



(10)授权公告号 CN 104106276 B

(21)申请号 201280061249.2

内哈·马尼亚尔

(22)申请日 2012.10.12

(74) 专利代理机构 中国专利代理(香港)有限公司 72001

(65)同一申请的已公布的文献号

代理人 臧永杰 陈岚

申请公布号 CN 104106276 A

(43)申请公布日 2014.10.15

(51) Int.Cl.

(30) 优先权数据

H04W 12/00(2009.01)

61/546084 2011.10.12 US

G06Q 40/02(2012.01)

61/619751 2012.04.03 US

G06Q 20/40(2012.01)

(85)PCT国际申请进入国家阶段日

(56)对比文件

2014.06.12

CN 101605294 A, 2009.12.16.

(86)PCT国际申请的申请数据

CN 101605294 A, 2009.12.16,

PCT/US2012/060038 2012.10.12

CN 101944032 A, 2011.01.12.

(87)PCT国际申请的公布数据

CN 101944032 A, 2011.01.12,

W02013/056104 EN 2013.04.18

US 2009288004 A1, 2009.11.19.

(73)专利权人 万事达移动交易方案公司

US 2009307300 A1, 2009.12.10,

地址 美国纽约州

CN 101945135 A, 2011.01.12,

(72)发明人 M.德赛 萨特延·皮特罗达

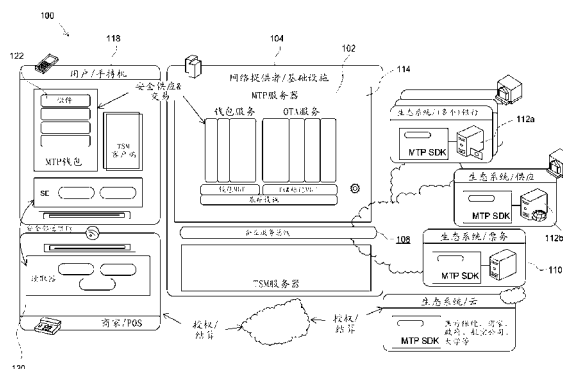
权利要求书6页 说明书92页 附图59页

(54)发明名称

多层安全移动交易使能平台

(57)摘要

一种用于在多域生态系统中执行安全个性化交易的平台包括个性化层,其使能对于存储在移动设备上的一个或多个生态系统元件的服务提供者个性化。此外,该平台包括使能层,用于促进个性化层与客户端设备之间的互操作。该平台此外包括服务层,其可以独立于使能层而操作,并且可以使能对于多个服务的服务递送。



1. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

在移动设备上的钱包容器中配置一个或多个微件模块,其中,所述钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述钱包容器促进每种类型的提供者特定的钱包的不同操作以用于在提供者特定的钱包与开发所述提供者特定钱包的提供者之间执行安全交易;以及

经由所述一个或多个微件模块来访问所述钱包容器中的一个或多个钱包模块。

2. 如权利要求1所述的计算机可读介质,此外包括:在访问所述一个或多个钱包模块之前认证所述一个或多个微件模块中的每一个。

3. 如权利要求1所述的计算机可读介质,其中,访问一个或多个钱包模块包括接收从服务提供者模块到钱包容器中第一微件模块的通信,并使能由第一微件模块对钱包模块的经认证访问。

4. 如权利要求1所述的计算机可读介质,其中,所述一个或多个钱包模块中的每一个通过网络由服务提供者配置和安装在钱包容器中。

5. 如权利要求1所述的计算机可读介质,其中,所述一个或多个钱包模块中的每一个通过网络由用户配置和安装在钱包容器中。

6. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

经由移动设备上的钱包容器来配置一个或多个微件模块以供执行,其中,所述一个或多个微件模块包括服务提供者的服务群组,

其中,所述钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易。

7. 如权利要求6所述的计算机可读介质,其中,所述钱包容器在移动设备上提供运行时环境,其中,微件模块被解译以用于递送所述服务群组的一个或多个服务。

8. 如权利要求6所述的计算机可读介质,其中,所述钱包容器与用于提供安全个性化交易的多层平台的使能层协作地操作,以向一个或多个微件模块提供对服务提供者的工作流的排他访问。

9. 如权利要求8所述的计算机可读介质,其中,所述钱包容器在操作于移动设备上的运行时环境中解译微件模块以提供排他访问。

10. 如权利要求6所述的计算机可读介质,其中,所述服务提供者是微件发行者。

11. 如权利要求10所述的计算机可读介质,其中,向所述微件发行者所发行的一个或多个微件模块提供对所述微件发行者的工作流的排他访问。

12. 如权利要求11所述的计算机可读介质,其中,所述钱包容器与用于提供安全个性化交易的多层平台的使能层协作地操作,以提供所述排他访问。

13. 如权利要求10所述的计算机可读介质,其中,向所述微件发行者所发行的一个或多个微件模块提供对所述微件发行者的用户接口的排他访问。

14. 如权利要求13所述的计算机可读介质,其中,所述钱包容器与用于提供安全个性化交易的多层平台的使能层协作地操作,以提供所述排他访问。

15. 如权利要求10所述的计算机可读介质,其中,防止所述微件发行者所发行的一个或多个微件模块访问另一微件发行者的工作流。

16. 如权利要求15所述的计算机可读介质,其中,所述钱包容器与用于提供安全个性化交易的多层平台的使能层协作地操作,以防止访问另一微件发行者的工作流。

17. 如权利要求10所述的计算机可读介质,其中,防止所述微件发行者所发行的一个或多个微件模块访问另一微件发行者的用户接口。

18. 如权利要求17所述的计算机可读介质,其中,所述钱包容器与用于提供安全个性化交易的多层平台的使能层协作地操作,以防止访问另一微件发行者的用户接口。

19. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

在移动设备上的钱包容器中配置一个或多个微件模块,所述钱包容器包括一个或多个钱包模块,其中,所述钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定钱包,并且所述钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

限制由所述一个或多个微件模块对包括以下各项的元件集合的访问:所述一个或多个钱包模块、所述移动设备、一个或多个客户端应用;以及

提供对发行者特定的安全性域和微件特定的发行者安全性域中的至少一个的一个或多个微件模块的访问。

20. 一种管理微件模块访问的方法,包括:

在移动设备上提供容器运行时环境,用于接收不同类型的提供者特定钱包,其中,所述容器运行时环境促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

访问移动设备驻留的微件模块以确定与微件相关联的访问约束,其中,所述访问约束关于:电子钱包访问、设备资源访问、设备驻留的生态系统应用、由移动设备可访问的网络资源、发行者特定的安全性域以及微件特定的安全性域;

经由所述容器来操作微件模块中至少一个以施加与微件模块相关联的访问约束;以及

促进由微件模块对与微件模块相关联的发行者特定的安全性域和微件特定安全性域中至少一个的访问。

21. 如权利要求20所述的方法,其中,施加微件模块访问约束包括防止对移动设备上的电子钱包资源的访问。

22. 如权利要求20所述的方法,其中,施加微件模块访问约束包括防止由第一微件对与第二微件相关联的钱包的访问。

23. 如权利要求20所述的方法,其中,施加微件模块访问约束包括基于钱包的状态而防止由微件对移动设备上的钱包的访问。

24. 如权利要求23所述的方法,其中,所述钱包的状态包括活动状态和非活动状态,在所述活动状态期间允许所述微件进行的访问,在所述非活动状态期间防止所述微件进行的访问。

25. 如权利要求20所述的方法,其中,促进对安全性域的访问包括允许对移动设备上的数字钱包的访问,所述数字钱包与所述微件模块共享安全性域。

26. 如权利要求20所述的方法,其中,促进对安全性域的访问包括允许对发行者的网络资源的访问,所述发行者与所述微件模块共享安全性域。

27. 一种用于移动交易处理安全性的方法,包括:

至少部分地通过联网的服务器来配置微件以提供对发行者特定服务群组的访问;

在操作于移动设备上的安全钱包容器中从所述联网的服务器接收部署所配置的微件的请求,其中,所述安全钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述安全钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

确定用于在所述移动设备上操作微件的微件隔离要求;以及

基于所述隔离要求在移动设备上通过所述安全钱包容器来安装所配置的微件。

28. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

在客户端设备上部署第一发行者特定微件以促进基于第一信任模型的安全个性化交易;以及

在所述客户端设备上部署第二发行者特定微件以促进基于第二信任模型的安全个性化交易,

其中,所述第一发行者特定微件和第二发行者特定微件被部署在钱包容器中,其中,所述钱包容器在所述客户端设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易。

29. 如权利要求28所述的计算机可读介质,其中,第一信任模型和第二信任模型中的至少一个是委派信任模型、直接信任模型和代理信任模型之一。

30. 如权利要求28所述的计算机可读介质,其中,所述基于第一信任模型的安全个性化交易和所述基于第二信任模型的安全个性化交易中的至少一个是至少部分地基于触发来促进的。

31. 如权利要求30所述的计算机可读介质,其中,所述触发对应于所述基于第一信任模型的安全个性化交易和所述基于第二信任模型的安全个性化交易中至少一个的货币值。

32. 一种用于移动交易处理安全性的方法,包括:

在移动设备处用多域安全钱包容器来接收警报,其中部署在移动设备上的现有微件的更新版本是可用的,其中,所述安全钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述安全钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

确认所述更新是部署在移动设备上的现有微件的更新;

配置所述钱包容器以接收更新的微件;

用所述钱包容器来接收更新的微件;

处置所述现有微件以防止对该微件的进一步使用;以及

将更新的微件存储在移动设备上。

33. 一种用于移动交易处理安全性的方法,包括:

用操作于移动设备上的多域钱包容器向服务器查询更新的微件的存在,其中,所述多

域钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述多域钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

从所述服务器接收指示经更新的微件的可用性的信息;

请求所述更新的微件;

在移动设备处接收所述更新的微件;

处置所述更新的微件所取代的现有微件以防止对所述现有微件的进一步使用;以及
将所述更新的微件存储在移动设备上。

34. 如权利要求33所述的方法,其中,查询服务器是以预定义的时间间隔而执行的。

35. 如权利要求33所述的方法,其中,查询服务器是响应于客户端设备上微件的执行而执行的。

36. 如权利要求33所述的方法,此外包括将存储了所述更新的微件的确认发送到所述服务器。

37. 一种用于移动交易处理安全性的方法,包括:

从操作于移动设备上的多域钱包容器接收针对存在更新的微件的查询,其中,所述多域钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定钱包,并且所述多域钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

将指示所述更新的微件的可用性的信息传输到所述移动设备的多域钱包容器;

从所述移动设备的多域钱包容器接收针对所述更新的微件的请求;以及

将所述更新的微件传输到所述移动设备的多域钱包容器。

38. 如权利要求37所述的方法,其中,查询是以预定义的时间间隔而接收的。

39. 如权利要求37所述的方法,其中,查询是响应于客户端设备上微件的执行而接收的。

40. 如权利要求37所述的方法,此外包括接收存储了所述更新的微件的确认。

41. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

在移动设备上的钱包容器中配置一个或多个微件模块,所述钱包容器包括一个或多个钱包模块,其中,所述钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定钱包,并且所述钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;以及

促进由微件中至少一个的发行者对钱包模块中至少一个的访问。

42. 一种存储程序指令的计算机可读介质,其中,通过计算机系统的一个或多个处理器执行所述程序指令使得所述一个或多个处理器实行以下步骤:

在移动设备上的钱包容器中配置一个或多个微件模块,所述钱包容器包括一个或多个钱包模块,其中,所述钱包容器在所述移动设备上可操作,用于接收不同类型的提供者特定的钱包,并且所述钱包容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;以及

配置至少一个小程序以与至少一个钱包模块结合执行来促进对多个交易协议的管理。

43. 一种用于移动交易处理安全性的方法, 包括:

将用于提供至少一个微件和至少一个钱包的运行时环境的容器布置在客户端设备的存储器中, 其中, 所述容器可操作用于接收不同类型的提供者特定的钱包, 并且所述容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易, 并且所述容器通过可共享接口来提供对所述至少一个微件和所述至少一个钱包的访问;

将容器伴随小程序布置在客户端设备的安全元件中, 当在所述运行时环境中执行时, 所述容器伴随小程序促进由至少一个其它小程序对与所述至少一个钱包相关联的安全钱包资源的访问。

44. 如权利要求43所述的方法, 其中, 所述可共享接口促进对经由所述容器可访问的移动钱包功能和移动微件功能的访问。

45. 一种移动交易处理系统, 包括:

部署在网络中的多个服务器和多个客户端设备, 每个服务器被配置为促进所述网络中的所述多个客户端设备和多个服务提供者服务器间的安全个性化交易;

所述多个客户端设备中的至少一个配置有在基于容器的执行环境中可操作的可容纳多租户的钱包, 其中, 所述钱包是通过布置在所述多个客户端设备的所述至少一个上的微件可访问的, 其中, 所述容器可操作用于接收不同类型的提供者特定的钱包, 并且所述容器促进每种类型的提供者特定钱包的不同操作以用于在提供者特定钱包与开发所述提供者特定钱包的提供者之间执行安全交易;

所述多个服务器还被配置为促进在经由所述微件的所述多个客户端设备中至少一个与经由多个信任模型中任一个的所述多个服务提供者服务器中至少一个之间的交易, 所述信任模型包括单个信任域、单个信任集群、多个信任集群以及直接信任关系。

46. 如权利要求45所述的移动交易处理系统, 其中, 所述多个不同信任模型包括以下各项中的至少一个: 单个信任域、单个信任集群、多个信任集群以及直接信任关系。

47. 如权利要求46所述的移动交易处理系统, 其中, 所述单个信任域包括中央钱包服务中心服务器, 其与用户设备上的电子钱包相接口, 并且促进建立与可信服务提供者的安全交易信道。

48. 如权利要求46所述的移动交易处理系统, 其中, 所述单个信任集群包括可信第三方服务器和钱包服务中心服务器, 所述可信第三方服务器用于与个人电子钱包安全地交换机密钱包信息, 所述钱包服务中心服务器用于促进由多个服务提供者中的每一个经由所述第三方服务器对用户的直接认证, 其中, 所述钱包服务中心服务器将用户标识和安全性密钥递送到所述多个服务提供者中的至少一个。

49. 如权利要求46所述的移动交易处理系统, 其中, 多个信任集群包括多个不同的可信第三方, 其各自至少配置有用于以下各项的服务器: 与个人钱包交换机密钱包信息, 并且此外与多个集群特定的服务提供者交换由钱包服务中心提供的用户和/或设备标识。

50. 如权利要求46所述的移动交易处理系统, 其中, 直接信任关系包括归属钱包服务中心服务器, 用于建立与电子钱包的交易上下文, 其促进直接在电子钱包与服务提供者之间建立认证的交易信道。

51. 如权利要求45所述的移动交易处理系统, 其中, 所述微件被配置用于与特定提供者

的安全交互。

52. 如权利要求45所述的移动交易处理系统,其中,所述微件被配置用于通过中介与特定提供者的安全交互。

53. 如权利要求51所述的移动交易处理系统,其中,通过在所述移动设备和与特定提供者相关联的联网的服务器之间的电子交互而在空中将所述微件配置在所述移动设备上。

多层安全移动交易使能平台

[0001] 相关申请的交叉引用

[0002] 本申请是目前未决的2006年10月5日提交的、标题为“Transactional Services”的美国专利申请11539024的部分继续。该申请要求2005年10月5日提交的、标题为“Methods and Systems for Transactional Services”的美国临时专利申请号60/724,066的权益。

[0003] 本申请要求2011年10月12日提交的美国临时专利申请61546084和2012年4月3日提交的美国临时专利申请61619751的权益。

[0004] 本申请与以下美国专利申请相关：2007年10月31日提交的、标题为“System and methods for servicing electronic transactions”的美国专利申请号11/931,872；和2002年10月31日提交的、标题为“System and methods for servicing electronic transactions”的美国专利申请号10/284,676。

[0005] 上述申请中的每一个通过引用以其整体被并入本文。

[0006] 本申请与以下美国专利相关：2000年6月6日提交的、标题为“Point of sale and display adapter for electronic transaction device”的美国专利号6,769,607；1999年11月15日提交的、标题为“Point of sale adapter for electronic transaction device”的美国专利6,705,520；1994年6月20日提交的、标题为“Universal electronic transaction card including receipt storage and system and methods of conducting electronic transactions”的美国专利号 5,590,038；1996年9月6日提交的、标题为“Device, system and methods of conducting paperless transactions device”的美国专利号5,884,271；1999年3月10日提交的、标题为“Device, system and methods of conducting paperless transactions”的美国专利号 6,925,439；1999年8月11日提交的、标题为“System and methods for servicing electronic transactions”的美国专利号 7,308,426；以及2001年1月19日提交的、标题为“Method and system for managing user activities and information using a customized computer interface”的美国专利号 7,366,990，这些美国专利中的每一个通过引用以其整体被并入本文。

背景技术

[0007] 领域：

[0008] 用于多域生态系统(ecosystem)中的安全个性化交易的多层移动交易平台的方法和系统一般地涉及移动交易处理安全性。

[0009] 相关领域的描述：

[0010] 移动交易正变成销售点支付的最普遍的形式。用于移动交易处理的现有系统不具有解决日益增长的对安全个性化交易服务和客户联系的需求以满足将来业务需求所需的可配置性的可伸缩性和灵活性。

发明内容

[0011] 移动交易平台 (MTP) 可以包括运营商等级的基础设施平台,其可以促进安全交易服务的开发,以及将安全交易服务(移动商务(例如在空中)和移动支付(例如,近场通信(NFC)邻近性)二者)递送到广泛的移动电话环境。MTP可以包括增强的软件开发方法,用以通过提供一致、公共开发环境来进一步简化开发并从开发者隐藏电话环境特定的复杂性。还可以在开发期间展露原生电话特征以允许开发者定义原生电话体验等,同时仍然受益于公共且鲁棒的开发方法和环境。使用MTP的一个益处是用于广泛的移动手持机的快速移动服务开发,用以快速构建有利的移动交易生态系统。

[0012] 另外,本文公开的是端对端安全交易环境,其中,应用信任模型,其不仅确保安全电子交易,而且通过使用对每个用户、用户操作的每个设备以及每个交易和/或服务域的动态认证而在用户、支付设施以及商家间提供安全且安稳的电子商业操作。所公开的信任模型例如确保用户和商家可以在不使用“中间人”的情况下进行交易来确保安全且可靠的商务。通过经由一个或多个主服务设施认证用户并且通过经由此类主服务设施认证商家和其它提供者,对于每个商家而言,有可能通过用户已经在其上向主服务设施经认证的任何设备而具有与每个用户的唯一而安全的关系。然而,通过使用用于认证的主服务设施和使能鲁棒的信任模型,多个商家(例如,产品、金融服务以及本文描述的许多其它服务的提供者)可以安全并直接地与单个用户交易。以这种方式,多个经认证的商家可以在聚集的选集(portfolio)中对用户是可用的,这可以大大促进改进的安全电子商务。

[0013] 电子商业环境的各方面可以包括提供者域(例如,银行、商家等),其可以通过钱包平台来访问并且提供增建钱包和微件能力的的能力以使能从风险管理视角查看电子交易环境。在示例中,跨生态系统的交叉销售可以利用本文描述的方法和系统,从而允许将风险管理映射到电子商务过程中。

[0014] 安全的多域生态系统环境的各方面可以将环境延伸至客户。一旦客户被认证到此类环境中,其就可以具有建立信任模型的能力,其可以使能通过单个信任模型来递送服务的特定实例。可以通过使用其它信任模型来递送其它产品/服务。

[0015] 而且,本文的方法和系统可以促进将安全性隧道延伸到商家,其可以具体化为隧道内的隧道,这可以使能核心安全性架构。以这种方式,商业可以避免随着安全性而陷入困境,而非集中于将提供可持续商业模型的应用。在示例中,本文的方法和系统可以使商业人员能够查看应用的使用频率(例如,3x/天与3x/月),以帮助针对不同用户交互模型的范围中的每个预想显著不同的信任模型。

[0016] 根据对优选实施例和附图的以下详细描述,本发明的这些及其它系统、方法、目的、特征和优点对于本领域技术人员将是显而易见的。本文提及的所有文档通过引用以其全部被并入于此。

附图说明

[0017] 可以通过参照以下附图来理解本发明及对其某些实施例的以下详细描述:

[0018] 图1图示了用于安全移动商务(mCommerce)和移动支付(mPayment)交易的动态生态系统100。

[0019] 图2图示了移动交易平台(MTP)高层级结构。

- [0020] 图3图示了移动交易平台(MTP)架构。
- [0021] 图4图示了具有MTP移动客户端(mClient)运行时的钱包应用的高层级架构视图。
- [0022] 图5参照开发周期图示了微件(widget)开发过程的概观。
- [0023] 图6图示了用于安全个性化交易的生态系统的概观。
- [0024] 图7图示了用于使用在用于安全个性化交易的生态系统中的示例性客户端架构。
- [0025] 图8图示了用于安全个性化交易的生态系统,其包括具有协议抽象支持能力的MTP结构配置。
- [0026] 图9图示了如图8中所图示的用于安全个性化交易的生态系统的可替换配置。
- [0027] 图10图示了可以跨越一系列生态系统元件的分层平台的概念。
- [0028] 图11图示了选择生态系统特征以用于包括在用于安全个性化交易的多域生态系统平台的使能(enabling)层、服务层和个性化层的每一个中的实施例。
- [0029] 图12图示了用于在用于安全个性化交易的多域生态系统中促进针对多个服务提供者的每一个修改个性化和服务层中的每一个的专家引擎。
- [0030] 图13图示了选择业务需求和设备功能性以用于包括在用于安全个性化交易的多域生态系统平台的使能层、服务层和个性化层的每一个中的实施例。
- [0031] 图14图示了开发微件的方法。
- [0032] 图15图示了微件使用的方法。
- [0033] 图16图示了用于安装微件的交易流程图。
- [0034] 图17图示了描绘MTP系统中微件的生命周期的状态图。
- [0035] 图18图示了从开发到执行的微件生命周期。
- [0036] 图19图示了访问控制机制的高层级视图。
- [0037] 图20图示了用于相对于访问控制器而加载和执行微件的方法。
- [0038] 图21图示了基于微件访问控制策略的微件运行时覆盖区(footprint)。
- [0039] 图22图示了微件批准过程。
- [0040] 图23图示了微件架构的示例性且非限制性实施例。
- [0041] 图24图示了客户端设备容器的高层级架构视图。
- [0042] 图24A图示了移动设备的移动交易平台相关元件的详细视图。
- [0043] 图24B图示了钱包伴随域特征,以及控制 and 数据流。
- [0044] 图25图示了供应或优惠券相关的交易流程图。
- [0045] 图26图示了根据示例的在交易流期间优惠券小程序的状态机图。
- [0046] 图27图示了在小程序与销售点终端之间的交互。
- [0047] 图28图示了根据示例的在交易流期间优惠券小程序(applet)的状态机图。
- [0048] 图29图示了示例性实施例中用于部署本发明的系统的高层级架构。
- [0049] 图30图示了描述通过使用具有下载URL的SMS而在用户的移动电话上安装移动钱包的方法的流程图。
- [0050] 图31A和31B图示了由用户进行的用于钱包激活的方法。
- [0051] 图32图示了作为搜索和下载用例的示例的方法。
- [0052] 图33图示了用于OTA交易的示例性方法。
- [0053] 图34图示了作为用于发卡用例的示例的方法。

- [0054] 图35图示了作为终止钱包的示例的方法。
- [0055] 图36图示了作为用于发布微件的示例的方法。
- [0056] 图37是用于第一次添加微件连同TSM交互的方法。
- [0057] 图38是参照微件加载时间签名、核实和执行时间访问核实的用于微件访问核实的系统的行为模型。
- [0058] 图39图示了用于安全商务和支付交易的动态生态系统。
- [0059] 图40图示了用于安全商务和支付交易的动态生态系统中的协议抽象的方法。
- [0060] 图41图示了在用于安全商务和支付交易的动态生态系统中对交易内容标记化(tokenization)的方法。
- [0061] 图42图示了用以从在移动设备上运行的移动钱包接收动态标记(token)的销售点设备。
- [0062] 图43图示了在用于安全商务和支付交易的动态生态系统中生成用于穿过网络的安全内容的电子交易封装器的标记的方法。
- [0063] 图44图示了在用于安全商务和支付交易的动态生态系统中对交易封装器标记化的方法。
- [0064] 图45图示了通过传输动态生成的标记化的封装器来执行跨开放网络的电子交易的方法,所述封装器包括表示在用于安全商务和支付交易的动态生态系统中的交易内容的标记。
- [0065] 图46图示了在交易流中的协议抽象的方法,其包括具有单个开证银行的多个采集方法。
- [0066] 图47图示了在空中交易流中的协议抽象的方法,其包括单个采集方法和多个开证银行。
- [0067] 图48图示了标记化的交易、标记化的协议抽象以及标记化的封装器的方法。
- [0068] 图49图示了单个信任域模型。
- [0069] 图50图示了如图50中所图示的单个信任集群模型,其可以假设可信第三方在生态系统中是可访问的。
- [0070] 图51图示了多个信任集群模型。
- [0071] 图52图示了直接信任关系,其中不强迫任何两个实体信任彼此。
- [0072] 图53图示了消息总线通信架构。
- [0073] 图54图示了支付促进器系统的各种子系统的高层级框图。
- [0074] 图55示出了钱包的各种组件。
- [0075] 图56图示了可以基于支付促进器容器的部署模型5600的高层级框图。

具体实施方式

- [0076] 尽管本文参照各种实施例进行了描述,但是理解的是,在所有情况中,除非另外指定,否则对“实施例”或“多个实施例”的引用是指一个或多个示例性并且非限制性实施例。同样,理解的是,在本文的所有描述中,除非另外指定,否则即使当不是明确引用“实施例”或“多个实施例”时也是指一个或多个示例性并且非限制性实施例。
- [0077] 多域生态系统可以被配置成经由多层安全移动交易使能平台而用于安全个性化

交易,所述多层安全移动交易使能平台可以包括使能层、服务层、个性化层、专家层和经验框架层。多域生态系统可以包括多个服务提供者、器件(instrument)发行者、移动交易处理器、交易获取器、第三方认证器以及经由各种各样的电子设备访问生态系统的多个用户。如本文所描述的多层安全移动交易生态系统使能平台可以促进任何生态系统参与者配置生态系统的各方面以满足一组独特的业务模型需求。多层安全移动交易生态系统使能平台可以提供软件开发和元件配置工具,用以准备和个性化目标特定业务模型和/或信任模型所需要的电子钱包、活动的设备微件、后端基础设施运行时代码等。通过促进安全、可信的生态系统操作(例如,电子钱包的发行、维护和使用),该平台可以支持经由单个移动设备与大量不同域进行安全交易。通过提供工具来个性化功能元件(例如,微件)以用于部署在移动设备中,该平台可以促进多个不同域(例如,不同服务提供者)与诸如客户之类的用户之间的安全的、定制的交易相关通信,这可以使用于与客户交互的机会增加到10倍或更多倍。

[0078] 可以可替换地铸造为移动交易平台或MTP的多层安全移动交易使能平台可以为用户递送安全交易功能性,从而使能参与者的生态系统,所述参与者除其它之外尤其包括服务提供者、器件和服务的发行者/获取者、相关支持和增值服务提供者以及分布网络。可以通过良好结构化的集中于递送能力的软件和/或硬件模块来递送多层安全移动交易使能平台,所述递送能力诸如对用户通信的直接服务提供者、消息传送和通知、安全性和认证、空中(OTA)供应、OTA可信服务管理器(TSM)代理操作、基于客户端的安全生态系统容器操作、钱包和微件管理、交易引擎操作、数字器件管理、位置和/或地理围栏(geo-fencing)支持、增强现实等。

[0079] 在多域生态系统中用于安全个性化交易的多层移动交易平台的方法和系统可以促进建立和操作市场地点或交易相关证书的交换。这些证书可以被标记化或者可以不被标记化,这服从于它们各自的发行者和获取者的、与支付和非支付服务相关的等等要求。这些证书可以在空中并且在邻近环境中通过诸如销售点终端等的信道主机来进行交易。通过采用可以使能这样的交易相关证书交换的这些方法和系统,可以解决与伸缩这样的生态系统相关的关键商业问题。交易相关证书的这种交换可以完全消除对于单个服务提供者将它们自己嵌入作为这样的交易证书的有效交换的需要,并且相反地,允许现有发行者、获取者和服务提供者(和/或这样的证书的消费者)继续利用它们的现有系统、商业和风险管理实践。这样的交换将通过利用本文描述的移动交易平台的各方面来增值,这些方面包括各种部署模型、可配置生态系统规则、底层聚集安全性架构和可配置安全性信任模型、必要工具、实用程序、web服务、移动设备和服务器应用(例如,钱包、容器、微件、钱包伴随域)等。结果可以是在高度可伸缩企业环境中的高质量服务递送,以用于确保不同生态系统参与者可以被整合并且可以添加新参与者,而没有繁重开销。

[0080] 图1图示了用于安全移动商务和移动支付交易的动态生态系统100。本文可以描述生态系统100。如下文所描述的,MTP 114可以被配置为对用于安全移动商务和移动支付交易的动态生态系统供以动力。MTP可以设置在网络提供者的域102中并且集成到网络提供者104的系统中。在示例中,网络提供者104的企业服务总线(ESB)108可以用于集成。MTP 114可以连接到服务和安全性提供者110的生态系统,其可以包括一个或多个可信服务管理者(TSM),例如112a、112b。网络提供者104可以使用MTP 114来创建以特定商业垂直面(vertical)为目标的移动应用。在示例中,移动应用可以是用于零售/金融域的移动钱

包(mWallet)或者用于医疗保健垂直面的移动健康(mHealth)应用。在示例中,移动应用可以向用户提供特定于一域的核心服务集,其可能针对该域而已经被创建。出于本发明的目的,移动应用可以是假设零售域应用的钱包。在示例中,钱包还可以促进应用生命周期和安全性、标准化用户体验以及微件管理职责。微件可以提供特定的商业服务并且遵照钱包指南。移动应用可以下载到用户手持机(handset)118上。服务110的生态系统可以被配置为对手持机118上进行的任何交易进行认证。在示例中,可以在商家终端120处使用用户手持机118。商家终端120可以被配置为从生态系统云110接收通信,其关于用户手持机118微件122当用在商家终端120附近以用于实现交易时的微件认证。

[0081] 在示例中,单独、独立的服务提供者可以使用MTP SDK来构建可以加载到钱包中的微件。这些微件可以提供增量式功能性,其可以增强移动应用的整体吸引力。钱包和微件可以为用户提供OTA增值服务(VAS)和邻近NFC服务。容器(或MTP移动客户端运行时)可以为钱包和微件提供安全运行时环境和服务,以与服务器(OTA服务)进行OTA通信,并且还与安全元件通信来为邻近NFC交易管理支付和非支付小程序。

[0082] 在示例中,微件可以具有在安全元件中运行的相关联的小程序。在示例中,微件可以没有安全元件中运行的相关联的小程序。在示例中,服务提供者可以仅选择仅提供OTA服务。在示例中,MTP和TSM可以一起协作来提供整个NFC体验。在示例中,钱包和微件(包括软卡)供应、设置和管理可以由MTP操控,而小程序发行和个性化可以由TSM完成。在示例中,网络提供者可以确保可以装备商家位置处的NFC读取器以操控邻近协议,所述邻近协议可以由可能已经加载到电话的SE中的各种小程序所使用。这些读取器然后通过获取网络来处理交易,所述获取网络可以将交易切换到云中的合适生态系统服务提供者。钱包和/或微件可以与生态系统云通信,以确定服务状态和各种其它VAS要求,像余额、交易历史、存储的充值等。

[0083] 在示例性且非限制性实施例中,MTP可以被配置用于提供钱包、微件,并且管理交易连同可以与向总体的各种移动环境递送钱包相关联的所有相关商业服务。在示例性且非限制性实施例中,MTP可以被配置用于提供可以帮助构建服务提供者的生态系统和钱包的改进的SDK,其可以创建具有精密特征集的微件而不必担心手持机分片(fragmentation)。在示例性且非限制性实施例中,MTP可以被配置用于建立与各种生态系统的连接器,以向终端用户递送无论何时及何地理位置都可以访问的动态用户体验和各种服务集。

[0084] MTP可以针对来自各个国家的客户进行部署,并且可以被使得适合于特定国家要求。例如,MTP可以使用在美国(USA)、日本、中国、印度、新加坡、墨西哥和玻利维亚,用于各种移动商务和移动支付服务。在示例性且非限制性实施例中,MTP可以被配置用于提供银行服务、票务服务和支付服务。

[0085] 在示例性且非限制性实施例中,MTP可以部署在云中,并且可以被配置为聚集各种不同的服务提供者,以向终端用户有效地提供一套个性化安全交易服务。在示例中,网络提供者可以部署MTP的使能层(例如,钱包和交易管理连同基础设施组件),其对于服务和信道可以是不可知的。MTP的使能层可以被配置为支持例如银行、商家、医疗保健提供者等的服务提供者的生态系统。MTP的使能层可以被配置为支持可以使用SDK来构建它们的例如安全交易应用的单独个性化应用的所有第三方开发者。

[0086] 图2图示了MTP高层级结构200。MTP 212可以是客户端服务器平台。客户端可以在

各种移动手持机上操作,并且服务器可以在服务提供者的“云”中操作。客户端和服务端可以遵循如图1中所示的高层级架构。该高层级架构可以具有增建(build out)生态系统可能需要的三个不同组件。所述不同组件可以包括移动使能层、服务层和软件开发套件(SDK)。不同组件中的每一个可以与客户端和服务端交互。在示例性且非限制性实施例中,移动使能层可以包括开发移动应用可能必需的基础设施或商业独立组件。在示例性且非限制性实施例中,服务层可以包括用于钱包生态系统和增值服务的参考服务实现的集合(collection)。在示例性且非限制性实施例中,SDK可以包括开发(本文档中描述的)钱包和微件服务以及构建综合生态系统可能必需的一组工具和API。

[0087] 在示例性且非限制性实施例中,移动使能层可以包括用于客户端和用于服务器的不同组件。例如,用于客户端的移动使能层可以包括通过使用移动电话的特定开发环境所构建的基础设施运行时容器软件(SW)。在示例中,移动使能层可以利用公共开发者API、UI解译和渲染引擎、商业执行环境、微件和钱包生命周期管理、用于OTA/邻近交易的模式等来向客户端提供对底层电话能力的公共抽象。在示例中,移动使能层可以提供在网络提供者域中部署的服务器基础设施软件,其可以被配置用于建立和管理安全移动交易生态系统。在示例中,移动使能层可以向服务器提供软件,所述软件被装备用于钱包管理、状态性交易引擎、对象生命周期管理、信道特定通信、多域安全性策略和风险管理、OTA供应等。

[0088] 在示例性且非限制性实施例中,服务层可以包括用于客户端和用于服务器的不同组件。在示例中,用于客户端的服务层可以包括公共平台服务库,其可以用于实现多个商业用例。公共平台服务可以在由使能层所提供的商业执行环境内运行。在示例中,服务层可以包括三个基本单元。第一单元可以是用例,例如,为各种交易服务所构建的客户端侧工作流程和模板。第二单元可以是器件,例如,可以促进到真实世界器件的映射的对应单个钱包器件。在示例中,器件可以提供用于可视化或显示的数据。在示例中,器件可以提供用于空中(OTA)交易的数据。在示例中,器件可以提供用于邻近交易的数据。在示例中,器件可以提供用于监管的数据。第三单元可以包括至少一个信任模型。信任模型可以促进认证方案的实现,其可以包括牵引(tow)因素认证(2FA)。2FA可以由不同微件提供者所需的并且可以是与生态系统相关的。

[0089] 在示例中,用于服务器的服务层可以包括相关联的服务模板和商业特定组件的库,其可以部分或整体地重用来开发客户为中心的提供。在示例中,服务可以包括钱包服务202和增值服务204。钱包服务202可以包括管理钱包和支付标记的生命周期。增值服务可以包括提供商业服务。服务层可以包括三个单元。第一单元可以是用例,例如,可以通过使用移动使能层的交易框架来构建服务器侧模板以用于实现特定用例。在示例中,可以存在用于商业服务(例如,账单支付、电影票务等)的一个或多个不同的模板。第二单元可以包括至少一个器件或标记。器件可以包括商业特定数据对象(例如,信用卡、银行帐户、账单、优惠券等),其可以跨各种服务被重用并且可以提供针对对象的共同理解定义以及管控对象的生命周期与交易的规则的实现。第三组件可以包括至少一个信任模型。该信任模型可以促进用于服务的不同认证方案的实现,包括对在具有它们的独立TSM的单独信任集群内操作的支持。

[0090] 在示例性且非限制性实施例中,SDK可以包括用于客户端和用于服务器的不同组件。在示例中,用于客户端的SDK可以划分成2部分。第一部分可以是钱包SDK 208,并且第二

部分可以是微件SDK 210。在示例中,钱包SDK 208可以提供对钱包服务202、特许API以及必要组件的访问以构建钱包容器应用或用户体验。在示例中,微件SDK 210可以促进生态系统合作伙伴构建它们的可以在钱包容器内操作的微件。在示例性且非限制性实施例中,SDK可以基本上促进客户端侧配置和用户体验。在示例中,SDK可以通过促进对于由客户端容器展露的参数的可定制性来促进配置。这可以包括设备特定参数、变量(PIN大小、退出确认、选择模块的包含物等)。在示例中,SDK可以通过促进跨手持机的差异化用户体验的开发来提供用户体验。

[0091] 在示例中,用于服务器的SDK可以包括至少一个库,其可以允许任何生态系统服务器与钱包通信、格式化微件的内容,以及向钱包应用展露服务。该库可以包括配置模块和接口模块。配置模块可以允许对于由服务器的移动使能和服务层所展露的参数的可定制性。可以在属性文件和资源束中配置参数。接口模块可以提供被开发来促进与各种后端系统的通信的连接器,所述后端系统可以协作来履行完整的端对端服务。接口模块还可以包括由平台所展露的web服务以集成外围系统,像客户关怀、用户门户等。

[0092] SDK视觉—在示例中,SDK可以指代工具和底层平台的API、实用程序、模式、接口、XML定义、抽象等的集体集合,其可以被使用和/或遵循来促进在MTP 212内运行的移动客户端应用或微件的创建。SDK的可以促进应用的开发,而无需对MTP或底层电话环境的深度知识。在示例中,安全、可靠的移动交易的复杂性可以被设计以使得是移动使能层的“隐藏在罩(hood)下”。

[0093] SDK可以支持对于第三方合作伙伴和声音幻觉(sound illusion,SI)团队的开放工具驱动开发。SDK可以授权开发者基于由钱包管理/使能层提供者(典型为网络提供者)所发行的指南来独立构建和分布它们自己的个性化安全交易微件。SDK可以开放各种层(基本上顶至底)。SDK可以相对于支持多手持机OS、鲁棒消息传送和通信、安全性和认证以及用于支付和非支付服务的基于NFC的安全邻近交易,提供对平台的横向能力的访问。SDK可以简化钱包和微件的开发。在示例中,MTP还可以具有用于直接构建原生(native)钱包的供应,以利用可能还未通过SDK展露的底层功能性。这可以给予开发者SDK和MTP二者中的最佳的,从而具有足够的灵活性以构建改进的用户体验。

[0094] 图3图示了MTP服务器300的详细架构。MTP服务器可以是用于构建钱包生态系统的使能基础设施,所述钱包生态系统可以支持移动商务(例如通过OTA)和移动支付(例如通过NFC邻近)交易服务。服务器可以提供前端网关,从而扩展由生态系统合作伙伴或服务提供者324(例如,商家、银行和运营商)通过移动钱包应用而提供给多个移动手持机328的服务。在示例性且非限制性实施例中,服务器可以包括组件集合,其可以协作来提供钱包管理、交易管理和生态系统集成。服务器可以用Java来开发并且可以支持各种应用服务器和数据库。在示例中,服务器可以是用于正由MTP提供的服务的容器。在示例中,服务器可以托管在集群化设置中的安全DMZ(非军事化(demilitarized)区)中,用于具有至生态系统云的连接性的关键任务应用。

[0095] 如图3中所图示,MTP架构可以包括服务器基础设施组件、服务模板和参考实现、NFC基础设施组件和主机集成框架。

[0096] 在示例中,MTP服务器可以包括多个信道302、通信模块304、OTA组件308、钱包管理模块310、交易引擎312、通知和服务总线314、指令管理模块、至少一个增值服务(VAS)模块

320、NFC基础设施322以及主机集成框架。在示例中,信道302可以提供信道特定适配,以用于要通过多个信道来接收的请求,诸如移动数据、SMS、USSD等。在示例中,通信模块304可以提供用于支持安全移动客户端服务器交互的框架。通信模块304可以促进来自单独商业组件的通信、认证、授权等。灵活架构可以促进服务开发者通过添加附加层来扩展安全性或者引入新要求。在示例中,OTA组件308可以提供对于促进可以在交易期间使用的应用、微件和个性化标记的OTA递送可能需要的支持。在示例中,OTA供应可以包括设备发现并确保可以将合适的版本递送给设备。在示例中,钱包管理310模块可以提供对于钱包状态管理、生命周期服务、版本管理、钱包历史等的实现。支付服务(例如软卡和个性化小程序的供应)也可以被包括作为钱包管理的一部分。在示例中,交易引擎312可以提供用于开发OTA交易服务的框架。可以通过遵循由交易框架所提供的模板来开发交易服务实现。可以通过交易框架来透明地管理可靠性、安全性、日志记录等的要求。交易框架可以提供对与内部虚拟帐户和外部支付网关的接口的集中式访问。在示例中,通知和消息总线314可以提供与客户端应用的对象交换总线。在示例中,通知和消息总线314可以包括对于向钱包推送警报和消息的支持。在示例中,器件管理模块318,可以存在若干组件,所述组件可以提供各种钱包器件(例如,信用卡、账单、票据等)并且管理与平台内的这些器件相关联的各种生命周期服务和配置。在示例中,VAS模块320中的至少一个可以包括用于公共商业服务的服务模板和实现方式的库,其可能已经通过使用MTP平台而被构建和部署。在示例中,NFC基础设施322组件是这样的一组组件,所述组件可以与NFC生态系统主机集成以用于精心安排(orchestrate)软卡和小程序的发行和个性化。所述集成可以是对于使能来自生态系统的全局平台顺从的NFC交易服务所需的支持。在示例中,主机集成框架可以是包括各种连接器的层,所述连接器可以插接到服务器中以与后端系统通信以用于促进交易服务。主机集成框架可以包括一系列接口定义,所述接口定义可能必须由服务开发者以连接器的形式来实现,以与外部主机系统通信。

[0097] 在本发明的各种示例性且非限制性实施例中,MTP服务器的主要职责可以包括为钱包用户社群提供钱包管理。在示例中,钱包管理可以包括钱包生命周期服务、支付、微件管理等。在本发明的各种示例性且非限制性实施例中,MTP服务器的主要职责可以包括以安全和可靠方式构建服务生态系统和精心安排来自钱包应用的与生态系统服务提供者的交易。在本发明的各种示例性且非限制性实施例中,MTP服务器的主要职责可以包括在构建和分布交易微件并且管理微件发现和递送中支持第三方开发者社群。在本发明的各种示例性且非限制性实施例中,MTP服务器的主要职责可以包括提供用于实现移动金融交易的所定义的模式和模板,其从服务开发者隐藏安全性、可靠性等的复杂性。

[0098] 图4图示了具有MTP移动客户端运行时400的钱包应用的高层级架构视图。出于该图的目的,钱包404和微件408a与408b可以与上面描述的模块类似,但是在功能性和职责上不同。在本发明的各种示例性且非限制性实施例中,MTP移动客户端402可以是用于快速移动应用开发的使能基础设施。移动客户端可以提供基于容器的途径来支持多租户(multi-tenant)应用架构。在示例中,移动客户端容器可以是电话特定运行时环境,用于可以通过使用MTP SDK所开发的钱包404和微件408a与408b。移动客户端容器可以促进应用执行、交易安全性、可靠性、设备特定实现等,从而允许开发者更多地集中于服务的独特功能。移动客户端容器可以构建在设备特定API的顶部并且可用于流行设备环境,例如,电话API 444。

移动客户端运行时可以从微件描述符生成原生应用屏幕。该屏幕可以确保屏幕上的按钮可以看起来好像相应设备上的原生Android®、Blackberry®或iPhone®按钮。移动客户端服务器可以包括至少一个电话独立的API 410。电话独立API 410可以确保通过使用SDK开发的微件408a与408b跨所有支持的手持机而运行。电话独立API 410可以特别地设计来提供开发者创建改进的用户体验可能需要的所有支持。可以配置移动客户端服务器402以便促进底层电话O/S内的原生实现,因为其可以通过运行时和API来抽象。在示例中,钱包应用可以像微件一样,因为钱包应用可以由移动客户端运行时402来解译和执行。在示例中,钱包404可以具有在移动应用上的特许控制。钱包404还可以为微件开发者定义附加API,其可以特定于应用的上下文(例如,有关于金融行业、零售行业、医疗保健行业、政府)。

[0099] 在本发明的各种示例性且非限制性实施例中,移动客户端运行时可以具有可以包裹所有主要电话平台开发者API的组件。在示例中,UI框架和工作流引擎可以渲染用户接口并操控本地商业功能的基于事件的执行。

[0100] 在本发明的各种示例性且非限制性实施例中,移动客户端运行时可以包括以下组件。移动客户端运行时可以包括UI框架412。在示例中,UI框架412可以提供必要的基础设施来渲染用户接口。在示例中,UI框架412可以包括UI引擎414、UI屏幕和布局418、样式集420以及多个UI元素422。UI框架412可以被配置为管理各种各样的手持机和屏幕能力。在示例中,UI引擎414可以基于在应用XML中提供的屏幕配置来管理屏幕418的生成和显示。移动客户端运行时402可以包括行动框架424。行动框架424可以提供必要的支持来执行商业特定逻辑(行动)。行动框架424可以以定制Java脚本(JavaScript)或预先存在的平台服务的形式。行动框架可以包括脚本引擎428。脚本引擎428可以控制行动的执行以及与用户接口的交互。移动客户端运行时402可以包括微件管理组件430。微件管理组件430可以促进管理微件生命周期服务432,诸如安装、加载、卸载、移除、更新等。微件管理组件可以包括访问控制器434,用以管理访问控制以仅准许微件访问它们在其微件描述符中具有针对其的准许的资源。移动客户端运行时402可以包括通信组件438。通信组件438可以被配置用于提供在客户端与服务器应用之间的基本通信服务。通信组件438可以提供对于HTTP(&HTTPS)以及SMS信道的通信支持。在示例中,通信组件438可以包括分组构造、编码/解码和基本HTTP差错处理。在示例中,通信组件438可以支持至用于像警报和广告一样的非必需商业对象的通信分组的附接。移动客户端运行时402可以包括数据库组件440。数据库440可以提供服务来存储、更新、移除和寻找来自本地数据库的数据。在示例中,数据库440可以提供可能从原生电话平台不可获得的API。移动客户端运行时402可以包括安全性组件442。安全性组件442可以提供加密API,用于加密、解密、基于散列的消息认证码(HMAC)、安全随机散列法等。移动客户端运行时可以包括NFC组件。NFC 448可以实现全局平台顺从NFC服务,并且提供用于与电话的安全元件上的小程序交互的API。NFC 448可以包含用于NFC标签和对等(P2P)模式的API。移动客户端运行时可以包括电话组件。电话可以提供平台服务以与电话组件相交互,所述电话组件像呼叫、SMS、LED、振动命令、日历功能、联系人管理等。移动客户端运行时可以包括微件408a与408b。微件可以是服务束,其可以封装用于商业服务集的屏幕、内容、资源、Java脚本和样式。微件可以通过使用MTP SDK来构建,所述MTP SDK可以包括在XML文件的预定义集上操作的工具集。

[0101] 在本发明的各种示例性且非限制性实施例中,移动客户端可以是在其之内可以安

装和运行微件的容器。在本发明的各种示例性且非限制性实施例中，移动客户端可以为整个移动应用来简化端对端可视工作流的开发。在本发明的各种示例性且非限制性实施例中，移动客户端可以提供一组良好测试的、标准化的API和平台服务，以用于应用开发者快速使用来构建他们的跨移动手持机平台的应用，而没有设备分片问题的风险。在本发明的各种示例性且非限制性实施例中，移动客户端可以生成改进的用户接口，其可以利用原生智能电话能力，但是仍然可以在有限能力设备上响应性的。在本发明的各种示例性且非限制性实施例中，移动客户端可以提供用于实现移动金融交易的所定义的模式，其可以被配置使得具有安全性、可靠性等的复杂性，如后端操作那样。

[0102] 图5图示了参照开发周期的微件开发过程的概观。

[0103] 在示例性且非限制性实施例中，MTP SDK可以被配置用于促进整体微件开发500并且向微件开发者提供更大程度的灵活性和独立性。微件开发中的第一阶段可以是设计阶段502。在示例中，开发者可以通过使用Microsoft office Visio®或类似工具及任何XML及Java脚本编辑器来创建移动应用。对开发进一步地，微件或微件文件504可以被封装。在示例中，开发者可以使用eclipse插件来封装微件工作空间并创建微件包(package)。可以将微件包发送到自动化构建服务器以用于微件生成508。微件文件504可以不以微件二进制514的形式。在示例中，自动化构建服务器可以生成包括移动客户端运行时以及微件包的应用二进制。对封装进一步地，可以使用测试容器510来测试微件。在示例中，开发者可以利用任何现成设备模拟器来核实微件流和脚本执行。对测试进一步地，微件可以被发布到MTP服务器512。在示例中，钱包用户可以能够发现微件并从MTP服务器512下载它们。

[0104] 在示例性且非限制性实施例中，多个工具可以用于微件开发，例如，MTP-SDK、MTP Microsoft Visio外附件(add-on)以及MTP eclipse插件。

[0105] 在示例中，MTP SDK用于服务器侧和客户端侧开发。客户端侧SDK(也称为移动客户端SDK)对于开发任何移动客户端微件可以是基本的。服务器SDK可以提供一组有用的协议和合约，其可以促进开发者在MTP的被证明的使能框架上构建。在示例中，还可以在不使用MTP服务器的情况下开发用于微件的独立web服务。

[0106] 在示例性且非限制性实施例中，MTP移动客户端SDK可以包括一组API，以访问各种原生电话平台服务，像数据库、无接触、通信等。所述API可以被提供作为Java脚本函数并且可以由微件开发者利用。在示例性且非限制性实施例中，MTP服务器SDK可以包括有用的库和合约，其可以使能与移动客户端微件的利用MTP的用于通信、安全性、可靠性、失效备援(failover)等的底层实现的快速集成。

[0107] 在示例中，诸如用SDK进行的MTP的元件的开发可以由可视化开发能力(例如，Microsoft Visio®)来支持，其促进开发者通过在MTP模板、型版(stencil)等的情况下执行拖放动作来定义用户接口工作流。MTP外附件可以促进工作流至MTP中、电话无关、XML格式(例如，MTP应用描述符)的导出。

[0108] 在示例性且非限制性实施例中，MTP eclipse插件、MTP SDK可以由可以用于从应用描述符生成钱包应用或微件的Eclipse插件所支持。MTP eclipse插件可以为所有所支持的设备平台提供单击构建选项。

[0109] 移动交易平台可以包括用于诸如容器、钱包、微件之类的元件和用于诸如金融、零售、健康、政府等之类的应用的参考实现。移动交易平台的特征和功能可以通过多个部署模

型来递送,其可以包括使用可以由MTP工具支持的原生客户端应用(例如,容器或移动客户端),提供者可以使用所述MTP工具来开发客户端功能,诸如钱包、微件、伴随小程序、优惠券发放小程序等。类似地,MTP可以促进(可以为每个提供者提供和/或定制的)web服务的部署,其可以促进展露MTP的不同特征等。诸如本文描述的多层安全移动交易使能平台之类的MTP可以包括可以用于开发钱包、微件、伴随小程序等的工具。用于配置和递送钱包、微件等的这些工具和方法还可以配置有向导(wizard)类实用程序以加快生态系统开发。附加的MTP工具可以被配置为监视使用和交易信息,并且此外基于各种能力和性能准则等来贡献用于优化的智能选项和解决方案。

[0110] 多层安全移动交易使能平台可以以对于可伸缩性、冗余性、互操作性、服务递送、消息定义等的必要支持来满足企业服务递送环境预期和需求。可以通过托管的用于服务/发行/获取提供者的模型和/或通过受管理的服务模型来递送平台。MTP促进跨如本文所描述的生态系统来实现规则(例如,商业、交易、信任等),其可以管控各种生态系统操作,除其它外尤其包括:参与者登上到生态系统中、参与者如何通过生态系统来访问和消费各种服务、如何可以从生态系统移除参与者、生态系统内的不同参与者如何可以彼此协作、不同参与者如何可以与生态系统外部的实体协作、参与者如何获取客户、参与者将如何支持客户、参与者如何可以捕捉与用户和交易相关的数据(静态和动态)、参与者将如何在生态系统内和外使用这样的数据、共享这样的数据和将这样的数据货币化。

[0111] MTP可以与专家引擎相关联,用于向生态系统中的客户以及提供者/参与者提供客户支持。可以利用专家引擎以通过本文描述的方法和系统来向客户以及提供者/参与者递送简化的用户体验。MTP可以架构有如本文所描述的若干层或小面(facet),并且为了描述而被标签为使能、服务、个性化等,其中每个层潜在地进一步被划分成其它层,诸如逻辑和物理层或方面。这样的多层架构或平台可以独特地帮助在如本文所描述的多域(和可选地多租户)生态系统中递送服务和功能性,而同时确保在服务提供者之中的独立所有权并支持差异化能力的演进,尤其是在多域生态系统环境中。

[0112] 可以通过可以促进生态系统宽泛能力、钱包和微件的容器来递送MTP,所述钱包可以促进差异化器件实现相关的能力和特征(例如,NFC、具有安全元件(SE)的NFC、标记化、通过QR码/条形码所展露的标记化等),所述微件可以促进提供者可以在生态系统内不经媒介(disintermediation)的情况下直接向外展露给终端用户的差异化能力和特征。

[0113] 诸如本文描述的多层安全移动交易使能平台之类的MTP可以基于生态系统参与者、规则等的后端要求来确保跨诸如本文描述的多域生态系统之类的生态系统的不同前端协议的聚集。可以此外通过提供抽象或包裹器(wrapper)能力和/或包裹器能力的标记化来优化不同前端协议的聚集。

[0114] MTP可以通过本文描述的方法和系统在企业服务递送环境上使得生态系统能够将协议层级功能性逐渐递送到前端中。可以此外通过提供本文描述的包裹器的标记化或聚集能力或者通过使用生态系统规则来增强协议层级功能性递送。

[0115] MTP可以设置在网络提供者的域中并且其部分集成到它们的系统中。MTP可以附加地连接到服务和安全性提供者的生态系统,包括一个或多个可信服务管理器(TSM)。网络提供者可以使用MTP来创建以特定商业垂直面为目标的移动应用。这样的品牌移动应用可以是用于例如零售/金融域的钱包,或者例如用于医疗保健垂直面的钱包。这样的钱包应

用可以向用户提供核心服务集,所述核心服务集特定于其被创建所针对的域。除了提供核心域服务之外,钱包还可以操控应用生命周期和安全性、标准化的用户体验以及钱包管理职责。微件可以提供特定商业服务并遵照钱包指南。

[0116] 图6描绘了如本文所描述的用于安全个性化交易的生态系统的概观。生态系统600可以包括多个参与者(诸如客户端设备的用户602、器件的发行者610、交易器件的获取者620、服务提供者或商家608)以及包括交易和处理资源604的各种基础设施元件,所述交易和处理资源604可以包括移动交易平台(MTP)622、规则、与工具和参与者的接口,其可以具体化为一个或多个企业服务总线(ESB)、销售点设施612、安全销售点转换功能性、用于抽象交易协议的功能性等。客户端设备602可以包括多个容器,其可以包括用于执行针对一个或多个服务/产品的交易(例如,支付交易)的多个钱包、钱包伴随小程序和多个微件,所述一个或多个服务/产品可以由诸如服务提供者608之类的服务提供者所供应。

[0117] 图6中描绘的MTP 622可以设置在网络提供者的域中并且集成在网络提供者的系统中(可选地通过它们的ESB)。如所示出的,MTP可以被配置为连接在服务提供者的生态系统600内。单独、独立的服务提供者或商家608可以使用MTP软件开发套件和环境来构建可以加载到在客户端设备602上可访问的钱包或钱包容器中的微件。这些微件可以提供增量式功能性,其可以增强钱包应用的整体吸引力。此外,MTP基础设施604可以包括规则,诸如用以提供钱包、微件和交易管理连同与向总体的(a universe of)各种移动环境递送钱包相关联的所有相关商业服务。此外,MTP可以建立与各种生态系统的连接,以向终端用户递送可以随时随地访问的动态用户体验和各种服务集。

[0118] 生态系统600此外可以包括多个交易器件发行者610。发行者610可以提供各种交易器件,诸如虚拟信用卡、礼品卡、忠诚卡、票据等。客户端的用户602可以通过使用一个或多个钱包和微件来选择这些器件以执行交易。在示例中,多个发行者610可以使用与MTP 622相关联地提供的工具来开发定制的微件以增强用户体验、提供安全性、遵照发行者 workflows等。此外,生态系统600可以包括数字钱包(例如,其可以安装在移动客户端602上),其可以包括用于存储这些器件、执行针对这些器件的交易等的功能性。

[0119] 生态系统600此外可以通过以下能力和特征来表征,所述能力和特征诸如:对于个性化交易的三维安全性(例如,设备、域和用户)、多个功能性层(例如,具有个性化、服务、使能层、专家和体验框架层或层次的架构)、对于客户端设备602上的多个独立容器的支持、容器内的多个不同微件、容器内多个不同且独立的钱包、对多个钱包的单个微件访问、通过多个微件的单个钱包访问、对于多个信任模型的支持等。生态系统600此外可以包括销售点设施或功能性612,其可以被配置为执行真实(例如,基于邻近)和/或虚拟(例如,在线)交易。生态系统600可以包括协议抽象组件614,其可以包括包裹器,诸如用以跨多种类型的协议在客户端602与销售点设施612之间执行交易等。例如,协议抽象组件614可以使客户端设备602能够独立于销售点设备612或聚集器交换机(aggregator switch)通过其而进行操作的协议来执行交易。

[0120] 生态系统600此外可以包括多个获取者620。获取者620中的每一个可以是与MTP 622相关联地提供的使用工具,用于开发定制的微件、钱包等。在示例中,生态系统600可以包括交换机618,用于从多个获取者选择获取者620用于执行交易。

[0121] 如图6中所描绘的,发行者610、服务提供者608、获取者620等可以以生态系统600

功能性的仅部分而具有对用于安全个性化交易的生态系统的其部分的访问或者可以配置所述部分。在示例中,获取者620a包括钱包功能性,而获取者620n包括微件功能性。同样地,发行者610a包括钱包和微件功能性,而发行者610n仅包括微件。类似地,服务提供者608a包括微件、钱包和容器,而服务提供者608n仅包括微件和钱包。

[0122] 图7描绘了用于使用在用于安全个性化交易的生态系统中的示例性客户端架构700。客户端架构700可以包括基于容器的途径,诸如用以支持多租户应用架构。客户端架构700可以被配置成可以由设备独立API、一个或多个设备特定的操作系统环境等支持的商业特定服务、钱包功能性、使能基础设施等。钱包功能性可以是基于容器的,用以提供包括商业规则附着、钱包和微件应用生命周期管理、用户体验管理的功能性,并且此外可以包括一个或多个容器714,其可以包括一个或多个钱包702。商业特定服务可以由一个或多个微件提供,诸如微件704a、微件704b、微件704c……,以及微件704n(本文总称为微件704)。通过客户端运行时环境708中的设备不可知API和服务执行环境可以促进使能基础设施。

[0123] 此外,客户端架构700可以包括移动客户端运行时容器708,其可以是用于通过使用MTP软件开发套件(SDK)所开发的钱包702和微件704的电话特定运行时环境。该容器可以操控与应用执行、交易安全性、可靠性等相关的复杂性,从而这可以允许开发者更多地集中于服务的独特功能并且不担心包括设备特定实现的大部分复杂性。移动客户端容器708可以构建在设备特定API的顶部并且可用于流行的设备操作系统环境710。运行时容器708可以从与微件704相关联的描述符生成原生应用屏幕。这确保按钮在相应设备上看起来像原生ANDROID、BLACKBERRYOS或IPHONEOS按钮。

[0124] 客户端架构700此外可以包括设备独立API层次712,其可以确保通过使用SDK所开发的微件可以跨所有支持的手持机而运行。这些API特别设计用于提供开发者创建丰富用户体验所需要的所有支持。然而,开发者可以不需要担心底层电话O/S内的原生实现,因为这通过客户端运行时容器708和API层次712而被抽象出。钱包702可以像微件那样执行,因为其可以由客户端运行时708解译和执行。然而,钱包702可以具有对应用的特许控制。钱包702还可以为微件开发者定义可以特定于应用的上下文(金融、零售、医疗保健、政府等)的附加API。

[0125] 图8描绘了包括具有协议抽象支持能力的MTP结构配置的用于安全个性化交易的生态系统。系统800可以包括通信地耦合到网络810的移动设备802、MTP服务器804和多个服务提供者,诸如服务提供者808a、服务提供者808b、服务提供者808c……,以及服务提供者808n。移动设备802可以包括多个容器,诸如容器812a和容器812n。容器中的每一个可以包括多个钱包,诸如钱包814a和钱包814n(本文中总称为钱包814)。容器中的每一个可以包括多个微件,诸如微件818a和微件818n(本文中总称为微件818)。

[0126] 不同的服务提供者可以利用如本文所描述的移动交易平台和/或钱包服务中心(WSC)的不同特征。例如,服务提供者808a可以访问MTP的钱包服务中心工具套件能力,服务提供者808b可以访问钱包服务中心插件能力,服务提供者808c可以访问钱包服务中心web门户服务,以及服务提供者808n可以提供不需要任何专用WSC或MTP驻留软件的服务包。各种服务提供者或商家可以通过网络810来访问WSC开发环境和WSC运行时。例如,服务提供者808n可以不被要求运行工具套件,并且可以直接访问如在MTP服务器804上可用的WSC工具套件。类似地,MTP服务器804可以向各种服务提供者提供对库的访问,其中,所述库可以包

括用于编码/解码的编解码器、认证/安全性方案等。不是每个服务提供者被要求运行WSC库。

[0127] 在示例中,MTP服务器804可以被配置为向多个服务提供者提供开发环境以及运行时环境。在任何时刻,服务提供者可以具有插件、库,或者可以从MTP服务器804直接访问这些组件。结果,该系统允许服务提供者或商家按照所期望的要求来定制配置。可替换地,MTP服务器804可以与诸如移动设备802之类的客户端设备直接连接以执行交易,诸如代表服务提供者(例如,PL808n)。

[0128] 生态系统可以包括诸如通过各种销售点(PoS)终端和通过空中交易的获取功能性。可以通过获取模块824可选地促进与交易获取相关联的协议抽象,所述获取模块824可以合并MTP和/或WSC获取功能性822,其可以向系统添加更多功能性以诸如使得交易更可靠、鲁棒和安全。PoS终端820可以经由各种获取协议中的任一种、通过一个或多个邻近通信信道来与移动设备802通信,所述信道包括但不限于NFC、蓝牙、条形码读取器等。可以经由包裹移动设备802与PoS终端820之间的这样的通信来操控协议抽象。在示例中,包裹器可以被实现用于抽象这样的协议:所述协议具体化钱包814与PoS终端820之间的交易。对于空中交易(例如,其不直接使用PoS终端820),可以经由包裹器、标记、标记化的包裹器等类似地生成协议抽象,所述包裹器、标记、标记化的包裹器等可以用于通过公共网络810(例如,因特网)来交换信息以实现交易。

[0129] 图9描绘了如图8中所描绘的用于安全个性化交易的生态系统的可替换配置,其不使用获取设施(例如,图8中的824)。

[0130] 本文描述的多域生态系统安全个性化交易的方法和系统包括在多域生态系统中用于安全个性化交易的诸如平台的系统。所述平台可以包括个性化层,用于使能存储在移动设备上的一个或多个生态系统元件的服务提供者个性化。可以从包括微件、钱包和小程序的组中选择所述一个或多个生态系统元件。所述平台此外可以包括使能层,用于促进个性化层与客户端设备之间的互操作。所述平台此外可以包括独立于使能层而操作的服务层,用以使能针对多个服务的服务递送。在示例中,可以从包括银行业务、票务和账单支付的组中选择所述多个服务。所述平台在生态系统参与者的分布式网络中可以是可操作的。生态系统参与者可以包括诸如服务提供者、器件发行者、器件获取者以及移动设备用户。所述平台此外可以包括多个功能模块。所述功能模块可以包括用于诸如通信、通知、安全性、认证、空中操作之类的一个或多个模块以及用以管理钱包和微件的设备运行时容器。所述平台此外可以包括软件开发环境,其可以包括诸如容器、钱包和微件的参考实现。软件开发环境此外可以包括诸如金融、零售、健康和政府域的参考实现。在示例中,可以通过使用原生客户端应用来部署所述平台。在示例中,可以通过使用原生客户端应用和一组软件开发工具来部署所述平台。该组软件开发工具可以用于开发客户端功能。可以从钱包、微件、伴随小程序和优惠券发放小程序的组中选择该组客户端功能。在示例中,可以通过使用原生客户端应用和一组web服务来部署所述平台,该组web服务可以由平台展露以集成外围系统。所述外围系统可以包括诸如客户关怀和用户门户。在示例中,可以用这样的工具来部署所述平台:所述工具可以用于诸如开发钱包、微件和伴随应用。所述工具可以包括向导类实用程序。在示例中,所述工具可以用于监视使用和交易信息。在示例中,所述工具可以用于提供智能优化选项和解决方案。优化解决方案可以基于所监视的能力和性能准则。在示例

中,所述平台可以被部署有企业服务递送环境中的必要支持。所述必要支持可以包括诸如对可伸缩性、冗余性、互操作性、服务递送以及消息定义的支持。在示例中,可以通过用于多个提供者的托管的模型来部署所述平台。可以从包括诸如服务、发行和获取提供者的组中选择所述多个提供者。在示例中,可以通过实现规则来递送所述平台,所述规则可以管控由生态系统参与者对服务的使用。在示例中,所述规则可以管控由参与者对服务的访问。在示例中,所述规则可以管控由参与者对服务的消费。在示例中,所述规则可以管控如何可以从生态系统中移除参与者。在示例中,所述规则可以管控在生态系统内参与者如何可以与彼此协作。在示例中,所述规则可以管控参与者如何可以与生态系统外部的实体协作。在示例中,所述规则可以管控参与者如何可以获取客户。在示例中,所述规则可以管控参与者如何可以支持客户。在示例中,所述规则可以管控参与者如何可以捕获与用户和交易相关的数据。在示例中,用户和交易可以是静态的。在示例中,用户和交易可以是动态的。在示例中,所述规则可以管控参与者如何可以在生态系统内使用所捕获到的数据。在示例中,所述规则可以管控参与者如何可以在生态系统外部使用所捕获到的数据。在示例中,所述规则可以管控参与者如何可以在生态系统内共享所捕获到的数据。在示例中,所述规则可以管控参与者如何可以在生态系统外部共享所捕获到的数据。在示例中,所述规则可以管控参与者如何可以在生态系统内将所捕获到的数据货币化。在示例中,所述规则可以管控参与者如何可以在生态系统外部将所捕获到的数据货币化。在示例中,可以通过利用专家引擎来向参与者提供客户支持以使得可以从客户和提供者的组中选择参与者来递送所述平台。在示例中,可以通过利用专家引擎来向参与者提供简化的用户体验以使得可以从客户和提供者的组中选择参与者来递送所述平台。在示例中,可以通过使用多层来架构所述平台。可以从包括诸如使能层、服务层和个性化层的组中选择所述多层。每层可以进一步被划分成附加层。可以从包括诸如逻辑层和物理层的组中选择所述附加层。

