



(12) 发明专利申请

(10) 申请公布号 CN 114631109 A

(43) 申请公布日 2022. 06. 14

(21) 申请号 202080075487.3

(22) 申请日 2020.10.28

(30) 优先权数据

16/675,172 2019.11.05 US

(85) PCT国际申请进入国家阶段日

2022.04.27

(86) PCT国际申请的申请数据

PCT/US2020/057668 2020.10.28

(87) PCT国际申请的公布数据

W02021/091739 EN 2021.05.14

(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 威廉·杜安 凯文·奥斯本

(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 20/32 (2012.01)

G06Q 20/38 (2012.01)

G06Q 20/40 (2012.01)

H04L 9/32 (2006.01)

H04L 9/40 (2022.01)

H04W 12/06 (2021.01)

G06F 21/34 (2013.01)

权利要求书2页 说明书14页 附图11页

(54) 发明名称

用于交叉耦合风险分析和一次性口令的系统及方法

(57) 摘要

示例实施例提供了用于使用诸如支持近场通信 (NFC) 的芯片的物理令牌而验证动作的系统和方法。服务器可以接收用于执行动作的请求，并且可以需要来自物理令牌的持有者的验证。物理令牌的持有者可以使用他们的登录信用证而登录到应用程序，从而提供第一级认证。然后，持有者可以利用他们的移动设备上的读取器而扫描物理令牌，这提供了第二级认证。扫描可以表明物理令牌上计数器的值，该值可以与服务器处的计数器进行比较，以便验证该物理令牌已经按预期使用。如果服务器认为适当，则可能需要第三 (或进一步) 级，诸如扫描持有者的照片标识。



1. 一种存储指令的非暂时性计算机可读介质,所述指令当由处理器执行时致使所述处理器:

从验证服务器接收请求,所述请求与用户账户相关联,所述用户账户与用户相关联;

通过在计算设备上认证所述用户的身份而执行第一验证动作;

通过经由短距离通信协议从物理令牌接收代码的扫描而执行第二验证动作;

基于所述第一验证动作和所述第二验证动作而生成验证响应分组,所述验证响应分组识别从所述物理令牌检索到的所述用户和所述代码;以及

向所述验证服务器传送所述响应分组。

2. 根据权利要求1所述的介质,其中,所述短距离通信协议是近场通信(NFC)协议。

3. 根据权利要求1所述的介质,其中,所述代码是被存储在物理令牌上的计数器,所述计数器在每次所述代码从所述物理令牌被读取时递增。

4. 根据权利要求1所述的介质,其中,所述物理令牌是被物理并入到信用卡的计算硬件。

5. 根据权利要求1所述的介质,其中,认证所述用户的身份包括:将所述用户登录到运行于所述计算设备的应用程序上的所述用户账户。

6. 根据权利要求1所述的介质,还存储用于以下操作的指令:

响应于传送所述响应分组而接收升级验证请求;

从所述计算设备的相机接收照片;和

生成对所述升级验证请求的响应,所述响应包括所述照片。

7. 根据权利要求6所述的介质,其中,所述升级验证请求是用于与所述用户相关联的标识的照片的请求。

8. 一种方法,包括:

接收用于确认执行与服务相关联的交易的请求;

接收来自与用户相关联的物理令牌的累积值;

访问日志,所述日志将所述服务的用户映射到所述用户的相应物理令牌的最后已知值;

从所述日志中检索与所述用户相关联的物理令牌的最后已知值;

识别在所述物理令牌的最后已知值附近的可接受值的窗口;

确定从所述物理令牌接收到的所述累积值在可接受值的窗口内;以及

当所述累积值在所述窗口内时致使所述交易被执行。

9. 根据权利要求8所述的方法,其中,所述物理令牌是信用卡。

10. 根据权利要求8所述的方法,其中,所述窗口是单个值。

11. 根据权利要求8所述的方法,其中,所述窗口是值的范围

12. 根据权利要求11所述的方法,其中,所述范围是动态范围,并且还包括基于用户简档信息来修改所述窗口,所述用户简档信息指示所述累积值被无意地递增的估计速率。

13. 根据权利要求8所述的方法,还包括:计算与所述交易相关联的风险值。

14. 根据权利要求13所述的方法,其中,所述窗口的大小根据所述风险值而变化。

15. 一种系统,包括:

验证服务器,被配置为传送用于认证与用户账户相关联的用户的请求;和

客户端设备,被配置为接收从来自物理令牌的代码的扫描中导出的信息,其中

所述验证服务器还被配置为认证所述信息,所述认证包括将从所述物理令牌接收到的代码与存储在所述验证服务器处的相应代码进行比较,其中,至少部分地基于风险评估来执行所述认证。

16. 根据权利要求15所述的装置,其中,所述认证包括使初始认证过程失败,并传送用于进一步认证的请求。

17. 根据权利要求16所述的装置,其中,所述验证服务器还被配置为确定所述进一步认证失败,并且响应于所述失败而增加与所述风险评估相关联的风险级别。

18. 根据权利要求16所述的装置,其中,所述验证服务器还被配置为确定所述进一步认证已经成功,并且响应于所述成功而维持或降低与所述风险评估相关联的风险级别。

19. 根据权利要求15所述的装置,其中,所述认证包括通过初始认证过程,并且响应于所述成功而降低与所述风险评估相关联的风险级别。

20. 根据权利要求15所述的装置,其中,所述验证服务器还被配置为基于在所述认证期间所确定的信息来确定调整所述风险评估。

用于交叉耦合风险分析和一次性口令的系统及方法

[0001] 相关申请的交叉引用

[0002] 本申请要求于2019年11月5日提交的美国专利申请16/675,172的优先权,其是于2018年11月29日提交的美国专利申请16/205,119的部分继续申请,其要求来自于2018年10月2日提交的美国临时申请62/740,352的优先权,其全部公开内容通过引用并入本文。

技术领域

[0003] 本公开涉及密码术,更具体地,涉及用于非接触式卡的加密认证的系统和方法。

背景技术

[0004] 数据安全性和交易完整性对企业和消费者而言至关重要。随着电子交易在商业活动中所占份额越来越大,这种需求持续增长。

[0005] 当处理有问题或可疑的交易时,可能需要对交易进行验证。按常规地,这可以涉及经由电子邮件或短消息服务(SMS)向用户发送消息,请求用户确认他们参与交易的意图。

[0006] 除繁琐之外,这些服务还容易受到攻击,因此可能无法提供充足的安全等级。另外,如果用户将他们的卡与他们的移动设备一起存放(例如,将两者保存在钱包中,或将卡保存在常与移动设备放在一起的钱包中),欺诈行为者可能持有被用于认证交易的设备。

附图说明

[0007] 图1A描绘了适用于示例性实施例的环境;

[0008] 图1B描绘了具有物理令牌的非接触式卡的示例。

[0009] 图1C描绘了示例性物理令牌的结构。

[0010] 图2A描绘了与非接触式卡的所有者相关联的移动应用的示例性界面。

[0011] 图2B描绘了当物理令牌由所有者的移动设备上的读取器读取时的示例性界面。

[0012] 图2C描绘了非接触式卡与客户端设备之间的数据交换的示例。

[0013] 图3描绘了根据实施例的用于非接触式卡与客户端设备之间或者客户端设备与远程服务器之间的消息的示例性数据结构。

[0014] 图4描绘了客户端设备与一个或多个远程服务器之间的示例性数据交换。

[0015] 图5是描述示例性客户端交易验证逻辑的流程图。

[0016] 图6是描述示例性服务器端交易验证逻辑的流程图。

[0017] 图7描绘了适用于示例性实施例的示例性计算系统。

[0018] 图8描绘了适用于示例性实施例的示例性网络环境。

具体实施方式

[0019] 示例性实施例提供了用于增加非接触式卡的安全性同时允许以更为有效和用户友好的方式进行交易的技术。这些实施例可用于确保卡在物理上存在于卡主处(这可以当卡出于欺诈性当面交易而被盗时防止交易),并且确保卡主授权交易(这可用于验证是当面

交易还是远程交易)。此外,验证交易的过程涉及与卡上的物理令牌进行交互。因为这种交互,必须使用该卡来授权当面和远程交易,并且可以快速识别并拒绝未授权的交易。

[0020] 更具体地,当用户希望访问他们的账户(例如,在移动设备上)时,系统请求卡主的授权。卡主需要登录到执行在他们移动设备上的应用,并且扫描与他们的卡相关联的物理令牌(例如,能够与移动设备进行无线通信(诸如NFC、蓝牙、WiFi等)或者有线通信(诸如通过USB连接)的非接触式芯片)。这些步骤证实了卡主实体持有该卡;理论上,只有卡主应该能够登录到移动应用,并且如果卡由本地NFC读取器扫描,则可以确认出卡主持有的卡的存在。

[0021] 每次使用该卡时,存储在物理令牌上的计数器值可以递增,并且被传送到远程服务器进行验证。作为验证交易的扫描过程的一部分,存在于卡上的计数器可以与存储在服务器上的远程副本进行核对。如果从卡读取的计数器值不是服务器所期望的值,这可能指示卡或卡主的帐户已经被用于未授权的交易(因为卡的计数器值不是服务器所期望的值,这指示卡已被使用并且交易未被记录,或者攻击者正在试图重放所捕捉的先前会话以试图重放交易)。

[0022] 在许多情况下,卡上的计数器值可能与存储在服务器上的计数器值不完全匹配。例如,在部分读取的情况下(如果用户将他们的卡放在他们的电话附近而不打算实际读取物理令牌上的值,则可能发生这种情况),远程服务器可能不会更新增加的计数器值,尽管令牌上的计数器可能在本地被更新。计数器值必须一致的程度可以取决于交易的风险级别和/或环境的当前风险状况(例如,银行机构当前是否受到攻击)。因此,对于低风险交易,卡上的计数器值必须在某个预定范围内与服务器上的计数器值相匹配(这允许系统考虑卡的意外读取)。对于高风险交易,计数器值必须完全匹配或在更窄的预定范围内。该范围可以基于已知的用户与卡的常规交互来动态地确定(例如,如果用户历史上容易受到令牌的意外读取,则与他的卡通常不容易受到这种读取的用户相比,该范围可以被设置得更高)。如果系统确定存在不符,第一动作步骤可以是请求用户利用他们的移动设备上的应用程序对他们的卡进行重新验证。在这种情况下,该附加认证的计数器值应该已经超出可疑认证请求中包含的值。如果系统仍然无法验证计数器值,或者对于特别高风险的请求,可能需要进一步验证(例如,应用可能需要用户提供生物特征验证、用户的照片或用户身份证的扫描件;备选地,可能需要用户亲自在诸如银行的某处到场进行当面验证)。这些动作允许验证过程适应风险状况。

