



(12) 发明专利申请

(10) 申请公布号 CN 105144217 A

(43) 申请公布日 2015. 12. 09

(21) 申请号 201480021600. 4

(22) 申请日 2014. 03. 06

(30) 优先权数据

13/832, 931 2013. 03. 15 US

(85) PCT国际申请进入国家阶段日

2015. 10. 15

(86) PCT国际申请的申请数据

PCT/US2014/021107 2014. 03. 06

(87) PCT国际申请的公布数据

W02014/149828 EN 2014. 09. 25

(71) 申请人 万事达卡国际股份有限公司

地址 美国纽约

(72) 发明人 特丽萨·史密斯

戴维·安东尼·罗伯茨

戴维·约翰·希尔维斯特

(74) 专利代理机构 北京聿宏知识产权代理有限公司 11372

代理人 吴大建 刘华联

(51) Int. Cl.

G06Q 20/40(2006. 01)

G06Q 20/32(2006. 01)

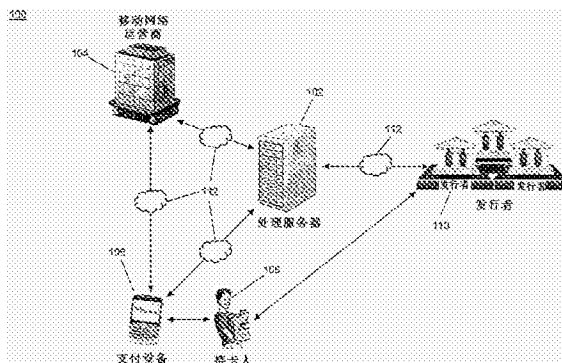
权利要求书2页 说明书8页 附图5页

(54) 发明名称

用于利用单个支付设备来使用多个支付帐户的系统及方法

(57) 摘要

一种用于传输供支付设备使用的多个支付账户的方法及系统。该方法包括：分配加密个人账户 (CPAN)，并产生与此 CPAN 相关的至少一个加密主密钥集；以及由传输设备传输至少一个所产生的加密主密钥集，以存储在支付设备中。另外，该方法还包括由接收设备接收至少一个设备自身账号 (DPAN)，其中至少一个 DPAN 中的每个 DPAN 与关联有消费者的支付账号相关联；由处理设备生成针对至少一个 DPAN 中的每个 DPAN 的个性化脚本，其中个性化脚本包括与相对应的 DPAN 相关联的数据集；以及由传输设备向支付设备传输至少一个个性化脚本。支付设备配置为将 CPAN 用于所选的加密运算，并将 DPAN 和相关联的数据集用于金融交易的其他方面。



1. 一种用于传输供支付设备使用的多个支付账户的方法,包括:
 - 分配加密个人账号 CPAN,并产生与此 CPAN 相关的至少一个加密主密钥集;
 - 由传输设备传输至少一个所产生的加密主密钥集,以存储在支付设备中;
 - 由接收设备接收至少一个设备自身账号 DPAN,其中至少一个 DPAN 中的每个 DPAN 与关联有消费者的支付账号相关联;
 - 由处理设备生成针对所述至少一个 DPAN 中的每个 DPAN 的个性化脚本,其中所述个性化脚本包括与相对应的 DPAN 相关联的数据集;以及
 - 由所述传输设备向所述支付设备传输至少一个个性化脚本,
 - 其中所述支付设备配置为:
 - 将所述 CPAN 用于所选的加密运算,以及
 - 将所述 DPAN 和相关联的数据集用于金融交易的其他方面。
2. 根据权利要求 1 所述的方法,其中所述个性化脚本配置为使所述支付设备将安全存储器中的现有的 DPAN 和相关联的数据集替换为包含在所述个性化脚本中的 DPAN 和相关联的数据集。
3. 根据权利要求 2 所述的方法,其中所述支付设备还配置为存储针对多个用途的个性化脚本。
4. 根据权利要求 2 所述的方法,其中所述支付设备配置为将所述个性化脚本存储在除所述安全存储器以外的存储器中。
5. 根据权利要求 4 所述的方法,其中所述支付设备配置为在由所述支付设备执行所述个性化脚本之前向所述安全存储器传输所述个性化脚本。
6. 根据权利要求 5 所述的方法,其中响应由用户接收到的指令而将所述个性化脚本传输至所述安全存储器。
7. 根据权利要求 6 所述的方法,其中所述用户是与关联有包含在所述个性化脚本中的 DPAN 的支付帐户相关联的消费者。
8. 根据权利要求 1 所述的方法,其中所述个性化脚本受保护而不被修改,并且任何这样的修改均可由所述支付设备检测到。
9. 根据权利要求 1 所述的方法,其中通过以仅所述支付设备能解密然后使用所述脚本的方式来对所述脚本进行解密,从而保护所述个性化脚本而不会使得其内容被无意公开。
10. 根据权利要求 1 所述的方法,其中所述支付设备配置为在接收并存储所述加密主密钥集的同时存储所述 CPAN。
11. 根据权利要求 10 所述的方法,其中所述支付设备还配置为提供作为所述金融交易的一部分的附加数据的 CPAN。
12. 根据权利要求 1 所述的方法,其中所述至少一个加密主密钥集在向所述消费者提供所述支付设备之前被传输,以便存储在所述支付设备中。
13. 根据权利要求 1 所述的方法,其中所述支付设备与所述消费者相关联。
14. 根据权利要求 1 所述的方法,其中每个个性化脚本配置为由存储在所述支付设备中且由其执行的软件应用所执行。
15. 根据权利要求 14 所述的方法,还包括:向所述支付设备传输所述软件应用。
16. 一种用于传输供支付设备使用的多个支付账户的系统,包括:

处理设备,用于分配加密个人账号 CPAN,并产生与此 CPAN 相关的至少一个加密主密钥集;

传输设备,配置为传输至少一个所产生的加密主密钥集,以存储在支付设备中;

接收设备,配置为接收至少一个设备自身账号 DPAN,其中至少一个 DPAN 中的每个 DPAN 与关联有消费者的支付账号相关联;以及

处理设备,配置为生成针对所述至少一个 DPAN 中的每个 DPAN 的个性化脚本,其中所述个性化脚本包括与相对应的 DPAN 相关联的数据集,其中

所述传输设备还配置为向所述支付设备传输至少一个个性化脚本,并且

所述支付设备配置为:

将所述 CPAN 用于所选的加密运算,以及

将所述 DPAN 和相关联的数据集用于金融交易的所有其他的方面。

17. 根据权利要求 16 所述的系统,其中所述个性化脚本配置为使所述支付设备将安全存储器中的现有的 DPAN 和相关联的数据集替换为包含在所述个性化脚本中的 DPAN 和相关联的数据集。