[0131] 用于安全个性化交易的多域生态系统平台可以包括用于生态系统元件的服务提供者个性化的个性化层、独立于服务层而操作的用于促进与客户端设备软件和硬件的互操作的使能层,所述服务层促进针对诸如银行业务、票务、账单支付等之类的各种服务的递送。这样的多域生态系统平台可以促进包括安全个性化交易的一般和专门的交易,可以在逻辑上和/或物理上分割成多个功能独立块、分段、单元、层次或层,使得它们结合通过接口使用数据或信息的交换来分离地操作,或者以预定或可配置顺序来与彼此无缝地操作,以履行较大功能或单元的交易或完整交易。作为示例,如本文所描述的多层生态系统使能平台可以由三层构成,即,个性化层、服务层和使能层。

[0132] 此外,作为示例,个性化层可以用于实现特定品牌化元素(诸如商标、徽标、主题、颜色等)、用户交互元素、工作流(例如,存储的帐户和交易数据,用以使能高效完成重复交易、购物车、单击交易以及许多其它)、用户接口效果(例如,过渡、内容格式、动态或任何其它行动)、可能由服务提供者对于特定要求所需要的原因和/或效果。个性化层次可以促进服务提供者的协作设计或交互哲学的部署,以及为消费者给出空间来调整至它们的个人需要和偏好,包括针对视觉上受损等。

[0133] 使能层可以促进与底层层次、平台或基底的交互,所述底层层次、平台或基底可以以软件或硬件或二者的组合的形式以与其通信和交互。使能层可以或者可以不充当将高于其的层次或层与低于使能层的那些有效隔离的抽象。

[0134] 服务层可以迎合诸如 workflows、商业逻辑、规则、智能之类的特定要求以及服务垂直面的需要,所述服务垂直面包括诸如但不限于以下各项的服务垂直面:银行业务、票务、账单支付、优惠券发放、忠诚及积分卡程序、停车以及其它生态系统服务。

[0135] 由这样的服务层所使能的服务可以包括移动银行业务、转账、账单支付、票务、优惠券发放、忠诚程序、市场和广告相关服务、教育相关服务、城市服务、移动健康服务、移动保险、诸如停车优惠券之类的运输服务、旅行服务、紧急情况或911服务、零售支付、后勤支持服务、商业智能解决方案、品牌化、购物、产品认证服务、调节服务、记录管理、交互电视服务、文本到语音服务、基于位置的服务等。

[0136] 尽管本文使用的示例说明了多层生态系统使能平台的概念,但是本文描述的方法和系统实际上涵盖更一般化的平台架构和/或结构概念,其包括多个功能独立的块、分段、单元、层次或层。图10描绘了可以跨越一系列生态系统元件的分层平台的概念,所述元件包括客户端设备(例如,移动设备)、钱包服务中心功能性、可信安全性管理器、移动交易平台服务器、钱包发行者、商家(亦称服务提供者)等。每个这样的生态系统元件可以至少包括使能、服务和个性化层。如本文中注意到的,还可以在多层安全移动交易生态系统使能平台的部署中并入附加层,诸如专家引擎和体验框架层。

[0137] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,其包括分析包括以下各项的集合中的一个或多个:生态系统参与者、服务要求、客户要求、调节要求、交易安全性要求、信任模型以及电子交易通信信道。所述方法此外可以包括基于分析来确定一个或多个生态系统特征以配置在包括服务层、使能层和个性化层中的至少一个的平台中。所述方法此外可以包括根据所述确定来配置所述一个或多个生态系统特征。在实施例中,所述一个或多个生态系统特征可以被配置以确保在服务提供者商业模型的上下文内满足每个所分析的要求。所述平台可以附加地包括专家引擎层和体验框架层。

[0138] 用于选择生态系统特征以用于包括在使能层、服务层和个性化层的每一个中的方法可以包括分析生态系统参与者、服务要求、客户要求、调节要求、交易安全性要求、信任模型以及电子交易通信信道,以确定生态系统特征以配置在服务层、使能层和个性化层中以确保在服务提供者商业模型的上下文内满足每个所分析的要求。可以对于诸如专家引擎和体验框架层之类的附加层类似地确定特征。

[0139] 将整体交易、服务或过程的部分分解成多层生态系统平台的方法或过程可以基于分析法、启发法和要求的组合,可选地通过包括专家引擎的工具基于人工智能概念来提供帮助。这样的方法或过程可以考虑生态系统中所有参与(目前和预期的将来)实体的视角和要求,所述实体包括但不限于:服务提供者;服务要求;客户要求;终端用户要求;调节委托&指南;安全性委托、指南和要求;信任模型;经济模型;商业逻辑和工作流;与其它服务的公共性;操作因素;设计&技术因素;目标设备&平台;规划的技术演进;其它相关&不相关服务;以及操作约束。

[0140] 在大多数情况中,上面提及的方面和参数可以导致服务要求在逻辑上被分割或分区成三层,即,个性化、服务和使能层。

[0141] 参照图11,选择生态系统特征以用于包括在用于安全个性化交易的多域生态系统平台的使能层、服务层和个性化层的每一个中的实施例。基于参与者商业目标和要求,生态系统特征分配引擎1102可以处理规则和控制,以诸如将生态系统的特征分配给使能层

1104、服务层1108和个性化层1110。

[0142] 在示例中,使能层1104可以包括对于开发移动应用可能必需的基础设施或商业独立组件。服务层1108可以包括对于钱包生态系统和增值服务的参考服务实现集。个性化层1110可以包括一组工具和API,其可能对于开发(本文档中描述的)钱包和微件服务以及构建综合生态系统是必需的。

[0143] 在示例中,使能层1104可以包括对于客户端和服务端不同的特征。在使能层1104中,客户端可以被配置为包括基础设施运行时容器软件(SW),其可以通过使用与移动设备相关联的特定开发环境来构建。在示例中,使能层1104可以向客户端提供对底层设备能力的公共抽象,所述底层设备能力具有公共开发者API、UI解译和渲染引擎、商业执行环境、微件和钱包生命周期管理、用于OTA/邻近交易的模式等。在服务器侧,使能层1104可以向服务器提供可以在网络提供者的域中部署的基础设施软件,其可以被配置用于建立和管理安全移动交易生态系统。在示例中,使能层1104可以配置服务器特征,诸如钱包管理、状态交易引擎、对象生命周期管理、信道特定通信、多域安全性策略和风险管理、OTA供应等。

[0144] 在示例中,服务层1108可以包括用于客户端的多个特征。例如,客户端可以被配置为包括可以用于实现多个商业用例的公共平台服务库。公共平台服务可以在由使能层1104提供的商业执行环境内运行。在示例中,服务层1108可以包括三个基本单元。第一单元可以是用例,例如,为各种交易服务所构建的一组客户端侧工作流和模板。第二单元可以是器件,例如,可以促进到真实世界器件的映射的对应单个钱包器件。在示例中,器件可以提供数据用于可视化或显示。在示例中,器件可以提供数据用于空中(OTA)交易。在示例中,器件可以提供数据用于邻近交易。在示例中,器件可以提供数据用于监管。第三单元可以包括至少一个信任模型。信任模型可以促进对于认证方案的实现,其可以包括两因素认证(2FA)。2FA可以由不同微件提供者所需的并且可以是与生态系统相关的。

[0145] 在示例中,服务层1108可以包括用于服务器的多个特征。服务器可以被配置为包括商业特定组件和相关联的服务模板的库,其可以部分或整体重用来开发客户为中心的供应。在示例中,服务可以包括钱包服务和增值服务。钱包服务可以包括管理钱包和支付标记的生命周期。增值服务可以包括提供商业服务。服务层1108可以包括三个单元。第一单元可以是用例,例如,可以通过使用用于实现特定用例的移动使能层1104的交易框架来构建服务器侧模板。在示例中,可以存在用于商业服务(例如,账单支付、电影票务等)的一个或多个不同的模板。第二单元可以包括至少一个器件或标记。器件可以包括商业特定数据对象(例如,信用卡、银行帐户、账单、优惠券等),其可以跨各种服务被重用并且可以提供对于对象的共同理解定义以及管控对象的生命周期与交易的规则的实现。第三组件可以包括至少一个信任模型。该信任模型可以促进用于服务的不同认证方案的实现,包括对在具有它们的独立TSM的单独信任集群内操作的支持。

[0146] 在示例性且非限制性实施例中,个性化层1110(也可以称为SDK层)可以包括用于客户端和用于服务器的不同特征。在示例中,与SDK层中的客户端相关联的特征可以划分成2部分。第一部分可以是钱包SDK,并且第二部分可以是微件SDK。在示例中,钱包SDK可以提供对钱包服务、特许API以及对于构建钱包容器应用或用户体验所必需的组件的访问。在示例中,微件SDK可以促进生态系统合作伙伴构建它们的可以在钱包容器内操作的微件。在示例性且非限制性实施例中,SDK可以基本上促进客户端侧配置和用户体验。在示例中,SDK可

以通过促进对于由客户端容器所展露的参数的可定制性来促进配置。这可以包括设备特定参数、变量(像PIN大小、退出确认、选择模块的包含物等)。在示例中,SDK可以通过促进跨手持机的差异化用户体验的开发来提供用户体验。

[0147] 在示例中,用于服务器的SDK可以包括至少一个库,其可以允许任何生态系统服务器与钱包通信、格式化对于微件的内容,以及向钱包应用展露服务。该库可以包括配置模块和接口模块。配置模块可以允许对于由服务器的移动使能层1104和服务层1108展露的参数的可定制性。可以在属性文件和资源束中配置参数。接口模块可以提供开发来促进与各种后端系统的通信的连接,所述后端系统可以协作来履行完整的端对端服务。接口模块还可以包括由平台所展露的web服务以集成外围系统,像客户关怀、用户门户等。

[0148] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种在平台中的方法,所述平台包括诸如服务层、使能层和个性化层中的至少一个。该方法包括应用专家引擎来分析一个或多个移动设备用户和交易环境要求。在示例中,专家引擎可以包括专家引擎层。专家引擎层可以与体验框架相交交互以适应所述一个或多个用户要求。在示例中,应用专家引擎可以包括应用专家引擎来分析用户的习惯。该方法此外可以包括根据分析来配置一个或多个平台特征。在实施例中,配置所述一个或多个生态系统特征可以包括基于一个或多个交易要求来配置用户接口。在示例中,配置所述一个或多个生态系统特征可以包括配置移动设备的一个或多个显示特征。在示例中,所述一个或多个显示特征可以基于与移动设备的位置相关联的地区偏好来配置。在示例中,所述一个或多个显示特征可以基于所识别的客户端基础来配置。

[0149] 多层安全移动交易使能平台可以促进将用于安全个性化交易的多域生态系统伸缩至数千万用户,包括应用专家引擎以用于分析用户和交易环境要求以及配置生态系统特征来简化交易,诸如基于交易要求来配置用户接口。专家引擎可以与体验框架相交交互以促进对用户要求的适应。

[0150] 预期的是,当提到使用设备和应用时,用户将具有变化的偏好、习惯、感知、视角、要求和风格。除了上面提及的参数之外,用户对于它们操作的结果的呈现具有单独的偏好、品味和要求。当前可获得的许多或大多数应用约束用户遵从特定生活规则(regimen)来实行交易和从系统获得与查看结果。

[0151] 本文档中描述的专家引擎层可以学习上面提及的用户习惯、偏好和其它参数,并且可以调整系统和/或应用以用最合适于单独用户的方式呈现其自身,包括地区偏好(“大部分法国人喜欢其是这种方式,而美国人喜欢其是那种方式”)、移动设备能力(屏幕尺寸、键盘可用或者仅在屏幕上等)以及客户端基础中的差异(低端相对于奢侈客户)。

[0152] 专家引擎层还可以管理生态系统中的变幻莫测(vagary),诸如通信中的中断、服务器响应中的延迟、诸如耗尽电池或信号下降之类的异常操作条件等,以确保对于用户的不中断或中断管理的体验。专家引擎可以确保操作故障被管理,并且随着和当常态已经被还原时,用户能够无缝地恢复操作。

[0153] 当我们向上面提及的问题添加具有大量不同用户的维度时,所述问题进一步加剧。估计数量多达数千万,其中数千个交易同时进行。

[0154] 专家引擎可以基本上如早前所概述的那样管理所有用户,并且还对交易、使用模式以及将帮助推理引擎的“学习”过程的其它参数实行分析。

[0155] 参照图12,如本文所描述的专家引擎被示例性描绘用于促进针对用于安全个性化交易的多域生态系统中的多个服务提供者中的每一个修改个性化和服务层中的每一个。

[0156] 专家引擎层/设施1208可以占据提供者特定个性化层1202,并且通过分析生态系统的各方面1214来适配它们以提供经适配的个性化层1210,所述方面包括:交易环境方面、用户历史方面、用户环境方面、历史交易相关数据方面、设备相关方面、生态系统状态(例如,响应性和/或稳定性等)、如可以从登记的参与者和/或生态系统交易活动的数量所确定的生态系统大小、提供者特定方面等。类似地,提供者特定服务层数据1204可以由专家引擎层/设施1208进行专家适配以产生一个或多个经专家适配的服务层1212。

[0157] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于在生态系统中使能多种类型的电子钱包的平台。该平台可以包括用于开发提供者特定钱包的软件开发套件。该软件开发套件可以至少部分地通过联网服务器可执行。该平台此外可以包括通过软件开发套件可访问的多个参考钱包。所述多个参考钱包可以包括诸如用于多个提供者中的每一个的参考钱包,所述多个提供者包括器件发行者、服务提供者以及器件获取者。该平台此外可以包括运行时容器,其在客户端设备上可操作用于接收不同类型的提供者特定钱包。所述容器可以促进每种类型的提供者特定钱包的不同操作以用于执行提供者特定钱包与开发该提供者特定钱包的提供者之间的安全交易。

[0158] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令可以使得所述一个或多个处理器实行下面的步骤,所述步骤包括在移动设备上的钱包容器中配置一个或多个微件模块。所述步骤此外可以包括通过一个或多个微件模块来访问钱包容器中的一个或多个钱包模块。在示例中,访问一个或多个钱包模块可以包括接收从服务提供者模块到钱包容器中的第一微件模块的通信,和使能通过第一微件模块对钱包模块的经认证的访问。在示例中,可以通过网络由服务提供者在钱包容器中配置和安装一个或多个钱包模块中的每一个。在示例中,可以通过网络由用户在钱包容器中配置和安装一个或多个钱包模块中的每一个。通过计算机可读介质实行的所述步骤此外可以包括在访问一个或多个钱包模块之前对一个或多个微件模块中的每一个进行认证。

[0159] 可以在发行者、服务提供者和器件获取者的多域生态系统中使能多种类型的电子钱包的安全生态系统基础设施可以包括客户端侧功能性,其包括在移动设备上可操作的钱包容器,所述钱包容器促进多个不同钱包的隔离并且此外促进通过被配置到钱包容器中且安全地维护为分离模块的微件模块来访问每个不同钱包,其中,每个微件必须被认证以访问任何钱包。这样的生态系统基础设施还可以包括在移动设备远程操作并且彼此不同的个性化服务提供者模块,其中,服务提供者模块与钱包容器中的微件通信,并且钱包容器促进通过微件对钱包的经认证的访问。另外,生态系统基础设施元件可以包括用于通过网络由服务提供者、发行者、代理等在钱包容器中配置和安装不同钱包中的每一个的能力。用于使能多种类型的电子钱包的安全生态系统基础设施的这些和其它特征此外在图8和9中进行了描绘和描述。

[0160] 本文描述的多域生态系统安全个性化交易的方法和系统包括这样的方法,所述方法包括分析至少一个要求。在示例中,所述至少一个要求可以选自包括以下各项的集合:商业策略、进入市场策略、退出策略、竞争策略、产品路线图(roadmap)、硬件发布安排和特征

列表、软件发布安排、特征列表以及应用编程接口。在示例中，可以在服务提供者商业模型的上下文内分析所述至少一个要求。该方法此外可以包括至少部分基于分析来配置服务层、使能层和个性化层。在示例中，使能层可以被配置为包括通过使用与移动设备相关联的特定开发环境所构建的基础设施运行时容器软件。在示例中，服务层可以被配置为包括可以用于实现多个商业用例的公共平台服务的库。

[0161] 用于选择新业务需求和设备功能性以用于包括在使能层、服务层和个性化层的每一个中的方法可以包括分析与商业策略、进入市场策略、退出策略、竞争策略、产品路线图、硬件发布安排和特征列表以及软件发布安排、特征列表和应用编程接口相关的要求，以在服务层、使能层和个性化层中进行配置以确保在服务提供者商业模型的上下文内满足每个分析的要求。可以为诸如专家引擎和体验框架层之类的附加层类似地确定特征。

[0162] 将整体交易、服务或过程的部分分解成多层生态系统平台的方法或过程可以基于分析法、启发法和要求的组合，可选地通过包括专家引擎的工具基于人工智能概念来提供帮助。这样的方法或过程可以考虑与以下各项相关的视角和要求（目前的和预期在将来的这二者）：商业策略、进入市场策略、退出策略、竞争策略、产品路线图、硬件发布安排和特征列表以及软件发布安排、特征列表和应用编程接口。

[0163] 在大多数情况中，上面提及的方面和参数可以导致服务要求在逻辑上被分割或分区成三层，即，个性化、服务和使能层。

[0164] 参照图13，选择业务需求和设备功能性以用于包括在用于安全个性化交易的多域生态系统平台的使能层、服务层和个性化层的每一个中的实施例。基于参与者业务需求和设备功能性，生态系统特征分配引擎1302可以处理规则和控制，以诸如将生态系统的特征分配给使能层1304、服务层1308和个性化层1310。

[0165] 在示例中，使能层1304可以包括开发移动应用可能必需的基础设施或商业独立组件。服务层1308可以包括用于钱包生态系统和增值服务的参考服务实现的集。个性化层1310可以包括一组工具和API，其可能是开发（本文档中描述的）钱包和微件服务以及构建综合生态系统所必需的。

[0166] 在示例中，使能层1304可以包括对于客户端和服务端不同的特征。在使能层1304中，客户端可以被配置为包括基础设施运行时容器软件（SW），其可以通过使用与移动设备相关联的特定开发环境来构建。在示例中，使能层1304可以向客户端提供对底层设备能力的公共抽象，所述底层设备能力具有公共开发者API、UI解译和渲染引擎、商业执行环境、微件和钱包生命周期管理、用于OTA/邻近交易的模式等。在服务器侧，使能层1304可以向服务器提供可以在网络提供者的域中部署的基础设施软件，其可以被配置用于建立和管理安全移动交易生态系统。在示例中，使能层1304可以配置服务器特征，诸如钱包管理、状态交易引擎、对象生命周期管理、信道特定通信、多域安全性策略和风险管理、OTA供应等。

[0167] 在示例中，服务层1308可以包括用于客户端的多个特征。例如，客户端可以被配置为包括可以用于实现多个商业用例的公共平台服务的库。公共平台服务可以在由使能层1304提供的商业执行环境内运行。在示例中，服务层1308可以包括三个基本单元。第一单元可以用例，例如，针对各种交易服务所构建的一组客户端侧工作流和模板。第二单元可以是器件，例如，可以促进到真实世界器件的映射的对应单个钱包器件。在示例中，器件可以提供用于可视化或显示的数据。在示例中，器件可以提供用于空中（OTA）交易的数据。在示

例中,器件可以提供用于邻近交易的数据。在示例中,器件可以提供用于监管的数据。第三单元可以包括至少一个信任模型。信任模型可以促进认证方案的实现,其可以包括两因素认证(2FA)。2FA可以由不同微件提供者所要求并且可以是与生态系统相关的。

[0168] 在示例中,服务层1308可以包括用于服务器的多个特征。服务器可以被配置为包括商业特定组件和相关联的服务模板的库,其可以部分或整体重用来开发客户为中心的供应。在示例中,服务可以包括钱包服务和增值服务。钱包服务可以包括管理钱包和支付标记的生命周期。增值服务可以包括提供商业服务。服务层1308可以包括三个单元。第一单元可以是用例,例如,可以通过使用移动使能层1304的用于实现特定用例的交易框架来构建服务器侧模板。在示例中,可以存在用于商业服务(例如,账单支付、电影票务等)的一个或多个不同模板。第二单元可以包括至少一个器件或标记。器件可以包括商业特定数据对象(例如,信用卡、银行帐户、账单、优惠券等),其可以跨各种服务被重用并且可以提供对于对象的共同理解定义和管控对象的生命周期与交易的规则的实现。第三组件可以包括至少一个信任模型。该信任模型可以促进用于服务的不同认证方案的实现,包括对在具有它们的独立TSM的单独信任集群内操作的支持。

[0169] 在示例性且非限制性实施例中,个性化层1310(也可以称为SDK层)可以包括用于客户端和用于服务器的不同特征。在示例中,与SDK层中的客户端相关联的特征可以划分成2部分。第一部分可以是钱包SDK,并且第二部分可以是微件SDK。在示例中,钱包SDK 可以提供对钱包服务、特许API以及构建钱包容器应用或用户体验必需的组件的访问。在示例中,微件SDK可以促进生态系统合作伙伴构建它们的可以在钱包容器内操作的微件。在示例性且非限制性实施例中,SDK可以基本上促进客户端侧配置和用户体验。在示例中,SDK可以通过促进对于由客户端容器所展露的参数的可定制性来促进配置。这可以包括设备特定参数、变量(像PIN大小、退出确认、选择模块的包含物等)。在示例中,SDK可以通过促进跨手持机的差异化用户体验的开发来提供用户体验。

[0170] 在示例中,用于服务器的SDK可以包括至少一个库,其可以允许任何生态系统服务器与钱包通信、格式化对于微件的内容,以及向钱包应用展露服务。该库可以包括配置模块和接口模块。配置模块可以允许对于由服务器的移动使能层1304和服务层1308所展露的参数的可定制性。可以在属性文件和资源束中配置参数。接口模块可以提供开发来促进与各种后端系统的通信的连接,所述后端系统可以协作来履行完整的端对端服务。接口模块还可以包括由平台所展露的web服务以集成外围系统,像客户关怀、用户门户等。

[0171] 在示例中,设备制造者可以确定NFC功能性将被提供作为新设备上的新通信选项,以便支持公司的商业目标。在检测到新NFC功能性的可用性时,业务需求和设备功能性分配引擎1302可以复查设备制造者的要求并且向使能层1304分配设备功能性。使能层1304于是可以使NFC设备功能性对于向其客户提供该设备的服务提供者可用。服务提供者于是可以通过服务层1308在设备上使能NFC功能性,并且通过使用由个性化层1310提供的SDK将NFC图标添加到移动微件来使终端用户能够激活NFC功能性作为支付方法。

[0172] 根据示例性且非限制性实施例,本公开提供可以构建用于移动支付和移动商务的安全且鲁棒的生态系统的移动交易平台(MTP)。在示例中,MTP可以并入微件架构,其可以允许服务提供者构建它们自己的可以被下载并安装在移动钱包应用内的独立微件。在示例中,MTP可以向服务提供者提供综合软件开发套件(SDK)。SDK可以允许服务提供者快速构建

它们的用于所有MTP手持机的微件，而不必编写电话特定的代码。尽管移动钱包应用可以由生态系统操作者分布和推广，但是服务提供者可以通过微件来构建和提供它们自己的独特服务并且利用由生态系统操作者创建的分布信道。移动钱包应用可以向微件提供安全且隔离的运行环境。

[0173] 在示例中，MTP可以通过使用微件管理组件来管理一个或多个微件，所述微件管理组件可以管理MTP内的微件的用例、设计、架构、数据结构、生命周期、版本等。

[0174] MTP可以包括移动客户端以诸如使能用于快速移动应用开发的基础设施。移动客户端可以提供基于容器的途径来诸如支持多租户应用架构。在示例中，移动客户端运行时可以是用于运行移动钱包应用的容器。钱包应用可以是支配的和主要的应用，其可以提供整体用户体验和服务器作为至微件的入口点。在示例中，微件可以包括由第三方开发的服务群组，并且在移动客户端容器内运行，独立且隔离于钱包应用。移动客户端可以操控与应用执行、安全性、可靠性等相关的复杂性，并且从而可以允许开发者更多地集中于服务的独特功能。移动客户端可以使得开发者能够不担心大部分复杂性，包括设备特定的实现。在示例中，移动客户端容器可以构建在设备特定应用编程接口(API)的顶部并且可用于流行设备环境。设备独立API可以确保可以通过使用SDK开发的应用可以跨所有支持的MTP手持机而运行。这些API可以被设计为提供开发者创建动态用户体验可能需要的所有支持。在示例中，钱包应用和微件可以通过使用MTP SDK来构建。在示例中，钱包应用和微件在结构上(屏幕、Java脚本、&CSS样式)可以是相同的，除了钱包应用可以访问相对更广的特许API集合之外。当钱包应用可以首先被调用时，钱包应用可以取得控制，直到用户可以选择到特定微件(卡图像、菜单选项等)中的入口点为止。作为整体UI设计的一部分的钱包开发者可以确定对于微件的一个或多个入口点。在选择了微件的入口点时，微件可以被发动(在相同运行时应用内)并且钱包可以被挂起。在示例中，钱包可以停止执行。一旦完成微件执行，钱包就可以恢复，并且用户从中离开钱包的屏幕可以返回到显示器。

[0175] 根据示例性且非限制性实施例，微件开发者可以取决于可以由服务提供者提供的要求来开发微件并进行测试。服务提供者可以向MTP服务器提交开发的微件。此外，生态系统提供者可以证明和发布微件，使得该微件对于钱包用户可以是可访问的。在示例中，钱包用户可以发现并下载微件以访问由服务提供者提供的移动服务。在示例中，微件可以已经安装在钱包用户的移动电话中。钱包用户可以发现微件的更高版本，并且相应地可以用更新的版本来更新微件的现有版本。在示例中，钱包用户可能对使用已安装微件不感兴趣，并相应地，钱包用户可以终止并从移动设备移除(即，卸载)微件。

[0176] 在示例中，微件开发者可以被培训以使用SDK和理解服务来构建微件。另外，微件开发者可以具有可以由生态系统提供者所指定的指南，以诸如确保微件可以遵照指南。

[0177] 在示例中，服务提供者可以是发行或拥有服务产品的实体。服务可以包括用于移动支付的信用卡、电影票务服务、移动银行服务等。在示例中，服务提供者可以委托微件开发并且与生态系统提供者签订商业协定。

[0178] 在示例中，生态系统操作者可以是可以在地区/地理或商业域内设立移动支付和移动商务生态系统的实体。生态系统不一定是支付或商务生态系统。在示例中，生态系统可以是医疗保健或其它复杂商业域。

[0179] 在示例中，钱包用户可以是可能已经在他们的电话上下载并激活了移动应用(或

钱包,如果关于支付域的话)的消费者。

[0180] 根据示例性且非限制性实施例,本公开提供用于微件的多个用例。在示例中,用于微件的一个或多个用例可以包括开发微件用例,其中,开发者可以按照由服务提供者提供的规范来构建微件。在示例中,用于微件的一个或多个用例可以包括测试微件用例,其中,开发者可以通过使用虚设容器和可能的沙盒钱包应用二者来测试微件。在示例中,用于微件的一个或多个用例可以包括批准微件用例,其中,服务提供者内的商业发起人可以复查和批准微件。这样的用例可以不在MTP服务器或客户端上。

[0181] 在示例中,用于微件的一个或多个用例可以包括提交微件用例,其中,服务提供者可以将微件连同一组测试案例一起发送给生态系统操作者。微件可以安装在生态系统提供者的测试/UAT环境上。在示例中,用于微件的一个或多个用例可以包括验证微件用例,其中,生态系统操作者可以复查微件测试案例、测试微件、验证微件的所有功能性,以及对着所有定义的指南来检查微件。在示例中,用于微件的一个或多个用例可以包括批准微件用例,其中,生态系统操作者可以批准微件并准许微件被包括在钱包应用内。

[0182] 在示例中,用于微件的一个或多个用例可以包括拒绝微件用例,其中,生态系统操作者可以出于某种原因拒绝或否决微件。一旦问题被解决,就可以重复目前为止的整个过程,并且可以提交新微件。在示例中,用于微件的一个或多个用例可以包括发布微件用例,其中,生态系统操作者可以发布微件并将微件加载到MTP服务器,使得钱包用户可以下载所发布的微件。在示例中,用于微件的一个或多个用例可以包括挂起微件用例,其中,生态系统操作者可以由于某种问题而挂起已经发布的微件直到该问题可以得到纠正为止。在示例中,用于微件的一个或多个用例可以包括发现微件用例,其中,可以通过警报或者通过对可用微件的主动搜索来向钱包用户警报微件的可用性。在示例中,用于微件的一个或多个用例可以包括下载微件用例,其中,微件可以被供应到用户的MTP移动客户端应用,并且可以被安装和就绪以供使用。在示例中,用于微件的一个或多个用例可以包括升级微件用例,其中,钱包用户可以将他们的微件升级为来自移动钱包应用内的更新的版本。在示例中,用于微件的一个或多个用例可以包括移除微件用例,其中,用户可以决定微件可能不再被期望。钱包用户可以从钱包应用移除微件和所有相关联的数据存储。

[0183] 在示例中,微件可以包括多个服务,其可以向钱包用户提供有意义的、域特定的功能性,所述功能性可以增大可以由钱包用户使用的移动应用的能力。微件可以称为微件束或服务舱(service capsule)。在示例中,微件束可以包括微件简档数据、微件用户接口、微件商业逻辑以及微件认可。

[0184] 在示例中,微件简档数据可以包括关于微件、服务提供者、版本等的信息。在示例中,微件用户接口可以包括可以由钱包容器用来渲染微件的用户接口的屏幕、内容和样式。在示例中,微件商业逻辑可以包含可以封装微件的商业逻辑的脚本,所述微件的商业逻辑在微件可以加载到移动设备上时可以被执行。在示例中,微件认可可以包括访问控制列表,所述访问控制列表可以包括在运行在移动应用内时生态系统操作者可能已经提供给微件的认可。

[0185] 根据示例性且非限制性实施例,本公开提供可以分组成两个大阶段的对微件的管理。第一阶段可以包括微件开发,并且第二阶段可以包括微件使用。微件开发阶段可以包括逐渐使得微件就绪以供使用的所有步骤,并且微件使用可以包括与微件的使用及其生命周

期相关的所有步骤。

[0186] 根据示例性且非限制性实施例,本公开提供根据示例的如图14中所图示的开发微件的方法1400。在1402处,方法1400可以开始,并且在1404处,方法1400可以允许构建微件。在示例中,开发者可以使用由MTP提供的SDK来根据由服务提供者指定的要求构建微件。在1408处,方法1400可以测试微件。在示例中,系统可以对微件的Java脚本执行静态代码核实。在1410处,可以做出决定,以诸如完成微件开发。如果微件开发未完成,则方法1400可以移动到1404,其中,开发者可以对微件进一步工作。如果微件开发完成,则方法1400可以移动到1412,其中,服务提供者可以复查微件。如果在1414处确定服务提供者对微件不满意,则方法1400可以移动到1404,其中,开发者可以并入服务提供者的反馈来构建微件。

[0187] 在服务提供者满意时,在1418处,可以将微件提交到生态系统操作者。在示例中,服务提供者的雇员可以通过在线提交模式而将微件提交到生态系统操作者。在1420处,生态系统操作者可以核实微件,以诸如识别微件中的任何错误。在1422处,生态系统操作者可以确定微件的通过或失败。如果微件未通过生态系统操作者的要求,则在1424处,生态系统操作者可以拒绝微件,并且方法1400可以在1428处结束。

[0188] 如果微件已经满足生态系统操作者的要求,则在1430处,可以证明微件,并且在1432处,可以发布微件。此外,在1434处,可以对微件执行发烟测试(smoke test)。在1438处,可以确定如微件是否已通过了发烟测试。如果微件可能未通过发烟测试,则在1440处,可以发起故障检修,并且方法1400可以移动到1420以重新核实微件。否则,在1442处,生态系统操作者可以向公众开放微件,使得公众可以下载并使用微件。在1444处,方法1400可以结束。

[0189] 根据示例性且非限制性实施例,本公开提供根据如图15中所图示的示例的微件使用的方法1500。在1502处,方法1500可以开始并分支成三个不同步骤。在1504处,钱包用户可以浏览微件注册,以诸如识别一个或多个微件。在1508处,钱包用户可以选择需要的微件,并且在1522处,方法1500可以允许钱包用户下载微件。

[0190] 在示例中,在1510处,钱包用户可以接收对于可以在钱包用户的设备中安装的微件的更新通知。钱包用户可能期望下载微件的更新,并且相应地,在1522处,方法1500可以允许微件用户下载在MTP服务器处可以是可获得的微件的最新版本。在示例中,在1512处,服务提供者可以利用用于向终端用户提供一个或多个服务的MTP服务器来登记。在1514处,可以批准一个或多个服务,并且在1518处,生态系统操作者可以向钱包用户通知关于服务提供者的经批准的服务。在1520处,钱包用户可以读取通知,并且在1522处,方法1500可以允许钱包用户下载与服务提供者的通知的服务相关联的微件。

[0191] 在1524处,钱包用户可以安装微件,并且相应地,在1528处,可以向生态系统操作者通知关于由钱包用户进行的微件的安装或更新。在1530处,可以向服务提供者通知关于微件的安装。

[0192] 根据示例性且非限制性实施例,本公开提供用于向服务提供者通知关于已安装微件的移除的方法1500。在1532处,钱包用户可以使用可以安装在钱包用户的设备中的微件。在1534处,可以做出关于钱包用户是否对已安装微件的连续使用感兴趣的确定。如果用户可能想要在将来使用微件,则方法1500可以移动到1532,其中,用户可以继续使用该微件。否则,方法1500可以移动到1538,其中,可以从设备中移除该微件。在1540处,可以向服务器

通知关于微件的移除,并且在1542处,可以向服务提供者通知关于微件的移除。

[0193] 根据示例性且非限制性实施例,本公开描述了其中可以创建服务提供者的用例。服务提供者也可以称为微件提供者。如上所讨论的,微件提供者可能已经与生态系统操作者签订了商业关系,以诸如创建和推广他们的微件。在示例中,在可以在系统中创建微件之前,可以要求服务提供者实体在系统中更新。例如,生态系统操作者的雇员可以登录系统管理控制台,并且可以选择微件管理的选项。此外,所述雇员可以选择添加服务提供者的链接,填充与服务提供者相关联的对应细节,并创建服务提供者记录。在示例中,系统可以向服务提供者发送关于他们的登记细节连同他们的唯一标识符的电子邮件。

[0194] 根据示例性且非限制性实施例,本公开描述了用例提交微件,其中,微件可以存储在生态系统操作者的域内的MTP测试台/UAT系统上。在示例中,可能已经通过使用MTP SDK工具的正确版本开发和创建了微件。此外,可以由服务提供者对微件进行内部测试和批准以供提交。在示例中,MTP系统可以允许以两种模式提交微件:在线和离线。

[0195] 在离线提交微件的示例中,服务提供者的雇员可以将与微件相关联的微件束发送到生态系统的经授权雇员,该经授权雇员可以从MTP系统管理控制台中选择微件管理。此外,生态系统的雇员可以选择提交微件和上传微件束的链接。MTP系统可以验证微件束,并且系统可以创建微件记录并将微件的状态设置为已提交。因此,系统可以向服务提供者的雇员确认微件已经成功提交。

[0196] 在在线提交微件的示例中,服务提供者的雇员可以配置Eclipse插件工具以指向正确的MTP服务器。此外,服务提供者的雇员可以配置他们的唯一微件提供者ID并且选择“提交微件”选项。Eclipse工具可以创建微件提交请求以将微件上传到MTP服务器,MTP服务器可以验证微件束、创建微件记录并将微件的状态设置为已提交。MTP服务器可以返回微件已经成功提交的确认,并且可以向生态系统的雇员发送新微件已经提交的通知。

[0197] 根据示例性且非限制性实施例,本公开描述了用例验证微件,其中,可以成功测试微件。在示例中,微件已经提交到MTP并且可以就绪以供测试。生态系统的雇员(EOE)可以从MTP系统控制台中选择微件管理。此外,EOE可以选择用于微件列表的链接,该微件列表可以示出已提交状态中的所有微件。EOE可以选择要测试的微件,并且MTP可以提示确认,其利用可以执行的所有所要求核实的检查表。EOE可以选择测试选项,并且系统可以将微件的状态从已提交改变为正在测试。在示例中,系统可以对微件的Java脚本执行静态代码核实,并且可以确认静态代码核实已通过。系统可以显示核实结果,并且提示EOE对其进行复查和确认。EOE可以确认核实结果批准,并且可以按照生态系统指南来执行所有其它测试。

[0198] 根据示例性且非限制性实施例,本公开描述了用例批准微件,其中,可以批准和发布微件。EOE可以登录MTP系统控制台并在微件管理区段中选择用于批准微件的链接。系统可以示出处于正在测试状态中的所有微件,并从而,EOE可以选择微件以批准。因此,系统可以提示确认,其利用要执行的所有所要求核实的检查表,并且EOE可以确认并检查所有已经执行的测试。此外,EOE可以输入任何评价/备注,并且选择批准选项。之后,系统可以将微件的状态改变为已批准,并且可以确认微件已被批准。

[0199] 根据示例性且非限制性实施例,本公开描述了用例发布微件,其中,微件可以被发布并且就绪以被下载到用户的钱包应用。EOE可以登录MTP系统控制台,并且在微件管理区段中选择用于发布微件的链接。系统可以示出处于已批准状态中的所有微件,并且EOE可以

选择要发布的微件。EOE可以输入任何评价/备注并且选择发布选项。系统可以提示以供确认,并且EOE可以确认可以发布微件。因此,系统可以将微件的状态改变为已发布,并且生成用于微件的签名。在示例中,系统可以创建要安全存储在SE中的钱包上的微件束的散列,并且用HMAC来对微件束进行签名并具有与钱包共享的密钥。在示例中,系统可以用RSA密钥对微件束进行签名,并且在钱包内包括证书。之后,系统可以确认微件已被发布。

[0200] 根据示例性且非限制性实施例,本公开描述了用例挂起微件,其中,微件状态可以转变为已挂起,并且其不再可以被主动下载。在示例中,EOE可以登录MTP系统管理控制台,并且在微件管理区段中选择用于挂起微件的链接。系统可以示出处于已发布状态中的所有微件,并且EOE可以选择微件以将该微件挂起。EOE可以输入任何评价/备注并选择挂起发布。此外,系统可以提示以供确认,并且EOE可以确认微件的挂起。因此,系统可以将微件的状态改变为已挂起,并且可以确认微件已经挂起。在示例中,系统可以向服务提供者生成微件已经挂起的电子邮件通知。

[0201] 图16图示了根据示例的用于安装微件的交易流程图。如图16中所示,客户端1602可以包括钱包1604和钱包运行时1608。服务器1610的一个或多个组件可以包括移动服务器1612、个性化模块1614以及企业服务总线(ESB) 1618。

[0202] 在示例中,在1620处,服务器1608可以使用ESB 1618向个性化模块1614发行软卡、服务提供者ID和产品ID。在1622处,可以向移动服务器1612发送请求,诸如得到微件简档、诸如提供者ID、产品ID之类的标识、平台、状态和SDK版本。在1624处,对象被推向钱包运行时1608。在1628处,个性化模块1614可以向移动服务器1612传送请求以创建微件实例,其可以包括钱包ID、提供者ID和小程序ID。在1630处,可以确定对象是平台对象。在1632处,可以操控和处理平台对象。在1634处,钱包运行时1608可以传送消费对象JS的请求。在1638处,钱包1604可以以用于下载对象JS的对象做出响应。

[0203] 在1640处,钱包运行时1608可以向移动服务器1612传送下载微件的请求。在1642处,移动服务器1612可以准备微件响应并将微件状态标记为SENT_FOR_DOWNLOAD(发送_用于_下载)。在1644处,移动服务器1612可以向钱包运行时1608发送微件二进制。在1648处,钱包运行时1608可以安装微件,并且相应地,在1650处,钱包运行时1608可以向钱包1604传达微件安装完成。在1652处,钱包1604可以向钱包运行时1608发送应答,钱包运行时1608进而在1654处可以向移动服务器1612应答。在1658处,移动服务器1612可以将微件状态标记为已安装。在1660处,移动服务器1612可以此外向个性化模块1614传送应答,个性化模块1614进而在1662处可以执行商业流。在1664处,个性化模块1614可以经由ESB 1618通知卡发行者。另外,在1668处,钱包运行时1608可以反过来对钱包1604的应答进行应答。在1670处,钱包1604可以发送确认,并且在1672处,钱包运行时1608可以清理可靠性队列。

[0204] 根据示例性且非限制性实施例,本公开描述了器件和钱包的关联。在示例中,平台(即,MTP)可以得到诸如用以在平台中推送器件(例如,软卡)之类的指令。可以使用和/或发布各种API,以诸如将发行者系统与MTP进行集成。MTP可以基于标识参数来从主记录得到服务产品。在示例中,标识参数可以包括提供者ID、服务产品的类型、网络提供者类型以及互相关身份(例如,移动号码)等。平台可以通过使用互相关身份来取出钱包帐户信息。平台可以创建可以与钱包帐户相关联的器件(即,服务帐户参考)记录。平台可以将器件记录状态标记为已注册,其可以由发行者系统来更新。此外,可以通过使用诸如WAITING_FOR_

ACTIVATION(等待_激活)、激活(ACTIVE)、关闭(CLOSED)等之类的状态来控制其生命周期。平台可以通过使用推送通知(PUSH)或背负信道(piggyback channel)触发钱包来递送器件。

[0205] 图17图示了描绘MTP系统中微件的生命周期的示例状态图。在1702处,可以利用MTP来提交微件。在示例中,EOE可以利用MTP来提交微件。在另一示例中,服务提供者的雇员可以使用在线提交特征来利用MTP提交微件。如图17中所示,在1704处,当状态为已提交(SUBMITTED)时,可以提交微件任意次数。这可以允许开发者在测试可以开始之前更新微件。在示例中,当微件处于不同于已提交状态的状态中时,不可以重新提交微件。

[0206] 在1708处,微件状态可以更新为正在测试(TESTING)。在该状态期间,系统可以对微件执行多个测试(例如,静态代码核实)。在该状态处,取决于测试结果,系统可以将微件的状态改变为已批准(APPROVED)或已拒绝(REJECTED)。在1710处,微件的已拒绝状态可以不允许开发者更新已拒绝的微件。换言之,一旦系统可以拒绝微件,就可以提交(具有相同微件ID&版本号的)新微件束,并且可以重复该过程。结果,可以创建微件表中的新记录。此外,如果具有相同微件ID和版本号的微件已经存在于除已提交或已拒绝之外的任何状态中,则微件不可以进入已提交状态。在1712处,微件状态可以更新为已批准,描绘了微件可能已经清理了正在测试的阶段。在1714处,已批准的微件可以被发布,并且对于下载可以是可获得的。此外,可以可能的是,已发布的微件可能需要更新或者系统可能需要挂起已发布的微件。因此,在1718处,微件可以被挂起,描绘了微件对于下载不可以是可获得的。在示例中,只有当所有之前的版本号处于已批准、已发布、已拒绝或已挂起状态中,具有数学上较大版本号的微件才可以是已提交的。在示例中,系统可以用日志记录微件的状态转变,连同时间戳、动作者的唯一标识以及已经由动作者输入的评价的审查跟踪(audit trail)。

[0207] 系统可以被配置为包括用于服务帐户管理的各种API。例如,系统可以被配置为包括创建相关API,其中,所述API可以创建服务产品记录、服务提供者记录、服务帐户参考记录等。在示例中,系统可以被配置为包括更新相关API,其中,所述API可以更新服务帐户参考记录、服务帐户参考状态(以诸如控制服务帐户参考生命周期)等。在示例中,系统可以被配置为包括列表相关API,其中,所述API可以对系统中可用的所有已注册的服务产品、系统中可用的所有已注册的服务提供者等进行列表。在示例中,系统可以被配置为包括检索相关API,其中,所述API可以检索基于钱包id过滤准则的服务帐户参考记录、基于微件ID过滤准则的服务帐户参考记录、基于产品ID过滤准则的服务帐户参考记录、基于状态过滤准则的服务帐户参考记录、基于服务帐户参考号的服务帐户参考记录、基于服务产品提供者id过滤准则的服务帐户参考记录、基于微件实例id过滤准则的服务帐户参考记录、基于服务产品id过滤准则的服务产品、通过提供者id过滤准则的服务产品提供者记录,等等。在示例中,状态值可以是已注册(REGISTERED)、WAITING_FOR_ACTIVATION(等待_激活)以及激活(ACTIVE)。所述状态值可以被扩展以用于进行定制,或者用以引入更细粒度水平的服务帐户参考状态。在示例中,服务帐户参考号可以由发行者系统共享的唯一标识符,其可以充当钱包平台和发行者系统内的互相关id。在示例中,系统可以被配置为包括更新相关API,其中,所述API可以更新服务产品记录、服务产品提供者记录等。

[0208] 根据示例性且非限制性实施例,本公开描述了各种数据映射的细节。在示例中,系统可以包括用于与服务提供者相关联的数据的各种数据字段。ID可以是服务产品提供者的

唯一系统标识符,并且可以自动生成。名称字段可以用于显示服务提供者的名称,并且当创建服务提供者的入口时,可以输入与服务提供者相关联的数据。类型字段可以标识服务提供者的服务类型,并且种类字段可以定义可以由服务提供者提供的服务产品的种类。电子邮件字段可以包括服务提供者的电子邮件地址。此外,系统可以包括一个或多个属性,其可以用键值对(例如,联系人号码)的形式存储并且可以用于向服务提供者引入任何定制属性。

[0209] 在示例中,系统可以包括用于与服务产品相关联的数据的各种数据字段。ID可以是服务产品的唯一系统标识符,并且ID可以由系统自动生成。如上文所讨论的,提供者ID可以是服务产品提供者的唯一系统标识符。产品ID可以是产品的唯一名称(例如,银行金卡、高端信用卡等),并且系统可以包括与服务产品相关联的应用(例如,银行业务)的应用ID。类型字段可以标识服务产品的类型(例如,信用卡),并且种类字段可以标识服务产品的种类(例如,支付)。名称字段可以标识服务产品的显示名称,并且描述可以标识服务产品的描述。此外,系统可以包括以键值对的形式存储的属性,并且属性可以用于向服务产品实体引入任何定制属性。

[0210] 在示例中,系统可以包括用于与器件(服务帐户参考)相关联的数据的各种数据字段。ID可以标识器件的唯一系统标识符,并且系统可以自动生成ID。钱包ID可以标识钱包的唯一标识符。发行者ID可以标识发行者的唯一标识符,并且产品ID可以标识服务产品的唯一标识符。微件实例ID可以标识微件实例的唯一标识符,并且帐户参考号可以标识器件在发行者端的唯一标识符。状态可以标识器件的状态(例如,已创建、已激活、已挂起等)。类似地,系统可以包括钱包平台状态。供应时间戳可以标识器件的供应日期(时间戳),并且下载时间戳可以标识器件的下载日期(时间戳)。激活时间戳可以标识器件的激活日期(时间戳),并且中断时间戳可以标识器件的中断日期(时间戳)。最后活动时间戳可以标识器件的最后活动日期(时间戳),并且最后状态改变时间戳可以标识最后状态改变的时间戳。此外,系统可以包括昵称字段(诸如用以标识用户提供的器件名称),其它字段(诸如OTA TX数据、邻近TX数据等)。

[0211] 有效期(expiry date)可以标识器件的有效期,并且到期日可以标识器件的到期日。系统可以包括额外属性,其可以用于容纳任何附加信息。这些属性可以不由平台使用,并且可以主要用于微件。此外,徽标图像可以标识可以用于在钱包应用上显示软卡的图像。该图像按照发行者的品牌化定义可以是联合品牌的。卡图像可以标识可以用于在钱包应用上显示软卡的图像。该图像按照发行者的品牌化定义可以是联合品牌。产品类型可以标识在设置期间在钱包平台处配置的服务产品的唯一标识符。AID(例如,HEXSTRING(十六进制字符串))可以标识小程序ID,其可以是在个性化期间安装在安全元件上的小程序的唯一标识符。OTA认可(OTA Permission)可以标识可以由发行者管理来控制OTA服务认可的空中服务认可标志,并且邻近认可(Proximity Permission)字段可以标识可以由发行者管理来控制邻近交易或服务的邻近服务认可标志。软卡品牌ID可以包括品牌化信息ID,并且网络操作者ID可以标识移动网络操作者。

[0212] 在示例中,系统可以包括用于与微件提供者相关联的数据的各种数据字段。ID可以标识微件提供者的唯一系统标识符,并且系统可以自动生成ID。名称文件可以标识微件提供者的显示名称,并且描述可以标识微件提供者的描述。电子邮件可以标识微件提供者

的电子邮件地址,并且状态可以指示微件提供者的状态。创建日期时间戳可以标识微件提供者的创建日期(时间戳),并且批准日期时间戳可以标识当微件提供者已被批准时的批准日期(时间戳)。

[0213] 在示例中,系统可以包括用于与微件提供者相关联的数据的各种数据字段。ID可以标识微件简档的唯一系统标识符,并且系统可以自动生成ID。应用ID可以标识微件应用ID,并且应用名称字段可以标识微件可以与其相关联的应用名称。提供者ID可以标识微件提供者的唯一标识符,并且提供者名称可以标识微件提供者的名称。最小运行时版本可以标识最小所需钱包平台版本,并且版本可以标识微件的版本。状态字段可以标识微件简档的状态(例如,已创建、已发布等)。

[0214] 在示例中,系统可以包括用于与微件实例相关联的数据的各种数据字段。ID可以标识微件实例的唯一系统标识符,并且系统可以自动生成ID。微件束ID可以将区外(foreign)键标识为wsc_widget_bundle。微件简档ID可以标识微件的唯一标识符,并且系统可以定义区外键:微件简档的ID。钱包ID可以标识钱包的唯一标识符。供应时间戳可以标识微件供应日期(以时间戳),并且安装时间戳可以标识微件安装日期(以时间戳)。激活时间戳是可选字段,并且移除时间戳可以标识微件实例移除日期。状态字段可以标识微件实例的状态。

[0215] 在示例中,系统可以包括用于与微件认可相关联的数据的各种数据字段。ID可以标识微件实例的唯一系统标识符,并且系统可以自动生成ID。微件简档ID可以标识对微件简档ID的参考,并且微件提供者ID可以标识对微件提供者ID的参考。

[0216] 在示例中,系统可以包括用于与微件束相关联的数据的各种数据字段。ID可以标识微件实例的唯一系统标识符,并且系统可以自动生成该ID。微件束可以标识微件文件(.wgt)的二进制数据,并且设备软件类可以标识与微件束相关联的设备软件类。微件简档ID可以标识对微件简档ID的参考,并且堤岸(bund)散列可以标识微件束文件的散列。

[0217] 在一些示例性且非限制性实施例中,本文描述的多域生态系统安全个性化交易的方法和系统包括可以支持安装和管理多个微件的移动钱包(也称为钱包)容器。这些微件中的每一个可以由不同发行者和服务提供者开发和拥有。钱包可以被配置为履行各种安全性要求。这里描述的示例性关键安全性环境中的一些包括微件完整性、微件访问控制和微件隔离。这些如以下所述:

[0218] 在示例中,可以通过使用像钱包服务器这样的受保护的供应服务器来将微件安全地供应到钱包运行时。可以将微件安装在手持机上。当在手持机上时,对微件的任何篡改可以被自动检测,并且可以采取必要行动。

[0219] 在示例中,对发行者安全性域小程序的访问可以专为发行者微件所独有。系统可以防止任何发行者微件访问另一发行者的安全性域。系统可以防止微件访问可能未被明确准予给定微件的系统动作。系统可以防止任何发行者微件访问不同于所明确准予给定微件的URL/域。

[0220] 在示例中,任何发行者微件可以具有对发行者的 workflow 代码的排他访问。系统可以被配置以使得任何发行者微件不可以访问任何其它发行者的 workflow 代码。系统可以被配置以使得任何发行者微件可以具有对发行者的用户接口(UI)代码的排他访问。系统可以被配置以使得任何发行者微件不可以访问任何其它发行者的UI代码。系统可以被配置以使得

任何发行者微件不能够访问任何其它微件的持久性数据。系统可以被配置以使得任何发行者微件不可以访问任何其它微件的静态资源(图像、文件等)。

[0221] 在一些示例性且非限制性实施例中,本文描述的多域生态系统安全个性化交易的方法和系统包括:访问控制机制(ACM)可以被配置为对着给定“策略”来管理“资源”。在一些示例性且非限制性实施例中,本文描述的多域生态系统安全个性化交易的方法和系统包括:被管理的少数示例性资源可以包括微件工作流代码、微件数据、微件UI代码(屏幕)、安全元件、服务器通信。在示例中,为了确定“策略”,本公开可以具有访问控制器,其可以将给定微件的“微件描述符”用作策略文件。微件描述符可以是简单的键值对结构,其由微件开发者创建(以描述必要资源),并且由移动交易平台(MTP)服务器基于钱包操作者的处理来签名。该访问控制机制可以牵涉在对着给定策略来管理资源的整个过程中的微件描述符生命周期和移动客户端访问控制。过程的这两个方面可以在下面进行描述。

[0222] 图18图示了从开发到执行的微件生命周期。在一些示例性且非限制性实施例中,微件生命周期(由1800表示)可以具有在发行者与JVL的子系统之间具有职责划分的阶段。所述阶段可以包括微件开发、微件核实和批准、微件递送、微件安装以及微件执行。微件生命周期的微件开发阶段可以包括工具套件1802。在示例中,工具套件1802可以基于Microsoft visio®。移动交易平台工具(MTP)1804可以支持工具套件1802以促进微件开发。微件开发之后可以是微件包生成阶段。在微件包生成期间,可以由MTP工具1804形成微件束1808。微件束1808可以包括微件描述符、屏幕支持文件和主题支持文件(这些可以在下文进行更详细的解释)。可以由MTP工具1804将微件束1808发送到移动交易平台(MTP)1810以用于静态核实、策略批准或策略供应。在示例中,可以通过使用可信服务管理器(TSM)1814来提供策略供应和微件供应简档。在示例中,如作为稍后的章节所解释的,可以通过使用访问控制列表(ACL)来提供微件供应。MTP 1810可以被配置用于在核实之后发布微件束1808。在示例中,微件供应和发布可以被同步并在MTP 1810和TSM 1814上同时发生。MTP 1810和TSM 1814可以在核实和发布之后将微件束1808发送到移动客户端1818。移动客户端1818可以被配置为包括微件束1808、用于平台服务的块、用于数据服务的块、用于通信服务的块以及用于安全元件的块。移动客户端1818可以定义用于微件束1808的运行时覆盖区。稍后可以通过图21来解释移动客户端。

[0223] 在一些示例性且非限制性实施例中,微件生命周期中的第一阶段可以是微件开发。在示例中,移动交易平台(MTP)可以支持基于Microsoft Visio的微件开发工具套件来使微件开发自动化。微件开发可以在发行者域中发生。微件可以由多个微件工件(artifact)构成。在示例中,微件可以由screen.xml文件、content.xml文件、theme.xml文件、多个脚本文件、多个图像以及微件描述符构成。在示例中,微件开发工具套件可以生成像屏幕、内容等的微件工件,连同微件描述符。微件描述符可以捕获开发者对于像动作/URL/小程序等的不同资源的微件访问要求(或请求)。

[0224] 在一些示例性且非限制性实施例中,微件生命周期中的下一阶段可以是微件核实和批准。在示例中,微件批准步骤可以涉及微件的验证。在示例中,微件核实可以在钱包平台(例如,JVL钱包平台-证明工具)处发生。微件批准步骤此外可以涉及微件的批准或供应。本发明提供了用于微件的静态分析的一组工具,其可以帮助整个批准过程。在示例中,微件批准的技术过程可以包括各种步骤。第一步骤可以是创建对于给定微件的静态分析报告,

其指示任何警告/复制/冲突。在示例中,这些指示可以涉及应用协议数据单元冲突(APDU)、统一资源定位符(URL)冲突、存在太多外部资源、使用了受限/受控的应用编程接口(API)。下一步骤可以是捕获对微件的手动批准,其记录批准条件和所接受/忽略的警告。下一步骤可以是创建微件供应简档。微件供应简档可以包括ACL和微件二进制的散列。下一步骤可以是创建微件包以通过使用钱包信道来下载。

[0225] 在一些示例性且非限制性实施例中,微件生命周期中的下一阶段可以是微件递送和安装。在示例中,微件一旦其被证明就可以就绪以供递送并且可以对于从钱包平台下载是可获得的。在一些示例性实施例中,可以由于各种事件而触发微件下载和安装。所述事件可以包括由发行者的新卡供应事件。

[0226] 在一些示例性且非限制性实施例中,移动客户端的微件管理者可以在安装微件的时候执行各种步骤。第一步骤可以是在已经下载了微件束之后核实微件束的完整性。在示例中,可以通过使用安全元件服务来进行核实。在微件束的完整性得到核实的情况下,可以将该微件束添加到移动客户端。在微件束的完整性未得到核实的情况下,将示出错误消息,并且该微件束将不被添加到移动客户端。

[0227] 在一些示例性且非限制性实施例中,微件生命周期中的下一阶段可以是微件执行。可以由钱包管理器为微件的每次运行确定微件的完整性和访问简档。微件执行和完整性检查可以包括加载时间完整性检查和运行时访问控制。加载时间完整性检查可以检查微件对于执行后成功安装是否可以就绪。每次加载微件以供执行时可以核实散列。可以要求该验证以确保微件或其数据在钱包或微件的空闲时间期间未被篡改。运行时访问控制可以检查微件是否一旦它通过在其加载时候的散列核实步骤就可以开始其功能。微件访问控制器可以确保微件尝试访问特定资源可以是按照恰当的授权,即隔离规则。

[0228] 移动客户端访问控制(也称为访问控制)——当微件描述符生命周期描述“建立策略”的过程时,移动客户端访问控制机制确保“策略的施行”。本章节描述了访问控制机制的高层级概观。

[0229] 图19图示了访问控制机制的高层级视图。如图19中所图示,可以通过经由访问控制器1902来控制资源访问。访问控制器1902可以基于微件描述符来确定访问权限。访问控制器1902可以使例如屏幕或动作或小程序等的特定资源有益于微件。在示例性且非限制性实施例中,访问控制器1902可以包括一组设计考虑事项。在示例中,访问控制器1902可能需要用于数据存储的系统1904。数据存储装置可以被配置为存储微件二进制。在示例中,微件简档供应和ACL信息可以安全地存储在安全元件1908中。安全元件1908可以与访问控制器1902进行通信。微件简档供应和ACL信息可以包括钱包安全性域1910、钱包小程序1912、发行者安全性域1914以及发行者小程序1918。访问控制器1902可以与微件策略文件1920进行通信。

[0230] 访问控制器1902可以与近场通信(NFC)芯片管理器1922、资源管理器1924以及通信管理器1928进行通信。NFC芯片管理器1922、资源管理器1924和通信管理器1928可以与脚本执行平台1930进行通信,脚本执行平台1930可以与屏幕管理器1932进行通信。如图19中所图示,微件可能没有对任何原生资源的API层级访问,并且所有资源使用可能必须由访问控制器1902来促进。例如,用于数据存储的系统1904可能必须与访问控制器1902通信,其可以促进NFC芯片管理器1922、资源管理器1924和通信管理器1928对于数据存储系统1904的

访问。在示例中,可以允许屏幕管理器1922在特定时间点仅执行一个微件。在示例性且非限制性实施例中,对于整个系统,可以仅存在一个访问控制器1902。

[0231] 在示例中,可以要求微件在每次其可以被加载或重载时使其散列被核实。在示例中,仅一个微件可以被允许执行。

[0232] 图20图示了用于相对于访问控制器而加载和执行微件的方法2000。

[0233] 方法2000可以在步骤2002处要求移动客户端加载钱包主页。移动客户端可以与用户在相接口。在钱包主页可以加载到移动客户端上之后,用户可以从钱包主页选择微件。移动客户端可以被配置为在方法2000的步骤2004处打开由用户选择的微件。移动客户端可以与应用数据库进行通信。移动客户端可以被配置用于在步骤2008处加载从应用数据库所选的微件的微件束。移动客户端可以与安全元件进行通信。在步骤2010处,安全元件可以通过执行散列核实来核实微件束的完整性。如上文所提及的,每当可以加载微件时,可以核实散列。在示例中,微件束可以包含在钱包小程序中用于具有核实。可以在微件供应的时候存储散列。散列核实对于方法2000可以是至关重要的,并且在散列核实失败的情况下,可以停止微件执行。在散列核实成功的情况下,移动客户端可以从安全元件中检索用于所选微件的微件描述符。在方法2000的步骤2012处,可以将微件描述符存储在MTP的主存储器中。在步骤2014处,在可以检索到微件描述符之后,屏幕管理器可以将下一屏幕加载到移动客户端上。在步骤2018处,移动客户端可以请求平台服务执行。在示例中,可以通过指定各种参数来请求他服务。平台服务对于所选微件可以是排他的(通过图21来解释平台服务)。在步骤2020处,移动客户端可以核实微件描述符,以使得确保微件可以具有对访问所请求的平台服务的特许。在方法2000的步骤2022处,在所选微件可以具有对访问所选平台服务的特许的情况下,移动客户端可以执行所请求的平台服务。方法2000可以要求步骤2020的微件描述符核实以用于进一步执行微件。例如,如果可能发现微件描述符不可以访问所选平台服务,则移动客户端可以终止该方法。在方法2000的步骤2024处,移动客户端可以向用户传送微件的执行,并且移动客户端可以提示用户在执行之后退出微件。在步骤2028处,移动客户端可以在执行后销毁微件。如果他用户可能想要执行另一微件,则移动客户端可以被配置为加载另一钱包主页。

[0234] 图21图示了基于微件访问控制策略的微件运行时覆盖区2100。每个微件可以基于其访问控制策略来在运行时创建逻辑覆盖区。访问控制策略可以在微件供应简档中定义。每个逻辑覆盖区可以包含UI工作流资源2102、动作/服务资源2104、数据资源2108、在线资源或通信资源2110以及安全元件资源2112。如由图21所图示的,可以在本文中描述微件运行时覆盖区2100的边界。

[0235] 每个微件可以具有其自己的屏幕2114和内容文件。微件A不可以使用来自微件B的内容文件,并且反之亦然。微件运行时覆盖区2100将会使用可以对于所有微件是公共的原生平台2118。每个微件可以具有可以仅由特定微件使用的一组特许服务2120。例如,微件A可以仅使用来自特许服务2120的微件A特许服务2120A,并且微件B可以仅使用来自特许服务2120的微件B特许服务2120B。微件运行时覆盖区2100具有平台服务块2122,其可以是移动客户端的一部分,并且因此可以由微件A或微件B或任何其它微件中的任何一个使用。任何微件都可以访问公共数据2124。公共数据默认存储在微件运行时覆盖区2100中。在示例中,微件可以定义其自己的数据存储,如果被授权这样做的话。例如,微件A可以定义数据源

2128A,并且微件B可以定义数据存储2128B。

[0236] 移动客户端可以具有公共URL平台2130。默认情况下,例如微件A或微件B的任何微件都可以访问来自公共URL平台2130的数据。在示例中,微件A和微件B中的每一个可以定义它们自己的通信端点2132A和2132B。通信端点可以是域名。在该示例中,微件A可以使用通信端点2132A,并且微件B可以使用通信端点2132B。

[0237] 微件中的任何一个可以没有对任何SE小程序的默认访问。可以在微件描述符中明确定义针对给定微件可以允许的每个小程序访问。基于由服务器的签名所准予的认可,一个或多个微件可以访问相同SE小程序。

[0238] 详述了微件隔离要求的设计。在一些示例性且非限制性实施例,本文描述的多域生态系统安全个性化交易的方法和系统包括用于访问控制的策略文件的整个生命周期。各种阶段描述了重要文件/数据结构及它们的变换/处理,其最终引起移动客户端容器处的访问控制实现。所述阶段可以包括开发阶段、供应阶段、微件发动阶段以及微件执行阶段。可以在本文中描述这些阶段。

[0239] 开发阶段可以包括微件描述符文件。微件描述符文件可以由开发者(例如,发行者)提供。微件描述符文件可以从开发者视角描述一组资源要求。在示例中,在开发阶段期间,微件连同微件描述符文件一起可以被提交用于微件批准过程。在示例性实施例中,可以在微件批准过程期间证明资源要求是合理的。在微件已经被批准之后,可以由供应管理机构(例如,JVL)对微件签名。

[0240] 供应阶段可以包括微件供应简档。微件供应简档可以由供应管理机构创建,作为批准过程的一部分。微件供应简档可以是具有一些附加信息的微件描述符文件的衍生。在示例中,所述附加信息可以包括用户ID、微件散列等。可以通过使用可信服务管理器(TSM)来提供微件供应简档。可以通过使用钱包认证/伴随小程序来将微件供应简档存储在安全元件(SE)内部。SE可以向钱包提供服务以接受用户ID和微件散列,并返回核实状态以及ACL。

[0241] 微件发动阶段可以包括至少一个微件访问记录。在示例中,微件发动阶段可以包括多于一个微件访问记录。可以通过微件管理器在钱包的主存储器内部创建和维持微件访问记录。微件访问记录可以是简单的记录结构,其中可以存储资源认可。当发动微件时,微件管理器可以联系SE以读取ACL,并且微件管理器在主存储器中装载微件访问记录。

[0242] 微件执行阶段可以包括微件访问上下文对象。微件访问上下文对象可以是运行时对象,其可以提供用以检查对于微件执行的认可的简单方法。微件访问记录可以用于填充微件访问上下文对象。微件访问上下文对象可以在内部维护认可的简单映射(键值对)。微件访问上下文对象可以由所有访问知晓(access aware)资源管理器用于检查给定微件的认可。资源管理器可以在内部决定是否需要对策略来检查给定资源。

[0243] 在一些示例性且非限制性实施例,微件描述符可以是中心位置,其中可以定义对于多个资源的所有访问权限。在示例中,所述多个资源可以包括动作、屏幕、至少一个URL和SE/小程序。在示例性实施例中,微件的构造可能要求有益于不同的资源,像动作、小程序、屏幕等。在示例性但非限制性实施例中,动作可以包括移动客户端平台可以提供4种不同类型的动作,即,系统动作、核心/基础设施动作、钱包动作以及任何其它发行者特定的定制动作。在示例中,动作可以是移动客户端平台的一部分,并由此跨微件被共享。在示例中,

任何微件可以访问核心和钱包动作。在示例中,在默认情况下,可以不允许微件访问任何系统动作。微件可能需要在描述符中指定其所需的所有系统动作。在示例中,微件可以指定任何微件特定的动作,其可以是意欲仅特定地用于该微件的动作。在示例性但非限制性实施例中,每个微件可以被要求具有单独的屏幕和内容文件集合,其不可以重用来自任何其它微件的屏幕和内容资源。在示例性但非限制性实施例中,可以准许微件做出至多个URL的连接。在示例性但非限制性实施例中,微件可以与多个小程序相接口。