[0023] 类似地,风险概况可以基于在验证过程期间收集的信息来改变。例如,如果交易最初被标记为低风险,但是在该过程期间读取的计数器值指示可能已经发生了欺诈活动,则可以提升与该交易相关联的风险。在另一示例中,如果计数器值的验证触发了重新验证过程,则可以提升与该用户和/或交易相关联的风险级别。

[0024] 此外,这两个选项(基于风险状况而调整认证强度和基于认证结果而调整风险概况)可以组合并协力使用。

[0025] 实施例的以下描述提供了参考数字的非限制性代表例,以特别地描述本发明的不同方面的特征和教导。从实施例的描述中,应当认识到,所描述的实施例能够与其他实施例分开地或组合地实现。实施例的描述应在某种程度上促进对本发明的理解,使得没有具体覆盖但在阅读了实施例的描述的本领域技术人员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。

[0026] 图1A说明了根据示例实施例的数据传输环境100。如下文进一步讨论的,系统100可以包括非接触式卡(包括物理令牌106),客户端设备104,网络114和多个服务器116、128。虽然图1A说明了组件的特定配置,但是本领域普通技术人员将理解,可以使用包括更多或更少组件或者另一配置中的组件的其他配置。

[0027] 环境100可以包括一个或多个非接触式卡,这将在下文参照图1B进一步说明。在一些示例中,非接触式卡130可以与客户端设备104进行无线通信,例如NFC通信。非接触式卡可以包括物理令牌106,诸如非接触式芯片(参见图1C)。物理令牌106可以维持上文所述的计数器值108的副本,该副本可以在每次由读取器(诸如NFC读取器110)读取物理令牌时递增。

[0028] 环境100可以包括客户端设备104,客户端设备104可以是网络启用的计算机(network-enabled computer)。如本文所引用,网络启用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、网络家电、个人计算机(PC)、工作站、移动设备、电话、手持式PC、个人数字助理(PDA)、瘦客户端、胖客户端、因特网浏览器或其他设备。客户端设备104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 Apple 的 iOS® 操作系统的任何其他移动设备,运行 Microsoft 的 Windows® Mobile 操作系统的任何设备,和/或任何其他智能电话或类似的可穿戴移动设备。

[0029] 客户端设备104和/或包括物理令牌106的非接触式卡可以与用户102相关联,用户102可以是非接触式卡的所有者。用户102可以定义用于访问客户端设备104上的移动应用的信任证,该移动应用可以是与非接触式卡的服务提供商相关联的应用。

[0030] 客户端设备104可以包括适合于与物理令牌106进行通信的近场通信读取器110;例如,NFC读取器100可用于从物理令牌106读取计数器值108。

[0031] 在根据本公开的各种示例中,环境100的客户端设备104可以执行一个或多个应用,诸如软件应用。软件应用可以使能与环境100的一个或多个组件进行网络通信并传送和/或接收数据。除了其他计算机可执行的逻辑之外,客户端设备104可以包括客户端验证逻辑112(诸如结合图5更详细地描绘的逻辑)。

[0032] 客户端设备104可以经由一个或多个网络114与一个或多个服务器116通信,并且可以作为与交易验证服务器116进行的相应前端对后端配对来操作。客户端设备104可以例如从在客户端设备104上执行的移动设备应用向服务器116传送一个或多个请求。一个或多个请求可以与从服务器116中检索数据相关联。服务器116可以从客户端设备104接收一个或多个请求。基于来自客户端设备104的一个或多个请求,服务器116可以被配置为从一个或多个数据库(未示出)中检索所请求的数据。基于从一个或多个数据库接收到所请求的数据,服务器116可以被配置为向客户端设备104传送所接收的数据,其中所接收的数据响应于一个或多个请求。

[0033] 环境100可以包括一个或多个服务器116、128。在一些示例中,服务器116、128可以包括耦合到存储器的一个或多个处理器。服务器116、128可以被配置为用于在不同时间控制和调用各种数据以执行多个工作流动作的中央系统、服务器或平台。服务器116、128可以被配置为连接到一个或多个数据库。客户端设备104可以连接到至少一个服务器116、128。

[0034] 在一个实施例中,第三方服务器128可以请求验证交易。例如,第三方服务器128可

以是与售卖产品或服务的供应商相关联的服务器,对于该服务器,以用户102的名义提交购买请求。第三方服务器128可以请求利用服务提供商对购买进行验证。

[0035] 为此,第三方服务器128可以经由网络114与隶属于服务提供商的交易验证服务器116通信。为了验证交易,服务器116可以执行服务器端验证逻辑118(诸如图6所描绘的逻辑)。逻辑118可以维持计数器窗口120,计数器窗口120定义了可接受的计数器值的范围(如上所述,其考虑了计数器值108的意外的读取及其他无意的递增)。计数器窗口120可以包括与不同风险等级相关联的若干不同的范围,诸如针对低风险交易的相对较宽的范围和针对高风险交易的相对较窄的范围(可能需要准确匹配)。

[0036] 计数器值126可以被存储在用户数据库122中,并且可以被索引到与物理令牌106相关联的记录124。当评估存储在用户数据库122中的计数器值126时,逻辑118可以应用计数器窗口120。例如,在接收到新计数器值108时,逻辑118可以将新计数器值108与存储的计数器值126进行比较,以查看新值108是否超过存储值126。如果是的话,逻辑118可以确定新值108是否超出存储值126大于最大窗口值(例如,存储值126和窗口120之和)。如果新值小于存储值126和窗口120的组合,则新值108可被确定为可接受的。如果不是的话,则可以拒绝新值108,并且可以采取进一步的行动(如本文所述)。用户数据库122不必是数据库,但可以是适用于存储与用户102的物理令牌106相关联的计数器值126的任何数据结构。

[0037] 图1B说明了一个或多个非接触式卡130,其可以包括由显示在卡130的正面或背面的服务提供商132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130与支付卡无关,并且可以包括但不限于身份证。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130可以包括基板134,其可以包括由塑料、金属和其他材料组成的单层或者一个或多个叠层。示例性基板材料包括:聚氯乙烯、聚氯乙烯乙酸酯、丙烯腈丁二烯苯乙烯、聚碳酸酯、聚酯类、阳极氧化的钛、钽、金、碳、纸以及生物可降解材料等。在一些示例中,非接触式卡130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130可以具有不同特性,并且本公开不需要在支付卡中实现非接触式卡。

[0038] 非接触式卡130也可以包括:在卡的正面和/或背面显示的识别信息136以及代表物理信令的接触片138。接触片138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、膝上型计算机、台式计算机或平板计算机。非接触式卡130也可以包括处理电路、天线和图1C中未示出的其他组件。这些组件可以位于接触片138的后面或基板134上的其他位置。非接触式卡138也可以包括磁条或磁带,其可以位于卡的背面(图1B中未示出)。

[0039] 如图1C所示,图1B的接触片138可以包括用于存储并处理信息的处理电路140,其包括微处理器142和存储器144。应当理解,处理电路140可以包含附加组件,包括如执行本文所述的功能所必需的处理器、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。

[0040] 存储器144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。只读存储器可以是厂商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

间点进行编程。一旦对存储器进行编程,则可能无法对其进行重写,但可以对其进行多次读取。读/写存储器可以在出厂后进行多次编程和重新编程。读/写存储器也可以被多次读取。

[0041] 存储器144可以被配置为存储一个或多个小应用程序146、一个或多个计数器108以及客户标识符148。一个或多个小应用程序146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 Card小应用程序。然而,应当理解,小应用程序146不限于Java Card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108可以包括足以存储整数的数字式计数器。客户标识符148可以包括被分配给非接触式卡130的用户的唯一字母数字式标识符,并且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148可以识别客户和被分配给该客户的账户两者,并且可以进一步识别与客户的账户相关联的非接触式卡。

[0042] 参照接触片描述了前述示例性实施例的处理器和存储器元件,但是本公开不限于此。应当理解,这些元件可以在片138之外或与片138完全地分离,或者作为除了位于接触片138之内的处理器142和存储器144以外的其他元件来实施。

[0043] 在一些示例中,非接触式卡130可以包括一个或多个天线150。一个或多个天线150可以被放置在非接触式卡130内且在接触片138的处理电路140周围。例如,一个或多个天线150可以与处理电路140构成一体,并且一个或多个天线150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150可以在接触片138和处理电路142的外部。

[0044] 在实施例中,非接触式卡130的线圈可以充当空芯变压器的次级。终端可以通过切断电力或幅度调制来与非接触式卡130通信。非接触式卡130可以使用非接触式卡的电力连接中的间隙来推断从终端传送的数据,其可以通过一个或多个电容器在功能性上维持。非接触式卡130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传。负载调制可以通过干扰在终端的线圈中来检测。

[0045] 如上所述,非接触式卡130可以建立在可在智能卡或具有有限存储器的其他设备(诸如JavaCard)上操作的软件平台上,并且一个或多个应用或小应用程序可以被安全地执行。在各种基于移动应用的使用案例中,可以将小应用程序添加到非接触式卡,以提供一次性密码(OTP)进行多因素身份认证(MFA)。小应用程序可以被配置为: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(NDEF)请求),并产生NDEF消息,该消息包括被编码为NDEF文本标签的加密安全OTP。

