拟卡片建立安全连接之前，执行了上述手动绑定并存储绑定因子等操作，
15 则在本方式二中，卡套与模拟卡片除了互相认证对方身份之外，还需要互相认证对方证书。

此外，本发明并不局限于上述卡套发起安全连接的建立，还可以由卡套触发模拟卡片发起安全连接的建立，此时，由模拟卡片发送第二安全连接指令至卡套，其他流程与上述流程实施主体相反即可实现，在此不再一一赘述。

当然，在上述方式一和方式二中生成卡套与模拟卡片之间进行数据安全传输的安全传输密钥的过程中，采用的绑定因子为卡套与模拟卡片在绑定过程中生成并保存的绑定因子，该绑定因子可以为通过上述卡套与模拟卡片互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子，或者可以为通过手动绑定的方式输入并存储的绑定因子。
20

另外，如果卡套与模拟卡片之间并未执行绑定操作，则上述方式一和方式二中采用的绑定因子可以为在建立安全连接过程中手动输入的随机值；或者在建立安全连接过程中，仅通过随机因子生成安全传输密钥，不予对绑定因子进行验证或者不采用绑定因子生成安全传输密钥。
25

2、卡套与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥：

30 在本发明中，卡套与真实卡片管理器可以通过如下方式建立安全连接：

方式一、卡套与真实卡片管理器互相认证对方身份，并在互相认证对方身份的过程中，比较双方存储的绑定因子是否相同，在比较双方存储的绑定因子相同且互相认证对方身份

通过后，生成卡套与真实卡片管理器之间进行数据安全传输的安全传输密钥（卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥）。

值得说明的是，如果在卡套与真实卡片管理器建立安全连接之前，执行了上述卡套与真实卡片管理器互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子的绑定操作，则在本方式一中，卡套与真实卡片管理器互相认证对方身份即为卡套与真实卡片管理器再次互相认证对方身份。

卡套与真实卡片管理器采用方式一建立安全连接的方案与卡套与模拟卡片采用方式一建立安全连接的方案区别仅在于：

一是执行主体不同：在卡套与真实卡片管理器采用方式一建立安全连接的方案中，执行主体为卡套和真实卡片管理器；在卡套与模拟卡片采用方式一建立安全连接的方案中，执行主体为卡套和模拟卡片。其中，卡套在该两种方案中执行操作相同，真实卡片管理器和模拟卡片在该两种方案中执行操作相同。

二是安全连接指令的生成方式不同：在卡套与真实卡片管理器采用方式一建立安全连接的方案中，第三安全连接指令可以为单独设置在卡套上的连接物理按键生成的，或者可以为卡套的触屏上的连接虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为卡套向真实卡片管理器发送登录请求时生成的，或者可以为在卡套屏幕上显示的菜单中选择连接功能生成的。

以下，仅对卡套与真实卡片管理器采用方式一建立安全连接的方案进行简单说明如下，在此不再详述。

图 9 示出了本发明实施例中卡套与真实卡片管理器建立安全连接方式一的流程图，应当理解的是，该建立安全连接方式一可以通过数据交互方法或数据交互系统实现。参见图 9，卡套与真实卡片管理器建立安全连接包括：

卡套向真实卡片管理器发送用于指示建立安全连接的第三安全连接指令，其中，第三安全连接指令包括：卡套利用真实卡片管理器证书中的真实卡片管理器公钥对卡套端第二绑定因子以及生成的第五连接随机因子进行加密获得的第五连接密文，卡套利用卡套私钥对卡套端第二绑定因子以及第五连接随机因子进行签名获得的第五连接签名；

真实卡片管理器接收第三安全连接指令，利用真实卡片管理器私钥对第五连接密文进行解密，获得卡套端第二绑定解密因子以及第五连接随机解密因子；

真实卡片管理器利用卡套证书中的卡套公钥、卡套端第二绑定解密因子以及第五连接随机解密因子对第五连接签名进行验证；

真实卡片管理器验证第五连接签名正确后，验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子是否相同；

真实卡片管理器验证卡套端第二绑定解密因子与真实卡片管理器端绑定因子相同后，生成第六连接随机因子；

真实卡片管理器利用卡套证书中的卡套公钥对第五连接随机解密因子以及第六连接随机因子进行加密获得第六连接密文，利用真实卡片管理器私钥对第五连接随机解密因子以及第六连接随机因子进行签名获得第六连接签名；

真实卡片管理器向卡套发送第三安全连接响应，其中，第三安全连接响应包括：第六连接密文以及第六连接签名；

卡套接收第三安全连接响应，利用卡套私钥对第六连接密文进行解密，获得解密后的第五连接随机解密因子和第六连接随机解密因子；

卡套利用真实卡片管理器证书中的真实卡片管理器公钥、解密后的第五连接随机解密因子和第六连接随机解密因子对第六连接签名进行验证；

卡套验证第六连接签名正确后，验证解密后的第五连接随机解密因子与第五连接随机因子是否相同；

卡套验证解密后的第五连接随机解密因子与第五连接随机因子相同后，至少利用第六连接随机解密因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器至少利用第六连接随机因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥。

当然，本发明中，真实卡片管理器至少利用第六连接随机因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥的步骤并不局限于本方式一中的步骤，还可以在真实卡片管理器生成第六连接随机因子之后生成真实卡片管理器端安全传输密钥，也可以在卡套验证解密后的第五连接随机解密因子与第五连接随机因子相同后，接收卡套发送的成功信息后生成真实卡片管理器端安全传输密钥。

由此可见，基于上述卡套与真实卡片管理器建立的安全连接，可以提高数据传输的安全性，同时，还可以验证双方是否进行了绑定，进一步提高了安全性。

如果卡套与真实卡片管理器建立安全连接之前，执行了上述手动绑定并存储绑定因子等操作，则在本方式一中，卡套与真实卡片管理器除了互相认证对方身份之外，还需要互相认证对方证书。

此外，本发明并不局限于上述卡套发起安全连接的建立，还可以由卡套触发真实卡片管理器发起安全连接的建立，此时，由真实卡片管理器发送第三安全连接指令至卡套，其他流程与上述流程实施主体相反即可实现，在此不再一一赘述。

方式二、卡套与真实卡片管理器互相认证对方身份，并在互相认证对方身份过程中生成安全传输密钥因子，在互相认证对方身份通过后，至少利用存储的绑定因子和安全传输

密钥因子生成卡套与真实卡片管理器之间进行数据安全传输的安全传输密钥（卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥），并验证双方生成的安全传输密钥是否相同。

值得说明的是，如果在卡套与真实卡片管理器建立安全连接之前，执行了上述卡套与真实卡片管理器互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子的绑定操作，则在本方式二中，卡套与真实卡片管理器互相认证对方身份即为卡套与真实卡片管理器再次互相认证对方身份。

卡套与真实卡片管理器采用方式二建立安全连接的方案与卡套与模拟卡片采用方式二建立安全连接的方案区别仅在于：

一是执行主体不同：在卡套与真实卡片管理器采用方式二建立安全连接的方案中，执行主体为卡套和真实卡片管理器；在卡套与模拟卡片采用方式二建立安全连接的方案中，执行主体为卡套和模拟卡片。其中，卡套在该两种方案中执行操作相同，真实卡片管理器和模拟卡片在该两种方案中执行操作相同。

二是安全连接指令的生成方式不同：在卡套与真实卡片管理器采用方式二建立安全连接的方案中，第四安全连接指令可以为单独设置在卡套上的连接物理按键生成的，或者可以为卡套的触屏上的连接虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为卡套向真实卡片管理器发送登录请求时生成的，或者可以为在卡套屏幕上显示的菜单中选择连接功能生成的。

以下，仅对卡套与真实卡片管理器采用方式二建立安全连接的方案进行简单说明如下，在此不再详述。

图 10 示出了本发明实施例提供的交互方法中卡套与真实卡片管理器建立安全连接方式二的流程图，应当理解的是，该建立安全连接方式二可以通过数据交互方法或数据交互系统实现。参见图 10，卡套与真实卡片管理器建立安全连接包括：

卡套接收真实卡片管理器发送的真实卡片管理器生成的第七连接随机因子和真实卡片管理器唯一标识；

卡套向真实卡片管理器发送用于指示建立安全连接的第四安全连接指令，其中，第四安全连接指令包括：卡套唯一标识、卡套利用真实卡片管理器证书中的真实卡片管理器公钥对第七连接随机因子以及生成的第八连接随机因子进行加密获得的第七连接密文、卡套利用卡套私钥对第七连接随机因子以及第八连接随机因子进行签名获得的第七连接签名；

真实卡片管理器接收第四安全连接指令，判断卡套唯一标识是否在真实卡片管理器端绑定列表中；

如果卡套唯一标识在真实卡片管理器端绑定列表中，真实卡片管理器利用真实卡片管

理器私钥对第七连接密文进行解密，获得第七连接随机解密因子以及第八连接随机解密因子；

真实卡片管理器利用卡套证书中的卡套公钥、第七连接随机解密因子以及第八连接随机解密因子对第七连接签名进行验证；

- 5 真实卡片管理器验证第七连接签名正确后，验证第七连接随机解密因子与第七连接随机因子是否相同；

如果第七连接随机解密因子与第七连接随机因子相同，真实卡片管理器利用真实卡片管理器私钥对第七连接随机解密因子以及第八连接随机解密因子进行签名获得第八连接签名；

- 10 真实卡片管理器向卡套发送第四安全连接响应，其中，第四安全连接响应包括：第八连接签名；

卡套接收第四安全连接响应，利用真实卡片管理器证书中的真实卡片管理器公钥、第七连接随机因子和第八连接随机因子对第八连接签名进行验证；

- 卡套验证第八连接签名正确后，至少利用第八连接随机因子以及卡套端第二绑定因子生成卡套与真实卡片管理器间的卡套端第二安全传输密钥；真实卡片管理器至少利用第八连接随机解密因子以及真实卡片管理器端绑定因子生成卡套与真实卡片管理器间的真实卡片管理器端安全传输密钥；
- 15

- 卡套利用卡套端第二安全传输密钥对第七连接随机因子以及第八连接随机因子进行第一处理后发送至真实卡片管理器；真实卡片管理器利用真实卡片管理器端安全传输密钥对第七连接随机解密因子以及第八连接随机解密因子进行第一处理后发送至卡套；
- 20

- 卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机因子以及第八连接随机因子是否相同；真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理，比较第二处理后的数据与第七连接随机解密因子以及第八连接随机解密因子是否相同。
- 25

由此可见，基于上述卡套与真实卡片管理器建立的安全连接，可以提高数据传输的安全性，同时，还可以验证双方是否进行了绑定，进一步提高了安全性。

- 当然，本发明中，真实卡片管理器生成真实卡片管理器端安全传输密钥的步骤并不局限于本方式二中的步骤，还可以在解密获得第八连接随机解密因子后生成真实卡片管理器端安全传输密钥，也可以在卡套验证真实卡片管理器发送的第八连接签名无误后，接收卡套发送的成功信息后生成真实卡片管理器端安全传输密钥；卡套生成卡套端第二安全传输密钥的步骤也不局限于本方式二中的步骤，还可以在卡套生成第八连接随机因子后生成卡
- 30

套端第二安全传输密钥。

如果卡套与真实卡片管理器建立安全连接之前，执行了上述手动绑定并存储绑定因子等操作，则在本方式二中，卡套与真实卡片管理器除了互相认证对方身份之外，还需要互相认证对方证书。

- 5 此外，本发明并不局限于上述卡套发起安全连接的建立，还可以由卡套触发真实卡片管理器发起安全连接的建立，此时，由真实卡片管理器发送第四安全连接指令至卡套，其他流程与上述流程实施主体相反即可实现，在此不再一一赘述。

当然，在上述方式一和方式二中生成卡套与真实卡片管理器之间进行数据安全传输的安全传输密钥的过程中，采用的绑定因子为卡套与真实卡片管理器在绑定过程中生成并保存的绑定因子，该绑定因子可以为通过上述卡套与真实卡片管理器互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子，或者可以为通过手动绑定的方式输入并存储的绑定因子。

10 另外，如果卡套与真实卡片管理器之间并未执行绑定操作，则上述方式一和方式二中采用的绑定因子可以为在建立安全连接过程中手动输入的随机值；或者在建立安全连接过程中，仅通过随机因子生成安全传输密钥，不予对绑定因子进行验证或者不采用绑定因子生成安全传输密钥。

另外，在本发明卡套与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥之前，卡套向真实卡片管理器发送登录请求；具体地，登录请求可以为单独设置在卡套上的登录物理按键生成的，或者可以为卡套的触屏上的登录虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为在卡套屏幕上显示的菜单中选择登录功能生成的；登录请求可以包括卡套唯一标识，以便真实卡片管理器知晓哪个卡套请求进行登录。

20 在卡套向真实卡片管理器发送登录请求，卡套与真实卡片管理器建立安全连接，获得卡套与真实卡片管理器之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥之后：

卡套通过卡套端第二安全传输密钥对接收到的登录密码进行第一处理后发送至真实卡片管理器；具体地，卡套还可以提示用户输入登录密码，在用户输入了登录密码后，利用卡套端第二安全传输密钥对登录密码进行第一处理后发送至真实卡片管理器，可以提高登录密码传输的安全性。

30 真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性；具体地，真实卡片管理器利用真实卡片管理器端安全传输密钥对卡套发送的数据进行第二处理后，获得用户输入的登录密

码，与其存储的合法登录密码进行比较，只有在用户输入的登录密码与其存储的合法登录密码相同时，才允许卡套登录真实卡片管理器，提高登录安全性，保证后续数据传输的安全性。如果本发明中真实卡片管理器具备报警功能，则可以预先在真实卡片管理器中设置合法登录密码和合法报警密码，此时，真实卡片管理器利用真实卡片管理器端安全传输密
5 钥对接收到的数据进行第二处理后，获得待验证密码；真实卡片管理器判断待验证密码是否为报警密码；如果待验证密码为报警密码，则真实卡片管理器确定待验证密码验证通过，并执行报警操作；如果待验证密码不是报警密码且为登录密码，则真实卡片管理器确定待验证密码验证通过。由于设置了报警密码，当用户输入的登录密码为报警密码时，真实卡片管理器可以识别出当前登录存在安全风险，并执行报警操作（例如真实卡片管理器发送
10 报警短信、拨打报警电话至执法部门等）。

真实卡片管理器在验证第二处理后的数据通过后，卡套登录真实卡片管理器。

由此可见，在建立卡套与真实卡片管理器之间的安全连接前，卡套先行发起登录请求，并在卡套发送登录请求的同时触发安全连接的建立，并在安全连接建立后，对登录密码进行验证，可以节约流程，提高处理速度。

15 另外，为了保证卡套端真实卡片信息列表的有效性，在卡套与真实卡片管理器建立安全连接，且卡套登录真实卡片管理器之后，卡套端真实卡片信息列表还可以通过如下方式进行更新：

方式一、卡套登录真实卡片管理器后，真实卡片管理器判断是否需要进行卡套端真实卡片信息列表的更新操作：

20 以下提供方式一的一种实现方案：

卡套查找卡套端标识列表；具体地，卡套端标识列表为卡套从真实卡片管理器中获取的真实卡片管理器端标识列表。

如果卡套查找到卡套端标识列表，则利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，利用真实
25 卡片管理器端安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同，如果不相同，则真实卡片管理器利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套，卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表；具体地，更新卡套端真实卡片信息列表
30 可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管

理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，

- 5 卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

- 如果卡套未查找到卡套端标识列表，则利用卡套端第二安全传输密钥对预设标识进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，真实卡片管理器确定第二处理后的数据用于指示卡套端未存储卡套端标识列表时，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套，卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括存储指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，
- 10 卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行存储操作。

- 基于方式一的上述实现方案，卡套通过将卡套端标识列表发送至真实卡片管理器进行判断是否一致，由于卡套端标识列表数据量远小于卡套端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了真实卡片管理器的判断速率。如果
- 20 卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，发送预设标识至真实卡片管理器，以便真实卡片管理器下发真实卡片管理器端标识列表以及真实卡片管理器端真实卡片信息列表至卡套，该预设标识可以为空标识、预定义数值、或者预定义字符等。

当然，本发明并不局限于方式一的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

- 25 由卡套向真实卡片管理器直接发送卡套端真实卡片信息列表，以便真实卡片管理器进行比对后判断是否更新；或者

由卡套向真实卡片管理器发送卡套端真实卡片信息列表的列表编号，以便真实卡片管理器比对列表编号是否相同判断是否更新；或者

- 30 由真实卡片管理器接收到用户输入的更新指令后，真实卡片管理器将真实卡片管理器端真实卡片信息列表发送至卡套。

当然，在真实卡片管理器判断出需要进行更新后，还可以发送更新询问请求至卡套，卡套提示该更新询问请求给用户，以使用户确认是否进行更新。

方式二、卡套登录真实卡片管理器后，卡套判断是否需要卡套端真实卡片信息列表更新操作：

真实卡片管理器利用真实卡套管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；

- 5 卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；具体地，如果卡套第一次使用或从未成功下载真实卡片管理器端标识列表，并未存储卡套端标识列表，则直接判定为不同即可。

如果不相同，则卡套向真实卡片管理器发送更新请求；

- 10 真实卡片管理器接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；

- 卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。
- 15
- 20

- 基于方式二的上述实现方案，真实卡片管理器通过将真实卡片管理器端标识列表发送至卡套进行判断是否一致，由于真实卡片管理器端标识列表数据量远小于真实卡片管理器端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了卡套的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，接收到真实卡片管理器下发真实卡片管理器端标识列表后，直接发送更新请求以便真实卡片管理器发送真实卡片管理器端真实卡片信息列表至卡套。
- 25

- 当然，本发明并不局限于方式二的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：
- 30

由真实卡片管理器直接向卡套发送真实卡片管理器端真实卡片信息列表，以便卡套直接存储；或者

由真实卡片管理器向卡套发送真实卡片管理器端真实卡片信息列表的列表编号，以便卡套比对列表编号是否相同判断是否更新；或者

由卡套接收到用户输入的更新指令后，卡套发送更新请求至真实卡片管理器，以便真实卡片管理器直接下发真实卡片管理器端真实卡片信息列表发送至卡套。

- 5 当然，在卡套判断出需要进行更新后，还可以提示用户确认是否进行更新，并在用户确认进行更新后，执行后续更新操作。

本发明的卡套除了具备正常工作模式之外，还具有心跳休眠模式，其中，心跳休眠模式为低功耗的非工作模式，即关闭一些不必要的耗电程序等。具体地，卡套可以在预设时间内没有操作后进入心跳休眠模式，也可以由用户的操作控制进入心跳休眠模式。

- 10 卡套在心跳休眠模式下，还可以判断是否保持卡套与真实卡片管理器之间建立的安全连接，以便在卡套由心跳休眠模式下恢复至工作模式时，无需再次与真实卡片管理器建立安全连接，提高便捷性。

以下提供一种卡套在心跳休眠模式下判断是否保持卡套与真实卡片管理器之间建立的安全连接的具体实现方式：

- 15 卡套在心跳休眠模式下，每隔第一预设时间向真实卡片管理器发送检测信息；
真实卡片管理器接收到检测信息，向卡套发送响应信息；

如果卡套在第二预设时间内未收到响应信息，则断开卡套与真实卡片管理器之间的安全连接；

- 20 如果卡套在第二预设时间内收到响应信息，则保持卡套与真实卡片管理器建立的安全连接。

卡套在第二预设时间内未收到响应信息，可能为卡套与真实卡片管理器之间的网络不稳定，或者真实卡片管理器工作异常，此时断开卡套与真实卡片管理器之间的安全连接保证了安全性；卡套在第二预设时间内收到响应信息，则卡套保持与真实卡片管理器之间的安全连接，在卡套恢复工作模式时，无需重新建立安全连接，方便使用。

- 25 当然，在心跳休眠模式下，用户也可以选择手动断开卡套与真实卡片管理器之间的安全连接，例如令卡套从真实卡片管理器中退出登录等操作，或者用户对卡套执行关机操作。

上述第一预设时间可以与第二预设时间相同或者不同。

以下提供在心跳休眠模式下，卡套端真实卡片信息列表更新的方式：

- 30 方式三、卡套登录真实卡片管理器后，卡套处于心跳休眠模式下，卡套判断是否需要
进行卡套端真实卡片信息列表更新操作：

在心跳休眠模式下，如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，则卡套存储更新提示信息；其中，更新提示信息为真实卡片管理器告知卡

套真实卡片管理器有真实卡片管理器端真实卡片信息列表更新的提示信息。

在卡套由心跳休眠模式进入工作模式后，卡套向真实卡片管理器发送更新触发请求；具体地，卡套可以通过如下方式由心跳休眠模式进入工作模式：卡套收到更新提示信息后自动进入工作模式，或者卡套接收用户输入的操作指令（例如用户进行按键输入的操作指令等）后，进入工作模式。

