(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 106031207 A
(43)申请公布日 2016.10.12

(21)申请号 201480074680.X

(22)申请日 2014.12.02

(30)优先权数据
61/910,819 2013.12.02 US
61/951,842 2014.03.12 US
61/955,716 2014.03.19 US
61/979,113 2014.04.14 US
61/979,132 2014.04.14 US
61/979,122 2014.04.14 US
61/980,784 2014.04.17 US
61/996,665 2014.05.14 US

(85)PCT国际申请进入国家阶段日
2016.08.01

(86)PCT国际申请的申请数据
PCT/US2014/068078 2014.12.02

(87)PCT国际申请的公布数据
WO2015/084797 EN 2015.06.11

(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 迈赫迪·克林格
迈克尔·克里斯多夫·沃德
帕特里克·斯梅茨
阿克塞尔·埃米尔·珍·查尔斯·卡特兰德
克里斯蒂安·拉杜

(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

(51)Int.Cl.
H04W 12/08(2006.01)
H04W 12/06(2006.01)

权利要求书3页 说明书23页 附图18页

(54)发明名称

用于向不带有安全元件的移动设备安全传送远程通知服务消息的方法及系统

(57)摘要

一种用于接收和处理数据消息的方法，包括：至少存储加密密钥；接收数据消息，其中数据消息至少包括经加密的消息和消息认证码，至少利用经加密的消息的一部分来生成消息认证码；至少利用包括在接收的数据消息中的经加密的消息的一部分来生成参考认证码；基于比对生成的参考认证码来检查包括在接收的数据消息中的消息认证码，来对接收的数据消息进行验证；以及，利用存储的加密密钥对包括在接收的数据消息中的经加密的消息进行解密，以得到经解密的消息。

CN 106031207 A

1.一种用于接收和处理数据消息的方法,包括:

在存储器中至少存储加密密钥;

由接收设备接收数据消息,其中所述数据消息至少包括经加密的消息和消息认证码,其中至少利用所述经加密的消息的一部分来生成所述消息认证码;

由处理设备至少利用包括在接收的所述数据消息中的经加密的消息的一部分来生成参考认证码;

由所述处理设备基于比对生成的所述参考认证码来检查包括在接收的所述数据消息中的消息认证码,来对接收的所述数据消息进行验证;

由所述处理设备利用存储的所述加密密钥对包括在接收的所述数据消息中的所述经加密的消息进行解密,以得到经解密的消息。

2.根据权利要求1所述的方法,其中,所述数据消息为经由远程通知服务接收的远程通知服务消息。

3.根据权利要求1所述的方法,其中

所述存储器还被配置为存储参考计数,并且

对接收的数据消息进行验证的步骤还包括:比对存储的所述参考计数来对包括在接收的所述数据消息中的消息计数进行检查。

4.根据权利要求1所述的方法,还包括:

响应于接收的所述数据消息,由传送设备传送接收通知。

5.根据权利要求4所述的方法,其中

所述方法还包括:

由所述处理设备基于所述经解密的消息来执行一个或多个动作;

由所述处理设备由于或基于执行的所述一个或多个动作来生成返回消息;

由所述处理设备利用存储的所述加密密钥来对生成的所述返回消息进行加密,以得到经加密的返回消息;以及

由所述处理设备至少利用所述经加密的返回消息的一部分来生成返回认证码,其中

所传送的所述接收通知包括所述经加密的返回消息和所述返回认证码。

6.根据权利要求5所述的方法,其中

所述存储器还包括返回计数,并且

所传送的所述接收通知还包括所述返回计数。

7.根据权利要求1所述的方法,其中

所述存储器还包括一个或多个认证码生成规则,并且

基于将存储的所述一个或多个认证码生成规则应用于包括在接收的所述数据消息中的所述经加密的消息的一部分上,来生成所述参考认证码。

8.根据权利要求1所述的方法,还包括:

由所述处理设备利用填充密钥对包括在接收的所述远程通知服务消息中的所述经加密的消息进行填充,其中

所述经加密的消息中用于生成所述参考认证码的那一部分为经过填充的经加密的消息。

9.根据权利要求8所述的方法,其中,所述填充密钥为所述加密密钥。

10.根据权利要求8所述的方法，其中，

所述存储器还包括认证码填充算法，并且

利用所述填充密钥对所述经加密的消息进行填充的步骤包括：基于将所述填充密钥应用于所述认证码填充算法，来对所述经加密的消息进行填充。

11.根据权利要求1所述的方法，还包括：

由所述处理设备基于一个或多个数据格式规则来检查所述经解密的消息的数据形式。

12.根据权利要求1所述的方法，其中，所述经解密的消息包括以下各项中的至少一项：在支付交易中使用的数字化卡片文件和一次性密钥。

13.根据权利要求1所述的方法，其中，还利用存储的所述加密密钥来生成所述参考认证码。

14.根据权利要求1所述的方法，其中，所述存储器为移动通信设备中的非安全元件型存储器。

15.一种用于接收和处理数据消息的系统，包括：

存储器，其被配置为至少存储加密密钥；

接收设备，其被配置为接收数据消息，其中所述数据消息至少包括经加密的消息和消息认证码，所述消息认证码至少利用所述经加密的消息的一部分来生成；

处理设备，其被配置为：

至少利用包括在接收的所述数据消息中的经加密的消息的一部分来生成参考认证码；

基于比对生成的所述参考认证码来检查包括在接收的所述数据消息中的消息认证码，来对接收的所述数据消息进行验证；

利用存储的所述加密密钥对包括在接收的所述数据消息中的所述经加密的消息进行解密，以得到经解密的消息。

16.根据权利要求15所述的系统，其中，所述数据消息为经由远程通知服务接收的远程通知服务消息。

17.根据权利要求15所述的系统，其中

所述存储器还被配置为存储参考计数，并且

对接收的数据消息进行验证的步骤还包括：比对存储的所述参考计数来对包括在接收的所述数据消息中的消息计数进行检查。

18.根据权利要求15所述的系统，还包括：

传送设备，其被配置为响应于接收的所述数据消息而传送接收通知。

19.根据权利要求18所述的系统，其中

所述处理设备还被配置为：

基于所述经解密的消息来执行一个或多个动作；

由于或基于执行的所述一个或多个动作来生成返回消息；

利用存储的所述加密密钥来对生成的所述返回消息进行加密，以得到经加密的返回消息；以及

至少利用所述经加密的返回消息的一部分来生成返回认证码，并且

所传送的所述接收通知包括所述经加密的返回消息、返回计数和所述返回认证码。

20.根据权利要求19所述的系统，其中

所述存储器还包括返回计数，并且

所传送的所述接收通知还包括所述返回计数。

21.根据权利要求15所述的系统，其中

所述存储器还包括一个或多个认证码生成规则，并且

所述参考认证码是基于将存储的所述一个或多个认证码生成规则应用于包括在接收的所述数据消息中的经加密的消息的一部分上来生成的。

22.根据权利要求15所述的系统，其中

所述处理设备还被配置为利用填充密钥对包括在接收的所述远程通知服务消息中的所述经加密的消息进行填充，并且

所述经加密的消息中用于生成所述参考认证码的那一部分为经过填充的经加密的消息。

23.根据权利要求22所述的系统，其中，所述填充密钥为所述加密密钥。

24.根据权利要求22所述的系统，其中，

所述存储器还包括认证码填充算法，并且

利用所述填充密钥对所述经加密的消息进行填充的步骤包括：基于将所述填充密钥应用于所述认证码填充算法，来对所述经加密的消息进行填充。

25.根据权利要求15所述的系统，其中，所述处理设备还被配置为基于一个或多个数据格式规则来检查所述经解密的消息的数据形式。

26.根据权利要求15所述的系统，其中，所述经解密的消息包括以下各项中的至少一项：在支付交易中使用的数字化卡片文件和一次性密钥。

27.根据权利要求15所述的系统，其中，所述参考认证码还利用存储的所述加密密钥来生成。

28.根据权利要求15所述的系统，其中，所述存储器为移动通信设备中的非安全元件型存储器。

用于向不带有安全元件的移动设备安全传送远程通知服务消息的方法及系统

[0001] 相关申请的交叉引用

[0002] 根据美国法典第35卷119(e),本申请要求享有:于2014年4月14日提交的在先美国临时专利申请No.61/979,113;于2013年12月2日提交的美国临时专利申请No.61/910,819;于2014年3月12日提交的美国临时专利申请No.61/951,842;于2014年3月19日提交的美国临时专利申请No.61/955,716;于2014年4月14日提交的美国临时专利申请No.61/979,132;以及于2014年4月17日提交的美国临时专利申请No.61/980,784;以及,特别是于2014年4月14日提交的美国临时专利申请No.61/979,122和于2014年5月14日提交的美国临时专利申请No.61/996,665的权益,其中每件申请的全部内容均通过引用并入本文。

技术领域

[0003] 本公开涉及向无需安全元件的移动设备传送远程通知服务消息,更具体地涉及在不使用安全元件的情况下利用加密代码和认证代码来安全地传送、接收并处理远程通知服务消息。

背景技术

[0004] 移动和通信技术的进步已经创造了巨大的机会,其中的一个机会是为移动计算设备的用户提供使用他们的移动设备来发起并支付支付交易的能力。能够在移动设备上进行此种操作的一种这样的方法是使用近场通信(NFC)技术来安全地将支付明细从移动设备发送给附近的非接触式销售点(POS)终端。为了实现此目的,使用带有安全元件硬件(例如安全元件(SE)芯片)的移动电话来安全地存储支付凭证。安全元件是那些可包括在一些具备NFC功能的设备中的、作为可安全管理应用程序及其机密数据的防入侵性平台的专用件。

[0005] 然而,并不是所有的移动设备都具有安全元件。此外,即使移动设备装备有这样的元件,一些金融机构也可能无法访问移动设备上的安全元件。因此,许多配有具有用于进行非接触式或其它类型的远程支付交易时所需的硬件的移动设备的消费者实际上可能无法利用这种能力。因为此类问题,所以就需要一种在不使用安全元件的情况下能使移动计算设备发起并进行支付交易的技术方案。

[0006] 在由Mehdi Collinge等人于2013年3月14日提交的题为"通过向不带有安全元件的移动设备提供凭证来处理移动支付的系统及方法"的美国专利申请No.13/827,042中可以找到一些使用缺少安全元件的移动设备、或对装配在移动设备中的安全元件不加使用地进行支付交易的方法及系统,该申请的全部内容通过引用并入本文。虽然这样的方法及系统可适于在不使用安全元件的情况下经由移动设备来进行支付交易,但是许多消费者、商家和金融机构可能会提防参与这种交易,这是因为他们对安全性的要求更高。

[0007] 因此,需要一种能够为在缺少安全元件的移动设备中进行的支付凭证的接收和存储提供更高安全性,并能够为金融交易进行期间将支付凭证从移动设备发送给销售点的传输提供更高安全性的技术方案。提高这些过程的安全性可使得所有参与实体的心境更平

静，这可导致利用移动设备来进行非接触式或远程支付交易的增加，从而可向消费者提供比传统支付方法更多的好处。

发明内容

[0008] 本公开提供了用于处理远程通知服务消息的系统及方法的描述。

[0009] 一种用于接收和处理数据消息的方法，包括：在存储器中至少存储加密密钥；由接收设备接收数据消息，其中数据消息至少包括经加密的消息和消息认证码，其中至少利用经加密的消息的一部分来生成消息认证码；由处理设备至少利用包括在接收的数据消息中的经加密的消息的一部分来生成参考认证码；由处理设备基于比对生成的参考认证码来检查包括在接收的数据消息中的消息认证码，来对接收的数据消息进行验证；由处理设备利用存储的加密密钥对包括在数据消息中的经加密的消息进行解密，以得到经解密的消息。

[0010] 一种用于接收和处理数据消息的系统，包括存储器、接收设备和处理设备。存储器被配置为至少存储加密密钥。接收设备被配置为接收数据消息，其中数据消息至少包括经加密的消息和消息认证码，其中消息认证码至少利用经加密的消息的一部分来生成。处理设备被配置为：至少利用包括在接收的数据消息中的经加密的消息的一部分来生成参考认证码；基于比对生成的参考认证码来检查包括在接收的数据消息中的消息认证码，来对接收的数据消息进行验证；以及，利用存储的加密密钥对包括在接收的数据消息中的经加密的消息进行解密，以得到经解密的消息。

附图说明

[0011] 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：

[0012] 图1是示出了根据示例性实施例的用于处理支付交易且在提供并存储支付凭证方面具有高安全性的高级系统架构的框图。

[0013] 图2是示出了根据示例性实施例的用于在不使用安全元件的情况下处理支付交易并安全地接收和存储支付凭证的图1的移动设备的框图。

[0014] 图3是示出了根据示例性实施例的图2的移动设备中用于存储支付凭证的卡片数据库的框图。

[0015] 图4是示出了的根据示例性实施例的图2的移动设备中用于存储用于生成高级存储密钥并生成应用密文的数据的存储器的框图。

[0016] 图5是示出了根据示例性实施例的用于处理与不带有安全元件的移动设备之间的支付交易的图1的交易管理服务器的框图。

[0017] 图6是示出了根据示例性实施例的图5的处理服务器中用于存储支付凭证和账户明细的账户数据库的框图。

[0018] 图7是示出了根据示例性实施例的用于在涉及缺少安全元件的移动设备的支付交易处理中对双重应用密文进行传输和验证的方法的流程图。

[0019] 图8是示出了根据示例性实施例的用于在涉及缺少安全元件的移动设备的支付交易处理中对双重应用密文进行传输和验证的备选方法的流程图。

[0020] 图9是示出了根据示例性实施例的用于新建、传输和验证向缺少安全元件的移动

设备提供的远程通知服务或其它数据消息的方法的流程图。

[0021] 图10A和图10B是示出了根据示例性实施例的用于新建、传输和验证由缺少安全元件的移动设备返回的消息的方法的流程图。

[0022] 图11是示出了根据示例性实施例的用于利用图2的移动设备来验证远程通知服务消息的方法的流程图。

[0023] 图12是示出了根据示例性实施例的用于利用图2的移动设备来生成高级存储密钥的框图。

[0024] 图13和图14是示出了根据示例性实施例的用于生成支付交易中的支付凭证的示例性方法的流程图。

[0025] 图15是示出了根据示例性实施例的用于接收并处理远程通知服务消息的示例性方法的流程图。

[0026] 图16是示出了根据示例性实施例的用于构建高级存储密钥的示例性方法的流程图。

[0027] 图17是示出了根据示例性实施例的计算机系统架构的框图。

[0028] 从下文提供的具体实施方式中，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

[0029] 术语表

[0030] 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、借记交易、资金划拨、账户取款等。支付网络可被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。被配置为作为支付网络的网络或系统的示例包括由MasterCard®、VISA®、Discover®、American Express®、PayPal®等运营的网络或系统。本文所使用的术语“支付网络”可以既指代作为实体的支付网络，又指代物理支付网络，例如包括支付网络的设备、硬件和软件。

[0031] 交易帐户——一种可用于为交易出资的金融帐户，例如支票帐户、储蓄账户、信用帐户、虚拟支付帐户等。交易帐户可与消费者相关联，消费者可以是与支付账户相关联的、可包括个人、家庭、公司、企业、非政府机构等的任何合适类型的实体。在一些情况下，交易帐户可以是虚拟的，例如那些由PayPal®等运营的帐户。

[0032] 支付卡——一种关联有交易帐户的、可被提供给商家以经由所关联的交易帐户为金融交易出资的卡或数据。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，或者可以是代表关联的交易帐户的数据(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，可将包括有支付账号的数据当做支付卡，来处理由关联的交易帐户出资的交易。在一些情况下，如果适用，可将支票认为是支付卡。

[0033] 支付交易——一种在两个实体之间进行的交易，其中从一个实体向另一个实体交换金钱或其它金融收益。支付交易可以是为了购买商品或服务、为了偿还债务或者为了交换相关领域技术人员将显而易见的任何其它金融收益而进行的转账。在一些情况下，支付

交易可以指经由支付卡和/或支付账户出资进行的交易(例如信用卡交易)。可经由发行方、支付网络和收单方来处理这样的支付交易。用于处理这样的支付交易的方法可包括认证、批处理、清算、结算和出资中的至少一项。认证可包括由消费者向商家出具支付明细、商家向他们的收单方提交交易明细(例如,包括支付明细)以及与用于为交易出资的消费者支付账户的发行方核对支付明细。批量处理可以指将经认证的交易与其它经认证的交易一起存储在一个批次中,以分发给收单方。清算可包括从收单方向用于处理的支付网络发送批量化的交易。结算可包括由支付网络针对发行方受益人所参与的交易而对发行方进行扣款。在一些情况下,发行方可经由支付网络向收单方付款。在其它情况下,发行方可直接向收单方付款。出资可包括针对已清算及已结算的支付交易,由收单方向商家付款。相关领域技术人员将显而易见的是,上面讨论的步骤的顺序和/或分类作为处理支付交易的一部分。

[0034] 销售点——一种被配置为接收与用户(例如,消费者、雇员等)进行的交互进而输入针对所购买和/或支付的商品和/或服务的交易数据、支付数据和/或其它合适类型的数据的计算设备或计算系统。销售点可以是位于消费者到访(这作为交易的一部分)的物理地点(例如位于实体店内)处的物理设备(例如,收银机、自助服务机、台式电脑、智能手机、平板电脑等),或者是电子商务环境中的虚拟设备(例如,利用诸如互联网的网络接收来自消费者的通信数据的在线零售商)。在销售点可以是虚拟的情况下,如果适用的话,可将由用户为了发起交易而操控的计算设备或者接收作为交易结果的数据的计算系统认为是销售点。

[0035] 使用不带有安全元件的移动设备来处理支付交易的系统

[0036] 图1示出了用于在移动设备无需使用安全元件的情况下利用移动设备来处理支付交易的系统100,其可包括向移动设备安全地提供支付凭证,安全地存储该支付凭证,以及用于生成用于验证和处理支付交易的多个应用密文。

[0037] 系统100可包括交易管理服务器102。交易管理服务器102(这将在下文进行更详细的讨论)可以是一个或多个经专门编程以执行本文所讨论的如下功能的计算设备:即,使用安全发送的远程通知消息来向移动设备104提供支付凭证,以及对由移动设备104所产生的支付凭证进行验证(这作为支付交易的一部分)。虽然本文所示出并讨论的是交易管理服务器102执行多种功能,但是相关领域的技术人员将显而易见的是,交易管理服务器102可包括被配置为执行本文讨论的功能的多个计算设备、服务器和/或计算网络。移动设备104(这将在下文进行更详细的讨论)可以是适于执行本文讨论的功能的任意类型的移动计算设备,其可包括蜂窝手机、智能手机、智能手表、其他可穿戴式和嵌入式计算设备、平板电脑、笔记本电脑等。在一些实施例中,移动设备104可缺少安全元件。在其它实施例中,移动设备104可包括安全元件,但是这样的元件可不与本文所讨论的方法及系统一起使用,或着也可与本文所讨论的方法及系统一起使用以提供附加的安全性。