[0046] 如上所述,示例性交易可以经由执行在客户端设备104上的逻辑102来验证与非接触式卡相关联的账户的交易请求。图2A-2B描绘了可以响应于逻辑而在客户端设备104上呈现的示例性界面。

[0047] 在显示界面前,可以将交易需要验证通知给客户端104的用户。例如,用户可以从服务提供商接收SMS消息,可以通过服务提供商的应用而接收通知,可以接收呼叫或电子邮件等。

[0048] 在接收到通知时,用户可以登录到服务提供商的应用。用户可以例如提供用户名和口令,这可以验证用户的身份。在其他实施例中,用户可以用其他方式进行验证,诸如通过生物特征数据。在一些实施例中,登录可以利用双因素身份认证(2FA)。

[0049] 当用户登录到应用时,可以向他们呈现界面,诸如图2A中描绘的界面200。在界面

中,可以显示出消息202,消息202指示有问题的交易已经被接收到并需要验证。消息202可以包括交易的细节,诸如交易额、试图验证交易的供应商的名称等。

[0050] 界面200可以包括可交互元件204,如果用户没有授权交易,则可交互元件204允许用户将该交易标记为欺诈性。在选择可交互元件204时,应用可以向交易验证服务器传送欺诈警报消息,其指示讨论中的交易未被认可。

[0051] 如果用户确实授权了交易,则消息202也可以包括用于验证交易的指令。在一个实施例中,如图2B所示,验证交易可以涉及将卡130轻击到客户端设备104的背面上的读取器。读取器可以从卡130上的物理令牌读取计数器值,并且可以生成包括计数器值304和认证密码306的消息300(参见图3)。消息300可以被加密。

[0052] 计数器值304可以对应于最近从卡读取计数器值,并且认证密码306可基于存储在物理令牌138上的密码密钥来生成,并可用于与交易验证服务器认证卡,并确保消息300尚未被篡改或毁坏。

[0053] 消息300也可以包括令牌标识符302,其可以识别卡130和/或与卡相关联的用户。例如,令牌标识符302可以对应于存储在物理令牌138中的唯一客户标识符148。

[0054] 在接收到消息300时,交易验证服务器可以解密消息300,基于密码306来验证卡和消息,基于令牌标识符302将消息与用户账户匹配,并且从对应于用户账户的交易验证服务器中检索用户记录124(参见图1A)。交易验证服务器然后将计数器值304与存储在用户数据库122中的相应计数器值126进行比较,以验证卡上的读取或交易次数与存储在服务器上的预期计数器值相匹配。这可以验证用户持有该卡(即,消息300不是伪造的),并且由用户执行的交易次数与服务提供商的期望相匹配。如果计数器值不同步,这可能指示曾经试图进行未经授权的交易,并可能导致当前交易被拒绝(或者可能导致需要额外的验证操作)。

[0055] 本领域普通技术人员将理解,消息300是以简化格式描绘的。在一些实施例中,其他组件可以存在于消息中,或者所描绘的组件可以被组合或修改。

[0056] 图2C是说明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。系统可以包括非接触式卡130和客户端设备104,客户端设备104可以包括应用(其可以包括逻辑112)和处理器。

[0057] 在步骤202,应用与非接触式卡130通信(例如,在被携带到非接触式卡130附近之后)。应用与非接触式卡130之间的通信可以涉及:非接触式卡130足够靠近客户端设备104的卡读取器(未示出),以使在应用122与非接触式卡130之间能够进行NFC数据传输。

[0058] 在步骤204,在客户端设备104与非接触式卡130之间已经建立了通信之后,非接触式卡130生成消息认证码(MAC)密码。在一些示例中,这可以当应用(例如,在客户端104上)读取非接触式卡130时发生。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,NDEF标签可以根据NFC数据交换格式来创建。例如,诸如应用的读取器可以传送诸如小应用程序选择消息的消息,其具有NDEF产生小应用程序的小应用程序ID。在确认选择时,可以传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130维持的计数器值,其随后可以是“读取NDEF文件”。此时,可以生成可包括报头(header)和共享秘密(shared secret)的消息。然后,可以生成会话密钥。MAC密码可以从消息中创建,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级联,并且可以采用会话密钥对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,并且以NDEF消息格式返回(响应于“读取NDEF文件”消息)。

[0059] 在一些示例中,MAC密码可以作为NDEF标签进行传送,并且在其他示例中,MAC密码可以被包括在统一资源指示符(例如,作为格式化的字符串)内。

[0060] 在一些示例中,应用可以被配置为向非接触式卡130传送请求,该请求包括用于生成MAC密码的指令。

[0061] 在步骤206,响应于来自客户端设备104的指令,非接触式卡130向应用发送MAC密码。

[0062] 在步骤208,应用与处理器传递MAC密码。

[0063] 在步骤210,处理器验证MAC密码。例如,可以解密MAC密码。在一些示例中,可以由除客户端设备104之外的设备(诸如连接到客户端设备104的服务器)执行验证MAC密码。例如,处理器可以输出MAC密码以传输到服务器120,服务器120可以验证MAC密码。

[0064] 图4是描绘客户端设备上的操作系统、客户端设备上的应用、交易验证服务器与处理交易的第三方服务器之间的示例性数据交换的时序图。

[0065] 在402处,第三方服务器(例如,与为其请求信用交易的供应商相关联的服务器)可以向与服务提供商相关联的交易验证服务器提交交易请求。交易请求可以响应于扫描信用卡、将信用卡号键入到供应商的支付系统、与供应商进行在线交易等而生成。服务提供商可以被识别为接收与卡相关的信息的过程的一部分。

[0066] 交易请求可以被传送到交易验证服务器,交易验证服务器可以将风险分析404应用到所请求的交易。风险分析404可以识别与交易相关联的风险级别。例如,风险分析404可以在确定交易是典型的用户活动(因而风险低)还是非典型的的用户活动(因而风险高)时,考虑购买的金额、购买的位置、用户先前的购买历史、整体风险环境(包括诸如发行非接触式卡130的银行等机构是否当前受到攻击,或者其他机构是否报告了最近欺诈增加等因素)等。

[0067] 基于风险分析404,初始风险评分可以被分配给该交易。可以定义一组风险等级,每个风险等级与一系列风险评分和所需的验证动作相关联。例如,对于低风险评分,低风险等级可能不需要验证动作。对于中风险评分,中风险等级可能需要用户通过利用其移动客户端扫描其物理令牌(结合登录到移动客户端上的应用程序)来进行验证。对于高风险评分,高风险等级可能需要中间等级的验证动作与所需的额外验证动作一起。对于极高的风险评分,交易可能会被直接拒绝。

[0068] 可以将初始风险评分与风险等级的风险评分范围进行比较,并将其分配给特定的风险等级。基于与风险等级相关联的验证动作,可以检索并执行关联的验证动作。

[0069] 图4的示例描绘了当初始风险评分与中风险相关联时发生的情况(即,需要通过扫描物理令牌来验证)。相应地,在406处,验证请求由服务器生成并被发送到客户端应用。验证请求可以致使生成通知,告知用户需要验证他们最近的交易。

[0070] 响应于通知,用户可以使用任何合适的手段(例如,用户名/口令组合、生物特征认证等)登录到客户端应用。然后,可以向用户呈现界面(诸如图2A中描绘的界面),并且用户可以扫描他们卡上的物理令牌。相应地,在408处,客户端应用可以从客户端设备的操作系

统请求对物理令牌读取器(例如,NFC读取器)的访问。在410处,客户端OS可以从读取器接收响应(例如,包括计数器值),并且可以将该响应转发到客户端应用。动作408和410可以涉及类似于上文结合图2C所描述的那些动作。

[0071] 在412处,客户端应用可以生成验证响应(例如,消息300),并将该响应传送到交易验证服务器。

[0072] 在414处,交易验证服务器可以执行验证分析。验证分析可以包括验证在验证响应412中包括的密码,并将从客户端接收到的计数器值与存储在服务器处的相应计数器值进行比较。

[0073] 如上所述,存储在物理令牌上的计数器值与存储在交易验证服务器上的计数器值之间的差异可以指示欺诈交易的存在。然而,存储在物理令牌上的计数器值可能出于正当的原因(例如,未传送到服务器的部分读取、OS启动时发生的初始读取等)而变得与存储在服务器上的计数器值不同步。与风险分析相关联的风险等级可以定义从客户端接收到的计数器值与存储在服务器上的计数器值之间的可接受的差异范围。例如,相对较低的风险等级可以提供相对较宽的变化范围,而相对较高的风险等级可以提供相对较窄的范围(甚至没有范围,需要准确匹配)。

[0074] 如果计数器值在可接受的范围内,则处理可以直接进行至426,并且对该交易的许可可以被传送到第三方服务器。

[0075] 除可接受的计数器值范围之外,风险等级可以定义各种升级范围。例如,如果计数器值不在可接受的范围之内但在第二范围之内,则可能需要进一步的验证动作来验证交易。备选地,可以按照来自客户端的计数器值与存储在服务器上的计数器值之间的不匹配来重新评估初始风险评分,并且可以基于新计算的风险评分将交易提升至更高的风险等级。

[0076] 如果计数器值在第二范围之外,则在426处可以拒绝交易。如果由于计数器值在可接受的范围之外而需要进一步的验证动作,则可以执行图4中描绘的虚线动作。

[0077] 为此,在416处,可以将升级验证请求传送到客户端应用。升级验证请求可以包括基于验证分析所需的升级的风险等级或升级的风险动作而要执行的所请求的验证动作。例如,升级验证动作可以涉及回答安全问题、提供生物特征认证、拍摄用户标识的照片或用户亲自出现在规定位置。

[0078] 在该示例中,升级验证请求416请求用户拍摄他们标识的图片,诸如驾照。相应地,在418处,应用可以从客户端操作系统请求访问设备相机。可以捕捉图片,并且在420处,可以将照片传送到客户端应用。基于所捕捉的照片,可以在422处生成升级验证响应,并将其传送到交易验证服务器。

