[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/60

[12]发明专利申请公开说明书

[21]申请号 00102262.8

[43]公开日 2000年9月13日

[11]公开号 CN 1266240A

[22]申请日 2000.2.12 [21]申请号 00102262.8

[30]优先权

[32]1999.2.12 [33]US [31]60/119,818

[32]1999.7.12 [33]US [31]60/144,927

[71]申请人 花旗银行全国协会(N.A.)

地址 美国纽约

[72]发明人 达恩·舒茨尔 阿兰·斯莱特

托马斯·西里洛

罗伯特·德罗德斯

[74]专利代理机构 隆天国际专利商标代理有限公司

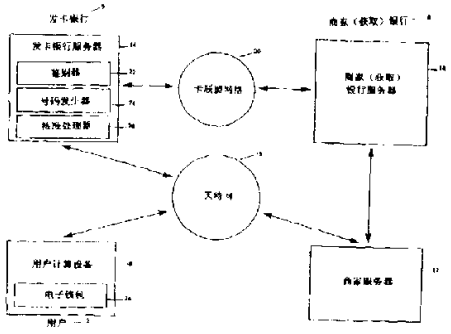
代理人 李 强 潘培坤

权利要求书8页 说明书22页 附图页数6页

[54]发明名称 用于实现银行卡交易的方法和系统

[57]摘要

一种完成银行卡交易的方法和系统,提供一个交易卡系统,以允许交易卡用户 向交易卡发卡人输入鉴别信息,产生一个匿名或替换卡号,并且维持在匿名或 替换卡号和交易卡用户的交易卡号之间的链接。本发明的一个可替换的方面例 如利用在一个本地计算设备上的软件,它核准交易卡用户并以和交易卡发卡人 的服务器同步的顺序产生匿名卡号。



ISSN1008-4274

00.02.17

权 利 要 求 书

1、由交易卡用户进行交易的方法，包括：

鉴别交易卡用户；

产生交易卡用户的一个匿名卡号；

使交易卡用户的匿名卡号与一个交易卡号相关联；

用交易卡用户的匿名卡号核准交易。

2、权利要求 1 的方法，其特征在于：交易卡用户的鉴别进一步还包括通过交易卡发卡人鉴别交易卡用户。

3、权利要求 2 的方法，其特征在于：交易卡用户的鉴别进一步还包括通过交易卡发卡人的服务器鉴别交易卡用户。

4、权利要求 2 的方法，其特征在于：交易卡用户的鉴别进一步还包括通过交易卡发卡人接收交易卡用户信息。

5、权利要求 4 的方法，其特征在于：接收交易卡用户信息包括从交易卡用户接收信息。

6、权利要求 5 的方法，其特征在于：接收交易卡用户信息进一步包括在耦合到交易卡发卡人的服务器的一个计算设备上接收信息。

7、 权利要求 6 的方法，其特征在于：接收交易卡用户信息进一步包括通过交易卡发卡人的服务器以加密形式接收信息。

8、权利要求 6 的方法，其特征在于：接收交易卡用户信息进一步包括在一个全球网络上耦合到交易卡发卡人的服务器的一个计算设备上接收信息。

9、权利要求 6 的方法，其特征在于：计算设备进一步包括一个个人计算机。

10、权利要求 9 的方法，其特征在于：计算设备进一步包括一个个人计算机的电子钱包应用。

11、权利要求 6 的方法，其特征在于：接收交易卡用户信息进一步包括接收交易卡用户的个人识别符、口令、生物样品、数字签字、和交易卡号中的至少一个。

12、权利要求 1 的方法，其特征在于：交易卡用户的鉴别进一步还包括在一个本地的计算设备上鉴别交易卡用户。

13、权利要求 12 的方法，其特征在于：本地计算设备进一步包括个人计算机、个人数字助手、和袖珍卡之一。

14、权利要求 12 的方法，其特征在于：交易卡用户的鉴别进一步还包括通过在一个本地的计算设备上的一个操作鉴别交易卡用户。

15、权利要求 14 的方法，其特征在于：本地计算设备的操作进一步包括电子钱包操作。

16、权利要求 12 的方法，其特征在于：交易卡用户的鉴别进一步还包括通过在本地的计算设备上的操作来接收交易卡用户信息。

17、权利要求 16 的方法，其特征在于：交易卡用户信息进一步包括交易卡用户的个人识别符、口令、生物样品、数字签字、和交易卡号中的至少一个。

18、权利要求 1 的方法，其特征在于：产生匿名卡号进一步包括由交易卡发卡人产生匿名卡号。

19、权利要求 18 的方法，其特征在于：产生匿名卡号进一步包括由交易卡发卡人的服务器产生匿名卡号。

20、权利要求 1 的方法，其特征在于::：产生匿名卡号进一步包括由交易卡发卡人的服务器的一个号码发生器产生匿名卡号。

21、权利要求 1 的方法，其特征在于：产生匿名卡号进一步包括在本地计算设备上产生匿名卡号。

22、权利要求 21 的方法，其特征在于：产生匿名卡号进一步包括通过对本地计算设备进行号码发生操作产生匿名卡号。

23、权利要求 22 的方法，其特征在于::：产生匿名卡号进一步包括通过对本地计算设备进行与交易卡发卡人的号码发生器同步的号码发生操作产生匿名卡号。

24、权利要求 1 的方法，其特征在于：产生匿名卡号进一步包括按照预先确定的参数产生匿名卡号，所说的预先确定的参数限制了除该交易卡用户的交易外的匿名卡号的应用。

25、权利要求 1 的方法，其特征在于：产生匿名卡号进一步包括按照预先确定的参数产生匿名卡号，所说的预先确定的参数限制

了在预定时间周期外的匿名卡号的使用。

26、权利要求 1 的方法，其特征在于：产生匿名卡号进一步包括按照一个预先选定的号码发生方案产生匿名卡号，所说预先选定的号码发生方案是从下述方案中选择出来的：随机数发生算法、随机序列发生程序、和安全散列算法。

