(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114868144 A
(43)申请公布日 2022.08.05

(21)申请号 202080089471.8

(22)申请日 2020.11.24

(30)优先权数据
16/727,294 2019.12.26 US

(85)PCT国际申请进入国家阶段日
2022.06.22

(86)PCT国际申请的申请数据
PCT/US2020/061972 2020.11.24

(87)PCT国际申请的公布数据
WO2021/133503 EN 2021.07.01

(71)申请人 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
斯里尼瓦沙·希古鲁帕蒂
杰弗里·鲁尔

(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 王天鹏

(51)Int.Cl.
G06Q 30/02(2006.01)

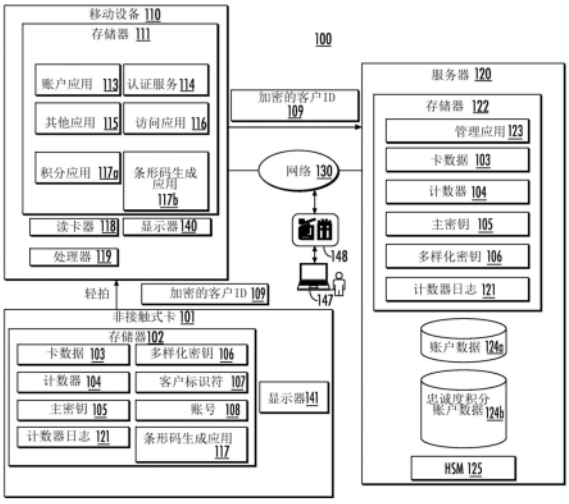
权利要求书2页 说明书21页 附图7页

(54)发明名称

访问和利用多个忠诚度积分账户

(57)摘要

各种实施例通常涉及利用离线和/或在线验证或认证协议来访问、兑换或以其他方式利用多个忠诚度积分和忠诚度账户。一种利用各种忠诚度积分的方法，包括：确定用户正在请求访问忠诚度积分账户数据库；接收基于密码算法和多样化密钥生成的加密数据；接收对用户的验证，该验证包括对包括了加密数据的数据组合进行验证，其中与发行者相关联的服务器可以基于密码算法和多样化密钥来解密数据组合；响应于接收到对用户的验证，访问与用户的忠诚度积分账户相关联的数据库，并授权兑换与忠诚度积分账户相关联的多个忠诚度积分。



CN 114868144 A

1.一种装置,包括:

处理器电路;以及

存储器,其存储了指令,所述指令在由所述处理器电路执行时致使所述处理器电路执行以下操作:

由在所述处理器电路上执行的应用发起用以执行与同多个忠诚度积分相关联的多个账户有关的至少一个操作的请求;

由所述应用从非接触式卡的通信接口接收加密数据,其中所述加密数据基于密码算法和多样化密钥,所述多样化密钥基于主密钥和计数器值;

由所述应用并从服务器接收指定所述服务器基于所述密码算法和所述多样化密钥验证了所述加密数据的指示;并且

响应于接收到所述验证的指示,授予执行所述至少一个操作的授权,其中所述至少一个操作包括以下至少一项:i)访问包含与至少一个用户和至少两个不同账户相关联的多个忠诚度标识符的数据库,每个账户与不同的忠诚度积分集合相关联,以及ii)在所述数据库中相关于所述至少两个不同账户存储多个忠诚度标识符中的至少一个。

2.根据权利要求1所述的装置,其中,所述存储器存储指令,其在由所述处理器电路执行时致使所述处理器电路执行以下操作:

选择所述至少两个账户之一;并且

相关于与所选账户相关联的不同忠诚度积分集合执行至少一个操作。

3.根据权利要求2所述的装置,其中,所述至少一个操作是兑换操作。

4.根据权利要求3所述的装置,其中,从所述非接触式卡接收到的加密数据基于所述非接触式卡对计算设备的第一次轻拍。

5.根据权利要求4所述的装置,其中,对所述加密数据的验证与密码相关联,所述密码与同多个账户中的至少一个相关联的至少一个用户标识组合。

6.根据权利要求5所述的装置,其中,所述组合基于逻辑操作。

7.根据权利要求6所述的装置,其中,所述逻辑操作包括异或操作。

8.一种方法,包括:

由在处理器电路上执行的应用确定用户正在请求访问忠诚度积分账户数据库;

由所述应用从与账户相关联的非接触式卡的通信接口接收加密数据,其中所述加密数据基于密码算法和多样化密钥而生成,所述多样化密钥存储在所述非接触式卡的存储器中并基于存储在所述非接触式卡的存储器中的计数器值和主密钥而生成;

由所述应用并从服务器接收对所述用户的验证,所述验证包括对包括了所述加密数据的数据组合进行验证,所述服务器基于存储在所述服务器的存储器中的多样化密钥和所述密码算法来解密所述数据组合以验证所述数据组合,其中存储在所述服务器的存储器中的多样化密钥基于存储在所述服务器的存储器中的计数器值和主密钥而生成;并且

响应于接收到对用户的验证,授权访问所述用户在所述数据库中的忠诚度积分账户,并授权兑换与所述忠诚度积分账户相关联的多个忠诚度积分。

9.根据权利要求8所述的方法,所述方法还包括:

由所述应用并从与所述处理电路相关联的计算机设备向所述服务器发送第一应用用户凭证;并且

在所述解密之前，在所述服务器处将所述第一应用用户凭证与由所述服务器存储的第二应用用户凭证进行比较。

10.根据权利要求9所述的方法，所述方法还包括：

在所述解密之前，并且响应于发现所述第一应用用户凭证和所述第二应用用户凭证之间的匹配，将与所述用户相关联的忠诚度标识符与所述加密数据组合，并且其中所述数据组合包括所述忠诚度标识符和所述加密数据的组合。

11.根据权利要求10所述的方法，其中将与所述用户相关联的忠诚度标识符与所述加密数据组合包括：

在所述服务器处对接收到的加密数据和所述忠诚度标识符执行操作。

12.根据权利要求11所述的方法，其中，所述忠诚度标识符存储在所述服务器上。

13.根据权利要求11所述的方法，其中，所述操作是异或操作。

14.根据权利要求10所述的方法，所述方法还包括：

在i)所述非接触式卡和ii)所述计算机设备中的任一个处生成条形码，其中所生成的条形码基于从所述服务器接收到的令牌。

15.根据权利要求14所述的方法，其中，所述令牌基于所述加密数据和所述忠诚度标识符的组合。

16.根据权利要求15所述的方法，所述方法还包括：

显示所生成的条形码；并且

使用扫描设备扫描所生成的条形码。

17.根据权利要求16所述的方法，所述方法还包括：

响应于对所生成的条形码的扫描，执行所述数据组合的解密。

18.一种非暂时性计算机可读存储介质，其存储了计算机可读程序代码，所述计算机可读程序代码能由处理器电路执行以致使处理器电路执行以下操作：

发起用以执行与同多个忠诚度积分相关联的多个账户有关的至少一个操作的请求；

从非接触式卡接收加密数据，其中所述加密数据基于密码算法和多样化密钥，所述多样化密钥基于主密钥和计数器值；

从服务器接收所述服务器基于所述密码算法和所述多样化密钥验证了所述加密数据的指示；并且

响应于接收到所述验证，授予执行所述至少一个操作的授权，其中所述至少一个操作包括以下至少一项：i)访问包含与至少一个用户和至少两个不同账户相关联的多个忠诚度标识符的数据库，每个账户与不同的忠诚度积分集合相关联，以及ii)在所述数据库中相关于所述至少两个不同账户存储多个忠诚度标识符中的至少一个。

19.根据权利要求18所述的计算机可读存储介质，还包括计算机可读程序代码，所述计算机可读程序代码能由所述处理器电路执行以致使所述处理器电路执行以下操作：

从所述服务器接收令牌。

20.根据权利要求19所述的计算机可读存储介质，还包括计算机可读程序代码，所述计算机可读程序代码能由所述处理器电路执行以致使所述处理器电路执行以下操作：

基于从所述服务器接收到的令牌生成条形码。

访问和利用多个忠诚度积分账户

[0001] 相关申请的交叉引用

[0002] 本申请要求2019年12月26日提交的题为“ACCESSING AND UTILIZING MULTIPLE LOYALTY POINT ACCOUNTS”的美国专利申请序列号16/727,294的优先权。上述专利申请的内容通过引用整体并入本文。

技术领域

[0003] 本文中的实施例总体上涉及计算平台,并且更具体地,涉及利用各种授权协议访问多个忠诚度账户。

背景技术

[0004] 激活许多卡、并且更具体地金融卡(例如,信用卡)涉及持卡人拨打电话号码或访问网站并输入或以其他方式提供卡信息的耗时过程。此外,虽然越来越多地使用基于芯片的金融卡为亲自购买提供了比以前的技术(例如磁条卡)更安全的特征,但账户访问典型地仍然依赖于登录凭证(例如用户名和密码)来确认持卡人的身份和/或以其他方式完成交易。但是,如果登录凭证被泄露,则另一个人可能访问该用户的账户。

[0005] 当尝试有效地访问多个账户时,账户安全问题变得更加严重,这是因为如果单个授权凭证或机制受到损害,则无论账户访问与支付、兑换活动还是一般访问有关,它都可能造成严重的安全风险。

[0006] 因此,需要改进用于账户访问和交易竞争的认证机制,包括支付和兑换交易。

发明内容

[0007] 本文公开的实施例提供了用于利用隐写方法编码的图像(steganographically encoded image)来验证用户和/或完成交易(包括但不限于支付交易)的系统、方法、制品和计算机可读介质。根据一个或多个示例,在线协议用于验证和/或认证用户,以便发起信息交换,该信息交换提供了对与忠诚度积分相关联的一个或多个账户的访问(或以其他方式使用该一个或多个账户)。

[0008] 根据一个示例,利用在计算机系统上执行的应用的计算机实施的方法可以发起事务以通过利用隐写方法编码的图像来验证用户的身份和/或授权交易。(在各种实施例中,可以通过轻拍用户设备(例如移动设备)上的非接触式卡来发起应用)。该方法可以包括:由在处理器电路上执行的应用确定用户正在请求访问忠诚度积分账户数据库;所述应用从与账户相关联的非接触式卡的通信接口接收加密数据,其中所述加密数据基于密码算法和多样化密钥而生成,所述多样化密钥存储在所述非接触式卡的存储器中并基于存储在所述非接触式卡的存储器中的计数器值和主密钥而生成;由所述应用并从服务器接收对所述用户的验证,所述验证包括对包括了所述加密数据的数据组合进行验证,所述服务器基于存储在所述服务器的存储器中的多样化密钥和所述密码算法来解密所述数据组合以验证所述数据组合,其中存储在所述服务器的存储器中的多样化密钥基于存储在所述服务器的存储

器中的计数器值和主密钥而生成;并且响应于接收到对所述用户的验证,访问与用户的忠诚度积分账户相关联的数据库,并授权兑换(redemption)与所述忠诚度积分账户相关联的多个忠诚度积分。

[0009] 根据另一示例,系统采用在线和/或离线认证以及隐写方法编码的图像来认证和/或验证用户和/或授权交易。该系统可以包括:处理器电路,以及存储了指令的存储器,所述指令在由处理器电路执行时致使处理器电路执行以下操作:由在处理器电路上执行的应用发起请求以执行与同多个忠诚度积分相关联的多个账户有关的至少一个操作;由应用从与账户相关联的非接触式卡的通信接口接收加密数据,其中该加密数据基于密码算法和多样化密钥而生成,该多样化密钥存储在非接触式卡的存储器中并且基于存储在非接触式卡的存储器中的计数器值和主密钥而生成;由应用并从服务器接收对加密数据的验证,该服务器基于存储在服务器的存储器中的多样化密钥和密码算法来对加密数据进行解密以验证加密数据,存储在服务器的存储器中的多样化密钥基于存储在服务器的存储器中的计数器值和主密钥而生成,并且响应于接收到所述验证,授予执行所述至少一个操作的授权,其中所述至少一个操作包括以下至少一项:i)访问包含与至少一个用户和至少两个不同账户相关联的多个忠诚度标识符的数据库,每个账户与不同的忠诚度积分集合相关联,以及ii)在所述数据库中相关于所述至少两个不同账户存储多个忠诚度标识符中的至少一个。

[0010] 根据又一示例,一种与同用户相关联的卡的发行者相关联的主机系统,该主机系统包括非暂时性计算机可读存储介质,其存储了可由处理器执行以执行以下操作的计算机可读程序代码:生成数据组合,该数据组合包括i)与多个忠诚度账户相关联的至少一个用户账户的忠诚度标识符、以及ii)基于密码算法和多样化密钥生成的加密数据;并且基于存储在服务器的存储器中的多样化密钥和密码算法来对加密数据进行解密以验证加密数据,存储在服务器的存储器中的多样化密钥基于存储在服务器的存储器中的计数器值和主密钥而生成。

附图说明

[0011] 图1示出了用于根据支付协议验证或认证用户的系统的实施例。

[0012] 图2示出了轻拍以利用授权协议验证用户的至少一个实施例。

[0013] 图3示出了基于图2的轻拍和验证生成条形码的至少一个实施例。

[0014] 图4A-图4B示出了示例非接触式卡。

[0015] 图5示出了第一逻辑流程的实施例。

[0016] 图6示出了第二逻辑流程的实施例。

[0017] 图7示出了计算架构的实施例。

具体实施方式

[0018] 本公开的方面包括用于提供经认证的持卡人访问的系统、方法和/或技术。通常,各种实施例涉及通过利用和生成利用在线认证协议的条形码来访问或以其他方式利用一个或多个忠诚度积分账户,其中该条形码可用于完成一个或多个交易,包括支付交易。在各种实施例中,条形码是根据在线认证协议生成的,但是为了进一步增强安全性,它仅对单次交易有效,并且此后过期以防止与单次交易相关联的应用的不当使用。与所公开的实施例

