(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102298741 A
(43)申请公布日 2011.12.28

(21)申请号 201010220936.7

(22)申请日 2010.06.22

(71)申请人 安智金融与工业公司
地址 法国塞纳河畔讷伊沙尔勒德高卢大街192号

(72)发明人 大卫·纳卡什

(74)专利代理机构 北京派特恩知识产权代理事务所(普通合伙) 11270
代理人 张颖玲

(51)Int.Cl.
G06Q 20/00(2006.01)

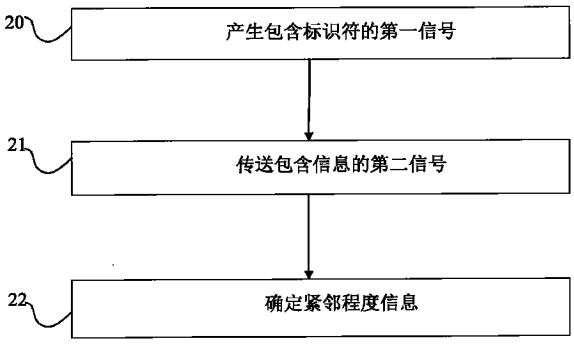
权利要求书 2 页 说明书 6 页 附图 3 页

(54)发明名称

用于确保交易安全的方法及其相应的设备和计算机程序

(57)摘要

本发明涉及一种用于确保通过电子卡进行交易时的安全的方法。根据本发明,所述电子卡至少搭配一个移动终端,其中负责管理交易的银行机构在与所述卡的所有人相关的数据中为所述移动终端预设记录一个标识符,该方法包括以下步骤:传输,通过所述移动终端传输至少一个有标识符信息的第一信号;接收,通过至少一个靠近移动终端的交易设备接收所述第一信号;传输,通过所述交易设备传输包含至少一个所述信息的第二信号到至少一个远程银行机构;分配,通过银行机构的控制服务器分配到涉及所述电子卡的交易中,并通过银行机构的控制服务器分配代表所述电子卡与所述移动终端之间的紧邻程度的信息,根据所述银行机构接收到的所述第二信号。



CN 102298741 A

1. 用于确保通过电子卡进行交易时的安全的方法，其中所述电子卡至少搭配一个移动终端，其中负责管理交易的银行机构在与所述卡的所有人相关的数据中为所述移动终端预设记录一个标识符，该方法包括一下步骤：

- 传输，通过所述移动终端传输至少一个有标识符信息的第一信号；

- 接收，通过至少一个靠近移动终端的交易设备接收所述第一信号；

- 传输，通过所述交易设备传输包含至少一个所述信息的第二信号到至少一个远程银行机构；

- 分配，通过银行机构的控制服务器分配到涉及所述电子卡的交易中，并通过银行机构的控制服务器分配代表所述电子卡与所述移动终端之间的紧邻程度的信息，根据所述银行机构接收到的所述第二信号。

2. 根据权利要求 1 所述的用于确保交易安全的方法，其包括以下步骤：

- 确定所述移动终端和所述交易设备之间的距离，通过代表所述电子卡与所述移动终端之间的紧邻程度的信息；

- 当所述距离大于预定阈值时拒绝所述交易及 / 或生成警告。

3. 根据任一权利要求 1 和 2 所述的确保交易安全的方法，其中所述预定阈值由确定所述代表紧邻程度的信息所经过的时间来确定。

4. 根据权利要求 1 到 3 中任一权利要求所述的确保交易安全的方法，其中所述信息包括至少一个银行参考信息和至少一个寻址信息指定所述银行机构。

5. 根据权利要求 1 到 4 中任一权利要求所述的确保交易安全的方法，其中所述第一信号根据一种属于下列通讯技术组中的技术传输：

- “蓝牙”技术；

- “无线局域网络”技术；

- “射频识别”技术；

- “近场通信”技术；

- 红外技术。

6. 用于通过电子卡的方式进行交易的交易设备，其中所述电子卡搭配至少一个移动终端，其中负责管理交易的银行机构在与所述卡的所有人相关的数据中为所述移动终端预设记录一个标识符，其中所述交易设备包含：

