(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118020095 A
(43)申请公布日 2024.05.10

(21)申请号 202280062943.X
(22)申请日 2022.09.16
(30)优先权数据
17/477,244 2021.09.16 US
(85)PCT国际申请进入国家阶段日
2024.03.18
(86)PCT国际申请的申请数据
PCT/US2022/043780 2022.09.16
(87)PCT国际申请的公布数据
WO2023/043987 EN 2023.03.23
(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 泰勒·梅曼 内加尔·卡尔巴西 萨利克·沙阿 马修·霍顿 阿卜杜卡迪尔·穆罕默德·本克蕾拉 菲比·阿特金斯 伊姆伦·乔哈尔
(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 胡彬
(51)Int.Cl.
G07C 9/00(2020.01)
G07C 9/27(2020.01)
G06Q 20/32(2012.01)
G06Q 20/34(2012.01)
G06Q 20/38(2012.01)

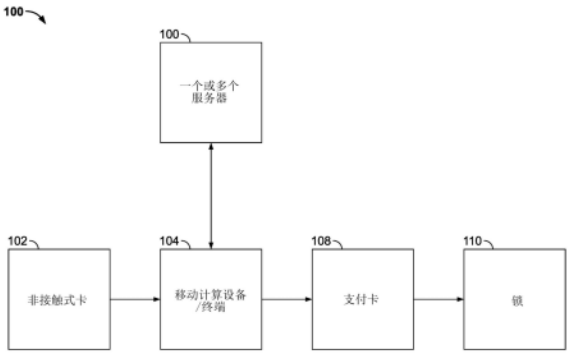
权利要求书2页 说明书9页 附图16页

(54)发明名称

使用支付卡对锁进行解锁

(57)摘要

示例性实施例可以在支付卡上提供用于解锁对如用户房间、安全位置、员工位置的门、行李箱、壁橱或其他锁定的位置或物品之类的某个位置的进入的密钥。支付卡的示例包括但不限于信用卡、借记卡、智能卡、员工识别卡等。可以将充当数字密钥的安全令牌上传到支付卡。然后可以将支付卡放在锁的无线读取器附近。无线读取器获得安全令牌并提取内容。如果内容正确,则锁将解锁。否则,锁将保持锁定。



CN 118020095 A

1.一种方法,所述方法包括:

经由无线通信协议接收来自非接触式卡的身份信息和证书;

基于所述身份信息和所述证书,确认一方的身份;以及

在确认所述身份之后,转发支付卡的代码,所述代码用作对锁进行解锁的数字密钥。

2.根据权利要求1所述的方法,其中,所述支付卡是具有针对所述无线通信协议的能力的智能卡或信用卡之一。

3.根据权利要求1所述的方法,其中,所述无线通信协议是近场通信(NFC)。

4.根据权利要求1所述的方法,其中,所述锁用于酒店房间。

5.根据权利要求4所述的方法,还包括,存储针对所述代码的房间号码,并将所述一方的身份存储到所述支付卡上。

6.根据权利要求1所述的方法,还包括,从计算设备接收所述代码。

7.根据权利要求1所述的方法,其中,所述身份信息和证书是在加密包中接收的。

8.一种方法,所述方法包括:

在便携式计算设备处经由无线通信协议从非接触式卡接收一方的证书和身份信息;

将所述证书和所述身份信息转发给认证机构;

接收对所述一方的身份的确认;以及

在确认所述一方的身份后,经由无线通信协议将代码转发给支付卡,所述代码用作对锁进行解锁的数字密钥。

9.根据权利要求8所述的方法,其中,所述便携式计算设备是智能手机、平板计算设备、智能手表或可穿戴设备之一。

10.根据权利要求8所述的方法,其中,所述无线通信协议是近场通信(NFC)协议。

11.根据权利要求8所述的方法,其中,所述锁用于酒店房间。

12.根据权利要求8所述的方法,其中,所述身份信息和证书是在加密包中接收的。

13.根据权利要求8所述的方法,其中,所述转发和接收确认是经由联网连接进行的。

14.根据权利要求13所述的方法,其中,所述网络连接是无线网络连接、蜂窝网络连接或有线网络连接之一。

15.一种智能卡,所述智能卡包括:

存储器,所述存储器用于存储:

关于用户的身份信息;

用于利用所述智能卡来对锁进行解锁的密钥代码;

用于利用所述密钥代码来解锁所述锁的计算机程序指令;

用于执行无线支付的计算机程序指令;

处理器,所述处理器用于执行被存储在所述存储器中的用于解锁所述锁的所述计算机程序指令和用于执行被存储在所述存储器中的用于执行无线支付的所述计算程序指令;以及

硬件,所述硬件使所述智能卡能够进行无线通信。

16.根据权利要求15所述的智能卡,其中,所述硬件实现近场通信(NFC)无线通信。

17.根据权利要求15所述的智能卡,其中,所述锁是用于门的锁。

18.根据权利要求17所述的智能卡,其中,所述锁用于酒店房间锁。

19.根据权利要求15所述的智能卡,其中,所述存储器还存储用于从设备下载所述密钥代码的计算机程序指令。

20.根据权利要求19所述的智能卡,其中,所述设备是智能手机。

使用支付卡对锁进行解锁

[0001] 相关申请的交叉引用

[0002] 本申请要求于2021年9月16日提交的题为“USE OF APAYMENT CARD TO UNLOCK ALOCK(使用支付卡解锁)”的美国专利申请序列号17/477244的优先权。前述申请的内容通过引用整体并入本文。

背景技术

[0003] 诸如酒店之类的住宿场所为其客人提供进入房间的钥匙。该钥匙通常是带有磁条的塑料钥匙卡或带有射频识别(RFID)标签的塑料钥匙卡。对于具有磁条的塑料钥匙卡,酒店职员在登记入住时在将塑料钥匙卡交给客人之前将关于客人的信息编码到卡的磁条上。例如,客人的标识符、有效日期/时间、到期日期/时间和房间号可以被编码到磁条上。当客人希望使用塑料钥匙卡时,客人将具有磁条的塑料钥匙卡的边缘穿过集成在客人房间门中的磁卡读取器。磁卡读取器从磁条上读取信息,信息由锁进行分析。如果该信息是用于对门进行解锁的正确信息,则门锁被解锁,以便客人可以进入房间。如果该信息不适合对门进行解锁,则拒绝进入,并且门保持锁定。

[0004] 带有RFID芯片的塑料钥匙卡的操作有些不同。酒店职员在登记入住时,在给客人塑料钥匙卡之前将客人信息编码到塑料钥匙卡的RFID芯片中。当客人希望使用塑料钥匙卡时,客人抵靠被集成到客房门中的RFID读取器放置塑料钥匙卡。RFID读取器从塑料钥匙卡中的RFID芯片无线读取信息。如果该信息是用于对门进行解锁的正确信息,则门锁被解锁,以便客人可以进入房间。如果该信息不适合对门进行解锁,则拒绝进入,并且门保持锁定。

[0005] 这种塑料钥匙卡也可以被用于其他用途。例如,雇主可以给雇员这种塑料钥匙卡,让他们进入雇主的办公场所或进入安全区域。例如,公司中的安全实验室可能需要钥匙卡来进入。塑料钥匙卡可以被用于进入被认为需要锁的其他位置。这种塑料钥匙卡甚至可以与诸如行李箱、保险箱等之类的被锁定的物品一起使用。

[0006] 使用这些种类的塑料钥匙卡存在缺点。例如,这些种类的塑料钥匙卡不是特别安全。磁条或RFID标签上的信息对于具有磁卡读取器或RFID读取器的一方来说是容易进入的。此外,这种塑料钥匙卡很容易放错地方。因此,塑料钥匙卡可能会落入错误人之手,或者用户可能无法进入锁定的位置或物品,直到获得新的卡。此外,用户不得不跟踪另外的卡是不方便的。最后,对于住宿业主来说,不得不购买塑料钥匙卡的成本很高,特别是考虑到许多钥匙卡已经丢失或毁坏的情况下。

发明内容

[0007] 根据一个发明方面,一种方法包括:经由无线通信协议接收源自非接触式卡的身份信息和证书。基于身份信息和证书,确认一方的身份。在身份确认之后,代码被转发用于支付卡。该代码用作对锁进行解锁的数字密钥。

[0008] 支付卡可以是具有用于无线通信协议功能的智能卡或信用卡。该无线通信协议可以是近场通信(NFC)协议。锁可以用于酒店房间。该方法还可以包括存储用于该代码的房间

号以及将该方的身份存储到支付卡上。该方法还可以包括从计算设备接收代码。身份信息和证书可在加密包中被接收。

[0009] 根据另一个发明方面,一种方法包括:经由无线通信协议在便携式计算设备处从非接触式卡接收一方的证书和身份信息。证书和身份信息被转发给认证机构。接收对该方身份的确认。在确认了该方的身份之后,经由无线通信协议将代码转发到支付卡。该代码用作对锁进行解锁的数字密钥。

[0010] 便携式计算设备可以是智能手机、平板计算设备、智能手表或可穿戴设备。无线通信协议可以是近场通信(NFC)协议。该锁可以用于酒店房间。身份信息和证书可在加密包中被接收。转发和接收确认可以经由联网连接。该联网连接可以是无线网络连接、蜂窝网络连接或有线网络连接。

[0011] 根据另一个发明方面,一种智能卡包括用于存储关于用户的身份信息的存储器、用于用智能卡对锁进行解锁的密钥代码、用于使用密钥代码对锁进行解锁的计算机程序指令以及用于执行无线支付的计算机程序指令。该智能卡还包括用于执行存储在存储器中的用于对锁进行解锁的计算机程序指令和存储在存储器中的用于执行无线支付的计算机程序指令的处理器。该智能卡还包括使该智能卡能够进行无线通信的硬件。

[0012] 硬件可以实现近场通信(NFC)无线通信。该锁可以是门锁。该锁可以是用于酒店房间的锁。存储器还可以存储用于从设备下载密钥代码的计算机程序指令。该设备可以是智能手机。

附图说明

[0013] 图1描绘了示例性实施例的示出性环境的示例。

[0014] 图2描绘了可以被执行以将数字密钥传送至支付卡的示出性步骤的流程图。

[0015] 图3描绘了在这种示例性实施例中可执行的示出性步骤的流程图。

[0016] 图4描绘了可适用于示例性实施例的示出性计算环境。

[0017] 图5描绘了在执行这种交互时各种组件的活动的图示。

[0018] 图6A描绘了适用于示例性实施例的示例性非接触式卡的正面。

[0019] 图6B示出了图6A的非接触式卡的组件。

[0020] 图7显示了示出非接触式卡和计算设备之间交互的组件图。

[0021] 图8A显示了描绘在示例性实施例中如何使用密码哈希函数的框图。

[0022] 图8B显示了在示例性实施例中可以被哈希的可能类型的输入的图。

[0023] 图9显示了描绘根据示例性实施例的安全包加密的框图。

[0024] 图10提供了在示例性实施例中认证客人身份时可执行的示出性步骤的流程图。

[0025] 图11描绘了示例性实施例中被存储为认证服务的一部分的的某些项目。

[0026] 图12描绘了示例性实施例中对发起方进行认证所执行的步骤流程图。

[0027] 图13描绘了示例性实施例中适用于我们的支付卡的框图。

[0028] 图14描绘了在示例性实施例中可以被执行以使用支付卡进行支付的示出性步骤的流程图。

具体实施方式

[0029] 示例性实施例可以提供密钥,用于解锁对用户支付卡上的位置或物品的进入。支付卡的示例包括但不限于信用卡、借记卡、智能卡、具有支付能力的员工识别卡。充当数字密钥的安全令牌可以被上传到用户的支付卡。例如,在密钥是用于住宿房间的情况下,客人可以登录网站或访问住宿应用,并通过提供个人信息和支付信息来登记入住。在某些情况下,客人然后可以进入自助服务终端,其使用充当数字密钥的安全令牌对支付卡进行编码。在其他情况下,用户可以利用移动计算设备(诸如智能手机、平板电脑、智能手表或可穿戴设备)的能力,使用应用或网站来下载安全令牌,然后将安全令牌传送给支付卡。然后可以将支付卡放在锁处的无线读取器附近。无线读取器获得安全令牌并提取内容。如果内容对于解锁所述锁是正确的,则锁被解锁。否则,锁保持锁定。

