(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104412285 A
(43)申请公布日 2015.03.11

(21)申请号 201380034886.5

(22)申请日 2013.04.05

(30)优先权数据
61/693,089 2012.08.24 US

(85)PCT国际申请进入国家阶段日
2014.12.29

(86)PCT国际申请的申请数据
PCT/US2013/035406 2013.04.05

(87)PCT国际申请的公布数据
WO2014/031183 EN 2014.02.27

(71)申请人 JVL风险投资有限责任公司
地址 美国纽约州

(72)发明人 C.W. 沃森

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 周少杰

(51)Int.Cl.
G06Q 20/34(2006.01)
G07F 7/10(2006.01)
G06F 21/77(2006.01)

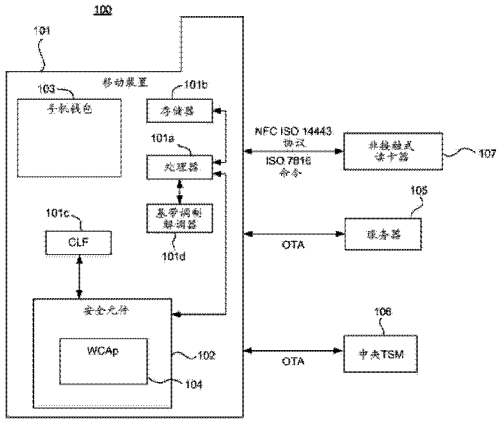
权利要求书2页 说明书16页 附图8页

(54)发明名称

用于保护和管理安全元件上的应用程序的系统、方法和计算机程序产品

(57)摘要

本发明提供用于保护和管理安全元件上的应用程序的系统、方法和计算机程序产品。手机钱包数据存储在至少一个存储器中。从手机钱包接收认证数据。基于所述认证数据和所述手机钱包数据的比较确定所述认证数据是否有效。如果所述认证数据有效，那么启动一个或多个命令的处理。从所述手机钱包接收第一命令。确定是否启动所述第一命令的处理且如果启动所述第一命令，那么处理所述第一命令。



CN 104412285 A

1. 一种用于保护和管理应用程序的系统，其包括：

至少一个存储器，其可操作来存储手机钱包数据；和

耦接到所述至少一个存储器的处理器，所述处理器可操作来：

从手机钱包接收认证数据；

基于所述认证数据和所述手机钱包数据的比较确定所述认证数据是否有效；

如果所述认证数据有效，那么启动一个或多个命令的处理；

从所述手机钱包接收第一命令；

确定是否启动所述第一命令的处理；且

如果启动所述第一命令的处理，那么处理所述第一命令。

2. 根据权利要求 1 所述的系统，所述至少一个存储器还可操作来存储安全状态，

其中所述安全状态是基于所述认证数据是否有效的所述确定，且

其中还基于所述安全状态启动所述一个或多个命令的处理。

3. 根据权利要求 2 所述的系统，其中所述安全状态是下列各项中的一个：(1) 非选定、(2) 选定非认证，或 (3) 认证。

4. 根据权利要求 1 所述的系统，其中所述手机钱包数据包括下列各项中的至少一个：(1) 用户身份模块标识符 (ID)、(2) 装置 ID、(3) 客户端 ID、(4) 密码、(5) 服务器密钥、(6) 服务器密钥验证码，或 (7) 小部件认证信息。

5. 根据权利要求 1 所述的系统，其还包括应用程序注册表，所述应用程序注册表包括每个具有对应状态的一个或多个应用程序标识符。

6. 根据权利要求 5 所述的系统，所述至少一个存储器还可操作来存储对应于所述一个或多个应用程序标识符中的每个的应用程序，其中所述第一命令是修改所述一个或多个应用程序的设置的命令。

7. 根据权利要求 5 所述的系统，所述处理器还可操作来接收对应于所述一个或多个应用程序标识符的更新信息。

8. 一种用于保护和管理应用程序的方法，所述方法包括以下步骤：

从手机钱包接收认证数据；

基于所述认证数据和存储在至少一个存储器中的手机钱包数据的比较确定所述认证数据是否有效；

如果所述认证数据有效，那么启动一个或多个命令的处理；

从所述手机钱包接收第一命令；

确定是否启动所述第一命令的处理；和

如果启动所述第一命令的处理，那么处理所述第一命令。

9. 根据权利要求 8 所述的方法，其中存储在所述至少一个存储器中的安全状态是基于确定所述认证数据是否有效的所述步骤，且其中还基于所述安全状态启动所述一个或多个命令的处理。

10. 根据权利要求 9 所述的方法，其中所述安全状态是下列各项中的一个：(1) 非选定、(2) 选定非认证，或 (3) 认证。

11. 根据权利要求 8 所述的方法，其中所述手机钱包数据包括下列各项中的至少一个：(1) 用户身份模块标识符 (ID)、(2) 装置 ID、(3) 客户端 ID、(4) 密码、(5) 服务器密钥、(6)

服务器密钥验证码，或 (7) 小部件认证信息。

12. 根据权利要求 8 所述的方法，其中所述至少一个存储器包括应用程序注册表，所述应用程序注册表包括每个具有对应状态的一个或多个应用程序标识符。

13. 根据权利要求 12 所述的方法，其中所述第一命令是修改存储在所述至少一个存储器中的对应于所述一个或多个应用程序标识符的一个或多个应用程序的设置的命令。

14. 根据权利要求 12 所述的方法，其还包括接收对应于所述一个或多个应用程序标识符的更新信息的步骤。

15. 一种具有在其上存储的指令序列的非暂时性计算机可读介质，所述指令序列用于使得一个或多个处理器进行下列各项：

从手机钱包接收认证数据；

基于所述认证数据和存储在至少一个存储器中的手机钱包数据的比较确定所述认证数据是否有效；

如果所述认证数据有效，那么启动一个或多个命令的处理；

从所述手机钱包接收第一命令；

确定是否启动所述第一命令的处理；且

如果启动所述第一命令的处理，那么处理所述第一命令。

16. 根据权利要求 15 所述的计算机可读介质，其中存储在所述至少一个存储器中的安全状态是基于所述认证数据是否有效的所述确定，且其中还基于所述安全状态启动所述一个或多个命令的处理。

17. 根据权利要求 16 所述的方法，其中所述安全状态是下列各项中的一个：(1) 非选定、(2) 选定非认证，或 (3) 认证。

18. 根据权利要求 15 所述的方法，其中所述手机钱包数据包括下列各项中的至少一个：(1) 用户身份模块标识符 (ID)、(2) 装置 ID、(3) 客户端 ID、(4) 密码、(5) 服务器密钥、(6) 服务器密钥验证码，或 (7) 小部件认证信息。

19. 根据权利要求 15 所述的方法，其中所述至少一个存储器包括应用程序注册表，所述应用程序注册表包括每个具有对应状态的一个或多个应用程序标识符。

20. 根据权利要求 19 所述的方法，其中所述第一命令是修改存储在所述至少一个存储器中的对应于所述一个或多个应用程序标识符的一个或多个付款应用程序的设置的命令。

21. 根据权利要求 19 所述的方法，其中所述指令序列还使得所述一个或多个处理器接收对应于所述一个或多个应用程序标识符的更新信息。

用于保护和管理安全元件上的应用程序的系统、方法和计算机程序产品

技术领域

[0001] 本发明大体涉及在移动商务中使用的移动装置中的钱包伴侣小应用程序和手机钱包，且更特定地涉及用于保护和管理安全元件上的应用程序的系统、方法和计算机程序产品。

背景技术

[0002] 付款和商务应用程序在移动商务环境中用来使用移动装置进行交易而不需要现金、支票、信用卡等等。这些交易可以是金融的（例如，付款）或非金融的（例如，验票入场）。在移动商务环境中，服务供应商 (SP) 提供这些移动应用程序以部署到顾客的移动装置。服务供应商是给顾客提供服务的公司、组织或实体，诸如银行、商家、卡协会、营销公司、高速运输管理局等等。

[0003] 服务可以是服务供应商允许或提供的活动、能力、功能、工作或用途，诸如付款服务、信用卡、借记卡、支票、赠品、优惠价或忠诚度服务、入境签证服务等等。服务链接到由 SP 发行的账户（例如，支票、借记卡、信用卡）。每个账户包括可以用来执行或记录移动商务环境中的交易的大量数据，诸如金融信息、个人顾客信息、交易历史等等。

[0004] 当移动付款应用程序充分配置和激活时，其被部署到移动装置上且链接到服务和 SP 发行的账户。顾客然后可使用移动装置以在装有支持近场通信 (NFC) 的读卡器模块等等的销售点 (PoS) 处进行交易，诸如非接触式付款。

[0005] 在非接触式交易期间，顾客将装有一个或多个付款应用程序的移动装置定位成紧靠读卡器模块，这将激活付款应用程序的请求传输到移动装置以进行非接触式交易。典型的付款应用程序使用所谓的“自激活”特权，允许每个应用程序独立地授权且激活非接触式交易。自激活意指每个应用程序独立地控制并管理其自身的激活和 / 或授权。在自激活特权配置中，一般使用个人识别码 (PIN) 验证授予这种授权。每个付款应用程序将对应的 PIN 存储在移动装置的存储器中。在非接触式交易期间，顾客例如凭借通过移动装置的用户界面输入 PIN 授权付款应用程序的激活。这然后又使得移动装置中的另一应用程序或硬件比较由顾客输入的 PIN 与所存储的 PIN 以进行配对。

[0006] 还可在没有这种自激活特权的情况下部署或配置付款应用程序。在这种配置中，读卡器模块与这些付款应用程序通信且访问这些付款应用程序而不需要任何授权或验证。

[0007] 一个技术挑战涉及使得付款应用程序更加安全。在非接触式交易期间通过访问移动装置上的应用程序，存在风险 :读卡器模块可用来执行多余或欺诈交易、资金损失、金融危机和危及顾客数据、身份盗用、移动装置和应用程序面临的风险等等。

[0008] 另一技术挑战涉及使得 SP（包括 SP 系统）和其对应的付款应用程序更加安全和有效。典型的 SP 面临以下任务 :将付款应用程序部署到多种移动装置，且保证每个付款应用程序被配置来安全地、有效地且有力地管理其自身的 PIN 和可访问性，同时与其它付款应用程序一起在相同移动装置上运行。与单独且更加安全的系统相比，存储和管理移动装

置的非易失性存储器上的 PIN 危及付款应用程序和移动装置的安全。

[0009] 每个移动装置可以具有用于每个 SP 的多个付款应用程序，其中每个付款应用程序具有其自身的 PIN。结果，顾客面临记忆多个 PIN、输入每个 PIN 以授权对应的非接触式交易的低效、复杂且潜在不安全的负担。

[0010] 此外，读卡器模块面临与潜在大量的付款应用程序进行通信的任务。一个技术挑战涉及结合确定与哪个适当的付款应用程序通信以授权非接触式交易来减小处理能力，同时提升可靠性和效率。

[0011] 从 SP 的观点来看最重要的是，付款应用程序被部署到移动装置且其付款应用程序可被访问和使用以安全地进行交易。从顾客的观点来看，最重要的是其可以最少的工作量或装置交互来安全地进行交易且不危及其移动装置或个人信息的安全性。从读卡器模块的观点来看，最重要的是，每个读卡器可有效且准确地管理每个交易，且处理器时间和资源尽可能少。

