(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 102187353 A
(43)申请公布日 2011.09.14

(21)申请号 200980141467.5

(22)申请日 2009.09.04

(30)优先权数据
61/094,654 2008.09.05 US

(85)PCT申请进入国家阶段日
2011.04.20

(86)PCT申请的申请数据
PCT/US2009/056118 2009.09.04

(87)PCT申请的公布数据
WO2010/028302 EN 2010.03.11

(71)申请人 吉弗坦戈公司
地址 美国俄勒冈州泰格德市

(72)发明人 戴维·A·尼尔森 莱斯利·阿里芬

(74)专利代理机构 上海瀚桥专利代理事务所（普通合伙） 31261
代理人 曹芳玲

(51)Int.Cl.
G06Q 20/00(2006.01)
G06F 21/20(2006.01)
G06K 17/00(2006.01)

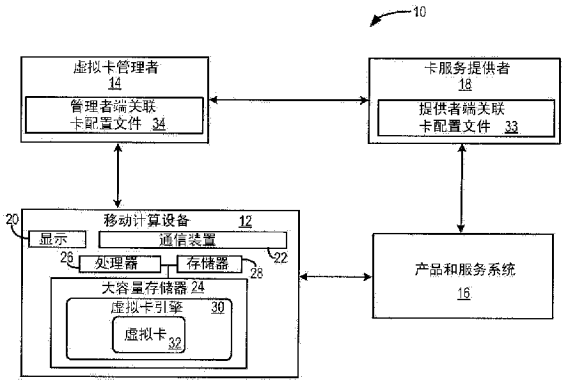
权利要求书 3 页 说明书 20 页 附图 11 页

(54)发明名称

用于虚拟储值卡的身份验证的系统和方法

(57)摘要

本发明提供一种虚拟卡管理系统，其包括可通过处理器执行的具有存储器的一个或多个服务器。该虚拟卡管理系统包括可在该一个或多个服务器上执行的虚拟卡管理者，该虚拟卡管理者具有配置为可通信地链接至少一个卡服务提供者和虚拟卡管理者的集成连接器引擎。该虚拟卡管理系统还可以包括配置为可通信地链接该虚拟卡管理者与至少一个虚拟卡引擎的虚拟卡管理平台，每个虚拟卡引擎包括一个或多个虚拟卡，该虚拟卡管理平台包括配置为基于预定的身份验证规则的集合选择性地启用至少一个虚拟卡和对应的卡服务提供者之间的虚拟卡交易的启用模块。



CN 102187353 A

1. 一种虚拟卡管理系统，其包括可通过处理器执行的具有存储器的一个或多个服务器，所述虚拟卡管理系统包括：

可在所述一个或多个服务器上执行的虚拟卡管理者，所述虚拟卡管理者包括：

配置为可通信地链接至少一个卡服务提供者和所述虚拟卡管理者的集成连接器引擎；及

配置为可通信地链接所述虚拟卡管理者与至少一个虚拟卡引擎的虚拟卡管理平台，每个虚拟卡引擎包括一个或多个虚拟卡，所述虚拟卡管理平台包括：配置为基于预定的身份验证规则的集合选择性地启用至少一个虚拟卡和对应的卡服务提供者之间的虚拟卡交易的启用模块。

2. 根据权利要求 1 所述的虚拟卡管理系统，其特征在于，所述启用模块还配置为基于预定的身份验证规则的第二集合选择性地启用至少第二虚拟卡，所述预定的身份验证规则的第一集合和所述预定的身份验证规则的第二集合具有不同的特性。

3. 根据权利要求 1 所述的虚拟卡管理系统，其特征在于，所述启用模块配置为选择虚拟卡的启用状态或禁用状态，启用状态包括允许虚拟卡和对应的卡服务提供者之间的虚拟卡交易的状态，禁用状态包括禁止虚拟卡和对应的卡服务提供者之间的虚拟卡交易的状态。

4. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，虚拟卡交易包括使虚拟卡与包括在对应的卡服务提供者中的对应的提供者端关联卡配置文件相关，及响应于所述虚拟卡交易的执行调整所述虚拟卡的一个或多个特性和提供者端关联卡配置文件中的至少一个。

5. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，所述虚拟卡管理平台还包括配置为管理与通过一个或多个虚拟卡引擎实现的多个虚拟卡对应的多个管理者端关联卡配置文件的关联配置文件模块，且其中当所述虚拟卡为启用状态时执行定期身份验证，所述定期身份验证包括校验虚拟卡的身份识别数据和管理者端关联卡配置文件中的配置文件身份识别数据之间的对应关系。

6. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，所述身份验证规则包括基于所述虚拟卡引擎的配置触发启用状态的配置规则，所述虚拟卡引擎的配置包括虚拟卡已被存取并开启以供使用的配置。

7. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，所述身份验证规则包括响应于虚拟卡交易的终止将虚拟卡设定为禁用状态的终止规则。

8. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，所述卡服务提供者配置为触发在所述虚拟卡管理者内对所述虚拟卡的选择性地启用的状态进行的调整。

9. 根据权利要求 3 所述的虚拟卡管理系统，其特征在于，一个或多个虚拟卡引擎配置为触发在所述虚拟卡管理者内对至少一个虚拟卡的选择性地启用的状态进行的调整。

10. 根据权利要求 1 所述的虚拟卡管理系统，其特征在于，所述身份验证规则包括基于用于执行所述虚拟卡的初始配置的系统调整选择性启用的卡履约规则，所述系统包括基于互联网的配置系统、产品和服务系统，及在移动计算设备上执行的移动配置应用程序。

11. 根据权利要求 1 所述的虚拟卡管理系统，其特征在于，所述身份验证规则包括基于使用中的卡的类型调整选择性启用的卡类型规则，所述卡的类型包括礼品卡、会员卡，及奖

励卡中的一个或多个。

12. 一种用于管理虚拟卡的方法，所述方法包括：

可通信地链接至少一个卡服务提供者和虚拟卡管理者，每个卡服务提供者包括至少一个提供者端关联卡配置文件；

可通信地链接至少一个虚拟卡引擎和所述虚拟卡管理者，所述虚拟卡引擎包括至少一个虚拟卡，且所述虚拟卡管理者包括与所述至少一个虚拟卡对应的至少一个管理者端关联卡配置文件；及

通过基于预定的身份验证规则的集合选择性地启用在所述至少一个虚拟卡和对应的卡服务提供者之间的虚拟卡交易，对所述至少一个虚拟卡进行定期身份验证。

13. 根据权利要求 12 所述的方法，其特征在于，还包括基于预定的身份验证规则的第二集合选择性地启用在第二虚拟卡和对应的卡服务提供者之间的第二虚拟卡交易，所述预定的身份验证规则的第一集合和所述预定的身份验证规则的第二集合具有不同的特性。

14. 根据权利要求 12 所述的方法，其特征在于，选择性地启用虚拟卡交易包括设定所述至少一个虚拟卡为启用状态或禁用状态，所述禁用状态包括禁止所述虚拟卡和所述卡服务提供者之间的虚拟卡交易的状态，所述启用状态包括允许虚拟卡交易的状态。

15. 根据权利要求 14 所述的方法，其特征在于，虚拟卡交易包括对所述提供者端关联卡配置文件和所述至少一个虚拟卡内的虚拟卡值进行调整的值交易或对提供者端关联卡配置文件内的特权数据进行存取和调整的特权交易。

16. 根据权利要求 14 所述的方法，其特征在于，设定所述至少一个虚拟卡为启用状态触发所述至少一个虚拟卡的定期身份验证，所述定期身份验证包括使包括在至少一个虚拟卡中的一个或多个唯一卡标识符相关于包括在管理者端关联卡配置文件中的具有唯一的卡标识符的提供者端关联卡配置文件。

17. 根据权利要求 14 所述的方法，其特征在于，还包括如果至少一个虚拟卡为启用状态且交易请求已由所述虚拟卡管理者接收，则允许所述交易请求。

18. 根据权利要求 12 所述的方法，其特征在于，所述选择性启用包括修改所述管理者端关联卡配置文件的一个或多个特性以启用或禁用至少一个虚拟卡服务提供者和至少一个虚拟卡之间的交易，所述特性包括虚拟卡状态指示符和关联于虚拟卡的唯一的卡标识符中的至少一个。

19. 根据权利要求 12 所述的方法，其特征在于，还包括响应于所述虚拟卡引擎和所述虚拟卡管理者之间的至少一次身份验证失败调整所述身份验证规则。

20. 根据权利要求 12 所述的方法，其特征在于，所述虚拟卡引擎的至少部分在移动或固定计算设备上执行，且其中所述至少一个虚拟卡包括礼品卡、会员卡和奖励卡中的至少一个。

21. 一种虚拟卡管理系统，其包括可通过处理器执行的具有存储器的一个或多个服务器，所述虚拟卡管理系统包括：

可在所述一个或多个服务器上执行的虚拟卡管理者，所述虚拟卡管理者包括：

配置为可通信地链接一个或多个卡服务提供者和所述虚拟卡管理者的集成连接器引擎；及

配置为可通信地链接所述虚拟卡管理者与一个或多个虚拟卡引擎的虚拟卡管理者平

台，每个虚拟卡引擎包括一个或多个虚拟卡，所述虚拟卡管理平台包括：配置为基于预定的身份验证规则的集合定期地启用或禁用虚拟卡以使所述虚拟卡定期地在启用状态和禁用状态之间切换的启用模块。

22. 根据权利要求 21 所述的虚拟卡管理系统，其特征在于，所述虚拟卡管理平台还包括配置为管理与通过虚拟卡引擎实现的虚拟卡对应的管理者端关联卡配置文件的关联配置文件模块，且其中定期身份验证在所述虚拟卡为启用状态时执行，所述定期身份验证包括校验包括在所述虚拟卡中的虚拟卡的身份识别数据和包括在对应的管理者端关联卡配置文件中的配置文件身份识别数据之间的对应关系。

23. 根据权利要求 21 所述的虚拟卡管理系统，其特征在于，所述启用模块还配置为基于预定的身份验证规则的第二集合选择性地启用至少第二虚拟卡，所述预定的身份验证规则的第一集合和所述预定的身份验证规则的第二集合具有不同的特性。

用于虚拟储值卡的身份验证的系统和方法

技术领域

[0001] 本发明总体上涉及用于虚拟卡的安全履约和身份验证的系统和方法，更具体地涉及用于通过移动计算设备出示的虚拟储值卡的履约和身份验证的系统和方法。

背景技术

[0002] 在当今的市场中，塑料礼品卡已成为支付的普遍形式。消费者通常购买选择的产品和服务系统的礼品卡，然后向实体位置出示塑料礼品卡以进行兑换。礼品卡的购买者常常会在兑换之前的一段时间中在其钱包内携带礼品卡。在兑换期间，用户可能整理其钱包并希望卡没有遗失或者放错地方。

[0003] 随着礼品卡的使用变得越来越普遍，消费者可能在其钱包内携带多个这样的礼品卡。通常，礼品卡只能够在单个产品和服务系统或商户的场所或有限数量的商户场所进行兑换。因此，由单个消费者携带并维护的礼品卡的数量很多。对于塑料或纸质的忠诚卡，诸如会员卡、奖励卡、点卡、优惠卡，和 / 或俱乐部卡，消费者也有类似问题。因此，使用这样的卡可能会进一步增加消费者的实体钱包大小。

[0004] 发明人在此认识到，对由消费者维护的大量卡进行管理是困难的。根据消费者可以管理的这些卡的数量，消费者通常在实体上扩大其钱包以携带大量的卡。消费者可能希望减少携带于实体钱包和手袋中的卡的数量。

[0005] 塑料卡的颁发还增加了卡遗失或放错地方的可能性。此外，如果卡遗失并由第三方兑换，则会发生卡的欺诈性使用。卡的不能履约(failure)可能对持卡人、产品和服务系统，和 / 或卡服务提供者以及整个行业造成负面影响。

[0006] 如发明人在此认识到颁发的塑料卡所面对的困难，已开发用于电子卡的替代方法和系统。这些以电子方式颁发并管理的卡在本文中称为虚拟卡。虚拟卡可以包括但不限于虚拟礼品卡、虚拟忠诚卡、虚拟会员卡，及虚拟奖励卡中的一个或多个。

发明内容

[0007] 如下文中进一步公开，提供在虚拟卡领域中构建新的安全性级别的系统和方法。因此，在一种方案中，提供一种虚拟卡管理系统，其包括可通过处理器执行的具有存储器的一个或多个服务器。该虚拟卡管理系统包括可在该一个或多个服务器上执行的虚拟卡管理者，该虚拟卡管理者包括配置为可通信地链接至少一个卡服务提供者和虚拟卡管理者的集成连接器引擎。该虚拟卡管理系统还可以包括配置为可通信地链接该虚拟卡管理者与至少一个虚拟卡引擎的虚拟卡管理平台，每个虚拟卡引擎包括一个或多个虚拟卡，该虚拟卡管理平台包括配置为基于预定的身份验证规则的集合选择性地启用至少一个虚拟卡和对应的卡服务提供者之间的虚拟卡交易的启用模块。

[0008] 以此方式，虚拟卡的状态可以在启用状态和禁用状态之间切换以增加虚拟卡管理系统的安全性。当卡为启用状态时，该卡可供使用。身份验证规则可以用于触发虚拟卡的状态的切换。可以基于选择的商户关于安全性的需要或愿望来建立和 / 或调整身份验证规

则。

[0009] 通过该系统，产品和服务系统可以围绕其卡项目构建规则，以保护其持卡人并防止损失或欺诈。卡服务提供者、产品和服务系统，及虚拟卡引擎之间的通信可以达到另一级别，允许增加促销能力和与持卡人的交互的级别。该新级别的安全性和身份验证可以为所涉及的各方提供安全交易体验。

附图说明

[0010] 图 1 示出根据本发明的实施例的虚拟卡管理系统的高级示意图。

[0011] 图 2A 和 2B 示出根据本发明的实施例的图 1 所示虚拟卡管理系统的详细示意图。

[0012] 图 3 示出可用于允许和禁止虚拟卡的使用的示例方法。

[0013] 图 4 示出可以通过根据本发明的实施例虚拟卡管理系统实现的设置和使用虚拟卡的方法的示例处理流程。

[0014] 图 5 示出设置虚拟卡的方法的示例处理流程。

[0015] 图 6 示出在移动计算设备上设置虚拟卡引擎以管理虚拟卡的方法的示例处理流程。

[0016] 图 7 至图 9 示出在显示上出示虚拟卡的示例移动计算设备的各种示意图。

具体实施方式

[0017] 图 1 示出根据本发明的实施例的虚拟卡管理系统 10 的示例性示意图。除了其他方面，该虚拟卡管理系统可以配置为基于预定的身份验证规则的集合选择性地启用至少一个虚拟卡的使用。因此，该系统提供允许通过移动和固定计算设备进行虚拟卡的履约的安全方法。递送虚拟卡到计算设备允许虚拟卡的使用及后续的由相关的第三方卡提供者启用 / 禁用虚拟卡。虚拟卡的出示允许识别谁在尝试使用该虚拟卡。基于身份识别信息和预先确定的身份验证规则，可以暂时地启用虚拟卡以供使用，且当未被出示以用于商户时，可以将虚拟卡保持在暂时禁用状态。以此方式，与塑料卡系统相比，虚拟卡的安全性得到增强，可防止该卡被未经授权的第三方使用。各种安全性特征，如选择性启用、身份验证等将在下文中详述。