[0030] 在示例性实施例中使用的合适的无线通信协议是近场通信(NFC)协议或其他无线通信协议。因此,移动计算设备或终端和支付卡可以具有NFC功能。在使用自助服务终端的情况下,终端可以经由NFC将安全令牌传送给支付卡。类似地,移动计算设备可以经由NFC将安全令牌传送给支付卡。支付卡还可以经由NFC将安全令牌传送给锁处的无线读取器。

[0031] 示例性实施例具有无需另外的塑料卡即可进入锁定位置或物品的优势。这消除了用户跟踪另外的塑料卡的需要。同样,这也有利于减少塑料钥匙卡发行者的费用,因为他们不再需要购买同样多的塑料钥匙卡,因为许多用户会选择将密钥编码到他们的支付卡中。在示例性实施例中使用的支付卡上的数字密钥不太可能被用户丢失,因为人们倾向于密切关注他们的支付卡,而用户通常不会密切关注他们的传统塑料钥匙卡,因为他们可以容易地获得新的塑料钥匙卡。示例性实施例中使用的密钥是安全的,因为充当数字密钥的每个安全令牌都是加密的,并且在没有解密安全包所需的一个或多个解密密钥的情况下是不可进入的。

[0032] 图1描绘了示例性实施例的示出性环境100的示例。示出性环境100包括非接触式卡102。非接触式卡102可以支持NFC协议并且经由NFC协议与其他设备进行通信。例如,当与移动计算设备或终端104足够接近(例如,在1.5英寸内)时,非接触式卡102可以与移动计算设备或终端104进行无线通信。下面提供了示出性非接触式卡102的细节。移动计算设备104可以是例如智能手机、平板计算设备、智能手表、可穿戴计算设备或移动的且具有本文所述的必要功能的其他移动计算设备。终端104可以是与一个或多个服务器106接口连接的具有NFC功能的终端或计算机系统。移动计算设备/终端104可以经由网络连接与一个或多个服务器106通信,该网络连接可以是无线的、有线的或其组合。一个或多个服务器106可以是web服务器,可以位于云上,或者可以通过局域网(LAN)、广域网(WAN)(诸如互联网)或经由它们的组合来访问。

[0033] 移动计算设备/终端104可以与用户的支付卡108进行通信。例如,如上所述,移动计算设备/终端104可以向支付卡108提供充当数字密钥的安全包。支付卡108可以与锁110交互,如下所述以对门进行解锁。

[0034] 支付卡上数字密钥的一种用途是解锁住宿场所(如汽车旅馆、酒店、客栈或出租屋)的门。在示例性实施例中,对于用户要使用支付卡上的数字密钥来解锁他们的住宿房间或出租屋的情况,可以使用至少两种方法来将数字密钥获取到支付卡108上。在第一种方法中,移动计算设备104将数字密钥传送给支付卡108。图2描绘了可以被执行以将数字密钥从

其传送给支付卡108的示出性步骤的流程图。最初,在202处,用户可以使用移动计算设备104来访问住宿的应用(诸如连锁酒店或出租房机构的应用)或访问住宿的网站进行登记入住。网站可以在一个或多个服务器106上运行,或者应用可以与一个或多个服务器106通信。为了登记入住,用户可能被要求提供诸如姓名、地址和电话号码之类的身份信息,并提供诸如信用卡号、借记卡号等之类的支付信息。在某些情况下,如下所述,可能会提示用户将非接触式卡102轻叩到移动计算设备104以认证身份。一旦客人成功地登记入住,就可以提示用户生成数字密钥以存储在支付卡108上的选项(参见204)。在用户选择生成数字密钥以存储在支付卡108上的选项的情况下,移动计算设备104将充当数字密钥的安全令牌传送给支付卡108(参见206)。如下所述,安全令牌可以从一个或多个服务器106被下载到移动计算设备108,然后被传送给支付卡108。

[0035] 用于住宿的另一种可替选方案是在住宿前台或一体机处从自助服务终端下载密钥。图3描绘了可以在这种示例性实施例中执行的示出性步骤的流程图300。最初,诸如如上所述,用户使用网站或应用或通过向前台或一体机提供所需的个人和支付信息来登记入住(参见302)。作为登记入住的一部分,用户可能被要求确认她/他的身份(参见304)。这可能需要出示适当的身份证明、通过一体机提供个人信息或使用非接触式卡102来确认身份。一旦用户的身份被确认,充当数字密钥的安全令牌可以经由终端104被上传给支付卡108(参见306)。终端104可以例如位于住宿场所的前台。在一些示例性实施例中,终端104具有NFC功能,并且使用NFC将安全令牌传送给用户的支付卡108,该支付卡108也具有NFC功能。

[0036] 图4比图1更详细地描绘了可适用于示例性实施例的示出性计算环境400。客人418可以访问移动计算设备/终端402。移动计算设备/终端402包括处理器408,该处理器408诸如中央处理单元(CPU)、图形处理单元(GPU)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他处理单元。处理器408可以执行指令,诸如在计算机程序(如应用414)中找到的指令,以执行本文所描述的功能。移动计算设备/终端402可以包括存储设备410,该存储设备410可以包括随机存取存储器(RAM)、只读存储器(ROM)、固态存储器、光盘存储设备、磁盘存储设备或用于存储数据和/或指令的其他各种存储器或存储设备。存储设备410可以包括保持处理器可执行指令的非瞬态计算机可读存储介质。该存储设备410可以存储应用414。该应用414可以提供如本文所描述的用于登记入住并将安全令牌传送给支付卡108的功能。该应用414还可以使得能够使用非接触式卡102来认证用户418的身份。在一些示例性实施例中,该应用414可以是网络浏览器。

[0037] 移动计算设备/终端402可以包括用于提供NFC能力的集成电路(IC)416。NFC IC 416可以包括用于参与NFC通信的NFC收发器和环形天线。非接触式卡420可以经由NFC与移动计算设备/终端402通信,诸如当非接触式卡片被轻叩在移动计算设备或终端402上时。非接触式卡420可以包括用于安全通信的计数器415。支付卡403可以经由NFC或另一无线协议与移动计算设备/终端无线通信。

[0038] 移动计算设备/终端402可以与服务器404和/或服务器430进行通信。在一些示例性实施例中,移动计算设备/终端403仅与服务器430直接通信。这些服务器404和430可以经由一个或多个网络406与移动计算设备/终端402连接。一个或多个网络406可以包括广域网(如互联网和/或蜂窝电话网络),以及诸如公司网络、以太网、WiFi网络等或内部网之类的局域网。服务器404可以包括一个或多个处理器422。该一个或多个处理器422可以采取与针

对一个或多个处理器408所描述的那些类似的许多形式。服务器404可以包括存储设备424，该存储设备424可以包括上面针对移动计算设备/终端402的存储设备410所描述的存储设备或存储器的形式。该存储设备424可以存储计算机编程指令440。在一些示例性实施例中，这些计算机编程指令440用于用户418可以访问的网站，以登记入住住宿并获得如上所描述的数字密钥。计算机编程指令也可以是与应用414交互以便于登记入住和获得数字密钥的服务器代码。服务器430可以在需要对用户的身份进行认证时使用，并且调用服务器430可以由服务器404调用以提供身份认证。服务器可以包括执行用于认证用户身份的认证服务432的一个或多个处理器433。服务器404和430可以访问诸如数据库等之类的数据434。

[0039] 如上所述，将支付卡用作住宿房间的数字支付卡的一种选项是用户使用非接触式卡来证明身份，并经由移动计算设备将数字密钥传送给支付卡。图5描绘了执行这种交互的各种组件的活动的图示。将参考图4中组件的描绘来描述图5。最初，用户418在移动计算设备402上打开应用414(参见502)。该应用可以是住宿场所的应用，或者是能够访问住宿场所的网站的网络浏览器。使用应用414，用户418与服务器440上包含计算机程序指令440的程序通信，并请求登记入住(参见503)。作为登记入住过程的一部分，应用414提示用户418将非接触式卡420轻叩到移动计算设备402(参见504)。非接触式卡420被轻叩，并且经由NFC以安全包的形式向移动计算设备402发送身份信息(参见506)。来自非接触式卡420的安全包的形成和内容将在下面更详细地描述。移动计算设备402向服务器404发送包含身份信息的安全包(参见508)。服务器430可以将该安全包转发给服务器430上的认证服务432。服务器430上的认证服务432然后对用户的身份进行认证(参见510)。一旦用户被认证，用户就可以诸如由服务器404登记入住。在示例性实施例中，服务器404可以要求服务器430执行用户身份的认证，并将结果通知服务器404。在没有成功认证的情况下，可以将拒绝发送到服务器404，并转发回移动计算设备402上的应用414。在认证成功的情况下，用户被登记入住，并且成功的登记入住由服务器404报告给移动计算设备402上的应用414(参见512)。

[0040] 然后，移动计算设备402上的应用414可以提示用户使用支付卡作为密钥(参见514)。用户可以肯定地响应用户希望使用支付卡作为密钥(参见516)。如果用户未选择此选项，则流程将暂停。否则，应用414然后可以向服务器404请求密钥(参见518)。服务器上的计算机程序指令440生成作为数字密钥的安全包。安全包的密钥代码和其他信息然后可以从服务器404被发送到移动计算设备402上的应用414(参见520)。应用414提示用户418将支付卡轻叩到移动计算设备402。支付卡被轻叩到移动计算设备403(参见524)。作为轻叩的结果，移动计算设备上的应用414可以经由NFC将保持数字密钥代码的安全包传送给支付卡。具体而言，移动计算设备402发送密钥代码(参见526)，并且密钥代码被存储在支付卡上(参见528)。

[0041] 现在讨论将集中在非接触式卡的使用细节上。图6A示出了非接触式卡600正面的示例，该非接触式卡600可由诸如商家、金融机构等之类的服务提供商606发行。在一些示例性实施例中，非接触式卡600可以包括识别卡。在某些情况下，卡600可以包括双接口非接触式支付卡。非接触式卡600可以包括基板608，该基板608可以包括由塑料、金属和其他材料构成的单层或层压层。示例性的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600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600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600可以具有不同的特性。

[0042] 非接触式卡600还可以包括被显示在卡的正面和/或背面的识别信息604以及接触垫602。接触垫602可以被配置为与另一通信设备建立联系,所述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。非接触式卡600还可以包括处理电路、天线和图6A中未示出的其他组件。这些组件可以位于接触垫602的后面或基板608上的其他地方。非接触式卡600还可以包括位于卡背面的磁条或磁带(图6A中未示出)。

[0043] 如图6B所示,图5A的接触垫602可以包括用于存储和处理信息的处理电路610,该处理电路610包括微处理器614和存储器616。应当理解,处理电路610可以包含执行本文所述功能所必需的附加组件,该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。

[0044] 存储器616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600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出厂后的某个时间点被编程。一旦对存储器进行了编程,它可能不会被重写,但可能会被多次读取。读/写存储器可以在出厂后进行多次编程和重新编程。它也可以被多次读取。