发明内容

[0012] 本发明提供用于保护和管理安全元件上的应用程序的系统、方法和计算机程序产品。

[0013] 在一个实施方案中，一种用于保护和管理应用程序的系统包括耦接到处理器的至少一个存储器。手机钱包数据存储在所述至少一个存储器中。从手机钱包接收认证数据。基于所述认证数据和所述手机钱包数据的比较确定所述认证数据是否有效。如果所述认证数据有效，那么启动一个或多个命令的处理。从所述手机钱包接收第一命令。确定是否启动所述第一命令的处理且如果启动所述第一命令，那么处理所述第一命令。

[0014] 在另一实施方案中，一种用于保护和管理应用程序的方法包括：从手机钱包接收认证数据；基于所述认证数据和存储在至少一个存储器中的手机钱包数据的比较确定所述认证数据是否有效；如果所述认证数据有效，那么启动一个或多个命令的处理；从所述手机钱包接收第一命令；确定是否启动所述第一命令的处理；和如果启动所述第一命令的处理，那么处理所述第一命令。

[0015] 在另一实施方案中，一种具有在其上存储的指令序列的非暂时性计算机可读介质，所述指令序列用于使得一个或多个处理器进行下列各项：从手机钱包接收认证数据；基于所述认证数据和存储在至少一个存储器中的手机钱包数据的比较确定所述认证数据是否有效；如果所述认证数据有效，那么启动一个或多个命令的处理；从所述手机钱包接收第一命令；确定是否启动所述第一命令的处理；和如果启动所述第一命令的处理，那么处理所述第一命令。

附图说明

[0016] 根据下文结合以下附图陈述的详细描述将更加明白本发明的其它特征和优点。

[0017] 图 1 是根据示例性实施方案的用于保护和管理安全元件上的应用程序的系统的图。

[0018] 图 2 是示出根据示例性实施方案的 WCAp 的生命周期的图。

[0019] 图 3 是示出根据示例性实施方案的 WCAp 安全状态的生命周期的图。

[0020] 图 4 是示出根据示例性实施方案的用于验证密码的程序的流程图。

[0021] 图 5 是根据示例性实施方案的 CRS 镜像的图。

[0022] 图 6 是示出根据示例性实施方案的用于选择并激活主付款应用程序的程序的次序图。

[0023] 图 7 是示出根据示例性实施方案的用于管理非接触式交易的程序的次序图。

[0024] 图 8 是示出根据示例性实施方案的手机钱包与服务器之间的相互认证程序的次序图。

[0025] 图 9 是有用于实施本发明的示例性系统的方框图。

具体实施方式

[0026] I. 概述

[0027] 本文中展现的示例性实施方案涉及用于保护和管理应用程序的系统、方法和计算机程序产品，所述应用程序现在本文中是针对移动商务环境中的示例性系统而描述。这只是为了方便起见且不旨在限制本发明的应用。事实上，在阅读以下描述之后，本领域一般技术人员将明白如何实施替代实施方案中的以下发明，诸如移动营销、广告、出票、信息服务、浏览等等。

[0028] 术语“应用程序”、“小应用程序”、“小部件”和 / 或这些术语的复数形式在本文中可交换使用以指代当由一个或多个处理器（例如，移动装置、读卡器、终端机、销售点 (POS) 系统或服务器中）执行时使得处理器执行具体任务的应用程序（独立地或结合其它应用程序运行）或指令或代码的集合或子集。例如，钱包应用程序可用来进行交易或界面相关功能，诸如存储、处理、访问或传输金融、忠诚度、优惠价、会员或账户数据。钱包应用程序还可以并有一个或多个付款应用程序或与一个或多个付款应用程序交互，所述一个或多个付款应用程序诸如快速付款形式的 American Express®、 Discover® Network Zip℠、MasterCard® PayPass™ 和 Visa payWave™ 付款小应用程序。

[0029] 术语“PIN”、“密码”和 / 或这些术语的复数形式在本文中可交换使用以指代用来认证系统、用户、实体等等的唯一标识符。

[0030] 一般来说，提供一种用于保护和管理安全元件 (SE) 中的应用程序的机制。特定地说，钱包伴侣小应用程序 (WCAp) 监控、管理和 / 或保护与手机钱包相关的某些类型的应用程序，诸如用于进行金融交易的付款应用程序或用于执行与处理忠诚度、优惠价、会员或账户数据相关的任务的商务应用程序。

[0031] WCAp 可以是在移动装置上运行的应用程序且执行以下功能，诸如 :安全地存储手机钱包数据、执行诸如奇偶校验和密码验证的认证、处理命令、维护注册表中的钱包应用程序数据、管理（例如，激活和禁用）应用程序、认证服务器，且参与非接触式交易的处理。WCAp 还可以是被配置来执行这些功能的独立式（即，独立）系统。

[0032] 在示例性实施方案中，WCAp 的状态指示其功能（例如，WCAp 将处理的命令类型）。例如在安全元件的制造期间，WCAp 被加载到安全元件上。然后 WCAp 又可以安装在安全元件上。在安装之后，WCAp 的功能可被限于（例如）处理诸如展示 WCAp 可选择的“选择”命令的某些命令。当可选择时，修改 WCAp 的功能以处理额外和 / 或不同命令。当可选择时，WCAp 还可处于非个人化或个人化状态。在非个人化状态中，WCAp 缺少进行交易所必需的信

息。WCAp 可以通过接收和 / 或存储诸如标识符和密码的信息而个人化。在一个实施方案中，WCAp 被置于个人化状态。即，在个人化状态中，WCAp 是活动的且安全地存储诸如手机钱包数据的信息。

[0033] 在替代示例性实施方案中，WCAp 可以处于多种安全状态中的一个中。基于 WCAp 从手机钱包接收的命令确定特定的安全状态。所述命令包括选择 WCAp、执行奇偶校验和 / 或密码验证的命令。在一个实施方案中，WCAp 安全状态是“非选定”、“选定非认证”和“认证”。在非选定状态中，WCAp 脱离上下文且只有资格接收和处理某些命令。在选定非认证状态中，WCAp 已（例如，通过处理“选择”命令）选择，且其在上下文中且可以处理无需认证 WCAp 的命令。在认证状态中，（例如，通过成功地执行奇偶校验或密码验证）认证 WCAp，且 WCAp 可以处理需要认证 WCAp 的命令。手机钱包的认证可以通过执行奇偶校验或密码验证来实现，在此期间 WCAp 比较从移动装置接收的数据与存储在 WCAp 上或结合 WCAp 的数据。

[0034] 如上文提及，WCAp 监控和保护某些应用。这通过维护包括关于付款应用程序的信息（诸如应用程序状态、错误和 / 或是否已选择应用程序）的注册表来完成。这种信息可以例如从应用程序或安全元件环境接收，且然后又用来跟踪与应用程序有关的更新。使用注册表，WCAp 管理（例如，允许和 / 或拒绝）在非接触式交易期间使用付款应用程序的激活。

[0035] 下文参考图 1 至图 9 进一步详细地讨论上述特征。

[0036] II. 系统

[0037] 图 1 是根据示例性实施方案的用于保护和管理安全元件上的应用程序的系统 100 的图。如图 1 中示出，系统 100 包括移动装置 101、安全元件 102、手机钱包 103、WCAp 104、手机钱包服务器（本文中称作“服务器”）105、中央信赖服务管理器 (TSM) 106 和非接触式读卡器 107。

[0038] 移动装置 101 可以是例如移动电话等等，且包括处理器 101a、存储器 101b、非接触式前端 (CLF) 101c、基带调制解调器 101d 和用户界面，诸如显示器。基带调制解调器 101d 是用于移动网络通信的数字调制解调器。CLF 101c 是处置非接触式传输链路的 NFC 通信和通信协议层的模拟部分的电路。此外，CLF 101c 用来交换安全元件 102 与非接触式读卡器 107 之间的数据，以例如执行非接触式交易。

[0039] 移动装置 101 还包括安全元件 102，其可以被实施为通用集成电路卡 (UICC)、嵌入式 SE 卡、安全微型安全数字 (microSD) 卡等等。安全元件 102 一般被认为是安全的，因为其是独立系统（包括专用存储器），且受通过独立测试验证的硬件和软件硬化技术保护。

[0040] 安全元件 102 可以包括操作系统，诸如 GlobalPlatform™ 环境（下文称作“Open”），其对安全元件上的应用程序提供应用程序设计界面和其它服务，诸如：命令调度、应用程序选择、逻辑通道管理和内容管理。在这样的环境中，安全元件 102 还可以包括非接触式注册表服务 (CRS)、CRS 应用程序（下文也称作“CRS 小应用程序”）和 / 或非接触式注册表事件监听器 (CREL) 应用程序。CRS 被配置来管理和提供对应用程序（诸如付款应用程序）的访问。CRS 应用程序被配置来对最终用户提供应用程序管理，包括 CRS 的管理。CREL 应用程序是被配置来接收关于应用程序的改变和 / 或更新的通知的应用程序。“GlobalPlatform Card - Contactless Services, Card Specification v2.2 - Amendment C, Version 1.0.1.8”中更加详细地描述了这样的环境。这种 GlobalPlatform™ 配置的一

个缺点是需要 CREL 应用程序，其独立地管理安全元件上的应用程序的集合或子集且使用单个密码提供和 / 或限制对所述应用程序的访问。

[0041] 安全元件 102 包括（例如，在其上存储的）WCAp 104（下文参考图 2 至图 5 进一步详细地描述）和一个或多个付款应用程序。每个付款应用程序链接到服务和由 SP 发行的账户。例如，在安全元件 102 的制造和 / 或配置期间，WCAp 104 和付款应用程序可被加载到安全元件上。WCAp 104 和付款应用程序可以被个人化来使得其使用能够进行交易。下文参考表格 1 进一步详细地描述 WCAp 104 的个人化。

[0042] 在一个实施方案中，由 TSM（诸如中央 TSM 106）个人化 WCAp104。通常，中央 TSM 管理往返于安全元件的通信，且可用来例如将数据加载到安全元件上。以引用的方式全部并入本文中的标题是“Systems,Methods,and Computer Program Products for InterfacingMultiple Service Provider Trusted Service Managers and Secure Elements”的第 13/653,160 号美国专利申请描述了用于管理与安全元件进行的通信的中央 TSM。

[0043] 手机钱包 103（即，手机钱包客户端）可以是存储在移动装置 101 中的应用程序。手机钱包 103 包括当由移动装置 101 的处理器执行时使得移动装置 101 用作例如用于处理诸如非接触式付款的交易的工具的指令。手机钱包 103 与 WCAp 104 通信以执行这些交易。特定地说，手机钱包 103 使用国际标准组织 (ISO)7816 命令与安全元件 102 和 / 或 WCAp 104 通信。应了解，装置之间的这些和其它通信可以包括与或通过其它介入系统、硬件和 / 或软件进行的通信。