18. 根据权利要求 17 所述的系统,其中所述支付设备还配置为存储针对多个用途的个性化脚本。

19. 根据权利要求 17 所述的系统,其中所述支付设备配置为将所述个性化脚本存储在除所述安全存储器以外的存储器中。

20. 根据权利要求 19 所述的系统,其中所述支付设备配置为在由所述支付设备执行所述个性化脚本之前向所述安全存储器传输所述个性化脚本。

21. 根据权利要求 20 所述的系统,其中响应由用户接收到的指令而将所述个性化脚本传输至所述安全存储器。

22. 根据权利要求 21 所述的系统,其中所述用户是与关联有包含在所述个性化脚本中的 DPAN 的支付帐户相关联的消费者。

23. 根据权利要求 16 所述的系统,其中所述个性化脚本受保护以免被修改,并且任何这样的修改可由所述支付设备检测到。

24. 根据权利要求 23 所述的系统,其中通过以仅所述支付设备能解密然后使用所述脚本的方式来对所述脚本进行解密,从而保护所述个性化脚本而不会使得其内容被无意公开。

25. 根据权利要求 16 所述的系统,其中所述支付设备配置为在接收并存储所述加密主密钥集的同时存储所述 CPAN。

26. 根据权利要求 24 所述的系统,其中所述支付设备还配置为提供作为所述金融交易的一部分的附加数据的 CPAN。

27. 根据权利要求 16 所述的系统,其中所述至少一个加密主密钥集在向所述消费者提供所述支付设备之前被传输,以便存储在所述支付设备中。

28. 根据权利要求 16 所述的系统,其中所述支付设备与所述消费者相关联。

29. 根据权利要求 16 所述的系统,其中每个所述个性化脚本配置为由存储在所述支付设备中且由该支付设备执行的软件应用所执行。

30. 根据权利要求 16 所述的系统,还包括向所述支付设备传输所述软件应用。

用于利用单个支付设备来使用多个支付帐户的系统及方法

发明领域

[0001] 本公开涉及经由单个支付设备来使用针对金融交易的多个支付帐户,具体地,涉及生成并向支付设备传输个性化脚本 (repersonalization scripts),从而通过个性化该设备来使用相关联的支付帐户。

背景技术

[0002] 为了进行金融交易,消费者通常利用基于物理的支付方法,例如现金、支票和信用卡。随着技术的发展,诸如电视、台式电脑、笔记本电脑、移动电话、智能电话、平板电脑等运算设备已发展成了用于发起或进行金融交易的支付设备。例如,许多电脑、智能电话和电视已配置为通过用户能提供随后将传输至商家的支付信息的方式经由互联网进行金融交易。

[0003] 为了最小化用户需要提供的支付信息量并增加支付帐户的安全性,各种类型的安全存储器(例如嵌入式安全组件)已被设计成包含在支付设备内,以存储支付证书。然而,在许多情况下,将这些安全组件设置成不能访问的,以维持安全性。因此,不能随意更换支付证书。因而使得用户不能利用单个支付设备来进行使用多个支付帐户的交易。

[0004] 因此需要一种使支付设备能够利用多个支付帐户来进行金融交易的技术方案。

发明内容

[0005] 本公开提供了用于传输针对供支付设备使用的多个支付帐户的细节的系统及方法的描述。

[0006] 一种用于传输供支付设备使用的多个支付账户的方法,包括:分配加密个人账号(CPAN),并产生与此CPAN相关的至少一个加密主密钥集,由传输设备传输至少一个此加密主密钥集,以存储在支付设备中;由接收设备接收至少一个设备自身账号(DPAN),其中至少一个DPAN中的每个DPAN与关联有消费者的支付账号相关联;由处理设备生成针对所述至少一个DPAN中的每个DPAN的个性化脚本,其中所述个性化脚本包括与相应的DPAN相关联的数据集;以及由所述传输设备向所述支付设备传输至少一个个性化脚本,其中所述支付设备配置为仅将与所述CPAN相关的密钥集用于所选的加密运算(因此由CPAN发行者来处理这些数据项),并将所述DPAN和相关联的数据集用于金融交易的所有其他的方面。

[0007] 一种用于传输供支付设备使用的多个支付账户的系统,包括传输设备、接收设备和处理设备。所述处理设备配置为用以分配加密个人账号(CPAN),并产生与此CPAN相关的至少一个加密主密钥集。所述传输设备配置为用以传输至少一个此加密主密钥集,以存储在支付设备中。所述接收设备接收至少一个设备自身账号(DPAN),其中至少一个DPAN中的每个DPAN与关联有消费者的支付账号相关联。所述处理设备还配置为用以生成针对所述至少一个DPAN中的每个DPAN的个性化脚本,其中所述个性化脚本包括与相应的DPAN相关联的数据集。所述传输设备还配置为向所述支付设备传输至少一个个性化脚本。所述支付设备配置为将所述CPAN用于所选的加密运算(因此由CPAN发行者来处理这些数据项),并

将所述 DPAN 和相关联的数据集用于金融交易的所有其他的方面。

附图说明

[0008] 通过结合附图阅读下文示例性实施例的详细描述可更好地理解本公开的范围。其中所包括的附图是：

[0009] 图 1 是示出了根据示例性实施例的用于向支付设备传输个性化脚本，以能够经由多个支付帐户进行交易的系统的高层体系架构。

[0010] 图 2 是示出了根据示例性实施例的图 1 的用于创建并传输个性化脚本和相关联的数据的处理服务器的框图。

[0011] 图 3 是示出了根据示例性实施例的用于生成个性化脚本并将其传输至支付设备的方法的流程框图。

[0012] 图 4 是示出了根据示例性实施例的用于传输供支付设备使用的多个支付帐户的示例性方法的流程图。

[0013] 图 5 是示出了根据示例性实施例的计算机系统架构的方框图。

[0014] 从下文提供的详细描述中，将显而易见本公开的其他应用领域。但是，应当理解，示例性实施例的详细描述仅用于说明性目的，因此，并非旨在必须限制本公开的范围。

具体实施方式

[0015] 术语定义

[0016] 支付网络——一种用于通过使用现金替代物来进行转帐的系统或网络。支付网络可利用多种不同的协议和程序来处理针对多种交易类型的转帐。通过支付网络进行的交易可包括购买产品或服务、赊购、借方交易、资金划拨、账户取款等。支付网络可配置为通过可包括支付卡、信用证、支票、金融帐户等的现金替代物来进行交易。配置为用作支付网络的网络或系统的示例包括由 MasterCard®、VISA®、Discover®、American Express®运作的网络或系统。