[0045] 存储器616可以被配置为存储一个或多个小程序618、一个或多个计数器620和唯一的客户标识符622。一个或多个小程序618可以包括被配置为在一个或更多个非接触式卡(诸如Java卡小程序)上执行的一个或多个软件应用。然而,应当理解,小程序618不限于Java卡小程序,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620可以包括足以存储整数的数字计数器。客户标识符622可以包括被分配给非接触式卡600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。在一些示例中,客户标识符622可以识别客户和被分配给该客户的账户,并且还可以识别与该客户的帐户相关联的非接触式卡。

[0046] 在一些示例中,非接触式卡600可以包括一个或多个天线612。该一个或多个天线612可以被放置在非接触式卡600内和接触垫602的处理电路610周围。例如,该一个或多个天线612可以与处理电路610集成在一起,并且该一个或多个天线612可以与外部升压线圈一起使用。作为另一示例,该一个或多个天线612可以在接触垫602和处理电路610的外部。

[0047] 在一个实施例中,非接触式卡600的线圈可作为空心变压器的次级线圈。终端可通过切断电源或调幅与非接触式卡600通信。非接触式卡600可以使用非接触式卡的电源连接中的间隙来推断从终端发送的数据,这可以通过一个或多个电容器来功能性地维持。非接触式卡600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回通信。通过干扰可以检测到终端线圈中的负载调制。

[0048] 如上所述,非接触式卡600可构建在可在智能卡或其他具有有限内存的设备(诸如JavaCard)上运行的软件平台上,并且可以安全地执行一个或多个应用或多个应用或小程序。可以将小程序添加到非接触式卡中,以在各种基于移动应用的使用情况下为多因素认证(MFA)提供一次性密码(OTP)。小程序可被配置为响应于来自诸如移动NFC读取器之类的读取器的一个或多个请求(诸如近场数据交换请求),并产生包括被编码为NDEF文本标签的

密码安全OTP的NDEF消息。

[0049] 图7显示了示出非接触式卡702和计算设备706之间交互的组件图。非接触式卡可以具有NFC功能。当非接触式卡接近移动计算设备708上的NFC读取器708时,安全包704中的身份信息被传送给计算设备。

[0050] 保持身份信息的安全包704的生成可以由诸如如MD5或SHA-1之类的密码哈希函数生成。图8A显示了描绘在示例性实施例中如何可以使用密码哈希函数的框图800。在图8A所示的示例中,三个输入802、804和806一起通过哈希函数808。描绘三个输入的选择旨在说明而非限制。在某些情况下可以使用其他数量的输入。哈希函数808产生输出哈希值812。由于哈希函数808的性质,在计算上难以在不知道哈希函数808所使用的密钥810的情况下从哈希值812导出输入802、804和806。密钥810是保密的。密钥810可以针对每个会话被动态地生成,并且可以是非接触式卡所特有的。因此,哈希函数808为被包括在安全包中的内容(例如,输入802、804和806)提供了安全层。

[0051] 在示例性实施例中,输入802、804和806可以根据各方希望交换的信息和用于认证发起方的协议而变化。图8B显示了在示例性实施例中可以被哈希的可能类型的输入832的图830。在这些示例性实施例中,可以包括由非接触式卡生成的一次性密码834作为输入。可以提供用于发起方的账户标识符836。这可以是唯一标识发起方的账户的账号或其他标识符。账户标识符836可以是发起方的电话号码。在某些情况下,发起方的电话号码可能不被包括在哈希值812中,但是可以根据从移动计算设备发送的消息导出。输入832可以包括发起方的计数器值838和/或名称840。

[0052] 作为增加的安全层,哈希值902可以被加密。图9显示了描绘这种加密的框图900。如上所讨论的所生成的哈希值902被传递到加密引擎904,该加密引擎使用加密密钥906对哈希值进行加密。所得到的输出是安全包908。加密引擎704可以使用多种密码算法中的任意一种,诸如DES、AES、RSA、DSA等。这些算法可以是如DES和AES之类的对称密码算法,或者是如RSA和DSA之类的非对称密码算法。假定认证服务432拥有用于对安全包进行解密的适当密钥。尽管图9中未显示,但其他内容可以与哈希值902一起被加密。

[0053] 图10提供了验证用户身份时可以执行的示出性步骤的流程图1000。用户将非接触式卡702轻叩到移动计算设备706,该移动计算设备706具有如上所讨论的NFC读取器708(见1002)。移动计算设备706向服务器430上的认证服务432发送包含从非接触式卡702获得的安全包的消息(参见1004)。提取安全包中的一次性密码(OTP)和其他信息(参见1006)。认证服务432使用所提取的信息来认证用户的身份(参见1008)。

[0054] 讨论不会更详细地集中在接收源自非接触式卡的安全包的认证服务上。图11描绘了被存储为认证服务1100的一部分的某些项目。这些项目包括可以被用于解密/加密操作的同步计数器1102。认证服务1100包括用于对安全包执行解密操作的解密代码1104。认证服务1100还可以存储多个解密密钥和加密密钥1106。

[0055] 通常,服务器430(或另一计算设备)和非接触式卡420可配备相同的主密钥(也称为主对称密钥)。更具体地,每个非接触式卡420可以用不同的主密钥编程,该主密钥在认证服务432中具有对应的密钥对。例如,当制造非接触式卡420时,可以将唯一的主密钥编程到非接触式卡420的存储器中。类似地,唯一的主密钥可以被存储在认证服务432可访问的账户信息中与非接触式卡420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

钥可以对非接触式卡432和认证服务432之外的所有方保密,从而增强系统的安全性。

[0056] 主密钥可以与计数器结合使用,以使用密钥多样化来增强安全性。计数器415和1102包括在非接触式卡420和认证服务432之间同步的值。计数器值可以包括每次在非接触式卡420和认证服务432之间交换数据时改变的数字。

[0057] 在移动计算设备402和非接触式卡420之间建立通信后,非接触式卡420可生成消息认证码(MAC)密码。在一些示例中,这可能在读取非接触式卡420时发生。具体而言,这可能在近场数据交换(NDEF)标签的读取(诸如NFC读取)时发生,该标签可以根据NFC数据交换格式被创建。例如,诸如NFC读取器之类的读取器可以发送具有NDEF产生小程序的小程序ID的消息,诸如小程序选择消息。在确认选择后,可以发送一系列选择文件消息,随后是读取文件消息。例如,该一系列选择文件可以包括“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420维护的计数器值415可以被更新或递增,之后可以是“读取NDEF文件”。此时,可以生成可以包括报头和共享秘密的消息。然后可以生成会话密钥。可以根据该消息创建MAC密码,该消息可以包括报头和共享秘密。然后,可以将MAC密码与一个或多个随机数据块串接,并且可以使用会话密钥对MAC密码和随机数(RND)进行加密。此后,密码和报头可以被串接,并且被编码为ASCII十六进制,并且以NDEF消息格式返回(响应于“读取NDEF文件”消息)。在一些示例中,可以将MAC密码作为NDEF标签来发送,而在其他示例中,MAC密码可以与统一的资源指示符一起被包括(例如,作为格式化的字符串)。非接触式卡420然后可以将MAC密码发送给移动计算设备402,移动计算设备402然后可以将MAC密码转发给认证服务432以进行验证,如下面所解释的。然而,在一些实施例中,移动计算设备402可以验证MAC密码。

[0058] 更一般地,当准备发送数据(例如,向服务器430)时,非接触式卡420可递增计数器415。非接触式卡420然后可以提供主密钥和计数器值作为密码算法的输入,该密码算法产生多样化的密钥作为输出。该密码算法可以包括加密算法、基于哈希的消息认证码(HMAC)算法、基于密文的消息认证码(CMAC)算法等。密码算法的非限制性示例可以包括诸如3DES或AES128之类的对称加密算法;诸如HMAC-SHA-256之类的对称HMAC算法;以及诸如AES-CMAC之类的对称CMAC算法。

[0059] 然后,非接触式卡420可以使用多样化的密钥对数据(例如,客户标识符和任何其他数据)进行加密。然后,非接触式卡420可以将被加密的数据传输到移动计算设备402(例如,经由NFC连接、蓝牙连接等)。移动计算设备402然后可以经由网络406将被加密的数据传输到服务器计算设备430上的认证服务432。在至少一个实施例中,非接触式卡420传输带有加密数据的计数器值。在这种实施例中,非接触式卡420可以传输被加密的计数器值或未被加密的计数器值。

[0060] 尽管计数器被用作示例,但其他数据可以被用于确保非接触式卡420、移动计算设备402和/或认证服务432之间的通信。例如,计数器可以用每次需要新的多样化密钥时生成的随机数、从非接触式卡420和认证服务432发送的计数器值的全值、从非接触性卡420和认证服务432发送的计数器值中的一部分、由非接触式卡420和认证服务432独立维护但不在两者之间发送的计数器、在非接触式卡420和认证服务432之间交换的一次性密码以及数据的密码哈希来替换。在一些示例中,各方可以使用多样化密钥的一个或多个部分来创建多个多样化密钥。

[0061] 图12描绘了一旦作为接收方的认证服务432接收到具有安全包的认证消息,就对发起方进行认证所执行的步骤的流程图1200。最初,认证服务432使用解密密钥1106来对安全包进行解密。此外,解密密钥1106用于解密哈希,以提取由哈希函数808被哈希在一起的输入(参见1202)。可以将所提取的密码和计数器值与有效密码和有效计数器值进行比较(参见1204)。确定密码是否匹配以及计数器值是否匹配,或者所提取的计数器值是否以其他方式指示密码尚未过期(参见1206)。如果密码匹配并且基于所提取的计数器值提取的密码没有过期,则可以比较其他提取的信息(参见1208)。

[0062] 其他信息可以是其他认证因素1002,诸如移动计算设备402的电话号码,其可以与用户418的记录电话号码进行比较。其他认证因素可以包括用户的地理位置。该地理位置可以是诸如GPS信息或区域码之类的信息,并且交换可以与关于用户的住所的信息进行比较的前缀信息。其他认证因素还可以包括在用户和认证服务432之间共享的共享秘密。

[0063] 再次参考图12,如果其他信息是有效的(参见1210),则用户418通过认证(参见1214)。如果不是有效的,用户418没有被认证(参见1212)。类似地,如果密码不匹配或者如所提取的计数器值所指示的密码已经过期,则用户未被认证(参见1212)。

[0064] 现在的讨论将集中在支付卡上。图13描绘了适用于示例性实施例的支付卡1300的框图。支付卡1300可以是信用卡、借记卡或能够用于支付的其他种类的卡。在一些实施例中,支付卡1300可以是诸如多功能卡或接触卡之类的智能卡。支付卡1300可以包括用于执行计算机编程指令的处理器1302和用于提供如上所描述的NFC能力的NFC硬件1314。支付卡1300还可以包括存储器1304。该存储器1304可以存储用于使用支付卡执行电子支付的指令1306。该存储器1304还可以存储如上所描述的用于解锁的指令1308。这些指令1306和1308可以由处理器1302执行,以执行上述支付卡1300的功能。存储器1304可以保持用于解锁的密钥代码1310,诸如门上的锁、区域的锁或物品上的锁。最后,存储器可以存储数据1312。