[0018] 本文中所用的虚拟卡可以是电子方式颁发和 / 或电子方式维护的虚拟值卡。虚拟值可以是任何类型的特权，并可以是货币式或非货币式。例如，虚拟值卡可以是储值卡，包括但不限于虚拟礼品卡、虚拟忠诚卡、虚拟奖励卡、预付卡，或保存预付值的其他适合的虚拟卡。该储值卡可以在虚拟卡上存储货币值或其他形式的值。在另一示例中，虚拟值卡可以是虚拟会员卡，其中这样的存储值包括会员特权或相关于身份识别的特权。虚拟会员卡的示例可以包括但不限于虚拟身份识别卡、俱乐部卡、促销卡、身份识别卡（ID 卡）等。

[0019] 如图 1 所示，虚拟卡管理系统 10 可以包括移动计算设备 12、虚拟卡管理者 14、至少一个产品和服务系统 16，及至少一个卡服务提供者 18。移动计算设备可以是允许用户存储和维护一个或多个虚拟卡的适合的计算设备。例如，移动计算设备可以是智能电话、手持式计算设备、具有类似于高级 PC 的能力的移动设备、膝上型计算机、便携式媒体播放器等。在一些实施例中，移动计算设备可以运行可识别的操作系统的软件并提供用于应用程序的标准化接口和平台。移动计算设备可以与一个或多个网络，如公共网络（例如因特网）联网，

以允许通信用于虚拟卡的身份验证。

[0020] 移动计算设备 12 可以包括配置为在设备上呈现图像的显示 20。移动计算设备还可以包括有助于移动计算设备和外部系统和设备(如,虚拟卡管理者、产品和服务系统,及卡服务提供者)之间的有线和 / 或无线通信的通信装置 22。如图所示,移动计算设备可以包括存储在大容量存储器 24 中并可通过处理器 26 使用存储器 28 的一部分执行的各种软件应用程序。在一些实施例中,大容量存储器 24 可以是硬盘驱动器、固态存储器、可重写盘等。大容量存储器 24 可以包括各种编程元素,诸如配置为管理一个或多个虚拟卡 32 的虚拟卡引擎 30。虚拟卡引擎 30 可以是配置为实现下文详述的各种虚拟卡功能的软件应用程序。

[0021] 虚拟卡 32 可以是储值卡,诸如礼品卡、会员卡、虚拟身份识别卡等。每个虚拟卡可以包括一个或多个相关的卡数据,包括但不限于身份识别(ID)号码、存储值、姓名、条码、图像数据(如,持卡人的照片)、与可通过其使用卡的相关产品和服务系统对应的数据等。虚拟卡 32 可以由用户在移动卡钱包中存储或维护。移动卡钱包可以是管理虚拟卡的虚拟电子钱包(文件或应用程序)。在一些系统中,移动卡钱包可以按照类似于有形的实体钱包允许存储塑料卡的方式,允许用户组织和存取虚拟卡。移动卡钱包可以是在移动计算设备上的基于客户机的软件,或可以是由移动计算设备存取的基于浏览器的软件。

[0022] 如本文所用,产品和服务系统 16(亦总称为商户)可以是配置为管理产品和服务交易的系统。因此,商户可以是销售或提供产品和 / 或服务并希望通过移动电子设备或其他电子设备电子地或虚拟地颁发其卡数据或存储值的店铺。在其他示例中,商户可以包括卡服务提供者,其可以是代表选择的商户提供礼品卡或其他卡服务的第三方服务或提供者。卡服务提供者可以是第三方存储值公司、商户现有的销售点(POS)软件和 / 或提供者的模块或软件组件,和 / 或由商户购买、创建或使用以代表该商户跟踪礼品卡服务的应用程序或软件。

[0023] 在一些示例中,产品和服务系统 16 可以配置为通过移动计算设备或其他电子设备虚拟地或电子地颁发卡数据,诸如忠诚数据、会员数据、值数据(如,货币数据)等。产品和服务系统可以包括 POS 系统,如下文中参考图 2 详述,该 POS 系统可以包括管理电子交易的软件和硬件。应理解,产品和服务系统 16 可以关联于一个或多个商户。商户可以包括一个或多个咖啡馆、快餐店、酒店、超市等。因此,在一些示例中,产品和服务系统 16 可以在实体位置处理交易。然而,在其他示例中,产品和服务系统 16 可以通过因特网处理交易。一种类型的示例交易可以包括电子交易,诸如下文中详述的虚拟卡交易。

[0024] 在一些实施例中,产品和服务系统 16 可以直接地管理和控制虚拟卡交易。换言之,卡服务提供者 18 可以包括在产品和服务系统 16 中。然而,在其他实施例中,产品和服务系统 16 可以使用外部的卡服务提供者。因此,在一些实施例中可以使用第三方卡服务提供者。卡服务提供者 18 可以允许产品和服务系统 16 执行虚拟卡交易。在一个示例中,第三方卡服务提供者可以是配置为代表选择的产品和服务系统执行虚拟卡交易的软件和硬件。如上所述,第三方卡服务提供者可以包括除了其他方面可以配置为电子地处理虚拟卡交易的硬件和软件两者。

[0025] 应理解,虚拟卡交易可以包括存储值管理交易,诸如货币交易,其中调整(如,减少或在一些情况中增加)虚拟卡中的存储值。另外,虚拟卡交易还可以包括电子特权(如,持

卡人特权）的管理，诸如对特定类型的数据的电子存取。因此，交易可以包括两个系统、设备等之间的通信，在该通信中交换和 / 或处理值和 / 或特权数据。例如，虚拟卡交易可以包括从虚拟卡中减去值以在关联于产品和服务系统的商户位置交换产品或服务。此外，在其他示例中，虚拟卡交易可以包括在关联于产品和服务系统的商户位置扫描或通信传输（如，NFC —近场通信）虚拟会员卡并对该商户位置授予存取特权。此外，应理解，在一些示例中，交易可以包括安全性协议的执行。

[0026] 如上简述，卡服务提供者 18 可以是第三方存储值系统，或由产品和服务系统创建或使用以跟踪代表产品和服务系统的虚拟卡服务的该产品和服务系统的现有 POS 系统的模块或软件组件。产品和服务系统的 POS 提供者可以是配置为在一个位置处理产品和服务交易的软件、硬件，和 / 或其他设备。通常 POS 可以具有模块或内建的能力，从而使得 POS 系统也成为“卡服务提供者”。

[0027] 卡服务提供者 18 可以配置为生成至少一个提供者端关联卡配置文件 33，每个关联卡配置文件对应于一个虚拟卡。提供者端关联卡配置文件 33 可以包括虚拟卡数据，诸如存储值（如，货币值、点值）、身份识别（ID）数据（如，ID 号码、个人身份识别号码）、持卡人姓名等。可以在虚拟卡交易期间存取和调整选择的提供者端关联卡配置文件。应理解，在一些实施例中，提供者端关联卡配置文件可以包括在产品和服务系统中。

[0028] 卡服务提供者 18 可以与虚拟卡管理者 14 可通信地链接。虚拟卡管理者 14 也可以与移动计算设备 12 可通信地链接。在一些系统中，应理解，虚拟卡管理者 14 也可以与产品和服务系统 16 可通信地链接。

[0029] 虚拟卡管理者 14 可以配置为管理多个虚拟卡。特别是，虚拟卡管理者 14 可以配置为管理虚拟卡的各种安全性特征，诸如选择性启用（如，通过身份验证进行存取控制）。例如，可以选择性地允许（如，允许或禁止）虚拟卡的使用。应理解，当选择性地启用虚拟卡时，虚拟卡可以具有“激活”状况（status）。因此，虚拟卡可以为“激活”但为启用或禁用的状态。以此方式，可以快速地“开启”和“关闭”虚拟卡的使用而不停用虚拟卡，从而与激活之后保持在启用状态的塑料礼品卡相比，可以增强虚拟卡的安全性。虚拟卡的身份验证和选择性启用在下文中参考图 2 —图 6 详述。

[0030] 虚拟卡管理者 14 可以包括至少一个管理者端关联卡配置文件 34。管理者端关联卡配置文件 34 可以包括虚拟卡数据，诸如存储值（如，货币值、点值）、身份识别（ID）数据（如，ID 号码、个人身份识别号码）、持卡人姓名等。可以在虚拟卡交易期间存取和调整选择的管理者端关联卡配置文件。如下文详述，该系统可以匹配提供者端关联卡配置文件 33 与虚拟卡的管理者端关联卡配置文件 34。

[0031] 如下文详述，在一个示例中，可以设置虚拟卡系统以使虚拟卡管理者能够启用和禁用虚拟卡。然后商户可以可通信地链接到虚拟卡管理者。商户能够选择安全性和 / 或欺诈保护的级别。取决于安全性级别，可以将规则集合应用于与商户关联的虚拟卡。然后将该规则集合应用于与商户关联的虚拟卡的使用。

[0032] 例如，可以通过计算设备，诸如固定计算设备或移动计算设备将虚拟卡递送给用户。在一个示例中，可以将虚拟卡递送到用户的移动计算设备以供使用。预定的身份验证规则，也称为安全性规则，可以关联于虚拟卡。可以执行身份验证规则以使虚拟卡的状态（如，启用状态、禁用状态等）可以由虚拟卡管理者管理。在一些系统中，虚拟卡管理者可以是远

程服务器，而在其他系统中，虚拟卡管理者可以在移动计算设备上。

[0033] 在一个示例中，取决于身份验证规则，虚拟卡的使用限于已识别的移动计算设备，以便阻止未识别的(未关联的)移动计算设备使用虚拟卡的尝试。当请求了这样的使用时，虚拟卡可以保持在禁用状态，从而防止卡的未授权使用。同样，取决于规则集合，在一些系统中，如果提供附加的身份识别，商户能够跳过(over-ride)禁用状态。虽然上述示例是相对于单个移动计算设备的身份识别描述的，在一些示例中，用户能够引入附加的计算设备作为授权的计算设备。在这样的系统中，规则集合可以允许将作出请求的计算设备识别为授权的计算设备以使卡的状态为启用。

[0034] 虽然在图 1 中仅示出单个卡服务提供者和移动计算设备，应理解，虚拟卡管理者 14 可以用作用于管理对应于多个卡服务提供者的大量的虚拟卡的公共平台。在一些示例中，卡服务提供者中的两个或多个可以具有不同的特性。例如，两个或多个卡服务提供者可以利用不同的通信协议并可以链接到不同的产品和服务系统，从而提供不同的服务。此外，卡服务提供者可以提供不同类型的卡服务。例如，一个卡服务提供者可以提供会员卡服务，而另一个卡服务提供者可以提供礼品卡服务。以此方式，单个虚拟卡管理系统可以用于管理大量的虚拟卡，有助于虚拟卡管理系统的可伸缩性，从而增强虚拟卡管理系统的市场吸引力。

[0035] 参考图 2A，示出虚拟卡管理系统 10 的详细示意图。虚拟卡管理系统 10 可以配置为提供和管理虚拟卡并生成用于多个卡服务提供者的公共平台。无论卡服务提供者的程序或数据需求如何，该公共平台允许各种卡服务提供者及产品和服务系统在不同的卡服务提供者之间交换数据和传输产品，诸如虚拟卡产品和服务。

[0036] 如图所示，虚拟卡管理者系统 10 可以包括虚拟卡管理者 14，虚拟卡管理者可以在如上所述的一个或多个服务器 202 上存储和执行。特别是，虚拟卡管理者 14 可以在一个或多个远程服务器上存储和执行。然而，在其他实施例中，虚拟卡管理者 14 可以在包括在产品和服务系统 16 和 / 或卡服务提供者 18 中的服务器上存储和执行。因此，可以在应用程序服务提供者(ASP)模型以及软件安装模型下提供所公开的虚拟卡管理者。例如，可以提供 API 方案，其中商户通过其自身的电子商务设置，诸如网站来销售虚拟卡。然后商户可以利用上述系统和方法来颁发虚拟卡并提供对虚拟卡的身份验证的跟踪。在其他实施例中，商户可以在其自身的服务器上直接安装上述系统或应用程序以对虚拟卡进行特定于商户的处理。

[0037] 如下文详述，应理解，在一些系统中，只要由 POS 或卡服务提供者提供的 API 或其他软件链接到虚拟卡管理者以允许与 POS 或卡服务提供者通信，虚拟卡管理者就可以总体上设置定期的虚拟卡身份验证，而各方不必作出任何编码改变。在一些实施例中，如果卡服务提供者希望在其一端作出编码改变，可以允许附加的选项或服务。

[0038] 虚拟卡管理者 14 可以包括配置为通过包括在卡服务提供者中的 API 206 或其他软件通信标准可通信地链接虚拟卡管理者 14 与至少一个卡服务提供者 18 的集成连接引擎 204。以此方式，虚拟卡管理者 14 可以和卡服务提供者 18 通信。当多个卡服务提供者可通信地链接到虚拟卡管理者 14 时，卡服务提供者的至少部分可以利用不同的通信协议、通信硬件、安全性协议等。因此，集成连接引擎 204 允许虚拟卡管理者 14 与多个不同的卡服务提供者交互。在其他实施例中，卡服务提供者 18 可能希望使用由虚拟卡管理者提供的 API

或其他软件以允许通信。在其他示例中，卡服务提供者 18 可以包括用于和虚拟卡管理者 14 通信的其他方法或系统。

[0039] 另外，应理解，集成连接引擎 204 可以包括配置为将发送到产品和服务系统和从该系统接收的数据修改为常见的编程语言，诸如 XML 的至少一个虚拟卡适配器。然而，在其他实施例中，集成连接引擎 204 可以不包括虚拟卡适配器。

[0040] 因此，应理解，一旦虚拟卡管理者 14 和卡服务提供者 18 已通过集成连接引擎 204 可通信地链接，则链接到卡服务提供者 18 的产品和服务系统 16 能够增加其虚拟卡能力。在一个示例中，虚拟卡管理者 14 和卡服务提供者 18 可以一起工作以提供各种能力，包括但不限于激活卡、停用卡、重新激活卡、注销银行卡、注销先前的交易、查询卡余额、更新卡值、查询用卡历史、定期身份验证能力、传送忠诚数据，卡履约到电子邮件，移动设备或其他设备等。系统能力将取决于虚拟卡管理者系统和卡服务提供者的系统之间的集成级别。上述能力本质上是示例性的且在其他实施例中可以提供附加的或替代的能力。

[0041] 如上所述，卡服务提供者 18 可以包括在产品和服务系统 16 中。然而，应理解，在其他实施例中，卡服务提供者可以不包括在产品和服务系统中。产品和服务系统可以包括配置为电子地处理产品和服务的销售点（POS）系统 208。然而，应理解，可以利用替代系统以电子地处理产品和服务。

[0042] 另外，虚拟卡管理者 14 可以包括虚拟卡管理平台 210，除了其他方面，该平台可以配置为通过外部客户机端产品 212 向多个移动计算设备提供虚拟卡服务，外部客户机端产品包括虚拟卡引擎 30 和 / 或电子商务服务 214。应理解，虚拟卡引擎可以存储在移动计算设备上。然而，在其他实施例中，虚拟卡引擎可以存储在连接到因特网的服务器上。因此，可以通过浏览器存取虚拟卡引擎。如上所述，图 2 所示的系统可以用作电子商务销售解决方案。在一些实施例中，可以提供 API 方案，其中产品和服务系统通过其自身的电子商务系统销售虚拟卡，然后利用上述系统颁发虚拟卡并提供对虚拟卡的跟踪和身份验证。在其他实施例中，产品和服务系统可以在其自身的服务器上直接地安装上述系统或应用程序以对虚拟卡进行特定于商户的处理。