[0038] 移动设备104可使用多个通信信道(例如利用双信道通信)与交易管理服务器102进行通信。双信道通信可包括在发送和接收例如用于验证和认证的数据时使用两个通信信道,以保证数据传输的更高安全性。移动设备104可包括移动支付应用程序(MPA),其被配置为由移动设备104运行用于实现本文所讨论的移动设备104的功能。可将MPA(这将在下文进行更详细的讨论)安装在移动设备104上,并且可利用相关领域技术人员显而易见的方法及系统并使用由交易管理服务器102提供的激活码来激活MPA,以使移动设备104和交易管理

服务器102可在使用共享数据的一个或多个通信信道之间安全地发送和接收通信消息。

[0039] 系统100还可包括发行方106。发行方106可以是向与交易账户相关联的消费方108发行支付卡或支付凭证的金融机构(例如发行银行)。发行方106可向交易管理服务器102提供与交易账户和/或支付卡相关联的支付明细。支付明细可包括例如交易账号、账户持有人姓名、有效期、安全码等。交易管理服务器102可将数据存储在帐户数据库中(这将在下文进行更详细的讨论)。交易管理服务器102还可向移动设备104提供支付凭证。如本文所使用地,术语"支付凭证"可以指在利用本文所讨论的方法及系统的支付交易中移动设备104和/或交易管理服务器102在传输和验证用于该支付交易中的支付信息时使用的任何数据,其包括但不限于支付明细、支付凭证、一次性密钥、会话密钥、应用密文、卡片主密钥等。

[0040] 在一些实施例中,可经由远程通知服务消息来向移动设备104提供支付凭证。如下面更详细讨论地,远程通知服务(RNS)消息可以是首先发送给移动设备104、然后由移动设备104进行验证的安全消息,以使包含在远程通知服务消息中的数据可免受其它设备和用户的危害。移动设备104的MPA可验证所接收的RNS消息的真实性,并且可对其进行解密,以获得其中包含的数据。然后,移动设备104可基于该数据来执行任何必要的功能(例如,通过执行包括在数据中的指令),并且,如果适用的话,移动设备104的MPA可生成待反向发送回交易管理服务器102的返回消息。在一些情况下,交易管理服务器102可对返回消息进行验证。

[0041] 在一些情况下,在移动设备104中对RNS消息进行验证,或者在交易管理服务器102处对返回消息进行验证,可至少利用消息计数和认证码。使用计数和认证码可确保只有标的性移动设备104才能对RNS消息中包括的数据进行验证和解密。此外,如果MPA中包括用于生成认证码的规则和/或算法,则只有还包括该应用程序的专用实例的移动设备104才能对RNS消息进行验证,这进一步提高了安全性。在RNS消息包括有支付凭证的情况下,这可确保:只有在适当的移动设备104上并且仅当用于访问支付凭证的MPA是适当且经认证的应用程序时,才可获得这些支付凭证。

[0042] 可将提供给移动设备104的支付凭证安全地存储在移动设备104中的存储器(例如卡片数据库,这将在下面进行更详细的讨论)中。在一些实施例中,移动设备104可被配置为生成用于将数据(例如支付凭证)安全地存储在移动设备104中的数据库或存储器中的高级存储密钥。生成高级存储密钥(这将在下面进行更详细的讨论)可利用唯一性设备信息、唯一性MPA信息和随机生成的信息,以便确定出可用于将数据安全地存储在移动设备104中的安全存储密钥。因此,可在不使用安全元件的情况下,将支付凭证或其它敏感数据存储在移动设备104中,这可使得移动设备104在不使用安全元件的情况下也能够发起并进行支付交易,从而在保持高水平的安全性的同时,增加了针对发行方106和消费者108的可用性。

[0043] 一旦移动设备104已经接收、验证针对交易账户的支付凭证并将其安全地存储在其中,消费者108可将移动设备104带到商家的销售点110来进行支付交易。消费者108可选择要购买的商品或服务,可向商家发起购买商品或服务的支付交易,并可使用移动设备104来传递支付凭证以用于为支付交易出资。向销售点110传递支付凭证可包括传输两个或更多个应用密文。使用两个或更多个应用密文可导致采用本文所讨论的方法及系统来进行的交易的安全性比从传统非接触式的远程交易(包括利用具有安全元件的移动设备104进行的交易)中获得的安全性的水平要高。

[0044] 移动设备104可采用单独的会话密钥和附加数据(这将在下面进行详细的讨论)来分别生成应用密文。利用存储在移动设备104中的数据(例如存储在存储器中、经由高级存储密钥保护且与MPA相关联的数据)生成的应用密文可确保应用密文能对移动设备104和MPA的专用实例进行认证。在一些情况下,应用密文中的一个密文和/或用于生成密文的会话密钥可使用由消费者108提供的信息,例如个人标识号(PIN)。使用PIN或其它消费者认证信息可使得密文能对消费者108和移动设备104同时进行认证。在此种情况下,由移动设备104生成的密文可包括能对移动设备104进行认证的一个密文,以及能对移动设备104和消费者108同时进行认证的第二个密文。

[0045] 作为进行支付交易的一部分,密文可例如经由近场通信而被销售点110接收。应用密文可伴随有附加支付信息,该附加支付信息例如是在任何合适类型的支付交易(例如非接触式交易、远程交易、安全远程支付交易、磁条交易和M/芯片EMV交易)中所要求的,并可采用根据相关领域技术人员显而易见的任何合适方法来传送给销售点110。可将密文发送给收单方112,该收单方可以是金融机构(例如与商家相关联的收单银行)。收单方112例如可向商家发放用于从消费者108处接收针对支付交易的支付资金的交易账户。收单方112可使用相关领域技术人员显而易见的方法及系统来向支付网络114提交密文和附加支付明细。例如,交易明细和应用密文可被包括在向支付路径中的支付网络114提交的认证请求中。

[0046] 在一些实施例中,两个应用密文可被包括在单个交易消息中。例如,移动设备104和/或销售点110可将两个应用密文均包括在传统交易信息的遗留数据字段中,以使用现存的支付系统和硬件来传输这两个应用密文。在一些情况下,交易管理服务器102可被配置为使用路径2数据来对应用密文进行验证(例如在磁条交易中)。在这种情况下,如果交易消息包括路径1数据,则交易管理服务器102可被配置为将路径1数据转换为路径2数据,这还可包括将经修改的路径1数据或路径2数据分别转换为未经修改的(例如,原始的、重构的等)路径1数据或未经修改的路径2数据。通过执行这些功能,并且通过将应用密文包括在遗留数据字段中,交易管理服务器102可被配置为在无需使用移动设备104上的安全元件的情况下,并在不修改遗留的支付系统的情况下,使用移动设备104以更高水平的安全性来对远程和非接触式支付交易进行处理和验证。

[0047] 支付网络114可采用相关领域技术人员显而易见的方法及系统来处理支付交易。作为处理的一部分,支付网络114可将应用密文传送给发行方106,以进行验证。在一些实施例中,可由支付网络114来执行验证。发行方106或支付网络114可与交易管理服务器102进行通信。在一些实施例中,可将应用密文传送给交易管理服务器102,并且利用交易管理服务器102生成有效的应用密文(利用本地存储的支付凭证生成的)来对应用密文进行验证。在其他实施例中,发行方106或支付网络114可从交易管理服务器102请求应用密文,交易管理服务器102可生成应用密文并将其返回给发行方106或支付网络114,以对照由移动设备104产生的密文进行验证。

[0048] 由于交易管理服务器102具有支付凭证和被移动设备104用以生成应用密文的其它数据,因此可通过将由移动设备104生成的应用密文与由交易管理服务器102生成的应用密文进行比较,来执行对由移动设备104产生的支付凭证的验证,以出资进行支付交易。在一些实施例中,交易管理服务器102可以是支付网络114或发行方106的一部分。在交易管理

服务器102是支付网络114的一部分的情况下，可在联系发行方106(这作为传统支付交易方法的一部分，例如，同意发行方106使用消费者108的交易账户为交易出资)之前执行验证。

[0049] 通过使用多个应用密文，可增加支付交易的安全性。此外，在每个密文可对单独的数据进行认证的情况下(例如，一个密文对移动设备104进行认证，而另一个密文例如经由消费者的PIN可对移动设备104和消费者108同时进行认证的情况下)，还可向发行方106提供用于决定同意或拒绝交易的附加数据和考虑。例如，如果两个密文都是不正确的(例如，由移动设备104生成的密文与由交易管理服务器102生成的那些密文不匹配)，则交易可能会被拒绝。如果一个密文正确而另一个密文不正确，则出于安全性的原因交易可能会被拒绝，或者被同意(例如基于发行方106的决定)。例如，当消费者认证失败而移动设备认证通过时，发行方106可同意交易，这是因为其它可得到的数据可表明是示经认证的用户(而不是消费者108)正在使用移动设备104进行交易。

[0050] 因此，使用两个密文可提供由支付网络114和发行方106在处理支付交易时使用的有价值的数据。此外，使用两个或多个密文可提供比传统的非接触式或远程支付方法更高的安全性，这可导致更少的欺诈行为并更能被消费者108、发行方106和商家所接纳。使用的两个或多个应用密文是由已采用本文所讨论的RNS消息传递方法及系统来安全地提供的支付凭证生成的，并且使用的两个或多个应用密文是经由采用本文所讨论的方法及系统生成的高级存储密钥来进行安全存储的，在上述情况下，与针对非接触式支付与交易方法的传统系统相比，系统100的整体安全性可得到迅速提高。因此，相比于传统的非接触式支付系统提供的安全性以及其它类型的远程支付交易和基本采用本文所讨论的方法及系统的支付交易所提供的安全性，系统100可在数据传输、存储和处理的若干方面提供更高的安全性。

[0051] 移动设备

[0052] 图2示出了系统100的移动设备104的实施例。对于相关领域技术人员而言，明显知道图2中所示的移动设备104的实施例仅是示意性的，而没有穷举适于执行本文所讨论的功能的移动设备104的所有可能的配置。例如，图17中所示的计算机系统1700(将在下文中进行更详细的讨论)可以是移动设备104的合适配置。

[0053] 移动设备104可包括接收单元202。接收单元202可被配置为通过一个或多个网络、经由一个或多个网络协议来接收数据。接收单元202可接收例如针对将被安装到移动设备104上并由移动设备104运行的一个或多个应用程序(例如将在下面进行更详细的讨论的移动支付应用(MPA))的程序数据。接收单元202还可接收远程通知服务(RNS)消息，例如由交易管理服务器102传送的包括具有支付凭证的RNS消息的那些消息。接收单元202还可接收适于执行移动设备104的传统功能(例如电话通信、蜂窝通信等)的附加数据。在一些情况下，移动设备104可包括多个接收单元202，例如各自被配置为经由合适的协议与一个多个单个网络进行通信的独立接收单元202。例如，移动设备104可包括用于接收针对NFC交易的数据的第一接收单元202，以及用于通过移动通信网络接收通信数据的第二接收单元202。

[0054] 移动设备104还可包括输入单元214。输入单元214可被配置为与在内部或外部连接至移动设备104、用于接收来自消费者108的输入的一个或多个输入设备进行通信，输入设备例如键盘、鼠标、点击轮、滚轮、触摸屏、麦克风、摄像头、接收器等。输入单元214可接收来自消费者108的输入，该输入可由处理单元204处理。

[0055] 处理单元204可被配置为执行本文所讨论的移动设备104的功能。处理单元204可执行存储在移动设备中的程序代码(例如针对MPA的程序代码),并可被配置为执行与每个应用程序相关联的多个功能以及移动设备104的其它功能。处理单元204可经由输入单元214来接收来自消费者108的输入,并执行相应的功能,例如如相关领域技术人员显而易见地那样,通过运行应用程序,来执行程序中的功能、接收数据、发送数据、显示数据等。例如,处理单元204可被配置为验证RNS消息、生成高级存储密钥并生成应用密文,这将在下面进行更详细的讨论。

[0056] 移动设备104还可包括显示单元210。显示单元210可被配置为与在内部或外部连接至移动设备104的、用于显示数据(例如由处理单元204传送给显示单元210的用于显示的数据)的一个或多个显示设备进行通信。显示设备可包括液晶显示器、发光二极管显示器、薄膜晶体管显示器、触摸屏显示器等。

[0057] 移动设备104还可包括传送单元206。传送单元206可被配置为通过一个或多个网络、经由一个或多个网络协议来传输数据。传送单元206可向交易管理服务器102传输RNS响应消息。传送单元206还可被配置为例如向销售点110传输在支付交易中使用的应用密文和/或支付凭证。传送单元206还可被配置为执行移动设备104的那些被相关领域技术人员显而易见的附加功能,例如移动通信设备中用于传输蜂窝通信数据的传统功能等。在某些情况下,移动设备104可包括多个被区分式地配置为与一个或多个单个网络进行通信的传送单元206,例如一个传送单元206被配置为经由NFC发送支付凭证和支付密文,而另一个传送单元206被配置为通过移动通信网络发送数据。

[0058] 移动设备104还可包括卡片数据库208。卡片数据库208(这将在下面进行更详细的讨论)可以是在移动设备104上、被配置为存储与一个或多个交易账户和/或支付卡相关联的数据的数据存储器。卡片数据库208可存储与交易帐户相关联的支付凭证(例如由交易管理服务器102向移动设备104提供的、在安全RNS消息中的支付凭证)以及可在生成应用密文中使用的附加数据(这将在下面进行更详细的讨论)。在一些情况下,可将卡片数据库208作为移动支付应用程序的一部分来进行存储。

[0059] 移动设备104还可包括存储器212。存储器212(这将在下面进行更详细的讨论)可被配置为存储针对移动设备104的、适于执行本文所讨论的移动设备104的功能的数据。例如,存储器212(例如将在下面进行更详细的讨论的卡片数据库208)可存储那些适于生成用于对移动设备104中的附加数据进行加密的高级存储密钥的数据。存储器212还可被配置为存储针对由处理单元204(例如操作系统)执行的应用程序的程序代码、用于经由输入单元204来接收数据以及经由显示单元210来显示数据的程序代码、用于执行本文所讨论的功能的规则和/或算法等。存储器212还可存储适于执行移动设备104的传统功能的数据,例如用于经由移动网络来发送和接收蜂窝通信数据的规则和/或算法。相关领域技术人员将显而易见那些存储在存储器212中的附加数据。

[0060] 移动设备卡片数据库

[0061] 图3示出了移动设备104的卡片数据库208的实施例,卡片数据库208用于存储支付凭证以及关联于交易账户的其它数据,以用于通过移动设备108来为支付交易出资。

[0062] 卡片数据库208可包括一个或多个支付文件302,支付文件302如图3中的支付文件302a、302b和302c所示。每个支付文件302可与能为支付交易出资的交易账户相关联,并可

至少包括支付凭证304、一个或多个一次性密钥306、第一会话密钥308、第二会话密钥310和应用交易计数312。

[0063] 支付凭证304可包括与相关的交易账户相关联的数据，支付网络114和/或发行方106在处理使用该相关的交易账户的支付交易时利用该数据进行识别和验证。支付凭证304可包括例如交易帐号、安全码、有效期限、持卡人姓名、经授权的用户名、跟踪数据、卡片布局说明数据、数字计数、位图等。

[0064] 一次性密钥306可以是对于单次支付交易有效的支付令牌，移动设备104的处理单元204使用该支付令牌来生成用于支付交易的一个或多个应用密文。在一些实施例中，一次性密钥306可包括一个或多个包括在支付文件302中的其它数据元素。例如，每个一次性密钥306可包括区分应用交易计数312，该区分应用交易计数不可单独地包括在支付文件302中。相关领域技术人员将显而易见在执行本文所公开的功能中使用的存储在支付文件302中的数据的不同配置。在一些情况下，一次性密钥306可包括或者由用于生成该一个或多个应用密文的密钥组成。在一些实施例中，第一会话密钥308和第二会话密钥310可被包括在向移动设备104提供的一次性密钥306中，和/或通过包括在一次性密钥306中的数据来生成。

[0065] 第一会话密钥308和第二会话密钥310可以是在生成发送给销售点110的应用密文(作为通过移动设备104而进行的支付交易的一部分)时由处理单元204使用的附加密钥。在一些实施例中，处理单元204例如使用存储在移动设备104的存储器212中的程序代码、规则或算法，可利用第一会话密钥308来生成第一应用密文。在生成第二应用密文中可使用第二会话密钥310。

[0066] 在一些实施例中，可由处理单元204生成第二会话密钥310。在此实施例中，可使用一次性密钥306和用户认证数据(例如，由消费者108例如经由输入单元214提供的PIN)来生成第二会话密钥310。在此实施例中，第二会话密钥310可以不被存储在支付文件302中，而是作为支付交易过程的一部分地被生成、使用和丢弃。当由利用一次性密钥306和消费者PIN生成的第二会话密钥310来生成第二应用密文时，第二应用密文因此可用于对移动设备104和消费者108同时进行认证。

[0067] 个人身份号(PIN)可以是由消费者108(例如，当在移动设备104上注册MPA期间，或者在向发行方106和/或交易管理服务器102注册交易账户期间)提供的、可用于认证消费者108的编号。在进行支付交易时，消费者108或移动设备104的其它用户可经由输入单元214提供PIN。在一些实施例中，如果所提供的PIN不正确(例如，与消费者108在注册期间提供的PIN不匹配)，则处理单元204可继续生成第二会话密钥310并随后生成第二应用密文。如果所提供的PIN不正确，则第二应用密文也因此是不正确的，这将导致交易管理服务器102、发行方106和/或支付网络114对第二应用密文的验证失败，这可使得发行方106有机会相应地拒绝交易或者仍同意进行交易。

[0068] 移动设备存储器

[0069] 图4示出了移动设备104的存储器212的实施例，该存储器用于存储在将数据安全地存储在移动设备104上时使用的、用于实施利用该移动设备104进行的支付交易时所使用的应用程序及其它数据。在示例性实施例中，存储器212可以不是安全元件。