真实卡片管理器接收更新触发请求，利用真实卡片管理器端安全传输密钥对真实卡片管理器端标识列表进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与卡套存储的卡套端标识列表是否相同；具体地，如果卡套第一次使用或从未成功下载真实卡片管理器端标识列表，并未存储卡套端标识列表，则直接判定为不同即可。

如果不相同，则卡套向真实卡片管理器发送更新请求；

真实卡片管理器接收更新请求，利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；

卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

基于方式三的上述实现方案，真实卡片管理器通过将真实卡片管理器端标识列表发送至卡套进行判断是否一致，由于真实卡片管理器端标识列表数据量远小于真实卡片管理器端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了卡套的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，接收到真实卡片管理器下发真实卡片管理器端标识列表后，直接发送更新请求以便真实卡片管理器发送真实卡片管理器端真实卡片信息列表至卡套。

当然，本发明并不局限于方式三的上述实现方案，还可以在卡套和真实卡片管理器并

不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

由真实卡片管理器直接向卡套发送真实卡片管理器端真实卡片信息列表，以便卡套直接存储；或者

由真实卡片管理器向卡套发送真实卡片管理器端真实卡片信息列表的列表编号，以便卡套比对列表编号是否相同判断是否更新；或者

由卡套接收到用户输入的更新指令后，卡套发送更新请求至真实卡片管理器，以便真实卡片管理器直接下发真实卡片管理器端真实卡片信息列表发送至卡套。

方式四、卡套登录真实卡片管理器后，卡套处于心跳休眠模式下，真实卡片管理器判断是否需要卡套端真实卡片信息列表更新操作：

卡套在心跳休眠模式下，如果卡套在第二预设时间内收到响应信息，且响应信息中还包含更新提示信息，则卡套存储更新提示信息；其中，更新提示信息为真实卡片管理器告知卡套真实卡片管理器有真实卡片管理器端真实卡片信息列表更新的提示信息。

在卡套由心跳休眠模式进入工作模式后，卡套利用卡套端第二安全传输密钥对卡套端标识列表进行第一处理后发送至真实卡片管理器；具体地，卡套可以通过如下方式由心跳休眠模式进入工作模式：卡套收到更新提示信息后自动进入工作模式，或者卡套接收用户输入的操作指令（例如用户进行按键输入的操作指令等）后，进入工作模式。如果卡套为第一次使用或者从未成功下载真实卡片管理器端标识列表，则卡套中并未存储卡套端标识列表，此时，卡套利用卡套端第二安全传输密钥对预设标识进行第一处理后发送至真实卡片管理器。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，判断第二处理后的数据与真实卡片管理器存储的真实卡片管理器端标识列表是否相同；具体地，真实卡片管理器接收到预设标识，也判断为不相同。

如果不相同，则真实卡片管理器利用真实卡片管理器端安全传输密钥对更新指令和更新数据进行第一处理后发送至卡套；

卡套接收到真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，更新卡套端真实卡片信息列表。具体地，更新卡套端真实卡片信息列表可以通过如下方式进行：真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加或者删除的真实卡片信息，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者真实卡片管理器发送的更新指令包括增加和/或删除指令，更新数据包括需要增加真实卡片信息或者需要删除的真实卡片信息对应的标识，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行增加和/或删除操作；或者，真实卡片管理器发

送的更新指令包括替换指令，更新数据包括最新的真实卡片管理器端真实卡片信息列表，卡套在接收到更新指令和更新数据后，根据更新指令和更新数据对卡套端真实卡片信息列表执行替换操作。

基于方式四的上述实现方案，卡套通过将卡套端标识列表发送至真实卡片管理器进行判断是否一致，由于卡套端标识列表数据量远小于卡套端真实卡片信息列表，因此，减小了数据传输的数据量，提高了数据传输速率，也提高了真实卡片管理器的判断速率。如果卡套为第一次使用，则卡套本身并未存储卡套端标识列表，此时，发送预设标识至真实卡片管理器，以便真实卡片管理器下发真实卡片管理器端标识列表以及真实卡片管理器端真实卡片信息列表至卡套，该预设标识可以为空标识、预定义数值、或者预定义字符等。

当然，本发明并不局限于方式四的上述实现方案，还可以在卡套和真实卡片管理器并不存储标识列表时，通过如下方式之一实现卡套端真实卡片信息列表的更新：

由卡套向真实卡片管理器直接发送卡套端真实卡片信息列表，以便真实卡片管理器进行比对后判断是否更新；或者

由卡套向真实卡片管理器发送卡套端真实卡片信息列表的列表编号，以便真实卡片管理器比对列表编号是否相同判断是否更新；或者

由真实卡片管理器接收到用户输入的更新指令后，真实卡片管理器将真实卡片管理器端真实卡片信息列表发送至卡套。

可选的，在真实卡片管理器开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限后，由于真实卡片管理器端真实卡片信息列表进行了更新，因此，真实卡片管理器会将开放了卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限的真实卡片信息发送至卡套，以便卡套更新卡套端真实卡片信息列表；或者在真实卡片管理器开放或关闭卡套对重要卡片区域内的全部或者部分真实卡片进行连接使用的权限后，触发卡套端真实卡片信息列表更新的流程，更新方式可以参照上述方式一和方式二的更新方式，在此不再详述。

六、绑定：

为了进一步提高数据交互的安全性，在卡套与模拟卡片建立安全连接之前，还可以包括：卡套与模拟卡片执行绑定操作的流程；

在卡套与真实卡片管理器建立安全连接之前，还可以包括：卡套与真实卡片管理器执行绑定操作的流程。

当然，上述两个流程可以同时执行，也可以不同时执行，可以仅执行其中一个流程，也可以两个流程均执行。

1、卡套与模拟卡片执行绑定操作：

在本发明中，卡套与模拟卡片可以通过如下方式进行绑定：

卡套与模拟卡片互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子。

5 以下，提供一种卡套与模拟卡片执行绑定操作的具体实现方式：

图 11 示出了本发明实施例中卡套与模拟卡片执行绑定操作的流程图，应当理解的是，该绑定操作可以通过数据交互方法或数据交互系统实现。参见图 11，卡套与模拟卡片执行绑定操作包括：

卡套接收用于指示与模拟卡片进行绑定的触发命令；具体地，在卡套使用之前，可以
10 先行对卡套执行开机操作，此时，可选的，卡套提示用户输入开机密码，并接收用户输入的开机密码，验证用户输入的开机密码的正确性，在验证用户输入的开机密码正确后，执行开机操作，卡套进入工作模式。在使用卡套与模拟卡片进行数据交互之前，可选的，将卡套与模拟卡片进行绑定，以提高后续数据交互的安全性。其中，卡套接收的用于指示卡套与模拟卡片进行绑定的触发命令可以为单独设置在卡套上的绑定物理按键生成的，或者
15 可以为卡套的触屏上的绑定虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为将模拟卡片插入至卡套后生成的，或者可以为在卡套屏幕上显示的菜单中选择绑定功能生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

卡套向模拟卡片发送第一绑定指令，其中，第一绑定指令包括：卡套生成的第一绑定随机因子、卡套证书以及卡套唯一标识；具体地，卡套可以通过接触式连接（通过接触式
20 接口）向模拟卡片发送第一绑定指令，卡套还可以通过非接触式连接（通过非接触式接口或者无线接口）向模拟卡片发送第一绑定指令，前者可以提高绑定安全性，后者可以提高绑定便捷性。第一绑定指令中携带第一绑定随机因子可以防止重放攻击，第一绑定指令中携带卡套证书以便模拟卡片对卡套进行认证，第一绑定指令中携带卡套唯一标识以便模拟卡片获知哪个卡套与其绑定；其中，第一绑定随机因子可以为卡套生成的随机数、随机字符或其组合，当然，在生成第一绑定随机因子后，还可以对第一绑定随机因子的随机性进行验证，以提高第一绑定随机因子的随机性，防止被破解；卡套唯一标识可以为卡套序列号、设备识别码、MAC 地址等任一或其组合以唯一标识卡套的标识。

模拟卡片接收第一绑定指令，利用根证书对卡套证书进行验证；具体地，模拟卡片预先存储根证书，利用该根证书完成对卡套证书的验证，以保证后续使用卡套证书的安全性。

30 模拟卡片验证卡套证书合法后，生成第二绑定随机因子；具体地，第二绑定随机因子可以为模拟卡片生成的随机数、随机字符或其组合；当然，在生成第二绑定随机因子后，还可以对第二绑定随机因子的随机性进行验证，以提高第二绑定随机因子的随机性，防止

被破解。

模拟卡片利用卡套证书中的卡套公钥对第一绑定随机因子以及第二绑定随机因子进行加密获得第一绑定密文，利用模拟卡片私钥对第一绑定随机因子以及第二绑定随机因子进行签名获得第一绑定签名；具体地，模拟卡片利用卡套公钥对第一绑定随机因子以及第二绑定随机因子进行加密以保证第一绑定随机因子以及第二绑定随机因子传输的安全性，模拟卡片利用模拟卡片私钥对第一绑定随机因子以及第二绑定随机因子进行签名，以保证后续卡套可以对模拟卡片身份的合法性进行认证。

模拟卡片向卡套发送第一绑定响应，其中，第一绑定响应包括：第一绑定密文、第一绑定签名、模拟卡片证书以及模拟卡片唯一标识；具体地，模拟卡片发送的第一绑定响应中携带模拟卡片证书以便卡套对模拟卡片进行认证，第一绑定响应中携带模拟卡片唯一标识以便卡套获知哪个模拟卡片与其绑定；其中，模拟卡片唯一标识可以为模拟卡片序列号、设备识别码、MAC 地址等任一或其组合以唯一标识模拟卡片的标识。

卡套接收第一绑定响应，利用根证书对模拟卡片证书进行验证；具体地，卡套预先存储根证书，利用该根证书完成对模拟卡片证书的验证，以保证后续使用模拟卡片证书的安全性。

卡套验证模拟卡片证书合法后，利用卡套私钥对第一绑定密文进行解密，获得第一绑定随机解密因子和第二绑定随机解密因子；具体地，利用卡套私钥对第一绑定密文进行解密，如果在数据传输中发生了数据传输错误，或者在数据传输中发生了篡改，则将导致无法成功解密，或者解密出的第一绑定随机解密因子以及第二绑定随机解密因子与第一绑定随机因子以及第二绑定随机因子不同。而通过卡套公钥进行加密，只有卡套私钥可以成功解密，从而也可以保证数据解密的安全性。

卡套利用模拟卡片证书中的模拟卡片公钥、第一绑定随机解密因子以及第二绑定随机解密因子对第一绑定签名进行验证；具体地，卡套利用验证通过后的模拟卡片公钥对模拟卡片发送的签名进行验证，以确保数据的合法来源。

卡套验证第一绑定签名正确后，验证第一绑定随机解密因子与第一绑定随机因子是否相同；具体地，卡套验证自身生成的第一绑定随机因子与第一绑定随机解密因子相同，可以保证数据并未被篡改，且加密的数据来源确实为卡套发送第一绑定随机因子的对象。

卡套验证第一绑定随机解密因子与第一绑定随机因子相同后，提示模拟卡片唯一标识；具体地，卡套可以显示模拟卡片唯一标识，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）模拟卡片唯一标识，以便用户对模拟卡片的真实性进行确认，提高绑定安全性。

卡套接收用于确认模拟卡片唯一标识正确的触发命令，利用卡套私钥对第一绑定随机

因子以及第二绑定随机解密因子进行签名，获得第二绑定签名，以及存储模拟卡片唯一标识、模拟卡片证书以及卡套端第一绑定因子至卡套端第一绑定列表，其中，卡套端第一绑定因子为第二绑定随机解密因子；具体地，卡套接收的用于确认模拟卡片唯一标识正确的触发命令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制；利用卡套私钥对第一绑定随机因子以及第二绑定随机解密因子进行签名以便后续模拟卡片对卡套的身份进行认证；当然，卡套还可以存储卡套端第一绑定列表，该卡套端第一绑定列表用于记录与卡套绑定的模拟卡片的相关信息，例如：模拟卡片唯一标识、模拟卡片证书等，另外，卡套端第一绑定列表还用于存储卡套端第一绑定因子，该卡套端第一绑定因子为密文传输的第二绑定随机因子，基于第二绑定随机因子是密文传输的，因此，该卡套端第一绑定因子是安全且未被篡改的。

卡套向模拟卡片发送第二绑定签名；具体地，卡套向模拟卡片发送第二绑定签名，以便模拟卡片对卡套身份进行认证。

模拟卡片接收第二绑定签名，利用卡套证书中的卡套公钥、第一绑定随机因子以及第二绑定随机因子对第二绑定签名进行验证；具体地，模拟卡片利用验证通过后的卡套公钥对卡套发送的签名进行验证，以确保数据的合法来源。

模拟卡片验证第二绑定签名正确后，存储卡套唯一标识、卡套证书以及模拟卡片端绑定因子至模拟卡片端绑定列表，其中，模拟卡片端绑定因子为第二绑定随机因子。具体地，模拟卡片还可以存储模拟卡片端绑定列表，该模拟卡片端绑定列表用于记录与模拟卡片绑定的卡套的相关信息，例如：卡套唯一标识、卡套证书等，另外，模拟卡片端绑定列表还用于存储模拟卡片端绑定因子，该模拟卡片端绑定因子为模拟卡片生成的第二绑定随机因子。

由此可见，基于上述卡套和模拟卡片进行绑定，可以保证后续卡套和模拟卡片之间数据交互的安全性。

另外，上述卡套与模拟卡片执行绑定的操作并非必须的步骤，根据不同应用场景的需求，可以选择不执行上述卡套与模拟卡片执行绑定的操作。

当然，上述卡套与模拟卡片执行绑定的操作，并不局限于上述提供的实现方式，例如还可以采用手动绑定，即在可信环境下，在卡套上输入待绑定的模拟卡片的标识作为卡套端第一绑定因子，模拟卡片默认模拟卡片的标识作为模拟卡片端绑定因子；或者将卡套与

模拟卡片进行接触式连接，在卡套上输入任意随机值作为卡套端第一绑定因子，卡套通过接触式连接将输入的随机值发送至模拟卡片作为模拟卡片端绑定因子等等，只要可以使得卡套与模拟卡片均获得相同的绑定因子均应属于本发明的保护范围。

2、卡套与真实卡片管理器执行绑定操作：

5 在本发明中，卡套与真实卡片管理器可以通过如下方式进行绑定：

卡套与真实卡片管理器互相认证对方证书及对方身份，并在双方均认证通过后，各自存储在认证过程中生成的绑定因子。

以下，提供一种卡套与真实卡片管理器执行绑定操作的具体实现方式：

10 图 12 示出了本发明实施例中卡套与真实卡片管理器执行绑定操作的流程图，应当理解的是，该绑定操作可以通过数据交互方法或数据交互系统实现。参见图 12，卡套与真实卡片管理器执行绑定操作包括：

卡套接收用于指示与真实卡片管理器进行绑定的触发命令；具体地，在卡套使用之前，可以先行对卡套执行开机操作，此时，可选的，卡套提示用户输入开机密码，并接收用户输入的开机密码，验证用户输入的开机密码的正确性，在验证用户输入的开机密码正确后，
15 执行开机操作，卡套进入工作模式。在使用卡套与真实卡片管理器进行数据交互之前，可选的，将卡套与真实卡片管理器进行绑定，以提高后续数据交互的安全性。其中，卡套接收的用于指示卡套与真实卡片管理器进行绑定的触发命令可以为单独设置在卡套上的绑定物理按键生成的，或者可以为卡套的触屏上的绑定虚拟按键生成的，或者可以为开机密码验证正确后生成的，或者可以为在卡套屏幕上显示的菜单中选择绑定功能生成的，当然，
20 还可以为其他任何方式生成的，在本发明中并不作限制。

卡套向真实卡片管理器发送第二绑定指令，其中，第二绑定指令包括：卡套生成的第三绑定随机因子、卡套证书以及卡套唯一标识；具体地，卡套可以通过无线方式（例如移动网络、WIFI 等）向真实卡片管理器发送第二绑定指令。第二绑定指令中携带第三绑定随机因子可以防止重放攻击，第二绑定指令中携带卡套证书以便真实卡片管理器对卡套进行
25 认证，第二绑定指令中携带卡套唯一标识以便真实卡片管理器获知哪个卡套与其绑定；其中，第三绑定随机因子可以为卡套生成的随机数、随机字符或其组合，当然，在生成第三绑定随机因子后，还可以对第三绑定随机因子的随机性进行验证，以提高第三绑定随机因子的随机性，防止被破解；卡套唯一标识可以为卡套序列号、设备识别码、MAC 地址等任一或其组合以唯一标识卡套的标识。

30 真实卡片管理器接收第二绑定指令，利用根证书对卡套证书进行验证；具体地，真实卡片管理器预先存储根证书，利用该根证书完成对卡套证书的验证，以保证后续使用卡套证书的安全性。

真实卡片管理器验证卡套证书合法后，生成第四绑定随机因子；具体地，第四绑定随机因子可以为真实卡片管理器生成的随机数、随机字符或其组合；当然，在生成第四绑定随机因子后，还可以对第四绑定随机因子的随机性进行验证，以提高第四绑定随机因子的随机性，防止被破解。

5 真实卡片管理器利用卡套证书中的卡套公钥对第三绑定随机因子以及第四绑定随机因子进行加密获得第二绑定密文，利用真实卡片管理器私钥对第三绑定随机因子以及第四绑定随机因子进行签名获得第三绑定签名；具体地，真实卡片管理器利用卡套公钥对第三绑定随机因子以及第四绑定随机因子进行加密以保证第三绑定随机因子以及第四绑定随机因子传输的安全性，真实卡片管理器利用真实卡片管理器私钥对第三绑定随机因子以及第四绑定随机因子进行签名，以保证后续卡套可以对真实卡片管理器身份的合法性进行认证。

10 真实卡片管理器向卡套发送第二绑定响应，其中，第二绑定响应包括：第二绑定密文、第三绑定签名、真实卡片管理器证书以及真实卡片管理器唯一标识；具体地，真实卡片管理器发送的第二绑定响应中携带真实卡片管理器证书以便卡套对真实卡片管理器进行认证，第二绑定响应中携带真实卡片管理器唯一标识以便卡套获知哪个真实卡片管理器与其绑定；其中，真实卡片管理器唯一标识可以为真实卡片管理器序列号、设备识别码、MAC地址等任一或其组合以唯一标识真实卡片管理器的标识。

15 卡套接收第二绑定响应，利用根证书对真实卡片管理器证书进行验证；具体地，卡套预先存储根证书，利用该根证书完成对真实卡片管理器证书的验证，以保证后续使用真实卡片管理器证书的安全性。

20 卡套验证真实卡片管理器证书合法后，利用卡套私钥对第二绑定密文进行解密，获得第三绑定随机解密因子和第四绑定随机解密因子；具体地，利用卡套私钥对第二绑定密文进行解密，如果在数据传输中发生了数据传输错误，或者在数据传输中发生了篡改，则将导致无法成功解密，或者解密出的第三绑定随机解密因子以及第四绑定随机解密因子与第三绑定随机因子以及第四绑定随机因子不同。而通过卡套公钥进行加密，只有卡套私钥可以成功解密，从而也可以保证数据解密的安全性。

25 卡套利用真实卡片管理器证书中的真实卡片管理器公钥、第三绑定随机解密因子以及第四绑定随机解密因子对第三绑定签名进行验证；具体地，卡套利用验证通过后的真实卡片管理器公钥对真实卡片管理器发送的签名进行验证，以确保数据的合法来源。

30 卡套验证第三绑定签名正确后，验证第三绑定随机解密因子与第三绑定随机因子是否相同；具体地，卡套验证自身生成的第三绑定随机因子与第三绑定随机解密因子相同，可以保证数据并未被篡改，且加密的数据来源确实为卡套发送第三绑定随机因子的对象。

卡套验证第三绑定随机解密因子与第三绑定随机因子相同后，提示真实卡片管理器唯

一标识；具体地，卡套可以显示真实卡片管理器唯一标识，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）真实卡片管理器唯一标识，以便用户对真实卡片管理器的真实性进行确认，提高绑定安全性。