[0244] 微件批准过程-图22图示了微件批准过程。

[0245] 如图22中所图示的微件批准过程可以涉及用户2202、微件证明管理器2204、微件贮存库管理器2208、静态核实实用程序2210以及二进制包生成器2212。用户2202可以从对于用户可用的各种微件束中选择微件束2214。在示例中,微件束2214可以包含application.xml文件、content.xml文件、theme.xml文件以及微件描述符(这些文件可以与上文描述的相同)。微件束2214可以由用户2202发送到微件证明管理器2204。微件证明管理器2204也可以是微件批准管理器。微件证明管理器2204可以是驱动批准过程的主控制器类。微件证明管理器2204可以将微件束2214发送到微件贮存库管理器2208,微件贮存库管理器2208可以管理关于所有已证明和未证明微件的细节与恰当时间戳细节。微件贮存库管理器2208可以具有对微件贮存库2218的访问。微件贮存库2218可以包含所有已证明和未证明微件与恰当时间戳细节。该信息可以帮助审查跟踪和静态核实。微件证明管理器2204可以将微件束2214发送到静态核实实用程序2210。静态核实实用程序2210可以对着静态规则来验证微件束2214。例如,如果客户端可能已经宣告client_Check_CardStatus(客户端_检查_卡状态)作为其定制动作之一,则可以不允许该客户端自身以外的任何其它发行者使用该特定动作。静态核实实用程序2210可以针对对可能由其它微件拥有的资产的任何意外/不正确引用而检查微件贮存库2218中的微件束2214。静态核实实用程序2210可以自动化访问核实过程的一部分,但是仍然可以要求手动核实。微件证明管理器2204可以从静态核实实用程序2210接收对着静态规则所核实的微件束2214。微件证明管理器2204可以将微件束2214发送到二进制包生成器2212。二进制包生成器2212可以生成与微件束2214对应的最终二进制包。二进制包可以就绪以供空中下载和递送。二进制包生成器2212可以将二进制微件文件2220发送到用户2202。

[0246] 微件环境方面-这里描述对于钱包软件的少数示例性但非限制性环境假设和依赖性。环境假设和依赖性可以包括安全通信、安全主存储器、安全应用环境、可靠API、SE访问管理、受保护数据库以及可靠匆促注册(rush registry)。在示例中,钱包软件可以假设底层平台和API提供用于安全通信的可靠和安全的HTTP与HTTPS连接。原生平台可以管理用于安全套接层(SSL)核实的根证书存储。在示例中,钱包软件可以假设由原生OS分配给钱包软件的主存储器可以受保护以免受其它应用(app)影响,并且可以安全地持有对于过渡范围的敏感数据元素。钱包软件可以假设钱包二进制可以由应用环境安全地存储和维护在电话上以提供安全的应用环境。通过使用可信内容证书的环境来核实app签名。该环境还可以在下载到电话上的所有app上强加严格的签名和访问控制规则。钱包软件可以假设所有Java或类似API可以受底层环境保护,并且对于处理用于可靠API的敏感数据可以是可信的。而且,所述API可以是受环境访问控制的。钱包软件可以假设对安全元件的访问可以由环境基础设施(例如,JSR 177)管理,并且对各种安全元件服务的访问可以是特许的。可以通过基

于app签名的环境来实现特许管理。钱包软件可以假设该环境可以将对持久性数据的访问限制于仅拥有者应用,并且所述应用不可以访问或修改彼此的数据。钱包软件可以假设该环境可以提供可靠的应用推送注册,其中对于钱包app的事件被可靠地传递给钱包(而没有讹误或入侵)。

[0247] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令可以使得所述一个或多个处理器实行以下步骤,所述步骤包括经由移动设备上的钱包容器来配置一个或多个微件模块以供执行。所述一个或多个微件模块可以包括服务提供者的服务群组。在示例中,钱包容器可以与用于提供安全个性化交易的多层平台的使能层协作地操作来为一个或多个微件模块提供对服务提供者的工作流的排他访问。在示例中,钱包容器可以解译在移动设备上操作的运行时环境中的微件模块以提供排他访问。在示例中,服务提供者可以是微件发行者。在示例中,可以向由微件发行者发行的微件模块中的一个或多个提供对微件发行者的工作流的排他访问。在示例中,钱包容器可以与用于提供安全个性化交易的多层平台的使能层协作地操作来提供排他访问。在示例中,可以向由微件发行者发行的微件模块中的一个或多个提供对微件发行者的用户接口的排他访问。在示例中,钱包容器可以与用于提供安全个性化交易的多层平台的使能层协作地操作来提供排他访问。在示例中,可以防止由微件发行者发行的微件模块中的一个或多个访问另一微件发行者的工作流。在示例中,钱包容器可以与用于提供安全个性化交易的多层平台的使能层协作地操作来防止访问另一微件发行者的工作流。在示例中,可以防止由微件发行者发行的微件模块中的一个或多个访问另一微件发行者的用户接口。在示例中,钱包容器可以与用于提供安全个性化交易的多层平台的使能层协作地操作来防止访问另一微件发行者的工作流。

[0248] 用于安全个性化交易的多域生态系统可以包括各种组件,包括服务器、客户端及其它类型的组件。客户端组件可以包括可以在本文或别处描述的各种软件程序、应用、小程序、数据集、接口、菜单等。一般而言,客户端功能性可以从在客户端设备上驻留和/或可执行的各种钱包、微件、小程序、容器等得到,所述客户端设备诸如移动电话、智能电话、平板、通用电子交易设施、膝上型计算机、笔记本计算机、上网本、自助服务机、器具、公用设备、汽车、飞机以及任何其它电子或机电设备。

[0249] 一般地,本文描述的方法和系统包括在本文及别处称为移动客户端、容器等的客户端软件,其充当用于快速移动应用开发的使能基础设施。其提供基于容器的途径来支持多租户应用架构。移动客户端容器提供用于钱包和微件的电话特定运行时环境。该容器操控与应用执行、交易安全性、可靠性等相关的复杂性,包括设备特定实现。移动客户端容器可以基于API,诸如设备特定的API。容器运行时环境促进从微件描述符生成原生应用屏幕。这促进确保触摸屏按钮看起来像相应设备上的原生ANDROID、BLACKBERRY、IPHONE或其它设备按钮。钱包应用可以与微件类似,因为它也可以由移动客户端运行时功能性来解译和执行。然而,如本文所描述的,钱包将具有对应用的特许控制以维护高度安全和分离的环境来使用 and 访问钱包信息,所述钱包信息除其它外尤其可以包括用户帐户、个人和交易相关内容。壁(wall)还可以被定义为提供域特定(例如,金融、零售、医疗保健、政府等)的功能性。

[0250] 参照图23,图示了微件架构的示例性且非限制性实施例,其可以促进在用于安全个性化交易的多域生态系统中的客户端设备上的钱包容器内隔离不同的服务提供者微件。

客户端容器2302可以操作为客户端运行时组件,以用于促进在用于安全个性化交易的多域生态系统中的客户端设备(诸如移动电话、计算机、PDA、膝上型计算机等)上的移动应用的执行。如所图示的,一个或多个钱包2304可以包括应用和数据,其可以提供整体用户数字钱包体验并且可以通过由用于一个或多个微件2306的容器2302管理的一个或多个安全入口点来访问。一个或多个微件2306可以包括由第三方服务提供者开发和/或发行的服务群组。根据示例性实施例,微件2306可以以独立方式与一个或多个钱包2304隔离地运行在客户端容器2302的安全环境内。当根据示例性实施例实现为分立的可执行代码单元时,微件可以以与其它微件、钱包和小程序的操作分离和不同的方式来执行和操作,或者相反地,可以以与一个或多个其它钱包、微件和/或小程序协作的方式来操作,以执行安全交易。

[0251] 如所图示的,客户端容器2302可以与包括一个或多个设备特定的API的API层次2308相接口。API层次2308可以支持各种和/或流行的设备环境。电话独立API层次2310可以确保应用跨所有支持的MTP手持机而运行,所述应用包括但不限于钱包、微件和小程序,诸如通过使用移动交易平台(MTP)软件开发套件(SDK)开发的那些。根据示例性实施例,钱包2304和微件2306二者可以在结构上(例如,屏幕、Java脚本&CSS样式)几乎相同,除了与微件2306所做的相比,钱包2304可以访问API层次2308内的更宽的特许API集合。在一些情况下,钱包2304可以能够有鲁棒的用户配置和个性化,在与一般的微件和特别是服务提供者得到的微件相比时尤其如此。结果,在一些情况下,钱包可以提供有对在客户端设备的功能性上施加控制的API的增加的访问。

[0252] 根据示例性且非限制性实施例,当被调用时,钱包2304可以取得应用控制,直到(例如由用户、钱包2304、容器2302、外部服务等)选择了微件2306入口点为止。微件2306的用户选择可以经由可以通过钱包2304接口而对用户可用的卡图像、菜单选项等来进行。响应于这样的选择,可以在包括钱包2304的运行时安全环境(例如,由容器2302提供的环境)内发动所选微件,并且可以挂起钱包2304的执行。

[0253] 一旦被发动,微件2306就可以操作来促进例如微件2306正在其上执行的移动客户端设备的钱包2304与服务提供者之间的安全交易,所述服务提供者诸如发行微件2306的服务提供者。在这样的情况下,由服务提供者发行的微件2306可以被准予排他访问发行服务提供者的工作流、移动设备上的资源(诸如钱包资源、安全元件资源)以及客户端设备的用户接口。同样地,由服务提供者发行的微件2306可以被拒绝访问其它服务提供者的工作流、钱包元件等以及诸如客户端设备的用户接口之类的某些移动设备资源。

[0254] 作为分离地可执行的代码单元,微件2306可以经由从移动操作系统可获得的执行分离功能和/或通过包括由容器提供的运行时环境的移动客户端的各方面而有效地相互隔离。另外,可以由服务提供者(例如,器件的发行者等)开发微件2306,所述服务提供者可以配置微件以合并提供者特定的安全性元件,其可以使得其它服务提供者开发的微件难以访问其资源、工作流等。可以包括这样的微件、容器、钱包、服务提供者软件(没有限制地包括本文稍后描述的钱包服务中心的各种方面)等的移动交易平台可以在所有这样的方面中加强且不同的安全性,使得例如由服务提供者A开发的微件不可以访问服务提供者B的(例如,基于服务器的)资源。这样的强安全性出于各种原因可以是重要的,包括保持域特定的信息自用户可以通过用户的移动设备与之交互的其它域(例如,金融域、健康域、法律域、商业域、个人域、身份域等)是分离且机密的。

[0255] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令可以使得所述一个或多个处理器实行以下步骤,所述步骤可以包括在移动设备上的钱包容器中配置一个或多个微件模块。钱包容器可以包括一个或多个钱包模块。由计算机可读介质实行的步骤此外可以包括限制由一个或多个微件模块对包括一个或多个钱包模块、移动设备、一个或多个客户端应用的元素集的访问。所述步骤此外可以包括提供对发行者特定的安全性域和微件特定的发行者安全性域中的至少一个的一个或多个微件模块的访问。

[0256] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法包括在移动设备上提供容器运行时环境。所述方法此外可以包括访问移动设备驻留微件模块以确定与微件相关联的访问约束,在示例中,访问约束可以关于电子钱包访问、设备资源访问、设备驻留生态系统应用、由移动设备可访问的网络资源、发行者特定的安全性域以及微件特定的安全性域。所述方法此外可以包括通过容器来操作微件模块中的至少一个,以施加与微件模块相关联的访问约束。所述方法此外可以包括促进由微件模块对该微件模块相关联的发行者特定的安全性域和微件特定的安全性域中的至少一个的访问。在示例中,施加微件模块访问约束可以包括防止对移动设备上的电子钱包资源的访问。在示例中,施加微件模块访问约束可以包括防止由第一微件对与第二微件相关联的钱包的访问。在示例中,施加微件模块访问约束可以包括基于钱包的状态来防止由微件对移动设备上的钱包的访问。钱包的状态可以包括活动状态和非活动状态,在活动状态期间,可以允许由微件的访问,并且在非活动状态期间,可以防止由微件的访问。在示例中,促进对安全性域的访问可以包括允许对移动设备上的可以与微件模块共享安全性域的数字钱包的访问。在示例中,促进对安全性域的访问可以包括允许对发行者的可以与微件模块共享安全性域的网络资源的访问。

[0257] 本文在上面描述了移动交易平台的用于隔离和限制域特定的资源之中的访问的各种方面,包括客户端特定的方面。除了这些重要的安全性和资源访问限制功能之外,关于对钱包、设备资源、应用、网络资源等的访问的应用相关限制也可以通过本文描述的方法和系统来促进,所述方法和系统包括开发、部署、执行以及交易方法和系统。

[0258] 根据示例性实施例,容器可以实现一个或多个触发来控制或以其它方式限制对一个或多个钱包、设备、客户端应用和网络资源的访问。关于访问的限制可以基于定位(例如,场所、位置、网络类型、提供者可访问性、钱包状态、花费限制、信用余额、信用评分等)。这里描述了关于对资源的微件访问的这些和其它限制的示例。可以由商家以个性化方式来管理钱包,使得例如当某人进入一场所时,可以不向那个人给出使用使能在该场所不接受的支付形式的微件的选项。在另一非限制性示例中,当用户在美国以外旅行时,可以通过一个触发或多个触发来增强对各种微件的访问。根据又其它的示例,基于信用卡余额/限制的触发可以此外增强一个或多个微件的操作,包括但不限于由一个或多个微件对客户端应用和网络资源的访问。在示例性实施例中,如果钱包不是活动的(诸如可能在容器和一个钱包或多个钱包驻留在其上的客户端设备被关断时或者当用户已经去活钱包(例如为了钱包资源的增强的安全性)时发生),则可以限制相关联的微件访问客户端设备以及通常由钱包控制或通过钱包访问的网络资源、钱包内容等。

[0259] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法

包括至少部分通过联网服务器来配置微件以通过对发行者特定的服务群组的访问。所述方法此外可以包括在操作于客户端设备上的安全钱包容器中接收来自联网服务器的部署所配置的微件的请求。所述方法此外可以包括确定用于在客户端设备上操作微件的微件隔离要求。所述方法此外可以包括基于隔离要求而在移动设备上通过安全钱包容器来安装所配置的微件。

[0260] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令可以使得所述一个或多个处理器实行以下步骤,所述步骤可以包括在客户端设备上部署第一发行者特定的微件以促进基于第一信任模型的安全个性化交易。所述步骤此外可以包括在客户端设备上部署第二发行者特定的微件以促进基于第二信任模型的安全个性化交易。在示例中,第一发行者特定的微件和第二发行者特定的微件可以部署在钱包容器中。在示例中,第一信任模型和第二信任模型中的至少一个可以是委派(delegated)信任模型、直接信任模型以及代理(brokered)信任模型之一。在示例中,基于第一信任模型的安全个性化交易和基于第二信任模型的安全个性化交易中的至少一个可以基于触发而被促进。在示例中,触发可以对应于基于第一信任模型的安全个性化交易和基于第二信任模型的安全个性化交易中的至少一个的货币值。

[0261] 根据示例性且非限制性实施例,在微件2306已经诸如由可以是服务提供者的发行者开发之后,微件2306的操作可以被核实和批准并且可以存储在服务器上以供随后下载到一个客户端设备或者在非用户特定的微件2306的情况下下载到多于一个客户端设备。如所注意到的,微件2306可以取决于它们所指向的功能任务而在性质上变化。作为结果,各种类型的微件2306包括但不限于钱包特定的微件、用户-钱包特定的微件、供应-特定的微件、市场特定的微件、审查特定的微件、多用途微件等等。在成功安装到客户端设备上之后,微件2306就绪以供执行。

[0262] 在示例性实施例中,一旦微件2306被安装,以应答形式的确认就可以从下载微件2306的根源发送到服务器。由服务器对应答的接收可以导致服务器存储与微件2306的成功下载相关的信息。例如,服务器可以存储指示下载和安装微件2306的版本号的信息。这样的信息可以例如用于确定存在比之前已下载的更新近版本的微件2306供下载。在一些示例性实施例中,客户端设备处微件2306的成功下载可以导致显示给客户端设备的用户的确认可视记号(indicia),诸如显示的文本消息。同样,用户可以提供有用于接受下载的微件、例如包括执行微件的非绑定性试验的装置。这样的微件安装的结果可以包括将新的图标放置在客户端设备的移动交易平台用户接口中。新的图标可以暂时区别于其它图标以促进指示其比其它图标更新。可替换地,新的微件可以不具有对于用户而言的视觉上可检测的差异。

[0263] 所部署或安装微件的完整性可以由本文所描述的容器(例如,移动客户端容器)来提供。用于确保微件完整性的一种技术是确保微件和/或其数据是不变的。根据示例性实施例,为了确保在微件2306的下载和其执行之间的时间期间微件2306或其数据都没有被篡改,可以采用散列。可以从包括微件2306的应用代码来计算散列,并且当微件被安装时,散列被核实、被访问以供执行、在客户端移动交易平台资源的审查期间被访问、被加载以供执行(例如,在cClient容器运行时环境中)等。在当微件被加载以供执行时核实散列的示例中,微件2306一旦其通过在其加载时候的散列核实就可以开始其功能。

[0264] 移动客户端容器运行时环境还可以促进微件的强隔离,使得不同的微件不能影响其它微件资源、变更这样的资源或微件应用代码,以及类似可能影响微件完整性的。

[0265] 如上面所注意到的,微件2306可以提供一个或多个安全入口点,经由所述安全入口点,钱包应用可以与微件2306的发行者交互。在示例性实施例中,微件2306的发行者还可以是其服务通过由用户使用发行的微件2306而在整体上或部分上被使能的服务提供者。在示例性且非限制性实施例中,一个或多个微件2306可以一致地行动来以不同的信任度来执行安全个性化交易。特别地,可以部署不同的微件2306来促进根据不同信任模型的安全个性化交易,所述不同信任模型除了其它以外尤其包括用于交易执行的直接、间接、代理以及第三方安全信任模型。

[0266] 根据示例性且非限制性实施例,多于一个信任模型的使用可以反映其中部署了客户端设备和相关联的微件2306的环境中的差异。如本文在别处所注意到的,当配置生态系统的元件时,钱包和微件发行者可以选择一个或多个信任模型。例如,也许包括服务提供者的发行者可以部署第一微件2306以在空中执行安全银行业务交易,其中,交易具有第一信任级别。发行者此外可以例如部署第二微件以在销售点(POS)自助服务机(kiosk)处执行安全银行业务交易,其中,由于客户端设备邻近于自助服务机和/或访问设备的用户的独立核实,所以交易具有更高的第二信任级别。这些微件中的任一个或二者可以部署到单个客户端设备,并且可以由钱包2304诸如基于如所述的交易性质、可用OTA网络的安全性等来执行对用于执行的微件的选择。

[0267] 根据其它示例性且非限制性实施例,微件部署可以取决于变量。例如,发行者可以配置多个微件2306,其各自以金融交易量相关的信任模型来操作。例如,要求相对低信任级别的微件可以被部署用于涉及少于五十美元的金融交易,而要求相对高信任级别的微件可以被部署用于涉及多于五十美元的金融交易。

[0268] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法包括在移动设备处用多域安全钱包容器接收警报,即在移动设备上部署的现有微件的更新版本是可获得的。所述方法此外可以包括确认所述更新是对在移动设备上部署的现有微件的更新。所述方法此外可以包括配置钱包容器以接收经更新的微件。所述方法此外可以包括用钱包容器接收经更新的微件。所述方法此外可以包括处置现有微件以防止该微件的进一步使用。所述方法此外可以包括在移动设备上存储经更新的微件。

[0269] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法包括以操作于移动设备上的多域钱包容器来向服务器查询更新的微件的存在。所述方法此外可以包括从服务器接收指示更新的微件的可用性的信息。所述方法此外可以包括请求更新的微件。所述方法此外可以包括在移动设备处接收更新的微件。所述方法此外可以包括处置更新的微件所取代的现有微件以防止进一步使用现有微件。所述方法可以附加地包括将更新的微件存储在移动设备上。在示例中,可以以预定时间间隔执行对服务器的查询。在示例中,可以响应于微件在客户端设备上的执行而执行对服务器的查询。所述方法此外可以包括向服务器发送存储更新的微件的确认。

[0270] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法包括从移动设备接收对于存在更新的微件的查询。所述方法此外可以包括向移动设备传输指示更新的微件的可用性的信息。所述方法此外可以包括从移动设备接收对于更新的微件

的请求。所述方法此外可以包括向移动设备传输更新的微件。在示例中,可以以预定时间间隔接收查询。在实施例中,可以响应于微件在客户端设备上的执行而接收查询。所述方法此外可以包括接收对存储更新的微件的确认。

[0271] 根据示例性且非限制性实施例,可以出于各种目的中的任何一个来更新在客户端容器2302的安全环境内被存储并且能够运行的微件2306(例如,周期地、诸如每周地以提供当前定价或供应(offer)、增加花费限制,响应于用户请求以改善安全性、添加对不同信任模型的访问等等)。在一个示例性实施例中,在复查和发布微件2306之后,微件提供者可以创建和发出警报,指示一个或多个微件2306的新或更新版本的可用性。

[0272] 在一个示例性实施例中,可以仅向之前已经成功下载了(或以其它方式已安装了)要更新的微件2306的版本的那些客户端设备发出警报。在这样的情况下,消息可以被发送到客户端设备以告知用户更新的微件2306是可获得以供下载的,并且向用户提供下载更新的微件2306的选择。

[0273] 在另一示例性实施例中,诸如可以存储在钱包服务器上的配置文件可以包含用户可定制信息,其定义了用户期望用于微件更新发生的方式。例如,用户可以定制相关联的配置文件以指示每当之前下载的微件2306的新版本变得可用时,微件的较新版本要被下载。相反地,客户端设备可以周期地,诸如在启动时或者在参与商业交易之前,查询钱包服务器以下载之前安装微件2306的较新版本。在其它实施例中,可以由或者针对微件发行者、相关钱包发行者等定制配置文件。

[0274] 根据其它示例性实施例,可以通过微件发行者的工作流向微件2306自身告知更新是可获得的,并且基于更新的微件的各方面(例如,安全性更新),所安装微件可以采取行动(例如,禁用其自身,向用户通知其不再是当前的,更新其自身的部分而非用新微件替代它等)。可以通过钱包的操作来实现另一更新机制。例如,可以更新钱包,并且作为结果,可以指示微件过时,触发各种微件行动(例如,通知用户、自动更新、请求更新等等)。

[0275] 在多域生态系统中提供用于安全个性化交易的多层移动交易平台的方法和系统可以包括一种方法,所述方法在移动设备上配置至少一个移动交易平台特定的应用编程接口以用于促进由移动设备上执行的钱包容器对移动设备安全资源的访问。所述方法此外可以包括将多个不同钱包容器布置在移动设备的存储器中,其中,每个钱包容器经由所述至少一个应用编程接口来与移动设备安全资源相接口。所述方法此外可以包括所述至少一个编程应用接口经由三层次移动交易平台的安全性准则来施加钱包容器隔离。这三个层次可以包括个性化层次、服务层次和使能层次。

[0276] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的钱包容器。钱包容器可以包括用于促进微件、钱包、安全性和对安全元件的访问的管理的运行时组件。钱包容器此外可以包括基于API的接口,用于访问由微件提供的商业特定服务和用于访问客户端设备特定资源。钱包容器可以促进多个不同钱包以及不同微件的用于访问所述多个不同钱包中至少一个的操作。

[0277] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令使得所述一个或多个处理器实行以下步骤,所述步骤可以包括在移动设备上的钱包容器中配置一个或多个微件模块。钱包容器可以包括一个或多个钱包模块。所述步骤此外可以包括促进由微件中至少一

个的发行者对钱包模块中至少一个的访问。

[0278] 钱包容器2302可以形成移动交易平台(MTP)使能基础设施的客户端驻留部分。如这样,容器可以为诸如移动手持机等客户端设备提供跨平台服务执行环境。

[0279] 如上文所注意到的,本文描述的方法和系统一般包括在本文和别处称为移动客户端、容器、运行时环境等的客户端软件,其充当用于快速移动应用开发的使能基础设施。其提供基于容器的途径以支持多租户应用架构。移动客户端容器为钱包和微件提供电话特定的运行时环境。容器操控与应用执行、交易安全性、可靠性等相关的复杂性,包括设备特定实现。移动客户端容器可以基于诸如设备特定的API之类的API。

[0280] 如所图示出的,一个或多个钱包2304可以包括应用和数据,所述应用和数据可以提供整体用户数字钱包体验,并且可以通过由用于一个或多个微件2306的容器2302管理的一个或多个安全入口点来访问。一个或多个微件2306可以包括由第三方服务提供者开发和/或发行的服务群组。根据示例性实施例,微件2306可以以与一个或多个钱包2304隔离的独立方式运行在客户端容器2302的安全环境内。当根据示例性实施例而实现为分立的可执行代码单元时,微件可以以与其它微件、钱包和小程序的操作分离和不同的方式执行与操作,或者相反地,可以以与一个或多个其它钱包、微件和/或小程序协作的方式操作以执行安全交易。

[0281] 参照图24,其描绘了客户端设备容器(例如,移动客户端)的高层级架构视图,呈现了容器的详细示例性方面。容器2402可以促进用户接口渲染和导航; workflow 执行; 对开发者API的访问; 以及此外可以包括应用容器基础设施。容器2402可以促进具有微件生命周期管理器能力2432、访问控制器2434等的微件管理2430,同时集成了微件和钱包上下文。容器此外可以包括用户接口框架2412,其可以包括UI引擎2414、屏幕和布局2418、样式2420、UI元素2422等。如图24中所描绘的容器此外可以包括 workflow 框架2424,其可以利用脚本引擎2428、服务管理器,并且可以包括java脚本功能、可编写脚本的对象等。其它容器能力可以包括数据库功能性2440,诸如寻找/搜索、插入/更新、删除等。可以通过用于发送(例如, sms、HTTP/S)、编码、解码、附接、拆卸等的容器来促进通信2438。还可以通过容器来支持近场通信功能性2448。容器此外可以通过与安全元件或如可以由客户端提供的其它安全框架的交互来促进安全性,所述交互包括小程序安装、移除、安全信道设置、APDU交换等。与容器相关联地提供的另外的安全性特征可以包括密码学2442(例如, AES、3DES、RSA等)、签名、核实(例如, HMAC)、散列计算和核实(例如, SHA/1)、密钥生成(例如, PKCS#5)、随机数功能(例如, PRNG)等。容器还可以与诸如电话功能之类的客户端资源交互以促进进行呼叫、到达和/或管理联系人,与日历交互以促进基于事件的功能、基于位置的服务等。

[0282] 本文描述的多域生态系统安全个性化交易的方法和系统包括管理多个交易协议的方法,其包括在客户端设备的存储器中布置钱包模块。所述方法此外可以包括在存储器中布置钱包伴随小程序。所述方法此外可以包括执行与在生态系统上进行的安全个性化交易相关联的钱包伴随小程序,在所述生态系统中,客户端设备被部署来管理对与客户端设备相关联的安全元件的所选内容的访问。在示例中,钱包伴随小程序可以使用所访问的安全元件内容来促进对访问钱包模块的认证以执行交易。

[0283] 本文描述的多域生态系统安全个性化交易的方法和系统包括包含程序指令的计算机可读介质。通过计算机系统的一个或多个处理器执行程序指令使得所述一个或多个处

理器实行以下步骤,所述步骤可以包括在移动设备上的钱包容器中配置一个或多个微件模块。钱包容器可以包括一个或多个钱包模块。所述步骤此外可以包括配置至少一个小程序来与至少一个钱包模块相结合地执行,以促进多个交易协议的管理。

[0284] 根据示例性且非限制性实施例,安全元件(SE)可以用作客户端处的安全数据存储设备,诸如用于包括标准智能电话的移动设备。在示例性且非限制性实施例中,SE可以以一个或多个选项来安装,包括UICC、可移除微SD,嵌入在电话硬件中,或者安装为外接背板或者根据一些其它示例性接口方法来安装。

[0285] 根据示例性且非限制性实施例,如果由控制和/或发行实体和生态系统的剩余部分认可,则诸如钱包之类的设备应用可以与SE进行通信。通信的模式和方法可以取决于来自上面提及的选项之中的SE的类型而变化。

[0286] 在一些示例性实施例中,取决于用于控制SE的安全性模型,可以认可钱包在SE中安装、加载和管理小程序。还可以或者仅可以允许通过包括发送和接收应用协议数据单元(APDU)的小程序通信的标准方法来与预先安装的小程序进行通信。

[0287] 如名称所暗示的,钱包伴随小程序可以具有与数字钱包(例如,客户端设备上的钱包应用)一起工作的工作主功能,并且可以由客户端设备用于实行多种任务,包括但不限于:存储由一个或多个钱包所需的重要和/或关键数据,或者用于通过使用钱包而进行交易的任何操作,或者控制被设计用以通过可共享接口和/或通过为该目的所设计和实现的APDU的通信来促进这样的控制的其它小程序的运转。

[0288] 根据各种示例性且非限制性实施例,与钱包伴随小程序协调的钱包应用可以管理、影响和/或控制如此被使能的其它小程序,以用于管理它们的交易协议。

[0289] 参照图24A,其描绘了所呈现的移动设备内容、移动设备应用和安全元件特征的详细视图。移动设备应用可以包括如本文所描述的MTP应用(例如,容器、钱包、微件等)。安全元件内容可以包括安全性域2450、钱包伴随小程序2452以及钱包伴随域2454。如图24A中所描绘的,安全元件可以被配置在各种物理设备中,包括UICC、微SD、封套、外接附件、嵌入式元件等。

[0290] 钱包伴随域2454可以在本文描述的伴随小程序上扩展以包含用于伴随小程序和特征的整个安全性域。钱包伴随域2454或安全性域可以促进加载、安装、管理和删除安全元件中多个小程序,作为与安全性域相关联的群组。每个安全性域可以具有唯一的安全性密钥,其可以由移动交易平台用于在安全元件中的小程序群组上执行操作。钱包伴随域2454可以通过以下方式管理:适配当前技术的安全性密钥安全性特征以使能用于移动交易平台的分离的安全性密钥,以管理安全元件中的钱包伴随域2454的内容。

[0291] 图24B描绘了与钱包伴随小程序相关联的各种特征和控制以及数据流。安全元件中的钱包伴随小程序可以提供诸如以下的特征:安全存储、认证、ID管理、激活控制、存储/取得功能、加密功能、密钥存储和生成功能、PIN控制等。钱包伴随小程序可以提供钱包接口功能,其可以促进管理由其它小程序、外部移动交易平台参与者等对钱包的访问。钱包伴随小程序可以包括小程序接口,用于访问安全元件中的小程序。钱包伴随小程序可以促进与可信安全性管理器(TSM)服务器、移动交易平台(MTP)服务器及用于安全个性化交易的多域生态系统中的其它参与者的安全交互。

[0292] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法

包括在客户端设备的存储器中布置钱包模块。所述方法此外可以包括在存储器的安全元件中布置钱包伴随小程序。所述方法此外可以包括执行钱包伴随小程序以促进对一个或多个附加钱包小程序的访问。在示例中,可以通过至移动钱包功能的可共享接口来促进所述访问。在示例中,钱包伴随小程序可以使能优惠券发放、安全性和支付中的至少两个。

[0293] 本文描述的多域生态系统安全个性化交易的方法和系统包括一种方法,所述方法包括在客户端设备的存储器中布置容器。所述方法此外可以包括在存储器的安全元件中布置容器伴随小程序。所述方法此外可以包括执行容器伴随小程序以促进对一个或多个附加容器伴随小程序的访问。在示例中,可以通过至经由容器可访问的移动微件功能及移动钱包功能的可共享接口来促进访问。

[0294] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的平台,其包括可以配置至少一个标记化微件的运行时组件。在示例中,所述至少一个标记化微件可以促进用于安全个性化交易的多域生态系统中的至少一个交易。

[0295] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的平台,其包括可以配置用于安全个性化交易的多域生态系统中的至少一个服务提供者微件的运行时组件。

[0296] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的平台,其包括可以配置用于安全个性化交易的多域生态系统中的至少一个客户端容器的运行时组件。

[0297] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的平台,其包括可以保护钱包中多个帐户的帐户信息的运行时组件。

[0298] 本文描述的多域生态系统安全个性化交易的方法和系统包括在客户端设备上可操作的平台,其包括可以提供由多个服务提供者对移动钱包的安全访问的运行时组件。

[0299] 用于将供应与在外部服务提供和用于安全个性化交易的多域生态系统中的移动钱包之间的交易进行集成的移动钱包可以包括在移动设备上可操作的多域数字钱包,其中,数字钱包包括来自至少两个不同服务提供者的帐户。还可以包括运行时容器,用于执行尝试访问数字钱包的微件。另外,可以包括在运行时容器中可操作的多个移动供应链管理微件,其通过与外部服务提供者通信而与不同的移动供应域相接口。最后,还可以包括通过运行时容器、多域数字钱包以及多个移动供应链管理微件的至少一部分的协作操作所提供的移动交易能力。

[0300] 根据示例性且非限制性实施例,本公开提供可以作为一套小程序的一部分的优惠券小程序,该套小程序被开发来促进更丰富且更便利的零售购物体验,该体验的目标可以是使能移动钱包应用与服务提供者之间的供应相关的流,诸如相关联于销售点 (PoS) 终端。

[0301] 优惠券小程序可以支持以单敲 (single tap) 以及多敲 (multi-tap) 用户体验形式的近场通信 (NFC) 交易。优惠券小程序的一个或多个版本可以支持用于以下各项的特征:将多个优惠券附到单个交易、在交易中呈现所附的优惠券 (例如,向 PoS 终端)、传送赎回 (redemption) 状态、管理供应、将供应匹配到钱包、(例如,通过服务提供者微件) 从服务提供者寻求供应等。为了促进易于开发和集成,优惠券小程序可以包括至少两个接口 API。一个 API 可以用于将一个或多个供应 (例如,优惠券) 与数字钱包应用 (例如,如本文所描述的移动钱包客户端) 相接口,并且另一个 API 可以用于将优惠券与服务提供者相接口,诸如通

过PoS终端。服务提供者API可以促进由PoS终端对优惠券小程序的访问以用于查询优惠券、更新优惠券赎回状态等。

[0302] 优惠券小程序的一个或多个版本可以使能直接前向流,通过该直接前向流,用户可以诸如通过PoS终端、通常通过具有安全元件(SE)的移动电话而在与服务提供者的交易中呈现从一个或多个源下载的优惠券。

[0303] 图25图示了供应或优惠券相关交易流程图。参与交易的实体可以包括用户2502、钱包客户端2504、优惠券小程序2508以及PoS终端2510。在示例中,用户可以接触各种优惠券服务、浏览优惠券并决定要使用哪些优惠券用于特定购买。用户可以经由可以与钱包客户端2504相关联的移动钱包应用来执行这些操作。在2512处,钱包客户端2504可以向用户2502呈现存储的优惠券,并且在2514处,用户2502可以选择可以附着的优惠券。

[0304] 此外,可以发起阶段1(本文也称为预交易设置阶段)。如图25中所示,在阶段1期间,钱包客户端2504可以将所选优惠券附到小程序,并因而,钱包客户端2504可以指示交易可以开始。

[0305] 在阶段1之后,可以发起阶段2(本文中也称为PoS交易阶段)。在阶段2期间,可以向PoS终端2510呈现认证标识(例如,来自安全元件的用户身份和/或帐户数据)以发起PoS交易阶段。PoS终端2510然后可以向优惠券小程序2508查询附着的优惠券,并且优惠券小程序2508作为响应可以发送回与附着的优惠券相关的数据。这基于优惠券的数目可以进行若干查询。一旦PoS终端接收了所有优惠券,其就可以处理这些优惠券。这样的处理可以包括验证优惠券、检查适用性、遵照其它商业规则以确定优惠券的适用性等。在该阶段的处理结束时,可以标识赎回的优惠券。可以将这些优惠券的状态传送到优惠券小程序2508。

[0306] 在阶段2之后,可以发起阶段3(本文也称为后交易查询&清理)。在该阶段期间,如果需要的话,钱包客户端2504可以查询赎回状态并重置所有优惠券。优惠券的重置可以标定阶段3的结束,和将状态复位为阶段1的开始。

[0307] 图26图示了根据示例的优惠券小程序在交易流期间的状态机图。状态2602可以指示READY FOR UPLOADING COUPONS(就绪以供上传优惠券)状态,其指示来自优惠券小程序的所有优惠券可能已经被重置,并且钱包客户端现在可以上传为该交易选择的优惠券。在示例中,如图26中所示,如果命令GET APPLLET STATUS(取得小程序状态)导致错误,则小程序可以保持在状态2602中。在接收到有效的ENABLE TRANSACTION(使能交易)命令时,优惠券小程序就可以转变到下一状态2604。

[0308] 2604状态可以包括READY FOR COUPON REDEMPTION(就绪以供优惠券赎回)状态,其指示钱包客户端可能已经将所有优惠券附着到优惠券小程序的存储器,并且PoS终端可以继续进行交易的阶段2。在示例中,如图26中所示,如果命令READ COUPONS(读取优惠券)导致错误,则优惠券小程序可以保持在状态2604。在接收到有效的SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令时,小程序就可以转变到下一状态2608。如图26中所示,在接收到有效的ABORT TRANSACTION(中止交易)命令时,优惠券小程序就可以转变到下一状态2610。

[0309] 状态2608可以包括TRANSACTION COMPLETED(交易完成)状态,其指示PoS终端可能已经完成了交易的阶段2,并且可能已经设置了COUPON REDEMPTION STATUS(优惠券赎回状态)。此外,该状态2608可以指示钱包客户端现在可以继续进行交易的阶段3。优惠券小程序

可以保持在该状态中,直到小程序接收到有效的RESET COUPONS(重置优惠券)命令或有效的ABORT TRANSACTION(中止交易)命令。

[0310] 状态2610可以包括TRANSACTION ABORTED(交易中止)状态,其指示(与优惠券呈现&赎回相关的)PoS终端交易可能已经由钱包客户端或PoS终端中止。优惠券小程序可以保持在该状态2610中,直到小程序接收到有效的RESET COUPONS(重置优惠券)命令。

[0311] 根据示例性且非限制性实施例,本公开提供支持优惠券相关功能性的命令,其可以相关于与PoS终端的交互。在示例中,这些命令可以基于如由ISO/IEC 7816所定义的用于与SE的所有通信的标准智能卡命令和响应协议。在示例中,表CAT1可以概括类字节(CLA)和指令(INS)字节的编码。

CLA	INS	命令
'00'	'A4'	选择
'C0'	'01'	取得小程序状态
'C0'	'03'	中止交易
'C0'	'11'	读取优惠券
'C0'	'41'	设置优惠券赎回状态

[0312] CAT1:命令概括CLA和INS命令。

[0313] 在示例中,优惠券小程序可以返回可以按照ISO/IEC 7816-4编码的状态字节。小程序可以返回在表CAT2中示出的一组一般状态字节。该表可以列出状态字SW1、状态字SW2及其相关联的含义。

SW1	SW2	含义
'90'	'00'	正常处理
'67'	'00'	错误长度
'69'	'85'	使用条件未满足
'6A'	'80'	命令数据中的不正确值
'6A'	'82'	未找到小程序
'6A'	'84'	存储器不够
'6A'	'86'	不正确参数 P1-P2
'6D'	'00'	指令不被支持
'6E'	'00'	类不被支持

[0314] CAT2:一般状态字节。

[0315] 在示例中,本公开可以包括ABORT TRANSACTION(中止交易)命令,其可以将小程序从其现有状态移动到交易中止状态。在示例中,ABORT TRANSACTION(中止交易)命令可以根据表CAT3来编码。该表可以列出一个或多个代码,诸如类字节(CLA)、指令字节(INS)、参数P1、参数P2等等。在示例中,可能不存在从该命令返回的数据。

代码	值
CLA	'C0'
INS	'03'
P1	'00'
P2	'00'

Lc	‘00’
数据	不存在
Le	‘00’

[0316] CAT3:ABORT TRANSACTION(中止交易)命令消息。

[0317] 此外,命令的成功执行可以由状态字节‘9000’指示。ABORT TRANSACTION(中止交易)命令可以返回诸如在表CAT1中列出的一般错误条件。另外,ABORT TRANSACTION(中止交易)可以返回如表CAT3中所列出的以下特定错误和警告条件中的一个。

SW1	SW2	含义
‘67’	‘00’	错误长度
‘69’	‘85’	使用条件未满足
‘6A’	‘86’	不正确参数P1-P2

[0318] CAT4:用于ABORT TRANSACTION(中止交易)的状态字节。

[0319] 在示例中,GET APPLETT STATUS(取得小程序状态)命令可以用于检索小程序的当前状态。该命令可以返回小程序的当前状态。表CAT5可以列出与该命令相关联的代码和对应值。

代码	值
CLA	‘C0’
INS	‘01’
P1	‘00’
P2	‘00’
Lc	‘00’
数据	不存在
Le	‘00’

[0320] CAT5:GET APPLETT STATUS(取得小程序状态)命令消息。

[0321] 响应于该命令,可以返回数据字段。在示例中,小程序状态可以被返回并编码为1字节,并且该数据字段的细节可以在本描述中如下所述的表CAT17中找到。此外,命令的成功执行可以由状态字节‘9000’指示。GET APPLETT STATUS(取得小程序状态)命令可以要么返回诸如在表CAT1中列出的一般错误条件。另外,GET APPLETT STATUS(取得小程序状态)命令可以返回如表CAT6中所列出的以下特定错误和警告条件中的一个。

SW1	SW2	含义
‘67’	‘00’	错误长度
‘6A’	‘86’	不正确参数P1-P2

[0322] CAT6:用于GET APPLETT STATUS(取得小程序状态)的状态字节。

[0323] 在示例中,READ COUPONS(读取优惠券)命令可以用于检索优惠券数据。此外,READ COUPONS(读取优惠券)命令可以根据表CAT7来编码。

代码	值
CLA	‘C0’
INS	‘11’
P1	‘00’

P2	见表 CAT8
Lc	‘00’
数据	不存在
Le	‘00’

[0324] CAT7:READ COUPONS (读取优惠券) 命令消息。

[0325] 表CAT7包括参考控制参数P2,其可以控制相继READ COUPONS (读取优惠券) 命令的数量。此外,参考控制参数P2可以根据下表CAT8来编码

P2	含义
‘00’	取得所有出现
‘01’	取得下一出现

[0326] CAT8:READ COUPONS (读取优惠券) 参考控制参数P2。

[0327] 在示例中,如果在当前应用会话内没有接收到之前的Read Coupons (读取优惠券) [取得所有出现],则可以拒绝Read Coupons (读取优惠券) [取得下一出现] 命令。此外,响应于READ COUPONS (读取优惠券) 命令,如可以在客户特定优惠券规范中定义的优惠券数据的多个出现可以被返回。

标签	Len	值
‘E1’	Var	客户特定优惠券数据

[0328] CAT9:READ COUPONS (读取优惠券) 数据字段。

[0329] 此外,该命令的成功执行可以由状态字节 ‘9000’ 指示。读取优惠券命令可以要么返回诸如在表CAT10中列出的一般错误条件。

SW1	SW2	含义
‘63’	‘10’	更多数据可用
‘67’	‘00’	错误长度
‘69’	‘85’	使用条件未满足
‘6A’	‘86’	不正确参数 P1-P2

[0330] CAT10:用于READ COUPONS (读取优惠券) 的状态字节。

[0331] 在示例中,SELECT (选择) 命令可以用于选择优惠券小程序。SELECT (选择) 命令可以根据表CAT11来编码。

代码	值
CLA	‘00’
INS	‘A4’
P1	‘04’
P2	‘00’
Lc	AID的长度
数据	AID值
Le	‘00’

[0332] CAT11:SELECT (选择) 命令消息。

[0333] 命令的“数据”字段可以包含可以选择的优惠券小程序的应用标识符(AID),其可以按客户要求来定制。

[0334] 响应于该命令,可以获得返回的消息。返回的消息可以包括数据字段,该数据字段可以包括文件控制接口 (FCI) 并且可以根据表CAT12来编码。

[0335]

标签	Len	值				存在
'6F'	Var	FCI 模板				M
		标签	Len	值		存在
		'84'	Var	DF 名称 (小程序 AID)		M
		'A5'	Var	专有数据		M
				标签	Len	值
				'9F07'	2B	C-SAM 优惠券小程序-版本 Lx API ID
				'9F09'	2B	C-SAM 优惠券小程序-版本 Lx API 版本
				'9F11'	2B	优惠券格式 ID
				'9F13'	2B	优惠券格式 版本

[0336] CAT12:SELECT (选择) 消息响应数据字段。

[0337] 服务提供者小程序的AID (标签 '84') 可以是如本文所描述的AID。优惠券小程序 API ID (标签 '9F07') 可以指示对优惠券小程序API的支持。此外,优惠券小程序API版本 (标签 '9F09') 对于该版本可以是 '0101'。优惠券格式ID可以是客户可定制的优惠券格式ID,并且优惠券格式版本可以是客户可定制的优惠券格式版本。此外,可以在表CAT12中列出附加的两个字节标签。

[0338] 此外,SELECT (选择) 命令的成功执行可以由状态字节 '9000' 指示。在出现错误时,SELECT (选择) 命令就可以返回诸如在表CAT1中列出的一般错误条件。另外,SELECT (选择) 命令可以返回如表CAT13中所列出的以下特定错误和警告条件中的一个。

SW1	SW2	含义
'67'	'00'	错误长度
'6A'	'80'	命令数据中的不正确值
'6A'	'82'	未找到小程序
'6A'	'86'	不正确参数P1-P2

[0339] CAT13:用于SELECT (选择) 的状态字节。

[0340] 在示例中,SET COUPON REDEMPTION STATUS (设置优惠券赎回状态) 命令可以用于设置优惠券赎回状态。在该命令成功执行时,小程序状态就可以改变为“交易完成”。SET COUPON REDEMPTION STATUS (设置优惠券赎回状态) 命令可以根据表CAT14来编码。

代码	值
CLA	'C0'
INS	'41'
P1	'00'
P2	'00'
Lc	'0A'

数据	优惠券赎回状态
Le	‘00’

[0341] CAT14:SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令消息。

[0342] 该命令的执行可以不返回任何数据。此外,SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令的成功执行可以由状态字节 ‘9000’ 指示。在出现错误时,SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令就可以返回诸如在表CAT1中列出的一般错误条件。另外,SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令可以返回如表CAT15中所列出的以下特定错误和警告条件中的一个。

SW1	SW2	含义
‘67’	‘00’	错误长度
‘69’	‘85’	使用条件未满足
‘6A’	‘86’	不正确参数 P1-P2

[0343] CAT15:用于SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)的状态字节。

[0344] 根据示例性且非限制性实施例,本公开提供在小程序与PoS终端之间的交互的细节。图27图示了在小程序2702与PoS终端2704之间的交互。

[0345] 在2708处,PoS终端2704可以发出SELECT(选择)命令以选择优惠券小程序2702。在2710处,优惠券小程序2702可以以文件控制信息(FCI)做出响应。在2712处,PoS终端2704可以发出GET APPLLET STATUS(取得小程序状态)命令。在2714处,优惠券小程序2702可以返回应用状态。在2718处,在确定了应用状态是“READY FOR COUPON REDEMPTION(就绪以供优惠券赎回)”时,PoS终端2704可以发出READ COUPONS(读取优惠券)命令,其中P2=Get All Occurrences(取得所有出现)。在2720处,优惠券小程序2702可以返回针对可用优惠券的优惠券数据。如果存在多个优惠券,则可以在响应数据中包括针对多个优惠券的优惠券数据。如果小程序可以包括所有优惠券数据,则小程序可以发送SW= ‘9000’。如果小程序不可以包括针对所有优惠券的优惠券数据,则小程序可以发送警告SW= ‘6310’,其指示可以存在更多数据。在2722处,PoS终端2704可以解析数据和SW。如果SW可以包括 ‘6310’,则PoS终端可以发出另一READ COUPONS(读取优惠券)命令,其中P2=Get Next Occurrences(取得下一出现)。

[0346] 在接收到其中P2=Get Next Occurrences(取得下一出现)的READ COUPONS(读取优惠券)命令时,在2724处,优惠券小程序2702就可以尝试发送针对剩余优惠券的优惠券数据。至于其中P2=Get All Occurrences(取得所有出现)的READ COUPONS(读取优惠券)命令,如果存在多个优惠券待决以发送,则优惠券小程序2702可以在响应数据中包括针对多个待决优惠券的优惠券数据,如图27中2724处所示。一旦小程序包括所有待决优惠券数据,小程序就可以发送SW= ‘9000’。如果小程序不包括针对所有待决优惠券的优惠券数据,则小程序可以发送警告SW= ‘6310’,其指示可以存在更多数据。

[0347] 在响应于READ COUPONS(读取优惠券)而接收到SW=’ 9000’ 时,在2728处,PoS终端2704就可以继续进行以处理优惠券。在处理优惠券数据之后,在2730处,PoS终端2704可以通过发出SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令来设置优惠券赎回状态。字节阵列始终为等于优惠券最大数量的长度。可能需要针对所有字节将优惠券赎回状态设置为有效优惠券状态——即使存在较少优惠券。如果接收到比最大值少的优惠券,

则对应于未接收到的那些的优惠券赎回状态字节可以被设置以指示“不存在优惠券”。响应于对READ COUPONS(读取优惠券)命令的各种调用,可以以优惠券数据的接收顺序设置优惠券赎回状态。即使在不存在赎回的优惠券的情况下,PoS终端2704也可能被要求发出以下两个命令之一:SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)或ABORT TRANSACTION(中止交易)。

[0348] 图28图示了根据示例的在交易流期间优惠券小程序的状态机图。状态2802可以指示READY FOR UPLOADING COUPONS(就绪以供上传优惠券)状态,其指示来自优惠券小程序的所有优惠券可能已经被重置,并且钱包客户端现在可以上传为该交易选择的优惠券。在示例中,如图28中所示,如果命令GET APPLET STATUS(取得小程序状态)导致错误,则小程序可以保持在状态2802中。在接收到有效的ENABLE TRANSACTION(使能交易)命令时,优惠券小程序就可以转变到下一状态2804。

[0349] 2804状态可以包括READY FOR COUPON REDEMPTION(就绪以供优惠券赎回)状态,其指示钱包客户端可能已经将所有优惠券附着到优惠券小程序的存储器,并且PoS终端可以继续进行交易的阶段2。在示例中,如图28中所示,如果命令READ COUPONS(读取优惠券)导致错误,则优惠券小程序可以保持在状态2804中。在接收到有效的SET COUPON REDEMPTION STATUS(设置优惠券赎回状态)命令时,小程序就可以转变到下一状态2808。如图28中所示,在接收到有效的ABORT TRANSACTION(中止交易)命令时,优惠券小程序就可以转变到下一状态2810。

[0350] 状态2808可以包括TRANSACTION COMPLETED(交易完成)状态,其指示PoS终端可能已完成了交易的阶段2,并且可能已经设置了COUPON REDEMPTION STATUS(优惠券赎回状态)。此外,该状态2808可以指示钱包客户端现在可以继续进行交易的阶段3。优惠券小程序可以保持在该状态中,直到小程序可以接收有效的RESET COUPONS(重置优惠券)命令或有效的ABORT TRANSACTION(中止交易)命令。

[0351] 状态2810可以包括TRANSACTION ABORTED(交易中止)状态,其指示(与优惠券呈现&赎回相关的)PoS终端交易可能已经由钱包客户端或PoS终端中止。优惠券小程序可以保持在该状态2810中,直到小程序可以接收有效的RESET COUPONS(重置优惠券)命令为止。

[0352] 在示例中,表CAT16可以列出接受命令应用数据单元的各种可适用条件。在拒绝的情况下,如下表中所示,优惠券小程序可以返回状态字SW='6985'。

命令	就绪以供上传优惠券	就绪以供优惠券赎回	交易完成	交易中止
选择	接受	接受	接受	接受
取得小程序状态	接受	接受	接受	接受
中止交易	拒绝	接受	拒绝	拒绝
读取优惠券	拒绝	接受	拒绝	拒绝
设置优惠券赎回状态	拒绝	接受	拒绝	拒绝

[0353] CAT16:命令接受矩阵。

[0354] 根据示例性且非限制性实施例,本公开提供与优惠券小程序相关联的各种数据对象。在示例中,可以公开包括优惠券小程序API ID的数据对象。优惠券小程序API ID可以编码为2字节结构。为了确定是否可以支持优惠券小程序API,PoS终端可以利用掩码'0102'对值执行逻辑与操作。与操作的结果当等于'0102'时可以指示可以支持优惠券小程序。

[0355] 在示例中,可以公开包括小程序API版本的数据对象。优惠券小程序版本可以编码为2字节结构。在示例中,最高有效字节可以表示主发布版本,并且最低有效字节可以表示次发布版本。在示例中,可以公开包括小程序状态的数据对象。小程序状态可以标识小程序的当前状态,并且可以编码为1字节。在示例中,表CAT17可以列出与小程序的不同状态相关联的状态值。

状态	描述
‘01’	就绪以供上传优惠券
‘02’	就绪以供优惠券赎回
‘40’	交易完成
‘80’	交易中止
‘FF’	未知状态

[0356] CAT17:小程序状态。

[0357] 在示例中,可以公开包括优惠券赎回状态的数据对象。优惠券赎回状态可以存储在每个所附优惠券的一个字节中。对于所支持的最大数量的优惠券的优惠券赎回状态可以存储在长度为最大数量优惠券的字节阵列中。在示例中,对于优惠券1的赎回状态可以存储在字节阵列的B1中,并且对于优惠券2的赎回状态存储在字节阵列的B2中。表CAT18可以列出优惠券赎回状态的各种受支持的值。

优惠券状态	描述
‘00’	未使用
‘01’	赎回
‘05’	拒绝
‘FF’	不存在优惠券

[0358] CAT18:优惠券赎回状态。

[0359] 在示例中,数据对象可以包括一个或多个优惠券,并且优惠券格式可以取决于实现的类型。

[0360] 根据示例性且非限制性实施例,本公开提供了PoS终端的各种处理特征。在示例中,PoS终端可以遵照ISO/IEC 14443-4。当执行交易时,PoS终端可以分析可以由小程序返回的数据对象。例如,PoS终端可以检查可以由小程序返回的强制性数据对象。如果PoS终端可能未找到强制性数据对象,则PoS终端可以中止交易。类似地,如果PoS终端可能在数据中重组了不正确的格式化,则PoS终端可以中止交易。PoS终端可以采取应有关注以确保可以以鲁棒方式操控处理例外(例如,不正确格式化等)。

[0361] 在示例中,PoS终端可以在执行交易时执行各种处理操作。PoS终端可以如上面所讨论那样格式化SELECT(选择)命令,并且可以核实可以包括在SELECT(选择)命令的响应消息中的FCI的格式化。在示例中,PoS终端可以根据表CAT12来核实FCI的格式化。如果可能检测到FCI未根据表CAT12来格式化,则PoS终端可以终止处理并且确保取消选择小程序。

[0362] 此外,PoS终端可以分析可以在FCI中返回的DF名称(标签‘84’)。如果DF名称与SELECT(选择)命令的数据字段中所提供的AID不相同,则PoS终端可以终止处理并且确保取消选择小程序。另外,PoS终端可以通过检查可以在FCI中返回的API ID(标签‘9F07’)来核实其可以支持API。如上文所讨论的,PoS终端可以利用掩码‘0102’来对值执行逻辑与操作

以确定对API的支持的可用性。如果与操作的结果不等于‘0102’，则PoS终端可以终止处理并确保取消选择小程序。

[0363] 在示例中，PoS终端可以核实其可以支持可以在FCI中返回的API版本（标签‘9F09’）。如果其不可以被确定，则PoS终端可以终止处理并确保取消选择小程序。在示例中，PoS终端可以核实其可以支持对可以在FCI中返回的优惠券格式ID（标签‘9F11’）的操控。如果这不可以被核实，则PoS终端可以终止处理并确保取消选择小程序。在示例中，PoS终端可以核实其可以支持对可以在FCI中返回的优惠券格式版本（标签‘9F13’）的操控。如果这不可以被核实，则PoS终端可以终止处理并确保取消选择小程序。

[0364] 在示例中，PoS终端可以处理GET APPLET STATUS（取得小程序状态）命令。在成功选择优惠券小程序之后，PoS终端可以通过使用GET APPLET STATUS（取得小程序状态）来查询当前小程序状态。在示例中，PoS终端可以识出小程序状态可以不是“就绪以供优惠券赎回”。在这样的条件中，PoS终端可以终止处理并且确保取消选择小程序。在示例中，PoS终端可以识出小程序状态可以是“就绪以供优惠券赎回”。在这样的条件中，PoS终端可以继续进行对优惠券的正常处理。

[0365] 在示例中，PoS终端可以处理READ COUPONS（读取优惠券）命令。PoS终端可以发出READ COUPONS（读取优惠券）[取得所有出现]命令以读取优惠券数据。该命令的成功执行可以由状态字节‘9000’指示。这可以指示所有优惠券数据可能已经被发送。此外，READ COUPONS（读取优惠券）命令可以返回其中SW=‘6310’的警告以指示“更多数据可用”。在接收到其中SW=‘6310’的响应时，PoS终端就可以发出后续的READ COUPONS（读取优惠券）[取得下一出现]以检索附加数据。在示例中，在当前应用会话中，如果READ COUPONS（读取优惠券）[取得下一出现]命令可以在之前并且在没有发出READ COUPONS（读取优惠券）[取得所有出现]的情况下发出，则可以拒绝该命令。此外，PoS终端可以检查以确保所有强制性数据对象存在。在示例中，PoS终端可能遇到标签（Tag）在优惠券对象中多于一次的出现。在这样的条件中，PoS终端可以拒绝优惠券。

[0366] 在示例中，PoS终端可以处理SET COUPON REDEMPTION STATUS（设置优惠券赎回状态）命令。在验证了所应用的优惠券时，PoS终端就可以发出SET COUPON REDEMPTION STATUS（设置优惠券赎回状态）命令以更新小程序上的优惠券赎回状态。可以仅针对自上一次READ COUPONS（读取优惠券）[取得所有出现]后可能已经读取的优惠券考虑优惠券赎回状态。此外，如果未发出READ COUPONS（读取优惠券）[取得所有出现]，则可以忽略所有优惠券赎回状态。如果自上一次对READ COUPONS（读取优惠券）[取得所有出现]的调用后未读取所有优惠券，则可以忽略针对未读取的优惠券的优惠券赎回状态。

[0367] 在示例中，PoS终端可以处理ABORT TRANSACTION（中止交易）命令。PoS终端可能遇到错误或者其中PoS可能不能够继续进行处理的状态。在这样的条件中，PoS终端可以发出ABORT TRANSACTION（中止交易）命令以中断交易。在成功处理ABORT TRANSACTION（中止交易）命令时，就可能失去优惠券赎回状态。此外，在接收到对ABORT TRANSACTION（中止交易）命令的响应时，PoS终端就可以终止处理并且确保取消选择小程序。

[0368] 对于典型部署的高层级架构——

[0369] 图29图示了在示例性实施例中本发明的部署的系统2900的高层级架构。

[0370] MTP 2902可以设置在生态系统提供者的域2904中，并且可以集成到域2904的企业

服务总线 (ESB) 2908 中。域 2904 可以包括钱包服务器 2918。钱包服务器 2918 可以包括至少一个钱包 2920 和 MTP 2902。钱包 2920 可以包括至少一个微件 2922。在示例中, ESB 2908 可以连接 MTP 2902 服务提供者的生态系统。ESB 2908 可以用于设计和实现面向服务的架构中的互相交互的软件应用之间的交互和通信, 如图 29 中所图示。可能需要 ESB 2908 以用于实现具有多个钱包应用的生态系统, 如图 29 中所图示。ESB 2908 可以监视和控制在各种服务之间 (例如在钱包服务器 2918 与钱包提供者 2924 之间) 的消息交换的路由。

[0371] MTP 2902 可以具有多个角色。例如, MTP 可以执行钱包和交易管理, 连同可以与将钱包递送给多个不同移动环境相关联的所有相关商业服务。在示例中, MTP 2902 可以提供构建用于钱包的微件的第三方开发者和提供者的生态系统的建立, 而不必担心手持机分片。在示例中, MTP 2902 可以建立与各种生态系统 (例如, 服务提供者的生态系统、多个移动环境) 的多个连接器。连接器连同 MTP 2902 一起可以提供改善的用户体验和多种服务集合, 所述服务集合无论时间或位置都可以对于终端用户是可访问的。

[0372] 生态系统提供者的域 2904 可以包括可信服务管理器 (TSM)。TSM 可以被配置用于微件的空中供应和密钥管理。TSM 1812 可以与 MTP 2902 协同以促进近场通信体验。在示例中, 微件 2922 的供应和钱包 2920 可以通过 MTP 2902 来促进 (通过图 30-36 来描述)。在示例中, 钱包 2920 的设置和管理可以通过 MTP 102 来促进 (通过图 30-36 来描述)。在示例中, 可以通过 TSM 来进行小程序发行和个性化 (通过图 30-36 来描述)。

[0373] 在示例中, 服务提供者可以使用 MTP 软件开发套件来构建可以在 MTP 钱包容器内运行的微件。微件可以提供 OTA 增值服务和邻近 NFC 服务二者。钱包容器可以向微件 2922 提供安全运行时环境和服务以与服务器进行 OTA 通信 (OTA 服务), 并且还与安全元件通信以管理用于邻近 NFC 交易的支付和非支付小程序。在示例中, 微件 2922 可以具有在安全元件中运行的相关的小程序。在示例中, 微件 2922 可以没有安全元件中运行的相关的小程序。在示例性实施例中, 服务提供者可以仅提供 OTA 服务。

[0374] 生态系统提供者 2904 可以确保在商家位置处的所有 NFC 读取器 2930 都可以被配备以操控由可以加载到安全元件中的各种小程序所使用的邻近协议。NFC 读取器 2930 可以通过获取网络来处理交易, 所述获取网络可以将交易转换到云中的适当生态系统服务提供者。在示例中, 钱包 2920 或微件 2922 可以与生态系统云进行通信以确定服务状态和各种其它保健 (hygiene) 要求, 像余额、交易历史、存储的充值等。

[0375] NFC 读取器 2930 可以促进安全元件形状因数、微 SD、嵌入式或 UICC 的最终化 (如通过图 31 所详细描述)。NFC 读取器 2930 和联合基础设施可以促进设备的最终化 (finalization)。NFC 读取器 2930 可以促进支付协议最终化。NFC 读取器 2930 可以促进读取器分布和支持。

[0376] 如图 29 中所图示, 移动钱包 2920 可以与来自系统 2900 的各种元件交互。移动钱包 2920 可以与钱包提供者 2924 以及多个微件提供者 2928 交互。在示例中, 移动钱包 2920 可以与像支持、消息服务器和其它服务提供者那样的各种基础设施系统交互。

[0377] 每个生态系统可以包括多个生态系统行动者 (actor)。在示例性实施例中, 生态系统行动者可以包括近场通信 (NFC) 小程序、应用商店、条形码读取器、生态系统提供者、发行者、消息源、移动电话、移动钱包、NFC 销售点终端、原始装备制造商 (OEM) 提供者、安全元件 (SE)、服务提供者 (或微件提供者)、电信运营商 (telco)、可信服务管理器 (TSM)、TSM 代理客

户端、用户、钱包管理员、钱包伴随小程序(WCAp)、钱包提供者、钱包服务器以及微件。在示例中,安全元件上的NFC小程序可以与NFC销售点读取器执行交易。在示例中,应用商店可以指代应用分布机制,其可以由诸如apple®、blackberry®/rim®以及android®/Google®之类的设备制造者所设立。在示例中,条形码读取器可以用于扫描条形码。在示例中,拥有和设立移动钱包生态系统的生态系统聚集器实体可以与生态系统操作者或合作伙伴协作。生态系统聚集器实体可以设立基础设施和聚集服务提供者以使能移动支付和移动商务生态系统。在示例中,发行者可以是发行卡、优惠券、忠诚度、礼品以及其它标记的实体。在示例中,消息源可以是使用钱包API创建用于钱包用户的信息的实体。在示例中,移动电话可以是钱包在其上运行的那个。在示例中,移动钱包可以是用于移动手持机的可下载客户端应用,用以向用户提供无缝支付体验连同套用于邻近(NFC)和空中交易二者的增值服务。在示例中,NFC销售点终端可以与NFC电话交互并执行交易。在示例中,OEM提供者可以提供设备、微SD、SE等。在示例中,SE可以表示NFC与用于安全和可信交易的智能卡技术的组合,其中,NFC可以提供用于连接性的RF前端,并且智能卡可以提供安全性/加密引擎。在示例中,服务提供者可以是创建钱包并向钱包用户提供支付和非支付服务的实体。在示例中,电信运营商(Telco)可以提供SMS和数据服务。在示例中,TSM可以管理安全元件上的小程序和卡数据的OTA发行,并且可以提供密钥管理服务。在示例中,TSM代理客户端可以位于移动电话上并且与TSM服务器和安全元件交互。在示例中,用户可以是移动钱包的终端用户。在示例中,钱包管理员可以管理钱包的后端操作,包括钱包生命周期。在示例中,钱包伴随小程序可以使能安全钱包&微件生命周期管理,其可以包括钱包&微件认证、钱包状态管理和设置,并利用钱包服务器提供用于安全认证的基于票据的核实。在示例中,钱包提供者可以是发动有品牌的钱包应用并将其提供给用户的实体。在示例中,钱包服务器可以是鲁棒的、可伸缩的服务器平台,其可以管理钱包生态系统、钱包生命周期、微件供应&与其它生态系统合作伙伴的集成。在示例中,微件可以是绑定在一起并利用为单个单元的一组商业特征。微件可以包含屏幕/UI、事件操控以及对应的商业逻辑。

[0378] 用例-概观

[0379] 在各种示例性且非限制性实施例中,钱包用例可以分类成各种种类。这些种类可以包括钱包下载、钱包激活&设置、交易&微件、生命周期活动以及监管&支持。在示例中,钱包下载可以包括用于钱包分布以及在消费者的移动电话上安装钱包软件的应用例和方法。可以要求这些服务以用于将用户引入到平台并且向移动电话供应移动软件。在示例中,钱包激活&设置种类可以包括用于认证用户证书并建立用户简档以及使用户能够使用移动钱包应用的应用例。在示例中,交易&微件种类可以包括用以使用户能够下载微件并得到支付&非支付标记,以及通过使用激活的移动钱包应用来进行交易的应用例。交易应用例可以包括NFC交易、基于条形码的交易以及空中交易。在示例中,生命周期活动可以包括使用户能够继续使用钱包应用的服务可能需要的应用例和特征。在示例中,监管&支持应用例可以有关于管理移动钱包平台的日常操作和支持活动,并且包括诸如改变设备、锁定和解锁设备等的应用例。

[0380] 在各种示例性且非限制性实施例中,微件下载可以是第一应用例场景,其后是钱包激活&设置。进一步在钱包激活&设置之后可以是交易&微件应用例。交易&微件应用例之后可以是生命周期活动,并且监管&支持应用例种类可以支持和帮助钱包下载、钱包激活&设置、交易&微件、生命周期活动种类。可以在本文中描述少数示例性应用例。

[0381] 在示例性且非限制性实施例中,微件下载可以是以具有下载URL(推送或拉取)的SMS用例的形式。在示例中,具有下载URL(推送或拉取)的SMS用例可以允许钱包提供者通过使用SMS推送/拉取在空中分布应用,而不在应用商店发布应用。在该示例中,移动钱包可以成功地安装在移动电话上,并且用户可以在主屏幕上看到移动钱包图标。具有下载URL(推送或拉取)的SMS用例可以使用像用户、生态系统提供者、移动电话和telco(电信运营商)的生态系统行动者。对于该用例所需的前提条件可以是要数据使能的移动电话。