一致，系统和方法可以利用一个或多个计算设备、处理器、网络服务器、账户服务器和/或非接触式设备(例如，射频识别(RFID)卡)。

[0019] 本公开的各种实施例在验证用户和完成交易(诸如支付交易)方面提供了一个或多个益处，包括利用由动态认证技术(例如，在线技术)提供的增强的安全性，同时还利用条形码完成交易(其提供了方便和额外安全性两者)。在各种实施例中，利用在线技术增强了计算机设备(例如移动电话)的效率，这通过提供单个方法来跨一个或多个应用对用户进行认证或验证，即使一个或多个应用在其用途上是不同的(例如运输应用关于娱乐应用)也是如此。因此，在各种实施例中，授权协议可用于跨不同应用和目的有效地且更安全地认证用户，并且然后利用作为验证结果而生成的条形码来完成与不同应用中的一个或多个应用相关联的交易，包括可能涉及或不涉及进行支付的交易和操作。

[0020] 图1描绘了与所公开的一致的示例性系统100的示意图。如示出的，系统100包括一个或多个非接触式卡101、一个或多个移动设备110和服务器120。非接触式卡101表示任何类型的支付卡，诸如信用卡、借记卡、ATM卡、忠诚度账户卡、礼品卡和诸如此类。在各种实施例中，非接触式卡101或卡101是虚拟支付卡。非接触式卡101可以包括一个或多个芯片(未描绘)，诸如射频识别(RFID)芯片，其被配置为经由NFC、EMV标准或无线通信中的其他短程协议与移动设备110通信。尽管NFC被用作示例通信协议，但是本公开同样适用于其他类型的无线通信，诸如根据EMV标准、蓝牙和/或Wi-Fi的其他合适的通信协议。移动设备110表示任何类型的网络使能的计算设备，诸如智能电话、平板计算机、可穿戴设备、手提电脑、便携式游戏设备和诸如此类。服务器120表示任何类型的计算设备，诸如服务器、工作站、计算机集群、云计算平台、虚拟化计算系统和诸如此类。

[0021] 如示出的，非接触式卡的存储器102包括卡数据103、计数器104、主密钥105、多样化密钥106、唯一客户标识符107和账号108的数据存储。卡数据103一般包括账户相关信息，诸如用于使用非接触式卡101处理支付的信息。例如，卡数据103可以包括账号、有效期、账单地址和卡验证值(CVV)。账号可以是任何类型的账号，诸如主账号(PAN)、虚拟账号和/或基于PAN生成的令牌。其他类型的账号也被考虑，并且账号或其他类型的卡数据103的使用不应被认为是对本公开的限制。卡数据103还可以包括姓名、账单地址、送货地址和其他账户相关信息。账号108存储一次性使用(one-time-use)的虚拟账号以及相关联的有效期和CVV值。例如，账号108可以包括数千个单次使用的虚拟账号、有效期和CVV值。

[0022] 如示出的一个或多个操作和/或执行与处理器活动相关联的任何其他合适的操作，包括比较操作和执行与存储器111相关联的指令。示例操作系统112包括Android® OS、iOS®、Linux®和Windows®操作系统。如所示出的，OS 112包括一个或多个应用，包括账户应用113、认证或验证应用或服务114(为方便起见下文称为“认证应用”)、一个或多个其他应用115和/或一个或多个访问应用116。账户应用113允许用户执行各种账户相关操作，诸如查看账户余额、购买物品和处理支付。最初，用户可以使用认证凭证进行认证来访问账户应用113。例如，认证凭证可以包括用户名和密码、生物特征凭证和诸如此类。

[0023] 认证应用114通常被配置为确定用户何时需要对交易、服务或可访问性请求进行认证，包括用于完成与应用相关联的支付。例如，认证应用114可以确定用户需要访问特定应用和/或完成与其相关联的交易或支付，诸如访问应用116。访问应用116可以是或可以包括被配置为授予对与用户账户相关联的特定服务的一个或多个特征的访问权限的应用，诸

如运输服务(例如公共交通)、银行账户、健康保险账户、包含账户余额、经纪信息或任何其他合适的金融数据的金融账户或金融应用、服务应用(零售服务、递送服务、娱乐服务、游戏服务等)、以及可能需要用户认证的任何其他合适的应用。在各种实施例中,访问应用116可以与支付特征相关联,例如用于进行支付或接收支付的信用账户或银行账户,和/或认证交易可能仍涉及用于认证或验证的非支付特征,例如信用卡或借记卡激活。在各种实施例中,访问应用116是零售或商品/服务供应应用,并且与访问应用116相关联的一个或多个特征涉及完成与关于访问应用116提供的商品或服务相关联的支付,其中,如下面讨论的,与其相关联的交易或支付可以通过扫描根据在线授权协议生成的条形码来完成。在各种实施例中,认证应用114可以利用单独的API接口促进认证协议并调用对访问应用116的访问。认证应用114可以被配置为通过利用任何合适的协议来验证用户,包括利用加密技术、EMV标准或符合EMV标准的认证协议的任何验证过程中的一个或多个。在各种实施例中,认证应用114被配置为同步与非接触式卡101相关联的计数器104以及与在用户认证发生时可以与同非接触式卡101和移动设备通信的发行者相关联的服务器120。

[0024] 在各种实施例中,认证应用114可以与服务器120和/或非接触式卡101协调以记录与计数器104相关的非支付交易的授权作为日志。日志可以是位于服务器120的存储器122或非接触式卡101的存储器102中的计数器日志121。日志可以保持交易作为支付交易和非支付交易的单独交易记录,而不论服务器120或非接触式卡101以及计数器104的总记录。与非接触式卡通信的服务器120和/或认证应用114可以利用其中包含的信息用于反欺诈措施。例如,如果非支付交易的阈值数量在非支付交易和支付交易之间太小(或太大),则认证应用114和/或服务器120可以拒绝支付交易,或者反之亦然。在各种实施例中,包含非支付和支付交易之间的区别信息(例如计数)的计数器日志121可以在在线验证协议期间用于任何其他合适的目的。

[0025] 在各种实施例中,认证应用114与账户应用113相关联。例如,认证应用114可以与账户应用113一起安装在移动设备110上,并且在安装之后提示用户启用认证应用114。更一般地,每次打开账户应用113时,账户应用113可确定是否启用认证应用114作为OS 112的默认认证应用。如果未启用认证应用114作为默认认证应用,则账户应用113可以提示用户启用认证应用114作为OS 112的默认认证应用和/或启用认证应用114的一个或多个功能。一旦启用作为OS 112的默认认证应用,认证应用114就可以以编程方式识别授权应用何时需要认证并且可以利用支付协议来启用验证,即使支付不与验证或授权相关联也是如此。在各种实施例中,为了发起认证或验证协议(例如,与在线验证技术或协议相关联的至少一个操作),认证应用114可以提示用户将非接触式卡101轻拍到移动设备110以发起认证应用114或与其相关联的一个或多个操作。

[0026] 通常,在本文描述的各种实施例中,在线验证或认证协议可以包括以下操作中的一个或多个:通过提示用户将非接触式卡101轻拍在计算机设备(例如,移动设备110)上,认证应用可以发起事务以验证用户的身份,其中认证应用可以全部或部分发起应用,例如访问应用116;和/或生成可以被扫描以访问应用116的特征和/或完成与其相关联的交易的条形码。交易可以涉及读卡器118和非接触式卡101之间的NFC通信,其中非接触式卡101可以向移动设备110提供一个或多个输入,包括最新版本的应用交易计数器(ATC),并且非接触式卡101或移动设备110(包括与其相关联的任何合适的组件)可以基于多个输入生成合适

的密码，并且然后非接触式卡101或移动设备110(包括与其相关联的任何合适的组件)可以将密码和ATC发送到非接触式卡101的发行者(例如，与发行者相关联的服务器120)。然后可以通过从发行者接收验证或授权用户的响应来验证用户并接收对与应用116相关联的一个或多个特征的访问，其中接收到的响应基于发行者(例如服务器120)响应于接收到密码而执行的至少一个密码操作。例如，如果服务器120能够解密密码，则服务器可以向移动设备110发送指定密码已经被验证的指示。

[0027] 在各种实施例中，一旦用户被验证，服务器120就可以将认证令牌(使用任何合适的令牌生成技术)发送到与移动设备110和非接触式卡101相关联的条形码生成应用117b，其中条形码生成应用117b可以致使移动设备110和/或非接触式卡101的显示器140、141显示可由任何合适的扫描设备扫描的条形码。认证令牌可以被配置为授予对访问应用116的一个或多个特征的访问权限，包括完成与访问应用116相关联的支付交易，并且在各种实施例中，为了增强与交易相关联的安全性，服务器120可以将认证令牌配置为授权与访问应用116相关联的单个交易，并且此后在不发生另一验证(在线或离线)的情况下禁用令牌/条形码授权与访问应用116相关的另一操作。

[0028] 在非接触式卡101是虚拟支付卡的各种实施例中，认证应用114可以通过访问在移动设备110上实施的数字钱包来检索与非接触式卡101相关联的信息，其中数字钱包包括虚拟支付卡。

[0029] 如示出的，服务器120还包括账户数据124a的数据存储和存储器122。账户数据124a包括多个用户和/或账户的账户相关数据。账户数据124a可以至少包括主密钥105、计数器104诸如应用交易计数器(“ATC”)104、客户ID 107、相关联的非接触式卡101、账户持有人姓名、账户账单地址、一个或多个送货地址、一个或多个虚拟卡号和用于每个账户的生物信息。存储器122包括管理应用123和来自账户数据124a的一个或多个账户的卡数据103、计数器104、主密钥105和多样化密钥106的实例。该系统还可以包括一个或多个忠诚度账户124b。

[0030] 系统100被配置为实施密钥多样化以保护数据，这在本文中可以被称为密钥多样化技术。系统100可以实施在线认证协议。

[0031] 在各种实施例中，认证应用114从用户接收与用户简档相关联的第一应用用户凭证。第一应用用户凭证可以包括生物特征数据、与用户识别相关联的已建立手势、用户名和密码组合和/或诸如此类。处理器119将第一应用用户凭证与存储的第二应用用户凭证进行比较。存储的第二应用用户凭证可以与用户身份相关联，并且它可以存储在移动设备110的存储器111或服务器120的存储器122中。在各种实施例中，存储的第二应用用户凭证在服务器120上维护并且第一匹配由服务器120执行。在各种实施例中，在确定出第一应用用户凭证和存储的第二应用用户凭证之间的第一匹配时，认证应用114可以授予用户对与访问应用116相关联的用户账户的一个或多个第一级用户账户选项的访问权限。用户账户可以是金融账户、健康保险账户和/或与任何服务提供商相关联的任何其他类似账户(例如，中转账户、娱乐账户等)。一旦确定出第一匹配，用户就可以访问与访问应用116相关联的某些第一级用户账户选项，而不会发生条形码的生成并且不会发生交易的完成，例如支付的完成。用户账户的第一级用户账户选项可以包括账户余额的显示、最近交易的显示和/或诸如此类。为了更好地访问和/或执行某些账户功能，即第二级用户账户选项，诸如执行支付交易，

可能需要第二级认证，诸如完全完成在线认证协议、响应于协议的成功完成而生成认证令牌、以及生成用于扫描的条形码(利用认证令牌)，其中扫描完成了与访问应用116相关联的交易，例如支付。

[0032] 通常，服务器120(或另一计算设备)和非接触式卡101可以配备有相同的主密钥105(也称为主对称密钥)。更具体地，每个非接触式卡101被编程有在服务器120中具有对应配对的不同主密钥105。例如，当制造非接触式卡101时，唯一的主密钥105可以被编程到非接触式卡101的存储器102中。类似地，唯一主密钥105可以存储在服务器120的账户数据124a中与非接触式卡101相关联的客户的记录中(和/或存储在不同的安全位置中)。主密钥可以对所有各方保密——除了非接触式卡101和服务器120之外，从而增强系统100的安全性。

[0033] 主密钥105可以与计数器104结合使用以使用密钥多样化来增强安全性。计数器104包括在非接触式卡101和服务器120之间同步的值。计数器值104可以包括每次在非接触式卡101和服务器120(和/或非接触式卡101和移动设备110)之间交换数据时改变的数字。为了使能非接触式卡101和移动设备110之间的NFC数据传输，当非接触式卡101足够靠近移动设备110的读卡器118(例如在NFC范围内)时，账户应用113可以与非接触式卡101通信。读卡器118可以是具有NFC能力的数字读取器，例如NFC读取器，并且可以被配置为从非接触式卡101读取和/或与其通信(例如，经由NFC、蓝牙、RFID等)。因此，示例读卡器118包括NFC通信模块、蓝牙通信模块和/或RFID通信模块。

[0034] 例如，用户可能需要授权或验证来对访问应用116进行访问。系统100的一个或多个组件(包括认证应用114)可以发起与访问应用的通信(例如，API调用或另一合适的机制)，以利用一个或多个支付协议来验证或认证用户，无论访问应用116或访问应用116的用户进行访问所寻求的特定方面是否涉及进行支付。

