(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114697124 A
(43)申请公布日 2022.07.01

(21)申请号 202210374872.9

(22)申请日 2018.11.28

(30)优先权数据
62/591,708 2017.11.28 US

(62)分案原申请数据
201880076718.5 2018.11.28

(71)申请人 维萨国际服务协会
地址 美国加利福尼亚州

(72)发明人 B·沙利文 Q·王 陈悦玺
C·阿艾拜 C·弗卢夏姆
P·哈普拉基

(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 徐倩 周全

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 67/75(2022.01)
H04W 4/80(2018.01)
H04W 12/122(2021.01)
G07F 15/00(2006.01)
G06Q 20/20(2012.01)
G06Q 20/38(2012.01)
G06Q 20/32(2012.01)
G06Q 20/40(2012.01)
G06Q 20/42(2012.01)

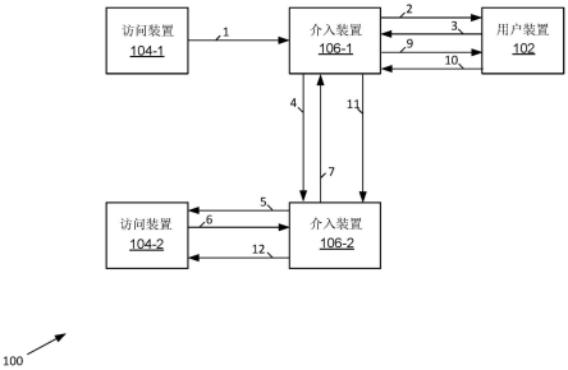
权利要求书3页 说明书22页 附图12页

(54)发明名称

用于防范中继攻击的系统和方法

(57)摘要

公开了用于防止中继攻击的系统、方法和装置。用户装置可以从介入装置接收(例如,当接近第一访问装置时)用于第一访问装置的装置标识数据。可以经由所述介入装置从第二访问装置接收消息。所述消息可以包括至少部分地基于第二访问装置标识数据生成的数字签名。所述用户装置可以利用所述数字签名和公钥验证所述消息。如果所述消息是无效的,那么所述用户装置可以丢弃所述消息。如果所述消息是有效的(例如,未改变),那么所述用户装置可以确定所述用户尚未确认与所述第二访问装置交互的意图,且因此可以终止与所述第二访问装置的进一步交互。



CN 114697124 A

1.一种方法,包括:

由第一访问装置从介入装置接收对应于连接请求的第一消息;

由所述第一访问装置生成对应于交互的交互数据,所述交互数据包括与所述第一访问装置相关联的访问装置标识数据,以及使用所述访问装置标识数据和与所述第一访问装置相关联的私钥生成的数字签名;

由所述第一访问装置生成包括所述交互数据的第二消息;以及

由所述第一访问装置发送所述第二消息,所述第二消息包括所述交互数据,所述第二消息经由所述介入装置发送到接近第二访问装置的用户装置,其中所述用户装置基于所述交互数据和所述数字签名来验证所述第二消息。

2.根据权利要求1所述的方法,其中所述介入装置为第一介入装置,并且其中所述交互数据经由所述第一介入装置和第二介入装置从所述第一访问装置发送到所述用户装置。

3.根据权利要求1所述的方法,其中所述交互数据包括对应于所述第一访问装置与所述用户装置之间的所述交互的值。

4.根据权利要求1所述的方法,其中所述第一访问装置和所述第二访问装置是自动加油机。

5.根据权利要求1所述的方法,其中所述交互数据还包括与所述第一访问装置相关联的位置。

6.根据权利要求1所述的方法,其中所述用户装置和所述介入装置是经由短程无线通信协议以通信方式连接的。

7.根据权利要求1所述的方法,其中所述交互数据还包括与所述第一访问装置相关联且对应于与所述第一访问装置相关联的所述私钥的公钥,并且其中所述方法还包括:

由所述第一访问装置经由所述介入装置从所述用户装置接收包括所述交互数据的一部分的第三消息;

由所述第一访问装置至少部分地基于所述交互数据的包括于所述第三消息中的所述部分来确定所述第三消息是否无效;以及

基于确定所述第三消息无效而终止对所述第三消息的处理。

8.根据权利要求7所述的方法,其中所述第二消息还包括与所述第一访问装置相关联的所述公钥,并且其中确定所述第二消息是否无效还包括将在所述第一消息中发送的所述公钥与从所述第二消息获得的额外公钥进行比较。

9.根据权利要求7所述的方法,其中所述第三消息包括由所述用户装置生成的第二数字签名和与所述用户装置相关联的证书,并且其中确定所述第三消息是否无效还包括:

从所述第三消息获得与所述第一访问装置相关联的所述公钥;

从所述证书获得与所述用户装置相关联的对应公钥;以及

验证使用与所述用户装置相关联的所述公钥从所述第三消息获得的与所述第一访问装置相关联的所述公钥与所述第一消息中提供的所述公钥不匹配。

10.根据权利要求1所述的方法,其中所述用户装置基于以下操作验证所述第一消息:

从所述第二消息获得由所述第一访问装置提供的公钥;

使用从所述第二消息获得的所述公钥从所述第二消息的所述数字签名获得第一散列值;

从所述交互数据生成第二散列值;以及

将所述第一散列值与所述第二散列值进行比较,其中当所述第一散列值和所述第二散列值匹配时,所述第二消息被确定为有效的。

11.一种访问装置,包括:

一个或多个处理器;以及

计算机可读存储介质,其包括指令,所述指令在由所述一个或多个处理器执行时使所述访问装置:

从介入装置接收对应于连接请求的第一消息;

生成对应于交互的交互数据,所述交互数据包括与所述访问装置相关联的访问装置标识数据,以及使用所述访问装置标识数据和与所述访问装置相关联的私钥生成的数字签名;

生成包括所述交互数据的第二消息;以及

发送包括所述交互数据的所述第二消息,所述第二消息经由所述介入装置发送到接近第二访问装置的用户装置,其中所述用户装置基于所述交互数据和所述数字签名来验证所述第二消息。

12.根据权利要求11所述的访问装置,其中所述用户装置至少部分地基于所述第二消息中提供的所述交互数据的公钥相对于与所述第二访问装置相关联的先前存储的公钥来验证所述第二消息。

13.根据权利要求11所述的访问装置,其中执行所述指令还使所述访问装置:

经由所述介入装置从所述用户装置接收第三消息,所述第三消息包括对应于所述用户装置的第一位置;以及

至少部分地基于确定对应于所述用户装置的所述第一位置在到对应于所述访问装置的第二位置的阈值距离之外而确定所述第三消息无效。

14.根据权利要求11所述的访问装置,其中与所述访问装置相关联的所述私钥是由所述访问装置生成的用于所述访问装置与所述用户装置之间的所述交互的公钥/私钥对的一部分。

15.一种方法,包括:

由用户装置从介入装置接收用于第一访问装置的第一访问装置标识数据;

由接近所述第一访问装置的所述用户装置经由所述介入装置从第二访问装置接收消息,所述消息包括消息数据,所述消息数据包括至少第二访问装置标识数据,以及通过用与所述第二访问装置相关联的公钥/私钥对的私钥来签署所述至少第二访问装置标识数据的散列而产生的数字签名;

由所述用户装置至少部分地基于所述第二访问装置标识数据和所述数字签名来确定所述消息是否无效;以及

当所述消息无效时,由所述用户装置自动终止与所述第二访问装置的任何进一步交互。

16.根据权利要求15所述的方法,其中所述消息数据还包括与所述第二访问装置相关联的公钥。

17.根据权利要求16所述的方法,其中确定所述消息无效还包括:

由所述用户装置使用所述公钥从所述数字签名获得所述散列；

由所述用户装置生成所述消息数据的第二散列;以及

由所述用户装置将所述散列与所述第二散列进行比较。

18.根据权利要求15所述的方法,还包括：

由所述用户装置在与所述第一访问装置交互的请求中向所述用户装置的用户呈现所述第一访问装置标识数据;以及

由所述用户装置从所述用户接收所述用户想要与所述第一访问装置交互的确认。

19.根据权利要求15所述的方法,当所述消息有效时：

由所述用户装置在与所述第二访问装置交互的后续请求中向所述用户装置的用户呈现所述第二访问装置标识数据;以及

由所述用户装置接收所述用户装置的所述用户想要与所述第二访问装置交互的额外确认。

20.根据权利要求15所述的方法,其中所述介入装置是经由短程无线通信协议与所述用户装置以通信方式连接的。

用于防范中继攻击的系统和方法

[0001] 本申请是国际申请日为2018-11-28,国际申请号为PCT/US2018/062759,进入中国国家阶段的申请号为201880076718.5,题为“用于防范中继攻击的系统和方法”的发明专利申请的分案申请。

[0002] 本申请案要求2017年11月28日提交的第62/591,708号美国临时申请案的优先权,所述美国临时申请案的公开内容出于所有目的以全文引用的方式并入本文中。

背景技术

[0003] 在接触访问交易以及例如非接触装置与非接触终端之间的支付交易等非接触访问交易中,中继攻击是可能的。举例来说,攻击者(例如,一个或多个人一起合作来盗窃信息或诈骗合法用户)可使用两个具有无线功能的移动装置以及所述具有无线功能的移动装置上的两个移动应用程序来进行中继攻击。在典型中继攻击中,攻击者使用具有第一移动应用程序的第一移动装置来与受害者的口袋中的非接触装置轻触和通信。攻击者可使用具有第二移动应用程序的第二移动装置来与例如在商家或其它资源提供商处的非接触终端轻触和通信。

[0004] 由非接触终端发出的命令消息是从第二移动装置中继到第一移动装置的,且随后由受害者的非接触装置接收。受害者的非接触装置随后对命令消息做出响应。装置上的访问信息(例如,例如主账号(PAN)等支付信息)可以随后从第一移动装置中继到第二移动装置,然后到达非接触终端。通过执行此中继攻击,攻击者可使用受害者的非接触装置进行访问交易(例如,购买交易)而无需取得受害者的装置的控制权。虽然此特定实例是涉及商家的一个实例,但是应了解,此问题可存在于期望访问资源的其它情形中(例如,进入建筑物的尝试,或访问计算机内部的数据的尝试)。

[0005] 使用低功耗蓝牙(Bluetooth Low Energy,BLE)在非接触装置与非接触终端之间通信的移动交易通常在装置与终端之间极为接近的情况下发生。然而,这些交易仍容易受到中继攻击。

[0006] 本文描述的实施例个别地且共同地解决了这些问题。

发明内容

[0007] 本公开的一个实施例是针对一种方法。所述方法可以包括由用户装置从介入装置接收用于第一访问装置的第一访问装置标识数据。所述方法还可以包括由接近第一访问装置的用户装置经由所述介入装置从第二访问装置接收消息。在一些实施例中,所述消息可以包括消息数据,所述消息数据包括至少第二访问装置标识数据以及通过用与第二访问装置相关联的公钥/私钥对的私钥签署所述至少第二访问装置标识数据的散列而产生的数字签名。所述方法还可以包括使用公钥从所述数字签名获得所述散列。所述方法还可以包括生成消息数据的额外散列。所述方法还可以包括由用户装置将所述散列与额外散列进行比较。所述方法还可以包括由用户装置确定所述散列是否匹配额外散列。所述方法还可以包括当所述散列不匹配额外散列时由用户装置自动终止与第二访问装置的任何进一步交互。

所述方法还可以包括当所述散列匹配额外散列时：确定所述用户装置的用户尚未确认与第二访问装置交互的意图，且至少部分地基于确定所述用户尚未确认与第二访问装置交互的意图而终止与第二访问装置的任何进一步交互。

[0008] 本公开的另一实施例是针对一种用户装置。在一些实施例中，所述用户装置可以包括处理器和非瞬态计算机可读介质。在一些实施例中，所述计算机可读介质可以包括可由处理器执行以用于实施本文所描述的任何方法的代码。

[0009] 本公开的另一实施例是针对一种系统。所述系统可以包括至少一个用户装置和至少一个访问装置。在一些实施例中，所述用户装置和/或访问装置可以包括处理器和非瞬态计算机可读介质。在一些实施例中，所述计算机可读介质可以包括可由处理器执行以用于实施本文所描述的任何方法的代码。

附图说明

[0010] 图1是示出根据一些实施例的示例性中继攻击的框图。

[0011] 图2示出根据一些实施例的用于建立到访问装置的连接的示例性用户界面。

[0012] 图3示出根据一些实施例的用于确认与访问装置的交互的示例性用户界面。

[0013] 图4示出根据一些实施例的示出用于防止中继攻击的示例性方法的框图。

[0014] 图5示出根据一些实施例的示出用于生成数字签名的示例性方法的示意图。

[0015] 图6示出根据一些实施例的示出用于防止中继攻击的另一示例性方法的框图。

[0016] 图7示出根据一些实施例的示出用于防止中继攻击的又一示例性方法的框图。

[0017] 图8示出根据一些实施例的示出用于防止中继攻击的又一示例性方法的框图。

[0018] 图9示出根据一些实施例的示出用于防止中继攻击的再一个示例性方法的框图。

[0019] 图10示出根据本发明的实施例的示例性用户装置的框图。

[0020] 图11示出根据本发明的实施例的示例性访问装置的框图。

[0021] 图12示出示出交易处理系统的框图。

[0022] 图13示出示出建筑物访问系统的框图。

具体实施方式

[0023] 低功耗蓝牙(BLE)是在大多数现代智能电话中可用的通信技术。BLE技术已经用于移动支付。潜在地使得对于低摩擦交互具有吸引力的BLE的特征在于，在装置(例如访问装置和用户的电话)之间建立连接是容易的。举例来说，当将一个装置连接到另一装置时，不需要像传统蓝牙的情况那样交换PIN或密码。

[0024] 然而，用户装置中的BLE能力的广泛可用性以及在用户装置与访问装置之间建立BLE连接的简单性不利地助长了欺诈者开发可模仿BLE访问装置的移动应用程序的期望。在应用程序协议级别无保护的情况下，欺诈者有可能执行中继攻击。举例来说，欺诈者可以模仿用户装置正尝试与之交互的访问装置，且可以说服用户装置的用户连接到欺诈性装置而不是访问装置。并非与本地真实的访问装置通信，欺诈者可以建立延伸到远程访问装置处的同伙的通信信道，且与欺诈者的装置一起可以操纵通信协议以使用户无意地与远程访问装置交互而不是与用户希望的访问装置交互。

[0025] 在论述本发明的特定实施例之前，可详细地描述一些术语。

[0026] “用户装置”可以包括用户可以运送和操作的任何合适的电子装置，所述装置还可提供与网络远程通信的能力。远程通信能力的实例包括使用移动电话(无线)网络、Bluetooth®、Bluetooth Low Energy®(BLE)、无线数据网络(例如，3G、4G或相似网络)、Wi-Fi、Wi-Max，或可以提供对例如因特网或专用网络等网络的访问的任何其它通信介质。用户装置的实例包括移动电话(例如，蜂窝式电话)、PDA、平板计算机、上网本、膝上型计算机、个人音乐播放器、手持式专用读取器等。用户装置的其它实例包括可穿戴装置，例如智能手表、健身手环、踝链、戒指、耳环等，以及具有远程通信能力的汽车。用户装置可以包括用于执行此类功能的任何合适硬件和软件，且还可包括多个装置或组件(例如，当装置通过网络共享到另一装置--即将另一装置用作调制解调器--而能够远程访问网络时，联系在一起的两个装置可被认为是单个用户装置)。

