(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113168635 B
(45)授权公告日 2025.02.18

(21)申请号 201980079697.7
(22)申请日 2019.10.01
(65)同一申请的已公布的文献号
申请公布号 CN 113168635 A
(43)申请公布日 2021.07.23
(30)优先权数据
62/740,352 2018.10.02 US
16/205,119 2018.11.29 US
16/351,365 2019.03.12 US
(85)PCT国际申请进入国家阶段日
2021.06.02
(86)PCT国际申请的申请数据
PCT/US2019/053963 2019.10.01
(87)PCT国际申请的公布数据
WO2020/072424 EN 2020.04.09

(73)专利权人 第一资本服务有限责任公司
地址 美国弗吉尼亚州
(72)发明人 凯文·奥斯本 杰弗里·鲁尔
詹姆斯·阿什菲尔德
斯里尼瓦沙·希古鲁帕蒂
(74)专利代理机构 北京品源专利代理有限公司 11332
专利代理师 谭营营 胡彬

(51)Int.Cl.
G06Q 20/38(2012.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
US 2016294550 A1,2016.10.06
审查员 吴娟

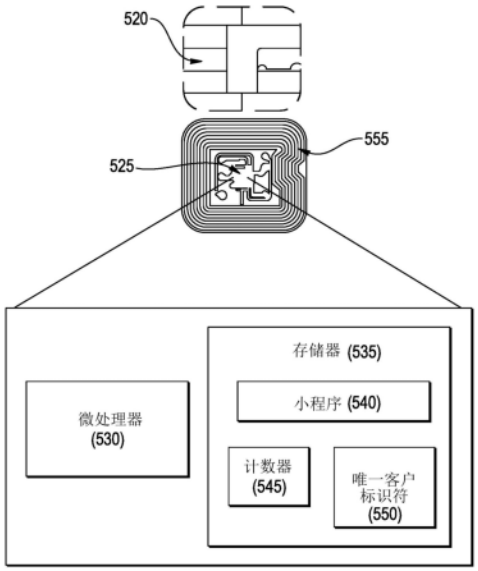
权利要求书3页 说明书32页 附图14页

(54)发明名称

用于非接触式卡的密码认证的系统和方法

(57)摘要

提供了用于传输和接收设备之间的数据传输和授权交易的系统和方法的示例实施例。在实施例中,一种方法包括:当交易的值超过预定值时,生成对至少一个认证因素的请求,其中至少一个认证因素包括密码;接收认证信号,认证信号包括密码;以及当接收到认证信号时,授权交易。



CN 113168635 B

1.一种认证系统,包括:

非接触式卡和认证服务器,

其中,所述认证服务器被配置为:

识别与涉及用户账户的交易请求相关联的交易,所述交易请求由所述认证服务器从商家服务器接收,

将所述交易识别为高风险,

向与所述用户账户相关联的客户端设备发送认证请求,

响应于所述认证请求从所述客户端设备接收密码,所述密码由所述客户端设备从所述非接触式卡接收,

使用加密算法基于会话密钥验证所述密码,并且

基于经验证的密码授权所述交易。

2.根据权利要求1所述的认证系统,其中所述认证服务器还被配置为:

基于主密钥和唯一标识符生成认证多样化密钥,并且

基于所述认证多样化密钥生成所述会话密钥。

3.根据权利要求1所述的认证系统,其中基于所述交易与所述用户账户的历史交易模式的比较将所述交易识别为高风险。

4.根据权利要求3所述的认证系统,其中,所述交易是在与所述历史交易模式不一致的时间进行的。

5.根据权利要求3所述的认证系统,其中,所述交易是在与所述历史交易模式不一致的地理区域进行的。

6.根据权利要求1所述的认证系统,其中基于所述商家与欺诈交易的关联将所述交易识别为高风险。

7.根据权利要求1所述的认证系统,其中:

基于所述商家的位置将所述交易识别为高风险,并且

所述商家的位置处于与欺诈交易相关联的地理区域。

8.根据权利要求1所述的认证系统,其中,所述密码由所述非接触式卡生成并且由所述客户端设备使用近场通信(NFC)接收。

9.根据权利要求1所述的认证系统,其中:

所述认证服务器还被配置为针对选自由生物特征信息和密码构成的组中的至少一个发送第二认证请求,并且

所述认证服务器还被配置为延迟所述交易,等待所述认证请求。

10.根据权利要求1所述的认证系统,其中所述认证服务器还被配置为:

在发送所述认证请求之前,将所述交易的值与阈值进行比较,并且

如果所述交易的值超过所述阈值,则发送所述认证请求。

11.一种利用非接触式卡进行安全电子认证的方法,所述方法包括:

由认证服务器的处理器识别与涉及用户账户的交易请求相关联的交易,所述交易请求由所述认证服务器从商家服务器接收;

由所述认证服务器的所述处理器将所述交易识别为高风险;

由所述认证服务器的所述处理器向与所述非接触式卡无线通信的客户端设备发送认

证请求,所述认证请求提示使所述非接触式卡进入所述客户端设备的通信场;

由所述认证服务器的所述处理器响应于所述认证请求接收由所述非接触式卡生成的密码,其中所述密码经由所述客户端设备被发送到所述认证服务器的所述处理器;

由所述认证服务器的所述处理器使用加密算法基于会话密钥验证所述密码;以及

由所述认证服务器的所述处理器基于经验证的密码授权所述交易。

12.根据权利要求11所述的方法,还包括:

由所述认证服务器的所述处理器基于主密钥和唯一标识符生成认证多样化密钥;以及

由所述认证服务器的所述处理器基于所述认证多样化密钥生成所述会话密钥。

13.根据权利要求11所述的方法,还包括由所述认证服务器的所述处理器针对选自由生物特征信息和密码构成的组中的至少一个发送第二认证请求。

14.根据权利要求11所述的方法,还包括由所述认证服务器的所述处理器延迟所述交易,等待所述认证请求。

15.根据权利要求11所述的方法,其中将所述交易识别为高风险包括:

由所述认证服务器的所述处理器将所述交易与所述账户的历史交易模式进行比较,以及

由所述认证服务器的所述处理器确定所述交易是在与所述历史交易模式不一致的时间进行的。

16.根据权利要求11所述的方法,其中将所述交易识别为高风险包括:

由所述认证服务器的所述处理器将所述交易与所述账户的历史交易模式进行比较,以及

由所述认证服务器的所述处理器确定所述交易是在与所述历史交易模式不一致的地理区域进行的。

17.一种认证服务器,包括:

处理器,

其中,所述处理器被配置为:

识别与涉及用户账户的交易请求相关联的交易,所述交易请求由所述处理器从商家服务器接收,

将所述交易识别为高风险,

向与所述用户账户相关联的客户端设备发送认证请求,

响应于所述认证请求从所述客户端设备接收密码,所述密码由所述客户端设备从存在于所述客户端设备的通信场内的非接触式卡接收,

使用加密算法基于会话密钥验证所述密码,并且

基于经验证的密码授权所述交易。

18.根据权利要求17所述的认证服务器,其中所述处理器还被配置为:

基于主密钥和唯一标识符生成认证多样化密钥,并且

基于所述认证多样化密钥生成所述会话密钥。

19.根据权利要求17所述的认证服务器,其中基于所述商家与欺诈交易的关联将所述交易识别为高风险。

20.根据权利要求17所述的认证服务器,其中:

基于所述商家的位置将所述交易识别为高风险,并且

所述商家的位置处于与欺诈交易相关联的地理区域。

用于非接触式卡的密码认证的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年3月12日提交的美国专利申请号16/351,365(该申请是于2018年11月29日提交的美国专利申请号16/205,119的部分延续并要求其优先权)的优先权,并要求于2018年10月2日提交的美国临时专利申请号62/740,352的优先权,这些专利申请的公开内容通过引用整体并入本文。

技术领域

[0003] 本公开涉及密码学,并且更具体地,涉及用于非接触式卡的密码认证的系统和方法。

背景技术

[0004] 数据安全和交易完整性对企业和消费者至关重要。随着电子交易构成越来越大的商业活动份额,这种需求继续增长。

[0005] 电子邮件可能被用作验证交易的工具,但电子邮件容易受到攻击,并且容易受到黑客或其他未经授权的访问的侵害。也可以使用短消息服务(Short message service,SMS)消息,但这也会遭到泄露。而且,甚至数据加密算法(诸如三重DES算法)也有类似的漏洞。

[0006] 激活许多卡(包括例如金融卡(例如信用卡和其他支付卡))涉及持卡人拨打电话号码或访问网站以及输入或以其他方式提供卡信息的耗时过程。进一步,尽管基于芯片的金融卡的越来越多的使用为个人购买提供了相比于以前的技术(例如,磁条卡)更安全的特征,但账户访问仍然可能依赖登录凭证(例如,用户名和密码)来确认持卡人的身份。然而,如果登录凭据遭到泄露,则另一人可能得以访问该用户的账户。

[0007] 这些和其他不足之处是存在的。因此,需要为用户提供克服这些缺陷的适当的解决方案,从而为非接触式卡提供数据安全性、认证和验证。进一步,需要激活卡的改进的方法和账户访问的改进的认证。

发明内容

[0008] 所公开技术的各方面包括用于非接触式卡的密码认证的系统和方法。各种实施例描述了用于实施和管理非接触式卡的密码认证的系统和方法。

[0009] 本公开的实施例提供了一种认证系统,包括:认证服务器;客户端应用,该客户端应用包括用于在与认证服务器进行数据通信的客户端设备上执行的指令;以及非接触式卡,该非接触式卡包含处理器和存储器;其中认证服务器被配置为:接收交易请求,其中交易请求包括请求参与交易的账户的账户信息和交易的交易信息;响应于接收到交易请求,当交易的值超过预定值时,向客户端应用发送请求至少一个认证因素(authentication factor)的认证请求,其中至少一个认证因素包括通过将非接触式卡放置在客户端设备的通信场中而生成的密码;从客户端设备接收认证信号,认证信号包括密码;并且当接收到认

证信号时,对交易进行认证。

[0010] 本公开的实施例提供了一种认证系统,包括:与网络进行数据通信的认证服务器;客户端应用,该客户端应用包括用于在与网络进行数据通信的客户端设备上执行的指令;以及非接触式卡,该非接触式卡包含处理器和存储器,其中非接触式卡与具有账户信息的账户相关联;其中所述认证服务器被配置为:接收交易请求,其中交易请求包括与非接触式卡相关联的账户的账户信息和交易的交易信息;响应于接收到交易请求,当交易的值超过预定值时,向客户端应用发送请求至少一个认证因素的认证请求;从客户端应用接收包括至少一个认证因素的认证信号;并且当从客户端应用接收到认证信号时,对交易进行认证。

[0011] 本公开的实施例提供了一种认证交易的方法,包括以下步骤:由认证服务器接收交易验证请求,其中交易验证请求包括请求参与交易的账户的账户信息和交易的交易信息;响应于接收到交易请求,当交易的值超过预定值时,由认证服务器向包括用于在客户端设备上执行的指令的客户端应用发送认证请求,认证请求请求至少一个认证因素,其中至少一个认证因素包括通过将非接触式卡放置在客户端设备的通信场中而生成的密码;由客户端应用经由传感器和通信接口中的至少一个来检测至少一个认证因素;由客户端应用向认证服务器发送包括认证因素的认证信号;响应于从客户端应用接收认证信号,由认证服务器验证至少一个认证因素;并且由认证服务器响应于认证因素的验证来授权交易。

[0012] 在下文中,将参考附图中示出的具体示例实施例更详细地解释所公开的设计的另外的特征以及由此提供的优点。

附图说明

[0013] 图1A是根据示例实施例的数据传输系统的示意图。

[0014] 图1B是示出根据示例实施例的用于提供经认证的访问的序列的图。

[0015] 图2是根据示例实施例的数据传输系统的图。

[0016] 图3是根据示例实施例的使用非接触式卡的系统的图。

[0017] 图4是示出根据示例实施例的密钥多样化的方法的流程图。

[0018] 图5A是根据示例实施例的非接触式卡的图示。

[0019] 图5B是根据示例实施例的非接触式卡的接触垫的图示。

[0020] 图6是描绘根据示例实施例的用于与设备通信的消息的图示。

[0021] 图7是描绘根据示例实施例的消息和消息格式的图示。

[0022] 图8是示出根据示例实施例的密钥操作的流程图。

[0023] 图9是根据示例实施例的密钥系统的图。

[0024] 图10是根据示例实施例的生成密码的方法的流程图。

[0025] 图11是示出根据示例实施例的密钥多样化的过程的流程图。

[0026] 图12是示出根据示例实施例的用于卡激活的方法的流程图。

[0027] 图13是根据示例实施例的认证系统的图。

[0028] 图14是示出根据示例实施例的认证交易的方法的流程图。

具体实施方式

[0029] 实施例的以下描述提供了参考附图标记的非限制性代表性示例,以具体描述本发

明不同方面的特征和教导。所描述的实施例应该被认为能够与来自实施例的描述的其他实施例分离地或以组合的方式实施。查阅实施例的描述的本领域普通技术人员应该能够学习和理解本发明的不同的所描述方面。实施例的描述应该有助于在这样的程度下对本发明进行理解,即没有具体涵盖但在已经阅读了实施例的描述的本领域的技术人员的知识范围内的其他实施方式将被理解为与本发明的应用一致。

[0030] 本公开的一些实施例的目的是将一个或多个密钥构建到一个或多个非接触式卡中。在这些实施例中,非接触式卡可以执行认证和许多其他功能,否则除了非接触式卡之外,这些功能可能需要用户携带分离的物理令牌。通过采用非接触式接口,可以为非接触式卡提供用于在用户的设备(诸如移动电话)和卡本身之间进行交互和通信的方法。例如,EMV协议(其是许多信用卡交易的基础)包括认证过程,该认证过程足以满足Android®操作系统,但对iOS®提出了挑战,iOS®在近场通信(near field communication,NFC)使用方面限制更严格,因为它只能以只读方式使用。本文描述的非接触式卡的示例实施例利用了NFC技术。

[0031] 图1A示出了根据示例实施例的数据传输系统。如下文进一步讨论的那样,系统100可以包括非接触式卡105、客户端设备110、网络115和服务器120。尽管图1A示出了组件的单个实例,但是系统100可以包括任意数量的组件。

[0032] 系统100可以包括一个或多个非接触式卡105,这将在下面参考图5A至图5B进一步解释。在一些实施例中,非接触式卡105可以利用示例中的NFC与客户端设备110进行无线通信。

[0033] 系统100可以包括客户端设备110,其可以是支持网络的计算机。如本文所述,支持网络的计算机可以包括但不限于计算机设备或通信设备,包括例如服务器、网络设备、个人计算机、工作站、电话、手持PC、个人数字助理、瘦客户端、胖客户端、互联网浏览器或其他设备。客户端设备110也可以是移动设备;例如,移动设备可以包括来自Apple®的iPhone、iPod、iPad或运行苹果的iOS®操作系统的任何其他移动设备、运行微软Windows® Mobile操作系统的任何设备、运行谷歌的Android®操作系统的任何设备、和/或任何其他智能手机、平板电脑或类似的可穿戴移动设备。

[0034] 客户端设备110设备可以包括处理器和存储器,并且应当理解的是,处理电路可以包含执行本文描述的功能所必需的附加组件,包括处理器、存储器、错误和奇偶校验/CRC检查器、数据编码器、防冲突算法、控制器、命令解码器、安全原语和防篡改硬件。客户端设备110还可以包括显示器和输入设备。显示器可以是用于呈现视觉信息的任何类型的设备,诸如计算机监控器、平板显示器和移动设备屏幕,包括液晶显示器、发光二极管显示器、等离子面板和阴极射线管显示器。输入设备可以包括用于将信息输入到用户的设备中的任何设备,该设备是可用的并且由用户设备支持,诸如触摸屏、键盘、鼠标、光标控制设备、触摸屏、麦克风、数码相机、录像机或便携式摄像机。这些设备可以用于输入信息并与软件和本文描述的其他设备交互。

[0035] 在一些示例中,系统100的客户端设备110可以执行实现例如与系统100的一个或多个组件的网络通信以及传输和/或接收数据的一个或多个应用,诸如软件应用。

[0036] 客户端设备110可以经由一个或多个网络115与一个或多个服务器120通信,并且

可以作为与服务器120的相应前端到后端对来操作。客户端设备110可以例如从在客户端设备110上执行的移动设备应用向服务器120传输一个或多个请求。一个或多个请求可以与从服务器120获取数据相关联。服务器120可以从客户端设备110接收一个或多个请求。基于来自客户端设备110的一个或多个请求,服务器120可以被配置为从一个或多个数据库(未示出)获取所请求的数据。基于从一个或多个数据库接收所请求的数据,服务器120可以被配置为向客户端设备110传输接收到的数据,接收到的数据响应于一个或多个请求。

[0037] 系统100可以包括一个或多个网络115。在一些示例中,网络115可以是无线网络、有线网络或无线网络和有线网络的任意组合中的一个或多个,并且可以被配置为将客户端设备110连接到服务器120。例如,网络115可以包括光纤网络、无源光网络、线缆网络、互联网、卫星网络、无线局域网(LAN)、全球移动通信、个人通信服务、个人区域网、无线应用协议、多媒体消息收发服务、增强型消息收发服务、短消息服务、基于时分复用的系统、基于码分多址的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE 802.11b、802.15.1、802.11n和802.11g、蓝牙、NFC、射频识别(RFID)、Wi-Fi和/或其他中的一个或多个。

[0038] 此外,网络115可以包括但不限于电话线、光纤、IEEE以太网902.3、广域网、无线个人区域网、LAN或诸如互联网的全球网络。此外,网络115可以支持互联网、无线通信网络、蜂窝网络等,或者它们的任意组合。网络115还可以包括一个网络,或者作为独立的网络或者彼此合作地操作的任何数量的以上提及的示例性类型的网络。网络115可以利用它们通信耦合到的一个或多个网络元件的一个或多个协议。网络115可以将其他协议转换成或从其他协议转换成网络设备的一个或多个协议。尽管网络115被描绘为单个网络,但是应当理解的是,根据一个或多个示例,网络115可以包括多个互连的网络,例如互联网、服务提供商的网络、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0039] 系统100可以包括一个或多个服务器120。在一些示例中,服务器120可以包括耦合到存储器的一个或多个处理器。服务器120可以被配置为用于在不同时间控制和调用各种数据来执行多个工作流动作的中央系统、服务器或平台。服务器120可以被配置为连接到一个或多个数据库。服务器120可以连接到至少一个客户端设备110。

[0040] 图1B是示出根据本公开的一个或多个实施例的用于提供经认证的访问的示例序列的时序图。系统100可以包括非接触式卡105和客户端设备110,该客户端设备可以包括应用122和处理器124。图1B可能参考如图1A所示的类似的组件。

[0041] 在步骤102处,应用122与非接触式卡105通信(例如,在被带到非接触式卡105附近之后)。应用122和非接触式卡105之间的通信可以涉及非接触式卡105足够靠近客户端设备110的读卡器(未示出),以实现应用122和非接触式卡105之间的NFC数据传送。