27、权利要求 1 的方法，其特征在于：关联匿名卡号进一步包括通过交易卡发卡人关联匿名卡号与交易卡用户的交易卡号。

28、权利要求 27 的方法，其特征在于：关联匿名卡号进一步包括通过交易卡发卡人的服务器关联匿名卡号与交易卡用户的交易卡号。

29、权利要求 28 的方法，其特征在于：关联匿名卡号进一步包括通过交易卡发卡人的服务器的一个号码发生器链接匿名卡号与交易卡用户的交易卡号。

30、权利要求 29 的方法，其特征在于：关联匿名卡号进一步包括通过交易卡发卡人的服务器的一个核准处理器链接匿名卡号与交易卡用户的交易卡号。

31、权利要求 1 的方法，其特征在于：关联匿名卡号进一步包括按照与一个本地计算设备的号码发生器同步的预先确定的序列链接匿名卡号与交易卡用户的交易卡号。

32、权利要求 31 的方法，其特征在于：关联匿名卡号进一步包括通过交易卡发卡人的服务器链接匿名卡号与交易卡用户的交易卡

号。

33、权利要求 1 的方法，其特征在于：核准交易包括由交易卡发卡人核准交易。

34、权利要求 33 的方法，其特征在于：核准交易进一步包括由交易卡发卡人的一个核准处理器核准交易。

35、权利要求 1 的方法，其特征在于：核准交易进一步包括接收链接到交易卡用户的交易卡号的匿名卡号。

36、权利要求 1 的方法，其特征在于：核准交易进一包括向一个商家发送用于交易卡用户的带有匿名卡号的核准。

37、交易卡用户完成一次交易的系统，包括：

鉴别交易卡用户的装置；

产生交易卡用户的一个匿名卡号的装置；

使交易卡用户的匿名卡号与一个交易卡号相关联的装置；

用交易卡用户的匿名卡号核准交易的装置。

38、权利要求 37 的系统，其特征在于：交易卡用户的鉴别装置进一步还包括交易卡发卡人的服务器。

39、权利要求 38 的系统，其特征在于：交易卡用户的鉴别装置进一步还包括一个耦合到交易卡发卡人的服务器的计算设备，用于接收交易卡用户信息。

40、权利要求 39 的系统，其特征在于：交易卡用户的鉴别装置

进一步还包括至少一个计算设备和用于加密交易卡用户信息交易卡发卡人的服务器。

41、权利要求 40 的系统，其特征在于：还包括在一个在全球网络上耦合到交易卡发卡人的服务器的计算设备。

42、权利要求 41 的系统，其特征在于：计算设备进一步包括个人计算机。

43、权利要求 42 的系统，其特征在于：计算设备进一步包括个人计算机的电子钱包操作。

44、权利要求 42 的系统，其特征在于：交易卡用户信息进一步包括接收交易卡用户的个人识别符、口令、生物样品、数字签字、和交易卡号中的至少一个。

45、权利要求 37 的系统，其特征在于：交易卡用户的鉴别装置进一步还包括一个本地计算设备。

46、权利要求 45 的系统，其特征在于：本地计算设备进一步包括个人计算机、个人数字助手、和袖珍卡之一。

47、权利要求 46 的系统，其特征在于：交易卡用户的鉴别装置进一步还包括在本地计算设备上的一个操作。

48、权利要求 47 的系统，其特征在于:：交易卡用户的鉴别装置进一步还包括在本地计算设备上的一个电子钱包操作。

49、权利要求 45 的系统，其特征在于：交易卡用户的鉴别装置

进一步还包括本地计算设备的一个输入设备，用于通过在本地计算设备上的一个操作接收交易卡用户信息。

50、权利要求 49 的系统，其特征在于：交易卡用户信息进一步包括接收交易卡用户的个人识别符、口令、生物样品、数字签字、和交易卡号中的至少一个。

51、权利要求 37 的系统，其特征在于：用于产生匿名卡号的装置进一步包括交易卡发卡人的服务器。

52、权利要求 51 的系统，其特征在于：用于产生匿名卡号的装置进一步包括交易卡发卡人的服务器的一个号码发生器。

53、权利要求 37 的系统，其特征在于：用于产生匿名卡号的装置进一步包括一个本地计算设备。

54、权利要求 53 的系统，其特征在于：用于产生匿名卡号的装置进一步包括对本地计算设备进行的一个号码发生操作。

55、权利要求 54 的系统，其特征在于：用于产生匿名卡号的装置进一步包括对本地计算设备进行的与交易卡发卡人的一个号码发生器同步的一个号码发生操作。

56、权利要求 37 的系统，其特征在于：用于产生匿名卡号的装置进一步包括按照预先确定的参数产生匿名卡号的装置，这些预先确定的参数限制了除该交易卡用户的交易外的匿名卡号的用户。

57、权利要求 37 的系统，其特征在于：用于产生匿名卡号的装置进一步包括按照预先确定的参数产生匿名卡号的装置，这些预先

确定的参数限制了预定时间周期以外的匿名卡号的使用。

58、权利要求 37 的系统，其特征在于：产生匿名卡号进一步包括按照一个预先选定的号码发生方案产生匿名卡号，所说预先选定的号码发生方案是从下述方案中选择出来的：随机数发生算法、随机序列发生程序、和安全散列算法。

59、权利要求 37 的系统，其特征在于：用于关联匿名卡号的装置进一步包括交易卡发卡人的服务器。

60、权利要求 59 的系统，其特征在于：用于关联匿名卡号的装置进一步包括交易卡发卡人的服务器的一个号码发生器。

61、权利要求 60 的系统，其特征在于：用于关联匿名卡号的装置进一步包括交易卡发卡人的服务器的一个核准处理器。

62、权利要求 37 的系统，其特征在于：用于关联匿名卡号的装置进一步包括按照与本地计算设备的一个号码发生器同步的预定序列的交易卡发卡人的服务器的一个号码发生器。

63、权利要求 37 的系统，其特征在于：用于核准交易的装置进一步包括交易卡发卡人的服务器。

64、权利要求 63 的系统，其特征在于：用于核准交易的装置进一步包括交易卡发卡人的服务器的一个核准处理器。

65、权利要求 37 的系统，其特征在于：用于核准交易的装置进一步包括向交易卡用户的商家发送用于交易的具有匿名卡号的核准的装置。

说　明　书

用于实现银行卡交易的方法和系统

本发明一般来说涉及银行卡交易领域，具体来说涉及利用一个匿名或替换卡号可靠地实现银行卡交易的方法和系统。

例如，通常一个持卡人利用可获得的标准通用网络浏览器和服务器能力（如 Swcure Sockets Layer(SSL)）在一个加密的链路上向商家服务器发送他或她的信用卡号或借方卡号，从而完成交易卡交易，这种交易在今天是发生在因特网上,其中利用了交易卡的基础结构。持卡人和商家之间的链路必须加密，以防止卡号被未经允许的第三方截获或欺骗读出。这种类型的欺诈行为有时称之为中间人员侵袭(the man-in-the-middle-attack)。链路要加密，以使窃听者听不到和偷不到卡号。然而，这种方法有一系列缺点。

例如，持卡人必须信任商家能够保护他的卡号。这就有可能使持卡人容易受到商家、或商家的雇员的欺作，或者有可能受到虽然诚实但在维持商家的网站不受侵袭方面有疏漏的商家的欺诈。这种风险的可能性是很大的，使消费者不敢在因特网上把他们的卡号交给他们不了解的或者他们无事前经验的商家的站点。

对于信用卡或借方卡，消费者保护法和相关规则将特殊的风险限制在一个最大的额度，如 50 美元的限制。此外，例如持有一个信用卡的持卡人在从他的帐目实际扣除之前有一个付款争辩的机会。

然而，这仍旧是很麻烦的，并且还有风险，而且一旦出现欺诈，就必须给持卡人放一个新卡和卡号。这种风险对于借方卡（debit card）就更大，因为债务的限制不会那么清楚，并且费用在通知他或她之前就已经从持卡人的帐目上扣除了。于是，持有借方卡的持卡人总是处在必须争辩扣除的位置，以便重新拿回他或她的已丢失的资金。

另一个缺点例如是，当商家在因特网（Internet）上从一个消费者那里接收一个卡号时，商家无法核实购买货物的消费者是否是实际的持卡人。这种交易作为邮寄订单／电话订单（MOTO）处理，也称之为“无卡交易“。在这样一种交易中，商家的交易成本和EXPOSURE 要比在销售点有顾客实际存在时大得多。如果对于已经进行的交易顾客的争辩成功，则发卡人要收回对商家的支付。

从持卡人和商家这两个方面的观点出发，这些缺点促使人们改进银行卡交易的安全性，这种交易还要快速、简单、和廉价。为解决这一需要，已经提出许多解决方案，最引人注意的是“信用卡协会"的标准规定“安全电子交易（SET）“协议。诸如 SET 之类的解决方案存在的问题是，它们明显增加了费用和性能方面的负担，要求持卡人和商家两者都要安装特殊的软件和硬件，这在金钱和时间这两方面明显增加了交易成本。

本发明的一个特征和优点是提供一种用于安全地完成银行卡交易的方法和系统，它使所有的帐号符合 SET 协议的安全性，并且能够鉴别顾客，同时还能保持在一个加密的链路上（如 SSL）发送交易卡号的简单性。

本发明的另一个特征和优点是提供一种用于安全地完成银行卡交易的方法和系统，它不再需要在因特网上向商家发送顾客的实际卡号，类似地也不再需要在顾客和商家之间的安全链路。

本发明的又一个特征和优点是提供一种用于安全地完成银行卡交易的方法和系统，例如信用卡或借方卡交易，这种交易是快速的并且容易实现，并且几乎不需要修改现存的因特网基础结构。

为了实现所述的和其它的特征、优点、和目的，本发明的一个实施例提供一种用于安全地完成银行卡交易的方法和系统，其中交易卡用户接收的是一个替换或匿名卡号，这不是用户的实际卡号，而是被设计用来例如通过由商家或商家银行进行的任何真实性检查的卡号。替换或匿名卡号只能在有限的时期内使用一次，不可能被复制或替换。交易卡发卡人一收到替换或匿名卡号，替换或匿名卡号就和真正的持卡人的发卡人相关联，从而核准持卡人的帐目。

在本发明的一个实施例中，交易卡用户向例如交易卡发卡人的服务器的一个鉴别器鉴别他或她自已。交易卡用户例如通过在一个计算设备上输入交易卡用户信息来鉴别（ authenticate ）他或她自已，所说的计算设备例如是个人计算机、个人数字助手、或袖珍卡，它们在一个网络上（如因特网）连到发卡人的服务器上。

此外，在本发明的一个实施例中，交易卡用户可利用计算设备的电子钱包操作，向交易卡用户的服务器发送交易卡用户信息以便进行用户确认。交易卡用户信息例如包括：一个或多个个人识别号、

口令、生物样品（biometric sample）、用于交易卡用户的数字签名或交易卡号，并且可对交易卡用户信息进行加密。

在本发明的一个实施例的另一方面，交易卡用户利用交易卡用户信息在本地的计算设备上核准他或她自己，所说的计算设备例如是个人计算机、个人数字助手、或交易卡用户的一个袖珍卡。就此而论，交易卡用户是在操作交易卡用户的本地计算设备（例如电子钱包操作） 中，通过在操作中在本地计算设备中输入交易卡用户信息，核准他或她自己。

在本发明的一个实施例中，当交易卡用户由交易卡发卡人核准时，交易卡发卡人的服务器的一个号码发生器就为交易卡用户产生一个匿名卡号。但在本发明的另一方面，即交易卡用户是在操作交易卡用户的本地的计算设备中核准他或她自己的，例如通过与交易卡发卡人的服务器的号码发生器同步的本地计算设备的一个号码产生操作，在本地计算设备上以类似的方式产生匿名卡号。

按照一种号码产生方案，例如随机号码产生算法、随机序列发生器、和／或安全散列算法（secure-hashing algorithm），可产生用于本发明的一个实施例的匿名卡号。此外，按照一些预定的参数来产生匿名卡号，这些参数可限制它对特定交易的使用和／或用于预定的时间周期。