[0027] “交互数据”可以包括与访问装置与用户装置之间的交互相关联的任何合适的信息。交互数据可以包括与交互相关联的任何合适的数据(例如，BLE广告消息、购买和/或预授权交易等)。在一些实施例中，交互数据可以包括以下各项的任何合适的组合：与访问装置相关联的标识数据(例如，访问装置的一个或多个标识符)，与用户装置相关联的标识信息(例如，与用户装置相关联的一个或多个标识符)，交互值(例如，交易金额，例如交易的预授权金额和/或购买价格)，支付数据(例如，与支付账户相关联的支付账户标识符)，各自与访问装置和/或用户装置相关联的一个或多个位置，或任何合适的信息。支付数据的实例可以包括PAN(主账号或“账号”)、用户名、到期日期、CVV(卡验证值)、dCVV(动态卡验证值)、CVV2(卡验证值2)、CVC3卡验证值等。CVV2通常被理解为是与支付装置相关的静态验证值。CVV2值通常对用户(例如，消费者)可见，而CVV和dCVV值通常嵌入存储器或授权请求消息中，用户不容易知道(尽管它们对发行方和支付处理器是已知的)。支付数据可以是标识支付账户或与支付账户相关联的任何信息。可以提供支付数据以便从支付账户进行支付。支付数据还可以包括用户名、到期日期、礼品卡号或代码以及任何其它合适的信息。

[0028] “应用程序”可以是存储在计算机可读介质(例如，存储器元件或安全元件)上的计算机代码或其它数据，所述计算机代码或其它数据可由处理器执行以完成任务。

[0029] “用户”可以包括个人。在一些实施例中，用户可与一个或多个个人账户和/或移动装置相关联。用户还可以称为持卡人、账户持有人或消费者。

[0030] “资源提供商”可以是可以提供例如商品、服务、信息和/或访问等资源的实体。资源提供商的实例包括商家、访问装置、安全数据访问点等。“商家”通常可以是参与交易并且可以出售商品或服务或提供对商品或服务的访问的实体。

[0031] “收单方”通常可以是与特定商家或其它实体具有商业关系的商业实体(例如，商业银行)。一些实体可以执行发行方和收单方两者的功能。一些实施例可以涵盖此类单个实体发行方-收单方。收单方可以操作收单方计算机，其也可一般称为“传输计算机”。

[0032] “授权实体”可以是授权请求的实体。授权实体的实例可以是发行方、政府机构、文档存储库、访问管理员等。“发行方”通常可以指代维持用户的账户的商业实体(例如，银行)。发行方也可以向消费者发行存储在例如蜂窝电话、智能卡、平板计算机或膝上型计算机等用户装置上的支付凭证。

[0033] “访问装置”可以是提供对远程系统的访问的任何合适的装置。访问装置还可用于与用户装置、资源提供商计算机、处理网络计算机、授权实体计算机和/或任何其它合适的

系统通信。访问装置一般可以位于任何合适位置，例如在商家的位置，或作为另一实例在建筑物的入口位置处。访问装置可以呈任何合适的形式。访问装置的一些实例包括POS或销售点装置(例如，POS终端)、蜂窝电话、PDA、个人计算机(PC)、平板PC、手持式专用读取器、机顶盒、电子现金出纳机(ECR)、自动柜员机(ATM)、虚拟现金出纳机(VCR)、营业亭、安全系统、访问系统等等。访问装置可使用任何合适的接触或非接触操作模式，以向用户装置发送或从其接收数据或者与用户装置相关联。在一些实施例中，访问装置可以被配置成至少部分地基于例如Bluetooth®和/或BLE等短程通信协议与用户装置通信。在一些实施例中，访问装置可以还被配置成利用任何合适的有线和/或无线网络来与资源提供商计算机、处理网络计算机、授权实体计算机和/或任何其它合适的系统通信。在访问装置可以包括POS终端的一些实施例中，可以使用任何合适的POS终端且其可以包括读取器、处理器和计算机可读介质。读取器可以包括任何合适的接触或非接触操作模式。例如，示例性读取器可以包括射频(RF)天线、光学扫描器、条形码读取器或磁条读取器，以与支付装置和/或移动装置交互。在一些实施例中，用作POS终端的蜂窝电话、平板计算机或其它专用无线装置可被称为移动销售点或“mPOS”终端。

[0034] “授权请求消息”可以是请求对交易的授权的电子消息。在一些实施例中，授权请求消息被发送给交易处理计算机和/或支付卡的发行方，以请求交易授权。根据一些实施例的授权请求消息可符合ISO8583，这是针对交换与用户使用支付装置或支付账户进行的支付相关联的电子交易信息的系统的标准。授权请求消息可以包括可以与支付装置或支付账户相关联的发行方账户标识符。授权请求消息还可以包括与“标识信息”对应的额外数据元素，包括(只作为实例)：服务代码、CVV(卡检验值)、dCVV(动态卡检验值)、PAN(主账号或“账号”)、支付令牌、用户名、到期日期等等。授权请求消息还可以包括“交易信息”，例如与当前交易相关联的任何信息，例如交易金额、商家标识符、商家位置、收单方银行标识号(BIN)、卡片接受器ID、标识正购买的项目的信息等，以及可以用确定是否标识和/或授权交易的任何其它信息。

[0035] “授权响应消息”可以是响应于授权请求的消息。在一些情况下，授权响应消息可以是由发行金融机构或交易处理计算机生成的对授权请求消息的电子消息应答。授权响应消息可以包括(仅借助于实例)以下状态指示符中的一个或多个：批准-交易被批准；拒绝-交易不被批准；或呼叫中心-响应等待更多信息，商家必须呼叫免费授权电话号码。授权响应消息还可包括授权代码，所述授权代码可以是信用卡发行银行响应于电子消息中的授权请求消息(直接地或通过交易处理计算机)返回到商家的访问装置(例如，POS设备)的指示交易被批准的代码。所述代码可以充当授权的证据。如上所述，在一些实施例中，交易处理计算机可以向商家生成或转发授权响应消息。

[0036] “服务器计算机”可以包括功能强大的计算机或计算机集群。举例来说，服务器计算机可以是大型主机、小型计算机集群或像单元一样工作的一组服务器。在一个实例中，服务器计算机可以是耦合到网络服务器的数据库服务器。服务器计算机可以耦合到数据库，并且可包括用于服务于来自一个或多个客户端计算机的请求的任何硬件、软件、其它逻辑或前述内容的组合。服务器计算机可以包括一个或多个计算设备，并且可以使用多种计算结构、布置和编译中的任一种来服务于来自一个或多个客户端计算机的请求。

[0037] 图1是示出根据一些实施例的示例性中继攻击的框图100。图1中所描绘的实例示

出欺诈者可以如何使用中继攻击来损害用户装置102与访问装置104-1之间的交互。图1包括用户装置102、访问装置104-1、访问装置104-2、介入装置106-1和介入装置106-2，但在其它实施例中可以利用任何合适数目和/或类型的装置。作为非限制性实例，访问装置104-1和104-2可以各自位于一个或多个加油站的单独燃料泵装置处(和/或作为相应燃料泵装置的部分来操作)。

[0038] 在步骤1，访问装置104-1(例如，位于加油站“SuperGas”在泵1处)可以传送广告消息(例如，经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。标识数据可以呈任何形式。举例来说，标识数据可以包括资源提供商的标识符(例如，商家，例如“SuperGas”、“SuperGas at 4th and Broadway,Seattle,WA.”或类似物)。在一些实施例中，与访问装置104-1相关联的标识数据还可包括装置标识符(例如，“泵1”)。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如，在接收例如BLE等短程无线通信协议的短程无线消息的范围内)。

[0039] 在步骤2，由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息中继到用户装置102。在一些实施例中，介入装置106-1可以在将消息中继到用户装置102之前改变广告消息(例如，标识数据)，而在其它实施例中，介入装置106-1可以保持广告消息不改变。

[0040] 在步骤3，用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说，用户装置102可以呈现图2的用户界面。图2示出根据一些实施例的用于与具有BLE功能的访问装置建立连接的示例性用户界面200。如图2中所描绘，用户界面200可以包括文字202。在一些实施例中，文字202可以指示连接到特定访问装置的意图。作为非限制性实例，文字202可以包括在图1的步骤3接收的标识数据的某一部分。如所描绘，文字202可以指示用户希望与访问装置1、终端1建立连接。在图1中提供的实例中，用户界面200可以包括指示用户希望与“SuperGas，泵1”建立连接的文字202。用户界面200可以包括确认按钮204和/或取消按钮206。在选择确认按钮204(或被配置成与由文字202指示的意图的确认相关联的任何合适的用户界面元件)时，用户装置102被配置成执行进一步操作。用户界面200的特定用户界面元件和/或格式可以变化。

[0041] 返回到图1，在呈现用户界面200且接收到用户已经确认与“SuperGas，泵1”建立连接的意图的指示时，可以在介入装置106-1与用户装置102之间利用任何合适的短程无线协议(例如，BLE)建立连接。因此，基于在步骤2中继消息，欺诈者可以在第一欺诈性非接触装置(介入装置106-1)与用户装置102之间建立BLE连接。用户装置102的用户可以相信(例如，基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而，用户装置102可能实际上连接到欺诈者的装置(例如，介入装置106-1)。

[0042] 一旦介入装置106-1与用户装置102之间的连接建立，介入装置106-1就可在步骤4经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例如，介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如，位于另一加油站“OtherGas”在“泵4”处的访问装置)。介入装置106-2可以在步骤5经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0043] 在此欺诈性交易流中，介入装置106-2可以从访问装置104-2接收交互数据(例如，包括与访问装置104-2相关联的标识信息、例如预授权金额的交互值等)。介入装置106-2可以在步骤7将接收的交互数据中继到介入装置106-1。

[0044] 在一些攻击中，介入装置106-1(和/或介入装置106-2)可以改变由访问装置104-2提供的交互数据。作为非限制性实例，介入装置106-1可以改变标识数据以指示交互数据是由访问装置104-1提供而不是由访问装置104-2提供。更具体地，介入装置106-1和/或106-2可以将与“OtherGas，泵4”相关联的交互数据改变为“SuperGas，泵1”。此改变的交互数据可以在步骤9中继到用户装置102。此改变的交互数据的接收可以使用户装置102呈现另一用户界面(例如，图3的用户界面300)以确认用户装置104与自称为访问装置104-1的介入装置106-1之间的交互。图3示出根据一些实施例的用于确认与具有BLE功能的访问装置的交互的示例性用户界面300。作为非限制性实例，用户界面300可以包括文字302，所述文字如图3中所描绘指示将与“访问装置1，终端1”进行交互。在图1的进行中实例中，文字302可以指示交互将与访问装置104-1发生(例如，“继续在SuperGas泵1处预先授权$99)。应了解，文字302可以包括由访问装置104-2提供和/或由介入装置106-1和/或106-2改变的交互数据的任何合适的部分。

[0045] 在一些实施例中，用户界面300可以被配置成利用用户装置102的任何合适的生物计量输入装置接收生物计量信息。举例来说，用户可以通过在用户装置102处经由指纹读取器扫描他的指纹来指示执行交互的意图(例如，预授权)。可以利用用于指示执行交互的意图的任何合适的机制(例如，经由类似于图2的确认按钮204的相似按钮，经由另一合适的生物计量输入装置(例如，相机、视网膜读取器和虹膜扫描仪等)。在一些实施例中，用户界面300还可包括取消按钮304或相似界面元件，用于指示用户不打算执行文字302中指示的交互。

[0046] 返回到图1的进行中实例，由于介入装置106-1先前自身已经作为“SuperGas，泵1”向用户装置102呈现，因此用户可能被骗认为他的用户装置102正与访问装置104-1(例如，位于用户装置102附近的“SuperGas”泵)进行交互以执行交易，但事实上正经由介入装置106-1和106-2实际上与访问装置104-2(“OtherGas”泵)进行交互。因此，用户可以基于读取图3的文字302认为交互是与SuperGas泵1进行来指示他执行交互的意图，但事实上用户装置102根本未与访问装置104-1进行交互。

[0047] 在接收到用户希望执行交互的指示时，用户装置102可以被配置成在步骤10提供支付数据。举例来说，在用户装置102上操作的应用程序可以生成芯片数据，所述芯片数据在步骤11经由介入装置106-1中继到介入装置106-2。在步骤12，介入装置106-2将支付数据提供到访问装置104-2。

[0048] 这可以使欺诈者的同伙(例如，操作介入装置106-2)能够填充其自己的油罐，可能比真实用户期望的数量大得多。在简单的中继攻击情形中，真实用户可能甚至没有机会填充其自己的罐。即，介入装置106-1可以在一旦得到执行欺诈性交易所必要的数据时就简单地终止与用户装置102的BLE连接。

[0049] 可了解到，此类型的攻击存在许多变化。以上描述仅是一个实例。也可以理解，访问装置104-1的提供商(例如，商家“SuperGas”)不会与欺诈者串通。就访问装置104-2的提供商(例如，商家“OtherGas”)来说，介入装置106-2表现为真实用户的装置。因此，访问装置104-2的提供商也无意中地成为欺诈性交易的一方。

[0050] 上文描述的中继攻击是可能的，因为没有检查用户认为他们正在交互的访问装置与实际交互正在执行的访问装置是相同的。

[0051] 图4示出根据一些实施例的示出用于防止中继攻击的示例性方法400的框图。图4示出其中访问装置(例如,访问装置104-2)利用私钥以数字方式签署传送的数据的用例。传送可以包括对应的公钥,使得如果介入装置修改数据,那么用户装置102通过使用公钥验证数字签名可以标识数据已被修改的事实。

[0052] 在图4中所描绘的实例中,用户装置102可以被配置有加密数据402。在一些实施例中,加密数据402可以包括由证书颁发中心(未描绘)发出的证书。在一些实施例中,证书可以是Europay、Mastercard®和Visa® (EMV)证书。在一些实施例中,证书可以包括与用户装置102相关联的公钥,所述公钥是由证书颁发中心利用与证书颁发中心相关联的私钥以数字方式签署的。加密数据402还可以包括与用户装置104相关联的私钥(例如,与由证书颁发中心以数字方式签署的认证公钥相关联的私钥)。访问装置104-1和104-2可以各自被配置成分别生成加密数据404和406。加密数据404和406中的每一个可以包括用于每一相应装置的未认证的公钥/私钥对。公钥/私钥对可以是不对称密钥对,例如Rivest、Shamir和Adelman(RSA)密钥,椭圆曲线密码术(ECC)密钥,或用于某一其它合适的加密算法的密钥。在一些实施例中,访问装置104-1和104-2可以被配置成生成用于与用户装置(例如,用户装置102)的每一潜在交互的新公钥/私钥对。在其它实施例中,访问装置104-1和104-2可以被配置成再使用相应单个公钥/私钥对来执行与多种用户装置的各种交互。

[0053] 在步骤1,访问装置104-1(例如,位于加油站“SuperGas”在泵1处)可以传送广告消息(例如,经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。举例来说,标识数据可以包括资源提供商的标识符(例如,商家,例如“SuperGas”)。在一些实施例中,与访问装置104-1相关联的标识信息还可包括装置标识符(例如,“泵1”)。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如,在接收短程无线通信协议的短程无线消息的范围内)。

[0054] 在步骤2,由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息未改变地中继到用户装置102。

[0055] 在步骤3,用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说,用户装置102可以呈现图2的用户界面。

[0056] 返回到图1,在呈现用户界面200且接收到用户希望与“SuperGas,泵1”建立连接的确认(例如,确认按钮204被选择的指示)时,可以在介入装置106-1与用户装置102之间利用任何合适的短程无线协议(例如,BLE)建立连接。用户装置102的用户可以相信(例如,基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而,用户装置102可能实际上连接到欺诈者的装置(例如,介入装置106-1)。

[0057] 一旦介入装置106-1与用户装置102之间的连接建立,介入装置106-1就可在步骤4经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例如,介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如,位于另一加油站“OtherGas”的访问装置)处。介入装置106-2可以在步骤5经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0058] 在一些实施例中,访问装置104-2可以生成交互数据(例如,包括与访问装置104-2相关联的标识信息、例如预授权金额的交互值等)用于传送。然而,在传送交互数据之前,访问装置104-2可以被配置成利用交互数据的至少一部分生成数字签名。图5示出根据一些实