[0043] 虚拟卡管理平台可以包括启用模块 215，其配置为基于预定的身份验证规则的第一集合 217 选择性地且定期地启用至少一个虚拟卡和对应的虚拟卡服务提供者之间的虚拟卡交易。因此，启用模块可以选择虚拟卡的启用或禁用状态。应理解，在调整虚拟卡的状态（如，选择启用或禁用状态）时，虚拟卡可以是“激活”的。启用状态可以包括允许虚拟卡和对应的卡服务提供者之间的虚拟卡交易的状态，禁用状态可以包括禁止虚拟卡和对应的卡服务提供者之间的虚拟卡交易的状态。对应的卡服务提供者可以管理相关于在使用中的虚拟卡的存储的数据。存储的数据可以包括在提供者端关联卡配置文件 33 中。

[0044] 在一些示例中，通过选择性地启用虚拟卡交易进行的定期身份验证可以包括将该卡从禁用状态切换到启用状态。在启用状态和禁用状态之间的该切换可以视为定期身份验证。卡的切换可以在选择的事件或时间下，诸如紧接虚拟卡使用之前发起。切换允许对使用虚拟卡的安全性有增强的控制，因为卡只能在启用状态下使用。在该处理期间保持存储在虚拟卡引擎上和 / 或提供者端关联卡上的值数据。如上所述，值数据可以包括货币数据和 / 或会员服务数据。应理解，可以使用不同的方法来切换虚拟卡的状态。例如，在一些系统中，切换可以允许根据由特定卡服务提供者或移动设备提供的能力开启和 / 或关闭存储

值。然而，应理解，可以使用其他技术来启用和禁用虚拟卡。

[0045] 不同方法可以用于当虚拟卡在启用状态和禁用状态之间切换（或相反）时实现虚拟卡的状态改变。在一些系统中，状态改变可以通过用户动作实现，和 / 或在其他系统中，基于对虚拟卡的使用或存取，状态改变可以是自动的、半自动的。例如，状态改变可以由于下述示例动作中的一个或多个造成 ：改变 PIN 码、改变密码、改变到期日、切换开关、移除值然后恢复值、基于时间的规则、安全性规则、使用规则。另外，动作，诸如用户确认动作或对使用的请求可以操作用于在禁用和启用状态之间切换卡。

[0046] 在一个示例中，用户动作，诸如请求使用虚拟卡可以触发卡的状态的切换。此外，在一些实施例中，动作，诸如翻转电子卡或存取条码区域或其他码可以触发卡的状态的切换。例如，在一些实施例中，虚拟卡可以呈现在用户计算设备上，且动作，诸如电子地翻转卡可以允许用户“看到”卡的反面，在那里可以存储条码或其他使用信息。翻转卡的动作可以触发启用状态。然后该卡可以保持在启用状态达预定时间，以使在定义的时间段期间未能使用该卡将导致该卡切换回禁用状态。在其他实施例中，一旦启用，卡可以无限地保持在启用状态，或直到发生了另一动作，诸如关闭虚拟卡，或达到了时间限制。

[0047] 在另一示例中，通过选择性地启用虚拟卡交易进行定期身份验证可以包括改变包括在管理者端关联卡配置文件中的关联于虚拟卡的 PIN/CID 码。例如，可以间歇性地改变包括在管理者端关联卡配置文件中的关联于虚拟卡的码以使只有虚拟卡管理者知道或可以识别对应的码。例如，当定期身份验证开启时，可以将该码发送到虚拟卡引擎。当定期身份验证回到关闭时，可以改变该码。这提供了暂时启用和禁用这些卡的方法。在另一非限制性示例中，可以提供虚拟卡状态指示符。例如，虚拟卡管理者和 / 或卡服务提供者可以包括能够暂时禁止卡的使用而不停用该卡的虚拟卡状态指示符或标志。在又一示例中，卡服务提供者可以和虚拟卡管理者一起工作以开发或使用专用于相对于通过虚拟卡引擎存取虚拟卡切换虚拟卡的用户的方法。应理解，上述选择性启用技术本质上是示例性的且在其他示例中可以利用其他选择性启用技术。

[0048] 在又一示例中，可以将虚拟卡递送到移动计算设备。可以控制初始递送时卡的状态，以在第一状态，诸如启用状态或禁用状态下颁发该卡。然后可以根据身份验证规则切换卡的状态。身份验证规则可以包括何时触发切换、保持特定状态的时间段、身份识别触发器等的规则。身份验证规则可以包括基于由卡服务提供者和 / 或产品和服务系统请求的期望的安全性级别由虚拟卡管理者设定的规则以及直接由卡服务提供者和 / 或产品和服务系统设定的规则。可以基于用户的计算设备进一步增强或限制规则。

[0049] 另外，在一些示例中，启用模块可以进一步配置为基于预定的身份验证规则的第二集合 219 选择性地启用第二虚拟卡，预定身份验证规则的第一集合和第二集合具有不同的特性。因此，身份验证规则的不同集合可以应用于不同的虚拟卡或虚拟卡的组。此外，在一些示例中，可以通过第一卡服务提供者和 / 或第一产品和服务系统调整（如，建立）预定的身份验证规则的第一集合，且可以通过第二卡服务提供者和 / 或第二产品和服务系统调整（如，建立）预定的身份验证规则的第二集合。然而，在其他示例中，可以通过第一产品和服务系统和 / 或第一卡服务提供者调整预定的身份验证规则的第一集合和第二集合。此外，在其他示例中，虚拟卡引擎可以调整身份验证规则的至少部分，包括预定的身份验证规则的第一集合和 / 或第二集合。然而，在其他示例中，可以禁止虚拟卡引擎调整预定的身份验

证规则。因此，可以针对特定的产品和服务系统、卡服务提供者，和 / 或虚拟卡引擎的具体情况，定制选择性地启用虚拟卡或虚拟卡的组的方式。

[0050] 在一些示例中，身份验证规则可以包括持久启用的规则，其中虚拟卡设定为永久启用状态。当不需要高级别的虚拟卡安全性时，诸如当虚拟卡是奖励卡或忠诚卡时，产品和服务系统和关联的卡服务提供者可以利用这样的规则。以此方式，产品和服务系统和 / 或卡服务提供者可以基于使用中的虚拟卡的类型调整安全性级别。

[0051] 此外，在一些实施例中，身份验证规则可以包括这样的存取规则，其中响应于在虚拟卡引擎中对虚拟卡的存取将虚拟卡设定为启用状态。例如，在一些系统中，可以当开启虚拟卡以用于在能够具有该类型的安全性的移动计算设备上进行查看时触发选择性启用（而如果提供给能力不足的设备则可能不启用）。在其他系统中，可以触发标志，其中卡可以处在高风险欺诈情况下（如，在预定时期中使用虚拟卡的重复尝试、使用该卡的多次尝试等）。另外，身份验证规则还可以包括终止规则，其中响应于虚拟卡交易的终止将虚拟卡设定在禁用状态。以此方式，可以在交易之前启用虚拟卡并在虚拟卡交易已完成之后禁用虚拟卡，以增加系统的安全性。应理解，在一些实施例中，可以确定终止时间间隔。例如，产品和服务系统可以确定在交易已完成之后触发禁用的阈值时间间隔（如，1 分钟、20 分钟等）。

[0052] 身份验证规则还可以包括卡履约规则，其中基于用于执行虚拟卡的初始配置的系统调整选择性启用，该系统包括基于互联网的配置系统、产品和服务系统，及在移动计算设备上执行的移动配置应用程序中的一个或多个。以此方式，当虚拟卡是从不太可信的来源生成的时，虚拟卡的安全性可以增强。例如，当使用基于互联网的配置系统生成虚拟卡时，可能有更高的欺诈行为可能性，因此可以在已执行多个级别的身份验证之后触发虚拟卡的选择性启用。例如，可以提示虚拟卡引擎的用户输入密码以选择性地启用虚拟卡的使用。另外，虚拟卡管理者可以确认虚拟卡的一个或多个唯一的卡标识符对应于（或匹配）在管理者端关联卡配置文件内存储的唯一的卡标识符以实现选择性启用。此外，可以在虚拟卡交易期间多次执行上述安全措施以降低卡的欺诈性使用的可能性。

[0053] 类似地，身份验证规则可以包括兑换规则，其中基于兑换的位置（如，执行虚拟卡交易的位置）调整选择性启用。兑换的位置可以是实体店铺或商户的网站中的一个。

[0054] 身份验证规则还可以包括卡类型规则，其中基于使用中的虚拟卡的类型调整选择性启用，卡的类型包括礼品卡、会员卡，及奖励卡中的一个或多个。例如，产品和服务系统可能希望在使用虚拟礼品卡时增加安全性级别并在使用奖励卡时降低安全性级别。如上所述，当使用虚拟礼品卡时，可以提示虚拟卡引擎的用户输入密码以选择性地启用虚拟卡的使用。另外，当使用虚拟礼品卡时，虚拟卡管理者可以确认虚拟卡的一个或多个唯一的卡标识符匹配存储在管理者端关联卡配置文件中的唯一的卡标识符以实现选择性启用。然而，当使用虚拟奖励卡时，可以永久地启用虚拟卡，或当虚拟奖励卡使用时，虚拟卡管理者可以在其确认虚拟卡的一个或多个唯一的卡标识符匹配存储在管理者端关联卡配置文件中的唯一的卡标识符之后，执行选择性启用。以此方式，各类型的虚拟卡可以具有变化的安全性级别。

[0055] 此外，身份验证规则可以包括这样的规则，其中可以基于虚拟卡引擎（如，移动电话）的位置调整虚拟卡交易的选择性启用。例如，可以当虚拟卡引擎是基于万维网的应用程序时执行提高的安全性级别，并当在移动计算设备上执行虚拟卡引擎时执行降低的安全性

级别。

[0056] 其他示例身份验证规则包括关于虚拟卡的使用的基于时间的规则。在一些实施例中，基于时间的规则可以是基础规则或基本规则，该规则要求根据产品和服务系统和 / 或卡服务提供者的至少一些定义。例如，产品和服务系统可以定义在启用之后必须于选择的时间段内（如，在 5、10、15、30、60、90 分钟内等）使用虚拟卡，否则其将被自动地禁用。

[0057] 其他示例身份验证规则包括使用规则。例如，在一些实施例中，在指定的时间段内只能使用虚拟卡选择的次数（如，1、2、3、4、5 次等）。在另一个非限制性示例中，产品和服务系统可以选择在单次使用之后永久禁用虚拟卡。

[0058] 产品和服务系统还可以进一步确定各种卡身份识别和安全性身份识别（CID）规则。这些规则可以允许产品和服务系统对身份验证过程具有一定控制。例如，产品和服务系统可以定义安全性代码标识符的大小，及围绕相对于用卡服务提供者管理身份验证使用该 CID 的规则。

[0059] 此外，在一些实施例中，产品和服务系统可以定义相关于持卡人的移动计算设备的规则。例如，产品和服务系统可以定义允许能够从多个移动 / 电子设备上使用虚拟卡或将这样的使用限制于单个设备的规则。因此，在一些实施例中，用户能够将虚拟卡从一个设备传输到另一个设备或传输到不同的用户。在其他实施例中，可以关闭或最小化这样的传输功能。此外，可以对允许出示单个虚拟卡的设备的数量施加限制。在一些系统中，产品和服务系统可以允许合并卡以创建具有更高值的单个卡。此外，一些系统可以允许将卡划分为多个单独的较低值的卡，且取决于由产品和服务系统定义的产品和服务系统规则，这些卡可以传输或不可以传输到另一移动设备或用户。

[0060] 在另一示例中，可以由产品和服务系统定义持卡人设定的身份验证规则。例如，产品和服务系统可以选择允许虚拟卡引擎修改由产品和服务系统设定的一些规则。例如，产品和服务系统可以默认对其虚拟卡使用较高安全性，但可以允许虚拟卡引擎选择不参与该较高的安全性级别。

[0061] 应理解，卡服务提供者和 / 或产品和服务系统可以选择一个或多个上述身份验证规则以在虚拟卡管理者中使用。然而，大量身份验证规则是可能的，因此，在其他实施例中，可以选择使用附加的或替代的身份验证规则。

[0062] 图 2B 示出根据本发明的实施例的启用模块的示例性用例。如图所示，启用模块 215 可以设定或允许在启用和禁用状态之间触发虚拟卡 250。然而，虚拟卡可以具有“激活”状况。因此，可以快速地“开启”和“关闭”虚拟卡的使用而不修改虚拟卡的状况（如，停用）。卡的激活状况可以指示卡可用，从而在卡上有存储值可用。在一些示例中，当虚拟卡是虚拟会员卡时，激活的卡可以是经颁发且以特权值衡量的值可用的卡。启用模块不影响卡上的存储值，而是管理卡的可用性。

[0063] 参考图 2A，虚拟卡管理平台还可以包括关联配置文件模块 216。关联配置文件模块可以配置为管理至少一个管理者端关联卡配置文件 34。每个管理者端卡配置文件可以具有对应的虚拟卡以及对应的提供者端关联卡配置文件。管理者端关联卡配置文件可以包括卡数据，诸如身份识别号码、密码、客户数据等中的一个或多个，以及在一些实施例中，还包括对应于虚拟卡的状态的数据。另外，虚拟卡管理平台可以包括可通信地链接到电子商务服务的应用程序接口（API）218 或其他适合的软件通信标准。因此，API 可以用作虚拟卡管

理者和电子商务服务之间的接口。

[0064] 虚拟卡管理平台 210 还可以包括管理模块 220，其配置为调整身份验证规则、管理者端相关卡配置文件，和 / 或可由虚拟卡管理者提供的其他卡服务。可以授予卡服务提供者、产品和服务系统，及虚拟卡引擎对由管理模块执行的至少部分功能的存取。然而，应理解，在一些实施例中，只有卡服务提供者和 / 或产品和服务系统能够存取管理模块。此外，在一些实施例中，虚拟卡管理者仅能够存取管理模块。以此方式，可以增强虚拟卡管理系统的安全性。

[0065] 虚拟卡管理平台 210 还可以包括使用模块 222，其配置为跟踪虚拟卡使用数据 224，诸如与虚拟卡管理者交互的虚拟卡的卡交易、身份验证事件等。以此方式，可以收集大量卡的使用数据，该使用数据可用于对虚拟卡管理系统的后续评估。使用数据还可以用于营销目的。虚拟卡管理者可以包括用于存储卡交易信息和数据，诸如使用数据的存储库 (如，数据库) 以及管理者端关联卡配置文件。然而在其他示例中，使用数据和管理者端关联卡配置文件可以存储在服务器 202 上。

[0066] 图 3 示出可以用于选择性地启用一个或多个虚拟卡的示例性方法 300。应理解，该方法可以使用上述系统、设备等实现。然而，在其他实施例中，可以使用其他适合的系统和设备实现方法 300。