[0070] 存储器212可包括设备信息402。设备信息402可包括与移动设备104相关联的一条

或多条数据，在一些情况下该一条或多条数据相对于移动设备104是唯一的。例如，设备信息402可包括媒体访问控制地址、参考号、序列号、标识号等。相关领域技术人员将显而易见那些能让设备信息402代表移动设备104的附加信息。

[0071] 存储器212还可包括移动支付应用程序(MPA)404。MPA 404可以是被配置为执行本文所讨论的移动设备104的功能(例如接收并存储支付凭证、验证RNS消息、以及生成用于进行支付交易的应用密文)的应用程序。如相关领域技术人员将显而易见地，MPA 404的附加特征可包括数字钱包的传统功能或其他类似应用程序。

[0072] MPA 404可包括程序代码406。程序代码406可以是由移动设备104的处理单元204执行的、使移动设备104的处理单元204和其它部件执行本文所讨论的MPA 404的功能的代码。例如，程序代码406可包括适于生成应用密文、验证RNS消息等的代码。程序代码406还可包括适于生成可用于生成高级存储密钥的随机值的程序代码。随机值可以是利用相关领域技术人员显而易见的方法及系统来生成的随机数或伪随机数。

[0073] MPA 404还可包括实例标识符408。实例标识符408对于特定MPA 404来说可以是唯一性的值，该实例标识符可在生成用于保护移动设备104(例如卡片数据库208)中的数据的高级存储密钥时使用。通过使实例标识符408唯一地对应MPA 404，可在没有任何一个MPA 404能访问由任何其它MPA 404安全存储的数据的情况下，将多个MPA 404安装在移动设备104上，从而可确保其它程序不能访问针对特定交易账户的那个支付文件302。实例标识符408可以是数字、字母数字值、十六进制值、或者对于MPA 404是唯一的任何合适的值。

[0074] 如将在下面更详细讨论地，移动设备104的处理单元204可被配置为利用设备信息402、使用MPA 404的程序代码生成的随机值、以及存储在MPA 404中的实例标识符408来生成多元值。同样存储在存储器212中的加密应用程序410可使用该多元值。加密应用程序410可以是被配置为能执行白盒加密和/或相关领域技术人员显而易见的任何其它合适的加密功能的应用程序。

[0075] 加密应用程序410可包括程序代码412。程序代码412可由移动设备104的处理单元204来执行，以使移动设备104的处理单元204和其它组件能执行本文所讨论的加密应用程序410的加密功能。功能可包括生成高级存储密钥。可利用由移动支付应用程序404生成的多元值和包括在加密应用程序410中的加密密钥414来生成高级存储密钥。在一些实施例中，可利用加密密钥414来对多元值进行解密，以得到高级存储密钥。

[0076] 加密应用程序410还可被配置为利用高级存储密钥来对移动设备104中的存储进行加密。在一些实施例中，可利用一种或多种白盒加密技术来执行加密。经加密的存储可以是卡片数据库208和/或移动设备104中的任何其它合适的存储，例如存储在MPA 404中的数据。在一些实施例中，加密应用程序410可被包括为MPA 404的一部分。高级存储密钥可存储在加密应用程序410或MPA 404中，或者，在某些情况下，当需要时可由MPA 404和加密应用程序410重新生成。

[0077] 存储器212还可包括存储在移动设备104中的、适于执行本文所讨论的功能以及移动设备的任何其他功能的任何附加数据。例如，存储器212可包括用于操控系统的程序代码、代码、规则、或用于接收和发送移动通信信息(例如电话呼叫等)的算法。

[0078] 在一些实施例中，移动设备104还可被配置为接收已利用高级存储密钥加密的数据，该数据可存储在移动设备104的经加密的本地存储器中(例如在存储器212、卡片数据库

208或其它合适的存储器中)。在这样的实施例中,移动设备104可被配置为将生成的随机值传送给交易管理服务器102或其它可信的实体,交易管理服务器102或其它可信的实体可利用相同的方法及系统、使用生成的随机值来生成高级存储密钥,并可对要向移动设备104提供的数据进行加密。移动设备104可因此接收已利用高级存储密钥进行加密的数据,以进行移动设备104中的本地存储。

[0079] 交易管理服务器

[0080] 图5示出了系统100的交易管理服务器102的实施例。对于相关领域技术人员而言,明显知道图5中所示的交易管理服务器102的实施例仅是示意性的,而没有穷举适于执行本文所公开的功能的交易管理服务器102的所有可能的配置。例如,图17中所示的计算机系统1700(将在下文中进行更详细的讨论)可以是交易管理服务器102的合适配置。

[0081] 交易管理服务器102可包括接收单元502。接收单元502可被配置为通过一个或多个网络、经由一个或多个网络协议来接收数据。接收单元502可接收来自移动设备104(例如接收消息或返回消息、确认消息、交易通知等)、支付网络114、发行方106或其它合适实体的数据。接收单元502可接收交易通知或加密请求,以发起对用于验证支付交易中的支付凭证的应用密文的生成。

[0082] 交易管理服务器102还可包括处理单元504。处理单元504可被配置为执行相关领域技术人员将显而易见的、本文所讨论的交易管理服务器102的功能。如下面更详细讨论地,处理单元504可因此被配置为:生成并加密RNS消息以及包括在RNS消息中的数据、对来自移动设备104的返回消息进行验证、生成支付凭证、生成应用密文、验证应用密文等。

[0083] 交易管理服务器102还可包括传送单元506。传送单元506可被配置为通过一个或多个网络、经由一个或多个网络协议来传输数据。传送单元506可传送RNS消息、支付凭证、应用密文、验证通知和相关领域技术人员显而易见的其它数据。传送单元506可被配置为向移动设备104(例如经由移动通信网络或互联网)、支付网络114、发行方106或任何其它合适的实体发送数据。

[0084] 交易管理服务器102还可包括帐户数据库508。帐户数据库508中(这将在下面进行更详细的讨论)可被配置为存储针对多个交易账户的账户信息。账户信息可包括用于生成应用密文(其用于验证在使用移动设备104进行的支付交易过程中接收到的支付凭证)的数据和密钥。账户数据库508还可被配置为存储针对涉及移动设备104的支付交易的交易数据以及其它数据(例如与相关交易账户的消费者108或其它认证用户相关联的数据)。

[0085] 交易管理服务器102还可包括存储器510。存储器510可被配置为存储交易管理服务器102在执行本文所公开的功能时使用的附加数据。例如,存储器510可存储用于验证应用密文的规则或算法、用于生成验证通知的规则或算法、用于生成会话密钥和应用密文的算法、用于对数据和RNS消息进行加密和解密的加密密钥等。相关领域技术人员将显而易见那些可存储在存储器510中的附加数据。

[0086] 交易管理服务器账户数据库

[0087] 图6示出了交易管理服务器102的账户数据库508的实施例,账户数据库508用于存储与交易账户相关的用于验证支付凭证的数据,并用于存储在进行包括有移动设备104的支付交易时所提供的其它交易数据。

[0088] 帐户数据库508可包括多个账户文件602,如图6中所示的账户文件602a、602b和

602c。每个帐户文件602可包括一个或多个一次性密钥604、第一会话密钥606、第二会话密钥608、应用交易计数610和第一卡片主密钥612。在一些实施例中，帐户文件602可进一步包括第二卡片主密钥612。

[0089] 每个帐户文件602可与向移动设备104提供的支付文件302相对应。同样地，存储在账户文件602中的一次性密钥604可对应于存储在与相同的交易账户相关的对应支付文件302中的一次性密钥306。数据可以是类似的，以使当交易管理服务器102或移动设备104生成应用密文时，应用密文应该是匹配的(如果数据是准确的且未被篡改的话)，从而能够对由移动设备104发布的支付凭证进行验证。

[0090] 在一些实施例中，帐户文件602可包括对应于存储在相应的支付文件302中的PIN 314的个人身份号(PIN)。在这样的实施例中，可通过安全消息(例如由移动设备104提供的接收消息，这将在下面进行更详细的讨论)将PIN 314提供给交易管理服务器102的接收单元202。在其他实施例中，可使用卡片主密钥(例如第一卡片主密钥612)来替代PIN。在此实施例中，交易管理服务器102的处理单元504可被配置为基于第二卡片主密钥614来生成第二会话密钥608，第二卡片主密钥614与由移动设备104利用一次性密钥306和PIN 314生成的第二会话密钥310相对应。在一些情况下，第二会话密钥608还可基于相应的一次性密钥604。在此实施例中，用于生成会话密钥和/或应用密文的算法可确保：由移动设备104和交易管理服务器102基于其中所使用的数据而生成的密文相互对应。

[0091] 交易管理服务器102的处理单元504可利用第一会话密钥606来生成第一应用密文，并利用第二会话密钥608来生成第二应用密文。在一些实施例中，可利用应用交易计数610来生成一个或多个会话密钥和/或应用密文。应用交易计数610可以是与将要进行的支付交易相对应的值，可在每个交易期间增加或反向修改该值。应用交易计数610可以与存储在移动设备104中的相应支付文件302中的应用交易计数312相对应，由此，使用应用交易计数610可确保：仅有有效的MPA 404才能具有正确的应用交易计数312，以生成有效的会话密钥和/或应用密文。可使用能进一步增加生成会话密钥和/或应用密文的安全性的其他技术，例如被相关领域技术人员显而易见的不可预测数字或其它技术。

[0092] 利用移动设备来处理支付交易

[0093] 图7示出了利用不带有安全元件的移动设备104并通过生成和验证两个或多个应用密文来处理支付交易的方法的过程。

[0094] 在步骤702中，交易管理服务器102(例如经由传送单元506)向移动设备104提供支付凭证304和其它帐户数据(例如经由在以下进行更详细讨论的RNS消息)。在步骤704中，移动设备104的接收单元202接收支付凭证304和其它帐户数据。在步骤706中，移动设备104的处理单元204将数据存储在卡片数据库208中的支付文件302中。帐户数据可包括支付凭证304、一个或多个一次性密钥308、以及任何其它合适的数据(例如一个或多个会话密钥308和310)。

[0095] 在步骤708中，处理单元204生成用于进行支付交易的两个应用密文。在一些实施例中，可由消费者108来发起步骤708，例如通过经由输入单元214来进行指示、通过将移动设备104放置在销售点110附近来发起经由近场通信的交易、或者通过其它合适的方法。应用密文的生成可包括利用存储在支付文件302中的第一会话密钥308来生成第一应用密文。可利用使用一次性密钥306和PIN 314生成的第二会话密钥310来生成第二应用密文。在一

些情况下，消费者108可在步骤708之前或在发起步骤708期间将PIN输入到移动设备104中(例如经由输入单元214)。在一些实施例中，还可利用应用交易计数312来生成一个或两个应用密文。

[0096] 一旦生成应用密文，则将该应用密文与支付凭证304一起经由销售点110、收单方112和支付网络114发送给发行方106。在步骤710中，由发行方106接收支付凭证304和应用密文。在步骤712中，移动设备104的传送单元206向交易管理服务器102传送交易通知。在步骤714中，交易管理服务器102的接收单元502接收交易通知。交易通知可向交易管理服务器102通知：移动设备104已利用支付文件302发起了支付交易。在一些情况下，交易通知可包括身份信息。

[0097] 在步骤716中，交易管理服务器102的处理单元504识别出对应于支付文件302的帐户文件602，并可利用其中包含的数据来生成两个应用密文。可利用使用第一卡片主密钥612生成的第一会话密钥606来生成第一应用密文。可利用第二会话密钥608来生成第二应用密文。在一些实施例中，一个或两个应用密文和/或会话密钥还可基于一次性密钥604、应用交易计数610或任何其它合适的数据。

[0098] 在步骤718中，交易管理服务器102的传送单元506向发行方106发送所生成的应用密文，发行方106在步骤718中接收该密文。在步骤720中，发行方106对由移动设备104提供的应用密文以及支付凭证304进行验证。验证应用密文可包括将移动设备104提供的应用密文和由交易管理服务器102生成并提供的应用密文进行比较。一旦执行验证，则在步骤722中，发行方106对该交易进行相应地处理。处理交易可包括同意支付交易(例如在一个或两个密文有效的情况下)，或者拒绝支付交易(例如在一个或两个密文都被确定无效的情况下)。

[0099] 在步骤724中，作为处理支付交易的一部分，发行方106或其它实体(例如支付网络114、收单方112等)可传送交易通知。在步骤726中，交易通知被传送给交易管理服务器102并被接收单元502接收。在步骤728中，交易通知还被移动设备104的接收单元202接收。交易通知可以是同意或拒绝支付交易的指令。由于接收到交易通知，移动设备104的处理单元204和交易管理服务器102的处理单元504可分别执行一个或多个功能。例如，如果交易被批准并成功进行的话，则各个文件中的应用交易计数310,610则会得到相应的更新。

[0100] 图8示出了用于处理使用移动设备104的支付交易的备选方法。

[0101] 在步骤802中，交易管理服务器102的传送单元506向移动设备104传送支付凭证304和其它帐户数据。在步骤804中，移动设备104的接收单元202接收支付凭证304和其它账户数据，在步骤806中它们被存储在支付文件302中。在步骤808中，移动设备104的处理单元204可生成上面讨论的两个应用密文，并(例如经由销售点110)向发行方106传送该密文、支付凭证304和其它合适的数据。

[0102] 在步骤810中，发行方106接收应用密文和其它合适的数据，发行方106利用该应用密文和其它合适的数据来验证交易数据和/或同意还是拒绝交易。在步骤812中，发行方106向交易管理服务器102提交验证密文的请求。在一些实施例中，请求可包括支付凭证304或适于由交易管理服务器102在鉴别将用于生成有效密文的账户文件602时使用的其它数据。在一个实施例中，请求还可包括由移动设备104为了验证而生成的两个应用密文。

[0103] 在步骤814中，交易管理服务器102的接收单元502接收密文请求。在步骤816中，交

易管理服务器102的处理单元504生成如上所讨论的将用于验证的两个应用密文。在密文请求还包括由移动设备104生成的两个应用密文的实施例中，步骤816还可包括由处理单元504利用两个新生成的应用密文来对两个密文进行验证。在适用的实施例中，通过传送单元506将验证密文或验证结果传送给发行方106。在步骤818中，发行方106接收验证密文和/或验证结果。

[0104] 在步骤820中，发行方106利用由交易管理服务器102生成的应用密文对由移动设备104提供的应用密文进行验证。在交易管理服务器102向发行方106提供验证结果的实施例中，步骤820可包括对两个应用密文中的每个应用密文的验证结果进行识别。在步骤822中，发行方106基于验证结果来相应地处理支付交易。在步骤824中，交易通知被传送给交易管理服务器102和移动设备104，并分别在步骤826和步骤828中被各自的接收单元502和202接收。

[0105] 远程通知服务和数据消息

[0106] 图9示出了用于对远程通知服务(RNS)消息和从交易管理服务器102向移动设备104发送的其它数据消息进行传输和验证的方法。可经由远程通知服务来传送RNS消息，例如利用与移动设备102相关联的移动通信网络的远程通知服务。可利用RNS消息来向移动设备104提供支付凭证304和其它账户数据(例如，在如上面讨论的处理支付交易中使用的账户数据，以及在建立移动设备104与交易管理服务器102之间的安全连接中使用的其它信息)。

[0107] 在步骤902中，交易管理服务器102的处理单元504生成消息。在与移动设备104建立相互认证的情况下，该消息可包括适于建立相互认证的信息，例如会话标识符。在其他情况下，例如当利用如图9所示及本文所讨论的方法来建立交易管理服务器102与移动设备104之间的相互认证时，所生成的消息，可包括支付凭证304和帐户数据，可包括将由移动设备104的MPA 404执行的一个或多个命令(例如移除一次性密钥306或支付凭证304等)，可以是将呈现给消费者108的通知(例如账户余额、支付通知等)，或者包括其它合适的数据。

[0108] 在步骤904中，处理单元504对所生成的消息进行加密。可利用私人/公用密钥对中的私人密钥来对消息进行加密，其中移动设备104可拥有相应的公用密钥。在一些情况下，可利用与移动设备104或MPA 404相关联的加密密钥(例如，加密密钥414)对消息进行加密。在步骤906中，处理单元504生成消息认证码。可利用经加密的消息来生成消息认证码，消息认证码可以是使用一个或多个专门配置的规则和/或算法而生成的密钥。例如，可利用一种或多种加密和模糊处理方法(例如填充)来生成消息认证码。在一些实施例中，可使用加密密钥来生成消息认证码。

[0109] 在步骤908中，交易管理服务器102的传送单元506向移动设备104传送组合数据消息。在正在执行相互认证的实施例中，组合数据消息可以是经由远程通知服务向移动设备104传送的远程通知服务消息。在步骤910中，由移动设备104的接收单元202对组合数据消息进行接收，该组合数据消息可包括消息认证码和经加密的消息。在一些情况下，组合数据消息还可包括附加标识符，例如使用验证用的MPA 404已知的方法来生成的附加标识符。在某些情况下，例如当已执行相互认证时，组合数据消息还可包括消息计数。

[0110] 在步骤912中，处理单元204产生参考认证码。可使用所接收的经加密的消息来生成参考认证码，并且可使用与交易管理服务器102生成消息认证码时相同的规则和算法来

生成参考认证码，以便在消息认证码由可信来源(例如交易管理服务器102)生成时所生成的参考认证码会与消息认证码相对应。在可利用加密密钥来生成消息认证码的实施例中，处理单元204可利用存储在存储器212中的加密密钥414或其它合适的加密密钥来生成参考认证码。

[0111] 在步骤914中，处理单元204可通过将消息认证码与所生成的参考认证码进行比较，来对包括在所接收的组合数据消息中的消息认证码进行验证。如果消息计数和消息认证码都是有效的，那么可确定组合数据消息可信(例如真实)地来自交易管理服务器102。在组合数据消息可包括消息标识符的情况下，处理单元204还可通过使用MPA404已知的生成和比较方法来生成消息标识符的方式，来对消息标识符进行验证。在组合数据消息可包括消息计数的实施例中，处理单元204可用存储在移动设备104中(例如存储在MPA 404中或存储在支付文件502中)的参考计数来对包括在所接收到的组合数据消息中的消息计数进行验证。

[0112] 在步骤916中，处理单元204对包括在接收到的组合数据消息中的经加密的消息进行解密。可利用密钥或者其它合适的解密方法对经加密的消息进行解密，密钥例如为存储在存储器212中(例如存储在加密应用程序410或MPA 404中)或存储在本地经加密的数据库(例如使用高级存储密钥进行加密的)中的密钥。在步骤918中，处理单元204基于从经加密的消息中解密出来的数据来执行一个或多个合适的动作。在图9中所示的示例中，移动设备104可与交易管理服务器102例如通过使用包括在经加密的消息中的、被处理单元204解密的会话标识符，来执行相互认证。在步骤920中，交易管理服务器102接收会话标识符并执行与移动设备104进行相互认证所必需的任何附加动作。在已执行相互认证的情况下，消息可包括适于执行本文所公开的功能的其它信息，例如支付凭证404、一次性密钥406、针对MPA 404的程序指令等。

