

(12) 发明专利申请

(10) 申请公布号 CN 101809633 A

(43) 申请公布日 2010. 08. 18

(21) 申请号 200880107195. 2

(74) 专利代理机构 上海专利商标事务所有限公
司 31100

(22) 申请日 2008. 09. 11

代理人 钱慰民 钱静芳

(30) 优先权数据

60/971, 813 2007. 09. 12 US

12/206, 564 2008. 09. 08 US

(51) Int. Cl.

G07F 7/10(2006. 01)

(85) PCT申请进入国家阶段日

2010. 03. 11

(86) PCT申请的申请数据

PCT/US2008/076046 2008. 09. 11

(87) PCT申请的公布数据

W02009/036191 EN 2009. 03. 19

(71) 申请人 设备保真度股份有限公司

地址 美国得克萨斯州

(72) 发明人 D·简恩

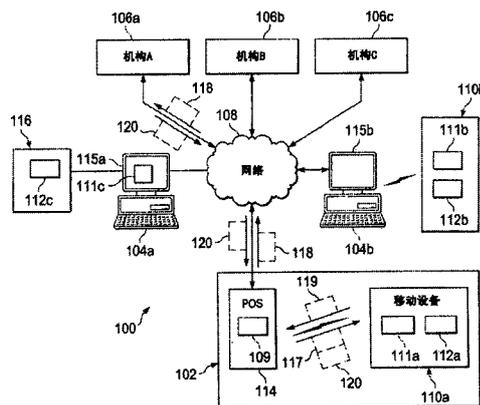
权利要求书 3 页 说明书 23 页 附图 13 页

(54) 发明名称

与不同的企业无线地执行交易

(57) 摘要

本发明针对一种用于与不同的机构无线地执行交易的系统和方法。在一些实现中,物理接口、通信模块、安全存储器、用户界面模块、以及交易模块。该物理接口连接到包括图形用户界面(GUI)的移动主机设备的一端口。该通信模块从接入终端无线地接收射频(RF)信号并向该接入终端无线地发送RF信号。该安全存储器存储多个可选用户凭证。使用至少一组用户凭证来与接入终端执行交易,并且每一组用户凭证都与不同的机构相关联。该交易模块响应于至少一事件在该多个可选用户凭证之间动态地切换并向接入终端无线地发送对所请求交易的响应,该响应包括从该多个可选用户凭证中选择的用户凭证。



1. 一种卡,包括:

物理接口,所述物理接口连接到移动主机设备的一端口,其中所述移动主机设备包括图形用户界面(GUI);

通信模块,所述通信模块从接入终端无线地接收射频(RF)信号并向所述接入终端无线地发送RF信号;

安全存储器,所述安全存储器存储多个可选用户凭证,其中所述用户凭证与接入终端执行交易并且每一个用户凭证都与不同的机构相关联;

用户界面模块,所述用户界面模块通过所述移动主机设备的GUI呈现并接收信息;以及

交易模块,所述交易模块响应于至少一事件在所述多个可选用户凭证之间动态地切换并向所述接入终端无线地发送对所请求交易的响应,所述响应包括从所述多个可选用户凭证中选择的用户凭证。

2. 如权利要求1所述的卡,其特征在于,所述物理接口包括安全数字(SD)接口、miniSD接口、microSD接口、MMC接口、miniMMC、microMMC、火线、或苹果iDock接口、或通用串行总线(USB)接口中的至少一个。

3. 如权利要求1所述的卡,其特征在于,所述通信模块独立于所述移动主机设备执行所述交易。

4. 如权利要求1所述的卡,其特征在于,所述存储器存储用于所述多个用户凭证的多个安全框架,所述通信模块使用来自所述多个安全框架的对应于所选用户凭证的安全框架来执行所请求交易。

5. 如权利要求1所述的卡,其特征在于,所述一个或多个事件包括用户选择通过所述移动主机设备的GUI所呈现的图形元素。

6. 如权利要求1所述的卡,其特征在于,所述用户界面模块通过所述移动主机设备的GUI呈现与所请求交易相关联的信息。

7. 如权利要求6所述的卡,其特征在于,所呈现的信息至少部分地基于所述交易期间的实时内容、存储在本地的离线内容、或与所述金融机构相关联的在线内容中的至少一个。

8. 如权利要求6所述的,其特征在于,所述用户界面模块还通过所述移动主机设备的GUI呈现对用户标识的请求,所述用户标识包括个人识别号(PIN)、用户ID及口令、或生物测定签名中的至少一个,所述处理模块在执行所请求交易之前还用存储在所述安全存储器本地的用户标识验证所提交的用户标识。

9. 如权利要求1所述的卡,其特征在于,所述通信模块响应于至少一事件在激活状态和停用状态之间有选择地切换RF天线。

10. 如权利要求1所述的卡,其特征在于,所述无线RF信号包括无接触信号、接近信号、近场通信(NFC)信号、蓝牙信号、超宽带(UWB)信号、或射频标识(RFID)信号中的至少一个。

11. 如权利要求1所述的卡,其特征在于,所述通信模块还包括在与所述零售终端和内部交易应用程序相兼容的各无线协议之间转换信号的协议转换模块。

12. 如权利要求1所述的卡,其特征在于,还包括密码模块,所述密码模块在所述交易模块处理之前解密接收到的信号并在无线发送之前加密所述交易响应的至少一部分。

13. 如权利要求 1 所述的卡,其特征在于,还包括认证模块,所述认证模块认证所述移动主机设备的网络、所述移动主机设备、或用户中的至少一个。

14. 如权利要求 1 所述的卡,其特征在于,还包括引导模块,所述引导模块至少响应于插入所述移动主机设备的所述端口中来执行一个或多个认证过程。

15. 如权利要求 14 所述的卡,其特征在于,所述一个或多个认证过程认证网络、移动主机设备、或用户中的至少一个。

16. 如权利要求 1 所述的卡,其特征在于,还包括激活模块,所述激活模块激活对来自所述多个可选用户凭证的用户凭证的访问并向相关联的金融机构发送激活相关联的用户账户的请求。

17. 如权利要求 16 所述的卡,其特征在于,对来自所述多个可选用户凭证的用户凭证的访问是至少部分地基于用户使用所述移动主机设备的 GUI 手动地输入激活码来激活的。

18. 如权利要求 1 所述的卡,其特征在于,所述移动主机设备的用户使用所述 GUI 来管理与所述多个可选用户凭证相关联的不同用户账户。

19. 如权利要求 1 所述的卡,其特征在于,所述通信模块还被配置成通过与蜂窝核心网络的无线连接或与宽带网络的有线连接来接收更新所述多个可选用户凭证的请求。

20. 如权利要求 19 所述的卡,其特征在于,所述通信模块还被配置成至少部分地基于所述更新请求来至少添加新的用户凭证集合或删除现有用户凭证。

21. 如权利要求 1 所述的卡,其特征在于,所述多个可选用户凭证包括默认用户凭证,所述通信模块还被配置成至少响应于使用所述多个可选用户凭证中的不同一个用户凭证完成所请求交易来切换到所述默认用户凭证。

22. 如权利要求 1 所述的卡,其特征在于,所述多个可选用户凭证包括默认用户凭证,所述安全模块还被配置成至少响应于使用非默认用户凭证完成交易的时间期满来切换到默认用户凭证。

23. 如权利要求 1 所述的卡,其特征在于,所述多个可选凭证各自从不同的机构被加载到所述安全存储器中。

24. 如权利要求 1 所述的卡,其特征在于,所述卡包括微安全数字卡。

25. 一种方法,包括:

连接到主机设备的一端口,其中所述移动主机设备包括 GUI;

与接入终端无线地传递 RF 信号;

存储多个可选用户凭证,其中所述用户凭证与接入终端执行交易并且每一个用户凭证都与不同的机构相关联;

通过所述移动主机设备的 GUI 呈现信息;以及

响应于至少一事件在所述多个可选用户凭证之间动态地切换;以及

向所述接入终端无线地发送对所请求交易的响应,所述响应包括从所述多个可选用户凭证中选择的用户凭证。

26. 如权利要求 1 所述的方法,其特征在于,所述端口包括 SD 接口、miniSD 接口、microSD 接口、MMC 接口、miniMMC、microMMC、火线、或苹果 iDock 接口、或 USB 接口中的至少一个。

27. 如权利要求 1 所述的方法,其特征在于,所请求交易是独立于所述移动主机设备来

执行的。

28. 如权利要求 1 所述的方法,其特征在于,还存储用于所述多个用户凭证的多个安全框架,所述交易是使用来自所述多个安全框架的对应于所选用户凭证的安全框架来执行的。

29. 一种系统,包括:

用于连接到移动主机设备的一端口的装置,其中所述移动主机设备包括图形用户界面 GUI;

用于与接入终端无线地传递 RF 信号的装置;

用于存储多个可选用户凭证的装置,其中所述用户凭证与接入终端执行交易并且每一个用户凭证都与不同的机构相关联;

用于通过所述移动主机设备的 GUI 呈现信息的装置;以及

用于响应于至少一事件在所述多个可选用户凭证之间动态地切换的装置;以及

用于向所述接入终端无线地发送对所请求交易的响应的装置,所述响应包括从所述多个可选用户凭证中选择的用户凭证。

与不同的企业无线地执行交易

[0001] 优先权要求

[0002] 本申请要求 2007 年 9 月 12 日提交的美国专利申请第 60/971, 813 号和 2008 年 9 月 8 日提交的美国专利申请第 12/206, 564 号的优先权, 这两份申请的整体内容通过引用结合于此。

技术领域

[0003] 本发明涉及网络通信, 并且更具体地涉及与不同的企业无线地执行交易。

[0004] 背景

[0005] 便携式电子设备和令牌已经成为日常用户体验的组成部分。用户拥有各种各样的便携式和手持式设备, 包括通信、商务、以及娱乐设备, 如蜂窝电话、音乐播放器、数码相机、智能卡、存储器令牌、以及上述设备和令牌的各种可能的组合。所有这些设备共享以下共性: 消费者大多数时候习惯于将它们随身携带到大多数地方。跨各种人口统计和年龄组都是如此, 而不管消费者的世故程度、他们的年龄组、他们的技术水平或背景。

[0006] 这些常见手持式设备提供用于可扩展存储器的选项。微安全数字 (microSD) 是高端蜂窝电话中的流行接口, 而 SD 和多媒体卡 (MMC) 接口在有限的模型中也是可用的。MicroSD 是这些设备和令牌中的大多数所支持的至少共同特征 (就大小而言)。另外, 适配器可用于将 microSD 转换成 MiniSD、SD、MMC、以及 USB。虽然大多数流行的 MP3 播放器 (iPOD) 提供专用接口, 但竞争设计确实提供标准接口。数码相机大多数都提供 SD 和 MMC, 而尖端数字 (xD) 是另一选项。这些接口的微型和袖珍版本在若干模型中也是可用的。Mini-USB 在蜂窝电话、数码相机、以及 MP3 播放器中日益可用于与膝上型计算机进行同步。

[0007] 概述

[0008] 本发明针对一种用于与不同的机构无线地执行交易的系统和方法。在一些实现中, 物理接口、通信模块、安全存储器、用户界面模块、以及交易模块。该物理接口连接到包括图形用户界面 (GUI) 的移动主机设备的一端口。该通信模块从接入终端无线地接收射频 (RF) 信号并向该接入终端无线地发送 RF 信号。该安全存储器存储多个可选用户凭证。使用至少一组用户凭证来与接入终端执行交易, 并且每一组用户凭证都与不同的机构相关联。该交易模块响应于至少一事件在该多个可选用户凭证之间动态地切换并向接入终端无线地发送对所请求交易的响应, 该响应包括从该多个可选用户凭证中选择的用户凭证。

[0009] 在附图和以下描述中阐明了本发明的一个或多个实施例的细节。本发明的其他特征、目标、以及优点从描述和附图以及权利要求书将变得显而易见。

[0010] 附图描述

[0011] 图 1 是根据本发明的一些实现的示例交易系统;

[0012] 图 2 是通过蜂窝核心网络发送交易信息的示例交易系统;

[0013] 图 3 是根据本发明的一些实现的图 1 的示例交易卡;

[0014] 图 4 是有选择地开关天线的示例智能卡;

[0015] 图 5 是根据本发明的一些实现的另一示例交易系统;

- [0016] 图 6 是示出智能卡的个性化过程的示意图；
- [0017] 图 7A 和 B 是示出用于初始化智能卡的示例方法的流程图；
- [0018] 图 8A-C 是示出使用智能卡进行呼叫会话的示例呼叫流程；
- [0019] 图 9 是示出用于激活交易卡的示例方法的流程图；
- [0020] 图 10 示出智能卡中的用于存储多个用户凭证的示例存储器；以及
- [0021] 图 11 是示出用于在用户账户之间动态地切换的示例方法的流程图。
- [0022] 在各附图中相同的附图标记指示相同的元素。
- [0023] 详细描述

[0024] 图 1 是示出用于使用单个智能卡来与不同的企业无线地执行交易的示例交易系统 100 的框图。例如，系统 100 可包括独立于移动主机设备来与不同的企业（例如，金融机构）执行交易的单个微安全数字（microSD）卡。例如，单个 microSD 卡可以与金融机构执行支付交易、与企业网络执行访问控制交易、与公共管理局执行票务购买交易、和 / 或与政府机构执行身份确认交易。在这些实现中，每一交易都可安全地标识用户和关于从不同企业接收到的服务的用户特权。除 microSD 之外，系统 100 可包括将智能卡连接到主机设备的其他大容量存储接口，诸如例如多媒体卡（MMC）、SD、通用串行总线（USB）、火线、和 / 或其他。主机设备可包括蜂窝电话、智能电话、个人数字助理（PDA）、MEPG-1 音频层 3（MP3）设备、数码相机、摄像放像一体机、客户机、计算机、和 / 或包括例如大容量存储器的其他设备。在一些实现中，智能卡可以是插入到主机设备并独立于该主机设备执行交易的卡。在执行交易时，该智能卡可以使用通过物理接口（例如，SD、MMC、USB）连接到主机设备并通过无线连接（例如，NFC、ISO 14443、蓝牙）连接到外部设备的双接口。该智能卡可使用该物理接口来控制或以其他方式操作移动主机设备的一个或多个硬件组件（例如，显示器、蜂窝无线电技术）并使用该无线接口来与接入终端无线地通信。在一些实现中，该智能卡包括多个用户凭证，每一身份集与一不同的机构相关联。例如，该智能卡可以存储信用卡、借记卡、预付卡、礼物卡、支票账户、和 / 或其他用户账户的用户凭证。另外，该智能卡还可存储用于其他应用程序的用户凭证，如忠诚度（用于购买的点）、航班（访问俱乐部、登记）、状态（驾照）、成员资格（俱乐部）、和 / 或使用用户凭证来标识用户以便可以提供商品和 / 或服务的其他情况。通过在单个智能卡中存储多个用户凭证，系统 100 可以在不需要多个装置的情况下与不同的机构执行交易。换言之，单个智能卡可用作在逻辑上存储不同用户账户的信息并响应于至少一个事件来在不同的用户账户之间进行切换的逻辑钱包。通过提供智能卡，系统 100 可以在不需要附加硬件、软件、和 / 或固件的情况下和 / 或在不需要对读取器终端的现有硬件、软件、和 / 或固件进行改变以使用户能够无线地执行交易的情况下与各机构无线地执行交易。另外，系统 100 可以消除、最小化、或以其他方式减少个人为使用不同用户账户来执行交易所要拥有的装置的数量。换言之，该智能卡可用作多个不同装置但被实现成单个设备。

[0025] 在高层次上，系统 100 包括通过网络 108 耦合到机构 106 的企业 102 以及客户机 104a 和 104b。尽管并未示出，但系统 100 可包括机构 106 和网络之间的若干中间方，如交易需方和 / 或支付网络主机。企业 102 包括具有交易卡 112a 的移动设备 110a 和与消费者执行交易的接入点 114。接入点 114 包括用于向用户呈现信息和 / 或从用户接收信息的图形用户界面（GUI）109。在一些实现中，接入点 114 可向交易卡 112 无线地发送执行交易的

请求。交易卡 112 可向接入点 114 发送认证信息。客户机 104 包括用于呈现与系统 100 相关联的信息的 GUI 115。客户机 104a 包括使交易卡 112c 与客户机 104a 进行接口的读卡器 116。机构 106 可至少部分地基于交易卡 112 所发送的信息来授权该交易。移动设备 110 包括用于呈现与用户交易相关联的信息的 GUI 111。