[0065] 图14描绘了可被执行用于使用支付卡1300进行支付的示出性步骤的流程图1400,诸如在住宿处、在工作场所处、在商店处等。首先,用户识别用户希望购买的东西(参见1402)。然后,用户将支付卡轻叩读取器以实现支付(参见1404)。例如,用户房间中的用户可以通过将支付卡轻叩位于用户房间内的读取器来为迷你酒吧的商品支付或为电影支付。读取器可以是NFC读取器,其可以经由NFC与支付卡无线通信以实现支付。作为另一个示例,员工可以具有NFC功能的识别卡,并且该识别卡可以被用于解锁工作中安全区域的锁。员工可以在餐厅结账时将识别卡轻叩到NFC读取器,以支付午餐费用。用户账户(诸如房间账户、员工账户或银行账户)被收取购买费用(参见1406)。

[0066] 虽然本申请侧重于示例性实施例,但应理解,在不脱离所附权利要求的范围的情况下,可以对形式和细节进行各种改变。

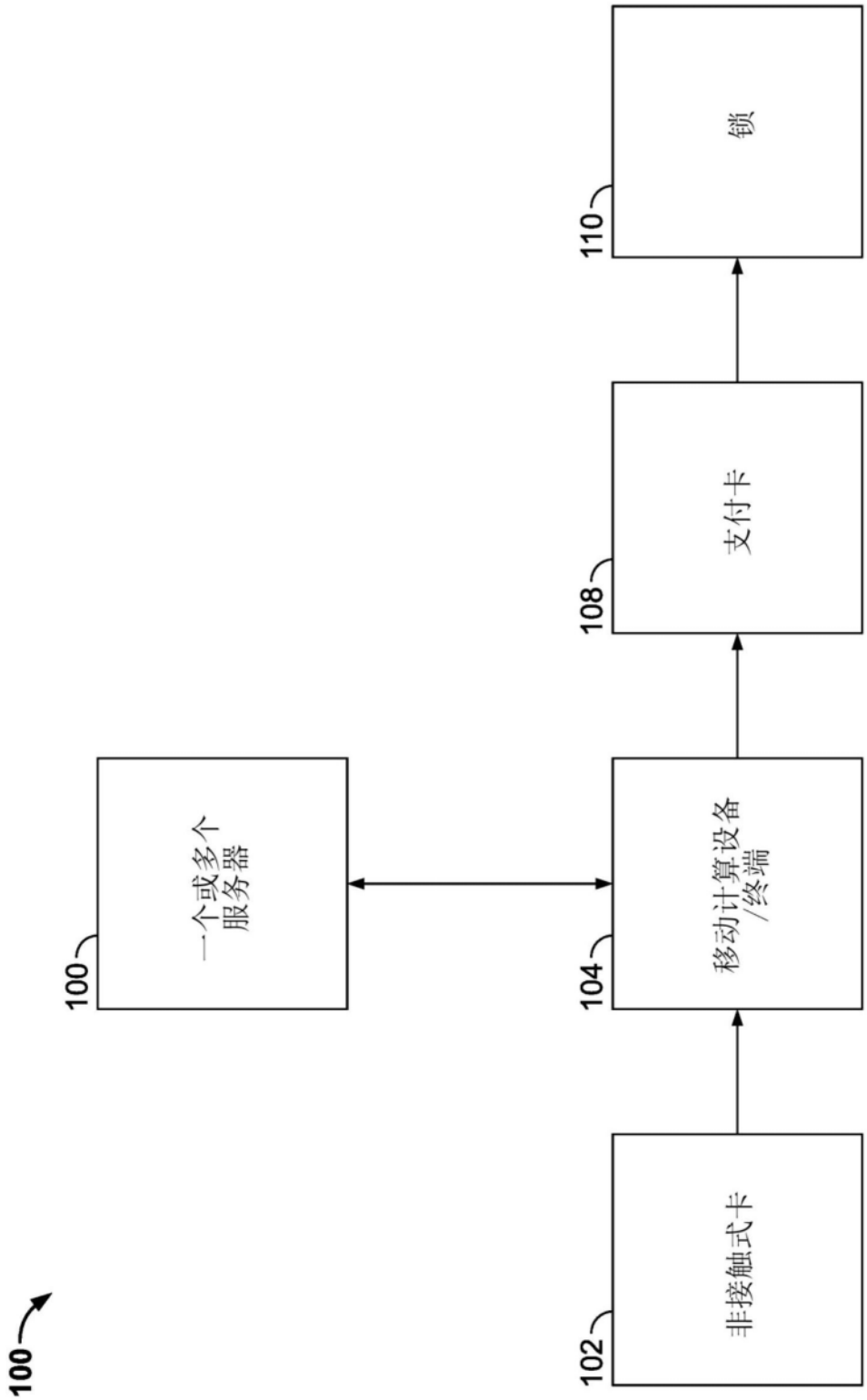


图1

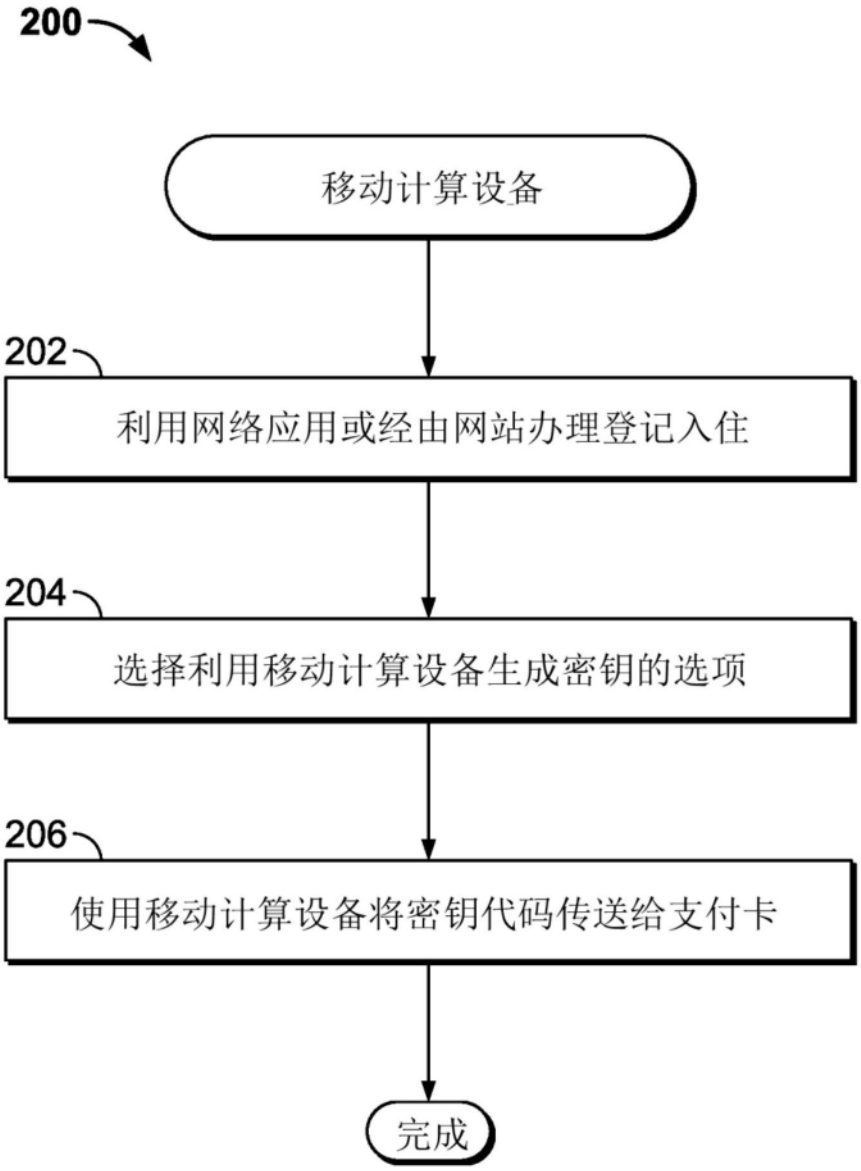

200
移动计算设备
202
利用网络应用或经由网站办理登记入住
204
选择利用移动计算设备生成密钥的选项
206
使用移动计算设备将密钥代码传送给支付卡
完成