[0044] 为了与 WCAp 104 通信，手机钱包 103 必须通过下文参考图 4 和表格 1 和 2 进一步详细地描述的成功 PIN 验证或奇偶校验来认证其自身。

[0045] WCAp 104 还包括近距离付款系统环境 (PPSE)。PPSE 是用来维护安全元件上的一系列付款应用程序的应用程序，且通过使得付款应用程序对系统或装置可见或不可见（即，可访问）来对每个付款应用程序提供可访问性。

[0046] 在一个实施方案中，顾客可以使用移动装置 101 以在装有非接触式读卡器 107（诸如近距离耦接装置 (PCD) 或支持 NFC 的读卡器）的 POS 处进行非接触式交易。顾客将移动装置 101 放置在非接触式读卡器 107 的预定必需距离内，非接触式读卡器 107 使用 NFC ISO14443 与移动装置 101 的 CLF 101c。非接触式读卡器 107 还与手机钱包 103、WCAp 104 和 / 或移动装置 102 上的付款应用程序通信以执行非接触式交易。

[0047] WCAp 104 还用来在手机钱包 103 与服务器 105 之间提供相互认证。例如在手机钱包的激活、手机钱包上的服务账户或付款应用程序的设置或手机钱包 PIN 的修改期间，手机钱包 103 与服务器 105 通信。特定地说，WCAp 104 通过生成和验证出票（例如，证书）来认证这些通信。下文参考图 8 进一步详细地描述这种相互认证。

[0048] III. 程序

[0049] A. 个人化 WCAp

[0050] 图 2 是示出根据示例性实施方案的 WCAp（例如，图 1，WCAp104）的生命周期 200 的图。在方框 201 中（“加载 WCAp”），例如在安全元件（例如，图 1，安全元件 102）的制造期间将 WCAp 104 加载到安全元件 102 上。在一个实施方案中，加载 WCAp 104 包括将数据包（包括 Java 转换小应用程序 (CAP) 文件，其包括 WCAp 104 的所有类别和界面）加载到安全

元件 102 上。在方框 201 中，WCAp104 不起作用（即，不能用来进行交易）。

[0051] 在方框 202 中（“安装 WCAp”），将 WCAp 104 安装在安全元件 102 中。特定地说，WCAp 104 的安装包括解包加载文件、链接可执行代码和分配安全元件 102 中的存储器。

[0052] 在方框 203 中（“WCAp 可选择”），例如，通过手机钱包 103 或中央 TSM（例如，图 1，中央 TSM 106）使得 WCAp 104 可选择。此外，除了可选择以外，WCAp 104 分别处于如由方框 203A 和 203B 示出的个人化（即 .，活动）或非个人化（即，不活动）状态。

[0053] 默认地，一旦 WCAp 104 从已安装改变为可选择，将 WCAp 104 置于非个人化状态。

[0054] 然后又可以通过中央 TSM 106 使用存储诸如手机钱包数据的信息的命令个人化（例如，激活）WCAp 104。一旦个人化，可由中央 TSM 106 更新 WCAp 104 以存储已更新的信息（例如，已更新的手机钱包数据）。个人化 WCAp 104 的程序包括从例如手机钱包 103 接收信息和将所述信息的至少一部分存储在 WCAp 104 中和 / 或存储与 WCAp 104 相关的所述信息的至少一部分。WCAp 104 用作数据（诸如由手机钱包 103 使用以处理交易的手机钱包数据）的次级安全存储装置。表格 1 在下文示出存储在 WCAp 104 中的数据的实例，包括元素和对应描述。

[0055] 表格 1

[0056] 存储在 WCAp 中的数据的实例

[0057]

元素	描述
SIM ID	SIM 卡的唯一标识符（*例如*，ICCID）
装置 ID	移动装置的唯一标识符（*例如*，IMEI、MEID、MAC 地址）
钱包 ID	手机钱包的唯一标识符
钱包密码	用来认证手机钱包的使用或用户的密码
钱包服务器密钥	用来对服务器认证手机钱包或 WCAp 的密钥
手机服务器密钥验证码	用来验证钱包服务器密钥的代码
小部件认证二进制对象	对应于小部件的唯一数据
钱包唯一代码	由 WCAp 生成和存储用于手机钱包的唯一代码

[0058] 参考表格 1，钱包密码（下文称作“密码”）是在 WCAp 104 的个人化期间最初由中央 TSM 106 分配的四字符代码。然而，随后可以改变密码。下文参考图 3 和图 4 进一步详细地描述密码。下文参考图 3 和图 8 进一步详细地描述服务器认证密钥和服务器认证密钥

验证码。

[0059] 小部件认证二进制对象包括对应于小部件的数据。小部件是可以结合其它应用程序运行的一种应用程序。小部件认证二进制对象包括诸如小部件 ID、小部件签名和小部件版本的数据。小部件 ID 是小部件的唯一标识符。小部件签名是由用于每个小部件的手机钱包计算的哈希值。小部件版本是每个小部件的版本号和 / 或标识符。

[0060] WCAp 104 存储并提供用于验证小部件数据的工具。特定地说，小部件认证二进制对象由 WCAp 使用来验证小部件的身份。这种验证可使用验证小部件命令来实现，其中与存储在 WCAp 104 中的小部件认证二进制对象数据相比，小部件数据是由手机钱包 103 发送至 WCAp 104。如果以命令发送的小部件数据匹配小部件认证二进制对象数据，那么 WCAp 104 将指示已验证小部件的响应传输到手机钱包。

[0061] 此外，在 WCAp 104 的个人化期间，中央 TSM 106 将 WCAp 104 注册为 CREL 应用程序。说，CREL 应用程序是用来使用 CRS 和 / 或 CRS 应用程序跟踪和 / 或管理多个应用程序的应用程序。CRS 是安全元件上的应用程序的注册表。

[0062] 被注册为 CREL 应用程序的 WCAp 104 包括 CRS 的镜像（即，拷贝或复制）（下文称作“CRS 镜像”）以跟踪和 / 或管理与手机钱包 103 相关的应用程序。WCAp 104 的 CRS 镜像跟踪和 / 或管理 CRS 中的全部或一个子集的应用程序，尤其是已由中央 TSM 106 安装和 / 或提供的应用程序。跟踪和 / 或管理应用程序包括与所述应用程序的使用、访问、授权、激活和或信息更新有关的任何功能和程序。

[0063] 作为 CREL，WCAp 104 接收与由 CRS 镜像跟踪的应用程序有关的事件的通知，诸如应用程序的状态改变。下文参考图 5 至图 7 进一步详细地讨论 CREL 和 CRS。在方框 204 中（“挂起 WCAp”），挂起 WCAp 104，在此期间锁定其功能。虽然图 2 中没有示出，但是可以终止 WCAp 104。在终止之后，由中央 TSM 106 从安全元件 102 删除 WCAp 104。

[0064] B. 认证 WCAp

[0065] 图 3 是示出根据示例性实施方案的 WCAp 安全状态（例如，非选定、选定非认证、认证）的生命周期 300 的图。WCAp 将根据 WCAp 的安全状态处理某些应用程序协议数据单元 (APDU) 命令（本文中称作“命令”）。

[0066] 在方框 301 中（“非选定状态”），WCAp（例如，图 1，WCAp 104）处于非选定状态。在非选定状态中，WCAp 104 脱离上下文且只有资格接收和处理某些命令。表格 2 在下文示出当 WCAp 104 处于特定安全状态时（包括当其处于非选定状态时）可由其处理的命令的实例。

[0067] 表格 2

[0068] WCAp 安全状态期间的可接受命令的实例

[0069]

命令	非选定	选定非认证	认证
选择	是	是	是
存储数据	否	N/A	N/A
获得数据	否	N/A	N/A
取得 WCAp 状态	否	是	是
奇偶校验	否	是	是
验证密码	否	是	是
验证小部件	否	否	是
生成 WS 出票	否	否	是
验证 WS	否	否	是
放置付款设置	否	否	是
恢复版本	否	是	是

[0070] 然后又可通过选择命令选择 WCAp 104(例如,图 2,方框 203,“WCAp 可选择”)。

[0071] 在方框 302 中(“选定非认证状态”),WCAp 104 在通过接收选择命令选择之后处于选定非认证状态。在选定非认证状态中,WCAp104 处于上下文中且可以处理不需要其处于认证状态的命令,如上文参考表格 2 描述。

[0072] 然后又可使用奇偶校验或密码验证来认证 WCAp 104,因而在方框 303 中(“认证状态”)将 WCAp 104 置于认证状态。如下文描述般执行奇偶校验和密码验证。

[0073] 在方框 303 中(“认证状态”),WCAp 104 在成功执行同位检测和 / 或密码验证(“成功密码验证”或“成功奇偶校验”)之后处于认证状态。在认证状态中,WCAp 104 可以如上文参考表格 2 描述般处理命令。

[0074] 图 3 中进一步示出、当开发 WCAp 104 的认证状态、它可以失去其上下文 (“上下文丢失”) 和被放置在非选中状态 (即,方框 301)。此外,可选择 WCAp 104(“WCAp 选择”) 且因此可将其置于选定非认证状态。

[0075] 1. 验证密码

[0076] 如上文参考表格 1 更加详细地讨论,WCAp 104 存储与手机钱包 (例如,图 1,手机钱包 103) 相关的密码。所述密码可以用来将 WCAp 104 置于认证状态和 / 或激活付款应用程序。密码可以被置于 ON 或 OFF 状态 (即,指示认证是否需要密码) 且所述状态存储在 WCAp 104 以外。

[0077] 最初在 WCAp 104 的个人化期间设置密码,这在上文参考图 2 和表格 1 加以描述。特定地说,在密码的设置期间,手机钱包 103 最初例如经由移动装置 101 的用户界面从移动装置 (例如,图 1,移动装置 101) 或用户取回和 / 或接收激活数据 (例如,密码、钱包 ID、装

置 ID、SE ID)。然后，手机钱包 103 又将激活对应于激活数据中的 SE ID 的 WCAp 104 的请求传输到服务器（例如，图 1，服务器 105)。服务器 105 然后将包括激活数据的请求传输到中央 TSM(例如，图 1，中央 TSM 106) 以激活 WCAp 104。中央 TSM 106 将所接收的激活数据的至少一部分（包括密码）存储在 WCAp 104 中。

[0078] WCAp 104 包括称作“重试计数器”的计数器，当密码验证尝试失败（即，已提交的密码不匹配存储在 WCAp 中的设置密码）时所述计数器递增。当重试计数器超过预定限制时，WCAp 104 和 / 或密码可能被锁定。每当密码验证尝试成功（即，已提交的密码匹配存储在 WCAp 中的设置密码）时，重试计数器被重设为零。

[0079] 图 4 是示出根据示例性实施方案的用于验证密码的程序 400 的流程图。在方框 401(“接收验证密码命令”)，WCAp 104 从手机钱包 103 接收验证密码命令，包括密码。

[0080] 在方框 402(“是否锁定 WCAp ？”)，WCAp 104 确定其是否被锁定（即，图 2，方框 204，“挂起 WCAp”)。例如，如果重试计数器超过预定限制，那么 WCAp 104 和 / 或密码可能被锁定。在被锁定之后，WCAp 104 不处理验证密码命令。如果确定 WCAp 104 被锁定，那么 WCAp 104 在方框 403(“错误 :锁定 WCAp”) 将指示 WCAp 104 和 / 或密码被锁定的错误响应传输到手机钱包 103。