[0067] 首先，在 302，该方法包括可通信地链接至少一个卡服务提供者和虚拟卡管理者。接下来，在 304，该方法包括可通信地链接至少一个虚拟卡引擎和虚拟卡管理者。因此，用户可以颁发虚拟卡到其移动计算设备上和 / 或其他设备上以便可以通过移动计算设备存取虚拟卡。应理解，本文提供的示例是相对于递送虚拟卡到移动计算设备描述的，然而，在一些系统中，该方法可以在固定计算设备上发起，诸如用于基于互联网的订单。因此，可以从任何联网的计算设备、无论是移动还是固定的设备发起并使用定期身份验证。

[0068] 在一个示例中，可以从可将虚拟值卡直接发送到用户的移动计算设备上的商户请求虚拟卡。用户可以在其电子钱包中存储虚拟值卡直到其准备使用该卡。如下文所述，可以通过对卡的状态的管理 (启用相对于禁用) 增强卡的安全性。卡在启用状态和禁用状态之间的切换可以基于身份验证规则，诸如预定的身份验证规则。规则的执行，因此对卡的状态的管理可以诸如通过远程的虚拟卡管理者远程地处理，和 / 或根据机载的规则，诸如通过移动计算设备处理。在通过移动计算设备处理卡的状态的示例中，具有规则集合的应用程序可以加载到移动计算设备上。

[0069] 在 306，该方法包括通过基于预定的身份验证规则的集合选择性地启用虚拟卡和对应的卡服务提供者之间的虚拟卡交易进行定期身份验证。例如，身份验证的时期可以由预定的身份验证规则设定。例如，该时期可以基于尝试的使用、预定的时间段、显示或选择显示虚拟卡等。如上所述，对虚拟卡交易进行定期身份验证可以包括设定虚拟卡为启用状态或禁用状态，禁用状态包括禁止虚拟卡和卡服务提供者之间的虚拟卡交易的状态，启用状态包括允许虚拟卡交易的状态。以此方式，可以基于预定的身份验证规则的集合允许或不允许交易。此外，在一些实施例中，通过选择性启用进行的定期身份验证还可以包括修改管理者端关联卡配置文件的一个或多个特性以启用或禁用至少一个虚拟卡服务提供者和至少一个虚拟卡之间的交易，该特性包括虚拟卡状态指示符和关联于虚拟卡的唯一的卡标识符中的至少一个。

[0070] 此外，在一些实施例中，虚拟卡交易可以包括值交易或特权交易，在值交易中调整提供者端关联卡配置文件和 / 或虚拟卡内的虚拟卡值，在特权交易中存取和 / 或调整提供者端关联卡配置文件内的特权数据。此外，在一些实施例中，设定虚拟卡为启用状态可以触发虚拟卡的定期身份验证。定期身份验证可以包括使包括在至少一个虚拟卡中的一个或多个唯一的卡标识符与具有包括在管理者端关联卡配置文件中的唯一的卡标识符的提供者端关联卡配置文件相关。

[0071] 接下来，在 308，该方法包括接收虚拟卡的交易请求。该交易请求可以是使用请求，诸如使用卡上的存储值的请求。如上所述，存储值可以是诸如在虚拟礼品卡中的货币值，或可以是诸如在会员卡中的特权值。

[0072] 在 310，确定虚拟卡为启用状态还是禁用状态。在一些实施例中，确定虚拟卡为启用状态还是禁用状态可以包括执行身份验证过程，诸如定期身份验证。定期身份验证可以基于预定的身份验证规则，并可以包括在一个或多个选择的时间在启用状态和禁用状态之间切换卡。切换可以由关联于该卡的事件，诸如尝试使用、虚拟卡的状况（如，在用户的移动计算设备上显示虚拟卡）等触发。身份验证过程可以通过虚拟卡管理者、卡服务提供者，和 / 或虚拟卡引擎之间的通信执行。如果虚拟卡为启用状态（如，如果身份验证得到确认），则该方法进入 312，其中该方法包括允许交易请求。然而，如果虚拟卡为禁用状态（如，如果身份验证失败），则该方法进入 314，其中该方法包括禁止交易请求。

[0073] 应理解，该方法可以在 312 或 314 结束。此外，虽然在 316 用预定的身份验证规则的第二集合描述第二交易，但应理解，预定的身份验证规则的第二集合可以不同于预定的身份验证规则的第一集合或与第二集合相同。

[0074] 接下来，在 316，该方法包括基于预定的身份验证规则的第二集合选择性地启用第二虚拟卡和对应的卡服务提供者之间的第二虚拟卡交易。应理解，该方法在 316 可以与该方法的第一部分同时进行。

[0075] 在 318，该方法包括接收第二虚拟卡的交易请求。在 320，确定第二虚拟卡为启用状态还是禁用状态。在一些示例中，确定第二虚拟卡为启用状态还是禁用状态可以包括执行身份验证过程。可以通过虚拟卡管理者和卡服务提供者和 / 或虚拟卡引擎之间的通信执行身份验证过程。如果第二虚拟卡为启用状态（如，如果身份验证得到确认），则该方法包括在 322 允许交易请求。然而，如果第二虚拟卡为禁用状态（如，如果身份验证失败），则该方法进入 324，其中该方法包括禁止交易请求。在一些示例中，该方法还可以包括在 326 响应于虚拟卡引擎和虚拟卡管理者之间的身份验证失败调整身份验证规则。以此方式，当怀疑第三方尝试对虚拟卡的欺诈性使用时，可以提高虚拟卡的安全性。然而，在其他实施例中，步骤 326 可以不包括在方法 300 中。在 322 和 326，该方法结束。以此方式，可以快速地启用和禁用虚拟卡，增强虚拟卡管理系统的安全性并降低虚拟卡由第三方进行欺诈性使用的可能性。

[0076] 如上所述，提供这样的方法，其中虚拟卡被颁发给用户并可以通过移动计算设备存取。为了增强安全性，可以管理虚拟卡以使该卡可以在启用和禁用状态之间切换。与其中礼品卡可由持有该礼品卡的任何人使用的现有系统相比，所述方法提供了定期身份验证以允许对虚拟卡的用户进行选择级别的身份识别。身份验证的级别可以基于商户的系统、预定的身份验证规则或安全性规则，和 / 或用户计算设备。卡的状态的管理（在启用状态和

禁用状态之间切换)增加了虚拟卡的安全性级别。应理解,卡的状态的管理可以由远程服务器通过通信链接,诸如因特网处理,从而虚拟卡管理者可以是远程服务器。在其他系统中,卡的状态的管理可以直接地或至少部分地由关联于虚拟卡的移动计算设备处理。因此,在一些示例中,虚拟卡管理者可以保持在移动计算设备中或至少部分地保持在移动计算设备上。

[0077] 现参考图 4,示出根据本发明的实施例的用于管理虚拟卡的方法 400 的示例处理流程。应理解,处理流程本质上是示例性的且在其他示例中可以使用大量的其他处理流程。在 402 执行初步设置过程。可以在产品和服务系统得到处理来自移动计算设备的虚拟卡的能力之前,执行该初步设置过程。该初步设置过程可以包括在 404 集成卡服务提供者与虚拟卡管理者。集成可以按多种方式实现。在一个示例中,该卡服务提供者可以具有允许虚拟卡管理者与卡服务提供者通信的应用程序接口(API)或其他方法。在这样的示例中,虚拟卡管理者可以使用集成连接器引擎链接包括在虚拟卡管理者中的软件系统与卡服务提供者 API 或其他软件通信标准。然而,在其他实施例中,卡服务提供者可以使用由虚拟卡管理者提供的 API 或其他软件。在其他示例中,卡服务提供者可以通过用于通信的其他方法或系统提供虚拟卡管理者。

[0078] 接下来,在406,该方法包括登录到由虚拟卡管理者提供的管理区域。例如,可以允许产品和服务系统和 / 或卡服务提供者存取上文参考图 2A 所述配置为调整一个或多个身份验证规则的管理模块。因此,在 408,该方法包括建立虚拟卡使用的身份验证规则以及其他规则。因此,用户(如,虚拟卡管理者代表、卡服务提供者代表、产品和服务系统代表)可以设置身份验证规则。然而,在其他示例中,可以自动地建立身份验证规则。以此方式,可以提供用于每个产品和服务系统和 / 或卡服务提供者的虚拟卡的身份验证规则的定制。因此,每个产品和服务系统和 / 或卡服务提供者可以定制虚拟卡管理系统以匹配其特定需要。

[0079] 建立虚拟卡使用的身份验证规则可以包括在 410 调整身份验证规则的集合,在 412 保存身份验证规则集合,及在 414 执行身份验证规则。因此,在一些示例中,可以根据通过产品和服务系统和 / 或卡服务提供者建立的身份验证规则集合,对一个或多个虚拟卡进行身份验证。虚拟卡管理者可以根据卡服务提供者和 / 或产品和服务系统身份验证规则集合及卡服务提供者能力来管理身份验证规则的转换。如上所述,身份验证规则可以决定选择性地启用虚拟卡的方式。

[0080] 接下来,在416,该方法包括生成虚拟卡。虚拟卡可以在线生成,在对应于产品和服务系统的实体位置生成,或在移动计算设备上生成。应理解,当生成虚拟值卡(如,虚拟礼品卡,或虚拟奖励卡)时,可以在虚拟卡管理系统内生成对应于虚拟礼品卡的货币值。另外,虚拟卡的生成还可以包括生成身份识别特性,诸如身份识别号码、条码、身份识别图像(如,卡用户的照片)、卡特权等。

[0081] 应理解,在示例实施例中,当生成(如,颁发)虚拟卡时,虚拟卡管理者可以设定卡为暂时禁用的状态。如上所述,虚拟卡可以为禁用状态但为“激活”的虚拟卡。暂时禁用虚拟卡可以保护持卡人免受欺诈性使用。此外,当通过虚拟卡引擎可以存取虚拟卡、向产品和服务系统出示虚拟卡等时,虚拟卡引擎可以与虚拟卡管理者通信以在紧接使用虚拟卡之前将虚拟卡设定为启用状态。

[0082] 在 418,该方法可以包括将虚拟卡递送(如,增加)到移动计算设备上的虚拟卡引

擎。应理解，在其他示例中，虚拟卡引擎可以不包括在移动计算设备中。重要的是注意，可以通过 POS 软件、卡服务提供者，或其他基于远程或本地的应用程序提供实用程序，以允许产品和服务系统具有快速容易地将虚拟卡递送到虚拟卡引擎从而递送到移动计算设备的能力。产品和服务系统还可向用户递送虚拟卡的实体表示（如，标准的塑料卡），然后可将该虚拟卡从移动设备软件传输到其移动计算设备。

[0083] 向移动计算设备上的虚拟卡引擎递送虚拟卡可以包括在 420 将虚拟卡管理者连接到卡服务提供者。如果提供者端关联卡配置文件未包括在卡服务提供者上，则该方法可以包括在 422 生成提供者端关联卡配置文件。此外，向虚拟卡引擎递送虚拟卡还可以包括在 424，基于通过产品和服务系统和 / 或卡服务提供者建立的身份验证规则选择性地禁用虚拟卡，以及在 426 通过到电子邮件的链接或代码、可扩展标记语言（XML）、短消息服务（SMS）、MMX 指令、无线应用协议（WAP），各种开放端口或其他适合的软件代码或链接，将虚拟卡递送到移动计算设备。

[0084] 图 5 示出可用于生成虚拟卡并将虚拟卡发送到移动计算设备的方法 500 的示意图。应理解，如上所述，移动计算设备可以包括个人计算机、膝上型计算机、便携式媒体播放器等。

[0085] 在 502，该方法包括请求虚拟卡以用于递送。可以在关联于产品和服务系统的实体位置、在移动计算设备上、通过因特网，或通过其他适合的系统做出该请求。在一些示例中，请求虚拟卡可以包括将卡数据从塑料卡传输到虚拟卡引擎。

[0086] 在 504，该方法包括确定产品和服务系统是否在递送之前要求虚拟卡的身份验证。身份验证的要求可以由通过产品和服务系统和 / 或虚拟卡管理者建立的预定的身份验证规则的集合决定。如果产品和服务系统不要求在递送之前虚拟卡的身份验证（在 504 为否），则该方法前进到 506，在 506 该方法包括将虚拟卡递送到虚拟卡引擎（如，移动计算设备）。在一些示例中，虚拟卡管理者可以响应于虚拟卡的递送，自动地增加虚拟卡数据到管理者端关联卡配置文件或帐号。

[0087] 然而，如果产品和服务系统要求在递送之前进行虚拟卡的身份验证（在 504 为是），则该方法包括在 507，接收对应于移动计算设备的身份识别数据（如，身份验证数据）以及在 508 将身份识别数据传输到移动计算设备、产品和服务数据库，和 / 或虚拟卡管理者。身份识别数据可以包括电话号码、电子邮件地址、身份验证信息、唯一标识符（如，身份识别号码）等。另外，产品和服务数据库可以是可执行的软件。例如，产品和服务数据库可以包括 POS 系统接口、万维网接口、卡服务提供者接口，及可配置为传送身份识别数据的其他软件中的至少一个。应理解，当从作为虚拟卡的预期接收者的移动计算设备做出递送虚拟卡的请求时，假设已经在虚拟卡管理者内创建帐号且因此在这样的示例中不将身份识别信息发送到虚拟卡管理者。

[0088] 接下来，在 510，该方法包括确定是否通过虚拟卡管理者识别出身份识别数据。识别的确定可以基于预定的身份验证规则的集合和 / 或卡服务提供者的能力。如果身份识别数据未由虚拟卡管理者识别出（在 510 为否），则该方法进入 512，在 512 确定是否可以查看虚拟卡而不设置虚拟卡引擎。如果不设置虚拟卡引擎就不能查看虚拟卡（在 512 为否），则该方法进入 514，在 514 该方法包括允许设置虚拟卡引擎。允许设置虚拟卡引擎可以包括通过电子邮件或其他适合的消息服务将附件或链接发送到便携式计算设备。然而，应理解，

替代技术可以用于允许虚拟卡引擎的设置。例如，可以通过实体邮件服务邮寄虚拟卡引擎。接下来，在 516，该方法包括在移动计算设备上设置虚拟卡引擎。可以用于在移动计算设备上设置虚拟卡引擎的示例方法在图 6 中示出，如下文详述。

[0089] 如果身份识别数据由虚拟卡管理者识别出（在 510 为是），或者如果不设置虚拟卡引擎也可以查看虚拟卡（在 512 为是），或在 516 之后，该方法包括在 518 确定是否应将虚拟卡设定为禁用状态。如上所述，禁用状态可以是禁止虚拟卡的使用的状态。

[0090] 如果确定应将虚拟卡设定为禁用状态（在 518 为是），则该方法进入 520，在 520 该方法包括禁用虚拟卡。在 520 之后，该方法进入 506。然而，如果确定虚拟卡不应设定为禁用状态（在 518 为否），则该方法进入 506。

[0091] 应理解，可以基于通过移动计算设备、产品和服务系统，和 / 或卡服务提供者系统建立或调整的身份验证规则的集合，将虚拟卡设定为禁用状态。如上所述，身份验证规则可以包括持久启用规则、存取规则、卡履约规则、兑换规则、卡类型规则，及基于时间的规则中的一个或多个。

[0092] 图 6 示出可用于设置基于客户机或基于浏览器的虚拟卡引擎的方法 600 的示意图。基于客户机的虚拟卡引擎可以在移动计算设备上存储、存取、和执行。另一方面，基于浏览器的虚拟卡引擎可以通过浏览器在因特网上或其他适合的联网系统上存取。