[0042] 在步骤104处,在客户端设备110和非接触式卡105之间已经建立通信之后,非接触式卡105生成消息认证码(MAC)密码。在一些示例中,这可能发生在由应用122读取非接触式卡105时。特别地,这可以在读取(诸如NFC读取)近场数据交换(NDEF)标签时发生,该标签可以根据NFC数据交换格式创建。例如,诸如应用122的读取器可以传输具有产生NDEF的小程序的小程序ID的消息(诸如小程序选择消息)。在确认选择后,可以传输随后是读取文件消息的所选择的文件消息序列。例如,序列可以包括“选择功能文件”、“读取功能文件”和“选择NDEF文件”。此时,由非接触式卡105维护的计数器值可以被更新或递增,随后可以是“读取NDEF文件”。此时,可以生成可以包括报头和共享秘密(secret)的消息。然后可以生成会

话密钥。MAC密码可以根据消息创建,该消息可以包括报头和共享秘密。MAC密码然后可以与一个或多个随机数据块连接,并且MAC密码和随机数(random number,RND)可以用会话密钥加密。此后,密码和报头可以被连接,并被编码为ASCII十六进制,并(响应“读取NDEF文件”消息)以NDEF消息格式返回。

[0043] 在一些示例中,MAC密码可以作为NDEF标签来传输,并且在其他示例中,MAC密码可以与统一资源指示符一起被包括(例如,作为格式化的字符串)。

[0044] 在一些示例中,应用122可以被配置为向非接触式卡105传输请求,该请求包括用于生成MAC密码的指令。

[0045] 在步骤106处,非接触式卡105向应用122发送MAC密码。在一些示例中,MAC密码的传输经由NFC发生,然而,本公开不限于此。在其他示例中,这种经由可以通过蓝牙、Wi-Fi或其他无线数据通信方式进行。

[0046] 在步骤108处,应用122将MAC密码传送给处理器124。

[0047] 在步骤112处,处理器124根据来自应用122的指令验证MAC密码。例如,可以验证MAC密码,如下面所解释那样。

[0048] 在一些示例中,验证MAC密码可以由除了客户端设备110的设备(诸如与客户端设备110进行数据通信的服务器120(如图1A所示))来执行。例如,处理器124可以输出MAC密码以便传输到服务器120,该服务器可以验证MAC密码。

[0049] 在一些示例中,MAC密码可以用作数字签名用于验证的目的。其他数字签名算法(诸如公钥非对称算法,例如数字签名算法和RSA算法、或者零知识协议)可以用于执行这种验证。

[0050] 图2示出了根据示例实施例的数据传输系统。系统200可以包括例如经由网络215与一个或多个服务器220通信的发送设备205、接收设备210。发送设备205可以与上面参考图1A讨论的客户端设备110相同或相似。接收设备210可以与上面参考图1A讨论的客户端设备110相同或相似。网络215可以类似于上面参考图1A讨论的网络115。服务器220可以类似于上面参考图1A讨论的服务器120。尽管图2示出了系统200的组件的单个实例,但是系统200可以包括任何数量的所示组件。

[0051] 当使用对称加密算法(诸如加密算法、基于哈希的消息认证码(hash-based message authentication code,HMAC)算法和基于密码的消息认证码(CMAC)算法)时,重要的是,密钥在最初使用对称算法和密钥处理被保护的数据的一方与使用相同加密算法和相同密钥接收和处理数据的一方之间保持秘密。

[0052] 同样重要的是,相同的密钥不被使用太多次。如果密钥使用或重复使用过于频繁,该密钥可能会被泄露。每次使用密钥时,它向攻击者提供附加的数据样本,该样本由加密算法使用相同的密钥进行处理。攻击者拥有的用相同密钥处理的数据越多,攻击者发现密钥的值的可能性就越大。频繁使用的密钥可能包含在各种不同的攻击中。

[0053] 而且,每次执行对称加密算法时,它可能会展现关于在对称密码操作期间使用的密钥的信息,诸如边信道数据。边信道数据可能包括在使用密钥的同时加密算法执行时出现的微小功率波动。可以对边通道数据进行充分的测量以展现关于密钥的足够信息,从而允许其被攻击者恢复。使用相同密钥交换数据会重复展现通过相同密钥处理的数据。

[0054] 然而,通过限制特定密钥将使用的次数,攻击者能够收集的边通道数据量是有限

的,并且从而减少了暴露于这种攻击和其他类型攻击。如本文进一步描述的那样,参与密码信息交换的各方(例如,发送者和接收者)可以结合计数器值根据初始共享主对称密钥独立地生成密钥,并且从而周期性地替换正在使用的共享对称密钥,需要求助于任何形式的密钥交换来保持各方同步。通过周期性地改变由发送者和接收者使用的共享秘密对称密钥,以上描述的攻击变得不可能。

[0055] 转回参考图2,系统200可以被配置为实施密钥多样化。例如,发送者和接收者可能期望经由相应设备205和210交换数据(例如,原始敏感数据)。如上所解释那样,尽管可以包括发送设备205和接收设备210的单个实例,但是应当理解的是,可以涉及一个或多个擦混输设备205和一个或多个接收设备210,只要每一方共享相同的共享秘密对称密钥。在一些示例中,发送设备205和接收设备210可以被提供有相同的主对称密钥。进一步,应当理解的是,持有相同秘密对称密钥的任何一方或设备可以执行发送设备205的功能,并且类似地,持有相同秘密对称密钥的任何一方可以执行接收设备210的功能。在一些示例中,对称密钥可以包括共享秘密对称密钥,该共享秘密对称密钥对除了参与交换安全数据的发送设备205和接收设备210之外的所有方保持秘密。还应当理解的是,发送设备205和接收设备210两者可以被提供有相同的主对称密钥,并且还应当理解的是,发送设备205和接收设备210之间交换的数据的一部分包括可以被称为计数器值的数据的至少一部分。计数器值可以包括每次在发送设备205和接收设备210之间交换数据时改变的数字。

[0056] 系统200可以包括一个或多个网络215。在一些示例中,网络215可以是无线网络、有线网络或无线网络和有线网络的任意组合中的一个或多个,并且可以被配置为将一个或多个发送设备205和一个或多个接收设备210连接到服务器220。例如,网络215可以包括光纤网络、无源光网络、线缆网络、互联网、卫星网络、无线LAN、全球移动通信、个人通信服务、个人区域网、无线应用协议、多媒体消息收发服务、增强型消息收发服务、短消息服务、基于时分复用的系统、基于码分多址的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE 802.11b、802.15.1、802.11n和802.11g、蓝牙、NFC、RFID、Wi-Fi和/或其他中的一个或多个。

[0057] 此外,网络215可以包括但不限于电话线、光纤、IEEE以太网902.3、广域网、无线个人区域网、LAN或诸如互联网的全球网络。此外,网络215可以支持互联网、无线通信网络、蜂窝网络等,或者它们的任意组合。网络215还可以包括一个网络,或者作为独立的网络或者彼此合作地操作的任何数量的以上提及的示例性类型的网络。网络215可以利用它们通信耦合到的一个或多个网络元件的一个或多个协议。网络215可以将其他协议转换成或从其他协议转换成网络设备的一个或多个协议。尽管网络215被描绘为单个网络,但是应当理解的是,根据一个或多个示例,网络215可以包括多个互连的网络,例如互联网、服务提供商的网络、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0058] 在一些示例中,一个或多个发送设备205和一个或多个接收设备210可以被配置为在彼此之间传送以及传输和接收数据,而不经过网络215。例如,一个或多个发送设备205和一个或多个接收设备210之间的通信可以经由NFC、蓝牙、RFID、Wi-Fi等中的至少一个来发生。

[0059] 在框225处,当发送设备205准备用对称密码操作处理敏感数据时,发送者可以更新计数器。此外,发送设备205可以选择适当的对称加密算法,该对称加密算法可以包括对称加密算法、HMAC算法和CMAC算法中的至少一个。在一些示例中,用于处理多样化值的对称

算法可以包括根据需要用于生成期望长度的多样化对称密钥的任何对称加密算法。对称算法的非限制性示例可以包括对称加密算法(诸如3DES或AES128)、对称HMAC算法(诸如HMAC-SHA-256算法)、以及对称CMAC算法(诸如AES-CMAC)。应当理解的是,如果所选择的对称算法的输出没有生成足够长的密钥,则诸如利用不同的输入数据和相同的主密钥处理对称算法的多次迭代的技术可以产生多个输出,这些输出可以根据需要进行组合以产生足够长的密钥。

[0060] 在框230处,发送设备205可以采用所选择的加密算法,并使用主对称密钥来处理计数器值。例如,发送者可以选择对称加密算法,并使用随着发送设备205和接收设备210之间的每次对话而更新的计数器。发送设备205然后可以使用主对称密钥利用所选择的对称加密算法加密计数器值,从而创建多样化对称密钥。

[0061] 在一些示例中,计数器值可能未加密。在这些示例中,计数器值可以在框230处在没有加密的情况下在发送设备205和接收设备210之间传输。

[0062] 在框235处,多样化对称密钥可以用于在将结果传输到接收设备210之前处理敏感数据。例如,发送设备205可以使用多样化对称密钥使用对称加密算法来加密敏感数据,其中输出包括受保护的加密数据。发送设备205然后可以将受保护的加密数据连同计数器值一起传输到接收设备210以便进行处理。

[0063] 在框240处,接收设备210可以首先获取计数器值,并且然后使用计数器值作为加密的输入以及主对称密钥作为用于加密的密钥,来执行相同的对称加密。加密的输出可以是由发送者创建的相同的多样化对称密钥值。

[0064] 在框245处,接收设备210然后可以获取受保护的加密数据,并使用对称解密算法以及多样化对称密钥来解密受保护的加密数据。

[0065] 在框250处,作为解密受保护的加密数据的结果,原始敏感数据可以被展现。

[0066] 下一次敏感数据需要从发送者经由相应发送设备205和接收设备210发送到接收者时,可以选择不同的计数器值从而产生不同的多样化对称密钥。通过利用主对称密钥和相同的对称加密算法处理计数器值,发送设备205和接收设备210两者可以独立地产生相同的多样化对称密钥。这种多样化对称密钥(而不是主对称密钥)用于保护敏感数据。

[0067] 如上所解释那样,发送设备205和接收设备210两者最初各自拥有共享的主对称密钥。共享主对称密钥不用于加密原始敏感数据。因为多样化对称密钥是由发送设备205和接收设备210两者独立创建的,所以它从不在双方之间传输。因此,攻击者不能截取多样化对称密钥,并且攻击者永远看不到利用主对称密钥处理的任何数据。只有计数器值是利用主对称密钥处理的,而敏感数据不是利用主对称密钥处理的。结果,展现了关于主对称密钥的减少的边信道数据。而且,发送设备205和接收设备210的操作可以由关于创建新的多样化值以及因此创建新的多样化对称密钥的频率的对称要求来管控。在实施例中,可以为发送设备205和接收设备210之间的每次交换创建新的多样化值,并因此创建新的多样化对称密钥。

[0068] 在一些示例中,密钥多样化值可以包括计数器值。密钥多样化值的其他非限制性示例包括:每次需要新的多样化密钥时生成的随机数,该随机数从发送设备205发送到接收设备210;从发送设备205和接收设备210发送的计数器值的全值;从发送设备205和接收设备210发送的计数器值的一部分;由发送设备205和接收设备210独立维护但不在两个设备

之间发送的计数器;在发送设备205和接收设备210之间交换的一次性通行码;以及敏感数据的密码散列。在一些示例中,可以由各方使用密钥多样化值的一个或多个部分来创建多个多样化密钥。例如,计数器可以用作密钥多样化值。进一步,可以使用上述示例性密钥多样化值中的一个或多个的组合。

[0069] 在另一示例中,计数器的一部分可以用作密钥多样化值。如果各方之间共享多个主密钥值,则可以通过本文描述的系统和过程获得多个多样化密钥值。可以在每当时创建新的多样化值,并且因此创建新的多样化对称密钥。在最安全的情况下,可以为发送设备205和接收设备210之间的敏感数据的每次交换创建新的多样化值。实际上,这可能会创建一次性使用的密钥,诸如单次使用的会话密钥。

[0070] 图3示出了使用非接触式卡的系统300。系统300可以包括非接触式卡305、一个或多个客户端设备310、网络315、服务器320、325、一个或多个硬件安全模块330和数据库335。尽管图3示出了组件的单个实例,但是系统300可以包括任意数量的组件。

[0071] 系统300可以包括一个或多个非接触式卡305,该一个或多个非接触式卡将在下面参照图5A至图5B进一步解释。在一些示例中,非接触式卡305可以与客户端设备310进行无线通信,例如NFC通信。例如,非接触式卡305可以包括被配置为通过NFC或其他短程协议进行通信的一个或多个芯片,诸如射频识别芯片。在其他实施例中,非接触式卡305可以通过其他方式与客户端设备310通信,包括但不限于蓝牙、卫星、Wi-Fi、有线通信和/或无线和有线连接的任何组合。根据一些实施例,非接触式卡305可以被配置为当非接触式卡305在读卡器313的范围内时,通过NFC与客户端设备310的读卡器313通信。在其他示例中,与非接触式卡305的通信可以通过物理接口来实现,例如通用串行总线接口或刷卡接口。

[0072] 系统300可以包括客户端设备310,其可以是支持网络的计算机。如本文所述,支持网络的计算机可以包括但不限于:例如计算机设备、或通信设备,包括例如服务器、网络设备、个人计算机、工作站、移动设备、电话、手持PC、个人数字助理、瘦客户端、胖客户端、互联网浏览器或其他设备。一个或多个客户端设备310也可以是移动设备;例如,移动设备可以包括来自Apple®的iPhone、iPod、iPad或运行苹果的iOS®操作系统的任何其他移动设备、运行微软Windows® Mobile操作系统的任何设备、运行谷歌的Android®操作系统的任何设备、和/或任何其他智能手机或类似的可穿戴移动设备。在一些示例中,客户端设备310可以与参考图1A或图1B描述的客户端设备110相同或相似。

[0073] 客户端设备310可以经由一个或多个网络315与一个或多个服务器320和325进行通信。客户端设备310可以例如从在客户端设备310上执行的应用311向一个或多个服务器320和325传输一个或多个请求。一个或多个请求可以与从一个或多个服务器320和325获取数据相关联。服务器320和325可以从客户端设备310接收一个或多个请求。基于来自客户端设备310的一个或多个请求,一个或多个服务器320和325可以被配置为从一个或多个数据库335获取所请求的数据。基于从一个或多个数据库335接收所请求的数据,一个或多个服务器320和325可以被配置为向客户端设备310传输接收到的数据,接收到的数据响应于一个或多个请求。

[0074] 系统300可以包括一个或多个硬件安全模块(HSM)330。例如,一个或多个HSM 330可以被配置为执行本文公开的一个或多个密码操作。在一些示例中,一个或多个HSM 330可以被配置为专用安全设备,这些专用安全设备被配置为执行一个或多个密码操作。HSM 330

可以被配置为使得密钥永远不会在HSM 330之外泄露,而是替代地保持在HSM 330内。例如,一个或多个HSM 330可以被配置为执行密钥导出、解密和MAC操作中的至少一个。一个或多个HSM 330可以包含在服务器320和325内,或者可以与服务器320和325进行数据通信。

[0075] 系统300可以包括一个或多个网络315。在一些示例中,网络315可以是无线网络、有线网络或无线网络和有线网络的任意组合中的一个或多个,并且可以被配置为将客户端设备315连接到服务器320和325。例如,网络315可以包括光纤网络、无源光网络、线缆网络、蜂窝网络、互联网、卫星网络、无线LAN、全球移动通信、个人通信服务、个人区域网、无线应用协议、多媒体消息收发服务、增强型消息收发服务、短消息服务、基于时分复用的系统、基于码分多址的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE 802.11b、802.15.1、802.11n和802.11g、蓝牙、NFC、RFID、Wi-Fi和/或其网络的任何组合中的一个或多个。作为非限制性示例,来自非接触式卡305和客户端设备310的通信可以包括NFC通信、客户端设备310和运营商之间的蜂窝网络以及运营商和后端之间的互联网。

[0076] 此外,网络315可以包括但不限于电话线、光纤、IEEE以太网902.3、广域网、无线个人区域网、局域网或诸如互联网的全球网络。此外,网络315可以支持互联网、无线通信网络、蜂窝网络等,或者它们的任意组合。网络315还可以包括一个网络,或者作为独立的网络或者彼此合作地操作的任何数量的以上提及的示例性类型的网络。网络315可以利用它们通信耦合到的一个或多个网络元件的一个或多个协议。网络315可以将其他协议转换成或从其他协议转换成网络设备的一个或多个协议。尽管网络315被描绘为单个网络,但是应当理解的是,根据一个或多个示例,网络315可以包括多个互连的网络,例如互联网、服务提供商的网络、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0077] 在根据本公开的各种示例中,系统300的客户端设备310可以执行一个或多个应用311,并且包括一个或多个处理器312以及一个或多个读卡器313。例如,一个或多个应用311(诸如软件应用)可以被配置为实现例如与系统300的一个或多个组件的网络通信,并传输和/或接收数据。应当理解的是,尽管在图3中仅示出了客户端设备310的组件的单个实例,但是可以使用任何数量的设备310。读卡器313可以被配置为从非接触式卡305读取和/或与该非接触式卡通信。结合一个或多个应用311,读卡器313可以与非接触式卡305通信。

[0078] 客户端设备310中的任何一个的应用311可以使用短程无线通信(例如,NFC)与非接触式卡305通信。应用311可以被配置为与被配置为与非接触式卡305通信的客户端设备310的读卡器313接口。应该注意的是,本领域技术人员应该理解,小于二十厘米的距离与NFC范围一致。

[0079] 在一些实施例中,应用311通过相关联的读取器(例如,读卡器313)与非接触式卡305通信。

[0080] 在一些实施例中,卡激活可以在没有用户认证的情况下发生。例如,非接触式卡305可以通过NFC通过客户端设备310的读卡器313与应用311通信。该通信(例如,在客户端设备310的读卡器313附近轻击卡)允许应用311读取与卡相关联的数据并执行激活。在一些情况下,轻击可以激活或启动应用311,并且然后发起一个或多个动作或与账户服务器325的通信,以激活卡供后续使用。在一些情况下,如果应用311没有安装在客户端设备310上,则卡对读卡器313的轻击可以发起应用311的下载(例如,导航到应用下载页面)。在安装之后,轻击卡可以激活或启动应用311,并且然后(例如,经由应用或其他后端通信)发起卡的

激活。在激活后,该卡可以用于各种交易,包括商业交易。

[0081] 根据一些实施例,非接触式卡305可以包括虚拟支付卡。在那些实施例中,应用311可以通过访问在客户端设备310上实施的数字钱包来获取与非接触式卡305相关联的信息,其中数字钱包包括虚拟支付卡。在一些示例中,虚拟支付卡数据可以包括一个或多个静态或动态生成的虚拟卡号。

[0082] 服务器320可以包括与数据库335通信的网络服务器。服务器325可以包括账户服务器。在一些示例中,服务器320可以被配置为通过与数据库335中的一个或多个凭证进行比较来校验来自非接触式卡305和/或客户端设备310的一个或多个凭证。服务器325可以被配置为授权来自非接触式卡305和/或客户端设备310的一个或多个请求,诸如支付和交易。