[0035] 在各种实施例中，一个或多个协议可以涉及如本文别处讨论的在线技术。认证应用114可以向用户提供提示，使得用户可以将非接触式卡101轻拍到移动设备110，从而使非接触式卡101充分靠近移动设备110的读卡器118，以使能非接触式卡101和移动设备110的读卡器118之间的NFC数据传输。在各种实施例中，移动设备110可以经由API调用而触发读卡器118。另外和/或可替选地，移动设备110可以基于周期性地轮询读卡器118来触发读卡器118。更一般地，移动设备110可以使用任何可行的方法来触发读卡器118参与通信。

[0036] 在各种实施例中，在发起与非接触式卡101、读卡器118和移动设备110有关的任何通信之前，和/或立即地在非接触式卡101和读卡器118之间建立通信之后，认证应用114可以接收第一应用用户凭证作为卡激活和/或开始在线认证协议的先决条件。用户可以在接收到来自认证应用的输入凭证的提示之后提供第一应用用户凭证。如上面提到的，第一应用用户凭证可以包括生物特征数据、与用户识别相关联的已建立手势、用户名和密码组合、面部识别和/或诸如此类。如上面提到的，在各种实施例中，认证应用114将第一应用用户凭证传送到处理器119。处理器119将第一应用用户凭证与存储的第二应用用户凭证进行比较。存储的第二应用用户凭证可以位于与移动设备110相关联的存储器111、与非接触式卡101相关联的存储器102和/或与服务器120相关联的存储器122内。在各种实施例中，第一应用用户凭证提供给服务器120，并且服务器120将第一应用用户凭证与存储的第二应用用户凭证进行比较。在各种实施例中，如上面提到的，处理器119将比较结果传送到认证应用114

(例如,用于匹配)。在各种实施例中,第一匹配可以发起或用作以下一项或多项的先决条件:i)发起在线验证协议的其余部分以验证或认证用户对访问应用116进行访问;和/或ii)授予用户对与访问应用116相关联的用户账户的第一级用户账户选项的访问权限(例如,账户余额和/或最近交易的显示);和/或iii)生成认证令牌,该认证令牌被提供给条形码生成应用117b以生成条形码,该条形码可以被扫描以访问与访问应用116相关联的一个或多个特征和/或以其他方式完成与其相关联的交易,例如支付交易。像这样,在各种实施例中,响应于找到了第一匹配,验证认证应用发起(与在线验证过程相关联的)附加操作以验证用户身份。

[0037] 在各种实施例中,系统100包括忠诚度积分应用117a,其基于在线验证协议来利用与访问应用116和/或零售商148相关联的忠诚度积分,该在线验证协议可以利用或可以不利用与条形码生成应用117b相关联的所生成的条形码。忠诚度积分应用117a可以允许用户执行与忠诚度积分有关的任何数量和类型的操作,诸如查看忠诚度积分余额、为产品、商品和/或服务兑换忠诚度积分、将忠诚度积分转移到其他账户和诸如此类。当用户请求执行忠诚度积分应用117a中的操作时,可能要求用户使用非接触式卡101验证他们的身份。如本文更详细描述的,可以基于服务器120验证由非接触卡101生成的加密数据、应用用户凭证的匹配和/或使用由条形码生成应用程序117b生成的条形码来授权所请求的操作。

[0038] 在各种实施例中,第一应用用户凭证与存储的第二应用用户凭证的第一匹配可以授予或可以不授予对应用(例如访问应用116)的第一级访问权限,但是第一匹配服务在任何情况下都可以用作发起至少一个在线授权协议的先决条件。在最初未授予第一级访问权限的各种实施例中,成功完成至少一个在线和/或离线协议导致了授予第一级访问权限。在各种实施例中,在完成在线和/或离线验证协议中的至少一个并且扫描由于这些协议之一完成而生成的条形码后,立即授予对访问应用116的第二级访问权限,其中第二级访问可以指完成与访问应用116有关的支付交易。

[0039] 在各种实施例中,不论任何其他先决条件如何,非接触式卡101在移动设备110上的第一次轻拍发起在线和离线验证协议,并且第二次轻拍(随后的轻拍)发起在线和离线验证协议中的另一个。

[0040] 在各种实施例中,无论是否应用或发生一个或多个先决条件,在移动设备110与非接触式卡101之间建立了通信之后,非接触式卡101生成消息认证码(MAC)密码。在各种实施例中,这可以在账户应用113读取非接触式卡101时发生。特别地,这可以发生在读取(诸如,NFC读取)近场数据交换(NDEF)标签时,其可以根据NFC数据交换格式来创建。例如,诸如账户应用113和/或读卡器118之类的读取器可以发送消息诸如小应用程序选择消息,其具有产生NDEF的小应用程序的小应用程序ID。在各种实施例中,所生成的密码可以是符合EMV标准的授权请求密码(ARQC)。

[0041] 在各种实施例中,在确认选择之后,可以发送选择文件消息随后是读取文件消息的序列。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,可以更新或递增由非接触式卡101维护的计数器值104,其随后可以是“读取NDEF文件”。此时,可以生成可包括报头(header)和共享机密的消息。然后可以生成会话密钥。可以从消息创建MAC密码,该消息可以包括报头和共享机密。然后可以将MAC密码与一个或多个随机数据块级联,并且可以用会话密钥对MAC密码和随机数(RND)进行加密。此后,可以将密码和报头

进行级联，并编码为ASCII十六进制，并以NDEF消息格式返回(响应于“读取NDEF文件”消息)。在各种实施例中，MAC密码可以作为NDEF标签被发送，并且在其他示例中，MAC密码可以以统一资源指示符(例如，作为格式化的字符串)被包括。非接触式卡101然后可以将MAC密码发送到移动设备110，移动设备110然后可以将MAC密码转发到服务器120用于验证，如下面说明的。(然而，在各种实施例中，移动设备110可以验证MAC密码)。

[0042] 更一般地，当准备发送数据(例如，到服务器120和/或移动设备110)时，非接触式卡101可以递增计数器值104。非接触式卡101然后可以提供主密钥105和计数器值104作为至密码算法的输入，其产生多样化密钥106作为输出。密码算法可以包括加密算法、基于散列的消息认证码(HMAC)算法、基于密码的消息认证码(CMAC)算法和诸如此类。密码算法的非限制性示例可包括对称加密算法，诸如3DES或AES128；对称HMAC算法，诸如HMAC-SHA-256；对称CMAC算法，诸如AES-CMAC；和/或与ISO/IEC 1833和/或ISO/IEC 7816的任何适用版本一致的任何其他算法或技术。非接触式卡101然后可以使用多样化密钥106来加密数据(例如，客户标识符107和任何其他数据)。然后非接触式卡101可以将加密数据(例如，加密的客户ID 109)发送到移动设备110的账户应用113(例如，经由NFC连接、蓝牙连接等)。移动设备110的账户应用113然后可以经由网络130将加密数据发送到服务器120。在至少各种实施例中，非接触式卡101将计数器值104与加密数据一起发送。在这样的实施例中，非接触式卡101可以发送加密的计数器值104或未加密的计数器值104。

[0043] 在接收到加密的客户ID 109时，服务器120的管理应用123可以使用计数器值104作为至加密的输入并且使用主密钥105作为用于加密的密钥来执行相同的对称加密。如上所述，计数器值104可以在从移动设备110接收到的数据中被指定，或者计数器值104可以由服务器120维护，以实施非接触式卡101的密钥多样化。加密的输出可以是由非接触式卡101创建的相同的多样化密钥值106。然后，管理应用123可以使用多样化密钥106解密经由网络130接收到的加密的客户ID 109，这揭示了由非接触式卡101发送的数据(例如，至少客户标识符107)。这样做允许管理应用123验证由非接触式卡101经由移动设备110发送的数据，例如通过将解密的客户ID 107与账户的账户数据124a中的客户ID进行比较。一旦被验证，管理应用123就可以向移动设备110发送成功验证的指示。

[0044] 尽管使用计数器104(例如，ATC)作为示例，但也可以使用其他数据来保护非接触式卡101、移动设备110和/或服务器120之间的通信。例如，计数器104可以替换为每次需要新的多样化密钥106时生成的随机数、从非接触式卡101和服务器120发送的计数器值的全部值、从非接触式卡101和服务器120发送的计数器值的一部分、由非接触式卡101和服务器120独立维护(但不在两者之间发送)的计数器、在非接触式卡101和服务器120之间交换的一次性密码以及数据的加密散列。在各种实施例中，各方可以使用多样化密钥106的一个或多个部分来创建多个多样化密钥106。

[0045] 如示出的，服务器120可以包括一个或多个硬件安全模块(HSM)125。例如，一个或多个HSM 125可被配置为执行一个或多个密码操作，如本文所公开的。在各种实施例中，一个或多个HSM 125可以被配置为专用安全设备，其被配置为执行一个或多个密码操作。HSM 125可以被配置为使得密钥永远不会在HSM 125外部泄露，而是被保持在HSM 125内。例如，一个或多个HSM 125可以被配置为执行密钥派生、解密和MAC操作中的至少一项。一个或多个HSM 125可以被包含在服务器120内或者可以与服务器120进行数据通信。

[0046] 如上所述，密钥多样化技术可用于使用非接触式卡101来执行安全操作。例如，一旦管理应用123使用密钥多样化验证了加密的客户ID 109，管理应用123就可以向认证应用114(或设备110的任何其他组件，诸如账户应用113、积分应用117A、应用116等)发送指示出用户被验证和/或认证的消息，并且认证应用114可以授予用户对访问应用116的访问权限作为结果。在各种实施例中，发送的输出可以包括授权响应密码(ARPC)。通常，在接收到指示出基于对加密的客户ID 109的验证而验证和/或认证了用户的消息时，移动设备110的接收组件可以允许任何数量的操作。例如，积分应用117A可以允许访问忠诚度账户，例如查看忠诚度积分、兑换忠诚度积分等。

[0047] 如在此描述的一个或多个实施例中所固有的，包括上面的讨论，服务器120可以用于在线认证或验证并且可以被配置为与EMV标准一致地操作，包括执行利用用于非支付目的的EMV支付协议的操作。主机服务器(或系统)120可以与同用户相关联的卡的发行者相关联，并且主机系统包括存储可由处理器执行的计算机可读程序代码的非暂时性计算机可读存储介质，其中处理器和存储介质可以包含一个或多个硬件或软件组件，包括图8中一般描述的那些。主机系统可以被配置为接收与访问应用116和/或非接触式卡101相关联的交易数据。如本文描述的，可以例如通过与移动设备110和用户(或其他合适的计算机设备)相关联的认证应用114(或移动设备110的其他合适的组件或应用)来促进交易数据的接收，其中认证应用114可以发起与一个或多个其他组件(例如非接触式卡101和读卡器118)的认证或验证交易。服务器120从认证应用114接收交易数据。交易数据可以包括i)计数器(例如ATC)和基于交易的一个或多个输入的密码、以及与卡关联的对称密钥。在各种实施例中，密码是授权请求密码(ARQC)。

[0048] 在各种实施例中，一旦服务器120接收到交易数据，管理应用123就可以向移动设备110的适当组件(例如，认证应用114、账户应用113、积分应用117a等)发送响应(例如，来自发行者)，以基于接收到的密码来验证用户的身份。响应于验证响应的接收，认证应用114可以授予对访问应用116的相关部分或特征的访问权限作为结果和/或促进对完成与访问应用116相关联的交易有用的条形码的生成。在各种实施例中，响应可以包括提供给与非接触式卡101和/或移动设备110相关联的条形码生成应用117b的认证令牌，该认证令牌可以由条形码生成应用117b使用以在显示器140和/或显示器141上显示条形码，其中条形码可以由合适的扫描设备扫描，该扫描设备可以解密认证令牌以便完成与访问应用116相关联的交易，例如支付交易，和/或以其他方式提供对与访问应用116相关联的特征的访问。此外，访问应用116可以允许访问移动设备110上的另一个应用(例如账户应用113和/或积分应用117a)的相关部分或特征。类似地，账户应用113和/或积分应用117a可以接收验证响应并允许访问应用的相关部分或特征，诸如访问积分应用117a中的忠诚度积分账户、使用忠诚度积分授权交易，等等。

[0049] 在各种实施例中，管理组件123可以将认证令牌配置为一旦发生对条形码的单次扫描就被禁用，其中扫描授予对与访问应用116相关联的特征的访问权限和/或以其他方式完成与其相关联的交易，这继而可以禁止未授权的随后使用条形码来对访问应用116的各方面进行访问。在各种实施例中，所生成的条形码可以用于超过一个的应用，例如多个访问应用116，这取决于用户决定做出的选择，前提是已经发生了认证协议。在各种实施例中，管理应用123可以接收来自用户或来自认证应用114的指令作为整体交易数据的一部分，以对

与访问应用116相关联的交易施加限制，例如，对支付交易的货币限制，其中管理应用123配置授权令牌(以及通过扩展的随后生成的条形码)以实施该限制。在各种实施例中，授权令牌可以是授权与访问应用116有关的支付交易的支付令牌，其具有或不具有关于可以花费的金额的预先规定的用户限制。