在本发明的一个实施例中，例如通过用交易卡发卡人的服务器的号码发生器和核准处理器之一或两者链接匿名卡号和交易卡号，

可以使由交易卡发卡人产生的匿名卡号与交易卡用户的交易卡号相关联。

然而，按本发明的另一方面，即其中的匿名卡号是在交易卡用户的本地计算设备产生的，匿名卡号是按照本地计算设备的号码发生器和交易卡发卡人的服务器之间的预定的序列同步状态而与交易卡号链接的。

在本发明的一个实施例中，匿名或替换卡号在交易中是由交易卡用户使用的，以替换交易卡用户的交易卡号。例如，交易卡用户向一个商家发送这个匿名卡号，商家又将这个卡号发送到商家银行请求核准。商家银行在卡联盟网络（card association network）上向交易卡发卡人发送这个匿名卡号。交易卡发卡人的核准处理器接收与交易卡号链接的匿名卡号，并且经卡联盟网络和商家银行向商家发送回去一个核准。

在本发明的另一个实施例中，在核准用户后匿名或替换卡号在交易中由交易卡发卡人使用。例如，交易卡用户向发卡银行核准他自己，并且发卡银行直接向商家发送匿名卡号，商家又向商家银行发送这个匿名卡号请求核准。

在本发明的另一个实施例中，交易卡用户向交易卡发卡人核准他自己，并且交易卡发卡人直接向商家发送这个匿名卡号和一个核准，商家则又向商家银行发送这个匿名卡号和核准这两者以便核实和处理。交易卡用户使用实际的交易卡号和替换卡号这两者记帐并

传达到它的交易卡用户，并且利用替换卡号和核准与商家银行和卡的处理网络结帐。

在下面的描述中部分地提出本发明的附加目的、优点、和新颖特征，在研究了下面的叙述的并且通过本发明的实践学习，本领域的普通技术人员将会更加明白本发明的这些附加目的、优点、和新颖特征。

图 1 是一个示意图，表示关键部件实例的略图和用于本发明的一个实施例的关键部件之间的信息流，在该实施例中由发卡人向一个持卡人发送一个匿名或替换卡号，用于在线银行卡交易；

图 2 是一个流程图，表示持卡人使用匿名或替换卡号完成一次银行卡交易的用于本发明的方法的例子，所说的匿名或替换卡号是由发卡人发送给持卡人的；

图 3 是一个示意图，表示关键部件实例的略图和用于本发明的一个实施例的关键部件之间的信息流，其中匿名或替换卡号是在用于在线银行卡交易的持卡人的计算设备上产生的；

图 4 是一个流程图，表示持卡人使用匿名或替换卡号完成一次银行卡交易的用于本发明的方法的例子，所说的匿名或替换卡号是由持卡人的计算设备产生的；

图 5 是一个示意图，表示关键部件实例的略图和用于本发明的一个实施例的关键部件之间的信息流，其中匿名或替换卡号是在用于持卡人的销售点产生的；

图 6 是一个示意图，表示用于产生本发明的一个实施例的匿名或替换卡号的一个线性反馈移位寄存器的样板。

现在详细参照本发明的一个实施例，在附图中表示的是实施例的一个例子，图 1 是一个示意图，表示关键部件实例的略图和用于本发明的一个实施例的关键部件之间的信息流，其中由发卡人向一个持卡人发送一个匿名或替换卡号，用于在线银行卡交易。本发明的这个实施例涉及一系列实体，例如持卡人 2、商家 4、商家（获取）银行 6、和发卡人 8。本发明的这个实施例还利用例如计算机的硬件和软件，例如持卡人的计算设备 10、商家的网站服务器 12、和发卡人服务器 14，它们中的每一个都耦合到一个网络上，例如因特网 16，并且商家（获取）银行服务器 18 耦合到商家服务器 12 上并且通过一个卡联盟网络 20 耦合到发卡银行服务器 14。此外，发卡人服务器例如包括一个鉴别器 22、一个替换卡号发生器 24、和一个核准处理器 26。

在本发明的一个实施例中，持卡人 2 从持卡人的发卡银行接收一个替换卡号（在这里，或者称之为匿名卡号，或者称之为“替换卡号”），这个卡号不是持卡人的实际卡号。在持卡人 2 直接向持卡人的发卡人 8 核准他或她自己后，发出这个匿名或替换卡号。这个匿名卡号只在一个有限的时间周期使用一次。将这个卡号设计成能通过商家 4 和商家银行 6 进行的任何有效性检查，并且不可能被复制或再用。在收到匿名卡号以便核准时，匿名卡号可能通过发卡银行 8 与真正的持卡人 2 和持卡人帐目相关联，并且可能被核准。

图 2 是一个流程图，表示用户 2 使用匿名或替换卡号完成一次银行卡交易的用于本发明的方法的例子，所说的匿名或替换卡号是由发卡人 8 发送给持卡人 2 的。在 S1，商家服务器 12 在因特网 16 上向用户 2 的用户计算设备 10 发出一个请求，要求一个和用户 2 的在线交易有关的交易卡号。在 S2，用户 2 在用户计算设备 10 上接收这个请求，并且在因特网 16 上向发卡人服务器 14 发送一个请求，借求一个替换卡号。在 S3，发卡人的鉴别器 22 接收这个请求，鉴别用户 2 并获得一个替换卡号 — 这个替换卡号从发卡人的号码发生器 24 链接到用户的实际卡号，并且在因特网 16 上向用户 2 的用户计算设备 10 发送这个替换卡号。在 S4，在用户计算设备 10 的用户 2 在因特网 16 上向商家服务器 12 发送这个替换卡号。

进一步参照附图 2，在本发明的一个实施例中，在 S5，商家服务器 12 接收并向商家银行（获取）服务器 18 发送替换卡号和核准请求。在 S6，商家（获取）银行服务器 18 接收这个核准的请求，并且在卡联盟网络上向发卡人服务器 14 发送有关替换卡号的请求。在 S7，发卡人的核准处理器 26 接收这个核准请求，链接替换卡号到用户的实际帐目以便核准，并且在卡联盟网络 20 上向商家（获取）银行服务器 18 发送这个替换卡号的核准。在 S8，商家（获取）银行服务器 18 接收这个核准，并且将它发送到商家服务器 12。在 S9，商家服务器 12 接收这个核准，并且完成与用户 2 的这次交易。

再次参照附图 2，在本发明的一个实施例中，持卡人 2 在 S2 在一个安全（加密）线路上，利用例如如图 1 所示的电子钱包，向发

卡银行 8 在线核准他或她自己。在鉴别持卡人 2 时，他或她在 S3 在同一线上接收这个匿名卡号。按另一种方式，在 S3，持卡人 2 可以使匿名卡号由发卡人 8 直接向商家 4 发送，在这种情况下，持卡人 2 没有必要在 S4 向商家 4 发送这个匿名卡号。

再次参照附图 2，在本发明的一个实施例中，持卡人 2 通过在用户计算设备 10 上键入他或她的卡号和一个密秘的 PIN（个人身份识别码）或口令、或者 PIN 的散列或口令，并且在 S2 阶段在一个加密的链路上将其送到发卡银行 8，就可以向这个持卡人的发卡银行 8 核准他或她自己。这个加密的链路要能保证绝不会有任何一个第三方可以窃听到或者偷到这个卡号或 PIN。持卡人 2 可能会感觉到发卡银行是安全的，因为发卡银行已经知道并且保护了这个信息。因为持卡人 2 用 PIN 或口令核准了他或她自己，所以发卡银行 8 能够向商家服务器 12 鉴别持卡人 2。如果交易或者顾客的历史，则发卡银行 8 可能要求更安全的鉴别，如附加的密码、匹配的生物统计特性、和 / 或数字签名。

按本发明的一个实施例的另一方面，发卡银行 8 可能在持卡人的个人计算机或信息设备 10（如袖珍卡或个人数字助手（PDA）型计算设备）上安装软件，这可能在持卡人 2 向软件和 / 或设备 10 识别他或她自己后产生匿名卡号。图 3 是一个示意图，表示关键部件实例的略图和用于本发明的一个实施例的关键部件之间的信息流，其中匿名卡号是在在线交易的持卡人的计算设备 10 上产生的。就此而论，发卡人 8 可在持卡人的计算设备 10 上安装软件 30，计算设

备 10 可能是一个个人计算机（PC）或硬件令牌（ to ken ），如袖珍卡，它根据持卡人 2 的鉴别就地产生匿名卡号。

图 4 是一个流程图，表示用户 2 完成一次银行卡交易的用于本发明的方法的例子，其中匿名卡号是由持卡人的计算设备 10 产生的。现在参照附图 4，在 S10，商家服务器 12 在因特网 16 上向持卡人 2 的持卡人计算设备 10 发出一个交易卡号请求。在 S11，持卡人 2 在持卡人计算设备 10 上接收这个请求，并且在持卡人的计算设备 10 上的号码发生软件 30 产生并且向商家服务器 12 发送一个替换卡号。在 S12，商家服务器 12 接收这个替换卡号，并且向商家（获取）银行服务器 18 发送带有替换卡号的鉴别请求。