[0083] 图4示出了根据本公开的示例的密钥多样化的方法400。方法400可以包括类似于图2中引用的发送设备205和接收设备210的发送设备和接收设备。

[0084] 例如,发送者和接收者可能期望通过发送设备和接收设备交换数据(例如,原始敏感数据)。如上所述,尽管可以包括这两方,但是应当理解的是,可以涉及一个或多个发送设备和一个或多个接收设备,只要每一方共享相同的共享秘密对称密钥。在一些示例中,发送设备和接收设备可以被提供有相同的主对称密钥。进一步,应当理解的是,持有相同秘密对称密钥的任何一方或设备可以执行发送设备的功能,并且类似地,持有相同秘密对称密钥的任何一方可以执行接收设备的功能。在一些示例中,对称密钥可以包括共享秘密对称密钥,该共享秘密对称密钥对除了参与交换安全数据的发送设备和接收设备之外的所有方保持秘密。还应当理解的是,发送设备和接收设备两者可以被提供有相同的主对称密钥,并且还应当理解的是,发送设备和接收设备之间交换的数据的一部分包括可以被称为计数器值的数据的至少一部分。计数器值可以包括每次在发送设备和接收设备之间交换数据时改变的数字。

[0085] 在框410处,发送设备和接收设备可以被提供有相同的主密钥,诸如相同的主对称密钥。当发送设备准备利用对称密码操作处理敏感数据时,发送者可以更新计数器。此外,发送设备可以选择适当的对称加密算法,该对称加密算法可以包括对称加密算法、HMAC算法和CMAC算法中的至少一个。在一些示例中,用于处理多样化值的对称算法可以包括根据需要用于生成期望长度的多样化对称密钥的任何对称加密算法。对称算法的非限制性示例可以包括对称加密算法(诸如3DES或AES128)、对称HMAC算法(诸如HMAC-SHA-256算法)、以及对称CMAC算法(诸如AES-CMAC)。应当理解的是,如果所选择的对称算法的输出没有生成足够长的密钥,诸如利用不同的输入数据和相同的主密钥处理对称算法的多次迭代的技术可以产生多个输出,这些输出可以根据需要进行组合以产生足够长的密钥。

[0086] 发送设备可以采用所选择的加密算法,并使用主对称密钥来处理计数器值。例如,发送者可以选择对称加密算法,并使用随着发送设备和接收设备之间的每次对话而更新的计数器。

[0087] 在框420处,发送设备然后可以使用主对称密钥利用所选择的对称加密算法加密计数器值,从而创建多样化对称密钥。多样化对称密钥可以用于在将结果传输到接收设备之前处理敏感数据。例如,发送设备可以使用多样化对称密钥使用对称加密算法来加密敏感数据,其中输出包括受保护的加密数据。发送设备然后可以将受保护的加密数据连同计数器值一起传输到接收设备以便进行处理。在一些示例中,可以执行除加密之外的密码操

作,并且在传输受保护数据之前,可以使用多样化对称密钥来执行多个加密操作。

[0088] 在一些示例中,计数器值可能未加密。在这些示例中,计数器值可以在框420处在没有加密的情况下在发送设备和接收设备之间传输。

[0089] 在框430处,可以使用一个或多个加密算法和多样化密钥来保护敏感数据。多样化会话密钥(其可以通过使用计数器的密钥多样化来创建)可以与一个或多个加密算法一起使用来保护敏感数据。例如,可以使用第一多样化会话密钥由MAC来处理数据,并且可以使用第二多样化会话密钥来加密所得到的输出,产生受保护数据。

[0090] 在框440处,接收设备可以使用计数器值作为加密的输入并且使用主对称密钥作为用于加密的密钥来执行相同的对称加密。加密的输出可以是由发送者创建的相同的多样化对称密钥值。例如,接收设备可以使用计数器独立地创建其自己的第一多样化会话密钥和第二多样化会话密钥的副本。然后,接收设备可以使用第二多样化会话密钥解密受保护数据,以展现由发送设备创建的MAC的输出。接收设备然后可以使用第一多样化会话密钥通过MAC操作来处理最终的数据。

[0091] 在框450处,接收设备可以使用具有一个或多个加密算法的多样化密钥来校验受保护数据。

[0092] 在框460处,可以校验原始数据。如果MAC操作的输出(通过接收设备使用第一多样化会话密钥)与通过解密展现的MAC输出相匹配,则数据可以被认为是有效的。

[0093] 下一次需要将敏感数据从发送设备发送到接收设备时,可以选择不同的计数器值,这产生不同的多样化对称密钥。通过利用主对称密钥和相同的对称加密算法处理计数器值,发送设备和接收设备两者可以独立地产生相同的多样化对称密钥。这种多样化对称密钥(而不是主对称密钥)用于保护敏感数据。

[0094] 如上所解释那样,发送设备和接收设备两者最初各自拥有共享的主对称密钥。共享主对称密钥不用于加密原始敏感数据。因为多样化对称密钥是由发送设备和接收设备两者独立创建的,所以它从不在双方之间传输。因此,攻击者不能截取多样化对称密钥,并且攻击者永远看不到利用主对称密钥处理的任何数据。只有较小的计数器值是利用主对称密钥处理的,而敏感数据不是利用主对称密钥处理的。结果,展现了关于主对称密钥的减少的边信道数据。而且,发送者和接收者可以例如通过事先安排或其他方式来商定多久创建一次新的多样化值并且因此创建新的多样化对称密钥。在实施例中,可以为发送设备和接收设备之间的每次交换创建新的多样化值,并因此创建新的多样化对称密钥。

[0095] 在一些示例中,密钥多样化值可以包括计数器值。密钥多样化值的其他非限制性示例包括:每次需要新的多样化密钥时生成的随机数,该随机数从发送设备发送到接收设备;从发送设备和接收设备发送的计数器值的全值;从发送设备和接收设备发送的计数器值的一部分;由发送设备和接收设备独立维护但不在两个设备之间发送的计数器;在发送设备和接收设备之间交换的一次性通行码;敏感数据的密码散列。在一些示例中,可以由各方使用密钥多样化值的一个或多个部分来创建多个多样化密钥。例如,计数器可以用作密钥多样化值。

[0096] 在另一示例中,计数器的一部分可以用作密钥多样化值。如果各方之间共享多个主密钥值,则可以通过本文描述的系统和过程获得多个多样化密钥值。可以在每当需要时创建新的多样化值,并且因此创建新的多样化对称密钥。在最安全的情况下,可以为发送设

备和接收设备之间的敏感数据的每次交换创建新的多样化值。实际上,这可能会创建一次性使用的密钥,诸如单个会话密钥。

[0097] 在其他示例中,诸如为了限制主对称密钥的使用次数,可以由发送设备的发送者和接收设备的接收者商定新多样化值并且因此新的多样化对称密钥将仅周期性地发生。在一个示例中,这可以是在预定次数的使用(诸如在发送设备和接收设备之间每10次传输)之后。在另一示例中,这可以是在某个时间段之后、传输之后的某个时间段之后,或者周期性地(例如,每天地在指定时间;每周地在指定日期的指定时间)。在另一示例中,这可以是每当接收设备向发送设备发信号通知它期望在下一次通信中改变密钥时。这可以根据策略来控制,并且可以由于例如由接收设备的接收者所感知的当前风险水平而变化。

[0098] 图5A示出了一个或多个非接触式卡500,该一个或多个非接触式卡可以包括由显示在卡500的正面或背面的服务提供商505发行的支付卡,诸如信用卡、借记卡或礼品卡。在一些示例中,非接触式卡500与支付卡无关,并且可以包括但不限于标识卡。在一些示例中,支付卡可以包括双接口非接触式支付卡。非接触式卡500可以包括基底510,该基底可以包括由塑料、金属和其他材料构成的单层或一个或多个层压层。示例性基底材料包括聚氯乙烯、聚氯乙烯乙酸酯、丙烯腈丁二烯苯乙烯、聚碳酸酯、聚酯、阳极化钛、钯、金、碳、纸和生物可降解材料。在一些示例中,非接触式卡500可以具有符合ISO/IEC 7810标准的ID-1格式的物理特性,并且非接触式卡可以另外符合ISO/IEC 14443标准。然而,应当理解的是,根据本公开的非接触式卡500可以具有不同的特性,并且本公开不要求在支付卡中实施非接触式卡。

[0099] 非接触式卡500还可以包括显示在卡的正面和/或背面的标识信息515,以及接触垫520。接触垫520可被配置为与另一通信设备(诸如用户设备、智能电话、膝上型电脑、台式电脑或平板电脑)建立联系。非接触式卡500还可以包括处理电路、天线和图5A中未示出的其他组件。这些组件可以位于接触垫520的后面或者基底510上的其他地方。非接触式卡500还可以包括可以位于卡的背面上(图5A中未示出)的磁条或磁带。

[0100] 如图5B所示,图5A的接触垫520可以包括用于存储和处理信息的处理电路525,该处理电路包括微处理器530和存储器535。应当理解的是,处理电路525可以包含执行本文描述的功能所必需的附加组件,包括处理器、存储器、错误和奇偶校验/CRC检查器、数据编码器、防冲突算法、控制器、命令解码器、安全原语和防篡改硬件。

[0101] 存储器535可以是只读存储器、一次写入多次读取存储器或读/写存储器,例如RAM、ROM和EEPROM,并且非接触式卡500可以包括这些存储器中的一个或多个。只读存储器可以是工厂可编程的只读存储器或一次性可编程存储器。一次性可编程性提供了一次写入然后多次读取的机会。一次写入/多次读取存储器可以在存储器芯片已经出厂后的某个时间点被编程。一旦存储器被编程,它可能不被重写,但它可能被多次读取。读/写存储器可以在出厂后被编程和再编程多次。其也可以读取多次。

[0102] 存储器535可以被配置为存储一个或多个小程序540、一个或多个计数器545和客户标识符550。一个或多个小程序540可以包括被配置为在一个或多个非接触式卡上执行的一个或多个软件应用,诸如Java卡小程序。然而,应当理解的是,小程序540不限于Java卡小程序,并且代替地可以是可在非接触式卡或具有有限存储器的其他设备上操作的任何软件应用。一个或多个计数器545可以包括足以存储整数的数字计数器。客户标识符550可以包

括分配给非接触式卡500的用户的唯一字母数字标识符,并且该标识符可以将非接触式卡的用户与其他非接触式卡用户区分开。在一些示例中,客户标识符550可以标识客户和分配给该客户的账户两者,并且可以进一步标识与该客户的账户相关联的非接触式卡。

[0103] 参照接触垫描述了前述示例性实施例的处理器和存储元件,但是本公开不限于此。应当理解的是,这些元件可以在垫520之外实施、或者与该垫完全分离、或者作为位于接触垫520内的处理器530和存储器535元件之外的其他元件。

[0104] 在一些示例中,非接触式卡500可以包括一个或多个天线555。一个或多个天线555可以放置在非接触式卡500内并围绕接触垫520的处理电路525。例如,一个或多个天线555可以与处理电路525一体,并且一个或多个天线555可以与外部升压线圈一起使用。作为另一示例,一个或多个天线555可以在接触垫520和处理电路525的外部。

[0105] 在实施例中,非接触式卡500的线圈可以充当空芯变压器的次级线圈。终端可以通过切断电力或调幅与非接触式卡500通信。非接触式卡500可以使用非接触式卡的电力连接件中的间隙来推断从终端传输的数据,该电力连接可以通过一个或多个电容器在功能方面进行保持。非接触式卡500可以通过切换非接触式卡的线圈上的负载或负载调制来进行通信。负载调制可以通过干扰在终端线圈中检测到。

[0106] 如上所解释那样,非接触式卡500可以构建在可在智能卡或具有有限的存储器的其他设备(例如JavaCard)上操作的软件平台上,并且可以安全地执行一个或多个应用或小程序。小程序可以被添加到非接触式卡中,以在各种基于移动应用的用例中为多因素认证(multifactor authentication,MFA)提供一次性密码(one-time password,OTP)。小程序可以被配置为响应来自读取器(诸如移动NFC读取器)的一个或多个请求(诸如近场数据交换请求),并且产生包括被编码为NDEF文本标签的密码安全的OTP的NDEF消息。

[0107] 图6示出了根据示例实施例的NDEF短记录布局(SR=1)600。一个或多个小程序可以被配置为将OTP编码为NDEF类型4(众所周知类型文本标签)。在一些示例中,NDEF消息可以包括一个或多个记录。小程序可以被配置为除了OTP记录之外还添加一个或多个静态标签记录。示例性标签包括但不限于标签类型:众所周知类型、文本、编码英语(en)、小程序ID:D2760000850101;功能:只读访问;编码:认证消息可以编码为ASCII十六进制;类型-长度-值(TLV)数据可以被提供为可以用于生成NDEF消息的个性化参数。在实施例中,认证模板可以包括具有用于提供实际动态认证数据的众所周知的索引的第一记录。

[0108] 图7示出了根据示例实施例的消息710和消息格式720。在一个示例中,如果要添加附加标签,则第一字节可以改变以指示消息开始,而不是结束,并且可以添加后续记录。因为ID长度为零,所以从记录中省略了ID长度字段和ID。示例消息可以包括:UDK AUT密钥;导出的AUT会话密钥(使用0x00000050);版本1.0;pATC=0x00000050;RND=4838FB7DC171B89E;MAC=<八个计算字节>。

[0109] 在一些示例中,可以通过在安全通道协议2下实施存储数据(E2),在个性化时将数据存储在非接触式卡中。一个或多个值可以由个性化局从(在由小程序ID指定的部分中的)EMBOSS文件读取,并且一个或多个存储数据命令可以在认证和安全通道建立之后被传输到非接触式卡。

[0110] pUID可以包括16位BCD编码的数字。在一些示例中,pUID可以包括14位。

[0111]

项目	长度（字节）	加密？	备注
pUID	8	否	
AutKey	16	是	用于导出 MAC 会话密钥的 3DES 密钥
AutKCV	3	否	密钥检查值
DEKKey	16	是	用于导出加密会话密钥的 3DES 密钥
DEKKCV	3	否	密钥检查值
卡共享随机数	4 字节	否	4 字节真随机数（预生成）
NTLV	X 字节	否	NDEF 信息的 TLV 数据

[0112] 在一些示例中,一个或多个小程序可以被配置为保持其个性化状态,以仅在解锁且认证的情况下才允许个性化。其他状态可以包括标准状态预个性化。在进入终止状态时,一个或多个小程序可以被配置为移除个性化数据。在终止状态下,一个或多个小程序可以被配置为停止响应所有应用协议数据单元(application protocol data unit,APDU)请求。

[0113] 一个或多个小应用可以被配置为维护可以在认证消息中使用的小程序版本(2字节)。在一些示例中,这可以被解释为最高有效字节主版本、最低有效字节次版本。版本中的每一个的规则被配置为解释认证消息:例如,关于主版本,这可以包括每个主版本包含特定认证消息布局和特定算法。对于次版本,除了错误修复、安全强化等之外,这可能不包括对认证消息或加密算法的更改,以及对静态标签内容的更改。

[0114] 在一些示例中,一个或多个小程序可以被配置为仿真RFID标签。RFID标签可以包括一个或多个多态标签。在一些示例中,每次读取标签时,呈现可以指示非接触式卡的真实性的不同的密码数据。基于一个或多个应用,可以处理标签的NFC读取,可以将令牌传输到诸如后端服务器的服务器,并且可以在服务器处校验令牌。

[0115] 在一些示例中,非接触式卡和服务器可以包括一些数据,使得卡可以被正确标识。非接触式卡可以包括一个或多个唯一标识符。每次发生读取操作时,计数器可以被配置为更新。在一些示例中,每次读取卡时,卡会被传输到服务器以便进行校验,并确定计数器是

否相等(作为校验的一部分)。

[0116] 一个或多个计数器可以被配置为防止重放攻击。例如,如果已经获得并重放密码,如果计数器已经被读取、使用或以其他方式被忽略,则该密码立即被拒绝。如果计数器没有被使用,它可能被重放。在一些示例中,在卡上更新的计数器不同于被更新用于交易的计数器。在一些示例中,非接触式卡可以包括第一小程序和第二小程序,该第一小程序可以是交易小程序。每个小程序可以包括计数器。

[0117] 在一些示例中,计数器可能在非接触式卡和一个或多个服务器之间脱离同步。例如,非接触式卡可以被激活,从而使得计数器被更新,并且由非接触式卡生成新的通信,但是该通信可以不被传输以便在一个或多个服务器处进行处理。这可能导致非接触式卡的计数器和一个或多个服务器处维护的计数器脱离同步。这可能会无意地发生,包括例如,在卡被存储为靠近设备(例如,被携带在带有设备的袋中)的情况下,以及在非接触式卡以一定角度被读取的情况下,可能包括卡未对准或未被定位成使得非接触式卡在NFC场中被上电但不可读。如果非接触式卡被定位为靠近设备,则设备的NFC长可以被打开以向非接触式卡供电,从而导致其中的计数器被更新,但是设备上没有应用接收通信。

[0118] 为了保持计数器同步,可以执行应用(诸如后台应用),该应用将被配置为检测移动设备何时醒来并与指示由于检测而发生读取的一个或多个服务器同步,然后使计数器向前移动。由于非接触式卡的计数器和一个或多个服务器可能脱离同步,所以一个或多个服务器可以被配置为允许非接触式卡的计数器在其被一个或多个服务器读取之前被更新阈值次数或预定次数,并且仍然被认为是有效的。例如,如果计数器被配置为对于每次出现指示非接触式卡激活而递增(或递减)1,则一个或多个服务器可以允许从非接触式卡读取的任何计数器值为有效,或者允许阈值范围(例如,从1到10)内的任何计数器值。而且,如果计数器值超过10但是在另一阈值范围值(诸如1000)以下,则该一个或多个服务器可以被配置为请求与非接触式卡相关联的手势,诸如用户轻击。通过用户轻击,如果计数器值在期望的或可接受的范围内,则认证成功。

[0119] 图8是示出根据示例实施例的密钥操作800的流程图。如图8所示,在框810处,两个发卡行识别码(bank identifier number,BIN)级主密钥可以与账户标识符和卡序列号结合使用,以每张卡产生两个唯一导出密钥。在一些示例中,发卡行识别码可以包括一个编号或一个或多个编号的组合(诸如由一个或多个服务器提供的账号或不可预测的编号),可以用于会话密钥生成和/或多样化。在个性化过程期间,UDK(AUTKEY和ENCKEY)可能存储在卡上。

[0120] 在框820处,计数器可以被用作多样化数据,由于它随着每次使用而改变,并且每次提供不同的会话密钥,而不是其中每张卡产生唯一一组密钥的主密钥导出。在一些示例中,优选的是使用4字节方法用于两种操作。因此,在框820处,可以为来自UDK的每个交易创建两个会话密钥,即,来自AUTKEY的一个会话密钥和来自ENCKEY的一个会话密钥。在卡中,对于MAC密钥(即根据AUTKEY创建的会话密钥),OTP计数器的两个字节的低位可以用于多样化。对于ENC密钥(即根据ENCKEY创建的会话密钥),可以将OTP计数器的全长用于ENC密钥。

[0121] 在框830处,MAC密钥可以用于准备MAC密码,并且ENC密钥可以用于加密密码。例如,MAC会话密钥可以用于准备密码,并且结果可以在其被传输到一个或多个服务器之前利用ENC密钥加密。