[0113] 在一些实施例中，移动设备104可(例如经由MPA404)被配置为生成返回消息并将其提交至交易管理服务器102。在一些情况下，如上面所讨论地，返回消息可包括响应于执行经解密的消息中所指示的动作而生成的数据。例如，返回消息可指示对支付凭证304或一次性密钥306的有效接收和存储。在其它情况下，返回消息可以是接收及验证组合数据信息的通知。在首次进行相互认证的情况下，返回消息可包括用于执行相互认证的会话标识符。

[0114] 图10A和10B示出了由移动设备101生成并传送返回消息并由交易管理服务器102对返回消息进行验证的过程。

[0115] 在步骤1002中，移动设备104的处理单元204生成接收消息。接收消息可基于存储在MPA 404中的程序代码406来生成，并且接收消息还可基于从交易管理服务器102接收到经解密的组合数据消息中指示执行的那些动作。例如，接收消息可包括针对成功接收并存储支付凭证304的通知。在步骤1004中，处理单元204使接收计数递增。接收计数可以为表示传送给交易管理服务器102的接收消息的数量的计数。可将接收计数存储在存储器212中，例如存储在MPA 404中或者利用高级存储密钥存储在经加密的数据库中。相关领域技术人员将显而易见的是，步骤1004可以作为可选的步骤，并仅可用于使用计数对数据消息进行验证的情况下。

[0116] 在步骤1006中，处理单元204对接收消息进行加密。可利用存储在加密应用程序410中的加密密钥414，或者存储在MPA 404中或本地加密数据库中的加密密钥414，对接收

消息进行加密。用于对接收消息进行加密的加密密钥可以是作为密钥对的一部分的私人密钥，并且交易管理服务器102拥有相应的公用密钥。在步骤1008中，处理单元204基于经加密的接收消息来生成接收认证码。在一些实施例中，可使用与上述所讨论的如图9的步骤902中所示的用于生成参考认证码所使用的相同规则、算法和/或方法来生成接收认证码。

[0117] 在步骤1010中，移动设备104的传送单元206向交易管理服务器102发送接收通知消息。接收通知消息可由交易管理服务器102的接收单元502接收，并可至少包括接收认证码、经加密的接收消息和接收计数。在一些实施例中，可利用移动通信网络(例如与移动设备104相关联的蜂窝网络)来将接收通知消息发送给交易管理服务器102。

[0118] 在步骤1014中，交易管理服务器102的处理单元504使确认计数递增。确认计数可表示从移动设备104接收的消息的数量，用于对从移动设备104接收的消息进行验证。可将确认计数存储在交易管理服务器102的存储器510中或其它合适的数据库中。例如，在一些实施例中，可将确认计数存储在与移动设备104相关联的账户文件602中。在一个示例中，每个帐户文件602可包括确认计数(例如和/或消息计数)，该确认计数将被用于向/从与相应的交易账户相关的交易管理服务器102和移动设备104发送的消息中。相关领域技术人员将显而易见的是，步骤1014可以作为可选的步骤，并不能在不使用计数对返回消息进行验证的情况下执行。

[0119] 在步骤1016中，处理单元504生成确认认证码。可基于包括在接收通知消息中的经加密的接收消息来生成确认认证码，并可使用与生成消息认证码所采用的相同的规则、算法和/或方法来生成确认认证码。在步骤1018中，处理单元504通过对接收计数与确认计数进行比较来对包括在接收通知消息中的接收计数进行验证。在步骤1020中，处理单元504通过对接收认证码与消息认证码进行比较来对接收认证码进行验证，以确保消息源于经认证的移动设备104。

[0120] 一旦对计数(例如如果适用)和认证码进行了验证，则在步骤1022中，处理单元504对包括在接收的接收通知消息中的经加密的消息进行解密。可利用存储的加密密钥或其它合适的解密方法来对经加密的消息进行解密。可对经加密的消息进行解密，以得到由移动设备104生成的接收消息。在步骤1024中，处理单元504基于包括在接收消息中的数据来执行所需的任何合适的动作。例如，如果接收消息包括成功接收并存储一次性密钥306的指示，那么处理单元204可激活相应的账户文件602中的相应一次性密钥604。

[0121] 验证数据消息

[0122] 图11示出用于对移动设备104从交易管理服务器102接收的数据消息进行验证的过程1100。

[0123] 在步骤1102中，移动设备104的处理单元204将加密密钥、认证生成密钥以及对它们进行使用及应用的规则和/或方法存储在本地存储器中，例如存储器212或者利用高级存储密钥进行加密的本地经加密存储器。在步骤1104中，移动设备104的接收单元202从交易管理服务器102接收数据消息。在一些实施例中，可在建立两个设备的相互认证(例如采用如图9所示的并如上面所讨论的方法)以后，从交易管理服务器102接收数据消息。

[0124] 在步骤1106中，处理单元204使参考计数递增。参考计数可存储在存储器212或其它本地存储器中，并且可用于表示从交易管理服务器102接收的消息的数量。在一些情况下，可利用算法使参考计数递增，以使得参考计数不是利用连续数而是经由移动设备104

(例如,经由MPA 404)和交易管理服务器102已知的算法来递增的。

[0125] 在步骤1108中,处理单元204对包括在所接收的数据消息中的消息计数进行验证。对消息计数进行验证可包括将消息计数与递增后的参考计数的值进行比较。验证失败可表示数据消息的来源不是交易管理服务器102,或者是不可信的。如果验证失败,则在步骤1110中,处理单元204执行与已失败的数据消息接收和/或验证相关联的一个或多个合适的动作。例如,处理单元204可丢弃该数据消息、可通知交易管理服务器102、可以锁定相关联的支付文件302,或者是对于相关领域技术人员显而易见的其它动作。

[0126] 如果消息计数通过验证,则过程1100可前进至步骤1112,在那里对经加密的消息进行填充。对经加密的消息进行填充可包括使经加密的消息及其相关联的数据与数值相加。可利用填充来提高消息验证过程的安全性,因为填充可以是必须由彼此相互知晓的移动设备104和交易管理服务器102来执行的另一功能,它需要由未经认证的实体来复制,以在无需认证的情况下成功地发送或接收数据消息。对于相关领域技术人员来说显而易见的是,步骤1112可以作为可选的步骤。在一些实施例中,可在过程1110的一些情况下应用步骤1112。例如,可在参考计数的某些增量处对经加密的消息进行填充。

[0127] 在步骤1114中,处理单元204生成参考认证码。可基于经加密的消息(如果适用的话,经填充的)、使用一个或多个规则或算法(例如存储在步骤1102中)来生成参考认证码。在一些实施例中,参考认证码可以是密钥或者可以是通过将密钥应用到经加密的数据上而生成的值。在步骤1116中,处理单元204对在RNS消息中接收的消息认证码进行验证。对消息认证码进行验证可包括将该码与所生成的参考认证码进行比较,以作为当接收的数据消息源于经认证的来源(例如交易管理服务器102)时的另一种识别方法。

[0128] 如果消息认证码验证失败,则过程1100可前进至步骤1110,在那里执行失败处理。如果消息认证码验证通过,那么在步骤1118中,处理单元204对包括在所接收的数据消息中的经加密的消息进行解密。可使用例如在步骤1102中存储在移动设备104中的一个或多个加密密钥/解密密钥、规则和/或算法对消息进行解密。例如,可利用存储在存储器212的加密应用程序410中的加密密钥414来对经加密的消息进行解密。在步骤1120中,处理单元204基于经解密的消息的内容来适当地执行一个或多个动作。例如,如果经解密的消息包括一次性密钥306,则可将一次性密钥306存储在卡片数据库208的合适支付文件302中,由此可利用高级存储密钥对卡片数据库208进行加密。

[0129] 高级存储密钥

[0130] 图12示出了移动设备104生成并利用高级存储密钥来将数据(例如在不使用安全元件的情况下安全存储到移动设备中并可在移动设备中被安全访问的支付文件302和其它数据)安全地存储到移动设备104中。

[0131] 存储在移动设备104的存储器212中的设备信息可包括三条或更多条设备信息1202,如图12中所示的设备信息1202a、1202b和1202c。每条设备信息1202可与移动设备104相关联。在一些情况下,每条设备信息1202对于移动设备104来说是唯一的。在其它情况下,一条或多条设备信息1202对于移动设备104来说不是唯一的(例如型号),但一起使用的三条设备信息1202对于移动设备104来说也可以是唯一的(例如唯一性组合)。设备信息1202可以是在移动设备104的寿命期间不发生改变的数据。

[0132] 移动设备104的处理单元204可基于三条设备信息1202a、1202b和1202c来生成移

动设备指纹1204。移动设备指纹1204可以是对于移动设备104来说唯一的值，并且可利用存储在存储器212中(例如包括在MPA 404的程序代码中)的一个或多个规则或算法来生成移动设备指纹1204。移动设备指纹1204可以是例如数字值、十六进制值、字符串等。

[0133] 处理单元204还可被配置为使用移动设备指纹1204来生成多元值1208。可通过对移动设备指纹1204与MPA 404的实例标识符408以及随机值1206进行组合来生成多元值。随机值1206可以是由处理单元204生成的随机值或伪随机值。在一些情况下，可根据存储在存储器212中的一个或多个规则或算法来生成随机值1206。还可利用例如存储在MPA 404的程序代码406中的一个或多个规则或算法来执行对移动设备指纹1204、实例标识符408和随机值1206的组合。使用实例标识符408来生成多元值可导致对与MPA 404的实例相关联的数据进行安全存储的能力，以使多次安装MPA 404也无法访问由MPA 404的其它实例存储的数据。

[0134] 处理单元204可随后通过对多元值1208应用被存储在加密应用程序410中的加密密钥414来生成高级存储密钥1210。在一些情况下，可通过利用加密密钥414对多元值1208进行解密来生成高级存储密钥1210。在其它情况下，高级存储密钥1210可以是利用加密密钥414对多元值1208进行加密所得到的值。在一些实施例中，可利用加密密钥414和多元值1208执行白盒加密来生成高级存储密钥1210。

[0135] 一旦生成高级存储密钥1210，则处理单元204可使用高级存储密钥1210来对本地数据库1210进行加密。本地数据库1210可以包括，例如，卡片数据库208、一个或多个支付文件302、部分存储器212或者其它合适的数据源。在一些情况下，本地数据库1210可以是移动设备104中的另一个数据库的一部分，例如卡片数据库208的一部分。例如，卡片数据库208可包括多个本地数据库1212，例如针对MPA 404的每个实例的、用于存储与实例相关联的支付文件302的独立本地数据库1212。所得到的经加密的本地数据库1214由此可以安全地存储数据，除了包括实例标识符408的MPA 404的特定实例外，该数据不能被位于移动设备104内部或外部的任何其它应用程序访问。因此，经加密的本地数据库可理想地存储支付凭证304、一次性密钥306和其它账户数据，并可在不使用安全元件的情况下提供对敏感账户信息的安全存储。

[0136] 在一些实施例中，存储密钥还可被使交易管理服务器102用于向移动设备提供经加密的数据，以将数据存储在经加密的本地数据库1214中。例如，移动设备104的传送单元206可将所产生的随机值1206传送给交易管理服务器102。在一些情况下，实例标识符408也可被发送给交易管理服务器102，或者可由交易管理服务器102事先拥有(例如在注册MPA 404期间)。交易管理服务器102然后可自身生成高级存储密钥1210，利用高级存储密钥1210对将要提供给移动设备104的数据(例如支付凭证304、一次性密钥等)进行加密，然后向移动设备104发送经加密的数据。移动设备104然后可将已加密的数据存储在经加密的本地数据库1214中。

[0137] 用于生成支付交易中的支付凭证的第一示例性方法

[0138] 图13示出用于生成支付交易中的支付凭证的方法1300，其包括在不带有安全元件的移动设备104中利用两个应用密文来安全地使用支付凭证。

[0139] 在步骤1302中，至少将一次性密钥(例如，一次性密钥306)存储在与交易账户相关联的存储器(例如支付文件302)中。在一些实施例中，存储器302可以是移动通信设备(例

如，移动设备104)中的非安全元件型存储器。在步骤1304，个人身份码(PIN)被接收设备(例如，接收单元202和/或输入单元214)接收。

[0140] 在步骤1306中，由处理设备(例如处理单元204)来确定第一会话密钥(例如第一会话密钥308)。在步骤1308，由处理设备204至少基于所存储的一次性密钥306和所接收的PIN码来生成第二会话密钥(例如第二会话密钥310)。

[0141] 在步骤1310中，由处理设备204至少基于第一会话密钥308来生成第一应用密文。在步骤1312中，由处理设备204至少基于第二会话密钥310来生成第二应用密文。

[0142] 在步骤1314中，由传送设备(例如，传送单元206)至少发送第一应用密文和第二应用密文，以供支付交易中使用。在一些实施例中，可将第一应用密文和第二应用密文发送给销售点设备(例如，销售点110)。在一个实施例中，方法1300可进一步包括：将与交易帐户相关联的卡片主密钥存储在存储器302中，其中确定第一会话密钥308包括由处理设备204至少基于存储的卡片主密钥来生成第一会话密钥308。

[0143] 在一些实施例中，方法1300还可包括：将应用交易计数(例如，应用交易计数312)存储在存储器302中，其中，确定第一会话密钥308包括由处理设备204至少基于所存储的应用交易计数312来生成第一会话密钥308。在一个实施例中，在生成第二会话密钥310之前，由处理设备204对所接收的PIN进行验证。在又一实施例中，处理设备204可被配置为在所接收的PIN验证失败时生成无效的第二会话密钥310。

[0144] 用于生成支付交易中的支付凭证的第二示例性方法

[0145] 图14示出了用于生成支付交易中的支付凭证的方法1400，其包括在移动设备不使用安全元件的情况下利用两个应用密文对由移动设备104生成的支付凭证进行验证。

[0146] 在步骤1402中，至少将卡片主密钥(例如，第一卡片主密钥612)存储在与交易账户相关联的存储器(例如，帐户文件602)中。在步骤1404中，由处理设备(例如处理设备504)至少基于存储的卡片主密钥612来生成第一会话密钥(例如第一会话密钥606)。在步骤1406中，由处理设备504生成第二会话密钥(例如第二会话密钥608)。

[0147] 在步骤1408中，由处理设备504至少基于第一会话密钥606来生成第一应用密文。在步骤1410中，由处理设备504至少基于第二会话密钥608来生成第二应用密文。在步骤1412中，由传送设备(例如传送单元506)至少发送第一应用密文和第二应用密文，以供在支付交易中使用。

[0148] 在一个实施例中，方法1400可进一步包括：将与交易账户相关联的交易账户序列号存储在存储器602中，其中，第一会话密钥还基于所存储的交易帐户序列号。在一些实施例中，方法1400还可包括：将与交易账户相关联的第二卡片主密钥(例如第二卡片主密钥614)存储在存储器602中，其中，第二会话密钥608至少基于所存储的第二卡片主密钥614。

[0149] 在一个实施例中，方法1400可进一步包括：由接收设备(例如接收单元502)接收第一对应应用密文和第二对应应用密文；由所述处理设备，(i)基于生成的第一应用密文来对接收的第一对应应用密文进行验证，以及(ii)基于生成的第二应用密文来对接收的第二对应应用密文进行验证；以及由传送设备506传送验证结果，以供支付交易中使用。在另一实施例中，可从销售点设备(例如销售点110)接收第一对应应用密文和第二对应应用密文。在再一实施例中，将验证结果发送给与交易帐户相关联的金融机构(例如发行方106)。

[0150] 用于处理数据消息的示例性方法

[0151] 图15示出了用于处理数据消息(例如,经由远程通知服务接收的远程通知消息)的方法1500,其包括在移动设备不使用安全元件的情况下由移动设备104对数据消息进行接收和验证。

[0152] 在步骤1502中,至少将加密密钥存储在存储器(例如,存储器212)中。在一些实施例中,存储器212可以是移动通信设备(例如移动设备104)中的非安全元件型存储器。在步骤1504中,由接收设备(例如接收单元202)接收数据消息,其中数据消息可至少包括经加密的消息和消息认证码,其中利用经加密的消息的至少一部分来生成消息认证码。在一些实施例中,数据消息可以是经由远程通知服务来接收的远程通知服务消息。

[0153] 在步骤1506中,由处理设备(例如处理单元204)至少利用包括在接收的数据消息中的经加密的消息的一部分来生成参考认证码。在一个实施例中,存储器212还可包括一个或多个认证码生成规则,并且可基于将存储的一个或多个认证码生成规则应用于包括在接收的数据消息中的经加密消息的一部分上来生成参考认证码。在步骤1508中,由处理设备204基于比对着生成的参考认证码来检查包括在所接收的数据消息中的消息认证码,来对所接收的数据消息进行验证。在一些实施例中,存储器还可包括参考计数,所接收的数据消息还可包括消息计数,可由处理设备204基于比对着所存储的参考计数来检查包括在所接收的数据消息中的消息计数,来进一步验证所接收的数据消息。

[0154] 在步骤1510中,由处理设备204利用存储的加密密钥来对包括在数据消息中的经加密的消息进行解密,以得到经解密的消息。在一个实施例中,经解密的消息可包括以下各项中的至少一个:在支付交易中使用的数字化卡片文件(例如,支付凭证304)和一次性密钥(例如一次性密钥306)。在一些实施例中,方法1500还可包括:由处理设备204基于一个或多个数据格式规则对经解密的消息的数据格式进行检查。

[0155] 在一个实施例中,方法1500可进一步包括:响应于所接收的数据消息,由传送设备(例如,传送单元206)发送接收通知。在另一实施例中,方法1500可进一步包括:由处理设备204基于经解密的消息来执行一个或多个动作;由处理设备204由于或者基于所执行一个或多个动作来生成返回消息;由处理设备204利用存储的加密密钥对所生成的返回消息进行加密,以获得经加密的返回消息;以及由处理设备204至少利用经加密的返回消息的一部分来生成返回认证码,其中所发送的接收通知包括经加密的返回消息和返回认证码。在又一实施例中,存储器212可进一步包括返回计数,并且所发送的接收通知可进一步包括返回计数。