[0093] 在 602，确定是否应在移动计算设备上设置虚拟卡引擎。如果确定不应在移动计算设备上设置虚拟卡引擎（在 602 为否），该方法结束。然而，如果确定应在移动计算设备上设置虚拟卡引擎（在 602 为是），该方法进入 604，在 604 该方法包括确定是通过浏览器还是客户机执行虚拟卡引擎。换言之，确定虚拟卡引擎是作为基于万维网的应用程序还是客户机端应用程序执行。

[0094] 如果确定通过客户机（如，移动计算设备）执行虚拟卡引擎，该方法进入 606，在 606 该方法包括将虚拟卡引擎加载到移动计算设备上。虚拟卡引擎可以通过因特网下载、通过移动计算设备的接口（如，通用串行总线端口、CD-ROM 驱动器等）上传等。例如，可以在电子邮件中提供虚拟卡引擎链接。该链接可以告知用户将该虚拟卡引擎增加到其移动计算设备的指示。这可以包括在可在该设备上查看虚拟卡之前（根据围绕产品和服务系统的该虚拟卡的规则）将虚拟卡引擎安装到该移动计算设备上。

[0095] 在一些示例中，虚拟卡引擎可以加上密钥以在设备上安装虚拟卡引擎。在一个示例中，唯一的和 / 或加密的唯一的密钥可以存储在管理者端关联卡配置文件或在虚拟卡管理者内的其他适合的存储库中，并可以连接到关联的虚拟卡引擎。可以识别具体的安装或使用移动软件平台上提供的其他唯一的密钥以区分虚拟卡引擎是来自该设备的。

[0096] 然而，如果确定虚拟卡引擎程序是通过浏览器执行的，该方法进入 608，在 608 通过因特网或其他适合的网络存取基于浏览器的虚拟卡引擎。

[0097] 在 606 和 608 之后，该方法进入 610，在 610 该方法包括建立用户身份，诸如用户名和 / 或密码。可以颁发身份验证码以校验虚拟卡、用户帐号和 / 或移动计算设备。在一些示例中，可以将对应于移动计算设备的虚拟卡管理者内的电话号码或其他适合的身份识别数据与使用中的移动计算设备的电话号码或其他识别数据进行检查比对。每个产品和服务系统可以设定不同级别的身份验证。例如，身份验证码可以颁发到电子邮件以校验电子邮件帐号。身份验证码还可以颁发到具有帐号设置信息的移动计算设备。因此可以通过电

话、SMS 或 MMS 消息等颁发该码。在又一个示例中，身份验证码可以颁发到邮件帐号，诸如常规的纸质邮件地址，以建立特定的会员级别。此外，在其他示例中，用户可以要求不进行上述任何身份验证。在虚拟卡引擎中该级别的对用户的身份验证可以允许代表产品和服务系统从移动计算设备上容易地建立会员卡或其他虚拟卡，因为用户（如，用户的移动计算设备）已预先经过身份验证。

[0098] 接下来在 612，该方法包括颁发身份验证码以在虚拟卡管理者内（如，在管理者端关联卡配置文件内）校验帐号。在一些示例中，身份验证码可以颁发给移动计算设备。校验可以包括用识别该请求的码检查存档的对应于移动计算设备的存储的信息。以此方式，可以实现虚拟卡是否属于用户的移动（或固定）计算设备的校验。

[0099] 接下来在 614，该方法包括执行校验过程。校验过程的执行可以包括登录到虚拟卡管理者内（如，管理者端关联卡配置文件内）的帐号和通过输入安全码到移动计算设备中来校验该帐号。

[0100] 接下来在 616，该方法包括确定是否已校验该帐号。在一些示例中，帐号的校验包括登录到帐号中并输入颁发的安全码。然而在其他示例中，可以使用替代的技术来校验帐号。

[0101] 如果确定该帐号未通过校验（在 616 为否），该方法进入 618，在 618 该方法包括禁止使用虚拟卡。在 618 之后，该方法结束。然而，如果确定该帐号通过校验（在 616 为是），该方法进入 620，在 620 允许使用虚拟卡。在一些示例中，当允许使用虚拟卡时，可以从虚拟卡引擎提供能力以可能购买、充值到虚拟卡、转换虚拟卡的权利，或转换塑料卡为虚拟卡。

[0102] 接下来，在 622，该方法包括通过虚拟卡管理者跟踪移动计算设备。当已对移动设备和用户进行身份验证时，跟踪移动计算设备允许虚拟卡管理者识别移动计算设备。取决于身份验证规则的产品和服务集合，产品和服务系统可以要求用户已经从接下来请求使用虚拟卡的同一移动计算设备进行身份验证。一旦帐号已经设置并经身份验证，虚拟卡引擎就可以接收要求任何级别的身份验证的虚拟卡。因此，一旦已增加持卡人，定期身份验证就可用于基于上述校验过程校验使用虚拟卡，诸如会员卡的人在从有资格进行该操作的设备上进行操作。

[0103] 因此，在一个示例实施例中，当用户使用基于浏览器的虚拟卡引擎时，虚拟卡管理者可以将帐号与设置了虚拟卡引擎的移动计算设备关联。可以通过使用 cookie（储存在用户本地终端上的数据）、网际协议（IP）地址或可放置在移动计算设备上的其他唯一标识进行该关联。虚拟卡管理者可以查找该 cookie（cookie 中的加密的密钥）、IP 地址或其他唯一标识，其将告知虚拟卡管理者所使用的移动计算设备是设置帐号的移动计算设备。例如，虚拟卡管理者可以在移动计算设备上存储加密的或未加密的密钥，当建立帐号时该密钥被发送到虚拟卡管理者，然后每次请求身份验证发生时被发送。因此，在一些实施例中，只有有资格的设备能够对虚拟卡进行身份验证，以减少和 / 或消除欺诈性虚拟卡的兑换。

[0104] 在一些示例中，如果用户尝试从未由虚拟卡管理者识别出的移动计算设备登录到帐号（如，管理者端关联卡配置文件），则用户可以请求执行附加的身份识别方法。这些附加的身份识别方法可以包括回答用户在初始帐号设置时建立的安全问题。在一些实施例中，未识别出移动计算设备会造成用户必须通过先前描述的方法再次重新建立该用户。可以询问用户是否希望改变其对该移动计算设备的安全性或将该移动计算设备重新建立为连接

到其帐号(如,管理者端关联卡配置文件)。还可能用户可以持有不要求该级别的身份验证的卡,其中用户连接到移动计算设备而不是只连接到其帐号。如果是这样的情况,则可以从在管理者端关联卡配置文件或用于存储虚拟卡数据的其他适合的存储库中连接到帐号的移动计算设备之外的其他移动计算设备提供这样的虚拟卡。也可能虚拟卡可以由两个不同的虚拟卡引擎存取。例如,夫妻可以共享相同的喜互惠(Safeway)奖励卡以使用会员特权。

[0105] 在浏览器模型下,用户可以增加虚拟卡到在其移动计算设备上的"收藏夹"以快速有效地从该移动计算设备上开启该虚拟卡。他们还可能希望通过 SMS 或 MMS 发出链接到其电话以允许他们快速地从浏览器中调出该虚拟卡。在该情况下,增加的"收藏夹"链接可以具有考虑由该卡的产品和服务系统指定的安全性的所涉及的逻辑,并确定用户是否可以立即查看该虚拟卡而不进行身份验证、立即查看虚拟卡(虚拟卡管理系统注意到表示他们在从与其帐号相关的设备上进行查看的 cookie)、查看虚拟卡但必须验证用户名和密码,和/或查看虚拟卡但必须进行身份验证且该设备必须是关联于其在管理者端相关卡配置文件或其他适合的存储库中的帐号的设备。

[0106] 回到图 4,在 428,该方法包括在移动计算设备,诸如移动电话的显示上呈现该虚拟卡。因此,用户可以通过虚拟卡引擎存取虚拟卡并查看虚拟卡。图 7 － 9 示出包括显示 702 的示例性移动计算设备 700。移动计算设备还可以包括适合的输入设备,诸如触摸屏 704 和各种按钮 706,以允许用户操纵移动计算设备。应理解,在一些示例中,触摸屏可以呈现键盘以有助于字母数字的输入。应理解,各种按钮、触摸输入等可以用于在显示的内容窗口之间进行导航。例如,可以提供"后退"按钮以允许用户导航到先前的窗口,且可以提供"增加"按钮以导航到配置为增加虚拟卡到虚拟卡引擎的内容窗口。此外,在各种图形、图标等上方执行的触摸输入可以允许存取对应于选择的图形或图标的特征。

[0107] 移动计算设备还可以包括存储在存储器中以用于通过一个或多个处理器实现上述功能的虚拟卡引擎。该存储器、处理器、以及附加的电子部件可以驻留在便携式计算设备 700 的设备主体 708 内或机载于其上。然而,在其他示例中,可以通过浏览器存取虚拟卡引擎。虚拟卡引擎可以配置为在显示上呈现多个虚拟卡并修改虚拟卡的排列及虚拟卡的外观。

[0108] 在一个示例中,虚拟卡可以根据卡类型(如,虚拟礼品卡、虚拟忠诚卡)组织在显示上,如图 7 所示。在其他系统中,可以基于商户、使用日期等组织卡。用户可以选择虚拟礼品卡,因此虚拟礼品卡可以呈现在显示上,如图 8 所示。因此,用户可以整理多个虚拟卡。然后用户可以选择特定的虚拟卡用于查看。选择的虚拟卡可以呈现在显示上,并带有虚拟卡信息,诸如个人身份识别号码(PIN)、虚拟卡的值、条码、虚拟卡的状态(如,开启或关闭)等,如图 9 所示。在一些示例中,用户可以通过按钮 710 在触摸屏上或其他适合的输入设备上调整虚拟卡的状态。以此方式,用户可以选择虚拟卡的启用,从而在虚拟卡管理者内触发选择性启用(如,设定虚拟卡为启用状态)。或者,在其他实施例中,虚拟卡的状态可以仅呈现在显示上且可以禁止通过用户交互对虚拟卡的状态进行操纵。此外,应理解,附加的技术可以用于触发选择性启用。例如,当存取(如,选择)虚拟卡以用于在移动计算设备上查看时,可以触发选择性启用,从而将虚拟卡设定为启用状态。

[0109] 回到图 4,在通过移动计算设备查看虚拟卡之后,方法 400 可以包括在 430 向卡服务提供者和/或产品和服务系统出示虚拟卡。虚拟卡可以对应于卡服务提供者和/或产品

和服务系统。即，可以通过卡服务提供者和 / 或产品和服务系统存储和 / 或存取关联于虚拟卡的卡数据(如，ID 号码和值数据)。

[0110] 在一个非限制性示例中，向卡服务提供者和 / 或产品和服务系统出示虚拟卡可以包括在 432，选择虚拟卡以向产品和服务系统显示。在一些示例中，在选择虚拟卡之后，通过产品和服务系统询问对虚拟卡的预期使用进行校验的消息可被发送到移动计算设备。向卡服务提供者和 / 或产品和服务系统出示虚拟卡还可以包括在 434，通过适合的通信方法(如，有线或无线通信)发送虚拟卡数据和身份验证信息到虚拟卡管理者。

[0111] 在一些实施例中，虚拟卡引擎可以与用户交互以确认关于虚拟卡的使用(如，用户是否意图使用虚拟卡以用于与产品和服务系统进行交易)的用户意图。接下来，用户可以通过输入设备触发虚拟卡的启用或替代地可以自动进行启用。

[0112] 虚拟卡引擎的用户还可以在虚拟卡引擎内选择各种设定，诸如一个或多个身份验证规则。因此，用户可以根据其喜好定制虚拟卡引擎。然而，在其他示例中，可以禁止由虚拟卡引擎进行身份验证规则的选择和 / 或调整。此外，在一些示例中，虚拟卡引擎还允许用户忽略选择性启用。因此，如果他们不介意承担可能导致卡的欺诈性使用的风险，用户可以选择将虚拟卡设定为永久启用状态以加速交易过程。然而，在其他示例中，产品和服务系统和 / 或卡服务提供者可以禁止永久启用状态的选择以保持期望的安全性级别。移动计算设备和虚拟卡管理者之间的通信可以经由基于万维网浏览器或基于客户机的应用程序通过通信的标准端口进行，因为如上所述这是标准的通信方法。

[0113] 此外，在一些实施例中，用户、卡服务提供者，和 / 或产品和服务系统可以用 MMS 或 SMS 呼叫或其他身份验证激活步骤触发选择性启用。例如，用户、卡服务提供者，或产品和服务系统可以作出请求，然后在返回的请求之后用其密码进行身份验证。在一些系统中，产品和服务系统还可以通过其 POS、卡服务提供者、基于浏览器的解决方案或其他软件具有跳过能力，以允许产品和服务系统跳过未成功进行身份验证的虚拟卡。替代地，可以呼叫支持电话号码以到达语音服务系统或虚拟卡服务代表，以使可以对跳过进行授权。多种方法可以用作主要的或备份的解决方案。应注意，如果身份验证不是标准身份验证，虚拟卡管理者可以记录所使用的身份验证的类型。然而，在其他示例中，虚拟卡管理者可以不记录所使用的身份验证的类型。

[0114] 当由虚拟卡管理者接收到正确的身份验证时，可以在虚拟卡管理者存储库(如，管理者端关联卡配置文件)中识别使用中的虚拟卡。之后，虚拟卡管理者可以在 436 选择性地启用虚拟卡。因此，虚拟卡为启用状态。此外，可以响应于选择性启用开启定期身份验证。

[0115] 在一些实施例中，可以在下述情况中的一个或多个下选择性地启用虚拟卡：已发起虚拟卡引擎以发起过程(如，交易)、虚拟卡身份识别(如，移动计算设备身份识别)与用户的身份验证匹配，虚拟卡引擎已通过由卡服务提供者和 / 或产品和服务系统要求的身份验证级别，且没有违反其他身份验证规则。然而，在其他实施例中，可以基于不同的准则选择性地启用虚拟卡。

[0116] 接下来在 438，该方法可以包括暂时启用虚拟卡。具体地，在一些实施例中，可以和卡服务提供者进行通信以暂时启用虚拟卡。例如，虚拟卡管理者可以和卡服务提供者进行通信以“开启”定期身份验证，从而以由卡服务提供者支持的方法“暂时启用”虚拟卡。以此方式，卡服务提供者可以准备好使用虚拟卡。

[0117] 在一些示例中，如果违反了一个或多个身份验证规则或来自虚拟卡引擎（如，移动计算设备）的身份验证不被接受，则虚拟卡管理者可以传送失败到虚拟卡引擎且可以在产品和服务系统内禁止交易。此外在一些示例中，违反身份验证规则会导致虚拟卡保持在暂时禁用状态，直到满足身份验证规则，从而通过产品和服务系统禁止虚拟卡使用。