[0079] 在424处,服务器可以对升级验证响应执行升级验证分析。例如,服务器可以将用户标识中的用户照片与存储在服务器处的照片进行比较,或者可以将用户标识上的用户签名与存储的签名进行比较,或者基于升级验证响应的任何其他合适的动作(例如,将生物特征与存储在服务器上的生物特征进行比较,或者接收客户端设备已经确认了生物特征的指示等)。

[0080] 可选地,在428处,服务器可以基于在验证过程期间所确定的信息来更新当前的风险评分。例如,如果计数器值是使得不需要额外的升级验证的值,则服务器可以更新风险评

分以指示风险正在降低。然而,如果需要额外的升级验证,并且额外的验证成功,则可以更新风险评分以维持当前的风险级别。如果认证失败,则可以更新风险级别以指示更高的风险级别。

[0081] 上述动作可以由客户端验证逻辑500(图5)与服务器端验证逻辑600(图6)合作来执行。

[0082] 客户端验证逻辑500可以包括用于在框502处向客户端服务提供商应用认证用户的逻辑。例如,该逻辑可以涉及用于验证用户名和口令的组合、验证生物特征登录信息等的指令。

[0083] 在框504处,可以从交易验证服务器接收到验证请求。验证请求可以指定待验证的交易细节和/或所需的验证动作(诸如,扫描卡的物理令牌)。

[0084] 框502和504可以反向地执行,使得在向应用进行认证之前接收到验证请求。

[0085] 响应于验证请求,在框506处,客户端应用可以调用客户端设备的短距离(例如NFC)读取器。在框508处,读取器可用于与物理令牌交换或读取信息(包括使用一个或多个安全密钥在令牌处加密编码的计数器值)。

[0086] 在框510处,设备可以生成验证响应。这可以包括从508处的令牌读取的加密编码的计数器值。在框512处,验证响应可以被传送到交易验证服务器。

[0087] 如果服务器确定需要升级验证,则在框514处,客户端可以接收升级验证请求,并且可以执行所指定的升级验证动作(例如,捕捉用户标识的照片)。客户端可以使用响应于升级验证动作而捕捉的信息来响应升级验证请求。

[0088] 图6描绘了由验证服务器执行的相应逻辑600。

[0089] 在框502处,验证服务器可以从供应商服务器接收交易请求。交易请求可以指定供应商的身份、交易额以及可以由框604处执行的风险分析所使用的任何其他相关细节。

[0090] 基于风险分析,可以计算初始风险评分,并且可以检索关联的验证动作。在一些情况下,可能不需要验证操作。系统可以在框606处确定是否是这种情况,并且如果不需要验证(例如,由于风险评分低于预定义的低阈值),则处理可以进行至框608,并且交易可以被许可。相应地,可以生成许可消息,并将其传送到供应商服务器。

[0091] 如果需要验证,则在框610处,服务器可以向与被分配给该交易的用户账户相关联的客户端设备传送验证请求(例如,基于从图1A的用户数据库122中检索的信息)。在框612处,服务器可以从客户端接收具有所请求的信息的验证响应。

[0092] 验证响应可被处理为例如认证验证响应中的密码并检索计数器值。在框614处,服务器可以识别由框604中执行的风险分析所确定的风险等级。

[0093] 在该示例中,定义了两个风险等级(高和低)。基于风险等级,可以定义计数器值范围(例如,高风险等级的窄窗口或者低风险等级的宽窗口)。在一些情况下,计数器值范围可以是与风险评分相关联的预定范围。在其他情况下,计数器值范围可以基于风险评分或风险因素(诸如环境的当前风险级别)来动态地确定。可以存在着多个不同的风险等级,每个风险等级具有自身的窗口大小。

[0094] 如果接收到的计数器值在风险等级的指定范围内(在框618或616处为“是”),则处理可以进行至框608,并且交易可以被许可。

[0095] 另一方面,如果计数器值不在风险等级的指定范围内(在框616或618处为“否”),

则处理可以进行至框620。可选地,升级验证可以在该框处执行。作为升级验证过程的一部分,可以计算更新的风险评分,并且可以将风险评分与新的风险等级相匹配。替选地,可以执行为当前风险等级定义的升级验证动作。

[0096] 如果升级验证成功,则处理可以进行至框608,并且交易可以被许可。如果升级验证不成功,或者如果在此阶段没有执行升级验证,则处理可以进行至框622,并且交易可以被拒绝。替选地,如果升级验证不成功,则处理可以返回至框620,并且可以计算其他更新的风险评分。该过程可以重复,直到经过了预定数量的最大迭代,直到风险评分超过预定的最大阈值,或者直到满足预定的停止条件。

[0097] 在该过程期间的任何时刻(例如,在框608和/或622处的许可或拒绝期间),来自认证过程的数据可以被反馈给系统以用作风险计算过程的一部分。因此,可以基于认证/验证过程来更新风险计算,反之亦然。这可以允许系统生成反馈回路,其中认证过程影响风险评估,并且风险评估影响认证过程。

[0098] 上述方法可以体现为计算机可读介质上的指令或体现为计算架构的一部分。图7说明了适用于实施如前所述的各种示例性计算架构700的实施例。在一个实施例中,计算架构700可以包括或被实施为电子设备的一部分,诸如计算机701。实施例不限于在该上下文中。

[0099] 如本申请所使用,术语“系统”和“组件”旨在是指计算机相关实体、硬件、硬件与软件的组合、软件或正在执行中的软件,其示例由示例性计算架构700提供。例如,组件可以是不限于:运行在处理器上的进程、处理器、硬盘驱动器、多个存储驱动器(光和/或磁存储介质)、对象、可执行文件、执行线程、程序和/或计算机。举例来说,运行在服务器上的应用和服务器两者都可以是组件。一个或多个组件可以驻留在进程和/或执行线程内,并且组件可以本地化在一台计算机上和/或分布在两台或更多台计算机之间。此外,组件可以由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递的信号的形式来传递信息。该信息可以被实现为分配给各种信号线的信号。在这种分配中,每条消息都是信号。然而,其他示例可以替选地使用数据消息。这种数据消息可以通过各种连接被发送。示例性连接包括并行接口、串行接口和总线接口。

[0100] 计算架构700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、存储器单元、芯片组、控制器、外围设备、接口、振荡器、定时设备、视频卡、声卡、多媒体输入/输出(I/O)组件、电源等等。然而,实施例不限于由计算架构700实现。

[0101] 如图7所示,计算架构700包括:处理单元702、系统存储器704和系统总线706。处理单元702可以是各种可商购获得的处理器中的任何一种,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;以及类似处理器。双微处理器、多核处理器及其他多处理器架构也可用作处理单元702。

[0102] 系统总线706提供用于系统组件到处理单元702的接口,系统组件包括但不限于系统存储器704。系统总线706可以是若干类型的总线结构中的任何一种,这些总线结构还可

以使用各种可商购获得的总线架构中的任何一种互连到存储器总线(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706。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)工业标准架构(EISA)、微通道架构(MCA)、网络用户总线(NuBus)、外围组件互联(拓展)(PCI(X))、PCI高速(PCI Express)、个人计算机存储卡国际协会(PCMCIA)和诸如此类。

[0103] 计算架构700可以包括或实施各种制造品。制造品可以包括用于存储逻辑的计算机可读存储介质。计算机可读存储介质的示例可以包括:能够存储电子数据的任何有形介质,包括易失性存储器或非易失性存储器,可移动存储器或不可移动存储器、可擦除或不可擦除存储器、可写或可重写存储器等等。逻辑的示例可以包括使用任何合适类型的代码所实施的可执行计算机程序指令,所述代码诸如,源代码、编译代码、解译代码、可执行代码、静态代码、动态代码、面向对象代码、视觉代码和诸如此类。实施例也可以至少部分地被实施为包含在非暂时性计算机可读介质中或其上的,其可以由一个或多个处理器读取并执行以使能执行本文所述的操作。

[0104] 系统存储器704可以包括以一个或多个高速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(DDR)、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)、闪存、诸如铁电聚合物存储器的聚合物存储器、双向存储器、相变或铁电存储器、硅-氧化物-氮化物-氧化物-硅(SONOS)存储器、磁卡或光卡、诸如独立磁盘冗余阵列(RAID)驱动器的设备阵列、固态存储设备(例如,USB存储器、固态驱动器(SSD))以及任何其他类型的适合于存储信息的存储介质。在图7所示的说明性实施例中,系统存储器704可以包括非易失性存储器708和/或易失性存储器710。基本输入/输出系统(BIOS)可以存储在非易失性存储器708中。

[0105] 计算架构700可以包括以一个或多个低速存储器单元的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)712、从可移动磁盘716读取或向其写入的磁软盘驱动器(FDD)714、和从可移动光盘720(例如,CD-ROM或DVD)读取或向其写入的光盘驱动器718。HDD 712、FDD714和光盘驱动器720可以分别由HDD接口722、FDD接口724和光盘驱动器接口726连接到系统总线706。用于外部驱动器实施方式的HDD接口722可以包括通用串行总线(USB)和IEEE 694接口技术中的至少一种或两种。

[0106] 驱动器及相关联的计算机可读介质提供了数据、数据结构、计算机可执行指令等等的易失性存储和/或非易失性存储。例如,多个程序模块(包括操作系统728、一个或多个应用程序730、其他程序模块732和程序数据734)可以存储在驱动器和存储器单元708、712中。在一个实施例中,一个或多个应用程序730、其他程序模块732和程序数据734可以包括例如消息系统500的各种应用和/或组件。

[0107] 用户可以通过一个或多个有线/无线输入设备(例如,键盘736和诸如鼠标738的定点设备)将命令和信息键入到计算机701。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、软件狗(dongle)、指纹读取器、手套、图形平板电脑、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、轨迹板、传感器、触针和诸如此类。这些及其他输入设备常通过耦合到系统总线706的输入设备接口740连接到处理单元702,但是也可以由诸如并行端口、IEEE 694串行端口、游戏端口、USB端口、

IR接口等的其他接口连接。

[0108] 监视器742或其他类型的显示设备经由诸如视频适配器744的接口而连接到系统总线706。监视器742可以在计算机701的内部或外部。除监视器742之外,计算机典型地还包括其他外围输出设备,诸如扬声器、打印机等等。