施例的示出用于生成数字签名的示例性方法的示意图500。

[0059] 示意图500描绘消息数据502。消息数据502可以包括对应于用于建立连接和/或执行访问装置和/或用户装置之间的交互的数据的任何合适组合的任何合适数目个数据字段。举例来说，消息数据502可以包括数据字段502A。在一些实施例中，数据字段502A可以包括与访问装置的提供商(例如，商家，例如图4的实例的“SuperGas”)相关联的标识符。消息数据502可以另外或替代地包括数据字段502B。在一些实施例中，数据字段502B可以包括装置标识符(例如，序列号、与提供商的特定装置(例如，图4的实例的“泵4”相关联的标识符)。在一些实施例中，消息数据502可以另外或替代地包括数据字段502C。在一些实施例中，数据字段502C可以对应于交互金额(例如，预授权金额、最终购买价格等)。在一些实施例中，消息数据502可以另外或替代地包括数据字段502D。在一些实施例中，数据字段502D可以对应于位置(例如，与访问装置相关联的位置)。在一些实施例中，消息数据502可以另外或替代地包括数据字段502E。在一些实施例中，数据字段502E可以对应于公钥(例如，与访问装置相关联的公钥)。可以(例如，由访问装置)利用数据字段504的任何合适的组合来生成数字签名506。应了解，消息数据502的次序在实施例之间可以不同。虽然未描绘，但在一些实施例中(例如，对于从用户装置传送到访问装置的消息)，数据字段还可包括用于传送支付数据的数据字段。

[0060] 在一些实施例中，可以通过散列数据字段504的任何合适的部分来(例如，由访问装置)生成数字签名506。举例来说，可以通过首先将数据字段502A和/或502B作为输入提供到散列算法中以产生散列值来生成数字签名506。产生的散列值可以随后连同私钥(例如，与访问装置相关联的私钥)一起输入到签署算法以产生数字签名506。可以连同对应于私钥的公钥一起利用数字签名506来验证用以产生数字签名的任何数据字段未改变。作为非限制性实例，消息数据502的接收器可以利用公钥(例如，数据字段502E中提供的公钥)从数字签名506检取散列值。接收器可以随后从数据字段504的预定组合(例如，数据字段502A和502B)产生散列以生成额外散列值。接收器可以随后将从数字签名506检取的散列与生成的散列进行比较。如果所述两个散列值匹配，那么对接收器确保消息是有效的(例如，未改变)。如果所述两个散列值并不匹配，那么接收器可以确定消息是无效的(例如，由于原始传送而已经改变)。应了解，在图5中提供的实例是说明性的且并不希望限制本公开的范围。在其它实施例中，可以利用数据字段504的任何合适的组合(例如，所有数据字段504，比上文已经描述的数据字段更多或更少的数据字段等)来生成数字签名506，数字签名又可用以确定此类数据在接收到时是否已改变。

[0061] 返回到图4，访问装置104-2可以利用交互数据的至少一部分在步骤6生成数字签名。举例来说，访问装置104-2可以利用交互数据的标识数据(例如，商家标识符、装置标识符等)以在图5中描述的方式生成数字签名。在一些实施例中，除标识数据之外，还可以使用其它交互数据(例如，位置、交互值等)生成数字签名。访问装置104-2可以在消息内插入数字签名以及对应于用以生成数字签名的私钥的公钥，且将消息传送到用户装置102。

[0062] 介入装置106-2可以在步骤7从访问装置104-2接收消息且在步骤8将消息中继到介入装置106-1。

[0063] 介入装置106-1(和/或介入装置106-2)可以改变由访问装置104-2提供的交互数据。作为非限制性实例，介入装置106-1可以改变标识数据以指示交互数据是由访问装置

104-1提供而不是由访问装置104-2提供。更具体地，介入装置106-1和/或106-2可以将与“OtherGas，泵4”相关联的交互数据改变为“SuperGas，泵1”。此改变的交互数据可以在步骤9中继到用户装置102。

[0064] 在步骤10，用户装置102可以被配置成利用在消息内接收的与访问装置104-2相关联的数字签名和公钥来验证接收到的消息。举例来说，接收到的消息中包括的公钥可用以提取消息中包括的数字签名的散列值。用户装置102可以随后基于数据字段的预定集合(例如，图5的数据字段502A和502B)计算额外散列值。用户装置102可以将提取的散列值与计算的散列值进行比较。

[0065] 在步骤11，由于散列值因数据改变而不匹配，因此用户装置102可以被配置成确定消息无效(例如，已改变，或至少数据字段的预定集合已改变)且终止与访问装置104-2的任何进一步交互。

[0066] 图6示出根据一些实施例的示出用于防止中继攻击的另一示例性方法600的框图。图6示出其中访问装置(例如，访问装置104-2)在传送之前利用其私钥以数字方式签署数据的用例。传送中可以包括对应于私钥的公钥。如果数据未被介入装置修改而是仅中继，那么数字签名的验证可以通过用户装置102处的验证。然而，即使消息可以被确定为有效的(例如，未改变)，也可以执行对消息的数据中的至少一些(例如，指示例如商家名称/标识符的标识数据)的额外检查。举例来说，来自访问装置104-2的消息的标识数据可以与在初始连接阶段接收的标识进行比较，以确保与用户装置进行交互的实体是用户装置102相信连接被批准的同一实体。

[0067] 在图6中描绘的实例中，如图4的实例中，用户装置102可以被配置有加密数据402。如上文相对于图4所论述，加密数据402可以包括由证书颁发中心(未描绘)发出的证书。访问装置104-1和104-2可以各自被配置成分别生成加密数据404和406，所述加密数据个别地可以包括用于每一相应装置的未认证公钥/私钥对。

[0068] 方法600的步骤1-10可以如上文结合图4所描述的方法400的步骤1-10的类似方式执行。

[0069] 在步骤1，访问装置104-1(例如，位于加油站“SuperGas”在泵1处)可以传送广告消息(例如，经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。举例来说，标识数据可以包括资源提供商的标识符(例如，商家，例如“SuperGas”)。在一些实施例中，与访问装置104-1相关联的标识数据还可包括装置标识符(例如，“泵1”)。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如，在接收短程无线通信协议的短程无线消息的范围内)。

[0070] 在步骤2，由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息未改变地中继到用户装置102。

[0071] 在步骤3，用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说，用户装置102可以呈现图2的用户界面。

[0072] 在呈现用户界面200且接收到用户希望与“SuperGas，泵1”建立连接的确认(例如，确认按钮204被选择的指示)时，可以在介入装置106-1与用户装置102之间利用任何合适的短程无线协议(例如，BLE)建立连接。用户装置102的用户可以相信(例如，基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而，用户装置102可能实际上连接

到欺诈者的装置(例如,介入装置106-1)。在此实施例中,用户装置102可以存储在广告消息中接收的数据的至少一部分。举例来说,用户装置102可以将标识数据(例如,“SuperGas”)存储为指示用户装置102据称连接到的装置。

[0073] 一旦介入装置106-1与用户装置102之间的连接建立,介入装置106-1就可在步骤4经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例如,介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如,位于另一加油站“OtherGas”的访问装置)处。介入装置106-2可以在步骤5经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0074] 在一些实施例中,访问装置104-2可以生成交互数据(例如,包括与访问装置104-2相关联的标识信息、例如预授权金额的交互值等)用于传送。然而,在传送交互数据之前,访问装置104-2可以被配置成以上文结合图4和5所论述的方式利用交互数据的至少一部分生成数字签名。

[0075] 在步骤6,访问装置104-2可以利用交互数据的至少一部分生成数字签名。举例来说,访问装置104-2可以图5中描述的方式利用交互数据的标识数据(例如,商家标识符、装置标识符,图5的数据字段504的任何合适组合等)来生成数字签名。访问装置104-2可以在消息内插入数字签名以及对应于用以生成数字签名的私钥的公钥,且将消息传送到用户装置102。

[0076] 介入装置106-2可以在步骤7从访问装置104-2接收消息且在步骤8将消息中继到介入装置106-1。介入装置106-1(和/或介入装置106-2)可以在步骤9将未改变的消息中继到用户装置102。应了解在进行中的实例中,消息仍指示对应于“OtherGas”的标识数据。

[0077] 在步骤10,用户装置102可以被配置成利用在消息内接收的与访问装置104-2相关联的数字签名和公钥来验证接收到的消息。举例来说,接收到的消息中包括的公钥可用以提取消息中包括的数字签名的散列值。用户装置102可以随后基于数据字段的预定集合(例如,图5的数据字段502A和502B)计算额外散列值。用户装置102可以将提取的散列值与计算的散列值进行比较。

[0078] 在步骤11,由于散列值可以因消息数据未改变而匹配,因此用户装置102可以被配置成确定消息是有效的(例如,未改变,或至少数据字段的预定集合未改变)。

[0079] 在步骤12,用户装置可以进一步被配置成确定数据字段的某一部分是否匹配存储的信息。举例来说,用户装置102可以确定在消息中接收的标识数据(例如,指示“OtherGas”)是否匹配存储于用户装置102处且与用户装置102假设连接的访问装置104-1相关联的标识数据(例如,“SuperGas”)。在进行中的实例中,用户装置102可以确定接收的标识数据(例如,“OtherGas”)不匹配存储的与连接装置相关联的标识数据(例如,“SuperGas”)。至少部分地基于此确定,用户装置102可以被配置成终止与访问装置104-2的任何进一步交互。

[0080] 图7示出根据一些实施例的示出用于防止中继攻击的又一示例性方法700的框图。图7是针对其中访问装置104-1在传送到用户装置102的连接消息中提供其公钥的实例。同一公钥可以用于验证来自访问装置104-2的后续消息。在中继攻击中,连接装置的公钥将不匹配后续消息的公钥,这可以造成对后续消息的验证检查在用户装置102处失败。

[0081] 在图7中描绘的实例中,如上文结合图4和6所描述,用户装置102可以被配置有加

密数据402(例如,证书和/或认证的公钥/私钥对)。访问装置104-1和104-2可以各自被配置成分别生成和/或存储加密数据404和406。加密数据404和406中的每一个可以包括用于每一相应装置的未认证的公钥/私钥对。举例来说,加密数据404可以包括公钥702和与公钥702相关联的私钥。

[0082] 在步骤1,访问装置104-1(例如,位于加油站“SuperGas”在泵1处)可以传送广告消息(例如,经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。举例来说,标识数据可以包括资源提供商的标识符(例如,商家,例如“SuperGas”)。在一些实施例中,与访问装置104-1相关联的标识数据还可包括装置标识符(例如,“泵1”)。在图7中提供的实例中,广告消息还可包括加密数据404的公钥702。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如,在接收短程无线通信协议的短程无线消息的范围内)。

[0083] 在步骤2,由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息未改变地中继到用户装置102。

[0084] 在步骤3,用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说,用户装置102可以呈现图2的用户界面200。在一些实施例中,用户装置102可以在用户装置102处存储加密数据404的公钥702。

[0085] 在呈现用户界面200且接收到用户希望与“SuperGas,泵1”建立连接的确认(例如,图2的确认按钮204被选择的指示)时,用户装置102可以在步骤4利用任何合适的短程无线协议(例如,BLE)与介入装置106-1建立连接。用户装置102的用户可以相信(例如,基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而,用户装置102可能实际上连接到欺诈者的装置(例如,介入装置106-1)。

[0086] 一旦介入装置106-1与用户装置102之间的连接建立,介入装置106-1就可在步骤5经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例如,介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如,位于另一加油站“OtherGas”的访问装置)处。介入装置106-2可以在步骤6经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0087] 在一些实施例中,访问装置104-2可以生成交互数据(例如,包括与访问装置104-2相关联的标识数据、例如预授权金额的交互值等)用于传送。然而,在传送交互数据之前,访问装置104-2可以被配置成如上文结合图4-7所描述利用交互数据的至少一部分生成数字签名。访问装置104-2可以利用交互数据的至少一部分在步骤7生成数字签名。举例来说,访问装置104-2可以利用交互数据的任何合适的部分(例如,商家标识符和/或装置标识符、商家标识符/装置标识符/和与访问装置相关联的位置,或图5的数据字段504的任何合适的组合)以上文的方式生成数字签名。访问装置104-2可以在消息内插入数字签名且将消息传送到用户装置102。在一些实施例中,在将消息传送到用户装置102之前,访问装置104-2可以(或可以不)在同一消息内插入用以生成数字签名的公钥。

[0088] 介入装置106-2可以在步骤8从访问装置104-2接收消息且在步骤9将消息中继到介入装置106-1。介入装置106-1可以在步骤10将消息未改变或已改变地转发到用户装置102。在一些实施例中,介入装置106-1和/或106-2可以改变消息的某一部分,而在其它实施例中,介入装置106-1和106-2简单地将消息未改变地中继到用户装置102。

[0089] 在步骤11，用户装置102可以被配置成利用数字签名和公钥702验证接收到的消息。举例来说，在连接时接收的公钥702可用以在步骤10提取所接收的消息中包括的数字签名的散列值。用户装置102可以随后基于数据字段的预定集合(例如，数据字段502A和502B，数据字段502A、502B和502D，或图5的数据字段504的任何合适的组合)计算额外散列值。用户装置102可以将提取的散列值与计算的散列值进行比较。

[0090] 在步骤12，由于散列值并不匹配(例如，至少部分地基于公钥702正用于验证消息且公钥702不对应于用以生成数字签名的私钥)，因此用户装置102可以确定消息是无效的。无论消息是改变还是未改变，此确定都可以发生。在一些实施例中，除了利用数字签名的验证之外或作为一个替代方案，用户装置102可以被配置成在步骤10将公钥702与所接收的消息中包括的公钥进行比较。如果公钥并不匹配，那么用户装置102可以被配置成如上文所描述利用数字签名和散列值确定消息是无效的，而不必验证消息。

[0091] 在步骤13，响应于确定消息是无效的，用户装置102可以终止与访问装置104-2的任何进一步交互。

[0092] 图8示出根据一些实施例的示出用于防止中继攻击的又一示例性方法的框图。图8是针对其中两个介入装置仅在访问装置与用户装置之间中继消息的实例。因为消息未被修改，所以对消息的验证检查可以指示消息是有效的(例如，未改变)。然而，可以向用户提供通知，所述通知可以使用户能够知道他相信他连接到的实体与随后请求额外数据(例如，支付数据)的实体之间的差异。用户可以利用此通知来进行由于此差异而取消交互。

[0093] 在图8中描绘的实例中，如上文结合图4、6和7所描述，用户装置102可以被配置有加密数据402(例如，证书和/或认证的公钥/私钥对)。访问装置104-1和104-2可以各自被配置成分别生成和/或存储加密数据404和406。加密数据404和406中的每一个可以包括用于每一相应装置的未认证的公钥/私钥对。

[0094] 在步骤1，访问装置104-1(例如，位于加油站“SuperGas”在泵1处)可以传送广告消息(例如，经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。举例来说，标识数据可以包括资源提供商的标识符(例如，商家，例如“SuperGas”)。在一些实施例中，与访问装置104-1相关联的标识数据还可包括装置标识符(例如，“泵1”)。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如，在接收短程无线通信协议的短程无线消息的范围内)。

[0095] 在步骤2，由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息未改变地中继到用户装置102。

[0096] 在步骤3，用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说，用户装置102可以呈现图2的用户界面200。

[0097] 返回到图8，在呈现用户界面200且接收到用户希望与“SuperGas，泵1”建立连接的确认(例如，图2的确认按钮204被选择的指示)时，可以在介入装置106-1与用户装置102之间利用任何合适的短程无线协议(例如，BLE)建立连接。用户装置102的用户可以相信(例如，基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而，用户装置102可能实际上连接到欺诈者的装置(例如，介入装置106-1)。

[0098] 一旦介入装置106-1与用户装置102之间的连接建立，介入装置106-1就可在步骤4经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例