[0017] 支付帐户——一种可用于出资进行交易的金融帐户，例如支票帐户、储蓄账户、信用帐户、虚拟支付帐户等。支付帐户可关联有可包括个人、家庭、公司、企业、非政府机构等的实体。在一些情况下，支付帐户可以是虚拟的，例如那些由 PayPal®等运作的帐户。

[0018] 支付卡——一种与可提供给商家以经由关联的支付帐户出资进行金融交易的支付帐户相关联的卡或数据。支付卡可包括信用卡、借记卡、记帐卡、储值卡、预付卡、燃油特惠卡、虚拟支付号、虚拟卡号、受控的支付号等。支付卡可以是可向商家提供的物理卡或者代表相关联的支付帐户的数据（例如存储在诸如智能电话或计算机的通信设备中）。例如，在一些情况下，可将包括支付账号的数据认为是用于处理由相关联的支付帐户出资进行交易的支付卡。在一些情况下，如果适用，可将支票认为是支付卡。

[0019] 用于结合支付设备来处理金融交易的系统

[0020] 图 1 示出了用于向支付设备传输个性化脚本来实现经由多个支付帐户的交易的系统 100。

[0021] 系统 100 可包括处理服务器 102。处理服务器 102（这将在下文进行更详细的讨论）可存储多个主加密个人账号（CPNAs, cryptographic personal account numbers）。每

个 CPAN 可以是与单个支付设备（例如支付设备 106）相关联的唯一值。处理服务器 102 可生成与每个 CPAN 相对应的加密主密钥集。CPAN 和相应的加密主密钥集可存储在密钥数据库中，该密钥数据库可作为处理服务器 102 的一部分进行存储，或者存储在处理服务器 102 的外部。

[0022] 处理服务器 102 可向支付设备 106 传输至少一个所生成的加密主密钥集，以使其存储在该支付设备 106 中。可经由网络 112（例如移动通信网络）来传输加密主密钥集。在一些实施例中，在向终端用户提供支付设备 106 之前，可将至少一个所生成的加密主密钥集传输至移动网络运营商 104，移动网络运营商 104 可将加密主密钥集存储在支付设备 106 的安全存储器中，以作为制造和 / 或分发支付设备 106 的一部分。相关领域技术人员将显而易见适于存储加密主密钥集的安全存储器的类型，其可包括嵌入式芯片、安全组件等。

[0023] 可将支付设备 106 提供给持卡人 108（例如由移动网络运营商 104）。持卡人 108 可以是与由一个或多个发行者 110（例如发行银行）操控的一个或多个支付帐户相关联的消费者。用于操控与持卡人 108 相关联的支付帐户的发行者 110 可经由网络 112 向处理服务器 102 传输与支付帐户相关联的设备自身账号（DPAN, device personal account number）。处理服务器可接收可能存在数据库中的 DPAN。

[0024] 然后，处理服务器 102 可针对从发行者 110 处接收的 DPAN 中的每个 DPAN 来生成个性化脚本，每个个性化脚本包括 DPAN 和与 DPAN 相关联的数据集，诸如银行号、截止日期、安全码、认证或相关领域技术人员将显而易见的其他任何用于出资进行金融交易和 / 或处理金融交易的合适数据。在一些实施例中，相关联的数据集可包括基于与 DPAN 相关联的支付帐户的帐户类型（例如支付卡、支票帐户、虚拟帐户等）的数据。

[0025] 处理服务器 102 可向支付设备 106 传输至少一个所生成的个性化脚本。然后，持卡人 108 可使用支付设备 106 在商家处进行交易。支付设备 106 可包括配置为执行个性化脚本的软件应用。执行个性化脚本可使得支付设备用存储在安全存储器中的数据来交换存储在个性化脚本中的任何带有 DPAN 的现有支付帐户和相关联的数据集。然后，支付设备 106 可配置为经由相关联的支付帐户来进行交易。

[0026] 支付设备 106 可配置为使用本领域技术人员将显而易见的系统和方法来向商家传输支付细节及其他数据（例如经由销售终端）。相关领域技术人员还将显而易见可包含在支付细节中的数据。支付设备 106 可配置为使用与 CPAN 相关联的加密主密钥集来执行所选的与通常在支付设备 106 和发行者 110 之间交换的数据项相关的加密运算（因此必须由 CPAN 发行者来处理这些数据项），并使用 DPAN 和相关联的数据集来执行金融交易的其他方面。

[0027] 处理设备

[0028] 图 2 示出了系统 100 的处理服务器 102 的实施例。对于相关领域技术人员而言，明显知道图 2 中所示的处理服务器 102 的实施例仅是示意性的，其对于适于执行此处所公开的功能的处理服务器 102 的所有可能的配置来说并非是详尽的。例如，图 5 中所示的计算机系统 500（这将在下文中进行更详细的讨论）可以是处理服务器 102 的合适配置。

[0029] 处理服务器 102 可包括传输单元 202。传输单元 202 可配置为向支付设备 106 和 / 或移动网络运营商 104 传输与 CPAN 相对应的至少一个加密主密钥集 212。在一些实施例中，与 CPAN 相对应的加密主密钥集 212 可由处理单元 206 生成和 / 或识别。处理单元 206

可将所识别的 / 所生成的加密主密钥集 212 存储在密钥数据库 210 中。在一些情况下, 处理单元 206 可将信息存储在使加密主密钥集 212 与相对应的支付设备 106 相关联的密钥数据库 210 中。适于使加密主密钥集 212 与相对应的支付设备 106 相关联的数据对于相关领域技术人员而言是显而易见的, 其可包括例如与支付设备 106 相关联的电话号码、IMEI 或媒体访问控制 (MAC) 地址。

[0030] 处理服务器 102 还可包括接收单元 204。接收单元 204 可配置为接收来自发行者 110 的 DPAN 214 (例如经由网络 112)。每个所接收的 DPAN 214 可与关联有消费者 (例如与被传输有加密主密钥集的支付设备 106 相关联的持卡人 108) 的支付帐户相关联。在一些实施例中, DPAN 214 可与加密主密钥集 212 相关联, 因此关联有持卡人 108 的每个 DPAN 214 可与向关联有该持卡人 108 的支付设备 106 传输的加密主密钥集 212 相关联。

[0031] 处理单元 206 还可配置为用以生成至少包含 DPAN 214 和与 DPAN 214 相关联的数据集的个性化脚本 218。与 DPAN 214 相关联的数据可由带有 DPAN 214 的发行者 110 提供, 或者单独由处理单元 206 确定和 / 或生成, 或者由接收单元 204 接收。在一些实施例中, 处理单元 206 可将所生成的个性化脚本 218 存储在脚本数据库 216 中。在另一实施例中, 脚本数据库 216 可作为密钥数据库 210 的一部分进行存储。在再一实施例中, 可将个性化脚本与相对应的 DPAN 214 相关联地存储在密钥数据库 210 中。