[0156] 在一些实施例中,方法1500还可包括:由处理设备204利用填充密钥对包括在接收的数据消息中的经加密的消息进行填充,其中经加密消息中用于生成参考认证码的那部分为经填充的加密消息。在另一实施例中,填充密钥可以是加密密钥。在又一实施例中,存储器212还可包括认证码填充算法,并且利用填充密钥对经加密消息进行填充可包括:基于将填充密钥应用于认证码填充算法来对经加密的消息进行填充。

[0157] 用于构建高级存储密钥的示例性方法

[0158] 图16示出了用于构建高级存储密钥的方法600,高级存储密钥用于在移动设备不使用安全元件的情况下对移动设备104中的本地数据进行安全加密和存储。

[0159] 在步骤1602中,至少将与移动通信设备(例如移动设备104)相关联的设备信息(例如,设备信息402)、与第一应用程序(例如移动支付应用程序404)相关联的程序代码(例如

程序代码406)、以及与第二应用程序(例如加密应用程序410)相关联的程序代码(例如程序代码412)存储在移动通信设备104的存储器(例如存储器212)中,其中与第一应用程序404相关联的程序代码406至少包括实例标识符(例如实例标识符408),并且与第二应用程序410相关联的程序代码412至少包括第一密钥(例如加密密钥414)。

[0160] 在一些实施例中,设备信息402可包括一个或多个与移动通信设备104相关联的唯一性标识符。在一个实施例中,实例标识符408对于第一应用程序404的实例来说可以是唯一的。在一些实施例中,第二应用程序410可被配置为利用第一密钥来执行白盒密码技术。在一个实施例中,第一密钥可以是动态密钥。在一些实施例中,与第二应用程序410相关联的程序代码412可被包括在与第一应用程序404相关联的程序代码406中。在其它实施例中,第二应用程序410可以是第一应用程序404的可执行功能。

[0161] 在步骤1604中,由处理设备(例如处理单元204)基于存储的设备消息、经由执行与第一应用程序404相关联的程序代码406,来生成与移动通信设备104相关联的设备指纹(例如移动设备指纹1204)。在步骤1606中,由处理设备204经由执行与第一应用程序404相关联的程序代码406,来生成随机值(例如随机值1206)。在一些实施例中,随机值1206可以是随机数或伪随机数。

[0162] 在步骤1608中,由处理设备204至少基于所生成的设备指纹1204、所生成的随机值1206以及包括在与第一应用程序404相关联的程序代码中的实例标识符408,来生成多元值(例如多元值1208)。在步骤1610中,由处理设备204利用存储在与第二应用程序410相关联的程序代码412中的第一密钥、经由执行与第二应用程序410相关联的程序代码412,来对构建的多元值1208进行解密,以得到存储密钥(例如高级存储密钥1210)。

[0163] 在一些实施例中,方法1600可进一步包括:将保护数据存储在移动通信设备104的本地数据库(例如本地数据库1212)中;由处理设备204利用存储密钥1210对存储在本地数据库1212中的保护数据进行加密。在一个实施例中,方法1600还可包括:将与第一应用程序404相关联的程序数据存储在数据库212中;以及将所生成的随机值1206存储在与第一应用程序404相关联的程序数据中。

[0164] 在一个实施例中,方法1600还可包括:由传送设备(例如传送单元206)至少发送随机值1206;由接收设备(例如接收单元202)接收一个或多个经加密的参数,其中利用存储密钥1210分别对一个或多个经加密的参数进行加密;以及,将所接收的一个或多个经加密的参数存储在移动通信设备104的本地数据库1212中。在另一实施例中,可将存储密钥1210发送给第三方(例如交易管理服务器102),并可从第三方102接收一个或多个经加密的参数。在某些其它实施例中,还可由传送设备206来发送实例标识符408。

[0165] 计算机系统架构

[0166] 图17示出了计算机系统1700,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的交易管理服务器102和移动设备104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1700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7、8、9A、9B、10A、10B、11和13-16的方法的模块和组件。

[0167] 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、小微型计算机、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。

[0168] 如本文中所讨论的处理器单元或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1718、可拆卸存储单元1722以及安装在硬盘驱动器1712中的硬盘。

[0169] 本公开的各种实施例都是根据本示例性计算机系统1700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。

[0170] 处理器设备1704可以是专用或通用处理器设备。处理器设备1704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1706。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1700还可包括主存储器1708(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1710。辅助存储器1710可包括硬盘驱动器1712和可拆卸存储驱动器1714(例如软盘驱动器、磁带驱动器、光盘驱动器，闪存等)。

[0171] 可拆卸存储驱动器1714可通过公知的方式来读取和/或写入可拆卸存储单元1718。可拆卸存储单元1718包括可由可拆卸存储驱动器1714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1714是软盘驱动器，那么可拆卸存储单元1718可以是软盘磁盘。在一个实施例中，可拆卸存储单元1718可以是非暂时性计算机可读记录介质。

[0172] 在一些实施例中，辅助存储器1710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1700中的其他类似设备，例如可拆卸存储单元1722和接口1720。这种设备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1722和接口1720。

[0173] 存储在计算机系统1700(例如存储在主存储器1708和/或辅助存储器1710)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)。数据可被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。

[0174] 计算机系统1700还可包括通信接口1724。通信接口1724可被配置为允许软件和数据在计算机系统1700与外部设备之间传递。示例性通信接口1724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1724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1726来传播，其中所述通信路径可被配置为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。

[0175] 计算机系统1700可进一步包括显示接口1702。显示接口1702可被配置为能在计算机系统1700和外部显示器1730之间传递数据。示例性的显示接口1702可包括高清晰度多媒体接口(HDMI)、数字视频接口(DVI)、视频图形阵列(VGA)等等。显示器1730可以是用于显示经由计算机系统1700的显示接口1702发送的数据的任何合适类型的显示器，其包括阴极射线管(CRT)显示器、液晶显示器(LCD)、发光二极管(LED)显示器、电容式触摸显示器、薄膜晶体管(TFT)显示器等等。

[0176] 计算机程序介质和计算机可用介质是指诸如主存储器1708和辅助存储器1717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1700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1708和/或辅助存储器1717中。计算机程序也可以经由通信接口1724来接收。这种计算机程序当执行时能够使计算机系统1700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1704执行这里所讨论的如图7、8、9A、9B、10A、10B、11及13-16所示的方法。因此，这种计算机程序可代表计算机系统1700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1714、接口1720和硬盘驱动器1712，或者利用通信接口1724而加载到计算机系统1700中。

[0177] 与本公开相一致的技术，除其他特征以外，提供了在不使用安全元件的情况下利用移动设备来处理支付交易的系统及方法，其包括对远程通知服务消息进行发送和验证，并利用高级存储密钥来对数据进行安全存储。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的而并非加以限制。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。

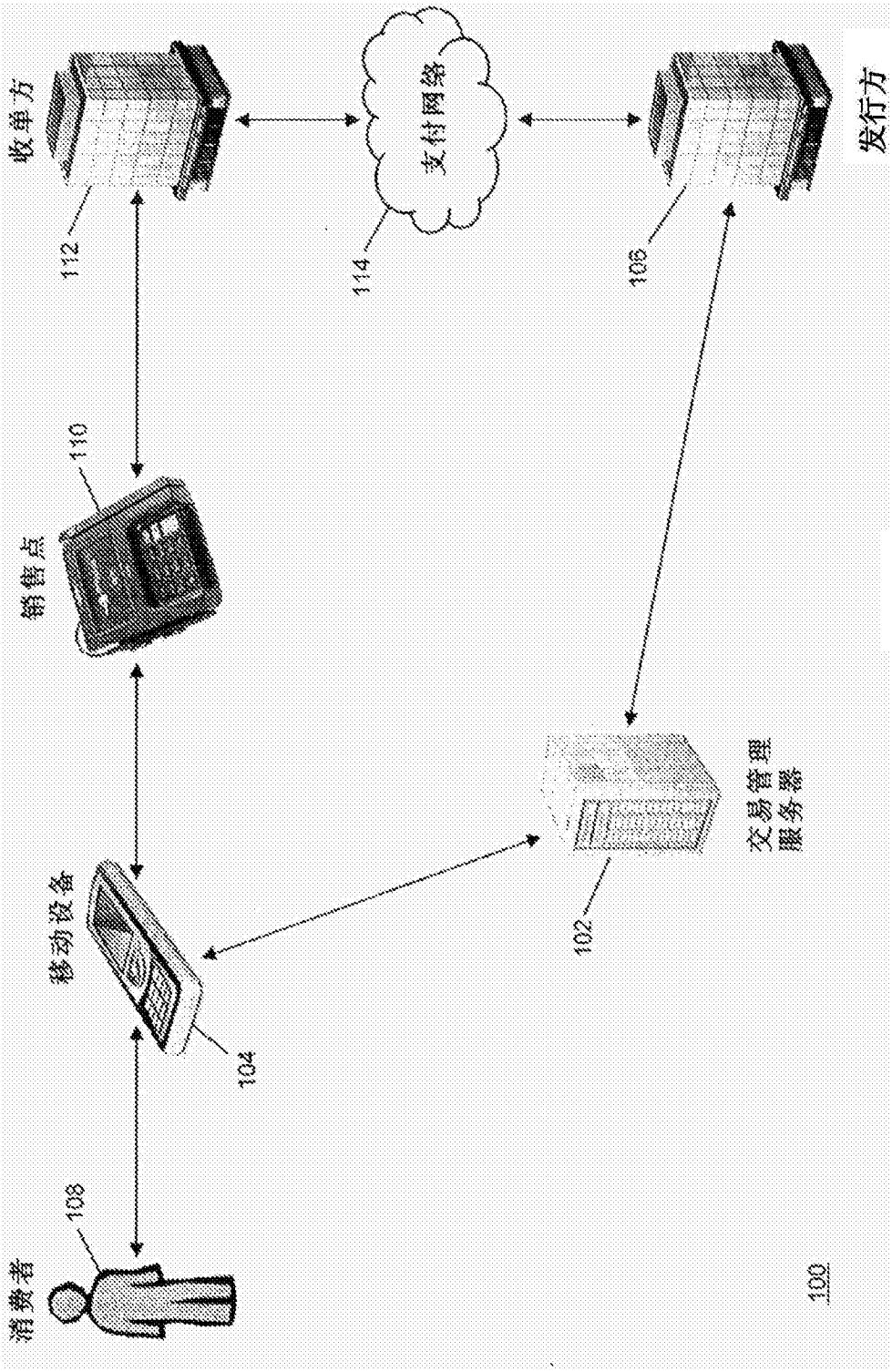
收单方
112
支付网络
114
发行方
116
销售点
110
移动设备
104
交易管理
服务器
102
消费者
108
100

图1

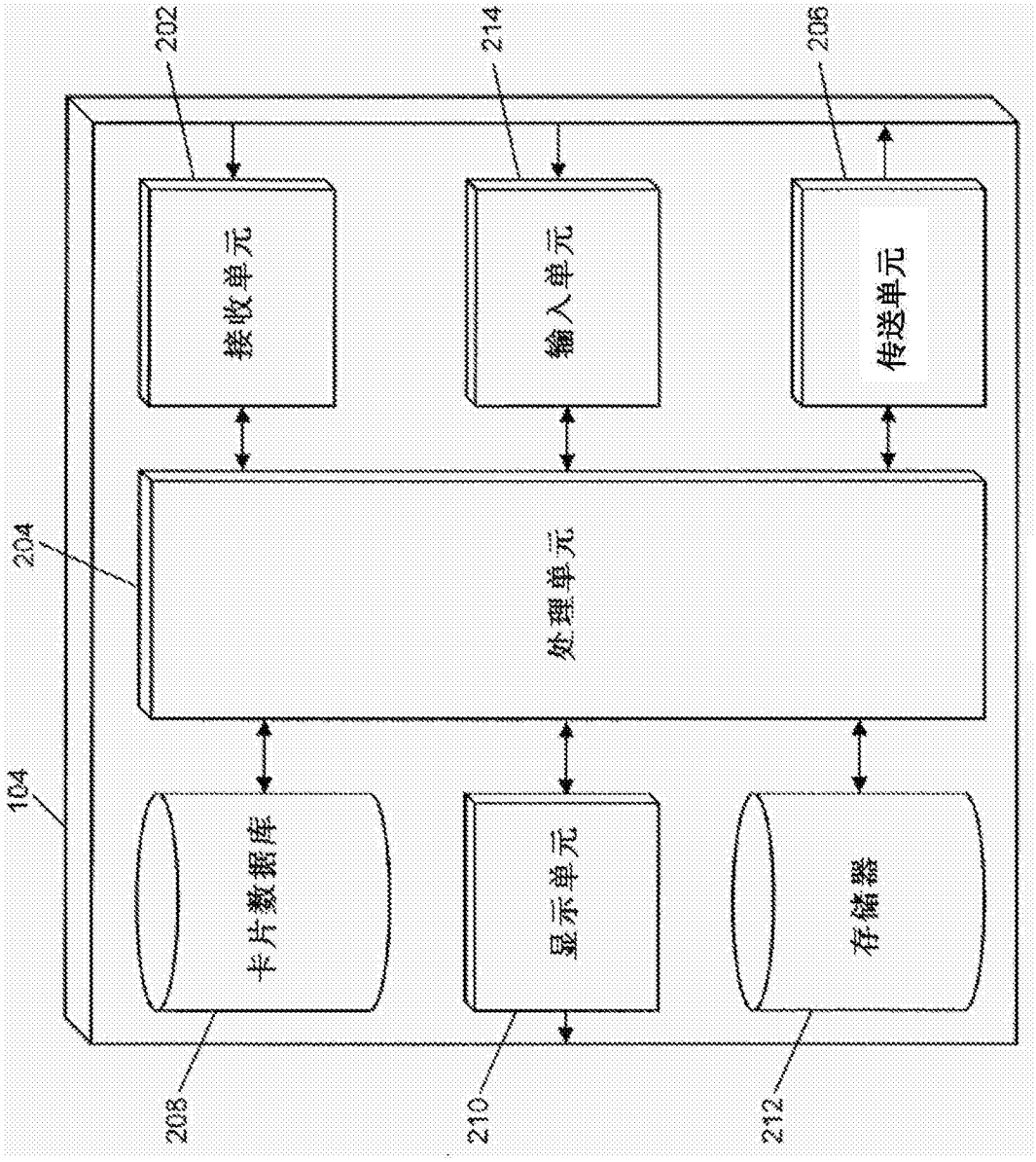
202
214
206
接收单元
输入单元
传送单元
处理单元
204
104
卡片数据库
显示单元
存储器
208
210
212

图2

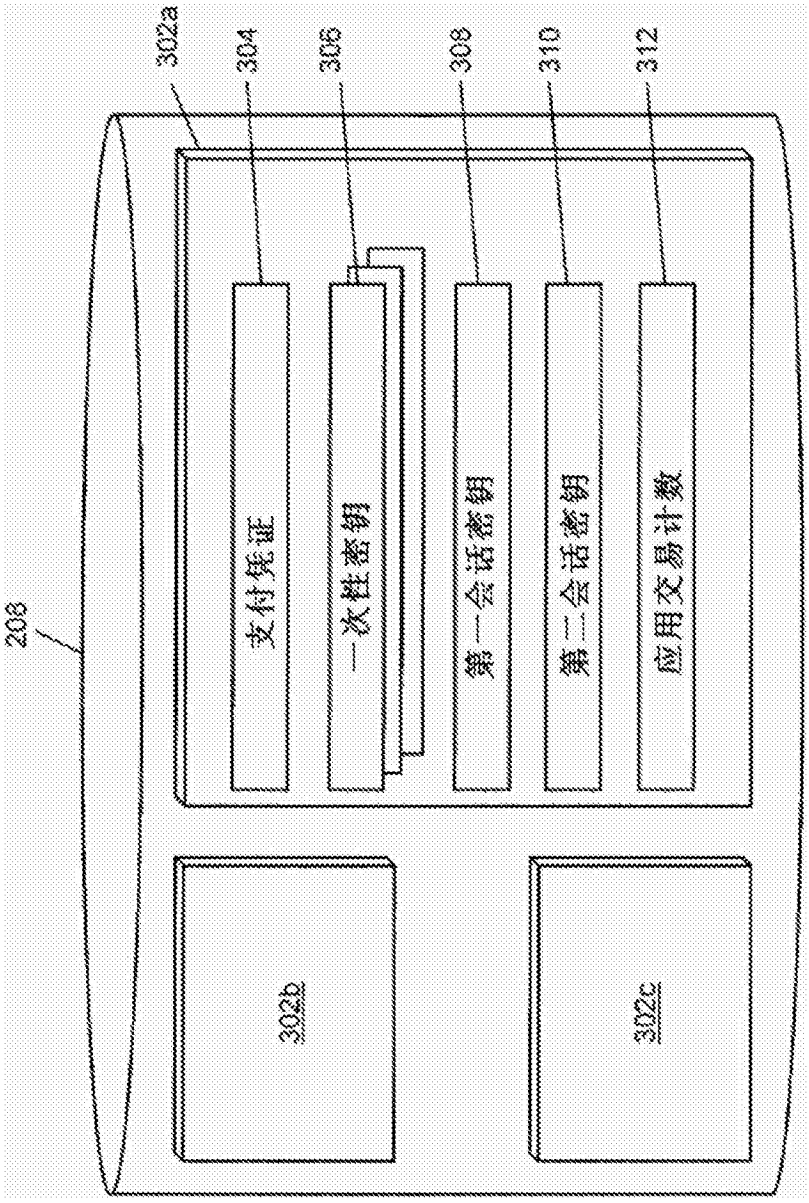
302a
304
306
308
310
312
208
支付凭证
一次性密钥
第一会话密钥
第二会话密钥
应用交易计数
302b
302c