[0026] 企业 102 一般是具有用于运作的物理存在（例如，建筑物）的企业的至少一部分。例如，企业 102 可在一物理位置（例如，实体店）直接向消费者销售商品和 / 或服务。在该示例中，企业 102 购买或以其他方式（例如，生产）从批发商（未示出）处接收商品，并随后可以向诸如移动设备 110 的用户等消费者销售这些商品。一般而言，企业 102 可以在提供商品和 / 或服务时提供与消费者的面对面体验。例如，企业 102 可以是实体店，以使用户使用因特网选择商品或服务并在企业 102 处购买和接收该商品或服务。企业 102 可以提供与商品相关联的以下服务中的一个或多个：商品目录、存货、分发、和 / 或运输。结果，企业 102 可能不直接经销从批发商接收到的商品。企业 102 可包括单个零售店、处于单个地理位置的一个或多个零售店、和 / 或在地理上分布的多个零售店。在某些情况下，两个或更多个实体可以表示同一实体的各部分或各附属实体。例如，企业 102 和批发商可以是一个企业内的各部门。总而言之，企业 102 可以与移动设备 110 无线地执行金融交易。

[0027] 每一移动设备 110 包括可用于与交易卡 112a 进行接口的电子设备。例如，移动设备 110 可以与系统 100 接收和发送无线和 / 或无接触通信。如在本发明中所使用的，移动设备 110 旨在涵盖蜂窝电话、数据电话、寻呼机、便携式计算机、SIP 电话、智能电话、个人数据助理 (PDA)、数码相机、MP3 播放器、摄像放像一体机、这些或其他设备内的一个或多个处理器、或能够与交易卡 112 传递信息的任何其他合适的处理设备。在一些实现中，移动设备 110 可以基于蜂窝无线电技术。例如，移动设备 110 可以是可用于与外部或不安全网络无线地连接的 PDA。在另一示例中，移动设备 110 可包括包含诸如小键盘、触摸屏、鼠标、或可接受信息的其他设备等输入设备和传达与同企业 102 的交易相关联的信息（包括数字数据、视觉信息、或 GUI 111）的输出设备的膝上型计算机。

[0028] GUI 111 包括可用于允许移动设备 110 的用户出于诸如执行交易和 / 或呈现交易历史等任何合适的目的来与系统 100 的至少一部分进行接口的图形用户界面。一般而言，GUI 111 向特定用户提供对系统 100 所提供的或在系统 100 中传递的数据的高效且用户友好的呈现，和 / 或还是供用户自我管理设置并访问机构 106 所提供的服务的高效且用户友好的工具。GUI 111 可包括具有可交互域的多个可定制框架或视图、下拉列表、和 / 或用户所操作的按钮。术语“图形用户界面”能以单数或复数来使用，以描述一个或多个图形用户界面和特定图形用户界面的每一显示。GUI 111 可包括处理系统 100 中的信息并向用户呈现结果的任何图形用户界面，如通用 web 浏览器或触摸屏。

[0029] 交易卡 112 可包括被配置成使用多个可选用户账户中的一个来与接入点 114 无线地执行交易的任何软件、硬件、和 / 或固件。例如，交易卡 112 可选择与多个可选用户账户中的一个（例如，金融账户）相关联的用户凭证，并使用所选账户且独立于移动设备 110a 来与接入点 114 执行无接触交易。换言之，交易卡 112 可无线地执行交易而无需移动设备 110 执行该交易的各方面。另外，交易卡 112 可本地地存储多个可选用户账户的用户凭证和 / 或应用程序（例如，支付应用程序、访问应用程序）。交易卡 112 可响应于至少一个事件来在用户凭证和支付应用程序之间动态地切换。切换事件可包括来自用户的通过 GUI 111

的选择、交易的完成、检测到一类信号、确定一类购买（例如，食品、衣物）、地理区域（例如，GPS）的改变、和 / 或其他事件。不同的用户账户可包括信用卡账户（例如，Visa（维萨）、MasterCard（万事达卡））、零售账户（例如，Target、Dillard）、预付卡、礼物卡、银行卡、（例如，美国银行）、航空卡、身份卡、驾照、和 / 或其他。在一些实现中，交易卡 112 可包括金融、零售、航空、社团、状态、和 / 或其他账户的任何组合的用户凭证。在一些实现中，交易卡 112 可本地地存储用于该多个可选用户账户的应用程序。例如，交易卡 112 可以为不同的用户凭证中的每一个执行一不同的应用程序。这些不同的应用程序可以使用不同的读取器基础结构、格式、协议、加密、与终端交换的用户凭证的类型 / 结构、和 / 或其他方面来执行交易。

[0030] 交易卡 112 可以使用诸如 NFC（例如，ISO 18092/ECMA 340）、ISO 14443、ISO 15693、Felica、MiFARE、蓝牙、超宽带（UWB）、射频标识（RFID）、和 / 或与零售支付终端（例如，接入点 114）相兼容的其他信号等短程信号来与接入点 114 执行交易。在一些实现中，交易卡 112 可包括执行操作系统和安全进程以独立地执行交易的一个或多个芯片组。在这样做时，移动设备 110 不需要附加硬件、软件、和 / 或固件来与接入点 114 无线地执行诸如 NFC 交易等交易。在一些实现中，交易卡 112 可执行以下各过程中的一个或多个：响应于至少一个或多个事件来在各用户凭证和 / 或各应用程序之间动态地切换；无线地接收来自接入点 114 的执行交易的请求和 / 或发送响应；在无线协议和与交易卡 112 相兼容的协议之间进行转换；在交易卡协议和与移动设备 110 相兼容的协议之间进行转换；通过 GUI 111 向用户呈现信息和从用户处接收信息（例如，PIN 请求、PIN）；对在交易卡 112 和接入点 114 之间无线地发送的信息进行解密和加密；执行本地地存储在交易卡 112 中的应用程序；至少部分地基于一个或多个事件来有选择地打开和关闭交易卡 112 的天线；至少部分地基于例如通过 GUI 111 接收到的信息来执行认证过程；至少响应于交易质询来向接入点 114 发送主机签名；至少部分地存储在卡 112 和接入点 114 之间执行的交易的细节；通过 GUI 111 向用户生成和 / 或呈现警告（例如，听觉 - 视觉警告）；在具有蜂窝能力的情况下使用移动设备 110 向机构 106 生成和 / 或发送无线消息警告；和 / 或其他。在一些实现中，交易卡 112 可以至少响应于用户选择 GUI 111 中的图形元素来发起交易。交易卡 112 可以至少响应于接入点 114 所发送的无线请求来发起与接入点 114 的交易。在一些实现中，交易卡 112 可以响应于一个或多个事件来有选择地在打开和关闭状态之间切换天线。该一个或多个事件可包括用户请求、交易的完成、卡 112 插入到不同的移动设备、位置改变、定时器事件、检测到用户输入的 PIN 不正确、该设备所连接的无线网络的变化、使用诸如 SMS 等无线通信方法从机构 106 接收到的消息、和 / 或其他事件。例如，交易卡 112 可以通过移动设备 110 从蜂窝网络（未示出）接收关闭天线的的一个或多个命令。

[0031] 关于在协议之间转换，交易卡 112 能用诸如 ISO 7816 等标准安全协议和 / 或其他协议来处理信息。在这种情况下，交易卡 112 可在 NFC 协议（例如，ISO18092）和交易卡协议之间进行转换。另外，交易卡 122 可以通过诸如 MicroSD、Mini-SD、或 SD 等物理接口来与移动设备 110 进行接口。关于安全进程，交易卡 112 可以实现一种或多种加密算法来保护诸如卡号（例如，信用卡卡号、借记卡卡号、银行账号）、PIN、和 / 或其他安全相关信息等交易信息。安全相关信息可包括有效期、卡验证码、用户名、家庭电话号码、用户邮政编码、和 / 或与验证持卡者身份相关联的其他用户信息。在一些实现中，交易卡 112 可以执行诸如 DES、TDES、和 / 或其他等私钥（对称算法），或诸如 RSA、椭圆曲线、和 / 或其他等公钥（非

对称算法)。另外,交易卡 112 可包括用于存储用户数据、应用程序、离线网页、和 / 或其他信息的存储器 (例如,闪存、EEPROM)。关于应用程序,交易卡 112 可以执行存储在本地应用程序并通过 GUI 111 向用户呈现信息和从用户处接收信息。例如,交易卡 112 可以执行用于使用 GUI111 和移动设备 110 来与机构 106 同步账户余额的应用程序。作为应用程序的替换或补充,交易卡 112 可以使用 GUI 111 向用户呈现离线网页。响应于发起交易,交易卡 112 可自动地通过 GUI 111 呈现离线网页。在一些实现中,离线网页可以与机构 106 相关联。在一些实现中,交易卡 112 可以向后兼容并用作大容量存储设备。例如,如果交易卡 112 的无线接口不可用或被停用,则交易卡 112 可用作使用户能够访问存储在存储器组件 (例如闪存) 中的数据的大容量存储设备。在一些实现中,交易卡 112 可以至少响应于被插入到移动设备 110 来执行一组初始化命令。这些初始化命令可包括确定移动设备 100 的设备相关信息 (例如,电话号码、签名、连接网络信息、位置信息、以及其他可用属性)、确定用户相关信息 (例如,PIN 码、激活码)、递增计数器、设置标志、以及根据预先存在的规则和 / 或算法来激活 / 停用功能。

[0032] 在一些实现中,交易卡 112 可自动地执行一个或多个欺诈控制过程。例如,交易卡 112 可以标识操作改变并至少部分地基于所标识的改变来自动地向金融机构发送通知。交易卡 112 可以执行两个欺诈控制过程:(1) 确定违反一个或多个规则;以及(2) 至少响应于该违反来自动地执行一个或多个动作。关于规则,交易卡 112 可在本地存储与对交易卡 112 的各操作方面的更新相关联的规则。例如,交易卡 112 可以存储指示移动主机设备 110 的改变是操作违反的规则。在一些实现中,交易卡 112 可以存储至少部分地基于对以下各项的一个或多个的更新的规则:主机设备 110 的电话号码;主机设备 110 的 MAC 地址;无线地连接到主机设备 110 的网络;主机设备的位置;和 / 或其他方面。响应于匹配或以其他方式违反规则的一个或多个事件,交易卡 112 可执行一个或多个进程来基本上阻止可能的欺诈活动或以其他方式向机构 106 通知该可能的欺诈活动。例如,交易卡 112 可以执行阻塞相关联的用户账户和 / 或交易卡 112 的命令。另选地或另外地,交易卡 112 可以向机构 106 发送呼叫移动主机设备 110 的命令。在一些实现中,交易卡 112 可以至少部分地基于事件类型来执行命令。在一些示例中,交易卡 112 可以至少响应于主机设备 110 号码的改变来发起与机构 106 的呼叫。在一些示例中,交易卡 112 可至少响应于指定事件类型来重新执行激活过程。在一些实现中,交易卡 112 可以执行将 GUI 111 从交易卡 112 断开的命令。交易卡 112 可以在执行该命令之前通过 GUI 111 呈现断开连接通知。在一些实现中,交易卡 112 可以向机构 106 发送停用与卡 112 相关联的账户的命令。

[0033] 在一些实现中,接入点 114 可以向交易卡 112 发送对用于生成授权请求 118 的信息的交易请求 117。至少响应于该交易请求,交易卡 112 可以发送标识与用户账户相关联的信息的一个或多个交易响应 119。在一些实现中,接入点 114 可向机构 106 发送授权交易的请求 118。该授权信息可包括账号、交易金额、用户凭证、和 / 或其他信息。至少响应于该交易请求 118,机构 106 可以向接入点 114 发送授权响应 120。在一些实现中,接入点 114 可以向交易卡 112 发送响应 120。交易响应 120 可包括例如可通过 GUI 111a 向用户呈现的收据。在一些实现中,机构 106 可以通过蜂窝核心网络 (参见图 2) 向移动设备发送授权响应 120。在该实现中,在用户注册过程期间、自动地在用户激活卡 112 时、在例如最初将卡 112 插入到移动设备 110 时、和 / 或在其他事件期间,机构 106 存储了移动设备 110 与交

易卡 112 之间的关联。在所示实现中,接入点 114 包括 GUI 109。

[0034] GUI 109 包括可用于允许接入点 114 的用户出于诸如用户输入交易信息(例如, PIN、接受交易)和 / 或呈现交易信息(例如,交易金额)等任何合适的目的来与系统 100 的至少一部分进行接口的图形用户界面。一般而言,GUI109 向特定用户提供对系统 100 所提供的或在系统 100 中传递的数据的高效且用户友好的呈现,和 / 或还是供用户无线地发起与交易卡 112 的交易的高效且用户友好的工具。GUI 109 可以向用户呈现用于例如接受交易和输入诸如 PIN 等安全信息的一系列屏幕画面或显示。

[0035] 在一些实现中,交易卡 112 可被不同地实现。交易卡 112 可被实现为 KeyFOB(密钥卡)并在移动设备 110 外作为 FOB 保持活动。在这种情况下,交易卡 112 可以是无源的并且从接入点 114 所生成的感应磁场中加电。交易卡 112 可被实现成用于安装在 PCB 或 IC 芯片上的工业集成电路芯片的形式。在一些实现中,交易卡 112 可被实现成由外部 AC 适配器或独立盒供电的自包含台式独立单元的形式。在一些实现中,交易卡 112 可被实现成移动设备 110 的外部附件(例如,容器)并使用诸如 USB、串行端口、iDock 苹果专用接口、和 / 或其他接口等外围接口被连接到该移动设备。

[0036] 在一些实现中,交易卡 112 可根据以下各模式中的一个或多个来操作:活动卡模拟;活动读取器;自训练;杀死(killed);存储器;和 / 或其他模式。交易卡 112 可操作活动卡模拟模式来将移动设备 110 转换成加载有金融工具(FV)的无接触支付设备,该金融工具(vehicle)可以是例如信用卡、借记卡、礼物卡、和 / 或其他零售支付产品。在该模式中,交易卡 112 可以在有能力接受无接触支付交易的任何零售支付终端(例如,接入点 114)处执行交易。例如,这些终端可以是当前商家使用的 MasterCard paypass 或 Visa paywave 程序之下的启用无接触的终端在交易卡 112 的天线以此模式激活之后,商家终端可以检测交易卡 112 的存在并提示用户诸如通过输入 PIN、在终端界面上签名、确认交易金额、和 / 或其他动作来授权交易。在该模式中,这些交易可以作为正常的信用卡存在(credit card present)交易来处理。在该实现中,终端或金融机构都不需要附加软件来执行交易。另外,处于该模式的交易卡 112 可用于其他应用程序,如物理门禁控制(以在企业环境或公共交通环境中打开门)、逻辑访问控制(以经由 PC 请求网络访问)、应用程序访问控制(以购买对诸如运输、电影等乐趣的访问或需要进行支付来获取对设施的访问的任何其他情况)、和 / 或其他应用程序。

[0037] 在活动读取器模式中,交易卡 112 可以将移动设备 110 转换成当处于发送终端(例如,接入点 114)的射程内时能够接收数据的无接触读取器设备。在一些实现中,这一模式需要专用 NFC 硬件,同时需要读取器模式能力作为交易卡 112 的一部分。在移动设备 110 靠近(例如,10cm 或更短)发送终端的情况下,可以激活交易卡 112 的读取器模式并通过 GUI 111 提示用户授权接收数据。该模式只可适用于具有诸如 OK 按钮和屏幕、用于指示正在请求数据接收的 LED、和 / 或其他界面等 UI 元素的移动设备 110。一旦用户授权了发送,则处于该模式的交易卡 112 可以接收并本地地存储、处理,并可以执行交易和 / 或将接收到的数据转发给另一实体。例如,处于该模式的交易卡 112 可以通过促销海报、确认对票的购买、和 / 或其他来接收内容。例如,处于该模式的交易卡 112 可用作从塑料无接触卡 / FOB 接收交易信息并指示移动设备 110 通过蜂窝核心网络准备向机构 106 的交易授权请求的移动 POS 终端。一旦机构 106 授权该交易,则移动设备 110 可以通过 GUI 111 向用户显

示对该交易的确认。

[0038] 关于自训练模式,交易卡 112 可以执行某一版本的读取器模式。在一些实现中,自训练模式可由专门动作(例如,对微小开关的针尖按压、经由 GUI 111 输入管理员口令)来激活。至少响应于激活该模式,交易卡 112 可被配置成通过例如短程无线接口从另一对等交易卡接收个性化数据,该另一对等交易卡诸如兼容该功能并由机构 106 发行的塑料无接触卡。在该模式中接收到的个性化数据可包括存储在交易卡 112 的安全存储器中的加密 FV 信息。在一些实现中,处于该模式的交易卡 112 可以通过发送机的无接触接口和 / 或其他来接收 FV 信息。交易卡 112 随后合成对应于用户账户的该 FV 信息并个性化安全元件。该自训练模式可用于在现场重新个性化该插件。在一些实现中,如果激活该自训练模式,则可以删除所有先前数据。该自训练模式可以是其中卡 112 可以从另一交易卡 112 接收个性化信息的对等个性化模式。该模式可以不包括可作为服务器到客户机个性化场景的工厂、店面、和 / 或空中 (OTA) 个性化场景。在一些实现中,该自训练模式可以是其中交易卡 112 从另一交易卡接收个性化信息的对等个性化模式。因为在该模式中使用了两个交易卡 112,所以该模式不是与像工厂、店面、和 OTA 个性化等服务器到客户机个性化场景。