[0032] 传输单元 202 还可配置为用以向支付设备 106 传输一个或多个所生成的个性化脚本 218。在一些实施例中, 响应由接收单元 204 接收到的针对个性化脚本 218 的接收请求而向支付设备 106 传输个性化脚本 218。例如, 持卡人 108 可请求个性化脚本 218, 以使得支付设备 106 能够与新支付帐户进行金融交易, 例如通过配置为用以执行个性化脚本的软件应用。接收单元 204 可接收请求和从请求发起处向支付设备进行传输的相应的个性化脚本 218。在一些情况下, 可通过一个运算设备 (例如计算机) 和传输至不同支付设备 (例如智能电话) 的相对应的个性化脚本 218 来提交请求。

[0033] 在一个实施例中, 在接收 DPAN 214 之前, 接收单元 204 可接收来自支付设备 106 和 / 或持卡人 108 的针对个性化脚本的请求。在这样的实施例中, 请求可包括用于表示持卡人 108 希望交易的支付帐户的识别信息。然后, 传输单元 202 可向相对应的发行者 110 传输针对 DPAN 214 的请求和关联有支付帐户的相关联的数据集。然后, 发行者 110 可返回随后会被处理单元 206 使用以生成个性化脚本 218 的 DPAN 214 和相关联的数据。

[0034] 在一些实施例中, 处理服务器 102 可包括密钥生成单元 208。密钥生成单元 208 可配置为用以生成与 CPAN 相对应的加密主密钥集 212。相关领域技术人员将显而易见基于账号来生成密钥集的方法。在一些实施例中, 密钥生成单元 208 还可配置为首先生成主 CPAN, 然后生成相对应的加密主密钥集 212。

[0035] 用于生成、传输及执行个性化脚本的方法

[0036] 图 3 是示出了用于生成、传输和执行个性化脚本的高层方法的流程框图。在步骤 301 中, 处理服务器 102 可向支付设备 106 提供加密主密钥集 212。在一些情况下, 可向移动网络运营商 104 提供加密主密钥集 212, 移动网络运营商 104 可在分发支付设备 106 之前就将加密主密钥集 212 存储在支付设备 106 的安全存储器中。在一些实施例中, 还可将与加密主密钥集 212 相对应的 CPAN 传输至支付设备 106。在另一实施例中, 也可将 CPAN 存储在支付设备 106 的安全存储器中。

[0037] 在步骤 301a 中,可将软件应用和相对应的数据下载到支付设备 106 上。软件应用可以是配置为由支付设备 106 执行的软件程序(例如钱包程序),并可被配置为执行个性化脚本和传输支付信息。适于执行此处所公开的功能的软件应用的类型,以及用于将软件应用下载并安装到支付设备 106 上的方法,对于相关领域技术人员而言是显而易见的。更显而易见的是,在一些情况下,可将软件应用预先包含在支付设备 106 中,例如由移动网络运营商 104 将软件应用安装在支付设备 106 中。

[0038] 在步骤 302 中,发行者 110 可向处理服务器 102 提供一个或多个 DPAN 214,其中每个 DPAN 与关联有持卡人 108 的支付帐户相关联。在示例性实施例中,持卡人 108 可与支付设备 106 相关联。在步骤 303 中,持卡人 108 可请求激活支付帐户。在一些情况下,可经由支付设备 106 向处理服务器 102 提交请求。在其他情况下,可经由单独的运算设备向处理服务器 102 提交请求。在此种情况下,请求可识别个性化脚本所要传向的支付设备 106,或者可识别使处理服务器 102 能够识别与持卡人 108 相关联的支付设备 106 的持卡人 108。相关领域技术人员将显而易见步骤 303 可在步骤 302 之前执行,或者步骤 303 可以是可选步骤(例如,因此个性化脚本是自动生成的,并且在未被持卡人 108 请求的情况下传输至支付设备 106)。

[0039] 在步骤 304 中,处理服务器 102 可生成包括 DPAN214 和关联有体现在所接收的来自持卡人 108 的请求中的支付帐户的相关联的数据集的个性化脚本 218。然后,在步骤 305 中,处理服务器 102 可向支付设备 106 传输所生成的个性化脚本 218。在步骤 306 中,支付设备 106 可执行个性化脚本 218(例如经由软件应用)。执行个性化脚本 218 可使得支付设备 106 用安全存储器(例如安全组件)中的现有的 DPAN 和相关联的数据集来交换存储在个性化脚本 218 中的 DPAN 和相关联的数据集。

[0040] 然后支付设备 106 可配置为进行由与 DPAN 相关联的支付帐户出资的金融交易。在一些情况下,支付设备 106 可将个性化脚本 218 存储在支付设备 106 的安全存储器中,因此该个性化脚本 218 可不被访问或修改。在此情况下,可多次使用个性化脚本 218,从而持卡人 108 可来回地在多个支付帐户之间进行切换。用于经由网络(例如网络 112)接收个性化脚本 218,以及将脚本存储在支付设备 106 内的安全存储器中的方法,对于相关领域技术人员来说是显而易见的。在另一种情况下,可将个性化脚本 218 存储在非安全的存储器中(例如在支付设备 106 的非安全的内存中),但是以一种一经修改即不能使用的方式进行保护,这样能多次使用个性化脚本 218,从而持卡人 108 可来回地在多个帐户之间进行切换。相关领域技术人员将显而易见用于使脚本免受此种修改的方法。

[0041] 用于向支付设备传输多个支付帐户的示例性方法

[0042] 图 4 示出了用于经由个性化脚本来传输供支付设备使用的多个支付帐户的示例性方法 400。

[0043] 在步骤 402 中,可由传输设备(例如传输单元 202)传输至少一个加密主密钥集(例如加密主密钥集 212),以使其存储在支付设备(例如支付设备 106)中,其中至少一个加密主密钥集 212 与主加密个人账号(CPAN)相对应。在一个实施例中,支付设备 106 可配置为一旦收到并存储加密主密钥集 212 就将 CPAN 存储起来。在一些实施例中,在向消费者提供支付设备 106 之前,可传输加密主密钥集 212,以使其存储在支付设备中。

[0044] 在步骤 404 中,由接收设备(例如接收单元 204)可接收至少一个设备自身账号

(DPAN) 和相关联的数据,其中至少一个 DPAN(例如 DPAN 214)中的每个 DPAN 与关联有消费者(例如持卡人 108)的支付帐户相关联。在一个实施例中,支付设备 106 可与消费者 108 相关联。

[0045] 在步骤 406 中,可由处理设备(例如处理单元 206)生成针对至少一个 DPAN214 中的每个 DPAN 的个性化脚本(例如个性化脚本 218),其中个性化脚本 218 包括与相对应的 DPAN 214 相关联的数据集。在一个实施例中,个性化脚本 218 可配置为使支付设备 106 将安全存储器中的现有的 DPAN 和相关联的数据集替换为包含在个性化脚本 218 中的 DPAN 214 和相关联的数据集。