- 接收装置，从移动终端接收至少一个包含所述标识符信息的第一信号；

- 传输装置，传输包含至少一个所述信息的第二信号到至少一个银行机构。

7. 用于管理通过电子卡进行交易的银行服务器，其中所述电子卡搭配至少一个移动终端，其中所述银行服务器包括：

- 用于在与所述卡的所有人相关的数据中为所述移动终端记录一个标识符的装置；

- 用于从交易设备中接收至少一个包含所述标识符信息的信号的装置；

- 用于在一笔涉及所述电子卡的交易中确定代表所述电子卡和所述移动终端之间紧邻程度的信息的装置。

8. 移动终端，其中包含向至少一个交易设备发送至少一个包含一个标识符信息的信号的装置。

9. 一个可在通信网络上下载和 / 或可记录在计算机可读介质和 / 或能够在处理器上运

行的计算机程序，其中包括运行根据权利要求 1 到 5 中至少一个权利要求所述的确保安全的方法的程序代码指令，当其被执行于一个交易设备上。

10. 一个可在通信网络上下载和 / 或可记录在计算机可读介质和 / 或能够在处理器上运行的计算机程序，其中包括运行根据权利要求 1 到 5 中至少一个权利要求所述的确保安全的方法的程序代码指令，当其被执行于一个移动终端上。

11. 一个可在通信网络上下载和 / 或可记录在计算机可读介质和 / 或能够在处理器上运行的计算机程序，其中包括运行根据权利要求 1 到 5 中至少一个权利要求所述的确保安全的方法的程序代码指令，当其被执行于一个银行服务器上。

用于确保交易安全的方法及其相应的设备和计算机程序

技术领域

[0001] 本发明的领域是通过交易设备进行的交易，例如用电子支付终端或者自动提款机进行的交易。

[0002] 更具体来说，本发明涉及对这种交易的安全性及可追溯性的改进。

现有技术

[0003] 一个典型的确保交易安全的技术包括通过持卡人所知的个人密码认证交易中涉及的电子卡，例如一个 4 位数字的密码。但是这种技术并不完全可靠，因为这种情况下密码可能被发现，例如在密码被输入时被观察到，或者通过程序进行检索，以便使用从持卡人那里偷来的卡。

[0004] 为克服这些缺点，一些技术特别地通过增加持卡人的生物认证来加强交易的安全性，例如获取指纹，语音识别等。

[0005] 然而，由于需要使用生物识别传感器，运用这些技术的价格昂贵，而且由于用户需要提供指纹，使得这些技术并不方便，它们由于耗时长，使得交易更加复杂。

[0006] 发明目的

[0007] 本发明的目的在于克服现有技术中存在的不足之处。

[0008] 更具体地说，根据至少一个具体实施方式，本发明的目的在于提供一种加强交易安全和认证的方法。

[0009] 进一步说，本发明旨在提供一种技术，使得在交易中不要求用户有任何额外的操作或者行为。

[0010] 本发明的另一个目的是提供一种技术，这种技术并不涉及对交易生效的限制和验证。

发明内容

[0011] 本发明提供了一种不包含任何现有技术中存在的缺陷的解决方案，表现为一种确保通过电子卡方式进行交易时交易安全的方法。

[0012] 根据本发明，所述电子卡至少搭配一个移动终端，其中负责管理交易的银行机构在与所述卡的所有人相关的数据中为所述移动终端预设记录一个标识符，该方法包括一下步骤：

[0013] - 传输，通过所述移动终端传输至少一个有标识符信息的第一信号；

[0014] - 接收，通过至少一个靠近移动终端的交易设备接收所述第一信号；

[0015] - 传输，通过所述交易设备传输包含至少一个所述信息的第二信号到至少一个远程银行机构；

[0016] - 分配，通过银行机构的控制服务器分配到涉及所述电子卡的交易中，并通过银行机构的控制服务器分配代表所述电子卡与所述移动终端之间的紧邻程度的信息，根据所述银行机构接收到的所述第二信号。

[0017] 因此，本发明是基于一种新的和创造性的方法来确保交易安全，它运用电子卡持卡人的移动终端，特别是手提电话和交易设备之间的紧邻程度来添加额外的因素确保交易的安全。

[0018] 事实上，如果交易涉及的电子卡的持卡人的移动终端靠近交易设备，或者在传输之前或之后处于距离交易设备很短的时间段内，则该交易很可能已经由持卡人执行了。

[0019] 相反，如果银行卡被盗且由盗贼所使用，通常持卡人的移动终端并不靠近交易设备，交易即被标记为“可疑”。

[0020] 根据本发明的一个具体实施方式，确保安全的方法包括下列步骤：

[0021] - 确定所述移动终端和所述交易设备之间的距离，通过代表所述电子卡与所述移动终端之间的紧邻程度的信息；

[0022] - 当所述距离大于预定阈值时拒绝所述交易及 / 或生成警告。

[0023] 因此，如果银行机构的控制服务器确定交易中涉及的持卡人的移动终端并不在预定的与交易设备之间的紧邻程度之内，或者相反地距离交易设备非常远，银行机构可以向持卡人发出警报，例如打电话确认交易的有效性。