[0039] 关于杀死模式,交易卡 112 可以永久停用无接触接口。在一些实现中,杀死模式是使用移动设备 110 通过物理接口(如 microSD 接口)来激活的。至少响应于对该杀死模式的激活,交易卡 112 可以永久担当大容量记忆棒。在一些实现中,在按下复位针尖的情况下,可以使交易卡 112 不进入任何其他模式。另外,交易卡 112 可以至少响应于该模式被激活来删除存储器中的金融内容。在一些实现中,无线运营商可以使用该模式来从物理丢失的交易卡 112 中删除数据。

[0040] 关于存储器模式,交易卡 112 可以用作大容量记忆棒,以使该存储器可通过常规方法来访问。在一些实现中,交易卡 112 可至少响应于被从主机设备移除、被插入到非授权主机设备、和 / 或其他事件来自动地激活该模式。交易卡 112 可以例如通过将卡 112 插入到授权设备来从该存储器模式切换到活动模式,或可以从该模式切换到自训练模式来为新主机设备或新用户账户重新个性化该设备。

[0041] 在一些实现中,可诸如使用软件设备管理进程和 / 或硬件复位来重新个性化 / 更新交易卡 112。例如,用户可能出于改变主机设备、要拥有多个主机设备、和 / 或其他原因而想要重新个性化交易卡 112。关于软件设备管理,用户需要挂载 (cradle) 新主机设备,插入交易卡 112 以启动该软件设备管理应用程序。在一些实现中,该软件管理应用程序可以是直接安装在客户机 104 上的、作为插件集成到诸如 ActiveSync(主动同步)等正常同步应用程序的、可经由在插件提供商网站上运行的浏览器插件获得的、和 / 或其他源的应用程序。用户可登录到该应用程序并验证其身份,并且响应于该验证,该应用程序可以允许访问设备管理应用程序中的设备部分。设备管理应用程序可以读取交易卡 112 并显示他将其插件插入到的设备的 MAC 地址、签名、和 / 或其他设备专用信息。移动设备 110 可被标记为活动的并且该主机设备可被示为禁止的或非活动的。该应用程序可以允许用户更新新主机设备的状态,并且至少响应于该选择,设备管理应用程序可以将签名安装在新主机设备上并在交易卡 112 的安全存储器中将更新状态标记为允许。用户还可能能够将移动设备 110 的状态更新成禁止。否则,两设备都可以是活动的并且交易卡 112 可以在这两设备之间切换。关于硬件复位进程,用户可以使用物理交易卡 112 上的复位针尖按钮来激活自训练模

式。在该模式中,财务数据可被删除并且必须被重新加载。如上所述,在将交易卡 112 插入到新主机设备时,可以开始供应 (provisioning) 过程。

[0042] 接入点 114 可包括无线地接收用于与一个或多个机构 106 执行交易的账户信息的任何软件、硬件、和 / 或固件。例如,接入点 114 可以是能够与交易卡 112a 无线地发送交易信息的电子现金出纳机。接入点 114 能以一种或多种以下格式发送信息:14443 类型 A/B、Felica、MiFare、ISO 18092、ISO 15693;和 / 其他。交易信息可包括验证信息、支票号码、银行号码 (routing number)、账号、交易金额、时间、司机驾照号、商家 ID、商家参数、信用卡卡号、借记卡卡号、数字签名、和 / 或其他信息。在一些实现中,交易信息可被加密。在所示实现中,接入点 114 可以从交易卡 112 无线地接收加密交易信息并将该信息电子地发送到机构 106 中的一个或多个以供授权。例如,接入点 114 可以接收已针对所标识的账户接受或拒绝了交易金额的指示和 / 或从交易卡 112 请求附加信息。

[0043] 如在本发明中所使用的,客户机 104 旨在涵盖个人计算机、触摸屏终端、工作站、网络计算机、台式计算机、公共电话亭、无线数据端口、智能电话、PDA、这些或其他设备内的一个或多个处理器、或用于查看与交易卡 112 相关联的交易信息的任何其他合适的处理或电子设备。例如,客户机 104 可以是可用于与外部或不安全网络无线地连接的 PDA。在另一示例中,客户机 104 可包括包含诸如小键盘、触摸屏、鼠标、或可接受信息的其他设备等输入设备和传达与同机构 106 执行的交易相关联的信息 (包括数字数据、视觉信息、或 GUI115) 的输出设备的膝上型计算机。在一些实现中,客户机 104b 可使用例如 NFC 协议来无线地与交易卡 112b 通信。在一些实现中,客户机 104a 包括具有用于与交易卡 112c 进行通信的物理接口的读卡器 116。在一些实现中,读卡器 116 至少可包括使客户机 104 所支持的接口 (例如,USB、火线、蓝牙、WiFi) 适合卡 112 所支持的物理接口 (例如,SD/NFC) 的适配器 116b。在这种情况下,客户机 104a 可不包括用于无线通信的收发机。

[0044] GUI 115 包括可用于允许客户机 104 的用户出于诸如查看交易信息等任何合适的目的来与系统 100 的至少一部分进行接口的图形用户界面。一般而言,GUI 115 向特定用户提供对系统 100 所提供的数据或在系统 100 内传递的数据的高效且用户友好的呈现。GUI 115 可包括具有可交互域的多个可定制框架或视图、下拉列表、和 / 或用户所操作的按钮。术语“图形用户界面”能以单数或复数来使用,以描述一个或多个图形用户界面和特定图形用户界面的每一显示。GUI 115 可包括处理系统 100 中的信息并向用户呈现结果的任何图形用户界面,如通用 web 浏览器或触摸屏。机构 106 可以使用例如 web 浏览器 (例如,微软 Internet Explorer 或 Mozilla Firefox) 从客户机 104 接受数据,并使用网络 108 向该浏览器返回适当的响应 (例如,HTML 或 XML)。在一些实现中,交易卡 112c 的 GUI 111c 可以通过客户机 104a 的 GUI 115a 来呈现。在这些实现中,GUI 115a 可以从 GUI 111c 中检索用户凭证并填充在 GUI 115a 中呈现的金融表单。例如,GUI 115a 可以向用户呈现用于输入信用卡信息以通过因特网购买商品的表单,且 GUI 115a 可以至少响应于来自用户的请求来使用 GUI111c 填充该表单。

[0045] 机构 106a-c 可包括可授权通过网络 108 接收到的交易的任何企业。例如,机构 106a 可以是至少部分地基于通过网络 106 接收到的信息来确定是否授权交易的信用卡提供商。机构 106 可以是信用卡提供商、银行、联盟 (例如,VISA)、零售商家 (例如,Target)、预付 / 礼物卡供应商、因特网银行、政府实体、俱乐部、和 / 或其他。一般而言,机构 106 可

执行以下各过程中的一个或多个：接收授权交易的请求；标识账号和其他交易信息（例如，PIN）；标识与所标识的账户相关联的资金和 / 或信贷限额；标识与该用户账户相关联的访问特权；确定该交易请求是否超过资金和 / 或信贷限额和 / 或是否违反与该账户相关联的任何其他规则；发送已经接受还是拒绝了该交易的指示；和 / 或其他过程。关于银行，机构 106 可以标识账号（例如，银行账户、借记卡卡号）和相关联的验证信息（例如，PIN、邮政编码）并确定该账户持有者可用的资金。至少部分地基于所标识的资金，机构 106 可接受或拒绝所请求交易或请求附加信息。至于加密，机构 106 可以使用诸如 RSA 或椭圆曲线等公钥算法和 / 或诸如 TDES 等私钥算法来加密和解密数据。

[0046] 网络 108 便于金融机构与诸如客户机 104 和接入点 114 等任何其他本地或远程计算机之间的无线或有线通信。网络 108 可以是企业或安全网络的全部或部分。尽管被示为单个网络，但只要网络 108 的至少一部分可便于机构 106、客户机 104、以及企业 102 之间的交易信息传递，则网络 108 可以是逻辑上被分成各个子网或虚拟网络的连续网络而不背离本发明的范围。在一些实现中，网络 108 涵盖可用于便于系统 100 中各计算组件之间的通信的一个或多个任何内部或外部网络、子网、或其组合。网络 108 可在网络地址之间传递例如网际协议 (IP) 分组、帧中继帧、异步传输模式 (ATM) 单元、语音、视频、数据、以及其他合适的信息。网络 108 可包括一个或多个局域网 (LAN)、无线电接入网络 (RAN)、城域网 (MAN)、广域网 (WAN)、被称为因特网的全球计算机网络的全部或部分、和 / 或一个或多个位置处的一个或多个任何其他通信系统。

[0047] 图 2 是示出用于使用蜂窝无线电技术来无线地传递交易信息的示例交易系统 200 的框图。例如，系统 200 可以使用移动主机设备 110 和蜂窝无线电技术向交易卡 112 无线地传递交易收据。在一些实现中，蜂窝无线电技术可包括全球移动通信系统 (GSM)、码分多址 (CDMA)、通用移动通信系统 (UMTS)、和 / 或任何其他蜂窝技术。机构 106 可响应于一个或多个事件来向交易卡 112 分配一个或多个移动主机设备 110。在一些示例中，用户可以结合例如请求相关联的交易卡 112 来向机构 106 注册该一个或多个移动设备 110。在一些示例中，交易卡 112 可至少响应于初始插入到设备 110 来向机构 106 注册移动主机设备 110。不管关联过程如何，系统 100 可以使用主机设备 110 的蜂窝能力来在机构 106 与交易卡 112 之间传递信息。在使用主机设备 110 的蜂窝无线电技术时，在卡 112 不靠近诸如图 1 的接入点 114 等零售设备的情况下，系统 200 可以与交易卡 112 通信。

[0048] 在所示实现中，蜂窝核心网络 202 通常包括用于提供蜂窝服务的各种交换元件、网关、和服务控制功能。蜂窝核心网络 202 通常经由多个蜂窝接入网络（例如，RAN）来提供这些服务并还经由 MSC 206 将该蜂窝系统与其他通信系统（如网络 108）进行接口。根据蜂窝标准，蜂窝核心网络 202 可包括用于处理语音呼叫的电路交换（或语音交换）部分以及用于支持诸如电子邮件消息和 web 浏览等数据传输的分组交换（或数据交换）部分。电路交换部分包括在无线电接入网络 (RAN) 204 和网络 108 或另一网络之间、在蜂窝核心网络或其他网络之间交换或连接电话呼叫的 MSC 206。在核心网络 202 是 GSM 核心网络的情况下，核心网络 202 可包括也被称为通用分组无线电服务 (GPRS) 的分组交换部分，包括类似于 MSC 206 的用于服务并跟踪通信设备 102 的 GPRS 服务支持节点 (SGSN)（未示出）和用于在分组交换网络与通信设备 110 之间建立连接的 GPRS 网关支持节点 (GGSN)（未示出）。SGSN 还可包含用于建立和换手呼叫连接的用户数据。蜂窝核心网络 202 还可包括用于维护

“永久”用户数据的自家位置寄存器 (HLR) 以及用于“临时”维护使用无线通信方法从 HLR 检索到的用户数据和这些通信设备 110 的位置上的最新信息的访客位置寄存器 (VLR) (和 / 或 SGSN)。另外,蜂窝核心网络 202 可包括为可用于访问 GSM 核心网络 202 的设备 110 执行认证、授权、以及计费任务的认证、授权、和计费 (AAA)。尽管参考 GSM 网络描述了核心网络 202 的说明,但核心网络 202 可包括其他蜂窝无线电技术 (如 UTM、CDMA、以及其他) 而不背离本发明的范围。

[0049] RAN 204 在移动设备与蜂窝核心网络 202 之间提供无线电接口,其可通过宏呼叫 (macrocall) 208 向移动设备提供实时语音、数据、以及多媒体服务 (例如,呼叫)。一般而言,RAN 204 经由射频 (RF) 链路传递空中帧。具体地,RAN 204 将空中帧转换成基于物理链路的消息以供通过蜂窝核心网络 202 来传输。RAN 204 可以在传输期间实现例如以下无线接口标准中的一个:高级移动电话服务 (AMPS)、GSM 标准、码分多址 (CDMA)、时分多址 (TDMA)、IS-54 (TDMA)、通用分组无线电服务 (GPRS)、全球进化增强数据率 (EDGE)、或专用无线电接口。用户可以预订 RAN 204 例如来接收蜂窝电话服务、全球定位系统 (GPS) 服务、XM 无线电服务等。

[0050] RAN 204 可包括连接到基站控制器 (BSC) 212 的基站 (BS) 210。BS 210 在 RAN 204 的地理区域内接收并发送空中帧 (即,由蜂窝设备 102e 发送) 并与连接到 GSM 核心网络 202 的其他移动设备 110 通信。每一 BSC 212 与一个或多个 BS 210 相关联并控制相关联的 BS 210。例如,BSC 212 可以提供各个功能,诸如换手、单元配置数据、对 RF 能级的控制、或用于管理无线电资源并路由来自和去往 BS 210 的信号的任何其他合适的功能。MSC 206 处理对 BSC212 和网络 108 的访问。MSC 206 可以通过诸如 A 接口 (A-interface) 等标准接口连接到 BSC 212。尽管参考 GSM 网络描述了 RAN 204 的各元件,但 RAN 204 可包括其他蜂窝技术,诸如 UMTS、CDMA、和 / 或其他。在 UMTS 的情况下,RAN 204 可包括节点 B 和无线网络控制器 (RNC)。

[0051] 无接触智能卡 214 是具有处理信息的嵌入式集成电路的袖珍卡。例如,智能卡 214 可无线地接收交易信息,使用嵌入式应用程序处理该信息,并无线地发送响应。无接触智能卡 214 可以通过 RFID 感应技术以 106 到 848kbps 的数据率与读卡器无线地通信。卡 214 可在 10cm (例如,ISO/IEC 14443) 到 50cm (例如,ISO 15693) 之间与临近读卡器无线地通信。无接触智能卡 214 独立于内部电源来操作并从入射的射频询问信号中捕捉能量来对嵌入的电子电路供电。智能卡 214 可以是存储器卡或微处理器卡。一般而言,存储器卡只包括非易失性存储器存储组件并可包括某些专用安全逻辑。微处理器卡包括易失性存储器和微处理器组件。在一些实现中,智能卡 214 可具有正常信用卡大小的尺寸 (例如,85.60×53.98×.76mm、5x15x.76mm)。在一些实现中,智能卡 214 可以是 fob 或其他安全令牌。智能卡 214 可包括具有防篡改属性的安全系统 (例如,安全密码处理器、安全文件系统、人类可读特征) 和 / 或可被配置成提供安全服务 (例如,所存储信息的秘密性)。

[0052] 在一些操作方面,机构 106 可使用蜂窝核心网络 202 与移动主机设备 110 无线地通信。例如,机构 106 可响应于至少一事件来向移动主机设备 110 发送信息。该信息可包括例如交易信息 (例如,交易收据、交易历史)、脚本、应用程序、网页、和 / 或与机构 106 相关联的其他信息。该事件可包括完成交易、确定交易卡 112 在接入点终端的操作范围之外、接收到来自移动主机设备的用户的请求、和 / 或其他。例如,机构 106 可以标识与执行交易

的卡 112 相关联的移动主机设备 110 并使用蜂窝核心网络 202 向该移动主机设备 110 发送交易信息。在使用蜂窝核心网络 202 时,机构 106 可以向交易卡 112 发送信息而无需接入点终端靠近卡 112。另外地或另选地,机构 106 可以使用蜂窝核心网络 202 从移动主机设备 110、交易卡 112、和 / 或用户请求信息。例如,机构 106 可以通过蜂窝核心网络 202 和移动主机设备 110 向卡 112 发送对交易历史的请求。在一些实现中,移动主机设备 110c 可以用作被配置成与智能卡 214 无线地执行交易的移动销售点 (POS) 终端。例如,商家可以是移动的 (例如,出租车司机) 并可包括带有交易卡 112c 的移动主机设备 110c。在该示例中,交易卡 112c 可从智能卡 214 无线地接收账户信息并使用移动主机设备 110 和蜂窝核心网络 202 向机构 106 发送授权请求。

[0053] 在一些实现中,系统 100 可以执行参考图 1 所讨论的各模式中的一个或多个。例如,可以使用移动主机设备 110 的蜂窝无线电技术来重新个性化 / 更新交易卡 112。用户可能出于改变主机设备、要拥有多个主机设备、和 / 或其他原因而想要重新个性化交易卡 112。关于软件设备管理,用户可以使用主机设备 110 的蜂窝无线电技术来向机构 106 发送重新个性化交易卡 112 的请求。

[0054] 图 3 是示出根据本发明的一些实现的图 1 的示例交易卡 112 的框图。一般而言,交易卡 112 包括独立于移动设备 110 来执行交易 (例如,金融) 的个性化模块。所示交易卡 112 是仅出于示例目的的,并且交易卡 112 可包括某些、全部、或不同的模块而不背离本发明的范围。