图3

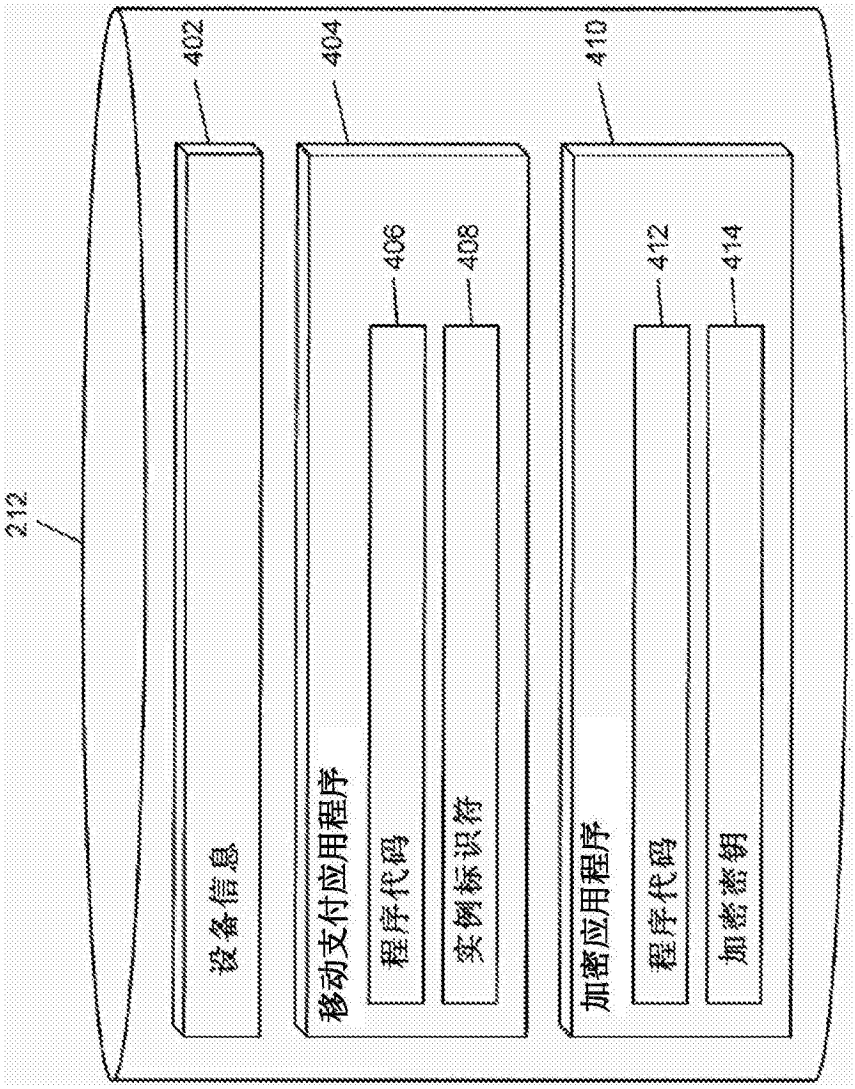
212
402
设备信息
404
移动支付应用程序
406
程序代码
408
实例标识符
410
加密应用程序
412
程序代码
414
加密密钥

图4

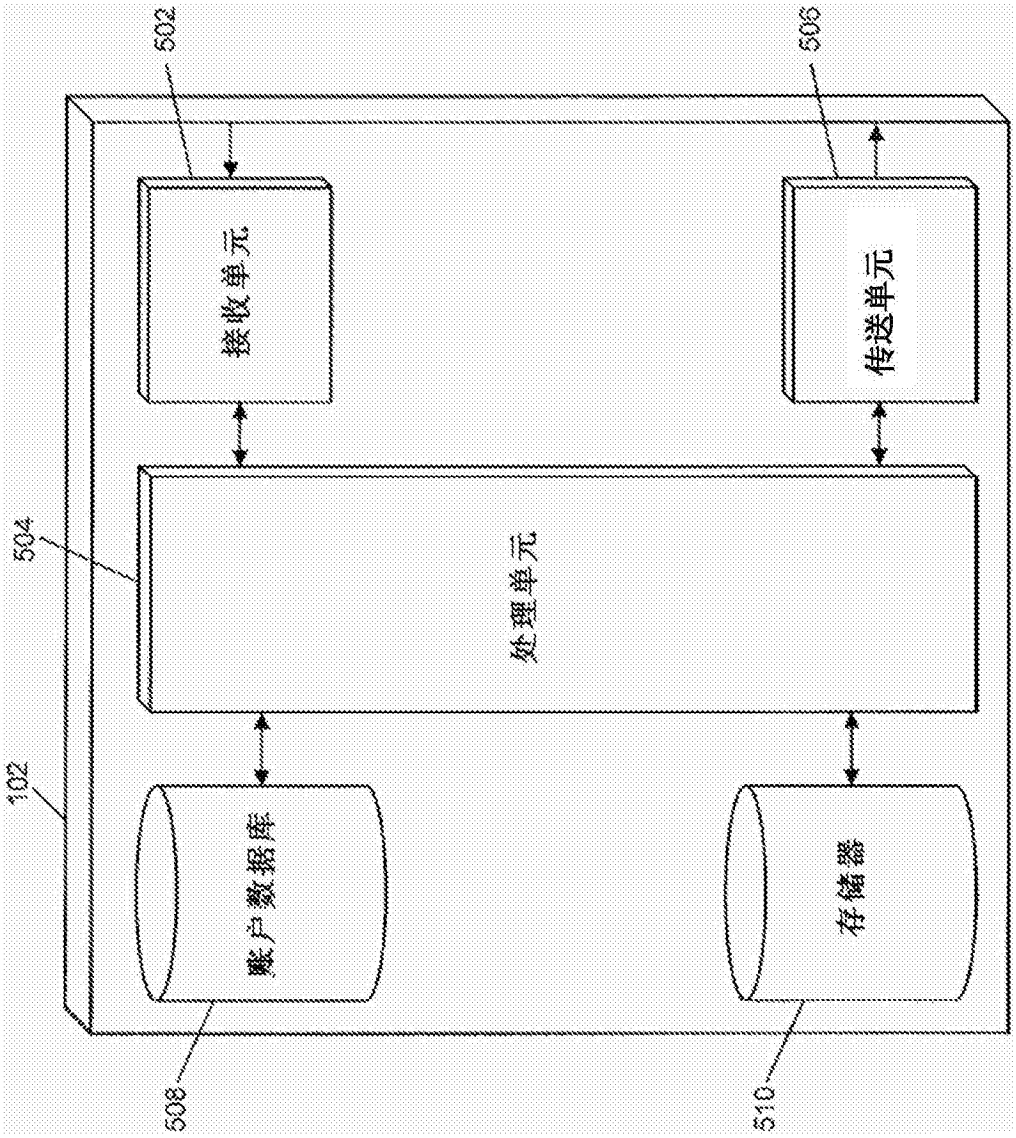

图5

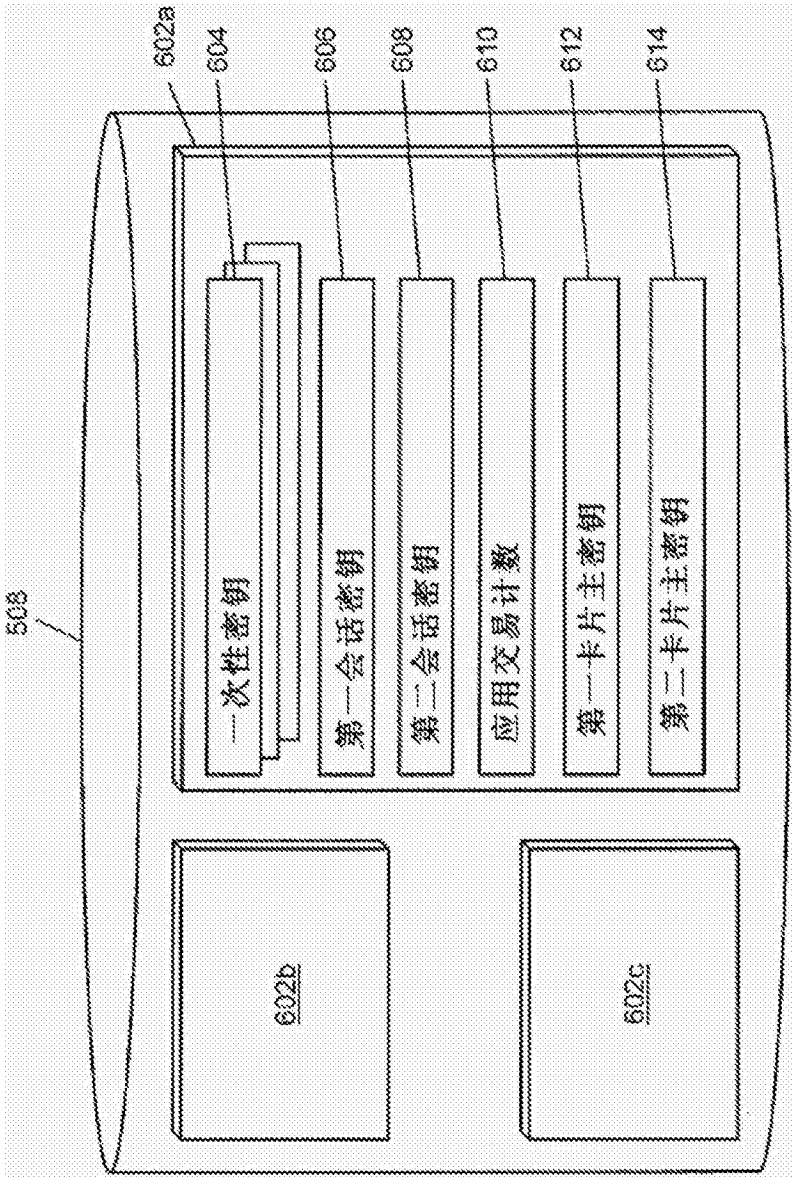
602a
604
606
608
610
612
614
一次性密钥
第一会话密钥
第二会话密钥
应用交易计数
第一卡片主密钥
第二卡片主密钥
602b
602c
508

图6

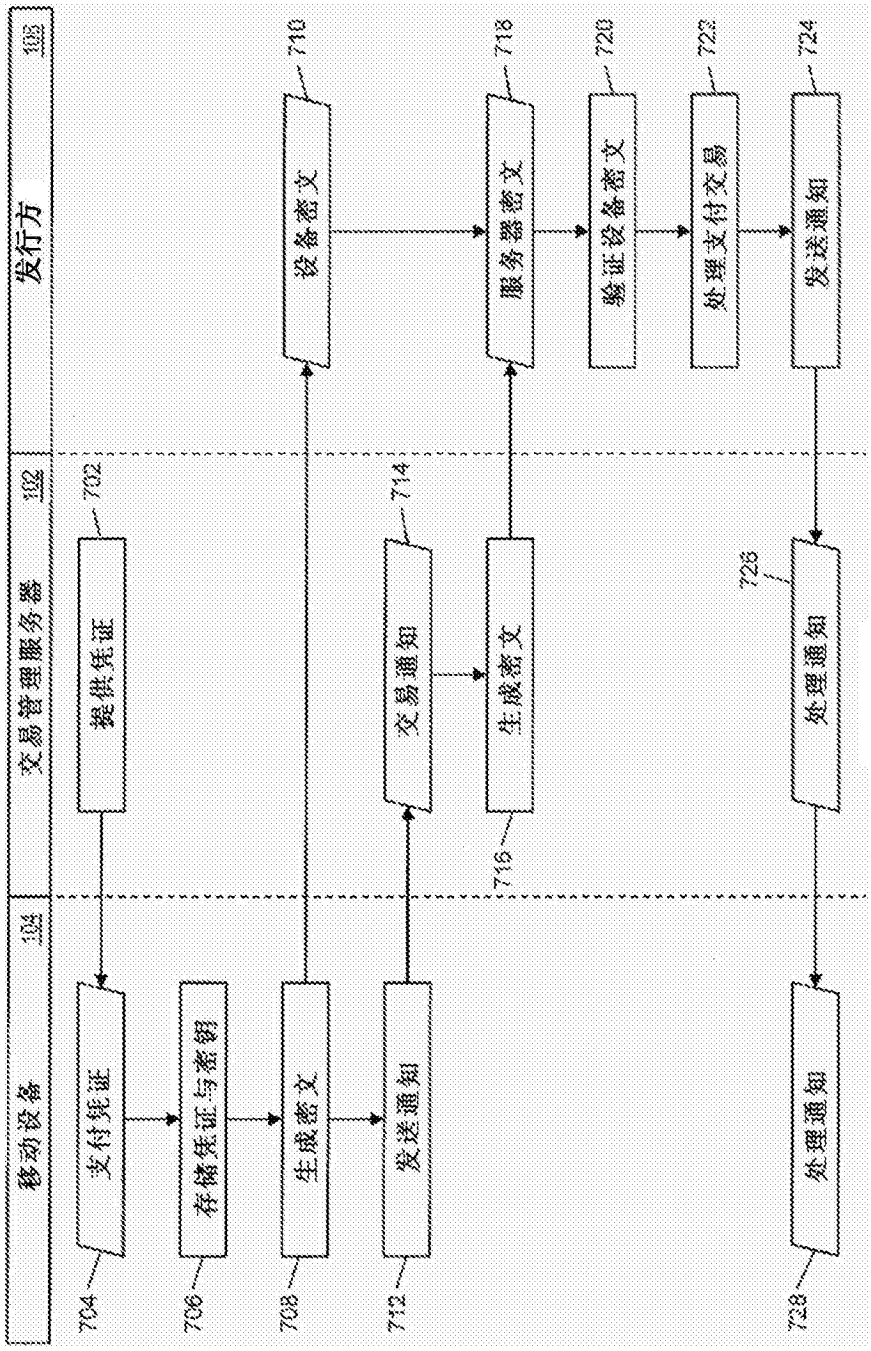
移动设备 104
交易管理服务器 102
发行方 103
提供凭证
702
支付凭证
704
存储凭证与密钥
706
生成密文
708
发送通知
712
交易通知
714
生成密文
716
设备密文
710
服务器密文
718
验证设备密文
720
处理支付交易
722
发送通知
724
处理通知
726
处理通知
728

图7

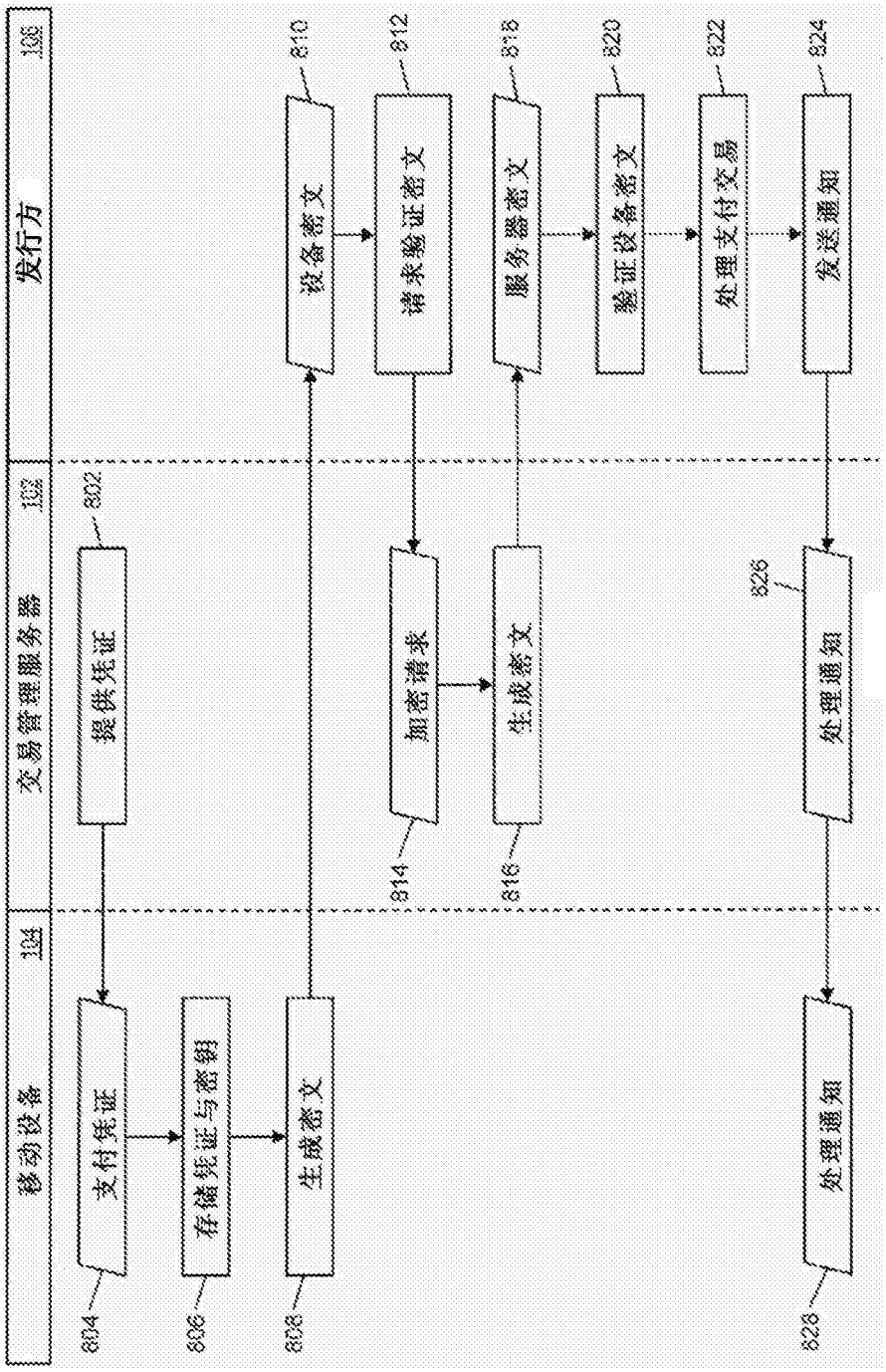
移动设备
104
交易管理服务器
102
发行方
106
802
提供凭证
804
支付凭证
806
存储凭证与密钥
808
生成密文
810
设备密文
812
请求验证密文
814
加密请求
816
生成密文
818
服务器密文
820
验证设备密文
822
处理支付交易
824
发送通知
826
处理通知
828
处理通知