[0109] 计算机701可以使用经由与一台或多台远程计算机(诸如远程计算机744)的有线和/或无线通信的逻辑连接而在网络化环境中操作。远程计算机744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机701所述的许多或所有的元件,尽管为了简洁的目的,仅示出了存储器/存储设备746。所描绘的逻辑连接包括与局域网(LAN)748和/或例如广域网(WAN)750的更大网络的有线/无线连接。这样的LAN和WAN网络环境在办公室和公司中极为常见,并且促进了企业范围的计算机网络(诸如内部网),所有这些网络都可以连接到全球通信网络(例如,因特网)。

[0110] 当在LAN联网环境中使用时,计算机701可以通过有线和/或无线通信网络接口或适配器752连接到LAN 748。适配器752可以促进与LAN 748的有线和/或无线通信,LAN 748也可以包括在其上设置用于与适配器752的无线功能性进行通信的无线接入点。

[0111] 当在WAN联网环境中使用时,计算机701可以包括调制解调器754,或者连接到WAN 750上的通信服务器,或者具有用于通过WAN 750(诸如借由因特网的方式)建立通信的其他装置。调制解调器754可以是内置或外置的有线和/或无线设备,它经由输入设备接口740连接到系统总线706。在网络化环境中,相对于计算机701或其部分所描绘的程序模块可以存储在远程存储器/存储设备746中。将理解,所示的网络连接是示例性的,并且可以使用建立计算机之间的通信链路的其他装置。

[0112] 计算机701可操作为与使用IEEE 802标准族的有线和无线的设备或实体(诸如,可操作地设置在无线通信(例如,IEEE 802.13空中调制技术)中的无线设备)通信。这除了别的以外至少包括Wi-Fi(或无线保真度)、WiMax和Bluetooth™无线技术。因此,通信可以是与常规网络一样的预定义结构,或者只是在至少两个设备之间的自组织通信(ad hoc communication)。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、连接到因特网以及连接到有线网络(其使用IEEE 802.3相关的介质和功能)。

[0113] 图8是描绘适用于实施前述各种实施例的示例性通信架构800的框图。通信架构800包括各种公共通信元件,诸如发射机、接收机、收发器、无线电、网络接口、基带处理器、天线、放大器、滤波器、电源等等。然而,实施例不限于由通信架构800实现。

[0114] 如图8所示,通信架构800包括一个或多个客户端802和服务器804。客户端可以实现客户端设备510。服务器804可以实现服务器设备526。客户端802和服务器804可操作地连接到一个或多个相应的客户端数据存储库806和服务器数据存储库808,这些客户端数据存储库806和服务器数据存储库808可用于存储相应的客户端802和服务器804的本地信息,诸如缓存文件和/或相关联的上下文信息。

[0115] 客户端802和服务器804可以使用通信框架810在彼此之间传递信息。通信框架810可以实施任何公知的通信技术和协议。通信框架810可以被实施为分组交换网络(例如,诸如因特网的公共网络、诸如企业内部网的专用网络等等)、电路交换网络(例如,公共交换电

话网络),或分组交换网络和电路交换网络的组合(具有合适的网关和转换器)。

[0116] 通信框架810可以实施各种网络接口,这些网络接口被布置为接受、通信和连接到通信网络。网络接口可以被视为输入/输出(I/O)接口的特殊形式。网络接口可采用连接协议,包括但不限于直接连接、以太网(例如,厚、薄、双绞线10/100/1000Base T和诸如此类)、令牌环、无线网络接口、蜂窝网络接口、IEEE 802.8a-x网络接口、IEEE 802.16网络接口、IEEE 802.20网络接口和诸如此类。此外,多个网络接口可用于与各种通信网络类型接合。例如,多个网络接口可用于允许通过广播、多播和单播网络进行通信。如果处理需求指定更大量的速度和容量,则分布式网络控制器架构可以类似地用于池、负载平衡,并以其他方式增加客户端802和服务端804所需的通信带宽。通信网络可以是有线和/或无线网络的任何一个和组合,包括但不限于直接互连、安全定制连接、专用网络(例如,企业内部网)、公共网络(例如,因特网)、个人局域网(PAN)、局域网(LAN)、城域网(MAN)、作为互联网节点的运行任务(OMNI)、广域网(WAN)、无线网络、蜂窝网络和其他通信网络。

[0117] 上述设备的组件和特征可以使用分立式电路、专用集成电路(ASIC)、逻辑门和/或单芯片架构的任何组合来实施。此外,设备的特征可以在合适地适当情况下,使用微控制器、可编程逻辑阵列和/或微处理器或者前述的任何组合来实现。注意,硬件、固件和/软件元件在本文中可以统称或单独称为“逻辑”或“电路”。

[0118] 将理解,上述框图所示的示例性设备可以表示许多潜在实施方式的功能描述性示例。相应地,附图中描绘的框功能的划分、省略或包括并非暗示用于实施这些功能的硬件组件、电路、软件和/或元件将必然会在实施例中划分、省略或包括。

[0119] 至少一个计算机可读存储介质可以包括指令,该指令在被执行时,致使系统执行任何本文所述的计算机实施方法。

[0120] 一些实施例可以使用表述“一个实施例”或“实施例”及其衍生词来描述。这些术语意味着结合实施例描述的特定特征、结构或特性被包括在至少一个实施例中。在说明书中各个地方出现的短语“在一个实施例中”不一定全都是指同一实施例。此外,除非另有说明,否则上述特征被认为能以任何组合一起使用。因此,任何单独讨论的特征可以彼此组合地使用,除非注意到这些特征彼此不相兼容。

[0121] 主要参照本文所使用的符号和命名,本文的详细描述可以依据在计算机或计算机网络上执行的程序过程来呈现。这些过程性描述和表示由本领域技术人员使用以将它们工作的实质最有效地传达给向本领域其他技术人员。

[0122] 这里的过程一般被构思为导致期望结果的自洽序列的操作。这些操作是那些需要对物理量进行物理操控的操作。虽然不是必须的,但是通常这些物理量采取能够被存储、传输、组合、比较和以其他方式操控的电、磁或光信号的形式。主要是出于习惯用语的原因,有时将这些信号称为比特、数值、元件、符号、字符、术语、数字等经证明是方便的。然而,应当注意,所有的这些和类似术语都与适当的物理量相关联,并且仅仅是应用于那些量的方便标记。

[0123] 此外,执行的操控经常以诸如添加或比较之类的术语指代,这常与人工操作员执行的心理操作相关联。在本文所述的形成一个或多个实施例的一部分的任何操作中,人类操作员的这种能力不是必需的,或者在大多数情况下不是可取的。相反,这些操作是机器操作。用于执行各种实施例的操作的有用机器包括通用数字计算机或类似的设备。

[0124] 一些实施例可以使用表述“耦合”和“连接”及其衍生词来描述。这些术语不一定旨在作为彼此的同义词。例如，一些实施例可以使用术语“连接”和/或“耦合”来描述，以指示两个或更多个元件彼此直接物理或电接触。然而，术语“耦合”也可以意味着两个或更多个元件彼此不直接接触，但还仍然彼此协作或作用。

[0125] 各种实施例也涉及用于执行这些操作的装置或系统。这种装置可以被特殊地构造用于所需的目的，或者它可以包括如由存储在计算机中的计算机程序选择性地激活或重新配置的通用计算机。本文所呈现的过程并非固有地涉及特定的计算机或其他装置。各种通用机器可以与根据本文教导编写的程序一起使用，或者它可以证明构造更专用的装置以执行所需的方法步骤是方便的。各种这些机器所需的结构将从给出的描述中出现。

[0126] 需要强调的是，提供本公开的摘要是为了允许读者快速确定本技术公开的实质。提交本摘要基于这样的理解，即本摘要将被不用于解释或限制权利要求的范围或含义。另外，在前面的详细描述中，可以看出，为了精简本公开的目的，各种特征在单个实施例中组合在一起。本公开的方法并非要被解释为反映所要求保护的实施例需要比每项权利要求中所明确叙述的内容更多特征的意图。相反，如以下权利要求反映，发明性主题在于要少于单个所公开的实施例的所有特征。因此，以下权利要求特此并入详细描述，其中每项权利要求其本身作为单独的实施例。在所附权利要求中，术语“包括(including)”和“其中(in which)”分别用作相应的术语“包括(comprising)”和“其中(wherein)”的简明英语等同物。此外，术语“第一”、“第二”、“第三”等仅用作标记，并非旨在对其对象强加数字要求。

[0127] 上文已经描述的内容包括所公开的架构的示例。当然，不可能描述组件和/或方法中的每个可想象到的组合，但是本领域普通技术人员可以认识到，许多其他组合和排列是可能的。因此，该新颖架构旨在涵盖落入所附权利要求的精神和范围内的所有此类替换、修改和变型。