[0046] 在步骤 408 中,可由传输设备 202 向支付设备 106 传输至少一个个性化脚本 218,其中支付设备 106 配置为将 CPAN 用于所选的加密运算(因此反而由 CPAN 发行者来处理这些数据项),并将 DPAN 和相关联的数据集用于金融交易的所有其他的方面。在一个实施例中,可使提供的 CPAN 作为金融交易的一部分的附加数据。在一些实施例中,支付设备 106 还可配置为存储针对多个用途的个性化脚本 218。

[0047] 在一个实施例中,支付设备 106 还可配置为将个性化脚本 218 存储在除安全存储器以外的存储器中。在另一实施例中,支付设备 106 可配置为在该支付设备 106 执行脚本之前就向安全存储器传输个性化脚本 218。在再一实施例中,响应由用户接收的指令而向安全存储器传输个性化脚本 218。在另一实施例中,用户可以是与关联有存储在个性化脚本 218 中的 DPAN 214 的支付帐户相关联的消费者 108。

[0048] 在一些实施例中,个性化脚本 218 可配置为其不会被支付设备 106 修改。在另一实施例中,支付设备 106 可配置为检测任何试图对个性化脚本 218 的修改。在一个实施例中,个性化脚本 218 可配置为由存储在支付设备 106 中且由该支付设备 106 执行的软件应用所执行。在另一实施例中,方法 400 还可包括由传输设备 202 向支付设备 106 传输软件应用。

[0049] 计算机系统架构

[0050] 图 5 示出了计算机系统 500,其中本公开的该计算机系统实施例或其部分可实施为计算机可读代码。例如,图 1 的移动设备 102、处理服务器 116、发行者 104、商家 112、捕获器 114 和移动网络运营商 110 可利用硬件、软件、固件、其中存储有指令的非暂时性计算机可读介质或它们的组合来实施在计算机系统 500 中,或者实施在一个或多个计算机系统或其他处理系统中。硬件、软件或它们的任意组合可体现为用于实施图 4A、4B、6 和 7 的方法的模块和组件。

[0051] 如果使用可编程逻辑,那么这种逻辑可执行在市售处理平台或专用的设备上。本领域普通技术人员可以理解,所公开主题的实施例可通过各种计算机系统配置来加以实践,这包括多核多处理器系统、小型计算机、大型计算机、具有分布式功能的链接或群集式计算机,以及可虚拟嵌入到任何设备中的遍布型计算机或微型计算机。例如,至少一个处理器设备和存储器可用于实现上述实施例。

[0052] 如本文中所述的处理器设备可以是单个处理器、多个处理器或它们的组合。处理器设备可具有一个或多个处理器“内核”。本文所讨论的术语“计算机程序介质”、“非暂时性计算机可读介质”和“计算机可用介质”用于一般性指代有形介质,诸如可拆卸存储单元 518、可拆卸存储单元 522 以及安装在硬盘驱动器 512 中的硬盘。

[0053] 本公开的各种实施例都是根据本示例性计算机系统 500 来进行描述的。相关领域技术人员在阅读本说明书之后,对于如何使用其他计算机系统和 / 或计算机架构来实现本发明将变得显而易见。尽管将操作描述为顺序的过程,但是一些操作实际上可并行、同时执行和 / 或在分布式环境中执行,并且通过由单个或多个处理器访问的本地或远程存储的程序代码来执行。此外,在一些实施例中,在不背离所公开主题的精神的情况下可重新排列操作顺序。

[0054] 处理器设备 504 可以是专用或通用处理器设备。处理器设备 504 可连接于诸如总线、消息队列、网络、多核消息传递方案等的通信基础设施 506。网络可以是适于执行此处所公开的功能的任何网络,并可包括局域网 (LAN)、广域网 (WAN)、无线网络 (例如 WiFi)、移动通信网络、卫星网络、因特网、光纤、同轴电缆、红外、射频 (RF) 或者它们的任意组合。相关领域技术人员将显而易见其他合适的网络类型和配置。计算机系统 500 还可包括主存储器 508 (例如随机访问存储器、只读存储器等),并且还可包括辅助存储器 510。辅助存储器 510 可包括硬盘驱动器 512 和可拆卸存储驱动器 514 (例如软盘驱动器、磁带驱动器、光盘驱动器,闪存等)。

[0055] 可拆卸存储驱动器 514 可通过公知的方式来读取和 / 或写入可拆卸存储单元 518。可拆卸存储单元 518 包括可由可拆卸存储驱动器 514 进行读取并写入的可拆卸存储介质。例如,如果可拆卸存储驱动器 514 是软盘驱动器,那么可拆卸存储单元 518 可以是软盘磁盘。在一个实施例中,可拆卸存储单元 518 可以是非暂时性计算机可读记录介质。

[0056] 在一些实施例中,辅助存储器 510 可包括用于允许将计算机程序或其他指令加载到计算机系统 500 中的其他类似装置,例如可拆卸存储单元 522 和接口 520。这种装置的示例可包括程序盒式存储器和盒式接口 (例如,如同在视频游戏系统中看到的那样)、可拆卸存储器芯片 (例如 EEPROM、PROM 等) 和相关的插座,以及相关领域技术人员显而易见的其他可拆卸存储单元 522 和接口 520。

[0057] 存储在计算机系统 500 中 (例如存储在主存储器 508 和 / 或辅助存储器 510 中) 的数据可存储在任何类型的合适的计算机可读介质中,例如光学存储器 (例如压缩盘、数字多功能盘、蓝光射线光盘等) 或磁带存储器 (例如硬盘驱动器)。数据可配置为例如关系数据库、结构化查询语言 (SQL) 数据库、分布式数据库、对象数据库等任何合适类型的数据库配置。相关领域技术人员将显而易见那些合适配置和数据库存储类型。

[0058] 计算机系统 500 还可包括通信接口 524。通信接口 524 可配置为允许软件和数据在计算机系统 500 与外部设备之间传递。示例性通信接口 524 可包括调制解调器、网络接口 (例如以太网卡)、通信端口、PCMCIA 槽和卡等。经由通信接口 524 传递的软件和数据可以是信号的形式,其可以是电子信号、电磁信号、光学信号或相关领域技术人员显而易见的其他信号。该信号可通过通信路径 526 来传播,其中所述通信路径可配置用于承载信号并可采用电线、电缆、光纤、电话线、蜂窝电话链路、射频链路等来实现。