[0081] 替代地，如果在方框 402 确定 WCAp 104 没有被锁定，那么 WCAp104 在方框 404(“所接收的密码＝所存储的密码？”) 确定验证密码命令中接收的密码是否匹配存储在 WCAp 104 中的密码。如果在方框 404 确定所接收的密码不匹配所存储的密码，那么 WCAp 104 在方框 405(“递增计数器”) 递增重试计数器。

[0082] 然后，WCAp 104 又在方框 406(“是否锁定 WCAp ？”) 确定 WCAp104 和 / 或密码是否被锁定。如果确定 WCAp104 和 / 或密码被锁定，那么 WCAp 104 在方框 403(“错误 :WCAp 被锁定”) 将指示 WCAp 和 / 或密码被锁定的错误响应传输到手机钱包 103。

[0083] 如果在方框 406 确定 WCAp 104 和 / 或密码没有被锁定，那么 WCAp 104 在方框 407(“错误 :密码验证失败”) 将指示验证密码命令失败（即，没有成功地验证密码）的错误响应传输到手机钱包 103。方框 407 传输的错误响应还可以包括指示重试计数器超过预定限制之前密码验证尝试的剩余次数的信息。

[0084] 如果在方框 404 确定所接收的密码匹配所存储的密码，那么 WCAp 104 在方框 408(“WCAp 状态被设置为认证”) 将其安全状态设置为认证。如上文参考表格 2 描述，WCAp 104 然后可以处理命令。

[0085] 在方框 409(“唯一代码＝唯一代码备份？”)，WCAp 104 确定钱包唯一代码是否匹配钱包唯一代码备份，钱包唯一代码和钱包唯一代码备份两者均存储在 WCAp 104 中。如果 WCAp 104 确定钱包唯一代码匹配钱包唯一代码备份，那么 WCAp 104 在方框 410(“传输响应 :密码验证”) 将包括钱包唯一代码的响应传输到手机钱包 103，指示成功地验证密码。

[0086] 如果在方框 409 确定钱包唯一代码不匹配钱包唯一代码备份，那么 WCAp 104 在方框 411(“生成新的唯一代码”) 确定方框 401 接收的验证密码命令是否包括生成新的钱包唯一代码的指令。如果是，那么 WCAp 104 在方框 412(“生成唯一代码和备份”) 生成并存储新的钱包唯一代码和钱包唯一代码备份，且在方框 410 将新的钱包唯一代码传输到手机钱包 103，指示成功地验证密码。

[0087] 替代地，如果在方框 411 确定方框 401 接收的验证密码命令不包括生成新的钱包

唯一代码的指令，那么 WCAp 104 在方框 413(“错误 :唯一代码验证失败”) 将错误响应传输到手机钱包 103，指示钱包唯一代码的验证失败。

[0088] 2. 执行奇偶校验

[0089] 如上文参考表格 1 更加详细地讨论，WCAp 104 存储数据，所述数据可以包括装置 ID、SIM ID 和 / 或钱包 ID。WCAp 104 使用这种数据的至少一部分执行奇偶校验。

[0090] 特定地说，手机钱包 103 将包括装置 ID、SIM ID 和 / 或钱包 ID 的奇偶校验命令传输到 WCAp 104。比较奇偶校验命令中接收的数据元素中的至少一个与存储在 WCAp 104 中的相同类型的数据元素。

[0091] 在一个实施方案中，比较奇偶校验命令中接收的装置 ID 和钱包 ID 与存储在 WCAp 104 中的装置 ID 和钱包 ID。如果确定所接收的装置 ID 和钱包 ID 匹配存储在 WCAp 104 中的装置 ID 和钱包 ID(例如，与存储在 WCAp 104 中的装置 ID 和钱包 ID 具有相同的值)，那么 WCAp 104 将指示奇偶校验成功的响应传输到手机钱包 103。

[0092] 替代地，如果确定所接收的装置 ID 和钱包 ID 不匹配存储在 WCAp 104 中的装置 ID 和钱包 ID，那么 WCAp 104 将指示奇偶校验失败的响应传输到手机钱包 103。WCAp 104 还可以响应于手机钱包 103 传输指示奇偶校验失败的原因的信息 (例如，命令中接收的值错误、命令中丢失信息、元素验证失败等等)。

[0093] C. 付款应用程序的 WCAp 管理

[0094] 如上文参考图 1 进一步详细地描述，将 WCAp(例如，图 1，WCAp 104) 注册为用于与手机钱包 103 相关的付款应用程序的 CREL 应用程序 (即，由中央 TSM(例如，图 1，中央 TSM 106) 安装或实例化的应用程序)。

[0095] 图 5 是根据示例性实施方案的 CRS 镜像 500 的图。CRS 镜像 500 是安全元件 (例如，图 1，安全元件 102) 上的 CRS 的拷贝或复制，且包括 CRS 的全部或部分应用程序信息。

[0096] 作为 CREL，WCAp 104 使用 CRS 镜像 500 跟踪和 / 或管理付款应用程序，CRS 镜像 500 包括用以跟踪和 / 或管理付款应用程序的信息。如图 5 中示出，CRS 镜像 500 包括关于某些类型的应用程序 (例如，由中央 TSM 106 安装或实例化的应用程序) 的信息。CRS 镜像 500 使用唯一对应的应用程序标识符 (AID) 跟踪和 / 或管理每个付款应用程序。图 5 包括用来跟踪识别为 AID-1 至 AID-6 的 6 个应用程序的信息。

[0097] 此外，作为 CREL 应用程序，WCAp104 接收关于 CRS 中与也由 CRS 镜像 500 跟踪的应用程序 (即，AID-1 至 AID-6) 有关的改变和 / 或更新的通知。这些通知可能是关于例如付款应用程序的激活。在接收这些通知时，WCAp104 更新 CRS 镜像 500 使得其信息匹配 CRS 中的信息。

[0098] CRS 镜像 500 还包括用于每个付款应用程序 (即，对应于每个 AID) 的信息，诸如 : CRS 状态 (即，激活或禁用) ;手机钱包选择 (即，是否经由例如选择命令来选择付款应用程序的指示) ;状态 (即，错误、没有错误、锁死) ;和 / 或速度计数器。图 5 包括对应于这些类型的信息中的每个的行。

[0099] 如 CRS 中指示，CRS 状态指示是否激活或禁用付款应用程序。

[0100] 当手机钱包将选择命令传输到 WCAp 并成功处理选择命令时，付款应用程序是“手机钱包选择”，且所述应用程序由于例如预定时间量截止而没有损失其选定状态。

[0101] CRS 镜像 500 中示出的付款应用程序的状态指示 CRS 状态栏与手机钱包选择栏之

间是否不匹配。例如，如果付款应用程序的 CRS 状态被列出为激活（即，应用程序在 CRS 中被列出为激活）且手机钱包选择栏是“是”，那么将状态设置为“没有错误”。替代地，如果付款应用程序的 CRS 状态被列出为禁用且手机钱包选择栏是“是”，那么将付款应用程序的状态列出为“错误”，指示 CRS 与 CRS 镜像不匹配。如果恶意应用程序试图使用付款应用程序或如果最初错误地激活付款应用程序，那么付款应用程序的状态还可以是“锁死”。

[0102] 速度计数器是限制可被执行和 / 或处理的交易的次数且不需要与移动装置上的手机钱包通信的安全机制。

[0103] 1. 选择和激活付款应用程序

[0104] 每个付款应用程序对应于和 / 或链接到可以被链接到付款工具（例如，信用卡）的账户（例如，信用卡账户）。图 6 是示出根据示例性实施方案的用于选择和激活主（即，默认）付款应用程序（即，链接到由手机钱包用来交易的主账户和 / 或付款工具）的程序 600 的次序图。图 6 中的步骤 650 至 660 示出了用于选择主付款应用程序的程序。

[0105] 在步骤 650（“选择”），手机钱包 601（例如，图 1，手机钱包 103）将选择命令传输到 WCAp 602（例如，图 1，WCAp 104），所述选择命令包括 CRS 镜像 602a（例如，图 5，CRS 镜像 500）。选择命令包括将选择的付款应用程序的 AID。WCAp 602 可以将指示是否成功处理选择命令或是否发生错误（例如，WCAp 锁定、未发现应用程序、链接到应用程序的账户挂起、AID 错误）的响应传输到手机钱包 601。

[0106] 然后，在步骤 652（“取得状态”），手机钱包 601 又将取得状态命令传输到 WCAp 602 以获得关于 WCAp 602 和其上安装 WCAp 602 的安全元件的信息。特定地说，WCAp 602 接收取得状态命令，且然后又从安全元件取回关于 WCAp 602 和安全元件上的其它付款应用程序的信息。这种信息包括（例如）安全元件上的应用程序的状态和 / 或设置。WCAp 602 然后可以将包括一些或全部取回的信息的响应传输到手机钱包 601。

[0107] 在步骤 654（“奇偶校验 / 验证密码”），手机钱包 601 将验证密码或奇偶校验命令传输到 WCAp 602，以认证 WCAp 602（即，将 WCAp602 置于认证状态），如上文参考图 3 和图 4 更加详细地讨论。WCAp602 可以将指示奇偶校验和 / 或密码验证是否成功的响应传输到手机钱包 601。即，特定地说，这个响应可以包括指示下列各项的信息：是否成功处理命令、命令数据中是否存在错误值、WCAp 是否不活动或仍未个人化，或密码验证或奇偶校验是否失败。

[0108] 如果成功处理验证密码和 / 或奇偶校验命令（即，WCAp 602 处于认证状态），那么手机钱包 601 然后又在步骤 656（“放置付款设置（选择主付款应用程序）”）将放置付款设置命令传输到 WCAp 602。放置付款设置命令可以用来启动交易和撤销交易，将付款置换 ON 和 OFF，且选择主付款应用程序。此外，当 WCAp 602 处于认证状态时，处理放置付款设置命令。

[0109] 步骤 656 传输的放置付款设置命令包括选择对应于包括在所述命令中的 AID 的应用程序作为主应用程序的指令。

[0110] 在替代实施方案中，选择主付款应用程序的放置付款设置命令可包括多个 AID，例如以选择多个付款应用程序作为主应用程序。

[0111] 在步骤 658（“设置 PPSE 参数”），WCAp 602 将设置 PPSE 参数命令传输到 PPSE 603。PPSE 参数包括：主付款 AID（即，主付款应用程序的 AID）、交易启动 / 撤销（即，是否可以处

理交易的指示符）和/或付款置换（即，移动装置是否有资格用于交易的指示符）。特定地说，在步骤658，设置PPSE参数命令包括AID和将对应于所述AID的应用程序设置为主付款应用程序的指令。

[0112] 在步骤660（“设置PPSE响应”），PPSE 603然后又处理设置PPSE响应命令。PPSE响应可以是错误、无效响应或正常响应。错误指示锁定密码、没有选择主应用程序和/或撤销（即，不启动）付款。无效响应指示付款置换是ON。正常响应指示选择主应用程序、付款置换是OFF，没有锁定密码且启动付款。正常响应还包括对应于一个或多个付款应用程序的信息（例如，AID、标签、优先级指示符），指示可以选择哪些应用程序来进行交易。PPSE 603可以将PPSE响应传输到其它系统，包括例如用于非接触式交易的非接触式读卡器。