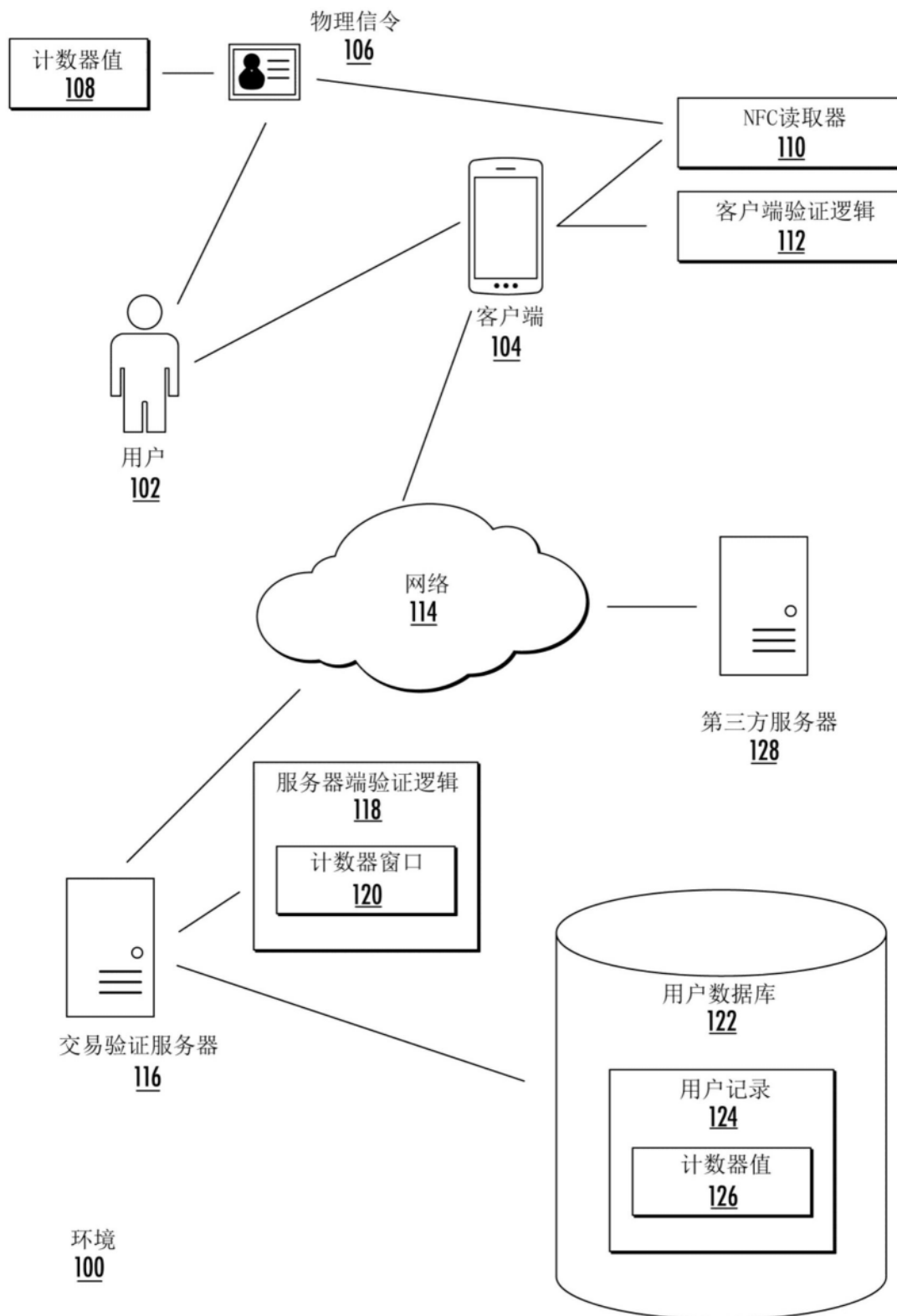


图1A

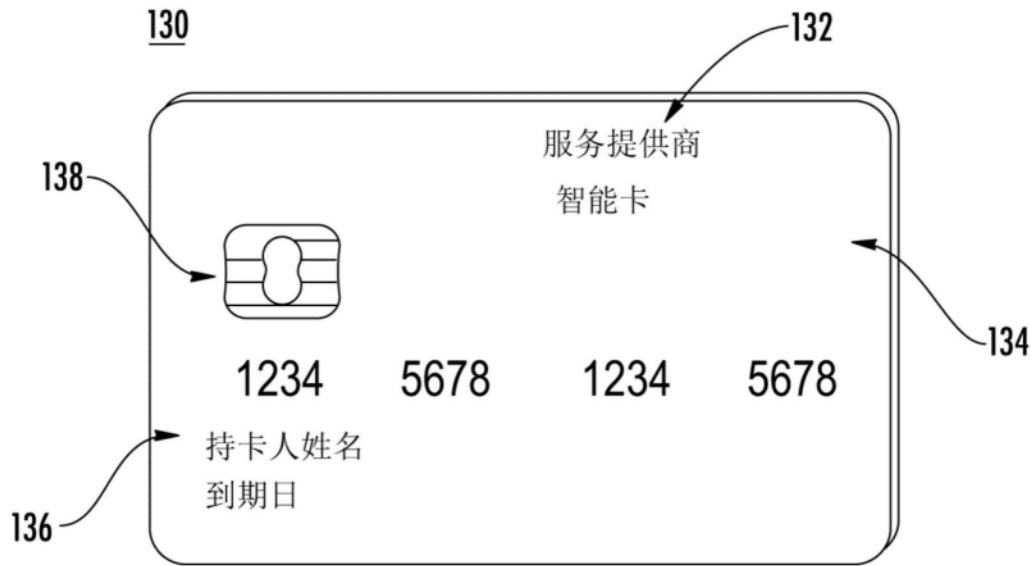


图1B

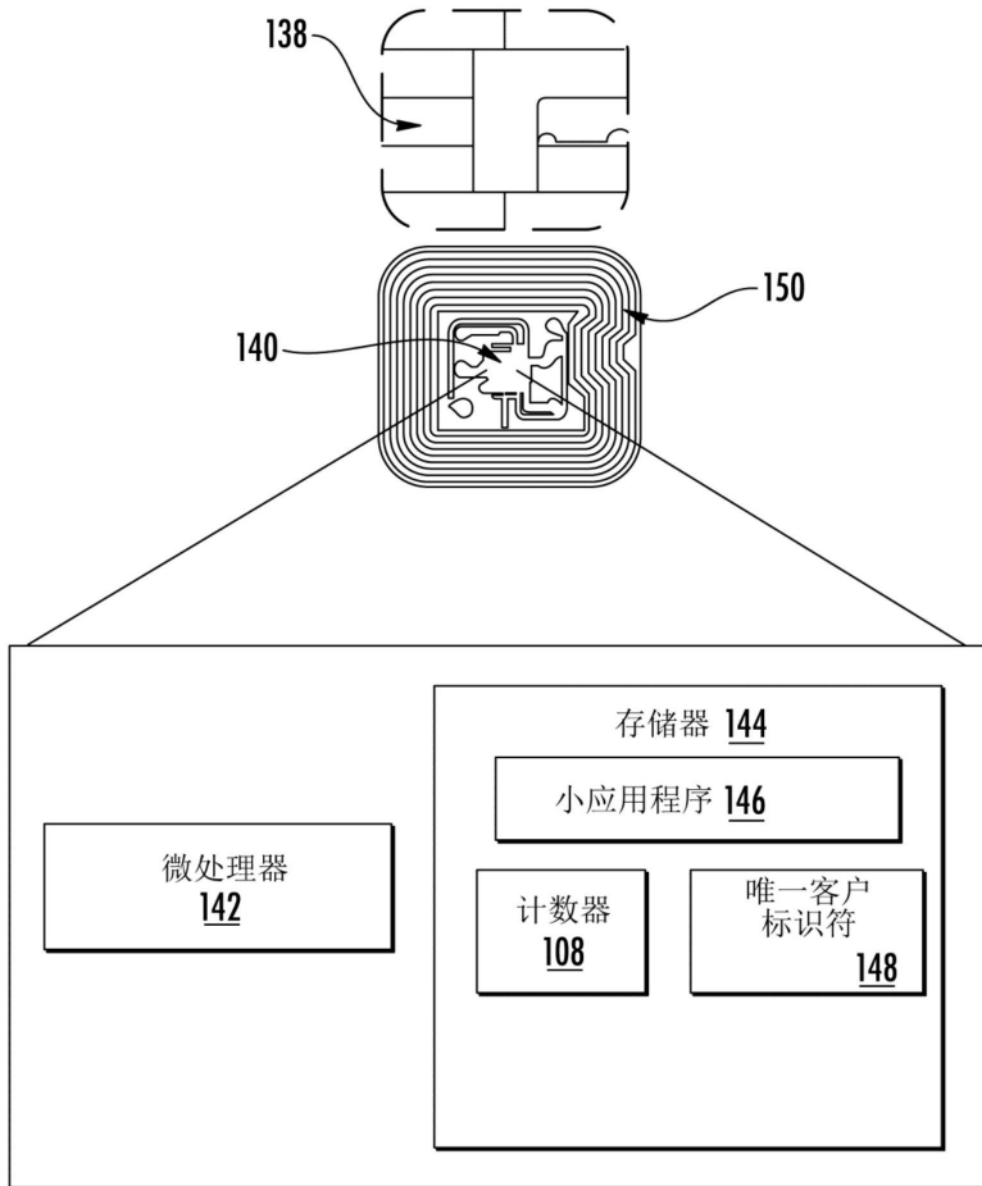


图1C





界面
200

图2B