[0050] 因此，在各种实施例中，如本文概述的所生成的条形码可以是显示在移动设备110和/或非接触式卡101的表面上的具有以下特征中的至少一个的动态条形码：i)该条形码可以被配置为在单次使用后禁用；ii)该条形码可用于超过一个的访问应用116(假设与认证令牌相关联的认证协议发生)，包括单个或多个用例，例如在单个用例中，一旦生成了条形码，但在扫描发生之前，认证应用114可以允许用户访问另一个访问应用116并利用条形码，而无需再次运行任何协议(例如计数器日志121可以由认证应用114利用以确保在生成条形码之后没有发生后续交易，这继而可以允许用户将条形码的使用切换到另一个访问应用116和/或访问最初选出的访问应用116的另一个特征，其与最初选出的不同)；iii)该条形码可以被配置为一旦发生了验证协议就对多次扫描和不同的访问应用116保持活动状态；和/或iv)授权令牌(以及通过扩展的条形码)可以被配置为与同关联于访问应用116的交易有关的预先规定的限制(由用户或其他方式)相关联，例如，针对访问应用116对要完成的支付交易设定货币限制。注意，在各种实施例中，本段描述的特征不仅适用于相对于上面描述的在线协议生成的条形码，而且适用于相对于此处描述的任何其他协议。

[0051] 在各种实施例中，服务器120可以利用计数器日志121来执行反欺诈措施。在各种实施例中，计数器日志121可以包括与同一个或多个非支付交易相关联的计数器值相关联的时间戳。在各种实施例中，计数器日志121可以包括与同一个或多个支付交易相关联的计数器值相关联的时间戳。在各种实施例中，与特定交易有关的ATC的计数器值(例如无论是支付交易还是非支付交易)都可能被记录。管理应用123可以被配置为比较发生在非支付交易之间的支付交易的一般性数量。如果在非支付交易之后支付交易的数量超过特定阈值，则管理应用123可以拒绝支付交易，即使该交易可以以其他方式完成也是如此(例如，由于假设用户可以使用支付协议进行非支付和支付协议，因此在非支付交易之后的过度大量的支付交易可能被认为是欺诈性的)。在各种实施例中，可以实施相反的情况，例如在支付交易超过阈值之后执行的大量非支付交易可能导致管理应用123在验证或认证发生时拒绝某个非支付交易。在各种实施例中，就超过最小或最大阈值而言，与任何交易(例如支付或非支付)之间的时间有关的阈值可能导致管理应用123拒绝认证或验证操作。计数器日志121可用于执行任何其他合适的操作，包括以任何其他合适的方式执行反欺诈措施。在各种实施例中，反欺诈措施可以通过指示移动设备的适当组件(例如认证应用114)拒绝应用来覆盖有效的授权令牌，即使与条形码相关联的认证令牌有效也是如此。

[0052] 图2是描绘轻拍以发起在线验证和/或认证协议来生成用于访问特征和/或完成与访问应用116有关的交易的条形码的示例实施例的示意图200。授权应用114在移动设备110上的图形用户界面的(GUI)可以包括轻拍非接触式卡101来发起对另一应用(例如访问应用116)的认证或验证的提示206，其中可以提供单独的API接口以通过认证应用114将验证或认证(一旦完成)传送到访问应用116。在各种实施例中，访问应用116提供提示202作为用于接收轻拍提示206的先决条件，或在轻拍发生之后但在任何附加在线验证操作之前提供提示，来输入用户凭证以比较(例如，如参考图1描述的)与访问应用116有关的第一级和/或第

二级信息访问。在各种实施例中，认证应用114为提示202提供界面，用于输入关于访问应用116和/或任何其他应用(例如其他应用115)的用户凭证。

[0053] 在各种实施例中，一旦非接触式卡101被轻拍到移动设备110，认证应用114就经由读卡器118(例如，经由NFC、蓝牙、RFID等)向非接触式卡发送指示。在各种实施例中，该指示可以指定执行如关于图1描述的一种或多种加密技术。在各种实施例中，使用在线认证技术，并且认证应用114从服务器120接收交易数据。在各种实施例中，在非接触式卡101和移动设备110之间发送数据的提示可以指定经由与EMV协议或标准一致的任何合适的协议将数据发送到认证应用114，其中在各种实施例中认证应用114经由与EMV协议或标准一致的协议直接从非接触式卡101接收任何合适的数据。

[0054] 图3是示意图300，描绘了在轻拍以发起在线验证和/或认证协议(以生成条形码)(例如用于访问特征和/或完成与访问应用116有关的交易)发生之后所生成的条形码的示例实施例。在各种实施例中，在移动设备的显示器上生成适合于由任何合适的扫描设备扫描的条形码307。在各种实施例中，服务器的管理应用123和/或移动设备110的认证应用114可以向与移动设备110(如图3中示出的)和/或非接触式卡101相关联的条形码生成应用117b提供认证令牌，并且条形码生成应用117b可以使用认证令牌来生成单次使用条形码307以授予对访问应用116的一个或多个特征的访问权限(和/或完成与其相关的交易)，和/或用于重复性使用以授予对访问应用116的一个或多个特征的访问权限(和/或完成与其相关的交易)。作为另一示例，条形码307可用于授权访问积分应用117a中的忠诚度账户和/或执行与积分应用117a中的忠诚度账户相关联的操作。

[0055] 图4A示出了非接触式卡101，其可以包括支付卡，诸如信用卡、借记卡和/或礼品卡。如示出的，非接触式卡101可以由显示在卡101正面或背面的服务提供商405发行。在各种实施例中，非接触式卡101与支付卡无关，并且可以包括但不限于身份证。在各种实施例中，支付卡可以包括双界面非接触式支付卡。非接触式卡101可以包括基板410，其可以包括由塑料、金属和其他材料构成的单层或一个或多个层压层。示例性基板材料包括聚氯乙烯、聚氯乙烯醋酸酯、丙烯腈丁二烯苯乙烯、聚碳酸酯、聚酯、阳极氧化钛、钯、金、碳、纸和可生物降解材料。在各种实施例中，非接触式卡101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，根据本公开的非接触式卡101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。

[0056] 非接触式卡101还可以包括显示在卡的正面和/或背面上的识别信息415，以及接触垫420。接触垫420可以被配置为与另一个通信设备建立接触，诸如移动设备110、用户设备、智能电话、手提电脑、台式计算机或平板计算机。非接触式卡101还可以包括处理电路、天线和图4A中未示出的其他组件。这些组件可以位于接触垫420的后面或基板410上的其他地方。非接触式卡101还可以包括磁条或磁带，其可以位于卡的背面(图4A中未示出)。非接触式卡101可以包括显示界面416，其可以显示可以如参考图1-图3和图5-图7B描述的所生成的条形码417，其中条形码417可以由任何合适的扫描设备扫描和解密，以便授予对应用的特征的访问权限和/或促进与应用相关联的交易(诸如支付交易)的完成。

[0057] 如图4B中示出的，非接触式卡101的接触垫420可以包括用于存储和处理信息的处理电路425，包括微处理器430和存储器102。应当理解，处理电路425可以包含附加组件，包括处理器、存储器、错误和奇偶校验/CRC校验器、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，如执行此处描述的功能所必需的。

[0058] 存储器102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101可以包括这些存储器中的一个或多个。只读存储器可以在工厂可编程为只读或一次性可编程。一次性可编程性提供了一次写入然后多次读取的机会。可以在存储器芯片出厂后的某个时间点对一次写入/多次读取的存储器进行编程。一旦存储器被编程，它就可能不会被重写，但它可能被多次读取。读/写存储器在出厂后可以多次编程和重新编程。读/写存储器在出厂后也可能被多次读取。

[0059] 存储器102可以被配置为存储一个或多个小应用程序(applet)440、一个或多个计数器104、客户标识符107和虚拟账号108。一个或多个小应用程序440可以包括一个或多个软件应用，其被配置为在一个或多个非接触式卡上执行，诸如Java®Card小应用程序。然而，应当理解，小应用程序440不限于Java卡小应用程序，而是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104可以包括足以存储整数的数字计数器。客户标识符107可以包括分配给非接触式卡101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来。在各种实施例中，客户标识符107可以识别客户和分配给该客户的账户并且可以进一步识别与客户的账户相关联的非接触式卡。如上所述，账号108可以包括与非接触式卡101相关联的数千个一次性使用虚拟账号。非接触式卡101的小应用程序440可以被配置为管理账号108。存储器102可以被配置为包含可以生成条形码417的条形码生成应用117b，该条形码417例如如图4A中示出的，其可以被任何合适的扫描设备扫描和解密，并用于本文描述的任何合适的目的。

[0060] 上述示例性实施例的处理器和存储器元件是参照接触垫描述的，但本公开不限于此。应当理解，这些元件可以在垫420的外部实施或与其完全分离，或者作为除了位于接触垫420内的处理器430和存储器102元件之外的另外的元件。

[0061] 在各种实施例中，非接触式卡101可以包括一个或多个天线455。一个或多个天线455可以放置在非接触式卡101内和接触垫420的处理电路425周围。例如，一个或多个天线455可以与处理电路425构成一体，并且一个或多个天线455可以与外部增强线圈一起使用。作为另一示例，一个或多个天线455可以在接触垫420和处理电路425的外部。

[0062] 在实施例中，非接触式卡101的线圈可以充当空气心变压器的次级。终端可以通过切断功率或幅度调制与非接触式卡101进行通信。非接触式卡101可以使用非接触式卡的功率连接中的间隙来推断从终端发送的数据，其可以通过一个或多个电容器在功能上保持。非接触式卡101可以通过切换非接触式卡的线圈上的负载或负载调制而向回通信。可以通过干扰在终端的线圈中检测到负载调制。更一般地，使用天线455、处理电路425和/或存储器102，非接触式卡101提供通信接口以经由NFC、蓝牙和/或Wi-Fi通信进行通信。

[0063] 如上面说明的，非接触式卡101可以构建在在智能卡或具有有限存储器的其他设备(诸如JavaCard)上可操作的软件平台上，并且可以安全地执行一个或多个或多个应用或小应用程序。小应用程序440可以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(MFA)提供一次性密码(OTP)。小应用程序440可以被配置为响应来自诸如移动NFC读取器(例如，移动设备110的)的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文本标签的加密安全OTP的NDEF消息。

[0064] NDEF OTP的一个示例是NDEF短记录布局(SR＝1)。在这样的示例中，一个或多个小应用程序440可以被配置为将OTP编码为NDEF类型4公知类型文本标签。在各种实施例中，NDEF消息可以包括一个或多个记录。小应用程序440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。

[0065] 在各种实施例中，一个或多个小应用程序440可以被配置为模拟RFID标签。RFID标签可以包括一个或多个多态标签。在各种实施例中，每次读取标签时，都会呈现不同的密码数据，这些密码数据可以指示非接触式卡的真实性。基于一个或多个应用，可以处理标签的NFC读取，可以将数据发送到服务器，诸如服务器120，并且可以在服务器处验证数据。

[0066] 在各种实施例中，非接触式卡101和服务器120可以包括某些数据，使得可以正确地识别卡。非接触式卡101可以包括一个或多个唯一标识符(未图示)。每次发生读取操作时，可以将计数器104配置为递增。在各种实施例中，每次读取来自非接触式卡101的数据(例如，通过移动设备110)时，将计数器104发送到服务器以进行验证并确定计数器值104是否相等(作为验证的一部分)。

[0067] 一个或多个计数器104可以被配置为防止重放攻击。例如，如果已获得并重放密码，则如果计数器104已被读取或使用或以其他方式传递，则立即拒绝该密码。如果计数器104没有被使用，则它可以被重放。在各种实施例中，在卡上递增的计数器不同于为交易递增的计数器。非接触式卡101无法确定应用交易计数器104，这是因为非接触式卡101上的小应用程序440之间没有通信。在各种实施例中，非接触式卡101可以包括第一小应用程序440-1(其可以是交易小应用程序)和第二小应用程序440-2。每个小应用程序440-1和440-2可以包括相应的计数器104。

[0068] 在各种实施例中，计数器104可能不同步。在各种实施例中，为了解决发起事务的意外读取，诸如以一定角度读取，计数器104可以递增但应用不处理计数器104。在各种实施例中，当移动设备110被唤醒时，NFC可以被使能并且设备110可以被配置为读取可用标签，但是没有采取任何动作来响应读取。

[0069] 为了使计数器104保持同步，可以执行诸如后台应用之类的应用，该应用可以被配置为检测移动设备110何时醒来并与服务器120同步，以指示由于检测而发生的读取然后向前移动计数器104。在其他示例中，可以利用散列一次性密码使得可以接受错误同步的窗口。例如，如果在10的阈值内，则计数器104可以被配置为向前移动。但是如果在不同的阈值数内，例如在10或1000内，则可以处理执行重新同步的请求，其经由一个或多个应用请求用户经由用户的设备轻拍、做手势或以其他方式指示一次或多次。如果计数器104以适当的序列增加，则可以知道用户已经这样做了。

[0070] 这里参考计数器104、主密钥105和多样化密钥106描述的密钥多样化技术是密钥多样化技术的加密和/或解密的一个示例。该示例密钥多样化技术不应被视为对本公开的限制，这是因为本公开同样适用于其他类型的密钥多样化技术。

[0071] 在非接触式卡101的创建过程期间，可以为每张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，并且它由非接触式卡101中的硬件实施。通过使用密钥多样化过程，一个或多个密钥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中派生。

[0072] 在各种实施例中，为了克服可能易受漏洞影响的3DES算法的缺陷，可以派生会话

密钥(诸如每个会话的唯一密钥),而不是使用主密钥,唯一的卡派生密钥和计数器可以用作多样化数据。例如,每次在操作中使用非接触式卡101时,可以使用不同的密钥来创建消息认证码(MAC)和执行加密。这导致了三层加密。会话密钥可以由一个或多个小应用程序生成,并通过使用应用交易计数器以一种或多种算法(如EMV 4.3第2册A1.3.1通用会话密钥派生中所定义)来派生。