[0059] 计算机程序介质和计算机可用介质是指诸如主存储器 508 和辅助存储器 510 的存储器,其可以是存储器半导体 (例如 DRAM 等)。这些计算机程序产品可以是用于向计算机系统 500 提供的软件的机构。计算机程序 (例如计算机控制逻辑) 可存储在主存储器 508 和 / 或辅助存储器 510 中。计算机程序也可以经由通信接口 524 来接收。这种计算机程序当执行时能够使计算机系统 500 执行这里所讨论的本发明的方法。具体地,计算机程序在

被执行时能够使处理器设备 504 执行这里所讨论的如图 4 所示的方法。因此,这种计算机程序可代表计算机系统 500 的控制器。在本发明采用软件来实现的情况下,该软件可存储在计算机程序产品中,并可利用移动存储驱动器 514、接口 520 和硬盘驱动器 512,或者利用通信接口 524 而加载到计算机系统 500 中。

[0060] 与本公开相一致的技术,除其他特征以外,提供了用于传输供支付设备使用的多个支付帐户的系统及方法。尽管上文已经描述了所公开系统和方法的各种示例性实施例,但应该理解的是,它们仅用于示例性的目而并非加以限制。本公开并非是详尽的,并且不限制所公开的精确形式。在不脱离本公开广度或范围的情况下,可根据上述教导进行修改及变型,或者从本公开的实践中获知修改及变型。