[0118] 在一些示例实施例中，当用户希望与产品和服务系统进行交易时，移动计算设备可能未可通信地连接到虚拟卡管理者，因此当预期到将来的交易时，可以在移动计算设备可通信地链接到虚拟卡管理者时选择性地启用虚拟卡。在一些示例中，可以确定阈值启用时间间隔以允许用户在启用虚拟卡之后有充足的时间使用虚拟卡。因此，身份验证规则可以包括基于时间的规则，其中确定阈值启用时间间隔。如果超过阈值启用时间间隔，则可以将虚拟卡设定为禁用状态。启用时间间隔可以在启用虚拟卡时开始。应理解，在一些实施例中，产品和服务系统可以确定基于时间的规则的参数（如，阈值启用时间间隔）。例如，产品和服务系统可以选择 1 分钟或 20 分钟的间隔。然而，在其他示例中，虚拟卡管理者可以设定基于时间的规则的参数。

[0119] 再次参考图 4，该方法可以包括在 440，输入虚拟卡数据到产品和服务系统中（如，POS 系统）。例如，可以手动地将虚拟卡身份识别号码输入到 POS 系统中和 / 或虚拟卡条码可以呈现在移动计算设备上并扫描到 POS 系统中。应理解，输入卡身份识别信息的任何适合的方法都可以用于识别呈现在移动计算设备上的虚拟卡。可以增加CID、安全码或变长度和字符的多个安全码以允许附加的安全性，或作为代表关联的卡服务提供者的定期身份验证一部分。可以使用各种通信方法，包括但不限于，蓝牙、远程识别器，或可将虚拟卡身份识别从移动或电子设备传送到产品和服务系统（如，POS 软件 / 硬件）的其他有线和无线技术。

[0120] 接下来，在 442，该方法可以包括运行交易和 / 或身份验证。在一些示例中，虚拟卡引擎可以发起身份验证。然而，在其他示例中，替代系统可以发起身份验证。如上所述，通过虚拟卡引擎存取和查看虚拟卡可以触发虚拟卡的暂时启用。这样的安全发起可以对于虚拟卡的用户不可见。

[0121] 运行交易和 / 或身份验证可以包括在 444 在包括在产品和服务系统中的 POS 系统和卡服务提供者之间发起通信，以及在 446 发送“成功”身份验证到 POS 系统。因此，POS 系统可以接收“成功”身份验证。在一些实施例中，虚拟卡管理者，使用由产品和服务系统设定的预定的身份验证规则，可以紧接虚拟卡的使用之前通过包括在产品和服务系统中的终端与卡服务提供者通信以允许使用虚拟卡。

[0122] 在其他实施例中，运行交易和 / 或身份验证可以包括在产品和服务系统（如，POS 系统）和卡服务提供者之间建立通信。接下来，卡服务提供者可以发起二次身份验证过程。然后卡服务提供者可以发起与虚拟卡管理者的通信。然后可以通过虚拟卡管理者校验身份验证。然后可以将对身份验证的校验（如，成功或失败）发送到卡服务提供者及产品和服务系统，从而允许或不允许交易。然而，应理解，可以使用替代技术运行交易和 / 或身份验证。例如，卡服务提供者可以发起启用和禁用。发起检查有效虚拟卡将要求卡服务提供者作出对虚拟卡管理者的第二次呼叫或通信，以在首先校验其自身的确认准则得以满足的之后确认身份验证。在一个示例中，卡服务提供者可以查询虚拟卡管理者以确定虚拟卡管理者是否考虑到根据确立的身份验证规则的身份验证。还应注意，虚拟卡管理者不需要在卡服务提供者和 / 或产品和服务系统处“切换开启或关闭”该卡。相反，卡服务提供者和 / 或产品

和服务系统可以与虚拟卡管理者通信以校验身份验证的规则，然后虚拟卡管理者返回成功或失败的指示符。

[0123] 应理解，在处理交易之后，可以通过虚拟卡管理者和 / 或卡服务提供者调整虚拟卡值。虚拟卡的值的调整可以包括减去货币值或存取会员特权。

[0124] 接下来，在 448，该方法可以包括向虚拟卡管理者通知虚拟卡的可能的使用。具体来说，在非限制性示例中，向虚拟卡管理者通知可能的使用可以包括在 450 通过虚拟卡引擎向虚拟卡管理者警告可能的交易和在 452 由虚拟卡管理者存取关于虚拟卡的到期的身份验证规则。另外，虚拟卡管理者可以匹配虚拟卡与对应的卡服务提供者。向虚拟卡管理者通知可能的使用还可以包括在 454 暂时禁用虚拟卡。

[0125] 特别是，在一个示例实施例中，可能发生交易的终止(如，通过移动计算设备关闭了虚拟卡引擎)。可以由虚拟卡引擎、移动计算设备、卡服务提供者等向虚拟卡管理者通知终止。例如，虚拟卡管理者可以在虚拟卡不再由虚拟卡管理者使用之后尝试定期地查找对于卡服务提供者的卡使用。替代地，或附加地，虚拟卡管理者可以等待身份验证窗口关闭。响应于交易的终止，虚拟卡管理者可以选择性地禁用虚拟卡并更新管理者端关联卡配置文件。然而，在其他示例中，其他技术可以用于禁用虚拟卡。

[0126] 接下来，在 456，该方法可以终止身份验证。步骤 458、460 和 462 提供终止身份验证的示例。在 458，该方法可以包括存取(如，检索)新的虚拟卡值。在 460，该方法还可以包括在虚拟卡管理者处将该卡设定为禁用状态。接下来，在 462，该方法还可以包括发送卡使用细节到移动计算设备。在一些实施例中，可以不通知该虚拟卡管理者暂时禁用该卡。在这样的情况下，当未向虚拟卡管理者通知卡禁用时，虚拟卡管理者可以通过可用的任何方法监视虚拟卡的使用。

[0127] 接下来，在 464，该方法还可以包括在移动计算设备上显示虚拟卡使用数据。例如，可以显示更新的值数据以及通过交易修改的附加的卡数据。

[0128] 应理解，多个上述过程也可以用于在电子商务中经递送以供使用的存储值。因此，用户可以存取来自移动计算设备的虚拟卡然后登录到计算机中并在电子商务世界中使用该虚拟卡，因为该虚拟卡仅从该设备进行了身份验证。通过允许产品和服务系统使卡“禁用”，然后紧接将卡用于电子商务交易之前“启用”该卡，虚拟卡管理者可以帮助确保正确的人在根据由产品和服务系统建立的规则使用虚拟卡。此外，虚拟卡管理者可以配置为识别分配给该虚拟卡的计算机并校验真实性。如果用户切换计算机或需要使用来自另一计算机的值，则虚拟卡管理者可以用新的 PIN 码重新颁发存储值到记录的电子邮件地址，因此在允许用户查看虚拟卡之前对用户重新进行身份验证。查看虚拟卡可以有效地允许卡在电子商务环境中的使用。

[0129] 此外，应理解，在一些实施例中，可以在移动计算设备上管理虚拟卡管理者服务和 / 或身份验证(如，胖客户机方案)。因此，当前由虚拟卡管理者保存的逻辑可以直接地存储在移动计算设备上，以允许其确定与哪个卡服务提供者通信或其他较高级别的决策能力。胖客户机方案可以例如在其驻留的设备上保持卡身份验证，并能够基于使用中的虚拟卡实现各种虚拟卡管理功能(如，选择性启用)。以此方式，做出通常可由外部虚拟卡管理者做出的决策的移动设备可以转移到移动计算设备自身。然而，在其他实施例中可以利用其他技术以保持身份验证。此外，在其他实施例中，可以不使用胖客户机方案。

[0130] 在一些示例系统中，可以存储虚拟卡用户数据以由虚拟卡管理者、卡服务提供者或移动计算设备的用户中的一个或多个使用。例如，可以汇编并整理关于使用、持卡人类型、持卡人维护该卡的时间长度，及关于持卡人的其他信息的细节，以向商户和／或其他产品和服务系统提供统计数据和／或持卡人信息。

[0131] 上述系统和方法允许基于可通过产品和服务系统建立的预定的身份验证规则，通过中间系统（如，虚拟卡管理者）快速地启用和禁用虚拟卡，从而提高虚拟卡管理系统的安全性。因此，产品和服务系统可以构建围绕其卡项目的身份验证规则以保护其持卡人并防止损失或欺诈。卡服务提供者、产品和服务系统，及虚拟卡引擎之间的通信可以达到另一级别，以作为该安全性的结果允许新级别的促销能力和与其持卡人的交互。该新级别的安全性和身份验证可以为涉及的所有各方提供安全交易体验。

[0132] 相信上文公开的内容涵盖了具有独立实用性的多个独特的发明。虽然这些发明中的每个都以其优选的形式公开，但在本文中公开和示出的具体实施例不应视为具有限制意义，因为大量的变体是可能的。本发明的主题包括本文公开的各种元素、特征、功能和／或属性的所有新颖和非显而易见的组合及子组合。

[0133] 在特征、功能、元素，和／或属性的各种组合及子组合中具体实现的发明可以在相关申请中请求保护。这样的权利要求无论是否涉及不同的发明或涉及相同的发明、无论在范围上与任何原始权利要求相比不同、更宽、更窄或相同，都应视为包括在本文公开的发明的主题之内。

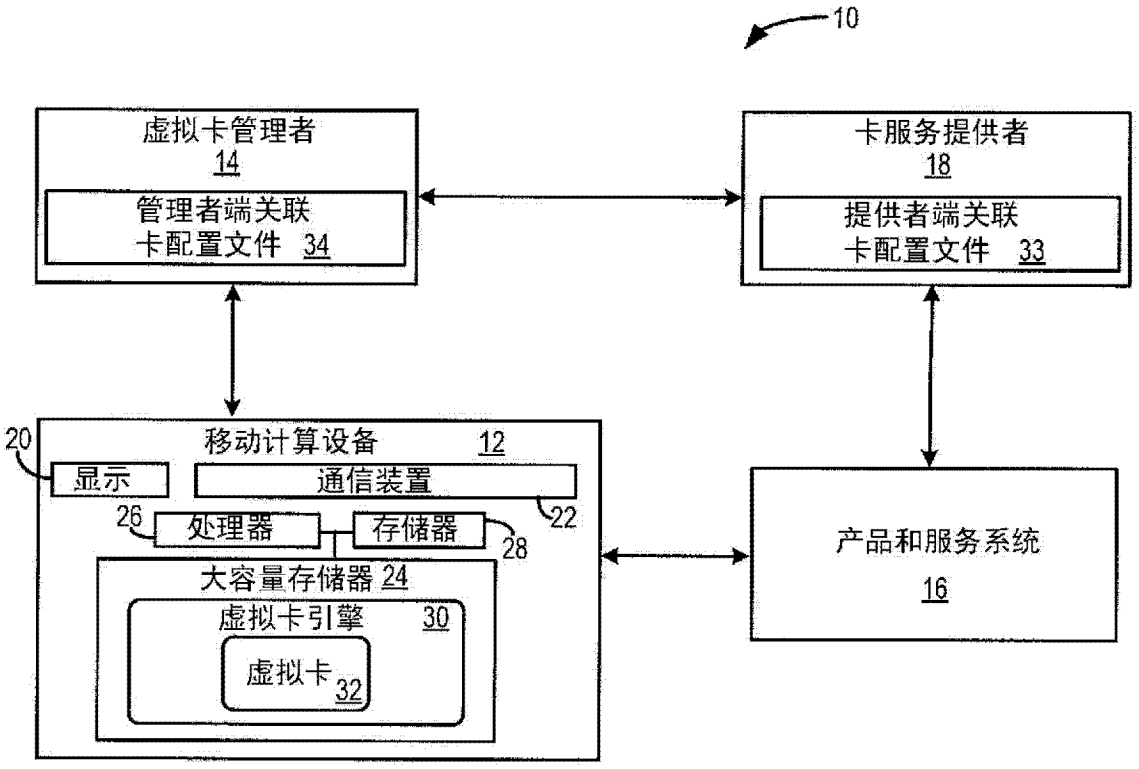

10
虚拟卡管理者
14
管理者端关联
卡配置文件 34
卡服务提供者
18
提供者端关联
卡配置文件 33
20
移动计算设备 12
显示
通信装置
22
26
处理器
存储器
28
大容量存储器 24
虚拟卡引擎 30
虚拟卡 32
产品和服务系统
16

图 1

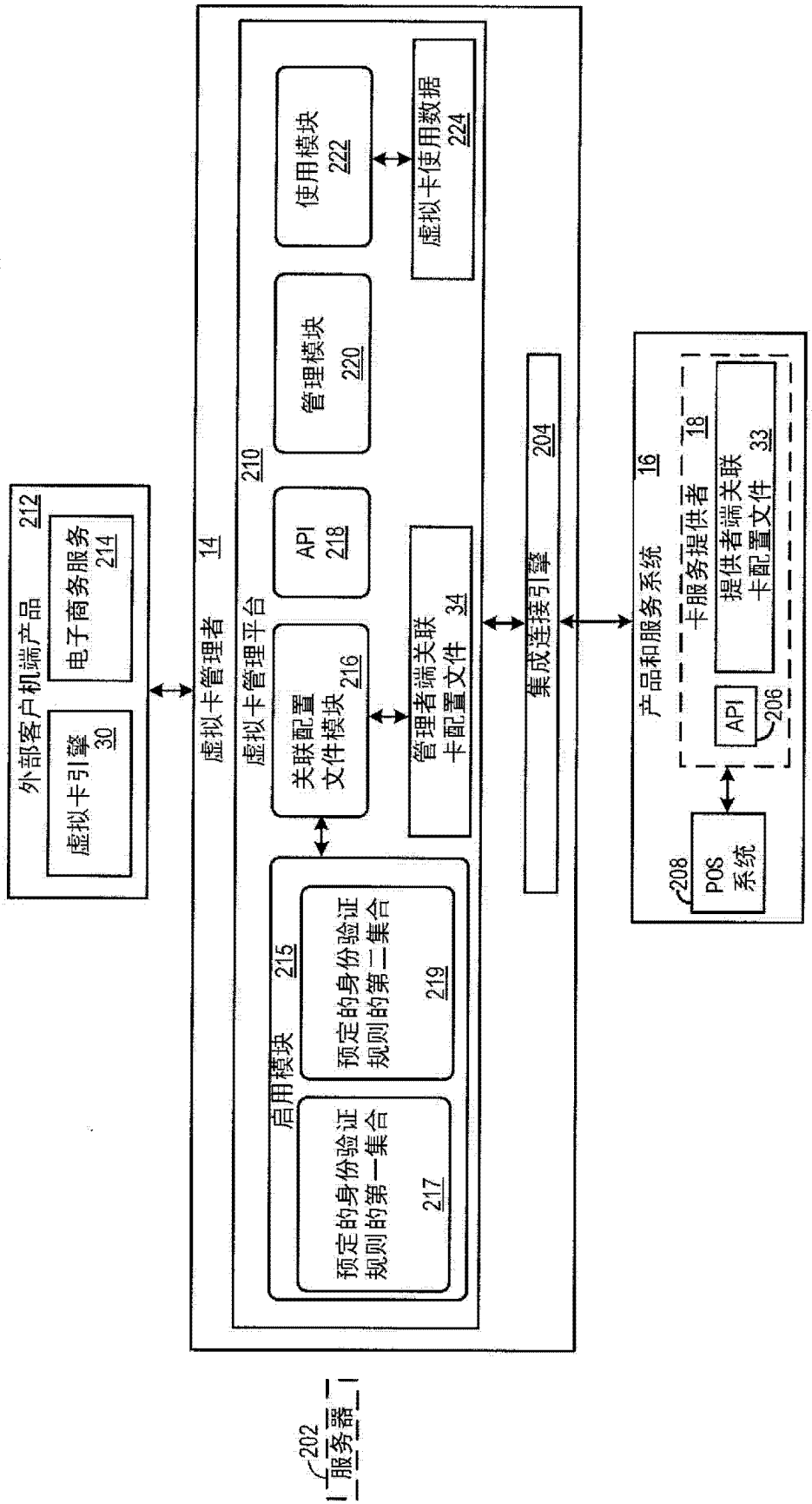

10
外部客户机端产品 212
虚拟卡引擎 30
电子商务服务 214
虚拟卡管理者 14
虚拟卡管理平台 210
关联配置文件模块 216
API 218
管理模块 220
使用模块 222
虚拟卡使用数据 224
管理者端关联卡配置文件 34
启用模块 215
预定的身份验证规则的第一集合 217
预定的身份验证规则的第二集合 219
集成连接引擎 204
产品和服务系统 16
卡服务提供者 18
API 206
提供者端关联卡配置文件 33
POS 系统 208
服务器 202