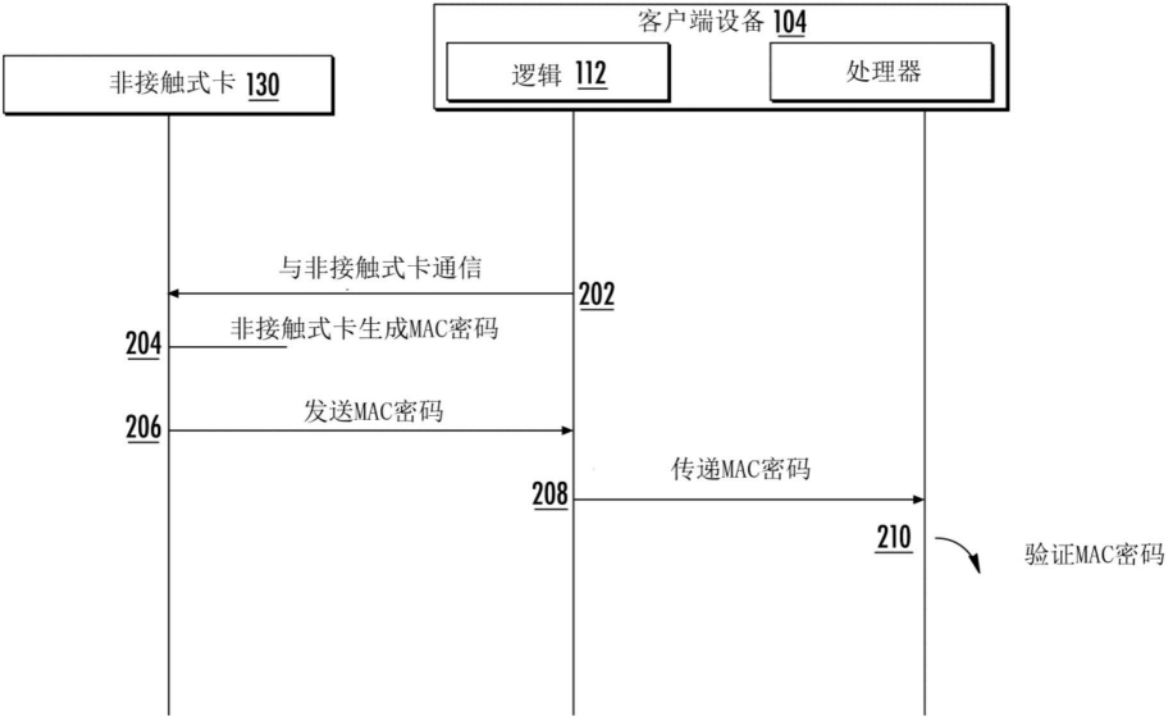


图2C

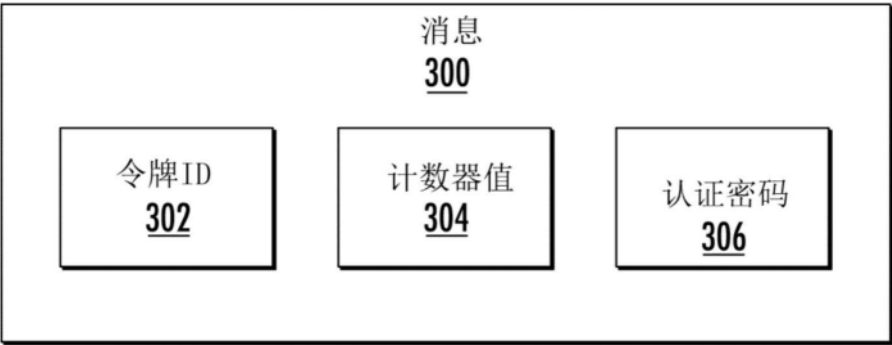


图3

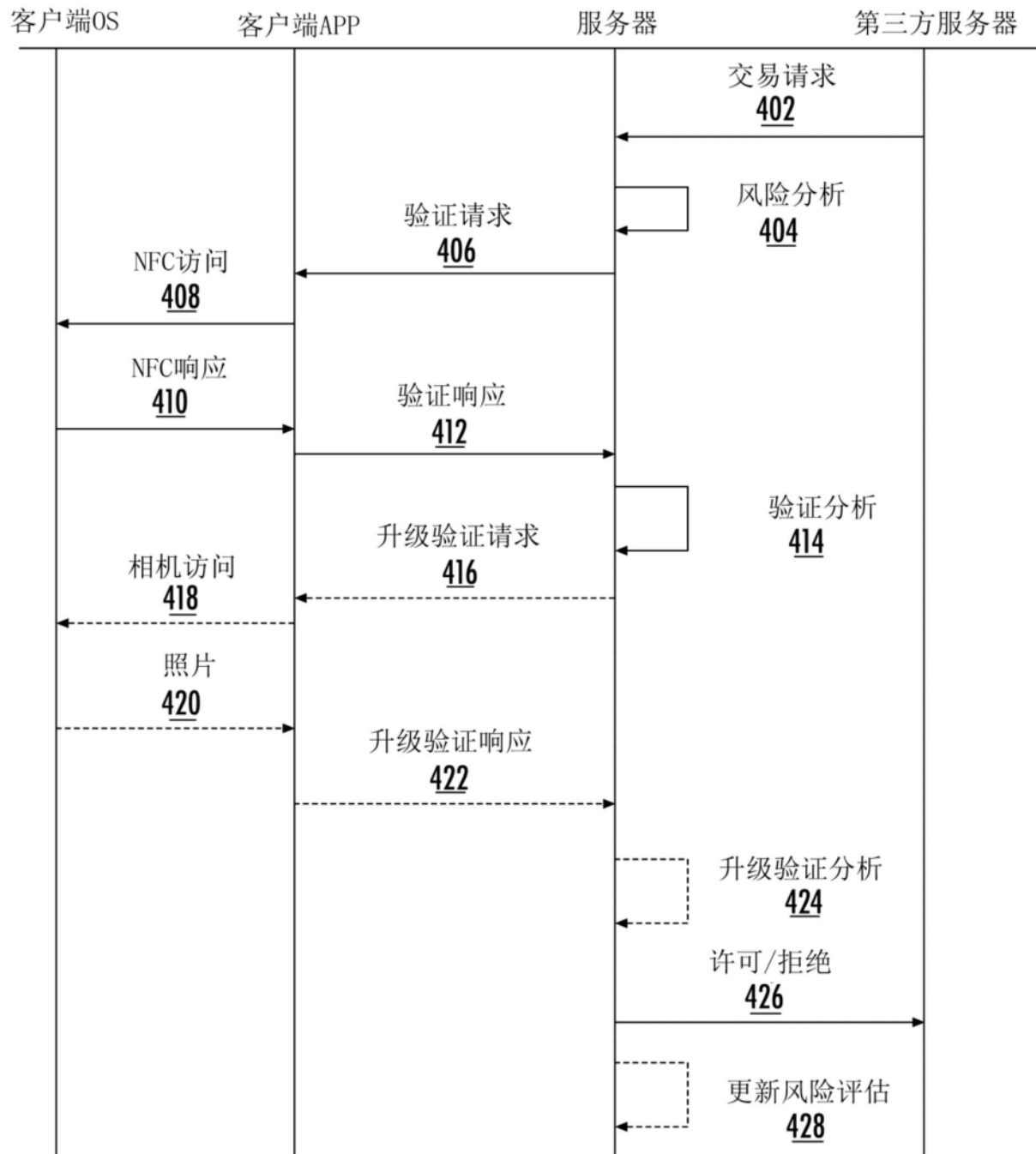


图4

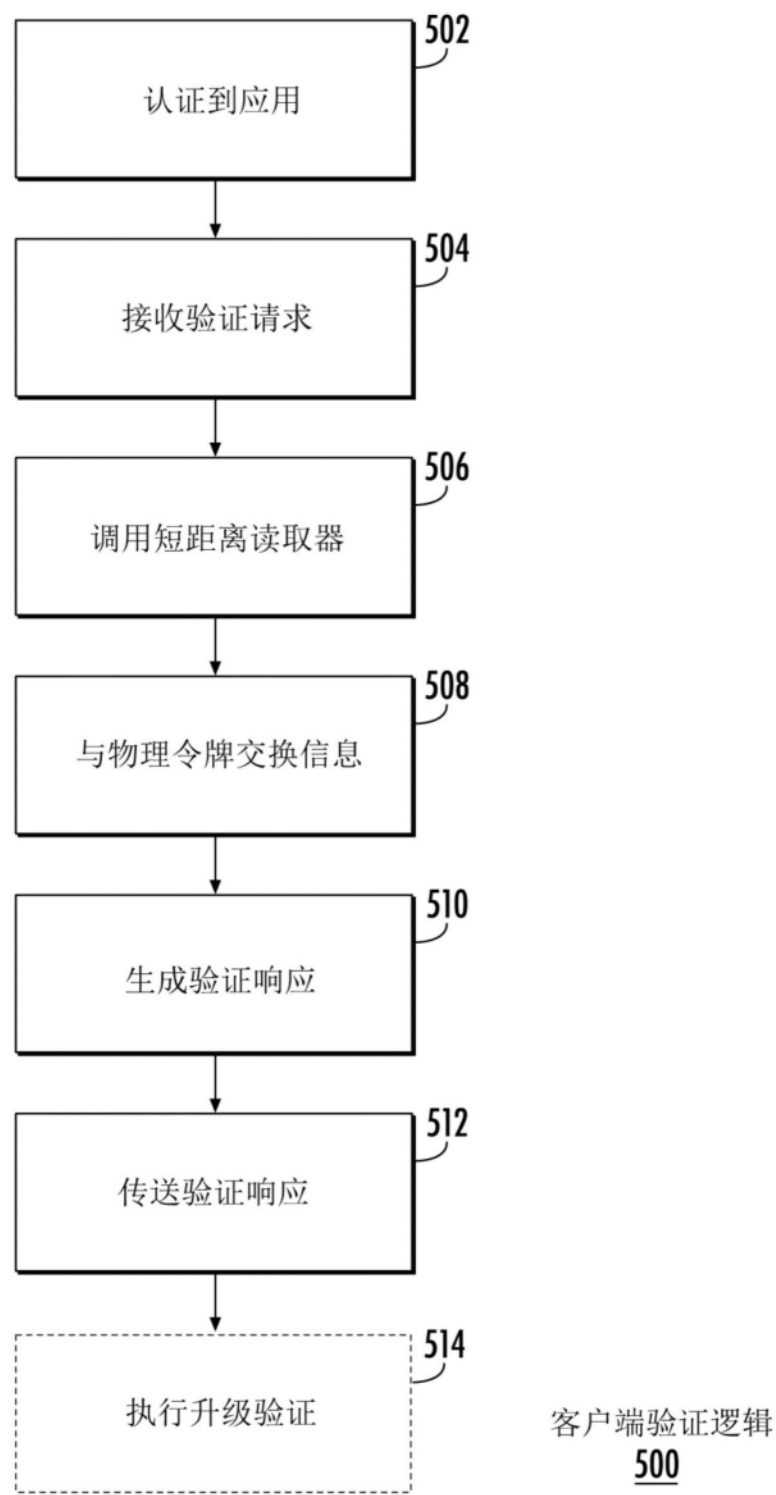