[0073] 此外,每张卡的增量可以是唯一的,并且通过个性化来分配,或者通过一些识别信息来算法分配。例如,奇数卡可以递增2,并且偶数卡可以递增5。在各种实施例中,增量也可以在顺序读取中变化,使得一张卡可以按序列递增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,或者从源自唯一标识符的一个或多个过程中定义。这会使重放攻击者更难从少量卡片实例中进行泛化。

[0074] 认证消息可以作为十六进制ASCII格式的文本NDEF记录的内容被递送。在另一个示例中,可以以十六进制格式对NDEF记录进行编码。

[0075] 图5示出了逻辑流程500的实施例。逻辑流程500可以表示由本文描述的一个或多个实施例执行的一些或所有操作。例如,逻辑流程500可以包括一些或所有操作以利用在线认证技术来验证或认证用户以访问与忠诚度积分相关联的一个或多个账户和/或以其他方式利用忠诚度积分。实施例不限于此上下文。

[0076] 如所示出的,逻辑流程500在框505处开始,其中认证应用114、OS 112、管理应用123和/或任何其他合适应用中的至少一个可以发起事务以验证用户的身份并生成条形码来访问与访问应用116相关联的特征。在各种实施例中,可以通过将非接触式卡101轻拍在移动设备110上来开始验证。在各种实施例中,访问应用116提供关于用于接收轻拍提示的先决条件的提示,或在轻拍发生后立即地、但在任何附加在线验证操作之前提供提示,来输入用户凭证以比较与访问应用116有关的第一级和/或第二级信息访问,其中第一级特征的性质在本文别处描述。在各种实施例中,用户凭证与用户简档相关联并且被输入到由移动设备110提供的界面中,其中如上所述,第一应用用户凭证可以包括生物特征数据、与用户识别相关联的已建立手势、用户名和密码组合和/或诸如此类。第一应用用户凭证可以由认证应用114发送到服务器120的管理应用123,其中将第一应用用户凭证与存储的第二凭证进行比较。

[0077] 在框510处,并且根据各种实施例,发起移动设备110与非接触式卡101之间的通信,其中该通信利用读卡器118并且其中该通信基于NFC协议。在各种实施例中,通信是关于导致匹配的第一级比较的条件,并且在各种实施例中,不是在服务器120处发送第一应用凭证用于比较,而是在移动设备110和非接触式卡101之间进行比较,其中所存储的第二凭证存储在非接触式卡的存储器102中。在各种实施例中,省略了关于用户凭证的比较,并且非接触式卡101对移动设备110的轻拍发起提示以选择哪个应用需要认证,例如访问应用116,并且非接触式卡101和移动设备110之间的NFC通信开始使用与EMV标准一致的支付协议来发起用户的在线验证或认证,但出于包括验证或认证的目的,而不仅仅是完成销售或购买的目的。在各种实施例中,如上所述,用户向移动设备110轻拍非接触式卡101以致使非接触式卡101生成和发送加密数据(例如,加密的客户ID 109)。响应于接收到用于生成加密数据的指示,非接触式卡101可以递增存储器102中的计数器值104。

[0078] 在各种实施例中,在框515处,非接触式卡101使用存储器102中的计数器值104和

主密钥105以及密码算法来生成多样化密钥106。在框520处，非接触式卡101使用多样化密钥106和密码算法来对数据进行加密(例如，客户标识符107)，从而生成了加密数据(例如，加密的客户ID 109)。

[0079] 在框525处，非接触式卡101可以例如使用NFC将加密数据发送到移动设备110的账户应用113。在至少一个实施例中，非接触式卡101还包括计数器值104的指示以及加密数据。在框530处，移动设备110的账户应用113可以将从非接触式卡101接收到的数据发送到服务器120的管理应用123。在框535处，服务器120的管理应用123可以使用主密钥105和计数器值104作为至密码算法的输入来生成多样化密钥106。在一个实施例中，管理应用123使用由非接触式卡101提供的计数器值104。在另一实施例中，管理应用123递增存储器122中的计数器值104以使存储器122中的计数器值104的状态与非接触式卡101的存储器102中的计数器值104同步。

[0080] 在框540处，管理应用123使用多样化密钥106和密码算法对经由移动设备110从非接触式卡101接收到的加密数据进行解密。这样做可以至少产生客户标识符107。通过产生客户标识符107，管理应用123可以在框545处验证从非接触式卡101接收到的数据。例如，管理应用123可以将客户标识符107与在账户数据124a中的相关联的账户的客户标识符进行比较，并基于匹配来验证数据。这样做可以致使管理应用123将验证的指示发送到移动设备110。

[0081] 在框550处，响应于框540和545的解密和验证，管理应用123可以提供对一个或多个忠诚度积分账户124b的访问并且可以允许兑换与其相关联的一个或多个忠诚度积分，包括与零售商148相关联的忠诚度积分。虽然被描述为存储在服务器120中，但是积分应用117a可以包括忠诚度积分账户124b的实例。在各种实施例中，在解密之前，管理应用123可以生成授权令牌，该授权令牌可以被发送到非接触式卡101和/或移动设备110的条形码生成应用117b，其中条形码然后可以通过显示器140和/或显示器141显示，其中授权令牌可以强加一个或多个限制和条件，如上文关于图1的各种组件所概述的，并且条形码可以由任何合适的扫描设备扫描，以便启用与忠诚度积分账户124b相关联的任何忠诚度积分的解密和利用。在各种实施例中，条形码生成应用117可以使用用于条形码生成的任何合适技术来生成条形码，其中所生成的条形码可以显示在移动设备的显示器140和/或非接触式卡101的显示器141上。

[0082] 图6示出了逻辑流程600的实施例。逻辑流程600可以表示由本文描述的一个或多个实施例执行的一些或所有操作。例如，逻辑流程600可以包括利用与图5相关联的所生成的条形码来授权与访问应用116相关联的交易。实施例不限于此上下文。

[0083] 如所示出的，逻辑流程600在图5的一个或多个操作完成之后开始，其中在各种实施例中，流程在图5的框530处开始。在框605处，系统100的任何合适的组件可以通过在处理器电路上执行的应用确定用户正在请求访问忠诚度积分账户数据库。在框610处，利用如本文所讨论的任何合适的技术，系统100的任何合适的组件可以由应用并从与处理电路相关联的计算机设备向服务器120发送第一应用用户凭证。在框615处，系统100的任何合适的组件可以在服务器处将第一应用用户凭证与存储的第二应用用户凭证进行比较，存储的第二应用用户凭证存储在服务器处。在框620处，响应于第一凭证和第二凭证的匹配，系统100的任何合适的组件可以由应用从与账户相关联的非接触式卡的通信接口接收加密数据，所述

加密数据基于密码算法和多样化密钥而生成，所述多样化密钥存储在非接触式卡的存储器中并基于存储在非接触式卡的存储器中的计数器值和主密钥而生成。在框625处，响应于第一凭证和第二凭证的匹配，系统100的任何合适的组件可以将与用户相关联的忠诚度标识符与加密数据组合，并且其中数据组合包括忠诚度标识符和加密数据的组合。该组合(和/或本文描述的任何其他组合操作)可以基于逻辑操作。逻辑操作可以是异或操作。在框630处，系统100的任何合适的组件可以在服务器处对接收到的加密数据和忠诚度标识符执行操作。在框635处，系统100的任何合适的组件可以在i)非接触式卡和ii)计算机设备中的任一个处生成条形码，其中所生成的条形码基于从服务器接收到的令牌并利用加密数据和忠诚度标识符。在框640处，系统100的任何合适的组件可以显示所生成的条形码。在框645处，系统100的任何合适的组件可以基于对所生成的条形码的扫描，由应用并从服务器接收对加密数据的验证，该服务器基于存储在服务器的存储器中的多样化密钥以及密码算法来对加密数据进行解密以验证加密数据，其中存储在服务器的存储器中的多样化密钥基于存储在服务器的存储器中的计数器值和主密钥而生成。在框650处，响应于接收到验证，系统100的任何合适的组件可以授予执行至少一个操作的授权，其中至少一个操作包括以下至少一项：i)访问包含与至少一个用户和至少两个不同账户相关联的多个忠诚度标识符的数据库，每个账户与不同的忠诚度积分集合相关联，以及ii)在数据库中相关于至少两个不同账户存储多个忠诚度标识符中的至少一个。

[0084] 在各种实施例中，可以将非接触式卡101轻拍到设备，诸如一个或多个计算机信息亭或终端，以验证身份，以便响应于购买而接收交易物品，诸如咖啡。通过使用非接触式卡101，可以建立在忠诚度程序中证明身份的安全方法。以不同于仅仅扫描酒吧卡的方式来建立安全地证明身份，例如，以获得奖励、优惠券、优惠或诸如此类或利益的接收。例如，加密交易可以发生在非接触式卡101和设备之间，其可以被配置为处理一个或多个轻拍手势。如上面说明的，一个或多个应用可以被配置为验证用户的身份，并且然后致使用户对其进行动作或响应，例如，经由一个或多个轻拍手势。在各种实施例中，可以将例如消费积分、忠诚度积分、奖励积分、保健信息等的数据写回到非接触式卡。

[0085] 在各种实施例中，非接触式卡101可以被轻拍到设备，诸如移动设备110。如上面说明的，用户的身份可以由一个或多个应用验证，该一个或多个应用然后可以基于身份验证授予用户期望的利益。

[0086] 在各种实施例中，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EMV标准的离线动态数据认证协议，并进行一些修改。例如，因为示例认证协议本身不用于与发卡机构/支付处理器完成支付交易，所以不需要一些数据值，并且可以在不涉及到发卡机构/支付处理器的实时在线连接的情况下执行认证。如本领域中已知的，销售点(POS)系统向发卡机构提交包括交易价值的交易。发行者是批准还是拒绝交易可以基于发卡机构是否识别出交易价值。同时，在本公开的某些实施例中，源自移动设备的交易缺乏与POS系统相关联的交易价值。因此，在各种实施例中，伪交易价值(即，可被发卡机构识别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次数(例如，交易计数器)拒绝交易。超过缓冲值的多次尝试可能会导致软拒绝；该软拒绝在接受交易之前需要进一步验证。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。

[0087] 在各种实施例中，非接触式卡101可以取决于接收方设备选择性地传送信息。一旦轻拍，非接触式卡101就可以识别轻拍指向的设备，并且基于这种识别，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发送完成即时动作或交易所需的信息，诸如支付或卡认证。通过限制数据的传输并且避免不必要的数据传输，可以提高效率和数据安全性。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、商业交易和逐步减少欺诈。

[0088] 如果非接触式卡101的轻拍针对运行Apple的iOS®操作系统的设备，例如iPhone、iPod或iPad，则非接触式卡可以识别iOS®操作系统并发送数据适当的数据以与该设备进行通信。例如，非接触式卡101可以经由例如NFC提供使用NDEF标签来认证卡所必需的加密身份信息。类似地，如果非接触式轻拍指向运行Android®操作系统的设备，例如Android®智能手机或平板电脑，则非接触式卡可以识别Android®操作系统并发送适当的数据以与该设备通信(诸如通过此处描述的方法进行认证所需的加密身份信息)。

[0089] 作为另一个示例，非接触式卡轻拍可以指向POS设备，包括但不限于信息亭、结账登记簿、支付站或其他终端。在执行轻拍时，非接触式卡101可以识别POS设备并且仅发送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设备时，非接触式卡101可以根据EMV标准传送完成交易所需的支付信息。

[0090] 在各种实施例中，参与交易的POS设备可以要求或指定要由非接触式卡提供的附加信息，例如设备特定信息、位置特定信息和交易特定信息。例如，一旦POS设备接收到来自非接触式卡的数据通信，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。

[0091] 在各种实施例中，POS设备可以隶属于授权商家或熟悉某些非接触式卡或习惯于执行某些非接触式卡交易的其他实体。然而，应当理解，执行所描述的方法不需要这种隶属关系。

[0092] 在各种实施例中，诸如购物店、杂货店、便利店或诸如此类，非接触式卡101可以在不必打开应用的情况下被轻拍到移动设备，以指示期望或意图利用奖励积分、忠诚度积分、优惠券、优惠或诸如此类中的一个或多个来覆盖一次或多次购买。因此，提供了购买背后的意图。

[0093] 在各种实施例中，一个或多个应用可以被配置为确定它是经由非接触式卡101的一个或多个轻拍手势发起的，使得发起发生在下午3:51，交易被处理，或发生在下午3:56，以便验证用户的身份。

[0094] 在各种实施例中，一个或多个应用可以被配置为响应于一个或多个轻拍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、确定成本最低的购买和/或实时地重新配置为另一动作。

[0095] 在各种实施例中，数据可以作为生物特征/手势认证在轻拍行为上收集。例如，加密安全的且不易被拦截的唯一标识符可被发送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次要信息。次要信息可以包括关于用户的个人可识别信息。在各种实施例中，次要信息可以存储在非接触式卡内。

[0096] 在各种实施例中，设备可以包括在多个个人当中拆分账单或支票以进行支付的应用。例如，每个个人可能拥有非接触式卡，并且可能是同一发行金融机构的客户，但这不是

必需的。这些个人中的每个都可以经由应用在他们的设备上收到推送通知，以拆分购买。可以使用其他非接触式卡，而不是仅接受一次卡轻拍来指示支付。在各种实施例中，具有不同金融机构的个人可能拥有非接触式卡101以提供信息以发起来自拍卡个人的一个或多个支付请求。