[0382] 图30图示了描述通过使用具有下载URL(推送或拉取)的SMS在用户的移动电话上安装移动钱包的方法3000的流程图。方法3000包括在步骤3002处通过向短代码发送SMS来发起SMS。在示例中,SMS可以由用户发送给Telco(电信运营商)或钱包提供者,这也称为SMS推送。在可替换实施例中,用户可以从telco(电信运营商)或钱包提供者接收SMS,这也称为SMS拉取。在可替换实施例中,用户可以从网站发起SMS。步骤3002的完成可以取决于SMS短代码(SMSC)的成功发起。方法3000此外可以包括在步骤3004处将SMS发送给用户。在示例中,Telco(电信运营商)可以将SMS发送给用户。在可替换实施例中,用户可以使用与SMSC的整合。步骤3004的完成可以取决于SMS整合的方法,其可以利用Telco(电信运营商)或SMSC。

[0383] 方法3000此外包括在步骤3008处由用户接收具有欢迎文本的URL。用户可以选择在SMS中提供的URL。步骤3008的完成可以取决于URL描述符和欢迎消息。方法3000此外包括在步骤3010处移动电话向钱包服务器发送请求以提供可下载文件。在方法3000的步骤3012处,钱包服务器可以此外被配置为用于将钱包软件提供给移动电话。在方法3000的步骤3014处,移动电话可以被配置用于在移动电话上下载应用并提示用户以安装应用。在已经由移动电话向用户提示了安装之后,在方法3000的步骤3018处,用户可以确认安装。在方法3000的步骤3020处,移动电话可以在接收到用户确认之后安装应用。

[0384] 在示例性且非限制性实施例中,钱包激活用例处理可以使用户能够激活移动钱包,并在用户诸如移动钱包、移动电话、安全元件、钱包服务器、TSM和钱包提供者之类的生态系统行动者之间建立安全链接。在示例中,钱包激活用例行动者像移动手持机、TSM、用户、移动钱包、钱包提供者、钱包服务器。钱包激活仅当用户可能已经在移动手持机上成功地安装了移动钱包(如通过图30所描述的由用户预加载或下载)时才可以发生。此外,为了钱包激活发生,SE可以与移动手持机相连接/相关联(用于像微SD和UICC的可移除SE)。此外,用户可以具有用于钱包激活发生的数据连接性。在钱包的成功激活之后,用户可以能够使用钱包应用。

[0385] 图31图示了由用户进行的钱包激活的方法3100。方法3100包括在步骤3102处移动钱包向用户示出注册&激活屏幕,其包括电子邮件地址和个人标识号(PIN)。在示例中,PIN可以是4数位号码。在示例中,PIN可以被配置为是数字的,并且具有与其相关联的商业规则,例如,4-10数位、无序列、无重复数字等。在示例中,可以定制注册屏幕以捕获附加参数,如创建用户简档所需要的,例如,用户名、用户照片或任何其它用户签名。方法3100此外包括在步骤3104处用户在注册和激活屏幕上键入所有需要的信息。方法3100此外包括在步骤3108处移动钱包向用户示出最新项目和条件(T&C)。在示例中,可以在运行时从服务器拉取T&C。在示例中,对于每个钱包提供者,T&C可以不同。在示例中,对T&C的接受可以连同版本号一起被告知给钱包提供者。方法3100可以在步骤3110处要求用户接受T&C。在示例中,如果用户可能拒绝T&C,则可以向用户示出消息,指示可能需要对T&C的接受以激活钱包。

[0386] 方法3100此外包括在步骤3112处移动钱包从移动电话取出安全元件ID(CIN)、设备ID(IMEI)和SIM ID(ICCID),并将信息(包括电子邮件ID、PIN和T&C版本以及时间戳)发送给钱包服务器。在示例中,并非在所有情况中所有信息都可以对移动钱包是可用的,并且可能需要分离的工作流或与Telco(电信运营商)或服务提供者的交互来捕获所需细节。例如,如果移动号码不能从SIM或设备API是可获得的,则其可以从来自设备的HTTP标头中捕获,如果Telco(电信运营商)提供它的话。方法3100在钱包激活中进一步继续进行之前可能需要来自Telco(电信运营商)的移动号码和SIM信息。方法3100此外包括在步骤3114处钱包服务器执行第一级别核实以检查是否有任何信息可以是复制。在示例中,如果用户记录可以已经是可用的,则钱包服务器可以向用户提供适当的错误消息。

[0387] 方法3100此外包括在步骤3118处钱包服务器向钱包提供者发送信息以用于核实。在步骤3120处,钱包提供者可以核实该信息并向钱包服务器发送核实结果。在示例中,核实过程可以包括由Telco(电信运营商)进行的KYC检查。核实过程可能是在进一步在钱包激活中继续进行之前由方法3100要求的。在步骤3122处,钱包服务器可以创建其中用户状态为“不活动”的钱包记录,并向移动钱包发送确认。在步骤3124处,移动钱包可以向用户示出消息,即钱包可能处于针对用户而被个性化的过程中。在步骤3128处,钱包服务器可以通过ESB向TSM发送请求与用户信息(如上所讨论的移动号码、SE ID、设备ID、钱包ID以及PIN)。

[0388] 方法3100此外包括在步骤3130处ESB被配置用于向TSM发送信息。在步骤3132处,TSM可以与TSM代理客户端通信,并且发起SE个性化过程。在步骤3134处,TSM可以利用钱包伴随小程序安装来使安全元件个性化,并且可以利用硬件和钱包相关信息来在其上执行存储数据。在步骤3138处,一旦个性化完成,TSM就可以向钱包服务器发送通知。在步骤3140处,钱包服务器可以更新钱包状态为“活动”,并且通知钱包客户端。在方法的步骤3142处,移动钱包可以向用户示出确认,其指示成功的钱包激活。

[0389] 在示例性且非限制性实施例中,交易和微件用例可以包括一系列微件管理用例。在示例中,微件管理用例可以包括一系列微件安装用例。在示例中,微件安装用例可以包括应用内用例警报。应用内用例警报可以允许用户基于由钱包提供者所接收的警报来下载微件。钱包提供者可以通过使用C-SAM的警报框架来发送警报。应用内用例警报可能需要移动钱包、服务提供者、用户、钱包提供者以及钱包服务器。在激活移动钱包之后,用户可以安装微件作为应用内案例。而且,用户可以登录到移动钱包。服务应当在应用内用例警报之前已经创建了微件。钱包提供者可以在应用内用例警报之前已经复查了微件并且发布了它。钱包提供者可以在应用内用例警报之前已经创建了警报。在应用内警报之后,用户可以已经成功下载了微件。在应用内用例警报中,移动钱包可以向用户示出警报。在示例中,可以在移动钱包消息收件箱中或者在与钱包服务器的通信期间向用户示出警报。然后,用户可以选择警报、查看消息并发起下载。在发起下载之后,移动钱包可以安装微件并且向钱包服务器发送确认。钱包服务器可以向移动钱包发送确认。移动钱包可以向用户示出确认。

[0390] 在示例中,微件安装用例可以包括搜索和下载用例。搜索和下载用例可以允许用户搜索微件并在移动钱包上下载和安装。搜索和下载用例可能需要移动钱包、钱包服务器、服务提供者、用户以及钱包提供者。搜索和下载用例可能需要用户已经激活了移动钱包、用户已经登录到移动钱包、服务提供者已经创建了微件,以及钱包提供者已经复查了微件并发布了它。作为搜索和下载用例的结果,用户可以成功地下载微件。

[0391] 图32图示了作为搜索和下载用例的示例的方法3200。方法3200可以包括在步骤3202处用户搜索或浏览可用微件的种类。在示例中，用户可以能够通过从服务列表选择微件或者在钱包中键入或选择适当准则来搜索微件。在步骤3204处，方法3200可以要求移动钱包将基于用户准则的请求发送给钱包服务器。在步骤3208处，钱包服务器可以向移动钱包发送与用户的搜索准则相匹配的所有可用微件的列表。在步骤3210处，移动钱包可以向用户示出微件的列表。在步骤3212处，用户可以查看来自钱包服务器发送的列表的任何微件的微件描述，并且发起所期望微件的下载。在方法3200的步骤3214处，移动钱包可以安装微件并向钱包服务器发送确认。在步骤3218处，钱包服务器可以向移动钱包发送确认。在步骤3220处，移动钱包可以向用户示出确认。

[0392] 在一些示例性且非限制性实施例中，交易用例可以包括空中 (OTA) 交易用例。空中交易用例可以描述基于OTA交易的交易过程。OTA交易可以包括用户、移动钱包、微件以及服务提供者。为了OTA交易发生，用户可能必须登录到移动钱包中，用户可能必须具有数据连接性，并且用户可能已经在移动钱包上加载了用于OTA交易的微件。在示例中，OTA交易可以促进由用户成功完成交易。

[0393] 图33图示了用于OTA交易的示例性方法3300。方法3300可以包括在步骤3302处用户选择微件。微件选择可以按对于用户可以可用的各种类型的服务来进行，所述服务例如票务、账单支付等。在步骤3304处，方法3300可以要求移动钱包在步骤3304处将微件加载到服务屏幕上(如也在上文讨论的)。在步骤3308处，用户可以浏览服务屏幕并选择要支付的产品/服务。工作流和用户体验对于不同服务可以不同。服务可以要求在用户可以到达支付屏幕之前的多个交互。在步骤3310处，钱包服务器可以将信息从用户发送到服务提供者。在步骤3312处，服务提供者可以向用户提供具有支付量的支付请求。在步骤3314处，用户可以选择支付卡并提供支付信息。在示例中，用户可以选择在钱包上可用的支付方法，并且其可以允许OTA交易。在示例中，用户可以键入卡信息，同时空中行进也在进行。方法3300的步骤3318可以要求钱包服务器向服务提供者提供支付信息。在步骤3320处，服务提供者可以通过支付网关/银行业务接口来结算支付，并且可以向钱包服务器提供交易确认。在步骤3322处，钱包服务器可以接收交易确认，并且可以向微件和钱包发送信息。在方法3300的步骤3324处，移动钱包可以向用户示出交易确认和细节。

[0394] 在示例性且非限制性实施例中，生命周期活动可以包括卡发行用例。卡发行用例可以允许卡发行者在钱包上发行卡数据。卡发行用例可以包括发行者、钱包服务器、TSM、用户以及移动钱包。为了卡发行发生，用户可能必须激活移动钱包，用户可能必须登录到移动钱包，服务提供者可能必须创建更新的微件，以及钱包提供者可能必须复查微件和发布其它。之后，卡发行成功完成；用户可以能够下载微件。

[0395] 图34图示了作为卡发行用例的示例的方法3400。方法3400可以在步骤3402处要求发行者批准支付帐户(例如，信用卡)。在步骤3404处，发行者可以在TSM的帮助下对安全元件进行个性化。在示例中，TSM可以安装支付小程序，并且可以用跟踪数据进行个性化。卡发行用例可以取决于支付卡和SE上的小程序发行&小程序的类型。在示例中，小程序可以是Pay-pass、zip等。在步骤3408处，方法3400可以要求用户经由ESB向钱包服务器提供软卡数据。软卡数据可以包含要用于交易的图像、余额、卡昵称以及AID。方法3400在步骤3410处此外可以要求钱包服务器创建用户的服务账户的记录。在步骤3412处，钱包服务器可以标识

要连同服务账户一起发送的微件。在步骤3414处,钱包服务器可以在微件上创建散列,并经由ESB将微件ID、版本和散列发送给TSM。在步骤3418处,TSM可以在来自TSM代理客户端的帮助下在安全元件上完成微件散列更新。在步骤3420处,一旦微件散列可能被更新,TSM就可以经由ESB通知钱包服务器。在步骤3422处,钱包服务器可以使软卡和微件可用于下载。移动钱包可以执行同步,并且可以在用户的移动电话上下载软卡和微件。

[0396] 在示例性且非限制性实施例中,支持和监管可以包括终止钱包用例。终止钱包用例可以允许钱包管理员终止钱包账户。终止钱包用例可以包括移动钱包、钱包服务器、TSM、TSM代理客户端。为了钱包终止,钱包管理员可能必须被注册,钱包管理员可能必须具有管理用户简档的特许,以及钱包管理员可能必须至钱包管理控制台。在钱包终止用例完成之后,钱包管理员可以成功终止钱包账户。

[0397] 图35图示了作为用以终止钱包的示例的方法3500。方法3500在步骤3502处可以要求钱包管理员发起挂起钱包活动。在可能发起挂起活动之后,在步骤3504处,钱包服务器可以更新钱包状态为“termination_pending”(终止_待决)。在步骤3508处,钱包服务器可以向ESB发送请求。在步骤3510处,ESB可以从钱包服务器检索服务账户列表。在步骤3512处,ESB可以向发行者发送请求以终止服务账户。在向发行者发送请求之前,ESB可以检查服务账户列表。在步骤3514处,发行者可以在TSM的帮助下在后端终止钱包账户,并且还从SE移除支付小程序。在步骤3518处,ESB可以向TSM发送请求以移除钱包伴随小程序。在步骤3520处,TSM可以向TSM代理客户端发送消息。在步骤3522处,TSM代理客户端可以从SE移除钱包伴随小程序。在步骤3524处,一旦更新可能完成,TSM就可以向ESB发送通知。在方法3500的步骤3528处,钱包服务器可以接收更新,并且可以将钱包状态改变为“已终止”。在步骤3528之后,可以成功终止钱包。

[0398] 在示例性且非限制性实施例中,微件管理包括发布微件用例。发布微件用例可以允许生态系统提供者发布经批准的微件。发布微件用例可以包括钱包管理员、钱包服务器和服务提供者。在发布微件之前,钱包管理员可能必须被注册,服务提供者可能必须被注册,钱包管理员可能必须登录到钱包管理控制台中,以及微件可能必须被验证和批准。

[0399] 图36图示了作为用于发布微件的示例的方法3600。方法3600在步骤3602处可以要求钱包管理员登录到钱包服务器系统管理控制台中。在步骤3604处,钱包管理员可以从钱包服务器系统管理控制台选择微件管理。在步骤3608处,钱包管理员可以从微件管理选择用于发布微件的链接。在步骤3610处,钱包服务器可以显示“已批准”状态下的所有微件。在步骤3612处,钱包管理员可以选择要发布的微件。在步骤3614处,钱包管理员可以键入任何评价或标注并选择发布钱包服务器系统管理控制台的一个正在发布的微件。在步骤3618处,钱包服务器可以提示钱包管理员进行确认。在步骤3620处,钱包管理员可以确认微件可以被发布。在步骤3622处,钱包服务器可以将微件的状态改变为“已发布”。在步骤3624处,钱包服务器可以生成用于微件的签名。在方法3600的步骤3628处,钱包服务器可以确认微件可以已经被发布。

[0400] 行为模型-添加微件-图37是用于第一次添加微件连同TSM交互的方法3700。方法3700在步骤3708处可以要求用户使用钱包3702以用于选择微件3704。在步骤3710处,微件脚本组件3712。在方法3700的步骤3718处,脚本组件3712可以与微件管理器3714通信以便检索微件3704的最新版本。在示例中,脚本组件3712可以与微件管理器3714通信以便检索

微件描述符。在示例中,脚本组件3712可以与微件管理器3714通信以便检索微件二进制。在方法3700的步骤3718处,微件管理器3714可以将微件描述符数据块、微件束的散列、MDN和微件实例ID发送给可信服务管理器(TSM)3720。微件管理器3714可以生成微件响应并传送给钱包3702。钱包3702可以包括用于存储来自微件管理器3714的微件二进制和微件响应的数据库。在步骤3728处,TSM 3720可以向安全元件3722添加微件3704。在示例中,安全元件3722可以是钱包小程序。

[0401] 图38是参照微件加载时间签名、核实和执行时间访问核实的用于微件访问核实的系统3800的行为模型。

[0402] 在示例性且非限制性实施例中,钱包3802可以被配置使得用户可以从微件列表中选择微件。钱包3802可以被配置使得钱包3802可以启动由用户选择的微件应用。钱包3802可以与微件管理器3804交互。微件管理器3804可以被配置为初始化资源管理器、控制器,创建默认访问上下文等。在示例中,微件管理器3804可以包括微件列表,并且可以促进通过钱包3802向用户示出微件列表。系统3800可以包括加密解密实用程序(crypto-utility)3808,其可以被配置为从数据库加载微件束。加密解密实用程序3808可以从微件束创建散列,例如,安全散列算法1(SHA1)散列。加密解密实用程序3808可以将散列和微件束传送到微件管理器3804。系统3800可以包括NFC芯片实用程序3810和安全元件或钱包小程序3812。加密解密实用程序3808可以发起请求来核实微件束,并且将请求发送给NFC芯片实用程序3810和钱包小程序3812。NFC实用程序3810可以促进3812的选择。小程序3812可以向微件访问上下文3814发送核实请求。微件访问上下文3814可以核实微件束、微件描述符。在示例中,微件管理器3804可以发起与微件访问上下文3814的通信。微件访问上下文3814可以与访问动作控制器3818进行通信。访问动作控制器3818可以检查认可和访问以用于所选微件的认可。在示例中,当核实可能通过或失败时,可以向用户发送适当消息。系统3800可以包括动作控制器3820,其可以在认可核实之后执行微件请求。访问知晓屏幕控制器3822可以包括在系统3800中,并且被配置为如果可以从访问动作控制器3818接收到认可访问则示出屏幕。系统3800可以包括屏幕控制器3824。屏幕控制器3824可以被配置为在检查到来自微件访问上下文3814的显示认可之后在钱包3802上显示屏幕。

[0403] 用于安全个性化交易的多域生态系统中的移动交易平台的方法和系统可以提供用于安全商务和支付交易的动态生态系统中的移动交易平台的协议抽象的方法。所述移动交易平台可以是运营商等级(carrier-grade)基础设施平台,其促进安全交易服务的开发以及在空中和通过NFC邻近性二者将所述安全交易服务递送到广泛的移动电话环境。所述方法可以包括使原始方法的信息元素分开,并将原始方法的信息元素映射到公共格式的新信息字段。这些新信息字段可以是空的、被填充的,或者通过标记化或一些其它转化方法被转化。该公共格式可以工作用于不同的输入协议,并且递送单个输出协议。该公共格式可以是与每个协议的数据结构一致的元模型。公共模型可以是服务抽象模型,其可以操控底层协议内的原生序列流。输入协议可以是销售点协议、NFC协议、信用卡协议、借记卡协议、票务协议、EPSON Esc/POS协议、UTC标准协议、AEDEX协议、ICD 2002协议、最终协议(Ultimate protocol)、CD 5220协议、DSP-800协议、ADM 787/788协议、HP协议、统一POS协议、用于销售点的OLE协议、JavaPOS、基于云的协议等等。

[0404] 可以经由通信链路在移动设备与销售点设备之间执行协议抽象的方法。移动设备

可以是智能电话、平板计算机、膝上型计算机等等。移动设备可以运行操作系统,诸如iOS、Android、Windows等等。移动设备可以运行应用,诸如容器、微件、钱包等等。应用可以存储与软卡相关的信息。软卡可以是信用卡、忠诚卡、礼品卡、储值卡、票据卡等等。可以从来自多个生态系统的多个服务提供者通过多个运营商或网络提供者来发行软卡。可以通过并由供应架构来供应、维护和使能软卡。供应架构可以包括移动使能层、服务层和软件开发套件。销售点设备可以是在邻近环境中操作的真实世界销售点设备,或者是在远程环境中操作的虚拟世界销售点设备。通信链路可以是有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。

[0405] 协议抽象的方法可以包括用于安全商务和支付交易的动态生态系统中的移动交易平台的标记化能力。该移动交易平台可以是运营商等级基础设施平台,其促进安全交易服务的开发以及在空中和通过NFC邻近性二者将安全交易服务递送到广泛的移动电话环境。标记化能力可以取得私人信息并用标记来替代它。私人信息可以包括pin号码、信用卡号、主账户号、其它个人可识别信息等等。标记可以由以下各项一致:数字字符、字母字符、字母和数字字符的组合、其中字母和数字字符替代主账户号的中间数位的截取的主账户号等等。标记可以是一次性使用标记。标记可以由用于安全商务和支付交易的动态生态系统中的可信实体发行。可信实体可以是位于支付网关、获取者或发行者处的服务器。标记可以生成成为数学可逆加密函数、单向不可逆加密函数,或者通过索引函数、序列号或随机生成的号码来指派。

[0406] 参照图39,图示了根据示例性且非限制性实施例的用于安全商务和支付交易的动态生态系统。用于安全商务和支付交易的动态生态系统3902包括销售点终端3908、在移动设备上运行的应用3910、销售点设备3908与移动设备上运行的移动应用3910之间的通信链路。与单个域3914相关联的单个协议3912可以连接销售点设备3908和在移动设备上运行的移动应用3910。

[0407] 继续参照图39的用于安全商务和支付交易的动态生态系统3904,与多个域3918相关联的多个协议3916可以连接销售点设备3908和在移动设备上运行的移动应用3910。

[0408] 继续参照图39的用于安全商务和支付交易的动态生态系统3906,与多个域3918相关联的多个协议3916可以通过使用封装器3920来抽象,如本说明书中之前所描述的,用以连接销售点设备3908和在移动设备上运行的移动应用3910。

[0409] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统在安全个性化交易中抽象协议的方法。该方法包括在多域生态系统中的联网设备处接收安全个性化交易中的电子交易消息,其包括多个信息字段。该方法此外可以包括用设备来确定多个信息字段中每一个的类型和内容。该方法此外可以包括将多个信息字段的至少一部分映射到公共格式消息字段。该方法此外可以包括基于映射来配置公共格式交易消息。该方法此外可以包括将公共格式交易消息从联网设备传输到多域生态系统中的第二联网设备。

[0410] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统在安全个性化交易中抽象协议的方法。该方法包括在多域生态系统中的联网设备处接收安全个性化交易中的电子交易消息,其包括多个信息字段。该方法此外可以包括用设备来确定多个信息字段中每一个的类型和内容。该方法此外可以包括用元模型将多个信息字段的

至少一部分映射到公共格式消息字段,所述元模型提供安全个性化交易协议的一致映射。该方法此外可以包括基于映射来配置公共格式交易消息。该方法此外可以包括将公共格式交易消息从联网设备传输到多域生态系统中的第二联网设备。

[0411] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统在安全个性化交易中抽象协议的方法。该方法包括在多域生态系统中的联网设备处接收安全个性化交易中的电子交易消息,其包括多个信息字段。该方法此外可以包括用设备来确定多个信息字段中每一个的类型和内容。该方法此外可以包括将多个信息字段的至少一部分映射到公共格式消息字段。该方法此外可以包括基于映射来配置公共格式交易消息。该方法此外可以包括在协议抽象内容封装器中封装公共格式交易。该方法此外可以包括将经封装的公共格式交易消息从联网设备传输到多域生态系统中的第二联网设备。

[0412] 参照图40,图示了根据示例性且非限制性实施例的在用于安全商务和支付交易的动态生态系统4002中的协议抽象的方法。销售点设备4004可以连接到运行在移动设备4008上的移动钱包4006。多个移动钱包可以在移动设备上运行。销售点设备4004可以通过通信链路4010与在移动设备4008上运行的移动钱包4006通信。通信链路4010可以有有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。

[0413] 继续参照图40,在移动设备4008上运行的移动钱包4006可以经由协议通过网络或无线提供者4014和网络4022与服务提供者4012通信。网络4022可以是基于网际协议的网络。经封装的获取信道4016可以被建立来促进在销售点设备4004、运行在移动设备4008上的移动钱包4006以及获取者设施4018之中的协议抽象的通信。如之前在本说明书中所描述的可以封装用于通信的协议的经封装的获取信道4016可以促进经由标准化通信协议在销售点设备4004与运行在移动设备4008上的移动钱包4006之间交换电子交易信息,该交换对于移动设备4008的用户是无缝的。移动设备4008的用户可以在销售点处操作移动设备,而不必知道在POS交易期间使用的协议类型。以这种方式,仅支持非基于IP的交易流的传统POS设备和能够支持聚集的协议交易流(例如,通过IP网络)的POS设备可以由用户无缝地操作。在移动设备4008上运行的移动钱包4006可以经由协议通过获取者4018和网络4022与服务提供者4012通信。网络4022可以是基于网际协议的网络。销售点设备4004可以经由现有的直接交易信道4020来通信。现有的直接交易信道可以是非基于网际协议的信道4020。

[0414] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统进行安全个性化交易的方法。该方法包括在多域生态系统中的联网设备处接收安全个性化交易中的电子交易消息,其包括多个非机密信息字段。该方法此外可以包括在联网设备处配置包括非机密信息和交易标识信息的标记。该方法此外可以包括将标记电子地传输到电子交易消息的源和传输到布置于多域生态系统中的服务提供者服务器。该方法此外可以包括将标记的认证连同标记标识信息一起从电子交易消息的源传输到服务提供者服务器以用于认证由标记所标识的交易。在示例中,服务提供者可以是器件发行者。在示例中,服务提供者可以访问联网设备不可访问的机密信息,以促进认证由标记标识的交易。机密信息可以与数字钱包相关联,该数字钱包布置于从其传输标记认证的设备上。在示例中,传输标记认证可以由在电子交易消息源自的设备上执行的提供者特定的微件来促进。

[0415] 参照图41,图示了根据示例性且非限制性实施例的在用于安全商务和支付交易的动态生态系统4102中的使交易内容标记化的方法。

[0416] 销售点设备4104可以由并入了请求执行诸如购买之类的电子交易的移动钱包4106的移动电话的附近存在来激活。POS设备4104和移动钱包4106可以交换描述所请求的交易的非个人信息(项目、花费、日期/时间、POS身份、POS服务提供者身份等)连同由移动钱包4106生成的唯一标识符。POS设备 4104可以向移动钱包4106发行在安全编码中并入该信息的标记,并且还可以向支付管理机构提交发行的标记的版本,所述支付管理机构诸如可能已经由移动钱包4106指定的发行银行4112。

[0417] 移动钱包4106和发行银行4112可以随后交换如标记中所描述的与交易相关的信息以完成交易。在示例中,移动钱包可以向发行银行提交包括对标记的引用(例如,标记ID)的查询,其可以向发行银行信号通知在标记中标识的交易是授权的。可替换地,发行银行可以向移动钱包提交针对标记中所引用交易的授权的请求。从POS设备4104和从发行银行4112接收的标记的交易信息可以相比较并呈现给移动设备4108的用户以进行认证。以这种方式,可以执行交易,而无需POS设备4104或POS通信路径中的其它实体具有对任何用户机密、个人或金融信息的访问,因为用户/移动钱包的所有机密、个人和金融信息可以保留在后端服务器(例如,发行银行4112)上,并且可以通过在移动钱包4106、POS设备4104、获取信道4120以及诸如发行银行4112之类的支付促进者之中交换的标记来间接访问。

[0418] 销售点设备4104可以连接到在移动设备4108上运行的移动钱包4106。多个移动钱包可以在移动设备上运行。销售点设备4104可以通过通信链路4110或基于可视信息交换(例如,QR码或条形码等)来与运行在移动设备4108上的移动钱包4106通信。通信链路4110可以是有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。可视信息交换可以包括用相机接收图像和/或在电子显示器上显示图像。

[0419] 继续参照图41,销售点设备4104可以从运行在移动设备4108上的移动钱包4106接收私人信息,存储私人信息,然后将私人信息发送给发行银行以供授权。发行银行可以直接通过空中接口4114或者通过服务提供者4116和网络4118来接收私人信息。在授权时,发行银行4112就可以用标记来替代私人信息。标记可以由以下各项一致:数字字符、字母字符、字母和数字字符的组合、其中字母和数字字符替代主账户号的中间数位的截取的主账户号等等。标记可以是一次性使用标记。标记可以由用于安全商务和支付交易的动态生态系统中的可信实体发行。可信实体可以是位于支付网关、获取者或发行者处的服务器。标记可以生成为数学可逆加密函数、单向不可逆加密函数,或者通过索引函数、序列号或随机生成的号码来指派。然后,发行银行4112可以将标记返回到销售点设备4104。然后,销售点设备4102可以用标记来替代私人信息,并且存储标记。标记可以包含在封装器中,如之前在本说明书中所描述的,并且可以通过经封装的获取信道4120在运行在移动设备4108上的移动钱包4106、销售点设备4104以及获取银行4112之中传送。

[0420] 继续参照图41,在移动设备4108上运行的移动钱包4106可以建立与发行银行4112的安全信道。在授权时,发行银行4112可以生成标记并将其映射到存储在发行银行4112处的私人信息。标记然后将被发送到在移动设备4108上运行的移动钱包4106,并且在移动设备4108上运行的移动钱包4106将使用标记来在销售点设备4104处完成交易。在移动设备4108上运行的移动钱包4106可以在个性化移动钱包4106时生成并存储标记栈,并且使用这些标记来在销售点设备4104处完成交易。在移动设备4108上运行的移动钱包4106可以在交易时生成并使用标记来在销售点设备4104处完成交易。

[0421] 参照图42,图示了根据示例性且非限制性实施例的在用于安全商务和支付交易的动态生态系统4202中的交易内容的动态标记化的方法。销售点设备4204可以连接到在移动设备4208上运行的移动钱包4206。多个移动钱包可以在移动设备上运行。销售点设备4204可以通过通信链路4210来与在移动设备4208上运行的移动钱包4206通信。通信链路4210可以是有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。可视信息交换可以包括用相机接收图像和/或在电子显示器上显示图像。

[0422] 继续参照图42,销售点设备4204可以从在移动设备4208上运行的移动钱包4206接收动态标记。动态标记可以是在个性化移动钱包4206时、在交易时等等由运行在移动设备4208上的移动钱包4206生成的动态标记之一。然后,销售点设备4204可以向发行银行4212发送动态标记以供验证。然后,发行银行4212可以经由空中接口4214通过验证标记和发行银行4212所知道的移动链路ID来验证标记,所述移动链路ID与生成该标记的移动钱包4206所驻留在的移动设备4208相关联。在验证了标记和移动链路ID时,发行银行4212于是授权销售点设备4204上的支付和移动钱包4206上的结算。

[0423] 本文描述的多域生态系统安全个性化交易的方法和系统包括标记移动缓存的方法,其包括用联网的服务器生成用于通过公共网络与客户端设备执行电子交易的标记。该方法此外可以包括通过公共网络向客户端设备提供标记。该方法此外可以包括在服务器可访问的存储器中存储标记,连同唯一地标识标记被提供给的客户端的信息。该方法此外可以包括将所存储的唯一地标识标记被提供给的客户端的信息与用标记接收的客户端标识信息进行比较以确定进行电子交易是否应当被认证。该比较可以在服务器处响应于从客户端设备接收电子消息而执行,以通过公共网络提供使用标记来进行电子交易。在示例中,电子消息可以包括从与标记被提供到的客户端相关联的安全元件得到的信息。

[0424] 为了增强移动交易安全性,如本文描述的标记化可以促进减少在设备之中的机密信息交换。然而,即便是标记也可能被第三方捕获并尝试用于未授权的交易。因此,对与标记化相关的移动信息的缓存可以确保标记是从其被递送到的移动设备接收的。这可以通过以下来实现:通过标记发行者(例如,发行银行)与POS/服务提供者之间的安全获取信道共享标记和移动标识信息,使得当移动设备提供标记时,如果移动设备标识信息不匹配标记,则可以拒绝交易。同样地,对与标记相关联的移动相关信息的缓存可以保留在诸如发行银行之类的支付促进者处。该信息可以与来自POS设备的标记化的获取交易相比较。在示例中,移动设备和银行可以通过IP网络交换信息,使得将标记提供给移动设备以用于进行一个或多个POS交易。移动设备可以将标记连同移动设备标识信息一起提交给POS设备。该组信息可以可选地进一步被标记化和/或作为集合发送给发行银行(例如,通过安全获取信道)。发行银行可以将所缓存的与从POS设备接收的标记相关联的移动相关信息与从POS接收的移动设备信息相比较,并且只有信息顺利地比得上才授权交易。

[0425] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统在安全个性化交易中将封装器标记化的方法。该方法可以包括在多域生态系统中的联网设备处接收安全个性化交易中的电子交易消息,其包括多个信息字段。该方法此外可以包括用设备来确定多个信息字段中每一个的类型和内容。该方法此外可以包括将多个信息字段的至少一部分映射到公共格式消息字段。该方法此外可以包括基于映射来配置公共格式交易消息。该方法此外可以包括在协议抽象内容封装器中封装公共格式交易。该方法此外可

以包括配置包括协议抽象内容封装器的标记。该方法此外可以包括将经封装的公共格式交易消息从联网设备传输到多域生态系统中的第二联网设备。

[0426] 参照图43,图示了根据示例性且非限制性实施例的在用于安全商务和支付交易的动态生态系统中生成用于穿过网络的安全内容的电子交易封装器的标记的方法。用于特定生态系统的协议4302可以用于在用于安全商务和支付交易的动态生态系统内存储和传送协议私有信息元素4304。协议私有信息元素可以包括信用卡有效期、主账户号(PAN)、卡持有者姓名、卡持有者地址等等。协议4302可以以特定顺序或配置来组织协议私有信息元素4304。例如,有效期可以保持在第一位置中、主账户号在第二位置中、卡持有者姓名在第三位置中,并且卡持有者地址在第四位置中。协议4302可以以特定配置来存储协议私有信息元素4304。例如,协议4302可以以MM/YYYY格式存储信用卡有效期。

[0427] 继续参照图43,封装器4306可以用于在用于安全商务和支付交易的动态生态系统之中存储和传送用于多个生态系统的封装器私有信息元素4308。封装器私有信息元素可以包括信用卡有效期、主账户号(PAN)、卡持有者姓名、卡持有者地址、账户余额、信用限制等等。封装器4306可以以特定顺序或配置来组织封装器私有信息元素4308。例如,主账户号可以保持在第一位置中、有效期在第二位置中、卡持有者姓名在第三位置中、卡持有者地址在第四位置中、账户余额在第五位置中,以及信用限制在第六位置中。封装器4306可以以特定配置来存储协议私有信息元素4304。例如,封装器4306可以以YYYY/MM格式存储信用卡有效期。

[0428] 继续参照图43,交易过程4310可以用于将协议私有信息元素4304映射到封装器私有信息元素4308。例如,交易过程4310可以从协议4302的第一位置取得有效期协议私有信息元素,并将其放置在封装器4306的第二位置中,并转换私有信息元素的配置MM/YYYY以匹配封装器信息元素YYYY/MM的配置。

[0429] 继续参照图43,标记化过程4314可以用于用标记4312来替代封装器私有信息元素。标记4312可以由以下各项一致:数字字符、字母字符、字母和数字字符的组合、其中字母和数字字符替代主账户号的中间数位的截取的主账户号等等。标记4312可以是一次性使用标记4312。标记4312可以由用于安全商务和支付交易的动态生态系统中的可信实体发行。可信实体可以是位于支付网关、获取者或发行者处的服务器。标记4312可以生成为数学可逆加密函数、单向不可逆加密函数,或者通过索引函数、序列号或随机生成的号码来指派。

[0430] 本文描述的多域生态系统安全个性化交易的方法和系统包括通过多域生态系统在安全个性化交易中将封装器标记化的方法。该方法可以包括在多域生态系统中的联网设备处接收用于安全个性化交易中的电子交易消息的封装器。该方法此外可以包括在联网设备处配置包括封装器和交易标识信息的标记。该方法此外可以包括将标记电子地传输到用于电子交易消息的封装器的源,以及传输到布置于多域生态系统中的服务提供者服务器。该方法此外可以包括将标记的认证连同标记标识信息一起从用于电子交易消息的封装器的源传输到服务提供者服务器以用于认证由标记标识的交易。在示例中,服务提供者可以是器件发行者。在示例中,服务提供者可以访问联网设备不可访问的机密信息,以促进认证由标记标识的交易。在示例中,机密信息可以与数字钱包相关联,该数字钱包布置于从其传输标记认证的设备上。在示例中,传输标记认证可以由在用于电子交易消息的封装器源自的设备上执行的提供者特定的微件来促进。

[0431] 参照图44,图示了根据示例性且非限制性实施例的在用于安全商务和支付交易的动态生态系统4402中对交易封装器进行标记化的方法。销售点设备4404可以连接到在移动设备4408上运行的移动钱包4406。在示例性且非限制性实施例中,多个移动钱包可以在移动设备上运行。销售点设备4404可以通过通信链路4410与在移动设备4408上运行的移动钱包4406通信。通信链路4410可以是有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。

[0432] 继续参照图44,在移动设备4408上运行的移动钱包4406可以建立与发行银行4412的安全信道。安全信道4414可以直接建立在运行在移动设备4408上的移动钱包4406之间,或者通过空中接口4414(诸如通过服务提供者4416和网络4418)来建立。在授权时,发行银行4412可以生成标记并将其映射到存储在发行银行4412处的封装器信息。标记然后将被发送到在移动设备4408上运行的移动钱包4406,并且在移动设备4408上运行的移动钱包4406将使用标记来在销售点设备4404处完成交易。在移动设备4408上运行的移动钱包4406可以在个性化移动钱包4406时生成并存储标记栈,并且使用这些标记来在销售点设备4404处完成交易。在移动设备4408上运行的移动钱包4406可以在交易时生成并使用标记来在销售点设备4404处完成交易。

[0433] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于在用于安全个性化交易的多域生态系统中执行标记化的电子交易的方法。该方法包括生成表示电子交易消息的标记,该电子交易消息标识至少一个交易和交易中的至少一个生态系统参与者。该方法此外可以包括封装表示电子交易消息的标记,并提供可以包括表示电子交易消息的标记的封装器。该方法此外可以包括生成表示封装器的标记,并提供用于电子消息的标记化表示的标记化封装器。该方法此外可以包括通过在两个参与者之间传输标记化的封装器来执行生态系统中两个参与者之间的电子交易。在示例中,生态系统中两个参与者之一可以是至少一个生态系统参与者。

[0434] 参照图45,图示了根据示例性且非限制性实施例的通过传输动态生成的标记化封装器来执行跨开放网络的电子交易的方法,所述封装器包括表示用于安全商务和支付交易的动态生态系统4502中的交易内容的标记。销售点设备4504可以连接到在移动设备4508上运行的移动钱包4506。多个移动钱包可以在移动设备上运行。销售点设备4504可以通过通信链路4510与在移动设备4508上运行的移动钱包4506通信。通信链路4510可以是有线通信链路、无线通信链路、NFC链路、蓝牙链路、局域网链路、广域网链路等等。

[0435] 继续参照图45,销售点设备4504可以从在移动设备4508上运行的移动钱包4506接收标记化的信息,在标记化的封装器中封装标记化的信息,以及将封装器信息发送到移动设备,该移动设备可以将包括标记化内容的标记化封装器传送到与移动钱包相关联的发行银行4512以供授权。移动设备4508可以直接通过空中接口4514或者通过服务提供者4516和网络4518将具有标记化内容的标记化封装器传输到发行银行。标记化的信息和/或标记化的封装器可以由以下各项一致:数字字符、字母字符、字母和数字字符的组合、其中字母和数字字符替代主账户号的中间数位的截取的主账户号等等。标记可以是一次性使用标记。标记可以由用于安全商务和支付交易的动态生态系统中的可信实体发行。可信实体可以是位于支付网关、获取者或发行者处的服务器。标记可以生成为数学可逆加密函数、单向不可逆加密函数,或者通过索引函数、序列号或随机生成的号码来指派。

[0436] 在包括多个获取方法与多个发行银行的交易流中的协议抽象的示例中,商家可能希望利用来自多个发行银行的多个支付信息获取设备,诸如近场通信(NFC)、条形码读取器和蓝牙,以便为商家的客户提供支付方法上的选择。在该示例中,将会在商家的销售点终端处使用协议抽象,以便通过将用于每一个获取设备的单独获取协议抽象成由商家的销售点终端理解的单个协议来允许多个支付获取设备经由诸如网际协议之类的单个通信协议和链路与单个销售点终端通信,所述单个协议然后可以通过一个或多个通信协议和链路而路由到多个发行银行。

[0437] 在包括多个获取方法与单个发行银行的交易流中的协议抽象的示例中,参照图46,商家可能希望利用来自单个发行银行4602的多个支付信息获取设备,诸如近场通信(NFC)4604、条形码读取器4606和蓝牙4608,以便为商家的客户提供支付方法上的选择。在该示例中,将会在商家的销售点终端4610处使用协议抽象,以便通过将用于每一个获取设备的多个获取协议抽象成由商家的销售点终端理解的单个协议来允许多个支付获取设备经由多个协议和链路4612与单个销售点终端通信,所述单个协议然后可以通过单个通信协议和链路4614而路由到发行银行。

[0438] 在包括单个获取方法与多个发行银行的交易流中的协议抽象的示例中,商家可能希望利用单个支付信息获取设备从多个发行银行获取支付信息,诸如近场通信(NFC)、条形码读取器和蓝牙,以便为商家的客户提供支付方法上的选择。在该示例中,将会从商家的销售点终端使用协议抽象,以便允许单个支付获取设备经由诸如网际协议之类的单个通信协议和链路与单个销售点终端通信,然后将用于单个获取设备的单独获取协议抽象成用于多个发行银行的多个通信协议,从而允许适当的交易通过多个通信协议和链路而路由到正确的发行银行。

[0439] 在包括多个获取方法和多个发行银行的空中交易流中的协议抽象的示例中,多个发行银行可能希望向利用诸如近场通信(NFC)、条形码读取器和蓝牙之类的多个支付信息获取设备的商家发送授权信息,以便为商家的客户提供支付方法上的选择。在该示例中,将会在商家的销售点终端处使用协议抽象,以便通过将用于每一个发行银行的单独通信协议抽象成由商家的销售点终端理解的单个协议来允许多个发行银行经由诸如网际协议之类的单个通信协议和链路与单个销售点终端通信,所述单个协议然后可以通过多个通信协议和链路传送到每个获取设备。

[0440] 在包括多个获取方法和单个发行银行的空中交易流中的协议抽象的示例中,单个发行银行可能希望向利用诸如近场通信(NFC)、条形码读取器和蓝牙之类的多个支付信息获取设备的商家发送授权信息,以便为商家的客户提供支付方法上的选择。在该示例中,将会在商家的销售点终端处使用协议抽象,该销售点终端经由诸如网际协议之类的单个通信协议和链路而连接到单个发行银行,并且将用于发行银行的单独通信协议抽象成由每个获取设备理解的多个协议,所述多个协议然后可以通过一个或多个通信协议和链路传送到一个或多个获取设备。

[0441] 在包括单个获取方法和多个发行银行的空中交易流中的协议抽象的示例中(如图47中所图示),多个发行银行4702可能希望向利用诸如近场通信(NFC)设备4704之类的单个支付信息获取设备的商家发送授权信息。在该示例中,将会在商家的销售点终端4710处使用协议抽象,以便通过将多个发行银行所使用的多个通信协议和通信链路4712抽象成由商

家的销售点终端理解的单个协议来允许多个发行银行经由单个通信协议和链路4714来与单个销售点终端通信,所述单个协议然后可以经由单个通信协议和链路4712而传送到单个获取设备。

[0442] 在标记化交易、标记化协议抽象和标记化封装器的示例中,参照图48,用户可以在销售点系统4806处向商家的NFC读取器4804呈现NFC使能的智能电话4802。NFC使能的智能电话4802动态地生成包含用户的信用卡号和有效期的标记,并通过NFC读取器4804将标记传递到销售点系统4806。销售点系统4806将标记传递到在发行银行4810处的移动交易平台服务器4808。发行银行4810处的移动交易平台服务器4808通过使用仅驻留在移动交易平台服务器上的密钥来解密标记,对交易进行认证,以及将授权码发送回销售点系统4806。然后,销售点系统4806通过NFC读取器4804完成与用户的交易。

[0443] 此外,在该示例中,多个发行银行可能希望向利用诸如近场通信(NFC)、条形码读取器和蓝牙之类的多个支付信息获取设备的商家发送授权信息,以便为商家的客户提供支付方法上的选择。在该示例中,可以在商家的销售点终端处使用协议抽象,以便通过将用于每一个发行银行的单独通信协议抽象成由销售点终端理解的单个协议来允许多个发行银行经由诸如网际协议之类的单个通信协议和链路与单个销售点终端通信,所述单个协议然后可以经由多个通信协议和链路而传送到每个获取设备。

[0444] 而且,用户A可以向使用协议X的商家NFC读取器呈现NFC使能的智能电话,并且用户B可以在销售点系统处向使用协议Y的商家条形码读取器呈现在智能电话上显示的条形码。这两个用户的智能电话动态地生成包含相应用户的信用卡号和有效期的标记,并且通过用于用户A的NFC读取器和用于用户B的条形码读取器而将标记传递到销售点系统。销售点系统将由NFC和条形码读取器用于与销售点通信的不同协议抽象成单个协议,所述单个协议可以用于经由单个协议和单个通信链路将用于这两个标记的信息传送到发行银行处的移动交易平台服务器。发行银行处的移动交易平台服务器通过使用仅驻留在移动交易服务器上的密钥来解密标记,对交易进行认证,以及将授权码发送回销售点系统。然后,销售点系统将经抽象的协议转换回由NFC和条形码读取器使用的单独协议以完成与用户A和用户B的交易。

[0445] 在可替换示例中,发行银行可能希望向利用诸如近场通信(NFC)、条形码读取器和蓝牙之类的多个支付信息获取设备的商家发送授权信息,以便为商家的客户提供支付方法上的选择。在该示例中,可以在商家的销售点终端处使用标记化的封装器,以便通过将用于每一个发行银行的单独通信协议抽象成由销售点终端理解的单个协议来允许多个发行银行经由诸如网际协议之类的单个通信协议和链路与单个销售点终端通信,所述单个协议然后可以经由多个通信协议和链路传送到每个获取设备。在又一示例中,用户A可以向使用协议X的商家NFC读取器呈现NFC使能的智能电话,并且用户B可以在销售点系统处向使用协议Y的商家条形码读取器呈现在智能电话上显示的条形码。这两个用户的智能电话发送相应用户的信用卡号和有效期,并且通过用于用户A的NFC读取器和用于用户B的条形码读取器而将信用卡号和有效期传递到销售点系统。销售点系统将由NFC和条形码读取器用于与销售点系统通信的不同协议封装成单个协议,所述单个协议可以用于经由单个协议和单个通信链路将用于信用卡号和有效期二者的信息传送到发行银行处的移动交易平台服务器。发行银行处的移动交易平台服务器用标记替代信用卡号和有效期,并将标记发送回销售点系

统。然后,销售点系统将经封装的标记转换回由NFC和条形码读取器使用的单独协议并将标记传递回NFC和条形码读取器。然后,NFC和条形码读取器用标记替代信用卡号和有效期。

[0446] 本文描述的多域生态系统安全个性化交易的方法和系统包括移动交易处理系统,其包括部署在网络中的多个服务器和多个客户端设备。每个服务器可以被配置为促进网络中的多个客户端设备和多个服务提供者服务器之中的安全个性化交易。此外,多个客户端设备中的至少一个可以配置有在基于容器的执行环境中可操作的可容纳多租户(multi-tenant capable)的钱包。钱包可以通过微件可访问的,该微件可以布置于多个客户端设备的至少一个上。另外,多个服务器可以此外被配置为促进在通过微件的多个客户端设备中至少一个与通过多个信任模型中任一个的多个服务提供者服务器中至少一个之间的交易,所述信任模型包括单个信任域、单个信任集群、多个信任集群以及直接信任关系。在示例中,多个不同信任模型可以包括单个信任域、单个信任集群、多个信任集群以及直接信任关系中的至少一个。在示例中,单个信任域可以包括中央钱包服务中心服务器,其可以与用户设备上的电子钱包相接口。中央钱包服务中心服务器可以促进建立与可信服务提供者的安全交易信道。在示例中,单个信任集群可以包括可信第三方服务器和钱包服务中心服务器,所述可信第三方服务器用于与个人电子钱包安全地交换机密钱包信息,所述钱包服务中心服务器用于促进由多个服务提供者中的每一个经由第三方服务器对用户的直接认证。在示例中,钱包服务中心服务器可以向多个服务提供者中的至少一个递送用户标识和安全性密钥。在示例中,多个信任集群可以包括多个不同的可信第三方。每个第三方可以至少配置有用于以下的服务器:与个人钱包交换机密钱包信息,并且此外与多个集群特定的服务提供者交换由钱包服务中心提供的用户和/或设备标识。

[0447] 在示例中,直接信任关系可以包括归属钱包服务中心服务器,用于建立与电子钱包的交易上下文。归属钱包服务中心服务器可以促进直接在电子钱包与服务提供者之间建立经认证的交易信道。在示例中,微件可以被配置用于与特定提供者的安全交互。在示例中,微件可以被配置用于通过中介与特定提供者的安全交互。在示例中,微件可以在空中通过移动设备与相关联于特定提供者的联网服务器之间的电子交互而配置在移动设备上。

[0448] 如本文所描述的移动交易平台可以促进经由多个不同信任模型在生态系统中进行安全个性化交易。在生态系统中的客户端设备与生态系统中的服务提供者服务器等之间的每个交易可以基于与交易、生态系统配置等相关的各种因素经由不同信任模型来进行。同样地,生态系统中的服务提供者或其他参与者可以确定通过其来进行与服务提供者的交易的优选或默认信任模型。通过提供对交易特定的信任模型确定的支持,平台可以促进可能受多个因素影响的动态信任模型确定和交易使用,所述多个因素包括交易因素、生态系统实例化因素、服务提供者偏好因素、移动网络提供者偏好等。

[0449] 信任模型可以包括单个信任域模型、单个信任集群模型、多个信任集群模型、直接信任关系等。单个信任域模型由移动设备与移动交易平台服务器(本文中也称为钱包服务中心(WSC)服务器)之间的一对一关系来表征。然而,WSC经历与隐式可信服务提供者的一对多关系。设备钱包和WSC为依赖于WSC的服务提供者操控用户认证、支付认证等,以确保交易和终端用户完整性。图49描绘了单个信任域模型的实施例。设备钱包4902以一对一关系直接与WSC服务器4904通信,如上文所描述的。多个可信服务提供者服务器4908a和4908b中的每一个通过网络与WSC服务器4904通信。WSC服务器4904可以执行所有钱包和用户相关认

证、验证、支付批准等，而服务提供者4908出于该目的而隐式地信任WSC服务器4904。钱包4902的用户可以通过WSC服务器4904来与各种服务提供者4908中任一个进行交易，而无需与服务提供者共享机密或个人可识别的信息。

[0450] 信任模型还可以包括如图50中所描绘的单个信任集群模型，其假设可信第三方(TTP)5002在生态系统中是可访问的。服务提供者4908既不经由设备4902维持与终端用户的直接信任关系，也不维持与WSC 服务器4904的隐式信任关系。替代地，WSC 服务器4904执行用户/移动设备4902的认证，并且可以经由移动设备4902可以显式提供给TTP 5002的票据或标记来共享这样的认证，在TTP 5002中，可以完成终端用户4902与服务提供者4908之间的交易。MTP服务器维持与TTP 5002的强关系，并且充当用户注册实体。例如，在PKI认证中，MTP服务器充当RA(注册管理机构)，而CA(证书管理机构)被认为是TTP 5002。如所注意到的，服务提供者不一定信任MTP服务器用于认证；然而，MTP服务器被信任为标识提供者(IdP)。每个服务提供者4908可以通过使用由MTP服务器转发的证书来认证由该ID标识的用户。经由钱包4902与TTP 5002之间的显式信任关系来进行交易，其中，钱包和TTP可以安全地彼此标识和认证。钱包的证书不需要与MTP服务器共享。

[0451] 信任模型可以包括如图51中所描绘的多个信任集群模型，其可以包括用于多个服务提供者集群5102中每一个的不同TTP 5002。每个集群特定的TTP可以与钱包4902建立直接信任。MTP服务器执行用户注册、身份提供等，如关于图50所描绘和描述的。

[0452] 信任模型还可以包括如图52中所描绘的直接信任关系，其中，没有两个实体被强制彼此信任。每个服务提供者5204维持与用户/客户端4902的直接证书，并且直接认证。

[0453] 该模型的主要特性包括：钱包/用户4902分离地维护用于每个服务提供者5204的证书。对于每个交易/服务，钱包必须由服务履行中涉及的每个实体所认证。MTP服务器不控制交易的所有方面；相反，在每个服务提供者之间共享交易上下文。钱包可以使用与服务提供者的任何类型的认证，只要其满足服务提供者的安全性/风险要求即可。在示例中，对于账单发行者，认证可以如用户的邮编和母亲的婚前姓氏一样简单。对于支付服务提供者，这可以是信用卡CVV或VbV/安全码口令。可以在直接信任关系模型中并入其它认证方法，无限制地包括用户、设备和域的三维认证。

[0454] 用多个信任模型进行交易处理的方法和系统可以包括提供能够在多个不同信任模型的情况下操作的用于安全个性化交易的多域生态系统平台。在这样的方法和系统中，移动交易处理系统可以配置有部署在网络中的多个服务器和多个客户端设备。每个服务器可以被配置为促进网络中的多个客户端设备和多个服务提供者服务器之中的安全个性化交易。所述系统可以包括多个客户端设备中的至少一个，所述客户端设备配置有在基于容器的执行环境中可操作的可容纳多租户的钱包，其中，钱包是通过微件可访问的，所述微件布置于多个客户端设备的至少一个上。系统中的多个服务器可以此外被配置为促进在经由微件的多个客户端设备中至少一个与经由多个信任模型中任一个的多个服务提供者服务器中至少一个之间的交易，所述信任模型包括单个信任域、单个信任集群、多个信任集群以及直接信任关系。单个信任域可以包括中央钱包服务中心服务器，其与用户设备上的电子钱包相接口，并且促进建立与可信服务提供者的安全交易信道。单个信任集群可以包括可信第三方服务器和钱包服务中心服务器，所述可信第三方服务器用于与个人电子钱包安全地交换机密钱包信息，所述钱包服务中心服务器用于促进由多个服务提供者中每一个经由

第三方服务器对用户的直接认证,其中,钱包服务中心服务器向多个服务提供者中至少一个递送用户标识和安全性密钥。多个信任集群可以包括多个不同的可信第三方,所述可信第三方各自至少配置有用于以下的服务器:与个人钱包交换机密钱包信息,并且此外与多个集群特定的服务提供者交换由钱包服务中心提供的用户和/或设备标识。同样,直接信任关系包括用于建立与电子钱包的交易上下文的归属钱包服务中心服务器,其促进直接在电子钱包与服务提供者之间建立经认证的交易信道。布置于(多个)客户端设备上的微件可以被配置用于与特定服务提供者的安全交互,或通过中介与特定提供者的安全交互。微件此外可以在空中通过在移动设备与相关联于特定提供者的联网服务器之间的电子交互而配置在移动设备上。

[0455] 本文描述的多域生态系统安全个性化交易的方法和系统包括在移动设备上操作的安全移动钱包。安全移动钱包可以包括多个不同的用户账户。在示例中,可以由提供者特定的信任模型通过布置于移动设备上的微件来促进对不同用户账户的访问。在示例中,微件可以被配置用于与特定提供者的安全交互。在示例中,微件可以被配置用于通过中介与特定提供者的安全交互。在示例中,微件可以在空中通过移动设备与相关联于特定提供者的联网服务器之间的电子交互而配置在移动设备上。

[0456] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于安全个性化交易的生态系统中的用于移动交易的信任模型确定方法。该方法可以包括配置部署在网络中的多个服务器以通过多个信任模型中的任一个来促进客户端设备与提供者特定的服务器之间的交易。多个信任模型可以包括诸如单个信任域、单个信任集群、多个信任集群以及直接信任关系。该方法此外可以包括分析用于移动设备与提供者特定的服务器之间的交易的默认信任模型,以确定与交易相关联的风险度量。该方法此外可以包括基于产生的风险度量、通过默认信任模型和来自多个信任模型的另一信任模型之一来进行交易。在示例中,进行交易可以包括经由在移动设备上执行的提供者特定的微件来访问移动设备上的钱包功能。可以基于产生的风险度量来选择提供者特定的微件。在示例中,风险度量可以基于移动设备的位置。在示例中,风险度量可以基于提供者特定的服务器相对于移动设备的位置。在示例中,风险度量可以基于移动设备正通过其进行交易的网络的各方面。

[0457] 生态系统中的安全个性化交易的方法和系统可以包括能够在多个不同信任模型的情况下操作的移动钱包。这样的安全移动钱包可以在移动或其它客户端设备上操作,并且可以包括多个不同的用户账户。可以由提供者特定的信任模型经由布置于移动设备上的微件来促进对不同用户账户的访问。如上文所注意到的,布置于(多个)客户端设备上的微件可以被配置用于与特定服务提供者的安全交互,或者通过中介与特定提供者的安全交互。还如上文所注意到的,微件此外可以在空中通过移动设备与相关联于特定提供者的联网服务器之间的电子交互而配置在移动设备上。

[0458] 如本文所描述的用于提供用于安全个性化交易的生态系统的移动交易处理系统可以促进用于移动交易的信任模型确定。模型确定可以包括配置部署在网络中的多个服务器以经由多个信任模型中任一个来促进客户端设备与提供者特定的服务器之间的交易,所述信任模型包括单个信任域、单个信任集群、多个信任集群以及直接信任关系。模型确定此外可以包括分析用于移动设备与提供者特定的服务器之间的交易的默认信任模型,以确定与交易相关联的风险度量。基于产生的风险度量,可以经由默认信任模型或从多个信任模

型选择的另一信任模型来进行交易,所述信任模型包括单个信任域、单个信任集群、多个信任集群以及直接信任关系。

[0459] 进行交易可以包括经由在移动设备上执行的提供者特定的微件来访问移动设备上的钱包功能。可以基于产生的风险度量来选择提供者特定的微件,所述风险度量可以基于移动设备的位置,或基于提供者特定的服务器相对于移动设备的位置的位置。同样,风险度量可以基于移动设备正通过其进行交易的网络的各方面。

[0460] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于使用在生态系统中的域特定的程序语言。生态系统可以包括器件发行者、服务提供者、获取者以及客户端。域特定的程序语言可以包括可以顺从诸如XML、CSS和Java脚本的语法。所述语言此外可以包括可以在客户端设备上使能钱包相关功能的对象。在示例中,所使能的钱包相关功能可以是钱包容器、钱包、微件和钱包伴随小程序中的至少一个。

[0461] 促进多域生态系统中的安全个性化交易的移动交易平台方法和系统可以包括多域生态系统的域特定的语言,其支持XML、CSS、Java脚本等,以用于创建可以被配置以作为容器的运行时组件而操作的钱包和微件。这样的语言可以包括一个或多个对象、标签、元数据元素等,其可以使能容器、钱包、微件、伴随小程序等。多域生态系统的域特定的语言可以提供域特定的Java脚本或XML功能,以访问移动交易平台的各种模块、功能和服务。另外,还可以包括用于使能NFC操作、访问条形码信息等的功能。

[0462] 通过在标准化软件模式(例如,官方语言)内创建域特定的功能集合,域特定的语言通过标准化模式揭示功能,使得用户和软件相关的架构师可以容易地确定域特定的语言正被模式化(patterned)。该域特定的语言应用于本文描述的生态系统的软件编程和模块配置,用以除其它外尤其简化生成用以对该域采取行动的代码。每个域特定的功能可以表示域特定的语言的独特新颖方面。MTP的软件开发环境可以允许将域特定的功能集合用作域特定的语言的变量。在示例中,用钱包使能功能来适配域特定的语言可以提供经修改的语言,所述经修改的语言特别适于使得能够创建支持安全、个性化、移动交易服务的服务的功能开发。开发者可以使用MTP域特定的语言来基于可以专用于创建安全移动交易的功能集合来创建服务。作为域特定的语言,可以提供有原生工具来检查语言;验证其使用;以及确保加密被适当使用。

[0463] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于服务多域生态系统中的安全个性化交易的平台。该平台可以包括解译器,用于解译用于使能钱包相关功能的域特定的程序语言对象,所述钱包相关功能与多个域中至少一个相关。在示例中,解译器可以是运行时解译器。在示例中,解译器可以是在客户端设备上执行的运行时容器。在示例中,所使能的钱包相关功能可以是钱包容器、钱包、微件和钱包伴随小程序中至少一个。

[0464] 除了XML、CSS和Java脚本顺从的语言以外,MTP可以包括域特定的语言解译器,其可以在客户端设备上操作(例如作为运行时客户端的部分)。运行时自身可以是语言解译器,其基于域特定的语言来解释代码并在客户端(例如,移动电话)上执行该功能性。客户端可操作的运行时(例如,容器)可以促进解译域特定的语言元素,其与域相关,所述域诸如本文描述的用于安全个性化交易的多域生态系统。尽管对域特定的语言的描述基于标准语言,所述标准语言是Java脚本、XML和CSS顺从的,但是域特定的语言可以基于几乎任何解释的语言(例如,VB 脚本、visual basic等)。

[0465] 用于在涉及器件发行者、服务提供者、获取者以及客户端的生态系统中使用的此类域特定的编程语言可以包括顺从XML、CSS和Java脚本的语法以及在客户端设备上使能钱包相关功能的域特定的对象/元素/标签。具体地,所使能的钱包相关功能可以是钱包容器、钱包、微件、钱包伴随小程序或其组合。

[0466] 用于服务多域生态系统中的安全个性化交易的平台,诸如MTP,可以包括解译器,用于解译用于使能钱包相关功能的域特定的程序语言对象,所述钱包相关功能与多个域中至少一个相关。解译器可以是运行时解释器、在客户端设备上执行的运行时容器等。同样,所使能的钱包相关功能可以是钱包容器、钱包、微件和钱包伴随小程序中的至少一个。

[0467] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于保护多域生态系统中的内容的一组工具。该组工具可以包括用于构造移动交易生态系统的软件开发套件。该组工具此外可以包括一组域特定的功能,用于使能微件、钱包、容器和伴随小程序中至少一个的客户端侧功能性。该组工具此外可以包括设备不可知应用编程接口。该组工具此外可以包括设备特定的应用编程接口。该组工具此外可以包括用于促进与客户端设备软件和硬件的互操作的使能层功能。该组工具此外可以包括微件公布模块,用以促进提供者特定的微件以供递送和下载到客户端设备的可用性。

[0468] 如本文所描述的,用于移动交易处理平台(MTP)的软件开发套件(SDK)可以促进保护用于安全个性化交易的多域生态系统中的内容。MTP SDK可以为服务提供者编程人员等提供用于实现和配置以下各项的工具来保护内容:交易 workflows、用于在客户端设备上使用的服务提供者特定的微件、包括可以通过API访问的设备特定的且设备不可知的能力的钱包等。SDK利用设备上的运行时容器,其进一步促进隔离微件、钱包等,以促进无缝内容安全性。本文中和别处也称为移动客户端的运行时容器还可以包括用户接口框架和工作流引擎,其提供服务执行、动作、应用(例如,微件)执行控制、脚本化以及用于各种通信信道的通信支持。用于保护用于安全个性化交易的多域生态系统中的内容的MTP工具可以促进开发过程,开发过程包括定义业务需求,创建用户接口流,开发微件、小程序和基于服务器的应用,构建和测试所开发的元件。

[0469] 本文描述的多域生态系统安全个性化交易的方法和系统包括网络使能的服务器,用于配置用于安全个性化交易的多域生态系统的一组服务提供者工具。网络使能的服务器可以包括移动交易平台服务器。网络使能的服务器此外可以包括在平台服务器上可操作的钱包服务中心开发环境。网络使能的服务器此外可以包括在平台服务器上可操作的钱包服务中心运行时模块。网络使能的服务器此外可以包括软件开发套件,用于构造和维护生态系统的基于服务器和基于客户端的元件。在示例中,生态系统的元件可以包括钱包、微件、伴随小程序以及容器。

[0470] MTP可以包括用于配置用于安全个性化交易的多域生态系统的一组服务提供者工具的平台。MTP可以包括网络使能的服务器,用于配置一组服务提供者工具,包括在网络使能的服务器上可操作的钱包服务中心开发环境、在服务器上可操作的钱包服务中心运行时模块,以及软件开发套件,所述套件用于构造和维护生态系统的基于服务器和基于客户端的元件。可以被维护的基于客户端的元件可以包括钱包、微件、伴随小程序、容器等等。

[0471] 移动交易平台的微件配置能力可以包括在生态系统中的客户端设备上可操作的一个或多个应用。(多个)微件配置应用可以包括初始表现为灰色微件的用户接口。所述配

置应用可以包括用户接口,通过该用户接口,微件用户接口图标等可以被置于灰色微件中、在外观和感觉(例如,布局、颜色等)上进行定制,并且保存在客户端设备上以供用作经验证的微件。这样的微件配置应用可以使微件接口的用户特定的定制。

[0472] 本文描述的多域生态系统安全个性化交易的方法和系统包括用于现场定制微件的一部分的移动应用。该移动应用可以包括用户接口模板,用于从在联网服务器上执行的微件开发过程接收微件功能代码和描述符。该移动应用此外可以包括用于促进通过由微件描述符定义的图标而对微件特征和功能进行访问的用户接口。该移动应用此外可以包括用于配置已下载到设备的微件的算法,用户接口可以基于用户接口中检测到的用户动作而显示在该设备上。在示例中,用户接口模板可以是基于微件描述符而自动可配置的。在示例中,用于现场定制微件的一部分的应用可以在移动设备上操作。在示例中,应用可以在移动客户端容器运行时环境内执行。

[0473] MTP可以包括用于现场定制微件的一部分的移动应用,其可以包括:用户接口模板,用于从在联网服务器上执行的微件开发过程接收微件功能代码和描述符;用于促进经由微件描述符定义的图标而对微件特征和功能进行访问的用户接口;以及用于配置已下载到设备的微件的算法,用户接口基于用户接口中检测到的用户动作而显示在该设备上。应用可以基于微件描述符来自动配置用户接口模板。用于现场定制微件的一部分的应用可以被适配以在移动设备上操作。所述应用可以在移动客户端容器运行时环境内执行。

[0474] 本文描述的多域生态系统安全个性化交易的方法和系统包括基于服务器的应用,其包括一组参考移动交易平台服务。所述应用此外可以包括自动化的向导应用,用于访问该组参考服务并基于用户输入来配置来自该组参考服务的至少一个服务。在示例中,自动化的向导应用可以促进基于用户输入来配置以下各项中的至少一个:客户端元件分布、发行者环境、结算环境、聚集服务、交易介质支持、对手持机类型的支持、用户体验、商业模型以及调节考虑事项。

[0475] 本文描述的多域生态系统安全个性化交易的方法和系统包括生态系统配置引导系统,其包括一组参考移动交易平台服务。该生态系统配置引导系统此外可以包括自动化的向导应用,用于接收与期望的生态系统配置相关联的用户输入。自动化的向导应用还可以可操作用于基于用户输入来推荐来自该组参考服务的至少一个服务的配置。在示例中,该组参考服务可以包括诸如分布服务、连续体使用服务、发行者服务、结算服务、聚集服务、交易介质要求、手持机和操作系统考虑、用户体验因素、商业建模以及调节考虑。在示例中,与期望的生态系统配置相关联的用户输入可以是超链接。在示例中,向导可以基于超链接来搜索信息,并且可以填充至少一个参考服务模板。在示例中,超链接可以是去往操作该向导的服务提供者的网站的链接。

[0476] 移动交易平台此外可以包括向导,用以促进配置用于安全个性化交易的多域生态系统的多个方面。该向导可以是自动化应用等,其访问一组参考移动交易平台服务并基于用户输入来配置来自该组参考服务的至少一个服务。在示例中,自动化的向导应用促进基于用户输入来配置以下各项中的至少一个:客户端元件分布、发行者环境、结算环境、聚集服务、交易介质支持、对手持机类型的支持、用户体验、商业模型以及调节考虑。