图2

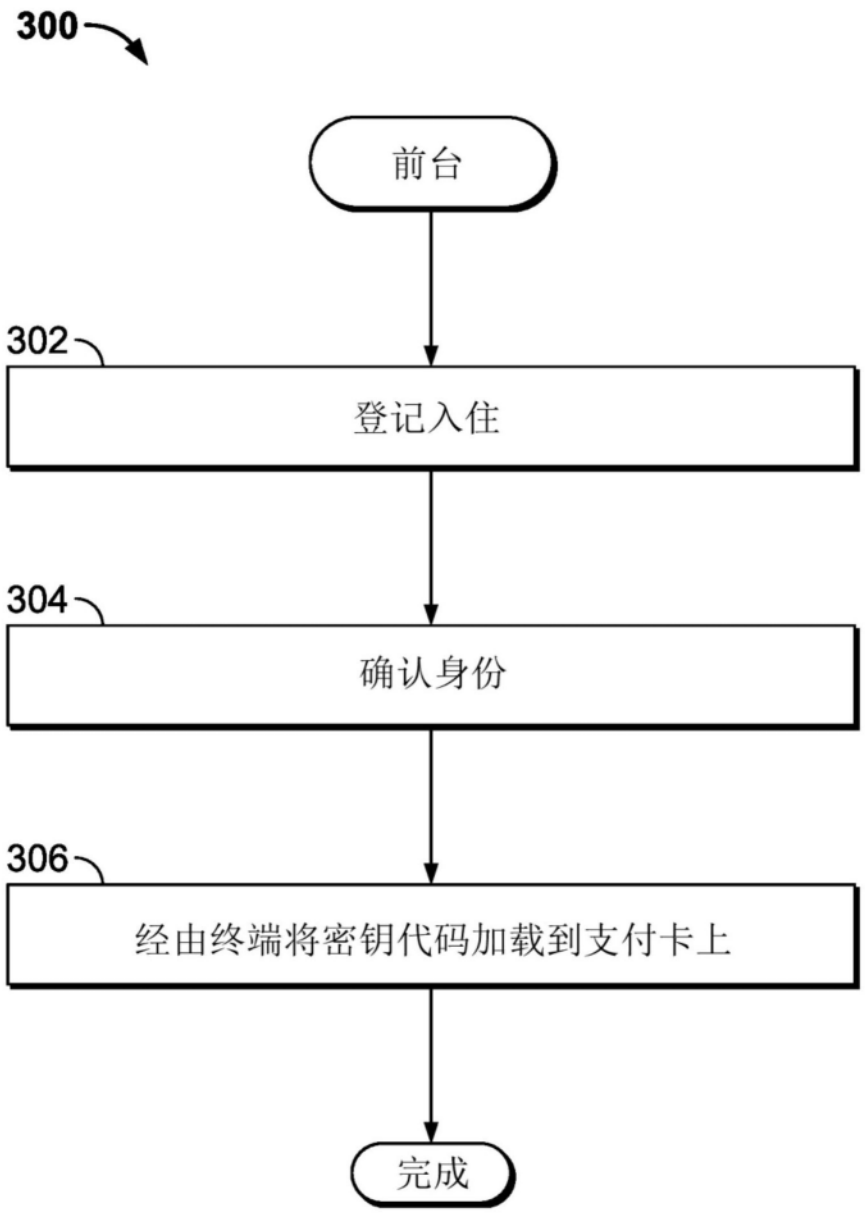


图3

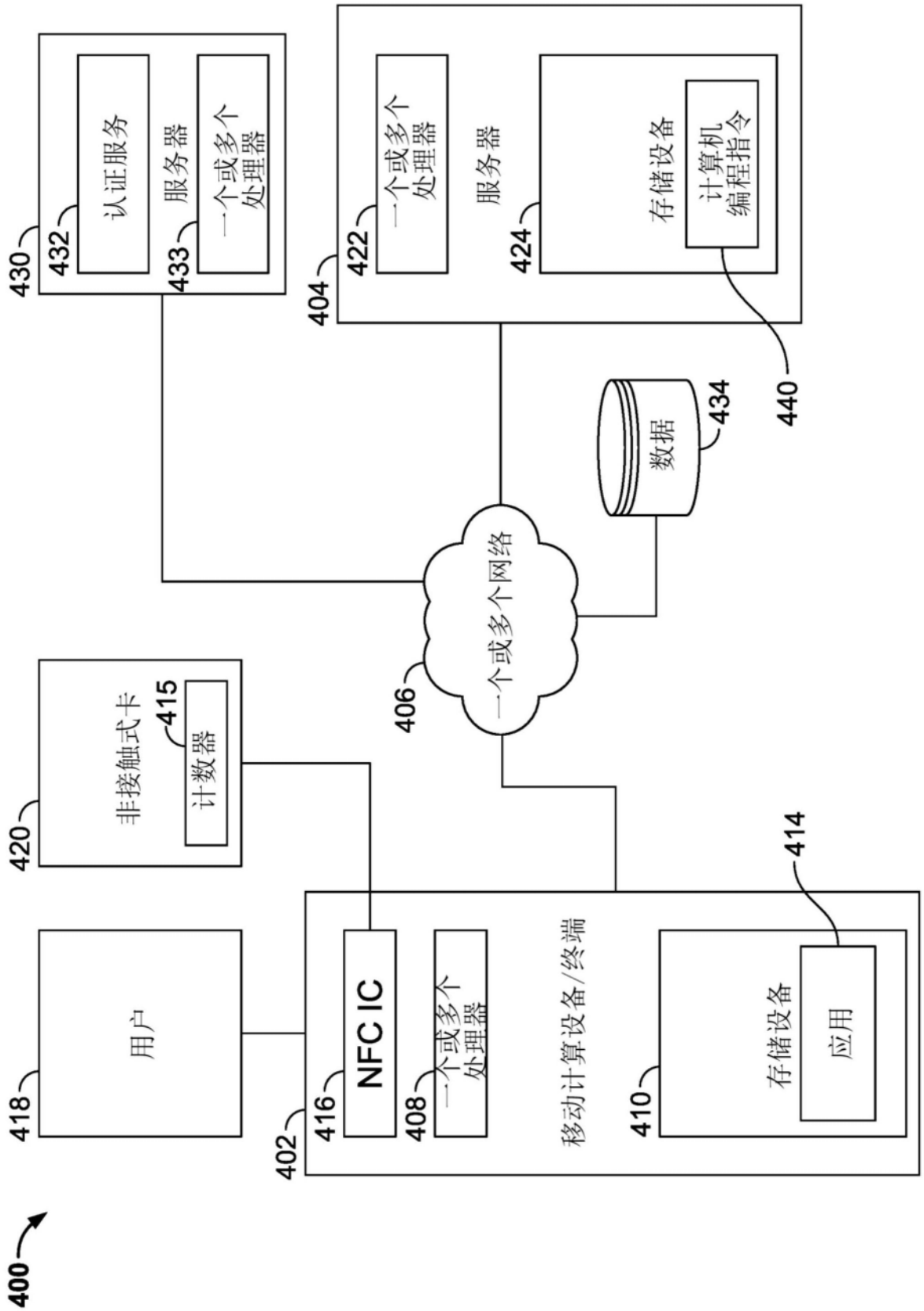

400
430
认证服务
432
服务器
一个或多个处理器
433
404
一个或多个处理器
422
服务器
424
存储设备
计算机编程指令
440
数据
434
一个或多个网络
406
非接触式卡
计数器
415
420
用户
418
NFC IC
416
一个或多个处理器
408
移动计算设备/终端
402
存储设备
应用
410
414

图4

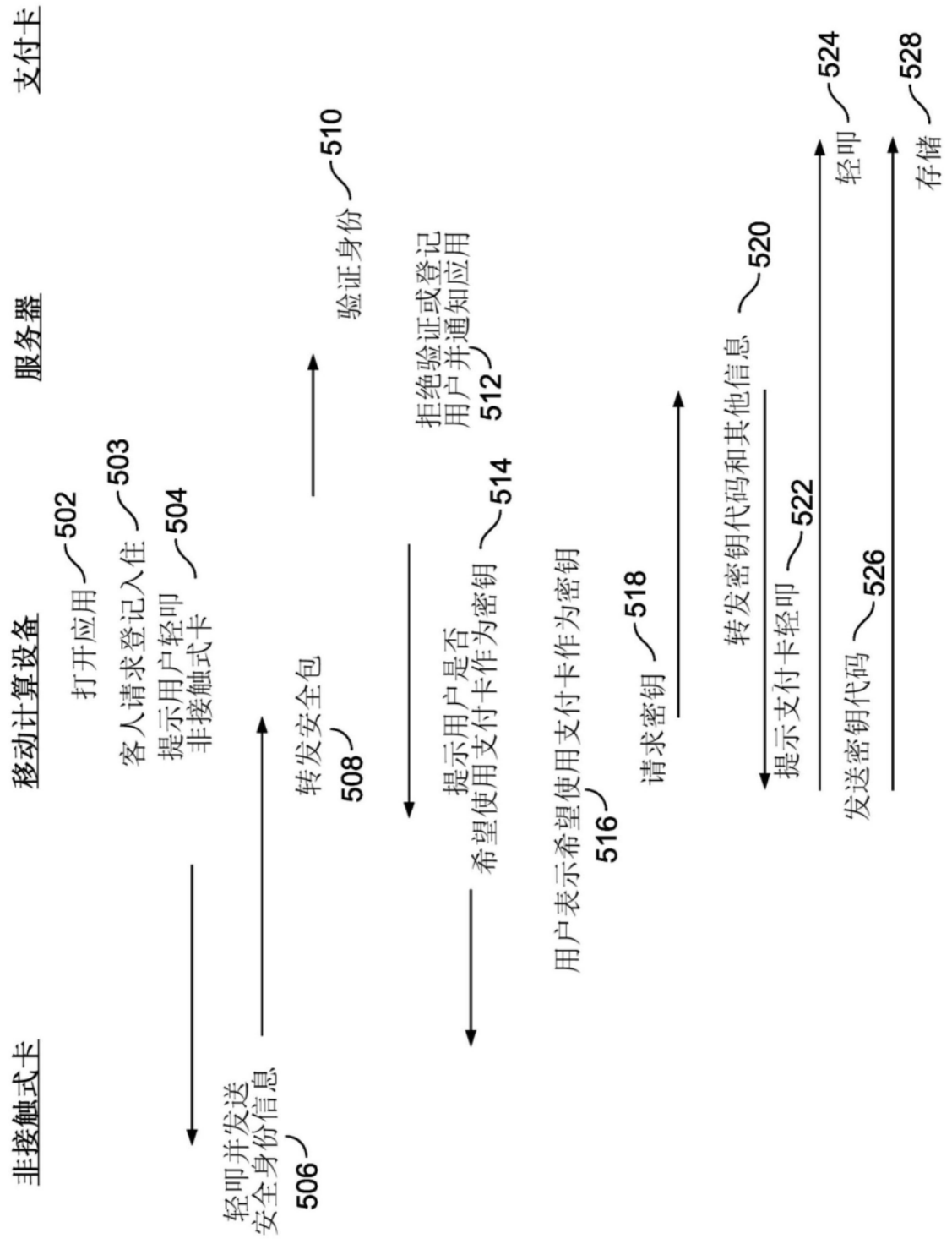

非接触式卡
移动计算设备
服务器
支付卡
打开应用
502
客人请求登记入住
503
提示用户轻叩
非接触式卡
504
轻叩并发送
安全身份信息
506
转发安全包
508
验证身份
510
拒绝验证或登记
用户并通知应用
512
提示用户是否
希望使用支付卡作为密钥
514
用户表示希望使用支付卡作为密钥
516
请求密钥
518
转发密钥代码和其他信息
520
提示支付卡轻叩
522
轻叩
524
发送密钥代码
526
存储
528