卡套接收用于确认真实卡片管理器唯一标识正确的触发命令，利用卡套私钥对第三绑定随机因子以及第四绑定随机解密因子进行签名，获得第四绑定签名，以及存储真实卡片管理器唯一标识、真实卡片管理器证书以及卡套端第二绑定因子至卡套端第二绑定列表，其中，卡套端第二绑定因子为第四绑定随机解密因子；具体地，卡套接收的用于确认真实卡片管理器唯一标识正确的触发命令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制；利用卡套私钥对第三绑定随机因子以及第四绑定随机解密因子进行签名以便后续真实卡片管理器对卡套的身份进行认证；当然，卡套还可以存储卡套端第二绑定列表，该卡套端第二绑定列表用于记录与卡套绑定的真实卡片管理器的相关信息，例如：真实卡片管理器唯一标识、真实卡片管理器证书等，另外，卡套端第二绑定列表还用于存储卡套端第二绑定因子，该卡套端第二绑定因子为密文传输的第四绑定随机因子，基于第四绑定随机因子是密文传输的，因此，该卡套端第二绑定因子是安全且未被篡改的。

卡套向真实卡片管理器发送第四绑定签名；具体地，卡套向真实卡片管理器发送第四绑定签名，以便真实卡片管理器对卡套身份进行认证。

真实卡片管理器接收第四绑定签名，利用卡套证书中的卡套公钥、第三绑定随机因子以及第四绑定随机因子对第四绑定签名进行验证；具体地，真实卡片管理器利用验证通过后的卡套公钥对卡套发送的签名进行验证，以确保数据的合法来源。

真实卡片管理器验证第四绑定签名正确后，存储卡套唯一标识、卡套证书以及真实卡片管理器端绑定因子至真实卡片管理器端绑定列表，其中，真实卡片管理器端绑定因子为第四绑定随机因子。具体地，真实卡片管理器还可以存储真实卡片管理器端绑定列表，该真实卡片管理器端绑定列表用于记录与真实卡片管理器绑定的卡套的相关信息，例如：卡套唯一标识、卡套证书等，另外，真实卡片管理器端绑定列表还用于存储真实卡片管理器端绑定因子，该真实卡片管理器端绑定因子为真实卡片管理器生成的第四绑定随机因子。

由此可见，基于上述卡套和真实卡片管理器进行绑定，可以保证后续卡套和真实卡片管理器之间数据交互的安全性。

另外，上述卡套与真实卡片管理器执行绑定的操作并非必须的步骤，根据不同应用场景的需求，可以选择不执行上述卡套与真实卡片管理器执行绑定的操作。

当然，上述卡套与真实卡片管理器执行绑定的操作，并不局限于上述提供的实现方式，例如还可以采用手动绑定，即在可信环境下，在卡套上输入待绑定的真实卡片管理器的标识作为卡套端第一绑定因子，真实卡片管理器默认真实卡片管理器的标识作为真实卡片管理器端绑定因子；或者在真实卡片管理器上输入待绑定的卡套的标识作为真实卡片管理器端绑定因子，卡套默认卡套的标识作为卡套端第二绑定因子；或者在卡套上输入任意随机值作为卡套端第二绑定因子，在真实卡片管理器上输入相同的随机值作为真实卡片管理器端绑定因子等等，只要可以使得卡套与真实卡片管理器均获得相同的绑定因子均应属于本发明的保护范围。

当然，上述卡套与模拟卡片执行绑定的操作，以及上述卡套与真实卡片执行绑定的操作并非需要同时执行，根据不同应用场景的需求，可以选择仅执行卡套与模拟卡片的绑定操作，或者仅执行卡套与真实卡片管理器的绑定操作，或者上述绑定操作均不予执行。

七、数据交互：

在卡套与模拟卡片建立安全连接之后，模拟卡片向卡套发送的第一数据利用模拟卡片端安全传输密钥进行第一处理后发送，卡套接收到第一处理后的第一数据，利用卡套端安全传输密钥进行第二处理。

在卡套与真实卡片管理器建立安全连接之后，卡套向真实卡片管理器发送的第一数据利用卡套端安全传输密钥进行第一处理后发送，真实卡片管理器接收到第一处理后的第一数据，利用真实卡片管理器端安全传输密钥进行第二处理。

由此保证数据交互的安全性。

以下提供一种在卡套与模拟卡片建立安全连接，且卡套与真实卡片管理器建立安全连接之后，本发明的数据交互方法，但本发明并不局限于此：

模拟卡片接收交易终端发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第一处理后发送至卡套；具体地，在数据交互过程中，将模拟卡片与交易终端（例如ATM机、POS机、公交卡充值机等）进行连接（接触式接口或者非接触式接口），模拟卡片接收交易终端发送的数据，该数据可以为待处理的数据（例如取款金额、扣款金额、真实卡片信息获取请求等）。

卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，接收用于确认第二处理后的数据正确的确认指令后，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；具体地，卡套接收模

拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，还可以显示待处理的数据，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）待处理的数据，以供用户确认该待处理的数据是否正确，只有在正确后，接收用户输入的确认待处理的数据正确的确认指令后，才将该待处理的数据发送至真实卡片管理器；如果用户
5 确认该待处理的数据不正确，则可以直接取消该次数据交互，以此，提高数据交互的安全性。卡套接收的用于确认第二处理后的数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认
10 指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片；具体地，真实卡片管理器将待处理的数据发送至选中的真实卡片，以便选中的真实卡片对待处理的数据进行处理。

15 基于上述数据交互流程，可以通过一张模拟卡片可以实现多种不同种类的真实卡片的功能，用户进行数据交互时，只需携带模拟卡片及卡套，无需携带真实卡片即可以完成，提高便捷性和安全性。

卡套可以将数据交互过程中需要确认的信息进行提示，由此，用户可以对数据交互过程中的需要确认的信息进行确认后再执行交互，从而保证数据交互的真实性，提高安全性。

20 在数据传输过程中，模拟卡片、卡套和真实卡片管理器之间进行数据交互均通过安全传输密钥进行加解密和/或校验操作，从而保证数据传输的安全性和完整性。

此外，由于可以选择使用与交易终端匹配的真实卡片，可以解决现有技术中用户未携带与交易终端匹配的真实卡片而产生的不必要的费用支出（例如银行跨行取款手续费等）。

25 八、充值：

利用本发明的数据交互架构，还可以实现充值（例如公交卡、水卡、电卡充值等）等操作，以方便用户仅携带本发明的卡套和模拟卡片即可以实现多种不同种类真实卡片的充值，方便用户携带，避免了真实卡片丢失造成的资产损失。

以下提供了一种具体充值流程，但本发明并不局限于此：

30 卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，可选的，在本步骤之前，还可以执行卡套开机、卡套登录真实卡片管理器的操作，在此不再赘述，具体可以参见上述

有关卡套开机和卡套登录真实卡片管理器的相关描述。在本步骤中，卡套获取卡套端真实卡片信息列表，还可以包括卡套更新卡套端真实卡片信息列表的步骤，在此也不再赘述，具体可以参见上述卡套更新卡套端真实卡片信息列表的相关描述。卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表后，将其存储在卡套的存储区域中，作为卡套端真实卡片信息列表，在卡套需要提示（例如显示或者语音播放等）卡套端真实卡片信息列表时，可以从本地直接获取该卡套端真实卡片信息列表，提高卡套的处理速度。

卡套提示卡套端真实卡片信息列表；具体地，卡套利用自身的显示装置或者借助外部显示装置显示卡套端真实卡片信息列表，或者卡套利用自身的语音播放装置或者借助外部语音播放装置语音播放（例如喇叭播放或者通过耳机听筒播放等）卡套端真实卡片信息列表，以供用户根据卡套端真实卡片信息列表来选择进行充值时需要使用的真实卡片，方便用户选择，增强用户体验。

卡套接收真实卡片选择指令，确定选中的真实卡片；以及模拟卡片接收充值终端发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第一处理后发送至卡套；具体地，卡套接收的真实卡片选择指令可以为单独设置在卡套上的选择物理按键生成的，或者可以为卡套的触屏上的选择虚拟按键生成的，或者可以为在卡套屏幕上显示的菜单中选中表示选择功能的菜单项生成的。卡套接收真实卡片选择指令，确定选中的真实卡片，卡套经由真实卡片管理器与选中的真实卡片实现数据传输。另外，在充值过程中，将模拟卡片与充值终端（例如充值机等）进行连接（接触式接口或者非接触式接口），模拟卡片接收充值终端发送的数据，该数据可以为待处理的充值数据（例如充值金额等），以便后续用户确认该待处理的充值数据是否正确。此外，在模拟卡片接收充值终端发送的待处理的充值数据之前，模拟卡片还可以接收充值终端发送的获取选中的真实卡片的真实卡片信息请求，卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片，选中的真实卡片接收真实卡片管理器端发送的数据，并将获取的真实卡片信息发送至真实卡片管理器，真实卡片管理器接收选中的真实卡片发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第一处理后发送至卡套，卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片，模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至充值终端，由此，充值终端获取到选中的真实卡片的真实卡片信息，以便后续针对该真实卡片进行充值。

卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据，并接收用于指示第二处理后的数据正确的确认指令后，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；具体地，卡套可以显示待处理的充值数据，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）待处理的充值数据，以供用户确认该待处理的充值数据是否正确，只有在正确后，接收用户输入的指示待处理的充值数据正确的确认指令后，才将该待处理的充值数据发送至真实卡片管理器；如果用户确认该待处理的充值数据不正确，则可以直接取消该笔充值，以此，提高充值的安全性。卡套接收的用于指示第二处理后的数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片；具体地，真实卡片管理器将待处理的充值数据发送至选中的真实卡片，以便选中的真实卡片对待处理的充值数据进行处理（例如执行充值操作）。

基于上述充值流程，可以通过一张模拟卡片可以实现多种不同种类的真实卡片的功能，用户进行充值时，只需携带模拟卡片及卡套，无需携带真实卡片即可以完成充值，提高充值便捷性和安全性。

卡套可以将充值过程中需要确认的信息进行提示，由此，用户可以对充值过程中的需要确认的信息进行确认后再执行充值，从而保证充值的真实性，提高安全性。

在数据传输过程中，模拟卡片、卡套和真实卡片管理器之间进行数据交互均通过安全传输密钥进行加解密和/或校验操作，从而保证数据传输的安全性和完整性。

此外，由于可以选择使用与充值终端匹配的真实卡片，可以解决现有技术中用户未携带与充值终端匹配的真实卡片而产生的不必要的费用支出（例如银行跨行取款手续费等）。

九、交易：

利用本发明的数据交互架构，还可以实现交易（例如 ATM 机取款转账、POS 机刷卡等）等操作，以方便用户仅携带本发明的卡套和模拟卡片即可以实现多种不同种类真实卡片的交易，方便用户携带，避免了真实卡片丢失造成的资产损失。

以下提供了一种具体交易流程，但本发明并不局限于此：

卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，可选的，在本步骤之前，还可以执行卡套开机、卡套登录真实卡片管理器的操作，在此不再赘述，具体可以参见上述有关卡套开机和卡套登录真实卡片管理器的相关描述。在本步骤中，卡套获取卡套端真实卡片信息列表，还可以包括卡套更新卡套端真实卡片信息列表的步骤，在此也不再赘述，具体可以参见上述卡套更新卡套端真实卡片信息列表的相关描述。卡套从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表后，将其存储在卡套的存储区域中，作为卡套端真实卡片信息列表，在卡套需要提示（例如显示或者语音播放等）卡套端真实卡片信息列表时，可以从本地直接获取该卡套端真实卡片信息列表，提高卡套的处理速度。

卡套提示卡套端真实卡片信息列表；具体地，卡套利用自身的显示装置或者借助外部显示装置显示卡套端真实卡片信息列表，或者卡套利用自身的语音播放装置或者借助外部语音播放装置语音播放（例如喇叭播放或者通过耳机听筒播放等）卡套端真实卡片信息列表，以供用户根据卡套端真实卡片信息列表来选择进行交易时需要使用的真实卡片，方便用户选择，增强用户体验。

卡套接收真实卡片选择指令，确定选中的真实卡片；以及模拟卡片接收交易终端发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第一处理后发送至卡套；具体地，卡套接收的真实卡片选择指令可以为单独设置在卡套上的选择物理按键生成的，或者可以为卡套的触屏上的选择虚拟按键生成的，或者可以为在卡套屏幕上显示的菜单中表示选择功能的菜单项生成的。卡套接收真实卡片选择指令，确定选中的真实卡片，卡套经由真实卡片管理器与选中的真实卡片实现数据传输。另外，在交易过程中，将模拟卡片与交易终端（例如 ATM 机、POS 机等）进行连接（接触式接口或者非接触式接口），模拟卡片接收交易终端发送的数据，该数据可以为待处理的交易数据（例如取款金额、扣款金额等），以便后续用户确认该待处理的交易数据是否正确。此外，在模拟卡片接收交易终端发送的待处理的交易数据之前，模拟卡片还可以接收交易终端发送的获取选中的真实卡片的真实卡片信息请求，卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片，选中的真实卡片接收真实卡片管理器端发送的数据，并将获取的真实卡片信息发送至真实卡片管理器，真实卡片管理器接收选中的真实卡片发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第一处理后发送至卡套，卡套接收真实卡片管理器发送的数

据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片，模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至交易终端，由此，交易终端获取到选中的真实卡片的真实卡片信息，以便后续针对该真实卡片进行交易。

卡套接收模拟卡片发送的数据，并利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据，并接收用于指示第二处理后的数据正确的确认指令后，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；具体地，卡套可以显示待处理的交易数据，也可以语音播放（例如喇叭播放或者通过耳机听筒播放等）待处理的交易数据，以供用户确认该待处理的交易数据是否正确，只有在正确后，接收用户输入的指示待处理的交易数据正确的确认指令后，才将该待处理的交易数据发送至真实卡片管理器；如果用户确认该待处理的交易数据不正确，则可以直接取消该笔交易，以此，提高交易的安全性。卡套接收的用于指示第二处理后的数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片；具体地，真实卡片管理器将待处理的交易数据发送至选中的真实卡片，以便选中的真实卡片对待处理的交易数据进行处理。

选中的真实卡片接收真实卡片管理器端发送的数据，并进行交易处理后将交易处理后获得的数据发送至真实卡片管理器；具体地，选中的真实卡片对待处理的交易数据进行交易处理，该交易处理为现有智能卡的交易处理的方案，在此不再赘述。

真实卡片管理器接收选中的真实卡片发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至交易终端。具体地，交易终端接收经过真实卡片交易处理后的数据后，

可以按照现有交易流程完成本次交易，例如取款出钞，转账，刷卡扣款等。

基于上述交易流程，可以通过一张模拟卡片可以实现多种不同种类的真实卡片的功能，用户进行交易时，只需携带模拟卡片及卡套，无需携带真实卡片即可以完成交易，提高交易便捷性和安全性。

- 5 卡套可以将交易过程中需要确认的信息进行提示，由此，用户可以对交易过程中的需要确认的信息进行确认后再执行交易，从而保证交易的真实性，提高安全性。

在数据传输过程中，模拟卡片、卡套和真实卡片管理器之间进行数据交互均通过安全传输密钥进行加解密和/或校验操作，从而保证数据传输的安全性和完整性。

- 10 此外，由于可以选择使用与交易终端匹配的真实卡片，可以解决现有技术中用户未携带与交易终端匹配的真实卡片而产生的不必要的费用支出（例如银行跨行取款手续费等）。

当然，上述具体实现仅公开了从交易终端至真实卡片，真实卡片至交易终端的单次数据交互，在实际应用中，可能存在多次数据交互，交互流程与上述单次数据交互相似，在多次数据交互中，可以根据交互的数据是否需要确认来设置在卡套处是否提示交互的数据来保证交互数据的真实性。

15

十、应用程序更新：

1、卡套应用程序更新：

在本发明中，卡套还可以对自身已经安装过的应用程序进行更新或者安装新应用程序，以便拓展卡套的各类应用或者对卡套的现有应用进行升级：

- 20 本发明提供一种卡套应用程序更新的具体实现方案，但本发明并不局限于此：

图 13 示出了卡套应用程序更新的流程图，应当理解的是，更新过程可以通过数据交互方法或数据交互系统实现。参见图 13，卡套应用程序更新包括：

- 25 卡套至少将卡套证书发送至更新平台；具体地，单独设置安全的更新平台以便完成卡套应用程序的更新。卡套将卡套证书发送至更新平台，以便更新平台知道是哪个卡套需要更新，同时也可以验证卡套的身份；卡套还可以将需要更新的应用程序标识或者其他告知更新平台需要更新或者下载的应用程序的信息发送至更新平台，以便更新平台知晓需要发送哪个应用程序安装包至卡套。

- 30 更新平台生成第一更新加密密钥；具体地，更新平台自身生成用于加密应用程序安装包的更新加密密钥，每次进行应用程序更新时生成的更新加密密钥可以相同也可以不同，不同则可以防止被破解，提高安全性。

更新平台利用第一更新加密密钥对卡套应用程序安装包进行加密获得第一安装包密文；具体地，更新平台利用生成的更新加密密钥加密卡套应用程序安装包，从而保证卡套

应用程序安装包传输的安全性。

更新平台利用更新平台私钥对第一安装包密文进行签名获得第一安装包签名；具体地，更新平台对第一安装包密文进行签名，以便后续卡套对更新平台的身份进行验证。

更新平台利用卡套证书中的卡套公钥加密第一更新加密密钥，获得第一更新加密密钥密文；具体地，更新平台利用卡套公钥加密更新加密密钥，可以保证更新加密密钥传输的安全性，同时，保证只有卡套才可以解密出更新加密密钥，提高应用程序安装包传输的安全性。

更新平台将卡套更新信息发送至卡套，其中，卡套更新信息包括：更新平台证书、第一安装包密文、第一安装包签名以及第一更新加密密钥密文；具体地，更新平台发送的更新信息中携带更新平台证书以便卡套对更新平台进行认证，更新信息中携带第一安装包密文保证应用程序安装包传输的安全性，更新信息中携带第一安装包签名以保证后续卡套可以对更新平台身份的合法性进行认证，更新信息中携带更新加密密钥密文保证更新加密密钥传输的安全性。

卡套接收卡套更新信息，利用根证书验证更新平台证书；具体地，卡套预先存储根证书，利用该根证书完成对更新平台证书的验证，以保证后续使用更新平台证书的安全性。

卡套验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第一安装包签名进行验签；具体地，卡套利用验证通过后的更新平台证书中的更新平台公钥对更新平台发送的签名进行验证，以确保数据的合法来源。

卡套验证第一安装包签名正确后，利用卡套私钥解密第一更新加密密钥密文，获得第一解密密钥；具体地，卡套利用卡套私钥解密出解密密钥，以便后续解密安装包密文获得卡套应用程序安装包。

卡套利用第一解密密钥解密第一安装包密文，获得卡套应用程序安装包；

卡套验证卡套应用程序安装包的数据格式是否正确；具体地，卡套还验证卡套应用程序安装包的数据格式是否正确，如果卡套应用程序安装包的数据格式不正确，则不执行安装操作，如果卡套应用程序安装包的数据格式正确，则执行安装。

如果卡套验证卡套应用程序安装包的数据格式正确，卡套根据卡套应用程序安装包进行安装。具体地，如果卡套是对已安装过的应用程序进行更新，则可以覆盖已安装的应用程序，或者对已安装的应用程序进行升级，或者先行卸载已安装的应用程序后再进行新的应用程序的安装，如果卡套是新安装应用程序，则可以直接安装该应用程序。

基于本发明的卡套对应用程序的更新，既可以更新已安装的应用程序，也可以下载新的应用程序并安装，拓展了卡套的功能，方便用户使用。

2、模拟卡片应用程序更新：

在本发明中，模拟卡片还可以对自身已经安装过的应用程序进行更新或者安装新应用程序，以便拓展模拟卡片的各类应用或者对模拟卡片的现有应用进行升级：

本发明提供一种模拟卡片应用程序更新的具体实现方案，但本发明并不局限于此：

图 14 示出了模拟卡片应用程序更新的流程图，应当理解的是，更新过程可以通过数据交互方法或数据交互系统实现。参见图 14，模拟卡片应用程序更新包括：

卡套从模拟卡片中获取模拟卡片证书，至少将模拟卡片证书发送至更新平台；具体地，卡套可以通过如下方式从模拟卡片中获取模拟卡片证书：卡套通过接触式或者非接触式检测到模拟卡片后，向模拟卡片发送获取模拟卡片证书的请求，模拟卡片接收到卡套发送的请求后，将模拟卡片证书发送至卡套；或者卡套通过接触式或者非接触式检测到模拟卡片后，模拟卡片主动将模拟卡片证书发送至卡套。可选的替代方案：卡套通过接触式或者非接触式检测到模拟卡片后，向模拟卡片发送获取模拟卡片唯一标识的请求，模拟卡片接收到卡套发送的请求后，将模拟卡片唯一标识发送至卡套，卡套接收到模拟卡片唯一标识后还可以根据该模拟卡片唯一标识从本地存储的卡套端第一绑定列表中获取模拟卡片唯一标识对应的模拟卡片证书；或者卡套通过接触式或者非接触式检测到模拟卡片后，模拟卡片主动将模拟卡片唯一标识发送至卡套，卡套接收到模拟卡片唯一标识后还可以根据该模拟卡片唯一标识从本地存储的卡套端第一绑定列表中获取模拟卡片唯一标识对应的模拟卡片证书。另外，单独设置安全的更新平台以便完成模拟卡片应用程序的更新。卡套将模拟卡片证书发送至更新平台，以便更新平台知道是哪个模拟卡片需要更新，同时也可以验证模拟卡片的身份；卡套还可以将需要更新的应用程序标识或者其他告知更新平台需要更新或者下载的应用程序的信息发送至更新平台，以便更新平台知晓需要发送哪个应用程序安装包至模拟卡片。