进一步参照附图 4，在本发明的这个实施例中，在 S13，商家（获取）银行服务器 18 接收这个请求并在卡联盟网络 20 上向发卡人服务器 14 发送这个请求。在 S14，发卡人的替换卡号发生器 24 接收这个请求，产生和持卡人的软件 30 同步的序列中的下一个号码，把该替换卡号链接到持卡人的实际卡号，并且向发卡人的核准处理器 26 发送持卡人的实际卡号。在 S15，发卡人的核准处理器 26 接收持卡人的实际卡号，并且在卡联盟网络 20 上向商家（获取）银行服务器 18 发送核准。在 S16，商家（获取）银行服务器 18 接收这个核准，并且将这个核准发送到商家服务器 12。在 S17，商家服务器 12 接收这个核准并且完成与用户 2 的交易。

按本发明的一个实施例的另一个方面，发卡人 8（如一个银行）提供一个电子钱包系统，它包括例如一个电子钱包服务器。就此而

论，发卡行 8 将使匿名卡号与实际用户帐目一致。如果电子钱包为持卡人 2 产生一个匿名卡号，并且对于持卡人 2 来说电子钱包服务器不是发卡银行，那么，匿名卡号要被送回到电子钱包服务器，以使匿名或替换卡号与实际用户卡号一致，并且将其发送到发卡银行 8 以便核准。在这种情况下，电子钱包实际上完成的是获取银行功能。

本发明的一个实施的另一方面允许持卡人 2 在一个实际的销售点完成交易而不泄漏持卡人的真正卡号。图 5 是一个示意图，表示关键部件实例和用于本发明的一个实施例的一个方面的关键部件之间的信息流，其中替换卡号是在完成银行卡交易的销售点产生的。本发明的这一方面利用例如一个卡 32，卡 32 没有任何模压的号码，但有一个输入设备 34（如一个键盘）、一个显示器 36（如液晶显示器（LCD））、和一个磁条 38，磁条 38 的记录内容可由卡内的一个内部微处理器 40 改变。本发明的这一方面利用了耦合到商家（获取）银行服务器 18 的一个销售点卡设备 42，商家（获取）银行服务器 18 在卡联盟网络 20 上耦合到发卡人服务器 14。

参照附图 5，按照本发明的一个实施例的用户 2 完成一次销售点银行卡交易的方法，用户 2 向输入设备 34（如键盘）输入一个口令，或者按另一种方式，用户 2 向输入设备 34（如生物特性输入设备）输入一个生物特性（如指纹）。在向输入设备 34 输入了正确的口令或生物特性后，在 LCD36 上显示匿名卡号，作为卡号，并且当卡 32 沉入卡设备 42 中时，磁条 38 输出这个匿名卡号。销售点银行

卡交易的其它部分类似于如图 4 所示的用户 2 完成在用户的计算设备 10 上产生匿名卡号的在线银行卡交易。

另外，在本发明的一个实施例的上述方面，当卡 32 沉入卡设备 42 中时，可能产生持卡人的实际卡号，但显示器 36 显示的是匿名卡号。在这种情况下，有欺诈行为的商家不可能读出持卡人的实际卡号。一旦在销售点手动输入这个匿名卡号，所显示的这个匿名卡号也只能一次性使用，这个卡号不可能复制和重复使用。在这种情况下，有欺诈行为的商家可能用欺诈手段通过刮擦磁条 38 获得持卡人的实际卡号，但可以改变磁条 38 的性质使刮擦和复制磁条很困难。同样的方法也可以用于例如电话订单，其中，在用户激励和鉴别后，持卡人的设备 10 通过电话系统向商家 4 发送一个替换卡号。

按照本发明的一个实施例，被规定为一次性使用的匿名卡号因为所有的所需数字都在正确的位置，所以可以通过由商家 4 和商家银行 6 进行的真实性检查。匿名卡号还有正确顺序的数字，从而可保证向正确的银行 8 发送这个交易，以便得到鉴别和核准的认同。当发卡银行 8 接收这个号码并且请求付给核准费用时，发卡银行 8 就将这个匿名卡号发送到一个特定的前端处理器 24。处理器 24 可以作为一个单独的硬件处理器实施，或者可以简单地例如是一个软件模块，这个模块也一起定位在主核准处理器 26 中。

用于本发明的一个实施例的前端处理器 24 维持在实际卡号和产生和匿名卡号之间的链接，并且维持这种链接有效的时间范围。如果这两个卡号一致，并且这个匿名卡号还没被使用或过期，那么就

用实际卡号去代表匿名卡号，并且将其发送到正常卡处理的核准系统 26。因此，核准了请求的交易费用，并且通过持卡人的发卡银行 8 将这个费用链接到持卡人的帐目，其条件是匿名卡号和由发卡银行 8 或它的硬件和／或软件提供的卡号一致并且这个卡号还没有使用过或者还没有过期。

在本发明的一个实施例中，如果交易被拒绝，持卡人 2 必须去例如持卡人的发卡银行的网站，并且请求一个新的匿名卡号。随机选择的匿名卡号只一次有效，且直到第一个随机指定的卡号被用过或到期，才会指定一个新的随机选择的卡号。提供给顾客 2 的接收必须显示匿名卡号和交易的时间。发卡银行 8 维持匿名卡号并且维持这些匿名卡号和真正帐号及交易的时间同日期的链接，从而能对顾客 2 提出争辩的交易进行调查研究。

在用于本发明的一个实施例的方法和设备的实施过程中，匿名或替换卡号不是持卡人的实际卡号。发卡银行在一个限定的时期内（例如 15—30 分钟）一次性使用地连接这个匿名卡号和持卡人的实际卡号。通过在持卡人的卡号的选定位置用新的匿名卡号代替实际卡号，从而可产生匿名卡号。

有许多方法都可产生用于本发明的实施例的匿名卡号。匿名卡号的产生涉及到例如使用一个随机数产生方案，这个方案有一个附加的要求，即在同一个时间周期期间相同的数不可能对多于一次的交易有效。随机数的产生时间和特定的随机数有关，并且该随机数和一个固定的时间有关，在这个固定的时间里该数能和持卡人 2 相

关联。

用于本发明的一个实施例的被指定的匿名或替换卡号可以包括例如 9—11 位数字。例如，用于发卡人识别符的 ISO7812“识别卡一编号系统和登记过程“规定：一个有效的卡号由一个银行识别号、加上一个单个帐识别符、再加上一个检查数字构成。银行识别号（BIN）是卡号的头 4 位或头 6 位，用于确定到正确的银行（如发卡人 8）的路线。单个帐识别符是由发卡单位 8 指定的一个个人的或单位的号码，用于识别单个帐目。检查数字是由卡号的其余的位计算的一个校验和。

最普通的发出的信用卡号包括 16 位。例如，用于金融机构（如发卡银行 8）的一个有效的信用卡号可以是 AAAAAA XXXXXXXXX C，其中 AAAAAA 代表 BIN,并且是固定的，XXXXXXXXX 是 9 个任意指定的位，C 代表校验和，并且是从其它位计算出来的。于是，发卡人 8 可以任意设定 16 位中的任意 9 或 11 位为一次性使用的任意的卡号，调节校验和它的新的正确值，通过商家 4 和商家银行 6 的核实系统可检查卡号的有效性。期望采用这个方案的银行必须获得一个新的 BIN，以便专门用于因特网交易。这就不再需要防止发出一次性使用的卡号，所说的一次性使用的卡号是现行的卡号或热卡号。

按另一种方式，在本发明的一个实施例中，银行（如发卡银行 8）使用现行的 BIN 的方法是在一个或多个特定的位置保留一个或多个特殊的数字，以识别这个卡号就是匿名卡号，例如 AAAAAA S

XXXXXXXXX C，其中的 S 就是在第 7 个指定位置的特殊符号。如果已经存在的读出的卡号在第 7 位置有符号 S，那么就不可能使用这些号作为匿名卡号，它们作为有效的匿名卡号必然被匿名卡号发生器拒绝。在这种情况下，银行只有 8 或 10 位可用来指定匿名卡号。如果修改卡的相关标准以便可允许较长的位流，或者相关的金融机构同意接收这些较长的位流，就可以产生较长的卡号。

在本发明的一个实施例中，被指定的一次性使用的匿名卡号因为它的所有的被请求的位都在合适的位置，所以可以通过由商家 4 和商家银行 6 进行的核实。因为 BIN 是正确的，所以这个卡号被传送到正确的发卡银行 8。匿名卡号通过持卡人的发卡银行 8 与持卡人的实际卡号正确地相关联，条件只是这个匿名卡号还没有传送过或没有过期。持卡人的发卡银行 8 用持卡人的实际卡号替换匿名卡号，并且传送这个卡号以进行正常的核准。

在本发明的一个实施例中，如果交易因为匿名卡号没通过一致性检验而被拒绝时，持卡人 2 必须去到持卡人的发卡银行 8 的网站，请求一个新的卡号。被指定的匿名卡号只适用于一次核实。直到第一个卡号用过或过期，才能颁发新卡。返回到商家的任何响应只有匿名卡号。

按照本发明的一个实施例的一个方面，在发卡银行服务器 14 产生匿名或替换卡号，这个匿名或替换卡号或者直接发送到商家 4，或者发送到持卡人的 PC 或令牌 10，以便转发到商家 4。然而，在本发明的一个实施例的另一个方面，匿名卡号可在持卡人的 PC 或