[0113] 图6的次序图还示出了用于如步骤662至670示出般激活付款应用程序的程序。

[0114] 一旦选择主付款应用程序（即，步骤650至660），手机钱包601在步骤662（“选择”）将选择命令传输到CRS小应用程序604。CRS小应用程序604包括CRS且用来管理安全元件上的付款应用程序。CRS小应用程序604还用作Open 605的界面，如上文参考图1描述，其是安全元件的平台和/或环境。

[0115] 步骤662传输的选择命令包括将被选择的付款应用程序的AID。CRS小应用程序604可以将指示是否成功处理选择命令或是否发生错误的响应传输到手机钱包601。

[0116] 在步骤664（“设置状态（激活AID）”），手机钱包601然后又将设置状态命令传输到CRS小应用程序604，设置状态命令包括AID、状态（例如，激活、禁用）和设置对应于将要激活的AID的付款应用程序的指令。在步骤666（“更新CRS”），CRS小应用程序604然后又将更新CRS命令传输到Open 605，更新CRS命令包括更新CRS以反映已激活对应于AID的付款应用程序的数据（例如，AID、状态）。

[0117] 在步骤668（“激活CREL反馈”），Open 605将CREL反馈传输到WCAp 602，CREL反馈指示已发生CRS镜像602a中跟踪的付款应用程序的更新。CREL反馈还包括用于更新CRS镜像602a以匹配CRS的信息（例如，AID、状态）。

[0118] 然后WCAp 602又在步骤670（“允许激活？”）确定是否允许激活付款应用程序。例如，WCAp 602确定CREL反馈中的AID的状态是否匹配CRS镜像602a中的手机钱包选择栏，如上文参考图5描述。如果不存在失配，那么WCAp 602允许激活付款应用程序且将CRS镜像602a中的对应AID的CRS状态设置为已激活。替代地，如果存在失配，那么WCAp 602将拒绝激活付款应用程序，且将会在CRS镜像602a中将付款应用程序重设为禁用。

[0119] 在替代实施方案中，付款应用程序可以链接（即，关联）多个账户（例如，信用卡账户、支票账户）。在这种情况下，每个账户链接到对应于付款应用程序的唯一AID。结果，选择主应用程序包括选择主AID，其对应于账户和付款应用程序。

[0120] 2. 管理非接触式交易和付款应用程序

[0121] 图7是示出根据示例性实施方案的用于管理非接触式交易700的程序的次序图。

[0122] 非接触式交易（例如，付款）是使用链接到安装在移动装置（例如，图1，移动装置101）上的手机钱包的应用程序（诸如付款应用程序704）来执行。付款应用程序还链接到账户（例如，支票账户）。

[0123] 通过将装有CLF 702的移动装置放置在PoS处的非接触式读卡器701的预定距离内来启用诸如非接触式交易700的交易。在步骤750（“14443通信Est”），在移动装置中

的 CLF 702 与 PoS 处的非接触式读卡器 701 之间建立 ISO 14443 通信（即，使用 NFC ISO 14443 协议）。然后，在步骤 752（“射频 ON”），CLF 702 又将 WCAp 706 的射频连转换为 ON 状态。

[0124] 在步骤 754（“选择 PPSE”），非接触式读卡器 701 将选择 PPSE 命令传输到 Open 703 以选择 PPSE 705。选择 PPSE 命令包括 PPSE 705 的 AID。在步骤 756（“激活 AID”），Open 703 然后又通过将所述命令中接收的 AID（即，PPSE 705 的 AID）的状态设置为已激活来激活 PPSE 705。将 AID 的状态设置为已激活包括用 AID 的状态更新 CRS。

[0125] 如果没有成功激活 PPSE 705，那么 Open 703 在步骤 758（“错误（如果没有激活 AID）”）将错误消息传输到非接触式读卡器 701。替代地，在步骤 760（“选择 PPSE（如果激活 AID）”），Open 703 将选择命令传输到 PPSE 705，所述选择命令包括 PPSE 705 的 AID。然后在步骤 762（“估算”），PPSE 705 执行估算以确定安全元件上的付款应用程序的状态（即，是否选择主付款应用程序、付款置换是否是 ON 或 OFF、是否锁定或解锁密码和 / 或是否启动或撤销付款）。

[0126] 在步骤 764（“PPSE 响应”），PPSE 705 将基于步骤 762 执行的估算的响应传输到非接触式读卡器 701。响应可以是错误、无效响应或正常响应。错误指示锁定密码、没有选择主应用程序和 / 或撤销（即，不启动）付款。无效响应指示付款置换是 ON。正常响应指示选择主应用程序、付款置换是 OFF，没有锁定密码且启动付款。正常响应还包括对应于一个或多个付款应用程序的信息（例如，AID、标签、优先级指示符），指示可以选择哪些应用程序来进行交易。

[0127] 在步骤 766（“选择付款应用程序”），非接触式读卡器 701 将选择命令传输到 Open 703，所述选择命令包括在交易中使用的付款应用程序（即，付款应用程序 704）的 AID。然后在步骤 768（“激活 AID”），Open 703 通过将对应于步骤 766 传输的 AID 的状态设置为已激活来激活付款应用程序。这可以例如通过改变 CRS 中的 AID 的状态而进行。

[0128] 如果没有成功激活付款应用程序，那么 Open 703 在步骤 770（“错误（如果没有激活 AID）”）将错误消息传输到非接触式读卡器 701。替代地，在步骤 772（“选择付款应用程序（如果激活 AID）”），Open703 将选择命令传输到付款应用程序 704，所述选择命令对应于包括在步骤 766 中传输的选择命令中的 AID。

[0129] 在步骤 774（“付款命令”），可以在非接触式读卡器 701 与付款应用程序 704 之间传输付款命令以执行非接触式交易。付款命令可以是根据 EMV（即 Europay、MasterCard®、Visa®）、ISO 7816 或 ISO 144443 标准传输的 APDU 命令，以完成付款交易。这些命令包括例如获得处理选项、外部认证、读取记录、计算密码等等。

[0130] 在步骤 776（“交易事件”），付款应用程序 704 将交易事件传输到 CLF 702。交易事件对手机钱包提供指示诸如非接触式付款的交易已完成的信息。

[0131] 然后，在步骤 778（“交易事件”），CLF 702 将交易事件传输到装在移动装置中的手机钱包 707。结果，手机钱包 707 接收由付款应用程序 704 产生的信息，指示交易已完成。

[0132] D. 手机钱包与服务器之间的相互认证

[0133] 图 8 是示出包括 WCAp 802（例如，图 1，WCAp 104）的手机钱包 801（例如，图 1，手机钱包 103）与服务器 805（例如，，图 1，服务器 105）之间的相互认证程序 800 的次序图。

[0134] 在步骤 850（“生成 WS 出票命令”），手机钱包 801 将生成 WS 出票命令传输到 WCAp

802。如上文参考表格 2 讨论，当 WCAp 处于认证状态时，由 WCAp 处理生成 WS 出票命令。

[0135] 然后，WCAp 802 又在步骤 852（“生成出票 ID 和出票令牌”）生成出票 ID 和出票令牌。出票 ID 是由 WCAp 802 维持的 8 位永久计数器。出票令牌是由与 WCAp 802 相关的安全元件生成的一次性 8 位随机标识符，且是针对每个生成 WS 出票命令而唯一地生成。在步骤 854（“计算出票”），WCAp 802 通过例如以密文块链式模式使用存储在 WCAp 802 中的钱包服务器密钥（上文参考表格 1 进一步详细地描述）和三重数据加密算法 (TDEA)（即，，对每个数据块应用三次数据加密标准 (DES) 密文算法）加密出票 ID 和出票令牌。

[0136] WCAp 802 在步骤 856（“出票响应”）将出票响应传输到手机钱包 801，所述出票响应包括步骤 852 和 854 生成的出票 ID、出票令牌和出票。替代地，出票响应可以包括错误，其指示不满足安全条件、没有加载和 / 或发现钱包服务器密钥和 / 或 WCAp 不活动和 / 或未被个人化。

[0137] 在步骤 858（“传输出票 ID、出票令牌、出票、钱包 ID”），手机钱包 801 将出票 ID、出票令牌和出票连同钱包 ID 一起传输到服务器 803。然后在步骤 860（“获得服务器认证密钥”），服务器 803 将包括钱包 ID 的请求传输到身份管理 (IDM) 系统 804 以获得服务器认证密钥，其应匹配用来在步骤 854 加密出票的钱包服务器密钥。IDM 804 是包括在服务器 803 中或耦接到服务器 803 的系统和 / 或应用程序，且用来管理认证、授权和 / 或系统内或跨系统的特权。

[0138] 作为响应，在步骤 862（生成服务器认证密钥），IDM 804 生成用于所接收的钱包 ID 的服务器认证密钥，且在步骤 864（“传输服务器认证密钥“）将其传输到服务器 803。

[0139] 然后在步骤 866（“解密出票“），服务器 803 解密在步骤 858 接收的出票。一旦解密，在步骤 868（”验证出票 ID 和出票令牌“）由服务器 803 验证用来加密出票的出票 ID 和出票令牌。服务器 803 然后在步骤 870（”生成会话令牌“）生成会话令牌。

[0140] 在步骤 872（“回修授权”），服务器 803 通过以密文块链式模式使用 TDEA 加密出票令牌和会话令牌来生成回修授权。然后在步骤 874（“传输会话令牌和回修授权”），服务器 803 将会话令牌和回修授权传输到手机钱包 801。

[0141] 手机钱包 801 在步骤 876（“验证 WS 命令“）将验证 WS 命令（上文参考表格 2 进一步详细地描述）传输到 WCAp 802。通常，验证 WS 命令用来验证手机钱包与所期服务器建立连接。当 WCAp 处于认证状态时，由 WCAp 处理验证 WS 命令。验证 WS 命令包括会话令牌和回修授权。WCAp 802 在步骤 878（”解密回修授权“）解密回修授权。一旦解密，在步骤 880（”验证会话令牌和出票令牌“）由 WCAp802 验证用来加密回修授权的会话令牌和出票令牌。

[0142] （发明者 :请解释如何实现回修授权的这种验证）。

[0143] 在步骤 882（“响应“），WCAp 802 将响应传输到手机钱包 801。所述响应包括指示是否验证服务器（即，认证是否成功）或是否发生错误的信息。错误指示不满足安全条件、命令试图颠倒次序、WCAp 没有被个人化和 / 或不活动、命令包括错误数据和 / 或服务器的认证失败。

[0144] G. 额外示例性实施方案

[0145] 本发明（例如，系统 100、生命周期 200 至 300、图 500、程序 600 至 800 或其任何部分或功能）可使用硬件、软件或其组合而实施，且可实施于一个或多个移动装置或其它处