[0024] 特别是所述预定阈值由确定所述代表紧邻程度的信息所经过的时间来确定。

[0025] 事实上，可接受的距离是变化的，基于确定紧邻程度信息所需的时间而定，还要考虑交易的时间。

[0026] 例如，如果银行机构从一个交易设备接收到一个信号，表明用户的移动终端出现在地点 X，而交易在 30 分钟后发生，在距离 2 公里的地点 Y，银行机构的控制服务器必须考虑经过的时间（即 30 分钟）以确定可以适用的阈值。事实上，用户有可能在 30 分钟内走 2 公里的距离。

[0027] 另外，如果交易在银行机构接收到信号后几个小时才发生，控制服务器会根据所经过的时间，考虑到紧邻程度信息而确定交易已经过期了。

[0028] 此外，每当持卡人的移动终端靠近一个使用本发明的交易设备，它会传送信号给银行机构的服务器来确定移动终端的位置。银行机构的服务器确定移动终端新的位置，并更新当前的信息，以便在任何时候确定代表最新紧邻程度的信息。

[0029] 根据本发明的一个具体的特点，所述的信息包括至少一个银行参考信息和至少一个寻址信息指定所述银行机构。

[0030] 因此，由移动终端传送的信息不仅包含所述终端的标识符，使得设备可以识别它（为了回应它，或者将信息传输的银行机构），还包含代表终端持有人银行账户及相关的卡的信息，以及交易设备发送第二信号的银行机构信息。

[0031] 例如，信息可以包含银行账户号码，或者与银行账户相关的电子卡号，以及一个负责管理所述银行账户的银行机构的电话号码或者电子邮件地址。

[0032] 这样交易设备可或者它发送的信息的接收器（银行机构），由此来表明由它识别的移动终端的位置。

[0033] 根据本发明的一个具体实施方式，所述第一信号根据一种属于下列通讯技术组中的技术传输：

[0034] - “蓝牙”技术；

[0035] - “无线局域网络”技术；

[0036] - “射频识别”技术；

[0037] - “近场通信”技术；

[0038] - 红外技术。

[0039] 因此，根据本发明不同的具体实施方式，交易设备和移动终端之间的交流由不同种类的移动终端而通过不同的技术进行。

[0040] 本发明还涉及一种通过使用电子卡而进行交易的交易设备。

[0041] 根据本发明，所述电子卡搭配至少一个移动终端，其中负责管理交易的银行机构在与所述卡的所有人相关的数据中为所述移动终端预设记录一个标识符，其中所述交易设备包含：

[0042] - 接收装置，从移动终端接收至少一个包含所述标识符信息的第一信号；

[0043] - 传输装置，传输包含至少一个所述信息的第二信号到至少一个银行机构。

[0044] 这种交易设备特别地适用于实施上述确保交易安全的方法的步骤。例如，这种设备是电子支付终端，或者自动提款机。

[0045] 本发明的另一方面还涉及一种负责管理使用电子卡的交易的银行服务器，其中所述电子卡搭配至少一个移动终端，包含：

[0046] - 用于在与所述卡的所有人相关的数据中为所述移动终端记录一个标识符的装置；

[0047] - 用于从交易设备中接收至少一个包含所述标识符信息的信号的装置；

[0048] - 用于在一笔涉及所述电子卡的交易中确定代表所述电子卡和所述移动终端之间紧邻程度的信息的装置。

[0049] 这种银行服务器特别地适用于实施上述确保交易安全的方法的步骤。

[0050] 本发明还涉及一个移动终端，包含向至少一个交易设备传输至少一个包含标识符的信息的传输装置。

[0051] 这种移动终端特别地适用于实施上述确保交易安全的方法的步骤。例如，这种移动终端可以是手提电话，或者个人数字助理 (PDA)。

[0052] 最后，本发明涉及一个可在通信网络上下载和 / 或可记录在计算机可读介质和 / 或能够在处理器上运行的计算机程序，其中包括运行上述的确保安全的方法的程序代码指令，当其被执行于一个银行服务器上。