硬件设备 10（如袖珍卡、个人数字助手（PDA）型设备、或安全动力型卡）本地产生。本地／客户软件可从发卡银行服务器 8 下载，或者安装这种软件。

按本发明的一个实施例，如果顾客 2 或顾客的电子钱包 28 例如在它和商家 4 的交易没有收到或收到但被窜改的情况下被要求重新提交替换卡号，则除非期满都要重新提交这个替换卡号。如果期满，则要产生和发送新的替换卡号。如果核准完成初次提交该替换卡号，则如果替换卡号相同，这个替换卡号就不可能被认为是一个重复的收费，因为对于相同的替换卡号的同一数量存在两个费用。如果商家 4 发送一个新的替换卡号，那么顾客 2 和他或她的发卡银行 8 将会认识它，因为顾客的信用卡说明将会反映出对于顾客的实际卡号的两次收费问题，顾客的实际卡号两次正确地代替了替换卡号。

在本发明的一个实施例中，如果商家 4 收到了替换卡号，但商家银行 6 要求商家 4 重新提交，或者如果信用卡网络 20 要求商家银行 6 重新提交，则要重新提交初始的替换卡号，而不管这个替换卡号是否已经过期。如果替换卡号已经过期，这个交易将不被同意，并且请求顾客 2 或顾客的电子钱包 28 发送一个新的替换卡号，结果顾客 2 或顾客的电子钱包 28 就发送了一个新的替换卡号。如果到达发卡银行要求核准时替换卡号已经过期，则核准被拒绝，顾客 2 和顾客的电子钱包 28 必须重新提交。

在本发明的一个实施例中，如果卡网络 20 因为发卡银行 8 的核准要花费太长的时间而顶替（stand – in），发卡银行 8 则认为这笔

费用是有效的，就像在任何其它顶替情况一样。发卡银行 8 知道和这笔费用有关的实际卡号，因为发卡银行 8 可能匹配替换卡号与实际卡号。

按照本发明的一个实施例，为了处理任何争端，发卡银行要维持一个记录，记录下数量、替换卡号、和实际卡号。商家 4 可以跟踪针对替换卡号的销售，顾客 2 可以跟踪他或她经过顾客的实际卡号进行的购买。发卡银行 8 可以使这两者发生关联或相互匹配，因为发卡银行 8 有一个替换卡号的挡案，而替换卡号是和交易的实际卡号相关的。如果替换卡号用于两次交易，发卡银行 8 也可以观察到这种情况。事实上，如果企图对于两个不同的费用两次使用同一个替换卡号，发卡银行 8 将拒绝第二次尝试。

按本发明的一个实施例，有几种不同的方法都可产生匿名卡号。例如，匿名卡号可在固定的时间间隔或在每个新的请求事件时连续地产生。实现这种情况可以有一系列方法，例如安全动态算法、随机序列发生方法、和安全散列算法。如果指定匿名或替换卡号序列的发卡银行（如发卡人 8）是核实它的同一个银行，则不需要同步时钟。

按照本发明的一个实施例，如果产生了一个已经指定的但还没有过期的号码，就不要再产生这个号码了，而要产生新的号码。截止期越短，并且在指定的序列中的位数越多，则号码发生冲突的可能性就越小。对匿名卡号发生算法进行设计，以便只发出新的卡号，这些新的卡号不和已经发出的并且没有过期的卡号或已经发出的实

际卡号冲突。这就是说，要对这种算法进行设计，以便可以防止发生卡号冲突，并且当冲突的确发生时能够在可接受的延迟时间内（例如不超过几秒）产生新的卡号。

另外，按照本发明的一个实施例，发卡银行能够并行地操作一系列匿名卡号，因此如果一个这样的发生器产生一个复制的卡号，则不可能从其它的号码发生器之一产生这个复制的卡号，或者可以预先产生一批替换卡号，可从这批卡号中选择下一个替换卡号。在本发明的一个实施例中，可使用单个共用卡号发生器服务于所有的持卡人的请求，或者对于每个有效的持卡人或者对于整个持卡人人群的某个分组指定一个不同卡号发生器。

按照本发明的一个实施例，截止间隔不是那样地短，因此在期满前持卡人 2 有时间向商家 4 发送这个序列、处理这个序列、并且再通过商家银行 6 返回到发卡银行 8。为此目的，截止间隔例如至少约为 15 分钟，但截止间隔是可以调节的，以适应于不同的应用场合和情况。如果每秒指定一个新卡号序列，那么每 15 分钟必须产生 900 个序列，一个典型的序列的长度是 9－11 位。对一个 9 位的号码发生器进行设计，使其在重复前可产生 10^9 个不重复的序列，保证在产生 900 个序列的 15 分钟的间隔内不产生重复的序列。

本发明的一个实施例利用了一系列替换卡号产生算法中的任何一个。例如，“线性同余生成程序（Lineur Congruential Generators）”是伪随机生成程序，具有如下形式：

$$Xn=(aXn1+b)\ 模\ m$$

其中 Xn 是序列的第 n 个卡号，Xn1 是该序列的前的卡号，a、b、m 是常数，其中 a 称之为乘数，b 称之为增量，m 称之为模数。当合理地选择 a、b、m 时，它们可以产生一个最大长度的伪随机序列，在它们自已重复之前的周期为 m。线性同余生成程序是快速算法，但线性同余生成程序的输出不是加密安全的。换言之，在一个实际的时间里，一个加密员可以通过检查序列中过去的卡号确定该序列的下一个卡号。因此，这种算法容易受到侵袭。

然而，就用于本发明的一个实施例的算法而论，一个窃听者不可能获得在加密的线上发送的过去的卡号。在这种情况下，窃听者必须在商家服务器上收集这些卡号，并且在特定的商家这些卡号不可能是按照一定的顺序的，因为购货者经常按一个相当随机的顺序往来于许多商家。从多个用来向多个持卡人提供卡号的可替换卡号发生器选择替换卡号，就可防止持卡人收集到一系列替换卡号。这就减小了单个窃听者从单个匿名卡号发生器捕获匿名卡号的足够长的序列以进行反向操纵的可能性。

“线性反馈移位寄存器”也可以用来产生用于本发明的一个实施例的卡号的伪随机序列，并且可被设计成具有最大的长度。图 6 是一个示意图，表示用于产生本发明的一个实施例的匿名或替换卡号的一个线性反馈移位寄存器的样板。线性反馈移位寄存器是用于产生伪随机数的唯一的一个这样的方法。按另一种方式，可以将一个随机数用作下面要讨论的任何其它方法的加密散列算法或数字签

字算法的一个种籽。“线性反馈移位寄存器“是快速的，也不是加密安全的，但可将它们组合构成序列，这些序列虽然还不可能证明是加密安全的，但还不知道曾被破坏过。它的例子包括“双侧停止和转向生成程序“和“N 阈生成程序“。

本发明的一个实施例的另一个处理方法是使用已知是安全的对称加密算法，例如 RSA Data Security 的 RC4，它要求有更大的处理能力。如果发卡银行服务器产生并且匹配了这个序列，就不一定要分配或供享密钥（ key ）。即使使用了已经知道是安全的加密算法，也存在某种程度的冒险。随着时间的流逝，由于计算机的性能在增长，先前认为是安全的加密算法也可能惨败于实际的侵袭。例如，40 位的“数据加密标准（DES）”不再被认为对于侵袭是安全的，因为今天可以得到的计算机已经表现出在合理的时间范围内用几个小时破坏这个算法的足够大的能力。

产生用于本发明的一个实施例的匿名或替换卡号的另外的处理方法是从已知的真正的随机数的表格（如 RAND 表）里拾取一个序列中的卡号。使用以上描述的一系列技术之一可以使从这个表中实际选择的卡号随机化。按另一种方式，从某些实际的随机物理过程（如测量键盘的等数时间或测量电子设备发出的电噪声）可以产生一个随机的序列。

按照本发明的一个实施例，通过组合技术可使伪随机序列甚致于更加安全保密，例如“线性反馈移位寄存器“法或对称算法，从而可从随机数表选择卡号，然后与一个算法（如“安全散列算法

（SHA）”）加密散列。

本发明的一个实施例的一个方面还提供代理鉴别的通用方式。例如，用户可以向用户的代理核准他或她自己，并且接收一个鉴别卡号。鉴别卡号例如用作一种一次性使用的鉴别令牌，将这个令牌发给用户，并且可使用这个令牌动去允许用户向任何其它服务部核准他或她自己，不需要附加的口令或密码。

按照本发明的一个实施例的另一方面，由于替换卡号是根据每次交易产生的，所以替换卡号可由卡的处理单位（如发卡人）使用，从而可始终监视它的位置（在哪一个通道）和对象（使用什么样的商家卡号）。例如，在提供给因特网商家（如商家 4）的因特网上，用户在一个钱包上（例如用户的电子钱包 28）提出有关一个替换卡号的请求。这时，发卡银行 8 可以识别和监视进行什么样的购买行动和与哪一个商家进行的购买行动。这一信息可用于欺诈管理和控制的目的，并且可以用于商业目的，例如在具体商家的促销或对在因特网上进行购买的顾客的促销。类似地，可用来监视在电话上或类似物上进行的购买行动。