更新平台生成第二更新加密密钥；具体地，更新平台自身生成用于加密应用程序安装包的更新加密密钥，每次进行应用程序更新时生成的更新加密密钥可以相同也可以不同，不同则可以防止被破解，提高安全性。

更新平台利用第二更新加密密钥对模拟卡片应用程序安装包进行加密获得第二安装包密文；具体地，更新平台利用生成的更新加密密钥加密模拟卡片应用程序安装包，从而保证模拟卡片应用程序安装包传输的安全性。

更新平台利用更新平台私钥对第二安装包密文进行签名获得第二安装包签名；具体地，更新平台对第二安装包密文进行签名，以便后续模拟卡片对更新平台的身份进行验证。

更新平台利用模拟卡片证书中的模拟卡片公钥加密第二更新加密密钥，获得第二更新加密密钥密文；具体地，更新平台利用模拟卡片公钥加密更新加密密钥，可以保证更新加密密钥传输的安全性，同时，保证只有模拟卡片才可以解密出更新加密密钥，提高应用程

序安装包传输的安全性。

更新平台将模拟卡片更新信息发送至卡套，其中，模拟卡片更新信息包括：更新平台证书、第二安装包密文、第二安装包签名以及第二更新加密密钥密文；具体地，更新平台发送的更新信息中携带更新平台证书以便模拟卡片对更新平台进行认证，更新信息中携带第二安装包密文保证应用程序安装包传输的安全性，更新信息中携带第二安装包签名以保证后续模拟卡片可以对更新平台身份的合法性进行认证，更新信息中携带更新加密密钥密文保证更新加密密钥传输的安全性。

卡套接收模拟卡片更新信息，利用卡套端第一安全传输密钥对模拟卡片更新信息进行第一处理后发送至模拟卡片；具体地，卡套利用卡套与模拟卡片之间建立安全连接时生成的安全传输密钥对模拟卡片更新信息进行处理后传输，可以提高数据传输的安全性。

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后，获得模拟卡片更新信息；

模拟卡片利用根证书验证更新平台证书；具体地，模拟卡片预先存储根证书，利用该根证书完成对更新平台证书的验证，以保证后续使用更新平台证书的安全性。

模拟卡片验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第二安装包签名进行验签；具体地，模拟卡片利用验证通过后的更新平台证书中的更新平台公钥对更新平台发送的签名进行验证，以确保数据的合法来源。

模拟卡片验证第二安装包签名正确后，利用模拟卡片私钥解密第二更新加密密钥密文，获得第二解密密钥；具体地，模拟卡片利用模拟卡片私钥解密出解密密钥，以便后续解密安装包密文获得模拟卡片应用程序安装包。

模拟卡片利用第二解密密钥解密第二安装包密文，获得模拟卡片应用程序安装包；

模拟卡片验证模拟卡片应用程序安装包的数据格式是否正确；具体地，模拟卡片还验证模拟卡片应用程序安装包的数据格式是否正确，如果模拟卡片应用程序安装包的数据格式不正确，则不执行安装操作，如果模拟卡片应用程序安装包的数据格式正确，则执行安装。

如果模拟卡片验证模拟卡片应用程序安装包的数据格式正确，模拟卡片根据模拟卡片应用程序安装包进行安装。具体地，如果模拟卡片是对已安装过的应用程序进行更新，则可以覆盖已安装的应用程序，或者对已安装的应用程序进行升级，或者先行卸载已安装的应用程序后再进行新的应用程序的安装，如果模拟卡片是新安装应用程序，则可以直接安装该应用程序。

基于本发明的模拟卡片对应用程序的更新，既可以更新已安装的应用程序，也可以下载新的应用程序并安装，拓展了模拟卡片的功能，方便用户使用。

当然，如果卡套与模拟卡片并未建立安全连接，在模拟卡片进行应用程序更新时，模拟卡片直接将数据发送至卡套，卡套直接将数据发送至模拟卡片。

3、真实卡片管理器应用程序更新：

在本发明中，真实卡片管理器还可以对自身已经安装过的应用程序进行更新或者安装新应用程序，以便拓展真实卡片管理器的各类应用或者对真实卡片管理器的现有应用进行升级：

本发明提供一种真实卡片管理器应用程序更新的具体实现方案，但本发明并不局限于此：

图 15 示出了真实卡片管理器应用程序更新的流程图，应当理解的是，更新过程可以通过数据交互方法或数据交互系统实现。参见图 15，真实卡片管理器应用程序更新包括：

真实卡片管理器至少将真实卡片管理器证书发送至更新平台；具体地，单独设置安全的更新平台以便完成真实卡片管理器应用程序的更新。真实卡片管理器将真实卡片管理器证书发送至更新平台，以便更新平台知道是哪个真实卡片管理器需要更新，同时也可以验证真实卡片管理器的身份；真实卡片管理器还可以将需要更新的应用程序标识或者其他告知更新平台需要更新或者下载的应用程序的信息发送至更新平台，以便更新平台知晓需要发送哪个应用程序安装包至真实卡片管理器。

更新平台生成第三更新加密密钥；具体地，更新平台自身生成用于加密应用程序安装包的更新加密密钥，每次进行应用程序更新时生成的更新加密密钥可以相同也可以不同，不同则可以防止被破解，提高安全性。

更新平台利用第三更新加密密钥对真实卡片管理器应用程序安装包进行加密获得第三安装包密文；具体地，更新平台利用生成的更新加密密钥加密真实卡片管理器应用程序安装包，从而保证真实卡片管理器应用程序安装包传输的安全性。

更新平台利用更新平台私钥对第三安装包密文进行签名获得第三安装包签名；具体地，更新平台对第三安装包密文进行签名，以便后续真实卡片管理器对更新平台的身份进行验证。

更新平台利用真实卡片管理器证书中的真实卡片管理器公钥加密第三更新加密密钥，获得第三更新加密密钥密文；具体地，更新平台利用真实卡片管理器公钥加密更新加密密钥，可以保证更新加密密钥传输的安全性，同时，保证只有真实卡片管理器才可以解密出更新加密密钥，提高应用程序安装包传输的安全性。

更新平台将真实卡片管理器更新信息发送至真实卡片管理器，其中，真实卡片管理器更新信息包括：更新平台证书、第三安装包密文、第三安装包签名以及第三更新加密密钥密文；具体地，更新平台发送的更新信息中携带更新平台证书以便真实卡片管理器对更新

平台进行认证，更新信息中携带第三安装包密文保证应用程序安装包传输的安全性，更新信息中携带第三安装包签名以保证后续真实卡片管理器可以对更新平台身份的合法性进行认证，更新信息中携带更新加密密钥密文保证更新加密密钥传输的安全性。

5 真实卡片管理器接收真实卡片管理器更新信息，利用根证书验证更新平台证书；具体地，真实卡片管理器预先存储根证书，利用该根证书完成对更新平台证书的验证，以保证后续使用更新平台证书的安全性。

真实卡片管理器验证更新平台证书通过后，利用更新平台证书中的更新平台公钥对第三安装包签名进行验签；具体地，真实卡片管理器利用验证通过后的更新平台证书中的更新平台公钥对更新平台发送的签名进行验证，以确保数据的合法来源。

10 真实卡片管理器验证第三安装包签名正确后，利用真实卡片管理器私钥解密第三更新加密密钥密文，获得第三解密密钥；具体地，真实卡片管理器利用真实卡片管理器私钥解密出解密密钥，以便后续解密安装包密文获得真实卡片管理器应用程序安装包。

真实卡片管理器利用第三解密密钥解密第三安装包密文，获得真实卡片管理器应用程序安装包；

15 真实卡片管理器验证真实卡片管理器应用程序安装包的数据格式是否正确；具体地，真实卡片管理器还验证真实卡片管理器应用程序安装包的数据格式是否正确，如果真实卡片管理器应用程序安装包的数据格式不正确，则不执行安装操作，如果真实卡片管理器应用程序安装包的数据格式正确，则执行安装。

如果真实卡片管理器验证真实卡片管理器应用程序安装包的数据格式正确，真实卡片
20 管理器根据真实卡片管理器应用程序安装包进行安装。具体地，如果真实卡片管理器是对已安装过的应用程序进行更新，则可以覆盖已安装的应用程序，或者对已安装的应用程序进行升级，或者先行卸载已安装的应用程序后再进行新的应用程序的安装，如果真实卡片管理器是新安装应用程序，则可以直接安装该应用程序。

25 基于本发明的真实卡片管理器对应用程序的更新，既可以更新已安装的应用程序，也可以下载新的应用程序并安装，拓展了真实卡片管理器的功能，方便用户使用。

十一、数据交互架构适用的应用场景：

1、给账户充值：

30 在本实施例提供的一种应用场景中，用户基于上述数据交互架构，可以实现对第三方账户的充值，例如给支付宝账户充值。

以下对本应用场景的实现进行具体说明，但本发明并不局限于此：

卡套通过网络登录账户平台；具体地，卡套通过无线网络登录账户平台，以便通过本

发明的数据交互架构中的卡套和真实卡片管理器完成对账户的充值。其中，账户平台可以为虚拟的第三方账户平台，例如：电子商务网站账户平台（例如支付宝等）、电费缴费平台、网络金融平台（例如基金等）。

卡套将充值请求发送至账户平台，其中，充值请求包括：充值信息；具体地，卡套将
5 充值请求发送至账户平台，以便账户平台根据充值请求反馈充值包。其中，充值信息包括：充值金额等，可选的，还可以包括待充值账户，以便账户平台知晓为哪个账户进行充值。

卡套接收充值包，其中，充值包由支付平台在接收充值请求后生成；具体地，卡套在
将充值请求发送至账户平台的同时或者再其之后，还将该充值请求发送至支付平台，或者，
账户平台接收到充值请求后，将充值请求发送至支付平台，以支付平台便进行支付。该支
10 付平台接收到充值请求后，还生成充值包，其中，充值包包括：充值金额、待充值账户等
信息，支付平台将充值包发送至卡套，或者支付平台将充值包发送至账户平台，再由账户
平台将充值包发送至卡套，以使用户在卡套上进行确认充值包是否无误。其中，支付平台
为与真实卡片对应的交易平台，例如网银等。

卡套提示充值包，接收用于确认充值包无误的确认指令；具体地，卡套在接收到充值
15 包后，还将充值包进行显示或者语音播放，以使用户对充值包中的信息进行确认，如果用户
确认无误，在卡套上进行确认操作（例如按下确认按键，选择菜单中的确认选项等方式）
生成用于确认充值包无误的确认指令，卡套接收该确认指令，以便卡套继续执行后续操作；
当然，如果用户确认充值包有问题，则可以在卡套上进行取消操作，以便取消该笔充值。
卡套接收的用于确认充值包无误的确认指令可以为单独设置在卡套上的确认物理按键生成
20 的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选
择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示
并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过
后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当
然，还可以为其他任何方式生成的，在本发明中并不作限制。当然，在本步骤的同时或者
25 在本步骤之前，卡套还需要登录真实卡片管理器，并选择为账户进行充值的真实卡片，卡
套登录真实卡片管理器的操作以及选择真实卡片的操作可以参照上述相关描述，在此不再
详述。

卡套利用卡套端第二安全传输密钥对充值包进行第一处理后发送至真实卡片管理器，
其中，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的，真实卡
30 片管理器与至少一个真实卡片相连接，并存储有真实卡片管理器端真实卡片信息列表，真
实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信
息；具体地，卡套接收到充值包，并在充值包确认无误后，将充值包进行第一处理后发送

至真实卡片管理器，提高充值包传输安全性，以便真实卡片管理器将真实的充值包发送至真实卡片进行处理。另外，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息，该真实卡片信息可以包括：卡号、卡片认证信息等信息，该卡片认证信息为认证真实卡片是否为正规渠道（例如银行、公交公司等）发行的卡片信息；该真实卡片可以为银行颁发的银行卡或者功能卡（例如公交卡、饭卡、购物卡、会员卡、积分卡等）。此外，卡套端第二安全传输密钥为的生成方式可以参照上述卡套端第二安全传输密钥的生成的相关描述，在此不再详述。可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，以便用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

真实卡片管理器接收卡套发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的，选中的真实卡片为：卡套提示卡套端真实卡片信息列表，并接收真实卡片选择指令后确定的真实卡片，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，真实卡片管理器接收卡套发送的数据后，对接收到的数据进行第二处理，将真实且完整的数据发送至真实卡片，保证真实卡片处理的数据的真实性和完整性，从而保证充值的安全性。其中，真实卡片管理器端安全传输密钥的生成方式可以参照上述真实卡片管理器端安全传输密钥的生成方式的描述，在此不再详述。选中的真实卡片的选择可参照上述真实卡片的选择的相关描述，在此不再详述。

选中的真实卡片接收真实卡片管理器发送的数据，对接收到的数据进行交易处理，获得充值处理包；具体地，选中的真实卡片接收到真实卡片管理器发送的真实且完整的数据后，对接收到的数据进行交易处理，以便确认可以完成交易，选中的真实卡片进行交易处理的过程可以参照现有的智能卡进行交易处理的流程，在此不再详述。

选中的真实卡片将充值处理包发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对充值处理包进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理后发送至支付平台；具体地，卡套接收到经过选中的真实卡片处理后的数据并将其发送至支付平台，以便支付平台进行支付。

账户平台接收支付平台发送的支付成功信息，执行充值操作，其中，支付成功信息为支付平台接收卡套发送的第二处理后的数据并执行交易处理操作后生成的。具体地，支付

平台在完成支付后，生成支付成功信息，并将该支付成功信息发送至账户平台，以便账户平台知晓支付完成，从而完成充值操作。当然，该支付成功信息中还可以包含验证信息，以便账户平台对支付成功信息进行验证，只有在验证通过后，才完成充值，提高安全性。

基于上述方式，本发明的数据交互架构可以完成对账户平台的充值，扩展了本发明数据交互架构的应用，方便用户使用。

2、给真实卡片充值：

在本实施例提供的一种应用场景中，用户基于上述数据交互架构，可以实现对真实卡片的充值，例如给公交卡充值。

以下对本应用场景的实现进行简要说明，但本发明并不局限于此：

10 卡套从与真实卡片管理器连接的真实卡片中，确定选中的真实卡片；

充值平台通过模拟卡片、卡套以及真实卡片管理器获取选中的真实卡片的卡片信息，其中，卡片信息包括：选中的真实卡片的卡号、卡片认证信息；

充值平台确定付款成功后，生成充值包并通过模拟卡片、卡套以及真实卡片管理器发送至选中的真实卡片，其中，充值包经过卡套进行提示和确认；

15 选中的真实卡片接收真实卡片管理器发送的数据，执行充值操作。

基于上述简要说明，以下提供一种具体实现方式，但本发明并不局限于此：

卡套登录真实卡片管理器，其中，真实卡片管理器与至少一个真实卡片相连接，并存储有真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；具体地，上述卡套登录步骤可以参照上述
20 卡套登录的相关描述，在此不再详述。可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，形成真实卡片管理器端真实卡片信息列表，以便用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，卡套如何获取真实卡片信息列表可以参照上述卡套获取真实卡片信息列表的相关描述，在此不再详述。

卡套提示卡套端真实卡片信息列表；

卡套接收真实卡片选择指令，确定选中的真实卡片；具体地，卡套确定选中的真实卡片为待充值卡片，例如公交卡等，此时，本数据交互架构中的模拟卡片可以作为待充值卡片（例如公交卡）使用。
30

模拟卡片接收充值平台发送的卡片信息获取请求，卡片信息获取请求至少包括选中的真实卡片的卡号、卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片

与充值平台进行连接，该充值平台可以包括前端充值机和后台充值处理平台，例如：公交卡充值平台等，模拟卡片接收充值平台发送的卡片信息获取请求，以便获取选中的真实卡片的真实卡片信息。

模拟卡片利用模拟卡片端安全传输密钥对卡片信息获取请求进行第一处理后发送至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到卡片信息获取请求后，利用与卡套之间的安全传输密钥对卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供数据传输安全性，且以便真实卡片管理器获得卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的真实卡片，以便选中的真实卡片获取卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的真实卡片将选中的真实卡片的卡片信息发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至充值平台；具体地，模拟卡片将获取到的卡片信息发送至充值平台，从而保证充值平台获知为哪个真实卡片进行充值。

充值平台确定付款成功后，生成充值包并将充值包发送至模拟卡片；具体地，充值平

台可以通过如下方式确定付款成功：收取现金，收取支票，POS 刷卡完成，转账等任意方式。充值平台确定付款成功后，生成充值包，以便选中的真实卡片根据充值包进行充值操作。其中充值包至少包括：充值金额。

5 模拟卡片接收充值平台发送的充值包，利用模拟卡片端安全传输密钥对充值包进行第一处理后发送至卡套；

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据；

卡套接收用于指示第二处理后的数据无误的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；

10 真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片；

选中的真实卡片接收真实卡片管理器发送的第二处理后的数据，执行充值操作。具体地，选中的真实卡片获取到充值包后，根据充值包执行充值操作，从而完成充值。

15 基于上述简要说明，本发明还提供一种通过刷卡充值的具体实现方式，但本发明并不局限于此；

卡套登录真实卡片管理器，其中，真实卡片管理器与至少一个真实卡片相连接，并存储有真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；具体地，上述卡套登录步骤可以参照上述卡套登录的相关描述，在此不再详述。可选的，真实卡片管理器可以设置为保存与其连接
20 的真实卡片中的全部或部分真实卡片的真实卡片信息，形成真实卡片管理器端真实卡片信息列表，以使用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，卡套如何获取真实卡片信息
25 列表可以参照上述卡套获取真实卡片信息列表的相关描述，在此不再详述。

卡套提示卡套端真实卡片信息列表；

卡套接收第一真实卡片选择指令，确定选中的第一真实卡片；具体地，卡套确定选中的第一真实卡片为扣款卡片，例如银行卡等，此时，本数据交互架构中的模拟卡片可以作为扣款卡片（例如银行卡）使用。

30 模拟卡片接收支付平台发送的第一卡片信息获取请求，第一卡片信息获取请求至少包括选中的第一真实卡片的卡号以及卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片与支付平台进行连接，该支付平台包含扣款终端（例如 POS 机等）以及支

付处理平台（例如银行后台），将模拟卡片与该扣款终端相连，以便进行扣款，模拟卡片接收支付平台发送的第一卡片信息获取请求，以便获取选中的第一真实卡片的真实卡片信息。

模拟卡片利用模拟卡片端安全传输密钥对第一卡片信息获取请求进行第一处理后发送至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到第一卡片信息获取请求后，利用与卡套之间的安全传输密钥对第一卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供数据传输安全性，且以便真实卡片管理器获得第一卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第一真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的第一真实卡片，以便选中的第一真实卡片获取第一卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的第一真实卡片将选中的第一真实卡片的卡片信息发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的第一真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至支付平台；具体地，模拟卡片将获取到的第一真实卡片的卡片信息发送至支付平台，从而保证支付平台获知使用哪个真实卡片进行扣款。

模拟卡片接收支付平台发送的扣款请求，利用模拟卡片端安全传输密钥对扣款请求进

行第一处理后发送至卡套；具体地，扣款请求可以至少包括扣款金额。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理，并将第二处理后的数据进行提示；具体地，卡套可以对扣款请求进行显示或者语音播放，以使用户对扣款请求中的信息进行确认。

- 5 卡套接收用于指示第二处理后的数据正确的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；具体地，如果用户确认无误，在卡套上进行确认操作（例如按下确认按键，选择菜单中的确认选项等方式）生成用于确认扣款请求无误的确认指令，卡套接收该确认指令，以便卡套继续执行后续操作；当然，如果用户确认扣款请求有问题，则可以在卡套上进行取消操作，以便取消该笔交易。卡套
- 10 接收的用于指示第二处理后的数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。
- 15