[0477] 移动交易平台可以可替换地包括生态系统配置引导系统,其可以包括一组参考移动交易平台服务,以及自动化的向导应用,其用于接收与期望的生态系统配置相关联的用

户输入并基于用户输入来推荐来自该组参考服务的至少一个服务的配置。在示例中,该组参考服务可以包括分布服务、连续体使用服务、发行者服务、结算服务、聚集服务、交易介质要求、手持机和操作系统考虑、用户体验因素、商业建模以及调节考虑。

[0478] 该生态系统配置引导系统可以接收超链接作为与期望的生态系统配置相关联的用户输入。向导可以基于超链接来搜索信息,并且可以填充至少一个参考服务模板。

[0479] 在另一示例中,超链接可以是去往操作该向导的服务提供者的网站的链接。

[0480] 在用于安全个性化交易的多域生态系统中的参与者之中的类型-长度可变的数据通信的方法可以包括:在作为多域生态系统中的参与者的生产者服务器处接收纯旧式java对象;将接收到的纯旧式java对象转换成遵照类型长度可变协议的类型长度可变流;以及经由单向消息总线将经转换的对象从生产者传输到多域生态系统中的移动设备参与者。纯旧式java对象可以遵从类型长度可变协议指南。类型长度可变协议可以支持流式传输(streaming)、浮点支持(float support),以及预先考虑的运行时类的类型信息。

[0481] 本方法可以提供用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线。消息总线可以使能在移动交易平台(MTP)内的组件之间的辅助数据的单向交换。消息总线可以是信道不可知的,以允许通过多个信道的数据交换。多个信道可以是专有协议信道、短消息服务(SMS)信道、移动网络运营商的推送通知框架等。专有协议信道可以是类型长度可变(TyLV)协议信道。TyLV协议信道可以使移动设备软件能够与交易平台通信。TyLV协议信道可以促进纯旧式java对象(POJO)转换成TyLV协议流以及TyLV协议流转换成POJO的转换。转换过程可以是自动化的转换过程。转换过程可以要求POJO遵从指南。指南可以要求POJO:是公共定义的类,实现标记接口com.csam.wsc.daf.tyLv.TyLVBindObject,具有均为非最终、非静态、非暂态且公共的数据成员值,为非负数,传递空值而非实际值来指示可选值,不是匿名类,必须提供默认构造器,提供用于解码操作的类的类型信息等等。TyLV协议还可以要求成员值类型被声明。成员值类型可以是:short(短)及其wrapper Short(封装器短)类,int及其wrapper Integer(封装器整数)类,long(长)及其wrapper Long(封装器长)类,Boolean(布尔)及其wrapper Boolean(封装器布尔)类,java.math.BigInteger,字节数组,java.util.Map及其子类型,java.util.List及其子类型,实现TyLVBindObject的合成的用户定义的类型,表示java修改的UTF编码的java.lang.String,java.util.Date,C-SAM定义的com.csam.wsc.core.util.BitSequence类的类型等等。TyLV协议还可以支持其它功能。其它功能可以包括对预先考虑为该类类型的实际数据的运行时类的类型信息、浮点支持、流式传输的继承支持等等。单向交换可以使能数据对象的发送,而不显式要求网络环程(round-trip)。辅助数据可以不是服务请求的主有效载荷。辅助数据可以由可以驻留在移动应用内的消费者接收和消费。移动应用可以是钱包应用等。辅助数据可以由生产者产生和发送。生产者可以是移动交易平台内的组件。

[0482] 用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线可以提供消息。消息可以是可以通过通信链路传输的数据原子分组。消息可以是可以通过消息总线交换的任何商业对象。消息可以由消息ID和有效载荷构成。消息ID可以由系统的开发者确定的消息的唯一标识符。有效载荷可以是在生产者与消费者之间交换的实际数据。有效载荷数据的格式可以是字符串。消息可以由信道上的组件发送。消息可以由接收器组件接收和处理。

[0483] 用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线可以提供消息信道。消息信道可以是发送器组件连接到接收器组件的虚拟管道。发送器组件可以将信息写到消息信道,并且接收器组件可以从消息信道读取信息。

[0484] 用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线可以提供消息类。消息类可以是平台消息或钱包消息。平台消息可以不意味着服务消费,并且可以由运行时消费和应答。开发者可以在Java脚本中接收针对消息的通知,并且消息可以被标志为已消费。消息可能不能够从Java脚本得到应答。可以忽略从Java脚本对平台消息进行应答的尝试。钱包消息可以产生以用于服务消费和从Java脚本进行应答。钱包消息可以由服务器产生,并且可以变换成等效的JSON格式并传递给设备。

[0485] 用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线可以提供用于消费者和生产者。消费者可以是负责消费消息的实体或组件。生产者可以是负责产生消息的实体或组件。消费者可以是在移动设备上运行的应用。生产者可以是服务器组件。生产者可以对着消息ID进行注册。消息ID可以唯一地标识消息。如果数据是由运行时拥有的,则消息的消费者可以是运行时。可以将消息传递到容器应用的中央消息操控功能。当消息由消费者经由消息总线返回给生产者时,生产者可以消费对于由生产者产生的消息的应答。

[0486] 参照图53,图示了根据示例性且非限制性实施例的用于安全商务和支付交易的动态生态系统中的移动交易平台的消息总线通信架构5302。当消息5304通过信道5306到达消息总线5308时,可以消费消息。信道可以是一组消息。信道5306中的消息5304可以是项目,其将被分发给已经用消息总线5308针对其进行注册的消费者。消息可以按它们在信道上的出现顺序来被分发。多个消息5304可以以批背负(batch piggybacked)而分发给相同响应分组。

[0487] 继续参照图53,消费策略5316可以确定用于项目的分发过程。该过程可以是按消息在信道5306上的出现顺序来分发消息5304。多个消息可以以批背负而争给相同响应分组。消费者5310可以当其消费消息5304时发送应答以指示消息5304的成功消费。应答可以保持指示消息5304的成功或未成功消费的值。当移动应用将其下一请求发送到服务器时,应答可以发送回服务器。可以在下一请求期间在下一新应用会话中发送应答。可以由消费者5310即时地和实时地发送应答,从而发起专门响应序列以对消息的处理进行应答(804)。

[0488] 继续参照图53,当要经由消息总线5308发送响应时,生产者5312可以开始消息产生。经注册的生产者可以产生消息并在输出信道上分发它们。然后,消息5304可以被编码,并且然后可以经由消息总线5308发送整个列表。基于服务器的生产者可以产生java对象,java对象然后可以由移动交易平台基础设施转换成等效的JSON对象。产生策略5314可以以生产者注册的次序在输出信道上分发消息。移动交易平台服务器可以提供生产者注册处,其中,开发者注册它们各自的生产者。生产者的注册次序可以是当存在递送消息的机会时调用生产者的次序。

[0489] 根据示例性且非限制性实施例,本公开提供类型映射方案和类型定义规则,用于将任何纯旧式Java对象(POJO)转换成类型长度可变(TyLV)流,并且反之亦然。该方案可以使开发者能够写出基于设备的用例以定义POJO,POJO可以在运行时(on the fly)被转换成对应的TyLV流。在示例中,TyLV流可以根据TyLV协议来使用,该TyLV协议可以使任何基于设

备的软件能够与交易提供者通信以完成任务。

[0490] 在实施例中,运行中的流式传输可以帮助开发者抽象出非本质的流式传输细节。这继而可以使得开发者免于理解大量TyLV协议相关细节。本发明的类型映射方案和类型定义规则可以基于TyLV协议而用在定义基于设备的用例和其它交互中。

[0491] 在示例中,映射和类型定义规则可以定义和使用为指南,诸如用以使得POJO被流式传输(streamed)至TyLV协议。遵循这些定义的指南集合的POJO可以称为TyLV顺从的POJO。在示例中,指南可以包括诸如用以将POJO定义为公共定义的类的规则。此外,POJO可以实现标记接口,诸如com.xyz.wsc.daf.tylv.TyLVBindObject。在这样的实现失败的情况下,可以生成ClassCastException(类转换异常)的性质的运行时错误。在各种实施例中,POJO的数据成员可以是非最终的、非静态的、非暂态的和公共的(而出于流式传输的目的可以忽略所有其它类型的对象)。在实施例中,整数性质的POJO成员可以不提供负值,因为未能这样做可能导致运行时异常,其与诸如“解码器不支持负数的长度计算”的消息一起抛出。指南可以包括用以允许POJO声明诸如以下各项的成员变量的规则:short(短)及其wrapper Short(封装器短)类,integer(整数)及其wrapper Integer(封装器整数)类,long(长)及其wrapper Long(封装器长)类,Boolean(布尔)及其wrapper Boolean(封装器布尔)类,java.math.BigInteger,字节数组,java.util.Map及其子类型,java.util.List及其子类型,实现TyLVBindObject的合成的用户定义的类型,java.lang.String(表示Java修改的UTF编码),java.util.Date, com.csam.wsc.core.util.BitSequence类的类型等等。在示例中,诸如不同于定义的那些,诸如不同于上面提及的那些的类型的变量的规范可能导致运行时异常。在诸如其中对象是聚集对象的情况下,该对象可以被声明为公共内部静态或非静态类。

[0492] 在示例中,按照为Java类格式所指定的规则,编译器可以生成用于非静态内部类的合成字段。

[0493] 在示例中,诸如包含在java.util.Map实例内的键值对可以为类型java.lang.String,并且覆盖Object.toString对于这样的键值对可能不是非常有帮助。

[0494] 在可替换示例中,TyLV协议实现可以允许布尔或布尔数据类型,但是在内部,其可以将该数据类型编码或解码为8比特类型。因此,布尔值真可以看作1,并且布尔值假可以看作0。同样,由TyLV协议支持的类的类型com.xyz.wsc.core.util.BitSequence可以在内部看作整型-32(integer-32)值。此外,数据类型可以以特定格式来字符串化。另外,不可以允许包含零条目的映射,并且空值可以用来将映射表示为可选值。

[0495] 在示例中,使用TyLV协议的系统可以支持由Java平台修改的通用字符集或USC变换格式(UTF)编码定义,因为java.lang.String类型可以是通用字符集或UCS变换格式(UTF)编码的。此外,原语类型成员可以不是可选的。

[0496] 在示例中,字节可以是非空的,并且合成类型可以基于它们的具体类型而非基于它们实现的接口来被声明。

[0497] 在示例中,TyLV协议可以支持同构的、可变长度的、具有相同类型对象的列表。对象类型可以是任何Java类的类型或任何用户定义的类型,并且可以包括封装器类型以支持原语类型数据。

[0498] 在可替换示例中,与POJO相关的附加指南可以包括定义用于任何POJO或任何其成

员变量的规则,使得传递空值而非实际值可以指示可选值。此外,可以定义规则以使得TyLV顺从的POJO可以不支持类型继承。同样,将POJO或任何其成员声明为匿名类可能导致运行时异常。另外,可能需要提供默认构造器,因为TyLV引擎可能不能使用所定义的构造器。

[0499] 在示例中,与POJO相关的附加指南可以包括规则使得TyLV编解码器可能需要用于解码操作的类类型信息,使得TyLV引擎可以正确地标识可以用解码的数据适当填充的BindObject接口实现类型或列表内容对象类型。在示例中,类的类型信息可以被提供为逗号隔开的完全限定(fully qualified)类名字符串值列表。在示例中,下面在此处包括了类的类型信息。

```
Public class Parent implements BindObject {
```

```
Public BindObject child1;
```

[0500]

```
Public int child2;
```

```
Public List child3;
```

```
}
```

[0501] 另外,可以以以下方式提供作为动作配置参数的类类型声明的示例:

[0502] *com.xyz.wsc.comms.Parent, com.xyz.wsc.comms.*

CertificateResponse, com.xyz.wsc.comms.Certificate

[0503] 在以上示例中,父类可以类似于可以由BindObject类型子级(child)1、int类型子级2和列表(List)类型子级3构成的父类类型。同样,在类类型声明示例中,第二类类型声明CertificateResponse(证书响应)可以用于标识子级1的运行时类型信息。类似地,第三类类型声明Certificate(证书)可以标识可以为列表中收集的对象的类型的子级3内容。该列表数据内容可以被提供为像整型、映射那样的任何封装器类型,或者可以是任何其它有效Java类型。如果未提供类类型信息,则可能导致运行时异常。

[0504] 在示例中,可以定义关于使用TyLV协议来流式传输对象图的附加规则。TyLV协议中的对象图的流式传输可以类似于Java对象串行化协议。然而,在TyLV协议中,构成该图的所有对象可以是TyLV顺从的。此外,图的根对象可以几乎始终是实现TyLVBindObject接口的对象。

[0505] 在示例中,TyLV顺从的POJO可以定义为纯值聚集对象,其可以不包含任何功能性。可以出于TyLV流式传输的目的而定义的这些POJO可以仅在其中流式传输是主要目标的场景中使用。此外,可以避免将计算放在POJO中。

[0506] 在示例中,整型数据类型的值的可能范围可以在定义它之前被标识。作为示例,如果对于变量的值的可能范围是已知的,则可以避免定义长变量用于承载可以用短类型容纳的值。为了实现该目的,可以通过诸如预期可能需要传递的最大值来指派类型。然而,在其它实施例中,诸如在最大值的预期是不可能的情況中,可以相应地选择最有适应性的类型。此外,可能明智的是关注代码中的下溢和上溢,这可能涉及数值计算。这可以帮助避免将负值指派给绑定对象成员,该指派可能不被引擎支持。

[0507] 在示例中,TyLV协议可以包括对流式传输的继承支持。此外,当协议改变时,可以

使能负值和浮点支持。同样, TyLV协议可以支持运行时类类型信息到该类类型的实际数据的预先考虑。这可以类似于Java中对象的串行化, 并且可以使解码引擎能够标识正确的实际绑定对象类型或列表内容对象类型。

[0508] 有效POJO的示例可以定义为:

```
Class ValidBindObject implements TyLVBindObject{  
  
    public String member1 ;  
    public int member2 ;  
    public AggregateObject member3 ;  
    public AnotherAggregateObject member4 ;  
    public AnotherAnotherAggregateObject member5 ;  
}
```

```
[0509] public static class AggregateObject implements TyLVBindObject{  
    public int member1 ;  
    public String member2 ;  
}  
  
public class AnotherAnotherAggregateObject implements TyLVBindObject{  
    public int member1 ;  
    public String member2 ;  
}
```

[0510] 无效POJO的示例可以定义为:

```

        class InvalidBindObject implements TyLVBindObject{ @1
            public final String member1 ; &&1
            public static int member2 ; &&2
            private int member3 ; &&3

[0511]    public TyLVBindObject invalidAggregateMember4 = new TyLVBindObject() { @2
        };

        public InvalidBindObject (String value){ @3
            //whatever
        }

        public TyLVBindObject invalidAggregateMember5; @4

```

[0512] 在以上示例中,可以诸如通过@XX来指示错误点,并且可以诸如通过&&来指示被忽略点。在示例中,这些错误可以是运行时错误。

[0513] 根据示例性且非限制性实施例,本文档公开了用于移动支付和移动商务生态系统的MTP 5.x钱包和微件基础设施模型。MTP 5.x模型可以在与MTP 4.x抽象模型相关联的各种特征上解决和并入客户反馈,MTP 4.x抽象模型可以涉及交付抽象模型和依赖于中间件来构建电话应用。模型5.x可以解决的MTP 4.x的示例性特征中的一些可以诸如但不限于客户期望诸如立即并入新电话特征,而不用等待来自中间件提供者的支持;对新专有工具的昂贵培训,这可以包括人力资源(HR)相关关注;从中间件迁移出时所需的大量返工和成本。

[0514] 在示例中,MTP 5.x模型可以支持开发简单性、降低进行中的维护努力以及支持第三方微件的能力。

[0515] 在示例中,MTP 5.x客户端可以为开发者提供灵活性,以诸如使用模型能力中的一个或多个。架构可以包括独立库,所述库可以包含基础设施组件,诸如Comms、NFC、加密等。根据MTP 5.x模型,这些组件可以被提取到独立库中。此外,部分或整个移动应用可以整体构建在原生电话操作系统上。这些部分可以包括用户接口组件、商业逻辑,或移动应用的任何其它组件。此外,可以通过诸如电话独立的应用编程接口(API)层次来支持模型中提供的微件。在示例中,微件还可以使用可以由移动应用提供的编程接口(API),其可以附加于从运行时可获得的应用编程接口(API)。在示例中,模型架构可以允许客户端运行时被捆绑在移动应用内。在可替换示例中,移动应用可以构建在运行时上。

[0516] 在示例中,MTP 5.x架构的模块性可以允许用于移动应用的三种类型的部署。这三种部署模型可以包括诸如独立的原生应用模型、混合生态系统应用模型,以及跨平台生态系统应用模型。可以在本发明的后续描述中更详细地讨论这些模型如下。

[0517] 独立的原生应用模型OM 1.1(为了简单,后文中称为模型1)可以以可能不需要微

件的客户为目标。这可以为这样的客户提供独特和定制的用户体验。模型1可以包括电话操作系统环境,其包括诸如多个移动库。这些库可以由诸如移动应用所使用,所述移动应用诸如移动钱包客户端应用。移动库可以促进客户利用现有移动库来构建移动应用组件,诸如加密组件或Comms组件,而非必须从头开始构建组件。库可以被设计为促进移动交易和钱包相关能力。在示例中,移动库可以耦合到MTP服务器,并且可以为移动应用的客户提供完全开箱即用(out of box)的基础设施解决方案。

[0518] 作为模型1的独立基础设施支持能力的示例,可以通过使用该模型来构建加密组件,使得其可以提供多于仅仅在原生加密操作上的封装器。该组件可以执行为安全性组件,其可以操控诸如以下的功能:密钥生成、密钥管理、个人标识号(PIN)管理等等。

[0519] 在示例中,每个库可以通过其自身来并入,而没有任何外部依赖性。移动应用OM214的开发者可以集成来自第三方源的最佳的种子库以提供完整的移动应用解决方案OM214。

[0520] 混合生态系统应用部署模型(为了描述的简单,后文中也称为模型2)可以以这样的客户为目标:所述客户可能需要独特、原生的体验,连同通过微件的服务扩展性能力。模型2可以包括可以诸如通过电话操作系统来构建的应用编程接口和移动应用。根据模型2,整个客户端运行时软件可以与移动应用捆绑在一起。电话操作系统可以包括可以由诸如移动钱包客户端应用之类的移动应用使用的多个库。模型2还可以包括可以由诸如电话独立的API支持的微件。在示例中,模型2可以能够不在用户体验、性能或应用功能性上折衷。该模型可能具有更高的开发成本,因为诸如移动钱包之类的移动应用的可变部分可以针对每个电话平台而定制地构建。

[0521] 在示例中,模型2的客户端运行时软件可以在原生屏幕与使用可扩展标记语言(XML)通过工具套件所构建的屏幕之间切换。运行时还可以允许集成诸如在Java脚本中开发的动作(其可以通过工具套件)以及通过原生实现而开发的动作。以这种方式,在示例性实施例中,移动应用的大部分(诸如百分之八十)可以利用运行时和工具套件相关的开发效率,而剩余部分可以针对可区分的体验而构建成原生的。可以通过使用工具套件,诸如使用XML、层叠样式表(CSS)以及Java脚本,来构建微件。这可以允许开发者有更大灵活性,同时保持与所有电话平台的更新,因为开发者可以绕过运行时来创建通过运行时可能不是可获得的功能性。在示例中,微件可以能够通过运行时来使用开发支持。然而,微件也可以使用移动应用的展露的应用编程接口(API)来用于开发。微件工具套件可以使生态系统服务提供者更容易且更平滑地开发微件。可以增强应用工具以支持混合组装和包装。

[0522] OM1.3表示 根据MTP 5.x架构的跨平台生态系统应用部署模型。跨平台生态系统应用部署模型(为了简单,后文中也称为模型3)可以是成本有效的模型,其可以以诸如他们的要求可以通过客户端应用运行时的能力来实现的客户为目标。该模型可以包括通过诸如可以包括多个库的电话操作系统所构建的API和移动应用。此外,根据跨平台生态系统应用部署模型,多个微件可以由诸如电话独立的API支持。此外,根据该模型,客户端应用和微件二者可以通过使用可以支持跨平台开发的工具套件来构建。

[0523] 在示例中,模型3可以类似于根据MTP架构的MTP 4.x版本的部署模型,除了与MTP 4.x版本相对地,MTP 5.x可以促进或支持平台扩展。

[0524] 图54图示了根据本发明的示例性实施例的如在服务递送平台生态系统(出于描述

简单的目的,在后文中称为SDP 5408并稍后讨论)的部署中使用的支付促进器系统5400的各种子系统的高层级框图。

[0525] 根据示例性实施例,支付促进器5400内的各种子系统可以包括销售点(POS) 5402终端、诸如移动应用5404之类的应用(APP) 5404、SDP 5408、若干发行者系统,诸如无限制地包括所描绘的发行者系统1 5410、发行者系统2 5412以及发行者系统3 5414。各种子系统可以通过诸如支付处理网络5418之类的网络连接。APP 5404此外可以包括一个或多个微件。

[0526] 图54的支付促进器5400可以促进在诸如POS 5402之类的物理商家POS 5402处利用移动电话来诸如进行商品和服务的支付。因此,移动电话可以用于促进支付,作为对基于塑料的物理交易卡的可替换方案,使得可以通过支付促进器来处理、路由和结算支付交易。因而,可以通过使用支付促进器5400来促进商家,因为其可以减少与交易相关联的整体成本。同样,支付促进器5400可以有利于客户或消费者,因为其提供有奖励的购物或可以节省金钱的交易体验,这诸如通过供应、忠诚度等促销方案或者由于商家从通过使用支付促进器5400的支付过程获得的节省而由商家提供的整体降低的价格。

[0527] 支付促进器5400可以向消费者提供具有跨像发行者的若干发行者的多个支付产品的选择。支付促进器5400可以向消费者提供与其它交易模式相比时改进的支付体验,并且可以与拔出诸如物理皮革钱包、选择卡以及在机器上刷卡一样简单。同样,与常规塑料卡和支付选项相比时,支付促进器5400可以提供具有更好的风险管理的安全平台。通过使用支付促进器5400还可以促进商家,诸如关于它们单独的POS装备使得若干可用于商家。另外,诸如优惠券、供应、忠诚度和收据的若干促销方案或增值服务可以集成到支付促进器5400中,用以为商家以及消费者提供整体零售体验。

[0528] 根据示例性实施例,图54从支付视角描绘了支付促进器5400。然而,当支付促进器5400缩放时,支付促进器5400的类似模型可以应用于其它非支付器件,诸如优惠券、忠诚卡等。

[0529] 在本发明的实施例中,如图54中所示的APP 5404可以是移动应用5404。移动应用5404可以包括诸如钱包(也称为虚拟钱包)作为其组件之一。消费者可以与一个或多个这样的钱包相关联。出于由钱包提供的便利性、紧凑性和互操作性的缘故,钱包可以诸如在支付过程期间促进消费者。每个钱包可以被配置为持有消费者的交易器件的子集。根据各种实施例,钱包可以安全地存储和保护消费者支付账户信息、组织和管理消费者支付账户的生命周期、实现如访问账户所要求的强认证,提供用于选择用于交易的特定账户的选项、用所选账户与POS 5402或支付网关执行交易,实现并执行商业规则来管控对账户的访问和使用这些账户的交易。根据若干实施例,虚拟钱包的若干形式和实现可以是可能的,这取决于各种参数,诸如无限制地包括托管钱包的实体、消费者通过其来进行交易的信道,以及支付证书所存储的位置等。

[0530] 在示例性场景中,消费者或用户可以创建钱包,诸如在购物商店或例如“merchant.com”的网站上,并且使用诸如web门户来添加支付卡。在示例中,这样的钱包可以称为在线钱包,其可以在诸如仅从“merchant.com”购买产品期间提供便利性。必须意识到,支付促进器5400可以促进消费者自己向虚拟钱包添加他们预先存在的支付账户。然而,在诸如商家发行的卡(例如,礼品卡)之类的一些其它情况中,可以自动添加支付账户。

[0531] 在一些示例中,诸如银行或任何其它金融机构(FI)之类的实体可以建立它们自己的虚拟钱包版本。在这样的情况中,该实体可以承担显著的风险级别,并且保障商家不受欺诈,因为它们可以提供诸如持有账户、对用户进行认证、卡选择等钱包功能性,并且是仅仅用于支付账户的发行。在这样的情况中,钱包因此可以限于自发行的器件。

[0532] 钱包和钱包的每种支付类型可以被配置为诸如通过从塑料钱包跨至虚拟钱包映射各种标准和支付定价模型来遵照诸如定义的商业规则、交换费、PCI顺从性等。在实施例中,钱包可以实现在诸如智能电话中,诸如实现在移动手持机或其它此类手持设备内或使用它们的能力来实现。这可以促进虚拟钱包从在线部署至物理POS 5402的扩展。

[0533] 根据本发明的实施例,如上所述,钱包可以是容器或移动应用5404的组件或子系统。移动应用5404(如图54中所示)可以包括若干服务和功能,诸如但不限于钱包。例如,可以提供具有作为若干移动服务、一个或多个附加服务或功能之一的钱包的移动应用5404,诸如以在消费者内产生购买激励。因此,虽然附加服务可以提升购买激励,钱包可以提供对于完成或执行购买所需的功能性,使得钱包的焦点可以在于在诸如物理POS 5402之类的POS 5402处所执行的购买。

[0534] 图55示出了本发明的示例性实施例中的钱包的各种组件。图55的钱包可以称为软件钱包5500。根据各种实施例并且取决于支付促进器和服务递送平台生态系统5502的设计,钱包的各种组件可以不同地位于移动电话或任何其它手持设备5504、SDP 5508或发行者系统5510的任何合适组合中。因此,钱包5500可以被构造并视为分布式组件或分布式组件的组合,其可以跨诸如图55中示出的多个系统或子系统而运行。如图55中所示,钱包可以包括电子仓库(vault) 5512、参考存储装置5514、钱包控制器5518以及钱包视图5520。

[0535] 电子仓库5512可以是与每个单独支付证书相关联的安全存储装置。在实施例中,电子仓库5512可以合并安全元件上。在另一实施例中,电子仓库5512可以跨若干系统或子系统而分布,使得诸如发行者之类的每个子系统或系统可以保留对支付证书的控制以及在请求时对诸如单个使用标记的释放。在实施例中,服务递送平台生态系统可以采用分布式模型,然而,必须意识到,使用合并的模型可以是可能的并且在本发明的范围内。

[0536] 参考存储装置5514可以用作与诸如钱包的内容相关的参考数据的贮存库。参考数据可以包括诸如但不限于原图(artwork)和品牌化、发行者信息、路由信息(和参考标识符)、掩蔽的账户数据、元数据等。在实施例中,这些数据元素的子集可以存储在诸如移动电话上,诸如在移动电话的存储器内,而完整集合或数据可以存储在与SDP 5508相关联的服务器上,该服务器称为SDP服务器(如稍后所详细讨论的)。

[0537] 钱包控制器5518可以被配置为实现诸如钱包特定的商业逻辑和生命周期。钱包控制器5518可以被配置为控制和管理钱包,并且向可以访问钱包的外部系统提供诸如API的接口。另外,钱包控制器5518可以被配置为实现协议诸如用以与POS通信。例如,在本发明的服务递送平台生态系统的典型部署中,钱包控制器5518可以驻留在SDP服务器上。

[0538] 钱包视图5520可以是与钱包相关联的用户接口,诸如用以促进由相应用户通过由钱包视图5520提供的装置而对钱包的访问、交互、填充和管理。由钱包视图5520提供的用户接口可以针对每个可以用于访问钱包的信道分离地并且优选一致地被创建,所述信道诸如包括但不限于移动电话、web、IPTV等。在本发明的实施例中,钱包视图5520可以被包括在被设计用于和关联于服务递送平台生态系统的容器应用中。在实施例中,钱包视图5520可以

被包括在通过服务递送平台生态系统所链接的用于消费者的web接口中。

[0539] 在示例性实施例中,支付促进器可以部署在移动钱包中。钱包可以部署在诸如基于移动支付的系统中,所述基于移动支付的系统诸如服务递送平台生态系统5502或支付促进器。钱包5500可以被配置以便促进消费者从云中选择经证明的应用来访问诸如与支付促进器相关联的钱包之类的钱包以执行支付。在实施例中,这些支付可以在POS处进行。在另一实施例中,这些支付可以在远程定位位置处进行。

[0540] 钱包架构可以包括诸如钱包视图5520、钱包控制器5518、钱包电子仓库5512、应用、参考存储装置5514、服务递送平台5508、诸如发行者系统5510-5514之类的多个发行者系统。服务递送平台5508此外可以包括主钱包和若干应用钱包,诸如第一应用钱包、第二应用钱包等等。应用可以包括诸如第一应用1、第二应用以及用于支付促进器的应用。

[0541] 在实施例中,SDP 5508架构可以包括若干SDP 5508和SDP钱包,它们间具有诸如分层父子关系。SDP 5508可以被配置为维护具有多个钱包的父子分层。诸如移动应用之类的每个应用可以链接到独立钱包实例。SDP 5508可以被配置为维护在诸如父支付促进器钱包与对应于相应父钱包的子应用钱包之间的父子关系。在这样的场景中,该架构可以被设计以便为消费者定义单个SDP 5508和单个钱包视图5520,使得消费者感觉好像在与从不同应用或不同钱包视图5520内所使用的SDP 5508和单个钱包相交互。

[0542] 在如上所讨论的分层架构中,所有器件可以被供应到父支付促进器钱包,即,供应到支付促进器的父钱包的参考存储装置5514。实际钱包电子仓库5512可以被配置为属于发行者系统5510并且在其控制之下。然而,在实施例中,可以将非敏感信息供应到SDP 5508。子钱包可以被配置为具有它们自己的参考存储装置5514,以诸如使能在支付促进器的父钱包的参考存储装置5514上的经过滤的视图。

[0543] 在实施例中,诸如PIN长度、所允许的PIN重试等的各种钱包生命周期规则在诸如由支付促进器设置的指南内针对每个钱包可以是独立可配置的。在支付时,移动应用可以从SDP 5508请求标记。SDP 5508可以被配置为使用企业服务总线(ESB)来检索用于支付帐户的标记。标记可以是诸如由发行者系统生成的一次性标记。对标记检索和生成的请求可以与通过SDP 5508进行的强认证过程以及对发行者系统可用的可选附加认证相关联。然后,可以在POS处通过可用信道之一来使用标记。在实施例中,单独移动应用可以通过标准web服务来传送来自SDP 5508的消费者服务以便访问对应钱包。

[0544] 根据钱包架构的一些示例性且非限制性实施例,在安全防护支付证书和发行标记中可以牵涉发行者。可以允许发行者控制标记的格式,并且可以包括如适当和相关的附加安全性措施。此外,发行者可以对退款和其它异常场景具有最小影响,因为发行者可以直接牵涉在供应和支付流中。该钱包架构还可以提供从多个移动应用(诸如从多个钱包视图5520)的钱包可访问性。同样,在认证期间,每个钱包可以用诸如独立口令被独立认证,并且可以被独立地管理或激活或锁定或挂起等,同时仍然向用户提供一致的用户体验。该钱包架构还可以使能可配置的基于规则的过滤,以用于为每个子钱包过滤参考存储装置5514,从而允许商家具有所有用户的支付卡的获允许子集。同样,该架构可以促进默认帐户容易地按照相应钱包被分别设置。该钱包架构还可以使能用消费者的主钱包中的支付证书来自动填充支付促进器的消费者有品牌的容器。这可以促进从单个位置对所有帐户的管理。此外,通过该基于单个位置的管理,用户还可以标识他们的用于访问支付促进器的他们的钱

包的其它应用。

[0545] 如上文所讨论和提到并且在图54中示出的SDP 5508可以被配置为这样的系统：其可以被配置为包装服务并且通过若干信道将服务递送给消费者。SDP 5508可以促进有组织的、易于消费方式的服务包装以及通过多个信道的服务递送。可以诸如在移动支付域中使能SDP 5508。SDP 5508可以被配置为执行诸如用户钱包实例的登记、了解你的客户(KYC)以及创建。SDP 5508可以被配置为管理钱包的生命周期，连同去往各种端点设备的链接。SDP 5508可以被配置为诸如向消费者提供标准化接口以用于服务发现和选择。SDP 5508可以被配置为诸如以统一方式提供经发行者管控的服务登记和供应。SDP 5508可以被配置为诸如围绕服务供应和消费而实现强认证、安全性和信任模型。SDP 5508可以被配置为针对诸如服务和钱包事件等维护详细的审查跟踪、日志和交易记录。SDP 5508可以被配置为机载(onboard)单独服务提供者、聚集不同的服务主机、执行服务实现标准以及管理生态系统的整体成长和执行若干其它功能。这里讨论的SDP 5508的功能和配置仅仅是示例性的而没有限制。在仍一些实施例中，SDP 5508可以被配置为基于诸如由SDP 5508递送的服务的性质来执行若干其它功能和任务。例如，与金融交易相关的服务可以具有对于安全性和可靠性的额外强制性要求，使得SDP 5508可以被配置为在递送金融服务的同时增强安全性相关的任务。此外，SDP 5508可以被配置为在大规模向公众递送服务时进一步增强系统可伸缩性和冗余性。

[0546] 在基于本文描述的MTP方法和系统的SDP 5508生态系统部署的示例性实施例中，SDP 5508可以被设计为包括专用于支付促进器的各种组件，其中所述生态系统部署包括钱包、容器、MTP服务器、服务提供者等等。在示例中，可以存在若干组件一起工作来履行SDP服务器功能。这些组件均可以以高度安全、高度可伸缩、高度可用性的企业服务器配置来部署。在示例中，ESB可以标准化和互连多个合作伙伴和系统，从所述合作伙伴和系统可以消费服务和将服务递送给移动容器。每个合作伙伴服务提供者可以通过在SDP 5508中建模的一系列步骤被机载。这些步骤可以由支付促进器来定义，并且通过服务提供的性质(例如，支付、供应、忠诚等)来管控。

[0547] 本文可以描述支付促进器SDP 5508的各种示例性组件。在示例中，支付促进器SDP 5508可以包括通信组件。通信组件可以处理通信协议、编解码、串行化、包封(enveloping)，以及通过多个数据信道与移动应用进行分组交换通信的复杂性。在示例中，支付促进器SDP 5508可以包括消息总线&通知组件。消息总线&通知组件可以支持基于生产/消费者的模型，用于与移动客户端进行对象连同消息结构的交换。在示例中，消息总线&通知组件还可以促进推送通知、警报等，从而允许SDP 5508主动地到达容器应用以执行某活动。在示例中，支付促进器SDP 5508可以包括安全性/认证组件。安全性组件可以促进用于强认证、数据保密、机密性/保密、数据完整性等的安全性相关的设计的实现，因为它们涉及整体信任模型以及对正递送的服务的风险管理。在示例中，支付促进器SDP 5508可以包括空中(OTA)供应组件。OTA供应可以被配置用于处理应用、微件、器件(支付、供应、忠诚度、票据等)以及代理服务的空中供应和递送以用于器件的标记化。在示例中，支付促进器SDP 5508可以包括OTA TSM代理组件。OTA可信服务管理器(TSM)代理组件可以仅在基于安全元件(诸如图55中所图示的)生态系统中被需要，以用于小程序的空中供应和管理安全元件安全性域。在示例中，OTA TSM代理可以典型地与外部第三方TSM相接口。在示例中，支付促进器SDP 5508可以包

括钱包和微件管理组件。钱包和微件管理可以创建和管理消费者的钱包的生命周期、钱包与一个或多个设备的关联,以及用一个或多个微件和那些微件的生命周期来使应用个性化。在示例中,支付促进器SDP 5508可以包括交易引擎。交易引擎可以被配置用于处理跨无线信道的交易可靠性,并维护正被递送的服务的完整审查跟踪。交易引擎可以促进收到和其它相关联的交易服务。在示例中,支付促进器SDP 5508可以包括器件管理组件。器件管理组件可以被配置用于管理消费者在其钱包中所填充的单独器件的生命周期。在示例中,支付促进器SDP 5508可以包括位置和地理围栏组件。位置和地理围栏组件可以帮助服务提供者在基于位置的服务中设立地理围栏和选择。在示例中,当消费者进入地理围栏时,位置和地理围栏组件可以生成用于服务提供者的触发,基于此,目标服务可以被递送。在示例中,支付促进器SDP 5508可以包括增强现实组件。增强现实组件可以提供可以在钱包和微件内并入的独特和先进的用户体验基础设施。

[0548] 在基于本文描述的MTP方法和系统的SDP 5502生态系统部署的示例性实施例中,可以针对ESB创建消息定义,其可以执行可以针对支付促进器而创建的标准和协议。然后,服务提供者可以实现ESB连接器,以诸如以支付促进器基础设施的各种利益相关者可以消费服务的方式向平台展露其服务。

[0549] 在基于本文描述的MTP方法和系统的SDP 5502生态系统部署的示例性实施例中,来自SDP 5508的服务供应可以是一组基本步骤。在一些实施例中,取决于服务的性质和服务提供者的偏好,一些步骤可以是可选的。在示例中,第一步骤可以包括注册和KYC。在该步骤处,消费者可以请求服务(钱包、支付帐户等),并提供所需的个人信息以便执行相关KYC步骤。对注册和KYC进一步地,可以要求服务批准以用于进行进一步处理。服务批准可以要求服务合作伙伴在遵循相关内部商业过程之后批准服务请求。服务批准可以创建用于消费者的相关证书以及任何服务有效载荷。在一些实施例中,服务批准可以是可选的。下一步骤可以是服务供应。在该步骤处,可以将服务供应给用户。服务供应可以包括向消费者电话递送服务的组件,或者在消费者服务器上创建必要的更新。服务供应之后可以是服务激活。可以要求服务激活以确认服务被正确供应给正确用户,并且对于要消费的服务,所有状态被设置为“就绪”。在一些实施例中,服务激活可以是可选的。下一步骤可以是服务执行。在该步骤处,消费者可以开始从其应用内使用服务。下一步骤可以是服务管理,其可以包括服务的所有更新和生命周期组件。

[0550] 在SDP 5502生态系统部署的示例性实施例中,用于支付促进器的SDP 5508架构可以允许服务合作伙伴以如下方式配置和控制它们的服务产品:它们遵照支付促进器规范(通过ESB接口),但是控制它们自己的过程、服务数据以及商业规则。这样的控制和管理对于可以吸引关键性大量服务提供者的开放式生态系统可能是必需的。

[0551] 在基于本文描述的MTP方法和系统的包括钱包、容器、MTP服务器、服务提供者等的SDP 5502生态系统部署的示例性实施例中,可以存在可以在POS处进行交易的移动电话替代物。本文描述了高层级移动支付场景的流。然而,应当注意,这些步骤是高层级的,并且可以被重新安排以适合特定用户体验,并且可以插入其它步骤以便提供附加功能性。本公开文档的目的是展示用于支付促进器的各种部署选项,而非支付的特定用例。

[0552] 在示例性且非限制性实施例中,为了对移动支付起作用,消费者可能必须首先到达结账终端并且可以扫描要购买的物品。然后,消费者可以发动移动电话上的移动应用,并

且可以被要求输入登录证书(例如,PIN、口令或口令短语等)。移动应用可以连接到SDP 5508以验证登录并对消费者和设备进行认证。在服务和设备成功认证时,移动应用可以呈现可以存储在消费者的移动钱包中的支付选项列表。可以要求消费者从提供给消费者的列表中选择支付选项(例如,礼品卡)。

[0553] 在可能选择了支付选项之后,移动应用可以发起与POS的结账过程。取决于POS和移动电话可以支持的信道,可以经由多个实现选项来发起支付选项。在示例中,标记化的NFC可以用于发起结账过程。针对该选项,POS可以被近场通信(NFC)使能。移动应用可以针对用于所选支付卡的标记而请求SDP 5508。SDP 5508可以认证移动应用,并且可以将该请求路由到相关发行者的对应标记生成器。可以要求消费者在NFC使能的POS处轻敲电话以传输标记。在示例中,NFC可以是国际标准化组织(ISO)和国际电工技术委员会(IEC)标准18092。在示例中,安全元件NFC(SE NFC)可以用于发起结账过程。在该情况中,可以要求消费者在NFC使能的POS处轻敲电话,其中支付证书存储在电话上的SE中。在示例中,NFC可以是国际标准化组织(ISO)和国际电工技术委员会(IEC)标准14443。在示例中,QR码扫描可以用于发起结账过程。移动应用可以针对用于所选支付卡的标记而请求SDP 5508。SDP 5508可以认证移动应用,并且可以将该请求路由到相关发行者的对应标记生成器。移动应用可以将标记转换成通过POS扫描的2D条形码。在示例中,虚拟读取器可以用于发起结账过程。移动应用可以通过扫描QR码或轻敲NFC标签来捕获商家、POS和交易信息。移动应用可以将数据连同所选卡通过OTA发送给SDP 5508。SDP 5508可以请求标记,并且通过后端过程将标记连同其它信息一起发送给POS。

[0554] 在发起结账过程之后的下一步骤可以要求POS处理交易并且将所述处理路由到支付促进器。在下一步骤处,支付促进器可以将交易路由到支付卡的发行者。在下一步骤处,发行者可以授权交易并且可以将批准递送给POS。POS可以确认交易并递送收据。在示例中,收据可以被打印、电子地递送给移动应用或者通过电子邮件发送到经核实的电子邮件地址。收据的递送可以使移动支付过程完成,并且消费者可以带着购买的物品离开结账终端。

[0555] 在基于本文描述的MTP方法和系统的包括钱包、容器、MTP服务器、服务提供者等的SDP 5502生态系统部署的示例性实施例中,商家可以采用各种部署模型。商家可以处于其单独移动策略中的各种阶段;并因此,可以要求其支持用于商家的多个部署模型以便采用公共支付促进器。支付促进器连同每个发行者一起可以从安全性和风险管理视角批准并证明整个交易路径,以诸如保持低交易成本。因此,具有可以在所有参与商家间共享的公共平台可以是重要的。

[0556] 在示例性且非限制性实施例中,可以存在可以用于部署的三个模型。这三个模型是共存的,并且商家可以取决于其单独策略来采用这些模型中的一个或多个。在示例性且非限制性实施例中,可以部署比本文描述的三个模型更多或更少的模型。在示例性且非限制性实施例中,这些模型可以被配置用于实现支付、供应、忠诚度供应等等。

[0557] 在基于本文描述的MTP方法和系统的SDP 5502生态系统部署的示例性实施例中,部署模型可以是具有子支付促进器钱包的商家应用。可以要求消费者通过使用他们现有的、市场上的商家移动应用来在POS处支付,所述商家移动应用通过由SDP 5508钱包平台供应和管理的直接子钱包而链接到他们的主支付促进器钱包。子钱包可以被独立配置,但是链接到主钱包。在示例中,现有的商家移动应用通过OTA web服务接口而直接与SDP 5508相

接口。SDP 5508可以提供对消费者的支付促进器钱包的经认证的、受控制的并且经过滤的访问,并且商家应用可以用于POS处的交易。在示例中,SDP 5508可以聚集支持多个支付信道的多个支付发行者,并且管理消费者的父支付促进器钱包和子商家钱包二者。

[0558] 在基于本文描述的MTP方法和系统的SDP 5502生态系统部署的示例性实施例中,部署模型可以是具有商家钱包的商家应用。商家可以在其移动应用内使用其独立第三方钱包,并且可以访问来自主支付促进器钱包的支付证书。

[0559] 在基于本文描述的MTP方法和系统的SDP 5502生态系统部署的示例性实施例中,部署模型可以基于支付促进器容器。消费者可以通过使用支付促进器品牌化的移动应用来支付,该移动应用可以从SDP 5502自动得以填充并且向消费者提供到其父支付促进器钱包中的统一视图。SDP 5502可以聚集支持多个支付信道的多个支付发行者,并且管理消费者的支付促进器钱包。在示例中,支付促进器移动应用可以与商家POS交互以执行交易,而不用商家进行任何附加开发。在示例中,商家和发行者可以可选地创建其自己的微件以在支付促进器应用内运行来创建定制体验。

[0560] 图56图示了可以基于支付促进器容器的部署模型5600的高层级框图。

[0561] 根据所图示的实施例,支付促进器内的各种子系统可以包括销售点(POS) 5602、诸如移动应用5604之类的应用(APP) 5604、SDP 5608、若干发行者系统,诸如无限制地包括所描绘的发行者1系统5610、发行者2系统5612以及发行者3系统5614。各种子系统可以通过诸如支付处理网络5618之类的网络来连接。APP 5604此外可以包括第一微件5620、第二微件5622以及钱包5624。

[0562] 所图示的实施例可以是支付促进器支付指南的一个示例,其可能必须跨诸如发行者系统5610-5614之类的多个发行者系统和多个商家来管理。消费者可以不知道移动交易的复杂后端操作,以便创建“选择卡并支付”的简单体验。可以通过支付促进器钱包容器应用5604来创建和市场推广支付促进器品牌。在实施例中,商家可以将支付促进器标准提升为支付接受品牌。在示例中,可以用不同的支付产品和多个POS 5602信道来支持多个发行者5610-5614,从而给予消费者对支付选项的选择,该选择可以跨多个商家而适合他们的需要。支付促进器容器可以要求在商家一方用以接受支付促进器支付选项的最小努力。可以要求POS 5602侧工作,因为微件可以是可选的。支付促进器容器可以确保支付处理顺从用于基于POS 5602的交易的支付促进器指南和标准。

[0563] 支付促进器容器模型可以利用SDP的全部力量,多个服务提供者的后和前端聚集。如图56中所图示,支付促进器品牌化的移动应用5604(容器)可以通过使用MTP钱包工具套件来构建。

[0564] 容器可以包括可以并入支付促进器规范的钱包实现。当消费者创建其支付促进器钱包时,钱包可以从SDP得以自动填充。在实施例中,支付促进器容器可以用于在支付促进器顺从的POS 5602处进行支付,而不用商家进行任何进一步开发。在实施例中,商家可以有能力通过使用MTP工具套件来创建微件,MTP工具套件可以专门设计用于在POS 5602处提供以商家为中心的用户体验。微件创建可以任凭商家决定,并且可以在任何时候被实现或添加。SDP可以聚集并允许机载多个发行者5610-5614,并且可以允许商家定义其支付促进器兼容的支付产品和其它增值服务(VAS)。在这样的机载期间,发行者5610-5614可以选择针对每个支付产品可以受支持的POS 5602交互协议。POS 5602交互协议可以确定哪些商家可

以接受哪些支付产品,因为商家的POS 5602信道可能必须支持发行者选择的协议中至少一个,例如,NFC、条形码、OTA等等。

[0565] 在一些示例性实施例中,SDP可以被配置为管理3维矩阵。该矩阵可以被配置用于商家的POS 5602支持的邻近信道,例如,NFC、2D条形码、OTA等等。该矩阵可以被配置用于商家POS 5602能力。该矩阵可以被配置用于发行者批准的信道。

[0566] 在基于本文描述的MTP方法和系统的SDP生态系统部署的示例性实施例中,支付促进器可以用于利用商家微件的移动支付。在示例性且非限制性实施例中,为了使移动支付起作用,消费者可能必须首先到达结账终端并且可以扫描要购买的物品。然后,消费者可以发动移动电话上的支付促进器移动应用5604,并且可以被要求输入支付促进器管理的登录证书(例如,PIN、口令或口令短语等)。然后,可以要求消费者从支付使能的商家的操纵盘(dashboard)选择商家。商家微件可以被发动于“支付”模式中,并且呈现在商家POS 5602处接受的支付选项列表。支付选项列表可以是消费者的钱包中本地存储的选项上经过滤的视图,以作为支付促进器容器的一部分。可以要求消费者从提供给消费者的列表中选择支付选项(例如,礼品卡)。

[0567] 商家微件可以从SDP请求交易有效载荷,其可以发送到商家POS 5602以用于由商家POS 5602支持的对应信道。SDP可以传递针对商家POS 5602格式化的交易有效载荷。在示例性实施例中,交易有效载荷可以用优惠券、忠诚度等形式。可以基于商家POS 5602能力来附接交易有效载荷。在接收到交易有效载荷时,商家微件可以发起与POS 5602的结账过程。该结账过程的发起可以类似于上面参照没有商家微件生成的示例所描述的那样来进行。

[0568] 在发起结账过程之后的下一步骤可以要求POS 5602处理交易并将所述处理路由到支付促进器。在下一步骤处,支付促进器可以将交易路由到支付卡的发行者。在下一步骤处,发行者可以授权交易并且可以将批准递送给POS 5602。POS 5602可以确认交易并递送收据。在示例中,收据可以被打印、电子地递送给移动应用5604或者通过电子邮件发送到经核实的电子邮件地址。收据的递送可以使移动支付过程完成,并且消费者可以带着购买的物品离开结账终端。

[0569] 在基于本文描述的MTP方法和系统的SDP生态系统部署的示例性实施例中,用户接口(UI)在支付促进器容器中。本文描述的UI概念可以仅仅用作对示例性实施例的参考。取决于用户需要,UI概念可以服从于改变。在示例性实施例中,UI概念可以包括钱包控制的模式和微件控制的模式。钱包控制模式可以被配置,使得支付促进器钱包可以控制商家POS 5602交互和支付体验。钱包控制模式可以绕过商家创建微件的需要。微件控制模式可以被配置,使得商家可以创建微件,并且微件可以将控制商家POS 5602处的交互和支付体验。

[0570] 本文描述的方法和系统可以部分地或整体地通过在处理器上执行计算机软件、程序代码和/或指令的机器来部署。处理器可以是服务器、客户端、网络基础设施、移动计算平台、固定计算平台或其它计算平台的部分。处理器可以是能够执行程序指令、代码、二进制指令等的任何种类的计算或处理设备。处理器可以是或者包括单个处理器、数字处理器、嵌入式处理器、微处理器或者诸如协处理器(数学协处理器、图形协处理器、通信协处理器等)的任何变体等,其可以直接或间接促进存储在其上的程序代码或程序指令的执行。另外,处理器可以使能多个程序、线程和代码的执行。线程可以同时执行以增强处理器的性能,并且促进应用的同时操作。作为实现方式,本文描述的方法、程序代码、程序指令等可以在一个

或多个线程中实现。线程可以繁衍 (spawn) 其它线程, 所述其它线程可以具有所指派的与它们相关联的优先级; 处理器可以基于优先级或者任何其它次序基于在程序代码中提供的指令来执行这些线程。处理器可以包括存储器, 其存储如本文及别处所描述的方法、代码、指令和程序。处理器可以通过接口来访问存储介质, 其可以存储如本文及别处所描述的方法、代码和指令。与处理器相关联的用于存储能够由计算或处理设备执行的方法、程序、代码、程序指令或其它类型的指令的存储介质可以包括但不限于以下各项中的一个或多个: CD-ROM、DVD、存储器、硬盘、闪速驱动器、RAM、ROM、高速缓存等。

[0571] 处理器可以包括可以增强多处理器的速度和性能的一个或多个核。在实施例中, 处理器可以是组合两个或多个独立核心 (称为管芯) 的双核处理器、四核处理器、其它芯片层级多处理器等。

[0572] 本文描述的方法和系统可以部分地或整体地通过在服务器、客户端、防火墙、网关、集线器、路由器或其它此类计算机和/或联网硬件上执行计算机软件的机器来部署。软件程序可以与服务器相关联, 服务器可以包括文件服务器、打印服务器、域服务器、互联网服务器、内联网服务器以及诸如辅助服务器、主机服务器、分布式服务器等的其它变体。服务器可以包括以下中的一个或多个: 存储器、处理器、计算机可读介质、存储介质、端口 (物理的和虚拟的)、通信设备以及接口等, 接口能够通过有线或无线介质来访问其它服务器、客户端、机器以及设备。如本文和别处所描述的方法、程序或代码可以由服务器执行。另外, 对于执行如本申请中所描述的方法所需的其它设备可以认为是与服务器相关联的基础设施的一部分。

[0573] 服务器可以提供至其它设备的接口, 所述其它设备无限制地包括: 客户端、其它服务器、打印机、数据库服务器、打印服务器、文件服务器、通信服务器、分布式服务器等。另外, 该耦合和/或连接可以促进跨网络的程序的远程执行。一些或所有这些设备的联网可以促进程序或方法在一个或多个位置处的并行处理, 而不偏离本范围。另外, 通过接口附接到服务器的任何设备可以包括能够存储方法、程序、代码和/或指令的至少一个存储介质。中央贮存库可以提供要在不同设备上执行的程序指令。在该实现中, 远程贮存库可以充当用于程序代码、指令和程序的存储介质。

[0574] 软件程序可以与客户端相关联, 客户端可以包括文件客户端、打印客户端、域客户端、互联网客户端、内联网客户端以及诸如辅助客户端、主机客户端、分布式客户端等的其它变体。客户端可以包括以下中的一个或多个: 存储器、处理器、计算机可读介质、存储介质、端口 (物理的和虚拟的)、通信设备以及接口等, 接口能够通过有线或无线介质来访问其它客户端、服务器、机器以及设备。如本文和别处所描述的方法、程序或代码可以由客户端执行。另外, 对于执行如本申请中所描述的方法所需的其它设备可以认为是与客户端相关联的基础设施的一部分。

[0575] 客户端可以提供至其它设备的接口, 所述其它设备无限制地包括: 服务器、其它客户端、打印机、数据库服务器、打印服务器、文件服务器、通信服务器、分布式服务器等。另外, 该耦合和/或连接可以促进跨网络的程序的远程执行。一些或所有这些设备的联网可以促进程序或方法在一个或多个位置处的并行处理, 而不偏离本范围。另外, 通过接口附接到客户端的任何设备可以包括能够存储方法、程序、应用、代码和/或指令的至少一个存储介质。中央贮存库可以提供要在不同设备上执行的程序指令。在该实现中, 远程贮存库可以充

当用于程序代码、指令和程序的存储介质。

[0576] 本文描述的方法和系统可以部分地或整体地通过网络基础设施来部署。网络基础设施可以包括诸如以下的元件：计算设备、服务器、路由器、集线器、防火墙、客户端、个人计算机、通信设备、路由设备以及如本领域所已知的其它有源和无源设备、模块和/或组件。与网络基础设施相关联的(多个)计算和/或非计算设备可以包括与其它组件分离的存储介质，诸如闪速存储器、缓冲器、栈、RAM、ROM等。本文和别处描述的过程、方法、程序代码、指令可以由一个或多个网络基础设施元件来执行。

[0577] 本文和别处描述的方法、程序代码和指令可以在具有多个小区的蜂窝网络上实现。蜂窝网络可以是频分多址(FDMA)网络或码分多址(CDMA)网络。蜂窝网络可以包括移动设备、小区站点、基站、中继器、天线、塔等。小区网络可以是GSM、GPRS、3G、EVDO、网络或其它网络类型。

[0578] 本文和别处描述的方法、程序代码和指令可以在移动设备上或通过移动设备来实现。移动设备可以包括导航设备、手机、移动电话、移动个人数字助理、膝上型计算机、掌上型计算机、上网本、寻呼机、电子书阅读器、音乐播放器等。这些设备可以包括与其它组件分离的存储介质，诸如闪速存储器、缓冲器、RAM、ROM以及一个或多个计算设备。与移动设备相关联的计算设备可以被使能来执行其上存储的程序代码、方法和指令。可替换地，移动设备可以被配置为与其它设备协同来执行指令。移动设备可以与基站通信，所述基站与服务器相接口且被配置为执行程序代码。移动设备可以在对等网络、网格网络或其它通信网络上通信。程序代码可以存储在与服务器相关联的存储介质上，并且由嵌入在服务器内的计算设备来执行。基站可以包括计算设备和存储介质。存储设备可以存储由与基站相关联的计算设备执行的程序代码和指令。

[0579] 计算机软件、程序代码和/或指令可以在机器可读介质上存储和/或访问，所述机器可读介质可以包括：计算机组件、设备和记录介质，其保留用于在某时间间隔内进行计算的数字数据；称为随机存取存储器(RAM)的半导体存储装置；典型地用于较永久存储的大容量存储装置，诸如光学盘、像硬盘、磁带、磁鼓、卡那样的磁存储形式及其它类型；处理器寄存器、高速缓冲存储器、易失性存储器、非易失性存储器；诸如CD、DVD的光学存储装置；可移动介质，诸如闪速存储器(例如，USB棒或U盾(USB key))、软盘、磁性带、纸带、穿孔卡、独立RAM盘、Zip驱动器、可移动大容量存储装置、离线装置等；其它计算机存储器，诸如动态存储器、静态存储器、读/写存储装置、易变存储装置(mutable storage)、只读存储装置、随机存取存储装置、顺序存取存储装置、位置可寻址存储装置、文件可寻址存储装置、内容可寻址存储装置、网络附接的存储装置、存储区域网络、条形码、磁性墨等。

[0580] 本文描述的方法和系统可以将物理和/或无形项目从一个状态变换到另一个状态。本文描述的方法和系统还可以将表示物理和/或无形项目的的数据从一个状态变换到另一个状态。

[0581] 本文描述和描绘的、包括在贯穿附图的流程图和框图中的元件暗含这些元件之间的逻辑边界。然而，根据软件或硬件工程实践，所描绘的元件及其功能可以通过计算机可执行介质而实现在机器上，所述机器具有能够执行程序指令的处理器，所述程序指令在其上存储为单片软件结构、独立软件模块或采用外部例程、代码、服务等模块或这些的任意组合，并且所有这样的实现可以在本公开的范围内。这样的机器的示例可以包括但是可以不

限于：个人数字助理、膝上型计算机、个人计算机、移动电话、其它手持计算设备、医疗装备、有线或无线通信设备、换能器、芯片、计算器、卫星、平板PC、电子书、小机件、电子设备、具有人工智能的设备、计算设备、联网装备、服务器、路由器等。此外，在流程图和框图中描绘的元件或任何其它逻辑组件可以实现在能够执行程序指令的机器上。因此，尽管前述附图和描述阐述了所公开系统的功能方面，但是除非明确声明或者从上下文另外清楚的，否则不应从这些描述中推断出用于实现这些功能方面的软件的任何特定布置。类似地，可以意识到，上文标识和描述的各种步骤可以变化，并且步骤顺序可以适应于本文公开的技术的特定应用。所有这样的变型和修改意图落入本公开的范围。因而，除非由特定应用要求或者明确声明或从上下文另外清楚的，否则针对各个步骤的顺序的描绘和/或描述不应理解为要求特定顺序来执行那些步骤。

[0582] 以上描述的方法和/或过程及其步骤可以实现在适于特定应用的硬件、软件或者硬件和软件的任何组合中。硬件可以包括通用计算机和/或专用计算设备或特定计算设备，或者特定计算设备的具体方面或组件。过程可以实现在一个或多个微处理器、微控制器、嵌入式微控制器、可编程数字信号处理器或其它可编程设备，连同内部和/或外部存储器中。过程还可以或者替代地具体化在以下各项中：专用集成电路、可编程门阵列、可编程阵列逻辑，或者可以被配置为处理电子信号的任何其它设备或设备的组合。此外可以意识到，一个或多个过程可以实现为能够在机器可读介质上执行的计算机可执行代码。

[0583] 计算机可执行代码可以通过使用诸如C的结构化编程语言、诸如C++的面向对象编程语言或任何其它高级或低级编程语言（包括汇编语言、硬件描述语言以及数据库编程语言和技术）来创建，所述计算机可执行代码可以被存储、编译或解译以在以上设备以及处理器的异构组合、处理器架构或者不同硬件和软件的组合或者能够执行程序指令的任何其它机器之一上运行。

[0584] 因此，在一个方面中，上文描述的每种方法及其组合可以具体化在计算机可执行代码中，所述计算机可执行代码当在一个或多个计算设备上执行时执行方法的步骤。在另一方面中，这些方法可以具体化在执行其步骤的系统中，并且可以以多种方式跨设备分布，或者所有功能性可以集成在专用的独立设备或其它硬件中。在另一方面中，用于执行与上文描述的过程相关联的步骤的装置可以包括上文描述的硬件和/或软件中的任何一个。所有这样的置换和组合意图落入本公开的范围。

[0585] 尽管已经结合详细示出和描述的某些优选实施例公开了本文描述的方法和系统，但是对其的各种修改和改进对于本领域技术人员可以容易变得显而易见。因此，本文描述的方法和系统的精神和范围将不受前述示例的限制，而是要在通过法律可允许的最广的意义上理解。