图5

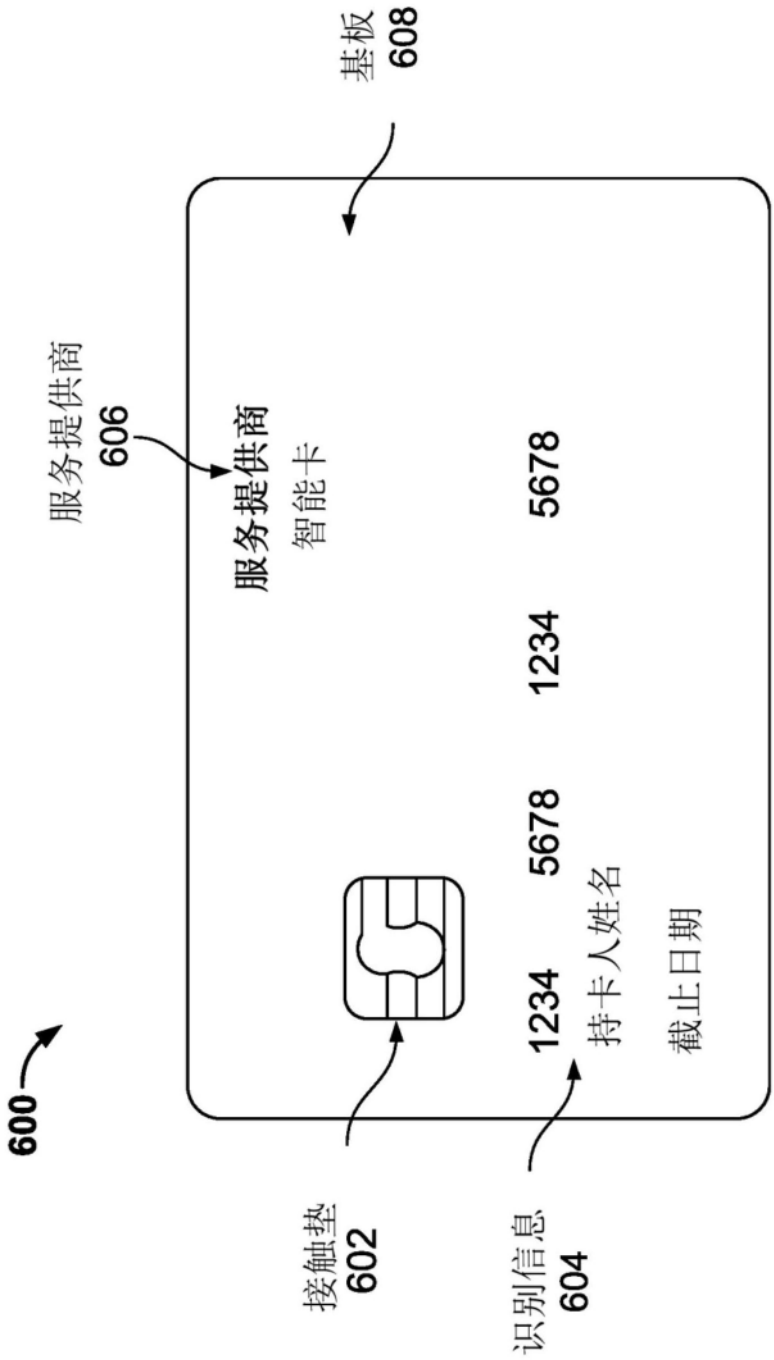

600
服务提供商
606
基板
608
服务提供商
智能卡
5678
1234
5678
1234
持卡人姓名
截止日期
接触垫
602
识别信息
604

图6A

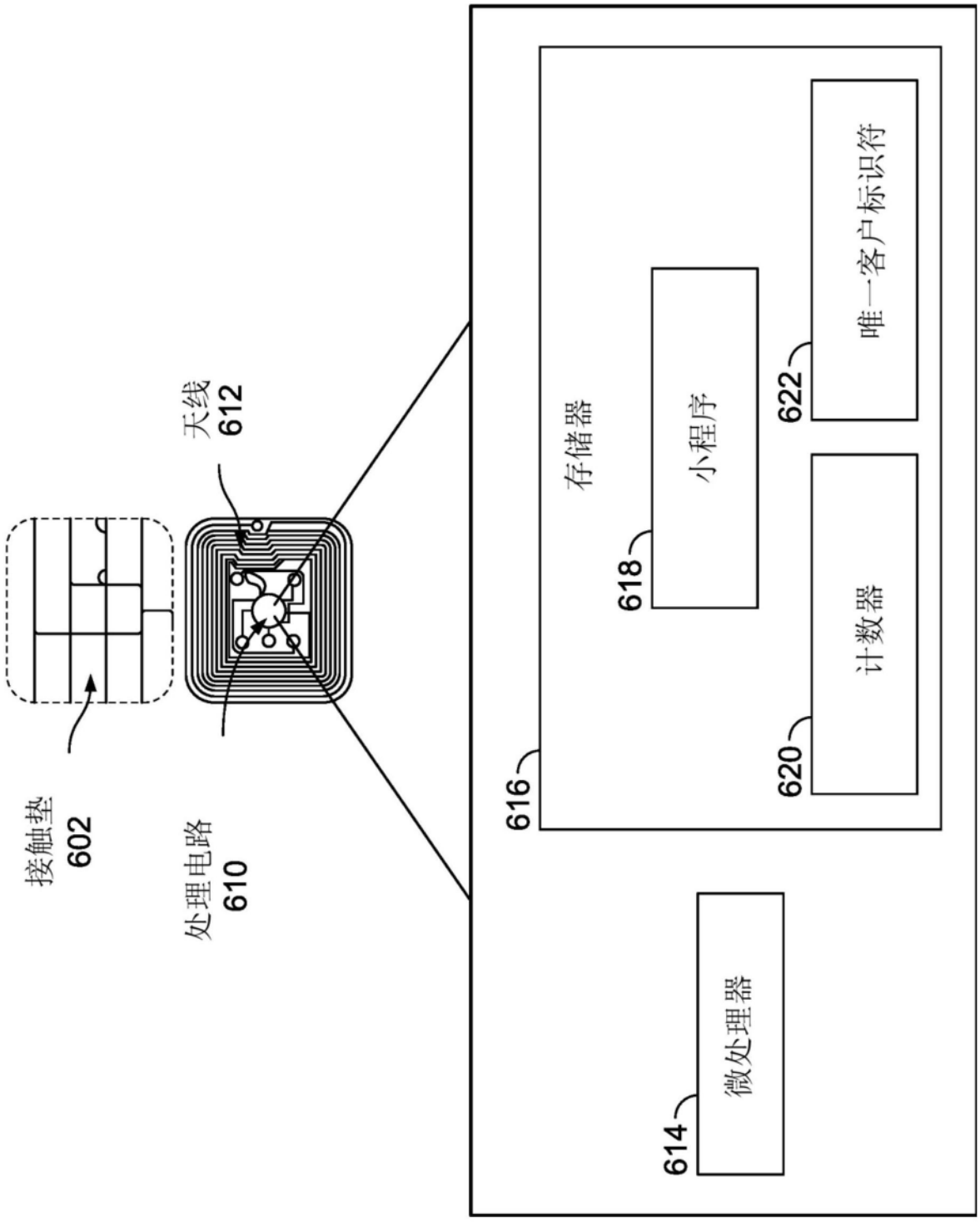

接触垫
602
处理电路
610
天线
612
存储器
616
小程序
618
计数器
620
唯一客户标识符
622
微处理器
614

图6B

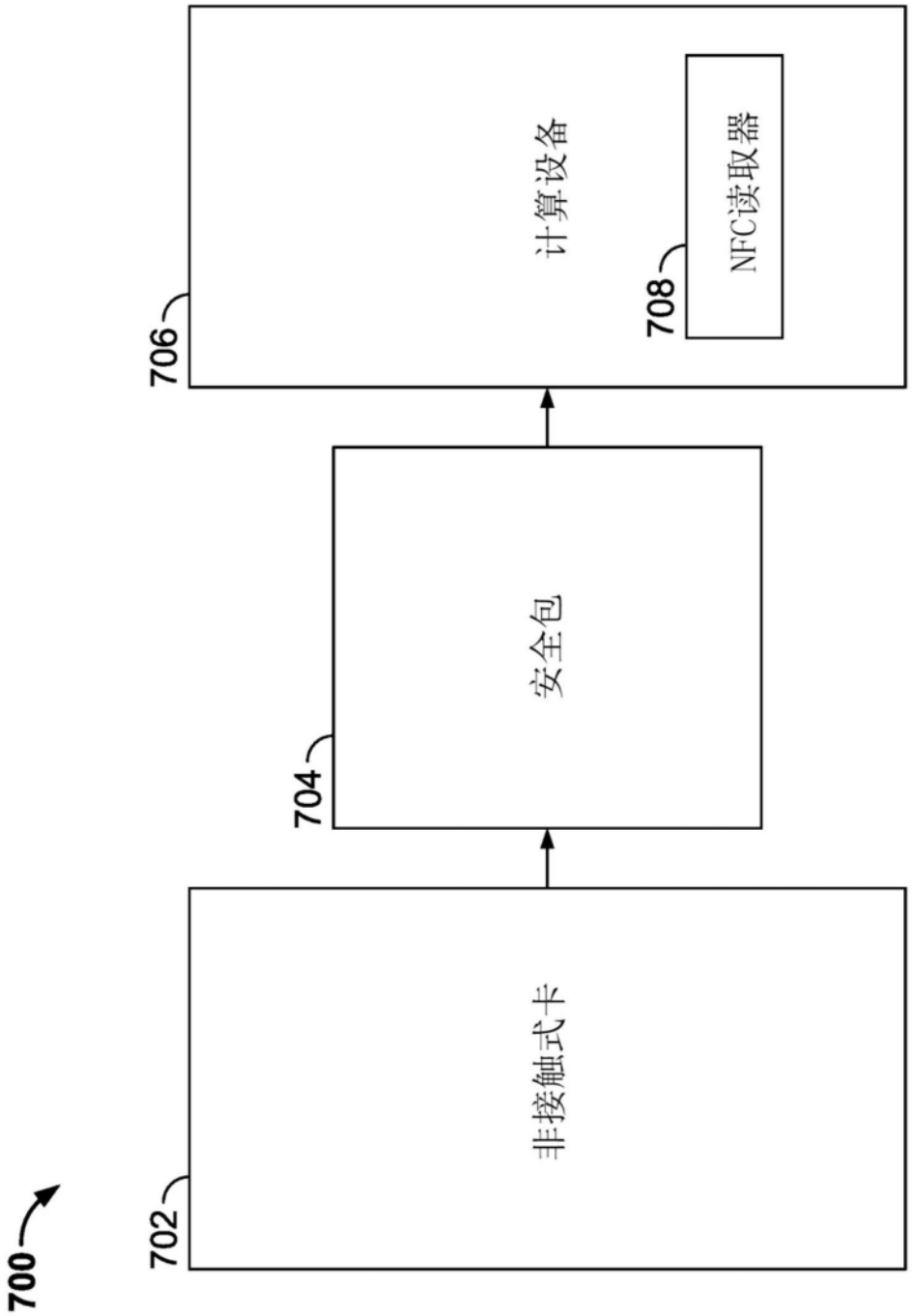


图7

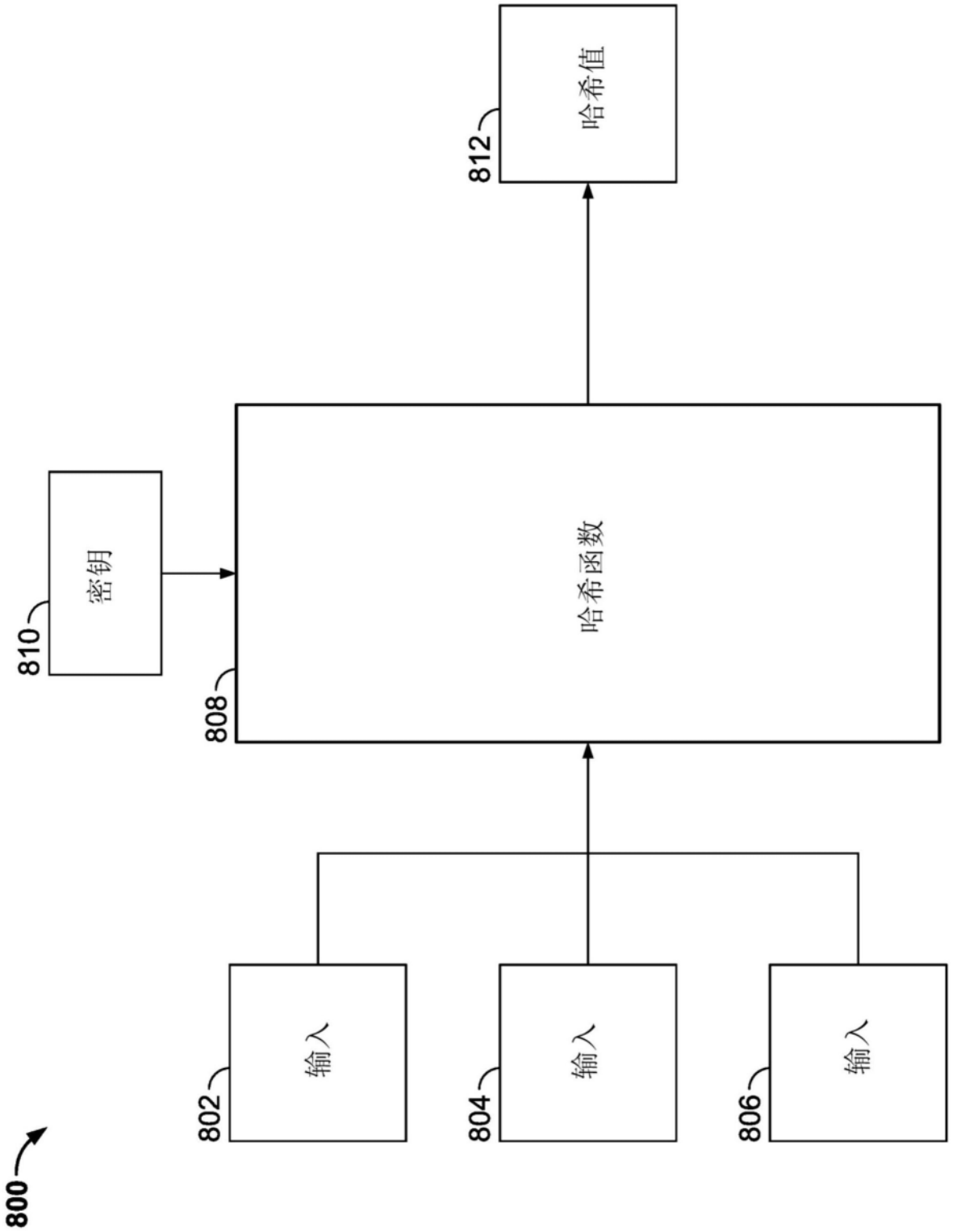