[0097] 在各种实施例中，本公开涉及非接触式卡的轻拍。然而，应当理解，本公开不限于轻拍，并且本公开包括其他手势(例如，卡片的挥动或其他移动)。

[0098] 图7示出了包括计算系统702的示例性计算架构700的实施例，该计算系统702可以适合于实施如前面描述的各种实施例。在各种实施例中，计算架构700可以包括或被实施为电子设备的一部分。在各种实施例中，计算架构700可以表示例如实施系统100的一个或多个组件的系统。在各种实施例中，计算系统702可以表示例如系统100的移动设备110和服务器120。实施例不限于此上下文。更一般地，计算架构700被配置为实施文本参考图1-图6描述的所有逻辑、应用、系统、方法、装置和功能。

[0099] 如本申请中所使用的，术语“系统”和“组件”以及“模块”旨在指代计算机相关实体：硬件、硬件和软件的组合、软件或执行中的软件，其示例由示例性计算架构700提供。例如，组件可以是但不限于在计算机处理器上运行的进程、计算机处理器、硬盘驱动器、(光学和/或磁存储介质的)多个存储驱动器、对象、可执行文件、执行线程、程序和/或计算机。借由说明，在服务器上运行的应用和服务器都可以是组件。一个或多个组件可以驻留在进程和/或执行线程中，并且组件可以位于一台计算机上和/或分布在两台或多台计算机之间。此外，组件可以通过各种类型的通信介质彼此通信地耦合以协调操作。协调可以涉及信息的单向或双向交换。例如，组件可以以通过通信介质传送的信号的形式来传送信息。该信息可以被实施为分配给各种信号线的信号。在这样的分配中，每个消息都是信号。然而，进一步的实施例可以可替选地采用数据消息。这样的数据消息可以跨各种连接发送。示例性连接包括并行接口、串行接口和总线接口。

[0100] 计算系统702包括各种常见的计算元件，诸如一个或多个处理器、多核处理器、协同处理器、处理电路存储器单元、芯片组、控制器、外围设备、接口、振荡器、计时设备、视频卡、音频卡、多媒体输入/输出(I/O)组件、电源等。然而，实施例不限于由计算系统702来实施。

[0101] 如图7中示出的，计算系统702包括处理器704、系统存储器706和系统总线708。处理器704可以是各种市售计算机处理器或计算机处理电路中的任何一种，包括但不限于：AMD® Athlon®、Duron®和Opteron®处理器；ARM®应用、嵌入式和安全处理器；IBM®和Motorola® DragonBall®和PowerPC®处理器；IBM和Sony®Cell处理器；Intel® Celeron®、Core®、Core(2) Duo®、Itanium®、Pentium®、Xeon®和XScale®处理器；和类似的处理器。双微处理器、多核处理器和其他多处理器架构也可以用作处理器704。处理器704可以由包含在系统存储器706中的相关联的存储器指令配置，使得当指令在处理器(例如处理器电路)704上重新执行时，处理器可以执行与图5-图7中的任何一个相关联的一个或多个操作和/或本文公开的任何其他操作或技术。

[0102] 系统总线708提供用于系统组件的接口，该系统组件包括但不限于到处理器704的系统存储器706。系统总线708可以是几种类型的总线结构中的任何一种，这些总线结构可

以使用各种市售总线架构中的任何一种进一步互连到存储器总线(具有或不具有存储器控制器)、外围总线和本地总线。接口适配器可以经由插槽架构连接到系统总线708。示例插槽架构可以包括但不限于加速图形端口(AGP)、卡总线、(扩展的)行业标准架构((E)ISA)、微通道架构(MCA)、NuBus、外围组件互连(扩展的)(PCI(X))、PCI Express、个人计算机存储器卡国际协会(PCMCIA)和诸如此类。

[0103] 系统存储器706可以包括以一个或多个较高速度的存储器单元形式的各种类型的计算机可读存储介质,诸如只读存储器(ROM)、随机存取存储器(RAM)、动态RAM(DRAM)、双数据速率DRAM(DDRAM)、同步DRAM(SDRAM)、静态RAM(SRAM)、可编程ROM(PROM)、可擦除可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)、闪速存储器(例如,一个或多个闪速阵列)、聚合物存储器(诸如铁电聚合物存储器)、双向存储器、相变或铁电存储器、硅-氧化硅-氮化硅-氧化硅-硅(SONOS)存储器、磁卡或光卡、设备的阵列(诸如独立磁盘冗余阵列(RAID)驱动器)、固态存储器设备(例如USB存储器)、固态驱动器(SSD)和适合存储信息的任何其他类型的存储介质。在图7中示出的实施例中,系统存储器706可以包括非易失性存储器710和/或易失性存储器712。基本输入/输出系统(BIOS)可以存储在非易失性存储器710中。

[0104] 计算系统702可以包括以一个或多个较低速度的存储器单元形式的各种类型的计算机可读存储介质,包括内部(或外部)硬盘驱动器(HDD)714、用于从可移动磁盘718读取或写入可移动磁盘718的磁软盘驱动器(FDD)716、以及从可移动光盘722读取或写入可移动光盘722(例如,CD-ROM或DVD)的光盘驱动器720。HDD 714、FDD 716和光盘驱动器720可以分别通过HDD接口724、FDD接口726和光盘驱动器接口728连接到系统总线708。用于外部驱动器实施方式的HDD接口724可以包括通用串行总线(USB)和IEEE 1394接口技术中的至少一项或两者。计算系统702通常被配置为实施本文参考图1-图6描述的所有逻辑、系统、方法、装置和功能。

[0105] 驱动器和相关联的计算机可读介质提供数据、数据结构、计算机可执行指令等的易失性和/或非易失性存储。例如,多个程序模块可以存储在驱动器和存储器单元710、712中,包括操作系统730、一个或多个应用732、其他程序模块734和程序数据736。在各种实施例中,一个或多个应用732、其他程序模块734和程序数据736可以包括例如系统100的各种应用和/或组件,例如操作系统112、账户应用113、认证应用114、其他应用115、访问应用116和管理应用123。

[0106] 用户可以通过一个或多个有线/无线输入设备(例如键盘738和诸如鼠标740的指点设备)将命令和信息输入到计算系统702中。其他输入设备可以包括麦克风、红外(IR)遥控器、射频(RF)遥控器、游戏垫、触笔、读卡器、加密狗、指纹读取器、手套、绘图板、操纵杆、键盘、视网膜读取器、触摸屏(例如,电容式、电阻式等)、轨迹球、触控板、传感器、手写笔和诸如此类。这些和其他输入设备通常通过耦合到系统总线708的输入设备接口742连接到处理器704,但是可以通过其他接口连接,诸如并行端口、IEEE 1394串行端口、游戏端口、USB端口、IR接口等。

[0107] 监视器744或其他类型的显示设备也经由诸如视频适配器746之类的接口连接到系统总线708。监视器744可以在计算系统702的内部或外部。除了监视器744之外,计算机典型地还包括其他外围输出设备,诸如扬声器、打印机等。

[0108] 计算系统702可以使用经由有线和/或无线通信到一台或多台远程计算机(诸如远

程计算机748)的逻辑连接在网络环境中操作。远程计算机748可以是工作站、服务器计算机、路由器、个人计算机、便携式计算机、基于微处理器的娱乐设备、对等设备或其他公共网络节点，并且典型地包括相对于计算系统702描述的许多或所有元素，尽管为简洁起见，仅示出了存储器/存储设备750。所描绘的逻辑连接包括到局域网(LAN)752和/或更大的网络(例如，广域网(WAN)754)的有线/无线连接。这样的LAN和WAN联网环境在办公室和公司中是司空见惯的，并且促进企业范围的计算机网络(诸如Intranet)，所有这些都可以连接到全球通信网络(例如Internet)。在实施例中，图1的网络130是LAN 752和WAN 754中的一个或多个。

[0109] 当在LAN联网环境中使用时，计算系统702通过有线和/或无线通信网络接口或适配器756连接到LAN 752。适配器756可以促进到LAN 752的有线和/或无线通信，这还可以包括布置在其上的无线接入点，用于与适配器756的无线功能进行通信。

[0110] 当在WAN联网环境中使用时，计算系统702可以包括调制解调器758，或者连接到WAN 754上的通信服务器，或者具有用于在WAN 754上建立通信的其他手段，诸如借由互联网。调制解调器758可以是内部或外部的，并且可以是有线和/或无线设备，其经由输入设备接口742连接到系统总线708。在网络环境中，相对于计算系统702描绘的程序模块或其部分可以存储在远程存储器/存储设备750中。应当理解，所示出的网络连接是示例性的，并且可以使用在计算机之间建立通信链路的其他手段。

[0111] 计算系统702可操作以使用IEEE 802系列标准与有线和无线设备或实体进行通信，诸如可操作地布置在无线通信中的无线设备(例如，IEEE 802.16空中调制技术)。这至少包括Wi-Fi(或Wireless Fidelity)、WiMax和Bluetooth™无线技术及其它。因此，该通信可以是与常规网络一样的预定义结构，或者仅仅是至少两个设备之间的自组织通信。Wi-Fi网络使用称为IEEE 802.11x(a、b、g、n等)的无线电技术来提供安全、可靠、快速的无线连接。Wi-Fi网络可用于将计算机彼此连接、连接到互连网和有线网络(其使用与IEEE 802.3相关的媒体和功能)。

[0112] 可以使用硬件元件、软件元件或两者的组合来实施各种实施例。硬件元件的示例可以包括处理器、微处理器、电路、电路元件(例如，晶体管、电阻器、电容器、电感器等)、集成电路、专用集成电路(ASIC)、可编程逻辑设备(PLD)、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、逻辑门、寄存器、半导体设备、芯片、微芯片、芯片组等。软件的示例可以包括软件组件、程序、应用、计算机程序、应用、系统程序、机器程序、操作系统软件、中间件、固件、软件模块、例程、子例程、功能、方法、过程、软件接口、应用接口(API)、指令集、计算代码、计算机代码、代码段、计算机代码段、字、值、符号或其任意组合。确定是否使用硬件元件和/或软件元件来实施实施例可以根据许多因素而变化，诸如期望的计算速率、功率水平、热容忍度、处理周期预算、输入数据速率、输出数据速率、存储器资源、数据总线速度和其他设计或性能限制。

[0113] 至少各种实施例的一个或多个方面可以通过存储在表示处理器内的各种逻辑的机器可读介质上的表示性指令来实施，当机器读取该表示性指令时致使机器制造逻辑以执行本文描述的技术。可以将这种表示(称为“IP核”)存储在有形的机器可读介质上，并提供给各种客户或制造设施，以加载到制造逻辑或处理器的制造机器中。例如，各种实施例可以使用机器可读介质或物品来实施，该机器可读介质或物品可以存储指令或指令集，如果该

指令或指令集由机器执行，则其可以致使机器执行根据实施例的方法和/或操作。这样的机器可以包括例如任何合适的处理平台、计算平台、计算设备、处理设备、计算系统、处理系统、计算机、处理器或诸如此类，并且可以使用硬件和/或软件的任何合适的组合来实施。机器可读介质或物品可以包括例如任何合适类型的存储器单元、存储器设备、存储器物品、存储器介质、存储设备、存储物品、存储介质和/或存储单元，例如存储器、可移动或不可移动介质、可擦除或不可擦除介质、可写或可重写介质、数字或模拟介质、硬盘、软盘、光盘只读存储器(CD-ROM)、可记录光盘(CD-R)、可重写光盘(CD-RW)、光盘、磁介质、磁光介质、可移动存储卡或磁盘、各种类型的数字多功能磁盘(DVD)、磁带、盒式磁带或诸如此类。指令可以包括任何适当类型的代码，诸如源代码、编译代码、解释代码、可执行代码、静态代码、动态代码、加密代码和诸如此类，这些代码使用任何适当的高级、低级、面向对象、可视化、编译和/或解释的编程语言实施。

[0114] 为了说明和描述的目的，已经呈现了示例实施例的前述描述。并不旨在穷举本公开或将本公开限制为所公开的精确形式。根据本公开，许多修改和变化是可能的。意图是，本公开的范围不由该详细描述限制，而是由在此所附权利要求限制。要求本申请的优先权的未来提交的申请可以以不同的方式要求公开的主题，并且通常可以包括如本文以各种方式公开或以其他方式证明的一个或多个限制的任何集合。