图8

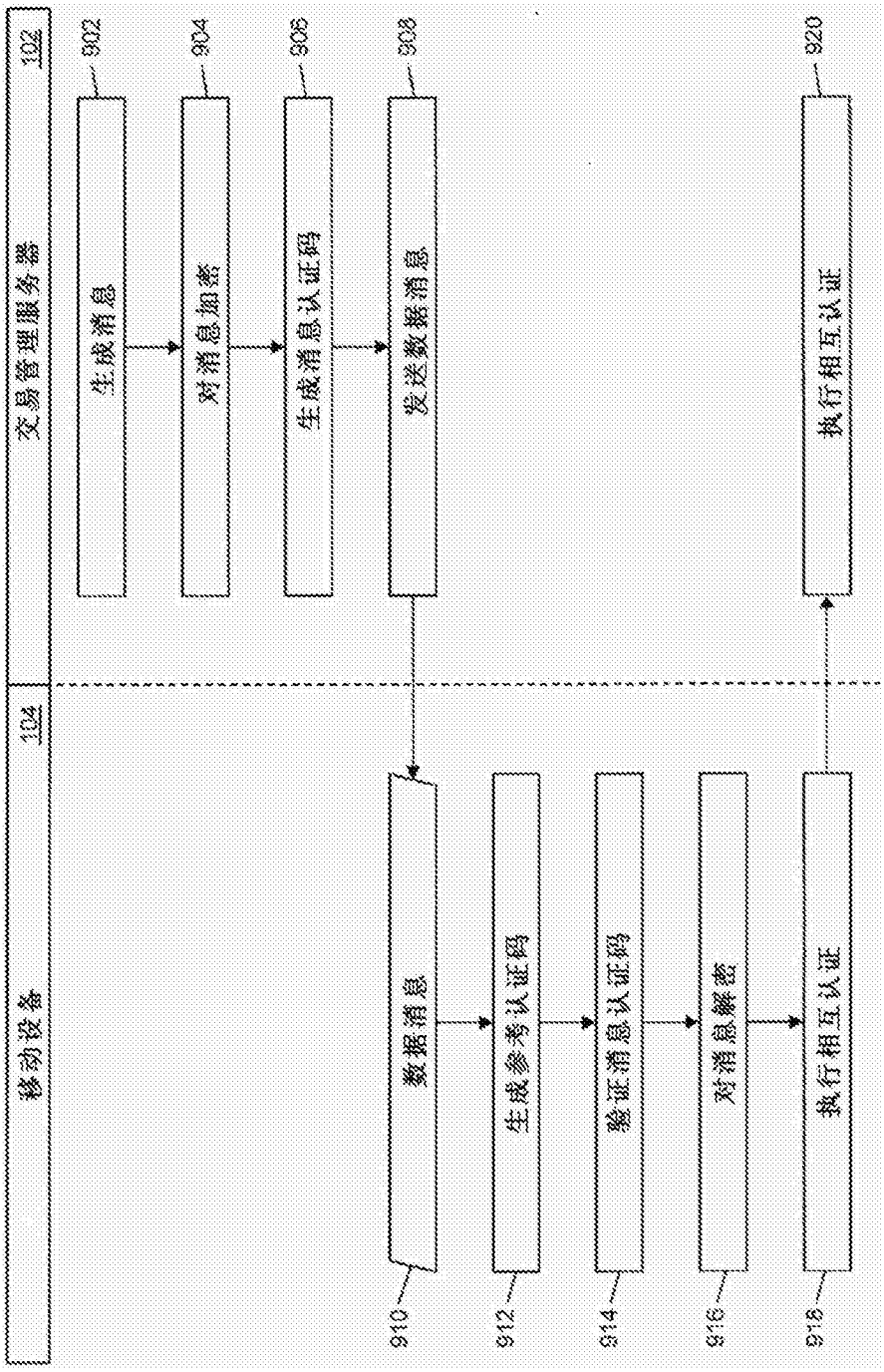
交易管理服务器
102
移动设备
104
902
生成消息
904
对消息加密
906
生成消息认证码
908
发送数据消息
920
执行相互认证
910
数据消息
912
生成参考认证码
914
验证消息认证码
916
对消息解密
918
执行相互认证

图9

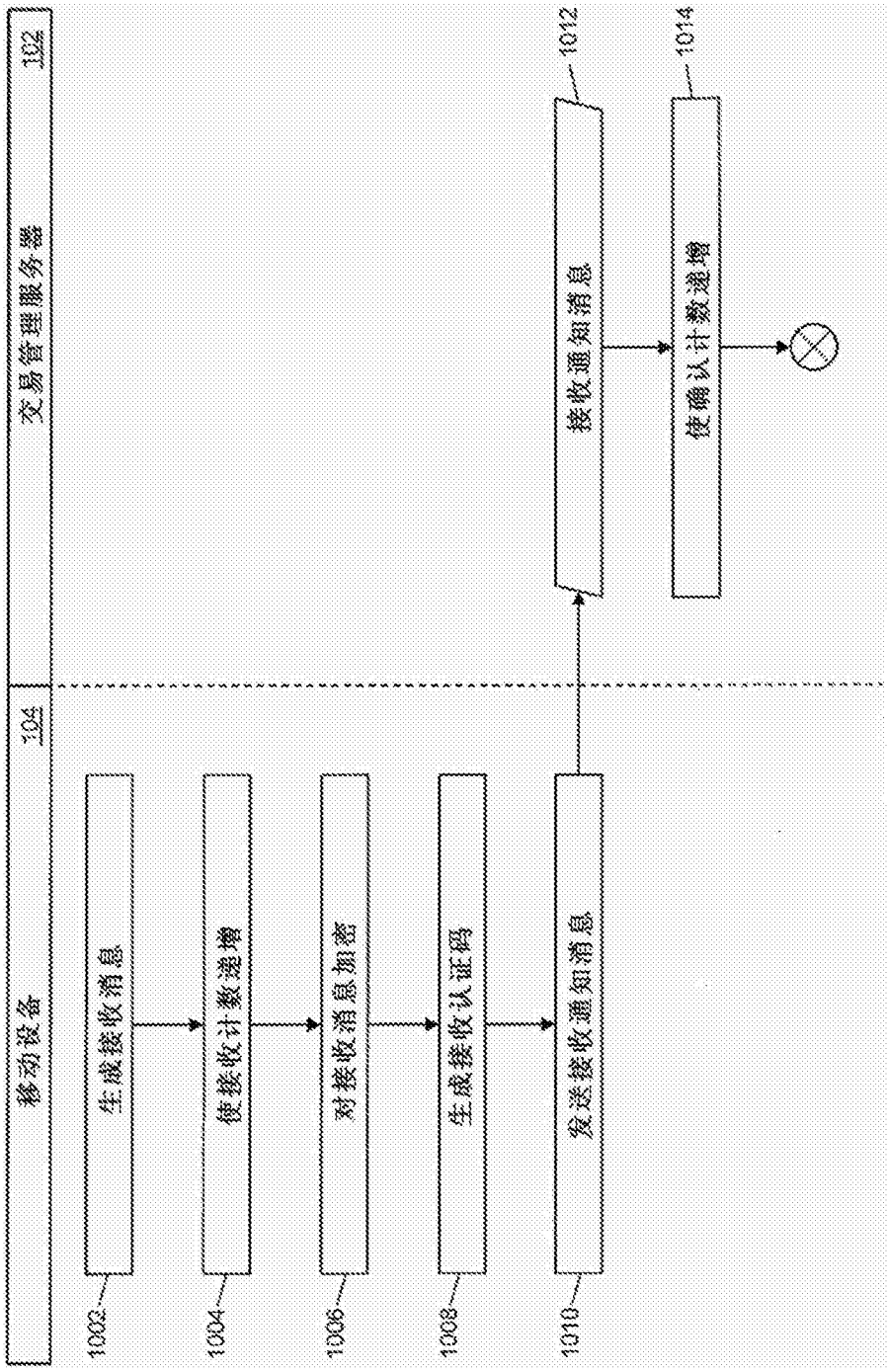
移动设备
104
交易管理服务器
102
生成接收消息
使接收计数递增
对接收消息加密
生成接收认证码
发送接收通知消息
接收通知消息
使确认计数递增
1002
1004
1006
1008
1010
1012
1014

图10A

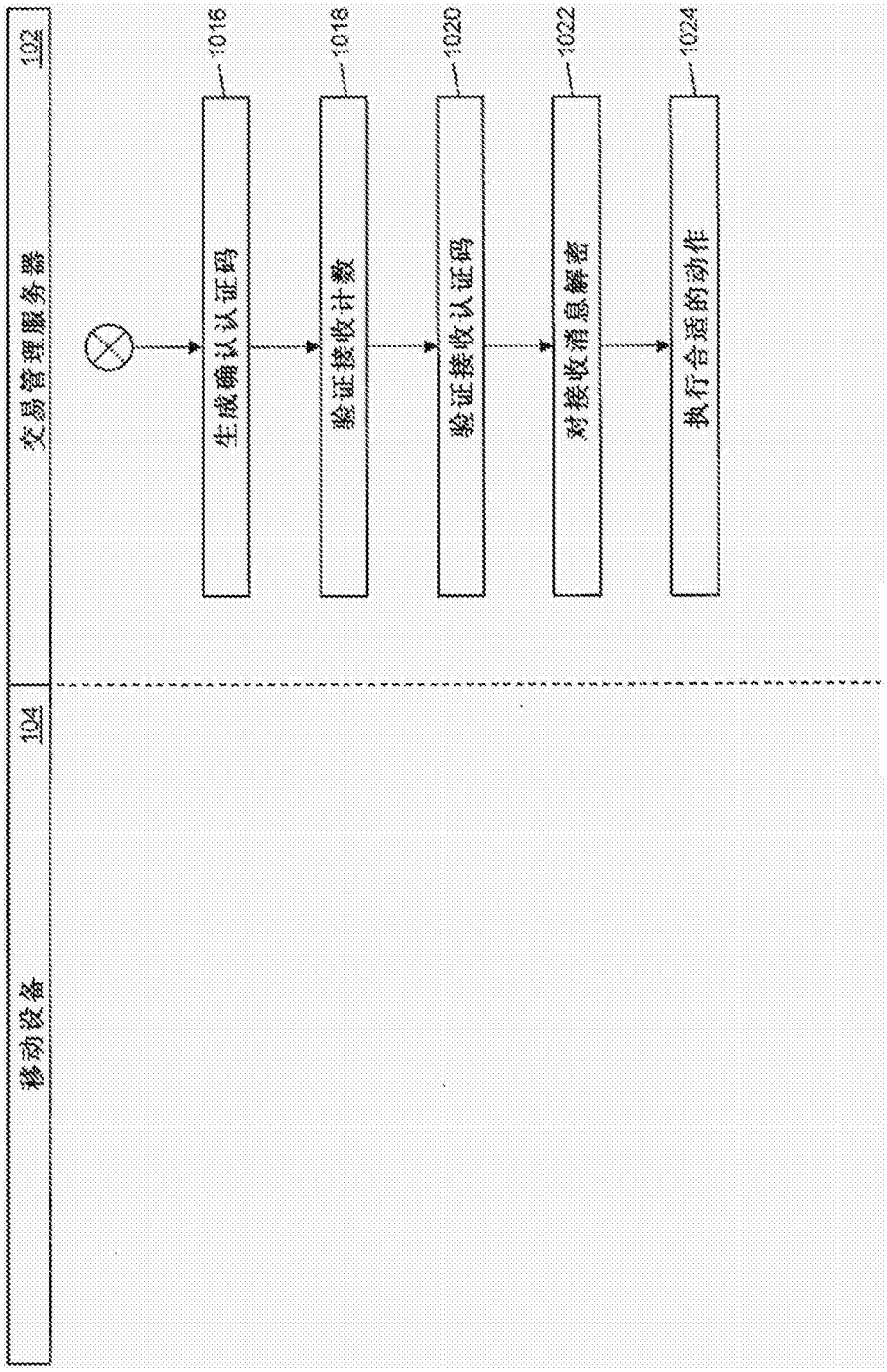
交易管理服务器
102
移动设备
104
1016
生成确认认证码
1018
验证接收计数
1020
验证接收认证码
1022
对接收消息解密
1024
执行合适的动作

图10B

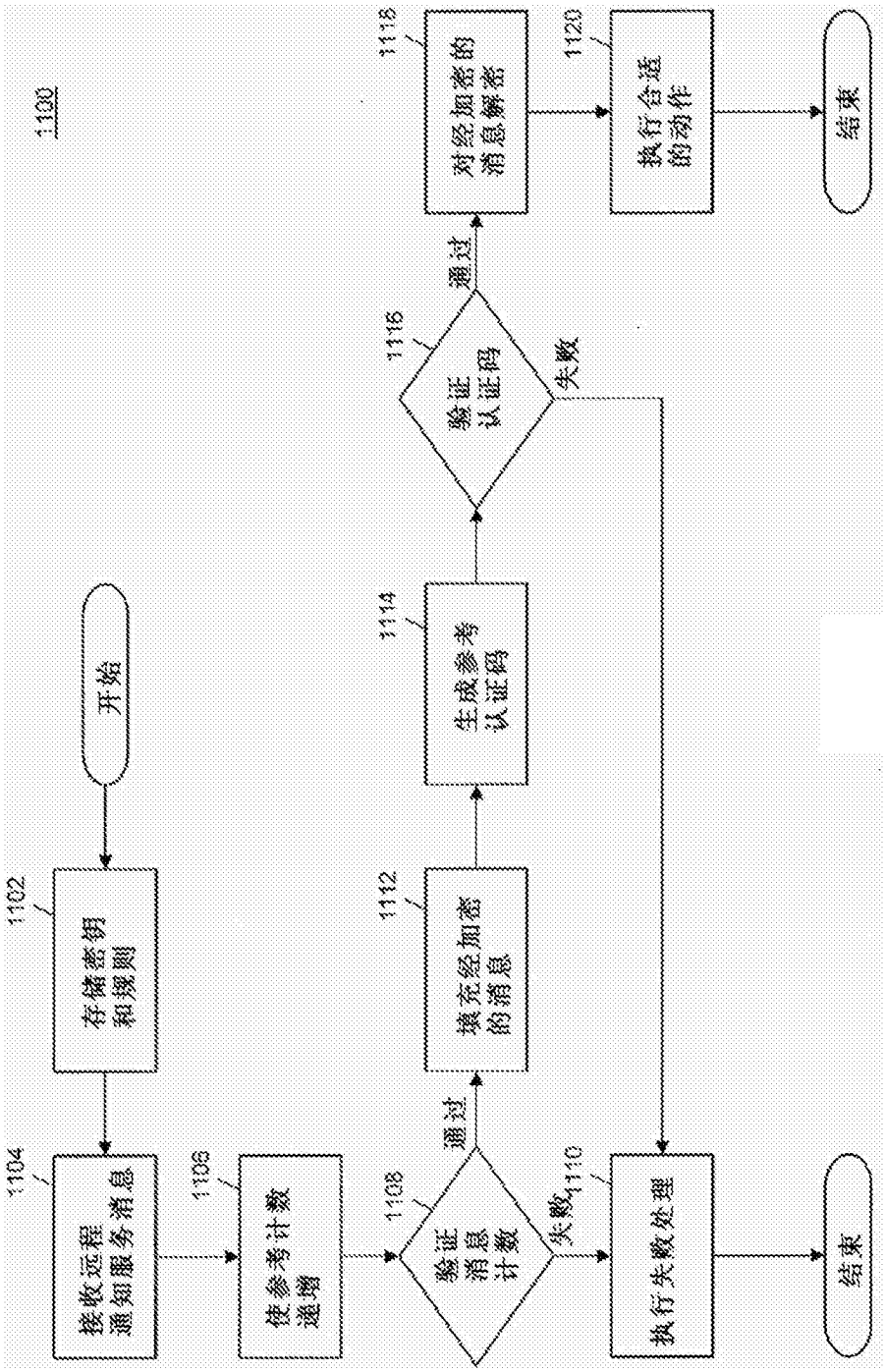
1100
开始
1102
存储密钥和规则
1104
接收远程通知服务消息
1106
使参考计数递增
1108
验证消息计数
失败
1110
执行失败处理
结束
通过
1112
填充经加密的消息
1114
生成参考认证码
1116
验证认证码
失败
通过
1118
对经加密的消息解密
1120
执行合适的动作
结束

图11

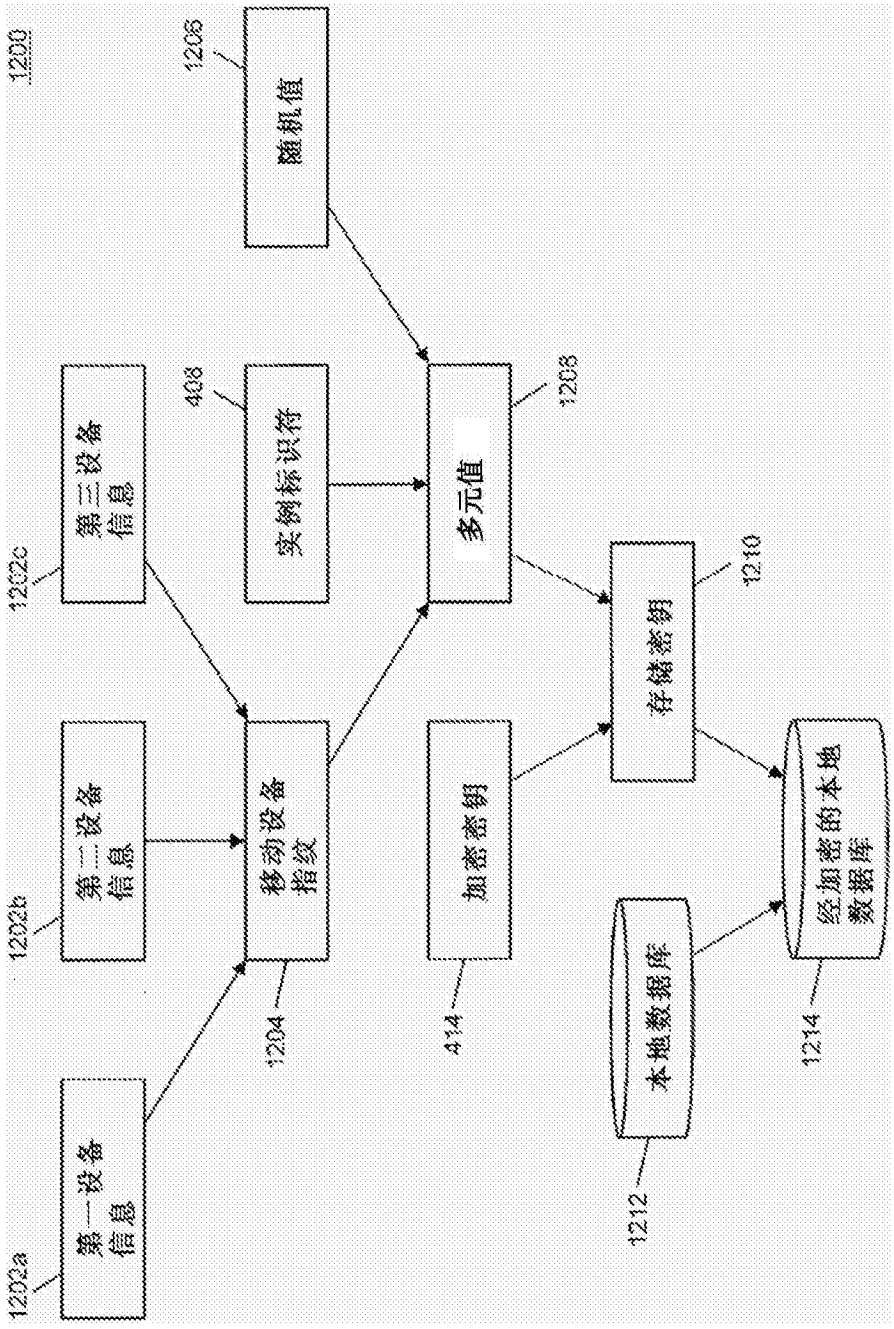
1206
随机值
1208
408
实例标识符
多元值
1202c
第三设备信息
1210
存储密钥
1202b
第二设备信息
移动设备指纹
加密密钥
经加密的本地数据库
本地数据库
1202a
第一设备信息
1204
414
1214
1212