[0122] 在框840处,简化了MAC的验证和处理,因为支付HSM的MAC认证功能中直接支持2字节多样化。密码的解密是在验证MAC之前进行的。会话密钥在一个或多个服务器处独立导出,从而产生第一会话密钥(ENC会话密钥)和第二会话密钥(MAC会话密钥)。第二导出密钥(即ENC会话密钥)可以用于解密数据,并且第一导出密钥(即MAC会话密钥)可以用于验证解密的数据。

[0123] 对于非接触式卡,导出可能与编码在卡中的应用主账号(primary account number,PAN)和PAN序列号相关的不同的唯一标识符。密钥多样化可以被配置为利用主密钥接收标识符作为输入,使得可以为每个非接触式卡创建一个或多个密钥。在一些示例中,这些多样化密钥可以包括第一密钥和第二密钥。第一密钥可以包括认证主密钥(卡密码生成/认证密钥——Card-Key-Auth),并且可以进一步被多样化以创建在生成和验证MAC密码时使用的MAC会话密钥。第二密钥可以包括加密主密钥(卡数据加密密钥——Card-Key-DEK),并且可以被进一步多样化以创建在加密和解密加密数据时使用的ENC会话密钥。在一些示例中,第一密钥和第二密钥可以通过将发行方主密钥与卡的唯一ID号(pUID)和支付小程序的PAN序列号(PAN sequence number,PSN)组合而将发行方主密钥多样化来创建。pUID可以包括16位数字值。如上所解释那样,pUID可以包括16位BCD编码的数字。在一些示例中,pUID可以包括14位数字值。

[0124] 在一些示例中,由于EMV会话密钥导出方法可以在2^16次使用时结束,所以诸如全32位计数器的计数器可以被添加到多样化方法的初始化数组中。

[0125] 在诸如信用卡的其他示例中,诸如账号或由一个或多个服务器提供的不可预测的编号的编号可以用于会话密钥生成和/或多样化。

[0126] 图9示出了被配置为实施本公开的一个或多个实施例的系统900的示意图。如下所解释的那样,在非接触式卡创建过程期间,可以为每个卡唯一地分配两个密码密钥。密码密钥可以包括对称密钥,该对称密钥可以用于数据的加密和解密两者。三重DES(3DES)算法可以由EMV使用,并由非接触式卡中的硬件实施。通过使用密钥多样化过程,可以基于需要密钥的每个实体的唯一可识别信息,从主密钥导出一个或多个密钥。

[0127] 关于主密钥管理,在其上发行一个或多个小程序的系列(portfolio)的每个部分可能需要两个发行方主密钥905、910。例如,第一主密钥905可以包括发行方密码生成/认证密钥(Iss-Key-Auth),并且第二主密钥910可以包括发行方数据加密密钥(Iss-Key-DEK)。如本文进一步解释的那样,两个发行方主密钥905、910被多样化为卡主密钥925、930,这些卡主密钥对于每张卡是唯一的。在一些示例中,作为后台数据的网络简档记录ID(pNPR)915和导出密钥索引(pDKI)920可以用于标识在用于认证的密码过程中使用哪些发行方主密钥905、910。执行认证的系统可以被配置为在认证时获取非接触式卡的pNPR 915和pDKI920的值。

[0128] 在一些示例中,为了增加解决方案的安全性,可以导出会话密钥(诸如每个会话的唯一密钥),但是不是使用主密钥,而是唯一的卡导出密钥和计数器可以被用作多样化数据,如上所解释那样。例如,每次在操作中使用卡时,可以使用不同的密钥用于创建消息认证码(MAC)和用于执行加密。关于会话密钥生成,用于生成密码和加密一个或多个小程序中的数据的密钥可以包括基于卡唯一密钥(Card-Key-Auth 925和Card-Key-Dek 930)的会话密钥。会话密钥(Aut-Session-Key 935和DEK-Session-Key 940)可以由一个或多个小程序

生成,并通过使用应用交易计数器945与一个或多个算法来导出。为了使数据适合一个或多个算法,仅使用4字节pATC 945的2个低位字节。在一些示例中,四字节会话密钥导出方法可以包括:F1:＝PATC(较低2个字节)||'F0'||'00'||PATC(四个字节)F1:＝PATC(较低2个字节)||'0F'||'00'||PATC(四个字节)SK:＝{(ALG(MK)[F1])||ALG(MK)[F2]},其中ALG可以包括3DES ECB,并且MK可以包括卡唯一导出主密钥。

[0129] 如本文所述,可以使用pATC 945计数器的较低两个字节来导出一个或多个MAC会话密钥。在非接触式卡的每次轻击时,pATC 945被配置为被更新,并且卡主密钥Card-Key-AUTH 925和Card-Key-DEK 930被进一步多样化为会话密钥Aut-Session-Key 935和DEK-Session-KEY 940。pATC 945可以在个性化或小程序初始化时初始化为零。在一些示例中,pATC计数器945可以在个性化时或之前初始化,并且可以被配置为在每次NDEF读取时递增1。

[0130] 进一步,每个卡的更新可以是唯一的,并且可以通过个性化来分配,或者通过pUID或其他标识信息在算法上被分配。例如,奇数卡可以递增或递减2,并且偶数卡可以递增或递减5。在一些示例中,更新也可以在顺序读取中变化,使得一张卡可以按顺序递增1、3、5、2、2、……重复。特定序列或算法序列可以在个性化时定义,或者根据从唯一标识符导出的一个或多个过程定义。这使得重放攻击者更难从较少数量的卡实例中进行归纳。

[0131] 认证消息可以作为呈十六进制ASCII格式的文本NDEF记录的内容递送。在一些示例中,可以仅包括认证数据和后边是认证数据的MAC的8字节随机数。在一些示例中,随机数可以在密码A之前,并且可以是一个块长。在其他示例中,在随机数的长度方面可能没有限制。在另外的示例中,总数据(即随机数加上密码)可以是块大小的倍数。在这些示例中,可以添加附加的8字节块来匹配由MAC算法产生的块。作为另一示例,如果所采用的算法使用16字节的块,甚至可以使用该块大小的倍数,或者输出可以被自动或手动填充到该块大小的倍数。

[0132] MAC可以通过功能密钥(AUT-Session-Key)935来执行。密码中指定的数据可以利用javacard.signature方法:ALG_DES_MAC8_ISO9797_1_M2_ALG3处理从而与EMV ARQC验证方法相关。如上所解释那样,用于这个计算的密钥可以包括会话密钥AUT-Session-Key 935。如上所解释那样,计数器的低位两个字节可以用于使一个或多个MAC会话密钥多样化。如下所解释那样,AUT-Session-Key 935可以用于MAC数据950,并且可以使用DEK-Session-Key 940对所得到的数据或密码A 955和随机数RND进行加密,以创建在消息中发送的密码B或输出960。

[0133] 在一些示例中,可以处理一个或多个HSM命令用于解密,使得最终的16(二进制、32十六进制)字节可以包括使用CBC模式的3DES对称加密,其中随机数的第四个零后面是MAC认证数据。用于这种加密的密钥可以包括从Card-Key-DEK 930导出的会话密钥DEK-Session-Key 940。在这种情况下,会话密钥导出的ATC值是计数器pATC945的最低有效字节。

[0134] 下面的格式表示二进制版本示例实施例。进一步,在一些示例中,第一个字节可以被设置为ASCII‘A’。

[0135]

消息格式				
1	2	4	8	8
0x43（消息类型‘A’）	版本	pATC	RND	密码 A（MAC）

[0136]

密码 A（MAC）	**8 字节**			
MAC				
2	8	4	4	18 字节输入数据
版本	pUID	pATC	共享秘密	

消息格式			
1	2	4	16
0x43（消息类型‘A’）	版本	pATC	密码 B
密码 A（MAC）	**8 字节**		
MAC			

[0137]

2	8	4	4	18 字节输入数据
版本	pUID	pATC	共享秘密	
密码 B	**16**			
对称加密				
8	8			

[0138]

RND	密码 A		

[0139] 另一示例性格式在下文示出。在这个示例中,标签可以以十六进制格式编码。

[0140]

消息格式				
2	8	4	8	8
版本	pUID	pATC	RND	密码 A（MAC）
8 字节				
8	8	4	4	18 字节输入数据
pUID	pUID	pATC	共享秘密	

[0141]

消息格式			
2	8	4	16
版本	pUID	pATC	密码 B
8 字节			

[0142]

8		4	4	18 字节输入数据
pUID	pUID	pATC	共享秘密	
密码 B	**16**			
对称加密				
8	8			
RND	密码 A			

[0143] 可以提取接收到的消息的UID字段,以从主密钥Iss-Key-AUTH 905和Iss-Key-DEK 910中导出该特定卡的卡主密钥(Card-Key-Auth 925和Card-Key-DEK 930)。使用卡主密钥(Card-Key-Auth 925和Card-Key-DEK 930),接收到的消息的计数器(pATC)字段可以用于导出该特定卡的会话密钥(Aut-Session-Key 935和DEK-Session-Key 940)。密码B 960可以使用DEK-Session-KEY解密,这产生密码A 955和RND,并且RND可以被丢弃。UID字段可以用于查找非接触式卡的共享秘密,该共享秘密与消息的版本、UID和pATC字段一起可以通过密码MAC使用重新创建的Aut-Session-Key进行处理,以创建MAC输出,诸如MAC'。如果MAC'与密码A 955相同,则这表明消息解密和MAC检查全部已通过。然后可以读取pATC以确定它是否有效。

[0144] 在认证会话期间,可以由一个或多个应用生成一个或多个密码。例如,可以通过一个或多个会话密钥(诸如Aut-Session-Key 935)使用具有方法2填充的ISO 9797-1算法3将一个或多个密码生成为3DES MAC。输入数据950可以采取以下形式:版本(2)、pUID(8)、pATC(4)和共享秘密(4)。在一些示例中,括号中的数字可以包括以字节为单位的长度。在一些示例中,共享秘密可以由一个或多个随机数生成器生成,该随机数生成器可以被配置为通过一个或多个安全过程来确保随机数是不可预测的。在一些示例中,共享秘密可以包括在由认证服务已知的个性化时间注入到卡中的随机4字节二进制数。在认证会话期间,共享秘密可以不从一个或多个小程序提供给移动应用。方法2填充可以包括向输入数据的末尾添加强制的0x'80'字节,并向所得到的数据的末尾添加0x'00'字节,直到8字节边界为止。所得到的密码在长度上可以包括8个字节。

[0145] 在一些示例中,利用MAC密码将非共享随机数加密为第一块的一个益处是,在使用对称加密算法的CBC(块链接)模式时,其充当初始化向量。这允许逐块地"加扰",而不必预先建立固定的或动态的IV。

[0146] 通过将应用交易计数器(pATC)包括作为包括在MAC密码中的数据的一部分,认证服务可以被配置为确定明文数据中输送的值是否已经被篡改。而且,通过将版本包含在一

个或多个密码中,攻击者难以在试图降低密码解决方案的强度时有目的地篡改应用版本。在一些示例中,pATC可以从零开始,并在每次一个或多个应用生成认证数据时更新1。认证服务可以被配置为跟踪在认证会话期间使用的pATC。在一些示例中,当认证数据使用等于或低于由认证服务接收的先前值的pATC时,这可能被解释为试图重放旧消息,并且被认证的消息可能被拒绝。在一些示例中,当pATC大于先前接收的值时,可以对其进行评估以确定它是否在可接受的范围或阈值内,并且如果它超过范围或阈值或在范围或阈值之外,则验证可以被认为已经失败或不可靠。在MAC操作936中,使用Aut-Session-Key 935通过MAC处理数据950,以产生加密的MAC输出(密码A)955。

[0147] 为了提供附加保护以防止暴露卡上密钥的暴力攻击,期望的是对MAC密码955进行加密。在一些示例中,密文中包括的数据或密码A 955可以包括:随机数(8)、密码(8)。在一些示例中,括号中的数字可以包括以字节为单位的长度。在一些示例中,随机数可以由一个或多个随机数生成器生成,该随机数生成器可以被配置为通过一个或多个安全过程来确保随机数是不可预测的。用于加密这个数据的密钥可以包括会话密钥。例如,会话密钥可以包括DEK-Session-Key 940。在加密操作941中,使用DEK-Session-Key 940处理数据或密码A 955和RND,以产生加密的数据,即密码B 960。数据955可以在密码块链接模式下使用3DES加密,以确保攻击者必须对全部密文进行任何攻击。作为非限制性示例,可以使用其他算法,诸如高级加密标准(Advanced Encryption Standard,AES)。在一些示例中,可以使用0x'00000000000000000'的初始化向量。试图强行破解用于加密这个数据的密钥的任何攻击者将无法确定何时已经使用了正确的密钥,因为正确解密的数据由于其随机出现而无法与不正确解密的数据区分开来。

[0148] 为了使认证服务校验由一个或多个小程序提供的一个或多个密码,必须在认证会话期间以明文的方式将以下数据从一个或多个小程序输送到移动设备:版本号,用于确定所使用的密码方法和用于密码的校验的消息格式,这使得该方法在将来能够改变;pUID,用于获取加密资产,并导出卡密钥;以及pATC,用于导出用于密码的会话密钥。

[0149] 图10示出了用于生成密码的方法1000。例如,在框1010处,网络简档记录ID(pNPR)和导出密钥索引(pDKI)可以用于标识在用于认证的密码过程中使用哪些发行方主密钥。在一些示例中,该方法可以包括执行认证以在认证时获取非接触式卡的pNPR和pDKI的值。

[0150] 在框1020处,可以通过将发行方主密钥与一个或多个小程序(例如支付小程序)的卡的唯一ID号(pUID)和PAN序列号(PSN)组合来使发行方主密钥多样化。

[0151] 在框1030处,可以通过使发行方主密钥多样化来创建Card-Key-Auth和Card-Key-DEK(唯一的卡密钥),以生成可以用于生成MAC密码的会话密钥。

[0152] 在框1040处,用于生成密码和加密一个或多个小程序中的数据的密钥可以包括基于卡唯一密钥(Card-Key-Auth和Card-Key-DEK)的框1030的会话密钥。在一些示例中,这些会话密钥可以由一个或多个小程序生成,并通过使用pATC导出,从而产生会话密钥Aut-Session-Key和DEK-Session-Key。

[0153] 图11描绘了示出根据一个示例的密钥多样化的示例性过程1100。最初,发送者和接收者可以被提供有两个不同的主密钥。例如,第一主密钥可以包括数据加密主密钥,并且第二主密钥可以包括数据完整性主密钥。发送者具有可以在框1110处被更新的计数器值以及发送者可以与接收者安全共享的其他数据(诸如要保护的数据)。

[0154] 在框1120处,计数器值可以由发送者使用数据加密主密钥加密以产生数据加密导出的会话密钥,并且计数器值也可以由发送者使用数据完整性主密钥加密以产生数据完整性导出的会话密钥。在一些示例中,在两次加密期间,可以使用整个计数器值或计数器值的一部分。

[0155] 在一些示例中,计数器值可能未加密。在这些示例中,计数器可以在发送者和接收者之间以明文的方式传输,即无需加密。

[0156] 在框1130处,发送者使用数据完整性会话密钥和密码MAC算法,利用加密MAC操作来处理要保护的数据。受保护数据(包括明文和共享秘密)可以使用会话密钥(AUT-Session-Key)中的一个来产生MAC。

[0157] 在框1140处,可以由发送者使用数据加密导出的会话密钥结合对称加密算法来加密要保护的数据。在一些示例中,MAC与等量的随机数据组合(例如每8字节长),并且然后使用第二会话密钥(DEK会话密钥)对其进行加密。

[0158] 在框1150处,加密的MAC被从发送者传输到接收者,具有足够的信息来标识附加的秘密信息(例如共享秘密、主密钥等)以便进行密码验证。

[0159] 在框1160处,接收方使用接收到的计数器值从两个主密钥中独立地导出两个导出的会话密钥,如上所解释那样。

[0160] 在框1170处,结合对称解密操作使用数据加密导出的会话密钥来解密受保护数据。然后将进行对交换的数据的附加处理。在一些示例中,在提取MAC之后,期望的是再现和匹配MAC。例如,当验证密码时,可以使用适当生成的会话密钥对其进行解密。受保护数据可以被重建以便进行验证。可以使用适当生成的会话密钥来执行MAC操作,以确定它是否匹配解密的MAC。由于MAC操作是不可逆的过程,唯一的验证方法是尝试从源数据中重新创建它。

[0161] 在框1180处,结合密码MAC操作使用数据完整性导出会话密钥来验证受保护数据没有被修改。

[0162] 当满足以下条件时,本文描述的方法的一些示例可以有利地确认何时确定成功认证。首先,验证MAC的能力表明导出会话密钥是正确的。只有在解密成功并产生正确的MAC值的情况下,MAC才可能是正确的。成功解密可能表明正确导出的加密密钥用于解密加密的MAC。由于导出的会话密钥是使用仅发送者(例如,发送设备)和接收者(例如,接收设备)已知的主密钥创建的,因此可以相信最初创建MAC并加密MAC的非接触式卡确实是真实的。而且,用于导出第一会话密钥和第二会话密钥的计数器值可以被示出为有效,并且可以用于执行认证操作。

[0163] 此后,可以丢弃两个导出的会话密钥,并且数据交换的下一次迭代将更新计数器值(返回到框1110),并且可以创建新的一组会话密钥(在框1120处)。在一些示例中,可以丢弃组合的随机数据。

[0164] 本文描述的系统和方法的示例实施例可以被配置为提供安全因素认证。安全因素认证可以包括多个过程。作为安全因素认证的一部分,第一过程可以包括通过在设备上执行的一个或多个应用登录并校验用户。作为第二过程,用户可以响应于通过一个或多个应用进行的第一过程的成功登录和校验,参与与一个或多个非接触式卡相关联的一个或多个行为。实际上,安全因素认证可以包括安全地证明用户的身份和参与与非接触式卡相关联的一种或多种类型的行为,包括但不限于一个或多个轻击手势。在一些示例中,一个或多个

轻击手势可以包括由用户针在设备上轻击非接触式卡。在一些示例中,该设备可以包括移动设备、信息亭、终端、平板电脑或被配置为处理接收到的轻击手势的任何其他设备。

[0165] 在一些示例中,非接触式卡可以在设备(诸如一个或多个计算机信息亭或终端)上被轻击,以验证身份,从而接收响应于购买的交易物品,诸如咖啡。通过使用非接触式卡,可以建立在忠诚计划(loyalty program)中证明身份的安全方法。以不同于仅仅扫描条码卡的方式来建立安全地证明身份,例如以获得奖励、优惠券、优惠等或益处的接收。例如,加密的交易可以发生在非接触式卡和设备之间,该设备可以被配置为处理一个或多个轻击手势。如上所解释那样,一个或多个应用可以被配置为校验用户的身份,并且然后使用户例如通过一个或多个轻击手势来行动或对其进行响应。在一些示例中,数据例如奖金积分、忠诚度积分、奖励积分、医疗保健信息等可以被写回到非接触式卡。

[0166] 在一些示例中,非接触式卡可以在诸如移动设备的设备上被轻击。如上所解释那样,用户的身份可以由一个或多个应用验证,然后该应用将基于身份的验证向用户授予期望的益处。