按照本发明的一个实施例的另一方面，当使用一个基于服务器的钱包（例如用户的电子钱包 28）时，电子钱包 28 接收商家支付请求形式、并且不仅产生替换卡号、而且还预先认可这个购买行动、并且向商家 4 同时提供替换卡号和核准代码，这在技术上是可行的。虽然在技术上可行，但还必须有由卡的关联性认同的一种方法。例如从商家发展的角度来看，这种方法节省了核准所需的时间。时间

对于在因特网上进行交易是至关重要的。

在使销售活动快速和方便用户的努力中，许多商家实际上用的是信用卡号，甚致于不打算实时地获得信用卡的核准。相反，他们积累多笔交易并在事后进行核准。在这种情况下，商家可能事后发现，这种核准太迟了，商家必须回头再去与顾客接触。在数字货物的情况下，拒绝的公开可能发生在数字货物和服务已经发送之后。

在基于服务器的电子钱包 28 也预先认可这个购买行动并且向商家 4 同时提供替换卡号和核准代码的这一方面，对于银行来说，这一核准流消除了顶替的风险，否则发卡银行（如发卡人 8）就不能足够快地找回，并且卡的相关性顶替了发卡银行 8，而且自动地认同了这一交易，发卡银行 8 同时还在冒收集的风险。

在实现了本发明的各个目的过程中也描述了本发明的各个优选实施例。应该认识到，这些实施例只是本发明的原理的说明。在不偏离本发明的本质和范围的条件下许多改进和适应性修改对于本领域的普通技术人员来说都是显而易见的。因此，本发明只由下面的权利要求书限定。

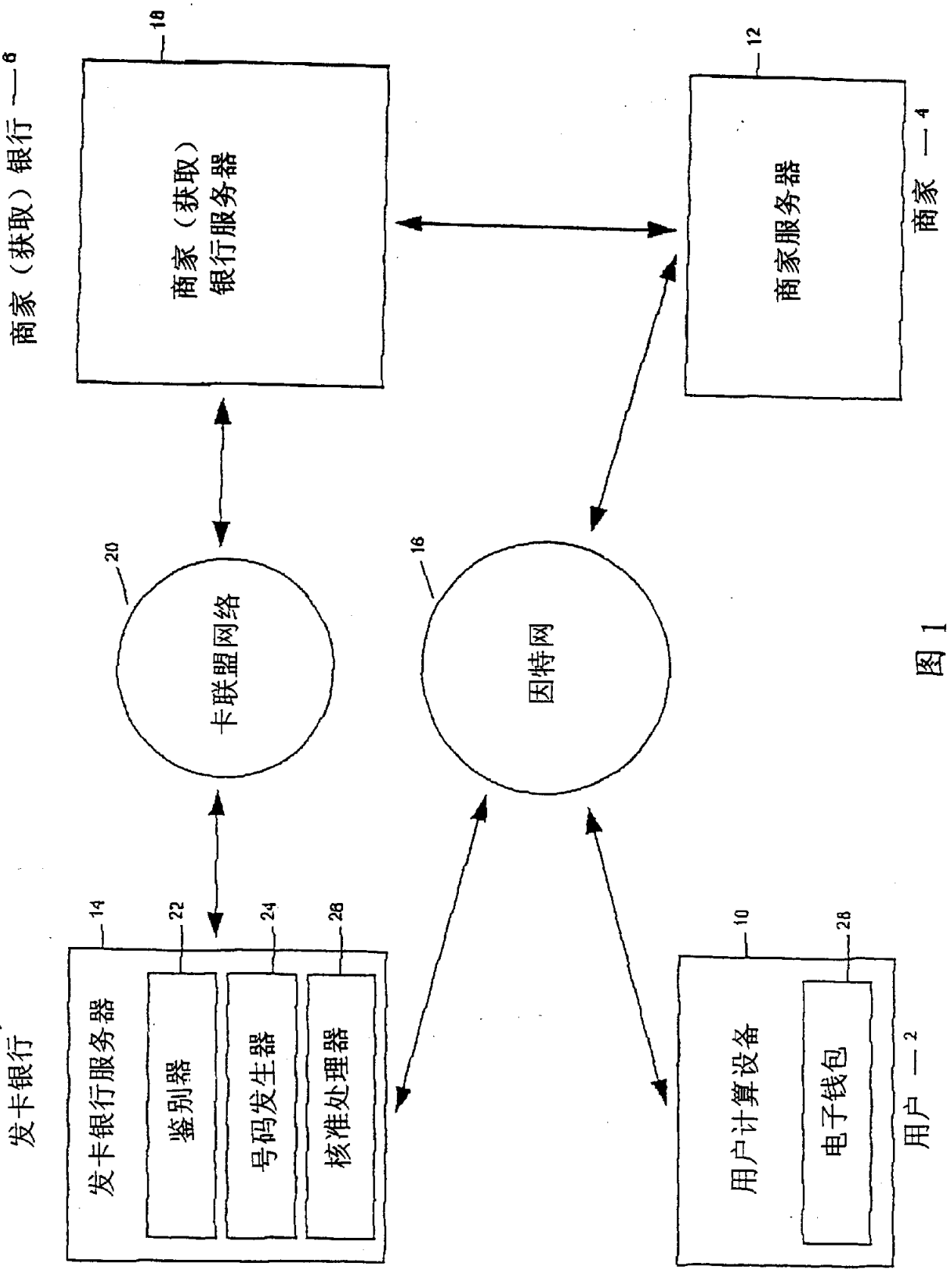

商家（获取）银行
6
18
商家（获取）
银行服务器
12
商家服务器
商家
4
20
卡联盟网络
16
因特网
发卡银行
8
发卡银行服务器
14
22
鉴别器
24
号码发生器
26
核准处理器
用户计算设备
10
28
电子钱包
用户
2