图12

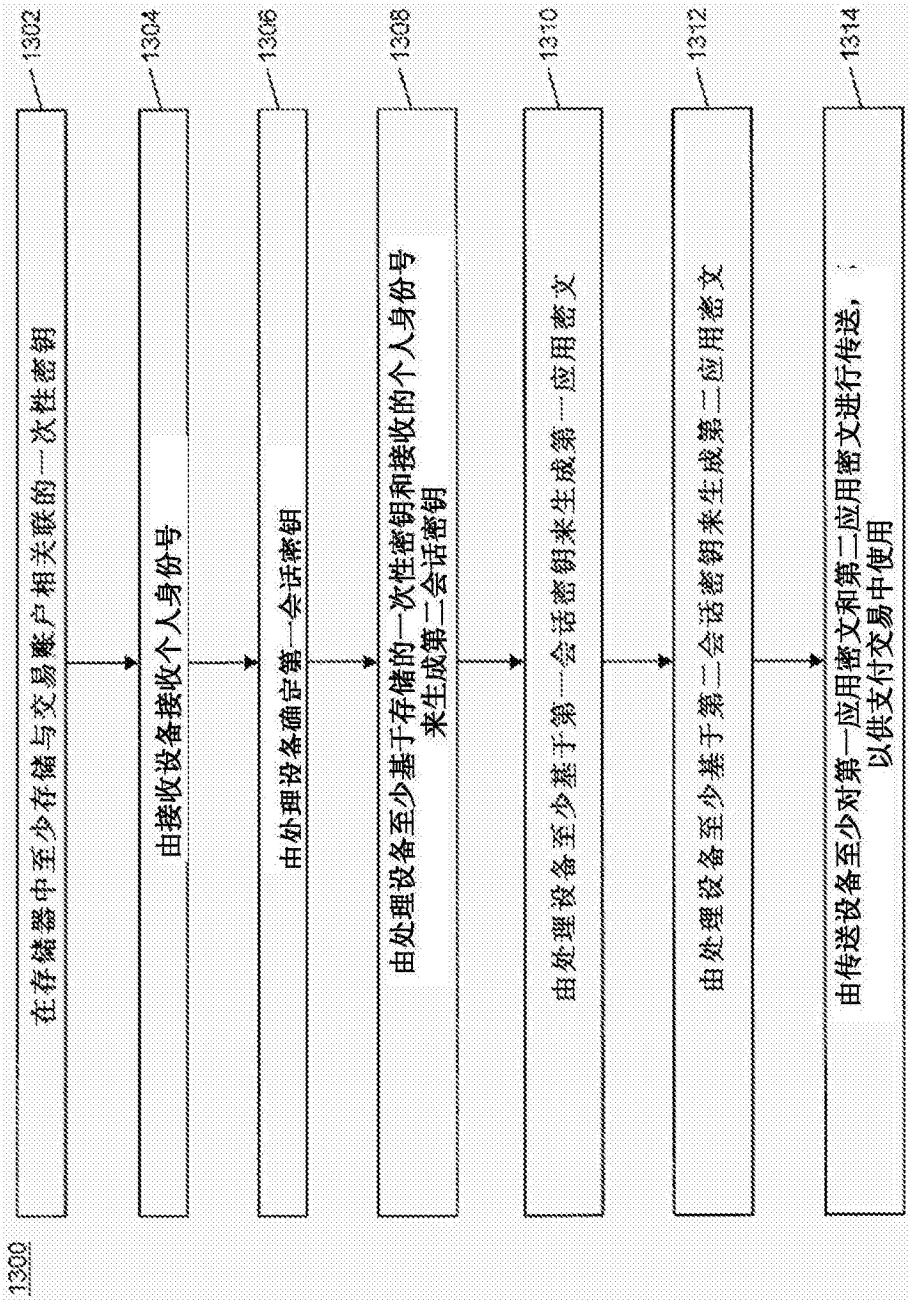
1300
1302
在存储器中至少存储与交易账户相关联的一次性密钥
1304
由接收设备接收个人身份号
1306
由处理设备确定第一会话密钥
1308
由处理设备至少基于存储的一次性密钥和接收的个人身份号来生成第二会话密钥
1310
由处理设备至少基于第一会话密钥来生成第一应用密文
1312
由处理设备至少基于第二会话密钥来生成第二应用密文
1314
由传送设备至少对第一应用密文和第二应用密文进行传送，以供支付交易中使用

图13

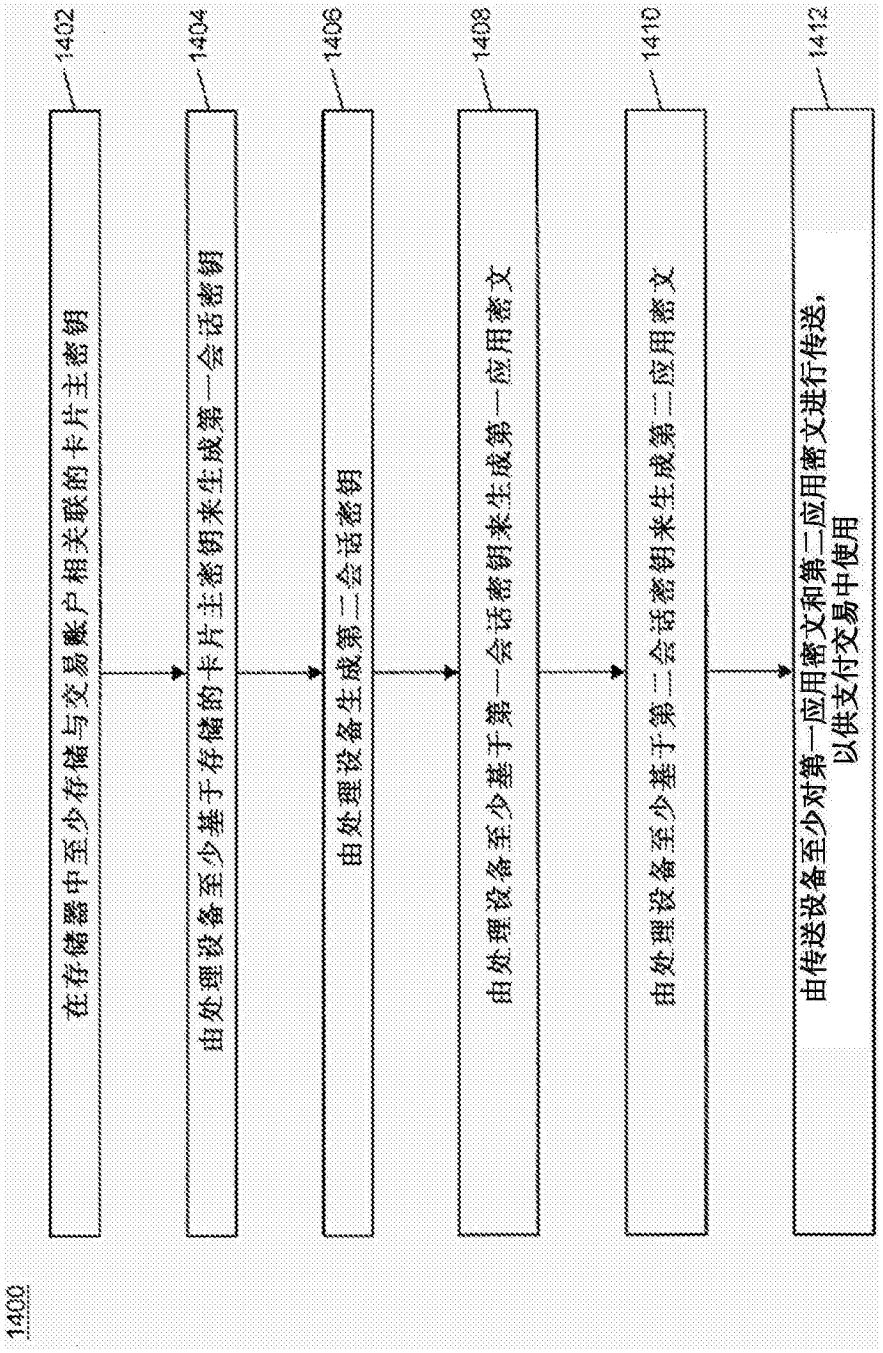
1400
1402
在存储器中至少存储与交易账户相关联的卡片主密钥
1404
由处理设备至少基于存储的卡片主密钥来生成第一会话密钥
1406
由处理设备生成第二会话密钥
1408
由处理设备至少基于第一会话密钥来生成第一应用密文
1410
由处理设备至少基于第二会话密钥来生成第二应用密文
1412
由传送设备至少对第一应用密文和第二应用密文进行传送，
以供支付交易中使用

图14

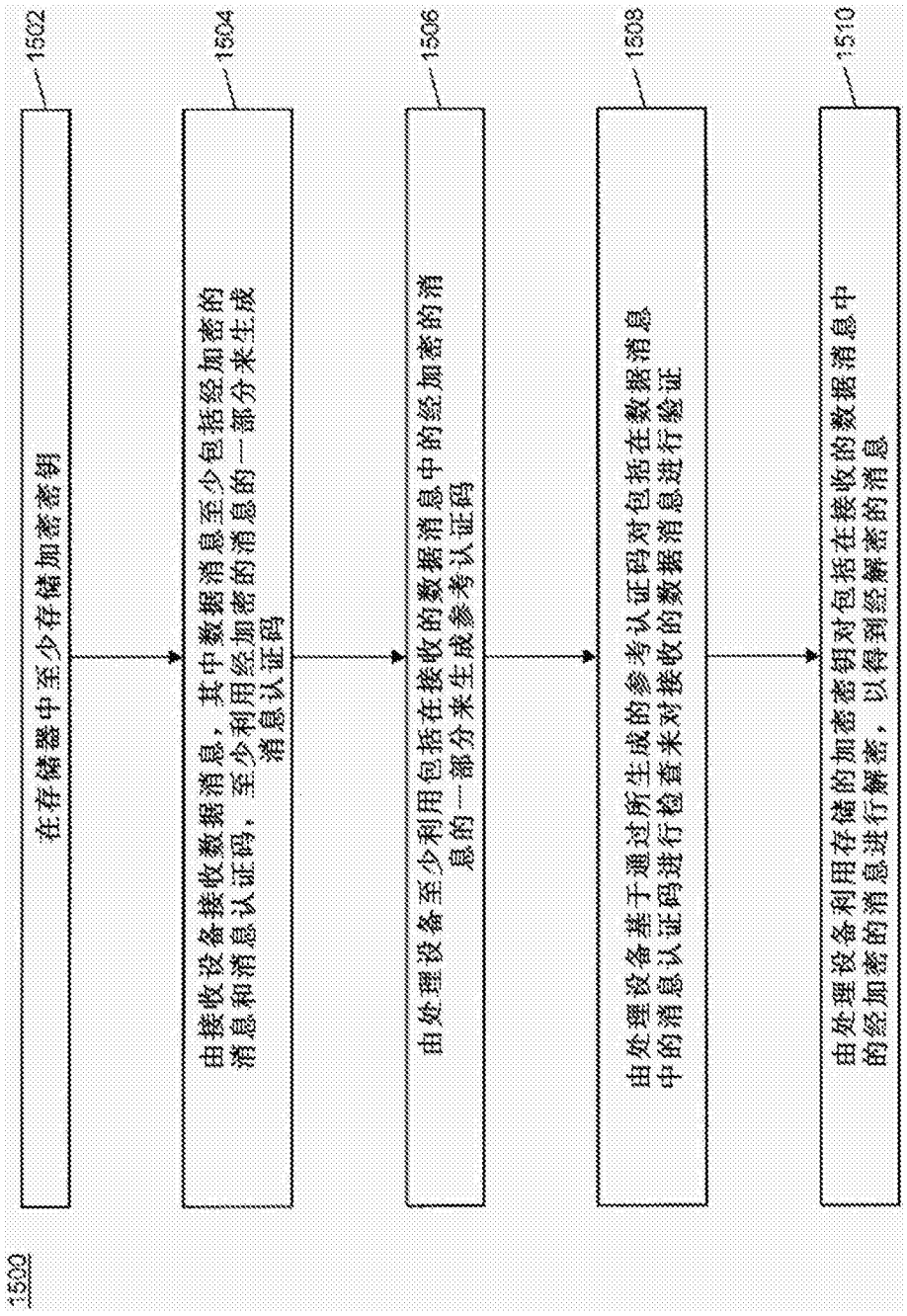
1502
在存储器中至少存储加密密钥
1504
由接收设备接收数据消息，其中数据消息至少包括经加密的消息和消息认证码，至少利用经加密的消息的一部分来生成消息认证码
1506
由处理设备至少利用包括在接收的数据消息中的经加密的消息的一部分来生成参考认证码
1508
由处理设备基于通过所生成的参考认证码对包括在数据消息中的消息认证码进行检查来对接收的数据消息进行验证
1510
由处理设备利用存储的加密密钥对包括在接收的数据消息中的经加密的消息进行解密，以得到经解密的消息
1500

图15


1600
1602
在移动通信设备的存储器中至少存储与移动通信设备相关联的设备信息、与第一应用程序相关联的程序代码（该程序代码至少包括实例标识符）以及与第二应用程序相关联的程序代码（该程序代码包括第一密钥）
1604
由处理设备基于存储的设备信息、经由执行与第一应用程序相关联的程序代码，来生成与移动通信设备相关联的设备指纹
1606
由处理设备经由执行与第一应用程序相关联的程序代码，来生成随机值
1608
由处理设备至少基于生成的设备指纹、生成的随机值和包括在与第一应用程序相关联的程序代码中的实例标识符，来构建多元值
1610
由处理设备利用存储在与第二应用程序相关联的程序代码中的第一密钥、经由执行与第二应用程序相关联的程序代码，来对构建的多元值 进行解密，以得到存储密钥

图16

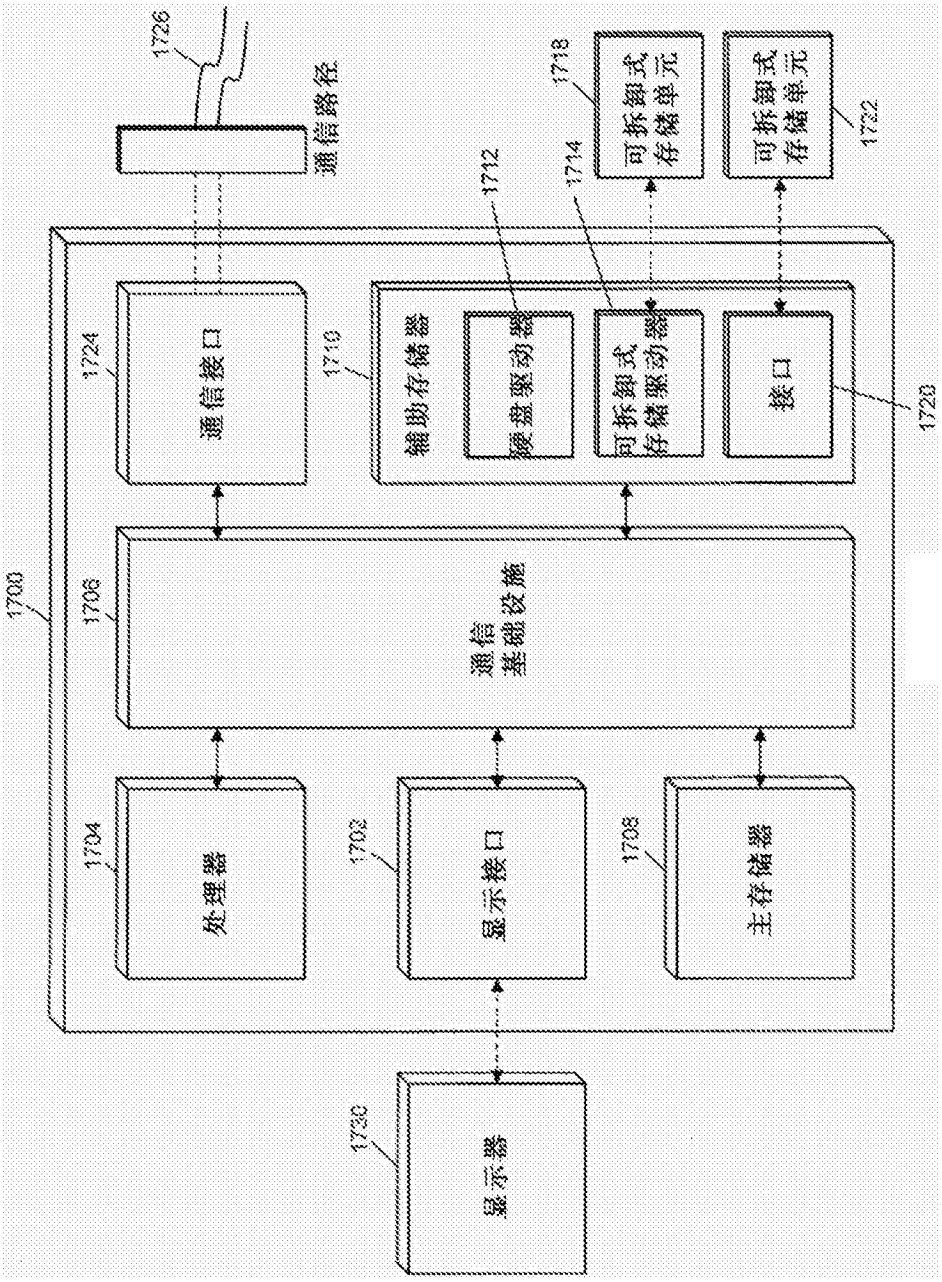
1726
通信路径
1718
可拆卸式存储单元
1722
可拆卸式存储单元
1712
1714
1724
通信接口
1710
辅助存储器
硬盘驱动器
可拆卸式存储驱动器
接口
1720
1700
1706
通信基础设施
1704
处理器
1702
显示接口
1708
主存储器
1730
显示器

图17