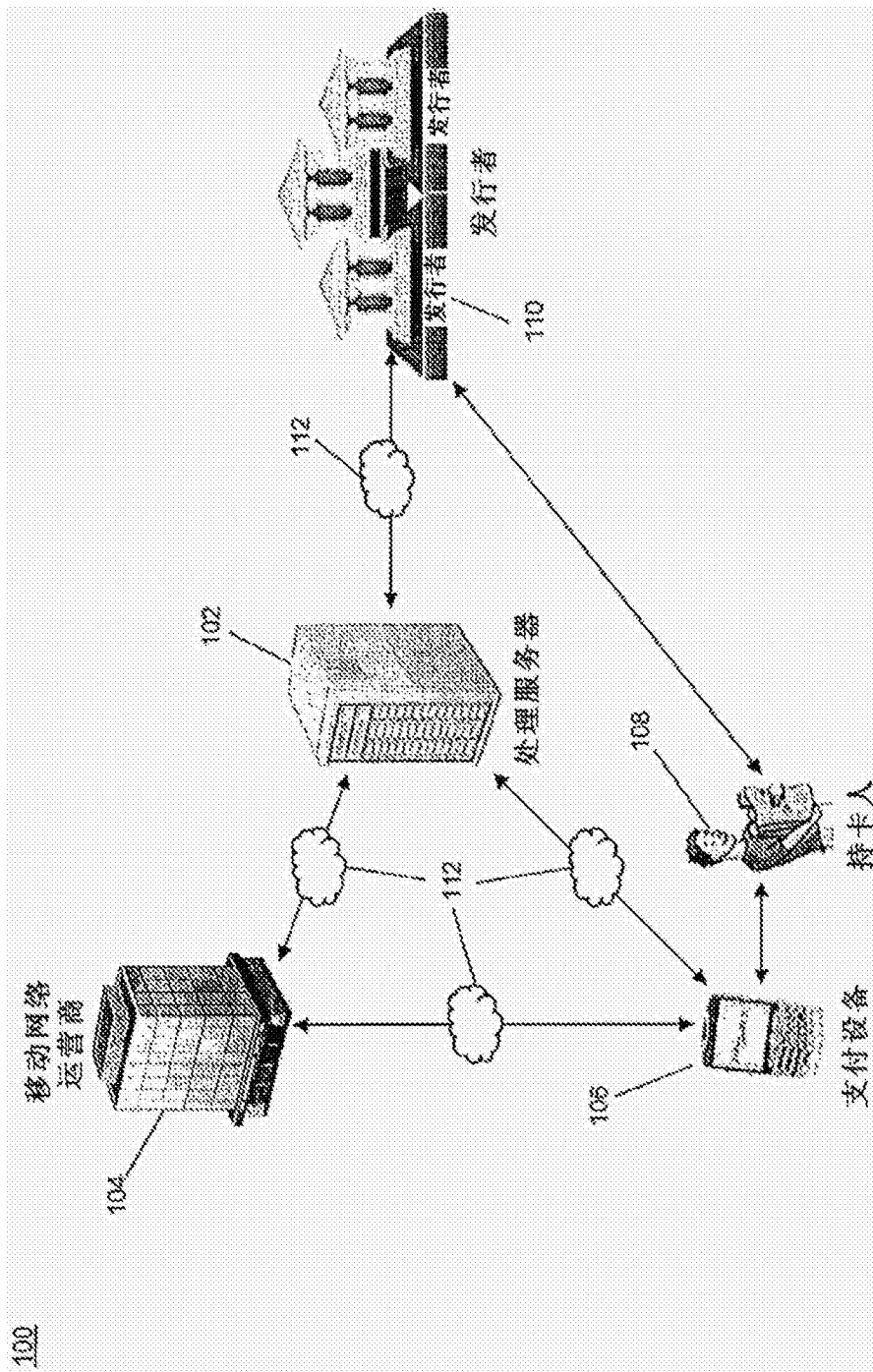


图 1

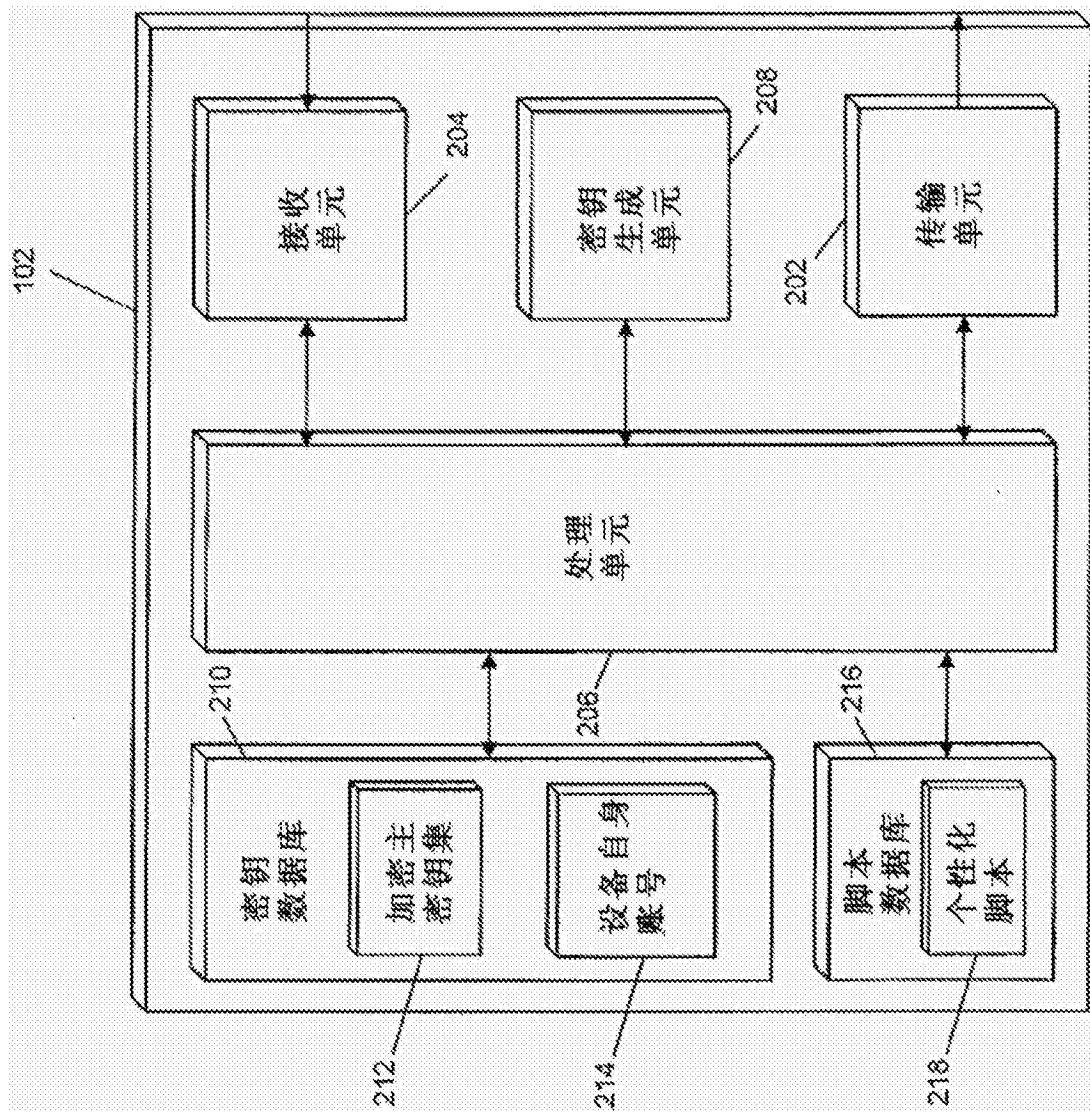


图 2

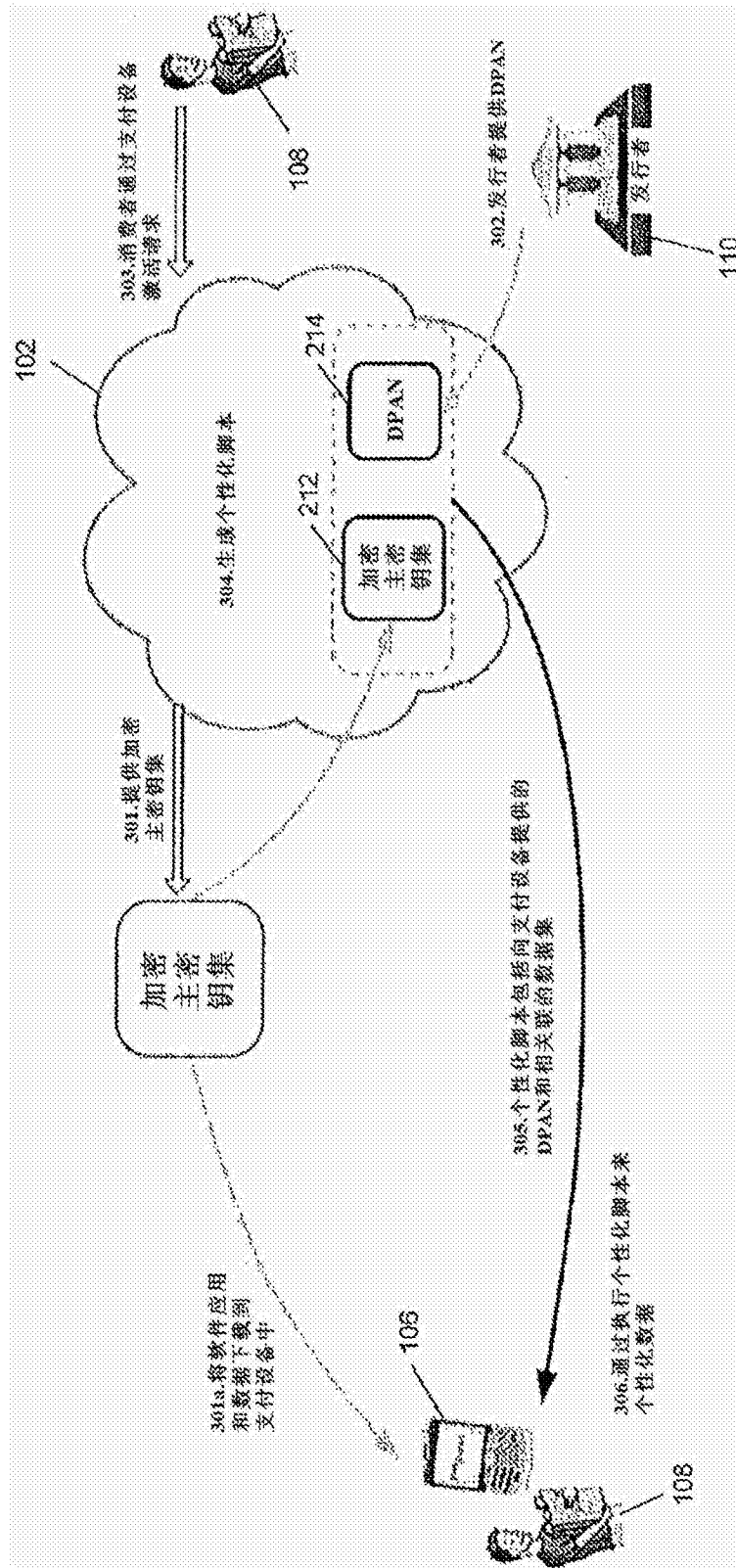