[0167] 在一些示例中,非接触式卡可以通过在诸如移动设备的设备上被轻敲来激活。例如,非接触式卡可以通过NFC通信经由设备的读卡器与设备的应用进行通信。其中在设备的读卡器附近轻击卡的通信可以允许设备的应用读取与非接触式卡相关联的数据并激活卡。在一些示例中,激活可以授权卡用于执行其他功能,例如购买、访问账户或受限信息或其他功能。在一些示例中,轻击可以激活或启动设备的应用,并且然后发起一个或多个动作或与一个或多个服务器的通信来激活非接触式卡。如果该应用没有安装在该设备上,则在读卡器附近轻击非接触式卡可以发起该应用的下载,诸如导航到该应用的下载页面。安装之后,轻击非接触式卡可以激活或启动应用,并且然后例如通过应用或其他后端通信发起非接触式卡的激活。激活后,非接触式卡可以用于各种活动,包括但不限于商业交易。

[0168] 在一些实施例中,专用应用可以被配置为在客户端设备上运行,以执行非接触式卡的激活。在其他实施例中,网络门户、基于网络的应用、小程序等可以执行激活。激活可以在客户端设备上执行,或者客户端设备可以仅充当非接触式卡和外部设备(例如,账户服务器)之间的媒介。根据一些实施例,在提供激活时,应用可以向账户服务器指示执行激活的设备的类型(例如,个人计算机、智能手机、平板电脑或销售点(point-of-sale,POS)设备)。进一步,取决于所涉及的设备类型,该应用可以向账户服务器输出不同的和/或附加的数据用于传输。例如,这样的数据可以包括与商家相关联的信息,诸如商家类型、商家ID、以及与设备类型本身相关联的信息,诸如POS数据和POS ID。

[0169] 在一些实施例中,示例认证通信协议可以模仿通常在交易卡和销售点设备之间执行的、具有一些修改的EMV标准的离线动态数据认证协议。例如,因为示例认证协议本身不用于完成与卡发行方/支付处理器的支付交易,所以不需要一些数据值,并且可以在不涉及与卡发行方/支付处理器的实时在线连接的情况下执行认证。如本领域所知,销售点(POS)系统向卡发行方提交包括交易值的交易。发行方是否批准或否定交易可能基于发行方是否认可交易值。同时,在本公开的一些实施例中,源自移动设备的交易缺少与POS系统相关联的交易值。因此,在一些实施例中,伪交易值(即,卡发行方可识别的并且足以允许激活发生的值)可以作为示例认证通信协议的一部分被传递。基于POS的交易也可以基于交易尝试的数量(例如,交易计数器)拒绝交易。超过缓冲值的尝试数量可能会导致软拒绝;软拒绝在接

受交易前需要进一步验证。在一些实施方式中,可以修改交易计数器的缓冲值,以避免拒绝合法交易。

[0170] 在一些示例中,非接触式卡可以根据接收方设备选择性地传送信息。一旦被轻击,非接触式卡可以识别轻击所针对的设备,并且基于这个识别,非接触式卡可以为该设备提供适当的数据。这有利地允许非接触式卡仅传输完成即时动作或交易(诸如支付或卡认证)所需的信息。通过限制数据传输和避免不必要的数据传输,可以提高效率和数据安全两者。信息的识别和选择性通信可以应用于各种场景,包括卡激活、余额转移、账户访问尝试、商业交易和逐步(step-up)欺诈减少。

[0171] 如果非接触式卡轻击是针对运行苹果iOS®操作系统的设备(例如iPhone、iPod或iPad)进行的,则非接触式卡可以识别iOS®操作系统并传输适当的数据来与这个设备通信。例如,非接触式卡可以通过例如NFC提供使用NDEF标签认证卡所需的加密的身份信息。类似地,如果非接触式卡轻击是针对运行Android®操作系统的设备(例如,Android®智能手机或平板电脑)进行的,则非接触式卡可以识别Android®操作系统,并传输适当的数据(诸如,通过本文描述的方法进行认证所需的加密的身份信息)以与这个设备通信。

[0172] 作为另一示例,非接触式卡轻击可以是针对POS设备(包括但不限于信息亭、结账登记器、支付站或其他终端)进行的。在执行轻击时,非接触式卡可以识别POS设备,并且仅传输动作或交易所需的信息。例如,在识别出用于完成商业交易的POS设备后,非接触式卡可以根据EMV标准传送完成交易所需的支付信息。

[0173] 在一些示例中,参加交易的POS设备可以要求或指定要由非接触式卡提供的附加信息,例如设备特定的信息、位置特定的信息和交易特定的信息。例如,一旦POS设备从非接触式卡接收到数据通信,POS设备就可以识别非接触式卡并请求完成动作或交易所需的附加信息。

[0174] 在一些示例中,POS设备可以附属于授权商家或熟悉一些非接触式卡或习惯于执行一些非接触式卡交易的其他实体。然而,应当理解的是,所描述的方法的执行不要求这种附属关系。

[0175] 在一些示例中,诸如购物商店、杂货店、便利店等,可以在移动设备上轻击非接触式卡而不必打开应用,以指示利用奖励积分、忠诚度积分、优惠券、优惠等中的一个或多个来覆盖一次或多次购买的期望或意图。因此,提供了购买背后的意图。

[0176] 在一些示例中,一个或多个应用可以被配置为确定它是经由非接触式卡的一个或多个轻击手势启动的,使得启动发生在下午3:51pm、交易在3:56pm处理或发生,以便验证用户的身份。

[0177] 在一些示例中,一个或多个应用可以被配置为响应于一个或多个轻击手势来控制一个或多个动作。例如,一个或多个动作可以包括收集奖励、收集积分、确定最重要的购买、确定最便宜的购买和/或实时地重新配置到另一动作。

[0178] 在一些示例中,可以收集关于轻击行为的数据作为生物特征/手势认证。例如,密码安全且不易被截取的唯一标识符可以被传输到一个或多个后端服务。唯一标识符可以被配置为查找关于个人的辅助信息。辅助信息可以包括关于用户的个人可标识信息。在一些

示例中,辅助信息可以存储在非接触式卡中。

[0179] 在一些示例中,该设备可以包括在多个个人之间划分支付的账单或支票的应用。例如,每个人可能拥有非接触式卡,并且可能是相同发行金融机构的客户,但这不是必需的。这些个人中的每一个可以通过应用在他们的设备上接收推送通知,以划分购买。可以使用其他非接触式卡,而不是只接受一次卡轻击来指示支付。在一些示例中,具有不同金融机构的个人可能拥有非接触式卡,以提供信息来发起来自卡轻击个人的一个或多个支付请求。

[0180] 以下示例用例描述了本公开的特定实施方式的示例。这些仅旨在用于解释目的,而非用于限制目的。在一种情况下,第一个朋友(付款人)欠第二个朋友(收款人)一笔钱。付款人希望使用非接触式卡通过收款人的智能手机(或其他设备)付款,而不是去ATM或需要通过对等应用进行兑换。收款人登录到其智能手机上的适当应用,并选择付款请求选项。作为响应,应用通过收款人的非接触式卡请求认证。例如,应用输出请求收款人轻击他的非接触式卡的显示。一旦收款人在具有所支持的应用的智能手机的屏幕上轻击他的非接触式卡,非接触式卡就会被读取和验证。接下来,应用显示付款人轻击他的非接触式卡发送付款的提示。在付款人轻击非接触式卡后,应用读取卡信息,并通过相关联的处理器向付款人的卡发行方传输付款请求。卡发行方处理交易,并向智能手机发送交易的状态指示符。然后,应用输出以便显示交易的状态指示符。

[0181] 在另一示例情况下,信用卡客户可以以邮件的方式接收新的信用卡(或借记卡、其他支付卡或需要激活的任何其他卡)。客户可以决定通过他或她的设备(例如,诸如智能手机的移动设备)上的应用来激活卡,而不是通过呼叫与卡发行方相关联的所提供的电话号码或访问网站来激活卡。客户可以从设备的显示器上显示的应用菜单中选择卡激活特征。应用可以提示客户在屏幕上轻击他或她的信用卡。在设备的屏幕上轻敲信用卡时,应用可以被配置为与服务器(诸如激活客户的卡的卡发行方服务器)通信。然后,应用可以显示指示卡的成功激活的消息。然后卡激活完成。

[0182] 图12示出了根据示例实施例的用于卡激活的方法1200。例如,卡激活可以由包括卡、设备和一个或多个服务器的系统来完成。非接触式卡、设备和一个或多个服务器可以引用前面参考图1A、图1B、图5A和图5B解释的相同或相似的组件,诸如非接触式卡105、客户端设备110和服务器120。

[0183] 在框1210中,卡可以被配置为动态生成数据。在一些示例中,该数据可以包括诸如账号、卡标识符、卡验证值或电话号码的信息,这些信息可以从卡传输到设备。在一些示例中,数据的一个或多个部分可以通过本文公开的系统和方法加密。

[0184] 在框1220中,动态生成的数据的一个或多个部分可以经由NFC或其他无线通信被传送到设备的应用。例如,在设备附近轻击卡可以允许设备的应用读取与非接触式卡相关联的数据的一个或多个部分。在一些示例中,如果设备不包括帮助激活卡的应用,则轻击卡可以指引设备或提示客户到软件应用商店下载相关联的应用来激活卡。在一些示例中,可以提示用户朝向设备的表面对卡充分地设置姿态、放置或定向,诸如以某个角度或者平坦地放置在设备的表面上、附近或邻近该设备的表面。响应于卡的足够的姿态、放置和/或定向,设备可以继续将从卡接收的数据的一个或多个加密的部分传输到一个或多个服务器。

[0185] 在框1230中,数据的一个或多个部分可以被传送到一个或多个服务器,诸如卡发

行方服务器。例如,数据的一个或多个加密的部分可以从设备传输到卡发行方服务器以激活卡。

[0186] 在框1240中,一个或多个服务器可以通过本文公开的系统和方法解密数据的一个或多个加密的部分。例如,一个或多个服务器可以从设备接收加密的数据,并且可以对其进行解密,以便将接收到的数据与一个或多个服务器可访问的记录数据进行比较。如果由一个或多个服务器进行的对数据的一个或多个解密的部分的所得到的比较产生成功的匹配,则卡可以被激活。如果由一个或多个服务器进行的对数据的一个或多个解密部分的所得到的比较产生不成功的匹配,则可以发生一个或多个过程。例如,响应于不成功匹配的确定,可以提示用户再次轻击、刷或挥动卡。在这种情况下,可能存在包括准许用户激活卡的尝试次数的预定阈值。可替选地,用户可以接收通知(诸如在他或她的设备上的指示卡验证的不成功尝试的并且用于呼叫、通过电子邮件发送或通过文本发送相关服务以帮助激活卡的消息)、或者另一通知(诸如在他或她的设备上的指示卡验证的不成功尝试的并且用于呼叫、通过电子邮件发送或通过文本发送相关联的服务以帮助激活卡的电话呼叫)、或者另一通知(诸如指示卡验证的不成功尝试的并用于呼叫、通过电子邮件发送或通过文本发送相关联的服务以帮助激活卡的电子邮件)。

[0187] 在框1250中,一个或多个服务器可以基于卡的成功激活来传输返回消息。例如,设备可以被配置为从一个或多个服务器接收指示由一个或多个服务器成功激活卡的输出。设备可以被配置为显示指示卡的成功激活的消息。一旦卡被激活,卡可以被配置为不继续动态生成数据,以避免欺诈性使用。以这样的方式,此后该卡可以不被激活,并且通知一个或多个服务器该卡已经被激活。

[0188] 在另一示例中,客户想要访问他或她的移动电话上的金融账户。客户在移动设备上启动应用(例如,银行应用),并输入用户名和密码。在这个阶段,客户可能会看到一级账户信息(例如,最近的购买),并能够执行一级账户选项(例如,支付信用卡)。但是,如果用户试图访问二级账户信息(例如,支出限额)或执行二级账户选项(例如,转移到外部系统),他必须具有二级身份验证。因此,应用请求用户提供交易卡(例如,信用卡)以便进行账户验证。然后,用户在移动设备上轻击他的信用卡,并且应用验证信用卡是否与用户的账户对应。此后,用户可以查看二级账户数据和/或执行二级账户功能。

[0189] 在本发明的一些实施例中,非接触式卡的密码认证可以用于为交易(包括支付交易)提供进一步的认证。进一步的认证可以为交易提供附加的安全级别,包括但不限于验证交易中涉及的特定账户的授权用户的存在和批准,从而创建对于随后的交易核对离线的授权用户的存在的密码证明,以及降低用户欺诈的可能性(例如,通过稍后声称授权交易未被授权)。此外,可以在各种情况下提供进一步的认证,而减少、最小化或不需要其他交易参与者(例如,供应商、商家等)升级交易处理装备和要求。

[0190] 图13示出了用于这种实施方式的示例系统,该图示出了使用非接触式卡的系统1300。类似于图3中示出的系统,系统1300可以包括非接触式卡1305、一个或多个客户端设备1310、网络1315、认证服务器1320、商家服务器1325和数据库1330。尽管图13示出了组件的单个实例,但是系统1300可以包括任意数量的组件。

[0191] 在一些示例中,非接触式卡1305可以与客户端设备1310进行无线通信,例如,NFC或其他形式的无线通信。非接触式卡1305可以参考图5A和图5B中示出的非接触式卡的相同

或相似组件。非接触式卡1305可以包括基底、处理器(例如EMV芯片)和存储器。在一些示例中,非接触式卡1305可以包括建筑物出入卡、信用卡、借记卡、身份证、忠诚计划卡和交通卡中的至少一种。

[0192] 非接触式卡1305还可以包括第一小程序1306和第二小程序1307。在一些示例中,第一小程序1306可以是与第二小程序1307不同的小程序,并且第一小程序1306和第二小程序1307两者可以各自与一个或多个小程序标识符相关联。在一些示例中,第一小程序1306可以是支付小程序(例如,Java卡支付小程序),并且可以被禁止与诸如客户端设备1310的其他设备通信。在一些示例中,第一小程序1306可以仅与第二小程序1307通信,并且第二小程序1307可以被配置为与客户端设备1310或其他设备通信。在这些示例中,第一小程序1306可以向第二小程序1307提供数据,用于与客户端设备1310或其他设备进行通信。在一些示例中,第二小程序1307可以是支付小程序,例如Java卡支付小程序,或者第二小程序1307可以是安全小程序、通信小程序、认证小程序、密码小程序、前述小程序的改编,或者能够执行本文描述的功能的其他小程序。进一步,尽管图13示出了第一小程序1306和第二小程序1307,但是应当理解,系统1300可以包括两个以上的小程序,并且第一小程序1306和第二小程序1307中的每一个的特征和功能可以在多个小程序之间划分并由多个小程序执行。还应当理解,可以包括附加的小程序来提供附加的功能。

[0193] 在一些示例中,第二小程序1307可以控制由第一小程序1306提供的数据何时可以被传送到客户端设备1310或其他设备。例如,第二小程序1307可以被配置为在完成认证程序时或者在从认证服务器1320接收认证已经完成的通知或信号时,允许由第一小程序1306进行数据的通信。示例性认证程序可以包括但不限于,将非接触式卡1305带入客户端设备1310的通信场内,提供访问凭证或其他标识信息(例如,密码或PIN),通过本文描述的方法生成密码,完成第二因素认证,提供生物特征信息,以及本文描述的其他方法,或其组合。第二小程序1307可以执行认证程序并提供支持这个程序的信息,或者认证过程可以由客户端设备1310、认证服务器1320或其组合来执行。在一些示例中,第二小程序1307在非接触式卡1305上的存在可以导致认证程序开始。

[0194] 在一些示例中,第一小程序1306可以被配置为直接向客户端设备1310或其他设备传送数据。这个通信可以由第二小程序1307控制,并且第二小程序1307可以阻止由第一小程序1306进行的通信,直到认证程序完成或者接收认证通知或认证信号为止。

[0195] 在一些示例中,客户端设备1310可以是计算机设备、或通信设备,包括例如服务器、网络设备、个人计算机(personal computer,PC)、工作站、移动设备、电话、手持PC、个人数字助理(personal digital assistant,PDA)、瘦客户端、胖客户端、互联网浏览器或其他设备。客户端设备1310也可以是移动设备;例如,移动设备可以包括来自Apple®的iPhone、iPod、iPad或运行苹果的iOS操作系统的任何其他移动设备、运行微软Windows® Mobile操作系统的任何设备、运行Android操作系统的任何设备、和/或任何其他智能手机或类似的可穿戴移动设备。客户端设备1310可以经由一个或多个网络1315与一个或多个服务器(诸如认证服务器1320和商家服务器1325)以及支付终端1335通信,并且可以作为与一个或多个服务器的相应前端到后端对来操作。客户端设备1310可以例如从在设备1310上执行的移动设备应用向一个或多个服务器传输一个或多个请求。一个或多个请求可以与从一个或多个服务器获取数据相关联。

[0196] 系统1300可以包括一个或多个网络1315。在一些示例中,网络1315可以是无线网络、有线网络或无线网络和有线网络的任意组合中的一个或多个,并且可以被配置为将客户端设备1310连接到一个或多个服务器。例如,网络1315可以包括光纤网络、无源光网络、线缆网络、互联网网络、卫星网络、无线LAN、全球移动通信系统(Global System for Mobile Communication,GSM)、个人通信服务(Personal Communication Service,PCS)、个人区域网、无线应用协议(Wireless Application Protocol,WAP)、多媒体消息收发服务(Multimedia Messaging Service,MMS)、增强型消息收发服务(Enhanced Messaging Service,EMS)、短消息服务(Short Message Service,SMS)、基于时分复用(Time Division Multiplexing,TDM)的系统、基于码分多址(Code Division Multiple Access,CDMA)的系统、D-AMPS、Wi-Fi、固定无线数据、IEEE 802.11b、802.15.1、802.11n和802.11g、蓝牙、近场通信(Near Field Communication,NFC)、射频识别(Radio Frequency Identification,RFID)、Wi-Fi和/或其他中的一个或多个。

[0197] 此外,网络1315可以包括但不限于电话线、光纤、IEEE以太网902.3、广域网(wide area network,WAN)、无线个人区域网、局域网(local area network,LAN)或诸如互联网的全球网络。此外,网络1315可以支持互联网、无线通信网络、蜂窝网络等,或者它们的任意组合。网络1315还可以包括一个网络,或者作为独立的网络或者彼此合作地操作的任何数量的以上提及的示例性类型的网络。网络1315可以利用它们通信耦合到的一个或多个网络元件的一个或多个协议。网络1315可以将其他协议转换成或从其他协议转换成网络设备的一个或多个协议。尽管网络1315被描绘为单个网络,但是应当理解的是,根据一个或多个示例,网络1315可以包括多个互连的网络,例如互联网、服务提供商的网络、线缆电视网络、诸如信用卡协会网络的公司网络、以及家庭网络。

[0198] 系统1300可以包括一个或多个服务器,诸如认证服务器1320和商家服务器1325。在一些示例中,一个或多个服务器可以包括耦接到存储器的一个或多个处理器。一个或多个服务器可以被配置为用于在不同时间控制和调用各种数据来执行多个工作流动作以便执行本文中描述的一个或多个功能的中央系统、服务器或平台。一个或多个服务器可以包含一个或多个数据库,或者与一个或多个数据库进行数据通信。一个或多个服务器可以与至少一个客户端设备1310进行数据通信。