如，介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如，位于另一加油站“OtherGas”的访问装置)处。介入装置106-2可以在步骤5经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0099] 在一些实施例中，访问装置104-2可以生成交互数据(例如，包括与访问装置104-2相关联的标识信息、例如预授权金额的交互值等)用于传送。然而，在传送交互数据之前，访问装置104-2可以被配置成如上文结合图4-7所描述利用交互数据的至少一部分生成数字签名。访问装置104-2可以利用交互数据的至少一部分在步骤6生成数字签名。举例来说，访问装置104-2可以图5中描述的方式利用标识数据(例如，商家标识符、装置标识符)和(在一些情况下)与访问装置相关联的位置来生成数字签名。访问装置104-2可以在消息内插入数字签名以及对应于用以生成数字签名的私钥的公钥，且将消息传送到用户装置102。

[0100] 介入装置106-2可以在步骤7从访问装置104-2接收消息且在步骤8将消息中继到介入装置106-1。介入装置106-1可以在步骤9将消息未改变地转发到用户装置102。

[0101] 在步骤10，用户装置102可以被配置成利用在消息内接收的与访问装置104-2相关联的数字签名和公钥来验证接收到的消息。举例来说，接收到的消息中包括的公钥可用以提取消息中包括的数字签名的散列值。用户装置102可以随后基于数据字段的预定集合(例如，数据字段502A和502B，数据字段502A、502B和502D，或图5的数据字段504的任何合适的组合)计算额外散列值。用户装置102可以将提取的散列值与计算的散列值进行比较。

[0102] 在步骤11，由于散列值因数据未改变而匹配，因此用户装置102可以被配置成确定消息是有效的(例如，未改变，或至少数据字段的预定集合未改变)。由于此确定，可以在用户装置102处呈现用户界面(例如，图3的用户界面300)以禁止来自用户的关于与访问装置104-2交互的意图的确认。情况可能是因为用户在连接时被呈现信息(例如，“SuperGas”)，所以他可以认识到现在呈现的数据(例如，“OtherGas”)是与他认为他连接的访问装置(例如，访问装置104-1)不同的访问装置(例如，访问装置104-2)相关联。用户可以指示(例如，经由图3的取消按钮304的选择)他不打算与访问装置104-2交互。

[0103] 在步骤12，虽然消息被确定为有效的，但是用户装置102可以至少部分地基于接收到用户不打算与访问装置104-2交互的指示而终止与访问装置104-2的任何进一步交互。

[0104] 图9示出根据一些实施例的示出用于防止中继攻击的再一个示例性方法900的框图。图9是针对其中用户装置(例如，用户装置102)错误地认为已与访问装置104-1(例如，与“SuperGas”相关联)做出连接但错误地授权与访问装置104-2(例如，“OtherGas”)的后续交互的实例，因为尽管被提供通知，用户也可能未注意到宣称的连接访问装置与请求后续交互的访问装置之间的差异。在此用例中，用户装置102可以数字方式签署回到访问装置104-2的数据。在接收到时，访问装置104-2可以检查消息的公钥(例如，先前发送到用户装置并且接着由用户装置以数字方式签署的访问装置104-2的公钥)。如果消息中包括的公钥与由访问装置104-2保持的公钥是相同的，那么可以认为交互是有效的。如果有效，那么可以将接收的数据的至少一部分发送到资源提供商以进行传统的授权请求过程。然而，如果消息是无效的，那么访问装置104-2可以被配置成停止处理。

[0105] 在图9中所描绘的实例中，用户装置102可以被配置有加密数据402。如上文相对于图4所论述，加密数据402可以包括由证书颁发中心(未描绘)发出的证书。访问装置104-1和104-2可以各自被配置成分别生成加密数据404和406。加密数据404和406中的每一个可以

包括用于每一相应装置的未认证的公钥/私钥对。

[0106] 在步骤1,访问装置104-1(例如,位于加油站“SuperGas”在泵1处)可以传送广告消息(例如,经由例如BLE的短程无线协议)。所述广告消息可以至少包括与访问装置104-1相关联的标识数据。举例来说,标识数据可以包括资源提供商的标识符(例如,商家,例如“SuperGas”)。在一些实施例中,与访问装置104-1相关联的标识数据还可包括装置标识符(例如,“泵1”)。用户装置102可以接近访问装置104-1以打破与访问装置104-1的阈值距离(例如,在接收短程无线通信协议的短程无线消息的范围内)。

[0107] 在步骤2,由第一欺诈者操作的介入装置106-1可以拦截广告消息且将消息未改变地中继到用户装置102。

[0108] 在步骤3,用户装置102可以接收广告消息且显示用于确认与访问装置104-1的连接的一个或多个用户界面。举例来说,用户装置102可以呈现图2的用户界面。

[0109] 在呈现用户界面200且接收到用户希望与“SuperGas,泵1”建立连接的确认(例如,确认按钮204被选择的指示)时,可以在介入装置106-1与用户装置102之间利用任何合适的短程无线协议(例如,BLE)建立连接。用户装置102的用户可以相信(例如,基于图2的用户界面200中提供的文字202)他们正连接到访问装置104-1。然而,用户装置102可能实际上连接到欺诈者的装置(例如,介入装置106-1)。

[0110] 一旦介入装置106-1与用户装置102之间的连接建立,介入装置106-1就可在步骤4经由任何合适的有线和/或无线连接连接(或另外传送数据)到同伙的第二欺诈性装置(例如,介入装置106-2)。介入装置106-2可位于例如另一访问装置(例如,位于另一加油站“OtherGas”的访问装置)处。介入装置106-2可以在步骤5经由第二BLE连接来连接(或另外传送数据)到访问装置104-2。

[0111] 在一些实施例中,访问装置104-2可以生成交互数据(例如,包括与访问装置104-2相关联的标识信息、例如预授权金额的交互值等)用于传送。然而,在传送交互数据之前,访问装置104-2可以被配置成以上文结合图4-8所论述的方式利用交互数据的至少一部分生成数字签名。

[0112] 在步骤6,访问装置104-2可以利用交互数据的至少一部分生成数字签名。举例来说,访问装置104-2可以上文所描述的方式利用交互数据的任何合适的部分(例如,商家标识符、装置标识符、图5的数据字段504的任何合适组合等)来生成数字签名。访问装置104-2可以在消息内插入数字签名以及对应于用以生成数字签名的私钥的公钥,且将消息传送到用户装置102。

[0113] 介入装置106-2可以在步骤7从访问装置104-2接收消息且在步骤8将消息中继到介入装置106-1。介入装置106-1(和/或介入装置106-2)可以在步骤9将未改变的消息中继到用户装置102。应了解在进行中的实例中,消息仍指示对应于“OtherGas”的标识数据。

[0114] 在步骤10,用户装置102可以被配置成利用在消息内接收的与访问装置104-2相关联的数字签名和公钥来验证接收到的消息。举例来说,接收到的消息中包括的公钥可用以提取消息中包括的数字签名的散列值。用户装置102可以随后基于数据字段的预定集合(例如,图5的数据字段502A和502B)计算额外散列值。用户装置102可以将提取的散列值与计算的散列值进行比较。

[0115] 在步骤11,由于散列值可以因消息数据未改变而匹配,因此用户装置102可以被配

置成确定消息是有效的(例如,未改变,或至少数据字段的预定集合未改变)。在用户装置处可以提供一个或多个用户界面(例如,图3的用户界面300。用户可能未认识到文字302指示与用户相信连接到用户装置102的访问装置(例如,访问装置104-1)不同的访问装置(例如,访问装置104-2)的交互。因此,用户可以在步骤12确认交互。

[0116] 在步骤13,响应于接收到用户确认与访问装置104-2的交互的指示,用户装置102可以被配置成提供支付数据和加密数据402(例如,由证书颁发中心发出的证书,未图示)。在一些实施例中,由用户装置102在消息中包括的支付数据可以呈令牌和/或可以由接收访问装置104-2解密的加密值的形式。用户装置102可以在步骤9在所接收的消息中包括由访问装置104-2原始提供的交互数据的某一部分。举例来说,用户装置102可以连同在步骤9接收且与访问装置104-2相关联的消息中提供的公钥一起包括与访问装置相关联的标识数据(例如,商家标识符和/或装置标识符)。在一些实施例中,用户装置102可以被配置成利用任何合适的消息数据(例如,标识数据、与访问装置104-2相关联的公钥、支付数据、加密数据402,或上文和/或图5的数据字段5024的任何合适组合)生成数字签名。

[0117] 介入装置106-1可以从用户装置接收消息且在步骤14将消息中继到介入装置106-2。介入装置106-2又可以将消息中继到访问装置104-2。

[0118] 在步骤16,访问装置104-2可以被配置成利用与用户装置102相关联的公钥验证所接收的消息。举例来说,在步骤15接收的消息中含有的与发出证书的证书颁发中心相关联的公钥可以从访问装置104-2的本地存储器检取。证书颁发中心的公钥可用以从证书检取与用户装置102相关联的公钥。访问装置104-2可以被配置成在步骤15利用与用户装置102相关联的公钥来验证所接收的消息。

[0119] 举例来说,访问装置104-2可以被配置成在步骤15利用与用户装置102相关联的公钥从所接收的消息的数字签名检取散列值。访问装置104-2可以随后利用预定散列算法和在步骤15接收的消息的数据字段的预定集合来生成额外散列值。举例来说,可以通过消息的标识数据、消息中包括的公钥和/或消息中包括的支付数据的任何合适组合作为输入提供散列算法来生成额外散列值。一旦生成,将可以将所得散列值与从数字签名检取的散列值进行比较。如果散列值并不匹配,那么访问装置104-2可以被配置成终止交互且不执行支付数据的进一步处理。

[0120] 如果散列值匹配,那么访问装置104-2可以被配置成继续,因为匹配可以指示不仅消息未改变,而且(例如,由用户装置102)利用与访问装置104-2相关联的正确公钥来验证在步骤7初始传送的消息。在一些实施例中,通过生成授权请求消息,访问装置104-2可以继续,所述授权请求消息可以随后传送到资源提供商计算机(例如,图12的资源提供商计算机1230)作为用于授权支付交易的传统过程的部分。关于图12进一步详细论述描述用于授权支付交易的过程的流程。如果授予授权请求,那么访问装置104-2可以对用户装置102启用对商品和/或服务(例如,由访问装置104-2管理的汽油)的访问。

[0121] 图9中提供的实例示出所公开的技术可如何成功地防止中继攻击。仅当在用户装置102与访问装置104-2之间传达的数据未改变时才可以进行成功的中继攻击。实际上,大多数用户将认识到他们位于的商家(例如,SuperGas)与他们被请求同意支付的商家(例如,OtherGas)之间的差异。即使用户无意中同意支付,在访问装置104-2处签名验证也将失败,图10示出根据本发明的实施例的示例性用户装置1002的框图。用户装置1002可以是图1、4

和6-9的用户装置102的实例。在一些实施例中，用户装置1002可以包括用以启用例如电话等某些装置功能的电路。负责启用那些功能的功能元件可包括处理器1002B，所述处理器可执行实施装置的功能和操作的指令。处理器1002B可访问存储器1002F(或另一合适的数据存储区或元件)以检取指令或用于执行指令的数据，例如提供脚本和移动应用程序。例如键盘或触摸屏等数据输入/输出元件1002D可以用于使用户能够操作用户装置1002和输入数据。数据输入/输出元件还可以被配置成输出数据(经由例如装置的扬声器)。显示器1002C也可用于向用户输出数据。通信元件1002E可以用于实现用户装置1002与有线或无线网络之间的数据传送(经由例如天线1002G)以帮助连接到因特网或其它网络，且实现数据传送功能。在一些实施例中，通信元件1002E可以利用短程无线通信协议(例如，BLE)。

[0122] 在一些实施例中，用户装置1002还可以包括非接触元件接口以实现非接触元件(未图示)与装置的其它元件之间的数据传送，其中非接触元件可以包括安全存储器和近场通信数据传送元件(或另一形式的短程通信技术)。蜂窝式电话或相似装置是根据本发明的实施例可以使用的用户装置1002的实例。然而，在不脱离本发明的基本概念的情况下可以使用其它形式或类型的装置。举例来说，用户装置1002可以替代地呈支付卡、密钥卡、PDA、平板计算机、网书、膝上型计算机、智能手表、具有远程能力的汽车等形式。

[0123] 存储器1002F可以包括应用程序1002H和/或任何其它合适的模块或数据。举例来说，在一些实施例中，存储器1002F可以包括签署模块1002I、验证模块1002J和/或加密数据1002K。用户装置1002可以具有安装或存储在存储器1002F上的任何数目的移动应用程序且不限于图10中示出的情况。存储器1002F还可以包括可由处理器1002B执行以用于实施本文所论述的方法的代码。

[0124] 应用程序1002H可以呈任何合适的形式。举例来说，应用程序1002H可以是可用以与访问装置(例如，图1的访问装置104-1、图11的访问装置1102等)交互的应用程序。在一些实施例中，应用程序1002H可以是被配置成提供任何合适的用户界面(例如，分别图2和3的用户界面200和300)或被配置成收集数据和/或确认用户装置1002与访问装置之间的交互的任何合适的用户界面的应用程序。在一些实施例中，应用程序1002H可用以执行针对商品和/或服务的交易，例如与访问装置交换支付数据和/或交互数据(例如，标识数据、交互值、公钥、位置、装置信息等)以获得燃料(或另一商品和/或服务)和/或对资源的访问(例如，如下关于图13所述进入建筑物的入口)。在一些实施例中，应用程序1002H(或另一合适的模块)可以被配置成使处理器1002B执行操作和/或呈现用于与一个或多个其它装置(例如，访问装置、介入装置等)建立连接(例如，BLE连接)的任何合适的用户界面。应用程序1002H(或另一合适的模块)可以还被配置成使处理器1002B执行操作和/或呈现用于确认与一个或多个其它装置(例如，访问装置、介入装置等)的交互的任何合适的界面。

[0125] 在一些实施例中，应用程序1002H可以被配置成向访问装置和/或介入装置传送和/或从访问装置和/或介入装置接收任何合适的消息。在一些实施例中，可以经由BLE和/或其它合适的短程无线通信协议传送和/或接收这些消息。应用程序1002H可以被配置成使处理器1002B在消息的传送之前激励签署模块1002I的功能性和/或在接收到消息时激励验证模块1002J的功能性。

[0126] 签署模块1002I可以被配置有代码，所述代码在由处理器1002B执行时可以使处理器1002B执行用于生成数字签名且传送至少包括所述数字签名的消息的任何合适的操作。

举例来说，签署模块1002I可以被配置成使处理器1002B散列消息数据的一个或多个数据字段(例如，与用户装置1002相关联的标识数据、与访问装置相关联的标识数据、与用户装置1002和/或访问装置相关联的一个或多个位置、交互值、访问装置的公钥、用户装置1002的证书和/或类似物)以产生散列值。在一些实施例中，签署模块1002I可以被配置成使处理器1002B用与用户装置1002相关联的私钥以数字方式签署散列值。一旦生成，数字签名就可以插入到消息中(例如，连同一个或多个其它数据字段一起，例如与用户装置1002相关联的标识数据、与访问装置相关联的标识数据、与用户装置1002和/或访问装置相关联的一个或多个位置、交互值、访问装置的公钥、用户装置1002的证书和/或类似物)且传送到访问装置。在一些实施例中，签署模块1002I可以作为应用程序1002H的部分操作。

[0127] 验证模块1002J可以被配置有代码，所述代码在由处理器1002B执行时可以使处理器1002B执行用于验证消息的任何合适的操作。在一些实施例中，验证模块1002J可以被配置成使处理器1002B接收包括访问装置的公钥的消息。在一些实施例中，验证模块1002J可以在存储器1002F内存储接收的公钥以用于后续使用。在一些实施例中，验证模块1002J可以被配置成使处理器1002B接收包括数字签名(例如，由访问装置利用与访问装置相关联的私钥生成的数字签名)的消息。在一些实施例中，接收到的消息还可以包括与访问装置相关联的公钥。验证模块1002J可以使处理器1002B利用公钥(例如，在包括数字签名的消息中接收或利用在前一消息中接收的存储的公钥)来验证接收到的消息。