图 2A

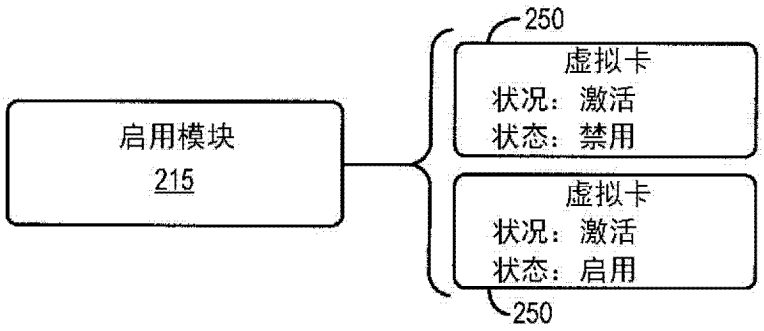


图 2B

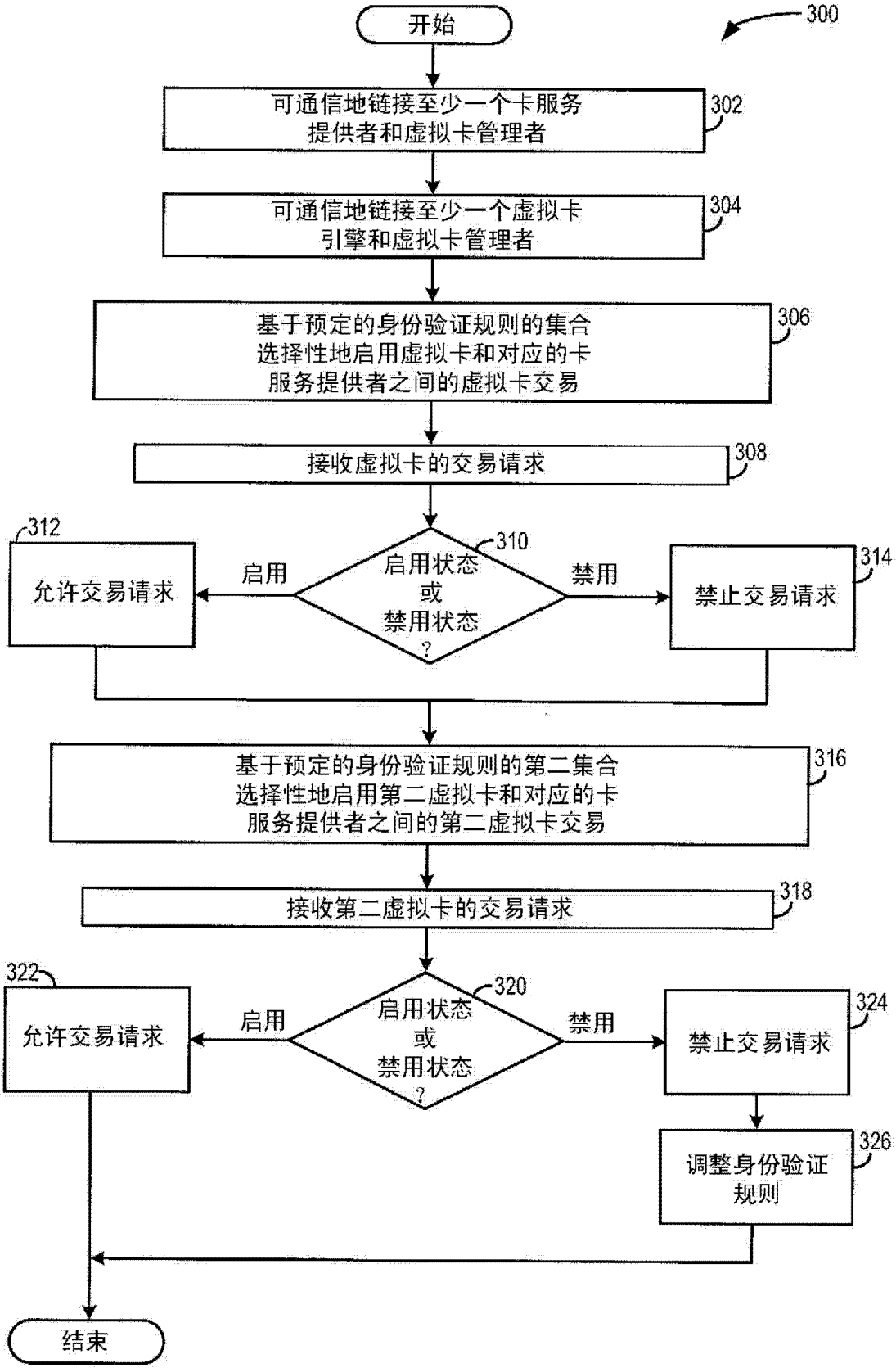
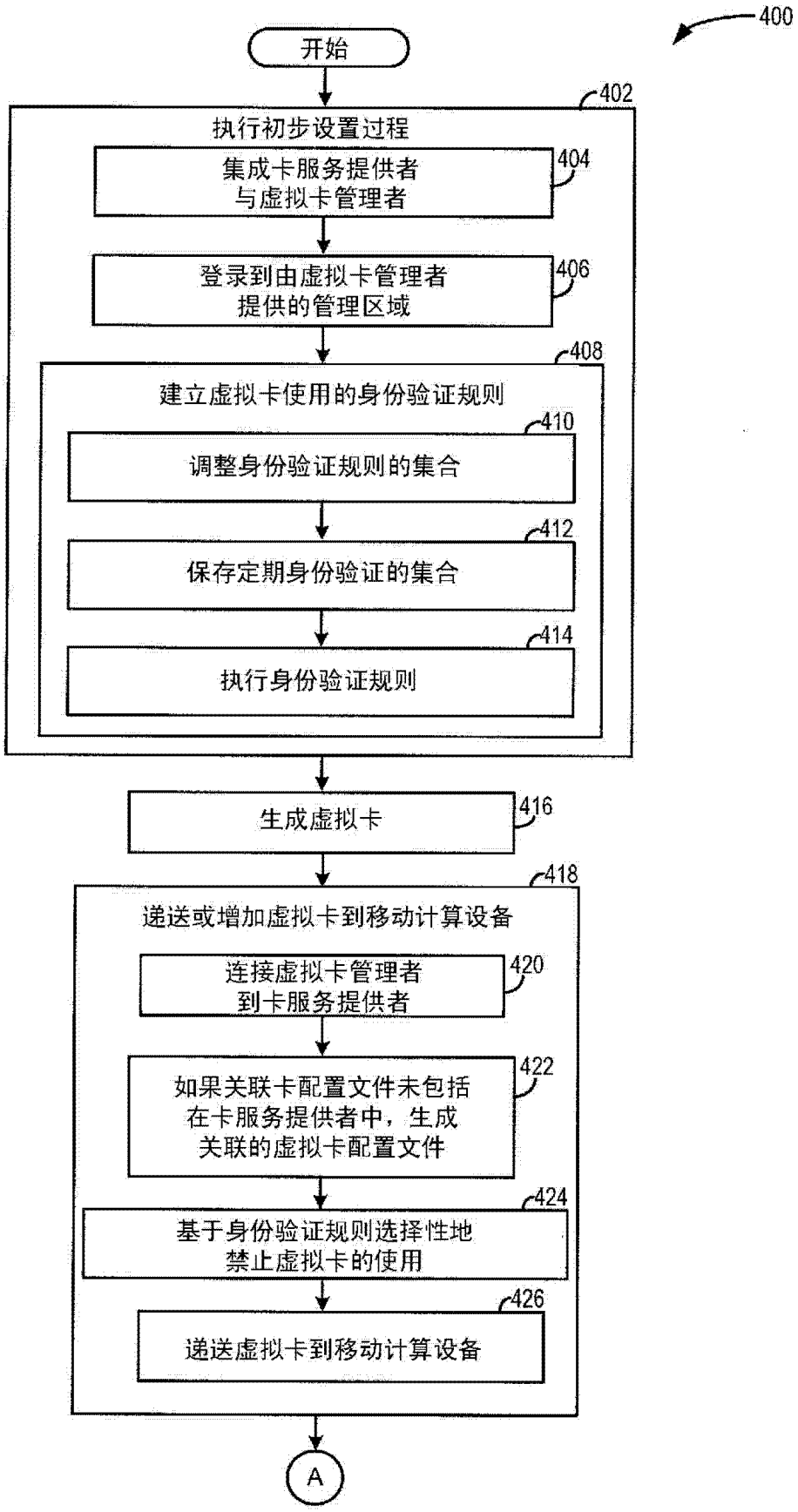
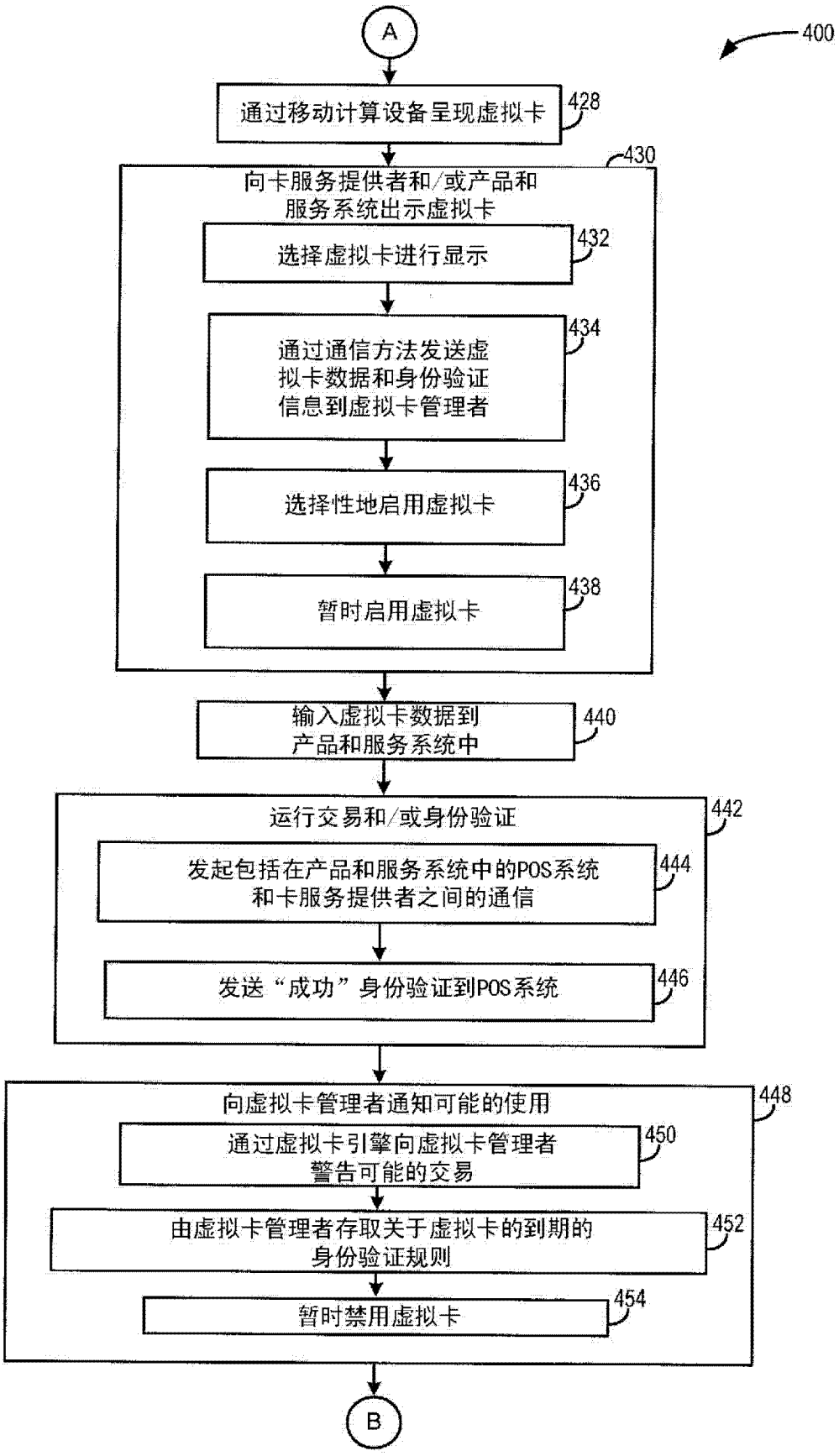

开始
300
可通信地链接至少一个卡服务提供者和虚拟卡管理者
302
可通信地链接至少一个虚拟卡引擎和虚拟卡管理者
304
基于预定的身份验证规则的集合选择性地启用虚拟卡和对应的卡服务提供者之间的虚拟卡交易
306
接收虚拟卡的交易请求
308
启用状态或禁用状态？
310
启用
禁用
312
允许交易请求
314
禁止交易请求
基于预定的身份验证规则的第二集合选择性地启用第二虚拟卡和对应的卡服务提供者之间的第二虚拟卡交易
316
接收第二虚拟卡的交易请求
318
启用状态或禁用状态？
320
启用
禁用
322
允许交易请求
324
禁止交易请求
调整身份验证规则
326
结束

图 3


400
开始
402
执行初步设置过程
404
集成卡服务提供者
与虚拟卡管理者
406
登录到由虚拟卡管理者
提供的管理区域
408
建立虚拟卡使用的身份验证规则
410
调整身份验证规则的集合
412
保存定期身份验证的集合
414
执行身份验证规则
416
生成虚拟卡
418
递送或增加虚拟卡到移动计算设备
420
连接虚拟卡管理者
到卡服务提供者
422
如果关联卡配置文件未包括
在卡服务提供者中，生成
关联的虚拟卡配置文件
424
基于身份验证规则选择性地
禁止虚拟卡的使用
426
递送虚拟卡到移动计算设备
A


A
400
通过移动计算设备呈现虚拟卡
428
430
向卡服务提供者和/或产品和服务系统出示虚拟卡
选择虚拟卡进行显示
432
通过通信方法发送虚拟卡数据和身份验证信息到虚拟卡管理者
434
选择性地启用虚拟卡
436
暂时启用虚拟卡
438
输入虚拟卡数据到产品和服务系统中
440
运行交易和/或身份验证
442
发起包括在产品和服务系统中的POS系统和卡服务提供者之间的通信
444
发送“成功”身份验证到POS系统
446
向虚拟卡管理者通知可能的使用
448
通过虚拟卡引擎向虚拟卡管理者警告可能的交易
450
由虚拟卡管理者存取关于虚拟卡的到期的身份验证规则
452
暂时禁用虚拟卡
454
B