[0586] 据此通过引用并入本文中引用的所有文档。

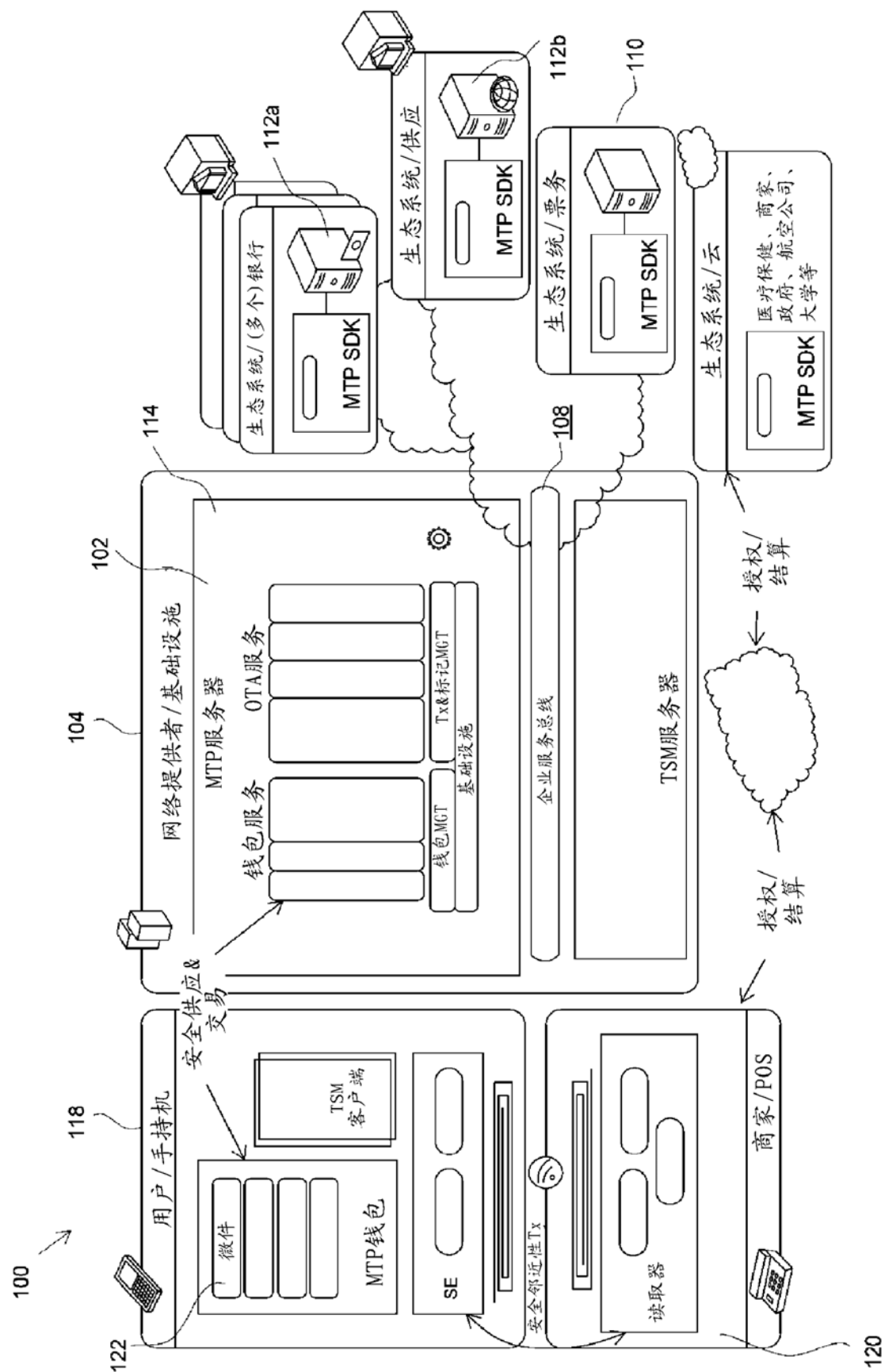


图 1

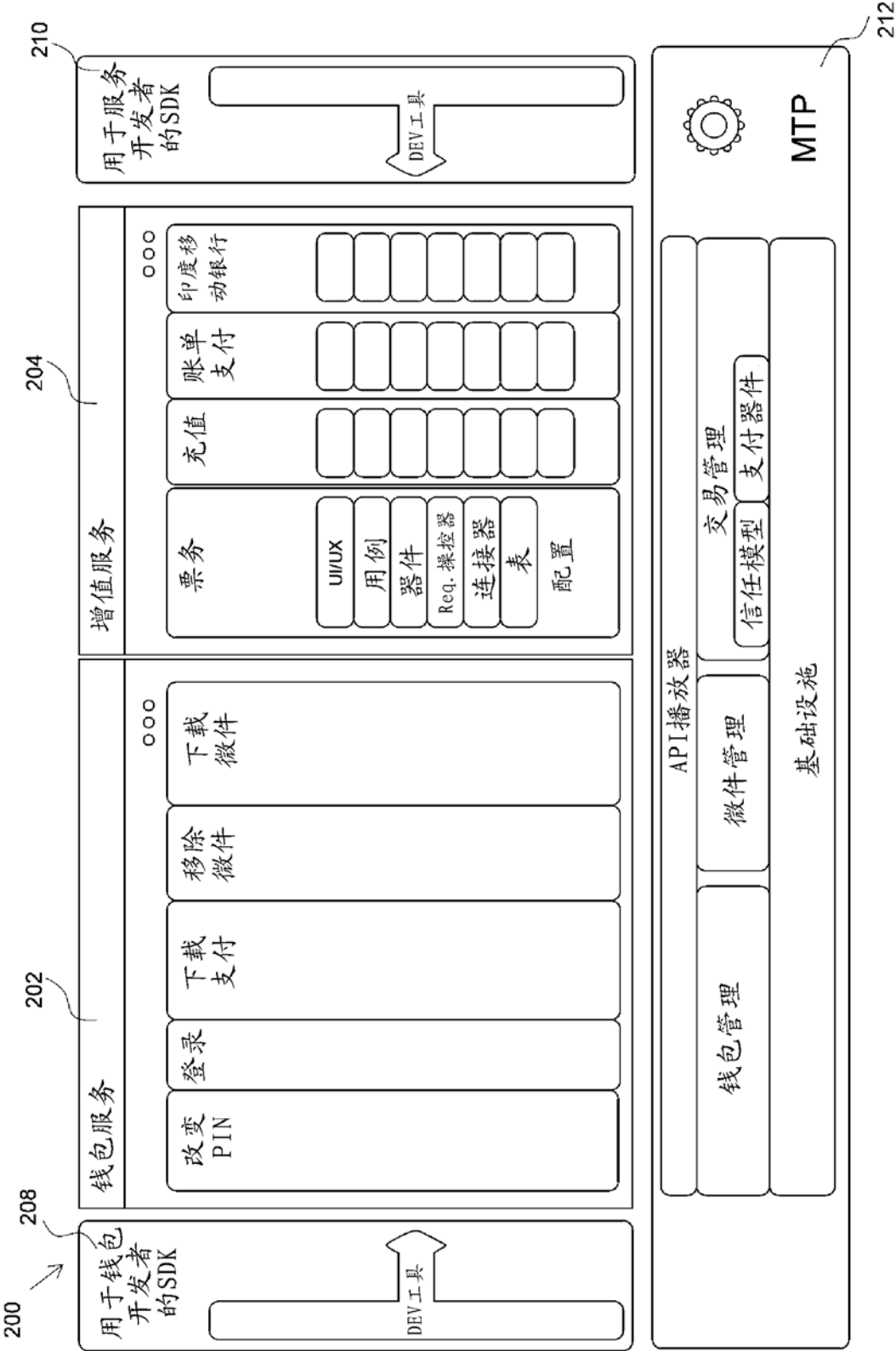


图 2

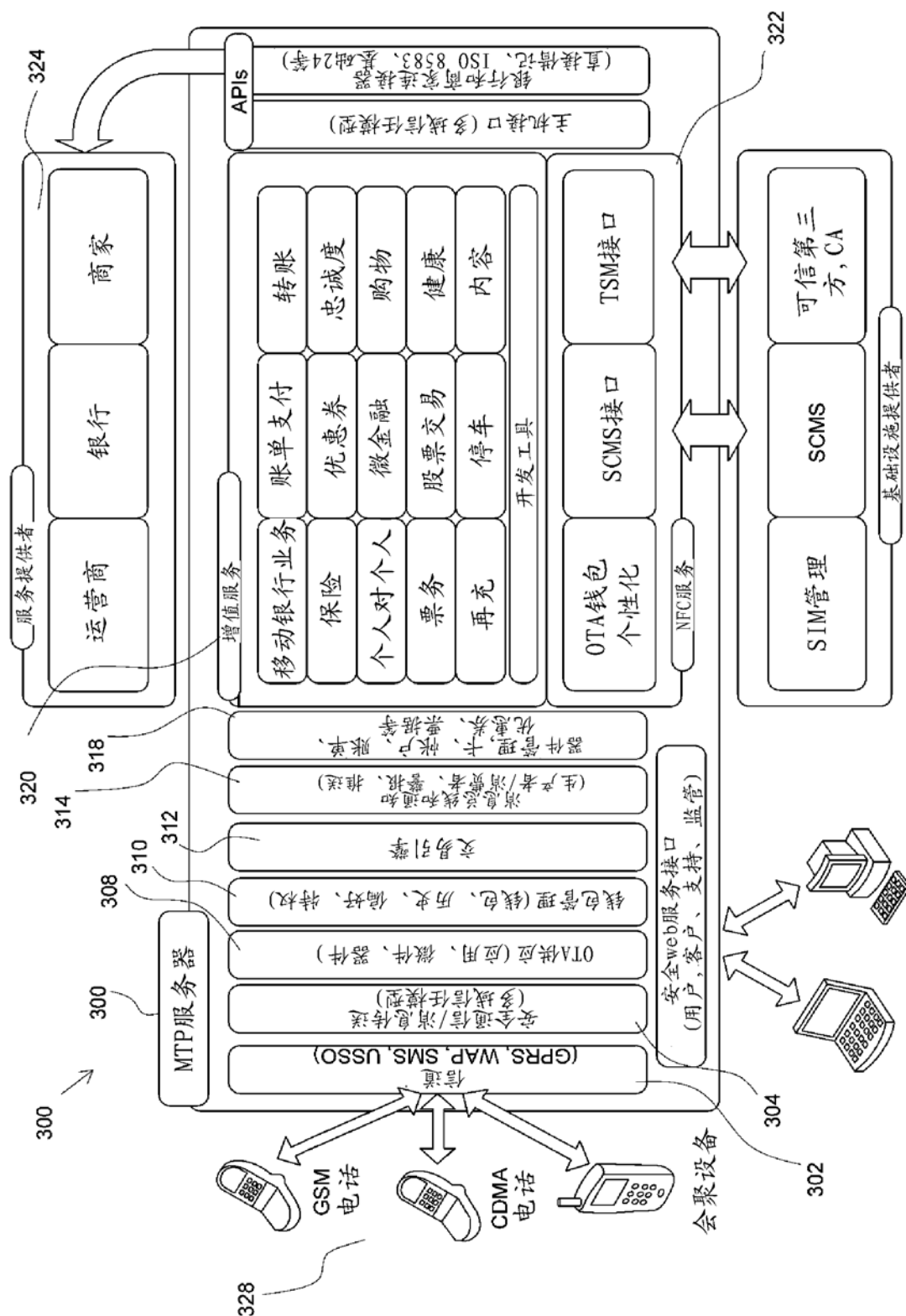


图 3

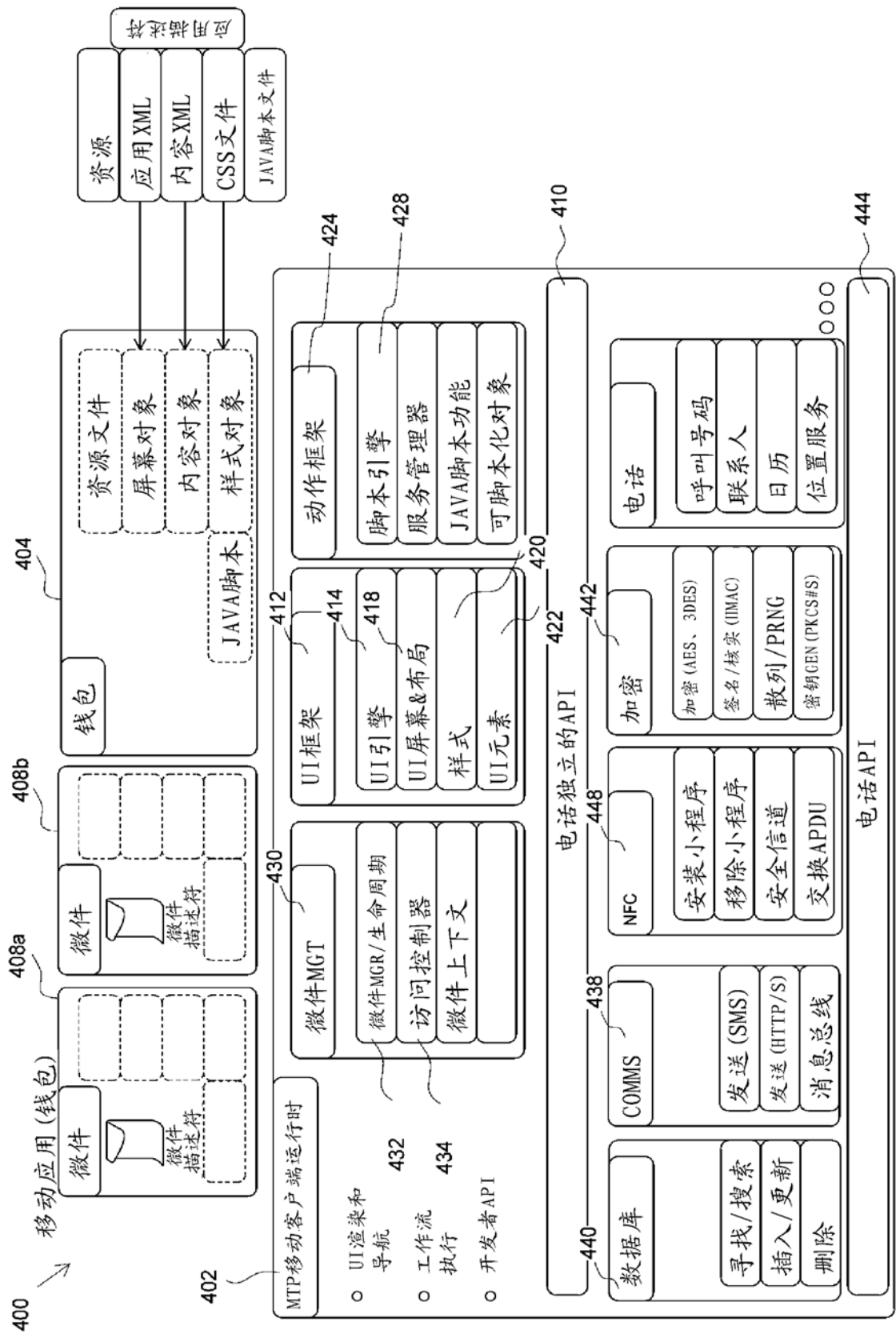


图 4

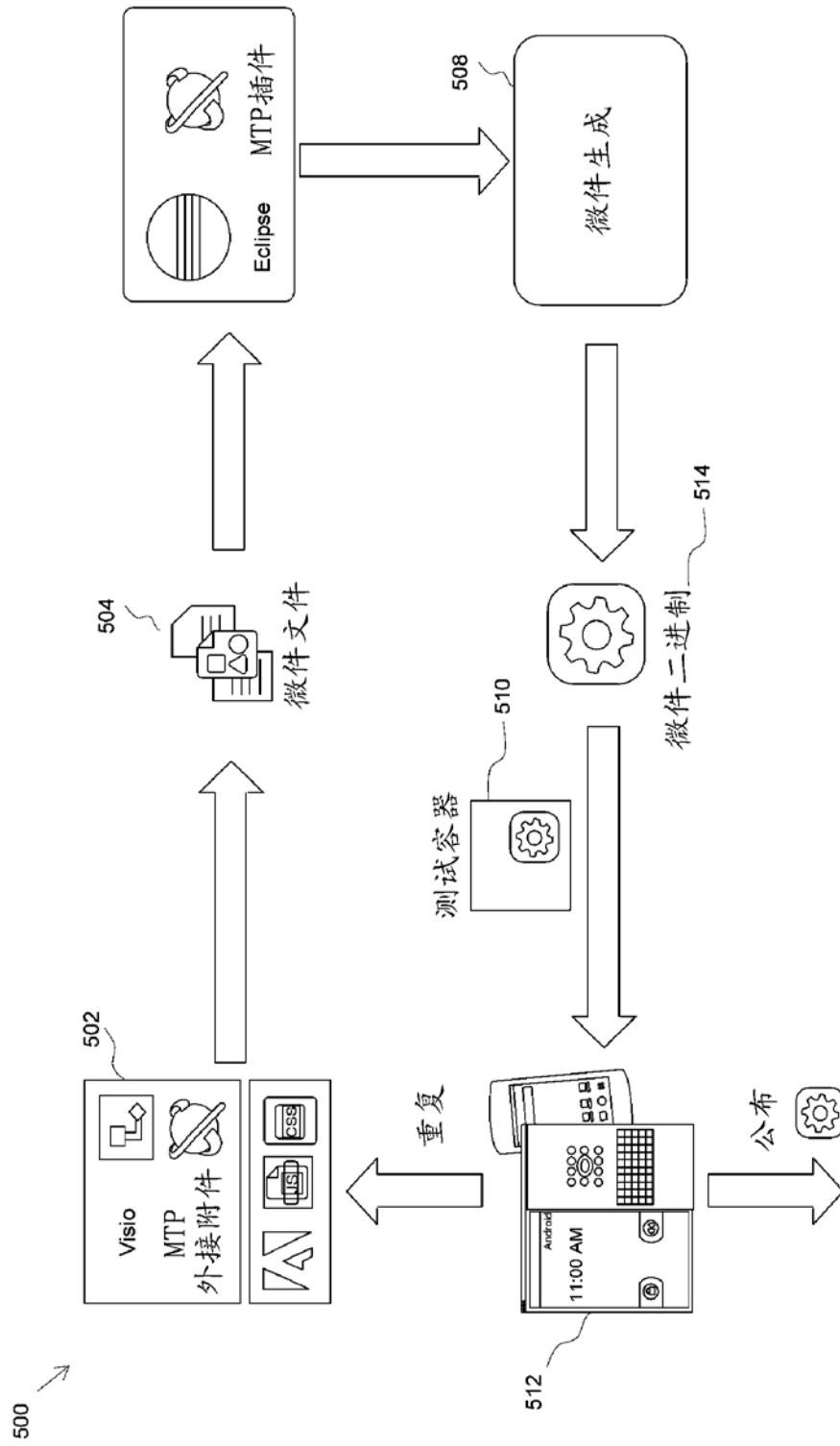


图 5

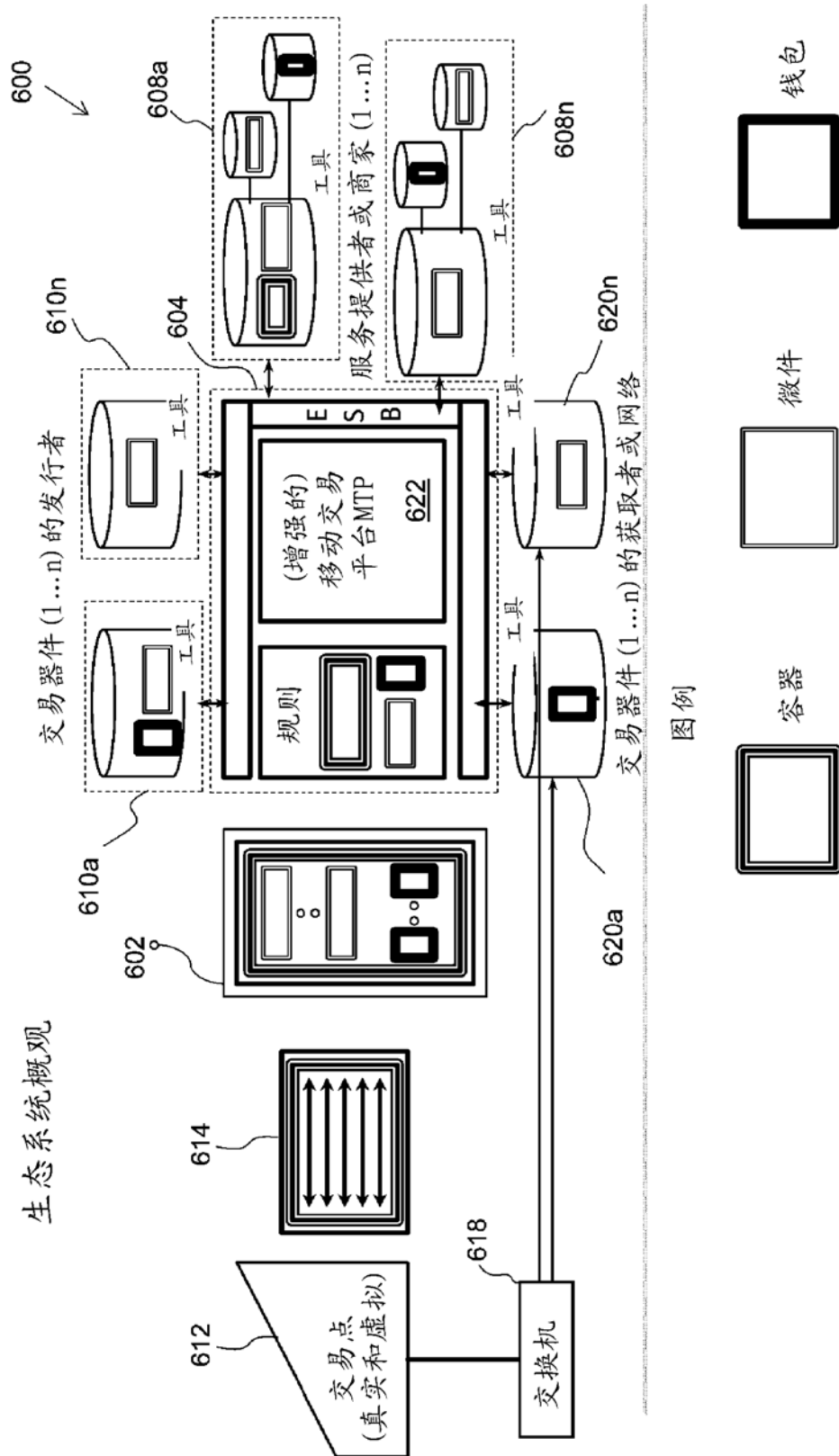


图 6

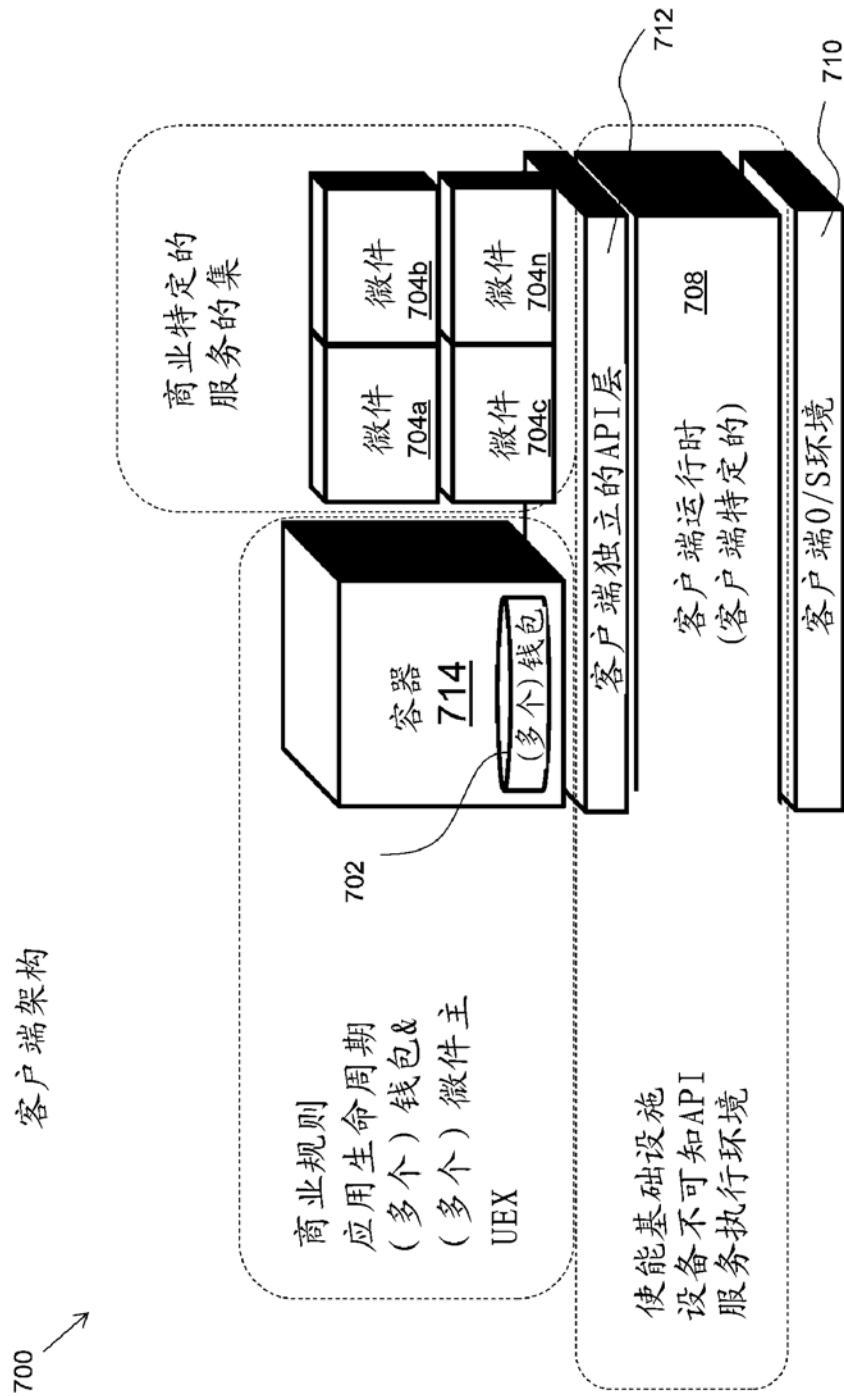


图 7

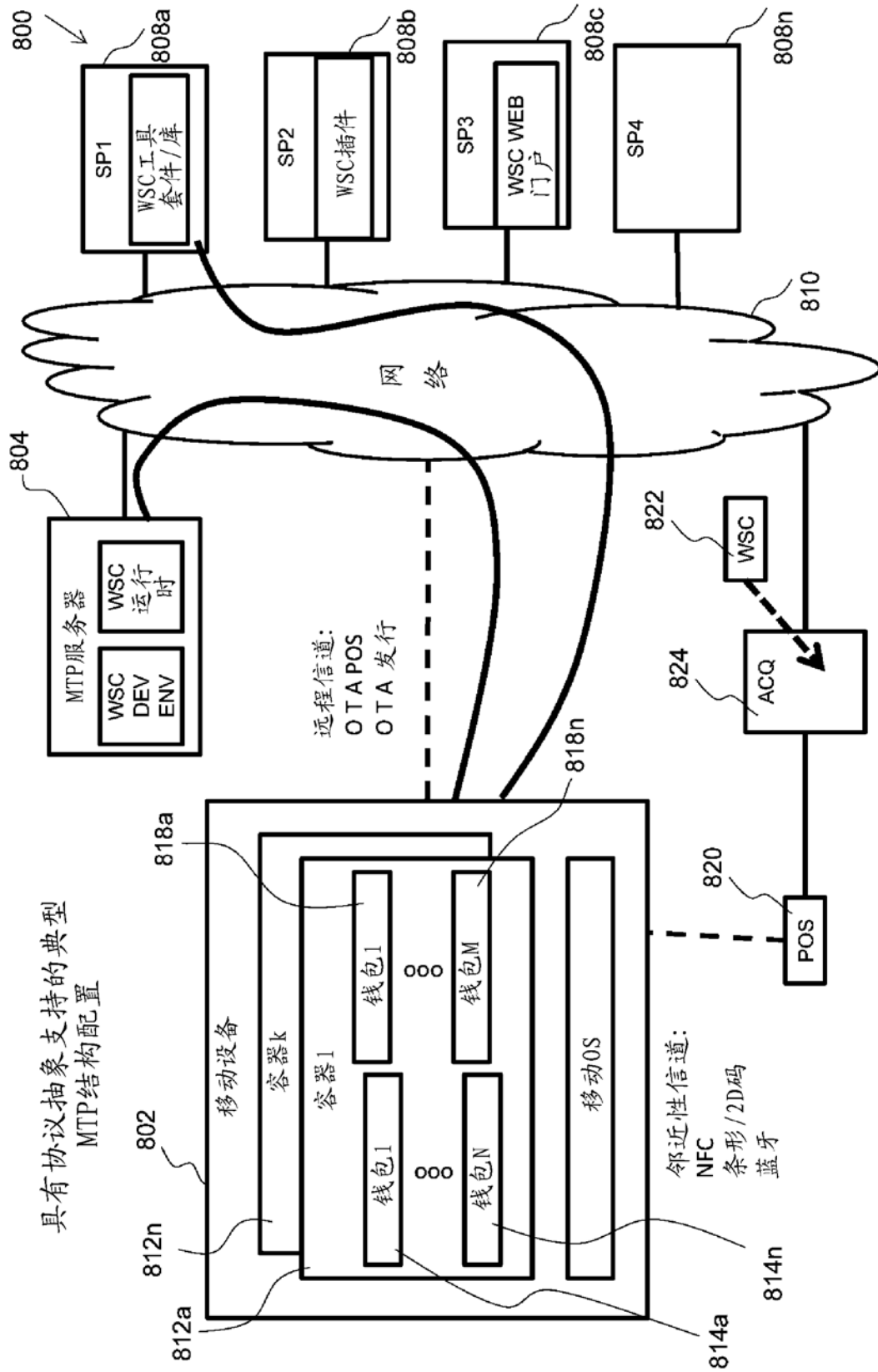


图 8

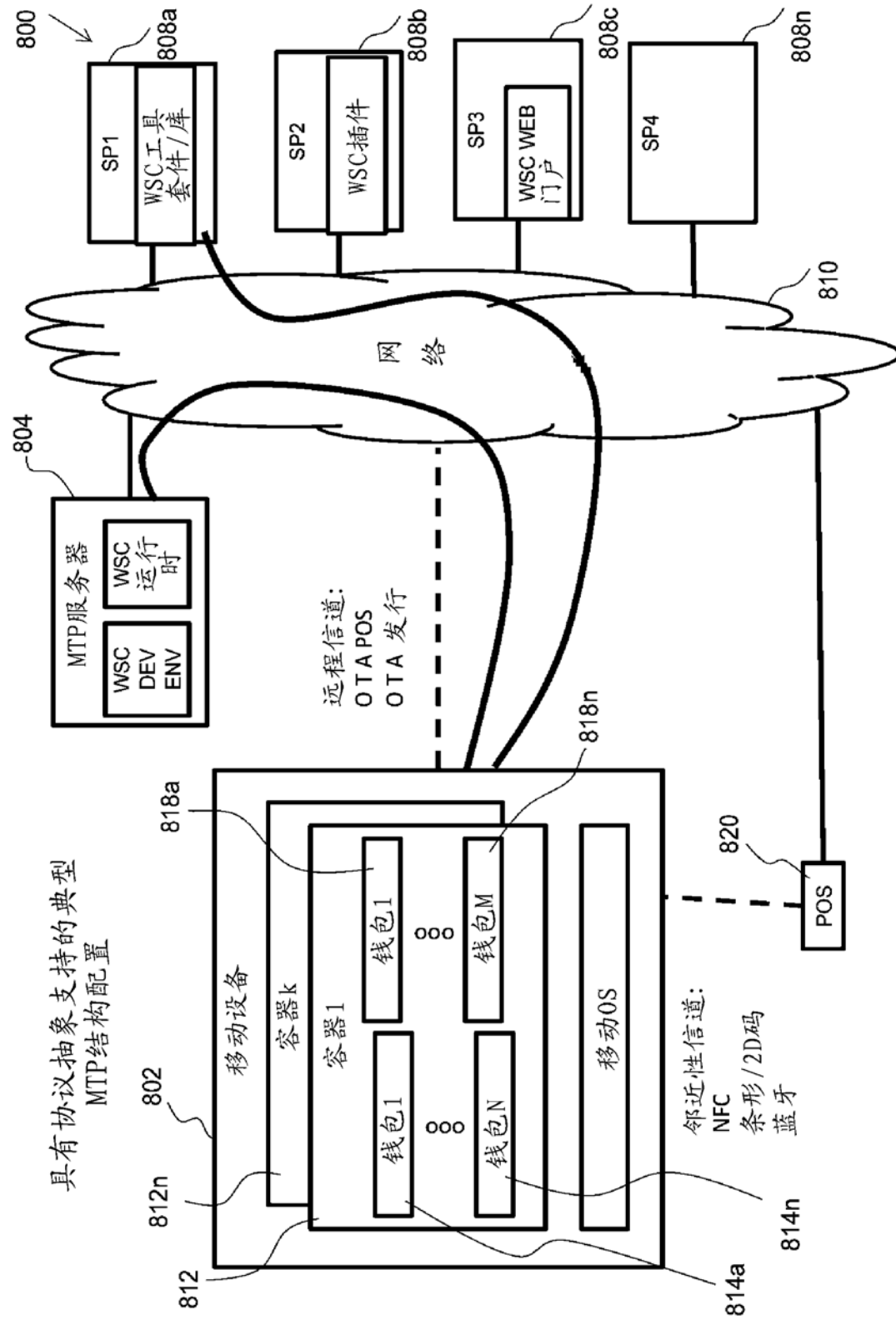


图 9

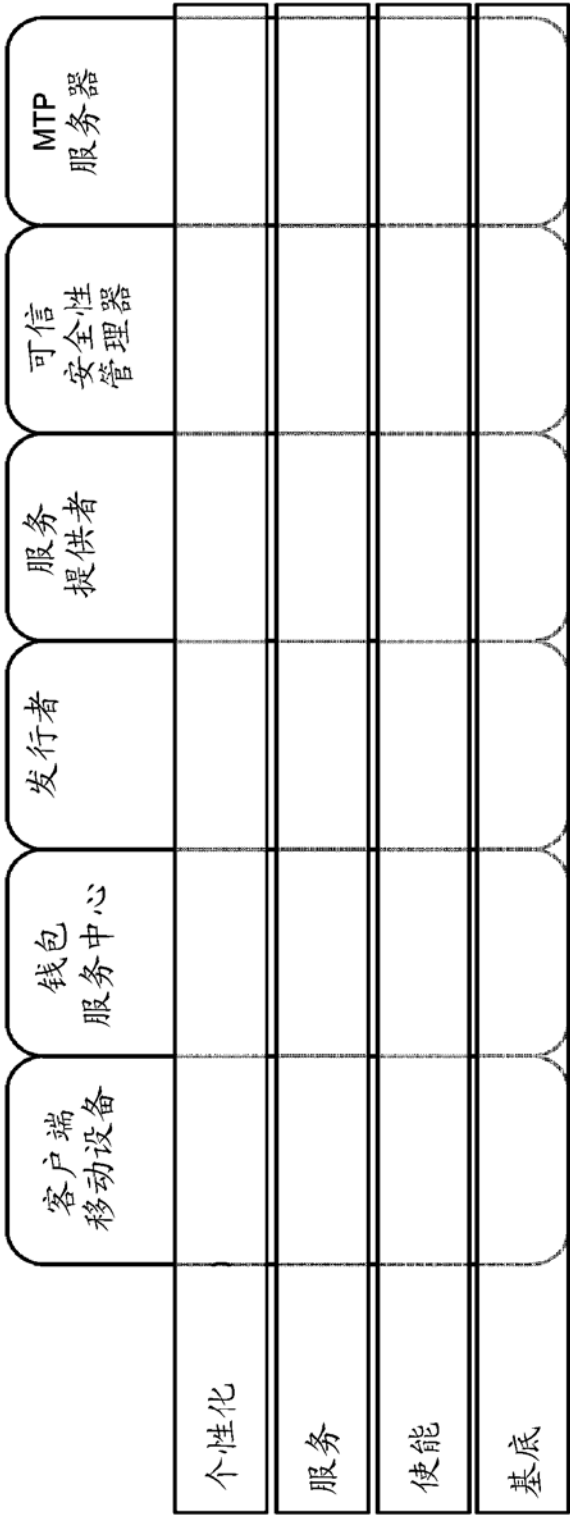


图 10

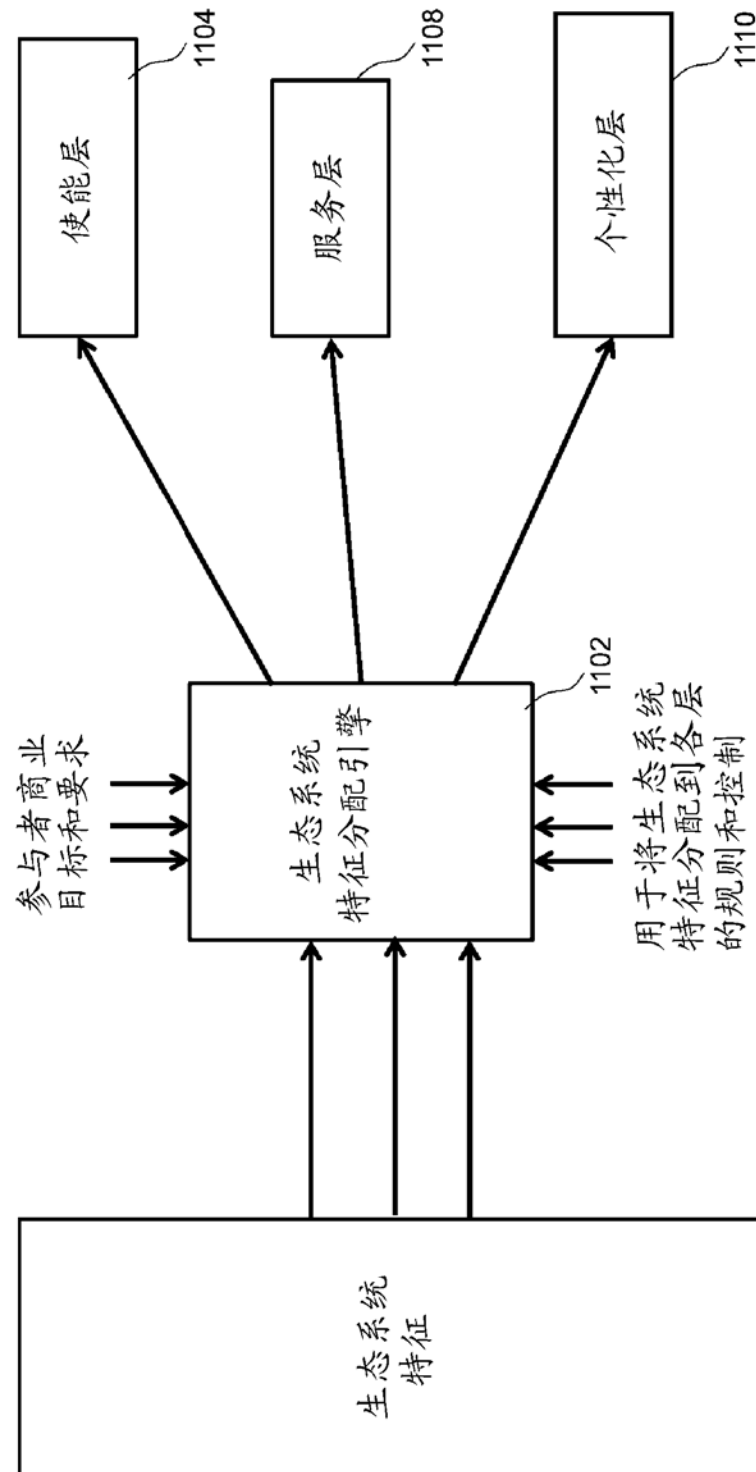


图 11

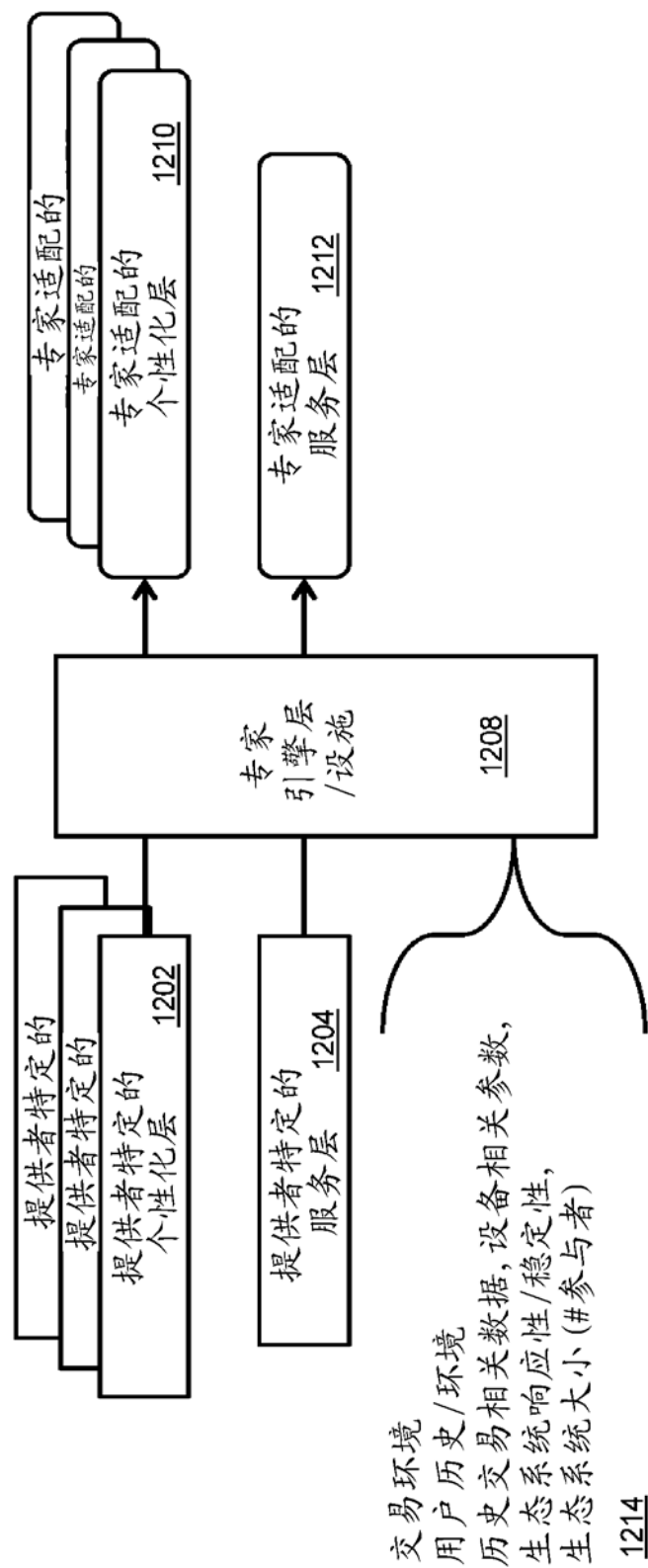


图 12

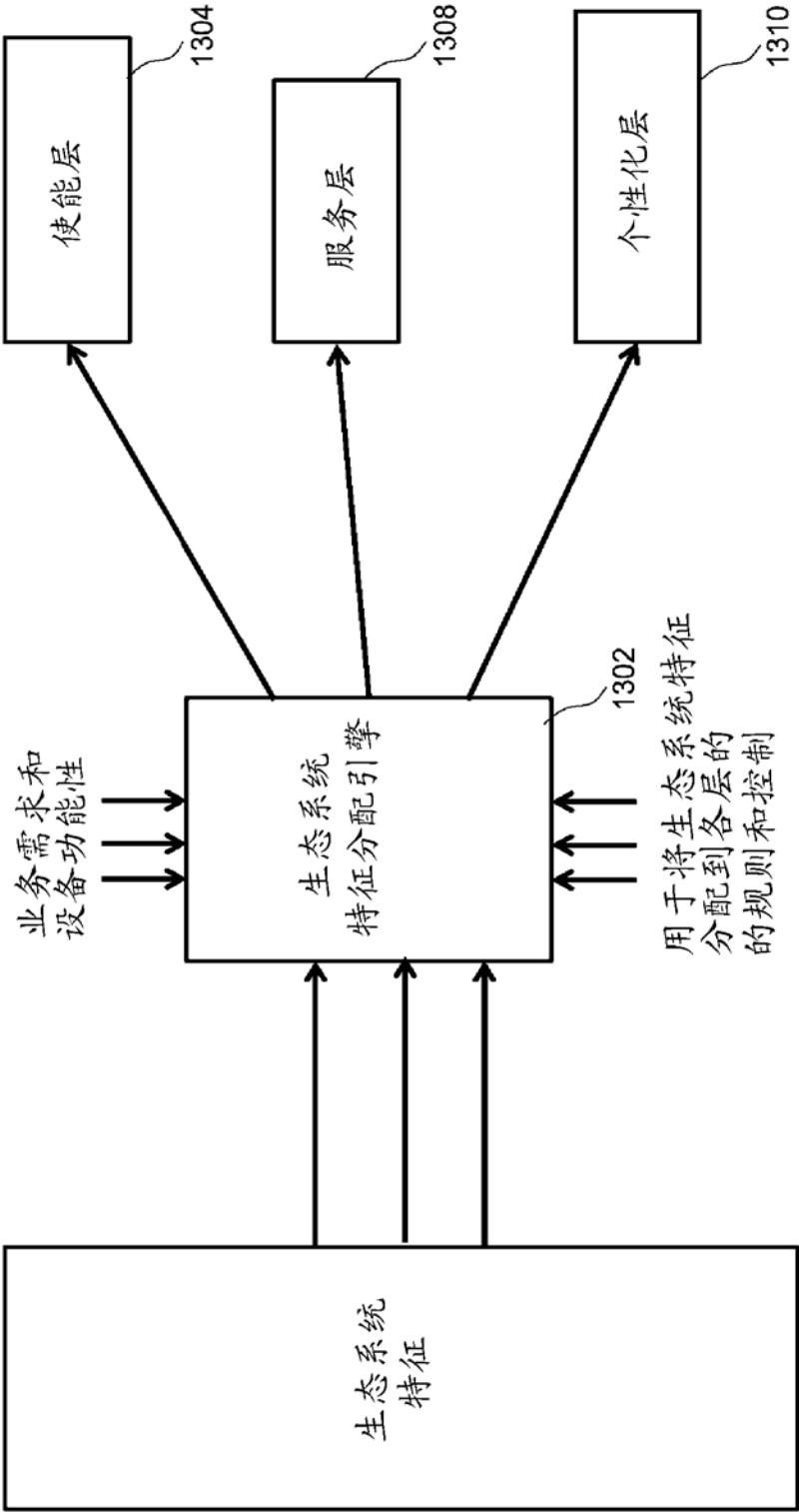


图 13

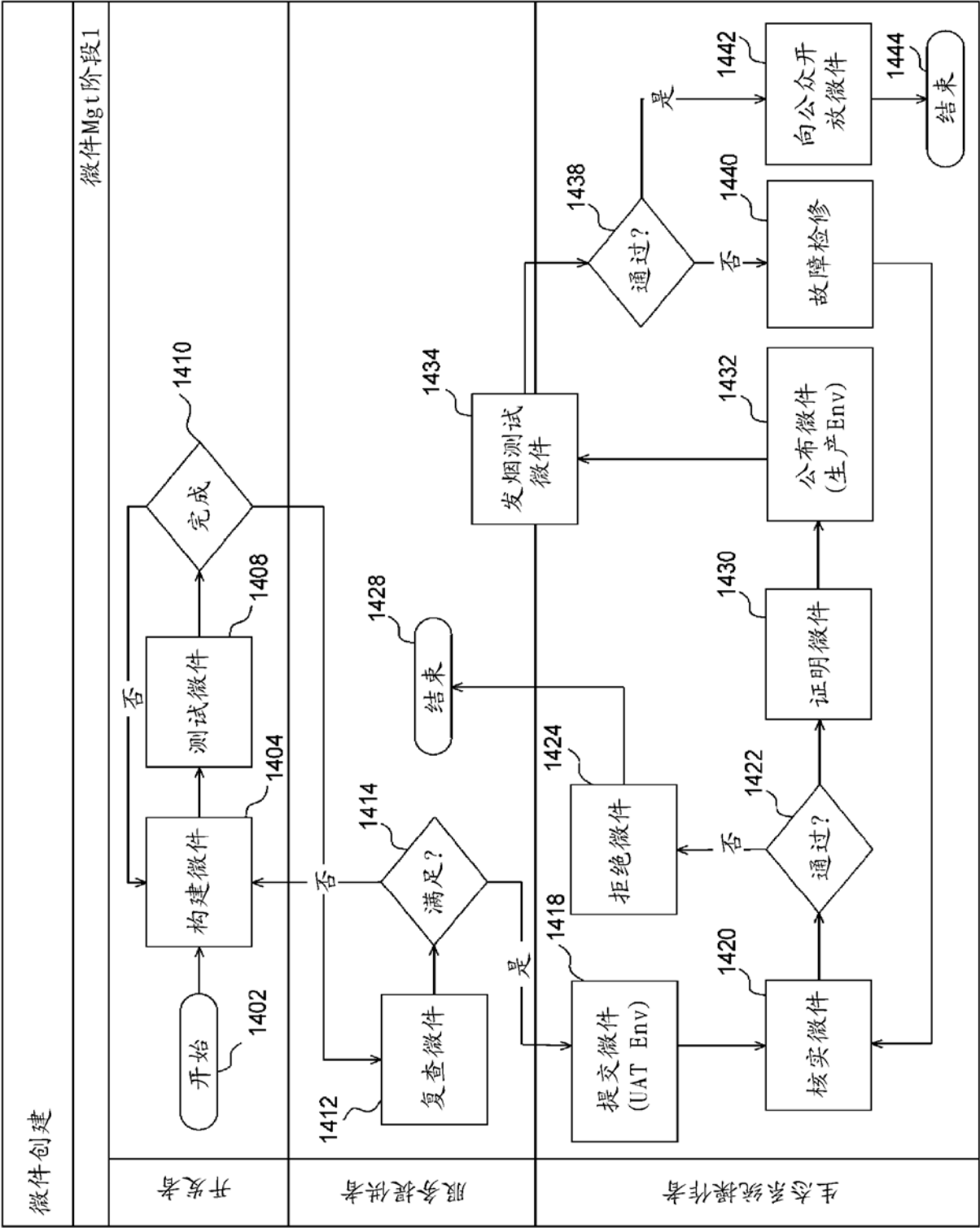


图 14

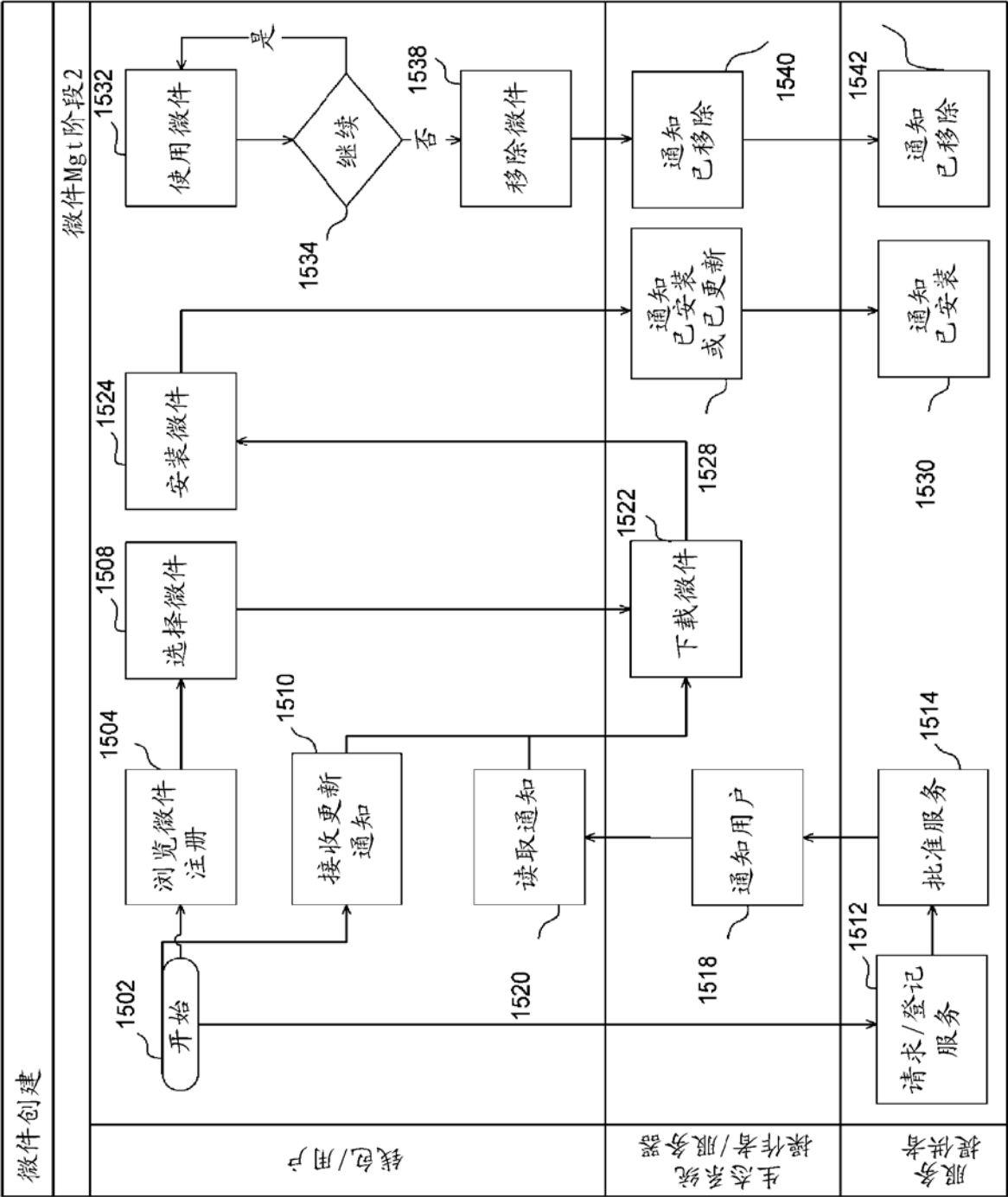


图 15

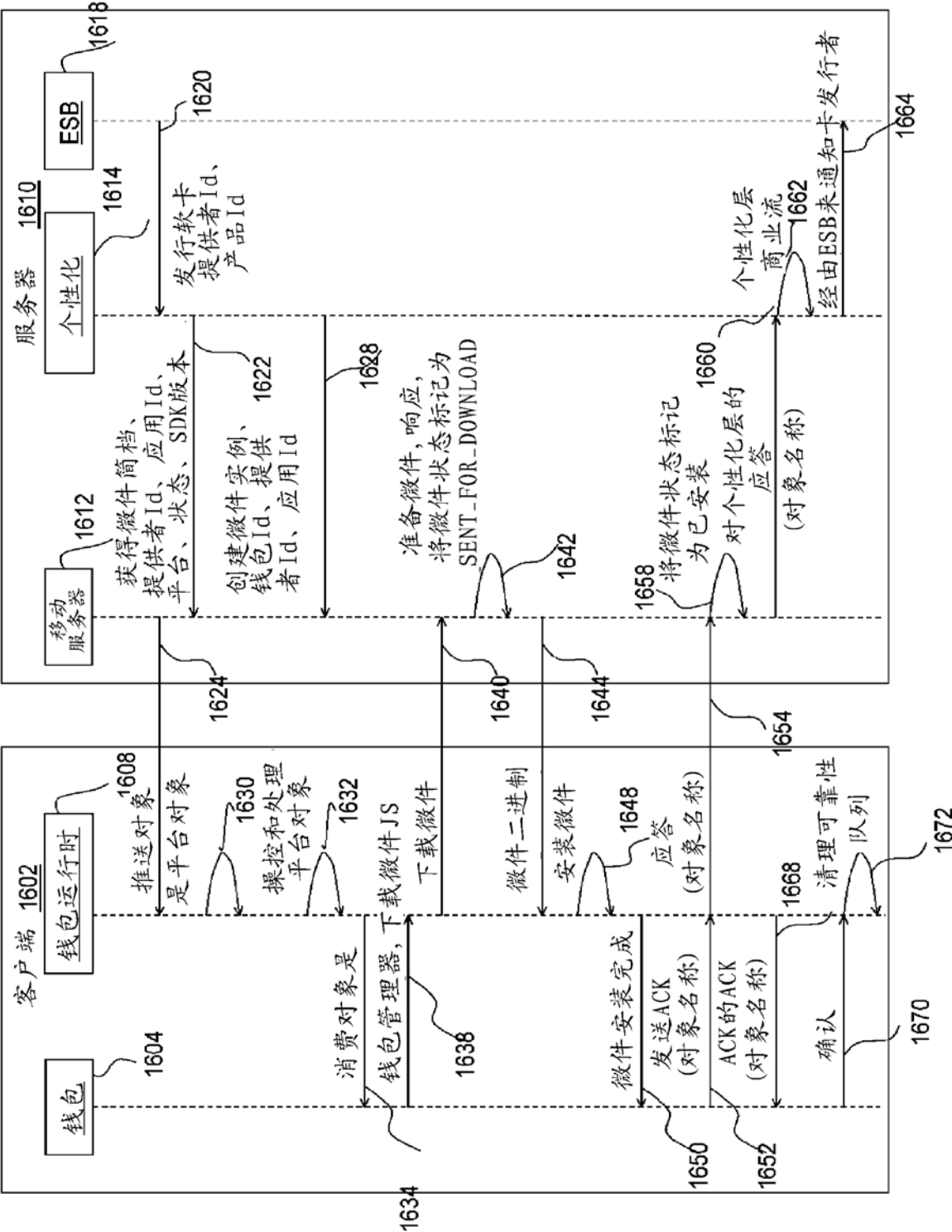


图 16

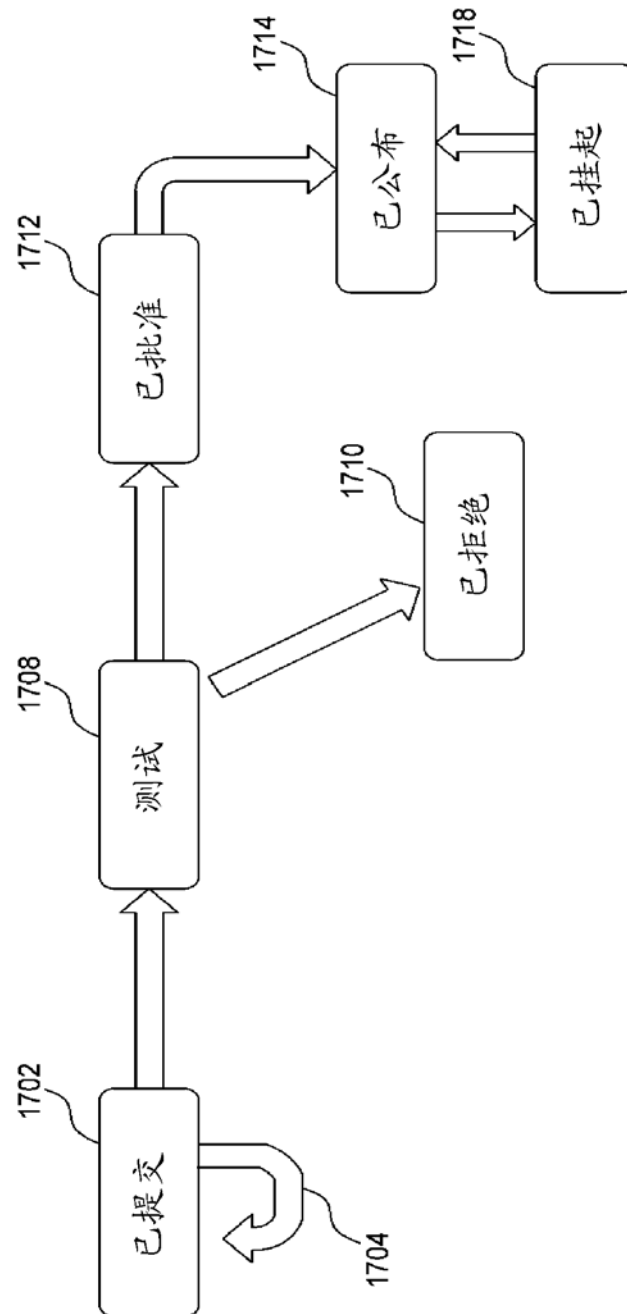


图 17

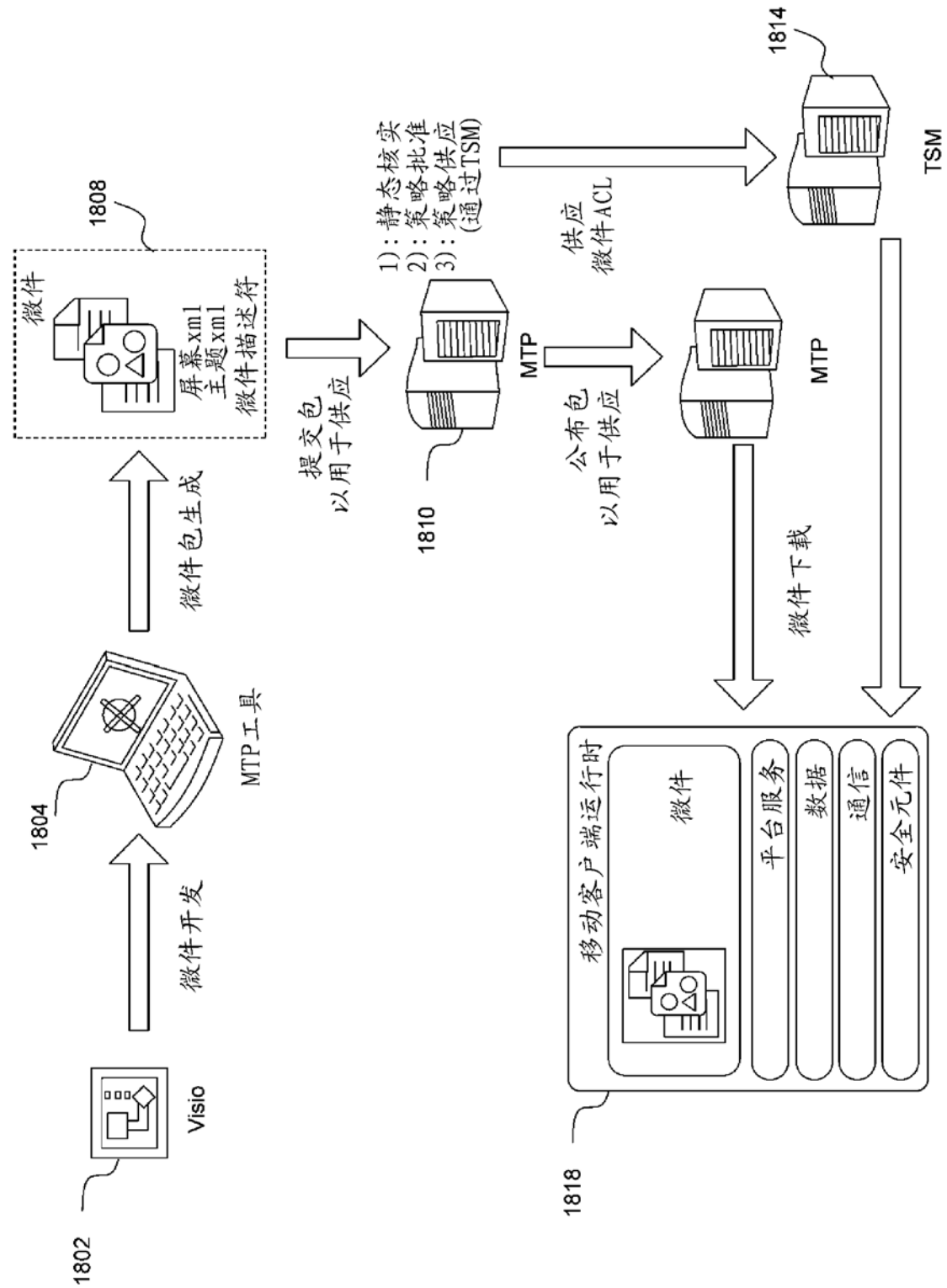


图 18

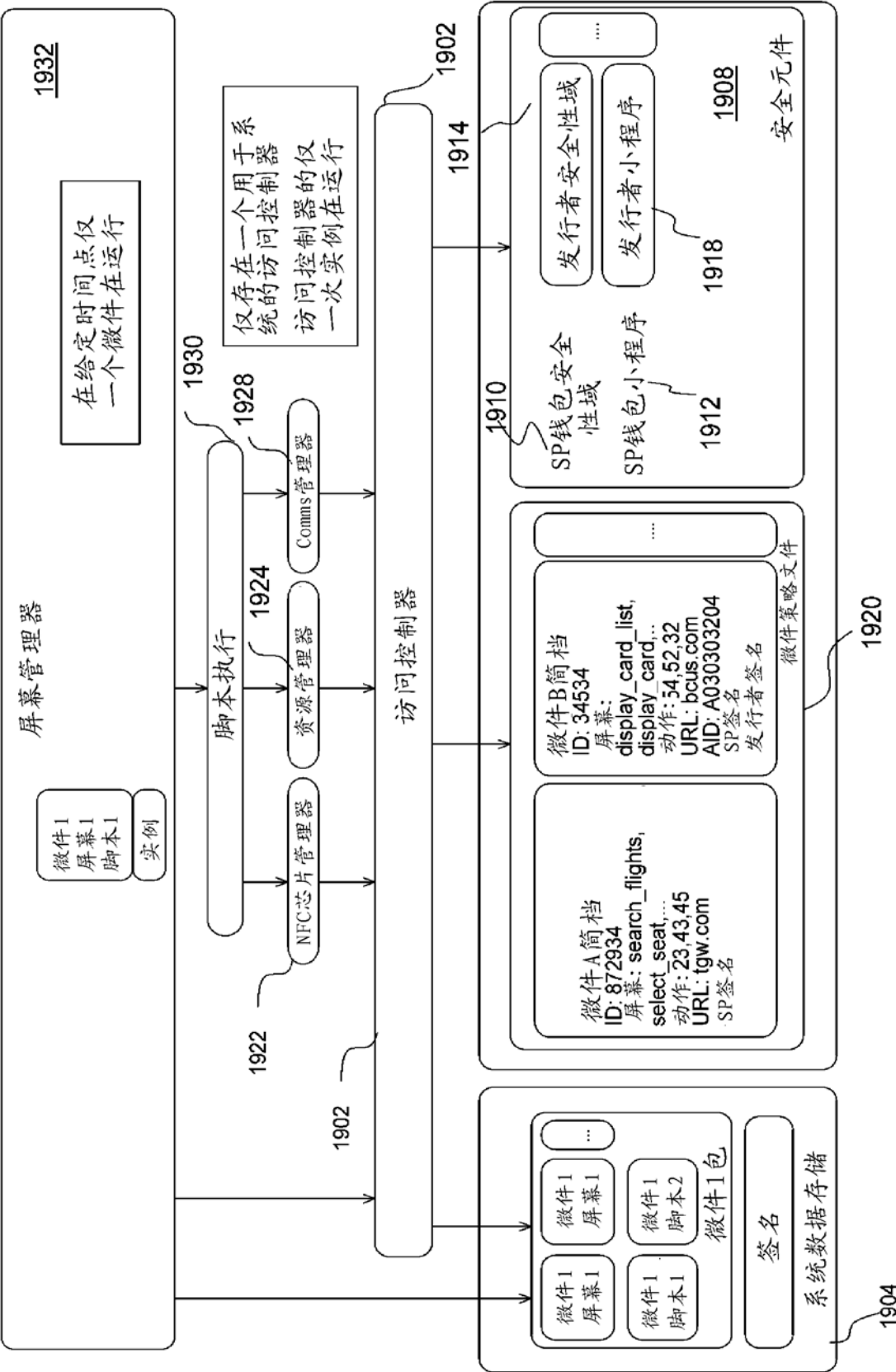


图 19