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第一真实卡片；

- 选中的第一真实卡片接收真实卡片管理器发送的数据，并对接收到的数据进行交易处理后将交易处理后获得的数据发送至真实卡片管理器；具体地，选中的第一真实卡片接收到真实卡片管理器发送的真实且完整的数据后，对接收到的数据进行交易处理，以便确认
- 20 可以完成交易，选中的第一真实卡片进行交易处理的过程可以参照现有的智能卡进行交易处理的流程，在此不再详述。

真实卡片管理器接收选中的第一真实卡片发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第一处理后发送至卡套；

- 25 卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

- 模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至支付平台进行扣款操作；具体地，支付平台接收到模拟卡片发送的选中的
- 30 的第一真实卡片交易处理后的数据，并验证通过后执行扣款操作，当然，在支付平台执行完扣款操作后，还可以生成支付成功信息，以便告知用户支付成功。

卡套提示卡套端真实卡片信息列表；具体地，在充值平台确定付款成功后，用户可选

择待充值卡片（例如银行卡），以便为待充值卡片进行充值。

卡套接收第二真实卡片选择指令，确定选中的第二真实卡片；具体地，卡套确定选中的第二真实卡片为待充值卡片，例如公交卡等，此时，本数据交互架构中的模拟卡片可以作为待充值卡片（例如公交卡）使用。

5 模拟卡片接收充值平台发送的第二卡片信息获取请求，第二卡片信息获取请求至少包括选中的第二真实卡片的卡号、卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片与充值平台进行连接，该充值平台可以包括前端充值机和后台充值处理平台，例如：公交卡充值平台等，模拟卡片接收充值平台发送的第二卡片信息获取请求，以便获取选中的第二真实卡片的真实卡片信息。

10 模拟卡片利用模拟卡片端安全传输密钥对第二卡片信息获取请求进行第一处理后发送至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到第二卡片信息获取请求后，利用与卡套之间的安全传输密钥对卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

15 卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供
20 数据传输安全性，且以便真实卡片管理器获得卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第二真实卡片，其中，真实卡片管理器端安全传输密
25 钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的真实卡片，以便选中的第二真实卡片获取卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的第二真实卡片将选中的真实卡片的卡片信息发送至真实卡片管理器；

30 真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的第二真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据

进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至充值平台；具体地，模拟卡片将获取到的第二真实卡片的卡片信息发送至
5 充值平台，从而保证充值平台获知为哪个真实卡片进行充值。

模拟卡片接收充值平台生成的充值包；具体地，充值平台确定付款成功并获取到选中的第二真实卡片的卡片信息后，生成充值包，以便选中的第二真实卡片可以根据充值包进行充值操作。其中充值包至少包括：充值金额。

模拟卡片利用模拟卡片端安全传输密钥对充值包进行第一处理后发送至卡套；

10 卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据；

卡套接收用于指示第二处理后的数据无误的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的
15 的数据进行第二处理后发送至选中的第二真实卡片；

选中的第二真实卡片接收真实卡片管理器发送的第二处理后的数据，执行充值操作。具体地，选中的第二真实卡片获取到充值包后，根据充值包执行充值操作，从而完成充值。

基于上述方式，本发明的数据交互架构可以完成对真实卡片的充值，扩展了本发明数据交互架构的应用，方便用户使用。

20 3、第二真实卡片为第一真实卡片充值：

在本实施例提供的一种应用场景中，用户基于上述数据交互架构，可以实现真实卡片对真实卡片的充值，例如通过银行卡刷卡给公交卡充值或者通过银行卡刷卡给电卡充值。在本应用场景中，第二真实卡片与第一真实卡片类型不同，第二真实卡片为可以扣款的真实卡片，第一真实卡片为待充值的真实卡片。

25 以下对本应用场景的实现进行简要说明，但本发明并不局限于此：

卡套从与真实卡片管理器连接的真实卡片中，确定选中的第一真实卡片；

充值平台通过模拟卡片、卡套以及真实卡片管理器获取选中的第一真实卡片的卡片信息，其中，卡片信息包括：选中的第一真实卡片的卡号、卡片认证信息；

卡套从与真实卡片管理器连接的真实卡片中，确定选中的第二真实卡片；

30 支付平台通过卡套、真实卡片管理器与选中的第二真实卡片进行扣款处理；

卡套从与真实卡片管理器连接的真实卡片中，确定选中的第一真实卡片；

充值平台生成充值包并通过模拟卡片、卡套以及真实卡片管理器发送至选中的真实卡

片，其中，充值包经过卡套进行提示和确认；

选中的真实卡片接收真实卡片管理器发送的数据，执行充值操作。

基于上述简要说明，以下提供一种具体实现方式，但本发明并不局限于此：

卡套登录真实卡片管理器，其中，真实卡片管理器与至少一个真实卡片相连接，并存储有真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；具体地，上述卡套登录步骤可以参照上述卡套登录的相关描述，在此不再详述。可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，形成真实卡片管理器端真实卡片信息列表，以使用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，卡套如何获取真实卡片信息列表可以参照上述卡套获取真实卡片信息列表的相关描述，在此不再详述。

卡套提示卡套端真实卡片信息列表；

卡套接收第一真实卡片选择指令，确定选中的第一真实卡片；具体地，卡套确定选中的第一真实卡片为待充值卡片，例如公交卡等，此时，本数据交互架构中的模拟卡片可以作为待充值卡片（例如公交卡）使用。

模拟卡片接收充值平台发送的第一卡片信息获取请求，第一卡片信息获取请求至少包括选中的第一真实卡片的卡号以及卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片与充值平台进行连接，该充值平台可以包括前端充值机和后台充值处理平台，例如：公交卡充值平台或者电卡充值平台等，将模拟卡片与该前端充值机相连，模拟卡片接收充值平台发送的第一卡片信息获取请求，以便获取选中的第一真实卡片的真实卡片信息。

模拟卡片利用模拟卡片端安全传输密钥对第一卡片信息获取请求进行第一处理后发送至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到第一卡片信息获取请求后，利用与卡套之间的安全传输密钥对第一卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，

卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供数据传输安全性，且以便真实卡片管理器获得第一卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第一真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的第一真实卡片，以便选中的第一真实卡片获取第一卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的第一真实卡片将选中的第一真实卡片的卡片信息发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的第一真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至充值平台；具体地，模拟卡片将获取到的第一真实卡片的卡片信息发送至充值平台，从而保证充值平台获知为哪个真实卡片进行充值。

卡套接收充值平台发送的充值标识，显示卡套端真实卡片信息列表；具体地，卡套接收充值平台发送的充值标识，以表明为哪张卡充值，同时提示用户选择为第一真实卡片（待充值卡）充值的第二真实卡片（扣款卡）。该充值标识可以包含待充值的第一真实卡片卡号、订单号、充值金额等一种或其组合。

卡套接收第二真实卡片选择指令，确定选中的第二真实卡片；具体地，卡套确定选中的第二真实卡片为扣款卡片，例如银行卡等。

模拟卡片接收支付平台发送的第二卡片信息获取请求，第二卡片信息获取请求至少包括选中的第二真实卡片的卡号以及卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片与支付平台进行连接，该支付平台包含扣款终端（例如 POS 机等）以及支付处理平台（例如银行后台），将模拟卡片与该扣款终端相连，以便进行扣款，模拟卡片接收支付平台发送的第二卡片信息获取请求，以便获取选中的第二真实卡片的真实卡片信息。

模拟卡片利用模拟卡片端安全传输密钥对第二卡片信息获取请求进行第一处理后发送

至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到第二卡片信息获取请求后，利用与卡套之间的安全传输密钥对第二卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供数据传输安全性，且以便真实卡片管理器获得第二卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第二真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的第二真实卡片，以便选中的第二真实卡片获取第二卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的第二真实卡片将选中的第二真实卡片的卡片信息发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的第二真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至支付平台；具体地，模拟卡片将获取到的第二真实卡片的卡片信息发送至支付平台，从而保证支付平台获知使用哪个真实卡片进行扣款。

模拟卡片接收支付平台发送的扣款请求，利用模拟卡片端安全传输密钥对扣款请求进行第一处理后发送至卡套；具体地，扣款请求可以至少包括扣款金额以及第一真实卡片卡号。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第

二处理，并将第二处理后的数据进行提示；具体地，卡套可以对扣款请求进行显示或者语音播放，以使用户对扣款请求中的信息进行确认。

卡套接收用于指示第二处理后的数据正确的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；具体地，如果用户确认无误，
5 在卡套上进行确认操作（例如按下确认按键，选择菜单中的确认选项等方式）生成用于确认扣款请求无误的确认指令，卡套接收该确认指令，以便卡套继续执行后续操作；当然，如果用户确认扣款请求有问题，则可以在卡套上进行取消操作，以便取消该笔交易。卡套接收的用于指示第二处理后的数据正确的确认指令可以为单独设置在卡套上的确认物理按键生成的，或者可以为卡套的触屏上的确认虚拟按键生成的，或者在卡套屏幕上显示的菜单
10 中选择确认功能生成的，或者可以为卡套的语音采集装置（例如麦克）接收到的语音确认指示并验证通过后时生成的，或者可以为卡套的指纹采集装置接收到指纹确认指示并验证通过后生成的，或者可以为卡套的虹膜采集装置接收到虹膜确认指示并验证通过后生成的，当然，还可以为其他任何方式生成的，在本发明中并不作限制。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第二真实卡片；
15

选中的第二真实卡片接收真实卡片管理器发送的数据，并对接收到的数据进行交易处理后将交易处理后获得的数据发送至真实卡片管理器；具体地，选中的第二真实卡片接收到真实卡片管理器发送的真实且完整的数据后，对接收到的数据进行交易处理，以便确认可以完成交易，选中的第二真实卡片进行交易处理的过程可以参照现有的智能卡进行交易处理的流程，在此不再详述。
20

真实卡片管理器接收选中的第二真实卡片发送的数据，并利用真实卡片管理器端安全传输密钥对接收到的数据进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，并利用卡套端第二安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后
25 发送至模拟卡片；

模拟卡片接收卡套发送的数据，并利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至支付平台；

模拟卡片利用模拟卡片端安全传输密钥对支付成功信息进行第一处理后发送至卡套，其中，支付成功信息为支付平台成功执行支付后生成的；具体地，支付平台在接收到选中的第二真实卡片交易处理后的数据，验证通过后，执行扣款操作，在执行完扣款操作后，
30 生成支付成功信息，该支付成功信息可以包括选中的第一真实卡片卡号或者其他表示为哪张卡充值的信息，只要充值平台后续知道为哪张卡充值的扣款成功执行即可。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理，提示卡套端真实卡片信息列表；

卡套接收第一真实卡片选择指令，确定选中的第一真实卡片；具体地，用户再次选中第一真实卡片，以便完成对第一真实卡片的充值操作。

- 5 模拟卡片接收充值平台发送的充值包，其中，充值包由充值平台接收到支付成功信息后生成；具体地，支付平台还可以直接将支付成功信息发送至充值平台，或者卡套将支付成功信息发送至充值平台，以便充值平台知晓支付成功，并生成充值包，以便将该充值包发送至选中的第一真实卡片完成充值。

模拟卡片利用模拟卡片端安全传输密钥对充值包进行第一处理后发送至卡套；

- 10 卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据；

卡套接收用于指示第二处理后的数据无误的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；

- 15 真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的第一真实卡片；

第一真实卡片接收真实卡片管理器发送的数据，执行充值操作。具体地，选中的第一真实卡片获取到充值包后，根据充值包执行充值操作，从而完成充值。

基于上述方式，本发明的数据交互架构可以完成利用第二真实卡片对第一真实卡片的充值，扩展了本发明数据交互架构的应用，方便用户使用。

- 20 4、账户给真实卡片充值：

在本实施例提供的一种应用场景中，用户基于上述数据交互架构，可以实现账户对真实卡片的充值，例如通过支付宝或者网银给公交卡充值。

以下对本应用场景的实现进行简要说明，但本发明并不局限于此：

卡套从与真实卡片管理器连接的真实卡片中，确定选中的真实卡片；

- 25 充值平台通过模拟卡片、卡套以及真实卡片管理器获取选中的真实卡片的卡片信息，其中，卡片信息包括：选中的真实卡片的卡号、卡片认证信息；

卡套登录支付平台，支付平台获取充值标识后进行扣款处理；

充值平台接收支付平台生成的支付成功信息后，生成充值包并通过模拟卡片、卡套以及真实卡片管理器发送至选中的真实卡片，其中，充值包经过卡套进行提示和确认；

- 30 选中的真实卡片接收真实卡片管理器发送的数据，执行充值操作。

基于上述简要说明，以下提供一种具体实现方式，但本发明并不局限于此：

卡套登录真实卡片管理器，其中，真实卡片管理器与至少一个真实卡片相连接，并存

储有真实卡片管理器端真实卡片信息列表，真实卡片管理器端真实卡片信息列表包括与真实卡片管理器连接的真实卡片的真实卡片信息；具体地，上述卡套登录步骤可以参照上述卡套登录的相关描述，在此不再详述。可选的，真实卡片管理器可以设置为保存与其连接的真实卡片中的全部或部分真实卡片的真实卡片信息，形成真实卡片管理器端真实卡片信息列表，以便用户根据对真实卡片的安全性要求做出不同设置，例如可以在真实卡片管理器上设置不允许获取某些真实卡片的真实卡片信息，从而保证这些真实卡片的安全性。

卡套获取卡套端真实卡片信息列表，其中，卡套端真实卡片信息列表为从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表；具体地，卡套如何获取真实卡片信息列表可以参照上述卡套获取真实卡片信息列表的相关描述，在此不再详述。

卡套提示卡套端真实卡片信息列表；

卡套接收真实卡片选择指令，确定选中的真实卡片；具体地，卡套确定选中的真实卡片为待充值卡片，例如公交卡等，此时，本数据交互架构中的模拟卡片可以作为待充值卡片（例如公交卡）使用。

模拟卡片接收充值平台发送的卡片信息获取请求，卡片信息获取请求至少包括选中的真实卡片的卡号、卡片认证信息；具体地，用户通过接触式或者非接触式方式将模拟卡片与充值平台进行连接，该充值平台可以包括前端充值机和后台充值处理平台，例如：公交卡充值平台等，模拟卡片接收充值平台发送的卡片信息获取请求，以便获取选中的真实卡片的真实卡片信息。

模拟卡片利用模拟卡片端安全传输密钥对卡片信息获取请求进行第一处理后发送至卡套，其中，模拟卡片端安全传输密钥为卡套与模拟卡片建立安全连接时生成的；具体地，模拟卡片接收到卡片信息获取请求后，利用与卡套之间的安全传输密钥对卡片信息获取请求进行第一处理后发送至卡套，提高数据传输安全性。模拟卡片端安全传输密钥的生成过程可以参照上述模拟卡片端安全传输密钥的生成过程的相关描述，在此不再详述。

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，再利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器，其中，卡套端第一安全传输密钥为卡套与模拟卡片建立安全连接时生成的，卡套端第二安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，卡套对模拟卡片发送来的数据进行第二处理，并进行第一处理后发送至真实卡片管理器，提供数据传输安全性，且以便真实卡片管理器获得卡片信息获取请求。卡套端第一安全传输密钥和卡套端第二安全传输密钥可以参照上述卡套端第一安全传输密钥和卡套端第二安全传输密钥生成过程的相关描述，在此不再详述。

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到

的数据进行第二处理后发送至选中的真实卡片，其中，真实卡片管理器端安全传输密钥为卡套与真实卡片管理器建立安全连接时生成的；具体地，真实卡片管理器对卡套发送的数据进行第二处理后发送至选中的真实卡片，以便选中的真实卡片获取卡片信息获取请求，从而将卡片信息回传。真实卡片管理器端安全传输密钥的生成过程可以参照上述真实卡片管理器端安全传输密钥的生成过程的相关描述，在此不再详述。

选中的真实卡片将选中的真实卡片的卡片信息发送至真实卡片管理器；

真实卡片管理器利用真实卡片管理器端安全传输密钥对接收到的选中的真实卡片的卡片信息进行第一处理后发送至卡套；

卡套接收真实卡片管理器发送的数据，利用卡套端第二安全传输密钥对接收到的数据进行第二处理，再利用卡套端第一安全传输密钥对第二处理后的数据进行第一处理后发送至模拟卡片；

模拟卡片接收卡套发送的数据，利用模拟卡片端安全传输密钥对接收到的数据进行第二处理后发送至充值平台；具体地，模拟卡片将获取到的卡片信息发送至充值平台，从而保证充值平台获知为哪个真实卡片进行充值。

卡套登录支付平台；具体地，卡套可以登录支付平台，该支付平台可以为支付宝，或者网银，以便完成扣款操作，例如用户登录支付宝直接从支付宝扣款，或者用户登录网银直接从网银扣款，或者用户登录支付宝并通过与支付宝绑定的网银扣款。

卡套接收支付平台发送的支付成功信息，其中，支付成功信息由支付平台在执行支付操作后生成；具体地，支付平台在完成支付后会生成支付成功信息，并将该支付成功信息发送给卡套，以便用户知晓支付成功。支付平台在执行支付操作之前，还获取充值标识，该充值标识可以通过如下方式获取：方式一、模拟卡片接收充值平台发送的充值标识，利用模拟卡片端安全传输密钥对充值标识进行第一处理后发送至卡套，卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理得到充值标识，并由卡套发送至支付平台。其中，充值标识为充值平台在接收模拟卡片第二处理后的数据后生成的，具体地，充值平台获取到模拟卡片发送的第一真实卡片的卡片信息后，可以生成充值标识，以指示为哪个真实卡片进行充值以及充值金额，该充值标识可以为本次充值生成的订单号等。方式二、充值平台在接收模拟卡片第二处理后的数据后生成充值标识，直接将该充值标识发送至支付平台。另外，支付平台根据充值标识进行支付，以便知晓为哪张真实卡片进行支付以及支付金额。

模拟卡片接收充值平台发送的充值包，其中，充值包由充值平台接收到支付平台生成的支付成功信息后生成；具体地，支付平台还将支付成功信息发送至充值平台，或者支付平台将支付成功信息发送至卡套，并由卡套发送至充值平台，以便充值平台知晓支付成功，

并生成充值包，以便将该充值包发送至选中的真实卡片完成充值。

模拟卡片利用模拟卡片端安全传输密钥对充值包进行第一处理后发送至卡套；

卡套接收模拟卡片发送的数据，利用卡套端第一安全传输密钥对接收到的数据进行第二处理后，提示第二处理后的数据；

- 5 卡套接收用于指示第二处理后的数据无误的确认指令，利用卡套端第二安全传输密钥对第二处理后的数据进行第一处理后发送至真实卡片管理器；

真实卡片管理器接收卡套发送的数据，利用真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后发送至选中的真实卡片；

- 10 真实卡片接收真实卡片管理器发送的数据，执行充值操作。具体地，选中的真实卡片获取到充值包后，根据充值包执行充值操作，从而完成充值。

基于上述方式，本发明的数据交互架构可以完成利用账户对真实卡片的充值，扩展了本发明数据交互架构的应用，方便用户使用。

- 15 在本发明的所有实施例中，卡套与模拟卡片之间所有的正常数据交互过程，模拟卡片均位于卡套的有效通信范围内，如果卡套检测出模拟卡片超出了卡套的有效通信范围，则卡套可以进行提示，或者卡套将提示信息发送至用户终端（例如智能手机、平板电脑等）处进行提示，以便提示用户模拟卡片的位置出现异常，由此提高模拟卡片使用安全性。

- 20 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，并且本发明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，这应被本发明的实施例所属技术领域的技术人员所理解。

- 25 应当理解，本发明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。

- 30 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。

此外，在本发明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时，也可以存储在一个计算机可读取存储介质中。

5 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发明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。

10

尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在不脱离本发明的原理和宗旨的情况下在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。本发明的范围由所附权利要求及其等同限定。

15

权利要求书

1、一种数据交互方法，其特征在于，包括：

卡套获取卡套端真实卡片信息列表，其中，所述卡套端真实卡片信息列表为所述卡套
5 从真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表，所述真实卡片管理器端
真实卡片信息列表包括与所述真实卡片管理器连接的真实卡片的真实卡片信息；