[0199] 系统1300可以包括支付终端1335。支付终端1335可以是服务器,如认证服务器1320或商家服务器1325,或者可以具有不同的配置。示例性配置包括但不限于电子支付亭、支付读取器、收银机或适合参与交易的任何其他设备。支付终端1335可以经由网络1315与系统1300的其他组件(包括客户端设备1310、认证服务器1320和商家服务器1325)进行数据通信。

[0200] 系统1300可以包括数据库1330。数据库1330可以是关系型或非关系型数据库,并且由数据库1330包含的数据可以存储在单个数据库或多个分离的数据库中。数据库1330可以包含但不限于账户和交易信息、标识信息、用户信息以及支持交易和执行本文描述的功能所需的其他信息。

[0201] 图14示出了根据示例实施例的认证交易的方法的流程图,其中该方法可以由例如系统1300实施。在步骤1402处,发起卡交易。例如,当在支付终端1335处呈现非接触式卡1305用于支付商品或服务时可以进行发起卡交易,这是“卡存在”交易。可替选地,当非接触

式卡1305用于“卡不存在交易”中的支付时,诸如当在网站上输入与卡相关联的账号来支付商品或服务时,可以进行发起卡交易。

[0202] 在步骤1404处,交易请求被发送到认证服务器1320。在卡存在交易的情况下,交易请求可以起源于支付终端1335。可选地,在卡不存在交易的情况下,交易请求可以源自客户端设备1310。交易请求最初可以被发送到商家服务器1325,即,属于正在从其购买商品或服务的商家的服务器。交易请求然后可以通过一个或多个中介(诸如银行服务器或支付机构服务器)从商家服务器发送到认证服务器1320。

[0203] 在步骤1406处,在接收交易请求时,认证服务器1320确定所请求的交易是否是高风险交易。例如在交易要和与欺诈交易有关联的商家进行的情况下,交易可能是高风险交易。作为另一示例,在交易要和与位于与欺诈交易相关联的地理区域中的商家进行的情况下,则交易也可能是高风险交易。进一步,如果交易不符合持卡人的历史交易模式,并且例如基于持卡人的交易历史在不寻常的时间或不寻常的地理区域进行,则该交易可以被指定为高风险交易。高风险交易附加地可以是以异常频率进行的那些交易,或者是在大量其他交易的预定时间段内发生的那些交易。高风险交易还可能是与已知过去有欺诈性活动或潜在的欺诈性的过去活动的其他账户、商家还是其他进行的那些交易。当做出确定时,认证服务器1320可以参考存储在数据库1330中的持卡人的交易历史。

[0204] 如果在步骤1406处,认证服务器1320确定交易不是高风险交易(否),则该方法进行到步骤1408。在步骤1408处,认证服务器1320确定交易的值是否超过预定阈值。例如,认证服务器1320可以确定所请求的交易是否超过一定的美元金额。预定阈值可以由持卡人设置,或者可以由认证服务器1320自动设置。

[0205] 如果在步骤1408处,认证服务器1320确定交易的值没有超过预定阈值,则该方法前进到步骤1418,并且由认证服务器1320允许交易。

[0206] 然而,如果在步骤1406处,认证服务器1320确定交易是高风险交易(是),则该方法进行到步骤1410。同样地,如果在步骤1408处,认证服务器1320确定交易的值超过预定值(是),则该方法进行到步骤1410。当该方法进行到步骤1410时,暂时保持所请求的交易,等待进一步的认证。

[0207] 在步骤1410处,认证服务器1320经由网络1315向客户端设备1310发送用于非接触式卡认证的请求。该请求可以呈应用内通知、弹出通知、SMS消息、电子邮件或任何其他合适的通知的形式。请求可以解释需要进一步认证来进行所请求的交易,并且可以进一步提示持卡人将非接触式卡1305带入客户端设备1310的通信场中。

[0208] 为了更进一步的安全性,除了将非接触式卡1305带入通信场中之外,认证服务器1320可以附加地请求持卡人向客户端设备1310提供生物特征信息、提供PIN、提供密码或提供其他标识信息。客户端设备1310可以对照存储在存储器中的参考生物特征信息来验证所提供的生物特征信息。生物特征信息可以包括例如指纹信息、光学数据、面部识别和/或视网膜信息。

[0209] 在步骤1412处,持卡人可以在经由客户端设备1310接收用于非接触式卡认证请求时,将非接触式卡1305带入客户端设备1310的通信场中。

[0210] 当非接触式卡1305处于客户端设备1310的通信场中时,非接触式卡1305被认证。非接触式卡1305可以通过本文描述的过程中的任何一个进行认证。在一些示例中,客户端

设备1310的处理器1311可以验证由非接触式卡1305生成的MAC密码。处理器1311然后可以向认证服务器1320传送非接触式卡1305已经被验证。可替选地,由非接触式卡生成的MAC密码可以被传输到认证服务器1320用于验证。

[0211] 如果在步骤1414处,非接触式卡没有被认证(否),则认证服务器1320在步骤1416处拒绝所请求的交易,从而禁止交易被执行。当交易被拒绝时,认证服务器1320可以附加地向客户端设备1310传输通知持卡人交易已经被拒绝的通知。然后该方法结束。

[0212] 如果在步骤1414处非接触式卡被认证(是),则认证服务器1320在步骤1418处允许交易。当交易被允许时,认证服务器1320可以附加地向客户端设备1310传输通知持卡人交易已经被批准的通知。然后该方法结束。

[0213] 本文描述的系统1300和方法1400为使用非接触式卡的交易提供了改进的安全性。具体而言,要求使用非接触式卡和客户端设备进行密码认证可以防止持卡人丢失她的非接触式卡、非接触式卡被盗或者打印在非接触式卡上的信息被盗的情形。通过要求密码认证,除了提供非接触式卡之外,试图参与交易的人基本上必须证明她也拥有与非接触式卡相关联的客户端设备,并且进一步证明她能够访问客户端设备(即,可以使用PIN、密码或生物特征解锁)。这降低了非接触式卡被用于欺诈性用途的可能性。附加地,可能仅对于是高风险交易的或用于超过预定值的金额的建议的交易需要要求密码认证,使得持卡人不为每次交易负担额外的认证层。系统1300和方法1400的另外的优点是将安全特征结合到非接触式卡中,以及非接触式卡本身的使用允许提供本文描述的安全特征,而不需要修改系统的其他组件。

[0214] 另外,要求密码认证无需限于其中使用非接触式卡支付商品或服务的交易。本文描述的方法1400可以类似地应用于提供非接触式卡。例如,如果持卡人试图提供非接触式卡用于在线支付服务,诸如谷歌支付或苹果支付,可能类似地需要密码认证来验证试图提供非接触式卡的人确实拥有非接触式卡,而不是简单地使用打印在卡上的信息。这可以针对由可能已经通过非法手段获得了卡号、CVC和到期日期但实际上并不拥有非接触式卡的个人使用非接触式卡提供了安全性。

[0215] 在一些示例中,本公开涉及非接触式卡的轻击。然而,应当理解的是,本公开不限于轻击,并且本公开包括其他手势(例如,挥动或卡的其他移动)。

[0216] 在整个说明书和权利要求书中,以下术语至少采用在此明确相关联的含义,除非上下文另有明确规定。术语“或”旨在表示包含性的“或”。进一步,术语“一”、“一个”和“该”旨在表示一个或多个,除非另有说明或从上下文中清楚地指向单数形式。

[0217] 在本说明书中,已经阐述了许多具体细节。然而,应当理解的是,可以在没有这些具体细节的情况下实施所公开的技术。在其他情况下,没有详细示出公知的方法、结构和技术以便不模糊对本说明书的理解。对“一些示例”、“其他示例”、“一个示例”、“示例”、“各种示例”、“一个实施例”、“实施例”、“一些实施例”、“示例实施例”、“各种实施例”、“一种实施方式”、“示例实施方式”、“各种实施方式”、“一些实施方式”等的引用表明如此描述的所公开的技术的一个或多个实施方式可以包括特定的特征、结构或特性,但是并非每个实施方式必须包括特定的特征、结构或特性。进一步,短语“在一个示例中”、“在一个实施例中”或“在一个实施方式中”的重复使用不一定指相同的示例、实施例或实施方式,尽管它可以指相同的示例、实施例或实施方式。

[0218] 如本文所用,除非另有说明,否则使用序数形容词“第一”、“第二”、“第三”等来描述共同的对象仅指示所指的是相似对象的不同实例,并不旨在意味着如此描述的对象必须在时间上、空间上、等级上或以任何其他方式处于给定的顺序。

[0219] 虽然已经结合目前被认为是最实用的各种实施方式描述了所公开的技术的一些实施方式,但是应当理解的是,所公开的技术不限于所公开的实施方式,而是相反,旨在覆盖包括在所附权利要求的范围内的各种修改和等同布置。虽然本文使用了特定的术语,但是它们仅以一般的描述性意义使用,而不是为了限制的目的。

[0220] 该书面描述使用示例来公开所公开技术的一些实施方式(包括最佳模式),并且还使本领域的任何技术人员能够实践所公开技术的一些实施方式,包括制造和使用任何设备或系统以及执行任何结合的方法。所公开技术的一些实施方式的可专利范围定义在权利要求中,并且可以包括本领域技术人员想到的其他示例。如果这样的其它实例具有与权利要求的字面语言没有不同的结构元素,或者如果它们包括与权利要求的字面语言没有实质差异的等同结构元素,则这样的其它实例旨在在权利要求的范围内。

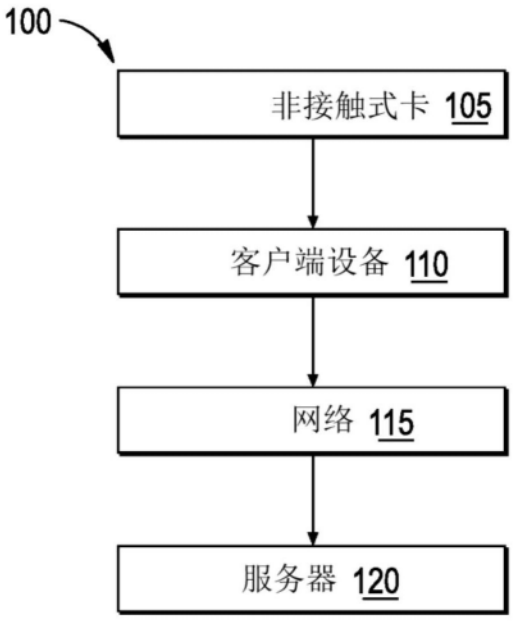

100
非接触式卡 105
客户端设备 110
网络 115
服务器 120

图1A

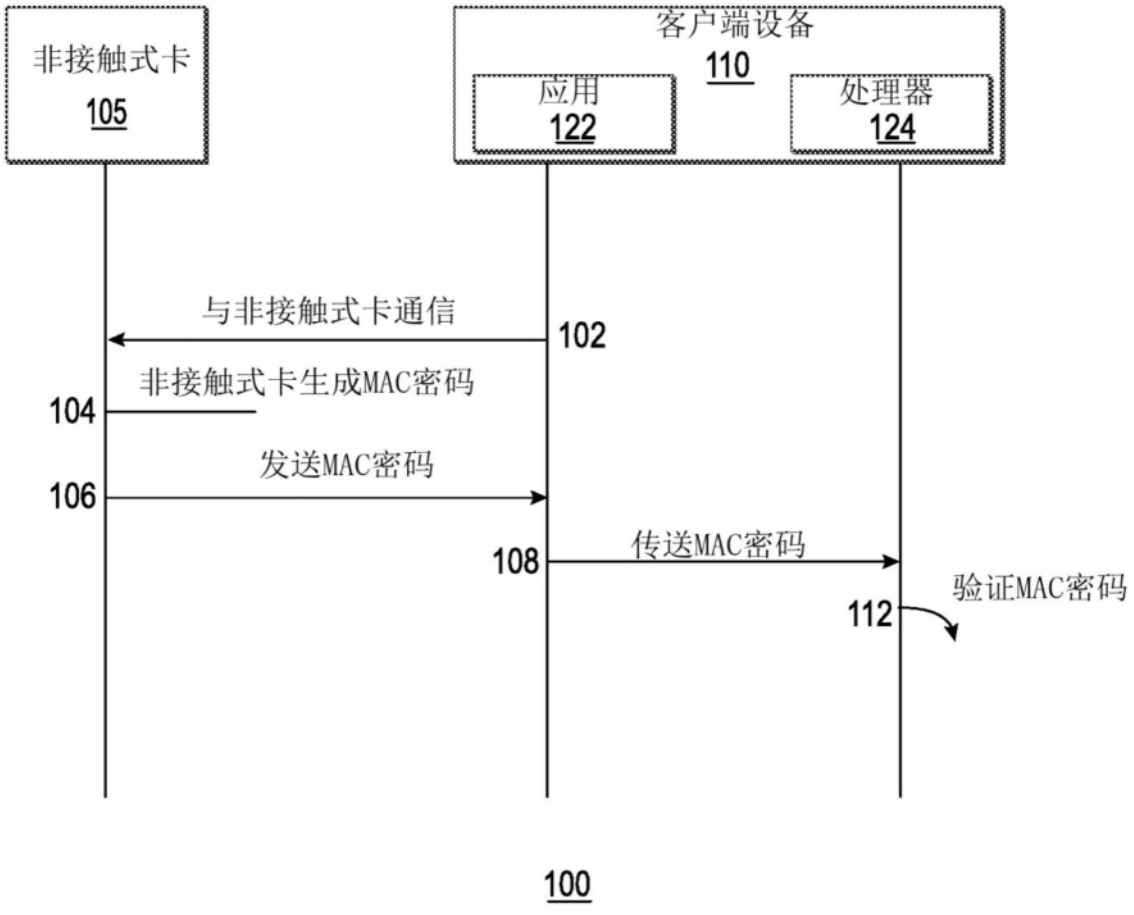

非接触式卡
105
客户端设备
110
应用
122
处理器
124
与非接触式卡通信
102
非接触式卡生成MAC密码
104
发送MAC密码
106
传送MAC密码
108
验证MAC密码
112
100

图1B

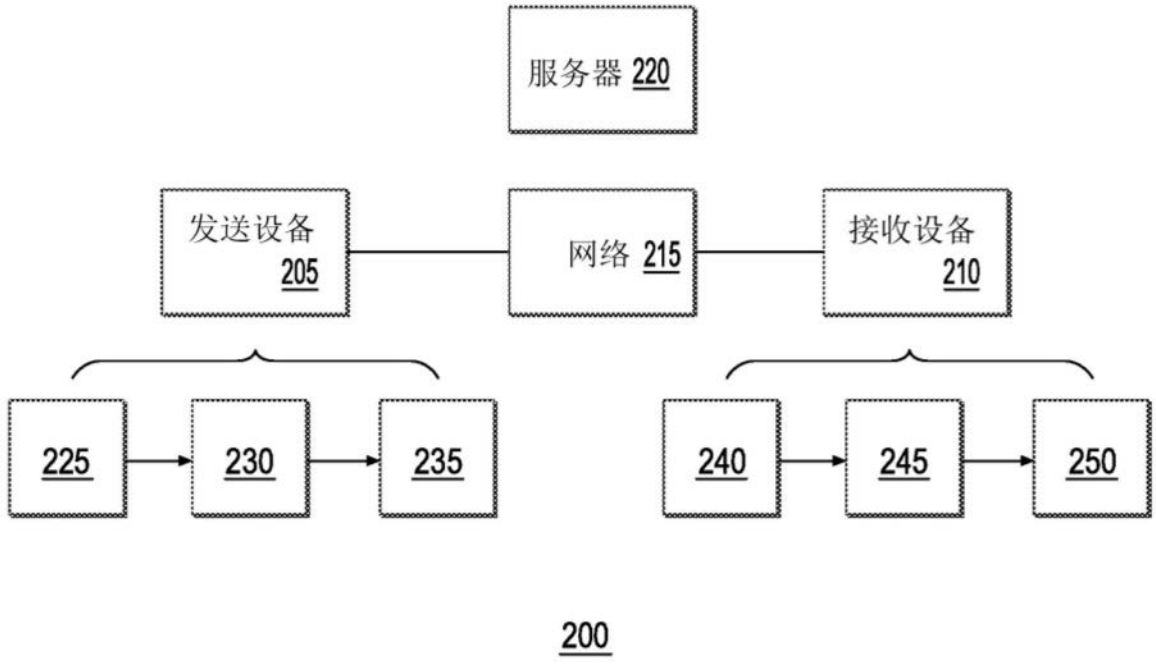

服务器 220
发送设备 205
网络 215
接收设备 210
225
230
235
240
245
250
200

图2

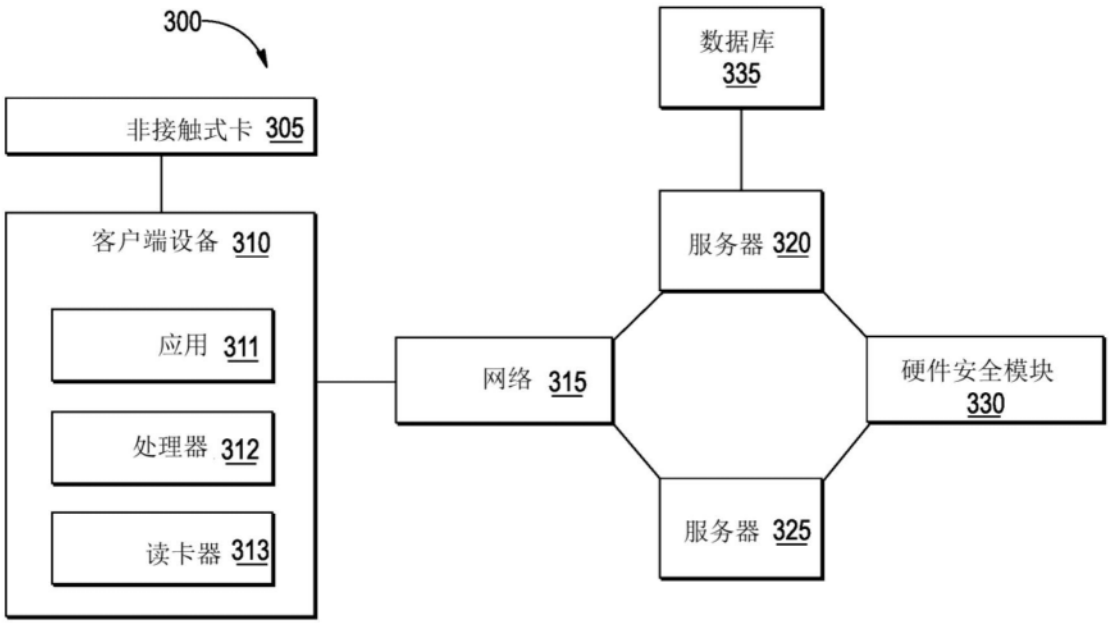

300
非接触式卡 305
客户端设备 310
应用 311
处理器 312
读卡器 313
网络 315
数据库 335
服务器 320
硬件安全模块 330
服务器 325