附图说明

[0053] 在阅读了对作为说明性且非限制性实例给出的本发明优先实施例和附图的以下描述之后，本发明的其它特征和优点将浮现出来，附图中：

[0054] 图 1 是根据一个具体实施方式实行本发明的一个系统的例子；

[0055] 图 2 是根据第一个具体实施方式，在图 1 所示的系统中实施确保安全的方法的主要步骤；

[0056] 图 3 是根据本发明的第二个具体实施方式进行交易的主要步骤；

[0057] 图 4 是根据本发明的第三个具体实施方式进行交易的主要步骤。

具体实施方式

[0058] 总原理

[0059] 本发明的总原理是确定银行交易中涉及的电子卡持卡人相关的移动终端的位置，并通过他或她的移动终端来确定在交易时间中持卡人与该卡的紧邻程度。

[0060] 这种紧邻程度信息由负责管理涉及问题电子卡交易的银行机构的服务器来确定，并能够为确保交易安全而添加额外的因素。

[0061] 事实上，在交易时间内，持卡人与卡之间的距离很远，会引起银行服务器的警惕并产生额外的交易确认行为（如在交易生效前打电话给持卡人，向交易设备发送警报以阻止交易，等等）。

[0062] 第一具体实施方式

[0063] 图 1 是根据第一具体实施方式实行本发明的一个系统的例子。

[0064] 10 为交易设备，例如电子支付设备，在它附近有用户 U，持有一个移动终端 11，包含至少一个传输天线 111，和一个电子卡 12.

[0065] 所述用户 U 的银行账户，特别是通过电子卡 12 进行的交易有一个银行机构来管理，该机构用服务器 13 来存储与交易有关的信息，它也称作控制服务器。

[0066] 根据本发明的这一具体实施方式，交易设备 10 能与用户 U 的移动终端 11，例如一个移动电话进行交流，更进一步说是当用户 U 在附近时接收和处理由它所传输的信号 S1。

[0067] 根据这个具体实施方式，交易设备 10 还能在收到信号 S1 后，发送信号 S2 到银行机构的服务器 13。

[0068] 参考图 2 可知，确保安全的方法的主要步骤将在本发明的第一具体实施方式中被描述，该步骤在图 1 所示的系统中实施。

[0069] 当用户 U 靠近交易设备 10 时，根据步骤 20，用户 U 的移动终端 11 传输特别包含移动终端 11 的标识符的第一信号 S1。例如，这个标识符可以是一个电话号码以便于移动终端被识别，或者是存储卡的序列号，等等。

[0070] 该信号 S1 由交易设备 10 接收并处理，并在步骤 21 中发送包含移动终端 11 的标识符的第二信号 S2 给银行服务器 13。

[0071] 根据这个具体实施方式，银行服务器 13 接收并处理该信号 S2，以提取其中的信息并用来在给定的时间内确定持有卡 12 的用户 U 的移动终端 11 的位置。

[0072] 在步骤 23 中，交易中（或者根据实施方式所示的交易后），控制服务器在交易时间中，13 根据典型交易信息及由信号 S2 中获取的信息，确定卡 12 的持卡人 U 与卡 12 之间的紧邻程度信息。

[0073] 第二具体实施方式

[0074] 参考图 3 可知，确保安全的方法的主要步骤，以及与交易本身相关的步骤将在本发明的第二具体实施方式中被描述。

[0075] 如图 1 所示，用户 U 持有电子卡 12 和移动电话 11。交易涉及的电子卡 12 由银行机构的服务器 13 管理。

[0076] 用户 U 的移动终端 11 能够根据本具体实施方式实施本方法，并且该移动终端的识别符是在步骤 30 中由服务器 13 根据与电子卡 2 相关的信息预先录制的。

[0077] 例如，与移动终端 11 相关联的一个电话号码，一个序列号，或者一个识别密码被服务器 13 记录，并与电子卡的信息建立关联，例如与账号相联系，识别密码，所有者的联系

方式，等等。

[0078] 此外，可认为数量为 n 的交易设备 D_i 能够根据本具体实施方式实施本方法，并能够分配到很多的商店（例如电子支付终端），餐厅（例如电子支付终端），商场（例如自动提款机），等等。

[0079] 由此，每当服务器预先记录的移动终端 11 位于这些设备 D_i 的任一个设备附近时，它就会发送信号 S1 到所述的设备 D_i（步骤 20）。

[0080] 事实上，根据这个具体实施方式，移动终端 11 会检测临近的设备 D_i 并向其发送信号 S1。

[0081] 根据一个可选择的具体实施方式，设备 D_i 可以检测移动终端 11，并发送给它一个信息，要求其用包含标识符的信号反馈。然后移动终端发送信号 S1 以回应交易设备 D_i 的要求。