所述卡套提示所述卡套端真实卡片信息列表；

所述卡套接收真实卡片选择指令，确定选中的真实卡片；以及所述模拟卡片接收交易
终端发送的第一数据，并将所述第一数据发送至所述卡套；

10 所述卡套提示所述第一数据，接收用于确认所述第一数据正确的确认指令，将所述第
一数据发送至所述真实卡片管理器；

所述真实卡片管理器接收所述卡套发送的所述第一数据，并发送至所述选中的真实卡
片。

2、根据权利要求1所述的方法，其特征在于，还包括：

15 所述卡套与所述模拟卡片建立安全连接，获得所述卡套与所述模拟卡片之间进行数据
安全传输的卡套端第一安全传输密钥和模拟卡片端安全传输密钥。

3、根据权利要求1或2所述的方法，其特征在于，还包括：

所述卡套与所述真实卡片管理器建立安全连接，获得所述卡套与所述真实卡片管理器
之间进行数据安全传输的卡套端第二安全传输密钥和真实卡片管理器端安全传输密钥。

20 4、根据权利要求2所述的方法，其特征在于，在所述卡套与所述模拟卡片建立安全连
接之前，还包括：

所述卡套与所述模拟卡片执行绑定操作。

5、根据权利要求3所述的方法，其特征在于，在所述卡套与所述真实卡片管理器建立
安全连接之前，还包括：

25 所述卡套与所述真实卡片管理器执行绑定操作。

6、根据权利要求3所述的方法，其特征在于，

在所述卡套与所述真实卡片管理器建立安全连接之前，还包括：

所述卡套向所述真实卡片管理器发送登录请求；

在所述卡套与所述真实卡片管理器建立安全连接之后，还包括：

30 所述卡套通过所述卡套端第二安全传输密钥对接收到的登录密码进行第一处理后发送
至所述真实卡片管理器；

所述真实卡片管理器接收所述卡套发送的数据，利用所述真实卡片管理器端安全传输

密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性；

所述真实卡片管理器在验证所述第二处理后的数据通过后，所述卡套登录所述真实卡片管理器。

- 5 7、根据权利要求6所述的方法，其特征在于，所述真实卡片管理器利用所述真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后验证第二处理后的数据的正确性包括：

所述真实卡片管理器利用所述真实卡片管理器端安全传输密钥对接收到的数据进行第二处理后，获得待验证密码；

所述真实卡片管理器判断所述待验证密码是否为报警密码；

- 10 如果所述待验证密码为报警密码，则所述真实卡片管理器确定所述待验证密码验证通过，并执行报警操作；

如果所述待验证密码不是报警密码且为登录密码，则所述真实卡片管理器确定所述待验证密码验证通过。

8、根据权利要求6所述的方法，其特征在于，还包括：

- 15 所述真实卡片管理器对与所述真实卡片管理器连接的真实卡片进行检测；

所述真实卡片管理器在检测到与所述真实卡片管理器连接的真实卡片后，获取所述真实卡片的真实卡片信息，其中，所述真实卡片信息至少包括：卡号；

所述真实卡片管理器获取所述真实卡片的真实卡片信息后，生成真实卡片管理器端真实卡片信息列表。

- 20 9、根据权利要求8所述的方法，其特征在于，还包括：

所述真实卡片管理器还生成真实卡片管理器端标识列表，所述真实卡片管理器端标识列表中的标识与所述真实卡片管理器端真实卡片信息列表中的真实卡片信息一一对应。

10、根据权利要求1所述的方法，其特征在于，所述卡套接收真实卡片选择指令，确定选中的真实卡片；包括：

- 25 所述卡套接收真实卡片选择指令，获取选中标识，其中，所述选中标识用于指示所述选中的真实卡片；

所述卡套将所述选中标识发送至所述真实卡片管理器；

所述真实卡片管理器根据所述选中标识从与所述真实卡片管理器连接的所述真实卡片中，确定与所述选中标识对应的所述选中的真实卡片。

- 30 11、根据权利要求2所述的方法，其特征在于，

在所述卡套与所述模拟卡片建立安全连接之后，所述模拟卡片向所述卡套发送的所述第一数据利用所述模拟卡片端安全传输密钥进行第一处理后发送，所述卡套接收到所述第

一处理后的所述第一数据，利用所述卡套端安全传输密钥进行第二处理；所述卡套向所述模拟卡片发送的所述第二数据利用所述卡套端安全传输密钥进行第一处理后发送，所述模拟卡片接收到所述第一处理后的所述第二数据，利用所述模拟卡片端安全传输密钥进行第二处理。

5 12、根据权利要求3所述的方法，其特征在于，

在所述卡套与所述真实卡片管理器建立安全连接之后，所述卡套向所述真实卡片管理器发送的所述第一数据利用所述卡套端安全传输密钥进行第一处理后发送，所述真实卡片管理器接收到所述第一处理后的所述第一数据，利用所述真实卡片管理器端安全传输密钥进行第二处理；所述真实卡片管理器向所述卡套发送的所述第二数据利用所述真实卡片管
10 理器端安全传输密钥进行第一处理后发送，所述卡套接收到所述第一处理后的所述第二数据，利用所述卡套端安全传输密钥进行第二处理。

13、根据权利要求1至12任一项所述的方法，其特征在于，所述真实卡片管理器根据真实卡片的安全性等级，对与所述真实卡片管理器连接的真实卡片的真实卡片信息的读写权限进行开启和/或关闭的设置。

15 14、根据权利要求1至13任一项所述的方法，其特征在于，所述卡套为移动设备。

15、根据权利要求1至13任一项所述的方法，其特征在于，所述卡套为移动设备和电子签名设备，或者所述卡套为电子签名设备。

16、一种数据交互系统，其特征在于，包括：模拟卡片、卡套以及真实卡片管理器；

所述卡套，用于获取卡套端真实卡片信息列表；提示所述卡套端真实卡片信息列表；
20 接收真实卡片选择指令，确定选中的真实卡片，其中，所述卡套端真实卡片信息列表为所述卡套从所述真实卡片管理器中获取的真实卡片管理器端真实卡片信息列表，所述真实卡片管理器端真实卡片信息列表包括与所述真实卡片管理器连接的真实卡片的真实卡片信息；