理系统中。就在人为操作方面参照由本发明执行的操控来说，在大部分情况下本文描述的形成本发明的部分的任何操作无需或不希望人操作者的这种能力。实情是，本文描述的操作是机器操作。用于执行本发明的操作的有用的机器包括移动电话、智能手机、个人数字助手 (PDA) 或类似装置。

[0146] 在一个实施方案中，本发明是针对能够实行本文描述的功能的一个或多个系统。图 9 中示出了系统 900 的实例。

[0147] 系统 900 包括一个或多个处理器，诸如处理器 901。处理器 901 耦接到通信基础设施 902（例如，通信总线、网络）。已就这个示例性系统描述了各个实施方案。在阅读这个说明之后，本领域一般技术人员应明白如何使用其它系统和 / 或结构实施本发明。

[0148] 系统 900 还包括主存储器 903，其可以是非易失性存储器等等。

[0149] 系统 900 还包括用于接收诸如命令的数据的接收模块 904。上文参考图 3 至图 8 进一步详细讨论接收请求。

[0150] 系统 900 还包括用于验证、认证和 / 或比较如上文参考图 3 至图 8 进一步详细讨论的数据的确定模块 905。

[0151] 系统 900 还包括启动如上文参考图 3 至图 8 进一步详细讨论的命令或操作的启动模块 906。

[0152] 系统 900 还包括用于处理如上文参考图 3 至图 8 进一步详细讨论的命令的处理模块 907。

[0153] 可以使用硬件、软件或所述两者的组合实施模块 904 至 907 中的每个。

[0154] 可以通过使用硬件、软件或所述两者的组合实施上文描述的示例性实施方案，诸如（例如）结合图 1 至图 8 描绘或讨论的系统和程序。所述实施可以在一个或多个计算机或其它处理系统中进行。虽然可能已就与由人操作者执行的心理操作共同相关联参照了由这些示例性实施方案执行的操控，但是执行本文描述的任何操作无需人操作者。换句话来说，可以使用机器操作完全实施所述操作。用于执行本文呈现的示例性实施方案的操作的有用的机器包括通用数字计算机或类似装置。

[0155] 部分的本发明的示例实施例可方便地使用一个通用计算机、专用数字计算机和 / 或微处理器编程根据本发明的教导、技术人员显而易见的计算机领域中。适合的软件代码可以很容易地制得熟练程序员基于本发明的教导。

[0156] 还可以通过准备专用集成电路、现场可编程门阵列或通过互连常规的组件电路的适当网络来实施一些实施方案。

[0157] 一些实施方案包括计算机程序产品。计算机程序产品可以是具有在其上或其中存储的可用来控制或使计算机执行本发明的示例性实施方案的任何程序的指令的非暂时存储介质。存储介质可以包括（不限于）软盘、微型光盘、光碟、蓝光光碟、DVD、CD 或 CD-ROM、微型驱动、磁光盘、ROM、RAM、EPROM、EEPROM、DRAM、VRAM、快闪存储器、闪卡、磁卡、光学卡片、纳米系统、分子存储器集成电路、RAID、远程数据存储装置 / 档案馆 / 仓库和 / 或适用于存储指令和 / 或数据的任何其它类型的装置。

[0158] 一些实施方式包括存储在非暂时计算机可读介质中的任何一个上的下列各项：用于控制通用和 / 或专用计算机或微处理器的硬件和用于使计算机或微处理器能够利用本发明的示例性实施方案的结果与人类用户或其它机构交互的软件。这种软件可以包括（不

限于）装置驱动器、操作系统和用户小应用程序。最终，这样的计算机可读介质还包括用于如上文描述般执行本发明的示例性方面的软件。

[0159] 在通用和/或专用计算机或微处理器的程序设计和/或软件中包括用于实施上文描述的程序的软件模块。

[0160] 应了解，系统900中的装置之间的通信可以包括与或通过介入系统、硬件和/或软件进行的通信。

[0161] 虽然上文已描述了本发明的各个示例性实施方案，但是应了解其是通过举例的方式（且无限制）来呈现。本领域一般技术人员应明白，其中可对形式和细节做出各种改变。因此，本公开内容不应受限于任何上文描述的示例性实施方案，但是应只根据以下权利要求和其等效物而定义。

[0162] 此外，应了解只出于示例性目的而呈现所述附图。本文呈现的示例性实施方案的结构足够灵活且可配置，使得可以按除了附图中示出的方式以外的方式利用并操纵所述结构。

[0163] 此外，摘要的目的是使美国专利与商标局和公众人物（一般且尤其是不熟悉专利或法律术语或措词的科学家、工程师和执业者）能够通过粗略的检查快速确定本申请的技术公开内容的本质和实质。摘要不旨在以任何方式限于本文呈现的示例性实施方案的范围。还应了解无需按所呈现的顺序执行权利要求中叙述的程序。

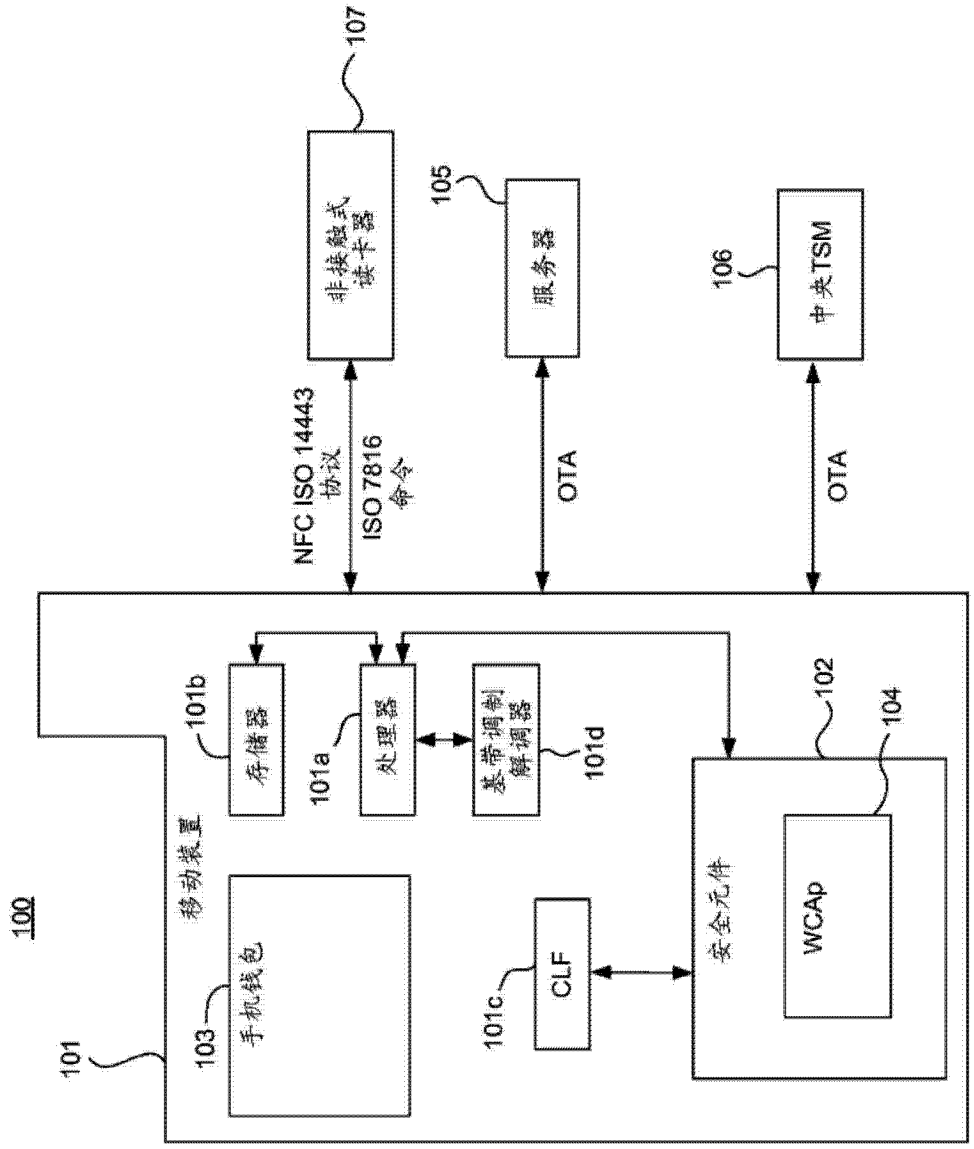

107
非接触式读卡器
105
服务器
106
中央TSM
NFC ISO 14443 协议
ISO 7816 命令
OTA
OTA
100
移动装置
101
101b
存储器
101a
处理器
基带调制解调器
101d
102
104
安全元件
WCAp
103
手机钱包
101c
CLF