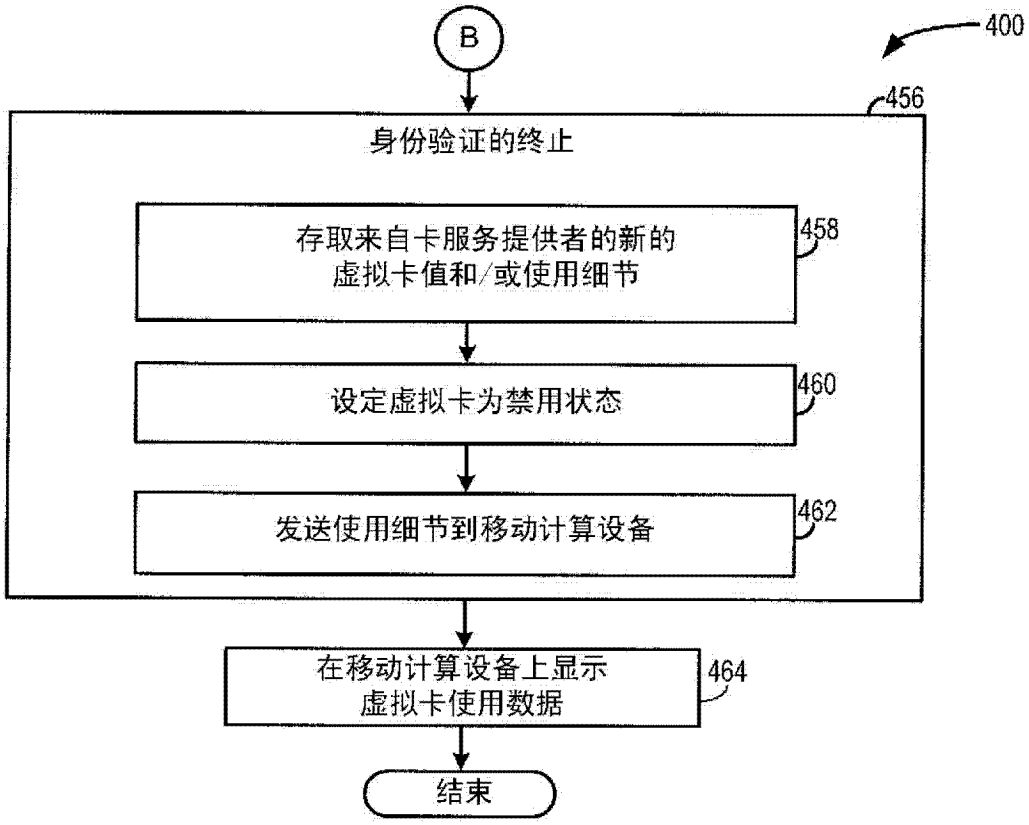

B
400
456
身份验证的终止
存取来自卡服务提供者的新的
虚拟卡值和/或使用细节
458
设定虚拟卡为禁用状态
460
发送使用细节到移动计算设备
462
在移动计算设备上显示
虚拟卡使用数据
464
结束

图 4

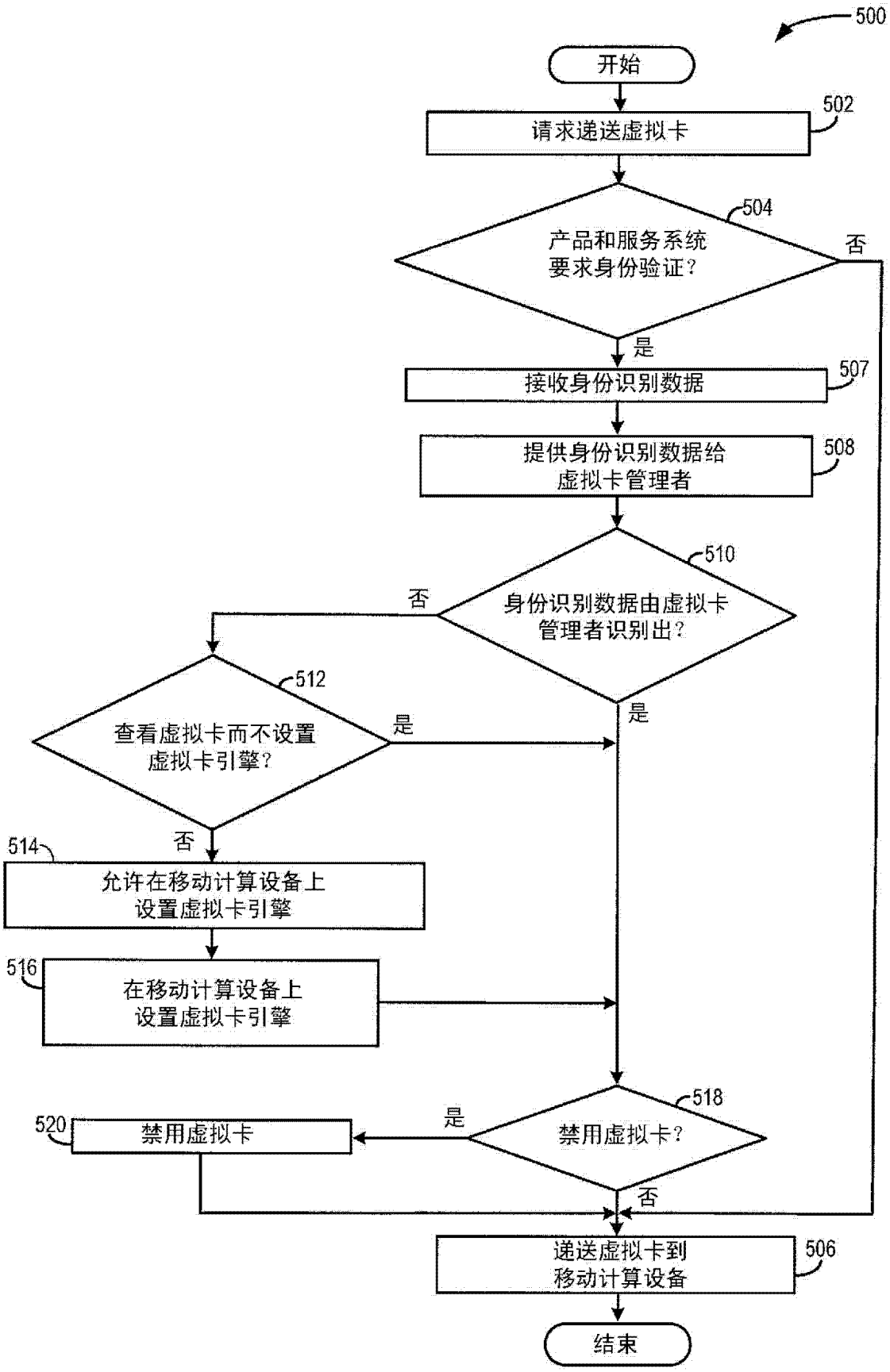

500
开始
请求递送虚拟卡
502
产品和服务系统要求身份验证？
504
否
是
接收身份识别数据
507
提供身份识别数据给虚拟卡管理者
508
身份识别数据由虚拟卡管理者识别出？
510
否
是
查看虚拟卡而不设置虚拟卡引擎？
512
是
否
允许在移动计算设备上设置虚拟卡引擎
514
在移动计算设备上设置虚拟卡引擎
516
禁用虚拟卡？
518
是
禁用虚拟卡
520
否
递送虚拟卡到移动计算设备
506
结束

图 5

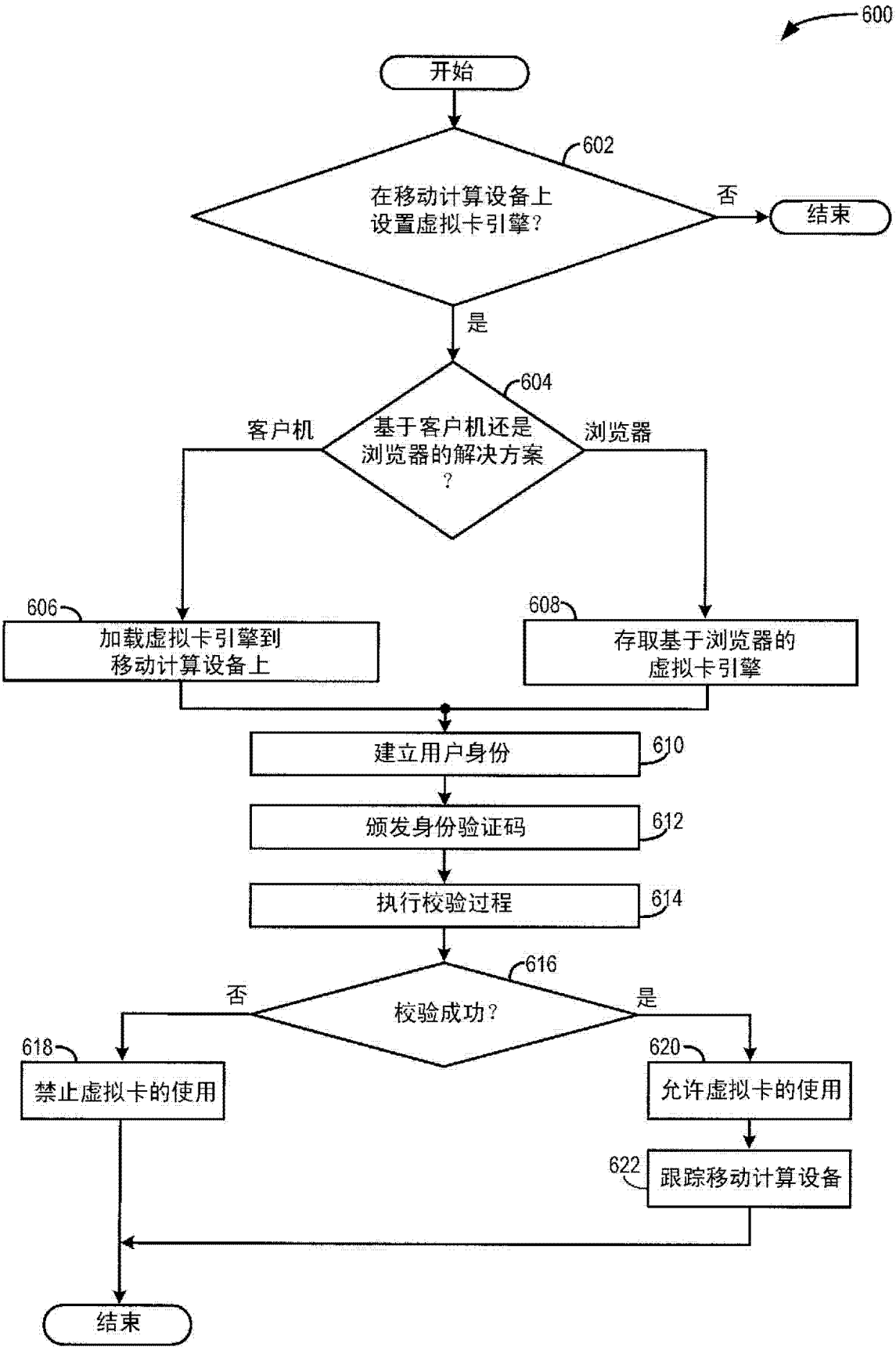

600
开始
602
在移动计算设备上
设置虚拟卡引擎?
否
结束
是
604
客户机
基于客户机还是
浏览器的解决方案
?
浏览器
606
加载虚拟卡引擎到
移动计算设备上
608
存取基于浏览器的
虚拟卡引擎
建立用户身份
610
颁发身份验证码
612
执行校验过程
614
616
否
校验成功?
是
618
禁止虚拟卡的使用
620
允许虚拟卡的使用
622
跟踪移动计算设备
结束

图 6

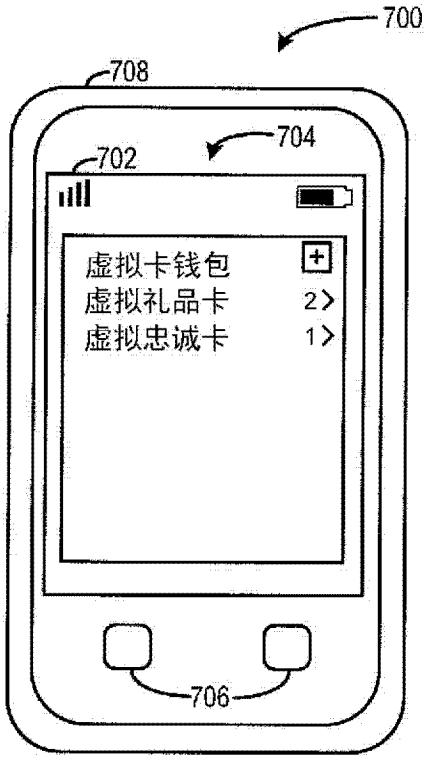

700
708
704
702
虚拟卡钱包
虚拟礼品卡 2>
虚拟忠诚卡 1>
706

图 7

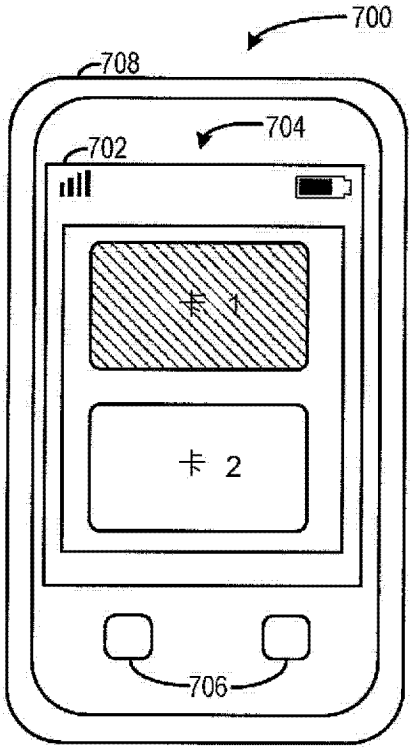

700
708
704
702
卡 1
卡 2
706

图 8

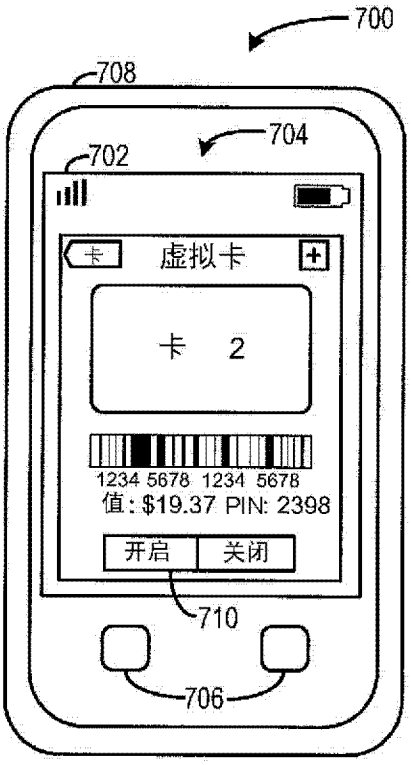

700
708
704
702
卡
虚拟卡
卡 2
1234 5678 1234 5678
值：$19.37 PIN: 2398
开启
关闭
710
706

图 9