所述模拟卡片，用于接收交易终端发送的第一数据，并将所述第一数据发送至所述卡
25 套；

所述卡套，还用于提示所述第一数据，接收用于确认所述第一数据正确的确认指令，将所述第一数据发送至所述真实卡片管理器；

所述真实卡片管理器，用于接收所述卡套发送的所述第一数据，并发送至所述选中的真实卡片。

30

附图

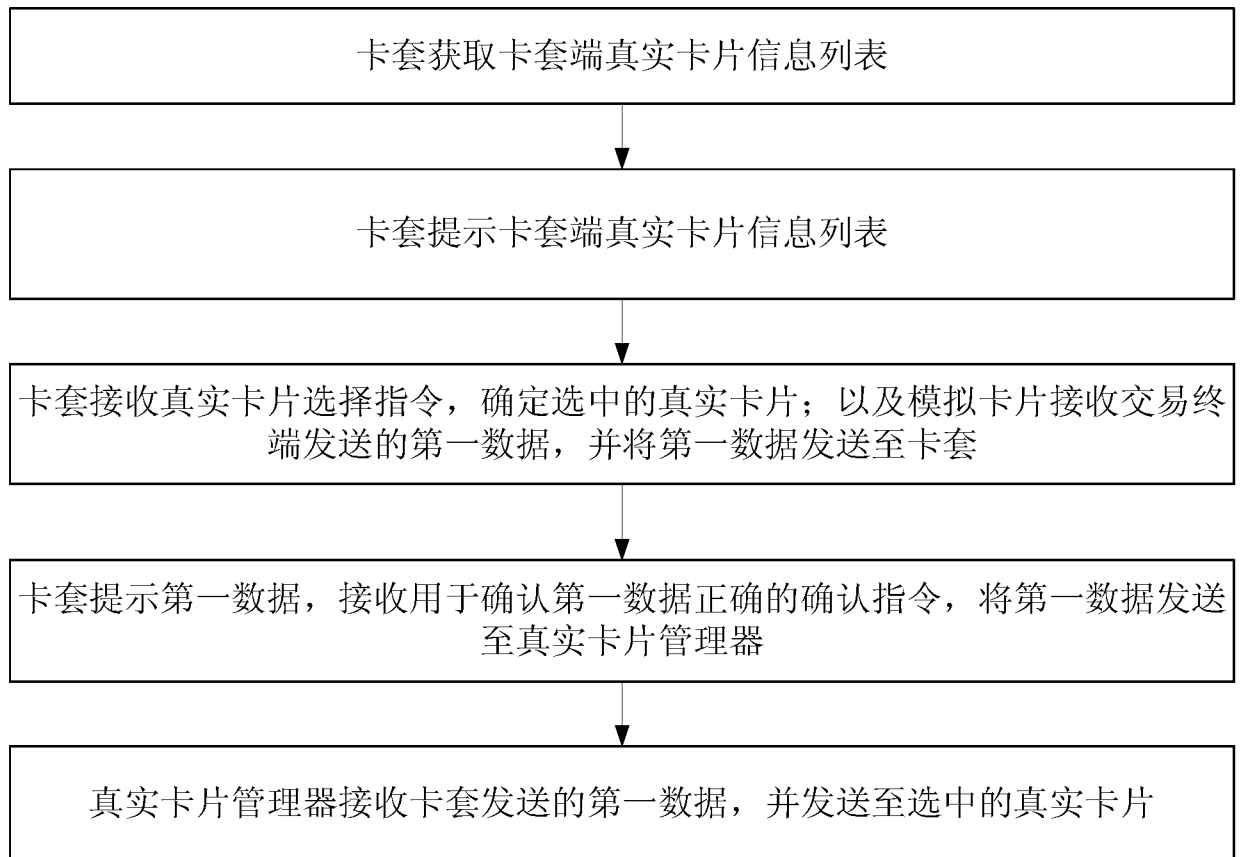


图 1

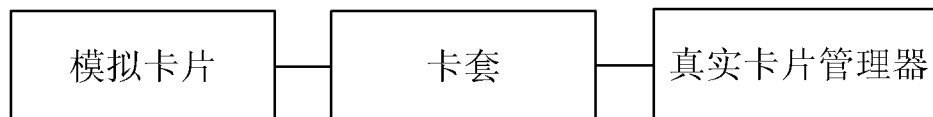


图 2

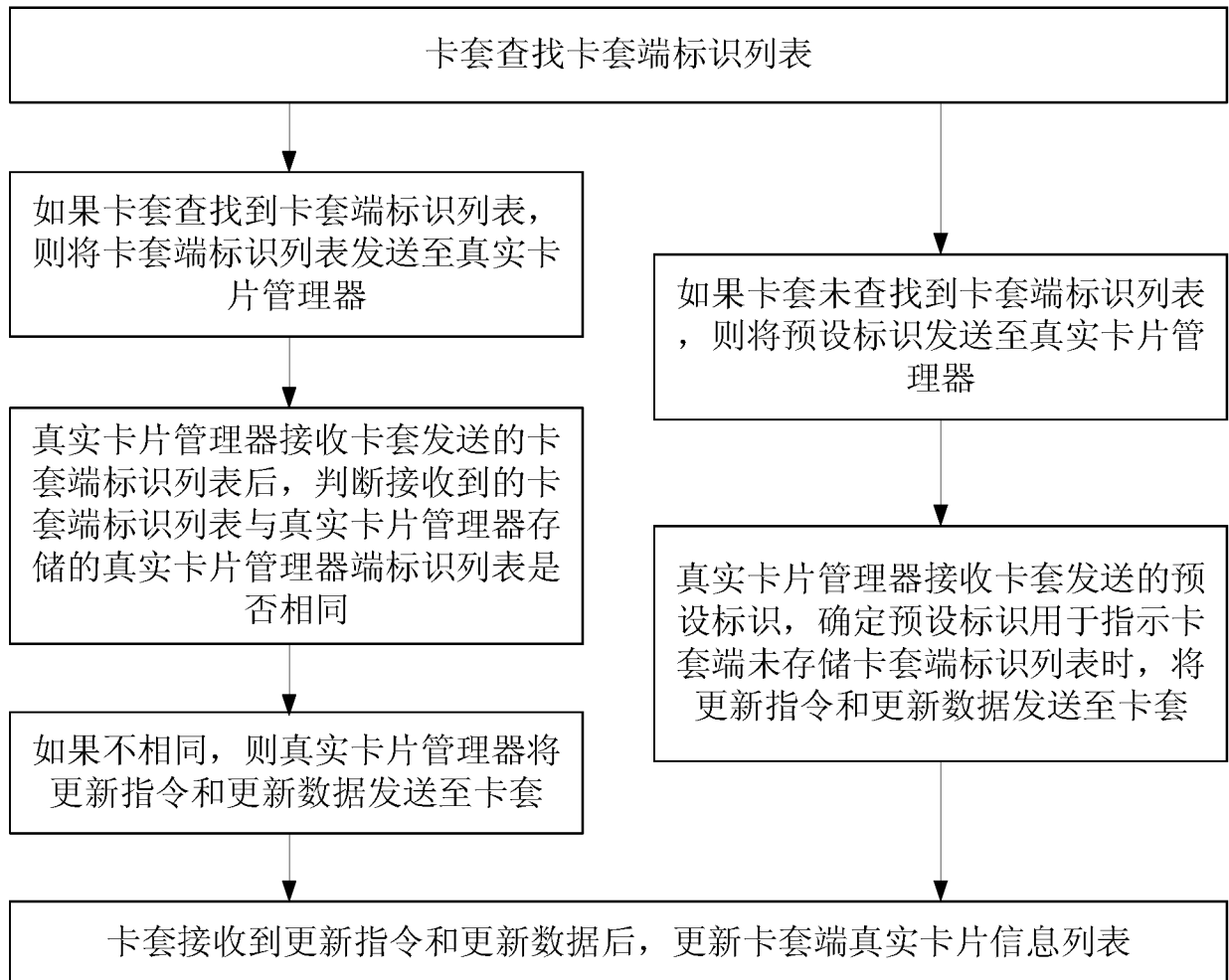


图 3

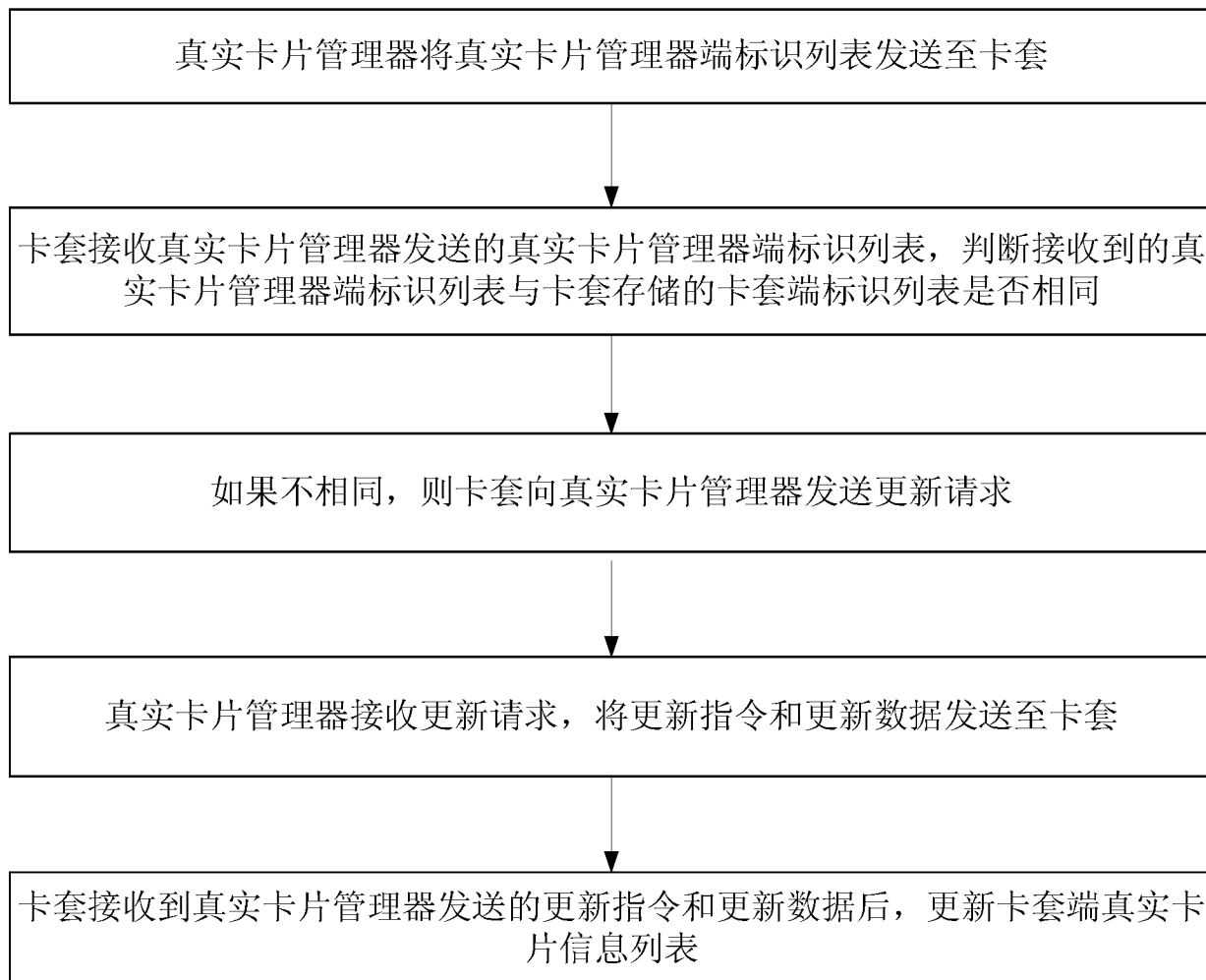


图 4

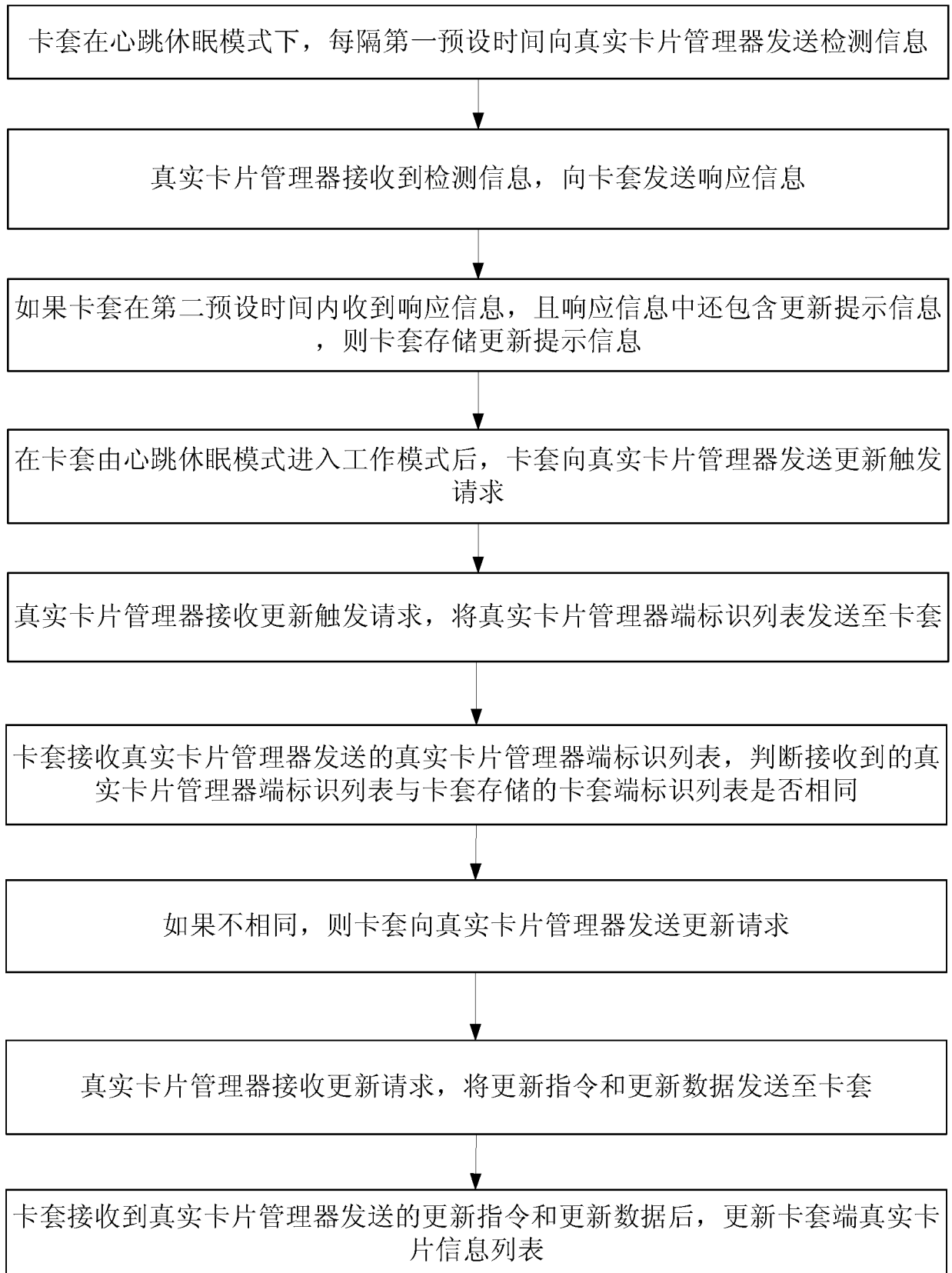


图 5

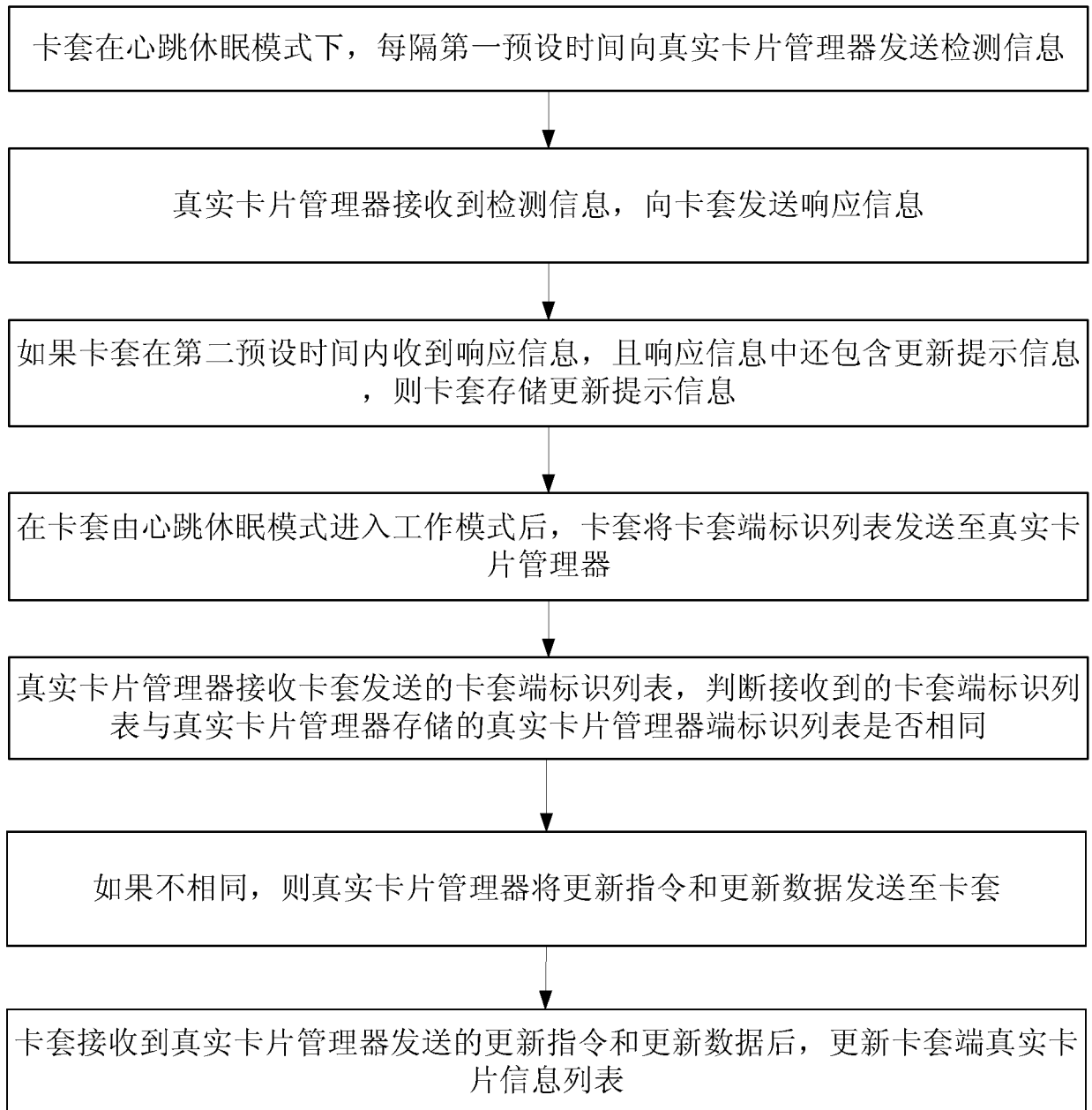


图 6

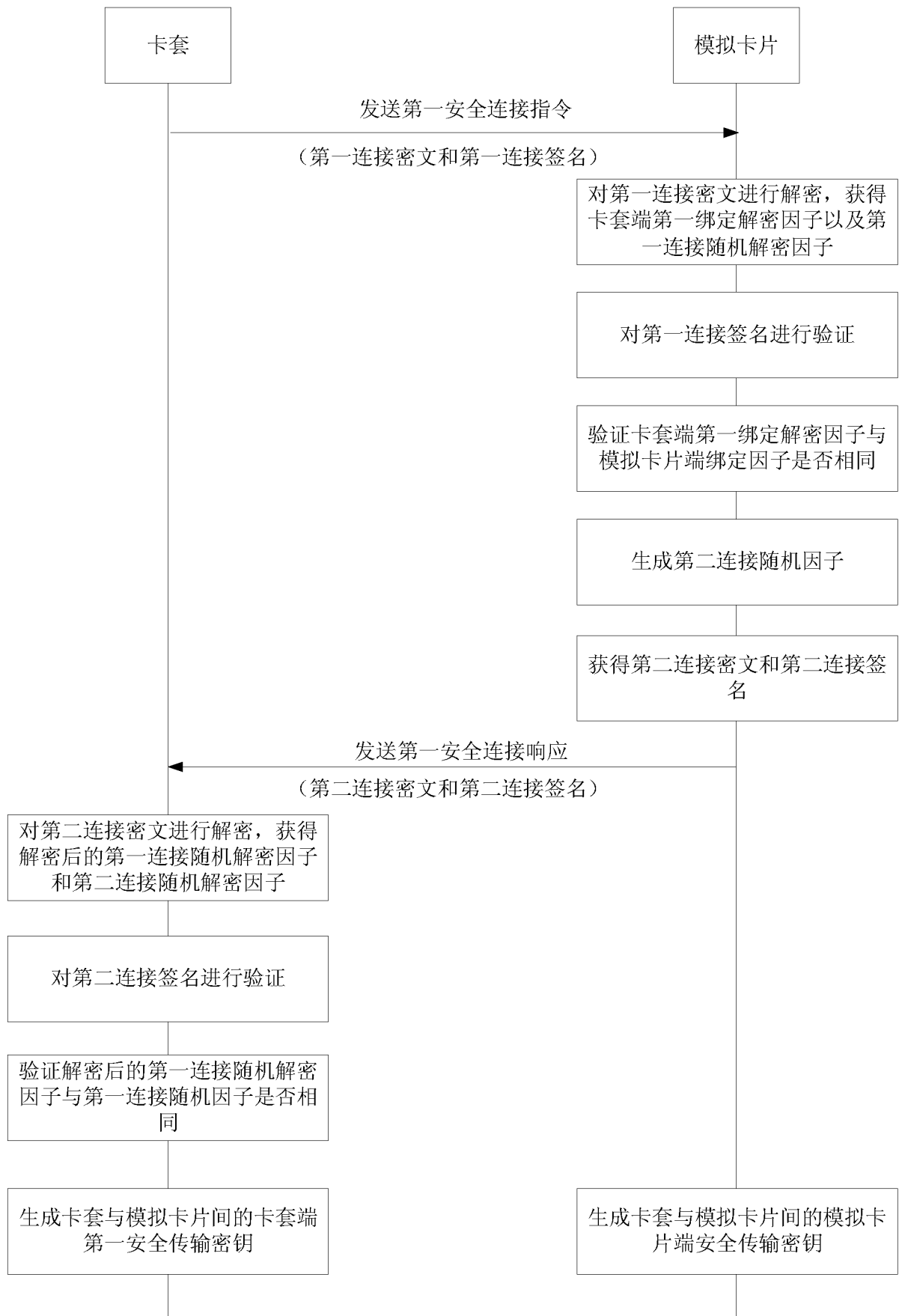


图 7

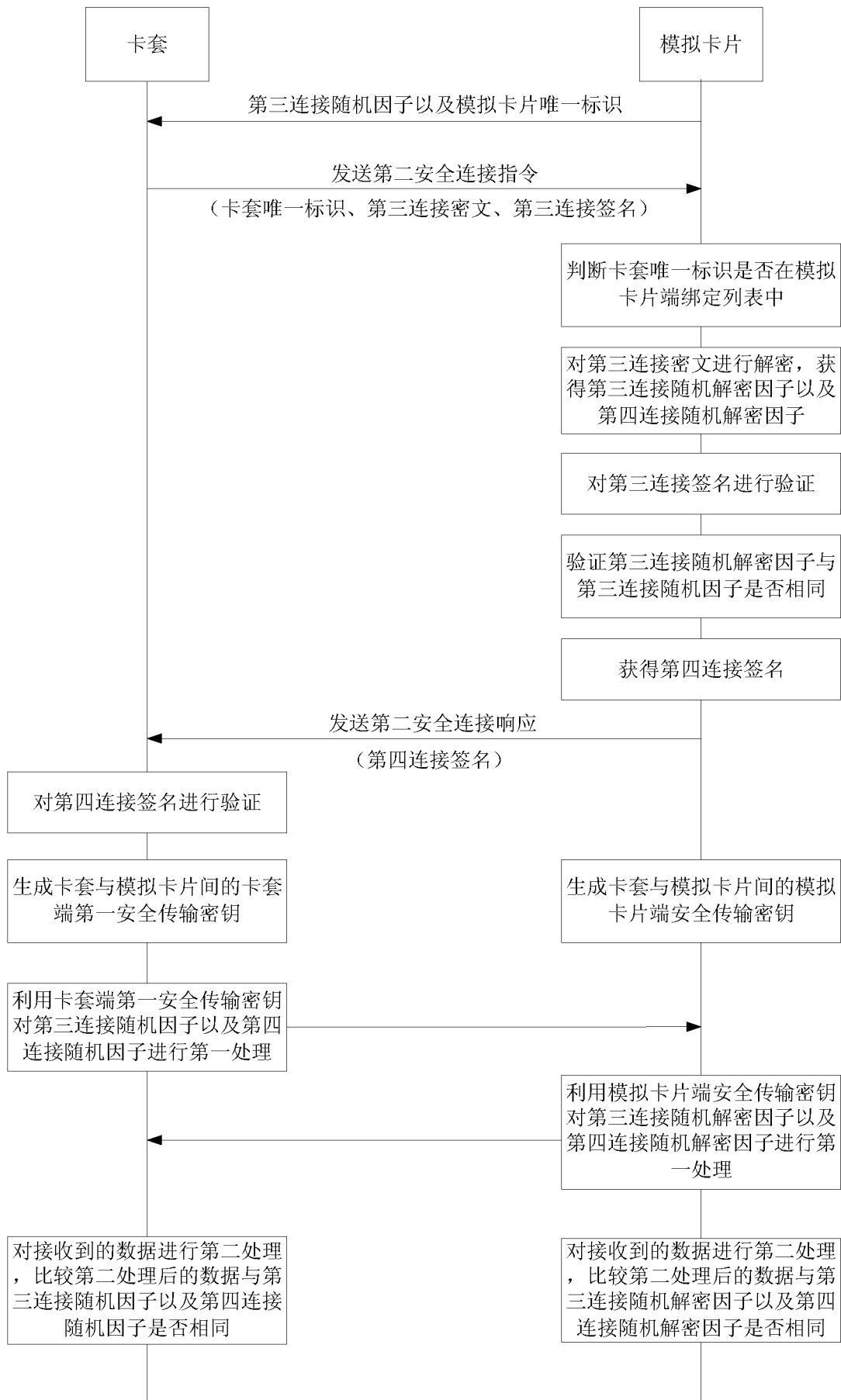


图 8

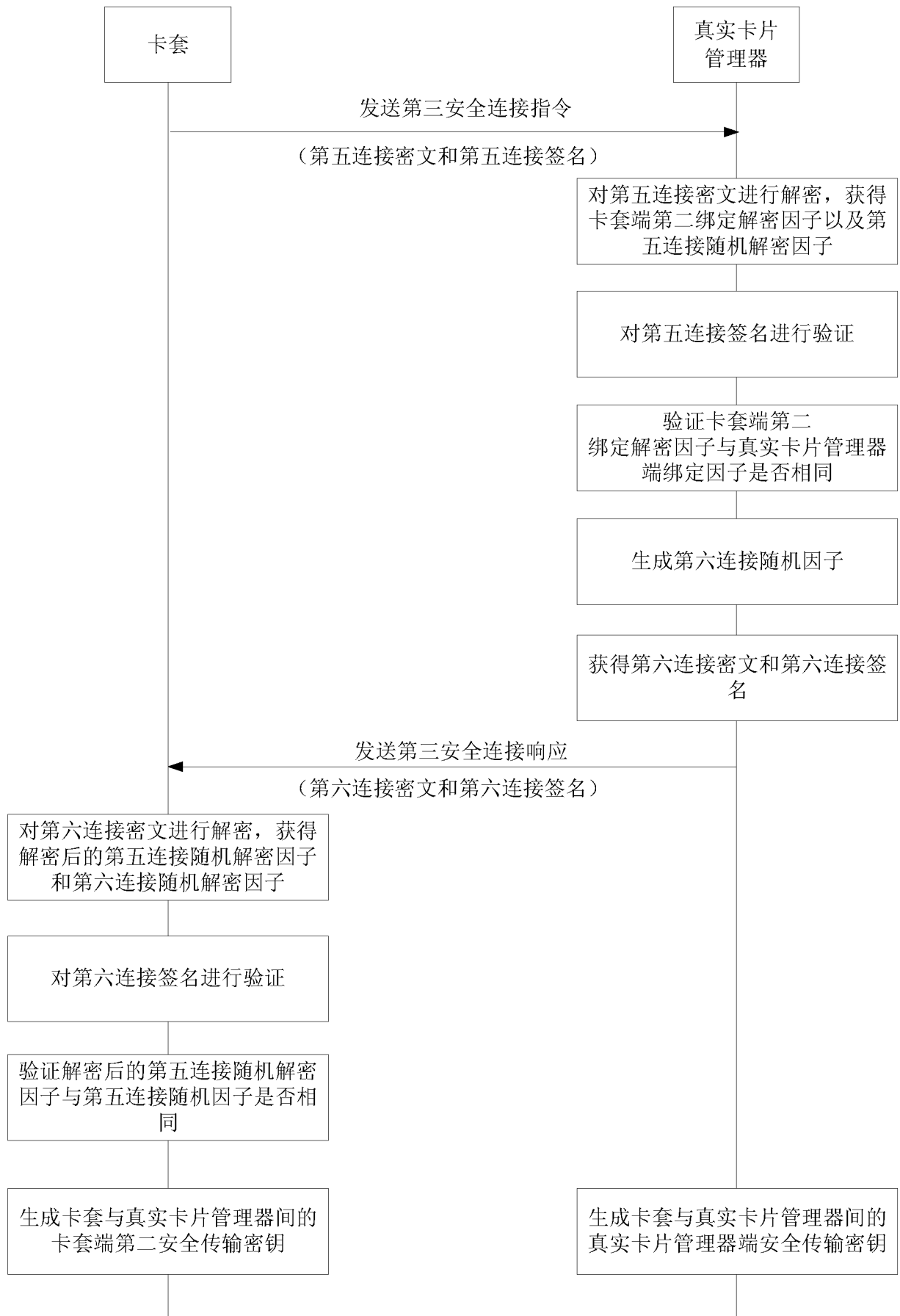


图 9

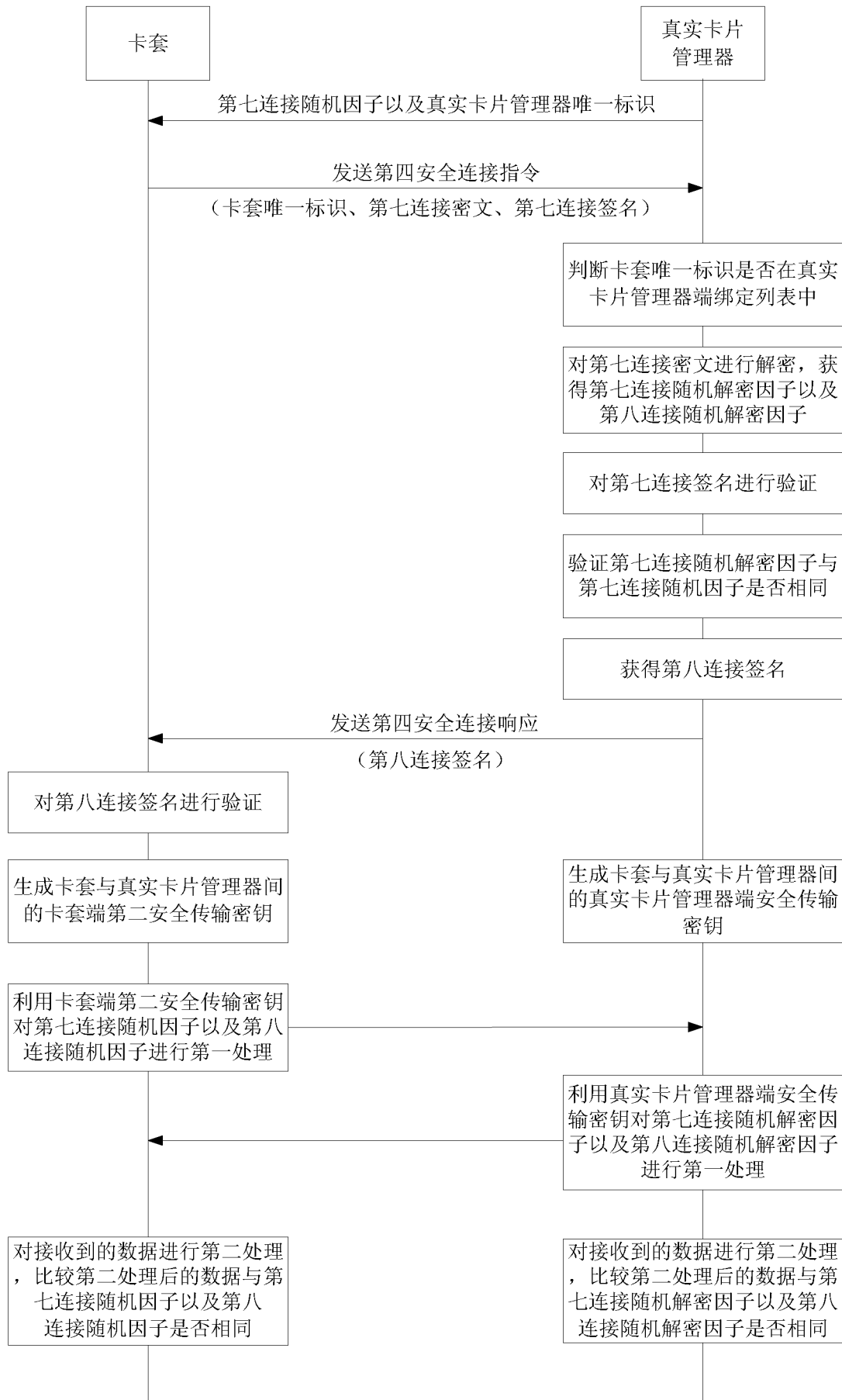


图 10

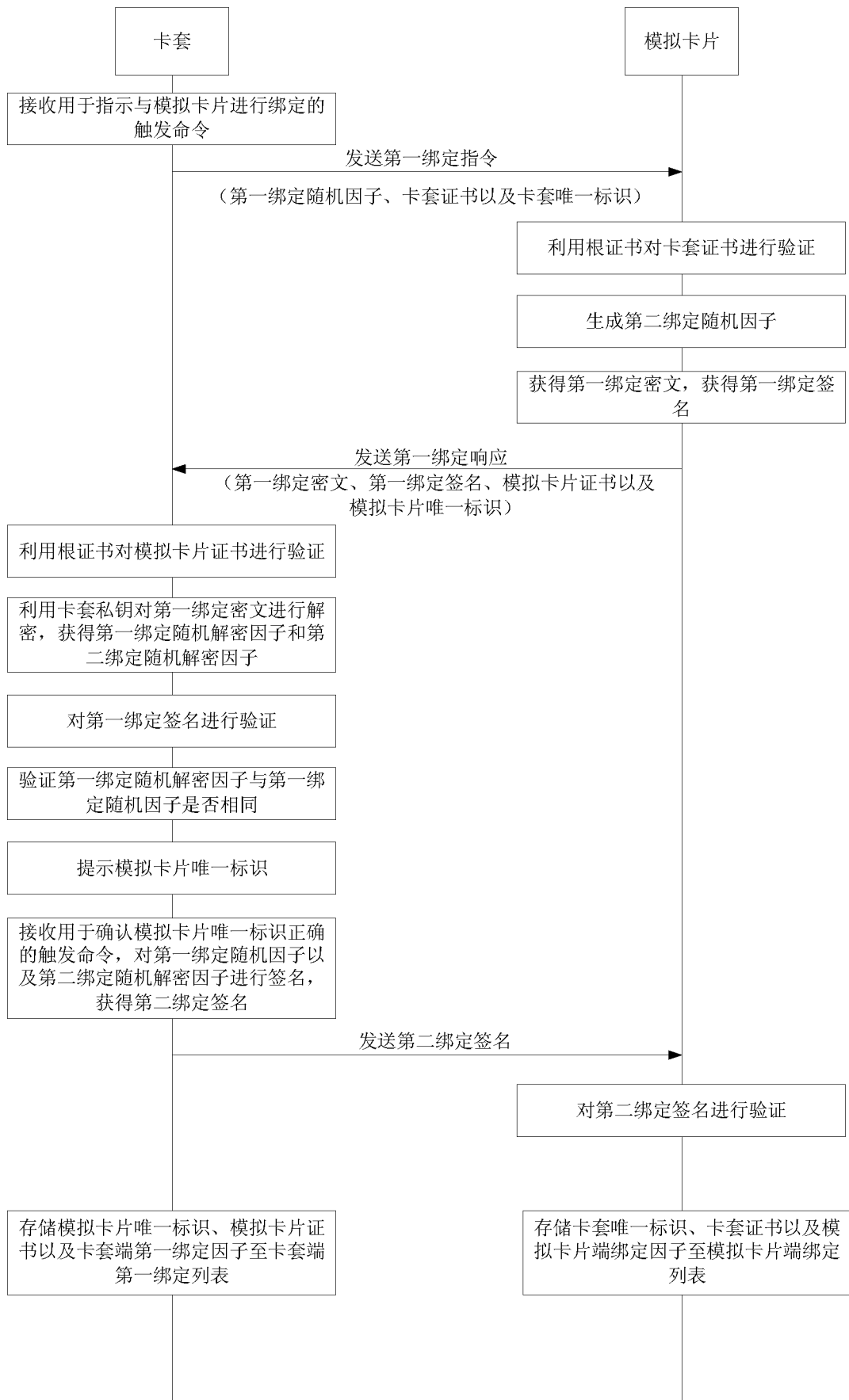


图 11

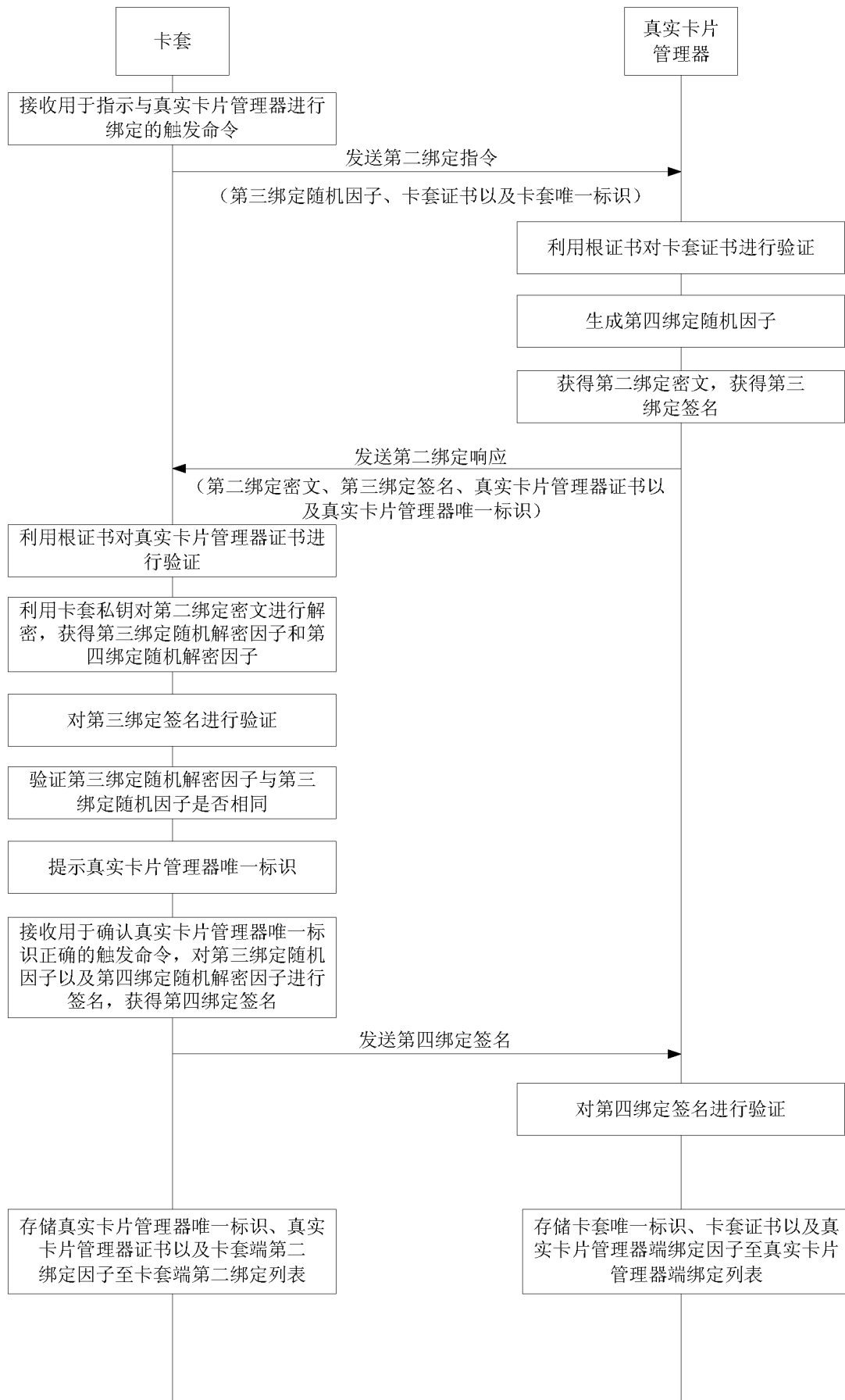


图 12

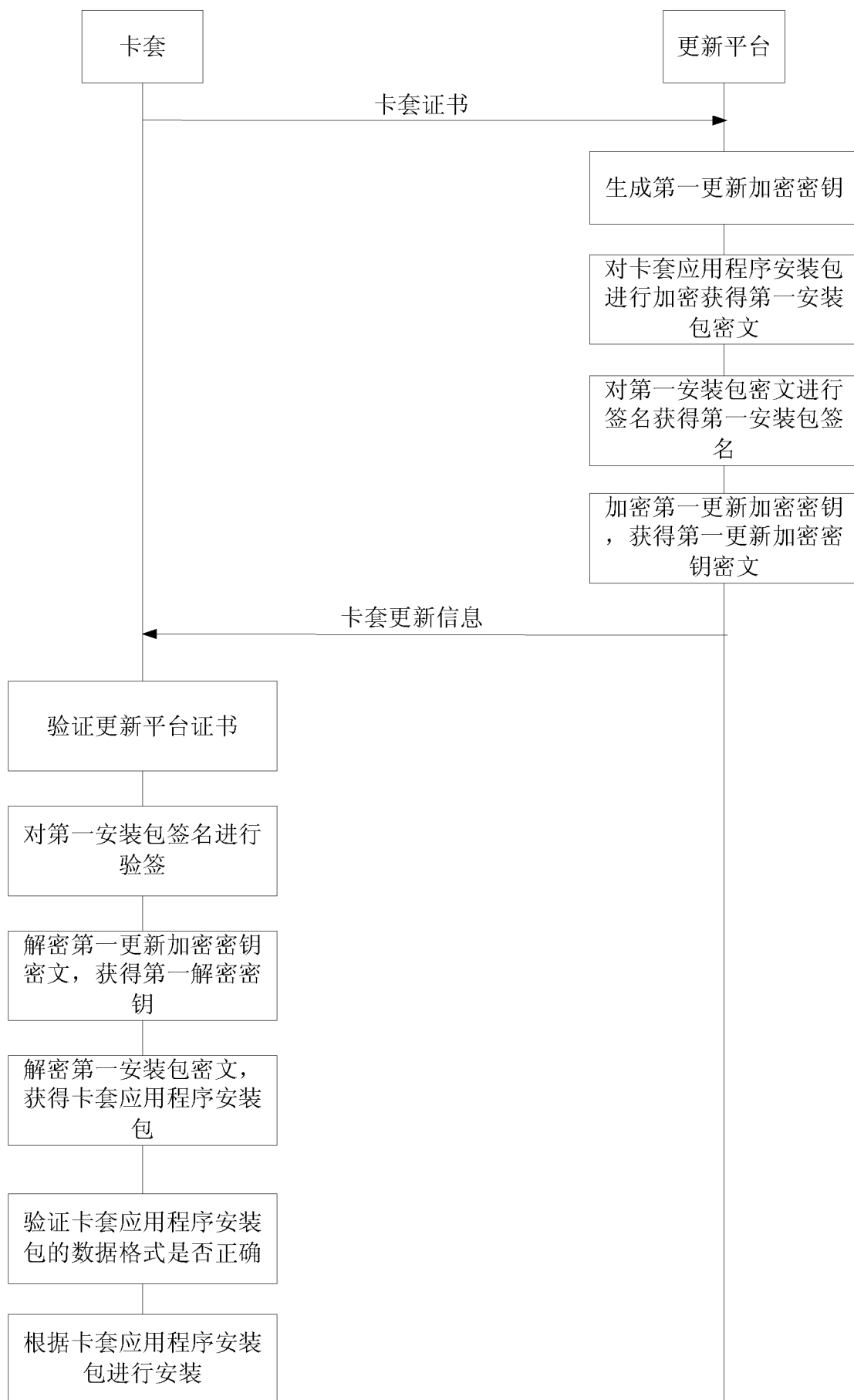


图 13

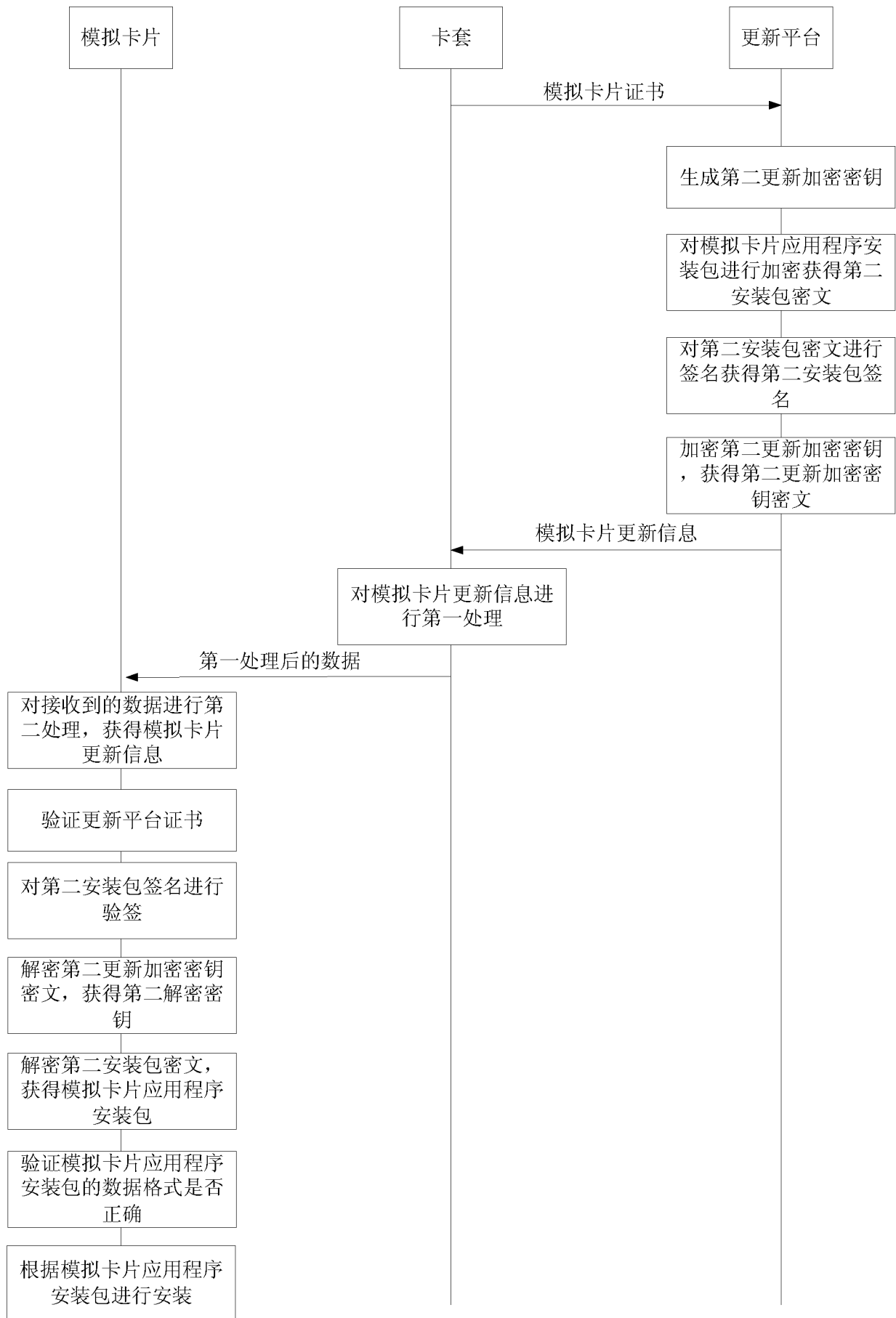


图 14

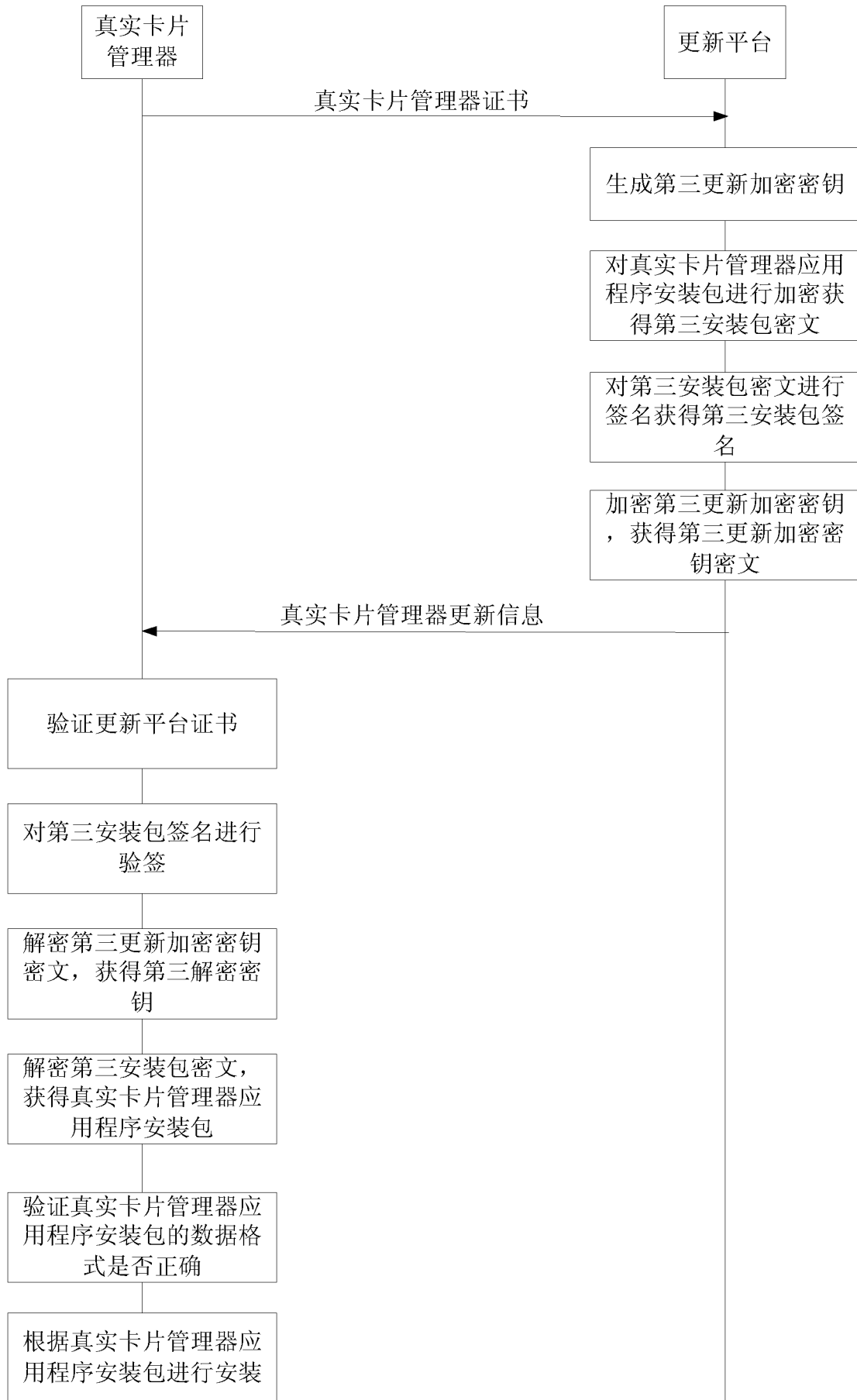


图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/093729

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

WPI, EPODOC, CNKI, CNPAT, IEEE: card, credit, bank, account, multi+, sleeve, transaction, trade, business, pay, simulative, virtual, actual, actual, list, select

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102610043 A (YU, Mengyuan) 25 July 2012 (25.07.2012) description, paragraphs [0007]-[0011]	1-16
A	CN 103903369 A (CHINA UNIONPAY CO., LTD.) 02 July 2014 (02.07.2014) the whole document	1-16
A	US 2012091199 A1 (TALKER, ALBERT) 19 April 2012 (19.04.2012) the whole document	1-16

☐ 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 08 January 2016	Date of mailing of the international search report 27 January 2016
Name and mailing address of the ISA 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 MA, Chunli Telephone No. (86-10) 82245490

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2015/093729