[0128] 举例来说，验证模块1002J可以被配置成使处理器1002B利用存储或接收的公钥从数字签名检取散列值。验证模块1002J还可以使处理器1002B散列接收到的消息的一个或多个数据字段(例如，与用户装置1002相关联的标识数据、与访问装置相关联的标识数据、与用户装置1002和/或访问装置相关联的一个或多个位置、交互值、访问装置的公钥、用户装置1002的证书及类似物)以产生额外散列值。在一些实施例中，验证模块1002J可以被配置成使处理器1002B将从数字签名检取的散列值与计算的散列值进行比较。如果散列值匹配，那么验证模块1002J可以激励应用程序1002H(或另一合适的模块)执行操作(例如，将包括接收到的消息数据的至少一部分的消息传送到另一装置，例如图12的资源提供商计算机1230)。

[0129] 在一些实施例中，如果散列值匹配，那么验证模块1002J可以确定消息是有效的(例如，未改变)。在一些实施例中，验证模块1002J可以被配置成使处理器1002B进行关于有效消息的位置是否在与用户装置1002相关联的位置的阈值距离内的又一确定。在这些实例中，验证模块1002J可以从例如1002的全球定位系统组件(例如，数据输入/输出元件1002D的实例)检取与用户装置1002相关联的位置。在更进一步的实施例中，验证模块1002J可以在确定消息是有效的(例如，基于检取的散列与计算的散列的比较)时执行将与用户装置1002假设连接到的访问装置相关联的存储标识符和与传送装置(例如，访问装置)相关联的接收到的消息的标识数据进行比较的额外操作。在一些实施例中，如果消息被确定为无效(例如，已改变，至少部分地基于检取的散列与计算的散列的比较)，和/或位置不在彼此的阈值距离内，和/或如果存储的标识符不匹配接收到的消息中包括的标识数据，那么验证模块1002J可以终止交互且不执行与传送装置的进一步处理。在一些实施例中，验证模块1002J可以作为应用程序1002H的部分操作。

[0130] 在一些实施例中，验证模块1002J(例如，在确定消息是有效的，和/或位置在彼此

的预定距离内，和/或存储的标识符匹配消息中包括的标识数据时)可以被配置成触发应用程序1002H以在显示器1002C处呈现用户界面以禁止来自用户装置1002的用户的他希望与传送装置(例如，消息中指示的访问装置)进行交互的确认。在接收到确认的指示时，应用程序1002H可以被配置成使处理器1002B执行与上文描述的签署模块1002I相关联的代码以传送可以包括如上文所描述由签署模块1002I生成的数字签名的消息。

[0131] 加密数据1002K可呈由证书颁发中心(例如，图12的处理网络计算机1250或任何合适的认证机构)提供的证书的形式。加密数据1002K还可包括由证书颁发中心发出且供应给用户装置1002的公钥/私钥。在一些实施例中，可以用与证书颁发中心相关联的私钥以数字方式签署证书。证书颁发中心的公钥可以分布到一个或多个访问装置。在一些实施例中，证书可以包括与用户装置1002相关联的公钥和/或任何合适的标识数据。证书可以由证书颁发中心以数字方式签署，以使得分布到访问装置的公钥可用以从证书检取与用户装置1002相关联的公钥。

[0132] 图10中示出根据本发明的实施例的访问装置1102的实例。访问装置1102可以是图1的访问装置104-1和/或104-2的实例。在一些实施例中，访问装置1102可以包括用以启用例如电话等某些装置功能的电路。负责启用那些功能的功能元件可包括处理器1102B，所述处理器可执行实施装置的功能和操作的指令。处理器1102B可访问存储器1102F(或另一合适的数据存储区或元件)以检取指令或用于执行指令的数据，例如提供脚本和移动应用程序。例如键盘或触摸屏等数据输入/输出元件1102D可以用于使用户能够操作访问装置1102和输入数据。数据输入/输出元件还可以被配置成输出数据(经由例如装置的扬声器)。显示器1102C也可用于向用户输出数据。通信元件1102E可以用于实现访问装置1102与有线或无线网络之间的数据传送(例如经由天线1102G)以帮助连接到因特网或其它网络，且实现数据传送功能。在一些实施例中，通信元件1102E可以利用短程无线通信协议(例如，BLE)。

[0133] 在一些实施例中，访问装置1102还可以包括非接触元件接口以实现非接触元件(未图示)与装置的其它元件之间的数据传送，其中非接触元件可以包括安全存储器和近场通信数据传送元件(或另一形式的短程通信技术)。销售点终端是根据本公开的实施例可以使用的访问装置1102的实例。然而，在不脱离本发明的基本概念的情况下可以使用其它形式或类型的装置。

[0134] 存储器1102F可以包括数据处理模块1102H和/或任何其它合适的模块或数据。举例来说，在一些实施例中，存储器1102F还可包括签署模块1102I、验证模块1102J和/或加密数据1102K。存储器1102F还可以包括可由处理器1102B执行以用于实施本文所论述的方法的代码。

[0135] 加密数据1102K可呈由访问装置1102生成的公钥/私钥对的形式。公钥/私钥对可以在任何合适的时间生成且存储于存储器1102F中用于后续使用。在一些实施例中，可以生成新公钥/私钥对以对应于与另一装置(例如，用户装置、介入装置等)的特定交互，以使得唯一公钥/私钥对可以对应特定消息交换。在其它实施例中，同一公钥/私钥对可以用于与任何合适的交互装置(例如，用户装置和/或介入装置)的任何合适的消息交换。

[0136] 数据处理模块1102H可以呈任何合适的形式。在一些实施例中，数据处理模块1102H可以被配置有代码，所述代码在由处理器1102B执行时使处理器1102B发送和/或接收消息(例如，向和/或从用户装置和/或介入装置)。在一些实施例中，数据处理模块1102H可

以被配置成传送至少指示例如访问装置1102的一个或多个标识符等标识数据的消息(例如,广告)。在一些实施例中,数据处理模块1102H可以被配置成使处理器1102B包括从加密数据1102K检取的与访问装置1102相关联的公钥。数据处理模块1102H可以在任何合适的消息传送(例如,广告消息、交互请求消息等)中包括公钥。在一些实施例中,数据处理模块1102H可以被配置成激励签署模块1102I的功能性以从要传送的消息的一个或多个消息数据字段生成数字签名。在一些实施例中,数据处理模块1102H可以被配置成至少部分地基于从装置(例如,用户装置和/或介入装置)接收到消息而激励验证模块1102J的功能性。

[0137] 通常,数据处理模块1102H可以被配置成向访问装置和/或介入装置传送和/或从访问装置和/或介入装置接收任何合适的消息。在一些实施例中,可以经由BLE和/或其它合适的短程无线通信协议传送和/或接收这些消息。数据处理模块1102H可以还被配置成使处理器1102B激励签署模块1102I和/或验证模块1102J的任何合适的功能性以执行本文所论述的方法。

[0138] 签署模块1102I可以被配置有代码,所述代码在由处理器1102B执行时可以使处理器1102B执行用于生成数字签名且传送至少包括生成的数字签名的消息的任何合适的操作。举例来说,签署模块1102I可以被配置成使处理器1102B散列消息的一个或多个数据字段(例如,与访问装置1102相关联的标识数据、与访问装置1102相关联的位置、交互值、访问装置的公钥和/或类似物)以产生散列值。在一些实施例中,签署模块1102I可以被配置成使处理器1102B用与访问装置1102相关联的私钥以数字方式签署散列值。一旦生成,数字签名就可以插入到消息中(例如,连同一个或多个其它数据字段,例如与访问装置1102相关联的标识信息、与访问装置相关联的标识信息、与访问装置1102相关联的位置、交易信息、访问装置1102的公钥和/或类似物)且传送到另一装置(例如,图1的用户装置102、图1的介入装置106-1等)。

[0139] 验证模块1102J可以被配置有代码,所述代码在由处理器1102B执行时可以使处理器1102B执行用于验证接收到的消息的任何合适的操作。在一些实施例中,验证模块1102J可以被配置成使处理器1102B接收包括据称由用户装置生成(例如,利用与用户装置102相关联的私钥)的数字签名的消息。消息还可包括与用户装置102相关联且由证书颁发中心发出的证书。在一些实施例中,访问装置1102可以在加密数据1102K内存储与证书颁发中心相关联的公钥。在检取证书颁发中心的公钥时,验证模块1102J可以被配置成利用证书颁发中心的公钥从所接收的证书检取与用户装置相关联的公钥。验证模块1002J可以使处理器1002B利用与用户装置相关联且从证书检取的公钥来验证接收到的消息的数字签名。

[0140] 举例来说,验证模块1102J可以被配置成使处理器1102B利用用户装置的公钥从数字签名检取散列值。验证模块1102J还可以使处理器1102B散列接收到的消息的一个或多个数据字段(例如,与访问装置1102相关联的标识信息、与用户装置102相关联的标识信息、支付数据和/或交易信息、用户装置102的证书及类似物)以产生额外散列值。在一些实施例中,验证模块1102J可以被配置成使处理器1102B将从数字签名检取的散列值与计算的散列值进行比较。如果散列值匹配,那么验证模块1102J可以激励数据处理模块1102H(或另一合适的模块)执行操作(例如,将包括接收到的消息数据的至少一部分的消息传送到另一装置,例如图12的资源提供商计算机1230)。

[0141] 在一些实施例中,如果散列值匹配,那么验证模块1102J可以确定消息是有效的

(例如,未改变)。在一些实施例中,验证模块1102J可以被配置成使处理器1102B从从用户装置(或从介入装置)接收的消息检取用于向用户装置102传送消息的访问装置的公钥。验证模块1102J可以被配置成使处理器1102B确定接收到的消息中包括的访问装置的公钥是否匹配曾用于向用户装置的过去传送的存储于加密数据1102K中的访问装置的公钥。如果公钥匹配,那么验证模块1102J可以被配置成使处理器1102B确定消息是有效的(例如,未改变)且导致接收到的消息的先前传送的消息由用户装置(例如,用户装置102)利用正确的公钥(例如,与先前传送的消息相关联的存储于加密数据1102K中的公钥)验证。在一些实施例中,如果消息被确定为无效(例如,已改变,至少部分地基于检取的散列与计算的散列的比较),和/或接收到的消息的公钥不匹配存储于加密数据1102K中且与向用户装置102的前一消息传送相关联的公钥,那么验证模块1102J可以终止交互且不执行与传送装置的进一步处理。

[0142] 上述用于防止中继攻击的系统和方法可以在任何合适的交易或交互过程中使用。举例来说,它们可以在支付过程或访问交易中使用。下文结合图12和13进一步详细描述这些实例。

[0143] 图12示出可使用用户装置102的交易处理系统的框图1200。图12示出可操作用户装置1210(例如,图1-10的用户装置102的实例、图10的用户装置1002等)的用户1206。用户1206可以使用用户装置1210在例如商家的资源提供商处为商品或服务支付。商家可以操作资源提供商计算机1230和/或访问装置1220(例如,图1-10的访问装置104-1和/或访问装置1102的实例)。商家可以经由由收单方操作的传输计算机1240和例如支付处理网络的处理网络1250与由发行方操作的授权实体计算机1260通信。

[0144] 支付处理网络可以包括用以支持和递送授权服务、异常文件服务以及清算和结算服务的数据处理子系统、网络和操作。示例性支付处理网络可以包括VisaNet™。例如VisaNet™等支付处理网络能够处理信用卡交易、借记卡交易和其它类型的商业交易。确切地说,VisaNet™包括处理授权请求的VIP系统(Visa集成支付系统)以及执行清算和结算服务的Base II系统。支付处理网络可以使用任何合适的有线或无线网络,包括因特网。

[0145] 可以如下描述在访问装置1220(例如,POS位置)使用用户装置1210的典型支付交易流程。用户1206向访问装置1220呈现他的用户装置1210以为物品或服务支付。用户装置1210和访问装置1220可以经由BLE通信协议交互。在一些实施例中,可以在用户装置1210与访问装置1220之间交换数据(例如,标识信息、公钥、证书、位置信息、交互数据等)。从访问装置1220传送到用户装置1210的数据可以由访问装置1220以上文所描述的方式以数字方式签署且由用户装置1210验证。类似地,从用户装置1210传送的数据可以由用户装置1210以上文所描述的方式以数字方式签署且由访问装置1220验证。如果允许交互且在装置之间交换的消息数据被验证为未改变,那么与交互有关的数据(例如,访问装置1220的标识数据、用户装置1210的标识数据、支付信息、图5的消息数据502或任何合适的数据)可以传送到资源提供商计算机1230。

[0146] 资源提供商计算机1230可以经由外部通信接口从访问装置1220接收此信息。资源提供商计算机1230可以随后生成包括从访问装置1220接收的信息的授权请求消息,且将此信息以电子方式传送到传输计算机1240。传输计算机1240可以随后接收、处理和转发授权请求消息到处理网络1250以用于授权。

[0147] 大体来说，在贷记或借记卡交易的发生之前，处理网络1250已经关于发行方的交易将如何被授权与每一发行方建立协议。在一些情况下，例如当交易金额低于阈值时，处理网络1250可以被配置成基于其具有的关于用户账户的信息而授权交易，而无需生成和传送授权请求消息到授权实体计算机1260。在其它情况下，例如当交易金额高于阈值时，处理网络1250可以接收授权请求消息，确定与用户装置1210相关联的发行方，且将用于交易的授权请求消息转发到授权实体计算机1260以用于验证和授权。一旦交易被授权，授权实体计算机960就可以生成授权响应消息(可以包括指示交易被批准或拒绝的授权代码)且经由其外部通信接口将此电子消息传送到处理网络1250。处理网络1250可以随后将授权响应消息转发到传输计算机1240，所述传输计算机又可以随后将包括授权指示的电子消息传送到资源提供商计算机1230，然后到访问装置1220。访问装置1220可以至少部分地基于接收到授权响应消息(例如，接收到指示交易被批准的授权响应消息)而提供对商品和/或服务的访问。

[0148] 在一天结束时或在某一其它合适的时间间隔，可以在交易上执行资源提供商计算机1230、传输计算机1240、处理网络1250和授权实体计算机1260之间的清算和结算过程。

[0149] 图13示出建筑物访问系统的框图。图13示出由用户1306操作的用户装置1310(例如，图1的用户装置102)。用户装置1310可以具备如上文所描述的证书。用户装置1310可与访问装置1320(例如，图1的访问装置104-1的实例)交互且将访问数据传递到访问装置1320。访问装置1320可以被配置成生成公钥/私钥。可以对由访问装置1320传送的广告和/或任何合适的消息数据(例如，访问装置1320的标识符、访问装置1320的位置、交互数据等)进行散列且使用私钥来签署所得散列值。访问装置1320可以在同一消息或不同消息中将公钥和数字签名提供到用户装置1310。用户装置1310可以利用提供的公钥(或在中继攻击的情况下从另一访问装置接收的公钥)来验证消息。如果消息是无效的，那么用户装置1310可以终止与访问装置1320的交互。如果消息是有效的，那么用户装置1310可以利用额外消息数据(例如，访问装置1320的位置)来执行距离检查，且如果用户装置1310的距离在到访问装置1320的位置的阈值距离之外则终止交互)。如果消息是有效的，那么可以向用户装置1310的用户呈现确认与访问装置1320的交互的选项。如果被确认，那么用户装置1310可以将消息传送回到访问装置1320。