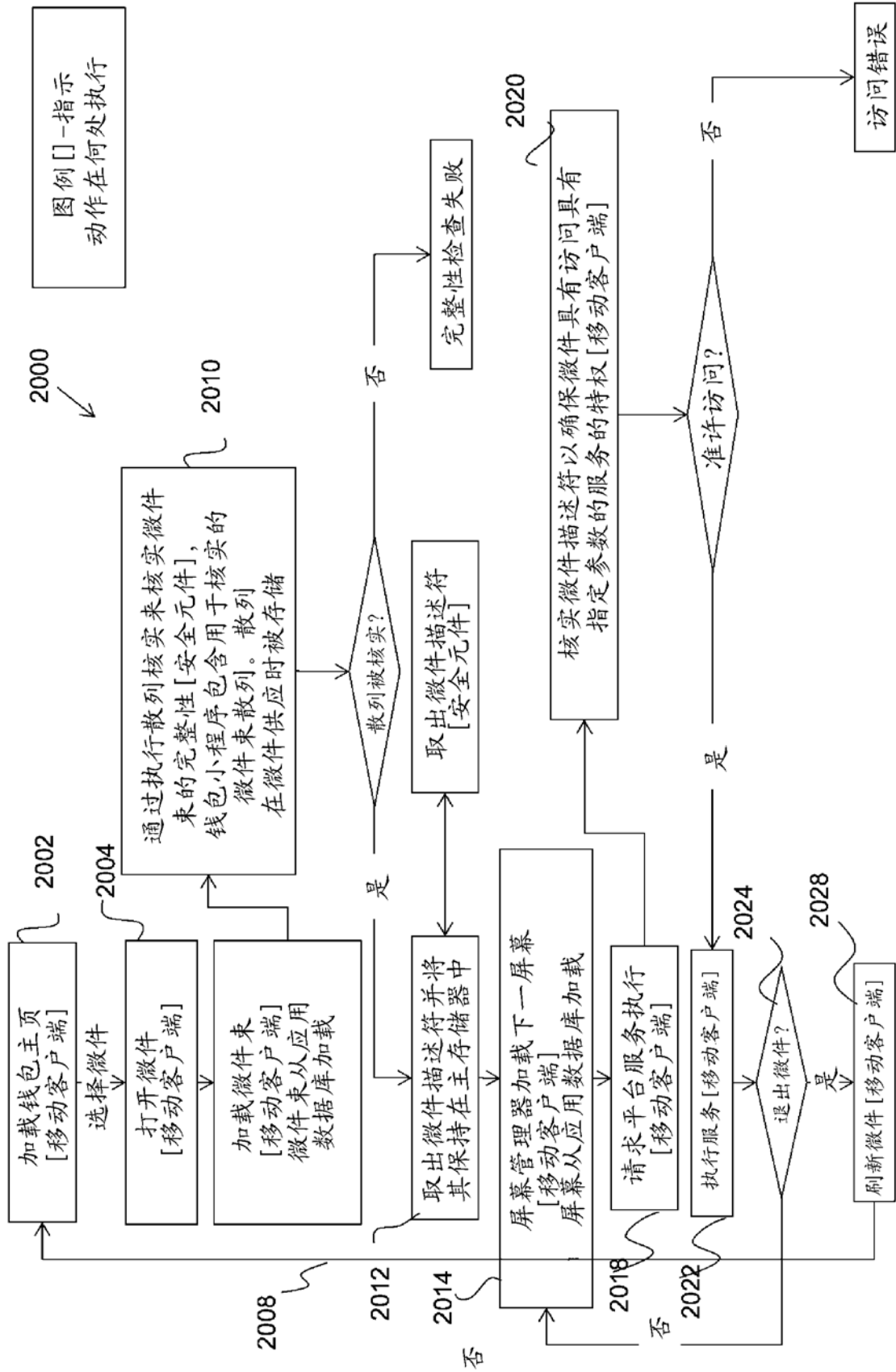


图 20

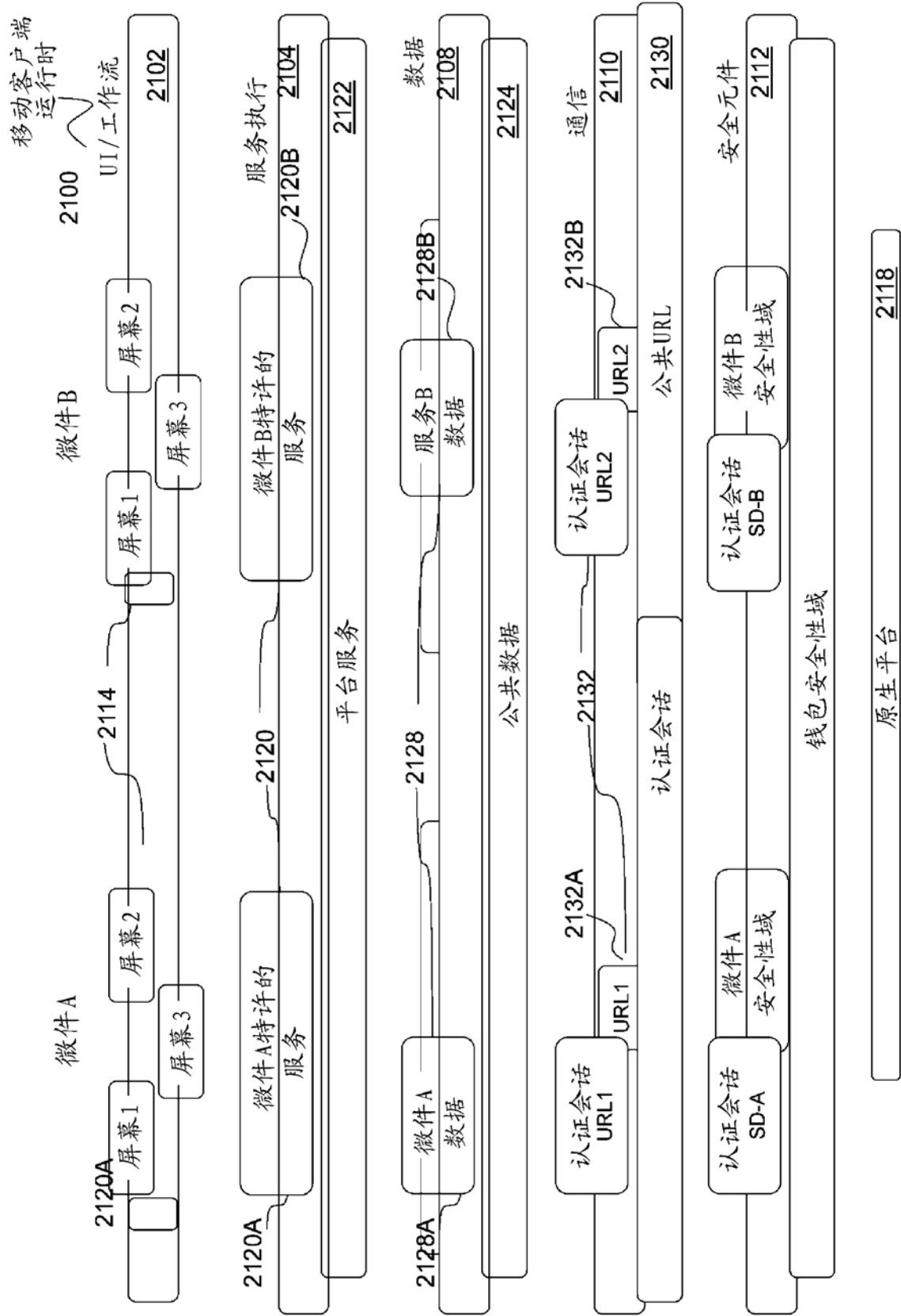


图 21

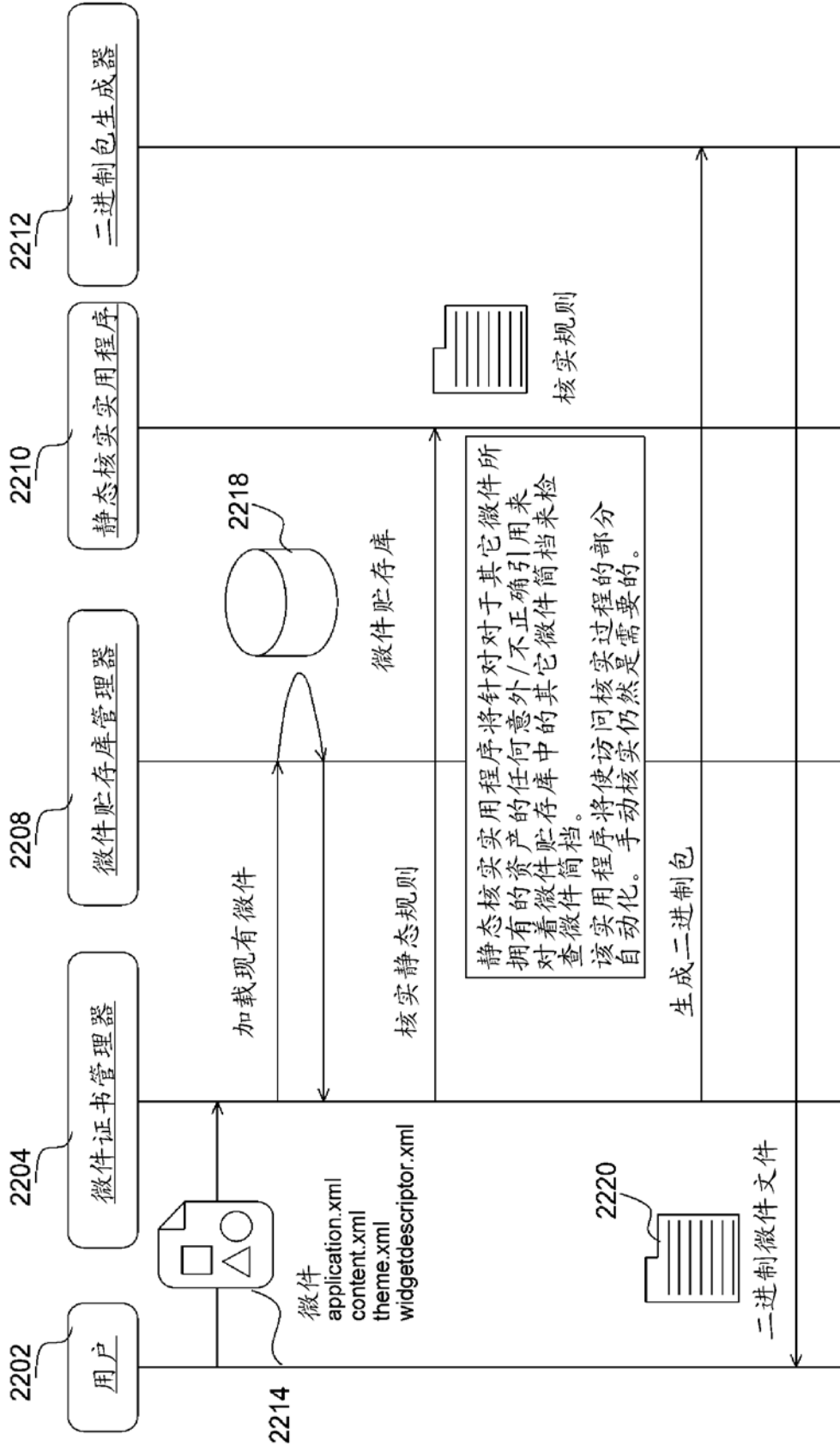


图 22

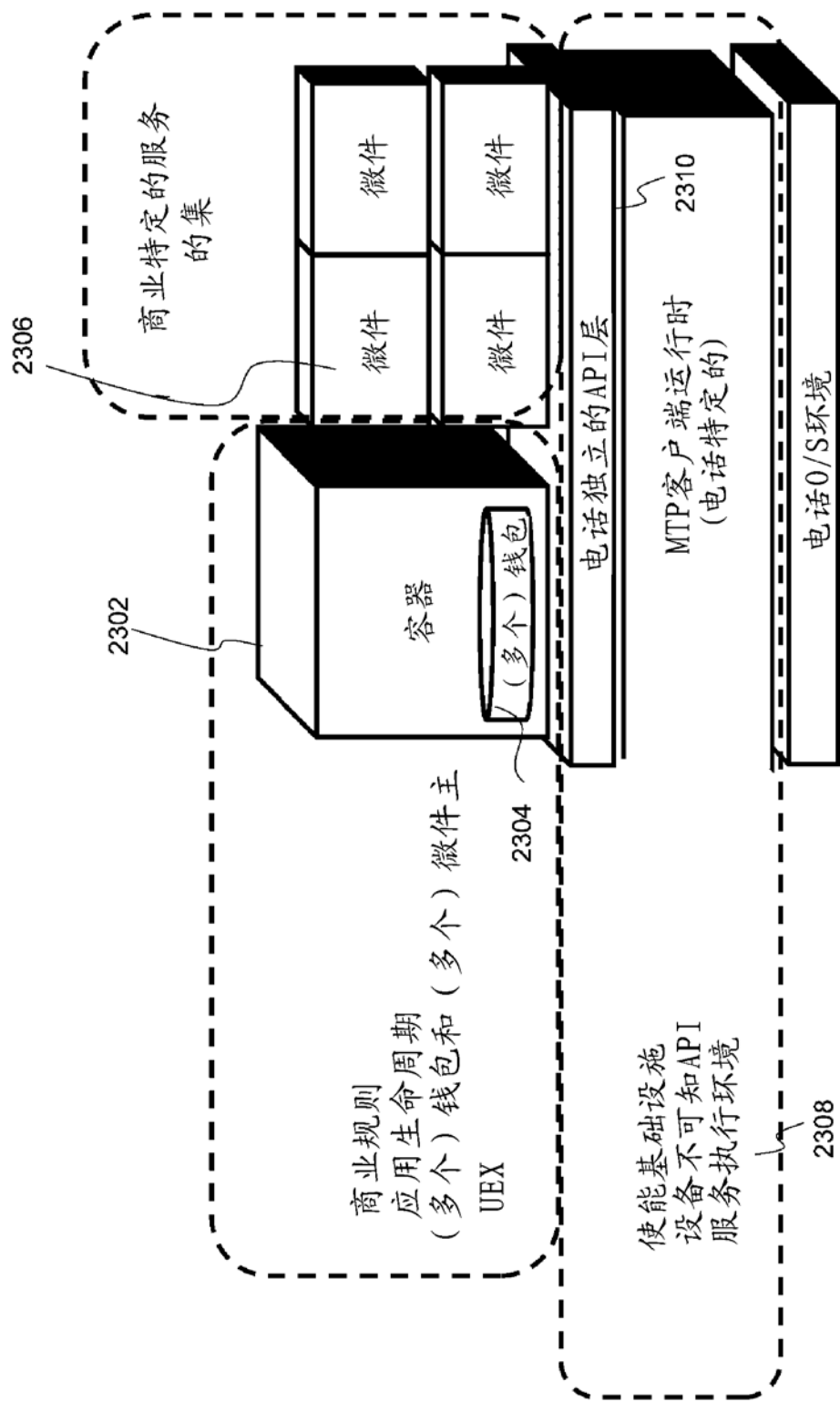


图 23

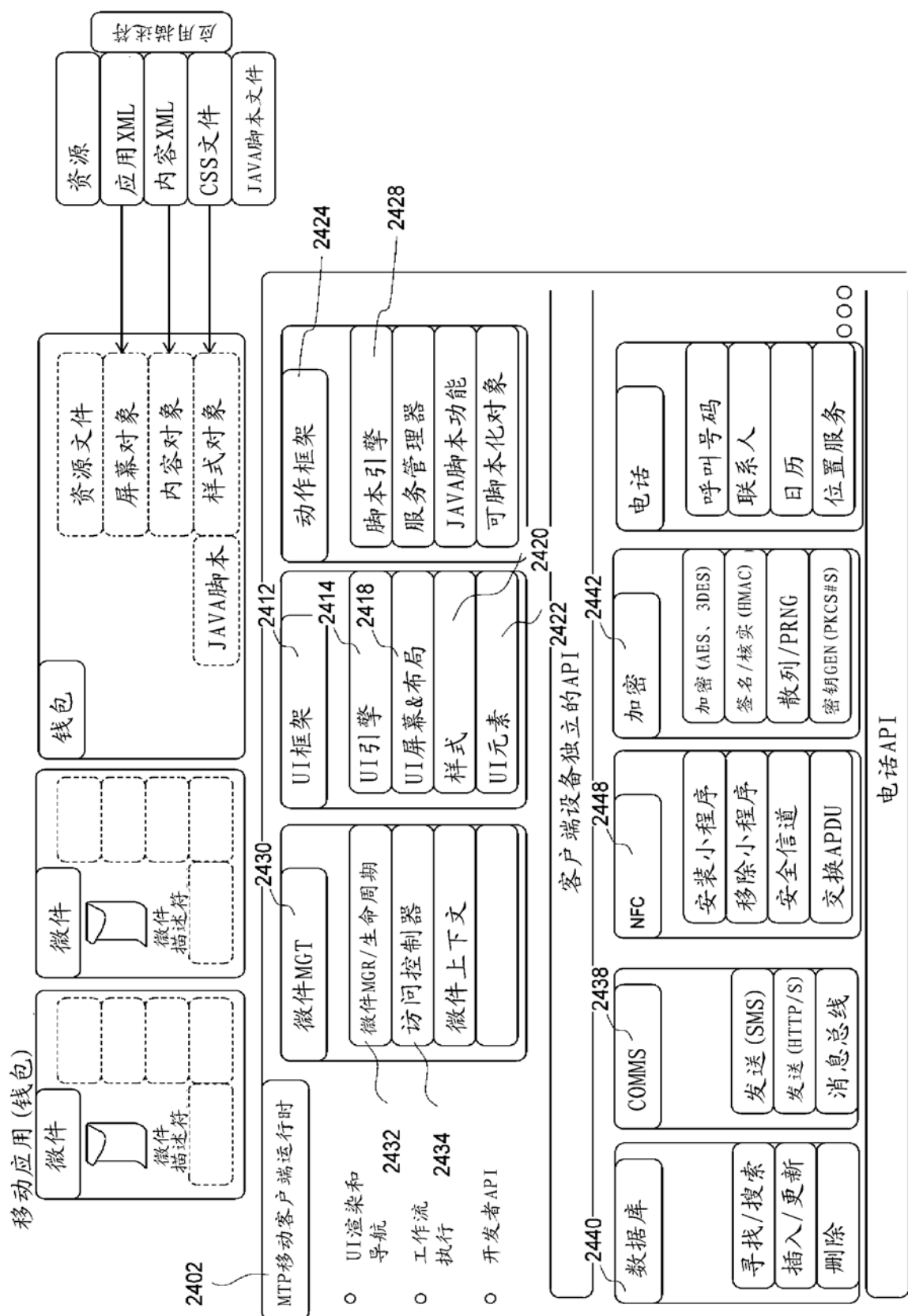


图 24

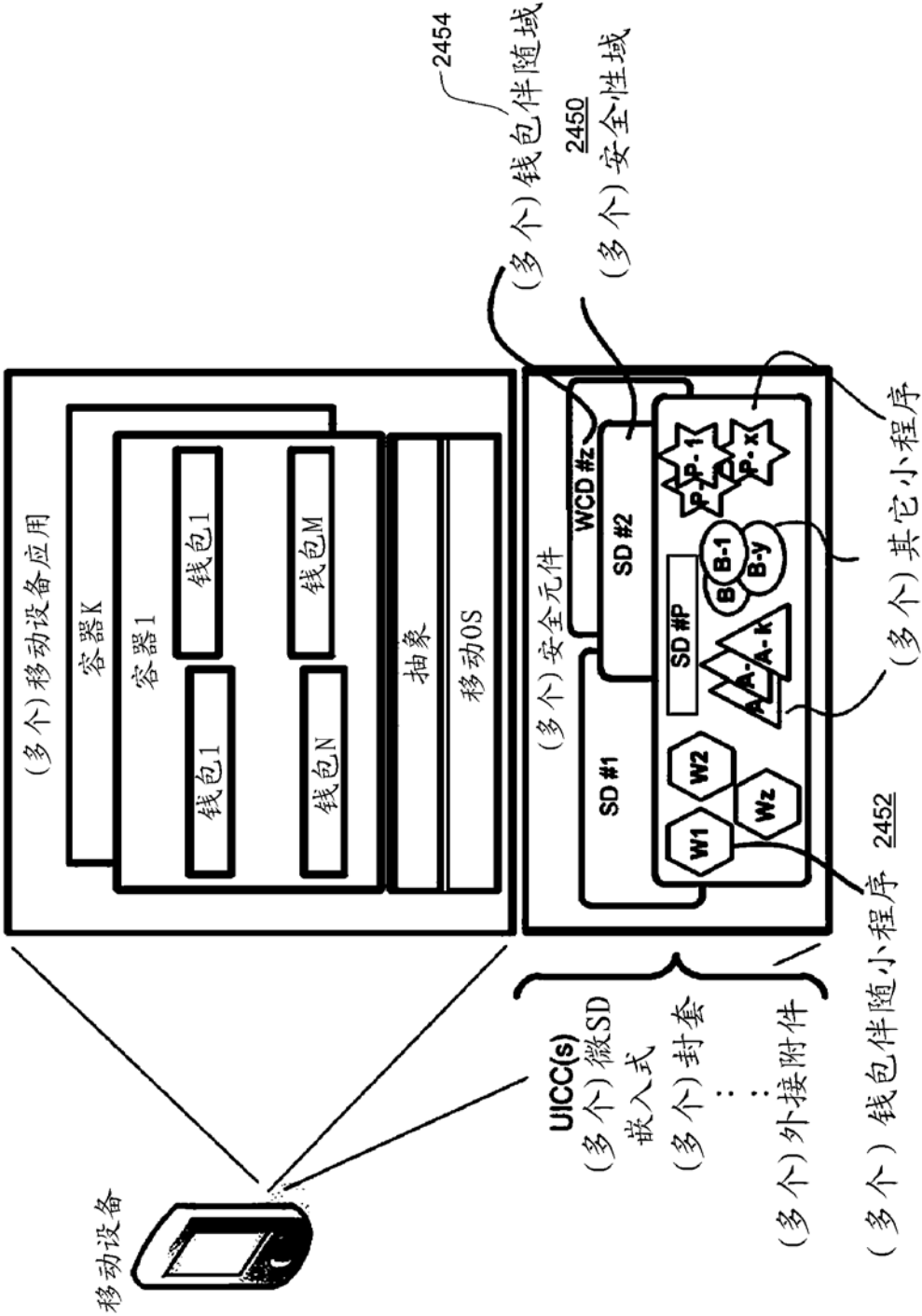


图 24A

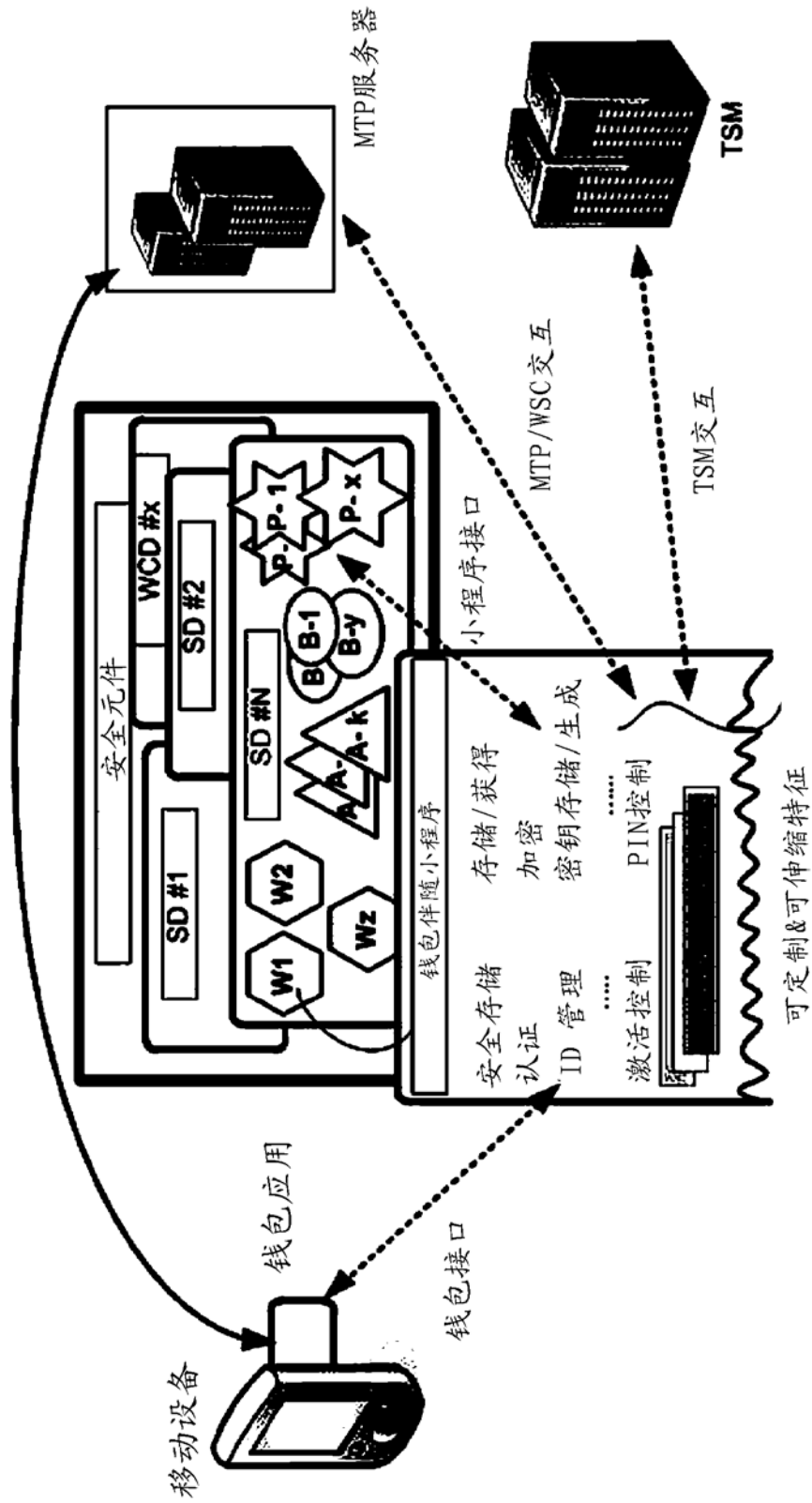


图 24B

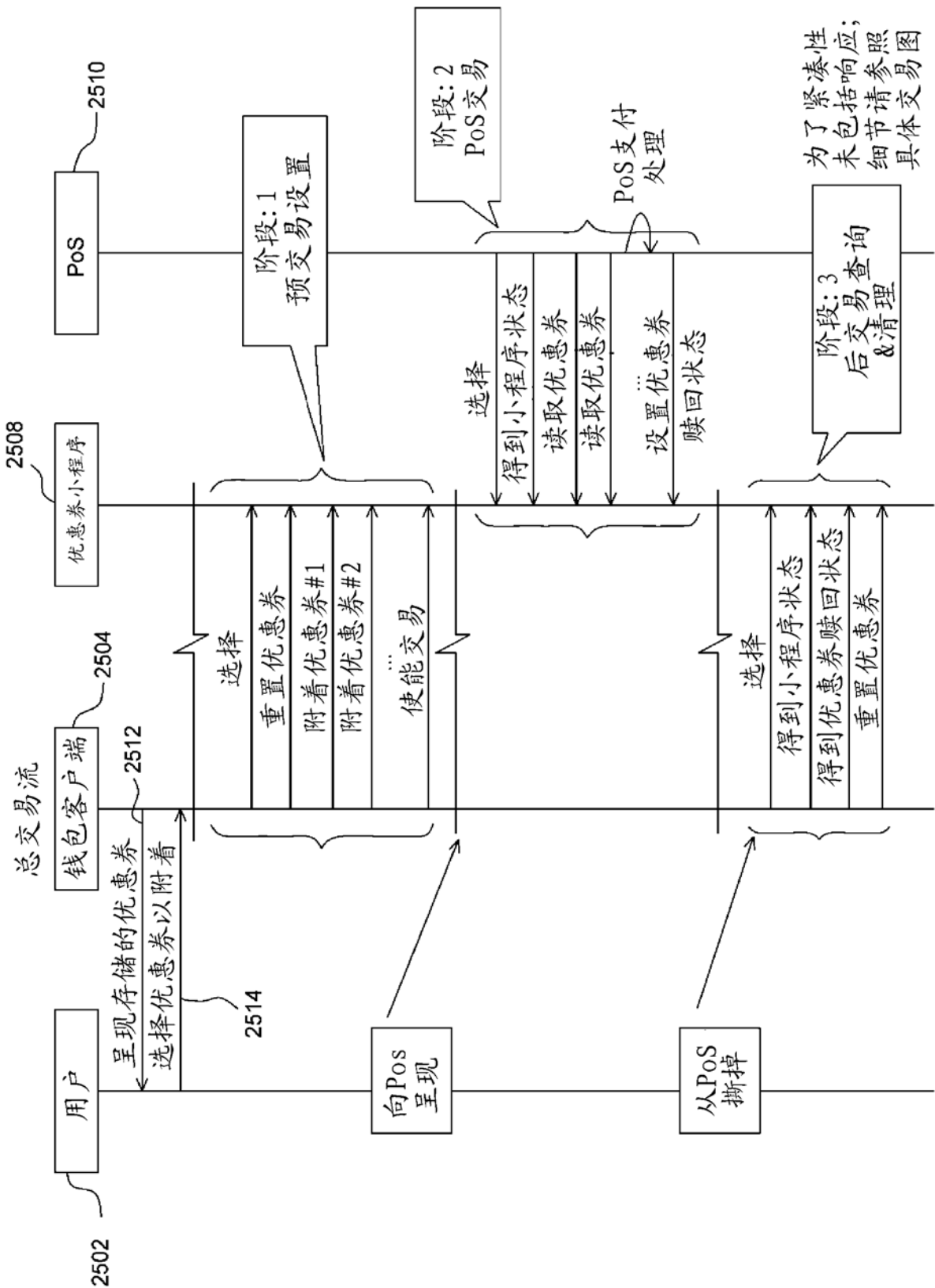


图 25

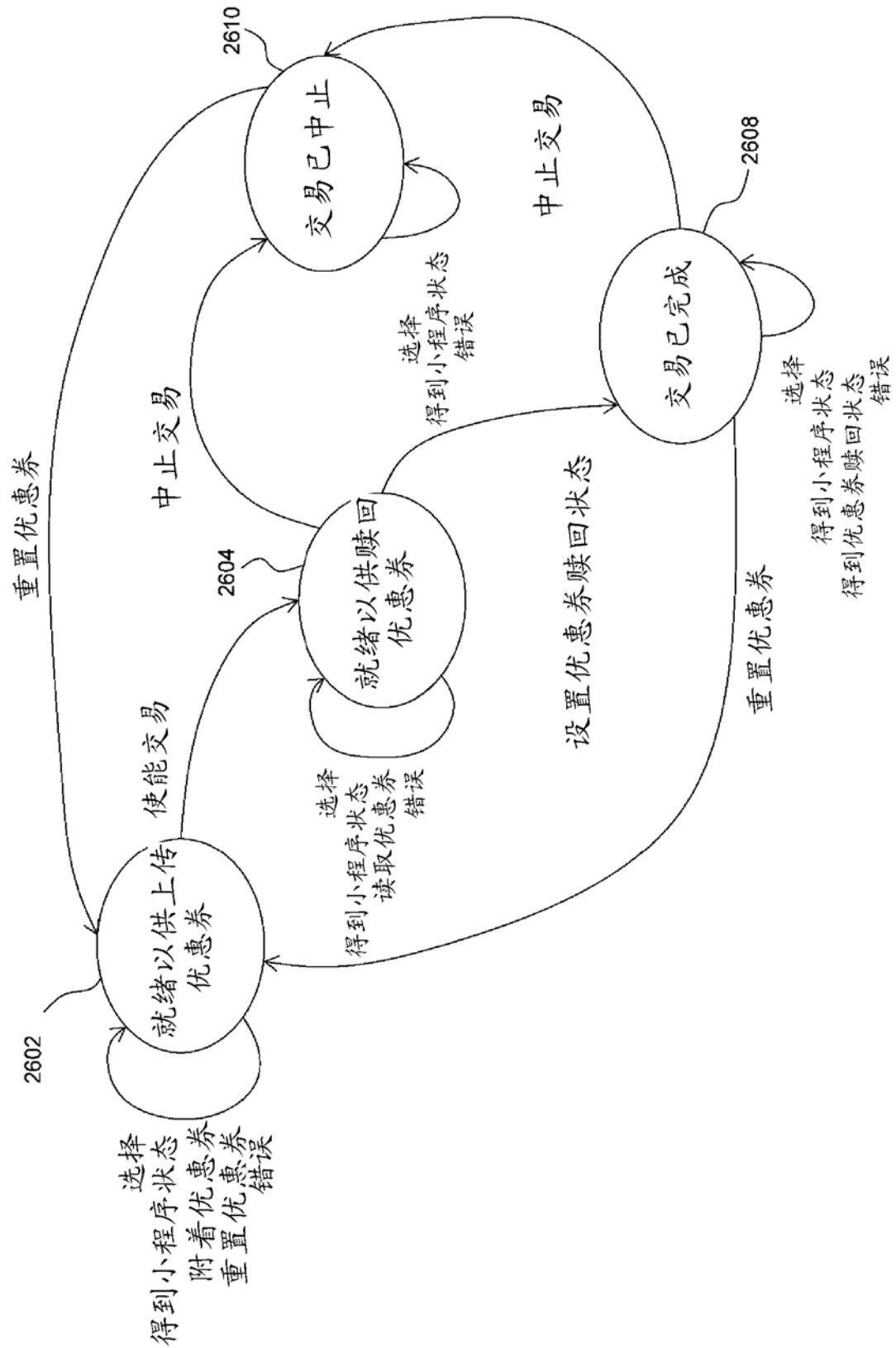


图 26

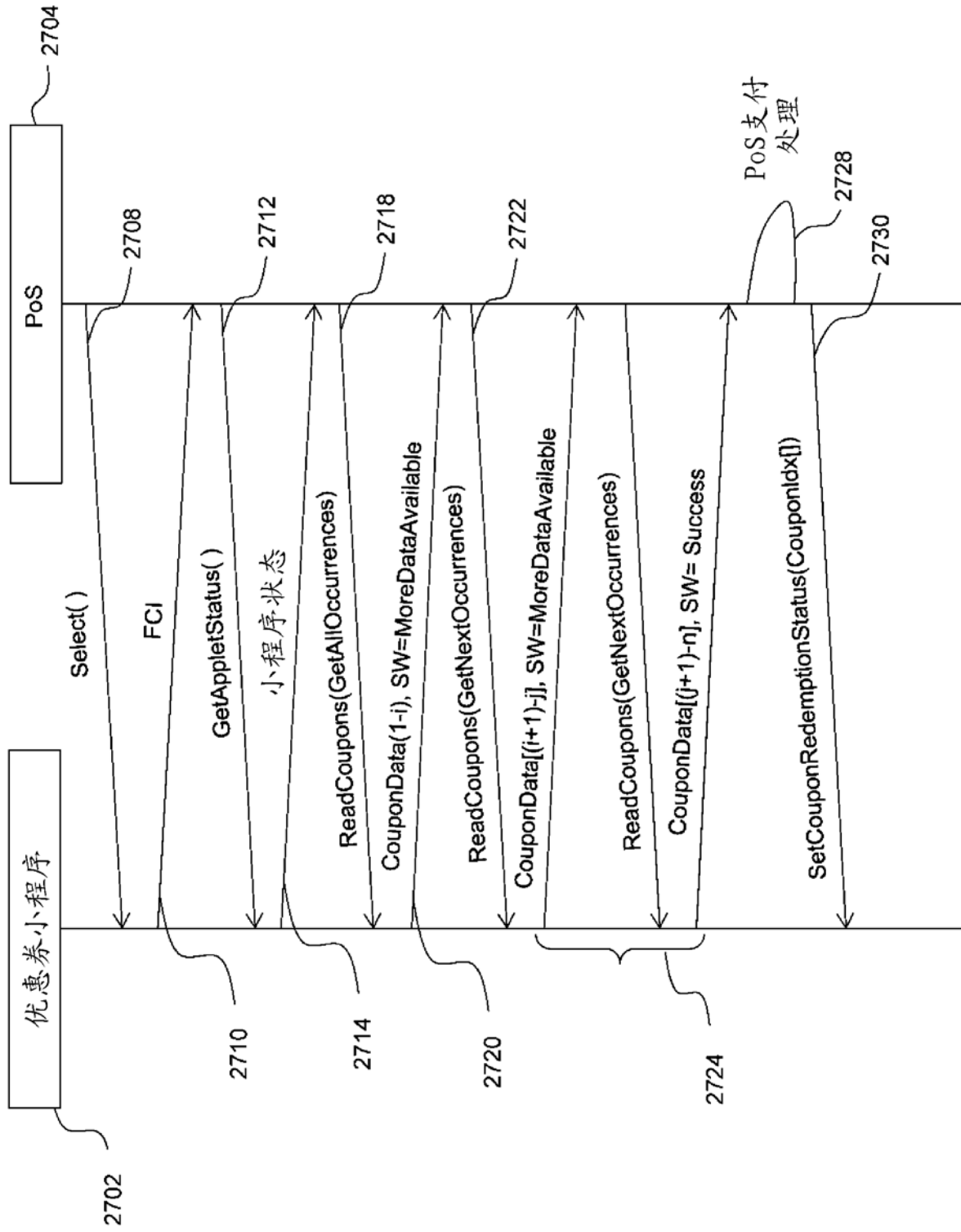


图 27

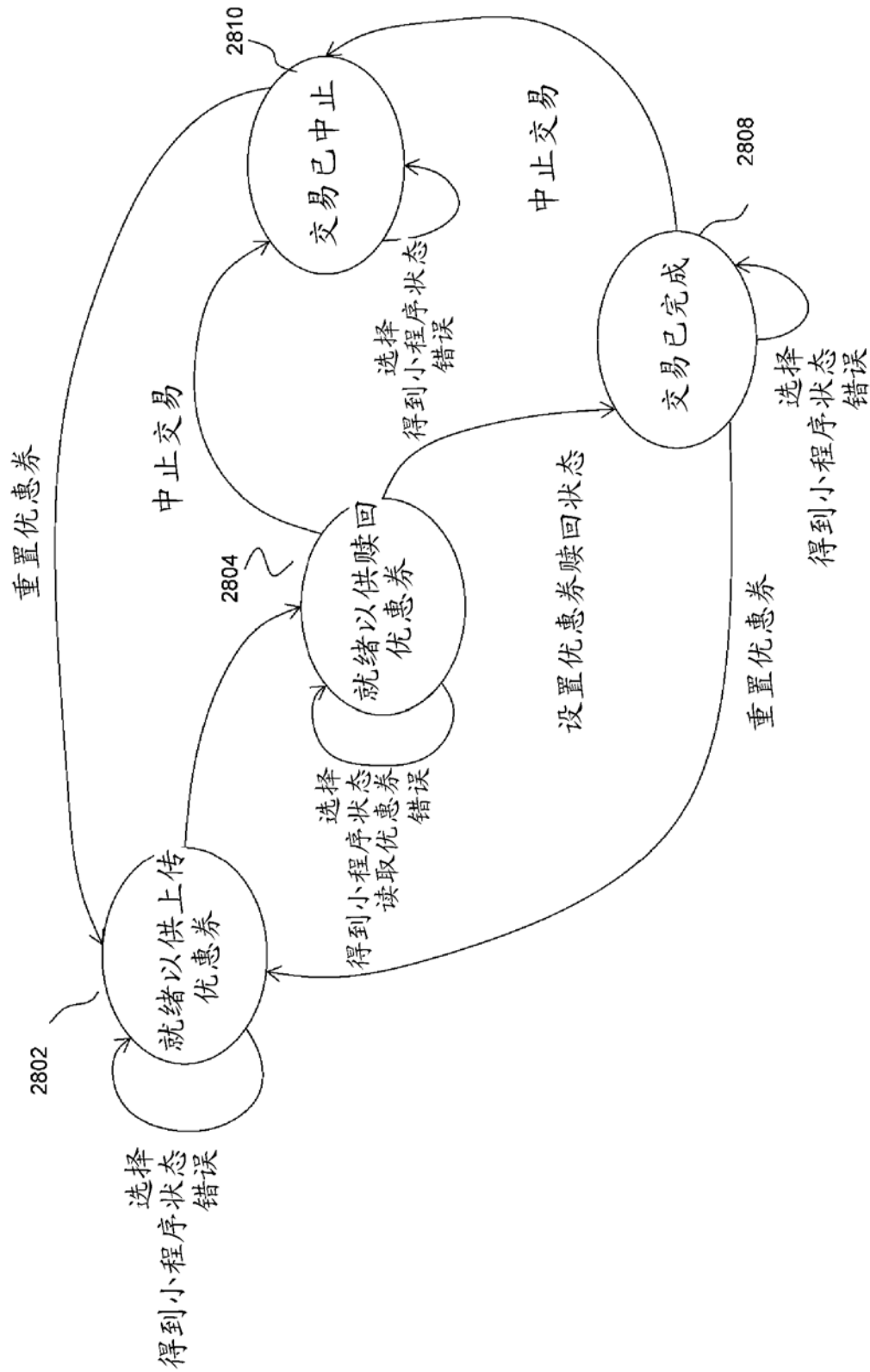


图 28

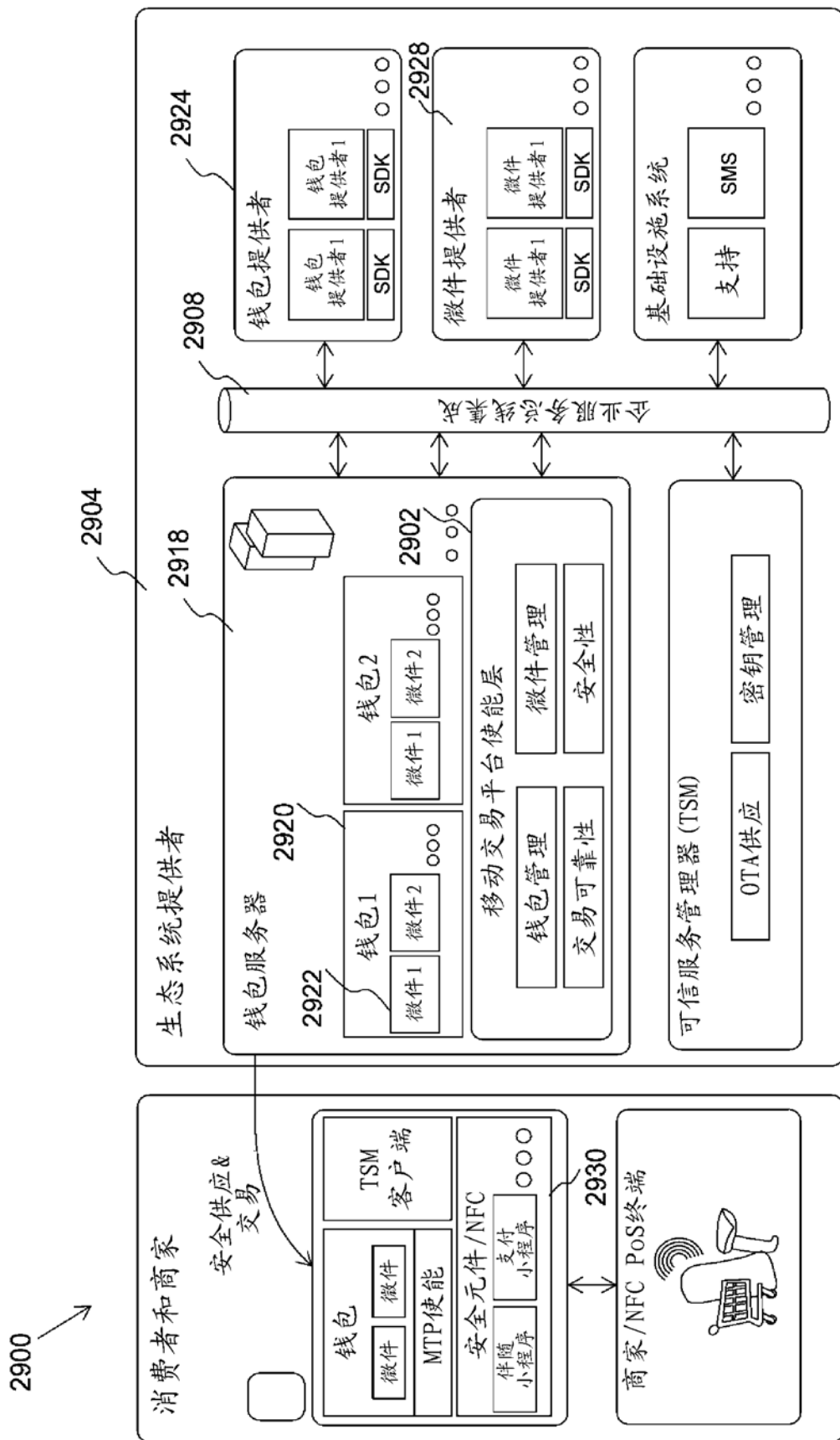


图 29

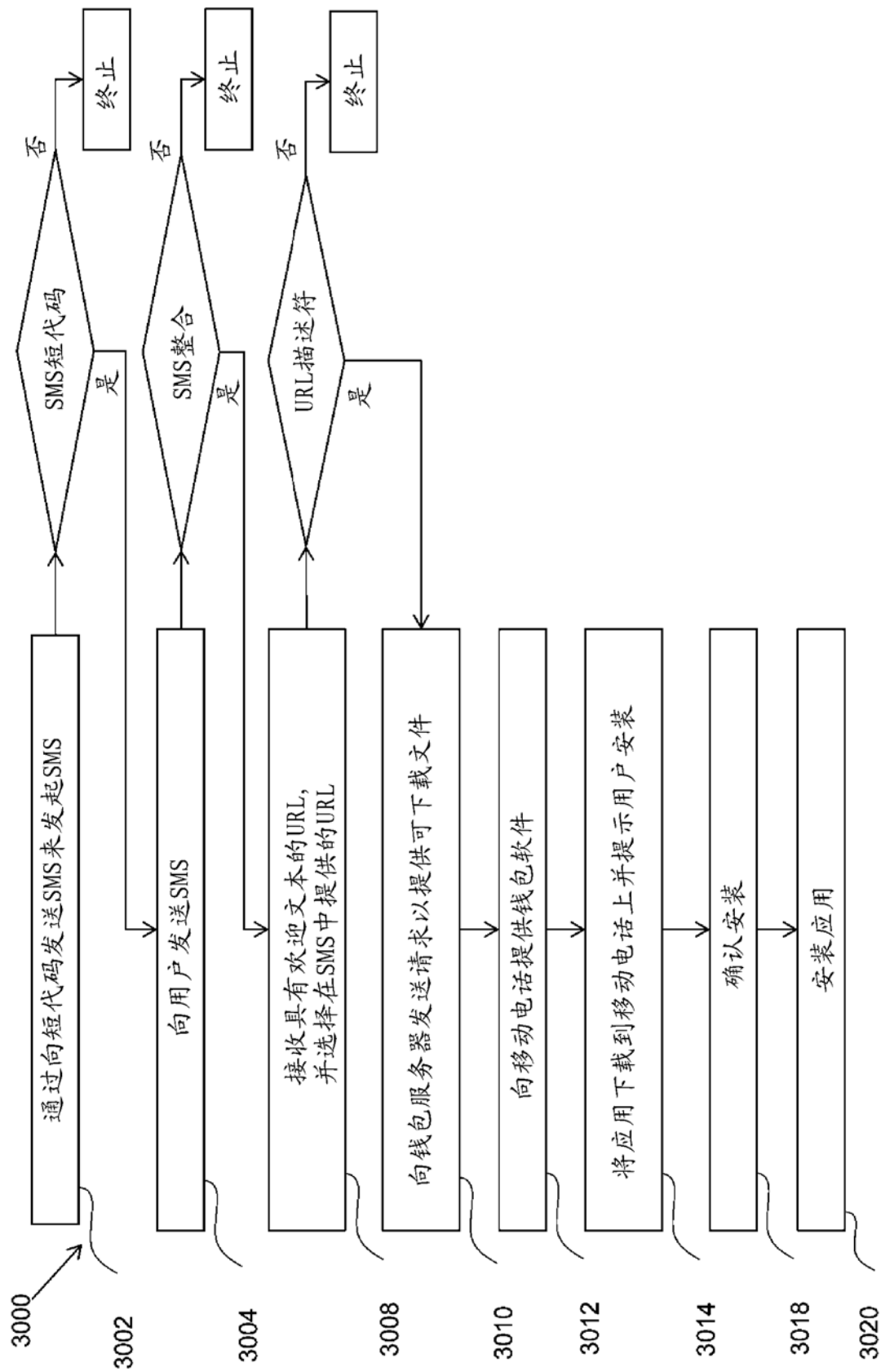


图 30

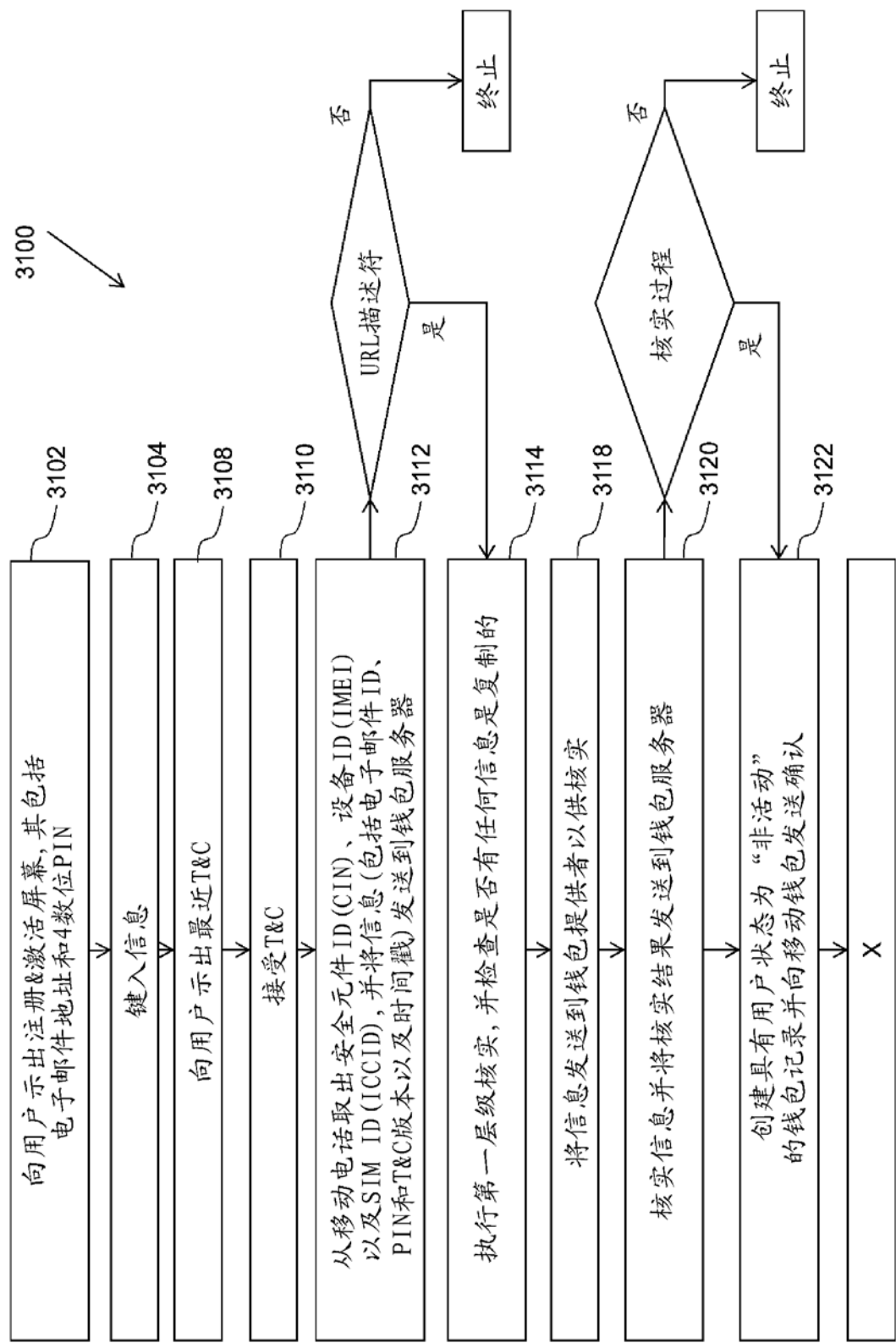


图 31A

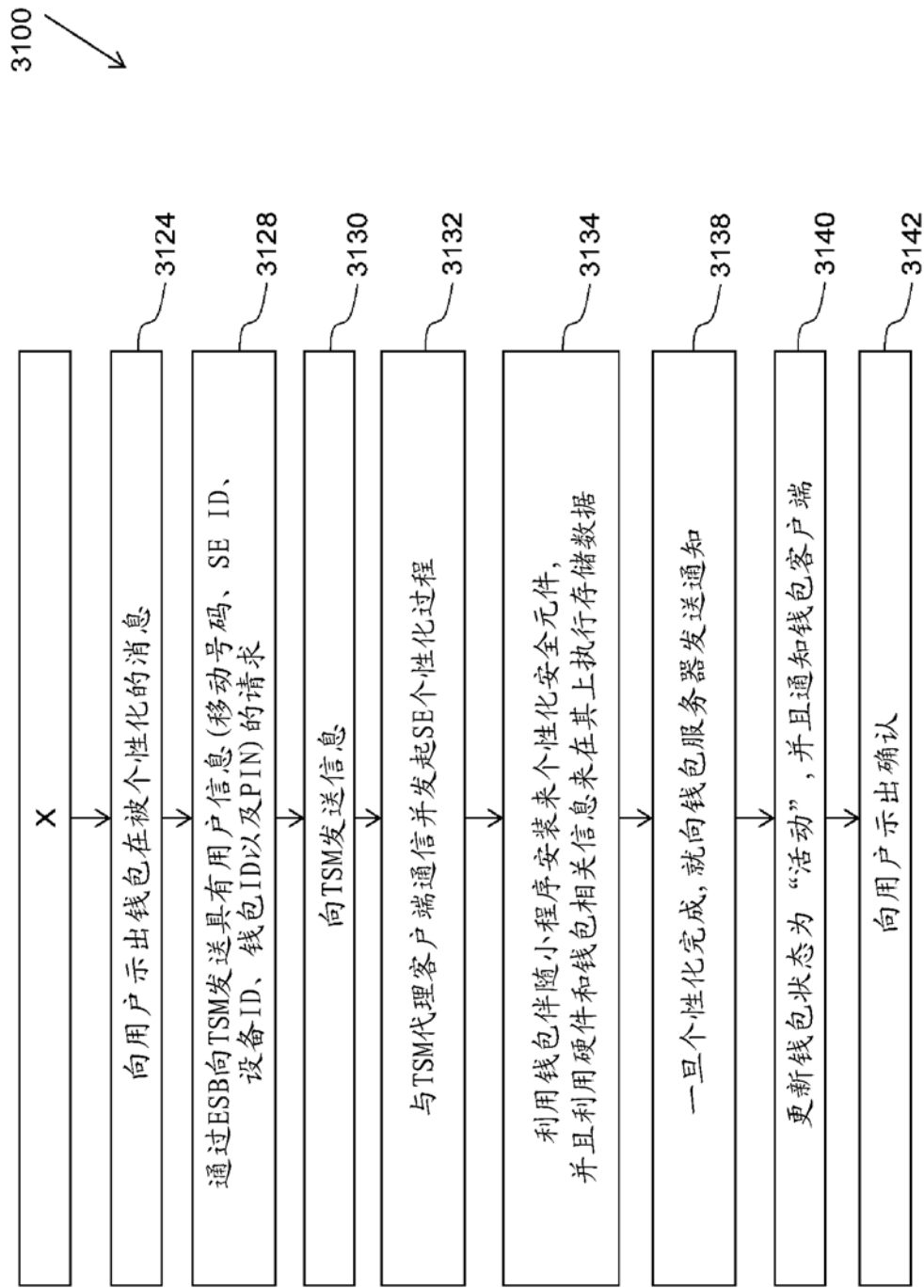


图 31B

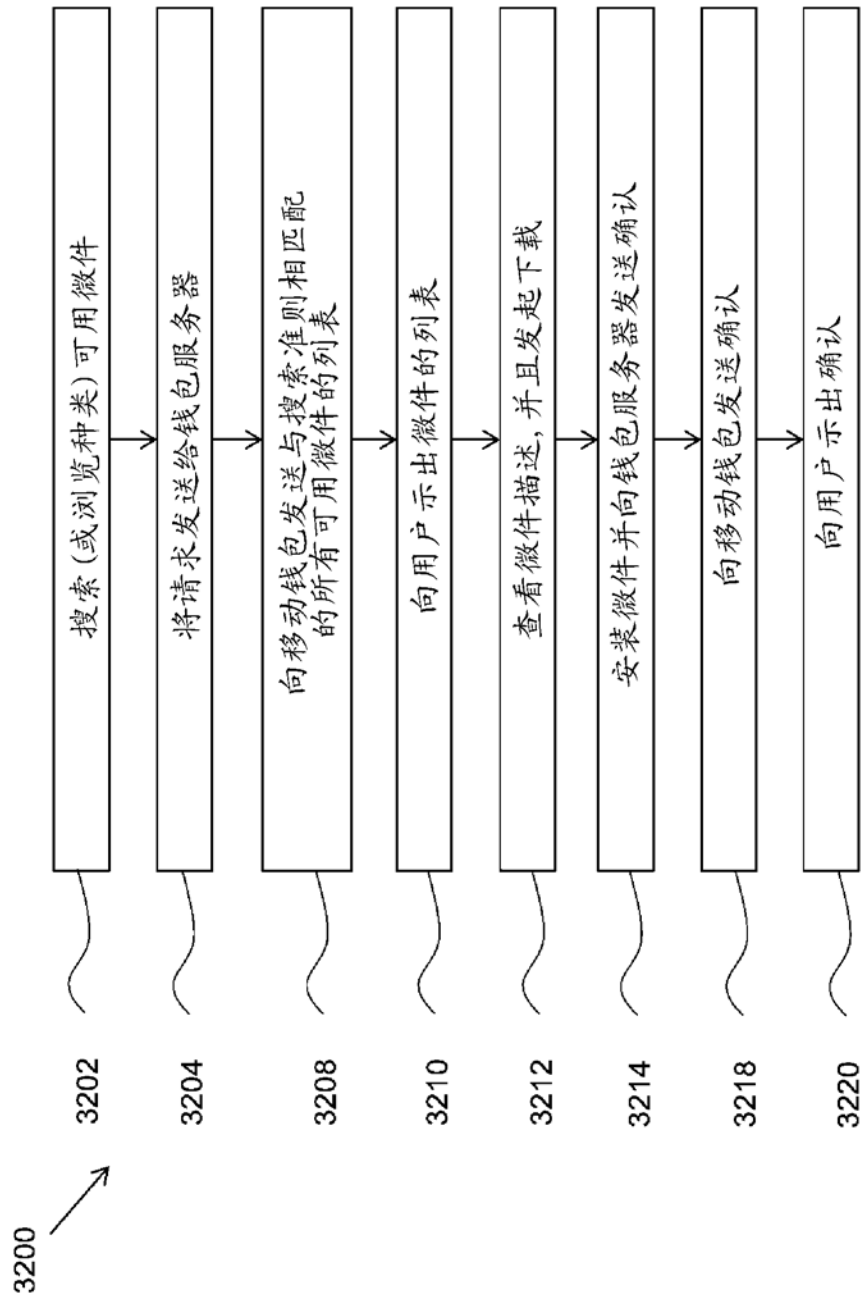


图 32

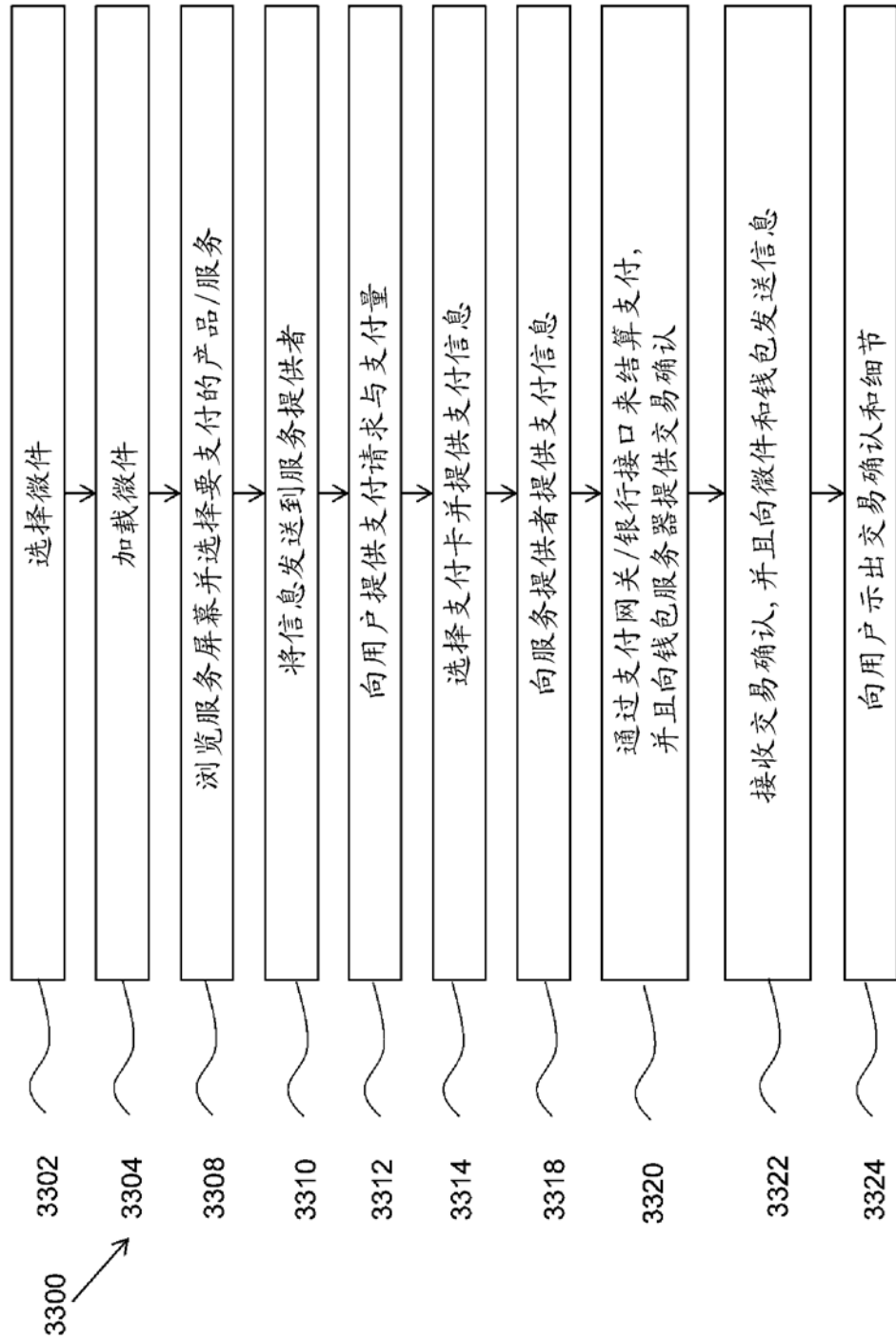


图 33

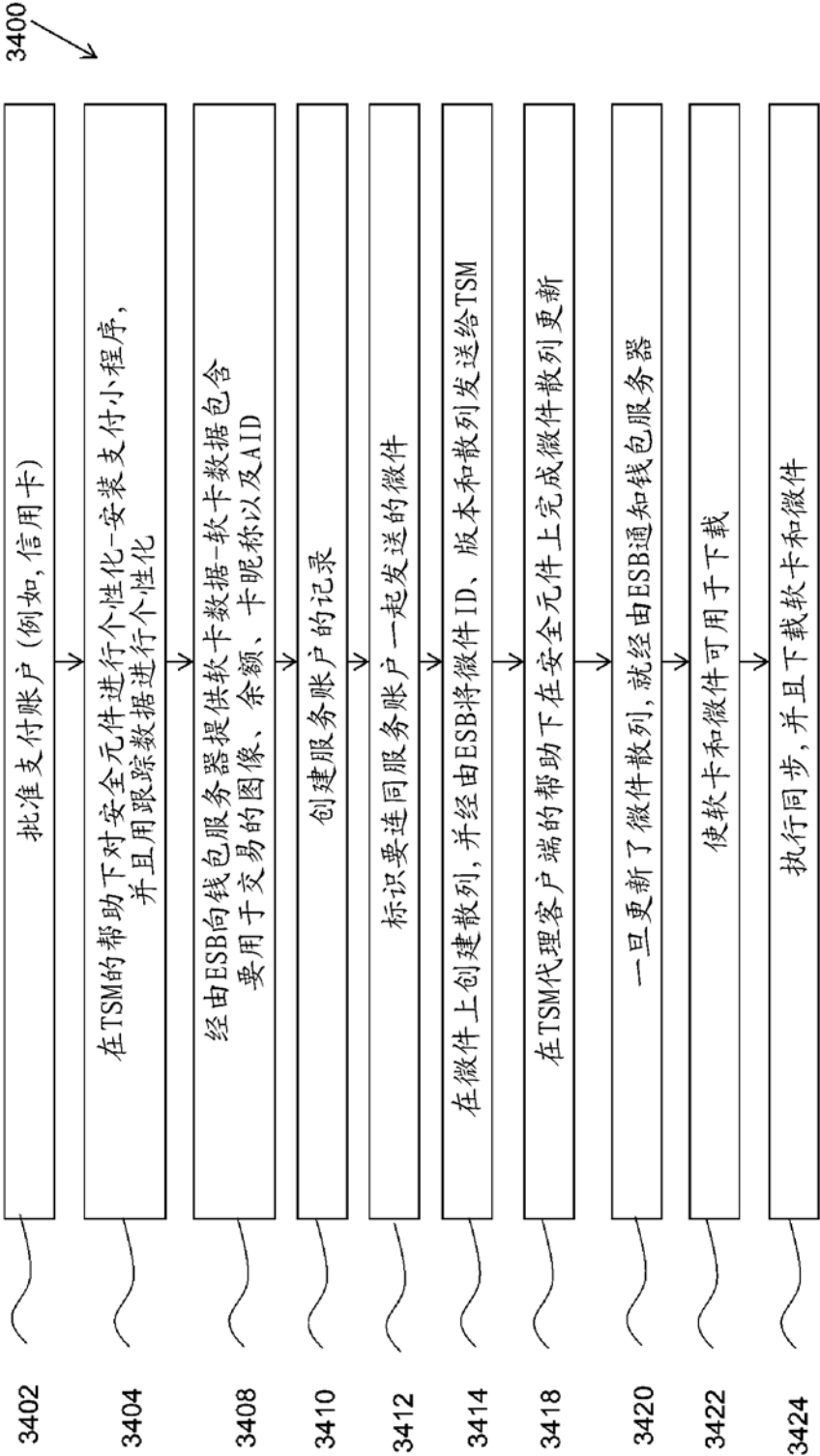


图 34



图 35

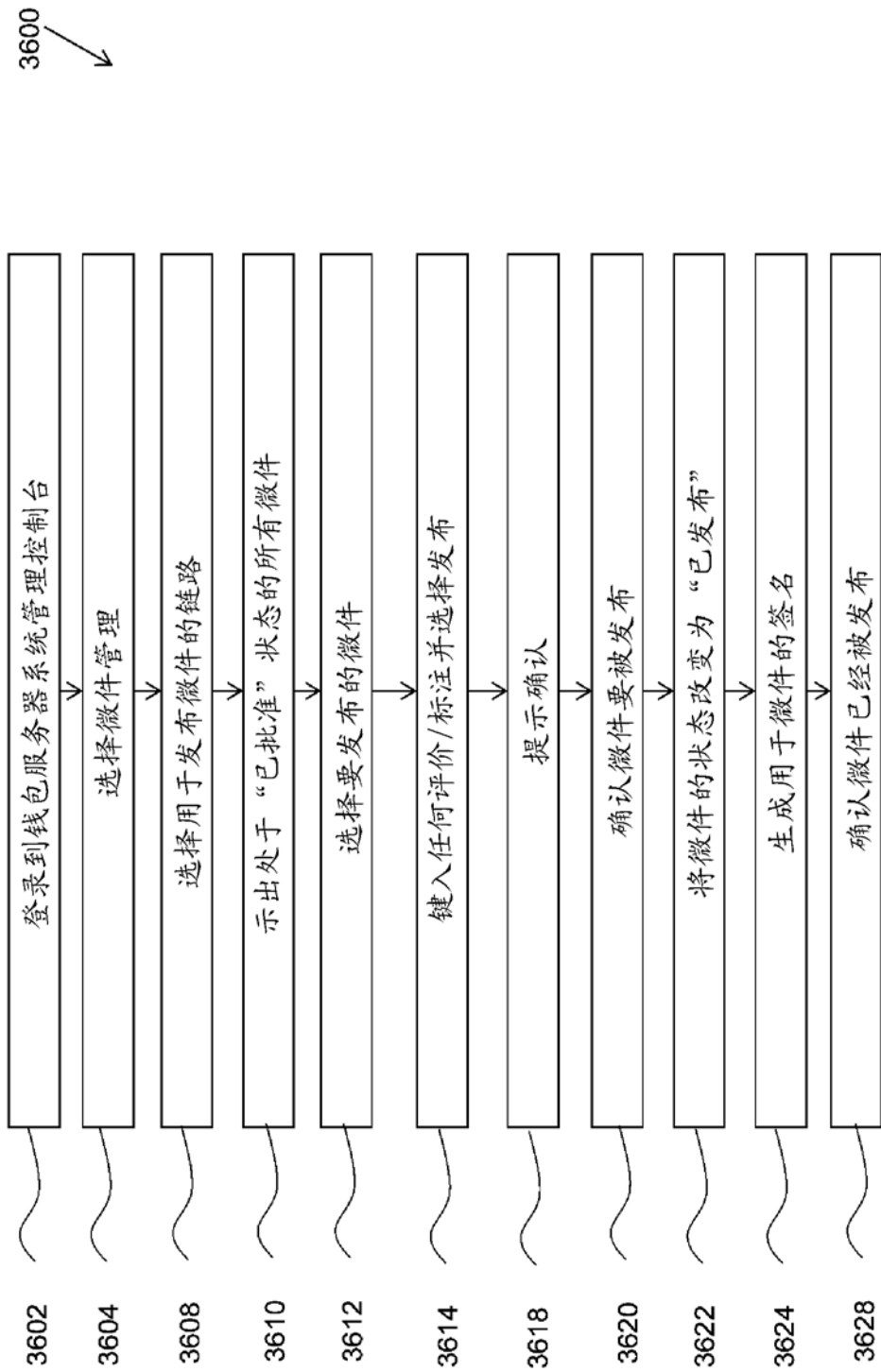


图 36