图 1

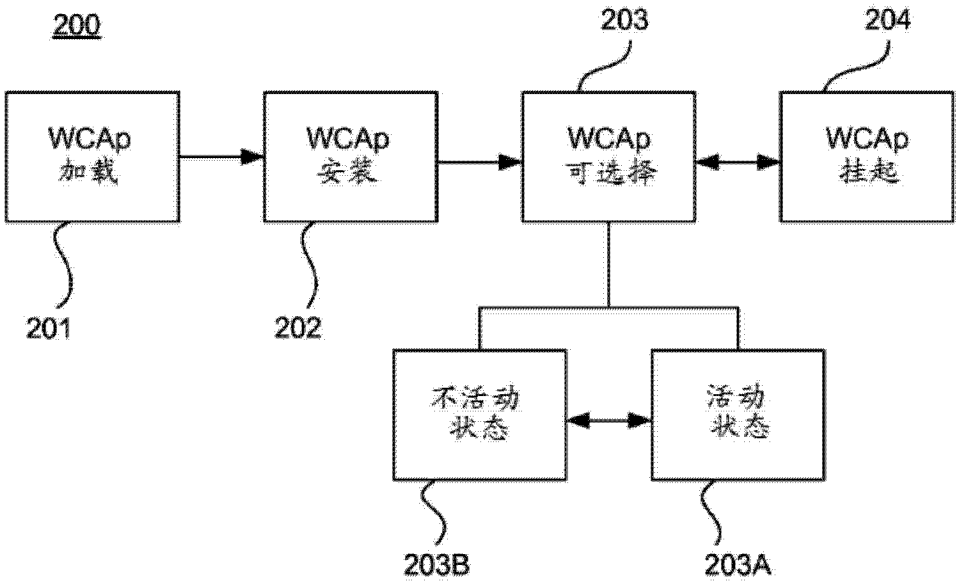

200
203
204
WCAp
加载
WCAp
安装
WCAp
可选择
WCAp
挂起
201
202
不活动
状态
活动
状态
203B
203A

图 2

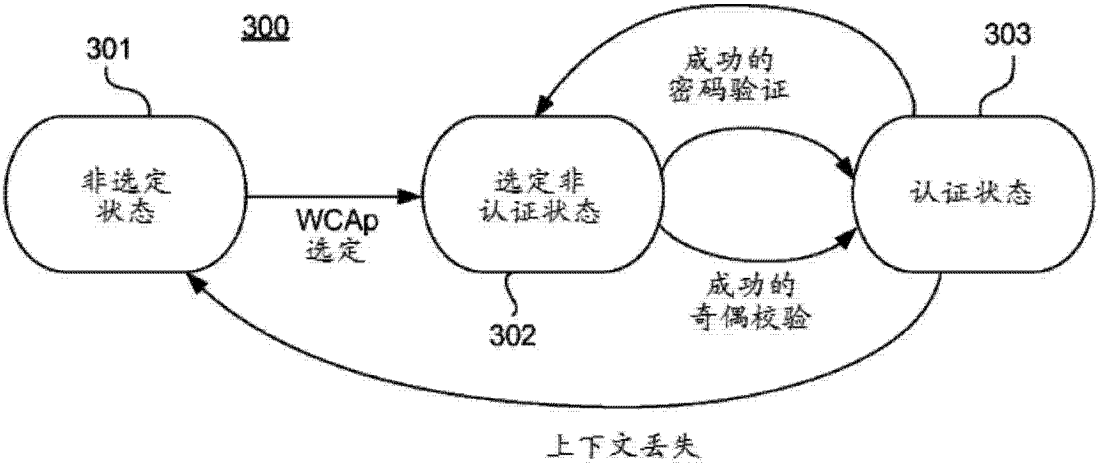

300
301
303
成功的
密码验证
非选定
状态
WCAp
选定
选定非
认证状态
认证状态
成功的
奇偶校验
302
上下文丢失

图 3

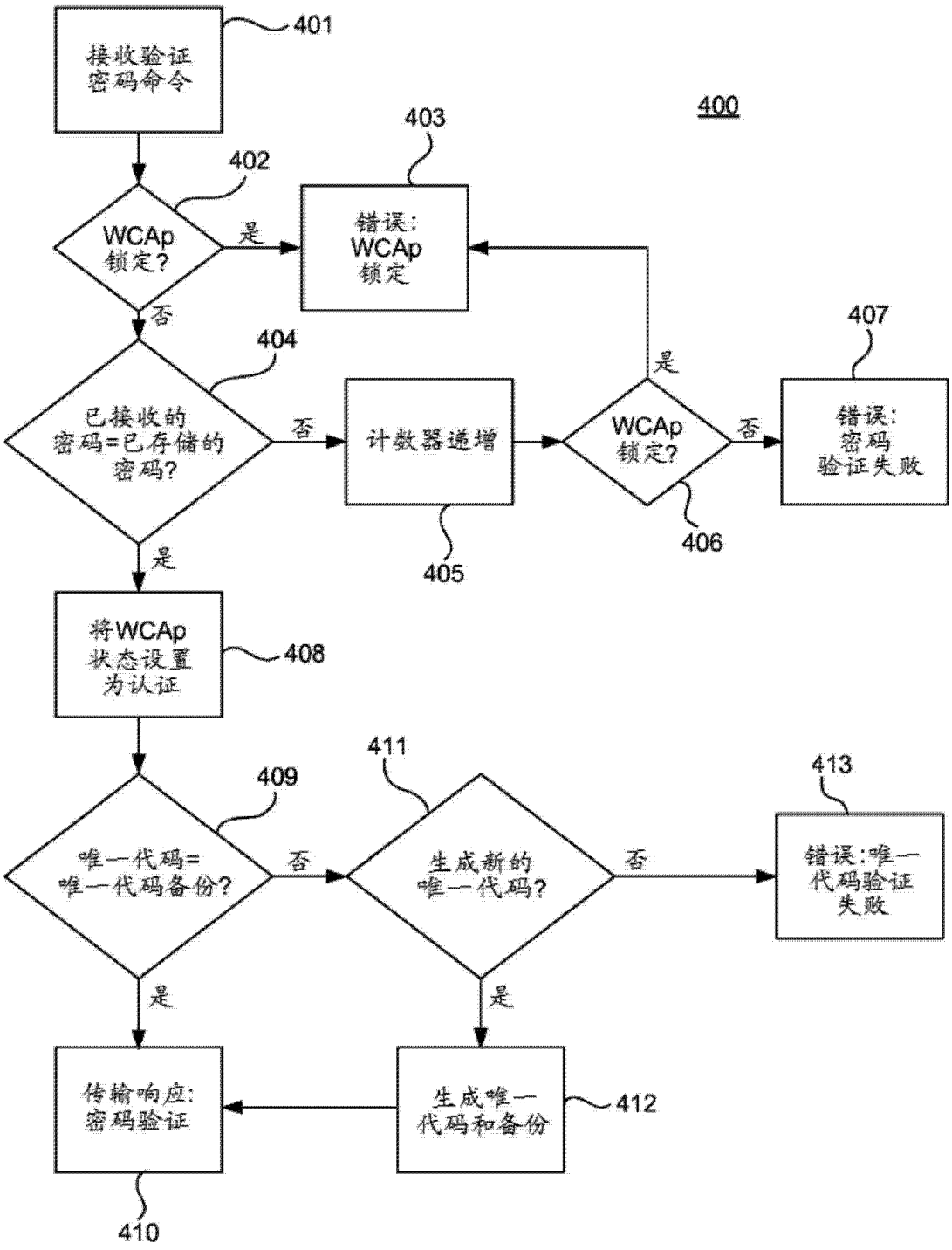

400
接收验证密码命令
401
WCAp锁定?
402
是
错误:WCAp锁定
403
否
已接收的密码=已存储的密码?
404
否
计数器递增
405
WCAp锁定?
406
是
否
错误:密码验证失败
407
是
将WCAp状态设置为认证
408
唯一代码=唯一代码备份?
409
否
生成新的唯一代码?
411
否
错误:唯一代码验证失败
413
是
是
传输响应:密码验证
410
生成唯一代码和备份
412

图 4

500

AID	CRS状态	手机钱包选定?	状态	速度计数器
AID-1	激活	是	无错误	0
AID-2	激活	是	无错误	0
AID-3	激活	否	错误	1
AID-4	激活	否	错误	2
AID-5	禁用	否	无错误	2
AID-6	禁用	否	无错误	2

图 5

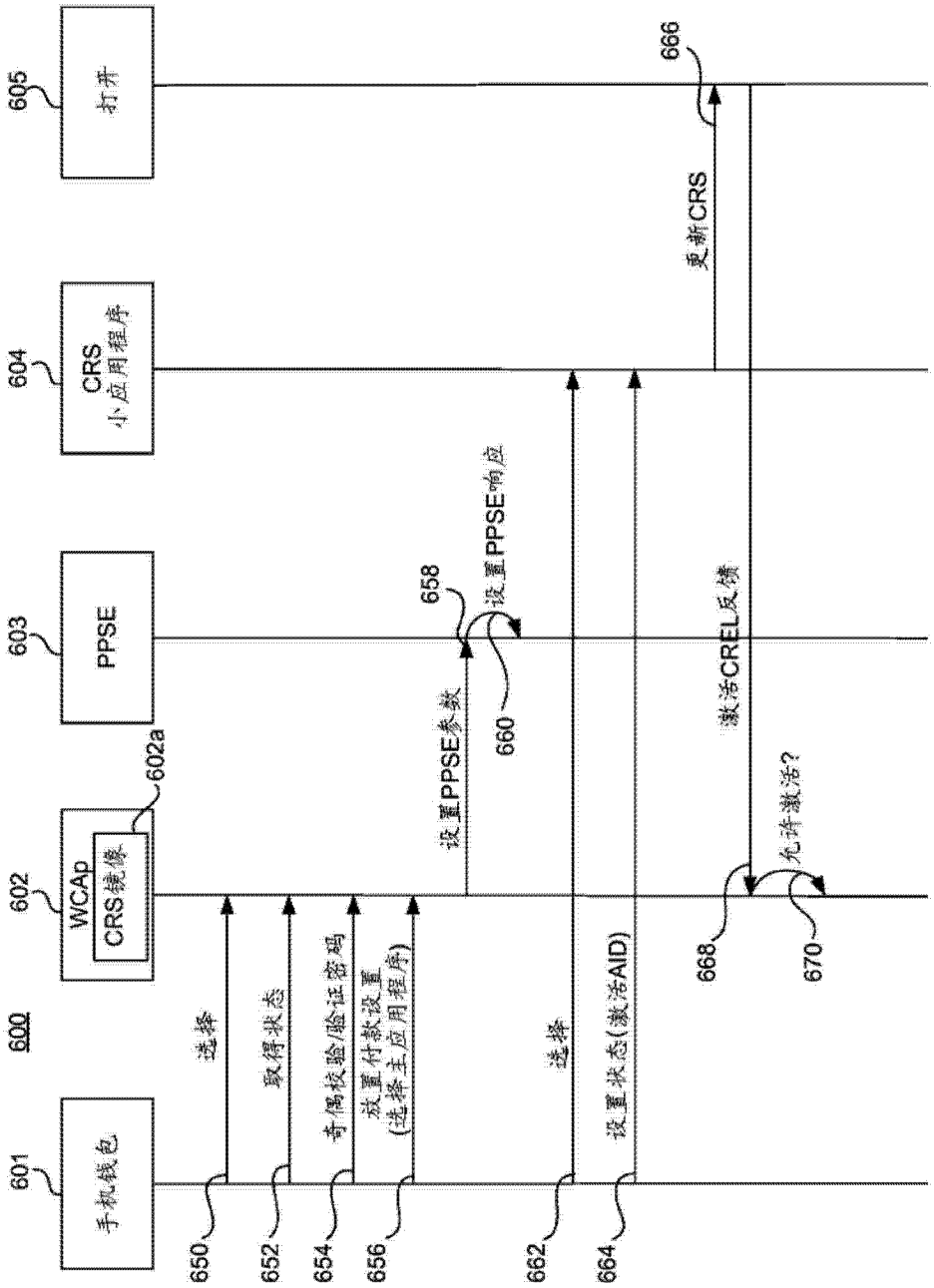

600
601
手机钱包
602
WCAp
602a
CRS镜像
603
PPSE
604
CRS
小应用程序
605
打开
选择
取得状态
奇/偶校验/验证密码
放置付款设置
(选择主应用程序)
设置PPSE参数
658
设置PPSE响应
660
选择
设置状态(激活AID)
更新CRS
666
激活CREL反馈
允许激活?
668
670
650
652
654
656
662
664