图8A

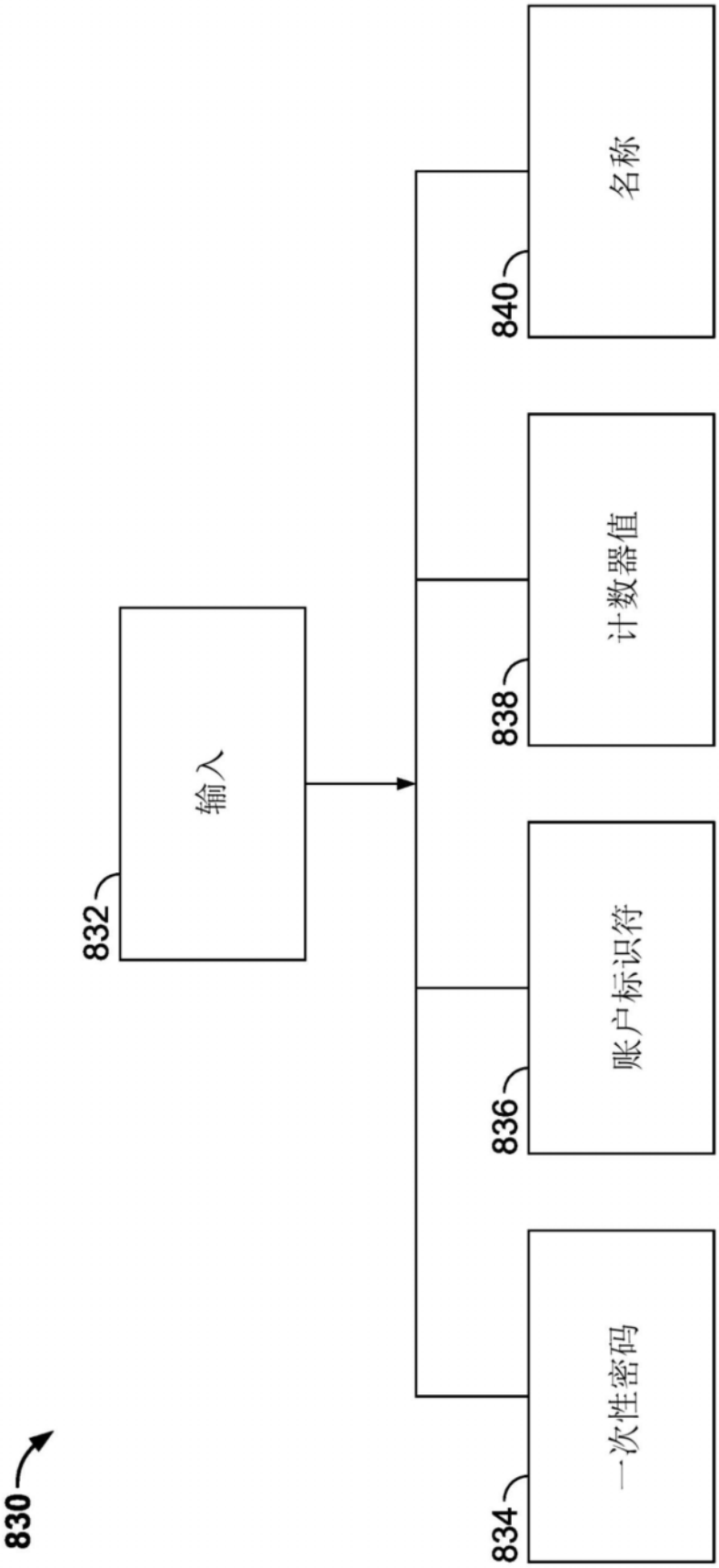


图8B

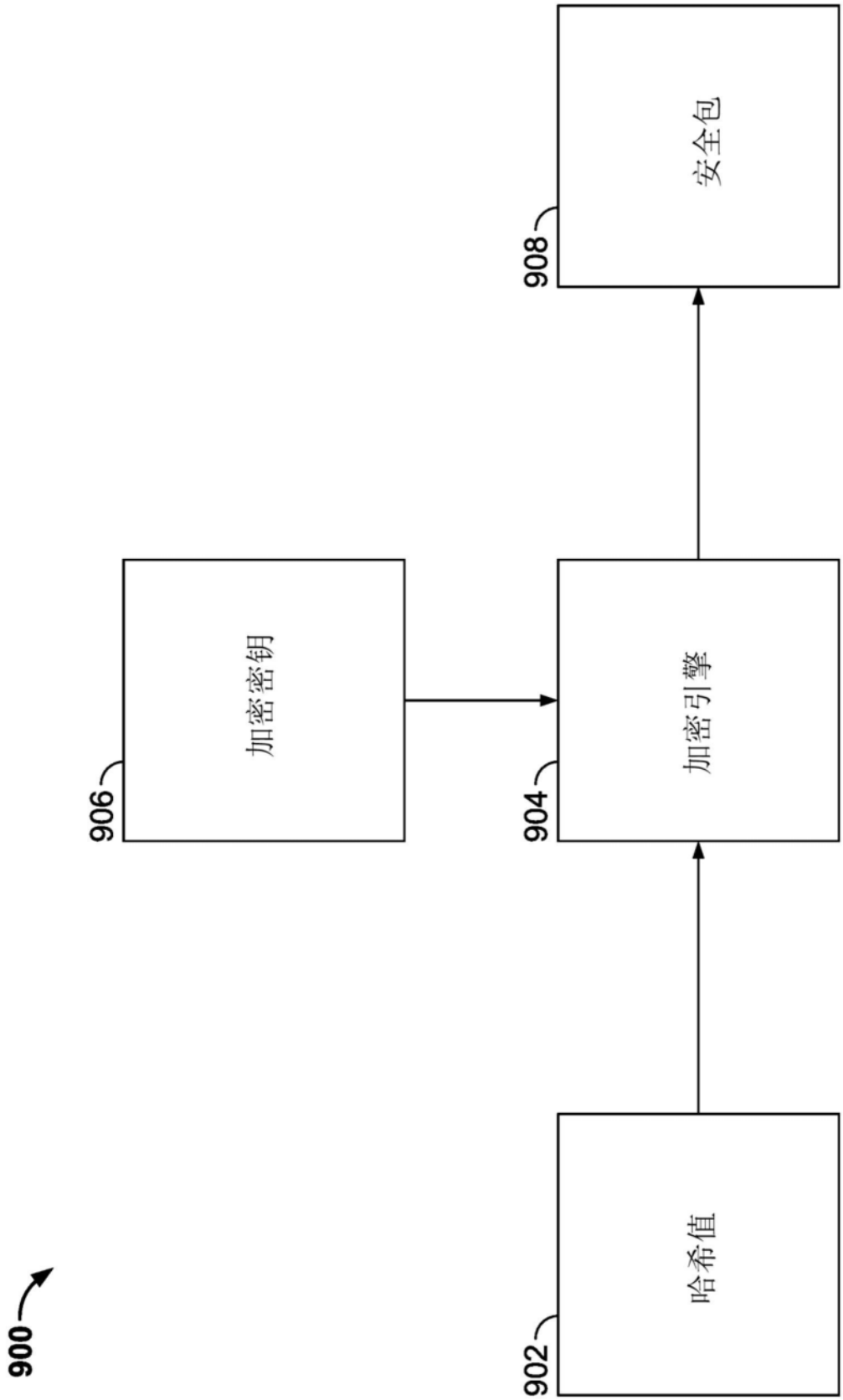


图9

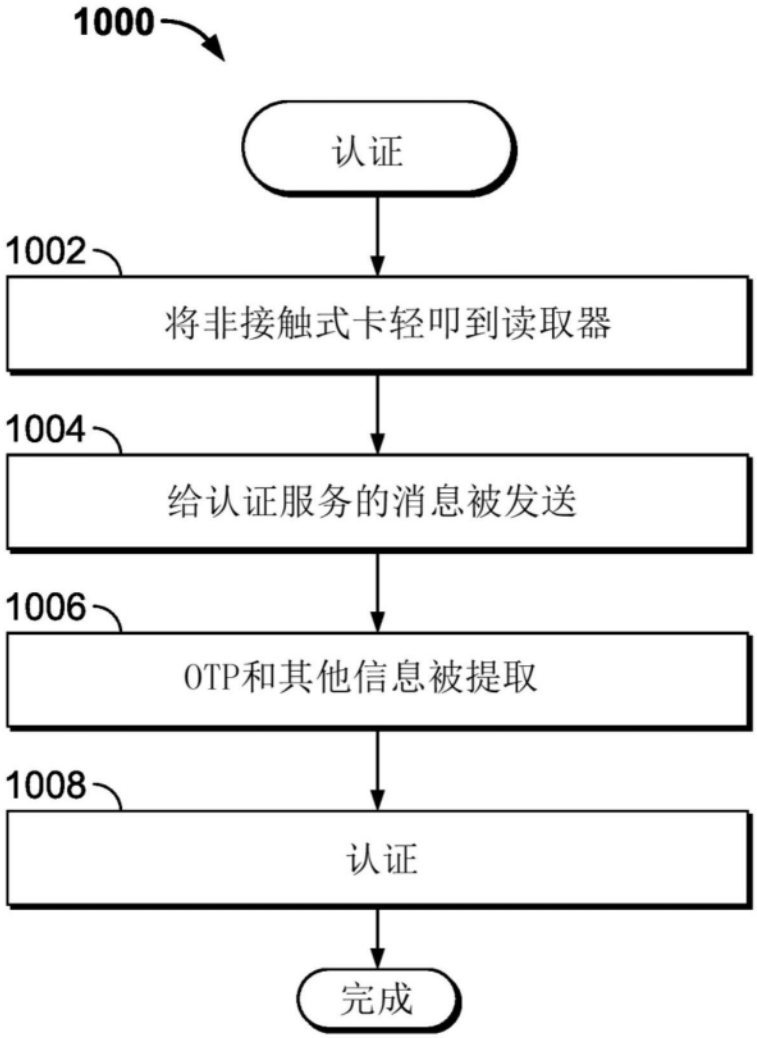

1000
认证
1002
将非接触式卡轻叩到读取器
1004
给认证服务的消息被发送
1006
OTP和其他信息被提取
1008
认证
完成

图10

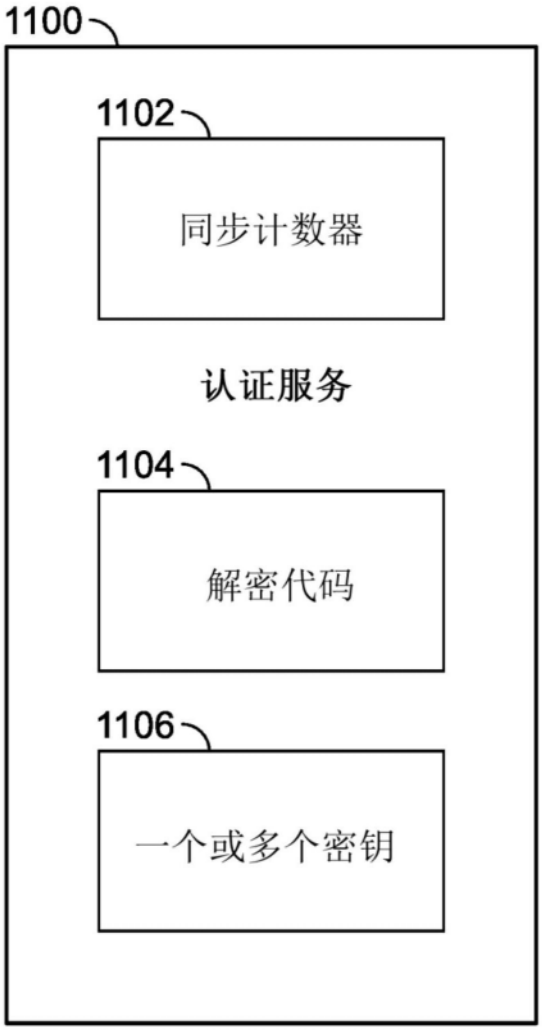


图11

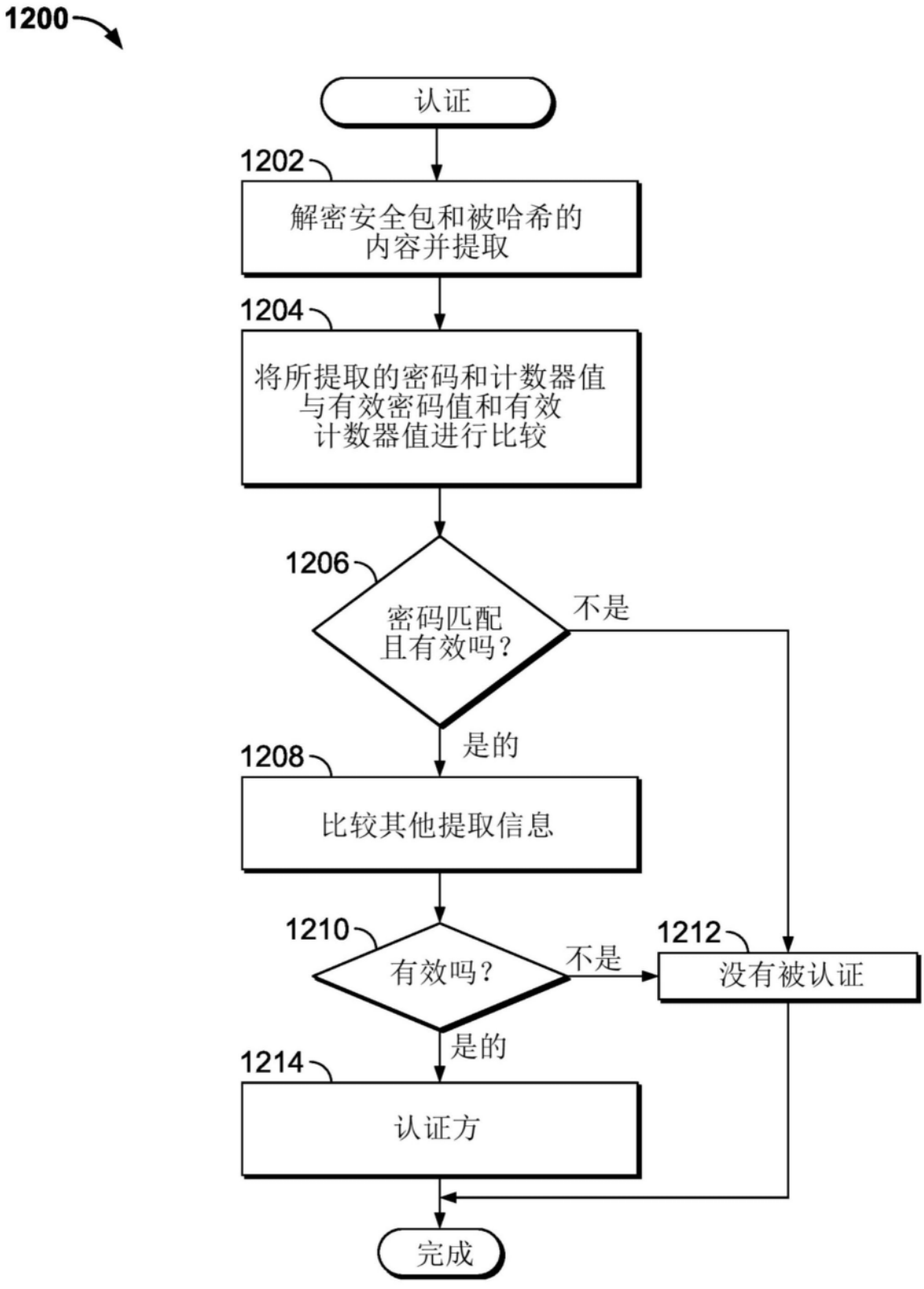