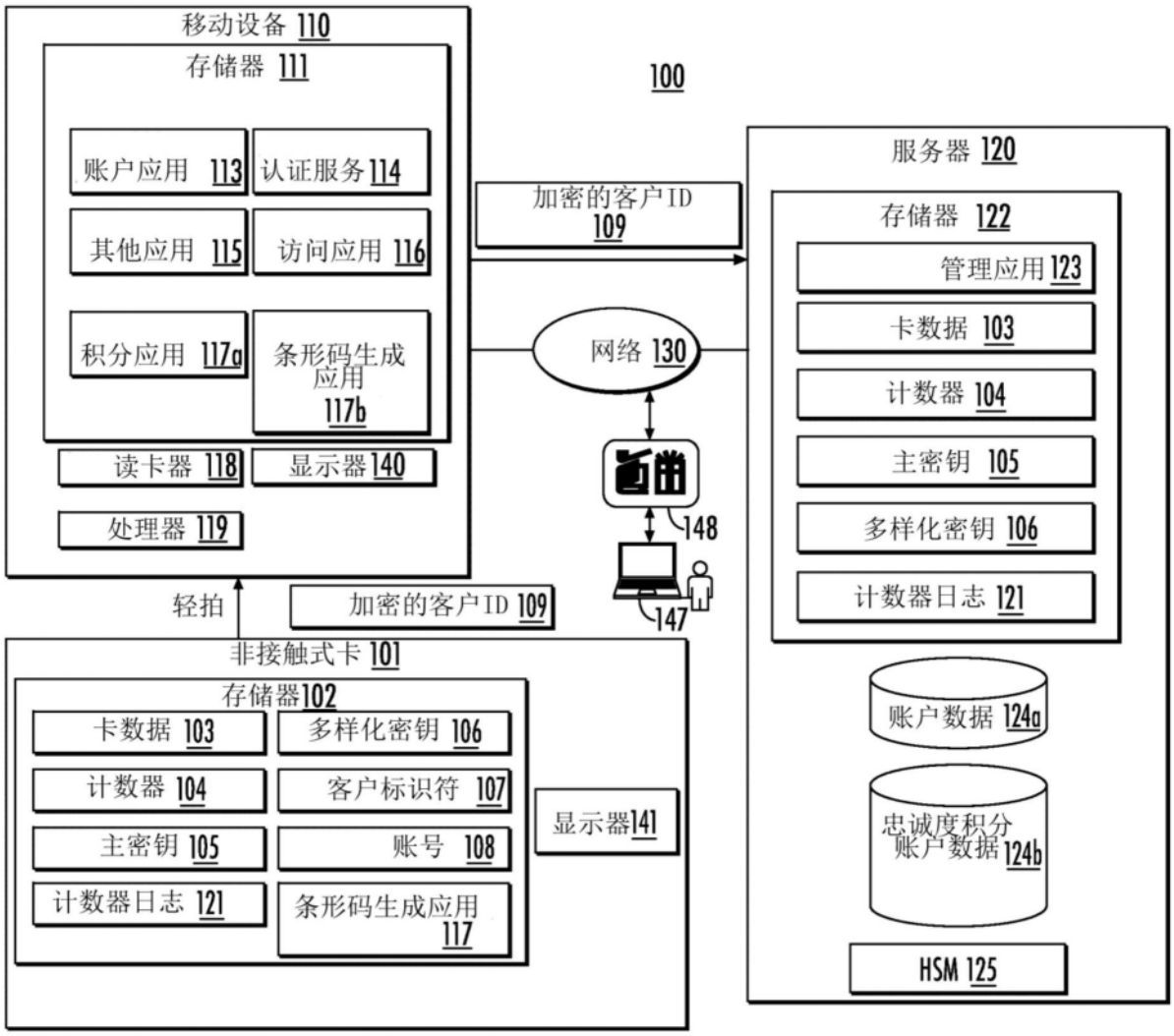

移动设备 110
存储器 111
账户应用 113
认证服务 114
其他应用 115
访问应用 116
积分应用 117a
条形码生成应用 117b
读卡器 118
显示器 140
处理器 119
100
加密的客户ID 109
网络 130
服务器 120
存储器 122
管理应用 123
卡数据 103
计数器 104
主密钥 105
多样化密钥 106
计数器日志 121
账户数据 124a
忠诚度积分账户数据 124b
HSM 125
148
147
轻拍
加密的客户ID 109
非接触式卡 101
存储器102
卡数据 103
多样化密钥 106
计数器 104
客户标识符 107
主密钥 105
账号 108
计数器日志 121
条形码生成应用 117
显示器141

图1

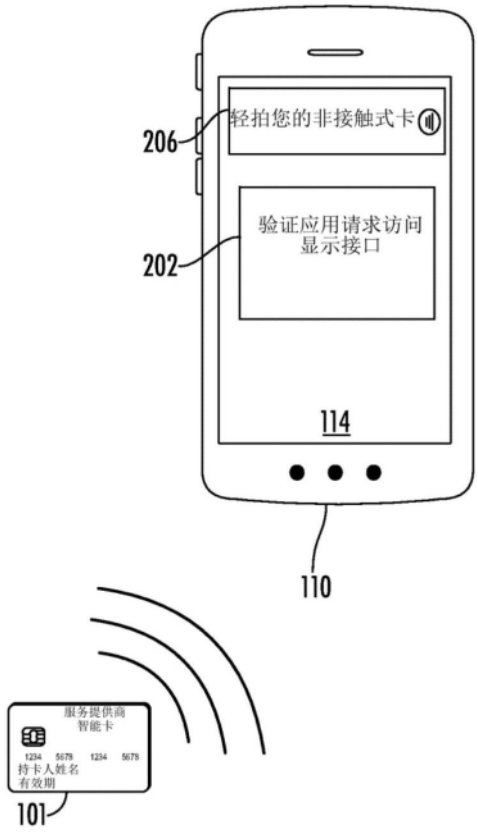

轻拍您的非接触式卡
206
验证应用请求访问
显示接口
202
114
110
服务提供商
智能卡
1234 5678 1234 5678
持卡人姓名
有效期
101