图 6

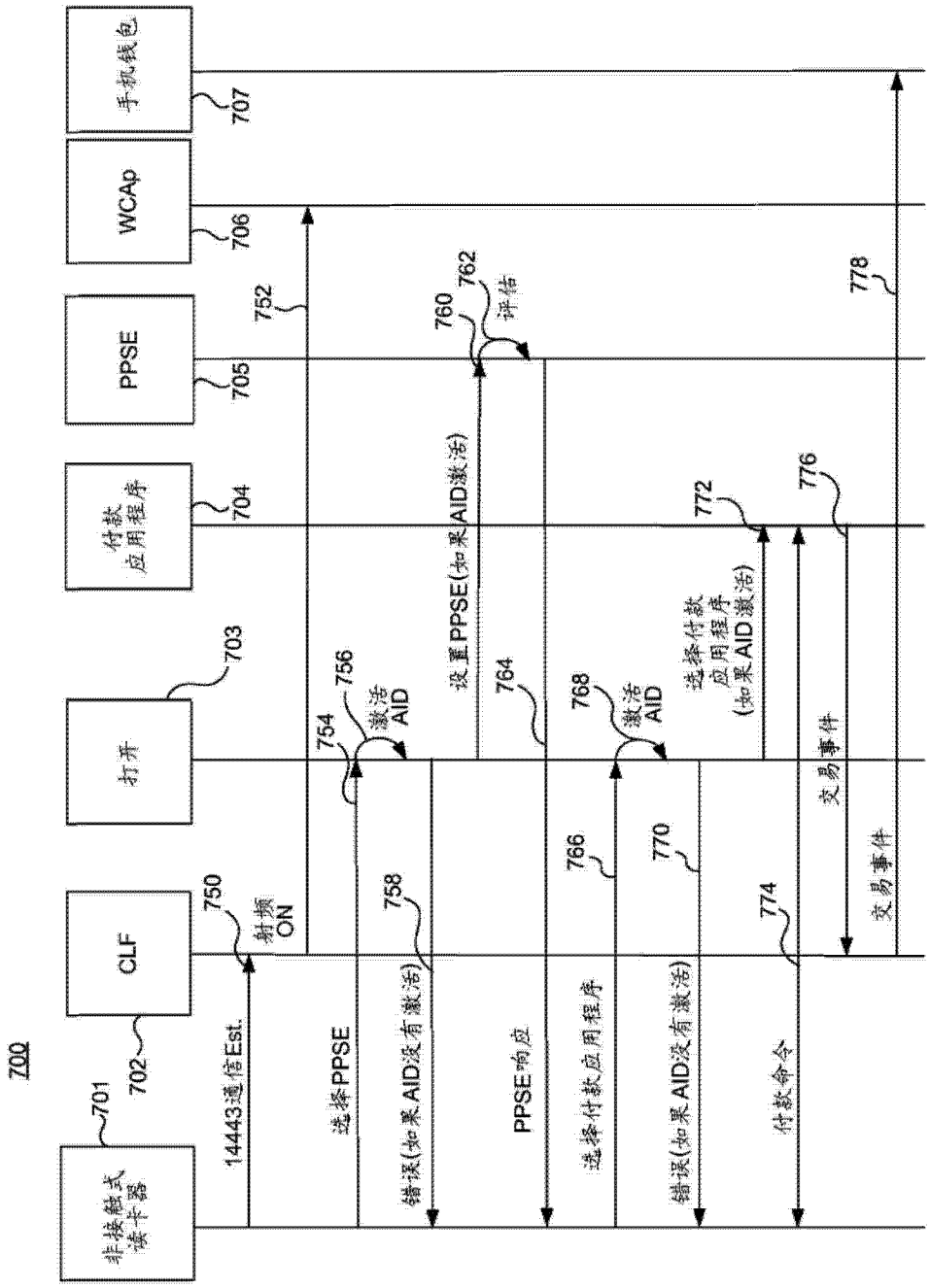

700
非接触式读卡器
701
CLF
702
打开
703
付款应用程序
704
PPSE
705
WCAp
706
手机钱包
707
14443通信Est.
射频ON
750
选择PPSE
752
错误(如果AID没有激活)
754
激活AID
756
758
PPSE响应
760
设置PPSE(如果AID激活)
762
评估
764
选择付款应用程序
766
激活AID
768
错误(如果AID没有激活)
770
选择付款应用程序(如果AID激活)
772
付款命令
774
交易事件
776
交易事件
778

图 7

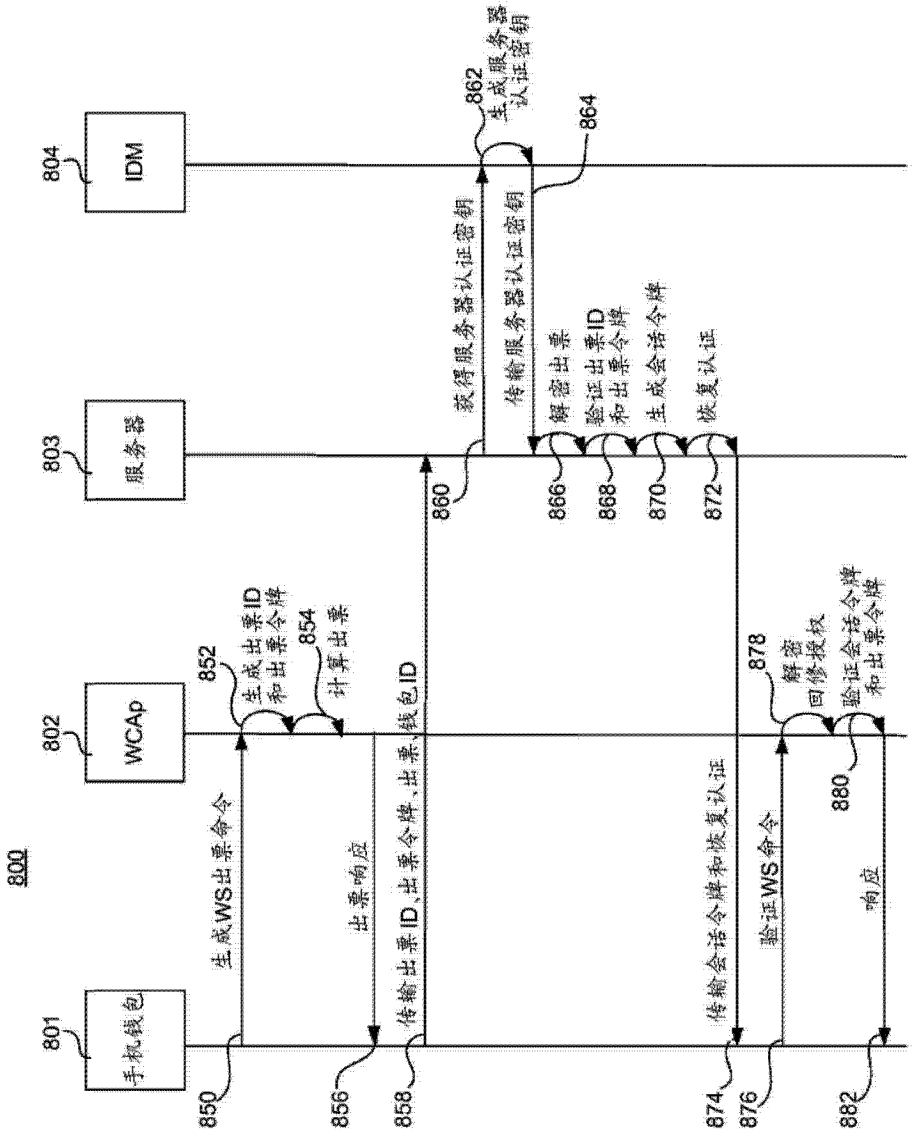

800
801
手机钱包
802
WCAp
803
服务器
804
IDM
生成WS出票命令
850
生成出票ID和出票令牌
852
计算出票
854
出票响应
856
传输出票ID、出票令牌、出票、钱包ID
858
获得服务器认证密钥
860
生成服务器认证密钥
862
传输服务器认证密钥
864
解密出票
866
验证出票ID和出票令牌
868
生成会话令牌
870
恢复认证
872
传输会话令牌和恢复认证
874
验证WS命令
876
解密回修授权
878
验证会话令牌和出票令牌
880
响应
882

图 8

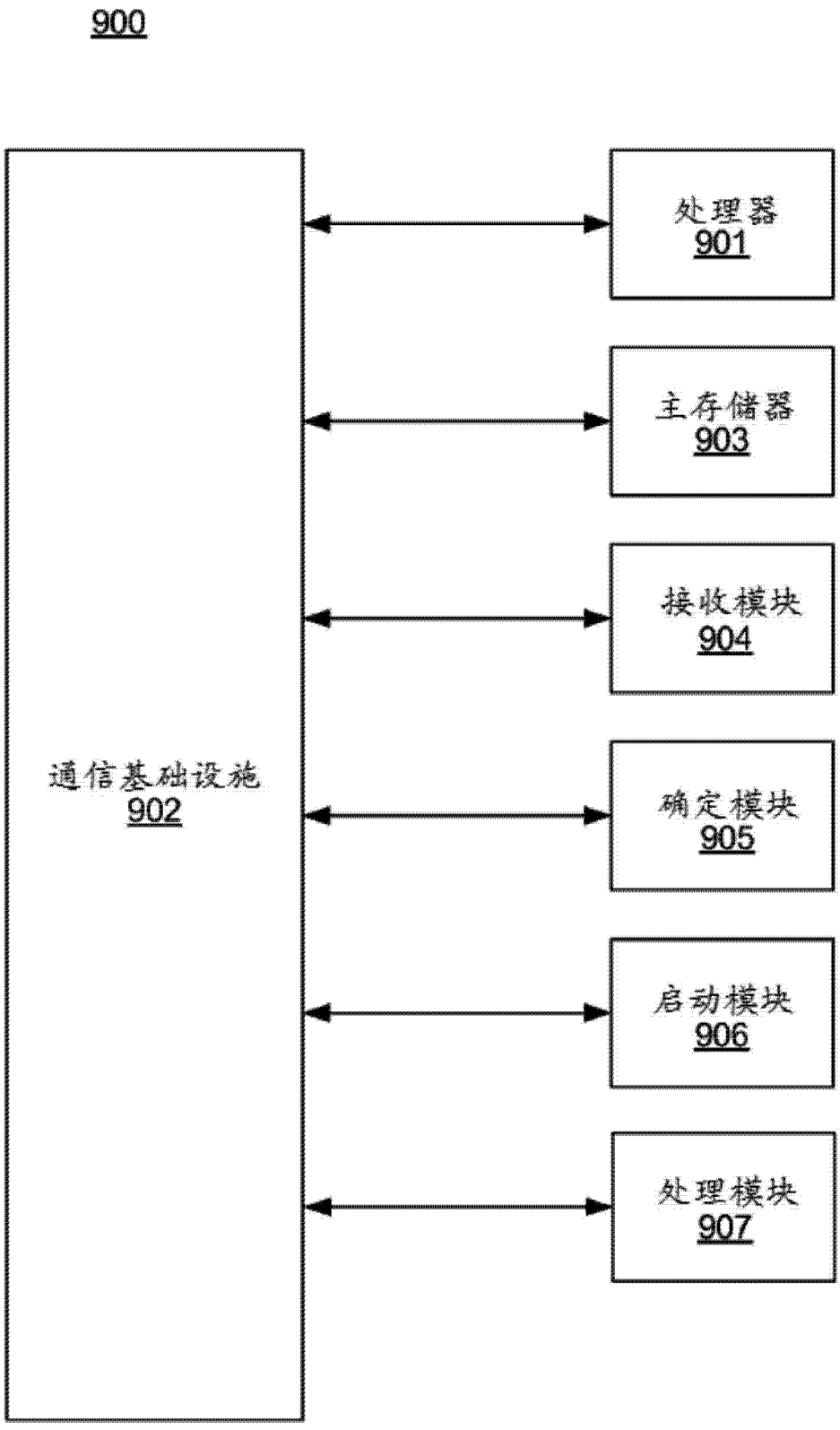

900
通信基础设施
902
处理器
901
主存储器
903
接收模块
904
确定模块
905
启动模块
906
处理模块
907

图 9