[0082] 这个信号 S1 可通过多种短距离通信技术传输，例如，“蓝牙”、“无线局域网络”、“射频识别”、“近场通信”，或者红外技术。

[0083] 这个第一信号 S1 包括特别是有移动终端 11 的标识符的信息。这个信号 S1 还可以包含能够确认银行机构的信息，更进一步说即服务器 13，考虑到随后由设备 D_i 发送给所述服务器的信号。

[0084] 例如，信号 S1 的信息可包含能够联系到服务器 13 的邮件地址，或者一个用于传送信息到服务器的网络地址，等等。

[0085] 设备 D_i 能够接收并处理这个信号，然后在步骤 21 中发送信号 S2 到控制服务器 13。该信号 S2 也包含有标识符的信息。另外信号 S2 还包含设备 D_i 的识别信息，由此特别地用于确定移动终端 11 的位置，以及时间戳信息来记录确定移动终端 11 所需要的时间。

[0086] 信号 S2 可以以短信，电话或者电子邮件的形式发送。

[0087] 信号 S2 可以被银行机构的服务器 13 接收和处理。例如，服务器为后续的步骤记录下信号 S2 中包含的信息，或者直接从中获取有用的信息并记录下来以备后续使用。有用的信息是指，例如移动终端 11 的标识符，设备 D_i 的识别信息，确定位置需要的时间，等等。

[0088] 当控制服务器连续收到大量与相同移动终端 11 有关的信号，即，上述的步骤向很多设备 D_i 实施，服务器会更新相应的信息。例如，它会更新设备 D_i 的识别信息，以及确认相关位置的时间。这样，控制服务器存储的是给定移动终端的最新的位置信息。

[0089] 当在交易中使用电子卡 12 时，例如通过设备 D_m，与该交易有关的典型交换如下所述：

[0090] - 步骤 31 中，通过有持卡人提供的个人识别码 PIN 的方式识别交易中使用的卡 12。卡的信息及识别密码通过第一电话网络传送给银行机构的服务器 13；

[0091] - 步骤 32 中，通过银行机构 13 确认所进行的交易，例如，之前确定的客户账户上的可用金额。确认的结果通过第一电话网络传送到设备 D_m 上；

[0092] - 步骤 33 为通过交易设备 D_m 传送借记数据到银行机构 13 的服务器上，也是通过第一电话网络；

[0093] - 步骤 34 为确定交易步骤；

[0094] - 步骤 35 为在银行服务器 13 的数据库中记录交易相关的数据。

[0095] 可以认为交易设备 D_m 根据本发明实施确保安全的方法。相应的，它不会发送信号

S2 到银行机构的控制服务器上，以在交易时间内确认电子卡 12 的持卡人的移动终端 11 的位置。

[0096] 还可以认为确保安全的方法是在交易时间内，通过控制服务器 13 进行的，由此来使交易生效，或者通过打电话给卡 12 的持有人 U 的移动终端 11 发送一个警报。

[0097] 例如，在步骤 22 确定卡持有人的移动终端与卡之间紧邻程度信息的步骤可在实施了典型步骤 32，确认交易进行的情况之后进行。

[0098] 因此，当服务器注意到涉及卡 12 的交易时，它会根据卡 12 相关的存储的信息，以及从设备 D_i 接收到的最新的位置信息，来确定紧邻程度。例如，代表最新的移动终端 11 位置与交易设备 D_m 之间距离的信息将被服务器所计算。

[0099] 这个距离被设为预定阈值，用来确定交易是否“可疑”。这个比较还会考虑到最新的移动终端 11 的时间和交易时间，以确定移动终端 11 是否有时间走完所述的距离。

[0100] 例如，如果计算的距离大于这个预定值，则可以推测推定有持卡人持有的移动终端并不在交易设备 D_m 附近。则很有可能卡持有人和所有人并没有携带他的或者她的移动终端。然而，也有可能持卡人并不是卡的所有人（因此也不是移动终端 11 的持有人），而是一个偷了所述卡并希望使用的人。

[0101] 如果距离比预定的阈值大，交易将不会生效，并且在步骤 36 中会发送一个警报。这个警报包含，例如，移动终端 11 的联系信息，以此确认交易实际上为卡的所有人及移动终端的持有人所实施。

[0102] 如果距离比预订阈值短，交易就会生效，接下来的步骤 (33 到 35) 也会被实施。

[0103] 根据一个可选择的具体实施方式，可以认为交易设备 D_m 能够根据本发明实施本方法。在交易时间中，或之前，如果持有移动终端 11 的卡所有人在交易设备 D_m 附近，它就会收到第一信息 S1。交易设备 D_m 发送第二信号 S2 到服务器 13 以发送移动终端 11 的位置信息。