图3

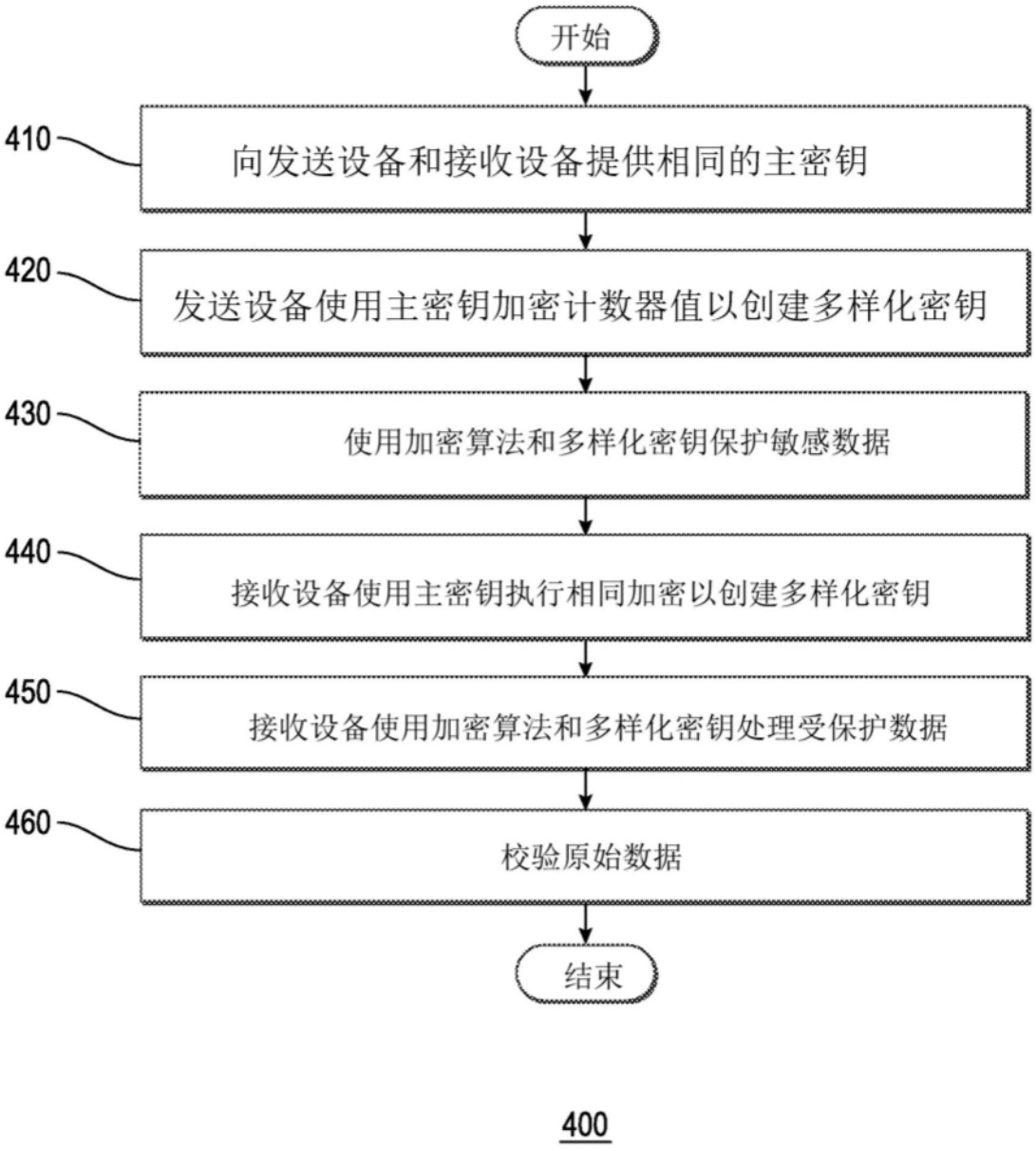

开始
410
向发送设备和接收设备提供相同的主密钥
420
发送设备使用主密钥加密计数器值以创建多样化密钥
430
使用加密算法和多样化密钥保护敏感数据
440
接收设备使用主密钥执行相同加密以创建多样化密钥
450
接收设备使用加密算法和多样化密钥处理受保护数据
460
校验原始数据
结束
400

图4

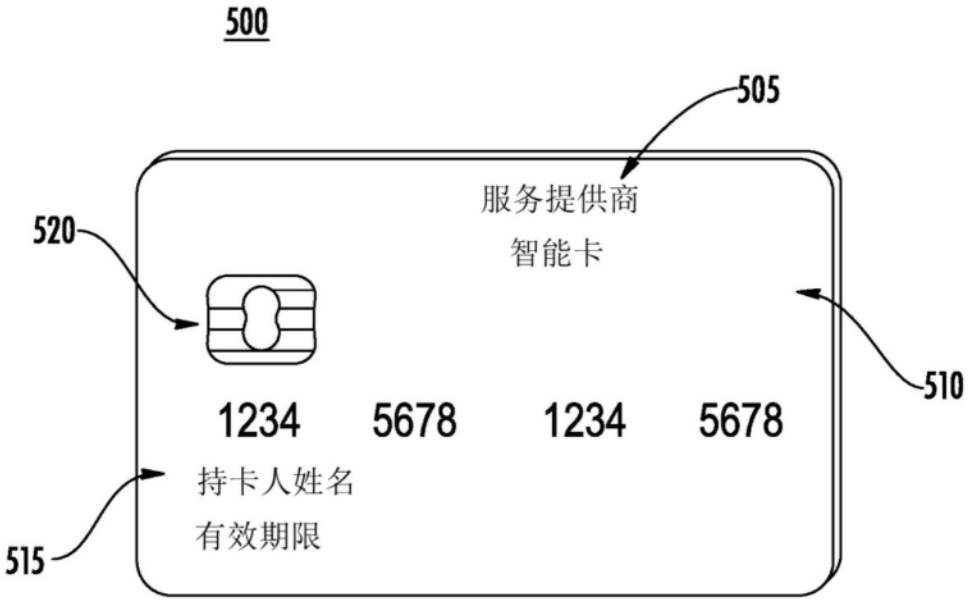


图5A

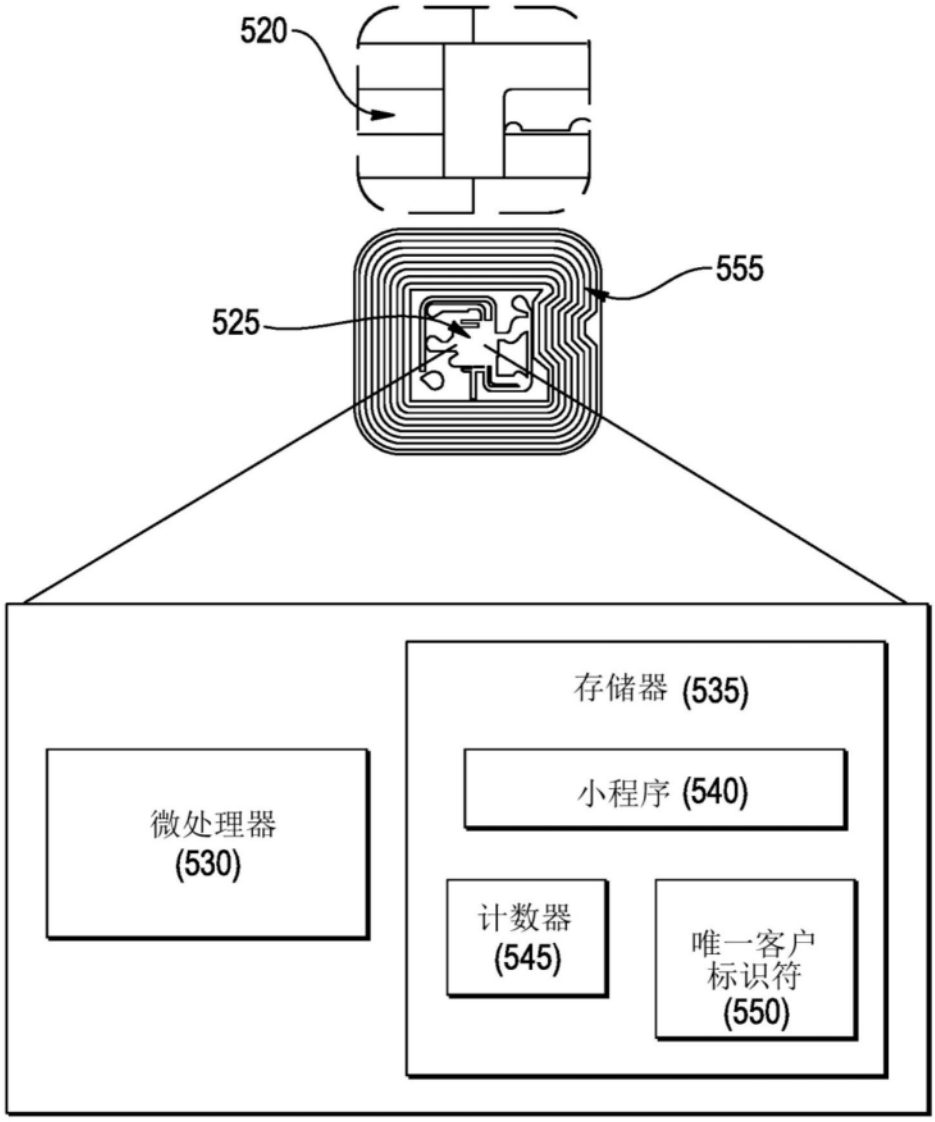


图5B

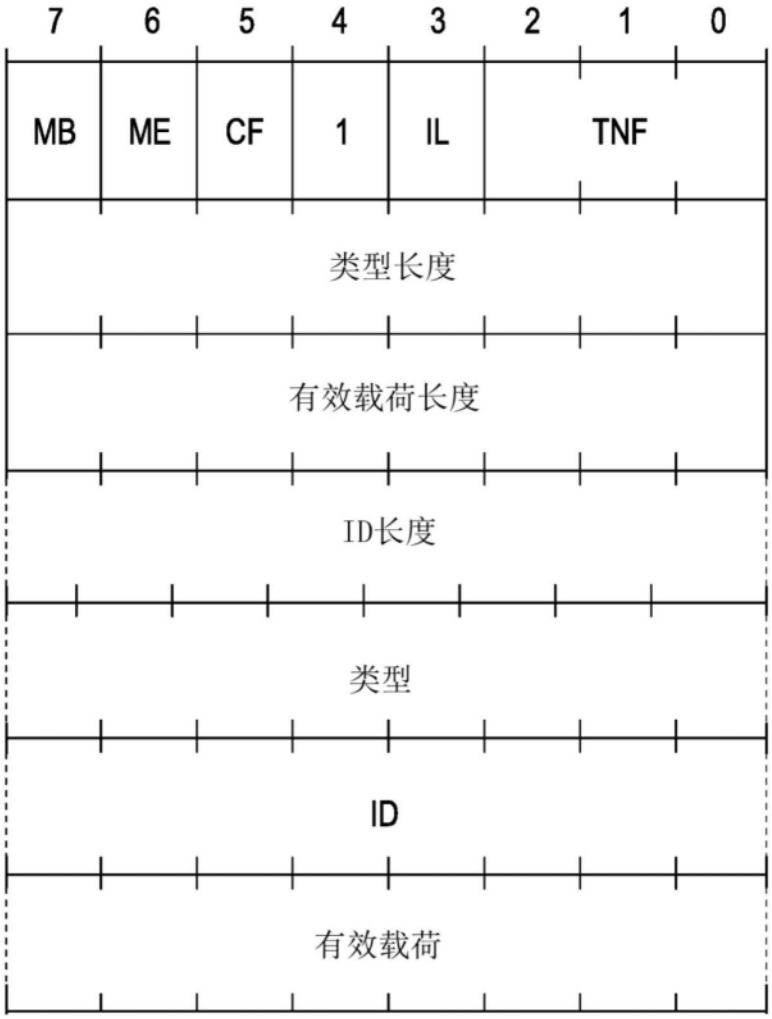


图6

00 D1 (消息开始 , 消息结束 , 短记录 无ID长度) 01 (已知类型) 01 01 文本类型
02 <有效负载长度包括记录ID和“EN”或内容长度+3) = 45+3 = 48 (DEC)
03 54 ('T')
04 02 记录ID
05 65 6E (语言长度 , 'en')
07 43 01 00 76 a6 62 7b 67 a8 cf bb < 八个mac字节 >
D101305402656E 43010076A6627B67A8CFBB < 八个mac字节 >

710

版本	pUID (8)	pATC	加密算法 (16)	
0100	0015399555360061	00000050	7D28B8B9D8666E5143153AC9C944E5A6	
解密算法				
随机数 (8)	MAC (8)			
4838FB7DC171B89E	CF3F3B8C56DA0BF1			
	MAC(T=[p 版本 (2 字节) || pUID (8 字节) || pATC (4 字节) || pSHSEC (4 字节) || '80' || '00 00 00 00 00'])			

720

图7

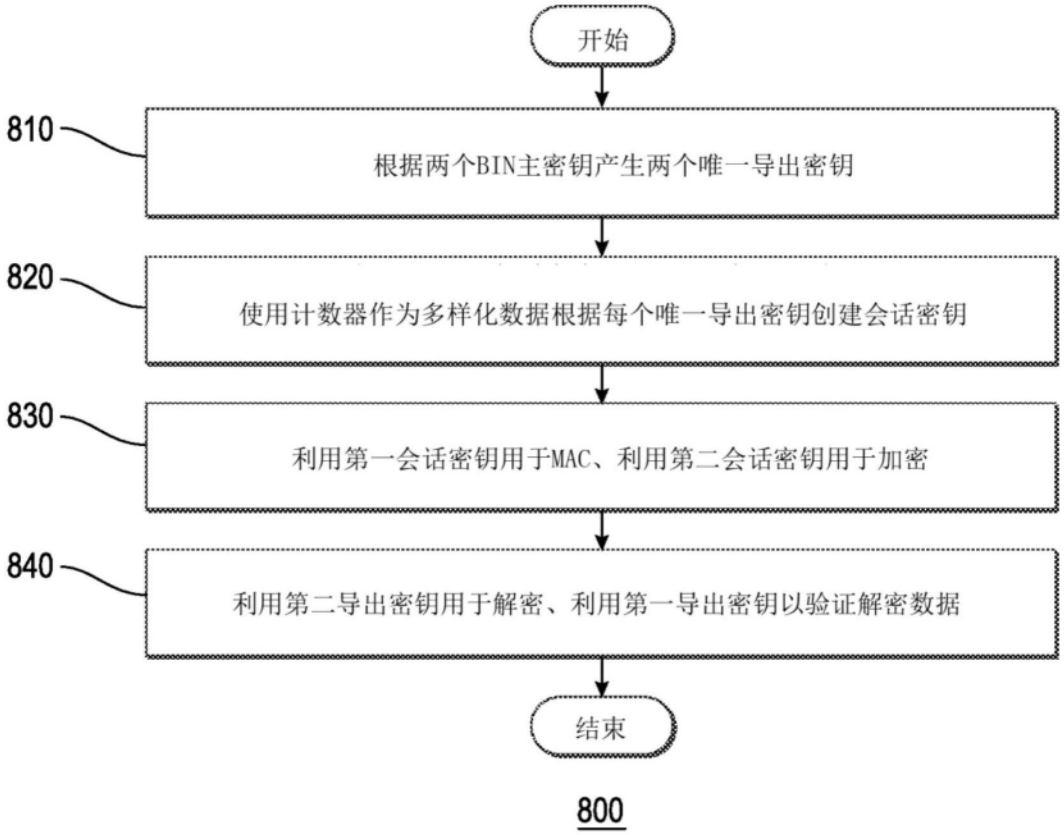

开始
810
根据两个BIN主密钥产生两个唯一导出密钥
820
使用计数器作为多样化数据根据每个唯一导出密钥创建会话密钥
830
利用第一会话密钥用于MAC、利用第二会话密钥用于加密
840
利用第二导出密钥用于解密、利用第一导出密钥以验证解密数据
结束
800

图8

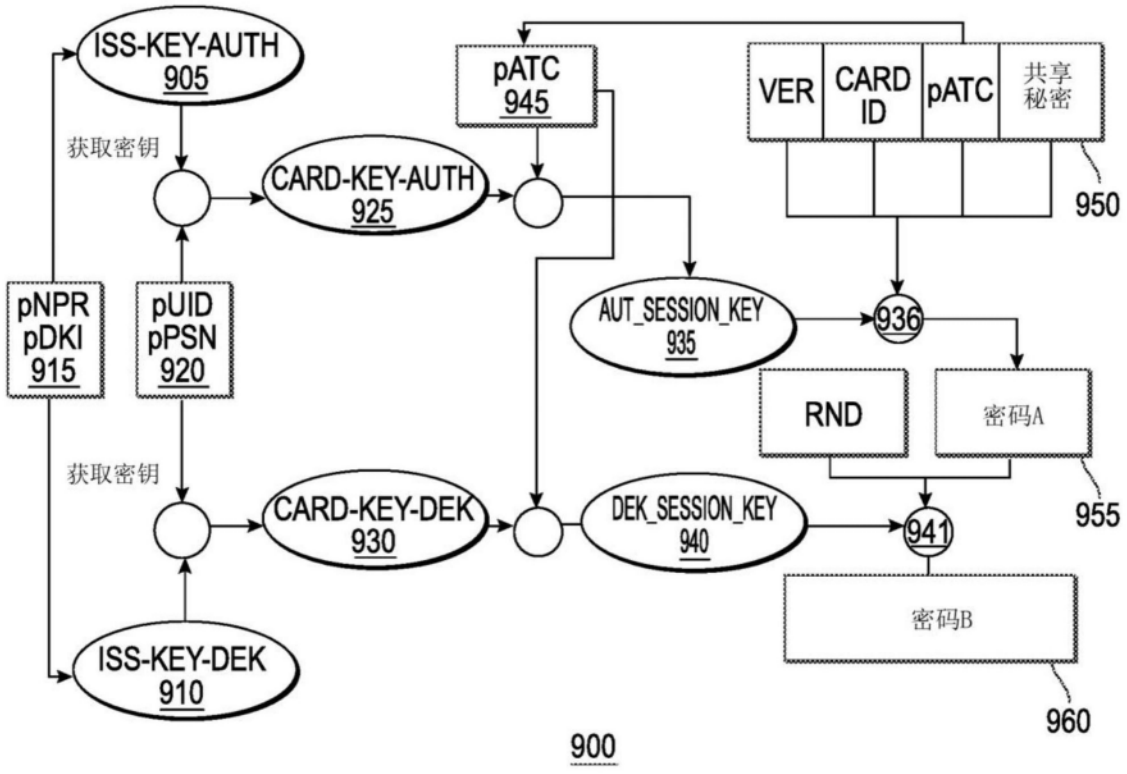

ISS-KEY-AUTH
905
获取密钥
CARD-KEY-AUTH
925
pATC
945
VER
CARD ID
pATC
共享秘密
950
pNPR
pDKI
915
pUID
pPSN
920
AUT_SESSION_KEY
935
936
RND
密码A
955
获取密钥
CARD-KEY-DEK
930
DEK_SESSION_KEY
940
941
密码B
960
ISS-KEY-DEK
910
900