[0055] 在一些实现中,交易卡 112 可包括接口层 302、API/UI 304、web 服务器 306、实时框架 308、支付应用程序 310、增值应用程序 312、多个用户凭证 314、实时操作系统 316、无接触芯片组 318、天线控制功能 320、天线 322、机构存储器 324、自由存储器 326、以及钱包管理系统 328。在一些实现中,主机控制器包括接口层 302、API/UI 304、web 服务器 306、实时框架 308、无接触芯片组 318、以及天线控制功能 320。在一些实现中,安全模块包括支付应用程序 310 和用户凭证 314。机构存储器 324 和自由存储器 326 可被包含在闪存中。在一些实现中,无接触芯片组 318 可以集成在安全模块中或独立地操作。天线 322 可以是电子电路。

[0056] 接口层 302 包括到主机设备的接口 (即,物理连接) 和外部世界的接口 (即,无线连接) 两者。在支付实现中,无线连接可以基于任何合适的无线标准,如无接触 (例如,ISP 14443A/B)、接近 (例如,ISO 15693)、NFC (例如,ISO18092)、和 / 或其他。在一些实现中,无线连接可以使用另一诸如蓝牙的短程无线协议、零售支付终端所使用的另一专用接口 (日本的 Felica、亚洲的 MiFare 等)、和 / 或其他。关于物理接口,接口层 302 可以使用诸如 MicroSD、Mini-SD、或 SD (全尺寸) 等 SD 协议来与移动设备 110 物理地进行接口。在一些实现中,物理接口可包括用于至少部分地基于移动设备 110 来在两种不同的协议之间进行转换的转换器 / 适配器。在一些实现中,移动设备 110 可以使用诸如 USB、MMC、iPhone 专用接口、或其他协议来进行通信。

[0057] API/UI 层 304 可包括用作移动设备 110 与交易卡 112 之间的 API 和用作 GUI 111 的任何软件、硬件、和 / 或固件。在执行交易之前,交易卡 112 可至少响应于插入来自动地在移动设备 110 中安装驱动程序。例如,交易卡 112 可在设备 110 中自动地安装 MicroSD 设备驱动程序以使交易卡 112 能够与移动设备 110 进行接口。在一些实现中,交易卡 112 可

以安装诸如带无线电的大容量存储器 (MMR) API 等增强设备驱动程序。在该实现中,该接口可以驱动包含大容量存储器的插件类以及无线电接口。MMR API 可以执行以下各过程中的一个或多个:连接/断开连接 MMR 控制器(插件中的微控制器);使用 MM 协议(例如,SD、MMC、XD、USB、火线)传送数据;向 MMR 控制器发送加密数据;接收对成功或出错的确认;接收指示出错描述的状态字;打开/关闭无线电;向交易卡 112 发送打开天线的指令并指定操作模式(例如,发送模式、监听模式);发送数据,如向控制器发送用于经由无线电发送数据的指令;监听数据,如向控制器发送用于监听数据的指令;读数据,如向控制器发送用于发送通过监听无线电而接收到的数据的指令;和/或其他。在一些实现中,MMR 可以兼容 TCP/IP。在一些实现中,除其他命令之外,封装 API 的 ISO 7816 命令可由安全模块处理。

[0058] 在一些实现中,该 API 可根据以下两个过程操作:(1) 交易卡 112 作为主机且移动设备 110 作为从机;和(2) 卡 UI 作为主机。在第一过程中,交易卡 112 可以响应于例如将交易卡 112 插入到移动设备 110 的槽中、交易卡 112 与接入点 114 之间的交易、和/或其他事件来向移动设备 110 传递一个或多个命令。在一些实现中,交易卡 112 可以请求移动设备 110 执行以下功能中的一个或多个:获取用户输入;获取签名;显示数据;发送数据;接收数据;和/或其他。“获取用户输入”命令可以通过 GUI 111 呈现来自用户的数据请求。在一些实现中,“获取用户输入”可以呈现对多个数据输入的请求。数据输入可以是任何合适的格式,如数字、字母数字、和/或其他字符串。“获取签名”命令可以请求移动设备 110 返回标识数据,如电话号码、网络码、连接状态、位置信息、Wi-Fi 信标、GPS 数据、和/或其他设备专用信息。“显示数据”命令可以通过 GUI 111 向用户呈现对话框。在一些实现中,该对话框可以在一段时间、用户选择、和/或其他事件之后消失。“发送数据”命令可以请求移动设备 110 使用其自己到外部世界的连接(例如,SMS、蜂窝、Wi-Fi)来发送分组数据。“接收数据”命令可以请求移动设备 110 打开具有特定参数的连接信道并标识通过该连接接收到的数据。在一些实现中,该命令可以请求移动设备 110 转发满足特定准则的要被转发到交易卡 112 的任何数据(例如,SMS)。

[0059] 关于 UI 作为主机,该 UI 可以执行以下命令中的一个或多个:智能卡命令/响应;激活/停用;闪存读/写;在加密或不加密的情况下发送数据;在解密或不解密的情况下接收数据;URL 获取数据/URL 通告(post)数据;和/或其他。这些安全模块命令可以涉及该卡所提供的安全功能并且针对交易卡 112 内的安全模块(例如,标准 ISO 7816 命令、专用命令)。在一些实现中,这些命令可包括加密、认证、供应数据、创建安全域、更新安全域、在验证密钥后更新用户凭证、和/或其他。在一些实现中,这些命令可包括非安全相关智能卡命令,如读交易历史命令。该读交易历史命令可以执行对交易卡 112 的安全存储器 324 的读。在一些实现中,在安全验证之后可以写安全存储器 324 的某些标志或区域。激活/停用命令可以激活或停用交易卡 112 的某些功能。闪存读/写命令可以对非安全存储器 326 的指定区域执行读/写操作。“在加密或不加密的情况下发送数据”命令可以指示交易卡 112 使用其与例如接入点 114 的无线连接来发送数据。另外,该数据在传输之前可由交易卡 112 使用例如存储在安全模块内的密钥和加密能力来加密。“在解密或不解密的情况下接收数据”命令可以指示交易卡 112 切换到监听模式以接收来自其与终端/读卡器(例如,接入点 114)的无线连接的数据。在一些实现中,数据解密可由安全模块使用例如该安全模块上可用的密钥和解密算法(即,板载解密)来请求。“URL 获取数据/URL 通告数据”命令可以指

示 web 服务器 306 使用例如离线 URL 来根据离线获取或通告指令返回页面。

[0060] 作为交易卡 112 的操作系统的一部分的 web 服务器 306 可以分配或以其他方式关联 URL 样式寻址到存储在交易卡 112 的存储器 326 (例如, 闪存) 中的特定文件。在一些实现中, web 服务器 306 使用该 URL 来定位文件并使用标准 HTTP、HTTPS 样式传输来将该文件返回给浏览器。在一些实现中, 这些文件的定义可以使用标准 HTML、XHTML、WML、和 / 或 XML 样式语言来格式化。该文件可包括指向存储器 326 中的附加离线存储位置或移动设备 110 可访问的因特网网站的链接。在一些实现中, web 服务器 306 可以支持诸如 SSL 等安全协议。web 服务器 306 可以将存储器 326 中的应用程序传输给移动设备 111 以供安装和执行。

[0061] 作为实时操作系统的一部分, 实时框架 308 可以至少部分地基于一个或多个时间段来执行一个或多个功能。例如, 实时框架 308 可使得 CPU 上可用的内部时钟能够至少响应于所请求的事件来提供时间戳。实时框架 308 可允许预先安排某些任务, 以便至少响应于某些基于时间和 / 或事件的触发器来执行这些任务。在一些实现中, 实时框架 308 可允许 CPU 在某些交易中插入延迟。在一些实现中, WAP 标准的被称为 WTAI (无线电话应用程序接口) 的一部分可被实现成允许卡 112 上的离线浏览器页面利用移动设备 110 所提供的功能 (例如, 发送 / 接收无线数据、发送 / 接收 SMS、进行语音呼叫、播放铃声等)。

[0062] 实时操作系统 316 可以执行或以其他方式包括以下各项中的一个或多个: 实时框架 308; 实现交易卡 CPU 与移动设备 110 之间的物理接口的主机进程; 实现交易卡 CPU 与安全模块之间的物理接口的接口; 实现交易卡 CPU 与存储器 324 和 / 或 326 之间的 ISO 7816 物理接口的存储器管理进程; 实现 API 和 UI 能力的应用层进程; web 服务器 306; 天线控制功能 320; 功率管理; 和 / 或其他。在一些实现中, 实时操作系统 316 可以管理交易卡 CPU 与安全存储器 324 之间的物理接口, 安全存储器 324 包括用于允许受限访问特定存储器区域的存储器分段和 / 或数据缓冲区 / 管道。在一些实现中, 安全模块可包括安全模块供应商所提供的安全模块操作系统并可以兼容 Visa 和 MasterCard 规范。该安全模块操作系统可以将安全模块中的数据结构化兼容 Paypass 和 / 或 payWave 规范或任何其他可用无接触零售支付工业规范。另外, 安全模块可以在安全元件 324 中存储主机设备签名和天线 322 的允许模式。在一些实现中, 实时操作系统 316 可包括被配置成诸如例如通过将原始 FV 数据 (账号、有效期、CVN、其他应用程序专用细节) 转换成安全的加密信息来个性化安全元件 324 的微控制器操作系统。另外, 微控制器操作系统可以将卡 112 作为 MicroSD 大容量存储来呈现给主机设备。微控制器操作系统可将该存储器分区成用户部分和保护设备应用程序部分。在该示例中, 设备应用程序部分可用于存储从该存储器部分操作或从该存储器部分安装在主机设备上的提供商专用应用程序。

[0063] 安全模块芯片可以提供防篡改硬件安全功能以用于使用多个安全域、用于个性化的板载处理能力、访问和存储、和 / 或其他来加密、认证、管理用户凭证。在一些实现中, 安全模块芯片可包括无接触芯片组 318。

[0064] 无接触芯片组 318 可以提供用于 RF 通信的硬件协议实现和 / 或驱动程序。例如, 无接触芯片组 318 可包括用于使用无线 / 无接触连接来与外部世界连接进行接口的板载 RF 电路。该无线连接可以是例如客户机到节点 (终端 / 读取器 / 基站)、节点到客户机 (无源标签)、或对等 (另一交易卡 112)。

[0065] 天线控制功能 320 可以控制 RF 天线的可用性。例如, 天线控制功能 320 可响应于

例如成功认证、完成操作系统 316 所建立的例程、和 / 或其他事件来激活 / 停用天线 322。天线 322 可以是经由诸如与非门或其他元件等软件开关连接到 NFC 镶嵌 (inlay) 的短程无线天线。

[0066] 在执行交易时,钱包管理系统 328 可有选择地在多个凭证 314 之间切换。例如,钱包管理系统 328 可以标识默认账户、切换规则、和 / 或其他信息。在一些实现中,钱包管理系统 328 可以响应于诸如使用非默认凭证完成交易等至少一个事件自动地切换到默认用户凭证。切换规则可以标识用户凭证和相关联的事件,以使钱包管理系统 328 至少响应于确定一事件来切换到用户凭证。

[0067] 图 4 是示出根据本发明的一些实现的示例智能卡 400 的框图。例如,可以根据所示智能卡 400 来实现图 1 的交易卡。一般而言,智能卡 400 可独立地访问服务和 / 或交易。智能卡 400 只是出于说明的目的并可包括部分、全部、或不同的元件而不背离本发明的范围。

[0068] 如图所示,智能卡 400 包括天线 402、开关加调谐电路 404、安全模块和无接触芯片组 406、CPU 408、以及存储器 410。天线 402 无线地发送并接收诸如 NFC 信号等信号。在一些实现中,开关加调谐电路 404 可动态地调整天线 402 的阻抗以调谐发送和 / 或接收频率。另外,开关加调谐电路 404 可至少响应于来自 CPU 408 的命令来有选择地打开和关闭天线 402。在一些实现中,天线 402 可以是经由诸如与非门或其他元件等软件开关连接到 NFC 镶嵌以允许来自 CPU 408 的代码打开和关闭天线 402 的短程无线天线。在一些实现中,盘 400 可包括 NFC 镶嵌 (未示出),NFC 镶嵌可作为 NFC 短程无线技术的、从读取器终端导出功率以发送回数据的无源实现或使用 eNFC 芯片组来对活动读取器模式和自训练模式供电的更强实现。另外,盘 400 可包括促使 CPU 408 解除存储器或安全元件的个性化的外部针尖复位 (未示出)。

[0069] CPU 408 可响应于诸如用户请求、交易完成、和 / 或其他等事件来发送开关命令。在打开时,安全芯片和无接触芯片组 406 连接到天线 402 并执行以下过程中的一个或多个:根据一种或多种格式来格式化信号以用于无线通信;解密接收到的消息并加密所发送的消息;认证本地地存储在存储器 410 中的用户凭证;和 / 或其他过程。存储器 410 可包括安全和非安全部分。在该实现中,安全存储器 410 可以存储不可由用户访问的一个或多个用户凭证。另外,存储器 410 可以存储离线网页、应用程序、交易历史、和 / 或其他数据。在一些实现中,存储器 410 可包括从 64MB 到 32GB 的闪存。另外,存储器 410 可被分成用户存储器和设备应用程序存储器。芯片组 406 可包括安全模块,该安全模块是例如经鉴定用于存储金融运输工具数据的 Visa 和 / 或 MasterCard 和 / 或是根据全球标准的。除用户金融运输工具之外,安全元件可以存储所允许的主机设备的签名和 / 或天线模式。

[0070] 在一些实现中,CPU 408 可至少部分地基于例如用户、批发商 (例如,金融机构、服务提供商) 等定义的个性化参数来在活动和非活动模式之间切换天线 402。例如,在智能卡 400 物理地连接到主机设备并且在成功地执行了与该主机设备的握手时,CPU 408 可激活天线 402。在一些实现中,在智能卡 400 从主机设备移除时,CPU 408 可自动地停用天线 402。在一些实现中,天线 402 总是活动的以使智能卡 400 可用作独立的接入设备 (例如,钥匙链上的设备)。关于握手过程,CPU 408 可以在激活智能卡 400 和 / 或天线 402 之前执行一个或多个认证过程,如图 7 所示。例如,CPU 408 可以执行物理认证、设备认证、和 / 或

用户认证。例如，CPU 408 可以至少响应于检测到与主机设备的物理接口（例如，SD 接口）的连接和在主机设备上成功安装用于大容量存储器访问的设备驱动程序（例如，SD 设备驱动程序）来激活天线 402。在一些实现中，除在存储在存储器（例如，安全模块）中的在首次使用（供应）期间创建的设备签名与使用例如主机设备的唯一参数计算的运行时签名之间进行的签名比较之外，设备认证可包括物理认证。在存储器中不存在主机设备签名的情况下，CPU 408 可绑定盘 400 所插入的第一个兼容主机设备。兼容主机设备可以是成功地实现物理认证的设备。如果主机设备签名存在于存储器中，则 CPU 408 将所存储的签名与当前主机设备的实时签名相比较。如果签名匹配，则 CPU408 可继续进行来完成引导操作。如果签名不匹配，则拒绝主机设备，中止引导并且将盘 400 返回到在插入到该设备之前的模式。

[0071] 用户认证可包括使用用户所输入的 PIN、用户唯一的且存储在主机设备上的 x. 509 类证书、和 / 或其他过程来验证与该用户的物理连接。设备和用户认证可通过设备签名的比较和通过用户 PIN 或证书的验证的用户认证来验证与设备的物理连接。在一些实现中，用户可以在供应时选择 PIN 或证书。如果是这种情况，则 CPU 408 可以在主机设备上实例化软件插件。例如，软件插件可以实时地请求用户的 PIN，读取安装在该设备上的用户证书（例如，x. 509）、和 / 或其他。软件插件的操作可由提供商来定制。无论如何，所返回的用户数据可以与存储在存储器中的用户数据相比较。在成功匹配的情况下，可以激活天线 402。在证书不成功匹配的情况下，停用盘 400。在不成功的 PIN 匹配的情况下，可请求用户重复 PIN 尝试直至成功的匹配或尝试次数超过阈值。盘提供商可定制该尝试阈值。

[0072] 关于网络认证，主机设备可以是蜂窝电话，以使盘 400 可以在激活之前请求网络认证。例如，盘 400 可以由需要网络认证的无线网络运营商 (WNO) 分发。在该示例中，存储器中的标志可被设为 ON(打开)，从而指示需要网络认证。如果该标志被设为 ON，则关于所允许网络的唯一身份被本地地存储在存储器中，该唯一身份诸如 GSM 网络的移动网络码、CDMA 网络的 NID、宽带网络的 SSID、和 / 或标识符。如果该标志是 ON，则 CPU 408 可至少响应于插入来请求将专用软件插件下载到主机设备并实例化。该软件插件可查询主机设备来自网络细节进行响应。在一些情况下，所使用的唯一网络身份的类型和用于从主机设备对它进行推断的方法是可变的并取决于网络提供商和该主机设备的能力。如果存储在本地的 ID 匹配请求 ID，则 CPU 408 激活天线 402 以允许访问，或否则拒绝服务。