图2

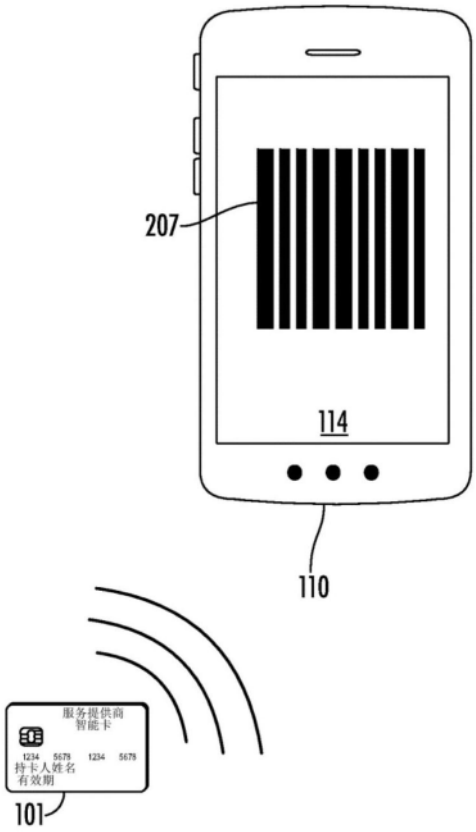

207
114
110
服务提供商
智能卡
1234 5678 1234 5678
持卡人姓名
有效期
101

图3

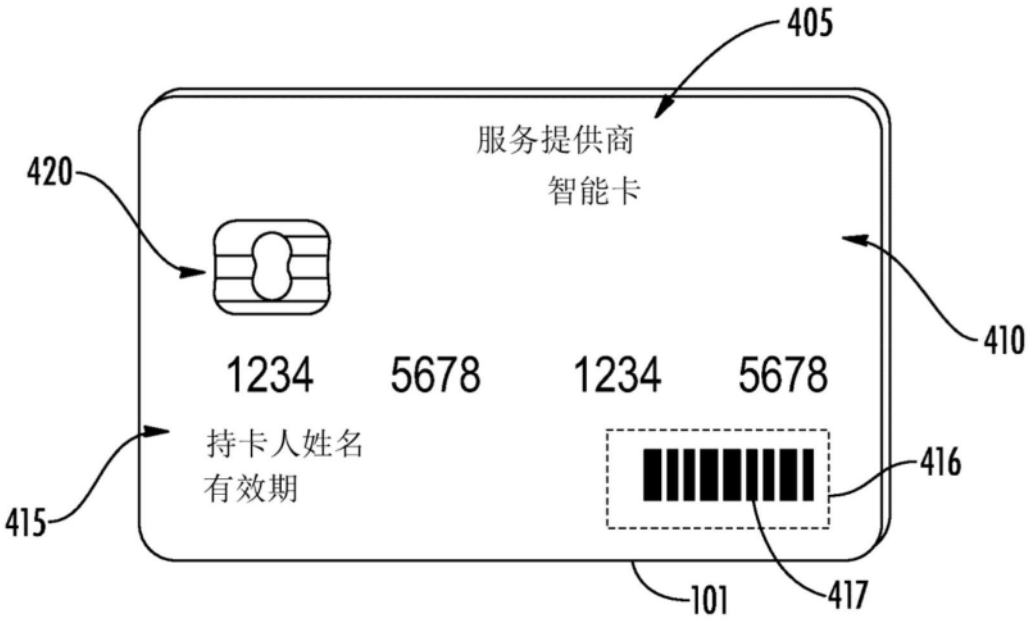

405
服务提供商
智能卡
420
410
1234 5678 1234 5678
持卡人姓名
有效期
415
416
417
101

图4A

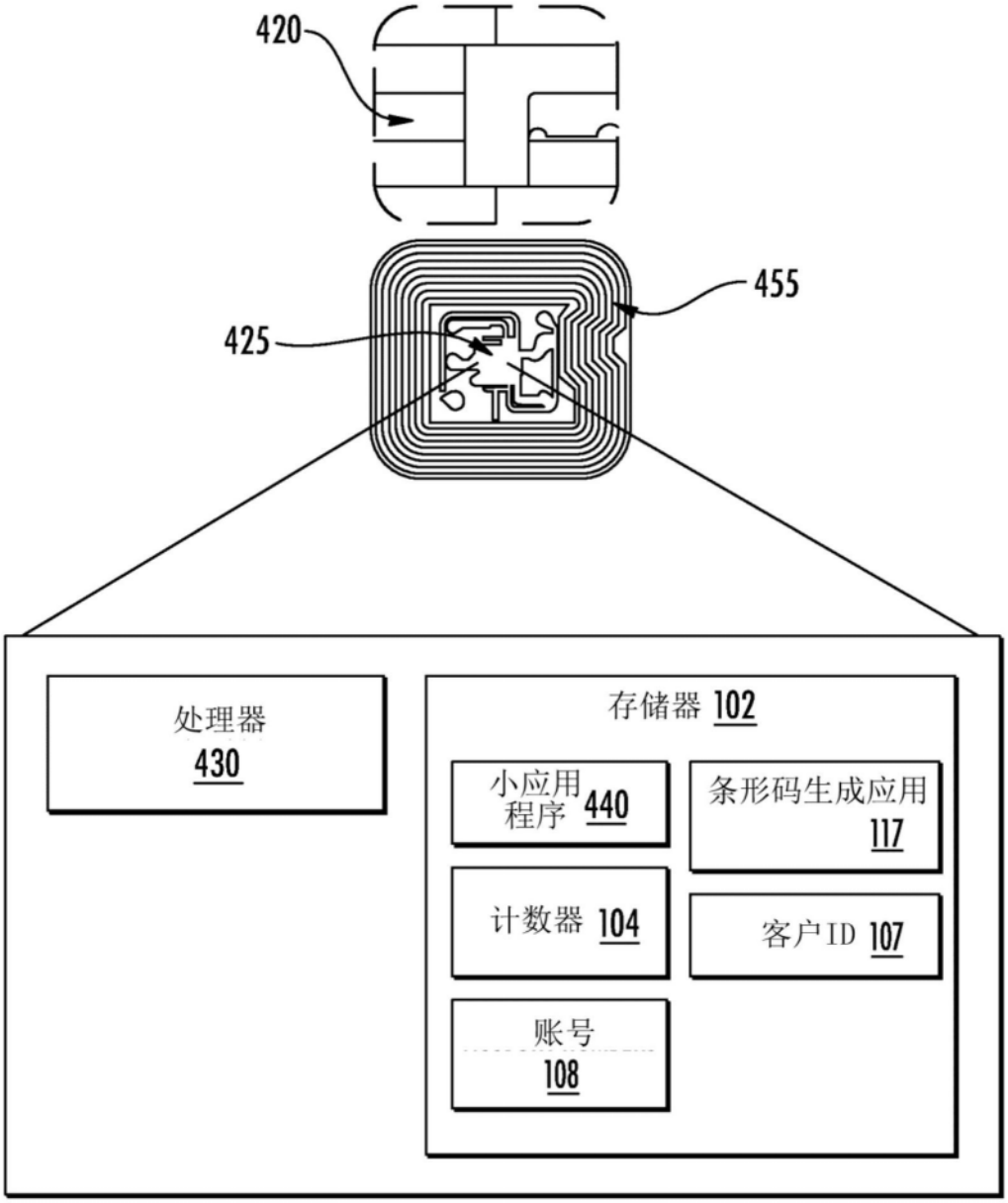

420
455
425
处理器
430
存储器 102
小应用程序 440
条形码生成应用
117
计数器 104
客户ID 107
账号
108

图4B

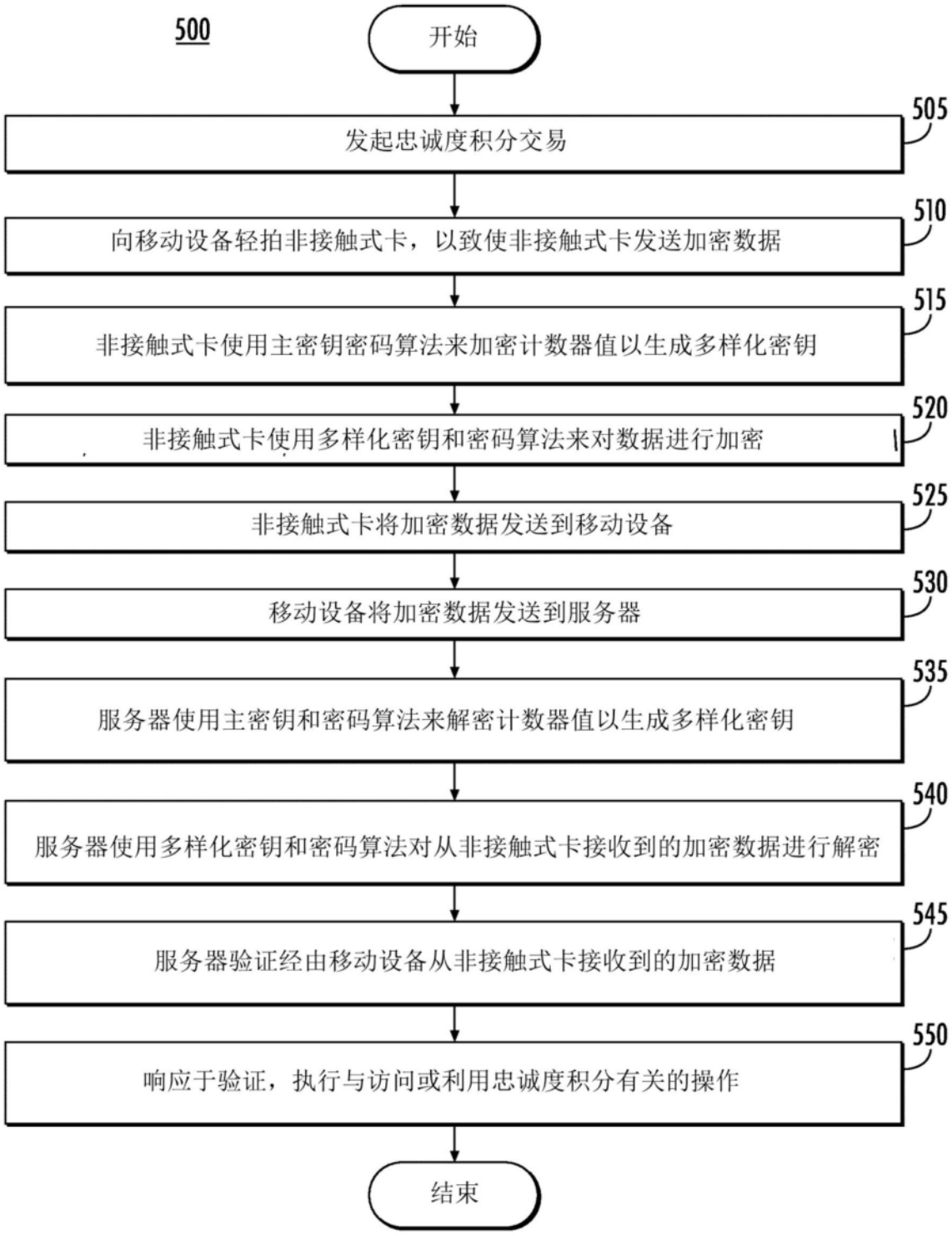

500
开始
505
发起忠诚度积分交易
510
向移动设备轻拍非接触式卡，以致使非接触式卡发送加密数据
515
非接触式卡使用主密钥密码算法来加密计数器值以生成多样化密钥
520
非接触式卡使用多样化密钥和密码算法来对数据进行加密
525
非接触式卡将加密数据发送到移动设备
530
移动设备将加密数据发送到服务器
535
服务器使用主密钥和密码算法来解密计数器值以生成多样化密钥
540
服务器使用多样化密钥和密码算法对从非接触式卡接收到的加密数据进行解密
545
服务器验证经由移动设备从非接触式卡接收到的加密数据
550
响应于验证，执行与访问或利用忠诚度积分有关的操作
结束

图5

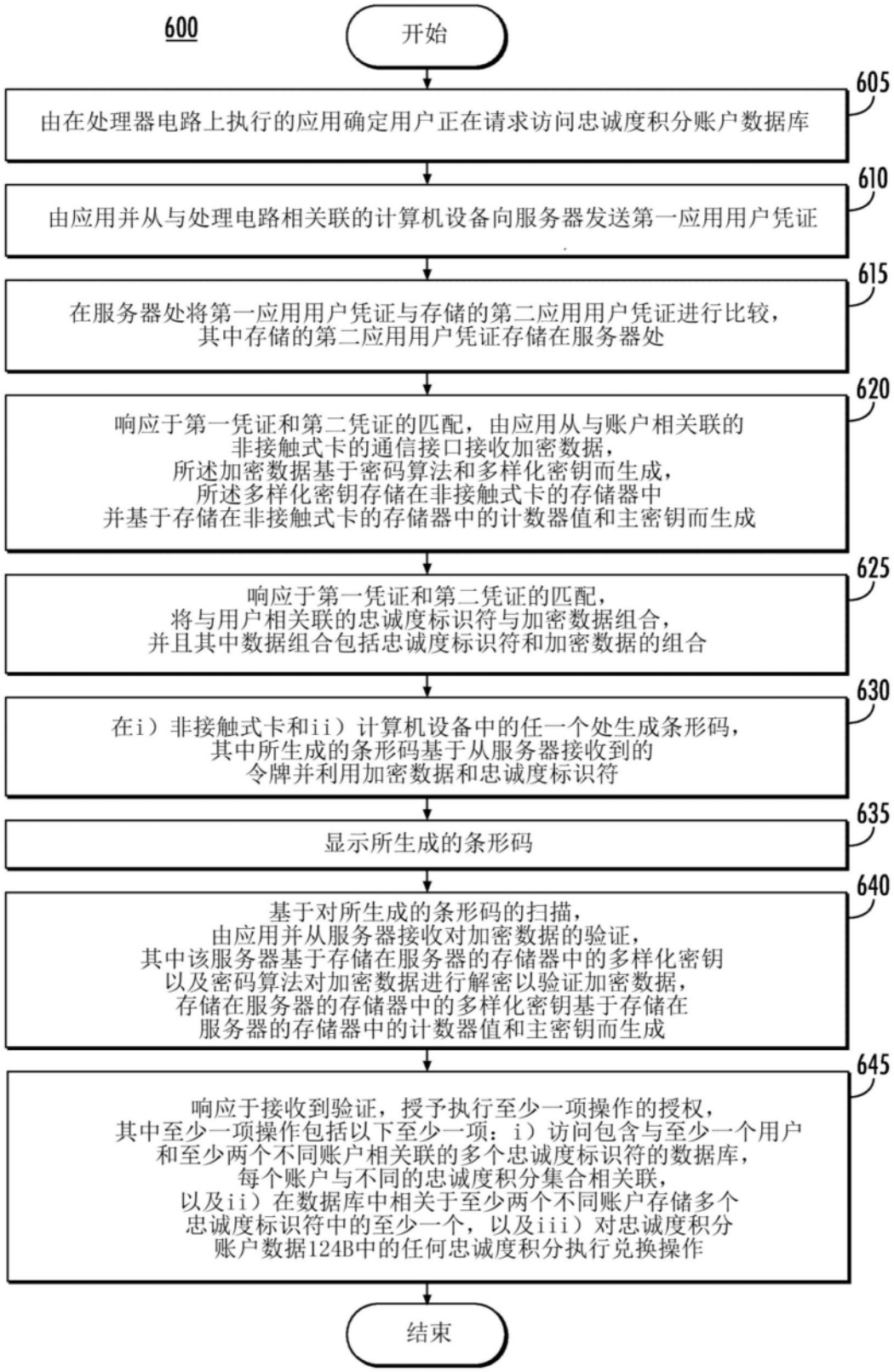

600
开始
605
由在处理器电路上执行的应用确定用户正在请求访问忠诚度积分账户数据库
610
由应用并从与处理电路相关联的计算机设备向服务器发送第一应用用户凭证
615
在服务器处将第一应用用户凭证与存储的第二应用用户凭证进行比较，
其中存储的第二应用用户凭证存储在服务器处
620
响应于第一凭证和第二凭证的匹配，由应用从与账户相关联的
非接触式卡的通信接口接收加密数据，
所述加密数据基于密码算法和多样化密钥而生成，
所述多样化密钥存储在非接触式卡的存储器中
并基于存储在非接触式卡的存储器中的计数器值和主密钥而生成
625
响应于第一凭证和第二凭证的匹配，
将与用户相关联的忠诚度标识符与加密数据组合，
并且其中数据组合包括忠诚度标识符和加密数据的组合
630
在i）非接触式卡和ii）计算机设备中的任一个处生成条形码，
其中所生成的条形码基于从服务器接收到的
令牌并利用加密数据和忠诚度标识符
635
显示所生成的条形码
640
基于对所生成的条形码的扫描，
由应用并从服务器接收对加密数据的验证，
其中该服务器基于存储在服务器的存储器中的多样化密钥
以及密码算法对加密数据进行解密以验证加密数据，
存储在服务器的存储器中的多样化密钥基于存储在
服务器的存储器中的计数器值和主密钥而生成
645
响应于接收到验证，授予执行至少一项操作的授权，
其中至少一项操作包括以下至少一项：i）访问包含与至少一个用户
和至少两个不同账户相关联的多个忠诚度标识符的数据库，
每个账户与不同的忠诚度积分集合相关联，
以及ii）在数据库中相关于至少两个不同账户存储多个
忠诚度标识符中的至少一个，以及iii）对忠诚度积分
账户数据124B中的任何忠诚度积分执行兑换操作
结束

图6

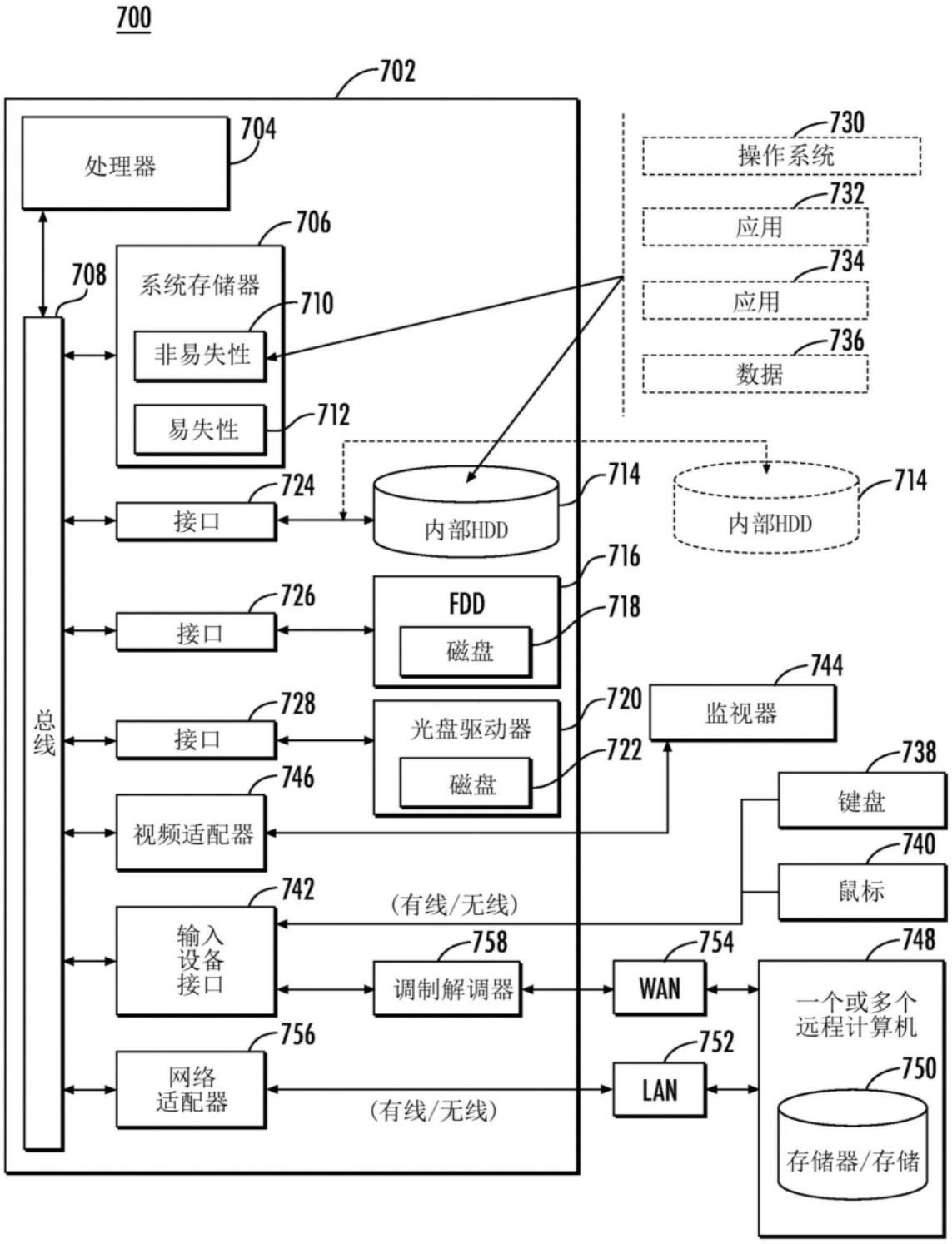

700
702
处理器
704
706
系统存储器
708
710
非易失性
712
易失性
730
操作系统
732
应用
734
应用
736
数据
724
接口
714
内部HDD
714
内部HDD
716
FDD
718
磁盘
726
接口
744
监视器
720
光盘驱动器
722
磁盘
728
接口
738
键盘
746
视频适配器
740
鼠标
742
输入
设备
接口
(有线/无线)
758
调制解调器
754
WAN
748
一个或多个
远程计算机
750
存储器/存储
752
LAN
756
网络
适配器
(有线/无线)
总线

图7