图9

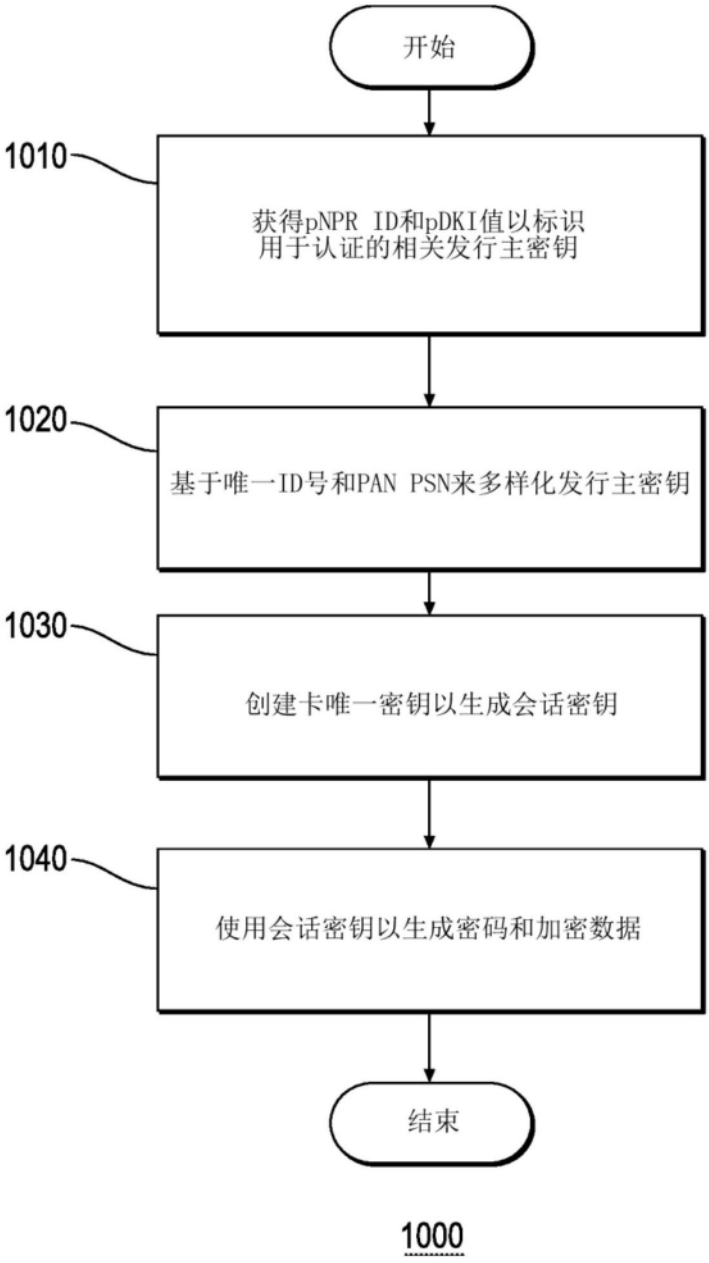

开始
1010
获得pNPR ID和pDKI值以标识
用于认证的相关发行主密钥
1020
基于唯一ID号和PAN PSN来多样化发行主密钥
1030
创建卡唯一密钥以生成会话密钥
1040
使用会话密钥以生成密码和加密数据
结束
1000

图10

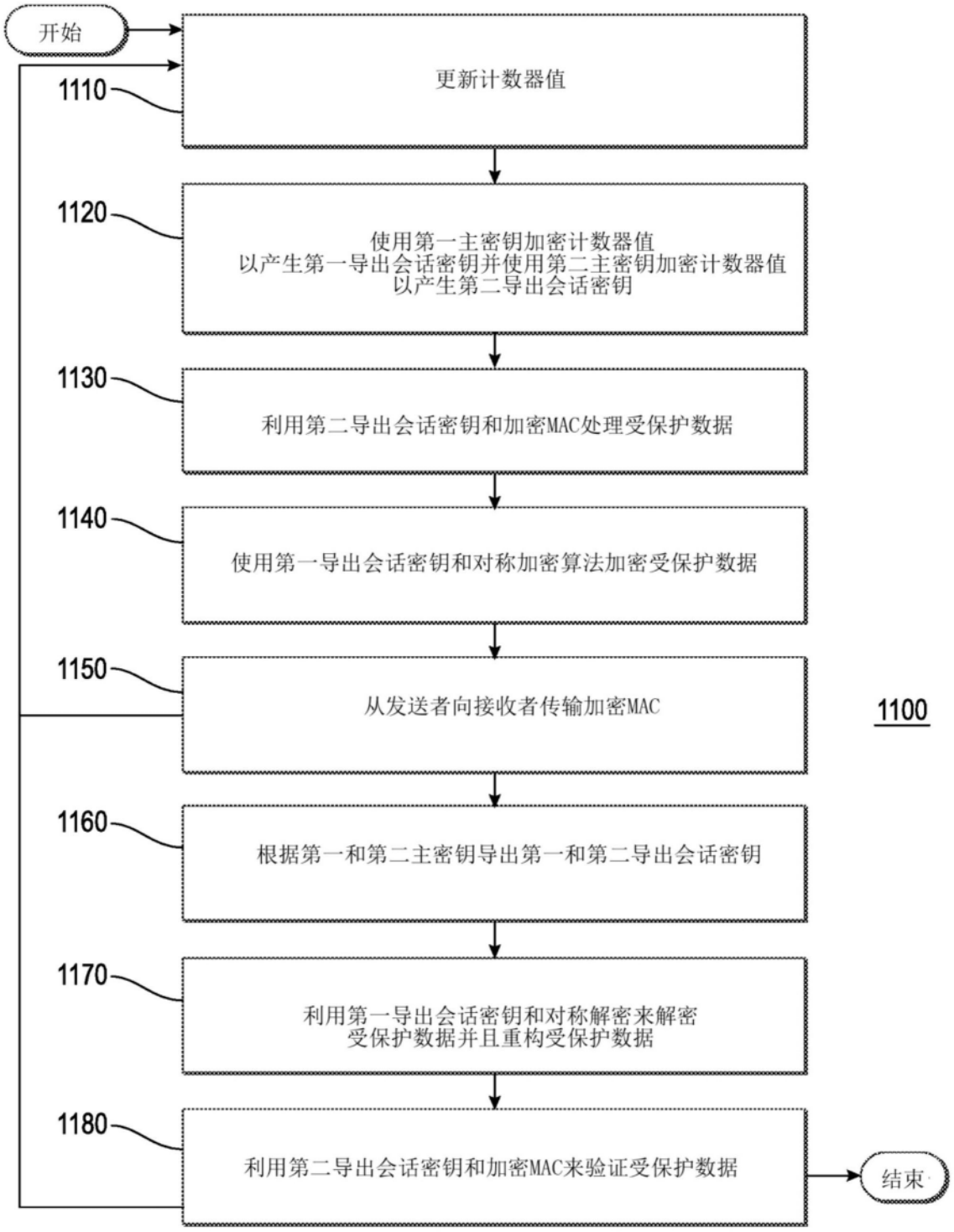

开始
1110
更新计数器值
1120
使用第一主密钥加密计数器值
以产生第一导出会话密钥并使用第二主密钥加密计数器值
以产生第二导出会话密钥
1130
利用第二导出会话密钥和加密MAC处理受保护数据
1140
使用第一导出会话密钥和对称加密算法加密受保护数据
1150
从发送者向接收者传输加密MAC
1100
1160
根据第一和第二主密钥导出第一和第二导出会话密钥
1170
利用第一导出会话密钥和对称解密来解密
受保护数据并且重构受保护数据
1180
利用第二导出会话密钥和加密MAC来验证受保护数据
结束

图11

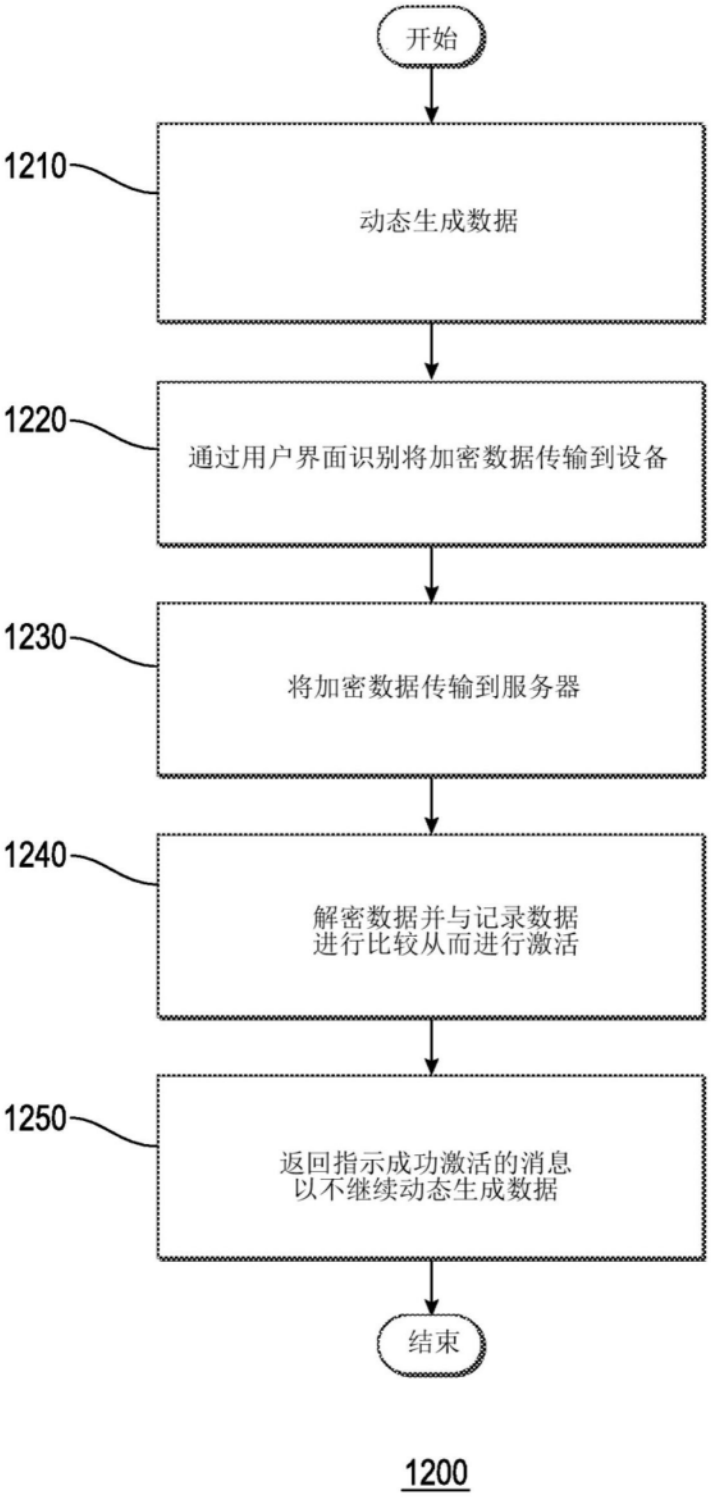
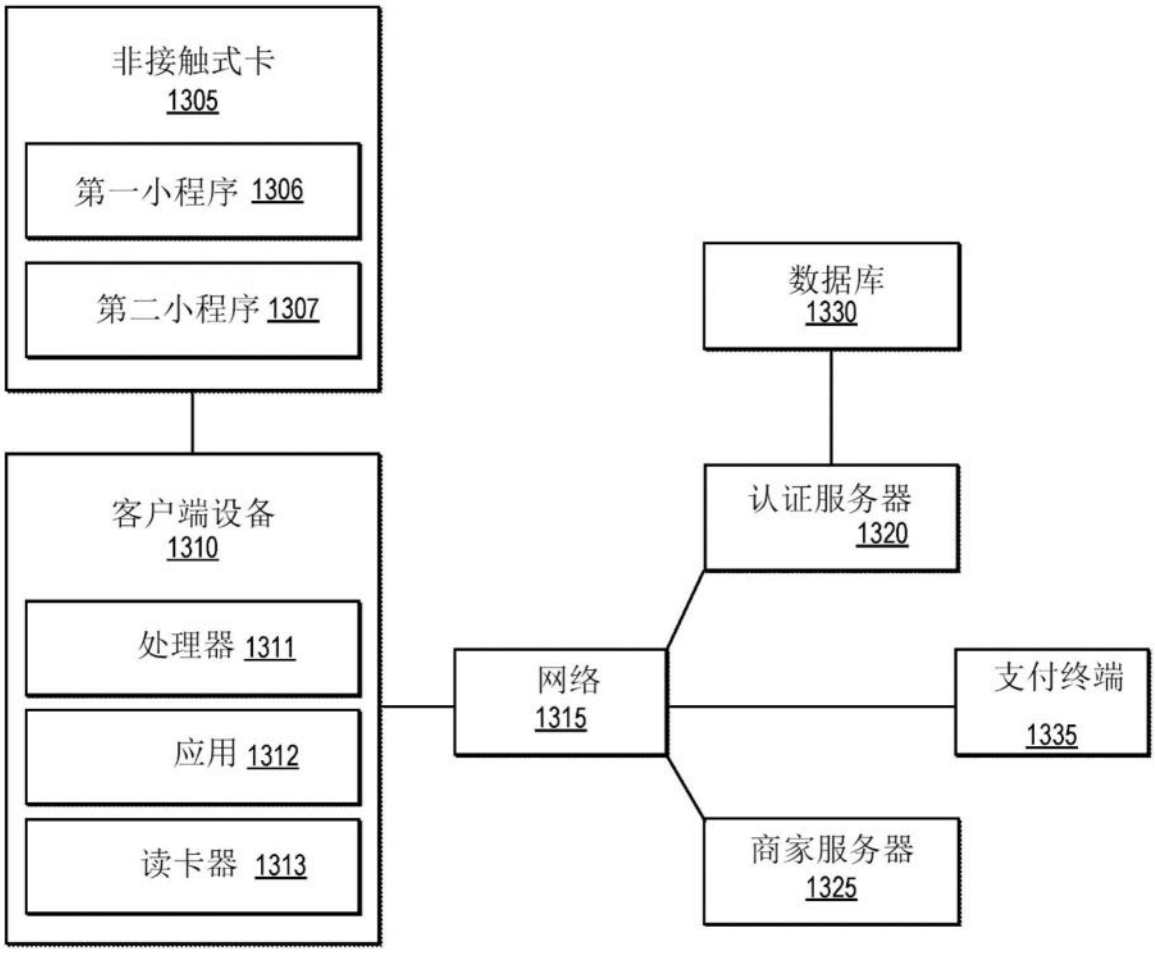

开始
1210
动态生成数据
1220
通过用户界面识别将加密数据传输到设备
1230
将加密数据传输到服务器
1240
解密数据并与记录数据
进行比较从而进行激活
1250
返回指示成功激活的消息
以不继续动态生成数据
结束
1200

图12


非接触式卡
1305
第一小程序 1306
第二小程序 1307
客户端设备
1310
处理器 1311
应用 1312
读卡器 1313
网络
1315
数据库
1330
认证服务器
1320
支付终端
1335
商家服务器
1325

1300

图13

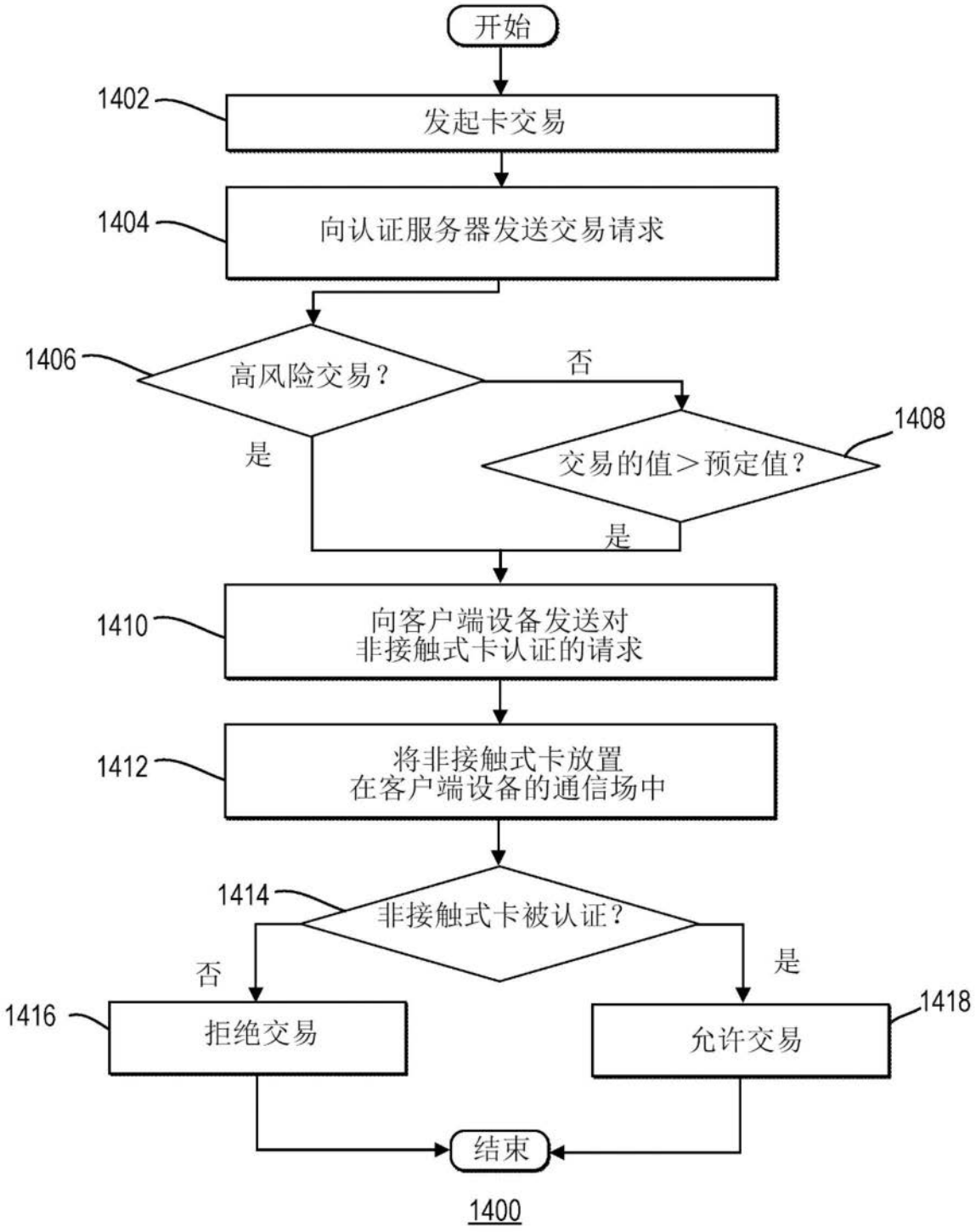

开始
1402
发起卡交易
1404
向认证服务器发送交易请求
1406
高风险交易？
否
1408
交易的值＞预定值？
是
是
1410
向客户端设备发送对
非接触式卡认证的请求
1412
将非接触式卡放置
在客户端设备的通信场中
1414
非接触式卡被认证？
否
是
1416
拒绝交易
1418
允许交易
结束
1400

图14