[0073] 图 5 示出用于使用多个接口中的一个来无线地传递交易信息的示例交易系统 500。例如，系统 500 可以使用有线或无线接口来与交易卡 112 进行接口。关于有线接口，系统 500 包括适配器 504 和读取器 506。适配器 504 可包括被配置成在与卡 112 相兼容的格式和与客户机 104c 相兼容的格式之间进行转换的任何软件、硬件、和 / 或固件。例如，适配器 504 可以在 microSD 协议与 USB 协议之间进行转换。读取器 506 可包括被配置成直接与卡 112h 进行接口的任何软件、硬件、和 / 或固件。例如，读取器 506 可以是 microSD 读取器，以使客户机 104d 使用 microSD 协议与卡 112h 进行接口。关于无线接口，系统 500 可包括蜂窝接口 502 和短程无线接口 508。关于蜂窝接口 502，机构 106 可使用移动设备 110e 的蜂窝无线电技术与交易卡 112e 无线地通信。例如，蜂窝接口 502 可以是 CDMA 接口、GSM 接口、UMTS 接口、和 / 或其他蜂窝接口。关于短程无线接口 508，机构 106 可使用例如 WiFi 技术与交易卡 112f 无线地通信。短程无线接口 508 可以是 802. 11 接口、蓝牙接口、和 / 或

其他无线接口。在这些实现中,客户机 104e 可包括用于与交易卡 112f 无线地通信的收发机。

[0074] 图 6 是智能卡(例如,交易卡 112、服务卡 210)的个性化的示意图 600。具体地,该智能卡在发行给用户之前(即,预发行)或在发行给用户之后(即,后发行)可被个性化。关于预发行,可以例如在工厂大批量地对智能卡进行个性化。在该示例中,每一智能卡可以加载有用户凭证、安全框架、应用程序、离线网页、和 / 或其他数据。在一些实现中,智能卡可在例如银行分行处被单独地个性化。在这种情况下,在例如购买智能卡后,该盘可以单独地加载有与用户相关联的数据。至于后发行,可以无线地个性化智能卡。例如,交易卡 112 可以通过使用移动设备 110 建立的蜂窝连接来个性化。在一些实现中,智能卡可通过与诸如客户机 104 等计算机进行同步来个性化。

[0075] 在一些实现中,智能卡的供应可以至少部分地基于分发实体(例如,金融机构、无线运营商、用户)。例如,智能卡可以由诸如银行等金融机构来分发。在该银行实现中,智能卡可与用户账户一起预先提供。在这种情况下,智能卡可以至少响应于初始插入到主机设备来激活。天线模式可被默认设置为只能物理认证。在一些示例中,用户可以自己选择 PIN 认证或在主机设备不具有屏幕和键盘的情况下通过 PC 支架 (cradle) 和插件管理软件来防止未授权使用。在无线运营商实现中,智能卡在激活之前需要设备认证。在一些示例中,用户可以使用若干方法中的一种来提供金融数据(例如,信用卡或借记卡)。另外,用户可以添加用户认证。在用户提供的实现中,用户可从例如零售商店或如 OEM 主机设备制造商等其他渠道取得智能卡。在这种情况下,用户可以使用提供商所选择的供应来在多个不同设备中激活该盘。

[0076] 关于针对金融交易来激活,智能卡可在用户从例如银行、无线运营商、第三方提供商、和 / 或其他取得该盘时被配置成存储器模式。激活该盘可包括以下两个层次:1) 物理上,在提供商所需的特定一组情况下指定天线可用性;和 b) 逻辑上,在金融机构处指示激活盘上所携带的金融运输工具的激活。在一些实现中,激活可至少部分地基于设备批发商、天线可用性选择、和 / 或主机设备的类型,如下表 1 所示。

[0077] 表 1

[0078]

插件销售商和分发模式	插件初始状态和天线可用性选择	设备不具有屏幕 / 键盘	设备具有屏幕和键盘
<p>FI :金融机构 (银行或零售商) 将插件直接运送给用户或通过再销售商 / 批发商的参与等。</p>	<p>插件处于存储器模式,其完全使用用户账户信息 (FV) 来个性化且天线模式被设为物理认证</p>	<p>手动 :用户必须呼叫 FI 的号码来激活他的账户,该设备只可操作单个账户。用户还可以使用另一 PC 访问 FI 在因特网上的站点来激活他的账户</p>	<p>如果该设备有无线访问的能力,则在插入后,插件产生一网页并将用户带到 FI 的网站。用户自己通过输入他的账号并匹配秘密个人信息 (例如, SSN 或家庭电话号码的最后四位) 来激活他的账户。同时,用户还可以任选地选择 PIN (将天线可用性改变成用户认证)。如果因特网连接不可用,则该设备可自动地向 FI 的号码拨打语音呼叫以激活账户。如果无线连接也不可用 (设备只是 PDA), 则用户必须退回到手动激活 (参见左栏)</p>
<p>WNO :无线网络运营商运送与主机设备一起打包的插件,如果用户想要使用该服务则该用户可以选择他优选的主机设备并将插件与它一起打包。</p>	<p>插件处于存储器模式,其被部分个性化的设备签名以防止用户改变主机设备) 而 FV 信息未加载。天线可用性被设为设备认证 (插件只可与运送它的主机设备一起使用)</p>	<p>不适用</p>	<p>假定 :设备具有可使用的无线连接。运营商提供打包的钱包管理应用程序。在用户点击该钱包管理应用程序时,邀请该用户向运营商的伙伴 FI 注册新账户。一旦注册成功,通过空中或通过因特网将账户数据下载到插件,并且激活它以供使用。在该场景中,设备可以使</p>

插件销售商和分发模式	插件初始状态和天线可用性选择	设备不具有屏幕 / 键盘	设备具有屏幕和键盘
			<p>用多个 FI 并存储多个 FV。用户可以选择输入针对钱包管理应用程序中的一 FV 的 PIN 以将天线可用性转换成用户和设备认证,因为该 FV 插件被绑定到设备签名。在从设备移除时,天线关闭并且插件转换成简单的大容量记忆棒。在将插件插入到另一主机设备时,该签名不匹配并且天线关闭。</p>
<p>WNO :无线网络运营商将插件作为附件来与针对兼容设备的建议一起运送,用户可以选择他优选的主机设备并尝试用它操作插件来利用该服务</p>	<p>插件处于存储器模式,它未被个性化。天线可用性被设为网络认证,网络认证被设为 ON。插件将绑定到其被插入的并且其中网络认证成功的第一设备</p>	<p>不适用</p>	<p>假定 :设备具有可用的无线连接。插件将产生到运营商门户的因特网连接并且在用户确认后钱包管理应用程序将被下载。用户可以拒绝下载并选择通过过去往第三方钱包提供商或直接去往 FI 网站来手动地供应 FV 数据。插件被绑定到该设备和网络提供商的网络。如果同一设备被解锁并被用于另一网络上,则该插件将停止操作并将回复到存储器模式。在从设备移除时,插件将回复到存储器模式。</p>

插件销售商和分发模式	插件初始状态和天线可用性选择	设备不具有屏幕 / 键盘	设备具有屏幕和键盘
OEM 1 :蜂窝电话制造商	设备认证 (设备与蜂窝电话绑定)	不适用	选项 A :设备制造商提供钱包管理应用程序,过程的其余部分与上述过程一样。选项 B :无线运营商提供钱包管理应用程序。用户通过空中去往无线运营商门户并下载该应用程序。该过程的其余部分与以上过程一样。选项 C :用户导航到第三方钱包管理应用程序 (例如, paypal 或 Google) 通过因特网来向参与的 FI 提供注册并且在插件上个性化 FV。选项 D :用户导航到 FI 的网站并且激活通过因特网在插件上个性化的新账户。
OEM 2 :其他制造商	设备认证	用户必须使用因特网连接将设备挂载到 PC 并通过直接去往 FI 的网站来在该 PC 上注册。经由该支架通过因特网下载账户并随后激活该设备。在该过程中,插件被绑定到设备签名。在从主机设备移除时,天线关闭。在被插入到另一设备时,设备签名失败并且该设备只用作大容量存储器设备。	如果设备具有无线连接 (其是无线 PDA) :同上。如果设备不具有无线连接 (其是未连接的 PDA) :参见左栏

[0079]

[0080]

[0081] 所示图表只是出于示例目的。用户可以使用相同、部分、或不同的过程来激活智能卡而不背离本发明的范围。

[0082] 在所示实现中,交易卡 112 可被升级来使用多个用户凭证执行钱包系统。例如,交易卡 112 可以通过无线或有线连接用例如钱包管理系统 328 来升级。除升级交易卡 112 之外,附加用户凭证可以被加载到存储器。在这种情况下,交易卡 112 可以至少部分地基于规则、用户选择、事件、和 / 或其他方面来有选择地在不同的用户凭证之间切换。

[0083] 图 7 是示出用于至少响应于插入到主机设备来自动地引导智能卡的示例方法 700 的流程图。一般而言,智能卡可以在激活之前执行一个或多个认证过程。该流程图中的许多步骤可以同时发生和 / 或以与所示次序不同的次序发生。系统 100 或系统 200 可以使用具有更多步骤、更少步骤、和 / 或不同步骤的方法,只要这些方法适当。

[0084] 方法 700 在步骤 702 开始,在此检测到插入主机设备。例如,交易卡 112 可以检测插入到移动设备 110。在判定步骤 704,如果该智能卡的任何方面都不需要认证,则执行结束。如果至少一方面需要认证,则执行继续进行到判定步骤 706。如果与主机设备的通信包括一个或多个错误,则在步骤 708,向用户指示失败。在该示例中,交易卡 112 可以使用 GUI 111 向用户呈现通信错误的指示。如果在判定步骤 706 未检测到通信错误,则执行继续进行到判定步骤 710。在一些实现中,智能卡将 SD 驱动程序上传到主机设备。如果智能卡只需要物理认证,则执行继续进行到判定步骤 712。如果网络认证标志未被设置为 ON,则在步骤 714,打开天线并且用主机设备签名更新智能卡。对于该示例,交易卡 112 可以激活天线以用于无线交易并用主机签名更新本地存储器。在判定步骤 712,如果网络认证标志被打开,则在步骤 716,智能卡向主机设备发送对网络 ID 的请求。接着,在步骤 718,智能卡检索存储在本地的网络 ID。在判定步骤 720,如果所存储的网络 ID 和请求网络 ID 相匹配,则在步骤 714 激活该盘。如果两个网络 ID 不匹配,则在步骤 722 停用天线。

[0085] 返回到判定步骤 710,如果认证不只是物理认证,则执行继续进行到判定步骤 724。如果认证过程包括设备认证,则在步骤 726,智能卡向主机设备发送对网络 ID 的请求。在步骤 728,智能卡检索存储在本地的设备签名。如果智能卡不包括至少一个设备签名,则执行继续进行到判定步骤 734。如果智能卡包括一个或多个设备签名,则执行继续进行到判定步骤 732。如果设备签名中的一个与请求网络 ID 相匹配,则执行继续进行到判定步骤 734。如果各签名与请求网络 ID 不匹配,则执行进行继续到步骤 722 以停用。如果用户认证未包括在认证过程中,则执行继续进行到判定步骤 712 以进行物理认证。在判定步骤 734,如果包括用户认证,则执行继续进行到步骤 738。

[0086] 返回到判定步骤 724,如果认证过程不包括设备认证,则执行继续进行到判定步骤 736。如果该过程不包括用户认证,则在步骤 722 关闭智能卡。如果包括用户认证,则在步骤 738,智能卡使用主机设备从用户处请求 PIN 号。再次返回该示例,交易卡 112 可以通过 GUI 111 向用户呈现输入 PIN 的请求。在步骤 740,智能卡检索存储在本地的 PIN。在判定步骤 742,如果请求 PIN 与所存储的 PIN 匹配,则执行继续进行到判定步骤 712 以进行物理认证。在判定步骤 742,如果请求 PIN 与所存储的 PIN 不匹配,则执行继续进行到判定步骤 744。如果尝试次数未超过指定阈值,则执行返回到步骤 738。如果尝试次数超过阈值,则在

步骤 722 停用天线。

[0087] 图 8 是根据本发明的一些实现的示例呼叫流程 800。如图所示,流程 800 包括网络 802、主机设备 804、智能卡 806、以及终端 808。主机设备 804 被配置成与网络 802 通信并包括供插入智能卡 806 的槽。智能卡 806 被配置成向主机设备 810 所执行的用户界面应用程序 810 发送命令并从中接收数据并且独立于主机设备 810 来执行交易。卡 806 包括用于执行交易的 CPU 812 和用于与终端 808 进行通信的无线芯片组 814。CPU 812 执行主机控制器 /API 界面 816,该主机控制器 /API 界面 816 被配置成以与主机设备 804 相兼容的形式发送命令并将数据从主机设备 804 转换成与 CPU 812 相兼容的形式。

[0088] 如图所示,流程 800 可包括主机设备 804 与卡 806 之间以及卡 806 与终端 808 之间的多个会话 820。会话 820a 示出卡 806 使用主机设备 810 的网络能力所管理的会话。在该示例中,卡 806 发送数据以通过连接到主机设备 804 的蜂窝网络传输,并且在接收到蜂窝数据后,主机设备 804 将该数据发送到网络 802。响应于从网络 802 接收到数据,主机设备 804 可自动地将接收到的数据发送到卡 806。在一些实现中,卡 806 可以向主机设备 804 发送对设备签名的请求,如在会话 820b 中所示。例如,卡 806 可以在引导过程期间请求设备签名。会话 820c 示出用户可以通过主机设备 804 的接口向卡 806 提交命令。例如,用户可以请求该盘通过主机设备 804 的界面显示用户的交易历史。

[0089] 在一些实现中,卡 806 可以通过主机设备 804 接收用于激活或停用天线的命令,如在会话 820d 中所示。例如,金融机构可以标识非正常交易并通过网络 802 发送停用卡 806 的命令。卡 806 可以通过使用主机设备 804 请求 PIN 来授权用户。如在会话 820e 中所示,用户可以使用主机设备 804 的界面向卡 806 提交 PIN,并响应于对所提交的 PIN 的评估,卡 806 可以通过主机设备 804 呈现用户验证成功或失败的指示。在一些实现中,用户和 / 或金融机构可以请求卡 806 的交易历史,如在会话 820f 中所示。例如,金融机构可以通过连接到主机设备 804 的网络 802 发送对交易历史的请求,并且卡 806 可以至少响应于该请求来使用连接到主机设备 804 的网络 802 向金融机构发送交易历史。在一些实现中,用户可以呈现存储在卡 806 中的离线网页,如在会话 820g 中所示。例如,卡 806 可以使用主机设备 804 从用户接收呈现离线网页的请求并使用该请求中的 URL 来呈现该离线网页。在一些实现中,存储在卡 806 的存储器中的数据可以通过例如主机设备 804 来呈现,如在会话 820h 中所示。例如,用户可以请求与交易相关联的关于特定数据的专用信息,并且卡 806 可以检索该数据并使用主机设备 804 将该数据呈现给用户。另外,用户可以向卡 806 中的存储器写数据,如在会话 820i 中所示。例如,用户可以用注释更新交易数据,并且卡 806 可以至少响应于该请求来指示该更新成功还是失败。呼叫会话 820m 示出可通过主机设备 804 接收到对用户凭证的选择。例如,会话 820m 可至少部分地基于用户通过设备 804 的 GUI 选择图形元素、主机设备 804 接收到的无线信号、和 / 或其他来切换用户凭证。

[0090] 关于卡 806 与终端之间的会话,流程 800 示出个性化会话 820k 和交易会 820l。关于个性化,金融机构可以用用户凭证、用户应用程序、网页、和 / 或其他信息来个性化卡 806,如在会话 820k 中所示。例如,终端 808 可以向卡 806 发送包括相关联的数据的供应请求。协议转换 818 可以将该个性化请求转换成与卡 806 相兼容的形式。至少响应于该请求,CPU 812 使用协议转换 818 发送该个性化成功与否的指示。在终端执行交易之前,终端 808 可以向卡 806 提交交易质询,如在会话 820l 中所示。在这种情况下,卡 806 可以标识主机

设备 804 的设备签名,通过主机设备 804 向用户呈现相关联的数据,并使用协议转换 818 向终端 808 发送该签名。

[0091] 图 9 是示出用于激活包括智能卡的无线交易系统的示例方法 900 的流程图。一般而言,智能卡可以响应于例如来自用户的选择执行一个或多个激活过程。该流程图中的许多步骤可以同时发生和 / 或以与所示次序不同的次序发生。系统 100 或系统 200 可以使用具有更多步骤、更少步骤、和 / 或不同步骤的方法,只要这些方法适当。