图 1

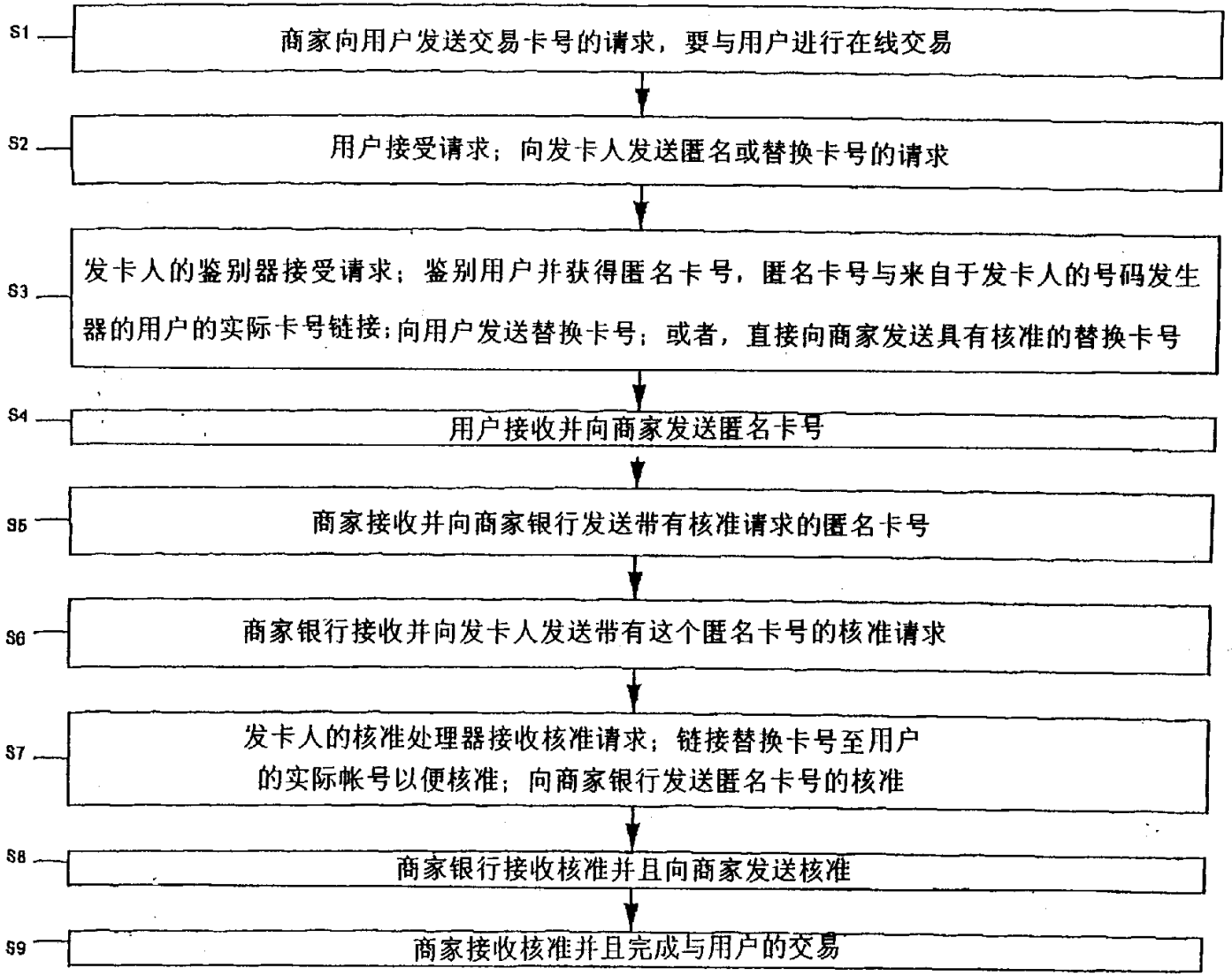

S1
商家向用户发送交易卡号的请求，要与用户进行在线交易
S2
用户接受请求；向发卡人发送匿名或替换卡号的请求
S3
发卡人的鉴别器接受请求；鉴别用户并获得匿名卡号，匿名卡号与来自于发卡人的号码发生器的用户的实际卡号链接；向用户发送替换卡号；或者，直接向商家发送具有核准的替换卡号
S4
用户接收并向商家发送匿名卡号
S5
商家接收并向商家银行发送带有核准请求的匿名卡号
S6
商家银行接收并向发卡人发送带有这个匿名卡号的核准请求
S7
发卡人的核准处理器接收核准请求；链接替换卡号至用户的实际帐号以便核准；向商家银行发送匿名卡号的核准
S8
商家银行接收核准并且向商家发送核准
S9
商家接收核准并且完成与用户的交易

图 2

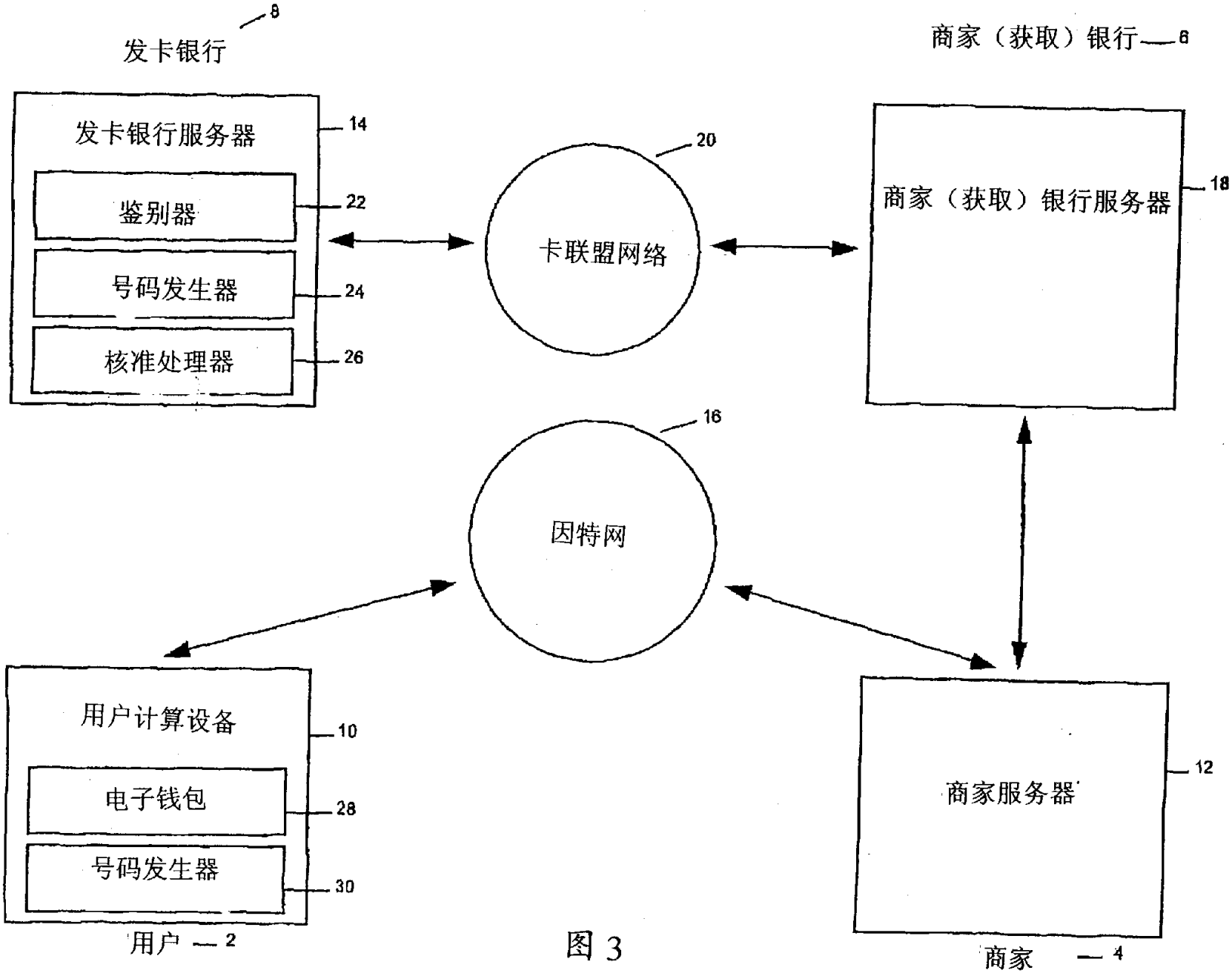

发卡银行
8
发卡银行服务器
14
鉴别器
22
号码发生器
24
核准处理器
26
卡联盟网络
20
商家（获取）银行
6
商家（获取）银行服务器
18
因特网
16
用户计算设备
10
电子钱包
28
号码发生器
30
用户
2
商家服务器
12
商家
4

图 3

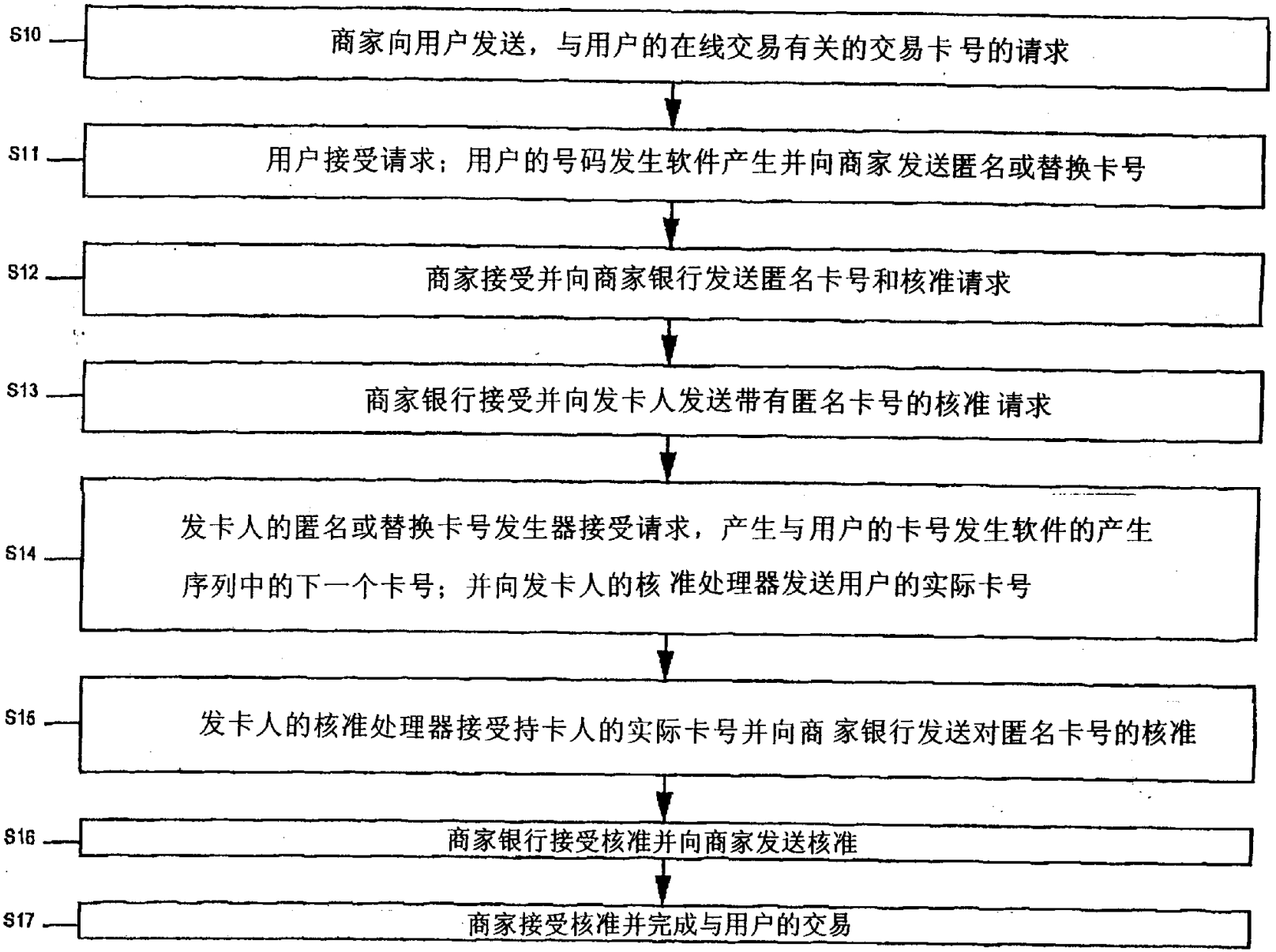

S10
商家向用户发送，与用户的在线交易有关的交易卡号的请求
S11
用户接受请求；用户的号码发生软件产生并向商家发送匿名或替换卡号
S12
商家接受并向商家银行发送匿名卡号和核准请求
S13
商家银行接受并向发卡人发送带有匿名卡号的核准请求
S14
发卡人的匿名或替换卡号发生器接受请求，产生与用户的卡号发生软件的产生序列中的下一个卡号；并向发卡人的核准处理器发送用户的实际卡号
S15
发卡人的核准处理器接受持卡人的实际卡号并向商家银行发送对匿名卡号的核准
S16
商家银行接受核准并向商家发送核准
S17
商家接受核准并完成与用户的交易