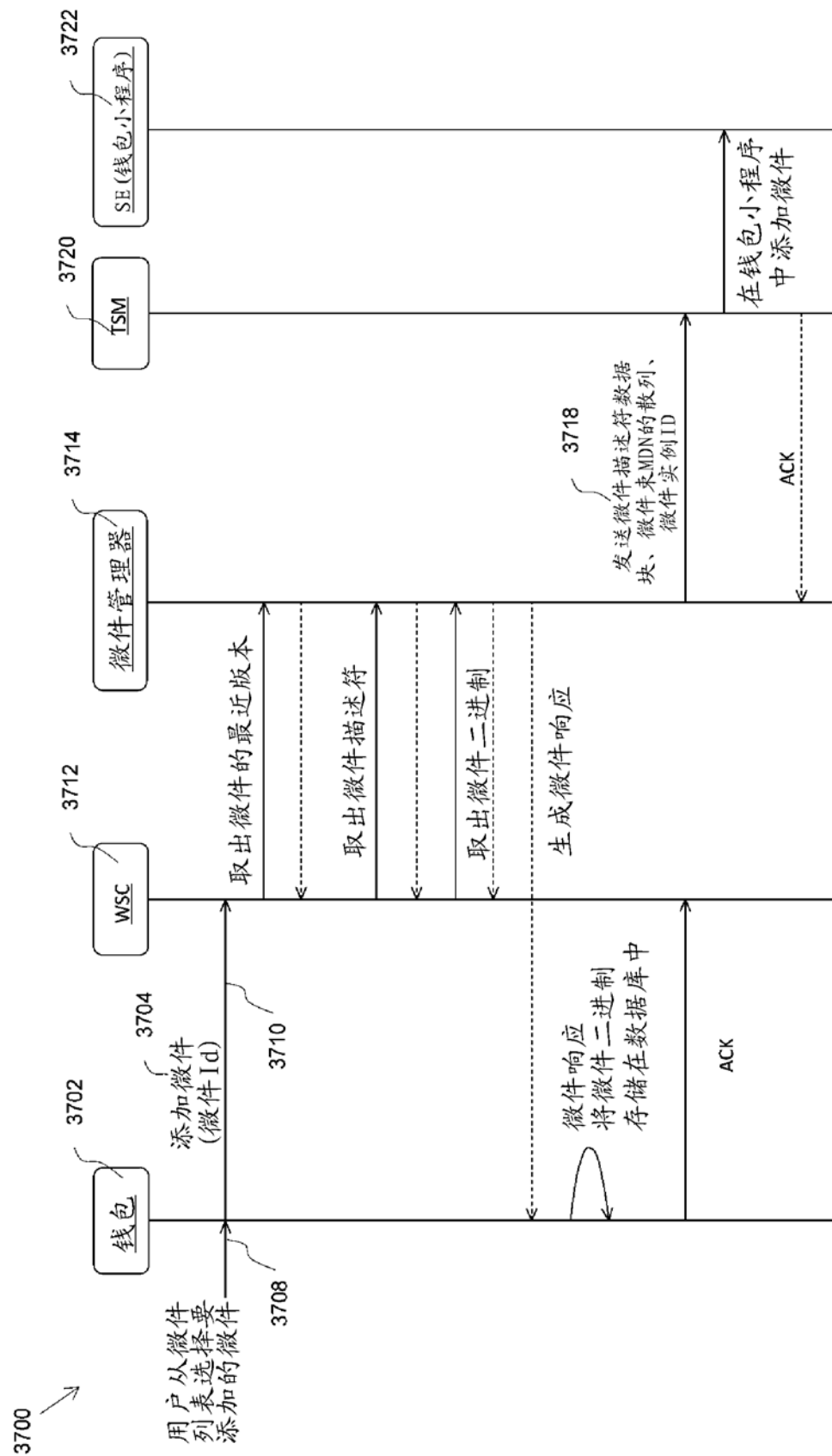


图 37

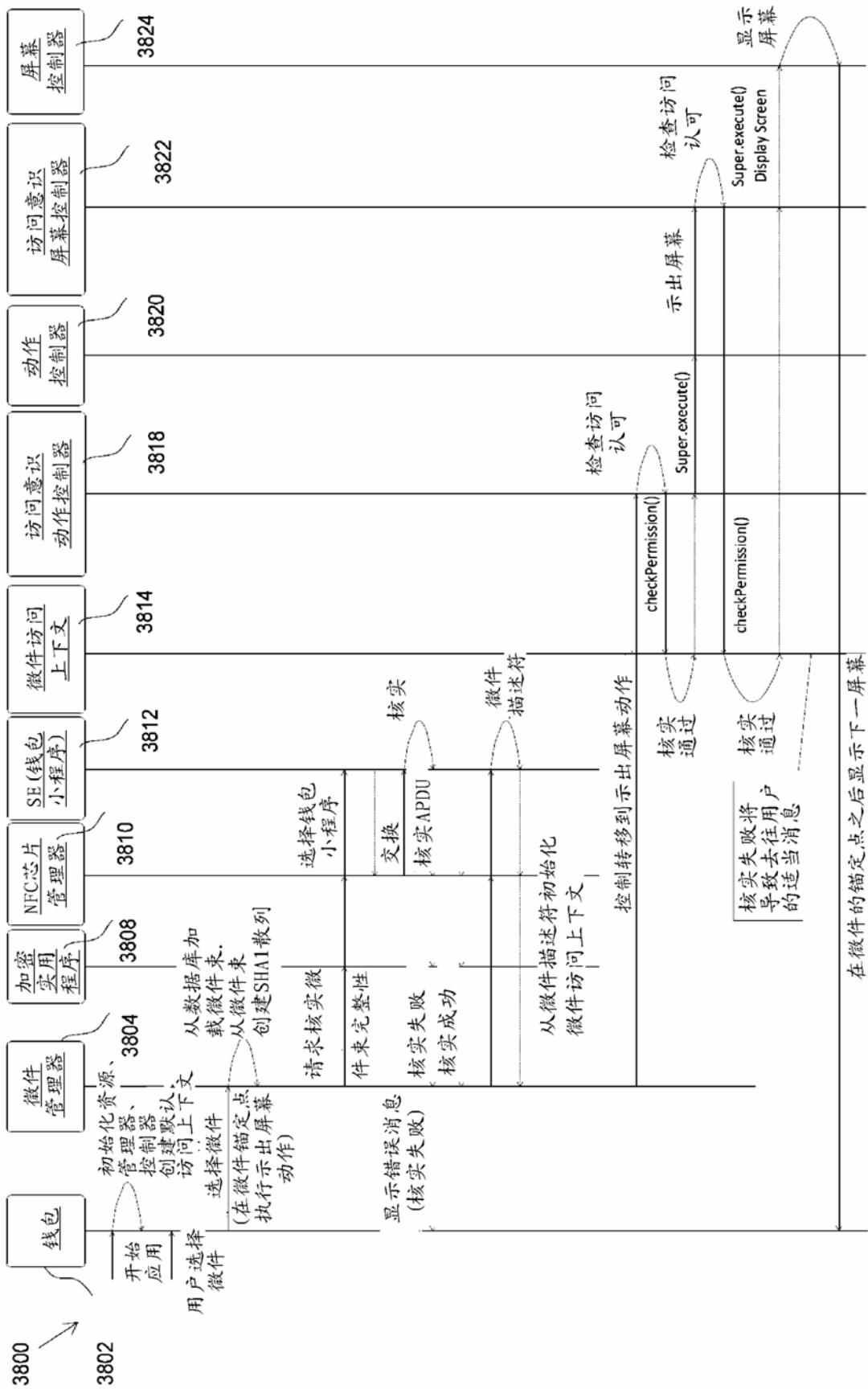


图 38

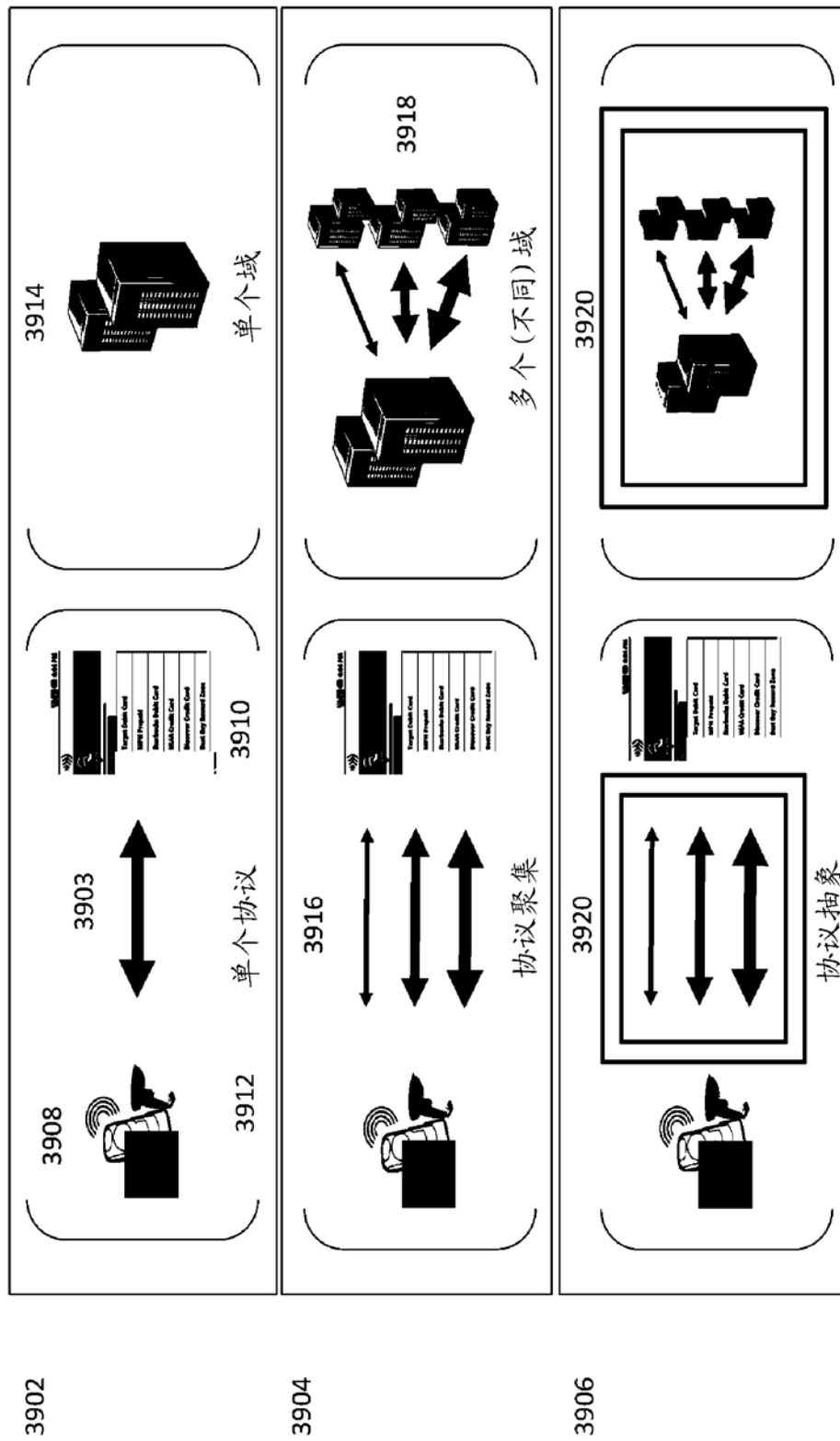


图 39

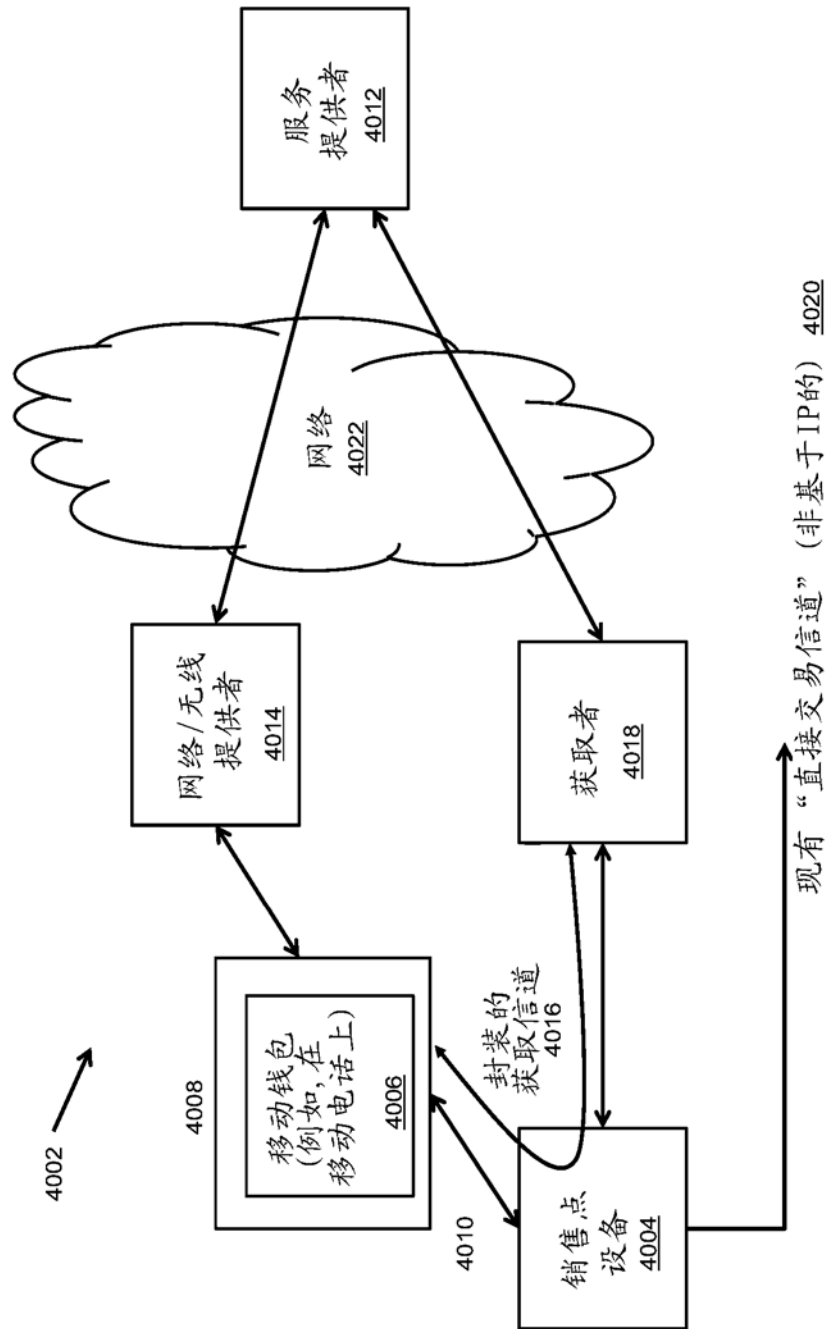


图 40

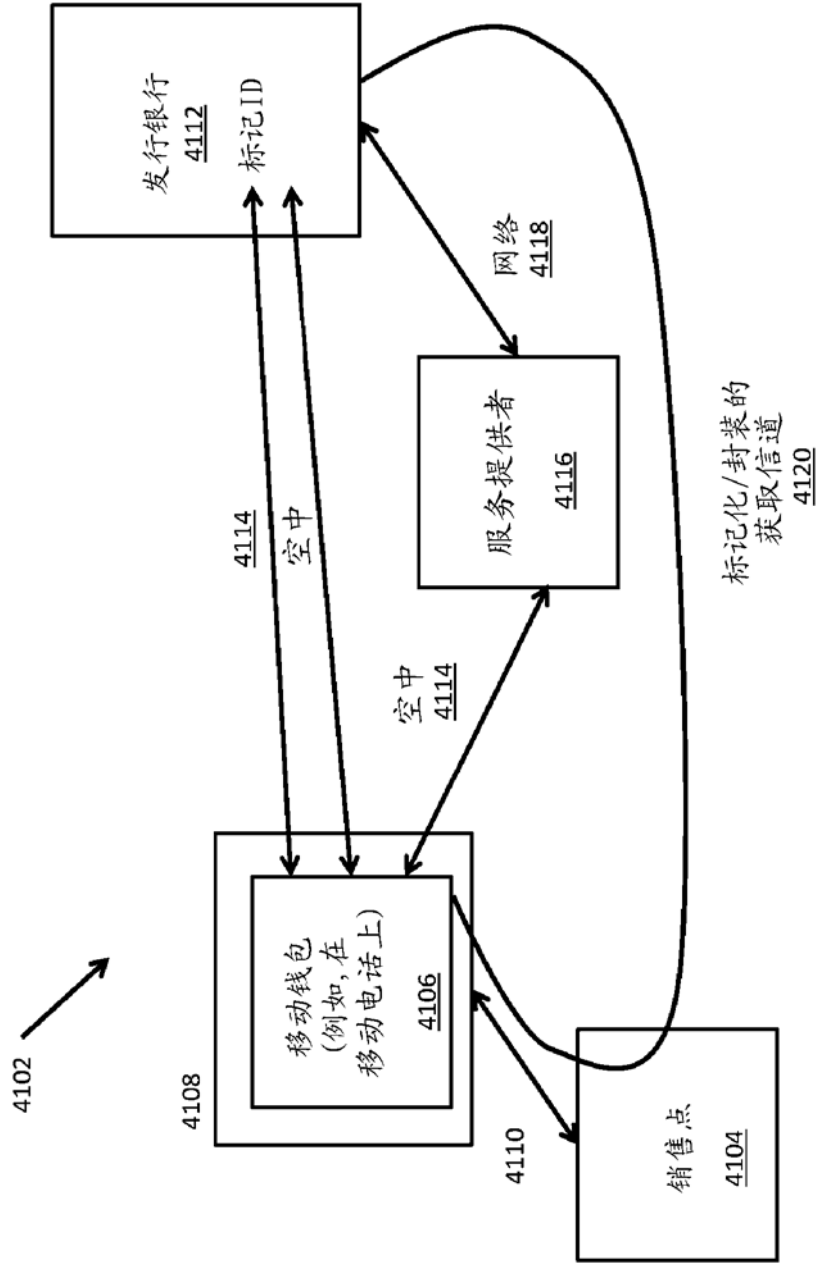


图 41

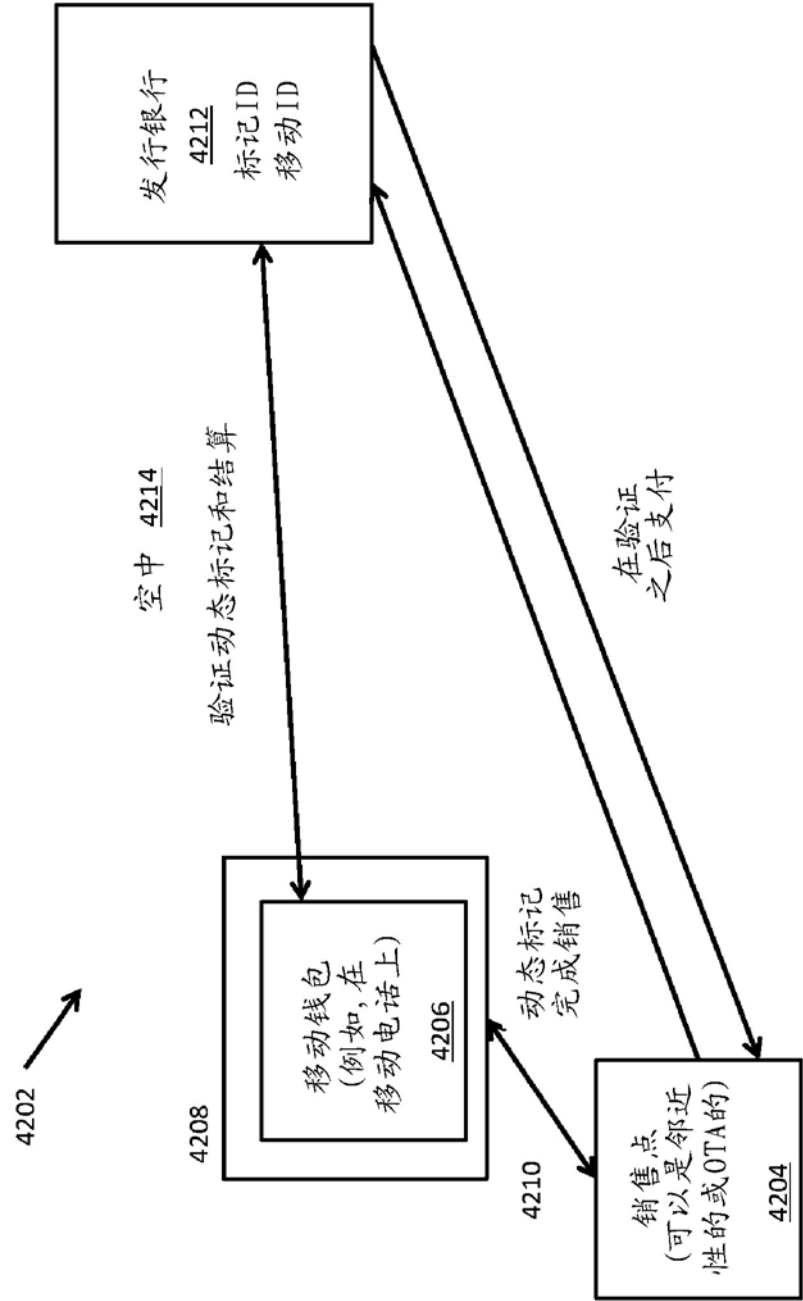


图 42

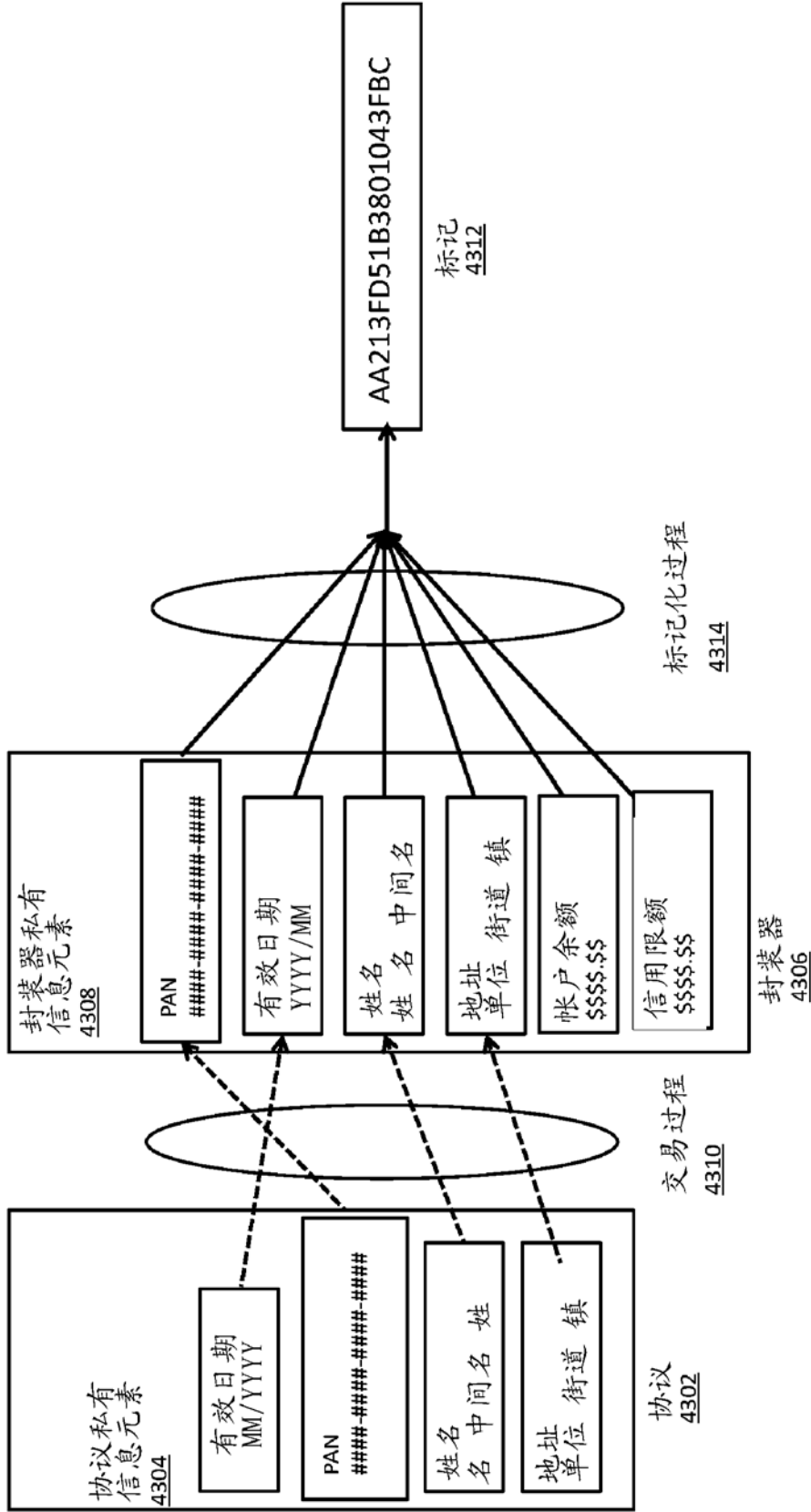


图 43

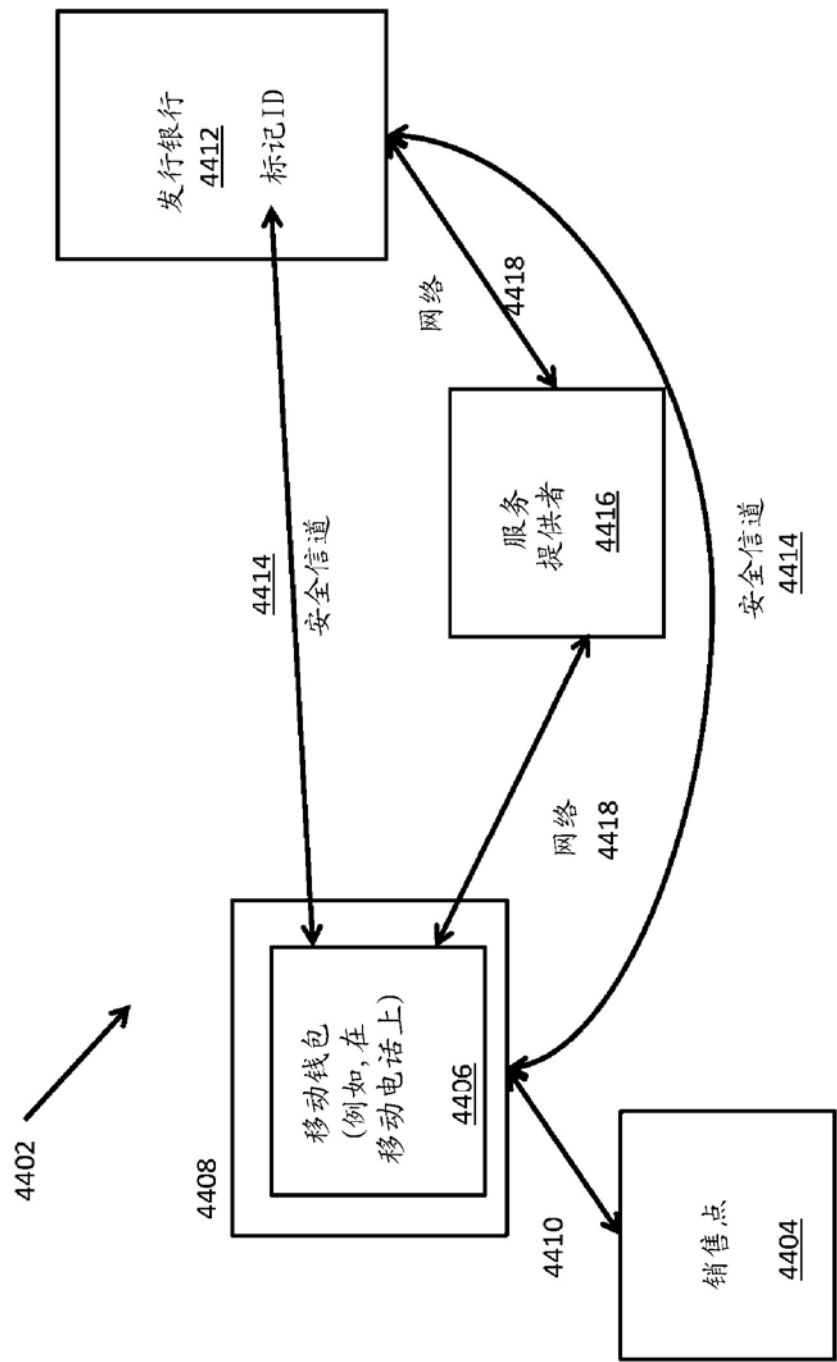


图 44

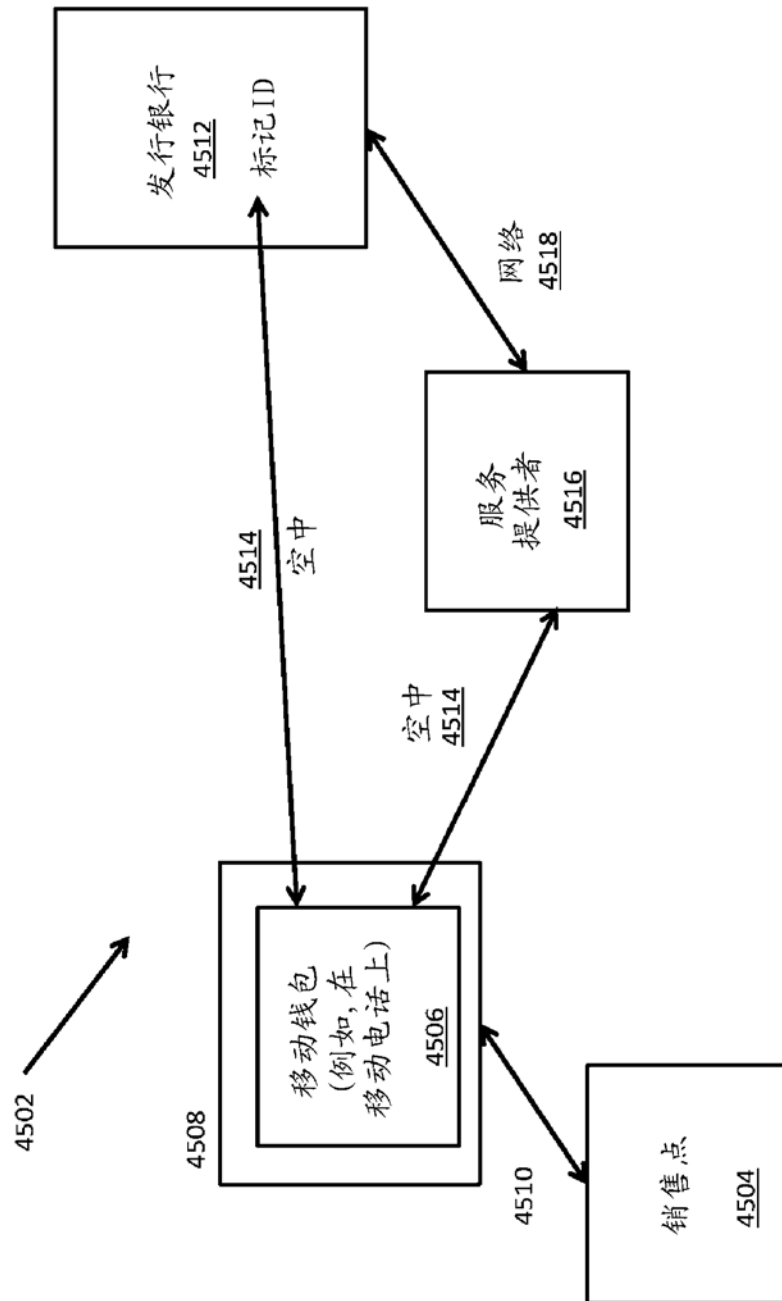


图 45

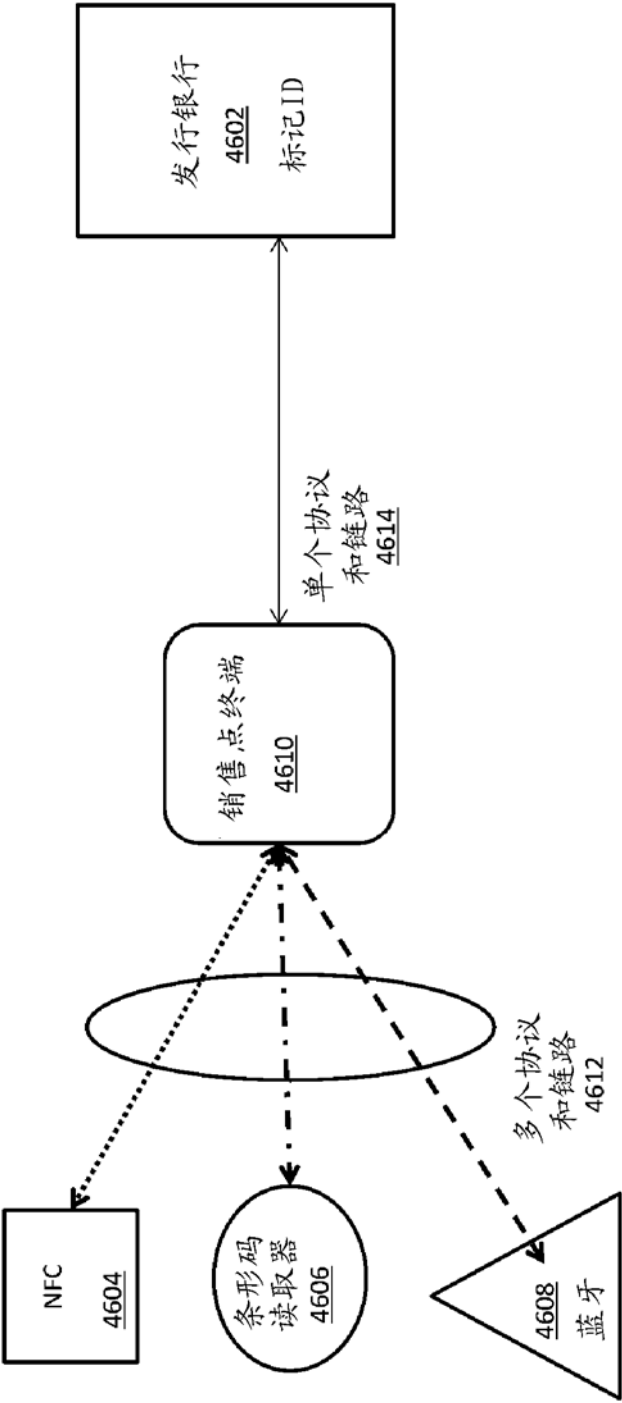


图 46

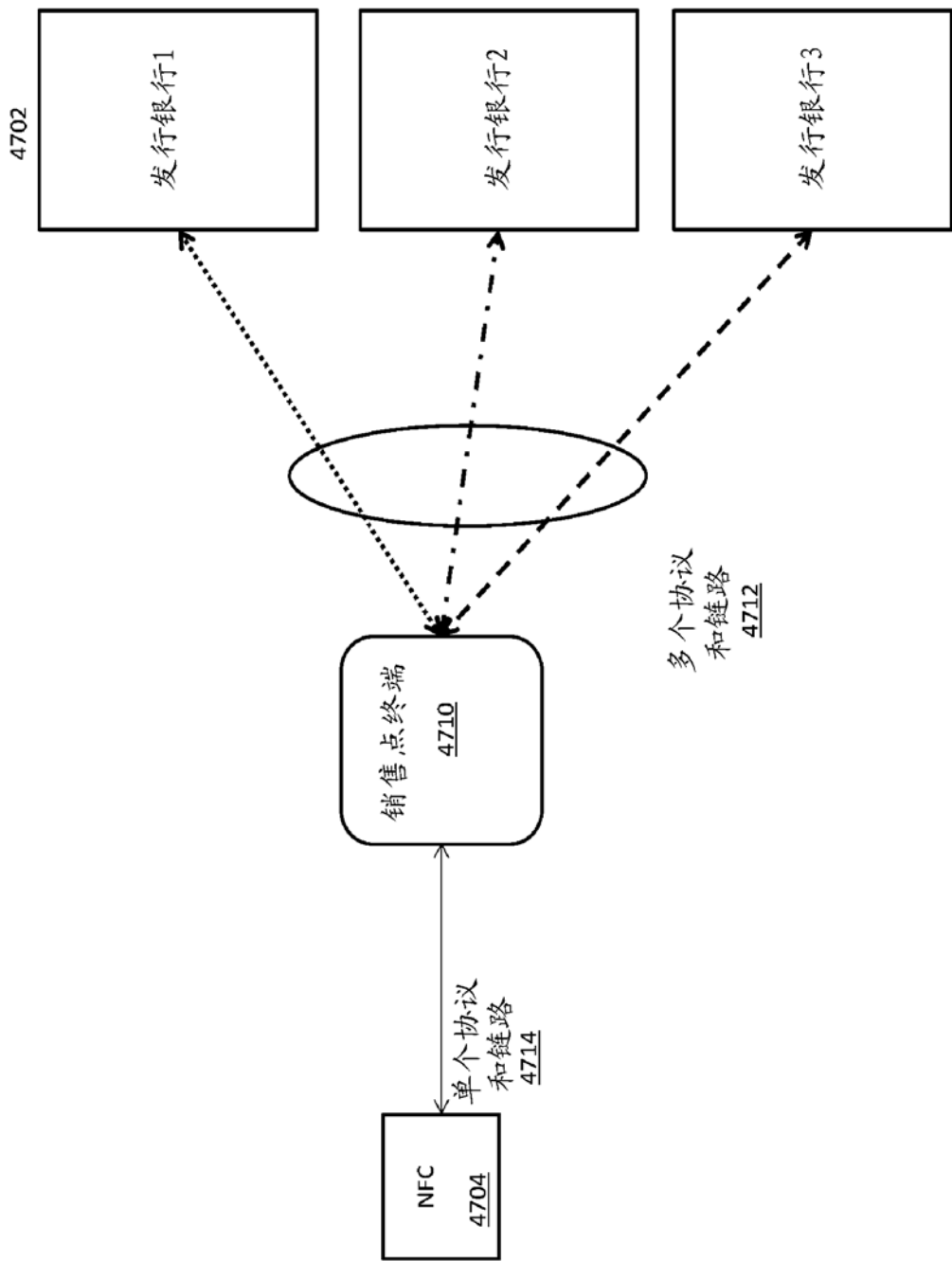


图 47

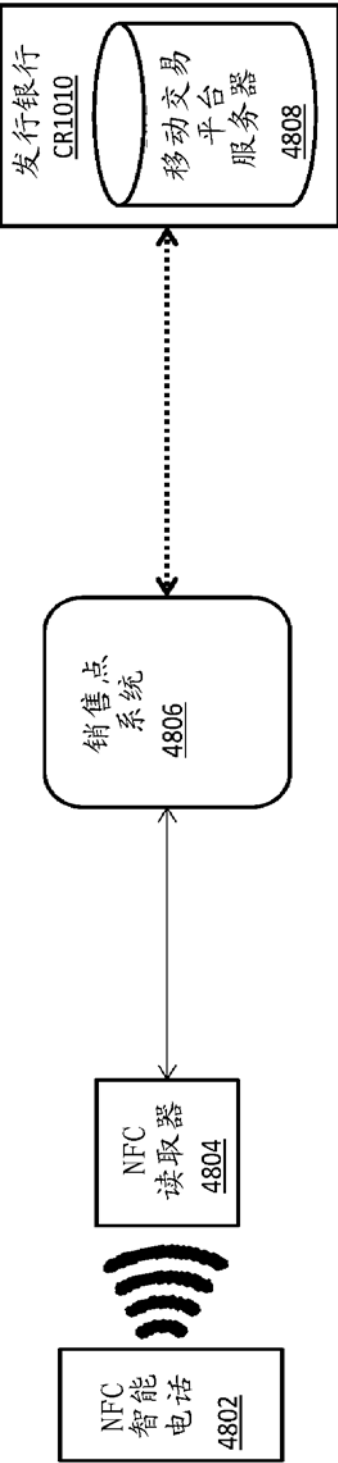


图 48

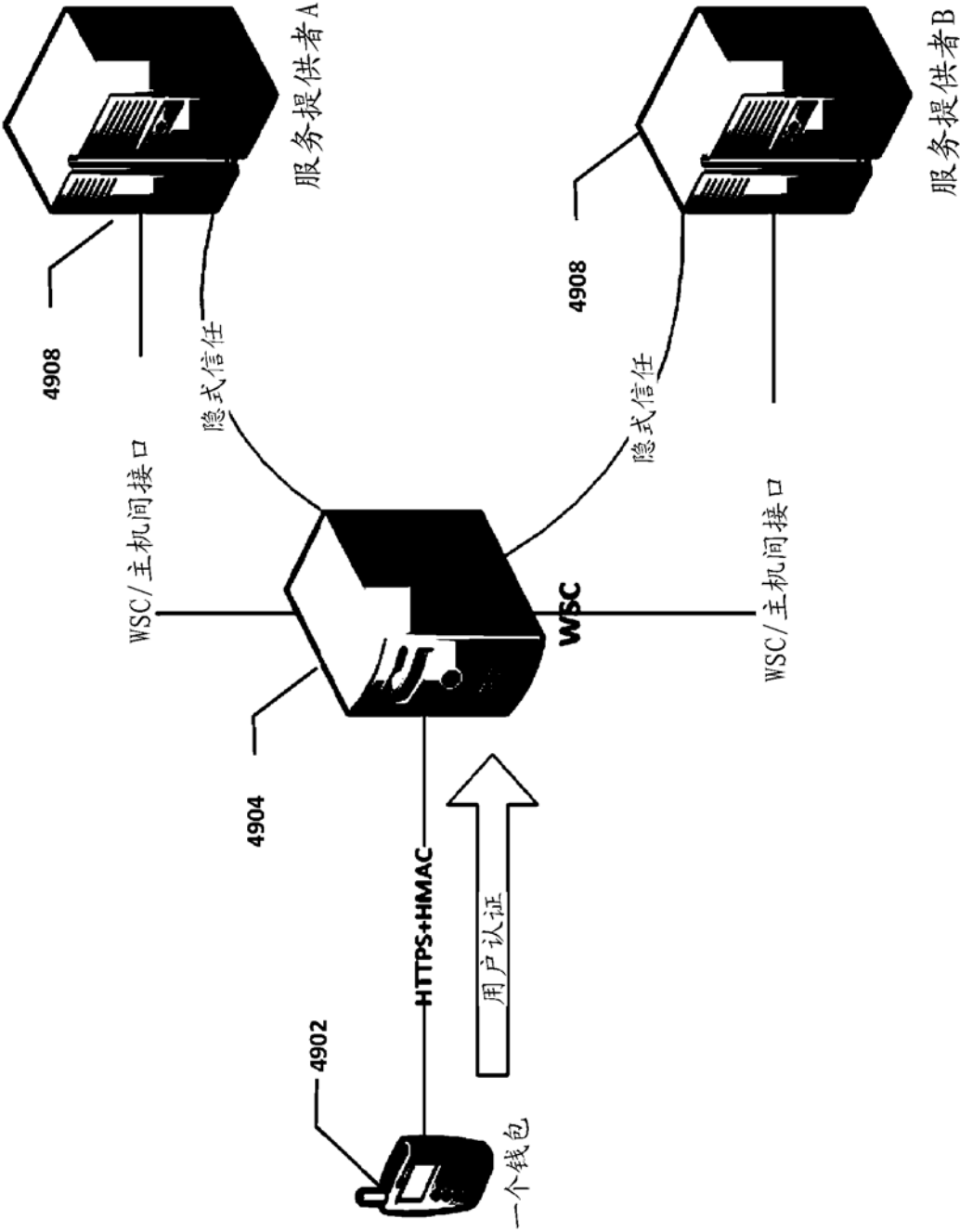


图 49

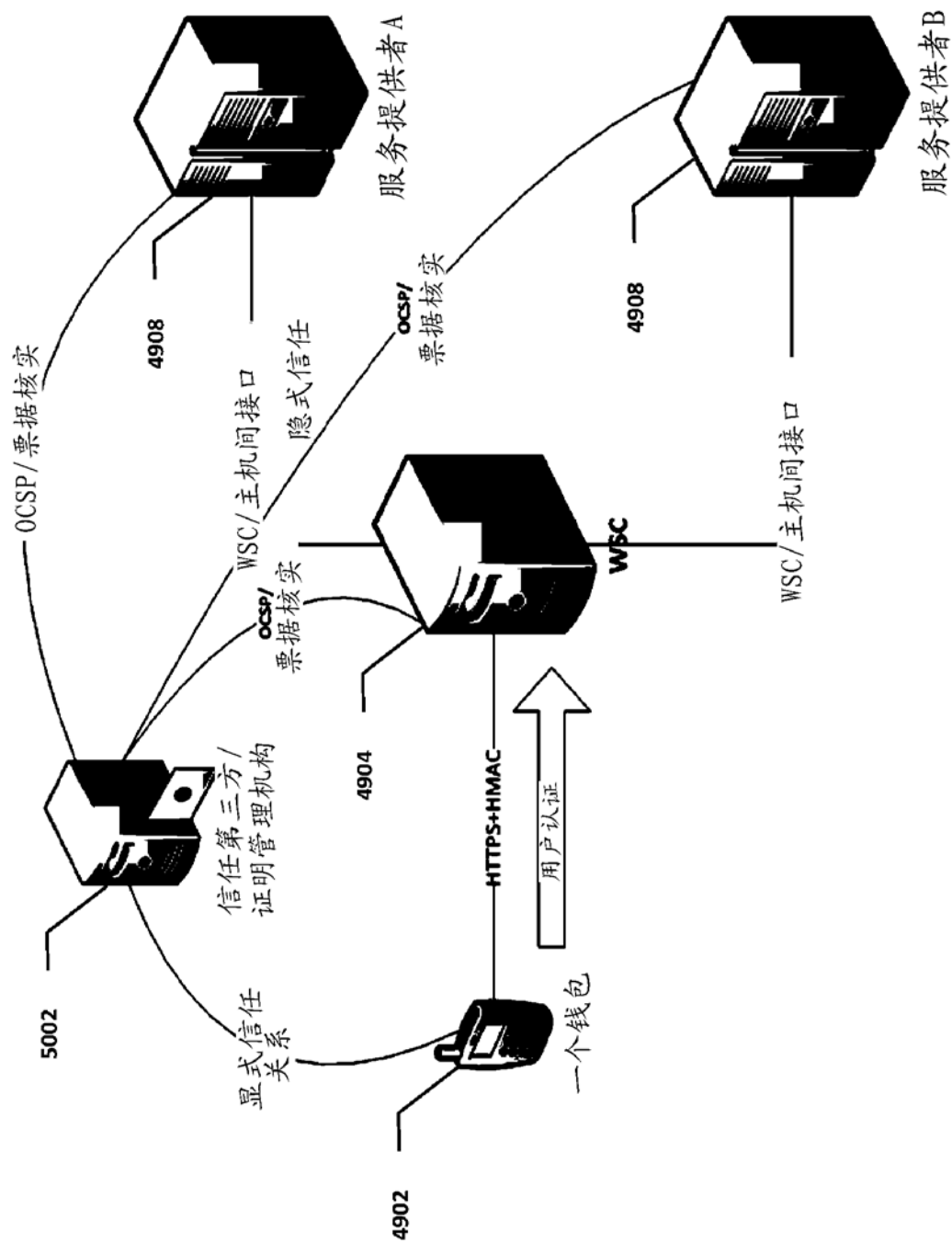


图 50

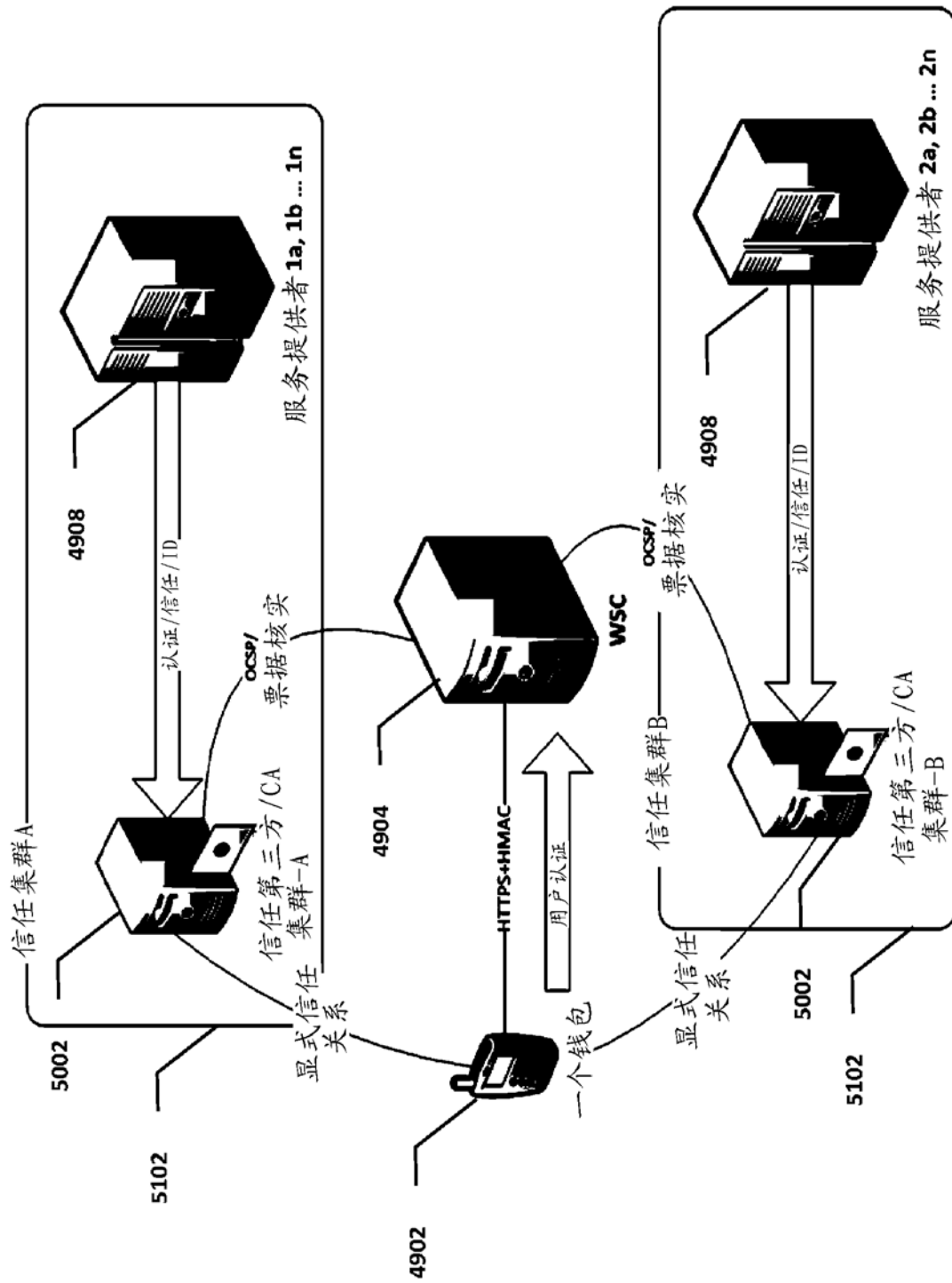


图 51

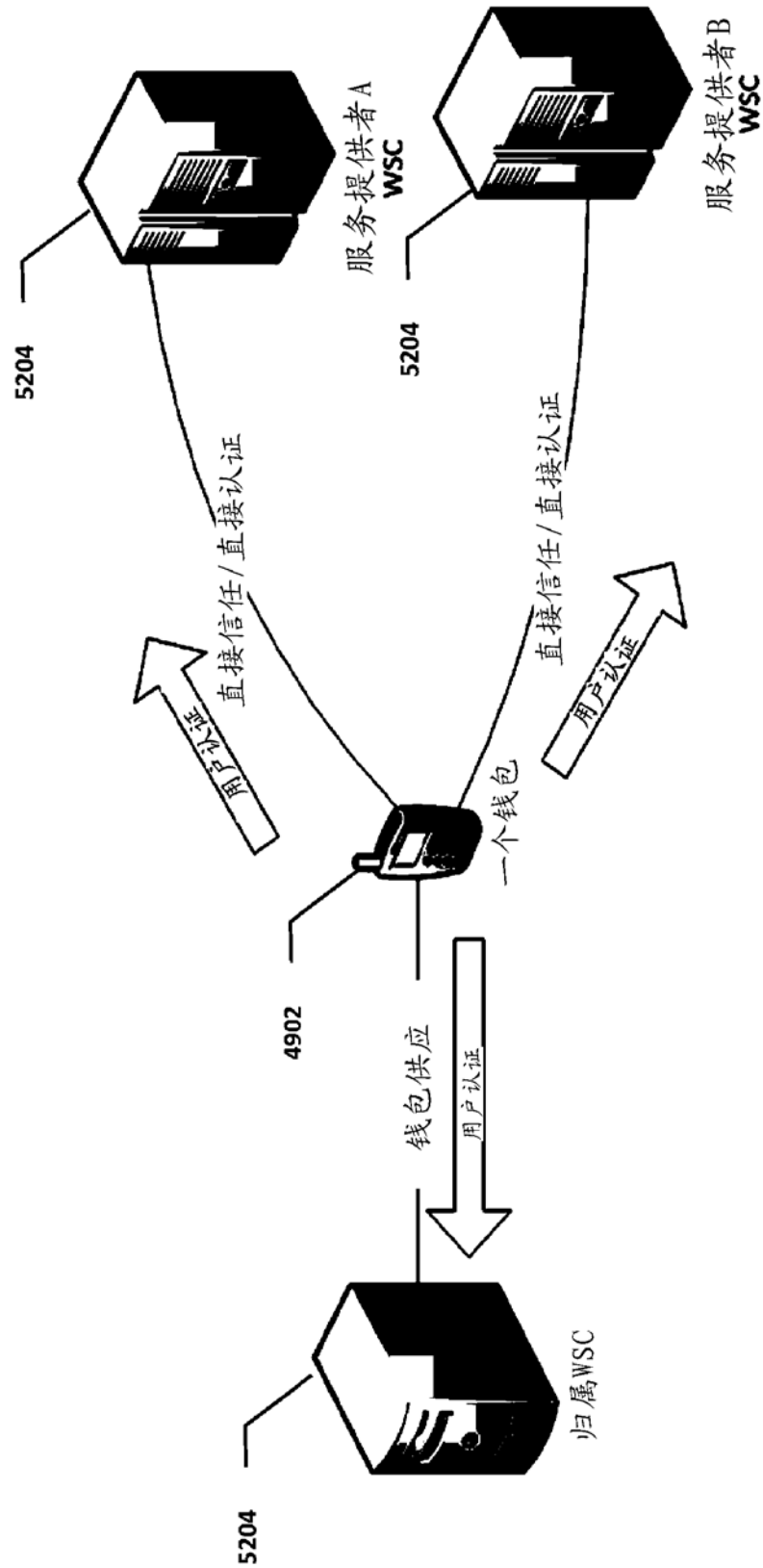


图 52

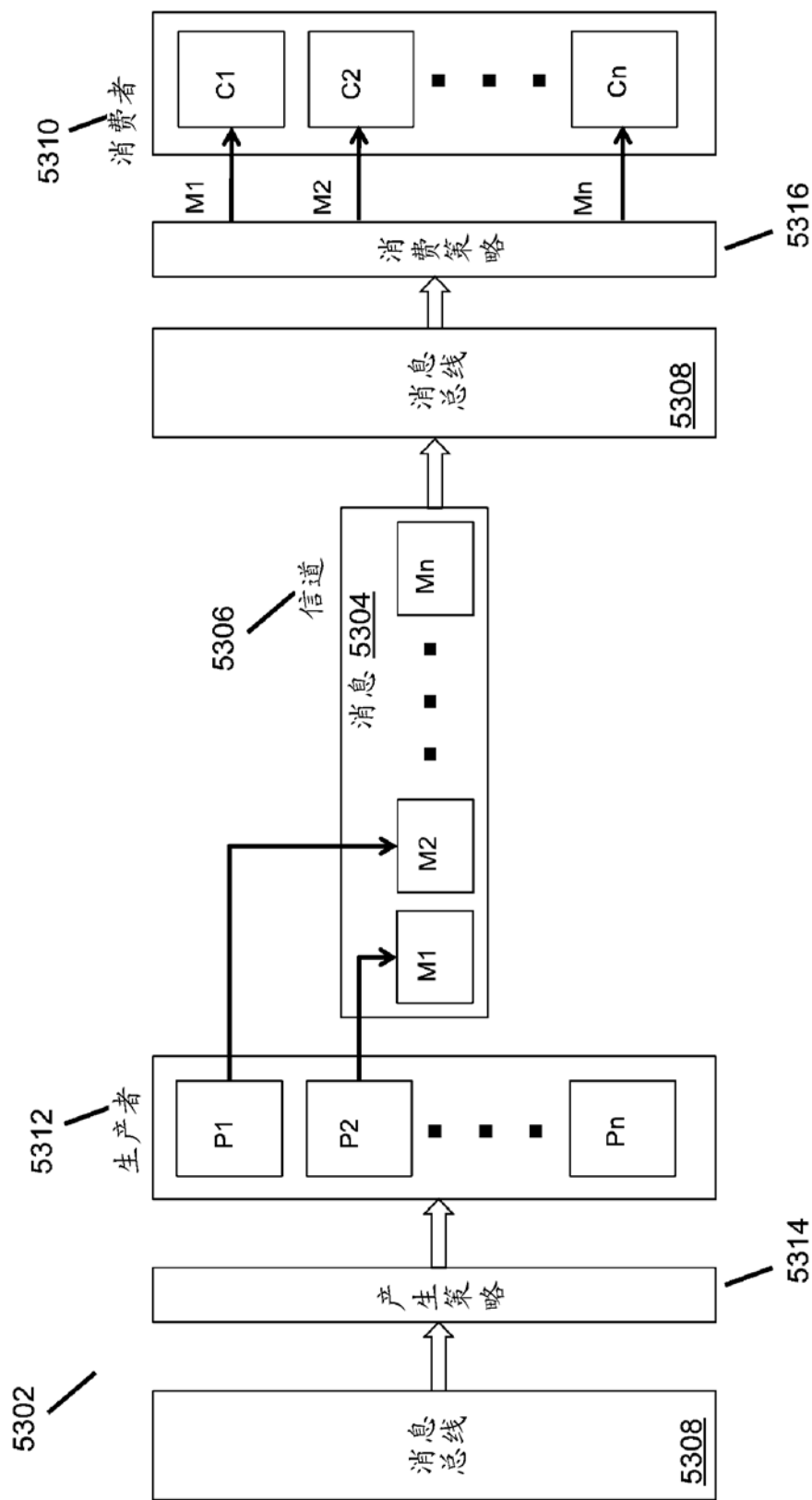


图 53

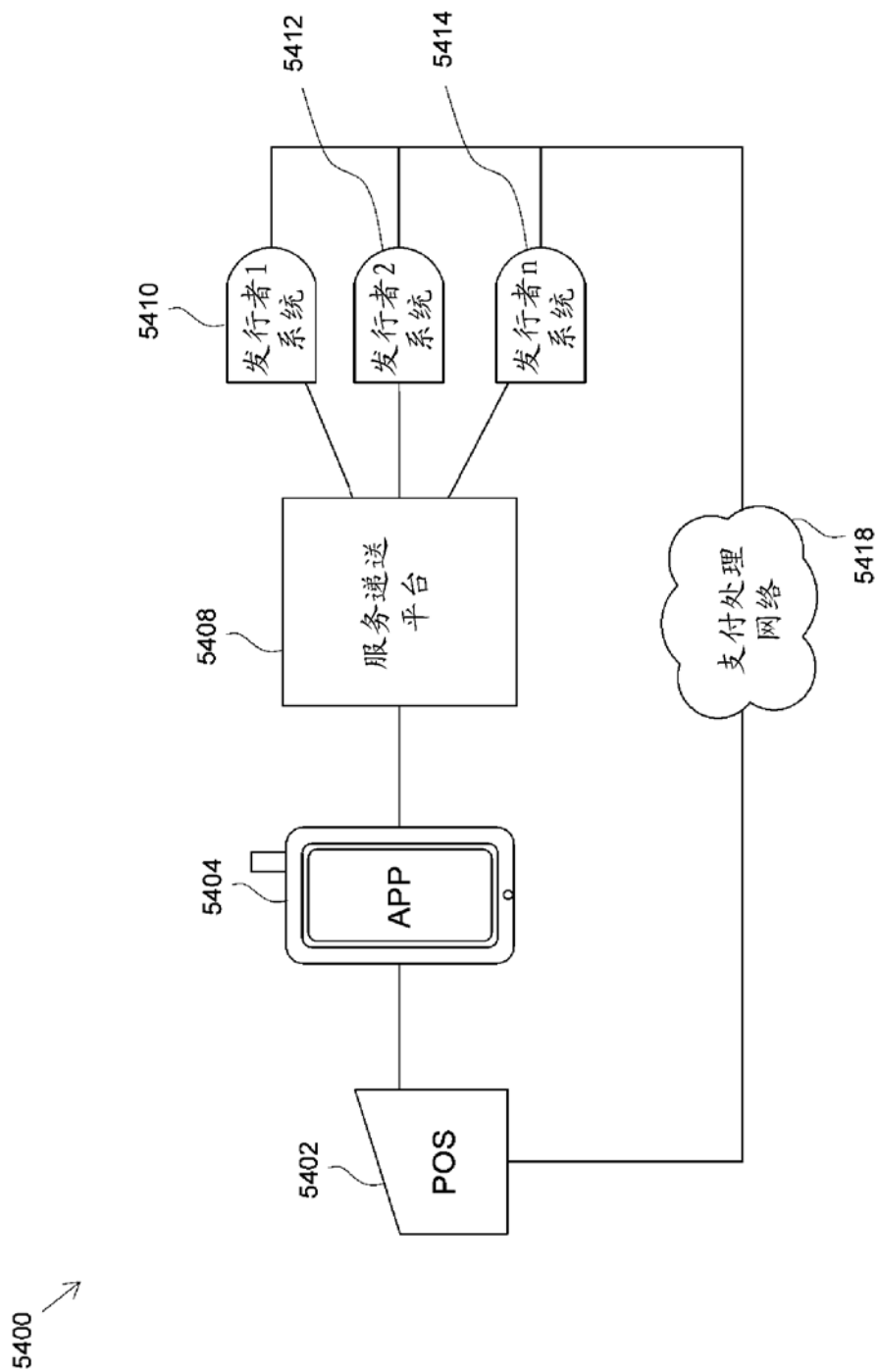


图 54

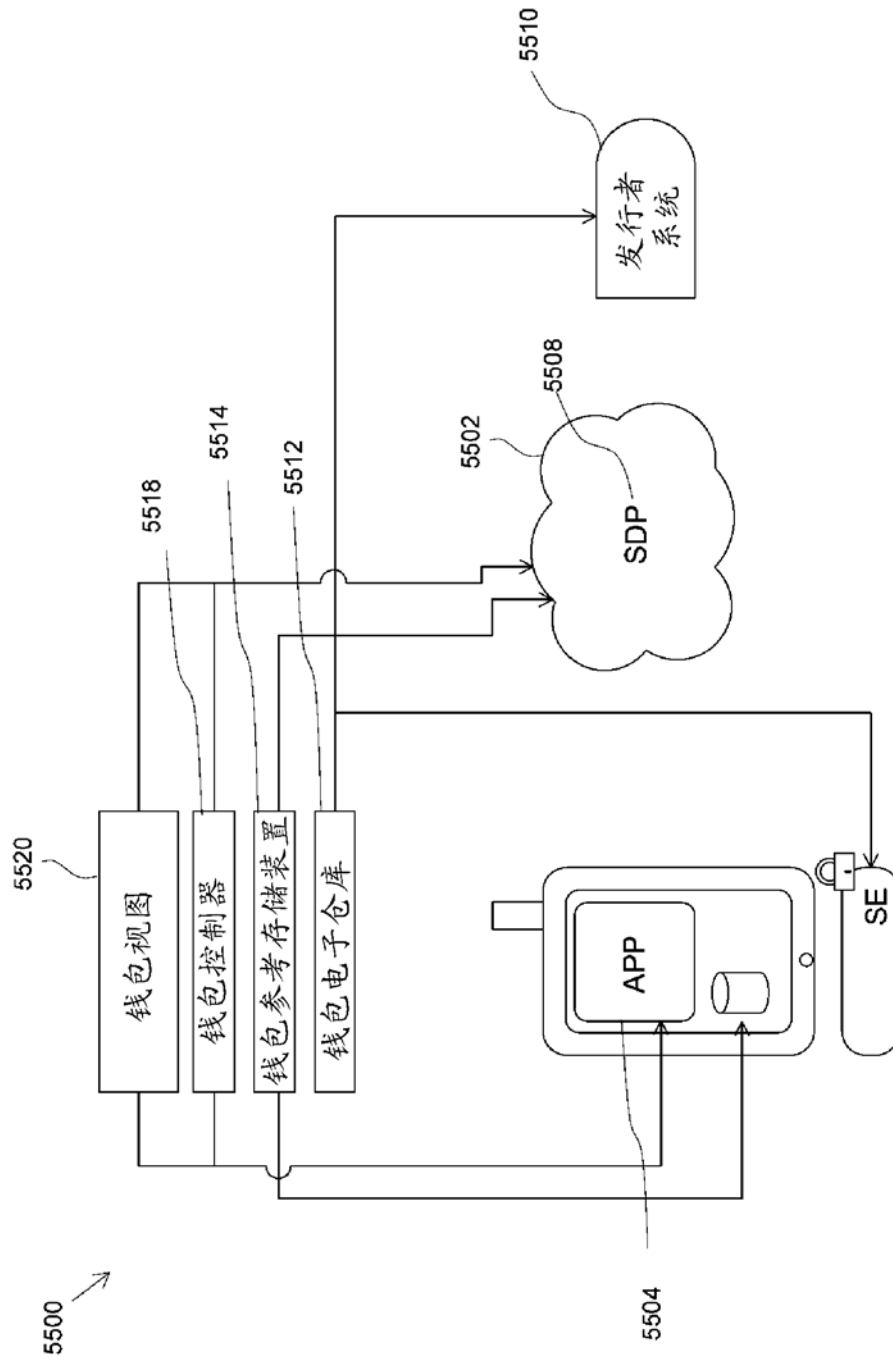


图 55

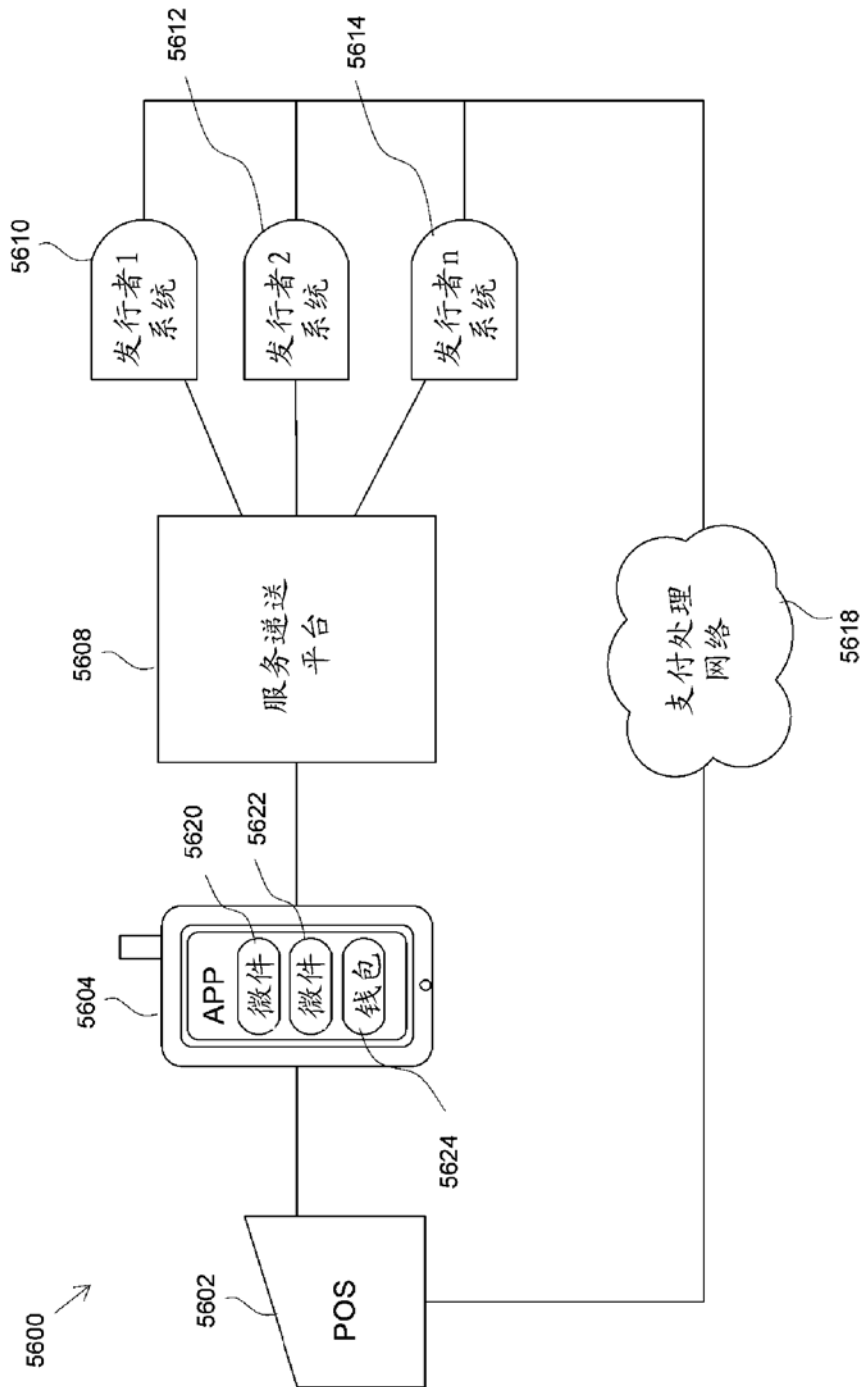


图 56