[0092] 方法 900 在步骤 902 开始,在此接收激活交易卡的请求。例如,用户可以选择通过图 1 中的移动主机设备 110 的 GUI 111 显示的图形元素。在判定步骤 904,如果包括账户激活,则在步骤 906,使用主机设备的蜂窝无线电技术将激活相关联的用户账户的请求无线地发送到金融机构。例如,图 2 的交易卡 112d 可以使用移动主机设备 110d 的蜂窝无线电技术向机构 106 无线地发送激活请求。如果不包括账户激活,则执行继续进行到判定步骤 908。如果不包括卡激活,则执行结束。如果包括卡激活,则执行继续进行到判定步骤 910。如果不包括激活码,则在步骤 912,使用主机设备的 GUI 向用户呈现一个或多个预编程的问题。返回到初始示例,交易卡 112 可以标识存储在本地的问题并使用移动主机设备 110 的 GUI 111 向用户呈现这些问题。在步骤 914,标识存储在本地的对于预编程的问题的答案。返回到判定步骤 910,如果包括激活码,则执行继续进行到判定步骤 916。如果激活码由用户手动地输入,则在步骤 918,通过移动主机设备的 GUI 向用户呈现对激活码的请求。在最初示例中,交易卡 112 可以通过移动主机设备 110 的 GUI 111 向用户呈现对诸如字符串等激活码的请求。如果激活码不是由用户手动地输入的,则在步骤 920,交易卡使用主机设备的蜂窝无线电技术无线地发送对激活码的请求。在该蜂窝示例中,交易卡 112 可以使用蜂窝核心网络 202 向金融机构发送请求。在任一示例中,在步骤 922,标识存储在本地的激活码。在判定步骤 924,如果存储在本地的信息与所提供的信息相匹配,则在步骤 926,激活交易卡。例如,交易卡 112 可以至少响应于用户通过 GUI 111 输入匹配的激活码来激活。如果所提供的信息不匹配存储在本地的信息,则执行结束。

[0093] 图 10 示出根据本发明的一些实现的示例安全存储器 1000。一般而言,安全存储器 1000 被配置成存储多个不同金融机构的用户凭证。例如,每一凭证可以与不同的用户账户(例如,信用卡、用户账户)相关联。在所示实现中,安全存储器 1000 包括由逻辑屏障 1010-c 分开的用户凭证 1002a-c 和相关联的安全框架 1006a-c。另外,安全存储器 1000 包括主凭证 1004 和主安全框架 1008。每一用户凭证 1002 可以与不同的用户账户和 / 或机构相关联。对于每一用户凭证 1002,都分配或以其他方式相关联一安全框架 1006。安全框架 1006 可以是智能卡至少响应于选择用户账户来执行的支付应用程序。例如,安全框架 1006 可以根据授权请求的指定格式、协议、加密、和 / 或其他方面来执行交易。在一些实现中,安全框架 1006 基本上可以阻止对用户凭证的未授权访问。例如,每一安全框架 1006 可以包含提供不同访问级别的多个密钥。框架 1006 内的每一应用程序随后可被配置成可根据特定安全级别来访问。在一些实现中,安全框架 1006 可为一种类型的金融工具(例如,Visa)包括不同版本的支付应用程序。在一些实现中,安全框架 1006 可以使用应用程序 ID 来标识。

[0094] 主凭证 1004 和主安全框架 1008 可以使金融机构能够存储或更新用户凭证 1002 和相关联的安全框架 1006。例如,对安全框架 1006 内的新密钥的创建可由主框架的根密钥

来保护。屏障 1010 可以在不同的可选用户凭证 502 和相关联的安全框架 1006 之间生成安全域。例如,金融机构可以访问用户凭证 1002 和相关联的安全框架 1006 以寻找所管理的用户账户,但可基本上阻止访问不同金融机构的用户凭证 1002 和相关联的安全框架 1006。

[0095] 在一些实现中,智能卡(例如,交易卡 112)可以响应于至少一事件来动态地在各用户凭证 1002 和各安全框架 1006 之间切换。例如,在完成交易后,智能卡可切换到默认用户凭证 1002 和对应的安全框架 1006。在一些实现中,智能卡可响应于来自用户的通过例如图 1 的 GUI 111 的选择来切换用户凭证 1002 和安全框架 1006。智能卡通常可至少部分地基于不同的情况来在不同的用户账户之间切换。关于添加用户账户,用户可以使用主机设备的 GUI 手动地输入用户凭证 1002。在一些实现中,存储器 1000 可以使用主机设备的蜂窝无线电技术来通过空中 (OTA) 更新。

[0096] 图 11 是示出用于动态地在用户账户之间切换的示例方法 1100 的流程图。一般而言,智能卡可响应于至少一事件来动态地在多个可选用户凭证和相关联的安全框架之间切换。该流程图中的许多步骤可以同时发生和 / 或以与所示次序不同的次序发生。系统 100 或系统 200 可以使用具有更多步骤、更少步骤、和 / 或不同步骤的方法,只要这些方法适当。

[0097] 方法 1100 在步骤 1102 开始,在此标识事件。例如,图 1 的交易卡 112 可以确定以下各项中的一个或多个已经更新:网络 ID、电话号码、MAC 地址、和 / 或其他信息。在一些实现中,该事件可包括标识交易或潜在交易的一个或多个方面。例如,交易卡 112 可以确定企业、企业类型、商品和 / 或服务、商品和 / 或服务的类型、和 / 或其他方面。在步骤 1104,确定当前选择的用户账户。在该示例中,交易卡 112 可以确定当前选择的用户凭证和安全框架。在判定步骤 1106,如果切换用户账户,则在步骤 1108,智能卡至少部分地基于所标识的事件将当前选择的用户账户动态地切换到不同的用户账户。同样在该示例中,交易卡 112 可至少部分地基于一个或多个事件在多个可选择用户账户之间动态地切换。接着,在步骤 1110,接收执行请求。对于该示例,交易卡 112 可直接接收与接入点 114 执行交易的无线请求。至少响应于该请求,在步骤 1112,向用户呈现执行交易的请求。在该示例中,交易卡 112 可以通过移动主机设备 110 的 GUI 111 向用户呈现该请求。在一些实现中,交易卡 112 可以通过 GUI 111 向用户呈现当前选择的用户账户。在步骤 1114,至少响应于来自用户的选择使用所选择的用户凭证和对应的安全框架来执行请求交易。同样在该示例中,交易卡 112 可以至少响应于用户选择移动主机设备 110 的 GUI 111 中的图形元素来执行请求交易并直接向接入点 114 无线地发送授权请求。在判定步骤 1116,如果对账户的选择切换到了默认账户,则智能卡将所选用户账户自动地切换到默认用户凭证和对应的安全框架。如果该选择不是切换到默认账户,则执行结束。