[0150] 在一些实施例中，由用户装置1310传送到访问装置1320的消息的消息数据可以包括与用户装置1310相关联的证书、访问装置1320的标识符，以及用于验证原始接收的消息的公钥。在一些实施例中，可以对访问装置1320的标识符和公钥进行散列且利用与用户装置1310相关联的私钥以数字方式签署。在接收到时或在任何合适的时间，访问装置1320可以利用与发出证书的认证机构相关联的公钥从证书检取用户装置1310的公钥。利用检取的公钥，访问装置1320可以利用由用户装置1310提供的数字签名来验证消息。作为验证的部分，访问装置1320可以至少部分地基于确定在消息中提供的公钥未改变(例如，利用消息的数字签名可确定)且提供的公钥匹配于由访问装置1320存储的公钥而验证其公钥由用户装置1310用于验证原始传送的消息。如果访问装置1320确定从用户装置1310接收的消息数据是有效的，那么访问装置1320可以随后前进到让用户1306进入建筑物1330。然而，如果访问装置1320确定用户装置1310使用错误的公钥用于验证，或消息数据中的任一个被改变(例如，使用数字签名可确定)，那么访问装置1320可以终止与用户装置1310的交互，且可以不

对用户1306给予建筑物1330的访问权。

[0151] 技术益处

[0152] 本发明的实施例实现若干优点。举例来说，通过配置所公开的访问装置以生成其自身的公钥/私钥，系统可以提供增强的验证功能性而不会带来证书颁发中心的额外密钥维护开销。利用本文公开的各种方法，用户装置102可以被配置成利用数字签名和公钥验证来自交互装置(例如，访问装置)的交互数据。通过此验证，用户装置102可以被配置成确定何时消息已改变，且可以被配置成自动拒绝和/或终止与访问装置的交互。这些技术可以确保用户装置102不将支付信息提供到介入装置。即使一个或多个介入装置将拦截消息且将消息中继到用户装置102，本文所公开的技术也使用户能够检测到正从并非用户确认连接到的装置的装置接收数据。可以为用户提供取消和/或终止交互的能力。即使当用户无法辨识差异时，用户装置102也可以当将数据传送回到访问装置(例如，潜在地无意中通过一个或多个介入装置)时以数字方式签署其交互数据(例如，包括其支付数据)。接收访问装置可以随后利用与用户装置相关联的公钥验证消息内的数据以确保：1)消息未改变，和2)利用与访问装置相关联的正确公钥验证传送到用户装置的原始消息。以此方式，增强了数据安全性，防止原本使欺诈者能够访问敏感信息(例如，支付数据)以用于欺诈性目的的中继攻击和/或中间人攻击。

[0153] 应理解，如上文描述的本发明可以以模块化或集成方式使用计算机软件以控制逻辑的形式来实现。基于本公开和本文中所提供的教示，所属领域的普通技术人员将知道并且了解使用硬件和硬件与软件的组合来实施本发明的其它方式和/或方法。上文提及的实体中的任何实体都可以操作被编程为执行文中描述的功能的计算机。

[0154] 本申请中描述的任何软件组件、流程或功能可使用任何合适的计算机语言(例如，使用诸如常规的或面向对象的技术的Java、C++或Perl)实施为由处理器执行的软件代码。软件代码可以被存储为计算机可读介质(例如，随机存取存储器(RAM)、只读存储器(ROM)、磁介质(例如硬盘驱动器或软盘)或光介质(例如CD-ROM))上的一系列指令或命令。任何这样的计算机可读介质可以驻留在单个计算设备上或内部，并且可以存在于系统或网络内的不同计算设备上或内部。

[0155] 附图中所描绘或上文所描述的组件的不同布置以及未示出或描述的组件和步骤是可能的。一些特征和子组合是有用的，并且可以不参照其它特征和子组合而使用。本发明的实施例已经出于说明性和不限定性目的描述，并且替代实施例将对于此专利的读者变得显而易见。因此，本发明不限于上文描述或附图中描绘的实施例，并且可以在不脱离随附权利要求书的范围的情况下做出各种实施例和修改。

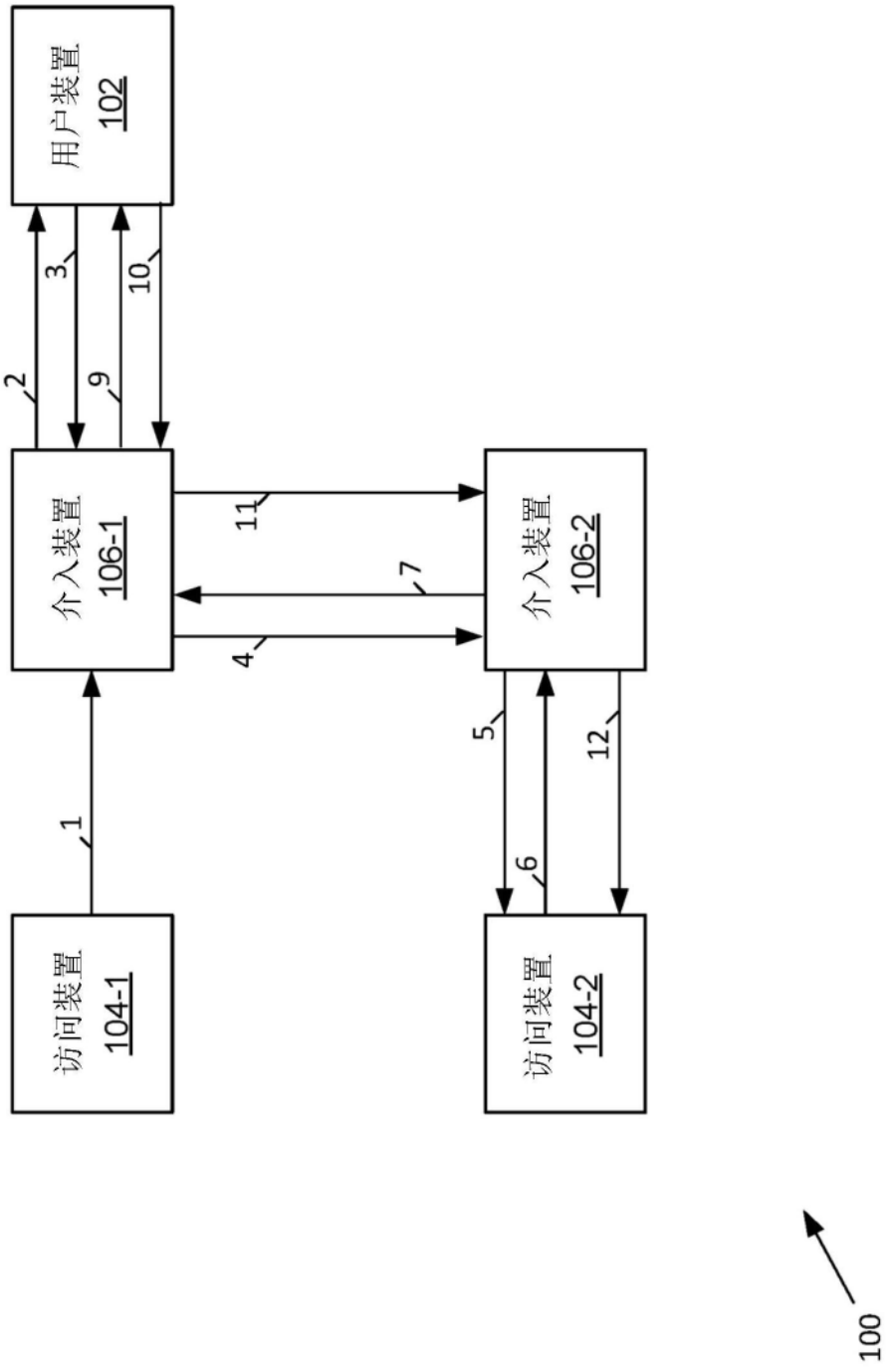

用户装置
102
介入装置
106-1
介入装置
106-2
访问装置
104-1
访问装置
104-2
1
2
3
4
5
6
7
9
10
11
12
100

图1


200
202
连接到访问装置 1、终端 1?
204
OK
取消
206

图2

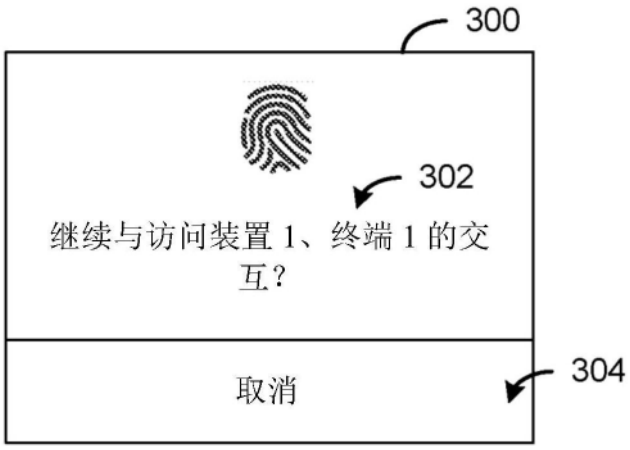

300
302
继续与访问装置 1、终端 1 的交互?
取消
304

图3

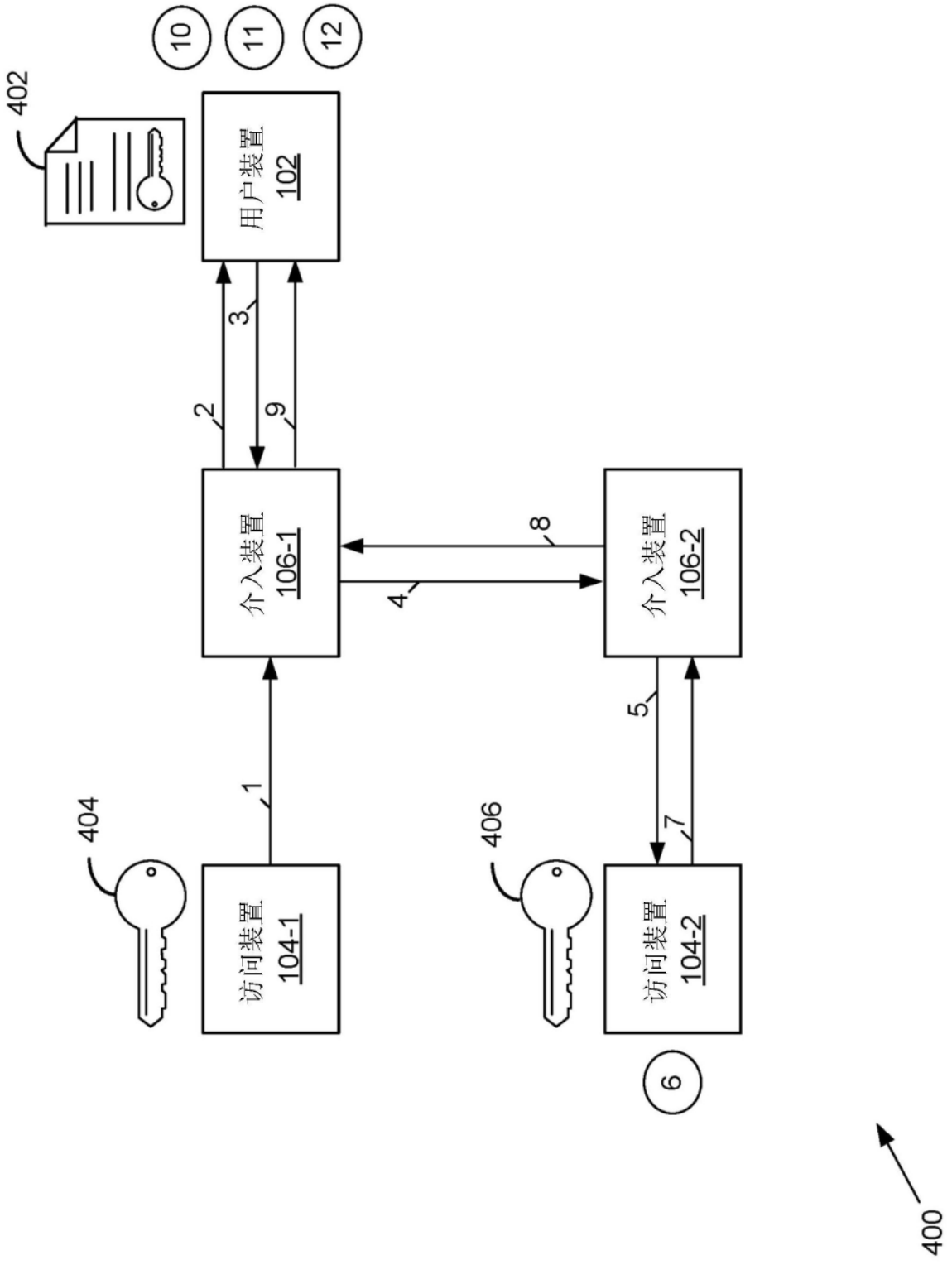

10
11
12
402
用户装置
102
3
2
9
介入装置
106-1
8
介入装置
106-2
4
5
1
404
406
7
访问装置
104-1
访问装置
104-2
6
400