1200
认证
1202
解密安全包和被哈希的内容并提取
1204
将所提取的密码和计数器值与有效密码值和有效计数器值进行比较
1206
密码匹配且有效吗？
不是
是的
1208
比较其他提取信息
1210
有效吗？
不是
1212
没有被认证
是的
1214
认证方
完成

图12

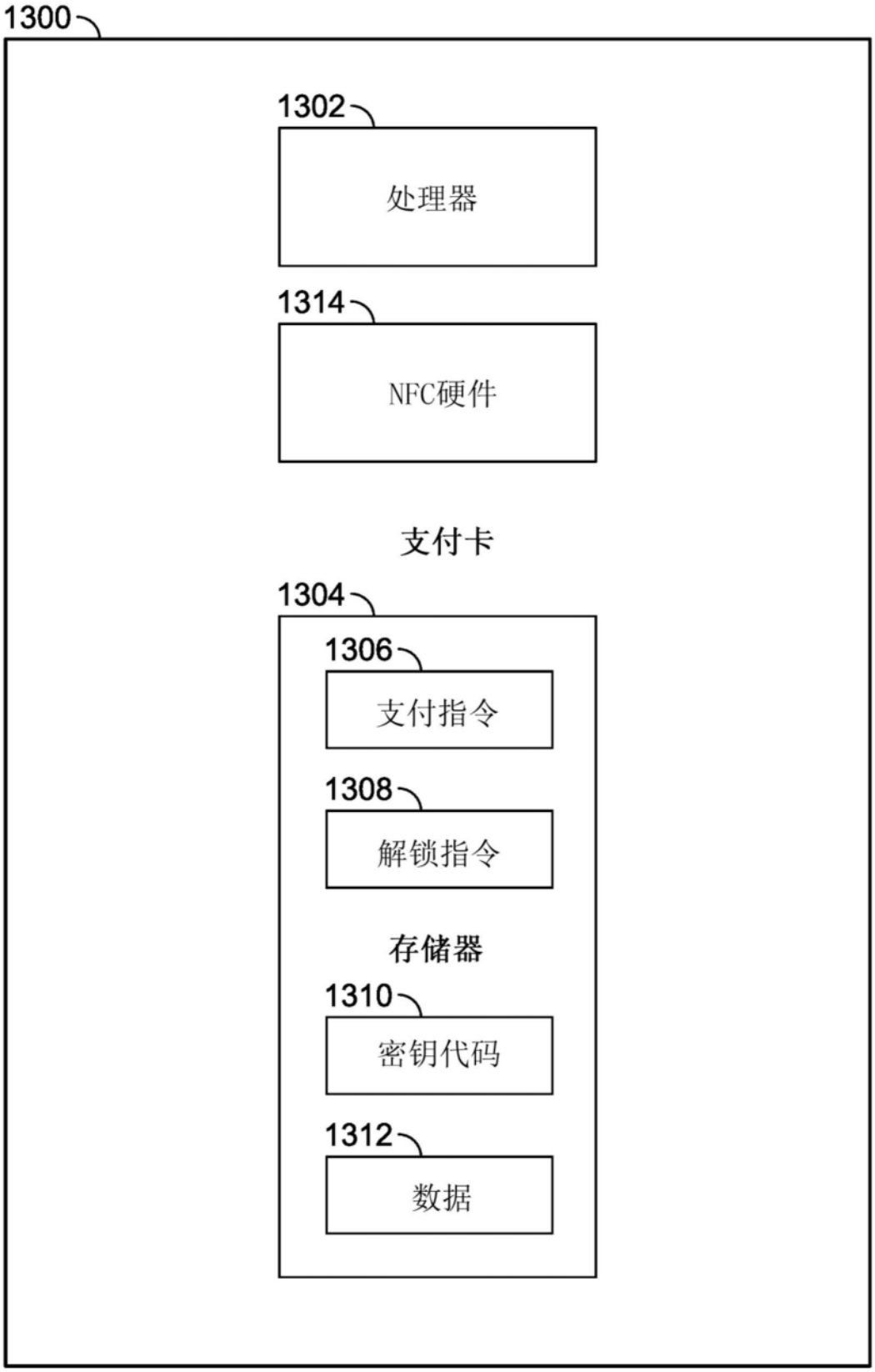

1300
1302
处理器
1314
NFC硬件
支付卡
1304
1306
支付指令
1308
解锁指令
存储器
1310
密钥代码
1312
数据

图13

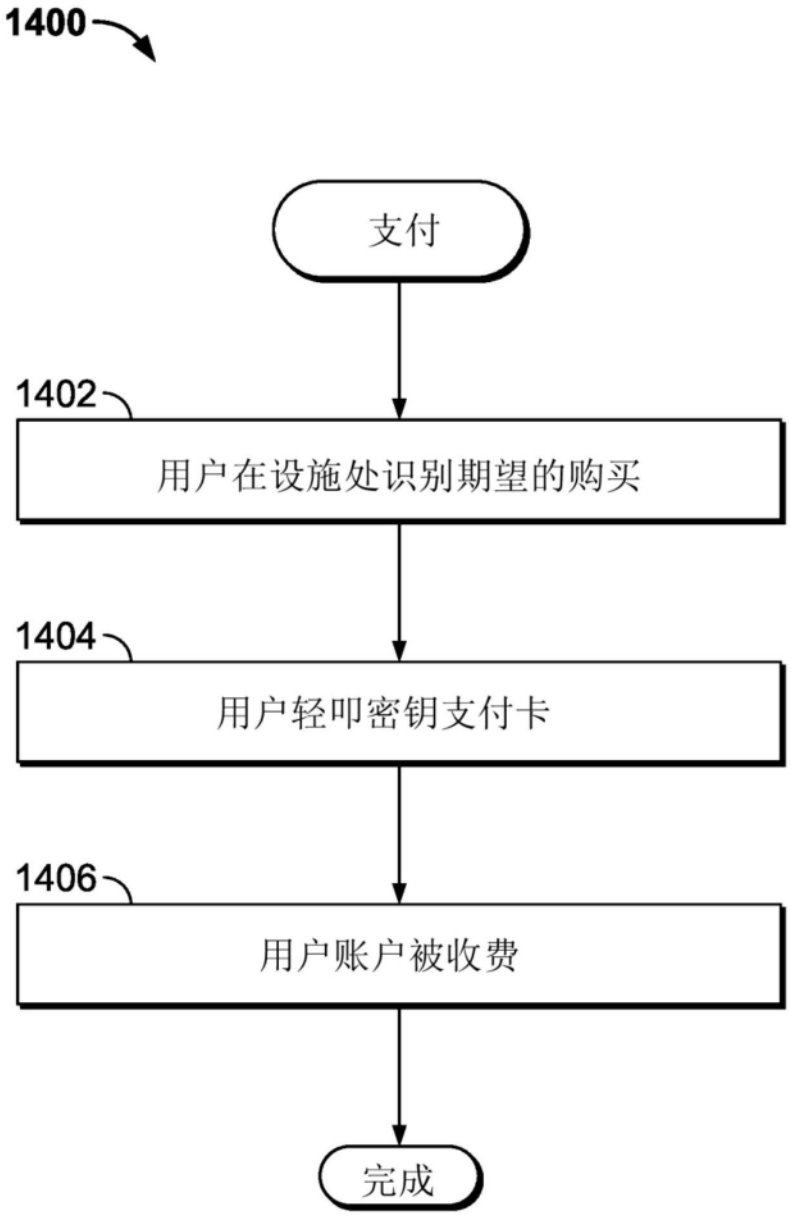


图14