[0098] 已经描述了本发明的多个实施例。然而,应当理解的是,在不背离本发明的精神和范围的情况下,可作出多种修改。因此,其他实施例也在所附权利要求的范围之内。

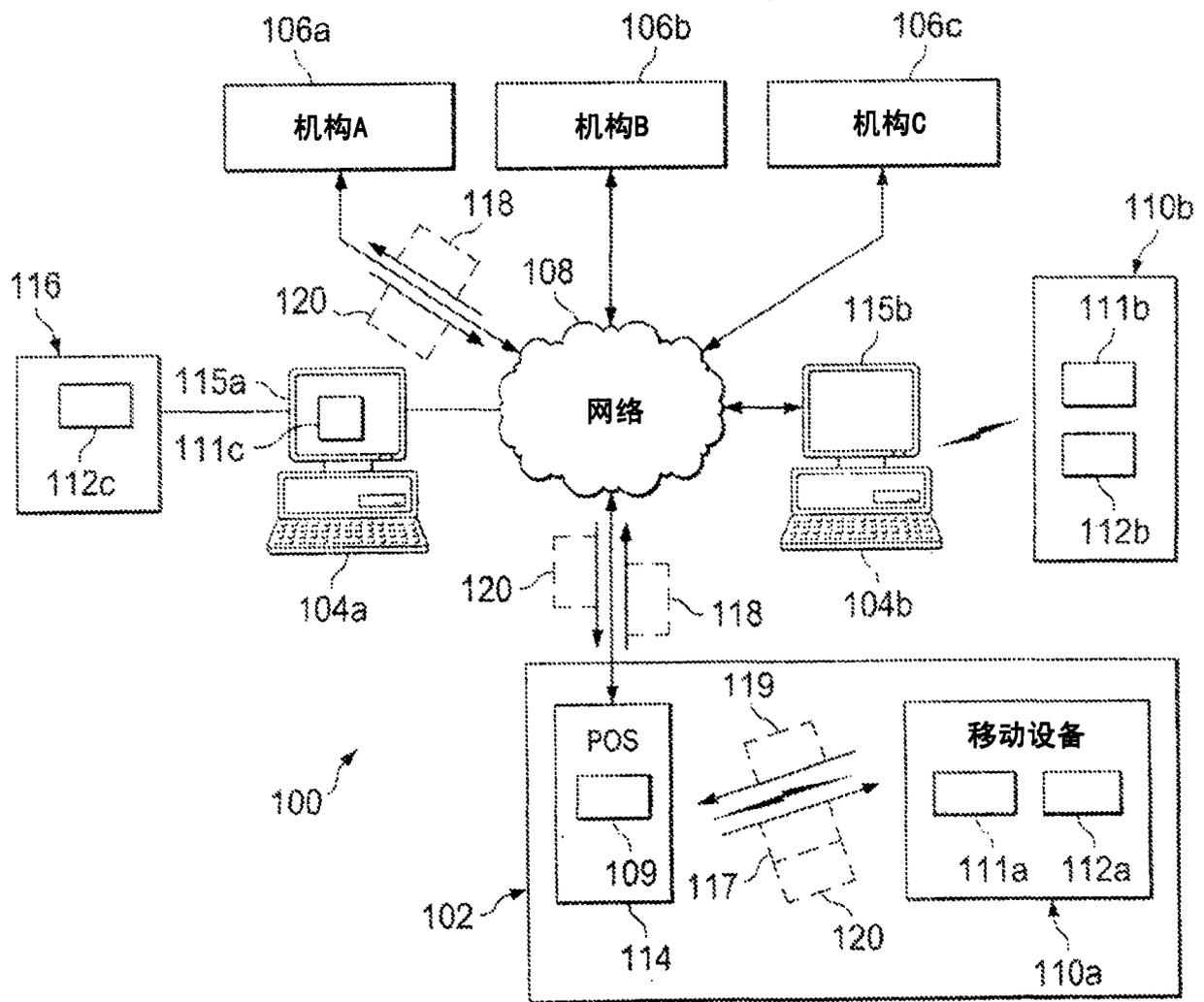


图 1

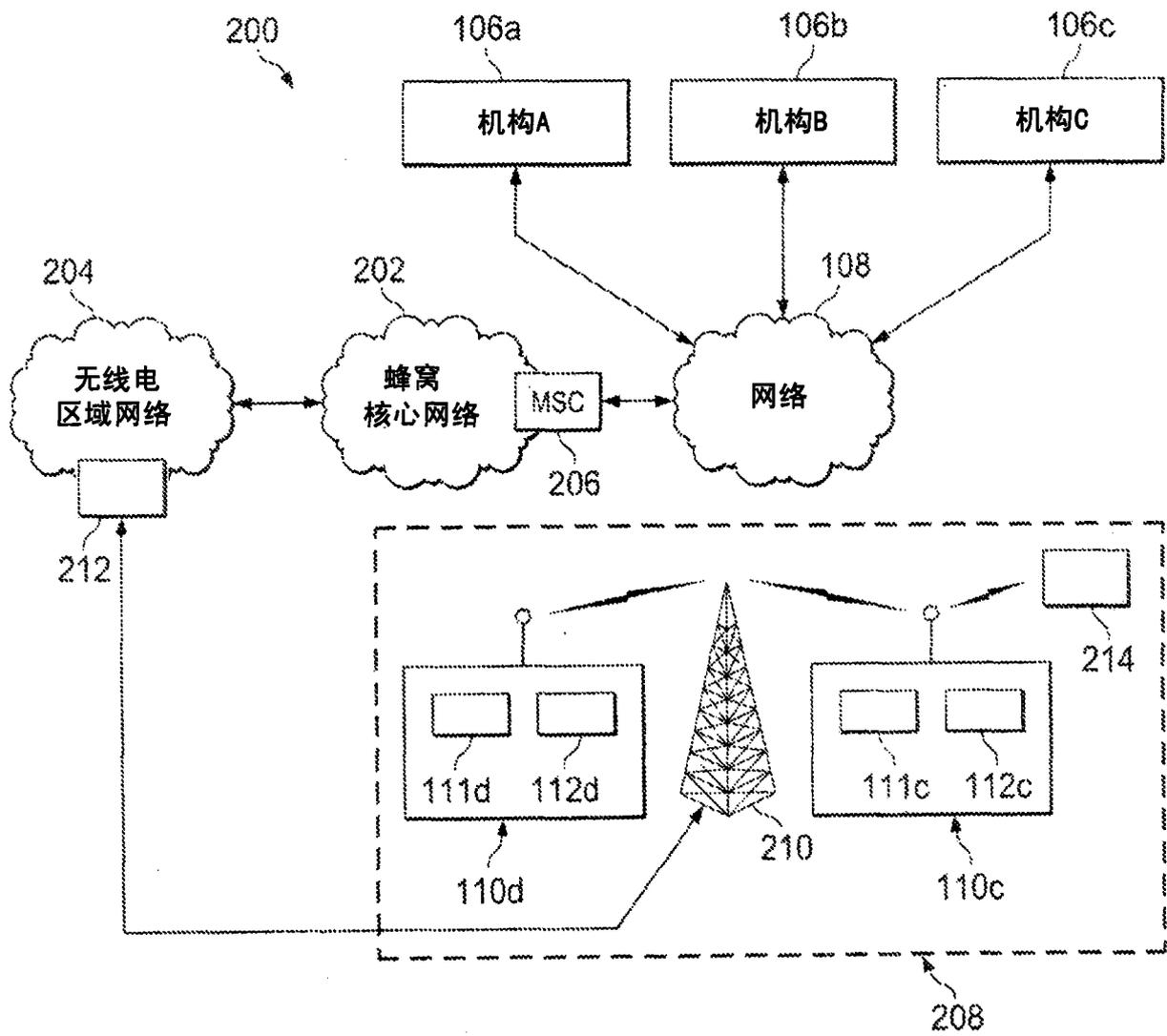


图 2

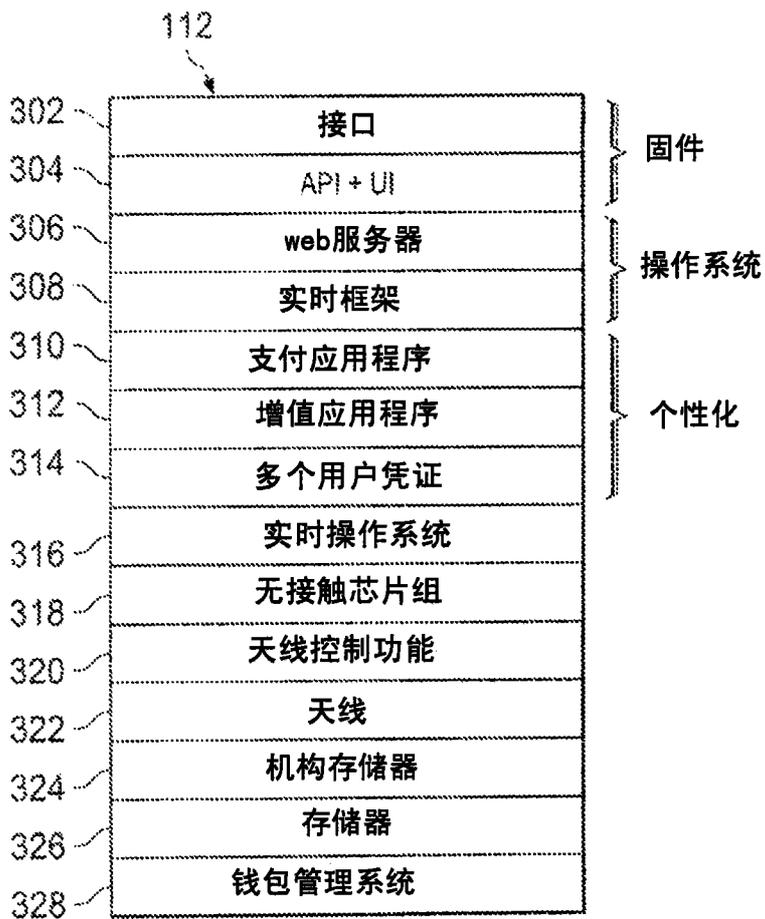


图 3

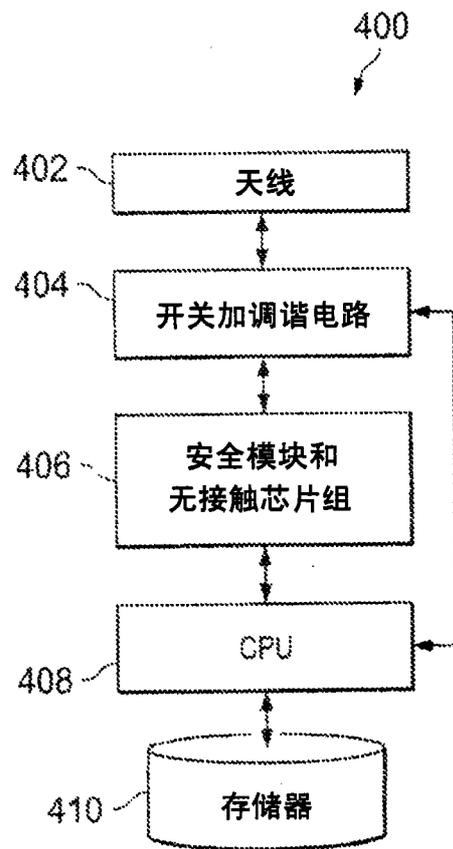


图 4

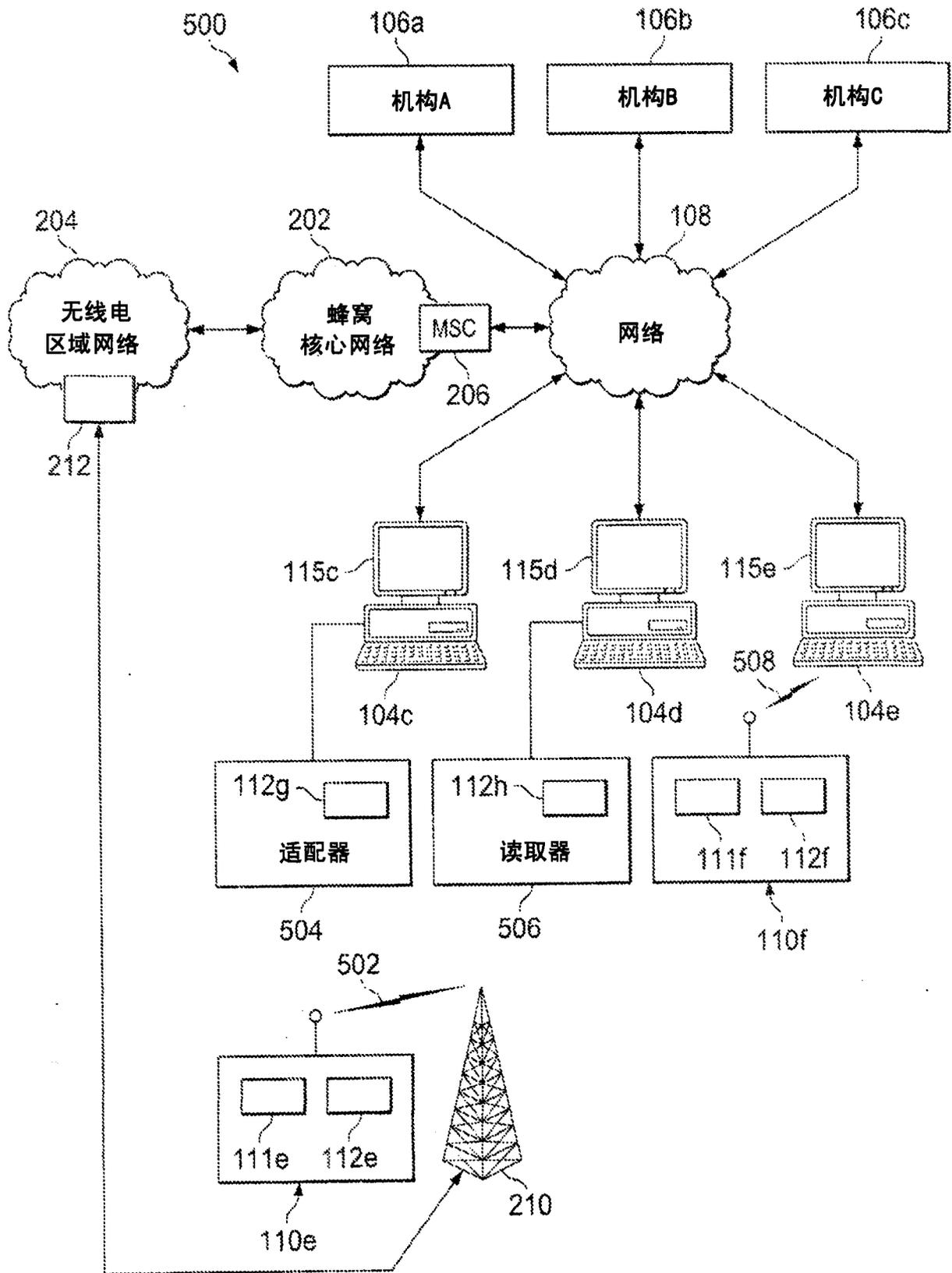


图 5

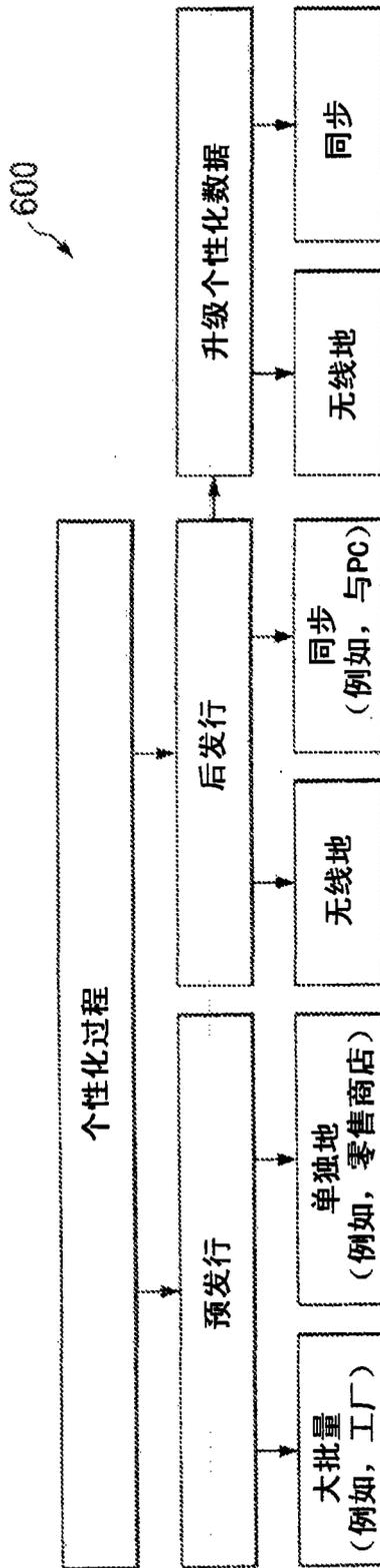


图 6