图4

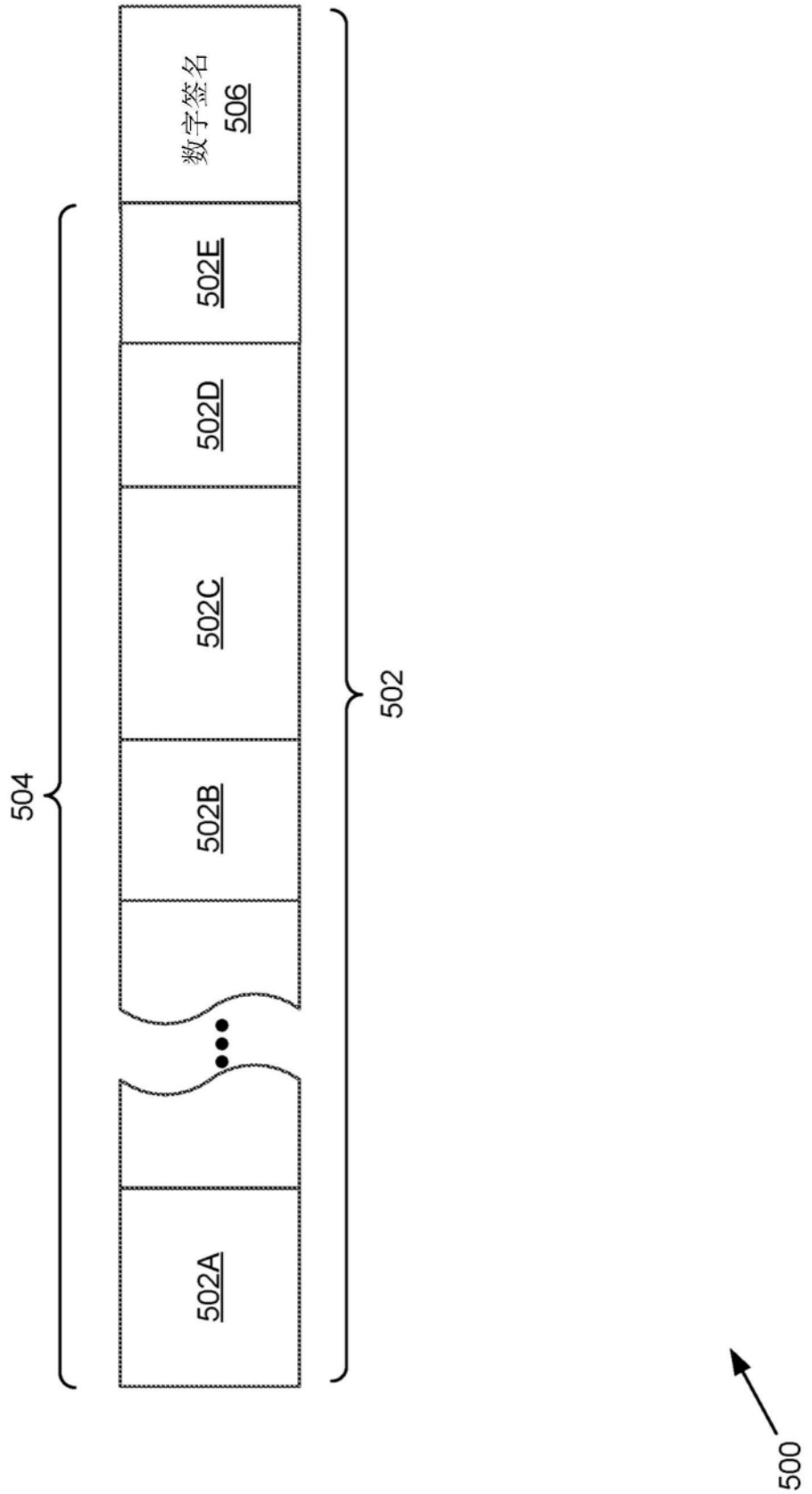


图5

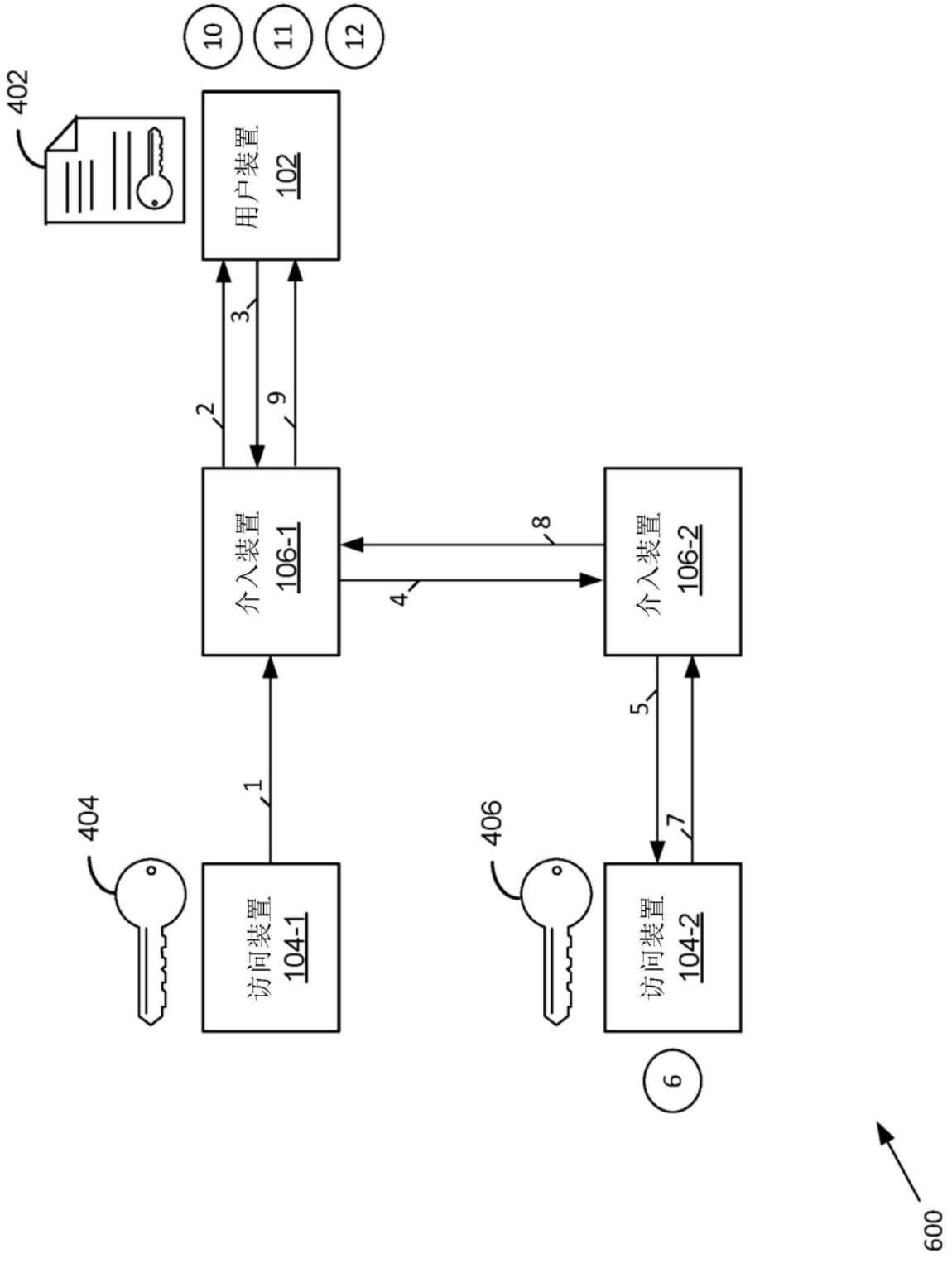

10
11
12
402
用户装置
102
3
2
9
介入装置
106-1
8
4
介入装置
106-2
5
404
1
406
7
访问装置
104-1
访问装置
104-2
6
600

图6

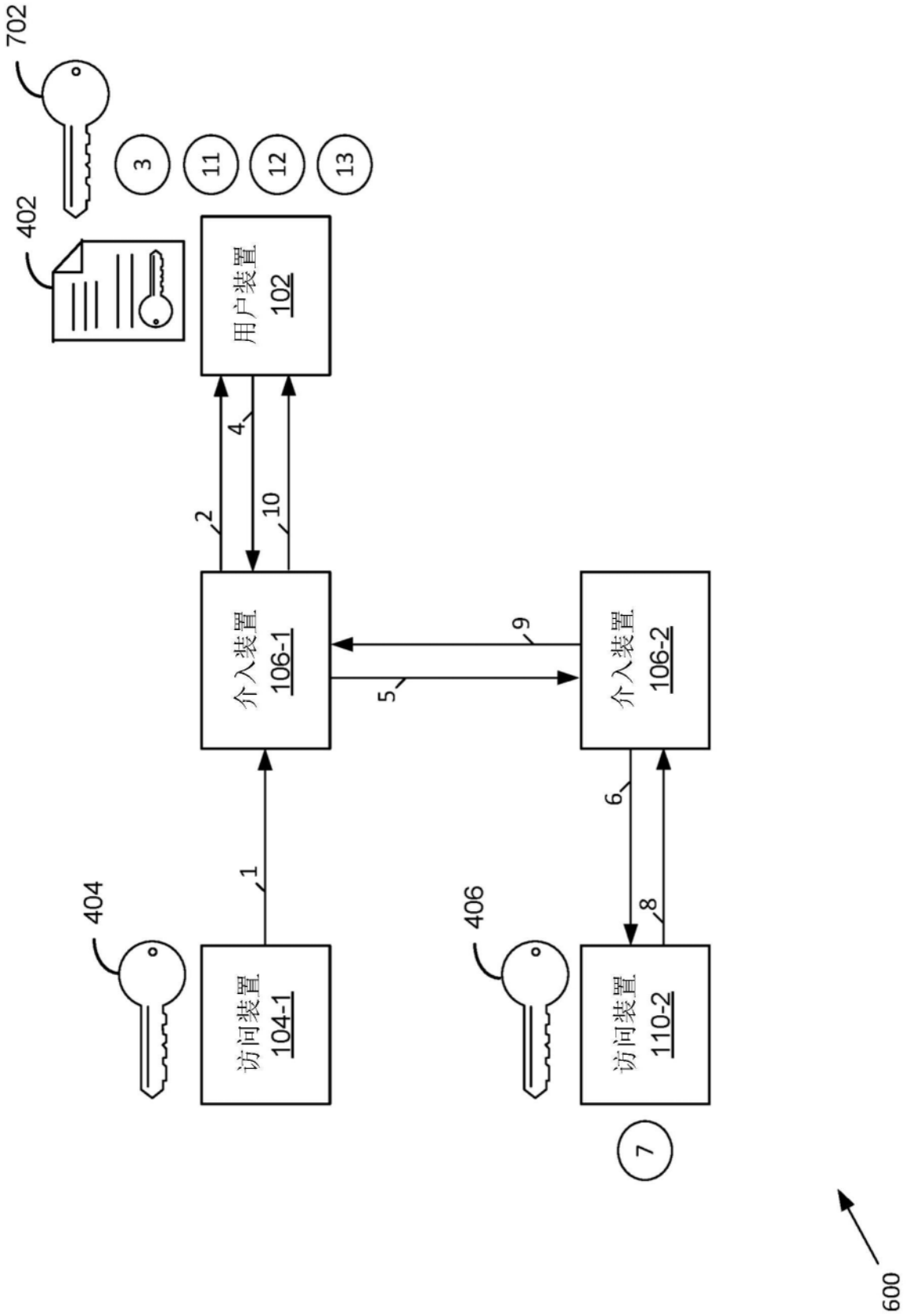

702
3
11
12
13
402
用户装置
102
4
2
10
介入装置
106-1
9
介入装置
106-2
5
6
1
404
406
8
访问装置
104-1
访问装置
110-2
7
600

图7

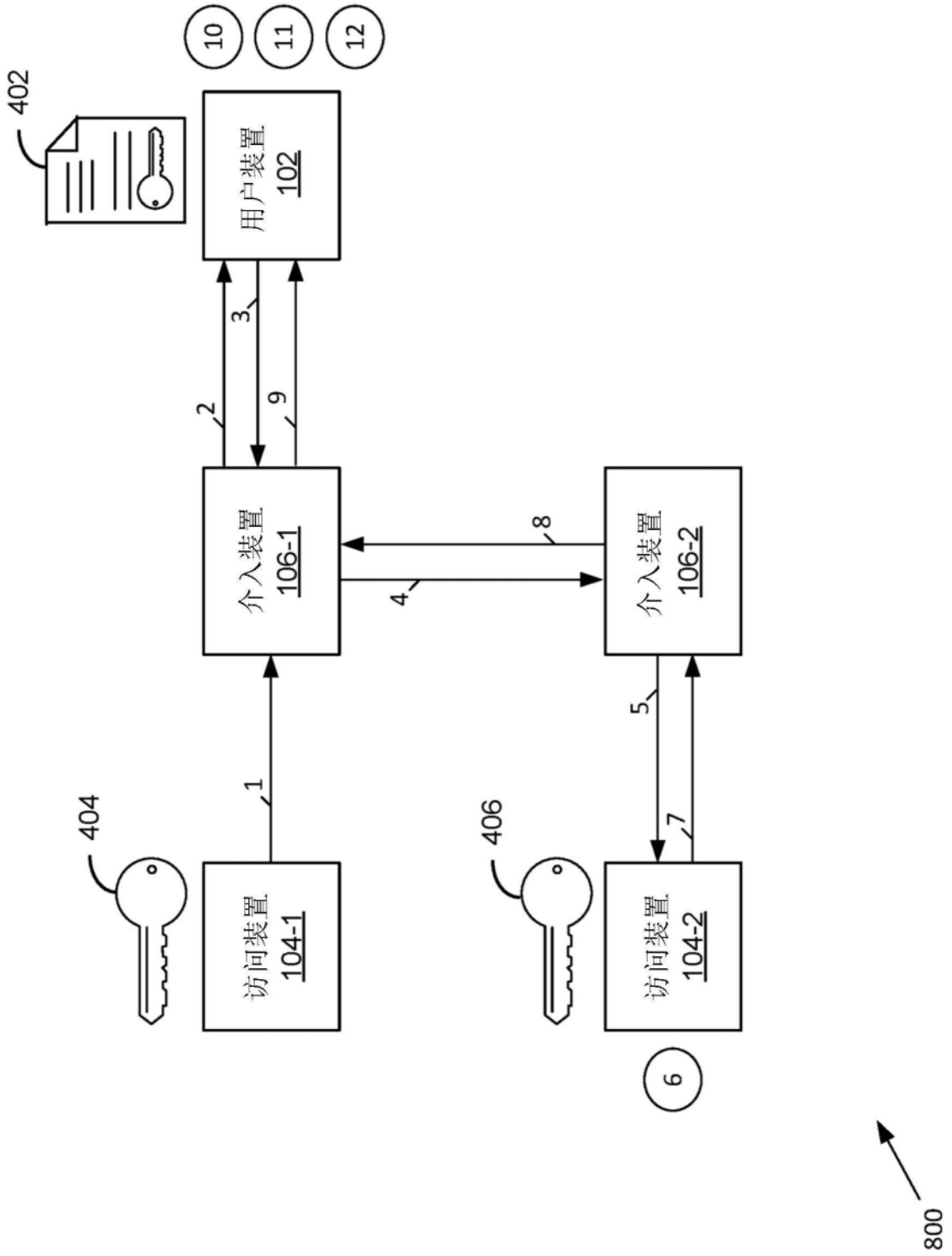

10
11
12
402
用户装置
102
3
2
9
介入装置
106-1
8
介入装置
106-2
4
5
1
404
406
7
访问装置
104-1
访问装置
104-2
6
800

图8

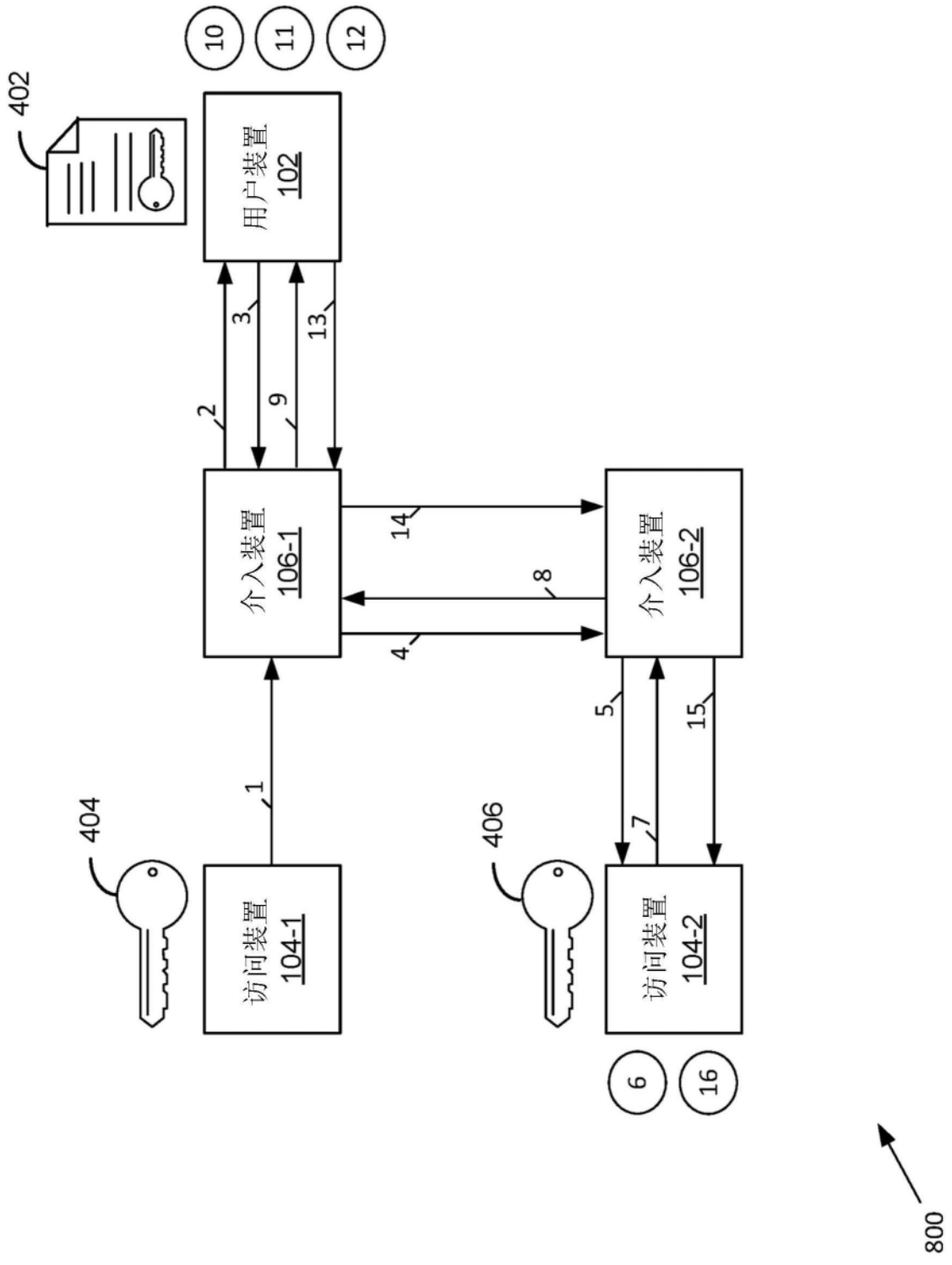

10
11
12
402
用户装置
102
3
13
2
9
介入装置
106-1
14
8
介入装置
106-2
4
5
15
1
404
406
7
访问装置
104-1
访问装置
104-2
6
16
800