[0104] 但是，如果电子卡被盗或持卡人没有移动终端 11，交易设备 D_m 不会发送信号 S2 到服务器 13，它会使用存储的信息。如果存在并有效，到最新的移动终端 11 的位置信息以确定紧邻程度信息。

[0105] 根据另一个可选的具体实施方式，当服务器没有在交易之前或之中收到交易设备 D_m 的位置信息，控制服务器可以认为交易是可疑的。控制服务器能够实施本发明。

[0106] 第三具体实施方式

[0107] 参考图 4 可知，确保安全的方法的主要步骤以及与交易本身有关的步骤将在本发明的第三具体实施方式中被描述。

[0108] 这个具体实施方式实践中与图 3 所示相同（因此本实施方式的步骤不再叙述），例外情况存在与步骤 22，确定紧邻程度信息的步骤，是在交易完成后实施的，而不是在交易进行时实施的。

[0109] 因此，交易在通常情况下进行，控制服务器随后实施步骤 22，例如每晚为了检查一天的交易情况，以及如有需要的警报步骤 36。

[0110] 这种方式不使用额外的确认步骤，不会延长交易的时间，但仍旧能够检测出“可疑”的交易并发送警报给所有人。

[0111] 警报可以以不仅是电话的方式发出，例如，一封紧急的电子邮件，或者短信。

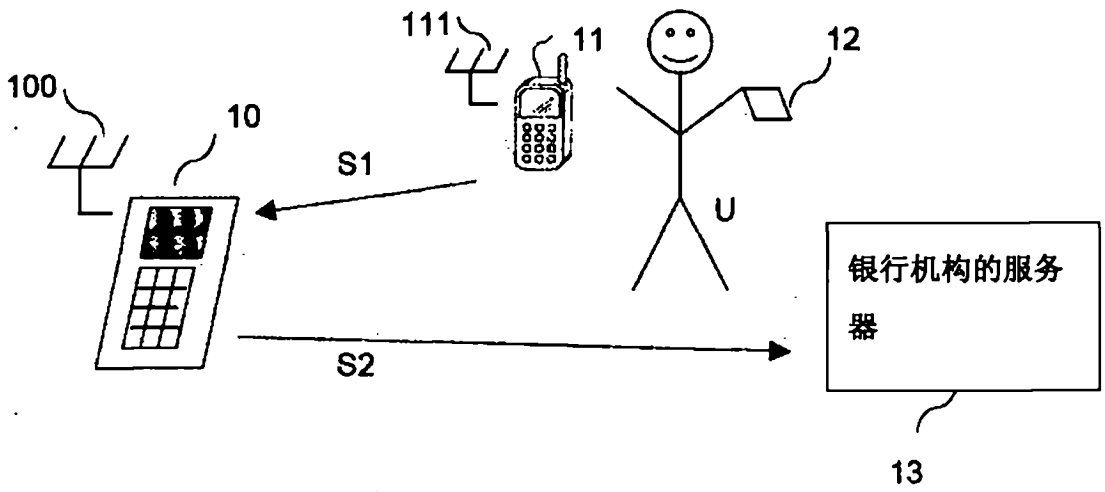

111
11
12
100
10
S1
U
银行机构的服务器
S2
13

图 1

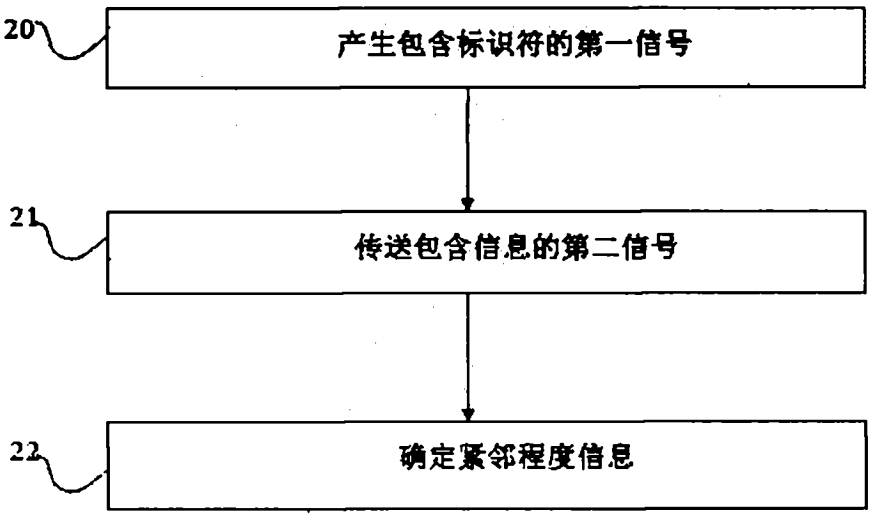

20
产生包含标识符的第一信号
21
传送包含信息的第二信号
22
确定紧邻程度信息

图 2

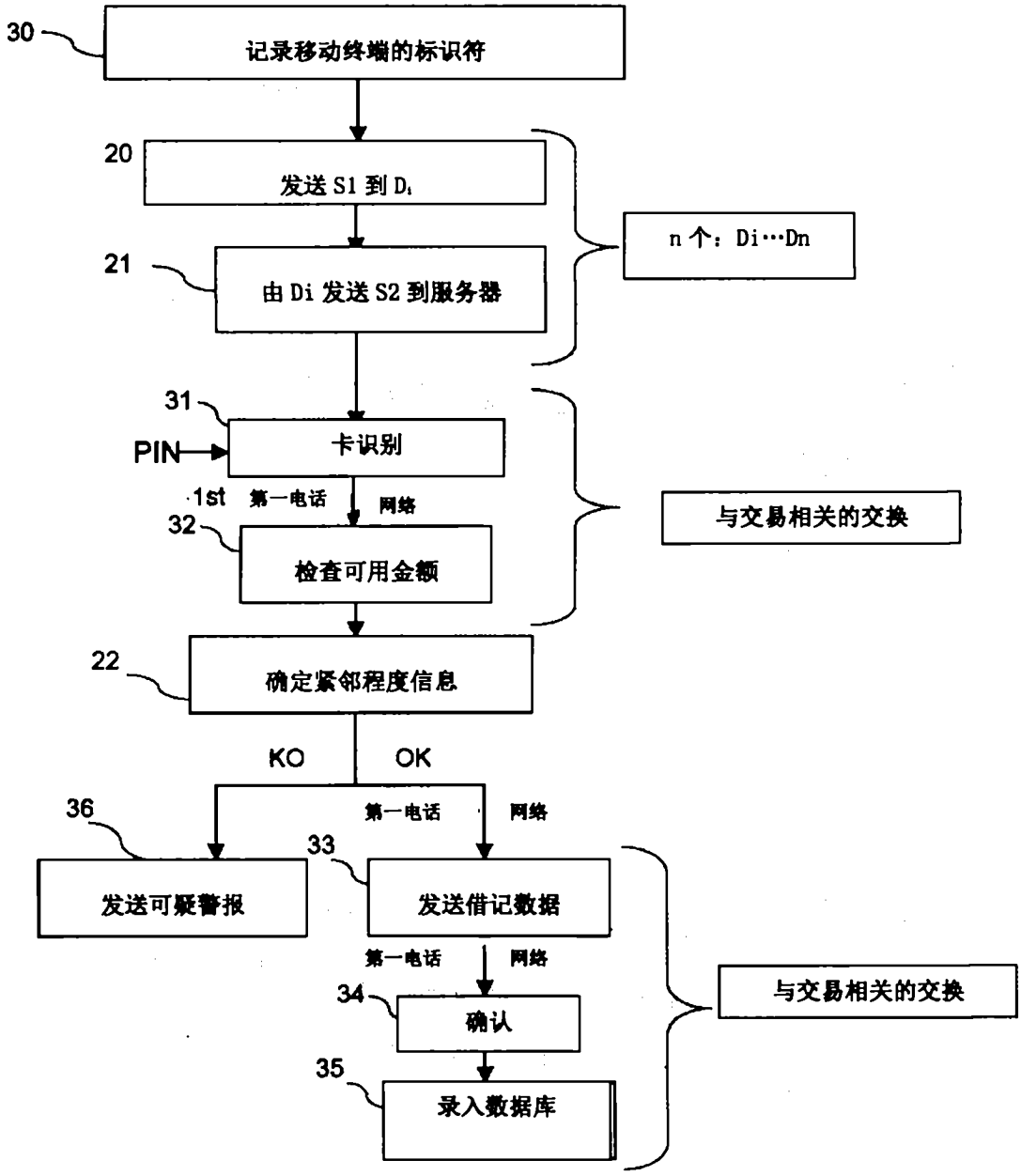

30
记录移动终端的标识符
20
发送 S1 到 Di
21
由 Di 发送 S2 到服务器
n 个：Di…Dn
31
PIN
卡识别
1st
第一电话
网络
32
检查可用金额
与交易相关的交换
22
确定紧邻程度信息
KO
OK
第一电话
网络
36
发送可疑警报
33
发送借记数据
第一电话
网络
34
确认
35
录入数据库
与交易相关的交换