图 4

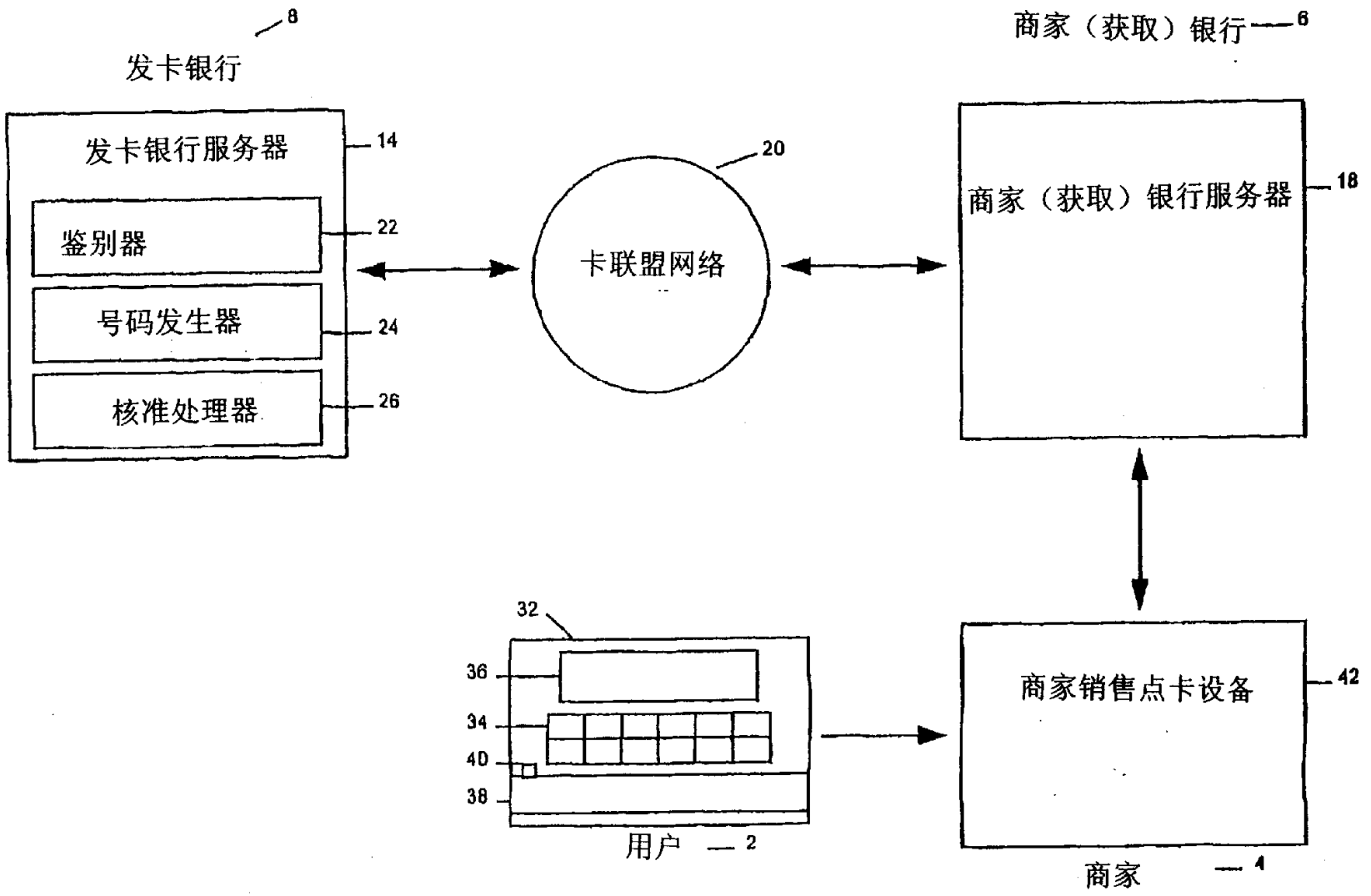

8
发卡银行
发卡银行服务器
14
鉴别器
22
号码发生器
24
核准处理器
26
20
卡联盟网络
商家（获取）银行
6
商家（获取）银行服务器
18
32
36
34
40
38
用户
2
商家销售点卡设备
42
商家
4

图 5

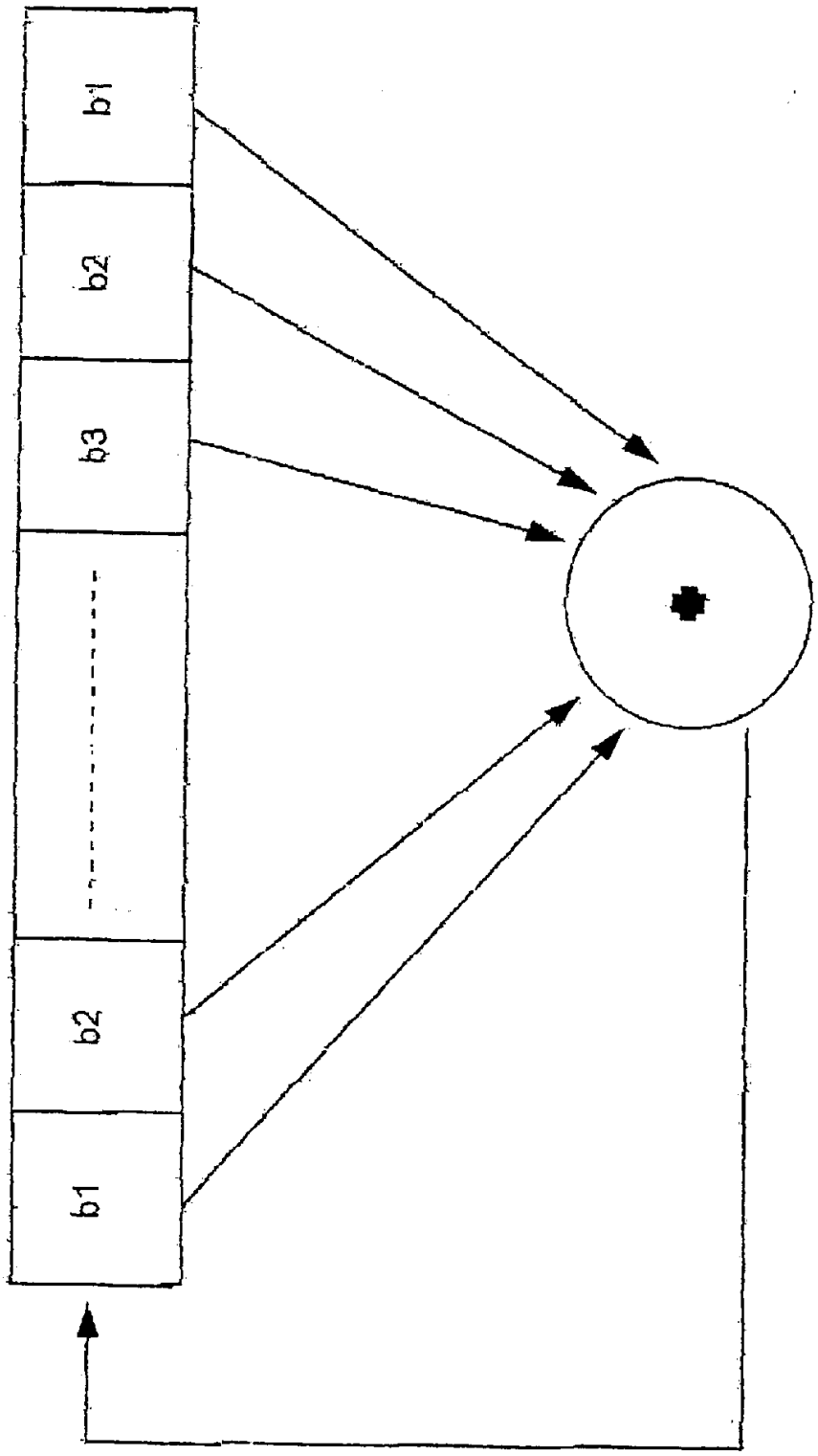


图 6