图9

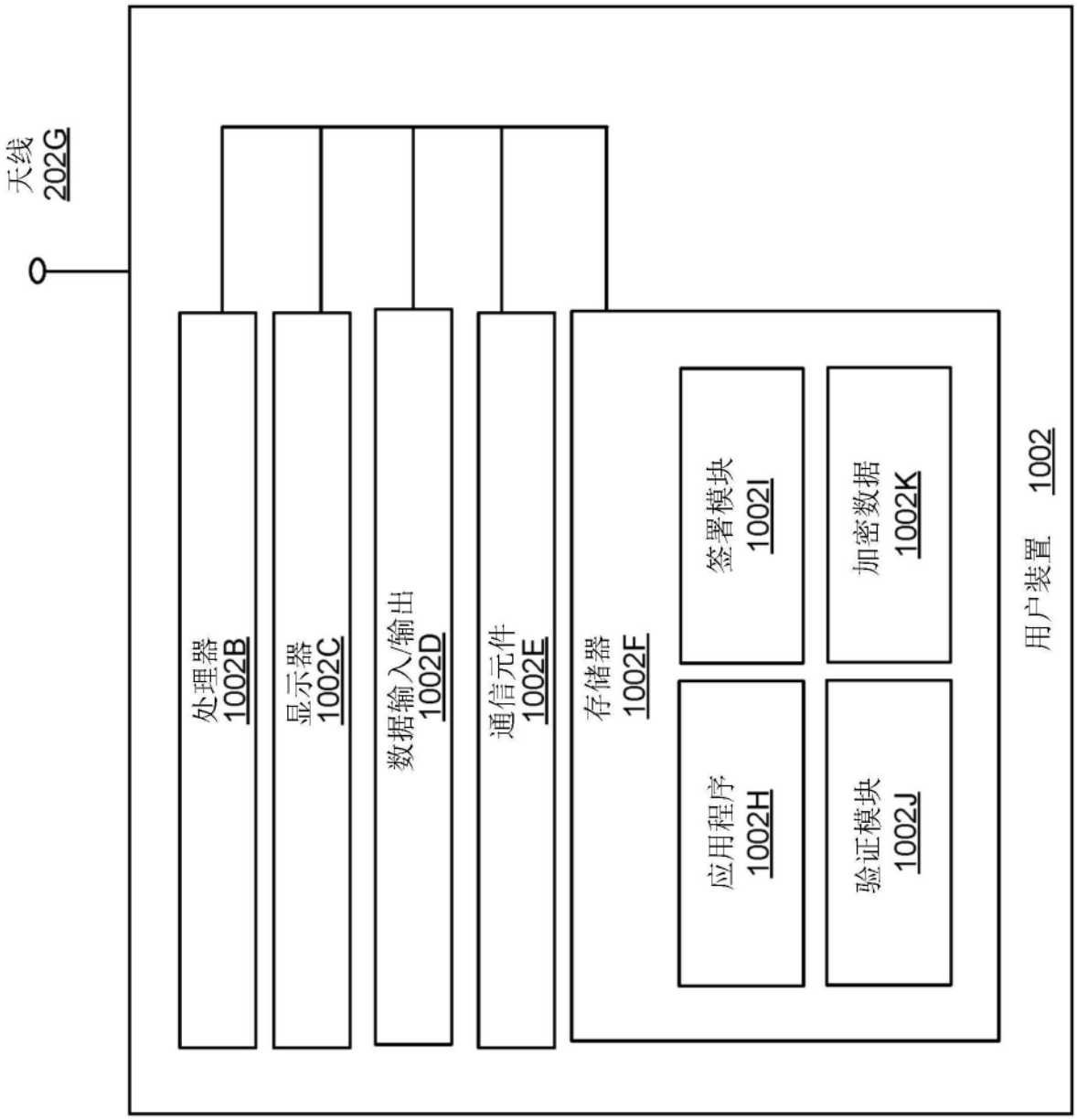

天线
202G
处理器
1002B
显示器
1002C
数据输入/输出
1002D
通信元件
1002E
存储器
1002F
应用程序
1002H
签署模块
1002I
验证模块
1002J
加密数据
1002K
用户装置 1002

图10

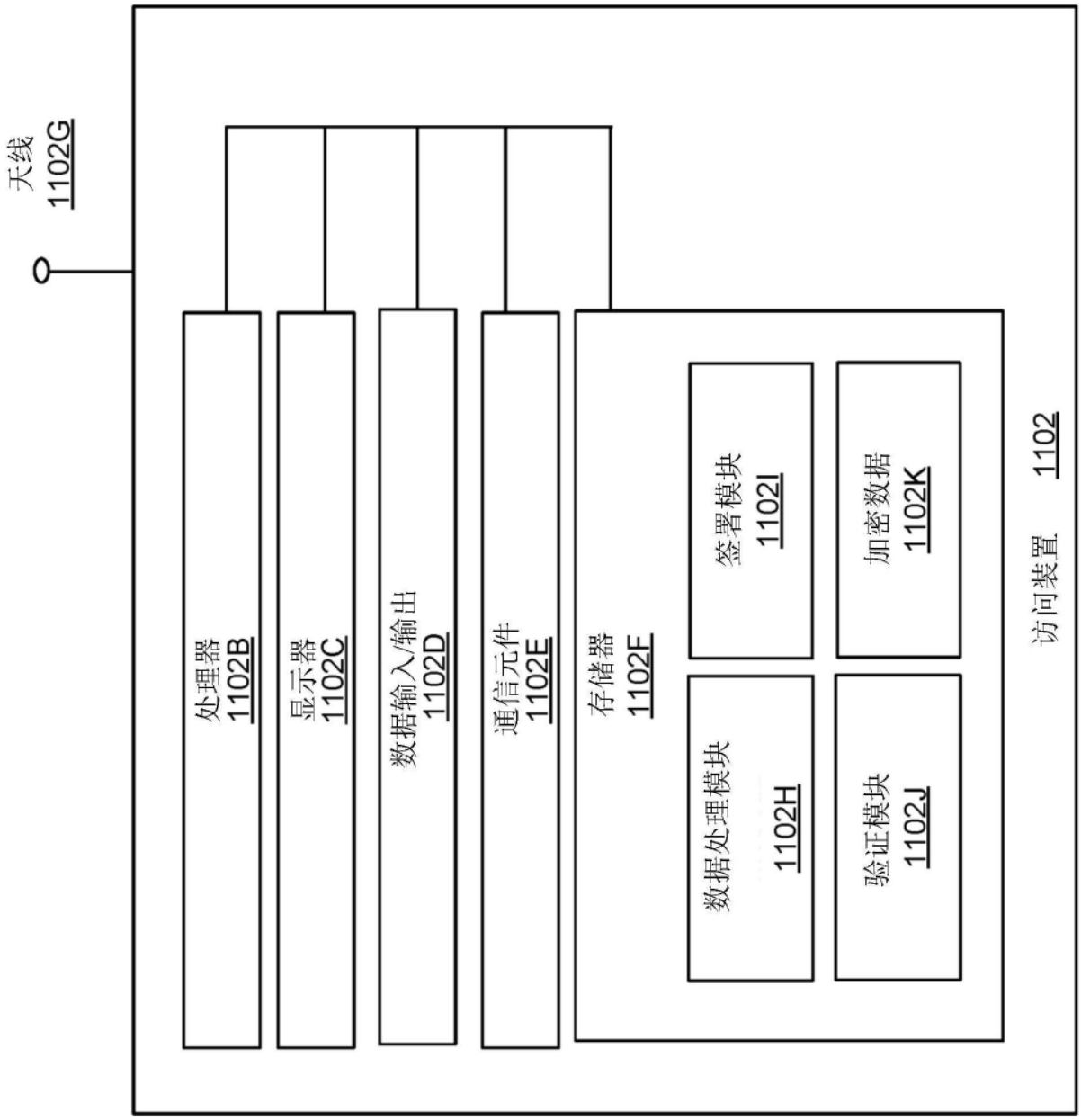

天线
1102G
处理器
1102B
显示器
1102C
数据输入/输出
1102D
通信元件
1102E
存储器
1102F
数据处理模块
1102H
签署模块
1102I
验证模块
1102J
加密数据
1102K
访问装置 1102

图11

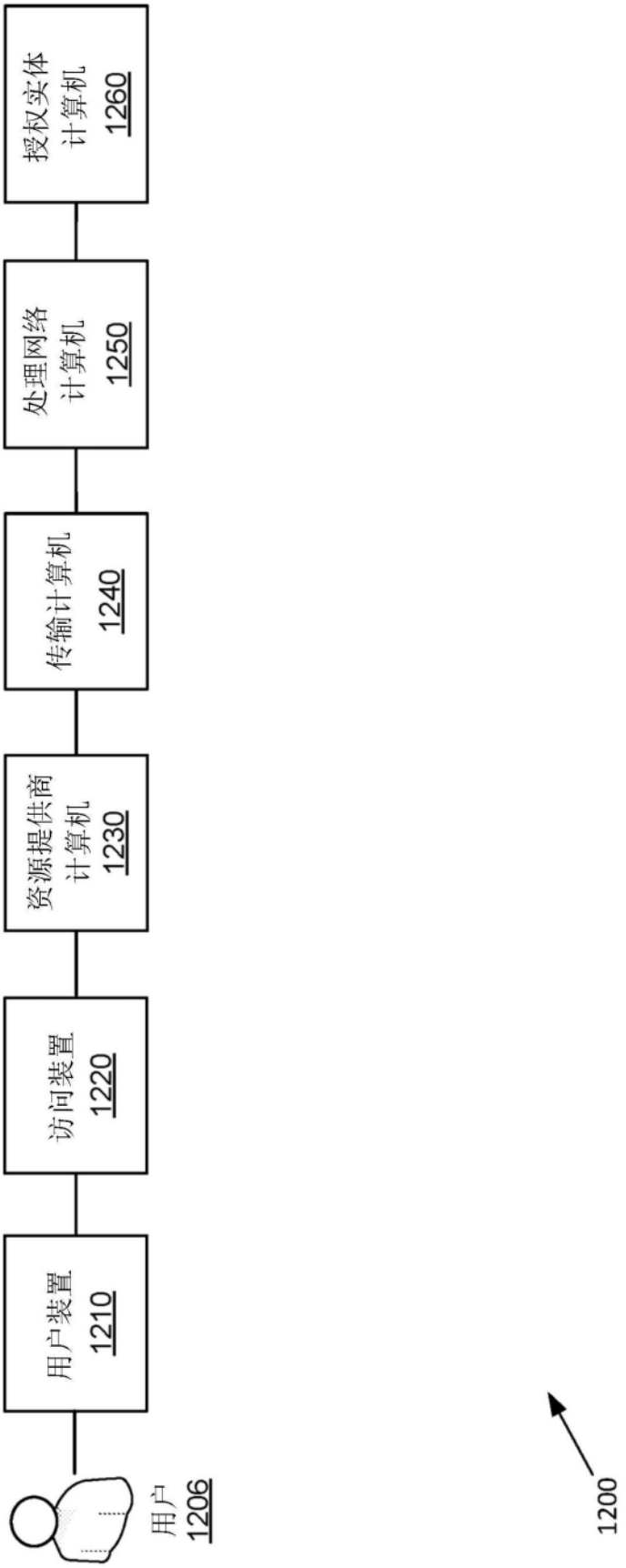

用户
1206
用户装置
1210
访问装置
1220
资源提供商
计算机
1230
传输计算机
1240
处理网络
计算机
1250
授权实体
计算机
1260
1200

图12

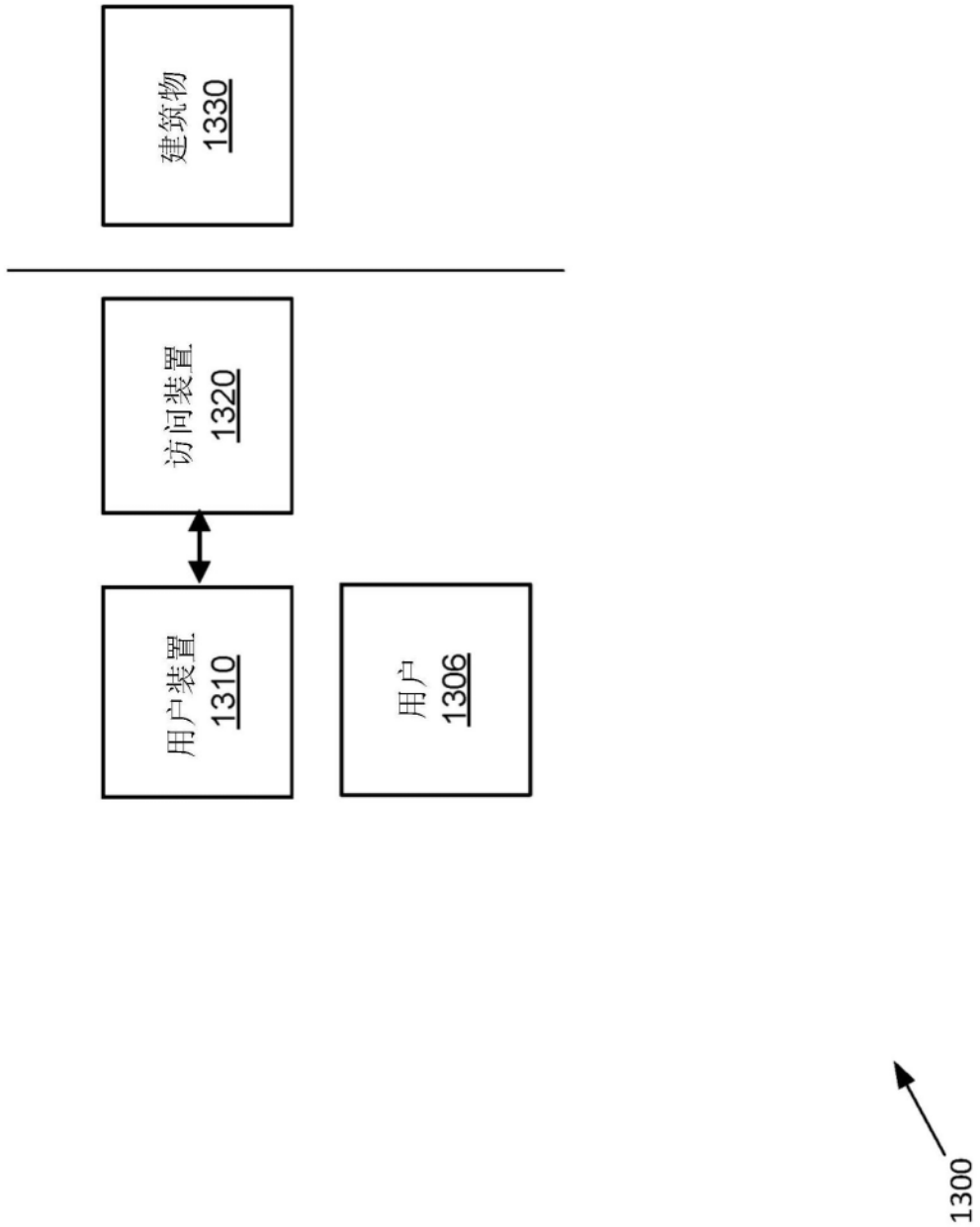


图13