图 3

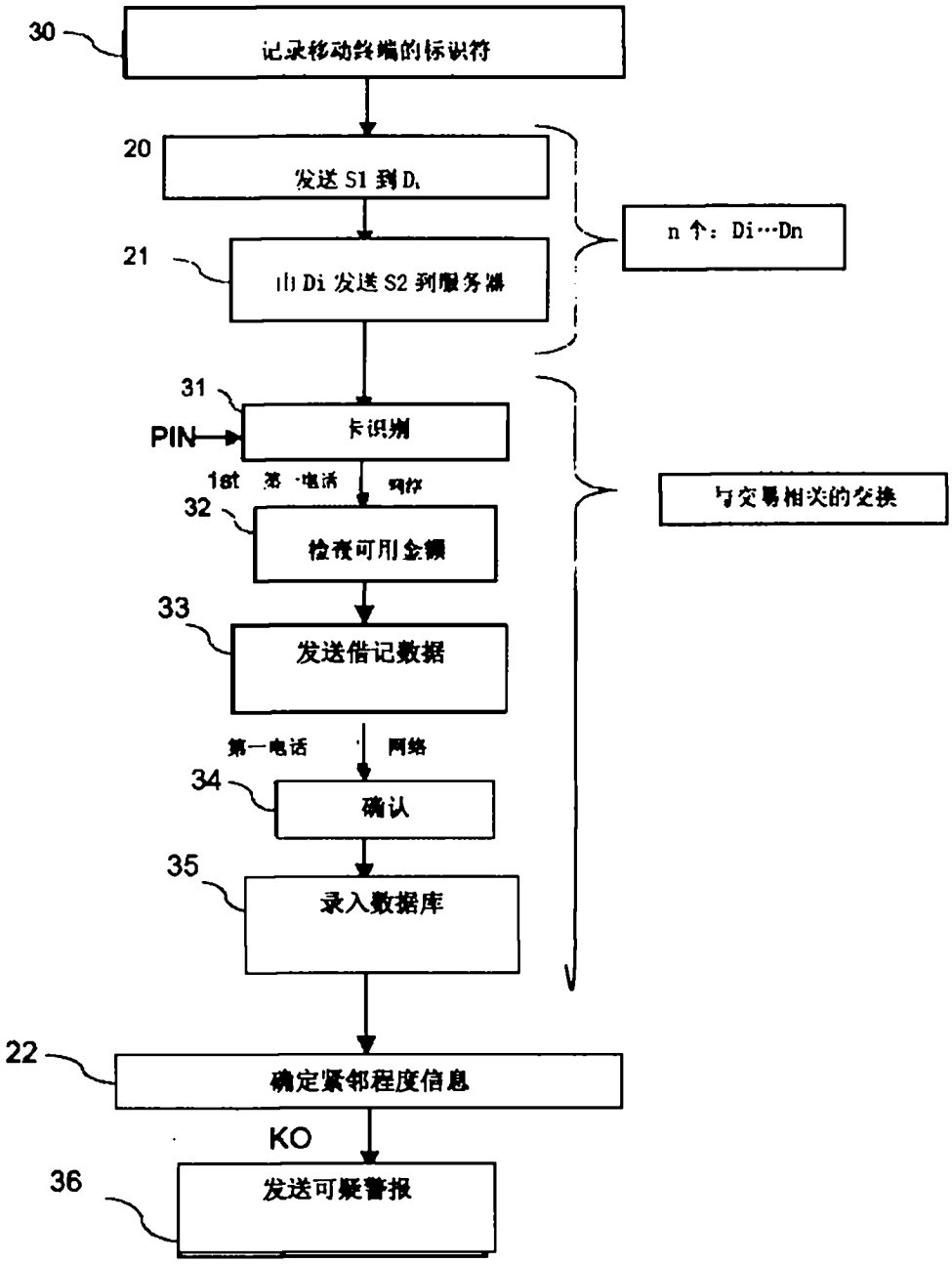

30
记录移动终端的标识符
20
发送 S1 到 Di
n 个：Di…Dn
21
由 Di 发送 S2 到服务器
31
PIN
卡识别
1st 第一电话
网络
与交易相关的交换
32
检查可用金额
33
发送借记数据
第一电话
网络
34
确认
35
录入数据库
22
确定紧邻程度信息
KO
36
发送可疑警报

图 4