图 3

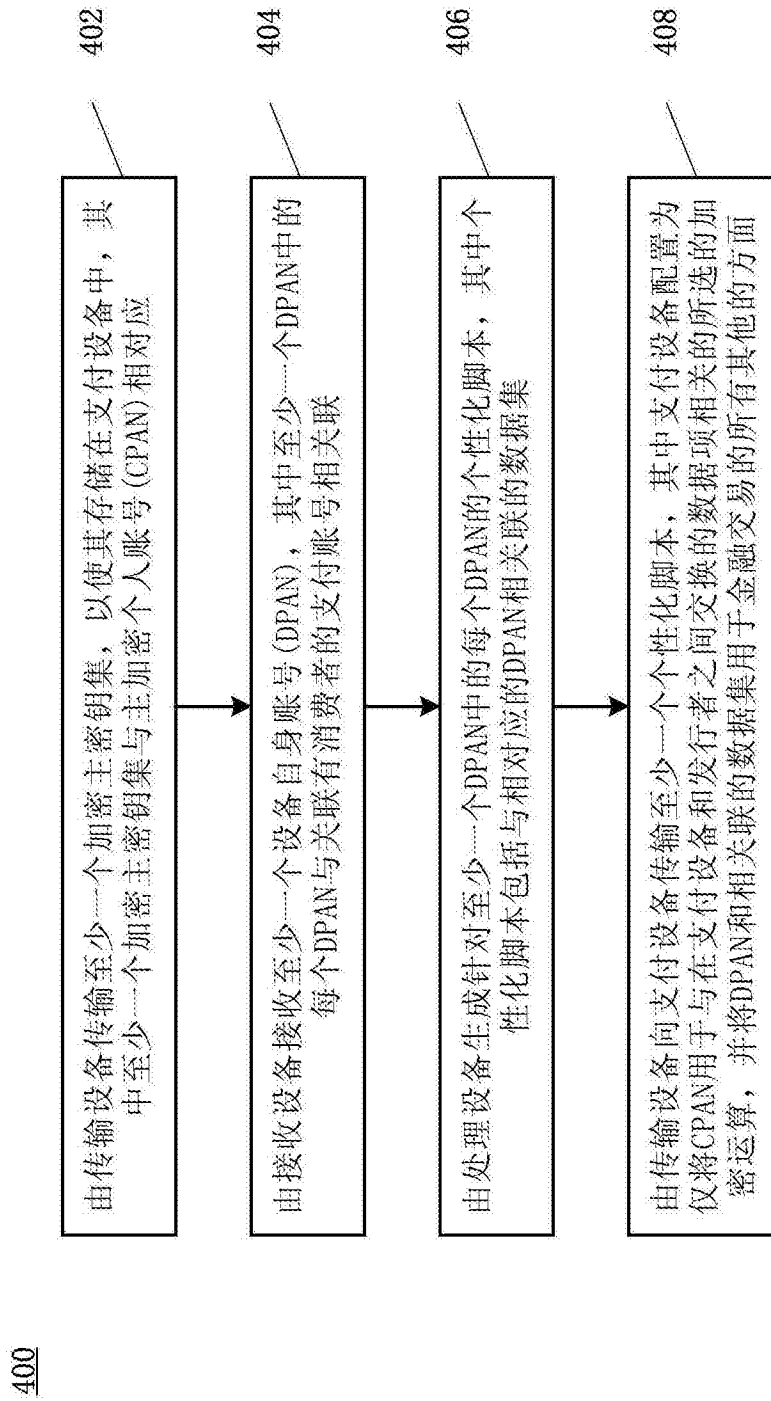


图 4

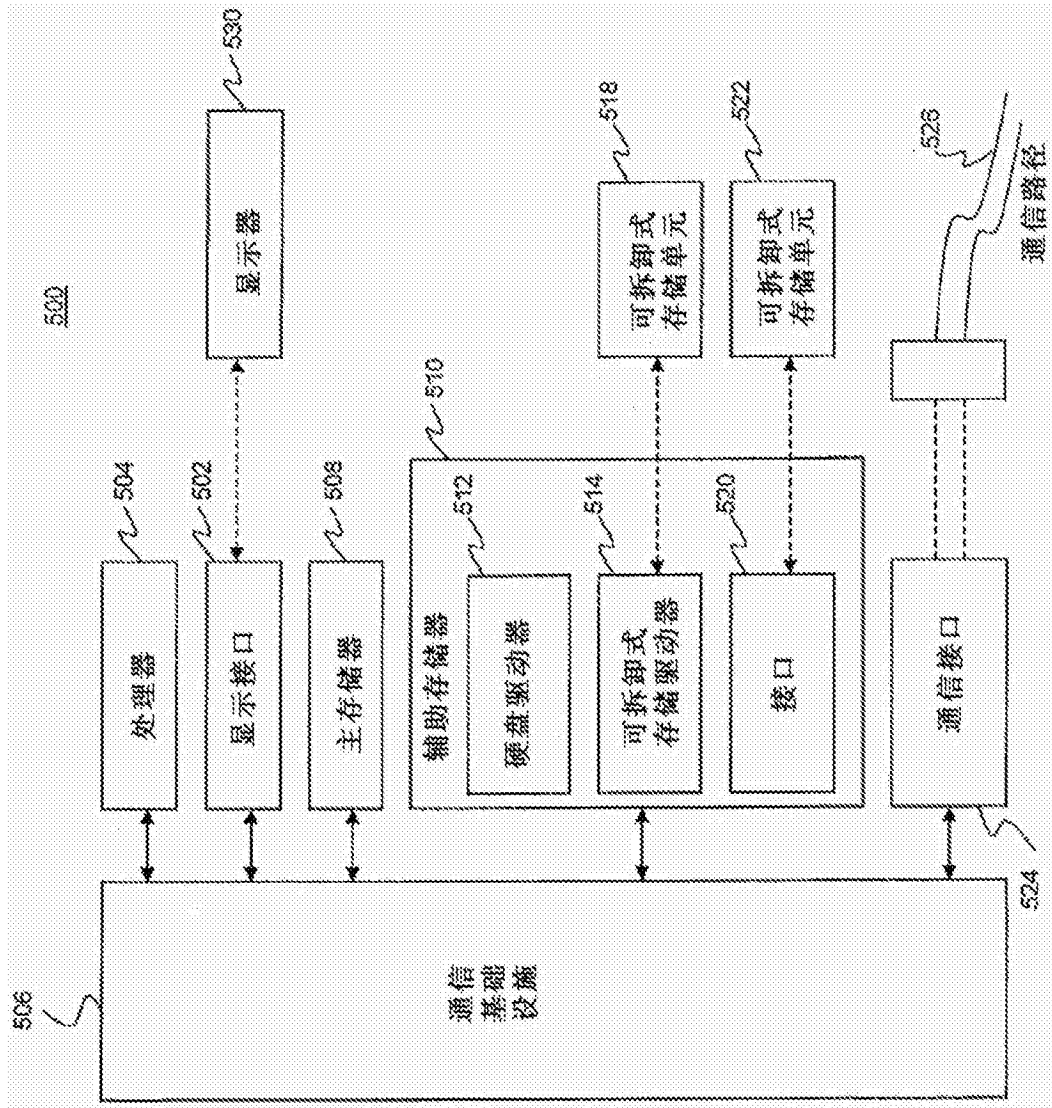


图 5