图5

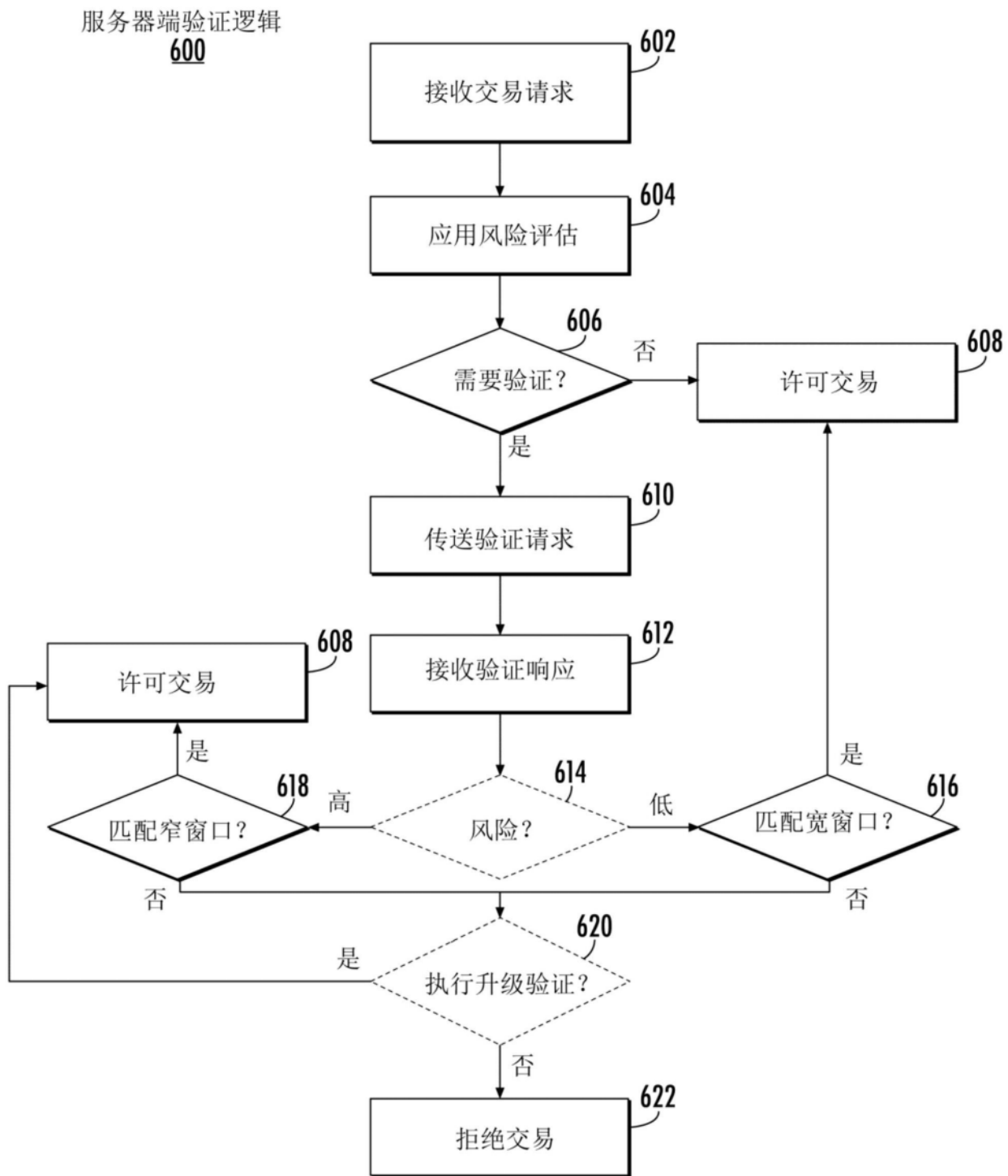


图6

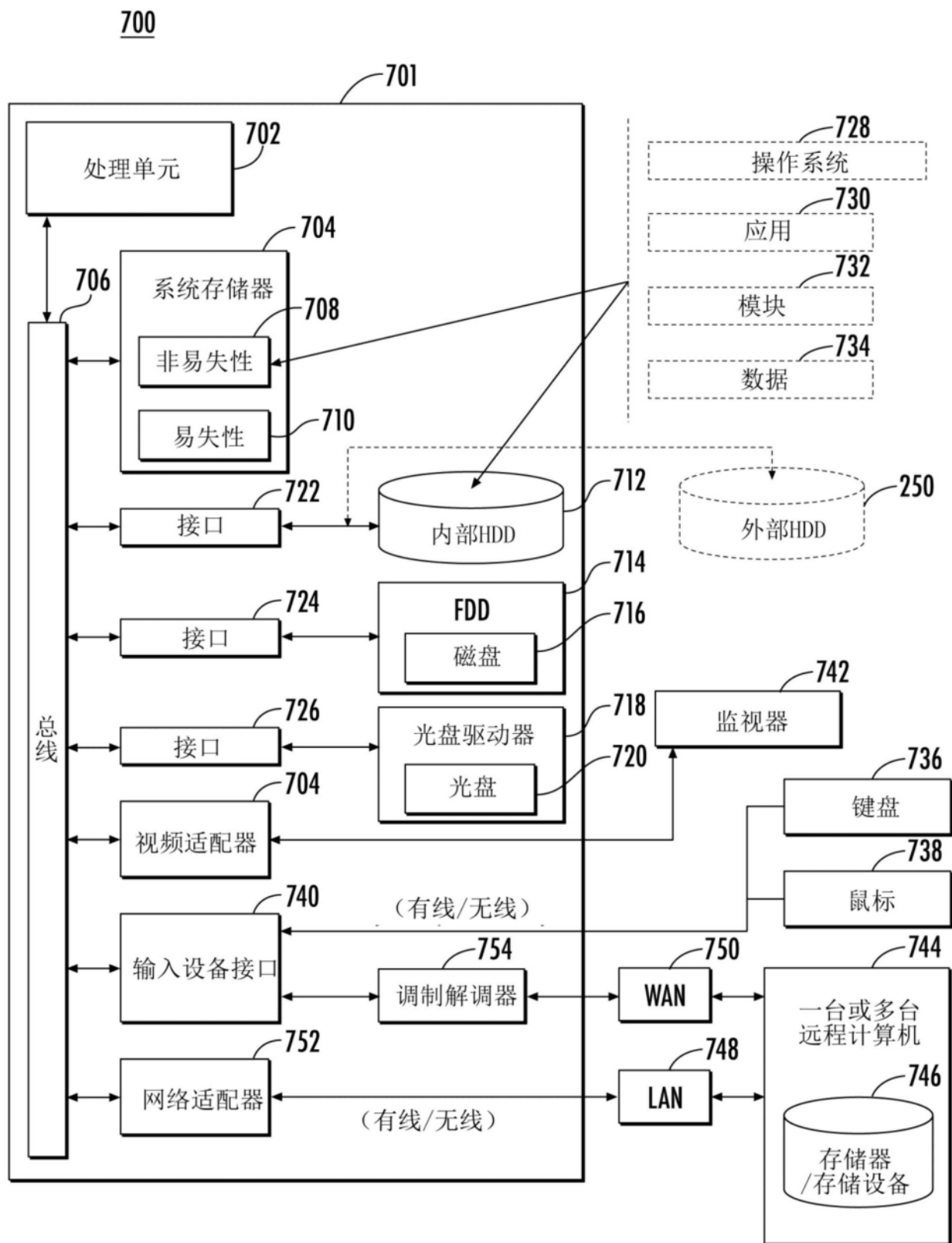


图7

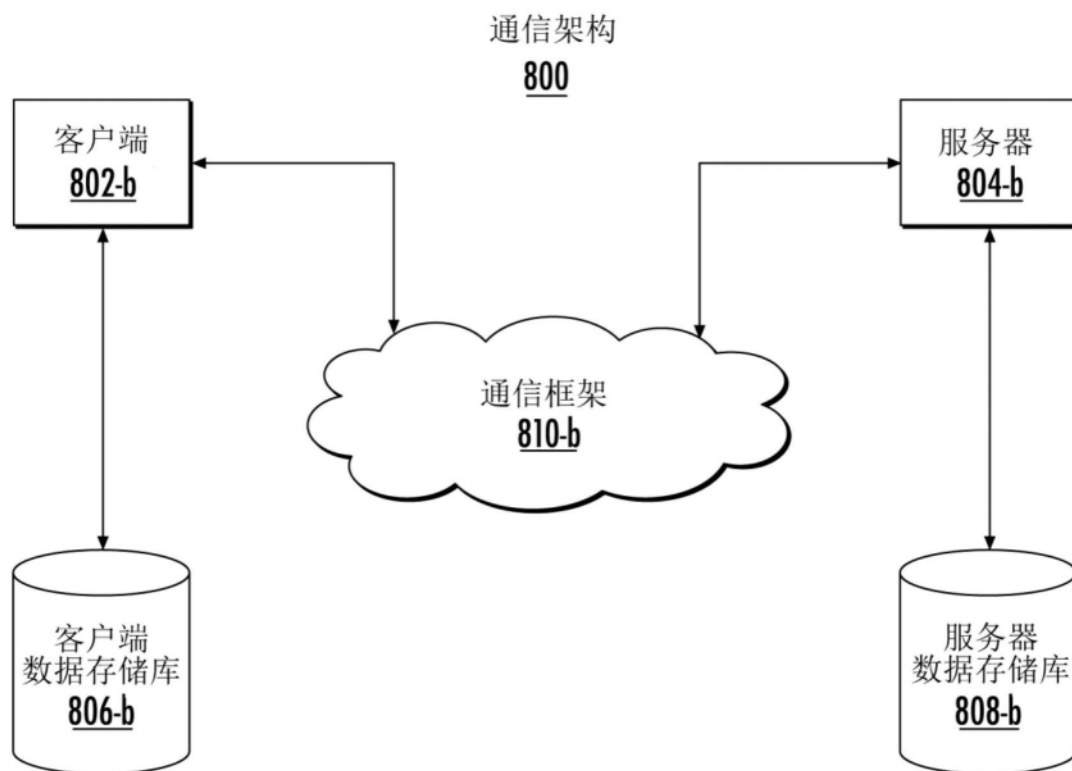


图8