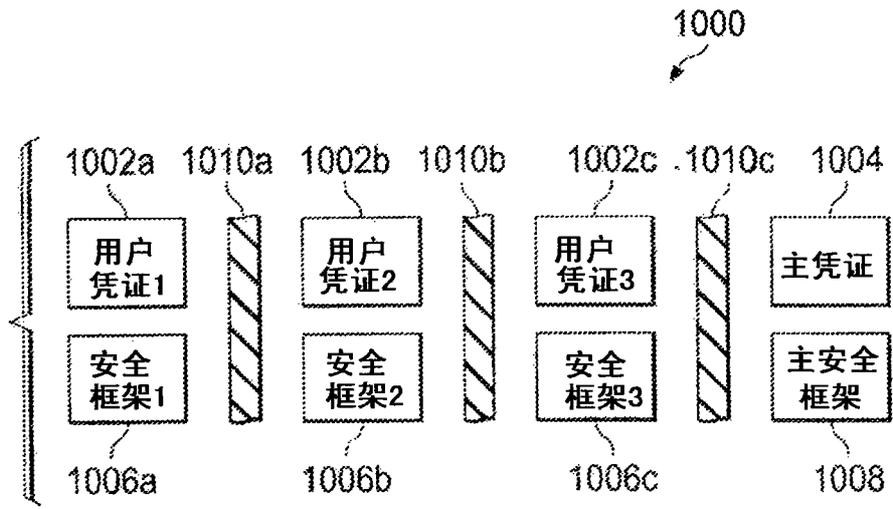


图 10

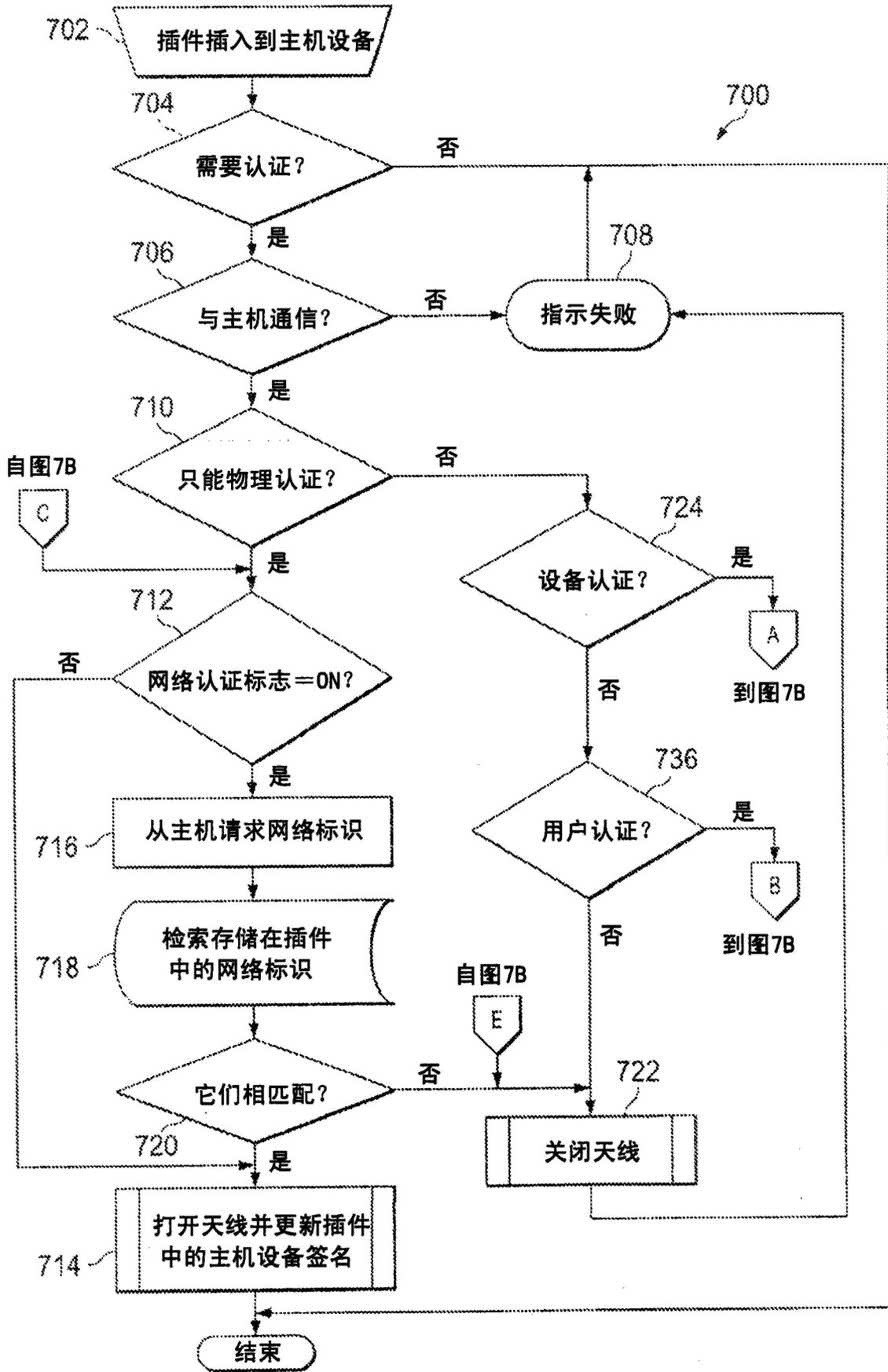


图 7A

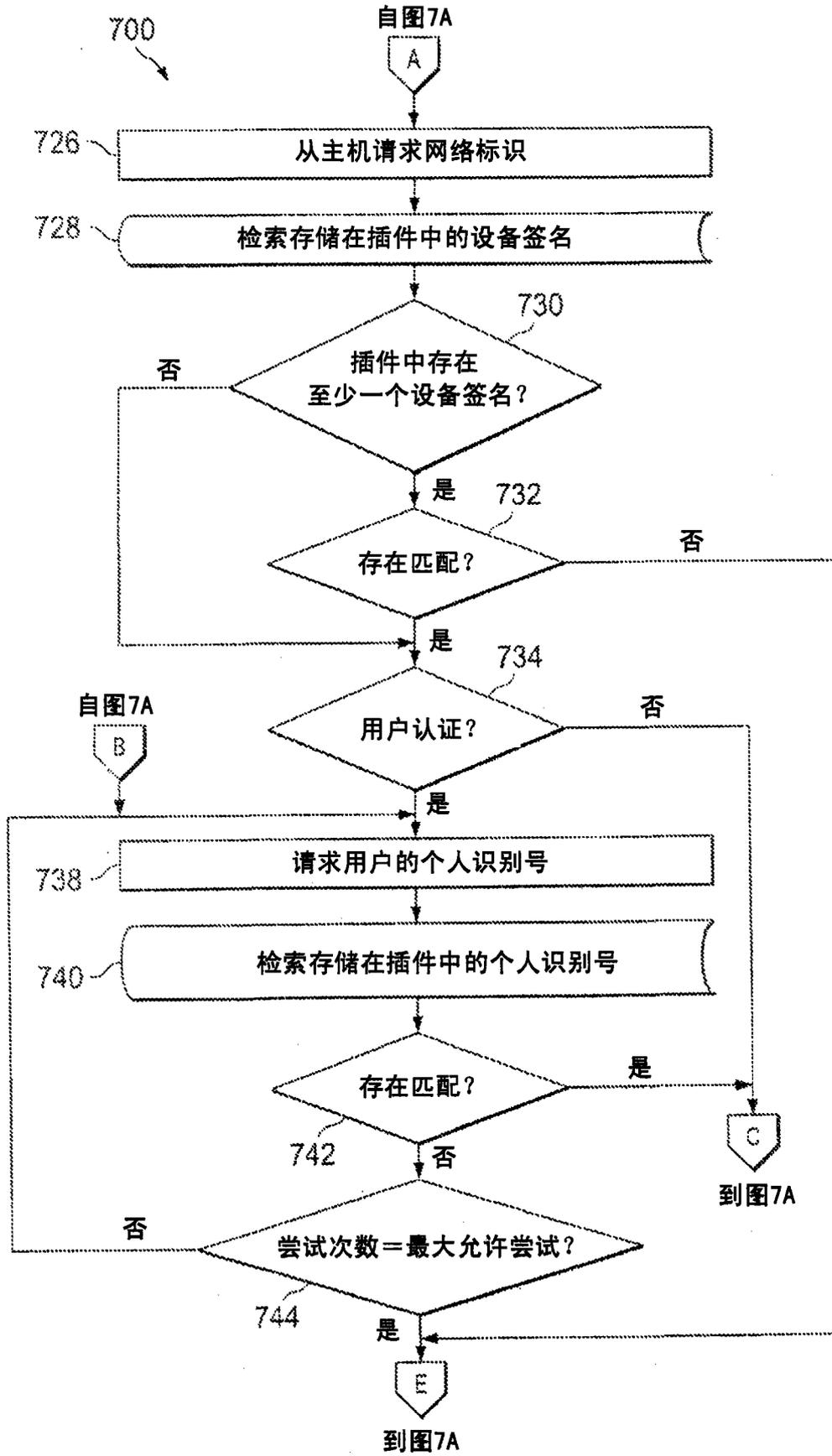


图 7B

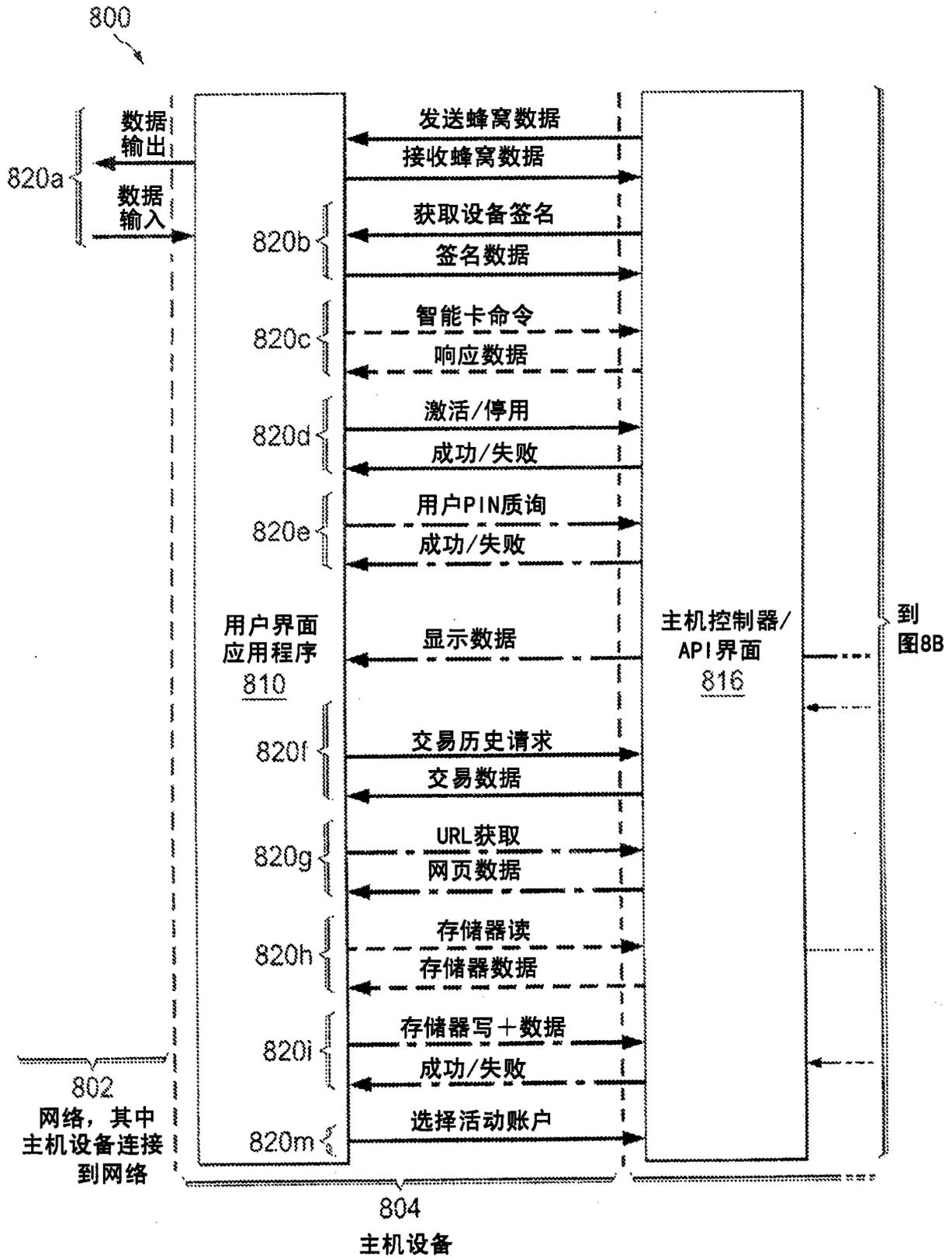


图 8A

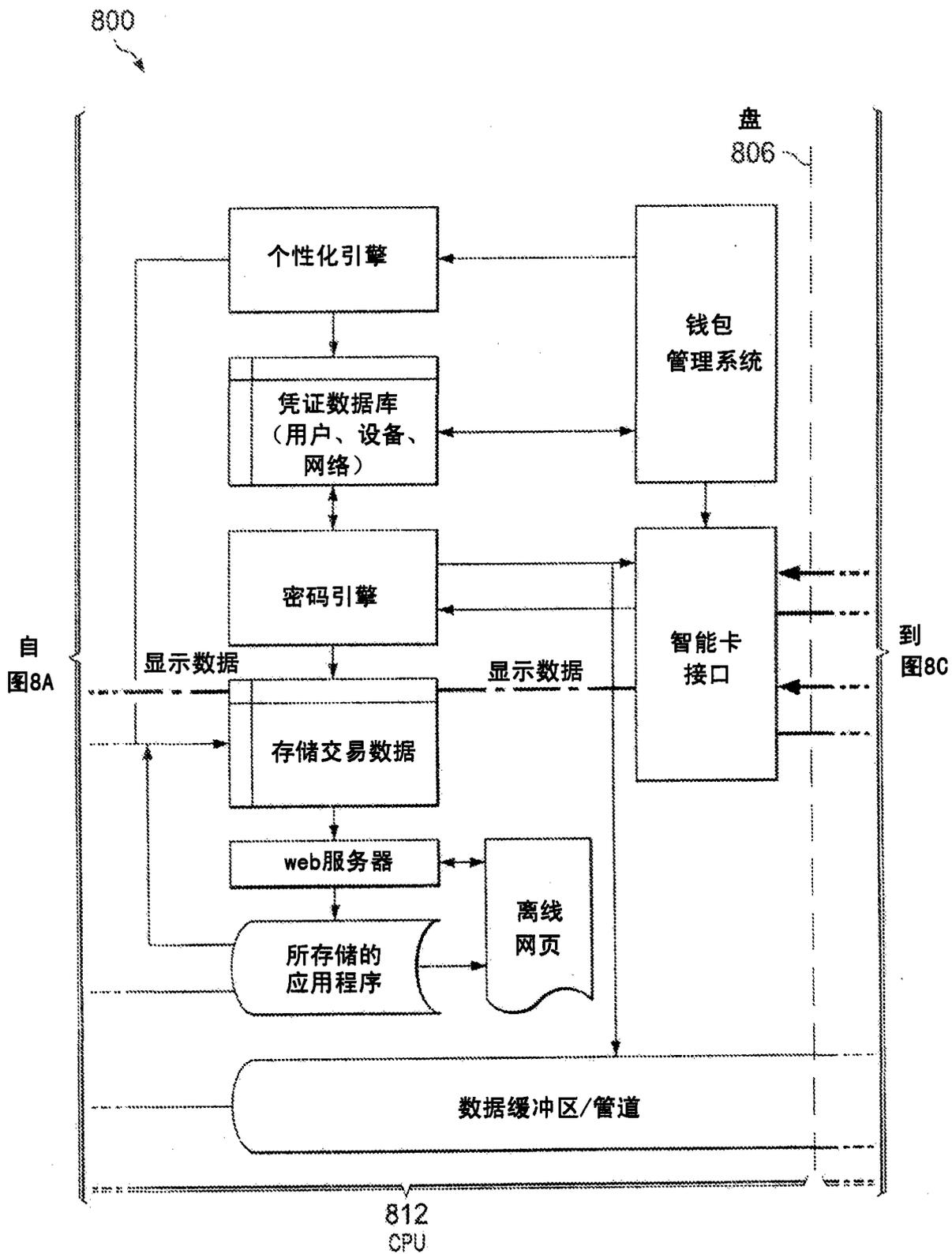


图 8B

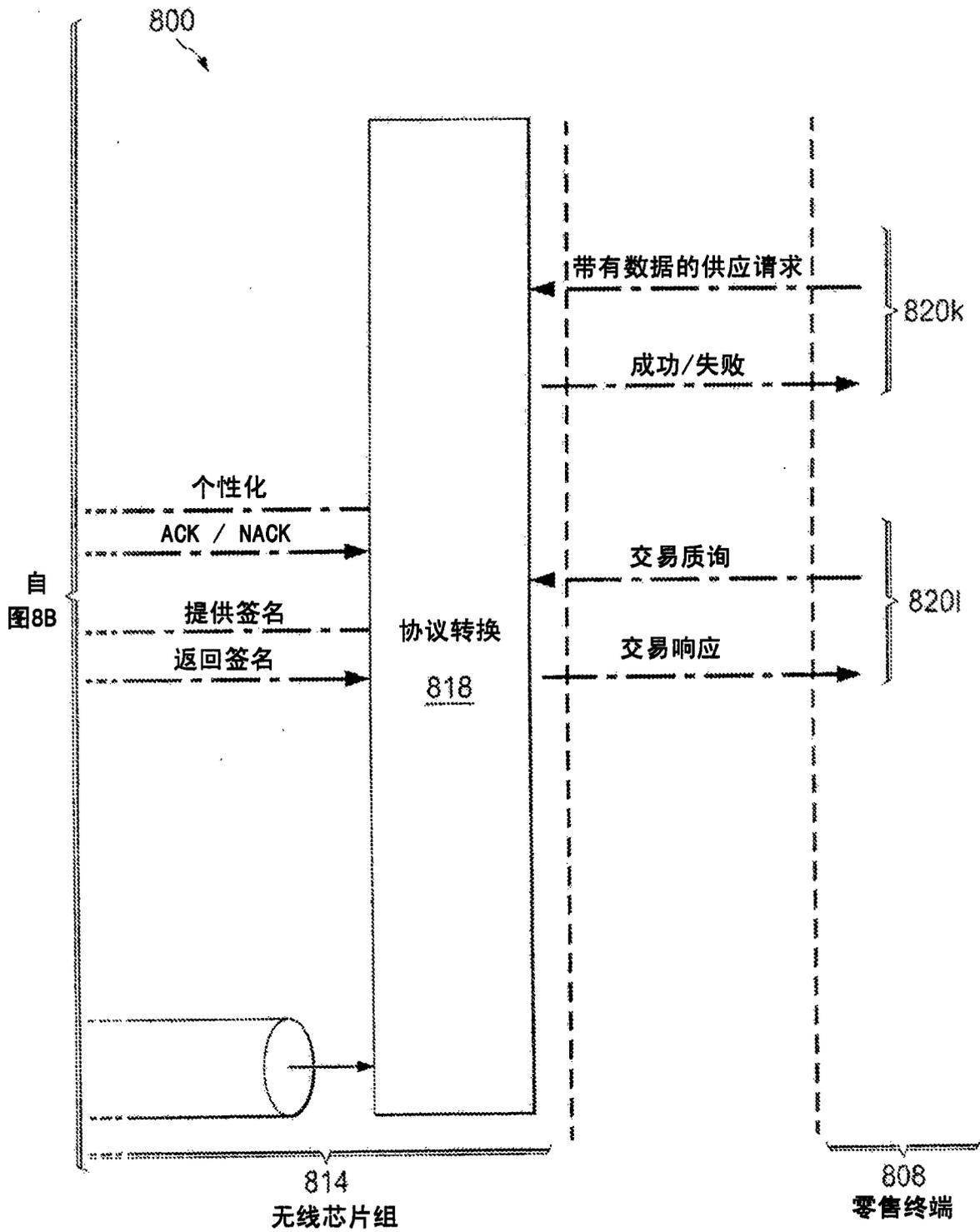


图 8C

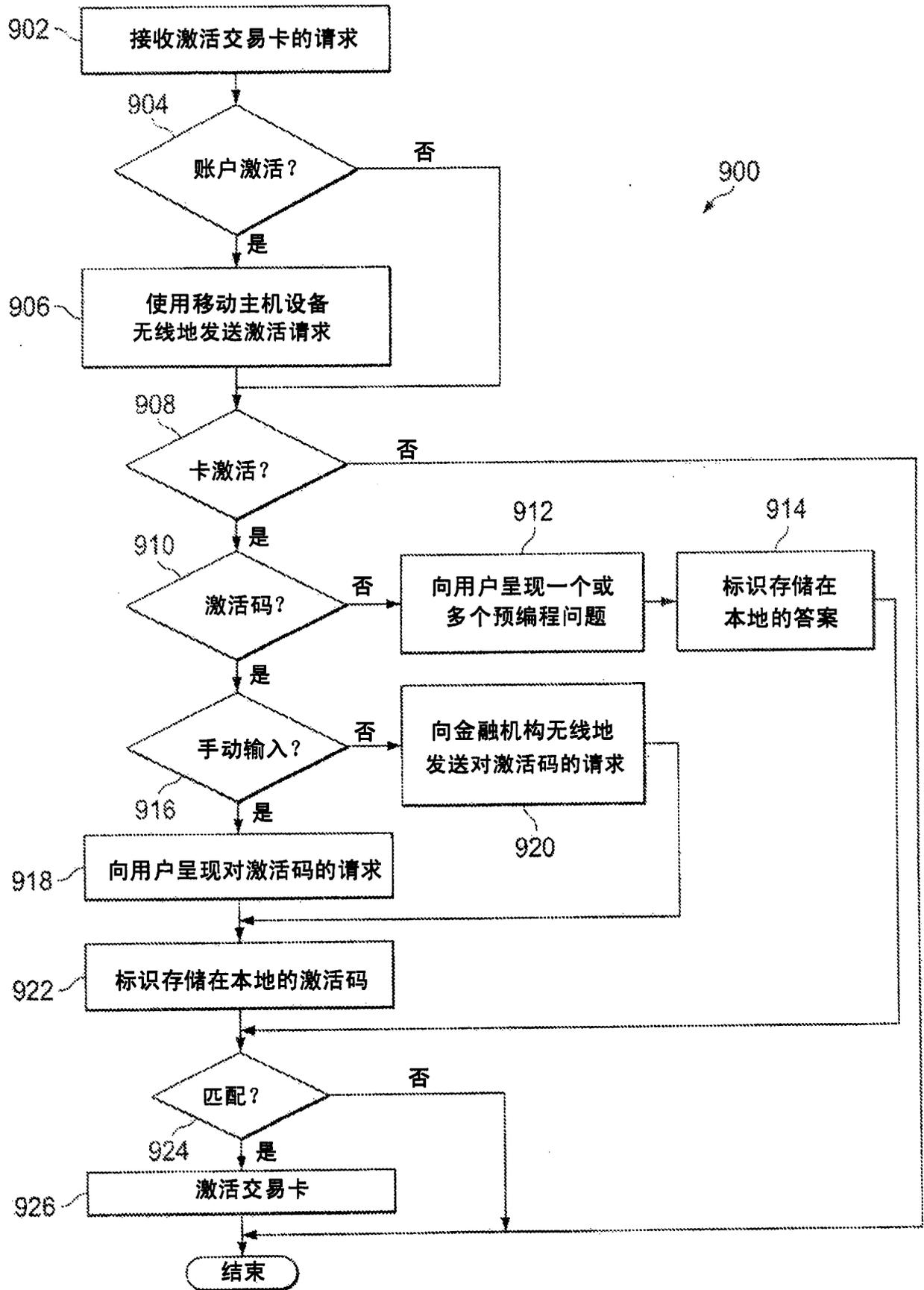


图 9

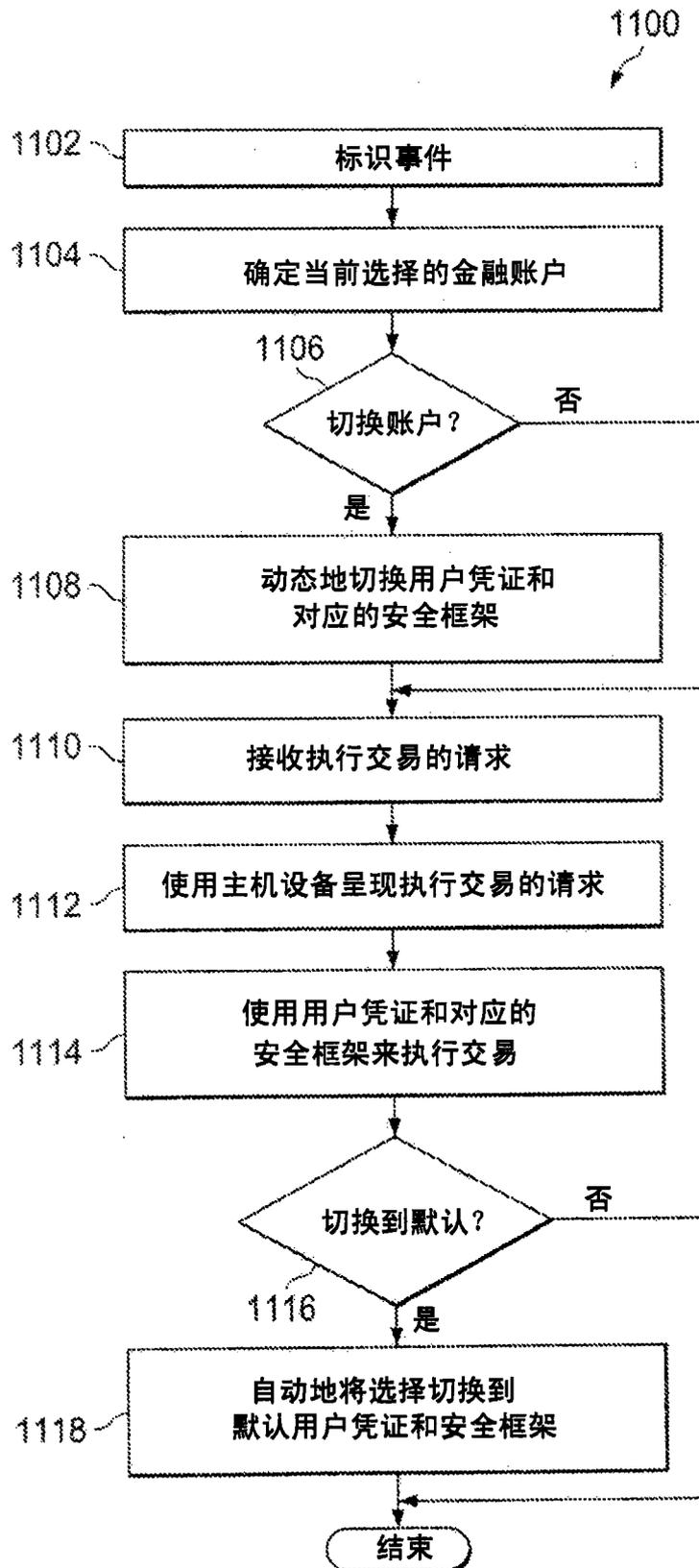


图 11