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102610043 A	25 July 2012	WO 2013117061 A1	15 August 2013
CN 103903369 A	02 July 2014	None	
US 2012091199 A1	19 April 2012	None	

A. 主题的分类 H04L 29/06 (2006.01) 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)) WPI, EPODOC, CNKI, CNPAT, IEEE: 信用卡, 银行卡, 账号, 多, 卡片, 卡套, 交易, 支付, 刷卡, 模拟, 虚拟, 真实, 列表, 选择, card, credit, bank, account, multi-, sleeve, transaction, trade, business, pay, simulative, virtual, actual, list, select														
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>A</td> <td>CN 102610043 A (于梦媛) 2012年 7月 25日 (2012 - 07 - 25) 说明书第[0007]-[0011]段</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>CN 103903369 A (中国银联股份有限公司) 2014年 7月 2日 (2014 - 07 - 02) 全文</td> <td>1-16</td> </tr> <tr> <td>A</td> <td>US 2012091199 A1 (TALKER, ALBERT) 2012年 4月 19日 (2012 - 04 - 19) 全文</td> <td>1-16</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	A	CN 102610043 A (于梦媛) 2012年 7月 25日 (2012 - 07 - 25) 说明书第[0007]-[0011]段	1-16	A	CN 103903369 A (中国银联股份有限公司) 2014年 7月 2日 (2014 - 07 - 02) 全文	1-16	A	US 2012091199 A1 (TALKER, ALBERT) 2012年 4月 19日 (2012 - 04 - 19) 全文	1-16
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
A	CN 102610043 A (于梦媛) 2012年 7月 25日 (2012 - 07 - 25) 说明书第[0007]-[0011]段	1-16												
A	CN 103903369 A (中国银联股份有限公司) 2014年 7月 2日 (2014 - 07 - 02) 全文	1-16												
A	US 2012091199 A1 (TALKER, ALBERT) 2012年 4月 19日 (2012 - 04 - 19) 全文	1-16												
☐ 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 1月 8日		国际检索报告邮寄日期 2016年 1月 27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 马春黎 电话号码 (86-10) 82245490												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/093729

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	102610043	A	2012年 7月 25日	WO	2013117061 A1	2013年 8月 15日
CN	103903369	A	2014年 7月 2日	无		
US	2012091199	A1	2012年 4月 19日	无		